Troubleshoot ASA Smart License on FXOS Firepower Appliances

Contents

- Introduction
- Background Information
  - Smart Licensing Architecture
  - Overall Architecture
    - Nomenclature
    - Smart Agent States
    - ASA Entitlements
- Configuration
  - Failover (High Availability)
    - Case Study: ASA HA License on FP2100
    - ASA Cluster
- Verification and Debugging
  - Chassis (MIO) Sample Outputs of Verification Commands
  - ASA Sample Outputs of Verification Commands
    - Successful Registration
    - Expired Authorization
  - Sample Outputs from Chassis CLI
    - Unregistered
    - Registration in Progress
    - Registration Error
    - Evaluation Period
- Common License Problems on FXOS Chassis (MIO)
  - Registration Error: Invalid Token
    - Recommended Steps
    - Registration Error: Product Already Registered
    - Recommended Steps
    - Registration Error: Date Offset Beyond the Limit
    - Recommended Step
    - Registration Error: Failed to Resolve Host
    - Recommended Steps
    - Registration Error: Failed to Authenticate Server
    - Recommended Steps
  - CLI Verification
    - Registration Error: HTTP Transport Failed
    - Recommended Steps
    - Registration Error: Could Not Connect to Host
    - Recommended Steps
    - Registration Error: HTTP Server Returns Error Code >= 400
    - Recommended Steps
    - Registration Error: Parse Backend Response Message Failed
    - Recommended Steps
  - License Issues on ASA - 1xxx/21xx Series

Registration Error: Communication Message Send Error
Recommended Steps
Special Requirements for Add-on Entitlements
Entitlement State During Reboot Operation
Engage Cisco TAC Support
FP41xx/FP9300
FP1xxx/FP21xx
Frequently Asked Questions (FAQs)
Related Information

Introduction

This document describes the Adaptive Security Appliance (ASA) Smart Licensing feature on Firepower eXtensible Operating System (FXOS).

Background Information

Smart Licensing on Firepower eXtensible Operating System (FXOS) is used when there is an ASA installed on the chassis. For Firepower Threat Defense (FTD) and Firepower Management Center (FMC) Smart Licensing, review the how to Use FMC and FTD Smart License Registration and Common Issues to Troubleshoot Guide.

This document mainly covers the scenarios where the FXOS chassis has direct internet access. If your FXOS chassis cannot access the internet, you must consider either a Satellite Server or a Permanent License Reservation (PLR). Check the FXOS configuration guide for more details on Offline Management.

Smart Licensing Architecture

A high-level overview of the chassis components:

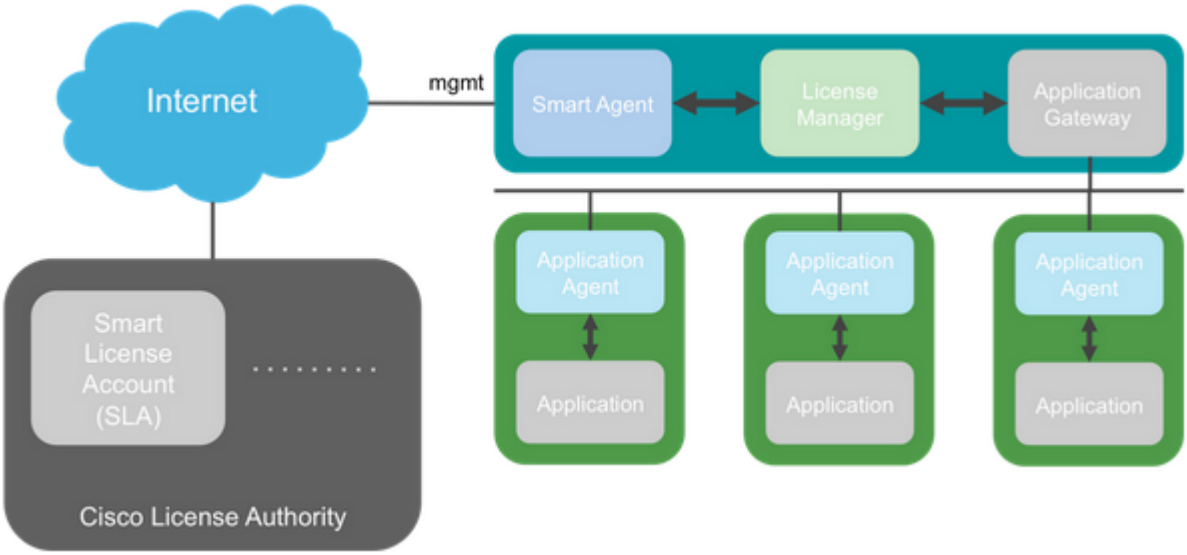


- Both Management Input/Output (MIO) and individual modules play roles in Smart Licensing.
- MIO does not require any licenses to operate.
- SA Application(s) on each module must be licensed

The FXOS supervisor is the MIO. and the MIO contains three main components:

- Smart Agent
- License Manager
- AppAG

Overall Architecture



Nomenclature

Term	Description
Cisco License Authority	The backend Cisco license for Smart Licensing. Maintains all product licensing-related information. This includes entitlements and device information.
Smart License Account	An account that has all entitlements for the appliance.
Token ID	An identifier used to distinguish the Smart License Account when the appliance is registered.
Entitlement	Equivalent to a license. Corresponds to an individual feature or an entire feature tier.
Product Activation Key (PAK)	The older licensing mechanism tied to a single appliance.

Smart Agent States

State	Description
Un-Configured	Smart licensing is not enabled.
Un-Identified	Smart licensing has been enabled, but the Smart Agent has not yet contacted Cisco to register.
Registered	The agent has contacted the Cisco licensing authority and registered.
Authorized	When an agent receives an in-compliance status in response to an entitlement authorization request.
Out Of Compliance (OOC)	When an agent receives an OOC status in response to an Entitlement Authorization request.
Authorization Expired	If the agent has not communicated with Cisco for 90 days.

ASA Entitlements

These are the supported ASA entitlements:

- Standard Tier
- Multi-Context
- Strong Encryption (3DES)
- Mobile/Service Provider (GTP)

Configuration

Use the instructions from these documents:

- Smart Software Licensing (ASAv, ASA on Firepower)
- License Management for the ASA

Before any feature tier configuration:

<#root>

asa(config-smart-lic)#

show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Invalid (0)

No entitlements in use

Serial Number: FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces   : Unlimited

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

*******************************************************************************



*                              WARNING                                        *



*                                                                             *



*    THIS DEVICE IS NOT LICENSED WITH A VALID FEATURE TIER ENTITLEMENT        *



*                                                                             *



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

Configure standard tier:

<#root>

asa(config)#

license smart

```
INFO: License(s) corresponding to an entitlement will be activated only after an entitlement request ha
asa(config-smart-lic)#
```

feature tier standard

```
asa(config-smart-lic)#
```

show license all

```
Smart licensing enabled: Yes

Compliance status: In compliance
```

Overall licensed status: Authorized (3)

```
Entitlement(s):

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

Serial Number: FCH12345ABC

License mode: Smart Licensing

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

Failover (High Availability)

As is documented in the ASA Configuration Guide, each Firepower unit must be registered with the License Authority or satellite server.

Verification from the ASA CLI:

```
<#root>

asa#

show failover | include host



        This host: Primary - Active


        Other host: Secondary - Standby Ready

asa#

show license all



Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

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

Serial Number:  FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
```

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

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

The standby unit:

<#root>

```
asa#
```

show failover | i host

This host: Secondary - Standby Ready

```
        Other host: Primary - Active
asa#
```

show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Not applicable in standby state

No entitlements in use

Serial Number: FCH12455DEF

License mode: Smart Licensing

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

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

Case Study: ASA HA License on FP2100

- On 2100, the ASA communicates with the Cisco Smart Licensing portal (cloud) through the ASA interfaces, not the FXOS management.
- You must register both ASAs to the Cisco Smart Licensing portal (cloud).

In this case, HTTP local authentication is used on an outside interface:

<#root>

```
ciscoasa(config)#
```

show run http

```
http server enable
http 0.0.0.0 0.0.0.0 outside
ciscoasa(config)#
```

show run aaa

```
aaa authentication http console LOCAL
ciscoasa(config)#
```

show run username

```
username cisco password ***** pbkdf2
```

You can only connect to the ASA via ASDM if there is a 3DES/AES license enabled. For an ASA that is not already registered, this is only possible on an interface that is management-only. Per the configuration guide, "Strong Encryption (3DES/AES) is available for management connections before you connect to the License Authority or Satellite server so you can launch ASDM. Note that ASDM access is only available on management-only interfaces with the default encryption. Through-the-box traffic is not allowed until you connect and obtain the Strong Encryption license."

In a different case you receive:

<#root>

```
ciscoasa(config)#
```

debug ssl 255

```
debug ssl enabled at level 255.
error:1408A0C1:SSL routines:ssl3_get_client_hello:

no shared cipher
```

To overcome the ASA, management-only is configured on the internet-facing interface, and thus ASDM connection is possible:

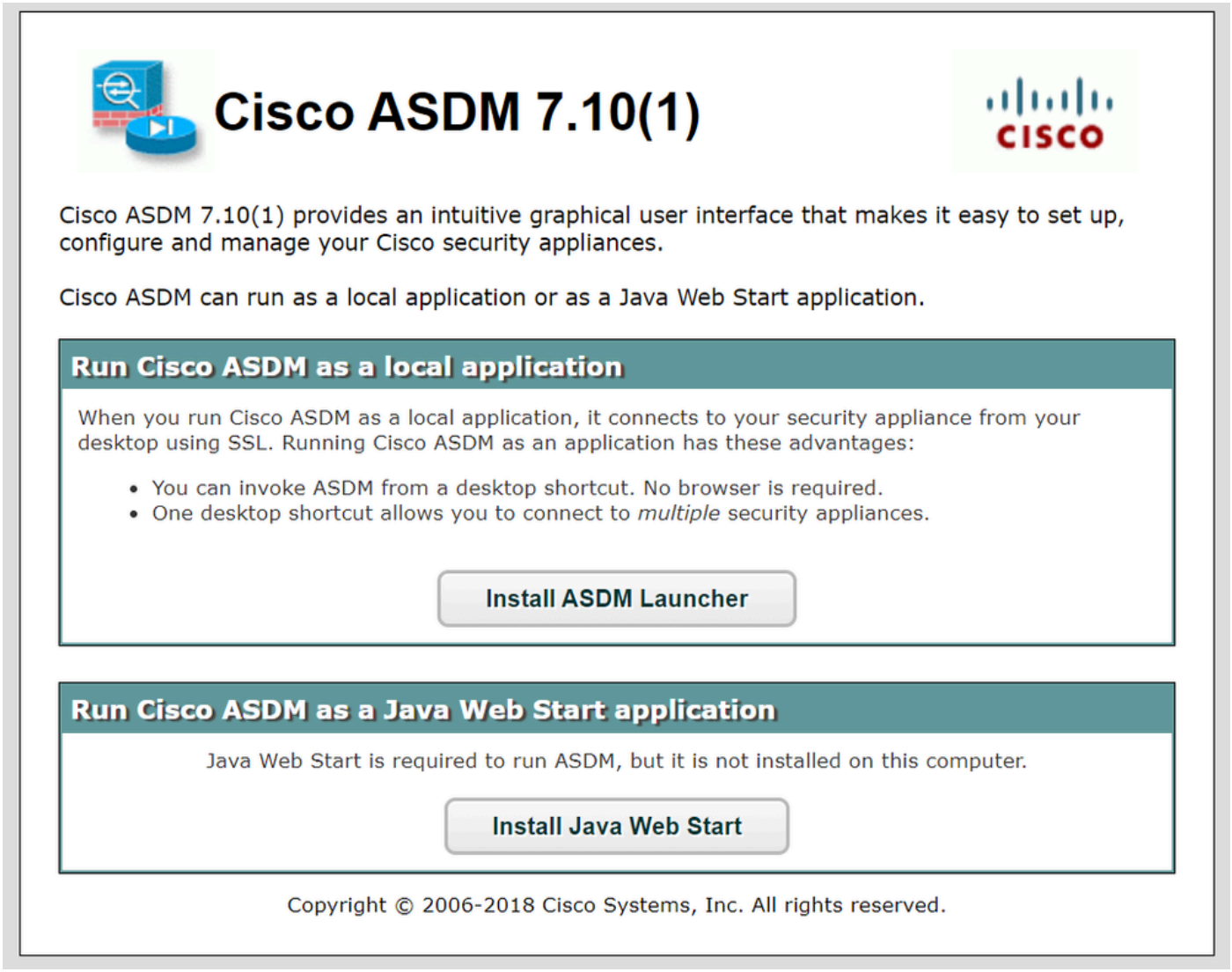
<#root>

```
interface Ethernet1/2

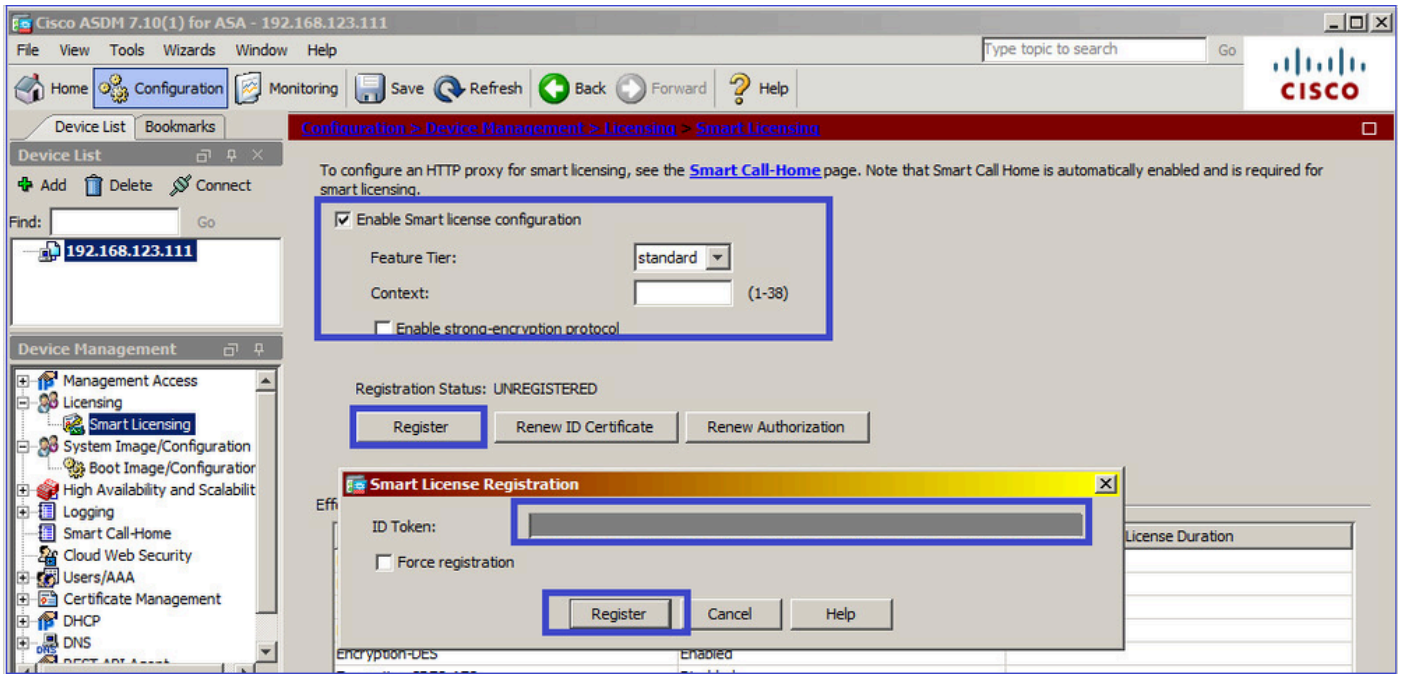
management-only


nameif outside
security-level 100

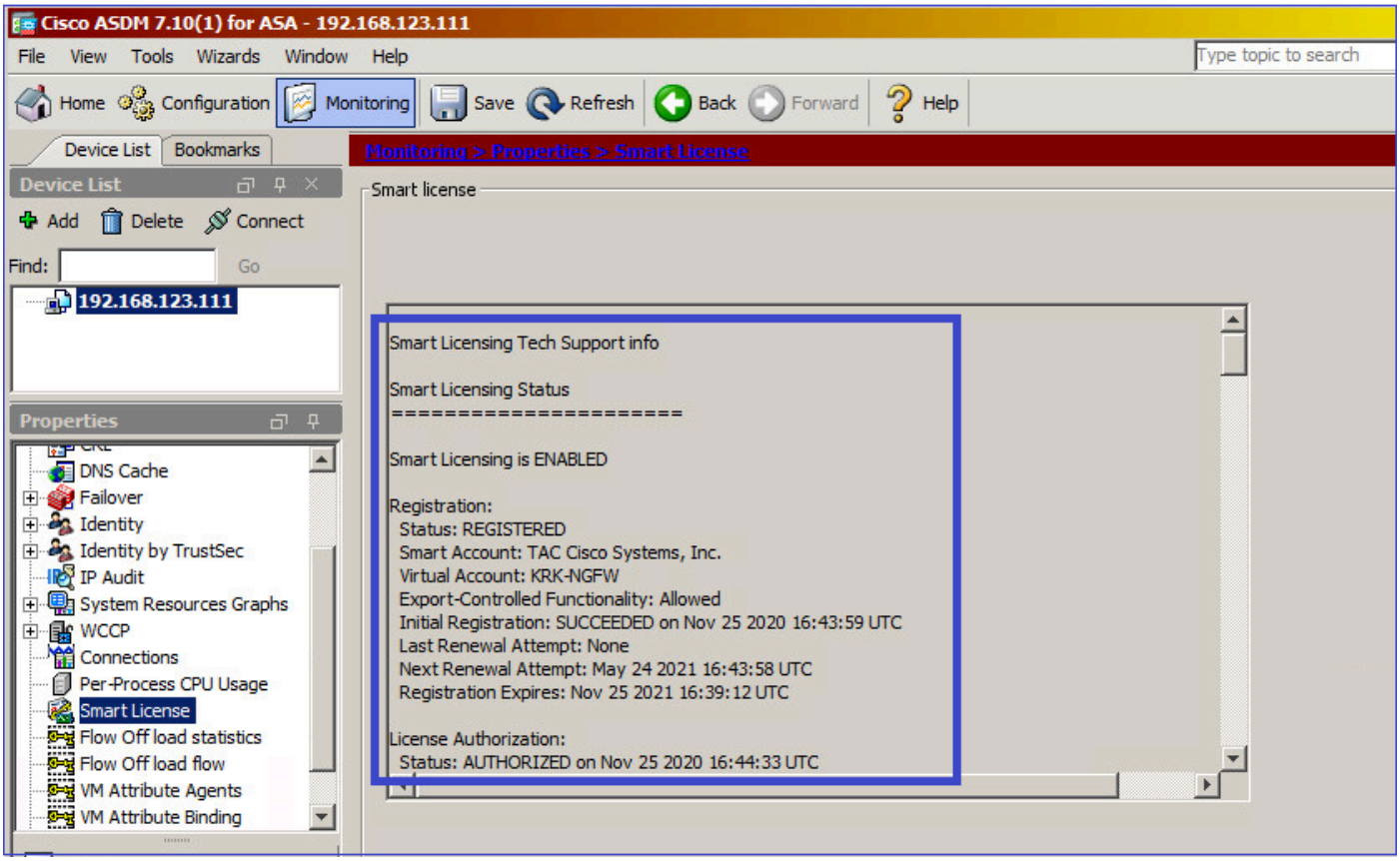
ip address 192.168.123.111 255.255.255.0 standby 192.168.123.112
```



Configure the Smart Licensing on Primary ASA:



Navigate to **Monitoring > Properties > Smart License** to check the status of the registration:



Primary ASA CLI verification:

<#root>

ciscoasa/pri/act#

show license all

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

Smart Licensing is ENABLED

Registration:
Status: REGISTERED
Smart Account: Cisco Systems, Inc.
Virtual Account: NGFW
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Nov 25 2020 16:43:59 UTC
Last Renewal Attempt: None
Next Renewal Attempt: May 24 2021 16:43:58 UTC
Registration Expires: Nov 25 2021 16:39:12 UTC

License Authorization:
Status: AUTHORIZED on Nov 25 2020 16:47:42 UTC
Last Communication Attempt: SUCCEEDED on Nov 25 2020 16:47:42 UTC
Next Communication Attempt: Dec 25 2020 16:47:41 UTC
Communication Deadline: Feb 23 2021 16:42:46 UTC

Utility:
Status: DISABLED

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

Transport:
Type: Callhome

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

Firepower 2100 ASA Standard (FIREPOWER_2100_ASA_STANDARD):
Description: Firepower 2100 ASA Standard
Count: 1
Version: 1.0
Status: AUTHORIZED

Product Information
===================
UDI: PID:FPR-2140,SN:JAD12345ABC

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

ciscoasa/pri/act#

show run license

```
license smart
feature tier standard
```

<#root>

```
ciscoasa/pri/act#
```

show license features

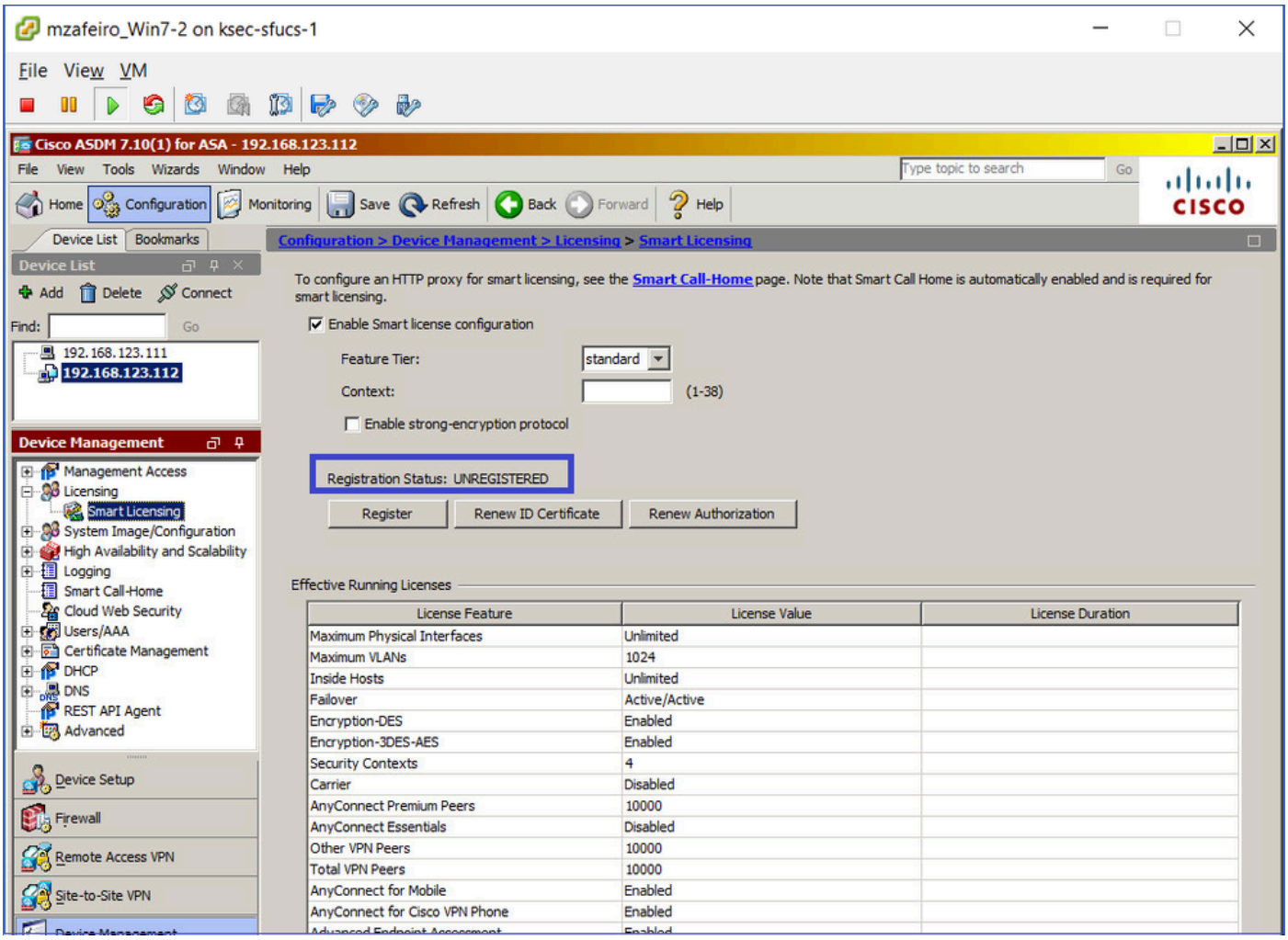
```
Serial Number: JAD12345ABC
Export Compliant: YES

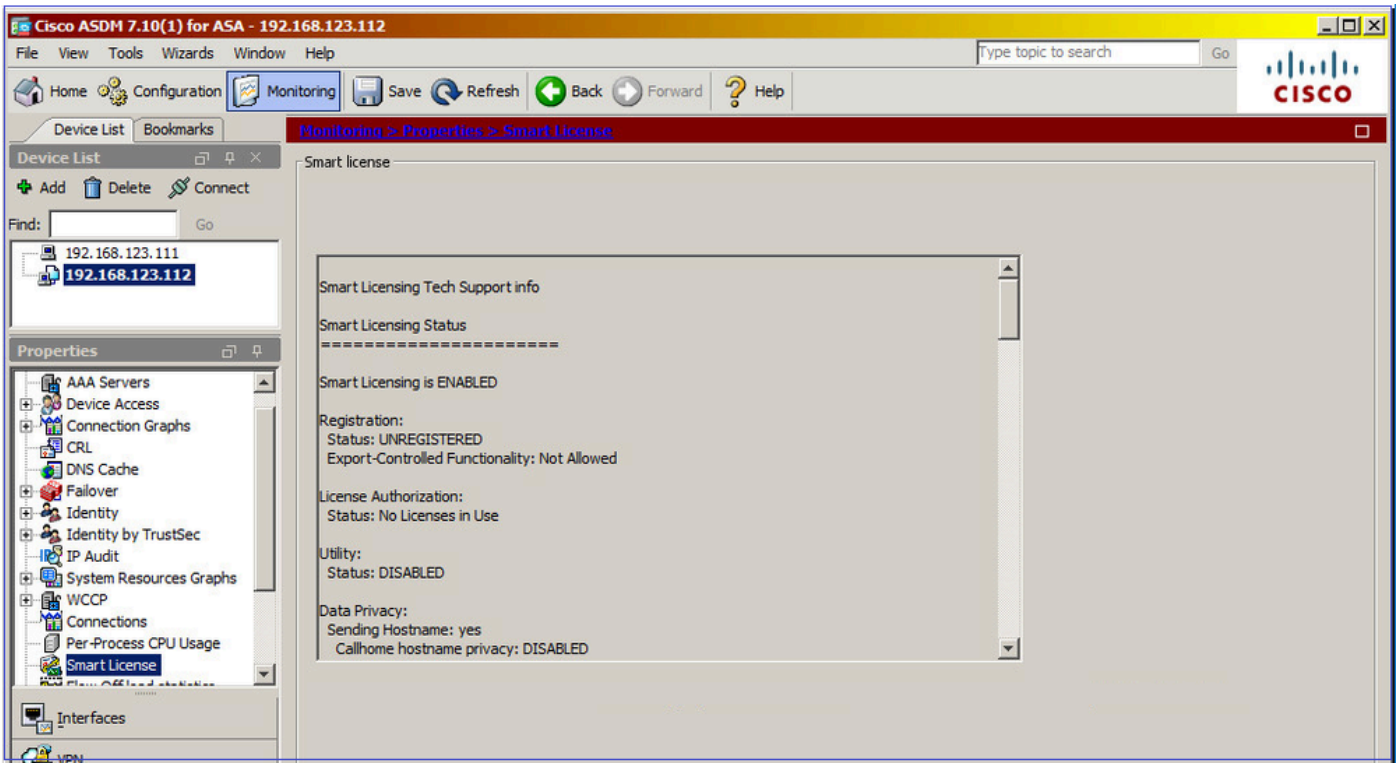
License mode: Smart Licensing

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


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

Connect via ASDM to the standby ASA (this is only possible if the ASA has been configured with a standby IP). The standby ASA is shown as UNREGISTERED and this is expected as it has not been registered to the Smart Licensing portal:





The standby ASA CLI shows:

<#root>

ciscoasa/sec/stby#

show license all

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

Smart Licensing is ENABLED

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

License Authorization:
Status: No Licenses in Use

Utility:
Status: DISABLED

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

Transport:

```
Type: Callhome

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

No licenses in use

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

Agent Version
=============
Smart Agent for Licensing: 4.3.6_rel/38
ciscoasa/sec/stby#
```

show run license

```
license smart
feature tier standard
```

The license features enabled on the standby ASA:

<#root>

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

show license features

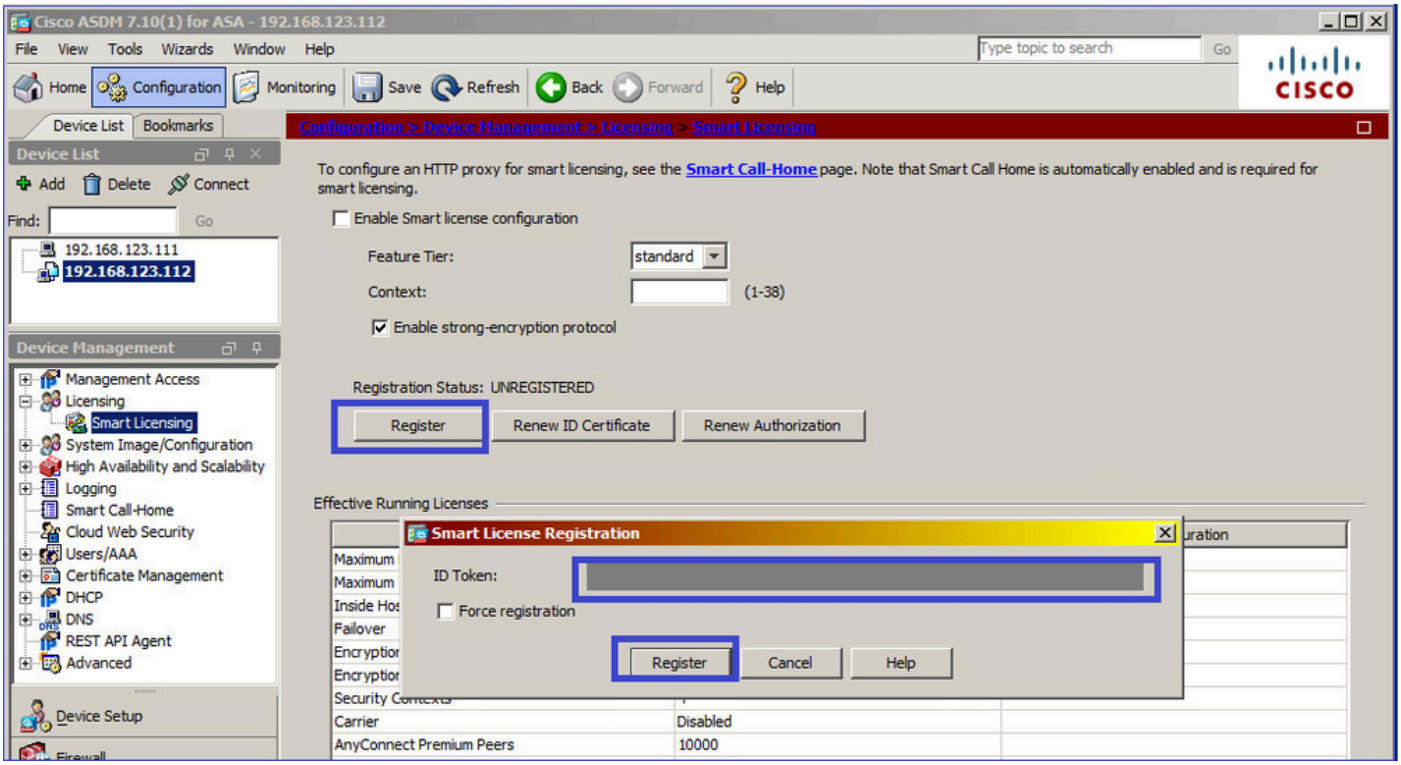
```
Serial Number: JAD123456A
Export Compliant: NO

License mode: Smart Licensing

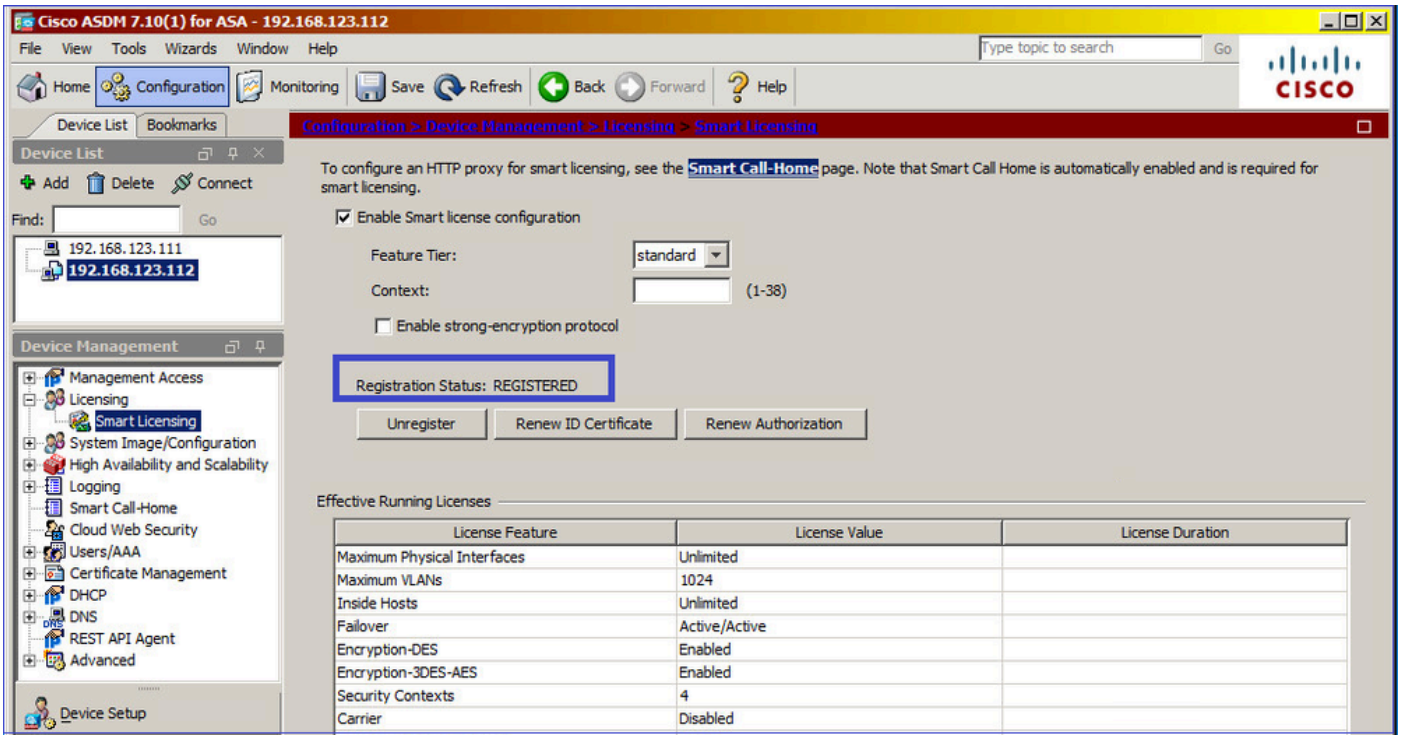
Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Disabled
Security Contexts : 2
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials :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

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

Register the standby ASA:



The result on standby ASA is that it is REGISTERED:



CLI verification on standby ASA:

<#root>

ciscoasa/sec/stby#

show license all

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

Smart Licensing is ENABLED

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

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

Utility:
Status: DISABLED
```

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

Transport:
Type: Callhome

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

No licenses in use

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

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

ciscoasa/sec/stby#
```

show license feature

```
Serial Number: JAD123456A
Export Compliant: YES

License mode: Smart Licensing

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


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

```
Security Contexts : 4
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled
```

ASA Cluster

If the devices have a license mismatch, then the cluster is not formed:

<#root>

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

rejected due to encryption license mismatch

A successful cluster setup:

<#root>

```
asa(config)#
```

cluster group GROUP1

```
asa(cfg-cluster)#
```

enable

Removed all entitlements except per-unit entitlement configuration before joining cluster as data unit.

```
Detected Cluster Control Node.
Beginning configuration replication from Control Node.
.
```

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

Cluster control node:

<#root>

```
asa#
```

show cluster info | i state

```
    This is "unit-1-1" in state CONTROL_NODE
    Unit "unit-2-1" in state DATA_NODE

asa#
```

show license all

```
Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
        Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-b3f7fb1cac
        Version: 1.0
        Enforcement mode: Authorized
        Handle: 2
        Requested time: Mon, 10 Aug 2020 08:12:38 UTC
        Requested count: 1
        Request status: Complete

Serial Number:  FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
```

```
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

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

Cluster data unit:

<#root>

```
asa#

show cluster info | i state


    This is "unit-2-1" in state DATA_NODE
    Unit "unit-1-1" in state CONTROL_NODE

asa#

show license all



Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Strong encryption:
        Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_ENCRYPTION,1.0_052986db-c5ad-40da-97b1-ee0438d3
```

```
        Version: 1.0
        Enforcement mode: Authorized
        Handle: 3
        Requested time: Mon, 10 Aug 2020 07:29:45 UTC
        Requested count: 1
        Request status: Complete

Serial Number:  FCH12345A6B

License mode: Smart Licensing

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

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

Verification and Debugging

Chassis (MIO) summary of verification commands:

<#root>

FPR4125#

show license all

FPR4125#

show license techsupport

FPR4125#

scope monitoring

FPR4125 /monitoring #

scope callhome

FPR4125 /monitoring/callhome #

show expand

FPR4125#

scope system

FPR4125 /system #

scope services

FPR4125 /system/services #

show dns

FPR4125 /system/services #

show ntp-server

FPR4125#

scope security

FPR4125 /security #

```
show trustpoint

FPR4125#
show clock

FPR4125#
show timezone

FPR4125#
show license usage
```

Configuration verification:

```
<#root>
FPR4125-1#
scope system

FPR4125-1 /system #
scope services

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

ASA summary of verification commands:

```
<#root>
asa#
show run license
```

```
asa#
```

show license all

```
asa#
```

show license entitlement

```
asa#
```

show license features

```
asa#
```

show tech-support license

```
asa#
```

debug license 255

Chassis (MIO) Sample Outputs of Verification Commands

<#root>

```
FPR4125-1#
```

show license all

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

Smart Licensing is ENABLED

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

License Authorization:
```

```
  Status: AUTHORIZED on Aug 04 2020 07:58:46 UTC
  Last Communication Attempt: SUCCEEDED on Aug 04 2020 07:58:46 UTC
  Next Communication Attempt: Sep 03 2020 07:58:45 UTC
  Communication Deadline: Nov 02 2020 07:53:44 UTC

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

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

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

Transport:
  Type: Callhome

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

Firepower 4100 ASA Standard (FIREPOWER_4100_ASA_STANDARD):
  Description: Firepower 4100 ASA Standard
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED

Product Information
====================
UDI: PID:FPR-4125-SUP,SN:JAD12345678

Agent Version
=============
Smart Agent for Licensing: 4.6.9_rel/104

Reservation Info
================
License reservation: DISABLED



<#root>

FPR4125-1#

scope monitoring



FPR4125-1 /monitoring #

scope callhome
```

```
FPR4125-1 /monitoring/callhome #
```

show expand

```
Callhome:
Admin State: Off
Throttling State: On
Contact Information:
Customer Contact Email:
From Email:
Reply To Email:
Phone Contact e.g., +1-011-408-555-1212:
Street Address:
Contract Id:
Customer Id:
Site Id:
Switch Priority: Debugging
Enable/Disable HTTP/HTTPS Proxy: Off
HTTP/HTTPS Proxy Server Address:
HTTP/HTTPS Proxy Server Port: 80
SMTP Server Address:
SMTP Server Port: 25

Anonymous Reporting:
Admin State
-----------
Off

Callhome periodic system inventory:
Send periodically: Off
Interval days: 30
Hour of day to send: 0
Minute of hour: 0
Time last sent: Never
Next scheduled: Never

Destination Profile:
Name: full_txt
Level: Warning
Alert Groups: All,Cisco Tac,Diagnostic,Environmental
Max Size: 5000000
Format: Full Txt
Reporting: Smart Call Home Data

Name: short_txt
Level: Warning
Alert Groups: All,Cisco Tac,Diagnostic,Environmental
Max Size: 5000000
Format: Short Txt
Reporting: Smart Call Home Data

Name: SLProfile
Level: Normal
Alert Groups: Smart License
Max Size: 5000000
Format: Xml
Reporting: Smart License Data
```

```
Destination:
Name Transport Protocol Email or HTTP/HTTPS URL Address
---------- ----------------- ------------------------------
```

SLDest Https

https://tools.cisco.com/its/service/oddce/services/DDCEService

<#root>

FPR4125-1#

scope system

FPR4125-1 /system #

scope services

FPR4125-1 /system/services #

show dns

```
Domain Name Servers:
    IP Address: 172.16.200.100
FPR4125-1 /system/services #
```

show ntp-server

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

Time Synchronized

```
    172.18.108.15                                                   Candidate
```

<#root>

FPR4125-1#

scope security

```
FPR4125-1 /security #
```

show trustpoint

```
Trustpoint Name: CHdefault
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
…
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
Cert Status: Valid
Trustpoint Name: CiscoLicRoot
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAyMQ4wDAYDVQQKEwVDaXNj
…
QYYWqUCT4ElNEKt1J+hvc5MuNbWIYv2uAnUVb3GbsvDWl99/KA==
-----END CERTIFICATE-----
Cert Status: Valid
Trustpoint Name: CSCO2099SUDI
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
…
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
Cert Status: Valid
Trustpoint Name: CSCOBA2099SUDI
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIDQTCCAimgAwIBAgIJAaZa8V7plOvhMA0GCSqGSIb3DQEBCwUAMD0xDjAMBgNV
…
b/JPEAZkbji0RQTWLyfR82LWFLo0
-----END CERTIFICATE-----
Cert Status: Valid
```

<#root>

```
FPR4125-1#
```

show clock

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

show timezone

```
Timezone:
```

<#root>

```
FPR4125-1#
```

scope system

```
FPR4125-1 /system #

scope services


FPR4125-1 /system/services #

show configuration


 scope services
     create ssh-server host-key rsa
     delete ssh-server host-key ecdsa
     disable ntp-authentication
     disable telnet-server
     enable https
     enable ssh-server

     enter dns 192.0.2.100



     enter ip-block 0.0.0.0 0 https
     exit
     enter ip-block 0.0.0.0 0 ssh
     exit

     enter ntp-server 10.62.148.75



         set ntp-sha1-key-id 0
 !       set ntp-sha1-key-string
     exit

     enter ntp-server 172.18.108.14



         set ntp-sha1-key-id 0
 !       set ntp-sha1-key-string
     exit

     enter ntp-server 172.18.108.15



         set ntp-sha1-key-id 0
 !       set ntp-sha1-key-string
     exit
     scope shell-session-limits
         set per-user 32
         set total 32
     exit
     scope telemetry
         disable
     exit
     scope web-session-limits
         set per-user 32
```

```
         set total 256
     exit
     set domain-name ""
     set https auth-type cred-auth
     set https cipher-suite "ALL:!DHE-PSK-AES256-CBC-SHA:!EDH-RSA-DES-CBC3-SHA:!
EDH-DSS-DES-CBC3-SHA:!DES-CBC3-SHA:!ADH:!3DES:!EXPORT40:!EXPORT56:!LOW:!MEDIUM:!NULL:!RC4:!MD5:!IDEA:+H
     set https cipher-suite-mode high-strength
     set https crl-mode strict
     set https keyring default
     set https port 443
     set ssh-server host-key ecdsa secp256r1
     set ssh-server host-key rsa 2048
     set ssh-server kex-algorithm diffie-hellman-group14-sha1
     set ssh-server mac-algorithm hmac-sha1 hmac-sha2-256 hmac-sha2-512
     set ssh-server encrypt-algorithm aes128-cbc aes128-ctr aes192-cbc aes192-ctr aes256-cbc aes256-ctr
     set ssh-server rekey-limit volume none time none
     set ssh-client kex-algorithm diffie-hellman-group14-sha1
     set ssh-client mac-algorithm hmac-sha1 hmac-sha2-256 hmac-sha2-512
     set ssh-client encrypt-algorithm aes128-ctr aes192-ctr aes256-ctr
     set ssh-client rekey-limit volume none time none
     set ssh-client stricthostkeycheck disable

     set timezone ""


 exit



<#root>

FPR4125-1#

show license usage



License Authorization:
  Status: AUTHORIZED on Aug 04 2020 07:58:46 UTC

Firepower 4100 ASA Standard (FIREPOWER_4100_ASA_STANDARD):
  Description: Firepower 4100 ASA Standard
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
```

ASA Sample Outputs of Verification Commands

<#root>

asa#

show run license

```
license smart
 feature tier standard
```

<#root>

asa#

show license all

```
Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

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

Serial Number:  FCH12345ABC

License mode: Smart Licensing

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

<#root>

asa#

show license entitlement

```
Entitlement(s):

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

<#root>

asa#

show license features

```
Serial Number:  FCH12345ABC

License mode: Smart Licensing

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

<#root>

asa#

show tech-support license

```
Smart licensing enabled: Yes
```

```
Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

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

Successful Registration

The output is from the chassis manager User Interface (UI):

<#root>

```
Smart Licensing is ENABLED

Utility:
Status: DISABLED

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

Transport:
Type: Callhome

Registration:

Status: REGISTERED


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

License Authorization:

Status: AUTHORIZED on Jul 05 2020 17:49:15 UTC
Last Communication Attempt: SUCCEEDED on Jul 05 2020 17:49:15 UTC


Next Communication Attempt: Aug 04 2020 17:49:14 UTC
```

```
Communication Deadline: Oct 03 2020 17:44:13 UTC

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

Export Authorization Key:
Features Authorized:
<none>

Cisco Success Network: DISABLED
```

Expired Authorization

The output is from the chassis manager UI:

<#root>

```
Smart Licensing is ENABLED

Utility:
Status: DISABLED

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

Transport:
Type: Callhome

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

License Authorization:

Status: AUTH EXPIRED


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

License Conversion:
```

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

Export Authorization Key:
Features Authorized:
<none>

Last Configuration Error
========================
Command : register idtoken ZDA2MjFlODktYjllMSOONjQwLTkOMmUtYmVkYWU2NzIyZjYwLTE1ODIxODY2%OAMzEwODV8K2RWV
Error : Smart Agent already registered

Cisco Success Network: DISABLED
```

Sample Outputs from Chassis CLI

Unregistered

<#root>

```
firepower#
```

show license all

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

Smart Licensing is ENABLED

Registration:

  Status: UNREGISTERED


License Authorization:

  Status: No Licenses in Use


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

No licenses in use

Product Information
===================
UDI: PID:F9K-C93OO-SUP-K9,SN:JAD12345678
```

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

Registration in Progress

<#root>

```
firepower#
```

scope license

```
firepower /license #
```

register idtoken <id-token>

```
firepower /license #
```

show license all

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

Smart Licensing is ENABLED

```
Registration:
```

  Status: UNREGISTERED - REGISTRATION PENDING

  Initial Registration: First Attempt Pending

```
License Authorization:
  Status: No Licenses in Use

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

No licenses in use
```

```
Product Information
==================
UDI: PID:F9K-C93OO-SUP-K9,SN:JAD12345678

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

Registration Error

<#root>

```
firepower /license #

show license all



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

Smart Licensing is ENABLED

Registration:

  Status: UNREGISTERED - REGISTRATION FAILED



  Initial Registration: FAILED on Aug 04 04:46:47 2020 UTC



    Failure reason: HTTP transport failed



License Authorization:
  Status: No Licenses in Use

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

No licenses in use

Product Information
==================
UDI: PID:F9K-C93OO-SUP-K9,SN:JAD12345678

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

Evaluation Period

```
<#root>

firepower#

show license all



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

Smart Licensing is ENABLED

Registration:
 Status: REGISTERING - REGISTRATION IN PROGRESS
 Initial Registration: FAILED on Aug 04 04:46:47 2020 UTC
 Next Registration Attempt: Aug 04 05:06:16 2020 UTC

License Authorization:

 Status: EVALUATION MODE



 Evaluation Period Remaining: 89 days, 14 hours, 26 minutes, 20 seconds

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

(ASA-SSP-STD):
 Description:
 Count: 1
 Version: 1.0

 Status: EVALUATION MODE




Product Information
===================
UDI: PID:F9K-C9300-SUP-K9,SN:JAD12345678

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

Common License Problems on FXOS Chassis (MIO)

Registration Error: Invalid Token

<#root>

FPR4125-1#

show license all

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

Smart Licensing is ENABLED

Registration:

Status: UNREGISTERED - REGISTRATION FAILED

Export-Controlled Functionality: NOT ALLOWED
Initial Registration: FAILED on Aug 07 2020 06:39:24 UTC

Failure reason: {"token"

:["The token 'ODNmNTExMTAtY2YzOS00Mzc1LWEzNWMtYmNiMm
UyNzM4ZmFjLTE1OTkxMTkz%0ANDk0NjR8NkJJdWZpQzRDbmtPR0xBWlVpUzZqMjlySnl5QUczT2M0YVI
vcmxm%0ATGczND0%3D%0B'

is not valid

."]}

Recommended Steps

1. Check if the call-home URL points to Cisco License Central.
2. Log in to the Cisco License Central and check if the token is generated from there, or if the token has expired.

Registration Error: Product Already Registered

<#root>

FPR4125-1#

show license all

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

Smart Licensing is ENABLED

Registration:
```

Status: UNREGISTERED - REGISTRATION FAILED

```
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 01:30:00 2020 UTC
```

Failure reason

```
: {"sudi":["The product 'firepower.com.cisco.
FPR9300,1.0_ed6dadbe-c965-4aeb-ab58-62e34033b453' and sudi {\"suvi\"=>nil,
\"uuid\"=>nil, \"host_identifier\"=>nil, \"udi_pid\"=>\"FPR9K-SUP\",
\"udi_serial_number\"=>\"JAD1234567S\", \"udi_vid\"=>nil, \"mac_address\"=>nil}
```

have already been registered

```
."]}
```

Recommended Steps

1. Log in to Cisco License Central.
2. Check the **Product Instances** tab in ALL virtual accounts.
3. Locate the old registration instance by SN and remove it.
4. This issue could be caused by:
    a. Failure to automatically renew when time/date is not set up correctly, for example, no NTP server is configured.
    b. Wrong order of operations when you switch between a Satellite and a Production server. For example, change the URL first and then issue deregister.

Registration Error: Date Offset Beyond the Limit

```
<#root>

FPR4125-1#
```

show license all

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

Smart Licensing is ENABLED

Registration:
```

Status: UNREGISTERED - REGISTRATION FAILED

```
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 01:30:00 2020 UTC
Failure reason: {"
```

timestamp

```
":["The device date '1453329321505'
```

is offset beyond the allowed tolerance limit

```
."]}
```

Recommended Step

Check the time/date configuration to ensure that an NTP server is configured.

Registration Error: Failed to Resolve Host

```
<#root>
FPR4125-1#
```

show license all

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

Smart Licensing is ENABLED

Registration:
  Status: REGISTERING - REGISTRATION IN PROGRESS
  Export-Controlled Functionality: NOT ALLOWED
```

```
  Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC
    Failure reason: Failed to resolve host
  Next Registration Attempt: Aug 07 2020 07:16:42 UTC

Registration Error: Failed to resolve host
```

Recommended Steps

1. Check if the callhome SLDest URL is correct (**scope monitoring > scope callhome > show expand**).
2. Check if the MIO DNS server configuration is correct, for example, from CLI:

```
<#root>

FPR4125-1#

scope system


FPR4125-1 /system #

scope services


FPR4125-1 /system/services #

show dns


Domain Name Servers:
    IP Address: 172.31.200.100
```

---

3. Try to ping from the chassis CLI the **tools.cisco.com** and see if it resolves:

```
<#root>

FPR4125-1#

connect local-mgmt


FPR4125-1(local-mgmt)#

ping tools.cisco.com
```

4. Try to ping from the chassis CLI the DNS server:

```
<#root>

FPR4125-1#

connect local-mgmt


FPR4125-1(local-mgmt)#

ping 172.31.200.100


PING 172.31.200.100 (172.31.200.100) from 10.62.148.225 eth0: 56(84) bytes of data.
^C
--- 172.31.200.100 ping statistics ---
4 packets transmitted, 0 received,

100% packet loss

, time 3001ms
```

---

5. Enable capture on chassis (MIO) mgmt interface (this is only applicable on FP41xx/FP93xx) and check the DNS communication as you run a ping test to the **tools.cisco.com**:

```
<#root>

FPR4125-1#

connect fxos


FPR4125-1(fxos)#

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


Capturing on 'eth0'
    1 2020-08-07 08:10:45.252955552 10.62.148.225 → 172.31.200.100 DNS 75 Standard query 0x26b4 A tools.cisco
    2 2020-08-07 08:10:47.255015331 10.62.148.225 → 172.31.200.100 DNS 75 Standard query 0x26b4 A tools.cisco
    3 2020-08-07 08:10:49.257160749 10.62.148.225 → 172.31.200.100 DNS 75 Standard query 0x5019 A tools.cisco
    4 2020-08-07 08:10:51.259222753 10.62.148.225 → 172.31.200.100 DNS 75 Standard query 0x5019 A tools.cisco
```

Registration Error: Failed to Authenticate Server

<#root>

FPR4125-1#

show license all

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

Smart Licensing is ENABLED

Registration:

Status: UNREGISTERED - REGISTRATION FAILED

Export-Controlled Functionality: Not Allowed
Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC

Failure reason: Failed to authenticate server

Recommended Steps

1. Check if the MIO trustpoint CHdefault has the correct certificate, for example:

<#root>

FPR4125-1#

scope security

FPR4125-1 /security #

show trustpoint

Trustpoint Name: CHdefault

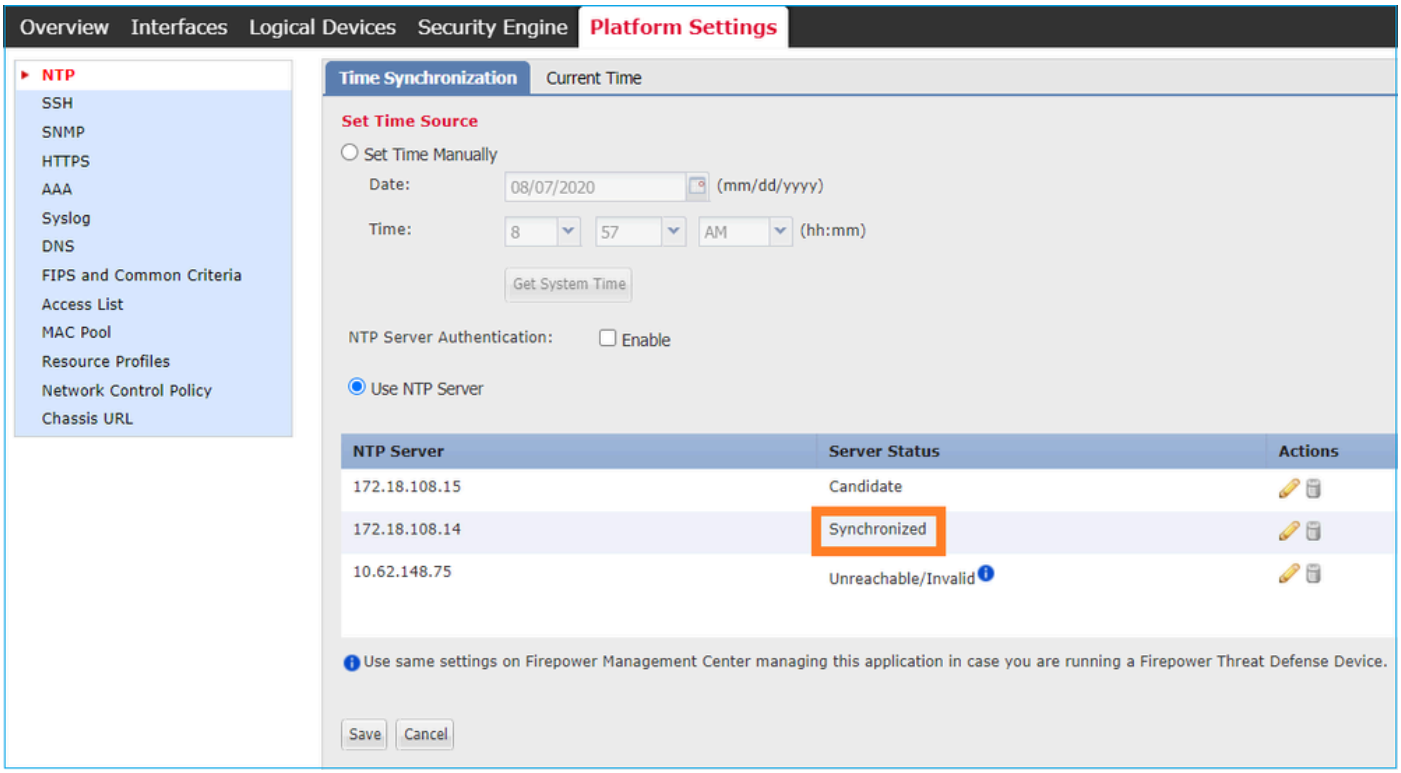
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----

```
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
...
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
```

Cert Status: Valid

---

2. Check if the NTP server and timezone are set correctly. Certificate verification must have the same time between the server and client. To accomplish this, use NTP to synchronize the time. For example, FXOS UI verification:



CLI Verification

<#root>

FPR4125-1#

scope system

FPR4125-1 /system #

scope services

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

show ntp-server

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

172.18.108.14 **Time Synchronized**

```
    172.18.108.15                                           Candidate
```

Enable a capture and check the TCP communication (HTTPS) between the MIO and the tools.cisco.com. You have a few options:

- You can close your HTTPS session to the FXOS UI and set a capture filter on the CLI for HTTPS, for example:

<#root>

```
FPR4100(fxos)#
```

ethanalyzer local interface mgmt capture-filter "tcp port 443" limit-captured-frames 50

```
Capturing on eth0
2017-01-12 13:09:44.296256 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [
```

SYN

```
] Seq=0 Len=0 MSS=1460 TSV=206433871 TSER=0 WS=9
2017-01-12 13:09:44.452405  72.163.4.38 -> 10.62.148.37 TCP https > 43278 [
```

SYN

,

ACK

```
] Seq=0 Ack=1 Win=32768 Len=0 MSS=1380 TSV=2933962056 TSER=206433871
2017-01-12 13:09:44.452451 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [
```

ACK

```
] Seq=1 Ack=1 Win=5840 Len=0 TSV=206433887 TSER=2933962056
2017-01-12 13:09:44.453219 10.62.148.37 -> 72.163.4.38
```

SSL Client Hello

```
2017-01-12 13:09:44.609171  72.163.4.38 -> 10.62.148.37 TCP https > 43278 [ACK] Seq=1 Ack=518 Win=32251
2017-01-12 13:09:44.609573  72.163.4.38 -> 10.62.148.37 SSL Continuation Data
2017-01-12 13:09:44.609595 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [ACK] Seq=518 Ack=1369 Win=82
2017-01-12 13:09:44.609599  72.163.4.38 -> 10.62.148.37 SSL Continuation Data
2017-01-12 13:09:44.609610 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [ACK] Seq=518 Ack=2737 Win=10
```

- Additionally, if you want to keep the FXOS UI open, you can specify in the capture the destination IPs (72.163.4.38 and 173.37.145.8 are the tools.cisco.com servers at the time of this writing). It is also highly recommended to save the capture in pcap format and check these in Wireshark. This is an example of a successful registration:

<#root>

```
FPR4125-1(fxos)#
```

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

```
Capturing on 'eth0'
    1 2020-08-07 08:39:02.515693672 10.62.148.225 → 173.37.145.8 TCP 74 59818 → 443 [
```

SYN

```
] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=800212367 TSecr=0 WS=512
    2 2020-08-07 08:39:02.684723361 173.37.145.8 → 10.62.148.225 TCP 60 443 → 59818 [
```

SYN, ACK

```
] Seq=0 Ack=1 Win=8190 Len=0 MSS=1330
    3 2020-08-07 08:39:02.684825625 10.62.148.225 → 173.37.145.8 TCP 54 59818 → 443 [
```

ACK

```
] Seq=1 Ack=1 Win=29200 Len=0
    4 2020-08-07 08:39:02.685182942 10.62.148.225 → 173.37.145.8 TLSv1 571
```

Client Hello

```
…
   11 2020-08-07 08:39:02.854525349 10.62.148.225 → 173.37.145.8 TCP 54 59818 → 443 [ACK] Seq=518 Ack=3991 W
```

- To export the pcap file to a remote FTP server:

```
<#root>
FPR4125-1#

connect local-mgmt


FPR4125-1(local-mgmt)#

dir



1 56936 Aug 07 08:39:35 2020

SSL.pcap

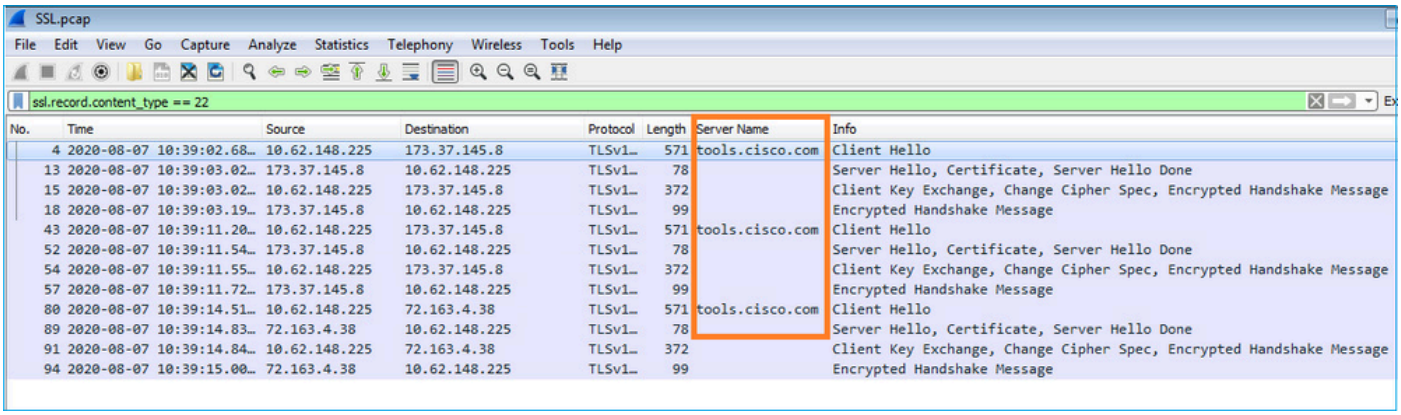


1    29 May 06 17:48:02 2020 blade_debug_plugin
1    19 May 06 17:48:02 2020 bladelog
1    16 Dec 07 17:24:43 2018 cores
2  4096 Dec 07 17:28:46 2018 debug_plugin/
1    31 Dec 07 17:24:43 2018 diagnostics
2  4096 Dec 07 17:22:28 2018 lost+found/
1    25 Dec 07 17:24:31 2018 packet-capture
2  4096 Sep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

Usage for workspace://
3999125504 bytes total
284364800 bytes used
3509907456 bytes free
FPR4125-1(local-mgmt)#

copy workspace:///SSL.pcap ftp://ftp_user@10.62.148.41/SSL.pcap


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



Registration Error: HTTP Transport Failed

<#root>

FPR4125-1#

show license all

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

Smart Licensing is ENABLED

Registration:

Status: UNREGISTERED - REGISTRATION FAILED

Export-Controlled Functionality: Not Allowed
Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC

Failure reason: HTTP transport failed

Recommended Steps

1. Check if the call-home URL is correct. You can check this from the FXOS UI or the CLI (**scope monitoring > show callhome detail expand**).
2. Enable a capture and check the TCP communication (HTTPS) between the MIO and the tools.cisco.com as it is demonstrated in the Failed to Authenticate Server section of this document.

Registration Error: Could Not Connect to Host

```
<#root>

FPR4125-1#

show license all



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

Smart Licensing is ENABLED

Registration:


Status: UNREGISTERED - REGISTRATION FAILED


 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC

 Failure reason: Could Not connect to host
```

Recommended Steps

1. If a proxy configuration is enabled, ensure the proxy URL and port are configured correctly.
2. Enable a capture and check the TCP communication (HTTPS) between the MIO and the tools.cisco.com as it is demonstrated in the Failed to Authenticate Server section of this document.

Registration Error: HTTP Server Returns Error Code >= 400

```
<#root>

FPR4125-1#

show license all



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

```
Smart Licensing is ENABLED

Registration:


Status: UNREGISTERED - REGISTRATION FAILED


 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC

 Failure reason: HTTP server returns error code >= 400. Contact proxy server admin if proxy configuratio
```

Recommended Steps

1. If a proxy configuration is enabled, contact the proxy server admin about proxy settings.
2. Enable a capture and check the TCP communication (HTTPS) between the MIO and tools.cisco.com as it is demonstrated in the Failed to Authenticate Server section of this document. Try to register again (force option) from the FXOS CLI:

```
<#root>

FPR4125-1 /license #

register idtoken ODNmNTExMTAtY2YzOS00Mzc1LWEzNWMtYmNiMmUyNzM4ZmFjLTE1OTkxMTkz%0ANDk0NjR8NkJJdWZpQzRDbmtP
```

Registration Error: Parse Backend Response Message Failed

```
<#root>

FPR4125-1#

show license all


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

Smart Licensing is ENABLED

Registration:
```

```
Status: UNREGISTERED - REGISTRATION FAILED

Export-Controlled Functionality: Not Allowed
Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC

Failure reason: Parsing backend response message failed
```

Recommended Steps

1. Auto-retry attempts later. Use renew to retry immediately.

```
<#root>
FPR4125-1#

scope license

FPR4125-1 /license #

scope licdebug

FPR4125-1 /license/licdebug #

renew
```

---

2. Check if the call-home URL is correct.

License Issues on ASA - 1xxx/21xx Series

Registration Error: Communication Message Send Error

```
<#root>
ciscoasa#

show license all
```

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

Smart Licensing is ENABLED

Registration:


 Status: REGISTERING - REGISTRATION IN PROGRESS


  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Aug 07 2020 11:29:42 UTC

    Failure reason: Communication message send error


  Next Registration Attempt: Aug 07 2020 11:46:13 UTC
```

Recommended Steps

1. Check the DNS settings:

```
<#root>

ciscoasa#

show run dns
```

---

2. Try pinging tools.cisco.com. In this case, the management interface is used:

```
<#root>

ciscoasa#

ping management tools.cisco.com


               ^
ERROR: % Invalid Hostname
```

---

3. Check the routing table:

```
<#root>

ciscoasa#

show route management-only
```

Ensure you have a license enabled, for example:

```
<#root>

ciscoasa#

show run license


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

---

4. Enable capture on the interface that routes towards the tools.cisco.com (if you take the capture without any IP filters, ensure you do not have ASDM open when you take the capture to avoid unnecessary capture noise).

```
<#root>

ciscoasa#

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

 **Warning**: Packet capture can have an adverse impact on performance.

---

5. Temporarily enable Syslog level 7 (debug) and check the ASA Syslog messages during the registration process:

<#root>

ciscoasa(config)#

logging buffer-size 10000000

ciscoasa(config)#

logging buffered 7

ciscoasa(config)#

logging enable

ciscoasa#

show logging

%ASA-7-717025: Validating certificate chain containing 3 certificate(s).
%ASA-7-717029: Identified client certificate within certificate chain. serial number: 3000683B0F7504F7B

tools.cisco.com

,O=Cisco Systems\, Inc.,L=San Jose,ST=CA,C=US.
%ASA-7-717030: Found a suitable trustpoint _SmartCallHome_ServerCA to validate certificate.
%ASA-6-717028:

Certificate chain was successfully validated

 with warning, revocation status was not checked.
%ASA-6-717022:

Certificate was successfully validated

. serial number: 3000683B0F7504F7B244B3EA7FC00927E960D735, subject name: CN=

tools.cisco.com

,O=Cisco Systems\, Inc.,L=San Jose,ST=CA,C=US.
%ASA-6-725002: Device completed SSL handshake with server management:10.62.148.184/22258 to 173.37.145.

Try to register again:

<#root>

ciscoasa #

```
license smart register idtoken <idtoken> force
```

Special Requirements for Add-on Entitlements

- A valid feature tier entitlement must be acquired before you configure any add-on entitlements.
- All add-on entitlements must be released before you release the feature tier entitlement.

Entitlement State During Reboot Operation

- Entitlement states are saved in the flash.
- During boot time, this information is read from the flash and the licenses are set based on the enforcement mode saved.
- The start up configuration is applied based on this cached entitlement information.
- Entitlements are requested again after each reboot.

Engage Cisco TAC Support

FP41xx/FP9300

If all items mentioned in this document fail, collect these outputs from the chassis CLI and contact Cisco TAC:

Output 1:

<#root>

```
FPR4125-1#
```

```
show license techsupport
```

Output 2:

<#root>

```
FPR4125-1#
```

```
scope monitoring
```

```
FPR4125-1 /monitoring #
```

scope callhome

```
FPR4125-1 /monitoring/callhome #
```

show detail expand

Output 3. FXOS chassis support bundle:

<#root>

```
FPR4125-1#
```

connect local-mgmt

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

show tech-support chassis 1 detail

Output 4 (highly recommended). Ethanalyzer capture from the chassis CLI:

FP1xxx/FP21xx

Output 1:

<#root>

```
ciscoasa#
```

show tech-support license

Output 2:

<#root>

```
ciscoasa#
```

```
connect fxos admin
```

```
firepower-2140#
```

```
connect local-mgmt
```

```
firepower-2140(local-mgmt)#
```

```
show tech-support fprm detail
```

Frequently Asked Questions (FAQs)

Q: On FP21xx, where is the Licensing tab on the chassis (FCM) GUI?
A: As of 9.13.x, FP21xx supports 2 ASA modes:

- Appliance
- Platform

In Appliance mode, there is no chassis UI.

In Platform mode, there is a chassis UI, but the license is configured from the ASA CLI or ASDM.
On the other hand, on FPR4100/9300 platforms, the license must be configured in FCM via GUI or FXOS CLI and ASA entitlements must be requested from ASA CLI or ASDM.
References:

- License Management for the ASA
- Logical Devices for the Firepower 4100/9300
- Licenses: Smart Software Licensing (ASAv, ASA on Firepower)
- ASA Platform Mode Deployment with ASDM and Firepower Chassis Manager

---

Q: How can you enable a Strong Encryption License?
A: This functionality is enabled automatically if the token used in the FCM registration had the option to allow export-controlled functionality on the products registered with this token enabled.

Q: How can you enable a Strong Encryption License if the Export-Controlled Features on the FCM level and the related Encryption-3DES-AES on the ASA level are disabled?
A: If the token does not have this option enabled, deregister the FCM and register it again with a token that has this option enabled.

Q: What can you do if the option to allow export-controlled functionality on the products registered with this token is not available when you generate the token?
A: Contact your Cisco Account team.

Q: Is it mandatory to configure the feature Strong Encryption on the ASA level?
A: The feature strong-encryption option is mandatory only if FCM is integrated with a pre-2.3.0 Satellite server. This is only one scenario where you must configure this feature.

Q: Which IPs must be allowed in the path between the FCM and the Smart Licensing Cloud?
A: The FXOS uses the address https://tools.cisco.com/ (port 443) to communicate with the licensing cloud. The address https://tools.cisco.com/ is resolved to these IP addresses:

- 72.163.4.38
- 173.37.145.8

Q: Why do you get an Out of Compliance error?
A: The device can become out of compliance in these situations:

- Over-utilization (the device uses unavailable licenses).
- License expiration: A time-based license expired.
- Lack of communication: The device cannot reach the Licensing Authority for re-authorization.

To verify whether your account is in, or approaches an Out-of-Compliance state, you must compare the entitlements currently in use by your Firepower chassis against those in your Smart Account. In an out-of-compliance state, you can make configuration changes to features that require special licenses, but the operation is otherwise unaffected. For example, over the standard license limit contexts that already exist continue to run, and you can modify their configuration, but you cannot add a new context.

Q: Why do you still get an Out of Compliance error after the addition of licenses?
A: By default, the device communicates with the License Authority every 30 days to check entitlements. If you want to trigger it manually, you must use these steps:

For FPR1000/2100 platforms it must be done via ASDM or via CLI:

<#root>

ASA#

license smart renew auth

For FPR4100/9300 platforms it must be completed via FXOS CLI:

```
<#root>
FP4100#
scope system

FP4100 /system #
scope license

FP4100 /license #
scope licdebug

FP4100 /license/licdebug #
renew
```

Q: Why is there no License In Use on the ASA level?
A: Ensure the ASA entitlement was configured on the ASA level, for example:

```
<#root>
ASA(config)#
license smart

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

Q: Why are licenses still not in use even after the configuration of an ASA entitlement?
A: This status is expected if you deployed an ASA Active/Standby failover pair and you check the license usage on the Standby device. Per the configuration guide, the configuration is replicated to the standby unit, but the standby unit does not use the configuration; it remains in a cached state. Only the active unit requests the licenses from the server. The licenses are aggregated into a single failover license that is shared by the

failover pair, and this aggregated license is also cached on the standby unit to be used if it becomes the active unit in the future. For reference: Failover or ASA Cluster Licenses.

Q: What can you do if FCM does not have access to the Internet?
A: As an alternative, you can deploy Cisco License Central On-Prem (formerly known as Satellite). This is a component of Cisco Smart Licensing that works in conjunction with the Cisco License Central. It offers near real-time visibility and reports capabilities of the Cisco licenses you purchase and consume. It also gives security-sensitive organizations a way to access a subset of Cisco License Central functionality without the usage of a direct internet connection to manage their install base.

Q: Where can you find more information about Cisco License Central On-Prem?
A: You can find this information in the FXOS Configuration Guide:

- Configure a Smart License Satellite Server for the Firepower 4100/9300 chassis
- Configure Firepower Chassis Manager Registration to a Cisco License Central On-Prem

---

Related Information

- Cisco ASA Series General Operations CLI Configuration Guide
- License Management for the ASA
- Technical Support & Documentation - Cisco Systems