

FXOS Firepower 어플라이언스에서 ASA Smart License 문제 해결

목차

[소개](#)

[배경 정보](#)

[Smart Licensing 아키텍처](#)

[전체 아키텍처](#)

[명명법](#)

[스마트 에이전트 상태](#)

[ASA 자격](#)

[설정](#)

[장애 조치\(고가용성\)](#)

[사례 연구: FP2100의 ASA HA 라이선스](#)

[ASA 클러스터](#)

[확인 및 디버깅](#)

[새시\(MIO\) 검증 명령의 샘플 출력](#)

[ASA 검증 명령의 샘플 출력](#)

[등록 성공](#)

[만료된 권한 부여](#)

[새시 CLI의 샘플 출력](#)

[등록되지 않음](#)

[등록 진행 중](#)

[등록 오류](#)

[평가 기간](#)

[FXOS 새시의 일반적인 라이선스 문제\(MIO\)](#)

[등록 오류: 잘못된 토큰](#)

[권장 단계](#)

[등록 오류: 제품이 이미 등록되었습니다.](#)

[권장 단계](#)

[등록 오류: 날짜 오프셋이 제한을 초과합니다.](#)

[권장 단계](#)

[등록 오류: 호스트를 확인하지 못했습니다.](#)

[권장 단계](#)

[등록 오류: 서버를 인증하지 못했습니다.](#)

[권장 단계](#)

[CLI 확인](#)

[등록 오류: HTTP 전송 실패](#)

[권장 단계](#)

[등록 오류: 호스트에 연결할 수 없습니다.](#)

[권장 단계](#)

[등록 오류: HTTP 서버에서 오류 코드 \$\geq 400\$ 을 반환합니다.](#)

[권장 단계](#)

[등록 오류: 백 엔드 응답 메시지를 구문 분석하지 못했습니다.](#)

[권장 단계](#)

[ASA의 라이선스 문제 - 1xxx/21xx Series](#)

[등록 오류: 통신 메시지 전송 오류](#)

[권장 단계](#)

[추가 기능 사용 자격에 대한 특별 요구 사항](#)

[재부팅 작업 중 자격 상태](#)

[Cisco TAC 지원 참여](#)

[FP41xx/FP9300](#)

[FP1xxx/FP21xx](#)

[자주 묻는 질문\(FAQ\)](#)

[관련 정보](#)

소개

이 문서에서는 Firepower FXOS(eXtensible Operating System)의 ASA(Adaptive Security Appliance) Smart Licensing 기능에 대해 설명합니다.

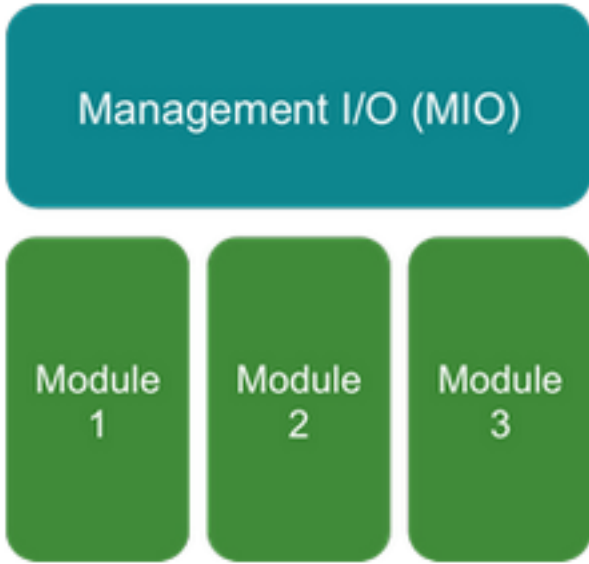
배경 정보

FXOS의 Smart Licensing은 새시에 ASA가 설치된 경우 사용됩니다. Firepower Threat Defense(FTD) 및 Firepower Management Center(FMC)의 경우 Smart Licensing은 FMC [및 FTD Smart License 등록 및 문제 해결을 확인합니다.](#)

이 문서에서는 FXOS 새시가 직접 인터넷에 액세스하는 시나리오를 주로 다룹니다. FXOS 새시에서 인터넷에 액세스할 수 없는 경우 Satellite Server 또는 PLR(Permanent License Reservation)을 고려해야 합니다. [오프라인](#) 관리에 대한 자세한 내용은 FXOS 컨피그레이션 가이드를 [참조하십시오.](#)

Smart Licensing 아키텍처

새시 구성 요소에 대한 개괄적인 개요:

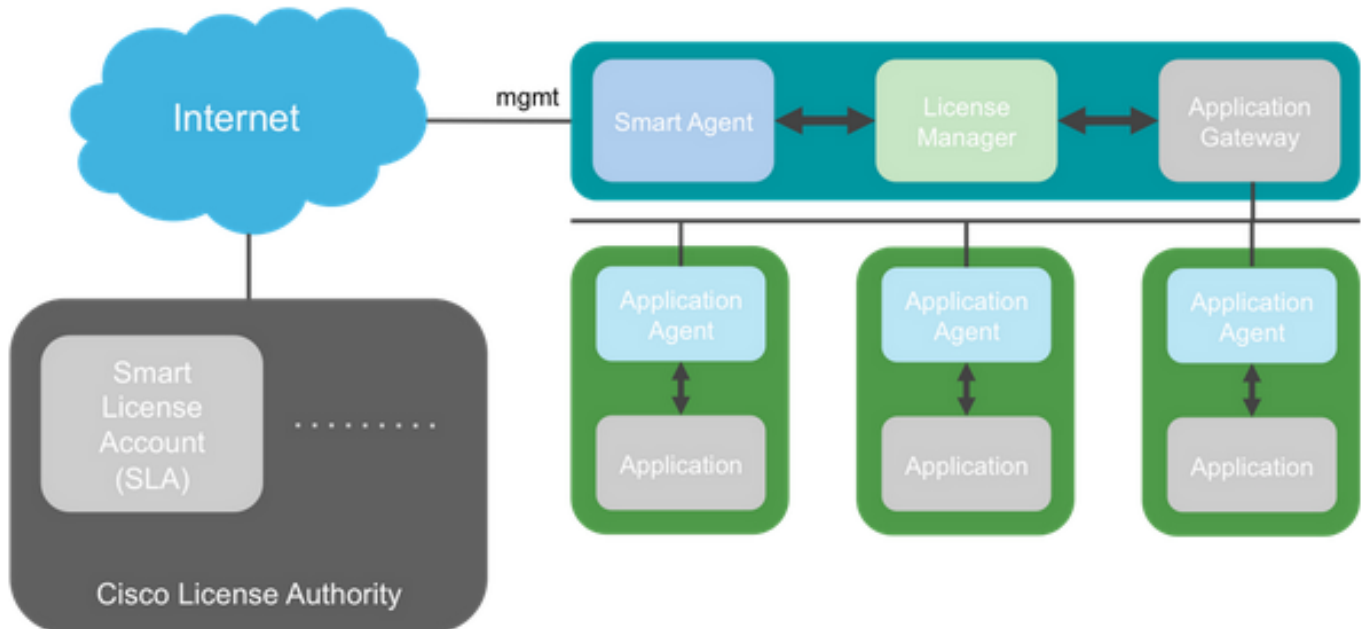


- MIO(Management Input/Output) 및 개별 모듈 모두 Smart Licensing에서 역할을 함
- MIO 자체에는 운영을 위한 라이선스가 필요하지 않습니다
- 각 모듈의 SA 애플리케이션에 대한 라이선스가 필요합니다.

FXOS 슈퍼바이저가 MIO입니다. MIO에는 세 가지 주요 구성 요소가 포함되어 있습니다.

- 스마트 에이전트
- 라이선스 관리자
- 앱AG

전체 아키텍처



명명법

용어
Cisco License Authority

설명
Smart Licensing용 Cisco 라이선스 백엔드 모든 제품 라이선싱 관련 정

Smart License 계정	보를 유지 관리합니다. 여기에는 자격 및 디바이스 정보가 포함됩니다.
토큰 ID	어플라이언스에 대한 모든 엔타이틀먼트가 있는 어카운트.
자격	식별자는 어플라이언스가 등록될 때 Smart License Account를 구별하는 데 사용됩니다.
PAK(Product Activation Key)	라이선스와 동일 개별 기능 또는 전체 기능 계층에 해당합니다. 이전 라이선싱 메커니즘. 단일 어플라이언스에 연결

스마트 에이전트 상태

상태	설명
구성되지 않음	스마트 라이선싱이 활성화되지 않았습니다.
식별되지 않음	스마트 라이선싱이 활성화되었지만 Smart Agent가 아직 Cisco에 등록하도록 연결하지 않았습니다.
등록됨	에이전트가 Cisco 라이선스 기관에 연락하여 등록했습니다.
승인	상담원이 자격 권한 부여 요청에 대한 응답으로 규정 준수 상태를 수신하는 경우
규정 위반(OOC)	상담원이 자격 권한 부여 요청에 대한 응답으로 OOC 상태를 수신하는 경우.
권한 부여 만료됨	90일 동안 상담원이 Cisco와 통신하지 않은 경우.

ASA 자격

지원되는 ASA 자격:

- 표준 계층
- 멀티 컨텍스트
- 강력한 암호화(3DES)
- 모바일/서비스 공급자(GTP)

설정

다음 문서의 지침을 따르십시오.

- [Smart Software Licensing\(ASAv, Firepower의 ASA\)](#)
- [ASA의 라이선스 관리](#)

기능 계층 컨피그레이션 전:

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

표준 계층을 구성합니다.

```
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-
b3f7fblcacfc

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
Clustertext

장애 조치(고가용성)

ASA 컨피그레이션 가이드에 설명되어 있듯이 각 Firepower 유닛은 License Authority 또는 Satellite 서버에 등록해야 합니다. ASA CLI에서 확인:

```
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-  
b3f7fblcacfc
```

```
  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
```

스탠바이 유닛:

```
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

```

사례 연구: FP2100의 ASA HA 라이선스

- 2100에서 ASA는 FXOS 관리가 아닌 ASA 인터페이스를 통해 Cisco Smart Licensing 포털(클라우드)과 통신합니다
 - 두 ASA를 모두 Cisco Smart Licensing 포털(클라우드)에 등록해야 합니다
- 이 경우 외부 인터페이스에서 HTTP 로컬 인증이 사용됩니다.

```

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

```

활성화된 3DES/AES 라이선스가 있는 경우에만 ASDM을 통해 ASA에 연결할 수 있습니다. 아직 등록되지 않은 ASA의 경우 management-only. 컨피그레이션 가이드에 따라: "Strong Encryption(3DES/AES)은 ASDM을 시작할 수 있도록 License Authority 또는 Satellite 서버에 연결하기 전에 관리 연결에 사용할 수 있습니다. ASDM 액세스는 기본 암호화를 사용하는 관리 전용 인터페이스에서만 사용할 수 있습니다. Through-the-box 트래픽은 사용자가 연결하여 Strong Encryption 라이선스를 얻을 때까지 허용되지 않습니다." 다른 경우에는 다음과 같은 이점이 있습니다.


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

ASA가 인터넷 연결 인터페이스에 관리 전용으로 구성되어 있으므로 ASDM 연결이 가능하다는 점을 극복하려면 다음을 수행합니다.

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



Cisco ASDM 7.10(1)



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

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

Run Cisco ASDM as a local application

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

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

[Install ASDM Launcher](#)

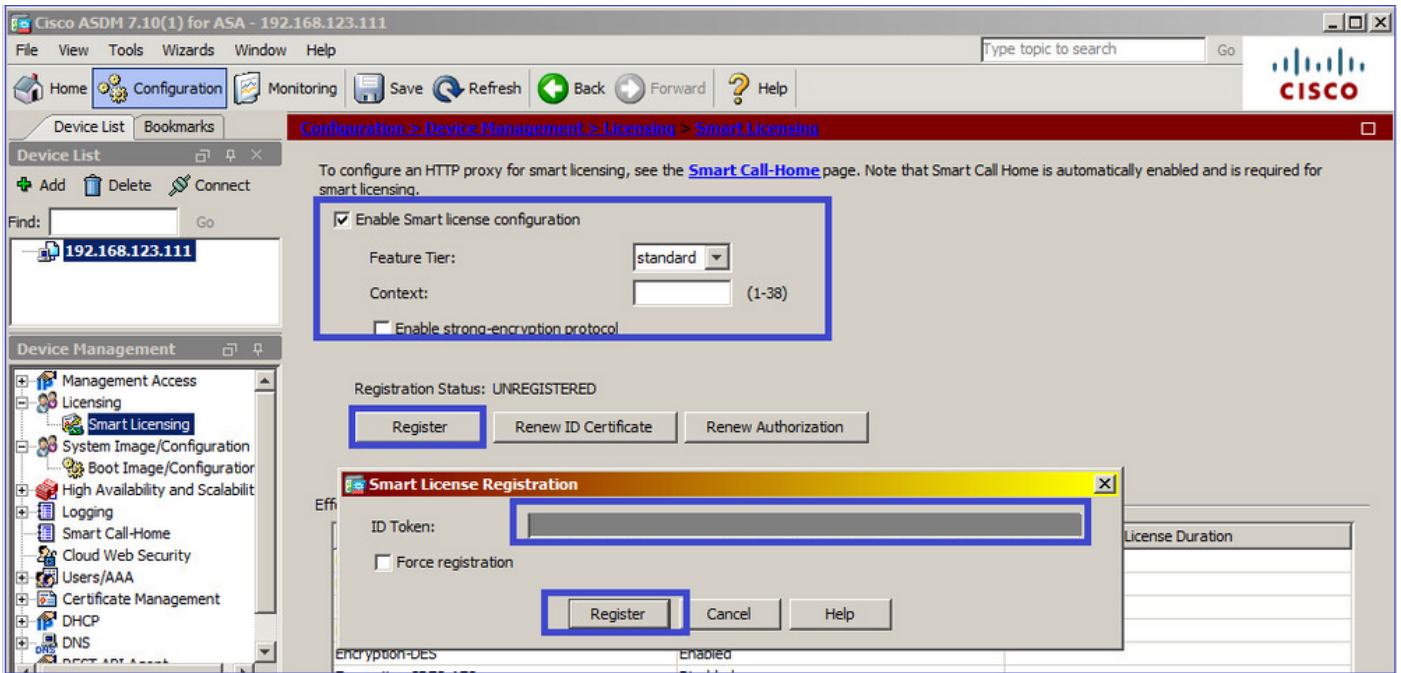
Run Cisco ASDM as a Java Web Start application

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

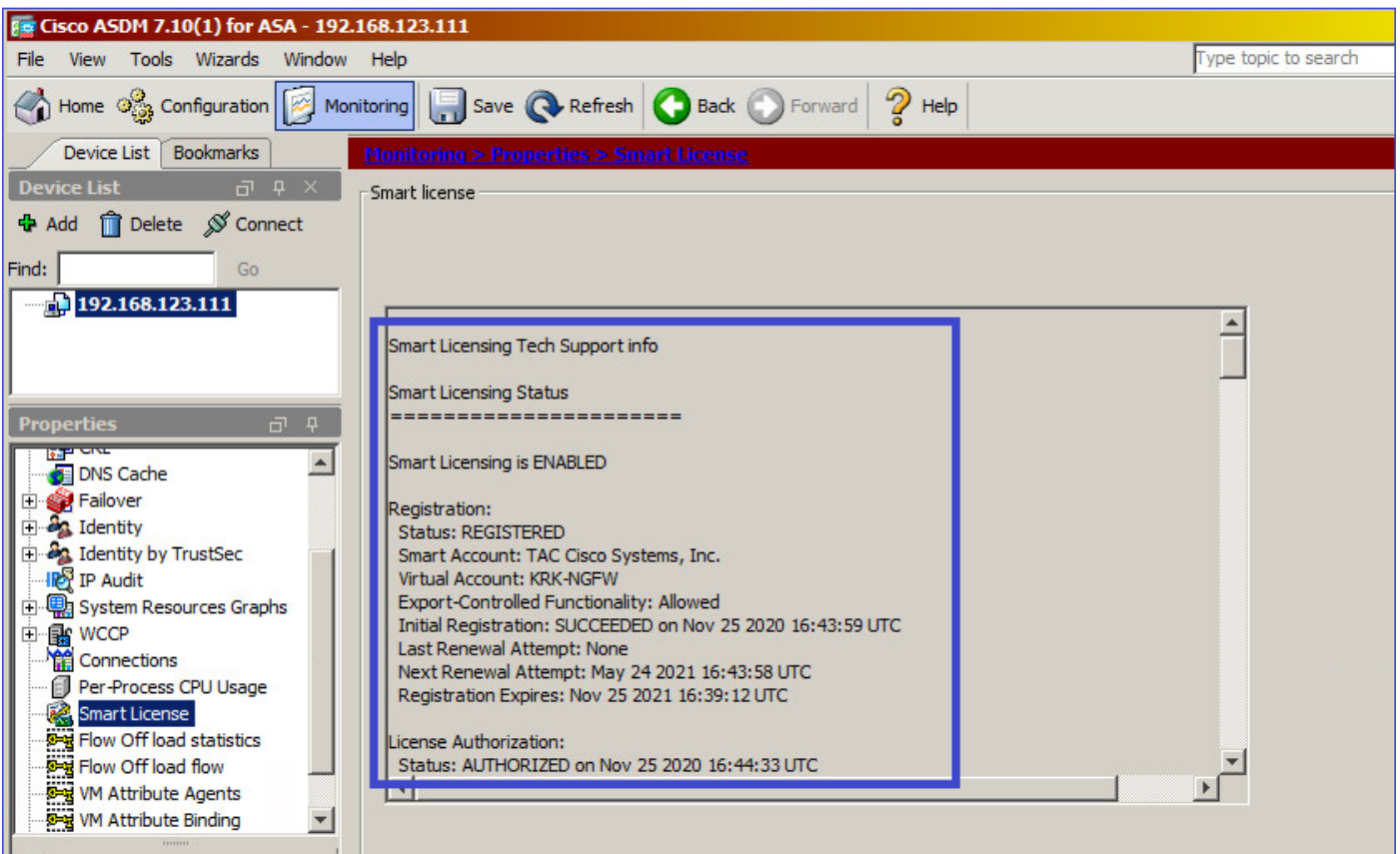
[Install Java Web Start](#)

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

기본 ASA에서 Smart Licensing을 구성합니다.



탐색 Monitoring > Properties > Smart License 등록 상태를 확인하려면



기본 ASA CLI 확인:

```
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

ASDM을 통해 대기 ASA에 연결합니다(ASA가 대기 IP로 구성된 경우에만 가능). 대기 ASA는 다음과 같이 표시됩니다 UNREGISTERED 이는 Smart Licensing 포털에 아직 등록되지 않았으므로 예상된 결과입니다.

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

Enable Smart license configuration

Feature Tier: (1-38)

Context: (1-38)

Enable strong-encryption protocol

Registration Status: UNREGISTERED

Register Renew ID Certificate Renew Authorization

Effective Running Licenses

License Feature	License Value	License Duration
Maximum Physical Interfaces	Unlimited	
Maximum VLANs	1024	
Inside Hosts	Unlimited	
Falover	Active/Active	
Encryption-DES	Enabled	
Encryption-3DES-AES	Enabled	
Security Contexts	4	
Carrier	Disabled	
AnyConnect Premium Peers	10000	
AnyConnect Essentials	Disabled	
Other VPN Peers	10000	
Total VPN Peers	10000	
AnyConnect for Mobile	Enabled	
AnyConnect for Cisco VPN Phone	Enabled	
Advanced Endpoint Assessment	Enabled	

Smart license

Smart Licensing Tech Support info

Smart Licensing Status
=====

Smart Licensing is ENABLED

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

License Authorization:
Status: No Licenses in Use

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED

대기 ASA CLI에는 다음이 표시됩니다.

```
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

스탠바이 ASA에서 활성화된 라이선스 기능은 다음과 같습니다.

```
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

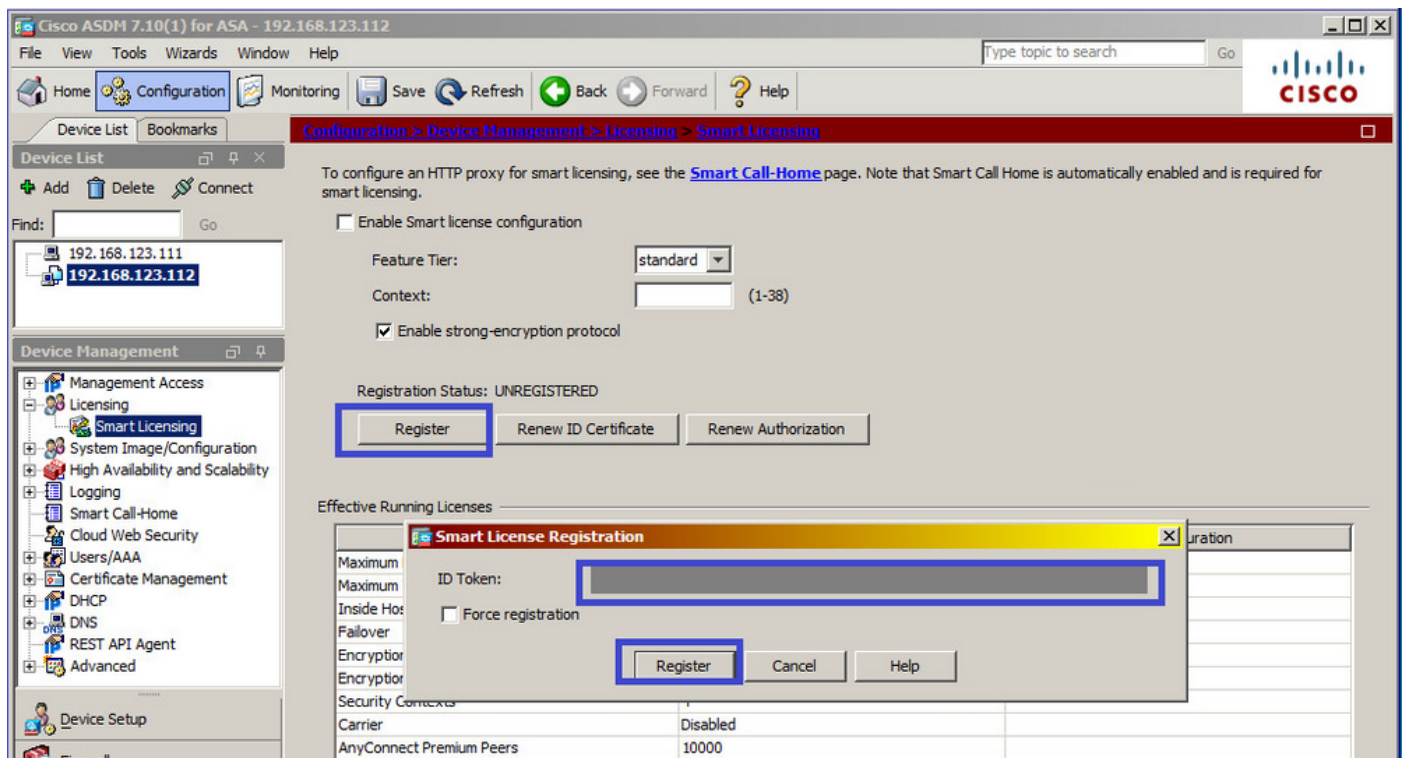
Advanced Endpoint Assessment : Enabled

Shared License : Disabled

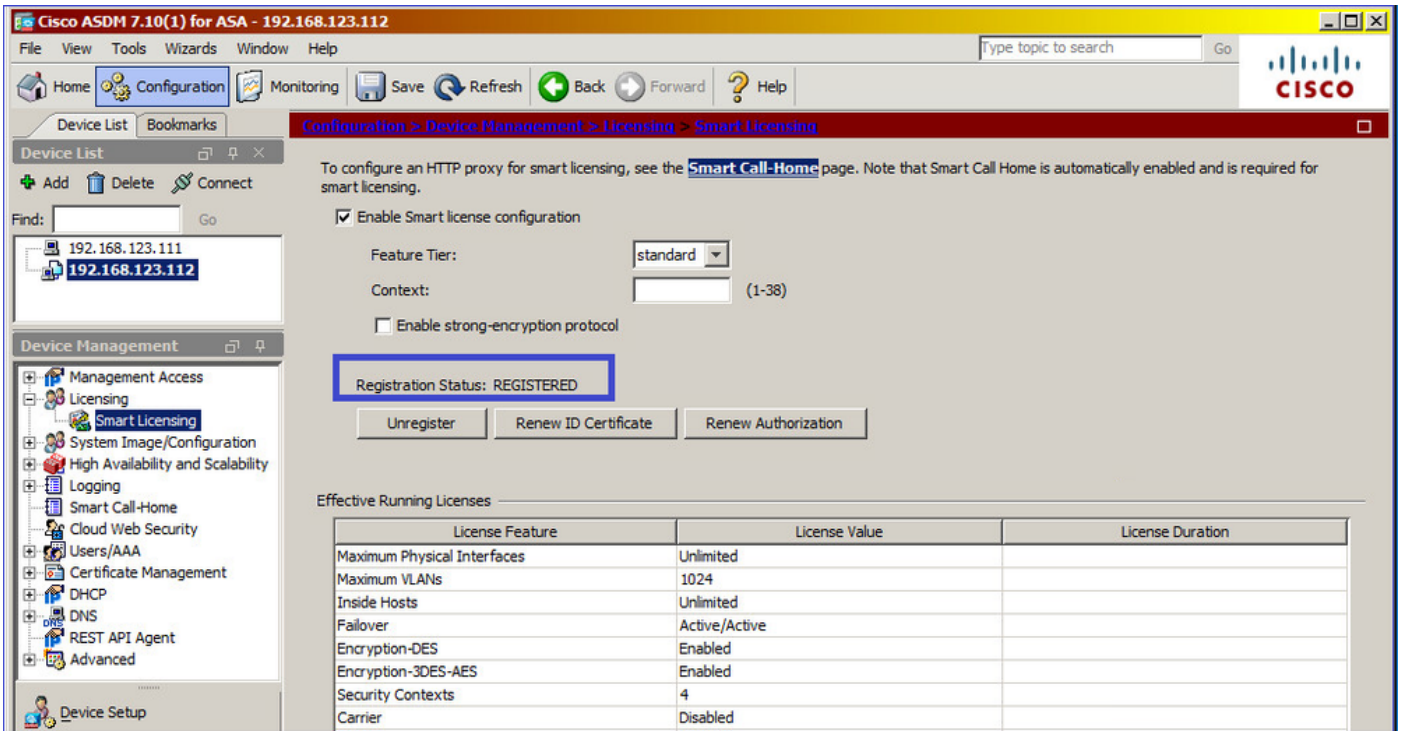
Total TLS Proxy Sessions : 10000

Cluster : Disabled

대기 ASA 등록:



스탠바이 ASA의 결과는 REGISTERED:



스탠바이 ASA에서 CLI 확인:

```
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 클러스터

디바이스에 라이선스 불일치가 있는 경우 클러스터가 형성되지 않습니다.

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

성공적인 클러스터 설정:

```
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.
```

클러스터 제어 노드:

```
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-b3f7fblcacfc
```

```
  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
```

클러스터 데이터 단위:

```
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

확인 및 디버깅

새시(MIO) 확인 명령 요약:

```
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
```

구성 확인:

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

ASA Summary of Verification 명령:

```
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
```

새시(MIO) 검증 명령의 샘플 출력

```
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+hvc5MuNbWlYv2uAnUVb3GbsvDWl99/KA==
-----END CERTIFICATE-----
Cert Status: Valid

```
Trustpoint Name: CSC02099SUDI
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIDIITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
...
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8DfleXbFg==
-----END CERTIFICATE-----
```

Cert Status: Valid

```
Trustpoint Name: CSC0BA2099SUDI
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIDQTCCAimgAwIBAgIJAAZa8V7p1OvhMA0GCSqGSIb3DQEBCwUAMD0xDjAMBgNV
...
b/JPEAZkbji0RQTWLyfr82LWFL00
-----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 검증 명령의 샘플 출력

```
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-  
b3f7fblcacfc
```

```
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-b3f7fblcacfc
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-b3f7fblcacfc

Version: 1.0

Enforcement mode: Authorized

Handle: 1

Requested time: Tue, 04 Aug 2020 07:58:13 UTC

Requested count: 1

Request status: Complete

등록 성공

출력은 새시 관리자 UI(User Interface)에서 옵니다.

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

만료된 권한 부여

출력은 새시 관리자 UI에서 옵니다.

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

ZDA2MjF1ODktYjllMS00NjQwLTk0MmUtYmVkyWU2NzIyZjYwLTF1ODIxODY2%0AMzEwODV8K2RWVTNURGF1K0tDYUhoSjg3b

jFsdytwbu1SUI81N20rQTPVN21T%0AdEtvYz0%3D%0A

Error : Smart Agent already registered

Cisco Success Network: DISABLED

새시 CLI의 샘플 출력

등록되지 않음

```
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
```

등록 진행 중

```
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

등록 오류

```
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

평가 기간

```
firepower# show license all
```

Smart Licensing Status

=====

Smart Licensing is ENABLED

Registration:

Status: REGISTERING - REGISTRATION IN PROGRESS

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

Next Registration Attempt: Aug 04 05:06:16 2020 UTC

License Authorization:

Status: EVALUATION MODE

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

License Usage

=====

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

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

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

FXOS 새시의 일반적인 라이선스 문제(MIO)

등록 오류: 잘못된 토큰

```
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 'ODNmNTExMTAtY2YzOS00Mzc1LWEzNWmtYmNiMmUyNzM4ZmFjLTE1OTkxMTkz%0ANDk0NjR8NkJJdWZpQzRDbmtPR0xBWlVpUzZqMjlySn15QUczT2M0YVIvcmxm%0ATGczND0%3D%0B' is not valid."]}
```

권장 단계

1. Call-home URL이 CSSM을 가리키는지 확인합니다.
2. CSSM에 로그인하여 토큰이 CSSM에서 생성되었는지 또는 토큰이 만료되었는지 확인합니다

등록 오류: 제품이 이미 등록되었습니다.

```
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."]}
```

권장 단계

1. CSSM에 로그인합니다.
2. 다음을 확인하십시오. Product Instances 모든 가상 어카운트의 탭입니다.
3. SN별로 이전 등록 인스턴스를 찾아 제거합니다.
4. 이 문제는 다음 두 가지 원인으로 인해 발생할 수 있습니다. 시간/날짜가 올바르게 설정되지 않은 경우(예: NTP 서버가 구성되지 않은 경우) 자동으로 갱신되지 않습니다.위성과 프로덕션 서버 간을 전환할 때 잘못된 작동 순서(예: 먼저 URL을 변경한 다음 '등록 취소'를 실행함)

등록 오류: 날짜 오프셋이 제한을 초과합니다.

```
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."]}
```

권장 단계

시간/날짜 컨피그레이션을 확인하여 NTP 서버가 구성되어 있는지 확인합니다.

등록 오류: 호스트를 확인하지 못했습니다.

```
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
```


권장 단계

1. Callhome SLDest URL이 정확한지 확인합니다(scope monitoring > scope callhome > show expand)
2. MIO DNS 서버 컨피그레이션이 올바른지 확인합니다(예: CLI에서).

```
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. 새시 CLI에서 ping을 시도하여 tools.cisco.com 해결되는지 확인합니다.

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

4. 새시 CLI에서 DNS 서버로 ping을 시도합니다.

```
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. 새시(MIO) 관리 인터페이스에서 캡처를 활성화하고(FP41xx/FP93xx에만 해당) 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
```

등록 오류: 서버를 인증하지 못했습니다.

```
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

권장 단계

1. MIO 신뢰 지점 CHdefault에 올바른 인증서가 있는지 확인합니다. 예를 들면 다음과 같습니다.

```
FPR4125-1# scope security
FPR4125-1 /security # show trustpoint
Trustpoint Name: CHdefault
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTElMAkGA1UEBhMCQk0x
...
8e0x79+Rj1QqCyXBjhnEUhAFzdWCEOrCMc0u
-----END CERTIFICATE-----
Cert Status: Valid
```

2. NTP 서버 및 표준 시간대가 올바르게 설정되었는지 확인합니다. 인증서 확인에는 서버와 클라이언트 간에 동일한 시간이 필요합니다. 이를 위해 NTP를 사용하여 시간을 동기화합니다. 예를 들어, FXOS UI 확인:

The screenshot shows the 'Platform Settings' page with the 'Time Synchronization' tab selected. Under 'Set Time Source', the 'Use NTP Server' radio button is selected. Below this, a table lists the configured NTP servers and their synchronization status.

NTP Server	Server Status	Actions
172.18.108.15	Candidate	[Edit] [Refresh]
172.18.108.14	Synchronized	[Edit] [Refresh]
10.62.148.75	Unreachable/Invalid	[Edit] [Refresh]

At the bottom of the page, there are 'Save' and 'Cancel' buttons. A note at the bottom states: 'Use same settings on Firepower Management Center managing this application in case you are running a Firepower Threat Defense Device.'

CLI 확인

```
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

캡처를 활성화하고 MIO와 간의 TCP 통신(HTTPS)을 tools.cisco.com. 몇 가지 옵션이 있습니다.

- FXOS UI에 대한 HTTPS 세션을 담은 다음 HTTPS용 CLI에서 캡처 필터를 설정할 수 있습니다. 예를 들면 다음과 같습니다.

```
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
```

- 또한 FXOS UI를 열어 두려는 경우 캡처에서 대상 IP(72.163.4.38 및 173.37.145.8)를 지정할 수 있습니다. tools.cisco.com 서버). 또한 캡처를 pcap 형식으로 저장하고 Wireshark에서 확인하는 것이 좋습니다. 다음은 성공적인 등록의 예입니다.

```
FPR4125-1(fxos)# ethanalyzer local interface mgmt capture-filter "tcp port 443 and (host 72.163.4.38 or host 173.37.145.8)" limit-captured-frames 0 limit-frame-size 10000 write workspace:///SSL.pcap
Capturing on 'eth0'
 1 2020-08-07 08:39:02.515693672 10.62.148.225 173.37.145.8 TCP 74 59818 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=800212367 TSecr=0 WS=512
 2 2020-08-07 08:39:02.684723361 173.37.145.8 10.62.148.225 TCP 60 443 59818 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1330
 3 2020-08-07 08:39:02.684825625 10.62.148.225 173.37.145.8 TCP 54 59818 443 [ACK] Seq=1 Ack=1 Win=29200 Len=0
 4 2020-08-07 08:39:02.685182942 10.62.148.225 173.37.145.8 TLSv1 571 Client Hello
...
11 2020-08-07 08:39:02.854525349 10.62.148.225 173.37.145.8 TCP 54 59818 443 [ACK] Seq=518 Ack=3991 Win=37240 Len=0
```

- pcap 파일을 원격 FTP 서버로 내보내려면

```

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)#

```

No.	Time	Source	Destination	Protocol	Length	Server Name	Info
4	2020-08-07 10:39:02.68...	10.62.148.225	173.37.145.8	TLSv1.2	571	tools.cisco.com	Client Hello
13	2020-08-07 10:39:03.02...	173.37.145.8	10.62.148.225	TLSv1.2	78		Server Hello, Certificate, Server Hello Done
15	2020-08-07 10:39:03.02...	10.62.148.225	173.37.145.8	TLSv1.2	372		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
18	2020-08-07 10:39:03.19...	173.37.145.8	10.62.148.225	TLSv1.2	99		Encrypted Handshake Message
43	2020-08-07 10:39:11.20...	10.62.148.225	173.37.145.8	TLSv1.2	571	tools.cisco.com	Client Hello
52	2020-08-07 10:39:11.54...	173.37.145.8	10.62.148.225	TLSv1.2	78		Server Hello, Certificate, Server Hello Done
54	2020-08-07 10:39:11.55...	10.62.148.225	173.37.145.8	TLSv1.2	372		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
57	2020-08-07 10:39:11.72...	173.37.145.8	10.62.148.225	TLSv1.2	99		Encrypted Handshake Message
80	2020-08-07 10:39:14.51...	10.62.148.225	72.163.4.38	TLSv1.2	571	tools.cisco.com	Client Hello
89	2020-08-07 10:39:14.83...	72.163.4.38	10.62.148.225	TLSv1.2	78		Server Hello, Certificate, Server Hello Done
91	2020-08-07 10:39:14.84...	10.62.148.225	72.163.4.38	TLSv1.2	372		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
94	2020-08-07 10:39:15.00...	72.163.4.38	10.62.148.225	TLSv1.2	99		Encrypted Handshake Message

등록 오류: HTTP 전송 실패

```

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

```

권장 단계

1. Call-home URL이 올바른지 확인합니다. FXOS UI 또는 CLI에서 확인할 수 있습니다(scope monitoring > show callhome detail expand).
2. 캡처를 활성화하고 MIO와 간의 TCP 통신(HTTPS)을 tools.cisco.com 이 문서의 '서버 인증 실패' 섹션에 나와 있습니다.

등록 오류: 호스트에 연결할 수 없습니다.

```
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
```

권장 단계

1. 프록시 컨피그레이션이 활성화된 경우 프록시 URL 및 포트가 올바르게 구성되었는지 확인합니다.
2. 캡처를 활성화하고 MIO와 간의 TCP 통신(HTTPS)을 tools.cisco.com 이 문서의 '서버 인증 실패' 섹션에 나와 있습니다.

등록 오류: HTTP 서버에서 오류 코드 >= 400을 반환합니다.

```
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
```

권장 단계

1. 프록시 컨피그레이션이 활성화된 경우 프록시 서버 관리자에게 프록시 설정에 대해 문의하십시오.
2. 캡처를 활성화하고 MIO와 간의 TCP 통신(HTTPS)을 tools.cisco.com 이 문서의 '서버 인증 실패' 섹션에 나와 있습니다. FXOS CLI에서 다시 등록('force' 옵션)을 시도합니다.

```
FPR4125-1 /license # register idtoken  
ODNmNTExMTAtY2YzOS00Mzc1LWEzNWmtYmNiMmUyNzY4ZmFjLWU1OTkxMTkz%0ANDk0NjR8NkYJdWZpQzRDbmtPR0xRW1VpU  
zZqMjlySn15QUczT2M0YVIvcxmx%0ATGczND0%3D%0A force
```

등록 오류: 백 엔드 응답 메시지를 구문 분석하지 못했습니다.

```
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
```

권장 단계

1. 나중에 자동으로 다시 시도합니다. 'renew'를 사용하여 즉시 다시 시도하십시오.

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

2. Call Home URL이 정확한지 확인합니다.

ASA의 라이선스 문제 - 1xxx/21xx Series

등록 오류: 통신 메시지 전송 오류

```
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
```

권장 단계

1. DNS 설정 확인

```
ciscoasa# show run dns
```

2. ping 시도 `tools.cisco.com`. 이 경우 관리 인터페이스가 사용됩니다.

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

3. 공정순서 테이블을 확인합니다.

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

다음과 같이 라이선스가 활성화되었는지 확인합니다.

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

4. 다음 방향으로 라우팅되는 인터페이스에서 캡처를 활성화합니다. `tools.cisco.com` (IP 필터 없이 캡처를 수행하는 경우 불필요한 캡처 노이즈를 방지하기 위해 캡처를 수행할 때 ASDM이 열려 있지 않아야 합니다.)

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

경고: 패킷 캡처는 성능에 악영향을 미칠 수 있습니다.

5. 일시적으로 Syslog 레벨 7(디버그)을 활성화하고 등록 프로세스 동안 ASA Syslog 메시지를 확인합니다.

```
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
```

다시 등록 시도:

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

추가 기능 사용 자격에 대한 특별 요구 사항

- 추가 기능 자격을 구성하기 전에 유효한 기능 계층 자격을 얻어야 합니다.
- 기능 계층 자격을 해제하기 전에 모든 추가 기능 자격을 해제해야 합니다

재부팅 작업 중 자격 상태

- 자격 상태는 플래시에 저장됩니다
- 부팅 시간 동안 이 정보는 플래시에서 읽히고 라이선스는 저장된 시행 모드에 따라 설정됩니다
- 시작 컨피그레이션은 이 캐시된 자격 정보를 기반으로 적용됩니다
- 재부팅 후 자격 부여가 다시 요청됨

Cisco TAC 지원 참여

FP41xx/FP9300

이 문서에 언급된 모든 항목에 장애가 발생하면 새시 CLI에서 이러한 출력을 수집하고 Cisco TAC에 문의하십시오.

출력 1:

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

출력 2:

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

출력 3:

FXOS 새시 지원 번들

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


출력 4(적극 권장):

새시 CLI에서 Ethalyzer 캡처

FP1xxx/FP21xx

출력 1:

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

출력 2:

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

자주 묻는 질문(FAQ)

FP21xx에서 새시(FCM) GUI의 Licensing(라이선싱) 탭은 어디에 있습니까?
9.13.x부터 FP21xx는 2개의 ASA 모드를 지원합니다.

- 어플라이언스
- 플랫폼

어플라이언스 모드에서는 새시 UI가 없습니다. 플랫폼 모드에서는 새시 UI가 있지만 라이선스는 ASA CLI 또는 ASDM에서 구성됩니다.

반면, FPR4100/9300 플랫폼에서는 GUI 또는 FXOS CLI를 통해 FCM에 라이선스를 구성해야 하며 ASA 엔타이틀먼트는 ASA CLI 또는 ASDM에서 요청해야 합니다.

참조:

- [ASA의 라이선스 관리](#)
- [Firepower 4100/9300용 논리적 디바이스](#)
- [라이선스: Smart Software Licensing\(ASA, Firepower의 ASA\)](#)
- [ASDM 및 Firepower Chassis Manager를 사용하는 ASA 플랫폼 모드 구축](#)

Strong Encryption License를 활성화하려면 어떻게 해야 하나요?

이 기능은 FCM 등록에 사용된 토큰에 이 토큰이 활성화된 상태로 등록된 제품에 대한 내보내기 제어 기능을 허용하는 옵션이 있는 경우 자동으로 활성화됩니다.

FCM 레벨의 Export-Controlled Features 및 ASA 레벨의 관련 Encryption-3DES-AES가 비활성화된 경우 Strong Encryption License를 활성화하려면 어떻게 해야 하나요?

토큰에 이 옵션이 활성화되어 있지 않으면 FCM을 등록 취소하고 이 옵션이 활성화된 토큰으로 다시 등록합니다.

토큰을 생성할 때 이 토큰으로 등록된 제품에 대한 수출 통제 기능 허용 옵션을 사용할 수 없는 경우 어떻게 할 수 있습니까?

Cisco 어카운트 팀에 문의하십시오.

ASA 레벨에서 Strong Encryption 기능을 구성해야 합니까?

강력한 암호화 기능은 FCM이 2.3.0 이전 Satellite 서버와 통합된 경우에만 필수 기능입니다. 이 기능은 이 기능을 구성해야 하는 한 가지 시나리오뿐입니다.

FCM과 Smart Licensing 클라우드 간의 경로에 어떤 IP를 허용해야 합니까?

FXOS는 주소 <https://tools.cisco.com/>(포트 443)를 사용하여 라이선싱 클라우드와 통신합니다. 주소 <https://tools.cisco.com/>은 다음 IP 주소로 확인됩니다.

- 72.163.4.38
- 173.37.145.8

규정 준수 위반 오류가 발생하는 이유는 무엇입니까?

다음과 같은 경우 디바이스가 규정을 준수하지 않을 수 있습니다.

- 초과 사용(디바이스에서 사용할 수 없는 라이선스 사용)
- 라이선스 만료 - 기간별 라이선스가 만료됨
- 통신 부족 - 장치가 다시 권한 부여를 위해 라이선싱 기관에 연결할 수 없습니다.

어카운트가 규정 위반 상태인지 또는 규정 위반 상태에 근접했는지 확인하려면 Firepower 새시에서 현재 사용 중인 엔타이틀먼트를 Smart Account의 엔타이틀먼트와 비교해야 합니다.

컴플라이언스 위반 상태에서 특별 라이선스가 필요한 기능에 대한 컨피그레이션을 변경할 수 있지만, 그 외에는 작업에 영향을 미치지 않습니다. 예를 들어, 이미 존재하는 표준 라이선스 제한 컨텍스트는 계속 실행되며, 해당 컨피그레이션을 수정할 수 있지만 새 컨텍스트를 추가할 수는 없습니다.

라이선스를 추가한 후에도 규정 준수 위반 오류가 발생하는 이유는 무엇입니까?

기본적으로 디바이스는 License Authority와 30일마다 통신하여 엔타이틀먼트를 확인합니다. 수동으로 트리거하려면 다음 단계를 수행해야 합니다.

FPR1000/2100 플랫폼의 경우 ASDM 또는 CLI를 통해 수행해야 합니다.

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

FPR4100/9300 플랫폼의 경우 FXOS CLI를 통해 수행해야 합니다.

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

ASA 레벨에서 사용 중인 라이선스가 없는 이유는 무엇입니까?

ASA 엔타이틀먼트가 ASA 레벨에서 구성되었는지 확인합니다. 예:

```
ASA(config)# license smart
```

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

ASA 엔타이틀먼트를 구성한 후에도 라이선스가 여전히 사용되지 않는 이유는 무엇입니까?

이 상태는 ASA 액티브/스탠바이 장애 조치 쌍을 구축하고 스탠바이 디바이스에서 라이선스 사용량을 확인하는 경우에 필요합니다.

컨피그레이션 가이드에 따라 컨피그레이션이 스탠바이 유닛에 복제되지만 스탠바이 유닛에서는 컨피그레이션을 사용하지 않으며 캐시된 상태로 유지됩니다. 활성 유닛만 서버에서 라이선스를 요청합니다. 라이선스는 장애 조치 쌍이 공유하는 단일 장애 조치 라이선스로 통합되며, 이 통합된 라이선스는 향후 액티브 유닛이 될 경우 사용할 스탠바이 유닛에도 캐시됩니다. 참조: [장애 조치 또는 ASA 클러스터 라이선스](#).

FCM이 인터넷에 액세스할 수 없는 경우 어떻게 할 수 있습니까?

또는 Cisco Smart Software Manager 온프레미스(이전의 Cisco Smart Software Manager Satellite)를 구축할 수 있습니다. Cisco Smart Software Manager와 함께 작동하는 Cisco Smart Licensing의 구성 요소입니다. 고객이 구매하고 사용하는 Cisco 라이선스에 대한 거의 실시간 가시성 및 보고 기능을 제공합니다. 또한 보안에 민감한 조직은 직접 인터넷 연결을 사용하여 설치 기반을 관리하지 않고도 Cisco SSM 기능의 일부에 액세스할 수 있습니다.

Cisco Smart Software Manager 온프레미스(온프레미스)에 대한 자세한 내용은 어디에서 확인할 수 있습니까?

이 정보는 FXOS 컨피그레이션 가이드에서 확인할 수 있습니다.

- [Firepower 4100/9300 새시용 Smart License Satellite Server 구성](#)
- [Smart Software Manager 온프레미스\(온프레미스\)에 Firepower Chassis Manager 등록 구성](#)

관련 정보

- [Cisco ASA Series 일반 운영 CLI 컨피그레이션 가이드](#)
- [ASA의 라이선스 관리](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.