

Hyperflex 라이선스 등록 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[Smart License란?](#)

[Hyperflex에서 라이선스의 작동 방식](#)

[엄격한 시행 정책](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[시나리오 1: HTTP/HTTP 연결](#)

[시나리오 2: 프록시 문제](#)

[시나리오 3: 클라우드 환경](#)

[시나리오 4: OCSP\(Online Certificate Status Protocol\)](#)

[시나리오 5: 인증서 변경됨](#)

[추가 절차](#)

[관련 정보](#)

소개

이 문서에서는 Hyperflex 등록 라이선스 문제의 가장 일반적인 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- Hyperflex Connect
- 라이선스 등록
- HTTP/HTTPS

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- HXDP(Hyperflex Data Program) 5.0.(2a) 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Smart License란?


Cisco Smart Licensing(Smart Licensing)은 지능형 클라우드 기반 소프트웨어 라이선스 관리 솔루션으로서 조직 전체에서 세 가지 핵심 라이선스 기능(구매, 관리 및 보고)을 간소화합니다.

[여기서](#) Smart License 어카운트에 액세스할 수 있습니다.

Hyperflex에서 라이선스의 작동 방식

Cisco Hyperflex는 Smart Licensing과 통합되며 Hyperflex 스토리지 클러스터를 생성할 때 기본적으로 자동으로 활성화됩니다. 그러나 Hyperflex 스토리지 클러스터에서 라이선스를 사용하고 보고하려면 Cisco Smart Account를 통해 Cisco SSM(Smart Software Manager)에 등록해야 합니다.

Smart Account는 클라우드 기반 저장소로, 회사 전체에서 구매한 모든 Cisco 소프트웨어 라이선스와 제품 인스턴스에 대한 완전한 가시성과 액세스 제어를 제공합니다.

 참고: Hyperflex 클러스터에서는 1년간 등록이 유효합니다. 이후 Hyperflex는 자동으로 재등록을 시도하므로 사람의 상호 작용이 필요하지 않습니다.

엄격한 시행 정책

버전 HXDP 5.0(2a)부터 클러스터가 라이선스를 준수하지 않는 경우 일부 기능이 Hyperflex Connect GUI에서 차단됩니다.

라이선스 상태 예제 시나리오:

이 시나리오에서 클러스터는 라이선스 상태를 준수합니다.

System Overview Nodes Disks Last refreshed at: 04/22/2022 8:17:58 AM

nitin-sl License Type: Datacenter Premier License Status: **In compliance** Actions

vCenter: https://10.33.16.26 Hypervisor: 6.7.0-17700523 Total Capacity: 4.82 TiB DNS Server(s): 10.33.24.8
 Uptime: 19 days, 20 hours, 26 minutes, 3 seconds HXDP Version: 5.0.2a-41522 Available Capacity: 4.66 TiB NTP Server(s): 10.33.24.12
 Encryption: Enabled Data Replication Factor: 3 Controller Access over SSH: Enable

Hyperconverged Nodes Disk View Options Disk View Legend

Node	Hypervisor	HyperFlex Controller	Disk Overview (1 in use 18 empty slots)
ucsblr530	Online	Online	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
HXAF240C-M5SX	10.20.16.96	10.20.16.102	21 22 23 24 25 26
	6.7.0-17700523	5.0.2a-41522	

다음 시나리오에서는 클러스터가 등록되지만 라이선스 상태가 규정 위반이며 유예 기간은 1일에서 90일 사이입니다.

이 경우 기능이 차단되지는 않지만, 유예 기간이 만료되기 전에 필요한 라이선스를 활성화하라는 배너가 메뉴 상단에 나타납니다.

System Overview Nodes Disks Last refreshed at: 04/22/2022 1:19:15 PM

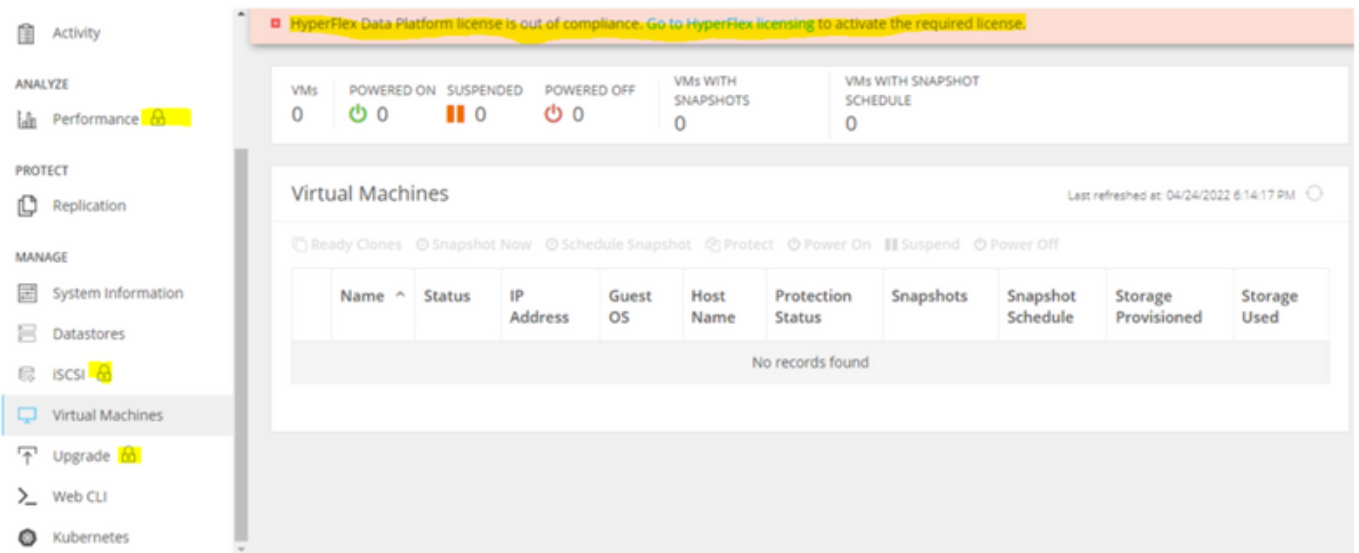
nitin-sl License Type: Datacenter Premier License Status: **Out of Compliance** Actions

vCenter: https://10.33.16.26 Hypervisor: 6.7.0-17700523 Total Capacity: 4.82 TiB DNS Server(s): 10.33.24.8
 Uptime: 20 days, 1 hours, 22 minutes, 45 seconds HXDP Version: 5.0.2a-41522 Available Capacity: 4.66 TiB NTP Server(s): 10.33.24.12
 Encryption: Enabled Data Replication Factor: 3 Controller Access over SSH: Enable

Hyperconverged Nodes Disk View Options Disk View Legend

Node	Hypervisor	HyperFlex Controller	Disk Overview (1 in use 18 empty slots)
ucsblr530	Online	Online	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
HXAF240C-M5SX	10.20.16.96	10.20.16.102	21 22 23 24 25 26
	6.7.0-17700523	5.0.2a-41522	

이 시나리오에서는 클러스터가 등록되고, 라이선스 상태가 규정 위반이며, 유예 기간은 0(영)입니다



구성

Smart License 계정에 Hyperflex를 등록하는 방법에 대한 지침은 [이 비디오를 참조하십시오.](#)

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인합니다.

CLI를 통해 라이선스 상태를 확인합니다. 등록 상태 및 권한 부여 상태를 확인합니다.

```
admin:~$ stcli license show all
```

Registration:

```
Status: REGISTERED
Smart Account: TAC Cisco Systems, Inc.
Virtual Account: DC TAC
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Apr 12 15:59:46 2022 EDT
Last Renewal Attempt: SUCCEEDED on Apr 12 15:59:46 2022 EDT
Next Renewal Attempt: Oct 9 15:59:46 2022 EDT
Registration Expires: Apr 12 15:54:43 2023 EDT
```

Registration Status:
Registered
Registered – Specific License Reservation
Unregistered
Unregistered – Registration Pending

License Authorization:

```
Status: AUTHORIZED on Jul 14 08:55:08 2022 EDT
Last Communication Attempt: SUCCEEDED on Jul 14 08:55:08 2022 EDT
Next Communication Attempt: Aug 13 08:55:08 2022 EDT
Communication Deadline: Oct 12 08:50:08 2022 EDT
```

Authorization Status:
Authorized
Eval Mode
Evaluation Period Expired
Authorized – Reserved
Authorized Expired
No licenses in use

Evaluation Period:

```
Evaluation Mode: Not In Use
EVALUATION PERIOD EXPIRED on Apr 11 10:09:30 2022 EDT
```

문제 해결

이 두 가지 상태가 모두 동일한 근본 원인에 의해 실패할 수 있는 몇 가지 일반적인 시나리오가 있습니다

니다.

시나리오 1: HTTP/HTTPS 연결

라이선스 등록은 TCP, 특히 HTTP 및 HTTPS를 통해 이루어지므로 이 통신을 허용하는 것이 중요합니다.

각 SCVM(Storage Controller VM)에서 연결성을 테스트합니다. 주로 CMIP(Cluster Management IP) SCVM에서 연결성을 테스트합니다.

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

예시에 표시된 출력을 가져와야 합니다. 그렇지 않으면 트래픽이 차단됩니다.

```
<h1>DDCEService</h1>
<p>Hi there, this is an AXIS service!</p>
<i>Perhaps there will be a form for invoking the service here...</i>
```

수신된 출력이 이전 출력과 다른 경우 연결을 확인하고 다음 명령을 사용하여 포트가 열려 있는지 확인합니다.

```
ping tools.cisco.com -c 5
nc -zv tools.cisco.com 80
nc -zv tools.cisco.com 443
```

시나리오 2: 프록시 문제

트래픽에 대한 보안 검사를 수행할 때 모든 웹 클라이언트와 공용 웹 서버 간에 프록시가 구성되는 경우도 있습니다.

이 경우 CMIP가 있는 SCVM과 [cisco.com](https://tools.cisco.com) 간에 프록시가 클러스터에 이미 구성되어 있는지 확인합니다(예시에 나와 있음).

<#root>

```
hxshell:/var/log/springpath$ stcli services sch show
cloudEnvironment: production
enabled: True
emailAddress: johndoe@example.com
portalUrl:

enableProxy: True
```

```
proxyPassword:
encEnabled: True
proxyUser:
cloudAsupEndpoint: https://diag.hyperflex.io/
proxyUrl:
proxyPort: 0
```

프록시에서 이미 구성된 것을 표시하는 경우 구성된 포트와 함께 프록시 URL 또는 IP 주소로 연결을 테스트합니다.

```
curl -v --proxy https://url:
```

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

```
curl -v --proxy <Proxy IP>:<Proxy Port> https://tools.cisco.com/its/service/oddce/services/DDCEService
```

또한 프록시에 대한 연결을 테스트합니다.

```
nc -vzw2 x.x.x.x 8080
```

시나리오 3: 클라우드 환경

특정 상황에서는 클라우드 환경이 devtest로 설정되어 등록이 실패합니다. 이 예에서는 프로덕션으로 설정되어 있습니다.

<#root>

```
hxshell:/var/log/springpath$ stcli services sch show
```

```
cloudEnvironment: production
```

```
cloudAsupEndpoint: https://diag.hyperflex.io/
```

```
portalUrl:
```

```
proxyPort: 0
```

```
enabled: True
```

```
encEnabled: True
```

```
proxyUser:
```

```
proxyPassword:
```

```
enableProxy: True
```


```
emailAddress: johndoe@example.com
```

```
proxyUrl:
```

로그에서 환경이 devtest로 잘못 설정된 경우 특정 오류를 볼 수 있습니다.

```
cat hxLicenseSvc.log | grep -ia "Name or service not known"
```

```
2021-09-01-18:27:11.557 [] [Thread-40] ERROR event_msg_sender_log - sch-alpha.cisco.com: Name or service
```

 **팁:** 5.0(2a) 버전에서는 사용자가 Hyperflex 버전 4.5.x에 도입된 priv 명령줄을 통해 액세스할 수 없는 제한된 폴더 및 명령에 대한 액세스와 관련된 문제 해결 권한을 더 많이 가질 수 있도록 diag 사용자를 사용할 수 있습니다.


환경 유형을 프로덕션으로 변경하고 등록을 다시 시도할 수 있습니다.

```
diag# stcli services sch set --email johndoe@example.com --environment production --e
```

시나리오 4: OCSP(Online Certificate Status Protocol)

Hyperflex는 OCSP 및 CRL(Certificate Revocation List) 서버를 활용하여 라이선스 등록 프로세스 중에 HTTPS 인증서를 검증합니다.

이러한 프로토콜은 HTTP를 통해 폐기 상태를 배포하도록 설계되었습니다. CRL 및 OCSP 메시지는 OCSP 검증이 실패하고 라이선스 등록도 실패할 경우 X.509 인증서의 폐기 상태를 나타내는 공개 문서입니다.

 **팁:** OCSP가 실패하면 그 사이에 있는 보안 디바이스가 HTTP 연결을 중단합니다.

OCSP 검증이 양호한지 확인하기 위해 예시에 나와 있는 것처럼 CMIP SCVM/tmp 파티션에 파일을 다운로드해 볼 수 있습니다.

```
hxshell:~$cd /tmp
hxshell:/tmp$ wget http://www.cisco.com/security/pki/trs/ios_core.p7b
--2022-08-18 00:13:37-- http://www.cisco.com/security/pki/trs/ios_core.p7b
Resolving www.cisco.com (www.cisco.com)... x.x.x.x aaaa:aaaa:aaaa:aaaa::aaaa
Connecting to www.cisco.com (www.cisco.com)|x.x.x.x|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 25799 (25K)
Saving to: 'ios_core.p7b'
```

```
ios_core.p7b 100%[=====]
2022-08-18 00:13:37 (719 KB/s) - 'ios_core.p7b' saved [25799/25799]
```

```
hxshell:/tmp$ ls -lath ios*
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b.1
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b.2
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b.3
-rw-r--r-- 1 admin springpath 26K Jun 30 18:00 ios_core.p7b.4
```

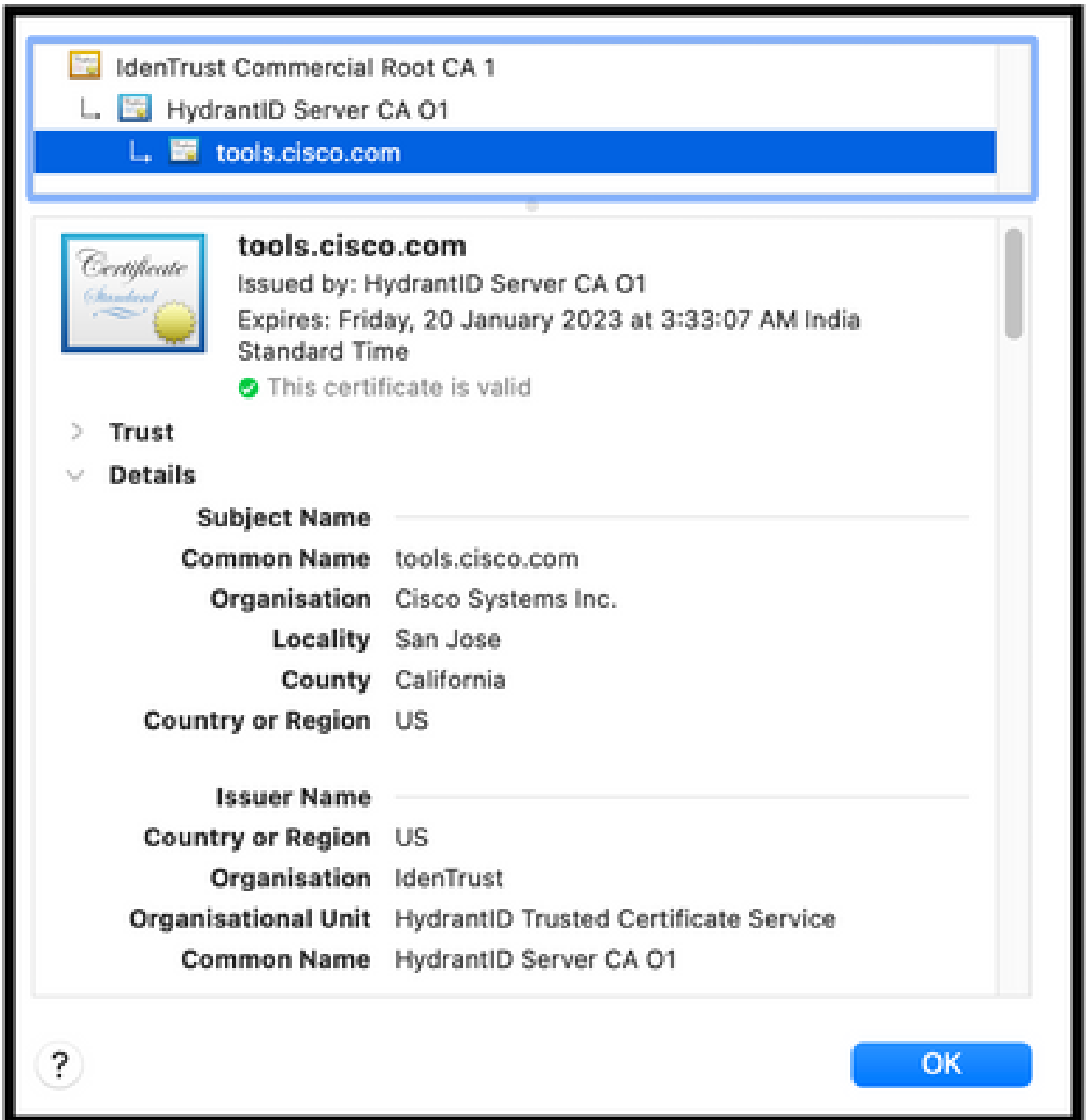
시나리오 5: 인증서 변경됨

일부 네트워크에서 프록시 및 방화벽 보안 디바이스는 SSL(Secure Sockets Layer) 검사를 실행하며 Hyperflex에서 from tools.cisco.com:443을 수신할 것으로 예상되는 인증서를 손상시킬 수 있습니다.

인증서가 프록시 또는 방화벽에 의해 변경되지 않았는지 확인하려면 CMIP를 보유한 SCVM에서 다음 명령을 실행합니다.

```
diag# openssl s_client -connect tools.cisco.com:443 -showcerts < /dev/null
```

Subject Name(주체 이름) 및 Issuer Name(발급자 이름) 정보가 이 예에 표시된 인증서와 일치해야 한다는 점을 유념해야 합니다.



⚠ 경고: 주체 또는 발급자의 필드가 하나 이상 다른 경우 등록이 실패합니다. Hyperflex 클러스터 관리 IP 및 tools.cisco.com:443에 대한 보안 SSL 검사의 우회 규칙을 통해 이를 해결할 수 있습니다.

이 예에서는 Hyperflex CMIP SCVM의 인증서에서 받은 동일한 정보를 검증하는 방법을 확인할 수 있습니다.

<#root>

```
hxshell:~$ su diag
```

```
diag# openssl s_client -connect tools.cisco.com:443 -showcerts < /dev/null
CONNECTED(00000003)
depth=2
```

```
C = US, O = IdenTrust, CN = IdenTrust Commercial Root CA 1
```

```
verify return:1
depth=1
```

```
C = US, O = IdenTrust, OU = HydrantID Trusted Certificate Service,
```

```
CN = HydrantID Server CA 01
```

```
verify return:1
depth=0
```

```
CN = tools.cisco.com, O = Cisco Systems Inc., L = San Jose, ST = California, C = US
```

```
verify return:1
```

```
---
```

```
Certificate chain
```

```
0 s:/
```

```
CN=tools.cisco.com
```

```
/
```

```
O=Cisco Systems Inc.
```

```
/
```

```
L=San Jose
```

```
/
```

```
ST=California
```

```
/
```

```
C=US
```

```
i:/
```

```
C=US
```

```
/
```

```
O=IdenTrust
```

```
/
```

```
OU=HydrantID Trusted Certificate Service
```

```
/C
```

```
N=HydrantID Server CA 01
```

```
...
```

```
<TRUNCATED>
```

```
...
```

```
1 s:/
```

C=US
/
O=IdenTrust
/
OU=HydrantID Trusted Certificate Service
/
CN=HydrantID Server CA 01

i:/
C=US
/
O=IdenTrust
/
CN=IdenTrust Commercial Root CA 1

...
<TRUNCATED>

...
2 s:/

C=US
/
O=IdenTrust
/
CN=IdenTrust Commercial Root CA 1

i:/
C=US
/
O=IdenTrust
/
CN=IdenTrust Commercial Root CA 1

...
<TRUNCATED>

...

Server certificate
subject=/
CN=tools.cisco.com

/

O=Cisco Systems Inc.

```
/
L=San Jose
/
ST=California
/
C=US

issuer=/
C=US
/
O=IdenTrust
/
OU=HydrantID Trusted Certificate Service
/
CN=HydrantID Server CA 01
```

```
---
...
<TRUNCATED>
...
---
DONE
```

추가 절차

이 절차는 지원되는 시나리오가 성공 또는 해결되었지만 라이선스 등록이 여전히 실패한 경우 활용할 수 있습니다.

라이선스를 등록 취소합니다.

```
hxshell:~$stcli license disable
hxshell:~$stcli license enable
hxshell:~$stcli license deregister
```

Smart Licensing에서 새 토큰을 획득하고 라이선싱 프로세스를 다시 시작한 후 라이선스 등록을 다시 시도하십시오.

```
hxshell:~$priv service hxLicenseSvc stop
hxshell:~$priv service hxLicenseSvc start
hxshell:~$stcli license register --idtoken IDTOKEN --force
```

관련 정보

- [Cisco HyperFlex HX Data Platform - 최종 사용자 설명서](#)

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.