

# Hyperflexライセンス登録問題のトラブルシューティング

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

#### [スマートライセンスとは](#)

#### [Hyperflexでのライセンスの動作方法](#)

#### [厳密な適用ポリシー](#)

### [設定](#)

### [確認](#)

### [トラブルシューティング](#)

#### [シナリオ1:HTTP/HTTPS接続](#)

#### [シナリオ2:プロキシの問題](#)

#### [シナリオ3:クラウド環境](#)

#### [シナリオ4:Online Certificate Status Protocol\(OCSP\)](#)

#### [シナリオ5:証明書の変更](#)

#### [追加手順](#)

### [関連情報](#)

---

## はじめに

このドキュメントでは、Hyperflex登録ライセンスの問題の最も一般的な問題をトラブルシューティングする方法について説明します。

## 前提条件

### 要件

次の項目に関する基本的な知識が推奨されます。

- Hyperflex接続
- ライセンス登録
- HTTP/HTTPS

### 使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

### スマートライセンスとは

Cisco Smart Licensing(Smart Licensing)は、インテリジェントなクラウドベースのソフトウェアライセンス管理ソリューションで、組織全体の3つの主要なライセンス機能(購入、管理、レポート)を簡素化します。


スマートライセンスアカウントには、[ここ](#)からアクセスできます。

### Hyperflexでのライセンスの動作方法

Cisco HyperflexはSmart Licensingと統合され、Hyperflexストレージクラスタの作成時にデフォルトで自動的に有効になります。ただし、Hyperflexストレージクラスタでライセンスを消費してレポートするには、Ciscoスマートアカウントを通じてCisco Smart Software Manager(SSM)に登録する必要があります。

スマートアカウントは、購入したすべてのシスコソフトウェアライセンスと会社全体の製品インスタンスに対する完全な可視性とアクセス制御を提供するクラウドベースのリポジトリです。

---

 注:Hyperflexクラスタでは、登録は1年間有効です。その後、Hyperflexは自動的に再登録を試みるため、手動による操作は不要です。

---

### 厳密な適用ポリシー

バージョンHXDP 5.0(2a)以降では、クラスタがライセンスに準拠していない場合、一部の機能はHyperflex Connect GUIからブロックされます。

ライセンスステータスのシナリオ例：

このシナリオでは、クラスタはライセンスステータスに準拠しています。

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	

次のシナリオでは、クラスタは登録されていますが、ライセンスの状態がコンプライアンスに違反しています。猶予期間は1 ~ 90日です。

この場合、機能はブロックされませんが、猶予期間が切れる前に必要なライセンスをアクティブにするよう求めるバナーがメニューの上部に表示されます。

HyperFlex Data Platform license is out of compliance and there are 90 days remaining in the grace period after which features will be blocked. Go to HyperFlex licensing to activate the required license. 90 d

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

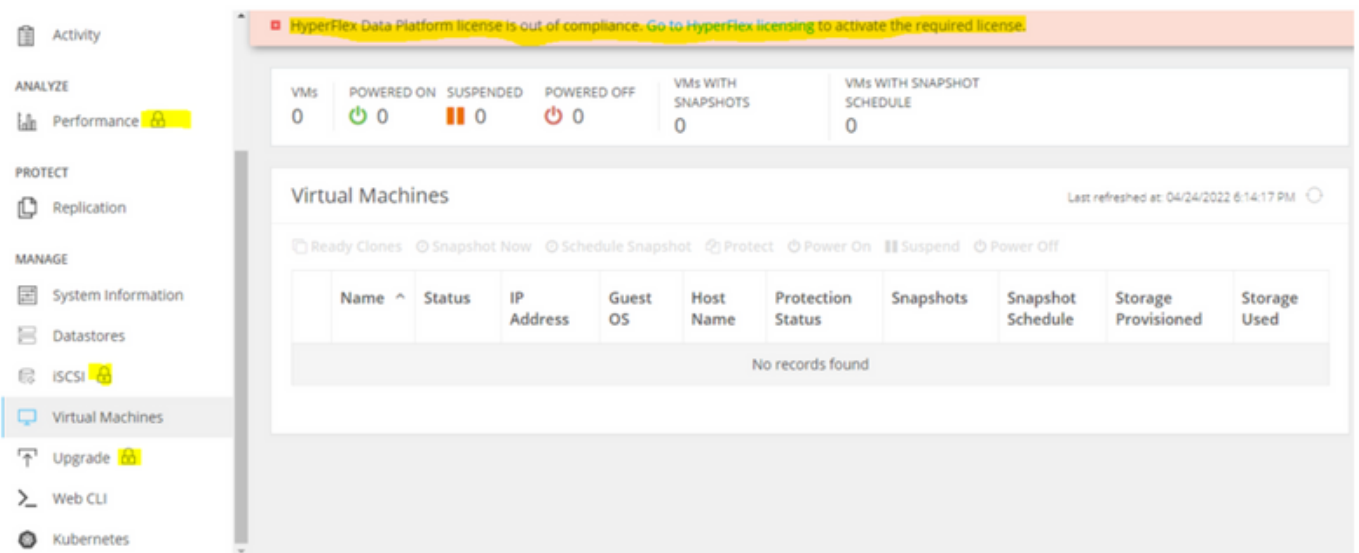
**nitin-sl** License Type: Datacenter Premier License Status: **Out of Compliance** Actions

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	

このシナリオでは、クラスタが登録され、ライセンスの状態がOut of Complianceで、猶予期間がゼロ(0)になっています。



## 設定

スマートライセンスアカウントでHyperflexを登録する方法については、[このビデオを確認してください。](#)

## 確認

設定が正しく動作していることを確認します。

CLIを使用してライセンスのステータスを確認します。登録ステータスと認証ステータスを表示します。

```
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
```

## トラブルシューティング

これら2つのステータスが失敗する可能性がある一般的なシナリオがいくつかあります。どちらのステータスも同じ根本原因によって引き起こされます。

## シナリオ1:HTTP/HTTPS接続

ライセンス登録はTCP、具体的にはHTTPおよびHTTPSを介して行われるため、この通信を許可することが重要です。

各ストレージコントローラVM(SCVM)からの接続をテストしますが、主にクラスタ管理IP(CMIP)SCVMからの接続をテストします。

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

例に示されている出力を取得する必要があります。取得しない場合は、トラフィックがブロックされていることを意味します。

```
<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>
```

受信した出力が前の出力と異なる場合は、接続を確認し、次のコマンドでポートが開いていることを確認します。

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

## シナリオ2：プロキシの問題

トラフィックのセキュリティ検査を実行する際に、すべてのWebクライアントとパブリックWebサーバの間にプロキシが設定されることがあります。

この場合は、CMIPを使用するSCVMとcisco.comの間で、プロキシがクラスタにすでに設定されていることを確認します（例を参照）。

```
<#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
```

プロキシがすでに設定済みと表示されている場合は、設定済みのポートとともに、プロキシ URL または IP アドレスを使用して接続をテストします。

```
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
```

さらに、プロキシへの接続をテストします。

```
nc -vzW2 x.x.x.x 8080
```

### シナリオ3：クラウド環境

特定の状況では、クラウド環境が devtest に設定されているため、登録が失敗します。この例では、実稼働に設定されています。

```
<#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:
```

環境がdevtestとして誤って設定されている場合、ログから特定のエラーを確認できます。

```
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
```

---

 ヒント:5.0(2a)バージョンからdiagユーザを使用できるようになりました。このユーザは、より多くの特権を持ち、Hyperflexバージョン4.5.xで導入されたprivコマンドラインではアクセスできない、制限されたフォルダやコマンドにアクセスしてトラブルシューティングを行うことができます。

---

環境タイプを実稼働に変更して、登録を再試行できます。


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

## シナリオ4:Online Certificate Status Protocol(OCSP)

Hyperflexは、OCSPおよび証明書失効リスト(CRL)サーバを利用して、ライセンス登録プロセス中にHTTPS証明書を検証します。

これらのプロトコルは、HTTPを介して失効ステータスを配信するように設計されています。CRLおよびOCSPメッセージは、OCSP検証が失敗した後にライセンス登録が失敗した場合にX.509証明書の失効ステータスを示す公開文書です。

---

 ヒント:OCSPに障害が発生した場合は、中間のセキュリティデバイスがHTTP接続を切断していることを意味します。

---

OCSP検証が適切かどうかを確認するには、例に示すように、ファイルをCMIP SCVM / tmpパーティションにダウンロードしてみてください。

```
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
```

## シナリオ5：証明書の変更

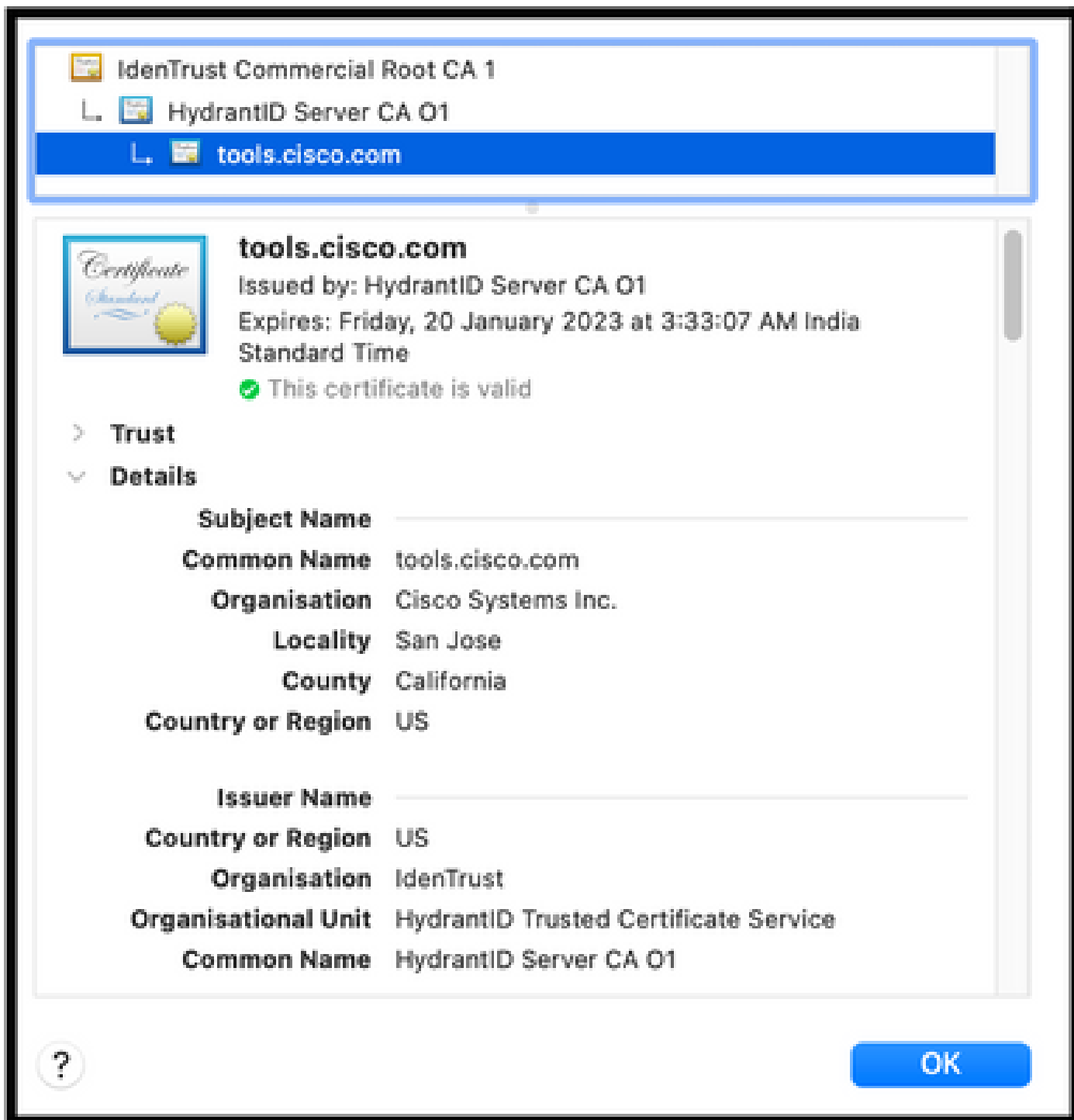
一部のネットワークでは、プロキシとファイアウォールのセキュリティデバイスがSecure Sockets Layer(SSL)インスペクションを実行し、Hyperflexがfrom tools.cisco.com:443の受信を想定している証明書を破損する可能性があります。

証明書がプロキシまたはファイアウォールによって変更されていないことを確認するには、CMIPを保持するSCVMで次のコマンドを実行します。

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

サブジェクト名と発行者名の情報は、この例に示す証明書と一致する必要があることに注意してください。





**⚠ 警告** : サブジェクトまたは発行者のフィールドが少なくとも1つ異なる場合、登録は失敗します。これは、Hyperflexクラスタ管理IPおよびtools.cisco.com:443のセキュリティSSLインスペクションのバイパスルールで修正できます。

この例では、Hyperflex CMIP SCVMの証明書から受信した同じ情報を検証する方法を確認できます。

<#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
```

## 追加手順

この手順は、対象となるシナリオが成功または解決しても、ライセンス登録が失敗する場合に利用できます。

ライセンスの登録を解除します。

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

スマートライセンスから新しいトークンを取得し、ライセンスプロセスを再起動して、ライセンス登録を再試行してください。

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

## 関連情報

- [Cisco HyperFlex HXデータプラットフォーム – エンドユーザガイド](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。