Nutanixハードウェアプロバイダーとの接続に関するCisco HCIの問題のトラブルシューティング

内容

はじめに

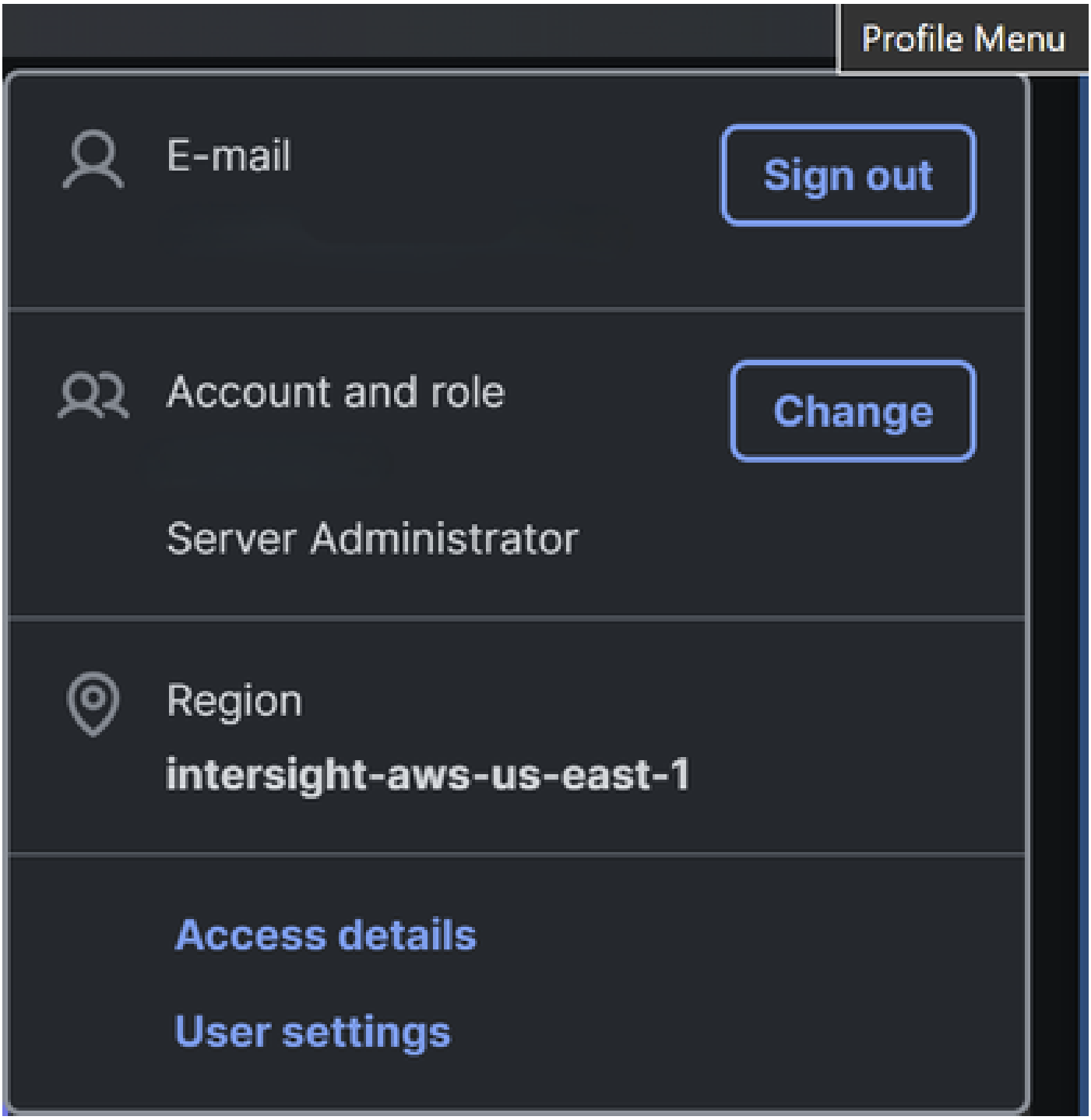
このドキュメントでは、Nutanix Foundation CentralからCisco Intersightへのハードウェアプロバイダー接続の問題をトラブルシューティングする方法について説明します。

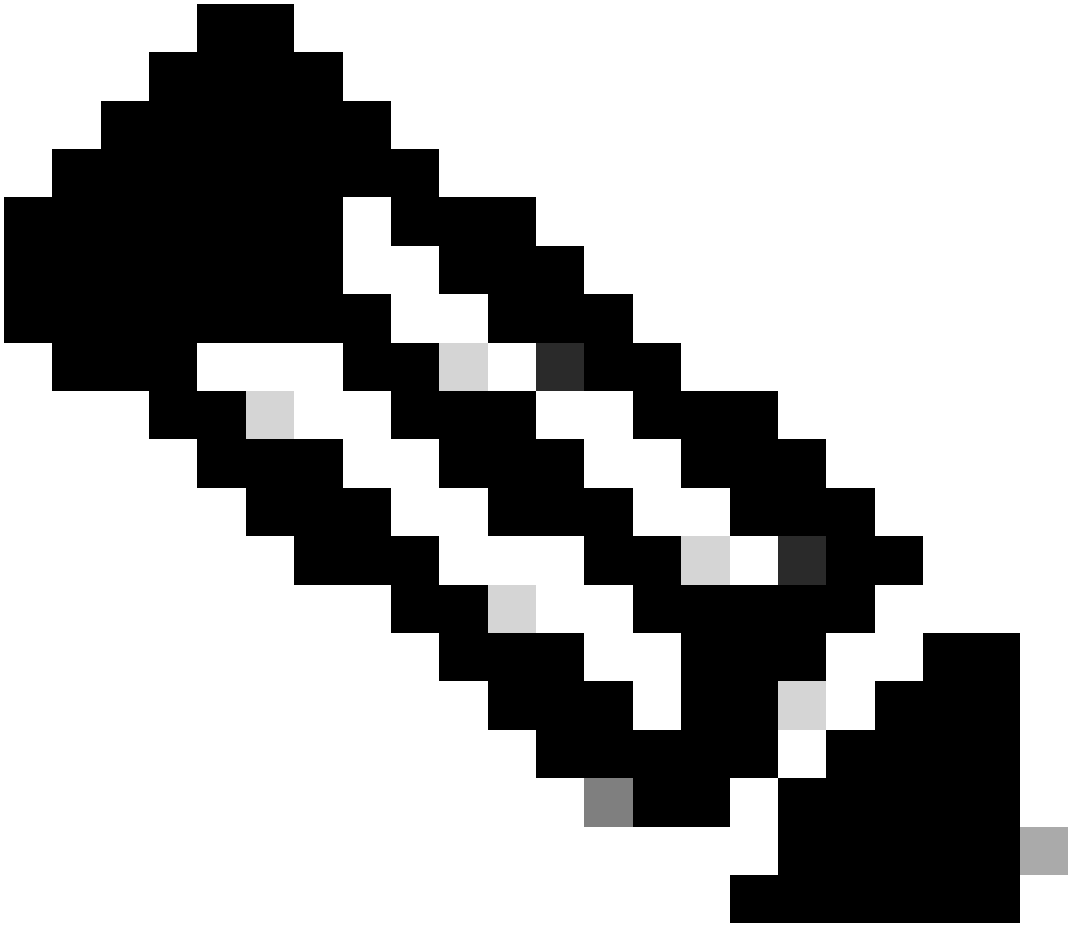
前提条件

要件

次のトピックに関する知識を身に付けておくことをお勧めします。

- ネットワーク接続の基本的な知識。
- Intersight APIキーに関する基本的な知識
- サーバ管理者権限を持つIntersightアカウント。


Profile Menu
E-mail
Sign out
Account and role
Change
Server Administrator
Region
intersight-aws-us-east-1
Access details
User settings



注:Intersightはロールベースアクセスコントロール(RBAC)を提供し、ユーザロールと権限に基づいて、ユーザへのシステムアクセスを許可または制限します。Intersightのユーザロールは、ユーザが一連の操作を実行するために必要な権限の集合を表し、リソースへのきめ細かなアクセスを提供します。Intersightは、個々のユーザまたはグループの下のユーザのセットに、ロールベースのアクセスを提供します。

使用するコンポーネント

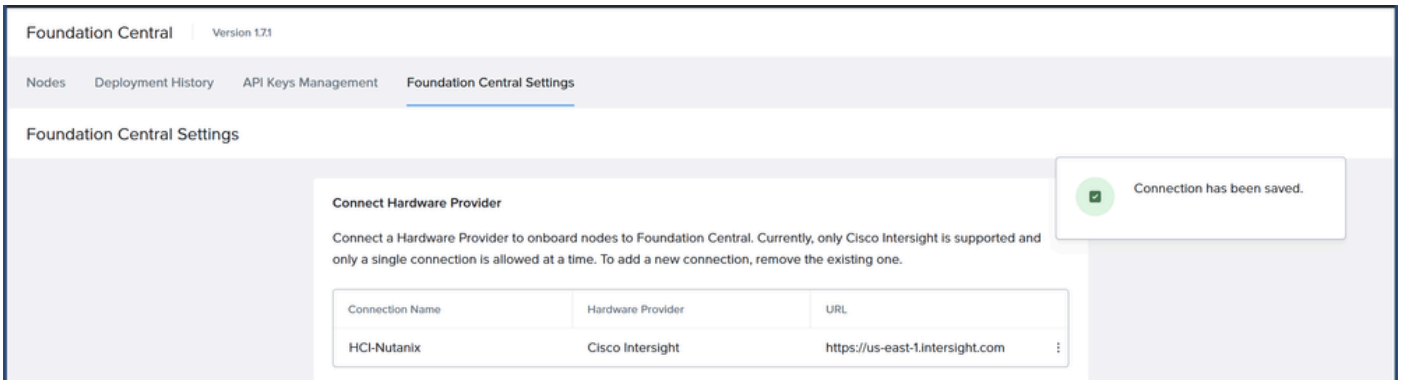
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Foundation Central 1.7.1以上
- Intersight SAAS、CVA、およびPVA。

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

IntersightスタンドアロンモードISMまたはIntersightマネージドモードIMMでCisco HCI with Nutanixソリューションを導入するには、ハードウェアプロバイダーとしてFoundation CentralをCisco Intersightに接続する必要があります。



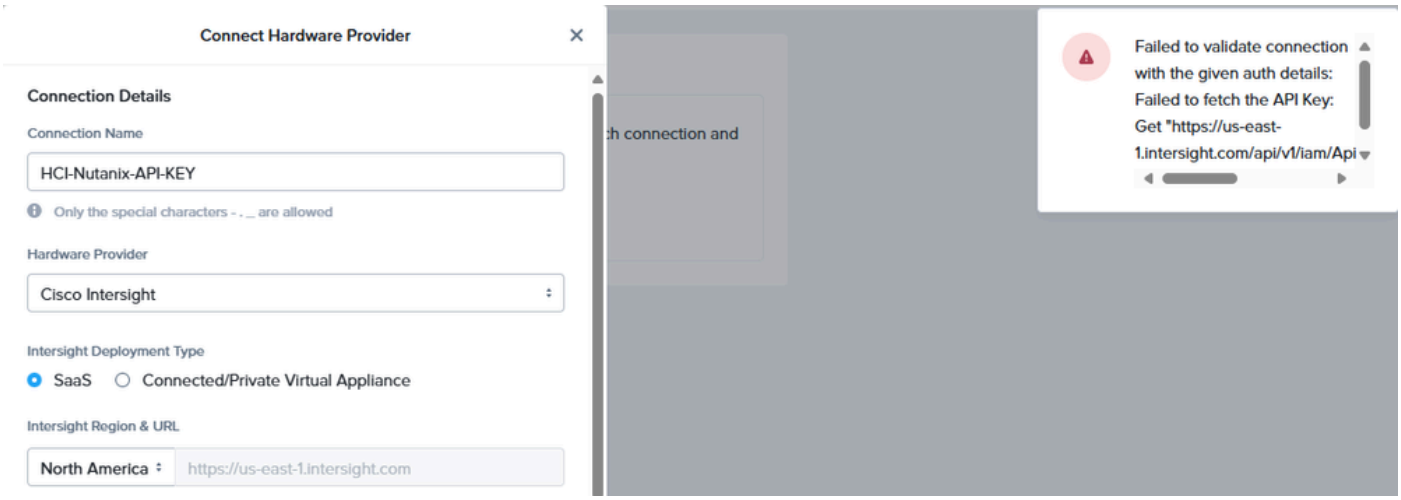
Intersightスタンドアロンモード：ノードはトップオブラック(ToR)スイッチのペアに接続され、サーバはCisco Intersight®を使用して一元管理されます。標準のNutanixクラスタを導入するには最低3つのノードが必要ですが、エッジやブランチのロケーションや、すでに高性能なネットワークファブリックがインストールされている状況では、単一ノードクラスタと2ノードクラスタを導入するオプションもあります。

Intersightマネージドモード：Intersightマネージドモードは、UCSシステムの機能とIntersightのクラウドベースの柔軟性を統合し、スタンドアロンおよびファブリックインターコネクトに接続されたシステムの管理エクスペリエンスを統合します。Intersight管理モデルは、UCS-FI-6454、UCS-FI-64108、UCS-FI-6536、UCSX-S9108-100Gファブリックインターコネクト、Cisco UCS Cシリーズ(M5、M6、M7、M8)、およびCisco UCS Xシリーズ(M6、M7、M8)サーバのポリシーおよび運用管理を標準化します。

トラブルシュート

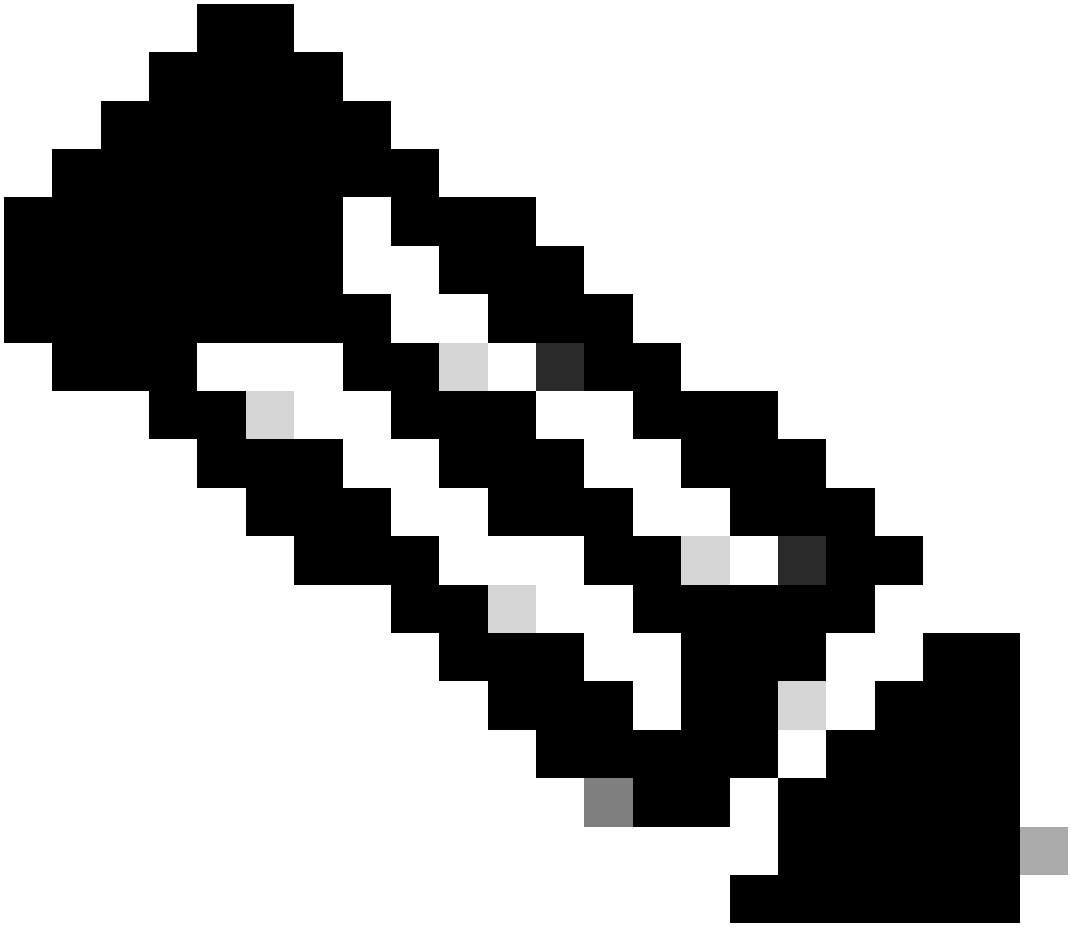
コンテキストの期限を超過

"指定された認証の詳細で接続を検証できませんでした： APIキーを取得できませんでした：コンテキストの期限を超過しました。"



Prism CentralとFoundation centralから、ポート443 TCP/UDPおよび80 TCPを介した次のURLへの接続が適切であることを確認します。

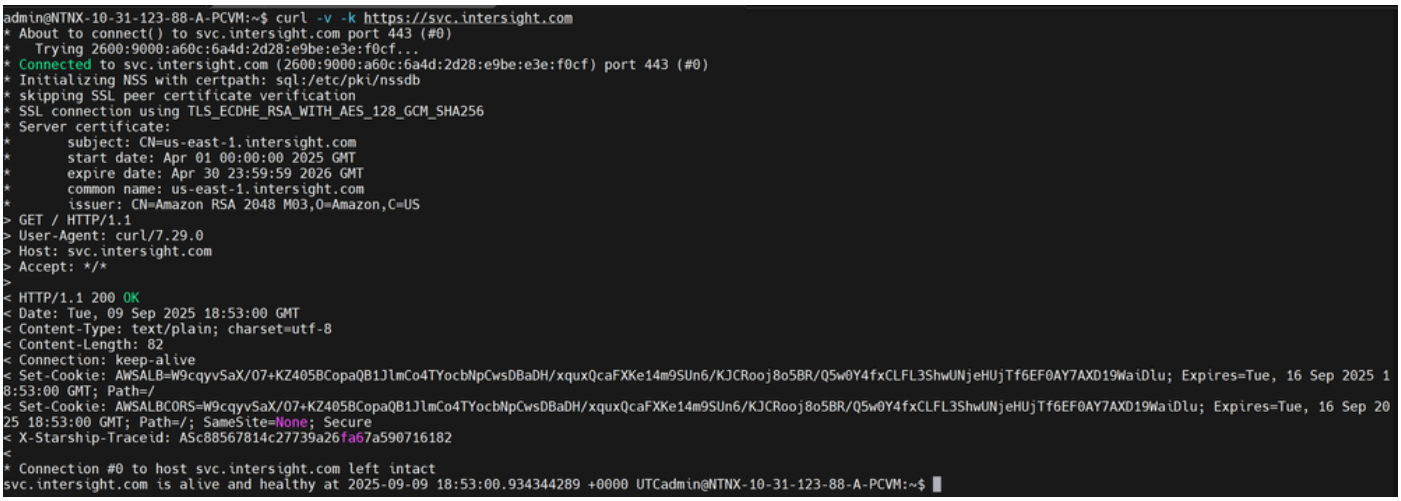
地域	URL	デバイスコネクタに必要なURL
北米	intersight.com us-east-1.intersight.com IPS: 52.223.48.112 99.83.178.202	svc.intersight.com svc.us-east-1.intersight.com svc-static1.intersight.com ucs-starship.com* ucs-connect.com*
EMEA	Intersight.com eu-central-1.intersight.com IPS: 52.223.57.109 99.83.140.236	svc.eu-central-1.intersight.com svc-static1.eu-central-1.intersight.com



注:Cisco Intersightは、既存の北米地域(us-east-1)と欧州、中東、アフリカ(EMEA)地域(eu-central-1)の2つの地域をサポートしています。

上記の情報を検証するには、Prism CentralまたはFoundation Central VMにSSHで接続し、前述のURLとポートに対してcurlコマンドを実行します。

```
curl -v -k https://svc.intersight.com
```



Curl接続テストに成功。

curlコマンドが失敗した場合は、ファイアウォールまたはアクセスリストにURLとポートが許可されていることをファイアウォールチームに確認してください。

```
admin@NTNX-10-31-123-88-A-PCVM:~$ curl -v -k https://svc.intersight.com
* About to connect() to svc.intersight.com port 443 (#0)
*   Trying 2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf...
* No route to host
*   Trying 2600:9000:a706:c634:41:731c:ad1e:bf00...
* No route to host
*   Trying 99.83.178.202...
* Connection timed out
*   Trying 52.223.48.112...
* After 86287ms connect time, move on!
* Failed connect to svc.intersight.com:443; Operation now in progress
* Closing connection 0
curl: (7) Failed connect to svc.intersight.com:443; Operation now in progress
admin@NTNX-10-31-123-88-A-PCVM:~$
```

curl接続テストに失敗しました。

DNSの適切な名前解決

一部のファイアウォールまたはアクセスリストでは、前述のURLから解決IPを追加する必要があります。これらのURLは両方とも、次のIPv4アドレスとIPv6アドレスに解決されます。

- 52.223.48.112
- 99.83.178.202
- 2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf
- 2600:9000:a706:c634:41:731c:ad1e:bf00

これは、nslookupコマンドを使用して検証できます。

```
nslookup svc.intersight.com
```

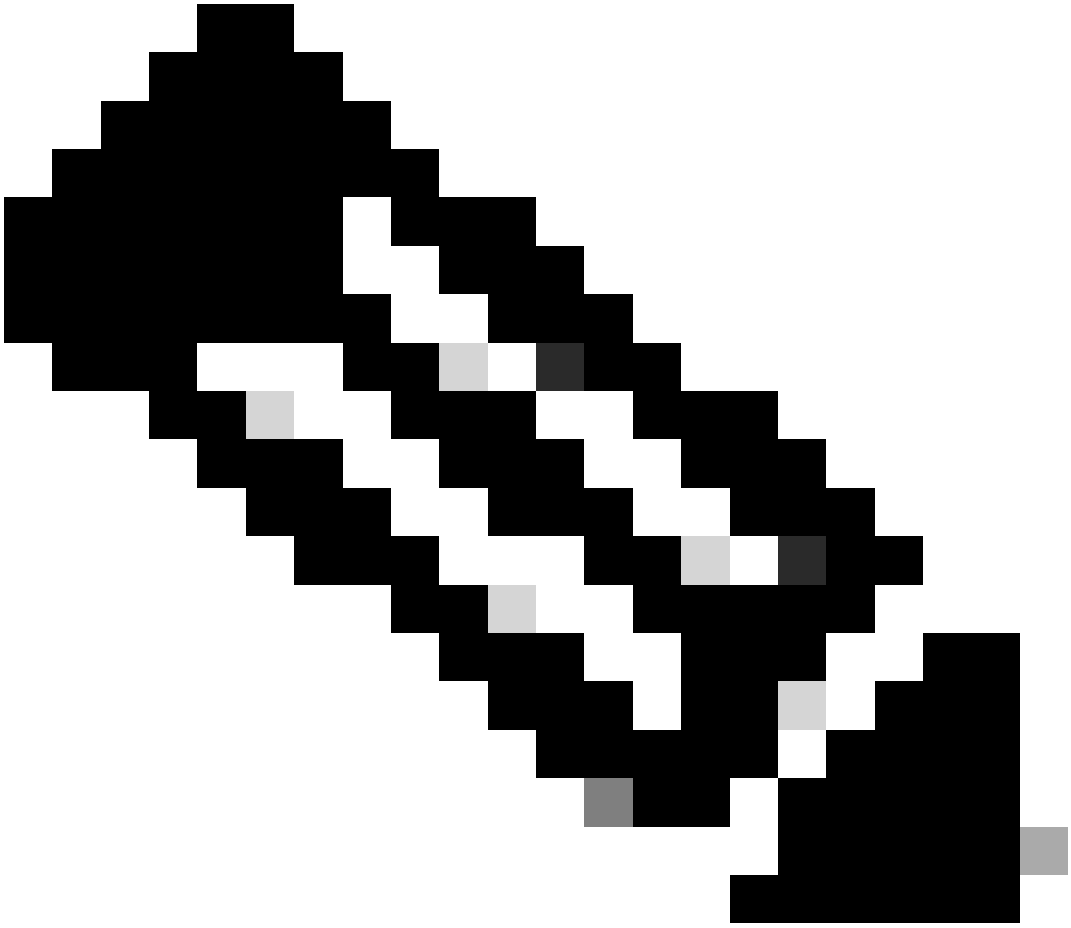
```
admin@NTNX-10-31-123-88-A-PCVM:~$ nslookup svc.intersight.com
Server:         10.31.123.60
Address:        10.31.123.60#53

Non-authoritative answer:
Name:   svc.intersight.com
Address: 52.223.48.112
Name:   svc.intersight.com
Address: 99.83.178.202
Name:   svc.intersight.com
Address: 2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf
Name:   svc.intersight.com
Address: 2600:9000:a706:c634:41:731c:ad1e:bf00

admin@NTNX-10-31-123-88-A-PCVM:~$
```

nslookup コマンド

Prism Central VMがIntersight CVA/PVAに接続できない

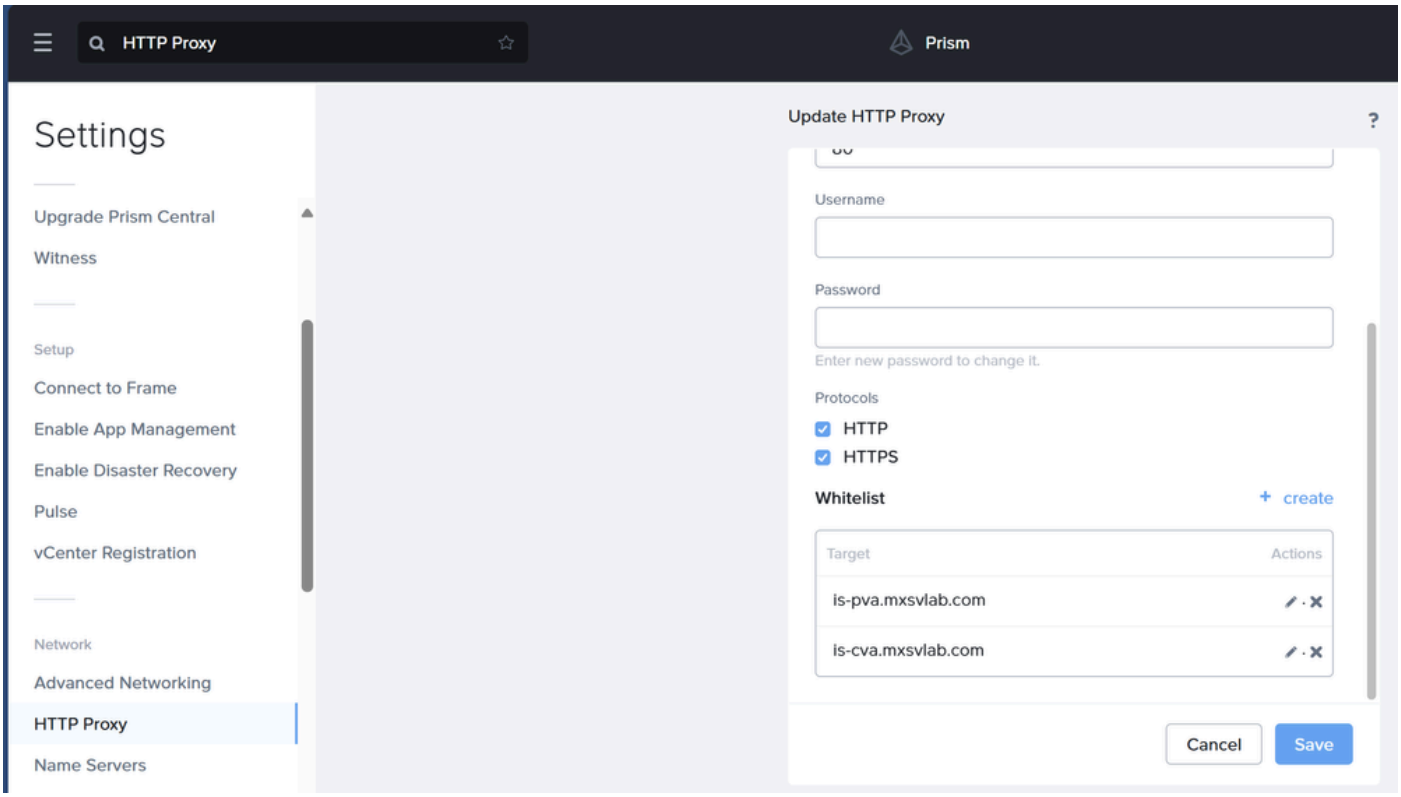
Prism CentralからIntersight CVA/PVAへの直接接続がある場合は、ポート443での接続が可能であることを確認します。

PC VMがソフトウェアダウンロードやLCMなどのタスクのためにインターネットに接続するように設定されている場合、Prism Central Proxy設定でIntersight CVA / PVA FQDNとIPアドレスをホワイトリストに登録する必要があります。



注：ホワイトリストエントリは、IPアドレスで識別される単一のホスト、またはネットワークアドレスとサブネットマスクで識別されるネットワークです。ホワイトリストエントリを追加すると、「このアドレスまたはネットワークのプロキシ設定を無視する」ことを意味します。

Prism Centralでこれを修正するには、設定>ネットワーク> HTTPプロキシ>鉛筆アイコンをクリックして編集>ホワイトリストに移動します。



HTTPプロキシ

curlコマンドを使用してIntersight CVA/PVAへの接続をテストすることで、これらの手順が成功したかどうかを確認できます。

```
curl -v -k https://is-pva.mxsvlab.com
```

```
                                                curl -v -k https://is-pva.mxsvlab.com
*   Trying            :443...
* Connected to is-pva.mxsvlab.com (            ) port 443
* ALPN: curl offers http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN: server accepted http/1.1
```

カールテスト

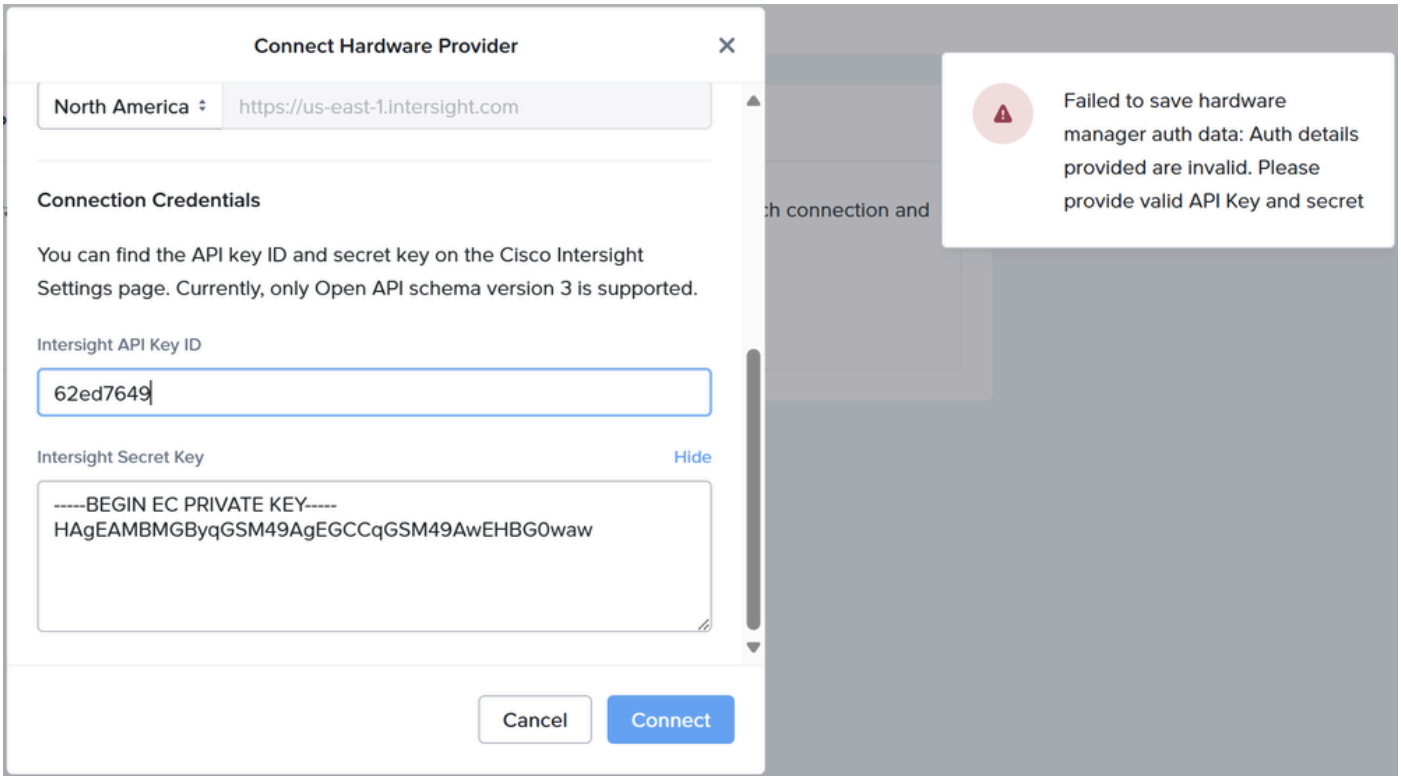
接続をテストするNetworkコマンド

コマンド	説明

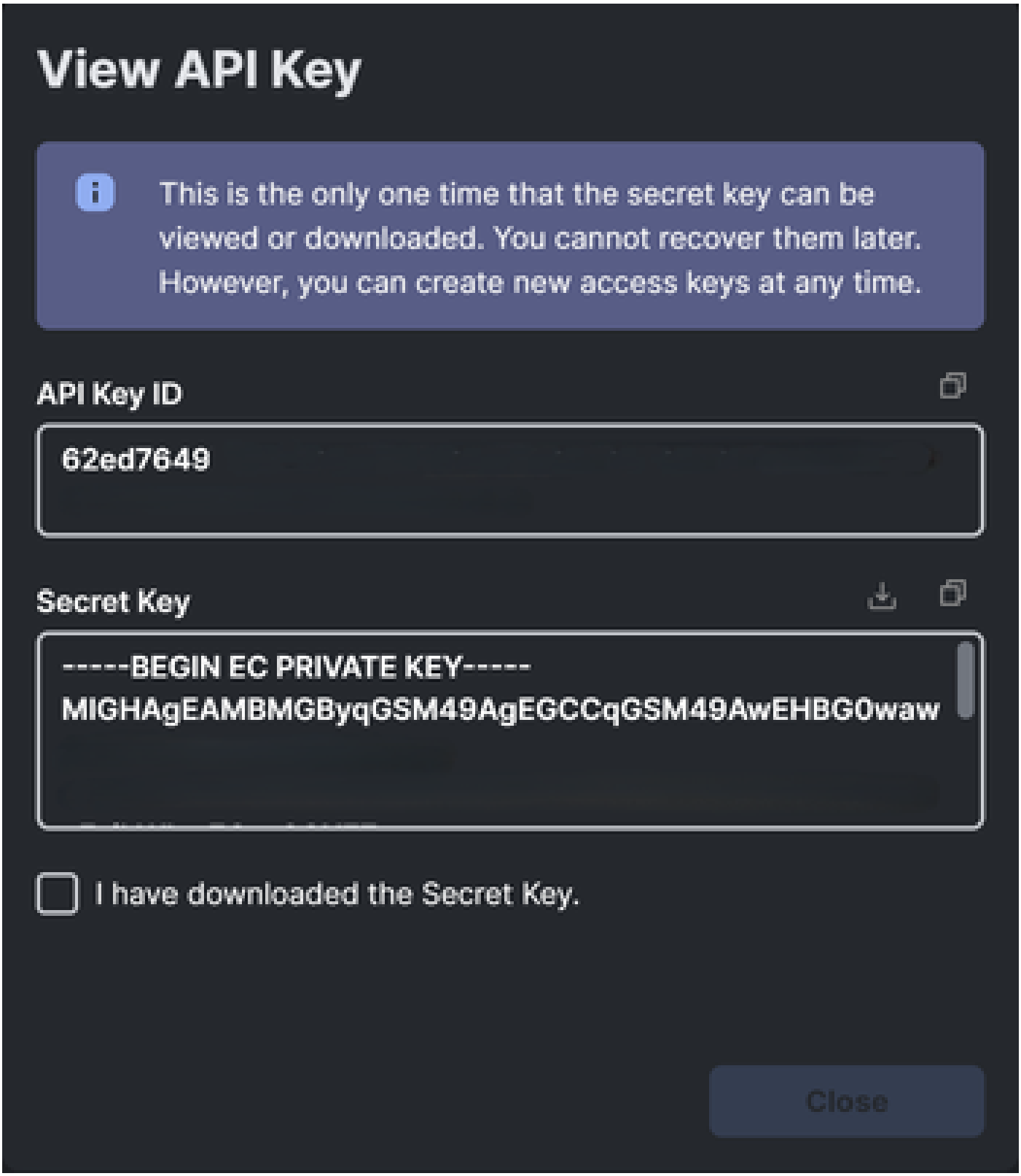
curl -v -k https://<Intersight URL> curl -v -k https://svc.intersight.com	Intersight required URLへの接続をテストする
curl -v -k —proxy <proxy address>:<port> <Intersight URL> curl -v -k —proxy http://proxy.esl.cisco.com:8080 https://svc.intersight.com	プロキシが必要なときに接続をテストする
curl -4|6 -v -k https://<Intersight URL> curl -4 -v -k https://svc.intersight.com	IPV4またはIPV6アドレスへの接続テストを指定します
tracepath <Intersight IP>（日本での対応時期未定） tracepath 99.83.178.202	宛先ホストに向かうパケットをトレースする
nslookup <URL> nslookup svc.Intersight.com	特定のアドレスに関連付けられたIPアドレスを決定する

指定された認証の詳細が無効です

“ハードウェアマネージャの認証データを保存できませんでした：指定された認証の詳細が無効です。有効なAPIキーとシークレットを指定してください。

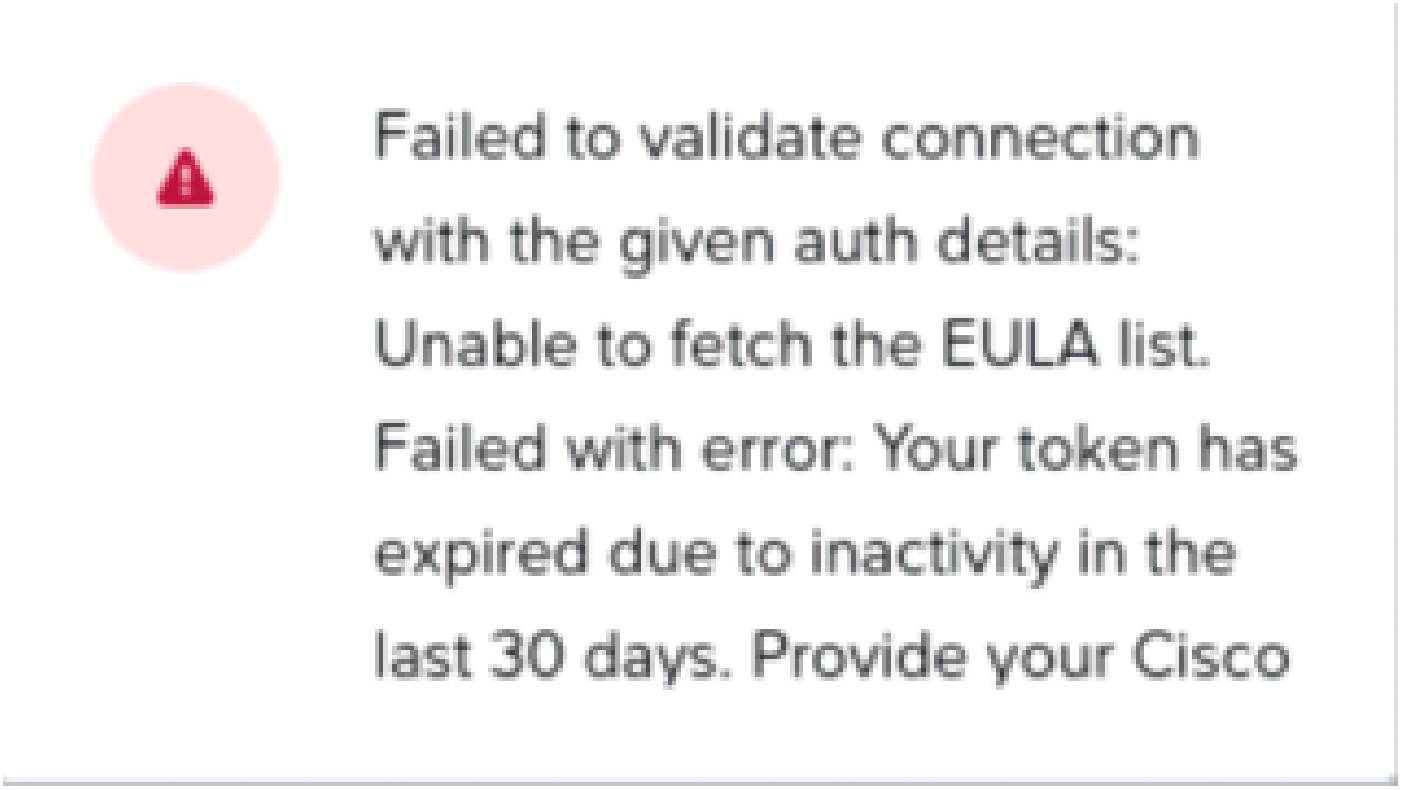


Intersight Secret Keyの入力または貼り付けの際に、入力エラーや文字の欠落がないことを確認する必要があります。そうしないと、ハードウェアプロバイダーへの接続を確立できません。

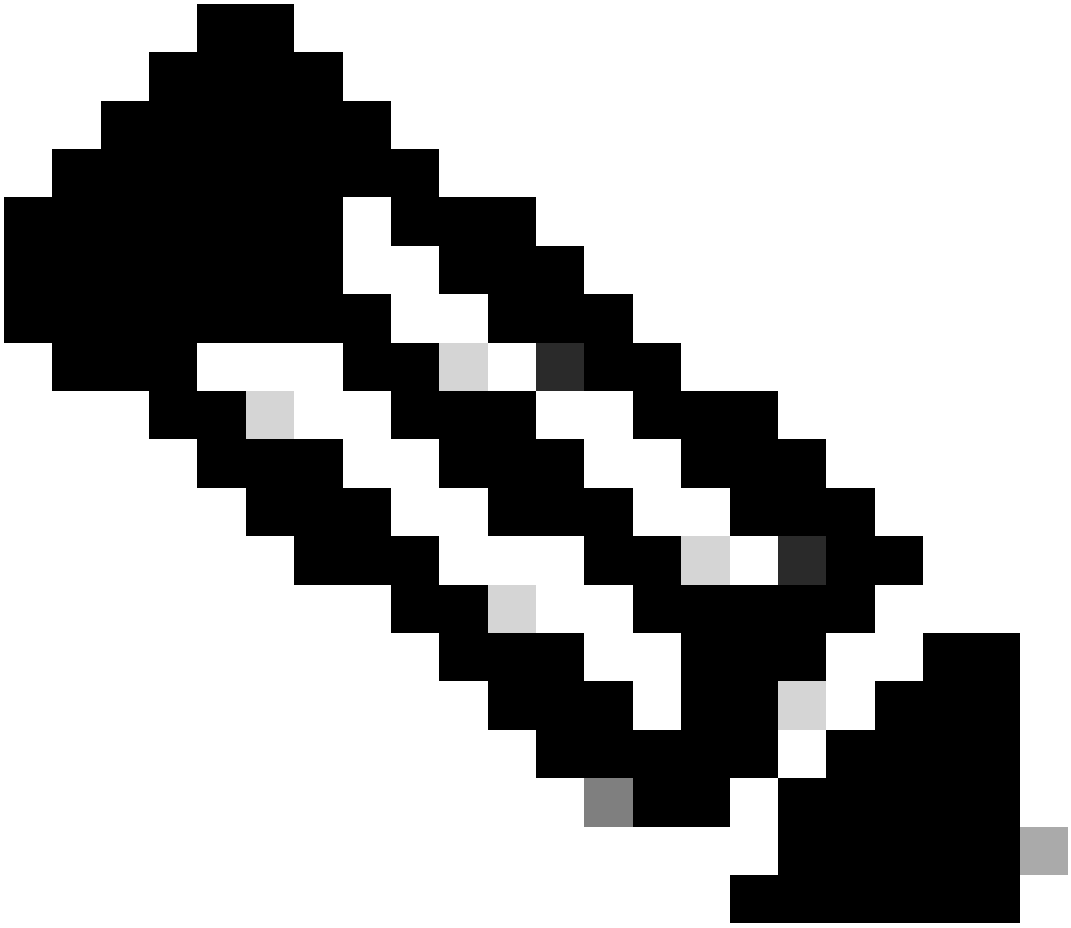


EULAリストを取得できません

“指定された認証の詳細で接続を検証できませんでした： EULAリストを取得できません。エラーで失敗しました：過去30日間の非アクティブによってトークンの有効期限が切れました。

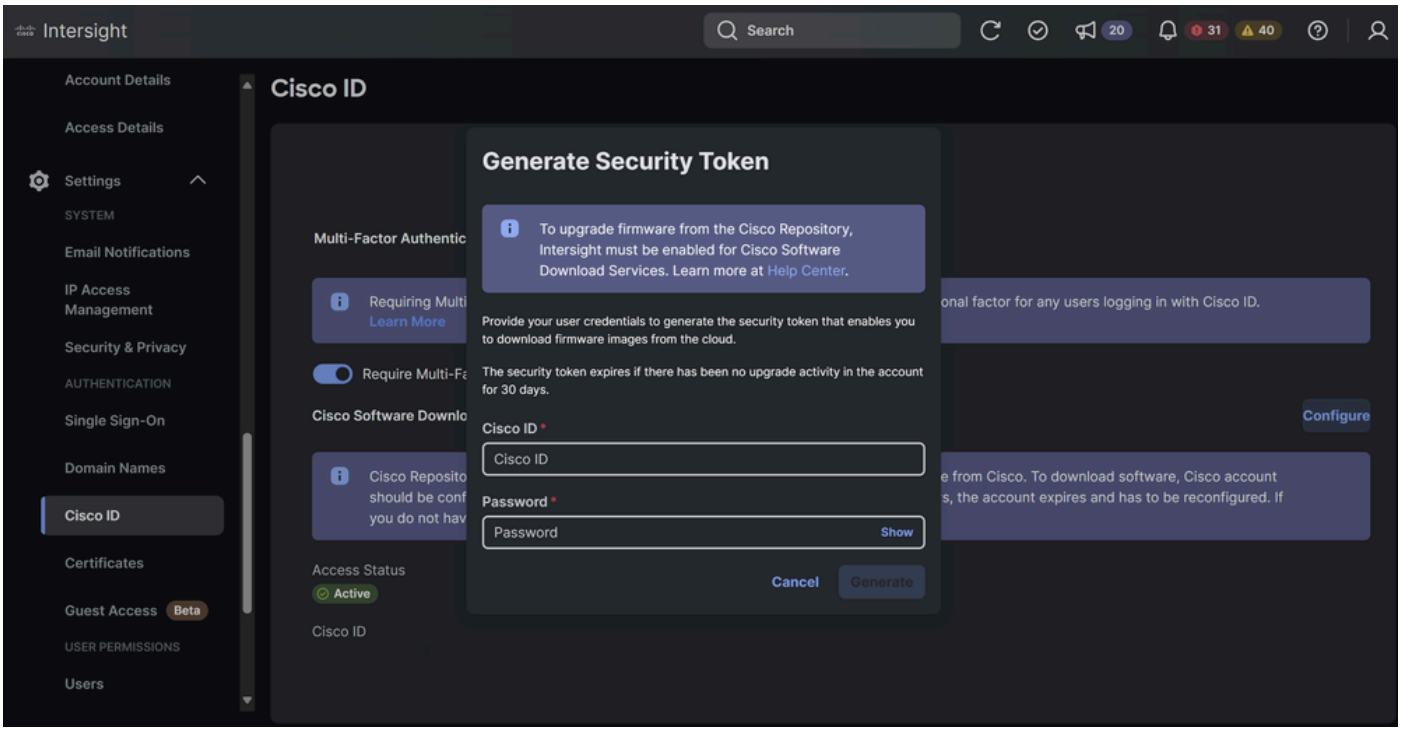


ノードのオンボーディングフェーズで、「Failed to connect to INTERSIGHT hardware manager with UUID」または「Your user credentials could have expired.」というエラーが発生する場合があります。 これは、EULAに関してIntersightアカウントの問題がある場合に表示されます。



注：今日の時点で、ISMにはEULAへの同意が必要です。ファームウェアのダウンロードにEULAを使用しなくなったため、これは将来的に変更されます。

Intersightでこれを修正するには、Settings > Cisco ID > Configure > Enter Cisco ID and Passwordの順に選択します。



関連情報

- Intersightにおける組織と役割
- ポート要件
- ターゲットの要求に必要なエンドポイントURL
- シスコソフトウェアリポジトリアクセスの許可とEULAの受け入れ

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。