Cisco HCI와 Nutanix 하드웨어 공급자 연결 문제 해결

목차

소개

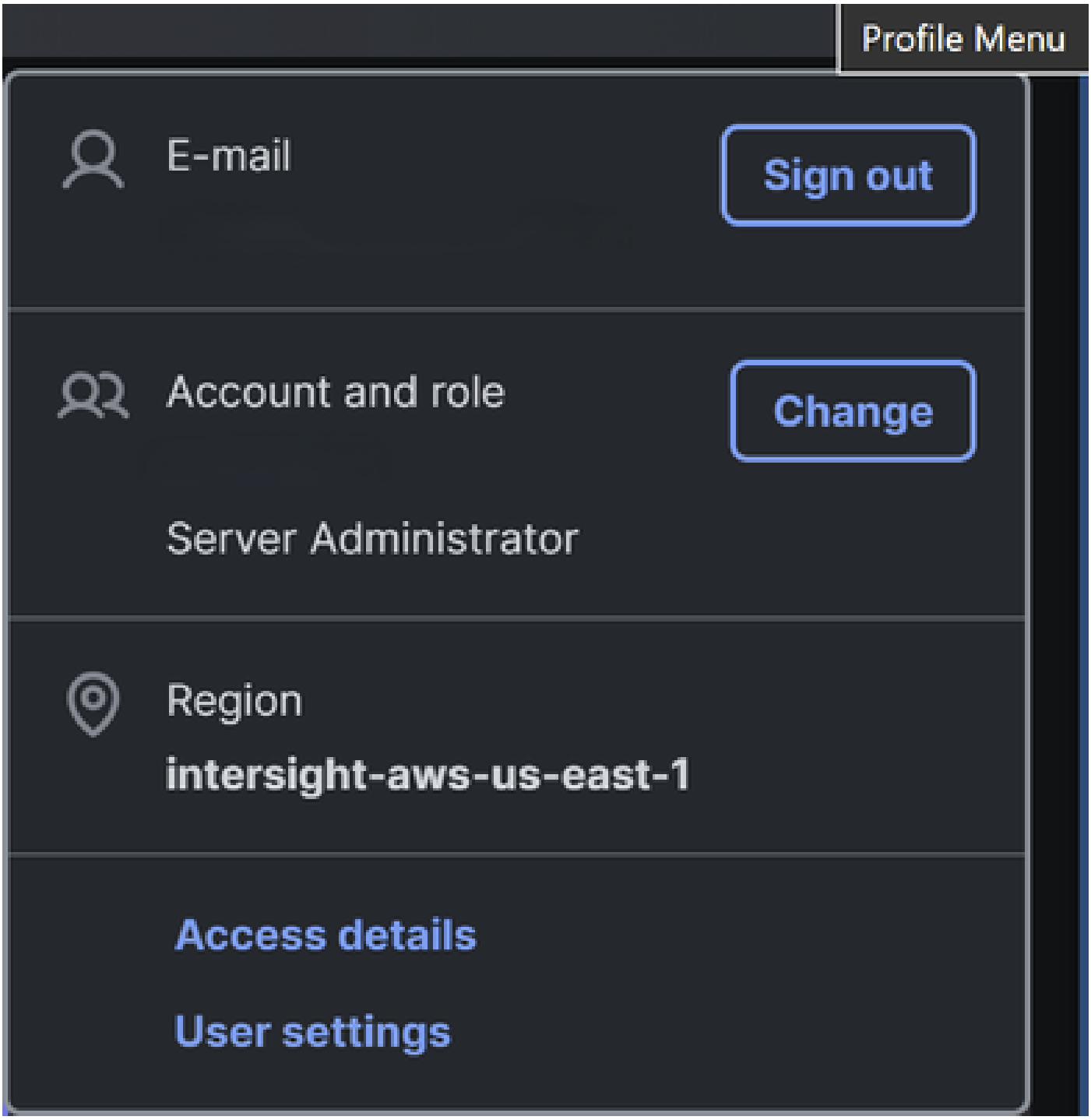
이 문서에서는 Nutanix Foundation Central에서 Cisco Intersight로의 하드웨어 공급자 연결 문제를 해결하는 방법에 대해 설명합니다.

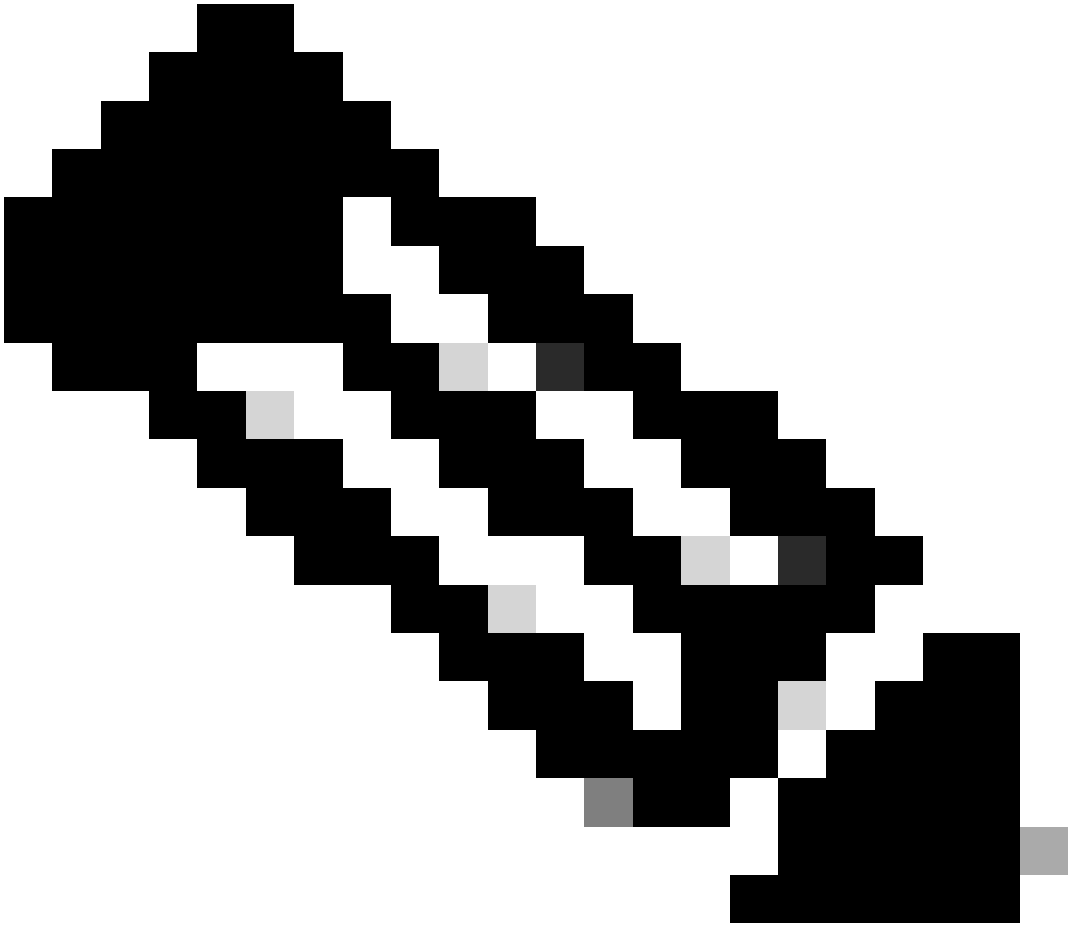
사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대해 알고 있는 것이 좋습니다.

- 네트워크 연결에 대한 기본적인 이해
- Intersight API 키에 대한 기본 이해
- 적어도 서버 관리자 권한이 있는 Intersight 계정입니다.


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



참고: Intersight는 사용자 역할 및 권한에 따라 사용자에 대한 시스템 액세스를 인증하거나 제한하는 RBAC(Role-Based Access Control)를 제공합니다. Intersight의 사용자 역할은 일련의 작업을 수행하기 위해 사용자가 갖는 권한의 모음을 나타내며 리소스에 대한 세분화된 액세스를 제공합니다. Intersight는 개별 사용자 또는 그룹 아래의 사용자 집합에 역할 기반 액세스를 제공합니다.

사용되는 구성 요소

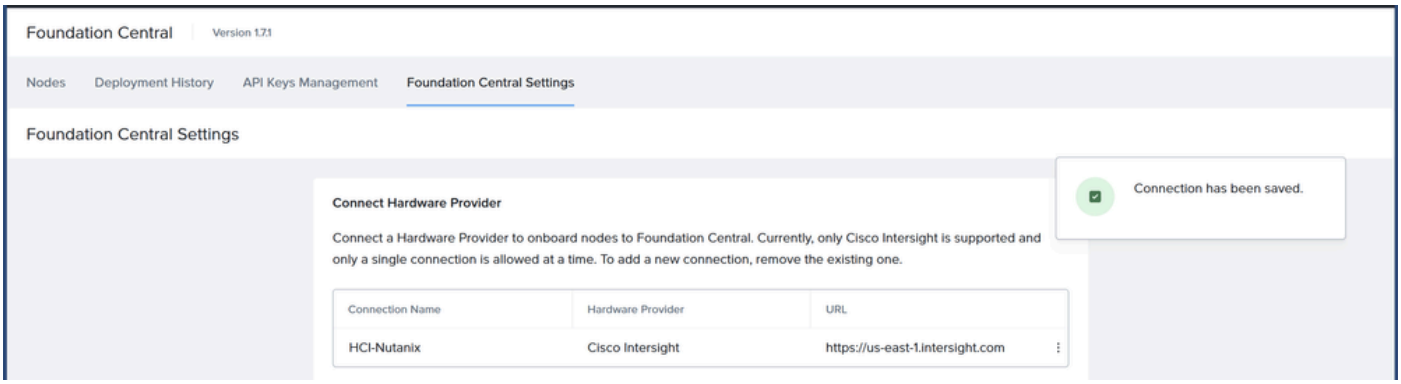
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Foundation Central 1.7.1 이상
- Intersight SAAS, CVA 및 PVA

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

Intersight Standalone Mode ISM 또는 Intersight Managed Mode IMM에서 Cisco HCI with Nutanix 솔루션을 구축하려면 하드웨어 공급자로서 Foundation Central을 Cisco Intersight에 연결해야 합니다.



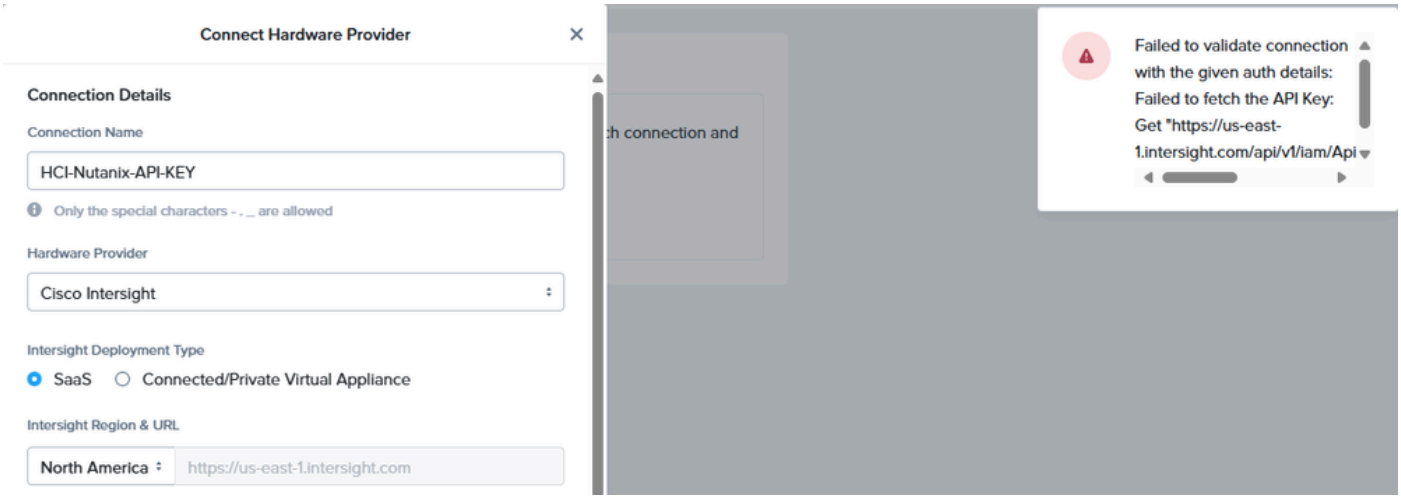
Intersight 독립형 모드: 노드가 ToR(Top-of-Rack) 스위치 쌍에 연결되고 서버는 Cisco Intersight®를 사용하여 중앙에서 관리됩니다. 표준 Nutanix 클러스터를 구축하려면 최소 3개의 노드가 필요하지만, 고성능 네트워크 패브릭이 이미 설치되어 있는 에지 및 지사 위치 및 상황을 위해 단일 노드 클러스터 및 2노드 클러스터를 구축하는 옵션도 제공합니다.

Intersight Managed Mode: Intersight Managed Mode는 UCS 시스템의 기능과 Intersight의 클라우드 기반 유연성을 통합하여 독립형 및 Fabric Interconnect 연결 시스템의 관리 환경을 통합합니다. Intersight Management 모델은 UCS-FI-6454, UCS-FI-64108, UCS-FI-6536, UCSX-S9108-100G Fabric Interconnect 및 Cisco UCS C-Series(M5, M6, M7, M8), Cisco UCS X-Series(M6, M7, M8) 서버에 대한 정책 및 운영 관리를 표준화합니다.

문제 해결

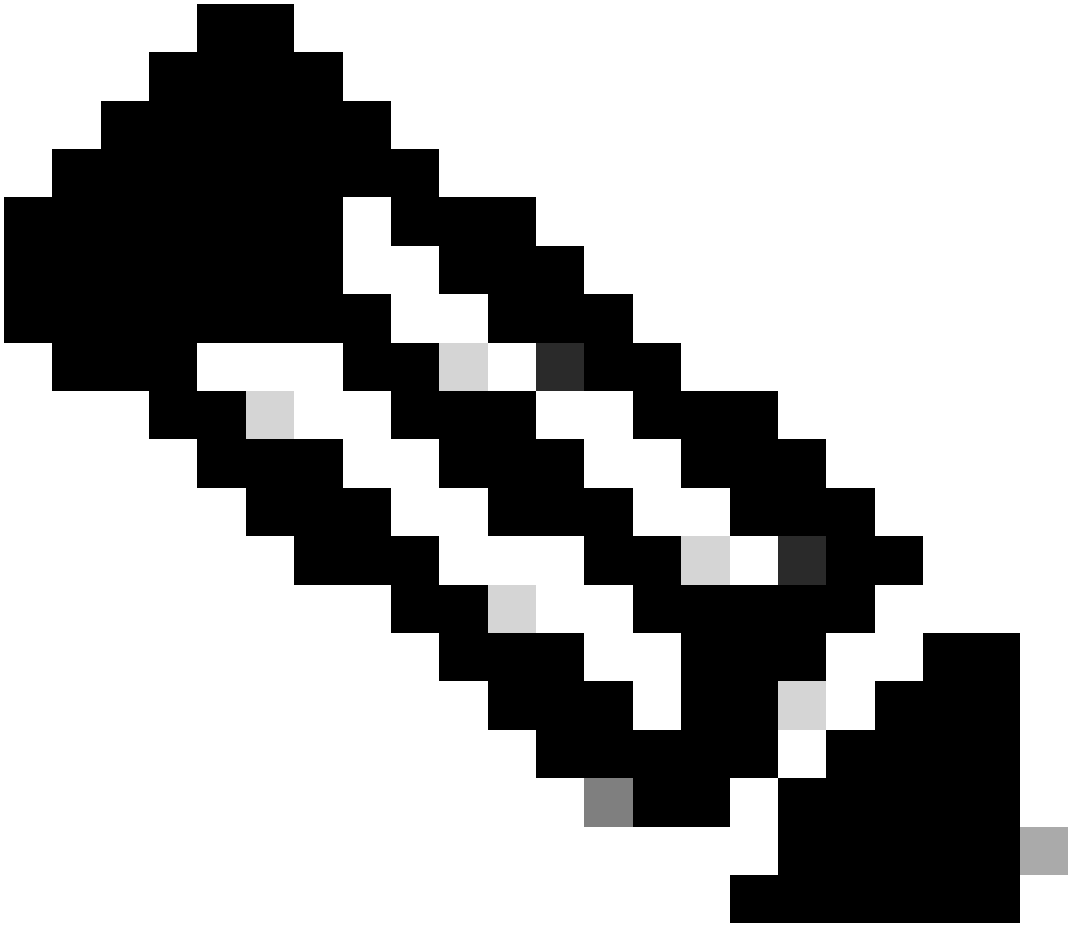
컨텍스트 마감일 초과

"지정된 인증 세부 정보와의 연결을 검증하지 못했습니다. API 키를 가져오지 못했습니다. 컨텍스트 마감일이 초과되었습니다."



Prism Central 및 Foundation Central에서 포트 443 TCP/UDP 및 80 TCP를 통해 다음 URL로 올바르게 연결할 수 있는지 확인합니다.

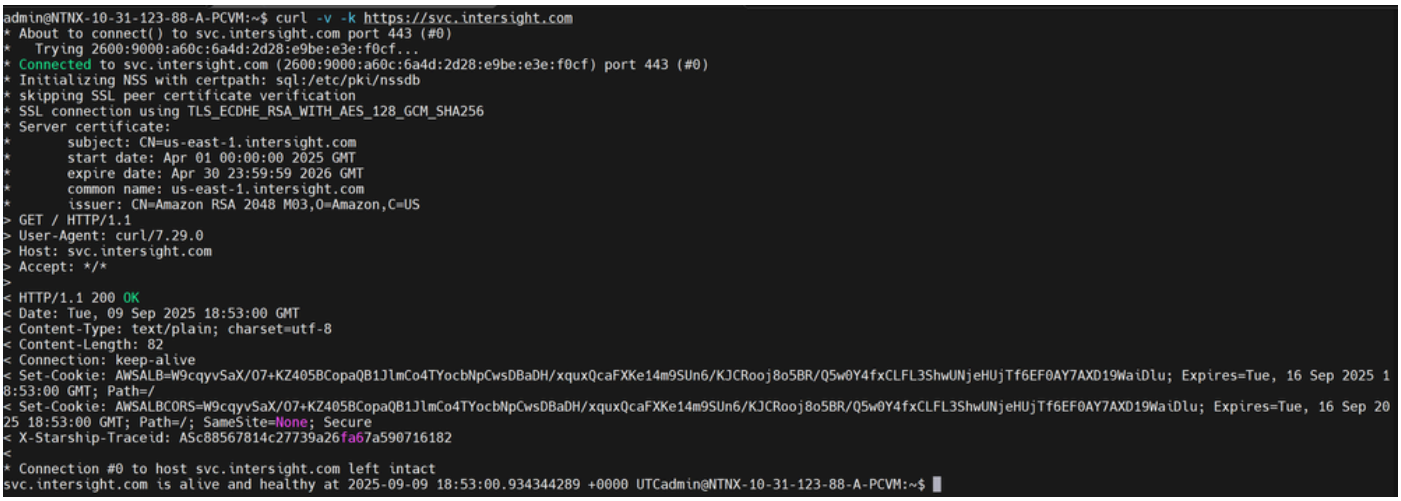
지역	URL	디바이스 커넥터에 필요한 URL
북미	intersight.com us-east-1.intersight.com Ips: 52.223.48.112 99.83.178.202	svc.intersight.com svc.us-east-1.intersight.com svc-static1.intersight.com ucs-starship.com* ucs-connect.com*
EMEA	Intersight.com eu-central-1.intersight.com Ips: 52.223.57.109 99.83.140.236	svc.eu-central-1.intersight.com svc-static1.eu-central-1.intersight.com



참고: Cisco Intersight는 두 개의 리전을 지원합니다. 기존 북미 지역(us-east-1) 및 유럽, 중동 및 아프리카(EMEA) 지역(eu-central-1)

이전 정보를 검증하려면 Prism Central 또는 Foundation Central VM에 SSH를 적용하고 언급된 URL 및 포트에 curl 명령을 수행하십시오.

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



Curl 연결 테스트에 성공했습니다.

curl 명령이 실패할 경우 방화벽 팀에 URL 및 포트가 방화벽 또는 액세스 목록에 허용되는지 확인하십시오.

```
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 연결 테스트에 실패했습니다.

DNS 적절한 이름 확인

일부 방화벽 또는 액세스 목록을 사용하려면 언급된 URL에서 확인 IP를 추가해야 합니다. 두 URL 모두 이러한 IPv4 및 IPv6 주소로 확인됩니다.

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

nslookup 명령을 사용하여 이를 확인할 수 있습니다.

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

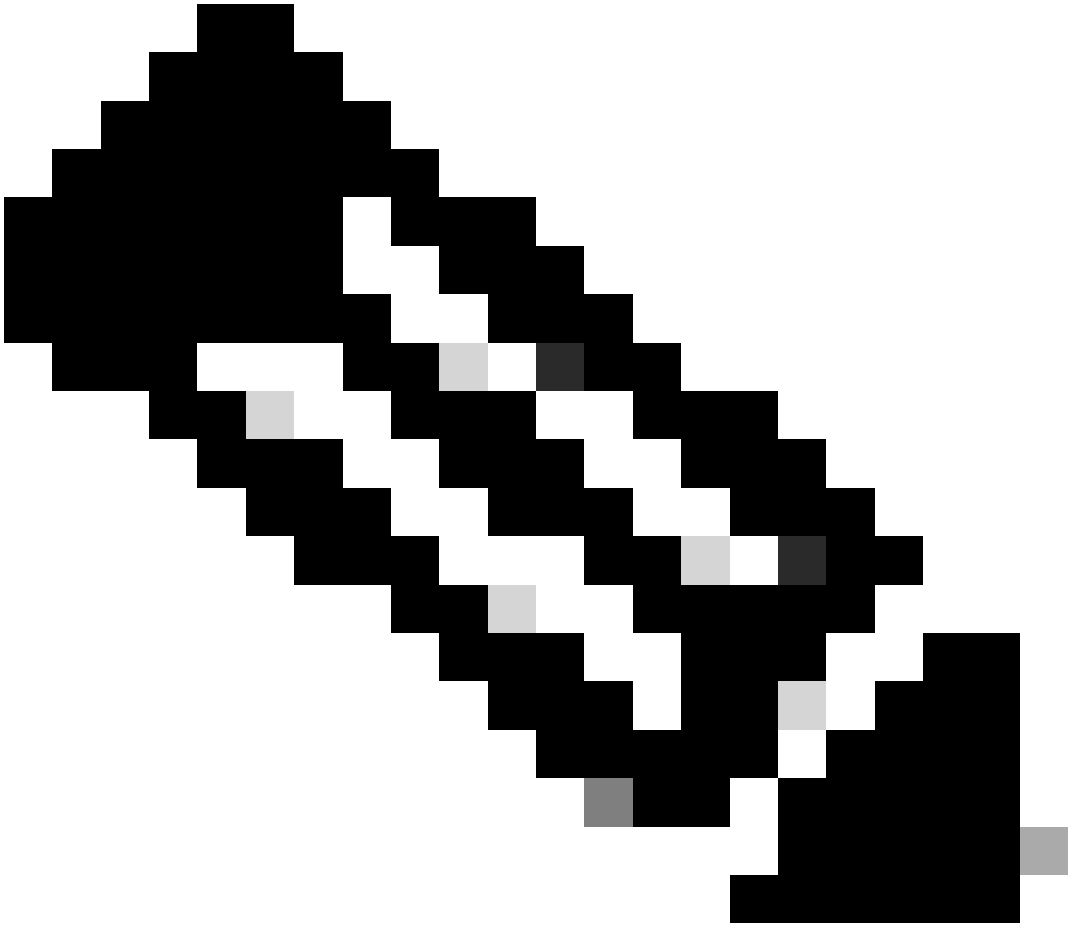
```
admin@NTNX-10-31-123-88-A-PCVM:~$ nslookup svc.intersight.com
Server:         10.31.123.60
Address:        10.31.123.60#53

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 명령

Prism Central VM이 Intersight CVA/PVA에 연결할 수 없음

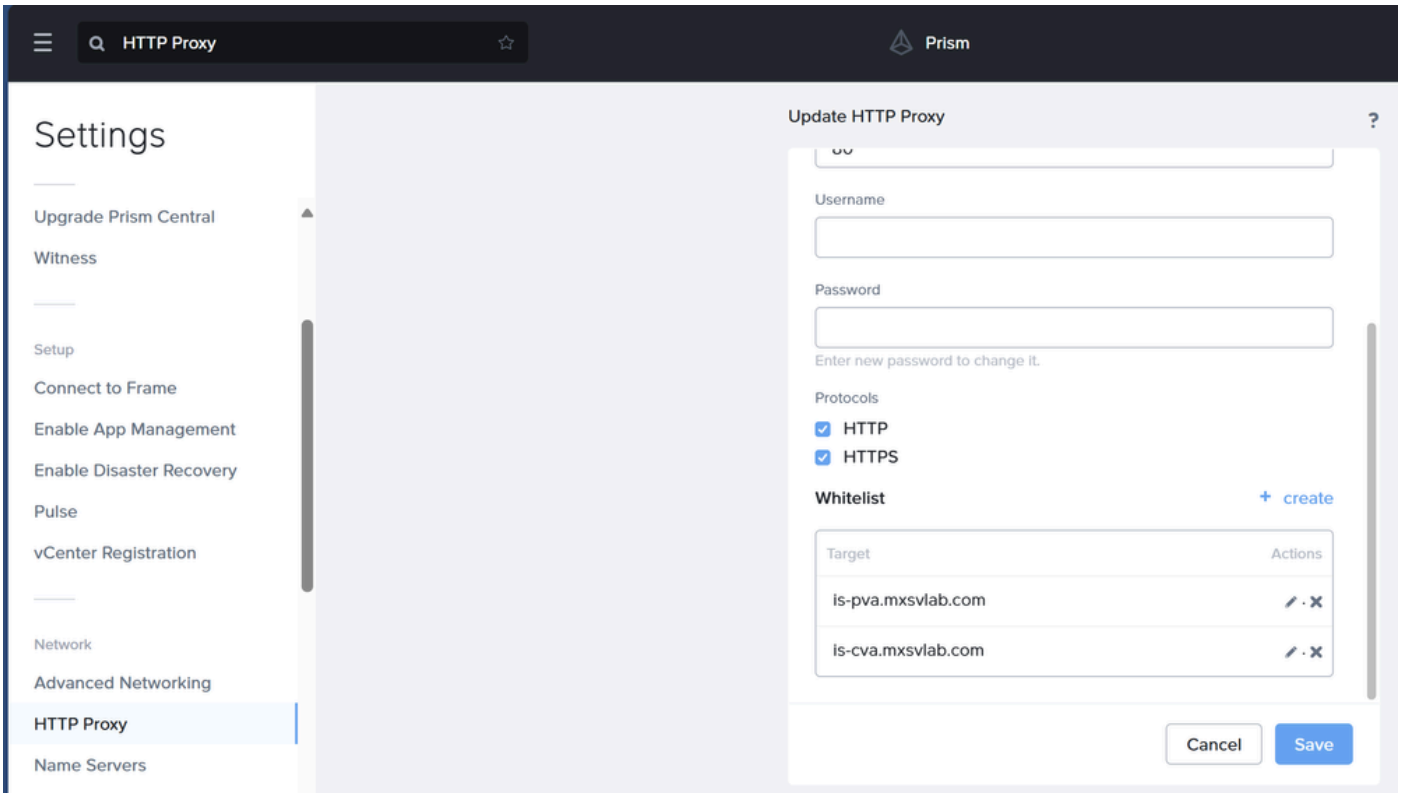
Prism Central에서 Intersight CVA / PVA로 직접 연결하는 경우 포트 443에서 연결할 수 있도록 합니다.

PC VM에 소프트웨어 다운로드나 LCM과 같은 작업을 위해 인터넷에 연결하도록 구성된 프록시가 있는 경우 Prism Central 프록시 설정에서 Intersight CVA/PVA FQDN 및 IP 주소를 화이트리스트에 추가해야 합니다.



참고: 화이트리스트 항목은 IP 주소로 식별되는 단일 호스트 또는 네트워크 주소 및 서브넷 마스크로 식별되는 네트워크입니다. 화이트리스트 항목을 추가하는 것은 "이 주소 또는 네트워크에 대한 프록시 설정을 무시합니다"를 의미합니다.

Prism Central에서 이 문제를 해결하려면 Settings(설정) > Network(네트워크) > HTTP Proxy(HTTP 프록시) > Click on pencil icon to edit(편집할 연필 아이콘 클릭) >Whitelist(화이트리스트)로 이동합니다.



HTTP 프록시

curl 명령으로 Intersight CVA / PVA에 대한 연결을 테스트하여 이러한 단계가 성공적이었는지 확인할 수 있습니다.

```
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
```

컬 테스트

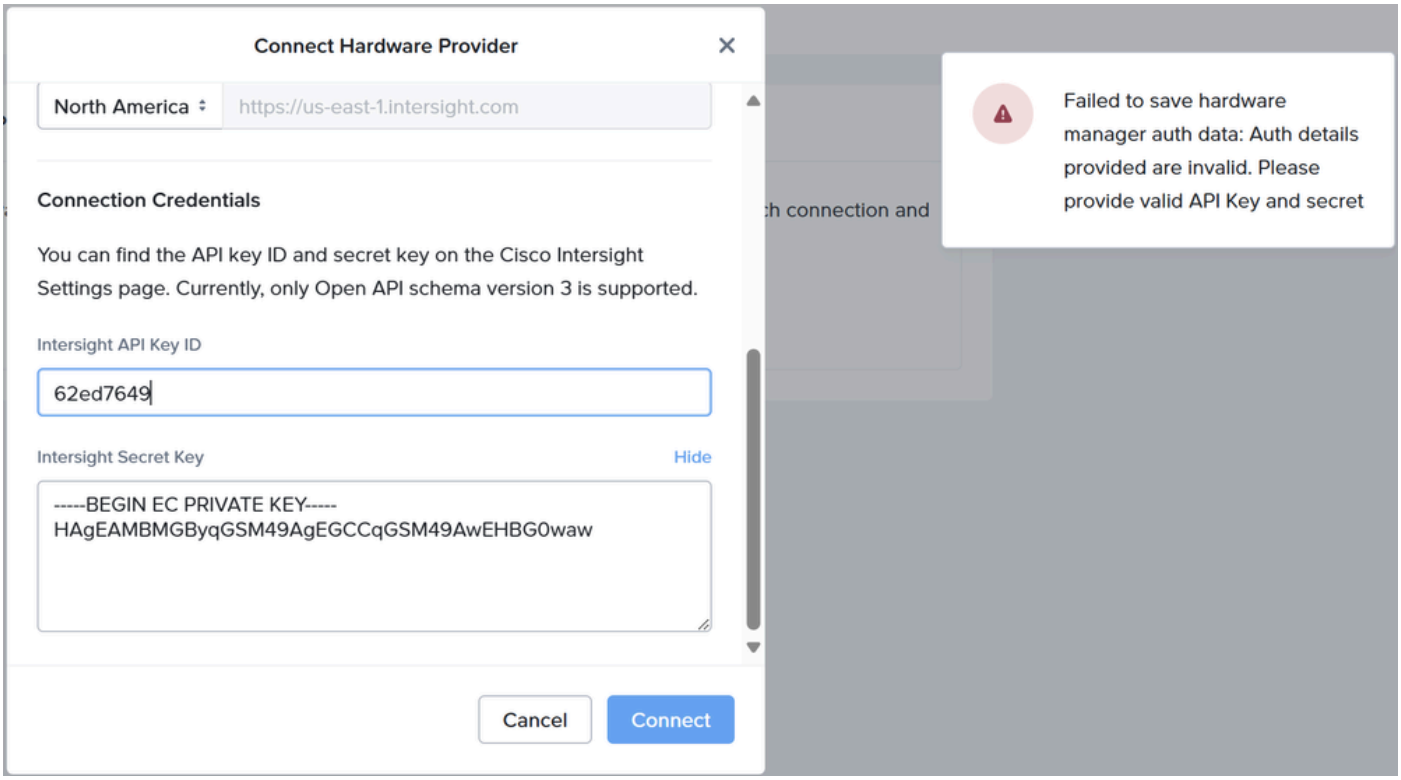
연결을 테스트하는 네트워크 명령

명령을 사용합니다	설명

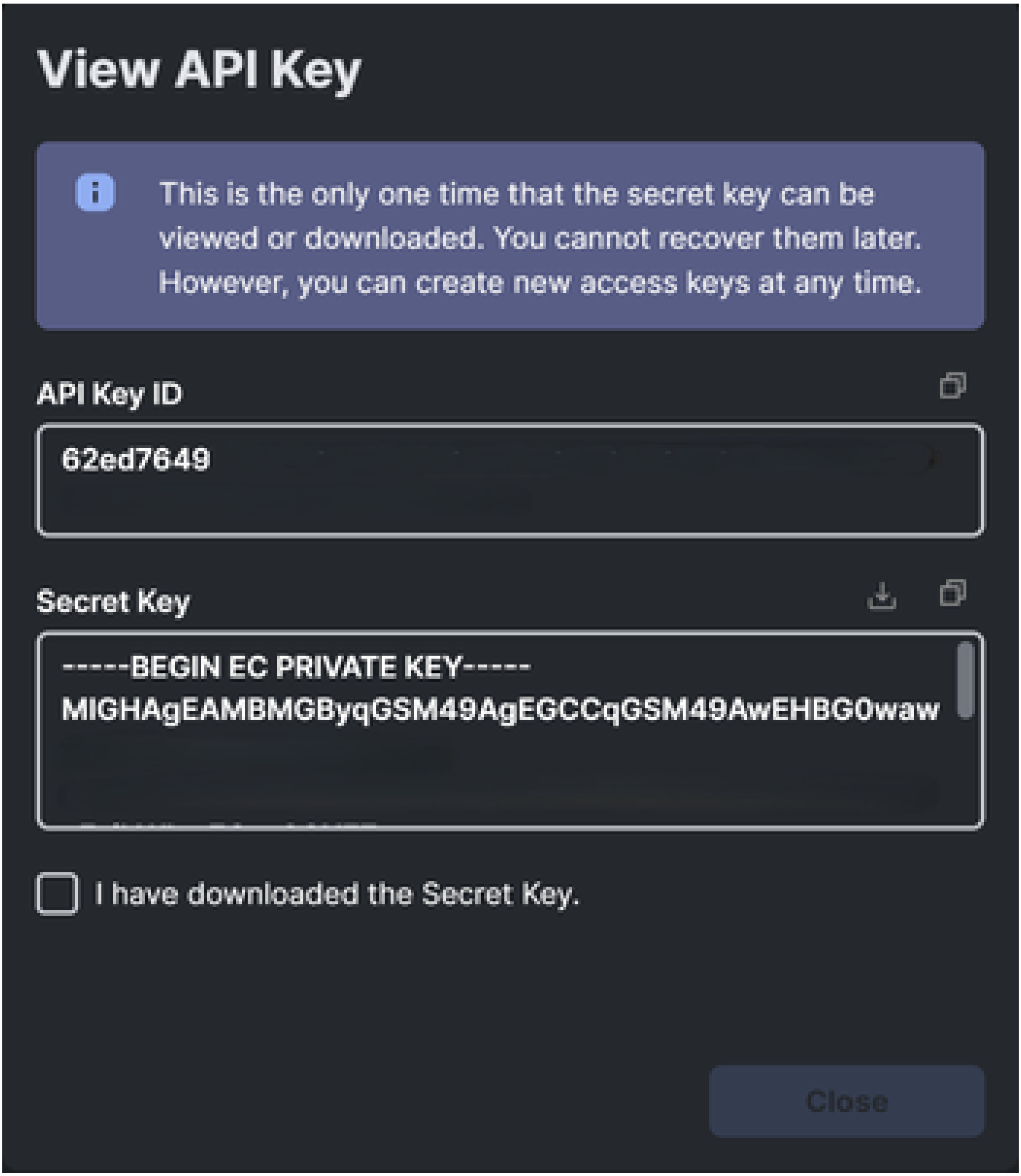
curl -v -k https://<Intersight URL> curl -v -k https://svc.intersight.com	Intersight 필수 URL에 대한 연결 테스트
curl -v -k —proxy <proxy address>:<port> <Intersight URL> curl -v -k —proxy http://proxy.esl.cisco.com:8080 https://svc.intersight.com	프록시가 필요한 경우 연결 테스트
curl -4|6 -v -k https://<Intersight URL> curl -4 -v -k https://svc.intersight.com	IPV4 또는 IPV6 주소 지정에 대한 연결 테스트 지정
tracepath <Intersight IP> tracepath 99.83.178.202	목적지 호스트로 향하는 패킷 추적
nslookup <URL> nslookup svc.Intersight.com	특정 주소와 연결된 IP 주소를 확인합니다.

제공된 인증 세부 정보가 잘못되었습니다.

"하드웨어 관리자 인증 데이터를 저장하지 못했습니다. 제공된 인증 세부 정보가 잘못되었습니다. 유효한 API 키와 암호를 입력하십시오."

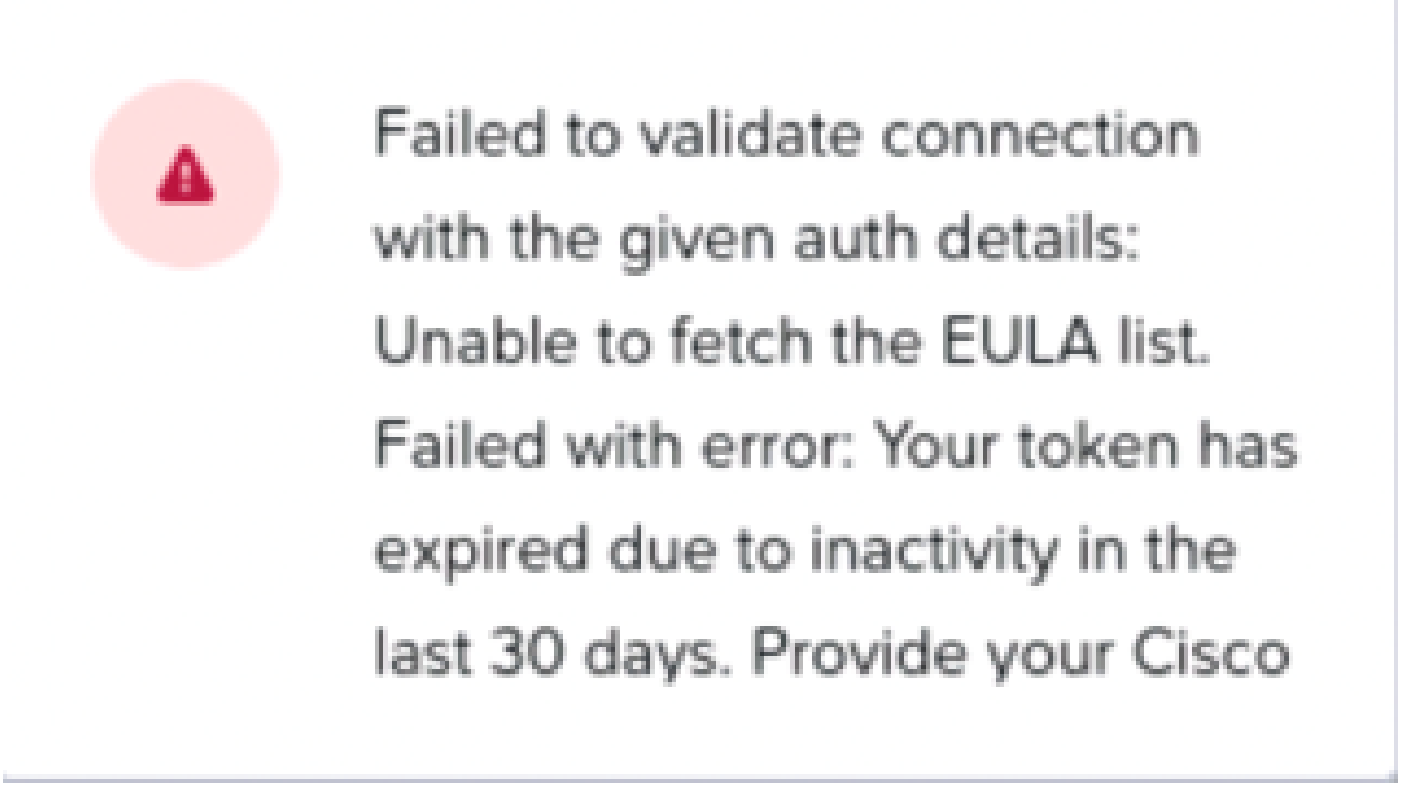


Intersight Secret Key를 입력하거나 붙여넣는 동안 오타 또는 누락된 문자가 없는지 확인해야 합니다. 그렇지 않으면 하드웨어 공급자에 대한 연결을 설정하지 못합니다.

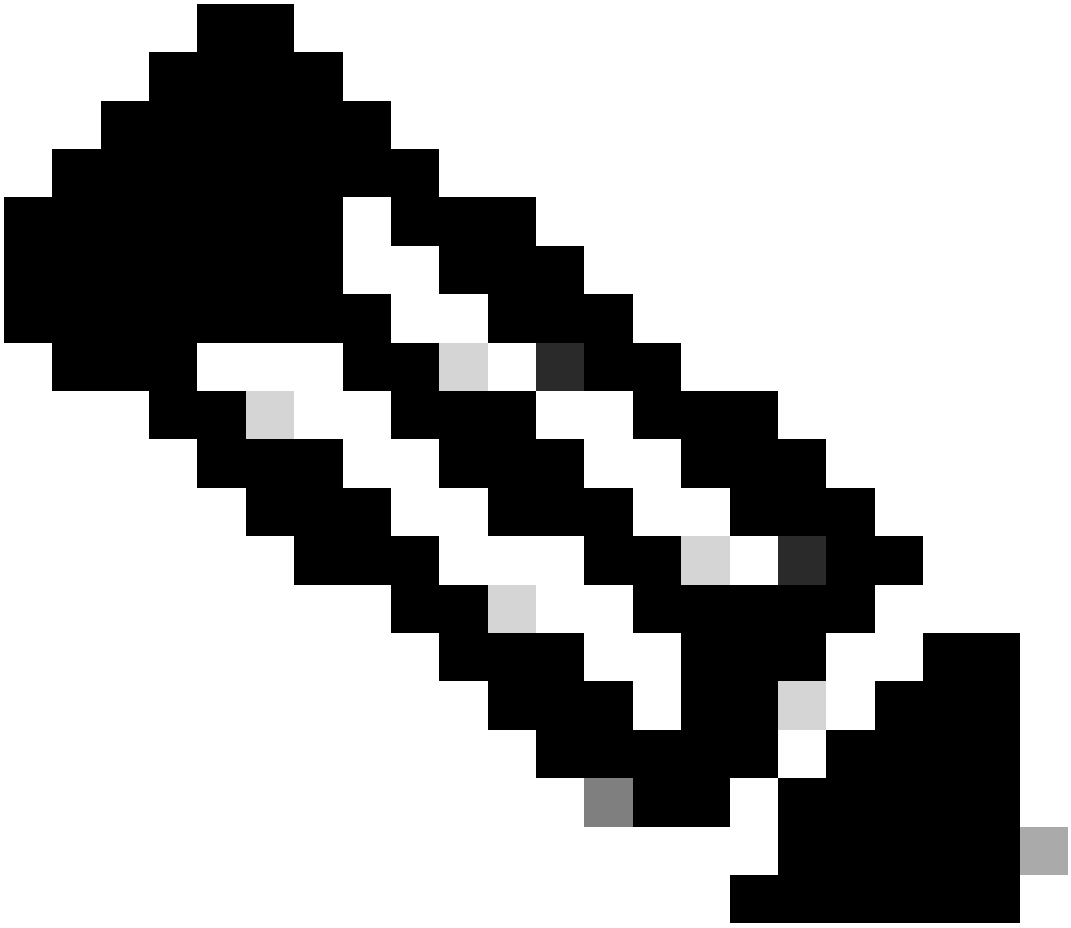


EULA 목록을 가져올 수 없음

"지정된 인증 세부 정보와의 연결을 검증하지 못했습니다. EULA 목록을 가져올 수 없습니다. 다음 오류로 인해 실패했습니다. 지난 30일 동안 활동이 없어 토큰이 만료되었습니다."

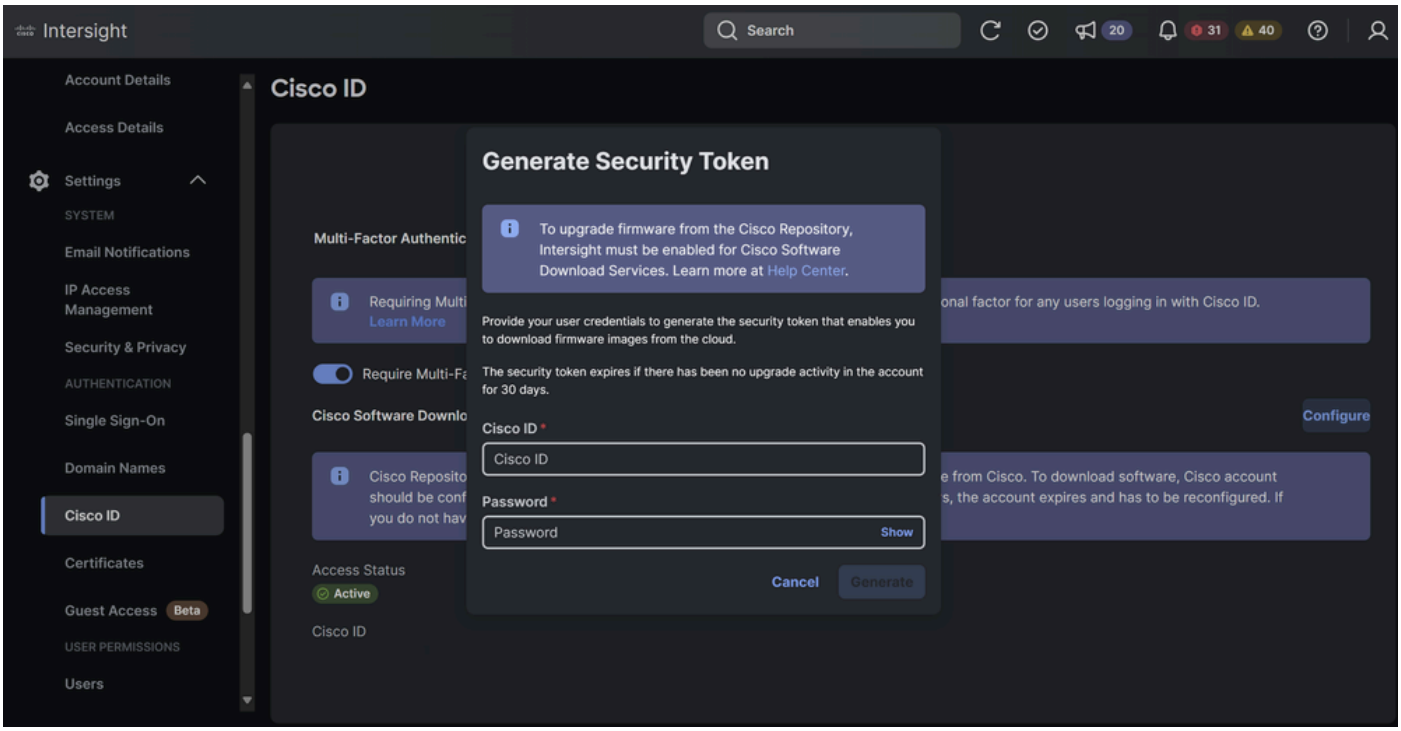


노드 온보딩 단계에서 "UUID를 사용하여 INTERSIGHT 하드웨어 관리자에 연결하지 못했습니다" 또는 "사용자 자격 증명이 만료되었을 수 있습니다."라는 오류가 발생할 수 있습니다. 이는 EULA와 관련하여 Intersight 어카운트 문제가 있는 경우에 나타납니다.



참고: 현재 ISM에는 EULA 동의가 필요합니다. 펌웨어 다운로드를 위해 EULA에 더 이상 의존하지 않기 때문에 앞으로 이 방법이 변경될 것입니다.

Intersight에서 이를 수정하려면 Settings(설정) > Cisco ID > Configure(구성) > Cisco ID 및 Password(Cisco ID 및 비밀번호 입력)로 이동합니다.



관련 정보

- Intersight의 조직 및 역할
- 포트 요구 사항
- 대상을 클레임하는 데 필요한 엔드포인트 URL
- Cisco Software Repository 액세스 권한 부여 및 EULA 동의

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.