

Problemen oplossen met Cisco HCI met Nutanix Hardware Provider Connection

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Problemen oplossen](#)

[Deadline voor context overschreden](#)

[DNS eigenaam resolutie](#)

[Prism Central VM kan geen verbinding maken met Intersight CVA / PVA](#)

[Netwerkopdrachten om connectiviteit te testen](#)

[De opgegeven Auth-gegevens zijn ongeldig](#)

[De EULA-lijst kan niet worden opgehaald](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u problemen met verbindingen tussen hardwareproviders kunt oplossen, van Nutanix Foundation Central tot Cisco Intersight.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan.

- Basiskennis van netwerkconnectiviteit.
- Basiskennis van Intersight API Keys.
- Intersight-account met ten minste serverbeheerdersrechten.



E-mail

Sign out



Account and role

Change

Server Administrator

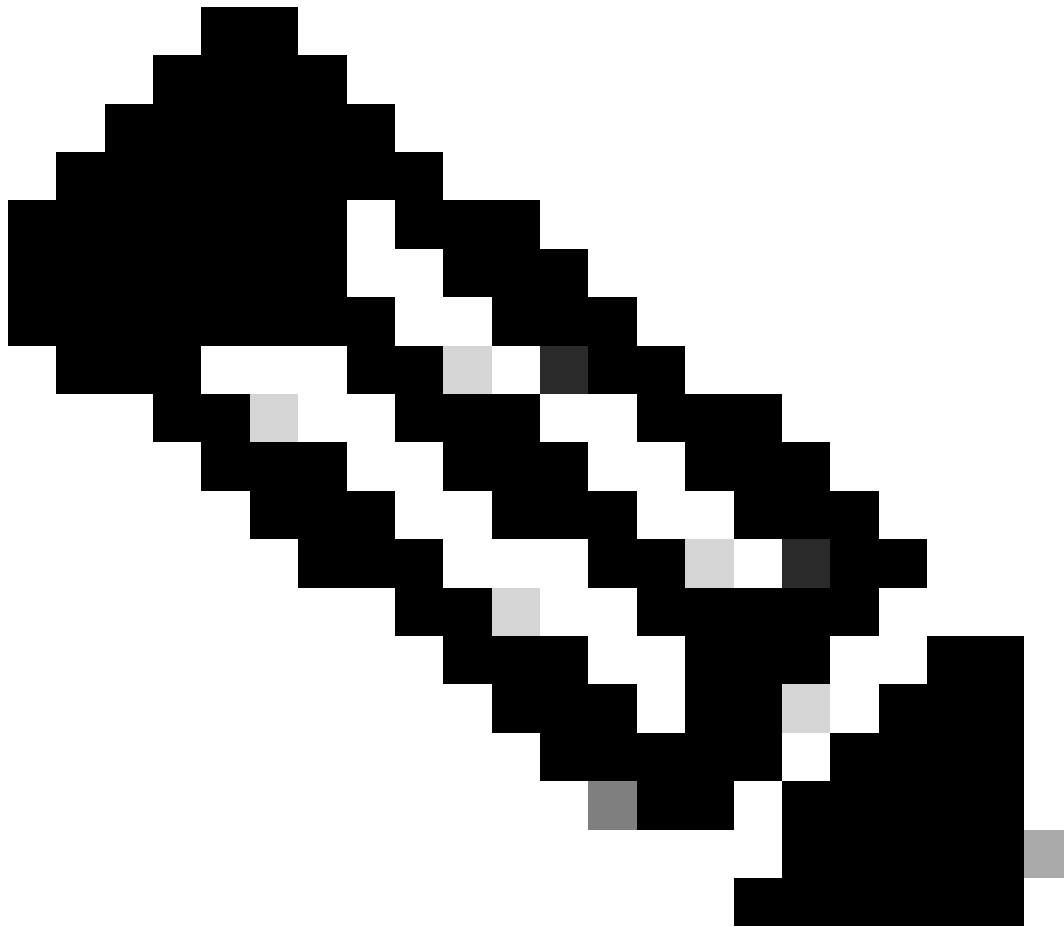


Region

intersight-aws-us-east-1

Access details

User settings



Opmerking: Intersight biedt Role-Based Access Control (RBAC) om systeemtoegang tot een gebruiker te autoriseren of te beperken, op basis van gebruikersrollen en -bevoegdheden. Een gebruikersrol in Intersight vertegenwoordigt een verzameling van de bevoegdheden die een gebruiker heeft om een reeks bewerkingen uit te voeren en biedt granulaire toegang tot bronnen. Intersight biedt op rollen gebaseerde toegang tot individuele gebruikers of een reeks gebruikers onder Groepen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

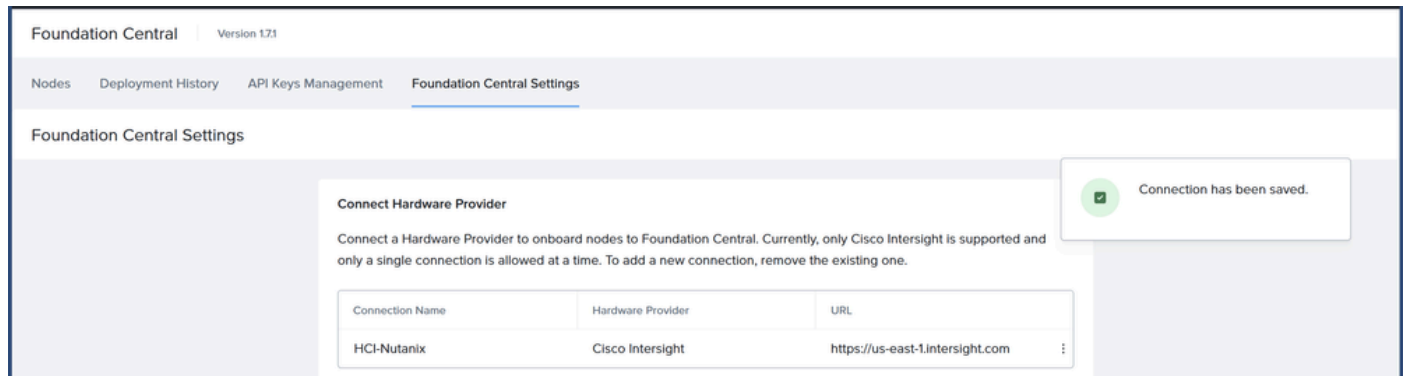
- Foundation Central 1.7.1 of hoger.
- Intersight SAAS, CVA en PVA.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Achtergrondinformatie

Het is vereist om Foundation Central te verbinden met Cisco Intersight als de hardwareprovider om de Cisco HCI met Nutanix-oplossing te implementeren in Intersight Standalone Mode ISM of Intersight Managed Mode IMM.



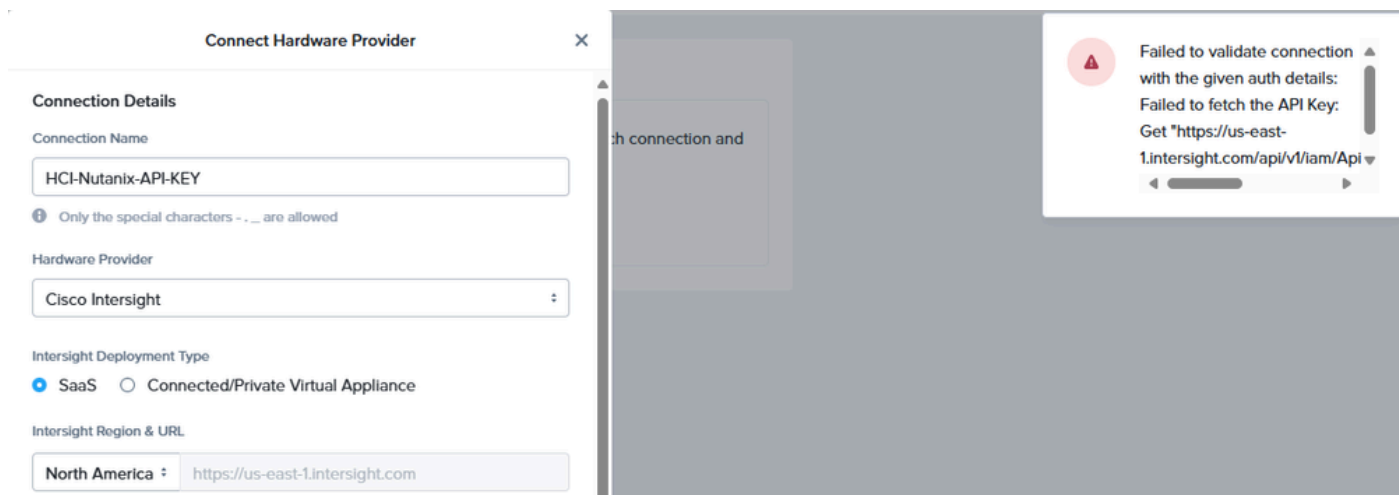
Standalone intervisiemodus: de knooppunten zijn verbonden met een paar Top-of-Rack (ToR)-switches en servers worden centraal beheerd met Cisco Intersight®. Hoewel er minimaal drie knooppunten nodig zijn om een standaard Nutanix-cluster te implementeren, bieden we ook de mogelijkheid om een cluster met één knooppunt en een cluster met twee knooppunten te implementeren voor Edge- en vertakkingslocaties en situaties waarin al een krachtige netwerkstructuur is geïnstalleerd.

Intersight Managed-modus: Intersight Managed-modus verenigt de mogelijkheden van de UCS-systemen en de cloudgebaseerde flexibiliteit van Intersight, waardoor de beheerervaring voor de op zichzelf staande en op Fabric Interconnect aangesloten systemen wordt verenigd. Het Intersight Management Model standaardiseert het beleid en het operationele beheer voor UCS-FI-6454, UCS-FI-64108, UCS-FI-6536, UCSX-S9108-100G Fabric Interconnects en Cisco UCS C-Series (M5, M6, M7, M8) en Cisco UCS X-Series (M6, M7, M8) servers.

Problemen oplossen

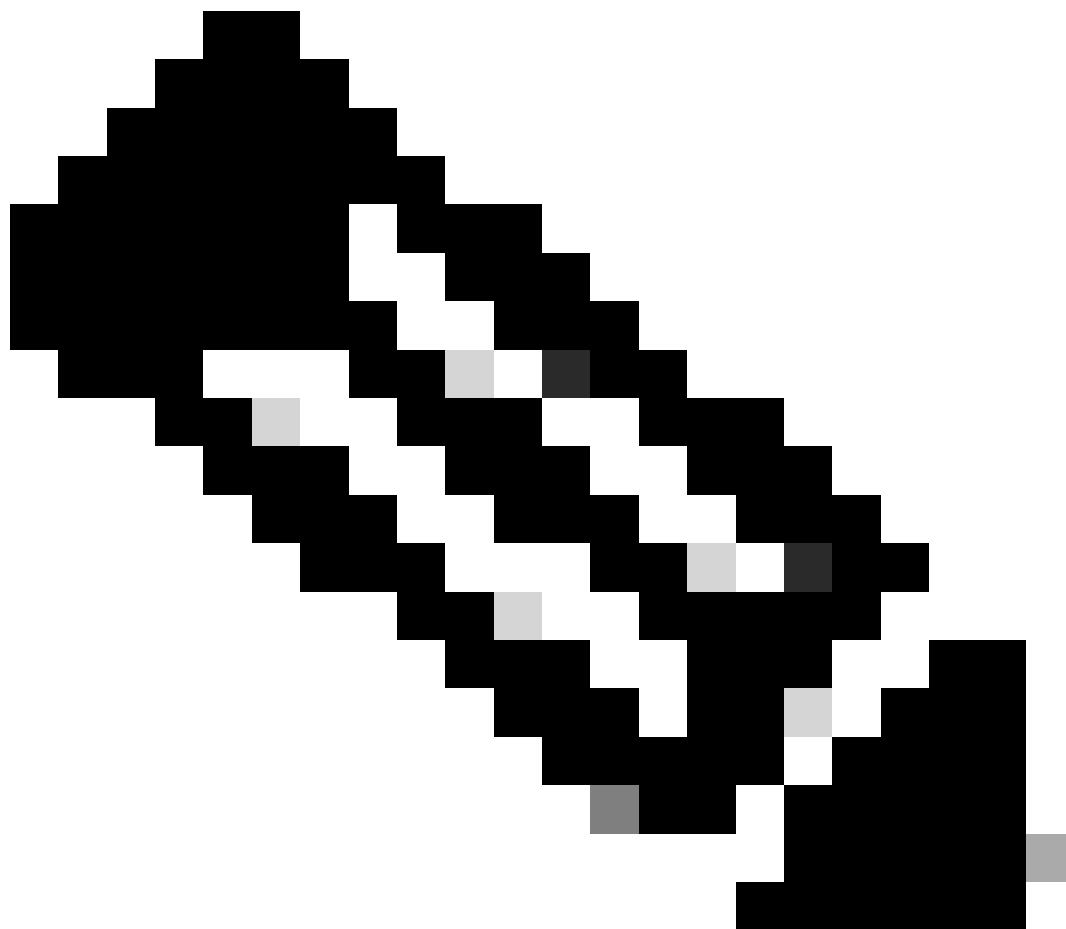
Deadline voor context overschreden

"De verbinding met de opgegeven auteursgegevens is niet gevalideerd: de API-sleutel is niet opgehaald: de contextdeadline is overschreden."



Zorg ervoor dat u de juiste connectiviteit hebt van Prism Central en Foundation Central naar de volgende URL's via de poorten 443 TCP/UDP en 80 TCP.

regio	URL	URL's vereist door apparaatconnectors
Noord-Amerika	intersight.com	svc.intersight.com
	us-east-1.intersight.com	svc.us-east-1.intersight.com
	Ips:	svc-static1.intersight.com
	52.223.48.112	ucs-starship.com*
	99.83.178.202	UCS-Connect.com*
EMEA	Intersight.com	
	eu-central-1.intersight.com	svc.eu-central-1.intersight.com
	Ips:	svc-static1.eu-central-1.intersight.com
	52.223.57.109	
	99.83.140.236	



Opmerking: Cisco Intersight ondersteunt twee regio's: de bestaande regio Noord-Amerika (VS-Oost-1) en de regio Europa, Midden-Oosten en Afrika (EMEA) (EU-Centraal-1).

Als u de vorige informatie wilt valideren, gaat u SSH in uw Prism Central of Foundation Central VM in en voert u een curl-opdracht uit naar de genoemde URL's en poorten.

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

```

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...
* Connected to svc.intersight.com (2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
*   subject: CN=us-east-1.intersight.com
*   start date: Apr 01 00:00:00 2025 GMT
*   expire date: Apr 30 23:59:59 2026 GMT
*   common name: us-east-1.intersight.com
*   issuer: CN=Amazon RSA 2048 M03,O=Amazon,C=US
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: svc.intersight.com
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 09 Sep 2025 18:53:00 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 82
< Connection: keep-alive
< Set-Cookie: AWSALB=W9cqyvSaX/07+KZ4058CopaQB1JlCo4TYocbNpCwsDBaDH/xquxQcaFXKe14m9SUn6/KJCRooj8o5BR/Q5w0Y4fxCLFL3ShwUNjehUjTf6EF0AY7AXD19WaiDlu; Expires=Tue, 16 Sep 2025 18:53:00 GMT; Path=/
< Set-Cookie: AWSALBCORS=W9cqyvSaX/07+KZ4058CopaQB1JlCo4TYocbNpCwsDBaDH/xquxQcaFXKe14m9SUn6/KJCRooj8o5BR/Q5w0Y4fxCLFL3ShwUNjehUjTf6EF0AY7AXD19WaiDlu; Expires=Tue, 16 Sep 2025 18:53:00 GMT; Path=/; SameSite=None; Secure
< X-Starship-Traceid: A5c88567814c27739a26fa67a590716182
* Connection #0 to host svc.intersight.com left intact
svc.intersight.com is alive and healthy at 2025-09-09 18:53:00.934344289 +0000 UTCadmin@NTNX-10-31-123-88-A-PCVM:~$ █

```

Succesvolle curl connectiviteitstest.

Als de opdracht curl mislukt, controleer dan bij uw firewallteam of de URL's en poorten zijn toegestaan in de firewall of de toegangslijst.

```

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:~$ █

```

Mislukte curl connectiviteitstest.

DNS eigen naam resolutie

Voor sommige firewall- of toegangslijsten moet het IP-adres van de genoemde URL's worden toegevoegd. Beide URL's lossen deze IPv4- en IPv6-adressen op:

- 52.223.48.112
- 99.83.178.202
- 2600:9000:A60C:6A4D:2D28:E9BE:E3E:F0CF
- 2600:9000:A706:C634:41:731C:AD1E:BF00

Dit kan worden gevalideerd met behulp van de opdracht nslookup.

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

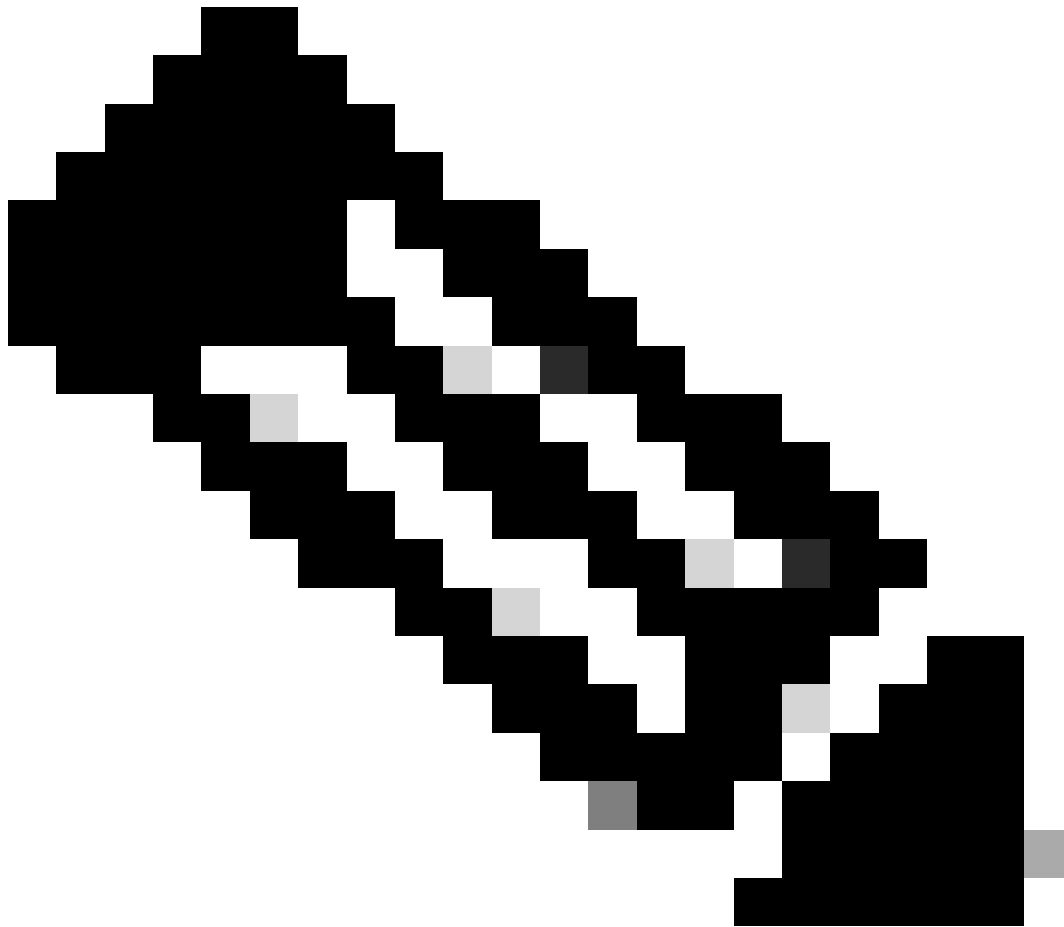
admin@NTNX-10-31-123-88-A-PCVM:~$ █
```

nslookup, opdracht

Prism Central VM kan geen verbinding maken met Intersight CVA / PVA

Wanneer er een directe verbinding is van Prism Central naar Intersight CVA / PVA, zorg er dan voor dat u verbinding toestaat op poort 443.

Als de PC VM een proxy heeft geconfigureerd om verbinding te maken met het internet voor taken zoals het downloaden van software of LCM, moet u de Intersight CVA / PVA FQDN en het IP-adres op de Prism Central Proxy-instellingen wit vermelden.



Opmerking: een whitelist is een enkele host die wordt geïdentificeerd door een IP-adres of een netwerk dat wordt geïdentificeerd door het netwerkadres en het subnetmasker. Het toevoegen van een whitelist betekent "negeer proxy-instellingen voor dit adres of netwerk".

Om dit in Prism Central te corrigeren, navigeert u naar: Instellingen > Netwerk > HTTP-proxy > Klik op het potloodpictogram om >Whitelist te bewerken.

The screenshot shows the Prism web interface. On the left, a sidebar lists various settings categories: Settings, Upgrade Prism Central, Witness, Setup, Connect to Frame, Enable App Management, Enable Disaster Recovery, Pulse, vCenter Registration, Network, Advanced Networking, HTTP Proxy (selected), and Name Servers. The main content area displays the 'Update HTTP Proxy' configuration window. This window includes input fields for 'Username' and 'Password', a note to 'Enter new password to change it.', checkboxes for 'HTTP' and 'HTTPS' protocols (both are checked), and a 'Whitelist' section. The whitelist is a table with two entries: 'is-pva.mxsvlab.com' and 'is-cva.mxsvlab.com', each with edit and delete icons. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

HTTP-proxy

U kunt bevestigen of deze stappen succesvol waren door de connectiviteit met Intersight CVA / PVA te testen met een curl-opdracht.

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

```
curl -v -k https://is-pva.mxsvlab.com
* Trying 10.10.10.10:443...
* Connected to is-pva.mxsvlab.com (10.10.10.10) 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
```

Krultest

Netwerkopdrachten om connectiviteit te testen

Opdracht	Beschrijving
----------	--------------

<pre>curl -v -k https://<Intersight URL> curl -v -k https://svc.intersight.com</pre>	Connectiviteit testen naar een vereiste URL voor Intersight
<pre>curl -v -k --proxy <proxy-adres>:<port> <Intersight URL> curl -v -k --proxy http://proxy.esl.cisco.com:8080 https://svc.intersight.com</pre>	Connectiviteit testen wanneer proxy vereist is
<pre>curl -4 6 -v -k https://<Intersight URL> curl -4 -v -k https://svc.intersight.com</pre>	Connectiviteitstest voor IPV4- of IPV6-adressering opgeven
<pre>tracpath <Intersight IP> Tracepath 99.83.178.202</pre>	Pakketten traceren naar een bestemmingshost
<pre>nslookup <URL> nslookup svc.Intersight.com</pre>	Bepaalt het IP-adres dat is gekoppeld aan het specifieke adres

De opgegeven Auth-gegevens zijn ongeldig

"De gegevens van de autorisatie van de hardwarebeheerder zijn niet opgeslagen: de verstrekte gegevens zijn ongeldig. Geef een geldige API-sleutel en geheim op."

Connect Hardware Provider

North America ⌵

Connection Credentials

You can find the API key ID and secret key on the Cisco Intersight Settings page. Currently, only Open API schema version 3 is supported.

Intersight API Key ID

Intersight Secret Key Hide

-----BEGIN EC PRIVATE KEY-----
HAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0waw

Cancel

Connect



Failed to save hardware manager auth data: Auth details provided are invalid. Please provide valid API Key and secret

U moet bevestigen dat er geen typografische fouten of ontbrekende tekens zijn tijdens het typen of plakken van de Intersight Secret-sleutel, anders wordt de verbinding met de hardwareprovider niet tot stand gebracht.

View API Key



This is the only one time that the secret key can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

API Key ID



62ed7649

Secret Key



-----BEGIN EC PRIVATE KEY-----

MIGHAgEAMBMGBByqGSM49AgEGCCqGSM49AwEHBG0waw

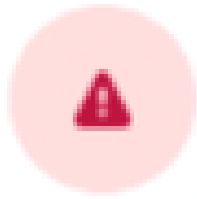
☐

I have downloaded the Secret Key.

Close

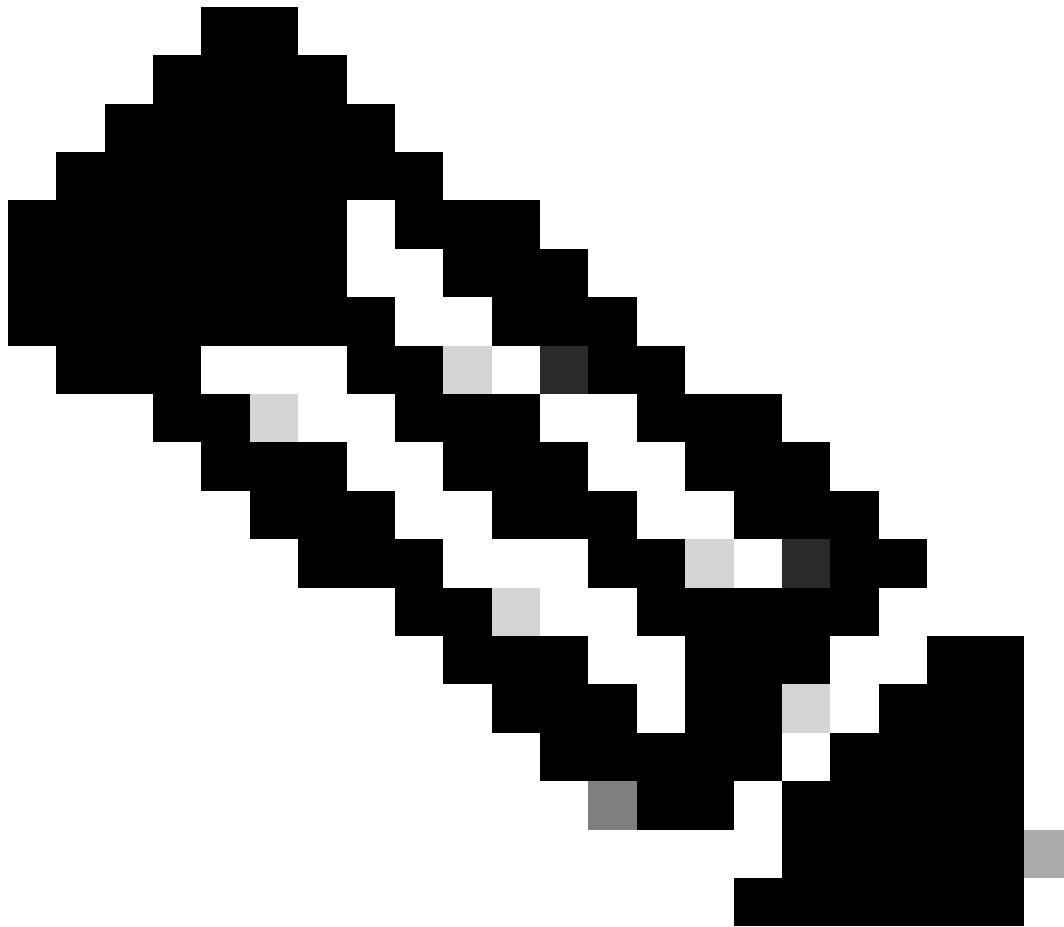
De EULA-lijst kan niet worden opgehaald

"De verbinding met de opgegeven auteursgegevens is niet gevalideerd: de EULA-lijst kan niet worden opgehaald. Fout: je token is verlopen vanwege inactiviteit in de afgelopen 30 dagen."



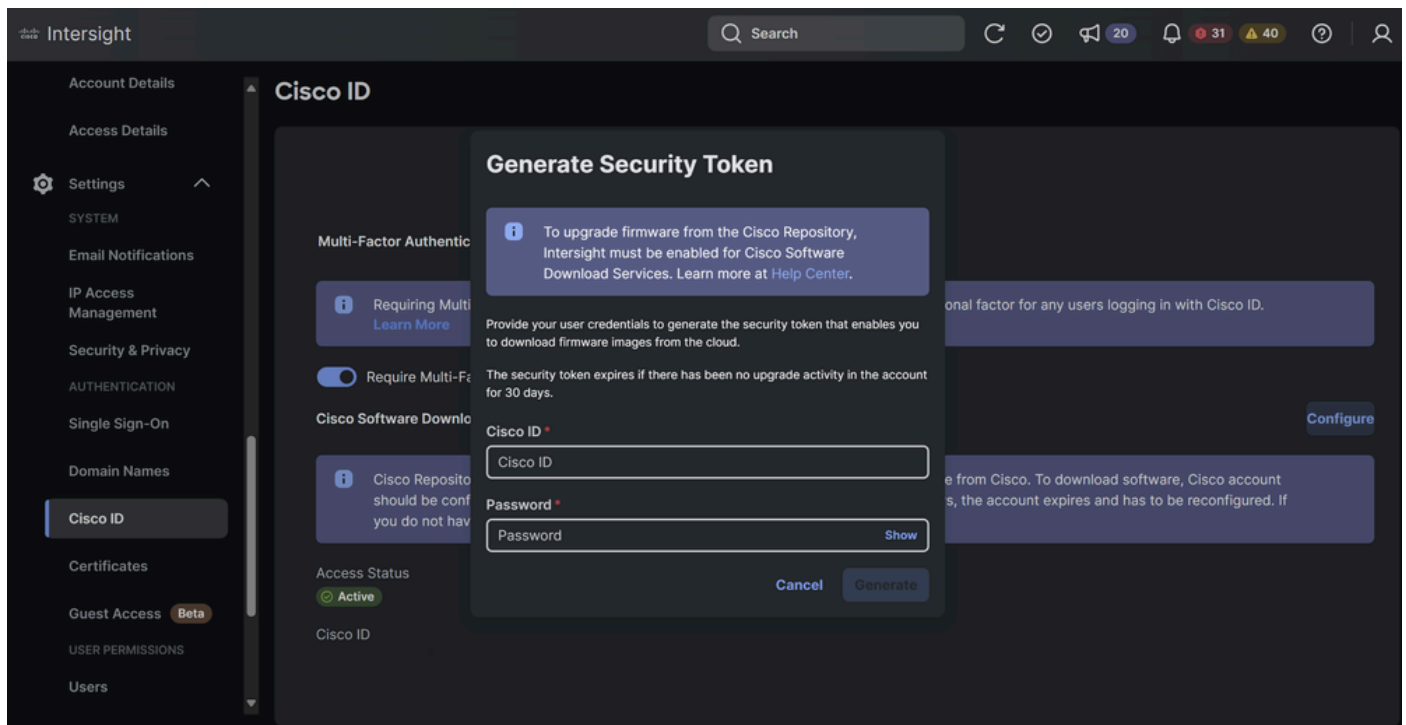
Failed to validate connection
with the given auth details:
Unable to fetch the EULA list.
Failed with error: Your token has
expired due to inactivity in the
last 30 days. Provide your Cisco

Tijdens de fase Onboarding Nodes kunt u een fout tegenkomen: "Kan geen verbinding maken met INTERSIGHT-hardwarebeheer met UUID" of "Uw gebruikersreferenties kunnen zijn verlopen." Dit wordt weergegeven als er een Intersight-accountprobleem is met betrekking tot de EULA.



Opmerking: Vanaf vandaag is EULA-acceptatie VEREIST voor ISM. Dit gaat in de toekomst veranderen, omdat we niet langer vertrouwen op de EULA voor het downloaden van firmware.

Om dit te corrigeren in Intersight Navigeer naar: Instellingen > Cisco ID > Configureren > Cisco ID en wachtwoord invoeren.



Gerelateerde informatie

- [Organisaties en rollen in intersight](#)
- [Havenvereisten](#)
- [Eindpunt-URL's vereist om doelen te claimen](#)
- [Toegang verlenen tot Cisco Software Repository en EULA accepteren](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.