

# Troubleshoot Cisco HCI with Nutanix Hardware Provider Connection Issues

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Troubleshoot](#)

[Context Deadline Exceeded](#)

[DNS Proper Name Resolution](#)

[Prism Central VM Can't Connect To Intersight CVA / PVA](#)

[Network Commands To Test Connectivity](#)

### [Auth Details Provided Are Invalid](#)

### [Unable To Fetch The EULA List](#)

### [Related Information](#)

---

## Introduction

This document describes how to troubleshoot hardware provider connections issues from Nutanix Foundation Central to Cisco Intersight.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics.

- Basic understanding of network connectivity.
- Basic understanding of Intersight API Keys.
- Intersight Account with at least Server Administrator privileges.



E-mail

Sign out



Account and role

Change

Server Administrator

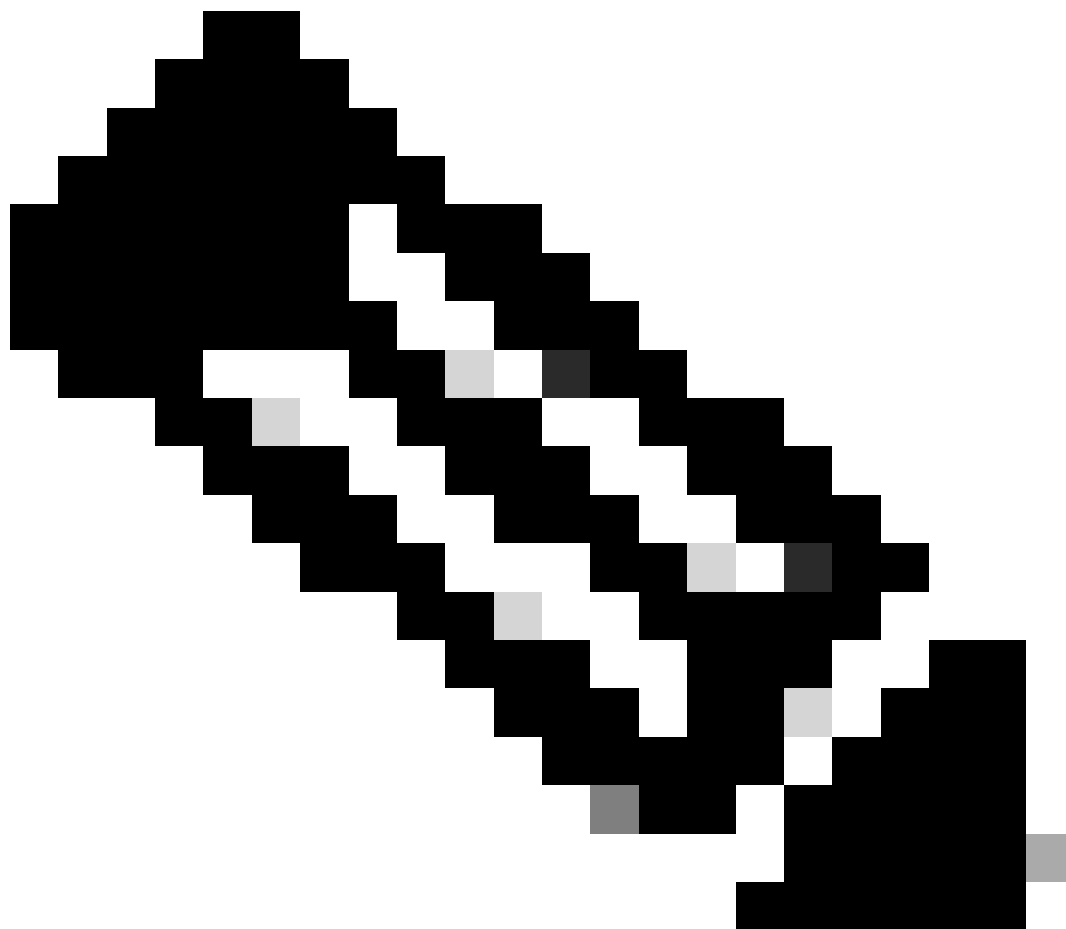


Region

**intersight-aws-us-east-1**

**Access details**

**User settings**



**Note:** Intersight provides Role-Based Access Control (RBAC) to authorize or restrict system access to a user, based on user roles and privileges. A user role in Intersight represents a collection of the privileges a user has to perform a set of operations and provides granular access to resources. Intersight provides role-based access to individual users or a set of users under Groups.

---

## Components Used

The information in this document is based on these software and hardware versions:

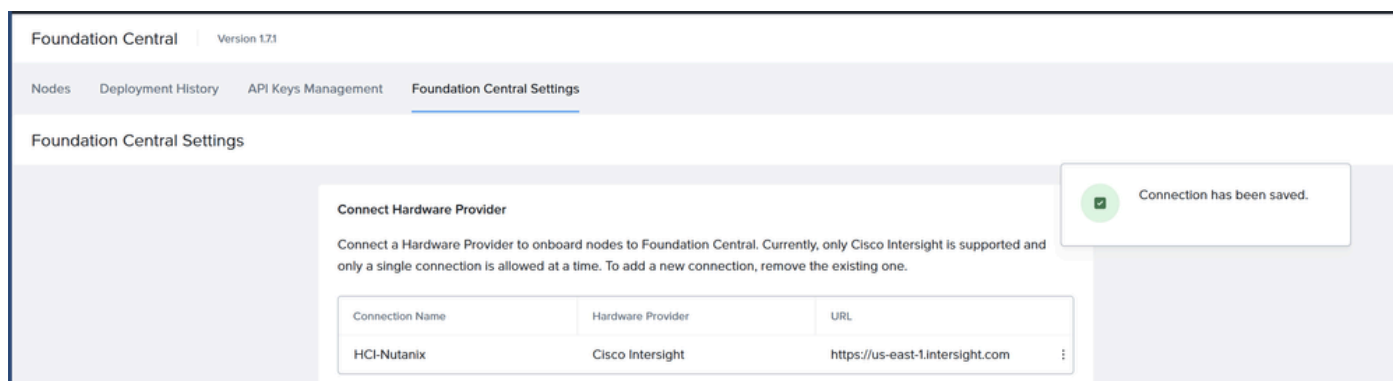
- Foundation Central 1.7.1 or higher.
- Intersight SAAS, CVA and PVA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

It is required to connect Foundation Central to Cisco Intersight as the hardware provider to deploy the Cisco

HCI with Nutanix solution in Intersight Standalone Mode ISM or Intersight Managed Mode IMM.



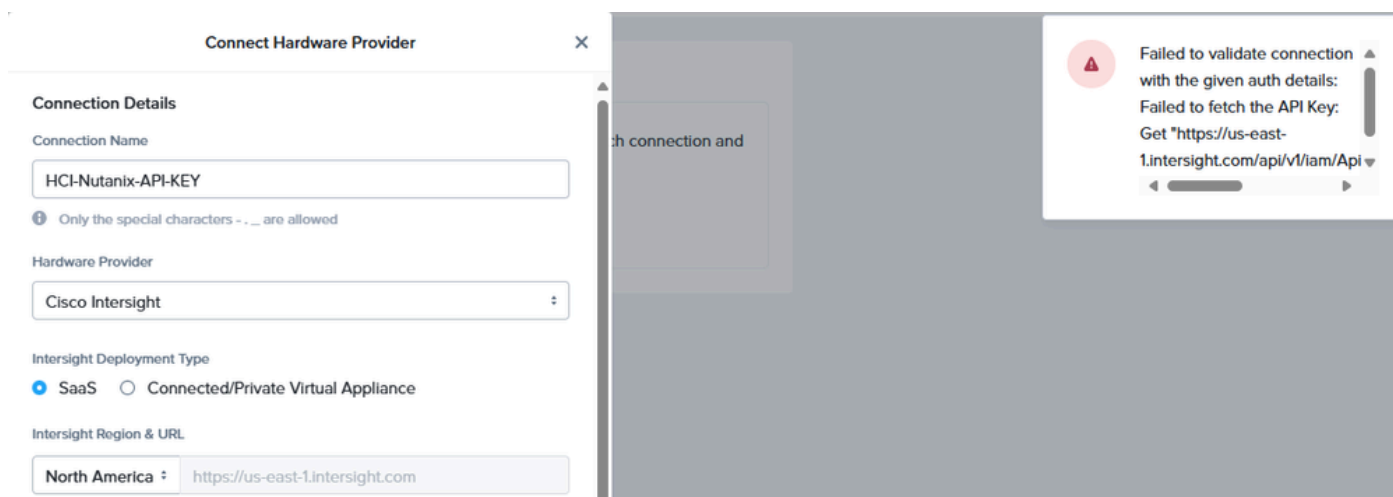
**Intersight Standalone mode:** The nodes are connected to a pair of Top-of-Rack (ToR) switches and servers are centrally managed using Cisco Intersight®. While a minimum of three nodes are required to deploy a standard Nutanix cluster, we also offer an option to deploy a single node cluster and a two-node cluster for Edge and branch locations and situations that already have a high-performance network fabric installed.

**Intersight Managed mode:** Intersight Managed Mode unifies the capabilities of the UCS Systems and the cloud-based flexibility of Intersight, thus unifying the management experience for the standalone and Fabric Interconnect attached systems. Intersight Management Model standardizes policy and operation management for UCS-FI-6454, UCS-FI-64108, UCS-FI-6536, UCSX-S9108-100G Fabric Interconnects and Cisco UCS C-Series (M5, M6, M7, M8), and Cisco UCS X-Series (M6, M7, M8) servers.

## Troubleshoot

### Context Deadline Exceeded

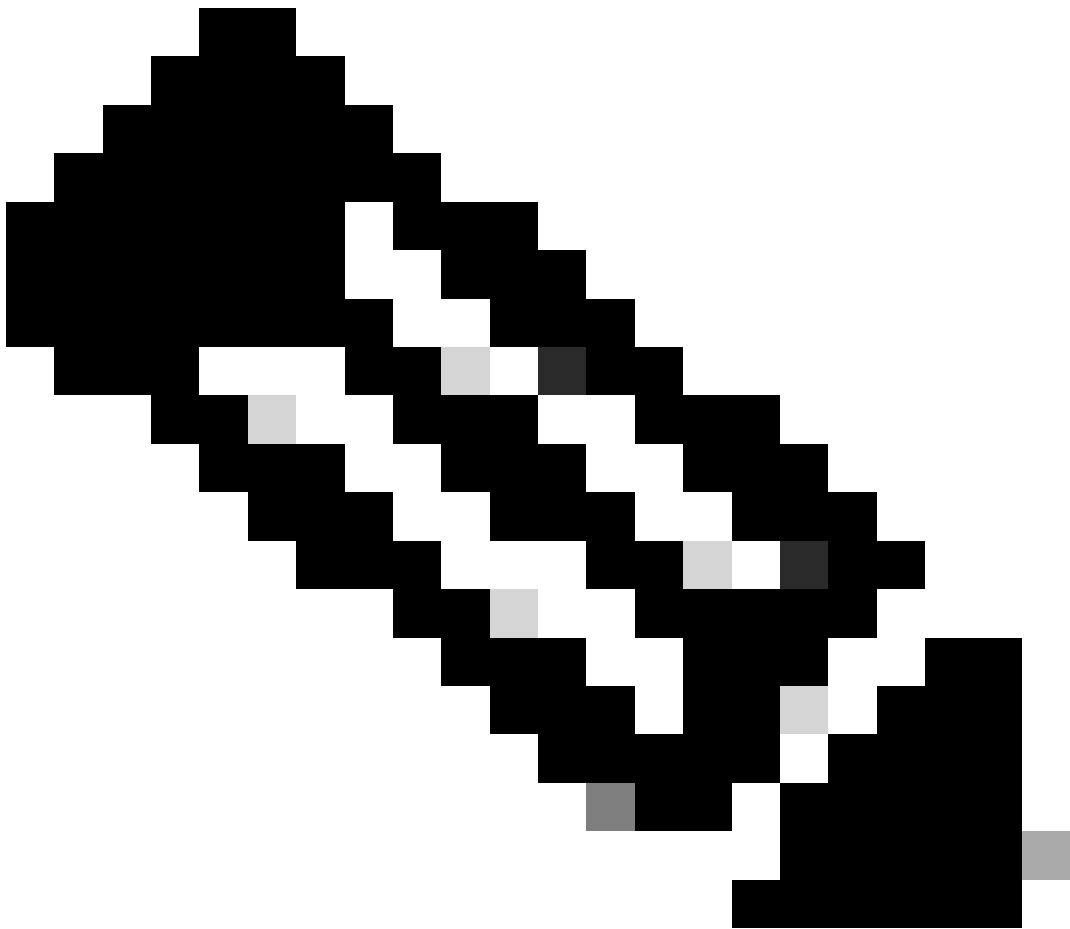
"Failed to validate connection with the given auth details: Failed to fetch the API Key: context deadline exceeded."



Ensure that you have proper connectivity from Prism Central and Foundation central to the next URLS through the ports 443 TCP/UDP and 80 TCP.

| Region        | URL            | URLs required by Device Connectors |
|---------------|----------------|------------------------------------|
| North America | intersight.com | svc.intersight.com                 |

|      |   |   |
|------|---|---|
|      | us-east-1.intersight.com<br>Ips:<br>52.223.48.112<br>99.83.178.202                      | svc.us-east-1.intersight.com<br>svc-static1.intersight.com<br>ucs-starship.com*<br>ucs-connect.com* |
| EMEA | Intersight.com<br>eu-central-1.intersight.com<br>Ips:<br>52.223.57.109<br>99.83.140.236 | svc.eu-central-1.intersight.com<br>svc-static1.eu-central-1.intersight.com                          |



**Note:** Cisco Intersight supports two regions: the existing North America region (us-east-1) and the

---

Europe, Middle East and Africa (EMEA) region (eu-central-1).

---

To validate the previous information, please SSH into your Prism Central or Foundation Central VM and perform a curl command to the mentioned URLS and ports.

```
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+KZ4058CopaQ81JlmCo4TYocbNpCwsDBaDH/xquxQcaFXKe14m9SUn6/KJCRowj8o5BR/Q5w0Y4fxCLFL3ShwUNjehUjTf6EF0AY7AXD19WaiDlu; Expires=Tue, 16 Sep 2025 18:53:00 GMT; Path=/
< Set-Cookie: AWSALBCORS=W9cqyvSaX/07+KZ4058CopaQ81JlmCo4TYocbNpCwsDBaDH/xquxQcaFXKe14m9SUn6/KJCRowj8o5BR/Q5w0Y4fxCLFL3ShwUNjehUjTf6EF0AY7AXD19WaiDlu; Expires=Tue, 16 Sep 2025 18:53:00 GMT; Path=/; SameSite=None; Secure
< X-Starship-Traceid: ASc88567814c27739a26fa67a590716182
<
* 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:~$
```

*Successful curl connectivity test.*

If the curl command fails, please check with your firewall team that the URLS and ports are allowed into the firewall or access list.

```
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:~$
```

*Failed curl connectivity test.*

## DNS Proper Name Resolution

Some firewall or access list requires adding the resolving IP from the mentioned URLS, Both of these URLS resolve to these IPv4 and IPv6 addresses:

- 52.223.48.112
- 99.83.178.202

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

This can be validated by using nslookup command.

```
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

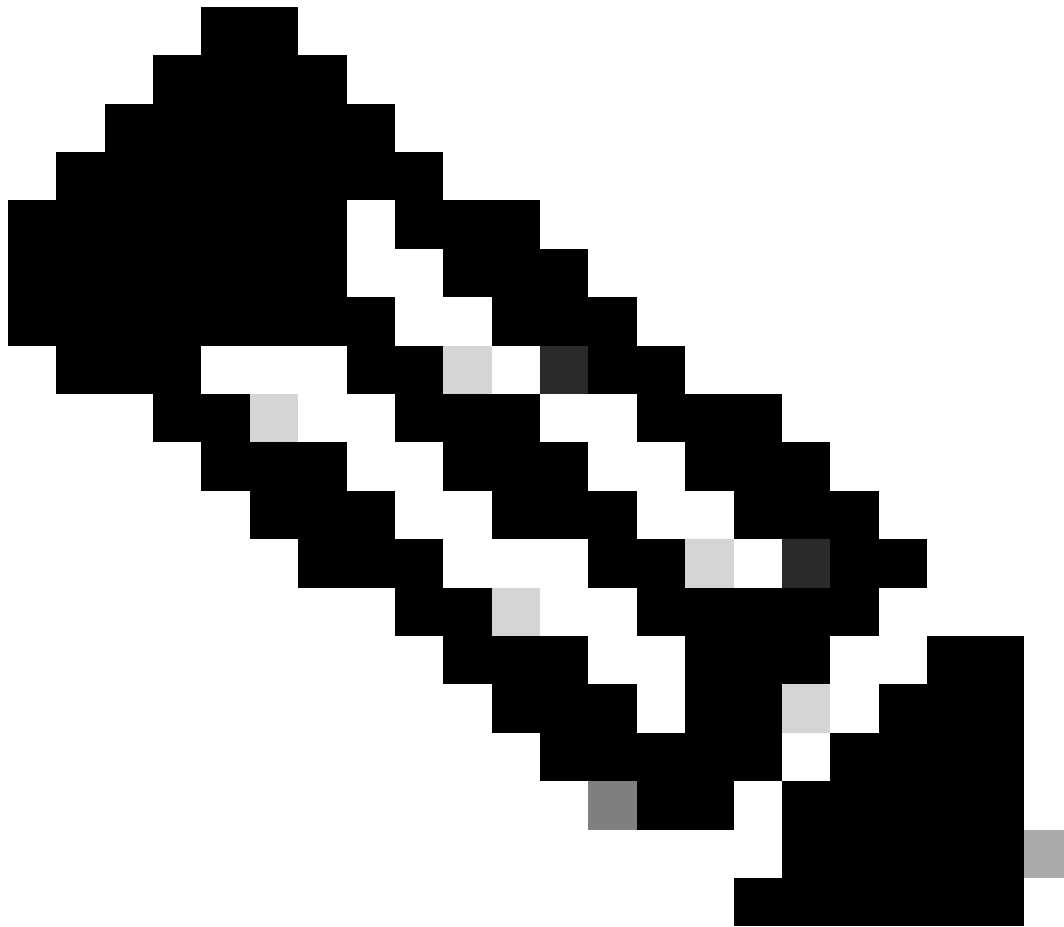
admin@NTNX-10-31-123-88-A-PCVM:~$ █
```

*nslookup command*

## **Prism Central VM Can't Connect To Intersight CVA / PVA**

When there is a direct connection from Prism Central to Intersight CVA / PVA make sure to allow connection on Port 443.

If PC VM has a proxy configured to connect to the internet for tasks like software downloads or LCM, you need to whitelist the Intersight CVA / PVA FQDN and IP address at Prism Central Proxy settings.

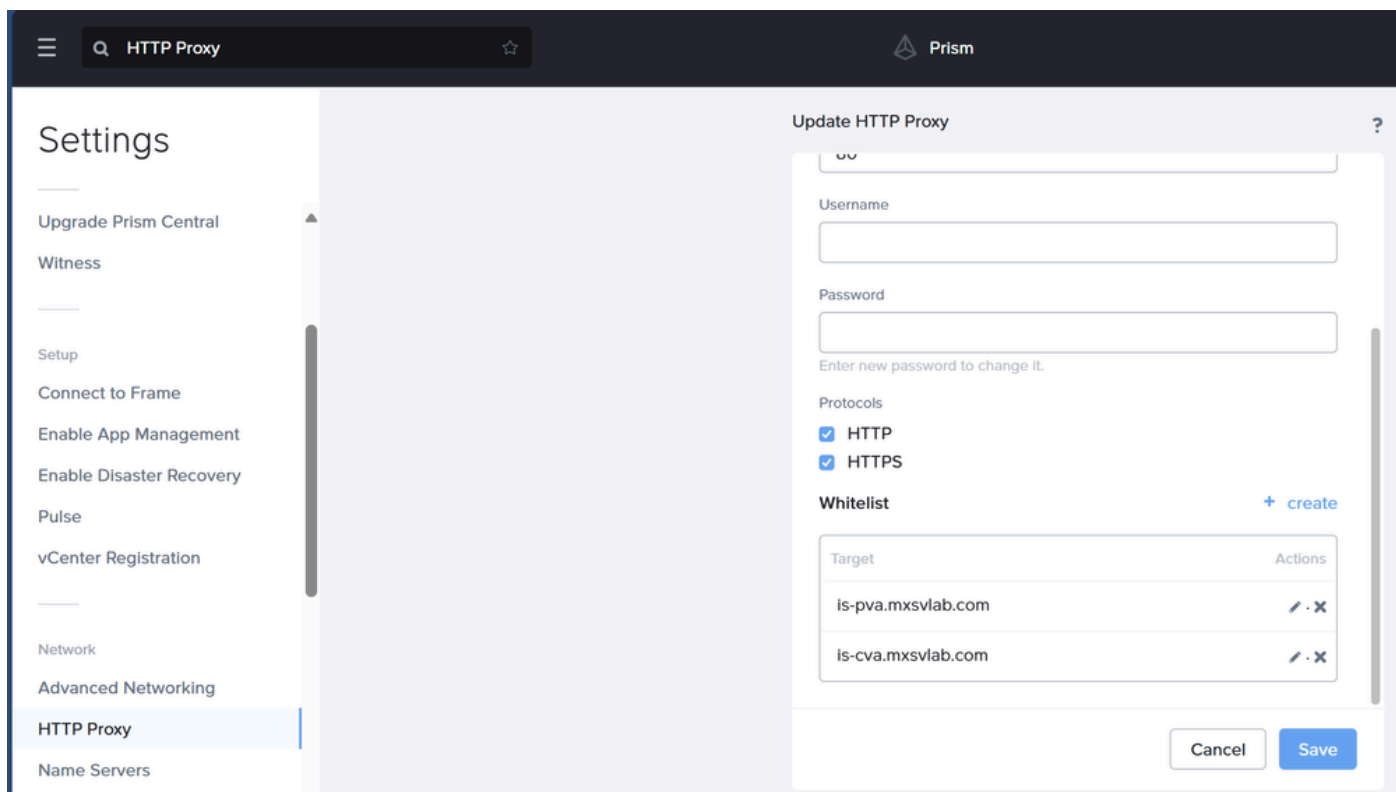


**Note:** A whitelist entry is a single host identified by IP address or a network identified by the network address and subnet mask. Adding a whitelist entry means “ignore proxy settings for this address or network”.

---

To correct this in Prism Central navigate to: Settings > Network > HTTP Proxy > Click on pencil icon to edit >Whitelist.





#### HTTP Proxy

You can confirm if these steps were successful by testing the connectivity to Intersight CVA / PVA with a curl command.

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

```
curl -v -k https://is-pva.mxsvlab.com
* Trying 192.168.1.100:443...
* Connected to is-pva.mxsvlab.com (192.168.1.100) 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
```

#### Curl test

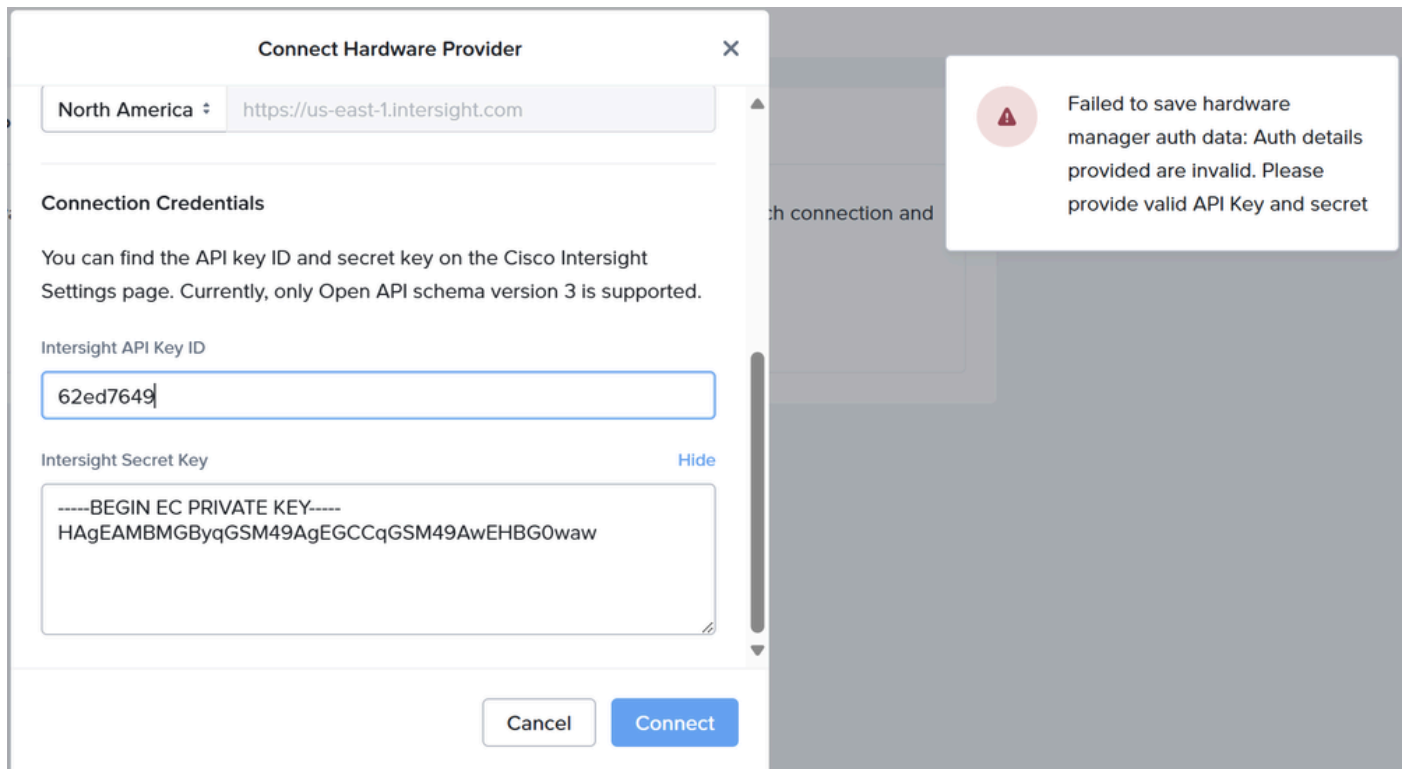
## Network Commands To Test Connectivity

| Command | Description |
|---------|-------------|
|---------|-------------|

|   |  |
|---|--|
| <pre>curl -v -k https://&lt;Intersight URL&gt;</pre> <p><b>curl -v -k https://svc.intersight.com</b></p>  | Test connectivity towards a Intersight required URL    |
| <pre>curl -v -k --proxy &lt;proxy address&gt;:&lt;port&gt; &lt;Intersight URL&gt;</pre> <p><b>curl -v -k --proxy <a href="http://proxy.esl.cisco.com:8080">http://proxy.esl.cisco.com:8080</a> https://svc.intersight.com</b></p> | Test connectivity when proxy is required               |
| <pre>curl -4 6 -v -k https://&lt;Intersight URL&gt;</pre> <p><b>curl -4 -v -k https://svc.intersight.com</b></p>  | Specify connectivity test to IPV4 or IPV6 addressing   |
| <pre>tracpath &lt;Intersight IP&gt;</pre> <p><b>tracpath 99.83.178.202</b></p>  | Traces packets towards a destination host              |
| <pre>nslookup &lt;URL&gt;</pre> <p><b>nslookup svc.Intersight.com</b></p>   | Determines IP address associated with specific address |

### Auth Details Provided Are Invalid


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



You need to confirm that there are no typographical errors or missing characters while typing or pasting the

Intersight Secret Key otherwise it fails to establish the connection to the hardware provider.

## 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

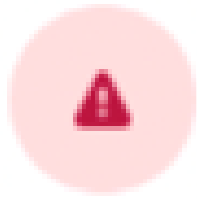
-----BEGIN EC PRIVATE KEY-----  
MIGHAgEAMBMGBByqGSM49AgEGCCqGSM49AwEHBG0waw

☐ I have downloaded the Secret Key.

Close

### Unable To Fetch The EULA List

"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."



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

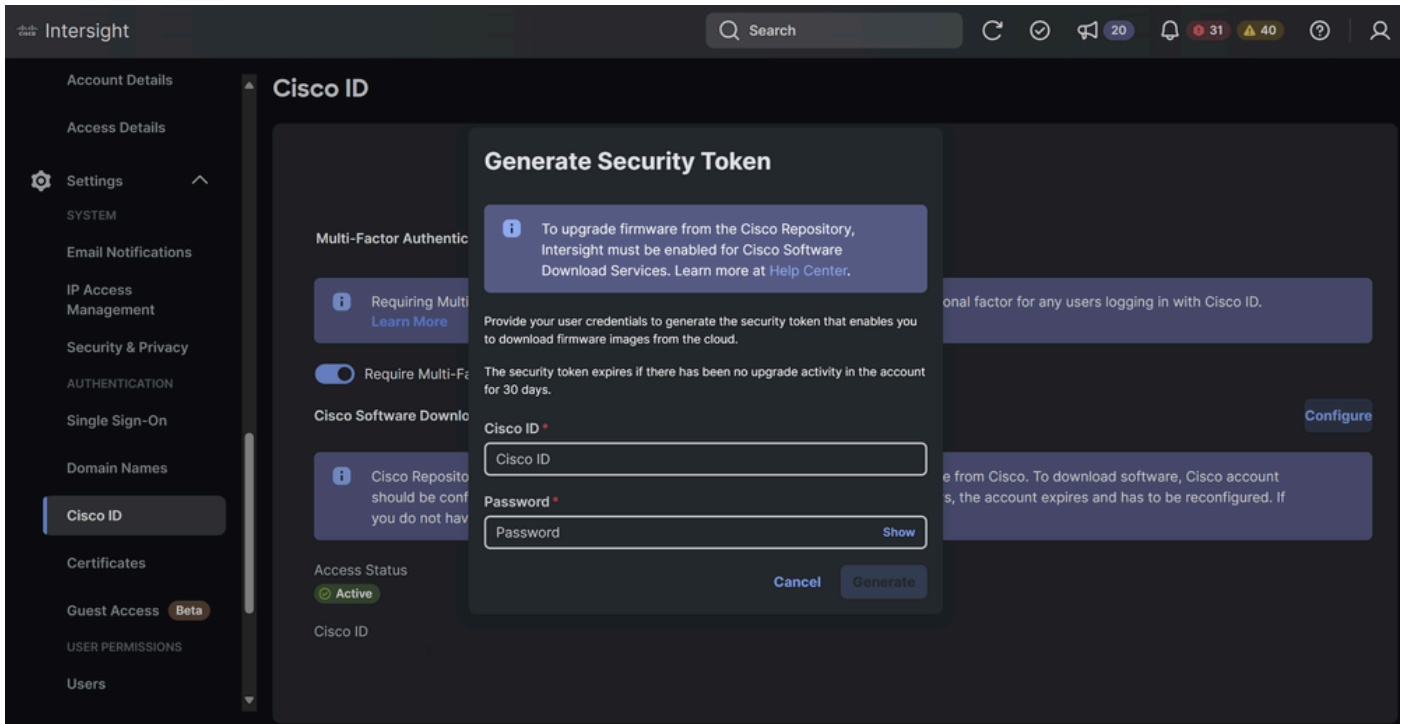
During the Nodes Onboarding phase, you might encounter an error "Failed to connect to INTERSIGHT hardware manager with UUID" or "Your user credentials could have expired.". This appears if there is an Intersight account issue with regards to the EULA.



**Note:** As of today, EULA acceptance is REQUIRED for ISM. This is going to change in the future since we no longer rely on the EULA for firmware downloads.

---

To correct this in Intersight Navigate to: Settings > Cisco ID > Configure > Enter Cisco ID and Password.



## Related Information

- [Organizations and Roles in Intersight](#)
- [Port Requirements](#)
- [Endpoint URLs Required to Claim Targets](#)
- [Grant Cisco Software Repository Access and Accept EULA](#)