

# Solución de problemas de conexión del proveedor de hardware de Cisco HCI con Nutanix

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Troubleshoot](#)

[Se excedió la fecha límite](#)

[Resolución de nombre adecuado de DNS](#)

[Prism Central VM no puede conectarse a Intersight CVA / PVA](#)

[Comandos de red para probar la conectividad](#)

[Los Detalles De Autenticación Proporcionados No Son Válidos](#)

[No se puede obtener la lista de EULA](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo resolver problemas de conexiones de proveedores de hardware desde Nutanix Foundation Central a Cisco Intersight.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas.

- Conocimiento básico de la conectividad de red.
- Comprensión básica de Intersight API Keys.
- Cuenta de interacción con al menos privilegios de administrador de servidor.



E-mail

[Sign out](#)



Account and role

[Change](#)

Server Administrator



Region

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

[Access details](#)

[User settings](#)



Nota: Intersight proporciona control de acceso basado en roles (RBAC) para autorizar o restringir el acceso del sistema a un usuario, en función de los roles y privilegios de este. Una función de usuario de Intersight representa una colección de los privilegios que tiene un usuario para realizar un conjunto de operaciones y proporciona acceso granular a los recursos. Intersight proporciona acceso basado en roles a usuarios individuales o a un conjunto de usuarios en Grupos.

---

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

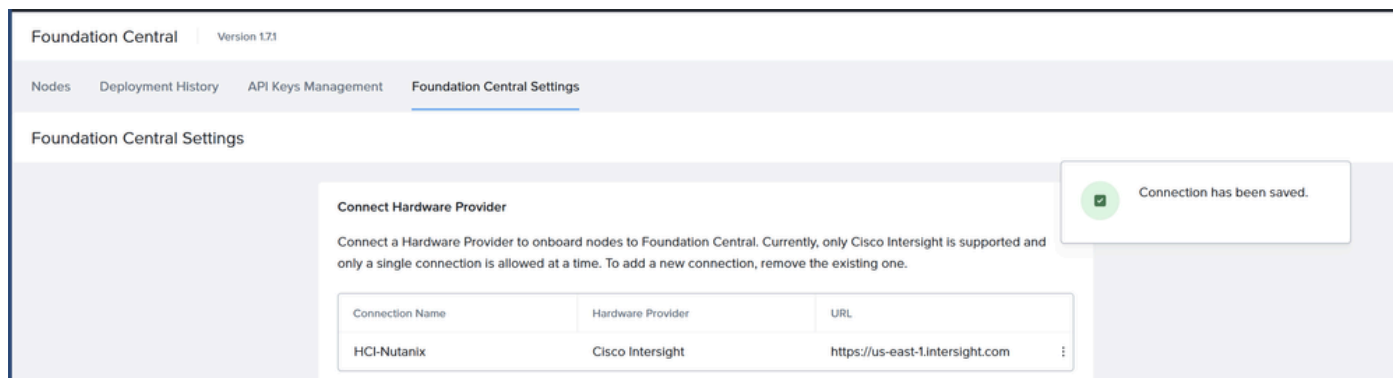
- Foundation Central 1.7.1 o superior.
- Intersight SAAS, CVA y PVA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Es necesario conectar Foundation Central a Cisco Intersight como proveedor de hardware para implementar la solución Cisco HCI con Nutanix en ISM en modo independiente de intersight o IMM en modo administrado de intersight.



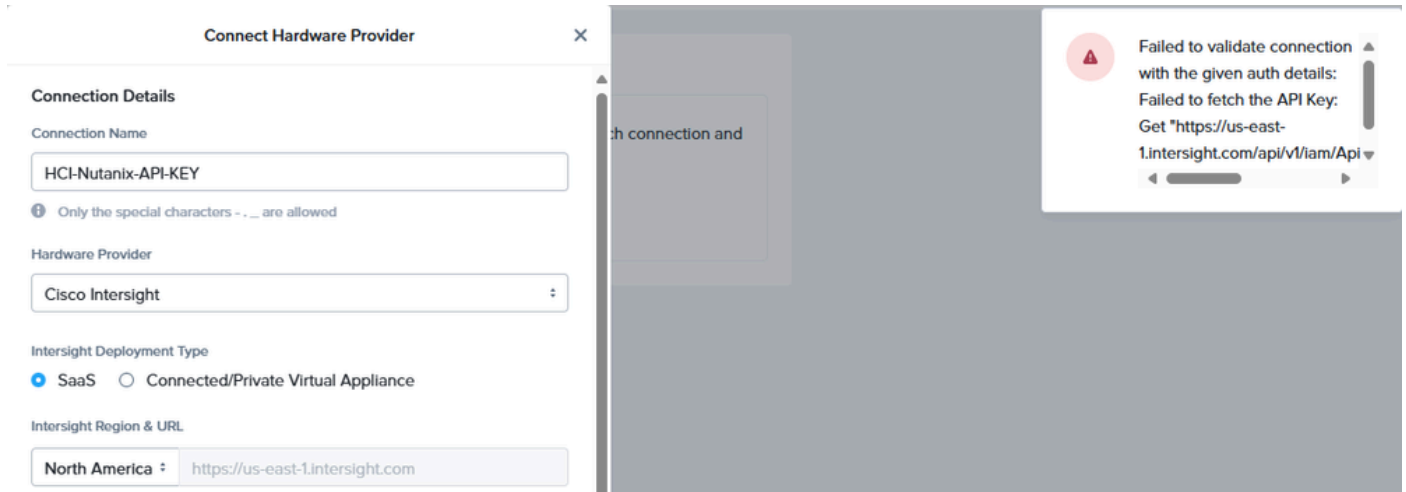
Intersight Standalone mode: los nodos están conectados a un par de switches top-of-rack (ToR) y los servidores se gestionan de forma centralizada mediante Cisco Intersight®. Si bien se requieren un mínimo de tres nodos para implementar un clúster Nutanix estándar, también ofrecemos la opción de implementar un clúster de un solo nodo y un clúster de dos nodos para ubicaciones de extremo y sucursal y situaciones que ya tienen instalado un fabric de red de alto rendimiento.

Intersight Managed Mode: Intersight Managed Mode unifica las capacidades de los sistemas UCS y la flexibilidad basada en la nube de Intersight, unificando así la experiencia de gestión para los sistemas conectados independientes y Fabric Interconnect. El modelo de gestión de información estandariza la gestión de operaciones y políticas para los servidores UCS-FI-6454, UCS-FI-64108, UCS-FI-6536, Fabric Interconnects UCS-S9108-100G y los servidores Cisco UCS serie C (M5, M6, M7, M8) y Cisco UCS serie X (M6, M7, M8).

## Troubleshoot

Se excedió la fecha límite

"No se pudo validar la conexión con los detalles de autenticación proporcionados: No se pudo obtener la clave de API: se ha superado la fecha límite del contexto."



Asegúrese de que dispone de la conectividad adecuada desde Prism Central y Foundation central a las siguientes URL a través de los puertos 443 TCP/UDP y 80 TCP.

Región	URL	URL requeridas por los conectores del dispositivo
América del Norte	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	



Nota: Cisco Intersight es compatible con dos regiones: la región existente de Norteamérica (us-east-1) y la región de Europa, Oriente Medio y África (EMEA) (eu-central-1).

---

Para validar la información anterior, introduzca SSH en la VM de Prism Central o Foundation Central y ejecute un comando curl para las URL y los puertos mencionados.

```
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+KZ4058CopaQB1JlMCo4TYocbNpCwsDBaDH/xquxQcaFXKe14m9SUn6/KJCRooj8o5BR/Q5w0Y4fxCLFL3ShwUNjehUjTf6EF0AY7AXD19WaidU; Expires=Tue, 16 Sep 2025 18:53:00 GMT; Path=/
< Set-Cookie: AWSALBCORS=W9cqyvSaX/07+KZ4058CopaQB1JlMCo4TYocbNpCwsDBaDH/xquxQcaFXKe14m9SUn6/KJCRooj8o5BR/Q5w0Y4fxCLFL3ShwUNjehUjTf6EF0AY7AXD19WaidU; 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:~$ █

```

Prueba de conectividad curl exitosa.

Si el comando curl falla, verifique con su equipo de firewall que las URL y los puertos están permitidos en el firewall o en la lista de acceso.

```

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:~$ █

```

Prueba de conectividad curl fallida.

## Resolución de nombre adecuado de DNS

Algunos firewalls o listas de acceso requieren que se agregue la dirección IP de resolución de las URL mencionadas. Ambas direcciones URL se resuelven en las siguientes direcciones IPv4 e IPv6:

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

Esto se puede validar mediante el comando 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:~$ █
```

comando nslookup

## Prism Central VM no puede conectarse a Intersight CVA / PVA

Cuando haya una conexión directa de Prism Central a Intersight CVA / PVA, asegúrese de permitir la conexión en el puerto 443.

Si la máquina virtual de PC tiene un proxy configurado para conectarse a Internet para tareas como descargas de software o LCM, debe incluir en la lista blanca el FQDN de Intersight CVA / PVA y la dirección IP en la configuración del proxy central de Prism.

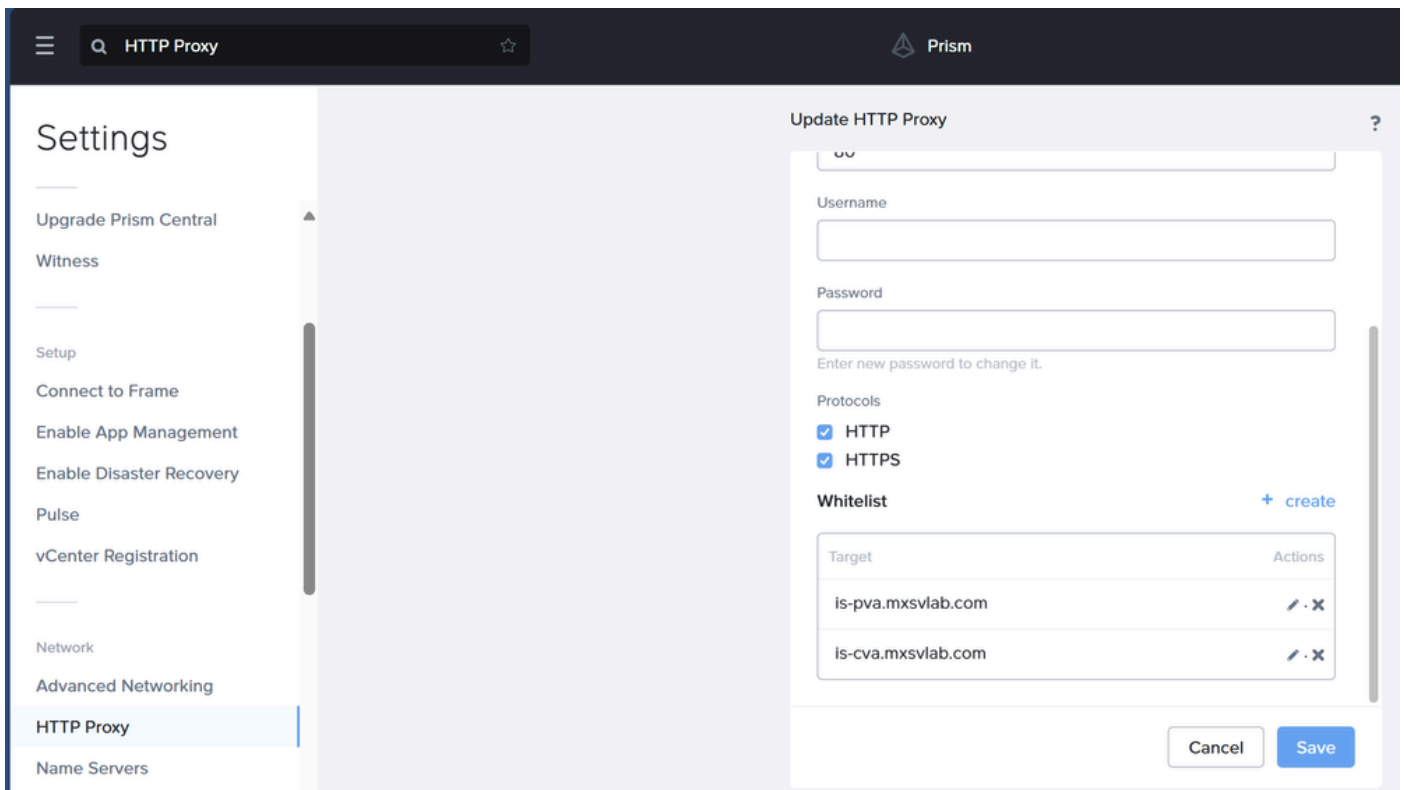




Nota: Una entrada de la lista blanca es un único host identificado por una dirección IP o una red identificada por la dirección de red y la máscara de subred. Agregar una entrada a la lista blanca significa "ignorar la configuración de proxy para esta dirección o red".

---

Para corregirlo en Prism Central, navegue hasta: Configuración > Red > Proxy HTTP > Haga clic en el icono del lápiz para editar > Lista blanca.



Proxy HTTP

Puede confirmar si estos pasos fueron exitosos probando la conectividad a Intersight CVA / PVA con un comando curl.

```
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
```

Ensayo de rizo

Comandos de red para probar la conectividad

Comando	Descripción
---------	-------------

<pre>curl -v -k https://&lt;Intersight URL&gt; curl -v -k https://svc.intersight.com</pre>	<p>Probar la conectividad hacia una URL necesaria de Intersight</p>
<pre>curl -v -k --proxy &lt;proxy address&gt;:&lt;port&gt; &lt;Intersight URL&gt; curl -v -k --proxy <a href="http://proxy.esl.cisco.com:8080">http://proxy.esl.cisco.com:8080</a> https://svc.intersight.com</pre>	<p>Pruebe la conectividad cuando se requiera proxy</p>
<pre>curl -4 6 -v -k https://&lt;Intersight URL&gt; curl -4 -v -k https://svc.intersight.com</pre>	<p>Especificar la prueba de conectividad para el direccionamiento IPV4 o IPV6</p>
<pre>tracert &lt;Intersight IP&gt; tracert 99.83.178.202</pre>	<p>Rastrea los paquetes hacia un host de destino</p>
<pre>nslookup &lt;URL&gt; nslookup svc.Intersight.com</pre>	<p>Determina la dirección IP asociada a una dirección específica</p>

### Los Detalles De Autenticación Proporcionados No Son Válidos

"Error al guardar los datos de autenticación del administrador de hardware: Los detalles de autenticación proporcionados no son válidos. Especifique una clave API y un secreto válidos."

The image shows a 'Connect Hardware Provider' dialog box with the following details:

- Region: North America
- URL: <https://us-east-1.intersight.com>
- Section: Connection Credentials
- Text: 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: 62ed7649
- Intersight Secret Key: -----BEGIN EC PRIVATE KEY-----  
HAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0waw
- Buttons: Cancel, Connect

An error message is displayed in the background:

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


Debe confirmar que no hay errores tipográficos ni caracteres que falten al escribir o pegar la clave secreta de intercepción; de lo contrario, no podrá establecer la conexión con el proveedor de hardware.

# View API Key

**i** 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  

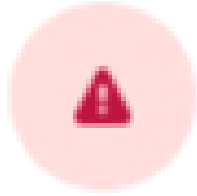
```
-----BEGIN EC PRIVATE KEY-----  
MIGHAgEAMBMGBByqGSM49AgEGCCqGSM49AwEHBG0waw
```

I have downloaded the Secret Key.

Close

No se puede obtener la lista de EULA

"No se pudo validar la conexión con los detalles de autenticación proporcionados: No se puede obtener la lista de EULA. Error con error: Su token ha caducado debido a la inactividad de los últimos 30 días."



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

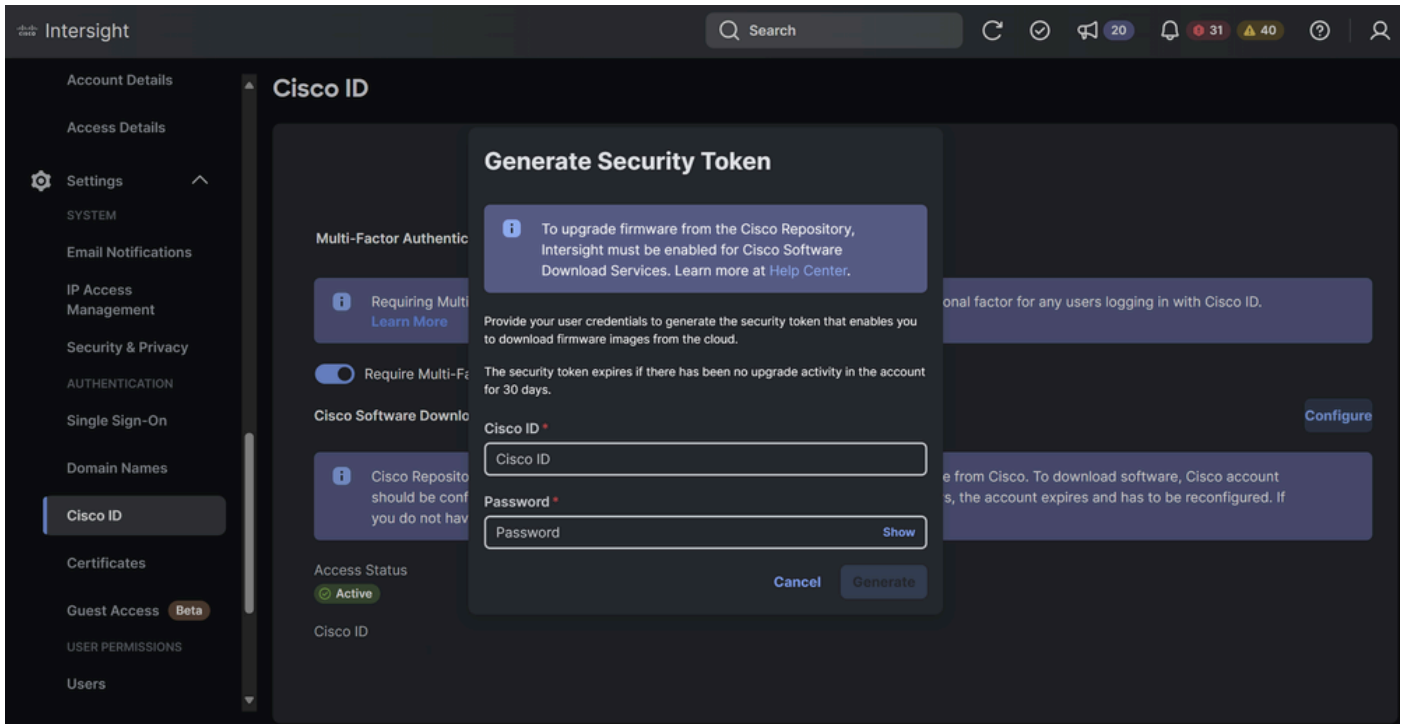
Durante la fase de Onboarding de los nodos, puede encontrar un error "Failed to connect to INTERSIGHT hardware manager with UUID" o "Your user credentials may have expired.". Esto aparece si hay un problema de cuenta de Intersight con respecto al CLUF.



Nota: A partir de hoy, se **REQUIERE** la aceptación del CLUF para ISM. Esto va a cambiar en el futuro, ya que ya no dependemos del CLUF para las descargas de firmware.

---

Para corregirlo en Intersight, vaya a: Settings > Cisco ID > Configure > Enter Cisco ID and Password .



## Información Relacionada

- [Organizaciones y funciones en Intersight](#)
- [Requisitos de puerto](#)
- [URL de terminales necesarias para reclamar los destinos](#)
- [Conceder acceso al repositorio de software de Cisco y aceptar EULA](#)



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).