

Solucionar problemas de conexão do Cisco HCI com o provedor de hardware Nutanix

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Troubleshooting](#)

[Prazo Final do Contexto Excedido](#)

[Resolução de Nome Apropriada de DNS](#)

[A VM do Prism Central não pode se conectar ao Intersight CVA/PVA](#)

[Comandos De Rede Para Testar A Conectividade](#)

[Os Detalhes De Autenticação Fornecidos São Inválidos](#)

[Não É Possível Buscar A Lista EULA](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como solucionar problemas de conexão do provedor de hardware do Nutanix Foundation Central ao Cisco Intersight.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos.

- Entendimento básico da conectividade de rede.
- Compreensão básica das chaves de API da Intersight.
- Conta Intersight com pelo menos privilégios de Administrador do Servidor.



E-mail

Sign out



Account and role

Change

Server Administrator

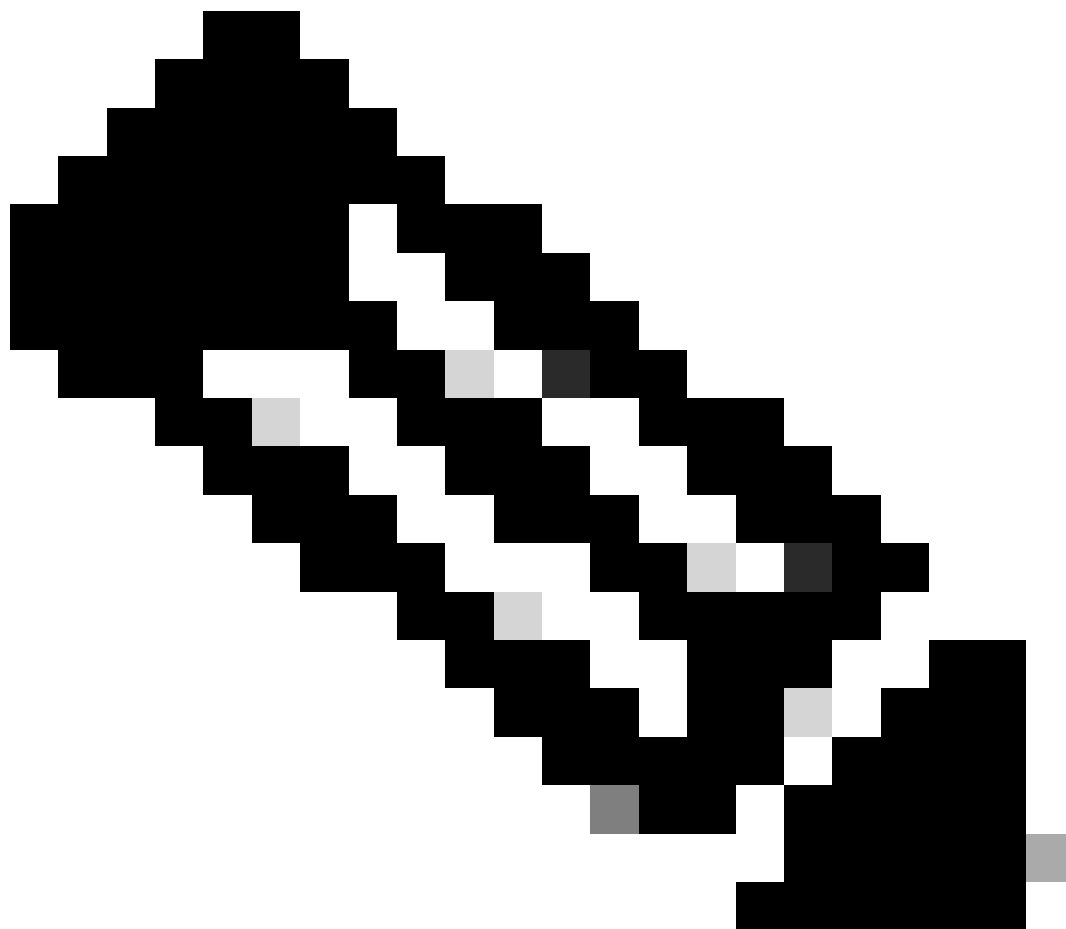


Region

intersight-aws-us-east-1

Access details

User settings



Note: A Intersight fornece RBAC (Role-Based Access Control, controle de acesso baseado em função) para autorizar ou restringir o acesso do sistema a um usuário, com base nas funções e privilégios do usuário. Uma função de usuário no Intersight representa uma coleção de privilégios que um usuário tem para executar um conjunto de operações e fornece acesso granular aos recursos. A Intersight fornece acesso baseado em funções a usuários individuais ou a um conjunto de usuários em Grupos.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

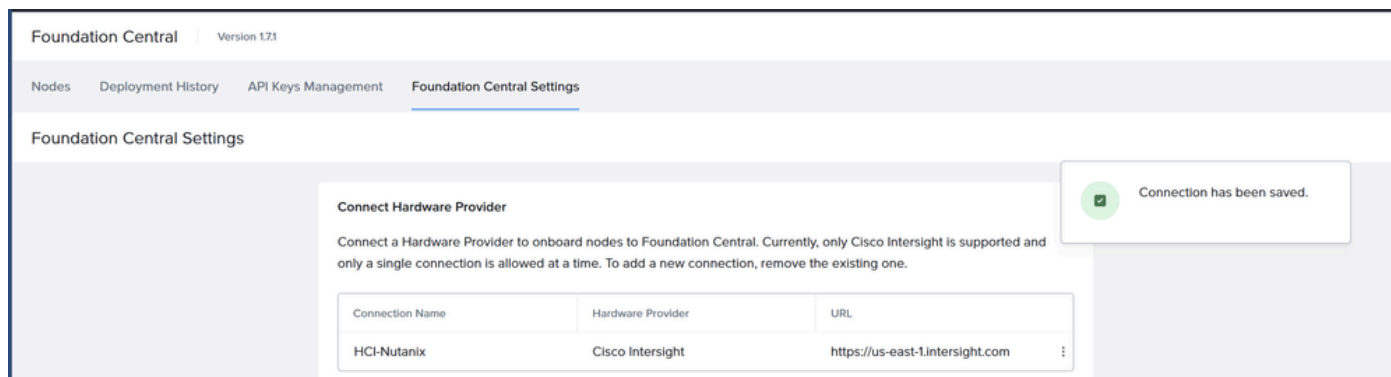
- Foundation Central 1.7.1 ou posterior.
- SAAS, CVA e PVA de Intersight.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

É necessário conectar o Foundation Central à Cisco Intersight como provedor de hardware para implantar a solução Cisco HCI com Nutanix no ISM do Modo Independente da Intersight ou no IMM do Modo Gerenciado da Intersight.



Modo independente da Intersight: os nós estão conectados a um par de switches de topo de rack (ToR) e os servidores são gerenciados centralmente com o Cisco Intersight®. Embora seja necessário um mínimo de três nós para implantar um cluster Nutanix padrão, também oferecemos uma opção para implantar um cluster de nó único e um cluster de dois nós para localizações de borda e filiais e situações que já tenham uma estrutura de rede de alto desempenho instalada.

Modo gerenciado da Intersight: o modo gerenciado da Intersight unifica os recursos dos sistemas UCS e a flexibilidade baseada em nuvem da Intersight, unificando assim a experiência de gerenciamento para os sistemas autônomos e conectados à Interconexão de estrutura. O Intersight Management Model padroniza o gerenciamento de políticas e operações para interconexões em malha UCS-FI-6454, UCS-FI-64108, UCS-FI-6536, UCSX-S9108-100G e servidores Cisco UCS C-Series (M5, M6, M7, M8) e Cisco UCS X-Series (M6, M7, M8).

Troubleshooting

Prazo Final do Contexto Excedido

"Falha ao validar a conexão com os detalhes de autenticação fornecidos: Falha ao buscar a chave de API: o prazo final do contexto foi excedido."

Connect Hardware Provider

Connection Details

Connection Name

Only the special characters - , _ are allowed

Hardware Provider

Intersight Deployment Type

☒ SaaS ☐ Connected/Private Virtual Appliance

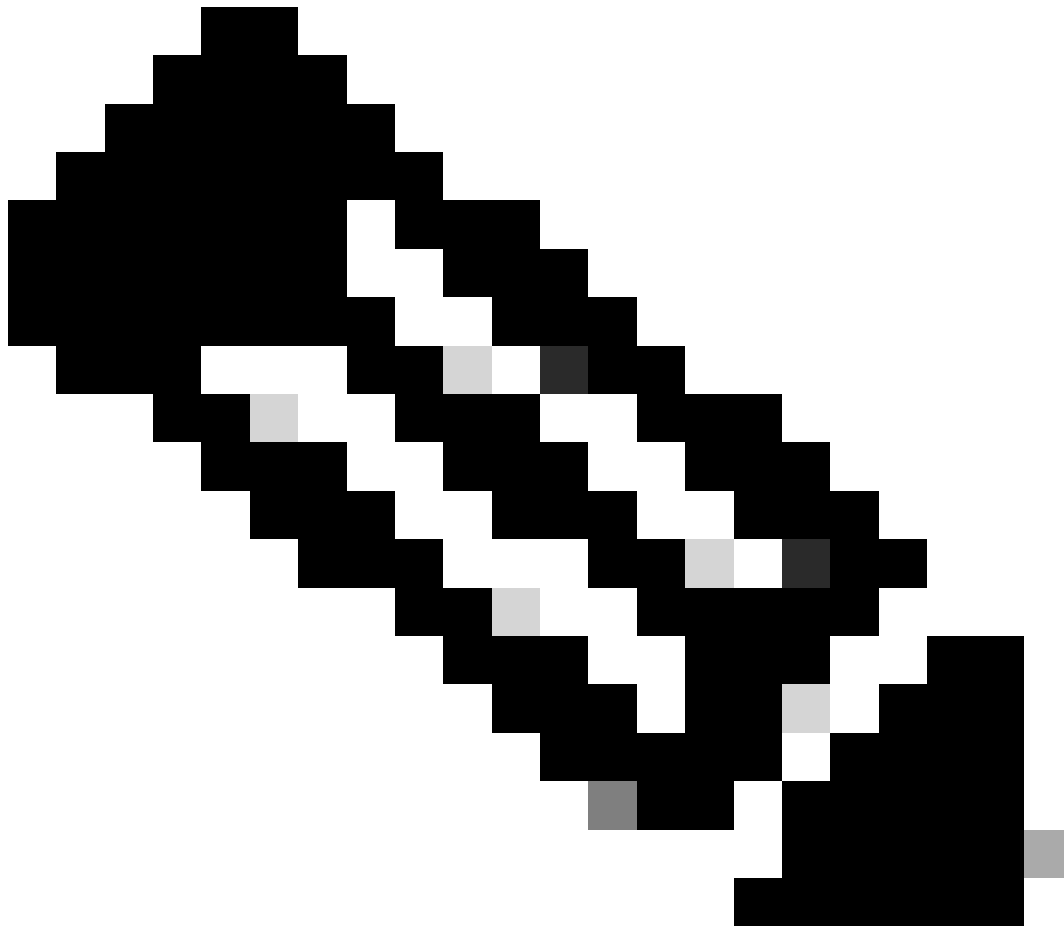
Intersight Region & URL

h connection and

Failed to validate connection with the given auth details:
Failed to fetch the API Key:
Get "https://us-east-1.intersight.com/api/v1/iam/Api"

Certifique-se de que você tenha a conectividade adequada do Prism Central e da Foundation Central para as próximas URLs através das portas 443 TCP/UDP e 80 TCP.

Região	URL	URLs exigidas pelos Conectores de Dispositivo
América do 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 (Europa, Oriente Médio e África)	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	



Note: A Cisco Intersight oferece suporte a duas regiões: a região existente da América do Norte (us-east-1) e a região da Europa, Oriente Médio e África (EMEA) (eu-central-1).

Para validar as informações anteriores, use SSH na Prism Central ou na Foundation Central VM e execute um comando curl para as URLs e portas mencionadas.

```
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/KJCRowj8o5BR/Q5w0Y4fxCLFL3ShwUNjehUjTf6EF0AY7AXD19WaiDlu; Expires=Tue, 16 Sep 2025 18:53:00 GMT; Path=/
< Set-Cookie: AWSALBCORS=W9cqyvSaX/07+KZ4058CopaQB1JlCo4TYocbNpCwsDBaDH/xquxQcaFXKe14m9SUn6/KJCRowj8o5BR/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:~$ █

```

Êxito no teste de conectividade de curva.

Se o comando curl falhar, verifique com sua equipe de firewall se os URLs e as portas estão permitidos no firewall ou na lista de acesso.

```

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:~$ █

```

Falha no teste de conectividade de curva.

Resolução de Nome Apropriada de DNS

Alguns firewalls ou listas de acesso exigem a adição do IP de resolução dos URLs mencionados. Ambos os URLs resolvem para esses endereços 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

Isso pode ser validado usando o 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

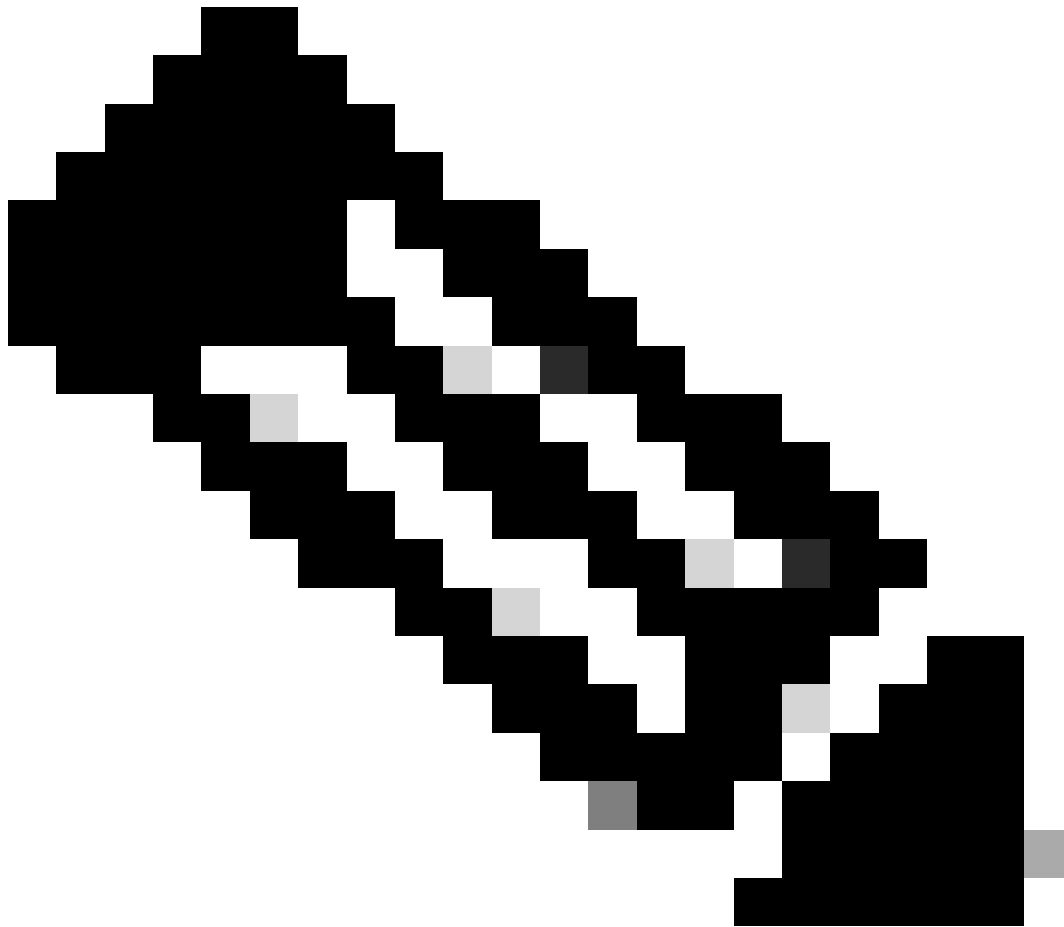
admin@NTNX-10-31-123-88-A-PCVM:~$ █
```

comando nslookup

A VM do Prism Central não pode se conectar ao Intersight CVA/PVA

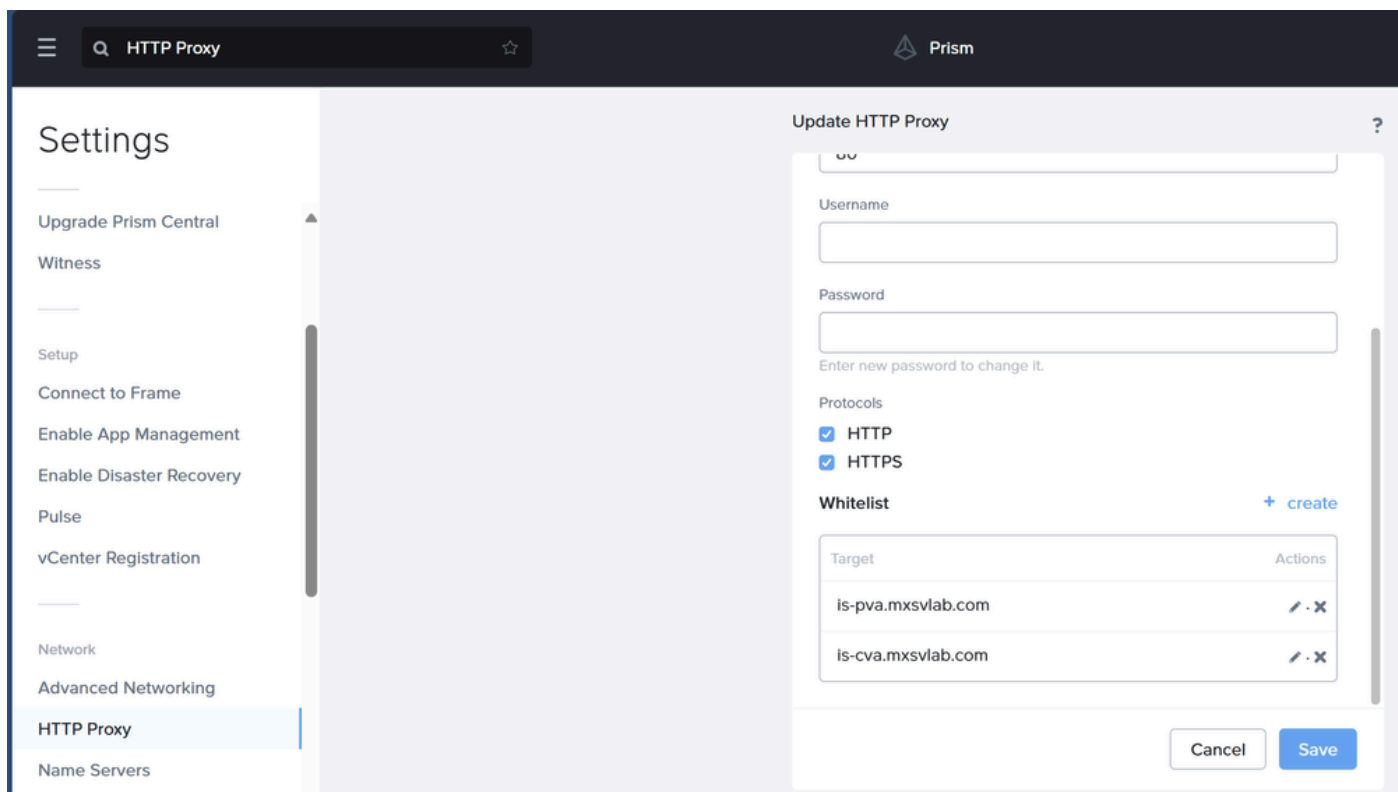
Quando houver uma conexão direta do Prism Central ao Intersight CVA/PVA, certifique-se de permitir a conexão na porta 443.

Se a VM do PC tiver um proxy configurado para se conectar à Internet para tarefas como downloads de software ou LCM, você precisará fazer uma lista branca do FQDN do Intersight CVA/PVA e do endereço IP nas configurações do Prism Central Proxy.



Note: Uma entrada da lista branca é um único host identificado pelo endereço IP ou uma rede identificada pelo endereço de rede e pela máscara de sub-rede. Adicionar uma entrada de lista branca significa "ignorar configurações de proxy para este endereço ou rede".

Para corrigir isso no Prism Central, navegue para: Configurações > Rede > Proxy HTTP > Clique no ícone do lápis para editar > Lista branca.



Proxy HTTP

Você pode confirmar se essas etapas foram bem-sucedidas testando a conectividade com o Intersight CVA/PVA com um 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
```

Ensaio de ondulação

Comandos De Rede Para Testar A Conectividade

Comando	Descrição
---------	-----------

<pre>curl -v -k https://<URL da Intersight> curl -v -k https://svc.intersight.com</pre>	Testar a conectividade para uma URL necessária para a Intersight
<pre>curl -v -k --proxy <endereço de proxy>:<porta> <URL da Intersight> curl -v -k --proxy http://proxy.esl.cisco.com:8080 https://svc.intersight.com</pre>	Testar a conectividade quando o proxy for necessário
<pre>curl -4 6 -v -k https://<URL da Intersight> curl -4 -v -k https://svc.intersight.com</pre>	Especificar teste de conectividade para endereçamento IPV4 ou IPV6
<pre>tracpath <Intersight IP> tracpath 99.83.178.202</pre>	Rastreia pacotes em direção a um host de destino
<pre>nslookup <URL> nslookup svc.Intersight.com</pre>	Determina o endereço IP associado ao endereço específico

Os Detalhes De Autenticação Fornecidos São Inválidos

"Falha ao salvar dados de autenticação do gerenciador de hardware: Os detalhes de autenticação fornecidos são inválidos. Forneça uma chave de API e um segredo válidos."

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

Você precisa confirmar que não há erros tipográficos ou caracteres ausentes ao digitar ou colar a chave secreta da Intersight, caso contrário, ela não estabelecerá a conexão com o provedor de hardware.

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

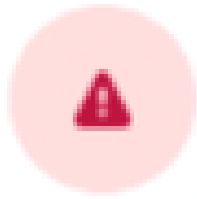
☐

I have downloaded the Secret Key.

Close

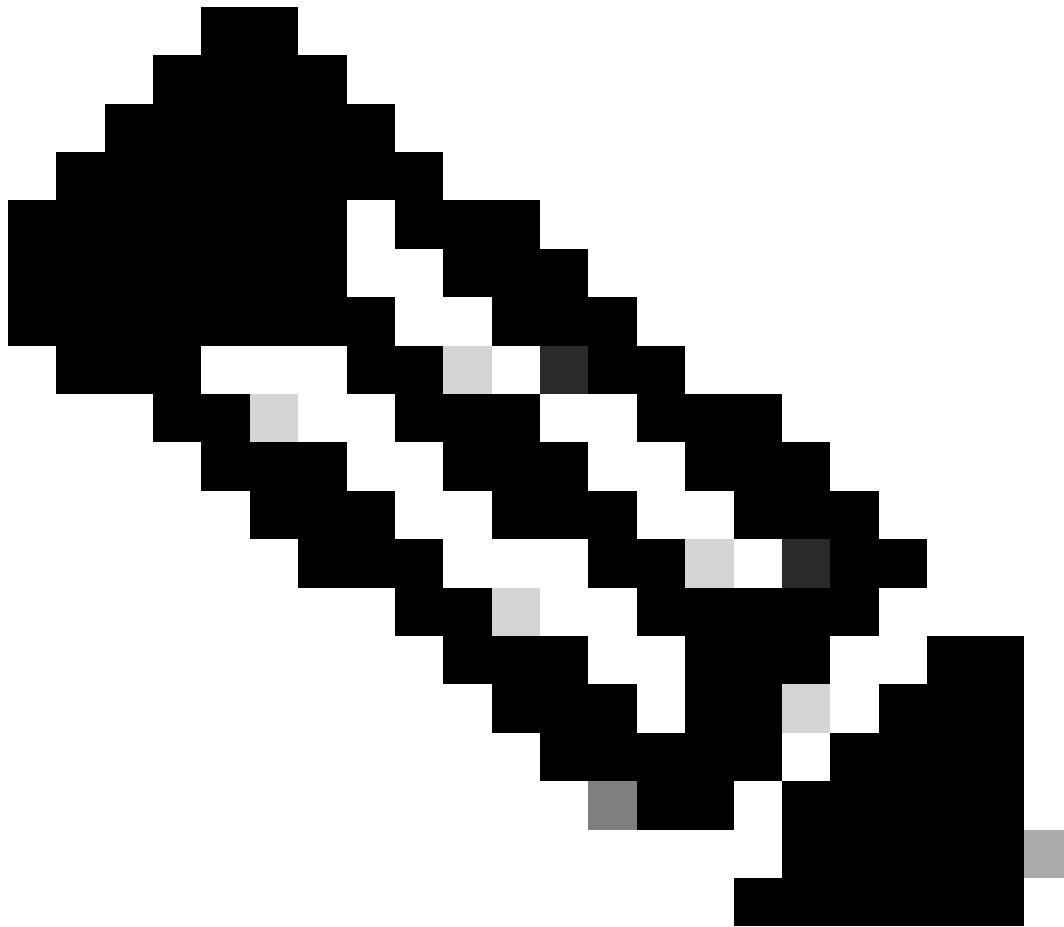
Não É Possível Buscar A Lista EULA

"Falha ao validar a conexão com os detalhes de autenticação fornecidos: Não é possível buscar a lista de EULA. Falha com erro: Seu token expirou devido à inatividade nos últimos 30 dias."



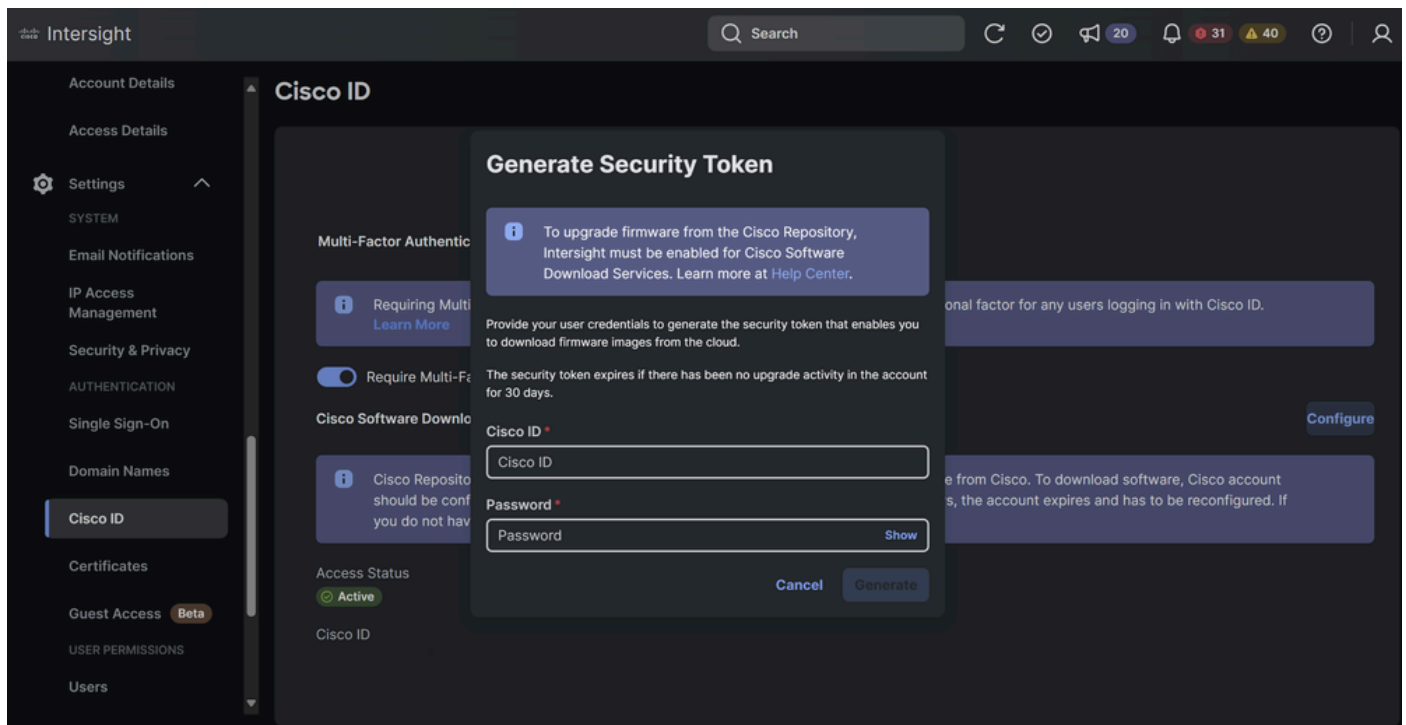
Failed to validate connection
with the given auth details:
Unable to fetch the EULA list.
Failed with error: Your token has
expired due to inactivity in the
last 30 days. Provide your Cisco

Durante a fase de Onboarding do nó, você pode encontrar um erro "Falha ao conectar ao gerenciador de hardware INTERSIGHT com UUID" ou "Suas credenciais de usuário podem ter expirado.". Isso será exibido se houver um problema na conta da Intersight com relação ao EULA.



Note: A partir de hoje, a aceitação do EULA é OBRIGATÓRIA para o ISM. Isso mudará no futuro, já que não dependemos mais do EULA para downloads de firmware.

Para corrigir isso no Intersight Navegue para: Settings > Cisco ID > Configure > Enter Cisco ID and Password.



Informações Relacionadas

- [Organizações e funções na Intersight](#)
- [Requisitos de porta](#)
- [URLs de endpoint necessárias para reivindicar destinos](#)
- [Conceder acesso ao repositório de software da Cisco e aceitar o EULA](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.