# Risoluzione dei problemi di connessione di Cisco HCI con Nutanix Hardware Provider

## Sommario



## Introduzione

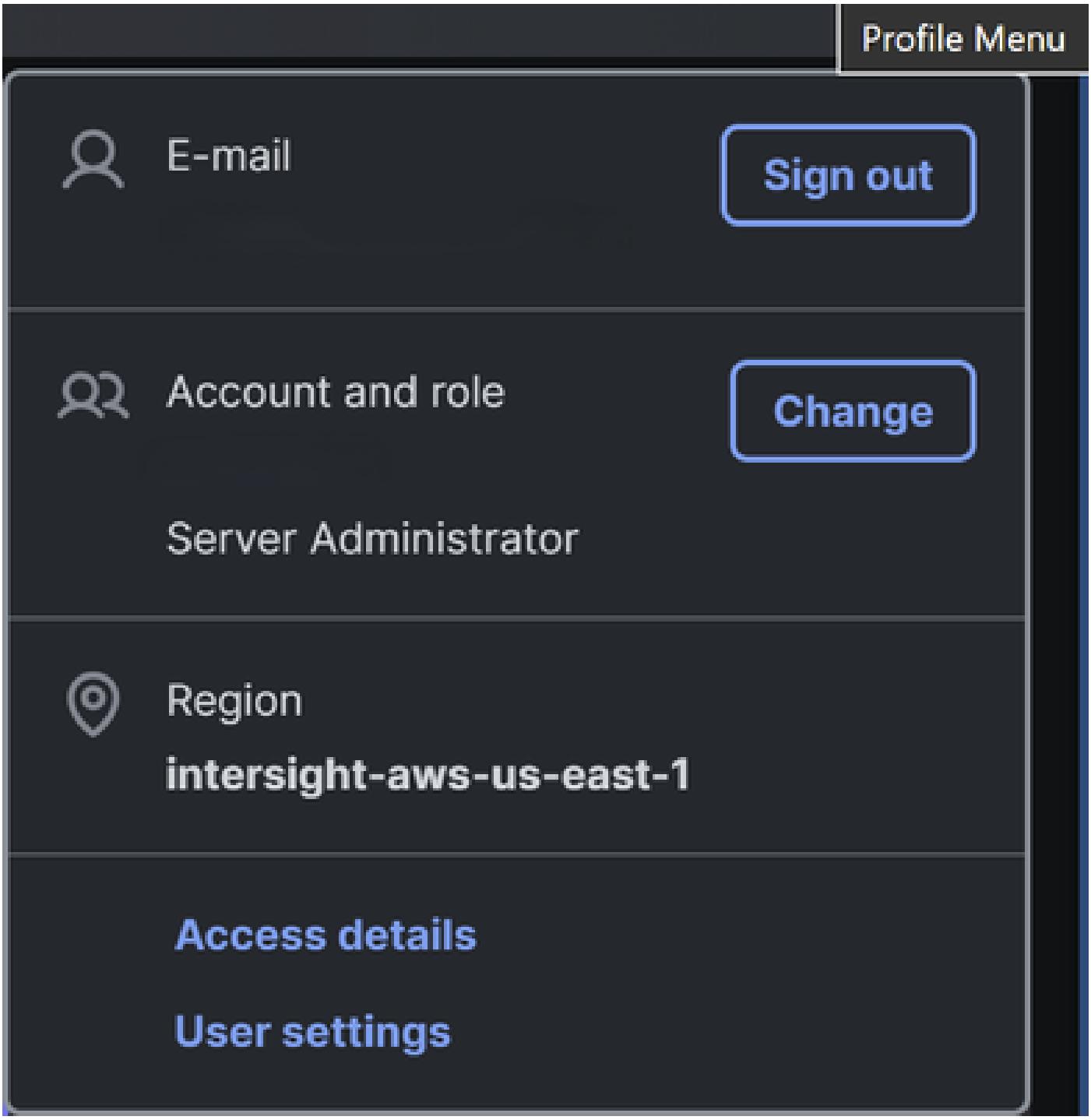
In questo documento viene descritto come risolvere i problemi di connessione dei provider hardware da Nutanix Foundation Central a Cisco Intersight.

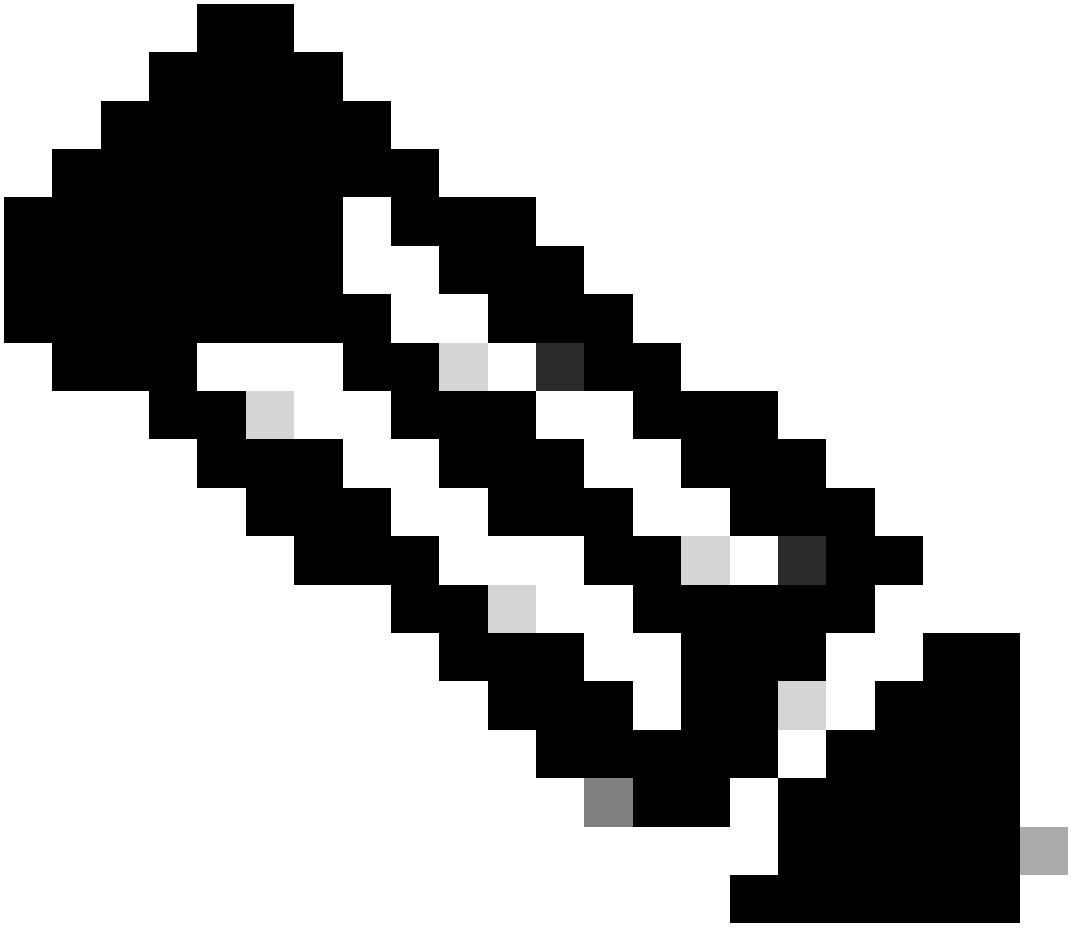
## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti.

- Conoscenze base della connettività di rete.
- Conoscenza di base delle chiavi API di Intersight.
- Account Intersight con almeno privilegi di amministratore del server.


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



Nota: Intersight fornisce il controllo di accesso basato sui ruoli (RBAC) per autorizzare o limitare l'accesso di sistema a un utente, in base ai ruoli e ai privilegi dell'utente. Un ruolo utente in Intersight rappresenta un insieme di privilegi di cui dispone un utente per eseguire un insieme di operazioni e fornisce accesso granulare alle risorse. Intersight fornisce l'accesso basato sui ruoli a singoli utenti o a un insieme di utenti in Gruppi.

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

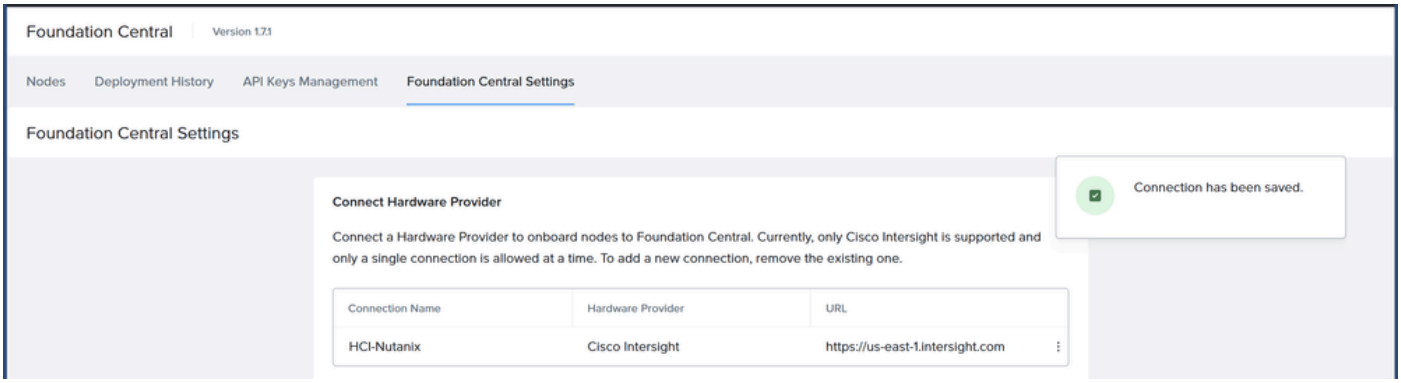
- Foundation Central 1.7.1 o versione successiva.
- Intersight SAAS, CVA e PVA.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

# Premesse

È necessario connettere Foundation Central a Cisco Intersight in qualità di provider hardware per implementare la soluzione Cisco HCI con Nutanix in modalità standalone Intersight ISM o in modalità gestita Intersight IMM.



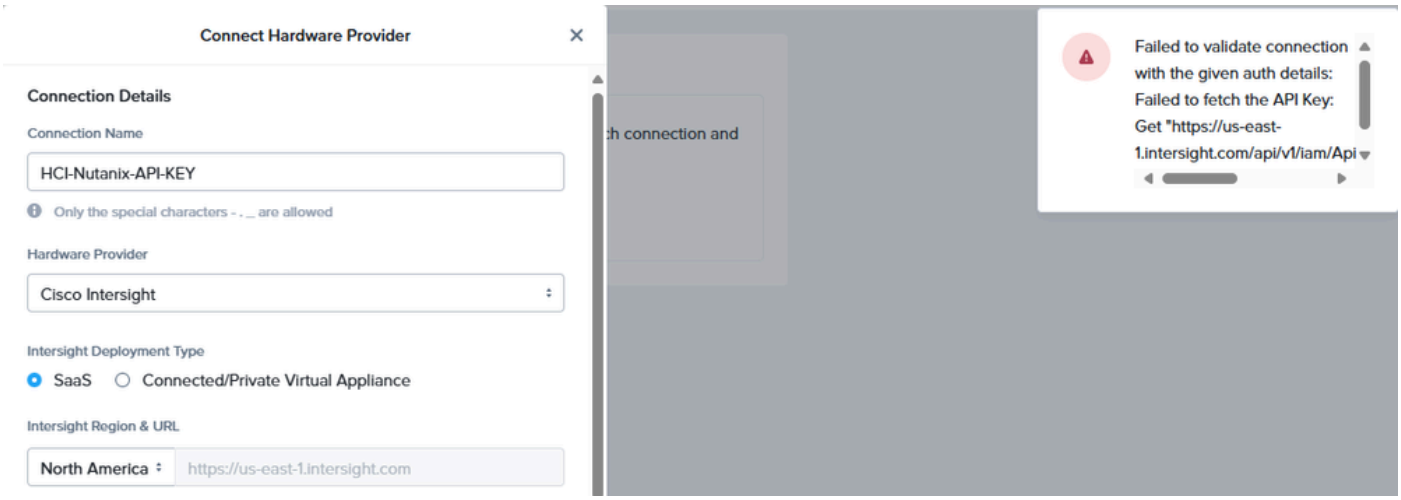

Modalità Intersight Standalone: i nodi sono connessi a una coppia di switch Top-of-Rack (ToR) e i server sono gestiti centralmente tramite Cisco Intersight®. Per l'installazione di un cluster Nutanix standard sono necessari almeno tre nodi, ma è anche disponibile un'opzione per l'installazione di un cluster a nodo singolo e un cluster a due nodi per le postazioni Edge e Branch e le situazioni in cui è già installato un fabric di rete ad alte prestazioni.

Modalità Intersight Managed: la modalità Intersight Managed unifica le funzionalità dei sistemi UCS e la flessibilità basata su cloud di Intersight, unificando così l'esperienza di gestione per i sistemi standalone e Fabric Interconnect. Intersight Management Model standardizza la gestione delle policy e delle operazioni per i server UCS-FI-6454, UCS-FI-64108, UCS-FI-6536, UCS-S9108-100G Fabric Interconnect e Cisco UCS serie C (M5, M6, M7, M8) e Cisco UCS serie X (M6, M7, M8).

# Risoluzione dei problemi

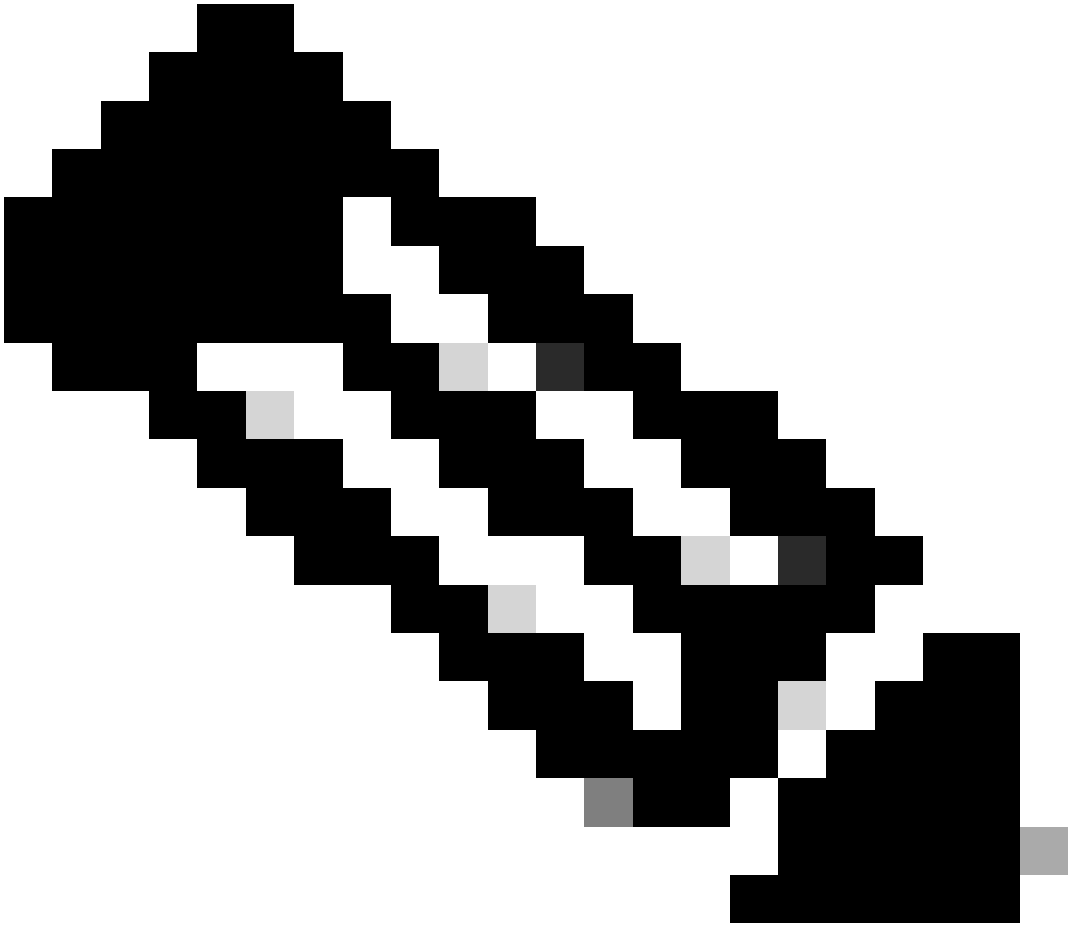
## Scadenza contesto superata

"Impossibile convalidare la connessione con i dettagli di autenticazione specificati: Impossibile recuperare la chiave API: scadenza del contesto superata."




Accertarsi di disporre della corretta connettività da Prisma Central e Foundation Central ai successivi URL attraverso le porte 443 TCP/UDP e 80 TCP.

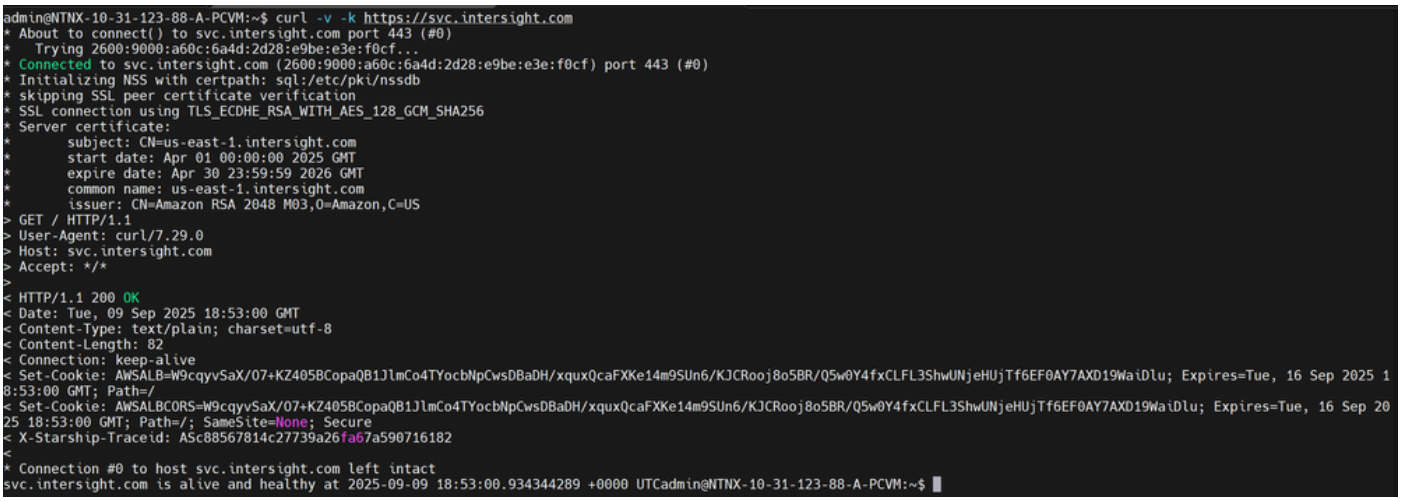
| Regione | URL | URL richiesti dai connettori di dispositivo |
|---|---|---|
| Nord America | intersight.com<br>us-east-1.intersight.com<br>Ip:<br>52.223.48.112<br>99.83.178.202 | svc.intersight.com<br>svc.us-east-1.intersight.com<br>svc-static1.intersight.com<br>ucs-starship.com*<br>ucs-connect.com* |
| EMEA | Intersight.com<br>eu-central-1.intersight.com<br>Ip:<br>52.223.57.109<br>99.83.140.236 | svc.eu-central-1.intersight.com<br>svc-static1.eu-central-1.intersight.com |



Nota: Cisco Intersight supporta due aree: la regione esistente del Nord America (us-east-1) e la regione Europa, Medio Oriente e Africa (EMEA) (eu-central-1).

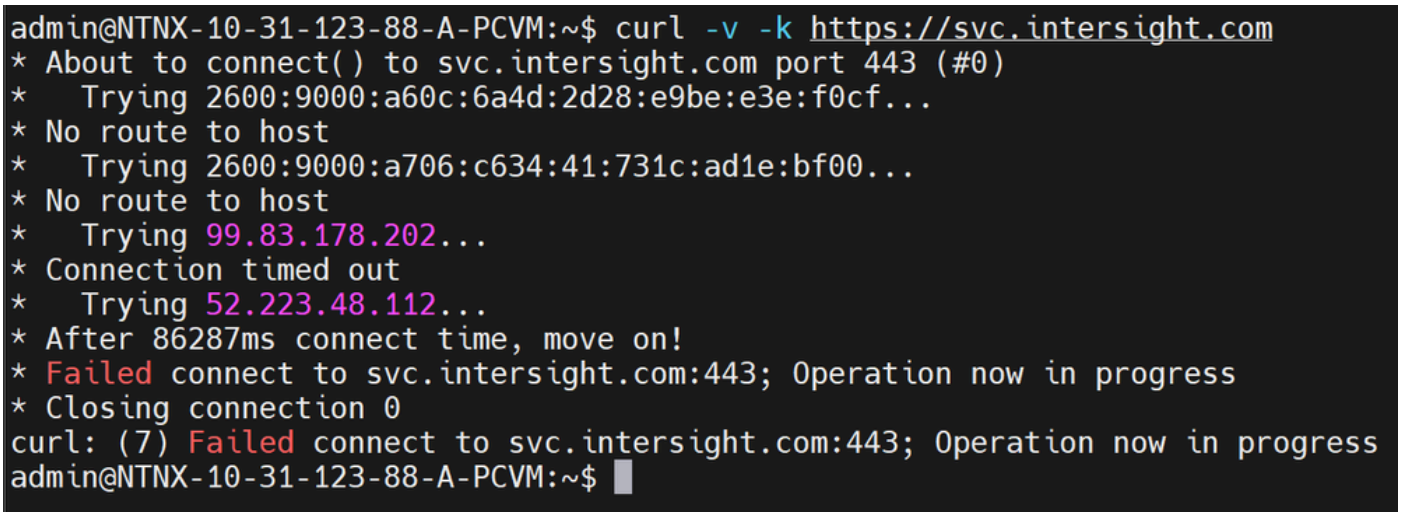
Per convalidare le informazioni precedenti, SSH nella VM Prisma Central o Foundation Central ed eseguire un comando curl sugli URL e sulle porte menzionati.

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




Test di connettività URL riuscito.

Se il comando curl ha esito negativo, verificare con il team del firewall che gli URL e le porte siano consentiti nel firewall o nell'elenco degli accessi.




Test di connettività dell'URL non riuscito.

## Risoluzione dei nomi DNS corretta

Per alcuni firewall o elenchi degli accessi è necessario aggiungere l'indirizzo IP di risoluzione dagli URL indicati. Entrambi questi URL vengono risolti nei seguenti indirizzi 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

È possibile convalidare questa condizione utilizzando il comando nslookup.

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

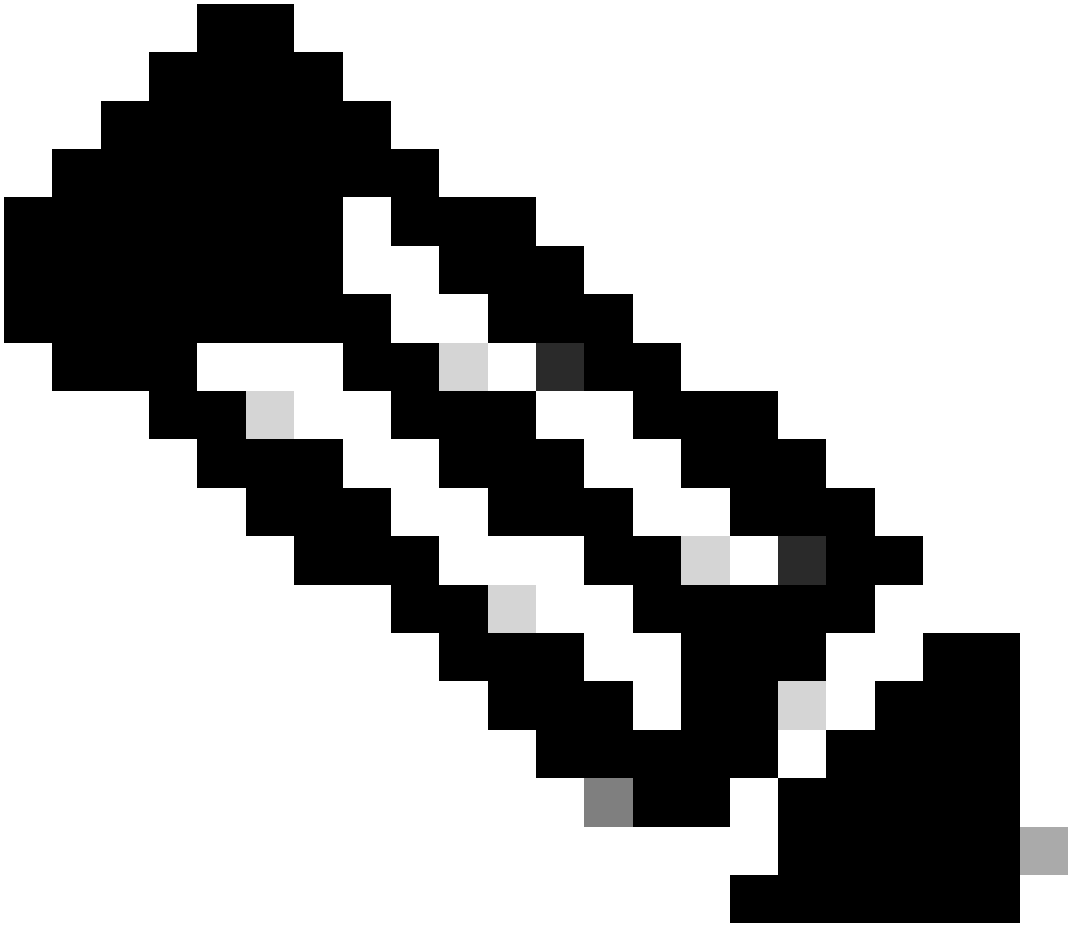
```
admin@NTNX-10-31-123-88-A-PCVM:~$ nslookup svc.intersight.com
Server:         10.31.123.60
Address:        10.31.123.60#53

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

## Prisma Central VM non può collegarsi a Intersight CVA/PVA

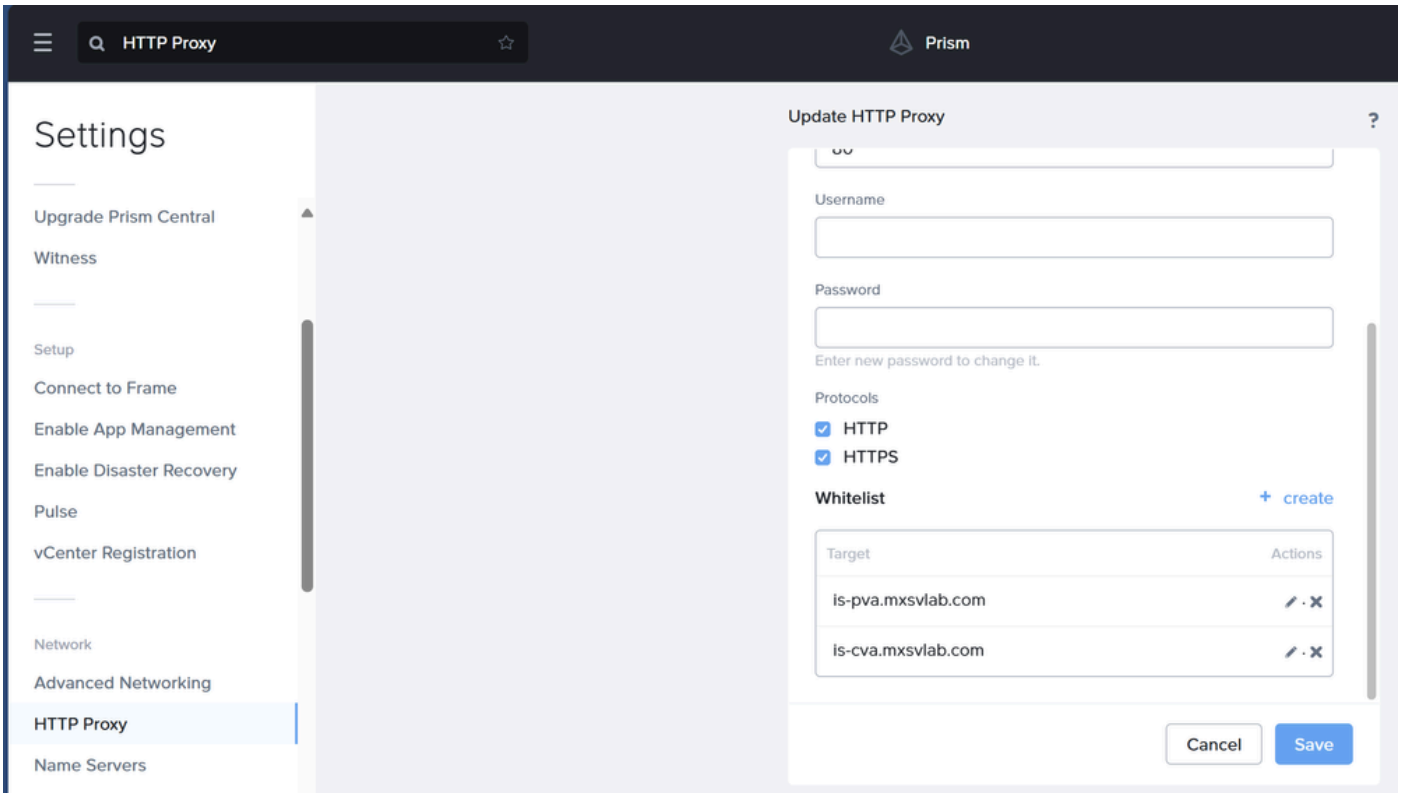
Quando c'è una connessione diretta da Prism Central a Intersight CVA / PVA assicurarsi di consentire la connessione sulla porta 443.

Se PC VM dispone di un proxy configurato per la connessione a Internet per attività quali download di software o LCM, è necessario inserire un elenco di nomi di dominio completi (FQDN) di Intersight CVA/PVA e l'indirizzo IP nelle impostazioni proxy di Prisma Central.



Nota: Una voce della lista bianca è un singolo host identificato dall'indirizzo IP o da una rete identificata dall'indirizzo di rete e dalla subnet mask. L'aggiunta di una voce nella lista bianca significa "ignorare le impostazioni proxy per questo indirizzo o questa rete".

Per risolvere questo problema in Prisma Central passare a: Impostazioni > Rete > Proxy HTTP > Fare clic sull'icona a forma di matita per modificare >Whitelist.




Proxy HTTP

Per verificare il corretto completamento di questi passaggi, provare la connettività 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           :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
```

Prova dei riccioli

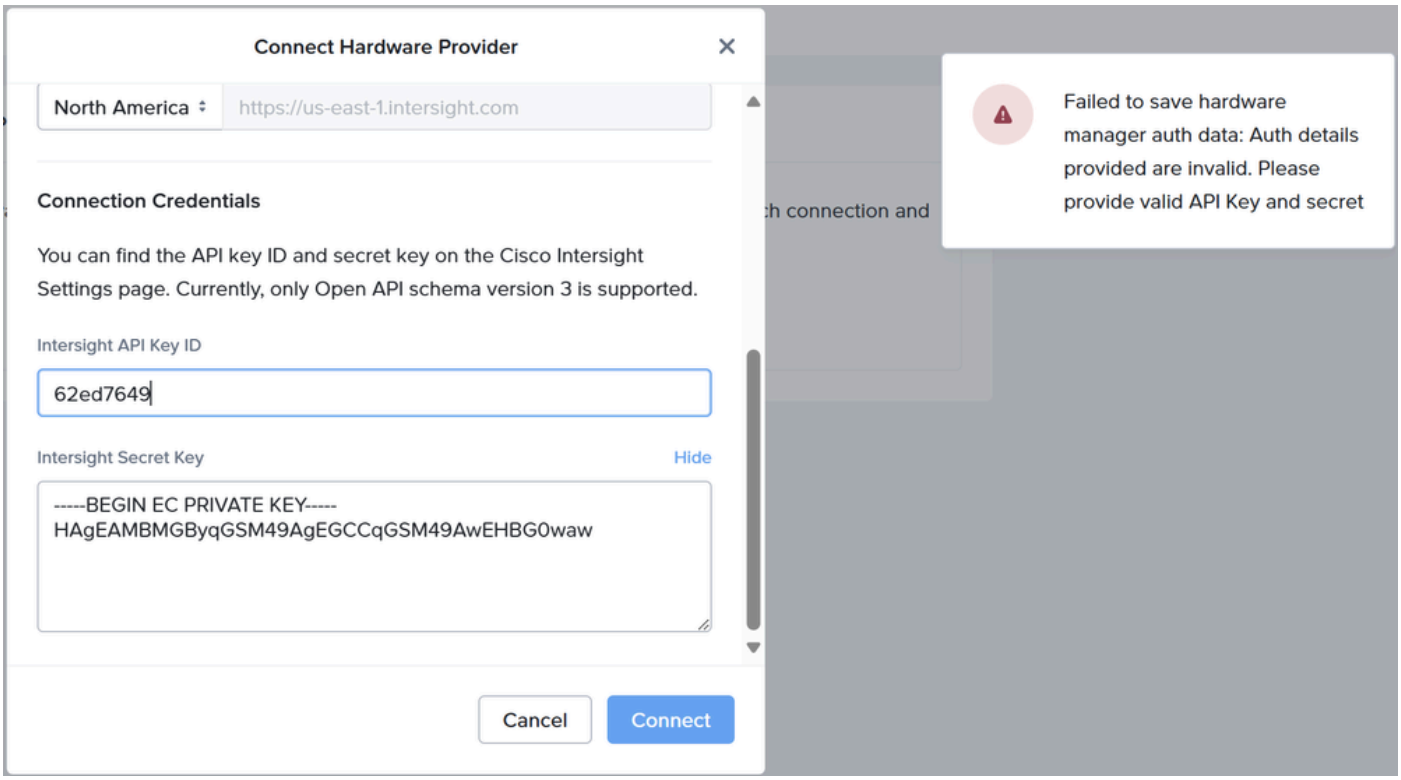
## Comandi Di Rete Per Verificare La Connettività

| Comando | Descrizione |
| --- | --- |

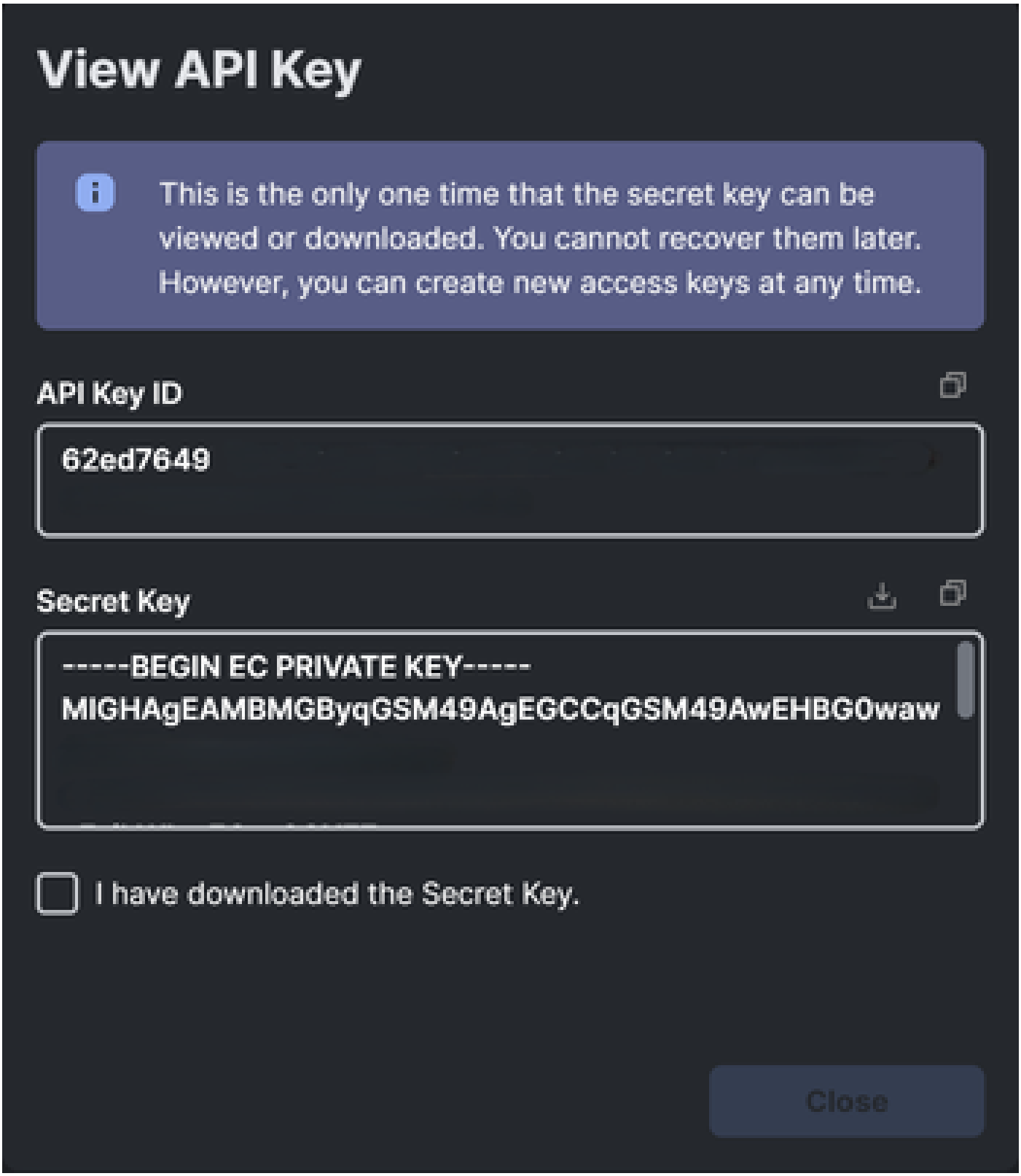
| | |
|---|---|
| curl -v -k https://<URL di Intersight><br><br>curl -v -k https://svc.intersight.com | Verifica della connettività verso un URL richiesto da Intersight |
| curl -v -k —proxy <indirizzo proxy>:<porta> <URL di Intersight><br><br>curl -v -k —proxy http://proxy.esl.cisco.com:8080 https://svc.intersight.com | Verifica della connettività quando è richiesto il proxy |
| curl -4\|6 -v -k https://<URL di Intersight><br><br>curl -4 -v -k https://svc.intersight.com | Specificare il test di connettività per l'indirizzamento IPV4 o IPV6 |
| tracepath <Intersight IP><br><br>tracepath 99.83.178.202 | Traccia i pacchetti verso un host di destinazione |
| nslookup <URL><br><br>nslookup svc.Intersight.com | Determina l'indirizzo IP associato all'indirizzo specifico |

I Dettagli Di Autenticazione Forniti Non Sono Validi

"Impossibile salvare i dati di autenticazione di Gestione hardware: I dettagli di autenticazione specificati non sono validi. Fornire una chiave API e un segreto validi."

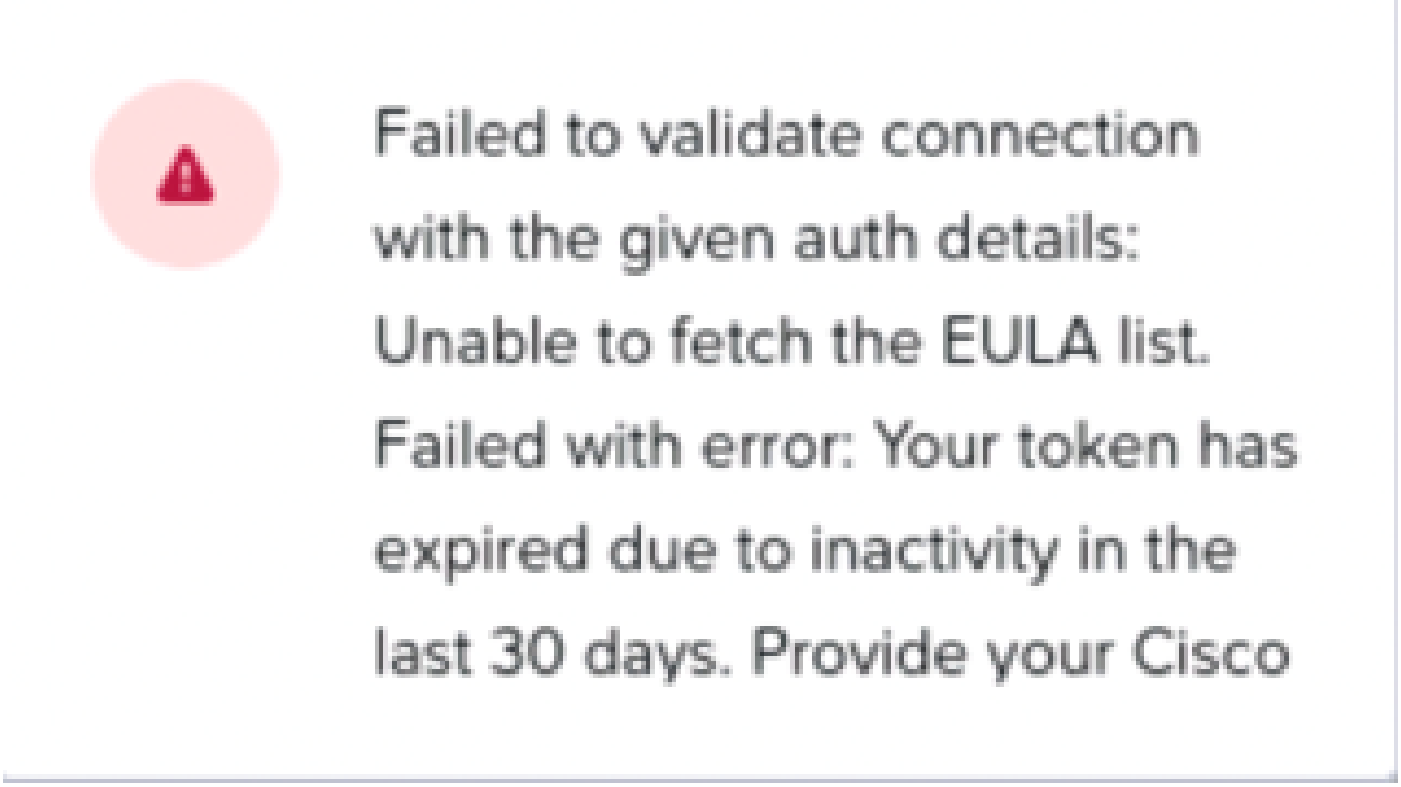



È necessario verificare che non vi siano errori tipografici o caratteri mancanti durante la digitazione o l'incollamento della chiave privata di Intersight, altrimenti non riesce a stabilire la connessione al provider hardware.

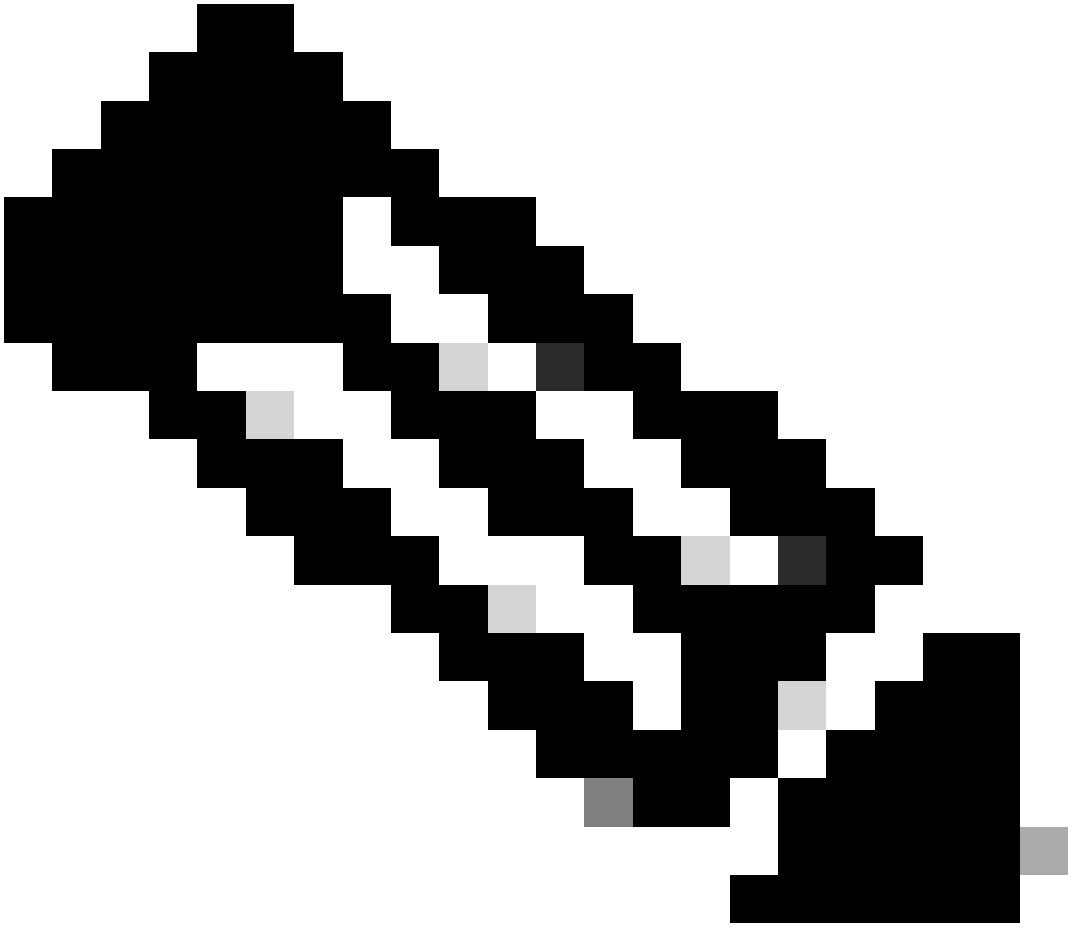



Impossibile Recuperare L'Elenco EULA

"Impossibile convalidare la connessione con i dettagli di autenticazione specificati: Impossibile recuperare l'elenco EULA. Operazione non riuscita con errore: Il token è scaduto a causa di inattività negli ultimi 30 giorni."

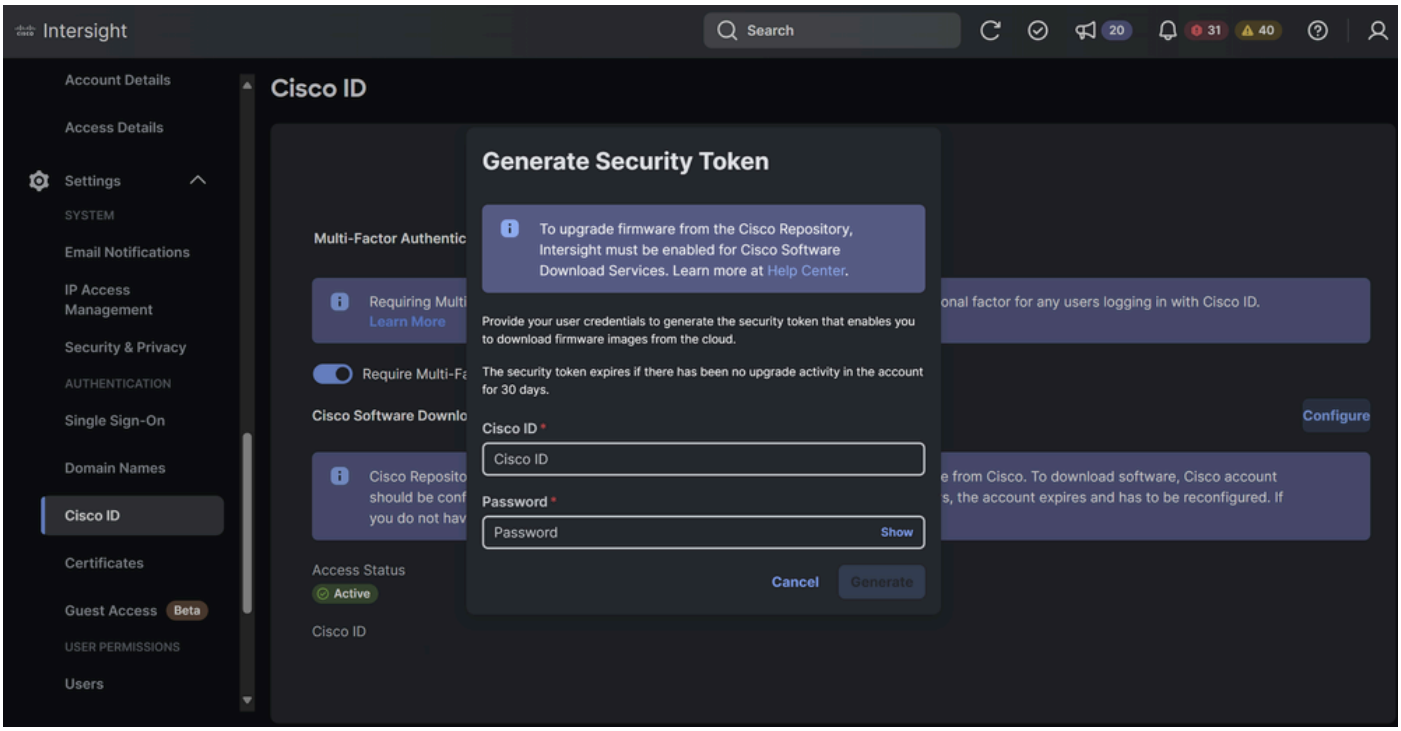



Durante la fase di caricamento dei nodi, è possibile che si verifichi un errore "Impossibile connettersi a INTERSIGHT hardware manager con UUID" o "Le credenziali utente potrebbero essere scadute". Questo messaggio viene visualizzato in caso di problemi relativi al conto Intersight in relazione al contratto di licenza.



Nota: Da oggi, per ISM è RICHIESTA l'accettazione dell'EULA. Questa situazione cambierà in futuro poiché non ci basiamo più sull'EULA per i download del firmware.

Per risolvere questo problema in Intersight, selezionare: Settings > Cisco ID > Configure > Enter Cisco ID and Password (Impostazioni > ID Cisco > Configura > Inserisci ID e password Cisco).




# Informazioni correlate

- Organizzazioni e ruoli in Intersight
- Requisiti delle porte
- URL endpoint necessari per le destinazioni attestazione
- Concessione dell'accesso al repository del software Cisco e accettazione del contratto di licenza

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).