

Nexus als Standalone-Lösung für Intersight-Verbindungen konfigurieren und beanspruchen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Vorteile der Netzwerkanbindung](#)

[QuickStart-Video](#)

[Manuelles Anfordern eines NXOS-Geräts](#)

[Verbindungsüberprüfung](#)

[TLS-Verifizierung mit OpenSSL Client](#)

[HTTPS-Erreichbarkeitsüberprüfung](#)

[Konfigurieren](#)

[Fordern Sie das Gerät an withinintersight.com](#)

[Auf dem Nexus-Gerät](#)

[Auf Interview-Portal](#)

[Claim One to Many Standalone Nexus Devices within intersight.com using Ansible@](#)

[Nexus NXAPI konfigurieren \(nur bei Verwendung von ansible.netcommon.httpapi\)](#)

[API-Schlüssel für Intersight generieren](#)

[Beispiel: Ansibleinventory.yaml](#)

[Beispiel:playbook.yamlExecution](#)

[Überprüfung](#)

[Auf dem Nexus-Switch](#)

[Versionen vor 10.3\(4a\)M](#)

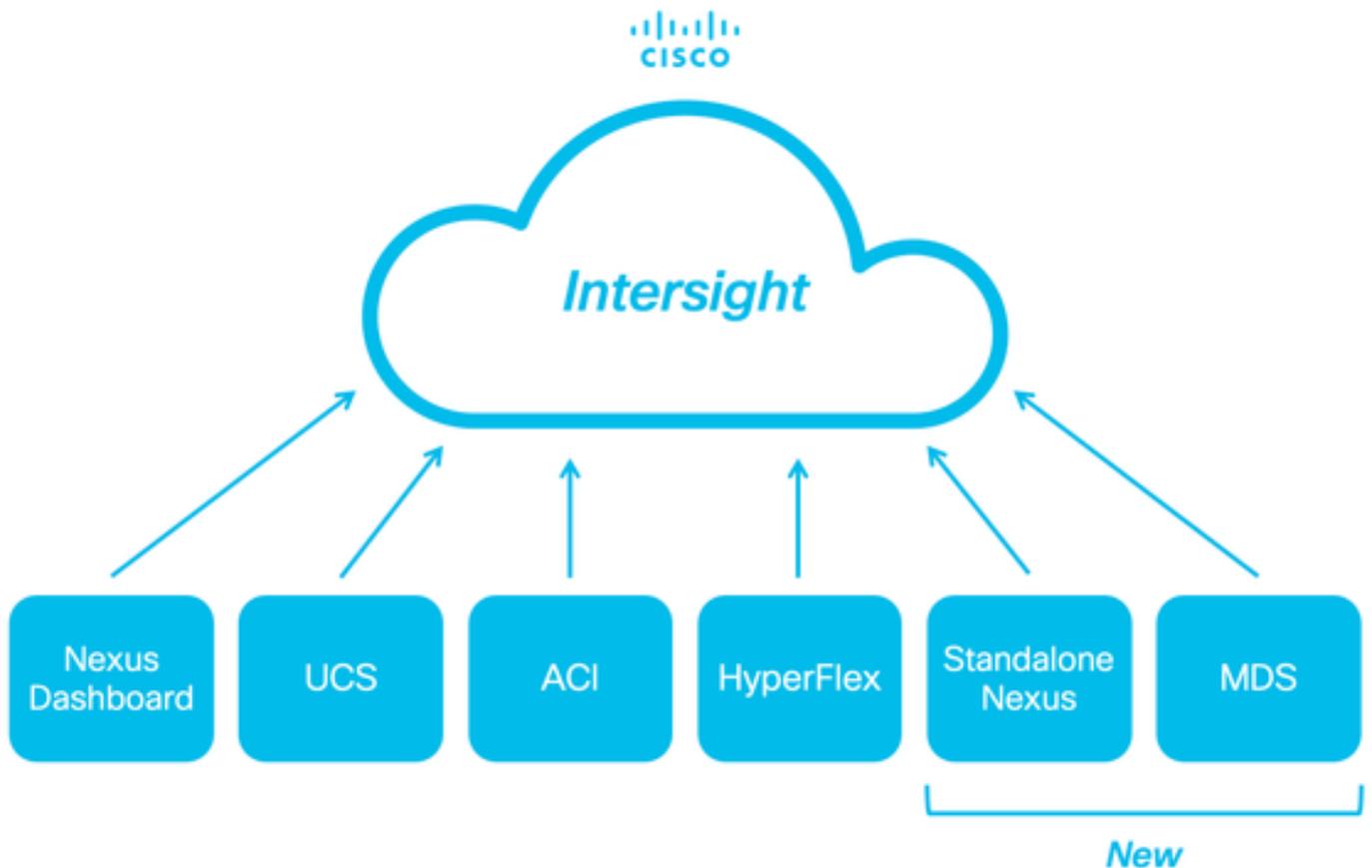
[Releases, die mit 10.3\(4a\)M beginnen](#)

[Ansible](#)

[Geräteanschluss deaktivieren](#)

Einleitung

In diesem Dokument werden die erforderlichen Schritte beschrieben, um eigenständige Nexus Switches zu aktivieren und in Intersight für erweiterten Cisco TAC-Support anzufordern.



Voraussetzungen

Sie müssen über ein Konto bei [Intersight.com](https://intersight.com) verfügen, es ist keine Lizenz für die Beantragung von Cisco NX-OS® erforderlich. Wenn ein neues Intersight-Konto erstellt werden muss, finden Sie weitere Informationen unter [Kontoerstellung](#).

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

Für den Standalone-Nexus-Switch gelten für NXDC folgende Richtlinien und Einschränkungen:

- Cisco NX-OS muss Version 10.2(3)F oder höher ausführen.
- [DNS](#) muss unter der richtigen VRF-Instanz (Virtual Routing and Forwarding) konfiguriert werden
- svc.intersight.com muss aufgelöst werden und ausgehende, initiierte HTTPS-Verbindungen auf Port 443 zulassen. Dies kann mit openssl und curl überprüft werden. ICMP-Anfragen (Internet Control Message Protocol) werden ignoriert.
- Wenn ein Proxy für eine HTTPS-Verbindung mit erforderlich ist, svc.intersight.com kann der Proxy in der Nexus Switch Device Connector (NXDC)-Konfiguration konfiguriert werden. Weitere Informationen zur Proxy-Konfiguration finden Sie unter [Konfigurieren von NXDC](#).

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Nexus N9K-C93240YC-FX2
- Cisco NX-OS 10.3(4a)M

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco Intersight ist eine Plattform für den Cloud-Betrieb, die aus optionalen, modularen Funktionen für erweiterte Infrastruktur, Workload-Optimierung und Kubernetes-Services besteht. Weitere Informationen finden Sie unter [Intersight Overview](#).

Die Geräte werden über einen NXDC, der in das Cisco NX-OS-Image jedes Systems eingebettet ist, mit dem Intersight-Portal verbunden. Ab der Cisco NX-OS-Version 10.2(3)F wird die Device Connector-Funktion unterstützt, mit der angeschlossene Geräte über eine sichere Internetverbindung Informationen senden und Steuerungsanweisungen vom Cisco Intersight-Portal erhalten können.

Vorteile der Netzwerkanbindung

Intersight-Verbindungen bieten die folgenden Funktionen und Vorteile für Cisco NX-OS-basierte Plattformen:

- Automatisierte Erfassung show tech-support details über [schnelle Problemlösung \(RPR für offene TAC Service Requests\)](#)
- On-Demand-Remote-Erfassung von show tech-support details
- Zukünftige Funktionen:
 - Eröffnung proaktiver TAC SRs bei Telemetrie- oder Hardwarefehlern
 - Remote-Erfassung einzelner Show-Befehle und mehr auf Anfrage

QuickStart-Video

Manuelles Anfordern eines NXOS-Geräts

Verbindungsüberprüfung



Hinweis: Ping-Antworten werden unterdrückt (ICMP-Pakete werden verworfen).

Zur Überprüfung der TLS- (Transport Layer Security) und HTTPS-Verbindungen wird empfohlen, Bash zu aktivieren, opensslBefehle auszuführen und curl in der gewünschten VRF-Instanz (ip netns exec <VRF>) zu verwenden.

! Enable bash

```
config terminal ; feature bash ; end
```

! Verify TLS

```
run bash ip netns exec management openssl s_client -connect svc.intersight.com:443
```

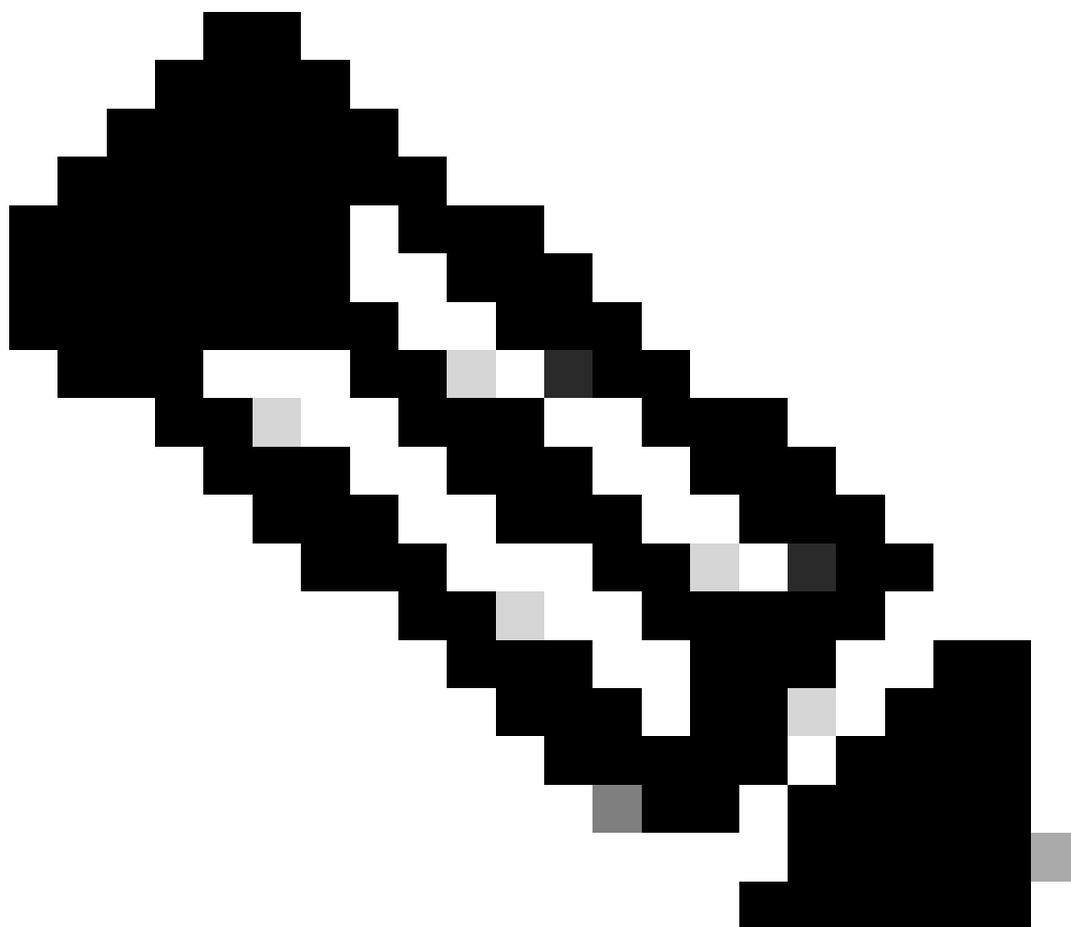
! Verify https

```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443
```

```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443 --proxy [protocol://]host[:port]
```

TLS-Verifizierung mit OpenSSL Client

Mit OpenSSL können Sie die TLS-Verbindung zu überprüfen svc.intersight.com:443. Wenn der Vorgang erfolgreich war, rufen Sie das öffentlich signierte Zertifikat vom Server ab, und zeigen Sie die Zertifikatskette an.

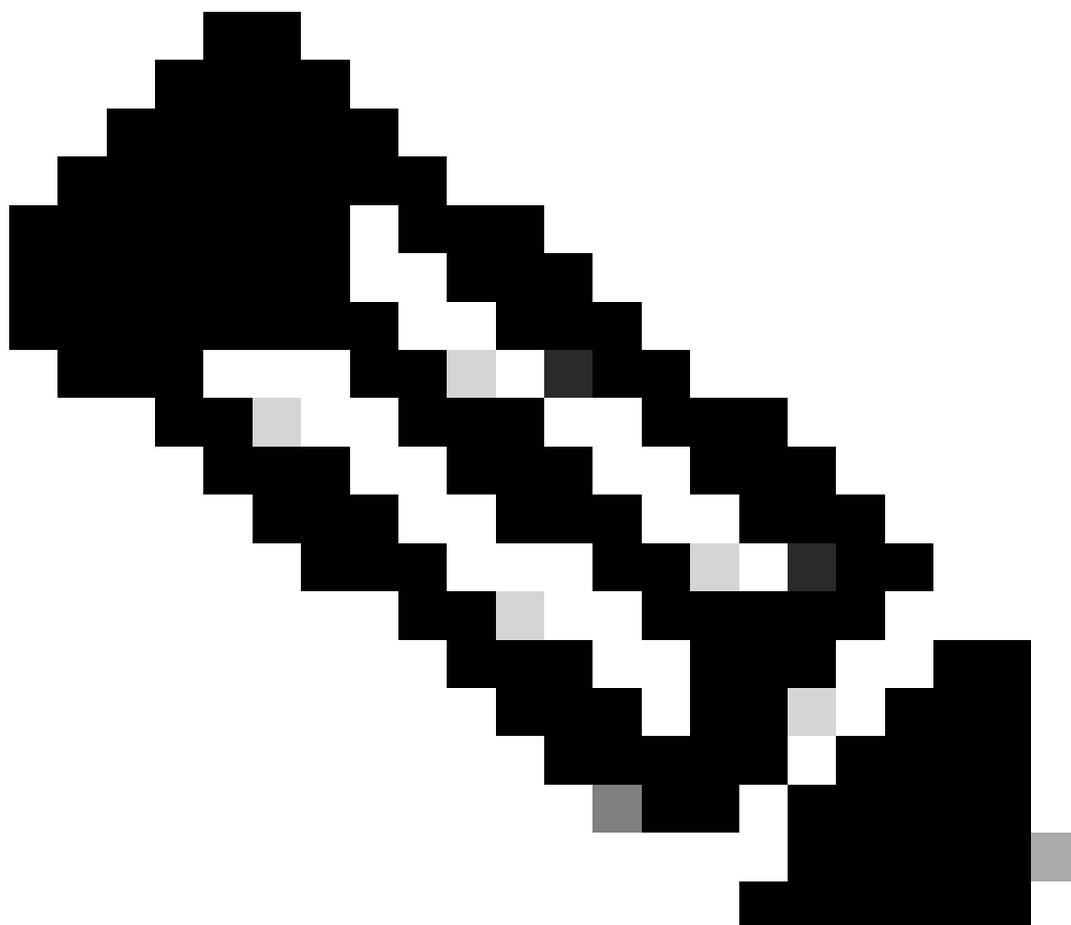


Hinweis: Im nächsten Beispiel wird der `openssl s_client` Befehl im VRF-Management ausgeführt. Ersetzen Sie den gewünschten Wert im `ip netns exec <VRF>` Konstrukt.

```
Switch# run bash ip netns exec management openssl s_client -connect svc.intersight.com:443 CONNECTED(00
```

HTTPS-Erreichbarkeitsüberprüfung

Um die HTTPS-Verbindung zu überprüfen, verwenden Sie den **curl**-Befehl mit dem **-v** verbose flag (zeigt an, ob ein Proxy verwendet wird oder nicht).



Hinweis: Um die Auswirkungen der Aktivierung oder Deaktivierung eines Proxys zu überprüfen, können Sie die Optionen `--proxy`

[protocol://]host[:port] oder --noproxy [protocol://]host[:port] hinzufügen.

Das Konstrukt `ip netns exec <VRF>` dient zur Curl-Ausführung in der gewünschten VRF, beispielsweise `ip netns exec management` zur VRF-Verwaltung.

```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443
```

```
run bash ip netns exec management curl -v -I -L -k https://svc.intersight.com:443 --proxy [protocol://]host[:port]
```

```
<#root>
```

```
#
```

```
run bash ip netns exec management curl -v -I -L -X POST https://svc.intersight.com:443 --proxy http://pr
```

```
Trying 10.201.255.40:80...
```

```
*
```

```
Connected to proxy.es1.cisco.com (10.201.255.40) port 80
```

```
* CONNECT tunnel: HTTP/1.1 negotiated
* allocate connect buffer
* Establish HTTP proxy tunnel to svc.intersight.com:443
> CONNECT svc.intersight.com:443 HTTP/1.1
> Host: svc.intersight.com:443
> User-Agent: curl/8.4.0
> Proxy-Connection: Keep-Alive
>
```

```
< HTTP/1.1 200 Connection established
```

HTTP/1.1 200 Connection established
< snip >

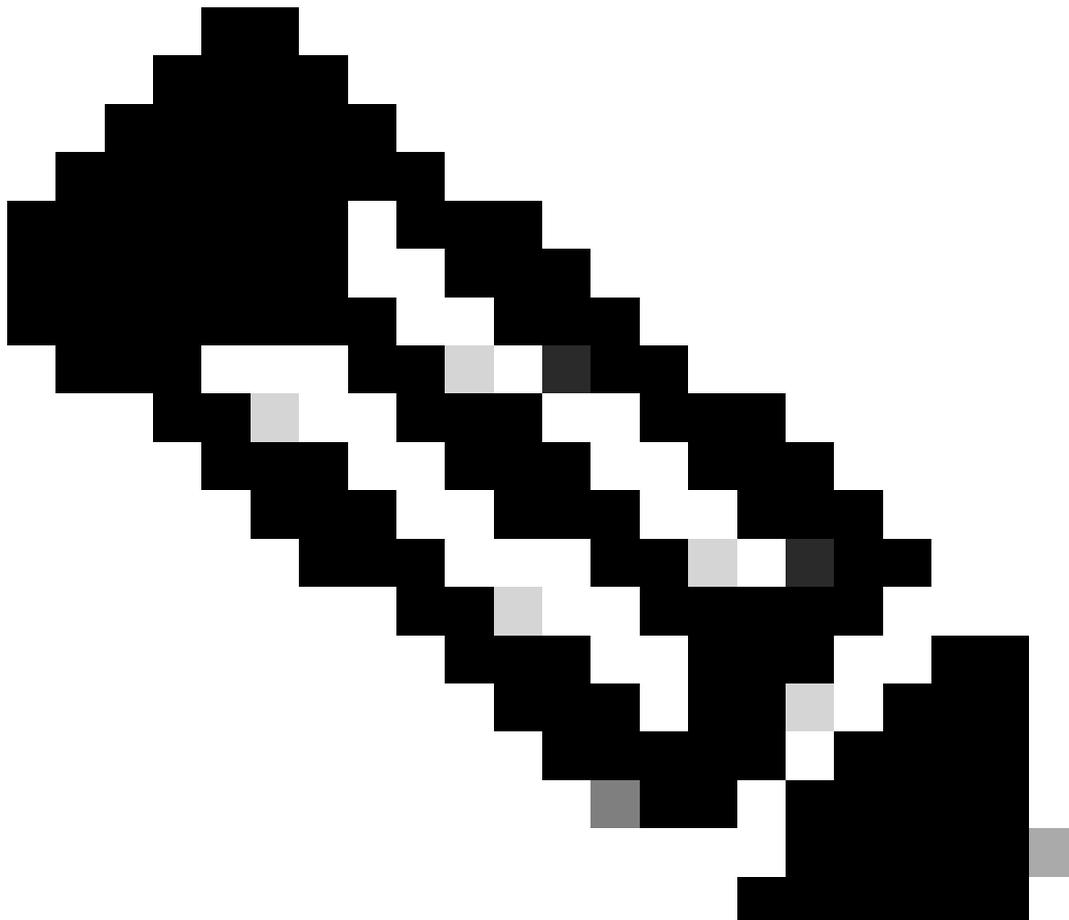
Konfigurieren

Beanspruchen Sie das Gerät intersight.com

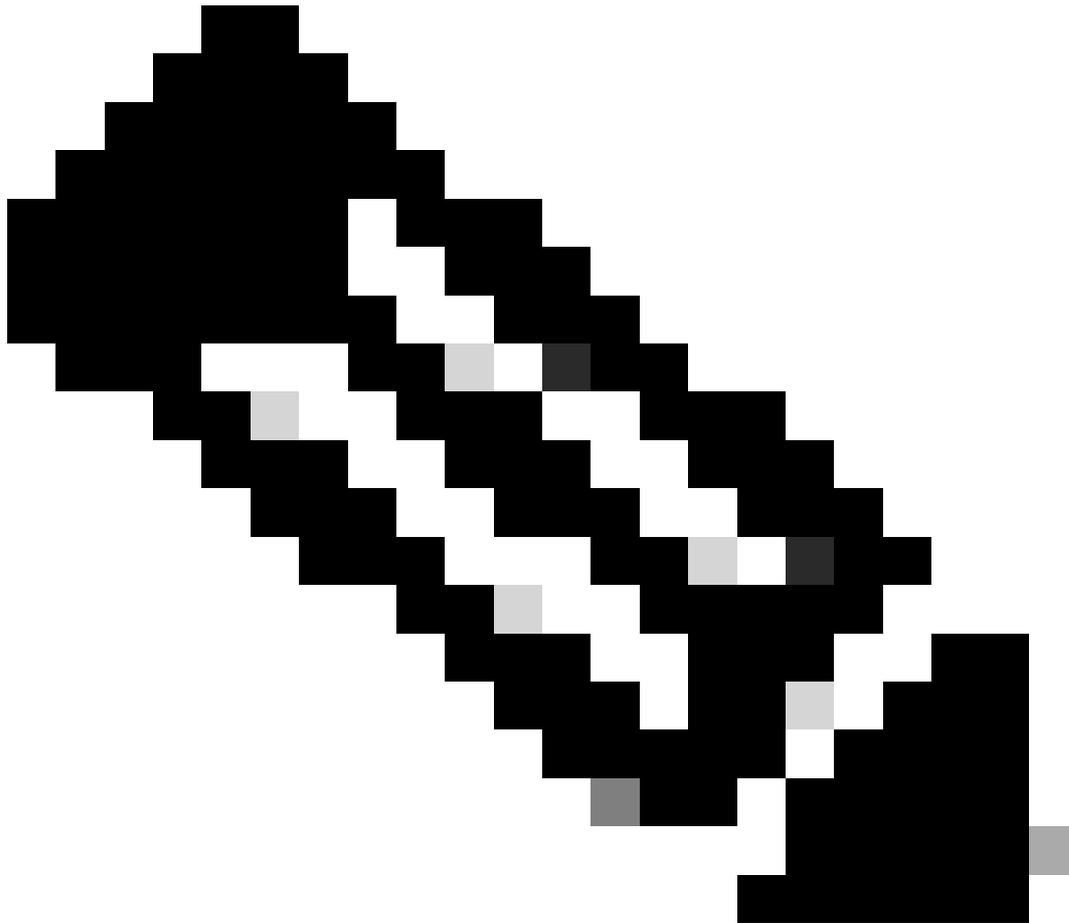
Um ein neues Ziel in Intersight zu erhalten, führen Sie die genannten Schritte aus.

Auf dem Nexus-Gerät

Geben Sie den Befehl Cisco NX-OS `show system device-connector claim-info` ein.



Hinweis: Verwenden Sie für Versionen vor NX-OS 10.3(4a) den Befehl "show intersight claim-info".



Hinweis: Die von Nexus generierten Anspruchsdaten sind folgenden Intersight-Anspruchsfeldern zugeordnet:

Seriennummer = Intersight **Claim ID**

Geräte-ID-Sicherheitstoken = Intersight **Claim Code (Beantragungscod für Intersight)**

```
# show system device-connector claim-info
SerialNumber: FDO23021ZUJ
SecurityToken: 9FFD4FA94DCD
Duration: 599
Message:
Claim state: Not Claimed
```

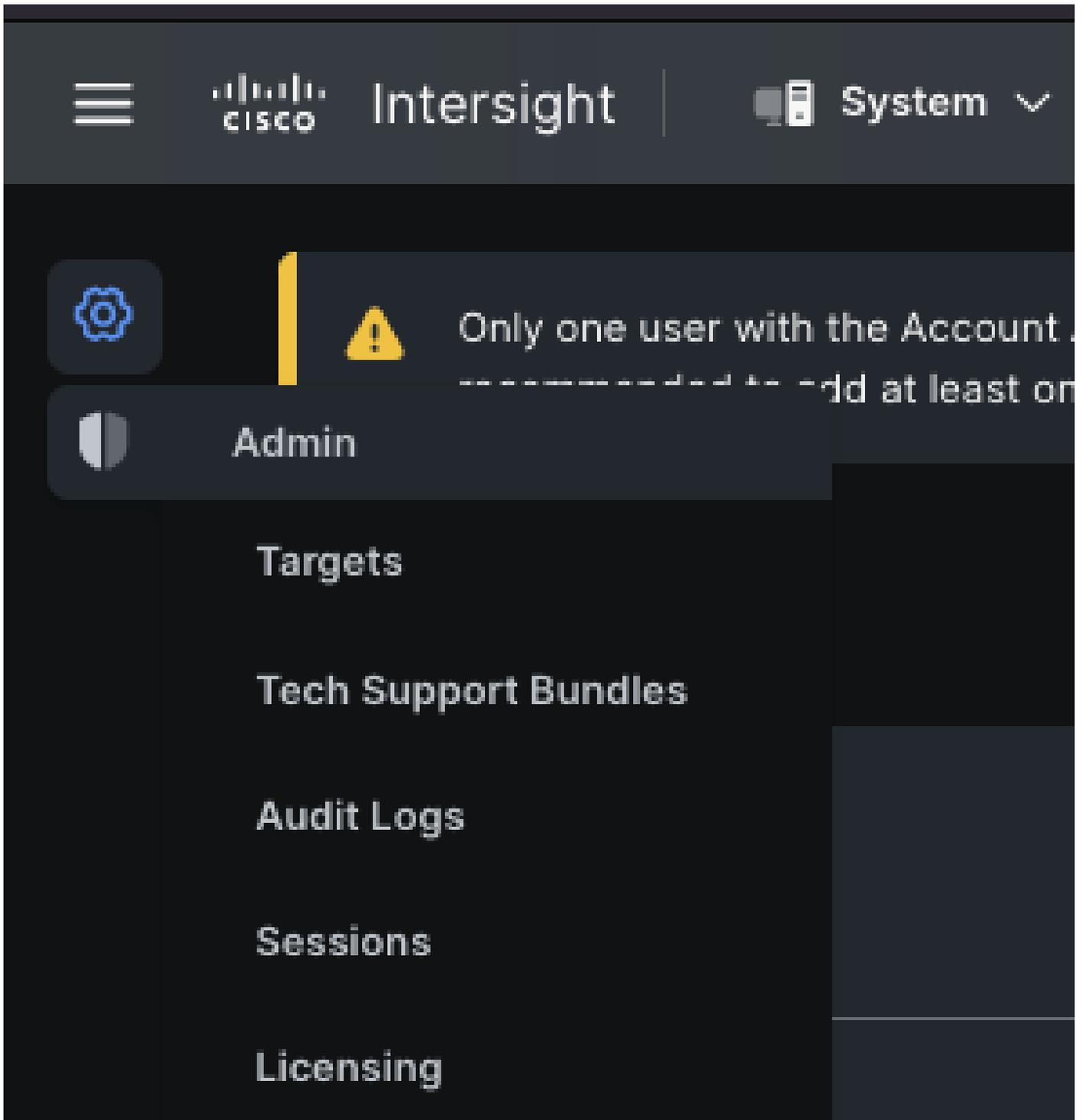
Die hier angegebene **Dauer** ist in Sekunden angegeben.

Auf Interview-Portal

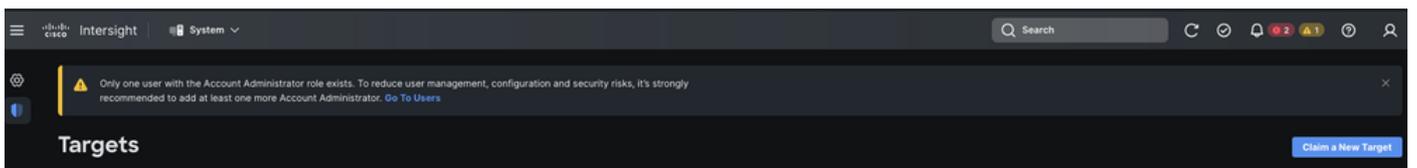
1. Melden Sie sich innerhalb von 10 Minuten bei **Intersight** mit den Berechtigungen des Kontoadministrators, des Geräteadministrators oder des Gerätetechnikers an.
2. Wählen Sie in der Dropdown-Liste "**Service Selector**" die Option **System**.



3. Navigieren Sie zu ADMIN > Targets > Claim a New Target.



3.1. Klicken Sie wie im Bild gezeigt auf **Neue Ziele beanspruchen**.



4. Wählen Sie **Verfügbar für Antrag** und wählen Sie den **Zieltyp** (z. B. Netzwerk) aus, den Sie beanspruchen möchten. Klicken Sie auf **Start**.



Only one user with the Account Administrator role exists. To reduce user management, configuration and security risks, it's strongly recommended to add at least one more Account Administrator. [Go To Users](#)



← Targets

Claim a New Target

Select Target Type

Filters

Available for Claiming

Categories

All

Cloud

Compute / Fabric

Hyperconverged

Network

Orchestrator

🔍 Search

Network

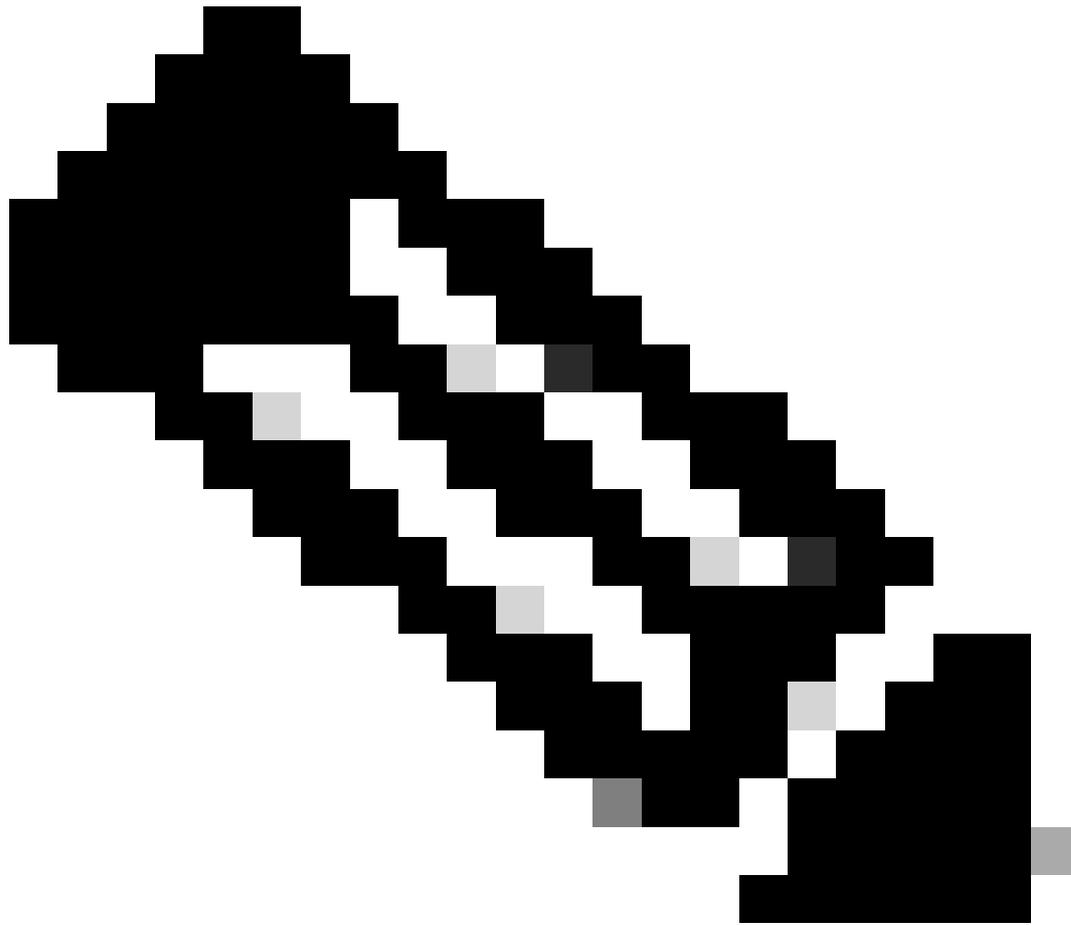
 Cisco MDS Switch	<input checked="" type="checkbox"/> Cisco Nexus Switch	<input type="checkbox"/> Cisco APIC
<input type="checkbox"/> Cisco Cloud APIC	<input type="checkbox"/> Cisco DCNM	<input type="checkbox"/> Cisco Nexus Dashboard

[Cancel](#) [Start](#)

5. Geben Sie die erforderlichen Details ein, und klicken Sie auf **Forderung**, um den Antragsprozess abzuschließen.



Hinweis: Das **Sicherheitstoken** auf dem Switch wird als Anspruchscode verwendet, und die **Seriennummer** des Switches ist die Geräte-ID.



Hinweis: Das Sicherheitstoken läuft ab. Sie müssen den Antrag zuerst bearbeiten, oder das System fordert Sie auf, den Antrag zu regenerieren.



The security token has expired. Please obtain a new security token to claim the device



[Details](#)

Melden Sie bei intersight.com mit Ansible® ein oder mehrere eigenständige Nexus-Geräte an

Um ein oder mehrere Nexus-Geräte für sich zu beanspruchen, kann ein Ansible-Leitfaden ausgeführt werden.

- Das ansible Inventar und der strategische Leitfaden können von <https://github.com/datacenter/ansible-intersight-nxos> geklont werden.
- In der Ansible inventory.yaml ist der ansible_connection Typ so festgelegt, dass Befehle an den Nexus-Switch gesendet werden können `ansible.netcommon.network_cli`. Dies kann geändert werden, um die Konnektivität über NXAPI zu ermöglichen `ansible.netcommon.httpapi`.
- Eine mögliche Verbindung zum Intersight-Endpunkt erfordert einen API-Schlüssel, der von Ihrem **intersight.com**-Konto generiert werden kann.

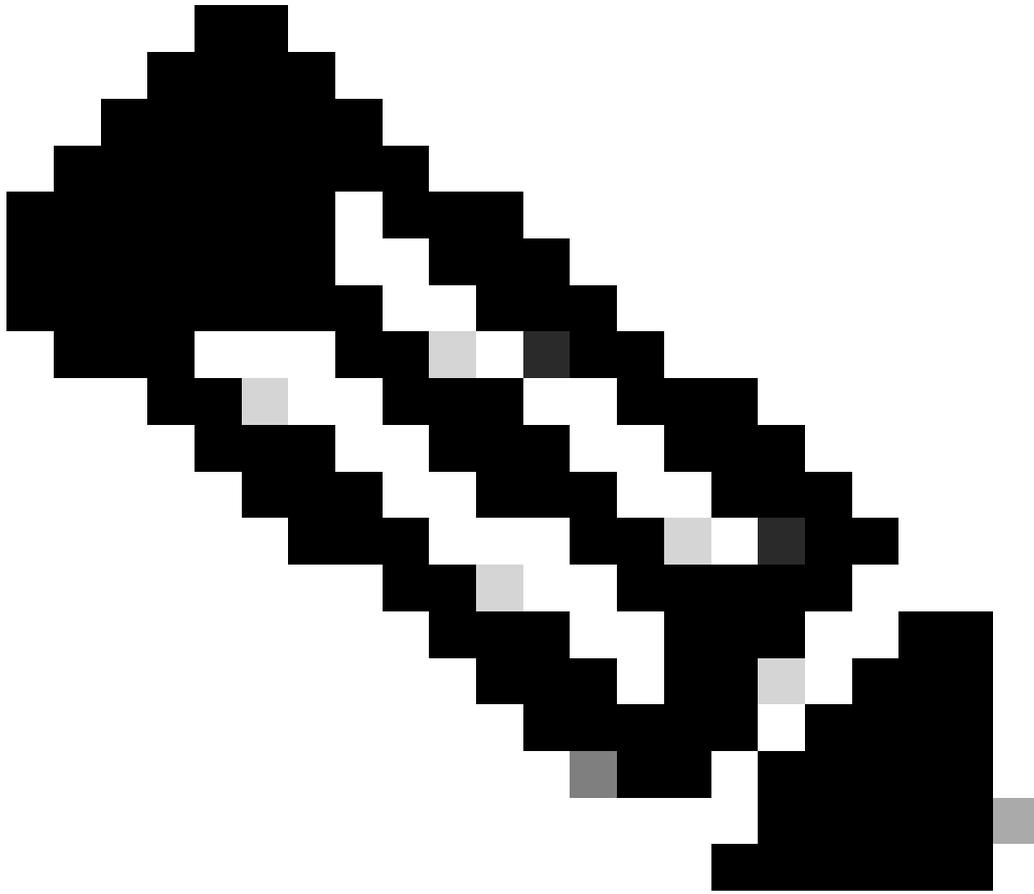
Nexus NXAPI konfigurieren (nur bei Verwendung von `ansible.netcommon.httpapi`)



Hinweis: Wenn ein Proxy auf Systemebene konfiguriert ist (**HTTP(S)_PROXY**) und Ansible keinen Proxy verwenden darf, um eine Verbindung mit dem Nexus NXAPI-Endpoint herzustellen, sollte festgelegt werden (Standard ist True).
ansible_httppapi_use_proxy: False

```
# configure terminal # cfeature nxapi # nxapi port 80 # no nxapi https port 443 # end # show nxapi nxap
```

Um die HTTP-Verbindung zum NXAPI-Endpoint unabhängig zu überprüfen, können Sie versuchen, eine show clock zu senden. Im nächsten Beispiel authentifiziert der Switch den Client mithilfe der Standardauthentifizierung. Es ist auch möglich, den NXAPI-Server zu konfigurieren, um Clients basierend auf dem X.509-Benutzerzertifikat zu authentifizieren.



Hinweis: Der Hash für die Standardauthentifizierung wird aus der base64-Codierung "**username:password**" abgeleitet. In diesem Beispiel ist **admin:cisco!123** base64 kodiert YWRtaW46Y2lzY28hMTIz.

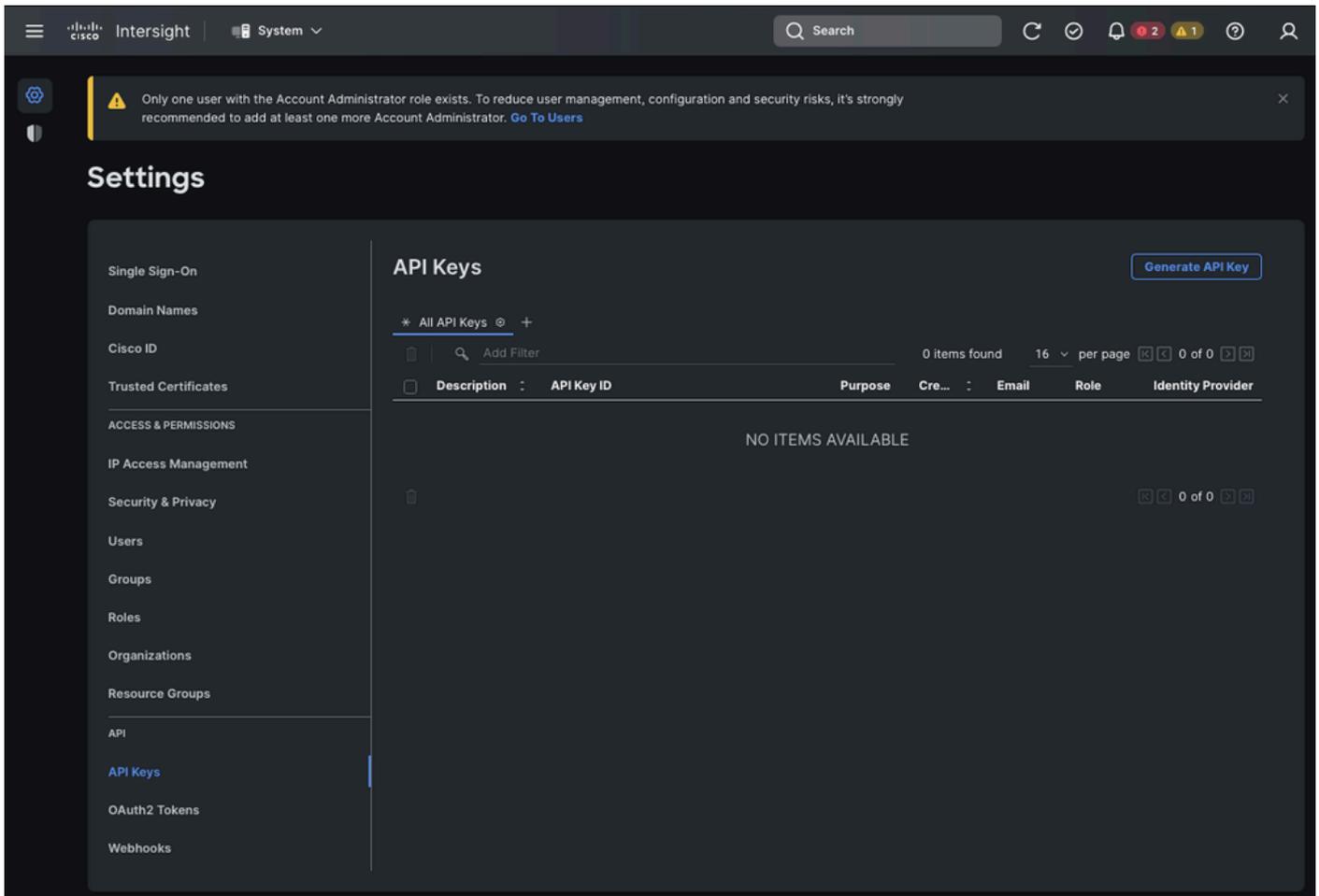
```
curl -v --no-proxy '*' \ --location 'http://10.1.1.3:80/ins' \ --header 'Content-Type: application/json'
```

Curl-Antwort:

```
* Trying 10.1.1.3... * TCP_NODELAY set * Connected to 10.1.1.3 (10.1.1.3) port 80 (#0) > POST /ins HTTP/
```

API-Schlüssel für Intersight generieren

Im Abschnitt [README.md](#) erfahren Sie, wie Sie den API-Schlüssel aus der Intersight System > Settings > API keys > Generate API Key abrufen.



Generate API Key



Description

Nexus Intersight key



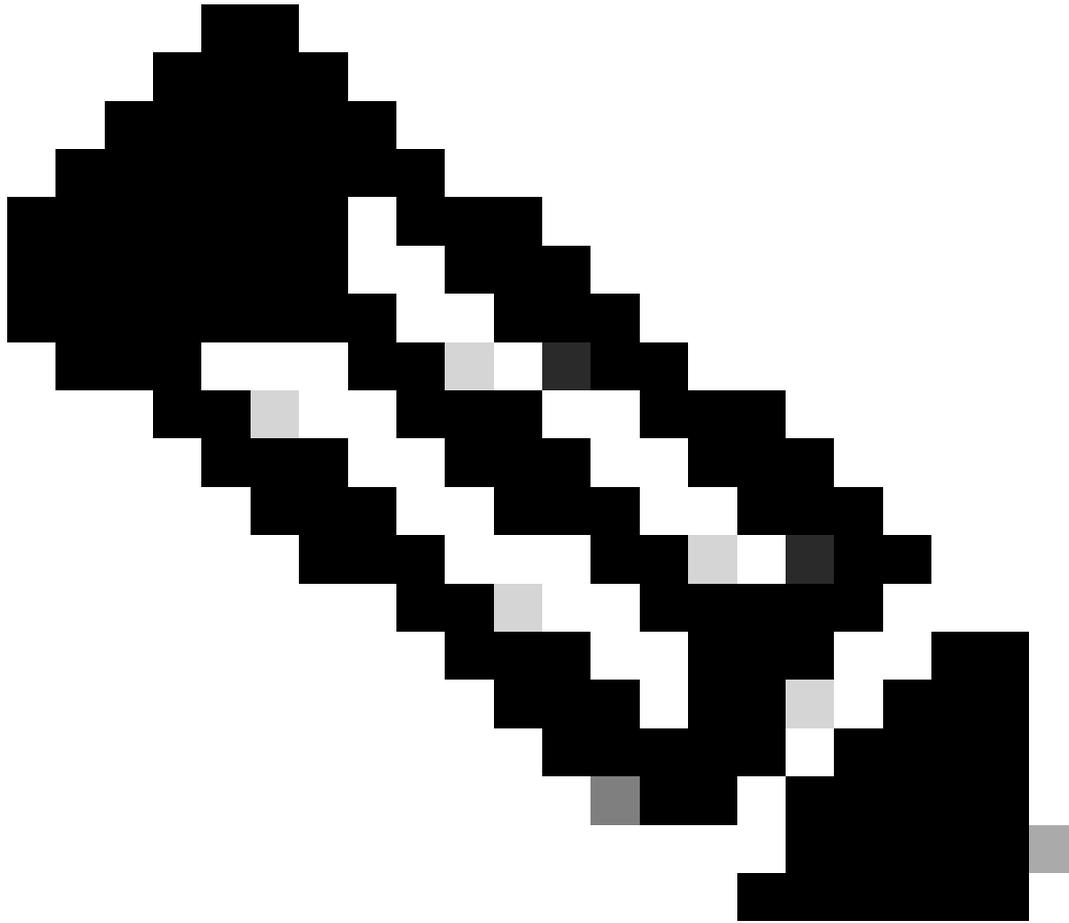
API Key Purpose

- API key for OpenAPI schema version 2 
- API key for OpenAPI schema version 3 (This is a feature in preview and for SDK developer use only) 

Close

Generate

Beispiel: Ansible inventory.yaml



Hinweis: Im nächsten Beispiel wurde Ansible konfiguriert, um die Proxyeinstellungen des Betriebssystems mit zu ignorieren `ansible_httpapi_use_proxy: False`. Wenn der Ansible-Server einen Proxy verwenden muss, um den Switch zu erreichen, können Sie diese Konfiguration entfernen oder auf `True` (Standard) setzen.



Hinweis: Die API-Schlüssel-ID ist eine Zeichenfolge. Der private API-Schlüssel enthält den vollständigen Pfad zu einer Datei, die den privaten Schlüssel enthält. Für die Produktionsumgebung wird empfohlen, den Ansible-Tresor zu verwenden.

```
---
all:
  hosts:
    switch1:
      ansible_host: "10.1.1.3"
      intersight_src: "mgmt0"
      intersight_vrf: "management"
```

```

vars:
  ansible_user: "admin"
  ansible_password: "cisco!123"
  ansible_connection: ansible.netcommon.network_cli
  ansible_network_os: cisco.nxos.nxos
  ansible_httpapi_use_proxy: False
  remote_tmp: "/bootflash"
  proxy_env:
    - no_proxy: "10.1.1.3/24"
  intersight_proxy_host: 'proxy.cisco.com'
  intersight_proxy_port: '80'

  api_key_id: "5fcb99d97564612d33fdfca1/5fcb99d97564612d33fdf1b2/65c6c09d756461330198ce7e"
  api_private_key: "/home/admin/ansible-intersight-nxos/my_intersight_private_key.txt"
...

```

Beispiel: playbook.yaml Ausführung

Weitere Informationen zur Programmierung eigenständiger Nexus-Geräte mit Ansible finden Sie im Abschnitt mit dem Applications/Using Ansible Cisco NX-OS im [Cisco Nexus NX-OS Programmierhandbuch der Serie 9000](#) für Ihre aktuelle Version.

```

> ansible-playbook -i inventory.yaml playbook.yaml PLAY [all] *****

```

Überprüfung

Gehen Sie folgendermaßen vor, um den Anspruch eines neuen Ziels zu überprüfen:

Auf dem Nexus-Switch

Versionen vor 10.3(4a)M

```
# run bash sudo cat /mnt/pss/connector.db
```

```
Nexus# run bash sudo cat /mnt/pss/connector.db { "AccountOwnershipState": "Claimed", "AccountOwnershipU
```

Releases, die mit 10.3(4a)M beginnen

```
# show system device-connector claim-info
```

```
N9k-Leaf-2# show system device-connector claim-info SerialNumber: FD023021ZUJ SecurityToken: Duration: 0
```

```
# show system internal intersight info
```

```
# show system internal intersight info Intersight connector.db Info: ConnectionState :Connected Connect
```

Ansible

Es ist möglich, am Ende des playbook.yaml eine Aufgabe hinzuzufügen, um die Switch-Intersight-Informationen abzurufen.

```
- name: Get intersight info nxos_command: commands: - show system internal intersight info register: i
```

Hier die entsprechende Ausgabe:

```
TASK [Get intersight info] *****
```

Geräteanschluss deaktivieren

	Befehl oder Aktion	Zweck
Schritt 1	kein Feature-Interview Beispiel: switch(config)# no feature intersight	Deaktiviert den Intersight-Prozess und entfernt alle NXDC-Konfigurationen und Protokollspeicher.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.