

Konfigurieren der benutzerdefinierten TACACS-Rolle für Nexus 9000 mit ISE 3.2

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Schritt 1: Konfigurieren von Nexus 9000](#)

[Schritt 2: Identity Service Engine 3.2 konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine benutzerdefinierte Nexus-Rolle für TACACS über die CLI auf NK9 konfigurieren.

Voraussetzungen

Anforderungen

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

- TACACS+
- ISE 3.2

Verwendete Komponenten

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

- Die Cisco Nexus 9000 NXOS-Image-Datei lautet: bootflash:///nxos.9.3.5.bin
- Identity Service Engine Version 3.2

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

Lizenzanforderungen:

Cisco NX-OS - TACACS+ erfordert keine Lizenz.

Cisco Identity Service Engine - Für neue ISE-Installationen verfügen Sie über eine 90-tägige Testlizenz mit Zugriff auf alle ISE-Funktionen. Wenn Sie keine Testlizenz besitzen, benötigen Sie für die Verwendung der ISE TACACS-Funktion eine Device Admin-Lizenz für den Policy Server Node, der die Authentifizierung übernimmt.

Nachdem sich die Admin-/Helpdesk-Benutzer auf dem Nexus-Gerät authentifiziert haben, gibt die ISE die gewünschte Nexus Shell-Rolle zurück.

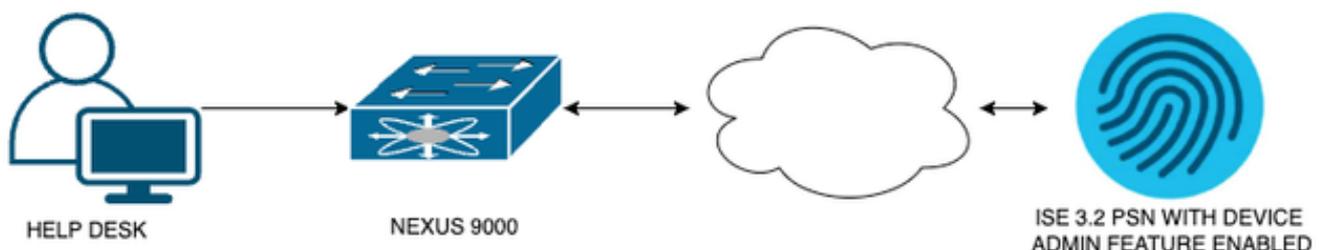
Der Benutzer mit dieser Rolle kann eine grundlegende Fehlerbehebung durchführen und bestimmte Ports zurückweisen.

Die TACACS-Sitzung, die die Nexus-Rolle übernimmt, muss nur die folgenden Befehle und Aktionen verwenden und ausführen können:

- Zugriff auf das konfigurierte Terminal, um NUR herunterzufahren und keine heruntergefahrenen Schnittstellen vom 1/1-1/21 und 1/25-1/30 auszuführen
- SSH
- SSH6
- telnet
- Telnet6
- Routenverfolgung
- Routenverfolgung6
- Ping
- Ping 6:
- Aktivieren

Konfigurieren

Netzwerkdiagramm



Schritt 1: Konfigurieren von Nexus 9000

1. AAA-Konfiguration



Warnung: Nach der Aktivierung der TACACS-Authentifizierung verwendet das Nexus-Gerät keine lokale Authentifizierung mehr und verwendet stattdessen die auf AAA-Servern basierende Authentifizierung.

```
Nexus9000(config)# feature tacacs+
Nexus9000(config)# tacacs-server host <Your ISE IP> key 0 Nexus3xample
Nexus9000(config)# tacacs-server key 0 "Nexus3xample"
Nexus9000(config)# aaa group server tacacs+ IsePsnServers
Nexus9000(config-tacacs+)# server <Your ISE IP>
Nexus9000(config)# aaa authentication login default group IsePsnServers local
```

2. Konfigurieren Sie die benutzerdefinierte Rolle mit den angegebenen Anforderungen.

```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)# description Can perform basic Troubleshooting and bounce certain ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# rule 4 permit command ssh6 *
Nexus9000(config-role)# rule 5 permit command ping *
Nexus9000(config-role)# rule 6 permit command ping6 *
Nexus9000(config-role)# rule 7 permit command telnet *
Nexus9000(config-role)# rule 8 permit command traceroute *
Nexus9000(config-role)# rule 9 permit command traceroute6 *
Nexus9000(config-role)# rule 10 permit command telnet6 *
Nexus9000(config-role)# rule 11 permit command config t ; interface * ; shutdown
Nexus9000(config-role)# rule 12 permit command config t ; interface * ; no shutdown
```

```
vlan policy deny
interface policy deny
```

```
Nexus9000(config-role-interface)# permit interface Ethernet1/1
Nexus9000(config-role-interface)# permit interface Ethernet1/2
Nexus9000(config-role-interface)# permit interface Ethernet1/3
Nexus9000(config-role-interface)# permit interface Ethernet1/4
Nexus9000(config-role-interface)# permit interface Ethernet1/5
Nexus9000(config-role-interface)# permit interface Ethernet1/6
Nexus9000(config-role-interface)# permit interface Ethernet1/7
Nexus9000(config-role-interface)# permit interface Ethernet1/8
Nexus9000(config-role-interface)# permit interface Ethernet1/8
Nexus9000(config-role-interface)# permit interface Ethernet1/9
Nexus9000(config-role-interface)# permit interface Ethernet1/10
Nexus9000(config-role-interface)# permit interface Ethernet1/11
Nexus9000(config-role-interface)# permit interface Ethernet1/12
Nexus9000(config-role-interface)# permit interface Ethernet1/13
Nexus9000(config-role-interface)# permit interface Ethernet1/14
Nexus9000(config-role-interface)# permit interface Ethernet1/15
Nexus9000(config-role-interface)# permit interface Ethernet1/16
Nexus9000(config-role-interface)# permit interface Ethernet1/17
Nexus9000(config-role-interface)# permit interface Ethernet1/18
Nexus9000(config-role-interface)# permit interface Ethernet1/19
Nexus9000(config-role-interface)# permit interface Ethernet1/20
Nexus9000(config-role-interface)# permit interface Ethernet1/21
Nexus9000(config-role-interface)# permit interface Ethernet1/22
Nexus9000(config-role-interface)# permit interface Ethernet1/25
Nexus9000(config-role-interface)# permit interface Ethernet1/26
Nexus9000(config-role-interface)# permit interface Ethernet1/27
Nexus9000(config-role-interface)# permit interface Ethernet1/28
Nexus9000(config-role-interface)# permit interface Ethernet1/29
Nexus9000(config-role-interface)# permit interface Ethernet1/30
```

```
Nexus9000# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
```

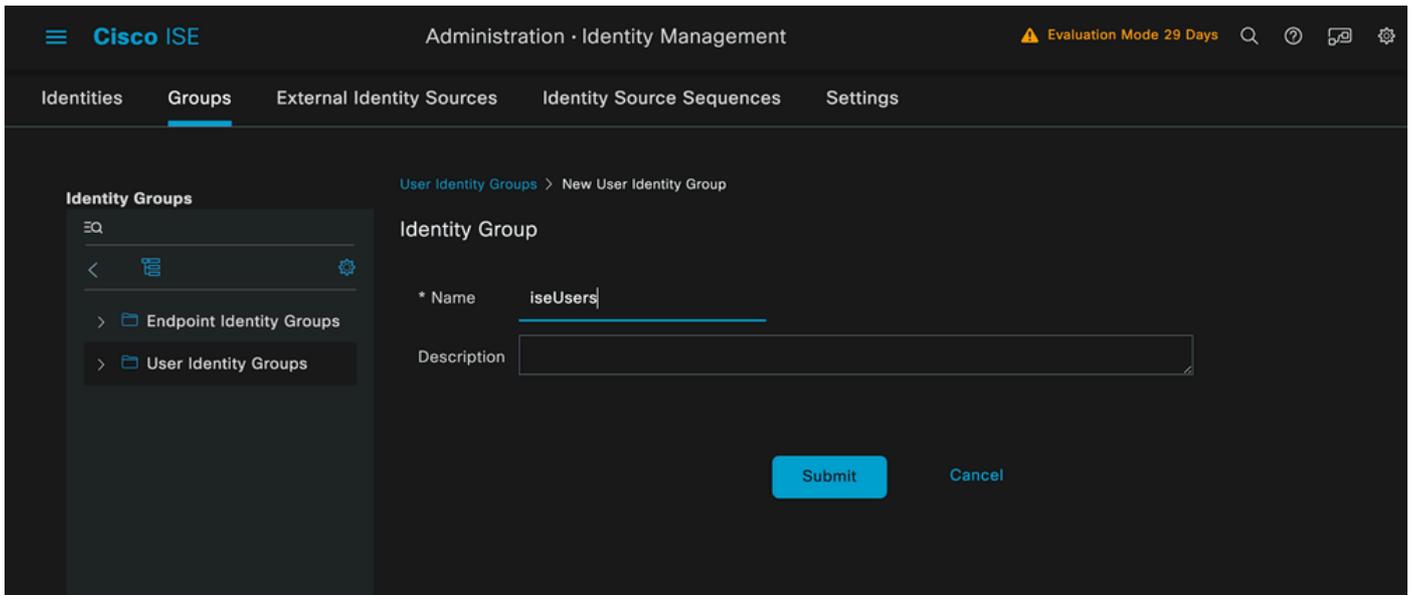
Copy complete.

Schritt 2: Identity Service Engine 3.2 konfigurieren

1. Konfigurieren Sie die Identität, die während der Nexus TACACS-Sitzung verwendet wird.

Die lokale ISE-Authentifizierung wird verwendet.

Navigieren Sie zur Registerkarte Administration > Identity Management > Groups (Verwaltung > Identitätsverwaltung > Gruppen), und erstellen Sie die Gruppe, der der Benutzer angehören muss. Die für diese Demonstration erstellte Identitätsgruppe lautet iseUsers (iseUsers).

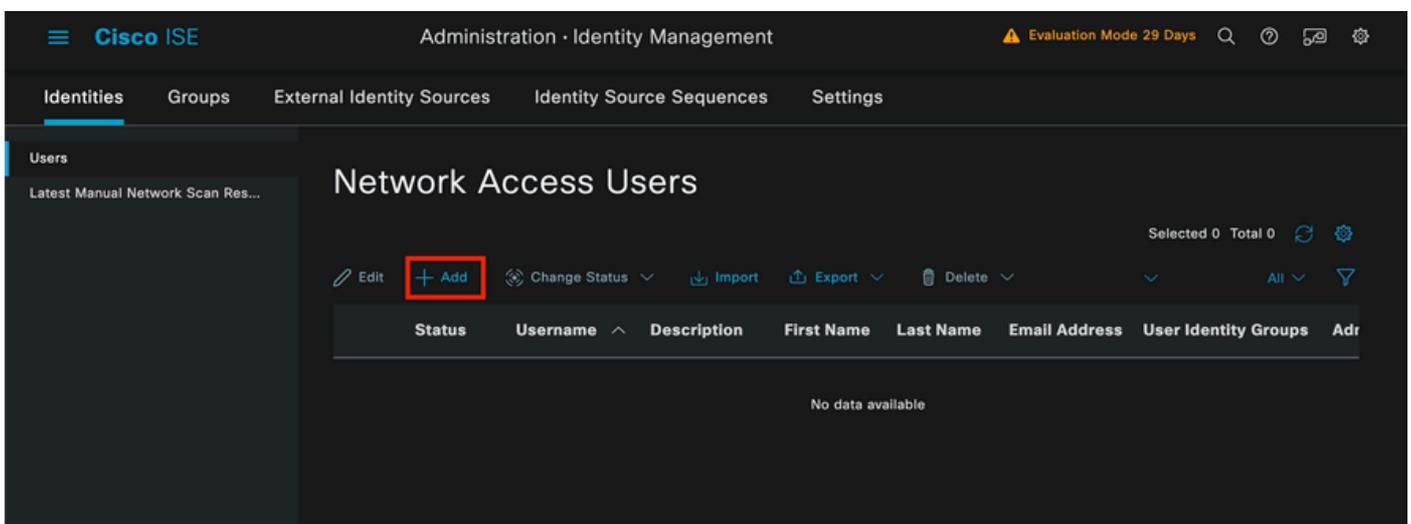


Erstellen einer Benutzergruppe

Klicken Sie auf die Schaltfläche "Senden".

Navigieren Sie anschließend zu Administration > Identity Management > Identity (Verwaltung > Identität).

Drücken Sie auf die Schaltfläche Hinzufügen.



Erstellung von Benutzern

Beginnen Sie in den Pflichtfeldern mit dem Namen des Benutzers. In diesem Beispiel wird der Benutzername iseiscool verwendet.

Network Access Users List > New Network Access User

Network Access User

* Username iseiscool

Status Enabled

Account Name Alias ⓘ

Email ⓘ

Benennen des Benutzers und Erstellen desselben

Der nächste Schritt besteht darin, dem erstellten Benutzernamen ein Kennwort zuzuweisen. VainillaSE97 ist das in dieser Demonstration verwendete Kennwort.

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration ⓘ
Password will expire in 60 days

Never Expires ⓘ

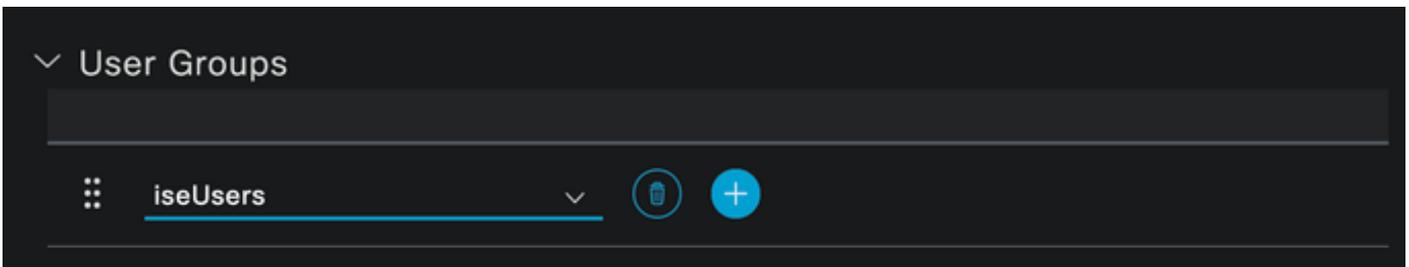
Password Re-Enter Password

* Login Password|| ⓘ

Enable Password|| ⓘ

Kennwortzuweisung

Weisen Sie schließlich den Benutzer der zuvor erstellten Gruppe zu, in diesem Fall iseUsers (iseUsers).

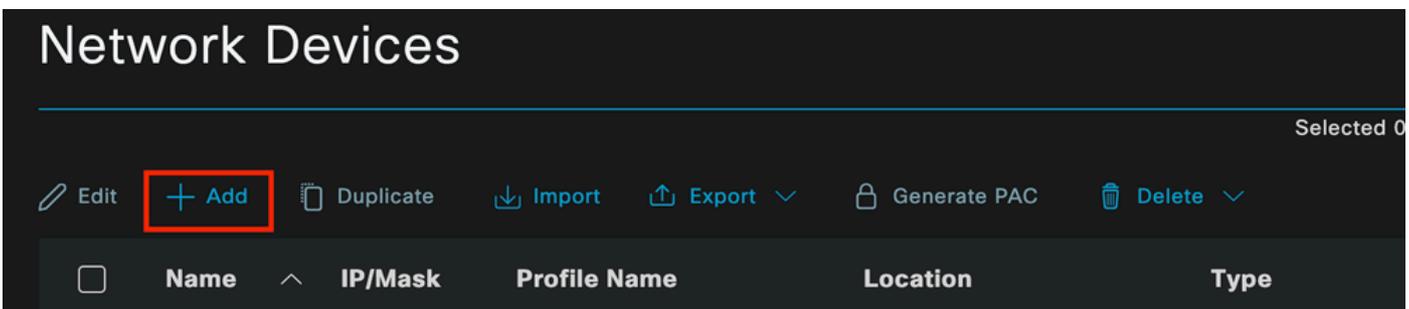


Gruppenzuweisung

2. Konfigurieren und Hinzufügen des Netzwerkgeräts

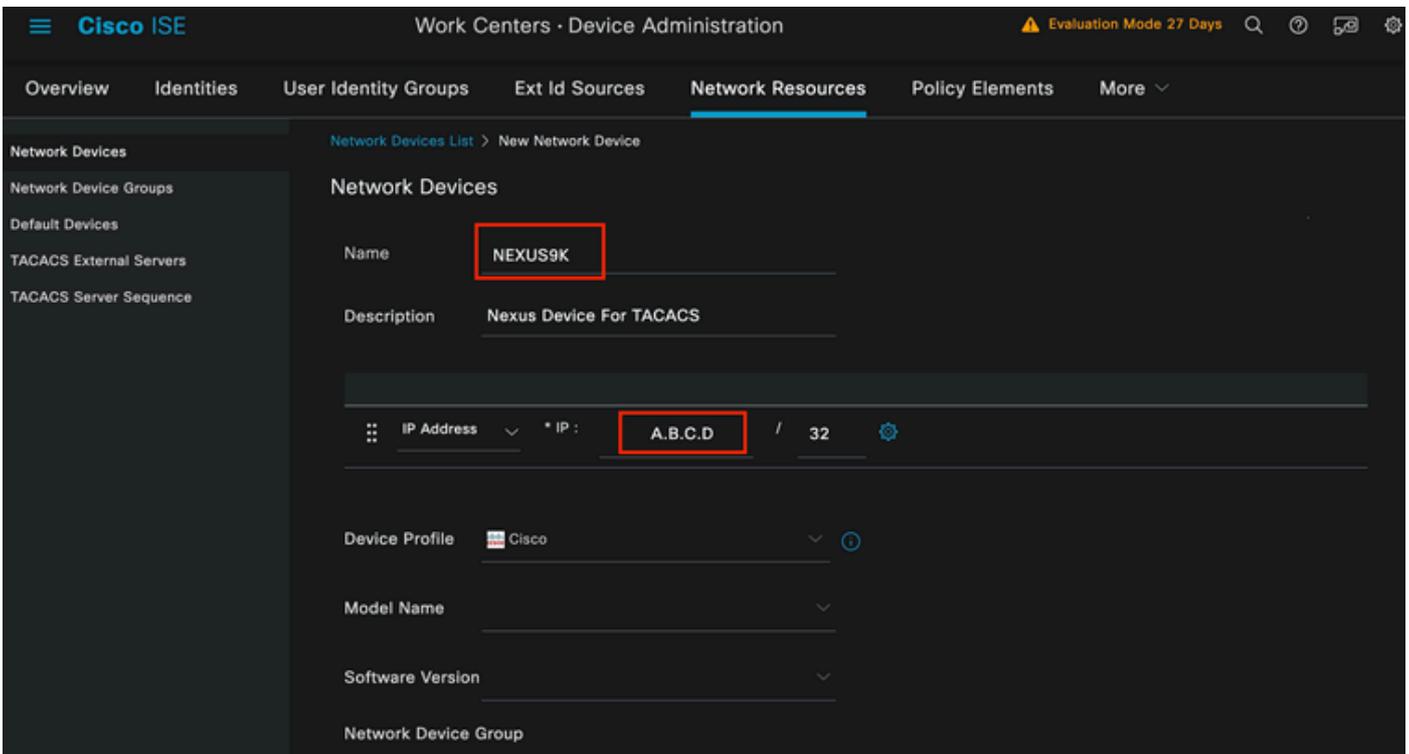
Fügen Sie das NEXUS 9000-Gerät der ISE-Administration > Network Resources > Network Devices hinzu.

Klicken Sie auf die Schaltfläche Hinzufügen, um zu starten.



Seite "Network Access Device"

Geben Sie die Werte in das Formular ein, weisen Sie dem von Ihnen erstellten NAD einen Namen und eine IP-Adresse zu, über die der NAD die ISE für die TACACS-Konversation kontaktiert.

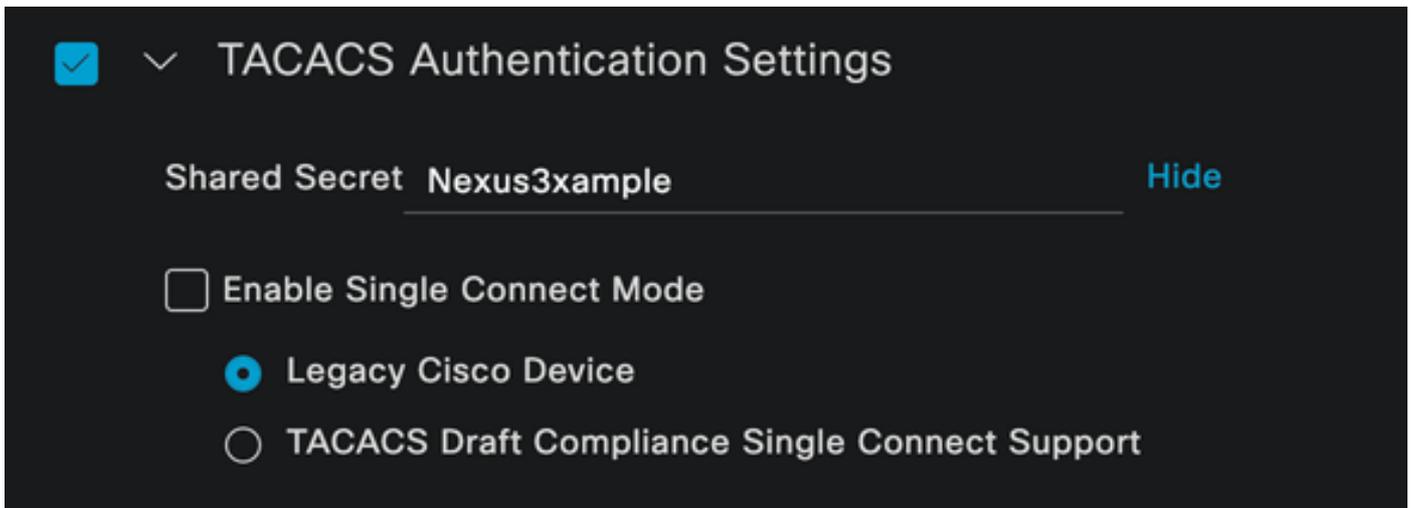


Netzwerkgerät konfigurieren

Die Dropdown-Optionen können leer gelassen und weggelassen werden. Mit diesen Optionen können Sie Ihre NADs nach Standort, Gerätetyp und Version kategorisieren und dann den Authentifizierungsfluss auf Basis dieser Filter ändern.

Wählen Sie Administration > Network Resources > Network Devices > Your NAD > TACACS Authentication Settings.

Fügen Sie den gemeinsamen geheimen Schlüssel hinzu, den Sie in der NAD-Konfiguration für diese Demonstration verwendet haben. In dieser Demonstration wird Nexus3xample verwendet.



TACACS Authentication Settings

Shared Secret **Nexus3xample** [Hide](#)

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

TACACS-Konfigurationsabschnitt

Speichern Sie die Änderungen, indem Sie auf die Schaltfläche Submit (Senden) klicken.

3. TACACS-Konfiguration auf der ISE.

Überprüfen Sie noch einmal, ob für das von Ihnen in Nexus 9000 konfigurierte PSN die Option Device Admin (Geräteadministrator) aktiviert ist.



Hinweis: Die Aktivierung des Geräte-Admin-Dienstes führt NICHT zu einem Neustart auf der ISE.



Enable Device Admin Service

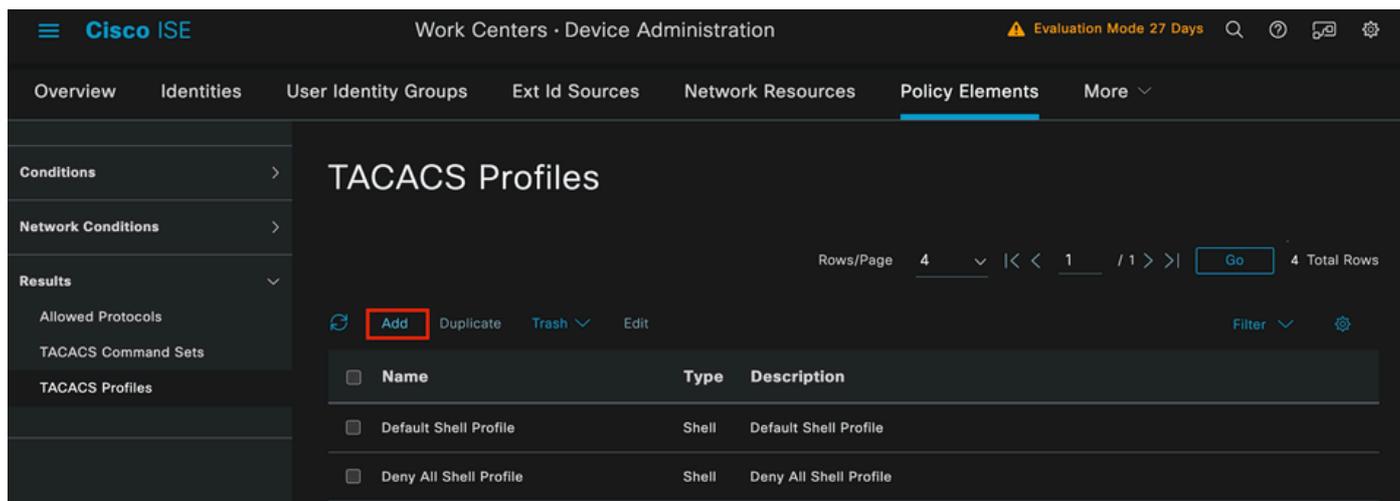


Funktionsüberprüfung für den PSN-Geräteadministrator

Dies kann über das ISE-Menü Administration > System > Deployment > Your PSN > Policy Server section > Enable Device Admin Services überprüft werden.

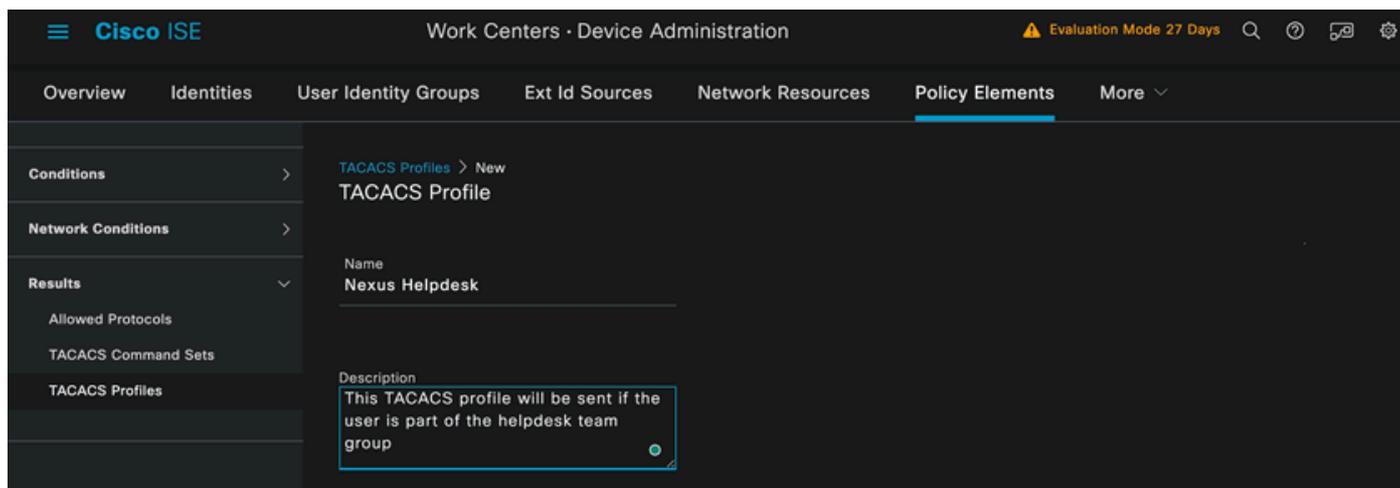
- Erstellen Sie ein TACACS-Profil, das bei erfolgreicher Authentifizierung die Rolle Helpdesk an das Nexus-Gerät zurückgibt.

Navigieren Sie im ISE-Menü zu Workcenters > Device Administration > Policy Elements > Results > TACACS Profiles, und klicken Sie auf die Schaltfläche Add (Hinzufügen).



TACACS-Profil

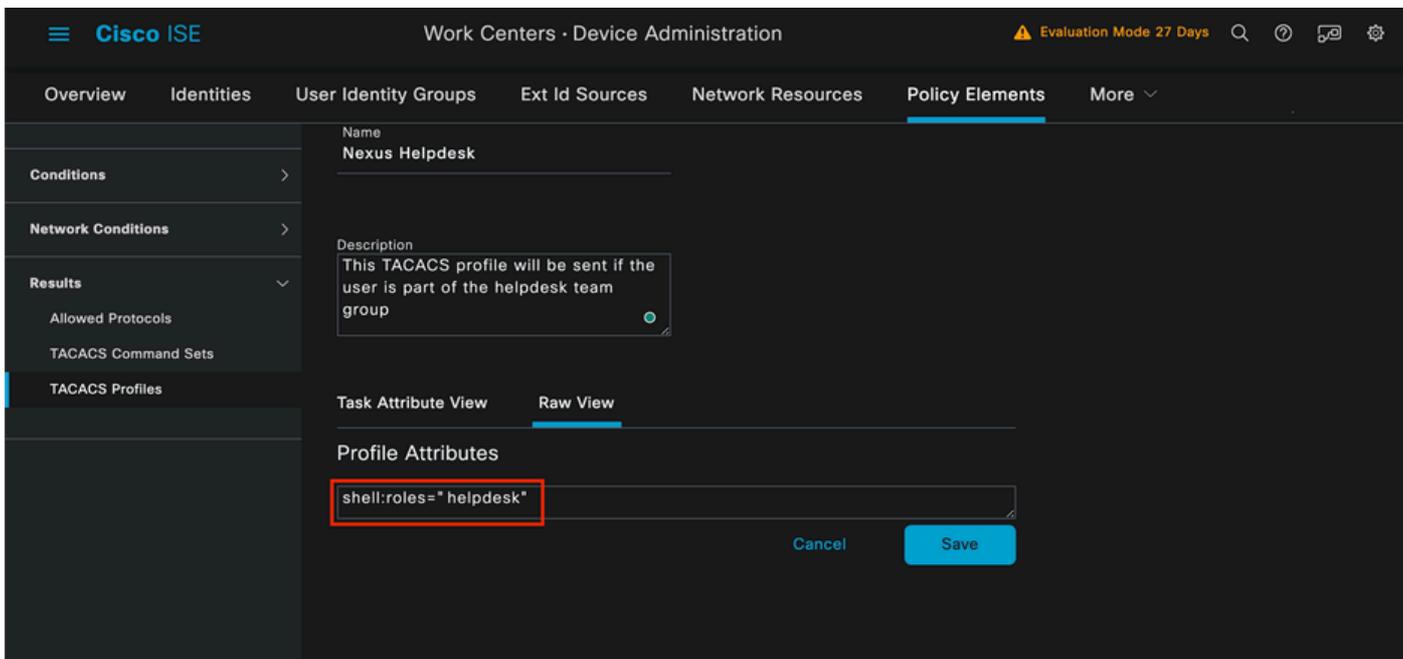
Zuweisen eines Namens und optional einer Beschreibung.



TACACS-Profil benennen

Ignorieren Sie den Abschnitt Aufgabenattributansicht, und navigieren Sie zum Abschnitt Rohansicht.

Geben Sie den Wert `shell:roles="helpdesk"` ein



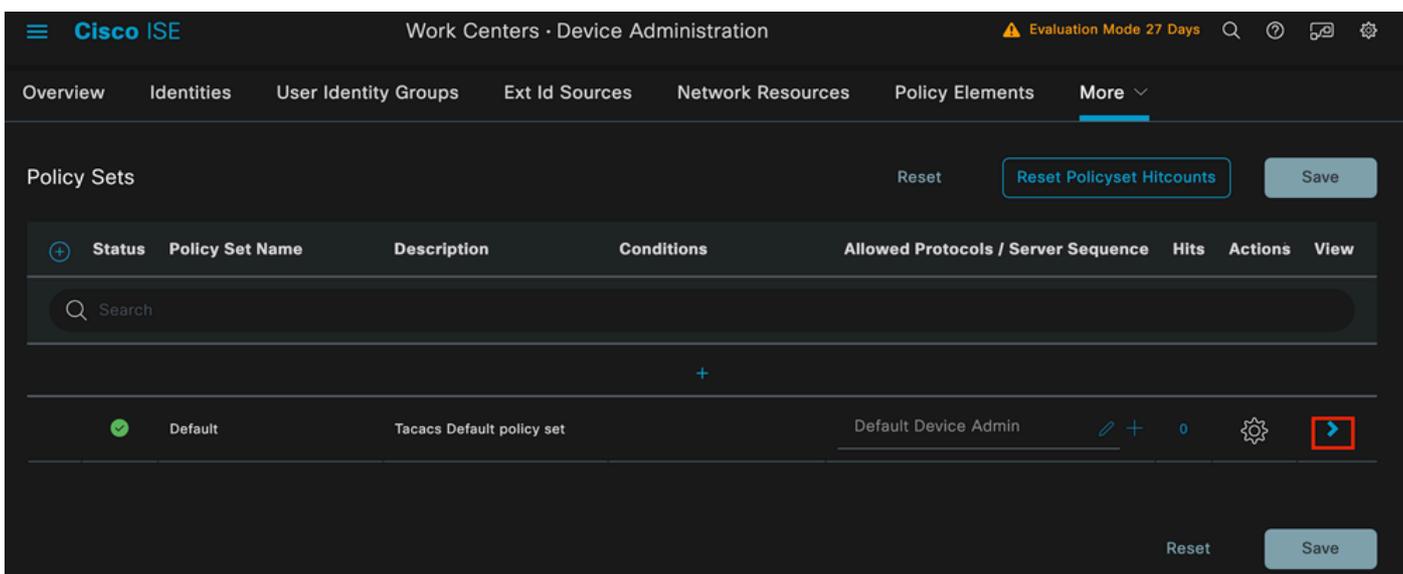
Profilattribut hinzufügen

Konfigurieren Sie den Richtlinienatz, der die Authentifizierungsrichtlinie und die Autorisierungsrichtlinie enthält.

Wählen Sie im Menü ISE Work Centers > Device Administration > Device Admin Policy Sets.

Zu Demonstrationszwecken wird die Standardrichtlinie verwendet. Es kann jedoch auch ein anderer Richtlinienatz erstellt werden, dessen Bedingungen bestimmten Szenarien entsprechen.

Klicken Sie auf den Pfeil am Ende der Zeile.

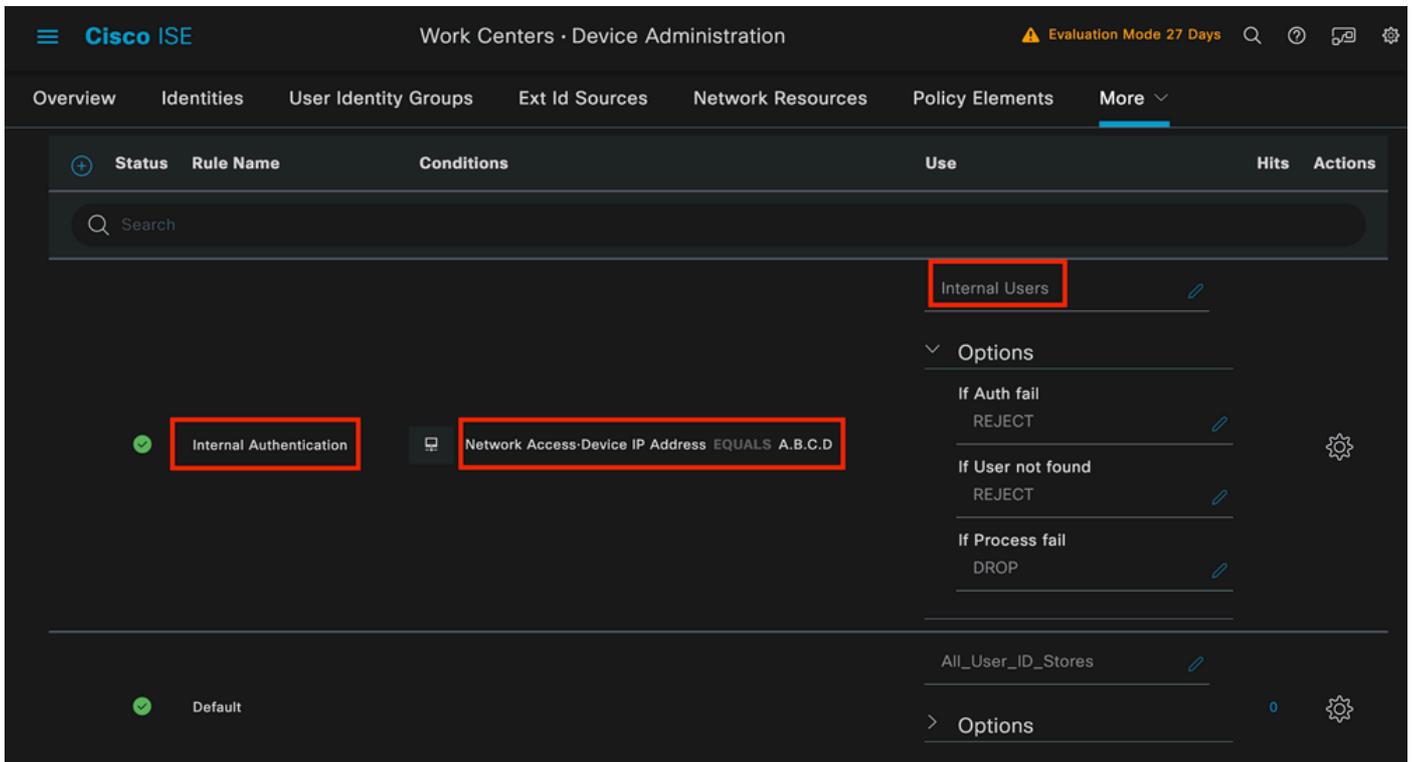


Seite "Device Admin Policy Sets"

Führen Sie innerhalb der Konfiguration des Richtlinienatzes einen Bildlauf nach unten durch, und erweitern Sie den Abschnitt Authentifizierungsrichtlinie.

Klicken Sie auf das Symbol Hinzufügen.

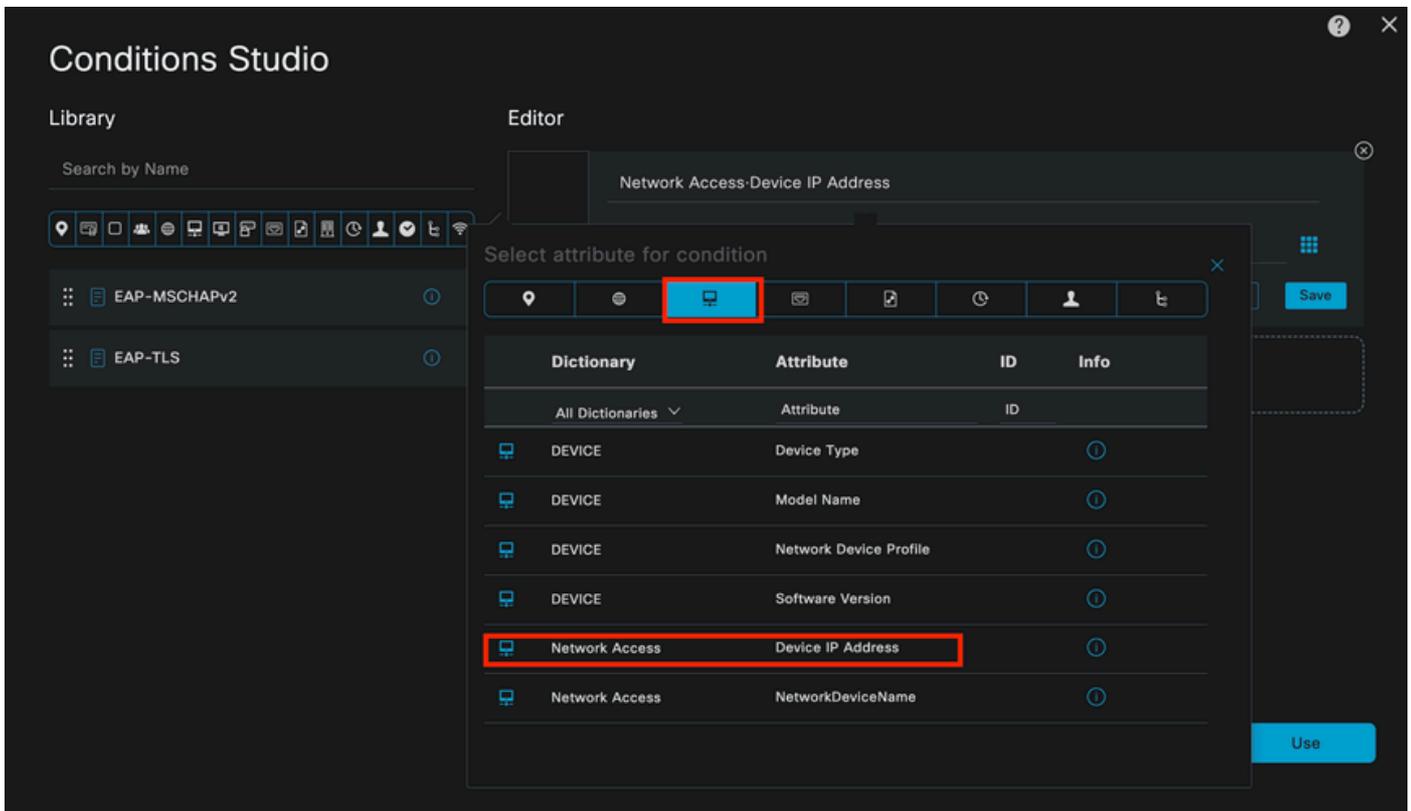
In diesem Konfigurationsbeispiel lautet der Name-Wert Internal Authentication (Interne Authentifizierung), und die ausgewählte Bedingung ist die IP-Adresse des Netzwerkgeräts (Nexus) (ersetzt A.B.C.D.). Diese Authentifizierungsrichtlinie verwendet den Identitätsspeicher für interne Benutzer.



Authentifizierungsrichtlinie

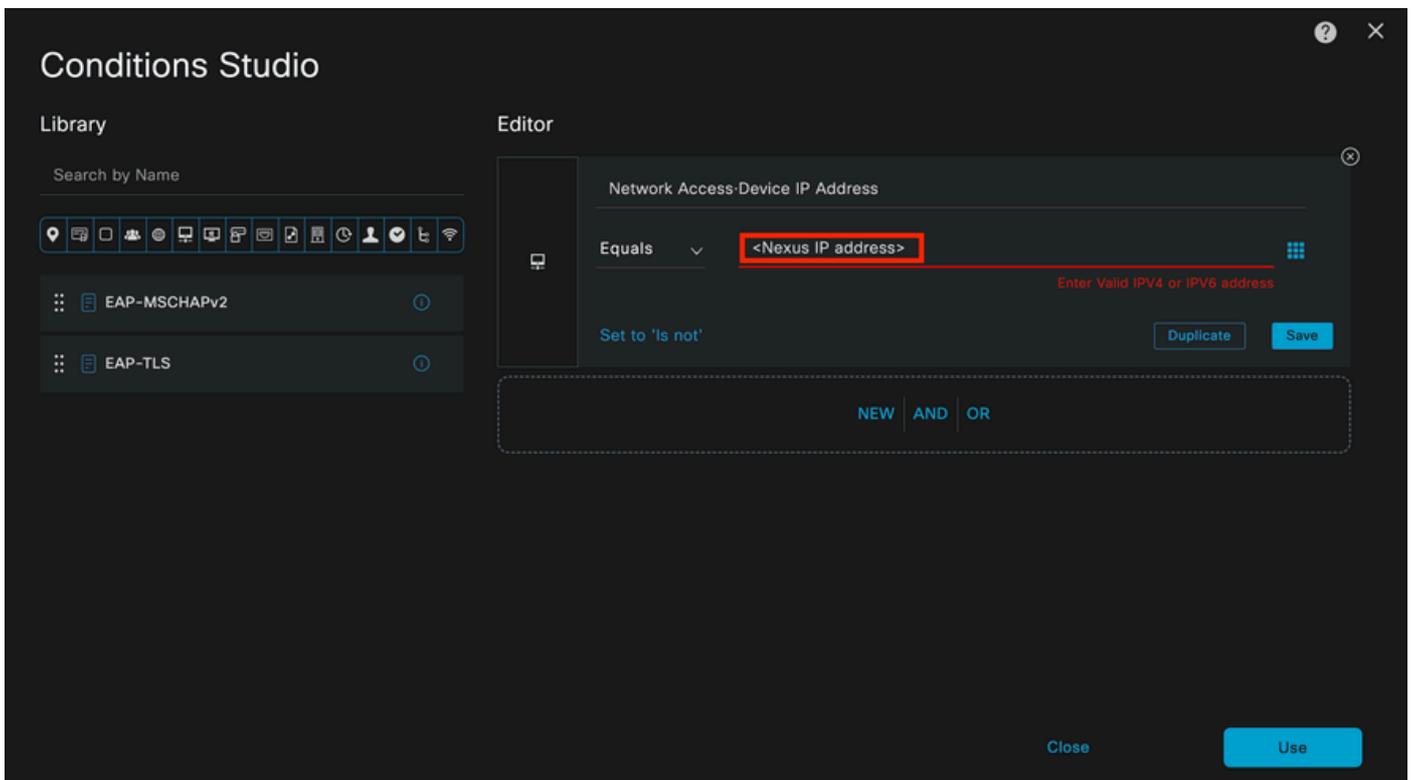
Hier sehen Sie, wie die Bedingung konfiguriert wurde.

Wählen Sie Network Access > Device IP address Dictionary Attribute aus.



Condition Studio für Authentifizierungsrichtlinien

Ersetzen Sie den Kommentar <Nexus IP address> durch die richtige IP.



Hinzufügen des IP-Filters

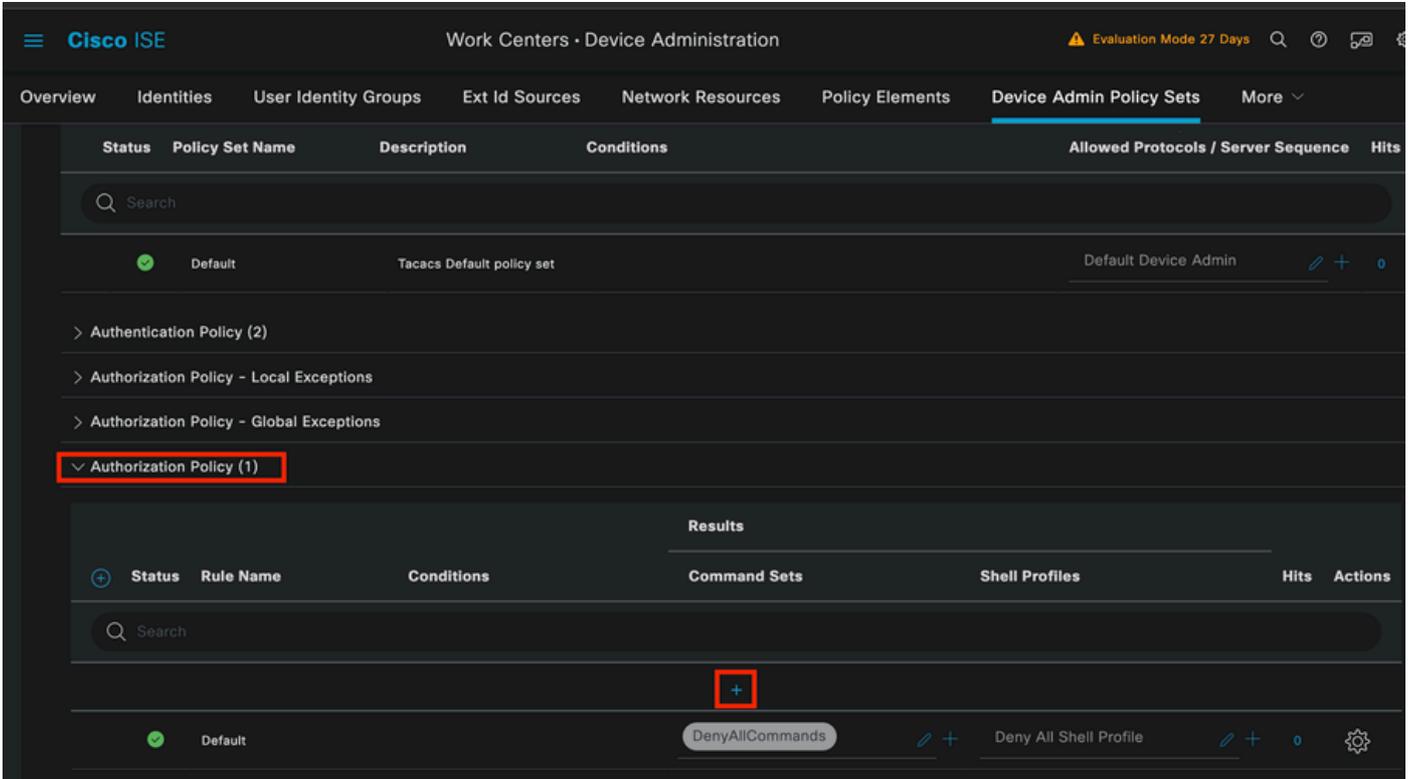
Klicken Sie auf die Schaltfläche Verwenden.

Diese Bedingung wird nur von dem von Ihnen konfigurierten Nexus-Gerät erfüllt. Wenn diese

Bedingung jedoch für eine große Anzahl von Geräten aktiviert werden soll, muss eine andere Bedingung berücksichtigt werden.

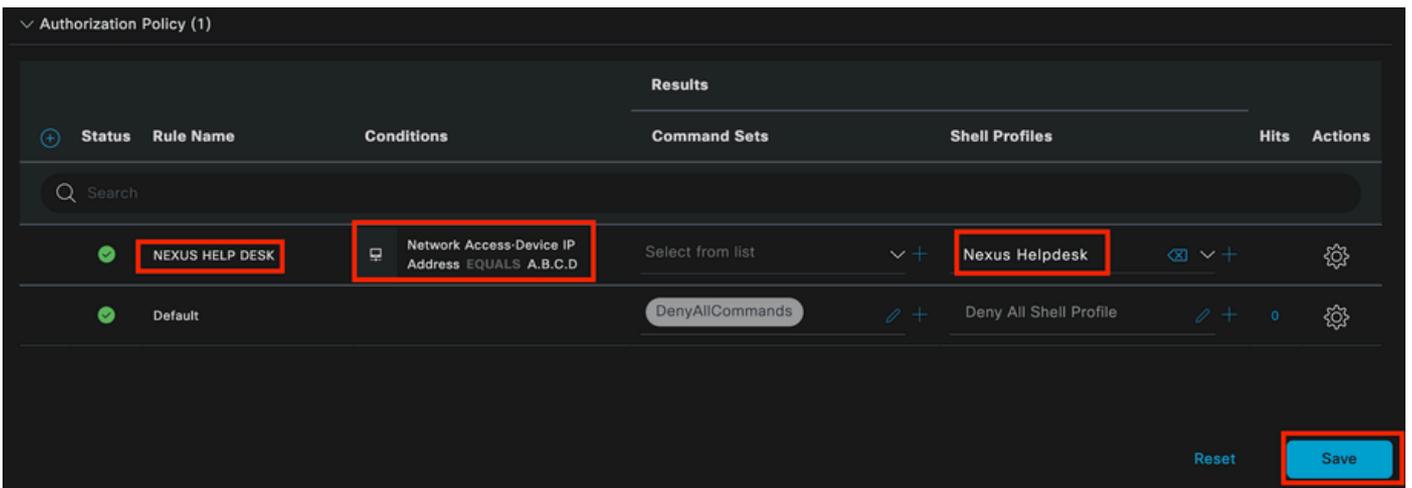
Navigieren Sie anschließend zum Abschnitt Autorisierungsrichtlinie, und erweitern Sie ihn.

Klicken Sie auf das Pluszeichen (+).



Abschnitt "Autorisierungsrichtlinie"

In diesem Beispiel wurde NEXUS HELP DESK als Name der Autorisierungsrichtlinie verwendet.



Condition Studio für Autorisierungsrichtlinien

Die in der Authentifizierungsrichtlinie konfigurierte Bedingung wird auch für die Autorisierungsrichtlinie verwendet.

In der Spalte Shell Profiles (Shell-Profil) wurde das Profil konfiguriert, bevor Nexus Helpdesk

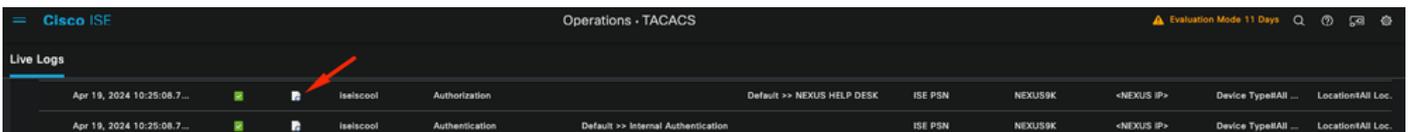
ausgewählt wurde.

Klicken Sie abschließend auf die Schaltfläche Speichern.

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Navigieren Sie in der ISE-GUI zu Operations > TACACS > Live Logs, geben Sie den Datensatz an, der mit dem verwendeten Benutzernamen übereinstimmt, und klicken Sie auf Live Log Detail (Live-Protokolldetail) des Autorisierungsereignisses.



TACACS-Live-Protokoll

Als Teil der Details, die dieser Bericht enthält, finden Sie einen Antwort-Abschnitt, in dem Sie sehen können, wie ISE den Wert `shell:roles="helpdesk"` zurückgibt.

Response

```
{Author-Reply-Status=PassRepl;  
AVPair=shell:roles=" helpdesk" ; }
```

Live-Protokolldetail-Antwort

Auf dem Nexus-Gerät:

```
Nexus9000 login: iseiscool  
Password: VainillaISE97
```

```
Nexus9000# conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Nexus9000(config)# interface ethernet 1/23  
% Interface permission denied
```

```
Nexus9000(config)# ?  
  interface  Configure interfaces  
  show      Show running system information  
  end       Go to exec mode  
  exit      Exit from command interpreter
```

```
Nexus9000(config)# role name test  
% Permission denied for the role
```

```
Nexus9000(config)#
```

```
Nexus9000(config)# interface loopback 0  
% Interface permission denied
```

```

Nexus9000(config)#
Nexus9000# conf t

Nexus9000(config)# interface ethernet 1/5
Notice that only the commands allowed are listed.
Nexus9000(config-if)# ?

no          Negate a command or set its defaults
show        Show running system information
shutdown    Enable/disable an interface
end         Go to exec mode
exit        Exit from command interpreter

Nexus9000(config-if)# cdp
Nexus9000(config-if)# cdp enable
% Permission denied for the role
Nexus9000(config-if)#

```

Fehlerbehebung

- Überprüfen Sie, ob die ISE vom Nexus-Gerät aus erreichbar ist.


```

Nexus9000# ping <Ihre ISE-IP>
PING <Ihre ISE IP> (<Ihre ISE IP> 56 Datenbytes
64 Bytes von <Ihre ISE-IP> : icmp_seq=0 ttl=59 time=1,22 ms
64 Bytes von <Ihre ISE-IP> : icmp_seq=1 ttl=59 time=0,739 ms
64 Bytes von <Ihre ISE IP> : icmp_seq=2 ttl=59 time=0,686 ms
64 Bytes von <Ihre ISE-IP> : icmp_seq=3 ttl=59 time=0,71 ms
64 Bytes von <Ihre ISE-IP> : icmp_seq=4 ttl=59 time=0,72 ms

```
- Stellen Sie sicher, dass der Port 49 zwischen der ISE und dem Nexus-Gerät geöffnet ist.


```

Nexus9000# Telnet <Ihre ISE-IP> 49
<Ihre ISE IP> wird versucht ...
Verbunden mit <Ihre ISE-IP> .
Das Escapezeichen ist '^]'.

```
- Verwenden Sie folgende Debugging-Optionen:

```

debug tacacs+ all
Nexus9000
Nexus9000# 2024 Apr 19 22:50:44.199329 tacacs: event_loop(): calls process_rd_fd_set
2024 Apr 19 22:50:44.199355 tacacs: process_rd_fd_set: callback for fd 6
2024 Apr 19 22:50:44.199392 takacs: fsrv didnt consume 8421 opcode
2024 Apr 19 22:50:44.199406 tacacs: process_implicit_cfs_session_start: input...
2024 Apr 19 22:50:44.199414 tacacs: process_implicit_cfs_session_start: exiting; we are in
distribution disabled state
2024 Apr 19 22:50:44.199424 tacacs: process_aaa_tplus_request: entry for aaa session id 0
2024 Apr 19 22:50:44.199438 tacacs: process_aaa_tplus_request:Checking for state of mgmt0
port with servergroup lsePsnServers
2024 Apr 19 22:50:44.199451 tacacs: tacacs_global_config(4220): input ...
2024 Apr 19 22:50:44.199466 tacacs: tacacs_global_config(4577): GET_REQ...

```

2024 Apr 19 22:50:44.208027 tacacs: tacacs_global_config(4701): got back the return value of global Protocol configuration operation:SUCCESS

2024 Apr 19 22:50:44.208045 tacacs: tacacs_global_config(4716): REQ:num server 0

2024 Apr 19 22:50:44.208054 tacacs: tacacs_global_config: REQ:num group 1

2024 Apr 19 22:50:44.208062 tacacs: tacacs_global_config: REQ:num timeout 5

2024 Apr 19 22:50:44.208070 tacacs: tacacs_global_config: REQ:num deadtime 0

2024 Apr 19 22:50:44.208078 tacacs: tacacs_global_config: REQ:num encryption_type 7

2024 Apr 19 22:50:44.208086 tacacs: tacacs_global_config: return retval 0

2024 Apr 19 22:50:44.208098 tacacs: process_aaa_tplus_request:group_info is populated in aaa_req, so Using servergroup lsePsnServers

2024 Apr 19 22:50:44.208108 tacacs: tacacs_servergroup_config: input für server group, index 0

2024 Apr 19 22:50:44.208117 tacacs: tacacs_servergroup_config: GETNEXT_REQ for Protocol server group index:0 name:

2024 Apr 19 22:50:44.208148 tacacs: tacacs_pss2_move2key: rcode = 40480003 syserr2str = kein solcher pss key

2024 Apr 19 22:50:44.208160 tacacs: tacacs_pss2_move2key: calls pss2_getkey

2024 Apr 19 22:50:44.208171 tacacs: tacacs_servergroup_config: GETNEXT_REQ got Protocol server group index:2 name:lsePsnServers

2024 Apr 19 22:50:44.208184 tacacs: tacacs_servergroup_config: got back the return value of Protocol group operation:SUCCESS

2024 Apr 19 22:50:44.208194 tacacs: tacacs_servergroup_config: return retval 0 for Protocol server group:lsePsnServers

2024 Apr 19 22:50:44.208210 tacacs: process_aaa_tplus_request: Group lsePsnServers found. entsprechendes vrf ist default, source-intf ist 0

2024 Apr 19 22:50:44.208224 tacacs: process_aaa_tplus_request: testing for mgmt0 vrf:management against vrf:default of requested group

2024 Apr 19 22:50:44.208256 tacacs: process_aaa_tplus_request:mgmt_if 83886080

2024 Apr 19 22:50:44.208272 tacacs: process_aaa_tplus_request:global_src_intf : 0, local src_intf ist 0 und vrf_name ist default

2024 Apr 19 22:50:44.208286 tacacs: create_tplus_req_state_machine(902): entry for aaa session id 0

2024 Apr 19 22:50:44.208295 tacacs: state machine count 0

2024 Apr 19 22:50:44.208307 tacacs: init_tplus_req_state_machine: entry for aaa session id 0

2024 Apr 19 22:50:44.208317 tacacs: init_tplus_req_state_machine(1298):tplus_ctx is NULL it should be if author and test

2024 Apr 19 22:50:44.208327 tacacs: tacacs_servergroup_config: entry for server grouplsePsnServers, index 0

2024 Apr 19 22:50:44.208339 tacacs: tacacs_servergroup_config: GET_REQ für Protokoll-Servergruppenindex:0 name:lsePsnServers

2024 Apr 19 22:50:44.208357 tacacs: find_tacacs_servergroup: entry for server group lsePsnServers

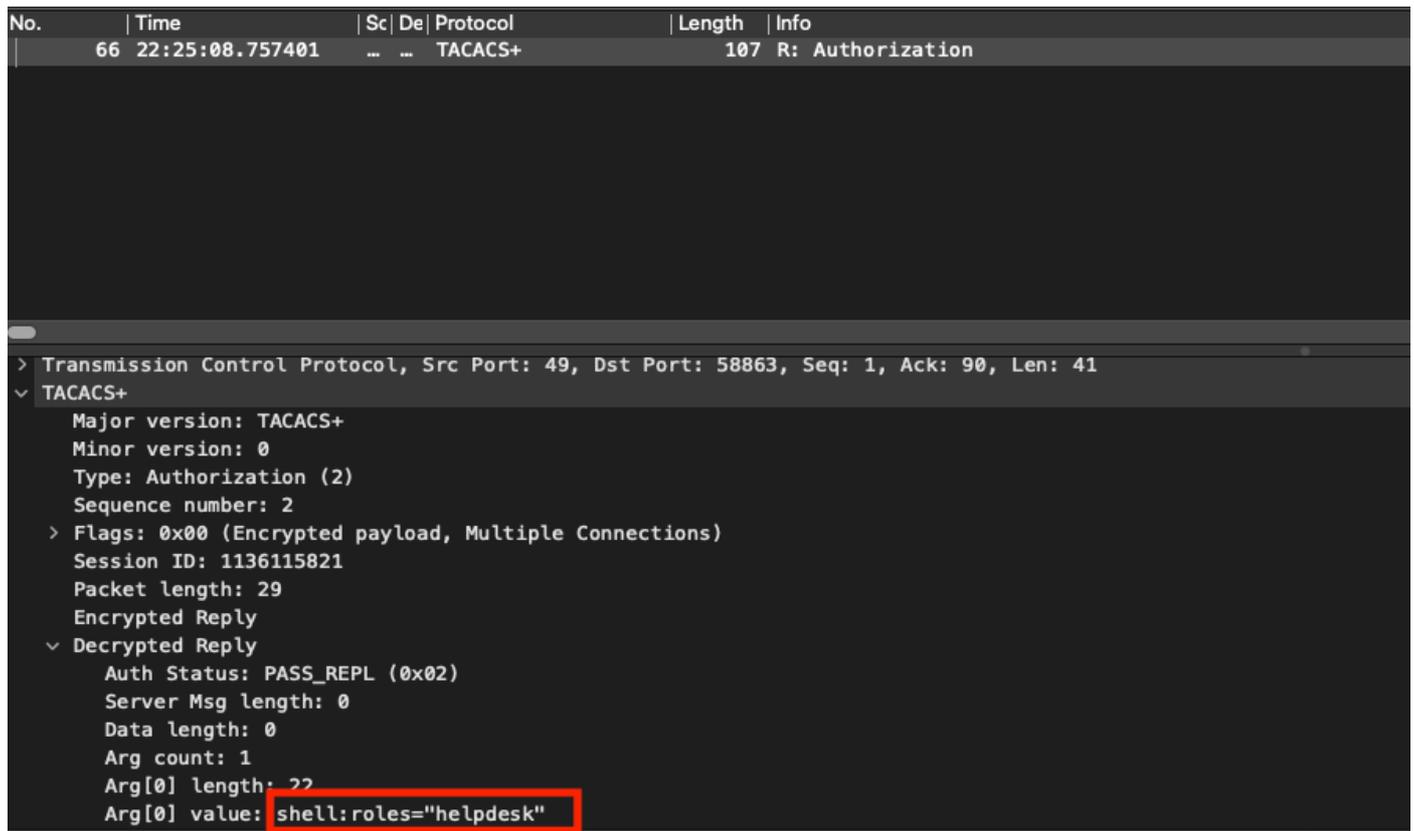
2024 Apr 19 22:50:44.208372 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCESS

2024 Apr 19 22:50:44.208382 tacacs: find_tacacs_servergroup: exiting for server group lsePsnServers index is 2

2024 Apr 19 22:50:44.208401 tacacs: tacacs_servergroup_config: GET_REQ: find_tacacs_servergroup error 0 for Protocol server group lsePsnServers

2024 Apr 19 22:50:44.208420 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCESS
2024 Apr 19 22:50:44.208433 tacacs: tacacs_servergroup_config: GET_REQ got Protocol server
group index:2 name:lsePsnServers
2024 A2024 19. April 2022:52024 19. April 2022:52024 19. April 22:5
Nexus9000

- Führen Sie eine Paketerfassung durch (Um die Paketdetails anzuzeigen, müssen Sie die Wireshark TACACS+-Einstellungen ändern und den von Nexus und der ISE verwendeten gemeinsamen Schlüssel aktualisieren).



```
No. | Time | Sc | De | Protocol | Length | Info
---|---|---|---|---|---|---
66 | 22:25:08.757401 | ... | ... | TACACS+ | 107 | R: Authorization

> Transmission Control Protocol, Src Port: 49, Dst Port: 58863, Seq: 1, Ack: 90, Len: 41
  TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 2
    > Flags: 0x00 (Encrypted payload, Multiple Connections)
    Session ID: 1136115821
    Packet length: 29
    Encrypted Reply
    Decrypted Reply
      Auth Status: PASS_REPL (0x02)
      Server Msg length: 0
      Data length: 0
      Arg count: 1
      Arg[0] length: 22
      Arg[0] value: shell:roles="helpdesk"
```

TACACS-Autorisierungspaket

- Überprüfen Sie, ob der gemeinsame Schlüssel auf ISE- und Nexus-Seite identisch ist. Dies kann auch in Wireshark überprüft werden.

TACACS+

```
Major version: TACACS+
Minor version: 1
Type: Authentication (1)
Sequence number: 1
Flags: 0x00 (Encrypted payload, Multiple Connections)
Session ID: 232251350
Packet length: 43
Encrypted Request
Decrypted Request
  Action: Inbound Login (1)
  Privilege Level: 1
  Authentication type: PAP (2)
  Service: Login (1)
  User len: 9
  User: iseiscool
  Port len: 1
  Port: 0
  Remaddr len: 12
  Remote Address: [REDACTED]
  Password Length: 13
  Password: VainillaISE97
```

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.