

Konfigurieren von TACACS+ mit ISE Gigabit Ethernet 1-Schnittstelle

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration der Identity Services Engine für TACACS+](#)

[Konfigurieren der IP-Adresse für die Gigabit Ethernet 1-Schnittstelle in der ISE](#)

[Gerätemanagement in ISE aktivieren](#)

[Hinzufügen eines Netzwerkgeräts zur ISE](#)

[Konfigurieren von TACACS+-Befehlssätzen](#)

[Konfigurieren des TACACS+-Profils](#)

[Konfigurieren des TACACS+-Authentifizierungs- und Autorisierungsprofils](#)

[Konfigurieren von Netzwerkzugriffsbenutzern für die TACACS-Authentifizierung von NAD in der ISE](#)

[Konfigurieren des Routers für TACACS+](#)

[Konfigurieren des Cisco IOS-Routers für die TACACS+-Authentifizierung und -Autorisierung](#)

[Switch für TACACS+ konfigurieren](#)

[Switch für TACACS+-Authentifizierung und -Autorisierung konfigurieren](#)

[Verifizierung](#)

[Überprüfung vom Router](#)

[Verifizierung des Switches](#)

[Fehlerbehebung](#)

[Überprüfung durch das Netzwerkgerät \(Switch\)](#)

[Überprüfung durch das Netzwerkgerät \(Switch\)](#)

[Referenz](#)

Einleitung

In diesem Dokument wird die ISE TACACS+-Konfiguration mit Gigabit Ethernet 1-Schnittstelle beschrieben, bei der Router und Switch als Netzwerkgeräte fungieren.

Hintergrundinformationen

Die Cisco ISE unterstützt bis zu 6 Ethernet-Schnittstellen. Es kann nur drei Bonds haben: Bond 0,

Bond 1 und Bond 2. Sie können die Schnittstellen, die Teil einer Bond-Beziehung sind, oder die Rolle der Schnittstelle in einer Bond-Beziehung ändern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

- Grundlegendes Netzwerkwissen
- Cisco Identity Service Engine

Verwendete Komponenten

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

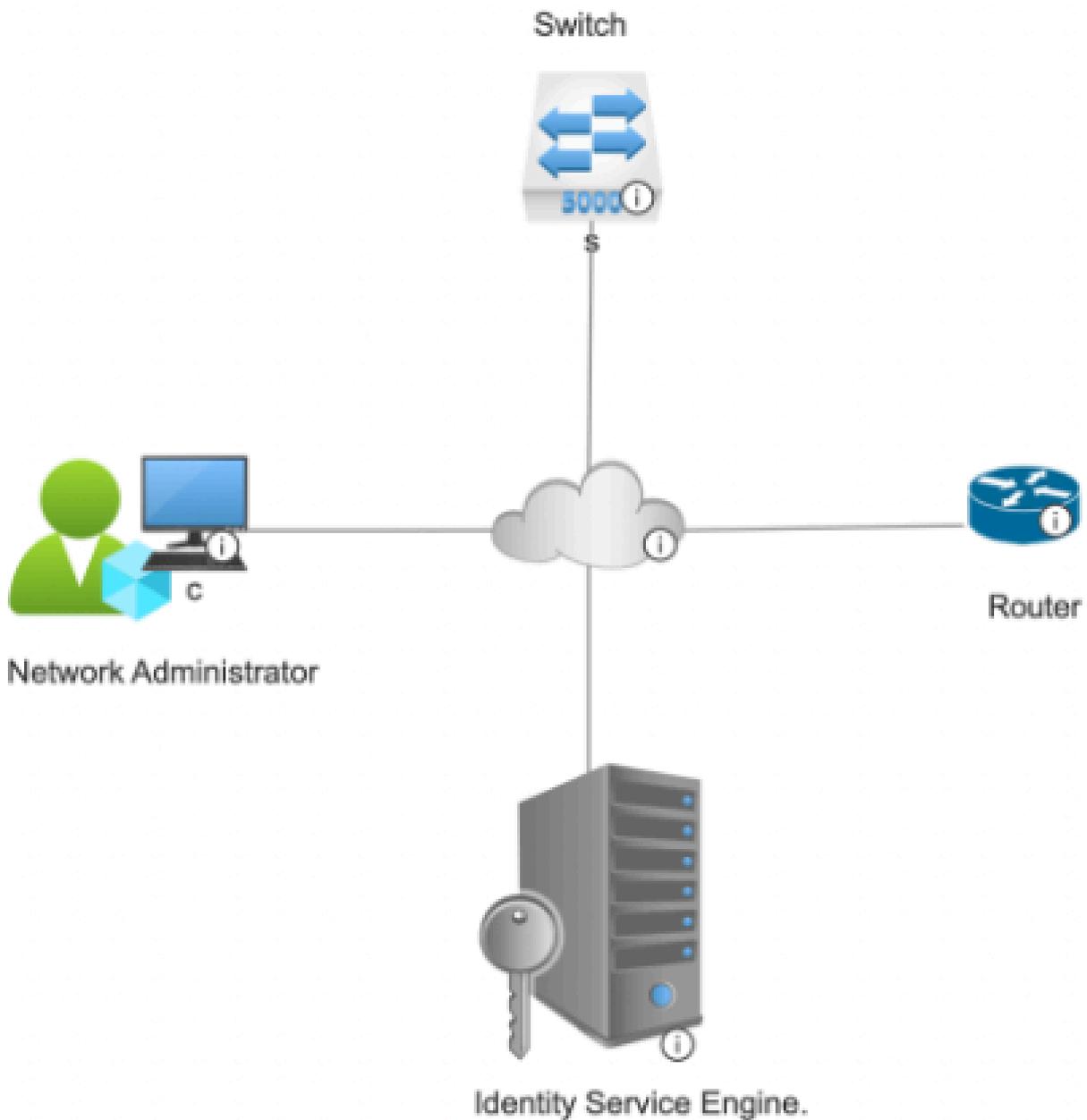
- Cisco Identity Service Engine v3.3
- Cisco IOS® Softwareversion 17.x
- Cisco Switch C9200

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.

Konfigurieren

Ziel der Konfiguration ist es, Konfigurieren von Gigabit Ethernet 1 der ISE für TACACS+ und Authentifizieren von Switch und Router mit TACACS+ mit ISE als Authentifizierungsserver.

Netzwerkdiagramm



Netzwerktopologie

Konfiguration der Identity Services Engine für TACACS+

Konfigurieren der IP-Adresse für die Gigabit Ethernet 1-Schnittstelle in der ISE

1. Melden Sie sich bei der CLI des ISE PSN-Knotens an, auf dem Device admin aktiviert ist, und überprüfen Sie die verfügbaren Schnittstellen mit dem Befehl `show interface`:

```
honey/admin# show interface
```

```
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 100.233.1.1 netmask 255.255.255.0 broadcast 100.233.1.255  
inet6 fe80::8ca9:c4ff:fe1b:6827 prefixlen 64 scopeid 0x20<link>  
ether 8e:a9:c4:1b:68:27 txqueuelen 1000 (Ethernet)  
RX packets 629139 bytes 226044590 (215.5 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 674817 bytes 100272799 (95.6 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 100.233.2 netmask 255.255.255.0 broadcast 100.233.1.255  
inet6 fd00::1:8:1 prefixlen 112 scopeid 0x0<global>  
inet6 fe80::304a:47ff:fe59:264a prefixlen 64 scopeid 0x20<link>  
ether 32:4a:47:59:26:4a txqueuelen 1000 (Ethernet)  
RX packets 438392 bytes 363642766 (346.7 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 481076 bytes 369977760 (352.8 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
GigabitEthernet 0
```

```
flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 10.233.30.13 netmask 255.255.255.0 broadcast 10.233.30.255  
inet6 fe80::250:56ff:fe8b:1b81 prefixlen 64 scopeid 0x20<link>  
ether 00:50:56:8b:1b:81 txqueuelen 1000 (Ethernet)  
RX packets 1271564 bytes 203676256 (194.2 MiB)  
RX errors 0 dropped 266 overruns 0 frame 0  
TX packets 76672 bytes 116577841 (111.1 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
GigabitEthernet 1
```

```
flags=4098<BROADCAST,MULTICAST> mtu 1500  
ether 00:50:56:8b:e1:af txqueuelen 1000 (Ethernet)  
RX packets 262 bytes 36180 (35.3 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 7 bytes 606 (606.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
GigabitEthernet 2
```

```
flags=4098<BROADCAST,MULTICAST> mtu 1500  
ether 00:50:56:8b:f8:5f txqueuelen 1000 (Ethernet)  
RX packets 268 bytes 36228 (35.3 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 6 bytes 516 (516.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



Anmerkung: In dieser Konfiguration werden nur drei Schnittstellen in der ISE konfiguriert, wobei der Schwerpunkt auf der Gigabit Ethernet 1-Schnittstelle liegt. Das gleiche Verfahren kann angewendet werden, um die IP-Adresse für alle Schnittstellen zu konfigurieren. Standardmäßig unterstützt die ISE bis zu sechs Gigabit Ethernet-Schnittstellen.

2. Weisen Sie der Gigabit Ethernet 1-Schnittstelle über die CLI desselben PSN-Knotens eine IP-Adresse zu. Verwenden Sie hierzu die folgenden Befehle:

```
hostnameImage#configure t
```

```
hostnameOise/admin(config)#interface Gigabit Ethernet 1
```

```
hostnameOise/admin(config-GigabitEthernet-1)#<IP-Adresse> <Subnetzmaske> % Wenn Sie die IP-Adresse ändern, werden die ISE-Dienste möglicherweise neu gestartet.
```

Mit IP-Adressänderung fortfahren?

Fortfahren? [ja, nein] ja

3. Bei der Durchführung von Schritt 2 werden die ISE-Knotendienste neu gestartet. Um den Status der ISE-Dienste zu überprüfen, führen Sie den Befehl `show application status ise` aus, und stellen Sie sicher, dass der Status der Dienste wie in diesem Screenshot dargestellt ausgeführt wird:

```
honey/admin#show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	1739169
Database Server	running	102 PROCESSES
Application Server	running	1755746
Profiler Database	running	1746379
ISE Indexing Engine	running	1757121
AD Connector	running	1759148
M&T Session Database	running	1752122
M&T Log Processor	running	1755926
Certificate Authority Service	running	1759026
EST Service	running	1786647
SXP Engine Service	disabled	
TC-NAC Service	disabled	
PassiveID WMI Service	disabled	
PassiveID Syslog Service	disabled	
PassiveID API Service	disabled	
PassiveID Agent Service	disabled	
PassiveID Endpoint Service	disabled	
PassiveID SPAN Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	1743222
ISE API Gateway Database Service	running	1745409
ISE API Gateway Service	running	1750887
ISE pxGrid Direct Service	running	1874179
Segmentation Policy Service	disabled	
REST Auth Service	disabled	
SSE Connector	disabled	
Hermes (pxGrid Cloud Agent)	disabled	
McTrust (Meraki Sync Service)	disabled	
ISE Node Exporter	running	1760519
ISE Prometheus Service	running	1762540
ISE Grafana Service	running	1765779
ISE MNT LogAnalytics Elasticsearch	running	1768218
ISE Logstash Service	running	1773207
ISE Kibana Service	running	1774914
ISE Native IPsec Service	running	1779658
MFC Profiler	running	1932013

Überprüfung des ISE-Servicestatus

4. Überprüfen Sie die IP-Adresse der Gig1-Schnittstelle mit dem Befehl `show interface`:

```

honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 10.100.20.1 netmask 255.255.255.0 broadcast 10.100.20.255
  inet6 fe80::8ca9:c4ff:fe1b:6827 prefixlen 64 scopeid 0x20<link>
  ether 8e:a9:c4:1b:68:27 txqueuelen 1000 (Ethernet)
  RX packets 633876 bytes 228753800 (218.1 MiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 680052 bytes 102100762 (97.3 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 10.100.20.1 netmask 255.255.255.0 broadcast 10.100.20.255
  inet6 fd00::1:8:1 prefixlen 112 scopeid 0x0<global>
  inet6 fe80::304a:47ff:fe59:264a prefixlen 64 scopeid 0x20<link>
  ether 32:4a:47:59:26:4a txqueuelen 1000 (Ethernet)
  RX packets 503576 bytes 516105026 (492.1 MiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 595701 bytes 383404526 (365.6 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

GigabitEthernet 0
  flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 10.100.20.56 netmask 255.255.255.0 broadcast 10.100.20.255
  inet6 fe80::250:56ff:fe8b:1b81 prefixlen 64 scopeid 0x20<link>
  ether 00:50:56:8b:1b:81 txqueuelen 1000 (Ethernet)
  RX packets 1387052 bytes 213478717 (203.5 MiB)
  RX errors 0 dropped 266 overruns 0 frame 0
  TX packets 136494 bytes 261900250 (249.7 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

GigabitEthernet 1
  flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 10.100.20.56 netmask 255.255.255.0 broadcast 10.100.20.255
  inet6 fe80::250:56ff:fe8b:e1af prefixlen 64 scopeid 0x20<link>
  ether 00:50:56:8b:e1:af txqueuelen 1000 (Ethernet)
  RX packets 5165 bytes 1072036 (1.0 MiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 28 bytes 2260 (2.2 KiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Überprüfung der IP-Adresse der ISE Gig2-Schnittstelle von CLI

5. Überprüfen Sie die Toleranz von Port 49 im ISE-Knoten mithilfe der Show-Ports. | inc 49 Befehl:

```

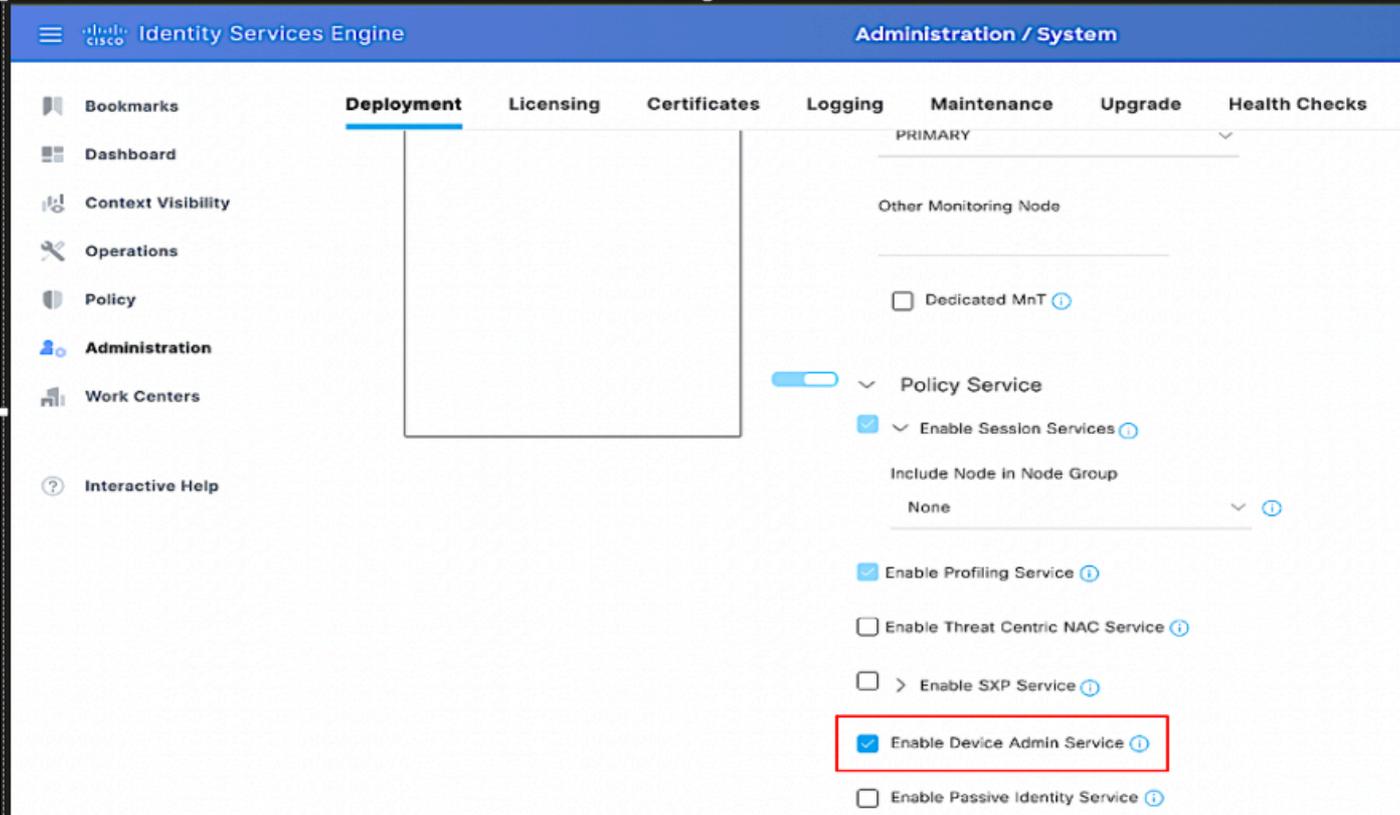
honey/admin#show ports | include 49
tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, 10.100.20.56:49,

```

Überprüfung der Zulassung von Port 49 in der ISE

Gerätemanagement in ISE aktivieren

Navigieren Sie zu GUI of ISE > Administration > Deployment > Wählen Sie den PSN-Knoten aus, und aktivieren Sie dann Enable Device Admin Service:



The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The 'Deployment' tab is selected, and the 'Enable Device Admin Service' checkbox is checked and highlighted with a red box. The interface includes a navigation menu on the left with options like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Help. The main content area shows the 'Deployment' tab with a 'PRIMARY' dropdown menu, 'Other Monitoring Node', 'Dedicated MnT', 'Policy Service' (checked), 'Enable Session Services', 'Include Node in Node Group' (None), 'Enable Profiling Service', 'Enable Threat Centric NAC Service', 'Enable SXP Service', 'Enable Device Admin Service' (checked), and 'Enable Passive Identity Service'.

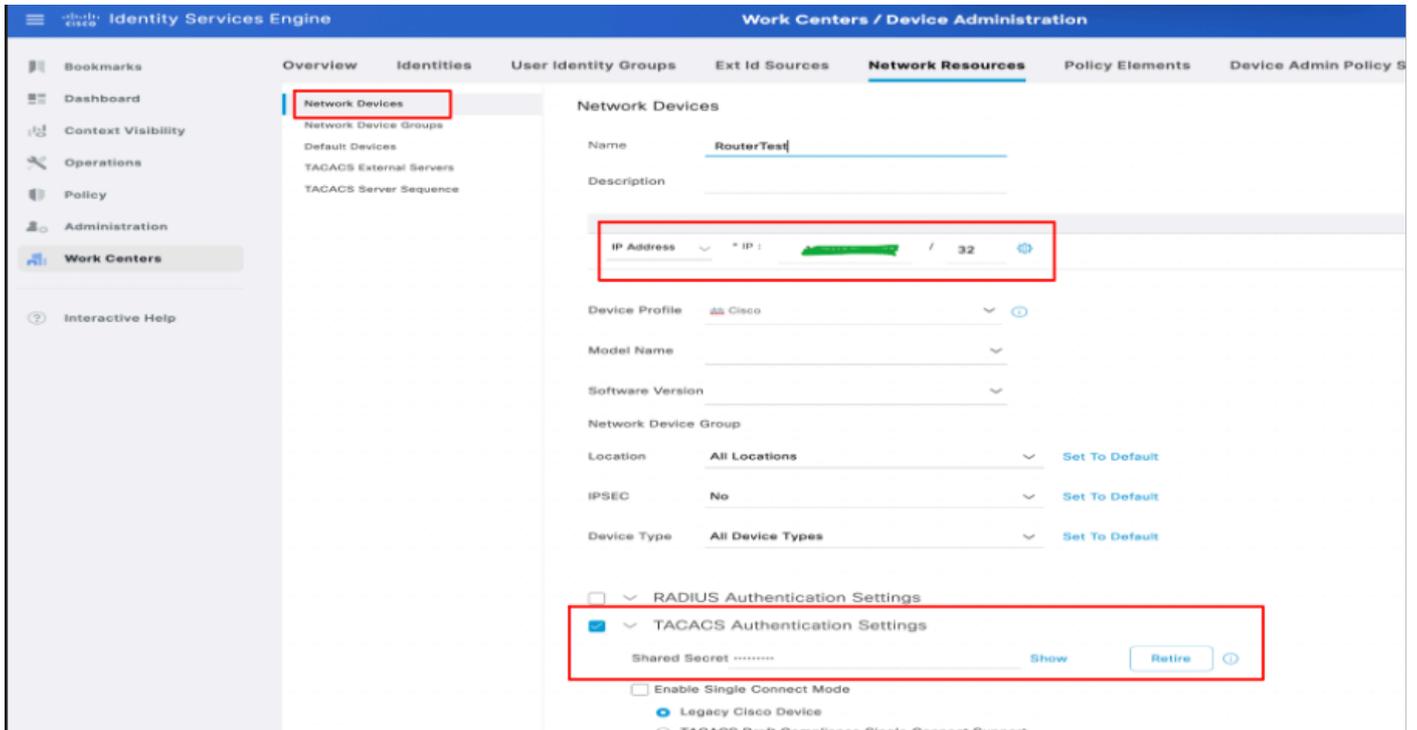
Aktivieren des Geräteverwaltungsdiensts in der ISE



Anmerkung: Um den Geräteverwaltungsdienst zu aktivieren, ist eine Geräteverwaltungslizenz erforderlich.

Hinzufügen eines Netzwerkgeräts zur ISE

1. Navigieren Sie zu Work Centers > Device Administration > Network Resources > Network Devices. Klicken Sie auf Hinzufügen. Geben Sie einen Namen und eine IP-Adresse ein. Aktivieren Sie das Kontrollkästchen TACACS+-Authentifizierungseinstellungen, und geben Sie den Schlüssel für den gemeinsamen geheimen Schlüssel an.



Konfiguration von Netzwerkgeräten in der ISE

2. Befolgen Sie die obige Prozedur, um alle erforderlichen Netzwerkgeräte für die TACACS-Authentifizierung hinzuzufügen.

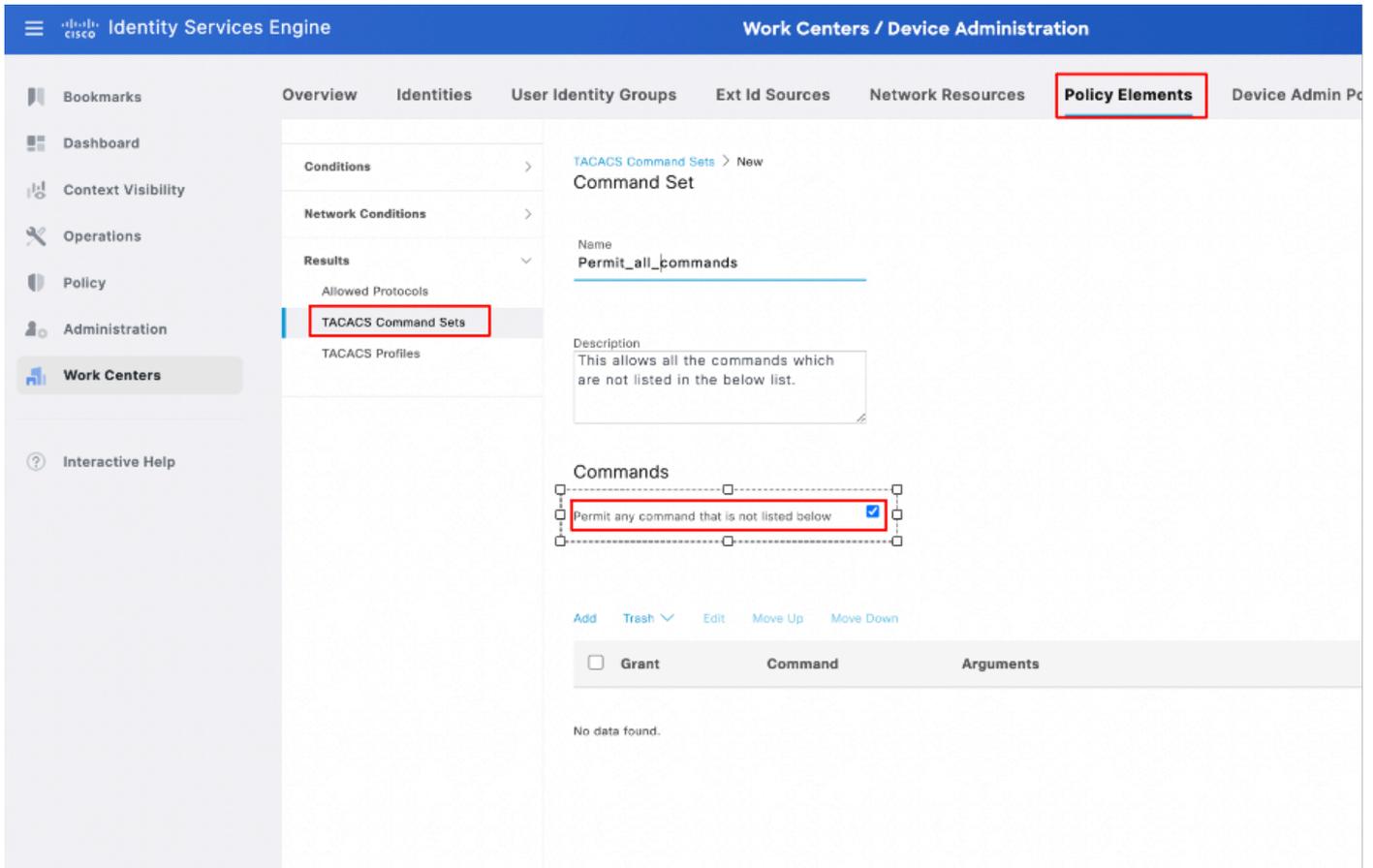
Konfigurieren von TACACS+-Befehlssätzen

Für diese Demonstration wurden zwei Befehlssätze konfiguriert:

Permit_all_commands, wird dem Benutzer admin zugewiesen und lässt alle Befehle auf dem Gerät zu.

permit_show_commands, wird einem Benutzer zugewiesen und lässt nur show-Befehle zu.

1. Navigieren Sie zu Work Centers > Device Administration > Policy Results > TACACS Command Sets. Klicken Sie auf Add. Geben Sie den Namen PermitAllCommands an, und aktivieren Sie dann das Kontrollkästchen Alle Befehle zulassen, die nicht aufgeführt sind. Klicken Sie auf Senden.



Konfiguration von Befehlssätzen in der ISE

2. Navigieren Sie zu Work Centers > Device Administration > Policy Results > TACACS Command Sets. Klicken Sie auf Add. Geben Sie den Namen PermitShowCommands ein, klicken Sie auf Add, und klicken Sie abschließend auf Allow show und exit Befehle. Wenn Argumente leer gelassen werden, sind standardmäßig alle Argumente enthalten. Klicken Sie auf Senden.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Device Administration'. The left sidebar contains various navigation options, with 'Work Centers' selected. The main content area shows the configuration for a TACACS Command Set named 'permit_show_commands'. The configuration includes a description: 'Only commands which are added in the below list are allowed.' and a table of commands. The table has columns for 'Grant', 'Command', and 'Arguments'. The commands listed are PERMIT, DENY, and PERMIT, with arguments 'exit', 'Config', and 'show' respectively. The 'Grant' column contains checkboxes, and the 'Arguments' column contains edit icons.

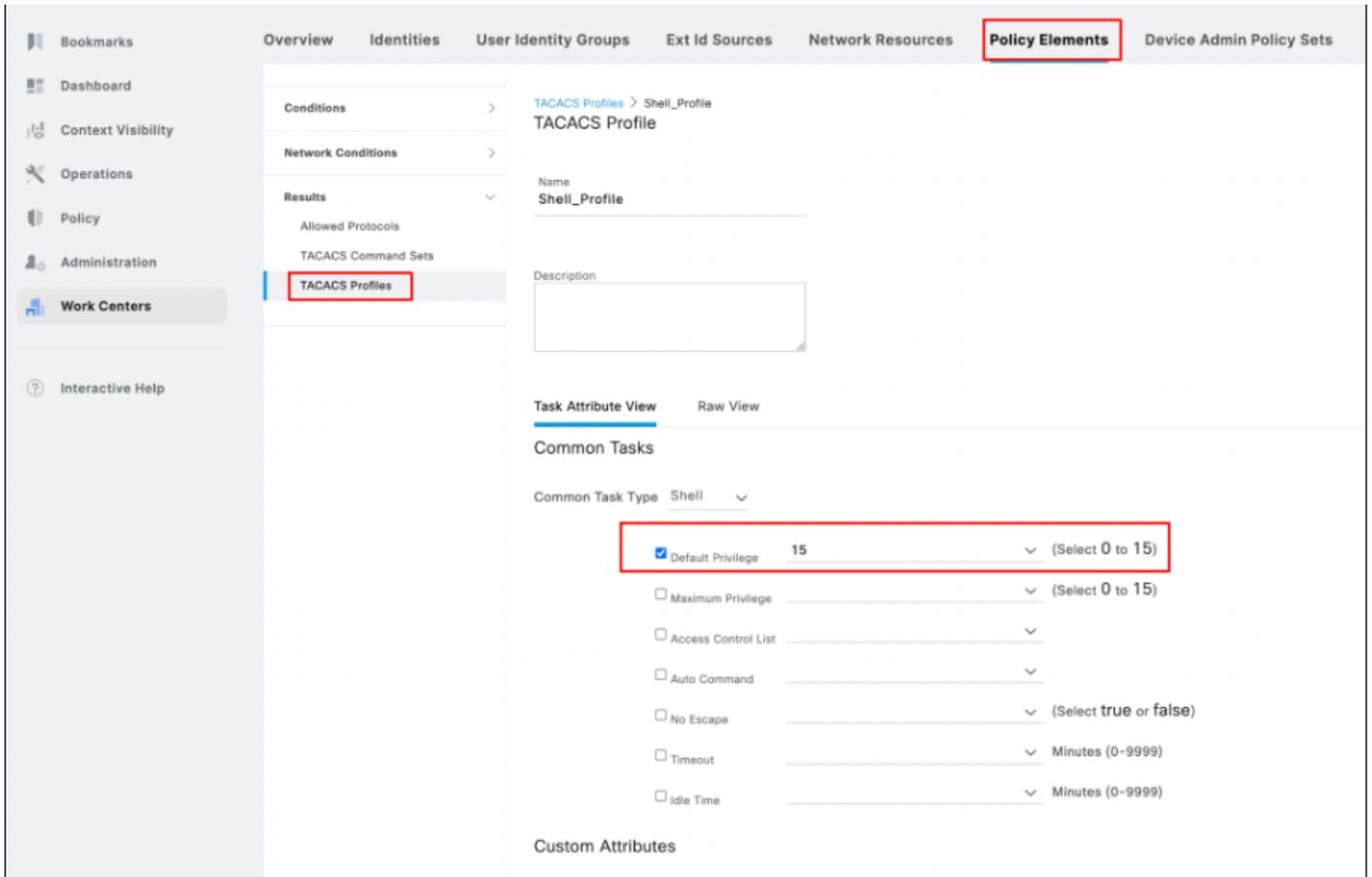
Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	exit
<input type="checkbox"/>	DENY	Config
<input type="checkbox"/>	PERMIT	show

Konfiguration von permit_show_commands in der ISE

Konfigurieren des TACACS+-Profils

Es wird ein einzelnes TACACS+-Profil konfiguriert, und die Befehlsautorisierung wird über Befehlsätze durchgeführt.

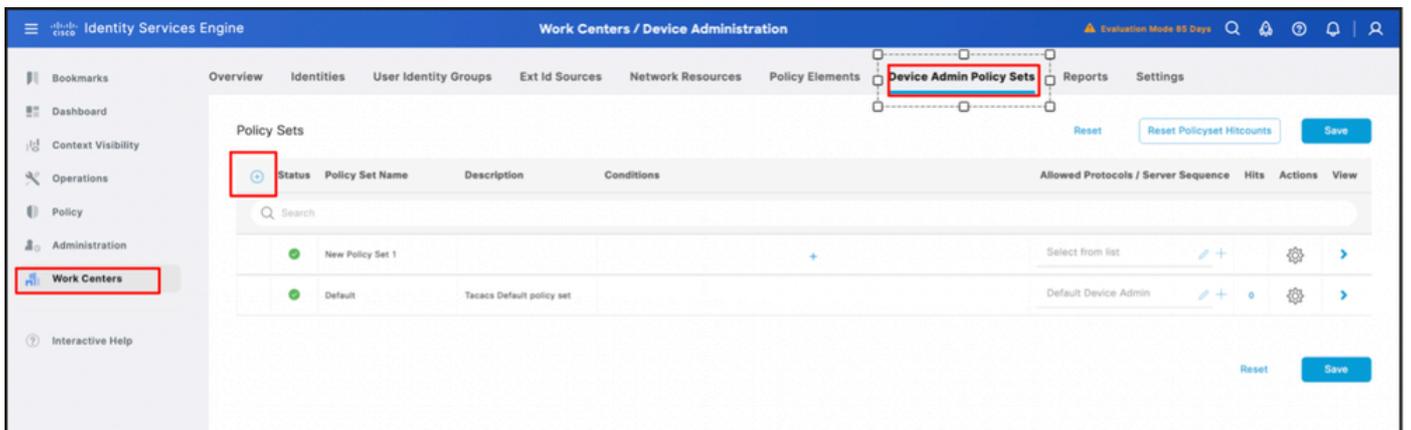
Um ein TACACS+-Profil zu konfigurieren, navigieren Sie zu Work Centers > Device Administration > Policy Results > TACACS Profiles. Klicken Sie auf Hinzufügen, geben Sie einen Namen für das Shell-Profil an, aktivieren Sie das Kontrollkästchen Standardberechtigung, und geben Sie den Wert 15 ein. Klicken Sie abschließend auf Senden.



Konfiguration des TACACS-Profiles in der ISE

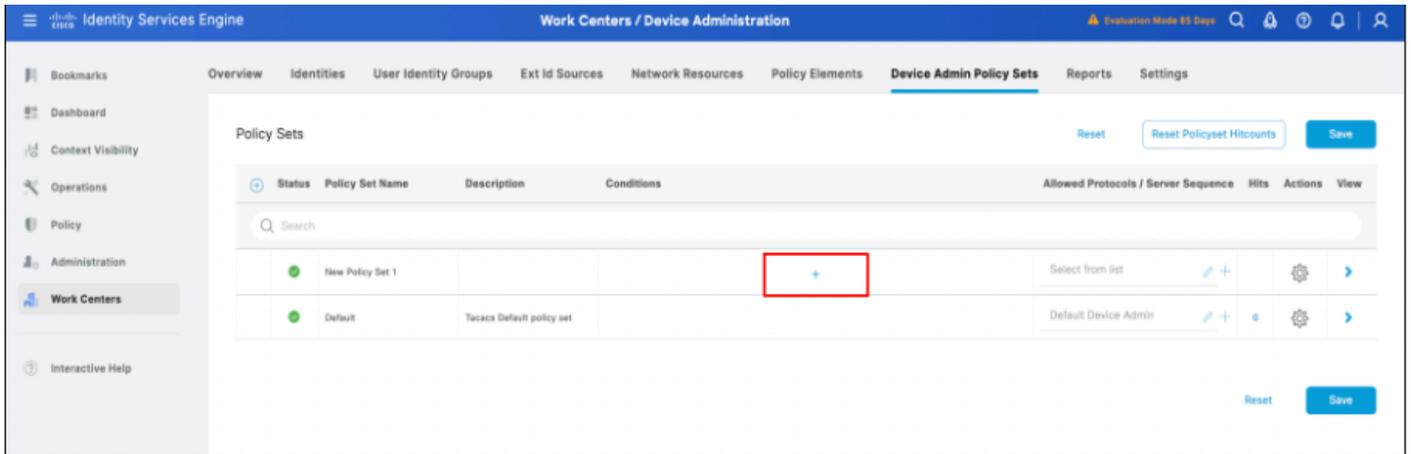
Konfigurieren des TACACS+-Authentifizierungs- und Autorisierungsprofils

1. Melden Sie sich bei der ISE PAN-GUI an -> Administration -> Work Centers -> Device Administration -> Device Admin Policy Sets. Klicken Sie auf das + (Plus)-Symbol, um eine neue Richtlinie zu erstellen. In diesem Fall erhält der Richtlinienatz den Namen Neuer Richtlinienatz 1.



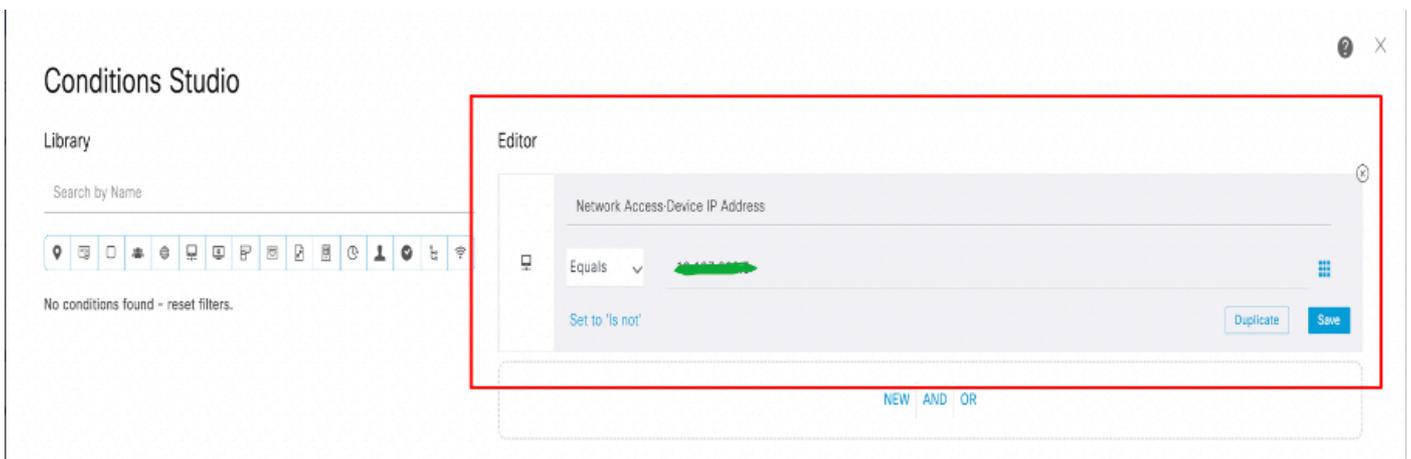
Konfiguration des Richtlinienatzes in ISE

2. Vor dem Speichern des Richtlinienatzes müssen die Bedingungen konfiguriert werden, wie in diesem Screenshot gezeigt. Klicken Sie auf das + (Plus)-Symbol, um die Bedingungen für den Richtlinienatz zu konfigurieren.

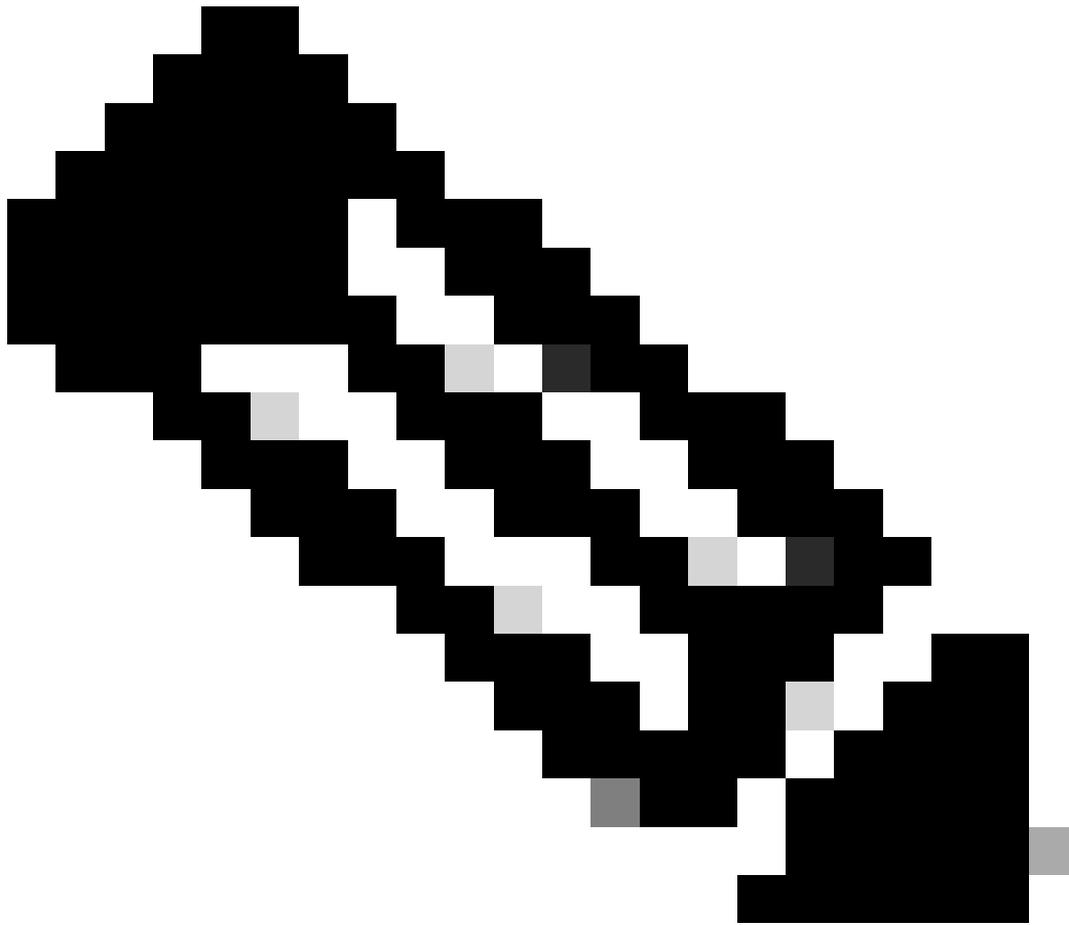


Konfiguration von Policy Set-Bedingungen in der ISE

3. Nachdem Sie auf das Symbol + (Plus) geklickt haben, wie in Schritt 2 erwähnt, wird das Dialogfeld Bedingungen Studio geöffnet. Konfigurieren Sie dort die erforderlichen Bedingungen. Speichern Sie die Bedingung mit den neuen oder vorhandenen Bedingungen, und führen Sie einen Bildlauf durch. Klicken Sie auf Verwenden.

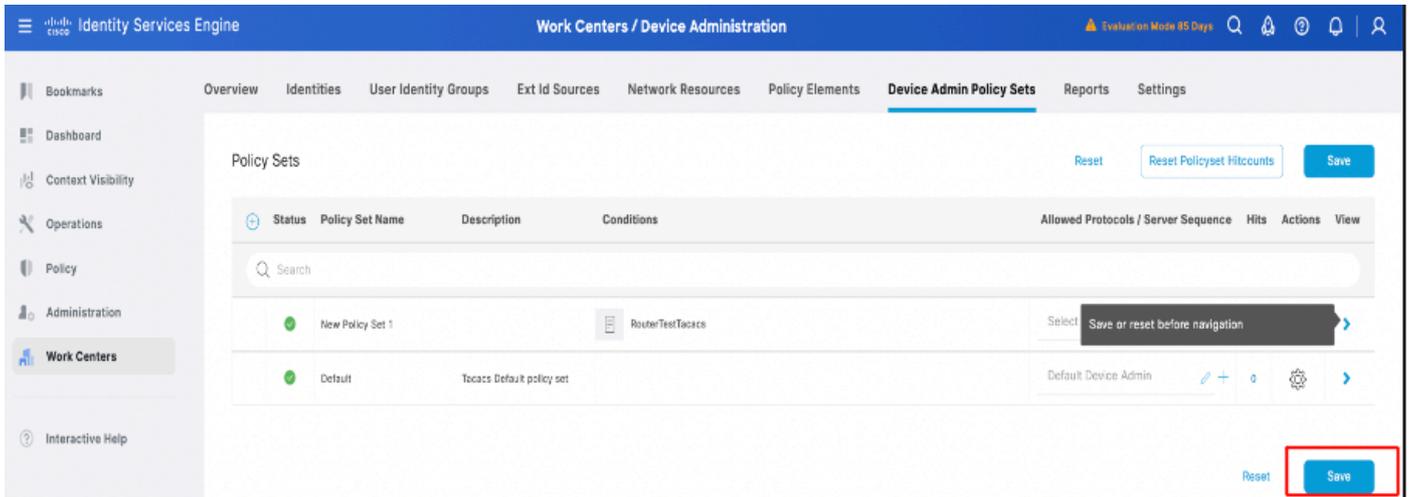


Konfiguration von Policy Set-Bedingungen in der ISE



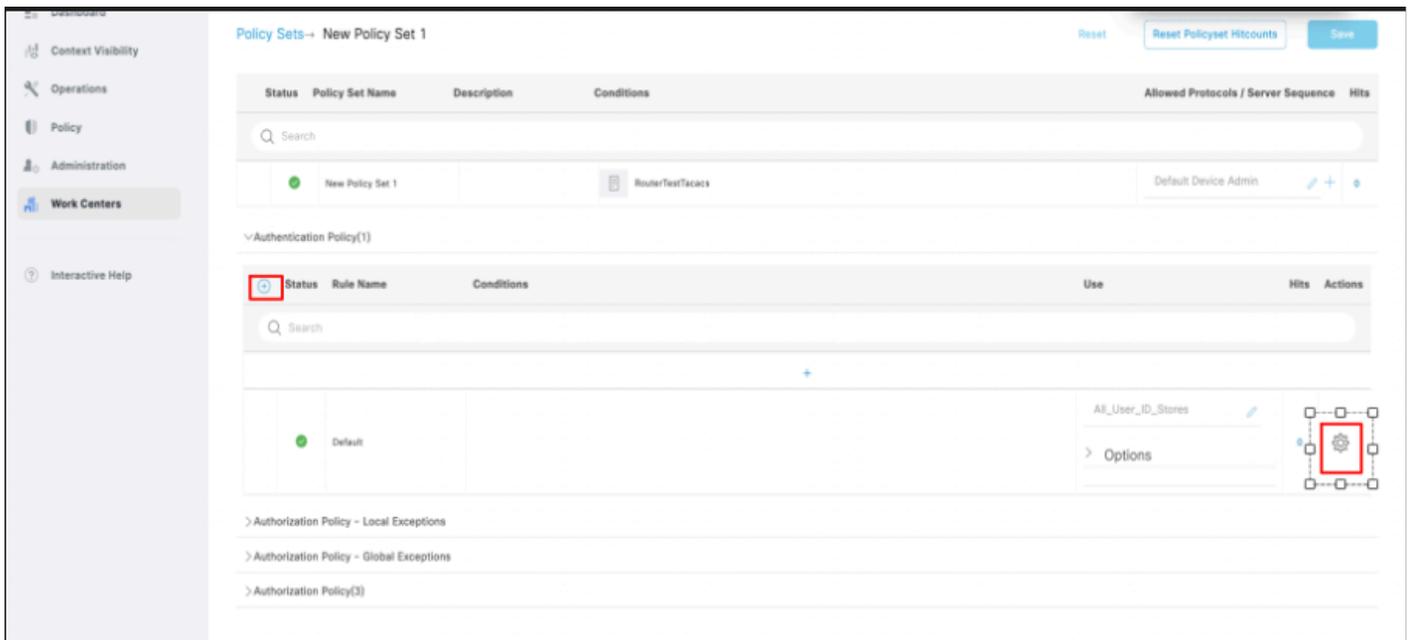
Anmerkung: In dieser Dokumentation stimmen die Bedingungen mit der IP des Netzwerkgeräts überein. Die Bedingungen können jedoch je nach Bereitstellungsanforderungen variiert werden.

4. Nachdem die Bedingungen konfiguriert und gespeichert wurden, konfigurieren Sie zulässige Protokolle als Standardgeräteadministrator. Speichern Sie den Richtliniensatz, der durch Klicken auf die Option Speichern erstellt wurde.



Bestätigung der Konfiguration des Policy Sets.

5. Erweitern Sie den Satz Neue Richtlinie -> Authentifizierungsrichtlinie (1) -> Erstellen Sie eine neue Authentifizierungsrichtlinie, indem Sie auf das Symbol + (plus) klicken oder auf das Zahnradsymbol und dann oben eine neue Zeile einfügen klicken.

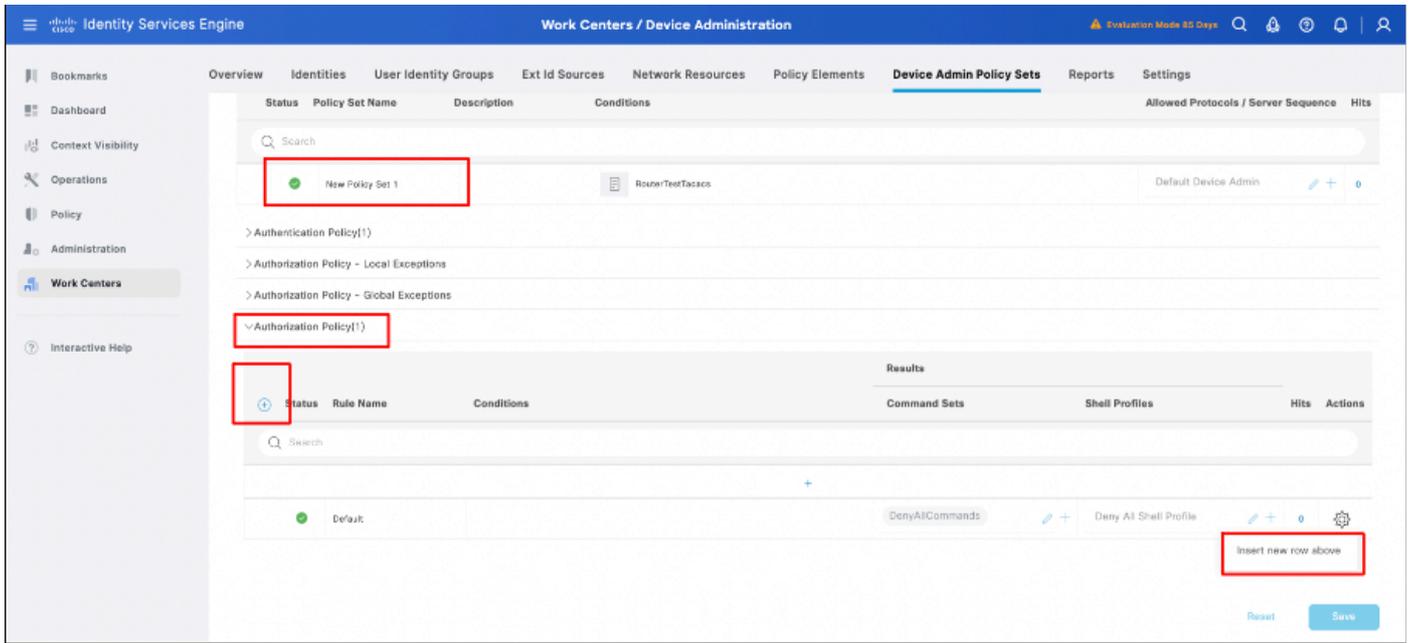


Konfiguration der Authentifizierungsrichtlinie im Richtlinienatz



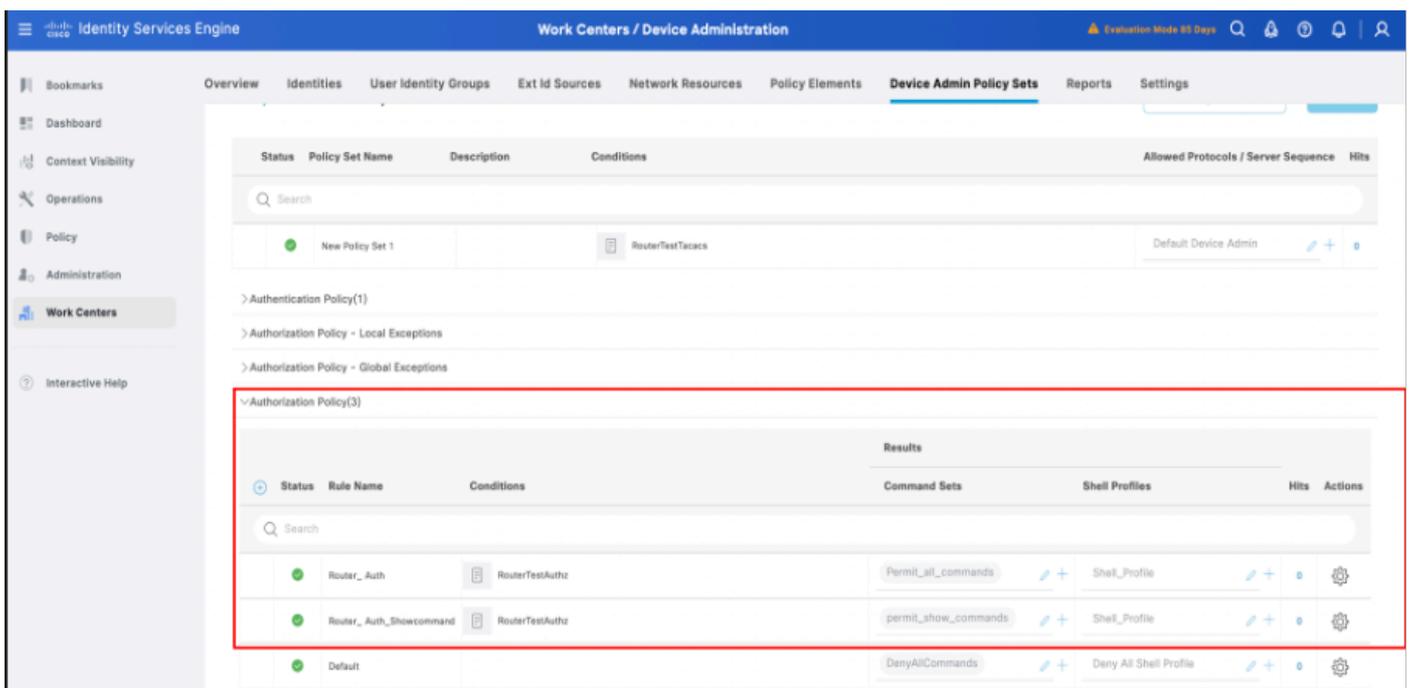
Anmerkung: Für diese Demonstration wird die standardmäßige Authentifizierungsrichtlinie mit "All_User_ID_Stores" verwendet. Die Verwendung der Identitätsdaten kann jedoch an die jeweiligen Bereitstellungsanforderungen angepasst werden.

6. Erweitern Sie den Satz Neue Richtlinie -> Autorisierungsrichtlinie (1). Klicken Sie entweder auf das + (Plus)-Symbol, oder klicken Sie auf das Zahnrad-Symbol. Fügen Sie dann oben eine neue Zeile zum Erstellen einer Autorisierungsrichtlinie ein.



Konfiguration der Autorisierungsrichtlinie

7. Konfigurieren Sie die Autorisierungsrichtlinie mit Bedingungen, Befehlsätzen und Shell-Profilen, die den Autorisierungsrichtlinien zugeordnet sind.



Vollständige Konfiguration der Autorisierungsrichtlinie in der ISE

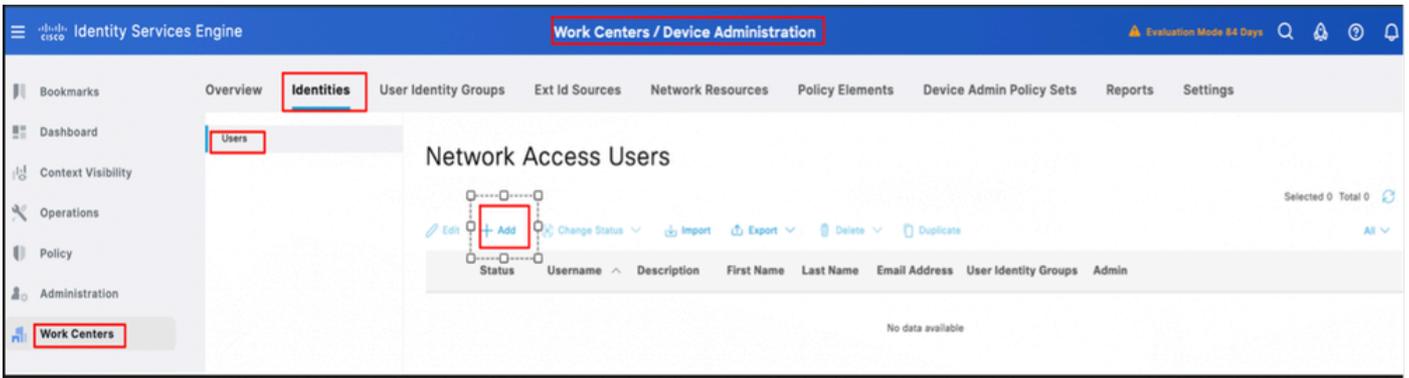


Anmerkung: Die konfigurierten Bedingungen entsprechen den Vorgaben für die Laborumgebung und können entsprechend den Bereitstellungsanforderungen konfiguriert werden.

8. Führen Sie die ersten 6 Schritte zum Konfigurieren der Richtlinienätze für den Switch oder ein anderes Netzwerkgerät aus, das für TACACS+ verwendet wird.

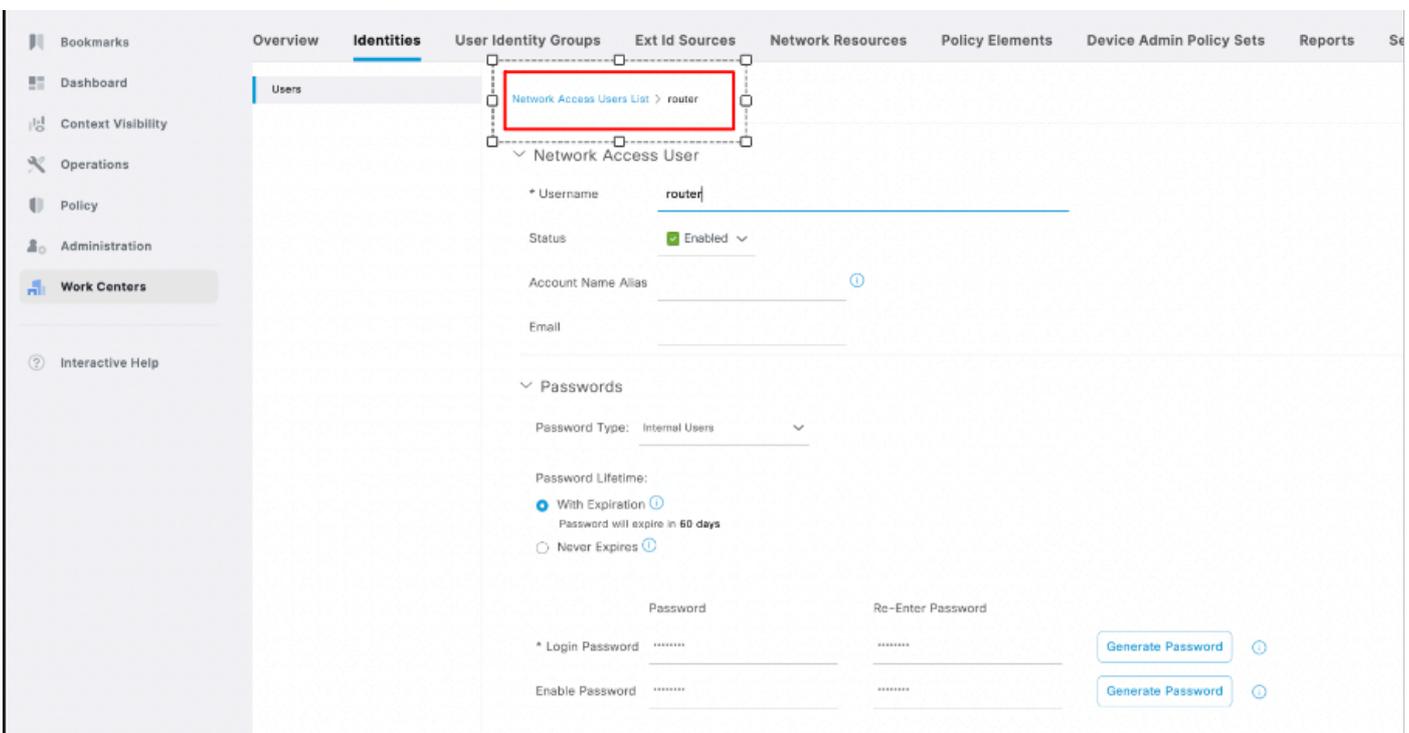
Konfigurieren von Netzwerkzugriffsbenutzern für die TACACS-Authentifizierung von NAD in der ISE

1. Navigieren Sie zu Workcenter -> Device Administration -> Identities -> Users. Klicken Sie auf das +(Plus)-Symbol, um einen neuen Benutzer zu erstellen.



Netzwerkzugriffsbutzer in der ISE konfigurieren

2. Geben Sie an, um die Details zu Benutzernamen und Kennwort zu erweitern, ordnen Sie den Benutzer einer Benutzeridentitätsgruppe zu (optional), und klicken Sie dann auf Senden.



Netzwerkzugriffsbutzer konfigurieren - Fortfahren

3. Nachdem Sie die Konfiguration des Benutzernamens in Work Centers -> Identitäten -> Benutzer -> Netzwerkzugriffsbutzer übermittelt haben, wird der Benutzer sichtbar konfiguriert und aktiviert.



Bestätigung der Benutzerkonfiguration für den Netzwerkzugriff.

Konfigurieren des Routers für TACACS+

Konfigurieren des Cisco IOS-Routers für die TACACS+-Authentifizierung und -Autorisierung

1. Melden Sie sich bei der CLI des Routers an, und führen Sie diese Befehle aus, um TACACS auf dem Router zu konfigurieren.

ASR1001-X(config)#aaa new-model - Befehl erforderlich, um aaa in NAD zu aktivieren

ASR1001-X(config)#aaa Sitzungs-ID gemeinsam. —Befehl erforderlich, um aaa in NAD zu aktivieren.

ASR1001-X(config)#aaa Authentifizierung Anmeldung Standardgruppe TACACS+ lokal

ASR1001-X(config)#aaa Autorisierung mit Standardgruppen-TACACS+

ASR1001-X(config)#aaa Autorisierung Netzwerkliste1 Gruppentaketen+

ASR1001-X(config)#tacacs server ise1

ASR1001-X(config-server-tacacs)#address ipv4 <IP-Adresse des TACACS-Servers > . — ISE-Schnittstelle G1 IP-Adresse.

ASR1001-X(config-server-tacacs)# Schlüssel XXXXX

ASR1001-X(config)# aaaa Group Server TACACS+ isegroup

ASR1001-X(config-sg-tacacs+)#server name ise1

ASR1001-X(config-sg-tacacs+)#ip vrf forwarding Mgmt-intf

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet0

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet1

ASR1001-X(Konfiguration)#exit

2. Nachdem Sie die TACACS+-Konfigurationen des Routers gespeichert haben, überprüfen Sie die TACACS+-Konfiguration mit dem Befehl show run aaa.

```
ASR1001-X#show run aaa
```

```
!
```

```
aaa Authentifizierung Anmeldung Standardgruppe isegroup lokal
```

```
aaa, Autorisierung, exec, Standardgruppenisegruppe
```

```
aaa, Autorisierungsnetzwerkliste1, Gruppenisegruppe
```

```
Benutzername admin Kennwort 0 XXXXXXXX
```

```
!
```

```
TACACS-Server ISE1
```

```
address ipv4 <IP-Adresse des TACACS-Servers>
```

```
Schlüssel XXXXX
```

```
!
```

```
!
```

```
aaa group server tacacs+ isegroup
```

```
Servername ise1
```

```
IP-VRF-Weiterleitung Mgmt-intf
```

```
ip tacacs source-interface GigabitEthernet1
```

```
!
```

```
!
```

```
!
```

```
aaa neues Modell
```

```
aaa, Sitzungs-ID gemeinsam
```

```
!
```

```
!
```

Switch für TACACS+ konfigurieren

Switch für TACACS+-Authentifizierung und -Autorisierung konfigurieren

1. Melden Sie sich bei der CLI des Switches an, und führen Sie diese Befehle aus, um TACACS im Switch zu konfigurieren.

```
C9200L-48P-4X#konfigurieren
```

Geben Sie die Konfigurationsbefehle ein, einen pro Zeile. Beenden Sie mit STRG+Z.

```
C9200L-48P-4X(config)#aaa neues Modell. — Befehl erforderlich, um aaa in NAD zu aktivieren
```

```
C9200L-48P-4X(config)#aaa Sitzungs-ID gemeinsam. — Befehl erforderlich, um aaa in NAD zu aktivieren.
```

```
C9200L-48P-4X(config)#aaa Authentifizierung Anmeldung Standardgruppe ISGroup lokal
```

```
C9200L-48P-4X(config)#aaa Autorisierung exec Standardgruppe isegroup
```

```
C9200L-48P-4X(config)#aaa Autorisierung Netzwerkliste1 Gruppe isegroup
```

```
C9200L-48P-4X(config)#tacacs server ise1
```

```
C9200L-48P-4X(config-server-tacacs)#address ipv4 <IP-Adresse des TACACS-Servers> - IP-Adresse der ISE-Schnittstelle G1.
```

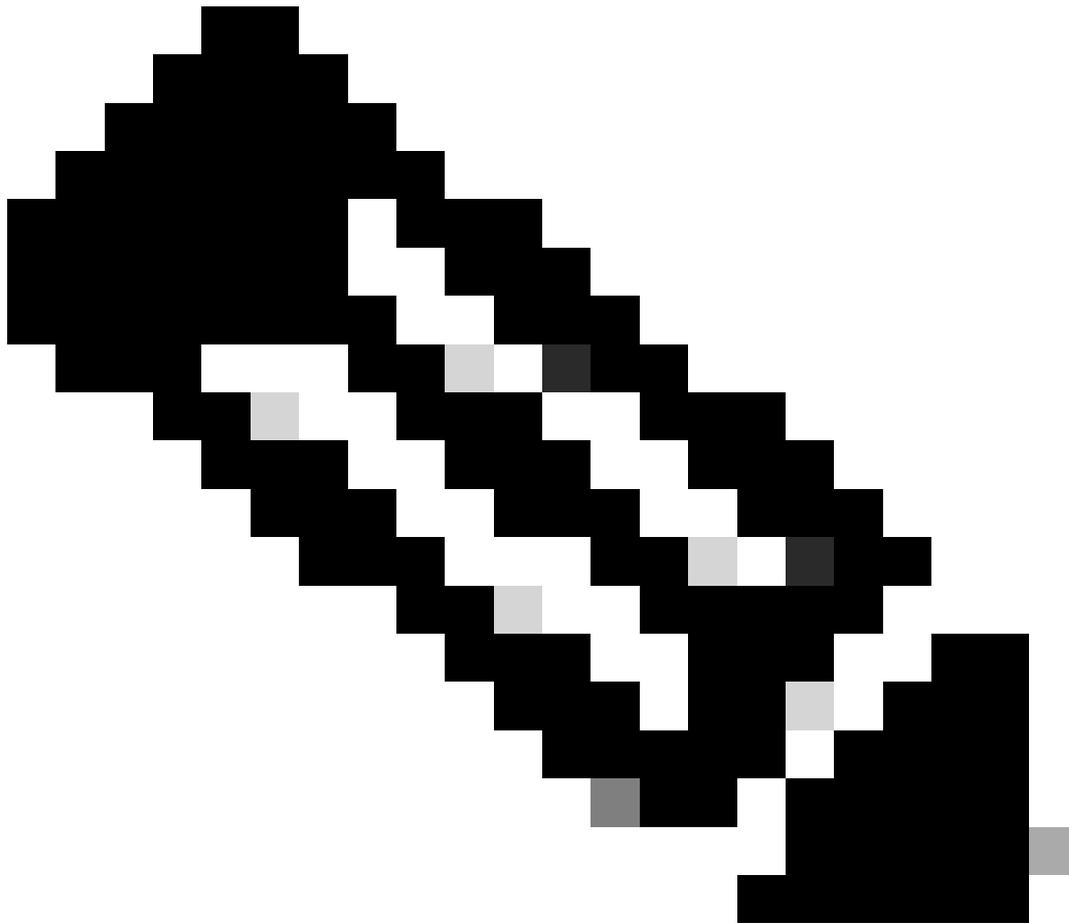
```
C9200L-48P-4X(config-server-tacacs)#key XXXXX
```

```
C9200L-48P(config)#aaa Gruppenserver TACACS+ Isogruppe
```

```
C9200L-48P(config-sg-tacacs+)#server name ise1
```

```
C9200L-48P-4X(Konfiguration)#exit
```

```
C9200L-48P-4X#wr mem
```



Anmerkung: In der NAD TACACS+-Konfiguration ist tacacs+ die Gruppe, die entsprechend den Bereitstellungsanforderungen angepasst werden kann.

2. Nachdem Sie die TACACS+-Konfigurationen des Switches gespeichert haben, überprüfen Sie die TACACS+-Konfiguration mit dem Befehl `show run aaa`.

```
C9200L-48P#show run aaa
```

```
!
```

```
aaa Authentifizierung Anmeldung Standardgruppe isegroup lokal
```

```
aaa, Autorisierung, exec, Standardgruppenisegruppe
```

```
aaa, Autorisierungsnetzwerkliste1, Gruppenisegruppe
```

```
Benutzername admin Kennwort 0 XXXXX
```

!

!

TACACS-Server ISE1

address ipv4 <IP-Adresse des TACACS-Servers>

Schlüssel XXXXX

!

!

aaa group server tacacs+ isegroup

Servername ise1

!

!

!

aaa neues Modell

aaa, Sitzungs-ID gemeinsam

!

!

Verifizierung

Überprüfung vom Router

Echtheitsauthentifizierung von TACACS+ gegenüber ISE mit Gigabit Ethernet 1-Schnittstelle über die CLI des Routers mit dem Befehl `test aaa group tacacsgroupname username password new`

Die Beispielausgabe von Router und ISE lautet wie folgt:

Verifizierung von Port 49 vom Router:

ASR1001-X#telnet ISE Gig 1-Schnittstelle IP 49

Es wird versucht, ISE G1g 1-Schnittstellen-IP, 49... Offen

ASR1001-X#test aaa group isegroup router XXXX neu

Kennwort wird gesendet

Benutzer erfolgreich authentifiziert

BENUTZERATTRIBUTE

Benutzername 0 "Router"

Antwortnachricht 0 "Kennwort:"

Melden Sie sich zur ISE-Verifizierung in den Live-Protokollen von GUI -> Operations -> TACACS an, und filtern Sie dann im Feld "Network Device Details" (Netzwerkgerätedetails) nach der Router-IP.

The screenshot displays the Cisco ISE interface with two main panels: 'Overview' and 'Authentication Details' on the left, and 'Steps' on the right.

Overview:

Request Type	Authentication
Status	Pass
Session Key	honey/530520237/15
Message Text	Passed-Authentication: Authentication succeeded
Username	router
Authentication Policy	New Policy Set 1 >> Default
Selected Authorization Profile	Shell_Profile

Authentication Details:

Generated Time	2025-03-06 05:52:51.374000 +00:00
Logged Time	2025-03-06 05:52:51.374
Epoch Time (sec)	1741240371
ISE Node	honey
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	router
Network Device Name	RouterTest
Network Device IP	[REDACTED]
Network Device Groups	IPSEC#Is IPSEC Device#No.Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	

Steps:

- 13013 Received TACACS+ Authentication START Request
- 15049 Evaluating Policy Group (Step latency=2ms)
- 15008 Evaluating Service Selection Policy (Step latency=0ms)
- 15048 Queried PIP - Network Access.Device IP Address (Step latency=4ms)
- 15041 Evaluating Identity Policy (Step latency=14ms)
- 22072 Selected identity source sequence - All_User_ID_Stores (Step latency=6ms)
- 15013 Selected Identity Source - Internal Users (Step latency=1ms)
- 24210 Looking up User in Internal Users IDStore (Step latency=0ms)
- 24212 Found User in Internal Users IDStore (Step latency=80ms)
- 13045 TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=1ms)
- 13015 Returned TACACS+ Authentication Reply (Step latency=0ms)
- 13014 Received TACACS+ Authentication CONTINUE Request (Step latency=3ms)
- 15041 Evaluating Identity Policy (Step latency=3ms)
- 22072 Selected identity source sequence - All_User_ID_Stores (Step latency=6ms)
- 15013 Selected Identity Source - Internal Users (Step latency=1ms)
- 24210 Looking up User in Internal Users IDStore (Step latency=0ms)
- 24212 Found User in Internal Users IDStore (Step latency=11ms)
- 22037 Authentication Passed (Step latency=1ms)
- 15036 Evaluating Authorization Policy (Step latency=2ms)
- 13015 Returned TACACS+ Authentication Reply (Step latency=11ms)

TACACS-Live-Protokolle von ISE - Router Verification

Verifizierung des Switches

Überprüfen Sie über die CLI des Switches die Authentifizierung von TACACS+ gegenüber ISE mit Gigabit Ethernet 1-Schnittstelle. Verwenden Sie dazu den Befehl test aaa group tacacsgroupname username password newn:

Hier ist eine Beispielausgabe von Switch und ISE.

Überprüfung von Port 49 vom Switch:

C9200L-48P# Telnet-ISE Gig1-Schnittstelle IP 49

Es wird versucht, die ISE Gig1-Schnittstelle IP, 49... Offen

C9200L-48P#test aaa group isegroup switch XXXX neu

Kennwort wird gesendet

Benutzer erfolgreich authentifiziert

BENUTZERATTRIBUTE

Benutzername 0 "switch"

Antwortnachricht 0 "Kennwort:"

Melden Sie sich zur ISE-Verifizierung in den GUI -> Operations -> TACACS Live Logs an, und filtern Sie dann mit der Switch-IP im Feld Network Device Details (Netzwerkgerätedetails).

The screenshot displays the Cisco ISE interface for a TACACS+ authentication event. The 'Overview' section shows the request type as 'Authentication', status as 'Pass', and session key as 'honey/530520237/11'. The message text is 'Passed-Authentication: Authentication succeeded'. The username is 'switch', and the authentication policy is 'New Policy Set 2 >> Default'. The selected authorization profile is 'Shell_Profile'. The 'Authentication Details' section shows the generated time as '2025-03-06 04:10:15.551000 +00:00', logged time as '2025-03-06 04:10:15.551', and epoch time as '1741234215'. The ISE node is 'honey'. The message text is 'Passed-Authentication: Authentication succeeded'. The failure reason, resolution, and root cause are all empty. The network device name is 'Switch' and the network device IP is redacted. The network device groups are 'IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types'. The device type is 'Device Type#All Device Types', and the location is 'Location#All Locations'. The device port is empty. The 'Steps' section shows a sequence of events: 13013 Received TACACS+ Authentication START Request, 15049 Evaluating Policy Group (Step latency=8ms), 15008 Evaluating Service Selection Policy (Step latency=0ms), 15048 Queried PIP - Network Access.Device IP Address (Step latency=11ms), 15041 Evaluating Identity Policy (Step latency=9ms), 22072 Selected identity source sequence - All_User_ID_Stores (Step latency=17ms), 15013 Selected Identity Source - Internal Users (Step latency=1ms), 24210 Looking up User in Internal Users IDStore (Step latency=1ms), 24212 Found User in Internal Users IDStore (Step latency=69ms), 13045 TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=0ms), 13015 Returned TACACS+ Authentication Reply (Step latency=1ms), 13014 Received TACACS+ Authentication CONTINUE Request (Step latency=7ms), 15041 Evaluating Identity Policy (Step latency=6ms), 22072 Selected identity source sequence - All_User_ID_Stores (Step latency=22ms), 15013 Selected Identity Source - Internal Users (Step latency=1ms), 24210 Looking up User in Internal Users IDStore (Step latency=36ms), 24212 Found User in Internal Users IDStore (Step latency=16ms), 22037 Authentication Passed (Step latency=0ms), 15036 Evaluating Authorization Policy (Step latency=1ms), and 13015 Returned TACACS+ Authentication Reply (Step latency=36ms).

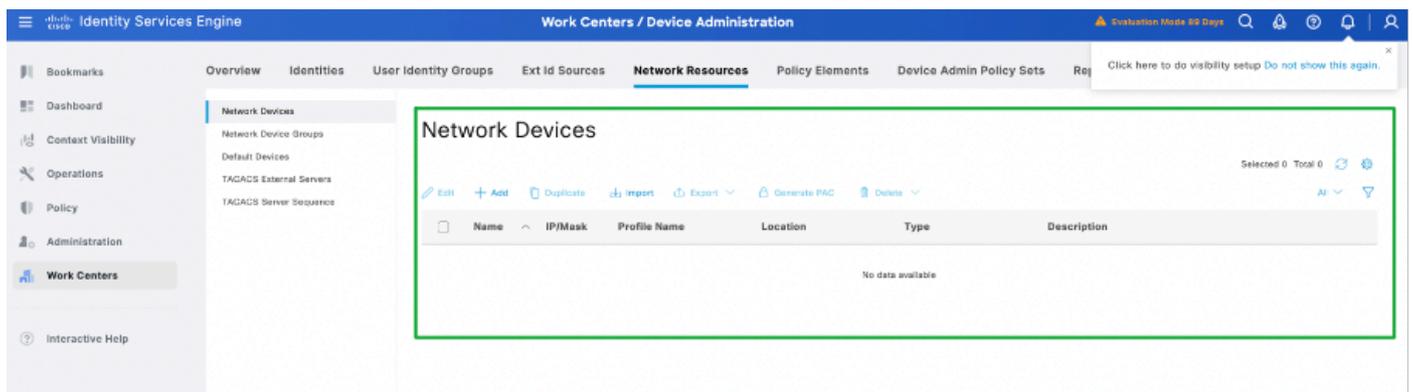
TACACS-Live-Protokolle von ISE - Switch-Verifizierung.

Fehlerbehebung

In diesem Abschnitt werden einige der häufigsten Probleme im Zusammenhang mit TACACS+-Authentifizierungen behandelt.

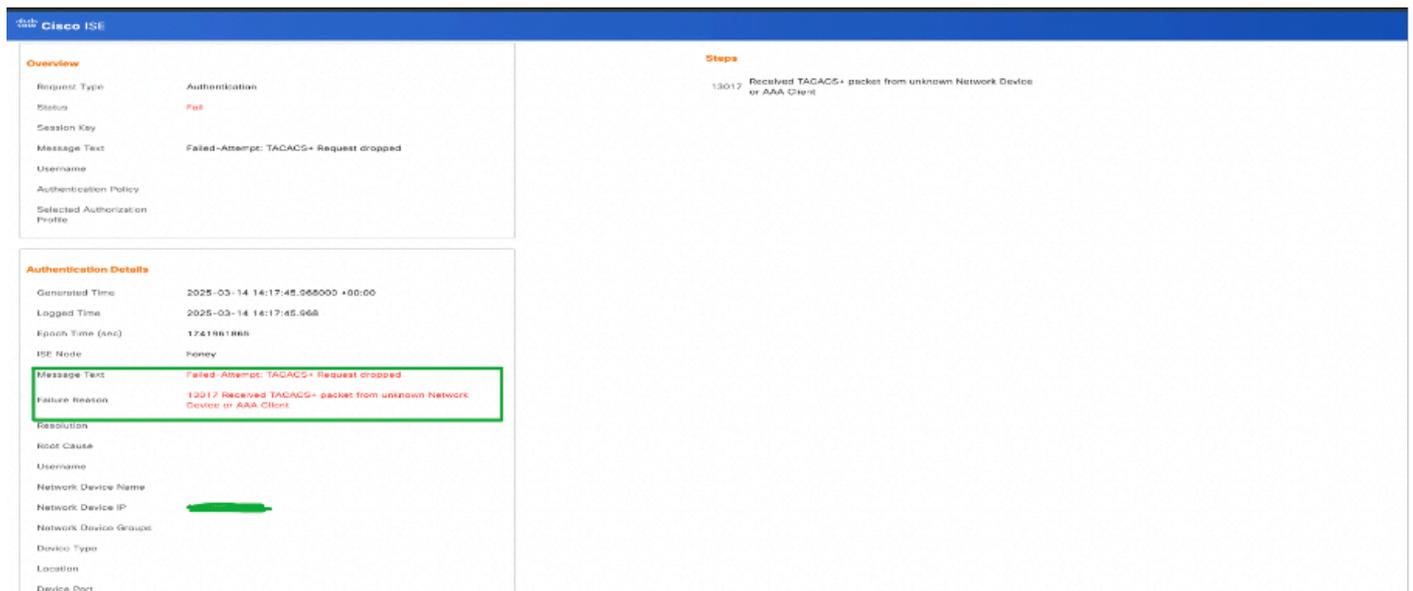
Szenario 1: Fehler bei der TACACS+-Authentifizierung: "Fehler: 13017 empfing TACACS+-Paket von unbekanntem Netzwerkgerät oder AAA-Client".

Dieses Szenario tritt ein, wenn das Netzwerkgerät in der ISE nicht als Netzwerkressourcen hinzugefügt wird. Wie in diesem Screenshot gezeigt, wird der Switch nicht zu den Netzwerkressourcen der ISE hinzugefügt.



Fehlerbehebungsszenario - Netzwerkgeräte werden in der ISE nicht hinzugefügt.

Wenn Sie jetzt die Authentifizierung vom Switch/Netzwerkgerät testen, erreicht das Paket erwartungsgemäß die ISE. Die Authentifizierung schlägt jedoch fehl mit dem Fehler "Error : 13017 Received TACACS+ packet from unknown Network Device or AAA Client" wie in diesem Screenshot gezeigt:



TACACS-Live-Protokolle - Fehler, wenn das Netzwerkgerät nicht zur ISE hinzugefügt wird.

Überprüfung durch das Netzwerkgerät (Switch)

Switch#test aaa group Isogruppe Switch XXXXXX neu

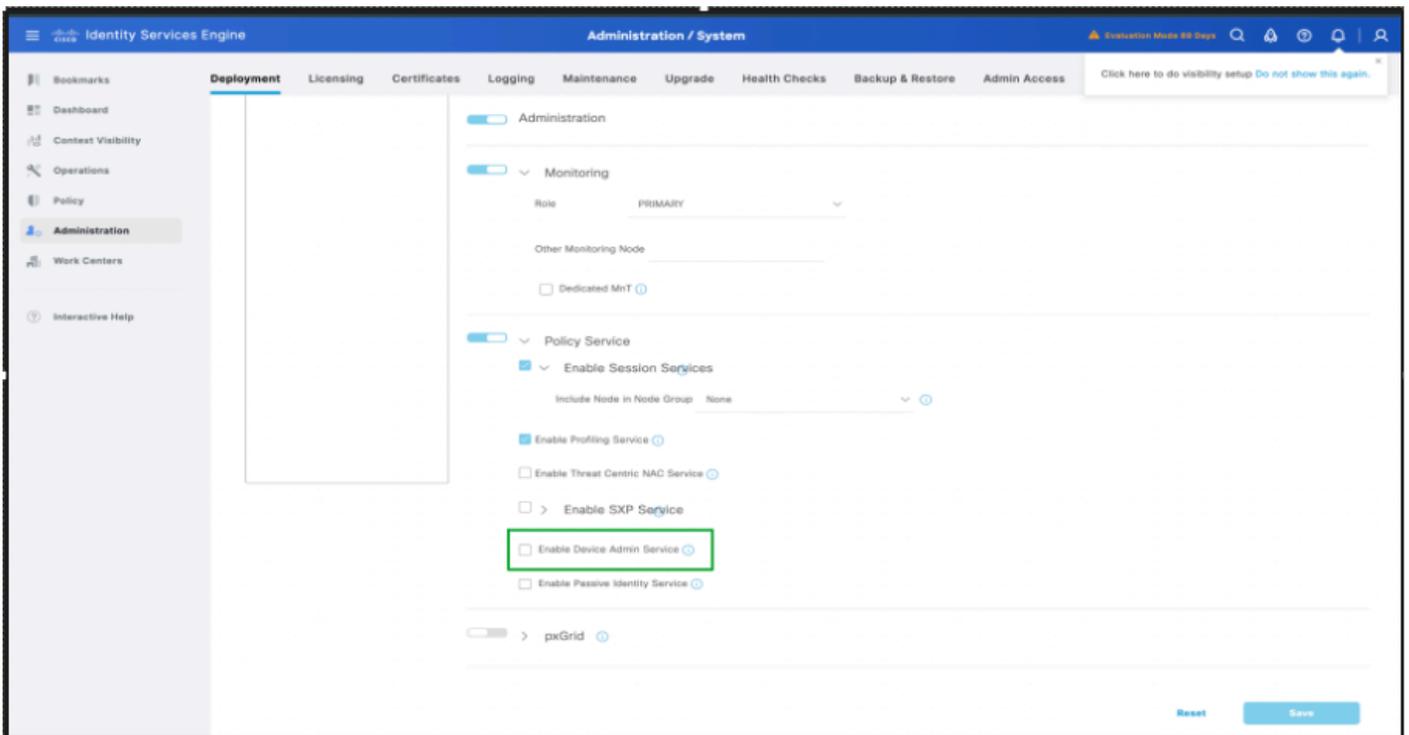
Benutzer abgelehnt

Lösung: Überprüfen Sie, ob der Switch/Router/das Netzwerkgerät in der ISE als Netzwerkgerät hinzugefügt wurde. Wenn das Gerät nicht hinzugefügt wird, fügen Sie das Netzwerkgerät der ISE-Liste der Netzwerkgeräte hinzu.

Szenario 2: Die ISE verwirft das TACACS+-Paket ohne Angabe von Informationen.

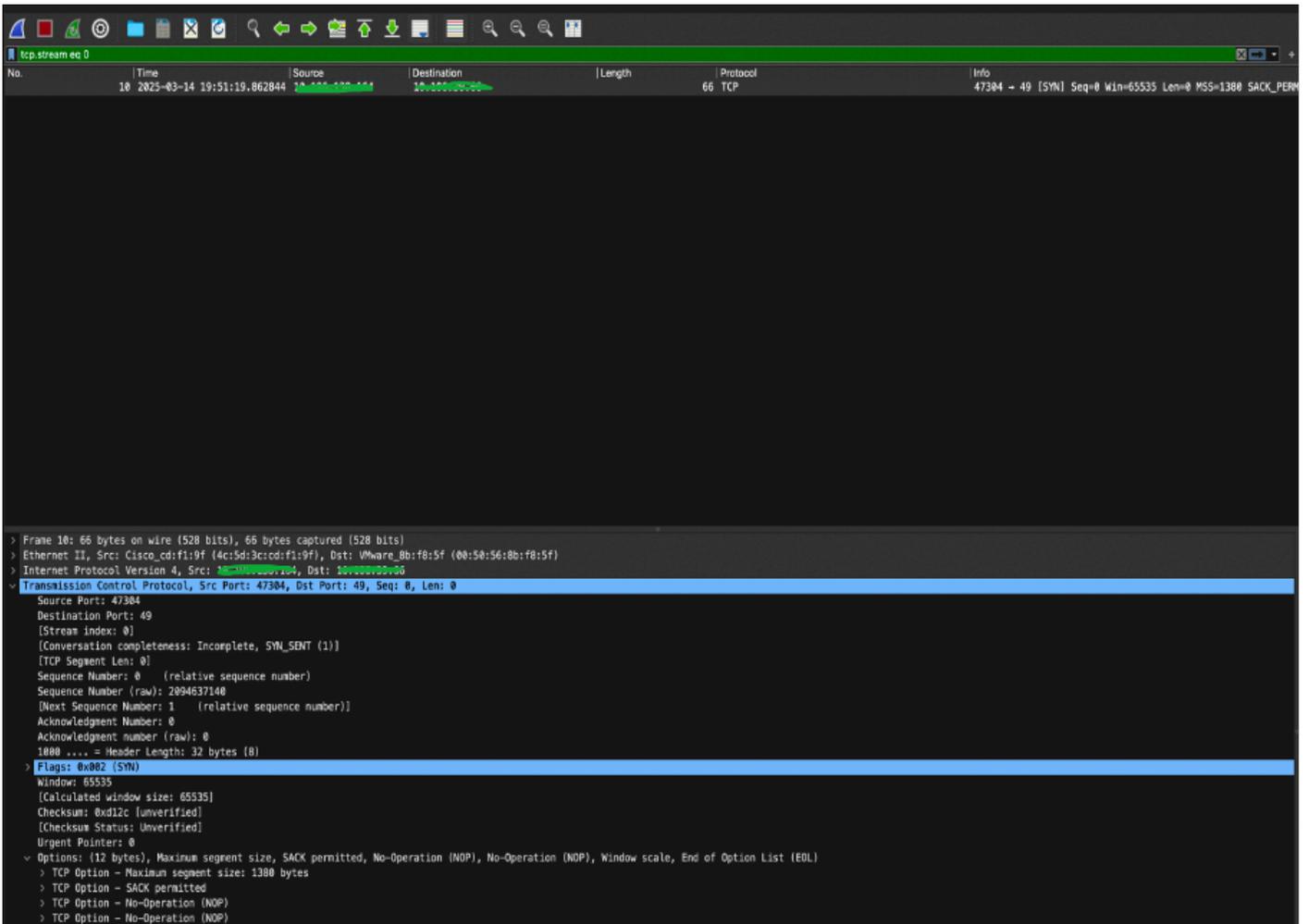
Dieses Szenario tritt auf, wenn der Device Administration Service in der ISE deaktiviert ist. In diesem Szenario verwirft die ISE das Paket, und es werden keine Live-Protokolle angezeigt, obwohl die Authentifizierung von dem Netzwerkgerät initiiert wird, das den Netzwerkressourcen der ISE hinzugefügt wird.

Wie in diesem Screenshot gezeigt, ist die Geräteadministration in der ISE deaktiviert.



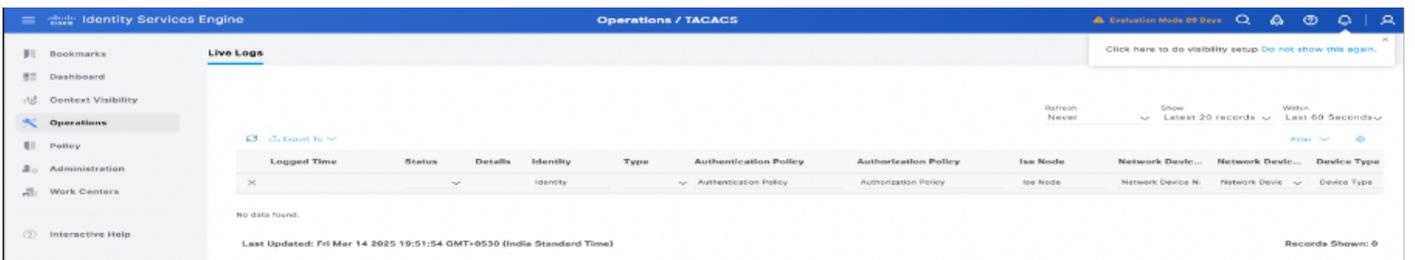
Szenario: Die Geräteverwaltung ist in der ISE nicht aktiviert.

Wenn ein Benutzer die Authentifizierung vom Netzwerkgerät aus initiiert, verwirft die ISE die Pakete ohne Informationen in den Live-Protokollen, und die ISE antwortet nicht auf das vom Netzwerkgerät gesendete Syn-Paket, um den TACACS-Authentifizierungsprozess abzuschließen. Siehe Screenshot:



ISE verwirft Pakete unbeaufsichtigt während TACACS

Die ISE zeigt während der Authentifizierung keine Live-Protokolle an.



Keine TACACS-Live-Protokolle - Überprüfung durch ISE

Überprüfung durch das Netzwerkgerät (Switch)

Switch#

Switch#test aaa group Isogruppe Switch XXXX neu

Benutzer abgelehnt

Switch#

*14. März 13:54:28.144: T+: Version 192 (0xC0), Typ 1, Folge 1, Verschlüsselung 1, SC 0

*14. März 13:54:28.144: T+: session_id 10158877 (0x9B031D), dlen 14 (0xE)

*14. März 13:54:28.144: T+: Typ:AUTHEN/START, priv_lvl:15 Aktion:LOGIN ascii

*14. März 13:54:28.144: T+: svc:LOGIN user_len:6 port_len:0 (0x0) raddr_len:0 (0x0) data_len:0

*14. März 13:54:28.144: T+: Benutzer: switch

*14. März 13:54:28.144: T+: anschluss:

*14. März 13:54:28.144: T+: rem_addr:

*14. März 13:54:28.144: T+: Daten:

*14. März 13:54:28.144: T+: Endpaket

Lösung: Aktivieren Sie die Geräteverwaltung in der ISE.

Referenz

- [Beheben von TACACS-Authentifizierungsproblemen](#)
- [Administratorleitfaden für die Cisco Identity Services Engine, Version 3.3](#)
- [VRF für TACACS-Server](#)

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.