

# FirePOWER eXtensible Operating System (FXOS) 2.2: Chassis-Authentifizierung/-Autorisierung für Remote-Management mit ISE unter Verwendung von TACACS+

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Konfigurieren des FXOS-Chassis](#)

[Konfigurieren des ISE-Servers](#)

[Überprüfen](#)

[Überprüfung der FXOS-Chassis](#)

[ISE 2.0-Verifizierung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie die TACACS+-Authentifizierung und -Autorisierung für das FirePOWER eXtensible Operating System (FXOS)-Chassis über die Identity Services Engine (ISE) konfiguriert wird.

Das FXOS-Chassis umfasst die folgenden Benutzerrollen:

- Administrator - Vollständiger Lese- und Schreibzugriff auf das gesamte System. Dem Standard-Administratorkonto wird diese Rolle standardmäßig zugewiesen, und es kann nicht geändert werden.
- Schreibgeschützt: Schreibgeschützter Zugriff auf die Systemkonfiguration ohne Berechtigung zum Ändern des Systemstatus.
- Betrieb - Lese- und Schreibzugriff auf die NTP-Konfiguration, Smart Call Home-Konfiguration für Smart Licensing und Systemprotokolle, einschließlich Syslog-Server und -Fehler. Lesezugriff auf den Rest des Systems.
- AAA - Lese- und Schreibzugriff auf Benutzer, Rollen und AAA-Konfiguration. Lesezugriff auf den Rest des Systems.

Über die CLI kann dies wie folgt angezeigt werden:

```
fpr4120-TAC-A /security* # Rolle anzeigen
```

Rolle:

Rollenname Priv.

— —

Aaa

Administrator

Betriebsabläufe

schreibgeschützt

Mitarbeiter: Tony Ramirez, Jose Soto, Cisco TAC Engineers.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis des FirePOWER eXtensible Operating System (FXOS)
- Kenntnis der ISE-Konfiguration
- In der ISE ist eine Lizenz für die TACACS+-Geräteadministration erforderlich.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco FirePOWER 4120 Security Appliance Version 2.2
- Virtuelle Cisco Identity Services Engine 2.2.0.470

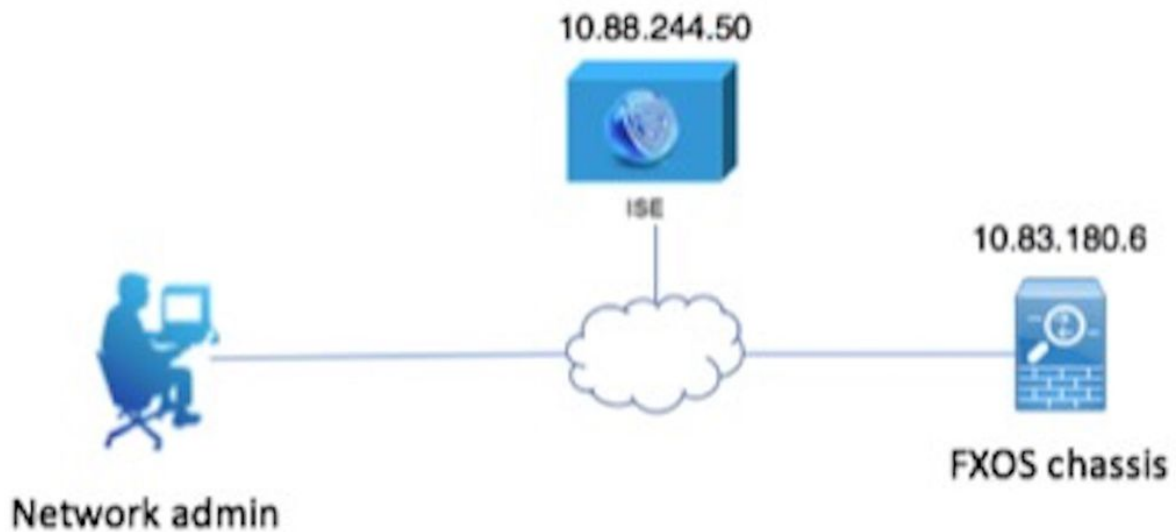
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren

Ziel der Konfiguration ist es,

- Authentifizierung von Benutzern, die sich über die webbasierte GUI und SSH von FXOS anmelden, mithilfe der ISE
- Autorisieren Sie Benutzer, die sich über die ISE in die webbasierte Benutzeroberfläche und SSH von FXOS einloggen, entsprechend ihrer jeweiligen Benutzerrolle.
- Überprüfung des ordnungsgemäßen Betriebs der Authentifizierung und Autorisierung auf dem FXOS mithilfe der ISE

# Netzwerkdiagramm



## Konfigurationen

### Konfigurieren des FXOS-Chassis

#### Erstellen eines TACACS+-Anbieters

Schritt 1: Navigieren Sie zu **Plattformeinstellungen > AAA**.

Schritt 2: Klicken Sie auf die Registerkarte **TACACS**.

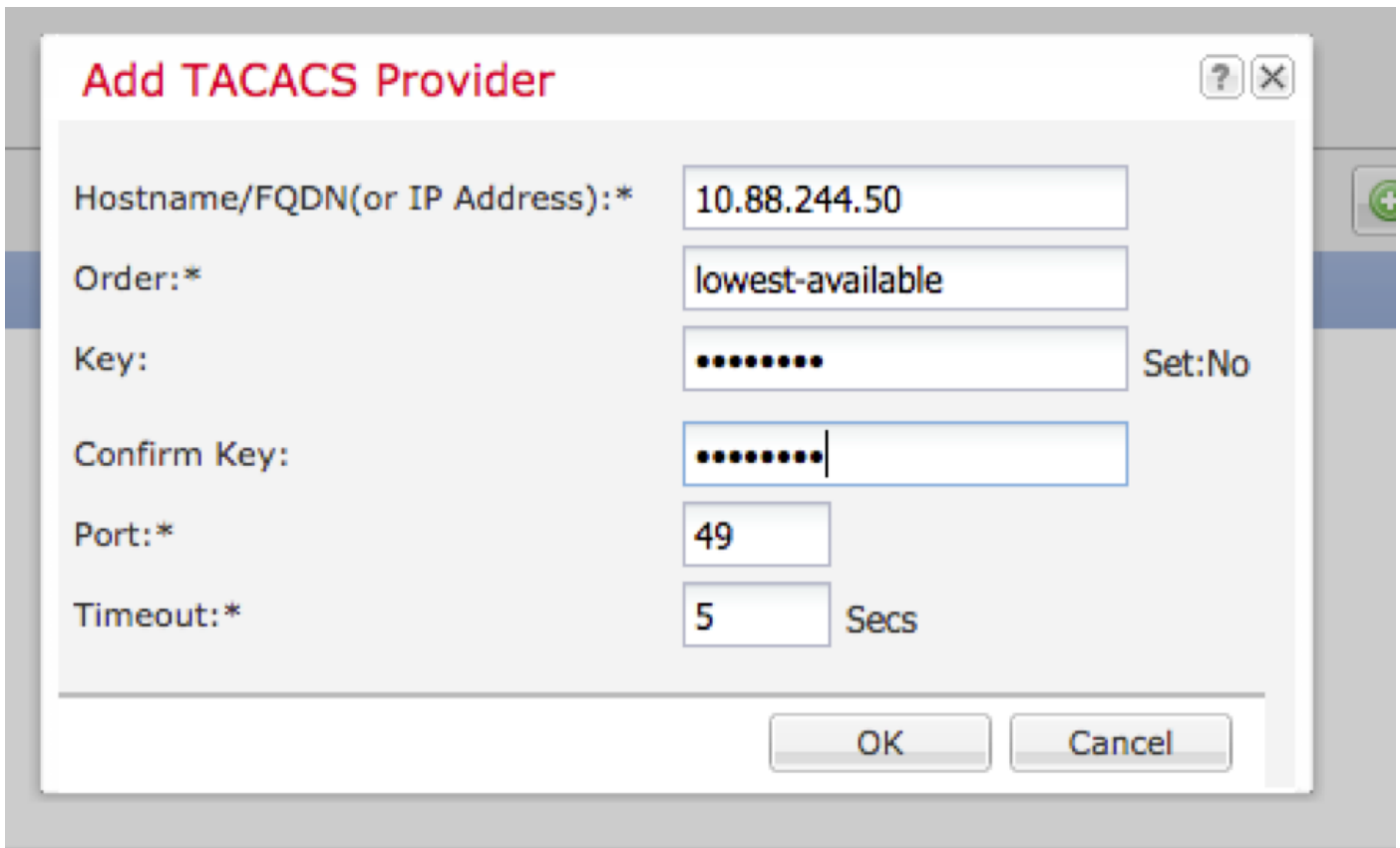


Schritt 3: Für jeden TACACS+-Anbieter, den Sie hinzufügen möchten (bis zu 16 Anbieter).

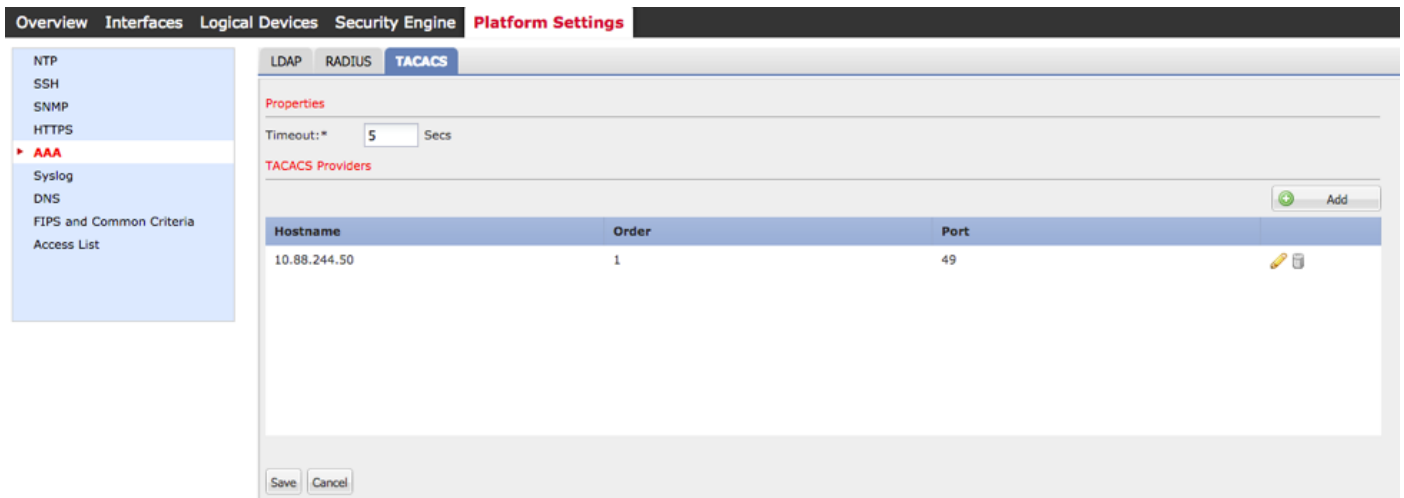
3.1 Klicken Sie im Bereich TACACS Providers (TACACS-Anbieter) auf **Add (Hinzufügen)**.

3.2 Geben Sie nach dem Öffnen des Dialogfelds TACACS-Anbieter hinzufügen die erforderlichen Werte ein.

3.3 Klicken Sie auf **OK**, um das Dialogfeld TACACS-Anbieter hinzufügen zu schließen.

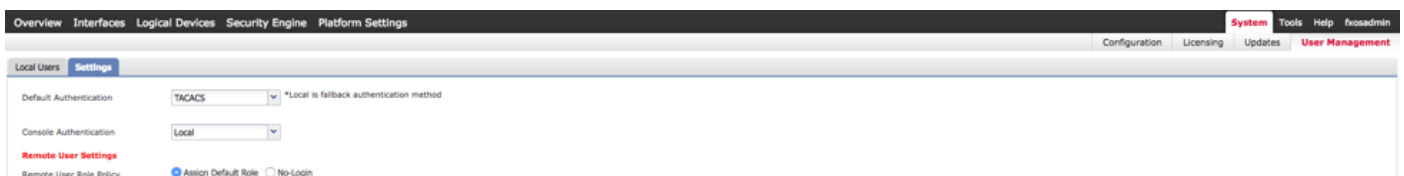


Schritt 4: Klicken Sie auf **Speichern**.



Schritt 5: Navigieren Sie zu **System > User Management > Settings**.

Schritt 6: Wählen Sie unter Standardauthentifizierung die Option **TACACS** aus.



## Erstellen eines TACACS+-Anbieters mithilfe der CLI

Schritt 1: Führen Sie die folgenden Befehle aus, um die TACACS-Authentifizierung zu aktivieren.

fpr4120-TAC-A# **Bereichssicherheit**

fpr4120-TAC-A/security # **scope default-auth**

fpr4120-TAC-A /security/default-auth # **Festlegen des Bereichstakus**

Schritt 2: Verwenden Sie den Befehl **show detail**, um die Konfiguration zu überprüfen.

fpr4120-TAC-A /security/default-auth # **Details anzeigen**

Standardauthentifizierung:

Admin-Bereich: **Taktiken**

Operativer Bereich: **Taktiken**

Aktualisierungszeitraum für Websitzungen (in Sekunden): 600

Sitzungs-Timeout (in Sekunden) für Web-, SSH-, Telnet-Sitzungen: 600

Absolutes Sitzungs-Timeout (in Sekunden) für Web-, SSH- und Telnet-Sitzungen: 3600

Timeout für serielle Konsolensitzung (in Sekunden): 600

Absolutes Sitzungs-Timeout für die serielle Konsole (in Sekunden): 3600

Servergruppe "Admin Authentication":

Operational Authentication Server-Gruppe:

Anwendung des zweiten Faktors: Nein

Schritt 3: Führen Sie zum Konfigurieren der TACACS-Serverparameter die folgenden Befehle aus.

fpr4120-TAC-A# **Bereichssicherheit**

fpr4120-TAC-A/Security # **Scope-Taks**

fpr4120-TAC-A /security/tacacs # **Server 10.88.244.50 eingeben**

fpr4120-TAC-A /security/tacacs/server # **"ACS Server" festlegen**

fpr4120-TAC-A /security/tacacs/server\* # **Schlüssel festlegen**

Geben Sie den Schlüssel ein: **\*\*\*\*\***

Schlüssel bestätigen: **\*\*\*\*\***

Schritt 4: Verwenden Sie den Befehl **show detail**, um die Konfiguration zu überprüfen.

fpr4120-TAC-A /security/tacacs/server\* # **Details anzeigen**

TACACS+-Server:

Hostname, FQDN oder IP-Adresse: 10,88,244,50

Beschreibung:

Bestellung: 1

Port: 49

Schlüssel: \*\*\*\*\*

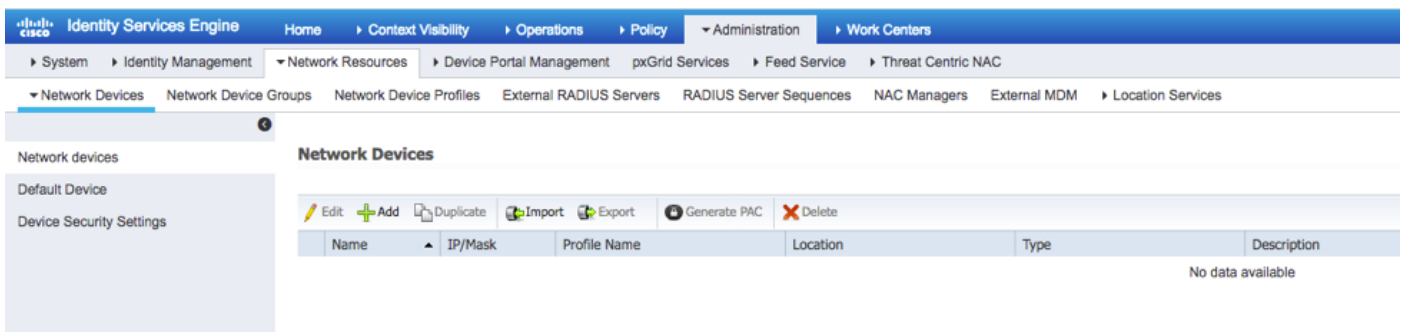
Timeout: 5

## Konfigurieren des ISE-Servers

### Hinzufügen des FXOS als Netzwerkressource

Schritt 1: Navigieren Sie zu **Administration > Network Resources > Network Devices**.

Schritt 2: Klicken Sie auf **HINZUFÜGEN**.



Schritt 3: Geben Sie die erforderlichen Werte ein (Name, IP-Adresse, Gerätetyp und TACACS+ aktivieren), und klicken Sie dann auf **Senden**.

**Identity Services Engine** Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM > Location Services

Network devices

Default Device

Device Security Settings

Network Devices List > FXOS

### Network Devices

\* Name

Description

\* IP Address:  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

## Erstellen von Identitätsgruppen und Benutzern

Schritt 1: Navigieren Sie zu **Administration > Identity Management > Groups > User Identity Groups (Administration > Identitätsverwaltung > Gruppen > Benutzeridentitätsgruppen)**.

Schritt 2: Klicken Sie auf **HINZUFÜGEN**.

**Identity Services Engine** Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Identities **Groups** External Identity Sources Identity Source Sequences > Settings

### Identity Groups

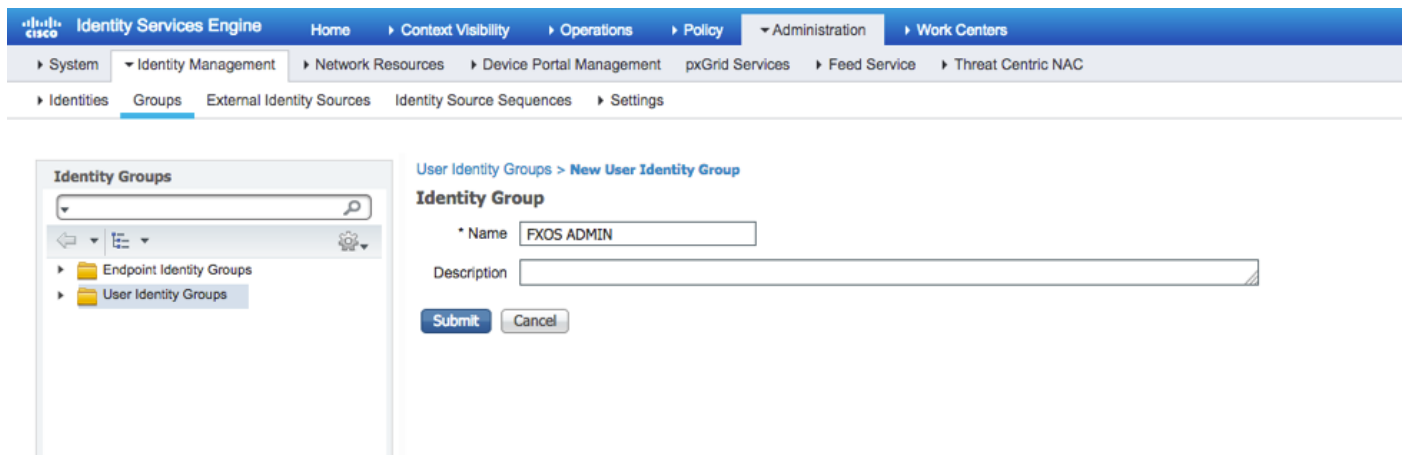
Endpoint Identity Groups

User Identity Groups

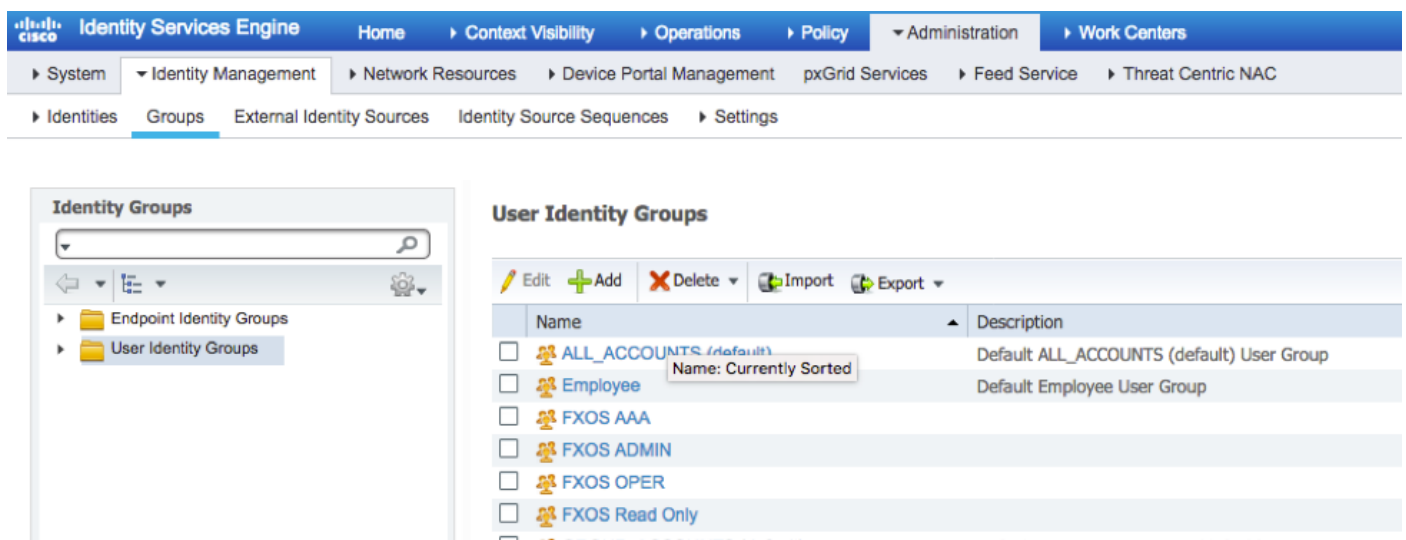
### User Identity Groups

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Schritt 3: Geben Sie den Wert für Name ein, und klicken Sie auf **Senden**.

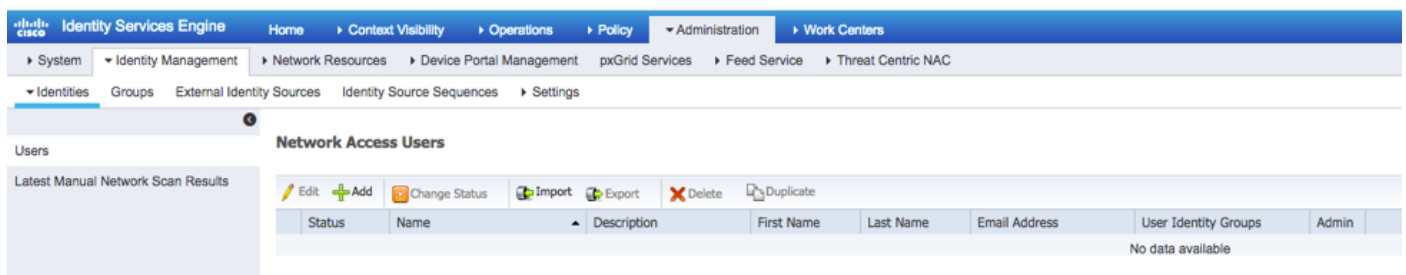


Schritt 4: Wiederholen Sie Schritt 3 für alle erforderlichen Benutzerrollen.



Schritt 5: Navigieren Sie zu **Administration > Identity Management > Identity > Users**.

Schritt 6: Klicken Sie auf **HINZUFÜGEN**.



Schritt 7: Geben Sie die erforderlichen Werte ein (Name, Benutzergruppe, Passwort).



Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

**Network Access User**

Name:

Status:  Enabled

Email:

**Passwords**

Password Type:

Password:  Re-Enter Password:

Enable Password:

**User Information**

First Name:

Last Name:

**Account Options**

Description:

Change password on next login:

**Account Disable Policy**

Disable account if date exceeds  (yyyy-mm-dd)

**User Groups**

Schritt 8: Wiederholen Sie Schritt 6 für alle erforderlichen Benutzer.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

**Network Access Users**

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> Enabled	fxosaaa					FXOS AAA	
<input type="checkbox"/> Enabled	fxosadmin					FXOS ADMIN	
<input type="checkbox"/> Enabled	fxosoper					FXOS OPER	
<input type="checkbox"/> Enabled	fxosro					FXOS Read Only	

## Erstellen des Shell-Profiles für jede Benutzerrolle

Schritt 1: Navigieren Sie zu **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles** und klicken Sie auf **+ADD**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

**TACACS Profiles**

0 Selected Rows/Page 4 / 1 / 1 Go 4 Total Rows

Refresh Add Duplicate Trash Edit Filter

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile

Schritt 2: Geben Sie die erforderlichen Werte für das TACACS-Profil ein.

### 2.1 Geben Sie den Namen ein.

TACACS Profiles > New

**TACACS Profile**

Name

Description

Task Attribute View Raw View

2.2 Konfigurieren Sie auf der REGISTERKARTE **RAW View** (RAW-Ansicht) den folgenden CISCO-AV-PAIR.

**cisco-av-pair=shell:roles="admin"**

### TACACS Profile

Name

Description

Task Attribute View

Raw View

### Profile Attributes

```
cisco-av-pair=shell:roles="admin"
```

Cancel

Submit

2.3 Klicken Sie auf **Senden**.

### TACACS Profile

Name

Description

**Task Attribute View** Raw View

### Common Tasks

Common Task Type

<input type="checkbox"/> Default Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Maximum Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Access Control List	<input type="text"/>	
<input type="checkbox"/> Auto Command	<input type="text"/>	
<input type="checkbox"/> No Escape	<input type="text"/>	(Select true or false)
<input type="checkbox"/> Timeout	<input type="text"/>	Minutes (0-9999)
<input type="checkbox"/> Idle Time	<input type="text"/>	Minutes (0-9999)

### Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="admin"	

Cancel Save

Schritt 3: Wiederholen Sie Schritt 2 für die verbleibenden Benutzerrollen mit den folgenden Cisco-AV-Paaren.

**cisco-av-pair=shell:roles="aaa"**

**cisco-av-pair=shell:roles="operations"**

**cisco-av-pair=shell:roles="schreibgeschützt"**

### Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="aaa"	

Cancel Save

## Custom Attributes

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="operations"	 

## Custom Attributes

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="read-only"	 

## TACACS Profiles

0 Selected

Rows/Page 8

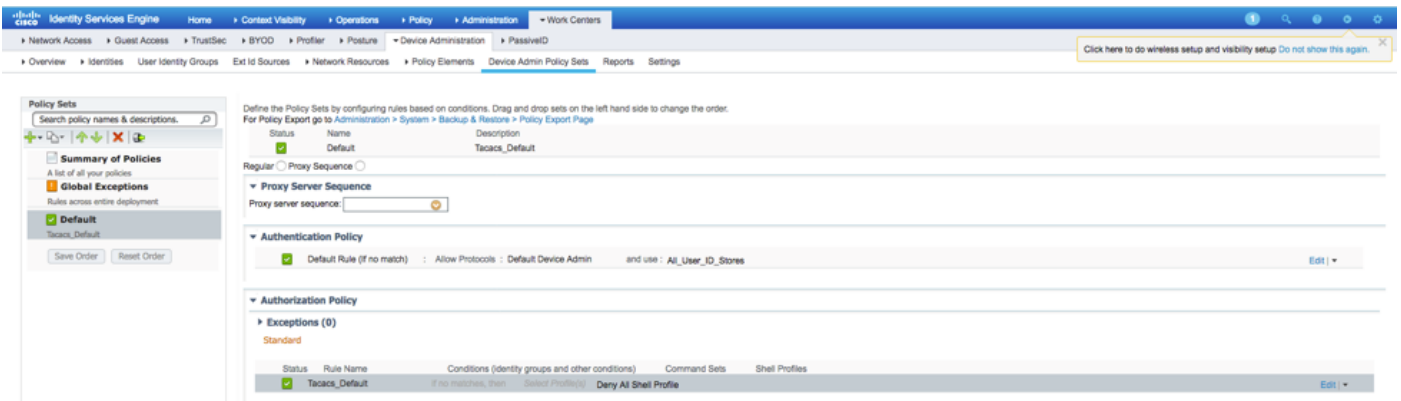
1 / 1

Go 8 Total Rows

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	FXOS_Admin_Profile	Shell	
<input type="checkbox"/>	FXOS_AAA_Shell	Shell	
<input type="checkbox"/>	FXOS_Operations_Shell	Shell	
<input type="checkbox"/>	FXOS_ReadOnly_Shell	Shell	

## Erstellen der TACACS-Autorisierungsrichtlinie

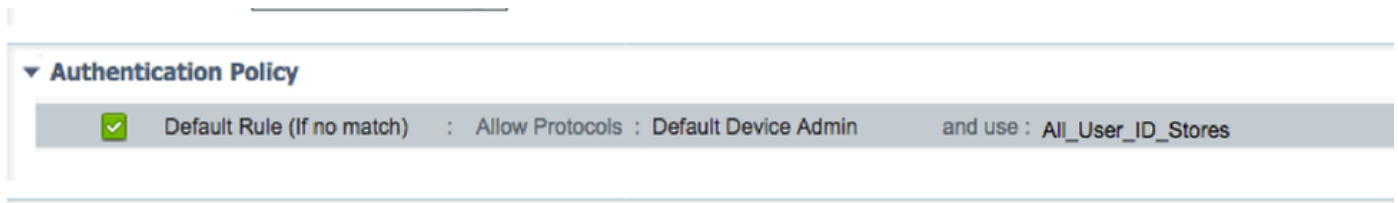
Schritt 1: Navigieren Sie zu **Work Center > Device Administration > Device Admin Policy Sets (Geräteverwaltung > Geräte-Admin-Richtliniensätze)**.



The screenshot displays the Cisco ISE configuration interface for Device Admin Policy Sets. On the left, a sidebar shows a list of policy sets, including 'Default' and 'Tactics\_Default'. The main area shows the configuration for the 'Tactics\_Default' policy set. The configuration includes sections for Proxy Server Sequence, Authentication Policy, and Authorization Policy. The Authorization Policy section shows a table of exceptions, including 'Deny All Shell Profile'.

Schritt 2: Stellen Sie sicher, dass die Authentifizierungsrichtlinie auf die Datenbank für interne

Benutzer oder den erforderlichen Identitätsspeicher verweist.



Schritt 3: Klicken Sie am Ende der standardmäßigen Autorisierungsrichtlinie auf den Pfeil, und klicken Sie oben auf Regel einfügen.

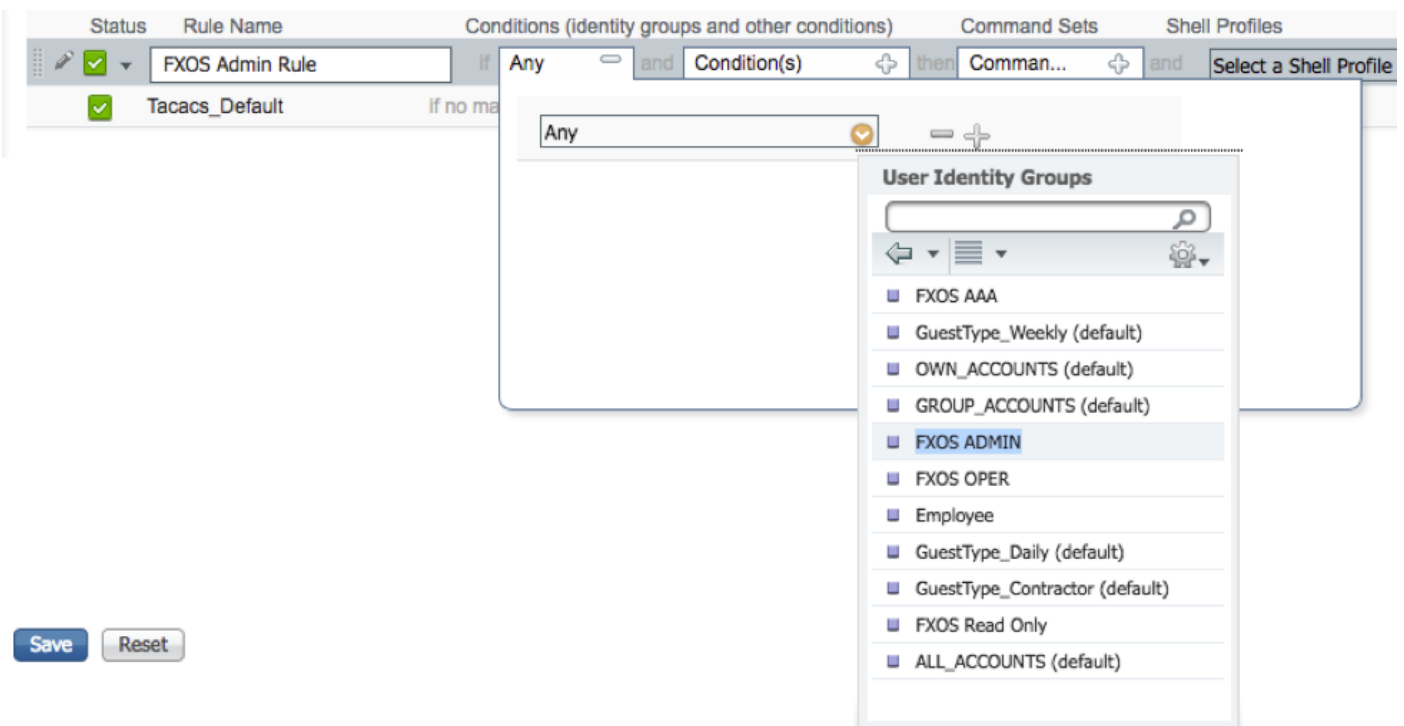


Schritt 4: Geben Sie die Werte für die Regel mit den erforderlichen Parametern ein:

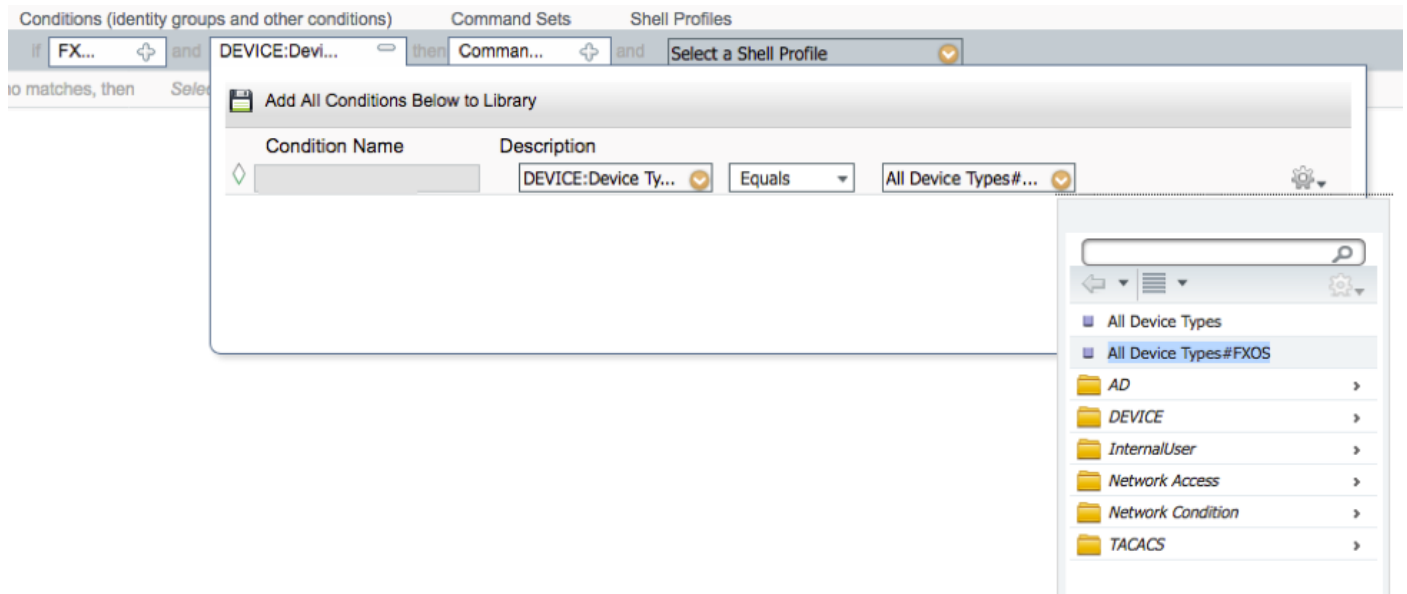
4.1 Regelname: FXOS-Admin-Regel.

4.2 Bedingungen.

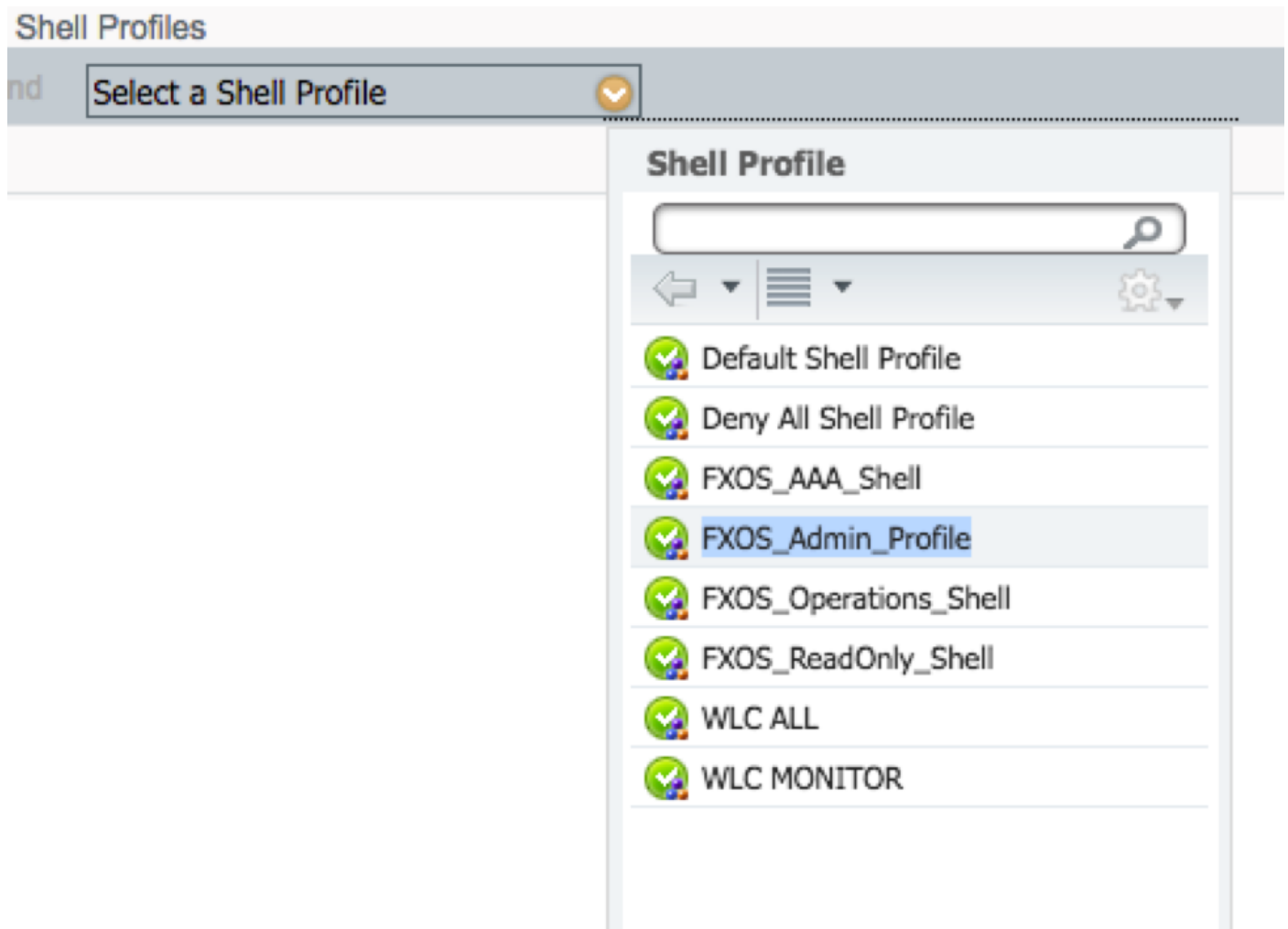
Wenn : Benutzeridentitätsgruppe: FXOS ADMIN



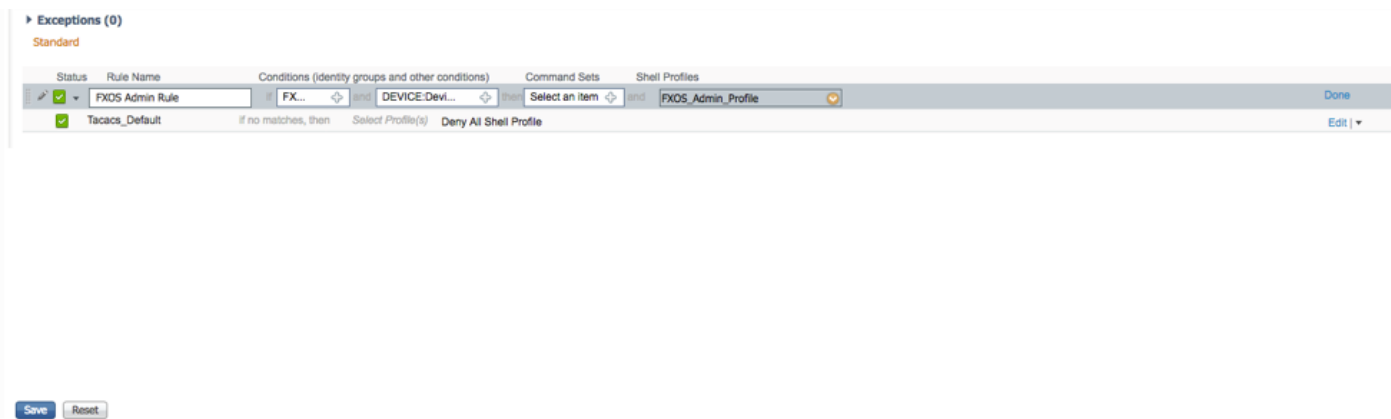
Und Gerät: Der Gerätetyp ist gleich allen Gerätetypen #FXOS.



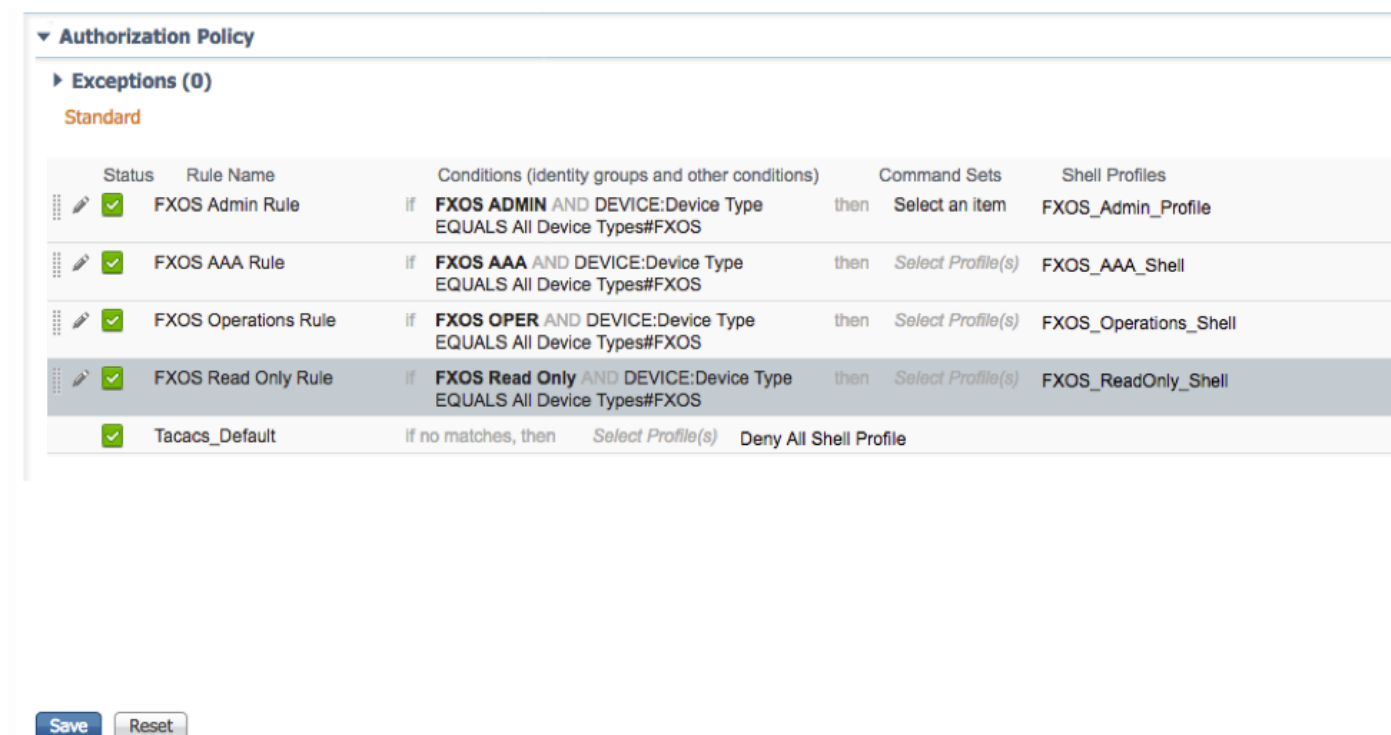
Shell-Profil: FXOS\_Admin\_Profile



Schritt 5: Klicken Sie auf **Fertig**.



Schritt 6: Wiederholen Sie die Schritte 3 und 4 für die übrigen Benutzerrollen, und klicken Sie abschließend auf **SPEICHERN**.



## Überprüfen

Sie können jetzt jeden Benutzer testen und die zugewiesene Benutzerrolle überprüfen.

### Überprüfung der FXOS-Chassis

1. Telnet oder SSH zum FXOS-Chassis und melden Sie sich mit einem der erstellten Benutzer auf der ISE an.

Benutzername: Fxosadmin

Kennwort:

fpr4120-TAC-A# **Scope Security**

fpr4120-TAC-A/security # **Details für Remote-Benutzer anzeigen**



Remote-Benutzer **fxosaa**:

Beschreibung:

Benutzerrollen:

Name: **Aaa**

Name: **schreibgeschützt**

Remote-Benutzer **fxosadmin**:

Beschreibung:

Benutzerrollen:

Name: **Administrator**

Name: **schreibgeschützt**

Remote-Benutzer-**Faxgerät**:

Beschreibung:

Benutzerrollen:

Name: **Betrieb**

Name: **schreibgeschützt**

Remote User **FXOTOR**:

Beschreibung:

Benutzerrollen:

Name: **schreibgeschützt**

Je nach dem eingegebenen Benutzernamen werden in der FXOS-Chassis-CLI nur die Befehle angezeigt, die für die zugewiesene Benutzerrolle autorisiert wurden.

Administratorbenutzerrolle.

fpr4120-TAC-A /security # ?

Bestätigung

Benutzersitzungen löschen

Erstellen verwalteter Objekte

Löschen verwalteter Objekte

Deaktivierung von Diensten

Aktivieren von Services

Geben Sie ein verwaltetes Objekt ein.

Bereich Ändert den aktuellen Modus

Festlegen von Eigenschaftenwerten

Systeminformationen anzeigen

Aktive CMC-Sitzungen beenden

fpr4120-TAC-A# **Connect-FXOS**

fpr4120-TAC-A (fxos)# **debug aaa-anfragen**

fpr4120-TAC-A (fxos)#

Reiner Lesezugriff auf Benutzerrollen.

fpr4120-TAC-A /security # ?

Bereich Ändert den aktuellen Modus

Festlegen von Eigenschaftenwerten

Systeminformationen anzeigen

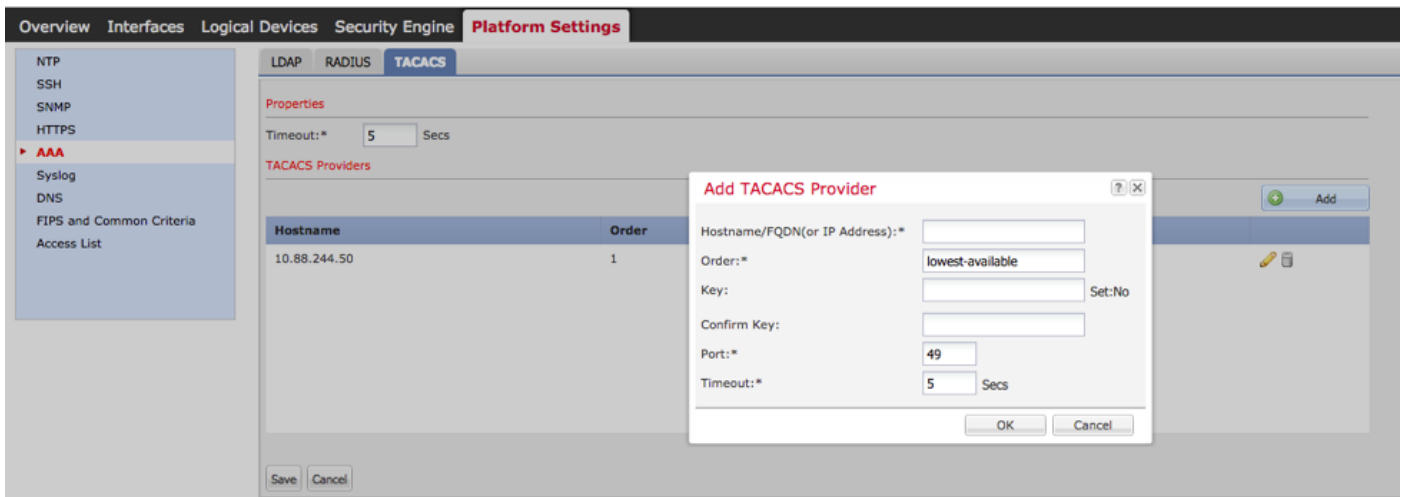
fpr4120-TAC-A# **Connect-FXOS**

fpr4120-TAC-A (fxos)# **debug aaa-anfragen**

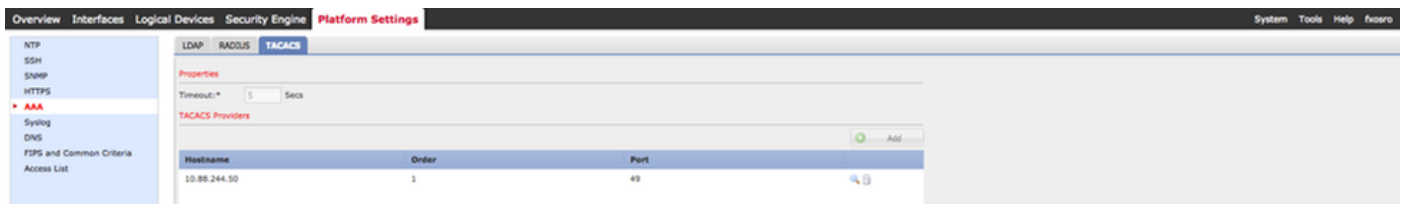
% Berechtigung verweigert für die Rolle

2. Navigieren Sie zur IP-Adresse des FXOS-Chassis, und melden Sie sich mit einem der erstellten Benutzer auf der ISE an.

Administratorbenutzerrolle.



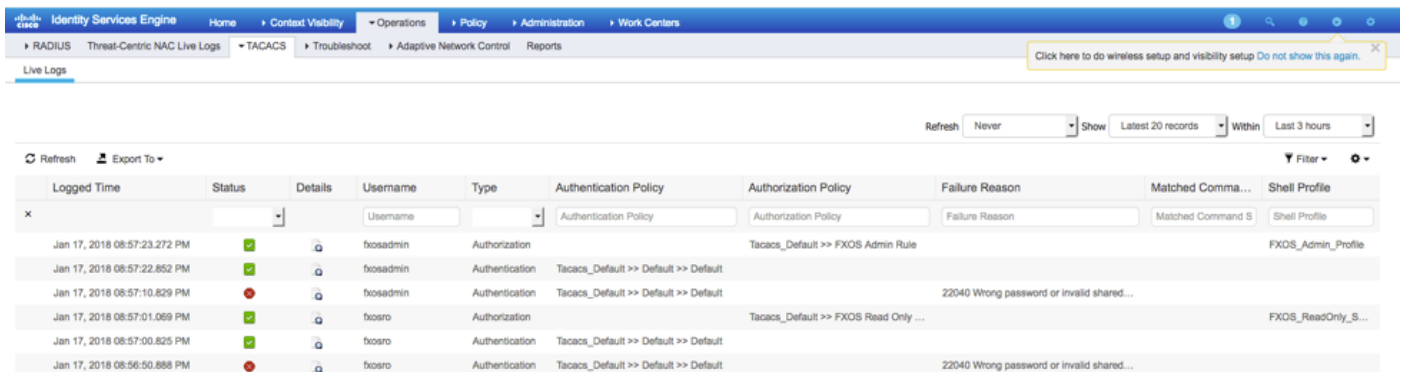
Schreibgeschützte Benutzerrolle.



**Hinweis:** Beachten Sie, dass die Schaltfläche **ADD** deaktiviert ist.

## ISE 2.0-Verifizierung

1. Navigieren Sie zu **Operations > TACACS LiveLog**. Erfolgreiche und fehlgeschlagene Versuche sollten angezeigt werden.



## Fehlerbehebung

Führen Sie zum Debuggen der AAA-Authentifizierung und -Autorisierung die folgenden Befehle in der FXOS-CLI aus.

```
fr4120-TAC-A# Connect-FXOS
```

```
fr4120-TAC-A (fxos)# debug aaa-anfragen
```

```
fr4120-TAC-A (fxos)# debug aaa event
```

```
fr4120-TAC-A (fxos)# debug aaa errors
```

fpr4120-TAC-A (fxos)# term mon

Nach einem erfolgreichen Authentifizierungsversuch wird die folgende Ausgabe angezeigt.

17.01.2018 15:46:40.305247 aaa: aa\_req\_process für die Authentifizierung. Sitzung Nr. 0

17.01.2018 15:46:40.305262 aaa: aaa\_req\_process: Allgemeine AAA-Anfrage von Anwendung:  
login appln\_subtype: Standard

17.01.2018 15:46:40.305271 aaa: try\_next\_aaa\_method

17.01.2018 15:46:40.305285 aaa: Die konfigurierten Methoden gesamt sind 1, der aktuelle Index ist 0.

17.01.2018 15:46:40.305294 aaa: Handle\_req\_using\_method

17. Januar 2018 15:46:40.305301 aaa: AAA\_METHODE\_SERVER\_GRUPPE

17. Januar 2018 15:46:40.305308 aaa: aa\_sg\_method\_handler group = takacs

17. Januar 2018 15:46:40.305315 aaa: Verwenden des an diese Funktion übergebenen  
sg\_protocol

17.01.2018 15:46:40.305324 aaa: Anfrage an TACACS-Dienst senden

17.01.2018 15:46:40.305384 aaa: Konfigurierte Methodengruppe erfolgreich

17. Januar 2018 15:46:40:554631 aaa: aaa\_process\_fd\_set

17. Januar 2018 15:46:40:555229 aaa: aa\_process\_fd\_set: mtscallback auf aaa\_q

17. Januar 2018 15:46:40:555817 aaa: mts\_message\_response\_handler: eine MTS-Antwort

17. Januar 2018 15:46:40:556387 aaa: prot\_daemon\_response\_handler

17. Januar 2018 15:46:40:557042 aaa: Sitzung: 0x8dfd68c aus Sitzungstabelle 0 entfernt

17. Januar 2018 15:46:40:557059 aaa: is\_aaa\_resp\_status\_Succ= 1

17. Januar 2018 15:46:40:557066 aaa: is\_aa\_resp\_status\_Success ist TRUE

17. Januar 2018 15:46:40:557075 aaa: aa\_send\_client\_response für die Authentifizierung.  
session->flags=21. aa\_resp->flags=0.

17. Januar 2018 15:46:40:557083 aaa: AAA\_REQ\_FLAG\_NORMAL

17. Januar 2018 15:46:40:557106 aaa: mts\_send\_response erfolgreich

17. Januar 2018 15:46:40:557364 aaa: aa\_req\_process für die Autorisierung. Sitzung Nr. 0

17. Januar 2018 15:46:40:557378 aaa: aaa\_req\_process called with context from appln: login  
appln\_subtype: default authen\_type:2, authen\_method: 0

17. Januar 2018 15:46:40:557386 aaa: aaa\_send\_req\_using\_context

17. Januar 2018 15:46:40:557394 aaa: aa\_sg\_method\_handler group = (null)

17. Januar 2018 15:46:40:557401 aaa: Verwenden des an diese Funktion übergebenen sg\_protocol

17. Januar 2018 15:46:40:557408 aaa: kontextbasiertes oder gerichtetes AAA req (Ausnahme: keine Relay-Anfrage). Keine Kopie einer Anforderung wird übernommen.

17. Januar 2018 15:46:40:557415 aaa: Anfrage an TACACS-Dienst senden

17. Januar 2018 15:46:40:801732 aaa: aa\_send\_client\_response für die Autorisierung. session->flags=9. aa\_resp->flags=0.

17. Januar 2018 15:46:40:801740 aaa: AAA\_REQ\_FLAG\_NORMAL

17. Januar 2018 15:46:40:801761 aaa: mts\_send\_response erfolgreich

17. Januar 2018 15:46:40:848932 aaa: ALTER OPACODE: accounting\_interim\_update\_update

17.01.2018 15:46:40:848943 aaa: aa\_create\_local\_acct\_req: user=, session\_id=, log=added user:fxosadmin to role:admin

17. Januar 2018 15:46:40:848963 aaa: aa\_req\_process for accounting. Sitzung Nr. 0

17. Januar 2018 15:46:40:848972 aaa: Die MTS-Anforderungsreferenz lautet NULL. LOKALE Anforderung

17.01.2018 15:46:40:848982 aaa: Festlegen von AAA\_REQ\_RESPONSE\_NOT\_NEEDED

17.01.2018 15:46:40:848992 aaa: aaa\_req\_process: Allgemeine AAA-Anfrage von Anwendung: default appln\_subtype: Standard

17. Januar 2018 15:46:40:849002 aaa: try\_next\_aaa\_method

17. Januar 2018 15:46:40:849022 aaa: Keine Standardmethoden konfiguriert

17. Januar 2018 15:46:40:849032 aaa: Keine Konfiguration für diese Anforderung verfügbar

17. Januar 2018 15:46:40:849043 aaa: try\_fallback\_method

17. Januar 2018 15:46:40:849053 aaa: Handle\_req\_using\_method

17. Januar 2018 15:46:40:849063 aaa: local\_method\_handler

17. Januar 2018 15:46:40:849073 aaa: aaa\_local\_accounting\_msg

17. Januar 2018 15:46:40:849085 aaa: Aktualisieren::Benutzer:fxosadmin zur Rolle hinzugefügt:admin

Nach einem fehlgeschlagenen Authentifizierungsversuch wird die folgende Ausgabe angezeigt.

17.01.2018 15:46:17.836271 aaa: aa\_req\_process für die Authentifizierung. Sitzung Nr. 0

17.01.2018 15:46:17.83616 aaa: aaa\_req\_process: Allgemeine AAA-Anfrage von Anwendung: login appln\_subtype: Standard

17.01.2018 15:46:17.837063 aaa: try\_next\_aaa\_method

17.01.2018 15:46:17.837416 aaa: Die konfigurierten Methoden gesamt sind 1, der aktuelle Index ist 0.

17.01.2018 15:46:17.83766 aaa: Handle\_req\_using\_method

17.01.2018 15:46:17.838103 aaa: AAA\_METHODE\_SERVER\_GRUPPE

17.01.2018 15:46:17.83847 aaa: aa\_sg\_method\_handler group = takacs

17.01.2018 15:46:17.83826 aaa: Verwenden des an diese Funktion übergebenen sg\_protocol

17.01.2018 15:46:17.839167 aaa: Anfrage an TACACS-Dienst senden

17. Januar 2018 15:46:17.840225 aaa: Konfigurierte Methodengruppe erfolgreich

17. Januar 2018 15:46:18.043710 aaa: is\_aa\_resp\_status\_Success status = 2

17. Januar 2018 15:46:18.044048 aaa: is\_aa\_resp\_status\_Success ist TRUE

17. Januar 2018 15:46:18.044395 aaa: aa\_send\_client\_response für die Authentifizierung. session->flags=21. aa\_resp->flags=0.

17. Januar 2018 15:46:18.04473 aaa: AAA\_REQ\_FLAG\_NORMAL

17.01.2018 15:46:18.045096 aaa: mts\_send\_response erfolgreich

17. Januar 2018 15:46:18.04567 aaa: aaa\_cleanup\_session

17. Januar 2018 15:46:18.045689 aaa: mts\_drop der Anfrage msg

17.01.2018 15:46:18.04569 aaa: aaa\_req sollte freigegeben werden.

17. Januar 2018 15:46:18.045715 aaa: aaa\_process\_fd\_set

17. Januar 2018 15:46:18.045722 aaa: aa\_process\_fd\_set: mtscallback auf aaa\_q

17. Januar 2018 15:46:18.045732 aaa: aa\_enable\_info\_config: GET\_REQ für eine Anmeldefehlermeldung

17. Januar 2018 15:46:18.045738 aaa: Rückgabewert des Konfigurationsvorgangs zurückerhalten:Unbekannter Sicherheitsaspekt

## Zugehörige Informationen

Der Ethanalyzer-Befehl in der FX-OS-CLI fordert Sie zur Eingabe des Kennworts auf, wenn die

TACACS/RADIUS-Authentifizierung aktiviert ist. Dieses Verhalten wird durch einen Fehler verursacht.

Bug-ID: [CSCvg87518](#)