

FirePOWER eXtensible Operating System (FXOS) 2.2: Chassis-Authentifizierung/-Autorisierung für Remote-Management mit ISE über RADIUS

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[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 Sie die RADIUS-Authentifizierung und -Autorisierung für das FirePOWER eXtensible Operating System (FXOS)-Chassis über die Identity Services Engine (ISE) konfigurieren.

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

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

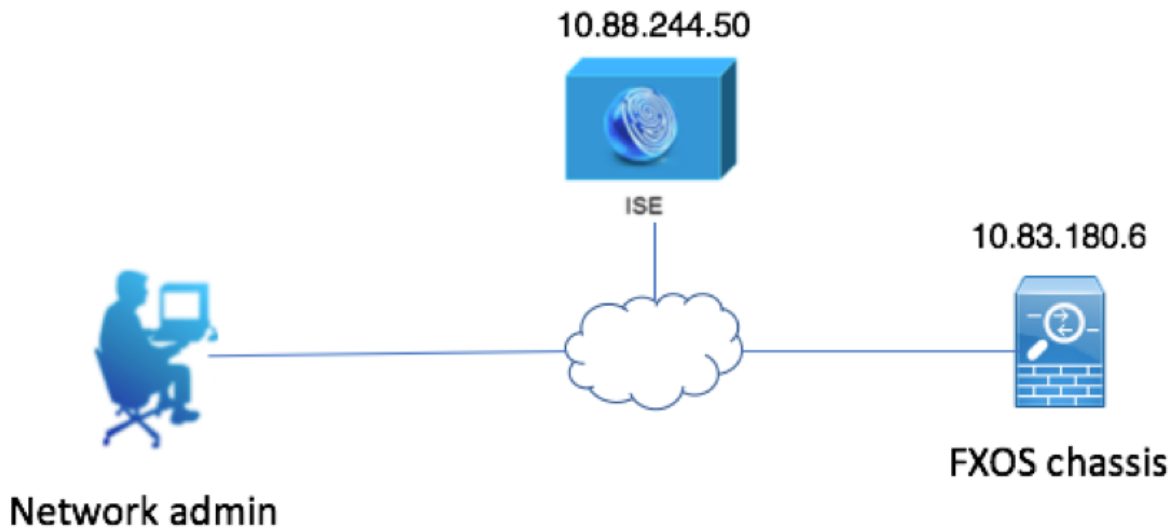
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines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



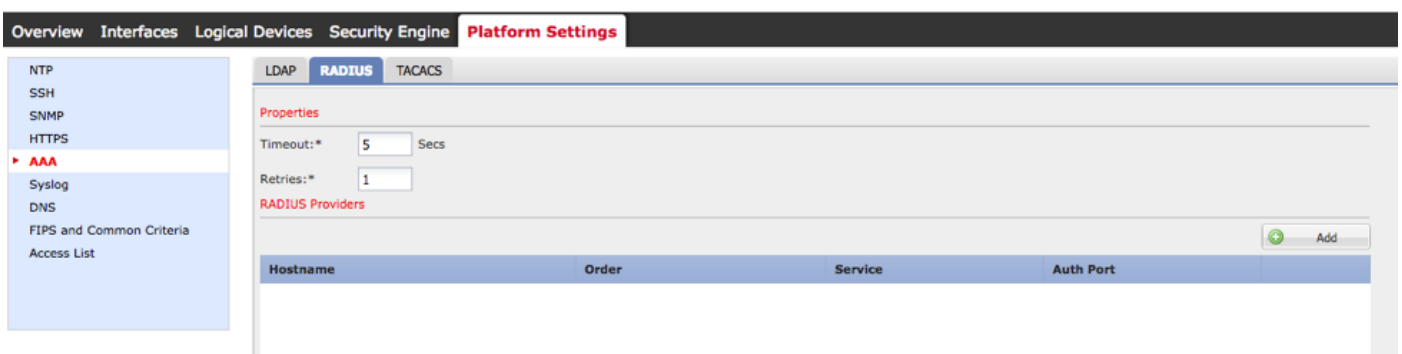
Konfigurationen

Konfigurieren des FXOS-Chassis

Erstellen eines RADIUS-Anbieters mithilfe des Chassis Managers

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

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



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

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

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

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

Edit 10.88.244.50

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: Yes

Confirm Key:

Authorization Port:*

Timeout:* Secs

Retries:*

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

Overview Interfaces Logical Devices Security Engine **Platform Settings**

NTP
SSH
SNMP
HTTPS
▶ **AAA**
Syslog
DNS
FIPS and Common Criteria
Access List

LDAP **RADIUS** TACACS

Properties

Timeout:* Secs

Retries:*

RADIUS Providers

Hostname	Order	Service	Auth Port
10.88.244.50	1	authorization	1812

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

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

Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help frosedmin

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication: *Local is fallback authentication method

Console Authentication:

Remote User Settings

Remote User Role Policy: Assign Default Role No-Login

Erstellen eines RADIUS-Anbieters mithilfe der CLI

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

```
fpr4120-TAC-A# Bereichssicherheit
```

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

```
fpr4120-TAC-A /security/default-auth # Bereichsradius festlegen
```

Schritt 2: Verwenden Sie den Befehl **show detail**, um die Ergebnisse anzuzeigen.

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

Standardauthentifizierung:

Admin-Bereich: **Radius**

Operativer Bereich: **Radius**

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 die folgenden Befehle aus, um RADIUS-Serverparameter zu konfigurieren.

```
fpr4120-TAC-A# Bereichssicherheit
```

```
fpr4120-TAC-A/Security # Gültigkeitsradius
```

```
fpr4120-TAC-A /security/radius # Geben Sie server 10.88.244.50 ein.
```

```
fpr4120-TAC-A /security/radius/server # setzen Sie die absteigende "ISE Server"
```

```
fpr4120-TAC-A /security/radius/server* # Schlüssel festlegen
```

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

Schlüssel bestätigen: *********

Schritt 4: Verwenden Sie den Befehl **show detail**, um die Ergebnisse anzuzeigen.

```
fpr4120-TAC-A /security/radius/server* # Details anzeigen
```

RADIUS-Server:

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

Beschreibung:

Bestellung: 1

Auth-Port: 1812

Schlüssel: *****

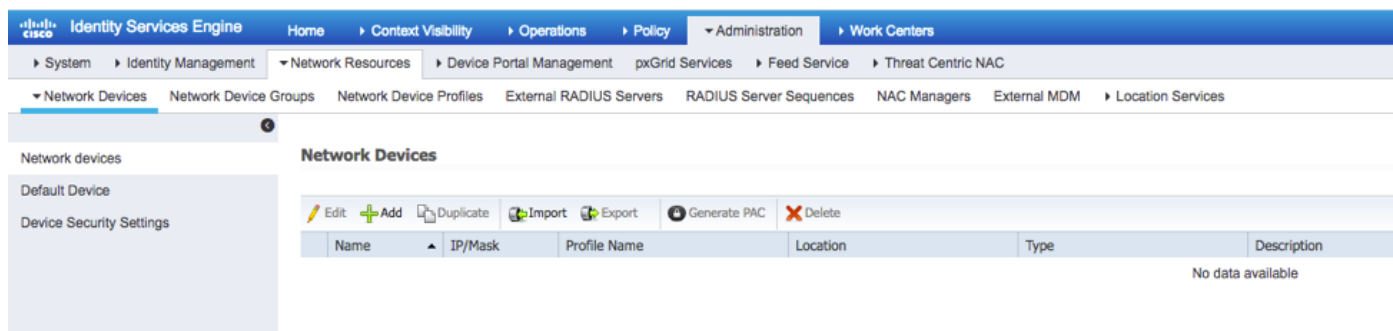
Timeout: 5

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**.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Network Devices. The main content area is titled "Network Devices" and contains a table with columns: Name, IP/Mask, Profile Name, Location, Type, and Description. The table is currently empty, with the text "No data available" displayed below it. The table header is as follows:

Name	IP/Mask	Profile Name	Location	Type	Description
------	---------	--------------	----------	------	-------------

Schritt 3: Geben Sie die erforderlichen Werte ein (Name, IP-Adresse, Gerätetyp und RADIUS aktivieren sowie SCHLÜSSEL SCHLÜSSEL hinzufügen), und klicken Sie 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 > New Network Device

Network Devices

* Name

Description

* IP Address: /

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

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

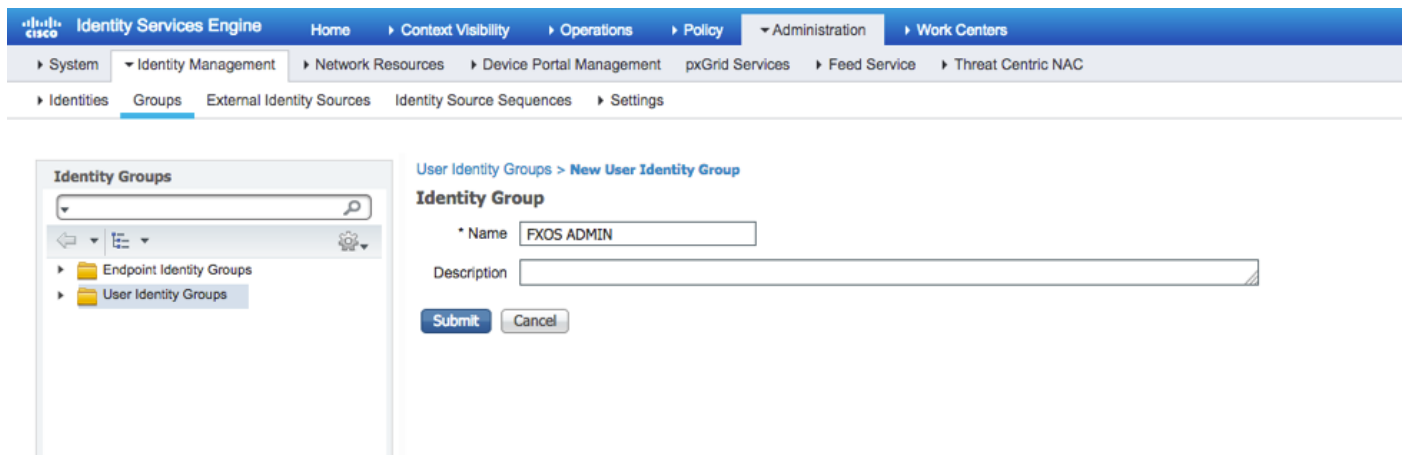
- Endpoint Identity Groups
- User Identity Groups**

User Identity Groups

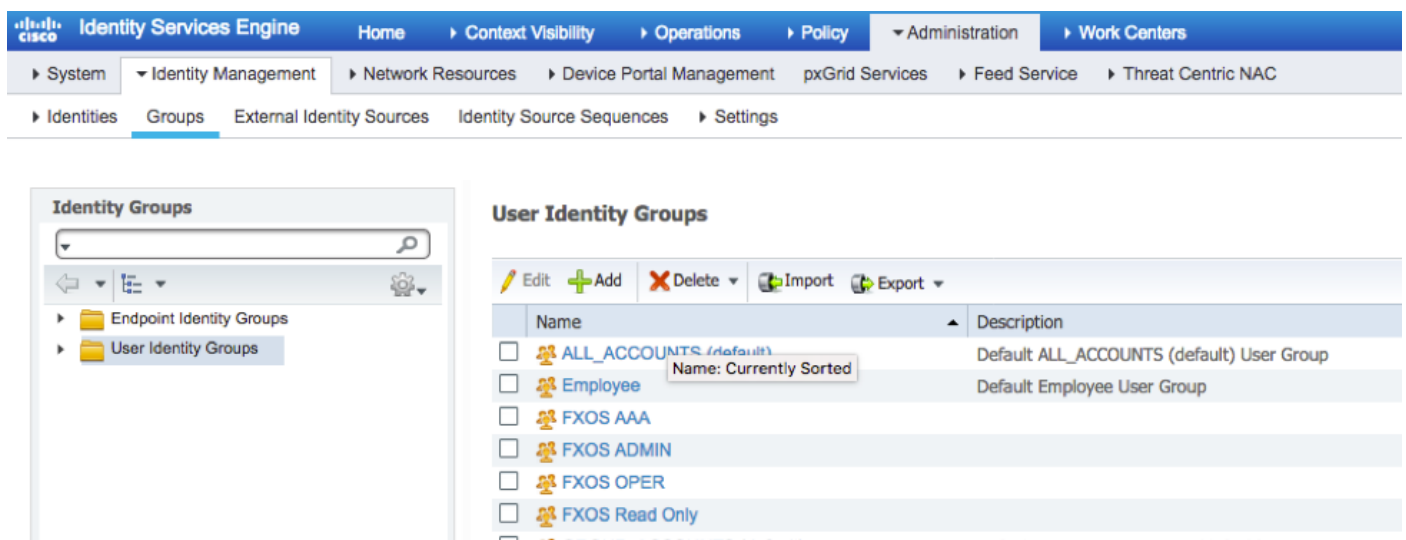
Edit Add Delete Import Export

<input type="checkbox"/>	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**.

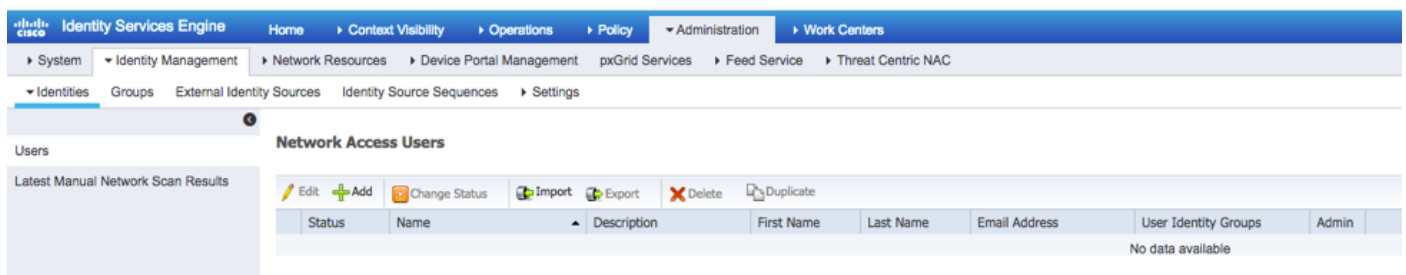


Schritt 4: Wiederholen Sie Schritt 3 für alle erforderlichen Benutzerrollen.



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 Autorisierungsprofils für jede Benutzerrolle

Schritt 1: Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**.

Standard Authorization Profiles
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Name	Profile	Description
<input type="checkbox"/> Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensu
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA port
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisionir
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/> DenyAccess		Default Profile with access type as Access-Reject
<input type="checkbox"/> PermitAccess		Default Profile with access type as Access-Accept

Schritt 2: Füllen Sie alle Attribute für das Autorisierungsprofil aus.

2.1 Konfigurieren Sie den Profilnamen.

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile: Cisco

2.2 Konfigurieren Sie unter **Erweiterte Attributeinstellungen** den folgenden CISCO-AV-PAIR

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

Advanced Attributes Settings

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

2.3 Klicken Sie auf **Speichern**.

Save Reset

Schritt 3: Wiederholen Sie Schritt 2 für die übrigen 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"

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="aaa" +

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="operations" +

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="read-only" +

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

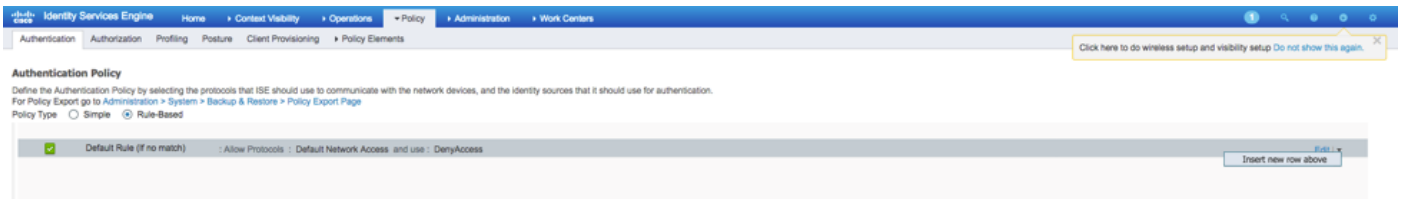
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco
<input type="checkbox"/>	Cisco_IP_Phones	Cisco
<input type="checkbox"/>	Cisco_WebAuth	Cisco
<input type="checkbox"/>	FXOS-AAA-PROFILE	Cisco
<input type="checkbox"/>	FXOS-ADMIN-PROFILE	Cisco
<input type="checkbox"/>	FXOS-OPER-PROFILE	Cisco
<input type="checkbox"/>	FXOS-ReadOnly-PROFILE	Cisco

Erstellen der Authentifizierungsrichtlinie

Schritt 1: Navigieren Sie zu **Richtlinien > Authentifizierung >** und klicken Sie auf den Pfeil neben Bearbeiten, um festzulegen, wo die Regel erstellt werden soll.



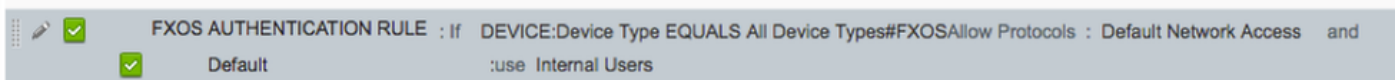
Schritt 2: Die Einrichtung ist einfach. Es kann detaillierter durchgeführt werden, aber für dieses Beispiel verwenden wir den Gerätetyp:

Name: **FXOS-AUTHENTIFIZIERUNGSREGEL**

IF Wählen Sie ein neues Attribut/einen neuen Wert aus: **Gerät:Der Gerätetyp ist gleich allen Gerätetypen #FXOS**

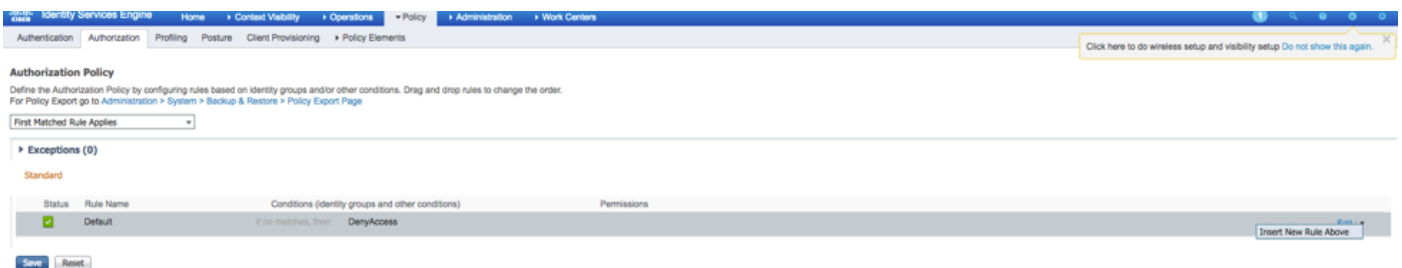
Protokolle zulassen: Standard-Netzwerkzugriff

Verwendung: Interne Benutzer



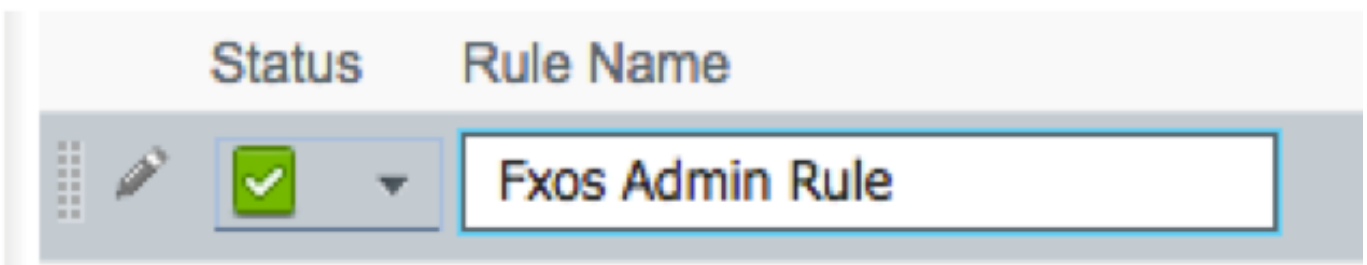
Erstellen der Autorisierungsrichtlinie

Schritt 1: Navigieren Sie zu **Richtlinien > Autorisierung >** und klicken Sie auf den Pfeil, um die Position zu bearbeiten, an der die Regel erstellt werden soll.

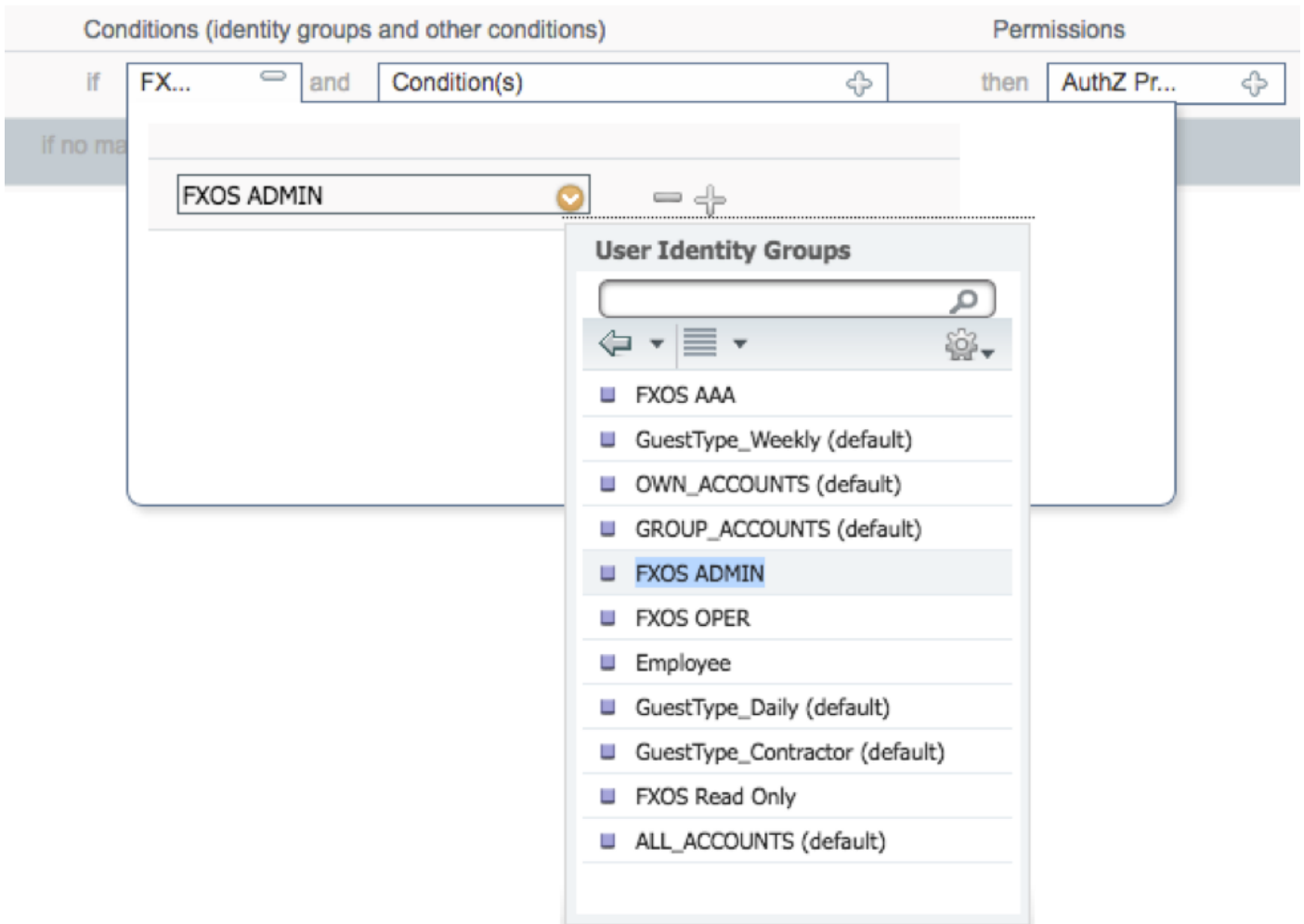


Schritt 2: Geben Sie die Werte für die Autorisierungsregel mit den erforderlichen Parametern ein.

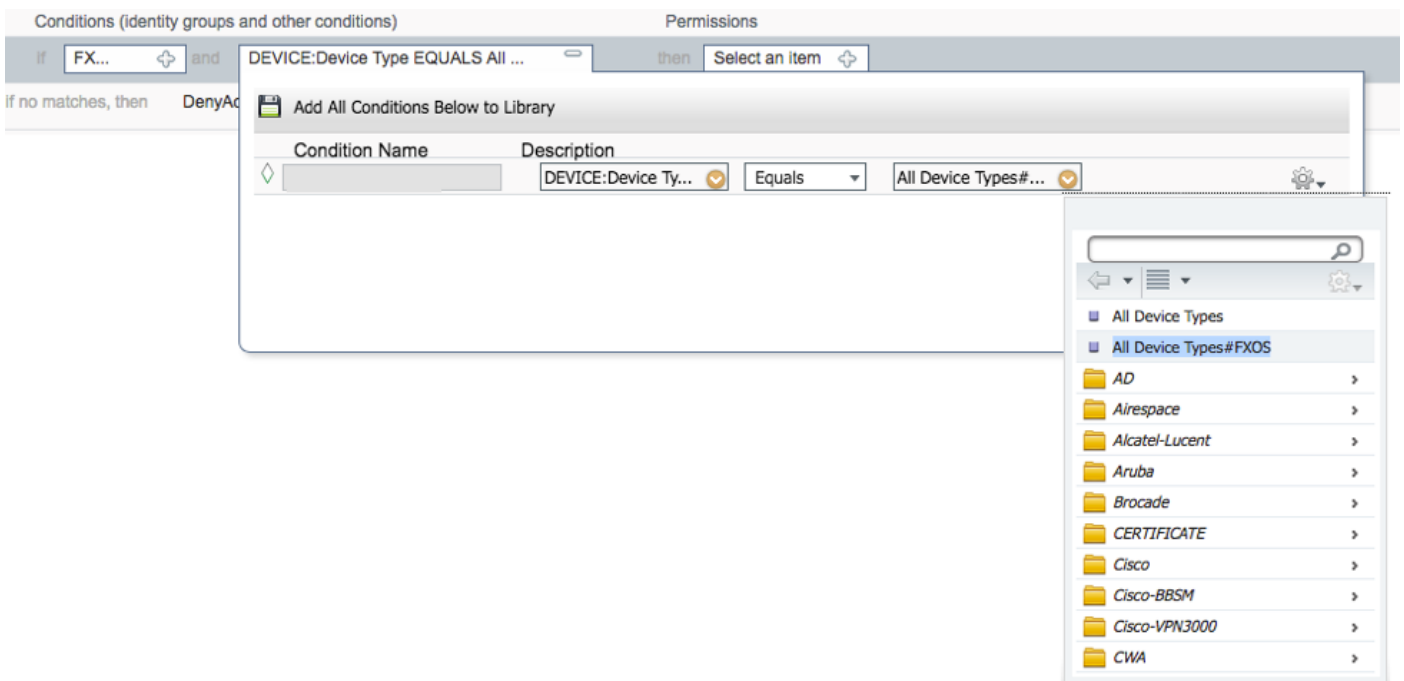
2.1 Regelname: **Fxos-Regel <BENUTZERROLLE>**.



2.2 Falls: Benutzeridentitätsgruppen > Wählen Sie **<BENUTZERROLLE>** aus.



2.3 UND: Neue Bedingung erstellen > Gerät: Der Gerätetyp entspricht **allen Gerätetypen #FXOS**.



2.4 Berechtigungen: Standard > **Benutzerrollenprofil** auswählen

Permissions

then FXOS-A...

FXOS-ADMIN-PROFILE

Standard

- Blackhole_Wireless_Access
- Cisco_IP_Phones
- Cisco_WebAuth
- DenyAccess
- FXOS-AAA-PROFILE
- FXOS-ADMIN-PROFILE**
- FXOS-OPER-PROFILE
- FXOS-ReadOnly-PROFILE
- NSP_Onboard
- Non_Cisco_IP_Phones
- PermitAccess

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Fxos Admin Rule	if FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE

Schritt 3: Wiederholen Sie Schritt 2 für alle Benutzerrollen.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Fxos Admin Rule	if FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE
<input checked="" type="checkbox"/>	Fxos AAA Rule	if FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-AAA-PROFILE
<input checked="" type="checkbox"/>	Fxos Oper Rule	if FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-OPER-PROFILE
<input checked="" type="checkbox"/>	Fxos Read only Rule	if FXOS Read Only AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ReadOnly-PROFILE
<input checked="" type="checkbox"/>	Default	if no matches, then DenyAccess	

Schritt 4: Klicken Sie unten auf der Seite auf **Speichern**.

 Save Reset

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

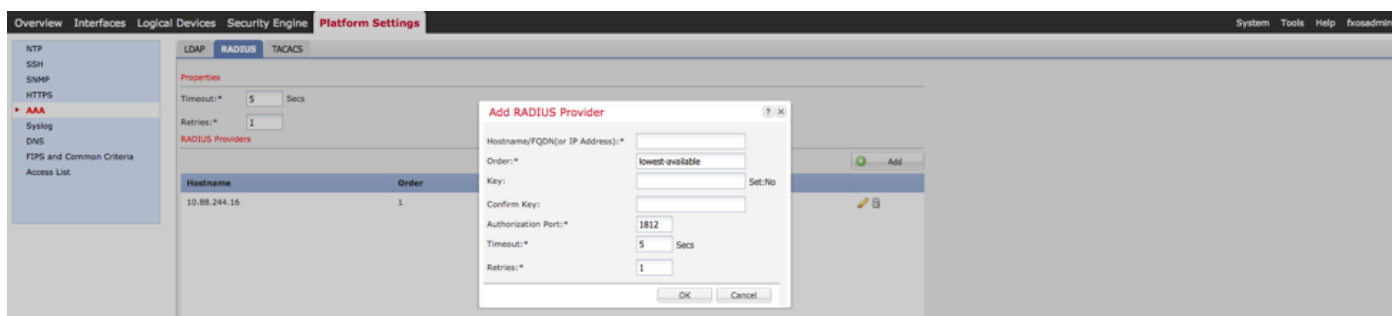
fp4120-TAC-A# Connect-FXOS

fp4120-TAC-A (fxos)# debug aaa-anfragen

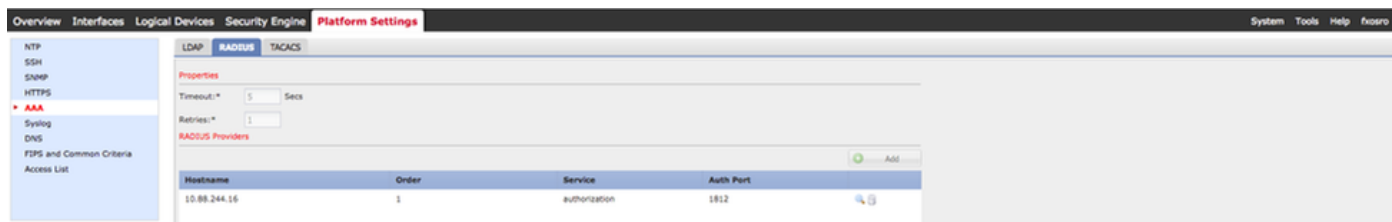
% Berechtigung verweigert für die Rolle

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

Administratorbenutzerrolle.



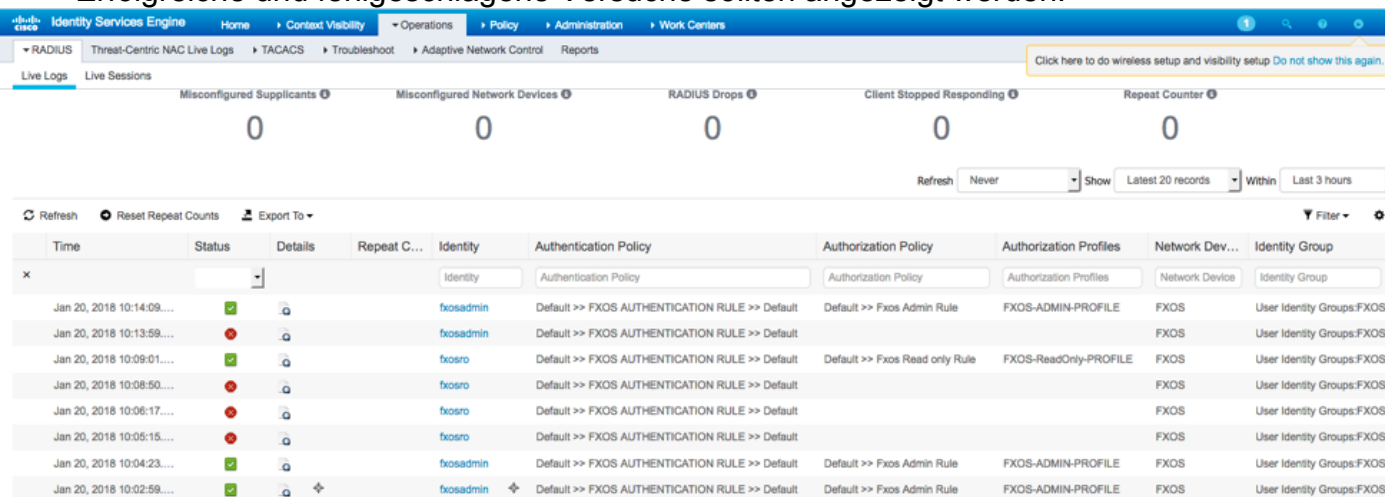
Schreibgeschützte Benutzerrolle.



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

ISE 2.0-Verifizierung

1. Navigieren Sie zu **Operations > RADIUS > Live logs (Vorgänge > RADIUS > Live-Protokolle)**. 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.

```
fpr4120-TAC-A# Connect-FXOS
```

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

```
fpr4120-TAC-A (fxos)# debug aaa event
```

```
fpr4120-TAC-A (fxos)# debug aaa errors
```

```
fpr4120-TAC-A (fxos)# term mon
```

Nach einem erfolgreichen Authentifizierungsversuch wird die folgende Ausgabe angezeigt.

```
20. Januar 2018 17:18:02.410275 aaa: aa_req_process für die Authentifizierung. Sitzung Nr. 0
```

```
20. Januar 2018 17:18:02.410297 aaa: aaa_req_process: Allgemeine AAA-Anfrage von  
Anwendung: login appln_subtype: Standard
```

```
20. Januar 2018 17:18:02.410310 aaa: try_next_aaa_method
```

```
20. Januar 2018 17:18:02.410330 aaa: Die konfigurierten Methoden gesamt sind 1, der aktuelle  
Index ist 0.
```

```
20. Januar 2018 17:18:02.410344 aaa: Handle_req_using_method
```

```
20. Januar 2018 17:18:02.410356 aaa: AAA_METHODE_SERVER_GRUPPE
```

```
20. Januar 2018 17:18:02.410367 aaa: aaa_sg_method_handler group = Radius
```

```
20. Januar 2018 17:18:02.410379 aaa: Verwenden des an diese Funktion übergebenen  
sg_protocol
```

```
20. Januar 2018 17:18:02.410393 aaa: Anfrage an RADIUS-Service senden
```

```
20. Januar 2018 17:18:02.41294 aaa: mts_send_msg_to_prot_daemon: Payload-Länge = 374
```

```
20. Januar 2018 17:18:02.412973 aaa: Sitzung: 0x8dfd68c zur Sitzungstabelle 1 hinzugefügt
```

```
20. Januar 2018 17:18:02.412987 aaa: Konfigurierte Methodengruppe erfolgreich
```

```
20. Januar 2018 17:18:02.656425 aaa: aaa_process_fd_set
```

```
20. Januar 2018 17:18:02.656447 aaa: aa_process_fd_set: mtscallback auf aaa_q
```

```
20. Januar 2018 17:18:02.656470 aaa: mts_message_response_handler: eine MTS-Antwort
```

```
20. Januar 2018 17:18:02.656483 aaa: prot_daemon_response_handler
```

20. Januar 2018 17:18:02.656497 aaa: Sitzung: 0x8dfd68c aus Sitzungstabelle 0 entfernt

20. Januar 2018 17:18:02.656512 aaa: is_aaa_resp_status_Succ= 1

20. Januar 2018 17:18:02.656525 aaa: is_aa_resp_status_Success ist TRUE

20. Januar 2018 17:18:02.656538 aaa: aa_send_client_response für die Authentifizierung.
session->flags=21. aa_resp->flags=0.

20. Januar 2018 17:18:02.65655 aaa: AAA_REQ_FLAG_NORMAL

20. Januar 2018 17:18:02.65657 aaa: mts_send_response erfolgreich

20. Januar 2018 17:18:02.700520 aaa: aa_process_fd_set: mtscallback auf aaa_accounting_q

20. Januar 2018 17:18:02.70068 aaa: ALTER OPCODE: accounting_interim_update_update

20. Januar 2018 17:18:02.700702 aaa: aa_create_local_acct_req: user=, session_id=,
log=Benutzer-FXOSOR hinzugefügt

20. Januar 2018 17:18:02.700725 aaa: aa_req_process for accounting. Sitzung Nr. 0

20. Januar 2018 17:18:02.700738 aaa: Die MTS-Anforderungsreferenz lautet NULL. LOKALE
Anforderung

20. Januar 2018 17:18:02.700749 aaa: Festlegen von AAA_REQ_RESPONSE_NOT_NEEDED

20. Januar 2018 17:18:02.700762 aaa: aaa_req_process: Allgemeine AAA-Anfrage von
Anwendung: default appln_subtype: Standard

20. Januar 2018 17:18:02.700774 aaa: try_next_aaa_method

20. Januar 2018 17:18:02.700798 aaa: Keine Standardmethoden konfiguriert

20. Januar 2018 17:18:02.700810 aaa: Keine Konfiguration für diese Anforderung verfügbar

20. Januar 2018 17:18:02.700997 aaa: aa_send_client_response für die Rechnungslegung.
session->flags=254. aa_resp->flags=0.

20. Januar 2018 17:18:02.7010 aaa: Antwort auf Buchungsanfrage der alten Bibliothek wird als
ERFOLG gesendet

20. Januar 2018 17:18:02.701021 aaa: Antwort nicht erforderlich

20. Januar 2018 17:18:02.701033 aaa: AAA_REQ_FLAG_LOCAL_RESP

20. Januar 2018 17:18:02.701044 aaa: aaa_cleanup_session

20. Januar 2018 17:18:02.701055 aaa: aaa_req sollte freigegeben werden.

20. Januar 2018 17:18:02.701067 aaa: Fallback-Methode lokal erfolgreich

20. Januar 2018 17:18:02.706922 aaa: aaa_process_fd_set

20. Januar 2018 17:18:02.706937 aaa: aa_process_fd_set: mtscallback auf aaa_accounting_q

20. Januar 2018 17:18:02.706959 aaa: ALTER OP CODE: accounting_interim_update_update

20. Januar 2018 17:18:02.706972 aaa: aa_create_local_acct_req: user=, session_id=, log=added user:fxosro to the role:read-only

Nach einem fehlgeschlagenen Authentifizierungsversuch wird die folgende Ausgabe angezeigt.

20. Januar 2018 17:15:18.102130 aaa: aaa_process_fd_set

20. Januar 2018 17:15:18.102149 aaa: aa_process_fd_set: mtscallback auf aaa_q

20. Januar 2018 17:15:18.102267 aaa: aaa_process_fd_set

20. Januar 2018 17:15:18.102281 aaa: aa_process_fd_set: mtscallback auf aaa_q

20. Januar 2018 17:15:18.102363 aaa: aaa_process_fd_set

20. Januar 2018 17:15:18.10237 aaa: aa_process_fd_set: mtscallback auf aaa_q

20. Januar 2018 17:15:18.102456 aaa: aaa_process_fd_set

20. Januar 2018 17:15:18.102468 aaa: aa_process_fd_set: mtscallback auf aaa_q

20. Januar 2018 17:15:18.102489 aaa: mts_aaa_req_prozess

20. Januar 2018 17:15:18.102503 aaa: aa_req_process für die Authentifizierung. Sitzung Nr. 0

20. Januar 2018 17:15:18.102526 aaa: aaa_req_process: Allgemeine AAA-Anfrage von Anwendung: login appln_subtype: Standard

20. Januar 2018 17:15:18.102540 aaa: try_next_aaa_method

20. Januar 2018 17:15:18.102562 aaa: Die konfigurierten Methoden gesamt sind 1, der aktuelle Index ist 0.

20. Januar 2018 17:15:18.102575 aaa: Handle_req_using_method

20. Januar 2018 17:15:18.102586 aaa: AAA_METHODE_SERVER_GRUPPE

20. Januar 2018 17:15:18.102598 aaa: aaa_sg_method_handler group = Radius

20. Januar 2018 17:15:18.102610 aaa: Verwenden des an diese Funktion übergebenen sg_protocol

20. Januar 2018 17:15:18.102625 aaa: Anfrage an RADIUS-Service senden

20. Januar 2018 17:15:18.102658 aaa: mts_send_msg_to_prot_daemon: Payload-Länge = 371

20. Januar 2018 17:15:18.102684 aaa: Sitzung: 0x8dfd68c zur Sitzungstabelle 1 hinzugefügt

20. Januar 2018 17:15:18.102698 aaa: Konfigurierte Methodengruppe erfolgreich

20. Januar 2018 17:15:18.273682 aaa: aaa_process_fd_set

20. Januar 2018 17:15:18.273724 aaa: aa_process_fd_set: mtscallback auf aaa_q

20. Januar 2018 17:15:18.273753 aaa: mts_message_response_handler: eine MTS-Antwort

20. Januar 2018 17:15:18.273768 aaa: prot_daemon_response_handler

20. Januar 2018 17:15:18.273783 aaa: Sitzung: 0x8dfd68c aus Sitzungstabelle 0 entfernt

20. Januar 2018 17:15:18.273801 aaa: is_aa_resp_status_Success status = 2

20. Januar 2018 17:15:18.273815 aaa: is_aa_resp_status_Success ist TRUE

20. Januar 2018 17:15:18.273829 aaa: aa_send_client_response für die Authentifizierung. session->flags=21. aa_resp->flags=0.

20. Januar 2018 17:15:18.273843 aaa: AAA_REQ_FLAG_NORMAL

20. Januar 2018 17:15:18.27387 aaa: mts_send_response erfolgreich

20. Januar 2018 17:15:18.273902 aaa: aaa_cleanup_session

20. Januar 2018 17:15:18.273916 aaa: mts_drop der Anfrage msg

20. Januar 2018 17:15:18.273935 aaa: aaa_req sollte freigegeben werden.

20. Januar 2018 17:15:18.280416 aaa: aaa_process_fd_set

20. Januar 2018 17:15:18.280443 aaa: aa_process_fd_set: mtscallback auf aaa_q

20. Januar 2018 17:15:18.280454 aaa: aa_enable_info_config: GET_REQ für eine Anmeldefehlermeldung

20. Januar 2018 17:15:18.280460 aaa: Rückgabewert des Konfigurationsvorgangs zurückerhalten:Unbekannter Sicherheitsaspekt

Zugehörige Informationen

Der Ethalyzer-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](#)