

# FirePOWER eXtensible Operating System (FXOS) 2.2: Chassis-Authentifizierung und -Autorisierung für Remote-Management mit ACS über RADIUS

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Konfigurieren des FXOS-Chassis](#)

[Konfigurieren des ACS-Servers](#)

[Überprüfen](#)

[Überprüfung des FXOS-Chassis](#)

[ACS-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 den Access Control Server (ACS) 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 ACS-Konfiguration

### Verwendete Komponenten

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

- Cisco FirePOWER 4120 Security Appliance Version 2.2
- Virtual Cisco Access Control Server Version 5.8.0.32

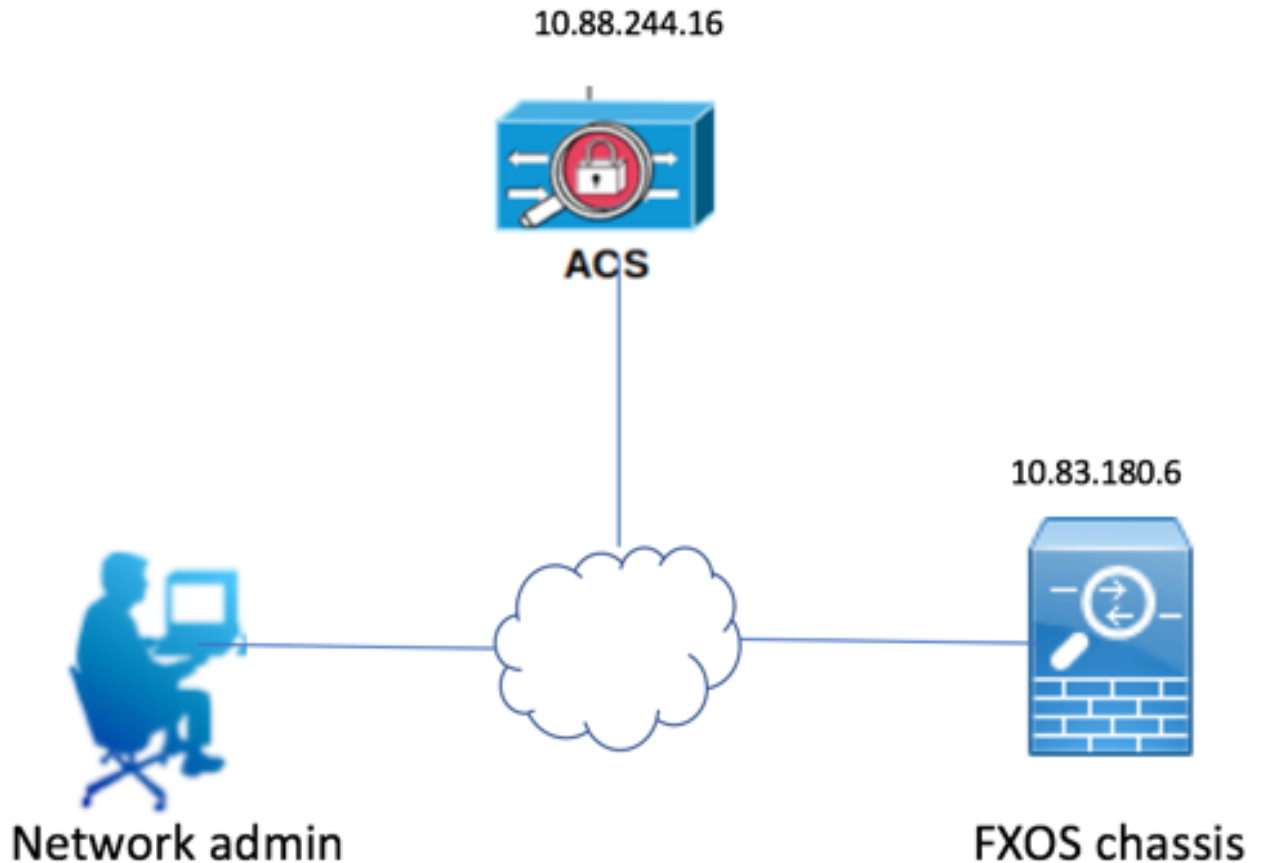
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines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

## Konfigurieren

Ziel der Konfiguration ist es,

- Authentifizierung von Benutzern, die sich über ACS in der webbasierten Benutzeroberfläche und im SSH von FXOS anmelden
- Autorisieren Sie Benutzer, die sich über ACS in der webbasierten GUI und im SSH von FXOS anmelden, entsprechend ihrer jeweiligen Benutzerrolle.
- Überprüfen Sie, ob die FXOS-Authentifizierung und -Autorisierung mit ACS ordnungsgemäß funktioniert.

# Netzwerkdiagramm



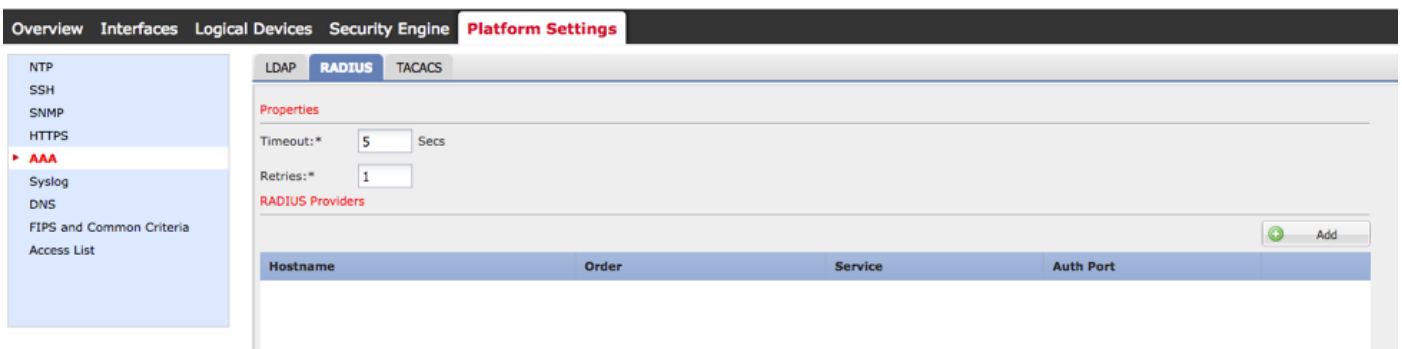
## Konfigurationen

### 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 im Dialogfeld RADIUS-Anbieter hinzufügen die erforderlichen Werte ein.

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

**Add RADIUS Provider**

Hostname/FQDN(or IP Address):\* 10.88.244.16

Order:\* lowest-available

Key: ..... Set:No

Confirm Key: .....|

Authorization Port:\* 1812

Timeout:\* 5 Secs

Retries:\* 1

OK Cancel

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

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

LDAP **RADIUS** TACACS

Properties

Timeout:\* 5 Secs

Retries:\* 1

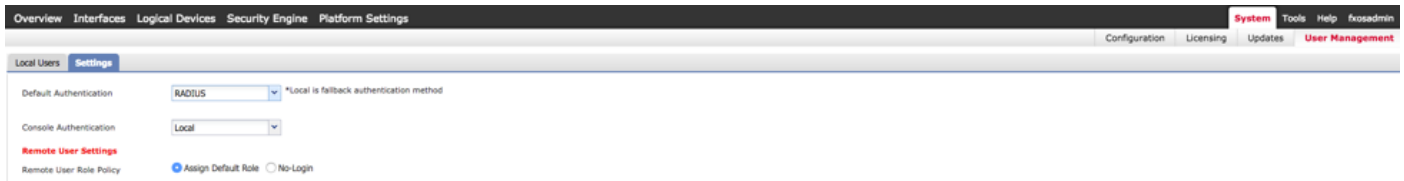
RADIUS Providers

Hostname	Order	Service	Auth Port	
10.88.244.16	1	authorization	1812	

Save Cancel

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

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



## 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 10.88.244.16 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: 10.88.244.16

Beschreibung:

Bestellung: 1

Auth-Port: 1812

Schlüssel: **\*\*\*\*\***

Timeout: 5

## **Konfigurieren des ACS-Servers**

### **Hinzufügen des FXOS als Netzwerkressource**

Schritt 1: Navigieren Sie zu **Netzwerkressourcen > Netzwerkgeräte und AAA-Clients**.

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

My Workspace

**Network Resources**

- Network Device Groups
  - Location
  - Device Type
  - Network Devices and AAA Clients**
  - Default Network Device
  - External Proxy Servers
  - OCSP Services
- Users and Identity Stores
- Policy Elements
- Access Policies
- Monitoring and Reports
- System Administration

Network Resources > Network Devices and AAA Clients

**Network Devices**

Filter:  Match if:

<input type="checkbox"/>	Name	IP Address	Description	NDG:Location	NDG:Device Type
<input type="checkbox"/>	<a href="#">APIC1P1</a>	10.88.247.4/32		All Locations	All Device Types
<input type="checkbox"/>	<a href="#">APIC1P22</a>	10.48.22.69/32		All Locations	All Device Types
<input type="checkbox"/>	<a href="#">ASA</a>	10.88.244.12/32		All Locations	All Device Types
<input type="checkbox"/>	<a href="#">ASA_10.88.244.60</a>	10.88.244.60/32	ASA_10.88.244.60	All Locations	All Device Types
<input type="checkbox"/>	<a href="#">Firesight</a>	10.88.244.11/32		All Locations	All Device Types
<input type="checkbox"/>	<a href="#">FMC 6.1</a>	10.88.244.51/32		All Locations	All Device Types
<input type="checkbox"/>	<a href="#">FXQS</a>	10.83.180.6/32		All Locations	All Device Types

|

Schritt 3: Geben Sie die erforderlichen Werte ein (Name, IP-Adresse, Gerätetyp und RADIUS aktivieren sowie SCHLÜSSEL hinzufügen).

Name:

Description:

**Network Device Groups**

Location

Device Type

**IP Address**

Single IP Address    IP Subnets    IP Range(s)

IP:

**Authentication Options**

▼ TACACS+

Shared Secret:

Single Connect Device

Legacy TACACS+ Single Connect Support

TACACS+ Draft Compliant Single Connect Support

▼ RADIUS

Shared Secret:

CoA port:

Enable KeyWrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format  ASCII    HEXADECIMAL

= Required fields

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



