

Firepower eXtensible Operating System (FXOS)

2.2: Chassis Verificatie en autorisatie voor extern beheer met ACS met TACACS+.

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Het FXOS-chassis configureren](#)

[De ACS-server configureren](#)

[Verifiëren](#)

[Verificatie FXOS-chassis](#)

[ACS-verificatie](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u TACACS+ verificatie en autorisatie voor het FirePOWER Xtensible Operating System (FXOS) chassis kunt configureren via Access Control Server (ACS).

Het FXOS-chassis bevat de volgende gebruikersrollen:

- Administrator - volledige toegang tot het volledige systeem voor lezen en schrijven. De standaard admin-account krijgt deze rol standaard toegewezen en kan niet worden gewijzigd.
- Alleen-lezen - alleen-lezen toegang tot de systeemconfiguratie zonder bevoegdheden om de systeemstatus te wijzigen.
- Operations - lees-en-schrijftoegang tot de NTP-configuratie, Smart Call Home-configuratie voor slimme licenties en systeemlogbestanden, inclusief systeemservern en fouten. Lees de toegang tot de rest van het systeem.
- AAA - lees-en-schrijf toegang tot gebruikers, rollen en AAA-configuratie. Lees de toegang tot de rest van het systeem.

Via CLI kan dit als volgt worden gezien:

```
fpr4120-TAC-A/security* # rol
```

Rol:

Functienaam Priv

— —

Aa aaa

beheerder

operaties

alleen-lezen

Bijgedragen door Tony Ramirez, Jose Soto, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van FirePOWER Xtensible Operating System (FXOS)
- Kennis van de ACS-configuratie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firepower 4120 security applicatie versie 2.2
- Virtual Access Control Server versie 5.8.0.32

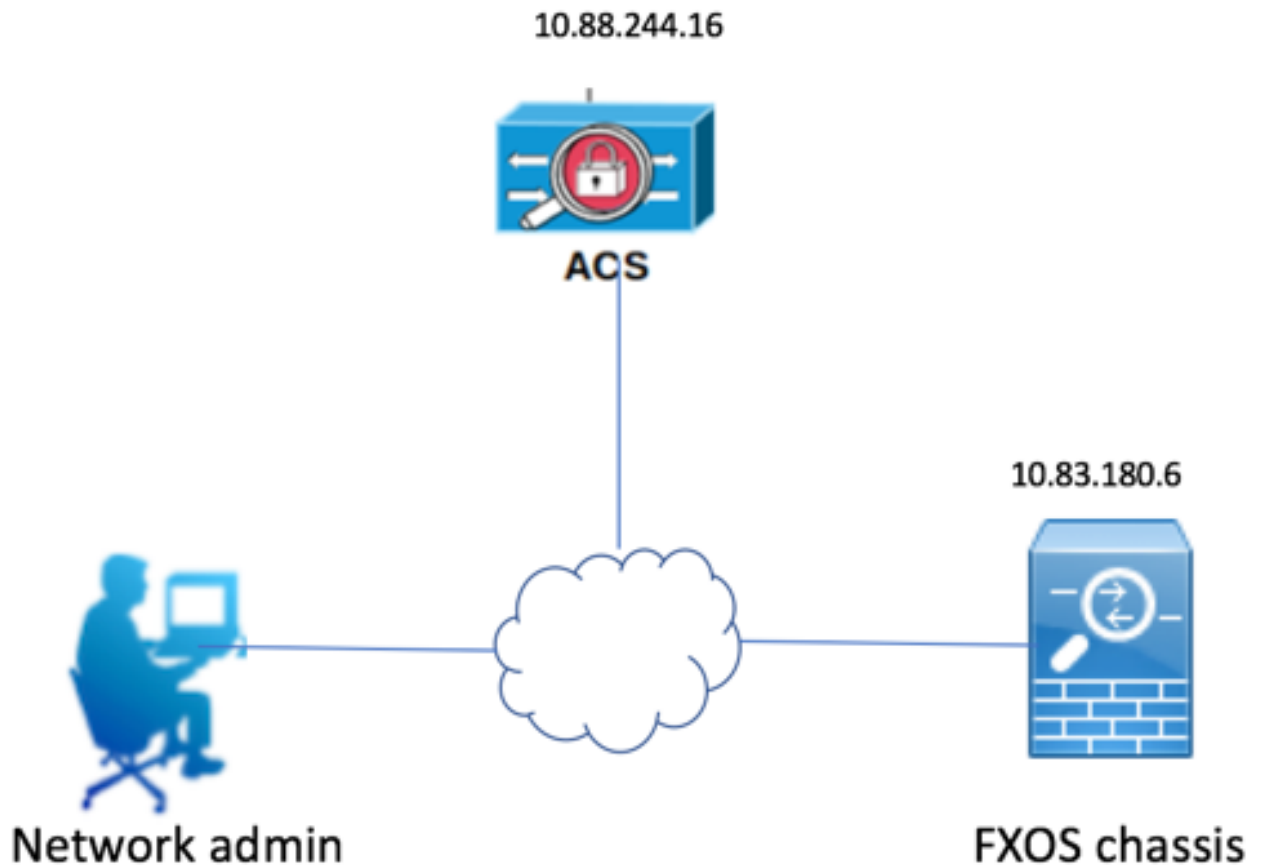
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Het doel van de configuratie is:

- Verifieer gebruikers loggen in de op Web-Based GUI en SSH van FXOS door middel van ACS.
- Geef gebruikers toestemming om te loggen in de op het web gebaseerde GUI en SSH van FXOS volgens hun respectieve gebruikersrol door middel van ACS.
- Controleer de goede werking van de echtheidscontrole en de vergunning op de FXOS door middel van ACS.

Netwerkdigram



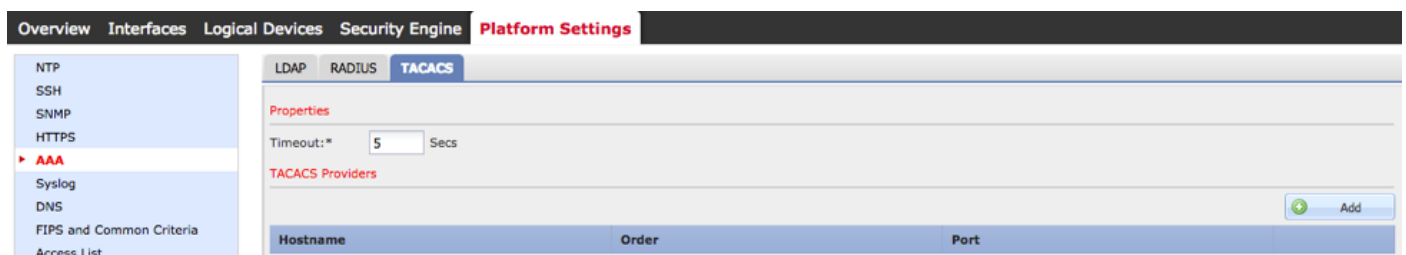
Configuraties

Het FXOS-chassis configureren

Een TACACS-provider maken met Chassis Manager

Stap 1. Navigeer naar **platform instellingen > AAA**.

Stap 2. Klik op het tabblad **TACACS**.



Stap 3. Voor elke TACACS+ provider die u wilt toevoegen (maximaal 16 providers).

3.1. Klik in het gebied TACACS Providers op **Toevoegen**.

3.2. Typ de gewenste waarden in het dialoogvenster TACACS-providers toevoegen.

3.3. Klik op **OK** om het dialoogvenster Add TACACS Provider te sluiten.

Add TACACS Provider

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: No

Confirm Key:

Port:*

Timeout:* Secs

Stap 4. Klik op Opslaan.

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

TACACS Providers

Hostname	Order	Port
10.88.244.16	1	49

Stap 5. Navigeer naar **Systeem > Gebruikersbeheer > Instellingen**.

Stap 6. Selecteer onder Standaardverificatie de optie **TACACS**.

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

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

Een TACACS+ provider maken met CLI

Stap 1. Om TACACS-verificatie mogelijk te maken, voert u de volgende opdrachten uit.

voor de **beveiliging** van 4120-TAC-A# bereik

fpr4120-TAC-A/security #bereik: standaardinstelling

fpr4120-TAC-A/security/default-auth #set-realm-tac's

Stap 2. Gebruik de opdracht **Details tonen** om de resultaten weer te geven.

fpr4120-TAC-A/security/default-auth # details laten zien

Standaardverificatie:

Admin Realm: **Tacacs**

Operationeel antwoord: **Tacacs**

Web sessie verfrissing periode (in seconden): 600

Session timeout (in s) voor web-, ssh-, telnet-sessies: 600

Absolute sessietijd (in seconden) voor web-, ssh-, telnet-sessies: 3600

Seriële console-sessietijd (in seconden): 600

Seriële console absolute sessietijd (in seconden): 3600

Admin-servergroep:

Vak Operationele verificatieserver:

Gebruik van de tweede factor: Nee

Stap 3. Om de TACACS-serverparameters te configureren voert u de volgende opdrachten uit.

voor de **beveiliging** van 4120-TAC-A# bereik

fr4120-TAC-A/security # tac-werkings sfeer

fpr4120-TAC-A/security/tacacs # server 10.8.244.50

fpr4120-TAC-A/security/tacacs/server # ingestelde "ACS-server"

fpr4120-TAC-A/security/tacacs/server* # ingestelde toets

Geef de toets op: *********

Bevestig de toets: *********

Stap 4. Gebruik de opdracht **Details tonen** om de resultaten weer te geven.

fpr4120-TAC-A/security/tacacs/server* # details laten zien

TACACS+ server:

Hostname, FQDN of IP-adres: 10.88.244.50

Descr:

Volgorde: 1

Port: 49

Sleutel: ****

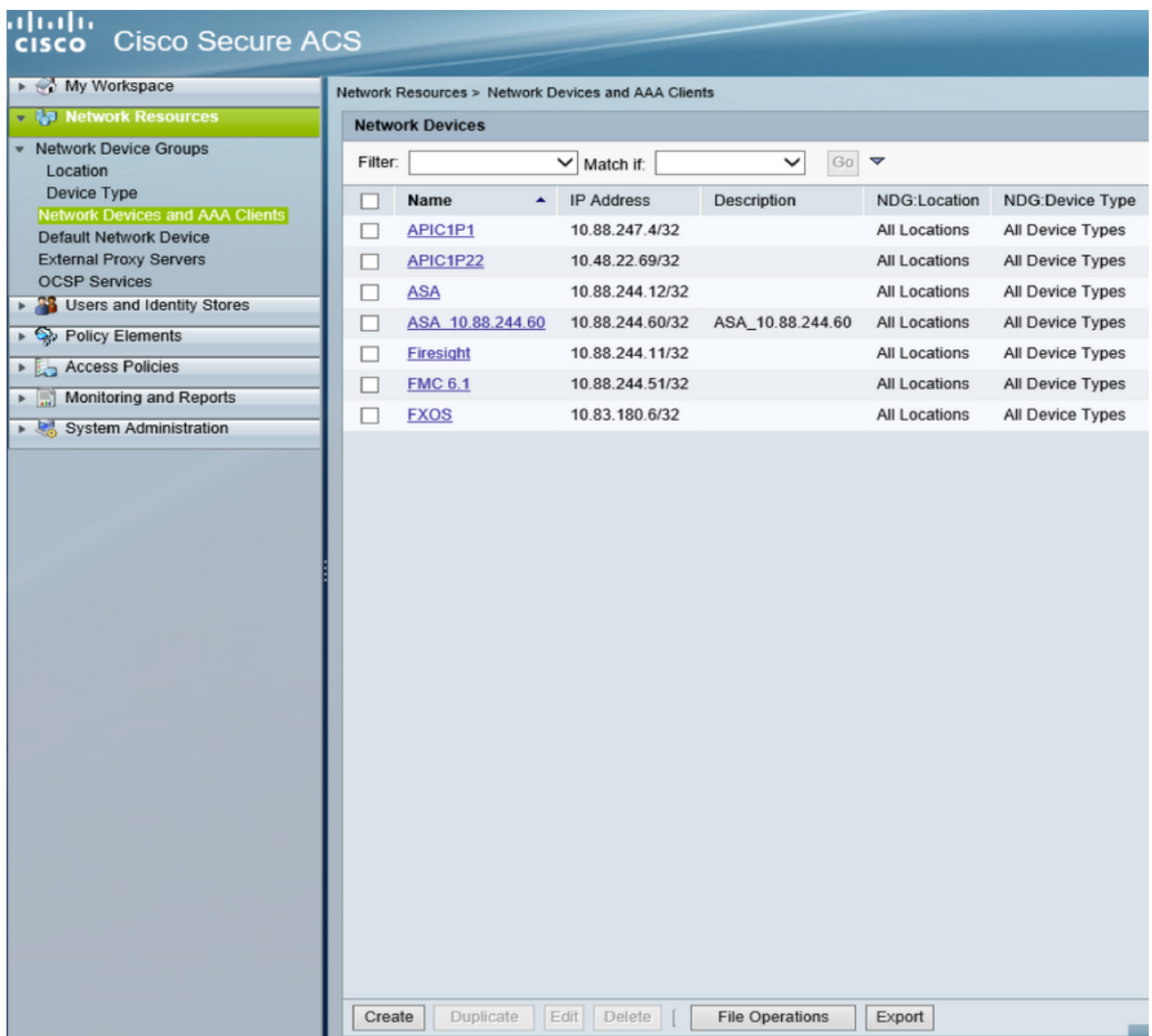
Time-out: 5

De ACS-server configureren

De FXOS als netwerkresource toevoegen

Stap 1. Navigeer naar **netwerkbronnen > Netwerkapparaten en AAA-clients**.

Stap 2. Klik op **Maken**.



The screenshot shows the Cisco Secure ACS web interface. The left-hand navigation menu is expanded to 'Network Resources', and 'Network Devices and AAA Clients' is selected. The main content area displays a table of network devices with the following columns: Name, IP Address, Description, NDG:Location, and NDG:Device Type. The table contains the following data:

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

At the bottom of the interface, there are buttons for 'Create', 'Duplicate', 'Edit', 'Delete', 'File Operations', and 'Export'.

Stap 3. Voer de gewenste waarden in (naam, IP-adres, apparaattype en TACACS+ inschakelen)

en voeg de SLEUTEL toe).

Network Resources > Network Devices and AAA Clients > Edit: "FXOS"

Name:

Description:

Network Device Groups

Location

Device Type

IP Address

Single IP Address IP Subnets IP Range(s)

IP:

TACACS+

RADIUS

= Required fields

Stap 4. Klik op **Indienen**.

