

Configureer ISE Radius-verificatie voor Secure Firewall Chassis Manager (FCM)

Inhoud

Inleiding

Dit document beschrijft het proces voor het configureren van RADIUS-autorisatie/verificatie-toegang voor Secure Firewall Chassis Manager met ISE.

Voorwaarden

Vereisten

Cisco raadt aan kennis te hebben van de volgende onderwerpen:

- Secure Firewall Chassis Manager (FCM)
- Cisco Identity Services Engine (ISE)
- Radius-verificatie

Gebruikte componenten

- Cisco FirePOWER 4110 security applicatie FXOS v2.12
- Cisco Identity Services Engine (ISE) v3.2-patch 4

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Configuraties

Secure Firewall-chassis beheer

Stap 1. Meld u aan bij de Firepower Chassis Manager GUI.

Stap 2. Naar platforminstellingen navigeren

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

FPR4K-1-029A78B 172.16.0.130
 Model: Cisco Firepower 4110 Security Appliance | Version: 2.12(0.8) | Operational State: Operable | Chassis Uptime 00:06:02:19

CONSOLE MGMT USB
 Power 1 - Running | Power 2 - Removed

Network Module 1: 1, 3, 5, 7, 2, 4, 6, 8
 Network Module 2 : Empty
 Network Module 3 : Empty

FAULTS 3(3) CRITICAL | 0(0) MAJOR
INTERFACES 3 DOWN | 5 UP
INSTANCES 0 DOWN | 1 UP
LICENSE Smart Agent UNREGISTERED
INVENTORY 1(1) Security Engine | 6(6) Fans | 1(2) Power Supplies

Severity	Description	Cause	Occurrence	Time	Acknowledged
CRITICAL	FPGA version lower than 2.00 is detected. A critical upgrade from the firmwar...	fpga-upgrade-required	1	2022-02-20T22:32:45.641	no
CRITICAL	Network Module 3 removed when in online state. It is recommended to set m...	module-surprise-removal	1	2022-11-07T09:03:02.022	no

8 Successful Login in last 24 hrs - View Details | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

Stap 3. Klik in het linkermenu op AAA. Selecteer Radius en voeg een nieuwe RADIUS-provider toe.

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

NTP
 SSH
 SNMP
 HTTPS
AAA
 Syslog
 DNS
 FIPS and Common Criteria
 Access List
 MAC Pool
 Resource Profiles
 Network Control Policy
 Chassis URL

LDAP **RADIUS** TACACS

Properties
 Timeout:* 5 Secs
 Retries:* 1

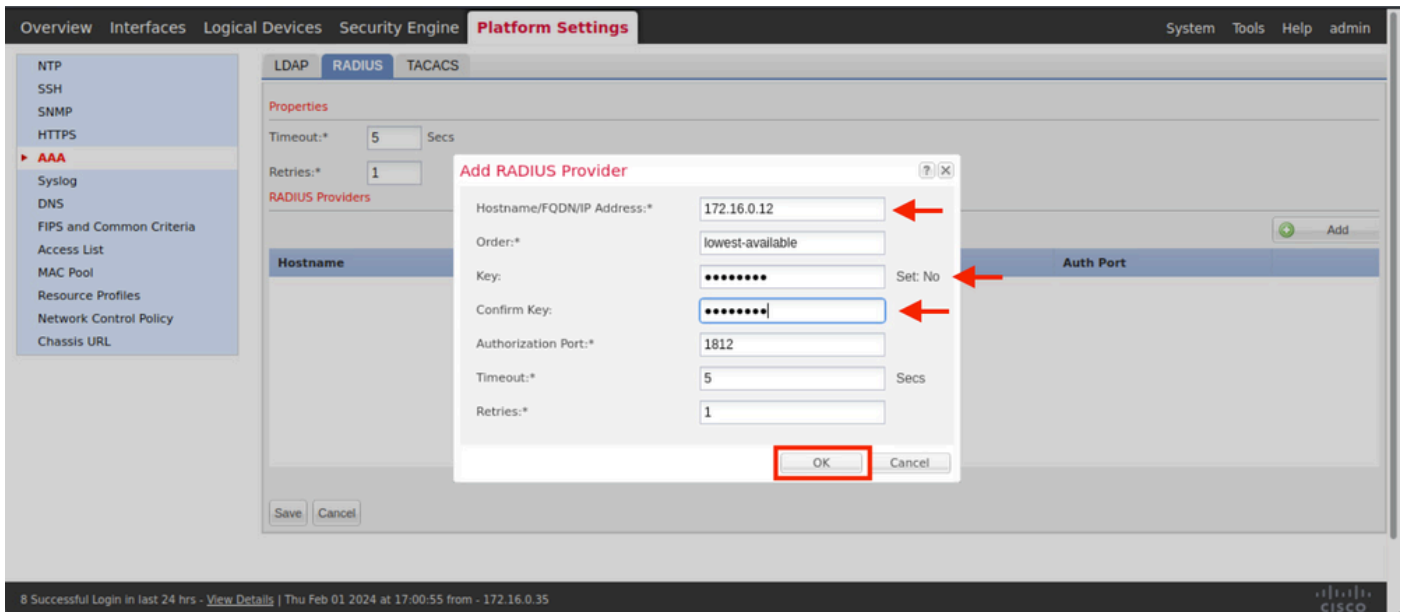
RADIUS Providers + Add

Hostname	Order	Service	Auth Port
----------	-------	---------	-----------

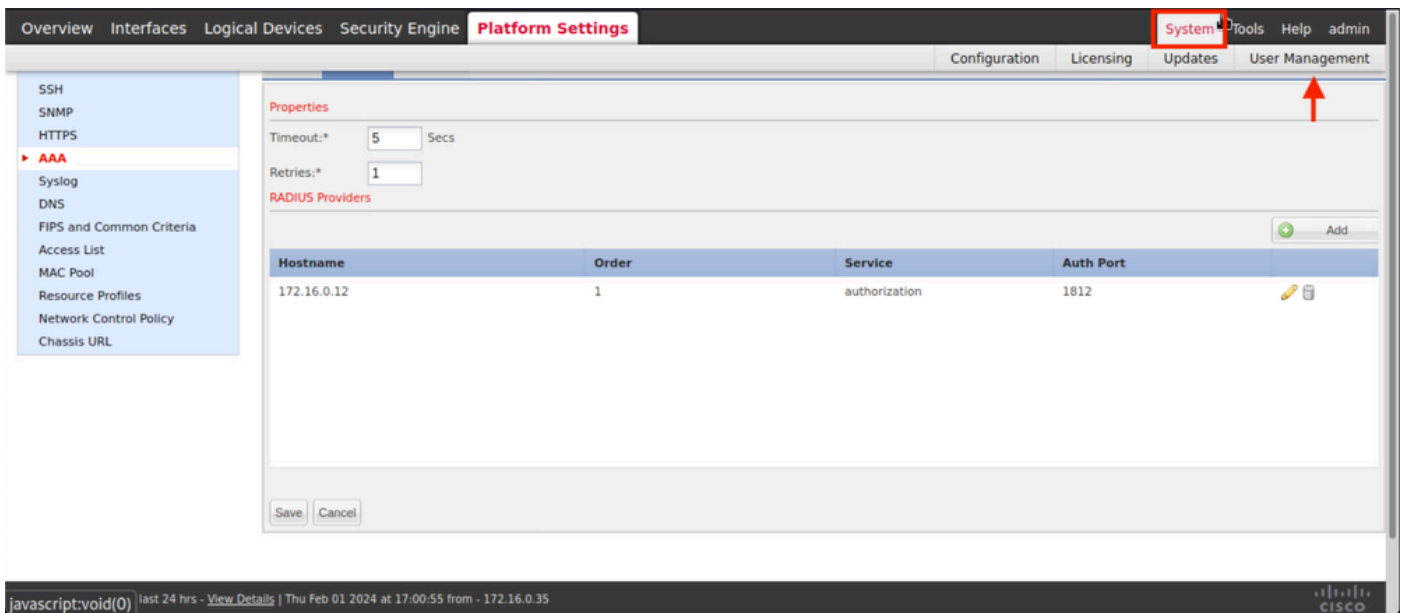
Save Cancel

8 Successful Login in last 24 hrs - View Details | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

Stap 4. Vul het promptmenu in met de gevraagde informatie van de Radius Provider. Klik op OK.



Stap 5. Navigeren naar systeem > Gebruikersbeheer



Stap 6. Klik op het tabblad Instellingen en stel de standaardverificatie in het uitrolmenu in op Straal, blader vervolgens naar beneden en sla de configuratie op.


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

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication

Local *Local is fallback authentication method

Local
RADIUS 
LDAP
TACACS
None
No-Login

Console Authentication

Remote User Settings

Remote User Role Policy

Local User Settings

Password Strength Check Enable

History Count (0-disabled,1-15)

Change Interval (1-730 hours)

Change Count (1-10)

No Change Interval (1-730 hours)

Days until Password Expiration (0-never,1-9999 days)

Password Expiration Warning Period (0-9999 days)

Expiration Grace Period (0-9999 days)

Password Reuse Interval (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet) (0-never,3600 seconds)

8 Successful Login in last 24 hrs - [View Details](#) | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

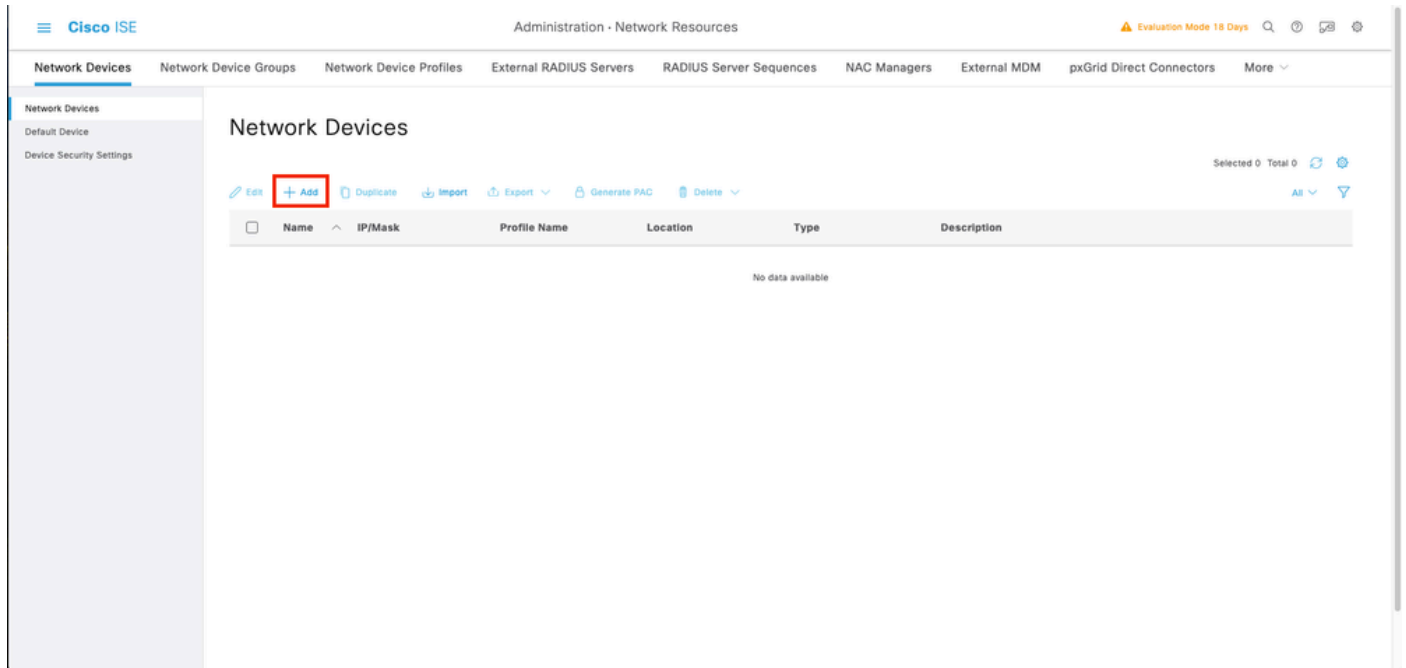
CISCO

Opmerking: de FCM-configuratie is op dit punt voltooid.

Identity Service Engine

Stap 1. Voeg een nieuw netwerkapparaat toe.

Navigeer naar het hamburgerpictogram ≡ in de linker bovenhoek > Beheer > Netwerkbronnen > Netwerkapparaten > +Add.

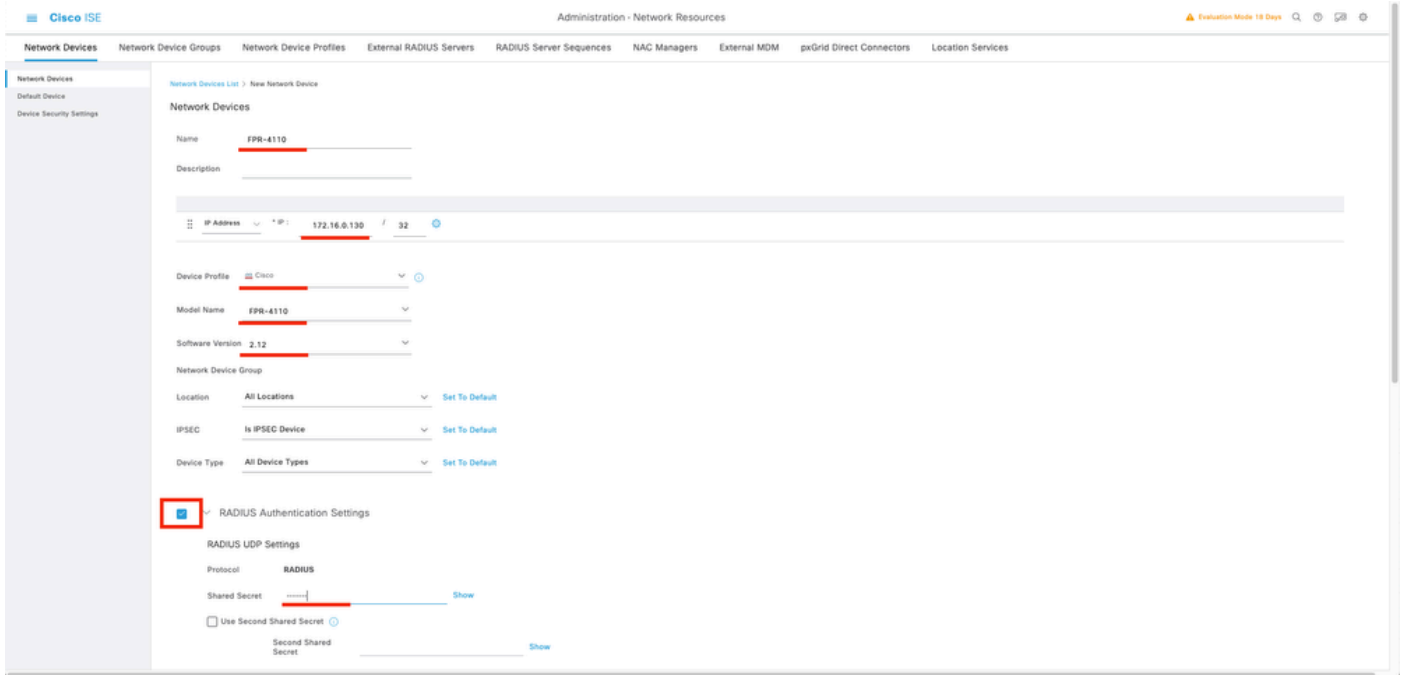


Stap 2. Vul de gevraagde parameters in over de nieuwe informatie over netwerkapparaten.

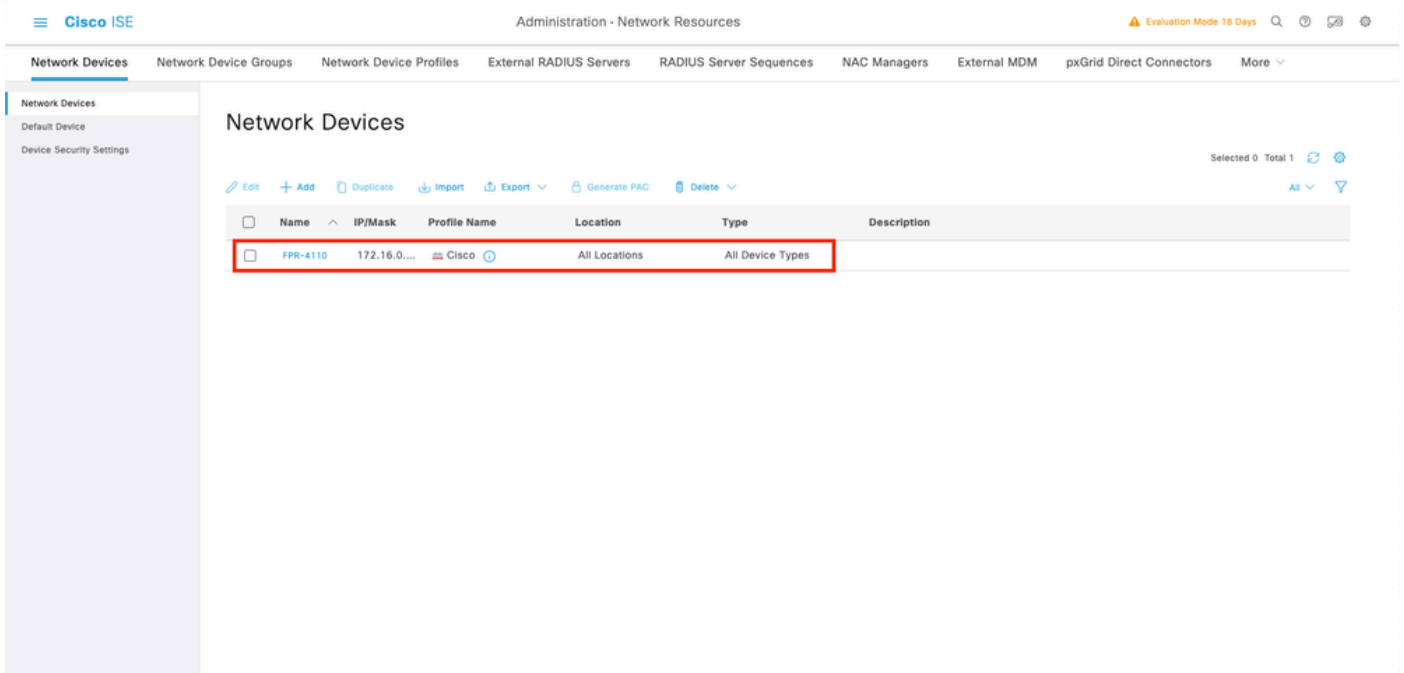
2.1 Schakel het aanvinkvakje RADIUS in

2.2. Configureer dezelfde gedeelde geheime sleutel als in de configuratie van de FCM-straal.

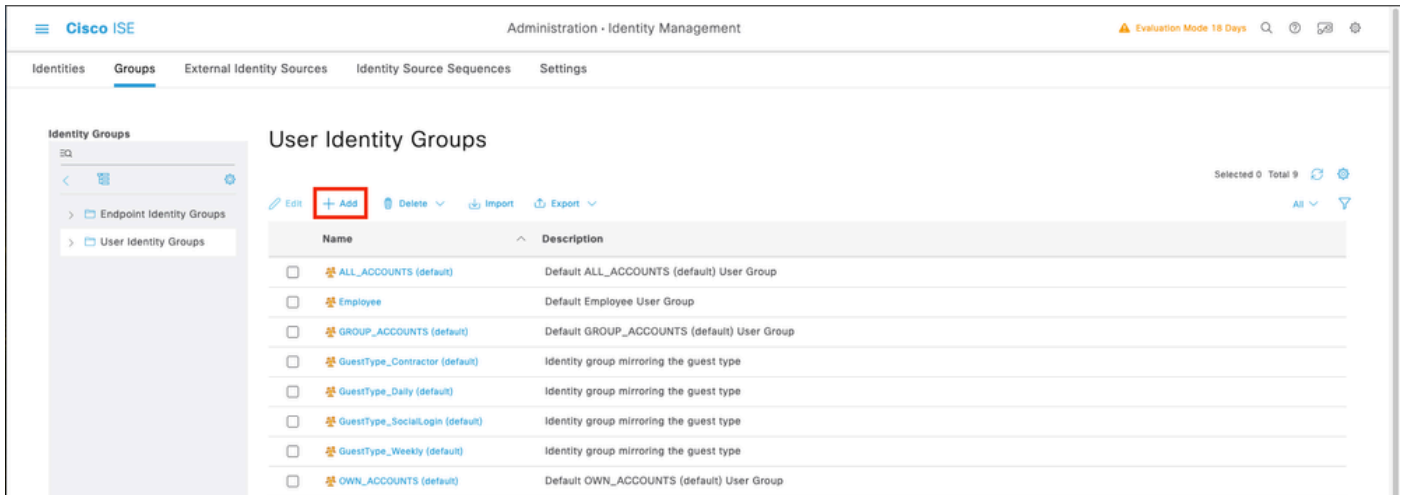
2.1 Scroll naar beneden en klik op Indienen.



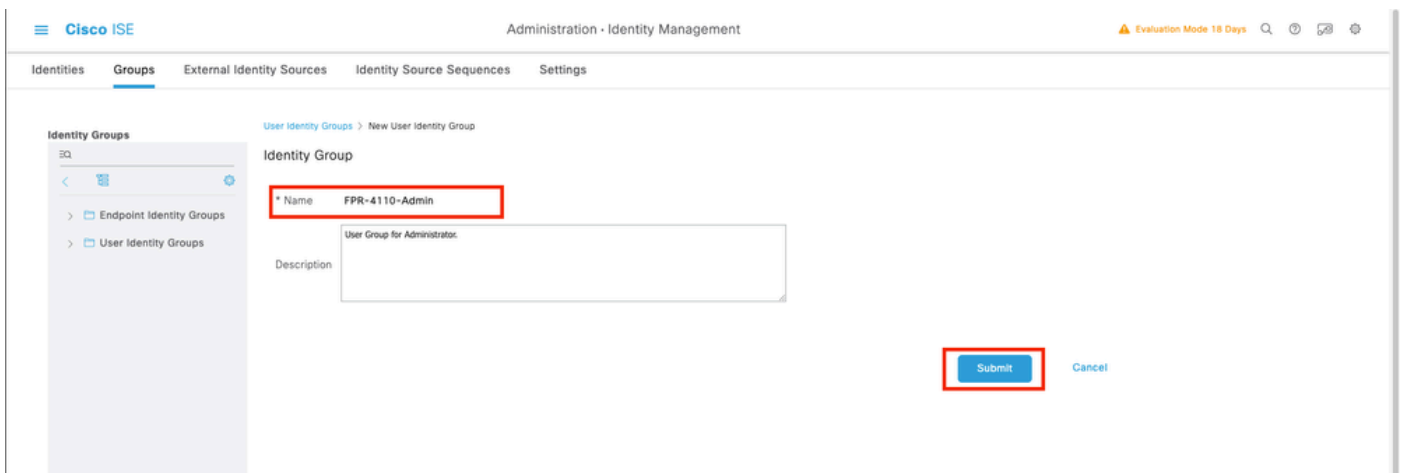
Stap 3. Het nieuwe apparaat valideren wordt weergegeven onder Netwerkkaparameters.



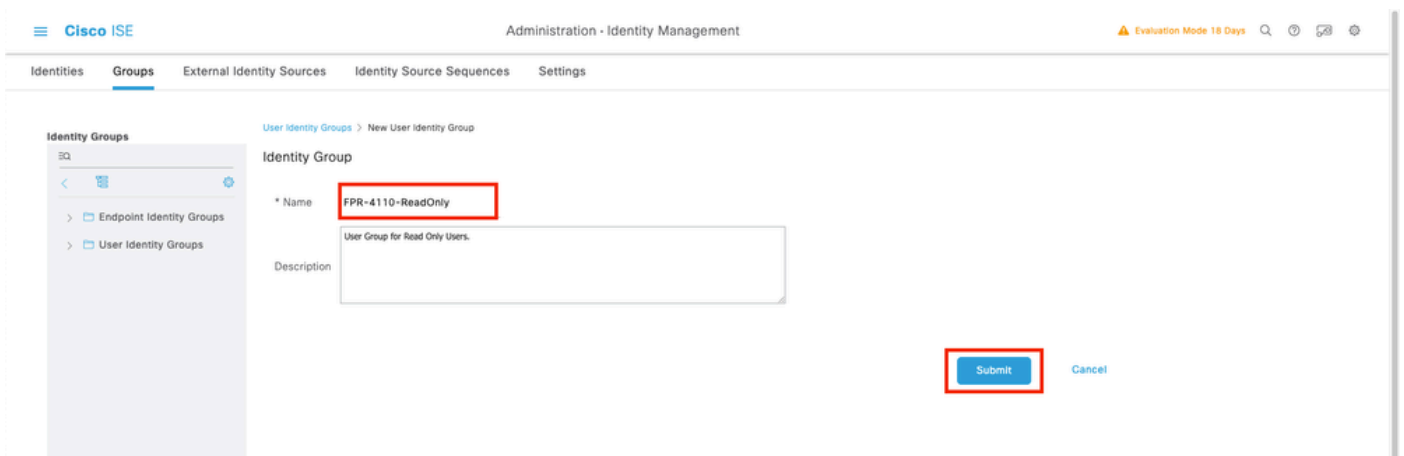
Stap 4. Maak de gewenste gebruikers-identiteitsgroepen. Navigeer naar het hamburgerpictogram ≡ in de linkerbovenhoek > Administratie > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen > + Toevoegen



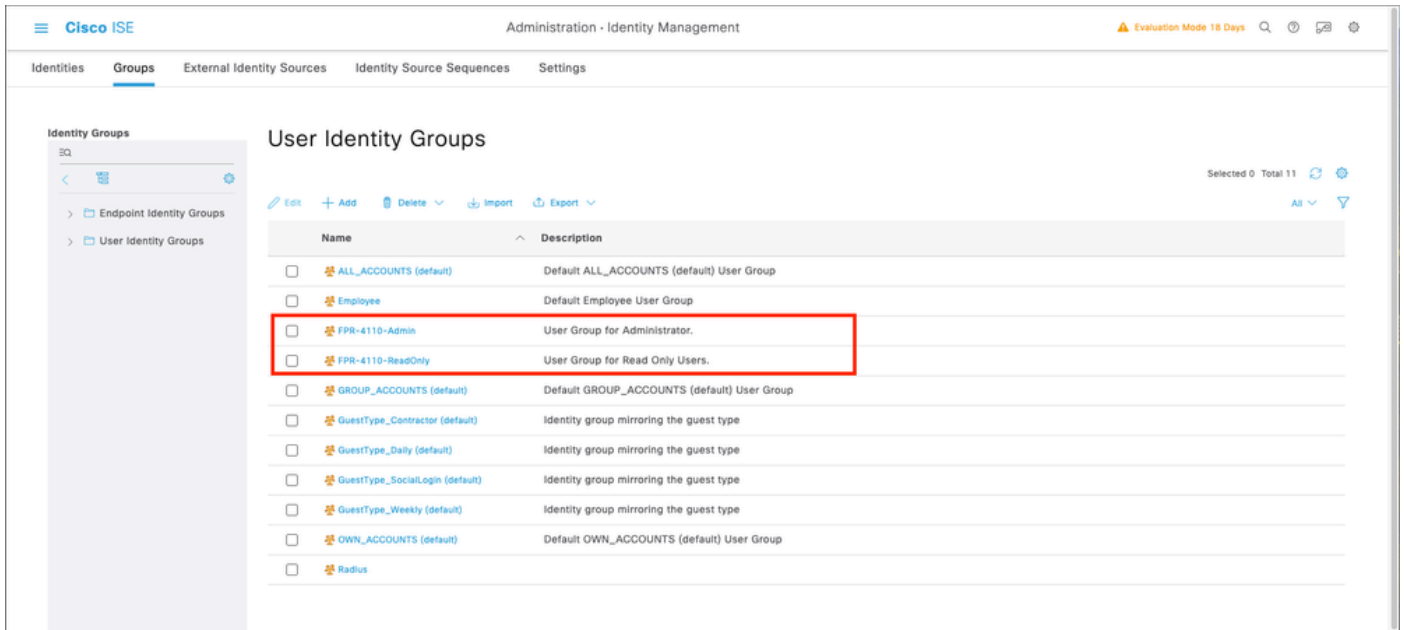
Stap 5. Stel een naam in voor de Admin User Identity Group en klik op Indienen om de configuratie op te slaan.



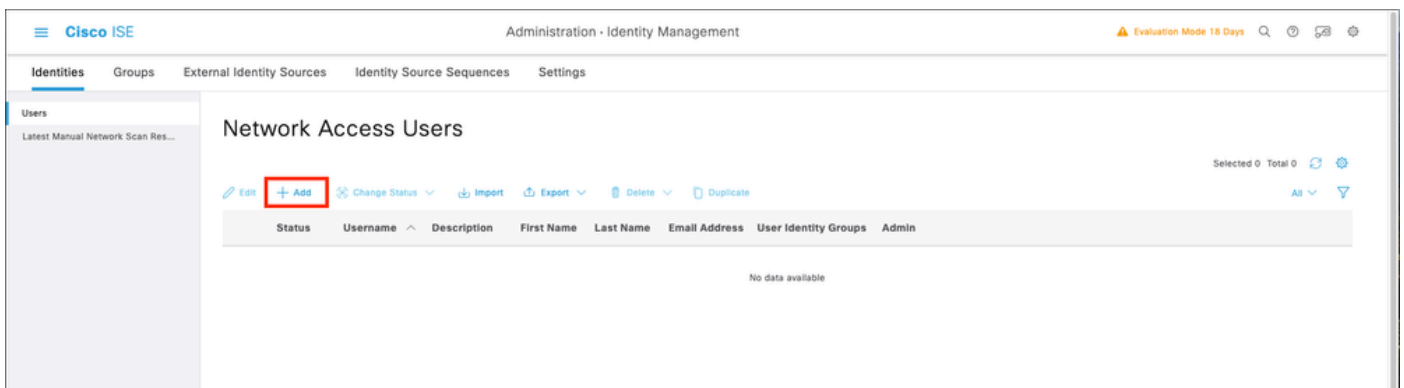
5.1 Herhaal hetzelfde proces voor alleen-lezen gebruikers.



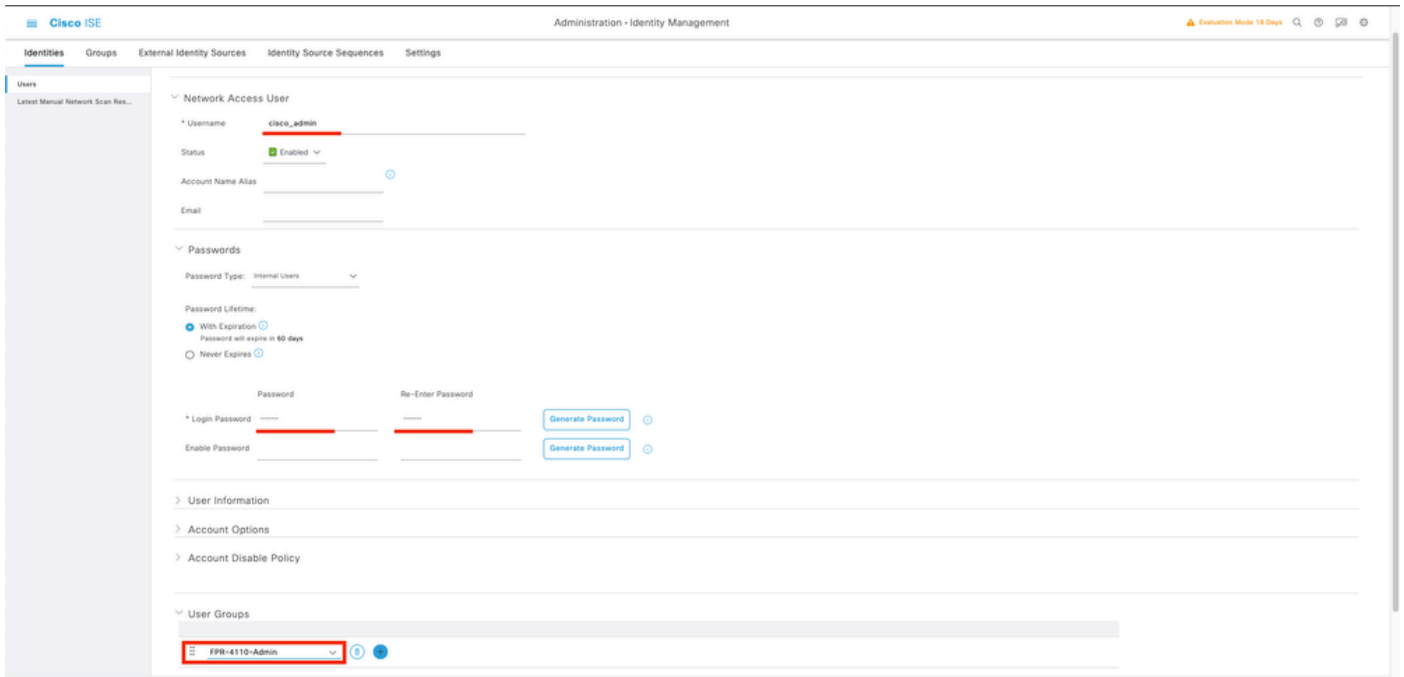
Stap 6. Bevestig de nieuwe gebruikersgroepen onder Gebruikersidentiteitsgroepen.



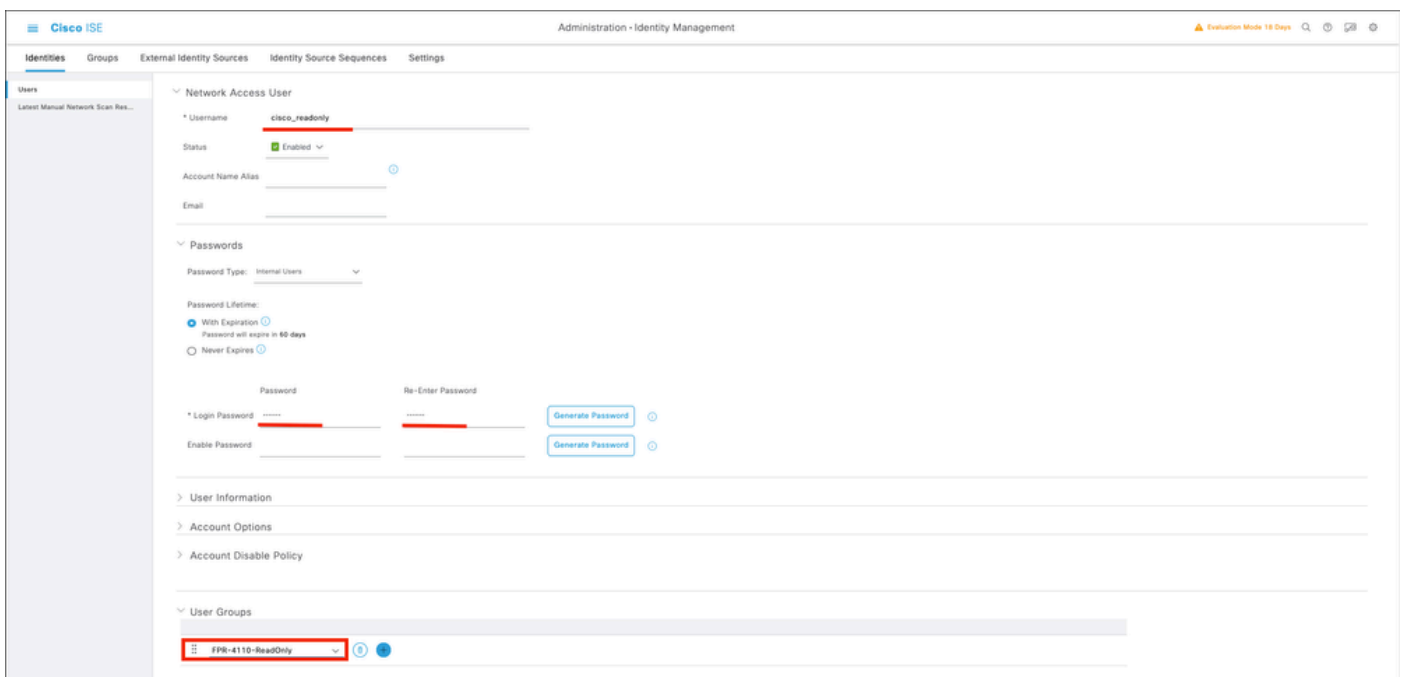
Stap 7. Maak lokale gebruikers en voeg ze toe aan hun correspondentengroep. Ga naar het hamburgerpictogram ≡ > Administratie > Identiteitsbeheer > Identiteiten > + Toevoegen.



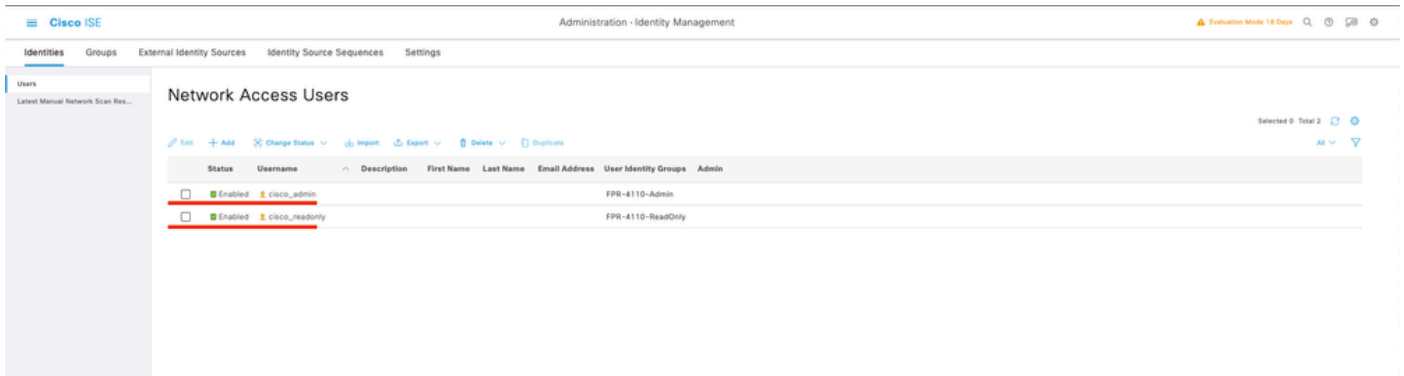
7.1 Voeg de gebruiker met beheerdersrechten toe. Stel een naam, wachtwoord in en wijs het toe aan FPR-4110-Admin, scroll naar beneden en klik op Indienen om de wijzigingen op te slaan.



7.2 Voeg de gebruiker toe met ReadOnly-rechten. Stel een naam, wachtwoord in en wijs het toe aan FPR-4110-ReadOnly, scroll naar beneden en klik op Indienen om de wijzigingen op te slaan.



7.3 Controleer of de gebruikers zich onder Netwerktogangsgebruikers bevinden.



Stap 8. Maak het autorisatieprofiel voor de beheerder.

Het FXOS-chassis bevat de volgende gebruikersrollen:

- Beheerder - Volledige lees-en-schrijftoegang tot het gehele systeem. De standaard admin account is standaard toegewezen aan deze rol en kan niet worden gewijzigd.
- Alleen-lezen - alleen-lezen toegang tot systeemconfiguratie zonder rechten om de systeemstatus aan te passen.
- Verrichtingen - Lees-en-schrijftoegang tot NTP-configuratie, Smart Call Home-configuratie voor slimme licentiëring en systeemlogbestanden, inclusief syslog-servers en -fouten. Lees de toegang tot de rest van het systeem.
- AAA - lees-en-schrijftoegang tot gebruikers, rollen en AAA-configuratie. Lees de toegang tot de rest van het systeem

Kenmerken voor elke rol:

cisco-av-pair=shell:rollen="admin"

Cisco-av-pair=shell:rollen="aaa"

Cisco-av-pair=shell:rollen="bewerkingen"

cisco-av-pair=shell:rollen="alleen-lezen"



Opmerking: deze documentatie definieert alleen admin- en alleen-lezen-kenmerken.

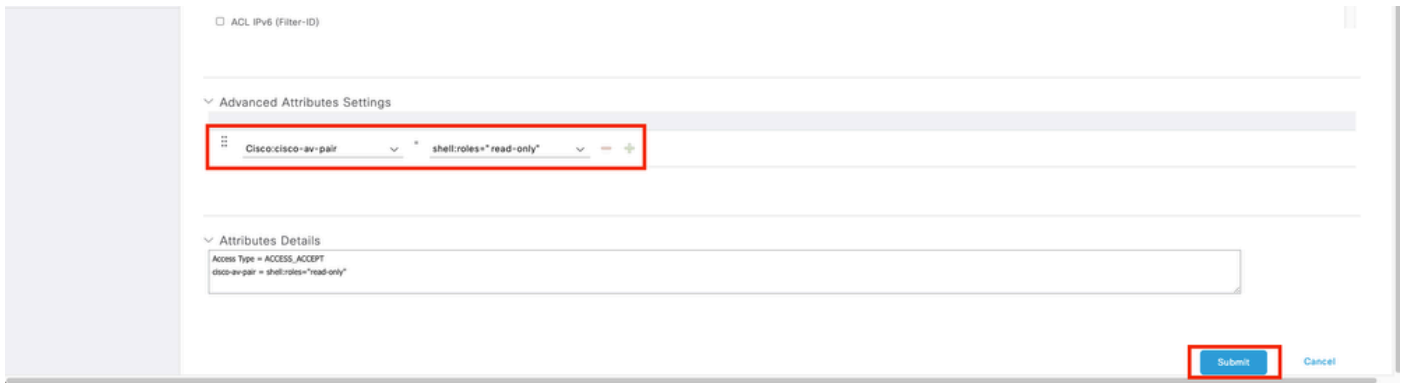
Navigeer naar hamburgerpictogram ≡ > Beleid > Beleidselementen > Resultaten > Vergunning > Vergunningsprofielen > +Add.

Definieer een naam voor het autorisatieprofiel, laat het toegangstype als ACCESS_ACCEPTEREN en voeg cisco-av-pair=shell toe onder de instellingen voor geavanceerde kenmerken:rollen="admin" met en klik op Submit.

The screenshot shows the Cisco ISE interface for configuring an Authorization Profile. The breadcrumb navigation is "Authorization Profiles > FPR-4110-Admins". The profile name is "FPR-4110-Admins" and the access type is "ACCESS_ACCEPT". Under "Advanced Attributes Settings", a rule is defined as "Cisco:cisco-av-pair" with the value "shell:roles=*admin*". The "Attributes Details" section shows the resulting configuration: "Access Type = ACCESS_ACCEPT" and "cisco-av-pair = shell:roles=*admin*". A "Submit" button is visible at the bottom right.

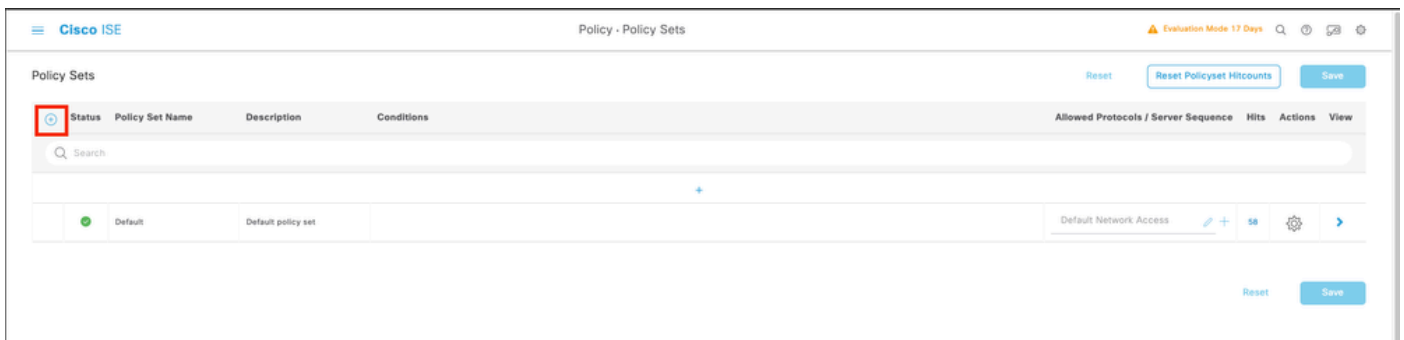
8.1 Herhaal de vorige stap om het autorisatieprofiel voor de alleen-lezen gebruiker te maken. Maak dit keer de Radius Class met de waarde read-only in plaats daarvan Administrator.

The screenshot shows the Cisco ISE interface for configuring a new Authorization Profile. The breadcrumb navigation is "Authorization Profiles > New Authorization Profile". The profile name is "FPR-4110-ReadOnly" and the access type is "ACCESS_ACCEPT". The "Attributes Details" section is empty, indicating that no attributes have been configured for this profile.

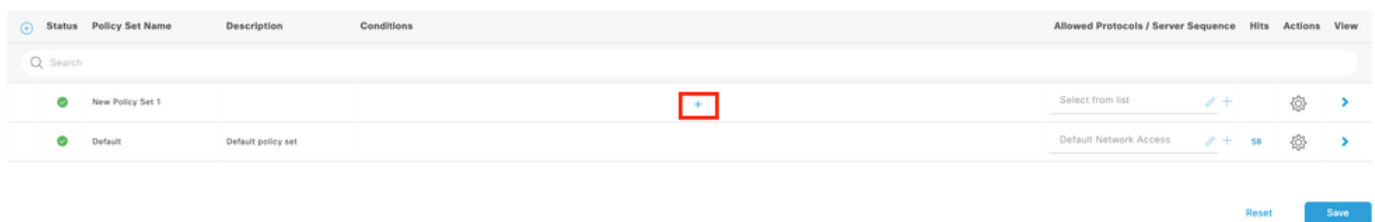


Stap 9. Maak een Policy Set die overeenkomt met het FMC IP-adres. Dit om te voorkomen dat andere apparaten toegang verlenen aan de gebruikers.

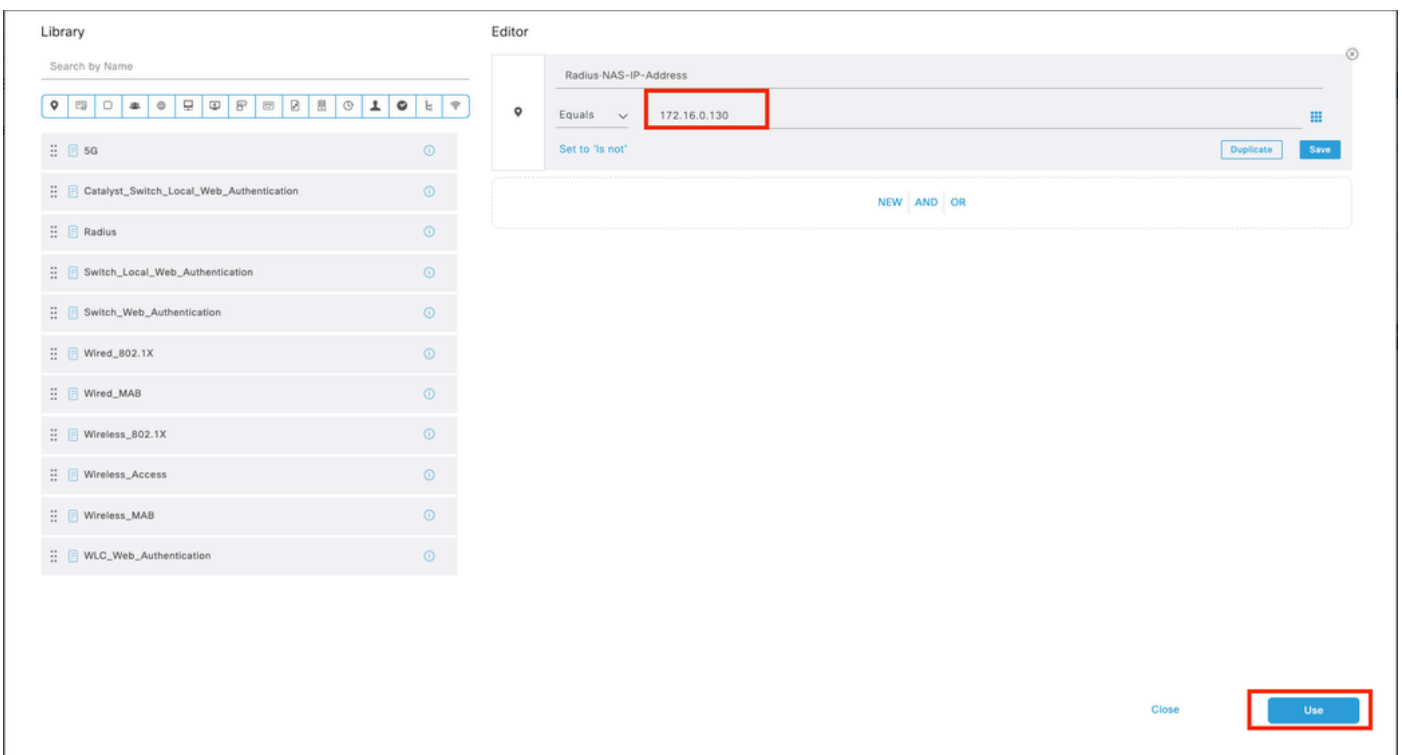
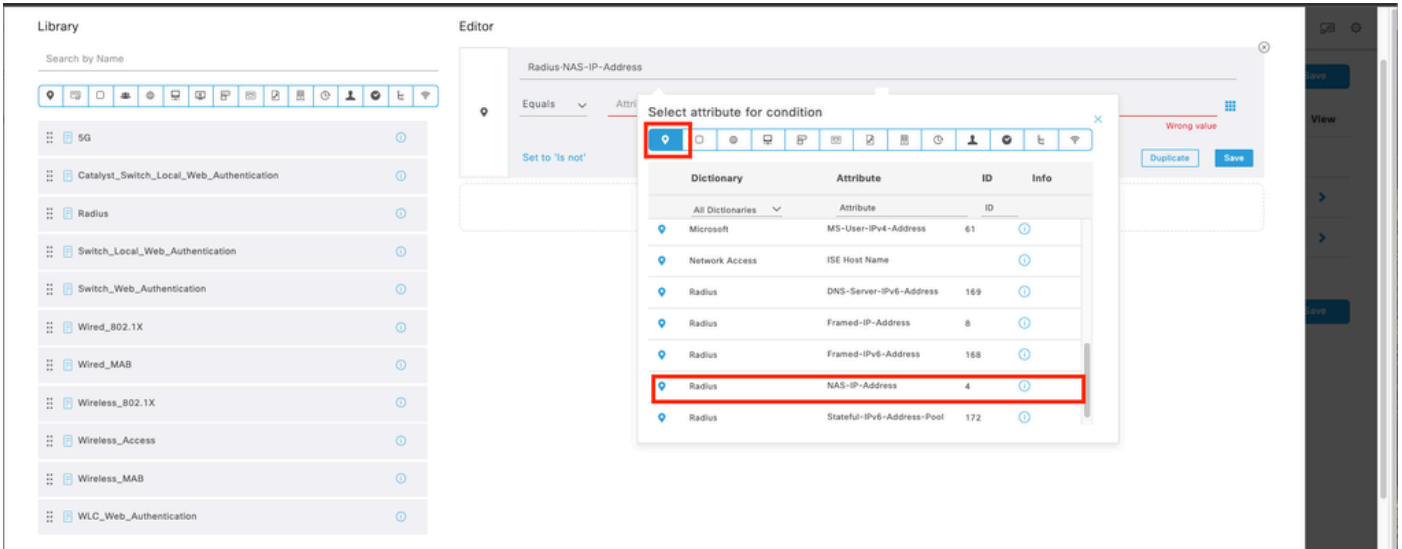
Navigeer naar ≡ > Beleidssets > Pictogramteken toevoegen linksboven.



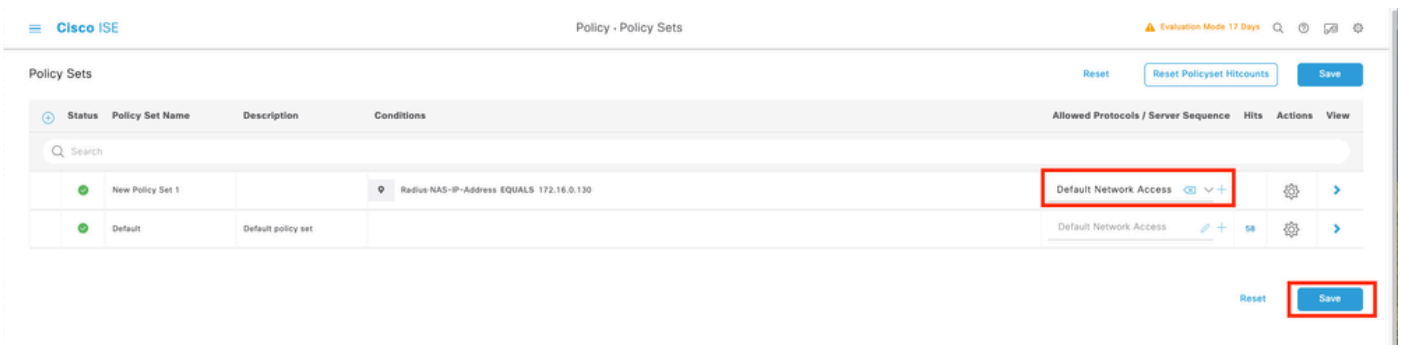
9.1 Bovenaan uw Policy Sets staat een nieuwe regel. Klik op het pictogram Add om een nieuwe voorwaarde te configureren.

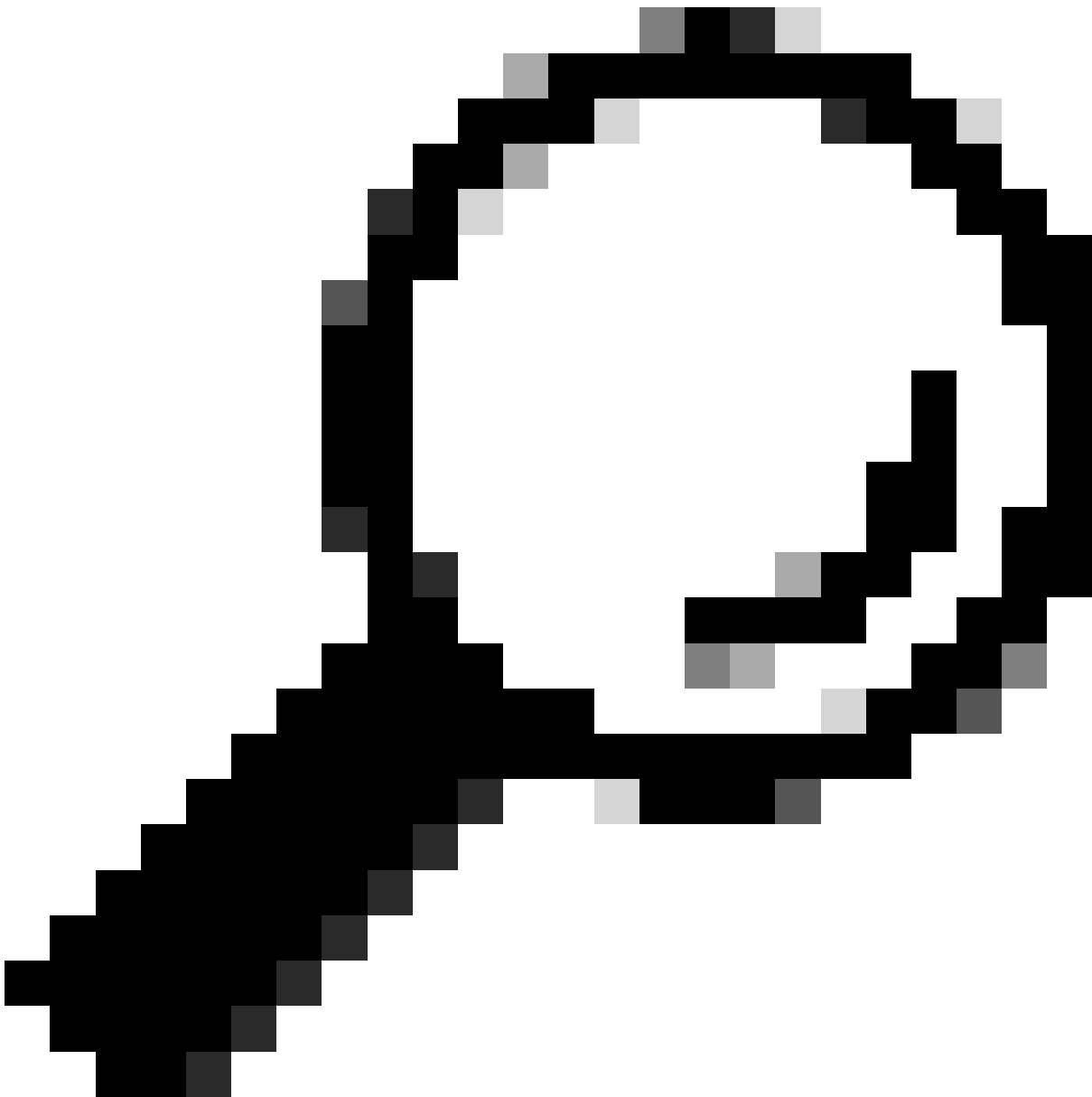


9.2 Voeg een topvoorwaarde toe voor RADIUS NAS-IP-Adressate overeenkomend met het FCM IP-adres, en klik vervolgens op Gebruik.



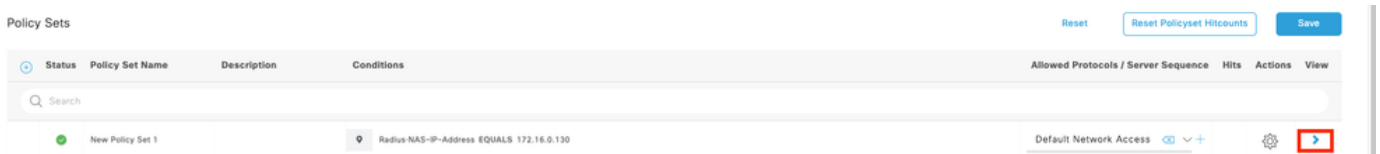
9.3 Klik op Opslaan als u klaar bent.



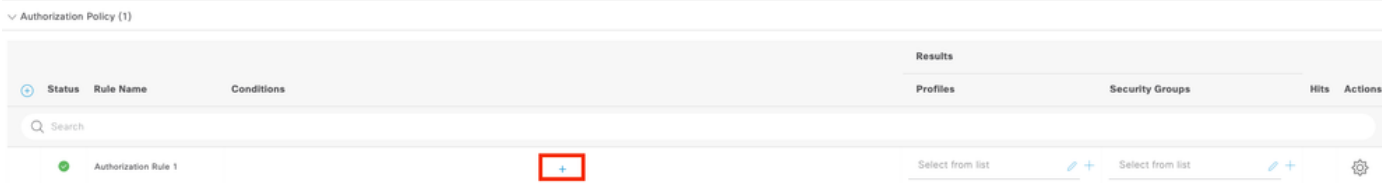


Tip: voor deze oefening hebben we de lijst Default Network Access Protocols toegestaan. U kunt een nieuwe lijst maken en deze indien nodig beperken.

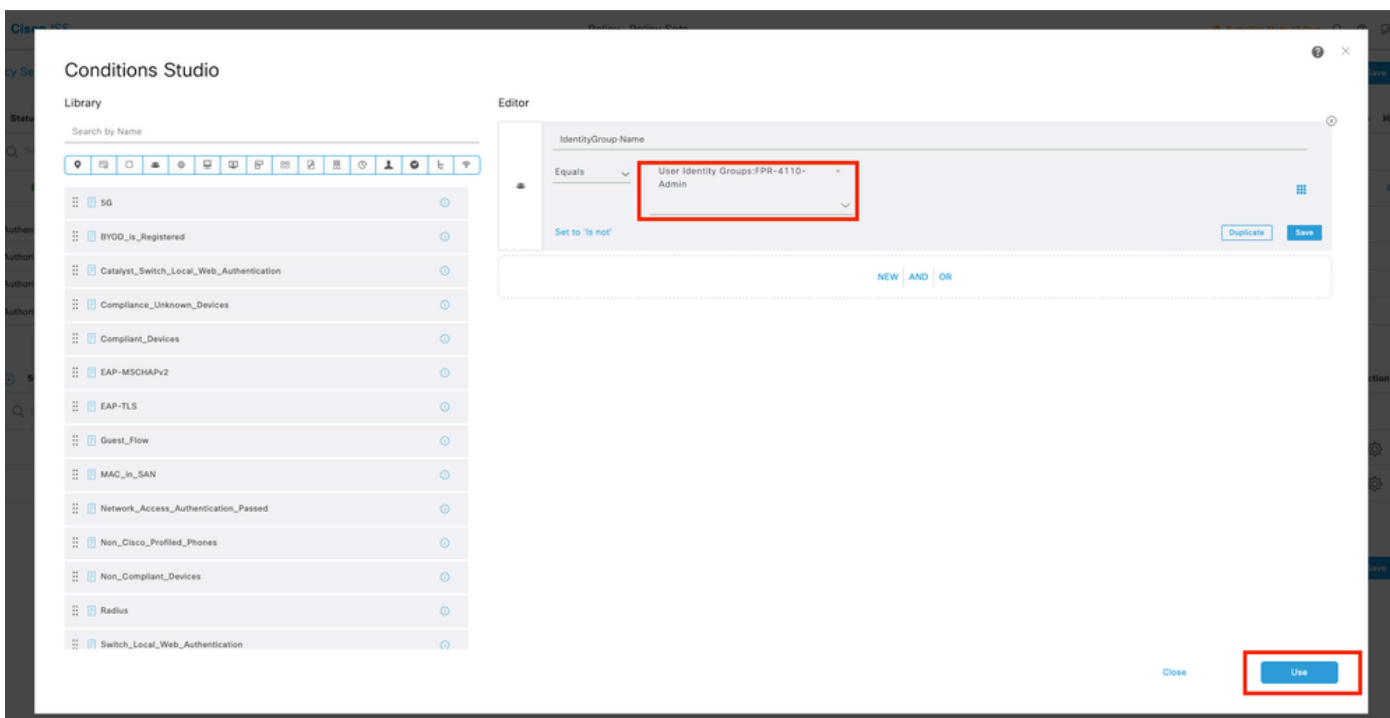
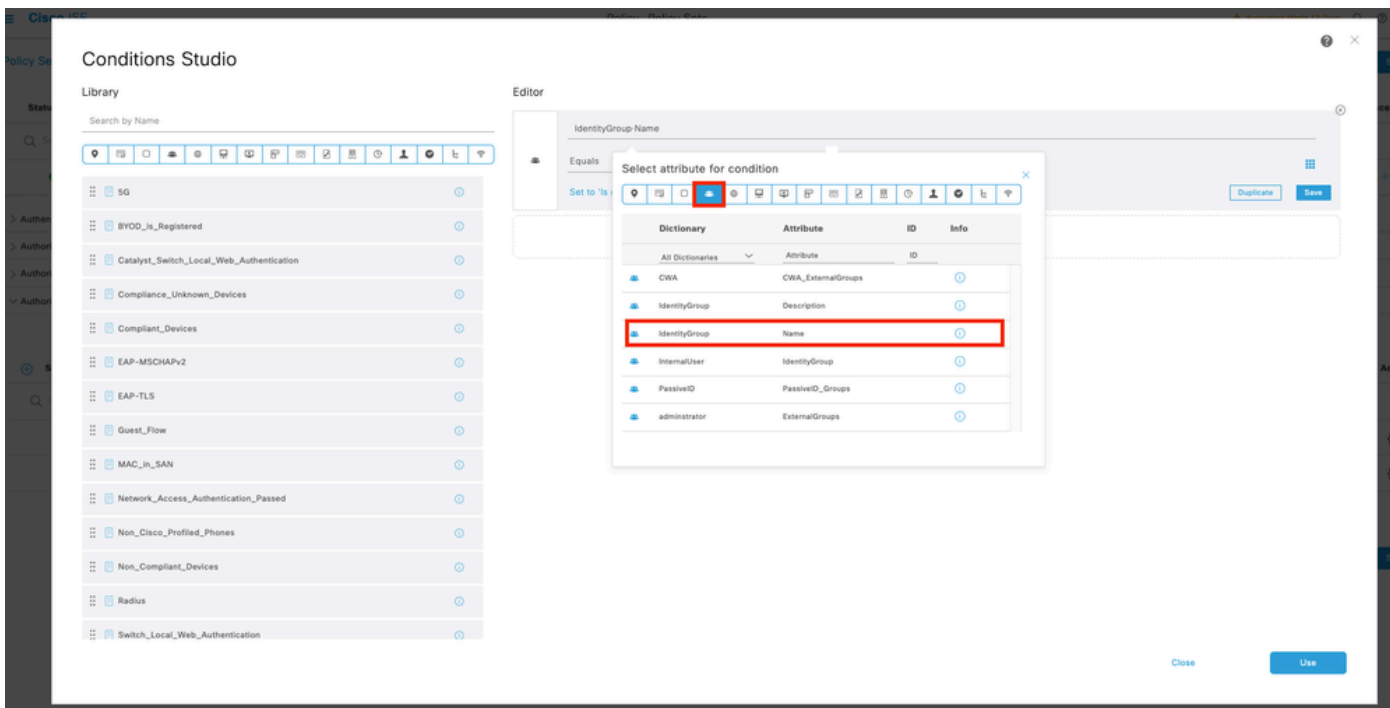
Stap 10. Bekijk de nieuwe Policy Set door op het >pictogram aan het einde van de rij te drukken.



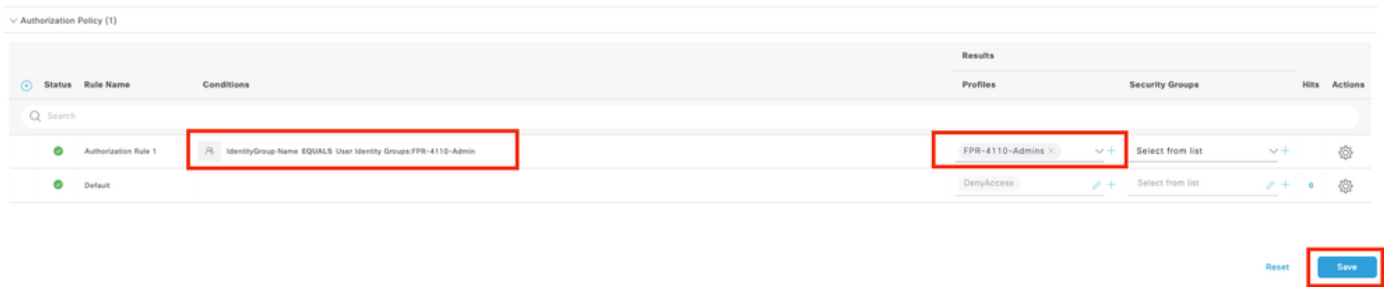
10.1 Breid het menu Autorisatiebeleid uit en klik in (+) om een nieuwe voorwaarde toe te voegen.



10.2 Stel de voorwaarden in om de DictionaryIdentity Group af te stemmen op AttributeName Equals User Identity Groups: FPR-4110-Admins (de groepsnaam die in Stap 7 is gemaakt) en klik op Use.



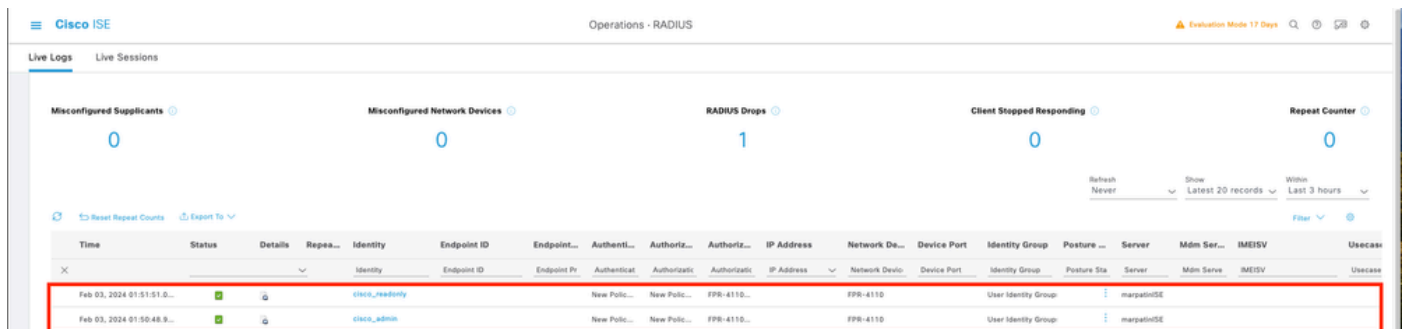
Stap 10.3 Controleer of de nieuwe voorwaarde is ingesteld in het autorisatiebeleid en voeg vervolgens een gebruikersprofiel toe onder Profielen.



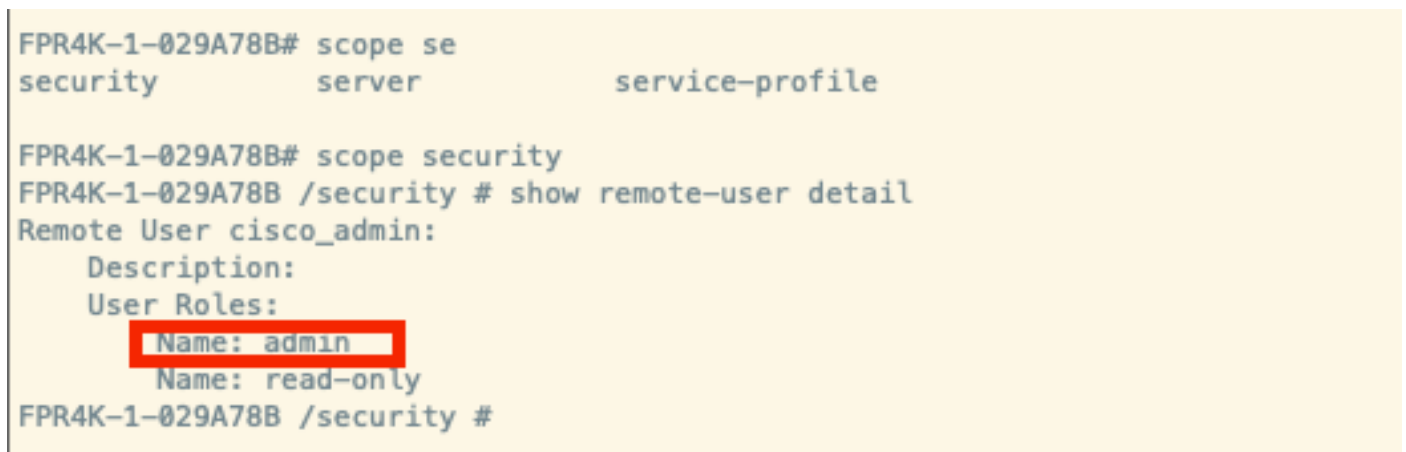
Stap 11. Herhaal hetzelfde proces in stap 9 voor alleen-lezen gebruikers en klik op Opslaan.

Verifiëren

1. Probeer met de nieuwe RADIUS-referenties in de FCM GUI in te loggen
2. Navigeer naar hamburgerpictogram ≡ > Bewerkingen > Straal > Live logs.
3. De weergegeven informatie toont of een gebruiker met succes is aangemeld.



4. Validatie van de rol van geregistreerde gebruikers van Secure Firewall Chassis CLI.



Problemen oplossen

1. Navigeer via ISE GUI naar het hamburgerpictogram ≡ > Operations > Radius > Live logs.

1.1 Valideren als het verzoek van de logsessie naar het ISE-knooppunt komt.

1.2 Voor een mislukte statusbeoordeling moeten de gegevens van de sessie worden bekeken.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authent...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server	Mdm Se
Feb 02, 2024 07:32:18.8...	✘	🔒		cisco_admin			Default >>...	Default			FPR-4110		User Identity Group:		marpat@ISE	
Feb 02, 2024 07:23:20.1...	✔	🔒		cisco_readonly			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group:		marpat@ISE	
Feb 02, 2024 07:15:32.2...	✔	🔒		cisco_admin			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group:		marpat@ISE	

2. Als verzoeken niet worden weergegeven in Radius Live-logs , controleert u of het UDP-verzoek de ISE-knooppunt bereikt via een pakketopname.

Navigeer naar hamburgerpictogram ≡ > Bewerkingen > Problemen oplossen > Diagnostische tools > TCP-dump. Voeg een nieuwe opname toe en download het bestand naar uw lokale machine om te bekijken of de UDP-pakketten aankomen op de ISE-knooppunt.

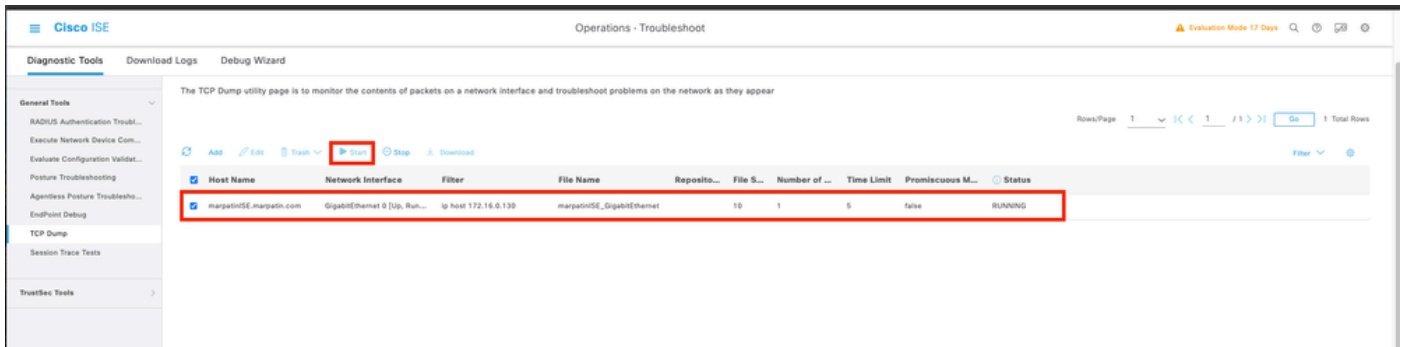
2.1 Vul de gevraagde informatie in, blader naar beneden en klik op Opslaan.

Host Name*
marpat@ISE

Network Interface*
GigabitEthernet 0 [Up, Running]

Filter
ip host 172.16.0.130
E.g. ip host 10.97.122.123 and net 10.172.122.119

2.2 Selecteer en start de opname.



2.3 Probeer u aan te melden bij het Secure Firewall-chassis terwijl de ISE-opname actief is

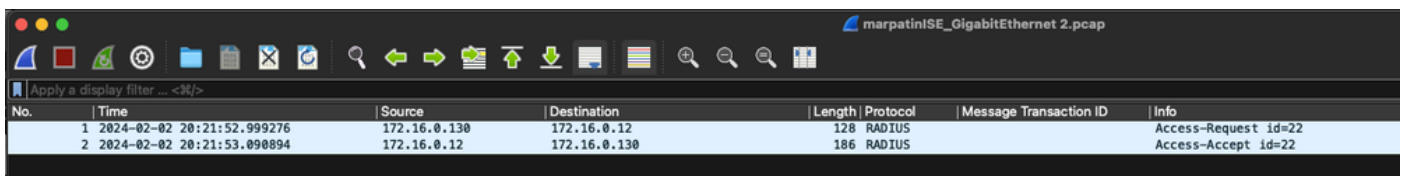
2.4 Stop de TCP Dump in ISE en download het bestand naar een lokale machine.

2.5 Bekijk de verkeersoutput.

Verwachte output:

Pakket nr. 1 Verzoek van de Secure Firewall aan de ISE-server via Port 1812 (RADIUS)

Pakket nr. 2 Het antwoord van de server van ISE dat het eerste verzoek goedkeurt.



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.