FMC- en FTD externe verificatie configureren met ISE als RADIUS-server

Inhoud

Inleiding

Dit document beschrijft een voorbeeld van externe verificatieconfiguratie voor Secure Firewall Management Center en Firewall Threat Defence.

Voorwaarden

Vereisten

Aanbevolen wordt kennis van deze onderwerpen te hebben:

- Cisco Secure Firewall Management Center - eerste configuratie via GUI en/of shell.
- Verificatie- en autorisatiebeleid configureren op ISE.
- Basiskennis van RADIUS.

Gebruikte componenten

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

- vFMC 7.2.5
- vFTD 7.2.5.
- ISE 3.2

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.

Achtergrondinformatie

Wanneer u externe verificatie inschakelt voor beheer- en beheergebruikers van uw Secure Firewall-systeem, controleert het apparaat de gebruikersreferenties met een Lichtgewicht Directory Access Protocol (LDAP) of RADIUS-server zoals opgegeven in een extern verificatieobject.

Externe verificatieobjecten kunnen worden gebruikt door de FMC- en FTD-apparaten. U kunt hetzelfde object tussen de verschillende apparaten-/apparaattypen delen of afzonderlijke objecten maken.

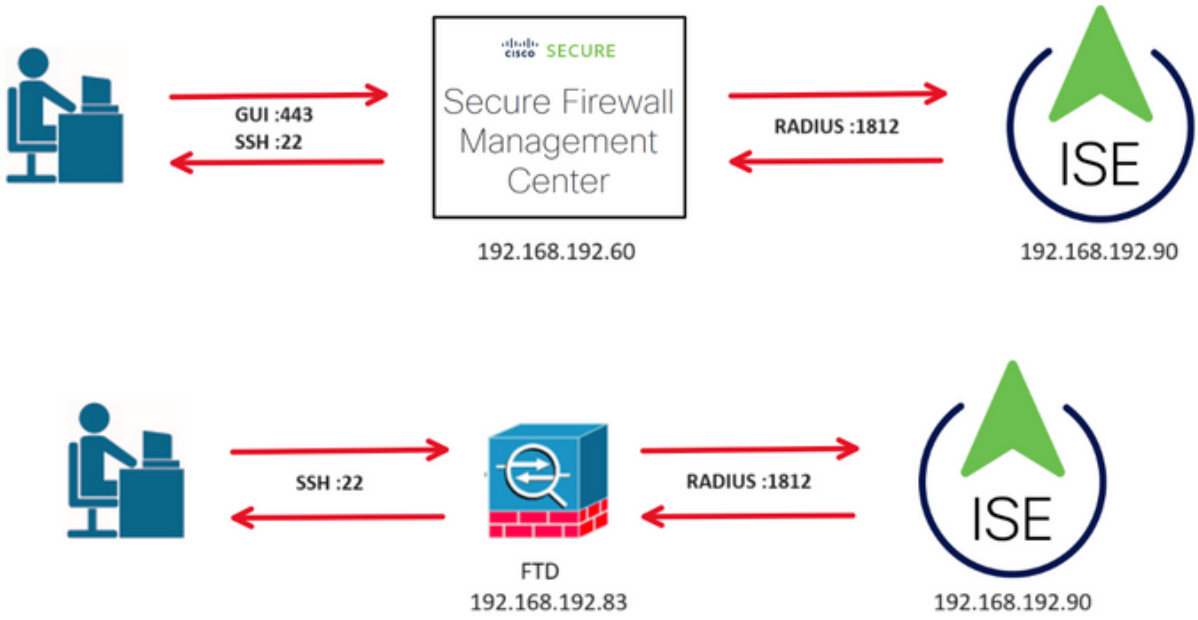
Externe verificatie voor VCC

U kunt meerdere externe verificatieobjecten configureren voor toegang tot de webinterface. Slechts één extern authentificatievoorwerp kan voor CLI of shell toegang worden gebruikt.

Externe verificatie voor FTD

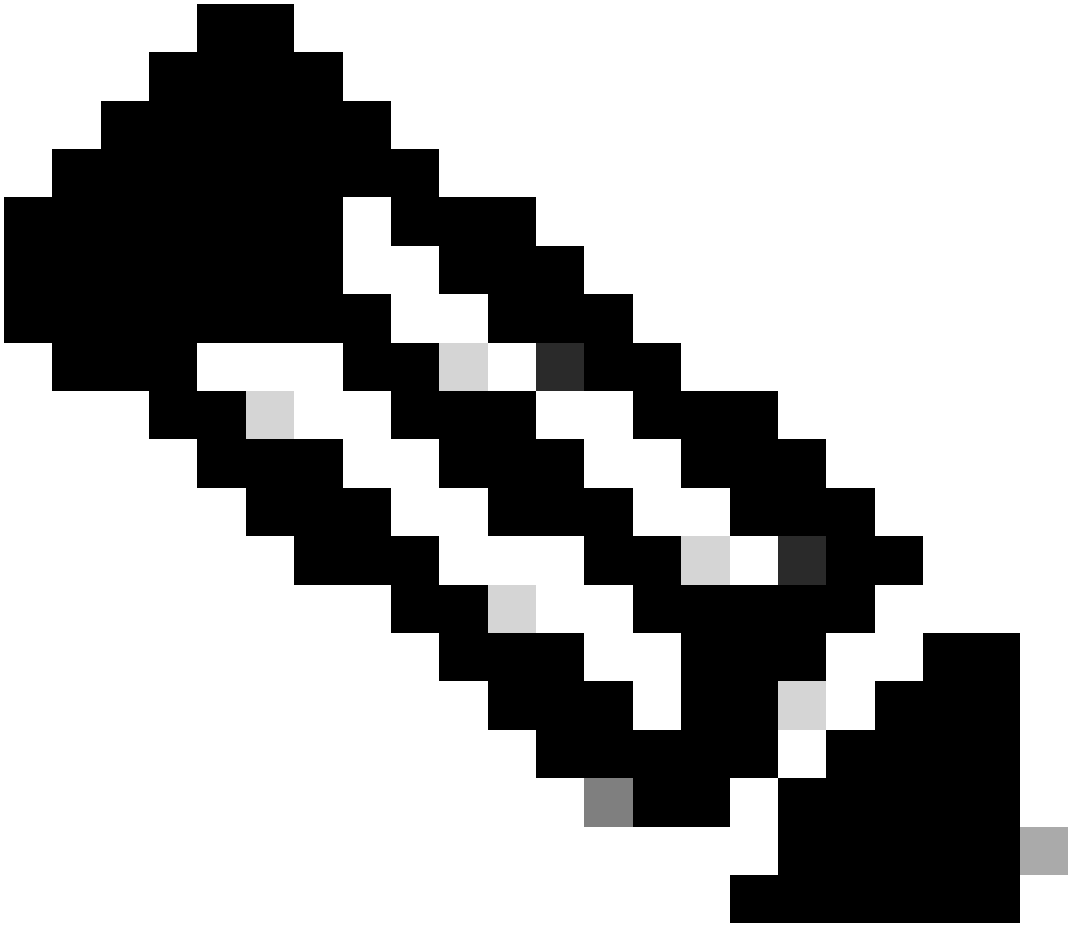
Voor de FTD kunt u slechts één extern verificatieobject activeren.

Netwerktopologie



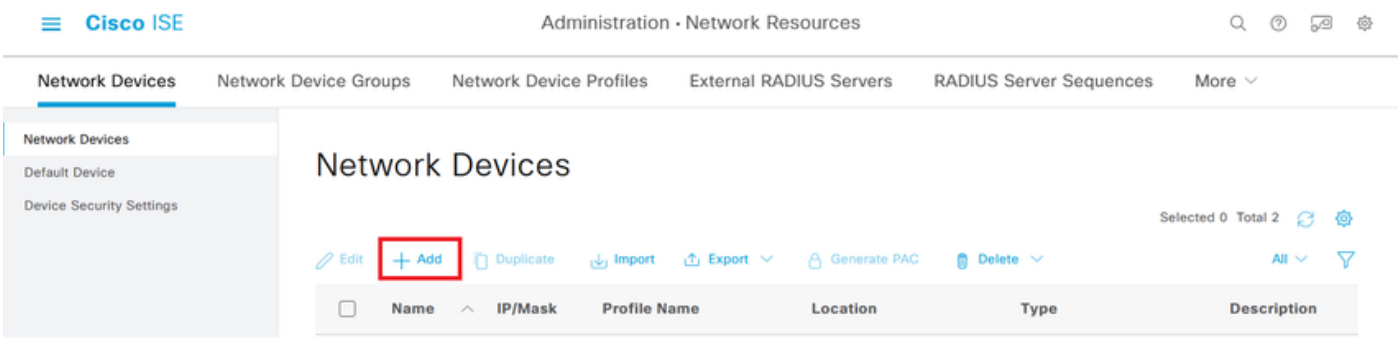
Configureren

ISE-configuratie



Opmerking: er zijn meerdere manieren om ISE-verificatie en -autorisatiebeleid voor Network Access Devices (NAD) zoals FMC in te stellen. Het voorbeeld dat in dit document wordt beschreven, is een referentiepunt waarin we twee profielen maken (een met beheerdersrechten en een ander alleen-lezen) en dat kan worden aangepast aan de basislijnen voor toegang tot uw netwerk. Op ISE kunnen een of meer machtigingsbeleidslijnen worden vastgesteld met terugkerende RADIUS-kenmerkwaarden aan het VCC die vervolgens worden toegewezen aan een lokale gebruikersgroep die in de beleidsconfiguratie van het VCC-systeem is gedefinieerd.

Stap 1. Voeg een nieuw netwerkapparaat toe. Navigeer naar het hamburgerpictogram linksboven >Beheer > Netwerkbronnen > Netwerkapparaten > +Add.

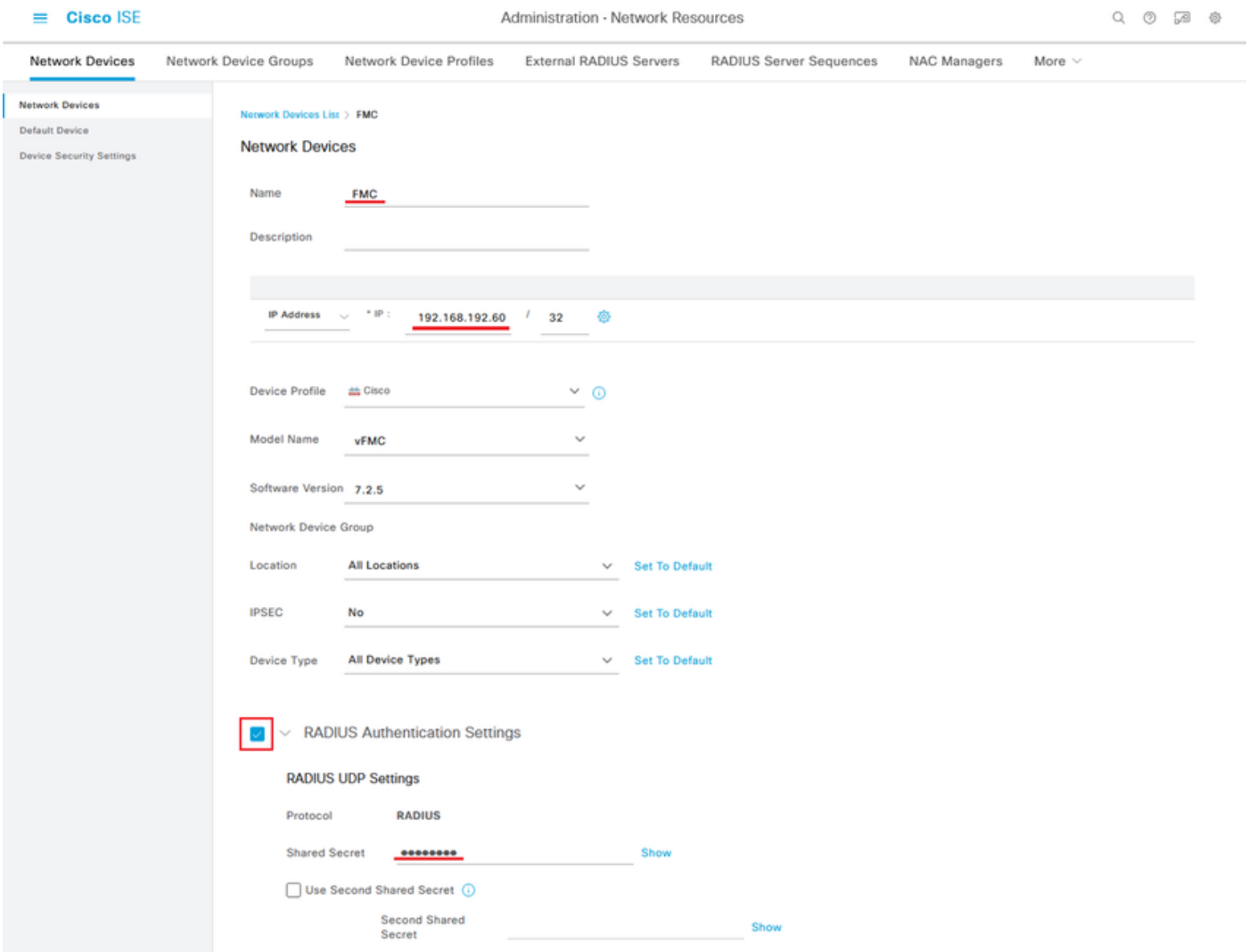


Stap 2. Wijs een naam toe aan het object van het netwerkapparaat en voer het FMC IP-adres in.

Controleer het aanvinkvakje RADIUS en stel een gedeeld geheim in.

Dezelfde toets moet later worden gebruikt om het VCC te configureren.

Klik op Opslaan als u klaar bent.

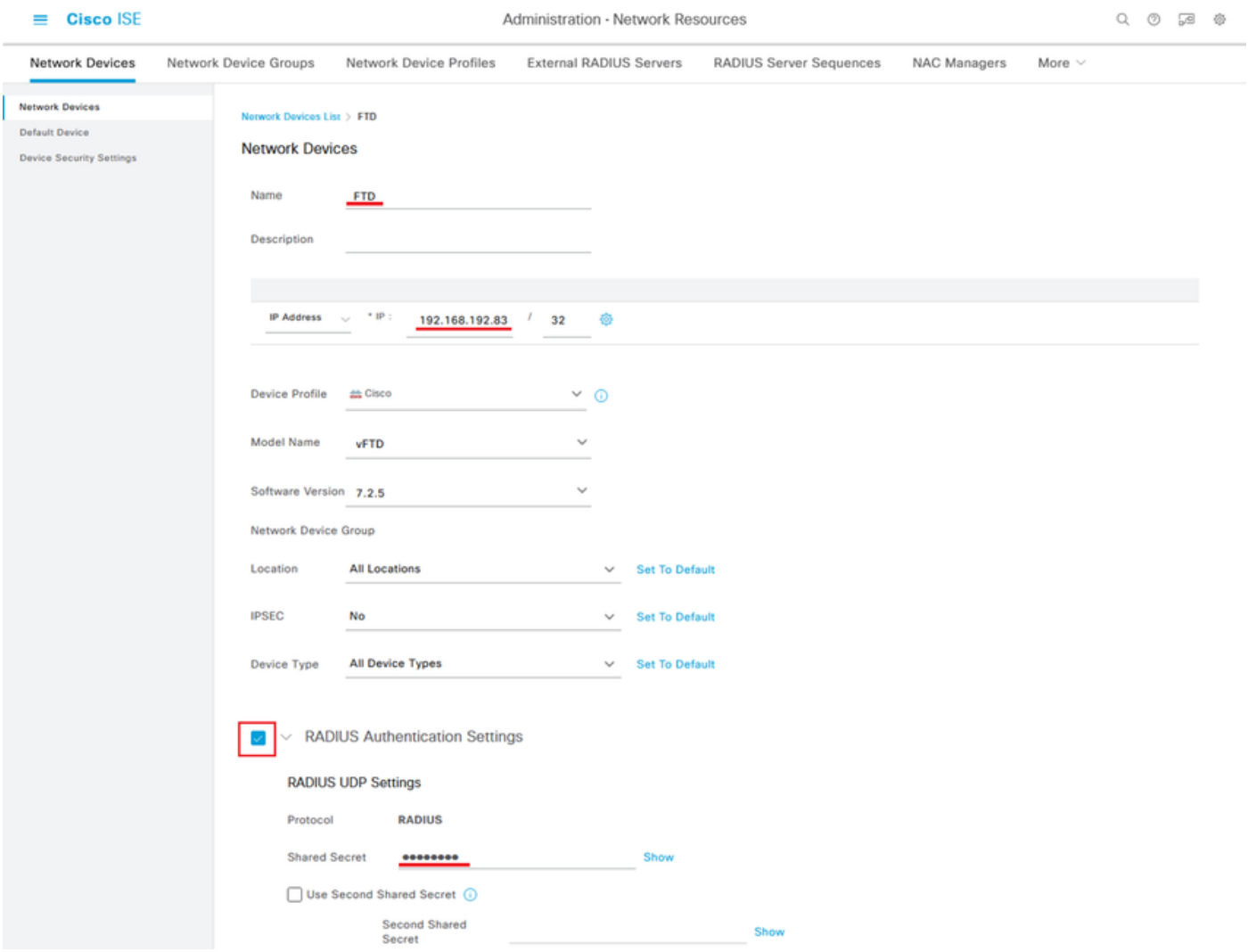


Stap 2.1. Herhaal hetzelfde om de FTD toe te voegen.

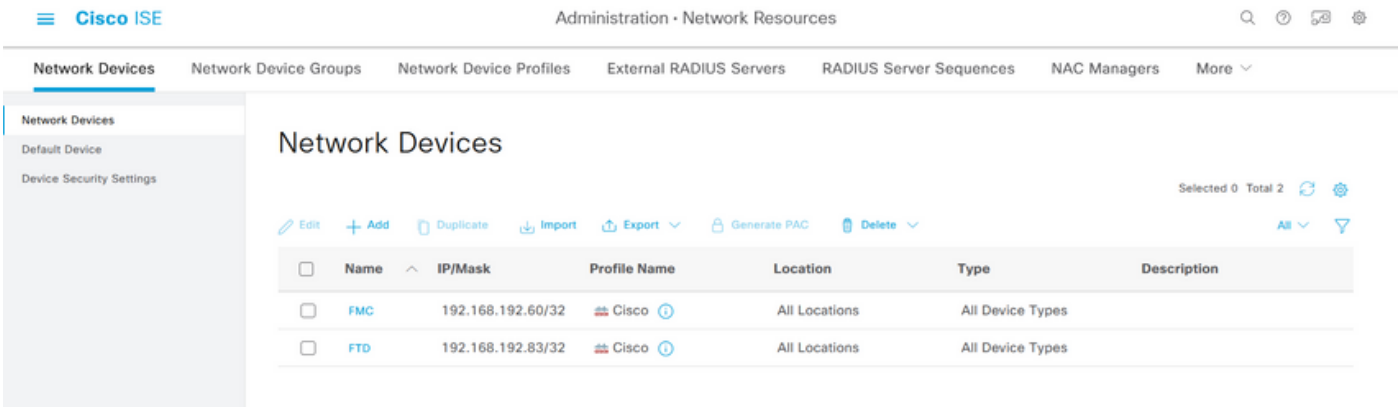
Wijs een naam toe aan het object van het netwerkapparaat en voer het FTD IP-adres in.

Controleer het aanvinkvakje RADIUS en stel een gedeeld geheim in.

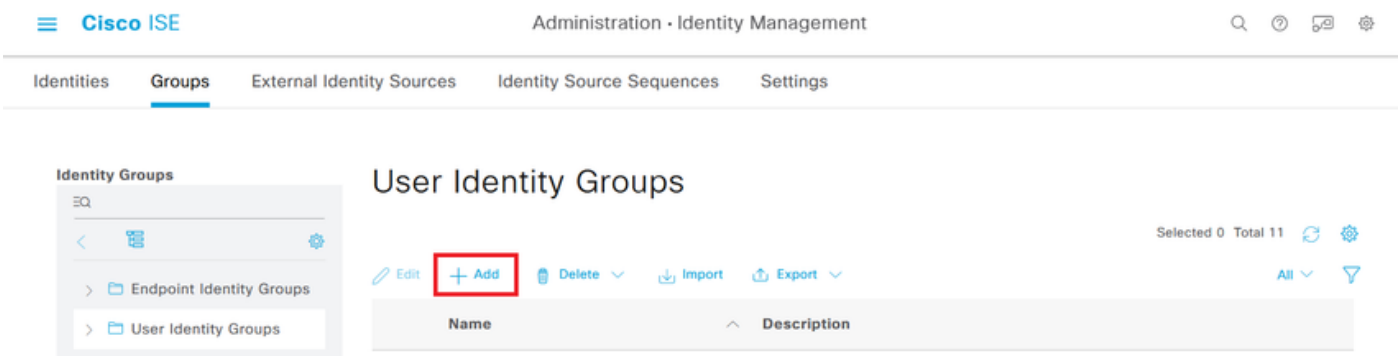
Klik op Opslaan als u klaar bent.



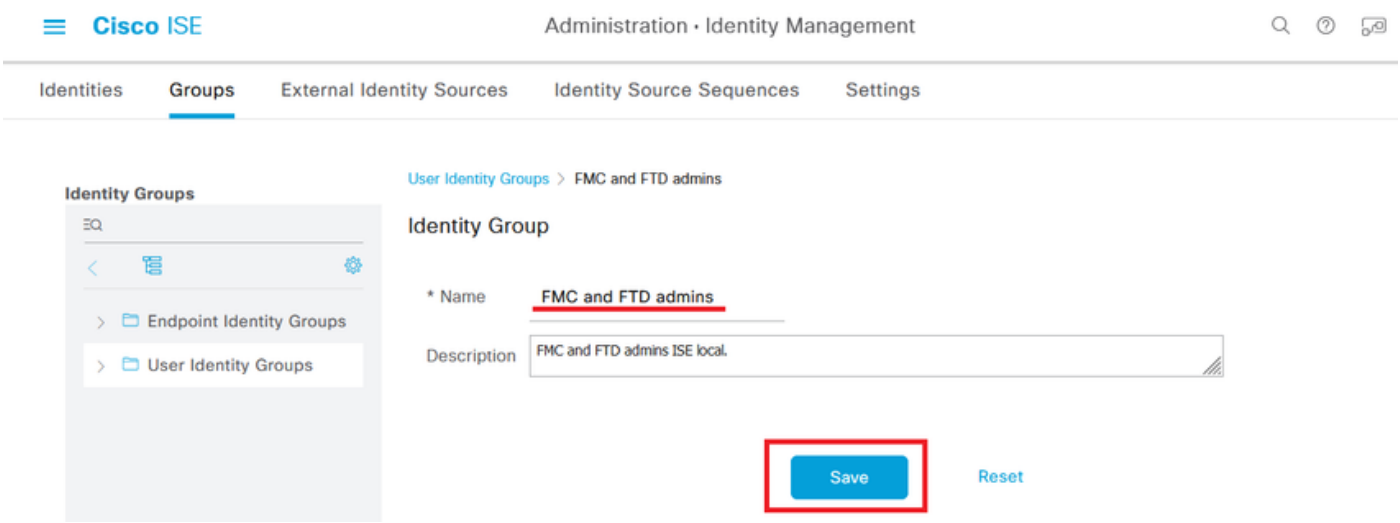
Stap 2.3. Controleer of beide apparaten worden weergegeven onder Netwerkapparaten.



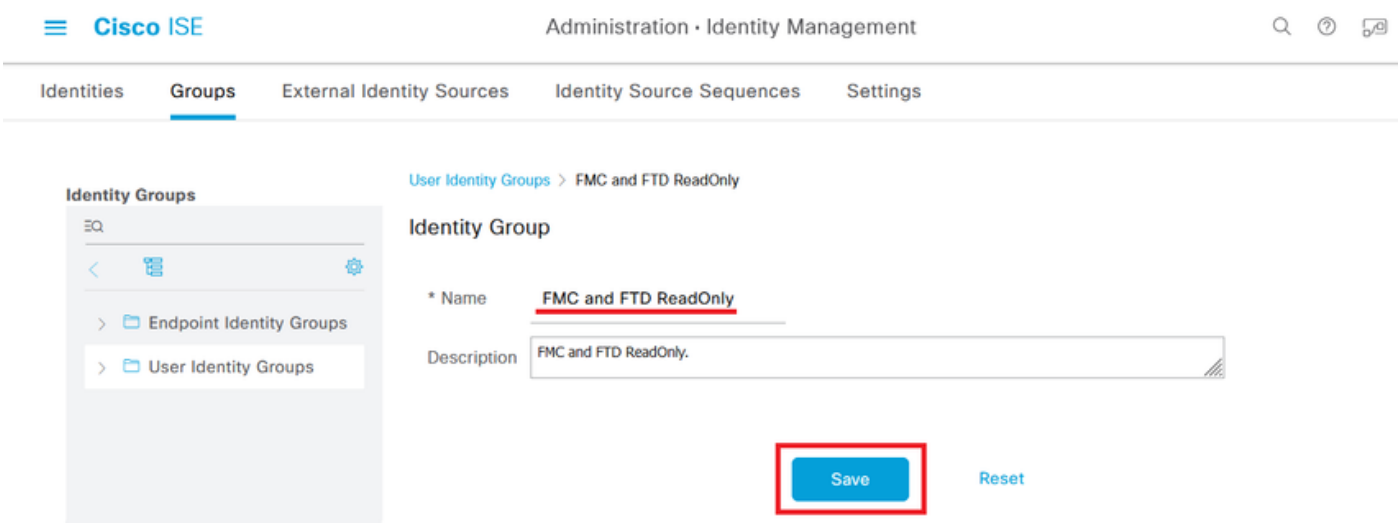
Stap 3. Maak de gewenste gebruikers-identiteitsgroepen. Navigeer naar het hamburgerpictogram ≡ linksboven >Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen > + Toevoegen



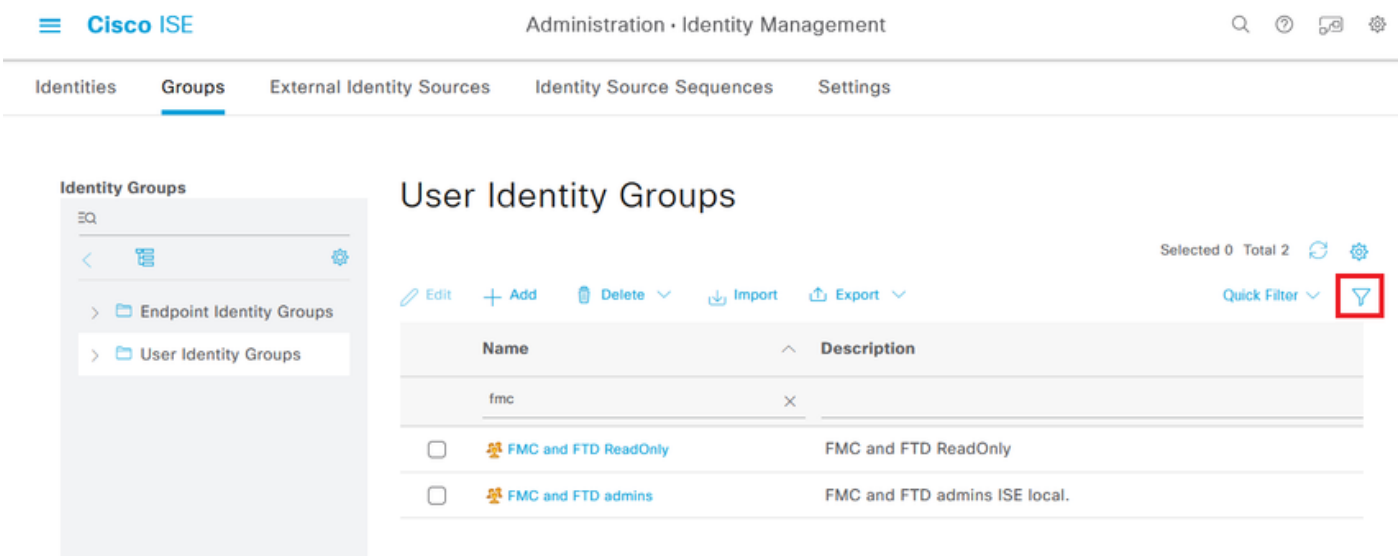
Stap 4. Geef elke groep een naam en sla afzonderlijk op. In dit voorbeeld maken we een groep voor beheerders en een groep voor alleen-lezen gebruikers. Maak eerst de groep voor de gebruiker met beheerdersrechten.



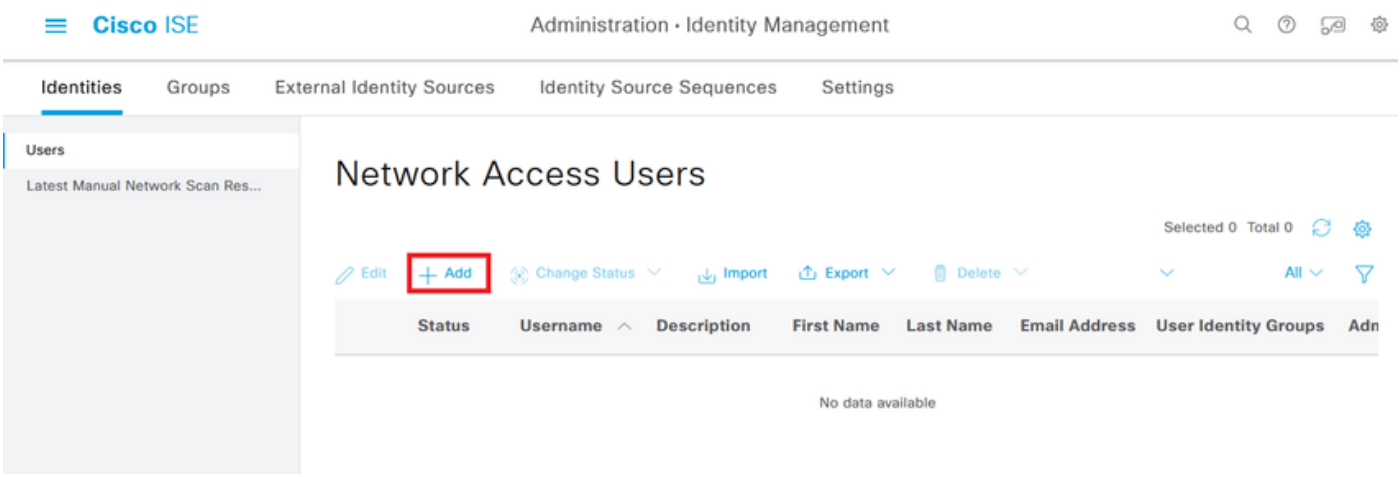
Stap 4.1. Maak de tweede groep voor de ReadOnly gebruiker.



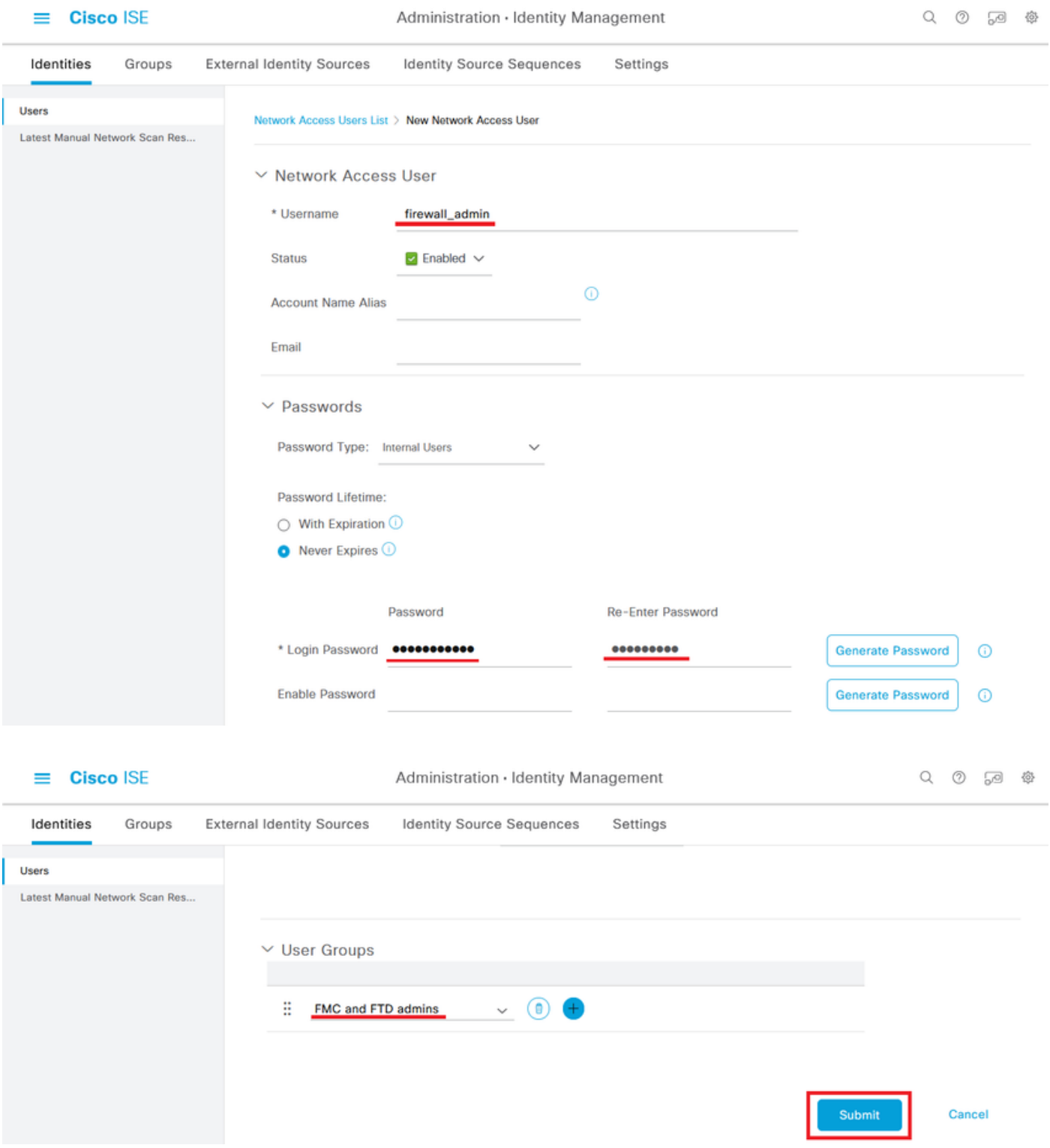
Stap 4.2. Bevestig beide groepen onder de lijst Gebruikersidentiteitsgroepen. Gebruik het filter om deze gemakkelijk te vinden.



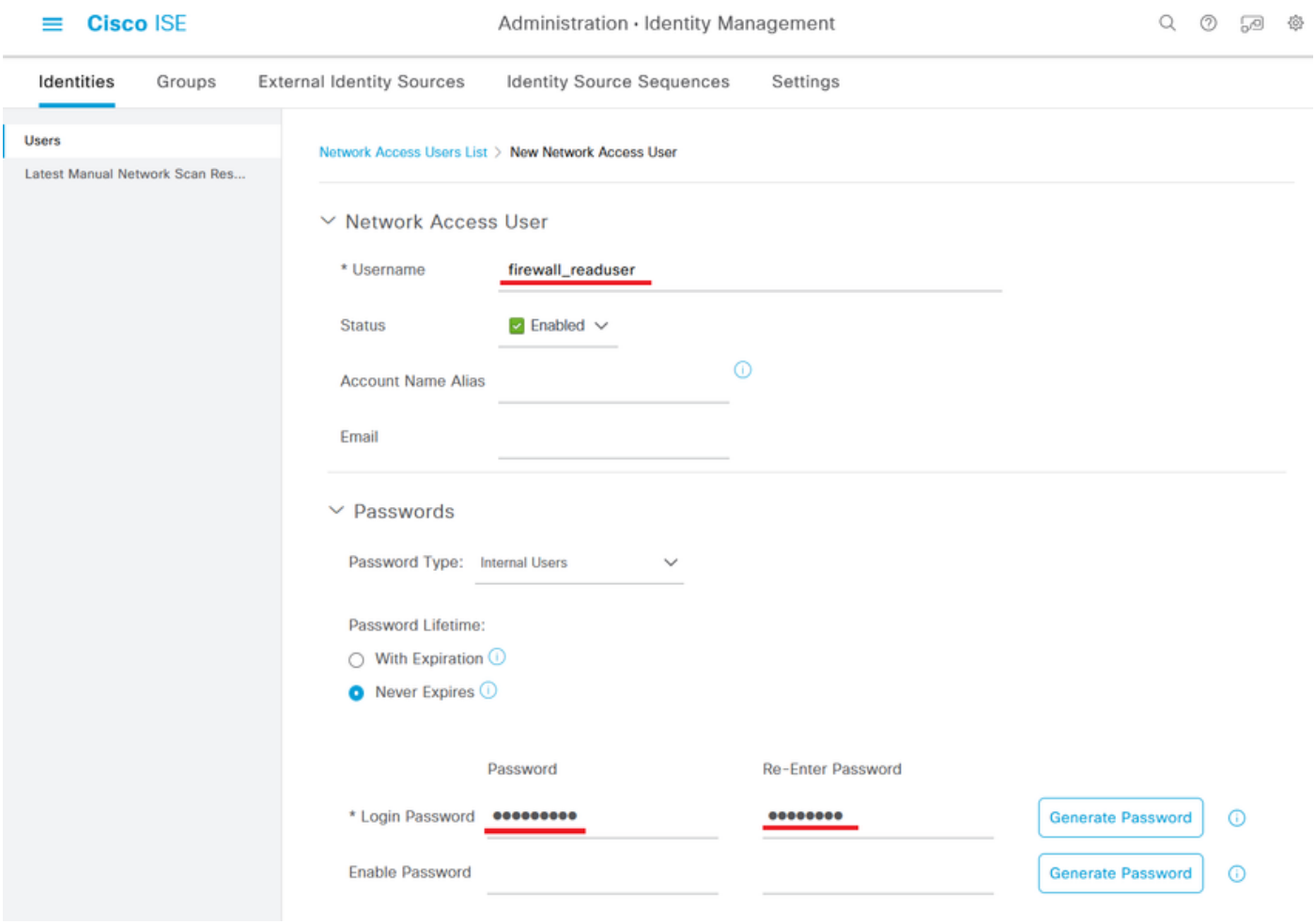
Stap 5. Maak lokale gebruikers en voeg ze toe aan hun correspondentgroep. Ga naar >Beheer > Identiteitsbeheer > Identiteiten > + Toevoegen.

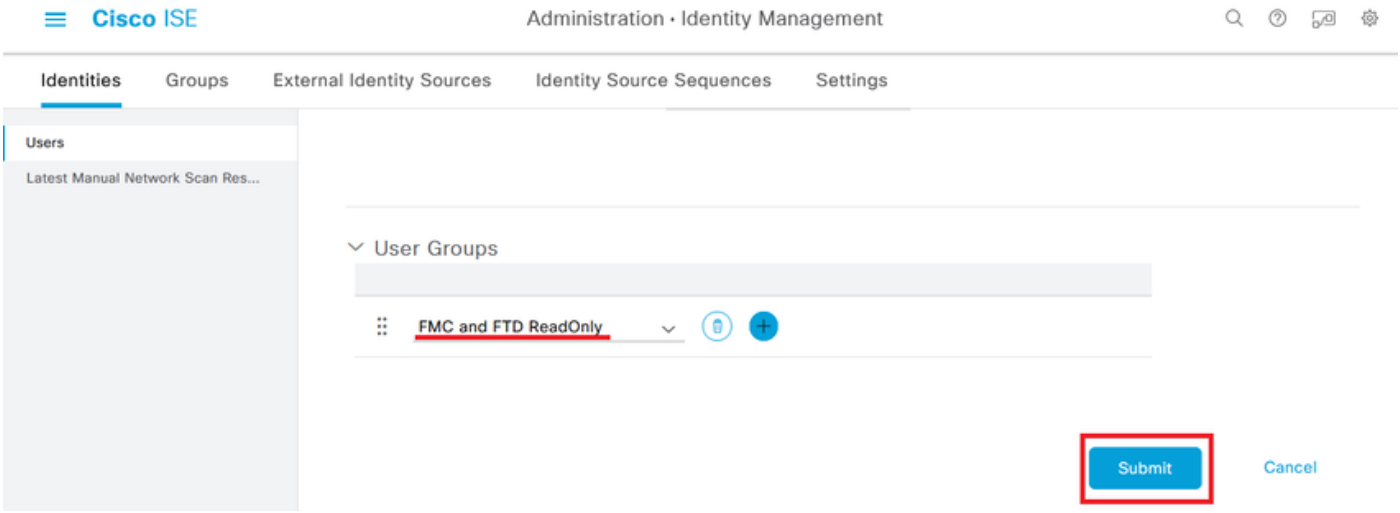


Stap 5.1. Maak eerst de gebruiker met beheerdersrechten. Geef het een naam, wachtwoord en de FMC- en FTD-beheerders van de groep.



Stap 5.2. Voeg de gebruiker met ReadOnly rechten toe. Wijs een naam, wachtwoord en de groep FMC en FTD ReadOnly toe.



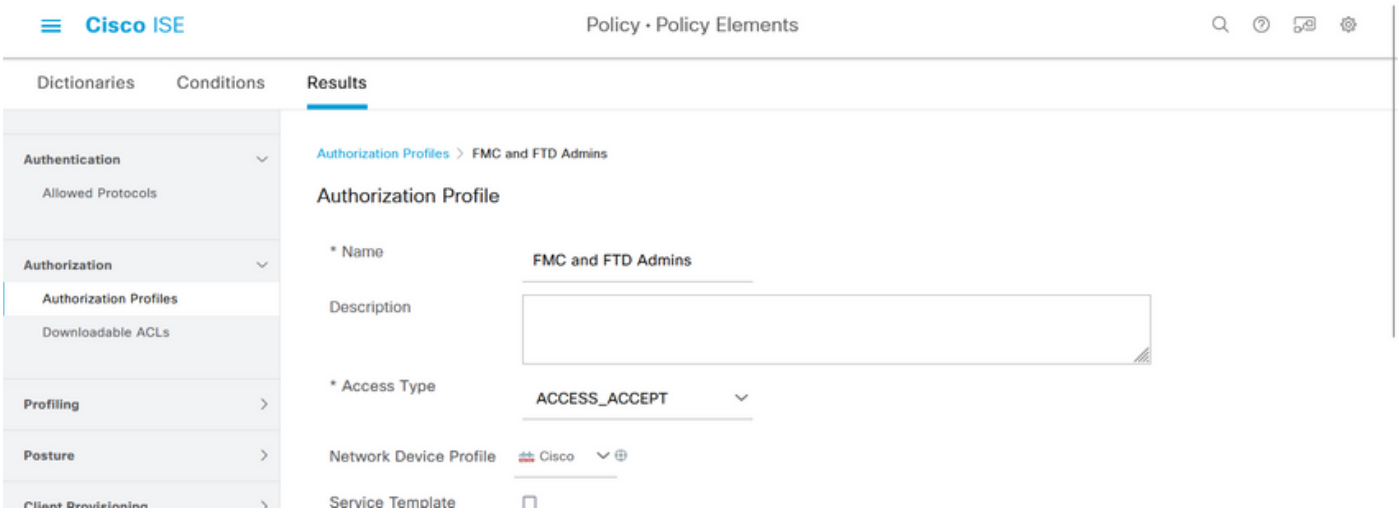


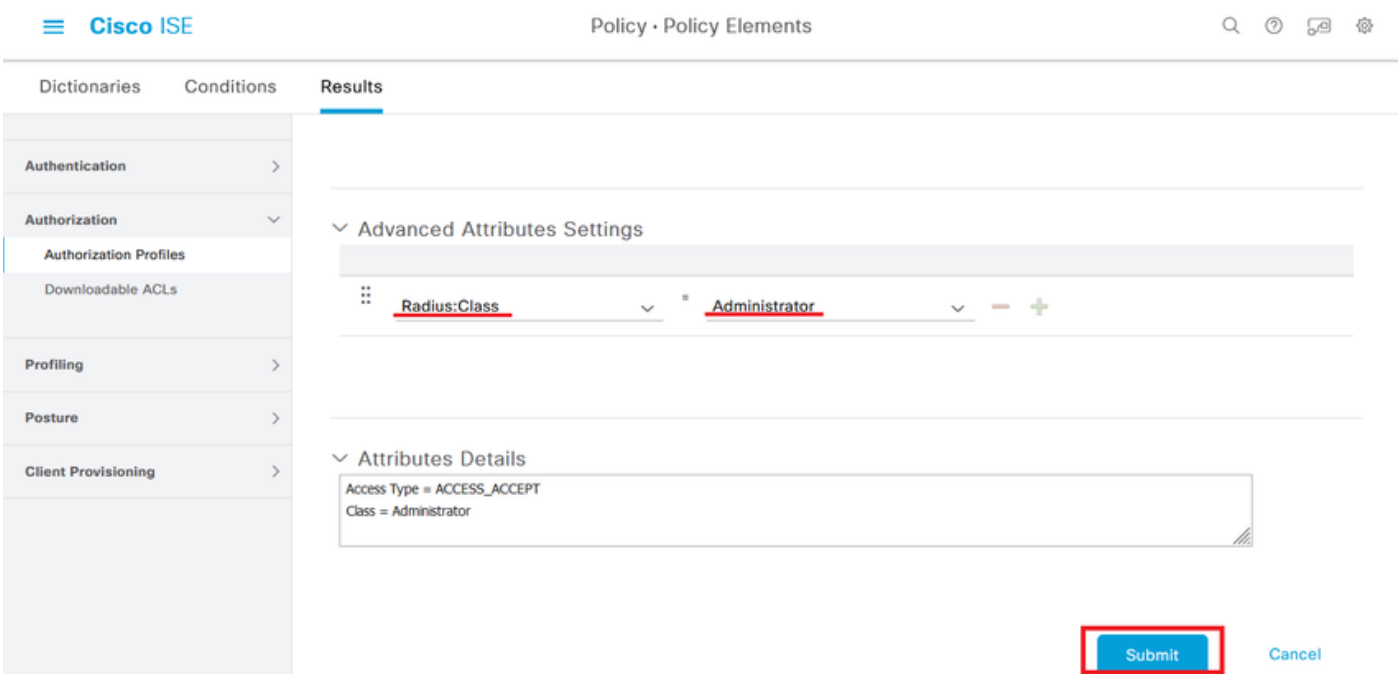
Stap 6. Maak het autorisatieprofiel aan voor de beheerder.

Navigeer naar

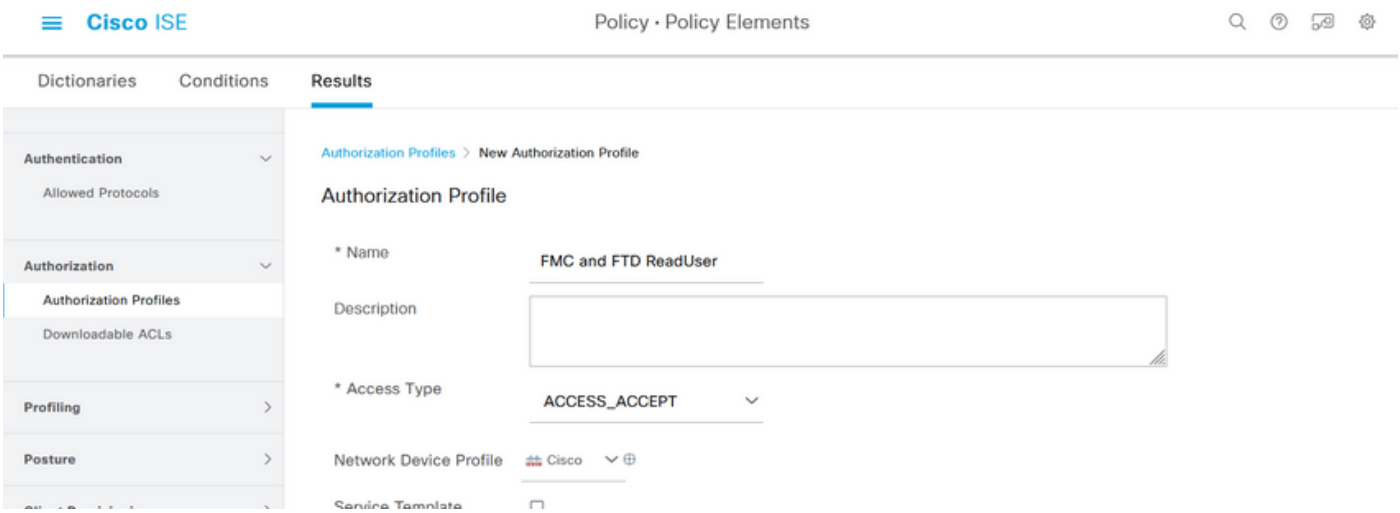
> Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen > +Add.

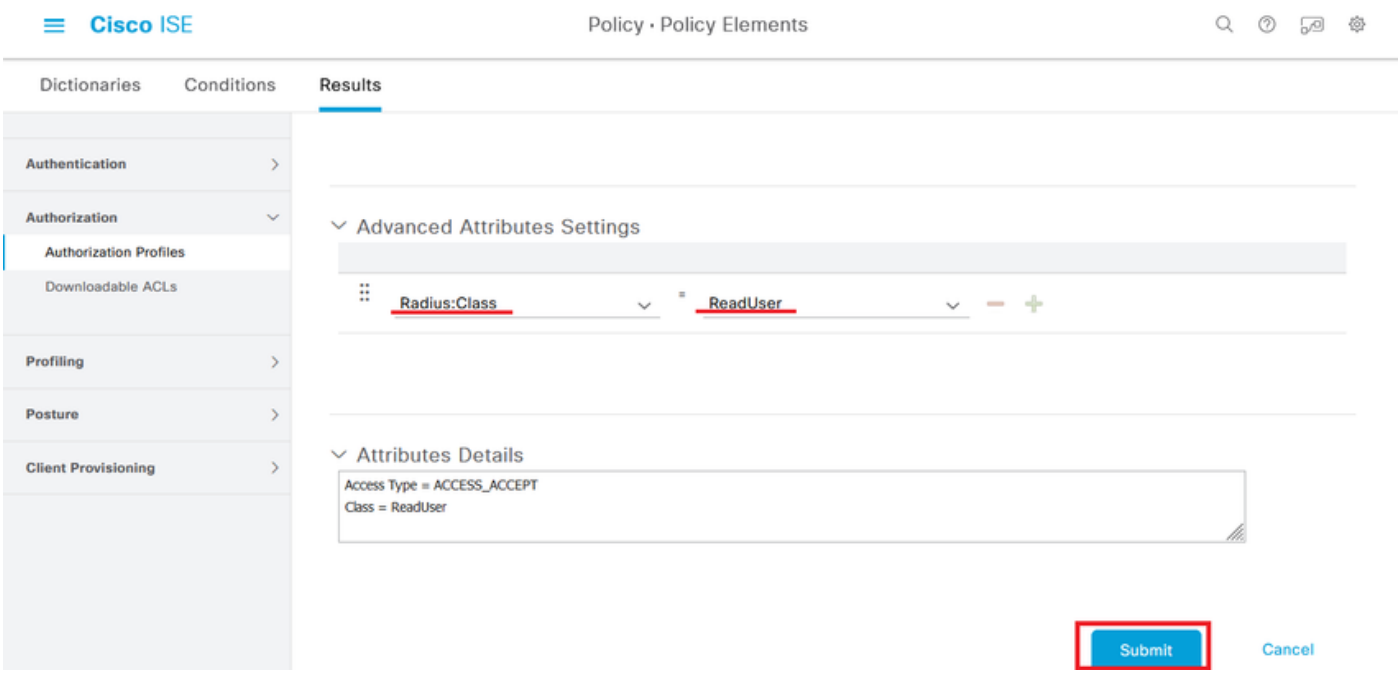
Definieer een naam voor het autorisatieprofiel, laat het toegangstype als ACCESS_ACCEPTEREN en voeg onder Geavanceerde Attributen-instellingen een straal > Klasse toe—[25] met de waarde Administrator en klik op Indienen.





Stap 7. Herhaal de vorige stap om het autorisatieprofiel voor de alleen-lezen gebruiker te maken. Maak nu de Radius Class met de waarde ReadUser in plaats van Administrator.

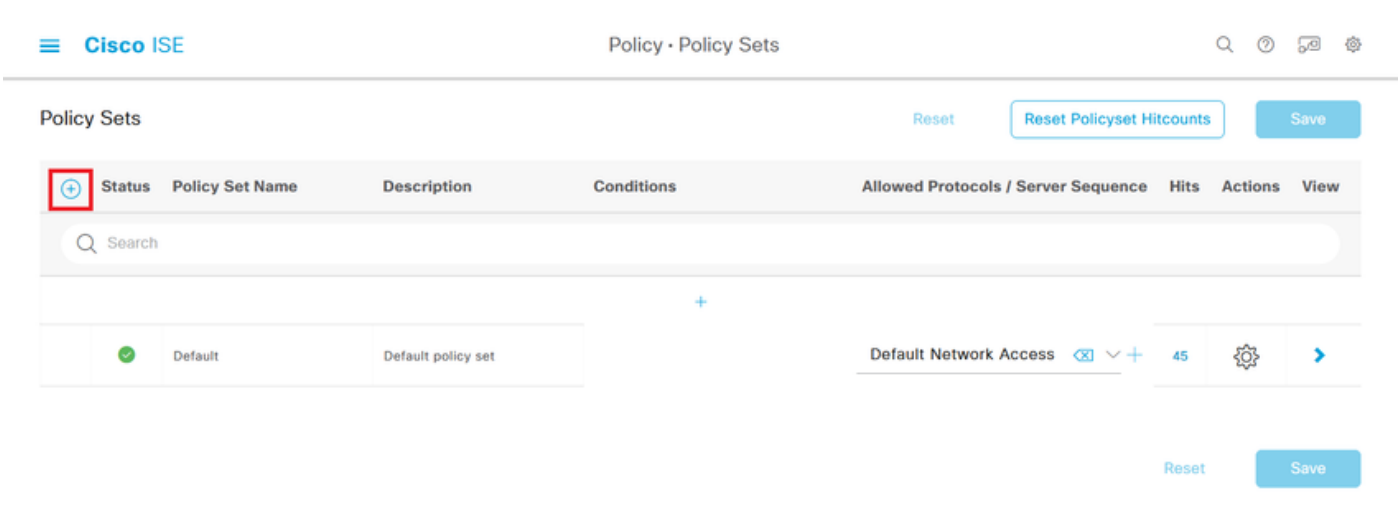




Stap 8. Maak een beleidsset die overeenkomt met het IP-adres van het VCC. Dit om te voorkomen dat andere apparaten toegang verlenen aan de gebruikers.

Navigeer naar
> Beleidssets > pictogram aan de linkerbovenhoek >

.

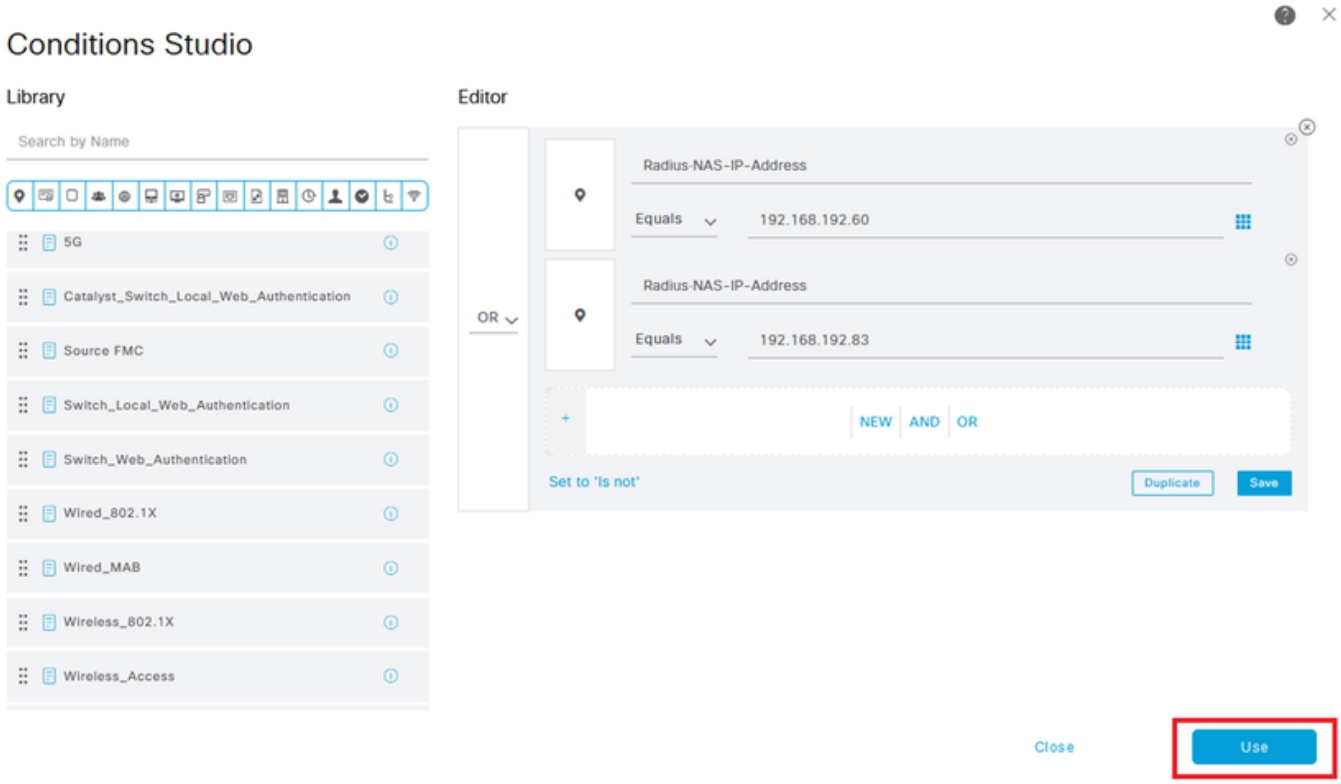

Cisco ISE
Policy · Policy Sets
Policy Sets
Reset
Reset Policyset Hitcounts
Save
Status
Policy Set Name
Description
Conditions
Allowed Protocols / Server Sequence
Hits
Actions
View
Search
Default
Default policy set
Default Network Access
45
Reset
Save

Stap 8.1. Een nieuwe regel wordt bovenaan uw Policy Sets geplaatst.

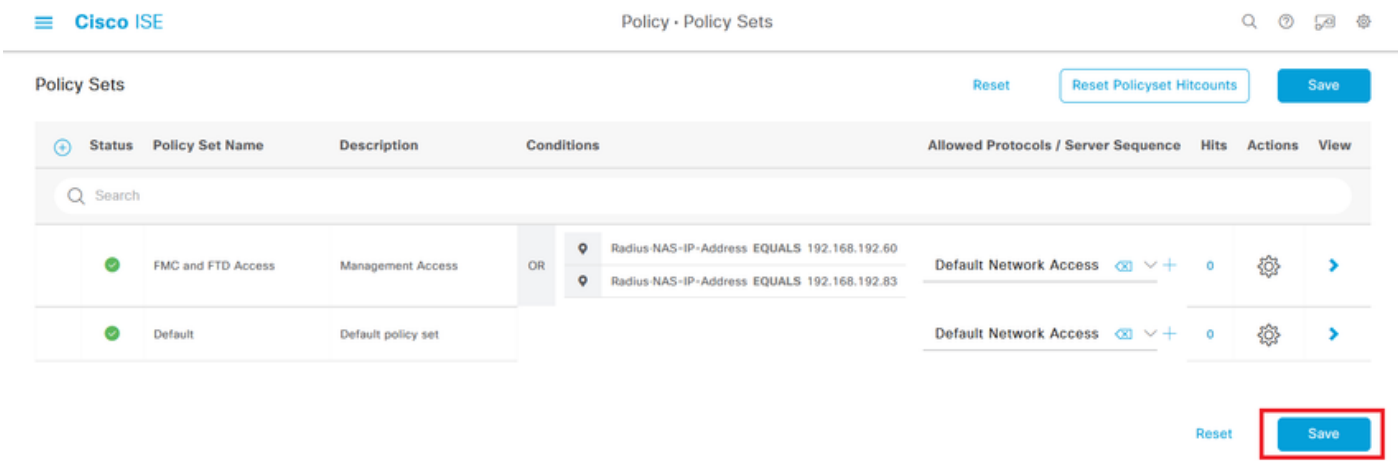
Noem het nieuwe beleid en voeg een topvoorwaarde voor RADIUS NAS-IP-Adres-attribuut dat overeenkomt met het FMC IP-adres.

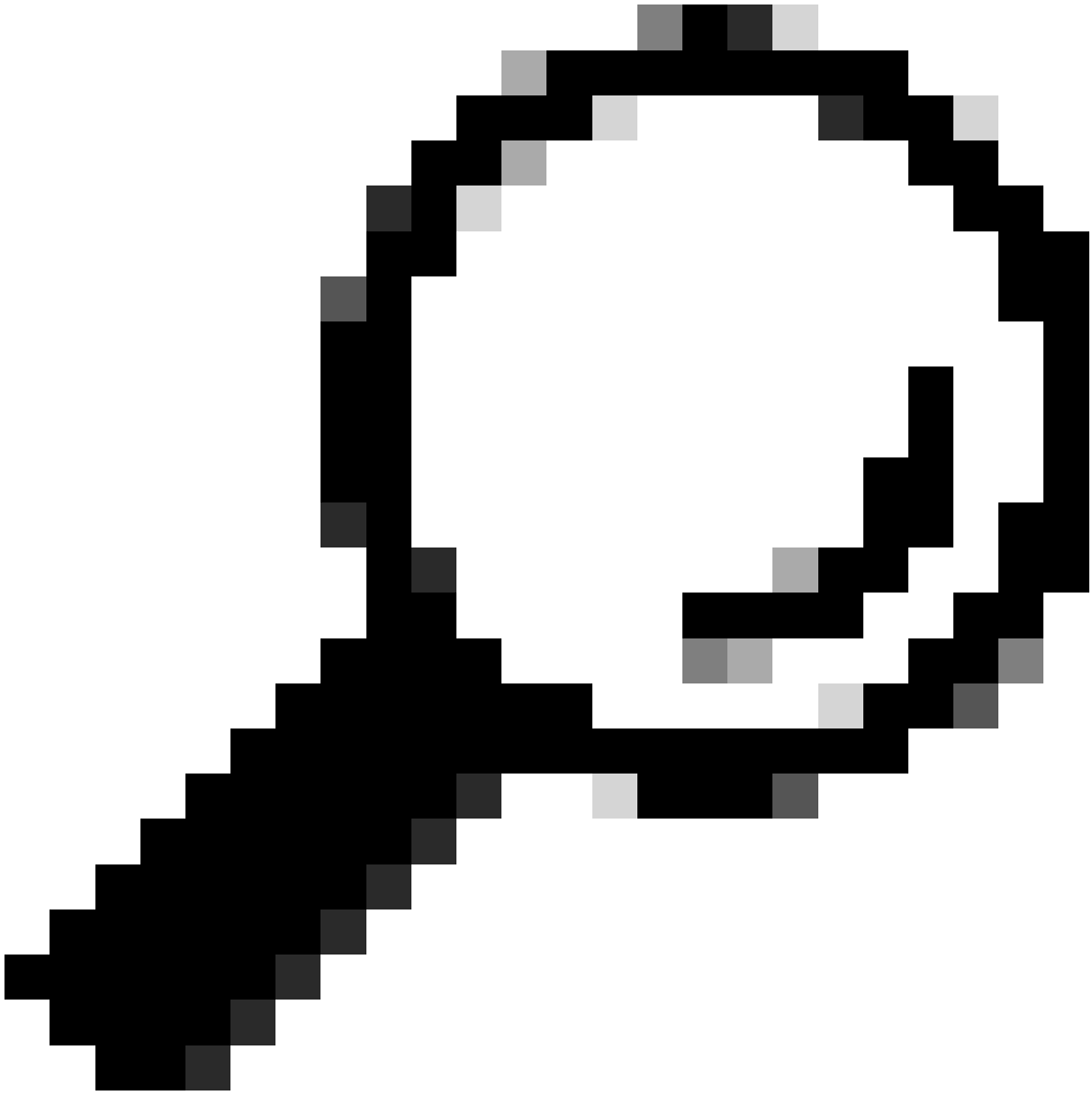
Voeg een tweede voorwaarde met OR combinatie toe om het IP-adres van de FTD op te nemen.

Klik op Gebruik om de wijzigingen te bewaren en de editor te verlaten.



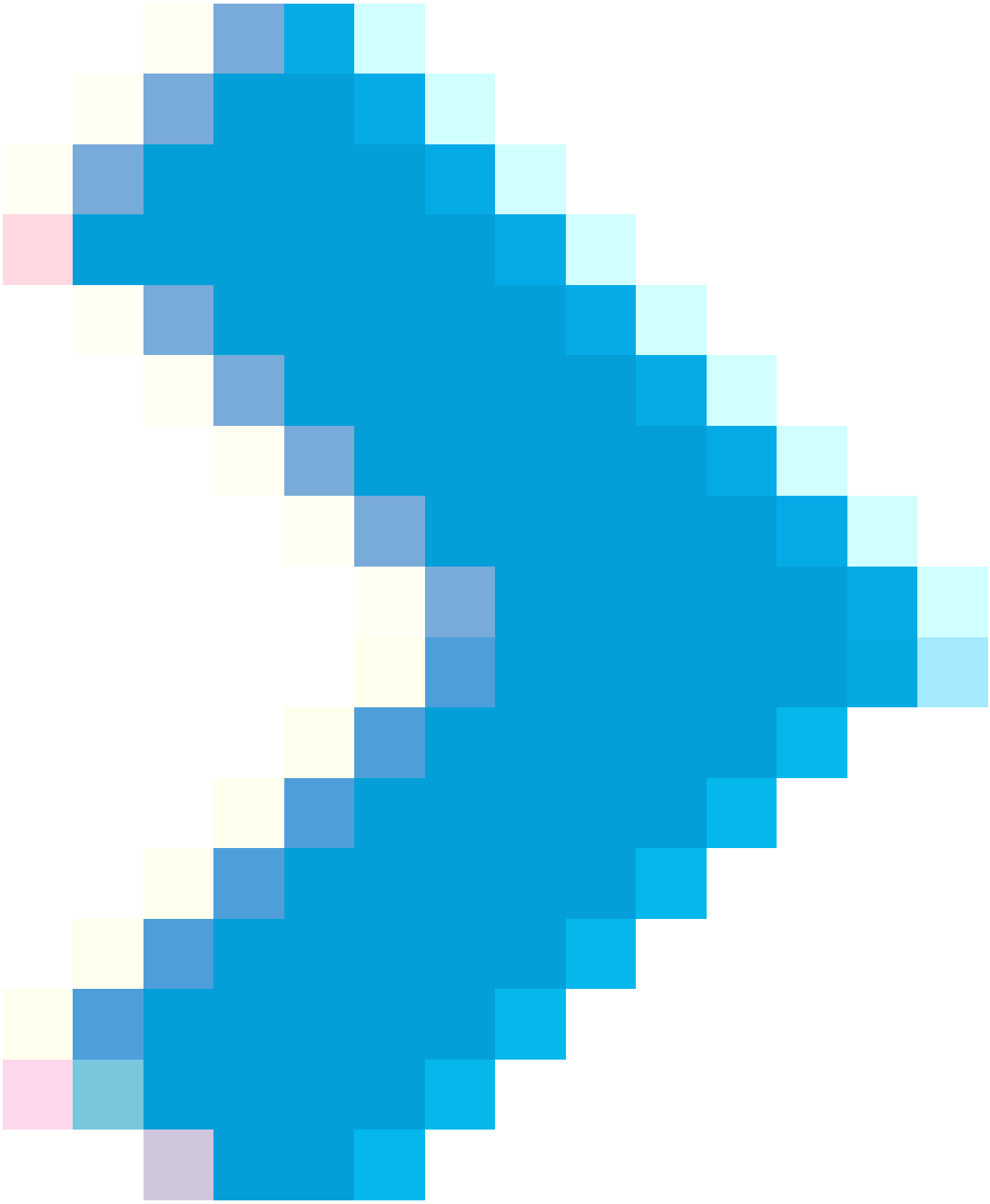
Stap 8.2. Klik op Opslaan als het proces is voltooid.





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 9. Bekijk de nieuwe Policy Set door op het



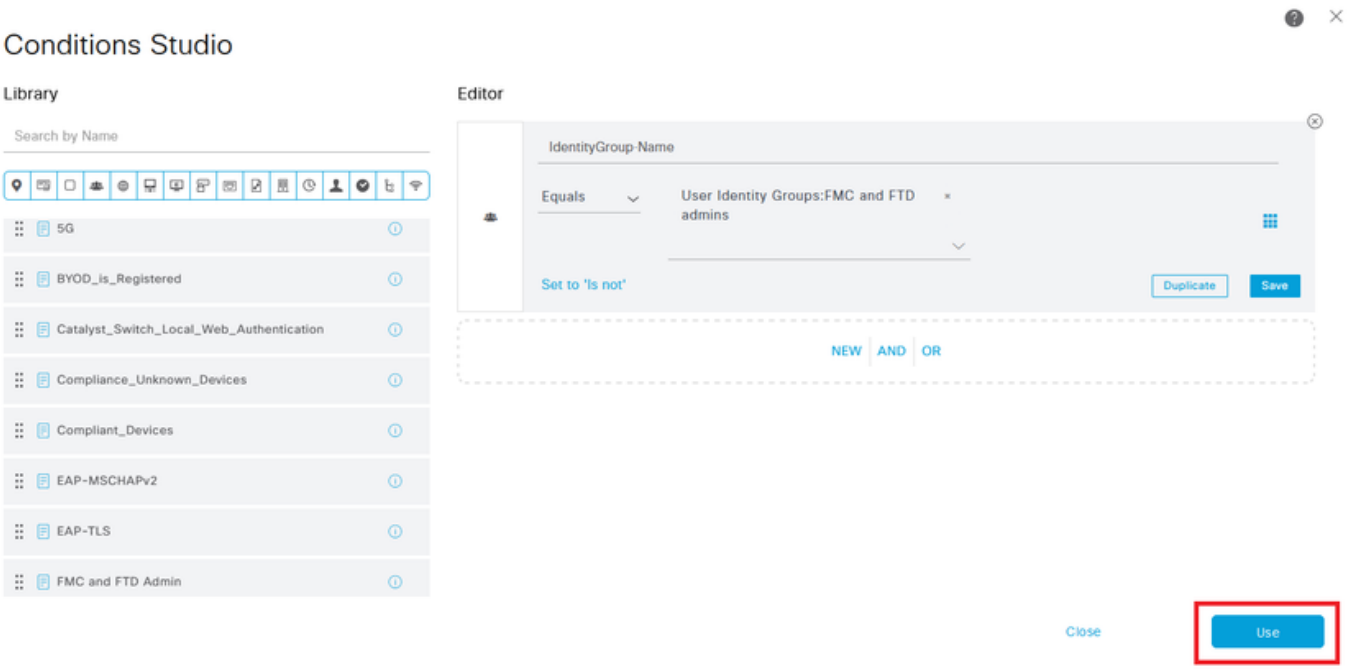
pictogram aan het einde van de rij te drukken.

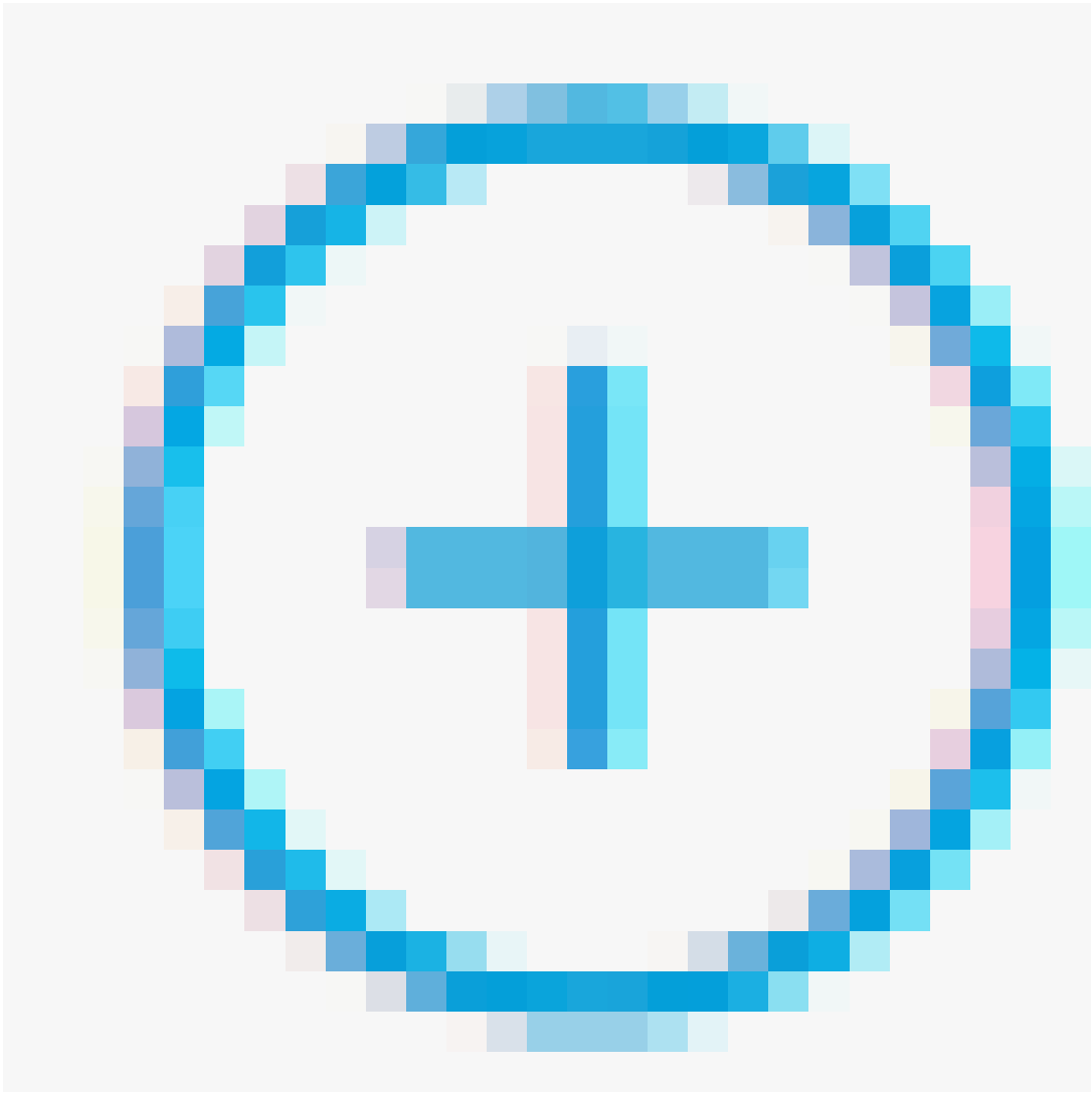
Breid het menu Autorisatiebeleid uit en druk op het

pictogram om een nieuwe regel toe te voegen om de toegang tot de gebruiker met beheerdersrechten toe te staan.

Geef het een naam.

Stel de voorwaarden in om de Dictionary Identity Group met Attribute Name gelijk te stellen aan User Identity Groups: FMC- en FTD-beheerders (de groepsnaam die in Stap 4 is gemaakt) en klik op Use.

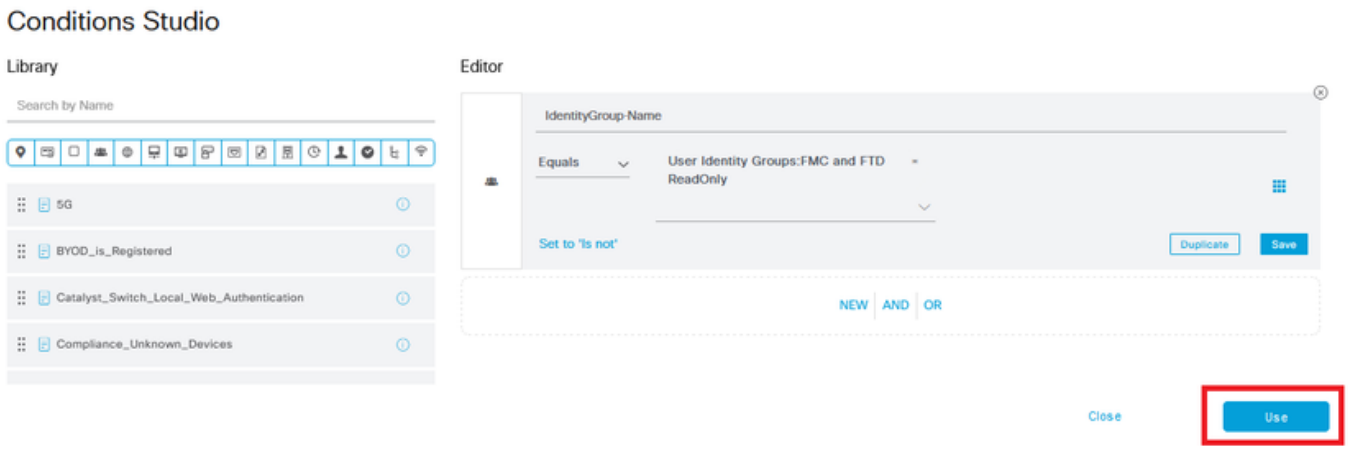




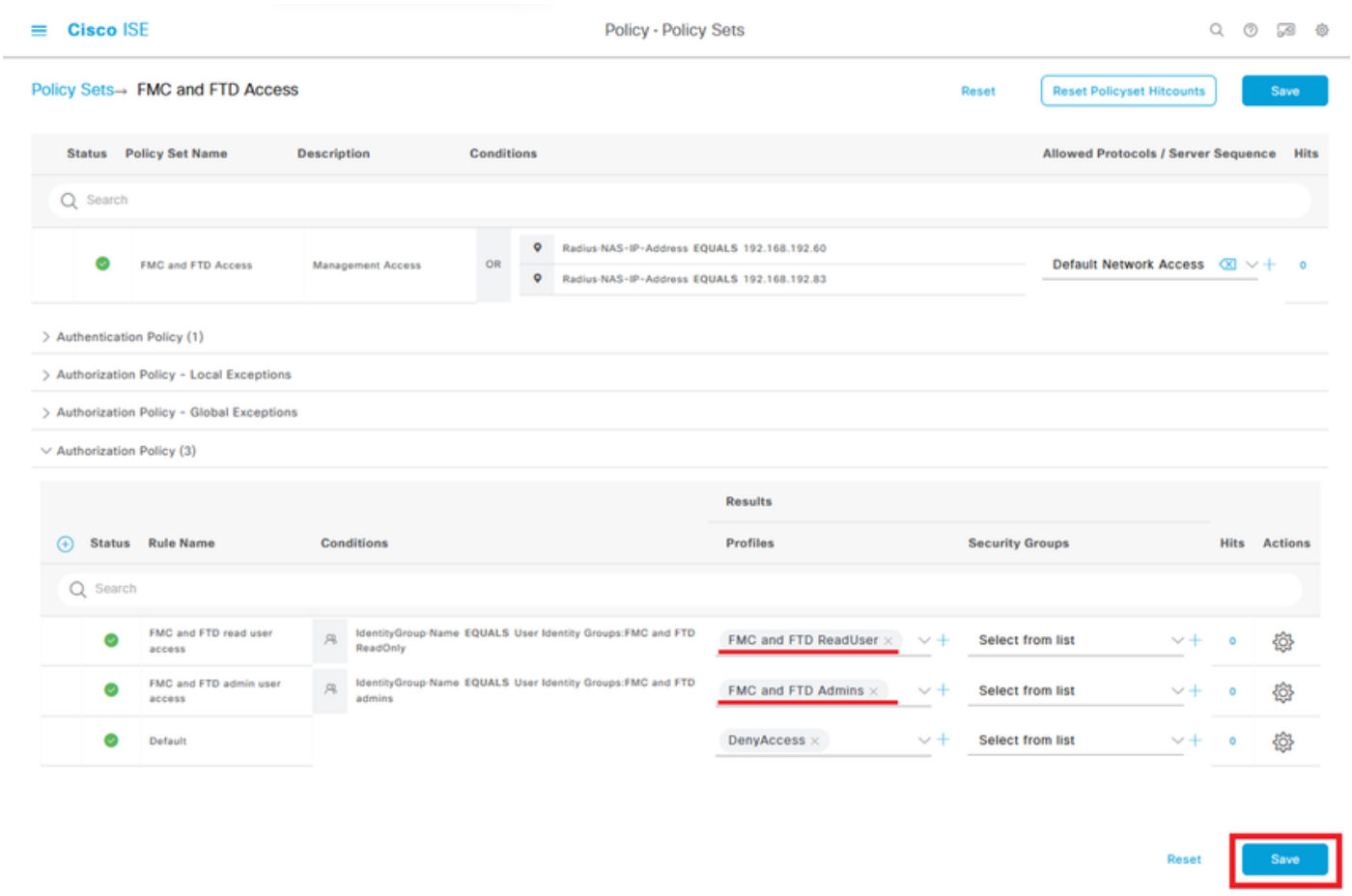
Stap 10. Klik op het pictogram om een tweede regel toe te voegen, zodat de gebruiker toegang heeft tot alleen-lezen rechten.

Geef het een naam.

Stel de voorwaarden in om de Dictionary Identity Group af te stemmen op de naam van het kenmerk Gelijk aan gebruikersgroepen: FMC en FTD ReadOnly (de groepsnaam die in stap 4 is gemaakt) en klik op Use.

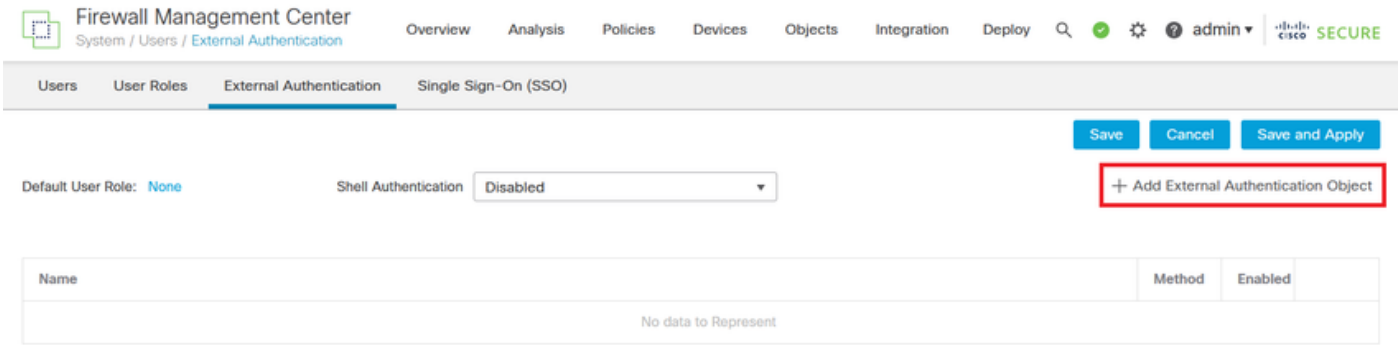


Stap 11. Stel de autorisatieprofielen voor elke regel in en druk op Opslaan.



FMC-configuratie

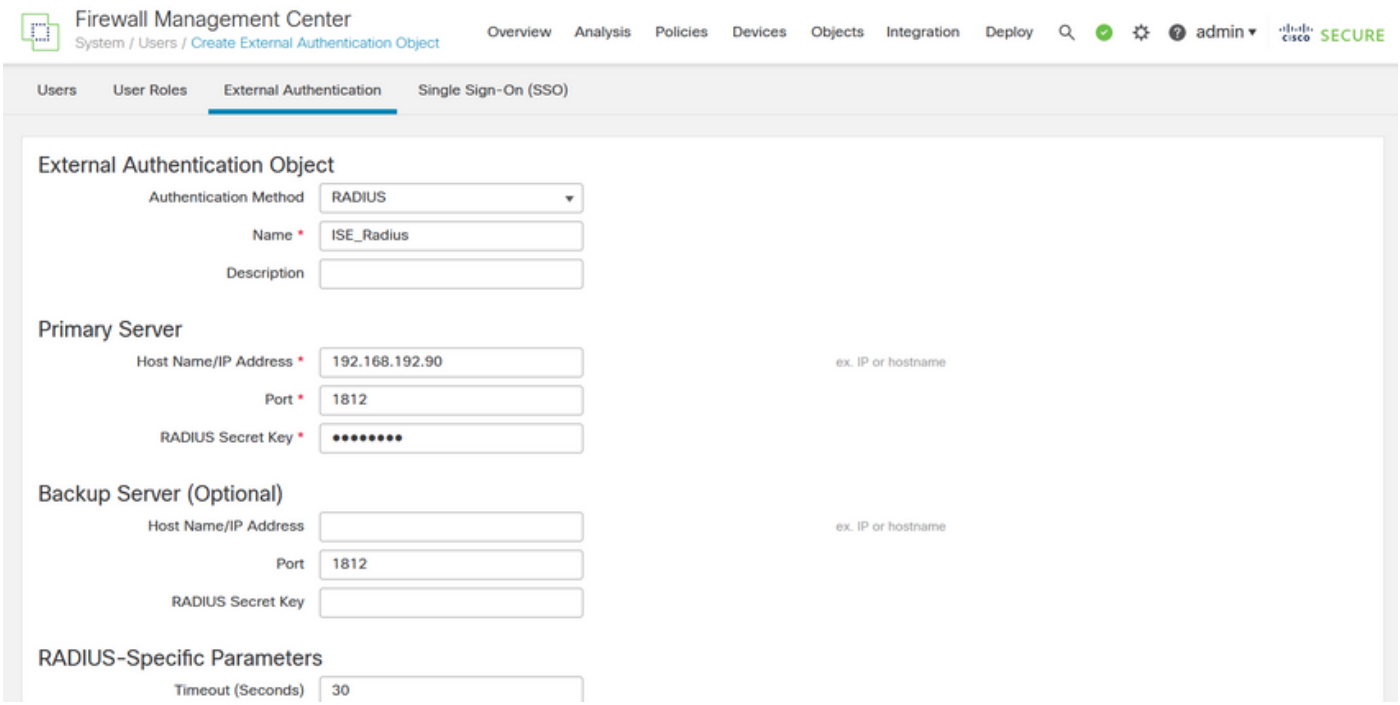
Stap 1. Maak het externe verificatie object onder Systeem > Gebruikers > Externe verificatie > + Add Externe verificatie object.



Stap 2. Selecteer RADIUS als verificatiemethode.

Geef onder Externe verificatie object een naam aan het nieuwe object.

Plaats vervolgens in de instelling Primary Server het ISE-IP-adres en dezelfde RADIUS Secret Key die u in stap 2 van uw ISE-configuratie hebt gebruikt.

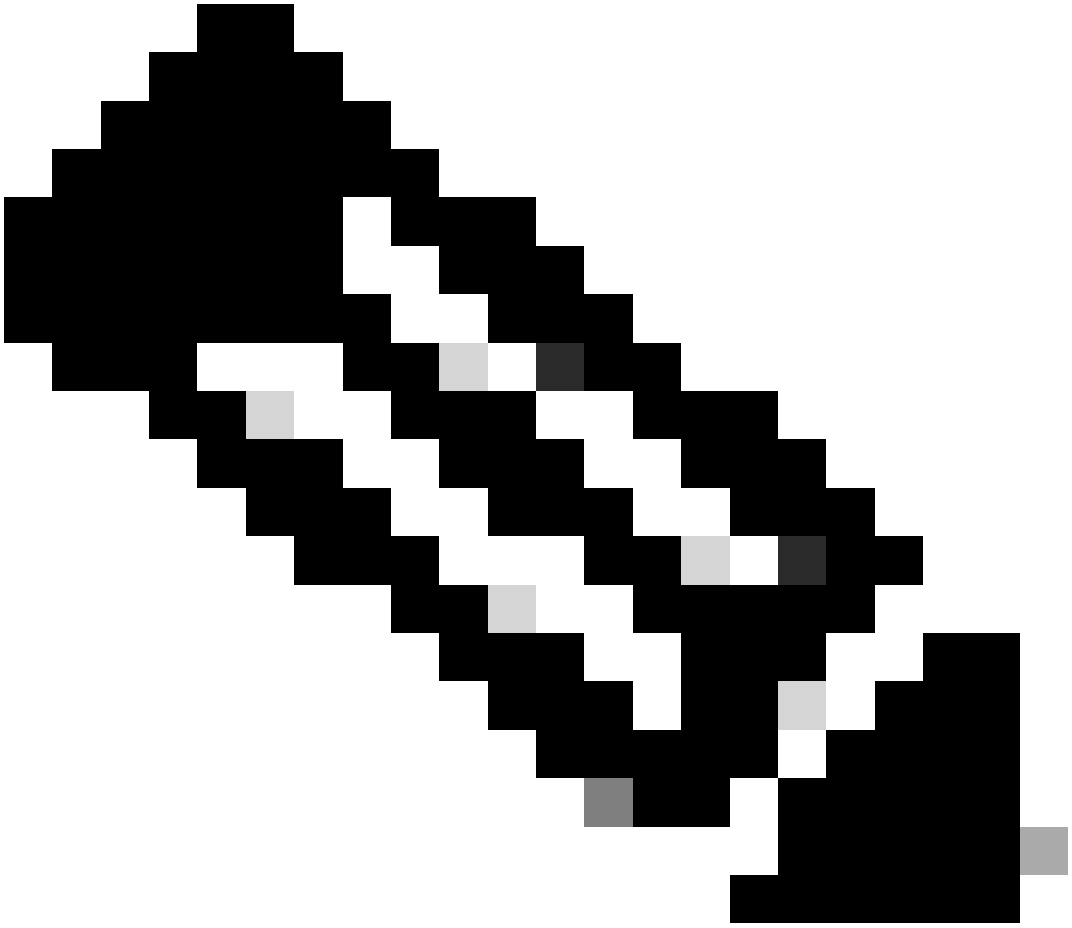


Stap 3. Plaats de waarden van de RADIUS-klasse die zijn geconfigureerd in stap 6 en 7 van ISE Configuration: Administrator en ReadUser voor respectievelijk firewall_admin en firewall_readuser.

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=Administrator
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	Class=ReadUser
Security Approver	
Threat Intelligence Director (TID) User	
Default User Role	Access Admin Administrator Discovery Admin External Database User

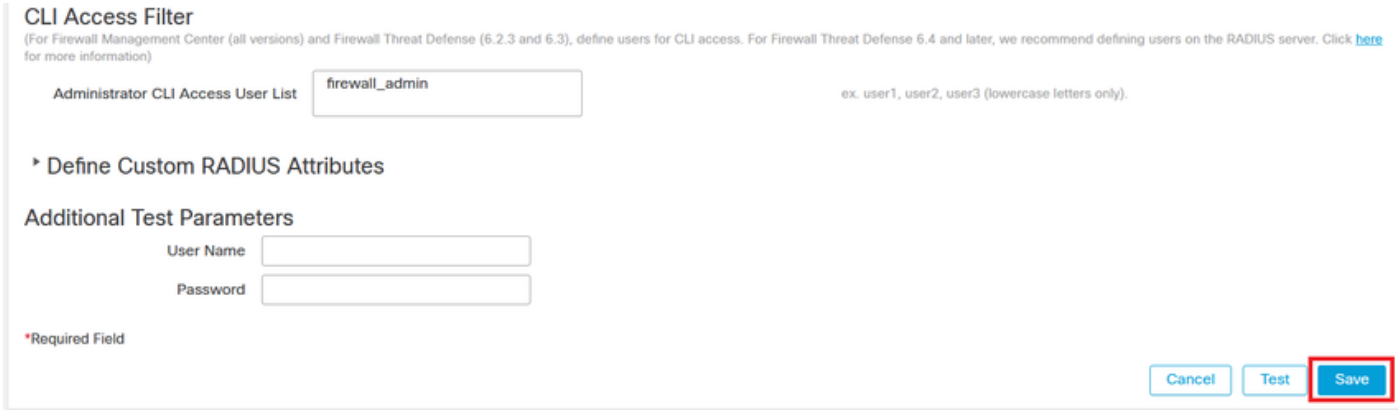
To specify the default user role if user is not found in any group



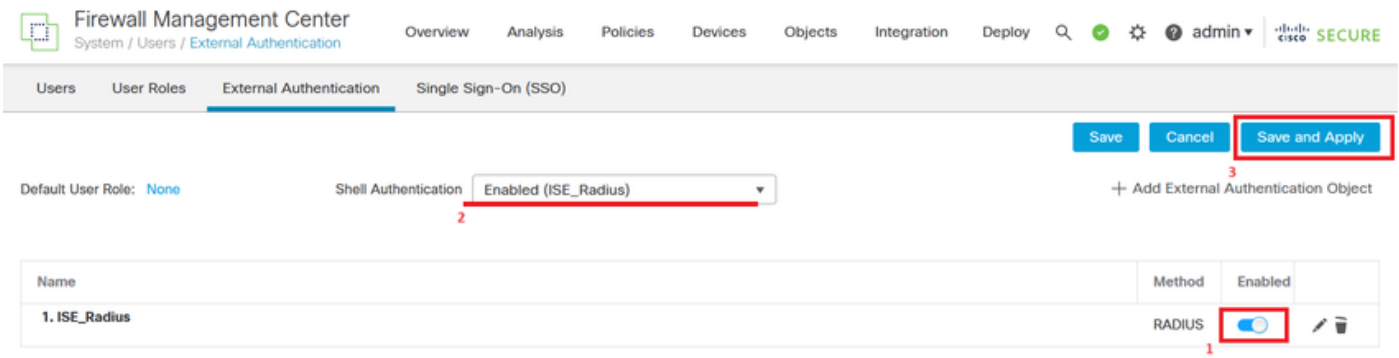
Opmerking: Het tijdsbereik is anders voor de FTD en de FMC. Als u dus een object deelt en de standaardwaarde van 30 seconden wijzigt, moet u ervoor zorgen dat u het kleinere tijdsbereik (1-300 seconden) voor FTD-apparaten niet overschrijdt. Als u de timeout op een hogere waarde instelt, werkt de Threat Defense RADIUS configuratie niet.

Stap 4. Bevolk de beheerder CLI Access User List onder CLI Access Filter met de gebruikersnamen die CLI-toegang kunnen verkrijgen.

Klik op Opslaan als u klaar bent.

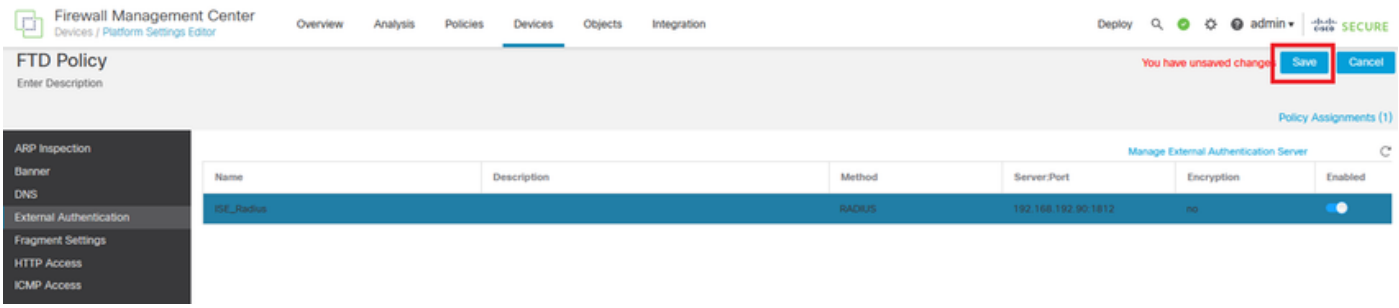


Stap 5. Schakel het nieuwe object in. Stel dit in als de Shell-verificatiemethode voor FMC en klik op Opslaan en Toepassen.

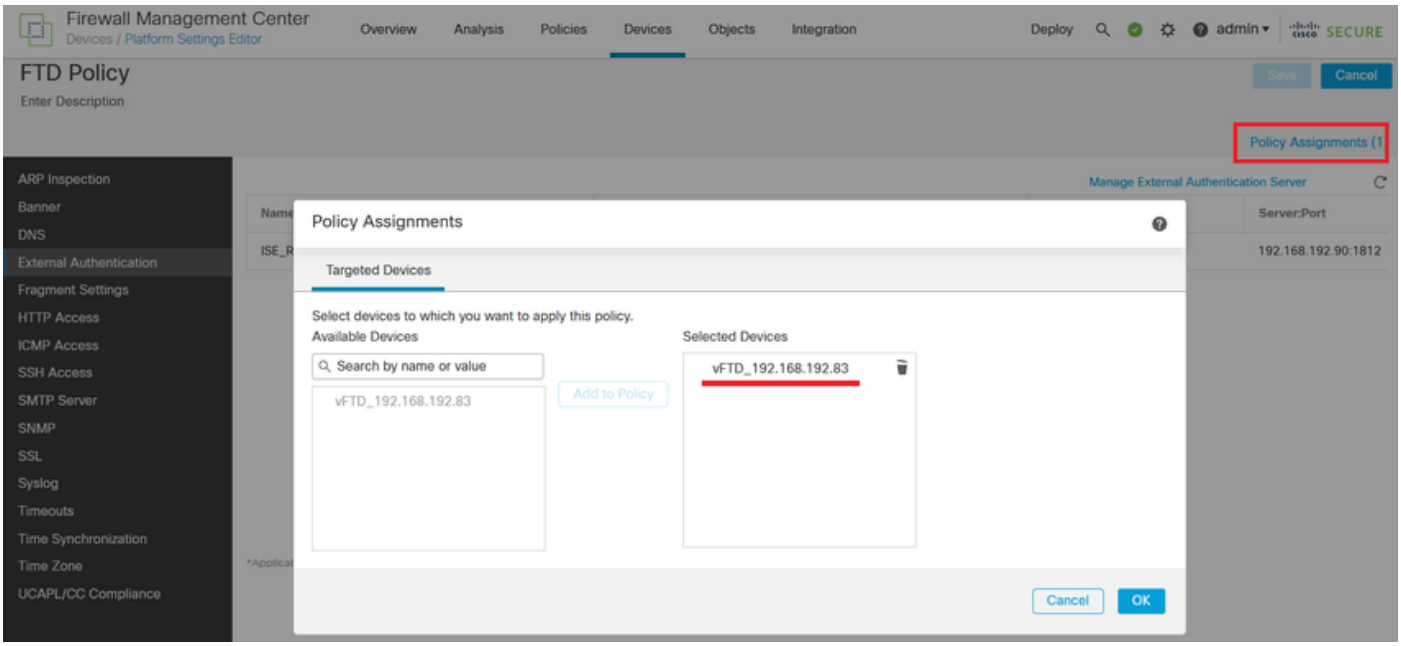


FTD-configuratie

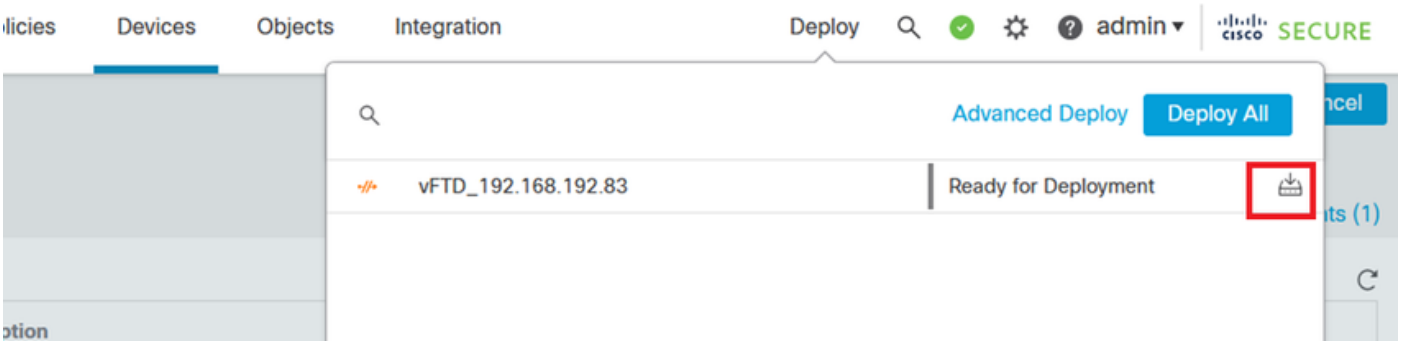
Stap 1. In FMC GUI navigeer je naar Apparaten > Platform-instellingen. Bewerk uw huidige beleid of maak een nieuwe als u geen toegewezen aan het FTD hebt u toegang tot nodig hebt. Schakel de RADIUS-server in onder Externe verificatie en klik op Opslaan.



Stap 2. Zorg ervoor dat de FTD die u moet bereiken, wordt vermeld onder Beleidstoewijzingen als geselecteerd apparaat.

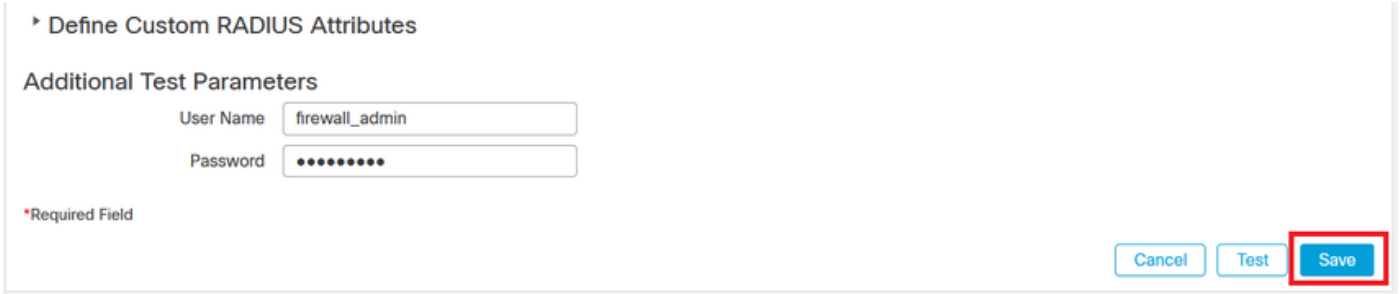


Stap 3. Voer de wijzigingen in.

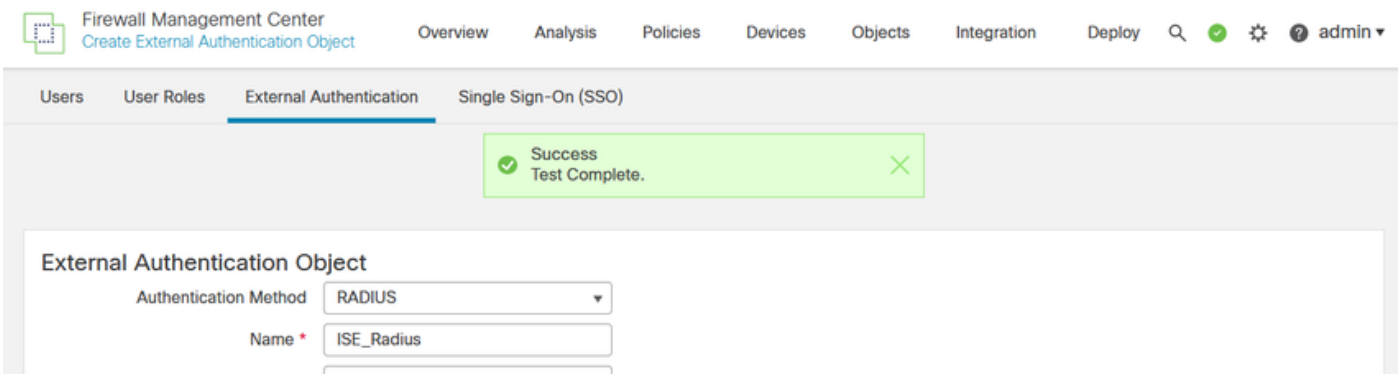


Verifiëren

- Test of uw nieuwe implementatie goed werkt.
- Navigeer in de FMC GUI naar de RADIUS-serverinstellingen en blader naar beneden naar de sectie Aanvullende testparameters.
- Voer een gebruikersnaam en wachtwoord in voor de ISE-gebruiker en klik op Test.



- Een succesvolle test toont een groen Success Test Compleet bericht boven in het browservenster.



- U kunt de Details onder de Test-uitgang uitvouwen voor meer informatie.

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.