Externe FMC-verificatie configureren in een omgeving met meerdere domeinen

Inhoud

Inleiding

Dit document beschrijft de implementatie van multitenancy (multi-domain) binnen de Cisco FMC en maakt gebruik van Cisco ISE voor gecentraliseerde RADIUS-verificatie.

Voorwaarden

Vereisten

Het wordt aanbevolen om kennis te hebben van deze onderwerpen:

- Cisco Secure Firewall Management Center eerste configuratie via GUI en/of shell.
- Volledige beheerdersrechten in het globale domein van de FMC om subdomeinen en externe verificatieobjecten te maken.
- Authenticatie- en autorisatiebeleid configureren op ISE.
- Basiskennis RADIUS

Gebruikte componenten

- Cisco Secure FMC: vFMC 7.4.2 (of hoger aanbevolen voor stabiliteit in meerdere domeinen)
- Domeinstructuur: een hiërarchie op drie niveaus (globaal > subdomeinen op het tweede niveau).
- Cisco Identity Services-engine: ISE 3.3

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

In grootschalige bedrijfsomgevingen of Managed Security Service Provider (MSSP)-scenario's is het vaak nodig om netwerkbeheer te segmenteren in afzonderlijke administratieve grenzen. In dit document wordt beschreven hoe de FMC kan worden geconfigureerd om meerdere domeinen te ondersteunen, met name voor een praktijkvoorbeeld waarbij een MSSP twee klanten beheert: Retail-A en Finance-B. Door externe RADIUS-verificatie via Cisco ISE te gebruiken, kunnen beheerders ervoor zorgen dat gebruikers automatisch alleen toegang krijgen tot hun respectieve gebruikersdomeinen op basis van hun gecentraliseerde referenties.

Het Cisco Secure Firewall-systeem gebruikt Domains om multitenancy te implementeren.

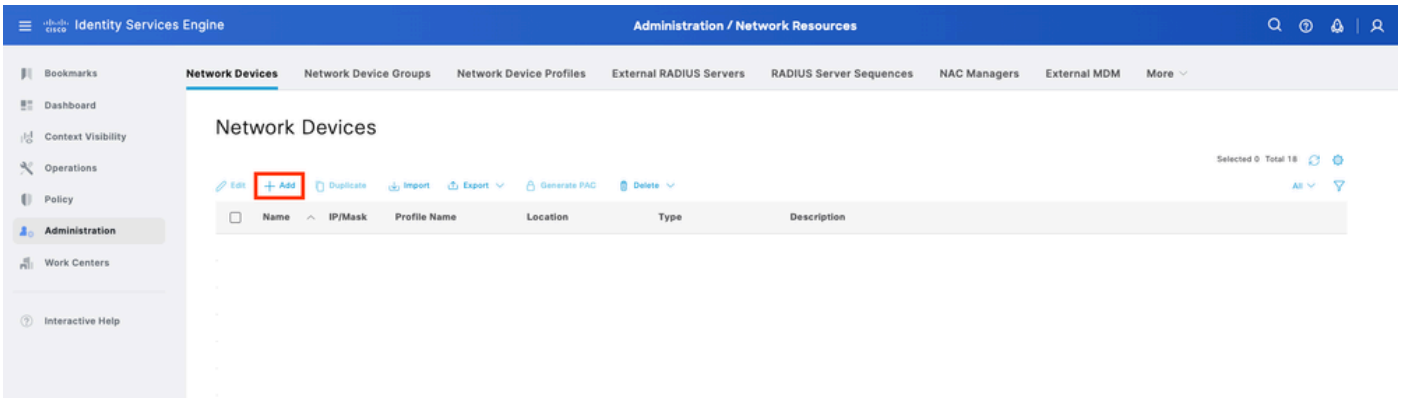
- Domeinhiërarchie: De hiërarchie begint bij het globale domein. U kunt maximaal 100 subdomeinen maken in een structuur met twee of drie niveaus.
- Leaf Domains: Dit zijn domeinen onderaan de hiërarchie zonder verdere subdomeinen. Cruciaal is dat elk beheerd FTD-apparaat moet worden gekoppeld aan precies één bladdomein.
- RADIUS Class Attribuut (Attribuut 25): In een configuratie met meerdere domeinen gebruikt de FMC het RADIUS Class-attribuut dat door ISE wordt geretourneerd om een geverifieerde gebruiker toe te wijzen aan een specifiek domein en een specifieke gebruikersrol. Hierdoor kan een enkele RADIUS-server dynamisch gebruikers toewijzen aan verschillende gebruikerssegmenten (bijvoorbeeld Retail-A vs. Finance-B) bij het aanmelden.

Configuratie

ISE-configuratie

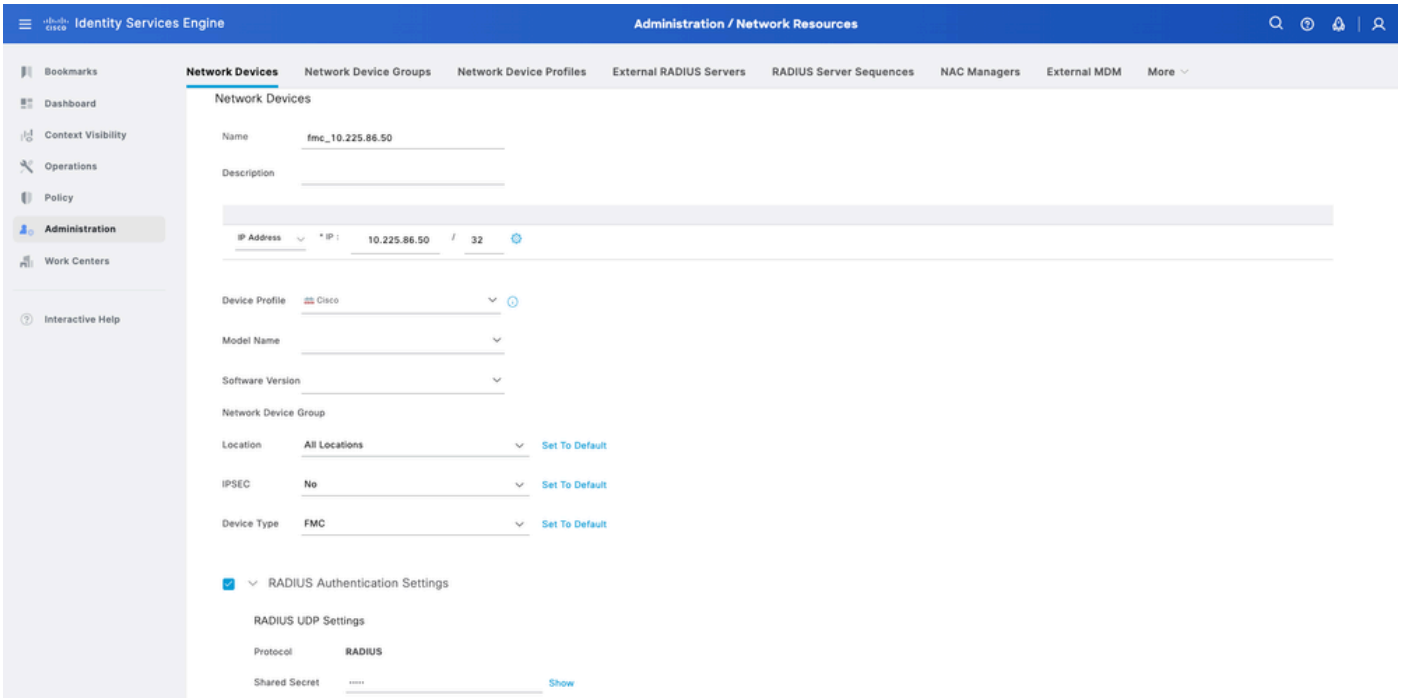
Voeg uw netwerkapparaten toe

Stap 1. Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten > Toevoegen.



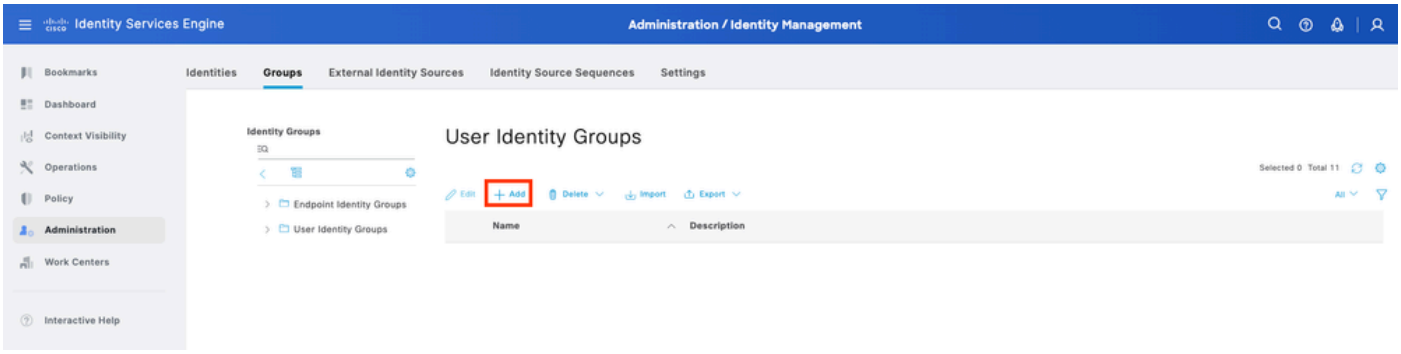
Stap 2. Wijs een naam toe aan het netwerkapparatobject en voer het IP-adres van de FMC in.

Schakel het selectievakje RADIUS in en definieer een gedeeld geheim. Dezelfde sleutel moet later worden gebruikt om de FMC te configureren. Als u klaar bent, klikt u op Opslaan.

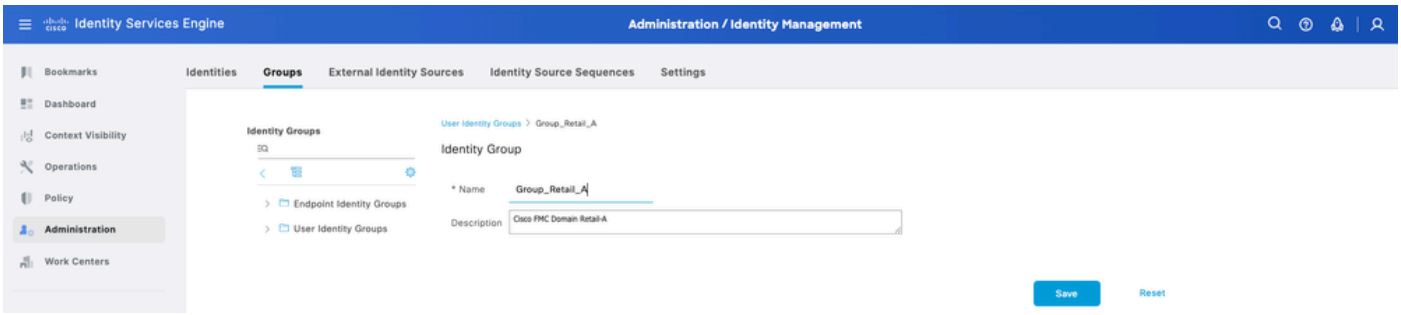


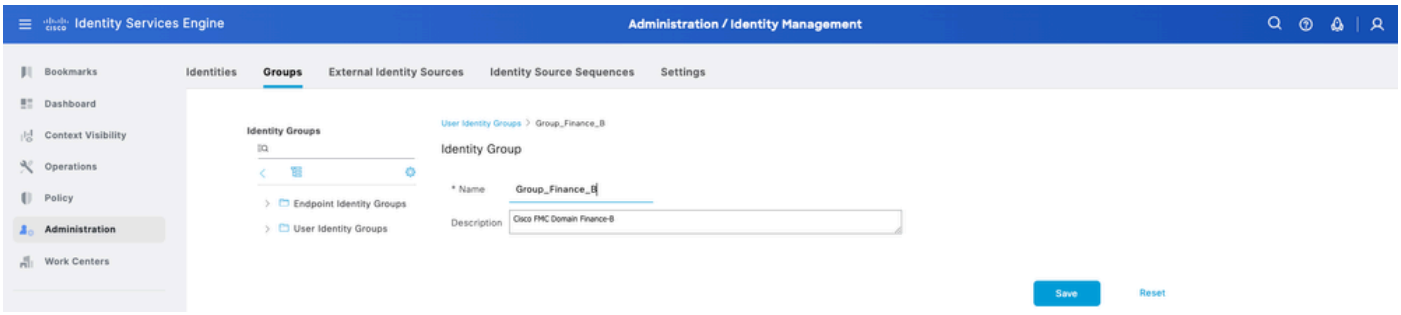
De lokale gebruikersidentiteitsgroepen en -gebruikers maken

Stap 3. Maak de vereiste groepen voor gebruikersidentiteit. Navigeer naar Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen > Toevoegen.

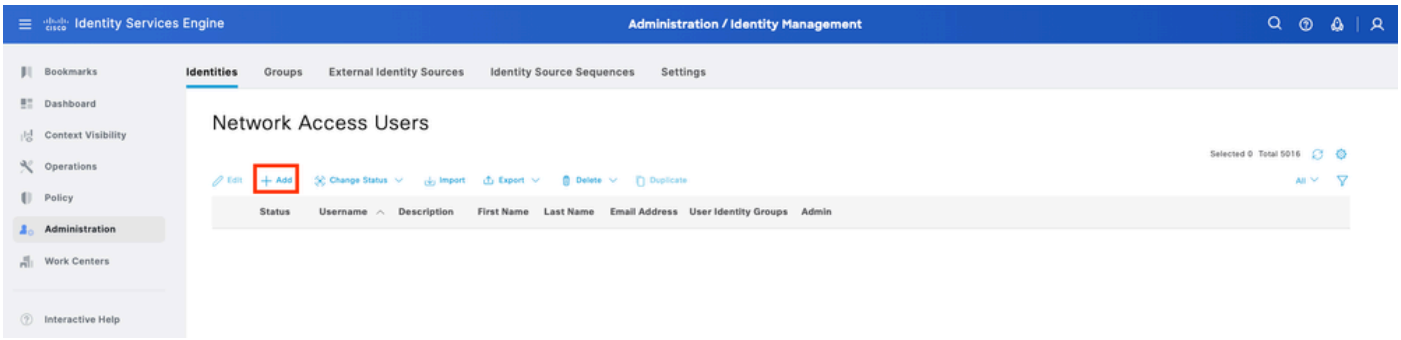


Stap 4. Geef elke groep een naam en bewaar afzonderlijk. In dit voorbeeld maakt u een groep voor beheerders. Maak twee groepen: Group_Retail_A en Group_Finance_B.

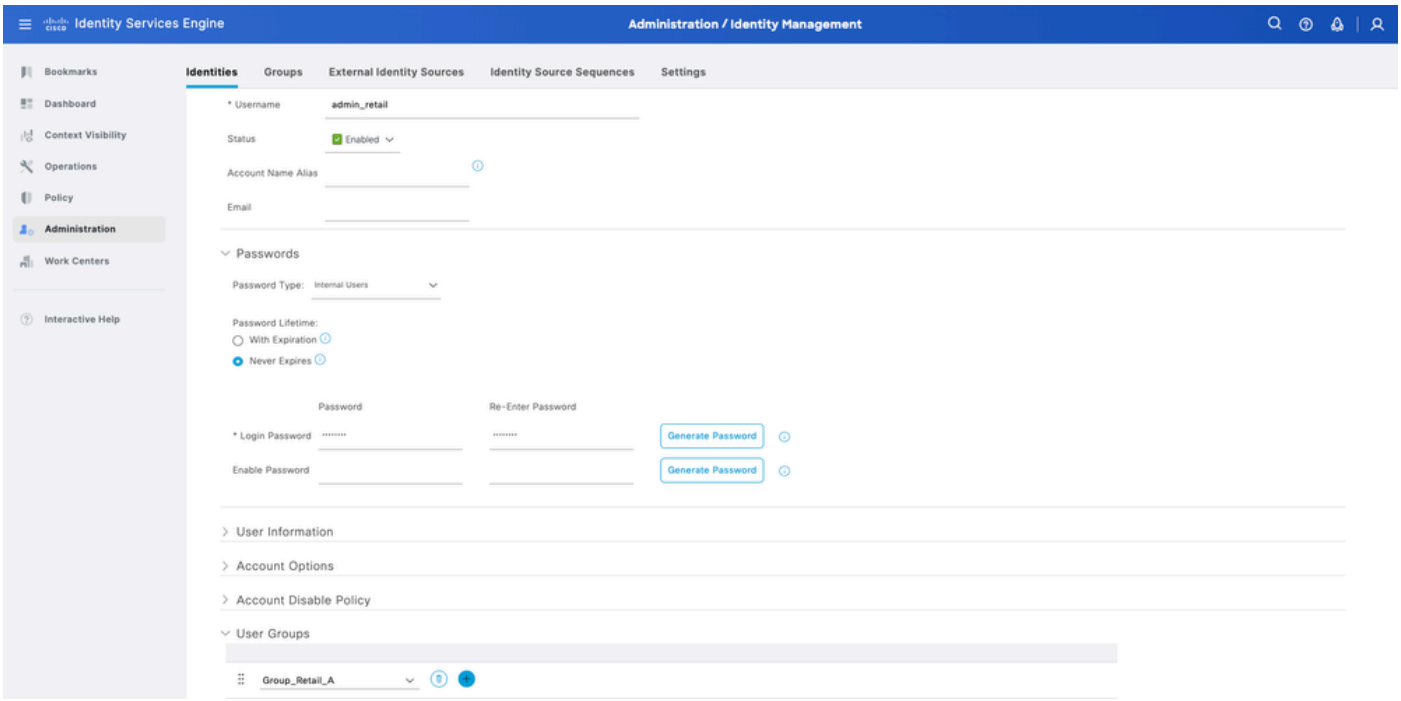




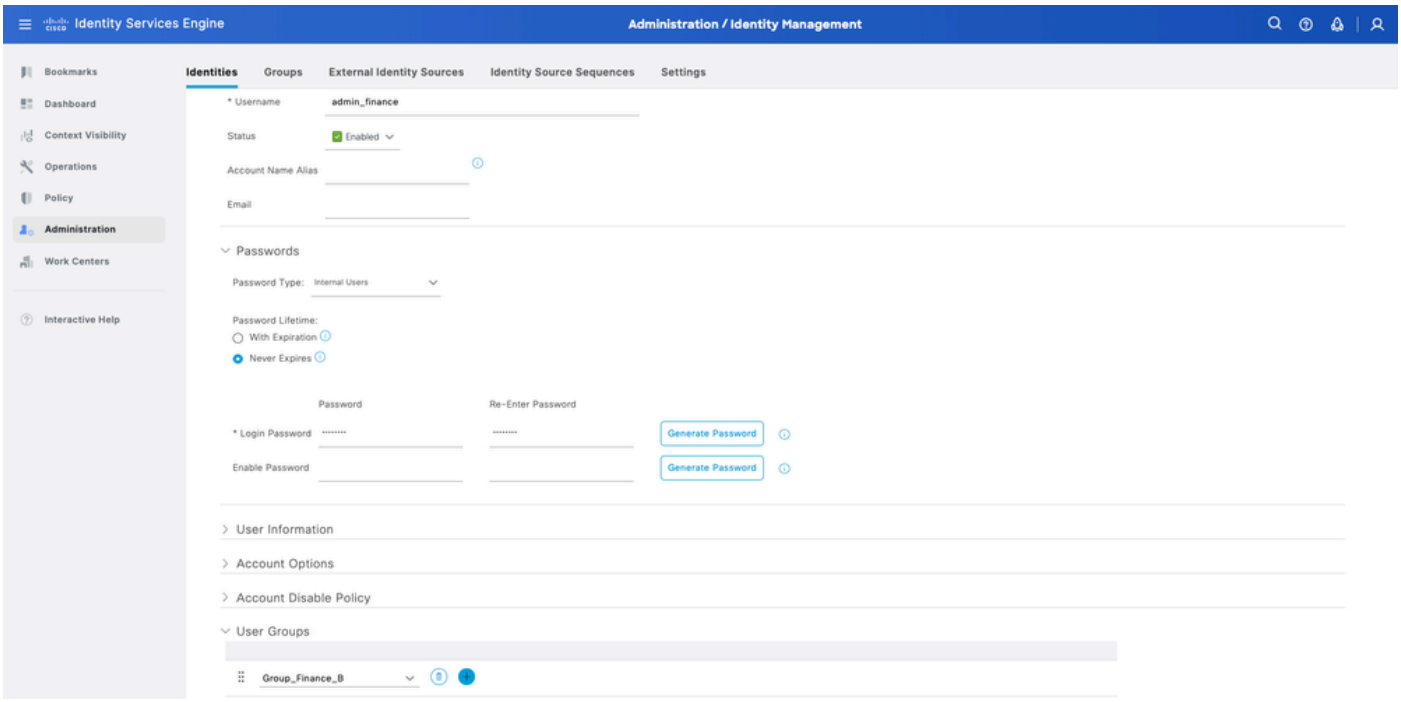
Stap 5. Maak de lokale gebruikers en voeg ze toe aan hun correspondentengroep. Navigeer naar Beheer > Identiteitsbeheer > Identiteiten > Toevoegen.



Stap 5.1. Maak eerst de gebruiker aan met beheerdersrechten. Wijs een naam toe aan admin_retail, wachtwoord en de groep Group_Retail_A.

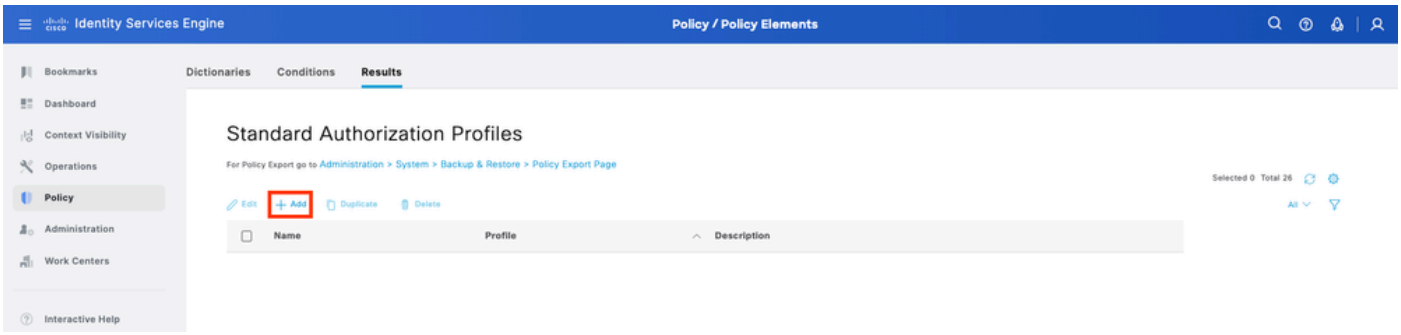


Stap 5.2. Maak eerst de gebruiker aan met beheerdersrechten. Wijs een naam toe aan admin_finance, wachtwoord en de groep Group_Finance_B.



Machtigingsprofielen maken

Stap 6. Maak het autorisatieprofiel voor de FMC Web Interface Admin-gebruiker. Navigeer naar Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen > Toevoegen.

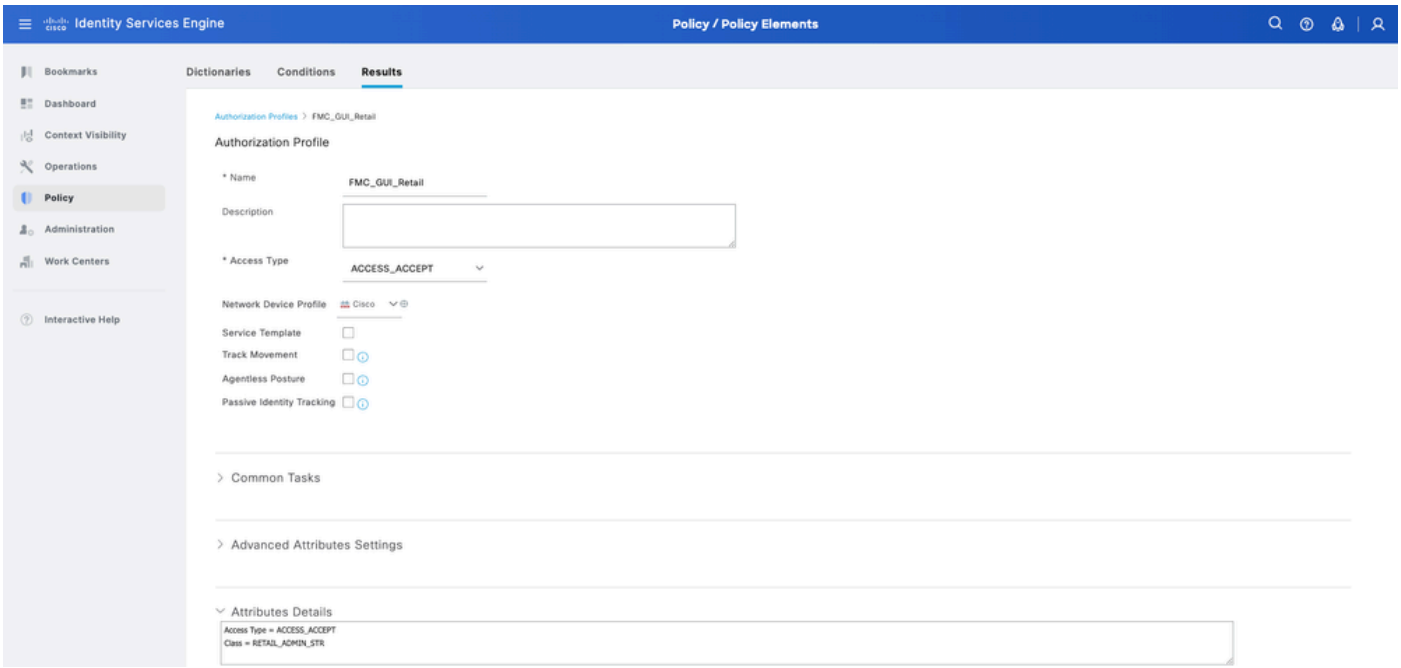


Definieer een naam voor het autorisatieprofiel en laat het toegangstype ACCESS_ACCEPT staan.

Voeg onder Geavanceerde Attributen instellingen een Straal > Klasse--[25] met de waarde toe en klik op Indienen.

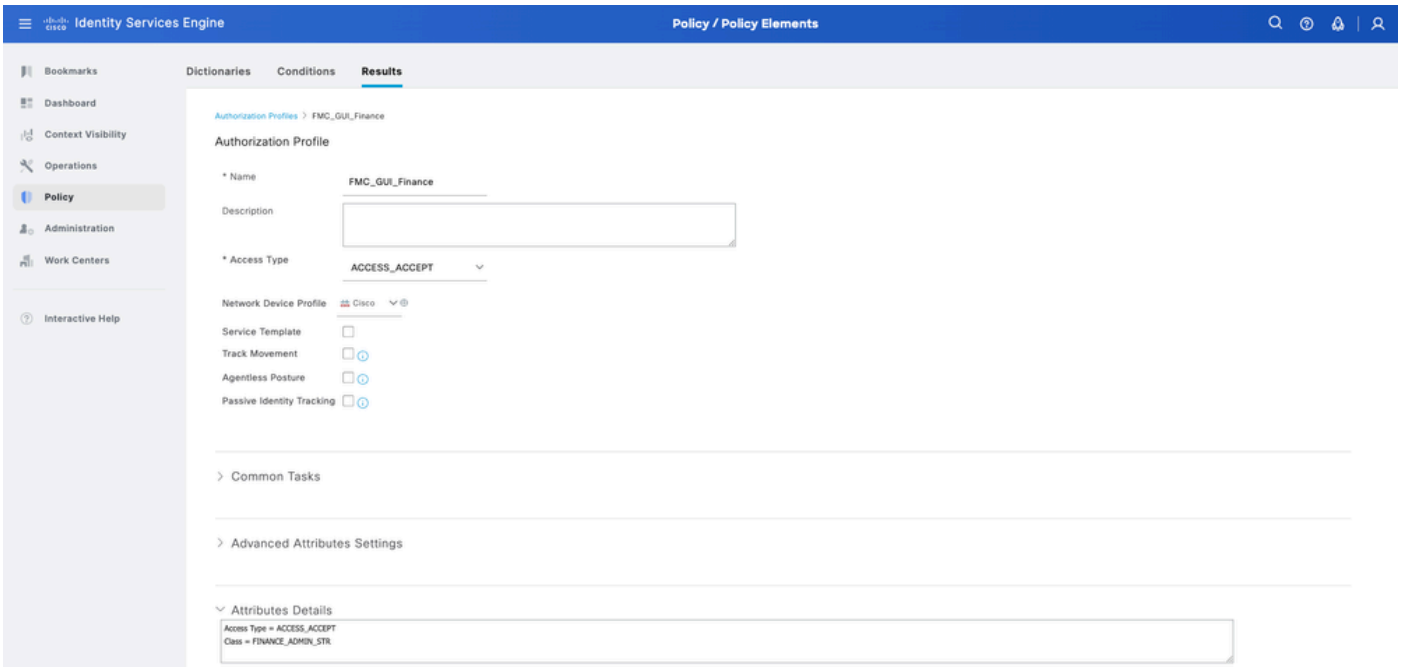
Stap 6.1. Profiel Retail: Onder Geavanceerde Attributen Instellingen, voeg Straal:Klasse met de waarde RETAIL_ADMIN_STR.

Tip: hier kan RETAIL_ADMIN_STR van alles zijn; zorg ervoor dat dezelfde waardebehoeften ook aan de FMC-kant worden geplaatst.



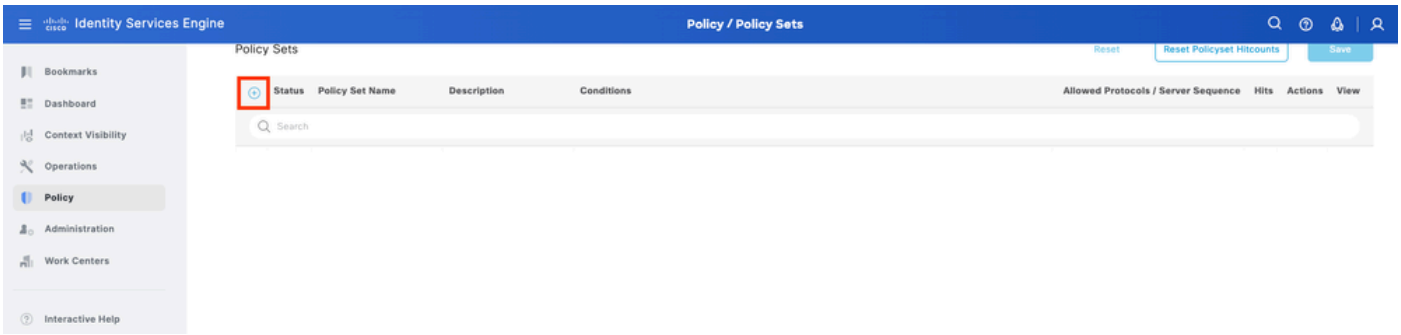
Stap 6.2. Profielfinanciering: onder Geavanceerde attributen instellingen, voeg Straal: Klasse met de waarde FINANCE_ADMIN_STR.

Tip: hier kan FINANCE_ADMIN_STR van alles zijn; zorg ervoor dat dezelfde waarde ook aan de FMC-kant wordt geplaatst.



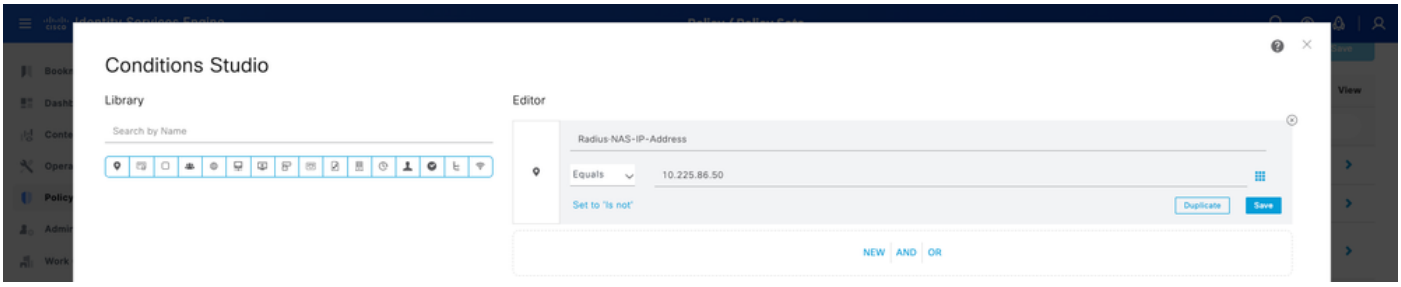
Een nieuwe beleidsset toevoegen

Stap 7. Maak een beleidsset die overeenkomt met het FMC IP-adres. Dit om te voorkomen dat andere apparaten toegang verlenen aan de gebruikers. Navigeer naar Beleid > Beleidssets > Plusteken pictogram geplaatst in de linkerbovenhoek.



Stap 8.1. Een nieuwe regel wordt bovenaan uw beleidssets geplaatst.

Geef het nieuwe beleid een naam en voeg een topvoorwaarde toe voor het RADIUS NAS-IP-Address-kenmerk dat overeenkomt met het FMC-IP-adres. Klik op Gebruik om de wijzigingen te behouden en de editor af te sluiten.



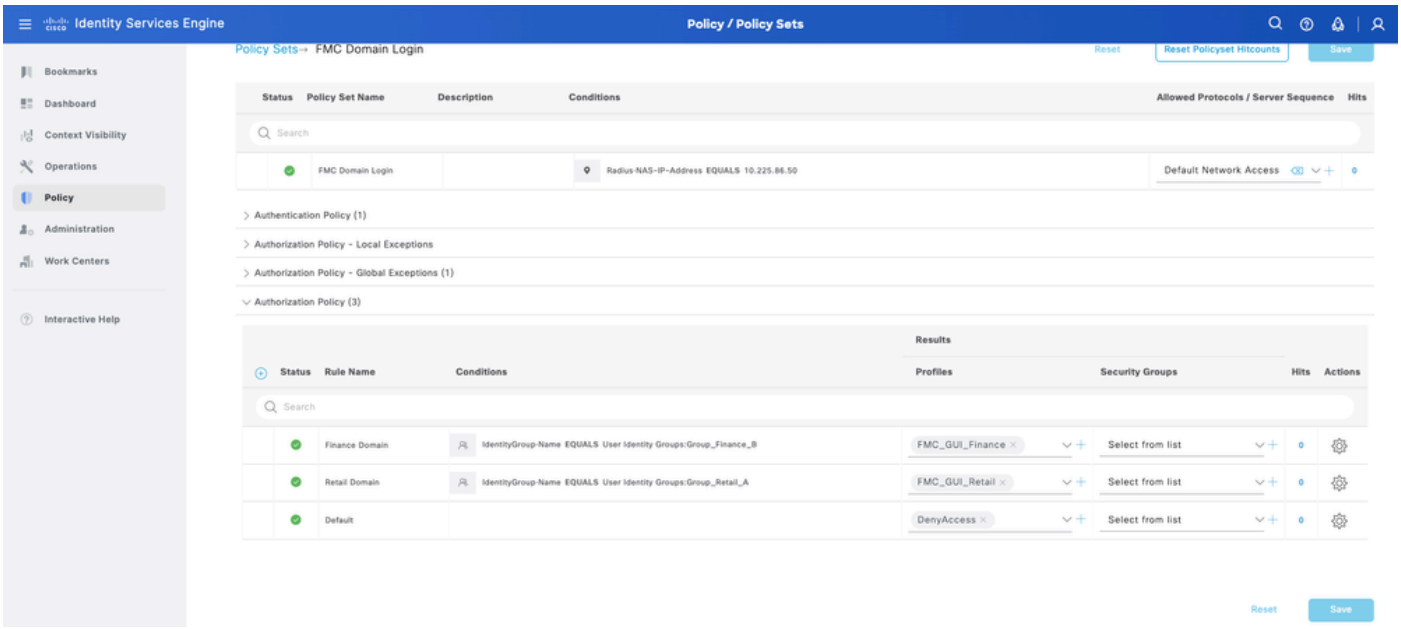
Stap 8.2. Klik op Opslaan als u klaar bent.

Stap 9. Bekijk de nieuwe beleidsinstelling door op het ingestelde pictogram aan het einde van de rij te drukken.

Vouw het menu Autorisatiebeleid uit en druk op het plusteken om een nieuwe regel toe te voegen zodat de gebruiker met beheerdersrechten toegang heeft. Geef het een naam.

Stel de voorwaarden in die overeenkomen met de woordenboekidentiteitsgroep met Attribuutnaam is gelijk en kies Gebruikersidentiteitsgroepen. Maak in het kader van het machtigingsbeleid regels:

- Regel 1: Als User Identity Group gelijk is aan Group_Retail_A, wijst u het Retail-profiel toe.
- Regel 2: Als User Identity Group gelijk is aan Group_Finance_B, wijst u de profielfinanciering toe.



Stap 10. Stel de autorisatieprofielen in voor elke regel en druk op Opslaan.

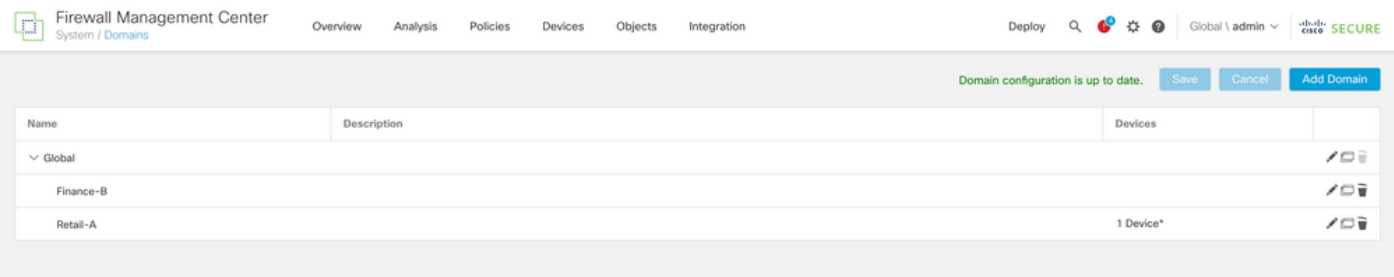
FMC-configuratie

Uw ISE RADIUS-server toevoegen voor FMC-verificatie

Stap 1: Bepaal de domeinstructuur:

- Meld u aan bij het FMC Global-domein.
- Navigeer naar Beheer > Domeinen.

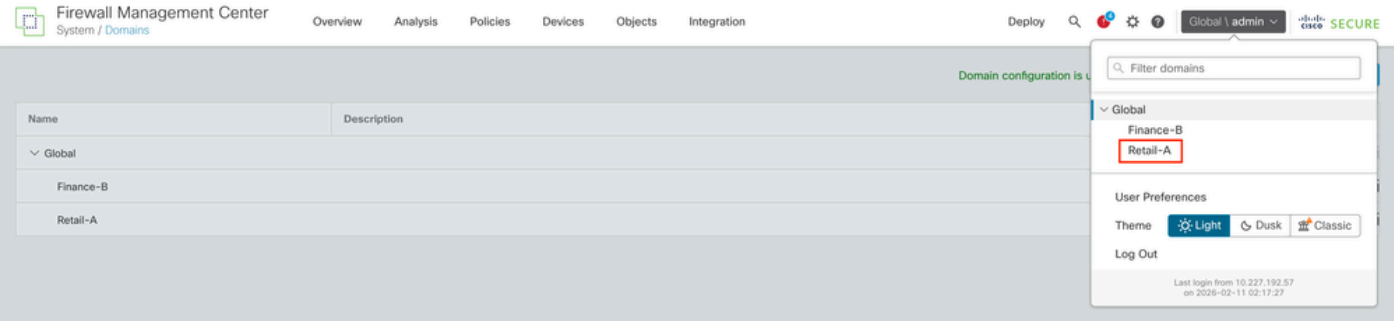
- Klik op Domein toevoegen om Retail-A en Finance-B te maken als subdomeinen van Global.

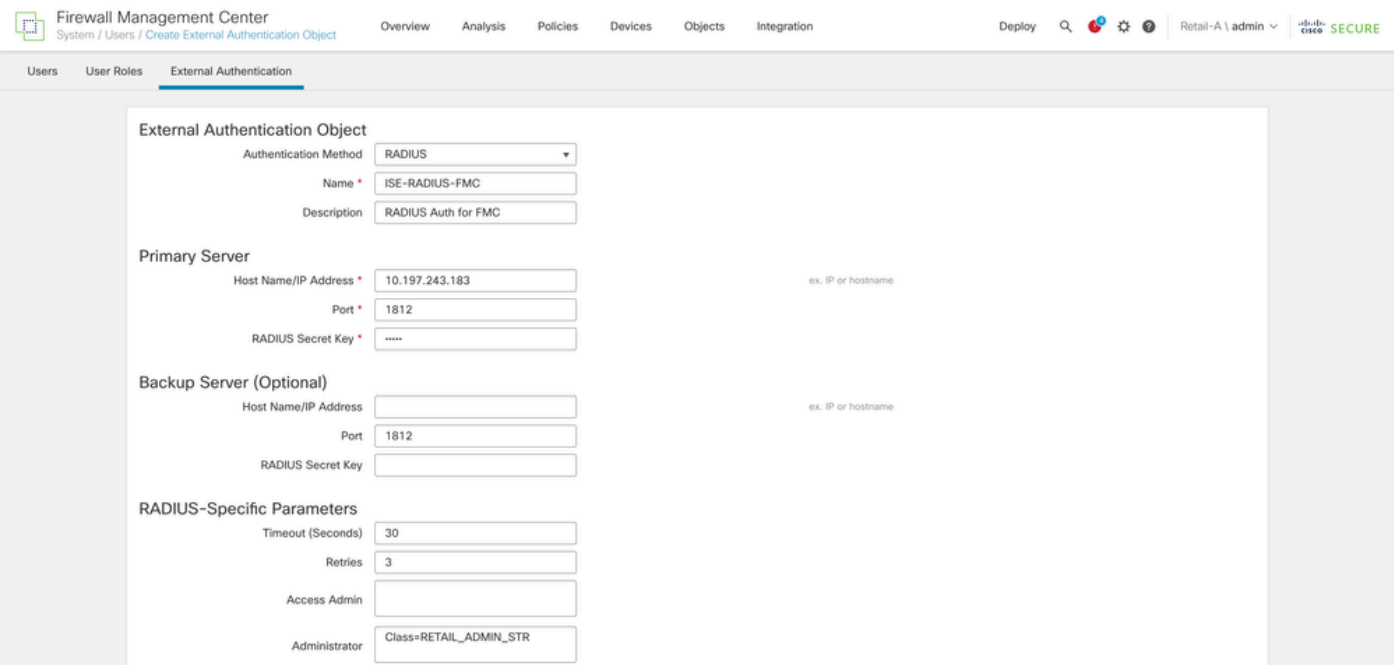


Stap 2.1. Het externe verificatieobject configureren onder Domain to Retail-A

- Switch Domain naar Retail-A.
- Ga naar Systeem > Gebruikers > Externe verificatie.
- Selecteer Extern verificatieobject toevoegen en kies RADIUS.
- Voer het ISE IP-adres in en het gedeelde geheim dat eerder is geconfigureerd.
- Voer de RADIUS-specifieke parameters in > Beheerder > class=RETAIL_ADMIN_STR

Tip: Gebruik dezelfde waarde voor klasse als geconfigureerd onder Autorisatieprofielen van ISE.

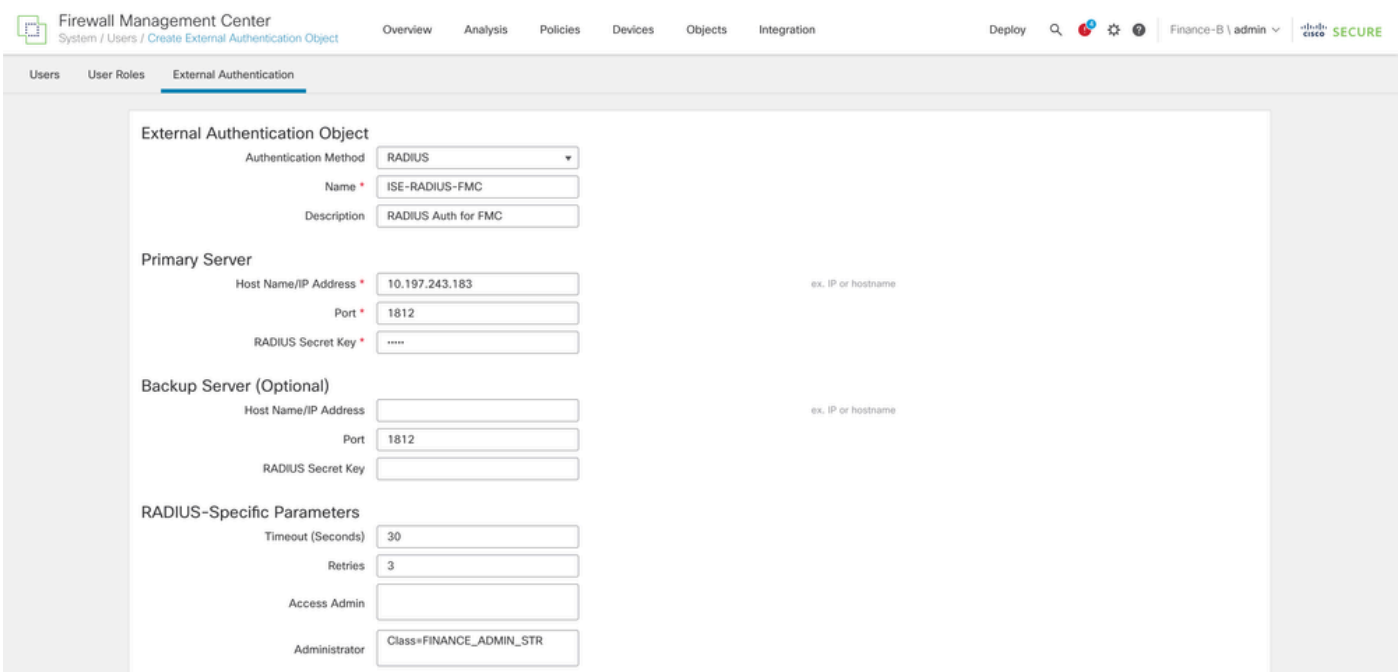




Stap 2.2. Configureer het externe verificatieobject onder Domain to Finance-B

- Switch Domein naar Finance-B.
- Ga naar Systeem > Gebruikers > Externe verificatie.
- Selecteer Extern verificatieobject toevoegen en kies RADIUS.
- Voer het ISE IP-adres in en het gedeelde geheim dat eerder is geconfigureerd.
- Voer de RADIUS-specifieke parameters in > Beheerder > class=FINANCE_ADMIN_STR

Tip: Gebruik dezelfde waarde voor klasse als geconfigureerd onder Autorisatieprofielen van ISE.



Stap 3. Verificatie activeren: Schakel het object in en stel het in als de Shell-verificatiemethode. Klik op Opslaan en Toepassen.

Verificatie

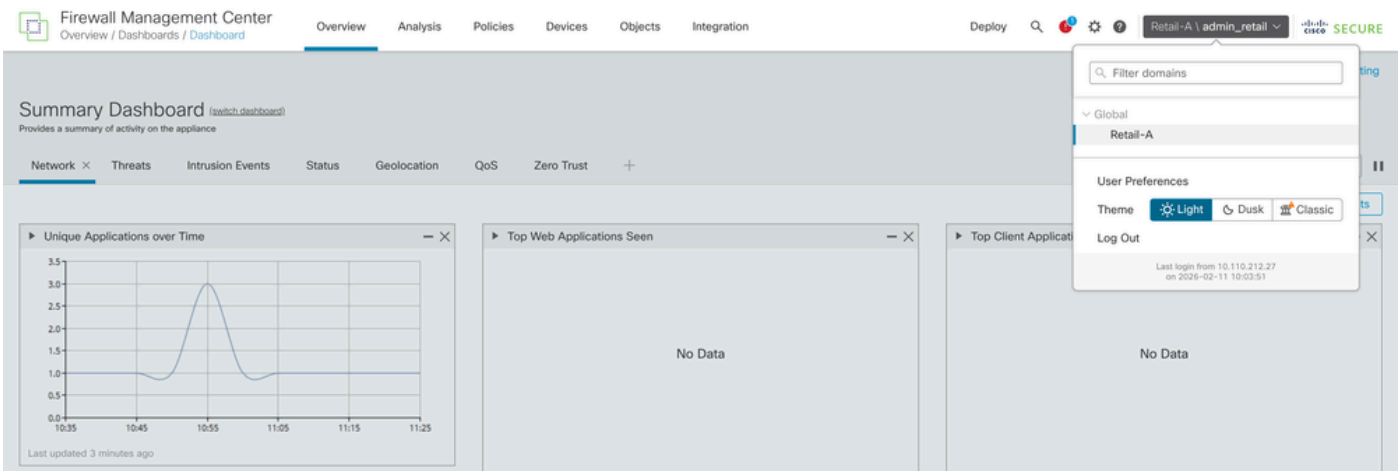
Inlogtest voor meerdere domeinen

- Probeer in te loggen op de FMC-webinterface met admin_retail. Controleer of het huidige

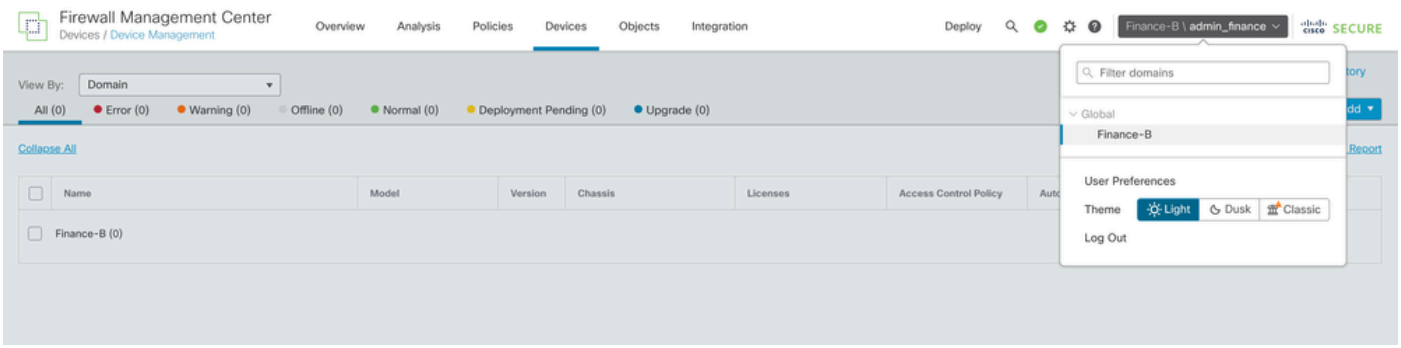
domein rechtsboven in de gebruikersinterface Retail-A is.

Tip: Wanneer u zich aanmeldt bij een specifiek domein, gebruikt u de gebruikersnaam format domain_name\radius_user_mapped_with_that_domain.

Als de gebruiker van de Retail-beheerder bijvoorbeeld moet inloggen, moet de gebruikersnaam Retail-A\admin_retail en het bijbehorende wachtwoord zijn.



- Log uit en log in als admin_finance. Controleer of de gebruiker beperkt is tot het Finance-B-domein en geen Retail-A-apparaten kan zien.

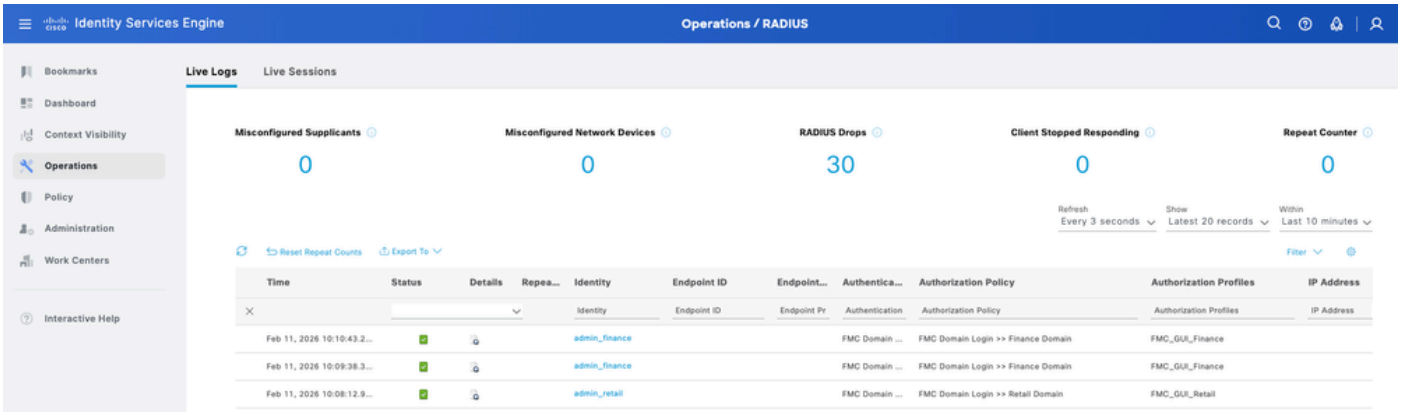


Interne FMC-tests

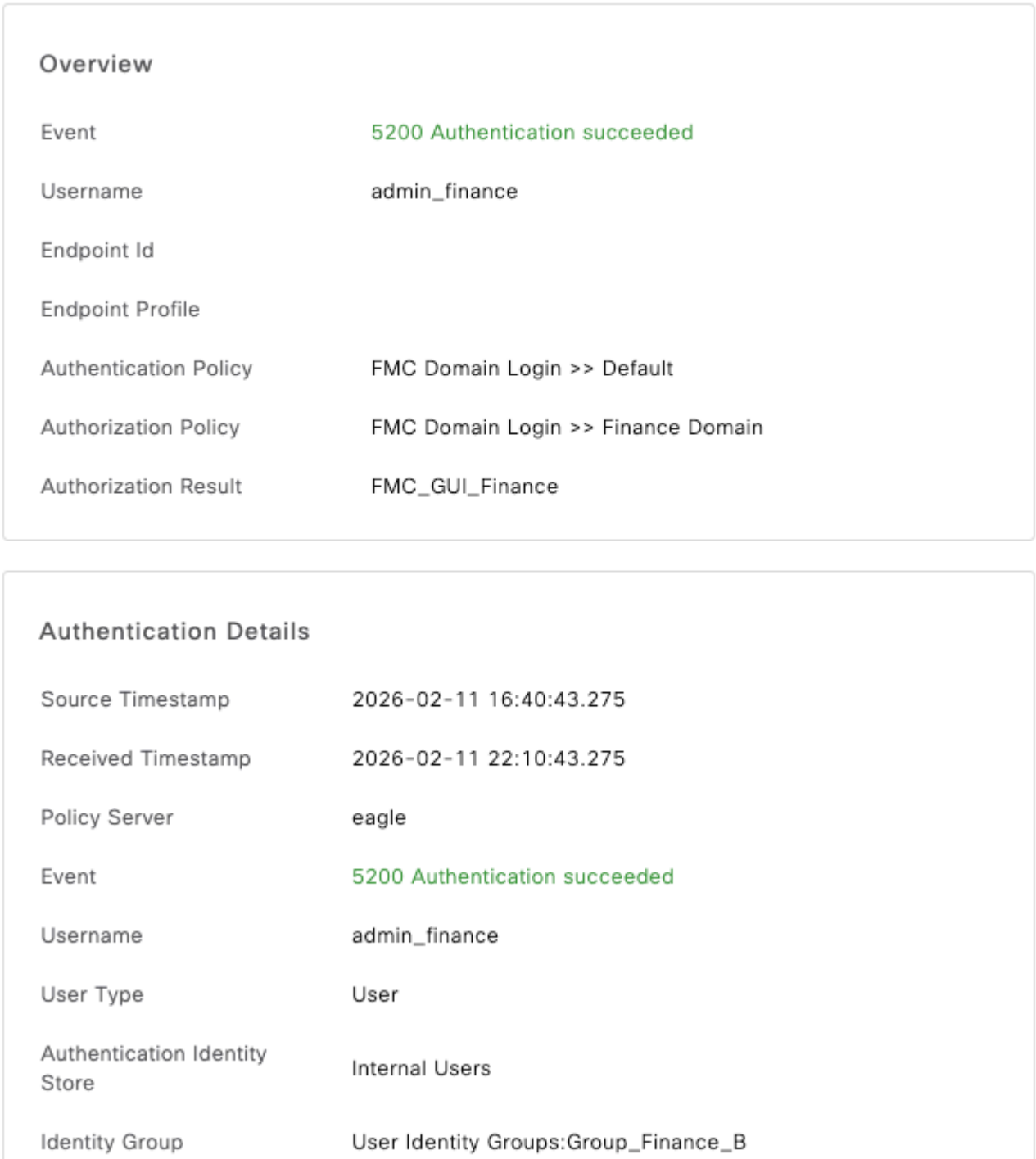
Ga naar de RADIUS-serverinstellingen in de FMC. Gebruik de sectie Extra testparameters om een gebruikersnaam en wachtwoord voor de test in te voeren. Een succesvolle test moet een groene succesboodschap tonen.

ISE Live Logs

- Navigeer in Cisco ISE naar Operations > RADIUS > Live Logs.



- Bevestig dat de verificatieverzoeken een Pass-status weergeven en dat het juiste autorisatieprofiel (en de bijbehorende Class-tekenreeks) is verzonden in het RADIUS Access-Accept-pakket.


Overview

Event	5200 Authentication succeeded
Username	admin_finance
Endpoint Id	
Endpoint Profile	
Authentication Policy	FMC Domain Login >> Default
Authorization Policy	FMC Domain Login >> Finance Domain
Authorization Result	FMC_GUI_Finance

Authentication Details

Source Timestamp	2026-02-11 16:40:43.275
Received Timestamp	2026-02-11 22:10:43.275
Policy Server	eagle
Event	5200 Authentication succeeded
Username	admin_finance
User Type	User
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Group_Finance_B

Result

Class	FINANCE_ADMIN_STR
Class	CACS:0ac5f3b7m0vFomvHHyC_igO13NsO1DZN6QciDbrc0cwlaYWHMto:eagle/556377151/553

Gerelateerde informatie

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

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.