De passieve identiteitsagent configureren met FMC

Inhoud

Inleiding

In dit document wordt beschreven hoe u de bron van de passieve identiteitsagent kunt configureren die sessiegegevens naar de FMC verzendt

Voorwaarden

Vereisten

- Cisco Secure Firewall Management Center met versie 7.6+
- Cisco Secure Firewall met versie 7.6+
- Windows Active Directory-server, de server moet Windows Server 2008 of hoger uitvoeren.
- U moet Snort 3 inschakelen op de apparaten van Secure Firewall Threat Defense.

Gebruikte componenten

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

- Cisco Secure Firewall Management Center 7.6.5
- Cisco Secure Firewall 7.6.5
- Microsoft Active Directory met Windows Server 2022.

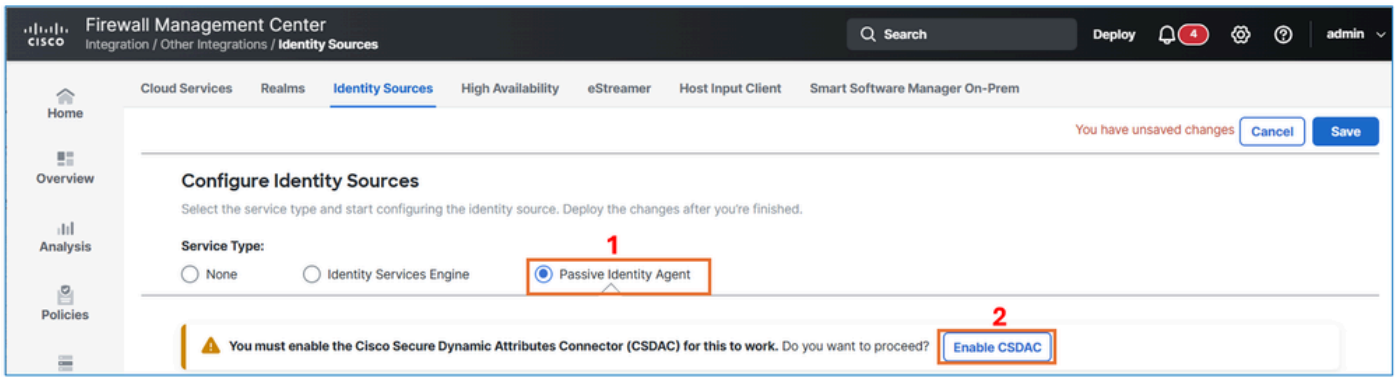
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuraties

Voordat u de agent configureert, moet u eerst de AD- en FMC-integratie voltooien.

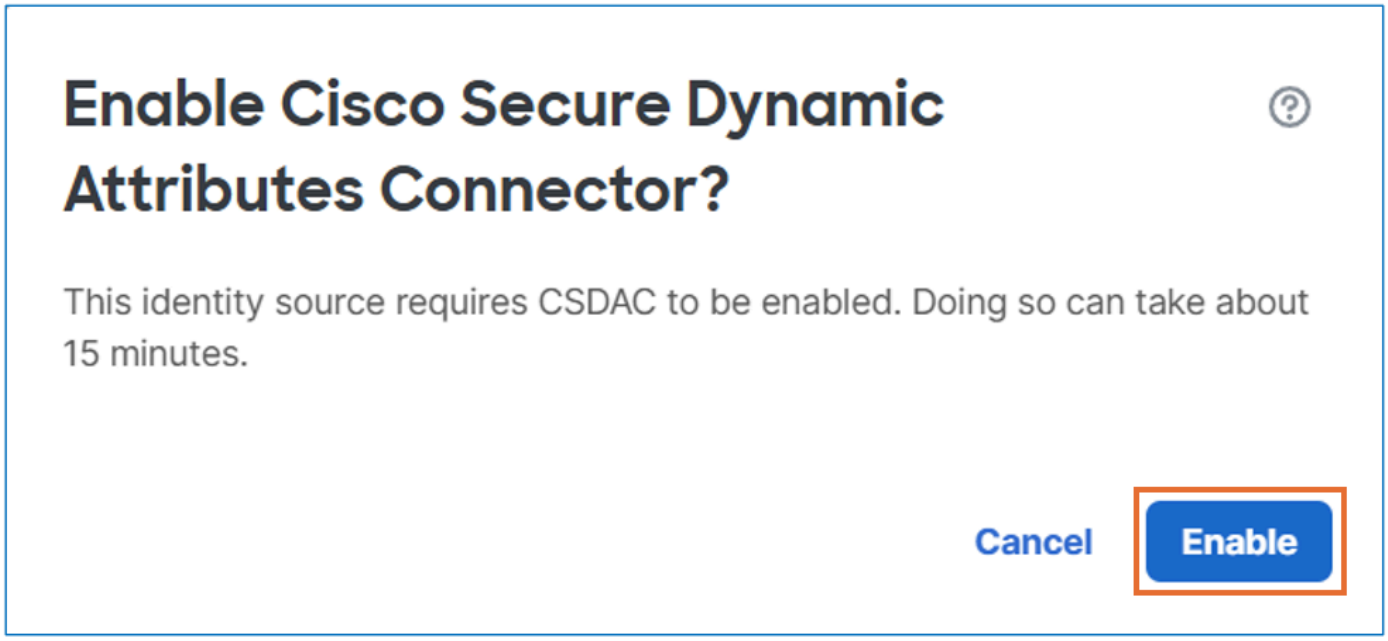
Een bron voor een passieve identiteitsagent configureren

Navigeer in de FMC UI naar Integratie > Andere integraties > Identiteitsbronnen, klik op Passieve Identiteitsagent. Als de Cisco Secure Dynamic Attributes Connector nog niet is ingeschakeld, wordt u gevraagd dit te doen door op CSDAC inschakelen te klikken.



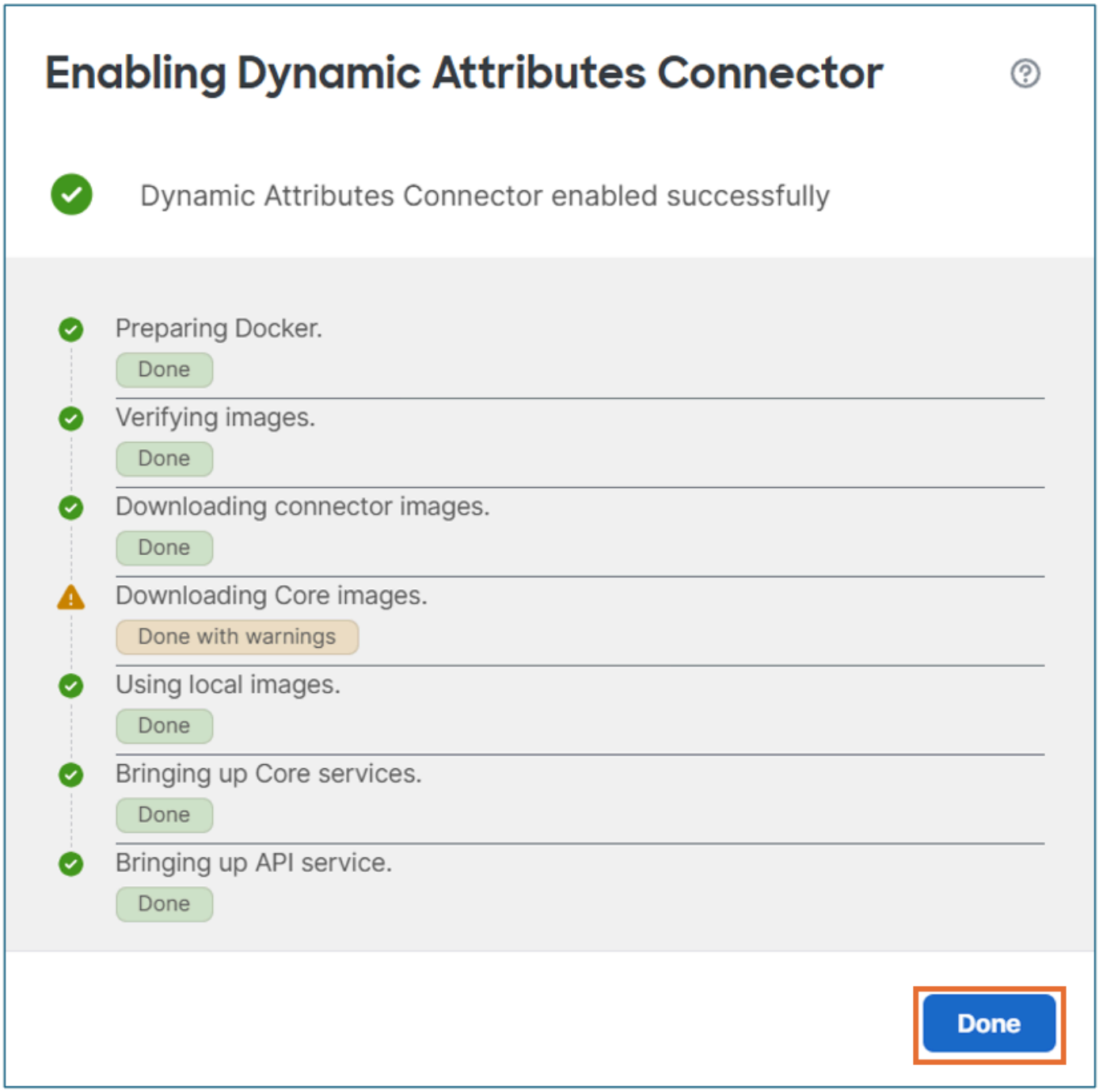
passieve identiteitsagent

Klik op de knop Inschakelen om de CSDAC in te schakelen.



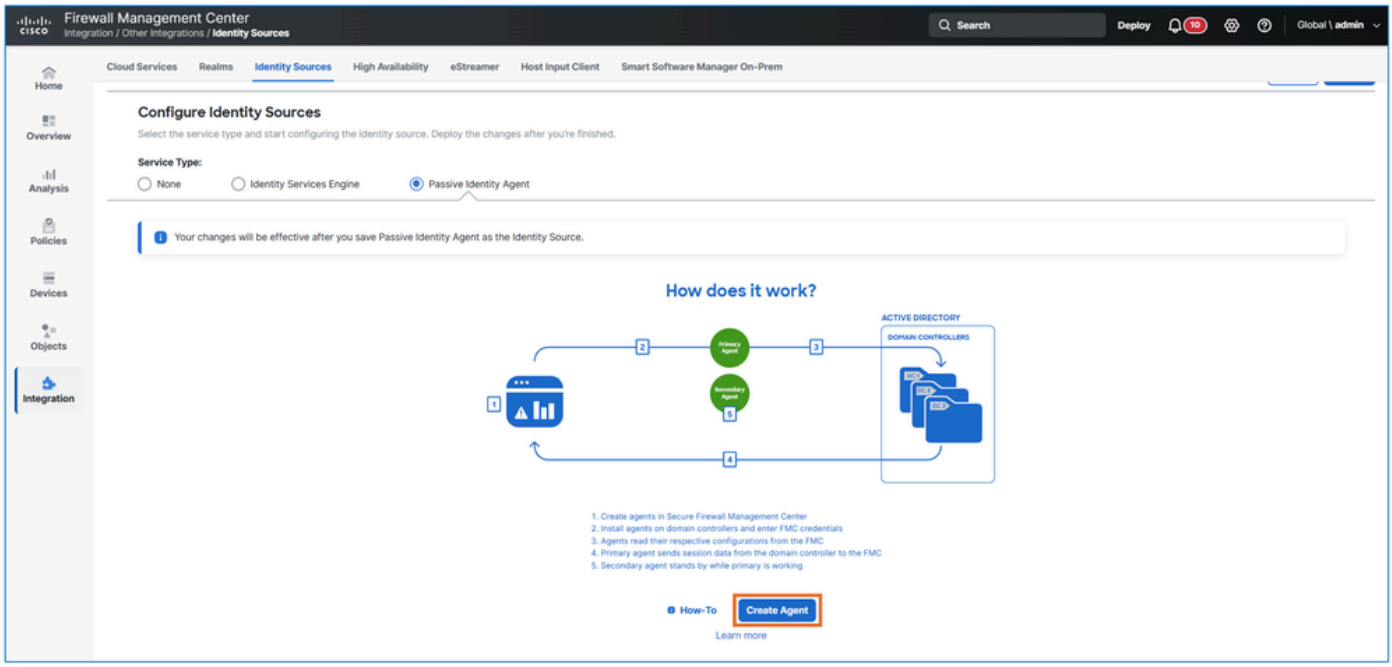
CSDAC inschakelen

Deze stap duurt ongeveer 10 minuten. Zodra de CSDAC correct is ingeschakeld, klikt u op de knop Doneom verder te gaan.



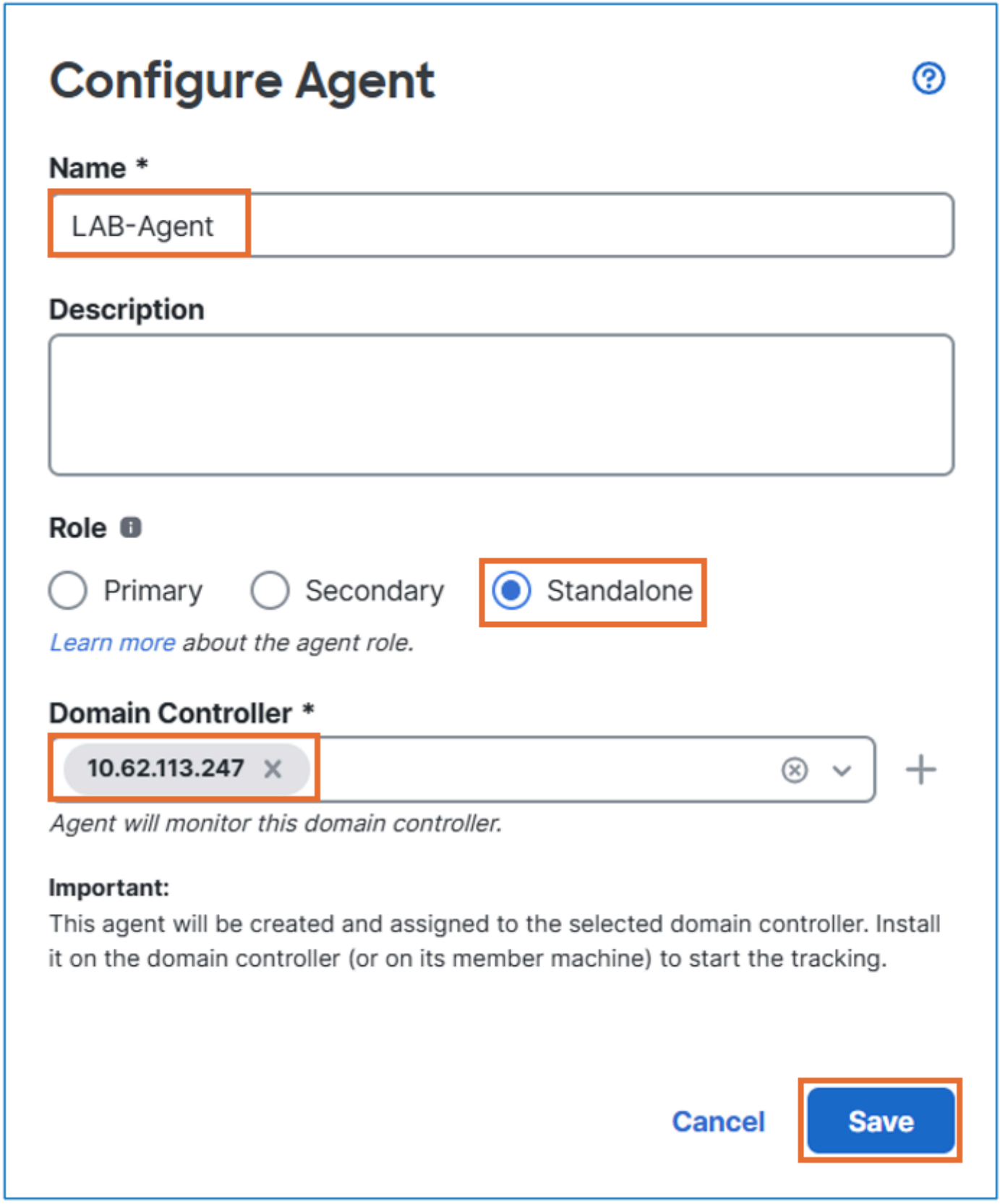
CSDAC ingeschakeld

Klik op de knop Agent maken.



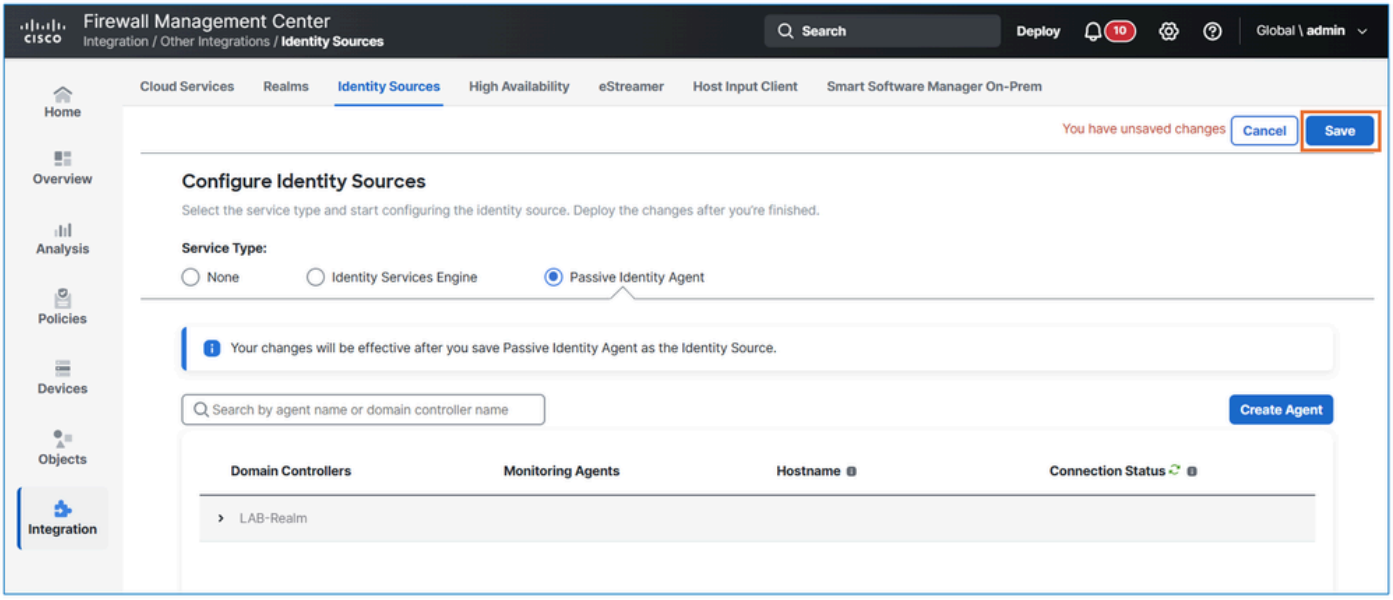
Agent maken

Definieer een naam voor de agent, selecteer de optie Standalone en koppel deze aan de juiste domeincontroller die in de vorige taak is gemaakt.



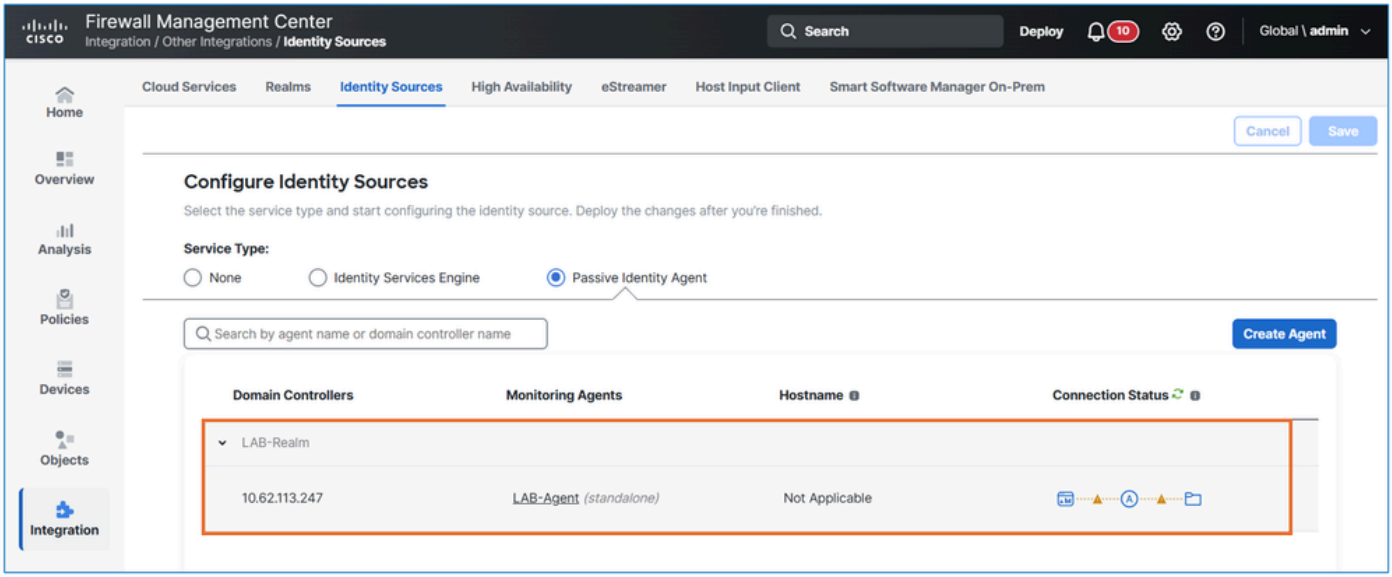
Agent configureren

Klik op de knop Opslaan.



Sla de configuratie op

Het resultaat.



Controleer de status

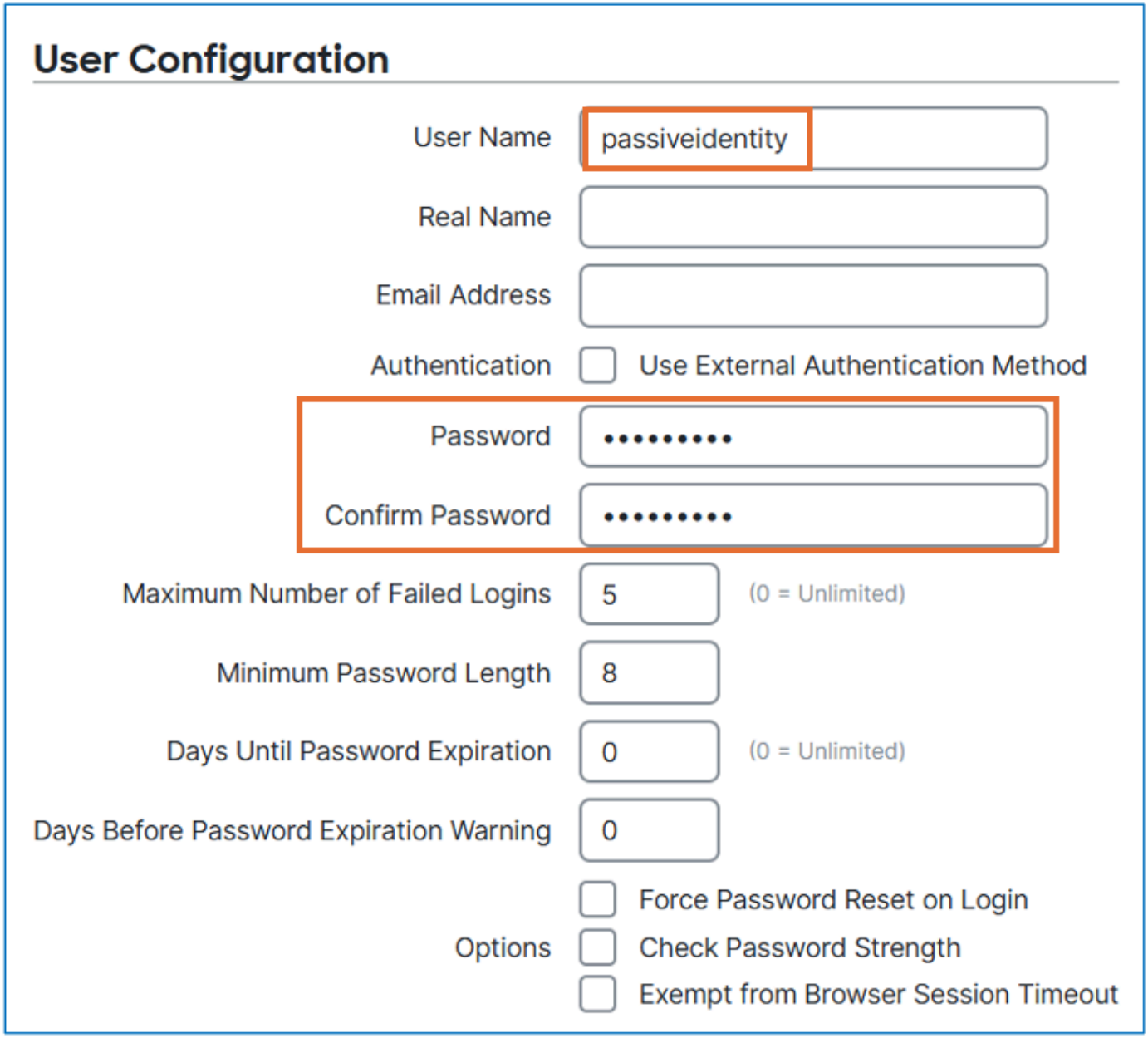
Opmerking: de passieve-identiteitsagent geeft de status aan met behulp van lijnen. Amber betekent dat de agent nooit met succes heeft gecommuniceerd met het Secure Firewall Management Center. Een nieuw gemaakte agentlijn is amberkleurig en blijft dit totdat de configuratie is voltooid.

Een gebruiker van een Passive Identity Agent maken in het Secure Firewall

Management Center

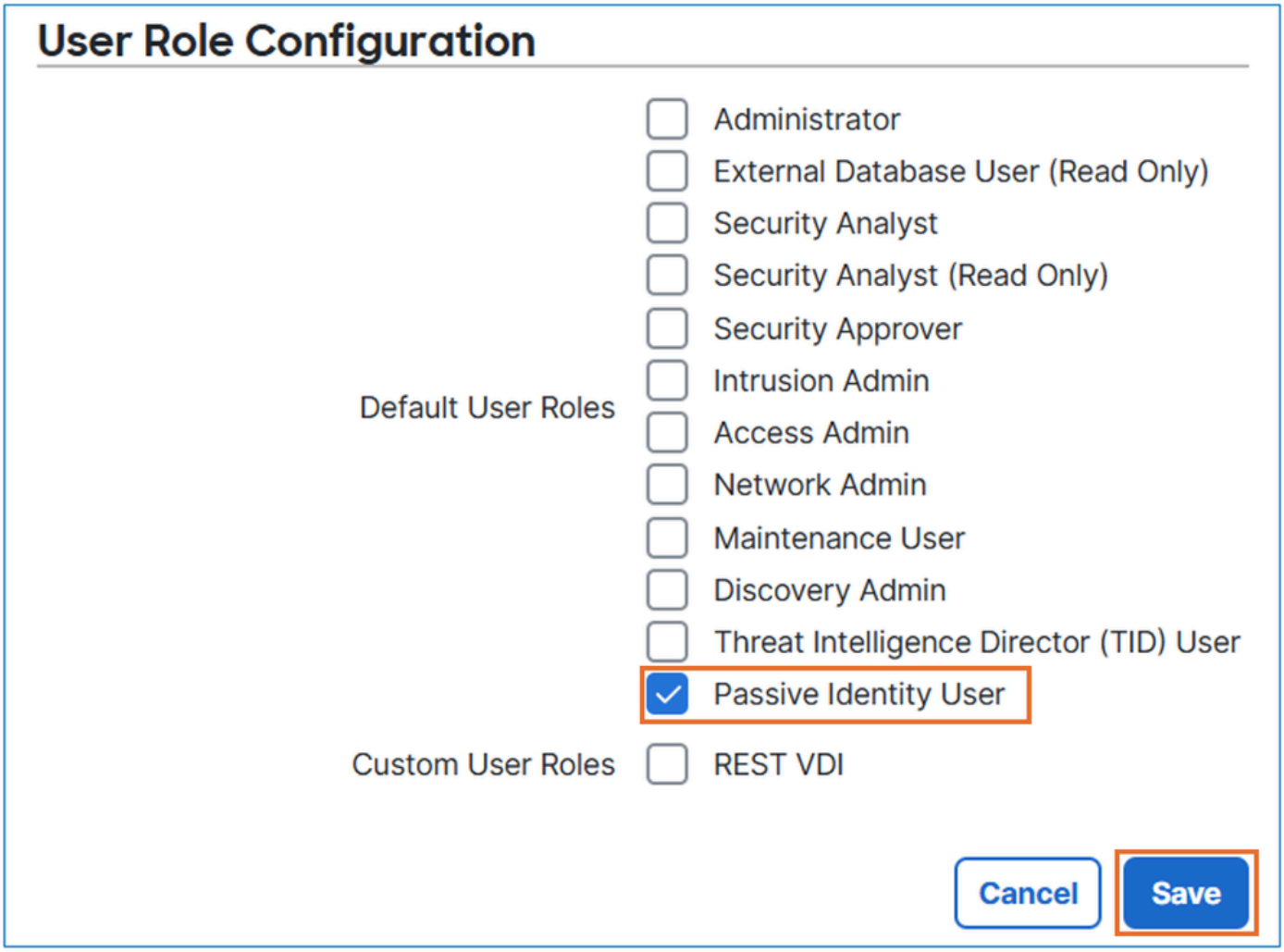
Maak een Secure Firewall Management Center-gebruiker met voldoende machtigingen om te communiceren met de passieve identiteitsagent. Deze gebruiker heeft beperkte bevoegdheden om andere taken uit te voeren; van de gebruiker wordt alleen verwacht dat hij communicatie met de passieve identiteitsagent mogelijk maakt.

Navigeer in de FMC UI naar Systeem > Gebruikers en klik op Gebruiker maken. Vul de gebruikersgegevens in volgens de taakvereisten.



Gebruiker maken

Wijs alleen de gebruikersrol Passieve identiteit toe. Klik op de knop Opslaan.

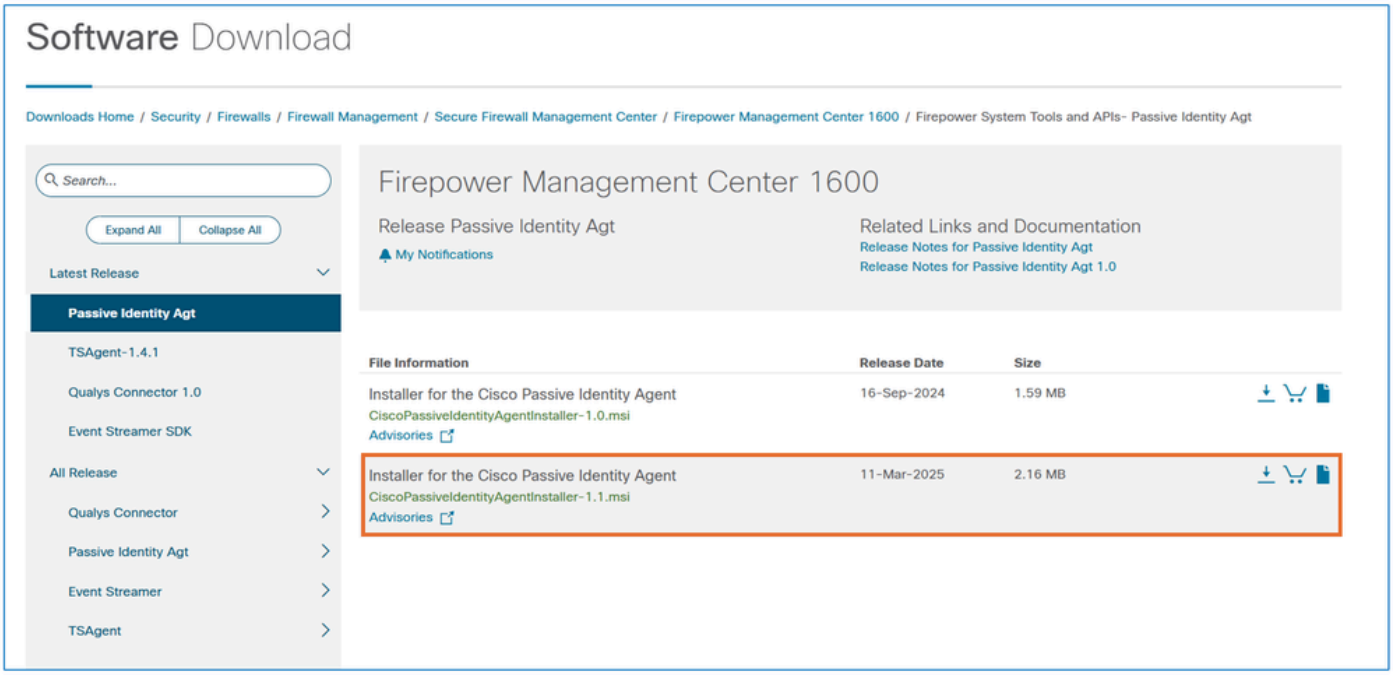


Selecteer de passieve identiteit van de gebruiker

De software van de Passive Identity Agent installeren en configureren

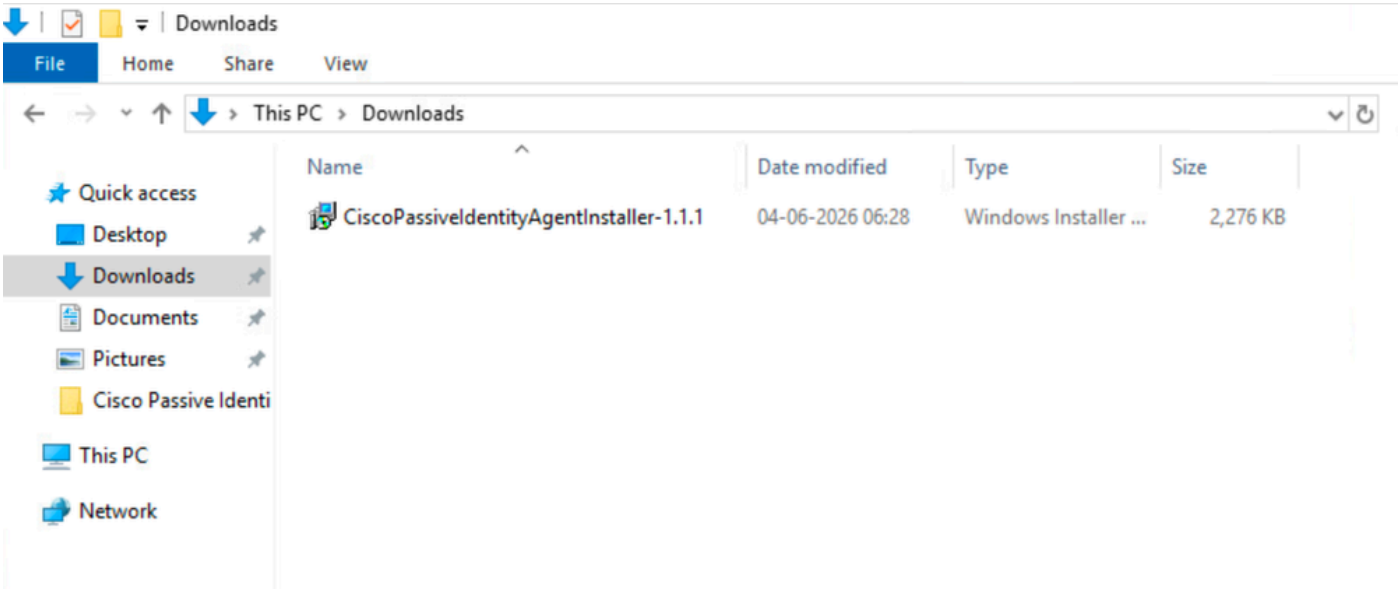
Installeer en configureer de Passive Identity Agent-software op de aangewezen domeincontroller.

Download de passieve identiteitsagent van software.cisco.com.



Download de software

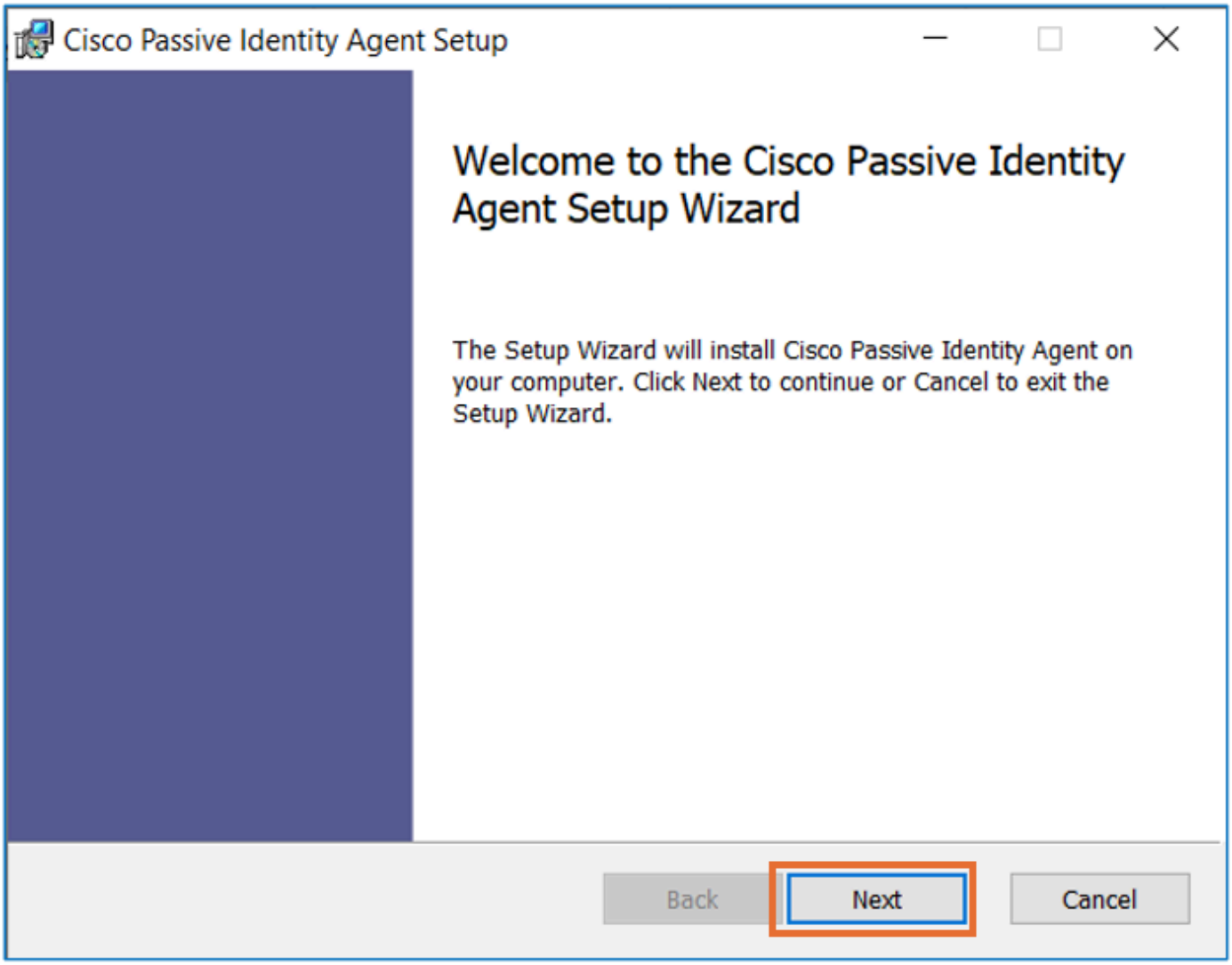
Nadat u de agent hebt gedownload, begint u met het installatie-proces op de domeincontroller.



agent

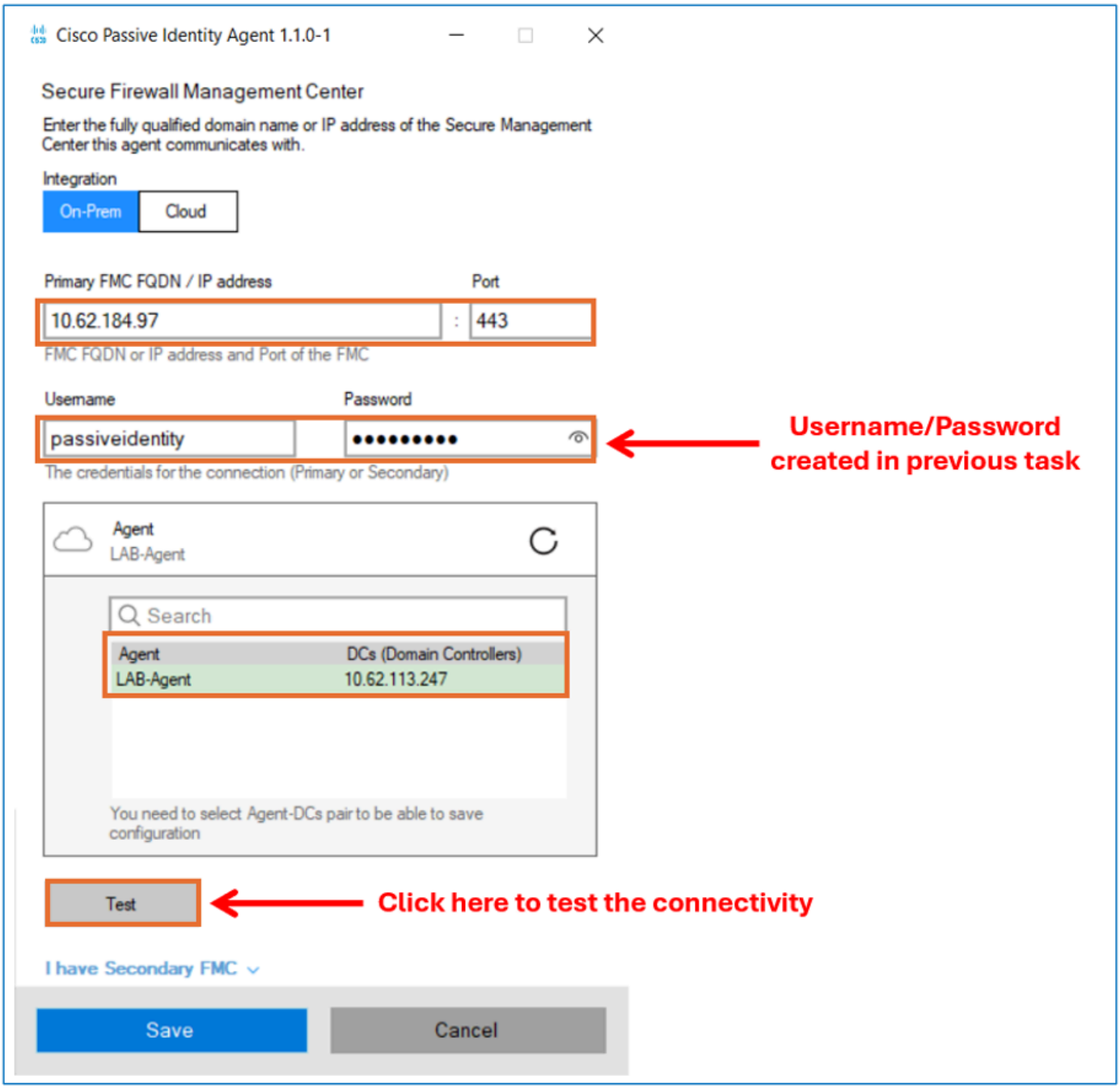
]

Raadpleeg de meegeleverde installatie-instructies om de installatie te voltooien.



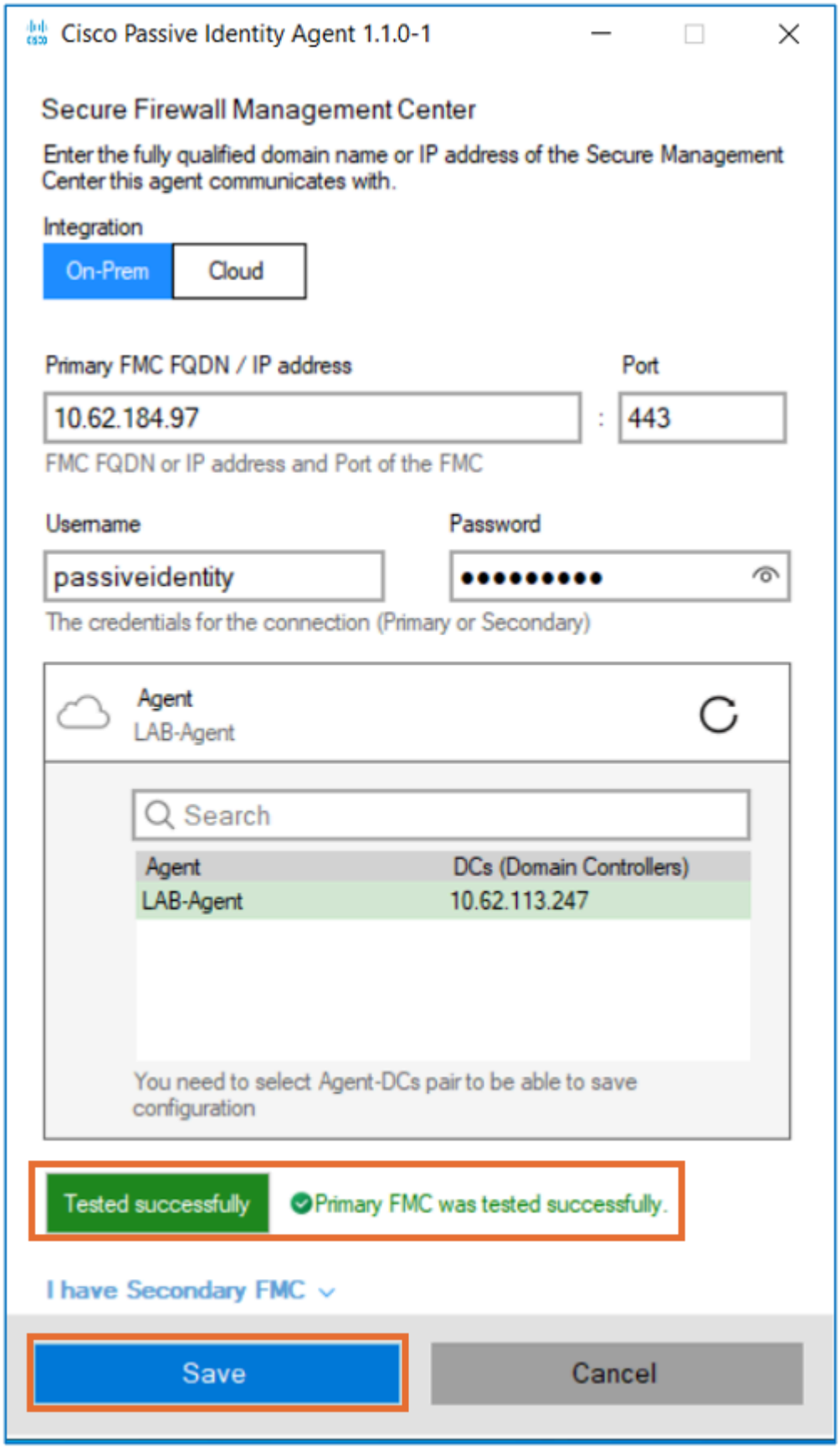
Installeren

Zodra de installatie is voltooid, opent u de Passive Identity Agent-software en voert u de vereiste informatie in zoals gespecificeerd in de taakvereisten. Klik op de knop Test om de connectiviteit met de FMC te controleren.



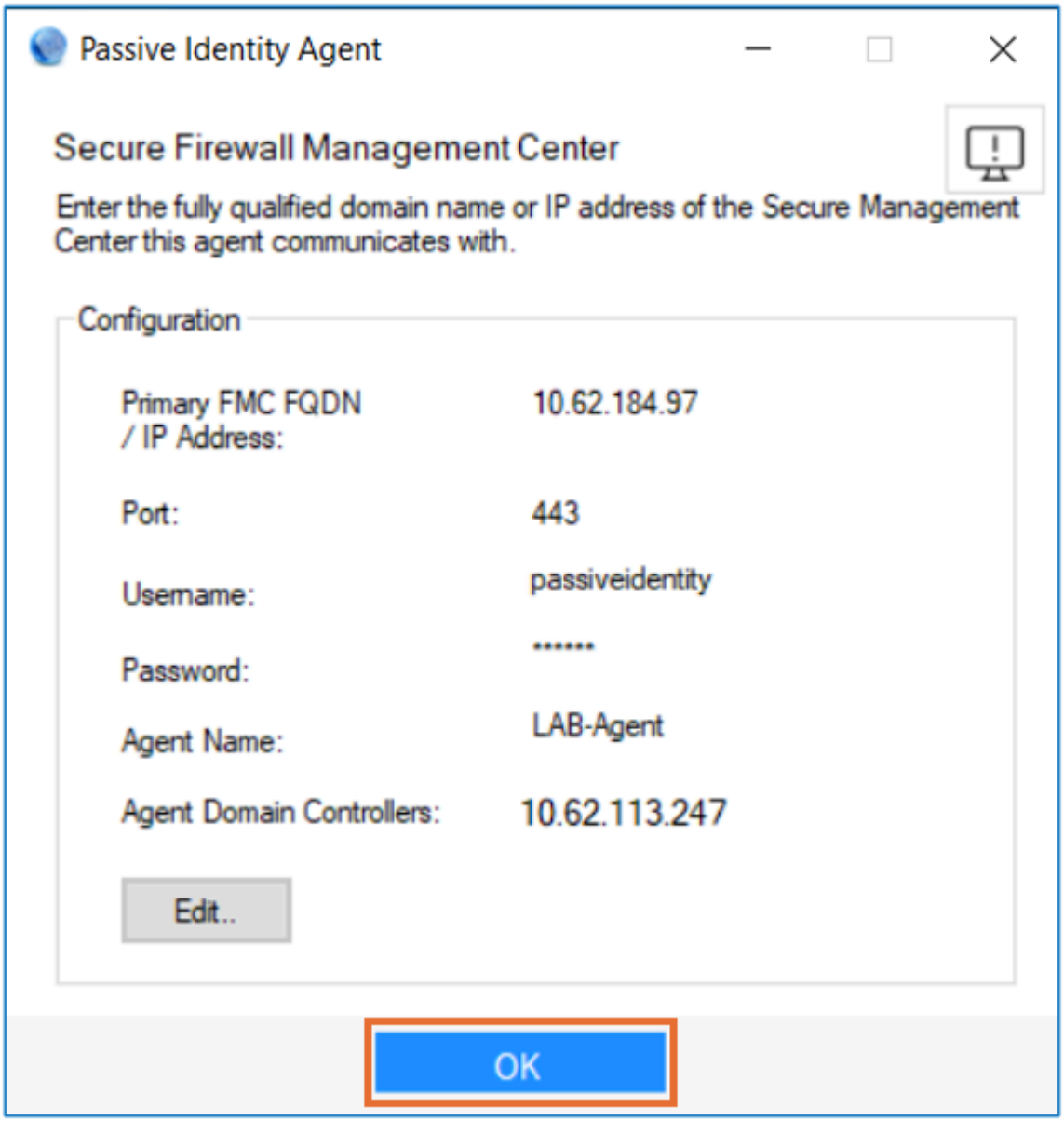
De agent configureren.

Nadat u de connectiviteit hebt getest, klikt u op de knop Opslaan.



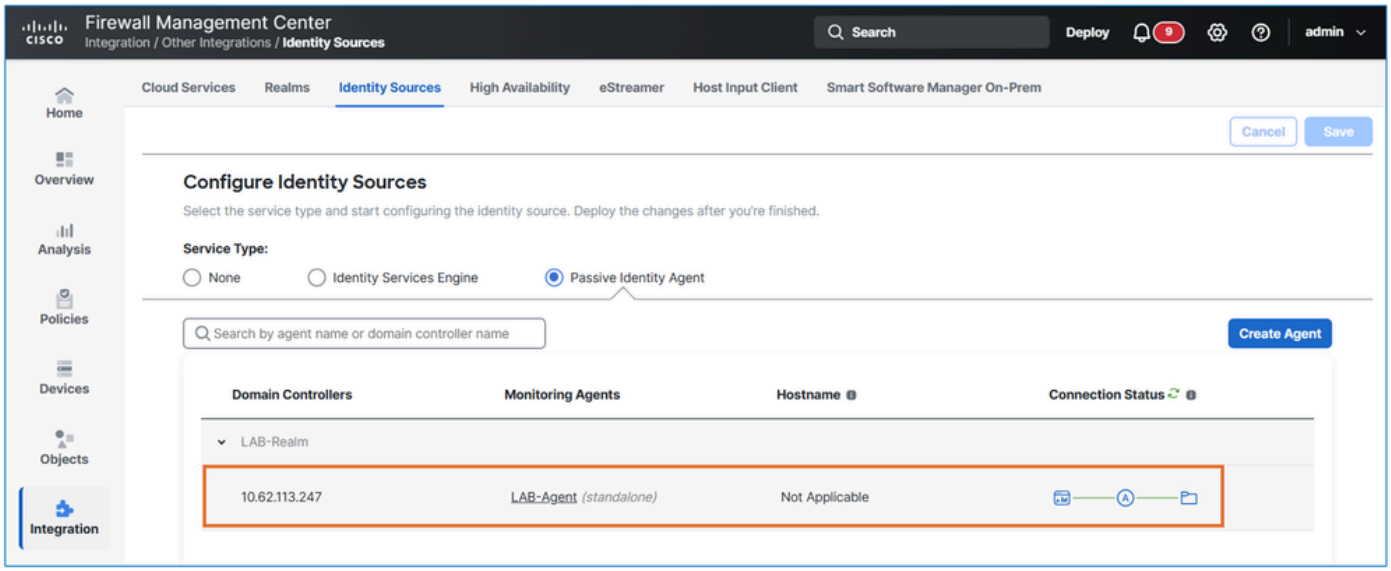
test

Klik op de knop OK om de agentconfiguratie te voltooien.



Agent wordt uitgevoerd

Navigeer in de FMC UI naar Integratie > Andere integraties > Identiteitsbronnen > Passieve identiteitsagent. Bevestig dat de Passive Identity Agent een groene status weergeeft.



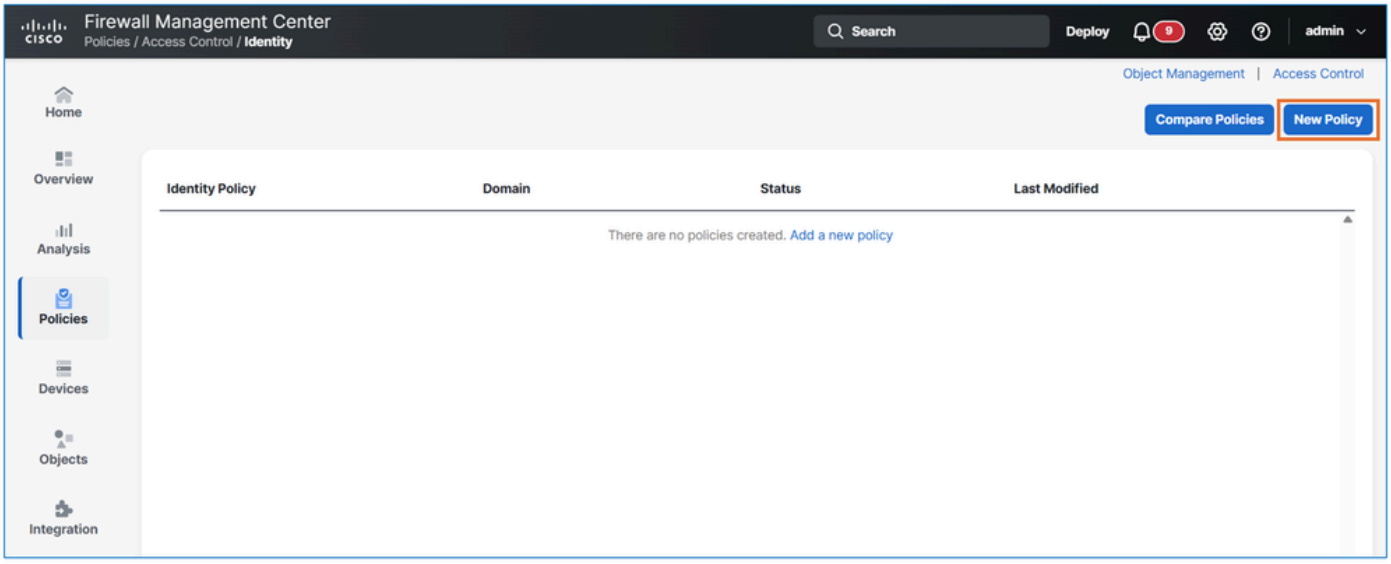
Controleer de communicatie van FMC

Identiteitsbeleid configureren

Maak een identiteitsbeleid op basis van de verstrekte tabel.

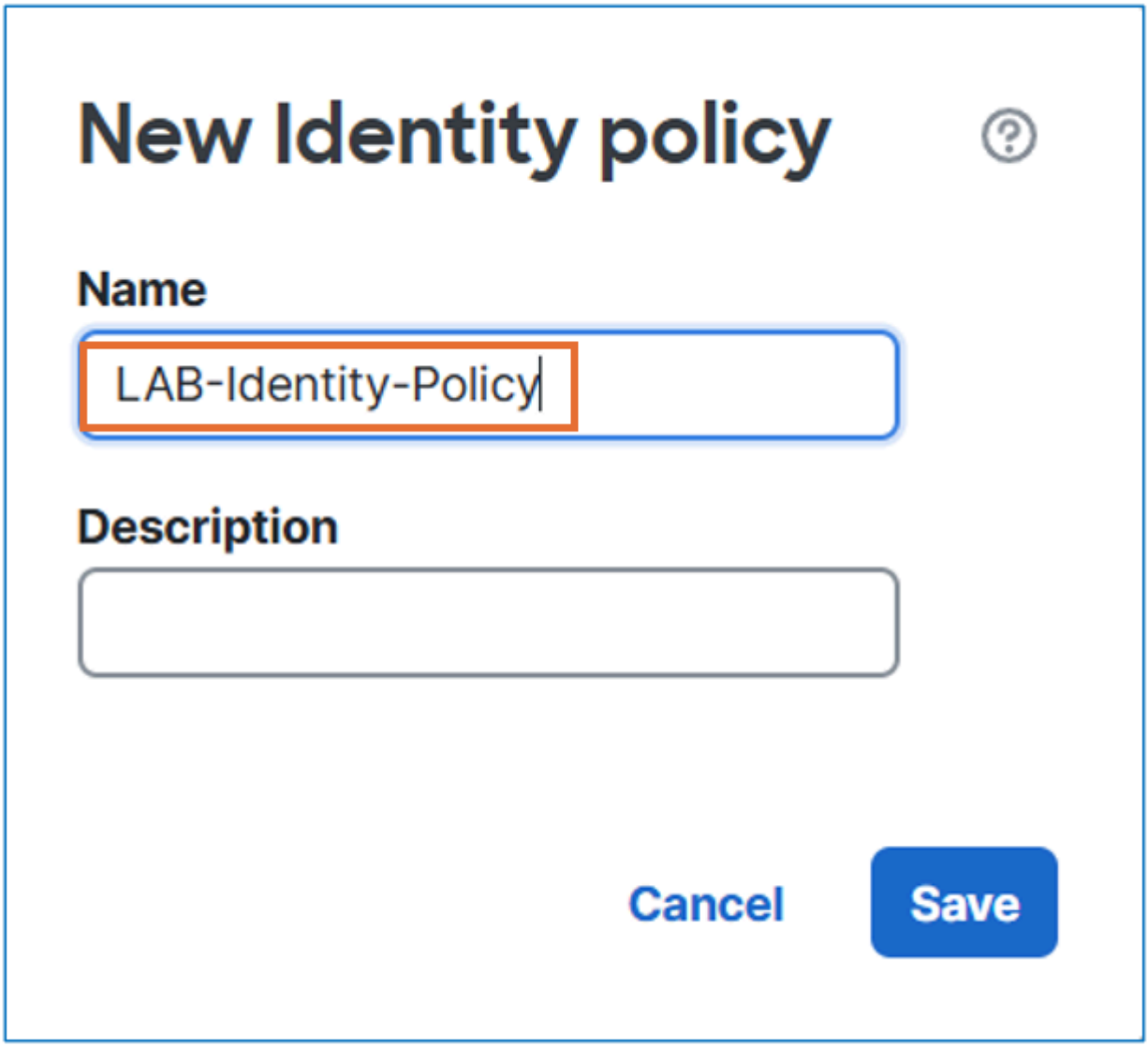
Naam beleid	Naam regel	verificatiereeks	Resterende instellingen
LAB-Identity-Policy	Regel1	LAB-Rijk	Als standaard opgeven

Navigeer in de FMC UI naar Beleid > Toegangscontrole > Identiteit. Klik op de knop Nieuw beleid.



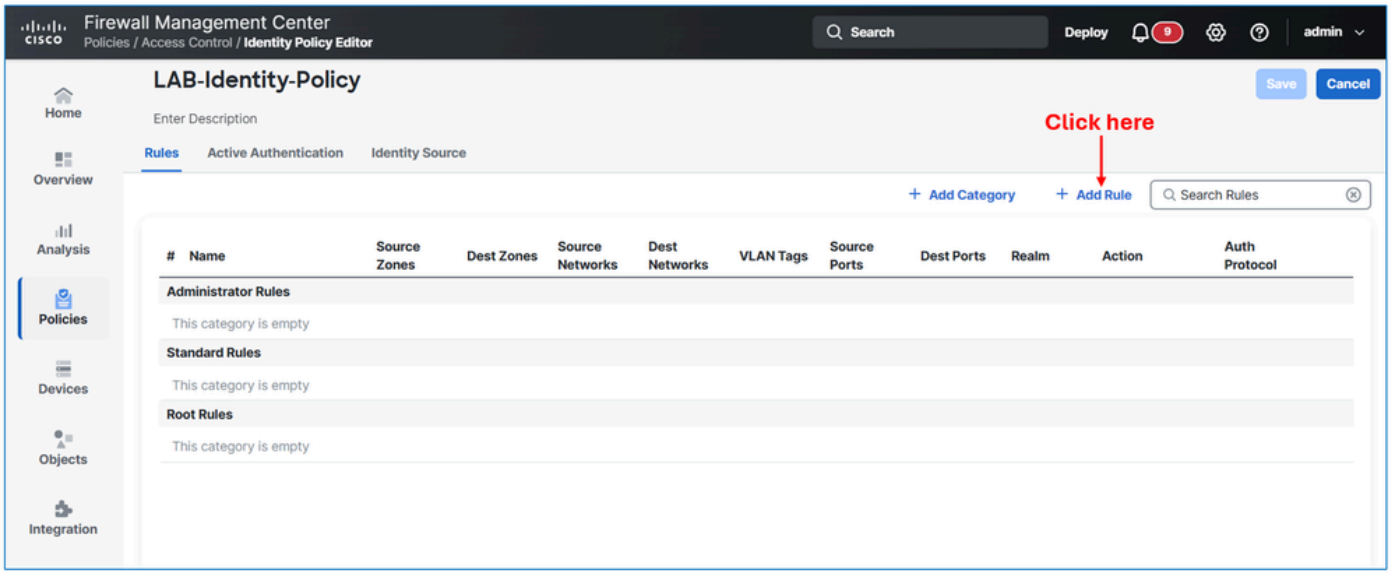
nieuw beleid

Voer de naam van het beleid in volgens de taakvereisten.



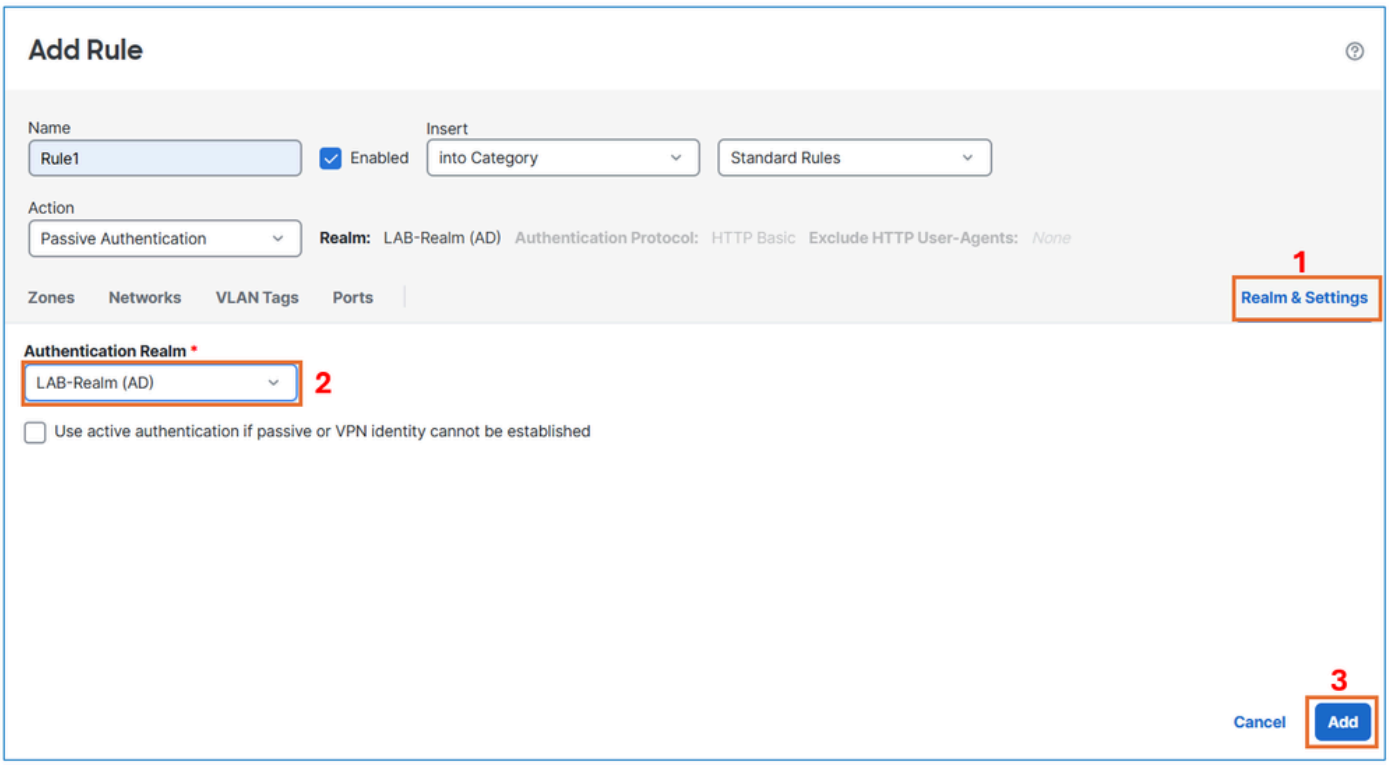
nieuw beleid

Klik op de knop Regels toevoegen.



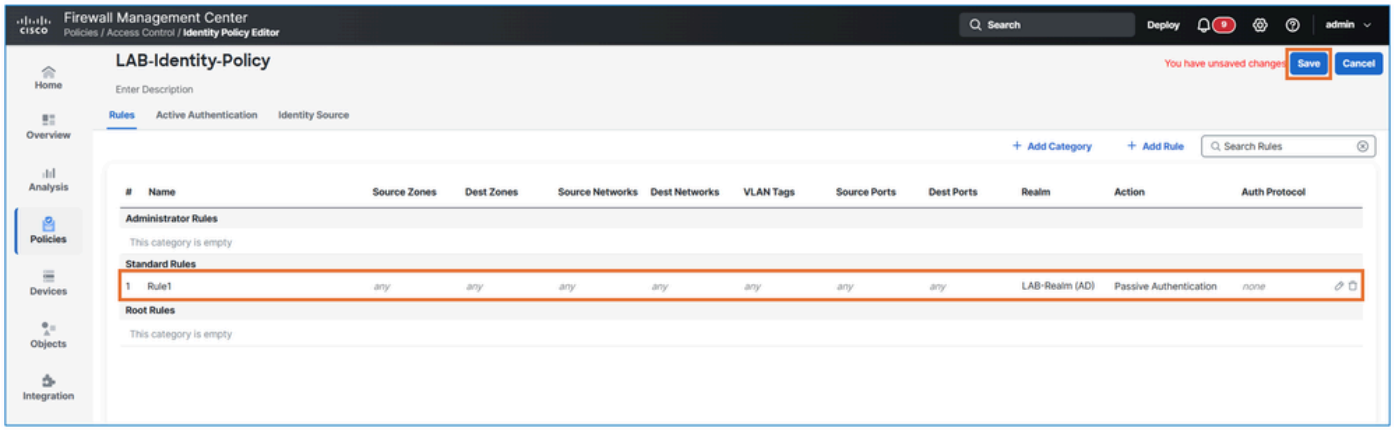
Regel maken

Navigeer naar de Realm & Settingstab en selecteer de Authentication Realm op basis van de taakvereisten. Klik ten slotte op de knop Toevoegen.



Realm instellen

Klik op de knop Opslaan.



Sla de configuratie op

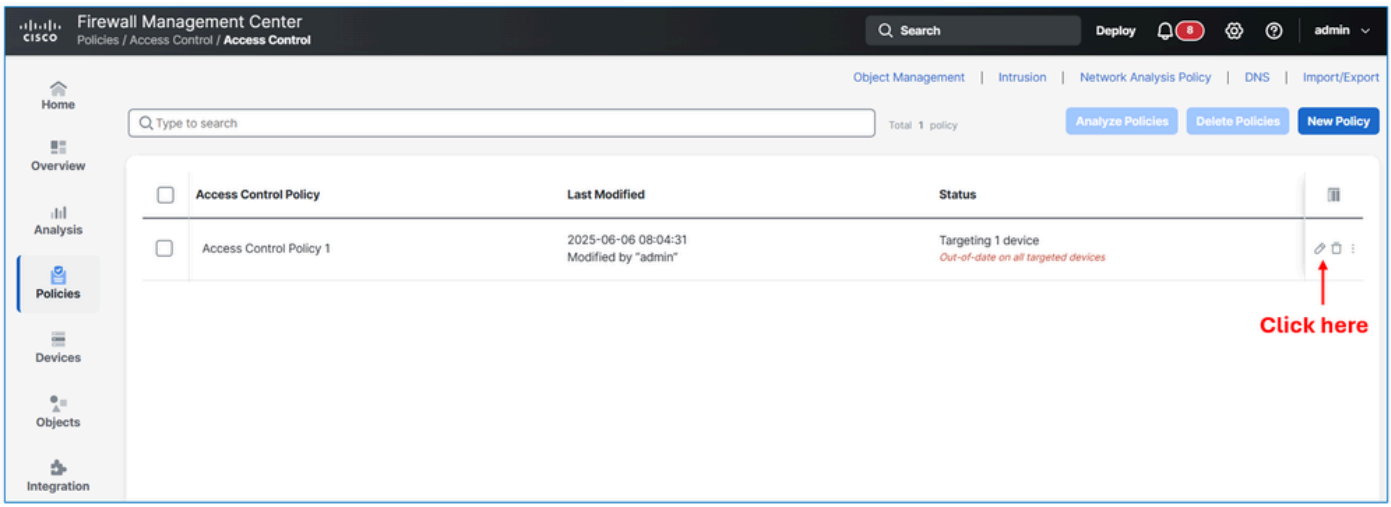
Beleid voor toegangscontrole configureren

Koppel het identiteitsbeleid aan het toegangscontrolebeleid en maak een regel voor het toegangsbeleid met de volgende kenmerken:

Attribuutnaam	Waarde
Naam regel	Regel1
Actie	Allow (toestaan)
bronzone	binnenzijde
bestemmingszone	buiten
Bronnetwerken	10.10.10.0/24
bestemmingsnetwerken	10.48.62.98/32
dienst	Dest-poort TCP 80 (HTTP)
Gebruikers	LAB-Realm/GROUP1
Logboekregistratie	Aan het einde van de verbinding

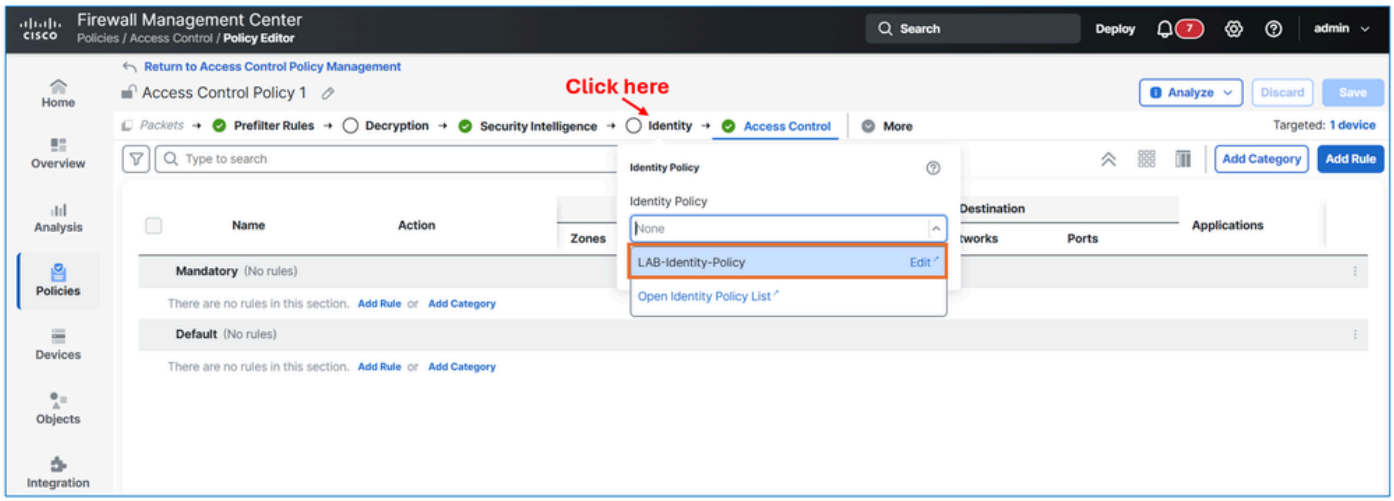
Stap 1. Koppel het identiteitsbeleid aan het toegangscontrole beleid van

Navigeer in de FMC UI naar Beleid > Toegangscontrole > Toegangscontrole. Klik op de knop Bewerken voor uw beleid.



Beleid bewerken

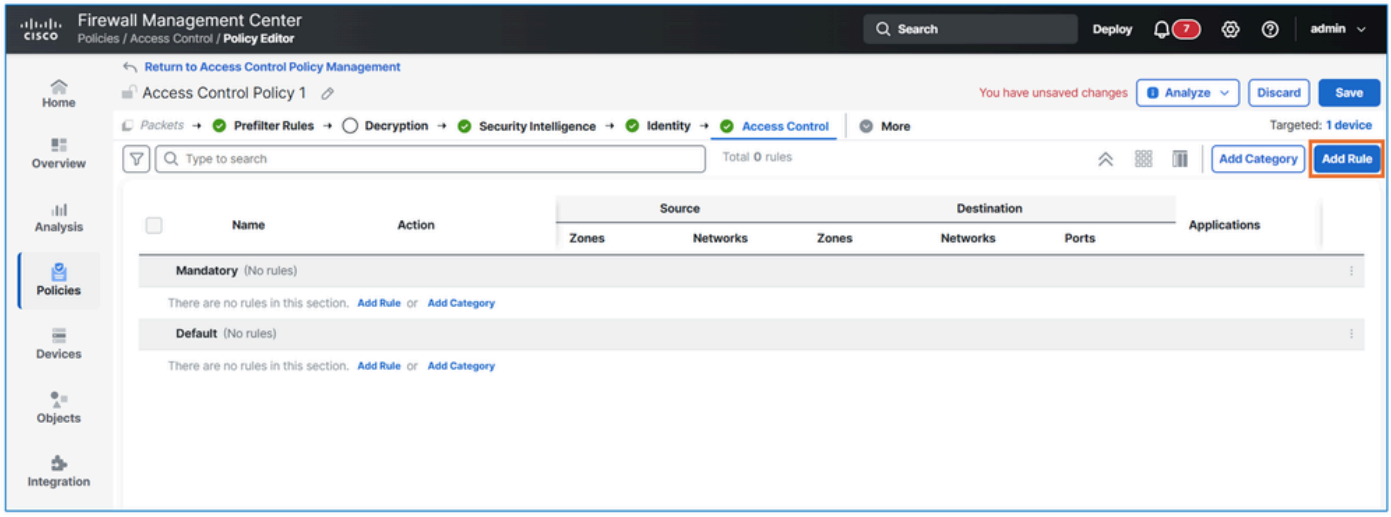
Navigeer naar het gedeelte Identiteit en koppel het Identiteitsbeleid dat in de vorige taak is gemaakt.



Identiteitsbeleid toevoegen

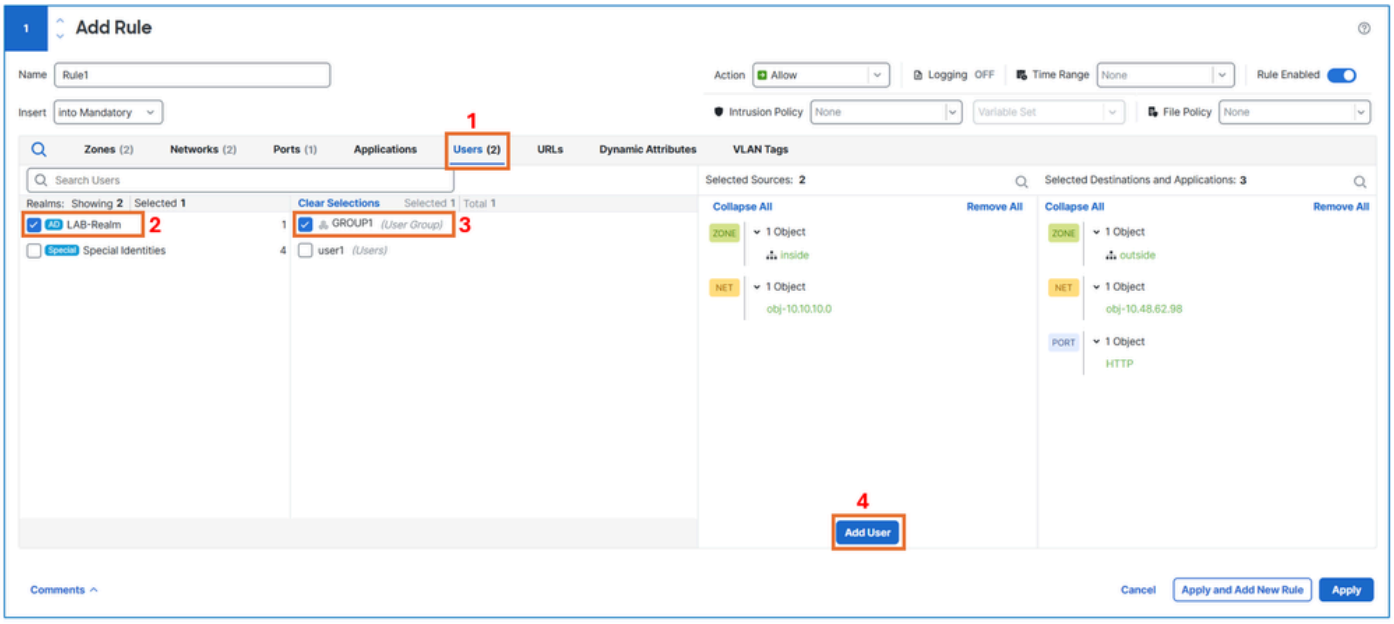
Klik op de knop Toepassen

Stap 2. Maak de regel voor toegangscontrole.



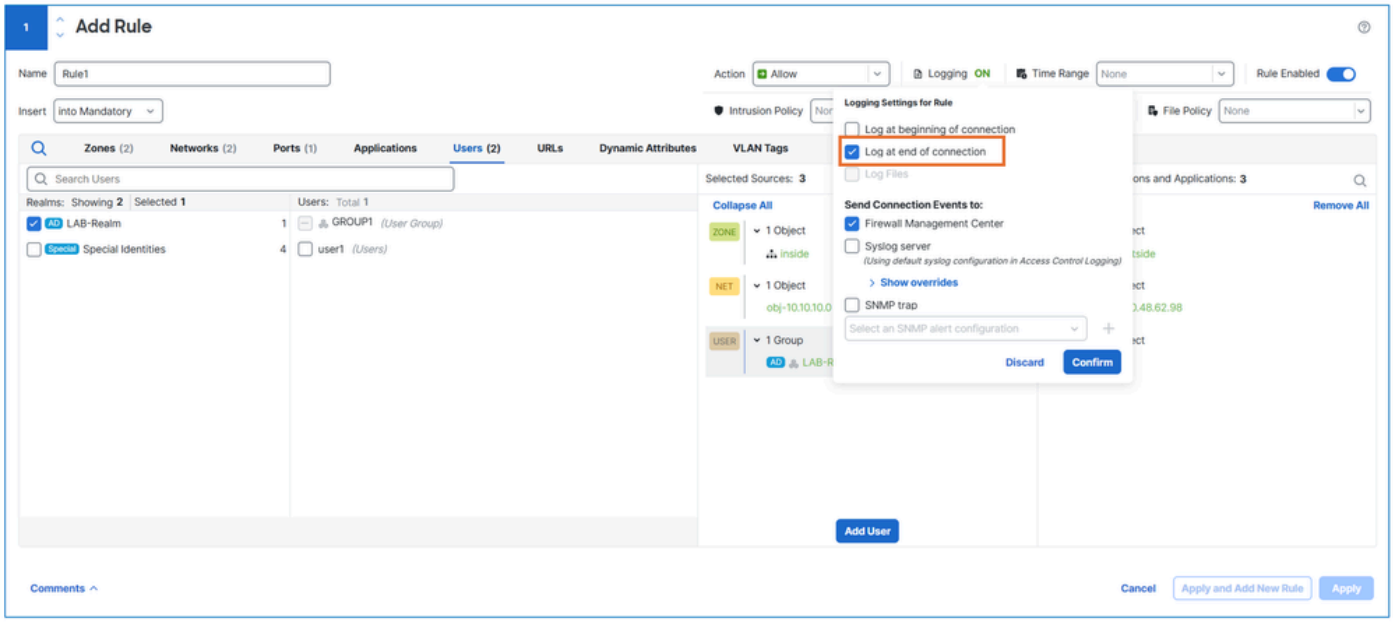
ACS creëren

Voer de details in volgens de taakvereisten, en het belangrijkste is, onder de UserStab, addGROUP1 van LAB-Realm.



Gebruikers toevoegen aan de regel

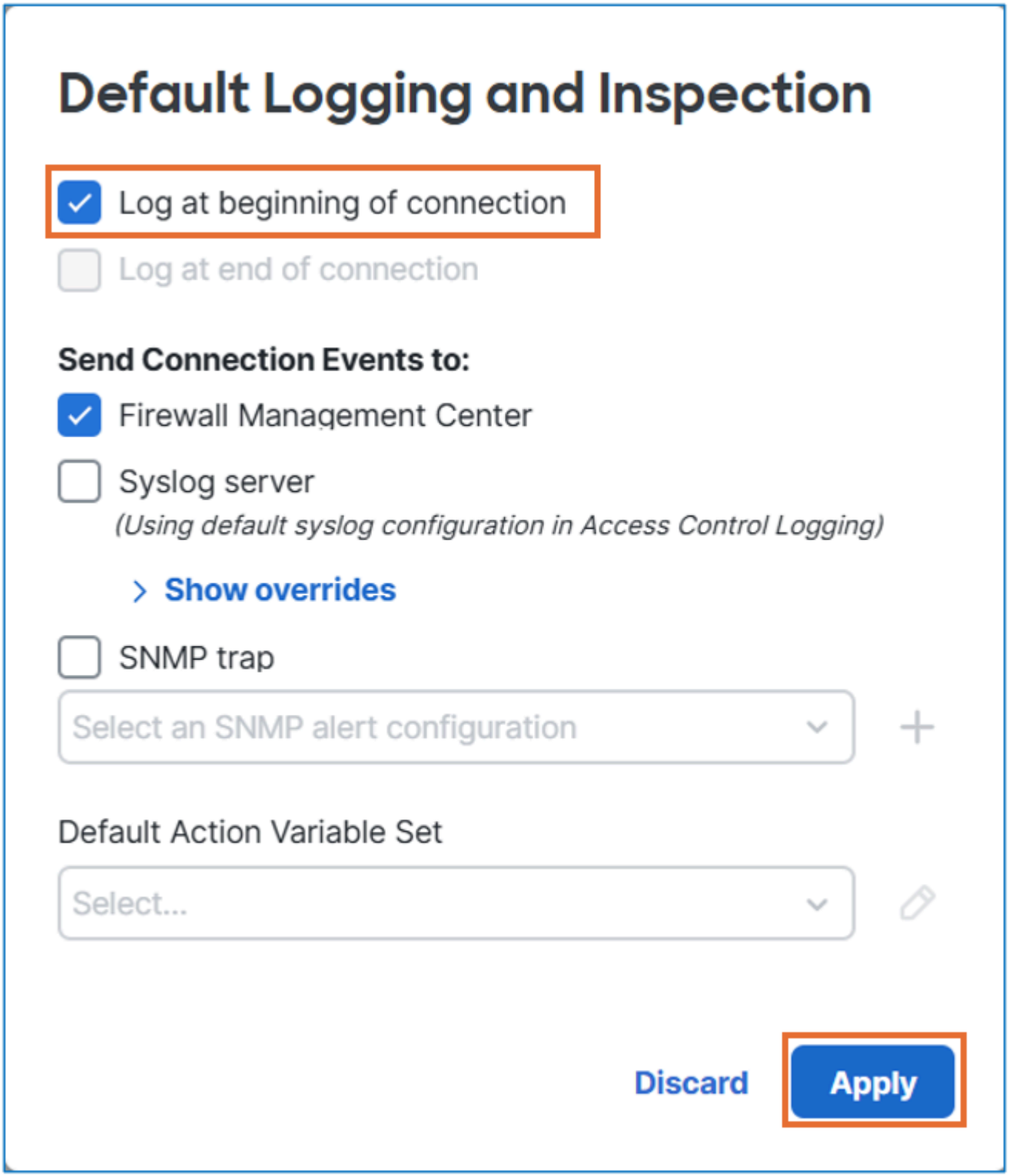
Schakel logboekregistratie voor de regel in door Log aan het einde van de verbinding te selecteren.



Logboekregistratie inschakelen

Stap 3. Logboekregistratie inschakelen voor de standaardactie.

Klik op het instellingenvak om de instellingen voor standaardactielogboeken te wijzigen.



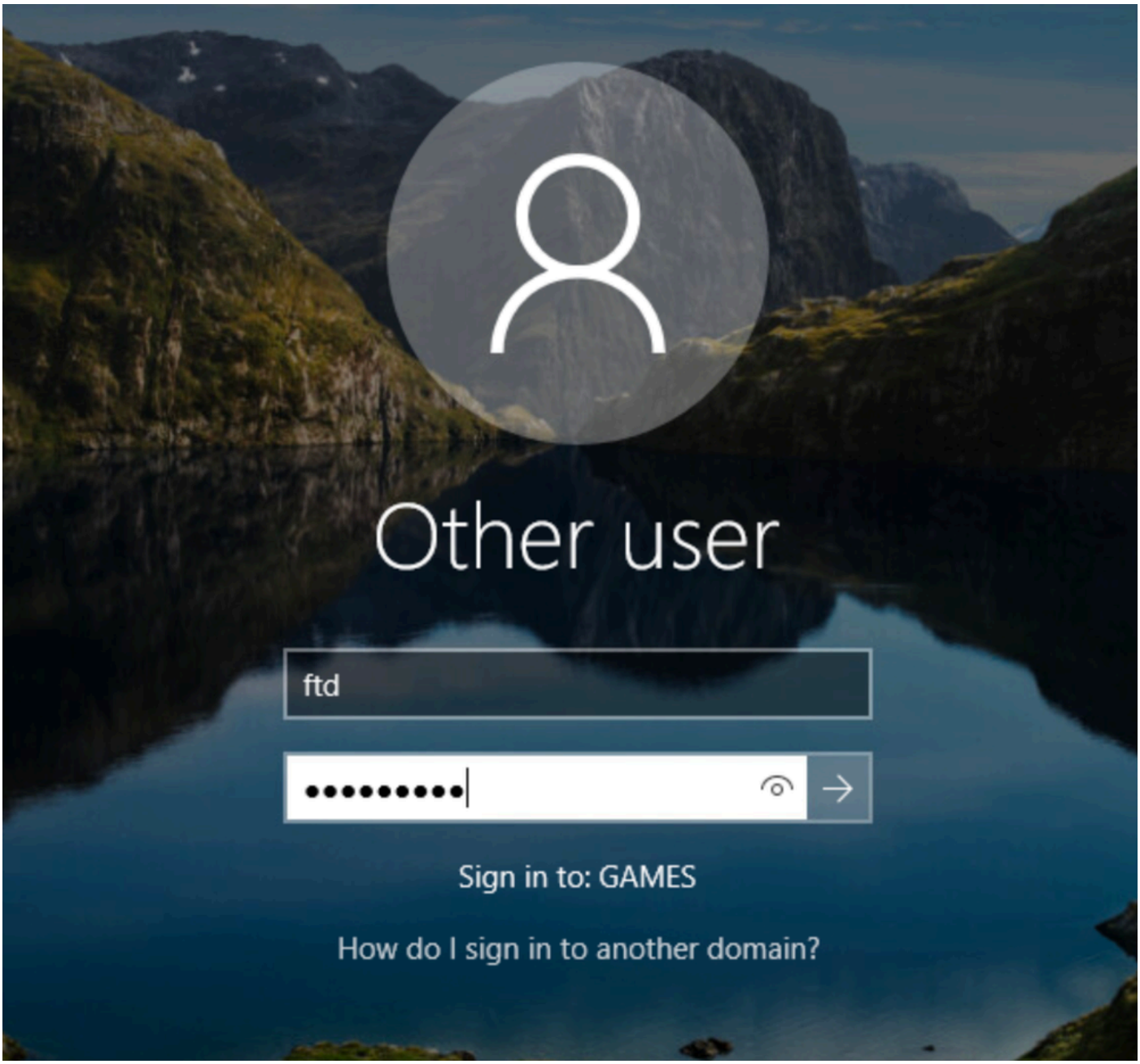
Logboekregistratie inschakelen

De configuratie opslaan en implementeren op de FTD.

Verificatie

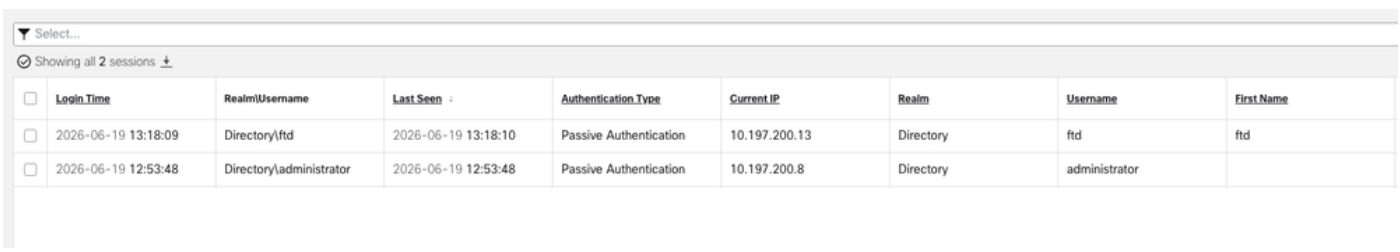
Verifieer de passieve identiteitsoperatie door te bevestigen dat verkeer uitsluitend is toegestaan voor ftd.

Log in bij de domeingebruiker vanaf het gebruikerssysteem.



gebruikersaanmelding

Nadat een gebruiker zich succesvol heeft aangemeld, controleert u vanuit FMC onder Analyse> gebruiker >actieve sessie om de actieve gebruikersdetails te bekijken.

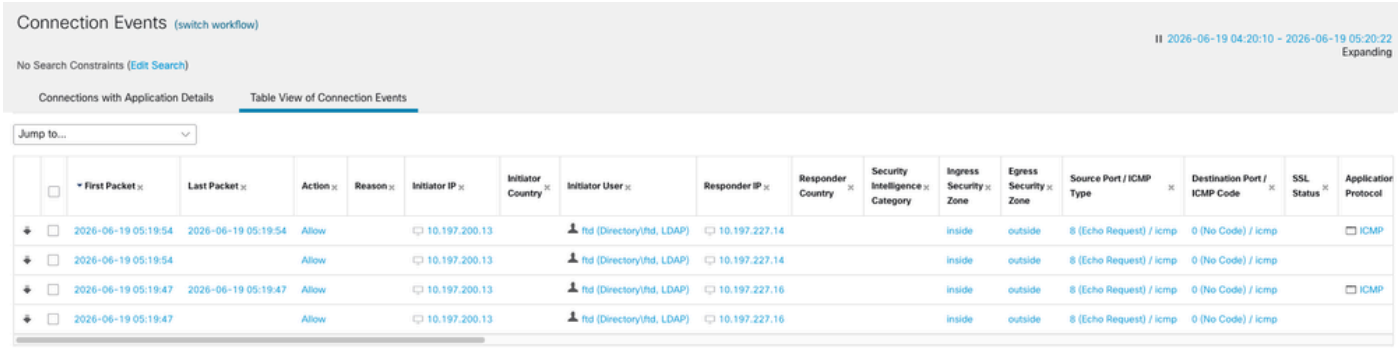

Select...

Showing all 2 sessions

Login Time	Realm\Username	Last Seen	Authentication Type	Current IP	Realm	Username	First Name
2026-06-19 13:18:09	Directory\ftd	2026-06-19 13:18:10	Passive Authentication	10.197.200.13	Directory	ftd	ftd
2026-06-19 12:53:48	Directory\administrator	2026-06-19 12:53:48	Passive Authentication	10.197.200.8	Directory	administrator	

Actieve sessies

Nadat u een verkeersverificatie hebt gestart vanaf de verbindingsgebeurtenissen, raadpleegt u de gebruikersgegevens in de verbindingsgebeurtenissen.

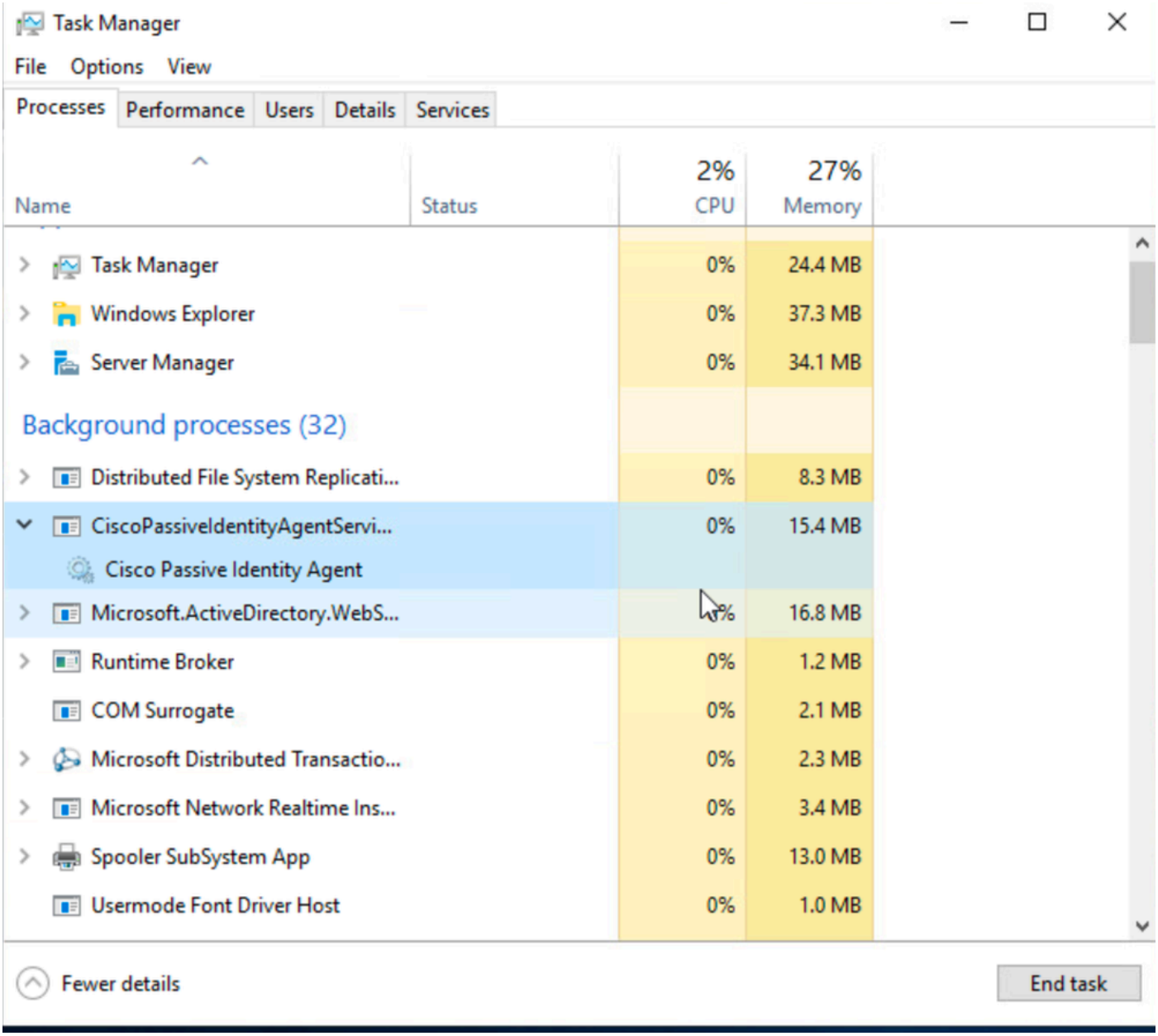


Actieve sessies

Probleemoplossing

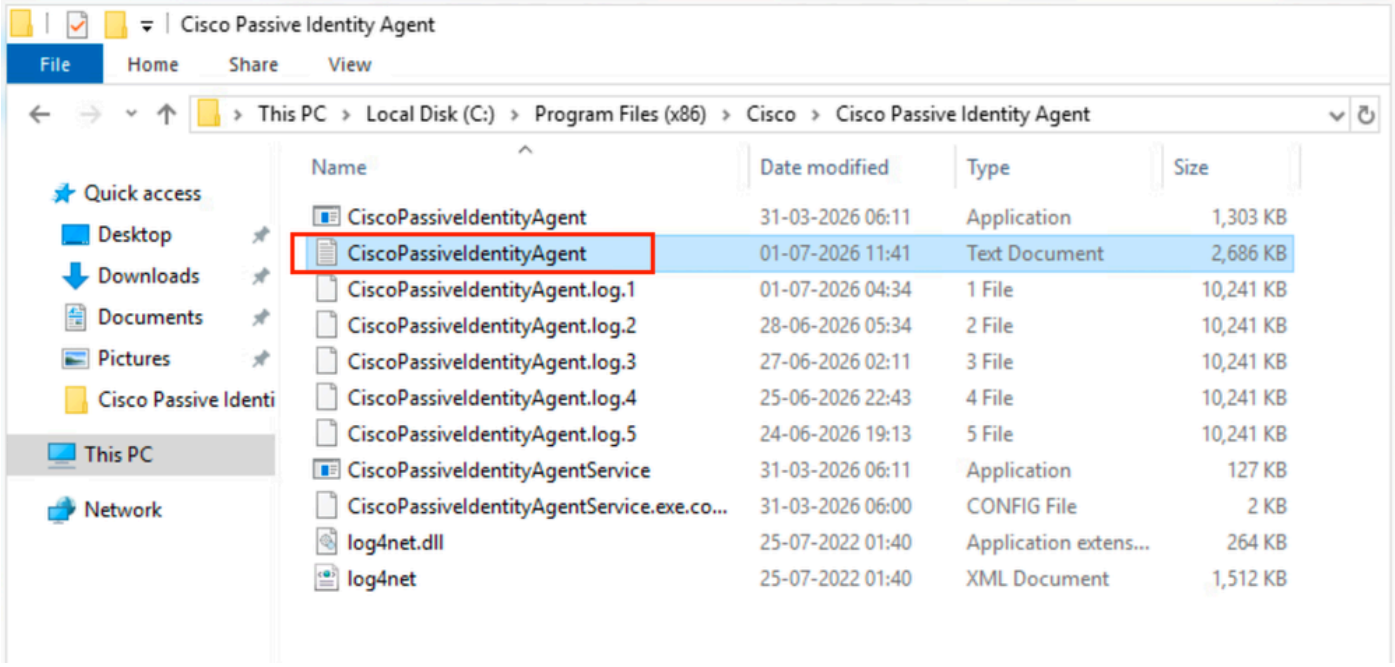
Logboeken van de controleagent

Op het Windows-systeem waarop de Agent wordt gehost, opent u Task Manager en controleert u of het achtergrondprocesCiscoPassiveIdentityAgentServices wordt uitgevoerd.



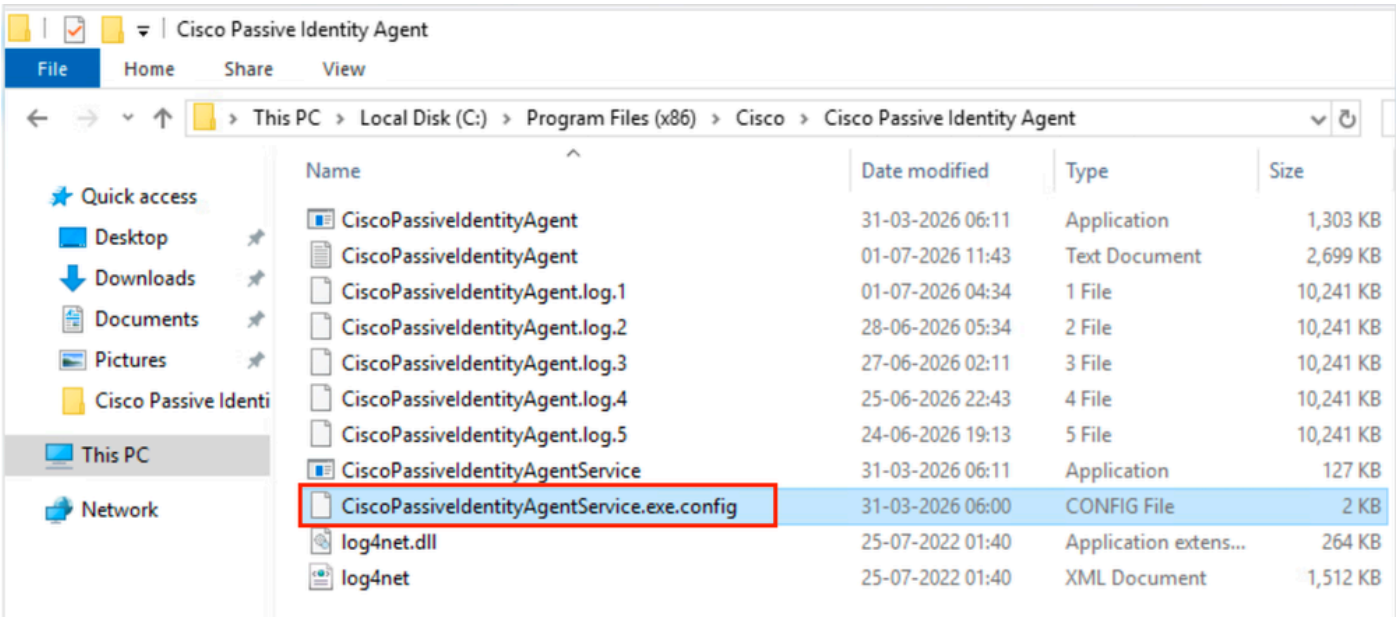
Uitvoerende taak

De agentlogs zijn te vinden in de CiscoPassiveIdentityAgent-bestanden. Deze bevinden zich standaard op: "C:\Program Files (x86)\Cisco\Cisco Passive Identity Agent\".



agent

De Agent-logs zijn standaard ingesteld op het INFO-niveau. Als u logboekregistratie op DEBUG-niveau wilt inschakelen, wijzigt u het bestand CiscoPassiveIdentityAgentService.exe. configfile en stelt u het logboekniveau in op ALLorDEBUG.



agentconfiguratie

infologboek

Logboeken van de agent controleren – Configuratie van de agent ophalen.

INFO Rest Client, Bulk Events: [f"domain":"games.cisco.com", "srcIpAddress": "X.X.X.X", "user": "fdm", "timestamp": "2026-07-01T19

INFO REST-client, toewijzingsstatus: OK

INFO Rest Client, REST-bericht succesvol voor userBatch fdm, latentie = 0, huidige DC-TIJD in UTC: 07/01/2026 19:47:34 GEBRUIKER aangemeld bij

INFO Rest Client, configuratie van agent aanvragen

FMC-logboeken

Voer deze opdracht uit om te zien of de toewijzing van gebruiker naar IP van de agent is ontvangen.

```
root@firepower123:/var/sf/user_enforcement# user_map_query.pl -u fdm

Current Time: 07/01/2026 11:36:03 UTC

Getting information on username(s)...


___
User #1: fdm
---

  ID:         10
  Last Seen:  Unknown
  for_policy: 1

==============================
|          Database          |
==============================

No IP Addresses


##) Group Name (ID)
 1) Domain Users (18)
 2) Users (48)
root@firepower123:/var/sf/user_enforcement#
```

FMC-uitvoer

Als de vorige opdracht geen toewijzing weergeeft, verzamelt u deze logs en neemt u contact op met Cisco TAC.

Dit is een lijst met relevante logs voor de FMC API. Het logboek omvat ze allemaal.

- /var/log/auth-daemon.log
- /var/log/messages
- /var/log/process_stdout.log
- /var/log/process_stderr.log

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.