

De passieve identiteitsagent configureren met FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuraties](#)

[Een bron voor een passieve identiteitsagent configureren](#)

[Een gebruiker van een Passive Identity Agent maken in het Secure Firewall Management Center](#)

[De software van de Passive Identity Agent installeren en configureren](#)

[Identiteitsbeleid configureren](#)

[Beleid voor toegangscontrole configureren](#)

[Verificatie](#)

[Probleemoplossing](#)

[Logboeken van de controleagent](#)

[FMC-logboeken](#)

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.

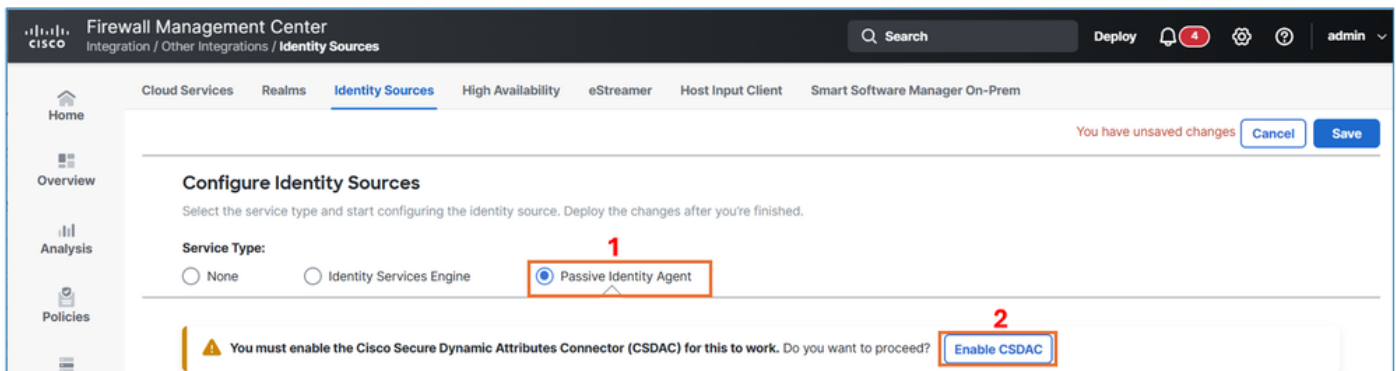
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

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.

Enable Cisco Secure Dynamic Attributes Connector?



This identity source requires CSDAC to be enabled. Doing so can take about 15 minutes.

Cancel

Enable

CSDAC inschakelen

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

Enabling Dynamic Attributes Connector



Dynamic Attributes Connector enabled successfully



Preparing Docker.

Done



Verifying images.

Done



Downloading connector images.

Done



Downloading Core images.

Done with warnings



Using local images.

Done



Bringing up Core services.

Done



Bringing up API service.

Done

Done

CSDAC ingeschakeld

Klik op de knop Agent maken.

Firewall Management Center
Integration / Other Integrations / Identity Sources

Search Deploy 10 Global | admin

Cloud Services Realms **Identity Sources** High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Home Overview Analysis Policies Devices Objects **Integration**

Configure Identity Sources

Select the service type and start configuring the identity source. Deploy the changes after you're finished.

Service Type:

☐ None ☐ Identity Services Engine ☒ Passive Identity Agent

1 Your changes will be effective after you save Passive Identity Agent as the Identity Source.

How does it work?

1. Create agents in Secure Firewall Management Center
2. Install agents on domain controllers and enter FMC credentials
3. Agents read their respective configurations from the FMC
4. Primary agent sends session data from the domain controller to the FMC
5. Secondary agent stands by while primary is working

How-To **Create Agent** Learn more

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.

Configure Agent



Name *

LAB-Agent

Description

Role

☐

Primary

☐

Secondary

☒

Standalone

[Learn more](#) about the agent role.

Domain Controller *

10.62.113.247



Agent will monitor this domain controller.

Important:

This agent will be created and assigned to the selected domain controller. Install it on the domain controller (or on its member machine) to start the tracking.

Cancel

Save

Agent configureren

Klik op de knop Opslaan.

Configure Identity Sources

Select the service type and start configuring the identity source. Deploy the changes after you're finished.

Service Type:

☐ None
 ☐ Identity Services Engine
 ☒ Passive Identity Agent

Your changes will be effective after you save Passive Identity Agent as the Identity Source.

Search by agent name or domain controller name

Create Agent

Domain Controllers	Monitoring Agents	Hostname	Connection Status
LAB-Realm			

Sla de configuratie op

Het resultaat.

Configure Identity Sources

Select the service type and start configuring the identity source. Deploy the changes after you're finished.

Service Type:

☐ None
 ☐ Identity Services Engine
 ☒ Passive Identity Agent

Search by agent name or domain controller name

Create Agent

Domain Controllers	Monitoring Agents	Hostname	Connection Status
LAB-Realm			
10.62.113.247	LAB-Agent (standalone)	Not Applicable	

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.

User Configuration

User Name	passiveidentity
Real Name	
Email Address	
Authentication	☐ Use External Authentication Method
Password	
Confirm Password	
Maximum Number of Failed Logins	5 (0 = Unlimited)
Minimum Password Length	8
Days Until Password Expiration	0 (0 = Unlimited)
Days Before Password Expiration Warning	0
Options	☐ Force Password Reset on Login ☐ Check Password Strength ☐ Exempt from Browser Session Timeout

Gebruiker maken

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

User Role Configuration

- Default User Roles
- ☐ Administrator
 - ☐ External Database User (Read Only)
 - ☐ Security Analyst
 - ☐ Security Analyst (Read Only)
 - ☐ Security Approver
 - ☐ Intrusion Admin
 - ☐ Access Admin
 - ☐ Network Admin
 - ☐ Maintenance User
 - ☐ Discovery Admin
 - ☐ Threat Intelligence Director (TID) User
 - ☒ Passive Identity User
- Custom User Roles
- ☐ REST VDI

Cancel

Save

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.

Software Download

[Downloads Home](#) / [Security](#) / [Firewalls](#) / [Firewall Management](#) / [Secure Firewall Management Center](#) / [Firepower Management Center 1600](#) / [Firepower System Tools and APIs- Passive Identity Agt](#)

Q Search...

Expand All Collapse All

Latest Release

Passive Identity Agt

TSAgent-1.4.1

Qualys Connector 1.0

Event Streamer SDK

All Release

Qualys Connector

Passive Identity Agt

Event Streamer

TSAgent

Firepower Management Center 1600

Release Passive Identity Agt

 My Notifications

Related Links and Documentation

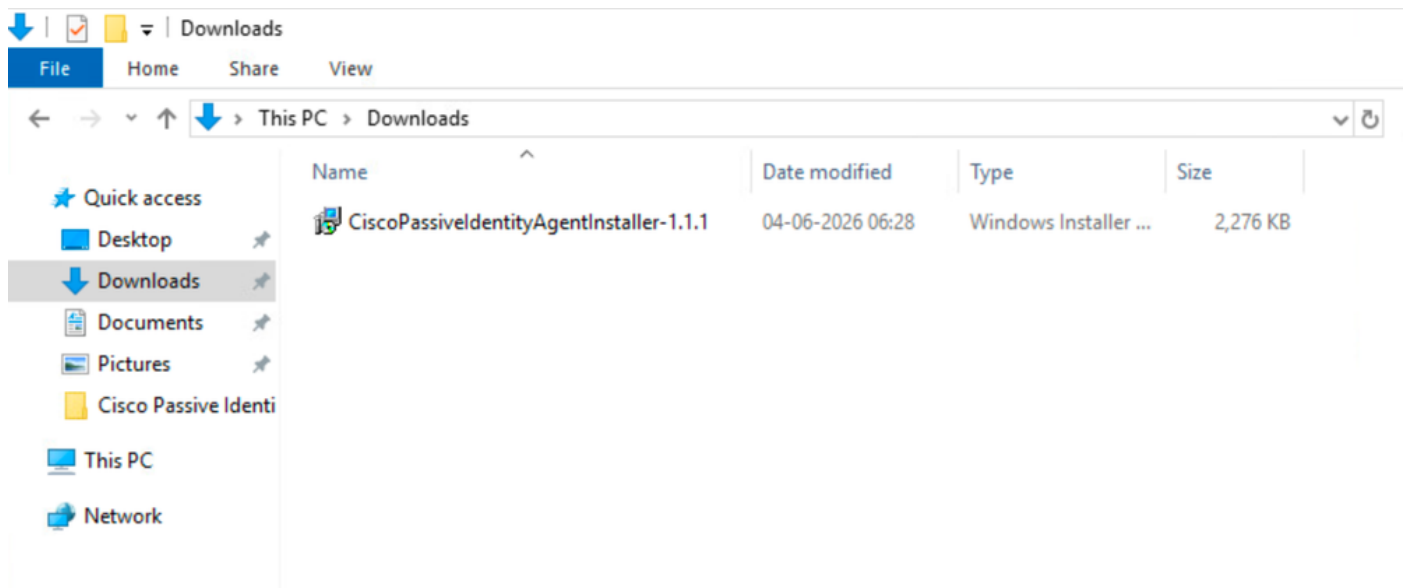
Release Notes for Passive Identity Agt

Release Notes for Passive Identity Agt 1.0

File Information	Release Date	Size	
Installer for the Cisco Passive Identity Agent CiscoPassiveIdentityAgentInstaller-1.0.msi Advisories	16-Sep-2024	1.59 MB	  
Installer for the Cisco Passive Identity Agent CiscoPassiveIdentityAgentInstaller-1.1.msi Advisories	11-Mar-2025	2.16 MB	  

Download de software

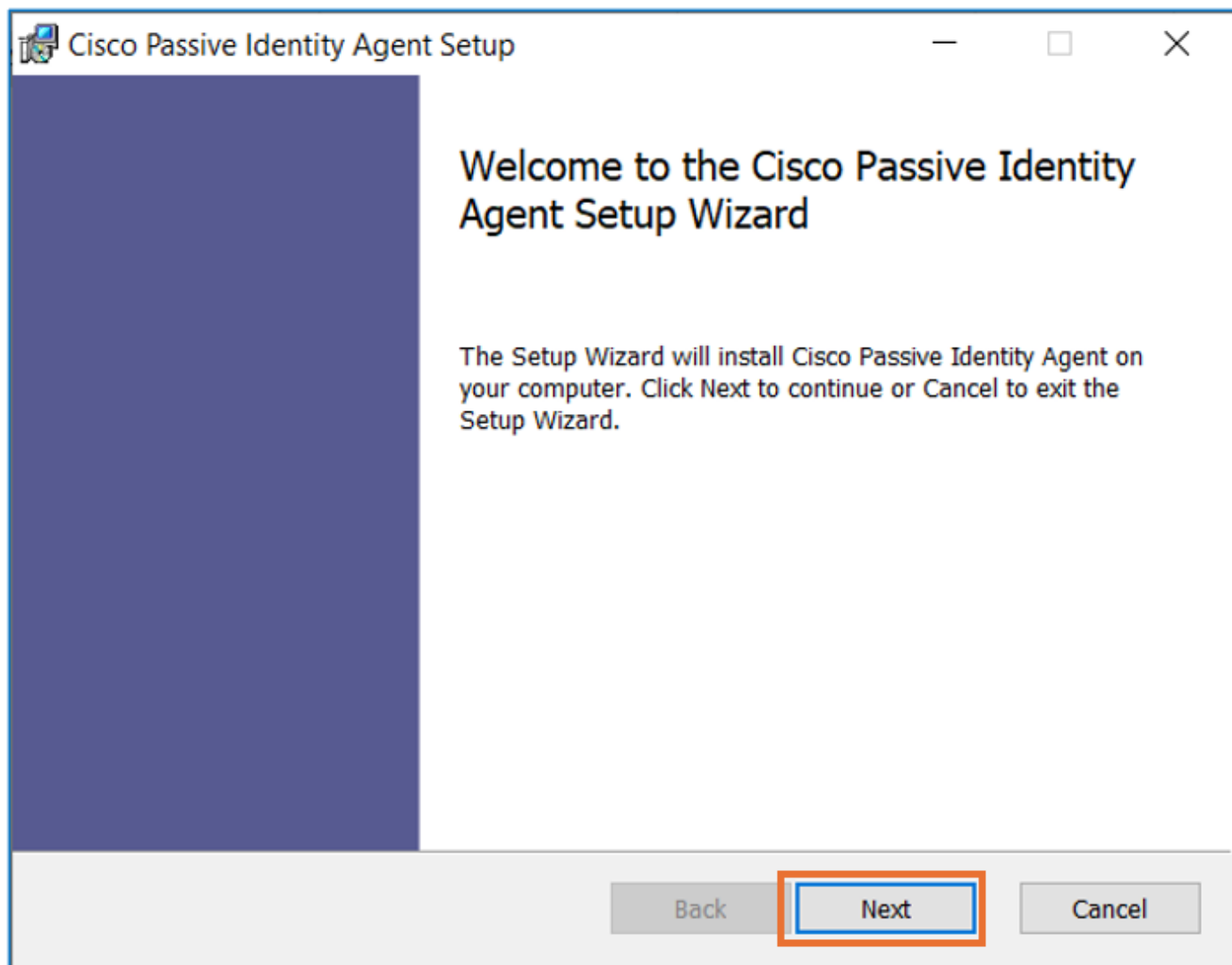
Nadat u de agent hebt gedownload, begint u met het installatie-proces op de domeincontroller.



agent

1

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.

Cisco Passive Identity Agent 1.1.0-1

Secure Firewall Management Center

Enter the fully qualified domain name or IP address of the Secure Management Center this agent communicates with.

Integration

On-Prem Cloud

Primary FMC FQDN / IP address Port

10.62.184.97 : 443

FMC FQDN or IP address and Port of the FMC

Username Password

passiveidentity ••••••••

The credentials for the connection (Primary or Secondary)

Agent LAB-Agent

Agent	DCs (Domain Controllers)
LAB-Agent	10.62.113.247

You need to select Agent-DCs pair to be able to save configuration

Test

I have Secondary FMC v

Save Cancel

Username/Password created in previous task

Click here to test the connectivity

De agent configureren.

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

 Cisco Passive Identity Agent 1.1.0-1

Secure Firewall Management Center

Enter the fully qualified domain name or IP address of the Secure Management Center this agent communicates with.

Integration

On-Prem

Cloud

Primary FMC FQDN / IP address

10.62.184.97

Port

443

FMC FQDN or IP address and Port of the FMC

Username

passiveidentity

Password

●●●●●●●●

The credentials for the connection (Primary or Secondary)

Agent

LAB-Agent

DCs (Domain Controllers)

10.62.113.247

You need to select Agent-DCs pair to be able to save configuration

Tested successfully

✔ Primary FMC was tested successfully.

I have Secondary FMC

Save

Cancel

test

Klik op de knop OK om de agentconfiguratie te voltooien.

Passive Identity Agent

Secure Firewall Management Center

Enter the fully qualified domain name or IP address of the Secure Management Center this agent communicates with.

Configuration

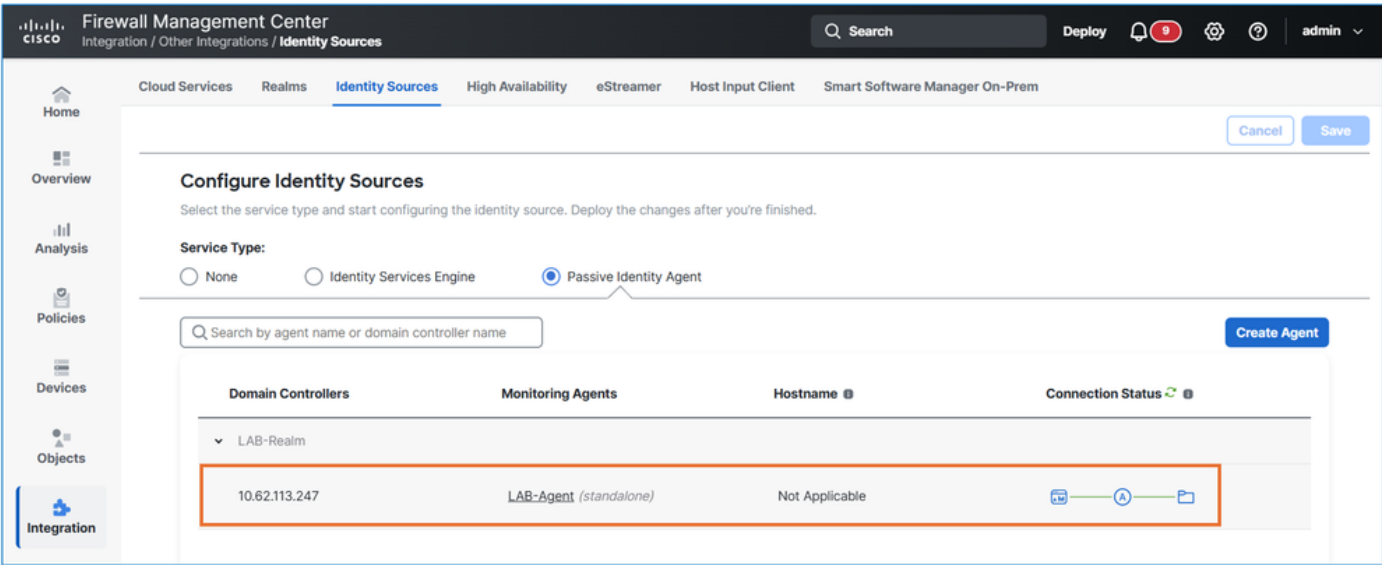
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

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.



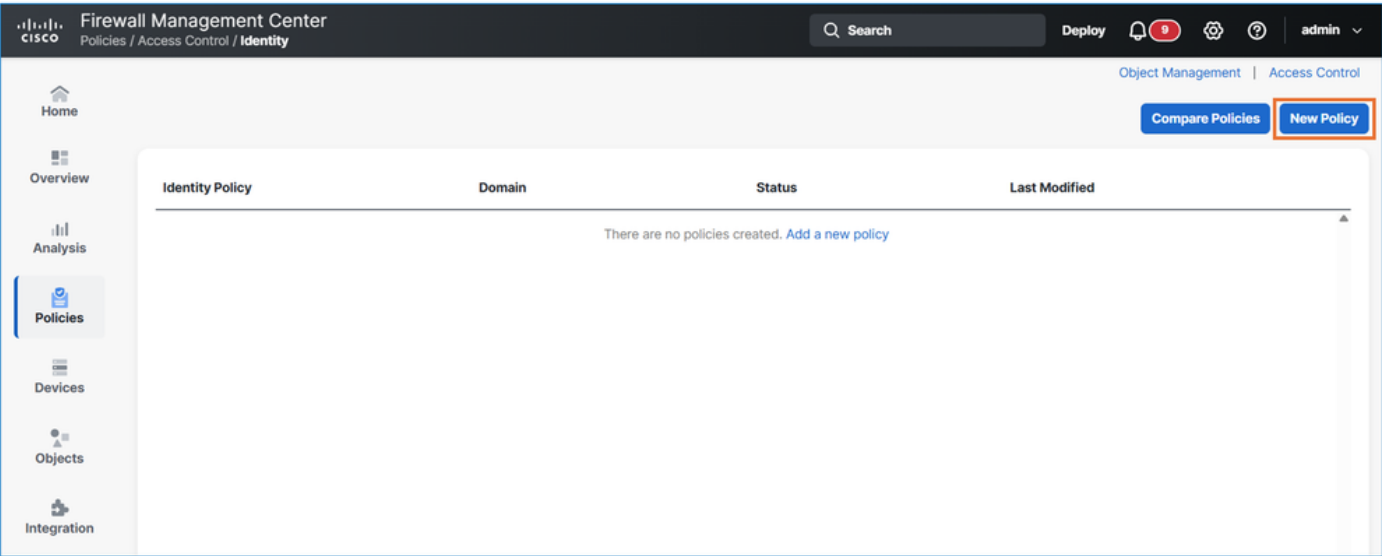
Controleer de communicatie van FMC

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.

New Identity policy

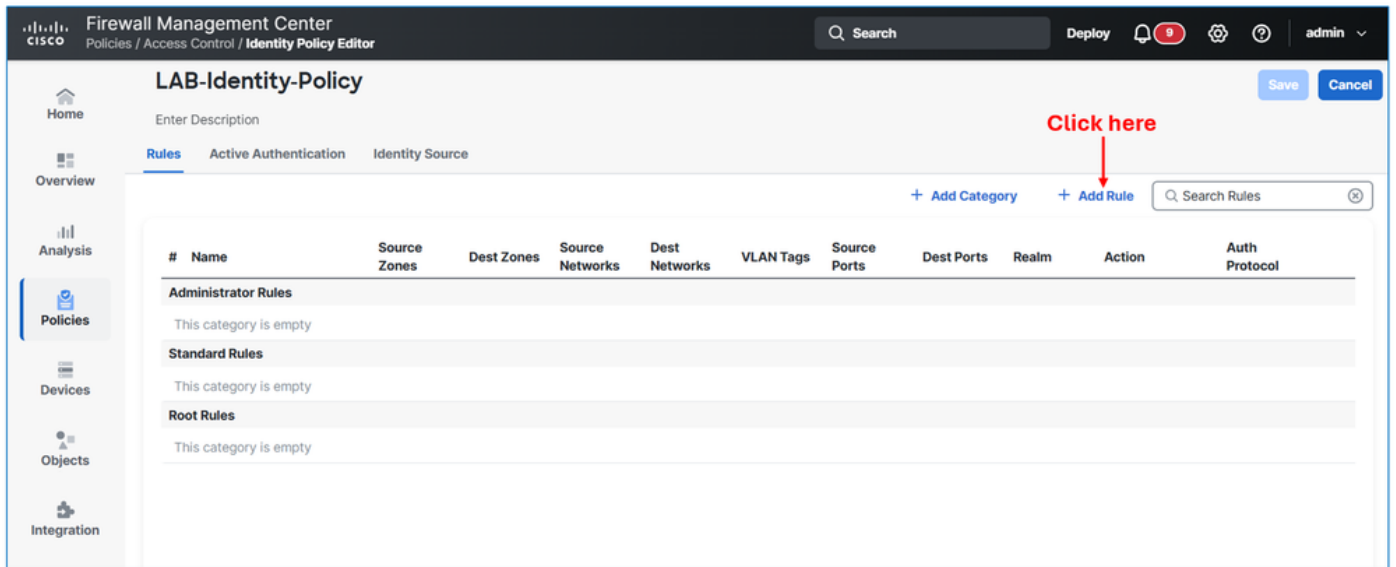
Name

Description

[Cancel](#) [Save](#)

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.

Add Rule

Name: Rule1 ☒ Enabled Insert into Category: Standard Rules

Action: Passive Authentication **Realm:** LAB-Realm (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Zones Networks VLAN Tags Ports **Realm & Settings**

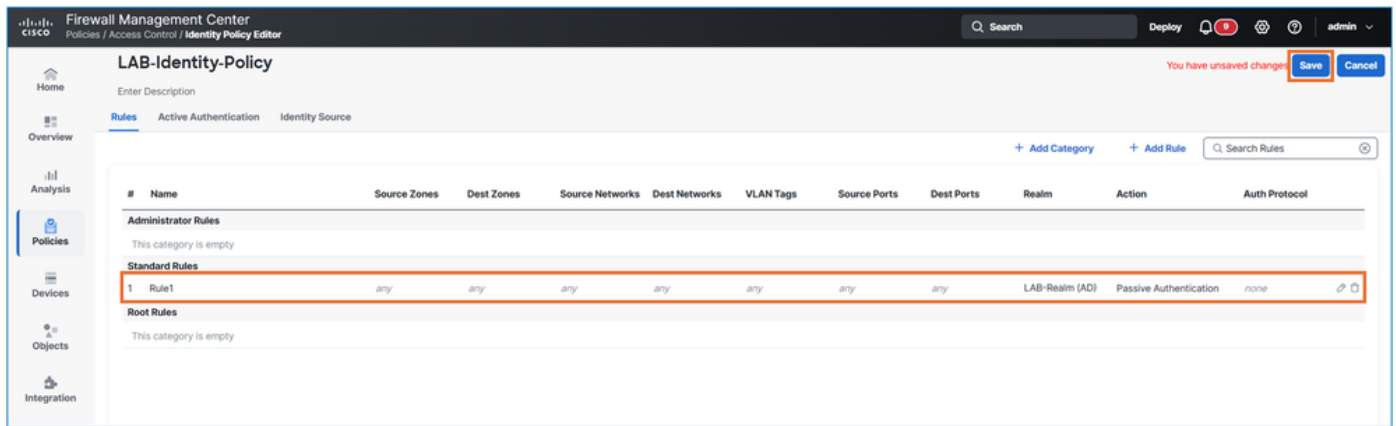
Authentication Realm *
LAB-Realm (AD)

☐ Use active authentication if passive or VPN identity cannot be established

Cancel **Add**

Realm instellen

Klik op de knop Opslaan.



Sla de configuratie op

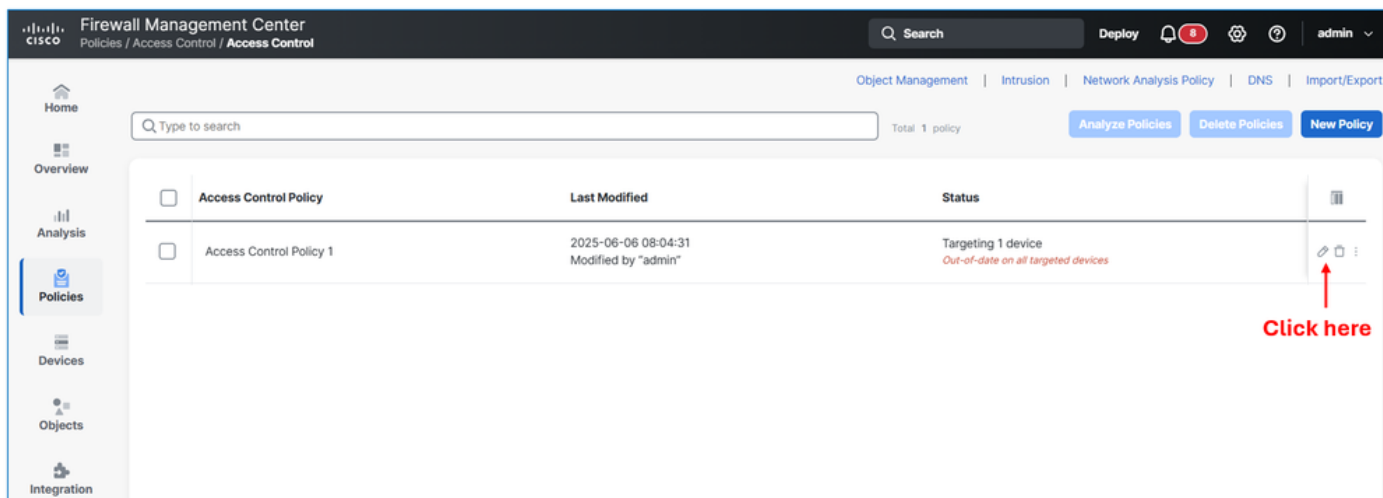
Beleid voor toegangscontrole configureren

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

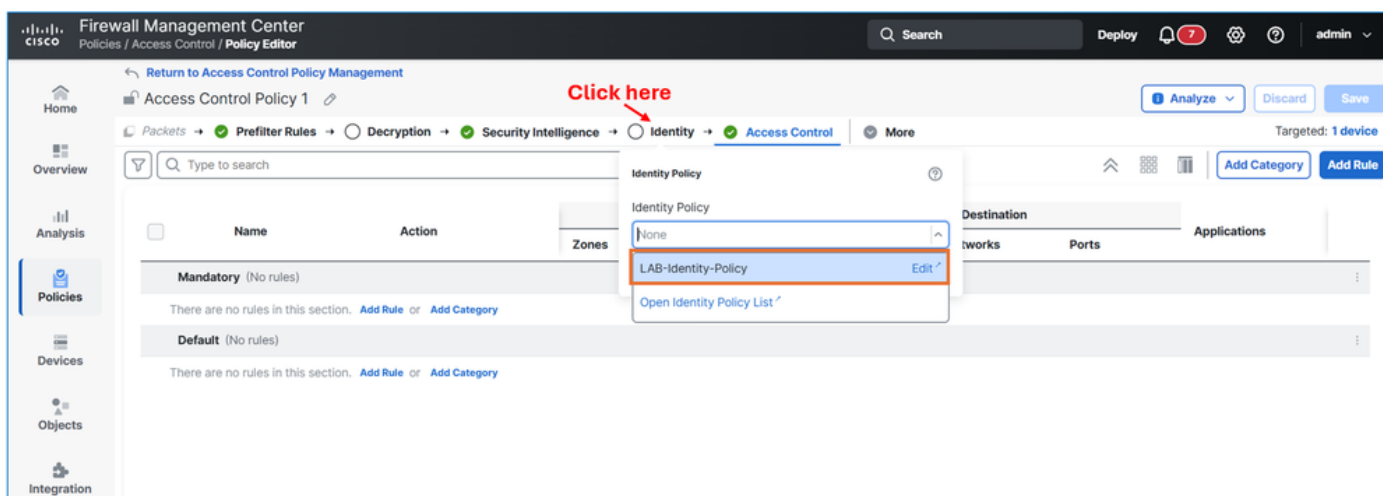
Stap 1. Koppel het identiteitsbeleid aan het toegangscontrole beleid van

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



Beleid bewerken

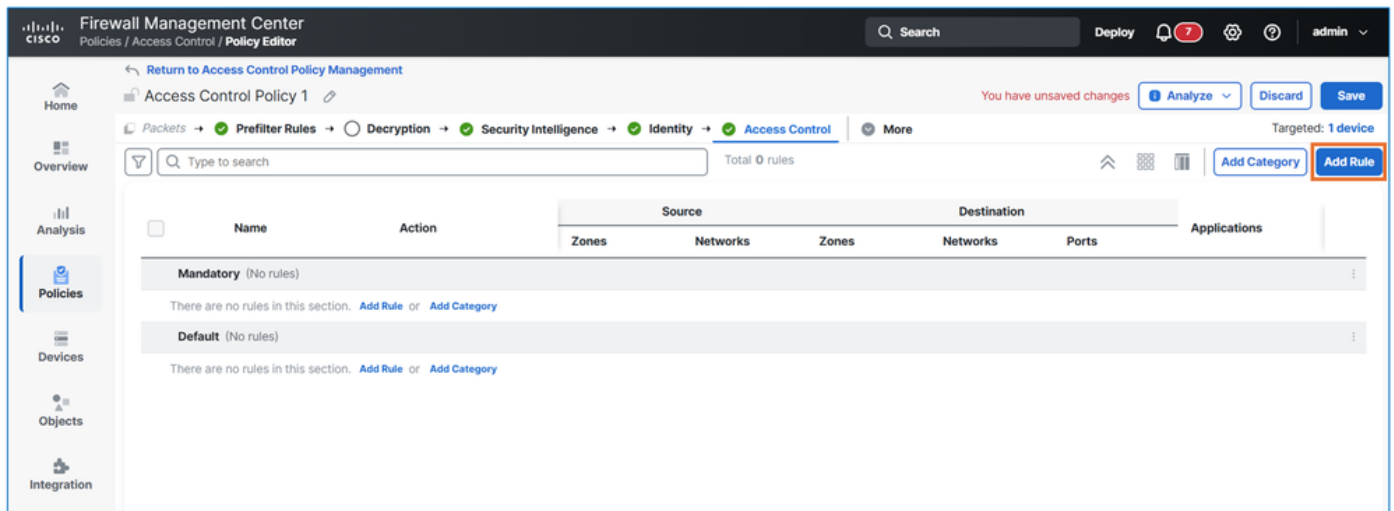
Navigeer naar het gedeelte Identiteit en koppel het Identiteitsbeleid dat in de vorige taak is gemaakt.



Identiteitsbeleid toevoegen

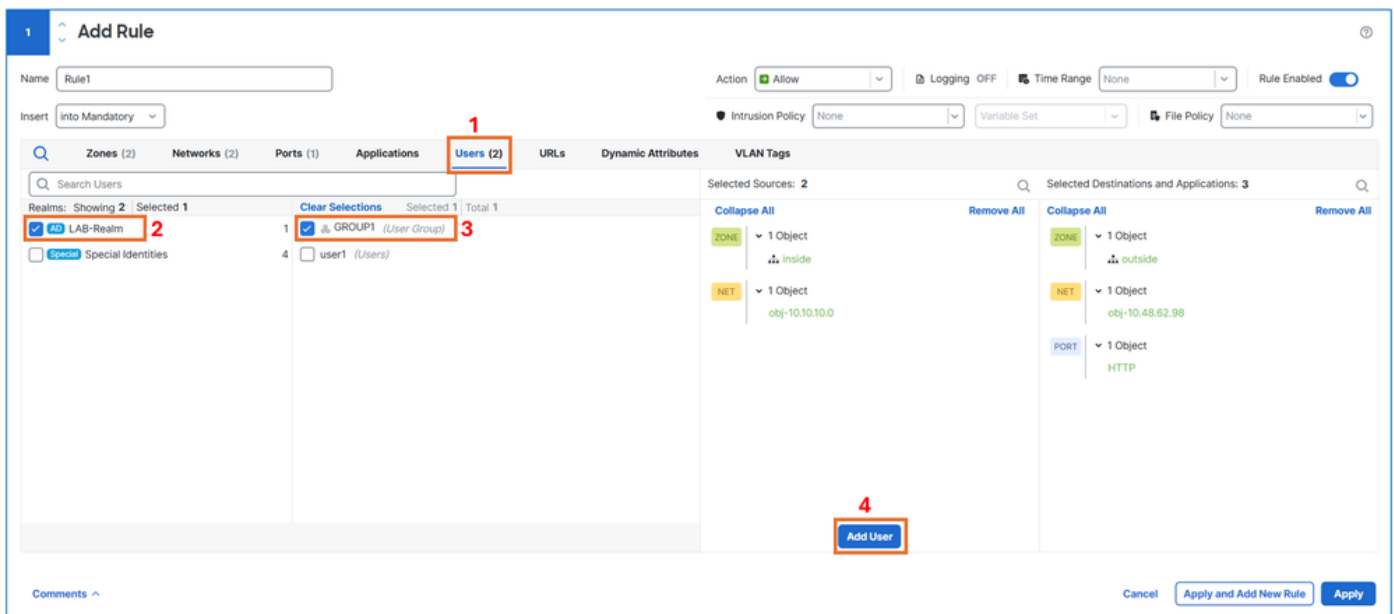
Klik op de knop Toepassen

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.

1 Add Rule

Name: Rule1

Action: Allow Logging: ON Time Range: None Rule Enabled: ☒

Insert: Into Mandatory

Intrusion Policy: None

Logging Settings for Rule

- ☐ Log at beginning of connection
- ☒ Log at end of connection
- ☐ Log Files

Send Connection Events to:

- ☒ Firewall Management Center
- ☐ Syslog server (Using default syslog configuration in Access Control Logging)
- ☐ SNMP trap

Select an SNMP alert configuration

Discard Confirm

File Policy: None

Search Users

Realms: Showing 2 Selected 1

- ☒ LAB-Realm
- ☐ Special Identities

Users: Total 1

- GROUP1 (User Group)
- user1 (Users)

Selected Sources: 3

- ZONE: 1 Object inside
- NET: 1 Object obj-10.10.10.0
- USER: 1 Group AD LAB-R

Comments ^

Cancel Apply and Add New Rule Apply

Logboekregistratie inschakelen

Stap 3. Logboekregistratie inschakelen voor de standaardactie.

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

Default Logging and Inspection

☒ Log at beginning of connection

☐ Log at end of connection

Send Connection Events to:

☒ Firewall Management Center

☐ Syslog server

(Using default syslog configuration in Access Control Logging)

[> Show overrides](#)

☐ SNMP trap

Select an SNMP alert configuration



Default Action Variable Set

Select...



Discard

Apply

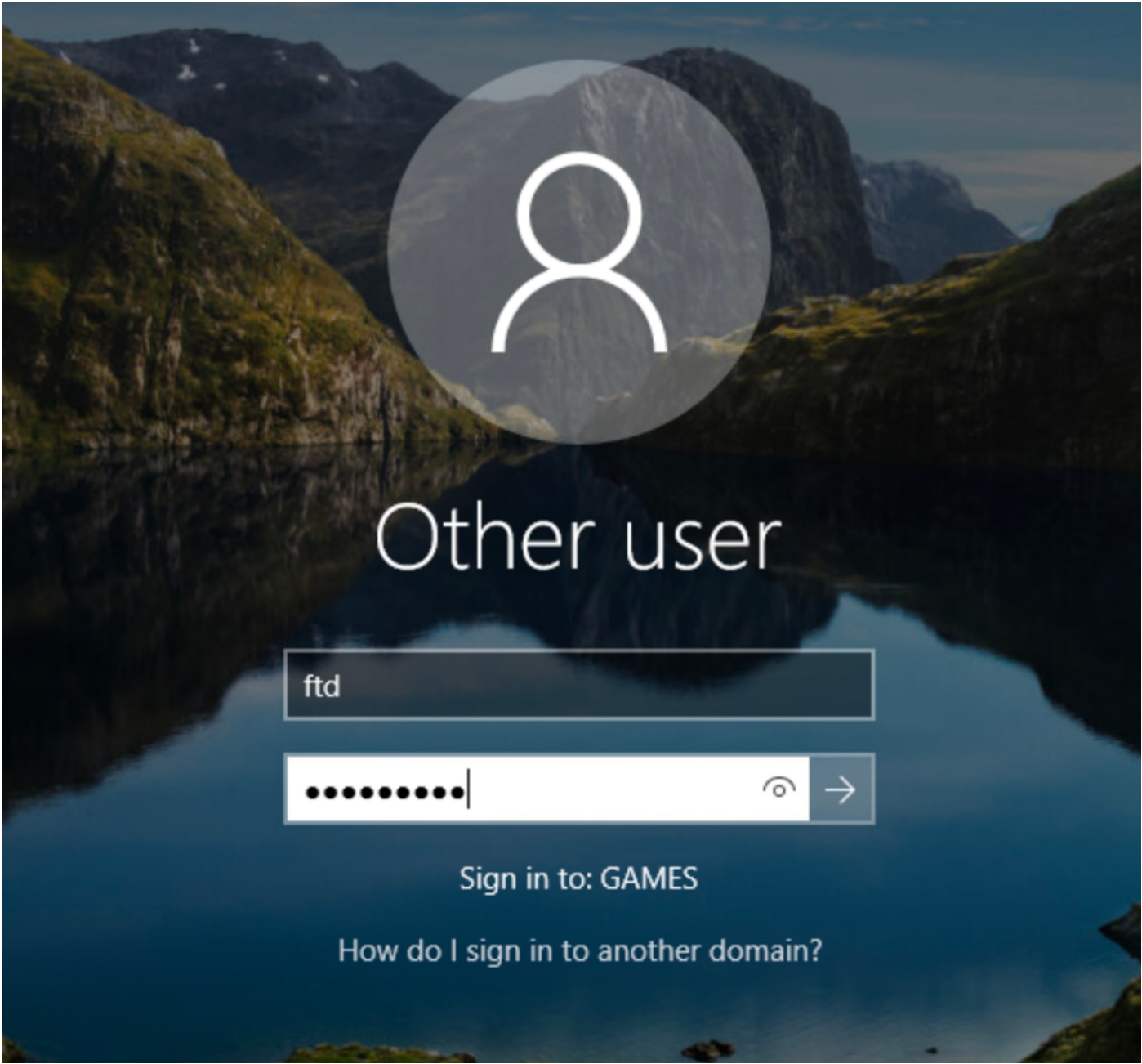
Logboekregistratie inschakelen

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.

Connection Events (switch workflow)

No Search Constraints (Edit Search)

Connections with Application Details Table View of Connection Events

II 2026-06-19 04:20:10 – 2026-06-19 05:20:22

Expanding

Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	Application Protocol
+	2026-06-19 05:19:54	2026-06-19 05:19:54	Allow		10.197.200.13		hd (Directory/hd, LDAP)	10.197.227.14			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP
+	2026-06-19 05:19:54		Allow		10.197.200.13		hd (Directory/hd, LDAP)	10.197.227.14			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		
+	2026-06-19 05:19:47	2026-06-19 05:19:47	Allow		10.197.200.13		hd (Directory/hd, LDAP)	10.197.227.16			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP
+	2026-06-19 05:19:47		Allow		10.197.200.13		hd (Directory/hd, LDAP)	10.197.227.16			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		

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.

Task Manager

File Options View

Processes
Performance
Users
Details
Services

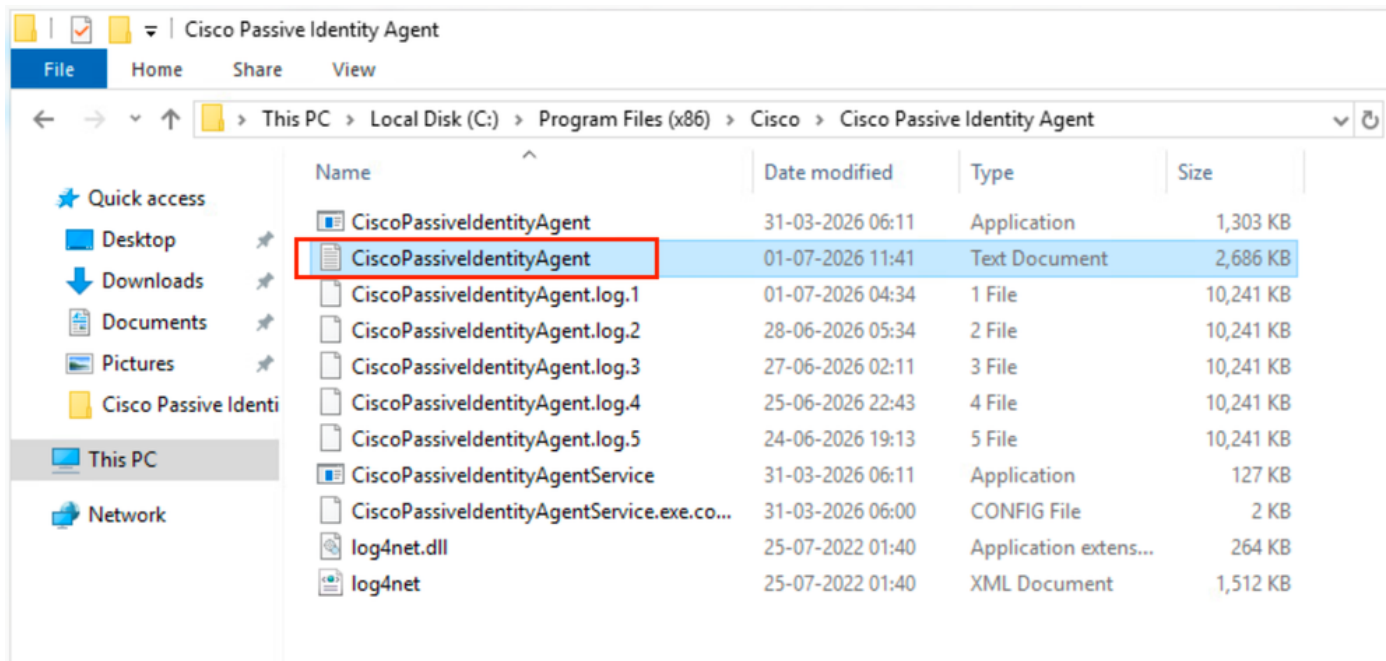
Name	Status	2% CPU	27% Memory
> Task Manager		0%	24.4 MB
> Windows Explorer		0%	37.3 MB
> Server Manager		0%	34.1 MB
Background processes (32)			
> Distributed File System Replicati...		0%	8.3 MB
CiscoPassiveIdentityAgentServi... Cisco Passive Identity Agent		0%	15.4 MB
> Microsoft.ActiveDirectory.WebS...		0%	16.8 MB
> Runtime Broker		0%	1.2 MB
COM Surrogate		0%	2.1 MB
> Microsoft Distributed Transactio...		0%	2.3 MB
> Microsoft Network Realtime Ins...		0%	3.4 MB
> Spooler SubSystem App		0%	13.0 MB
Usermode Font Driver Host		0%	1.0 MB

Fewer details

End task

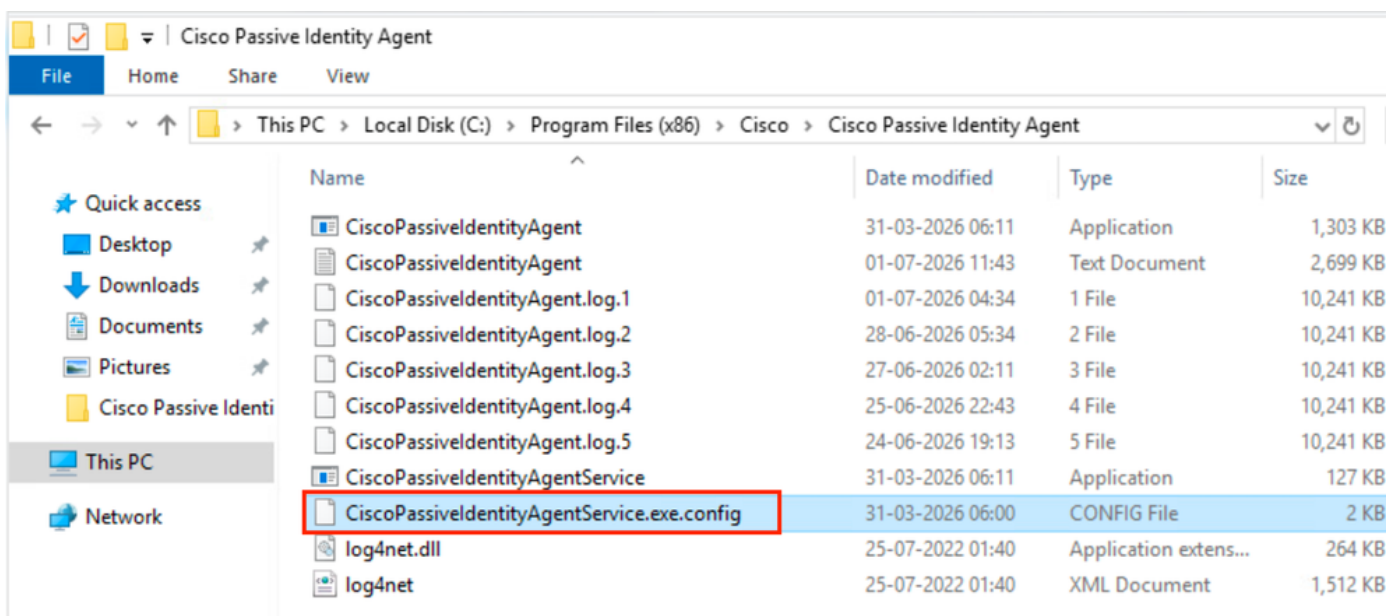
Uitvoerende taak

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.config en stelt u het logboekniveau in op ALLorDEBUG.



agentconfiguratie



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler, log4net" />
  </configSections>
  <log4net>
    <root>
      <level value="INFO" />
      <!-- Logging Levels: OFF, FATAL, ERROR, WARN, INFO, DEBUG, ALL -->
      <appender-ref ref="RollingFileAppender" />
    </root>
    <appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
      <file value="CiscoPassiveIdentityAgent.log" />
      <appendToFile value="true" />
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="5" />
      <maximumFileSize value="10MB" />
      <staticLogFileName value="true" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%date %level - %message%newline" />
      </layout>
    </appender>
  </log4net>
</configuration>
```

infologboek

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

INFO Rest Client, Bulk Events: [{"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.