

Configuration de Passive Identity Agent à l'aide de FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurations](#)

[Configuration d'une source d'agent d'identité passive](#)

[Création d'un utilisateur d'Identity Agent passif sur le Secure Firewall Management Center](#)

[Installation et configuration du logiciel Passive Identity Agent](#)

[Configurer les stratégies d'identité](#)

[Configurer les stratégies de contrôle d'accès](#)

[Vérification](#)

[Dépannage](#)

[Vérification des journaux des agents](#)

[Journaux FMC](#)

Introduction

Ce document décrit comment configurer l'agent d'identité passif Source qui envoie des données de session à FMC

Conditions préalables

Exigences

- Cisco Secure Firewall Management Center version 7.6+
- Cisco Secure Firewall version 7.6+
- Serveur Windows Active Directory, le serveur doit exécuter Windows Server 2008 ou version ultérieure.
- Vous devez activer Snort 3 sur les périphériques Secure Firewall Threat Defense.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

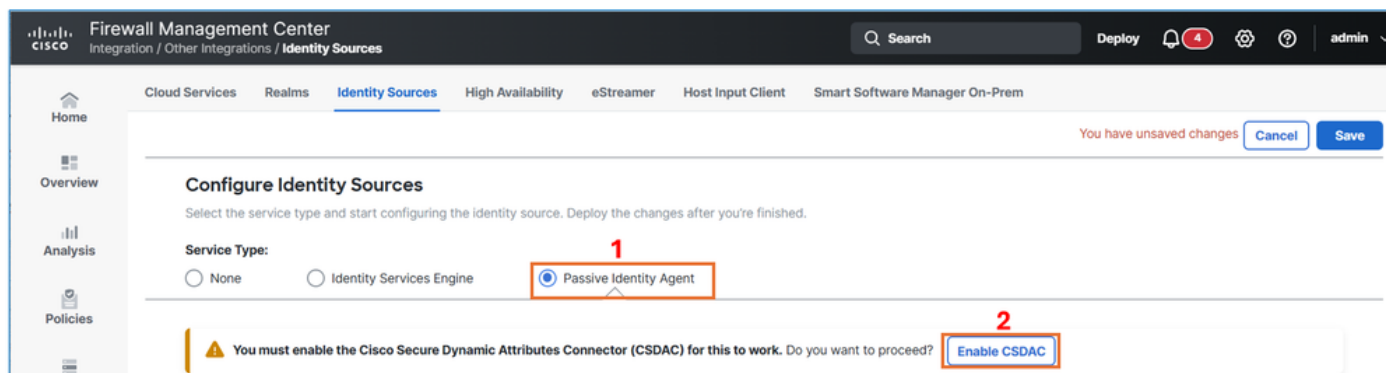
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurations

Avant de configurer l'agent, veuillez terminer l'intégration d'AD et de FMC.

Configuration d'une source d'agent d'identité passive

Dans l'interface utilisateur de FMC, accédez à Intégration > Autres intégrations > Sources d'identité, cliquez sur Agent d'identité passif. Si le connecteur d'attributs dynamiques sécurisés Cisco n'a pas encore été activé, vous êtes invité à le faire en cliquant sur Activer CSDAC.



Agent d'identité passif

Cliquez sur le bouton Activer pour activer le CSDAC.

Enable Cisco Secure Dynamic Attributes Connector?



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

Cancel

Enable

Activer CSDAC

Cette étape prend environ 10 minutes. Une fois que le CSDAC est correctement activé, cliquez sur le bouton Terminer pour continuer.

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 activé

Cliquez sur le bouton Créer un agent.

Firewall Management Center
Integration / Other Integrations / Identity Sources

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

Créer un agent

Définissez un nom pour l'agent, sélectionnez l'option Autonome et associez-la au contrôleur de domaine approprié créé dans la tâche précédente.

Configure Agent



Name *

LAB-Agent

Description

Role ⓘ



Primary



Secondary



Standalone

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

Domain Controller *

10.62.113.247 X



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

Configurer l'agent

Cliquez sur le bouton Enregistrer.

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**

You have unsaved changes Cancel Save

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

i 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			

Enregistrez la configuration

Le résultat .

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**

Cancel Save

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	

Vérifier l'état



Remarque : L'agent d'identité passif indique l'état à l'aide de lignes, l'orange signifie que l'agent n'a jamais communiqué avec le Centre de gestion du pare-feu sécurisé. Une ligne d'agent nouvellement créée est orange et le reste jusqu'à ce que la configuration soit terminée.

Création d'un utilisateur d'Identity Agent passif sur le Secure Firewall Management

Center

Créez un utilisateur Secure Firewall Management Center disposant des autorisations suffisantes pour communiquer avec l'agent d'identité passif. Cet utilisateur dispose de privilèges limités pour effectuer d'autres tâches ; l'utilisateur doit uniquement activer la communication avec l'agent d'identité passif.

Dans l'interface utilisateur de FMC, accédez à Système > Utilisateurs et cliquez sur Créer un utilisateur. Renseignez les détails de l'utilisateur en fonction des exigences de la tâche.

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

Créer un utilisateur

Attribuez uniquement le rôle d'utilisateur Identité passive. Cliquez sur le bouton Enregistrer.

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

sélectionnez l'utilisateur d'identité passive

Installation et configuration du logiciel Passive Identity Agent

Installez et configurez le logiciel Passive Identity Agent sur le contrôleur de domaine désigné.

Téléchargez l'agent d'identité passif depuis 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

Search...

Expand AllCollapse 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	Download Cart File
Installer for the Cisco Passive Identity Agent CiscoPassiveIdentityAgentInstaller-1.1.msi Advisories	11-Mar-2025	2.16 MB	Download Cart File

télécharger le logiciel

Après avoir téléchargé l'agent, commencez le processus d'installation sur le contrôleur de domaine.

Downloads

FileHomeShareView

This PC > Downloads

Quick access

Desktop

Downloads

Documents

Pictures

Cisco Passive Identi

This PC

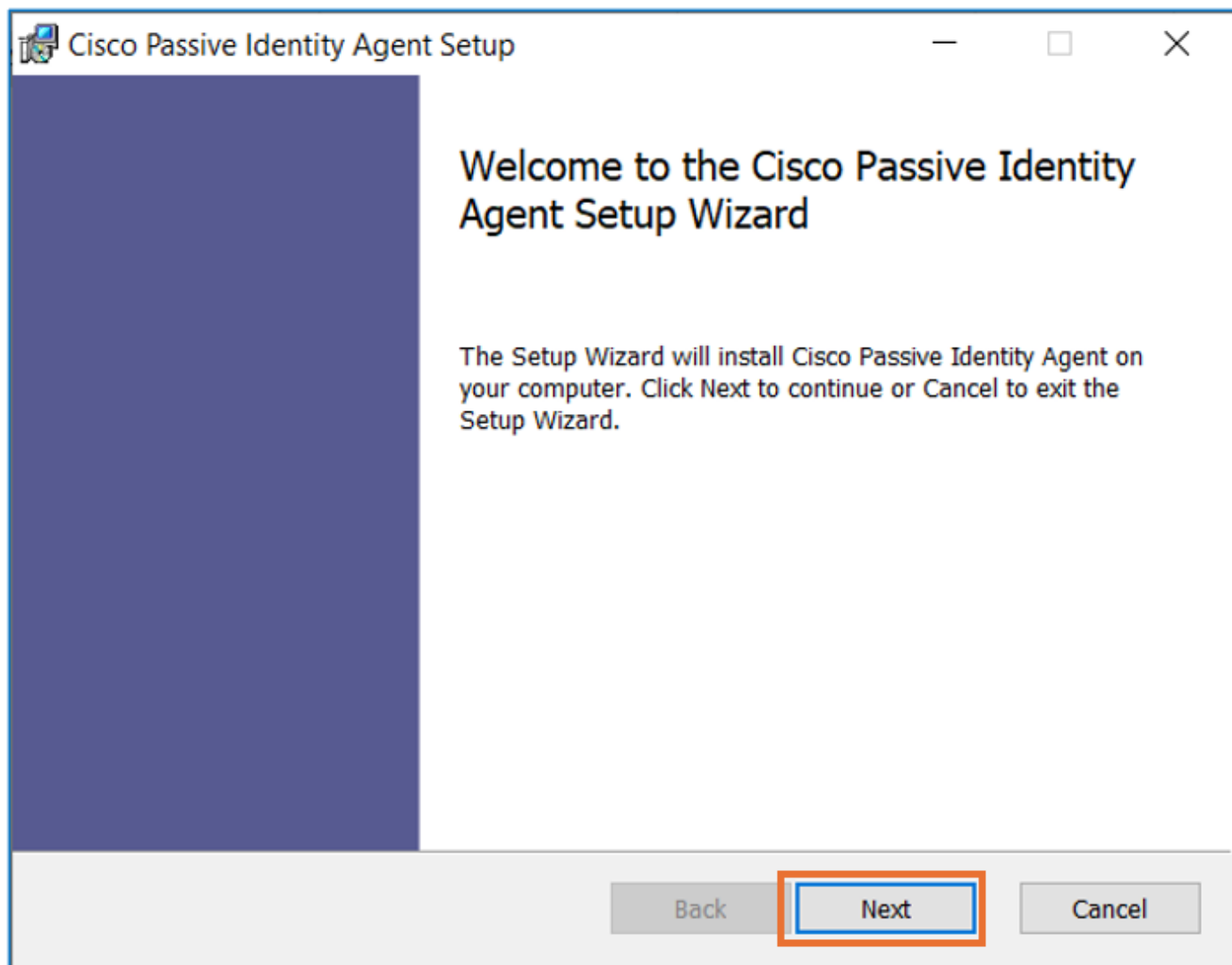
Network

Name	Date modified	Type	Size
CiscoPassiveIdentityAgentInstaller-1.1.1	04-06-2026 06:28	Windows Installer ...	2,276 KB

préposé

]

Reportez-vous aux instructions d'installation fournies pour terminer la configuration.



Install

Une fois l'installation terminée, ouvrez le logiciel Passive Identity Agent et entrez les informations requises comme indiqué dans les exigences de la tâche. Cliquez sur le bouton Test pour vérifier la connectivité avec le FMC.

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

Primary FMC FQDN / IP address **Port**

:

FMC FQDN or IP address and Port of the FMC

Username **Password**

The credentials for the connection (Primary or Secondary)

Agent
LAB-Agent

Q Search

Agent	DCs (Domain Controllers)
LAB-Agent	10.62.113.247

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

I have **Secondary FMC** ▾

**Username/Password
created in previous task**

Click here to test the connectivity

configurez l'agent.

Après avoir testé la connectivité, cliquez sur le bouton Enregistrer.

 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

Search

Agent	DCs (Domain Controllers)
LAB-Agent	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

épreuve

Cliquez sur le bouton OK pour terminer la configuration de l'agent.

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

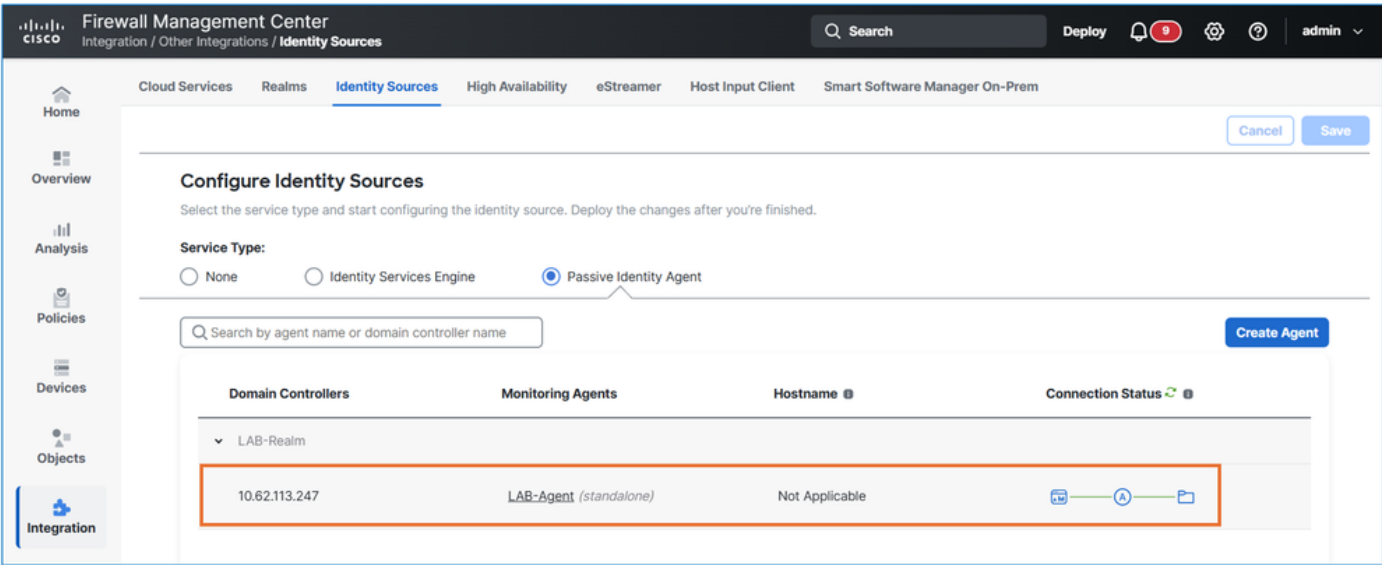
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

l'agent est en cours

Dans l'interface utilisateur de FMC, accédez à Intégration > Autres intégrations > Sources d'identité > Agent d'identité passif. Vérifiez que l'agent d'identité passif affiche un état vert.



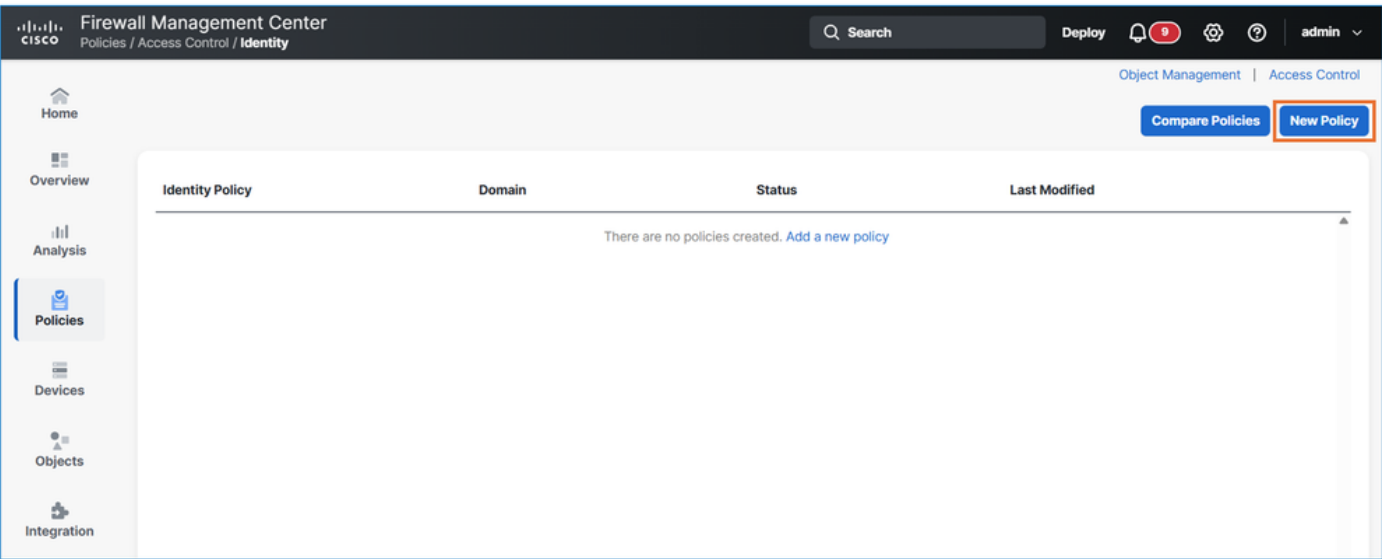
vérification de la communication de fmc

Configurer les stratégies d'identité

Créez une politique d'identité basée sur la table fournie.

Nom de stratégie	Nom de règle	Domaine d'authentification	Paramètres restants
LAB-Identity-Policy	Règle1	Domaine de travaux pratiques	Laisser par défaut

Dans l'interface utilisateur de FMC, accédez à Politiques > Contrôle d'accès > Identité. Cliquez sur le bouton Nouvelle stratégie.



nouvelle police

Entrez le nom de la stratégie en fonction des exigences de la tâche.

New Identity policy

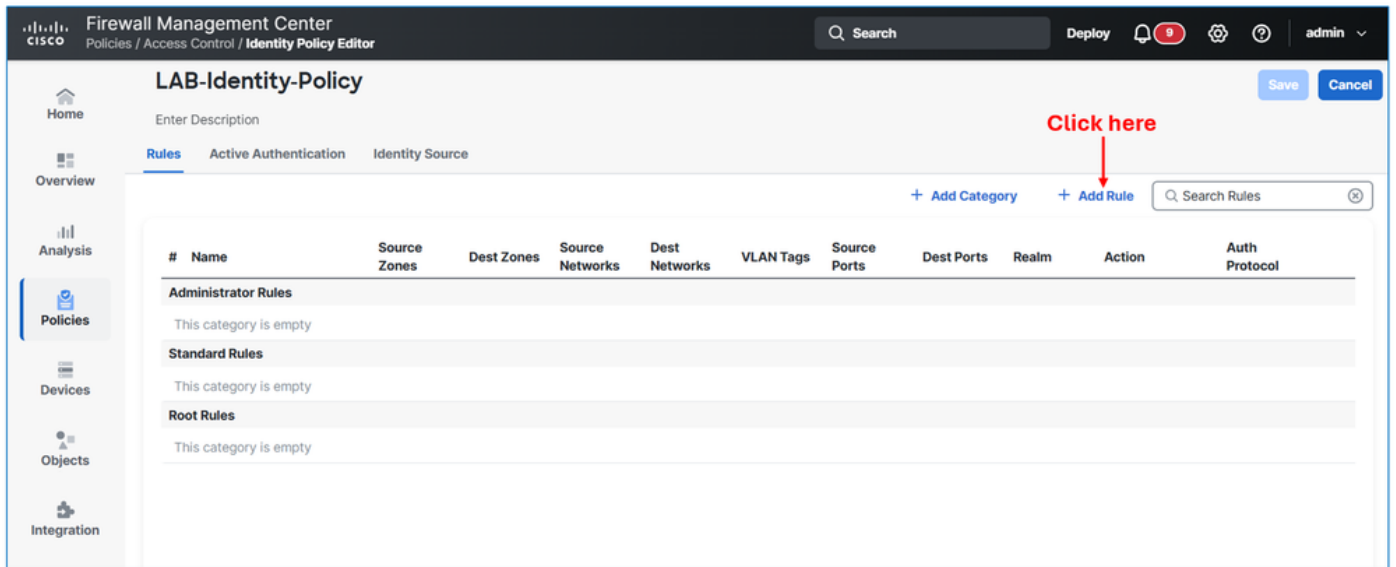
Name

Description

Cancel **Save**

nouvelle police

Cliquez sur le bouton Ajouter une règle.



créer une règle

Accédez à l'onglet **Domaine** et paramètres et sélectionnez le domaine d'authentification en fonction des exigences de tâche. Enfin, cliquez sur le bouton **Ajouter**.

Add Rule

Name
☒ 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

Authentication Realm *

LAB-Realm (AD)

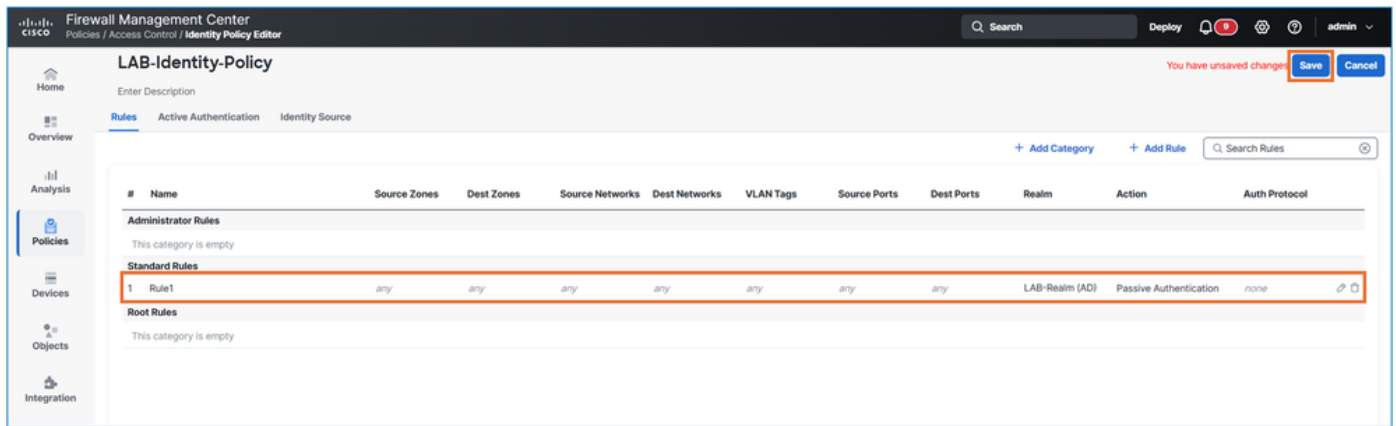
☐ Use active authentication if passive or VPN identity cannot be established

Cancel

Add

Paramètre du domaine

Cliquez sur le bouton **Enregistrer**.



enregistrez la configuration

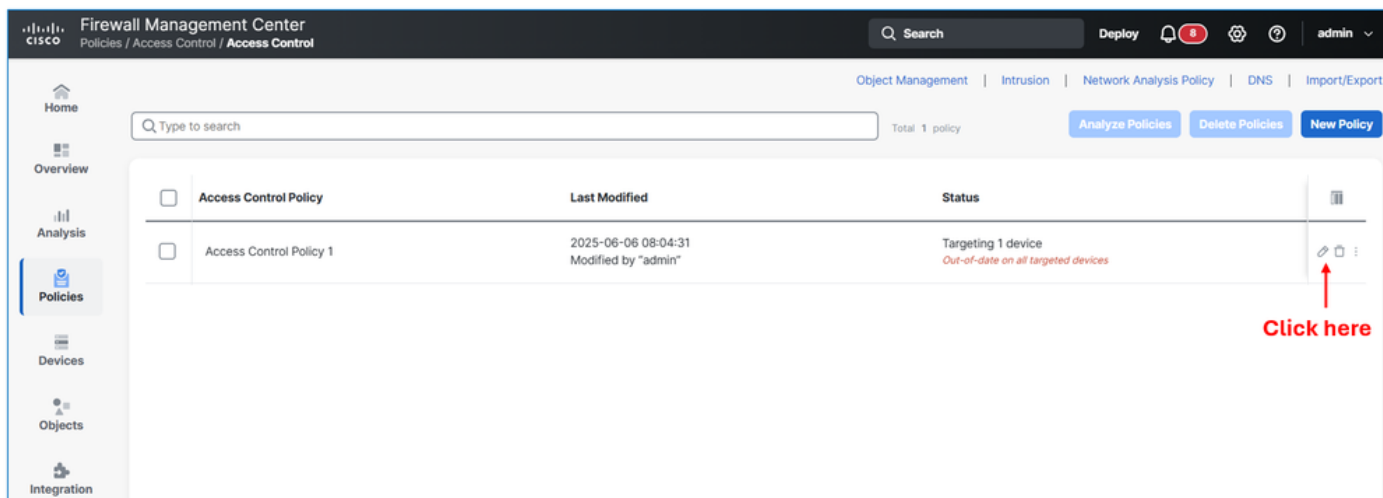
Configurer les stratégies de contrôle d'accès

Liez la stratégie d'identité à la stratégie de contrôle d'accès et créez une règle de stratégie d'accès avec les attributs suivants :

Nom d'attribut	Valeur
Nom de règle	Règle1
Action	Allow
Zone source	Intérieur
Zone de destination	Extérieur
Réseaux sources	10.10.10.0/24
Réseaux de destination	10.48.62.98/32
Service	Port de destination TCP 80 (HTTP)
Utilisateurs	LAB-Realm/GROUPE1
Journalisation	À la fin de la connexion

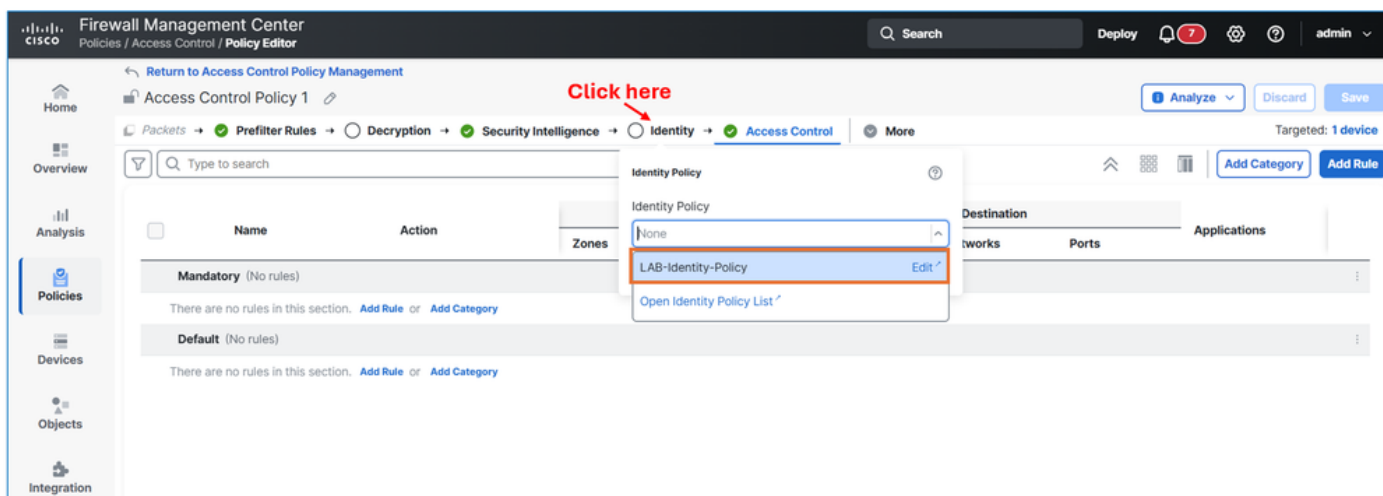
Étape 1. Lier la stratégie d'identité à la stratégie de contrôle d'accès

Dans l'interface utilisateur de FMC, accédez à Politiques > Contrôle d'accès > Contrôle d'accès. Cliquez sur le bouton Modifier correspondant à votre stratégie.



Modifier la stratégie

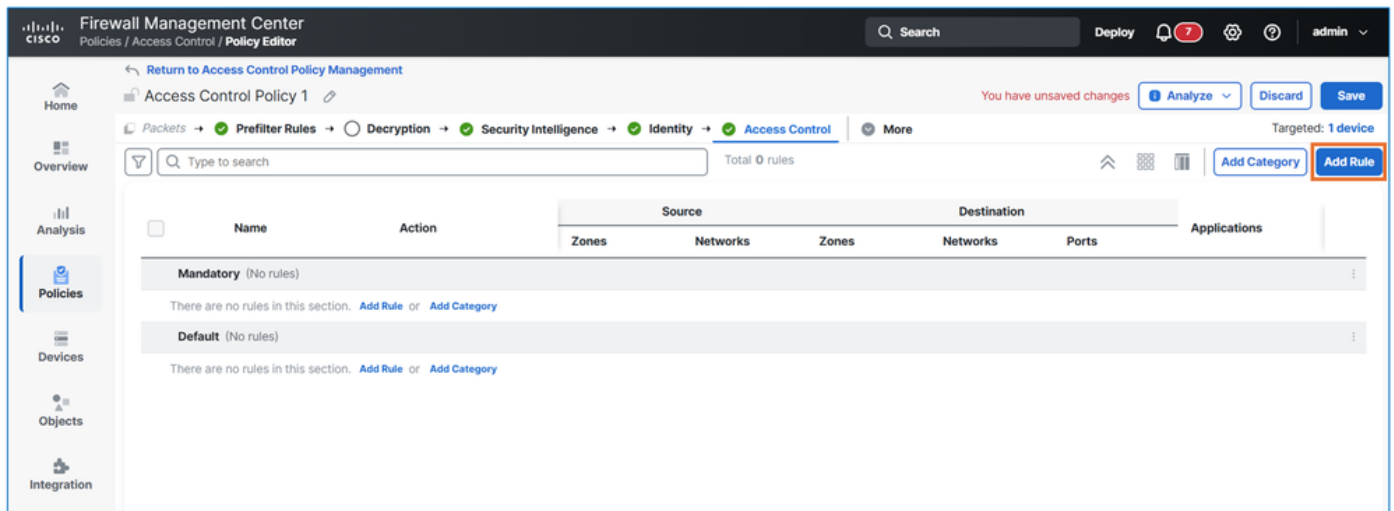
Accédez à la section Identité et liez la politique d'identité créée dans la tâche précédente.



ajouter une stratégie d'identité

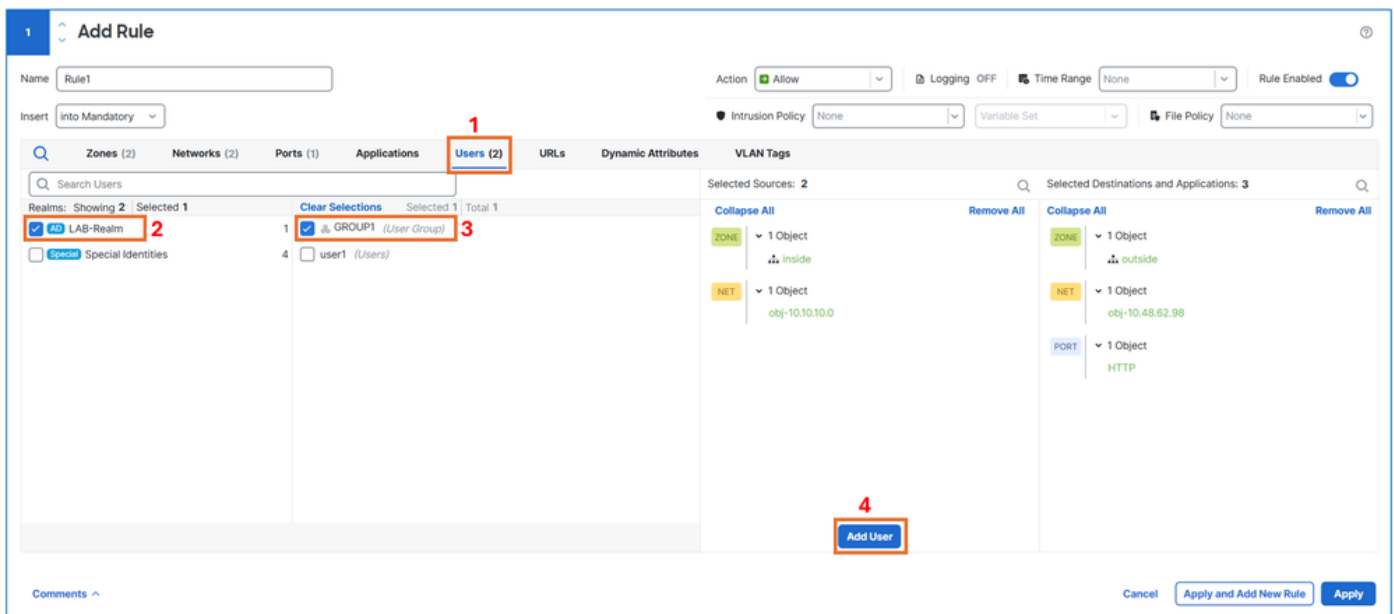
Cliquez sur le bouton Appliquer

Étape 2 : création de la règle de contrôle d'accès.



créer ACP

Entrez les détails en fonction des exigences de la tâche et, plus important encore, sous l'onglet Utilisateurs, addGROUP1fromLAB-Realm.



ajouter des utilisateurs à la règle

Activez la journalisation pour la règle en sélectionnant Log à la fin de la connexion.

1 Add Rule

Name:

Action: Logging: ☒ ON Time Range: Rule Enabled: ☒

Insert:

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:

Realms: Showing 2 | Selected 1

☒ AD LAB-Realm

☐ Special Special Identities

Users: Total 1

1 ☐ GROUP1 (User Group)

4 ☐ user1 (Users)

Selected Sources: 3

Zone: 1 Object

☒ inside

Net: 1 Object

☒ obj-10.10.10.0

User: 1 Group

☒ AD LAB-R

activer la journalisation

Étape 3 : activation de la journalisation de l'action par défaut

Cliquez sur cette icône pour modifier les paramètres de consignment des actions par défaut.

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

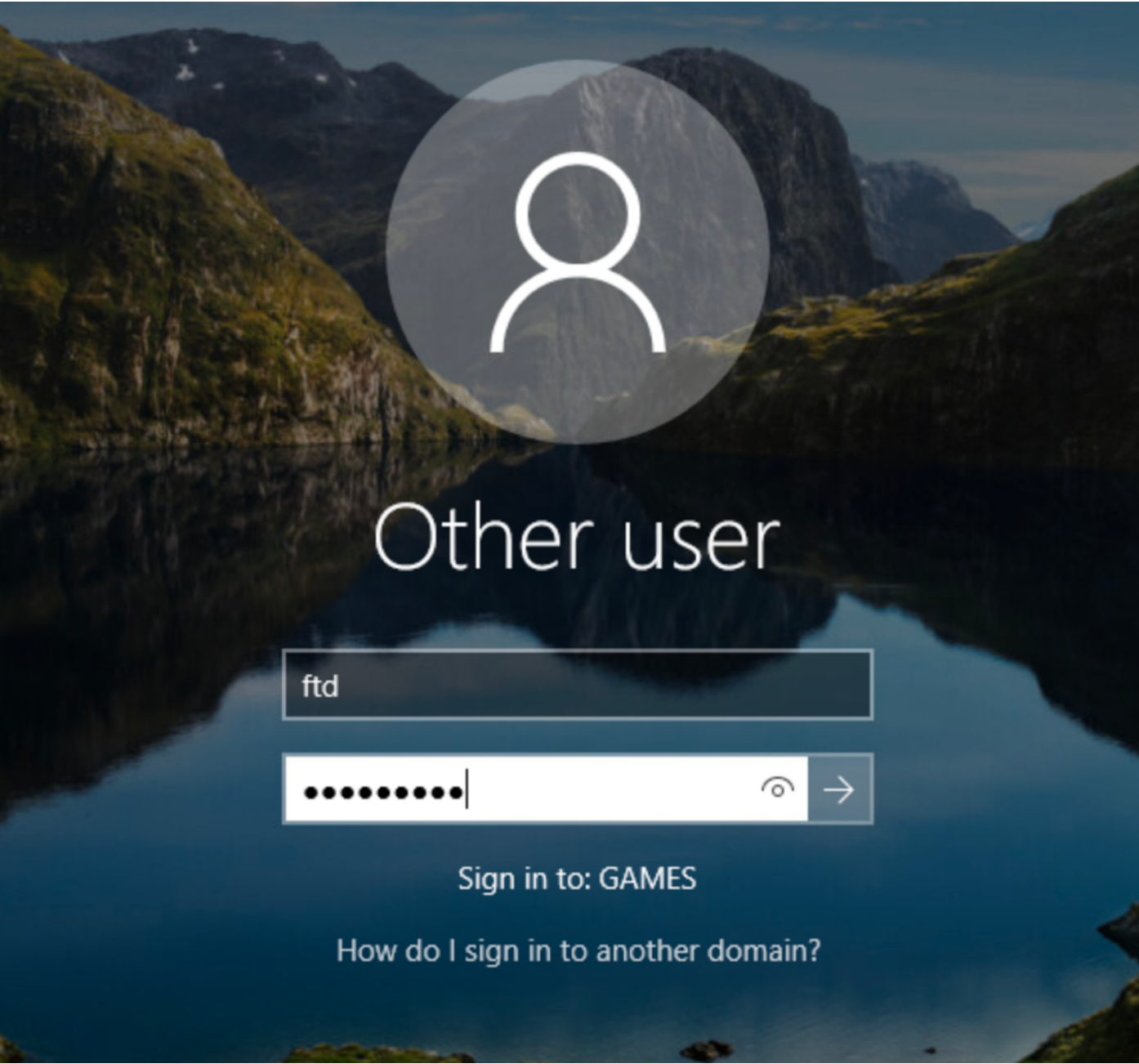
Activer la journalisation

Enregistrer et déployer la configuration sur le FTD.

Vérification

Vérifiez l'opération d'identité passive en confirmant que le trafic est autorisé exclusivement pour ftd.

Connectez-vous à l'utilisateur du domaine à partir de l'ordinateur utilisateur.



login utilisateur

Une fois qu'un utilisateur s'est connecté avec succès, vérifiez à partir de FMC sous Analysis> user >active session pour afficher les détails de l'utilisateur actif.

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	

Après avoir initié une vérification du trafic à partir des événements de connexion, consultez les détails de l'utilisateur dans les événements de connexion.

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		

Dépannage

Vérification des journaux des agents

Sur l'ordinateur Windows hébergeant l'agent, ouvrez Task Manager et vérifiez que le processus en arrière-planCiscoPassiveIdentityAgentService est en cours d'exécution.

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

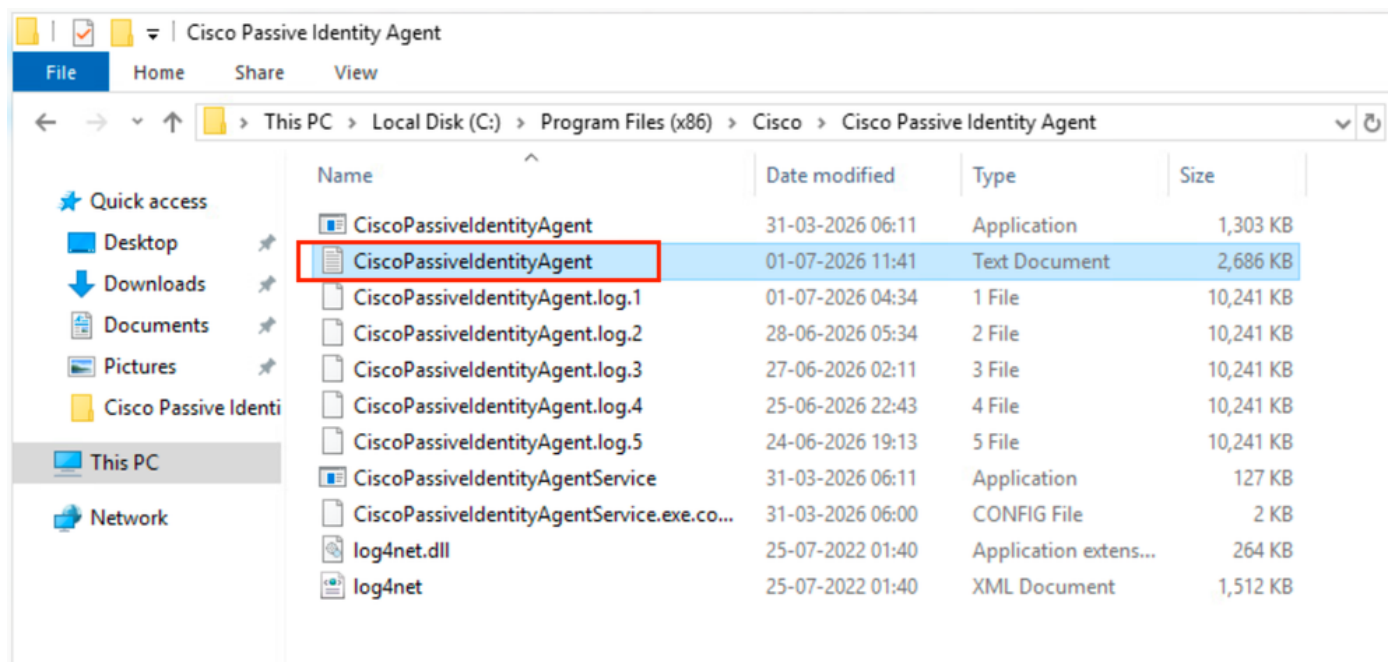
⬆

Fewer details

End task

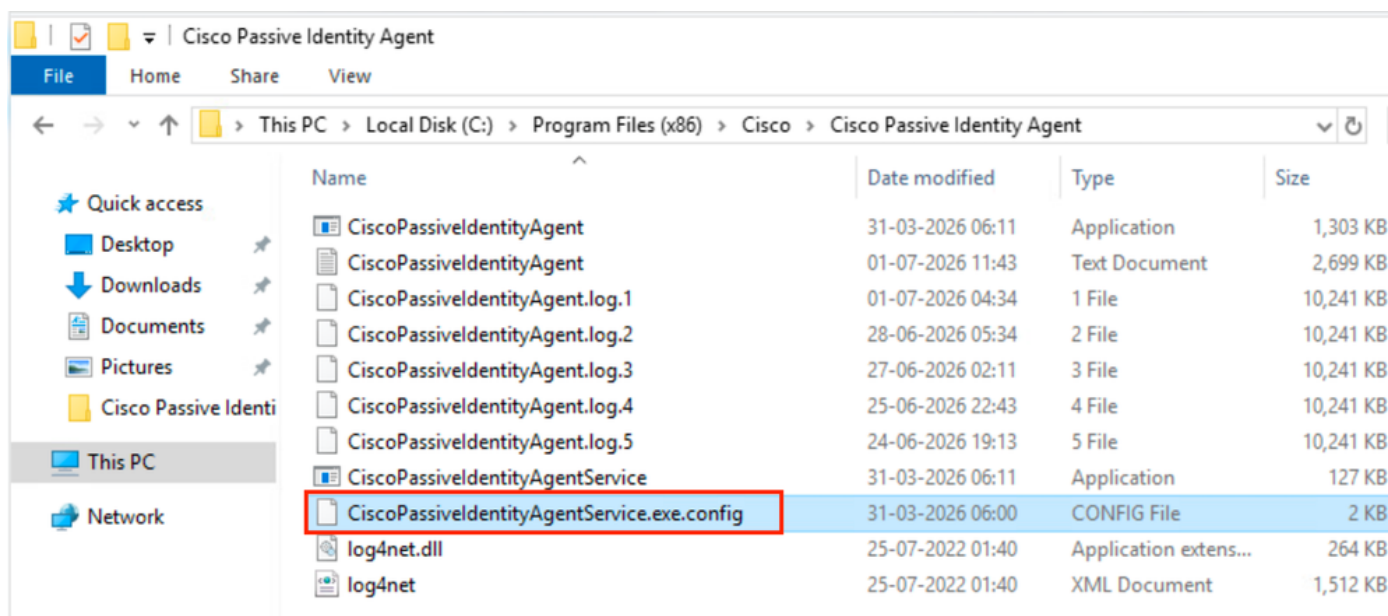
Tâche en cours

Les journaux de l'agent se trouvent dans les fichiers CiscoPassiveIdentityAgent, situés par défaut à l'adresse suivante : "C:\Program Fichiers (x86)\Cisco\Cisco Passive Identity Agent\".



préposé

Par défaut, les journaux de l'agent sont définis sur le niveau INFO. Pour activer la journalisation de niveau DEBUG, modifiez le fichier CiscoPassiveIdentityAgentService.exe.config et définissez le niveau de journalisation sur ALL ou DEBUG.



configuration de l'agent



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler, log4ne
  </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>
```

journal d'information

Vérification des journaux des agents - Récupérer la configuration des agents.

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

INFO Rest Client, état du mappage : OK

INFO Rest Client, REST post successful for userBatch fdm, latency = 0, current DC TIME in UTC :
01/07/2026 19:47:34 UTILISATEUR connecté

INFO Rest Client, Demande de configuration de l'agent

Journaux FMC

Exécutez cette commande pour vérifier si le mappage utilisateur-IP a été reçu de l'agent.

```

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#

```

sortie fmc

Si la commande précédente n'affiche aucun mappage, collectez ces journaux et contactez le centre d'assistance technique Cisco.

Il s'agit d'une liste de journaux pertinents pour l'API FMC. La grue de quenouilles les englobe toutes.

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.