

Configuración del agente de identidad pasivo mediante FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuraciones](#)

[Configuración de un Origen de Agente de Identidad Pasivo](#)

[Creación de un usuario pasivo de Identity Agent en Secure Firewall Management Center](#)

[Instalación y configuración del software Passive Identity Agent](#)

[Configurar políticas de identidad](#)

[Configurar políticas de control de acceso](#)

[Verificación](#)

[Resolución de problemas](#)

[Comprobando registros de agentes](#)

[Registros de FMC](#)

Introducción

Este documento describe cómo configurar el Origen de agente de identidad pasivo que envía datos de sesión a FMC

Prerequisites

Requirements

- Cisco Secure Firewall Management Center con versión 7.6+
- Cisco Secure Firewall con versión 7.6+
- Servidor de Windows Active Directory, el servidor debe ejecutar Windows Server 2008 o posterior.
- Debe activar Snort 3 en los dispositivos de Secure Firewall Threat Defence.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

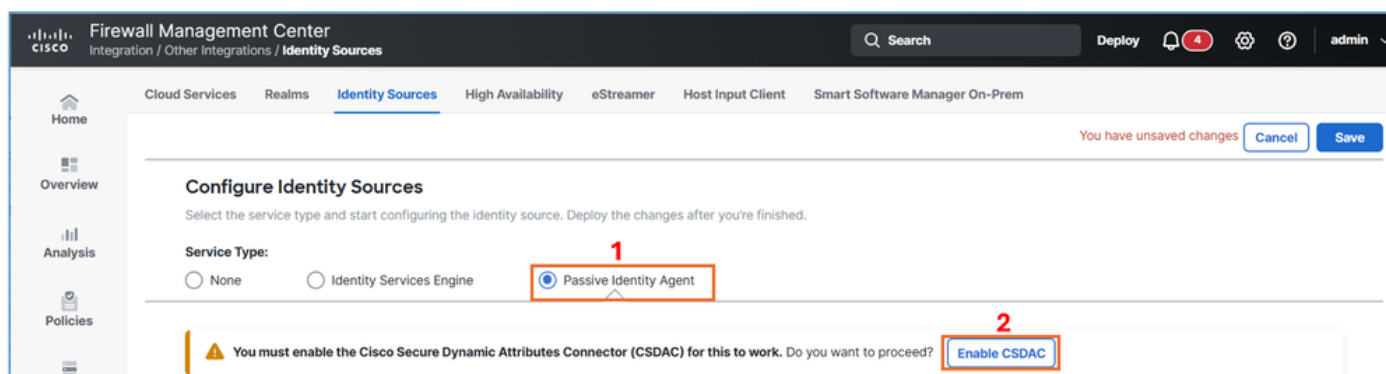
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuraciones

Antes de configurar el agente, complete la integración de AD y FMC.

Configuración de un Origen de Agente de Identidad Pasivo

En la interfaz de usuario de FMC, vaya a Integración > Otras integraciones > Orígenes de identidad, haga clic en Agente de identidad pasivo. Si Cisco Secure Dynamic Attributes Connector aún no se ha habilitado, se le pedirá que lo haga haciendo clic en Enable CSDAC.



Agente de identidad pasivo

Haga clic en el botón Enable (Activar) para activar CSDAC.

Enable Cisco Secure Dynamic Attributes Connector?



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

Cancel

Enable

Habilitar CSDAC

Este paso dura aproximadamente 10 minutos. Una vez que CSDAC esté habilitado correctamente, haga clic en el botón Finalizado para continuar.

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 activado

Haga clic en el botón Crear agente.

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?

```

    graph LR
      FMC[Firewall Management Center] -- 1 --> Agents[Primary Agent / Secondary Agent]
      Agents -- 2 --> DC[ACTIVE DIRECTORY DOMAIN CONTROLLERS]
      DC -- 3 --> Agents
      Agents -- 4 --> FMC
      Agents -- 5 --> Agents
  
```

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](#)

Crear agente

Defina un nombre para el agente, seleccione la opción Standalone y asócielo al controlador de dominio adecuado creado en la tarea anterior.

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

Configurar agente

Haga clic en el botón Guardar.

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**

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

Information: 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			

Guarde la configuración

El resultado.

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**

[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	

Verificar el estado



Nota: El agente de identidad pasivo indica el estado mediante líneas; el color ámbar significa que el agente nunca se ha comunicado correctamente con Secure Firewall Management Center. Una línea de agente recién creada es de color ámbar y permanece así hasta que se completa la configuración.

Creación de un usuario pasivo de Identity Agent en Secure Firewall Management

Center

Cree un usuario de Secure Firewall Management Center con permisos suficientes para comunicarse con el agente de identidad pasivo. Este usuario tiene privilegios limitados para realizar otras tareas; se espera que el usuario sólo habilite la comunicación con el agente de identidad pasivo.

En la interfaz de usuario de FMC, vaya a Sistema > Usuarios y haga clic en Crear usuario. Rellene los detalles del usuario de acuerdo con los requisitos de la tarea.

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

Crear usuario

Asigne solo la función de usuario de identidad pasiva. Haga clic en el botón Guardar.

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

seleccione el usuario de identidad pasiva

Instalación y configuración del software Passive Identity Agent

Instale y configure el software Passive Identity Agent en el controlador de dominio designado.

Descargue el agente de identidad pasivo de 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

descargar el software

Después de descargar el agente, inicie el proceso de instalación en el controlador de dominio.

Downloads

FileHomeShareView

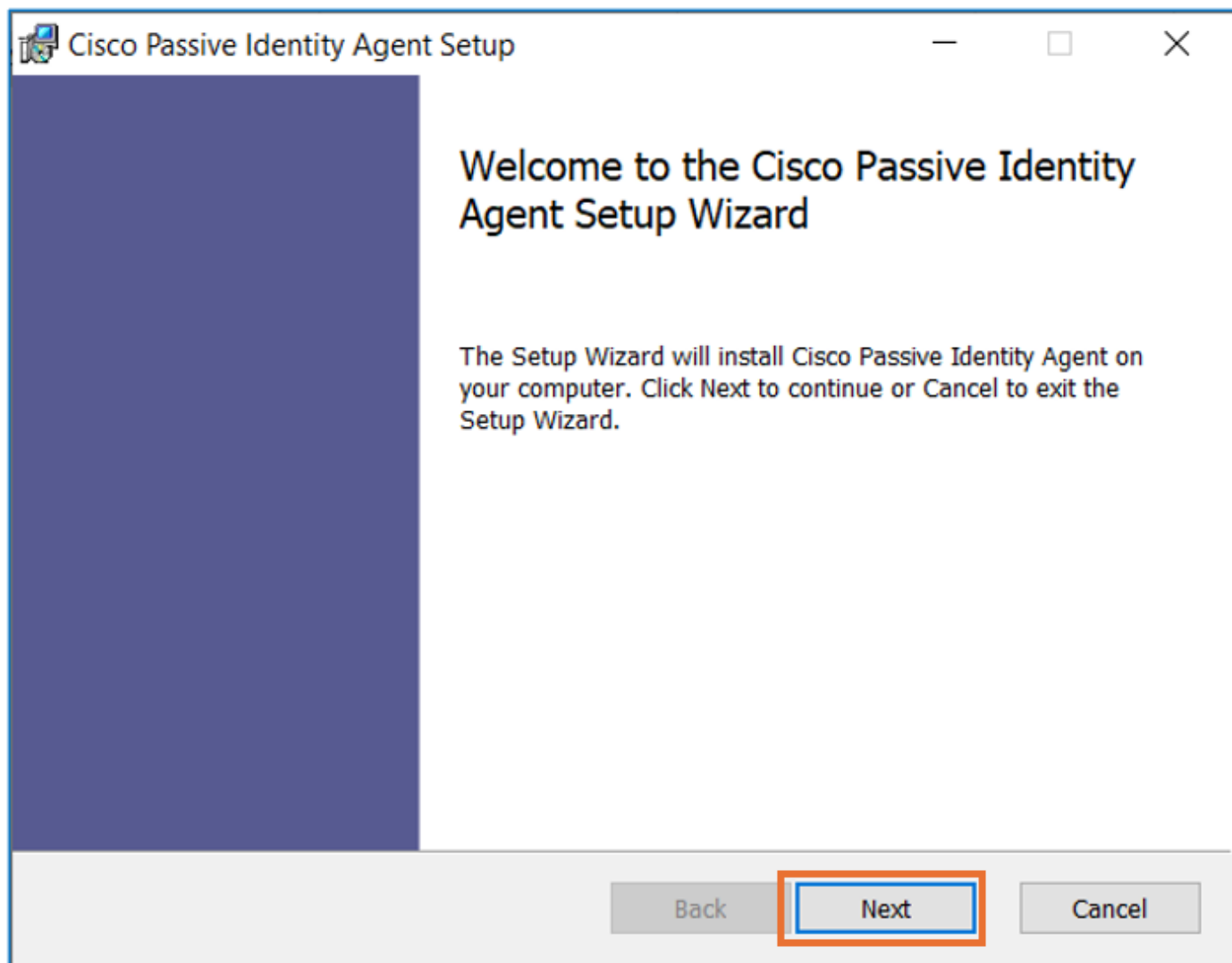
This PC > Downloads

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

agente

]

Consulte las instrucciones de instalación proporcionadas para completar la instalación.



Instalar

Una vez finalizada la instalación, abra el software Passive Identity Agent e introduzca la información necesaria tal y como se especifica en los requisitos de la tarea. Haga clic en el botón Test para verificar la conectividad con el 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

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

Click here to test the connectivity

I have Secondary FMC ▾

Save Cancel

configure el agente.

Después de probar correctamente la conectividad, haga clic en el botón Guardar.

Cisco

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

C

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

prueba

Haga clic en el botón Aceptar para completar la configuración del agente.

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

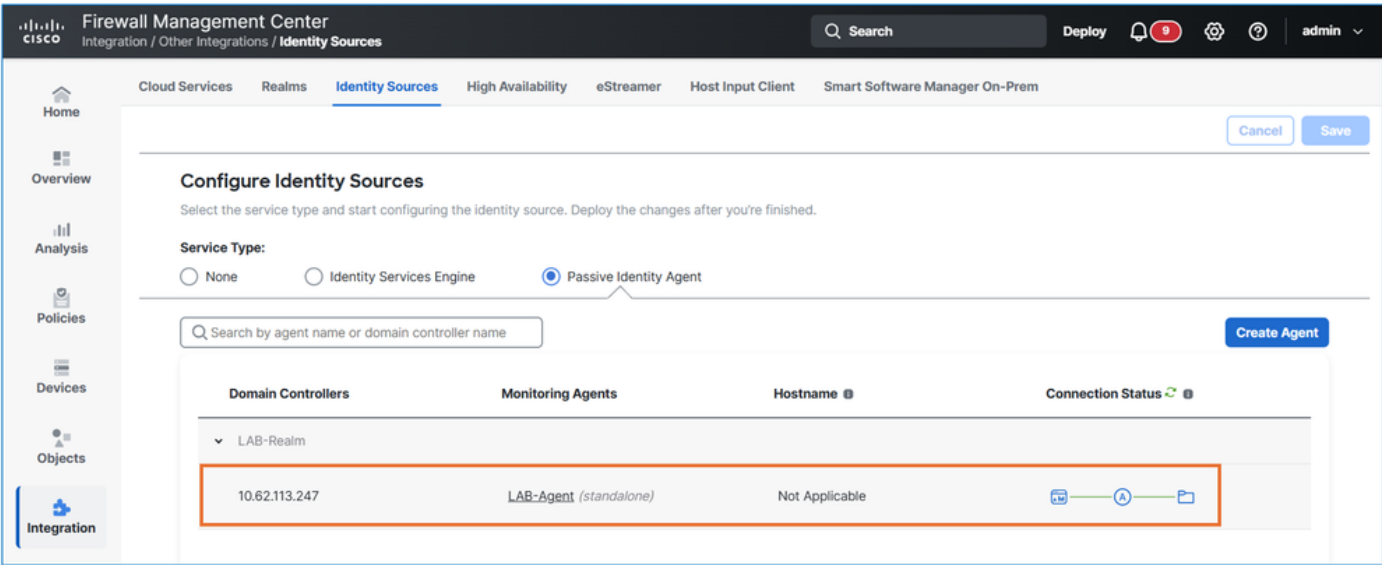
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

el agente se está ejecutando

En la interfaz de usuario de FMC, navegue hasta Integración > Otras integraciones > Orígenes de identidad > Agente de identidad pasivo. Confirme que el Agente de identidad pasivo muestra un estado verde.



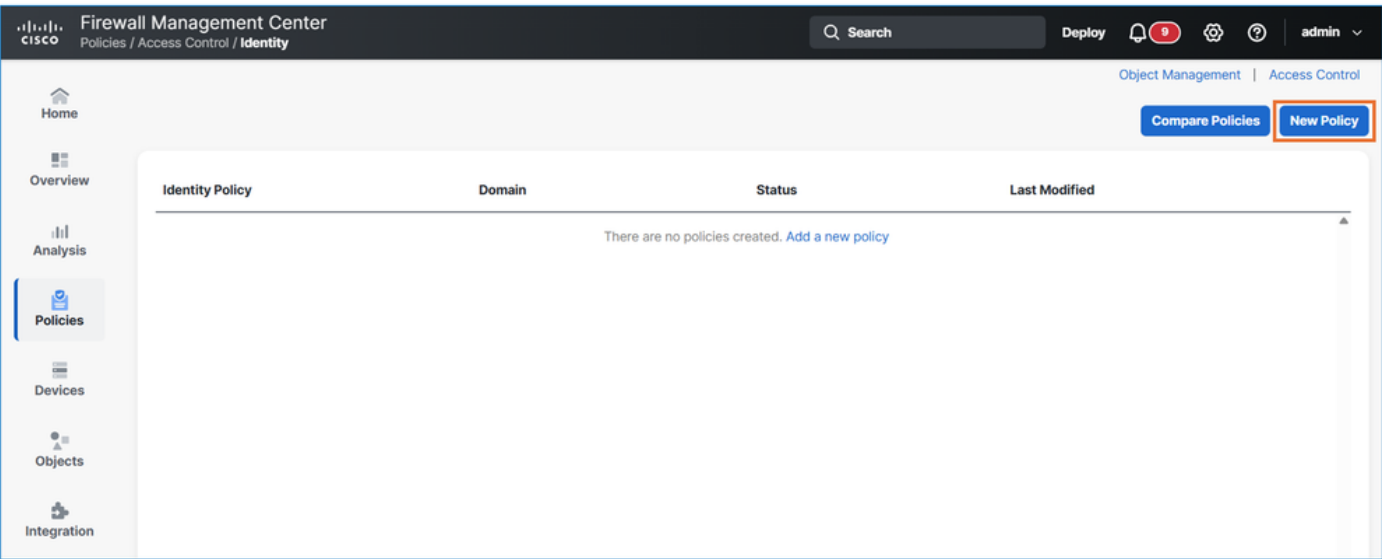
verificar la comunicación desde fmc

Configurar políticas de identidad

Cree una política de identidad basada en la tabla proporcionada.

Nombre de política	Nombre de regla	Rango de autenticación	Configuración restante
LAB-Identity-Policy	Regla1	LAB-Realm	Dejar como predeterminado

En la interfaz de usuario de FMC, vaya aPolíticas > Control de acceso > Identidad. Haga clic en el botónNueva directiva.



nueva política

Ingrese el nombre de la política de acuerdo con los requisitos de la tarea.

New Identity policy

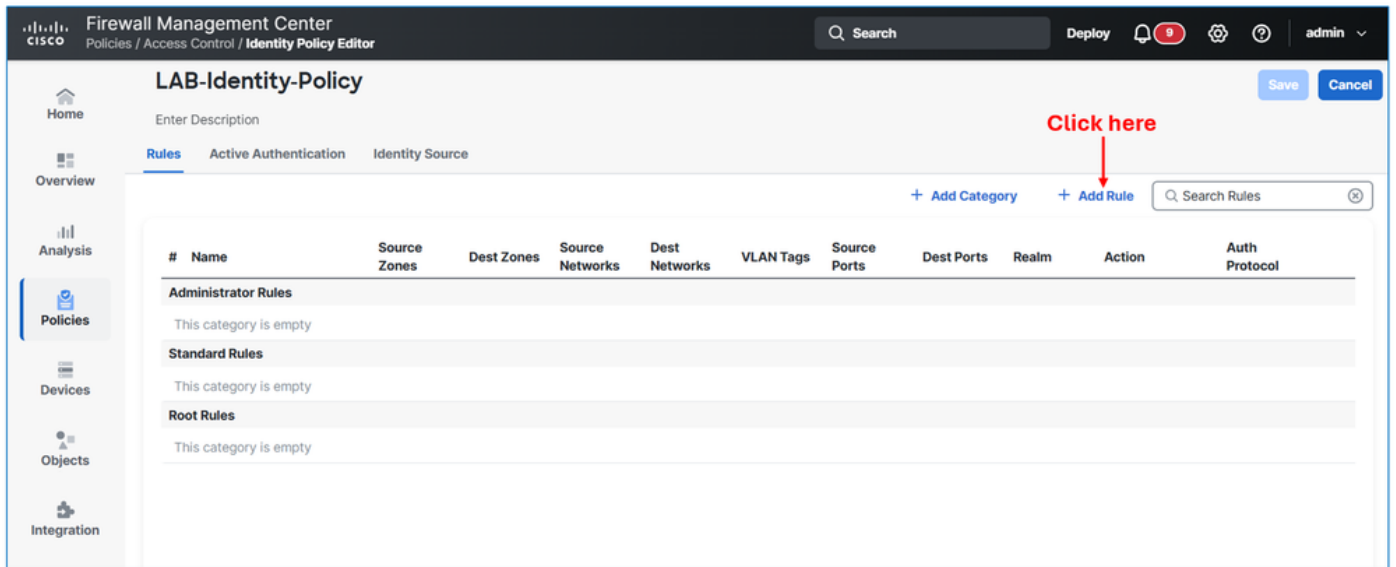
Name

Description

CancelSave

nueva política

Haga clic en el botón Agregar regla.

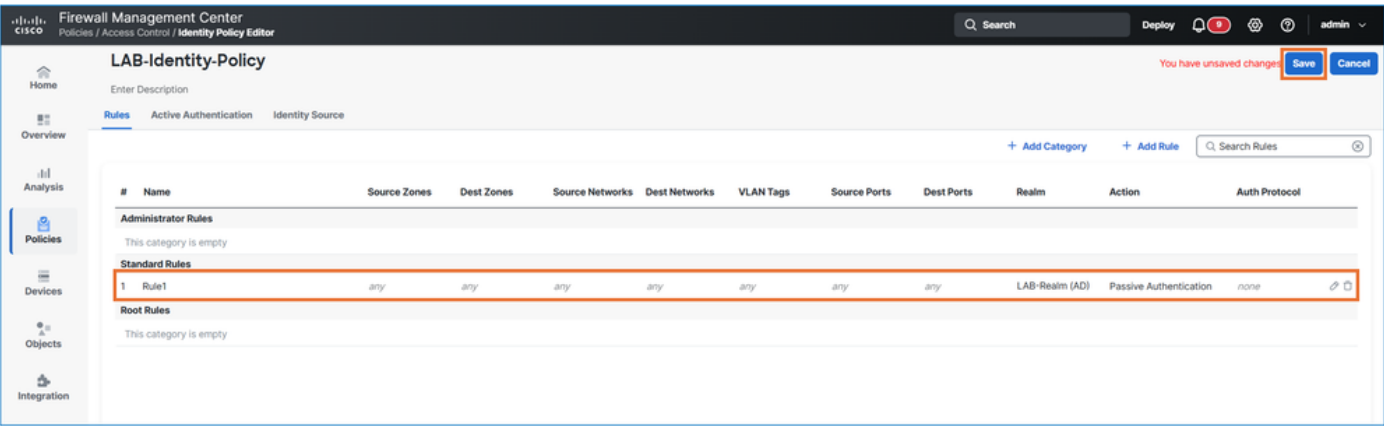


crear regla

Navegue hasta la pestaña Rango y Configuración y seleccione el rango de autenticación en función de los requisitos de la tarea. Por último, haga clic en el botón Agregar.

Configuración de rango

Haga clic en el botón Guardar.



guardar la configuración

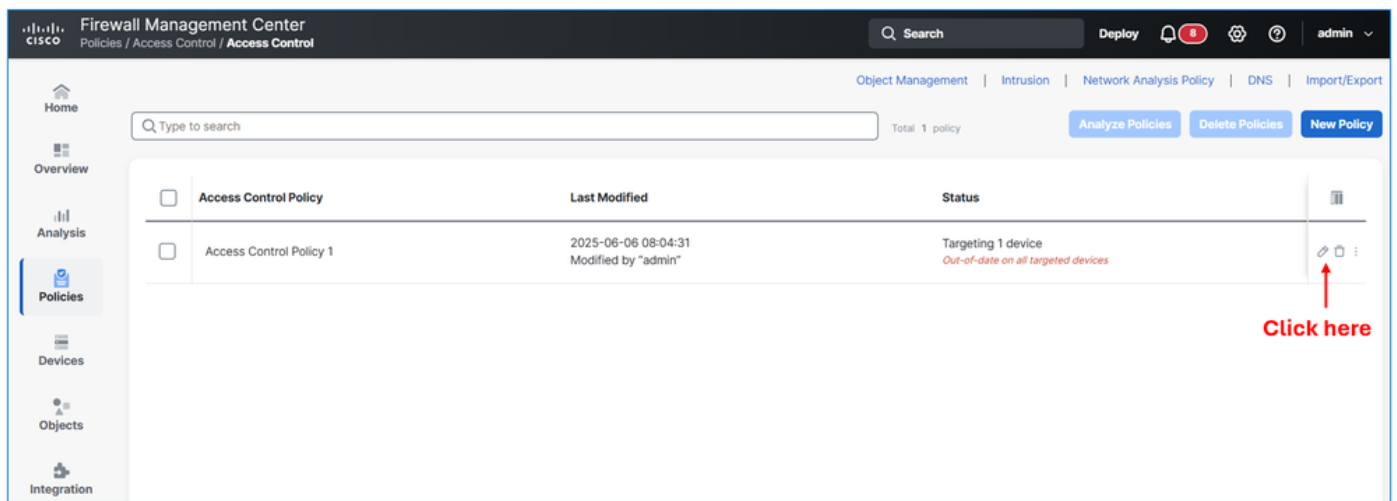
Configurar políticas de control de acceso

Vincule la política de identidad a la política de control de acceso Access y cree una regla de política de acceso con los atributos:

Nombre del atributo	Valor
Nombre de regla	Regla1
Acción	Permiso
Zona de origen	Dentro
Zona de destino	Fuera
Redes de origen	10.10.10.0/24
Redes de destino	10.48.62.98/32
Servicio	Puerto de destino TCP 80 (HTTP)
Usuarios	LAB-Realm/GROUP1
Registro	Al final de la conexión

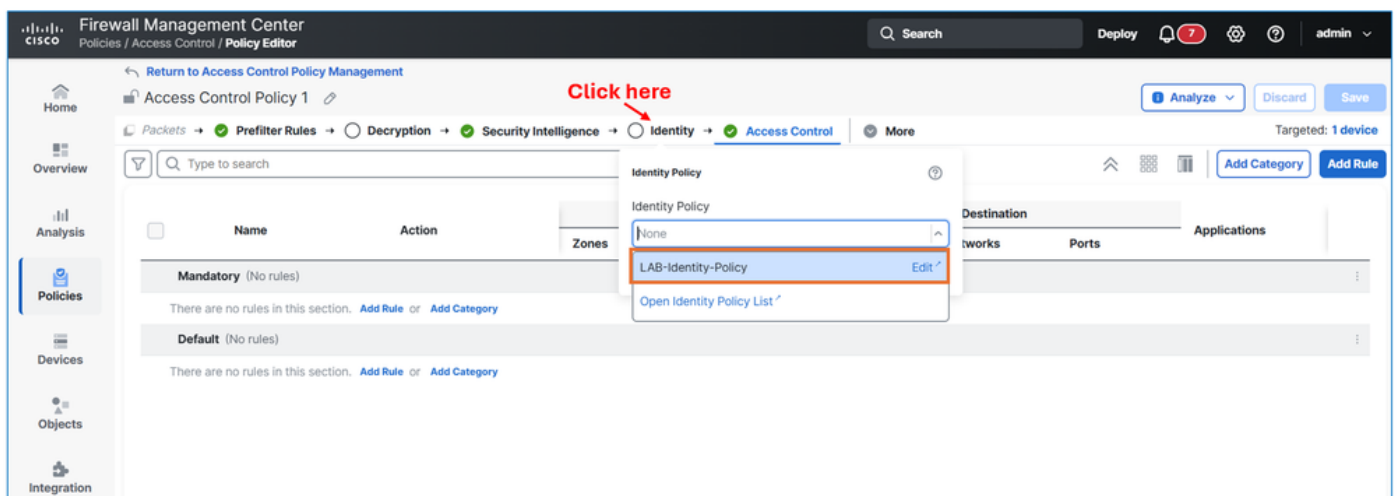
Paso 1. Vincular la Política de Identidad a la Política de Control de Acceso

En la interfaz de usuario de FMC, vaya a Políticas > Control de acceso > Control de acceso. Haga clic en el botón Editar de la directiva.



Editar directiva

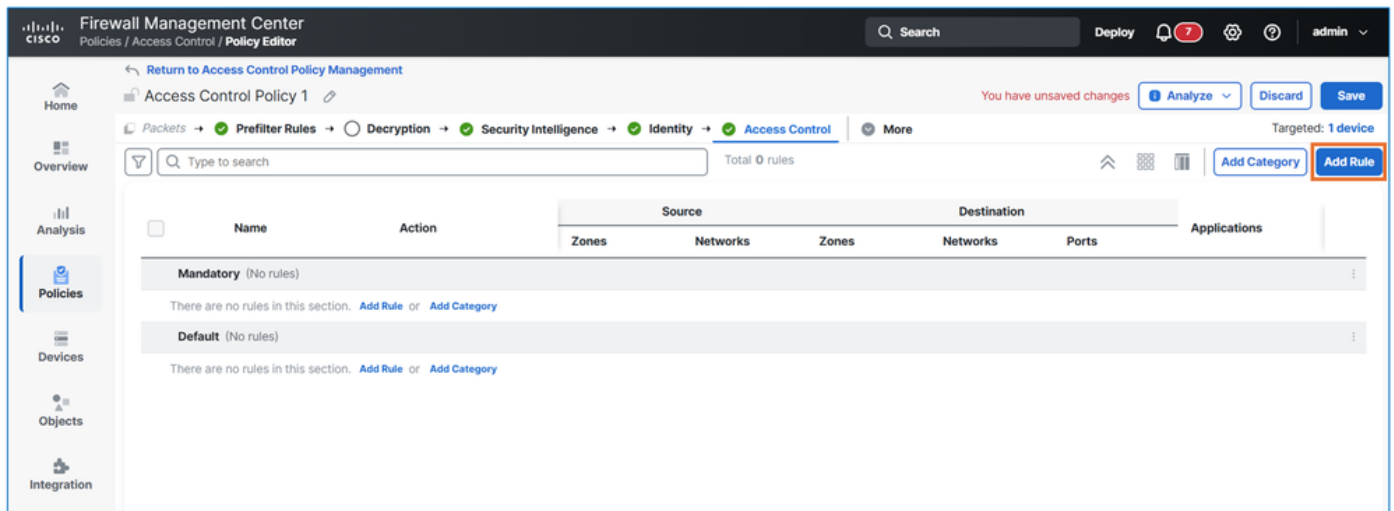
Navegue hasta la sección Identidad y vincule la Política de Identidad creada en la tarea anterior.



agregar política de identidad

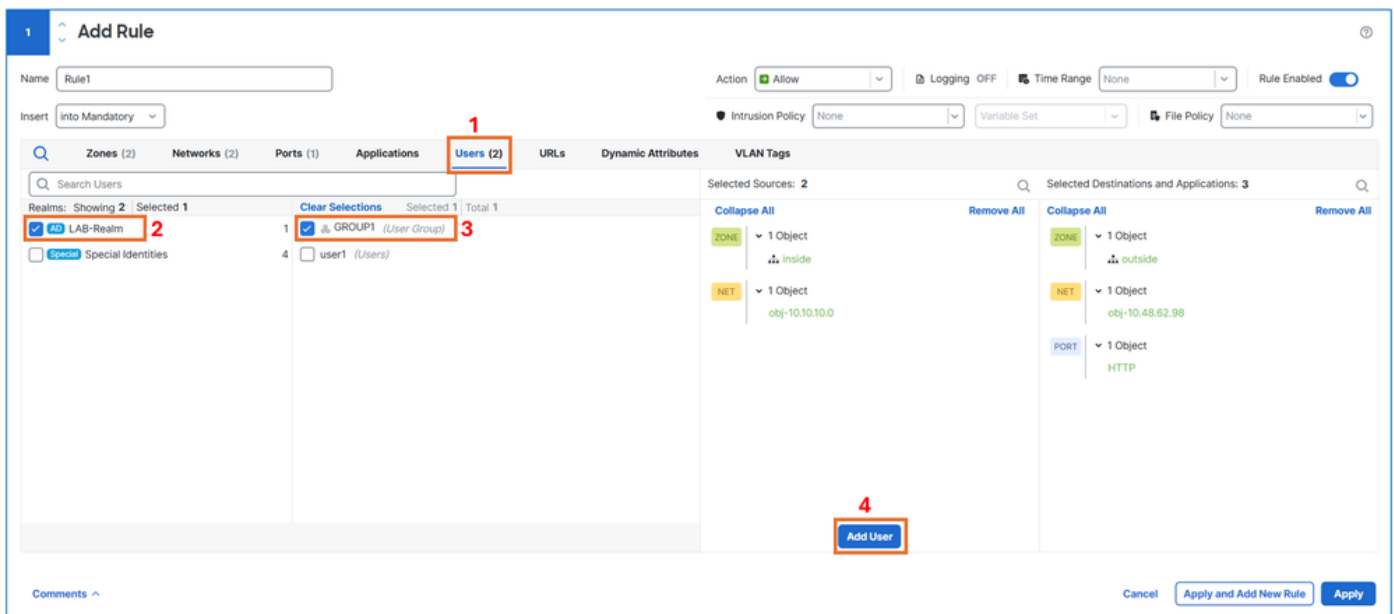
Haga clic en el botónAplicar

Paso 2. Cree la regla de control de acceso.



crear ACP

Introduzca los detalles según los requisitos de la tarea y, lo que es más importante, en la ficha Usuario, addGROUP1fromLAB-Realm.



agregar usuarios a la regla

Active el registro de la regla seleccionando Registro al final de la conexión.

1 Add Rule

Name:

Insert:

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

Intrusion Policy:

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:

File Policy

Realms: Showing 2 Selected 1

☒ AD LAB-Realm

☐ Special Special Identities

Users: Total 1

1 ☐ GROUP1 (User Group)

4 ☐ user1 (Users)

VLAN Tags

Selected Sources: 3

Collapse All

ZONE

1 Object

inside

NET

1 Object

obj-10.10.10.0

USER

1 Group

AD LAB-R

Comments ^

enable logging

Paso 3. Habilite el registro para la acción predeterminada.

Haga clic en el icono Configuración para modificar la configuración de registro de acciones predeterminada.

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

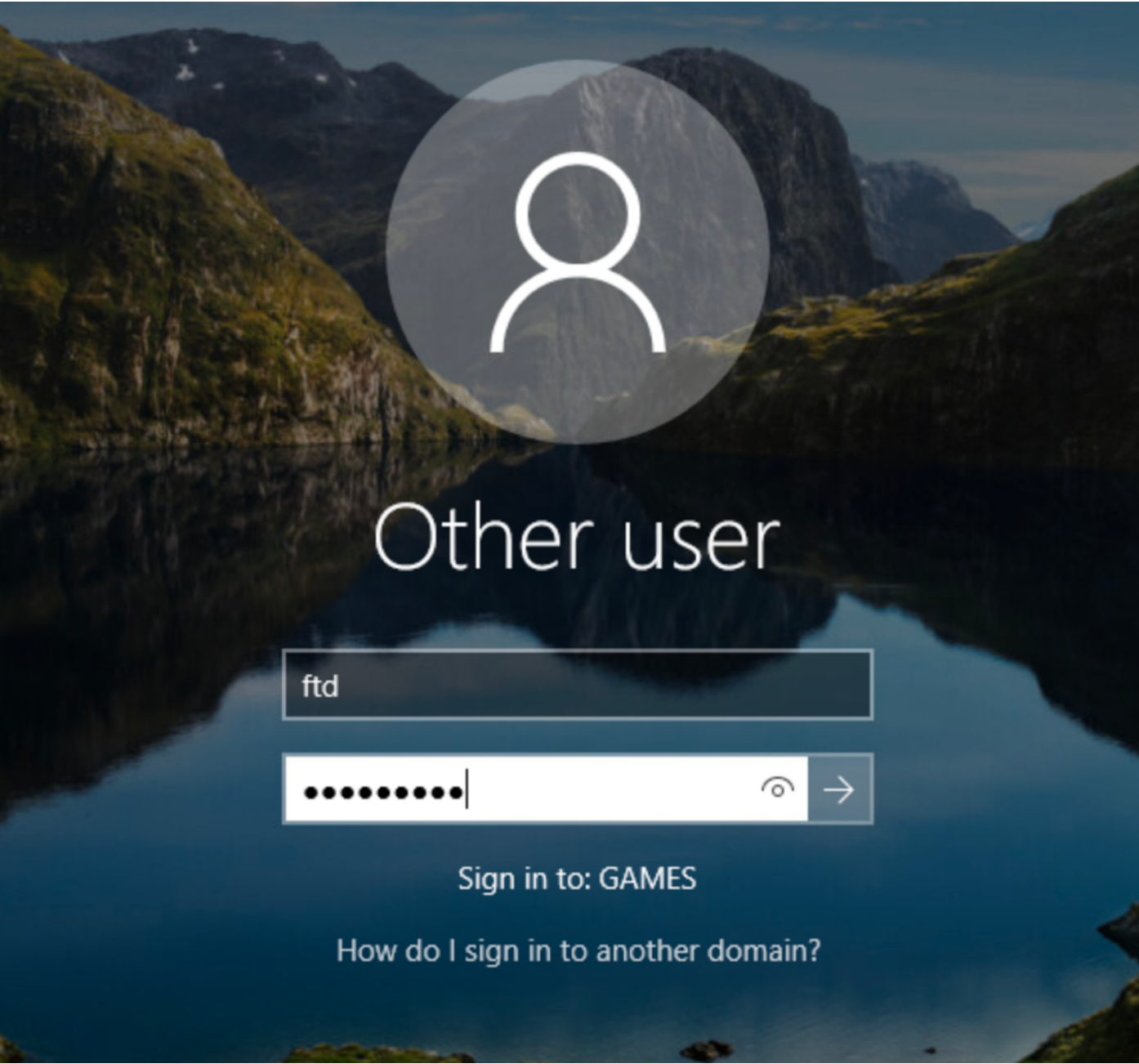
Activar registro

Guarde e implemente la configuración en el FTD.

Verificación

Verifique la operación de identidad pasiva confirmando que el tráfico está permitido exclusivamente para ftd.

Inicie sesión en el dominio user desde el equipo del usuario.



inicio de sesión del usuario

Después de que un usuario inicie sesión correctamente, verifique desde FMC en Analysis> user >active session para ver los detalles del usuario activo.

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	

Después de iniciar la verificación del tráfico a partir de los eventos de conexión, consulte los detalles del usuario en los eventos de conexión.

Connection Events (switch workflow)

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

Expanding

No Search Constraints (Edit Search)

Connections with Application Details

Table View of Connection Events

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		hfd (Directory/hfd, 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		hfd (Directory/hfd, 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		hfd (Directory/hfd, 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		hfd (Directory/hfd, LDAP)	10.197.227.16			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		

Sesiones activas

Resolución de problemas

Comprobando registros de agentes

En la máquina con Windows que aloja el agente, abra Task Manager y verifique que el proceso en segundo plano CiscoPassiveIdentityAgentService se esté ejecutando.

Task Manager

File Options View

Processes

Performance

Users

Details

Services

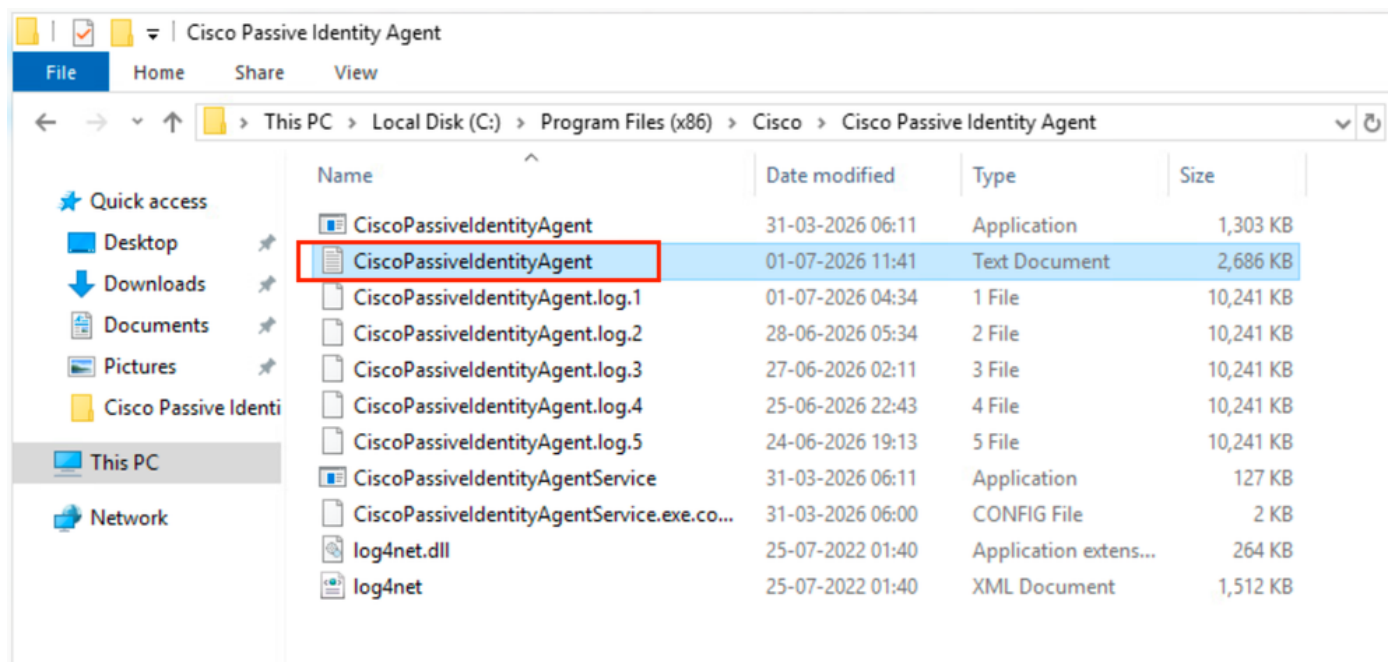
Name	Status	2% CPU	27% Memory
> Task Manager		0%	24.4 MB
> Windows Explorer		0%	37.3 MB
> Server Manager		0%	34.1 MB
Background processes (32)			
> Distributed File System Replicati...		0%	8.3 MB
▼ CiscoPassiveIdentityAgentServi... Cisco Passive Identity Agent		0%	15.4 MB
> Microsoft.ActiveDirectory.WebS...		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

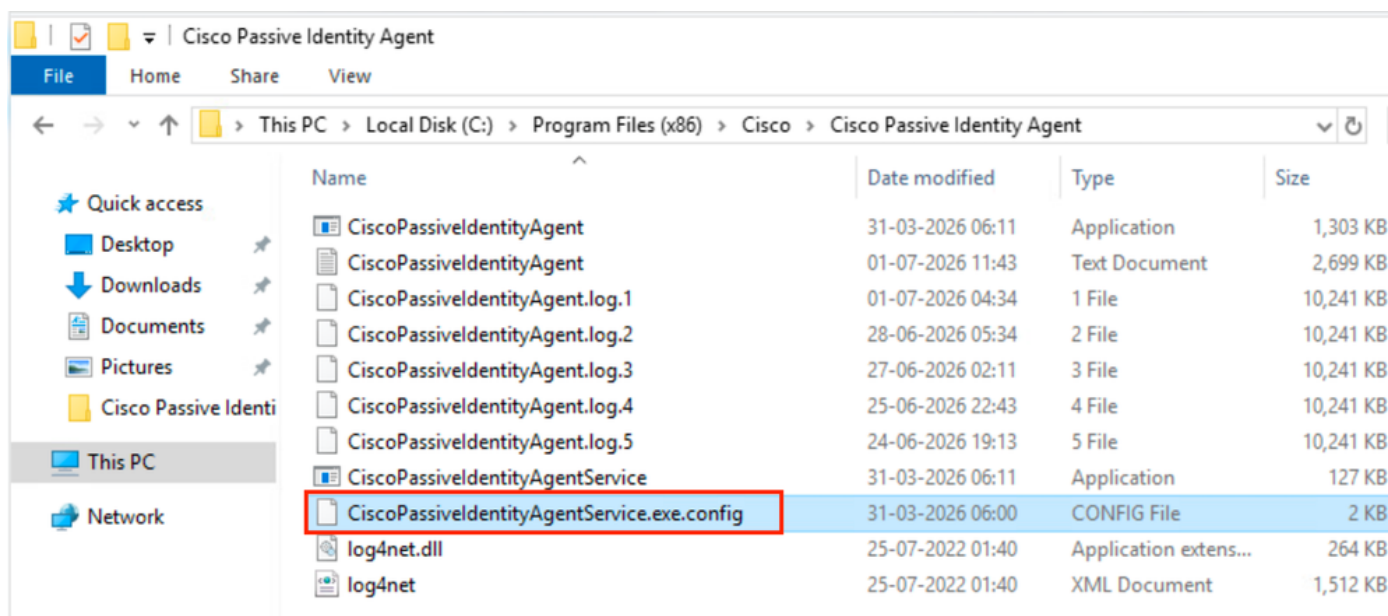
Ejecutando tarea

Los registros del agente se pueden encontrar en los archivos CiscoPassiveIdentityAgent, que se encuentran de forma predeterminada en: "C:\Program Files (x86)\Cisco\Cisco Passive Identity Agent\".



agente

De forma predeterminada, los registros del agente se establecen en el nivel INFO. Para habilitar el registro en el nivel DEBUG, modifique el archivo CiscoPassiveIdentityAgentService.exe.config y establezca el nivel de registro en ALL o DEBUG.



configuración del agente

registro de información

Comprobando registros de agente: recuperar configuración de agente.

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

INFO Rest Client, Estado de asignación: OK

INFO Rest Client, post de REST exitoso para userBatch fdm, latencia = 0, hora DC actual en UTC: 07/01/2026 19:47:34 USUARIO registrado en

INFO Rest Client, Solicitando configuración del agente

Registros de FMC

Ejecute este comando para ver si se ha recibido la asignación de usuario a IP del agente.

```

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#

```

salida de FMC

Si el comando anterior no muestra ninguna asignación, recopile estos registros y comuníquese con el TAC de Cisco.

Esta es una lista de registros relevantes para la API FMC. El registro de cola de cerdo abarca todos ellos.

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).