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.

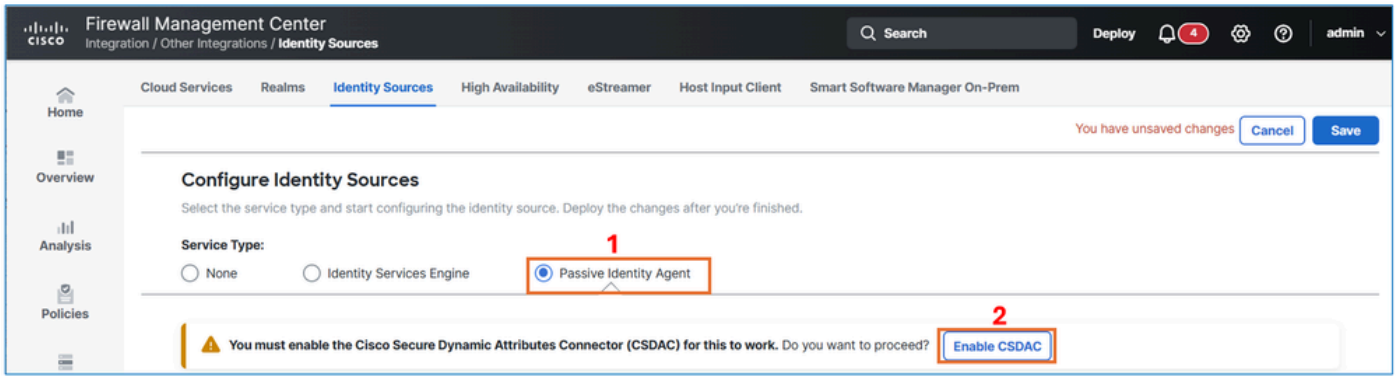
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Configuraciones

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

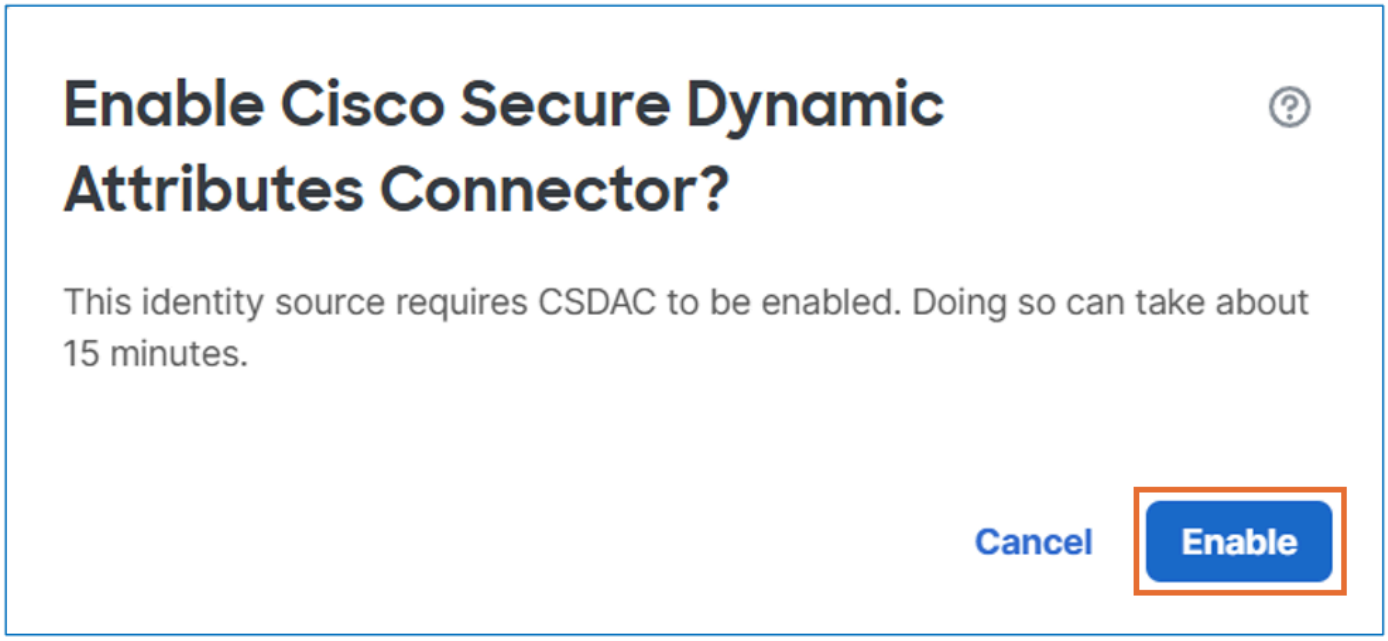
Configuración de un Origen de Agente de Identidad Pasivo

En la interfaz de usuario de FMC, vaya aIntegración > 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.



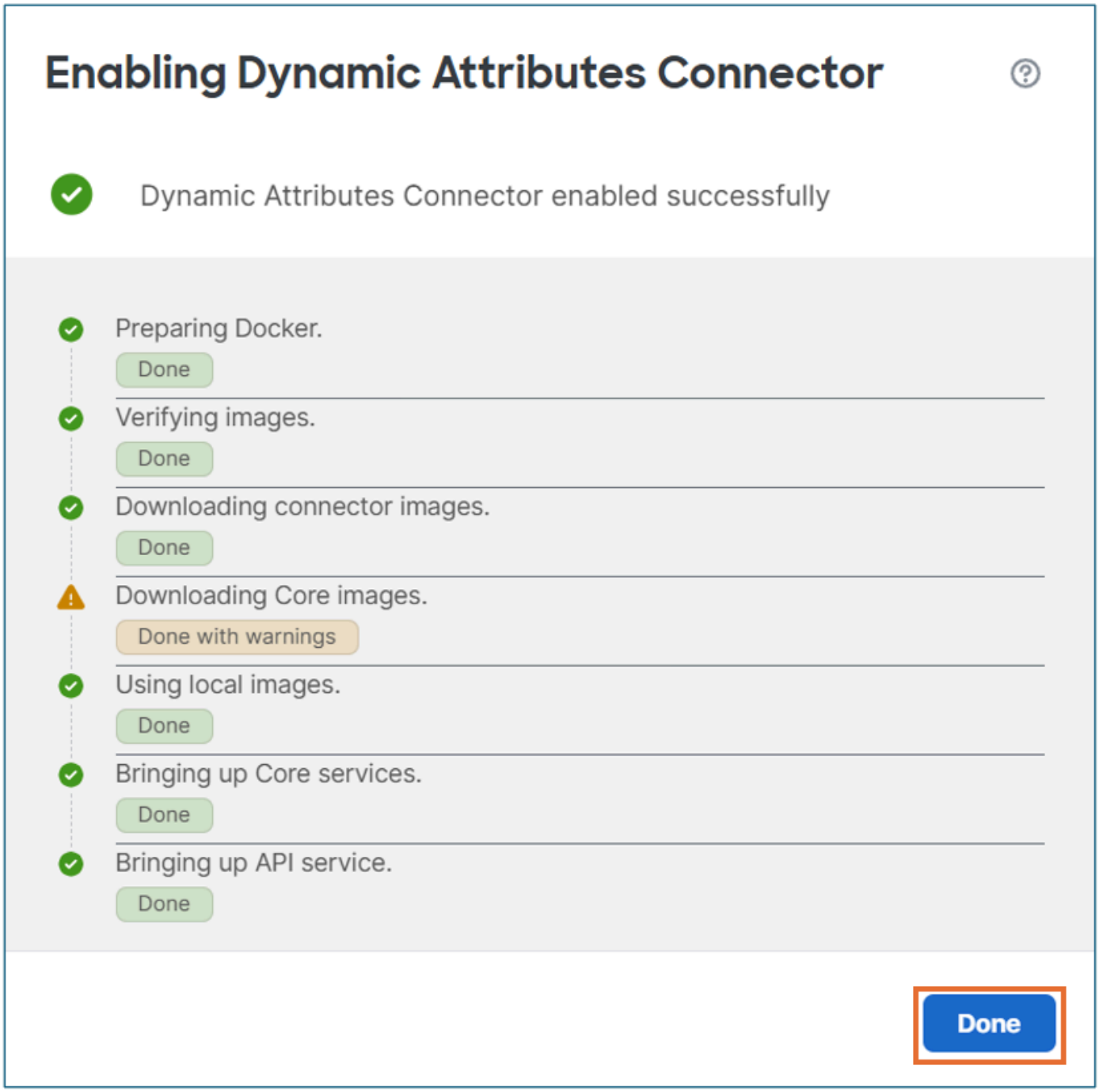
Agente de identidad pasivo

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



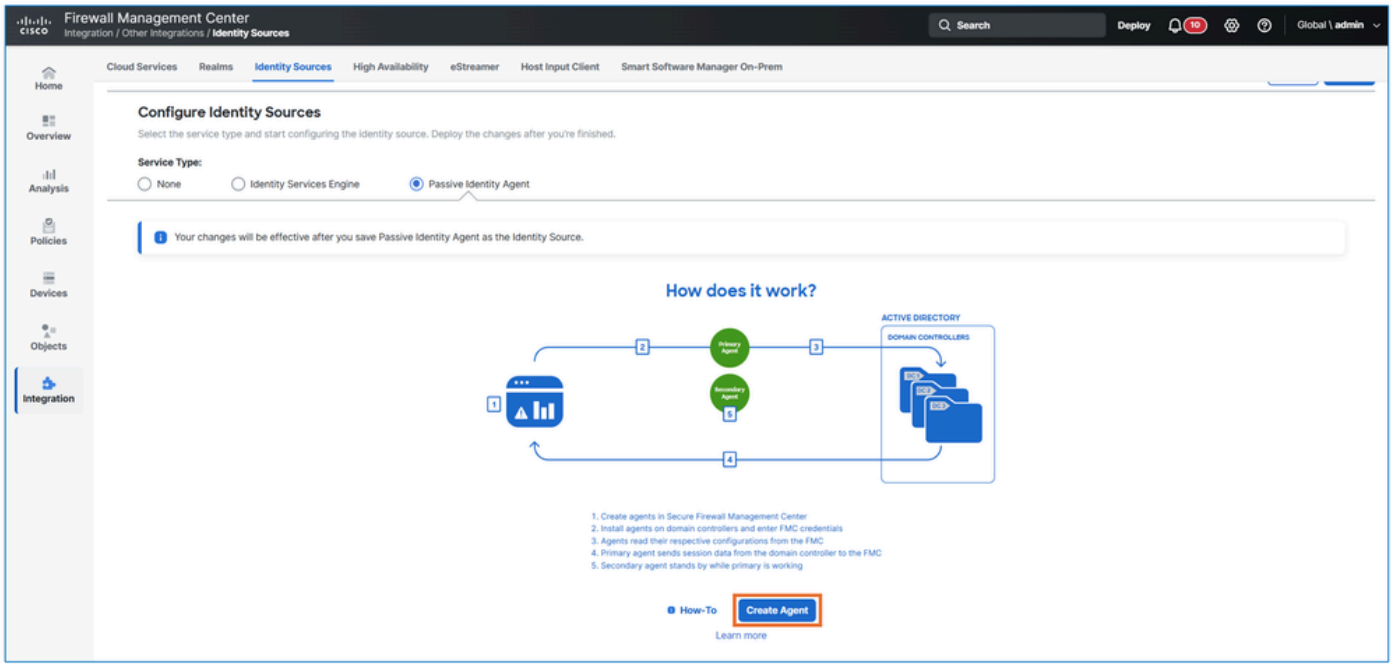
Habilitar CSDAC

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



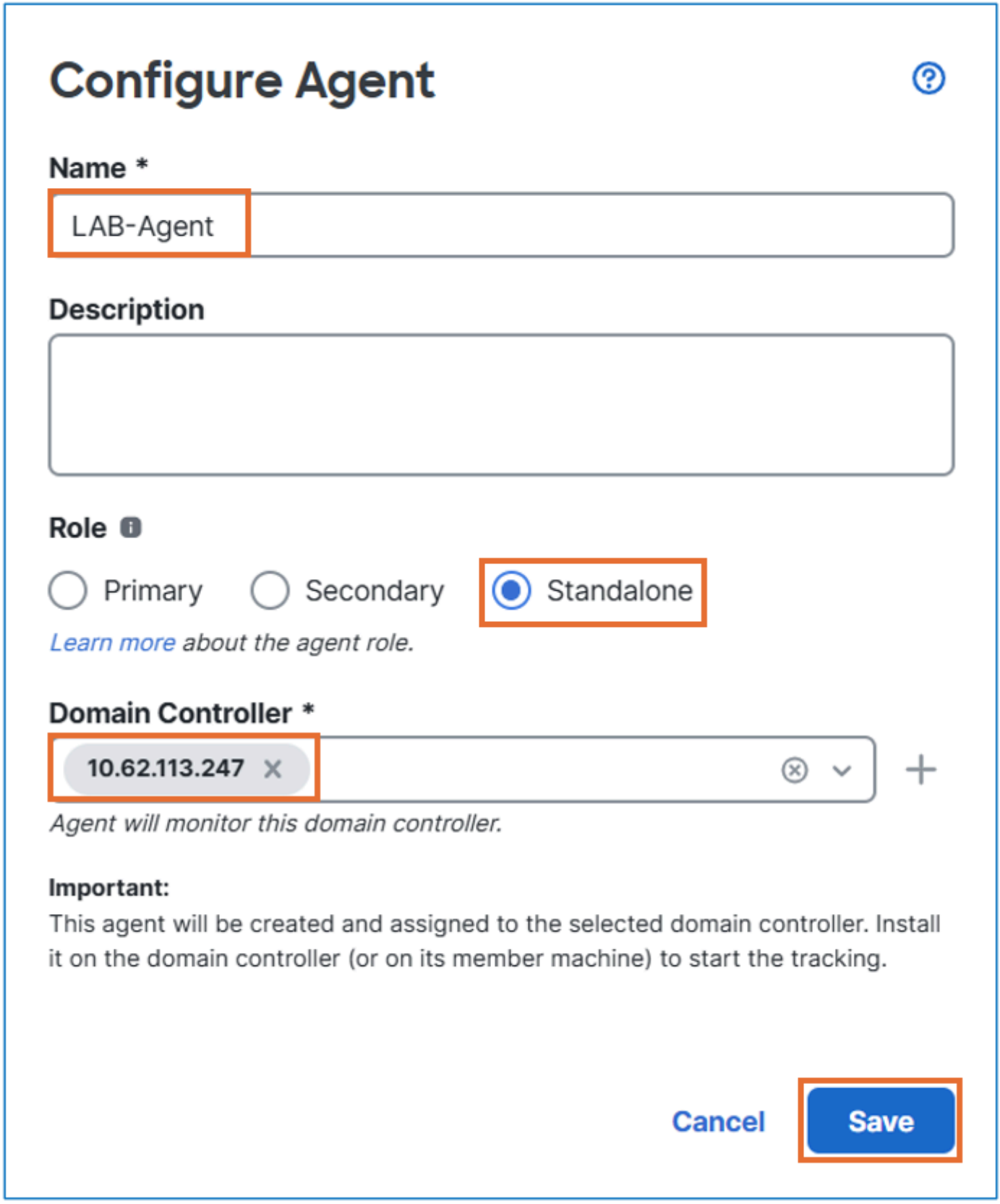
CSDAC activado

Haga clic en el botónCrear agente.



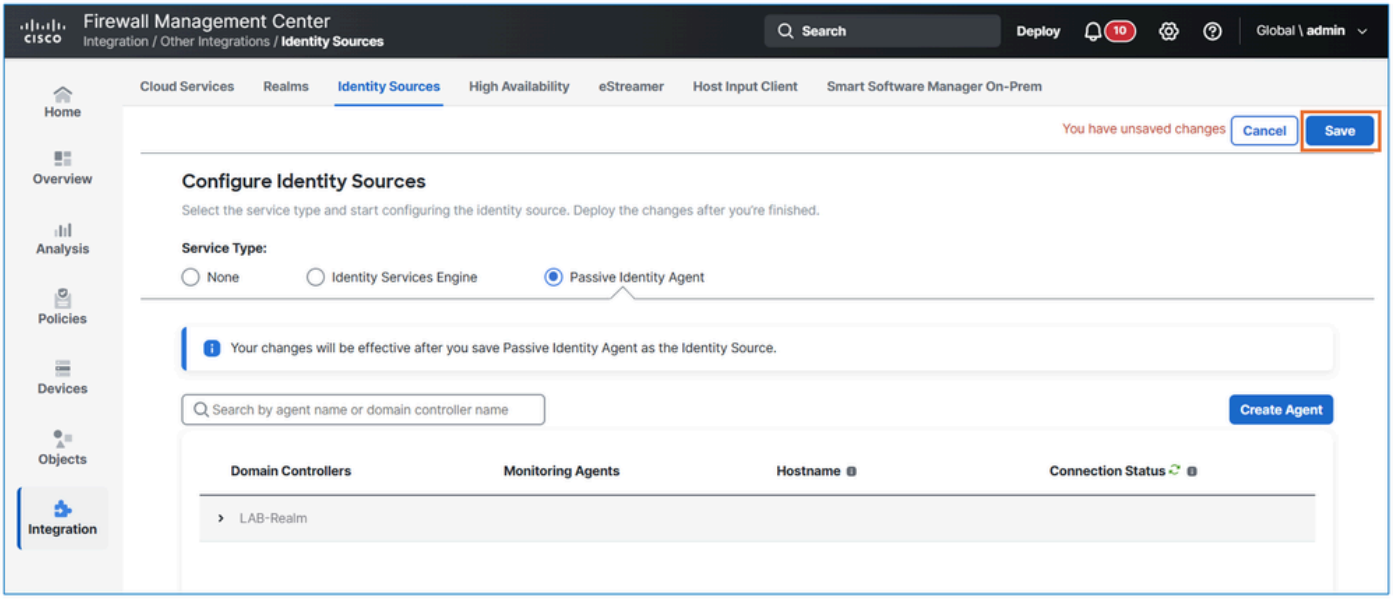
Crear agente

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



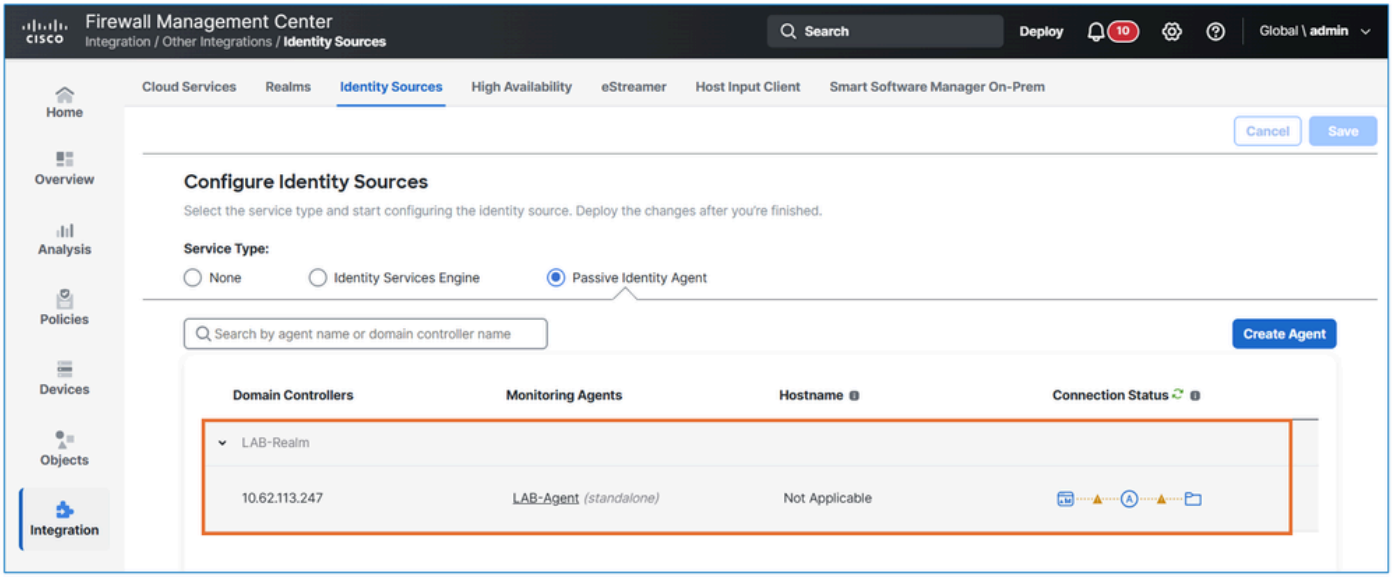
Configurar agente

Haga clic en el botónGuardar.



Guarde la configuración

El resultado.



Verificar el estado

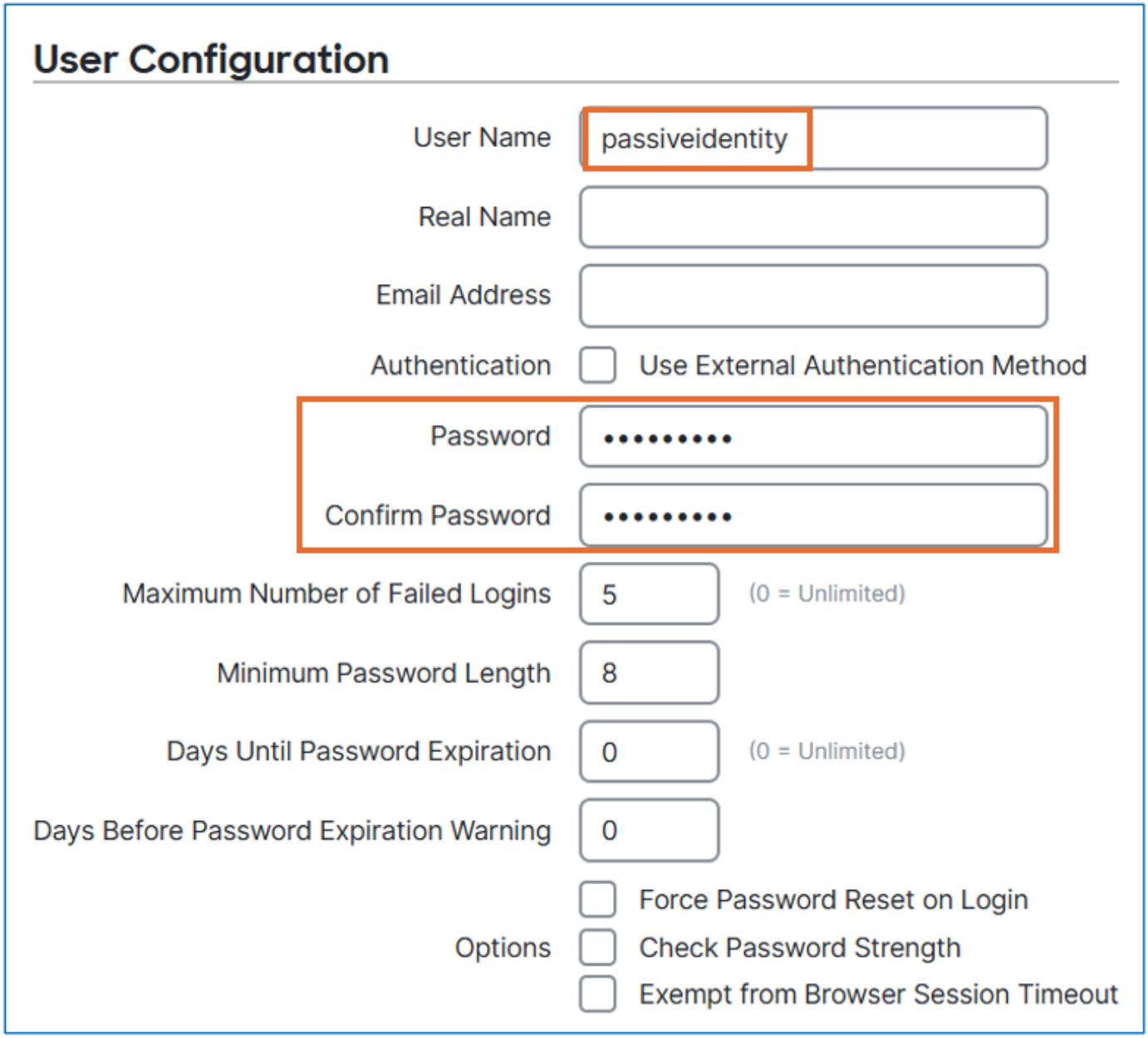
Nota: El agente de identidad pasivo indica el estado mediante líneas; el color ámbar significa que el agente nunca se ha comunicado correctamente con Secure Firewall Management Center. Una línea de agente recién creada es de color ámbar y permanece así hasta que se completa la configuración.

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

Center

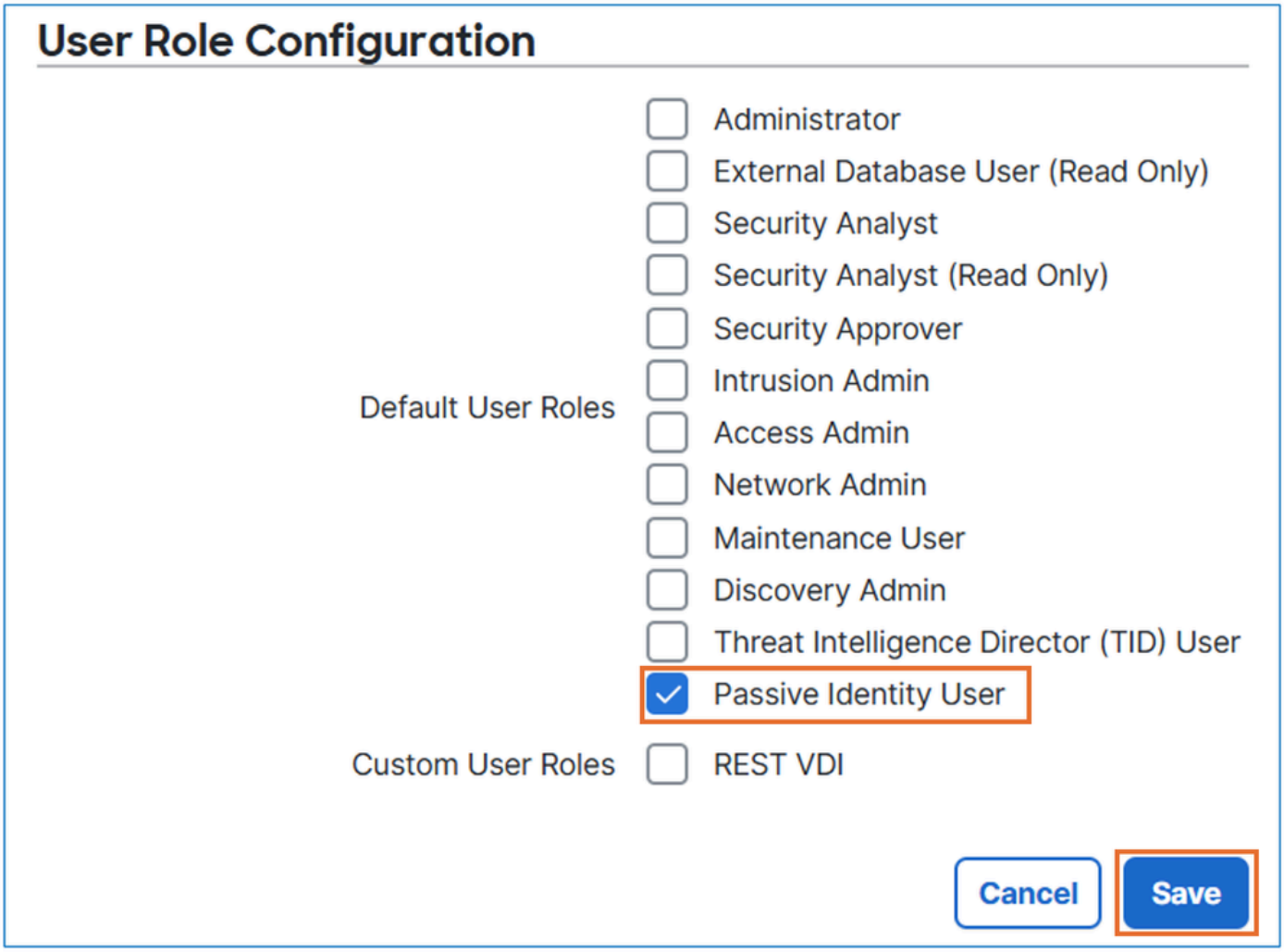
Cree un usuario de Secure Firewall Management Center con permisos suficientes para comunicarse con el agente de identidad pasivo. Este usuario tiene privilegios limitados para realizar otras tareas; se espera que el usuario sólo habilite la comunicación con el agente de identidad pasivo.

En la interfaz de usuario de FMC, vaya aSistema > Usuarios y haga clic enCrear usuario. Rellene los detalles del usuario de acuerdo con los requisitos de la tarea.



Crear usuario

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

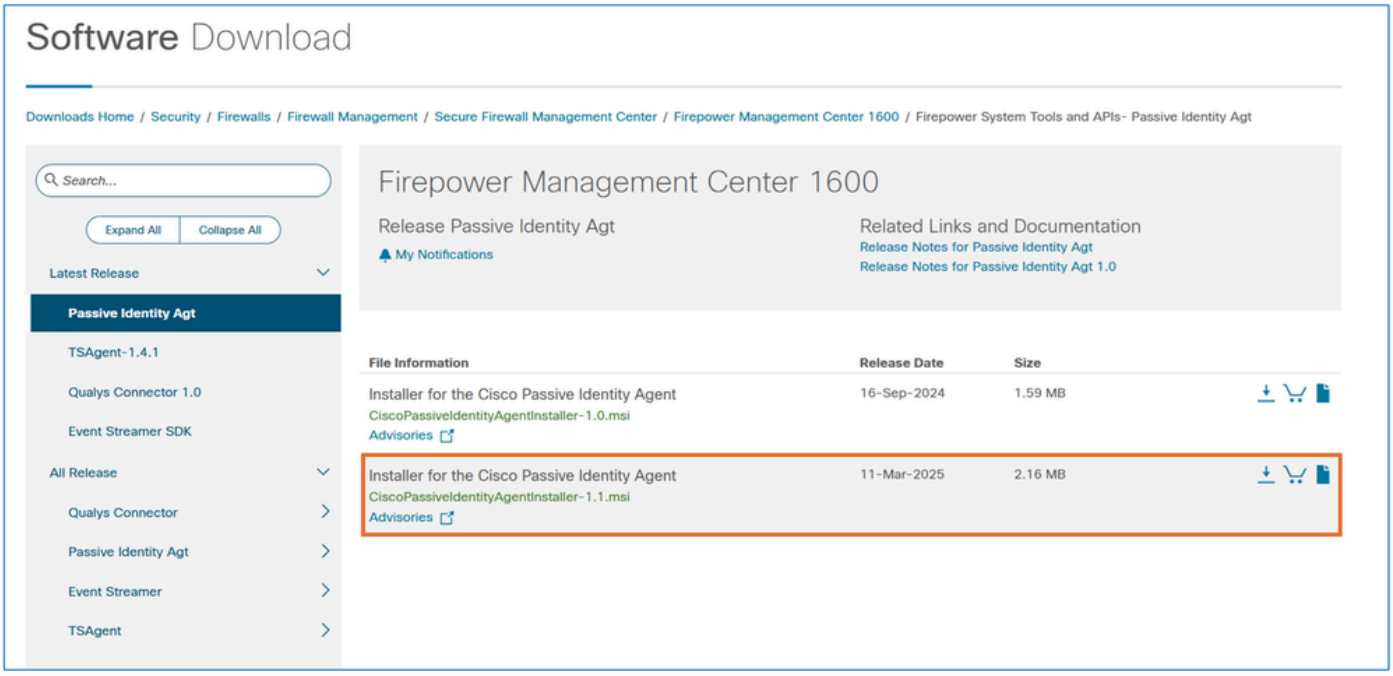


seleccione el usuario de identidad pasiva

Instalación y configuración del software Passive Identity Agent

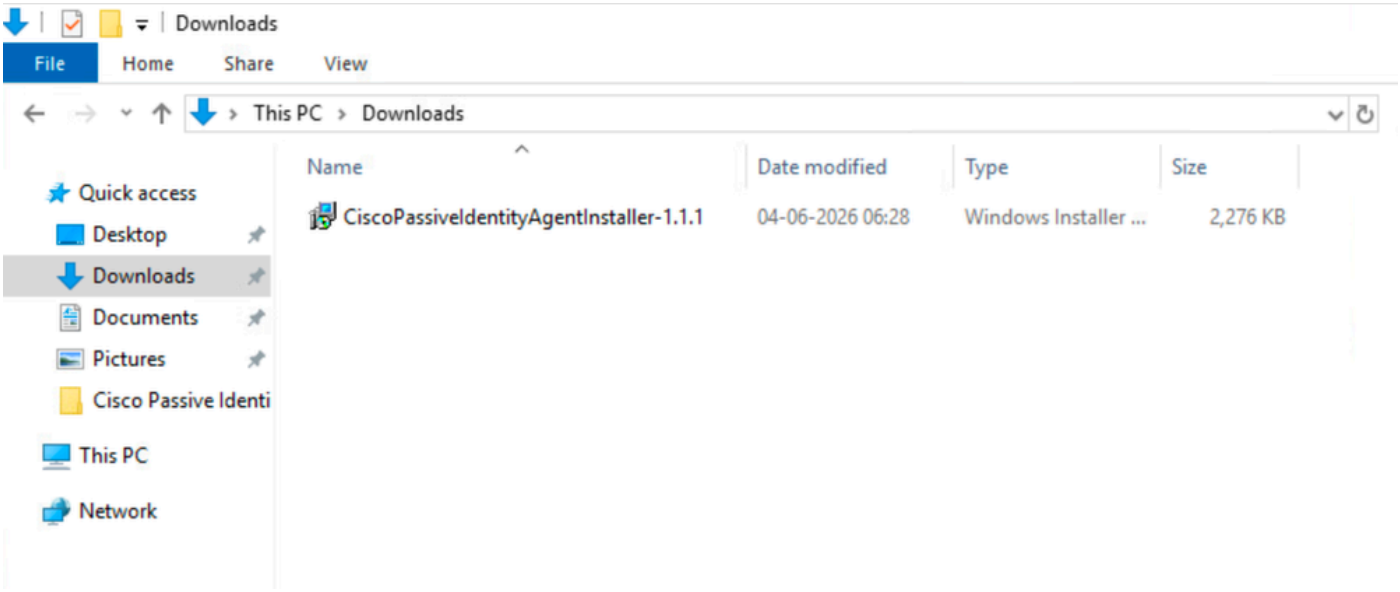
Instale y configure el software Passive Identity Agent en el controlador de dominio designado.

Descargue el agente de identidad pasivo de software.cisco.com.



descargar el software

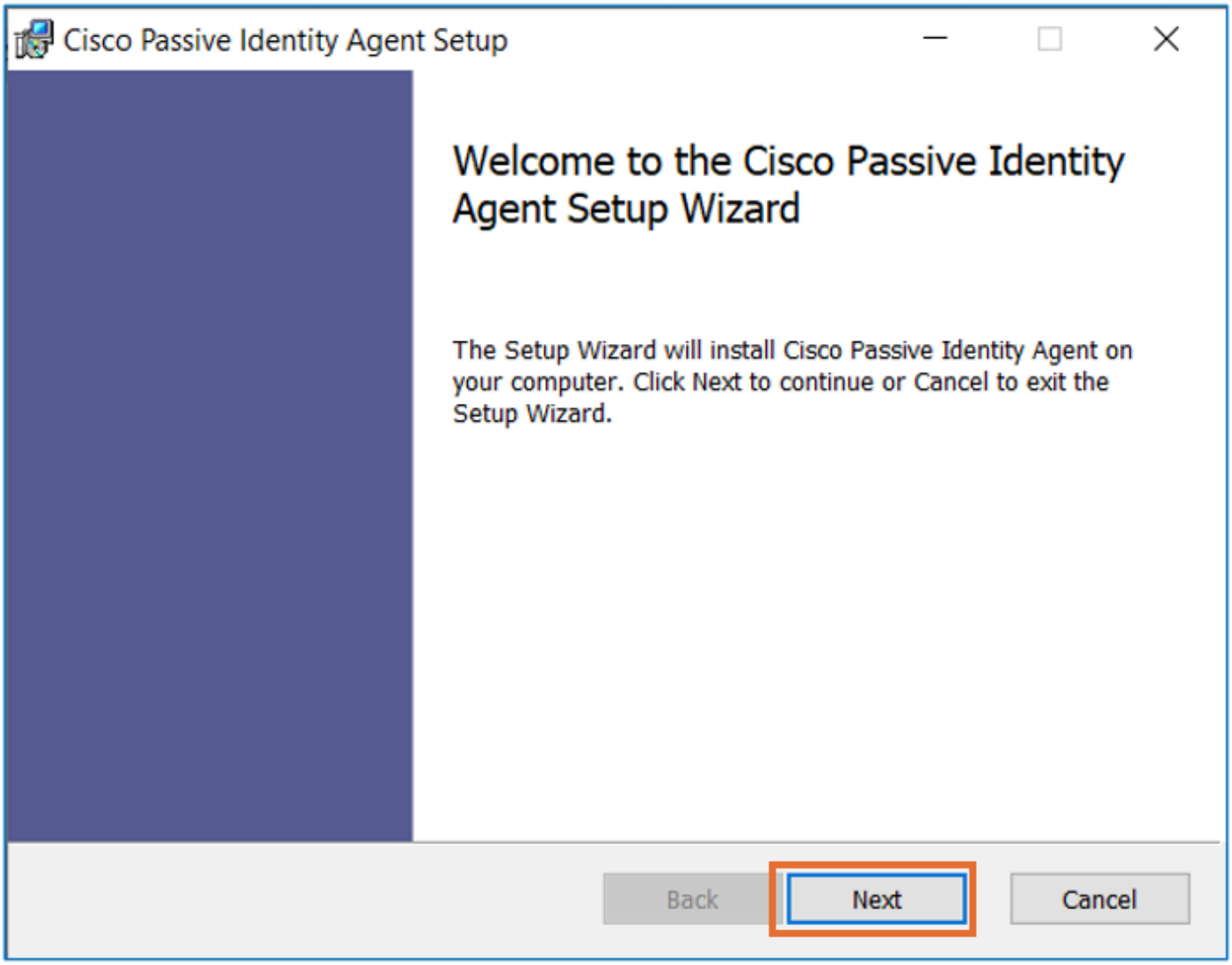
Después de descargar el agente, inicie el proceso de instalación en el controlador de dominio.



agente

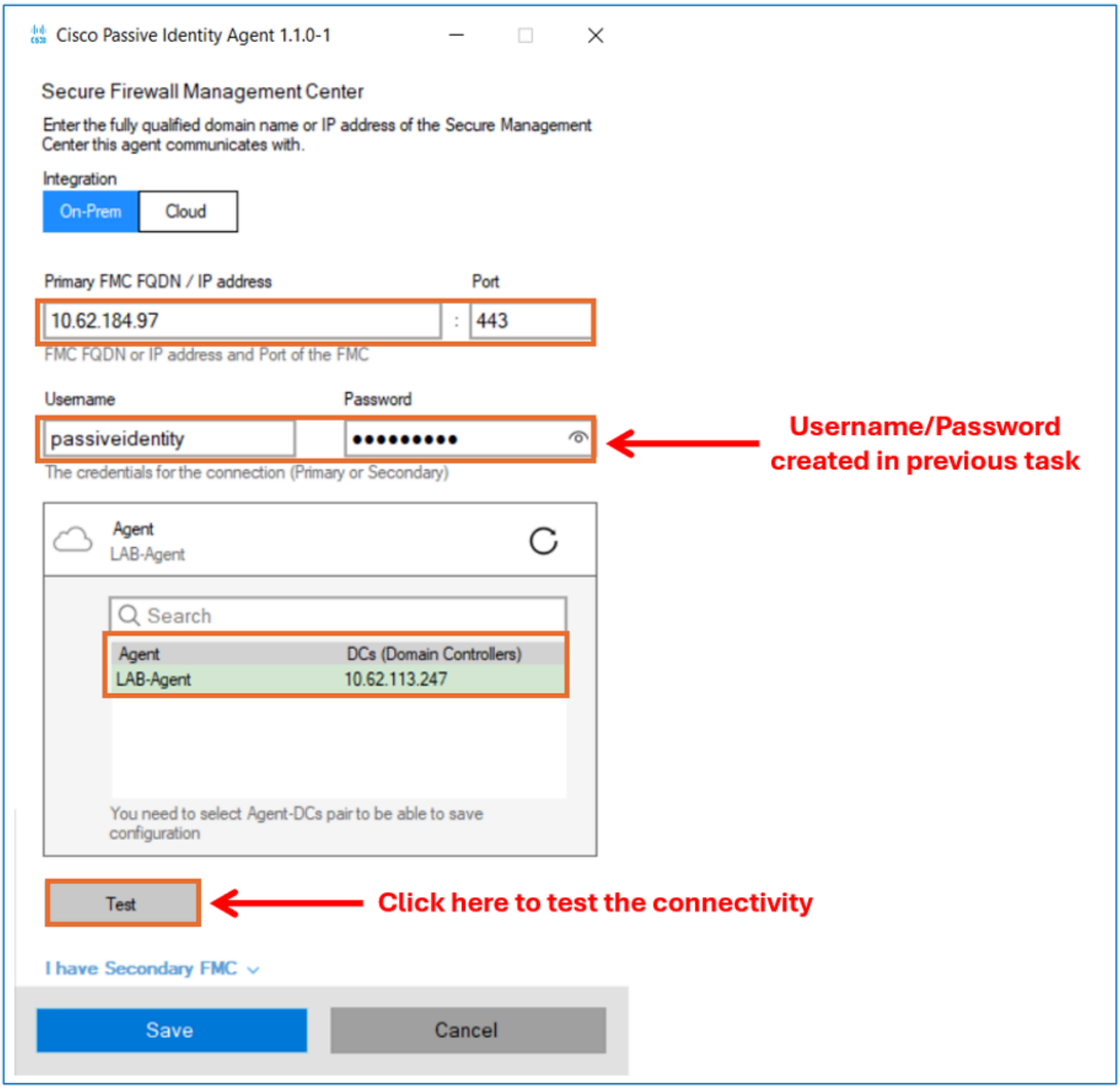
]

Consulte las instrucciones de instalación proporcionadas para completar la instalación.



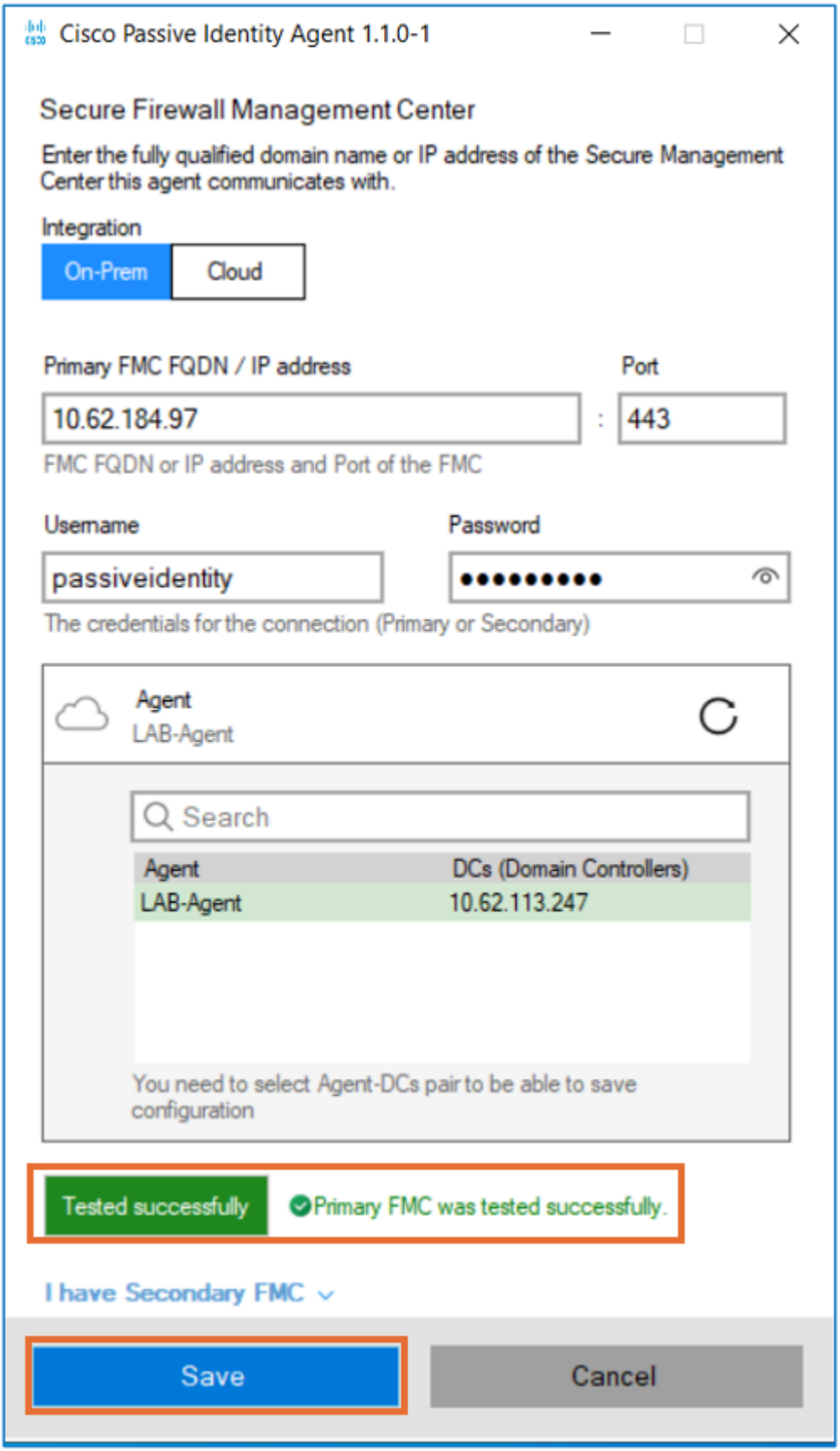
Instalar

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.



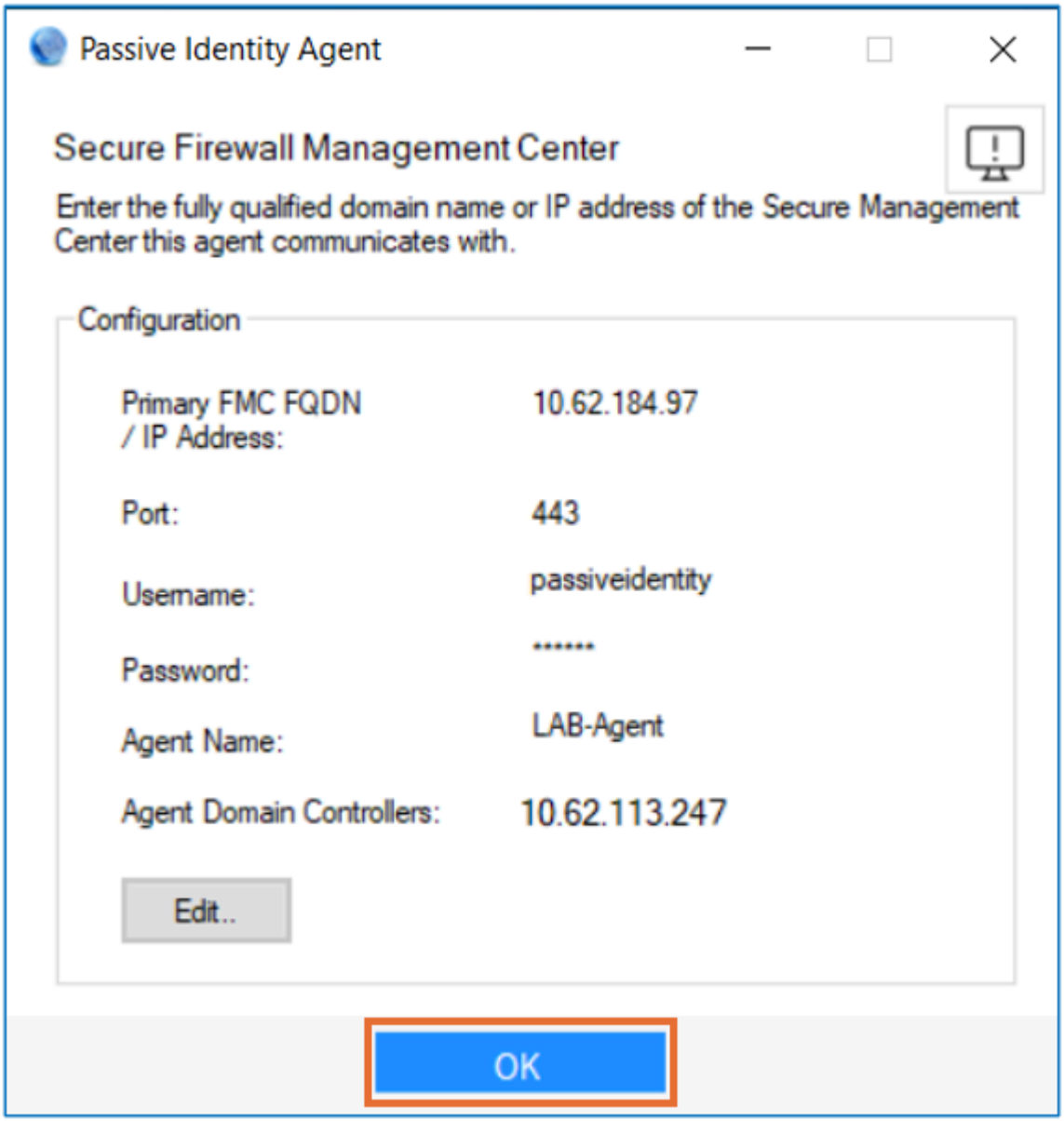
configure el agente.

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



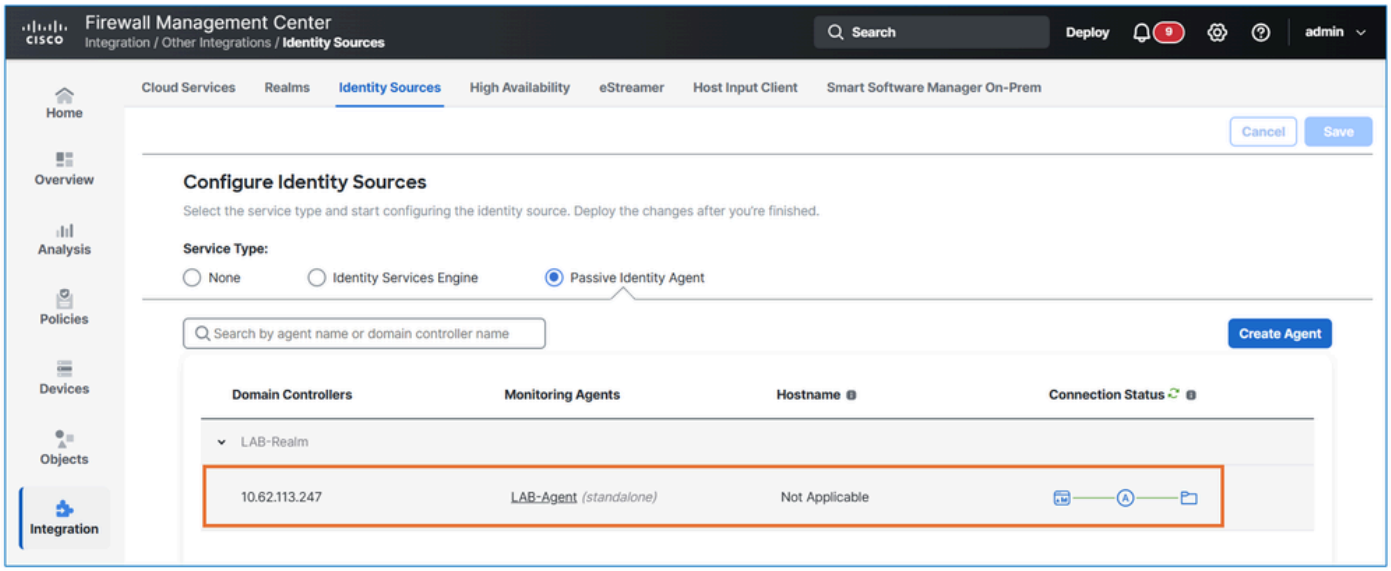
prueba

Haga clic en el botónAceptar para completar la configuración del agente.



el agente se está ejecutando

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



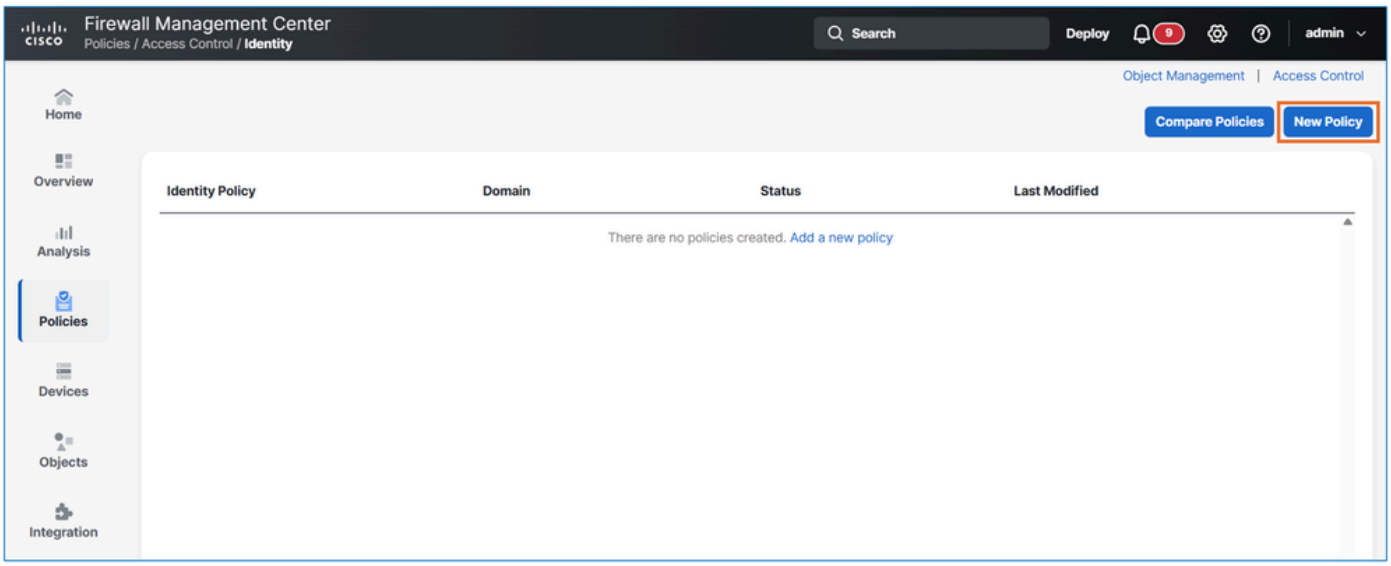
verificar la comunicación desde fmc

Configurar políticas de identidad

Cree una política de identidad basada en la tabla proporcionada.

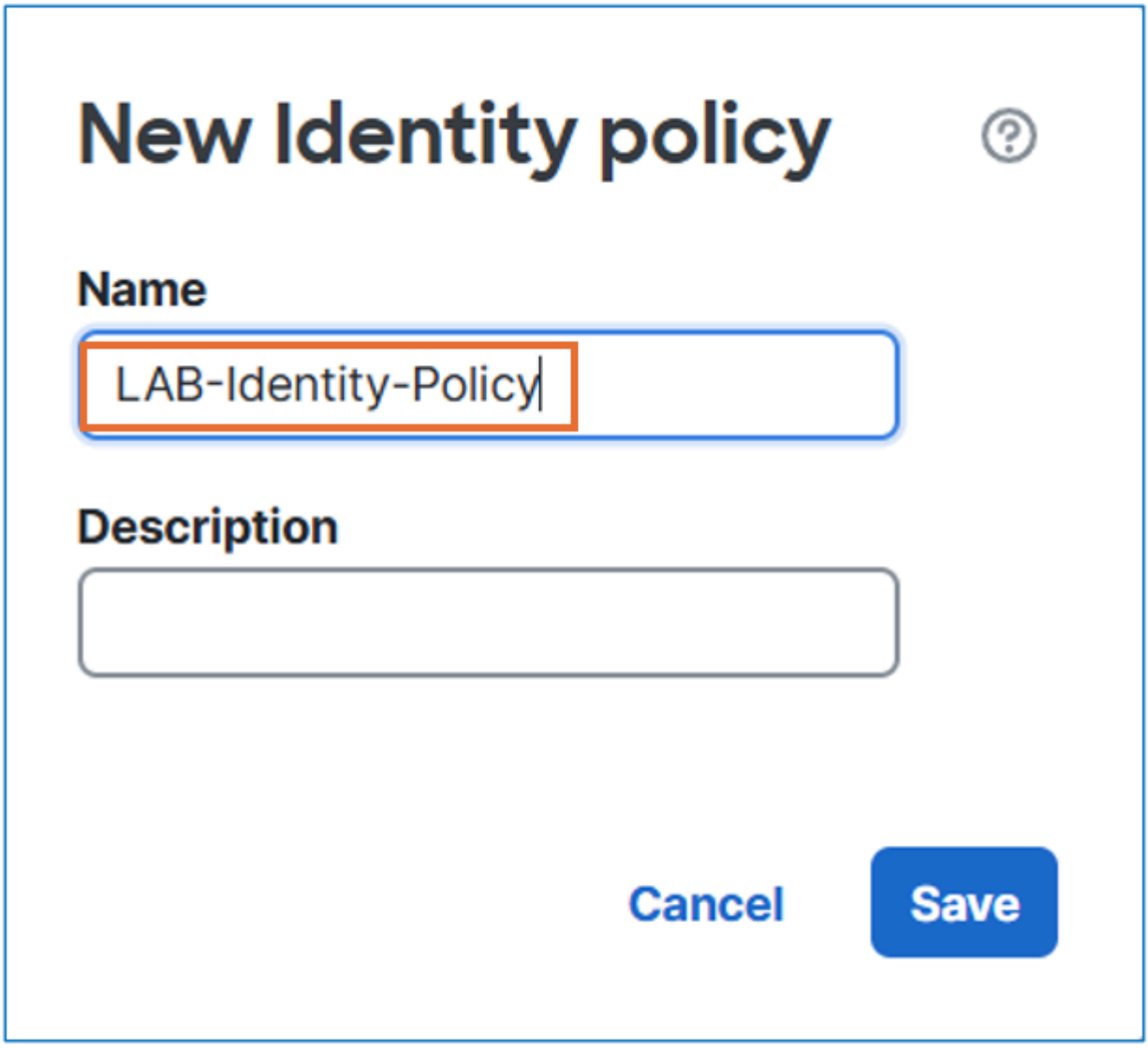
Nombre de política	Nombre de regla	Rango de autenticación	Configuración restante
LAB-Identity-Policy	Regla1	LAB-Realm	Dejar como predeterminado

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



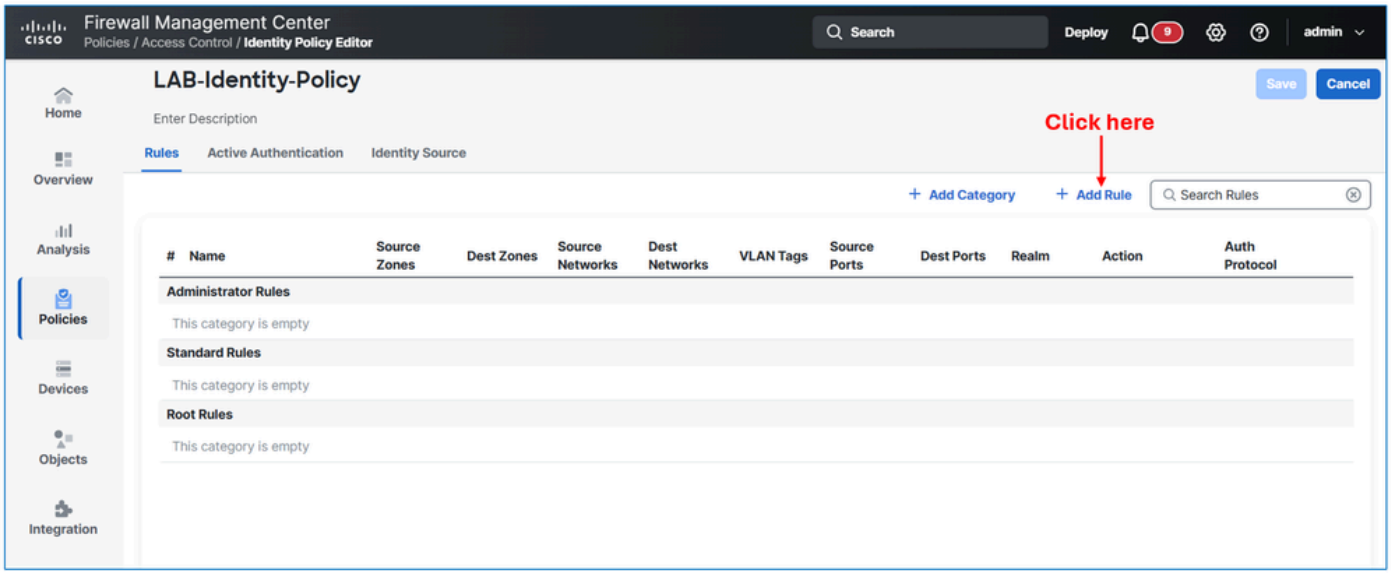
nueva política

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



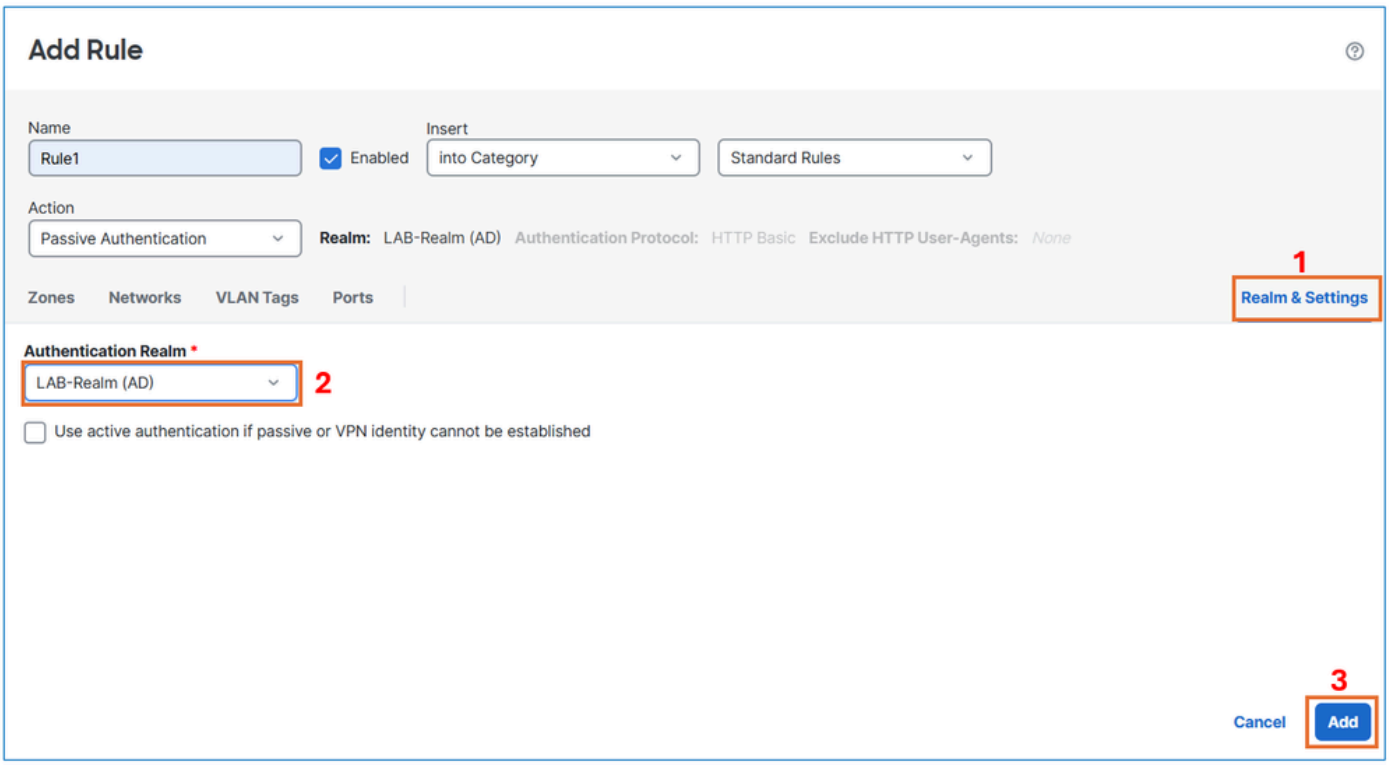
nueva política

Haga clic en el botónAgregar regla.



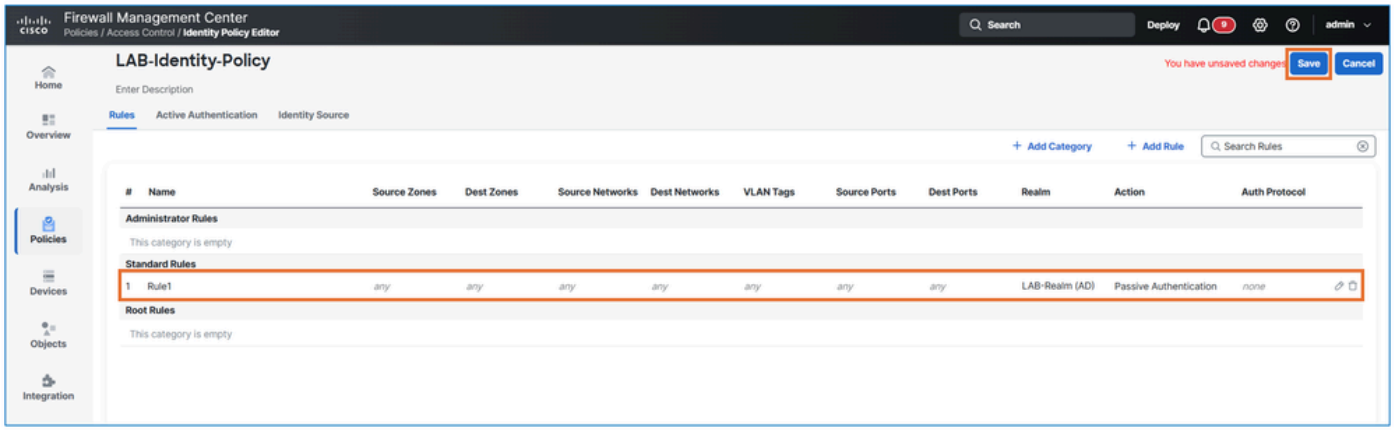
crear regla

Navegue hasta la pestañaRango y Configuración y seleccione el rango de autenticación en función de los requisitos de la tarea. Por último, haga clic en el botónAgregar.



Configuración de rango

Haga clic en el botónGuardar.



guardar la configuración

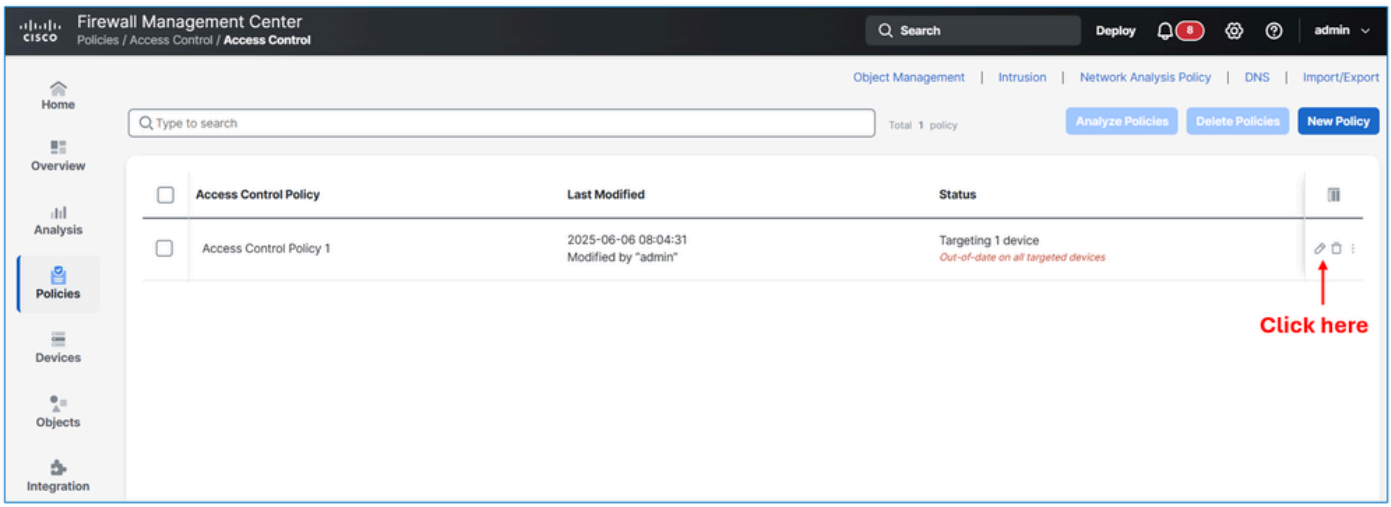
Configurar políticas de control de acceso

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

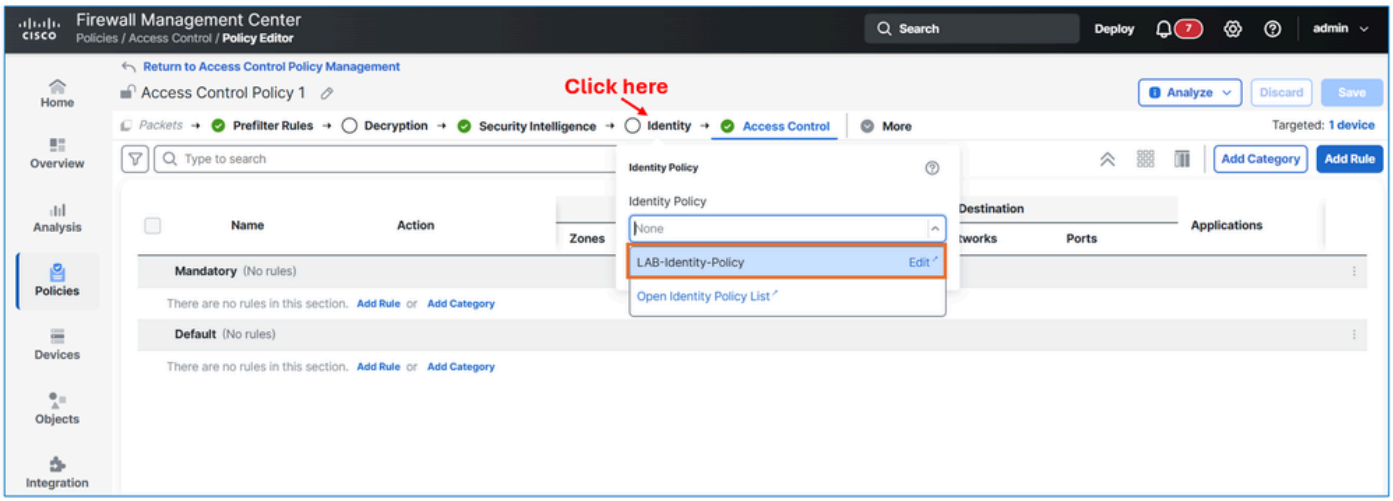
Paso 1. Vincular la Política de Identidad a la Política de Control de Acceso

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



Editar directiva

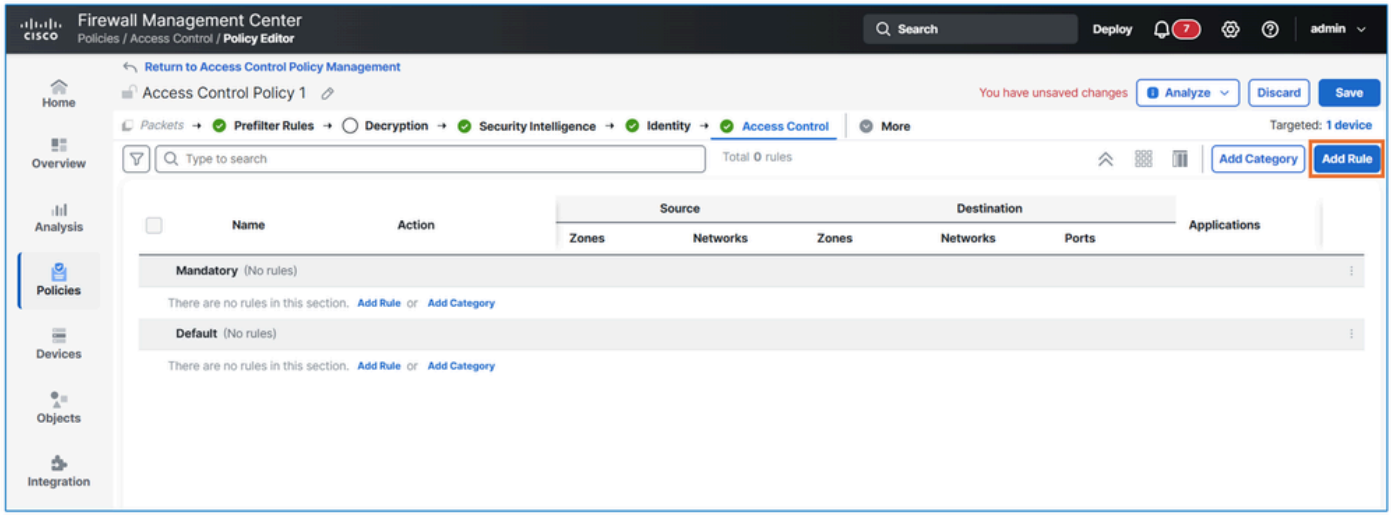
Navegue hasta la sección Identidad y vincule la Política de Identidad creada en la tarea anterior.



agregar política de identidad

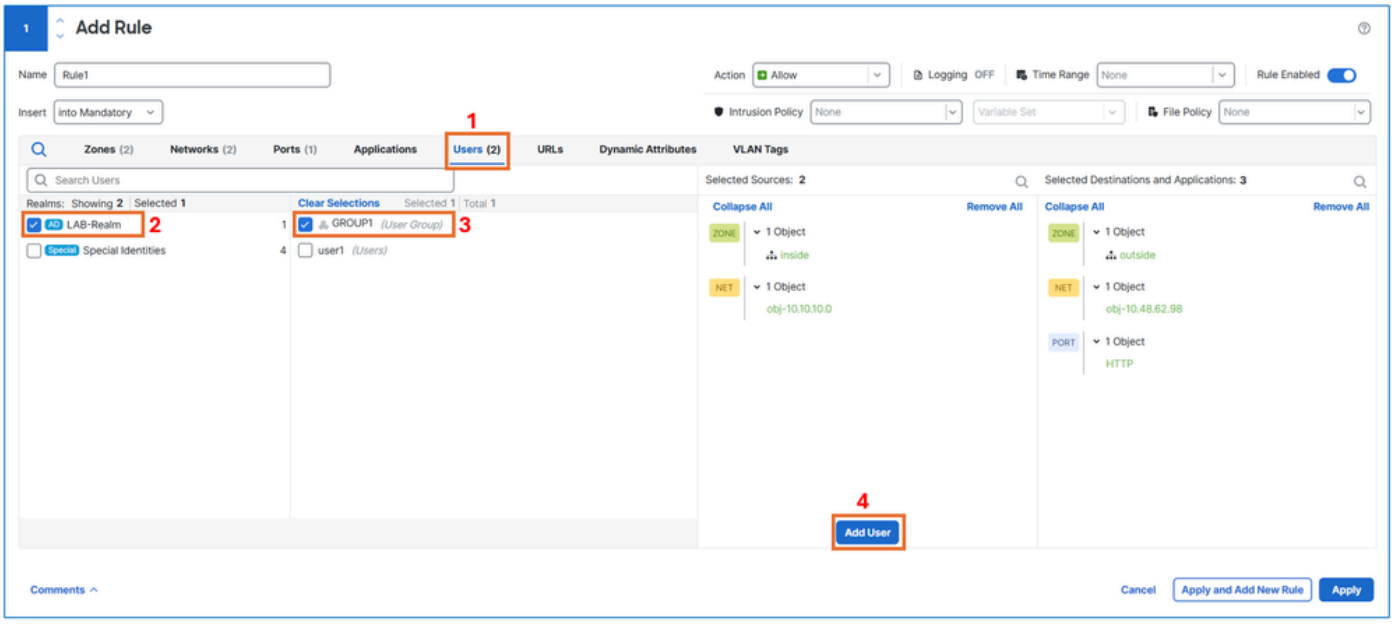
Haga clic en el botónAplicar

Paso 2. Cree la regla de control de acceso.



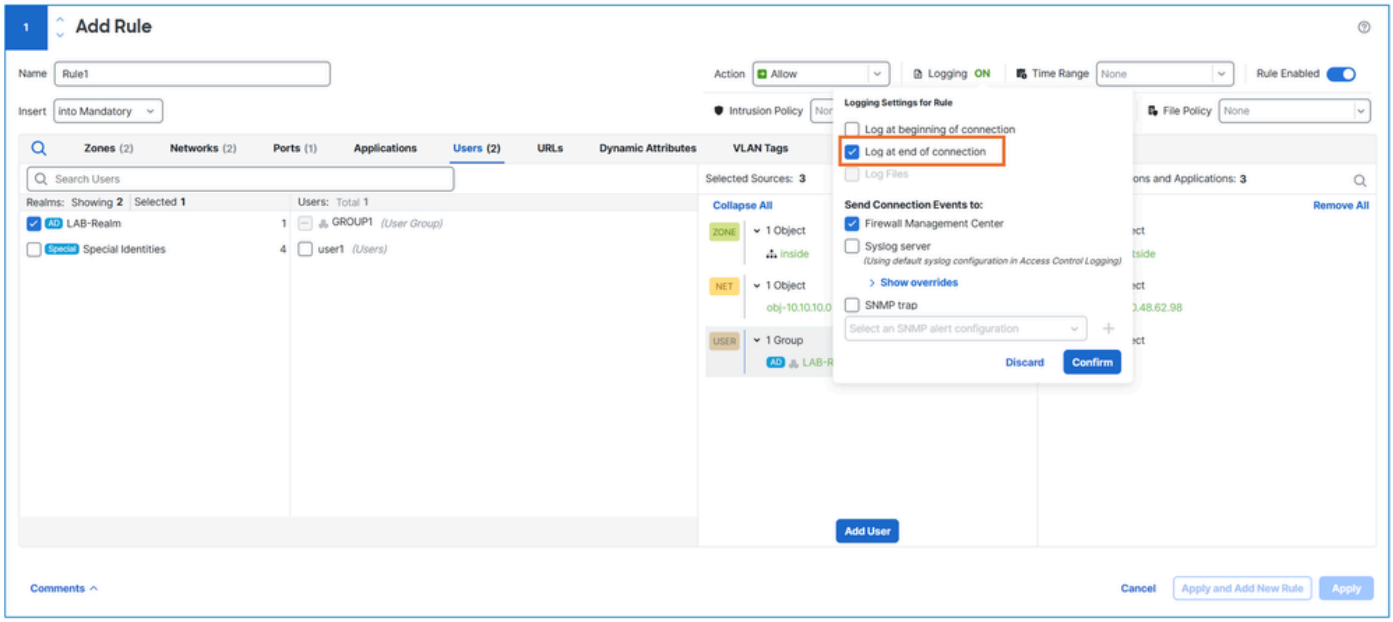
crear ACP

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



agregar usuarios a la regla

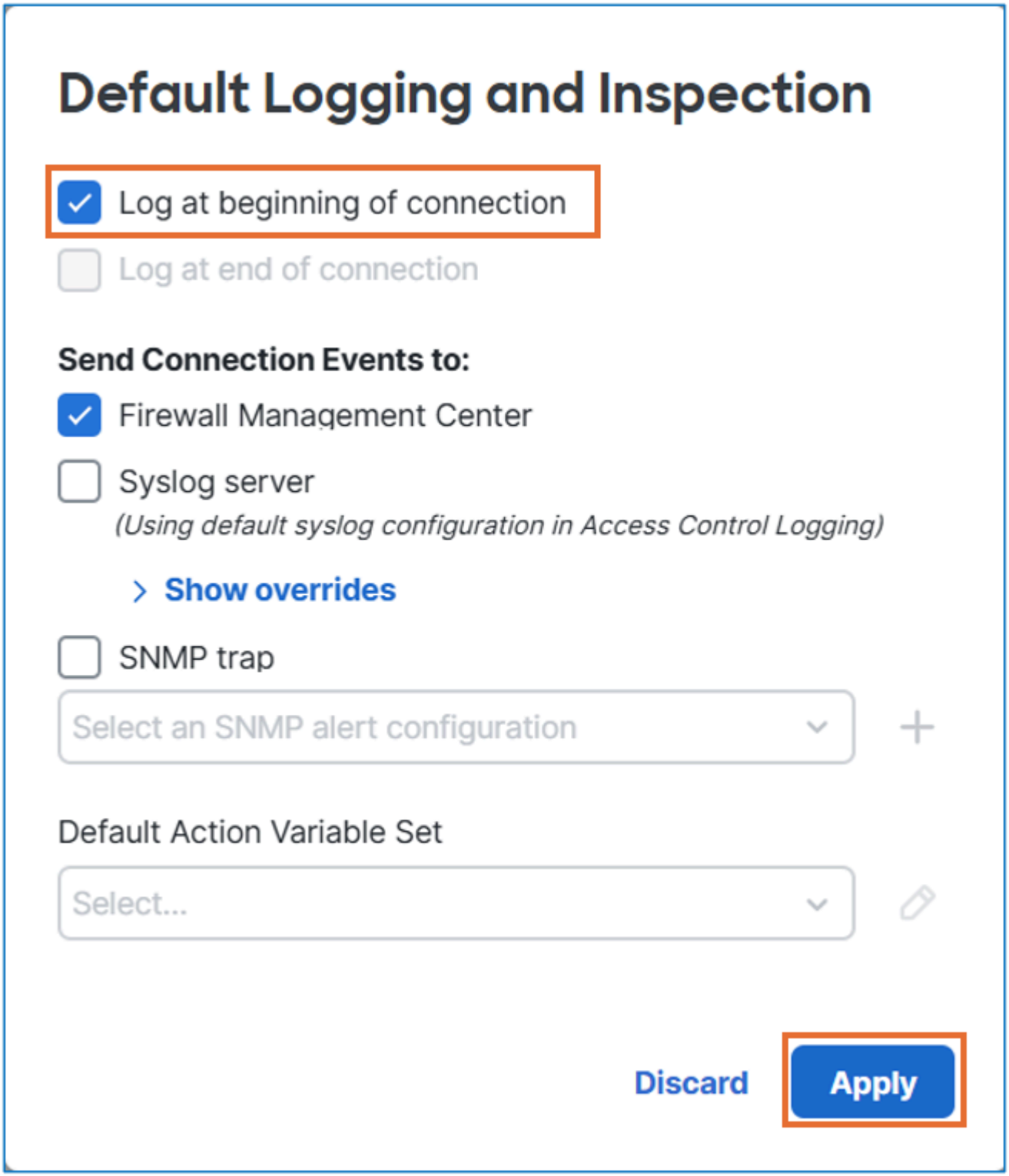
Active el registro de la regla seleccionando Registro al final de la conexión.



enable logging

Paso 3. Habilite el registro para la acción predeterminada.

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



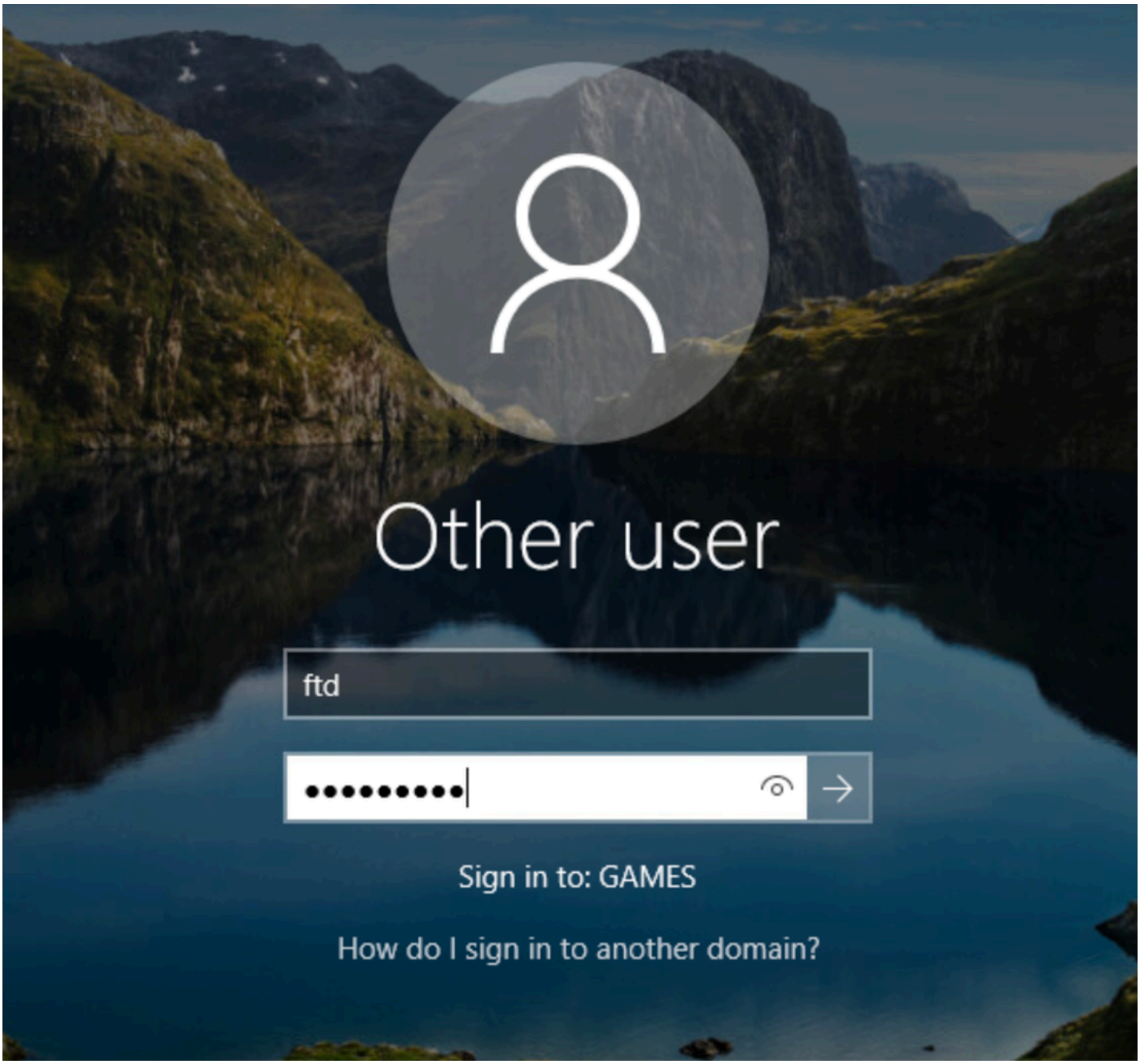
Activar registro

Guarde e implemente la configuración en el FTD.

Verificación

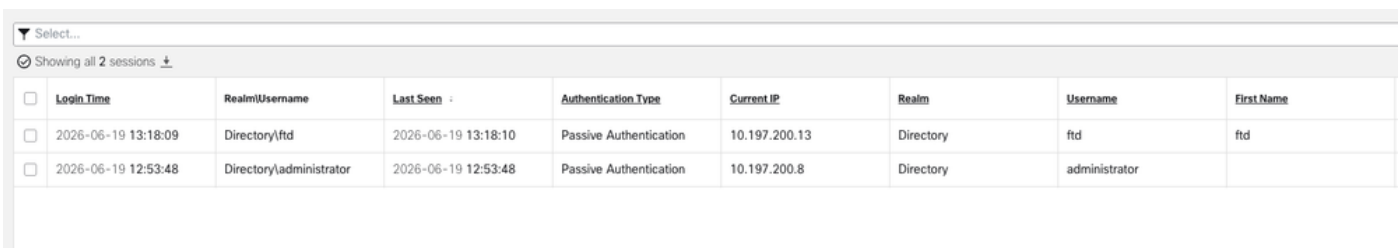
Verifique la operación de identidad pasiva confirmando que el tráfico está permitido exclusivamente para ftd.

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.



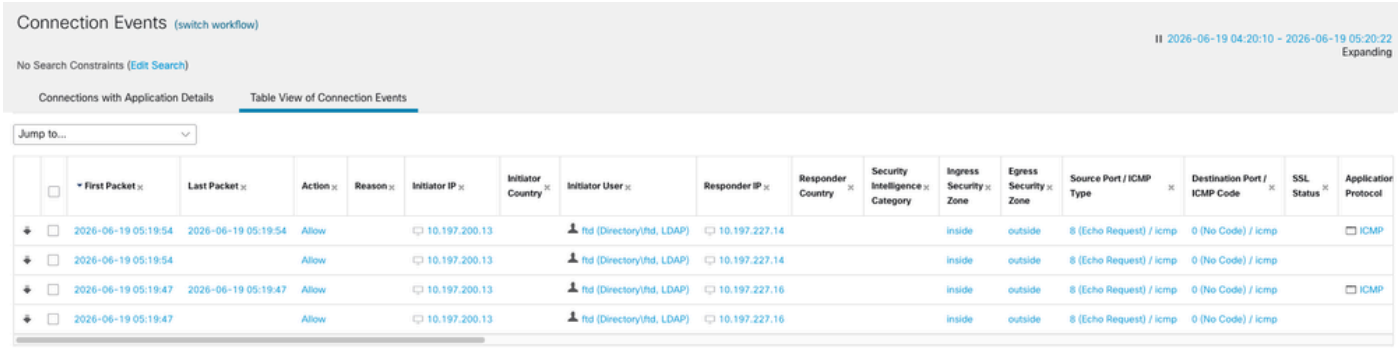
Select...

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	

Sesiones activas

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

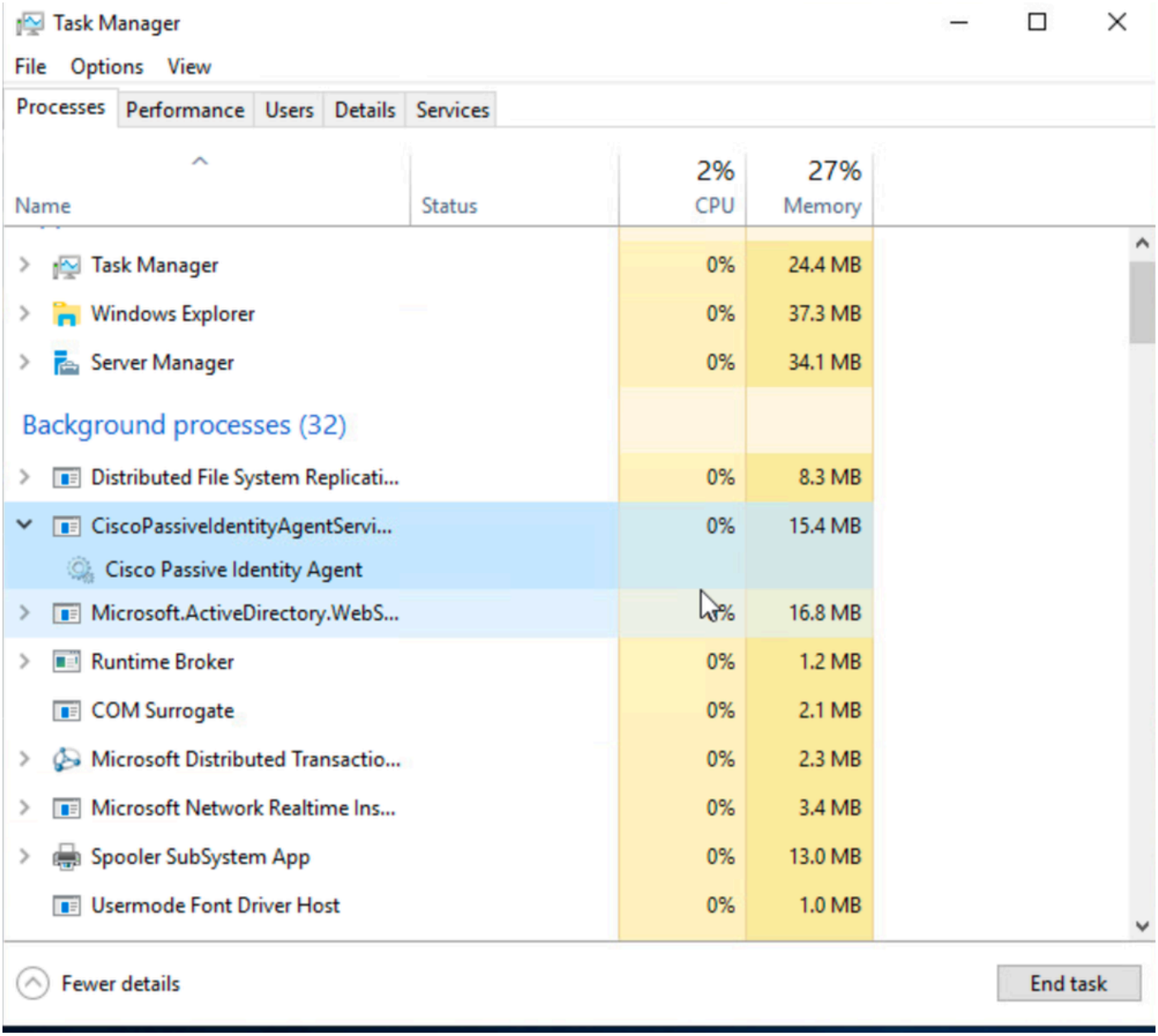


Sesiones activas

Resolución de problemas

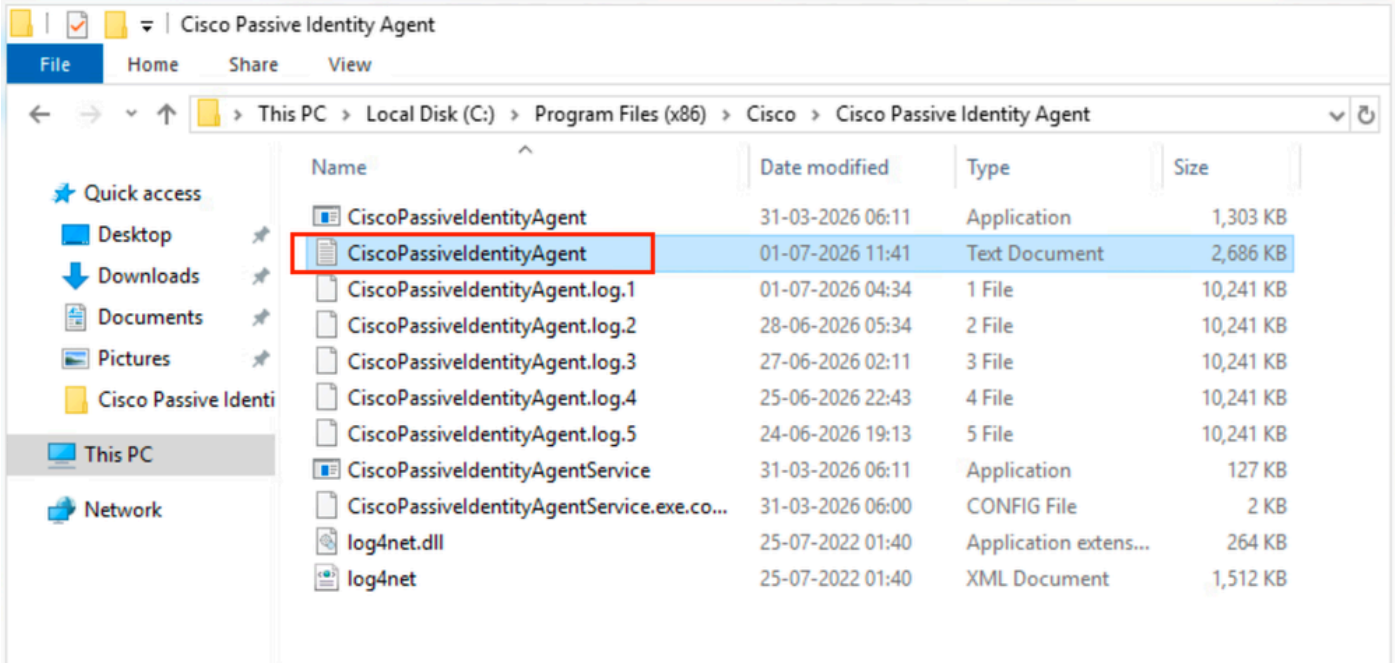
Comprobando registros de agentes

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



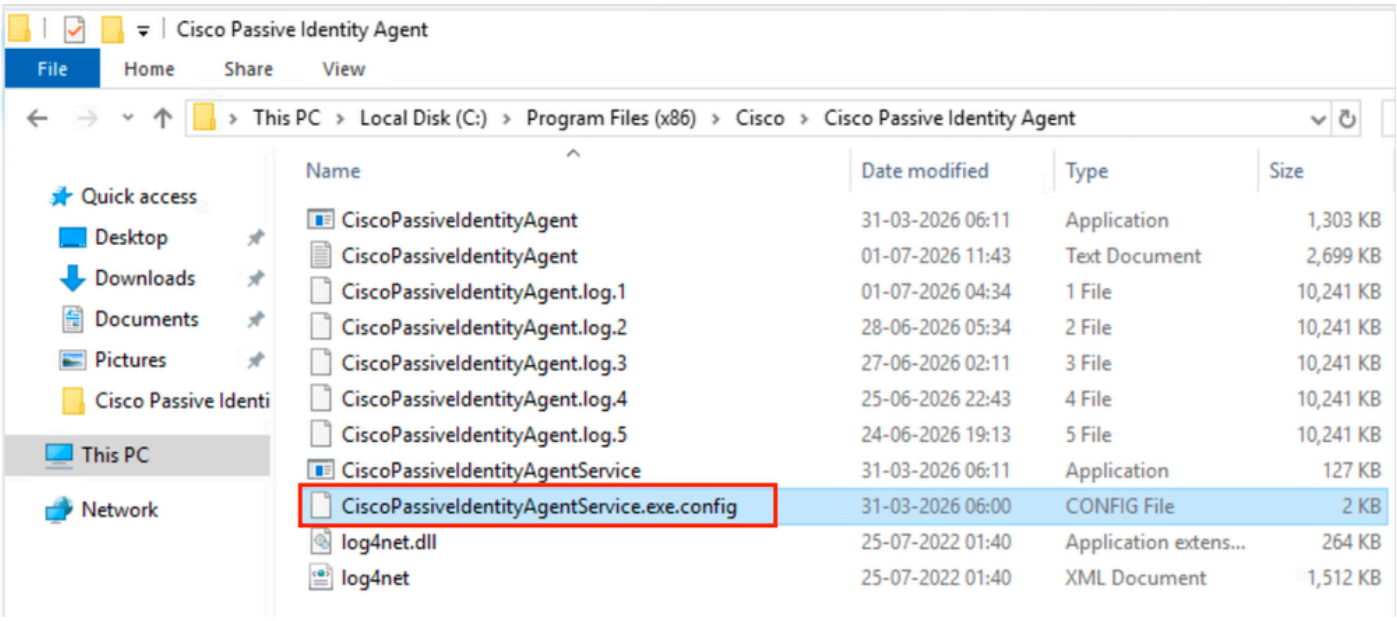
Ejecutando tarea

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 nivelINFO. Para habilitar el registro en el nivel DEBUG, modifique el archivoCiscoPassiveIdentityAgentService.exe.config y establezca el nivel de registro en ALLorDEBUG.



configuración del agente

registro de información

Comprobando registros de agente: recuperar configuración de agente.

INFO Rest Client, Bulk Events: [f"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).