Configurar o Passive Identity Agent usando o FMC

Contents

Introdução

Este documento descreve como configurar a Origem do agente de identidade passiva que envia dados de sessão ao FMC

Pré-requisitos

Requisitos

- Cisco Secure Firewall Management Center executando a versão 7.6+
- Cisco Secure Firewall executando a versão 7.6+
- Windows Ative Diretory Server, o servidor deve executar o Windows Server 2008 ou posterior.
- Você deve habilitar o Snort 3 nos dispositivos Secure Firewall Threat Defense.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall Management Center 7.6.5
- Cisco Secure Firewall 7.6.5
- Microsoft Ative Diretory em execução no Windows Server 2022.

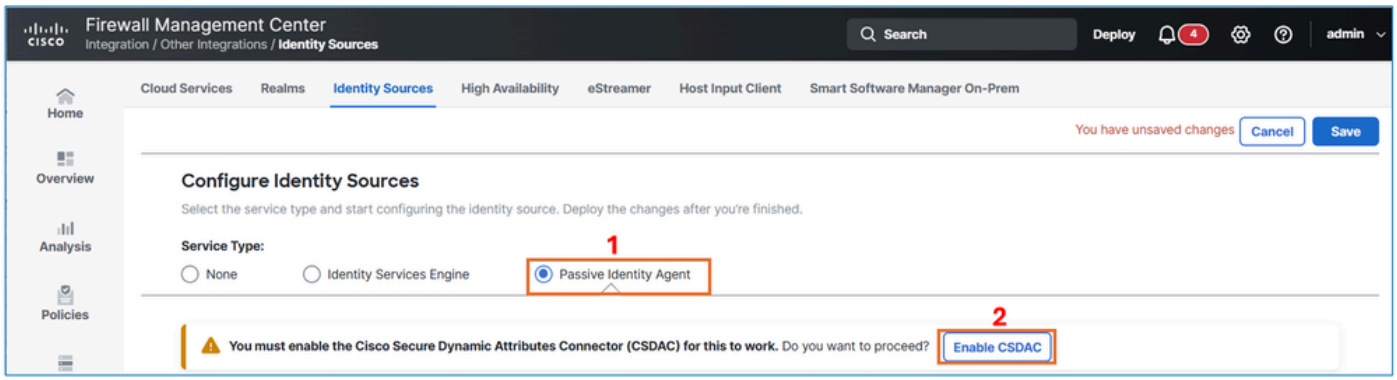
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurações

Antes de configurar o agente, conclua a integração do AD e do FMC.

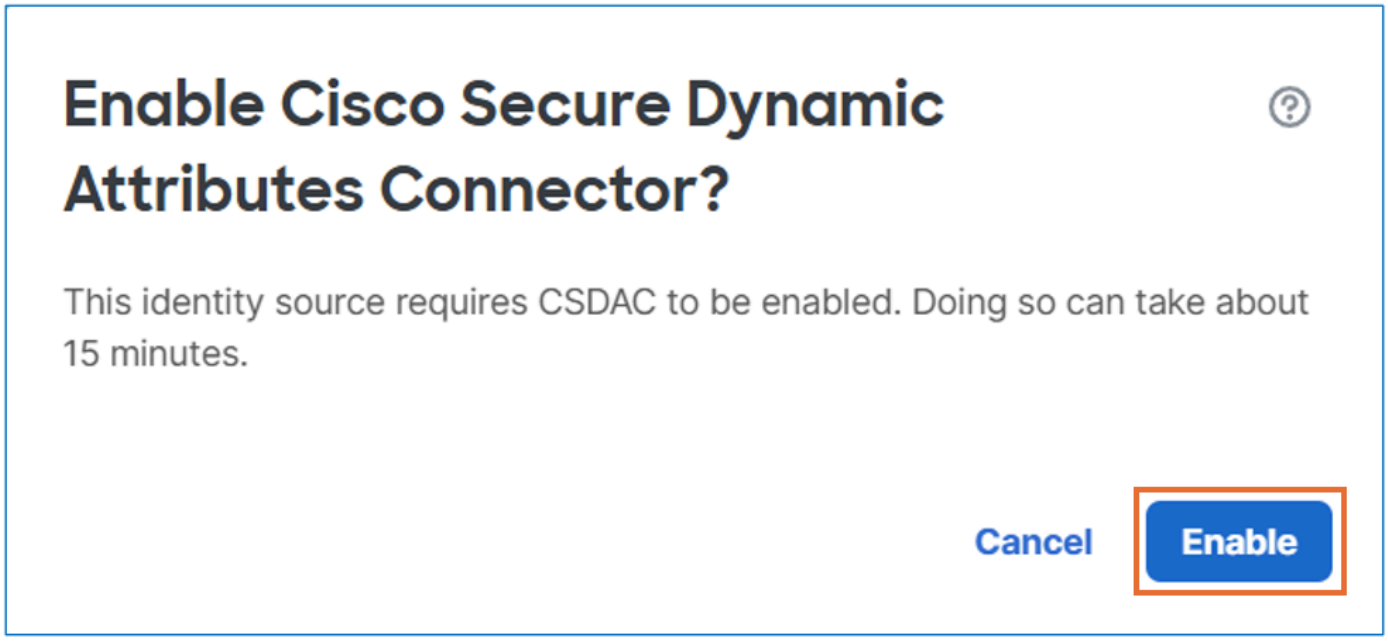
Configuração de uma Origem do Agente de Identidade Passiva

Na interface do usuário do FMC, navegue paraIntegração > Outras integrações > Fontes de identidade, clique em Agente de identidade passivo. Se o Cisco Secure Dynamic Attributes Connector ainda não tiver sido ativado, você será solicitado a fazê-lo clicando em Enable CSDAC.



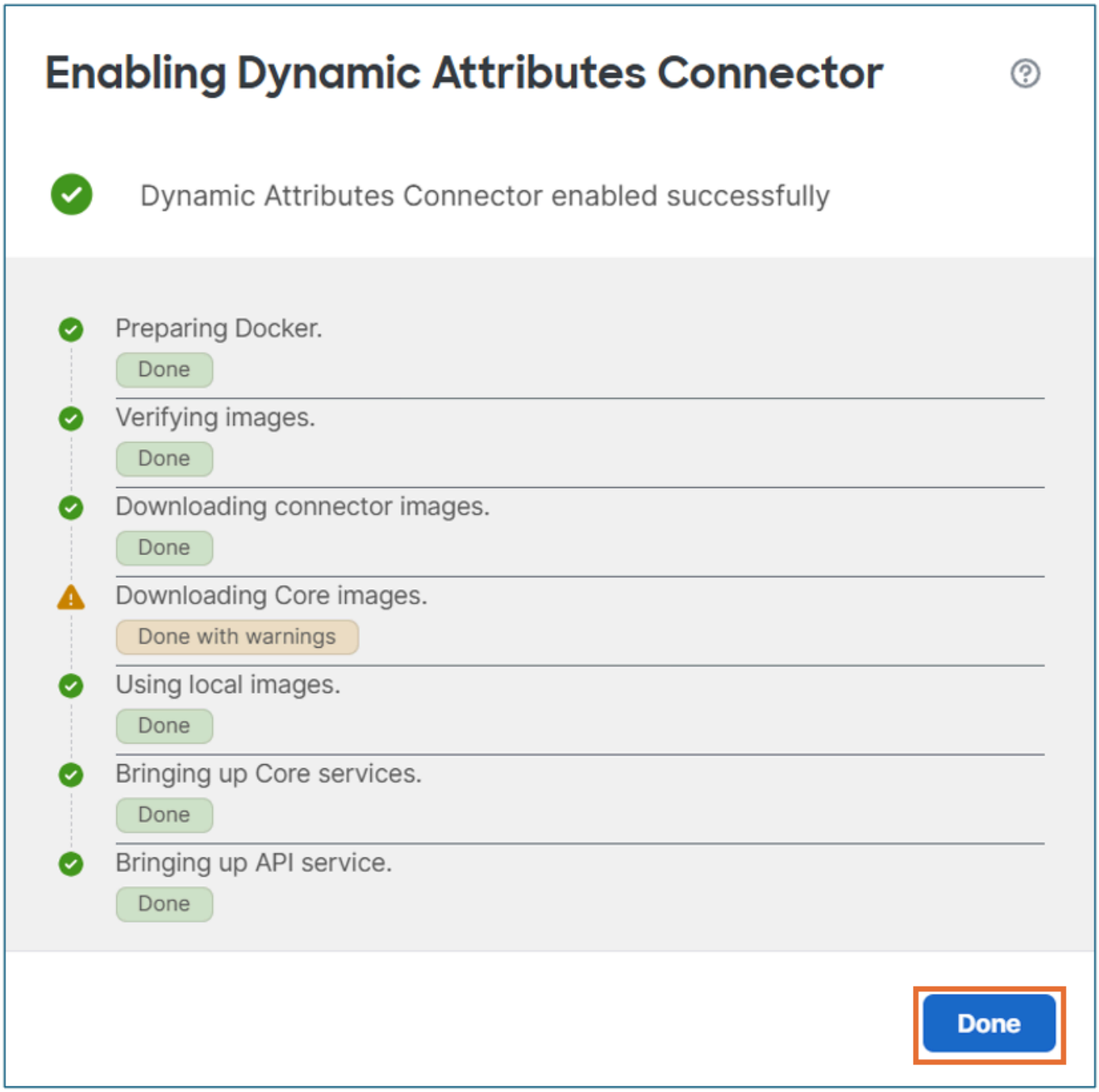
Agente de identidade passivo

Clique no botão Habilitar para habilitar o CSDAC.



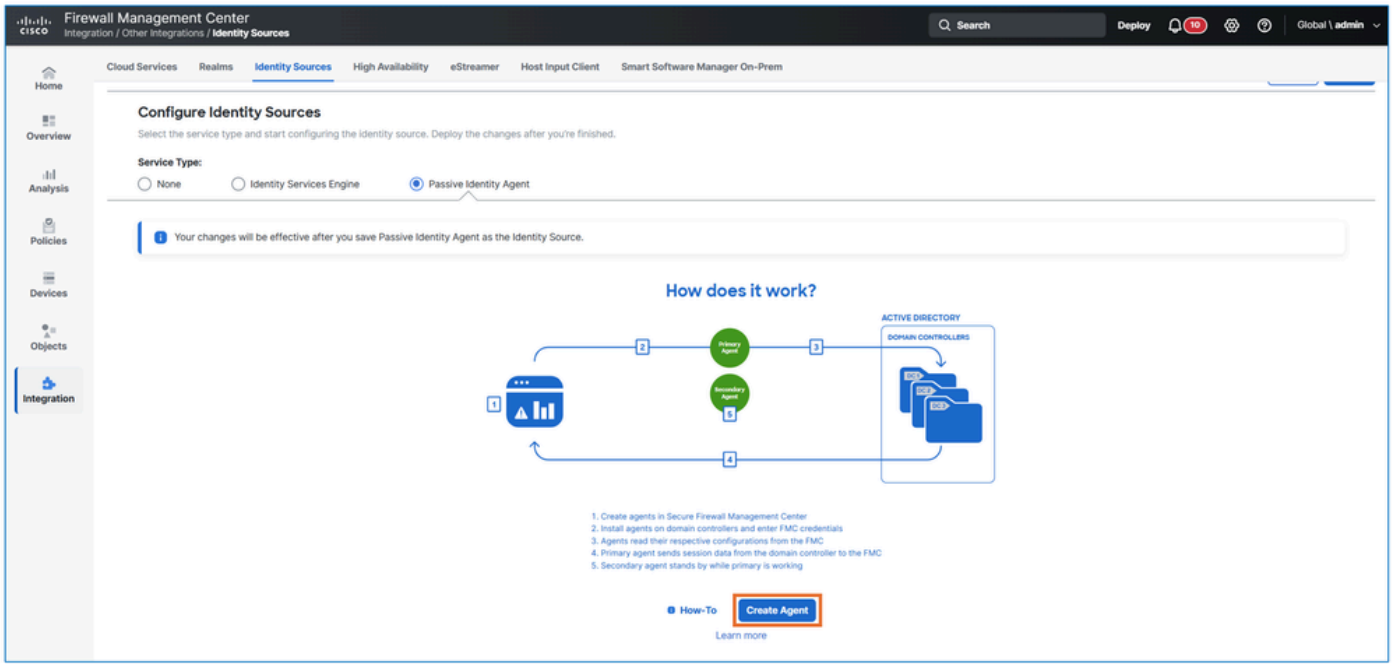
Habilitar CSDAC

Essa etapa leva aproximadamente 10 minutos. Depois que o CSDAC for ativado corretamente, clique no botãoConcluir para continuar.



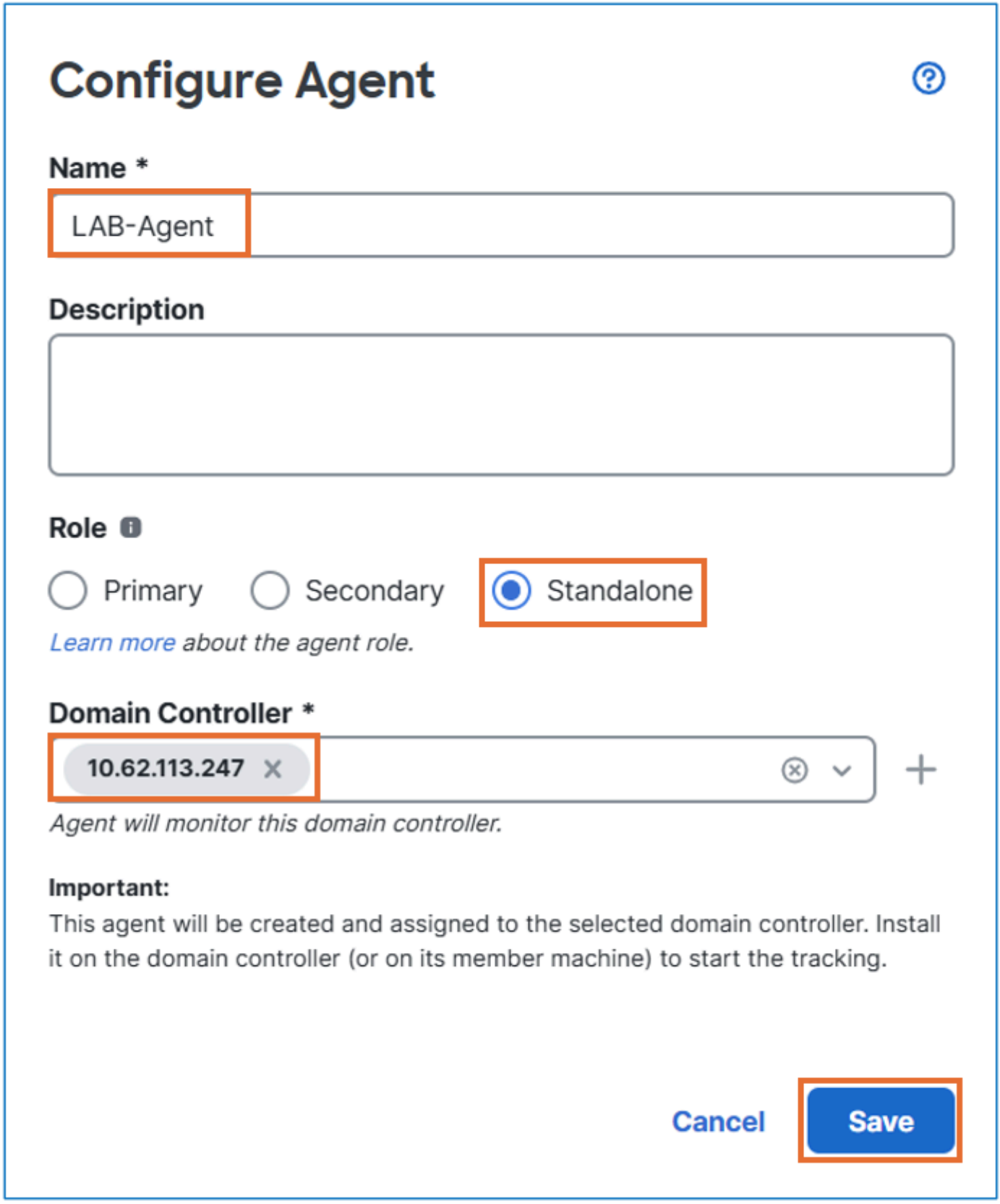
CSDAC Habilitado

Clique no botão Criar agente.



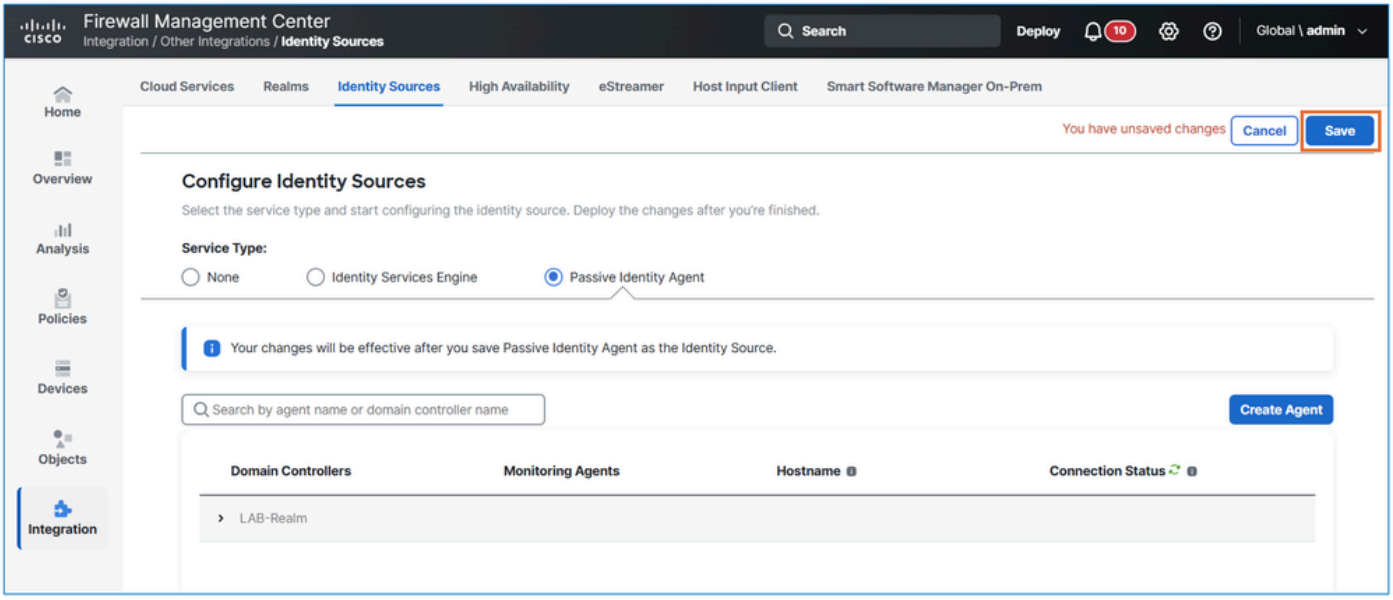
Criar agente

Defina um nome para o agente, selecione a opçãoIndependente e associe-a ao Controlador de Domínioapropriadocriado na tarefa anterior.



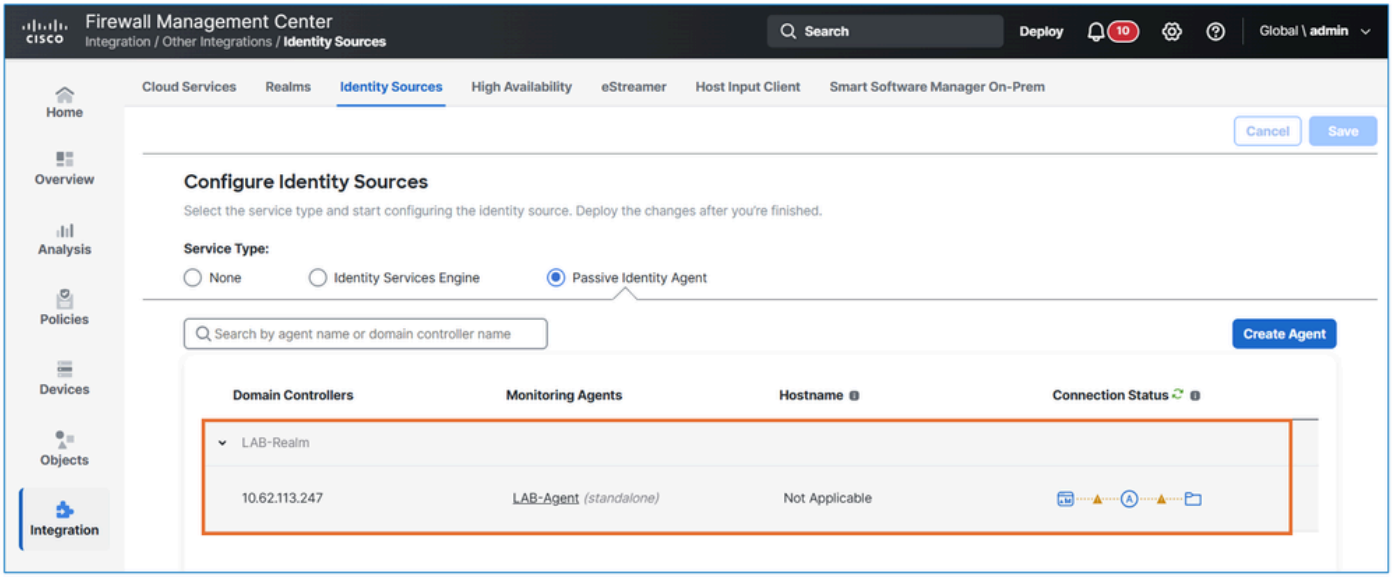
Configurar agente

Clique no botão Salvar.



Salve a configuração

O resultado.



Verificar o status

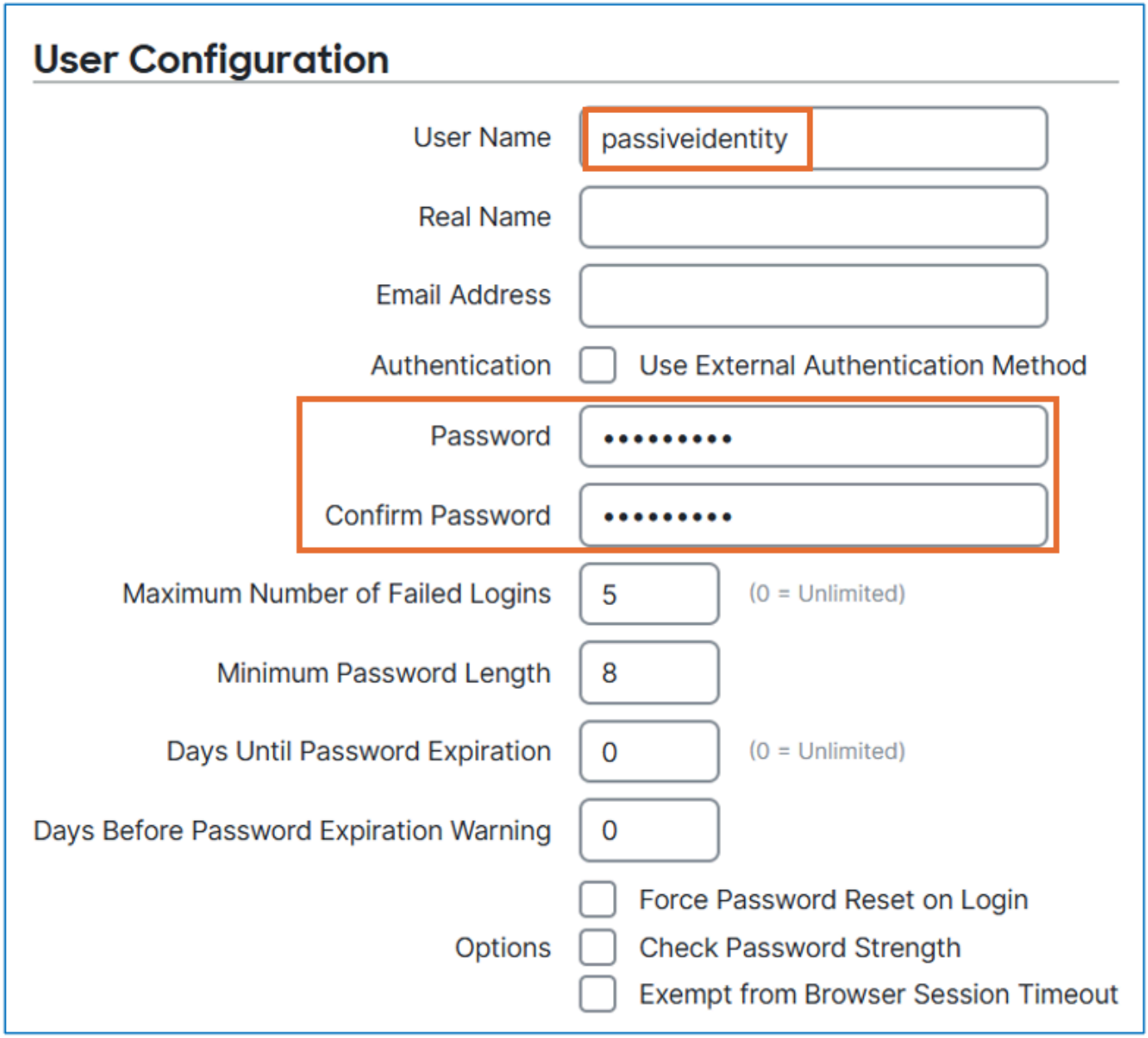
Note: O agente de identidade passiva indica o status usando linhas; âmbar significa que o agente nunca se comunicou com êxito com o Secure Firewall Management Center. Uma linha de agente recém-criada fica na cor âmbar e assim permanece até que a configuração seja concluída.

Criação de um usuário de agente de identidade passivo no Secure Firewall

Management Center

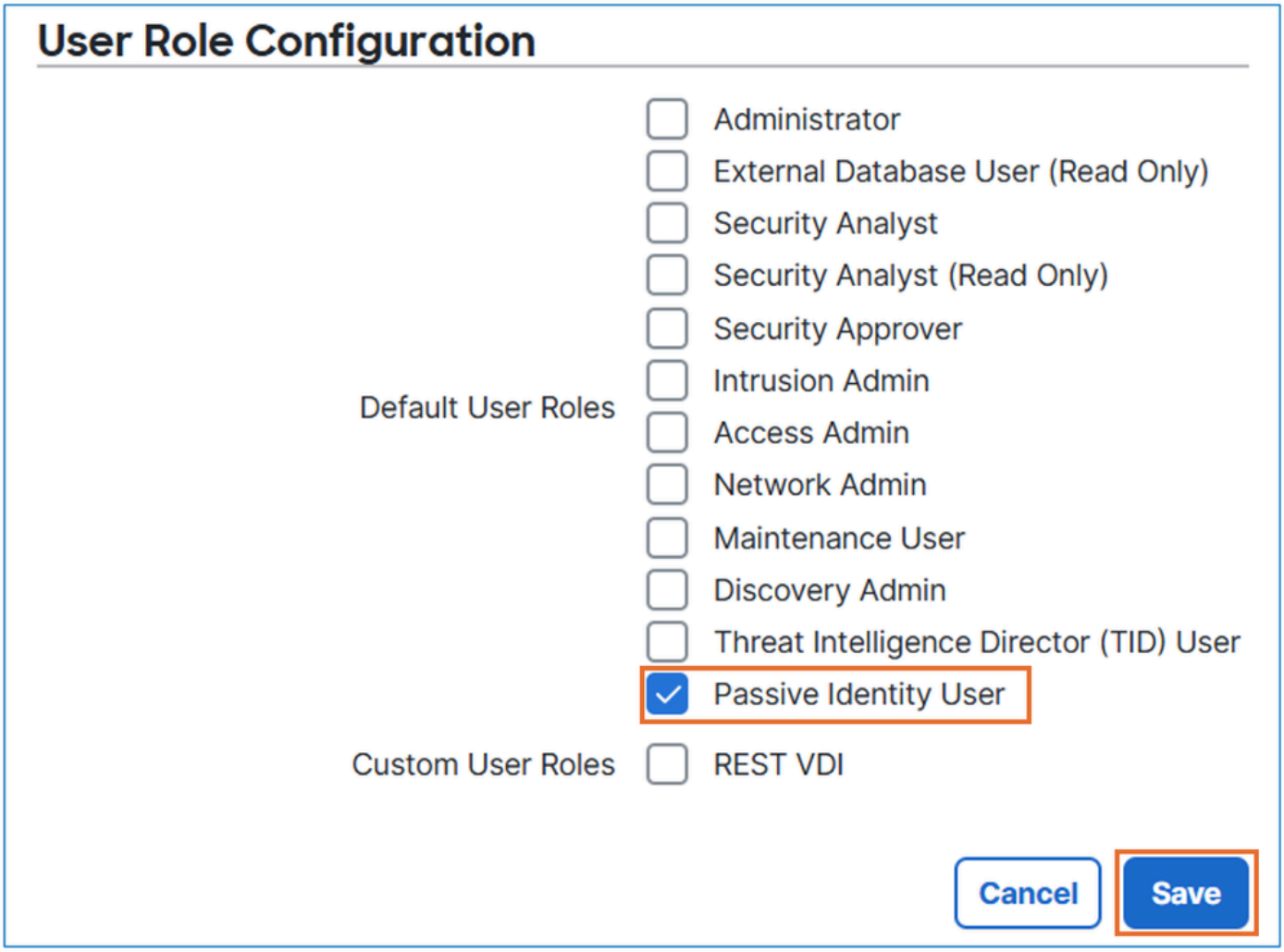
Crie um usuário do Centro de Gerenciamento de Firewall Seguro com permissões suficientes para se comunicar com o agente de identidade passiva. Esse usuário tem privilégios limitados para executar outras tarefas; espera-se que o usuário somente habilite a comunicação com o agente de identidade passiva.

Na interface do usuário do FMC, navegue paraSistema > Usuáriose clique em Criar usuário. Preencha os detalhes do usuário de acordo com os requisitos da tarefa.



Criar usuário

Atribua somente a função de usuário Identidade passiva. Clique no botão Salvar.

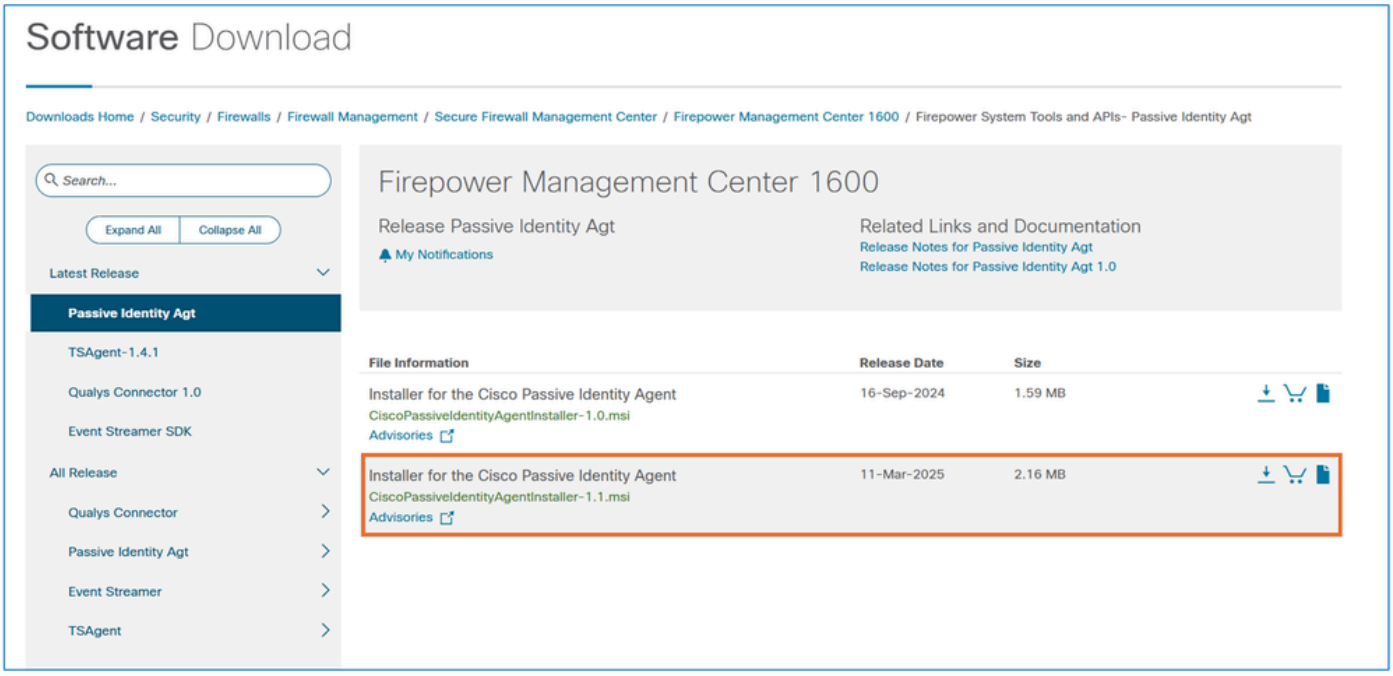


selecione o usuário de identidade passiva

Instalar e configurar o software Passive Identity Agent

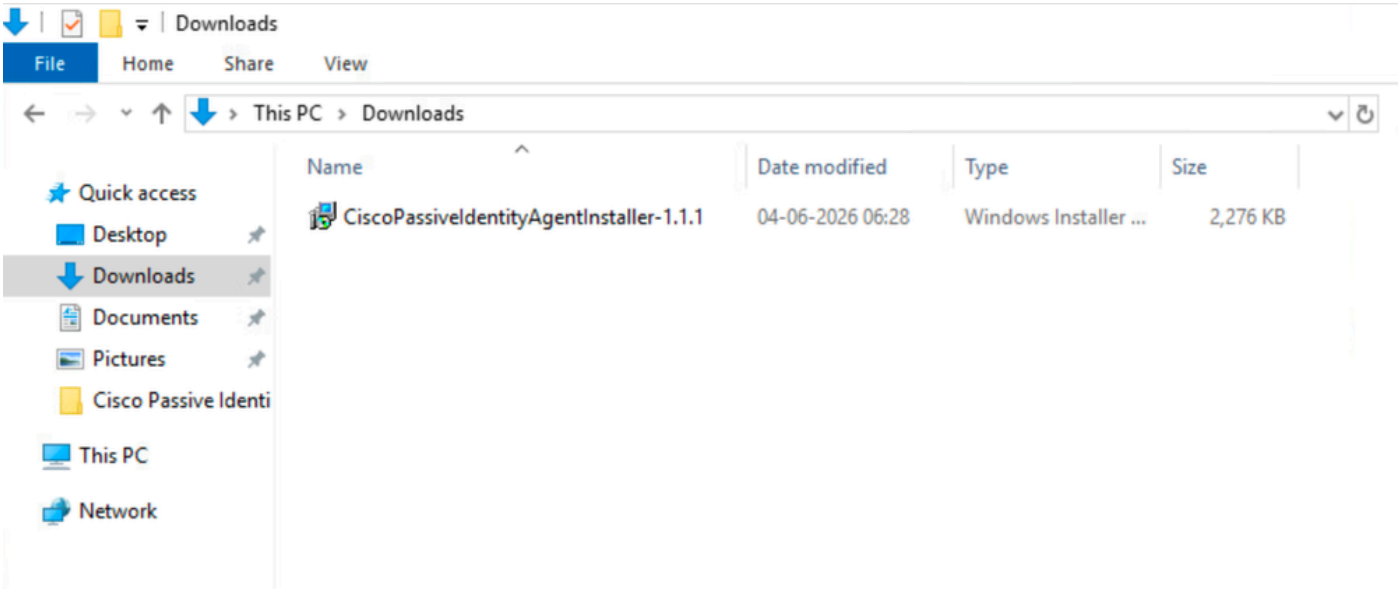
Instale e configure o software do Agente de Identidade Passiva no Controlador de Domínio designado.

Faça o download do agente de identidade passiva em software.cisco.com.



baixar o software

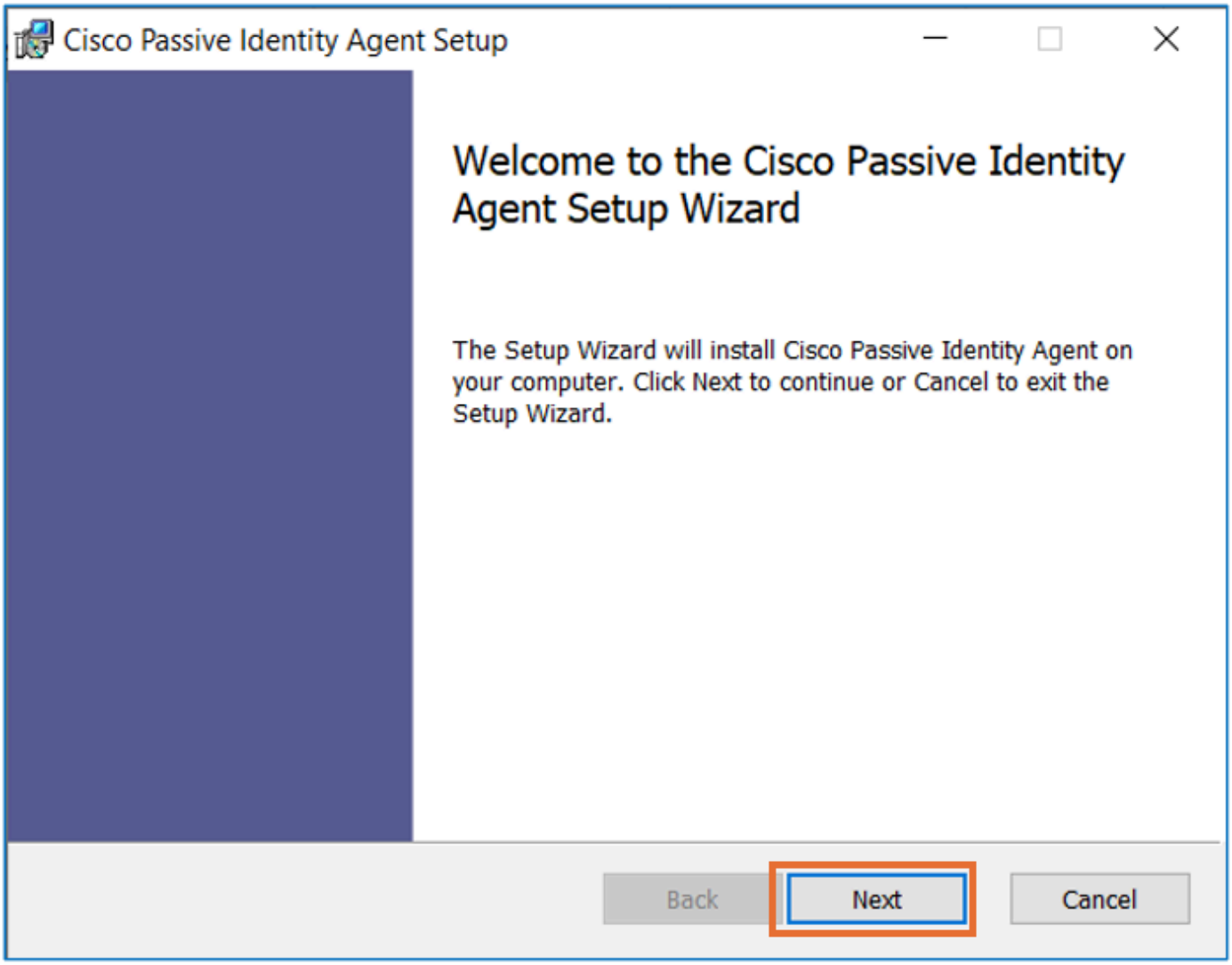
Após fazer o download do agente, inicie o processo de instalação no controlador de domínio.



agente

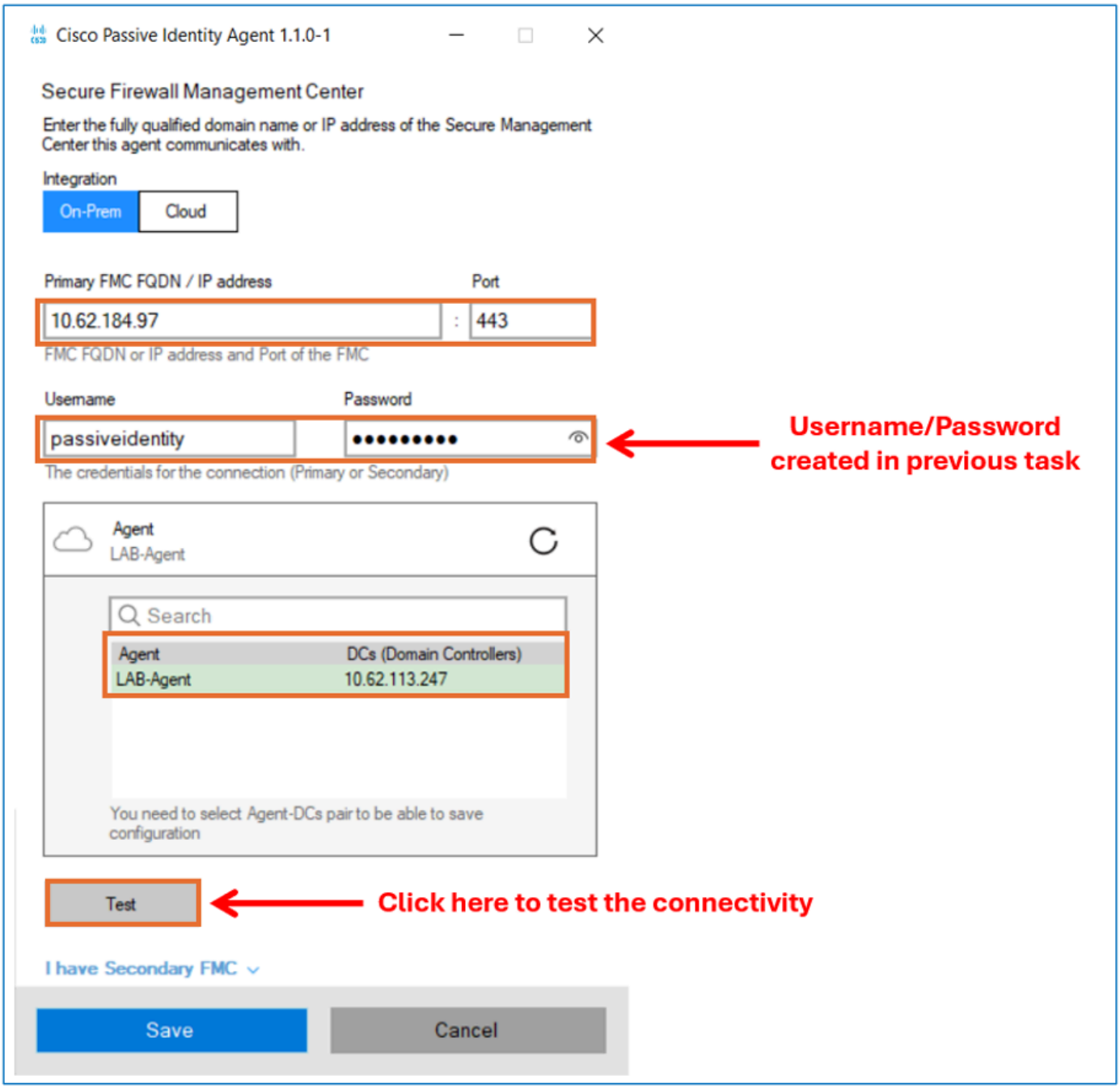
]

Consulte as instruções de instalação fornecidas para concluir a configuração.



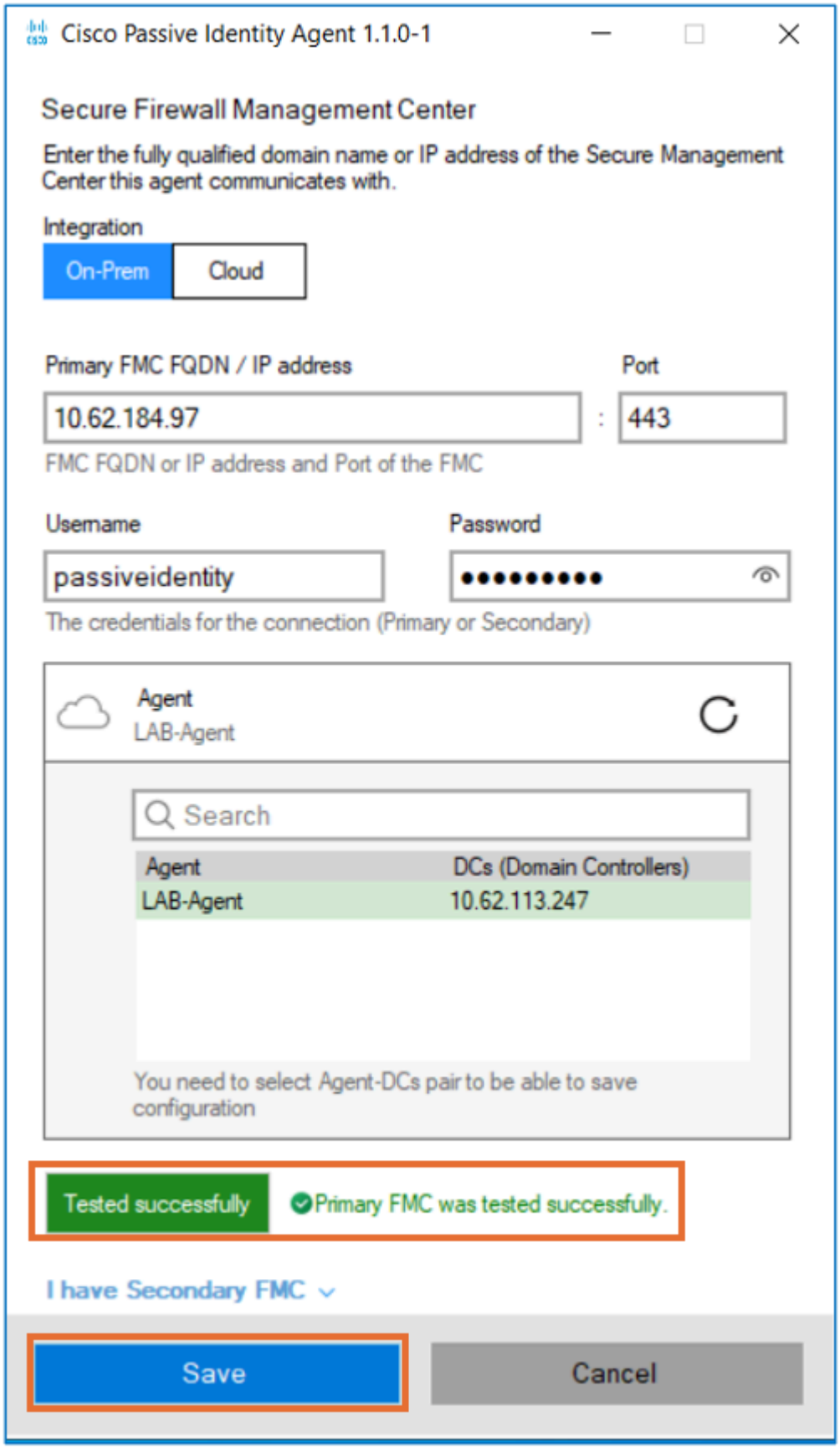
Instalação

Quando a instalação estiver concluída, abra o software Passive Identity Agent e insira as informações necessárias conforme especificado nos requisitos da tarefa. Clique no botão Test para verificar a conectividade com o FMC.



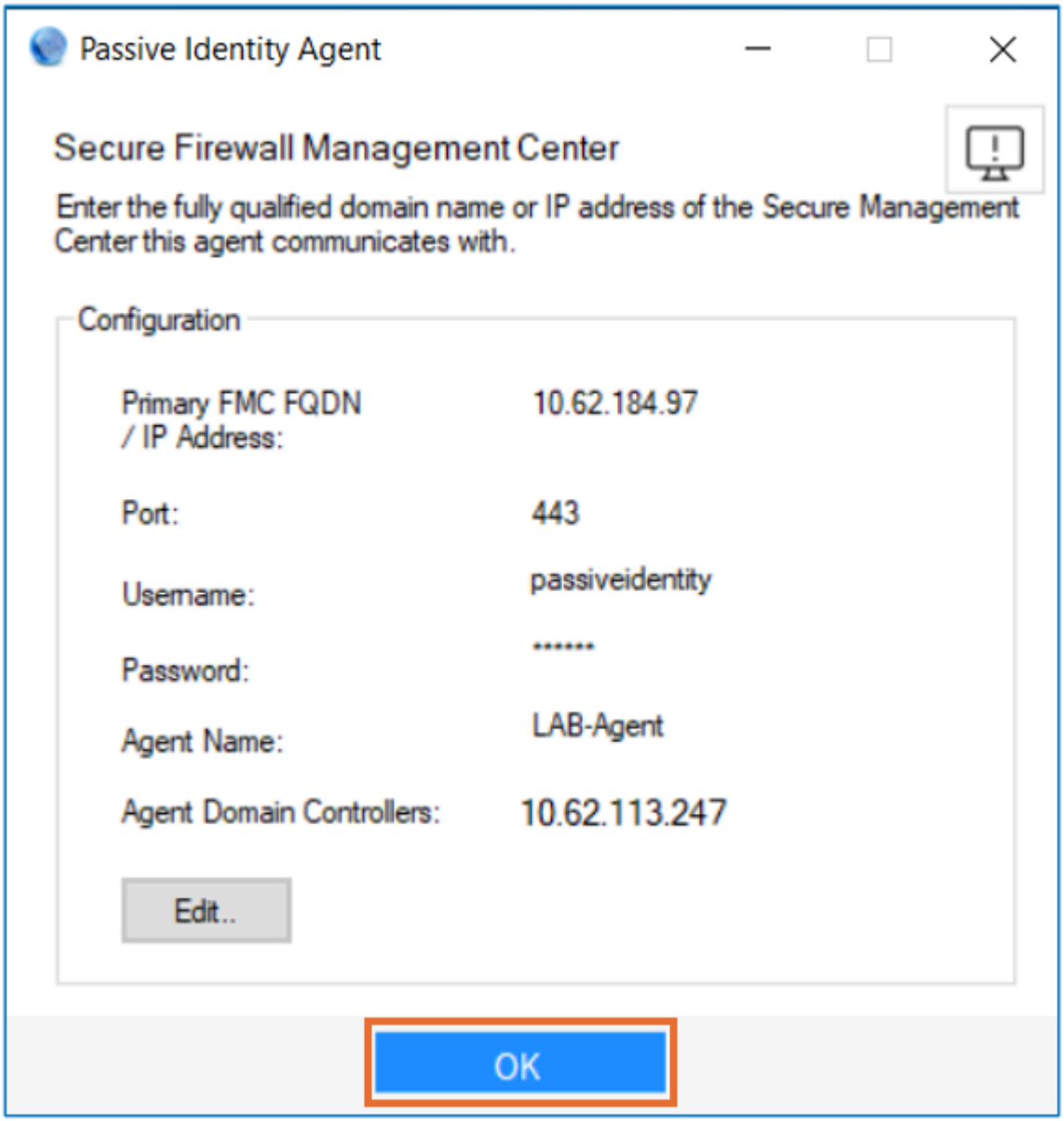
configurar o agente.

Depois de testar a conectividade com êxito, clique no botão Salvar.



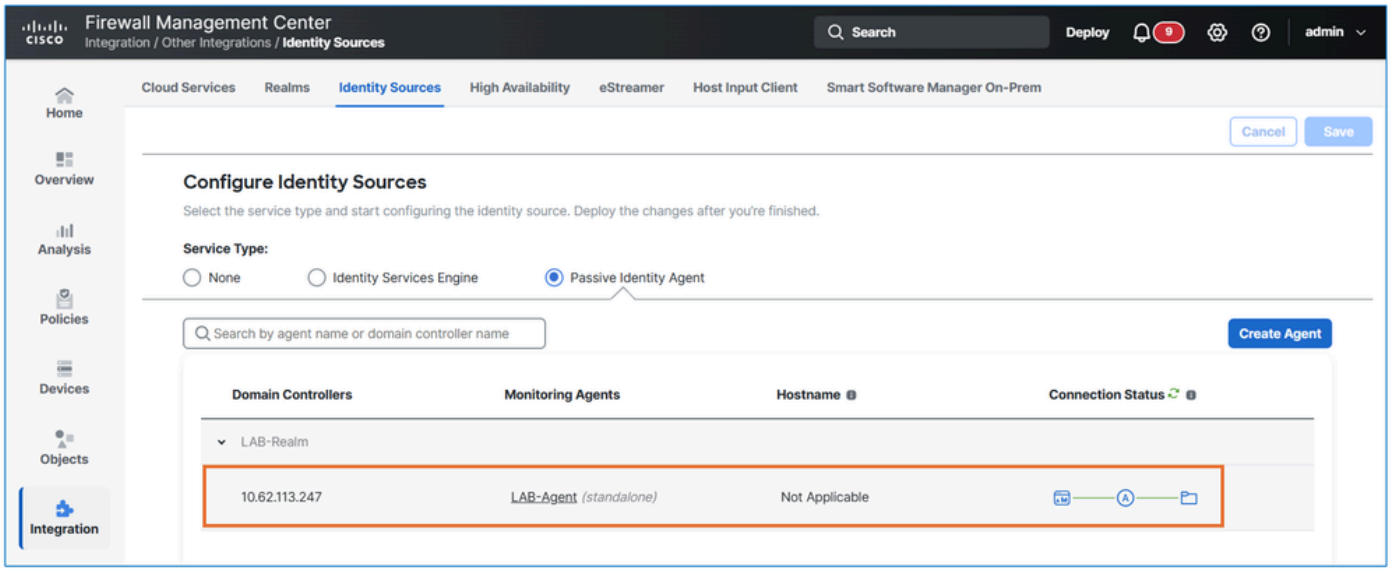
teste

Clique no botão OK para concluir a configuração do agente.



o agente está em execução

Na interface do usuário do FMC, navegue para Integração > Outras integrações > Fontes de identidade > Agente de identidade passivo. Confirme se o Agente de identidade passivo exibe um status verde.



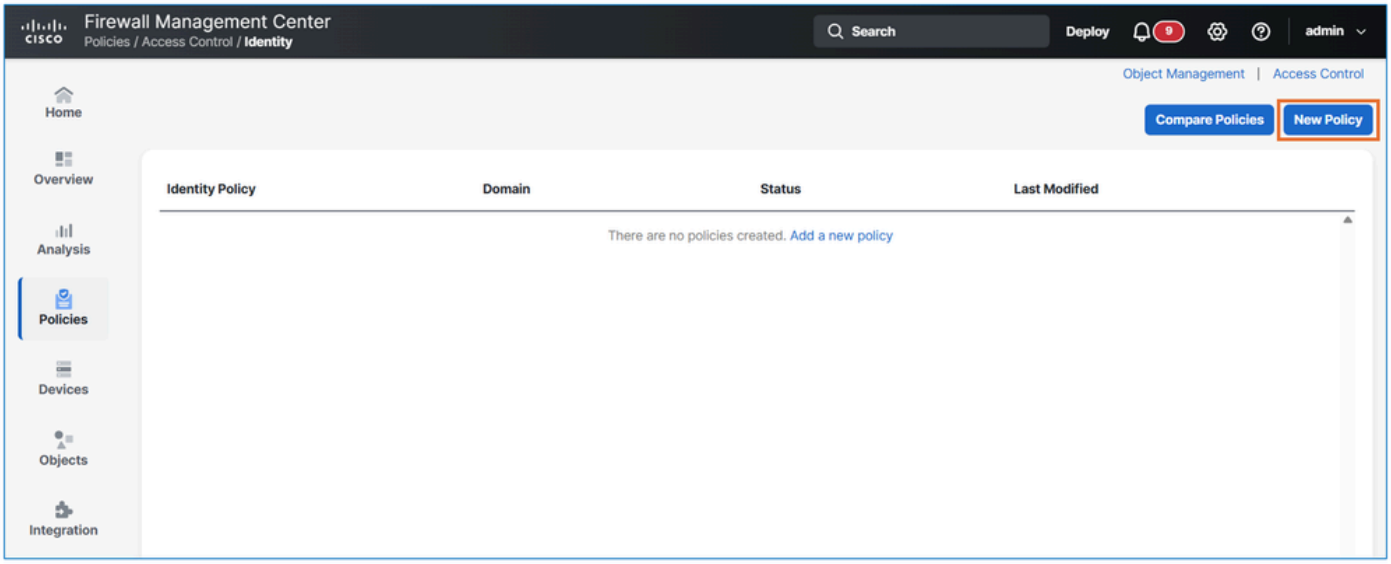
verificar a comunicação do fmc

Configurar políticas de identidade

Crie uma política de identidade com base na tabela fornecida.

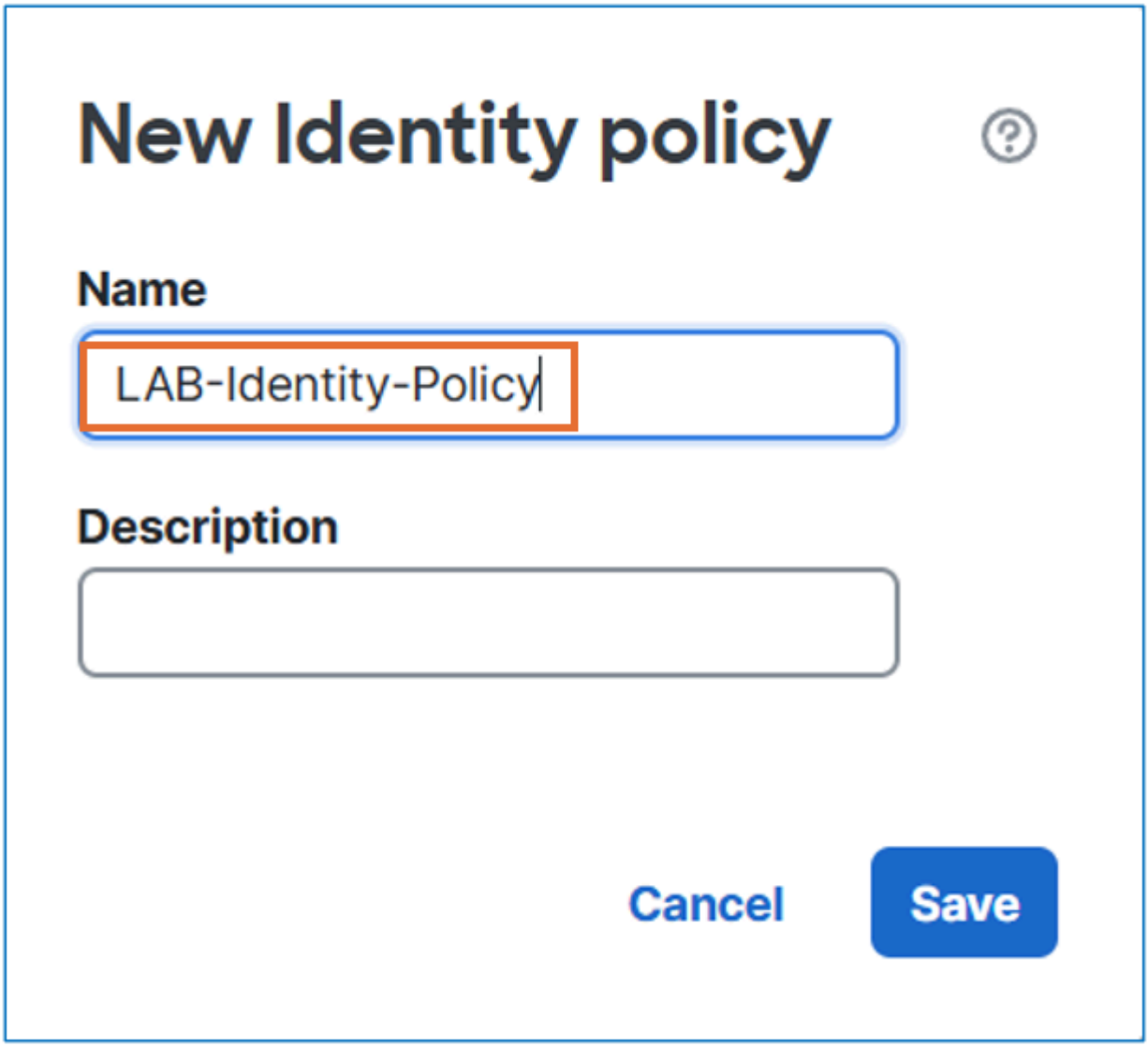
Nome da política	Nome da regra	Autenticação de território	Configurações restantes
LAB-Identity-Policy	Regra1	Território do LAB	Deixar como padrão

Na interface do usuário do FMC, navegue paraPolicies > Access Control > Identity. Clique no botãoNova política.



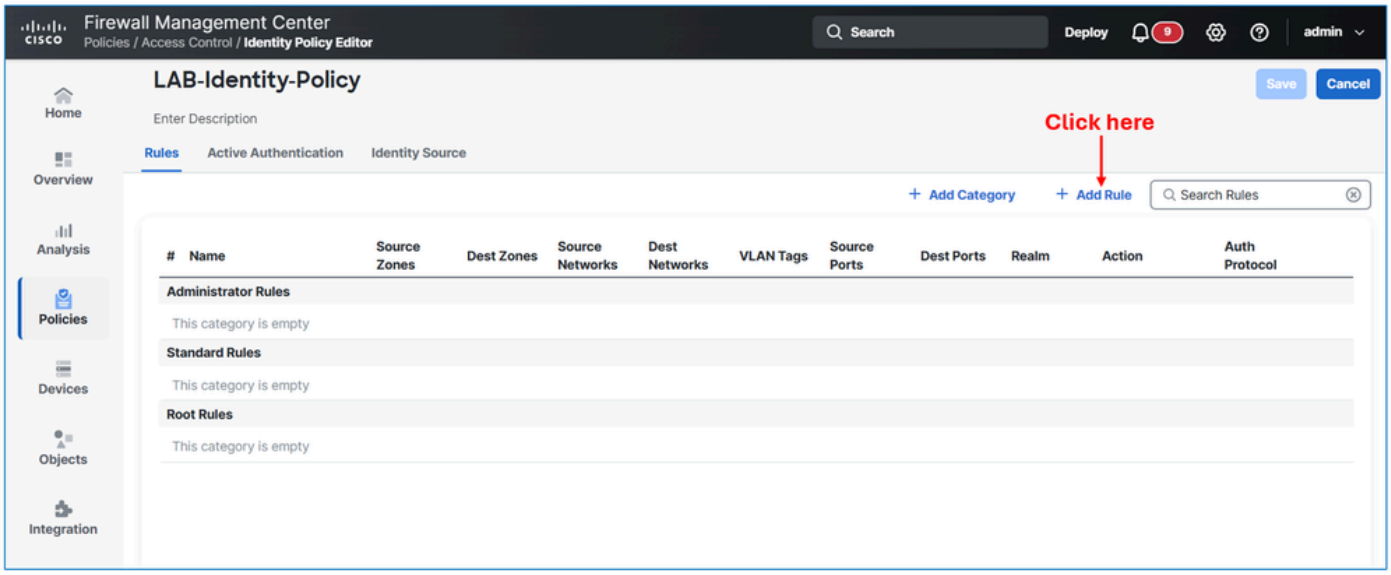
nova política

Insira o nome da política de acordo com os requisitos da tarefa.



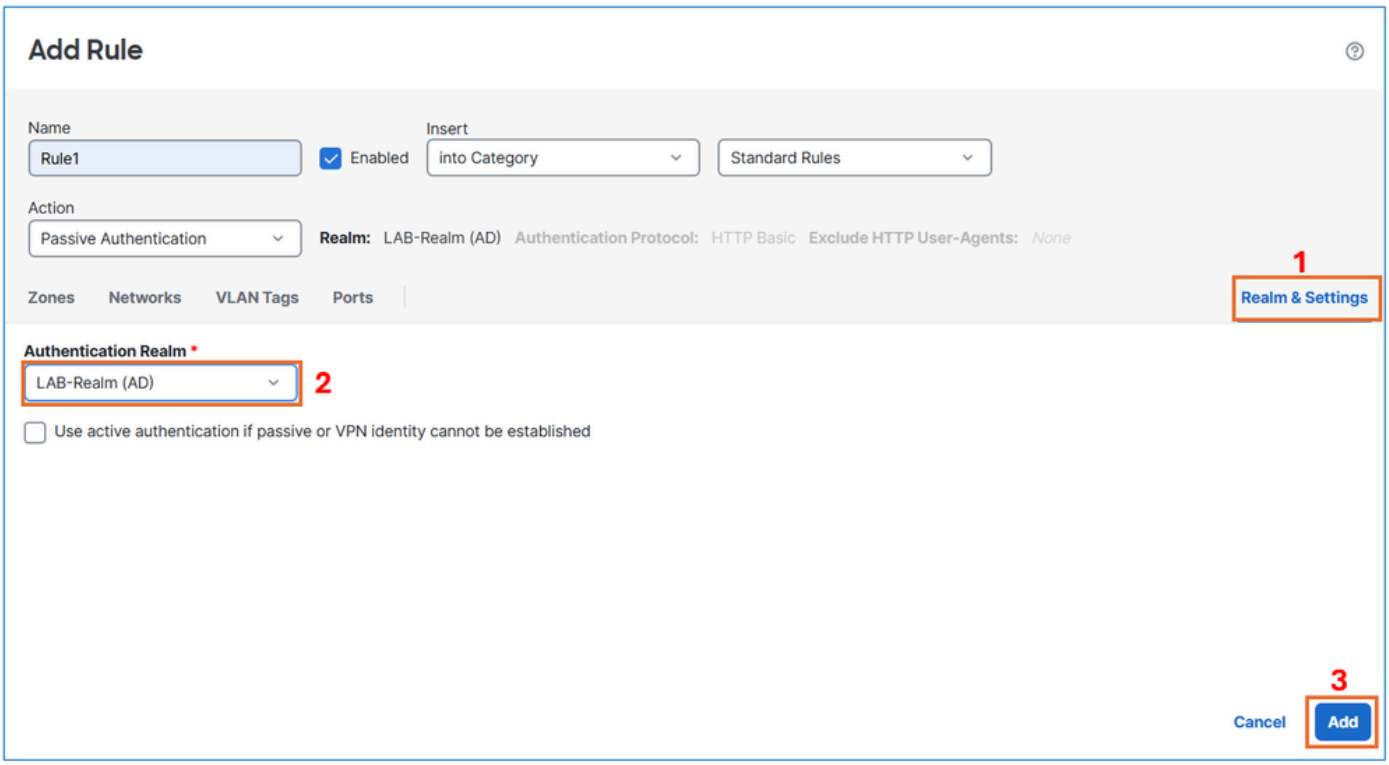
nova política

Clique no botão Adicionar regra.



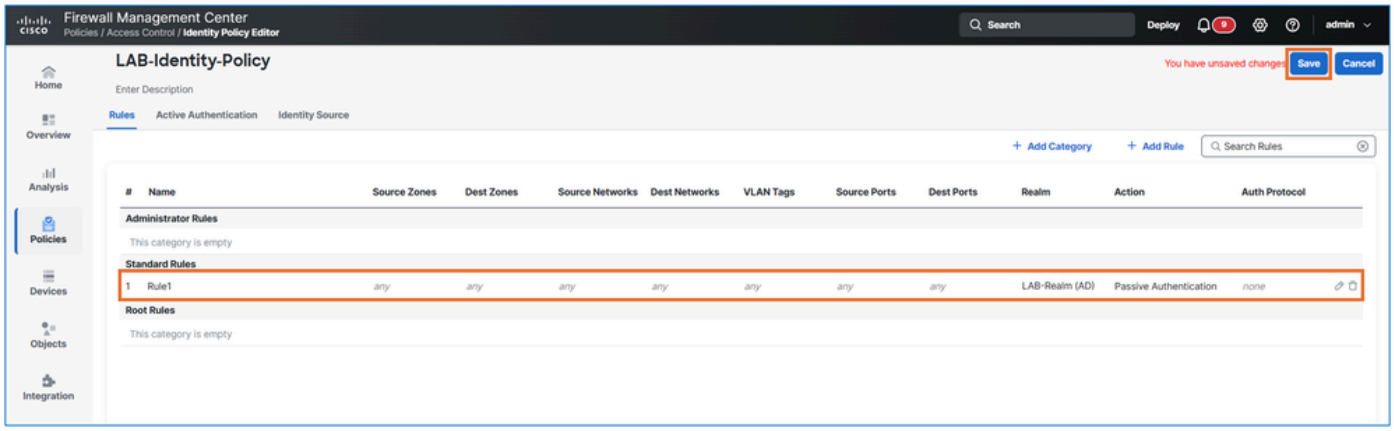
criar regra

Navegue até a guia Realm & Settings e selecione oRealm de autenticação com base nos requisitos da tarefa. Finalmente, clique no botãoAdd.



Configuração de território

Clique no botão Salvar.



salvar a configuração

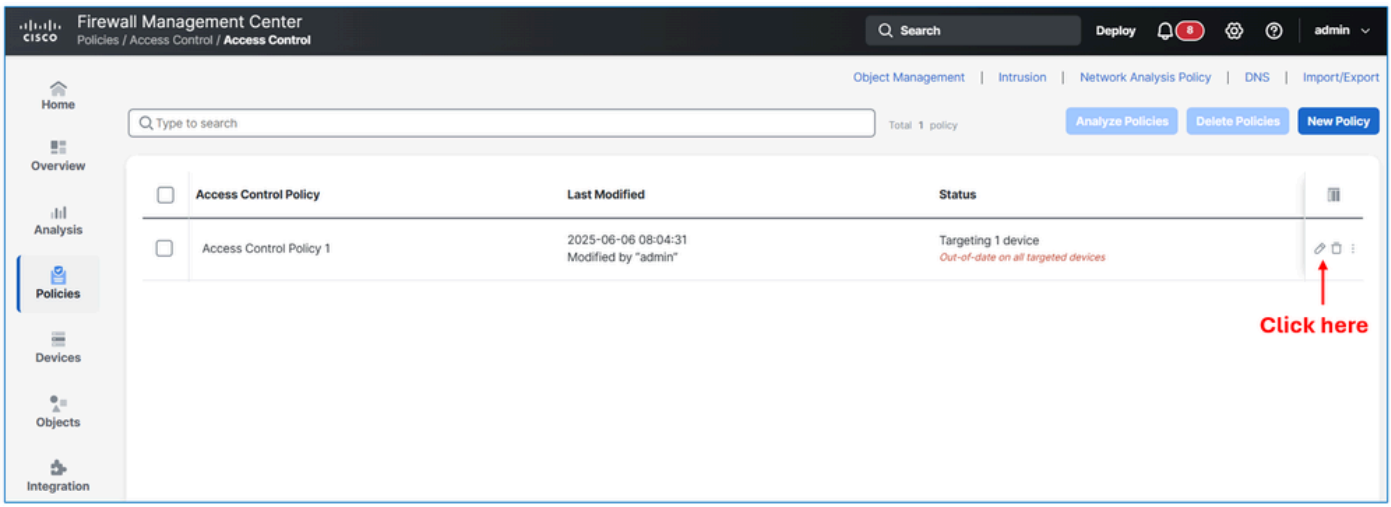
Configurar Políticas de Controle de Acesso

Vincule a política de identidade à política de controle de acesso e crie uma regra de política de acesso com os atributos:

Nome do atributo	Valor
Nome da regra	Regra1
Ação	Permissão
Zona de Origem	Interna
Zona de destino	Externa
Redes de Origem	10.10.10.0/24
Redes de destino	10.48.62.98/32
Serviço	Porta Dest TCP 80 (HTTP)
Usuários	LAB-Realm/GROUP1
Registro	No fim da conexão

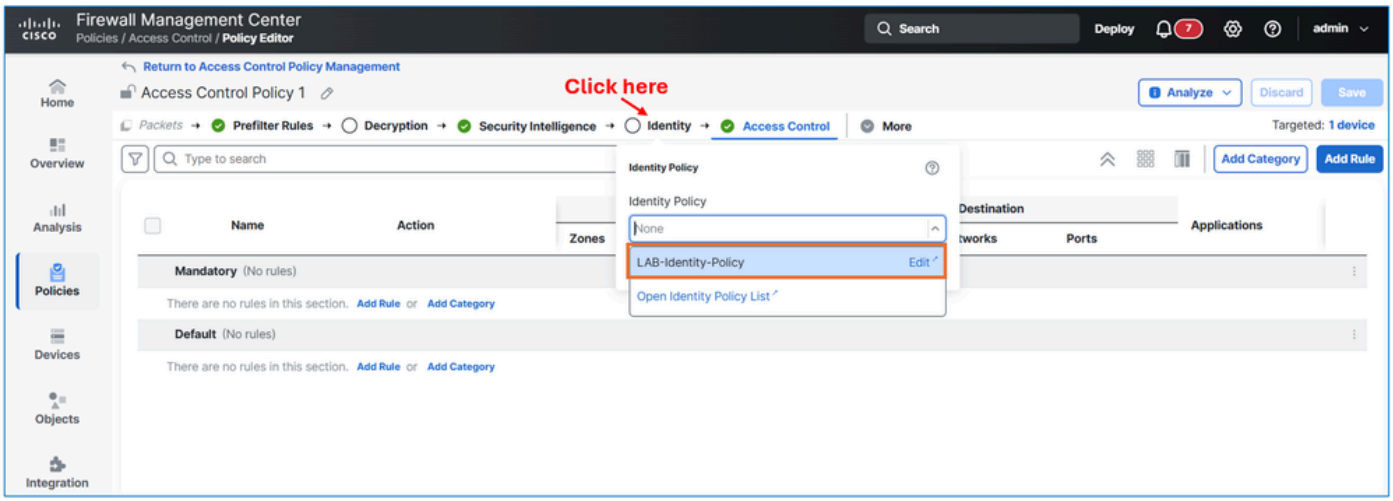
Etapa 1. Vincular a política de identidade à política de controle de acesso

Na interface do usuário do FMC, navegue paraPolicies > Access Control > Access Control. Clique no botão Editar da política.



Editar política

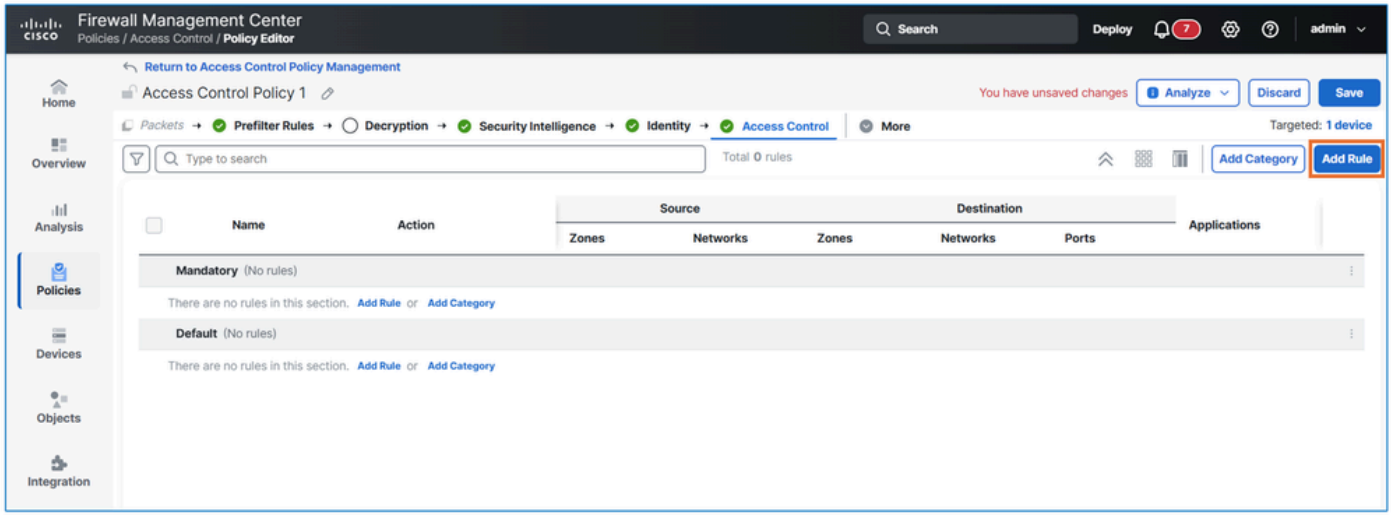
Navegue até aSeçãoIdentidade e vincule a Política deIdentidade criada na tarefa anterior.



adicionar política de identidade

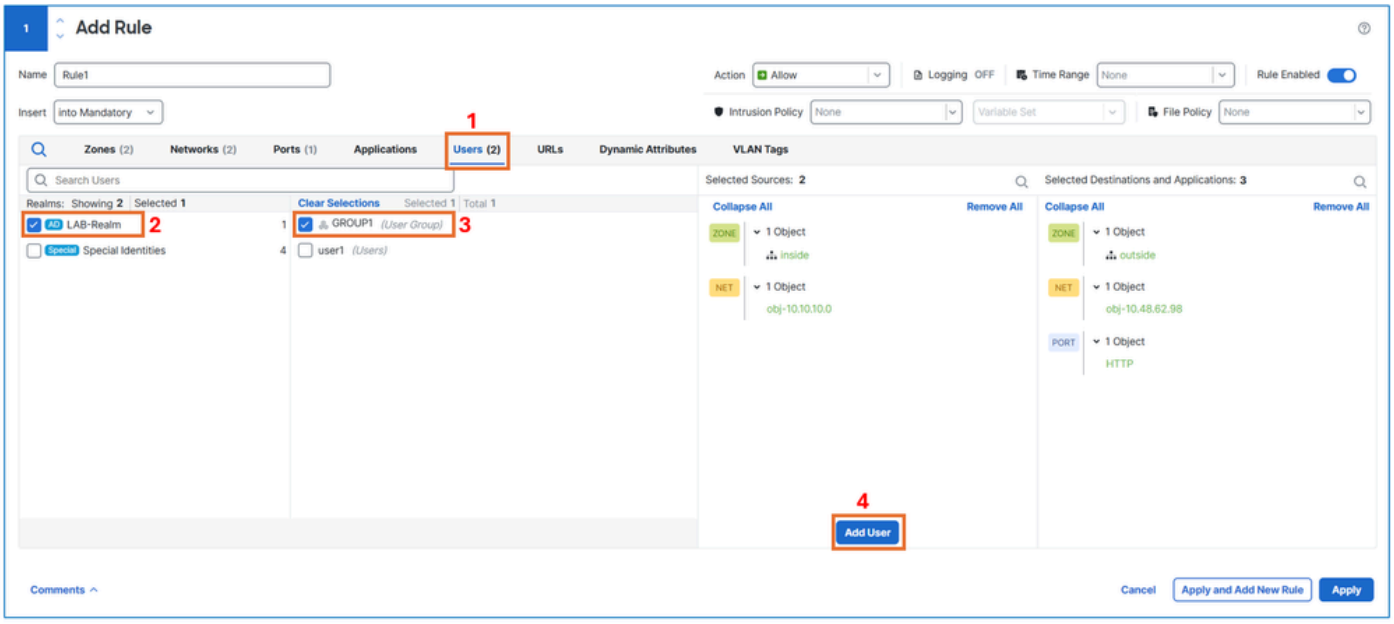
Clique no botão Aplicar

Etapa 2. Crie a Regra de Controle de Acesso.



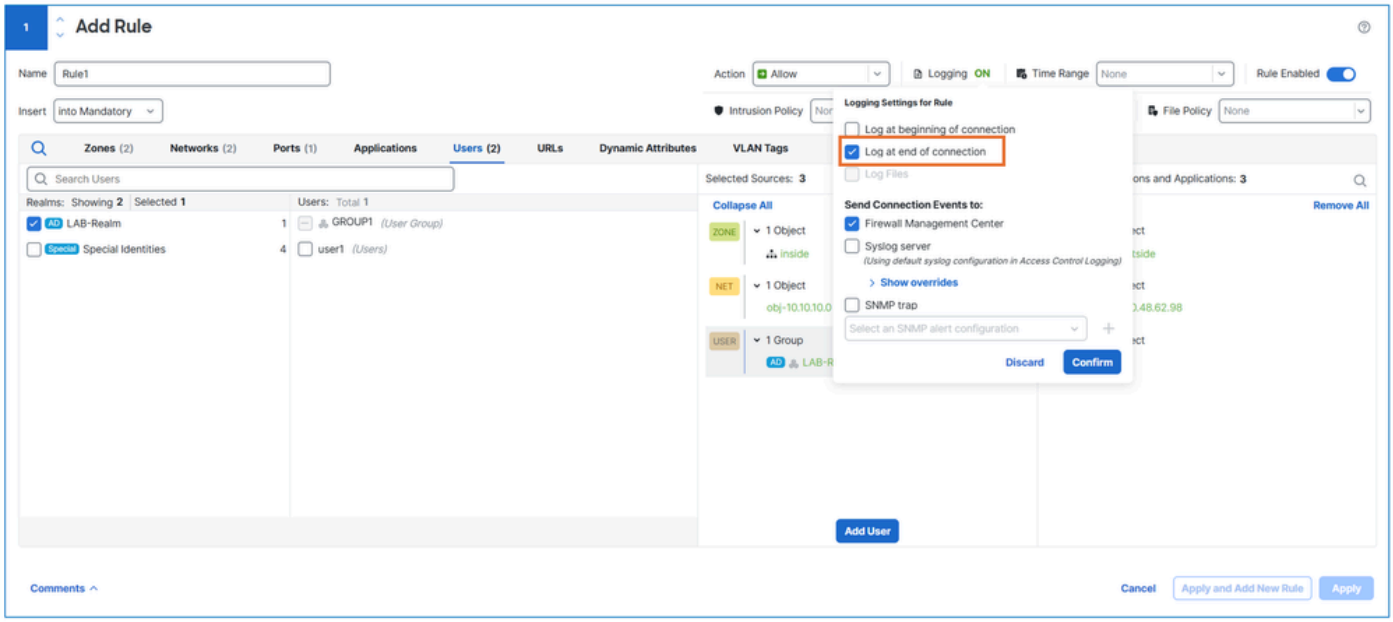
criar ACP

Insira os detalhes de acordo com os requisitos da tarefa e, mais importante, na guia Usuário, addGROUP1fromLAB-Realm.



adicionar usuários à regra

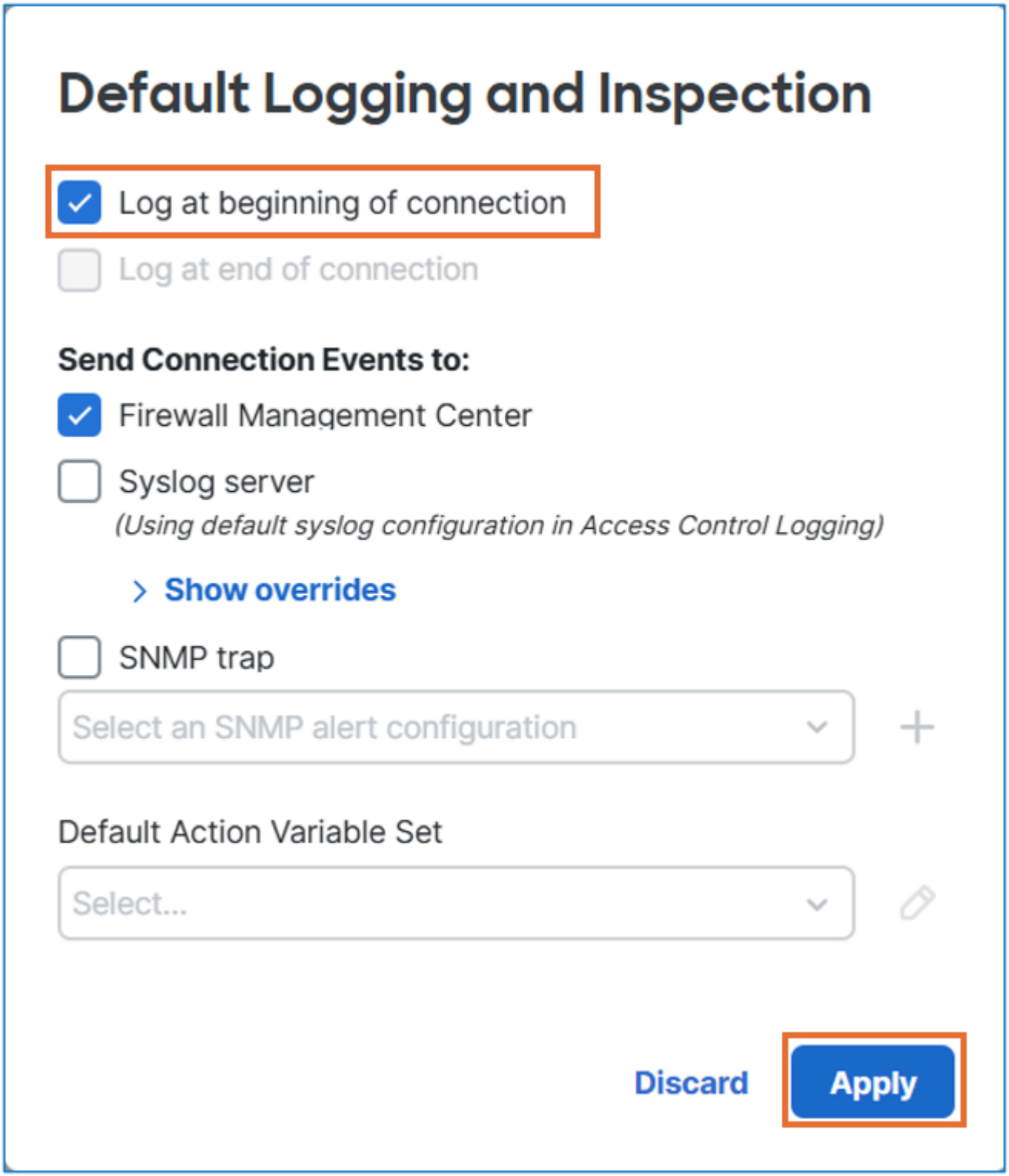
Ative o registro para a regra selecionandoRegistrar no final da conexão.



Habilita o registro em log

Etapa 3. Ative o registro para a ação padrão.

Clique no íconede configurações para modificar as configurações padrão do registro de ações.



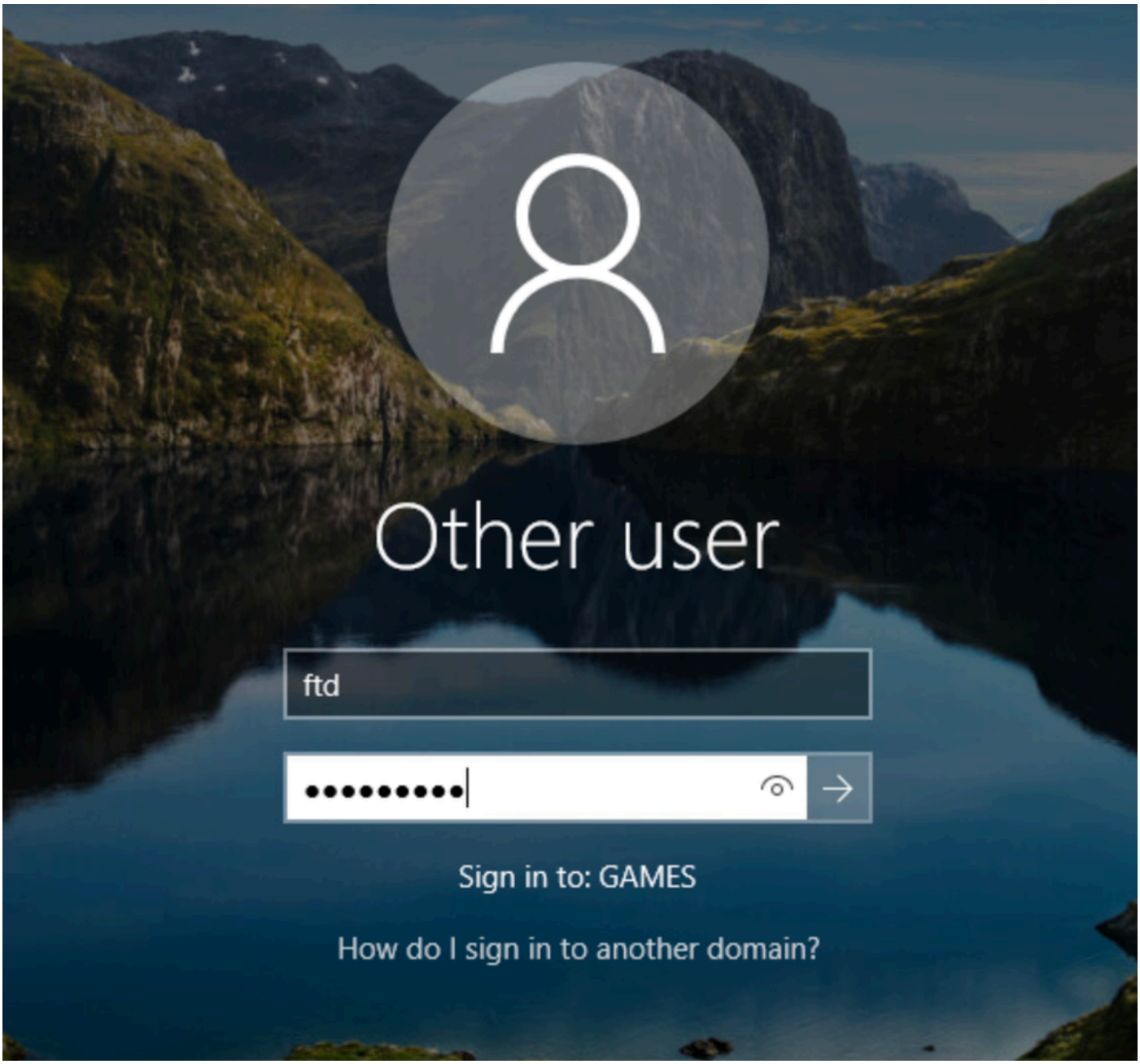
Habilita o registro em log

Salve e implante a configuração no FTD.

Verificação

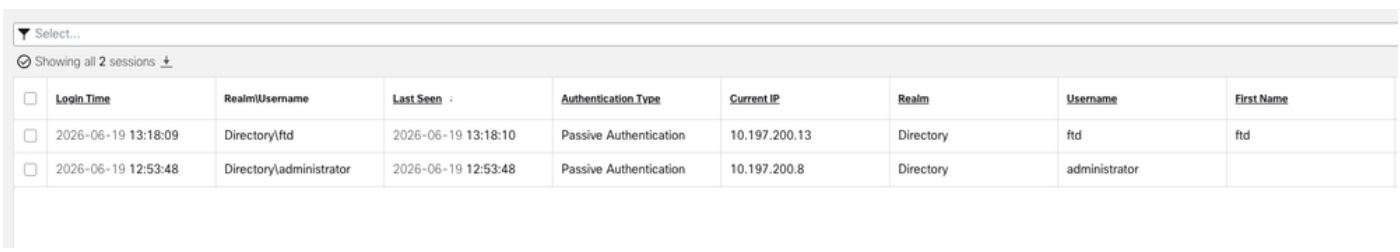
Verifique a operação de Identidade Passiva confirmando se o tráfego é permitido exclusivamente para ftd.

Faça login no domínio usuário do computador do usuário.



login de usuário

Depois que um usuário fizer login com êxito, verifique no FMC em Analysis> user >ative session para exibir os detalhes do usuário ativo.



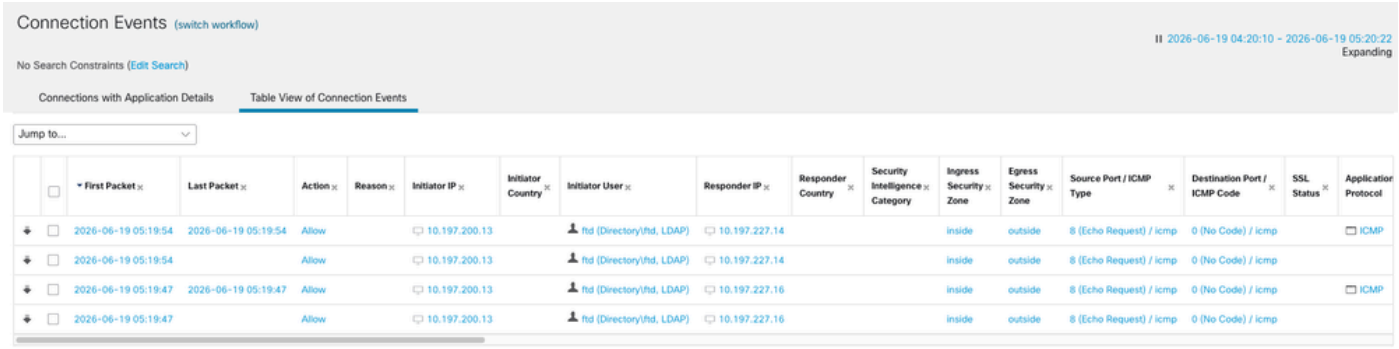
Select...

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	

Sessões ativas

Depois de iniciar alguma verificação de tráfego a partir dos eventos de conexão, consulte os detalhes do usuário nos eventos de conexão.

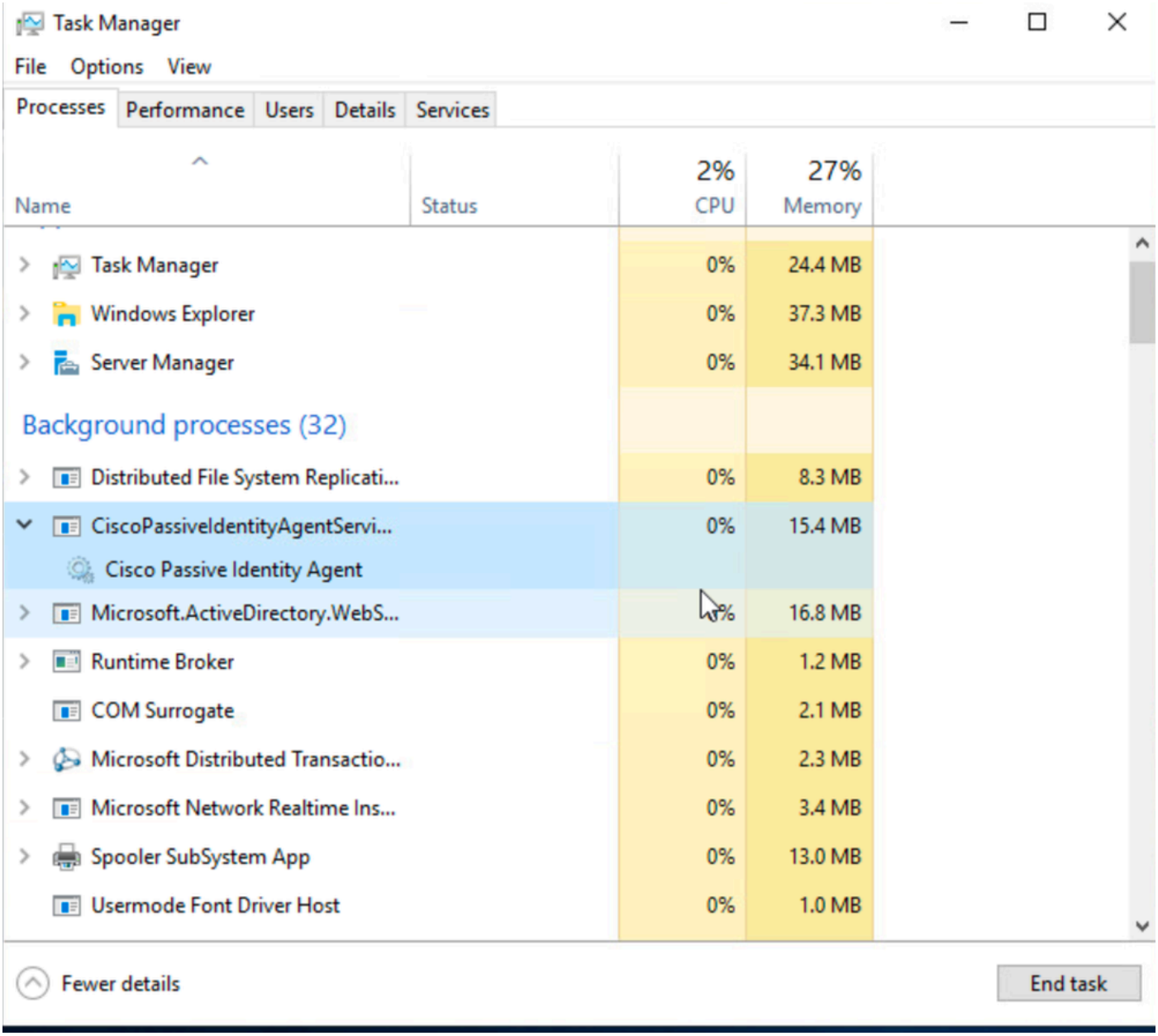


Sessões ativas

Troubleshooting

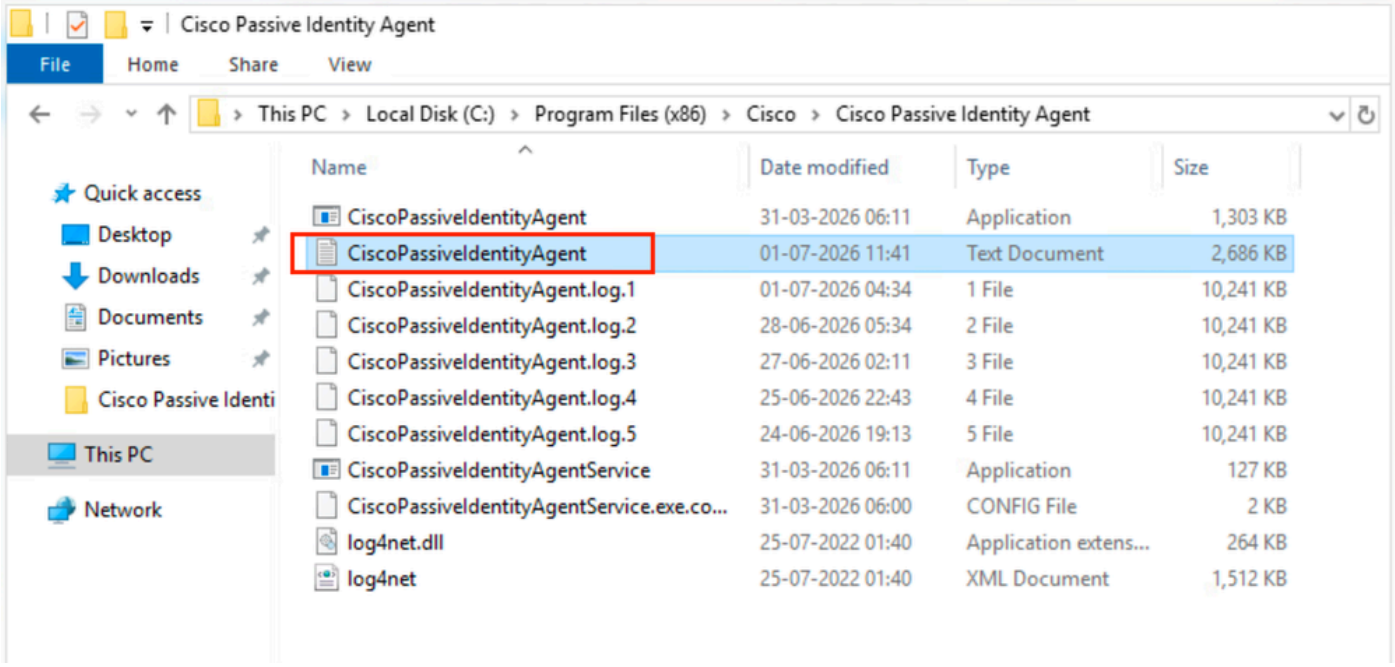
Verificando Logs de Agentes

Na máquina Windows que hospeda o Agente, abra o Gerenciador de Tarefas e verifique se o processo em segundo planoCiscoPassiveIdentityAgentService está em execução.



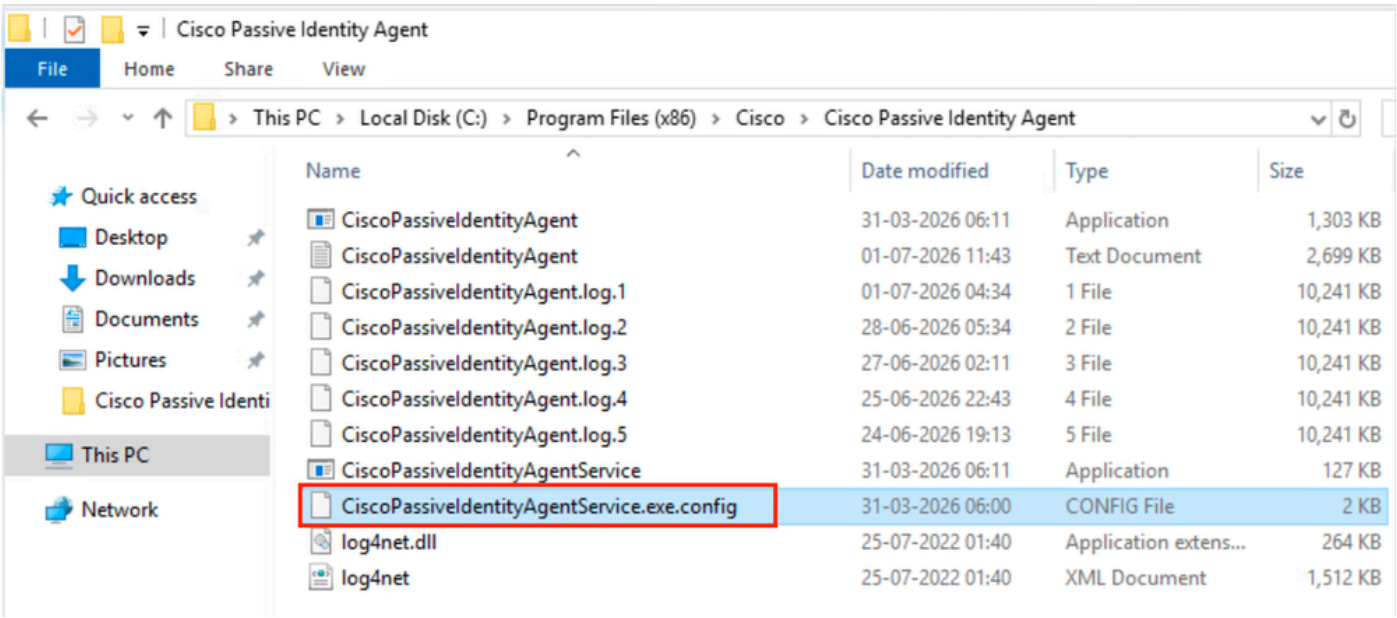
Executando tarefa

Os logs do agente podem ser encontrados nos arquivos CiscoPassiveIdentityAgent, localizados por padrão em: "Arquivos C:\Program (x86)\Cisco\Cisco Passive Identity Agent\".



agente

Por padrão, os logs do agente são definidos para o nível deINFORMAÇÕES. Para habilitar o log de nível DEBUG, modifique o arquivo de configuração CiscoPassiveIdentityAgentService.exe.e defina o nível de log como ALLorDEBUG.



configuração de agente

log de informações

Verificando Logs de Agentes - Buscar Configuração do Agente.

INFO Cliente Rest, Eventos em massa: [f"domain":"jogos.cisco.com", "srcIpAddress": "X.X.X.X", "usuário": "fdm", "timestamp": "19-07-2026

INFO Cliente Rest, Status do Mapeamento: OK

INFO Cliente Rest, postagem REST bem-sucedida para fdm userBatch, latência = 0, DC TIME atual em UTC: 01/07/2026 19:47:34 Usuário conectado em

INFO Rest Client, solicitando configuração do agente

Registros FMC

Execute este comando para ver se o mapeamento de usuário para IP foi recebido do 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#
```

saída de FMC

Se o comando anterior não mostrar nenhum mapeamento, colete esses registros e entre em contato com o TAC da Cisco.

Esta é uma lista de logs relevantes para a API do FMC. O log de cauda de igel abrange todos eles.

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.