

Configurar o Passive Identity Agent usando o FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurações](#)

[Configuração de uma Origem do Agente de Identidade Passiva](#)

[Criação de um usuário de agente de identidade passivo no Secure Firewall Management Center](#)

[Instalar e configurar o software Passive Identity Agent](#)

[Configurar políticas de identidade](#)

[Configurar Políticas de Controle de Acesso](#)

[Verificação](#)

[Troubleshooting](#)

[Verificando Logs de Agentes](#)

[Registros FMC](#)

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 Active Directory 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 Active Directory em execução no Windows Server 2022.

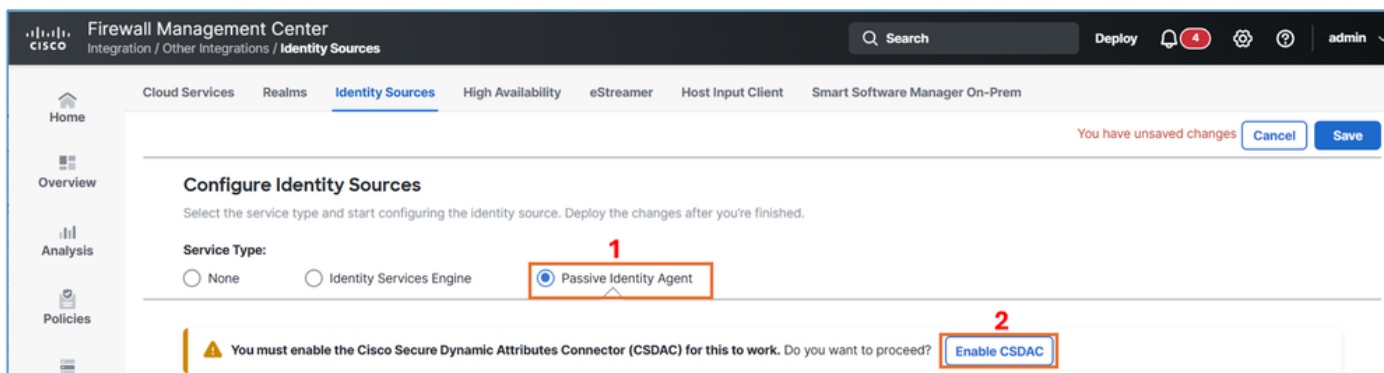
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

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

Essa etapa leva aproximadamente 10 minutos. Depois que o CSDAC for ativado corretamente, clique no botão Concluir 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 Habilitado

Clique no botão Criar 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?

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

Criar agente

Defina um nome para o agente, selecione a opção Independente e associe-a ao Controlador de Domínio apropriado criado na tarefa 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

Clique no botão Salvar.

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 Create Agent			

Salve a configuração

O 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 Create Agent			
10.62.113.247	LAB-Agent (standalone)	Not Applicable	

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 para **Sistema > Usuários** e clique em **Criar usuário**. Preencha os detalhes do usuário de acordo com os requisitos da tarefa.

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

Criar usuário

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

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

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.

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

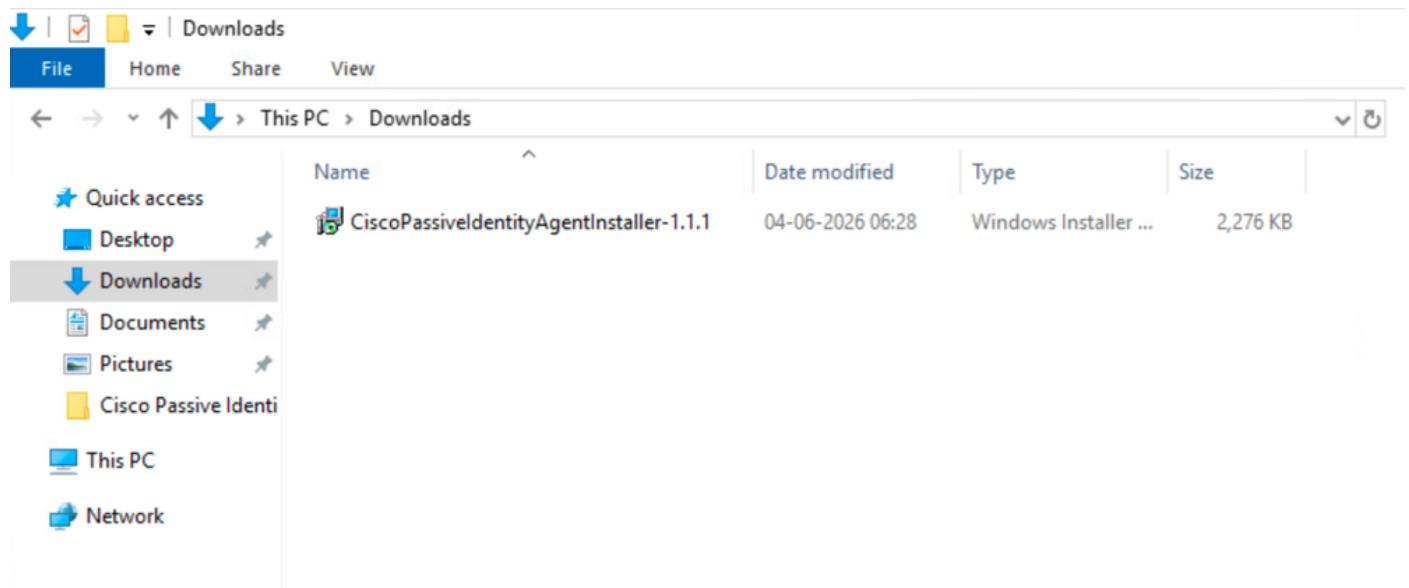
Release Notes for Passive Identity Agt

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	  

baixar o software

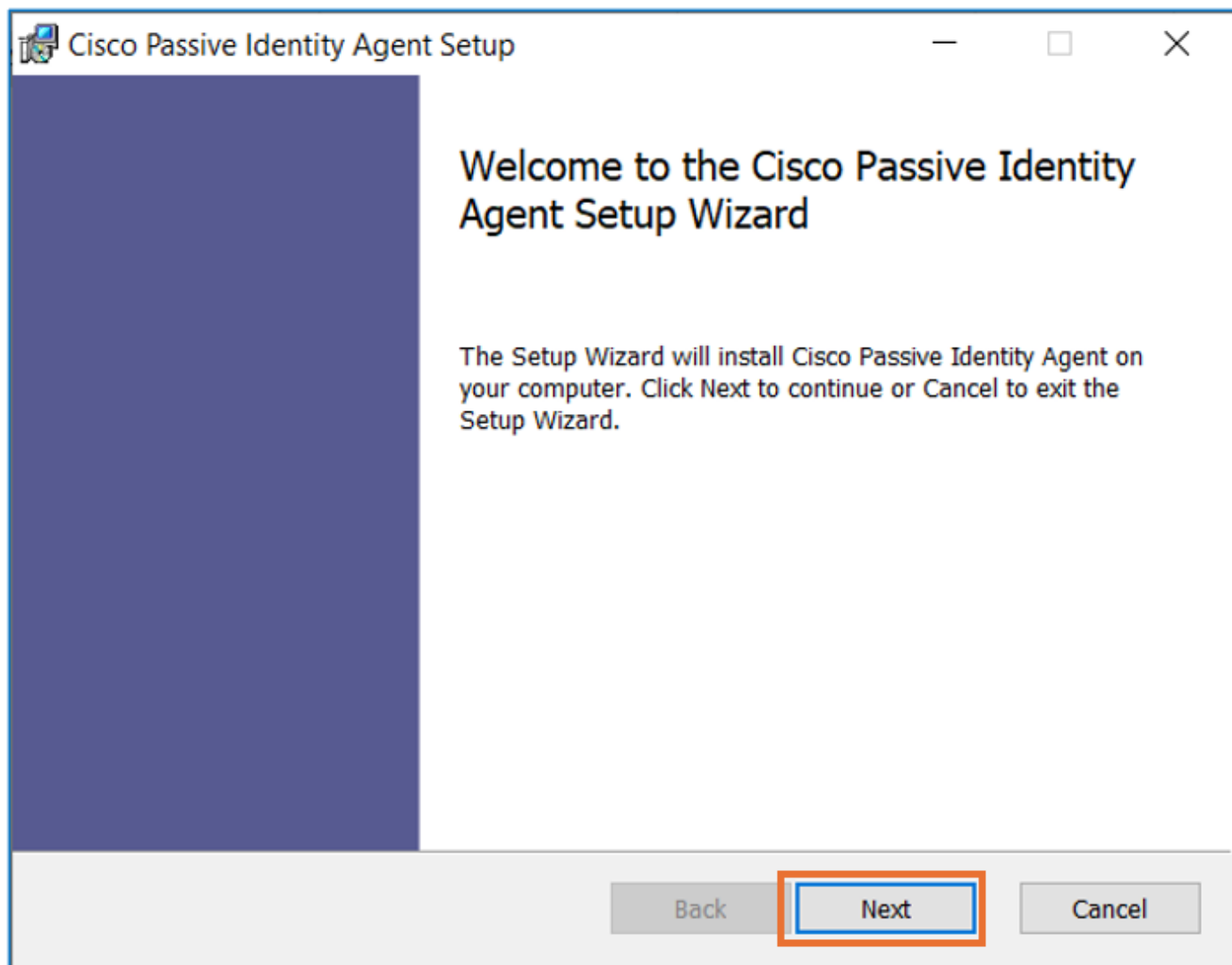
Após fazer o download do agente, inicie o processo de instalação no controlador de domínio.



agente

1

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.

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**

configurar o agente.

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

 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

teste

Clique no botão OK para concluir a configuração do 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

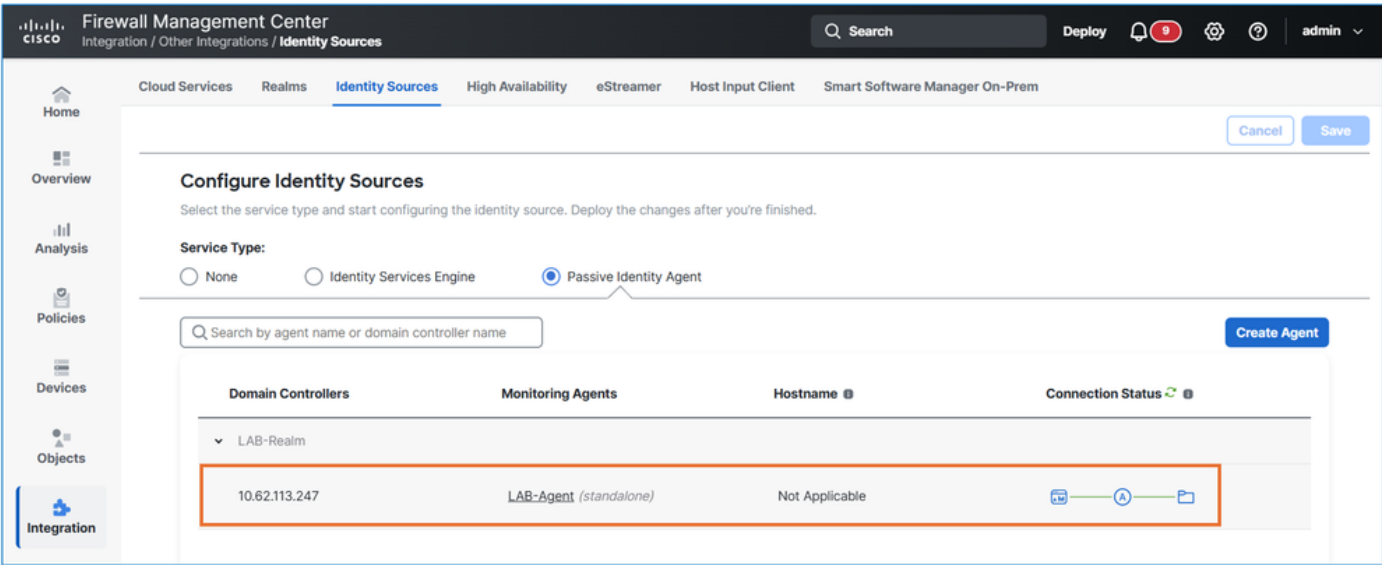
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

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.



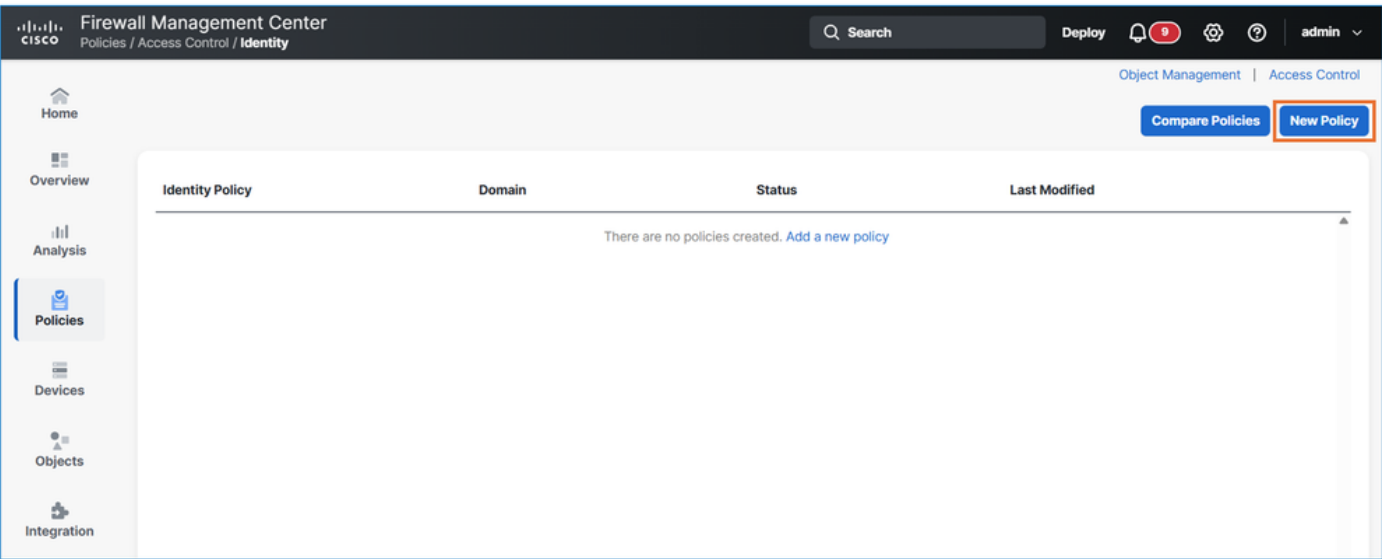
verificar a comunicação do fmc

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.

New Identity policy

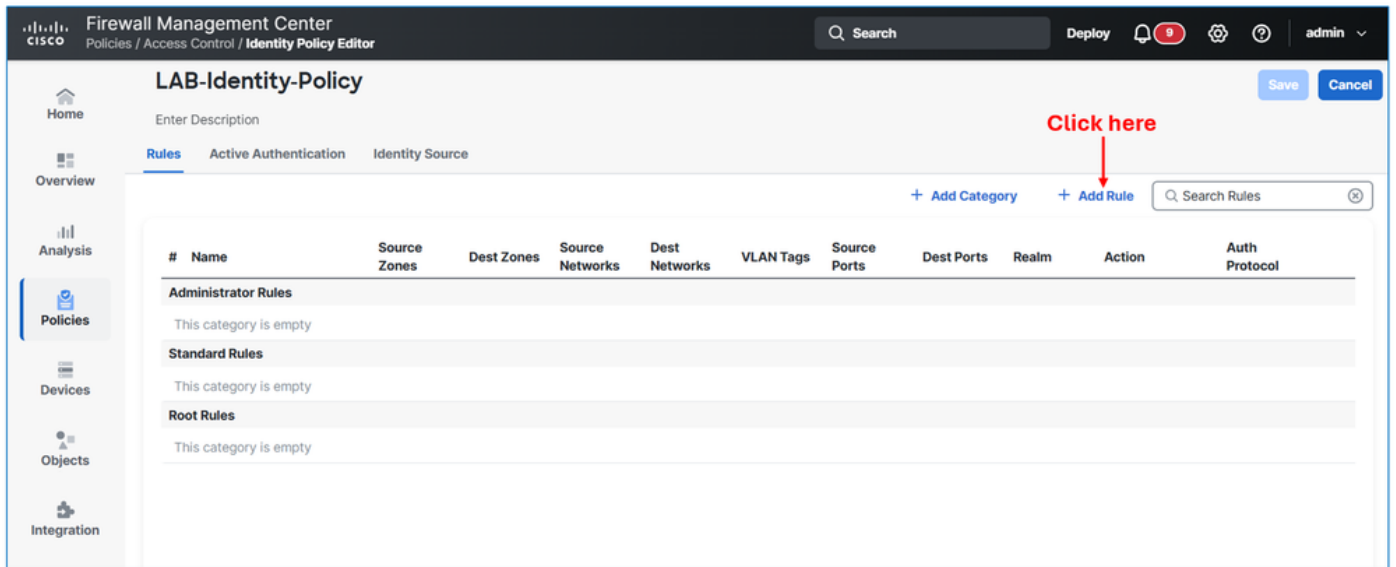
Name

Description

CancelSave

nova política

Clique no botão Adicionar regra.



criar regra

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

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

1

Realm & Settings

Authentication Realm *

LAB-Realm (AD)

2

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

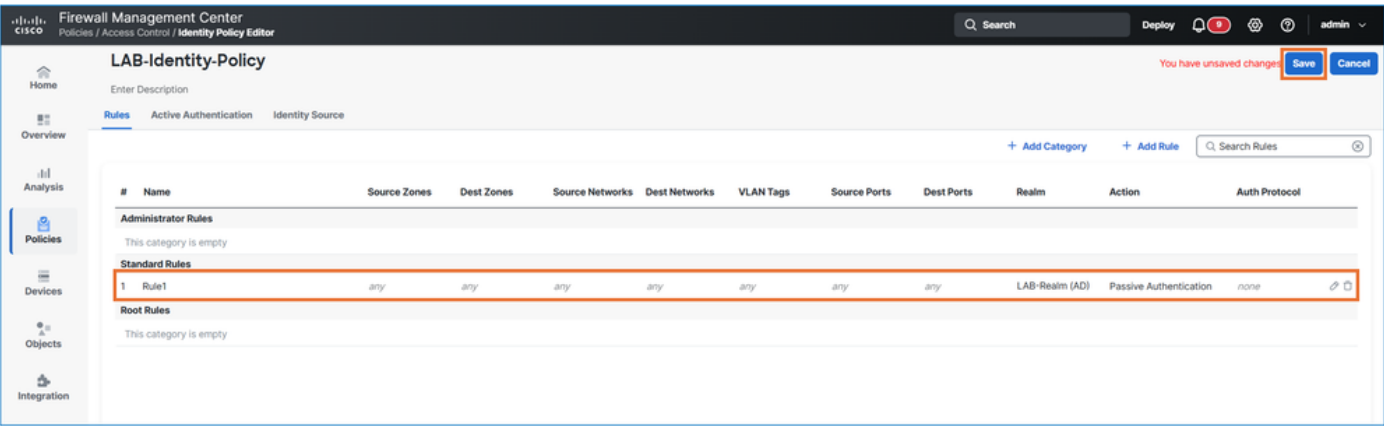
3

Cancel

Add

Configuração de território

Clique no botão Salvar.



salvar a configuração

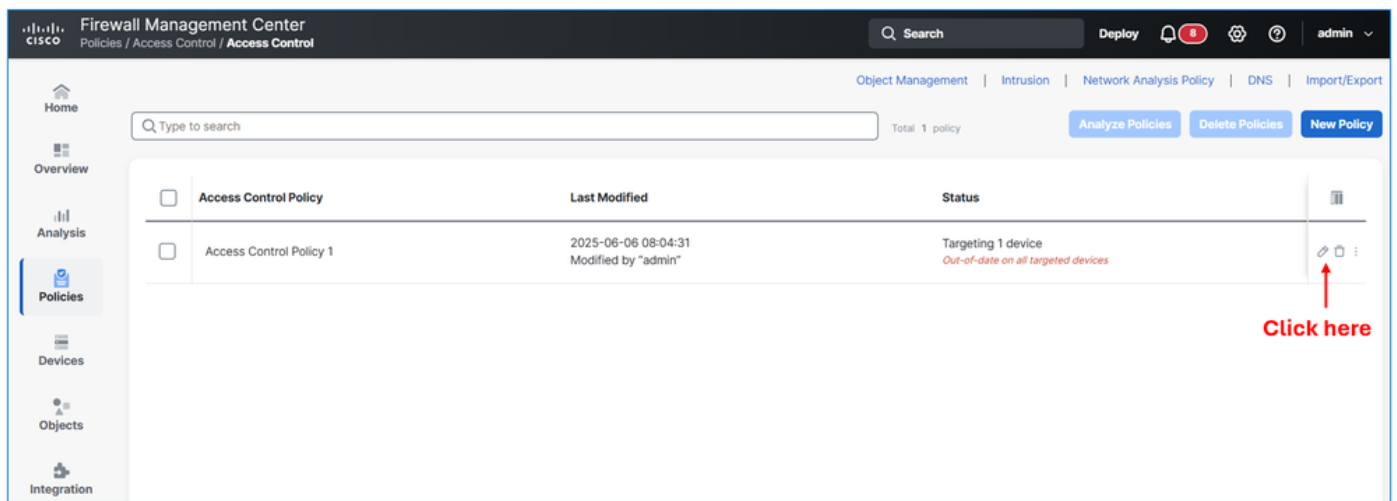
Configurar Políticas de Controle de Acesso

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

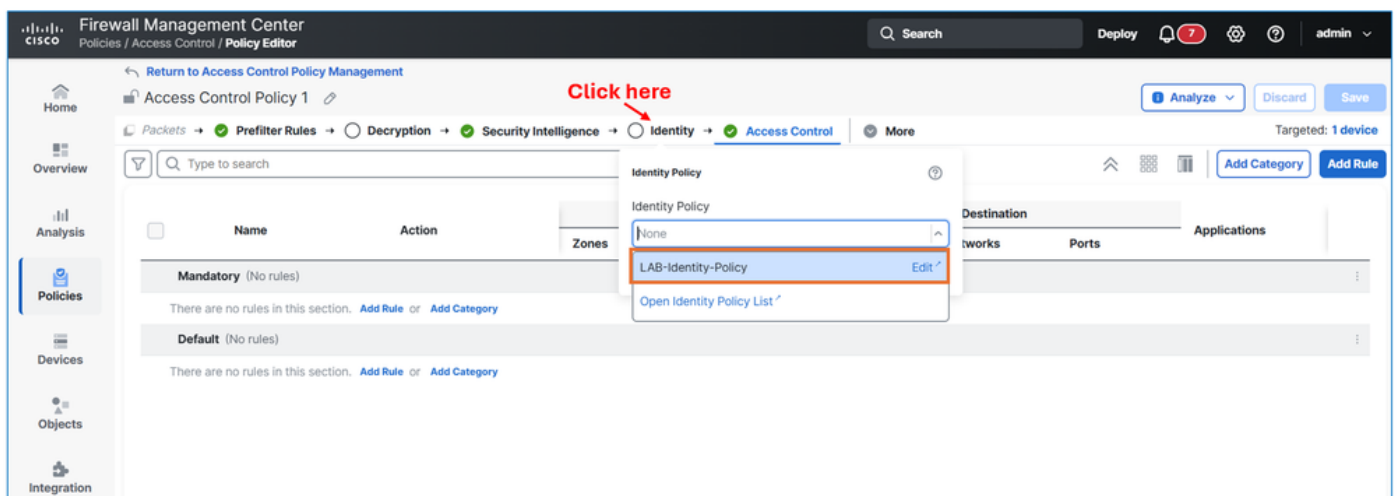
Etapa 1. Vincular a política de identidade à política de controle de acesso

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



Editar política

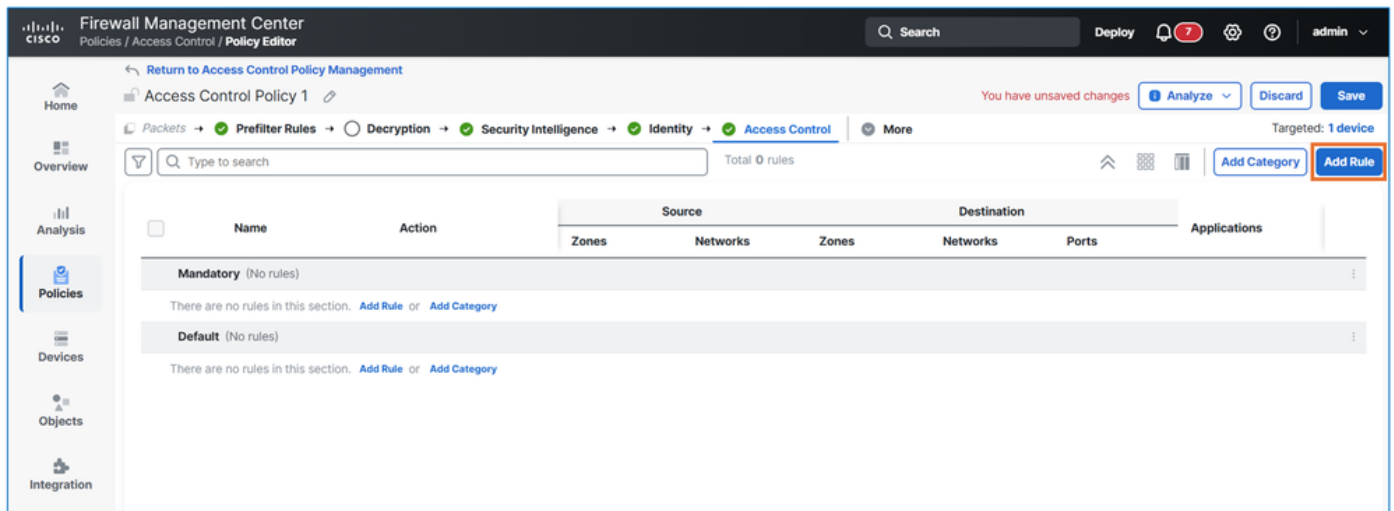
Navegue até a **Seção Identidade** e vincule a Política de identidade criada na tarefa anterior.



adicionar política de identidade

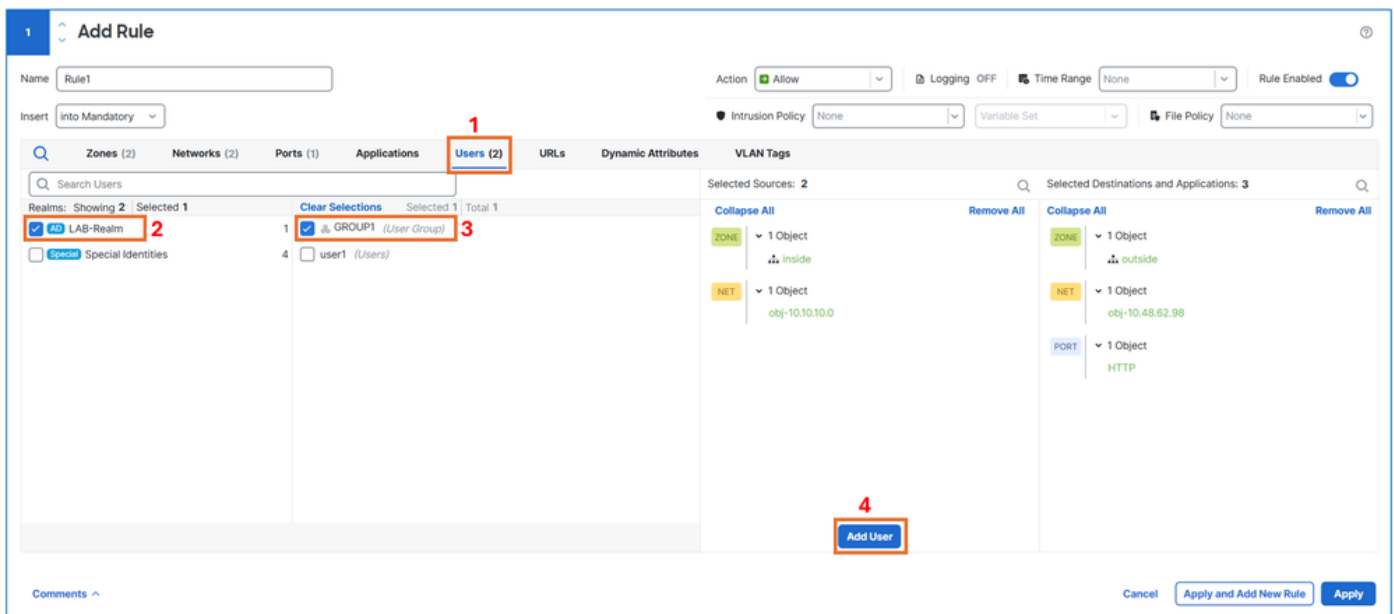
Clique no botão **Aplicar**

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 selecionando Registrar no final da conexão.

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

- ☒ AD LAB-Realm
- ☐ Special Special Identities

Users: Total 1

- 1 GROUP1 (User Group)
- 4 user1 (Users)

Selected Sources: 3

Collapse All

- 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

Habilita o registro em log

Etapa 3. Ative o registro para a ação padrão.

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

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

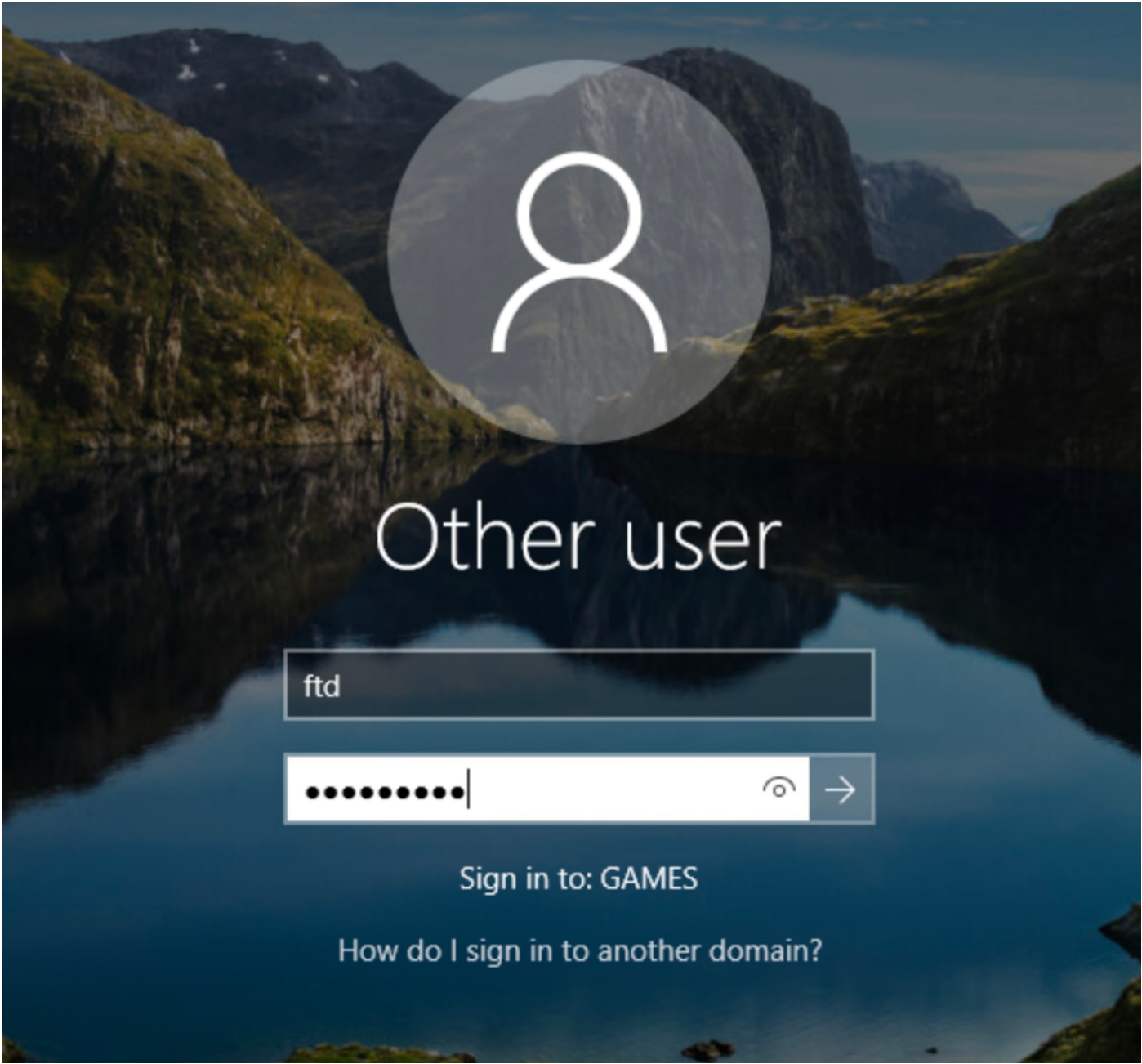
Habilita o registro em log

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 >active 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.

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		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		

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.

Task Manager

File Options View

Processes Performance Users Details Services

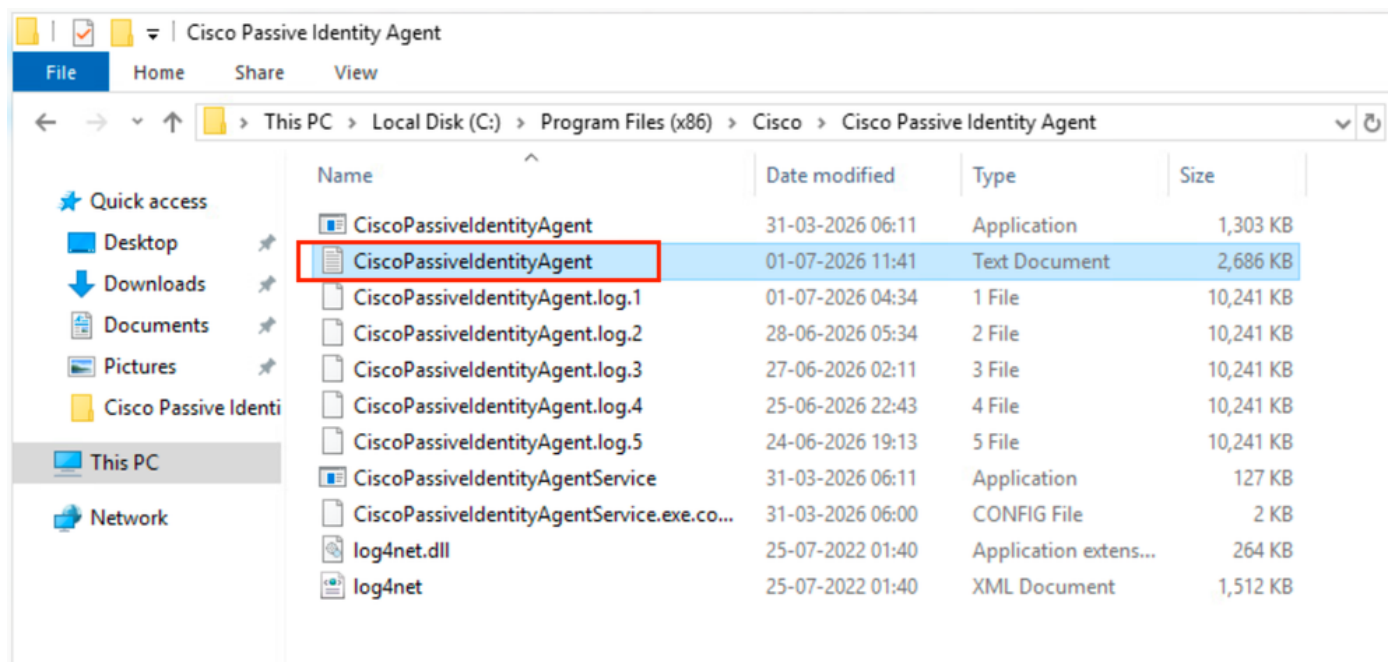
Name	Status	2% CPU	27% Memory
> Task Manager		0%	24.4 MB
> Windows Explorer		0%	37.3 MB
> Server Manager		0%	34.1 MB
Background processes (32)			
> Distributed File System Replicati...		0%	8.3 MB
▼ CiscoPassiveIdentityAgentServi...		0%	15.4 MB
Cisco Passive Identity Agent			
> Microsoft.ActiveDirectory.WebS...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

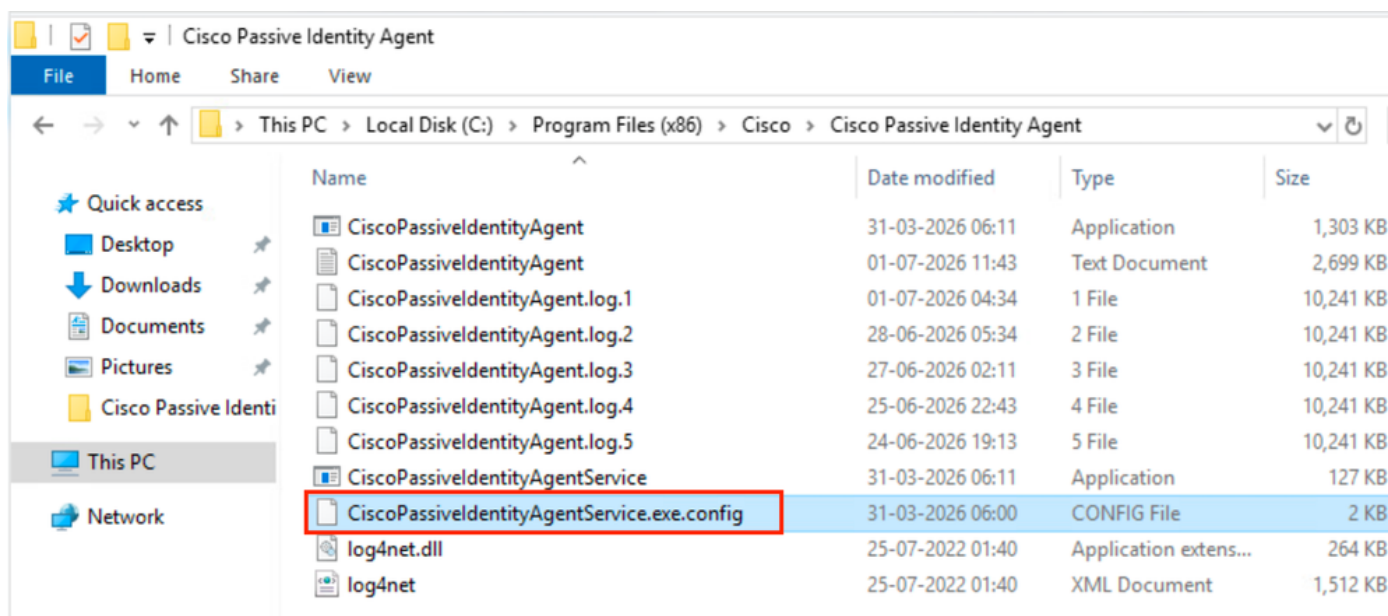
Executando tarefa

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 de INFORMAÇÕES. Para habilitar o log de nível DEBUG, modifique o arquivo de configuração CiscoPassiveIdentityAgentService.exe.e defina o nível de log como ALL ou DEBUG.



configuração de agente



```
<?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>
</startun>
```

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.