

使用FMC配置被动身份代理

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[配置被动身份代理源](#)

[在安全防火墙管理中心创建被动身份代理用户](#)

[安装和配置被动Identity Agent软件](#)

[配置身份策略](#)

[配置访问控制策略](#)

[确认](#)

[故障排除](#)

[检查代理日志](#)

[FMC日志](#)

简介

本文档介绍如何配置向FMC发送会话数据的被动身份代理源

先决条件

要求

- 运行版本7.6+的思科安全防火墙管理中心
- 运行版本7.6+的Cisco安全防火墙
- 在Windows Active Directory服务器上，服务器必须运行Windows Server 2008或更高版本。
- 必须在安全防火墙威胁防御设备上启用Snort 3。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全防火墙管理中心7.6.5
- 思科安全防火墙7.6.5
- Windows Server 2022上运行的Microsoft Active Directory。

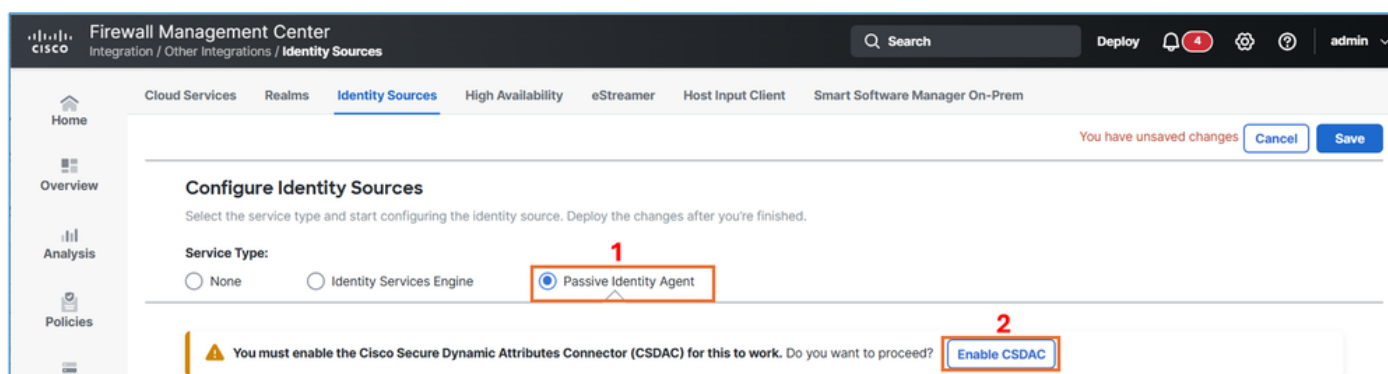
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

在配置代理之前，请完成AD和FMC集成。

配置被动身份代理源

在FMC UI中，导航到集成>其他集成>身份源，单击被动身份代理。 如果Cisco Secure Dynamic Attributes Connector尚未启用，则通过点击Enable CSDAC来提示您执行此操作。



被动身份代理

单击Enablebutton（启用）按钮启用CSDAC。

Enable Cisco Secure Dynamic Attributes Connector?



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

Cancel

Enable

启用CSDAC

此步骤大约需要10分钟。正确启用CSDAC后，点击Donebutton以继续。

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

已启用CSDAC

单击Create Agent按钮。

Firewall Management Center

Integration / Other Integrations / Identity Sources

Search

Deploy

10

Global | admin

Home

Overview

Analysis

Policies

Devices

Objects

Integration

Cloud Services

Realms

Identity Sources

High Availability

eStreamer

Host Input Client

Smart Software Manager On-Prem

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

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 / Standalone 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

创建代理

定义代理的名称，选择Standaloneoption，并将其与上一个任务中创建的相应Domain Controller关联。

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:

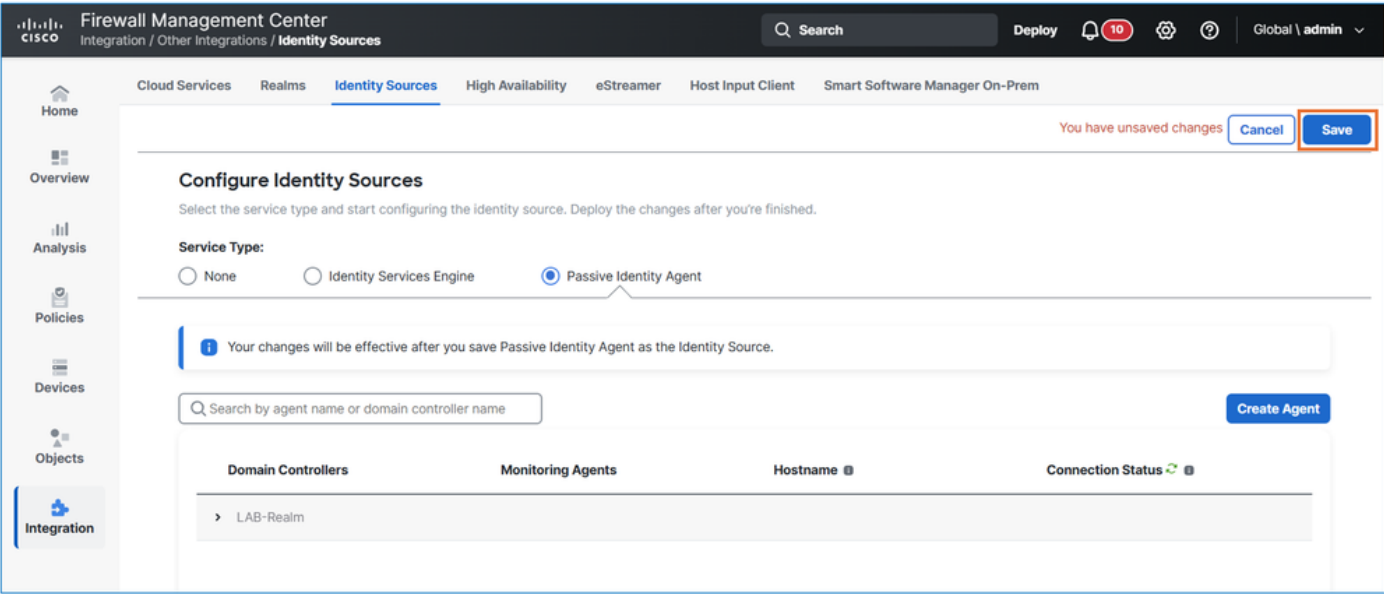
This agent will be created and assigned to the selected domain controller. Install it on the domain controller (or on its member machine) to start the tracking.

Cancel

Save

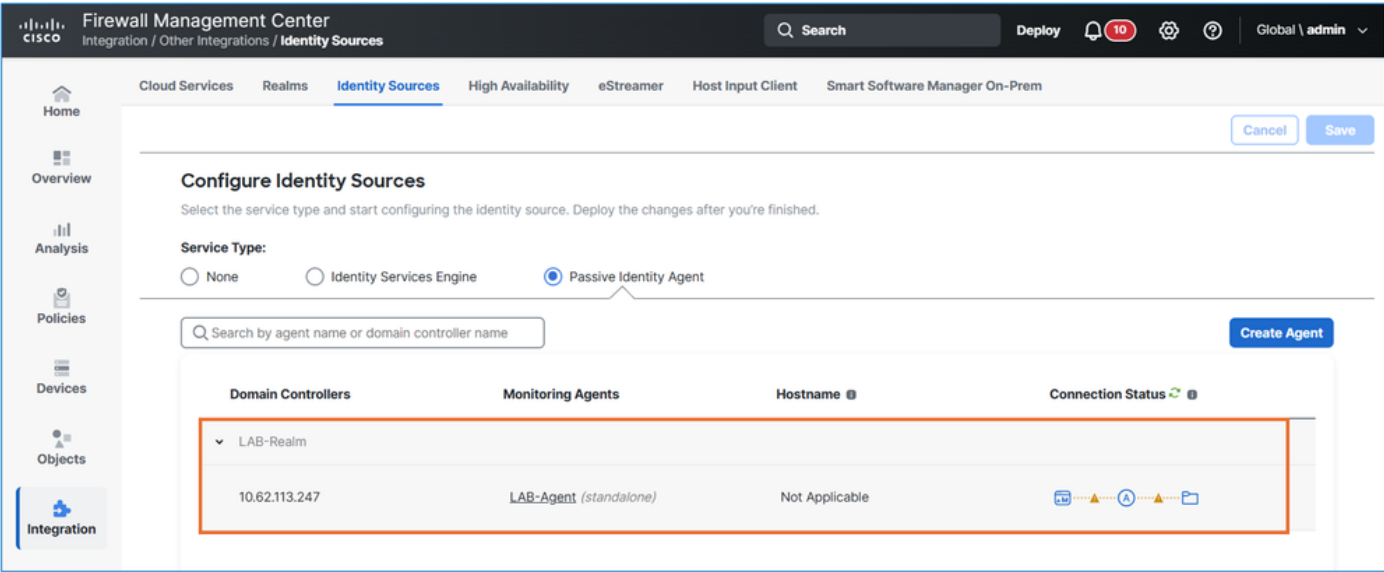
配置代理

单击Savebutton。



保存配置

结果。



检验状态

 注意：被动身份代理使用线路指示状态，琥珀色表示该代理从未成功与安全防火墙管理中心通信。新创建的代理线路呈琥珀色，在配置完成前保持琥珀色。

在安全防火墙管理中心创建被动身份代理用户

创建有足够权限与被动身份代理通信的安全防火墙管理中心用户。此用户执行其他任务的权限有限

；用户应仅启用与被动身份代理的通信。

在FMC UI中，导航到System > Users，然后单击Create User。根据任务要求填写用户详细信息。

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

☐ Force Password Reset on Login

Options

☐ Check Password Strength

☐ Exempt from Browser Session Timeout

创建用户

仅分配被动身份用户角色。单击Savebutton。

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

选择被动身份用户

安装和配置被动Identity Agent软件

在指定域控制器上安装并配置被动身份代理软件。

从software.cisco.com下载被动身份代理。

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

下载软件

下载代理后，在域控制器上开始安装过程。

Downloads

FileHomeShareView

This PC > Downloads

Quick access

Desktop

Downloads

Documents

Pictures

Cisco Passive Identi

This PC

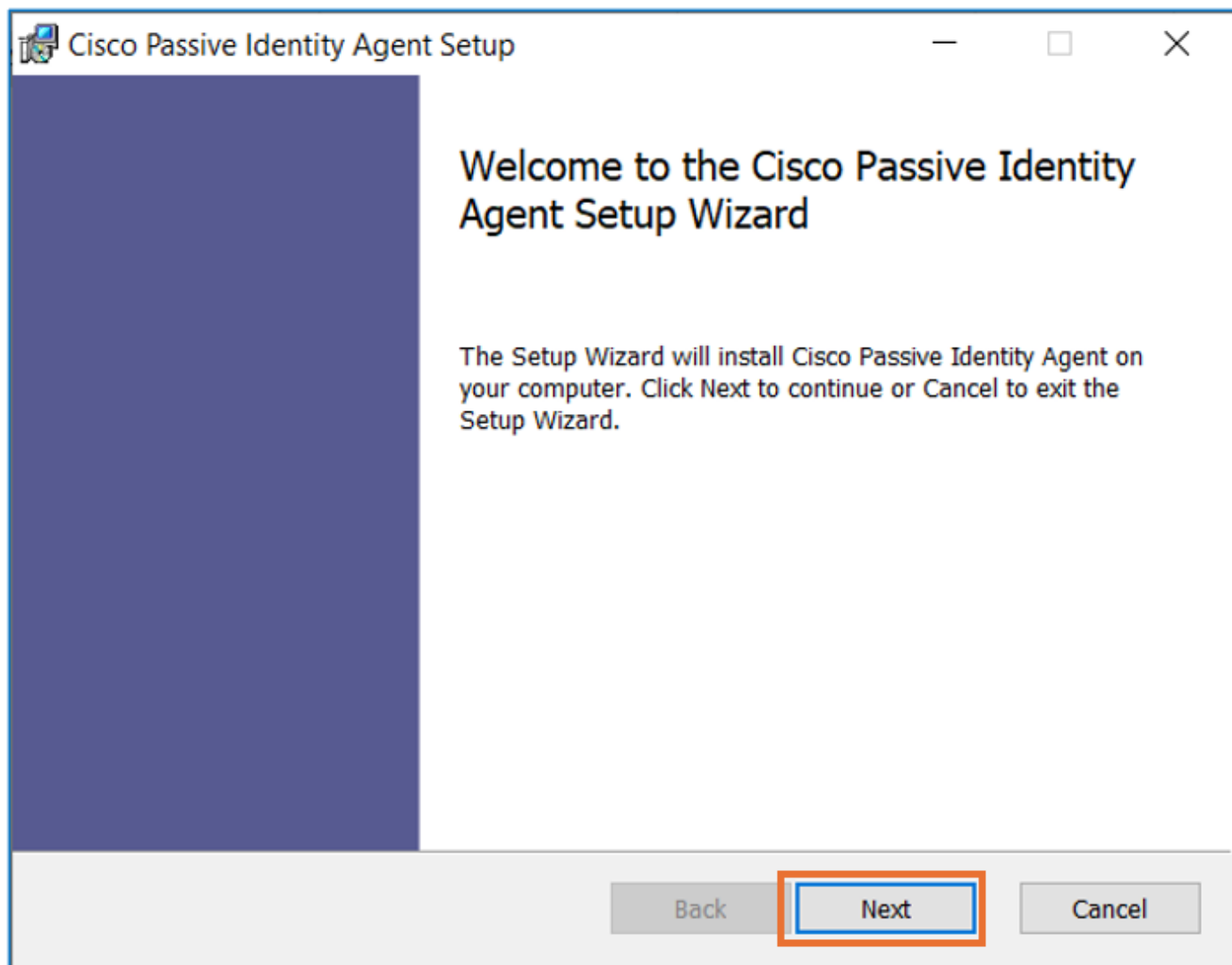
Network

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

代理

]

请参阅提供的安装说明以完成设置。



Install (安装)

安装完成后，打开Passive Identity Agent软件，然后按照任务要求中的指定输入所需信息。单击Test按钮验证与FMC的连接。

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

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

Click here to test the connectivity

I have Secondary FMC ▾

配置代理。

成功测试连接后，单击Savebutton。

 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

测试

单击OK按钮完成代理配置。

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

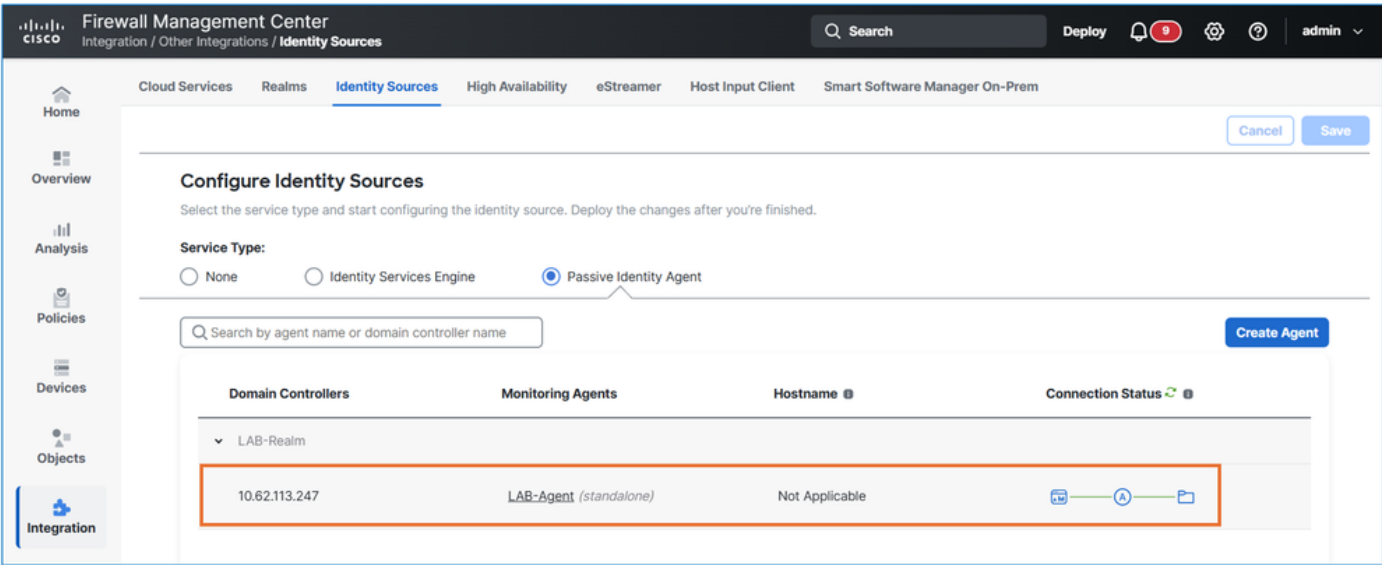
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

代理正在运行

在FMC UI中，导航到集成>其他集成>身份源>被动身份代理。确认被动身份代理显示绿色状态。



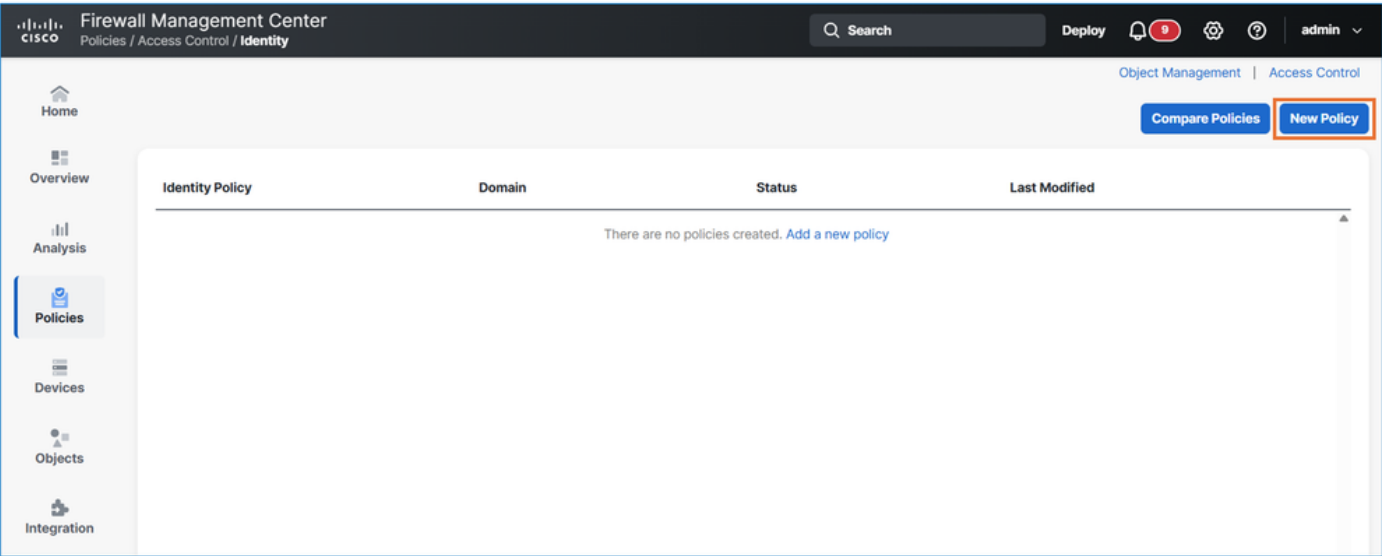
验证来自fmc的通信

配置身份策略

根据提供的表创建身份策略。

策略名称	规则名称	身份验证领域	剩余设置
实验室身份策略	规则1	实验室领域	保留为默认值

在FMC UI中，导航到Policies > Access Control > Identity。单击New Policy按钮。



新策略

根据任务要求输入策略名称。

New Identity policy

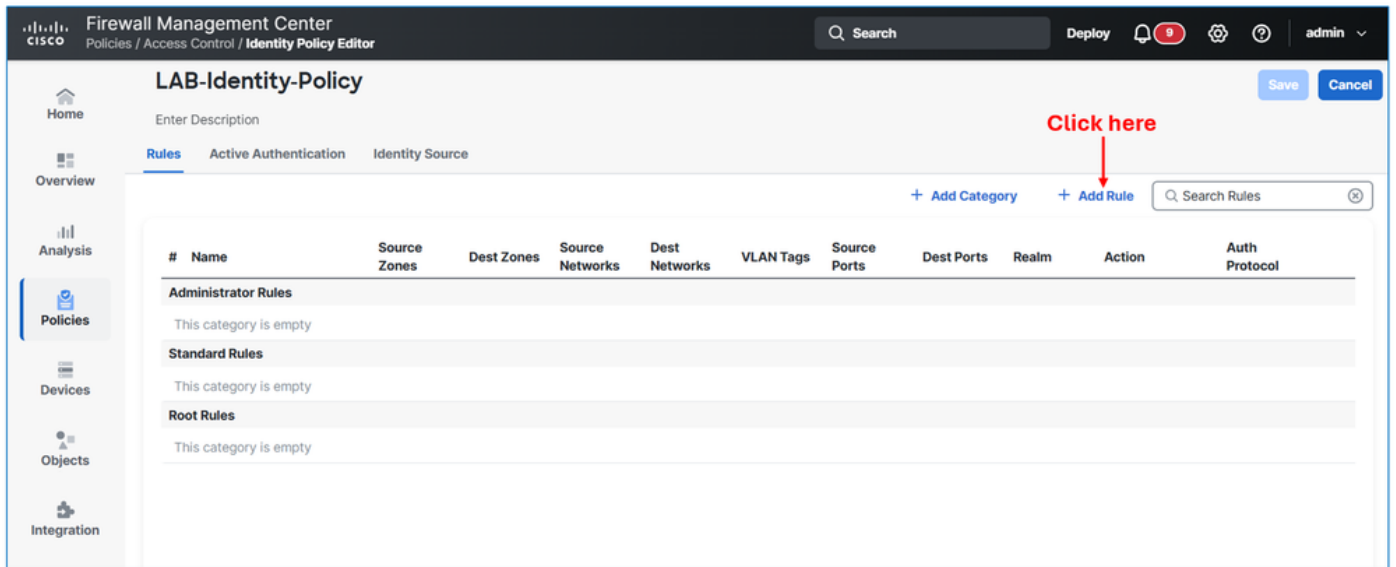
Name

Description

CancelSave

新策略

单击Add Rule按钮。



创建规则

导航到Realm & Settingstab，然后根据任务要求选择Authentication Realmbed。最后，单击Addbutton。

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 *

2

LAB-Realm (AD)

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

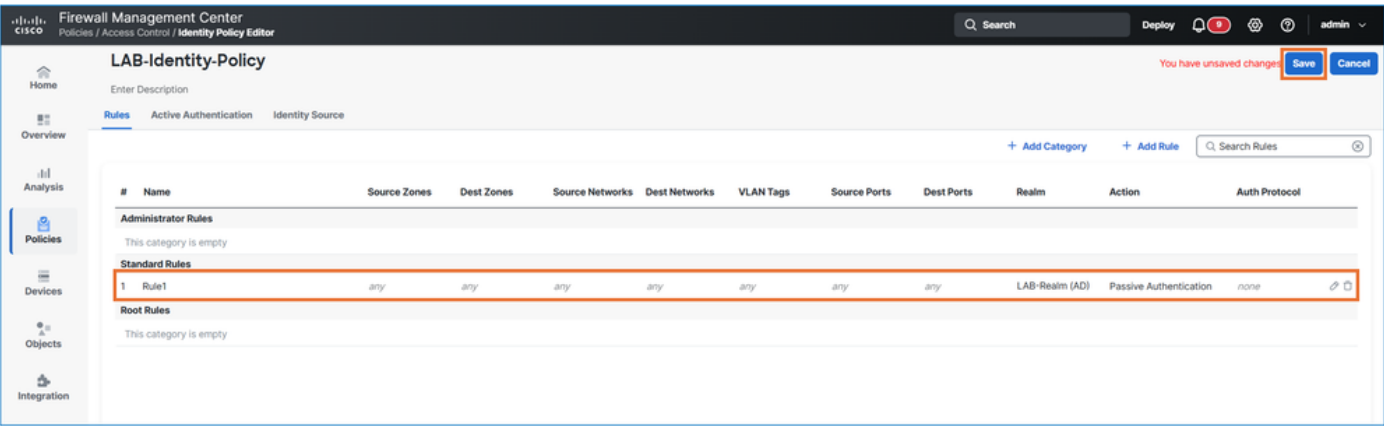
3

Add

Cancel

领域设置

单击Savebutton。



保存配置

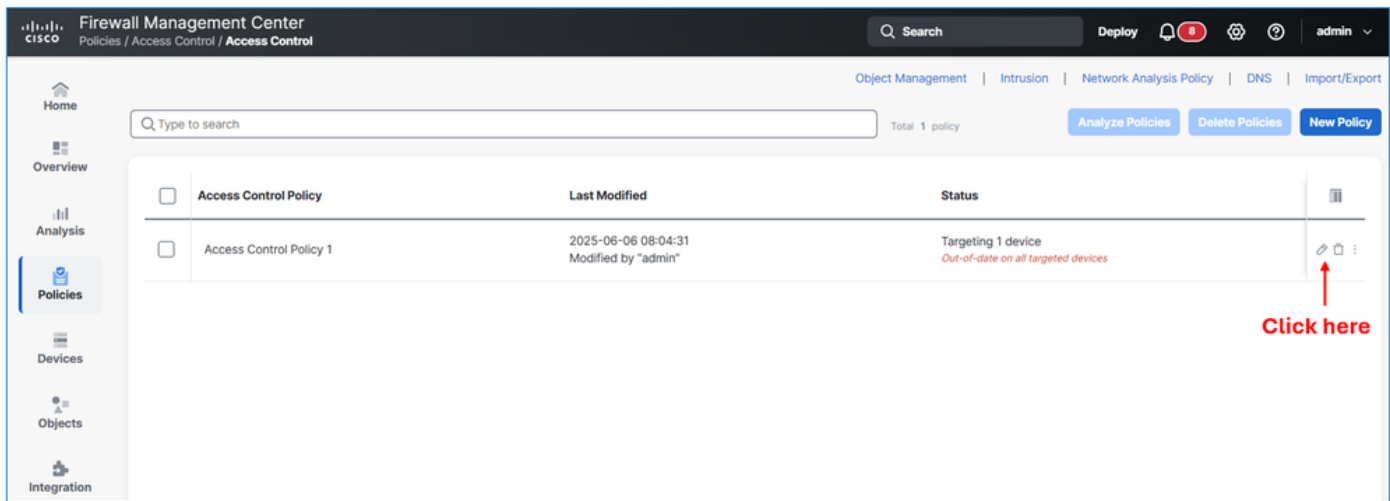
配置访问控制策略

将身份策略链接到访问控制策略，并使用以下属性创建访问策略规则：

属性名称	价值
规则名称	规则1
操作	允许
源区域	内部
目标区域	外部
源网络	10.10.10.0/24
目标网络	10.48.62.98/32
服务	目的端口TCP 80(HTTP)
用户	实验室领域/组1
日志记录	在连接结束时

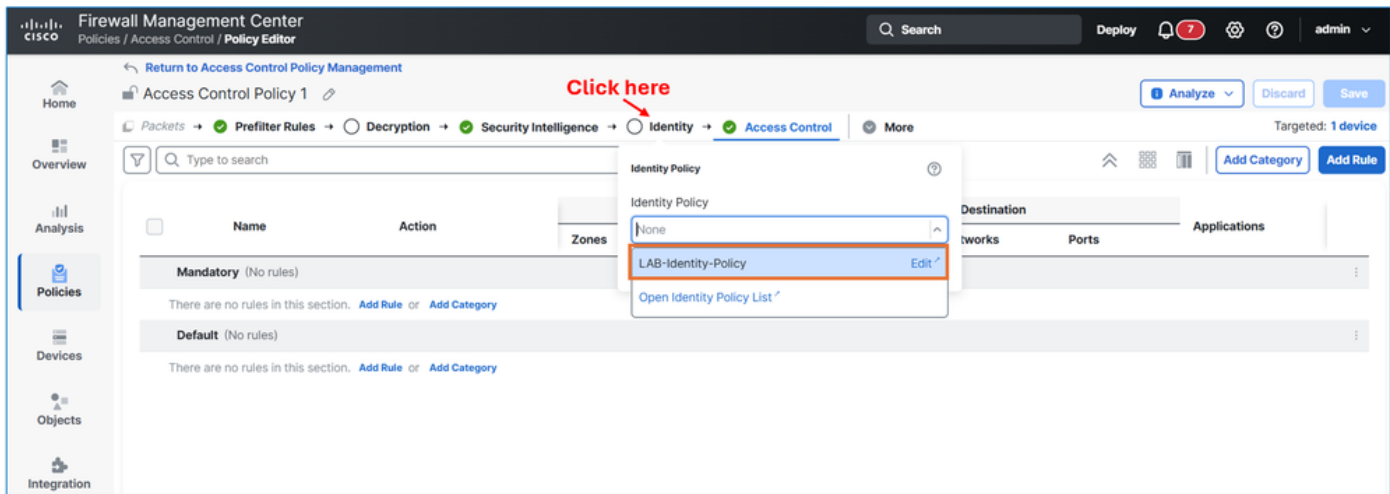
步骤1.将身份策略链接到访问控制策略

在FMC UI中，导航至策略>访问控制>访问控制。点击策略的“编辑”按钮。



编辑策略

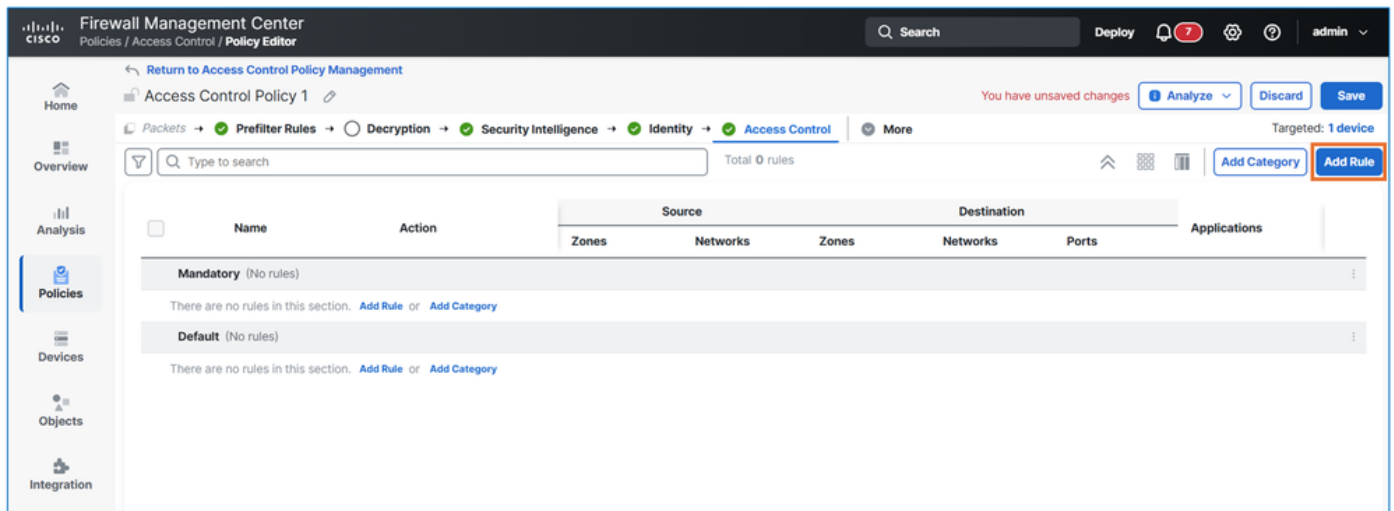
导航到Identitysection并链接在上一个任务中创建的身份策略。



添加身份策略

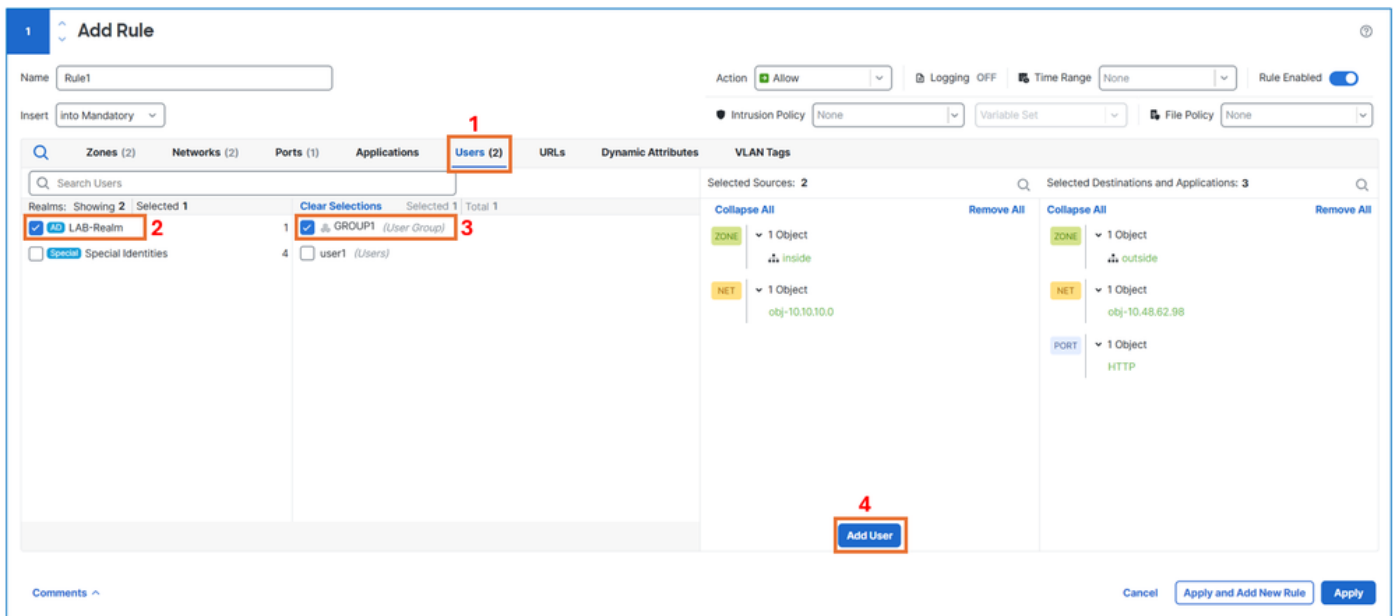
单击Applybutton

步骤2.创建访问控制规则。



创建ACP

根据任务要求输入详细信息，最重要的是，在Userstab下，从LAB-Realm添加GROUP1。



在规则中添加用户

通过选择连接结束时的Log启用规则的日志记录。

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

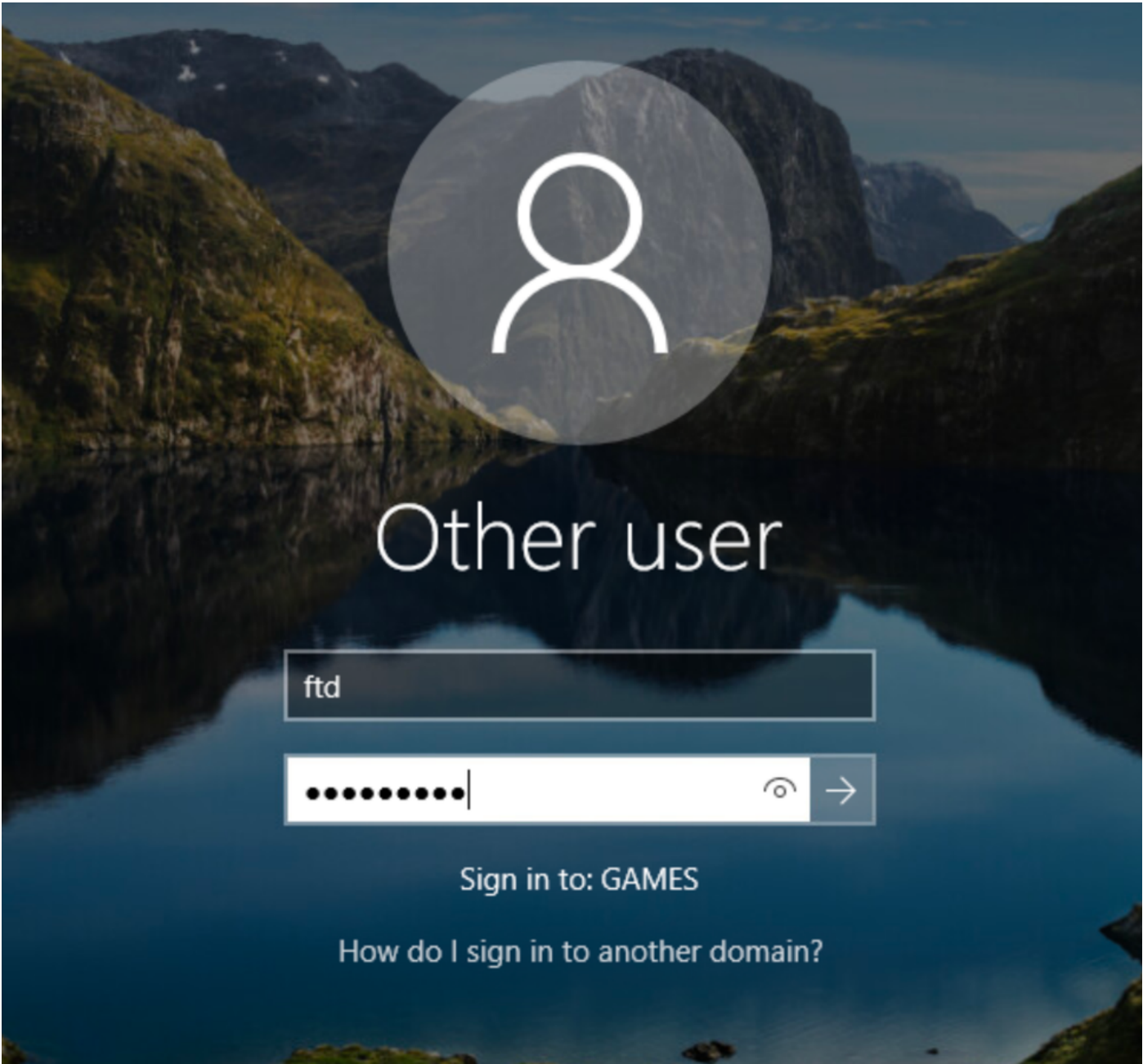
启用日志

保存并部署FTD上的配置。

确认

通过确认仅允许流量用于ftd来验证被动身份操作。

从用户计算机登录到域用户。



用户登录

用户成功登录后，从FMC在Analysis > user >active session下验证，以查看活动用户详细信息。

Select...

Showing all 2 sessions 

☐	Login Time	RealmUsername	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	

活动会话

从连接事件启动某些流量验证后，请参阅连接事件中的用户详细信息。

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

活动会话

故障排除

检查代理日志

在托管代理的Windows计算机上，打开任务管理器，并验证后台进程 CiscoPassiveIdentityAgentServiceis正在运行。

Task Manager

FileOptionsView

ProcessesPerformanceUsersDetailsServices

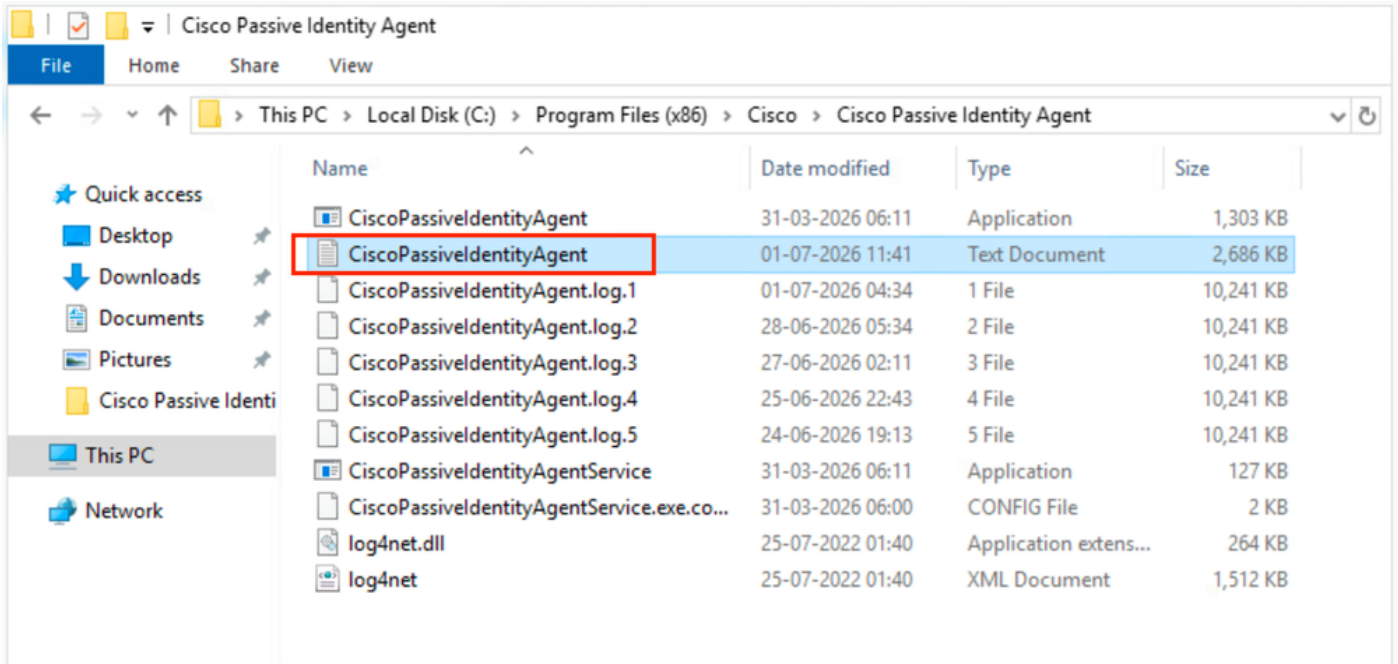
Name	Status	2% CPU	27% Memory
> Task Manager		0%	24.4 MB
> Windows Explorer		0%	37.3 MB
> Server Manager		0%	34.1 MB
Background processes (32)			
> Distributed File System Replicati...		0%	8.3 MB
▼ CiscoPassiveIdentityAgentServi...		0%	15.4 MB
Cisco Passive Identity Agent			
> Microsoft.ActiveDirectory.WebS...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

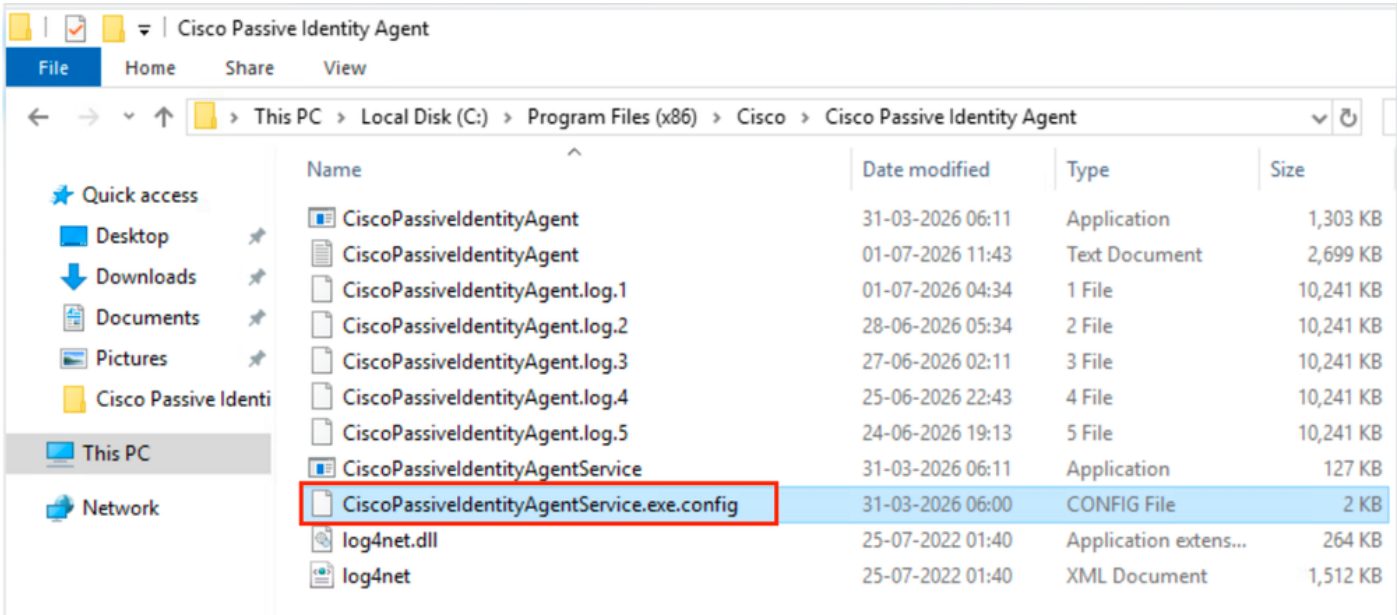
正在运行的任务

代理日志可以在CiscoPassiveIdentityAgent文件中找到，默认位置为："C:\Program文件(x86)\Cisco\Cisco被动身份代理\"。



代理

默认情况下，代理日志设置为INFOlevel。要启用DEBUG级别日志记录，请修改 CiscoPassiveIdentityAgentService.exe.configfile，并将日志记录级别设置为ALL或DEBUG。



代理配置



```
<?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>
```

信息日志

检查代理日志 — 获取代理配置。

INFO Rest客户端，批量事件：[{"domain":"games.cisco.com", "srcIpAddress":"X.X.X.X", "用户": "fdm", "timestamp":"2026-07-01T19

INFO Rest客户端，映射状态：确定

INFO Rest客户端，REST发布成功于userBatch fdm，延迟= 0，当前DC时间(UTC):07/01/2026 19:47:34登录用户

INFO Rest客户端，请求代理配置

FMC日志

运行此命令以查看是否已从代理收到用户到IP的映射。

```
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#
```

fmc输出

如果之前的命令未显示任何映射，请收集这些日志并联系思科TAC。

这是FMC API的相关日志列表。猪尾日志包含所有条目。

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。