使用FMC配置被动身份代理

目录

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。

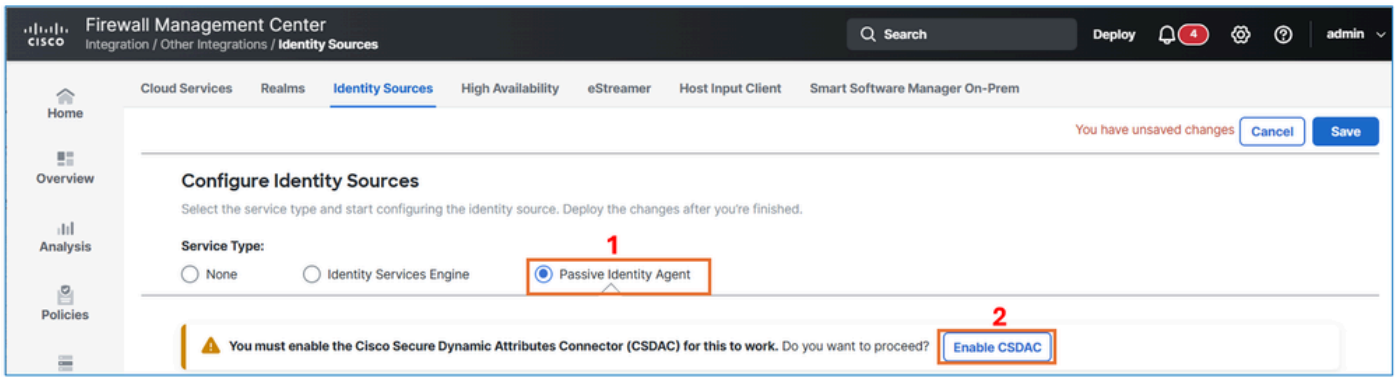
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

在配置代理之前，请完成AD和FMC集成。

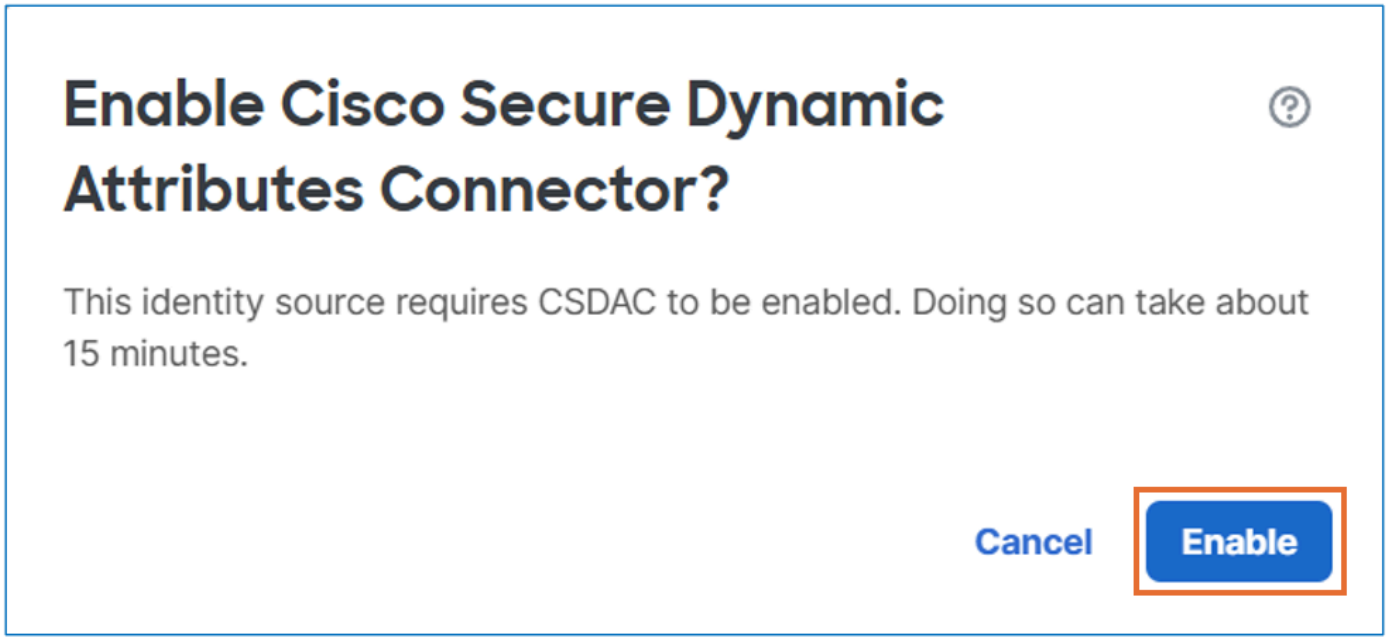
配置被动身份代理源

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。



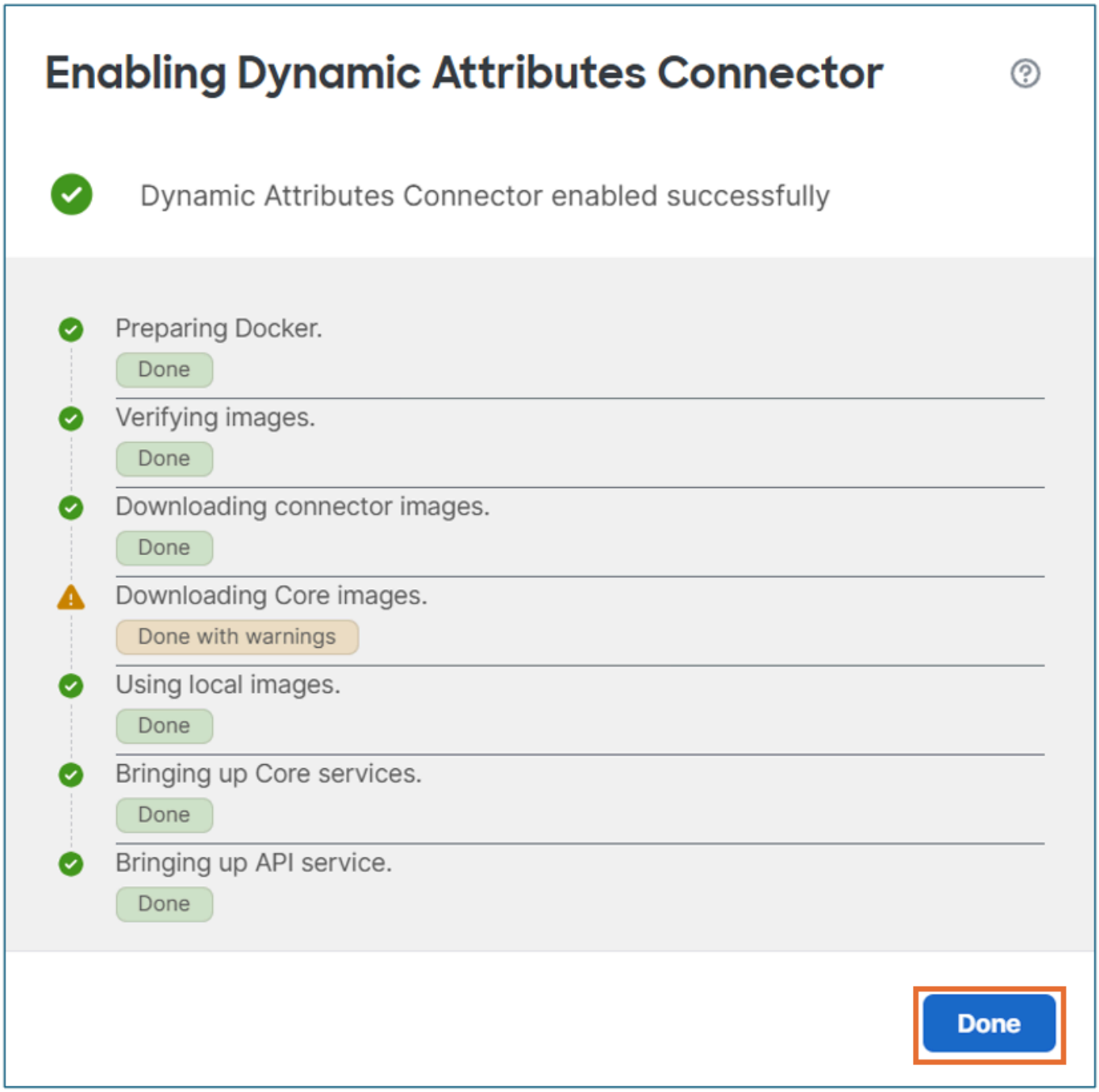
被动身份代理

单击Enablebutton（启用）按钮启用CSDAC。



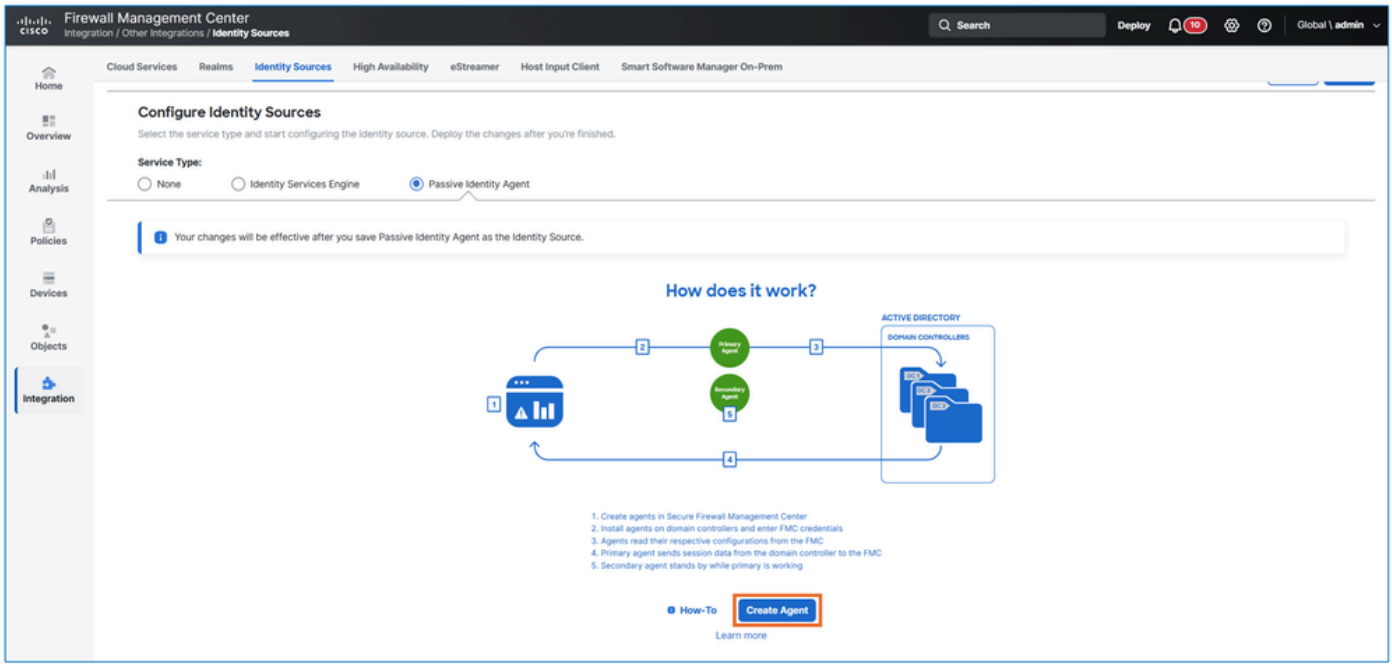
启用CSDAC

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



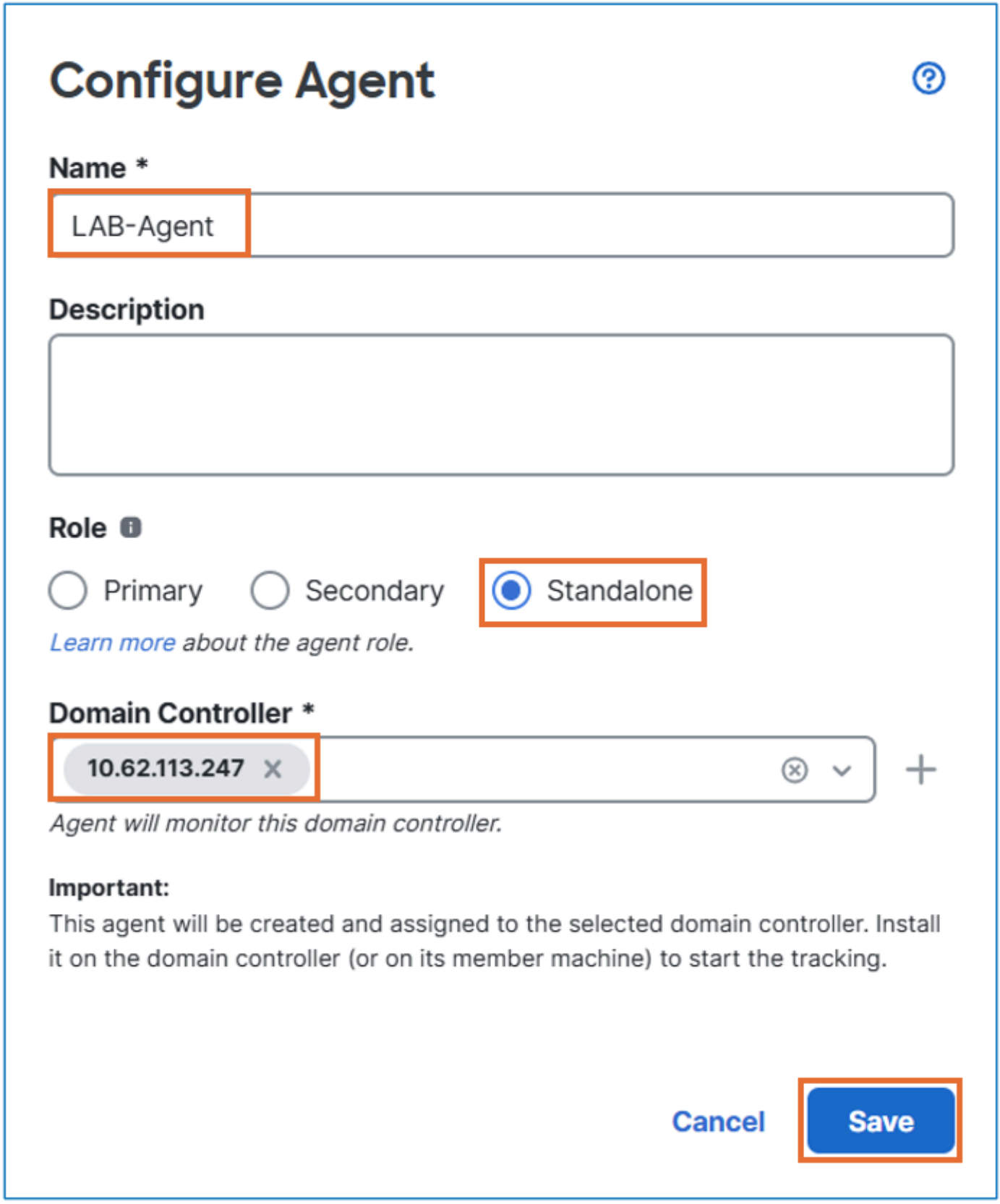
已启用CSDAC

单击Create Agent按钮。



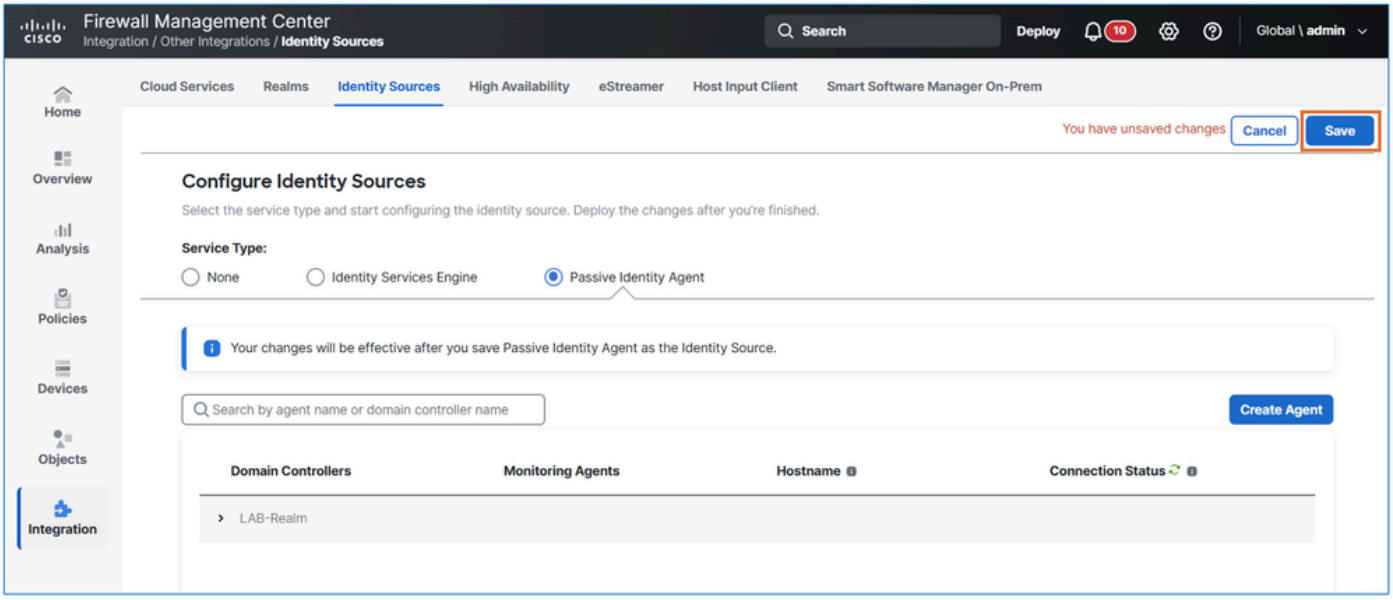
创建代理

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。



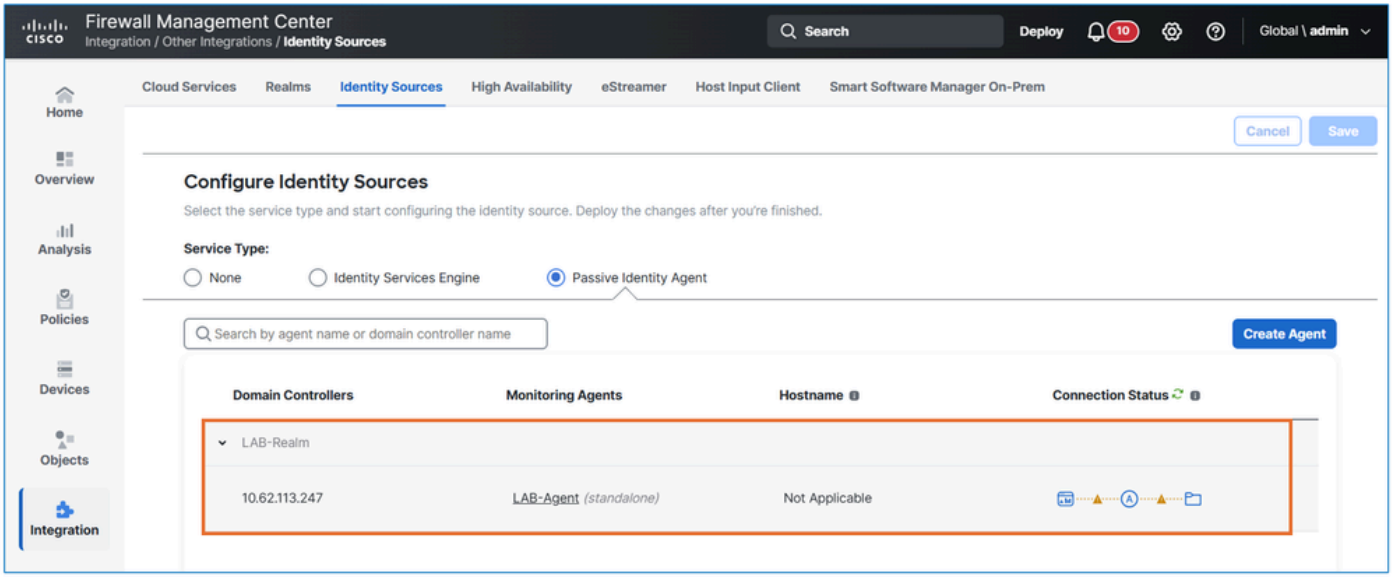
配置代理

单击Savebutton。



保存配置

结果。



检验状态

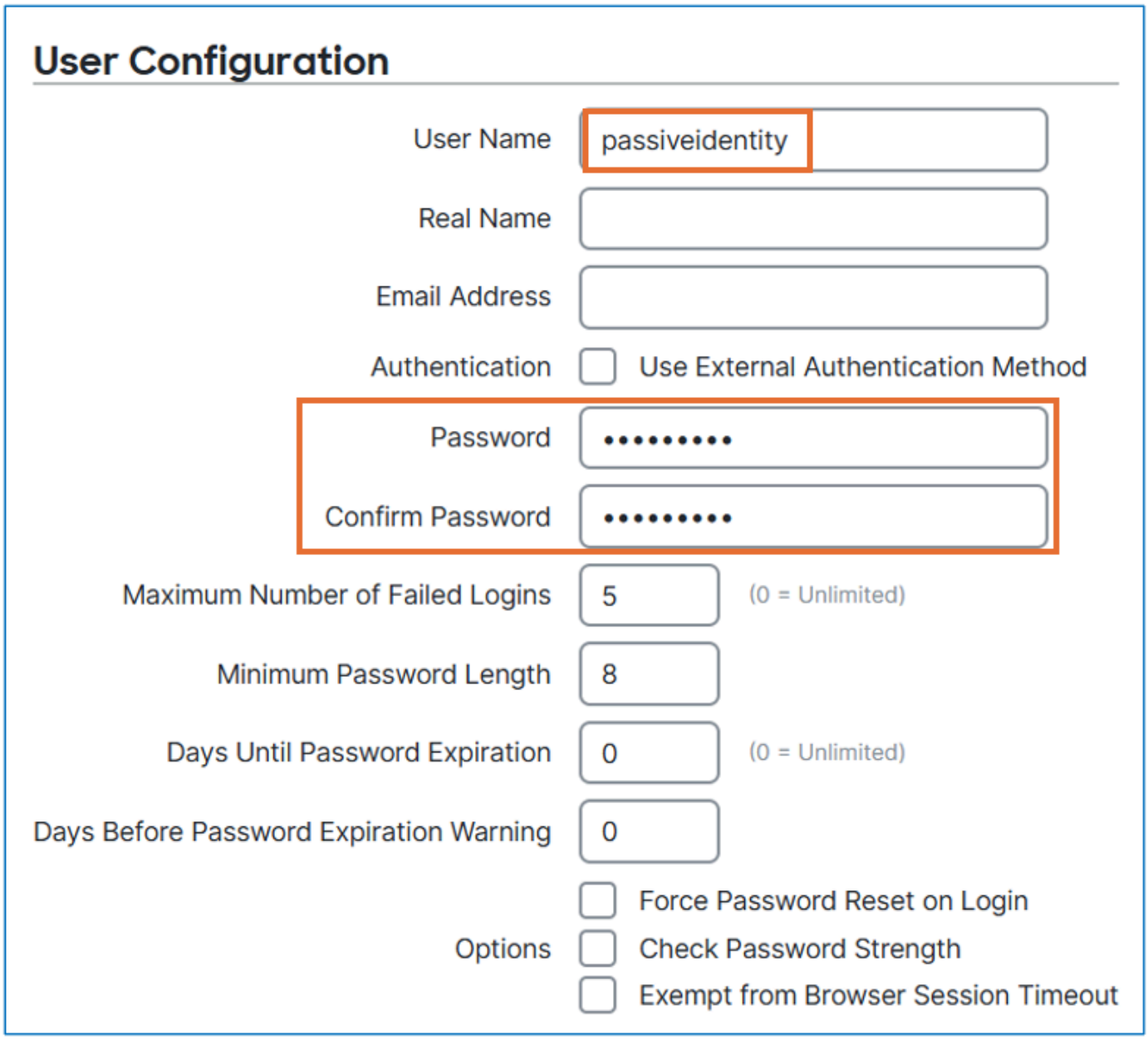
注意：被动身份代理使用线路指示状态，琥珀色表示该代理从未成功与安全防火墙管理中心通信。新创建的代理线路呈琥珀色，在配置完成前保持琥珀色。

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

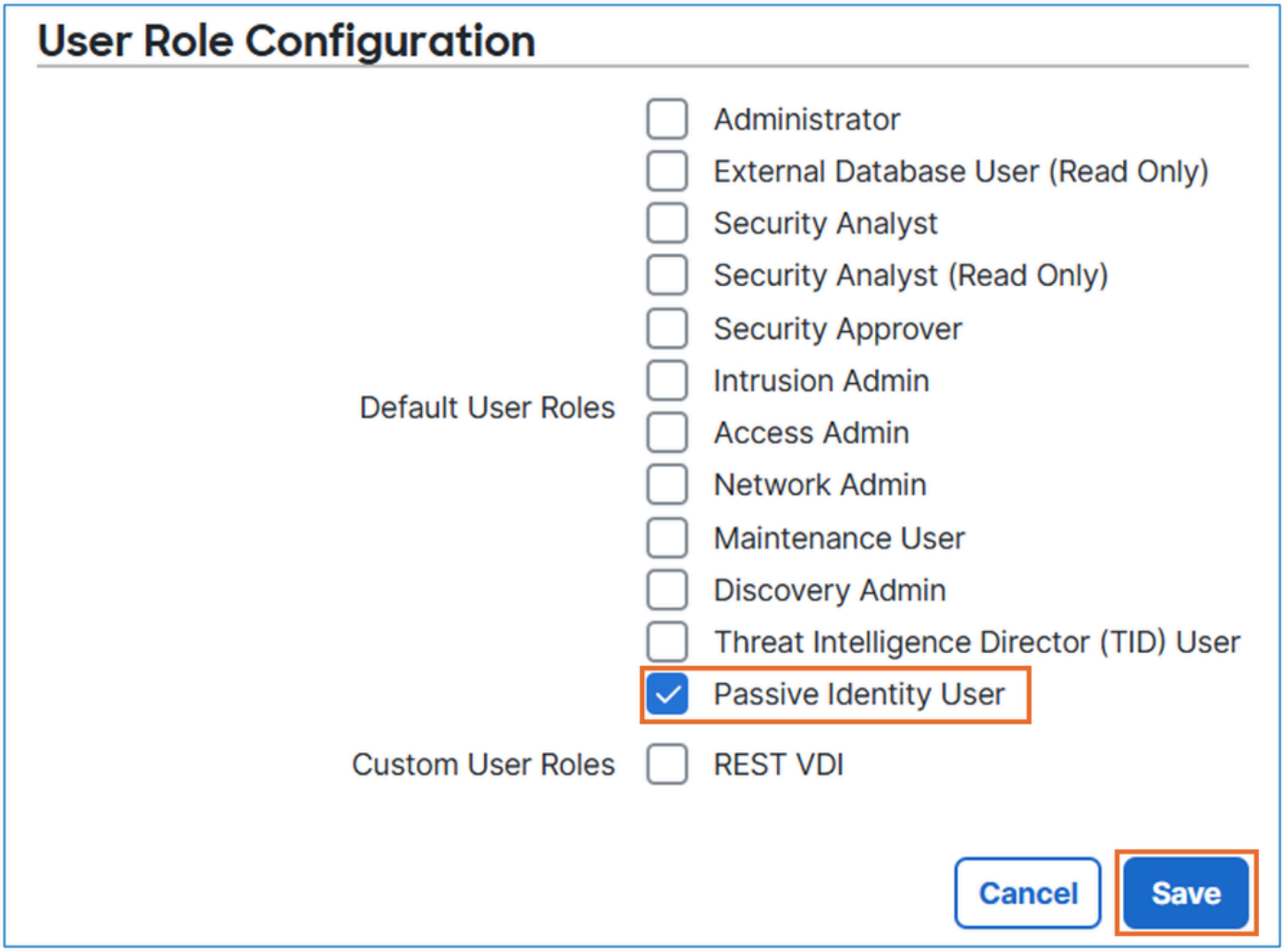
；用户应仅启用与被动身份代理的通信。

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。



创建用户

仅分配被动身份用户角色。单击Savebutton。

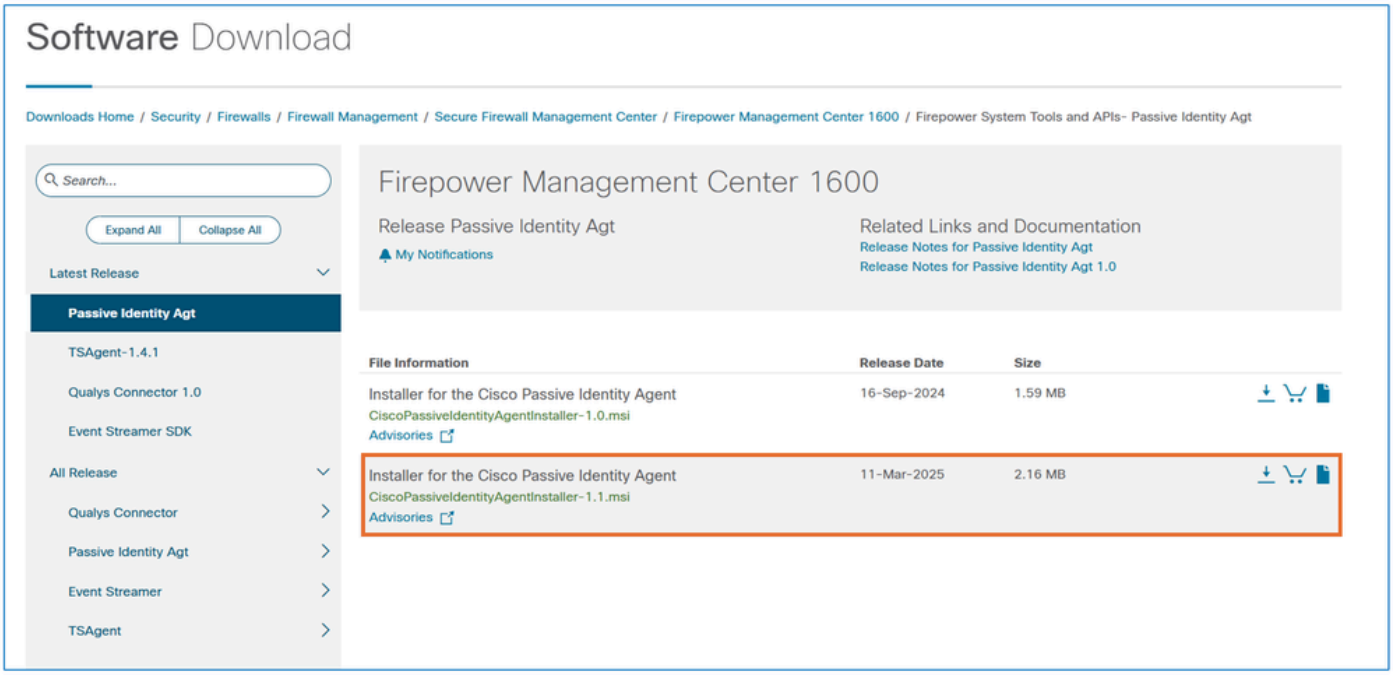


选择被动身份用户

安装和配置被动Identity Agent软件

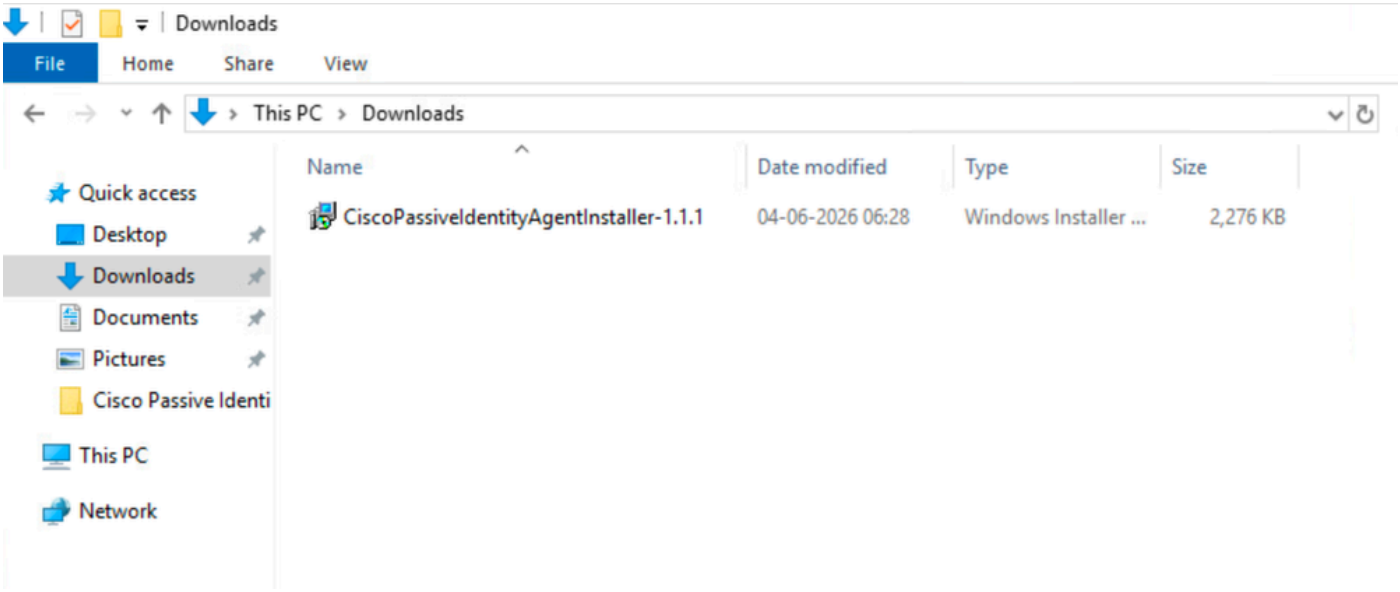
在指定域控制器上安装并配置被动身份代理软件。

从software.cisco.com下载被动身份代理。



下载软件

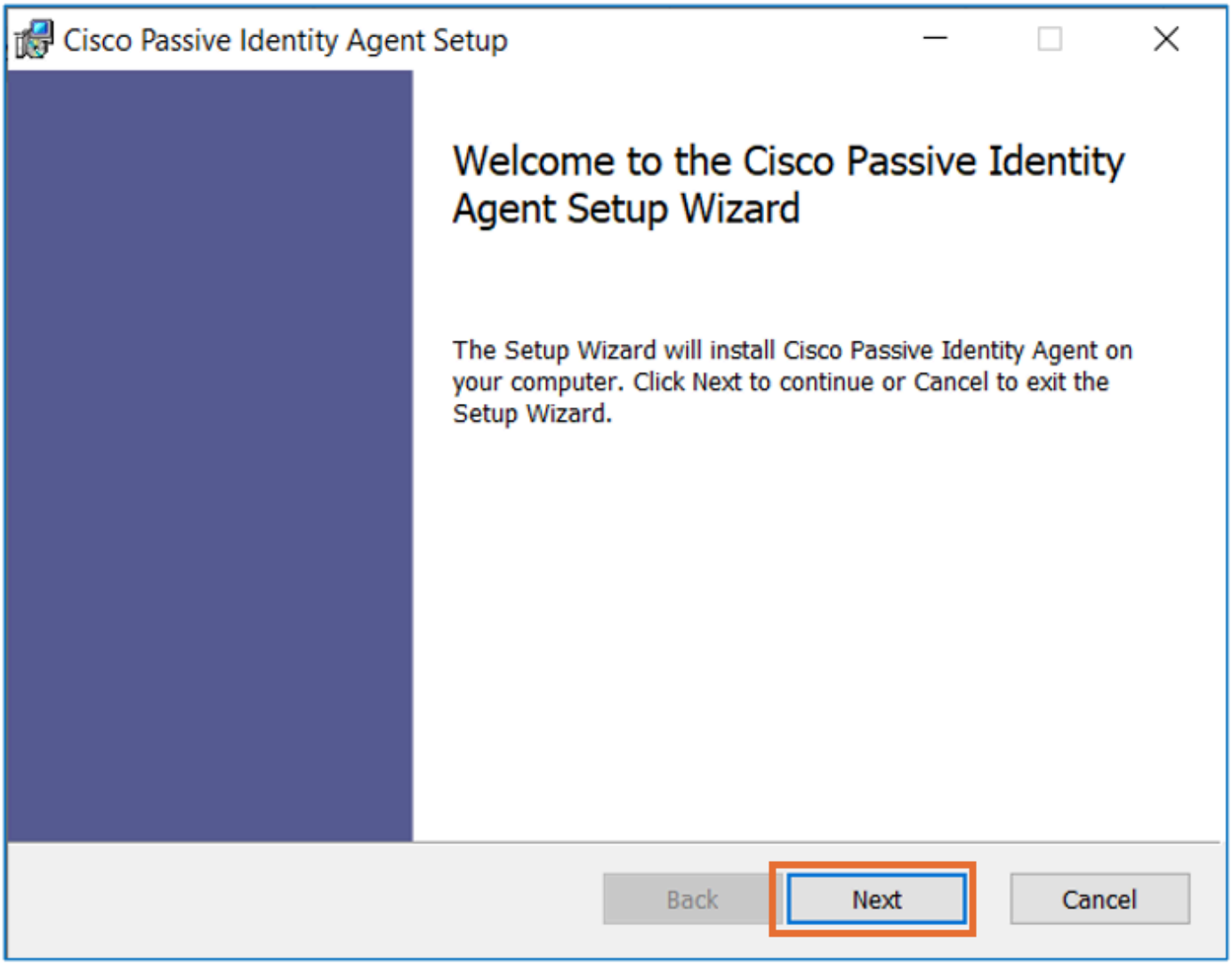
下载代理后，在域控制器上开始安装过程。



代理

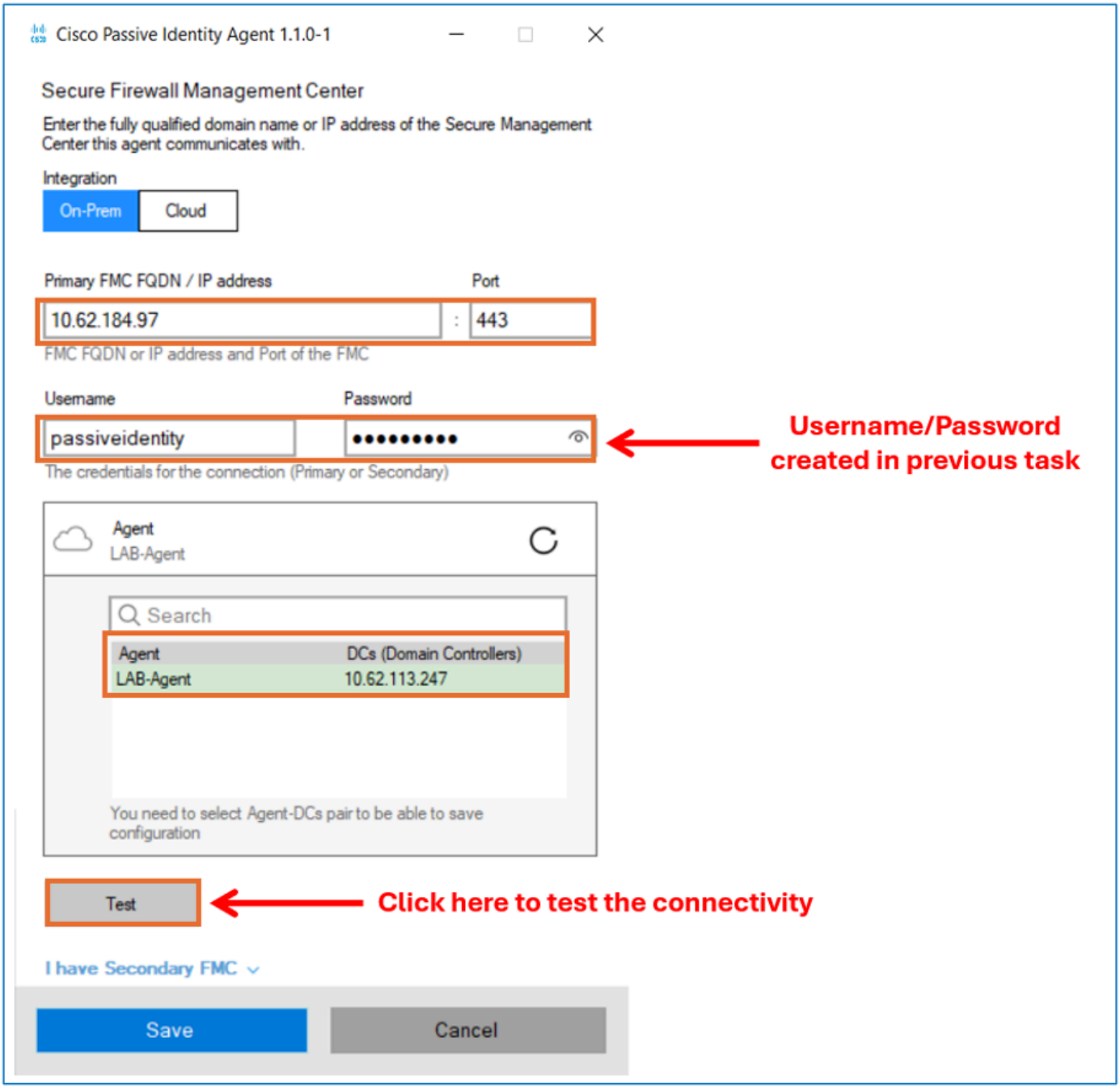
]

请参阅提供的安装说明以完成设置。



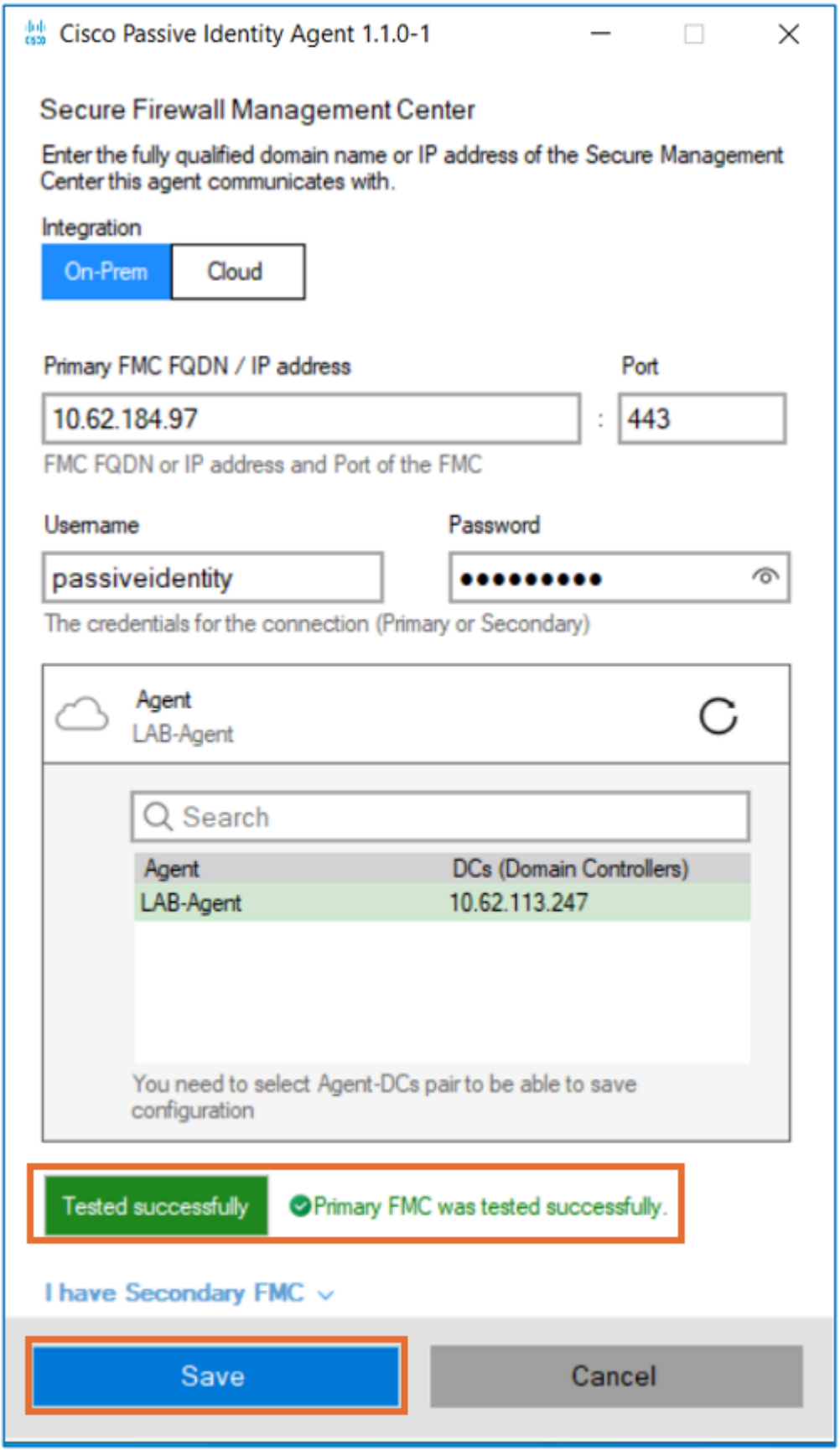
Install（安装）

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。



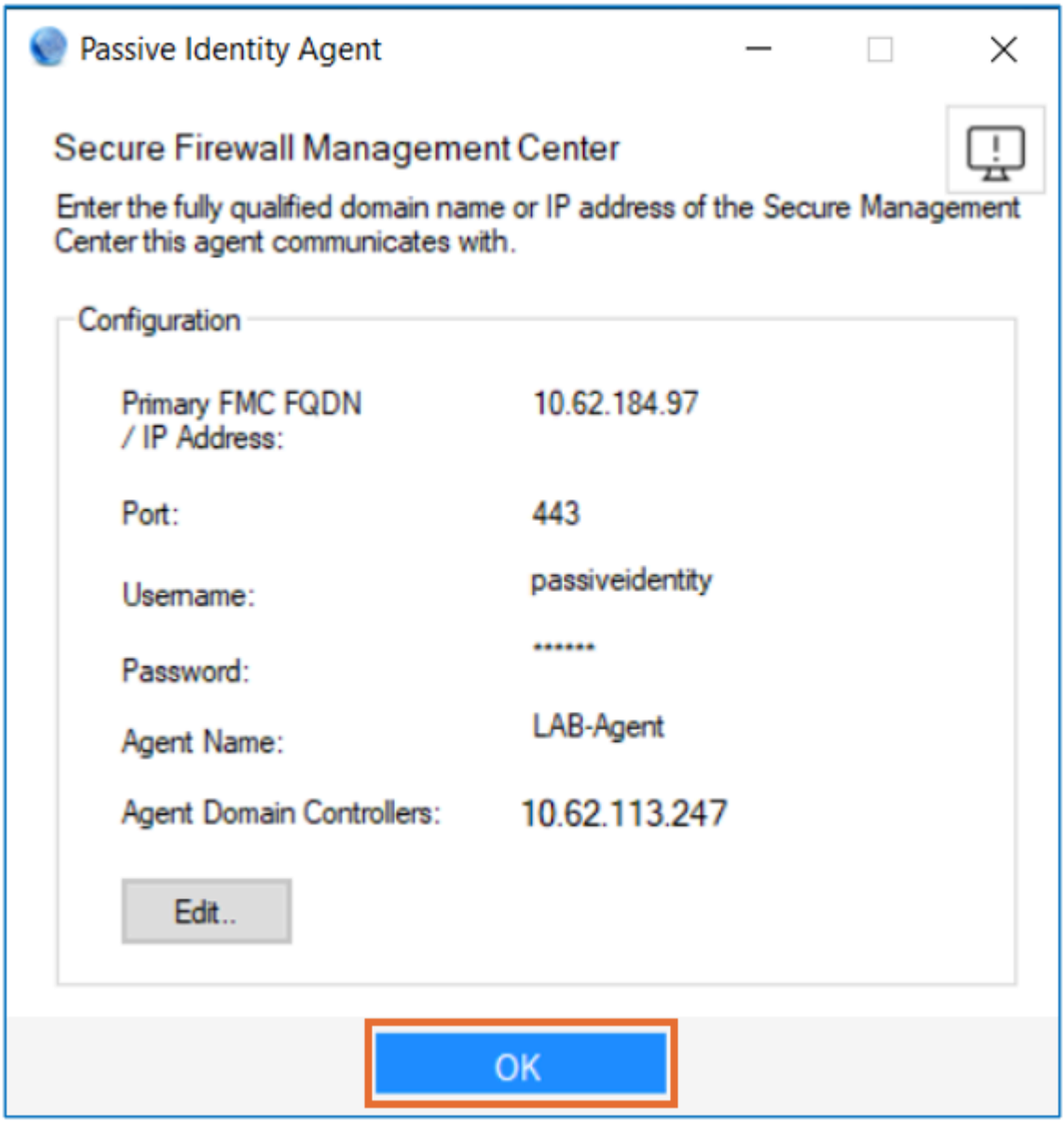
配置代理。

成功测试连接后，单击Savebutton。



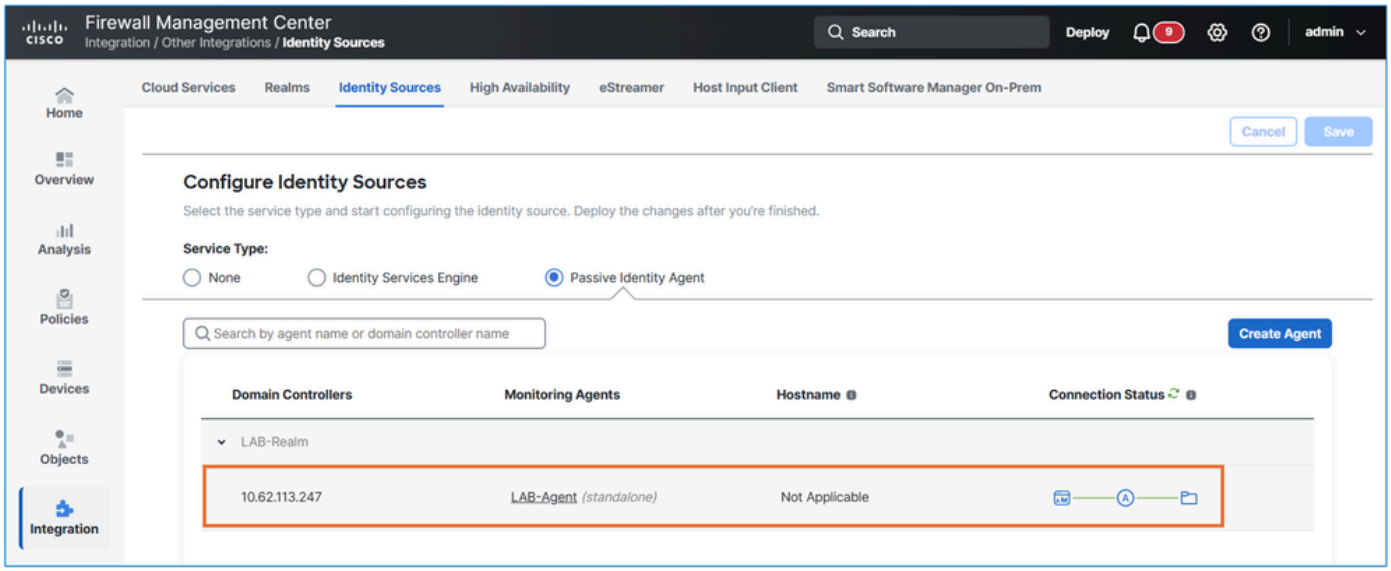
测试

单击OK按钮完成代理配置。



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。



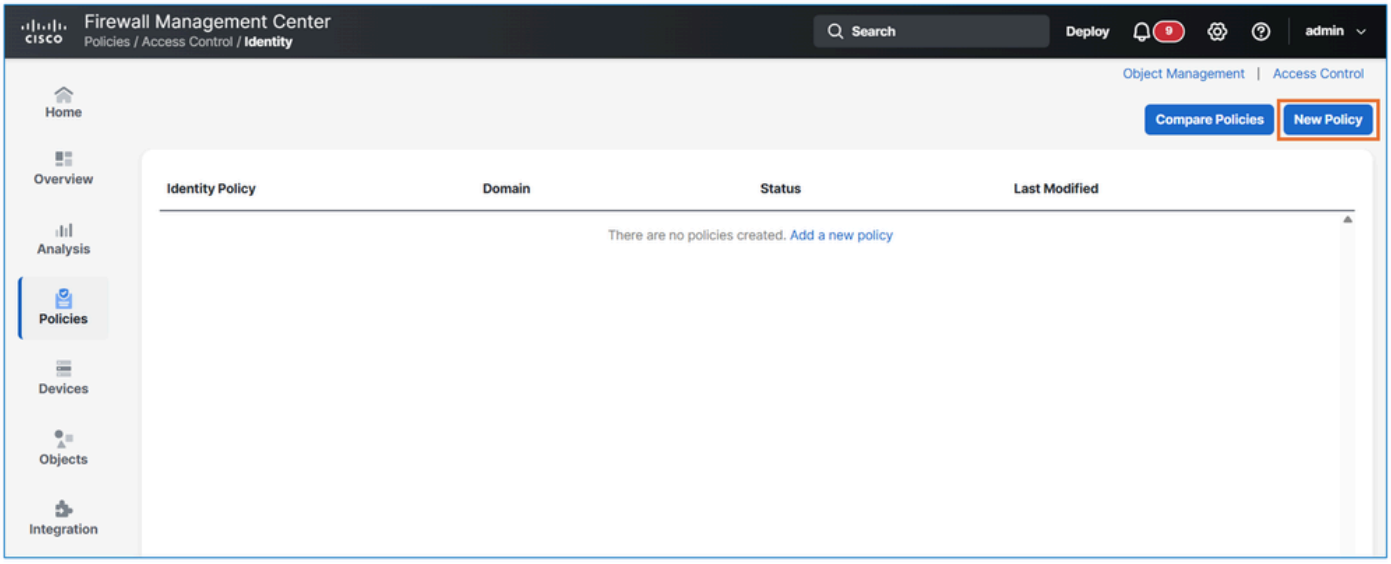
验证来自fmc的通信

配置身份策略

根据提供的表创建身份策略。

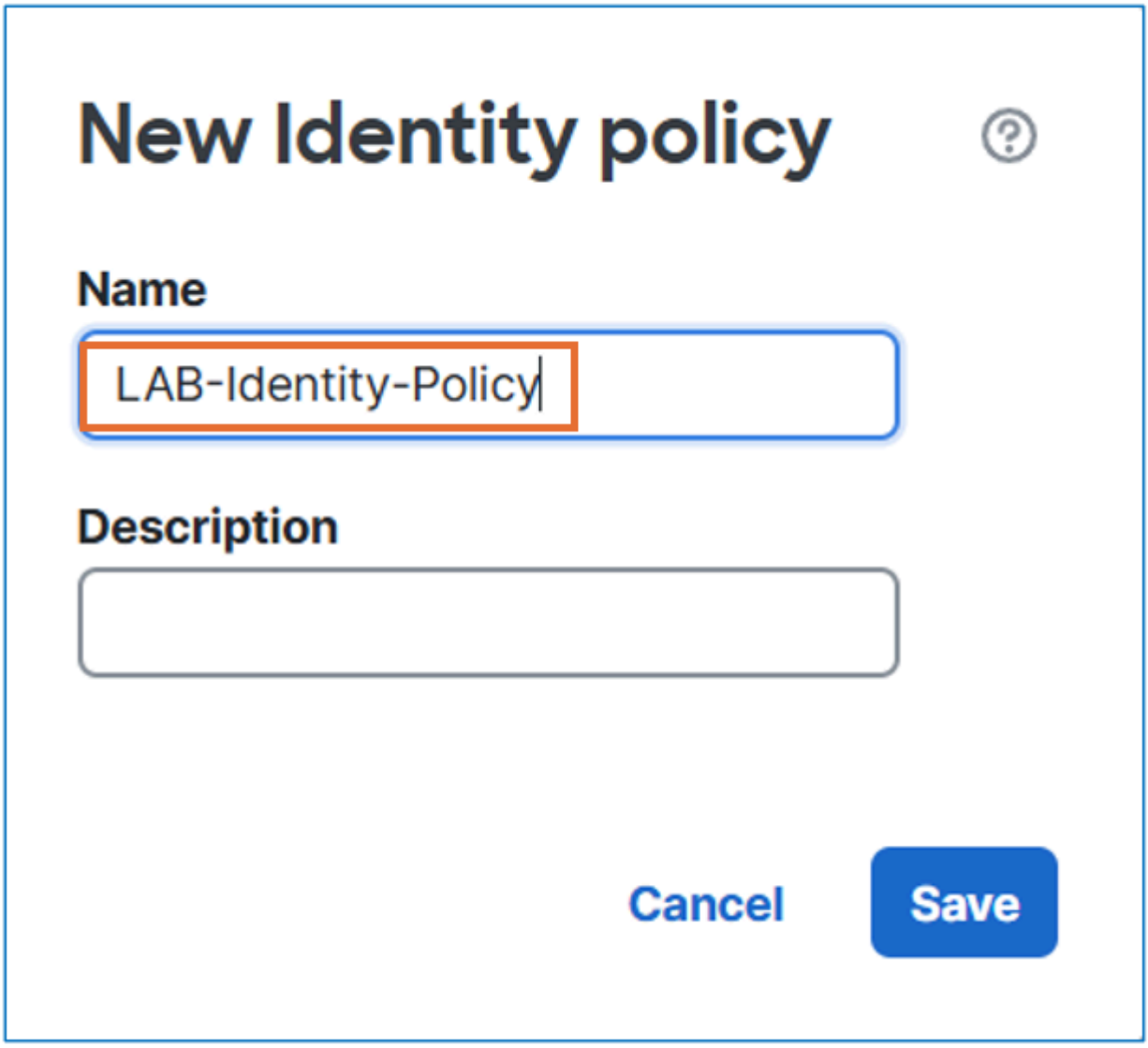
策略名称	规则名称	身份验证领域	剩余设置
实验室身份策略	规则1	实验室领域	保留为默认值

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



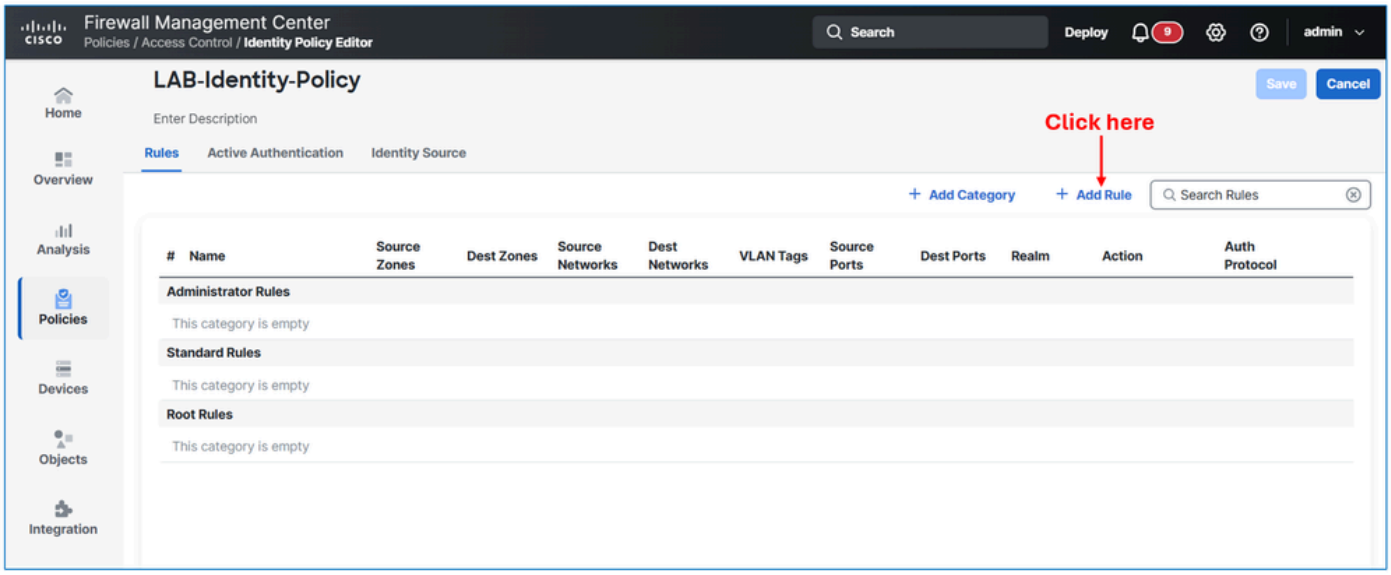
新策略

根据任务要求输入策略名称。



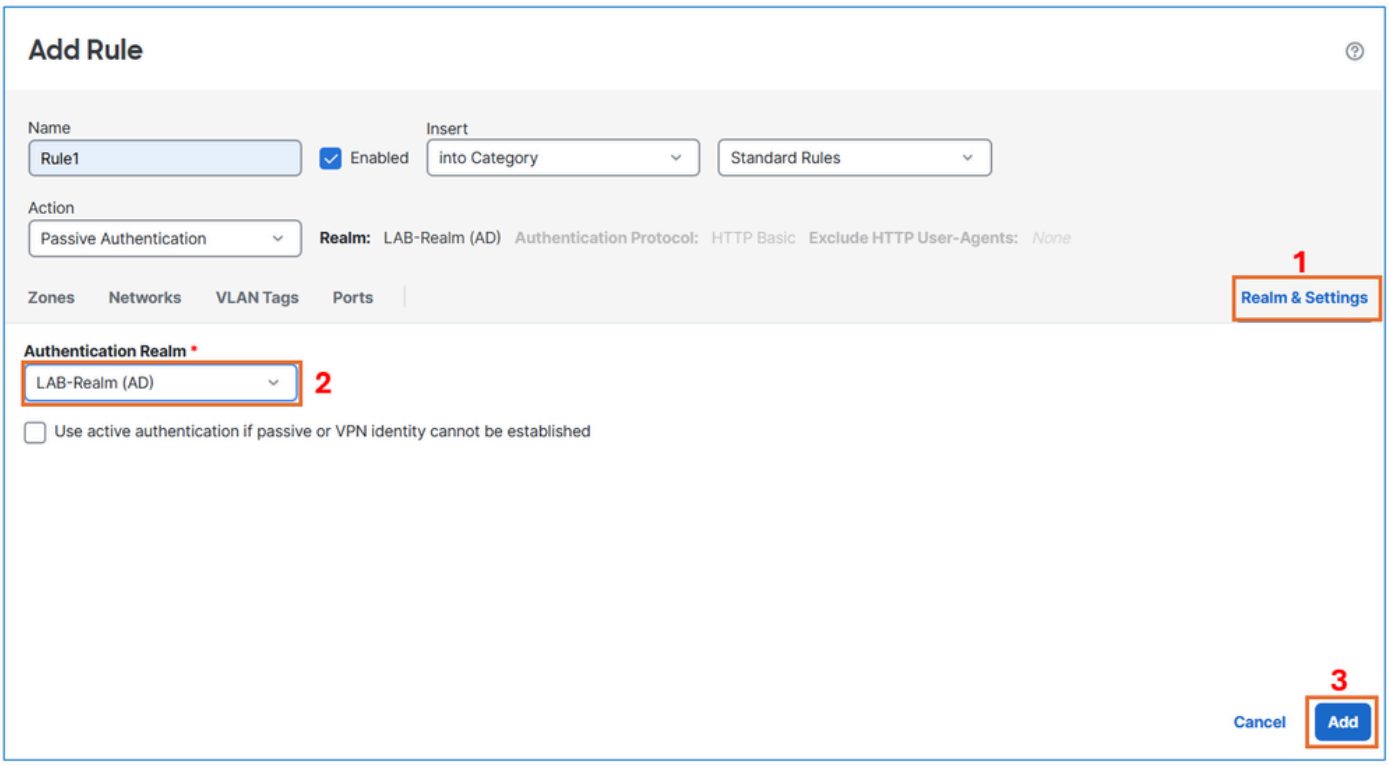
新策略

单击Add Rule按钮。



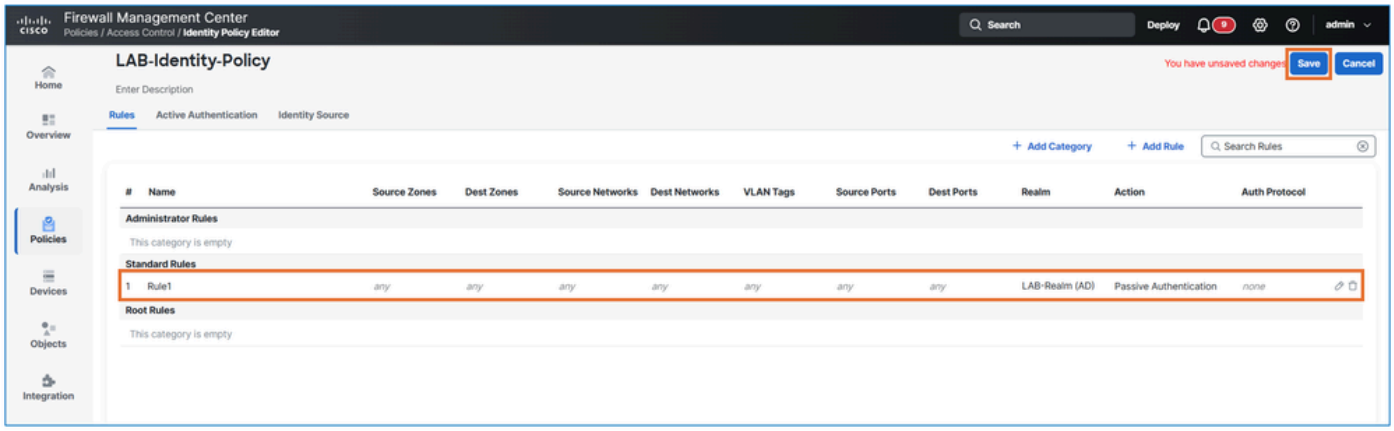
创建规则

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



领域设置

单击Savebutton。



保存配置

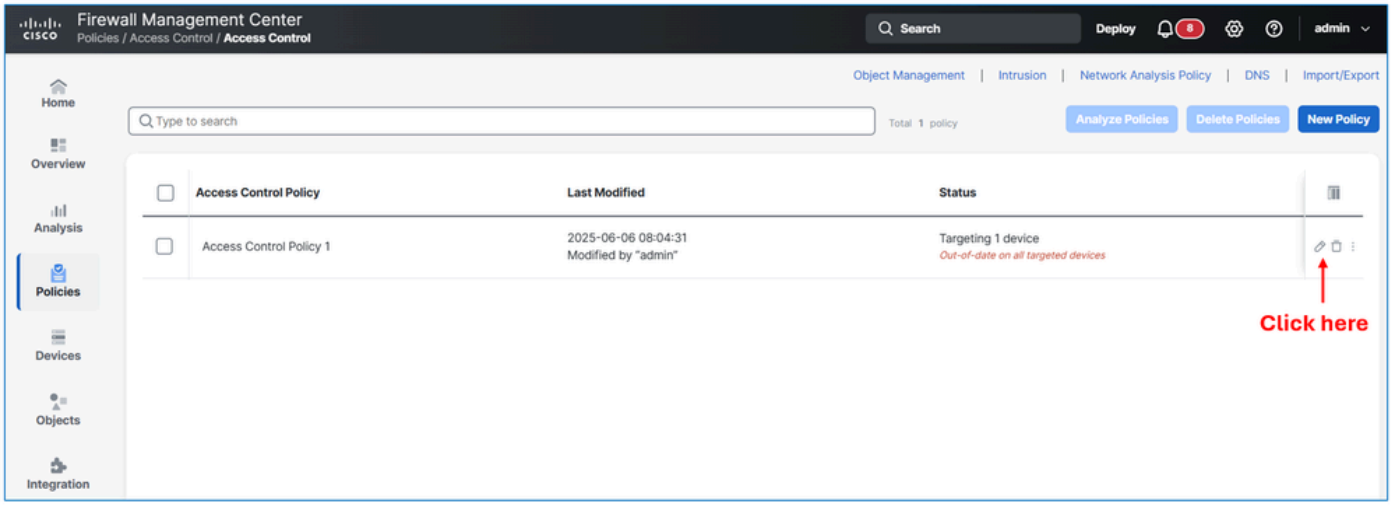
配置访问控制策略

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

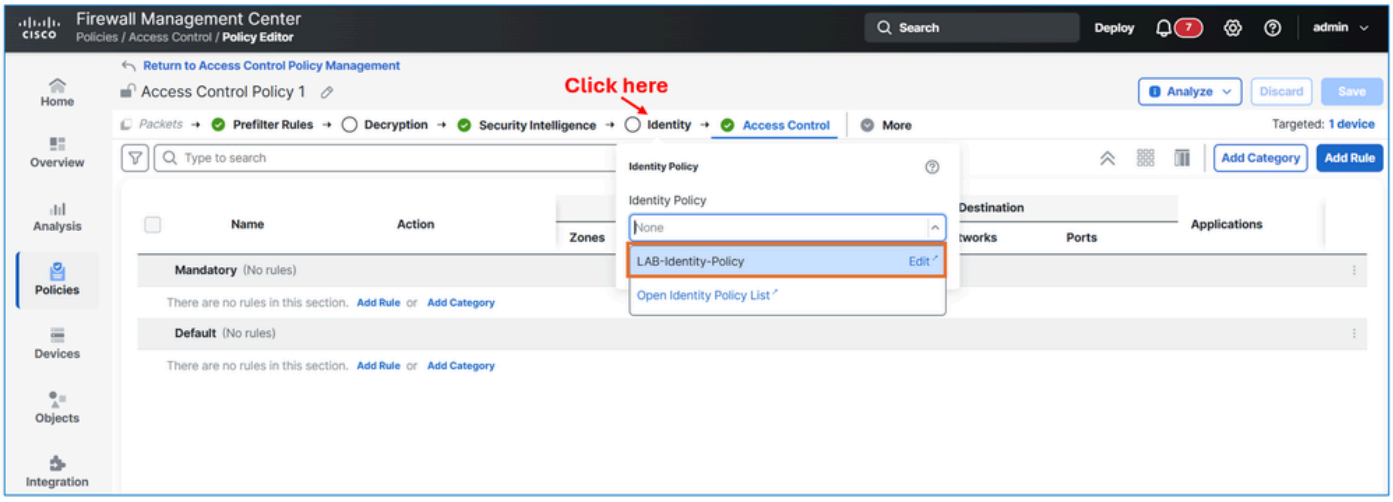
步骤1.将身份策略链接到访问控制策略

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

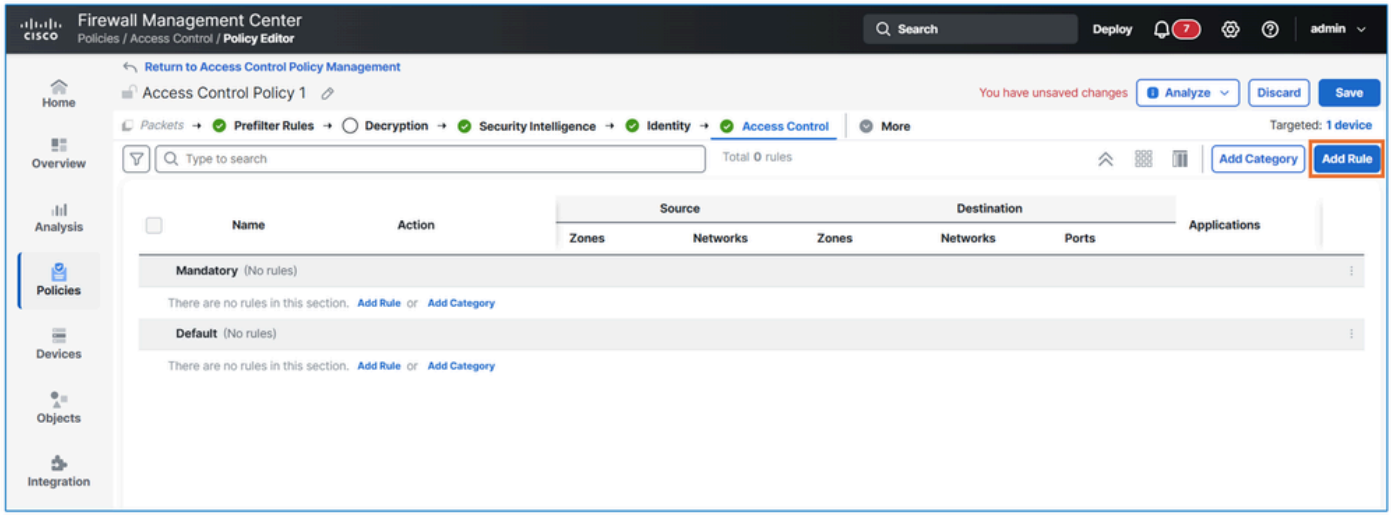
导航到Identitysection并链接在上一个任务中创建的身份策略。



添加身份策略

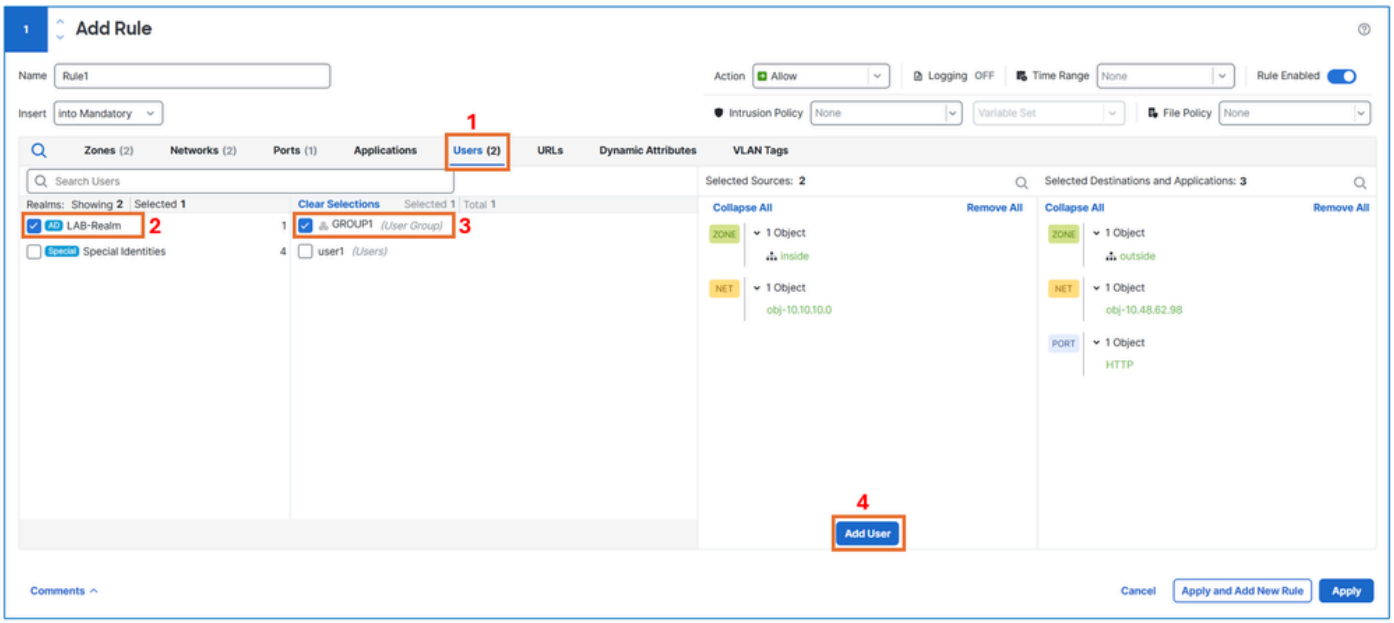
单击Applybutton

步骤2.创建访问控制规则。



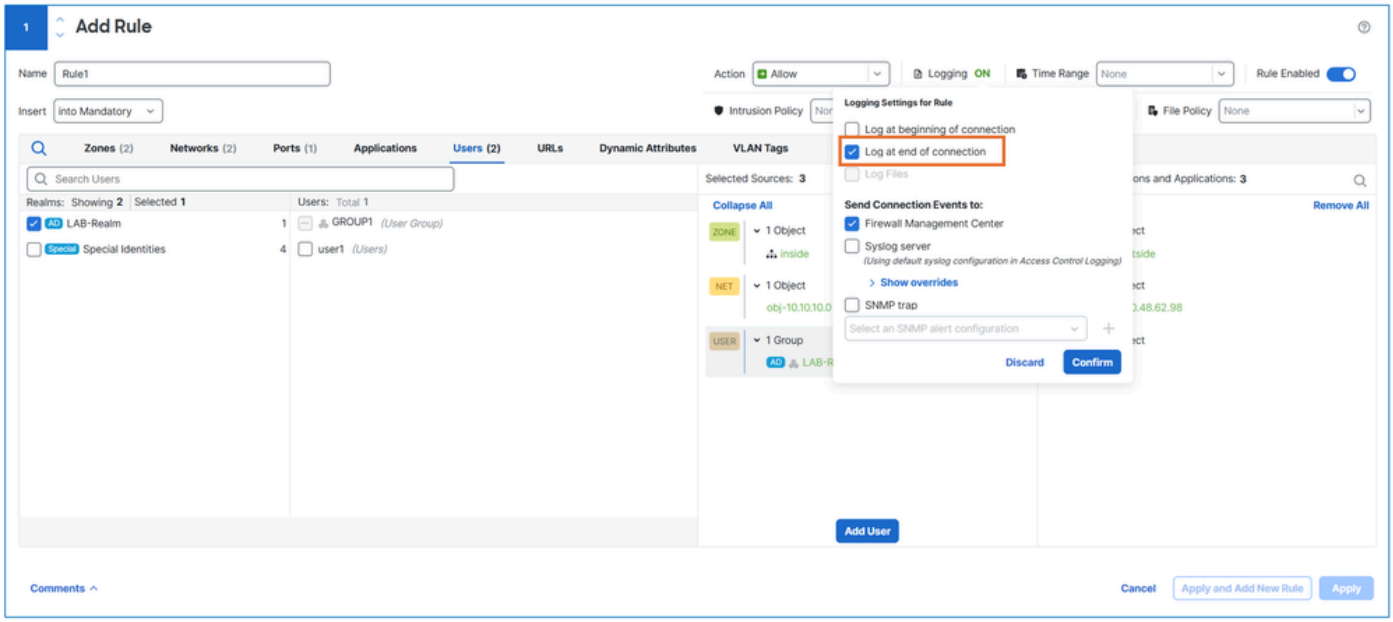
创建ACP

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

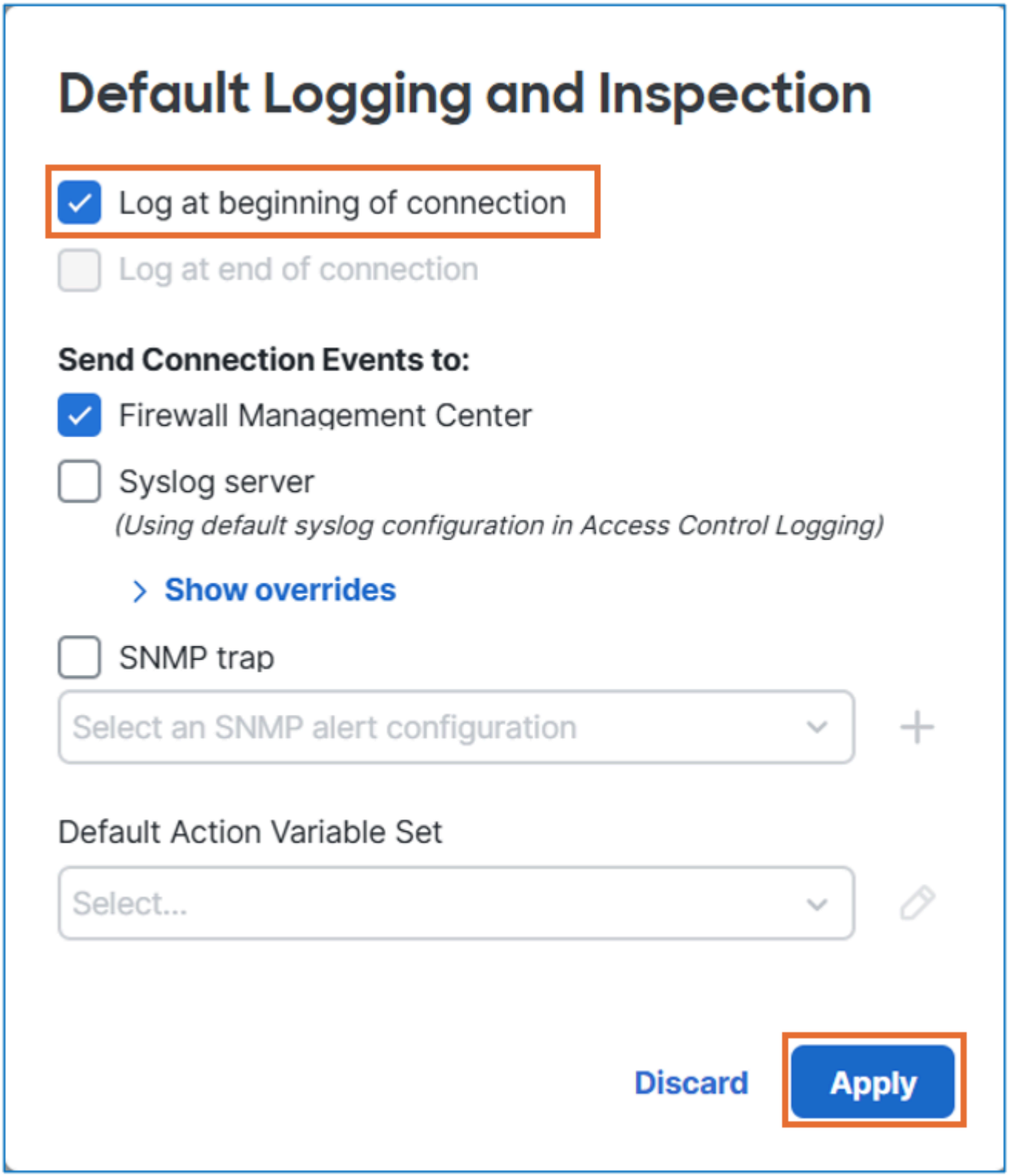
通过选择连接结束时的Log启用规则的日志记录。



启用日志

步骤3.为默认操作启用logging。

点击这些按钮图标以修改Default Actionlogging设置。



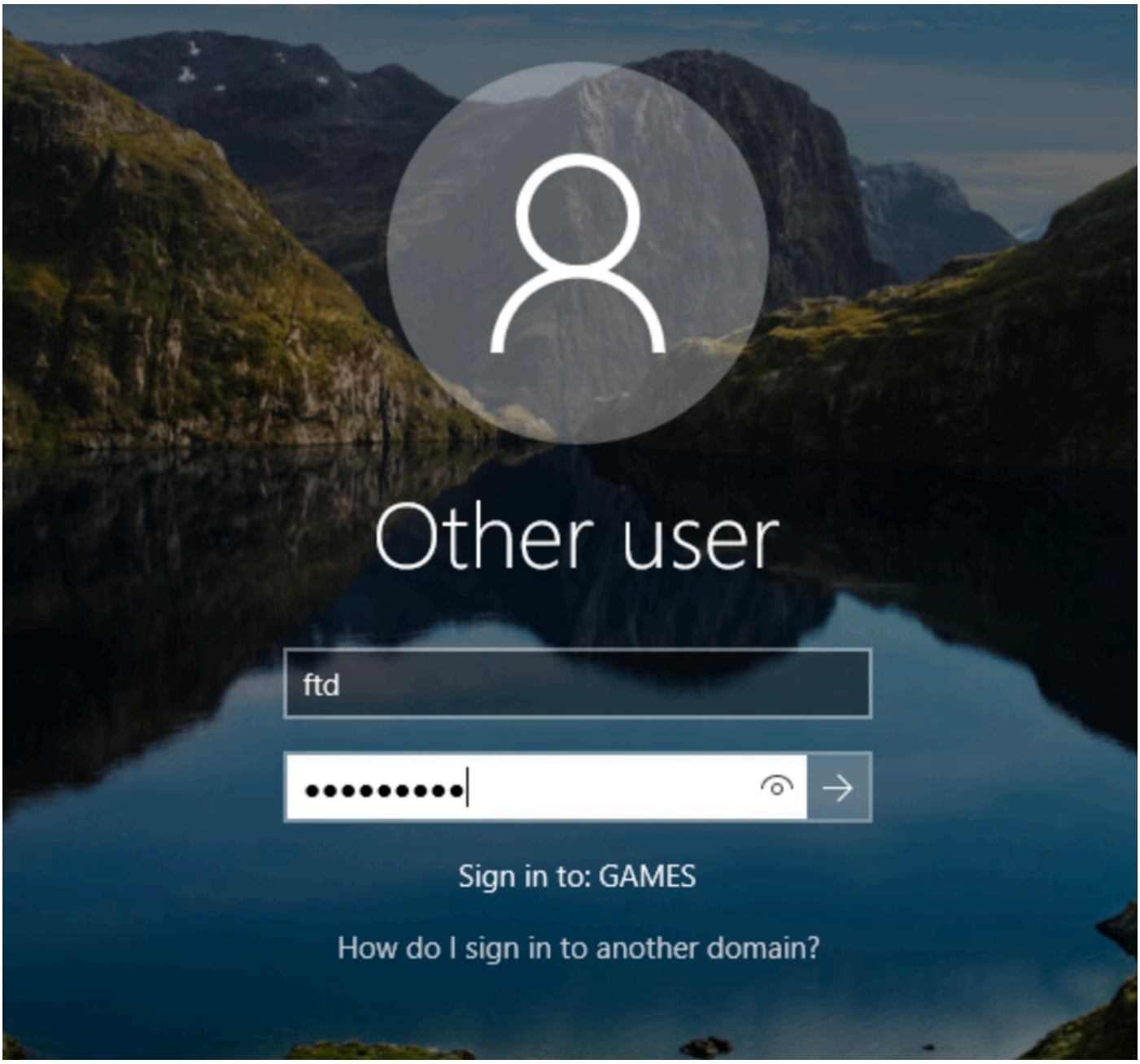
启用日志

保存并部署FTD上的配置。

确认

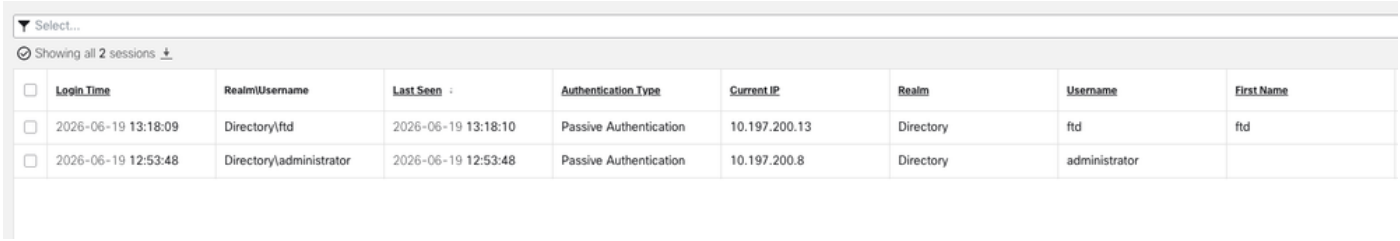
通过确认仅允许流量用于ftd来验证被动身份操作。

从用户计算机登录到域用户。



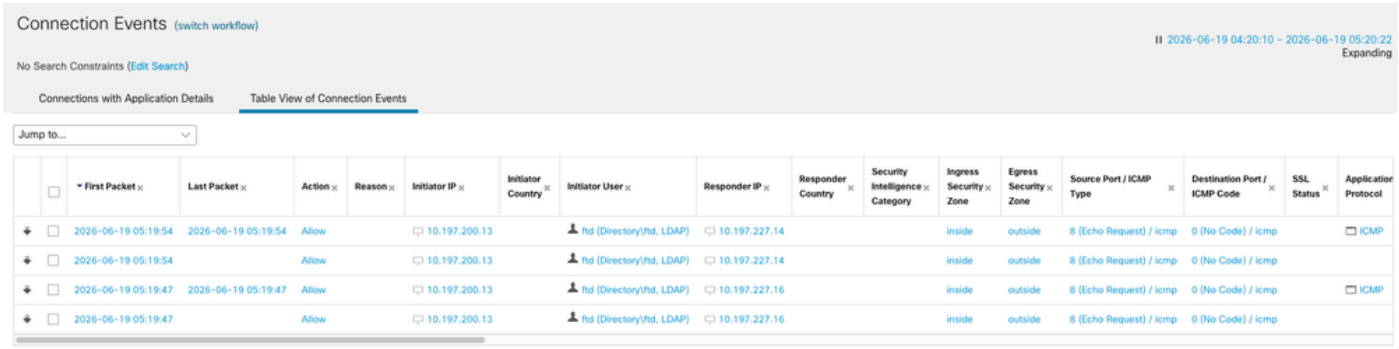
用户登录

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。



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。

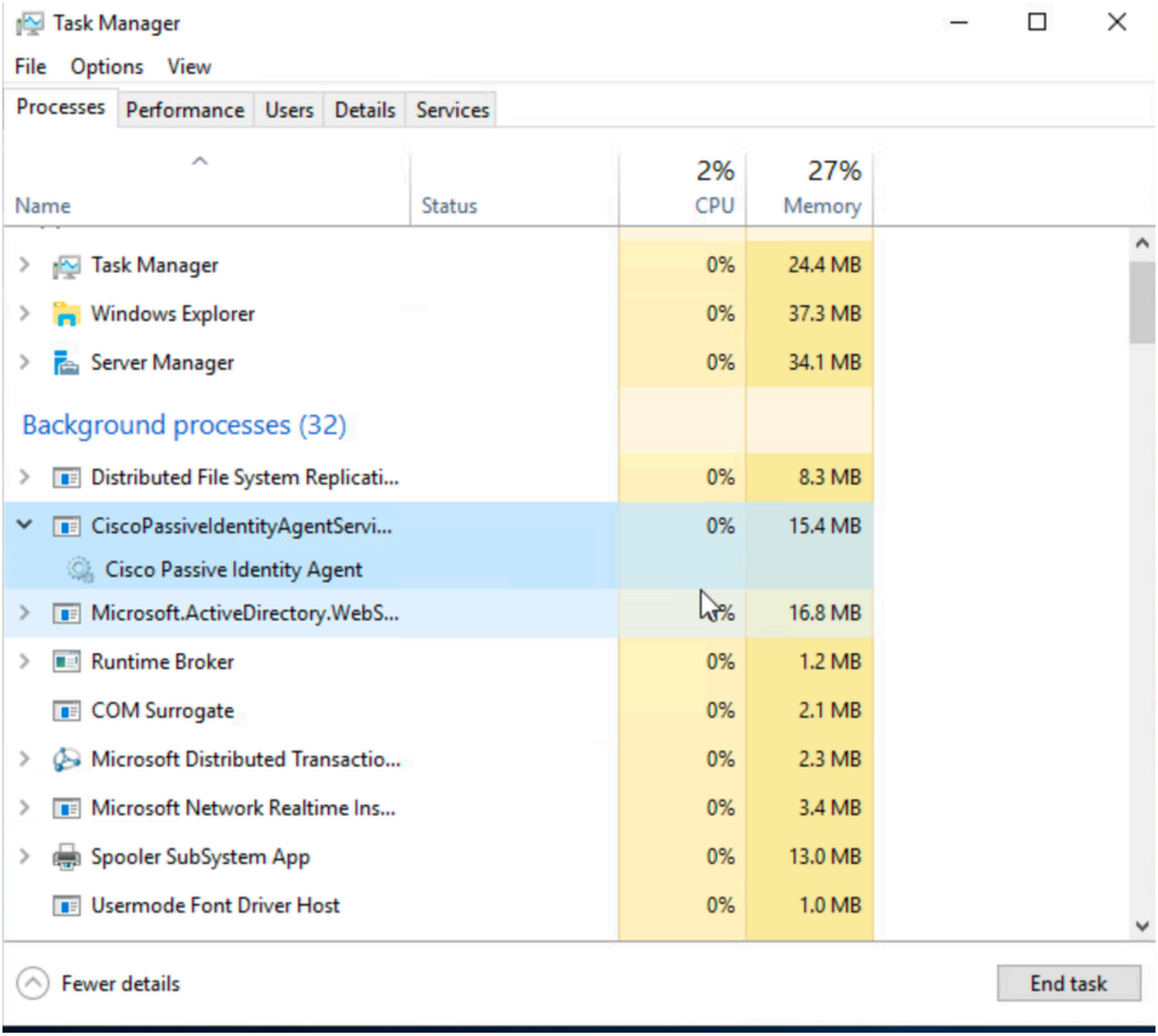


活动会话

故障排除

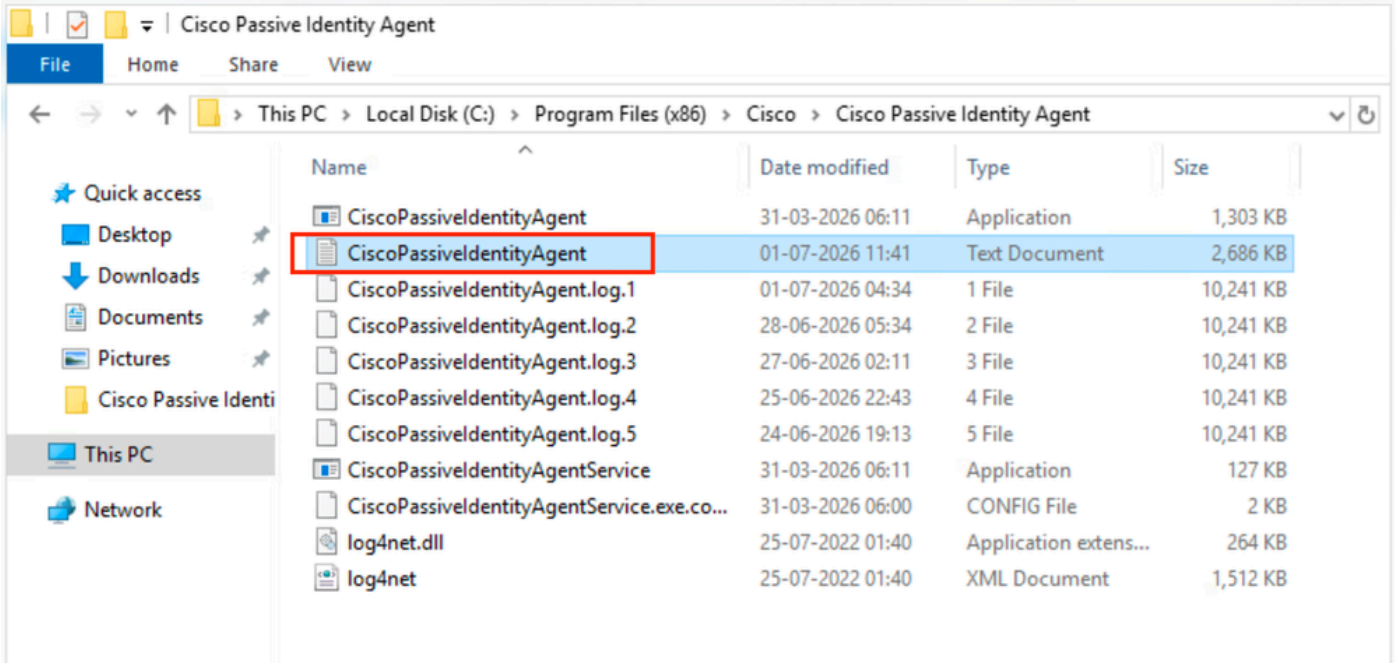
检查代理日志

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。



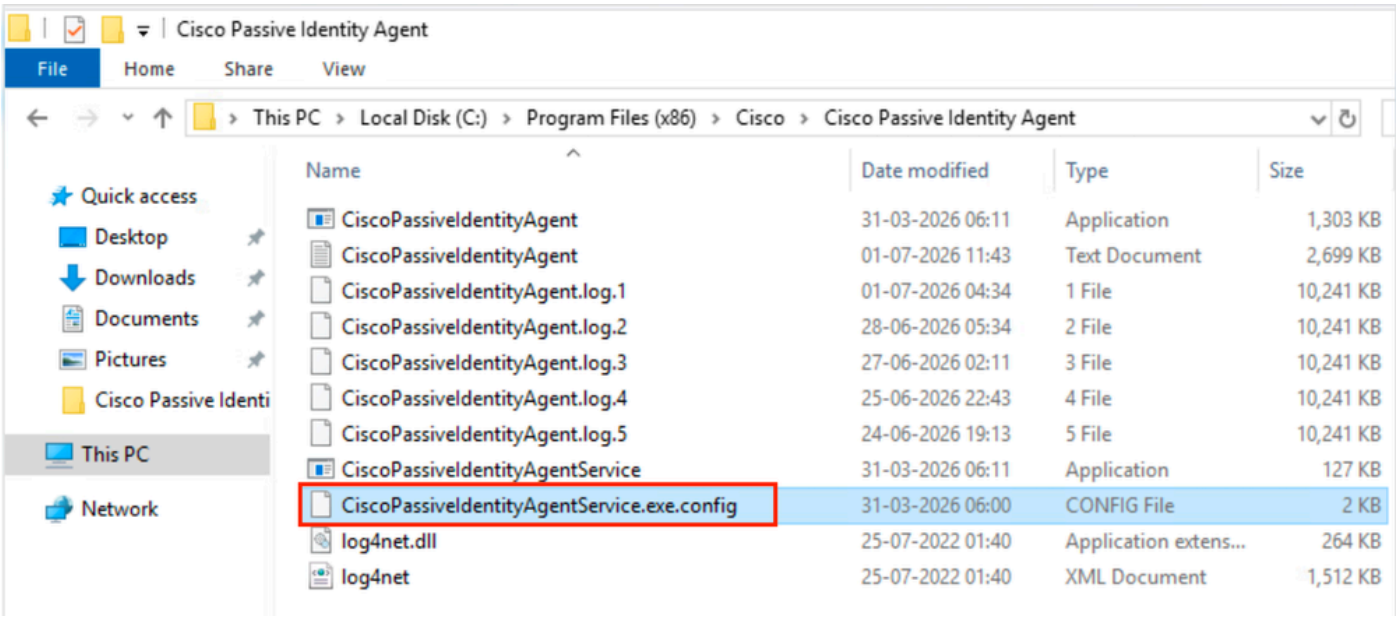
正在运行的任务

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

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：[f"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）。