

使用FMC配置被動身份代理

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[組態](#)

[配置被動身份代理源](#)

[在安全防火牆管理中心上建立被動身份代理使用者](#)

[安裝和配置被動身份代理軟體](#)

[配置身份策略](#)

[配置訪問控制策略](#)

[驗證](#)

[疑難排解](#)

[檢查代理日誌](#)

[FMC日誌](#)

簡介

本文檔介紹如何配置將會話資料傳送到FMC的被動身份代理源

必要條件

需求

- 運行版本7.6+的Cisco安全防火牆管理中心
- 運行版本7.6+的思科安全防火牆
- 在Windows Active Directory伺服器中，伺服器必須運行Windows Server 2008或更高版本。
- 必須在安全防火牆威脅防禦裝置上啟用Snort 3。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆管理中心7.6.5
- 思科安全防火牆7.6.5
- Windows Server 2022上運行的Microsoft Active Directory。

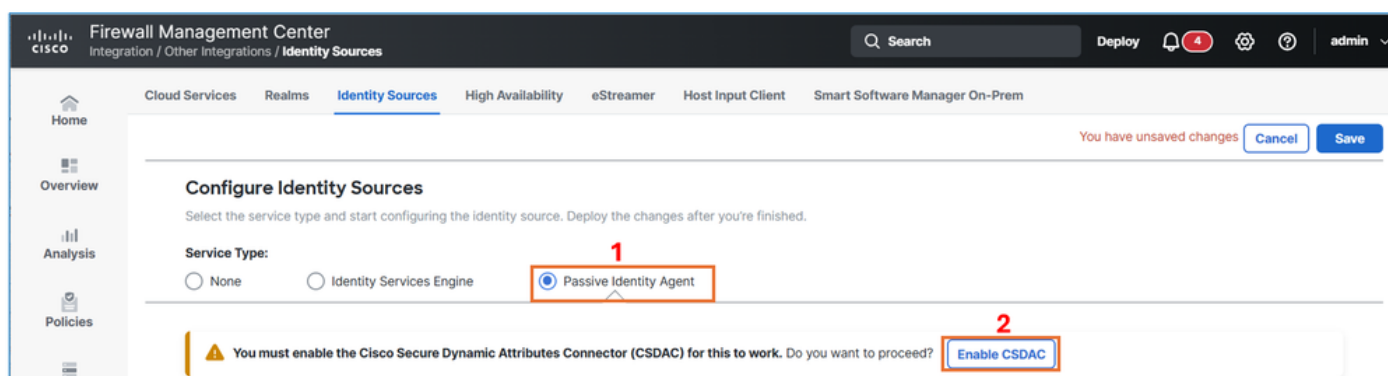
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

在配置代理之前，請完成AD和FMC整合。

配置被動身份代理源

在FMC UI中，導航至Integration > Other Integrations > Identity Sources，然後點選Passive Identity Agent。如果尚未啟用Cisco Secure Dynamic Attributes Connector，則會通過按一下Enable CSDAC來提示您啟用它。



被動身分識別代理

按一下Enablebutton以啟用CSDAC。

Enable Cisco Secure Dynamic Attributes Connector?



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

Cancel

Enable

啟用CSDAC

此步驟大約需要10分鐘。正確啟用CSDAC後，按一下Donebutton繼續。

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

已啟用CSDAC

按一下Create Agent按鈕。

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?

```
graph LR; FMC[Firewall Management Center] -- 1 --> Agents[Agents]; Agents -- 2 --> DCs[Domain Controllers]; DCs -- 3 --> Agents; Agents -- 4 --> FMC; Agents -- 5 --> FMC;
```

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

建立代理

定義代理的名稱，選擇Standaloneoption，然後將其與上一個任務中建立的Domain Controller關聯

。

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:

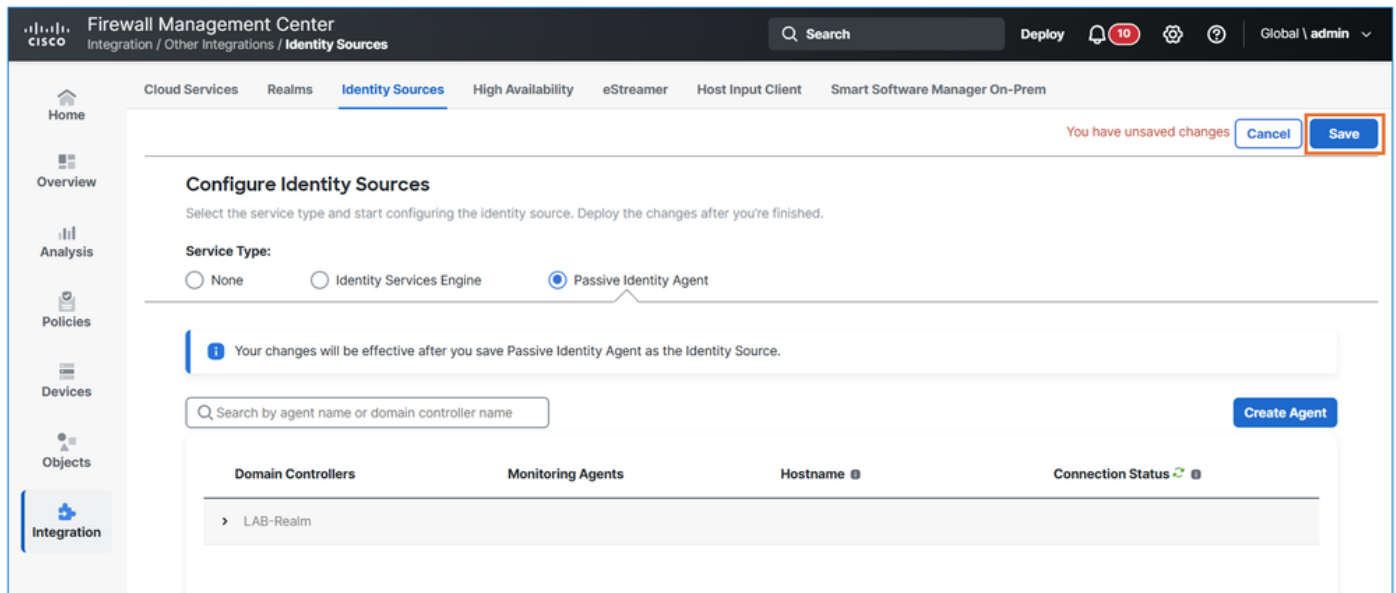
This agent will be created and assigned to the selected domain controller. Install it on the domain controller (or on its member machine) to start the tracking.

Cancel

Save

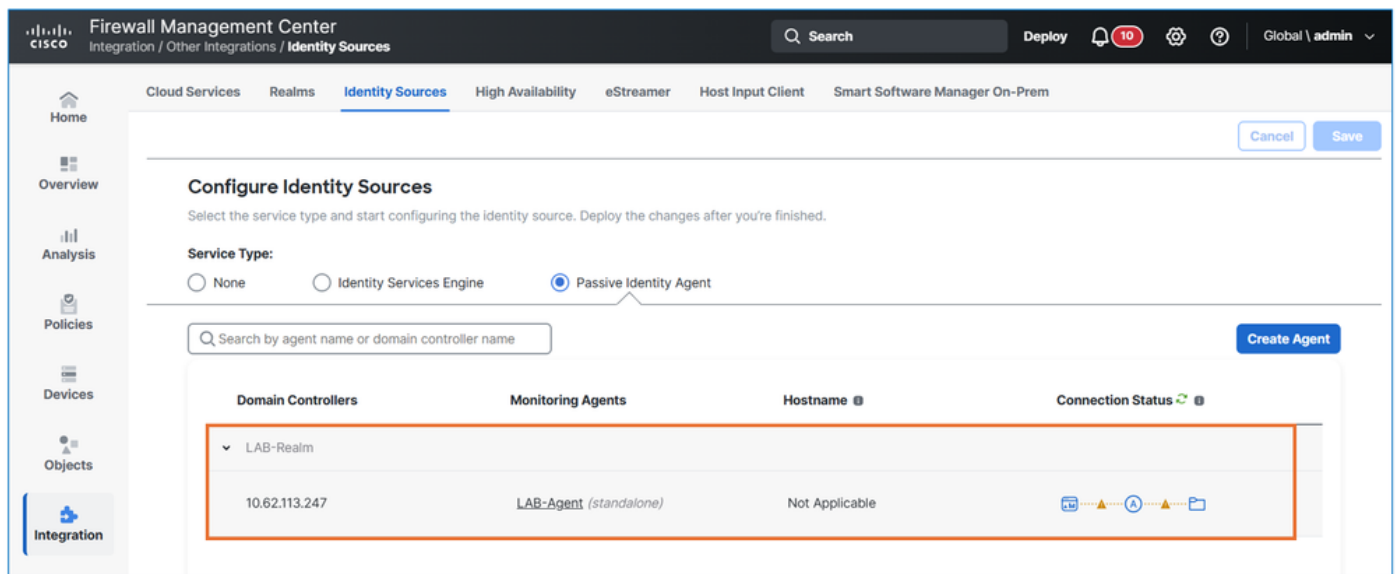
配置代理

按一下「儲存」按鈕。



儲存組態

結果。



驗證狀態



附註：被動身份代理使用線路指示狀態，琥珀色表示該代理從未成功與安全防火牆管理中心通訊。新建立的代理線路為琥珀色，在配置完成前保持琥珀色。

在安全防火牆管理中心上建立被動身份代理使用者

建立有足夠許可權與被動身份代理通訊的Secure Firewall Management Center使用者。此使用者執

行其他任務的許可權有限；使用者應僅啟用與被動身份代理的通訊。

在FMC UI中，導航至System > Users，然後點選Create User。根據任務要求填寫使用者詳細資訊。

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

建立使用者

僅分配被動身份使用者角色。按一下「儲存」按鈕。

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

選擇被動身份使用者

安裝和配置被動身份代理軟體

在指定的域控制器上安裝並配置被動身份代理軟體。

從software.cisco.com下載被動身份代理。

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

下載軟體

下載代理後，在域控制器上開始安裝過程。

Downloads

FileHomeShareView

This PC > Downloads

Quick access

Desktop

Downloads

Documents

Pictures

Cisco Passive Identi

This PC

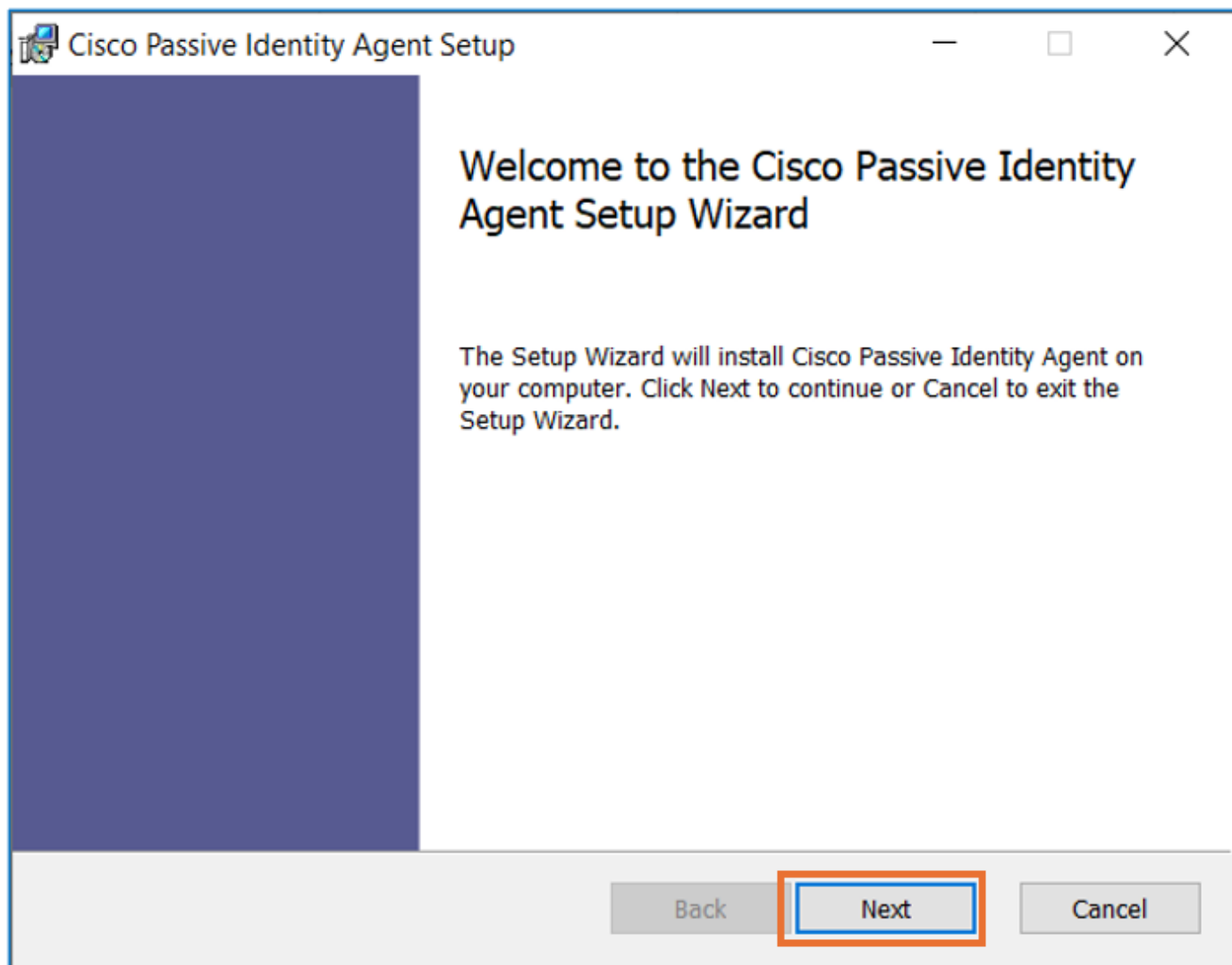
Network

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

代理

]

請參閱提供的安裝說明以完成設定。



安裝

安裝完成後，開啟被動Identity Agent軟體，然後按照任務要求中的指定輸入所需的資訊。按一下Test按鈕驗證與FMC的連線。

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

I have Secondary FMC ▾

Username/Password created in previous task

Click here to test the connectivity

配置代理。

成功測試連線後，按一下Savebutton。

Cisco

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

測試

按一下OK按鈕完成代理配置。

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

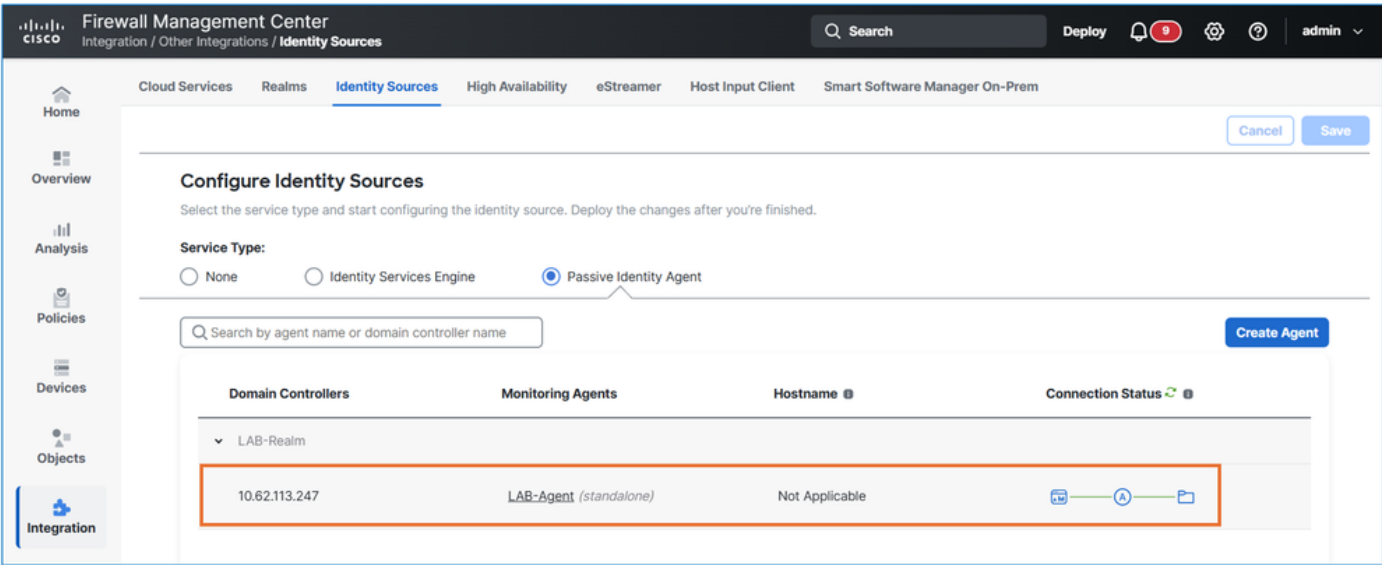
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

代理正在運行

在FMC UI中，導航到整合>其他整合>身份源>被動身份代理。確認被動身份代理顯示綠色狀態。



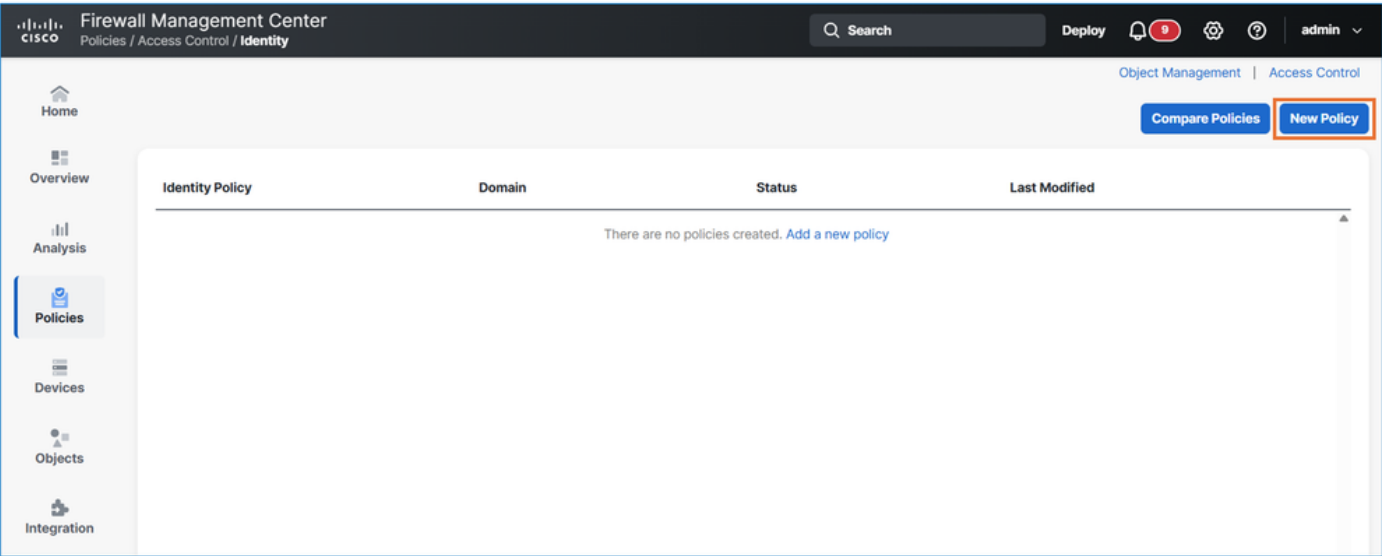
驗證來自fmc的通訊

配置身份策略

根據提供的表建立身份策略。

策略名稱	規則名稱	身份驗證領域	剩餘設定
LAB-Identity-Policy	Rule1	實驗室領域	保留為預設值

在FMC UI中，導航至Policies > Access Control > Identity。按一下New Policy按鈕。



新策略

根據任務要求輸入策略名稱。

New Identity policy

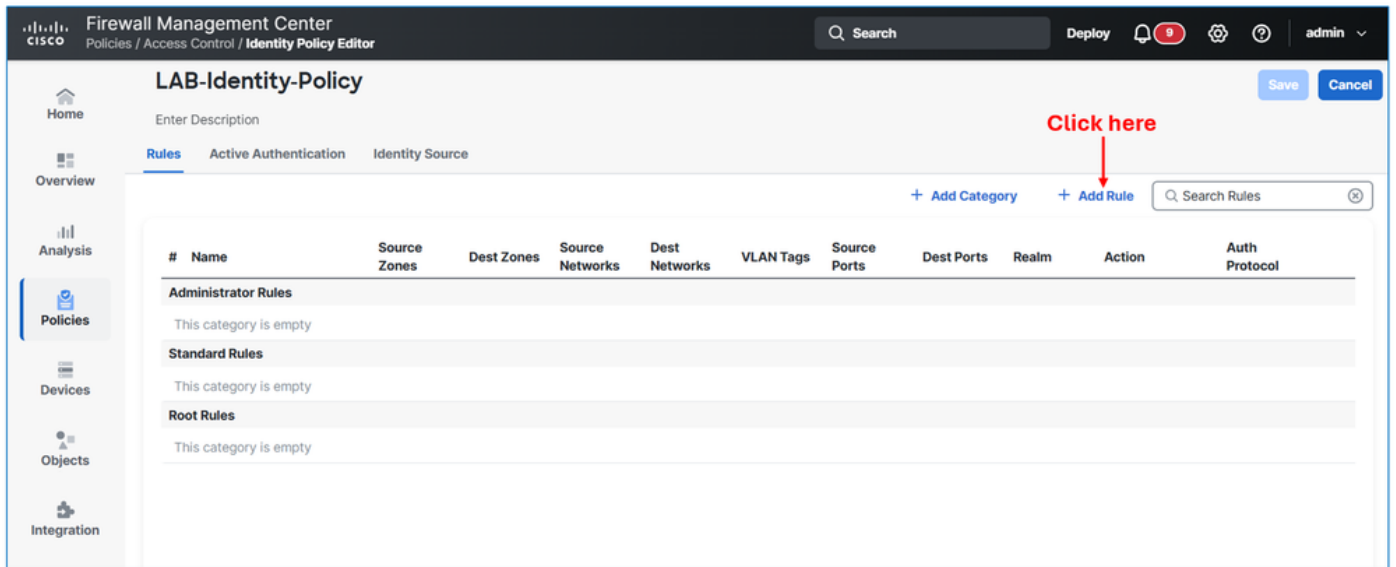
Name

Description

CancelSave

新策略

按一下Add Rule按鈕。

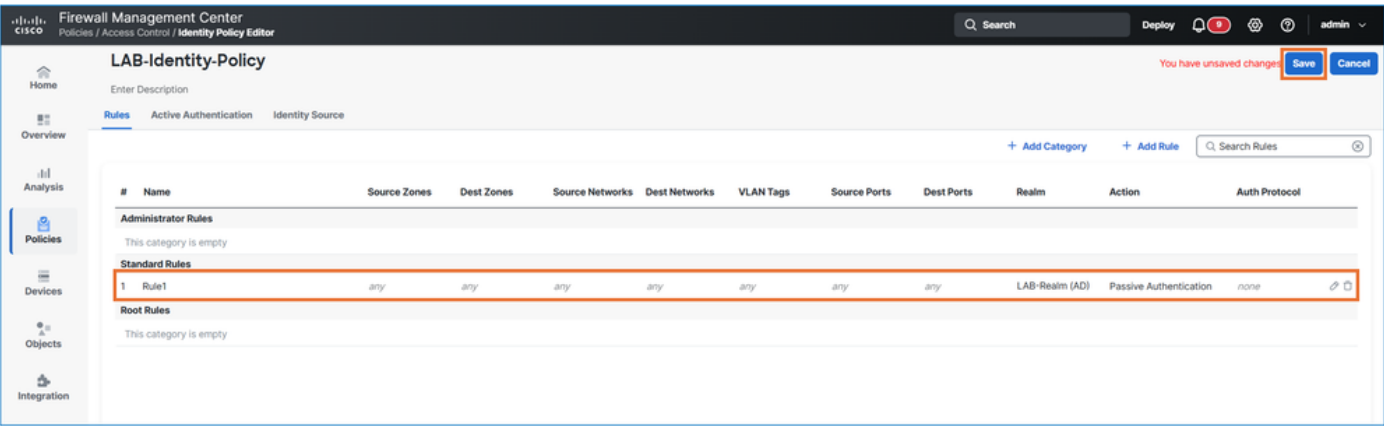


建立規則

導覽至Realm & Settings表，然後根據任務要求選擇Authentication。最後，按一下Addbutton。

領域設定

按一下「儲存」按鈕。



儲存組態

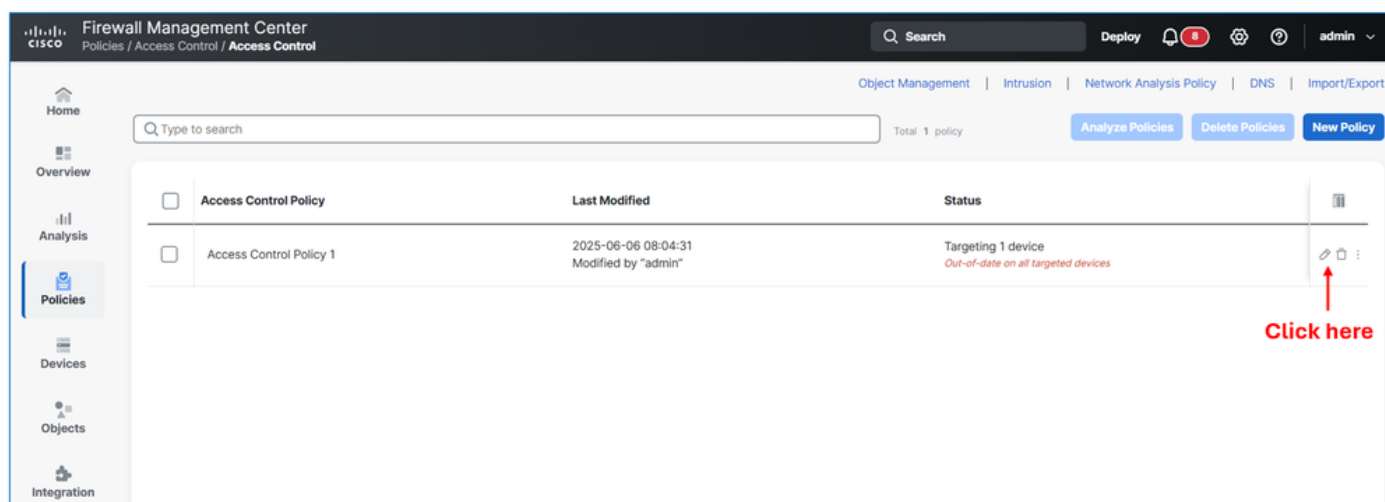
配置訪問控制策略

將身份策略連結到訪問控制策略，並建立具有以下屬性的訪問策略Rule:

屬性名稱	價值
規則名稱	Rule1
動作	允許
源區域	INSIDE
目標區域	OUTSIDE
來源網路	10.10.10.0/24
目的地網路	10.48.62.98/32
服務	目標埠TCP 80(HTTP)
使用者	實驗室領域/組1
日誌記錄	在連線結束時

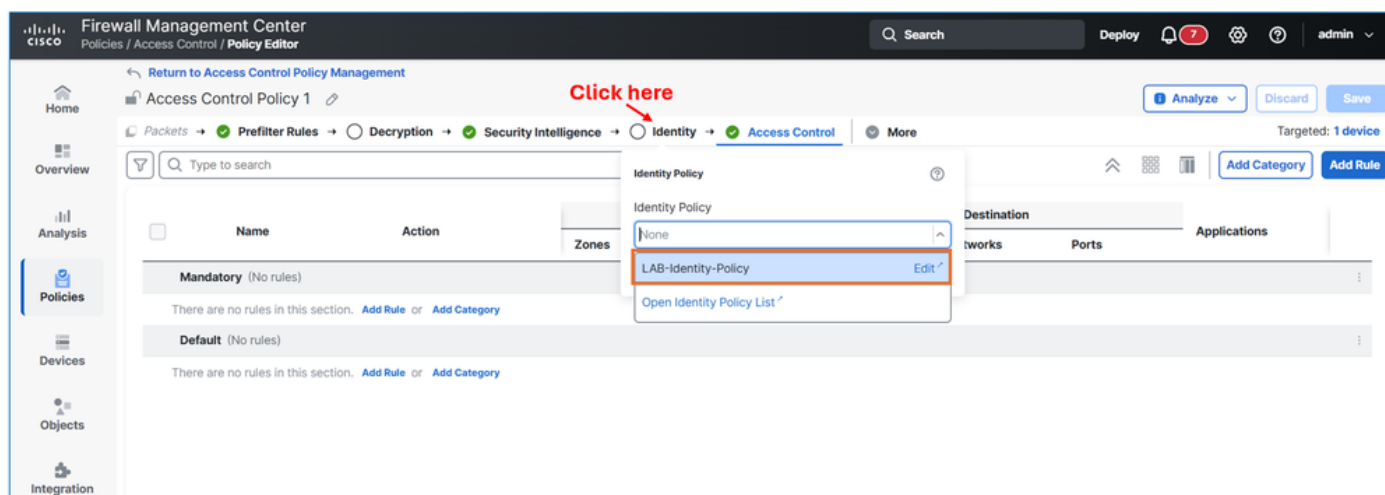
步驟1.將Identity 策略連結到Access Control 策略

在FMC UI中，導航至Policies > Access Control > Access Control。按一下策略的「編輯」按鈕。



編輯策略

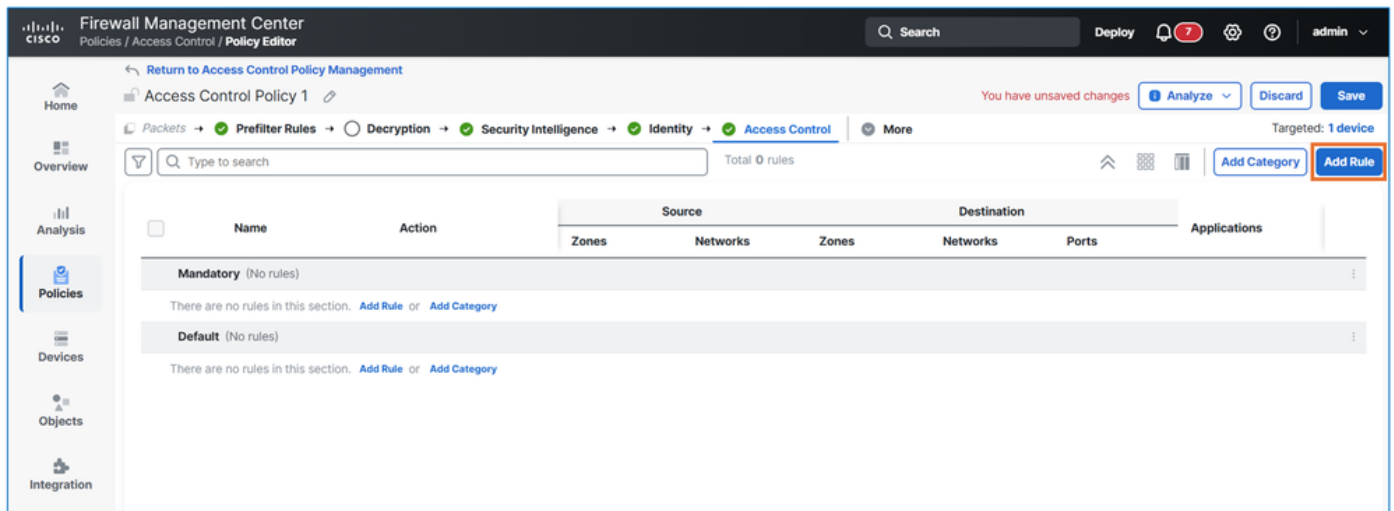
導航到Identitysection並連結在上一個任務中建立的Identity Policy。



新增身份策略

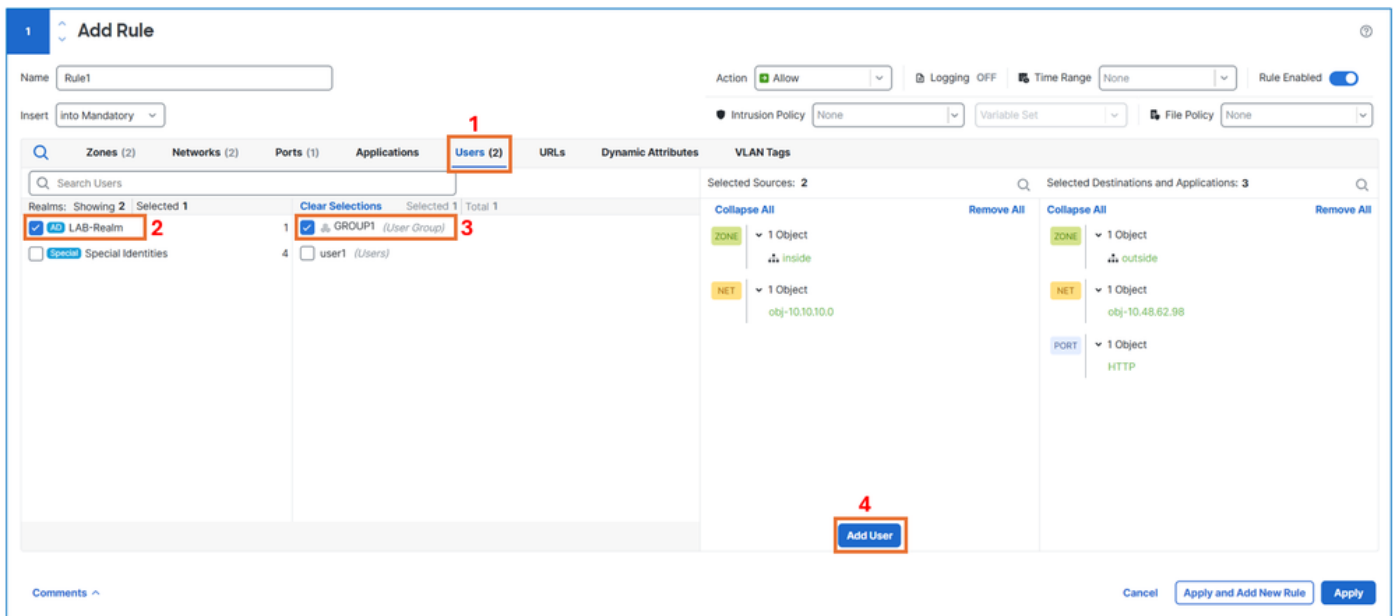
按一下Applybutton

步驟2.建立存取控制規則。



建立ACP

根據任務要求輸入詳細資訊，最重要的是，在Userstab下，從LAB-Realm新增GROUP1。



在規則中新增使用者

通過在連線結束時選擇Log啟用規則的日誌記錄。

1 Add Rule

Name:

Insert:

Action: Logging: ☒ ON Time Range: Rule Enabled: ☒

Intrusion Policy:

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:

File Policy

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 ^

啟用記錄

步驟3.為預設操作啟用logging。

按一下這些設定圖示可修改預設操作日誌設定。

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

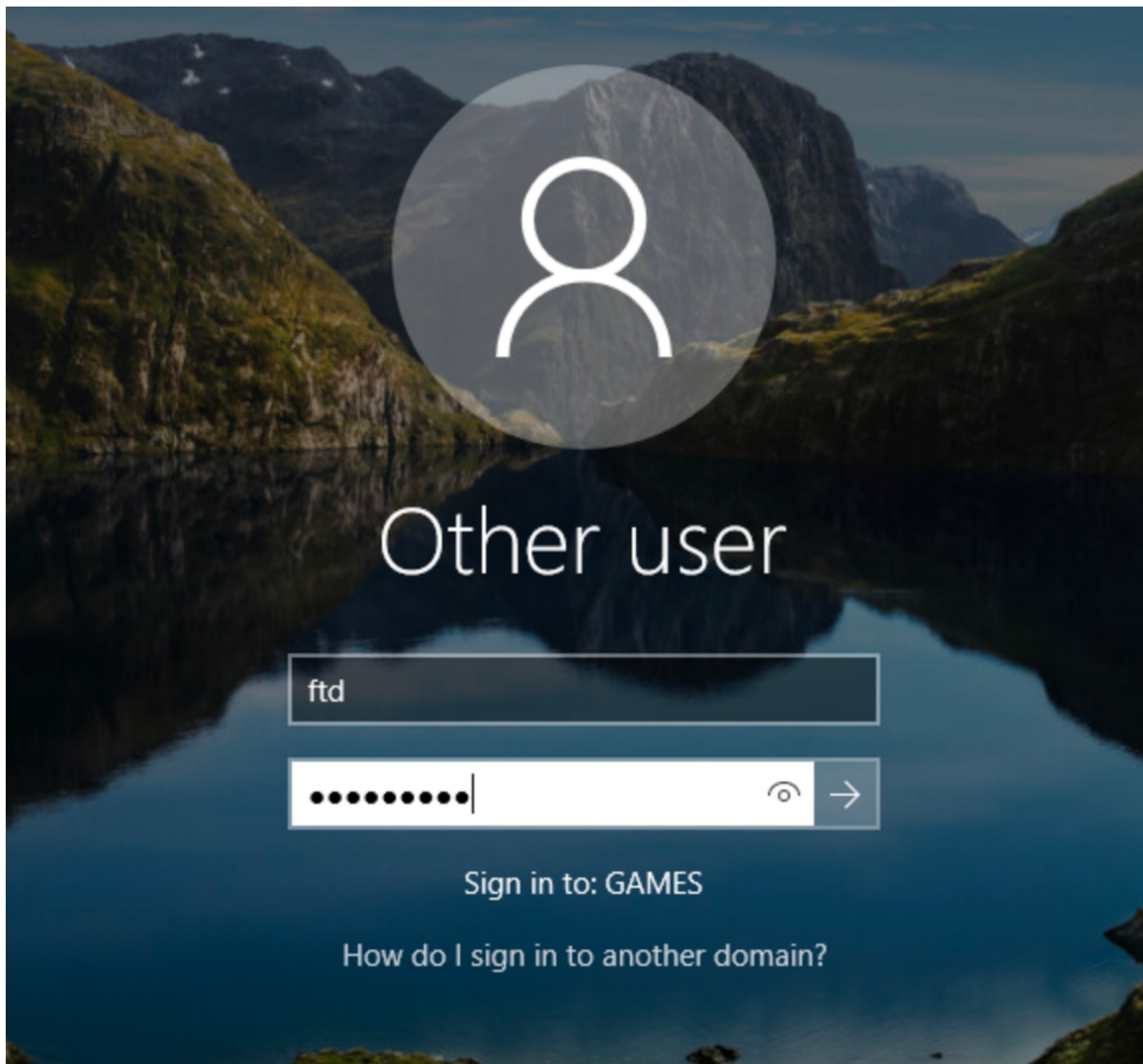
啟用記錄

儲存並部署FTD上的組態。

驗證

通過確認允許流量專門用於ftd來驗證被動身份操作。

從使用者電腦登入到域使用者。



使用者登入

使用者成功登入後，在Analysis> user >active session下從FMC進行驗證，以檢視活動使用者詳細資訊。

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	

活動會話

從連線事件啟動某些流量驗證後，請參閱連線事件中的使用者詳細資訊。

Connection Events (switch workflow)

No Search Constraints [\(Edit Search\)](#)

Connections with Application Details

Table View of Connection Events

II 2026-06-19 04:20:10 - 2026-06-19 05:20:22

Expanding

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		

活動會話

疑難排解

檢查代理日誌

在承載代理的Windows電腦上，開啟任務管理器，並驗證後台進程CiscoPassiveIdentityAgentServiceis是否正在運行。

Task Manager

File Options View

Processes Performance Users Details Services

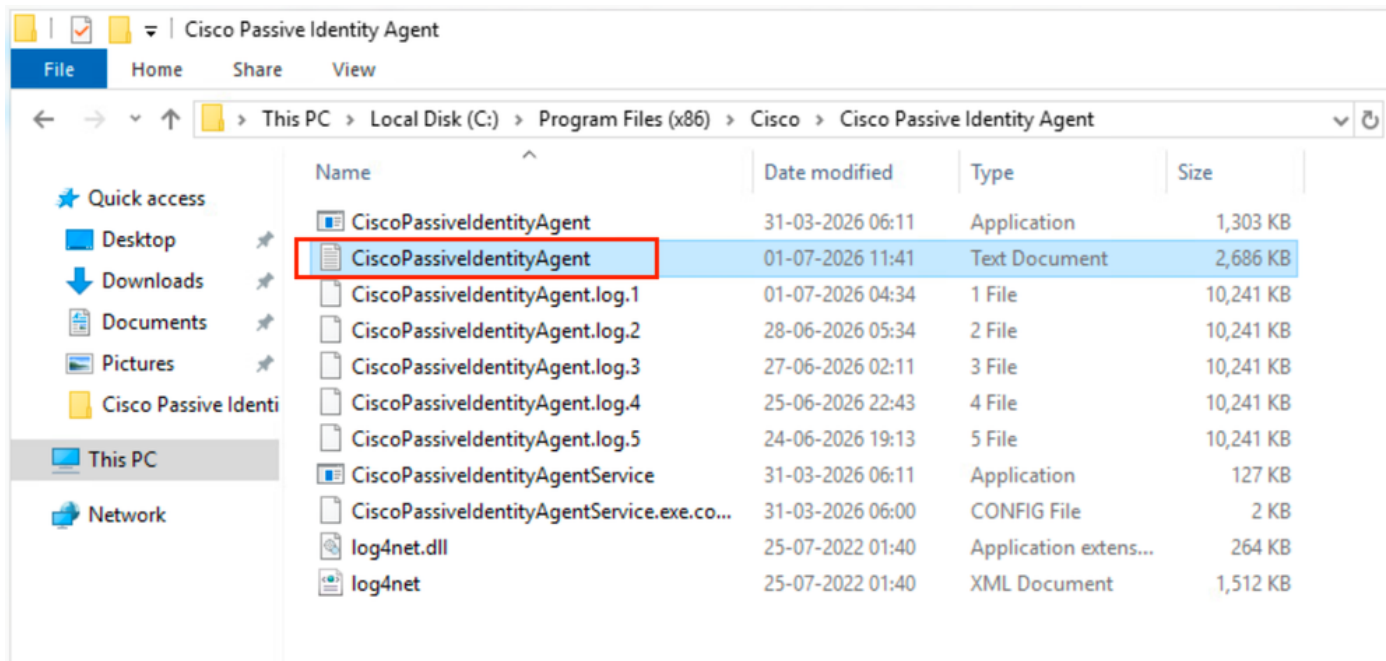
Name	Status	2% CPU	27% Memory
> Task Manager		0%	24.4 MB
> Windows Explorer		0%	37.3 MB
> Server Manager		0%	34.1 MB
Background processes (32)			
> Distributed File System Replicati...		0%	8.3 MB
▼ CiscoPassiveIdentityAgentServi...		0%	15.4 MB
Cisco Passive Identity Agent			
> Microsoft.ActiveDirectory.WebS...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

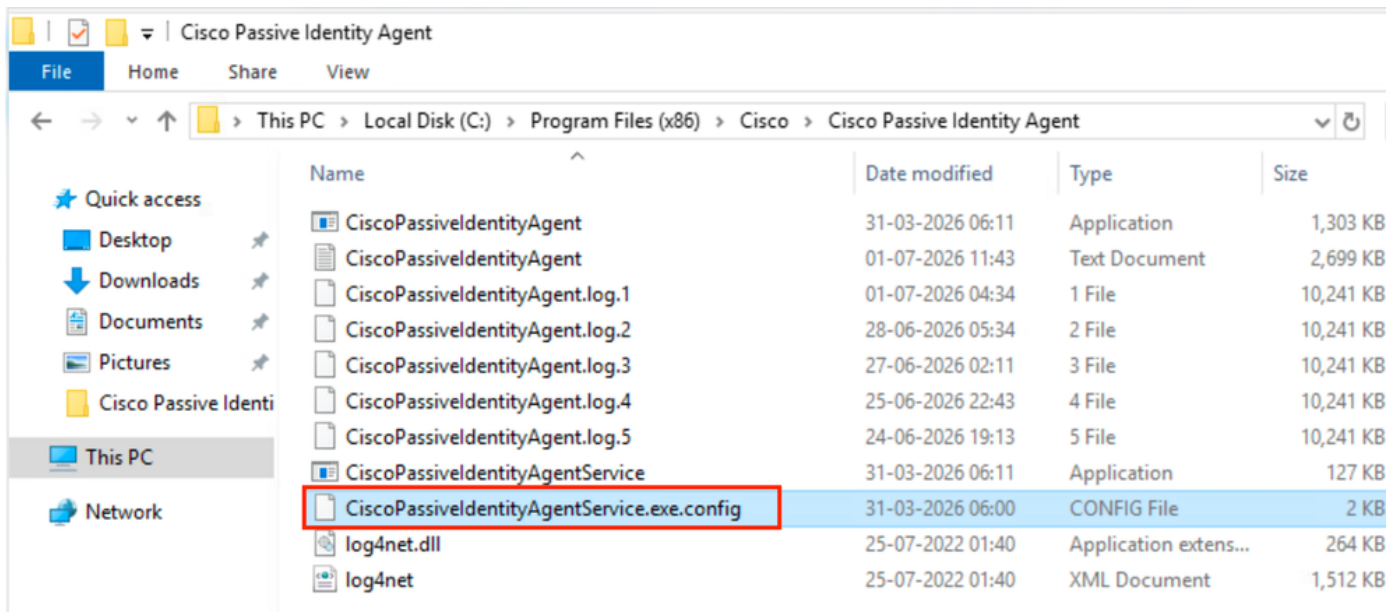
正在運行任務

可以在CiscoPassiveIdentityAgent檔案中找到代理日誌，預設位置為："C:\Program Files(x86)\Cisco\Cisco Passive Identity Agent\"。



代理

預設情況下，代理日誌設定為INFO level。要啟用DEBUG級別日誌記錄，請修改 CiscoPassiveIdentityAgentService.exe.config 並將日誌記錄級別設置為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>
```

資訊日誌

檢查代理日誌 — 獲取代理配置。

INFO Rest客戶端，批次事件：[{"domain":"games.cisco.com", "srcIpAddress":"X.X.X.X", "使用者":"fdm", "timestamp": "2026-07-01T19

INFO Rest客戶端，對映狀態：確定

INFO Rest客戶端，使用者Batch fdm的REST發佈成功，延遲= 0，當前DC時間(UTC):07/01/2026 19:47:34登入使用者

INFO Rest客戶端，請求代理配置

FMC日誌

運行此命令，檢視是否已從代理接收到使用者到IP的對映。

```

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輸出

如果上述命令未顯示任何對應，請收集這些日誌並與Cisco TAC聯絡。

這是FMC API的相關日誌清單。豬尾日誌包含所有這些資訊。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。