

Configure the Passive Identity Agent Using FMC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configurations](#)

[Configuring a Passive Identity Agent Source](#)

[Creating a Passive Identity Agent User on the Secure Firewall Management Center](#)

[Install and Configure the Passive Identity Agent software](#)

[Configure Identity Policies](#)

[Configure Access Control Policies](#)

[Verification](#)

[Troubleshooting](#)

[Checking Agent Logs](#)

[FMC Logs](#)

Introduction

This document describes how to configure the passive identity agent Source which sends session data to FMC

Prerequisites

Requirements

- Cisco Secure Firewall Management Center running version 7.6+
- Cisco Secure Firewall running version 7.6+
- Windows Active Directory server, the server must run Windows Server 2008 or later.
- You must enable Snort 3 on the Secure Firewall Threat Defense devices.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Management Center 7.6.5
- Cisco Secure Firewall 7.6.5

- Microsoft Active Directory running on Windows Server 2022.

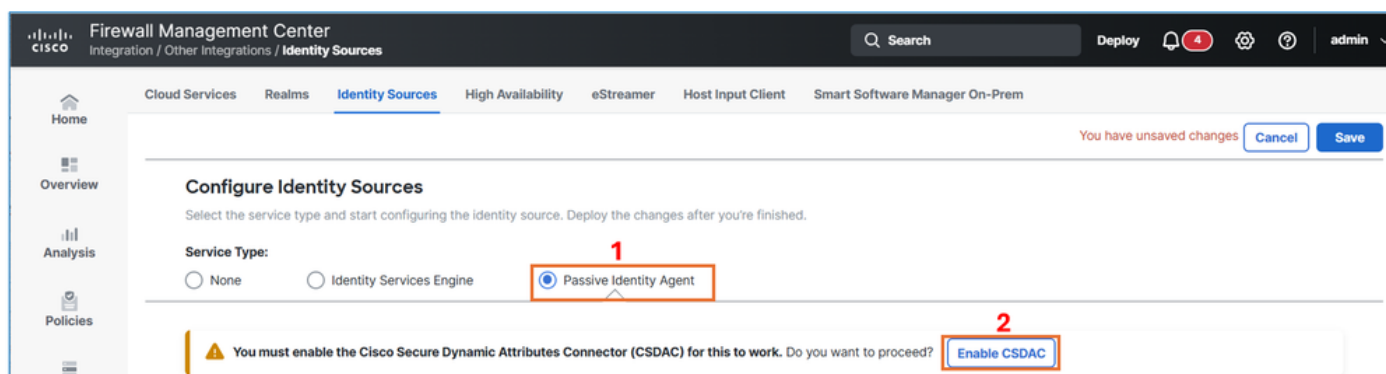
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configurations

Before configuring the agent, please complete the AD and FMC integration.

Configuring a Passive Identity Agent Source

In the FMC UI, navigate to **Integration > Other Integrations > Identity Sources**, click **Passive Identity Agent**. If the Cisco Secure Dynamic Attributes Connector has not been enabled yet, you are prompted to do so by clicking **Enable CSDAC**.



Passive Identity Agent

Click the **Enable** button to enable the CSDAC.

Enable Cisco Secure Dynamic Attributes Connector?



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

Cancel

Enable

Enable CSDAC

This step takes approximately 10 minutes. Once the CSDAC is properly enabled, click the **Done** button to proceed.

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 Enabled

Click the **Create Agent** button.

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[Primary Agent / Secondary 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

Create agent

Define a **name** for the agent, select the **Standalone** option, and associate it with the appropriate **Domain Controller** created in the previous task.

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

Configure agent

Click the **Save** button.

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.

Search by agent name or domain controller name Create Agent

Domain Controllers	Monitoring Agents	Hostname	Connection Status
LAB-Realm			

Save the configuration

The result.

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	LAB-Agent (standalone)	Not Applicable	

Verify the status



Note: The passive identity agent indicates status using lines, amber means that the agent has never successfully communicated with the Secure Firewall Management Center. A newly created agent line is amber and remains so until configuration is complete.

Creating a Passive Identity Agent User on the Secure Firewall Management Center

Create a Secure Firewall Management Center user with sufficient permissions to communicate with

the passive identity agent. This user has limited privileges to perform other tasks; the user is expected only to enable communication with the passive identity agent.

In the FMC UI, navigate to **System > Users** and click **Create User**. Fill in the **user details** according to the task requirements.

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

Create user

Assign the **Passive Identity User** role only. Click the **Save** button.

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
		☒
Custom User Roles	☐	REST VDI

Cancel

Save

select the passive identity user

Install and Configure the Passive Identity Agent software

Install and configure the Passive Identity Agent software on the designated Domain Controller.

Download the passive identity agent from 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

[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	Download Cart File
Installer for the Cisco Passive Identity Agent CiscoPassiveIdentityAgentInstaller-1.1.msi Advisories	11-Mar-2025	2.16 MB	Download Cart File

download the software

After downloading the agent, begin the **installation process** on the domain controller.

Downloads

File Home Share View

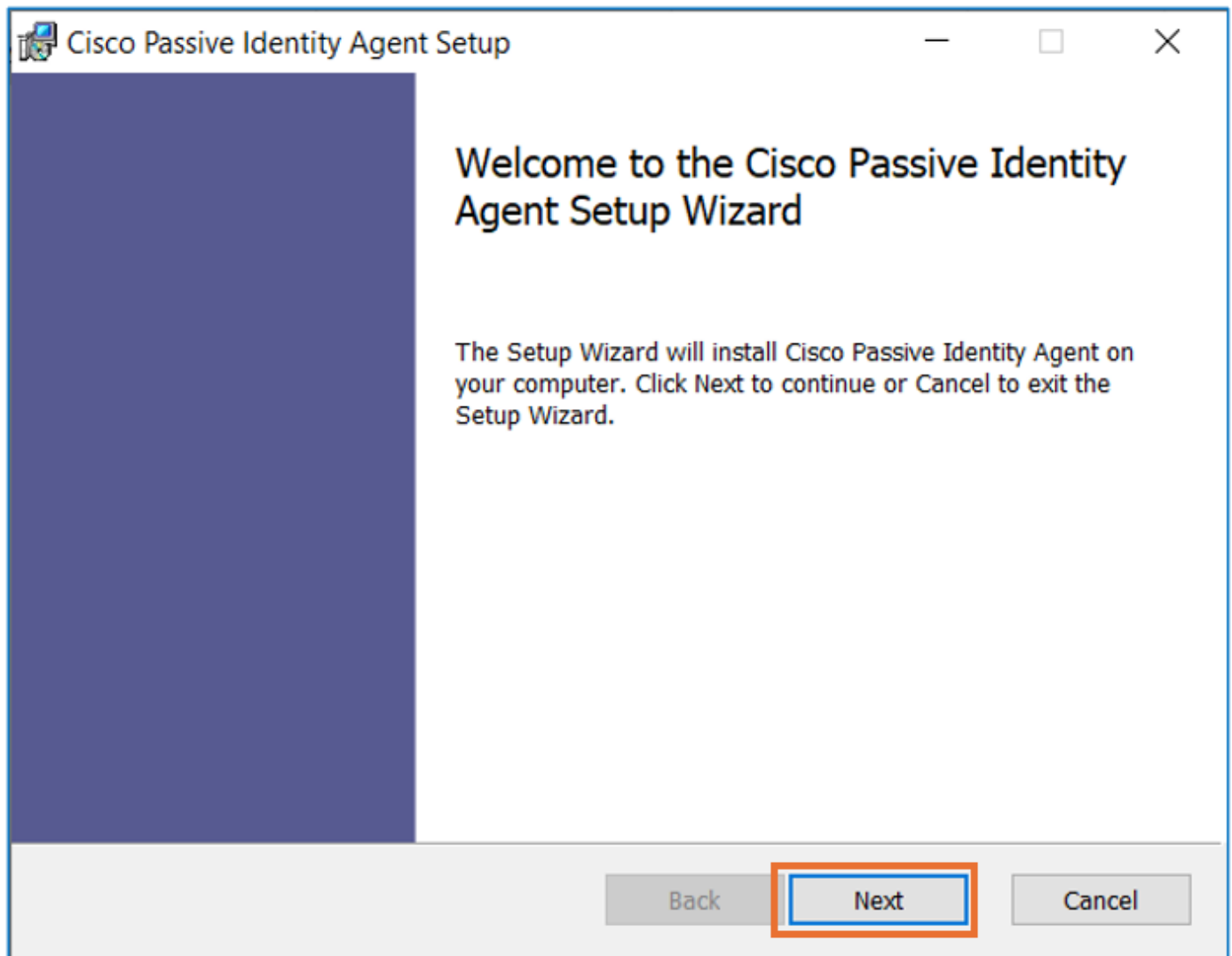
This PC > Downloads

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

agent

]

Refer to the provided installation instructions to complete the setup.



Install

Once the installation is complete, open the **Passive Identity Agent software** and enter the **required information** as specified in the task requirements. Click the **Test** button to verify connectivity with the 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

Primary FMC FQDN / IP address **Port**

:

FMC FQDN or IP address and Port of the FMC

Username **Password**

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

configure the agent.

After successfully testing the connectivity, click the **Save** button.

 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

test

Click the **OK** button to complete the agent configuration.

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

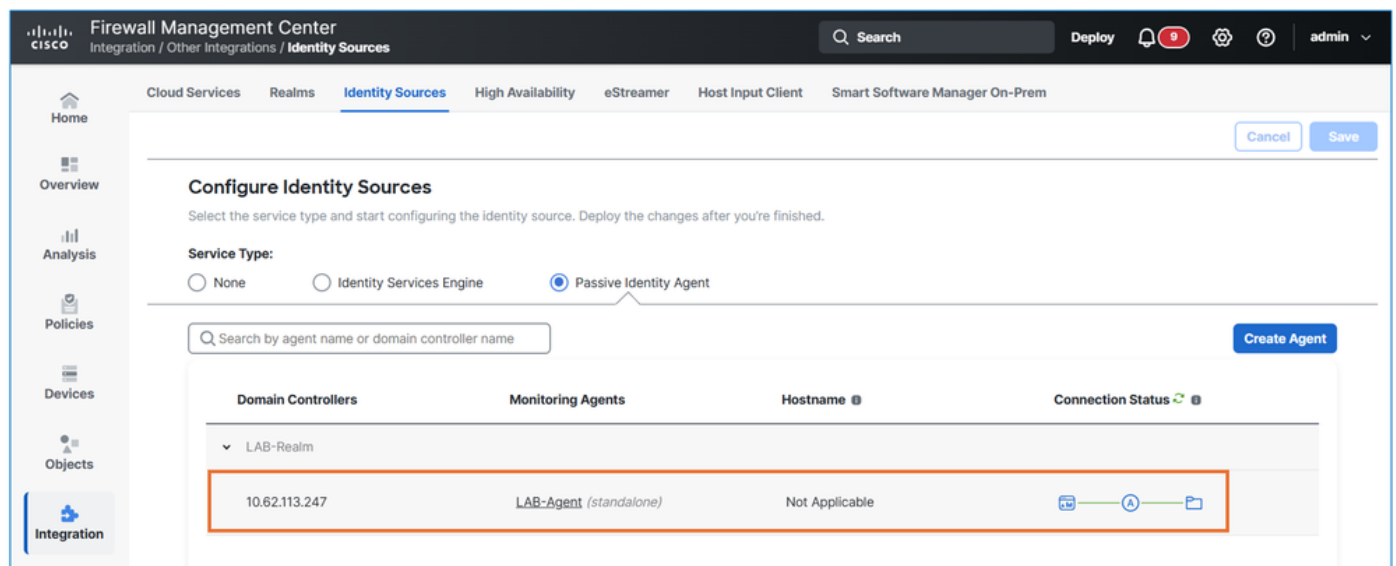
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

agent is running

In the FMC UI, navigate to **Integration > Other Integrations > Identity Sources > Passive Identity Agent**. Confirm that the Passive Identity Agent displays a green status.



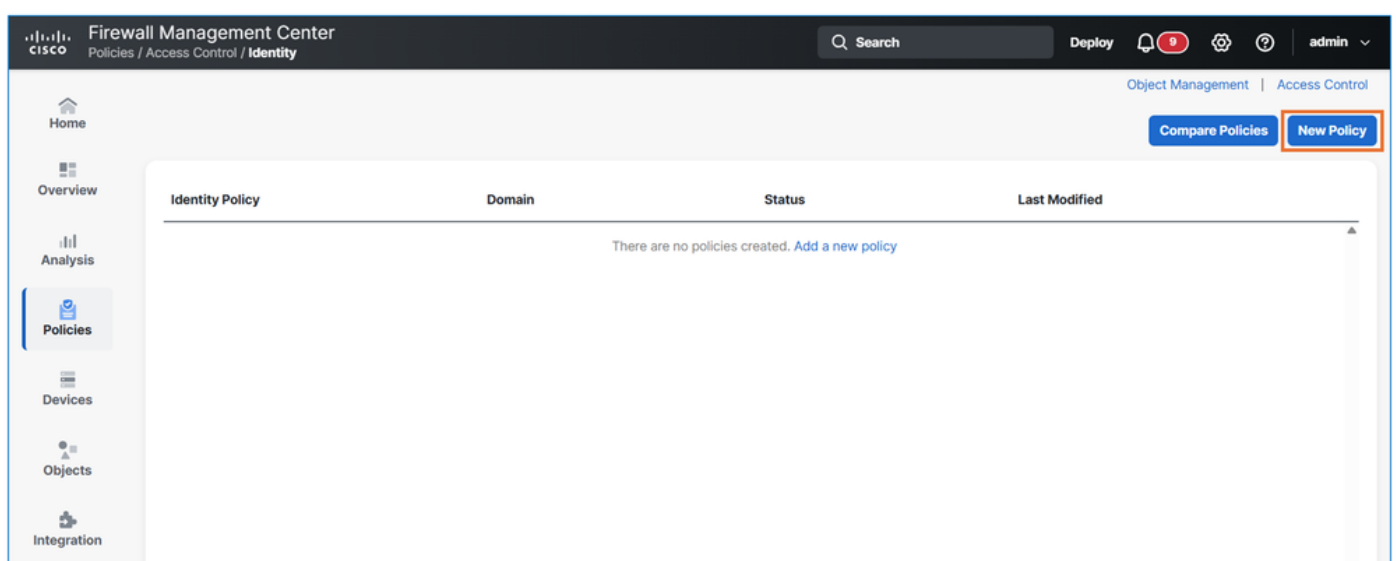
verify the communication from fmc

Configure Identity Policies

Create an Identity Policy based on the table provided.

Policy Name	Rule Name	Authentication Realm	Remaining settings
LAB-Identity-Policy	Rule1	LAB-Realm	Leave as default

In the FMC UI, navigate to **Policies > Access Control > Identity**. Click the **New Policy** button.



new policy

Enter the **policy name** according to the task requirements.

New Identity policy



Name

LAB-Identity-Policy

Description

Cancel

Save

new policy

Click the **Add Rule** button.

Firewall Management Center
Policies / Access Control / Identity Policy Editor

LAB-Identity-Policy

Enter Description

Rules Active Authentication Identity Source

+ Add Category + Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
This category is empty											
Root Rules											
This category is empty											

create rule

Navigate to the **Realm & Setting** tab and select the **Authentication Realm** based on the task requirements. Finally, click the **Add** button.

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 **Realm & Settings**

Authentication Realm *
LAB-Realm (AD)

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

Cancel **Add**

Realm setting

Click the **Save** button.

LAB-Identity-Policy

Enter Description

Rules Active Authentication Identity Source

You have unsaved changes **Save** Cancel

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	Rule1	any	any	any	any	any	any	any	LAB-Realm (AD)	Passive Authentication	none
Root Rules											
This category is empty											

save the config

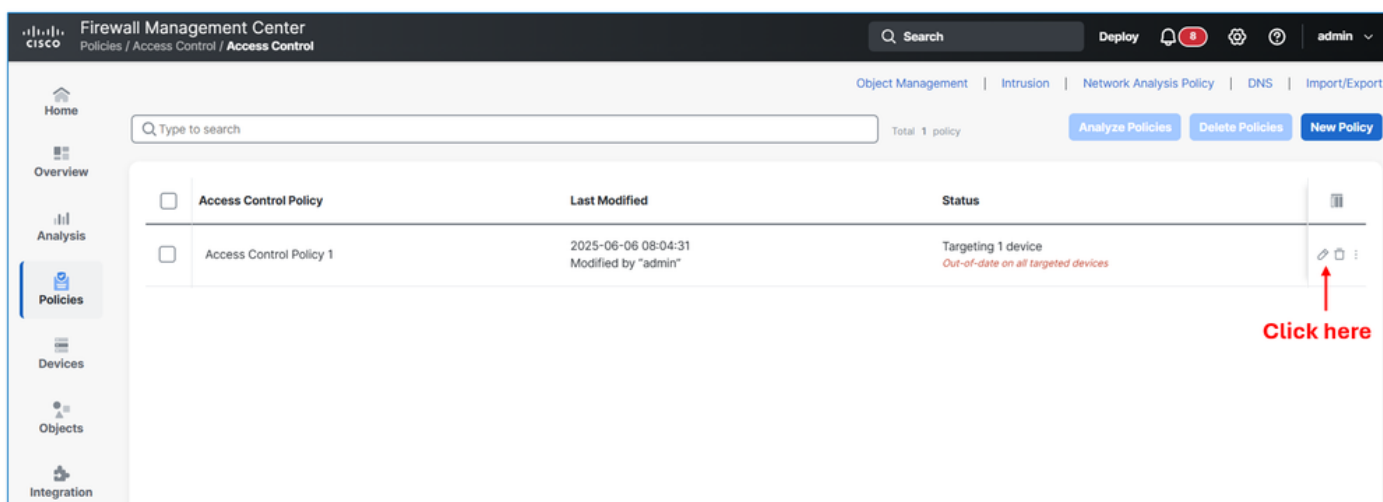
Configure Access Control Policies

Link the **Identity Policy** to the **Access Control Policy** and create an **Access Policy Rule** with the attributes:

Attribute name	Value
Rule name	Rule1
Action	Allow
Source Zone	Inside
Destination Zone	Outside
Source Networks	10.10.10.0/24
Destination Networks	10.48.62.98/32
Service	Dest Port TCP 80 (HTTP)
Users	LAB-Realm/GROUP1
Logging	At the End of Connection

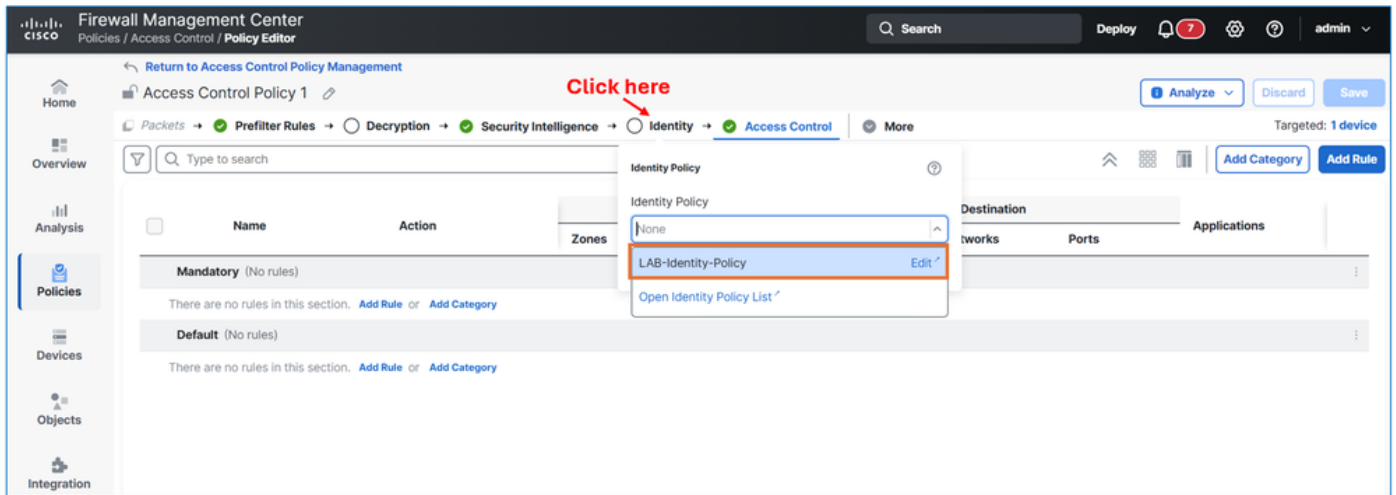
Step 1. Link the **Identity Policy** to the **Access Control Policy**

In the FMC UI, navigate to **Policies > Access Control > Access Control**. Click the **Edit** button for your policy.



Edit policy

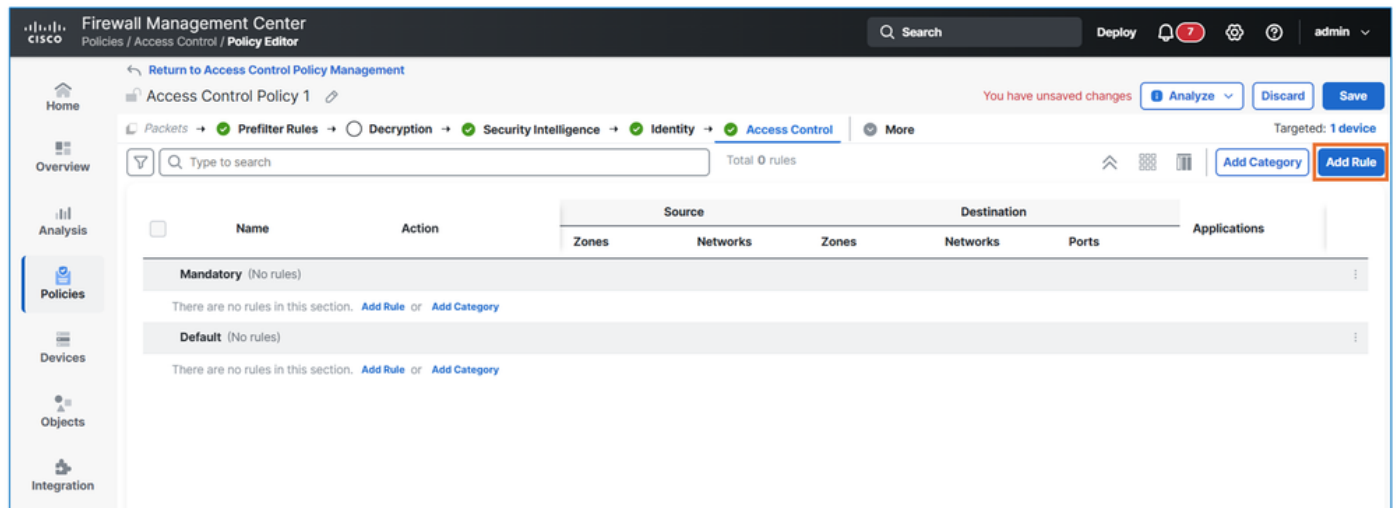
Navigate to the **Identity** section and link the **Identity Policy** created in the previous task.



add identity policy

Click the **Apply** button

Step 2. Create the **Access Control Rule**.



create ACP

Enter the details according to the task requirements, and most importantly, under the **Userstab**, add **GROUP1** from **LAB-Realm**.

Add Rule

Name: Rule1

Action: Allow | Logging: OFF | Time Range: None | Rule Enabled: ON

Intrusion Policy: None | Variable Set: | File Policy: None

Insert: Into Mandatory

Tabs: Zones (2) | Networks (2) | Ports (1) | Applications | **Users (2)** | URLs | Dynamic Attributes | VLAN Tags

Search Users

Realms: Showing 2 | Selected 1

- ☒ LAB-Realm
- ☐ Special Identities

Clear Selections

Users: Total 1

- ☒ GROUP1 (User Group)
- ☐ user1 (Users)

Selected Sources: 2

- ZONE: 1 Object (inside)
- NET: 1 Object (obj-10.10.10.0)

Selected Destinations and Applications: 3

- ZONE: 1 Object (outside)
- NET: 1 Object (obj-10.48.62.98)
- PORT: 1 Object (HTTP)

Add User

Comments ^

Cancel | Apply and Add New Rule | Apply

add users in the rule

Enable logging for the rule by selecting **Log at end of connection**.

Add Rule

Name: Rule1

Action: Allow | Logging: ON | Time Range: None | Rule Enabled: ON

Intrusion Policy: None | File Policy: None

Insert: Into Mandatory

Tabs: Zones (2) | Networks (2) | Ports (1) | Applications | **Users (2)** | URLs | Dynamic Attributes | VLAN Tags

Search Users

Realms: Showing 2 | Selected 1

- ☒ LAB-Realm
- ☐ Special Identities

Users: Total 1

- ☐ GROUP1 (User Group)
- ☐ user1 (Users)

Selected Sources: 3

- ZONE: 1 Object (inside)
- NET: 1 Object (obj-10.10.10.0)
- USER: 1 Group (LAB-Realm)

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

Add User

Comments ^

Cancel | Apply and Add New Rule | Apply

enable logging

Step 3. Enable **logging** for the Default Action.

Click the **settings** icon to modify the **Default Action** logging settings.

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

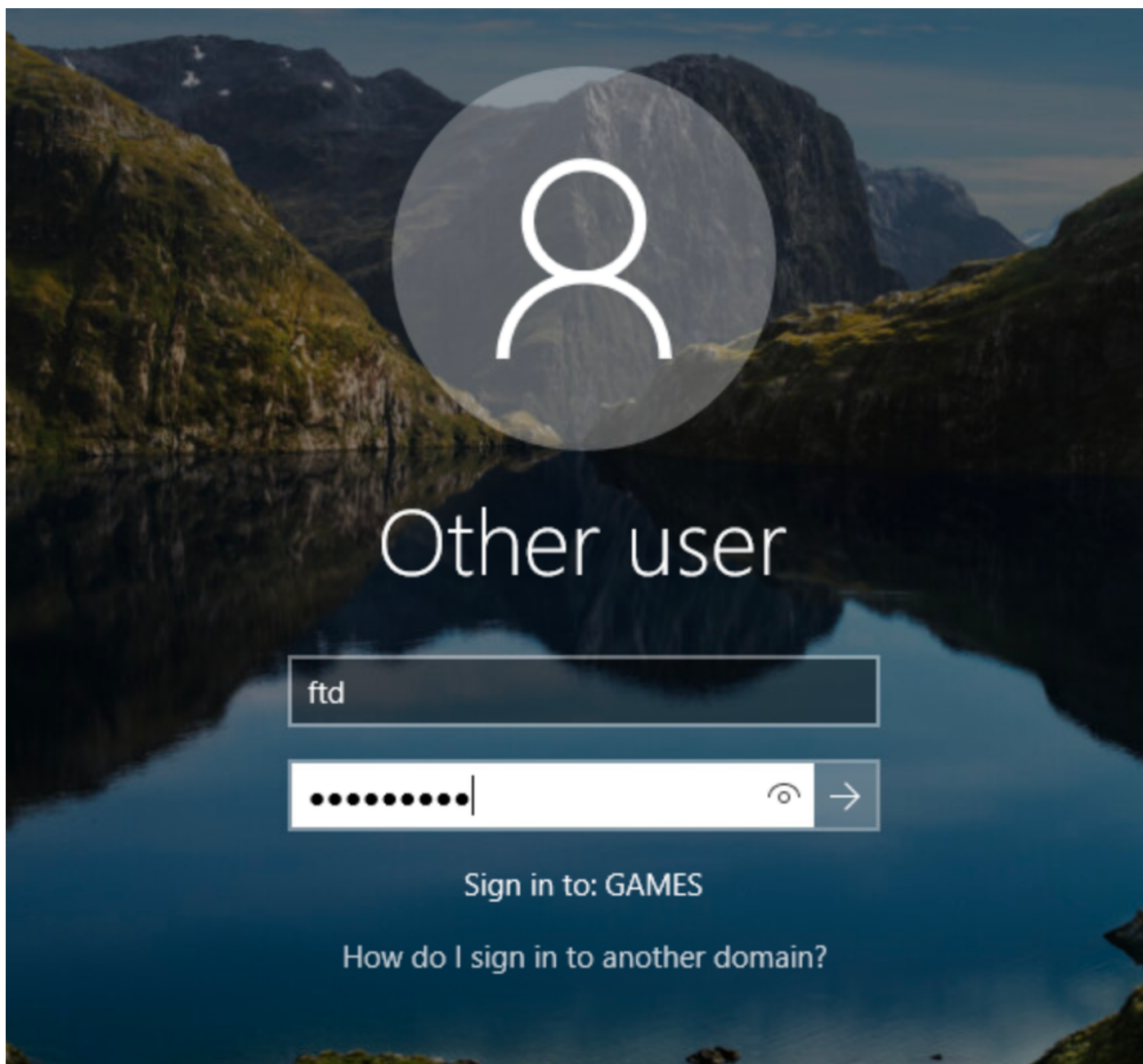
Enable logging

Save and **Deploy** the configuration on the FTD.

Verification

Verify the Passive Identity operation by confirming that traffic is allowed exclusively for ftd.

Log in to the **domain user** from the user machine.



user login

After a user successfully logs in, verify from FMC under **Analysis> user >active session to view the active user detail.**

▼ 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	

Active sessions

After initiating some traffic verification from the connection events, see the user details in the connection

events.

Connection Events (switch workflow)

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

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

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		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		

Active sessions

Troubleshooting

Checking Agent Logs

On the Windows machine hosting the Agent, open **Task Manager** and verify that the background process **CiscoPassiveIdentityAgentService** is running.

Task Manager

File Options View

Processes Performance Users Details Services

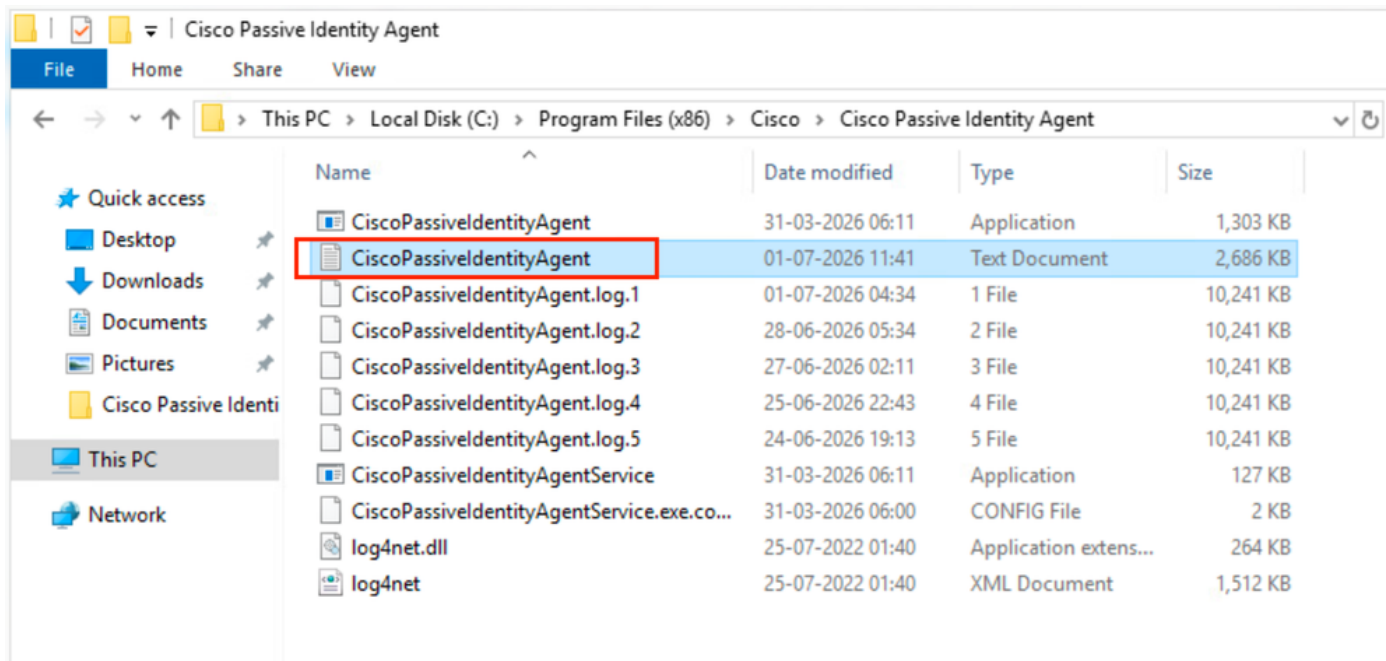
Name	Status	2% CPU	27% Memory
> Task Manager		0%	24.4 MB
> Windows Explorer		0%	37.3 MB
> Server Manager		0%	34.1 MB
Background processes (32)			
> Distributed File System Replicati...		0%	8.3 MB
▼ CiscoPassiveIdentityAgentServi...		0%	15.4 MB
Cisco Passive Identity Agent		0%	15.4 MB
> Microsoft.ActiveDirectory.WebS...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

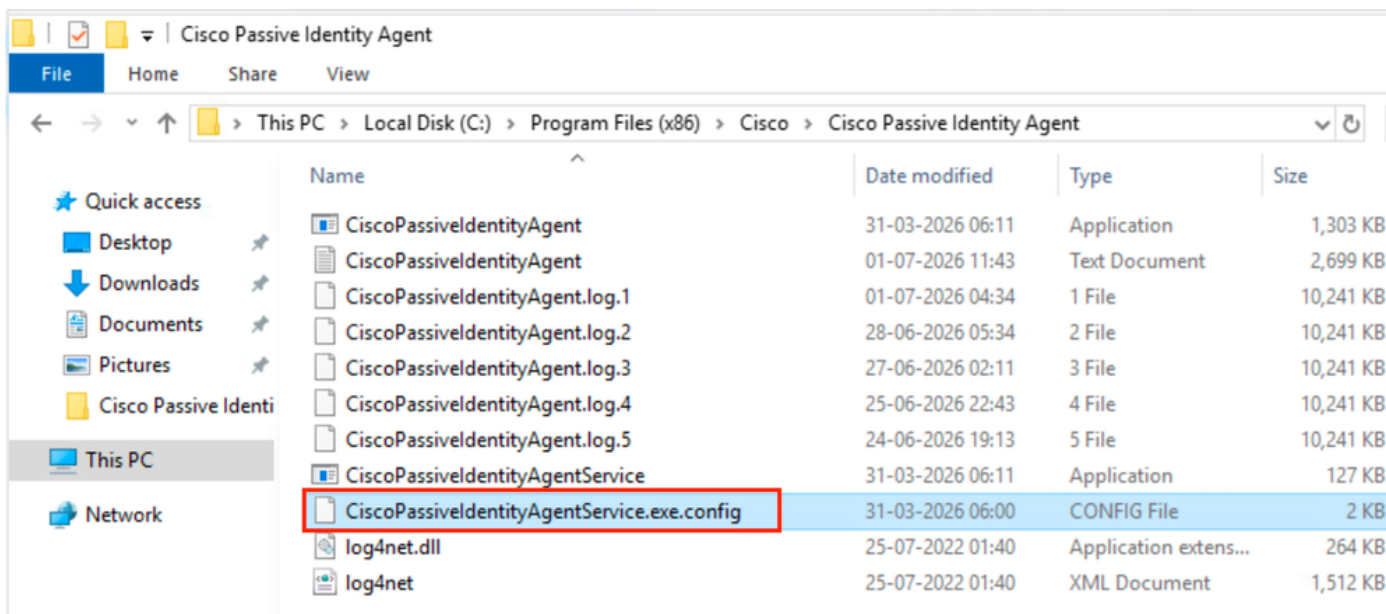
Running task

Agent logs can be found in the CiscoPassiveIdentityAgent files, located by default at: "C:\Program Files (x86)\Cisco\Cisco Passive Identity Agent".



agent

By default, the Agent logs are set to the **INFO** level. To enable **DEBUG** level logging, modify the **CiscoPassiveIdentityAgentService.exe.config** file and set the logging level to either **ALL** or **DEBUG**.



agent config

info log

Checking Agent Logs – Fetch Agent Configuration.

INFO Rest Client, Bulk Events: [{"domain": "games.cisco.com", "srcIpAddress": "X.X.X.X", "user": "fdm", "timestamp": "2026-07-01T19

INFO Rest Client, Mapping Status: OK

INFO Rest Client, REST post successful for userBatch fdm, latency = 0, current DC TIME in UTC: 07/01/2026 19:47:34 USER logged at

INFO Rest Client, Requesting agent configuration

FMC Logs

Run this command to see if the user-to-IP mapping has been received from the agent.

```

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 output

If the previous command does not show any mapping, collect these logs and contact Cisco TAC.

This is a list of relevant logs for the FMC API. Thepigtail log encompasses all of them.

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