# Configure the Passive Identity Agent Using FMC

## Contents



## 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.

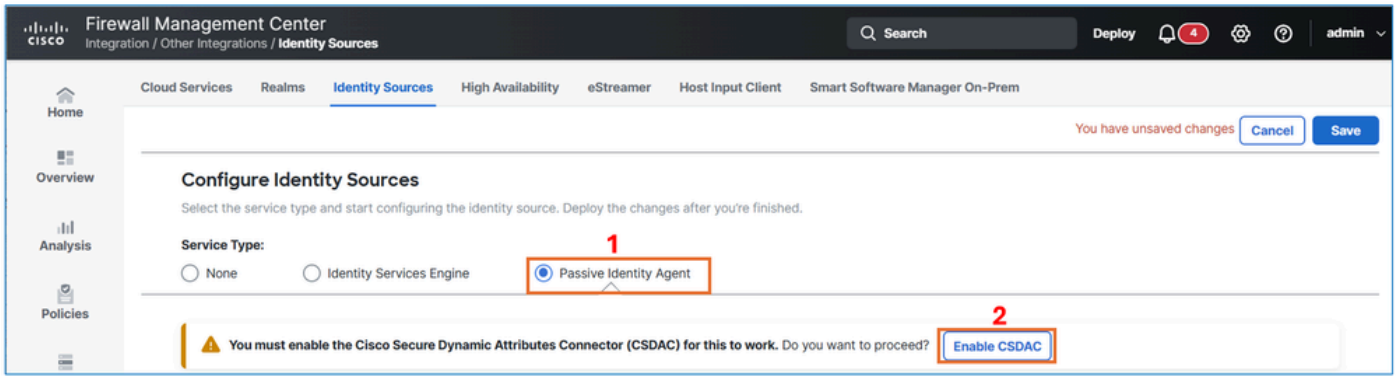
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Configurations

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

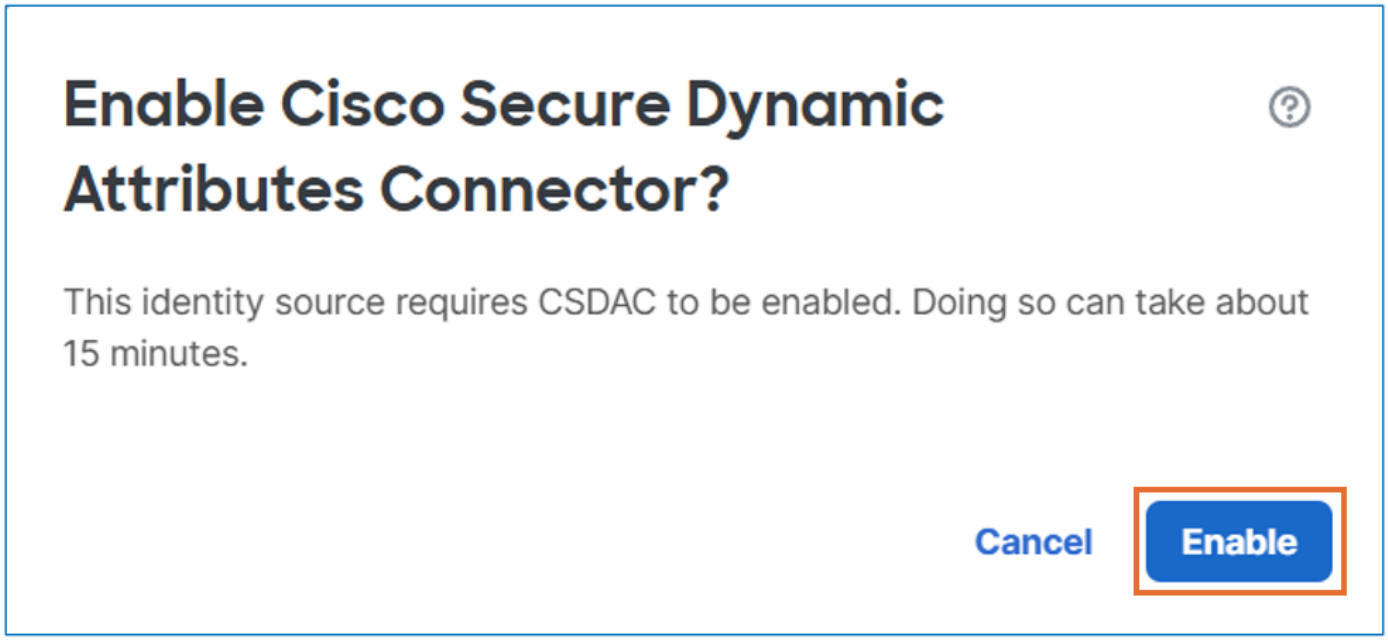
## Configuring a Passive Identity Agent Source

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**.



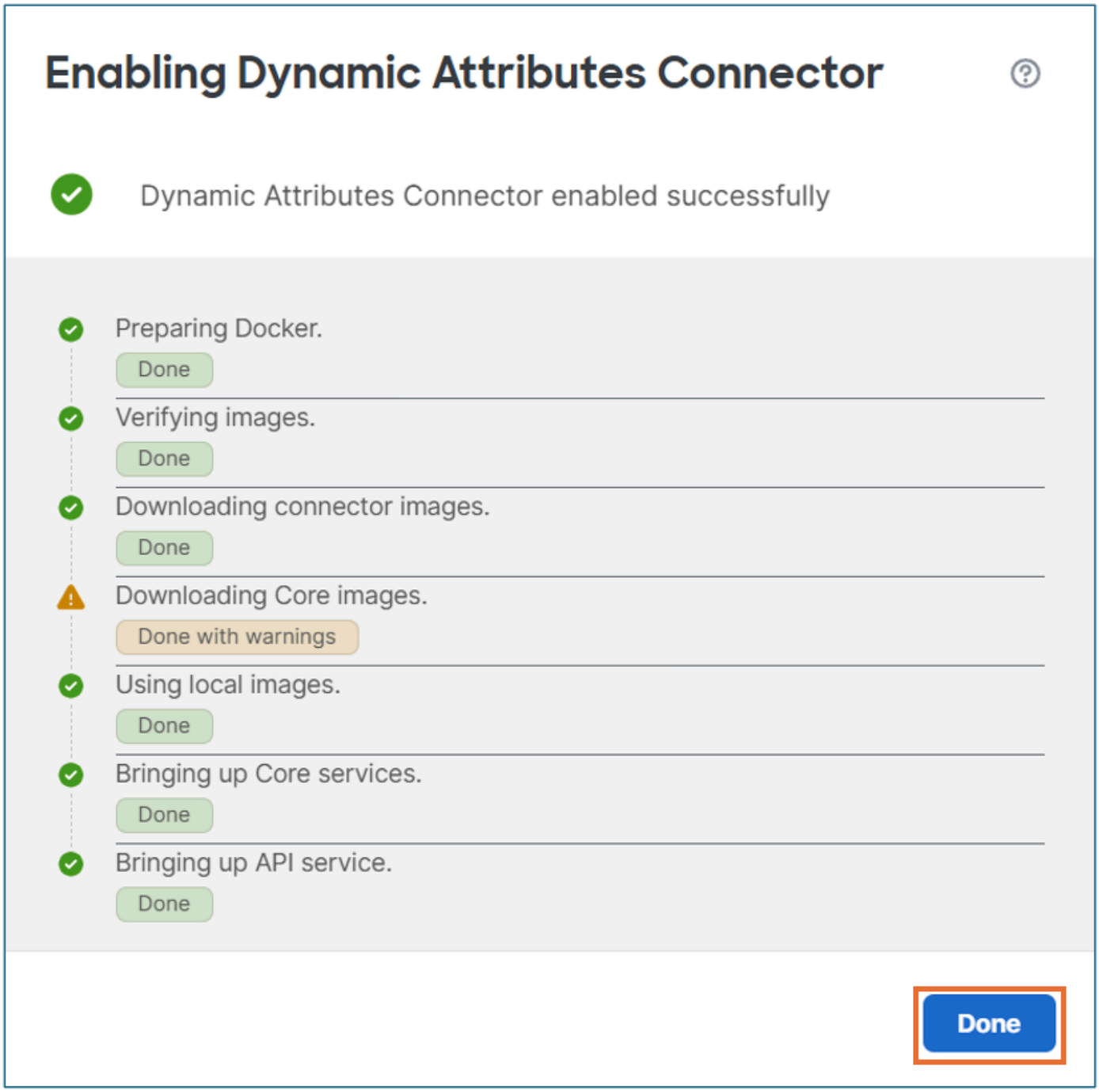

*Passive Identity Agent*

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



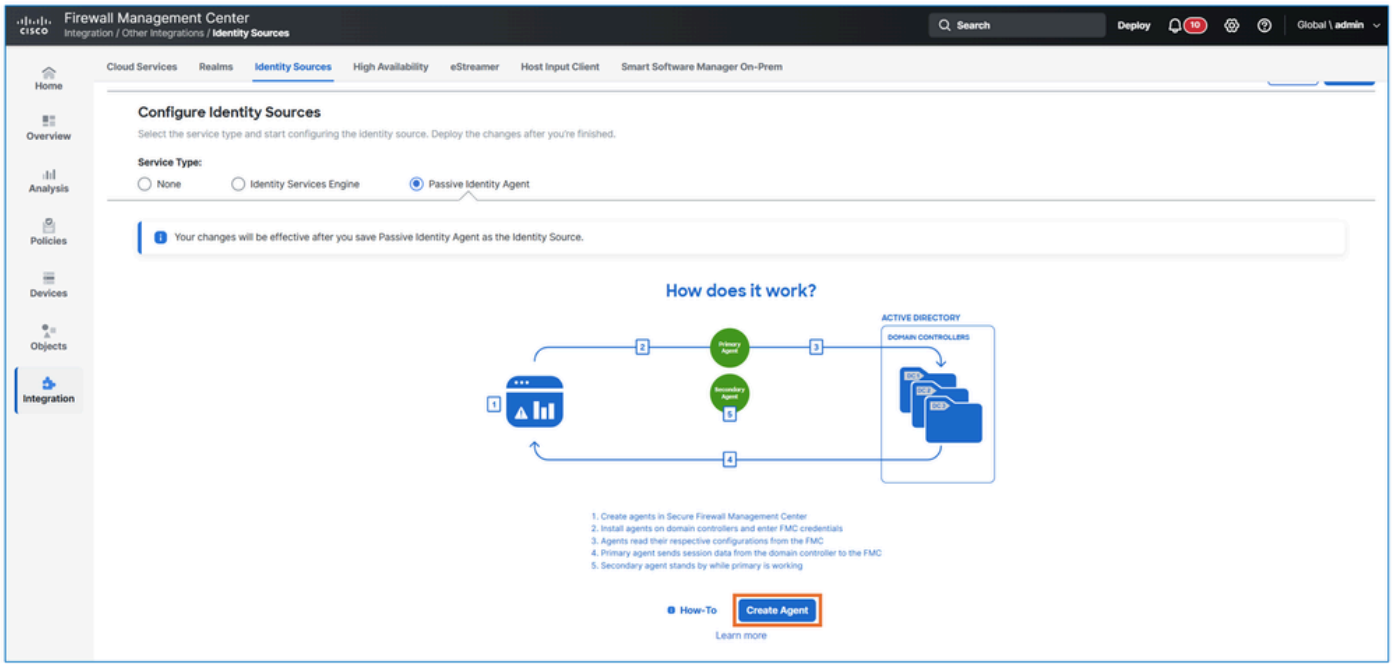

*Enable CSDAC*

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



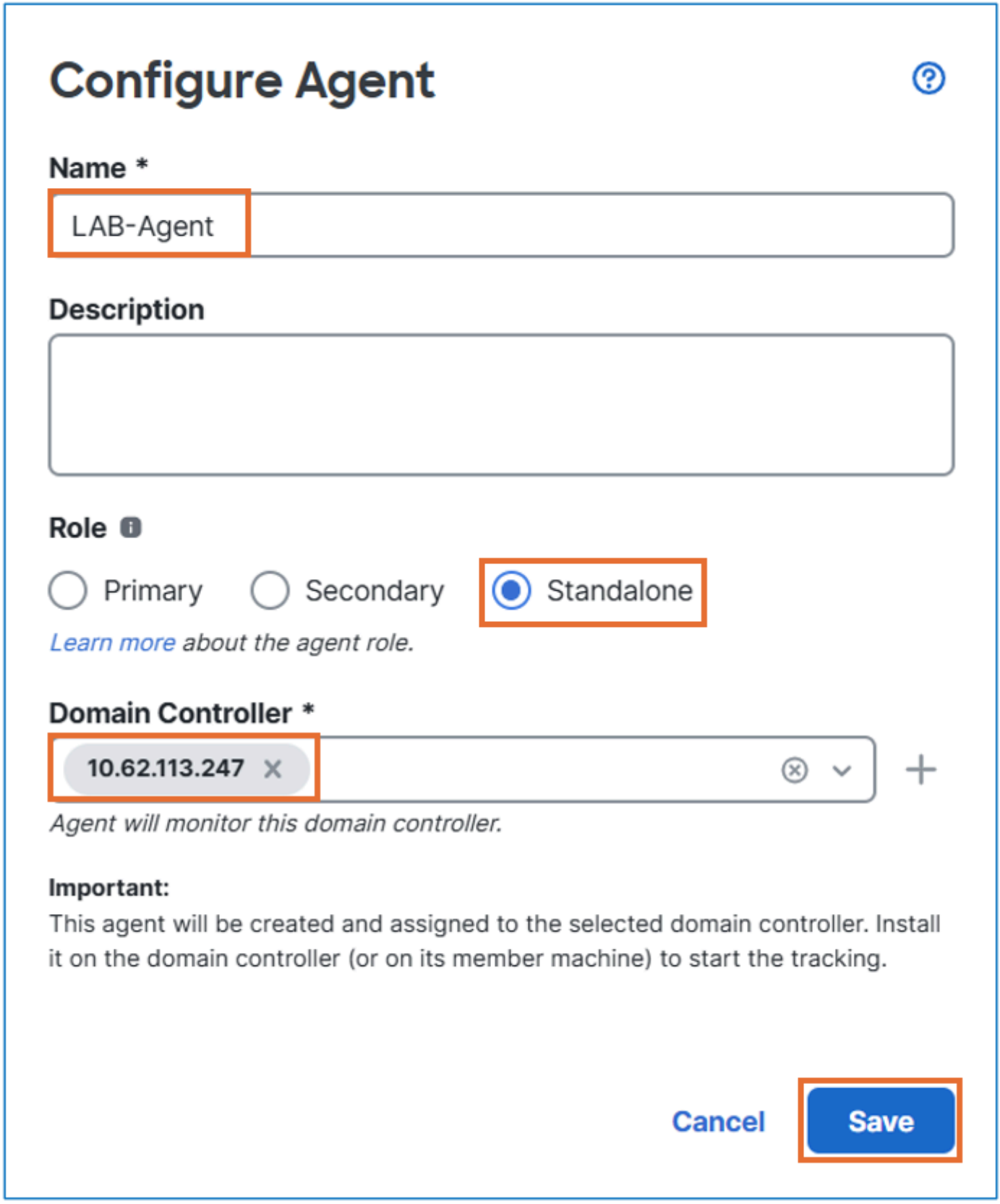

*CSDAC Enabled*

Click the**Create Agent**button.



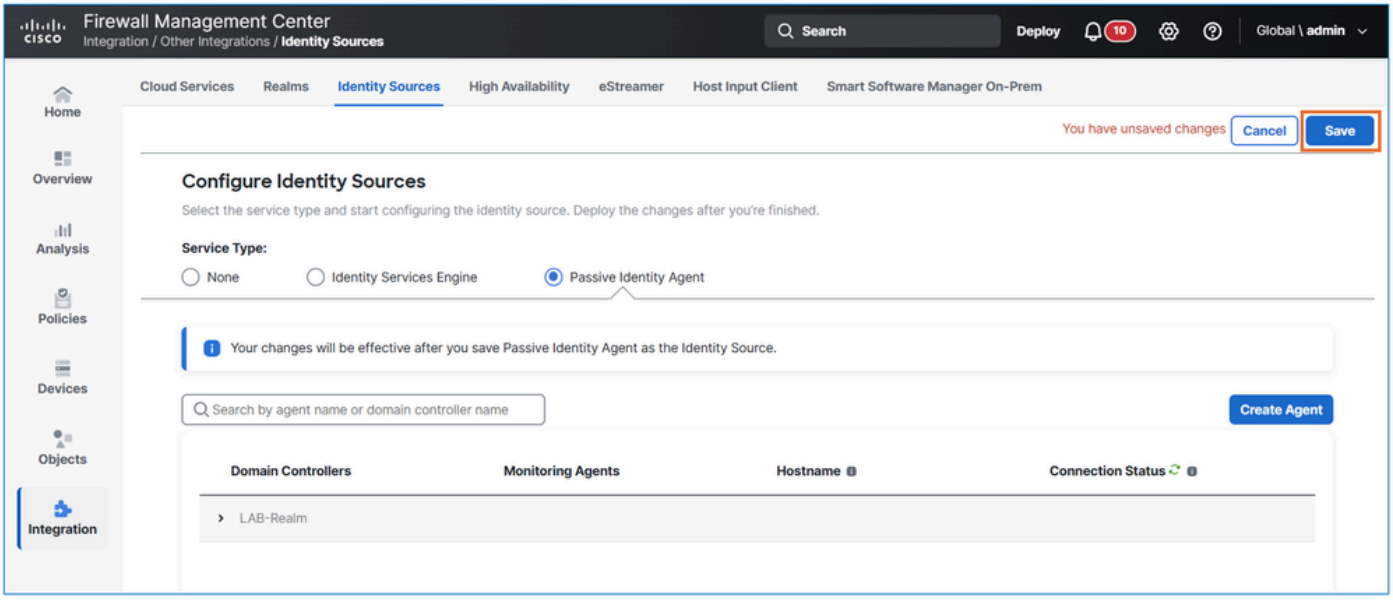

*Create agent*

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



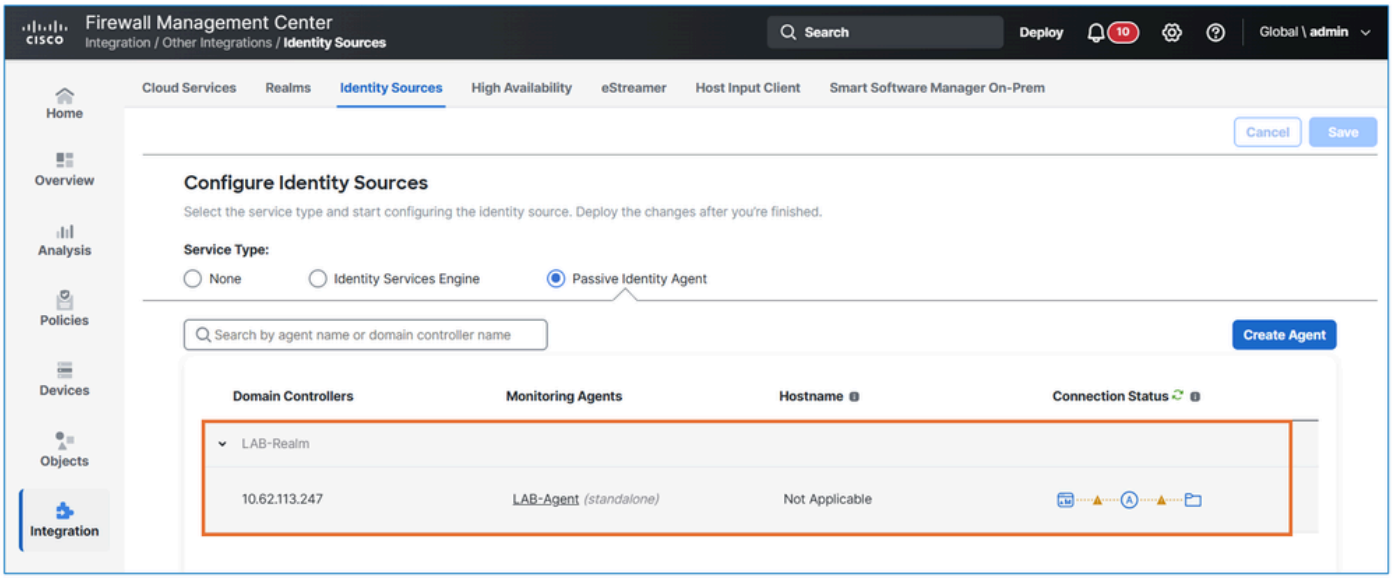

*Configure agent*

Click the**Save**button.




*Save the configuration*

The result.




*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.

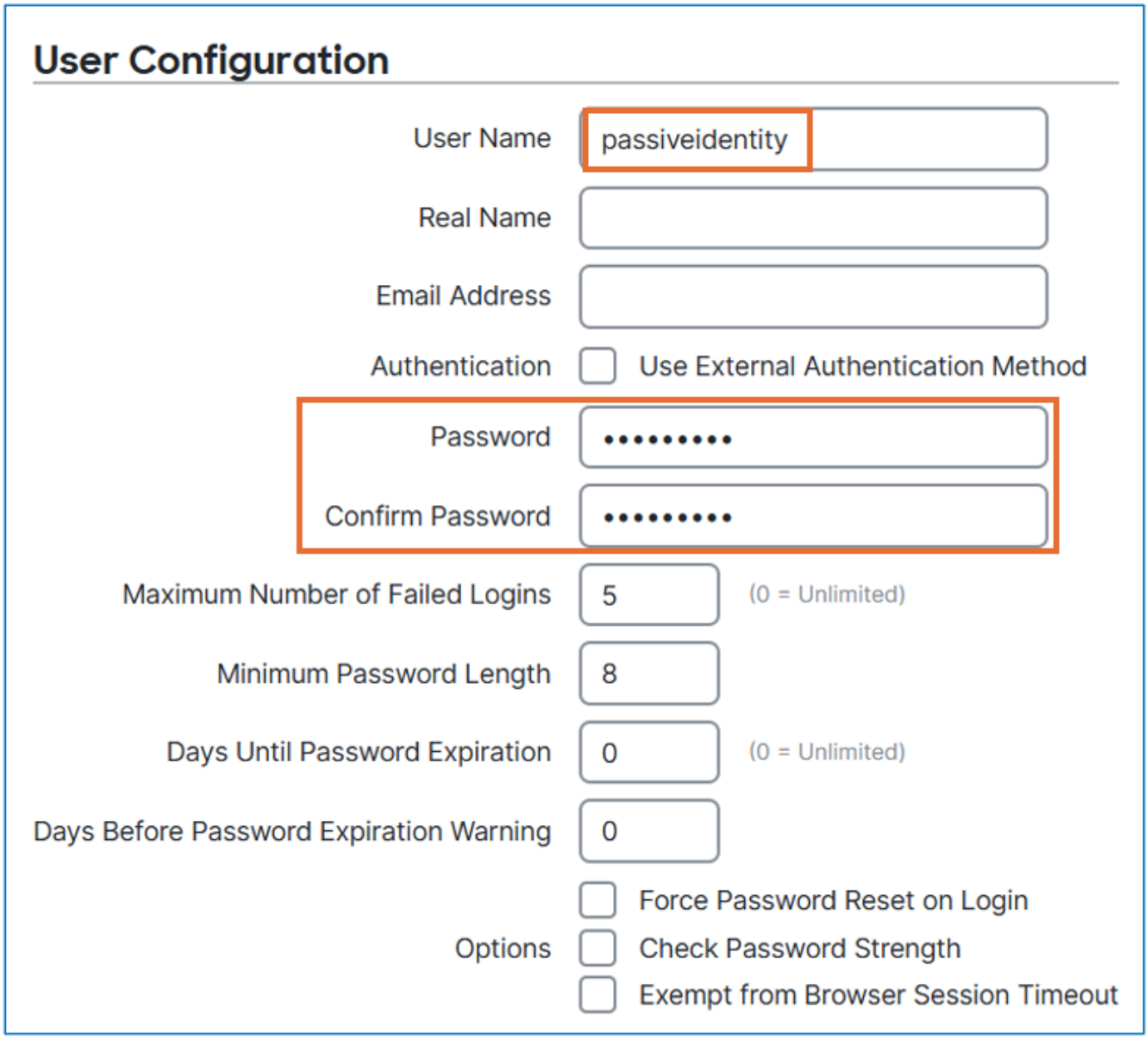
---

## 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

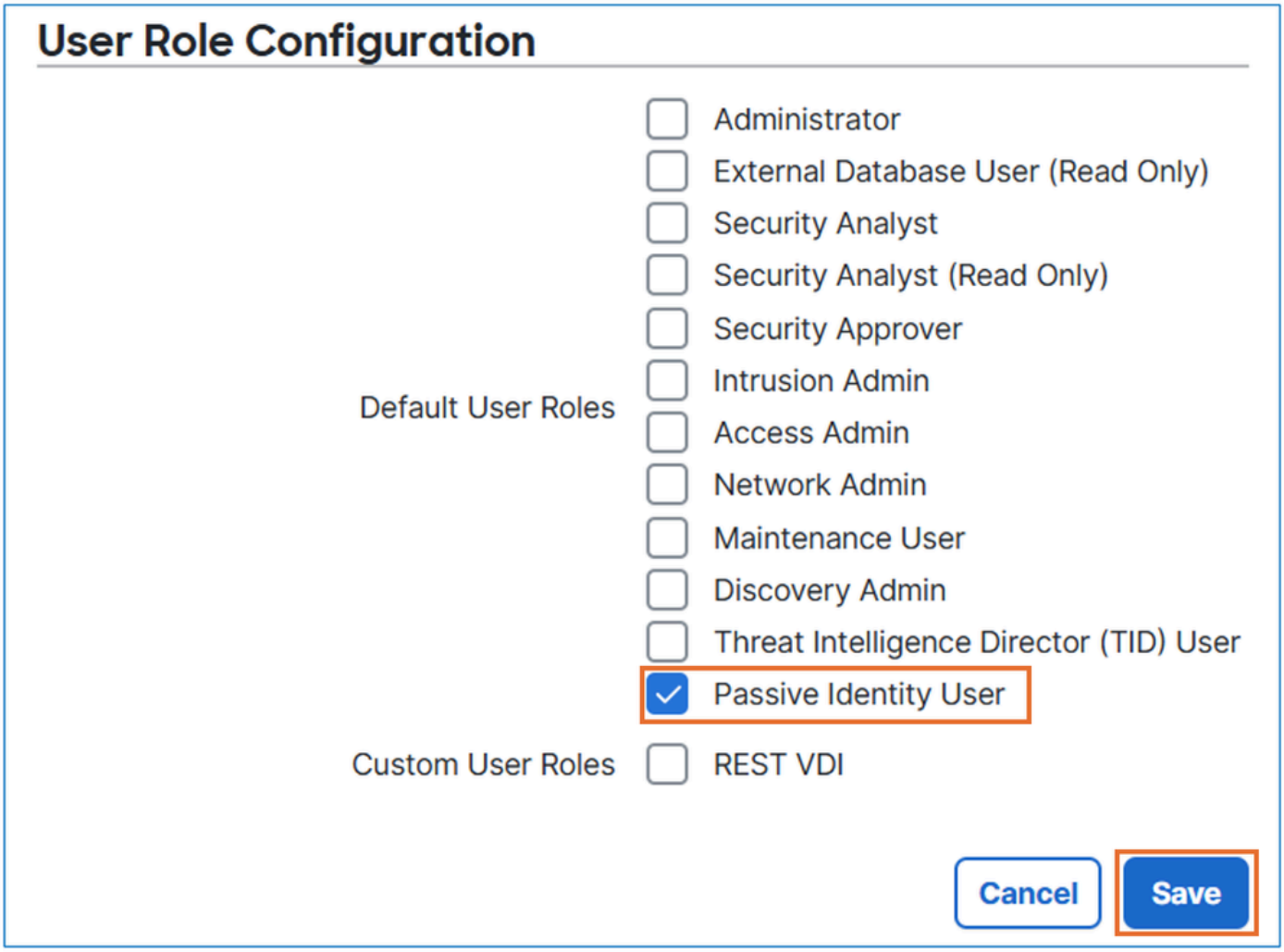
the passive identity agent. This user has limited privileges to perform other tasks; the user is expected only to enable communication with the passive identity agent.

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




*Create user*

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

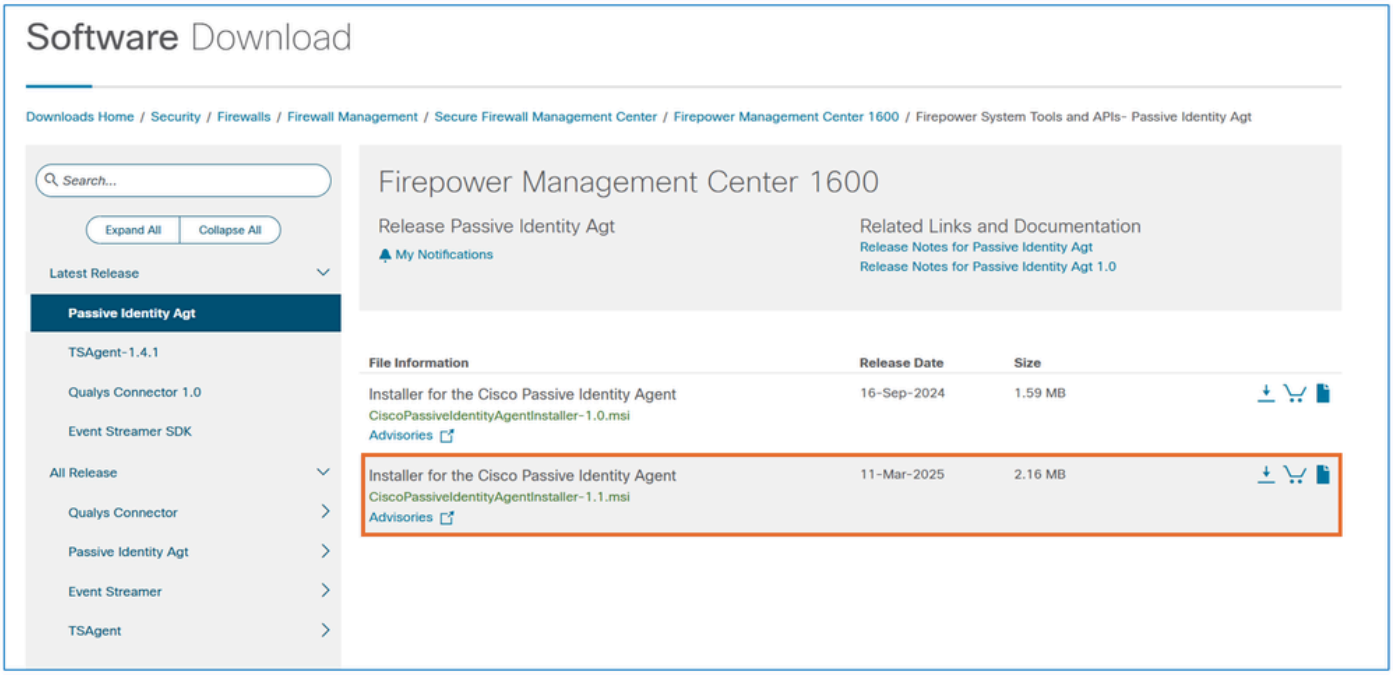



*select the passive identity user*

## Install and Configure the Passive Identity Agent software

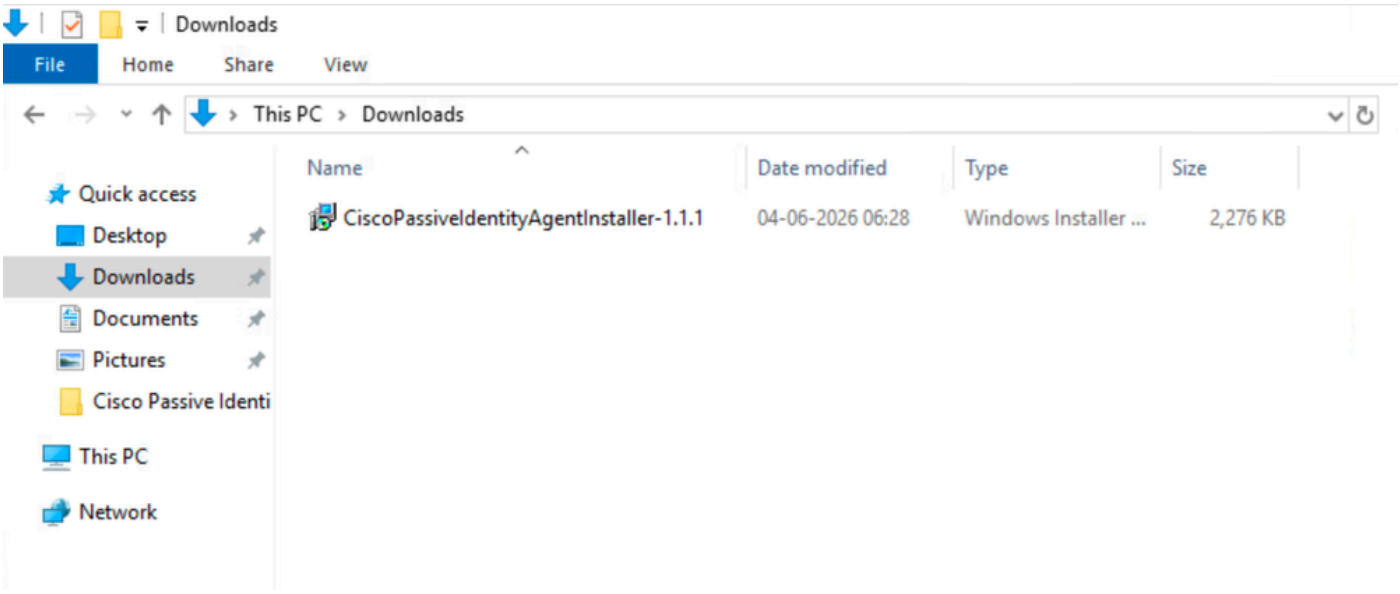
Install and configure the Passive Identity Agent software on the designated Domain Controller.

Download the passive identity agent from [software.cisco.com](software.cisco.com).




*download the software*

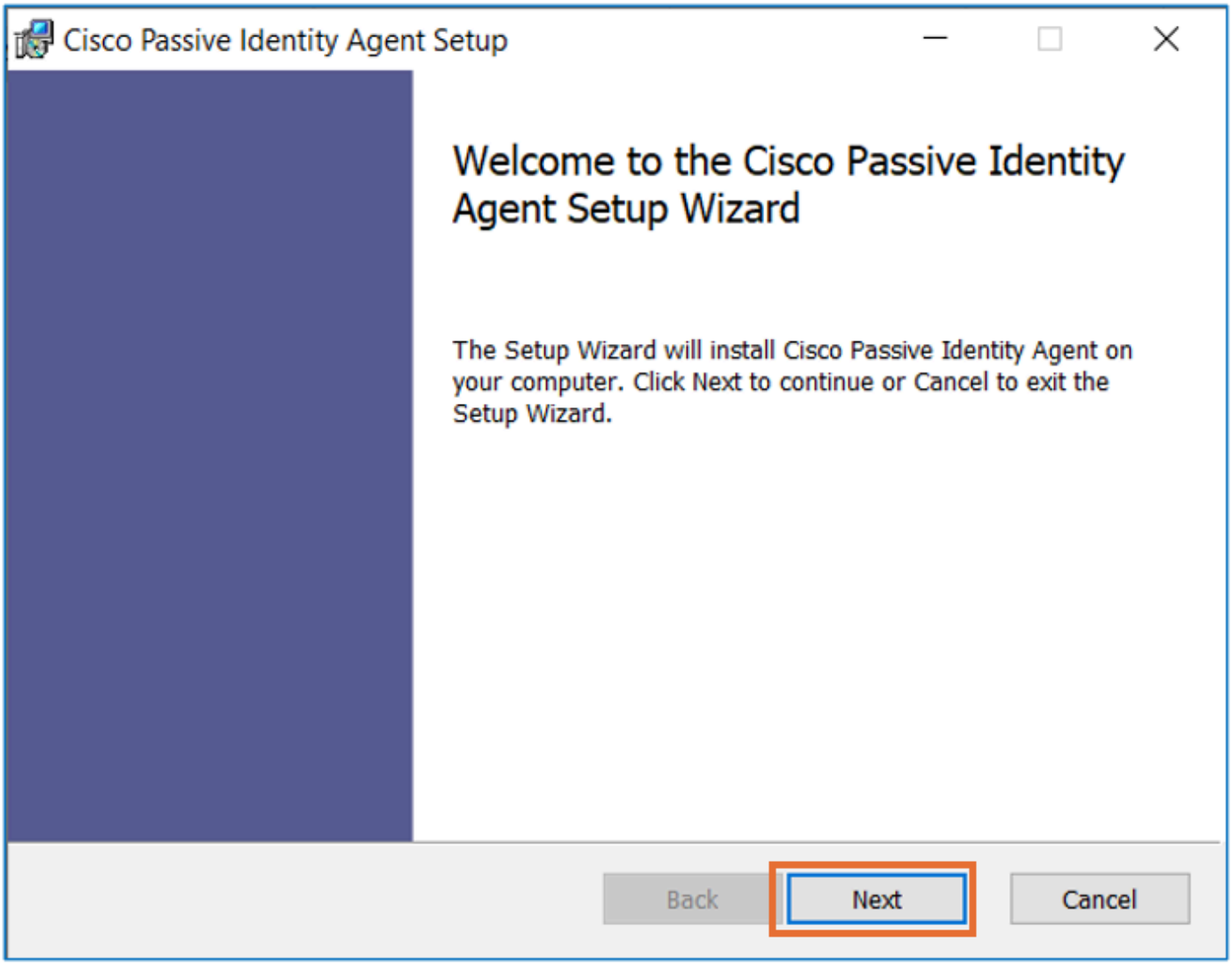
After downloading the agent, begin the **installation process** on the domain controller.




*agent*

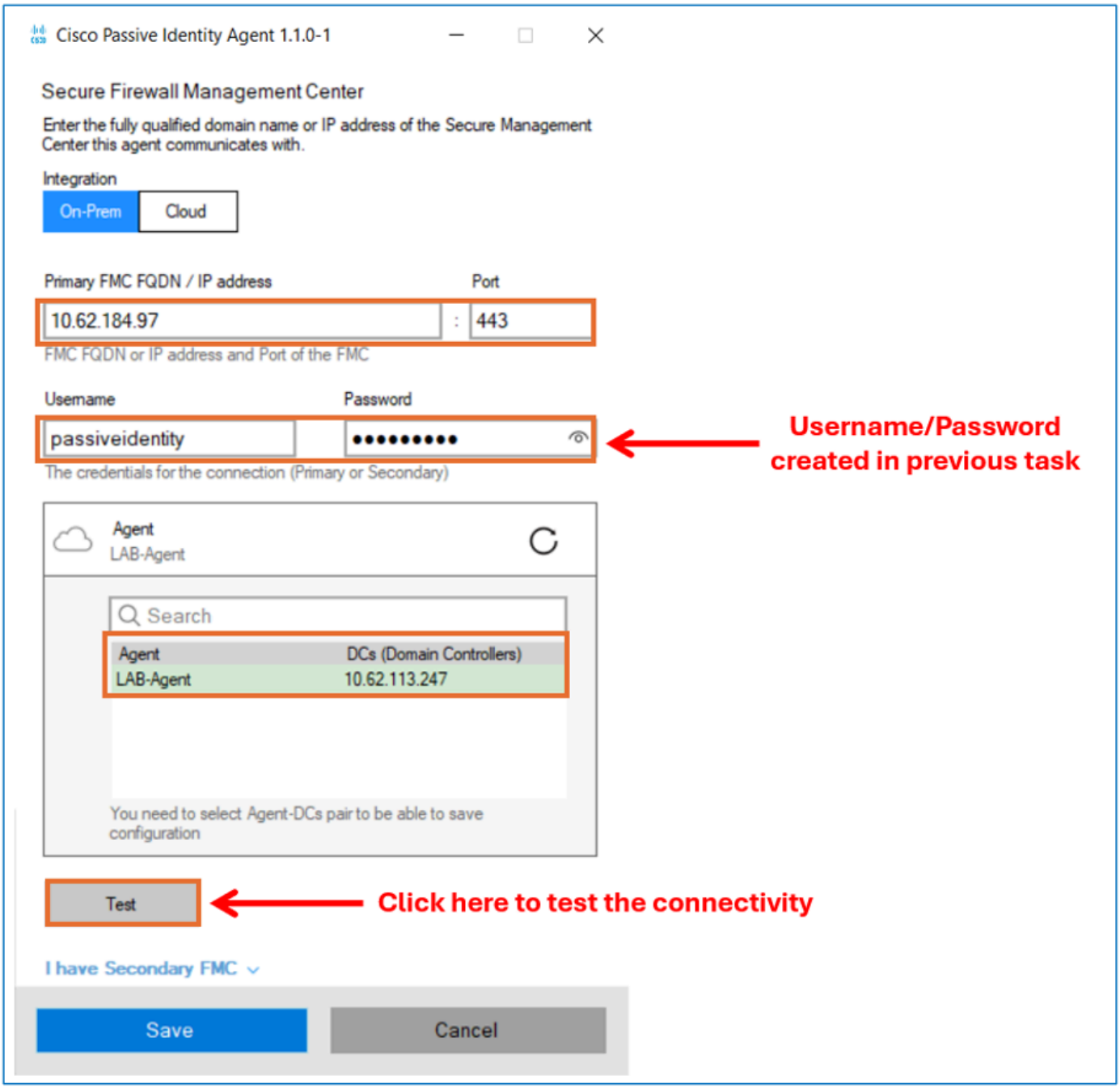
]

Refer to the provided installation instructions to complete the setup.



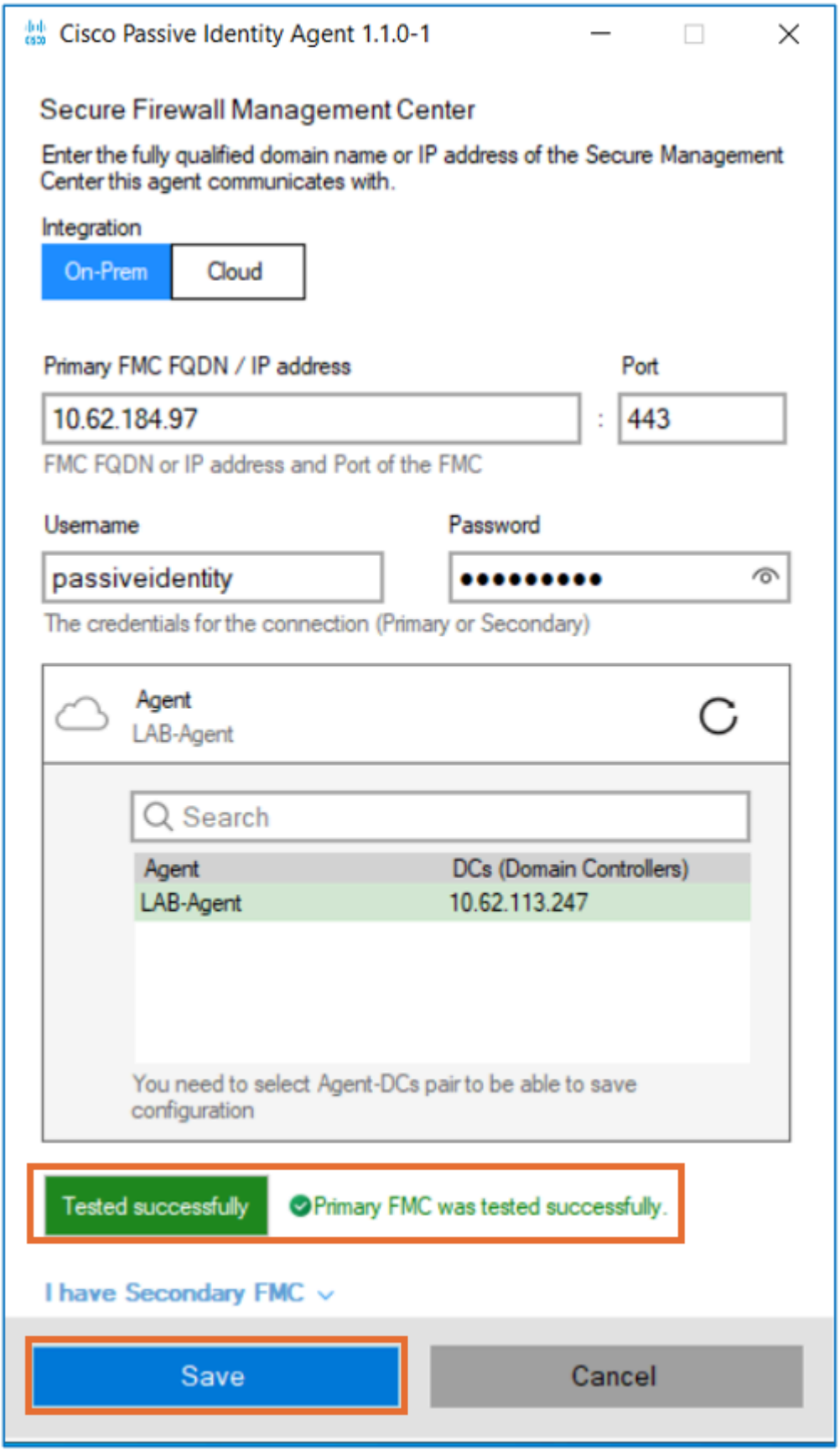

*Install*

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.



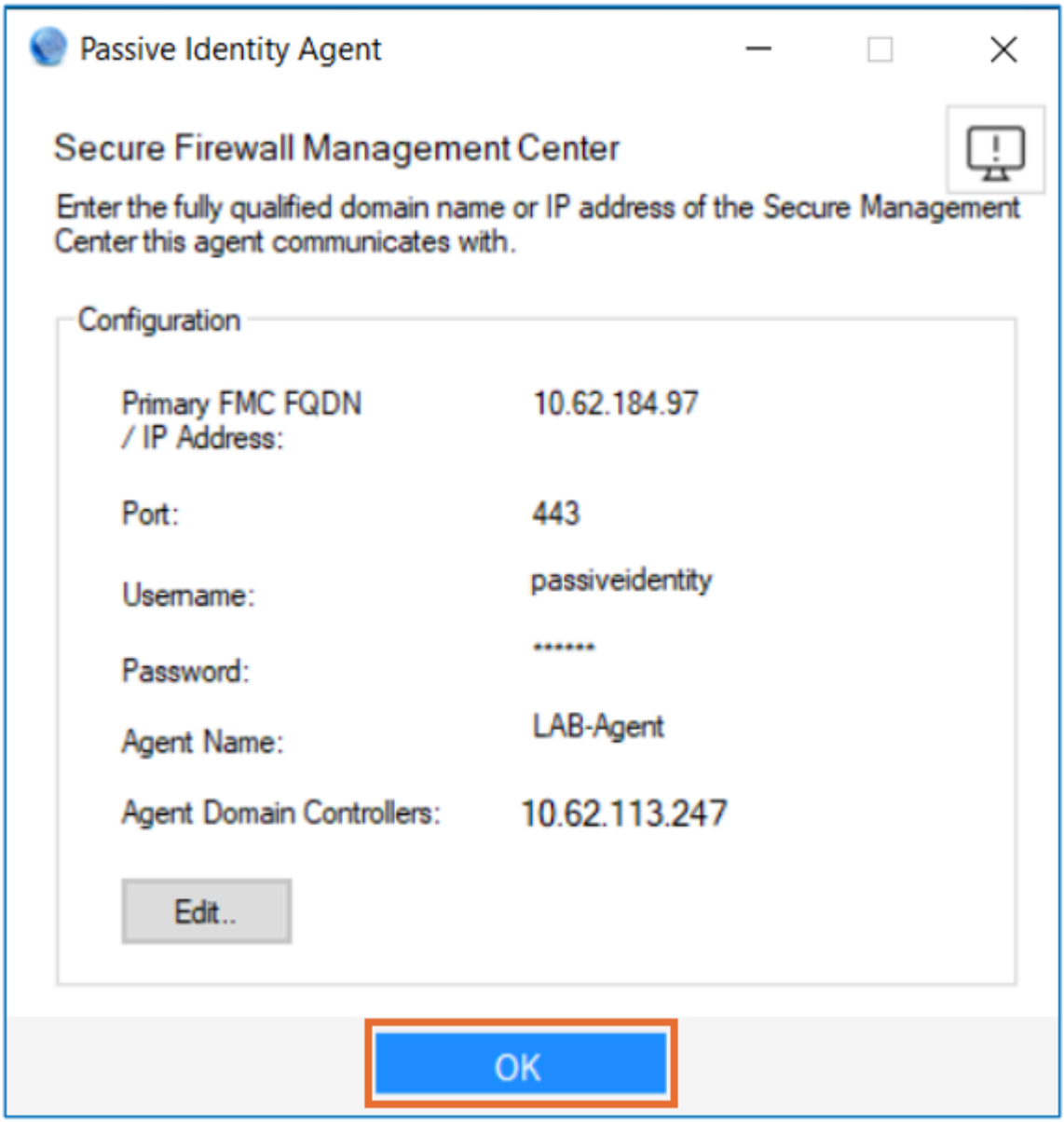

*configure the agent.*

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



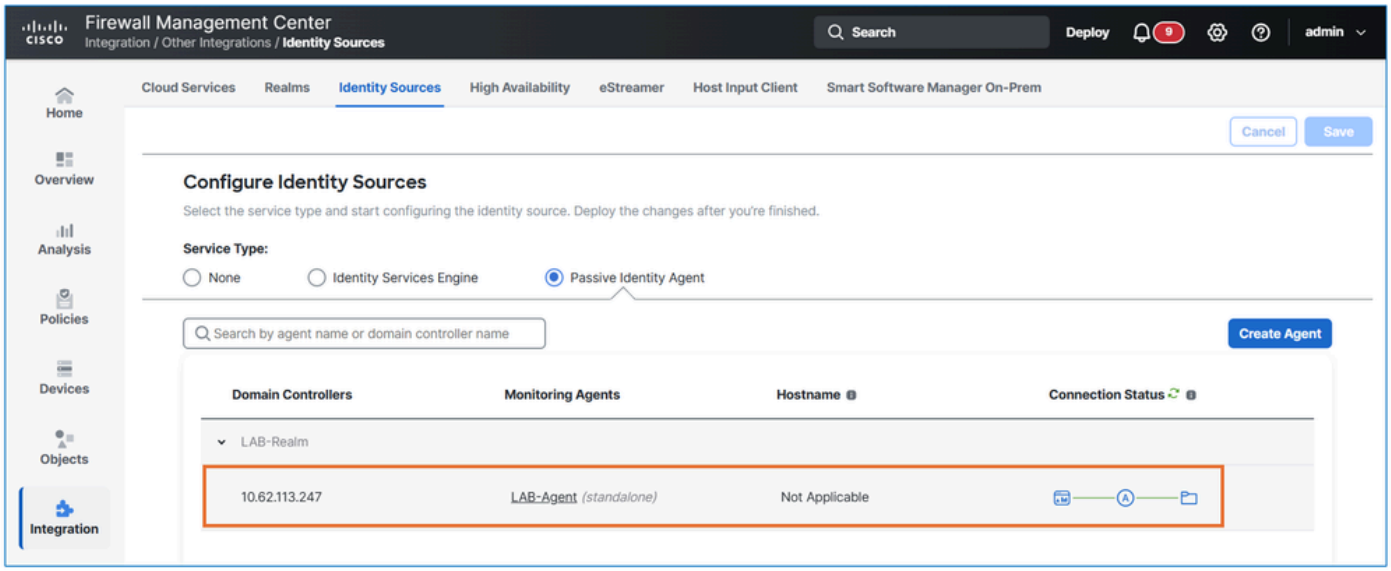

*test*

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




*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.



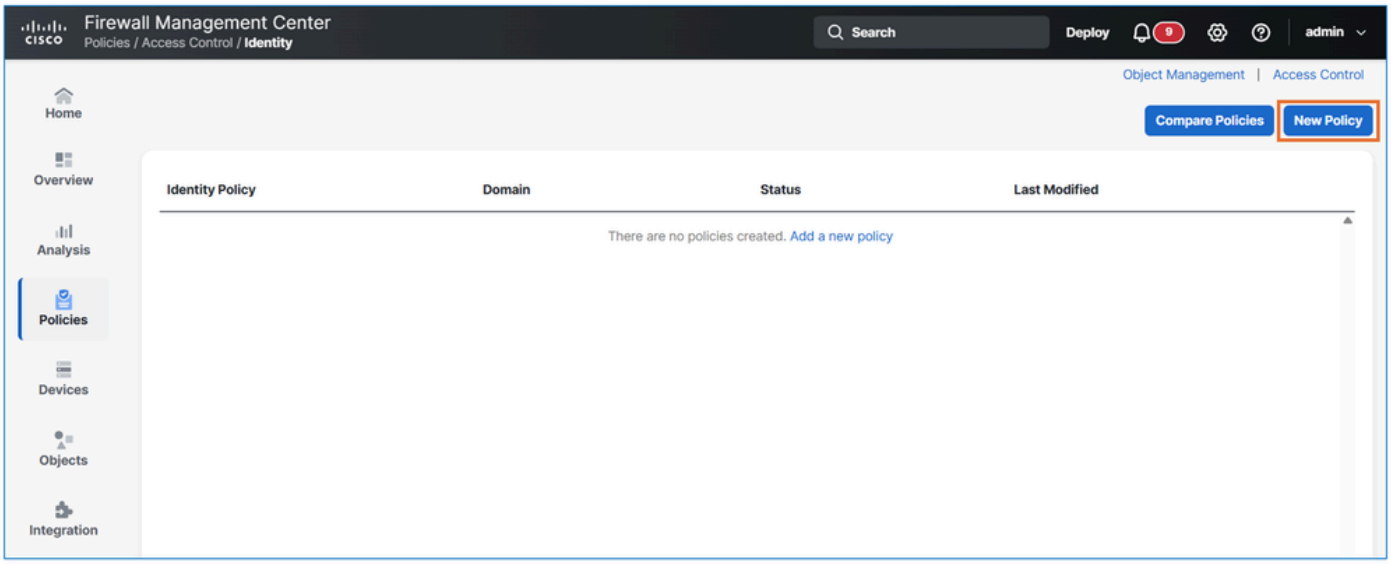

*verify the communication from fmc*

## Configure Identity Policies

Create an Identity Policy based on the table provided.

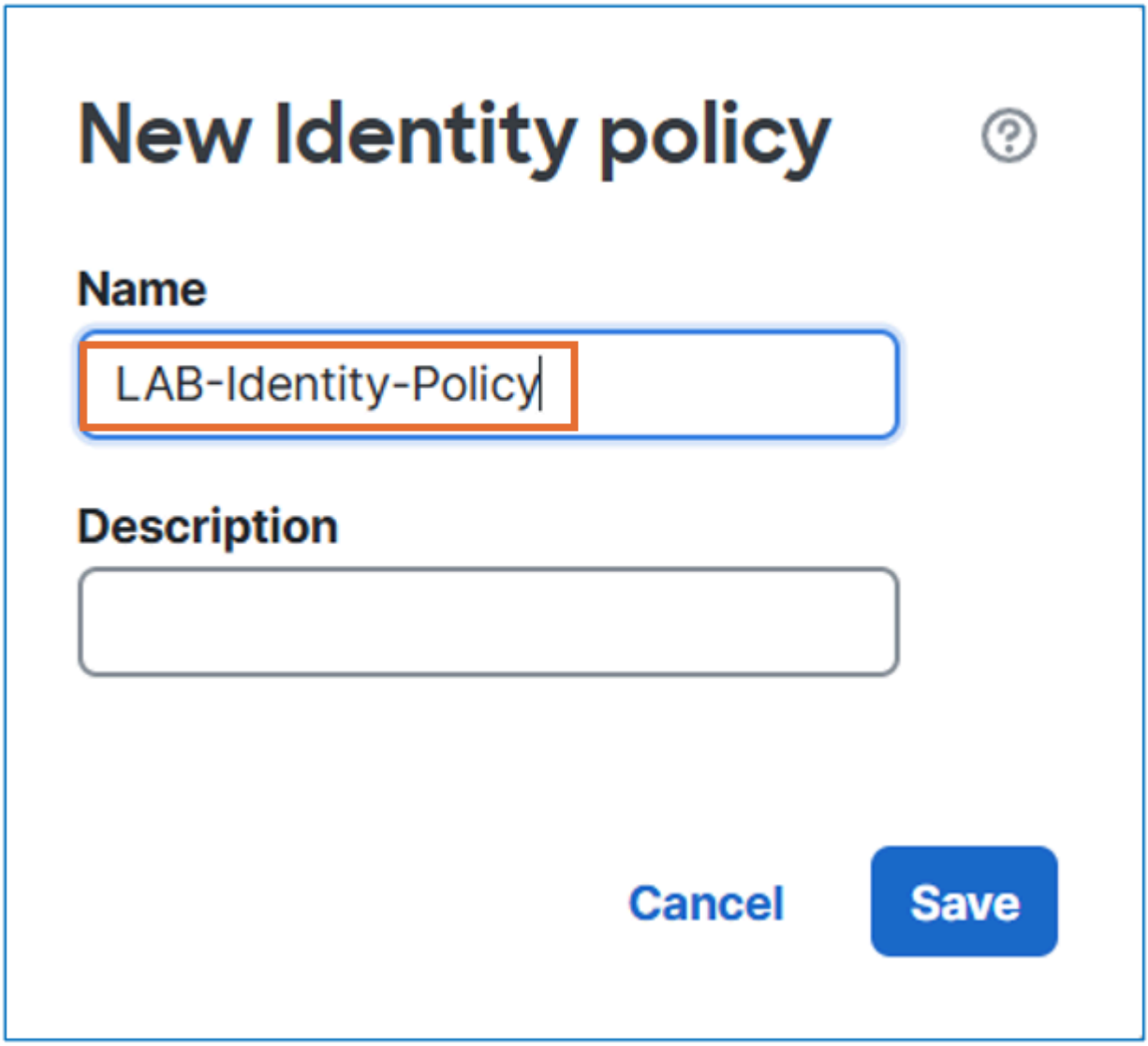
| Policy Name | Rule Name | Authentication Realm | Remaining settings |
|---|---|---|---|
| LAB-Identity-Policy | Rule1 | LAB-Realm | Leave as default |

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



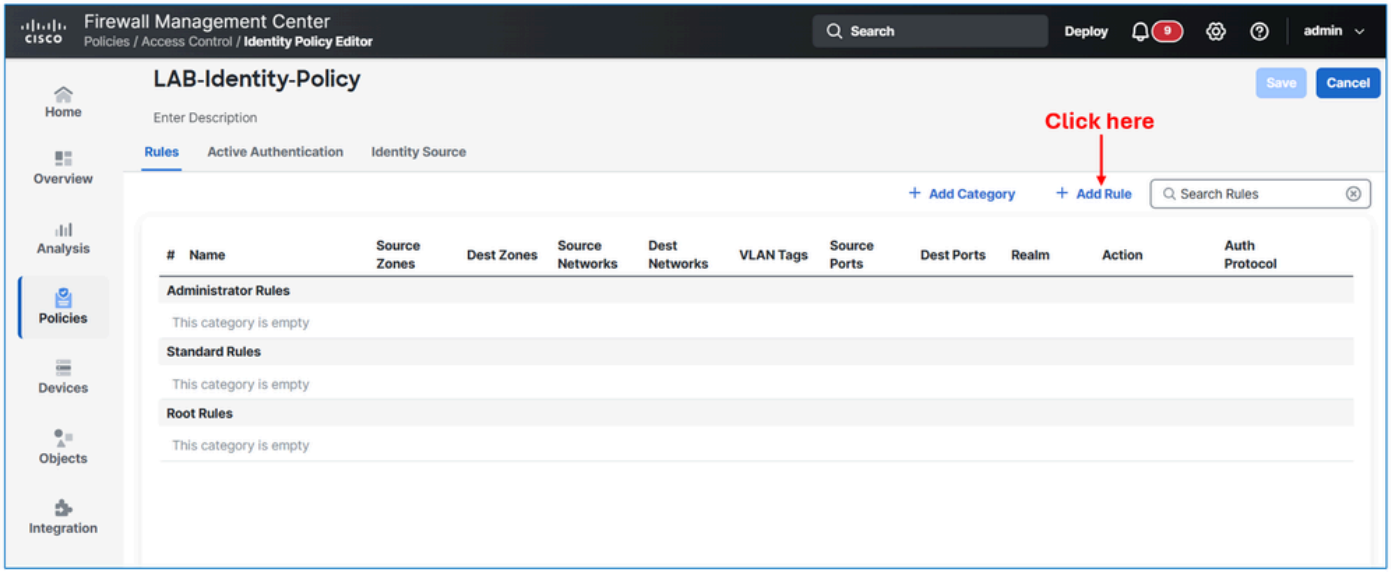

*new policy*

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



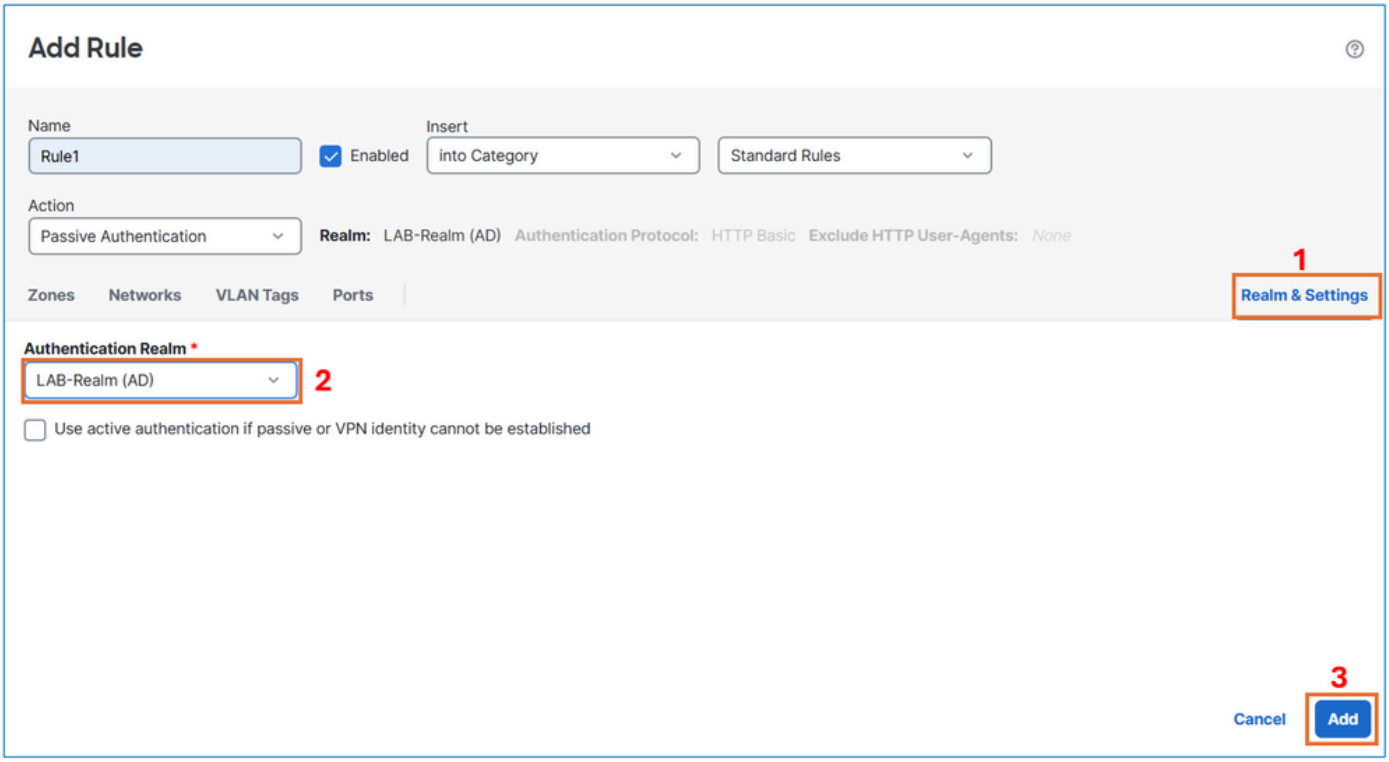

*new policy*

Click the**Add Rule**button.



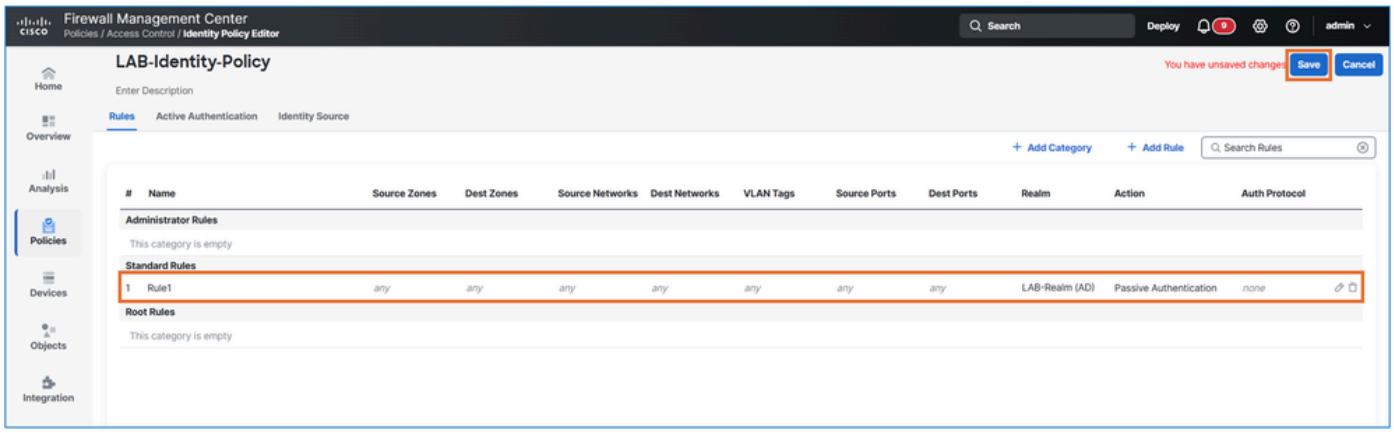
*create rule*

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




*Realm setting*

Click the**Save**button.




*save the config*

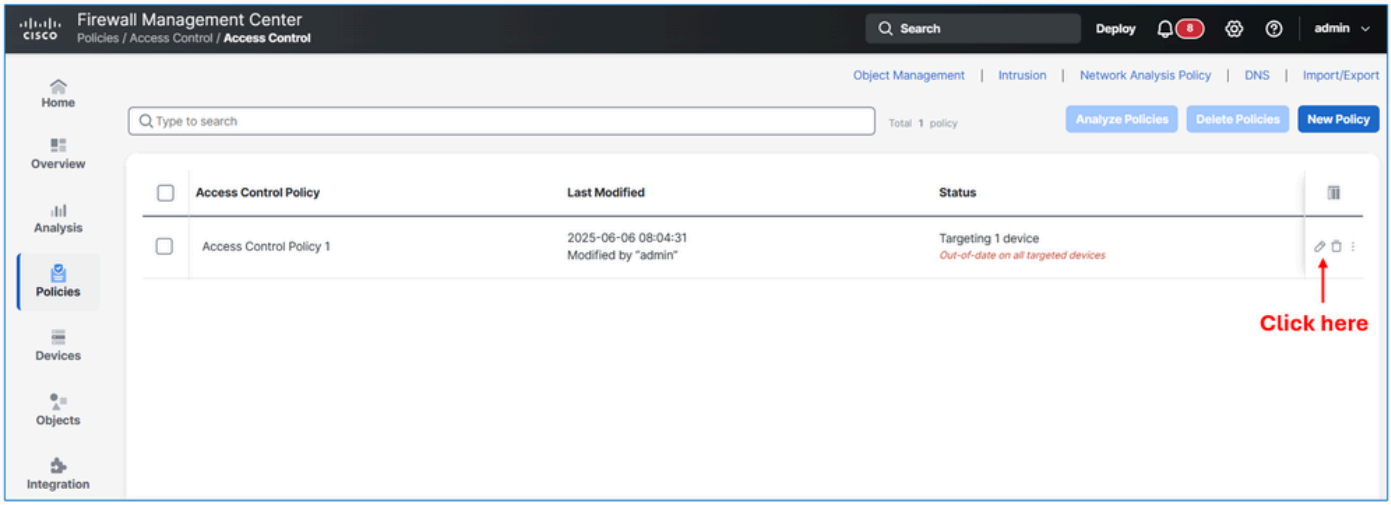
## Configure Access Control Policies

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 |

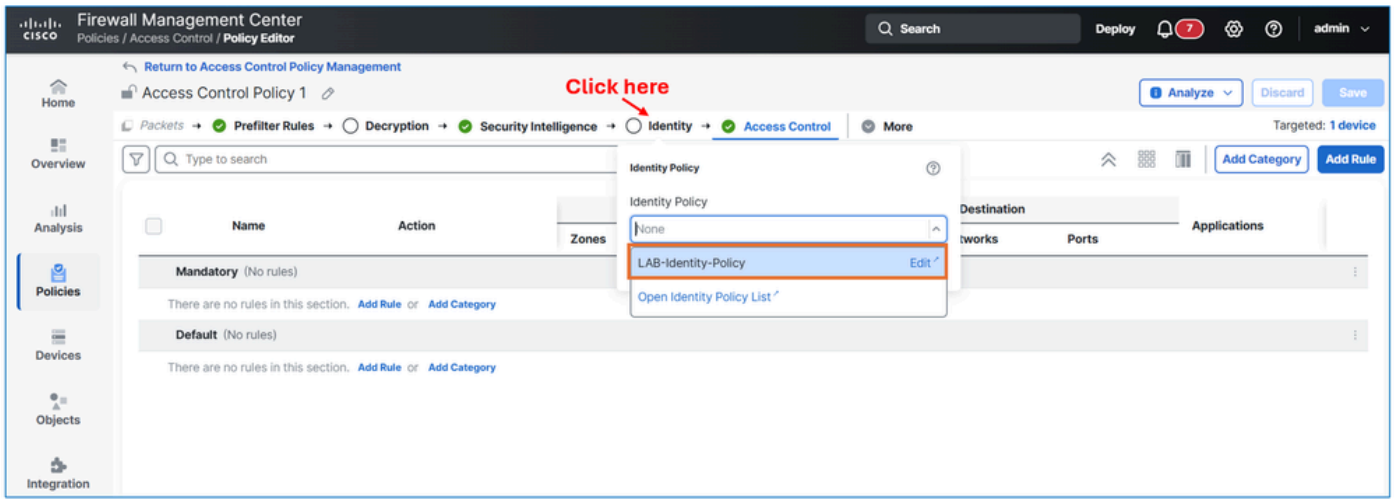
Step 1. Link the **Identity Policy** to the **Access Control Policy**

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




*Edit policy*

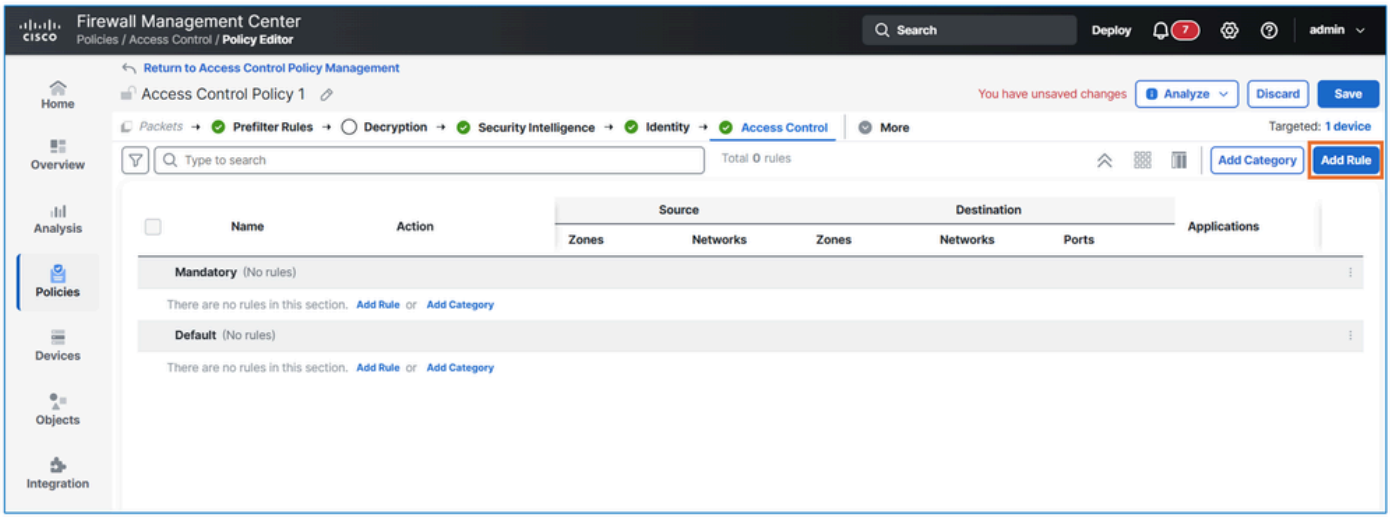
Navigate to the**Identity**section and link the **Identity Policy** created in the previous task.




*add identity policy*

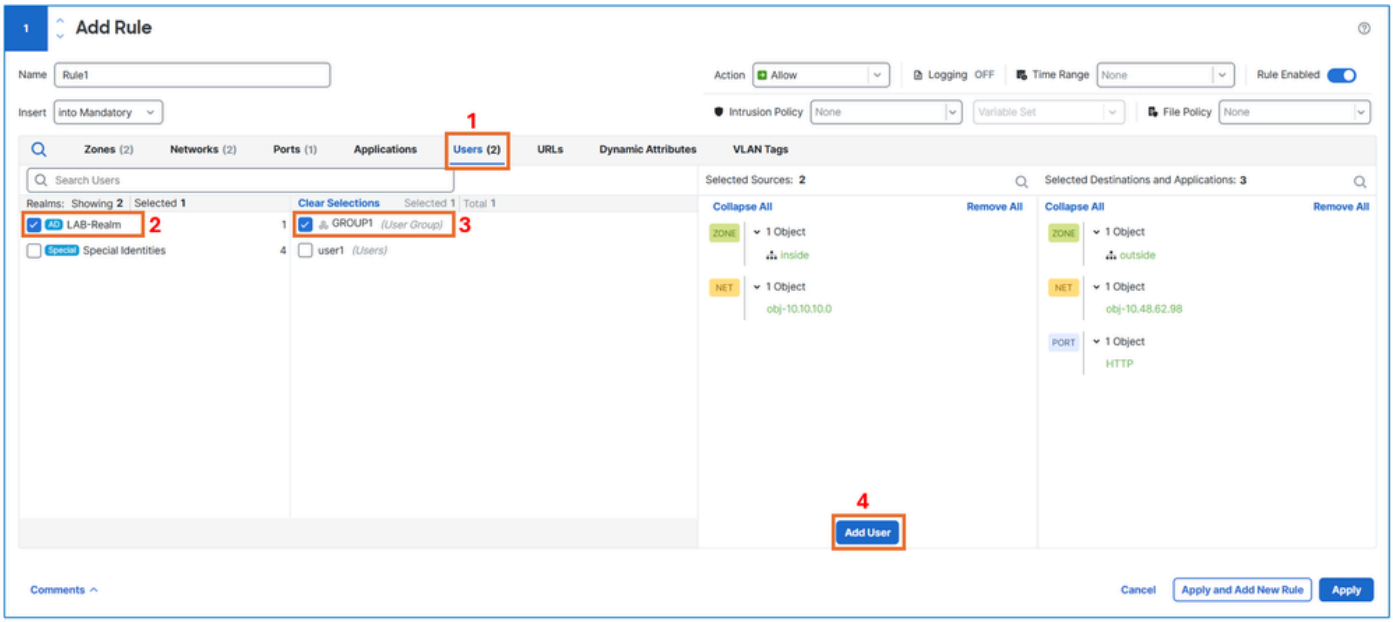
Click the**Apply**button

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



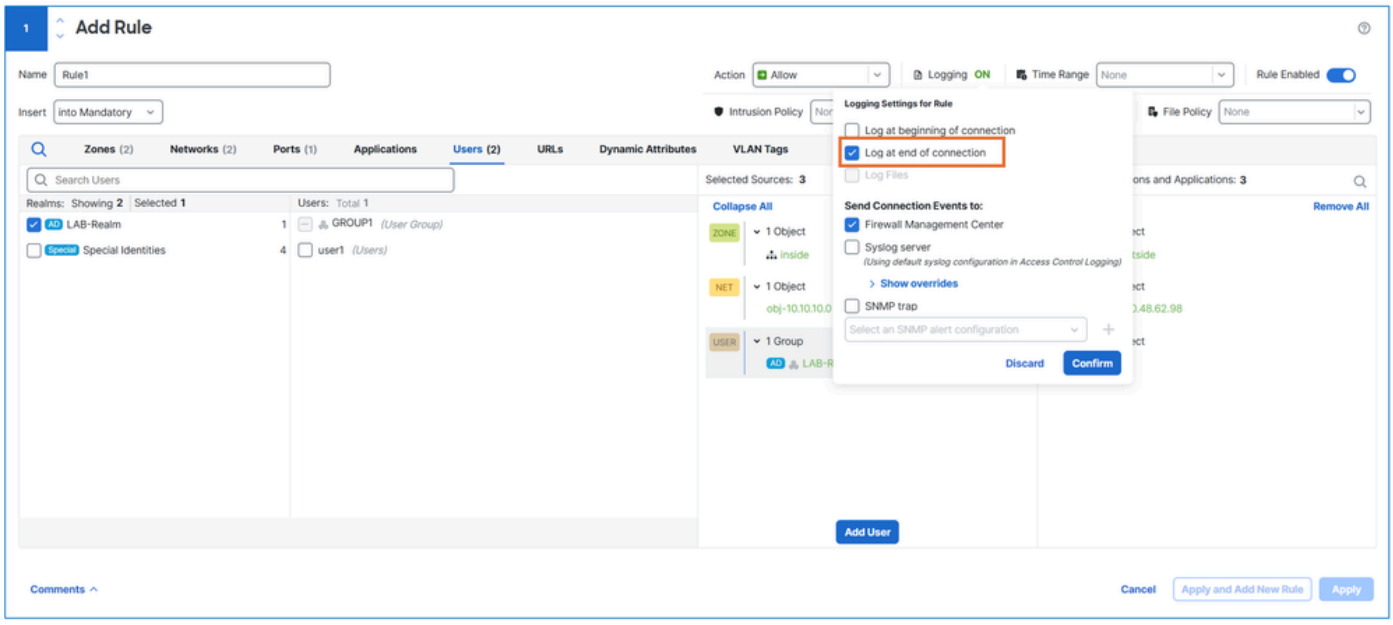

*create ACP*

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




*add users in the rule*

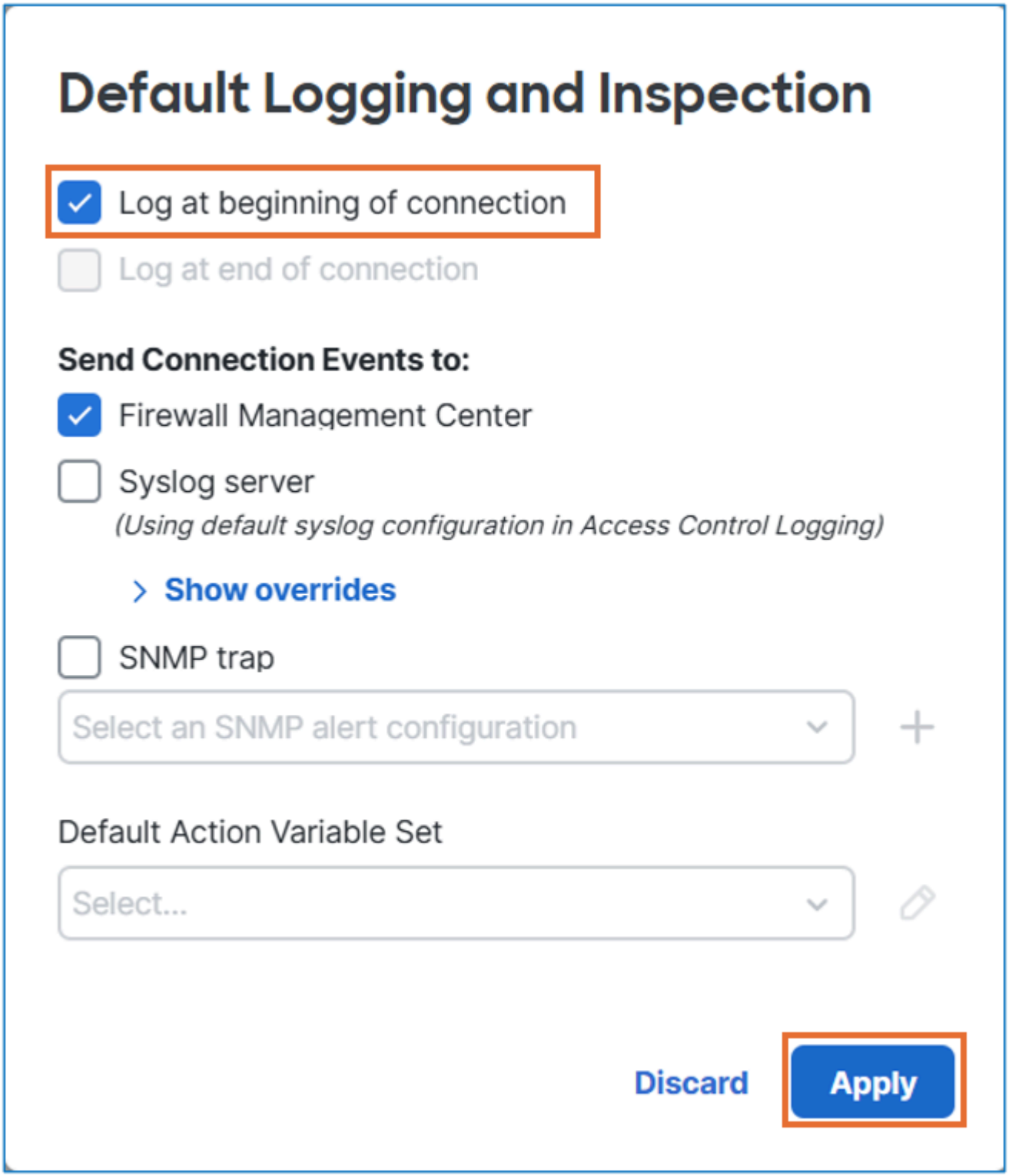
Enable logging for the rule by selecting**Log at end of connection**.




*enable logging*

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

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



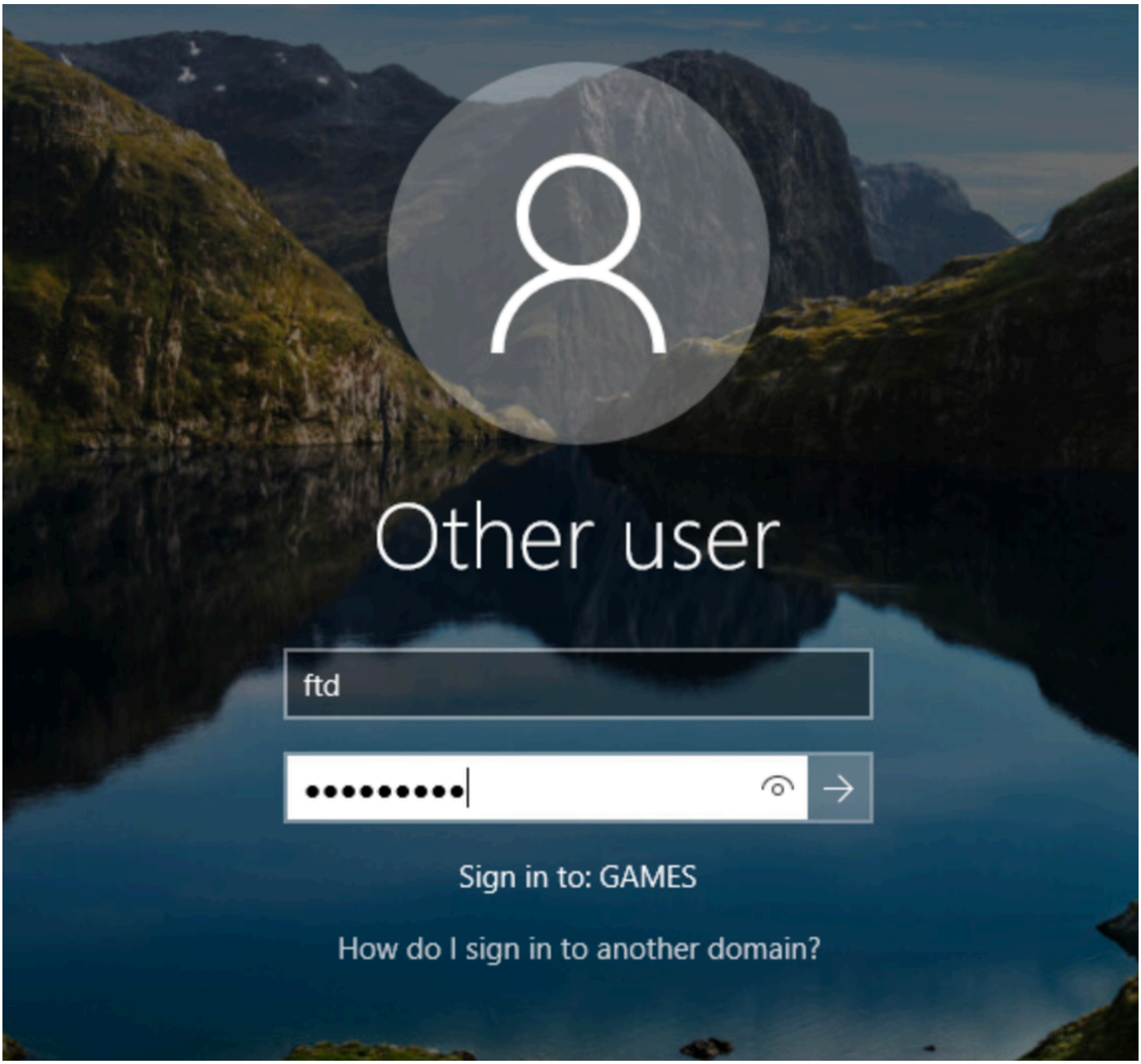

*Enable logging*

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

## Verification

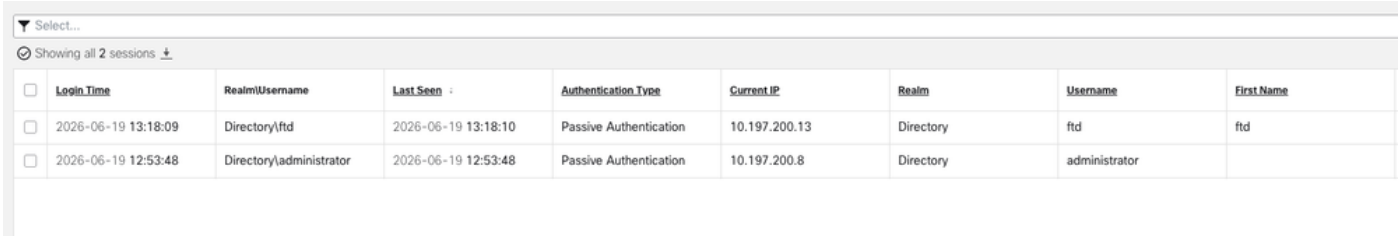
Verify the Passive Identity operation by confirming that traffic is allowed exclusively for ftd.

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




*user login*

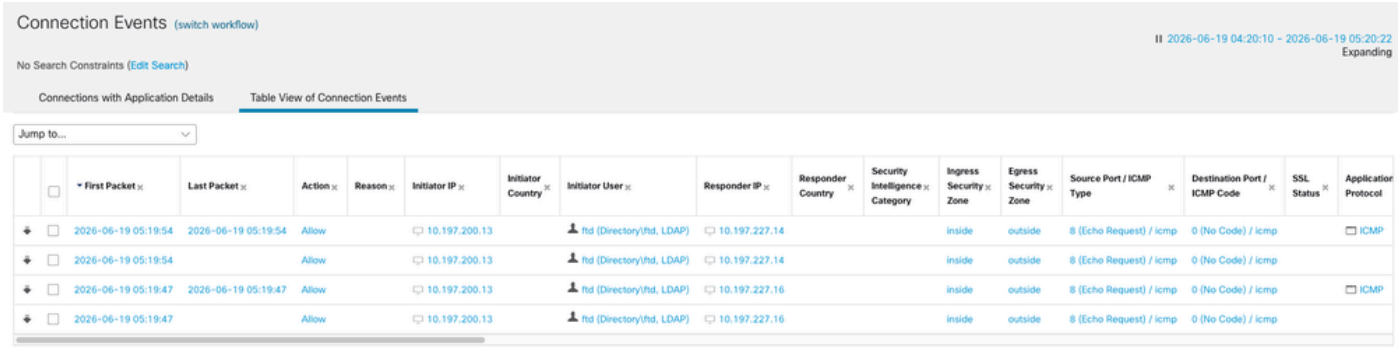
After a user successfully logs in, verify from FMC under **Analysis> user >active session to view the active user detail**.




*Active sessions*

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

events.

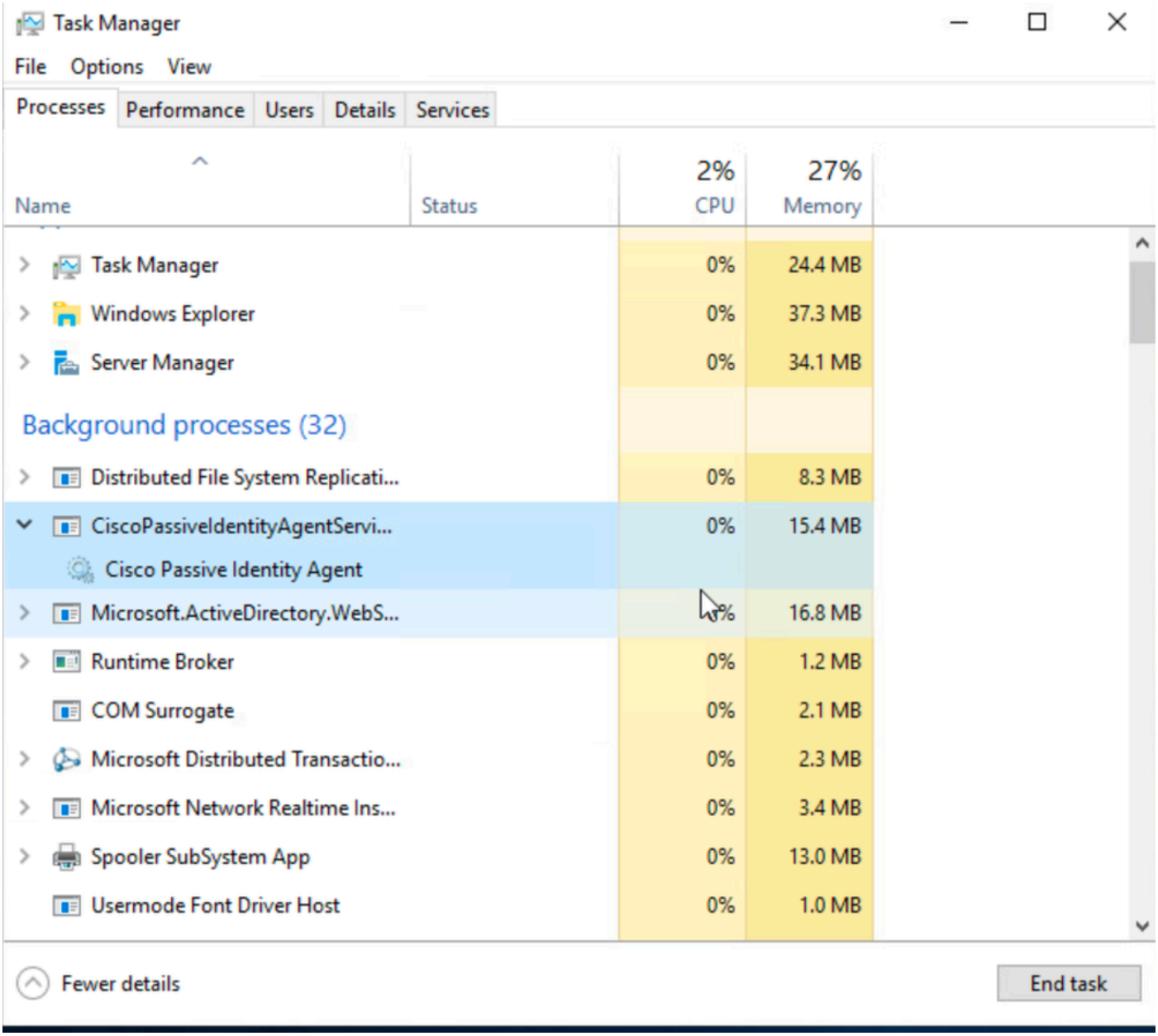



*Active sessions*

# Troubleshooting

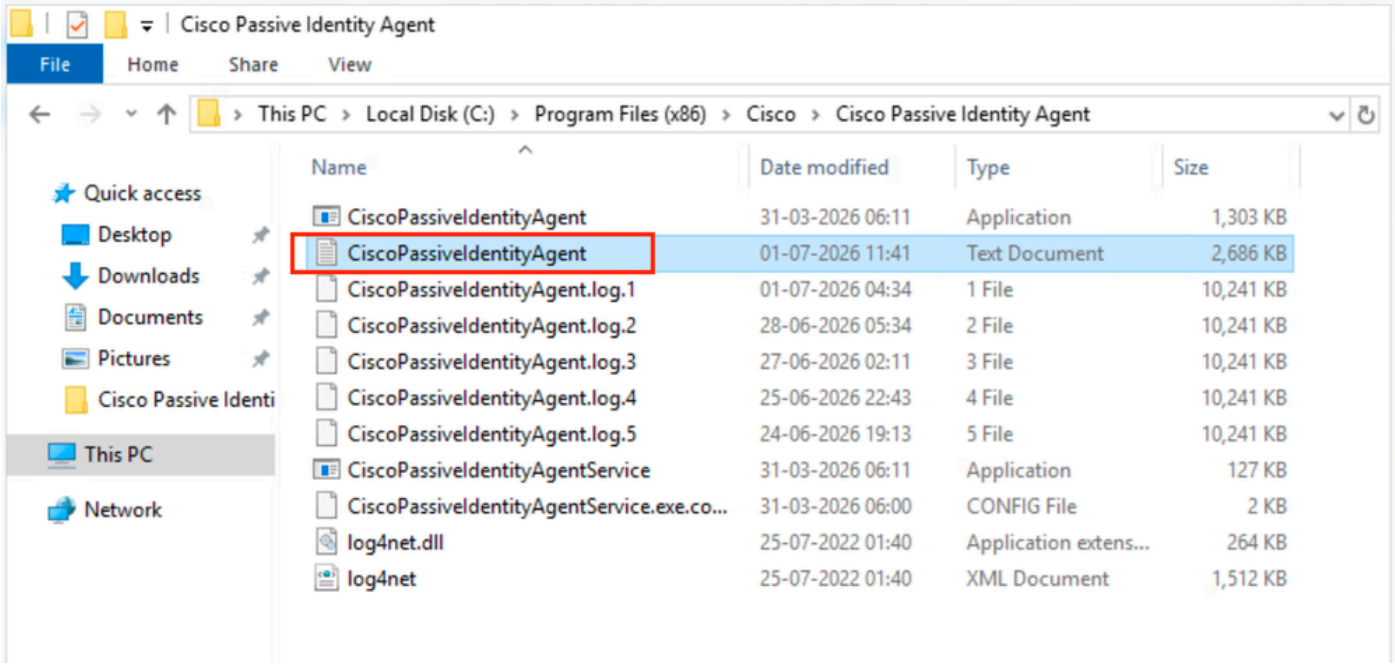
## Checking Agent Logs

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



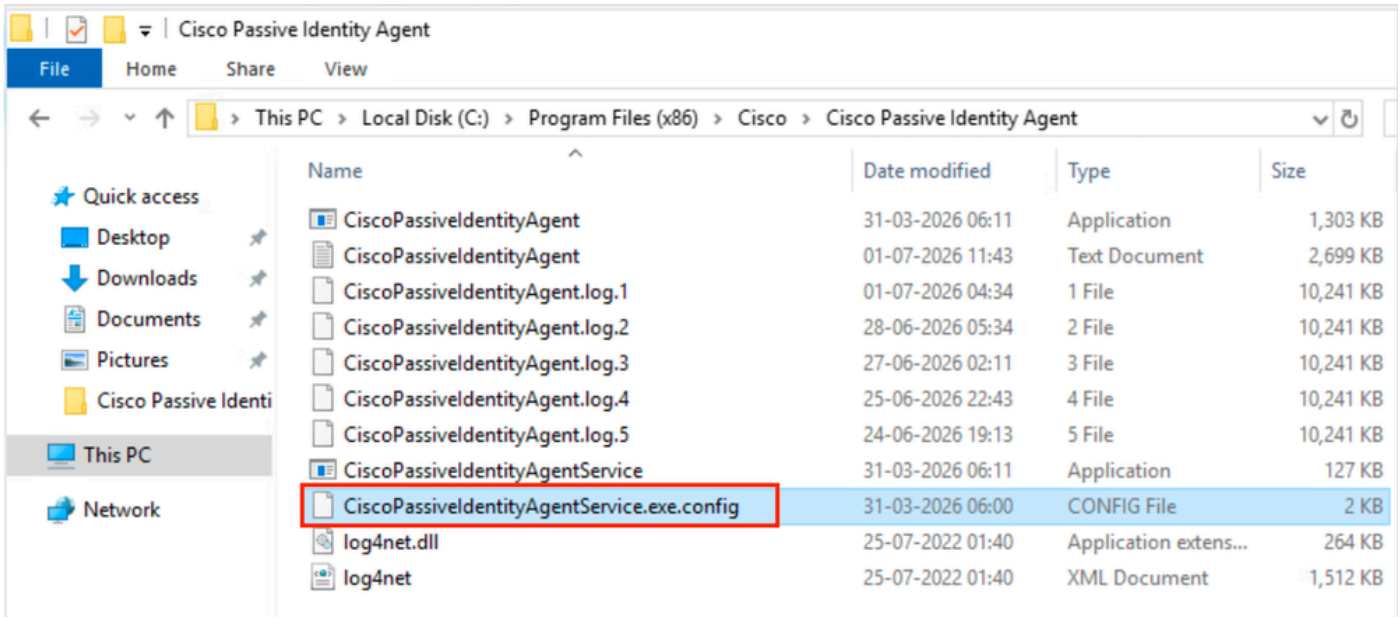

*Running task*

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: [f"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