

Configurare l'agente di identità passiva utilizzando FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazioni](#)

[Configurazione di un'origine dell'agente di identità passiva](#)

[Creazione di un utente Passive Identity Agent in Secure Firewall Management Center](#)

[Installare e configurare il software Passive Identity Agent](#)

[Configura criteri di identità](#)

[Configura criteri di controllo di accesso](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Controllo dei log dell'agente](#)

[Registri FMC](#)

Introduzione

In questo documento viene descritto come configurare l'origine dell'agente di identità passivo che invia i dati della sessione a FMC

Prerequisiti

Requisiti

- Cisco Secure Firewall Management Center con versione 7.6+
- Cisco Secure Firewall con versione 7.6+
- Windows Active Directory, il server deve eseguire Windows Server 2008 o versione successiva.
- È necessario abilitare lo Snort 3 sui dispositivi Secure Firewall Threat Defense.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Firewall Management Center 7.6.5
- Cisco Secure Firewall 7.6.5
- Microsoft Active Directory in esecuzione su Windows Server 2022.

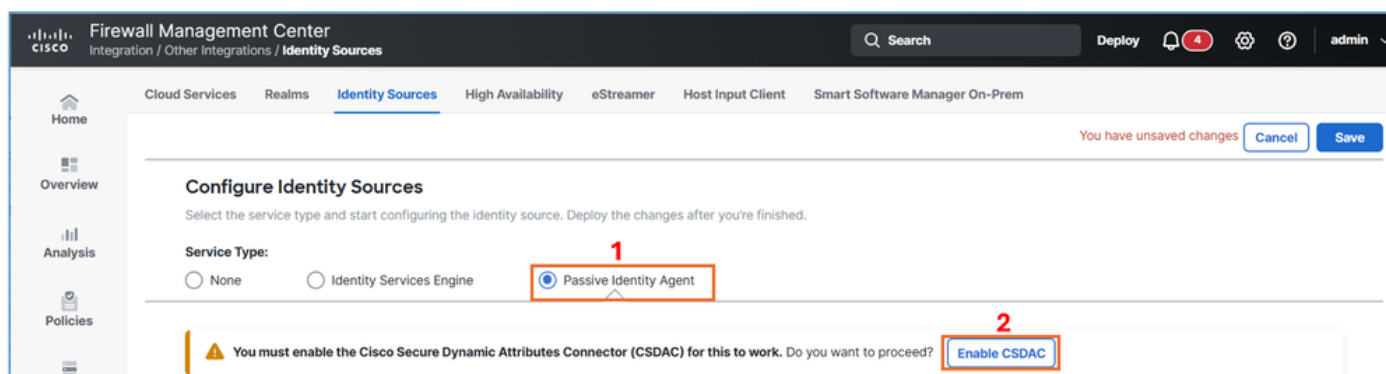
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazioni

Prima di configurare l'agente, completare l'integrazione di AD e FMC.

Configurazione di un'origine dell'agente di identità passiva

Nell'interfaccia utente di FMC, selezionare Integrazione > Altre integrazioni > Origini identità, quindi fare clic su Agente di identità passivo. Se Cisco Secure Dynamic Attributes Connector non è stato ancora abilitato, verrà richiesto di farlo facendo clic su Abilita CSDAC.



Passive Identity Agent

Fare clic sul pulsante Abilita per abilitare CSDAC.

Enable Cisco Secure Dynamic Attributes Connector?



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

Cancel

Enable

Abilita CSDAC

Questa operazione richiede circa 10 minuti. Una volta che il CSDAC è stato abilitato correttamente, fare clic sul pulsante Donebutton per procedere.

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 abilitato

Fare clic sul pulsante Crea agente.

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?

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

Crea agente

Definire un nome per l'agente, selezionare l'opzione Standalone e associarlo al controller di dominio appropriato creato nell'attività precedente.

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:

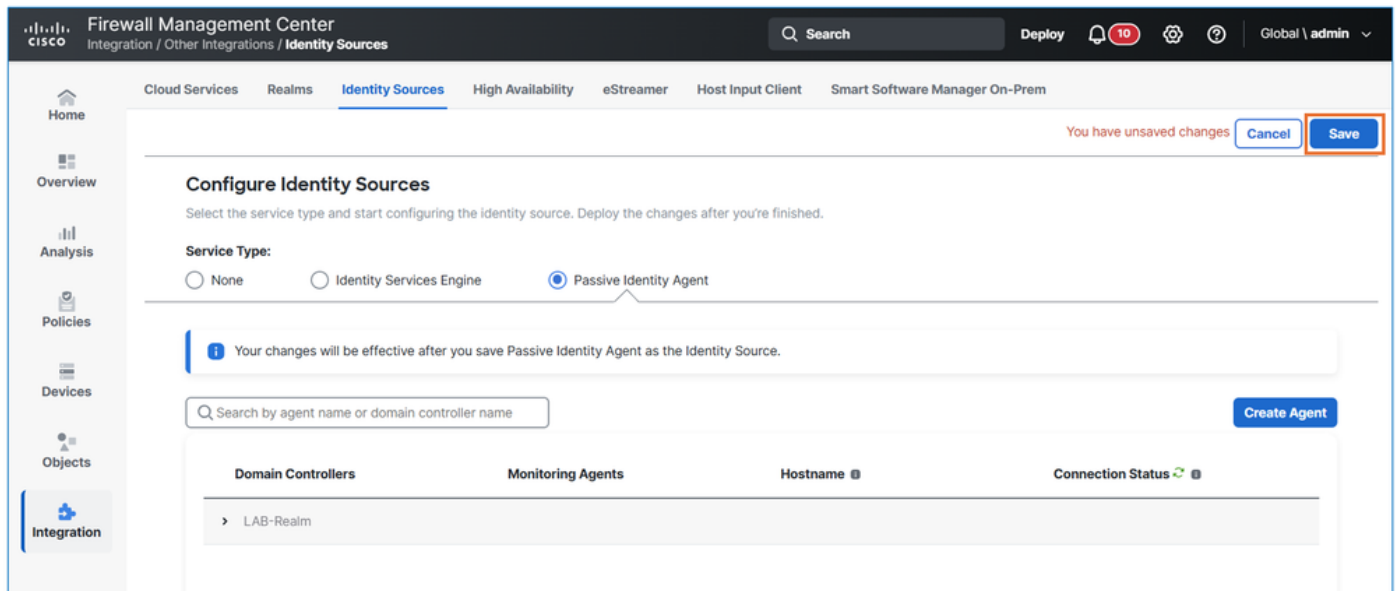
This agent will be created and assigned to the selected domain controller. Install it on the domain controller (or on its member machine) to start the tracking.

Cancel

Save

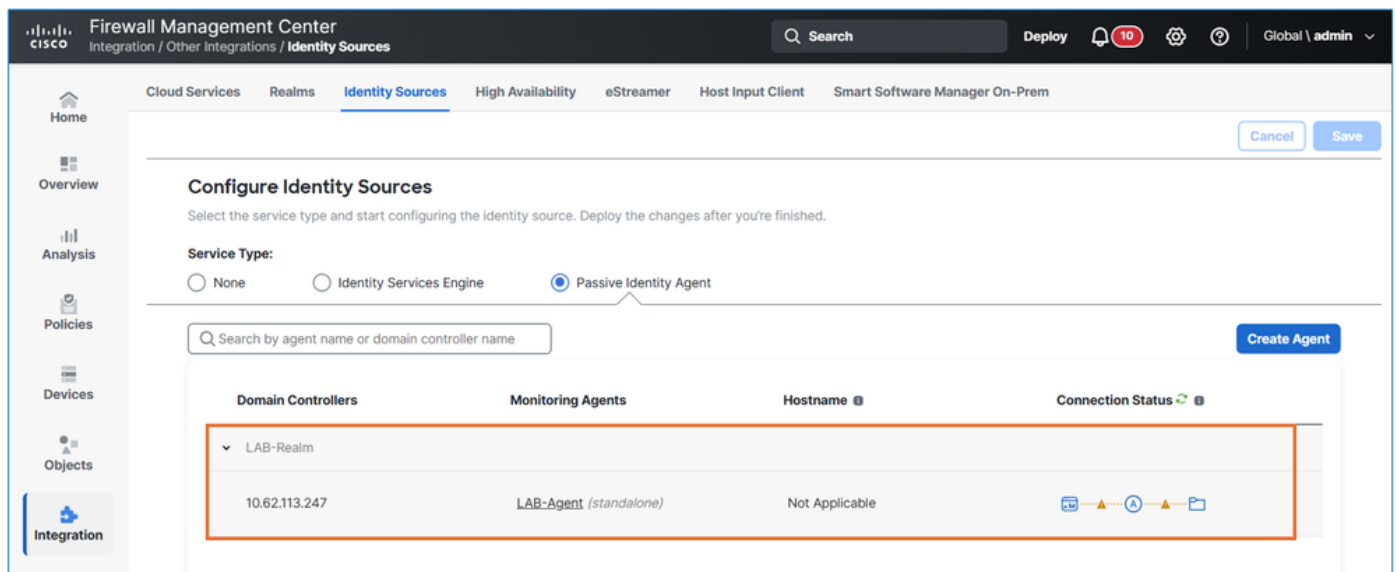
Configura agente

Fare clic sul pulsante Salva.



Salvare la configurazione

Il risultato.



Verifica dello stato



Nota: L'agente di identità passiva indica lo stato utilizzando delle righe. Il colore ambra indica che l'agente non ha mai comunicato correttamente con il centro di gestione Secure Firewall. Una nuova linea dell'agente è di colore ambra e rimane tale fino al completamento della configurazione.

Creazione di un utente Passive Identity Agent in Secure Firewall Management

Center

Creare un utente di Centro gestione firewall sicuro con autorizzazioni sufficienti per comunicare con l'agente di identità passiva. L'utente dispone di privilegi limitati per eseguire altre attività. l'utente deve abilitare solo la comunicazione con l'agente di identità passiva.

Nell'interfaccia utente di FMC, selezionare Sistema > Utenti e fare clic su Crea utente. Immettere i dettagli utente in base ai requisiti del task.

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

Crea utente

Assegnare solo il ruolo Utente identità passiva. Fare clic sul pulsante Salva.

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

selezionare l'utente dell'identità passiva

Installare e configurare il software Passive Identity Agent

Installare e configurare il software Passive Identity Agent nel controller di dominio designato.

Scaricare l'agente di identità passiva da 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

Search...

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

16-Sep-2024

1.59 MB

CiscoPassiveIdentityAgentInstaller-1.0.msi

Advisories



Installer for the Cisco Passive Identity Agent

11-Mar-2025

2.16 MB

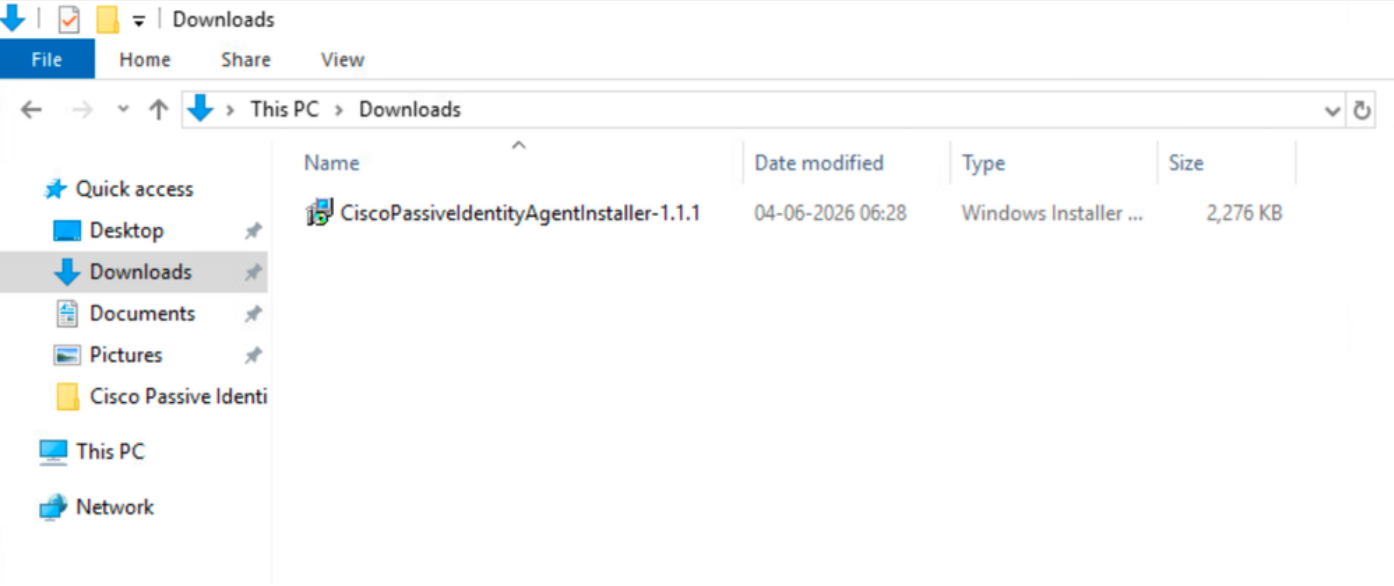
CiscoPassiveIdentityAgentInstaller-1.1.msi

Advisories



scaricare il software

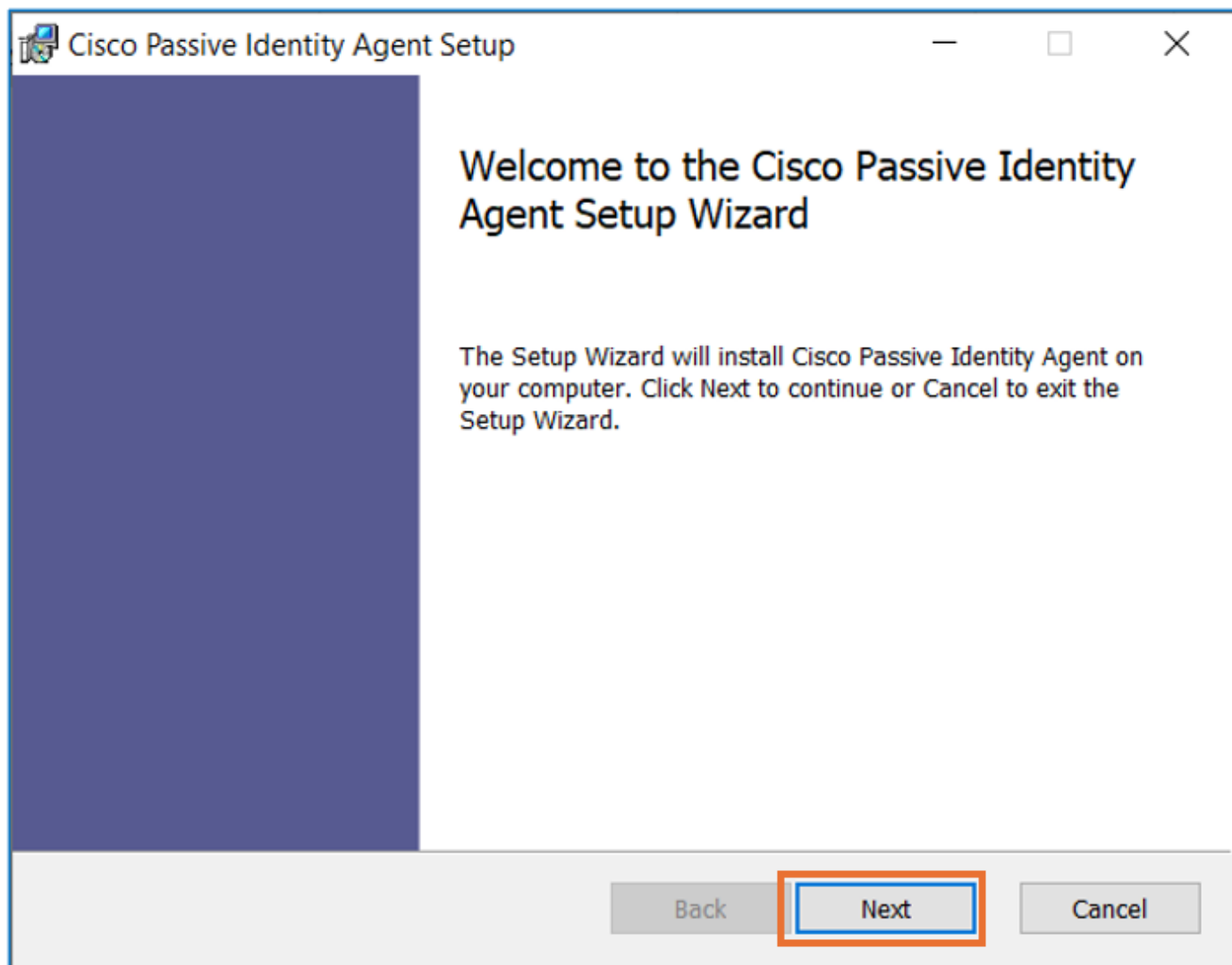
Dopo aver scaricato l'agente, avviare il processo di installazione nel controller di dominio.



agente

]

Fare riferimento alle istruzioni di installazione fornite per completare l'installazione.



Install

Una volta completata l'installazione, aprire il software Passive Identity Agent e immettere le informazioni richieste come specificato nei requisiti del task. Fare clic sul pulsante Test per verificare la connettività con 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**

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

Test

Click here to test the connectivity

I have **Secondary FMC** ▾

Save **Cancel**

configurare l'agente.

Dopo aver verificato la connettività, fare clic sul pulsante Salva.

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

C

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

Fare clic sul pulsante OK per completare la configurazione dell'agente.

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

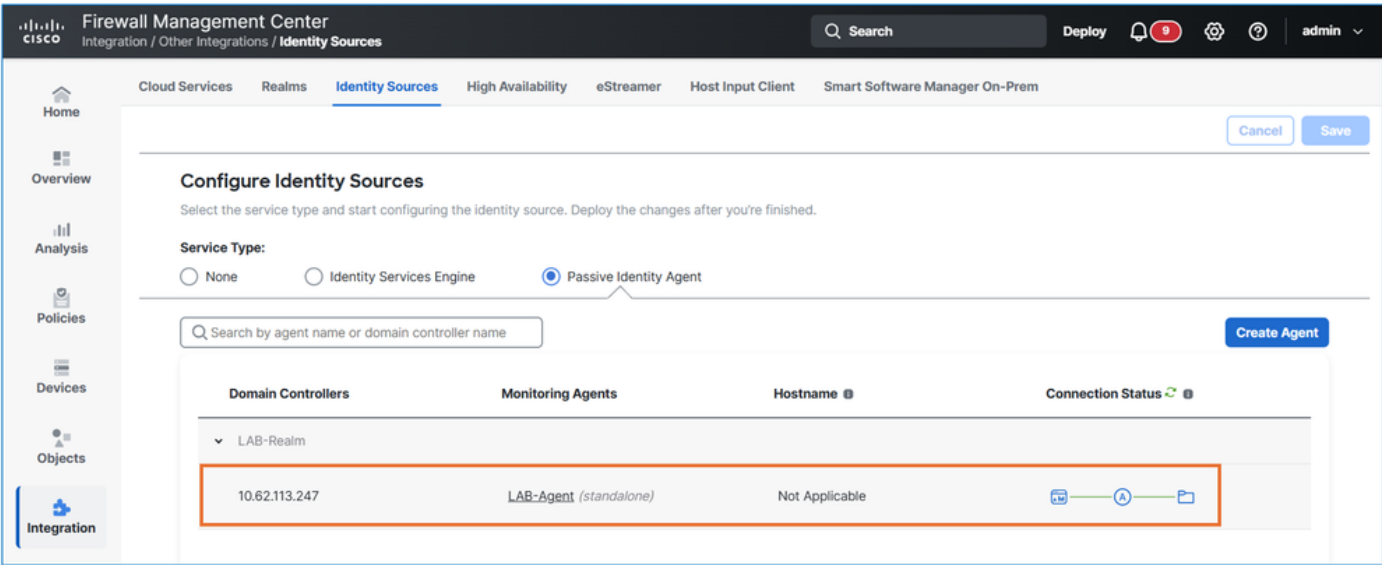
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

agente in esecuzione

Nell'interfaccia utente di FMC, selezionare Integrazione > Altre integrazioni > Origini identità > Agente identità passiva. Confermare che l'Agente identità passiva visualizzi uno stato verde.



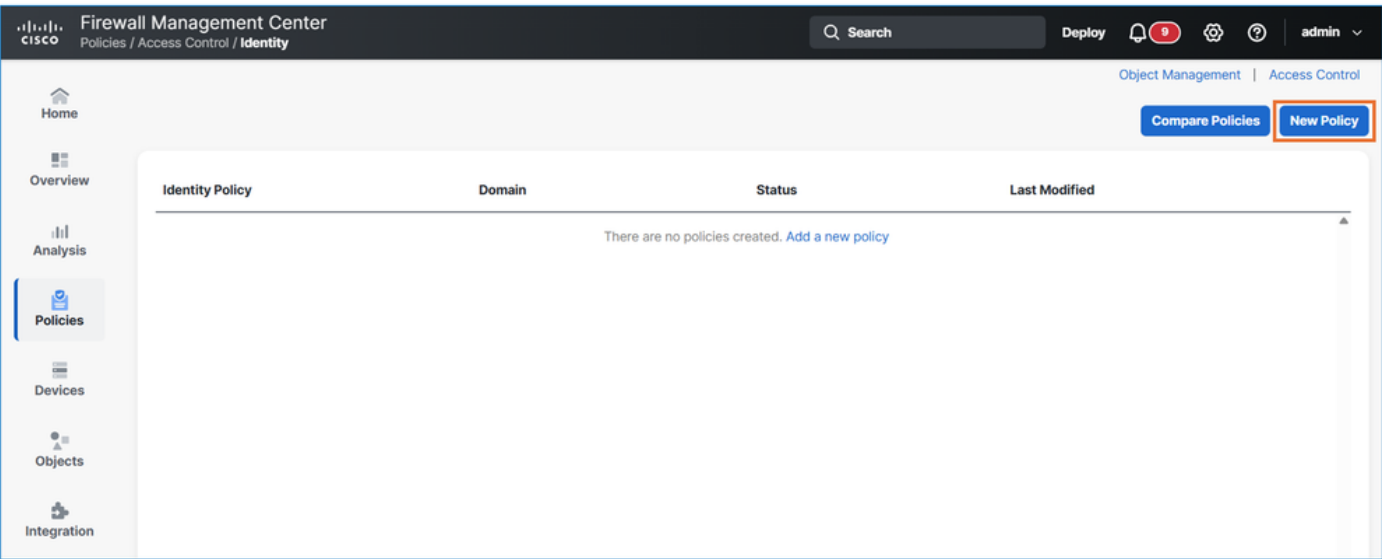
verifica la comunicazione da fmc

Configura criteri di identità

Creare un criterio di identità in base alla tabella fornita.

Nome criterio	Nome regola	Realm di autenticazione	Impostazioni rimanenti
LAB-Identity-Policy	Regola1	Area di autenticazione	Lascia come predefinito

Nell'interfaccia utente di FMC passare a Criteri > Controllo di accesso > Identità. Fare clic sul pulsante Nuovo criterio.



nuovo criterio

Immettere il nome del criterio in base ai requisiti dell'attività.

New Identity policy

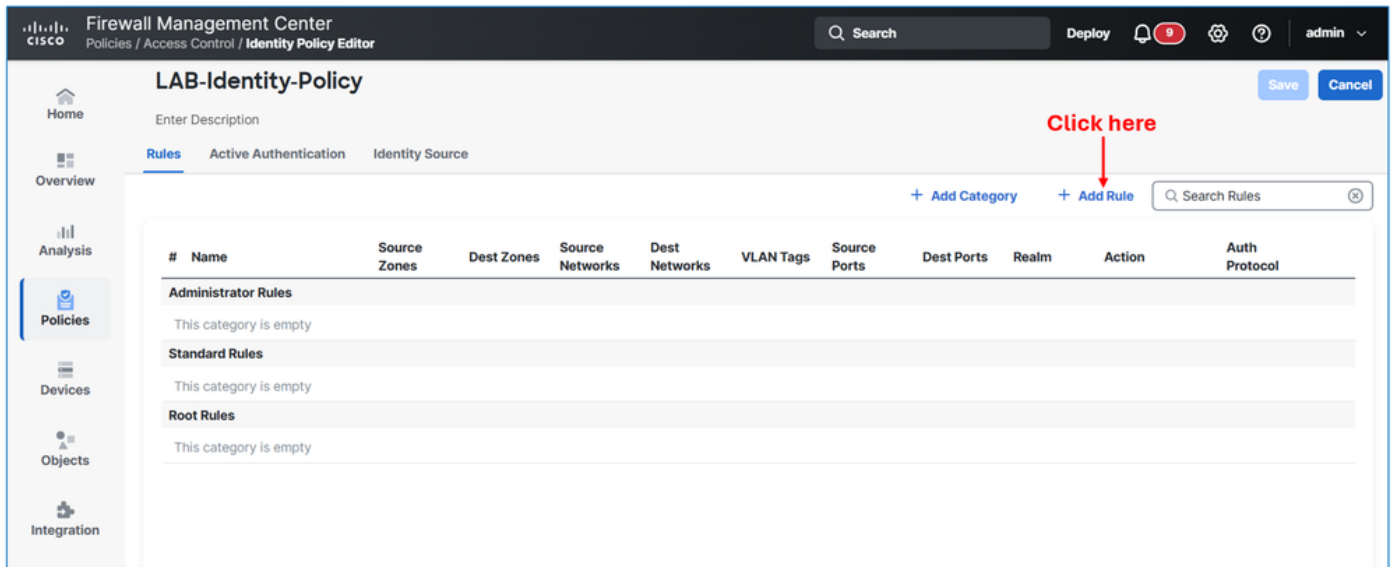
Name

Description

CancelSave

nuovo criterio

Fare clic sul pulsante Aggiungi regola.

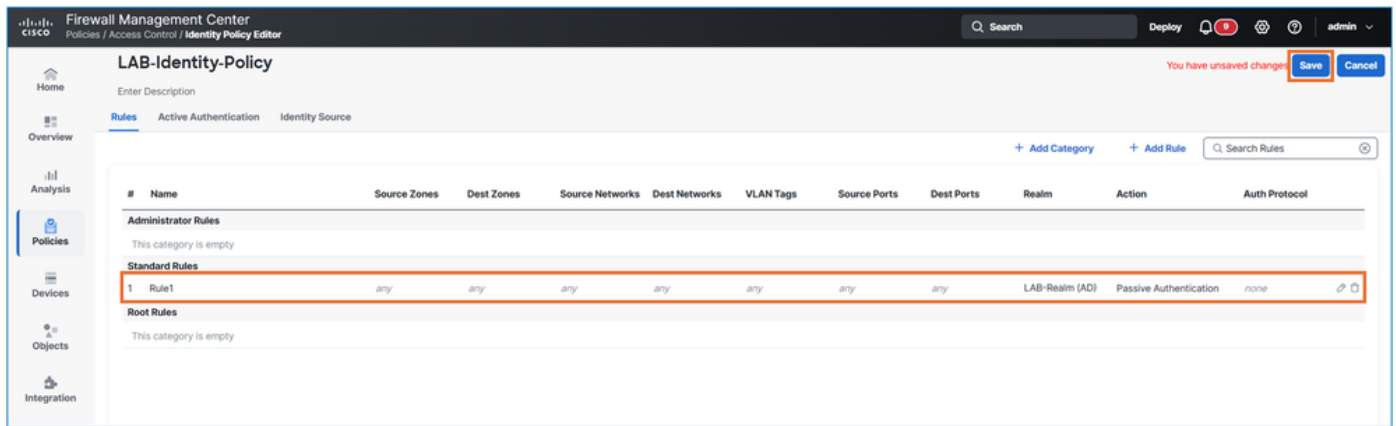


crea regola

Passare alla scheda Realm e impostazioni e selezionare il realm di autenticazione in base ai requisiti del task. Infine, fare clic sul pulsante Aggiungi.

Impostazione realm

Fare clic sul pulsante Salva.



salvare la configurazione

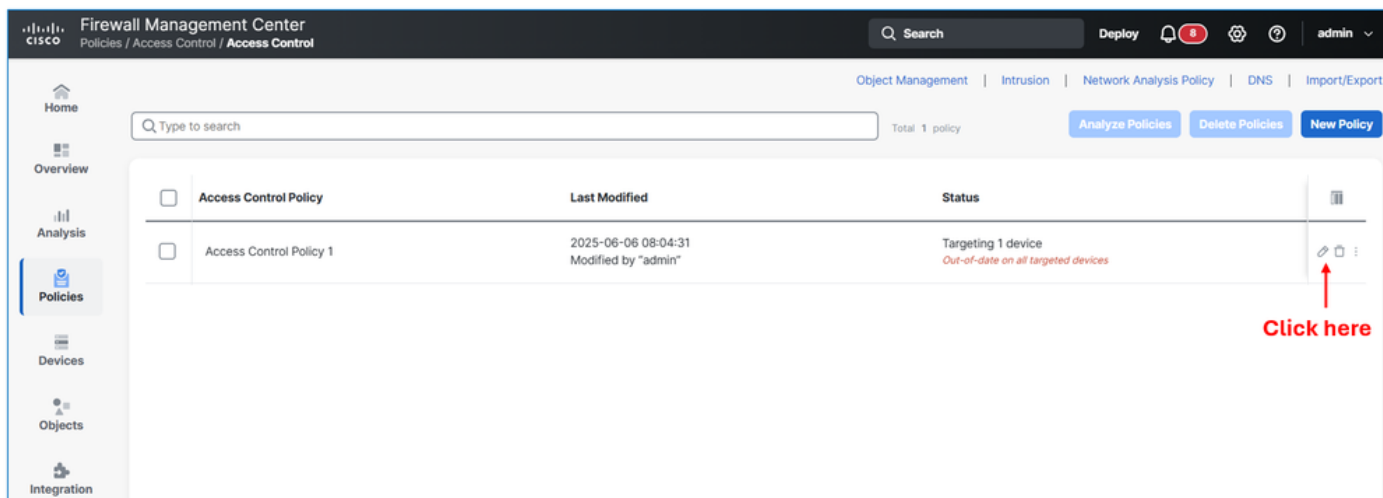
Configura criteri di controllo di accesso

Collegare il criterio di identità al criterio di controllo dell'accesso e creare una regola di criterio di accesso con gli attributi riportati di seguito.

Nome attributo	Valore
Nome regola	Regola1
Azione	Allow (Autorizza)
Zona di origine	Interno
Zona di destinazione	Esterno
Reti di origine	10.10.10.0/24
Reti di destinazione	10.48.62.98/32
Servizio	HTTP (Dest Port TCP 80)
Utenti	LAB-Realm/GROUP1
Registrazione	Alla fine della connessione

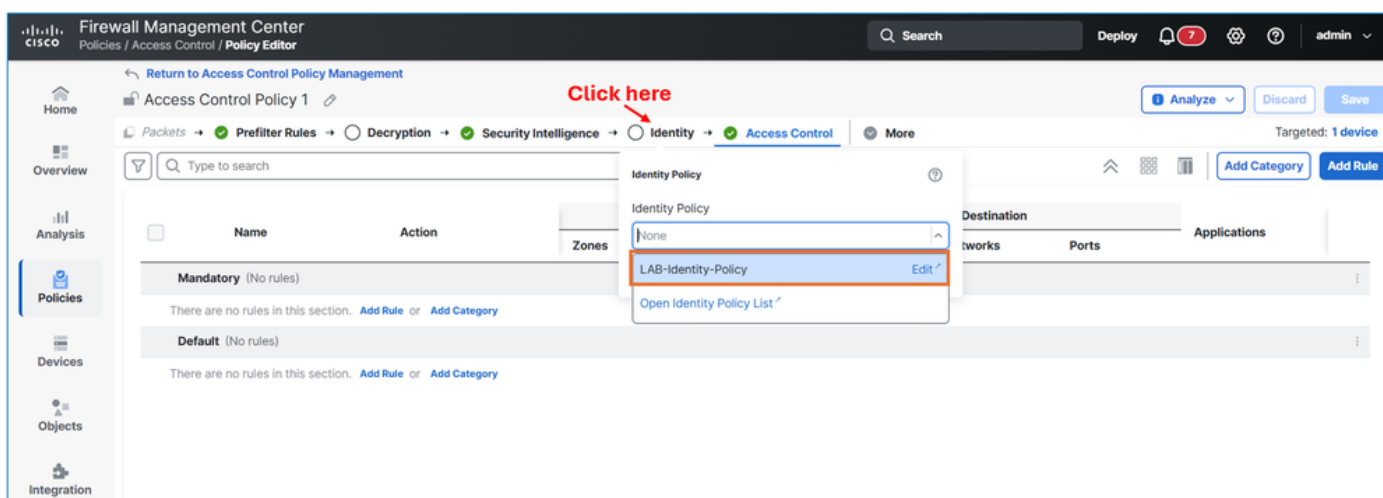
Passaggio 1. Collegare il criterio di identità al criterio di controllo di accesso

Nell'interfaccia utente di FMC, selezionare Policy > Controllo di accesso > Controllo di accesso. Fare clic sul pulsante Modifica relativo al criterio.



Modifica criterio

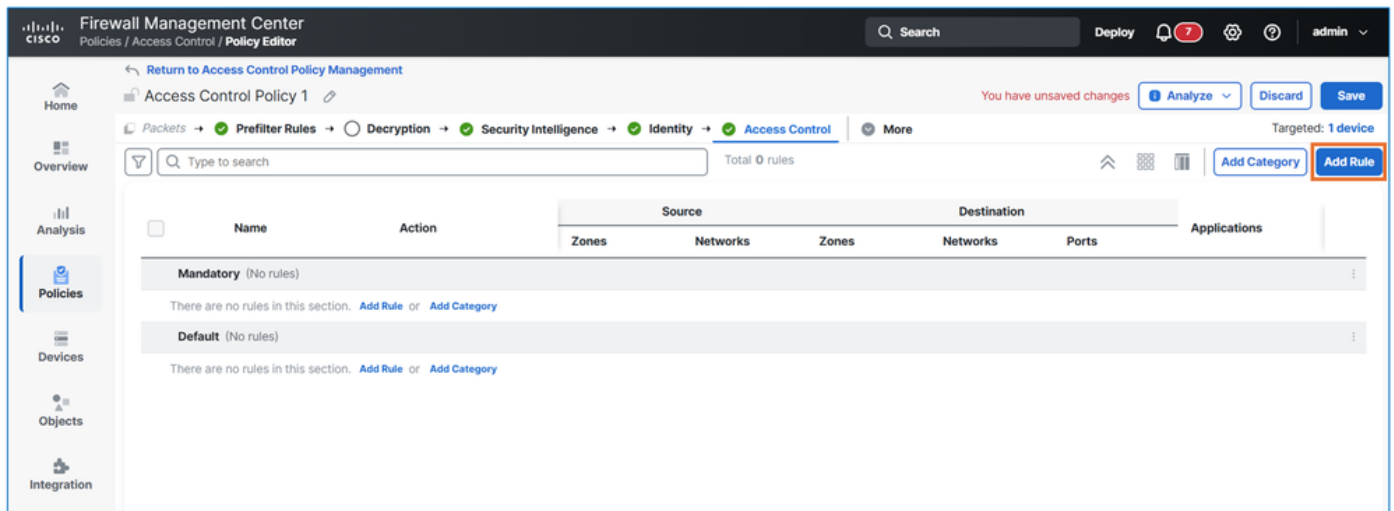
Passare alla sezione Identity e collegare il criterio di identità creato nell'attività precedente.



aggiungi criterio di identità

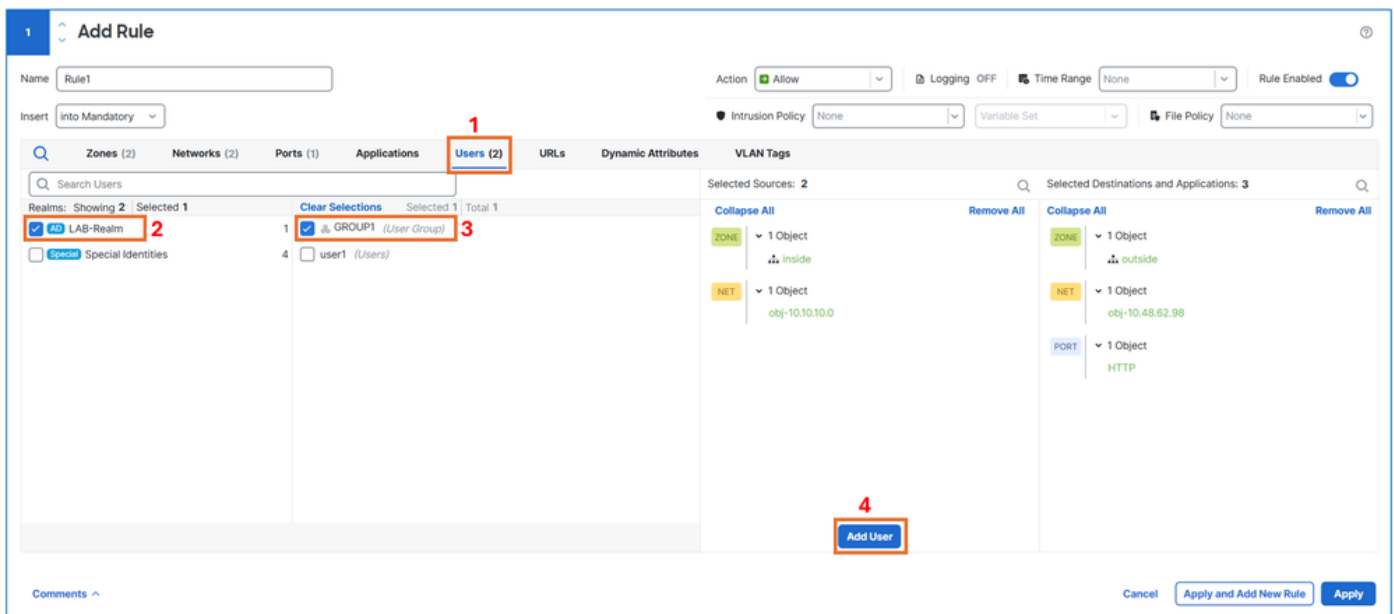
Fare clic sul pulsante Applica

Passaggio 2. Creare la regola di controllo di accesso.



crea ACP

Immettere i dettagli in base ai requisiti dell'attività e, soprattutto, nella scheda Utente, addGROUP1fromLAB-Realm.



aggiungere utenti alla regola

Abilitare la registrazione per la regola selezionando Log alla fine della connessione.

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**

abilitare la registrazione

Passaggio 3. Abilitare la registrazione per l'azione predefinita.

Fare clic sull'icona Impostazioni per modificare le impostazioni di registrazione delle azioni predefinite.

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

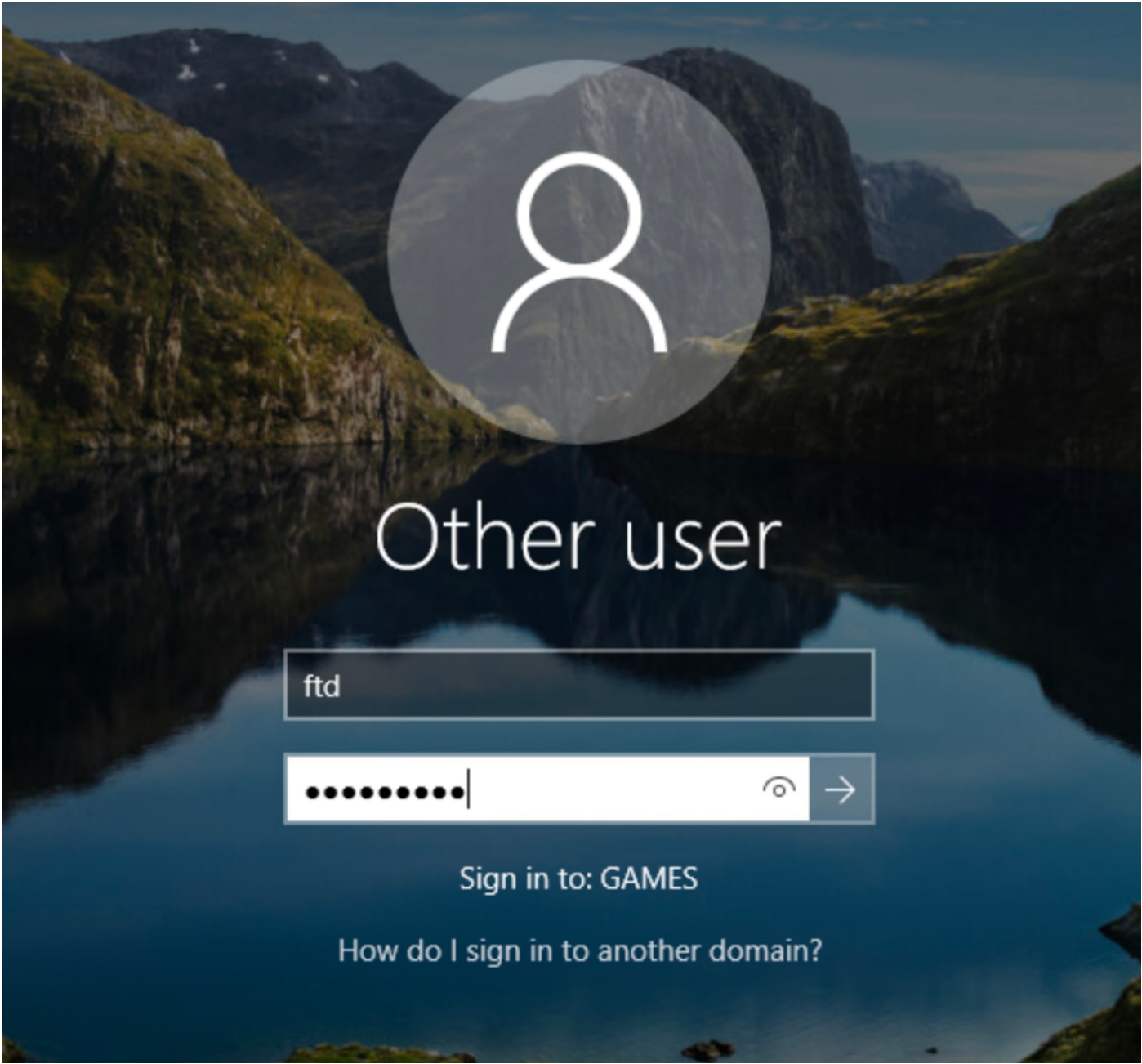
Abilita registrazione

Salvare e distribuire la configurazione sull'FTD.

Verifica

Verificare l'operazione di identità passiva confermando che il traffico è consentito esclusivamente per ftd.

Accedere all'utente del dominio dal computer dell'utente.



accesso utente

Dopo che un utente ha eseguito correttamente l'accesso, verificare da FMC in Analisi > utente > sessione attiva per visualizzare i dettagli dell'utente attivo.

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	

Sessioni attive

Dopo aver avviato la verifica del traffico dagli eventi di connessione, vedere i dettagli utente negli eventi di connessione.

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

Sessioni attive

Risoluzione dei problemi

Controllo dei log dell'agente

Sul computer Windows che ospita l'agente, aprire Task Manager e verificare che il processo in background CiscoPassiveIdentityAgentService sia in esecuzione.

Task Manager

File Options View

Processes Performance Users Details Services

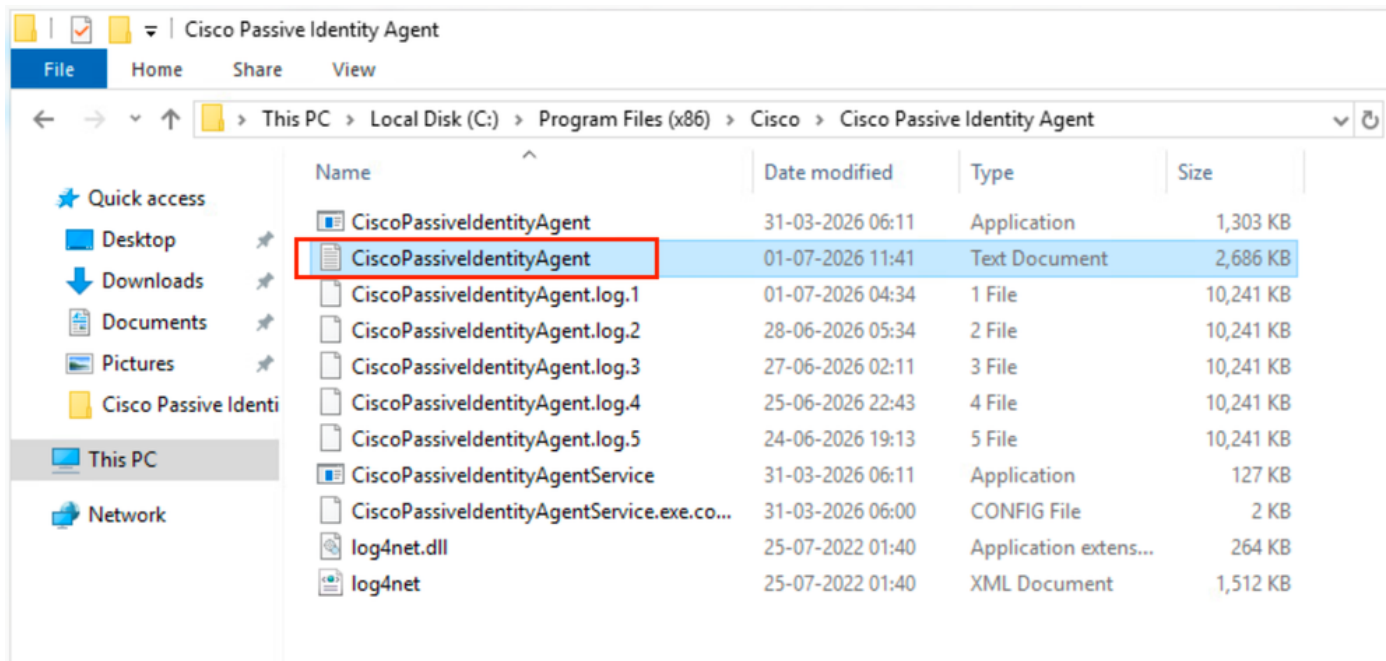
Name	Status	2% CPU	27% Memory
> Task Manager		0%	24.4 MB
> Windows Explorer		0%	37.3 MB
> Server Manager		0%	34.1 MB
Background processes (32)			
> Distributed File System Replicati...		0%	8.3 MB
▼ CiscoPassiveIdentityAgentServi... Cisco Passive Identity Agent		0%	15.4 MB
> Microsoft.ActiveDirectory.WebS...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

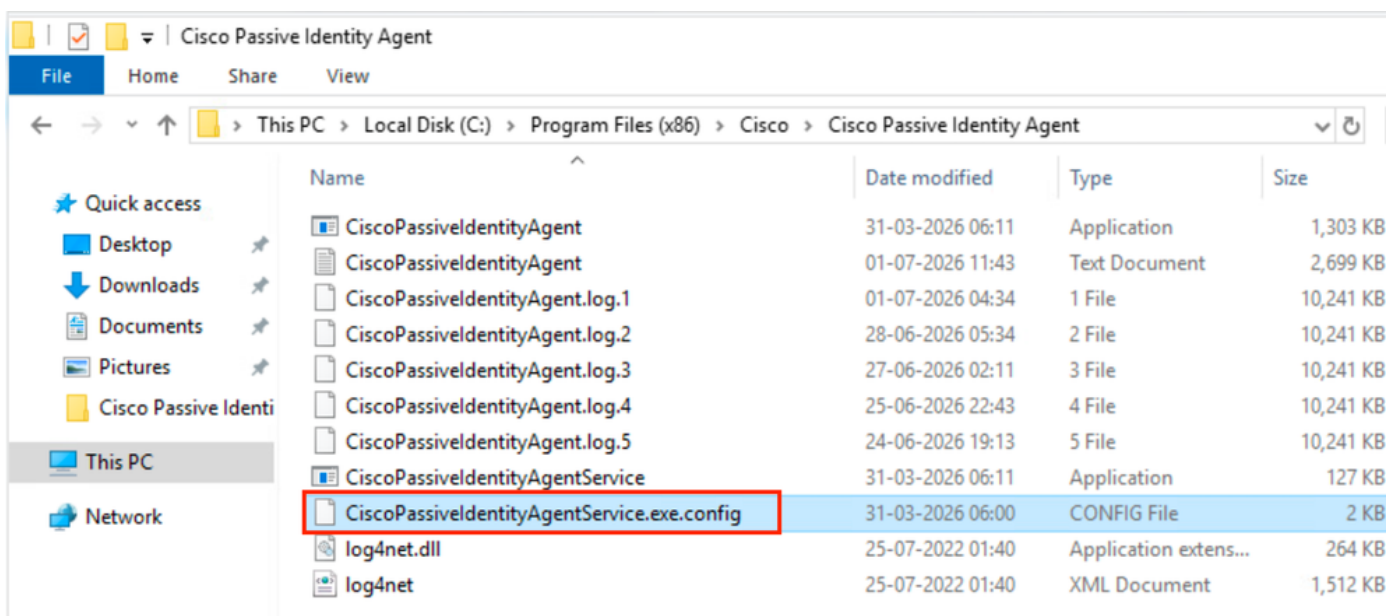
Attività in esecuzione

I registri dell'agente sono disponibili nei file CiscoPassiveIdentityAgent, che per impostazione predefinita si trovano in: "C:\Program Files (x86)\Cisco\Cisco Passive Identity Agent\".



agente

Per impostazione predefinita, i log dell'agente sono impostati sul livello INFO. Per abilitare la registrazione a livello DEBUG, modificare CiscoPassiveIdentityAgentService.exe.configfile e impostare il livello di registrazione su ALLO DEBUG.



configurazione agente



```
File Edit Format View Help
<?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>
```

registro informazioni

Controllo dei registri dell'agente - Recupero della configurazione dell'agente.

Client inattivo INFO, eventi in blocco: [f"domain":"games.cisco.com", "srcIpAddress": "X.X.X.X",
"user": "fdm", "timestamp": "2026-07-01T19

Client inattivo INFO, stato mapping: OK

INFO Rest Client, POST REST riuscito per userBatch fdm, latenza = 0, ora corrente DC in UTC:
07/01/2026 19:47:34 Utente registrato a

INFO Rest Client, richiesta configurazione agente

Registri FMC

Eseguire questo comando per verificare se il mapping utente-IP è stato ricevuto dall'agente.

```

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#

```

uscita fmc

Se il comando precedente non mostra alcuna mappatura, raccogliere i log e contattare Cisco TAC.

Elenco dei registri pertinenti per l'API del CCP. Il log di coda racchiude tutti questi elementi.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).