Configurare l'agente di identità passiva utilizzando FMC

Sommario

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.

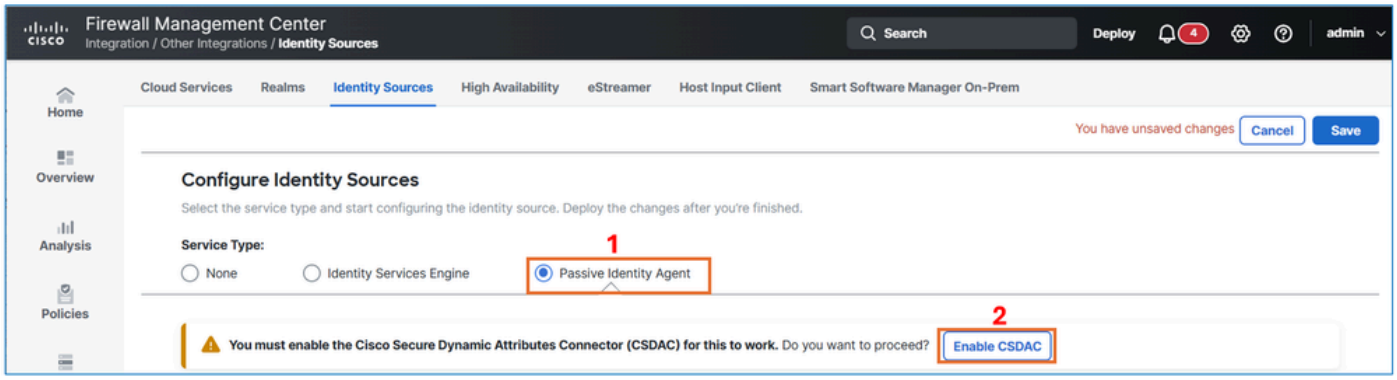
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazioni

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

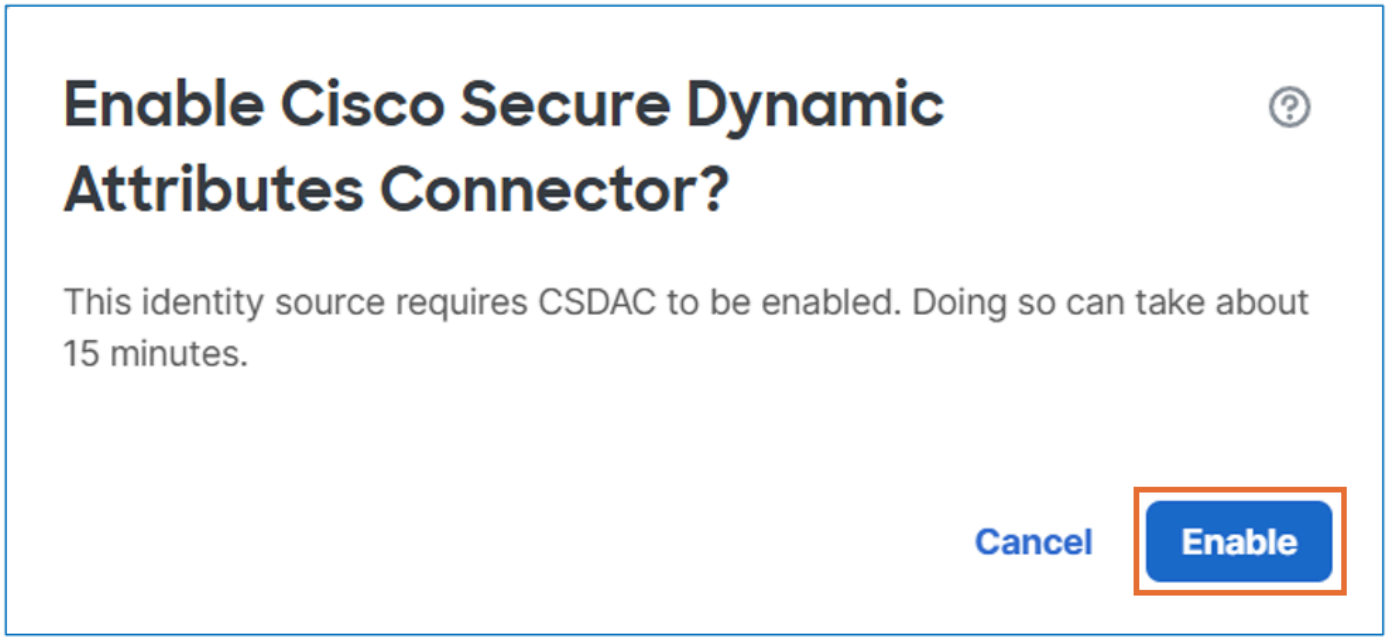
Configurazione di un'origine dell'agente di identità passiva

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.



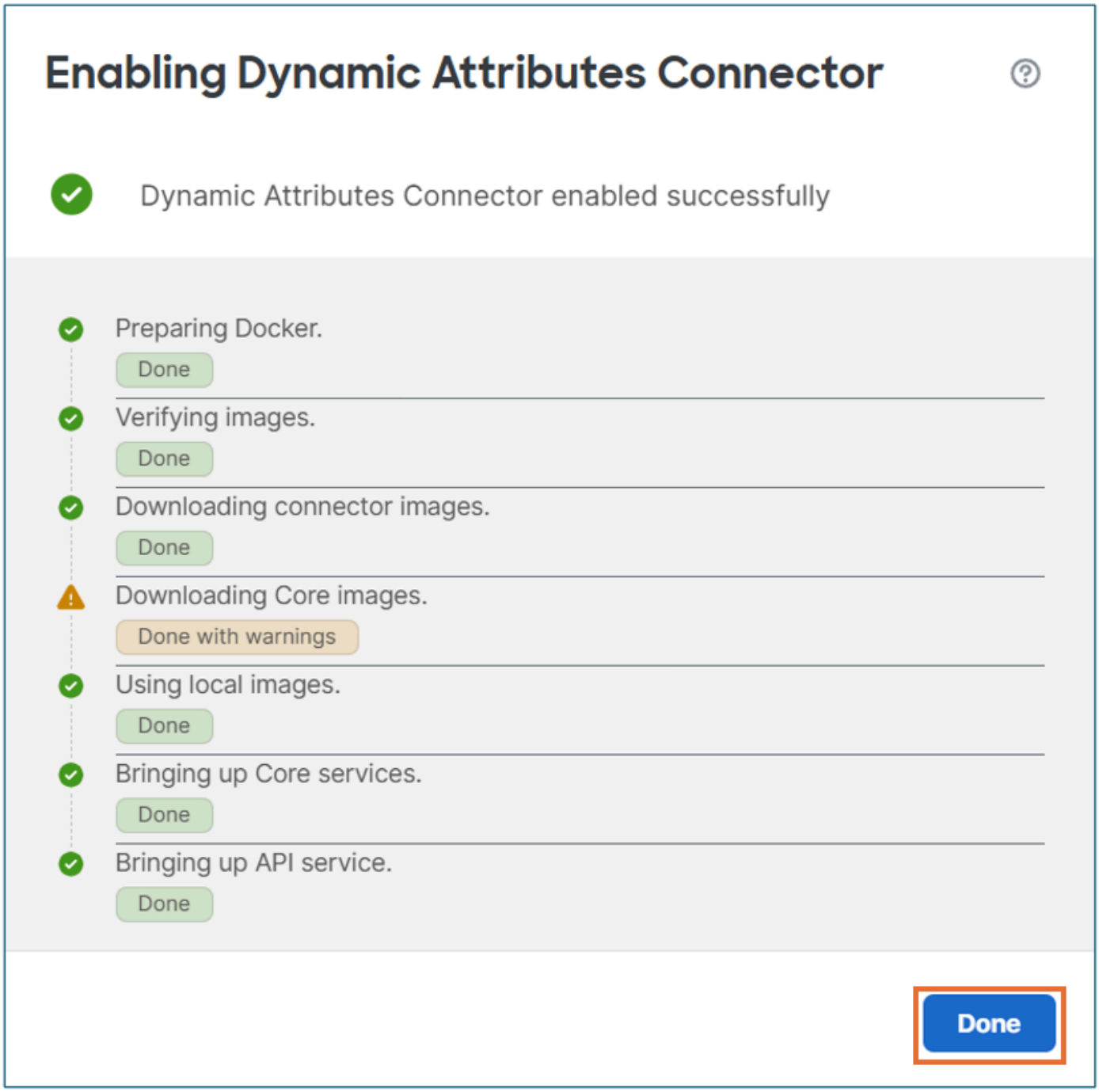
Passive Identity Agent

Fare clic sul pulsante Abilita per abilitare CSDAC.



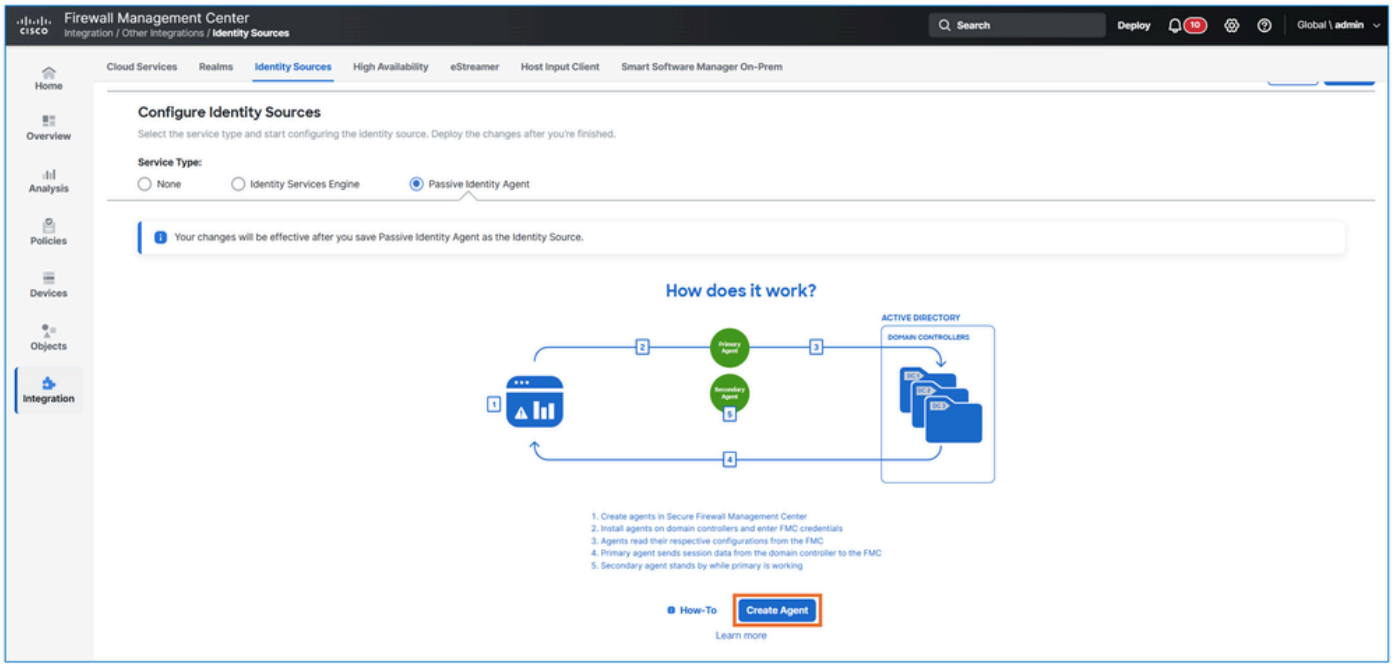
Abilita CSDAC

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



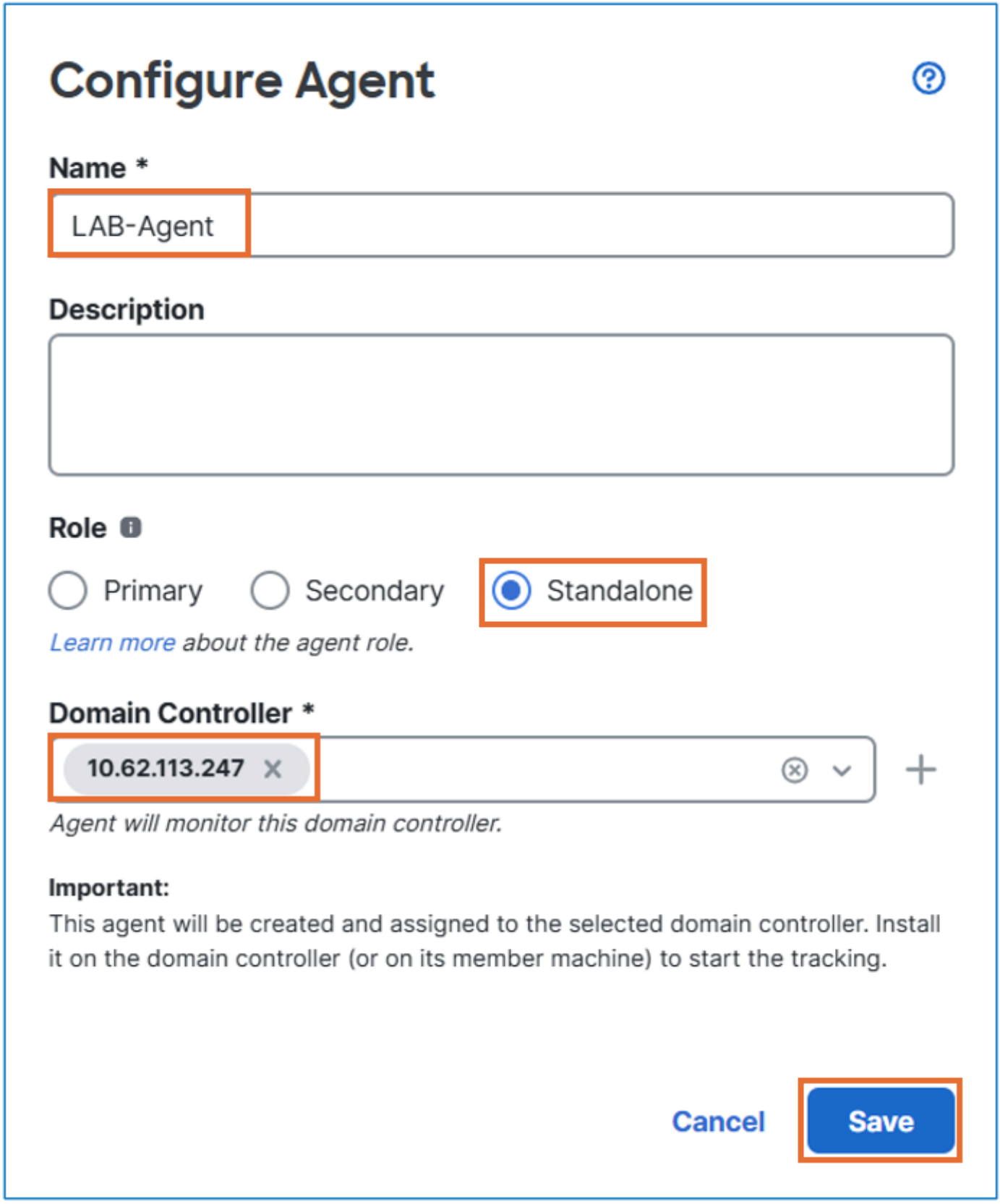
CSDAC abilitato

Fare clic sul pulsante Crea agente.



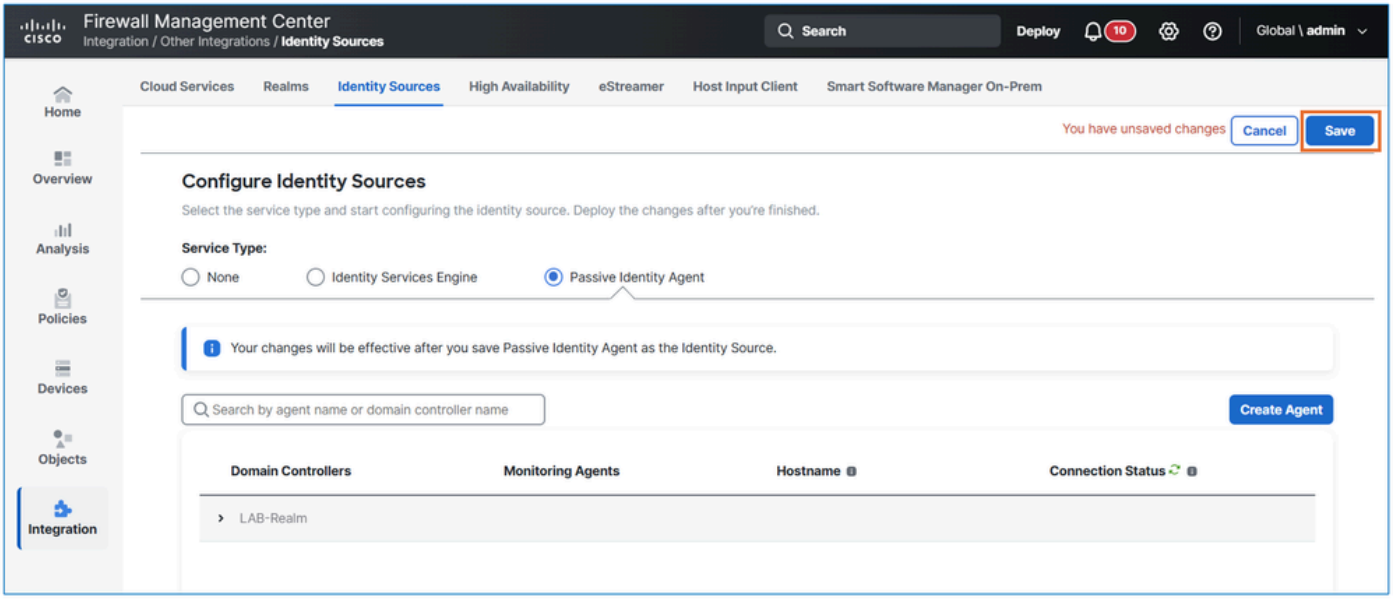
Crea agente

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



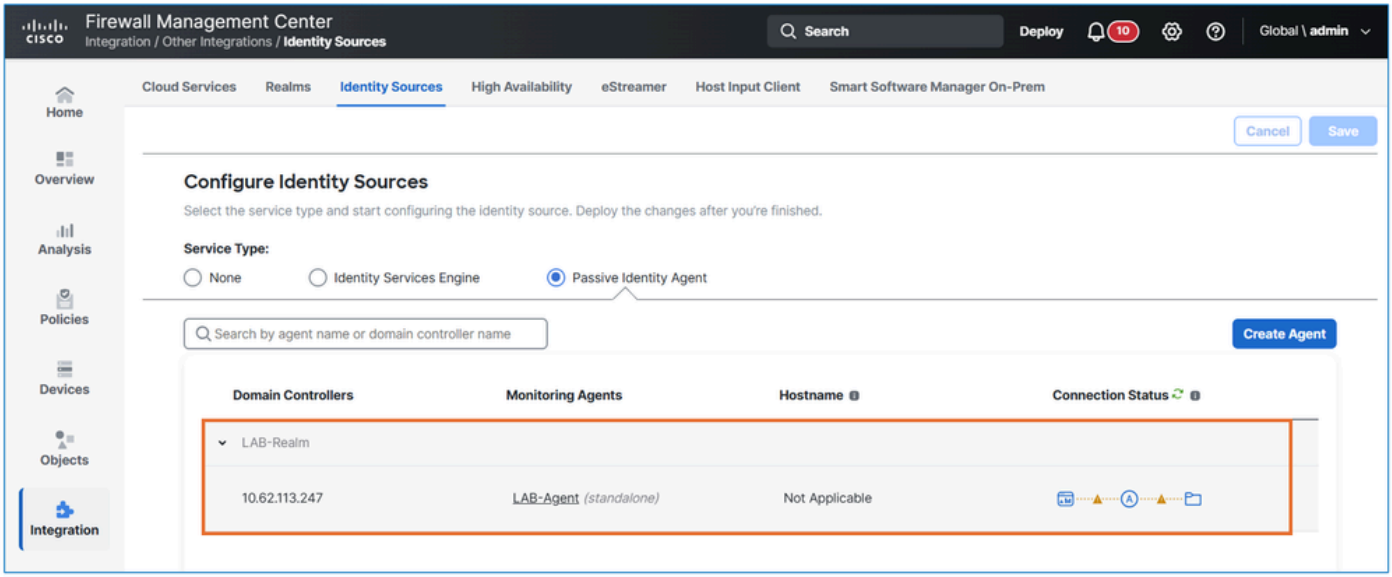
Configura agente

Fare clic sul pulsante Salva.



Salvare la configurazione

Il risultato.



Verifica dello stato

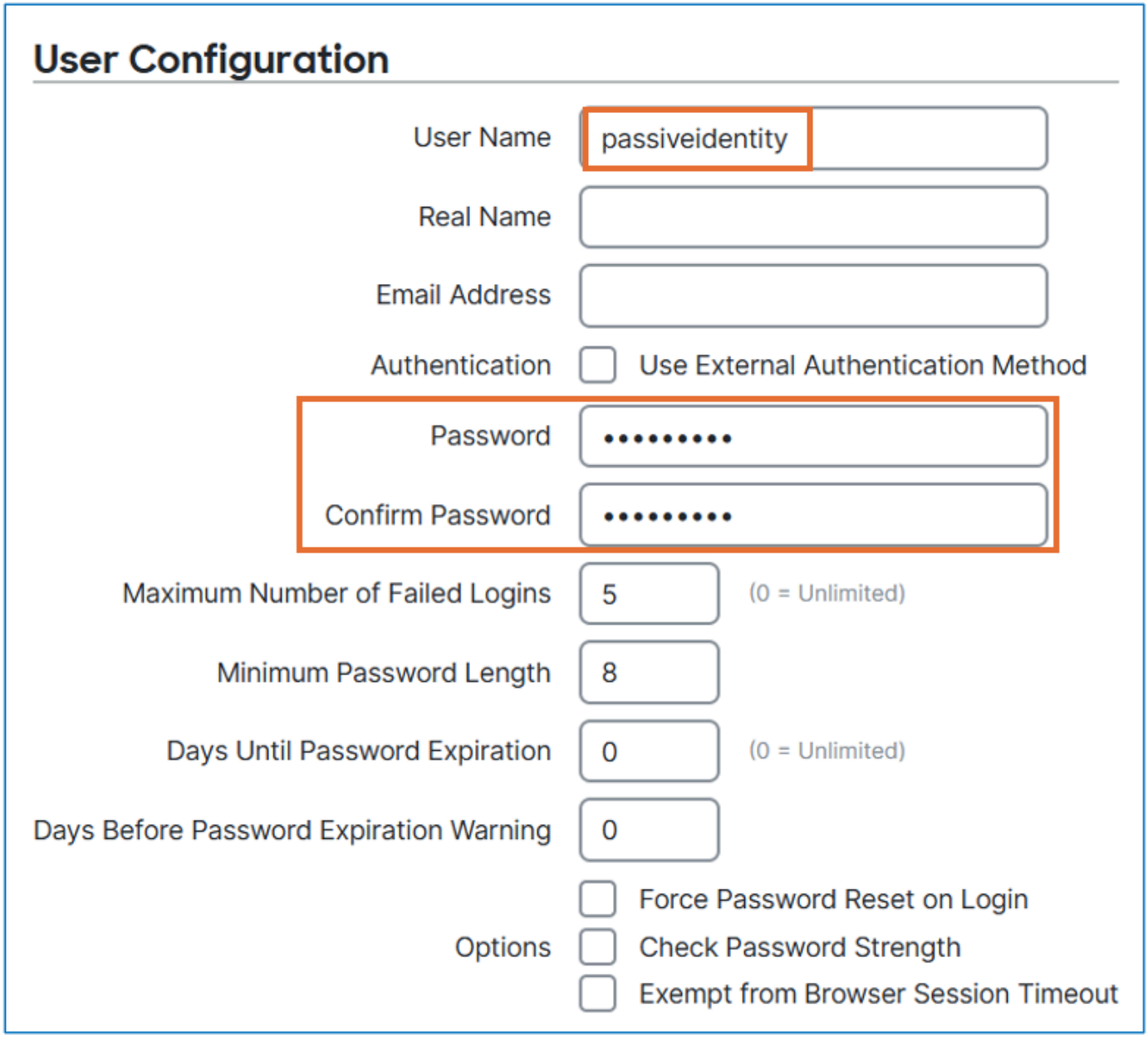
Nota: L'agente di identità passiva indica lo stato utilizzando delle righe. Il colore ambra indica che l'agente non ha mai comunicato correttamente con il centro di gestione Secure Firewall. Una nuova linea dell'agente è di colore ambra e rimane tale fino al completamento della configurazione.

Creazione di un utente Passive Identity Agent in Secure Firewall Management

Center

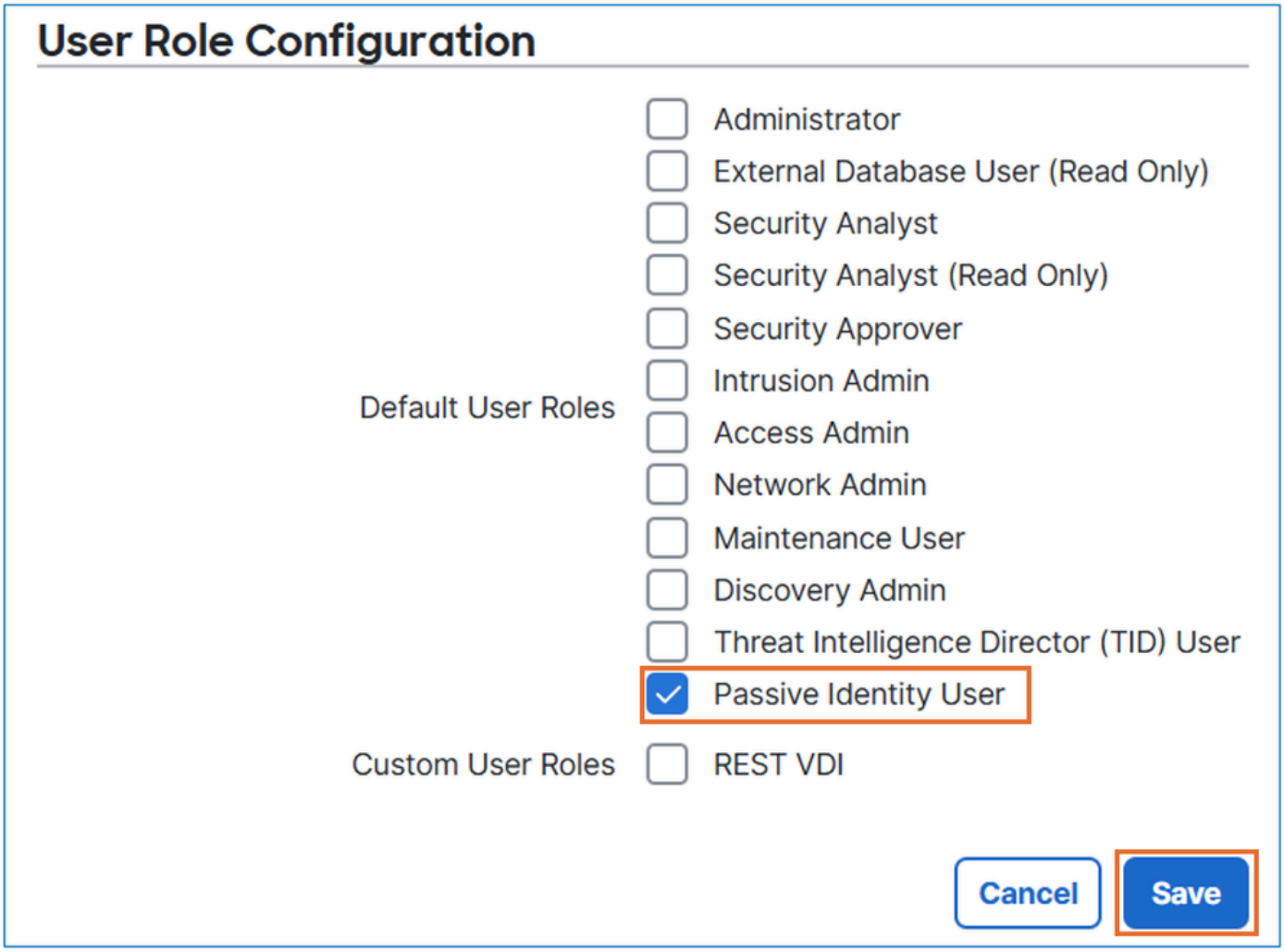
Creare un utente di Centro gestione firewall sicuro con autorizzazioni sufficienti per comunicare con l'agente di identità passiva. L'utente dispone di privilegi limitati per eseguire altre attività. l'utente deve abilitare solo la comunicazione con l'agente di identità passiva.

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



Crea utente

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

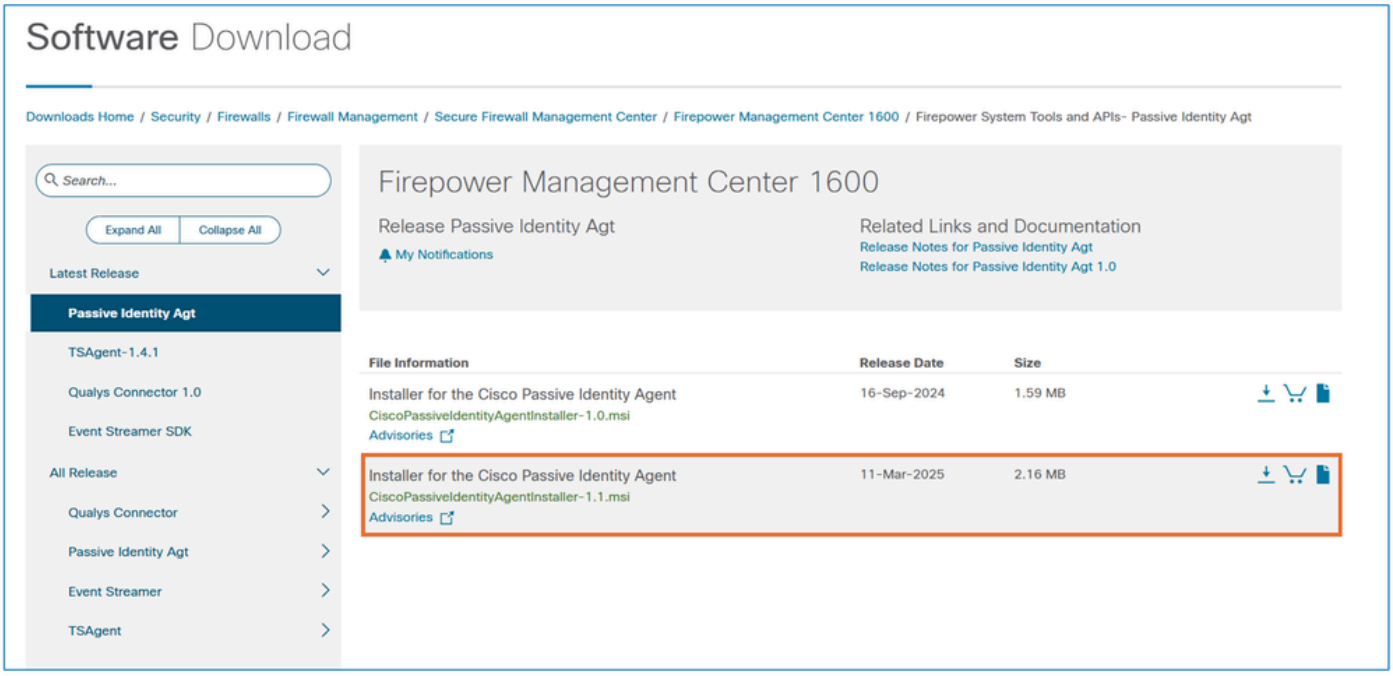


selezionare l'utente dell'identità passiva

Installare e configurare il software Passive Identity Agent

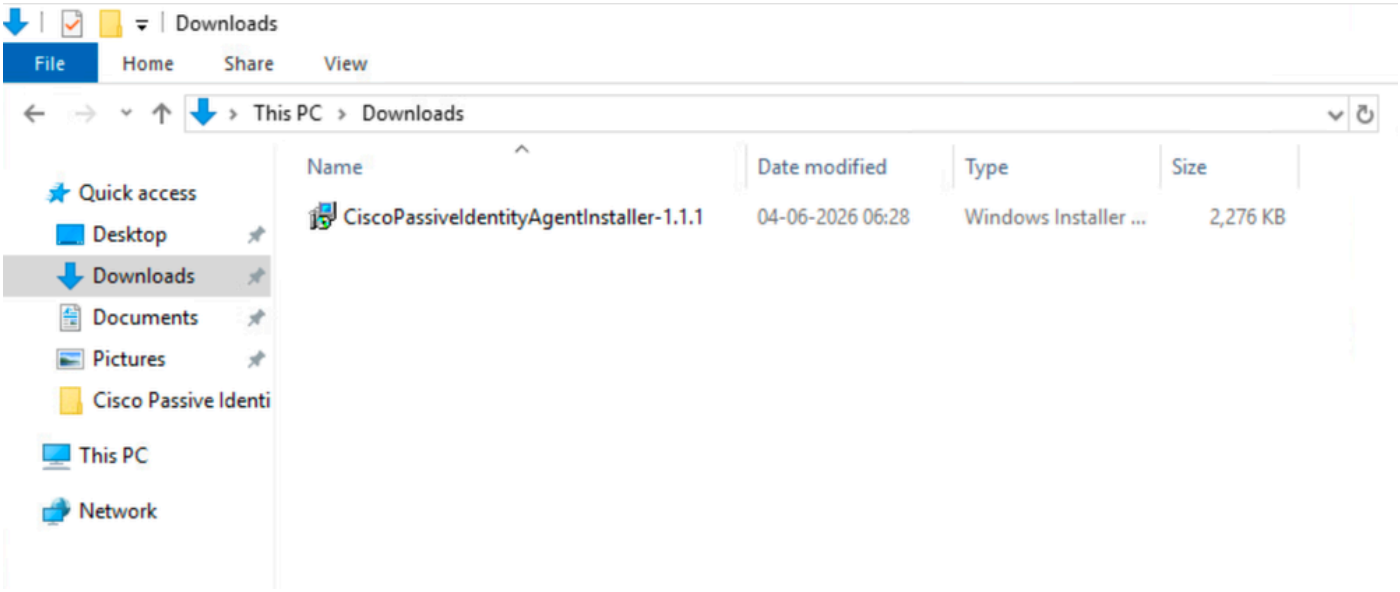
Installare e configurare il software Passive Identity Agent nel controller di dominio designato.

Scaricare l'agente di identità passiva da software.cisco.com.



scaricare il software

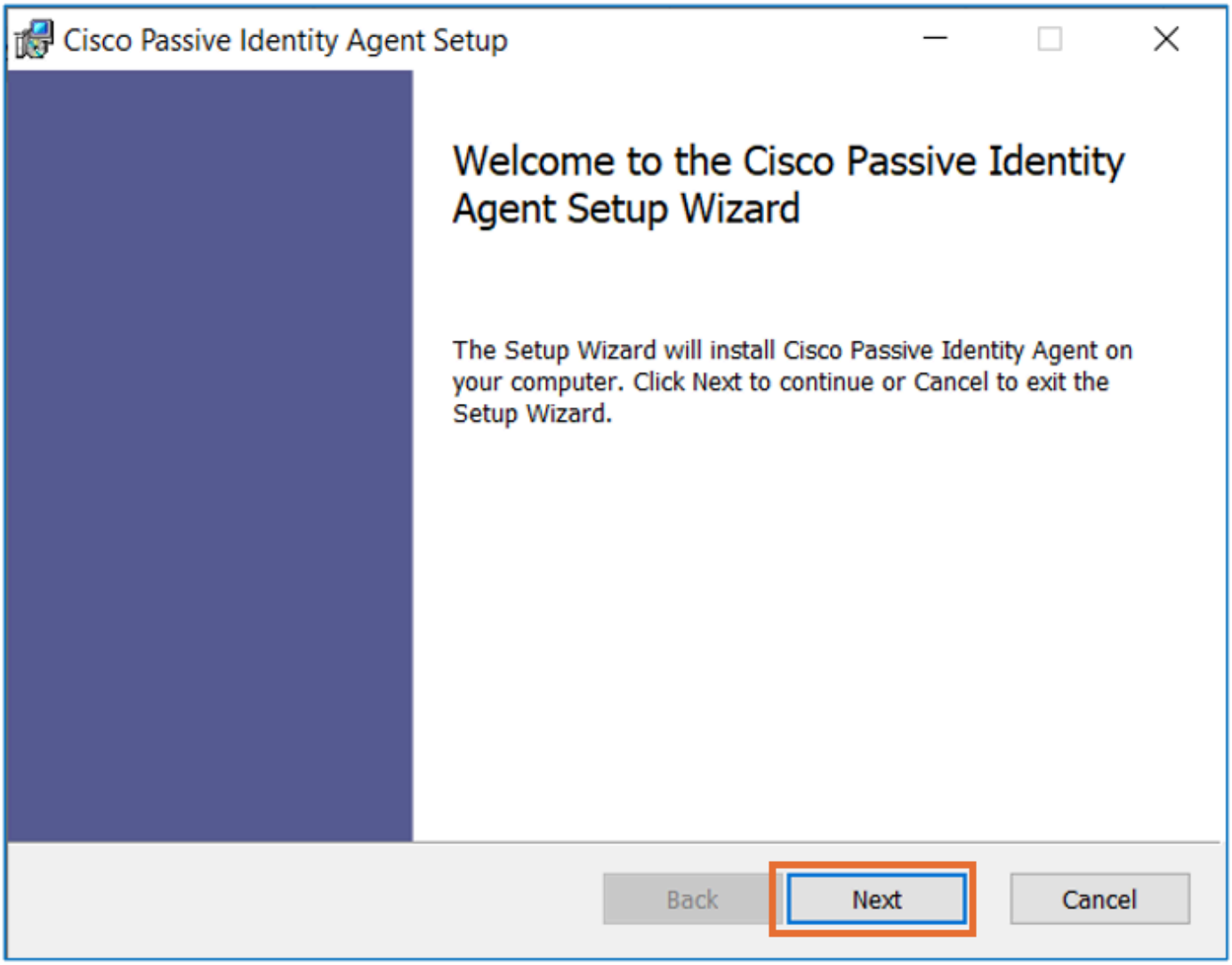
Dopo aver scaricato l'agente, avviare il processo di installazione nel controller di dominio.



agente

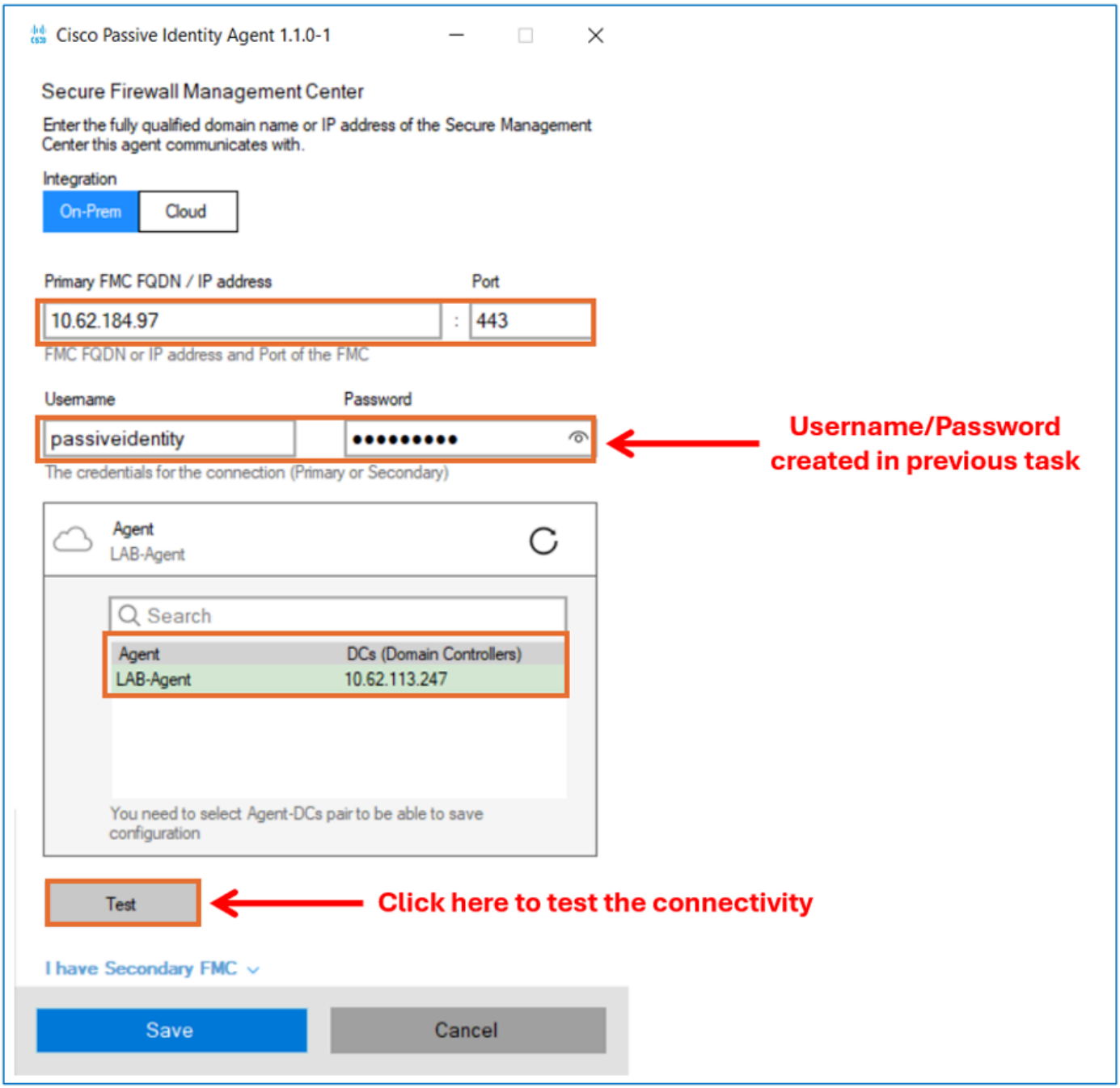
]

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



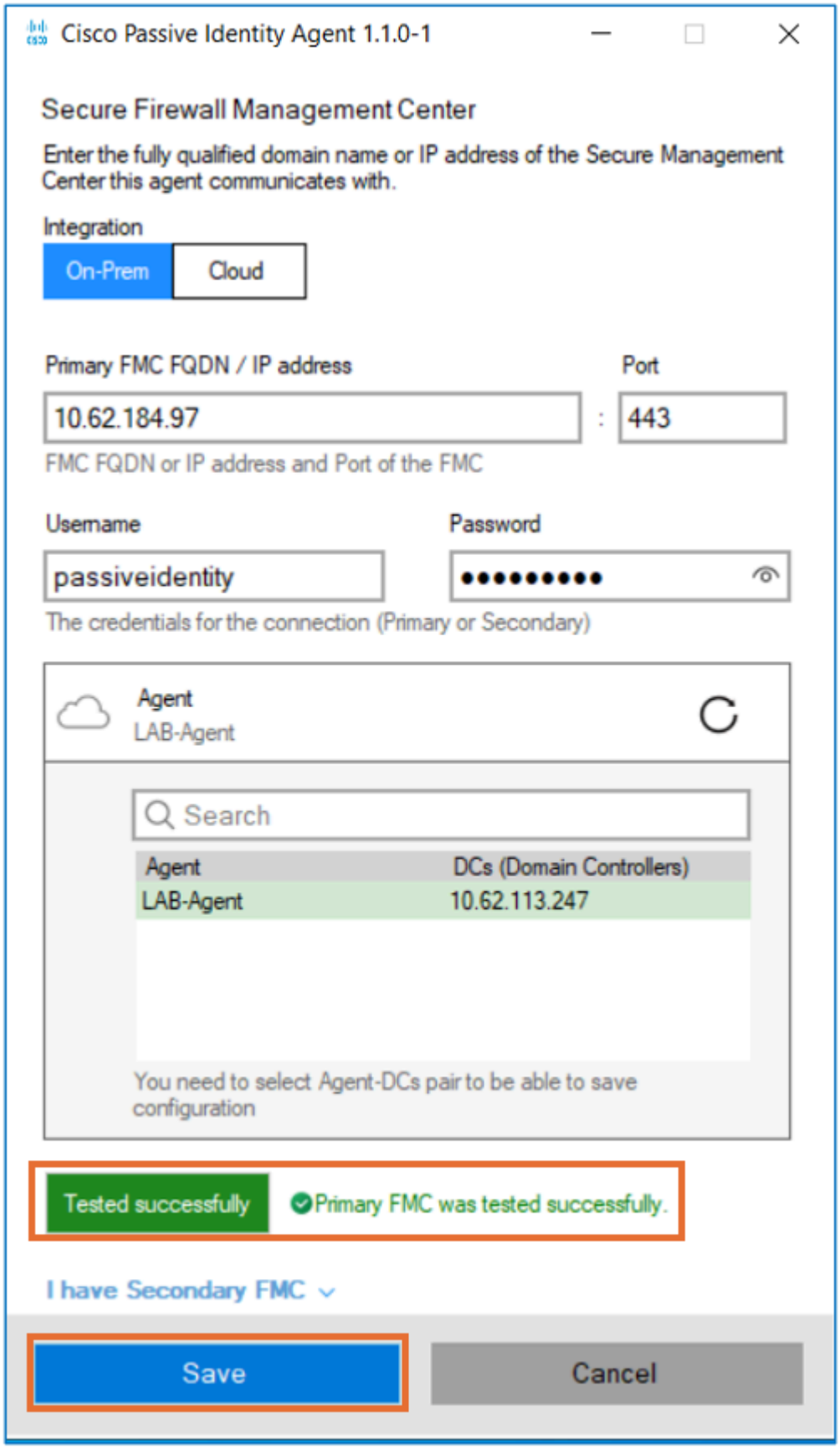
Install

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.



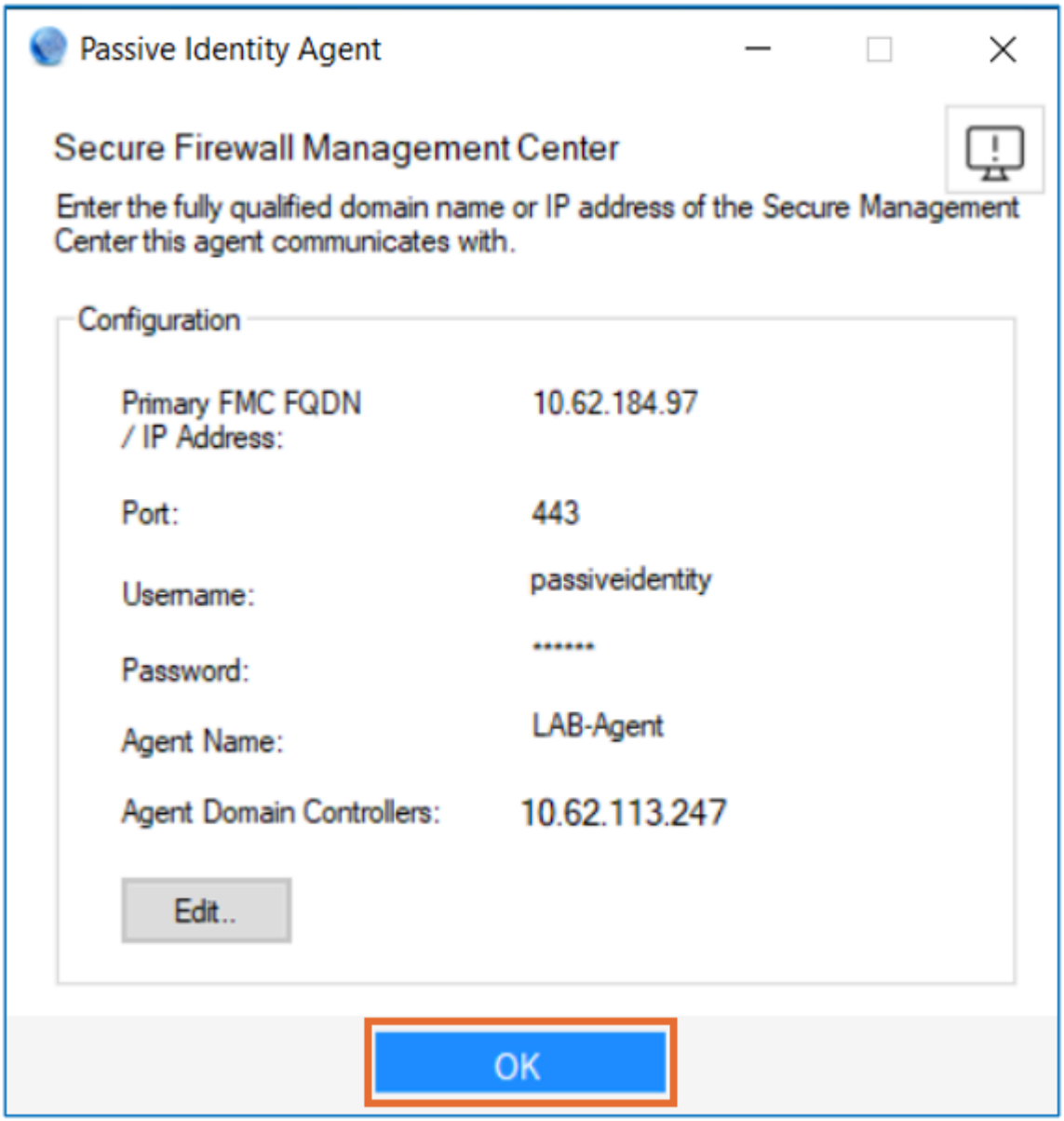
configurare l'agente.

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



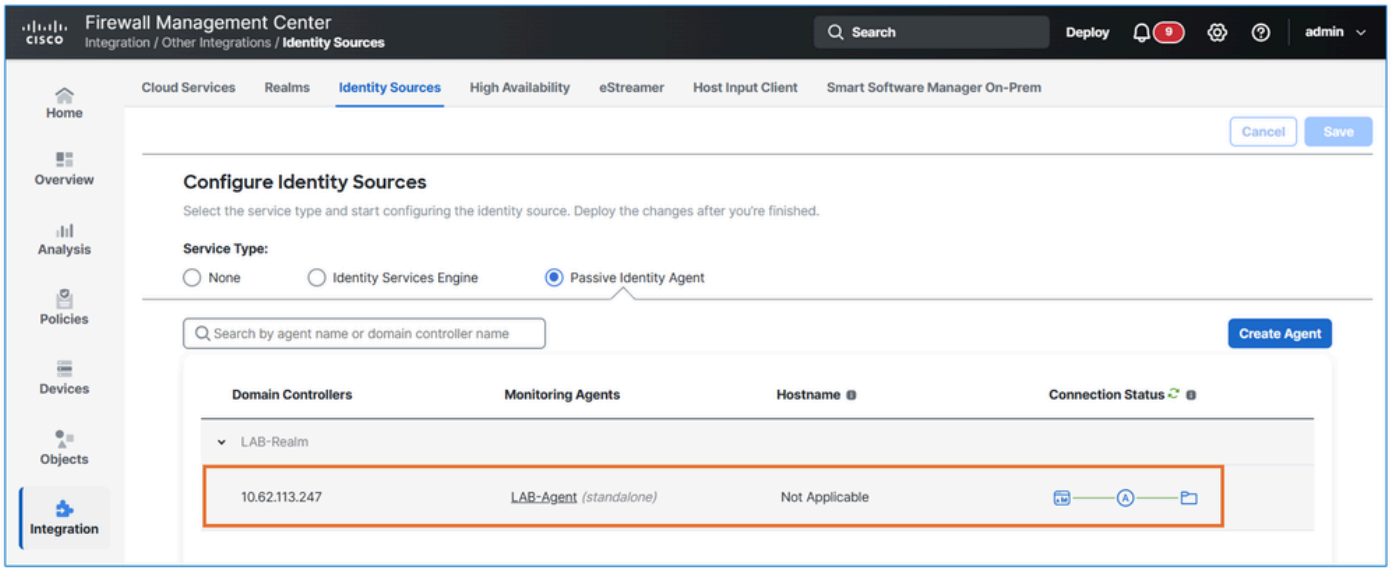
test

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



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.



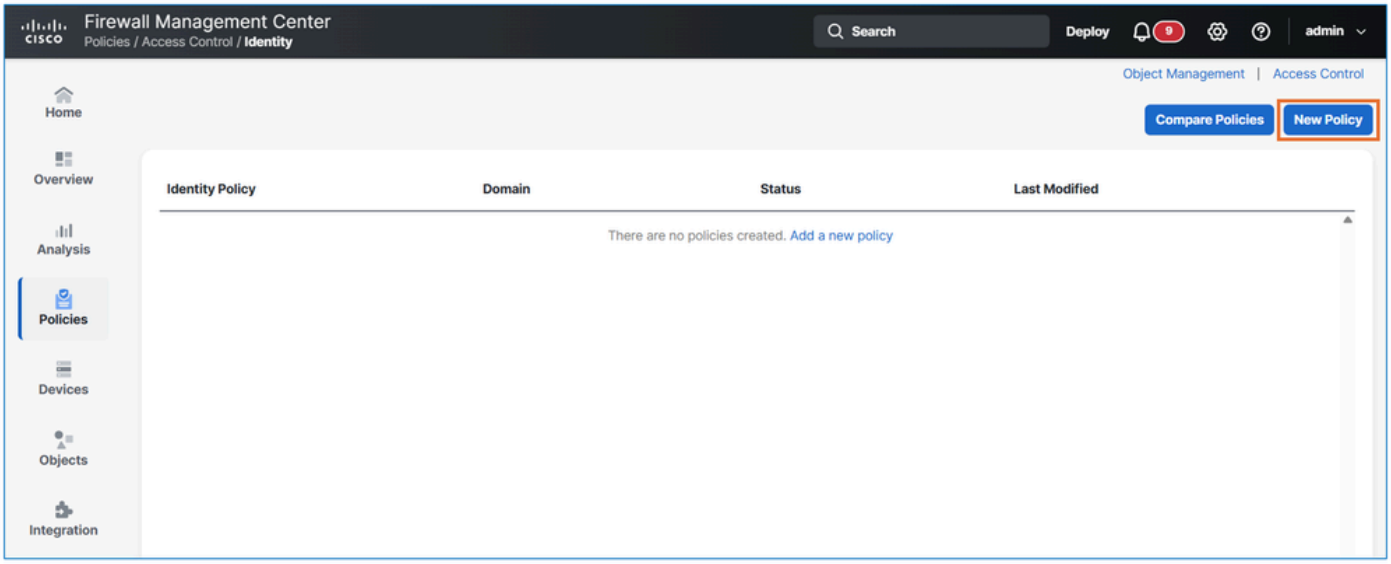
verifica la comunicazione da fmc

Configura criteri di identità

Creare un criterio di identità in base alla tabella fornita.

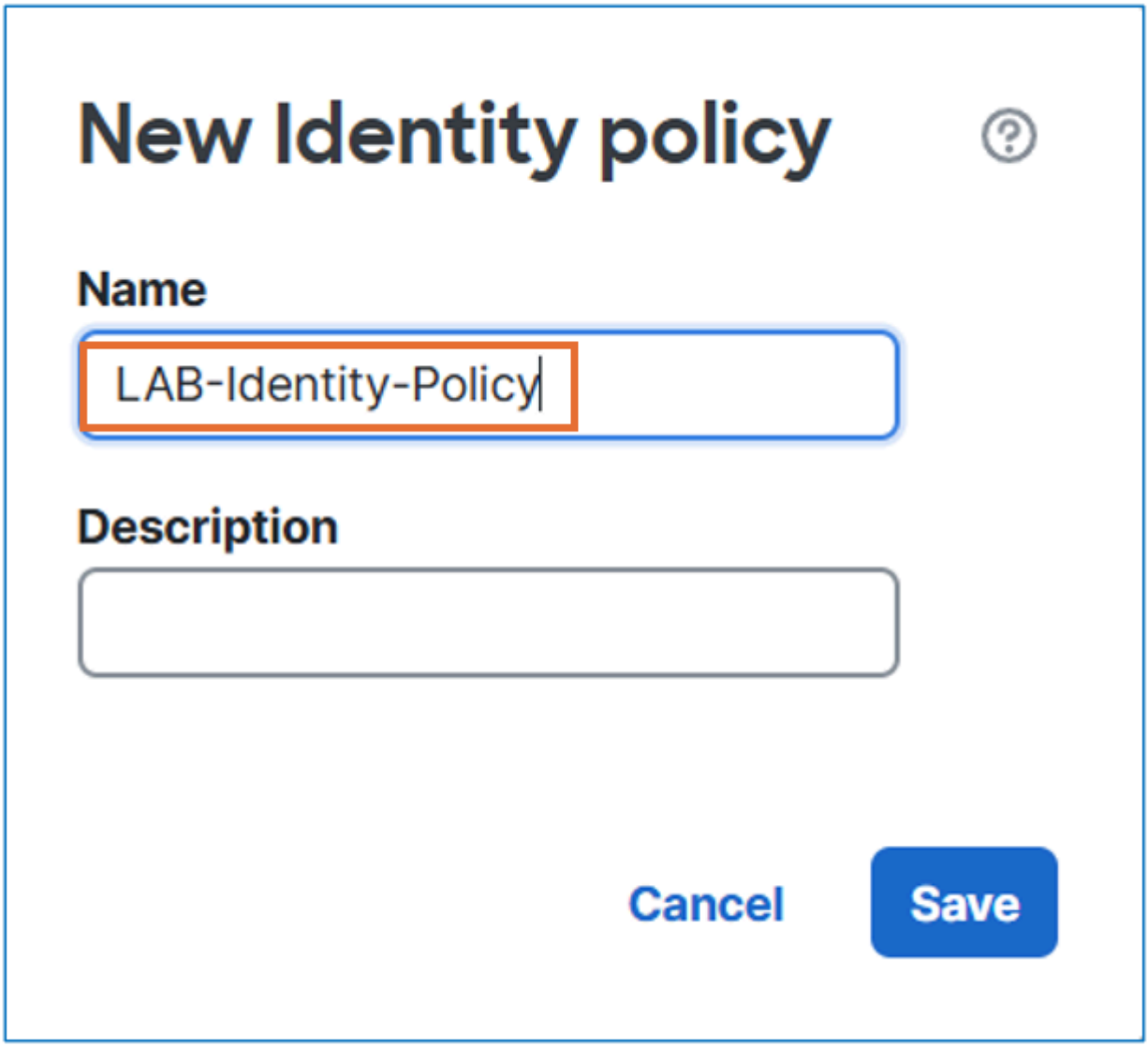
Nome criterio	Nome regola	Realm di autenticazione	Impostazioni rimanenti
LAB-Identity-Policy	Regola1	Area di autenticazione	Lascia come predefinito

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



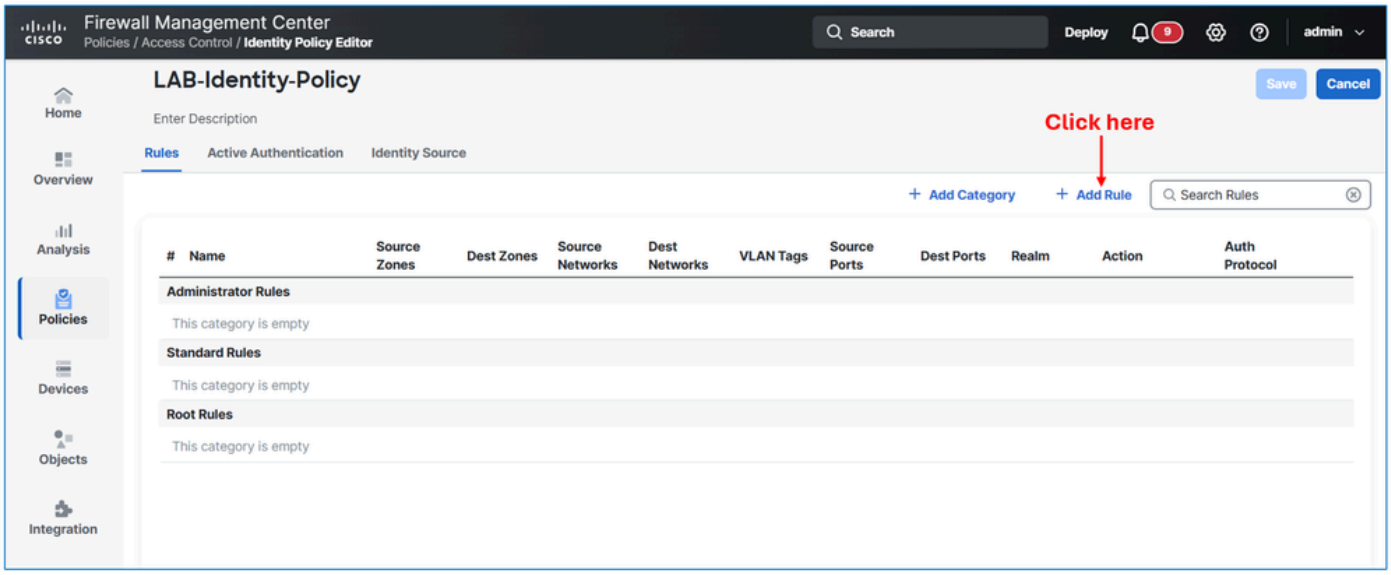
nuovo criterio

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



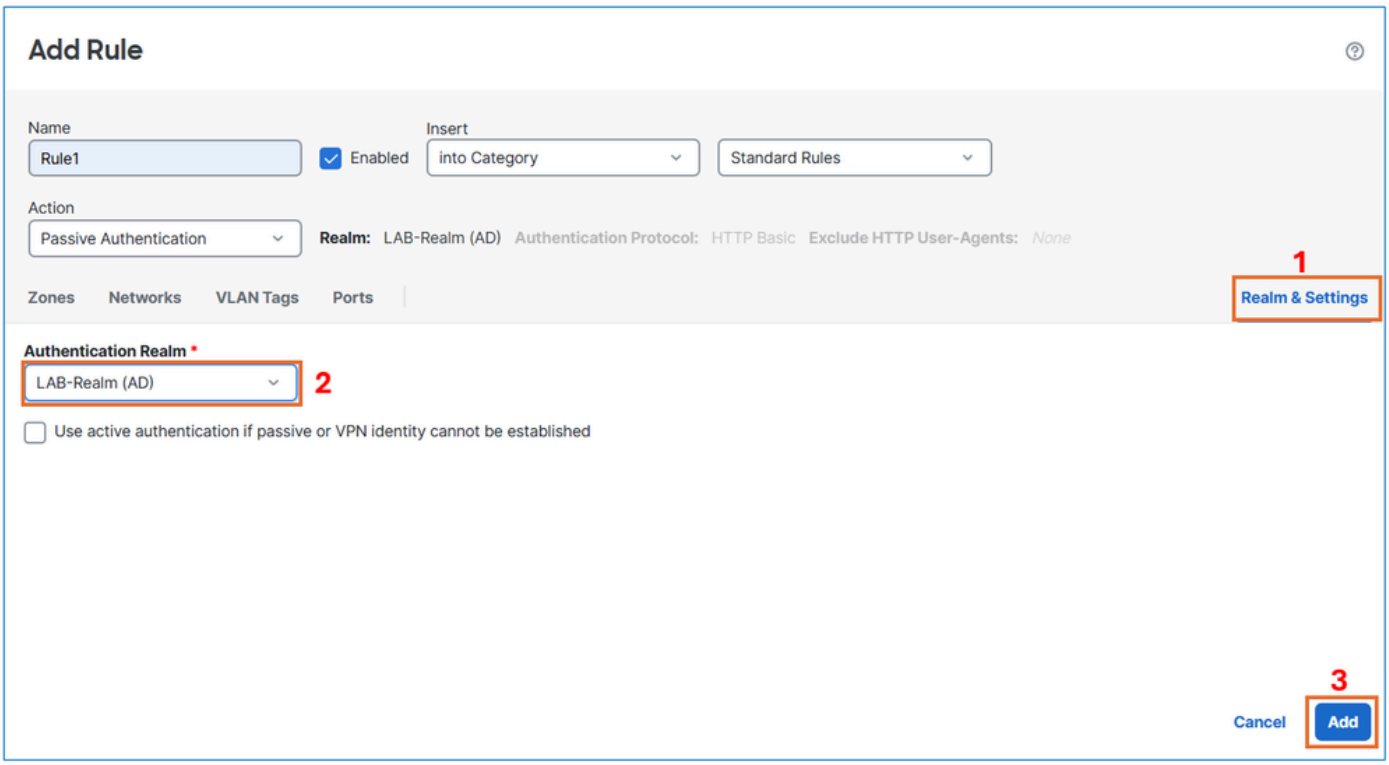
nuovo criterio

Fare clic sul pulsante Aggiungi regola.



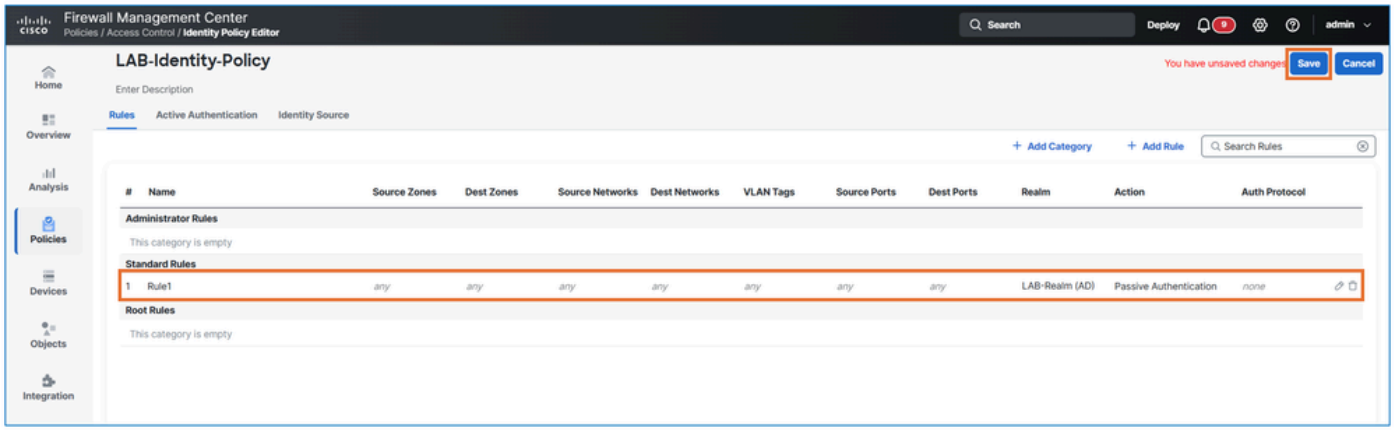
crea regola

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

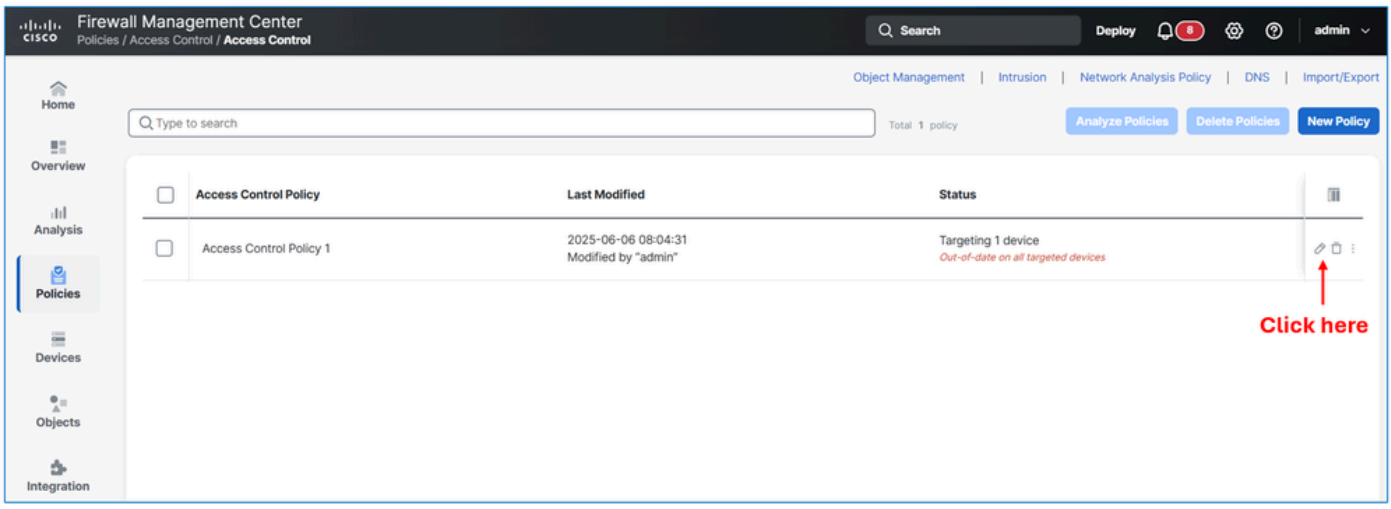
Configura criteri di controllo di accesso

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

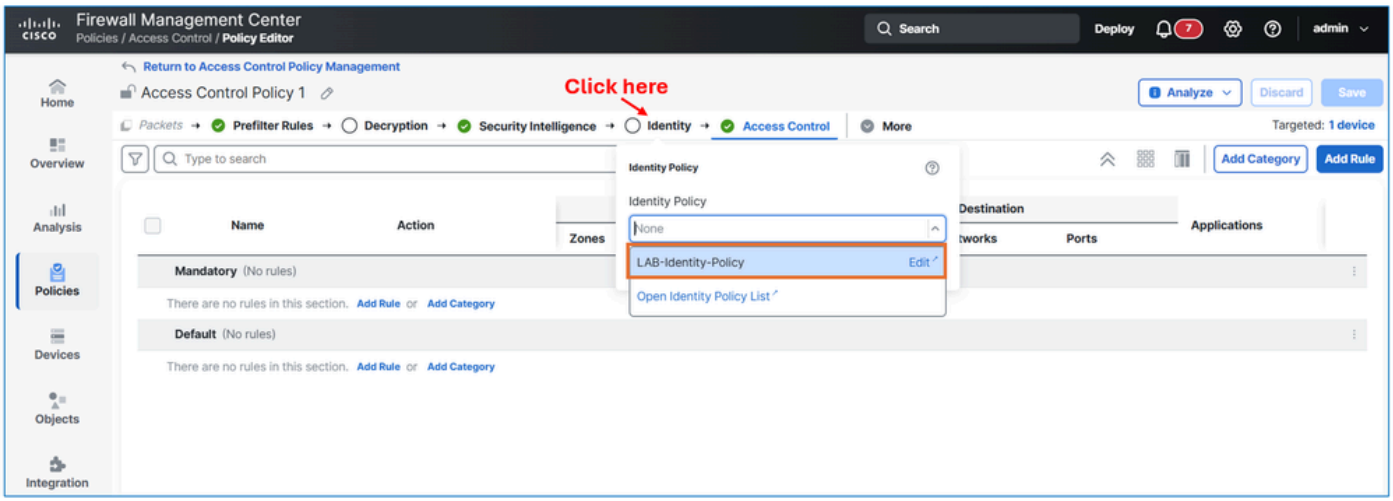
Passaggio 1. Collegare il criterio di identità al criterio di controllo di accesso

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



Modifica criterio

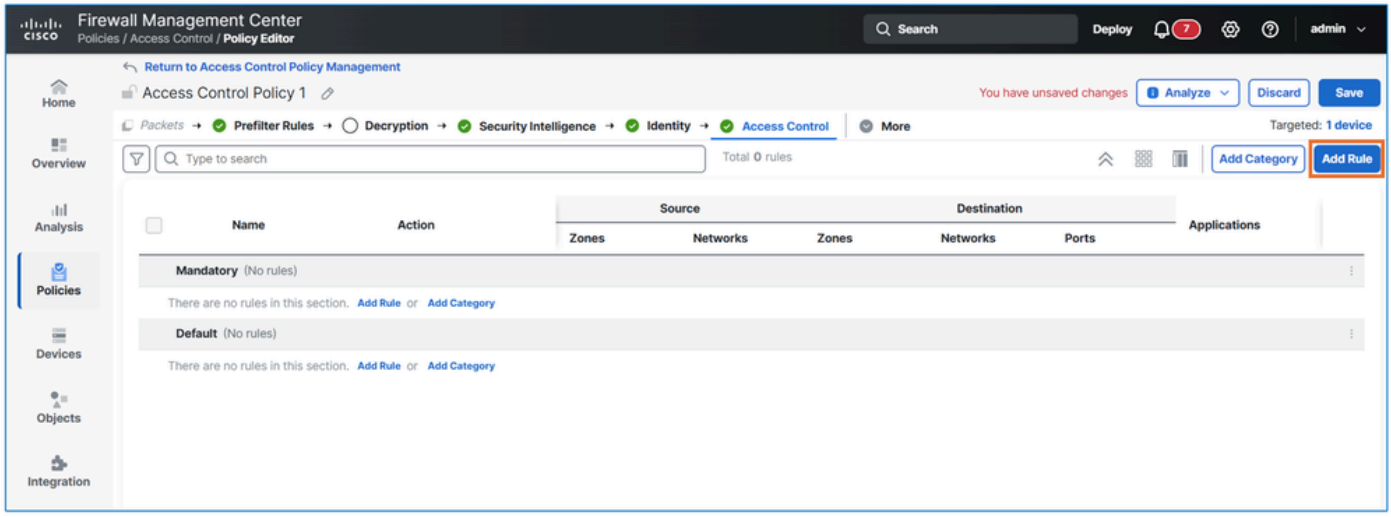
Passare alla sezione Identity e collegare il criterio di identità creato nell'attività precedente.



aggiungi criterio di identità

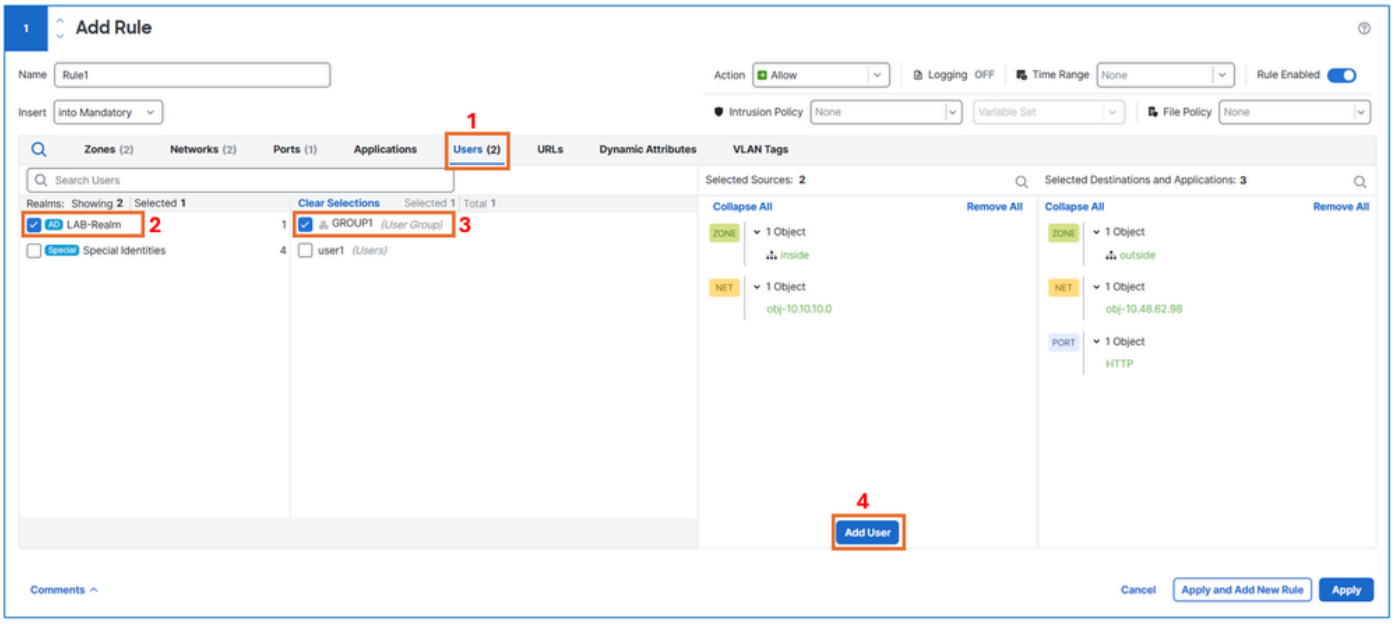
Fare clic sul pulsante Applica

Passaggio 2. Creare la regola di controllo di accesso.



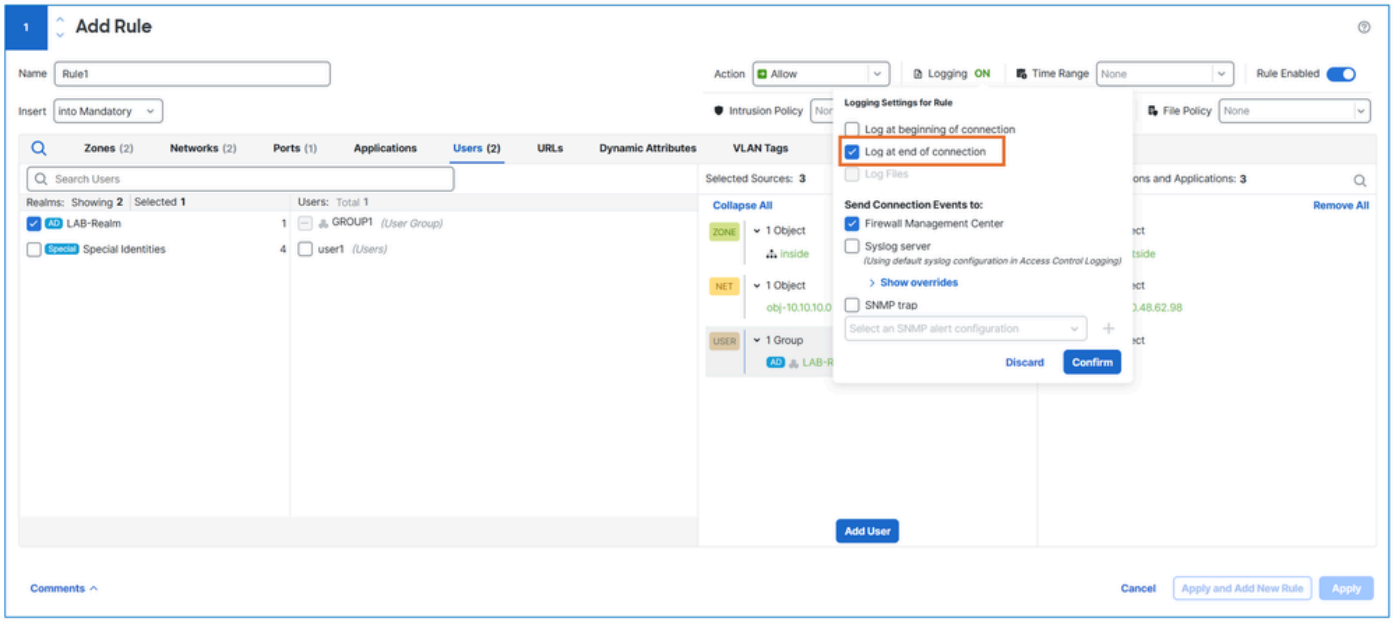
crea ACP

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



aggiungere utenti alla regola

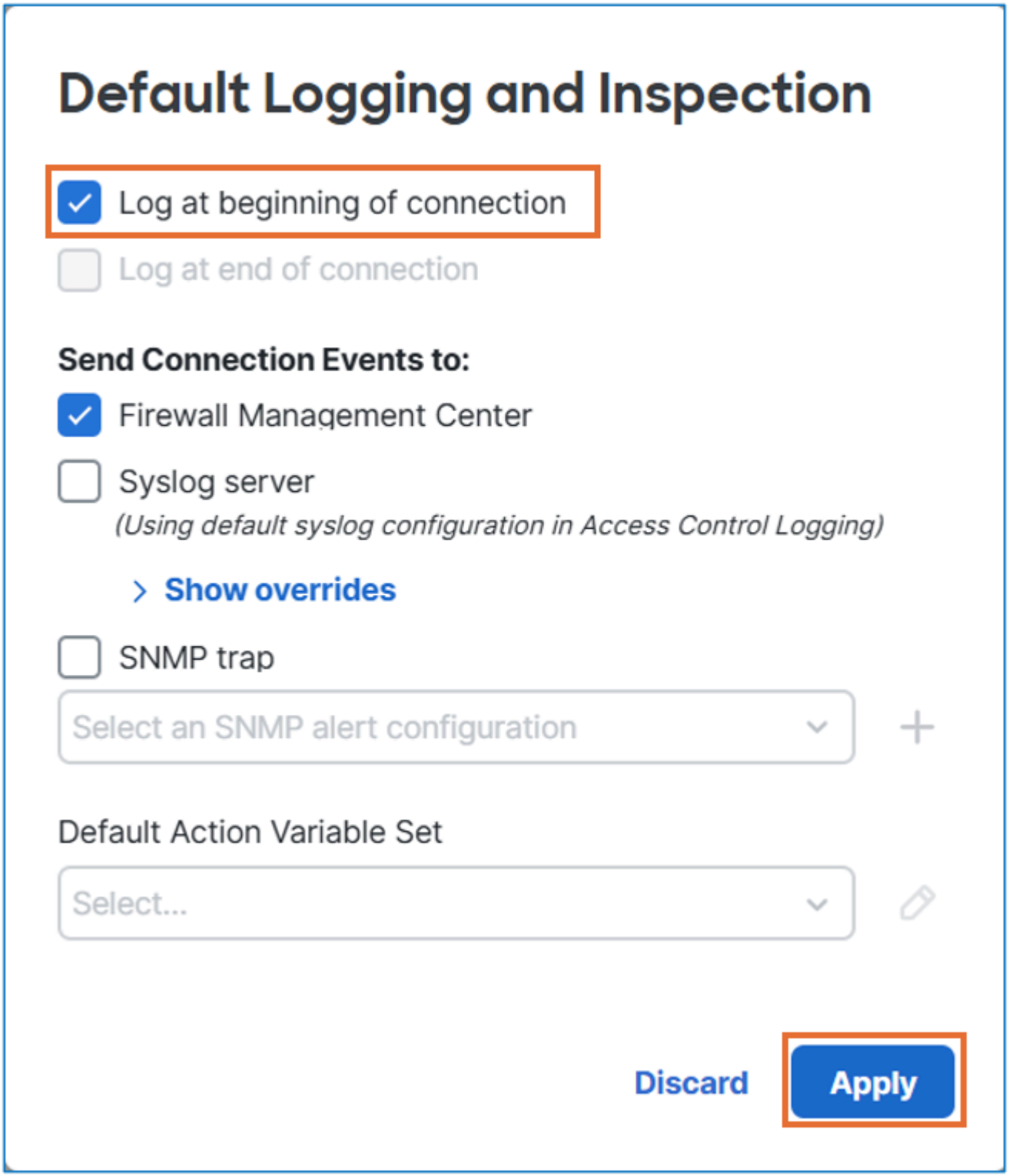
Abilitare la registrazione per la regola selezionando Log alla fine della connessione.



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.



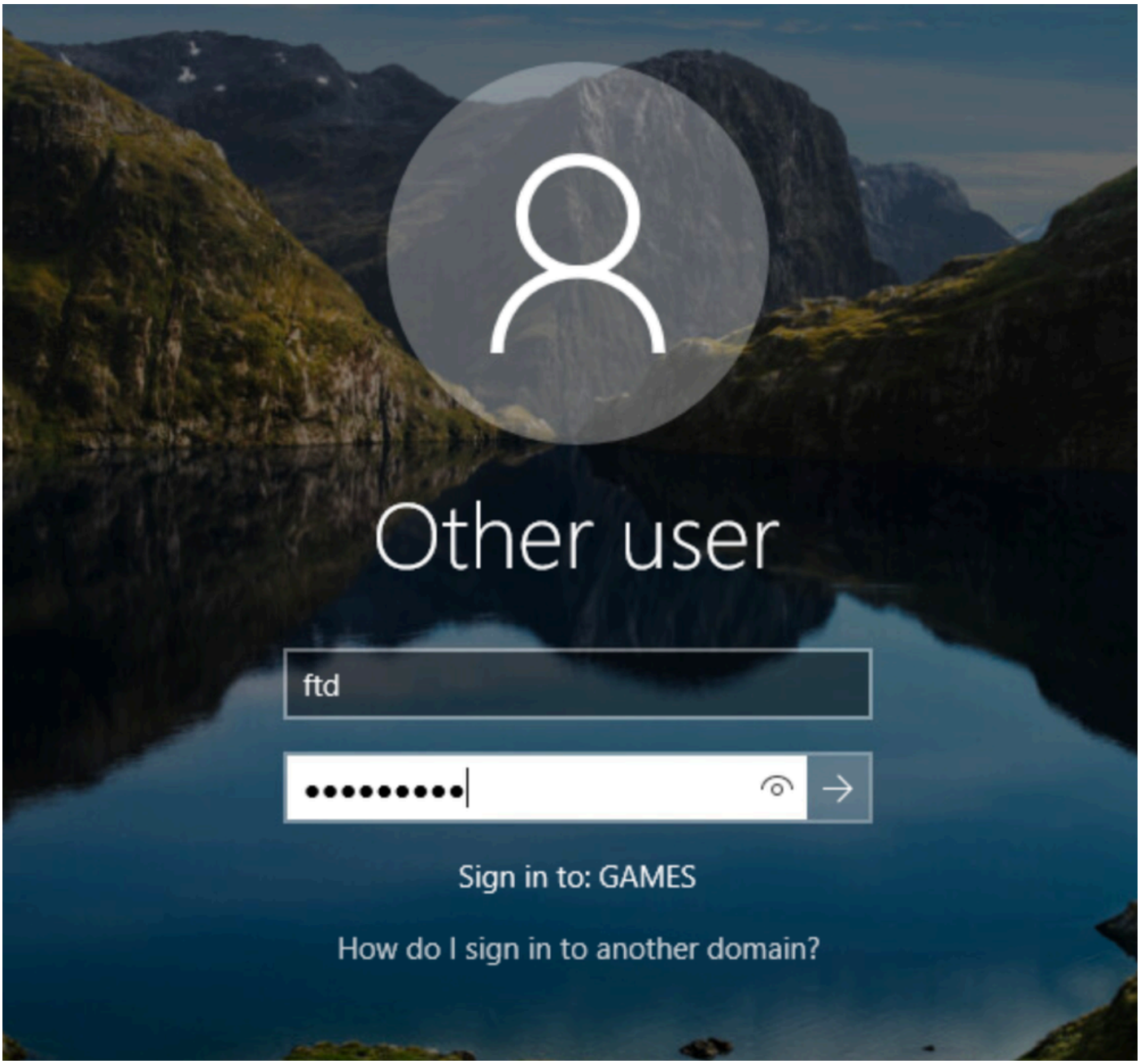
Abilita registrazione

Salvare e distribuire la configurazione sull'FTD.

Verifica

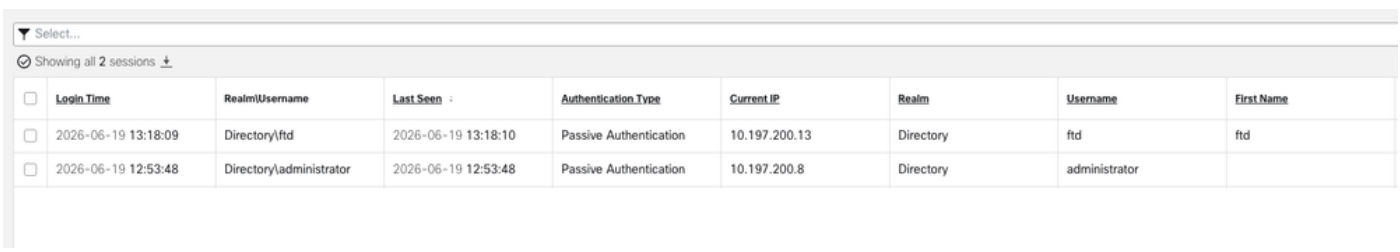
Verificare l'operazione di identità passiva confermando che il traffico è consentito esclusivamente per ftd.

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.



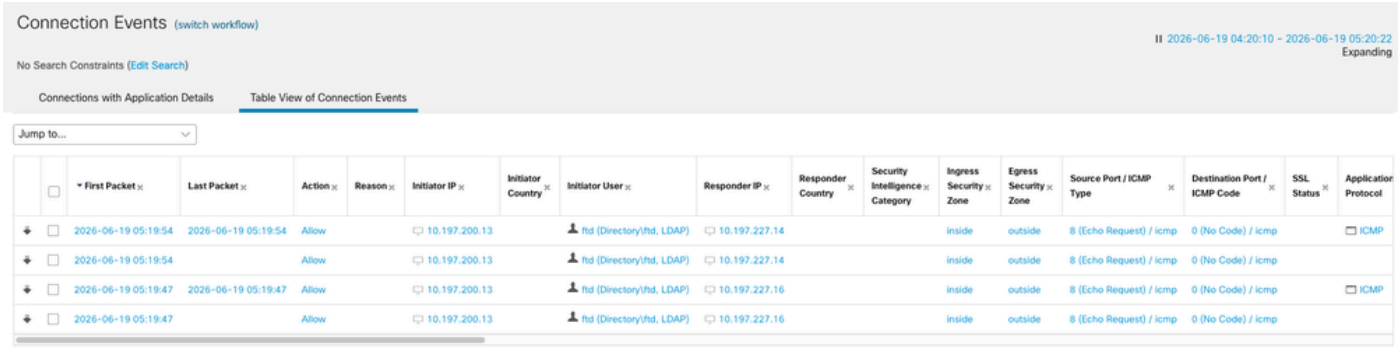
Select...

Showing all 2 sessions

Login Time	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	

Sessioni attive

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

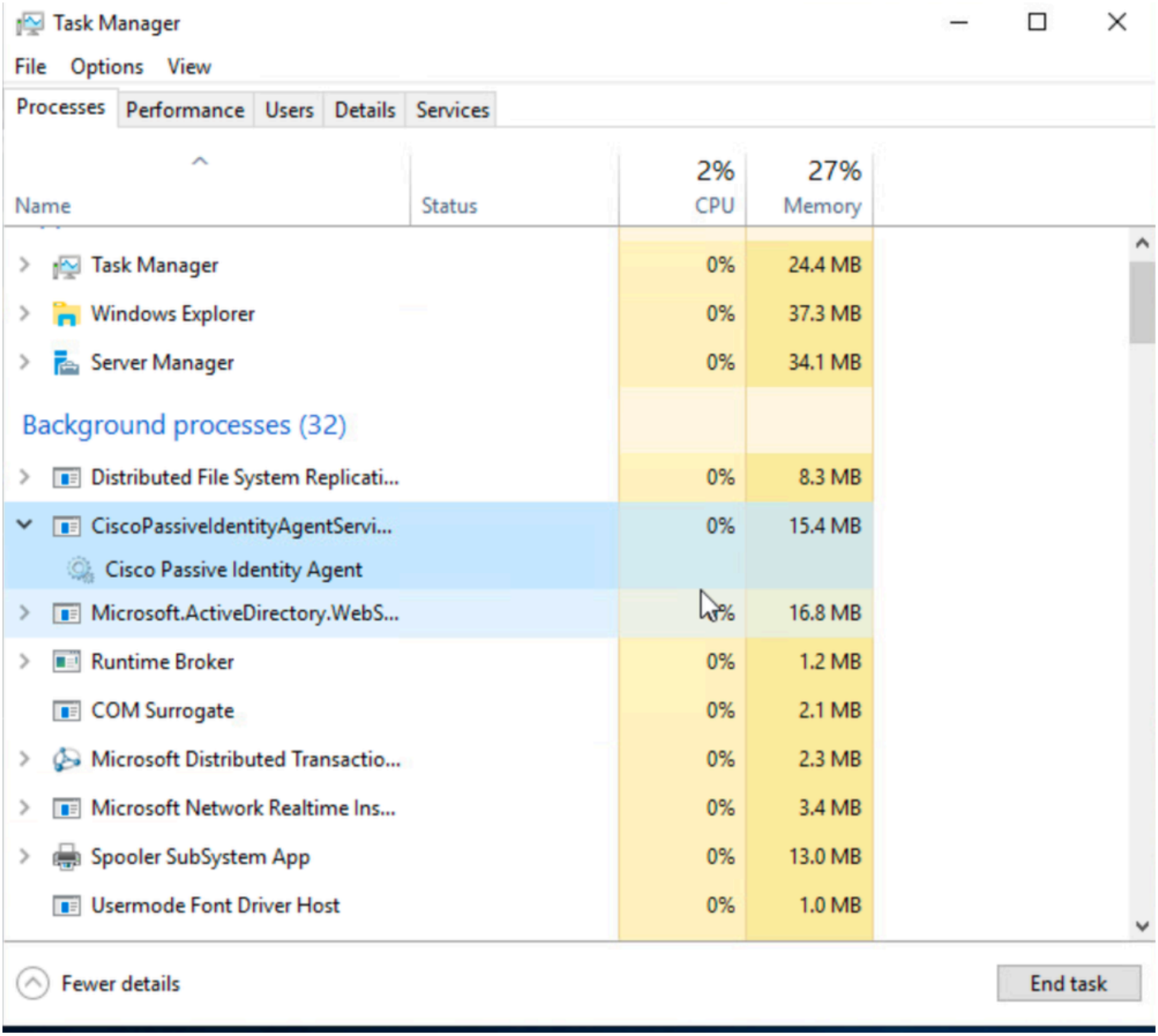


Sessioni attive

Risoluzione dei problemi

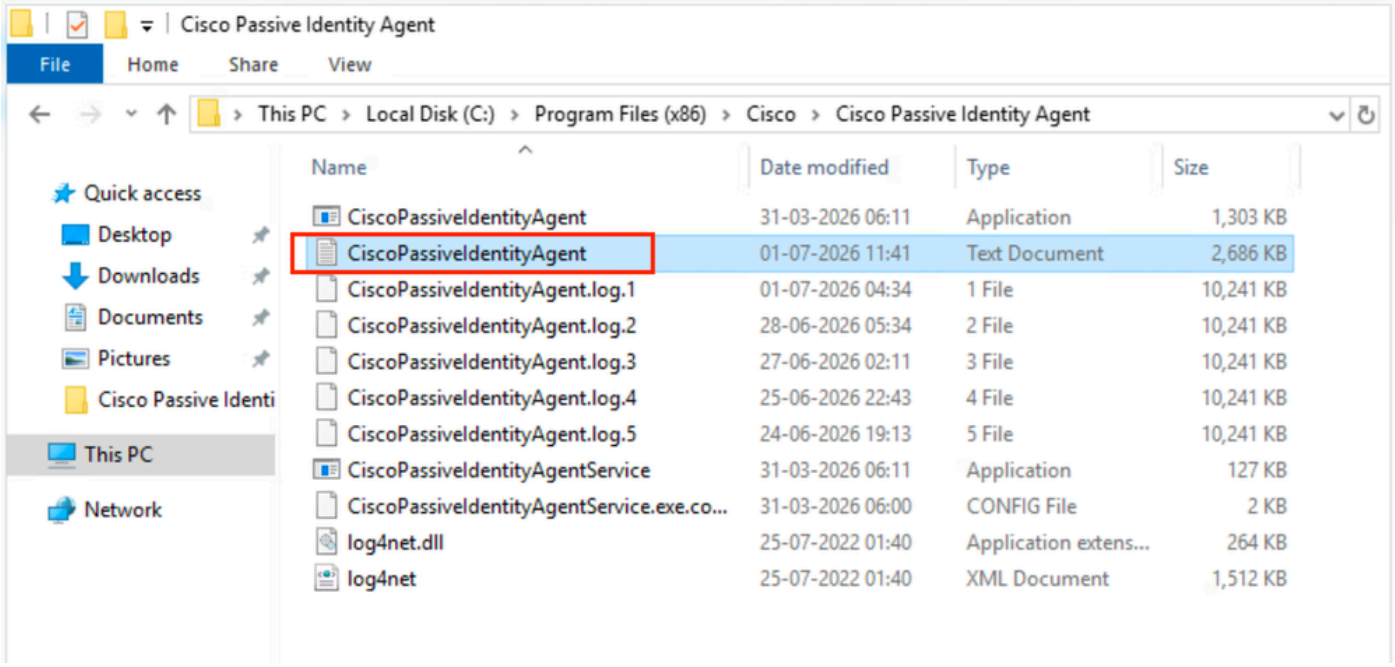
Controllo dei log dell'agente

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



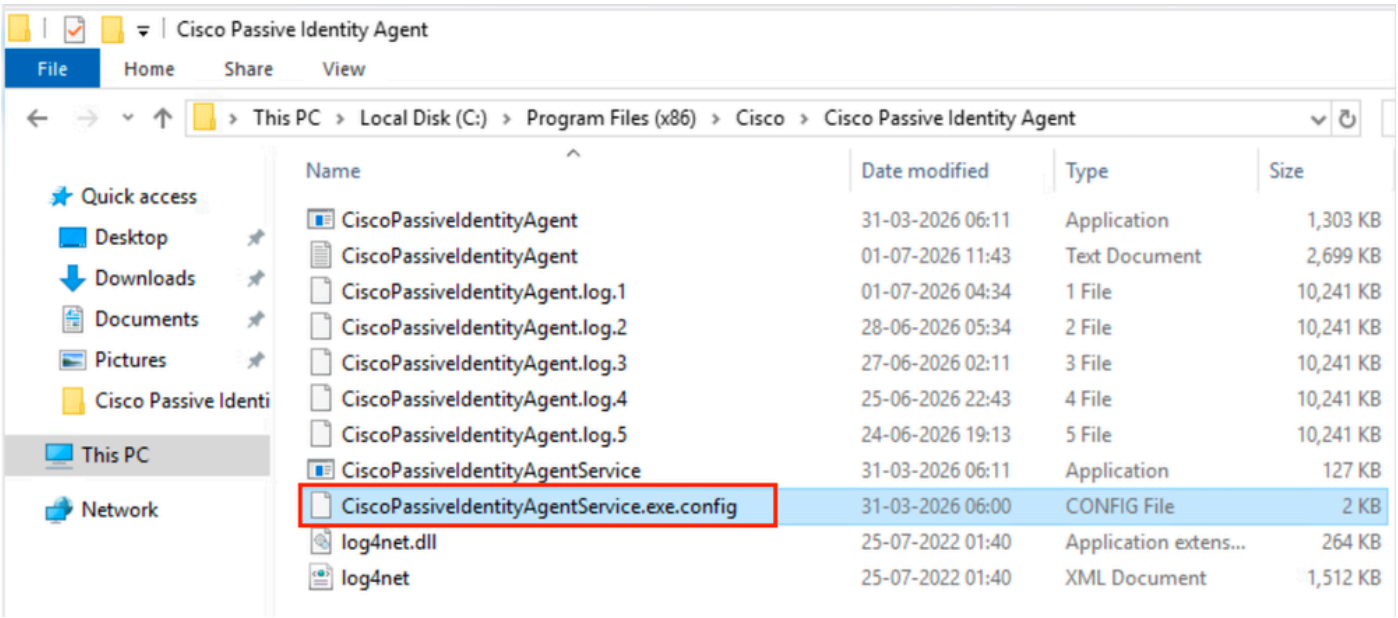
Attività in esecuzione

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

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).