Konfigurieren des passiven Identitätsagenten mit FMC

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie der passive Identitäts-Agent "Source" konfiguriert wird, der Sitzungsdaten an das FMC sendet.

Voraussetzungen

Anforderungen

- Cisco Secure Firewall Management Center mit Version 7.6+
- Cisco Secure Firewall mit Version 7.6+
- Windows Active Directory-Server. Auf dem Server muss Windows Server 2008 oder höher ausgeführt werden.
- Sie müssen Snort 3 auf den Secure Firewall Threat Defense-Geräten aktivieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Firewall Management Center 7.6.5
- Cisco Secure Firewall 7.6.5
- Microsoft Active Directory auf Windows Server 2022.

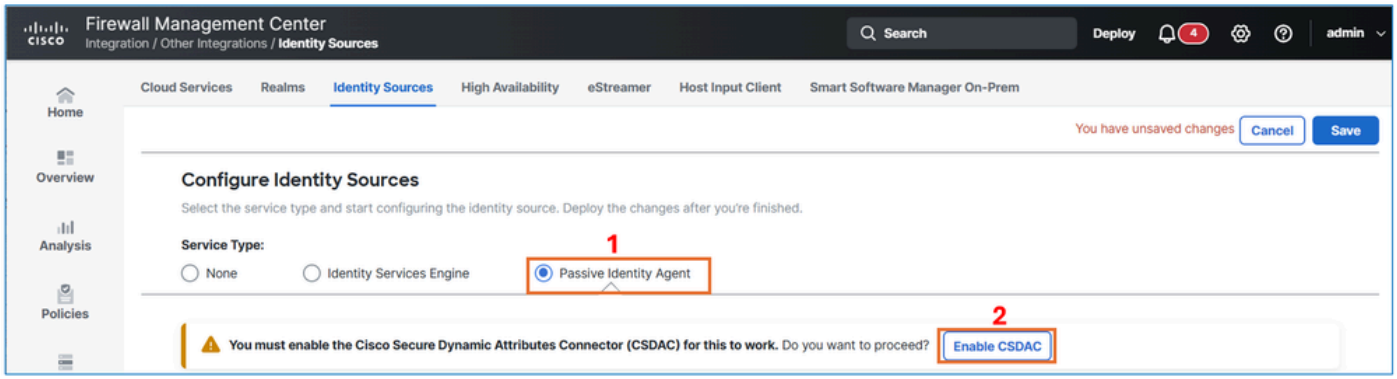
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurationen

Bevor Sie den Agenten konfigurieren, schließen Sie die AD- und FMC-Integration ab.

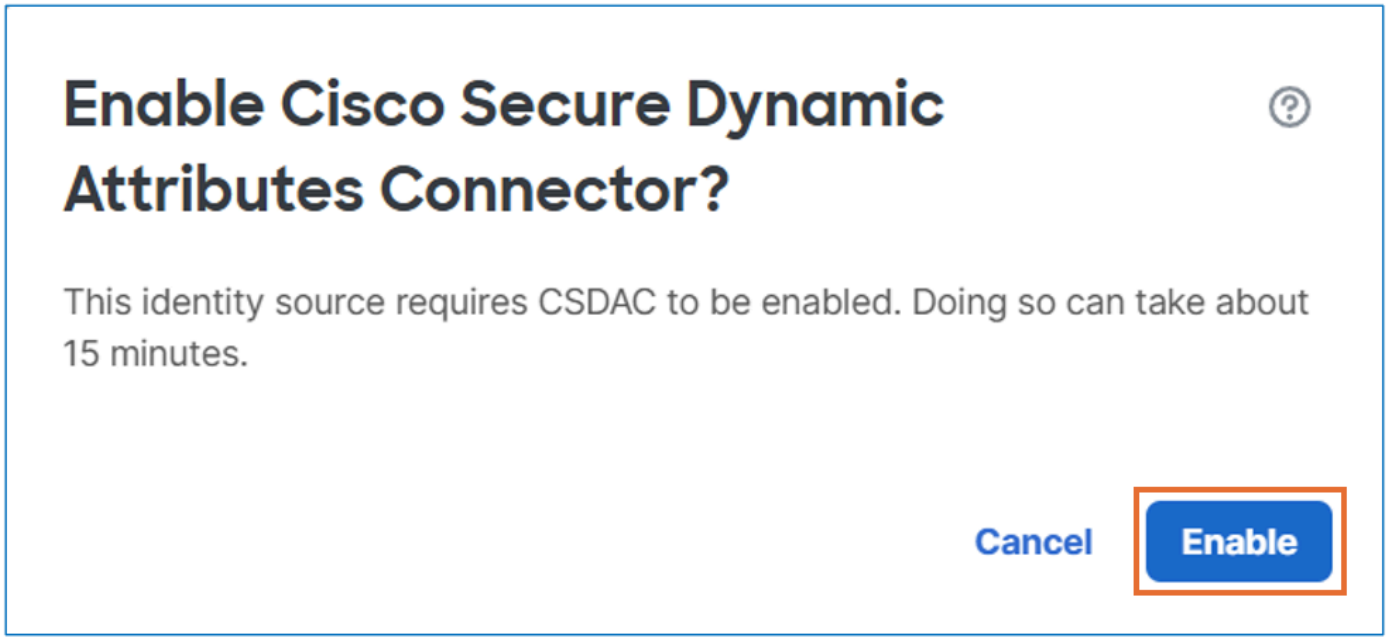
Konfigurieren einer passiven Identity Agent-Quelle

Navigieren Sie in der FMC-Benutzeroberfläche zuIntegration > Other Integrations > Identity Sources, und klicken Sie auf Passive Identity Agent. Wenn der Cisco Secure Dynamic Attributes Connector noch nicht aktiviert wurde, werden Sie aufgefordert, dies zu tun, indem Sie auf CSDAC aktivieren klicken.



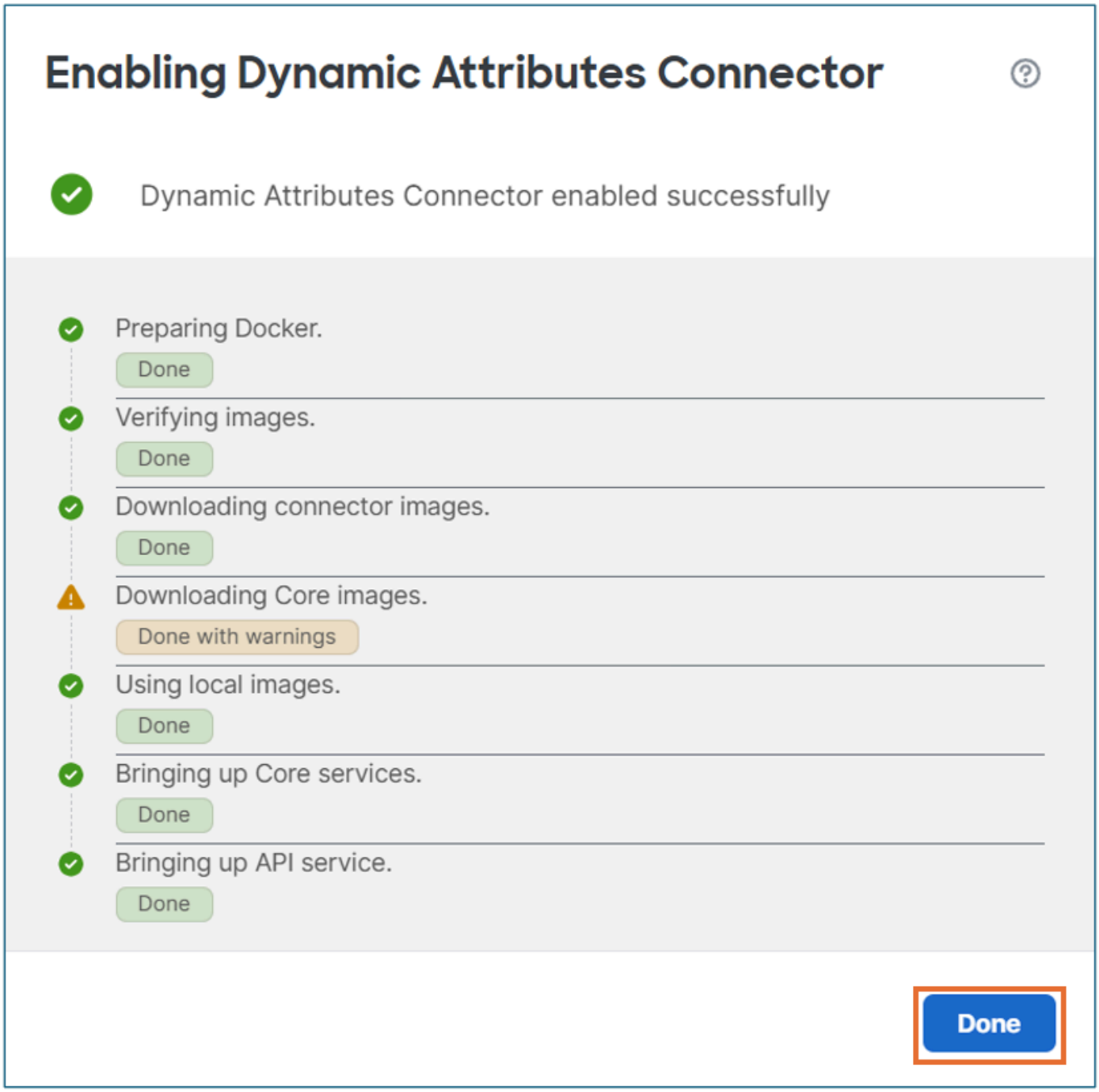
Passiver Identitätsagent

Klicken Sie auf die Schaltfläche Enabled (Aktiviert), um CSDAC zu aktivieren.



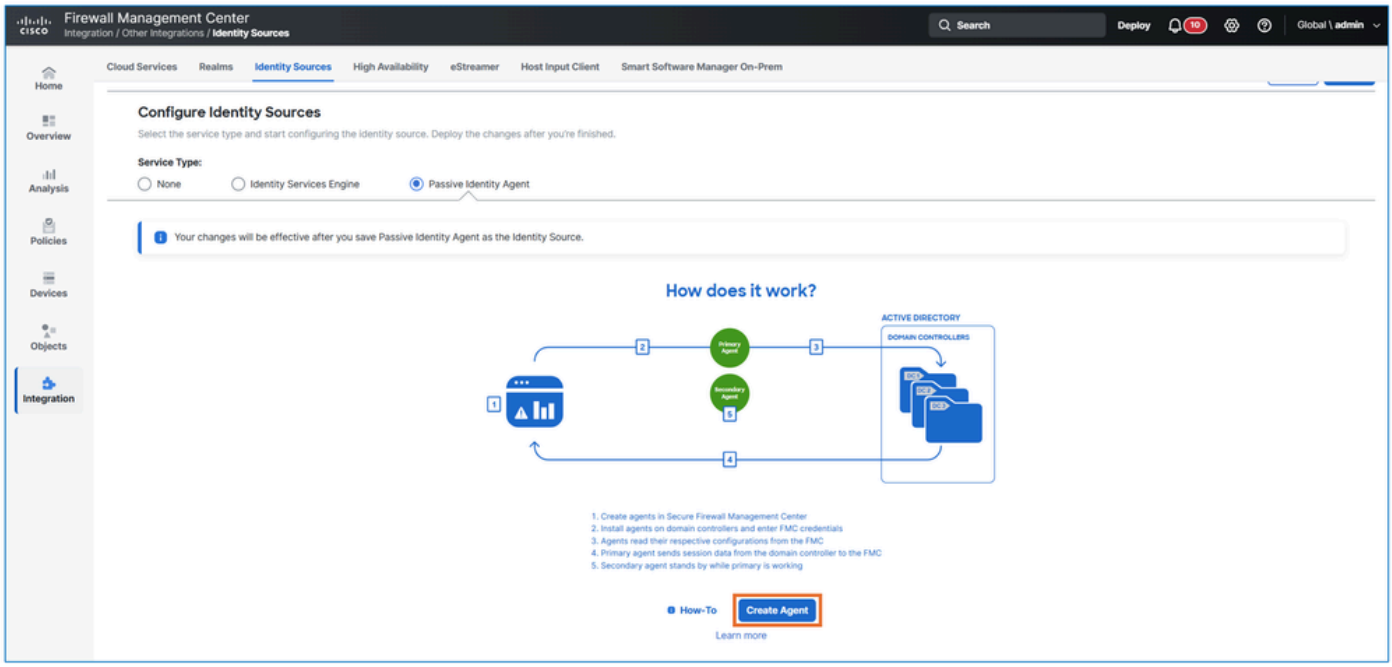
CSDAC aktivieren

Dieser Schritt dauert ungefähr 10 Minuten. Wenn das CSDAC ordnungsgemäß aktiviert wurde, klicken Sie auf die Schaltfläche Donebutton, um fortzufahren.



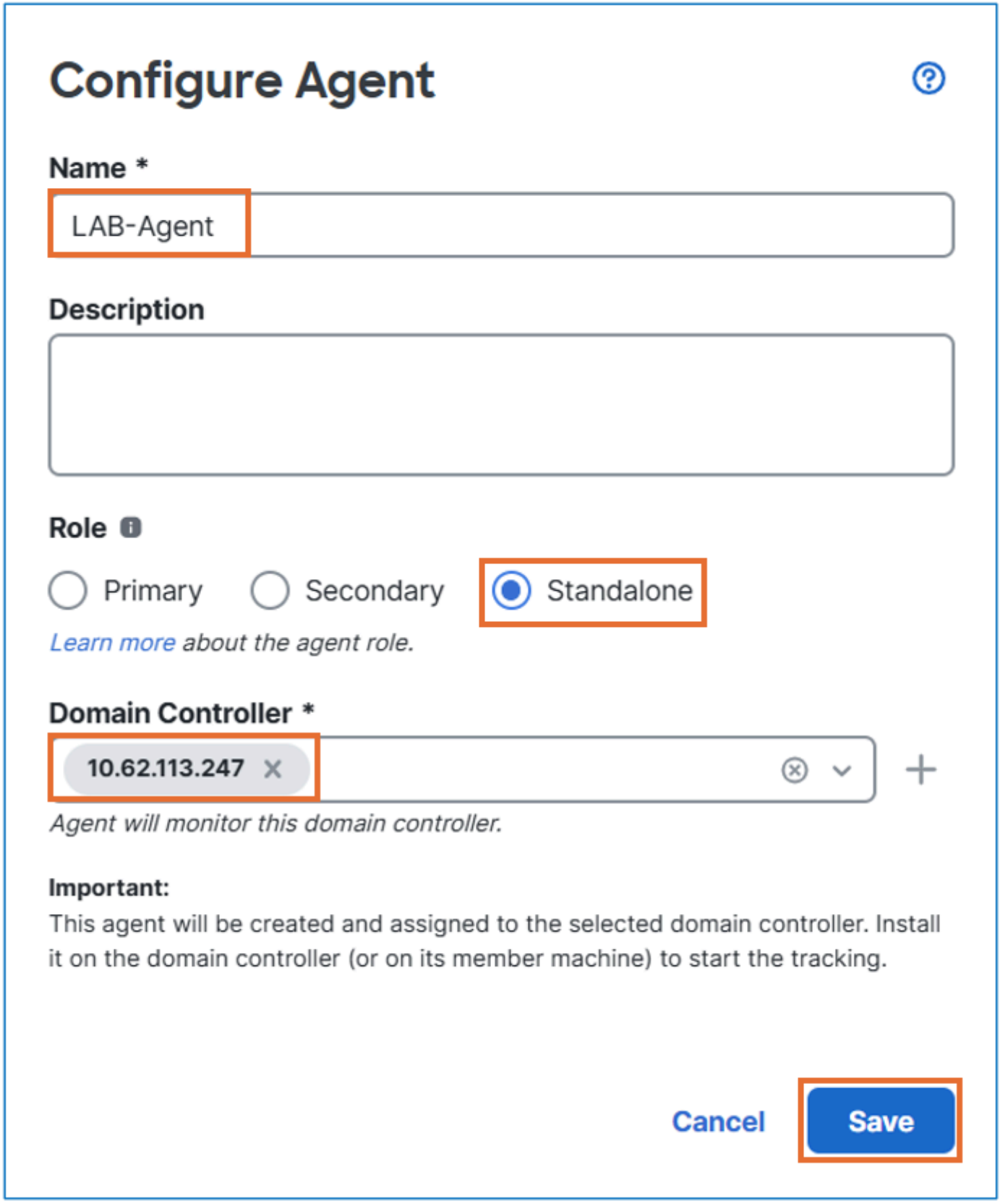
CSDAC aktiviert

Klicken Sie auf die Schaltfläche Agent erstellen.



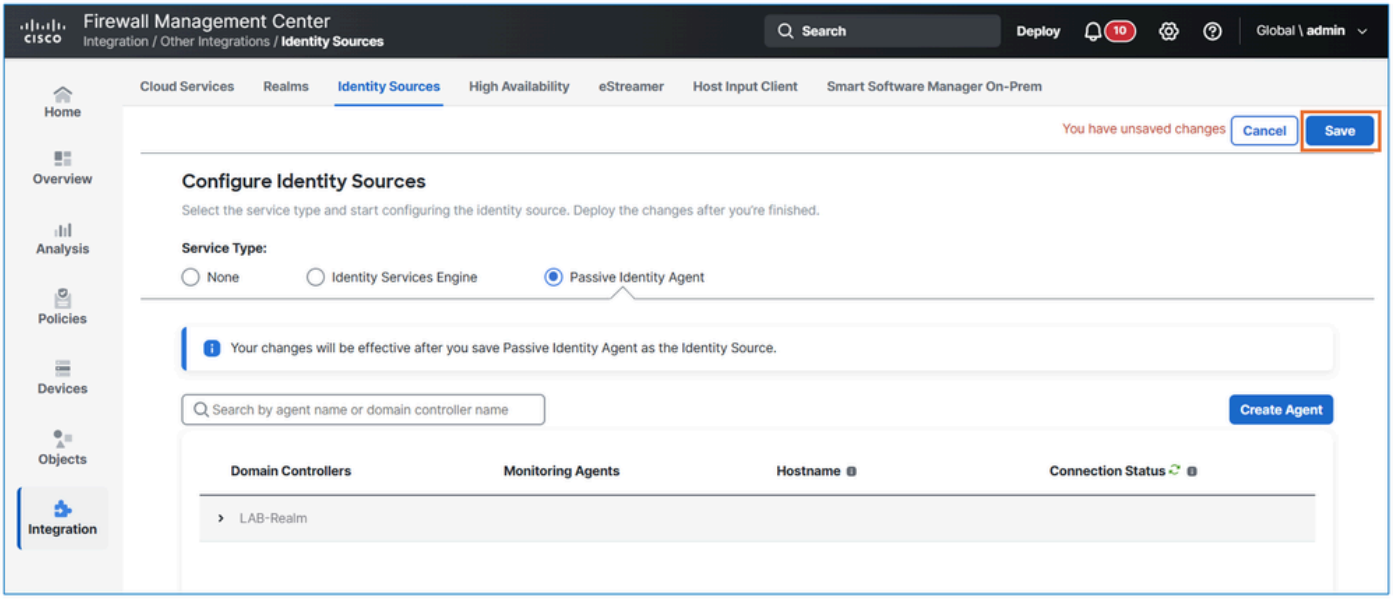
Agent erstellen

Definieren Sie einen Namen für den Agenten, wählen Sie dieStandalone-Option aus, und ordnen Sie ihn dem entsprechenden Domänencontroller zu, der im vorherigen Task erstellt wurde.



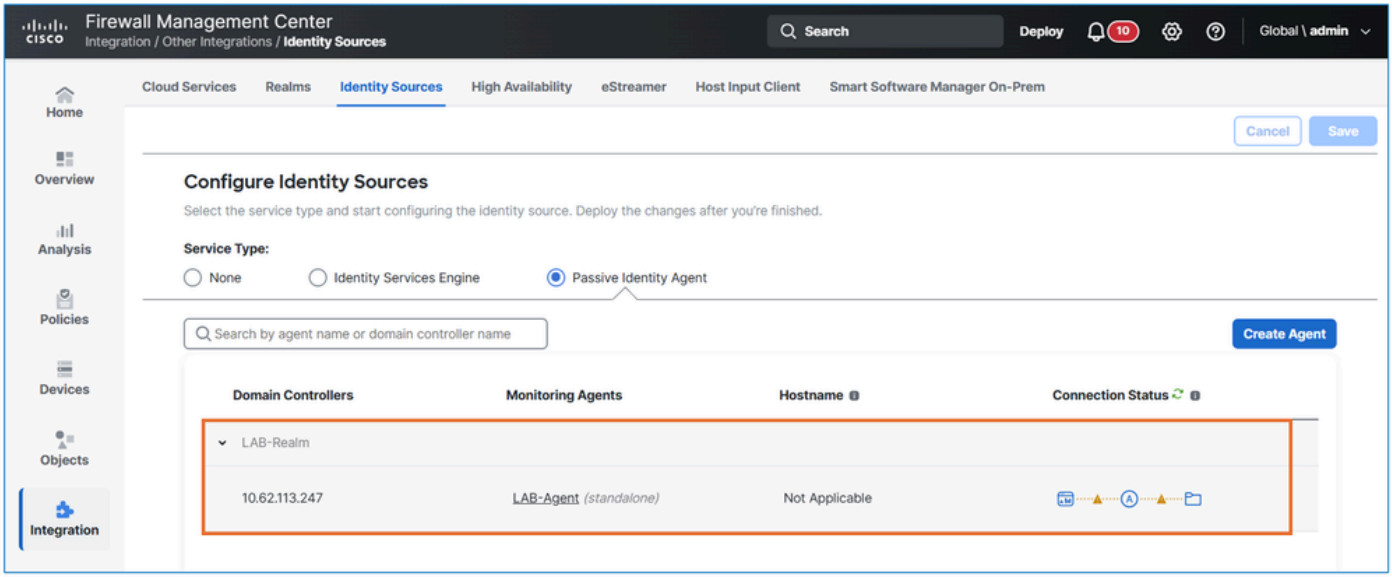
Agent konfigurieren

Klicken Sie auf die Schaltfläche Speichern.



Speichern Sie die Konfiguration.

Ergebnis.



Status überprüfen

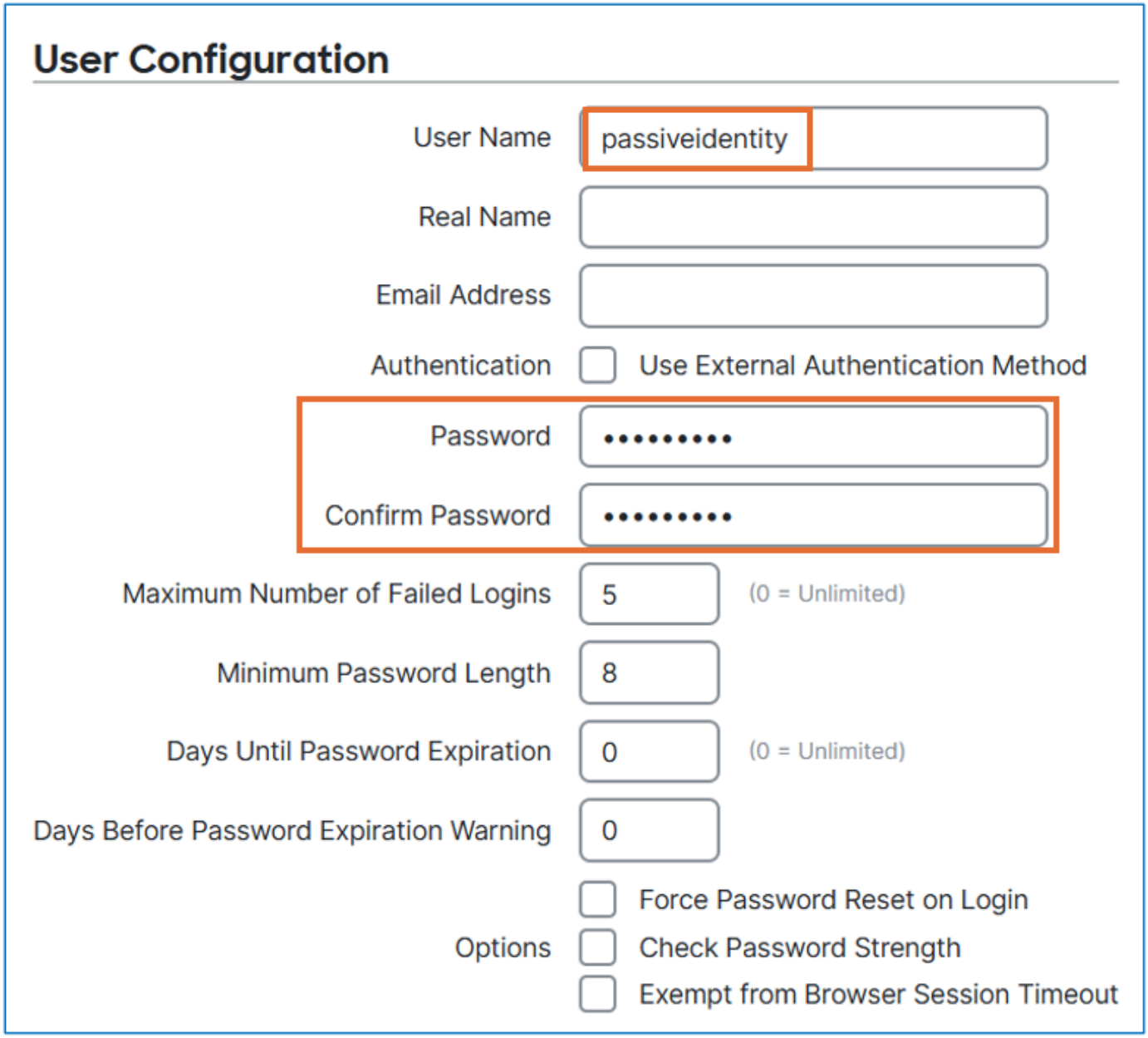
Anmerkung: Der passive Identitätsagent zeigt den Status mithilfe von Leitungen an. Gelb bedeutet, dass der Agent nie erfolgreich mit dem Secure Firewall Management Center kommuniziert hat. Eine neu erstellte Agentenzeile ist gelb und bleibt so, bis die Konfiguration abgeschlossen ist.

Erstellen eines passiven Identity Agent-Benutzers im Secure Firewall Management

Center

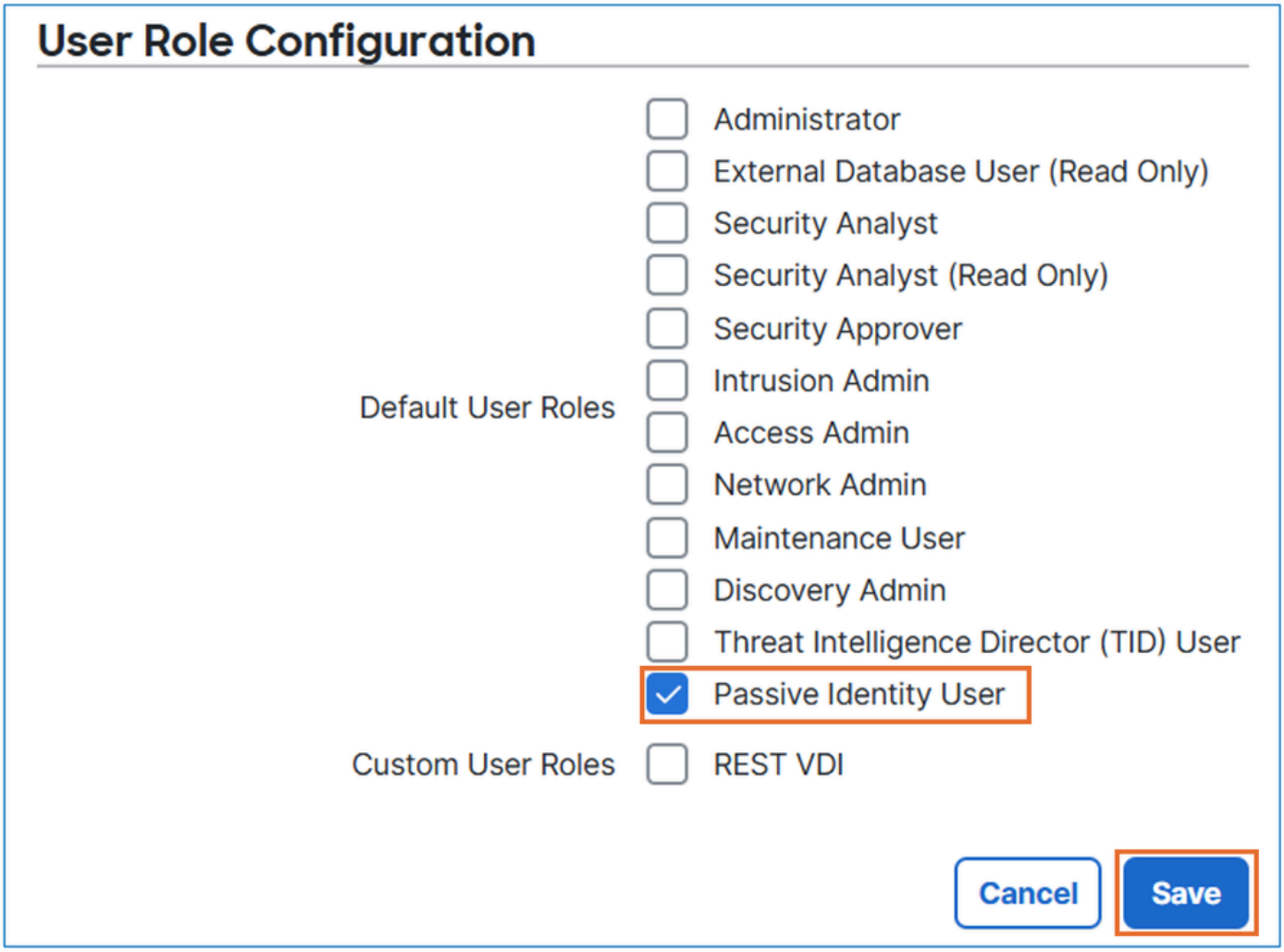
Erstellen Sie einen Secure Firewall Management Center-Benutzer mit ausreichenden Berechtigungen, um mit dem passiven Identitäts-Agent zu kommunizieren. Dieser Benutzer verfügt über eingeschränkte Berechtigungen zum Ausführen anderer Aufgaben. Es wird erwartet, dass der Benutzer nur die Kommunikation mit dem passiven Identitätsagenten aktiviert.

Navigieren Sie in der FMC-Benutzeroberfläche zu System > Users, und klicken Sie auf Create User. Geben Sie die Details des Benutzers entsprechend den Aufgabenanforderungen an.



Benutzer erstellen

Weisen Sie nur die Benutzerrolle für passive Identität zu. Klicken Sie auf die Schaltfläche Speichern.

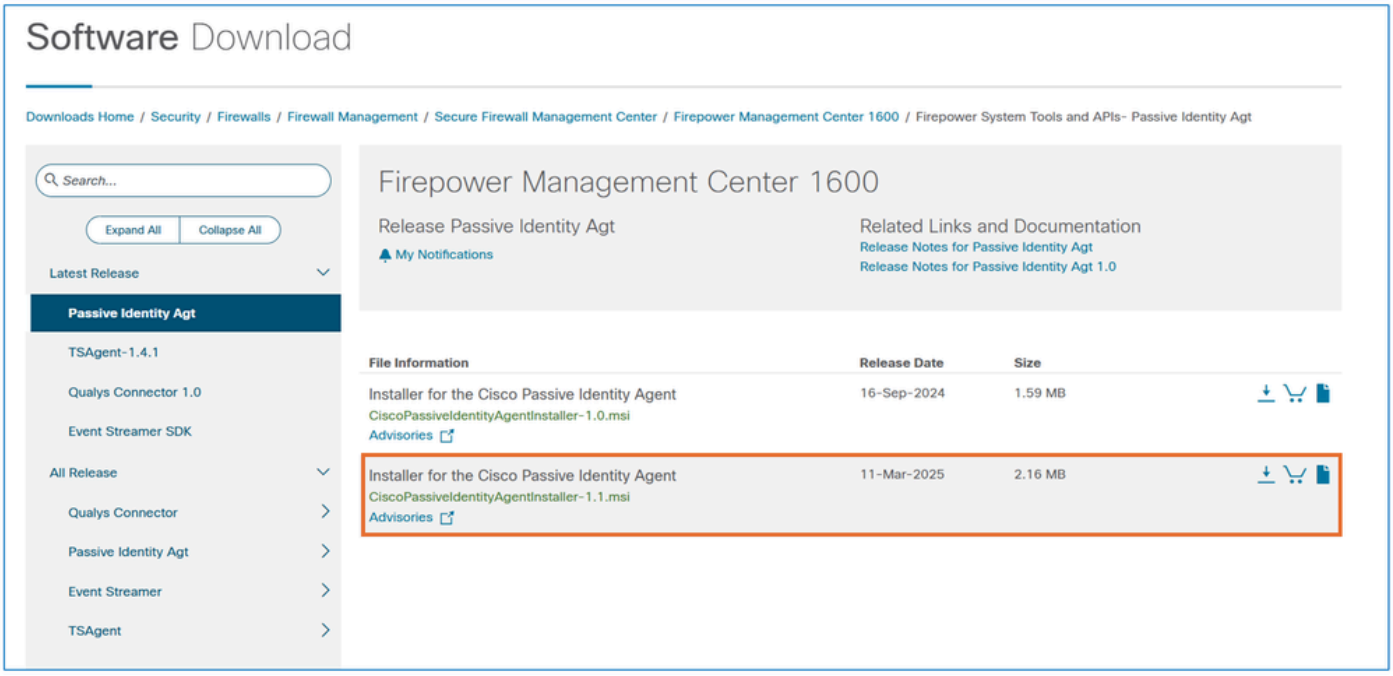


Passiven Identitätsbenutzer auswählen

Installation und Konfiguration der Software für den passiven Identitätsagent

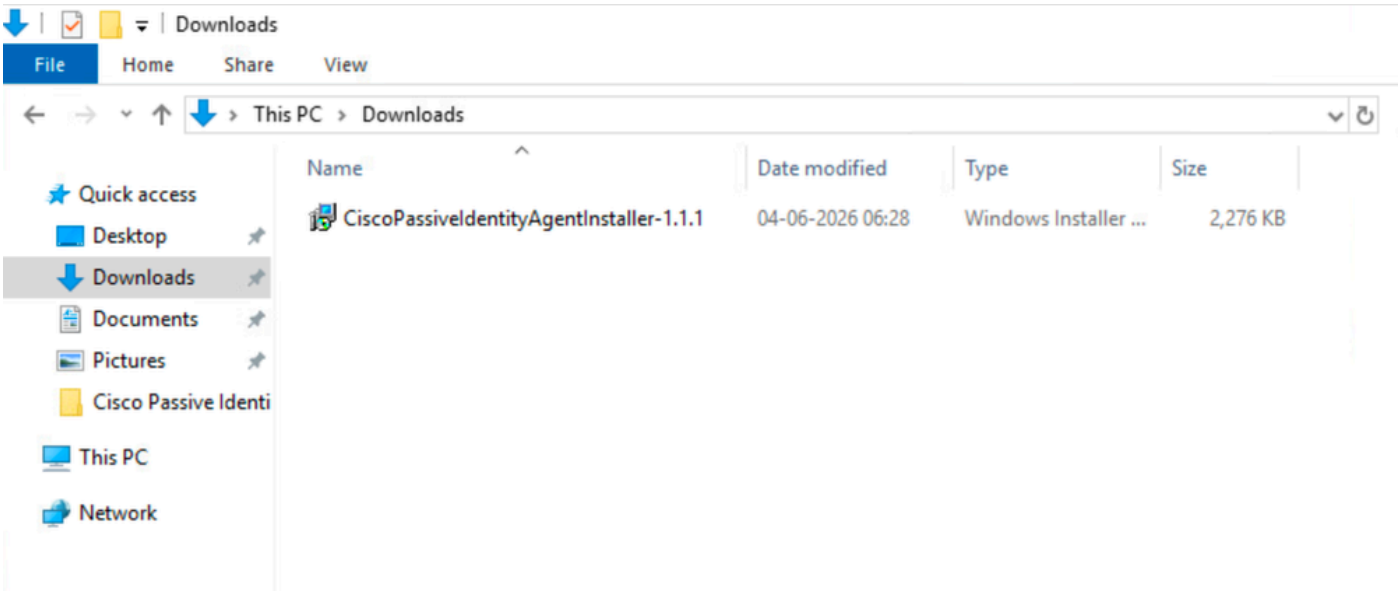
Installieren und konfigurieren Sie die Software für den passiven Identitäts-Agent auf dem designierten Domänencontroller.

Laden Sie den passiven Identitäts-Agent von software.cisco.com herunter.



Software herunterladen

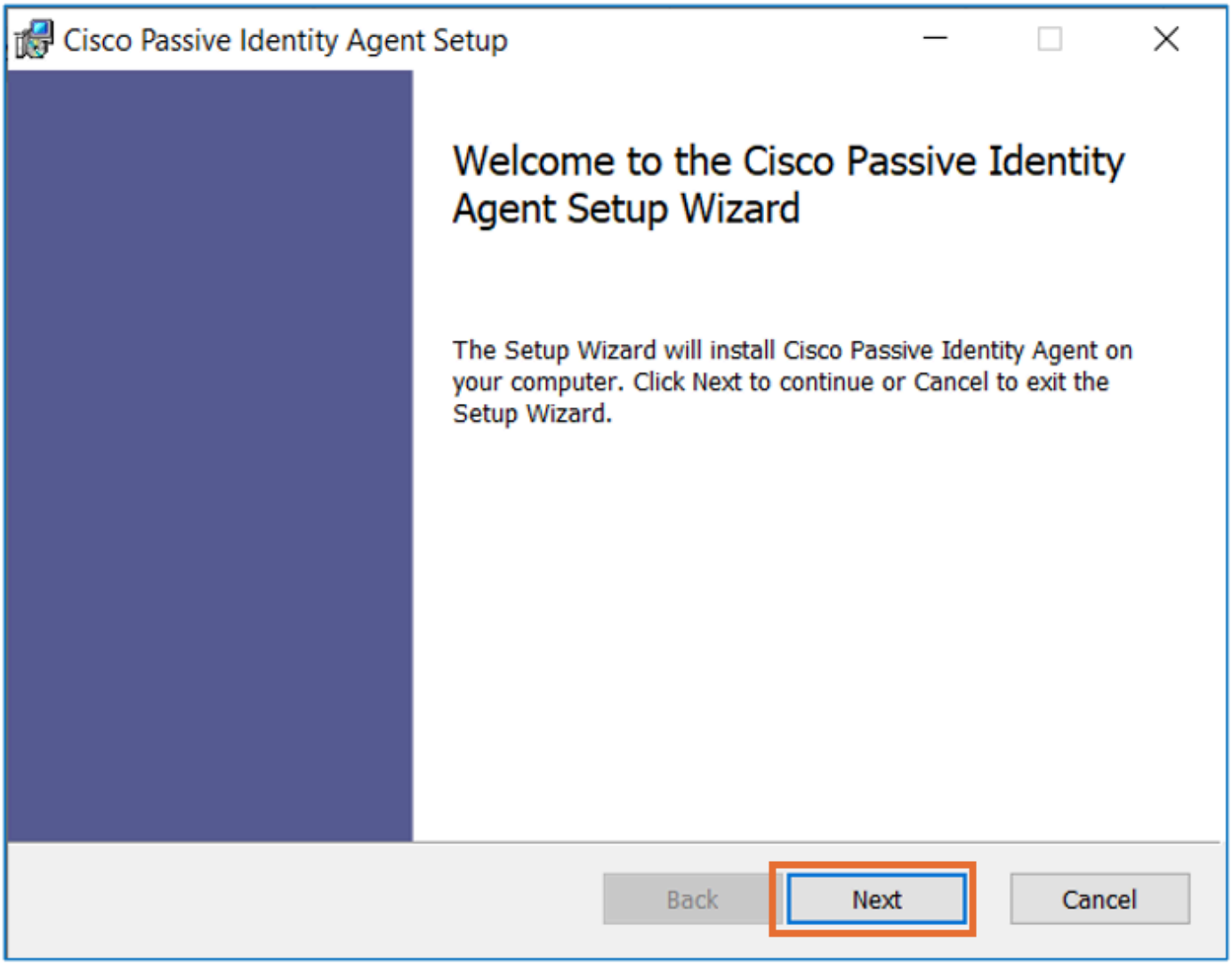
Starten Sie nach dem Herunterladen des Agenten den Installationsvorgang auf dem Domänencontroller.



Agent

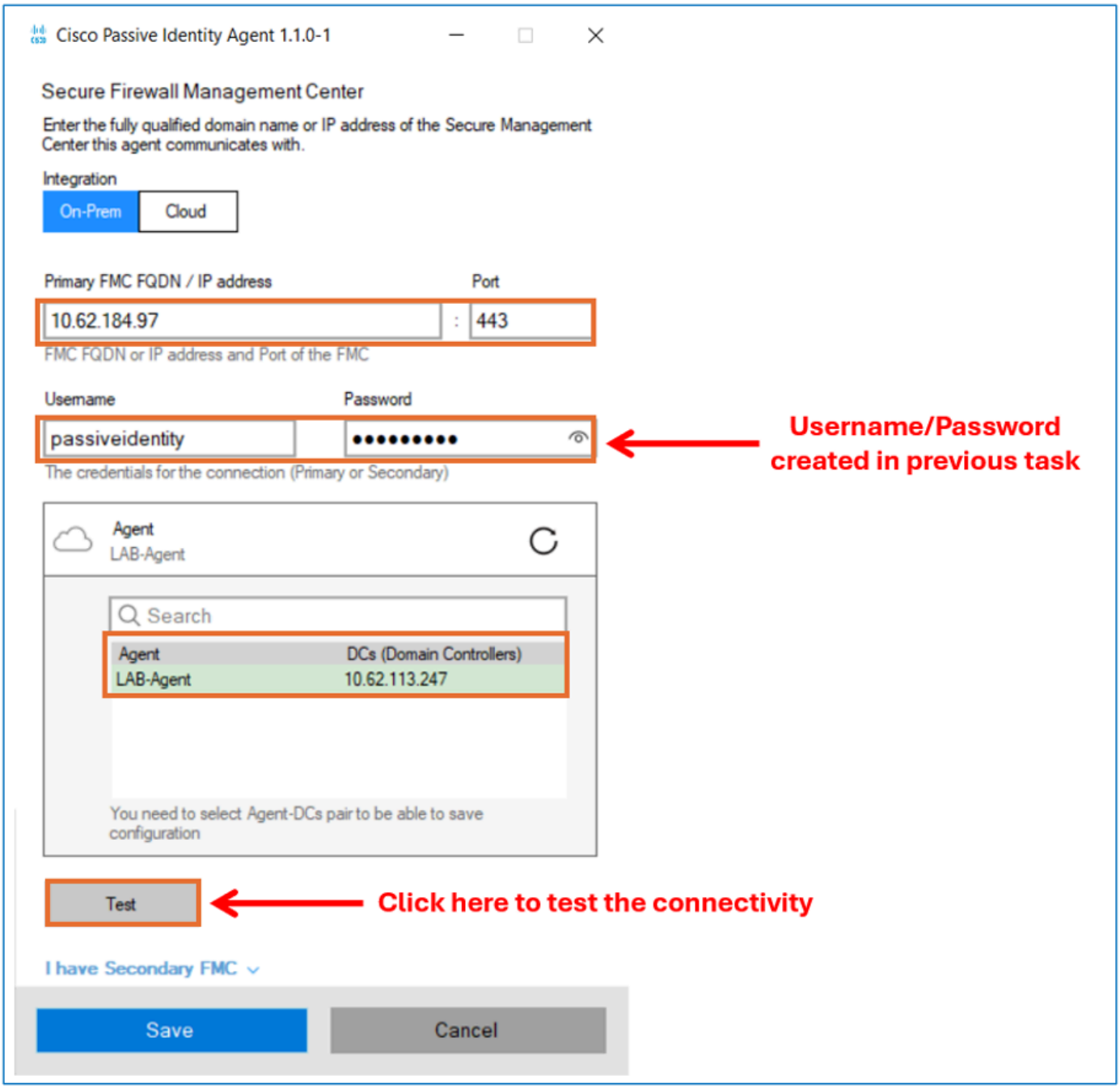
]

Lesen Sie die Installationsanweisungen, um das Setup abzuschließen.



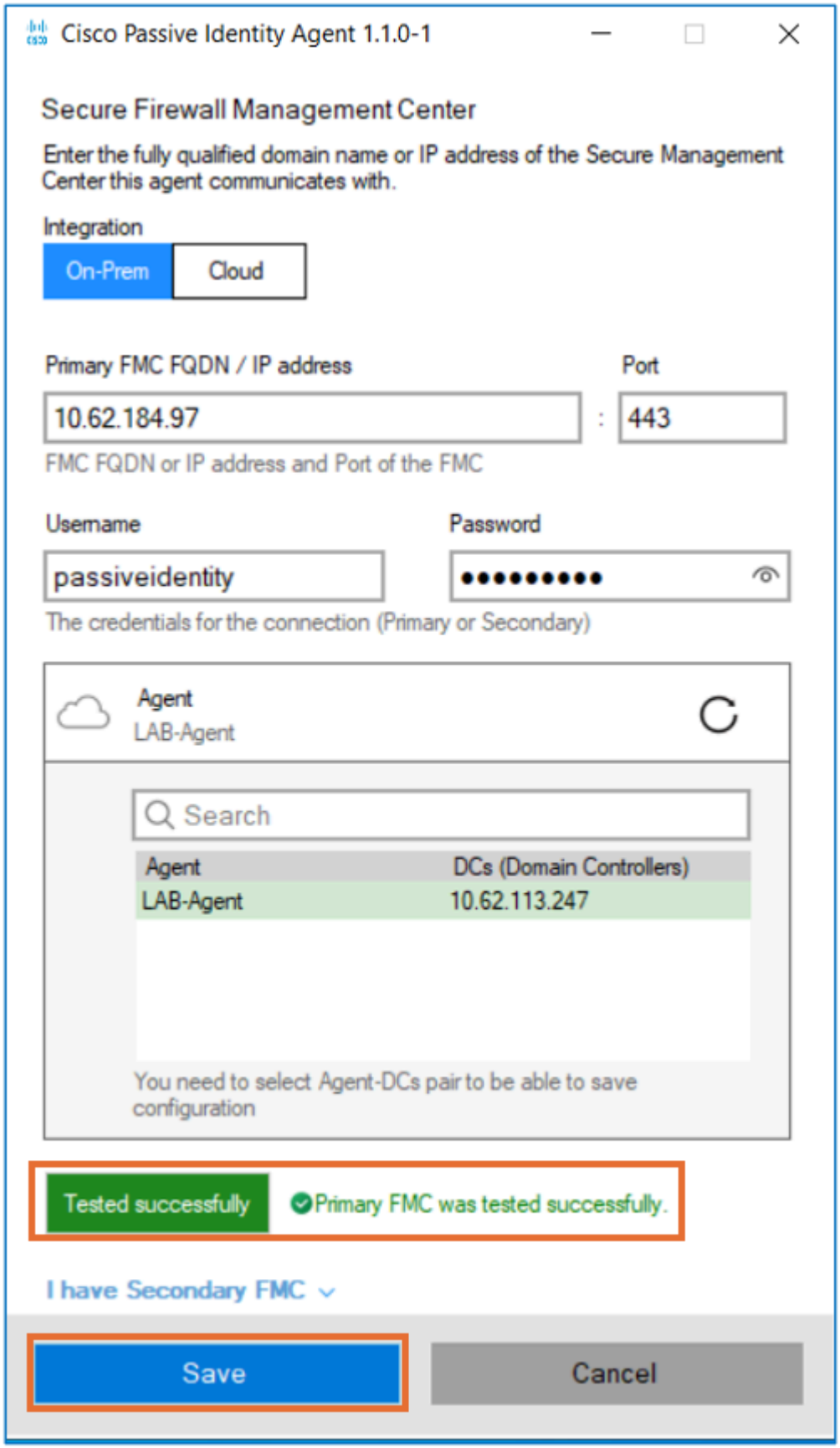
Install

Sobald die Installation abgeschlossen ist, öffnen Sie die Passive Identity Agent-Software, und geben Sie die erforderlichen Informationen gemäß den Aufgabenanforderungen ein. Klicken Sie auf die Schaltfläche Test, um die Verbindung mit dem FMC zu überprüfen.



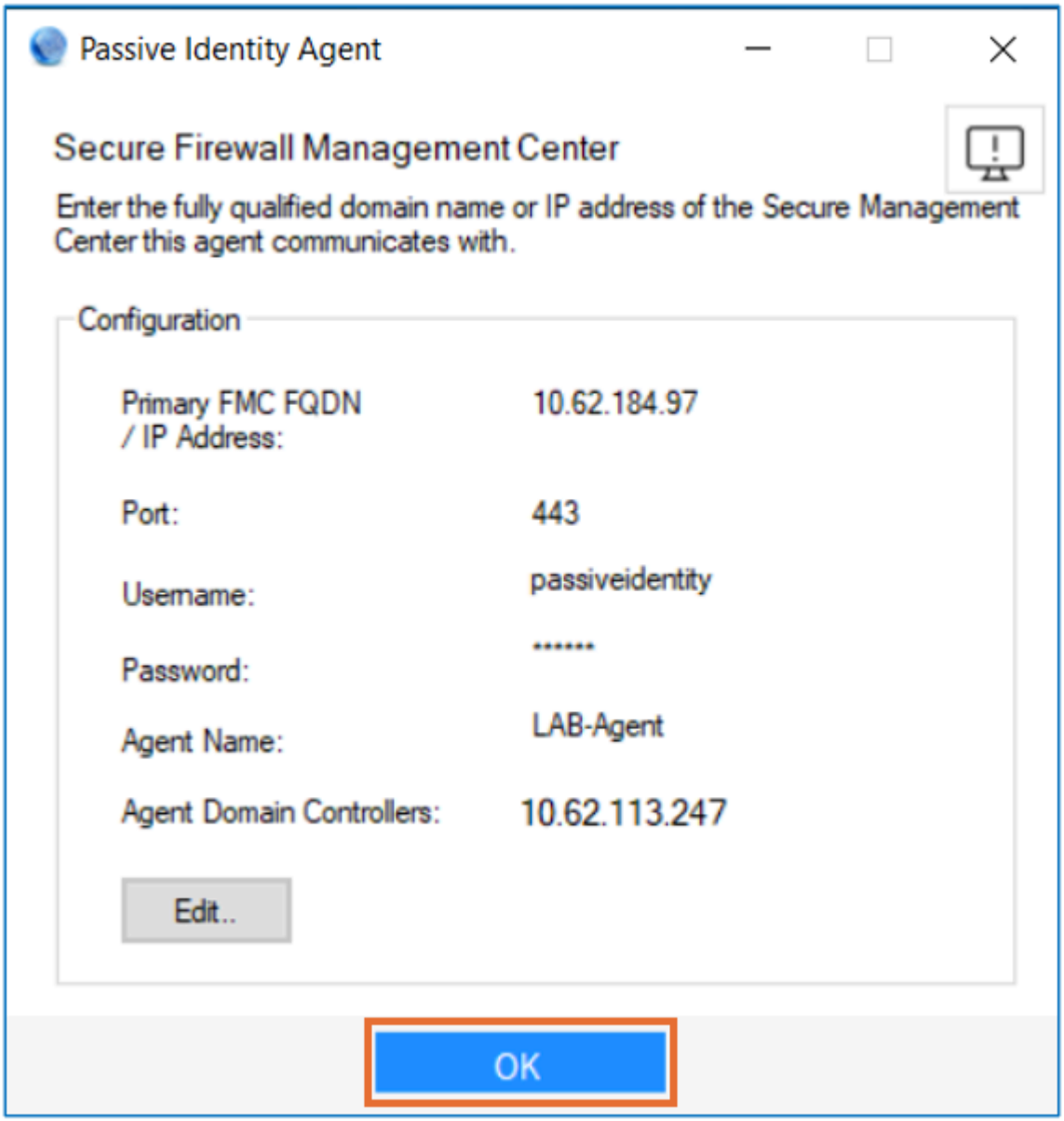
Konfigurieren Sie den Agenten.

Nachdem Sie die Verbindung erfolgreich getestet haben, klicken Sie auf die Schaltfläche Speichern.



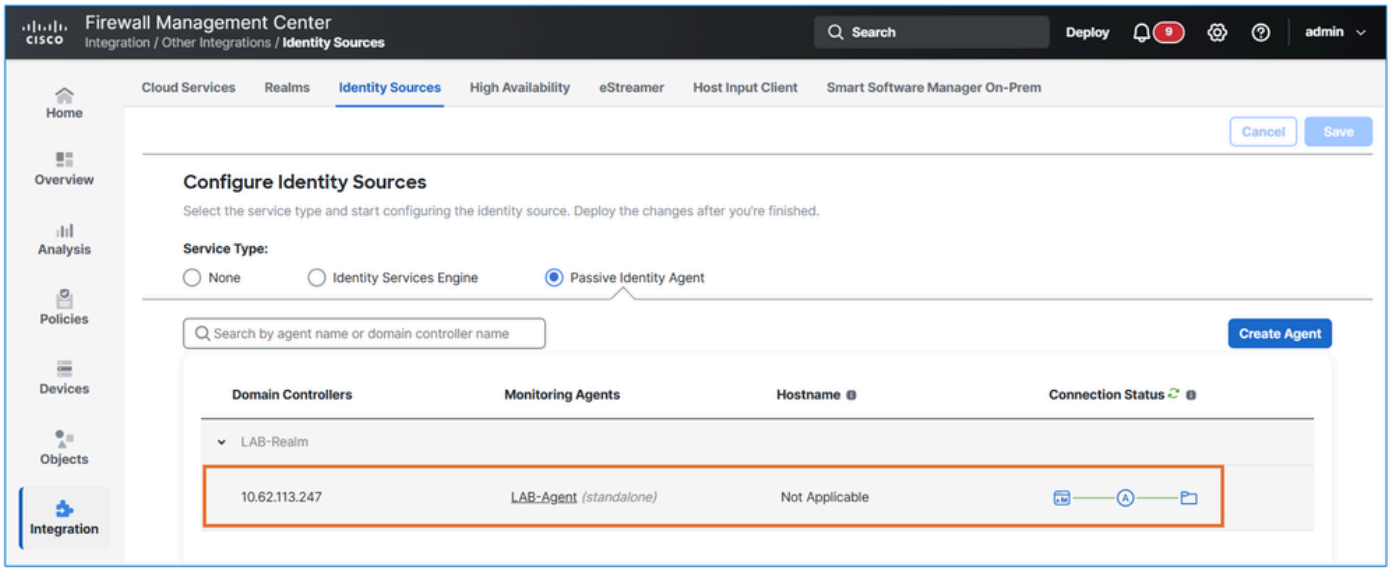
Test

Klicken Sie auf OK, um die Agentenkonfiguration abzuschließen.



Agent wird ausgeführt

Navigieren Sie in der FMC-Benutzeroberfläche zuIntegration > Weitere Integrationen > Identitätsquellen > Passiver Identitätsagent. Bestätigen Sie, dass der passive Identitätsagent den Status "Grün" anzeigt.



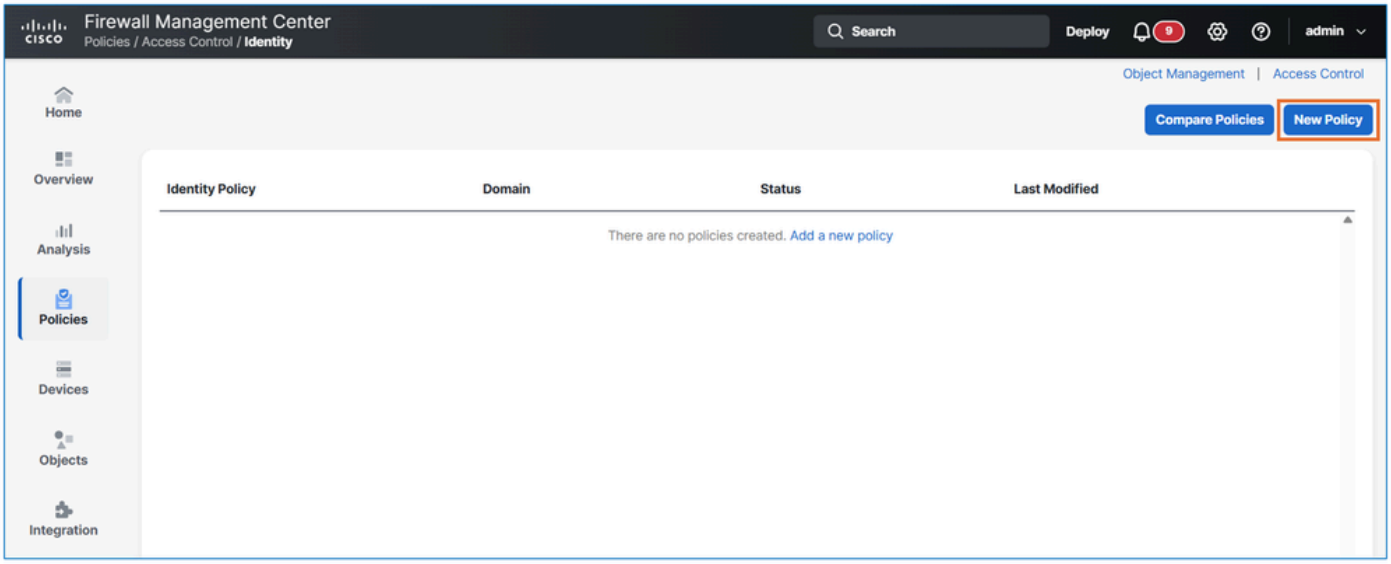
die Kommunikation von fmc überprüfen

Identitätsrichtlinien konfigurieren

Erstellen Sie eine Identitätsrichtlinie auf Basis der bereitgestellten Tabelle.

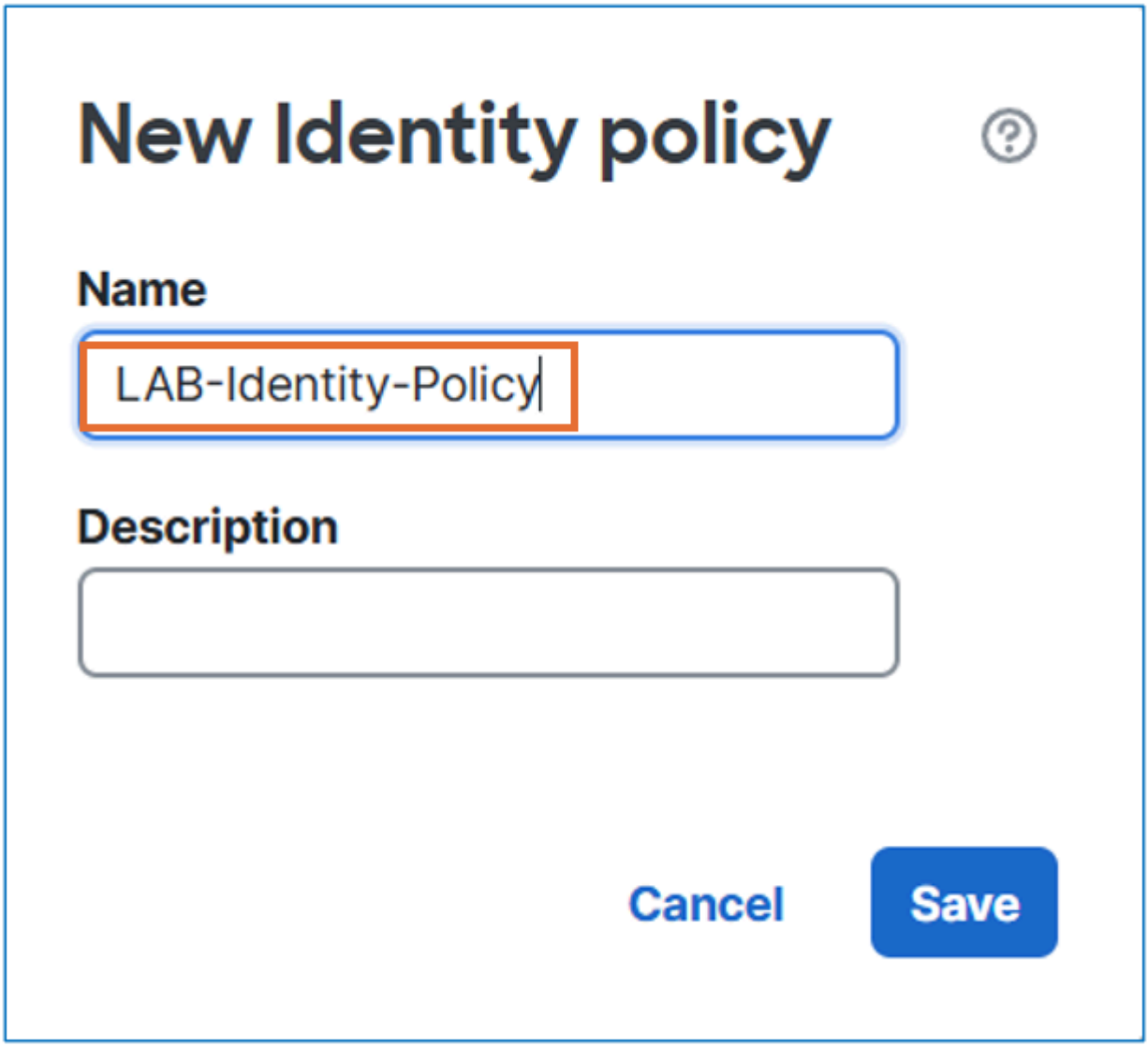
Richtlinienname	Regelname	Authentifizierungsbereich	Verbleibende Einstellungen
LAB-Identitätsrichtlinie	Regel 1	LAB-Bereich	Als Standard beibehalten

Navigieren Sie in der FMC-Benutzeroberfläche zuRichtlinien > Zugriffskontrolle > Identität. Klicken Sie auf die Schaltfläche Neue Richtlinie.



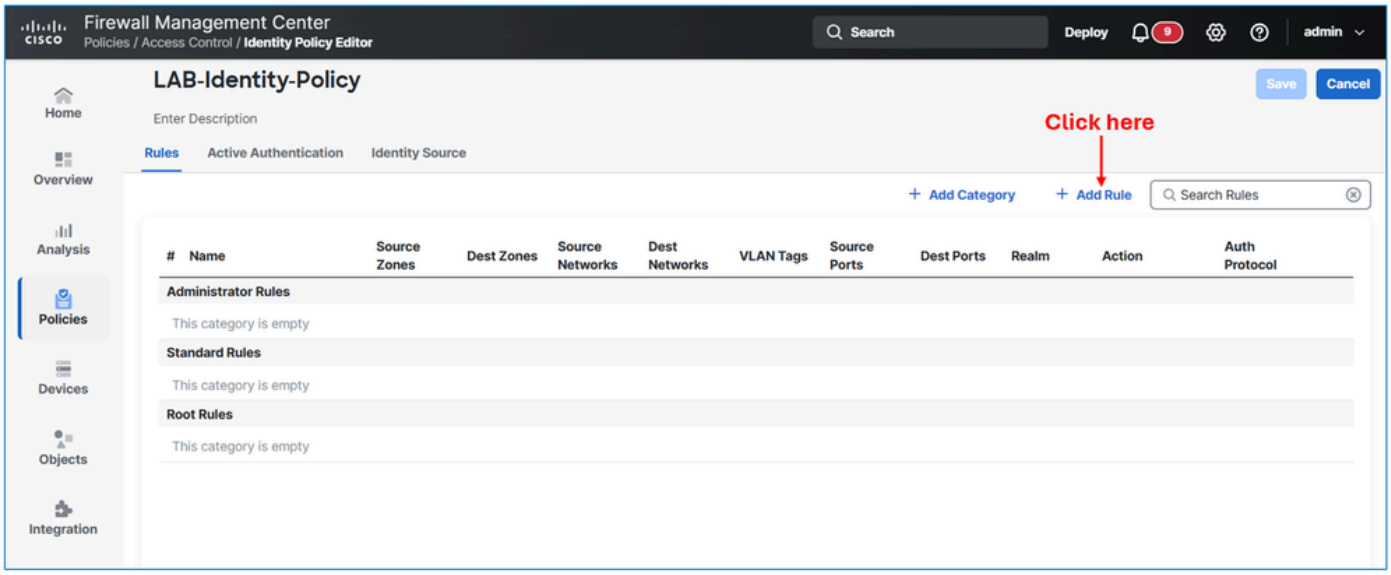
neue Politik

Geben Sie den Namen der Richtlinie entsprechend den Aufgabenanforderungen ein.



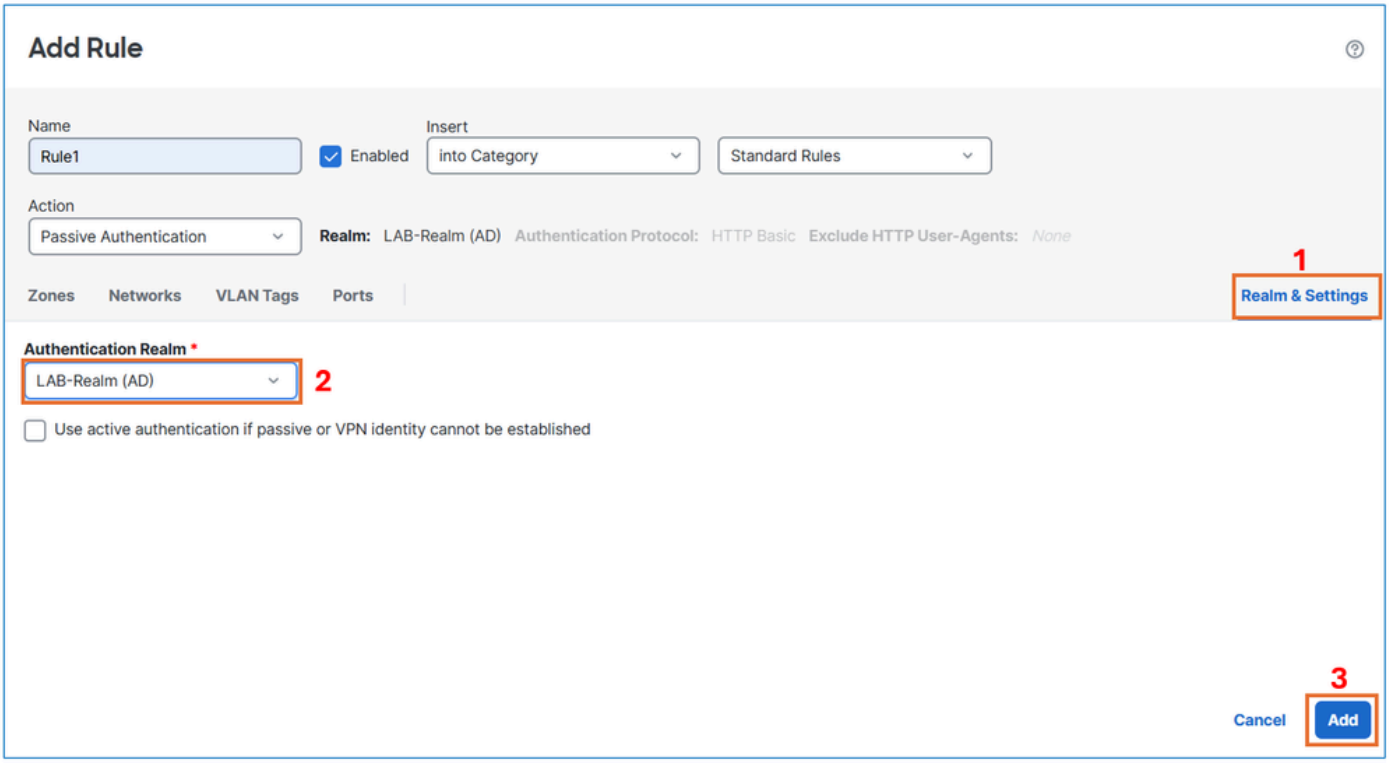
neue Politik

Klicken Sie auf die Schaltfläche Regel hinzufügen.



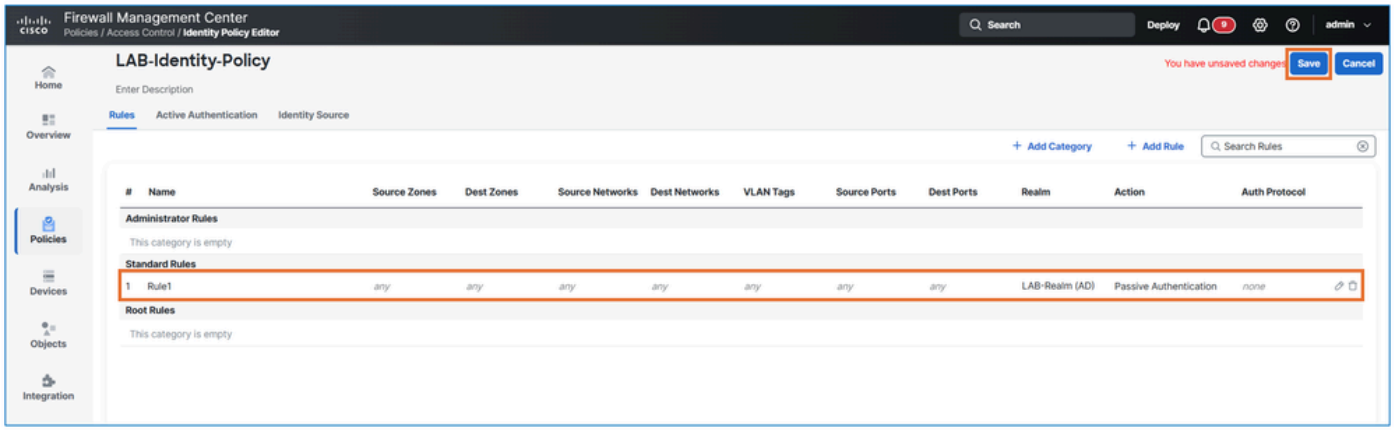
Regel erstellen

Navigieren Sie zu der Registerkarte Realm & Settings (Bereich und Einstellungen), und wählen Sie je nach Aufgabenanforderungen den Authentifizierungsbereich aus. Klicken Sie abschließend auf die Schaltfläche Hinzufügen.



Bereichseinstellung

Klicken Sie auf die Schaltfläche Speichern.



Konfig. speichern

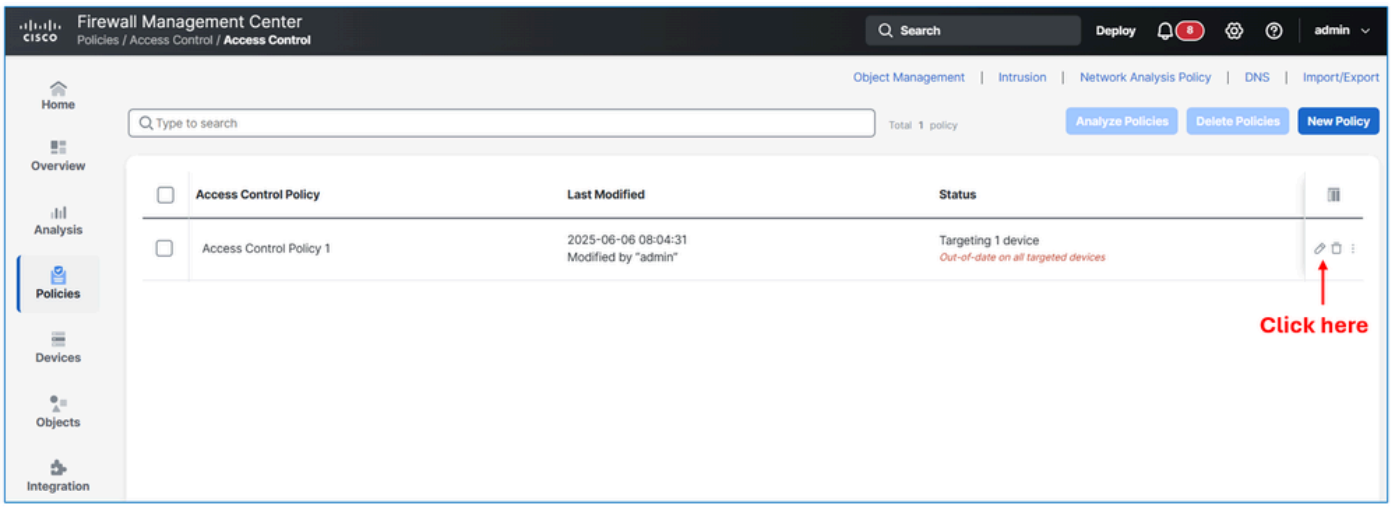
Zugriffskontrollrichtlinien konfigurieren

Verknüpfen Sie die Identitätsrichtlinie mit der Zugriffskontrollrichtlinie, und erstellen Sie eine Zugriffsrichtlinien-Regel mit den folgenden Attributen:

Attributname	Wert
Regelname	Regel 1
Aktion	Zulassen
Quellzone	Intern
Zielzone	Außen
Quellnetzwerke	10.10.10.0/24
Zielnetzwerke	10.48.62.98/32
Service	Ziel-Port TCP 80 (HTTP)
Benutzer	LAB-Bereich/GRUPPE1
Protokollieren	Am Ende der Verbindung

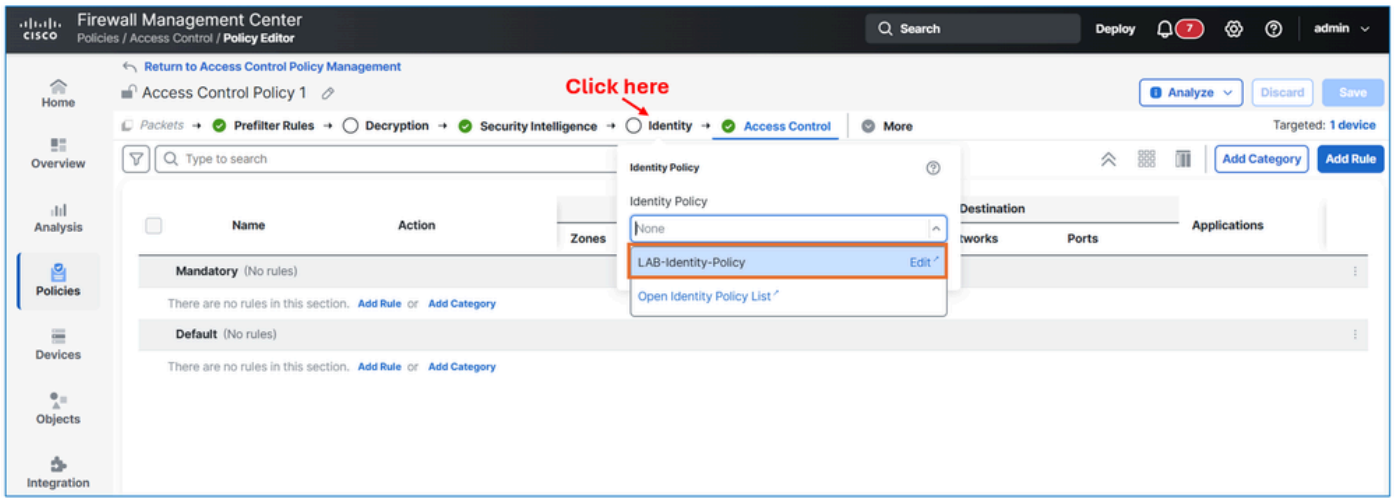
Schritt 1: Verknüpfen der Identitätsrichtlinie mit der Richtlinie für die Zugriffskontrolle

Navigieren Sie in der FMC-Benutzeroberfläche zuRichtlinien > Zugriffskontrolle > Zugriffskontrolle. Klicken Sie für Ihre Richtlinie auf die Schaltfläche Bearbeiten.



Richtlinie bearbeiten

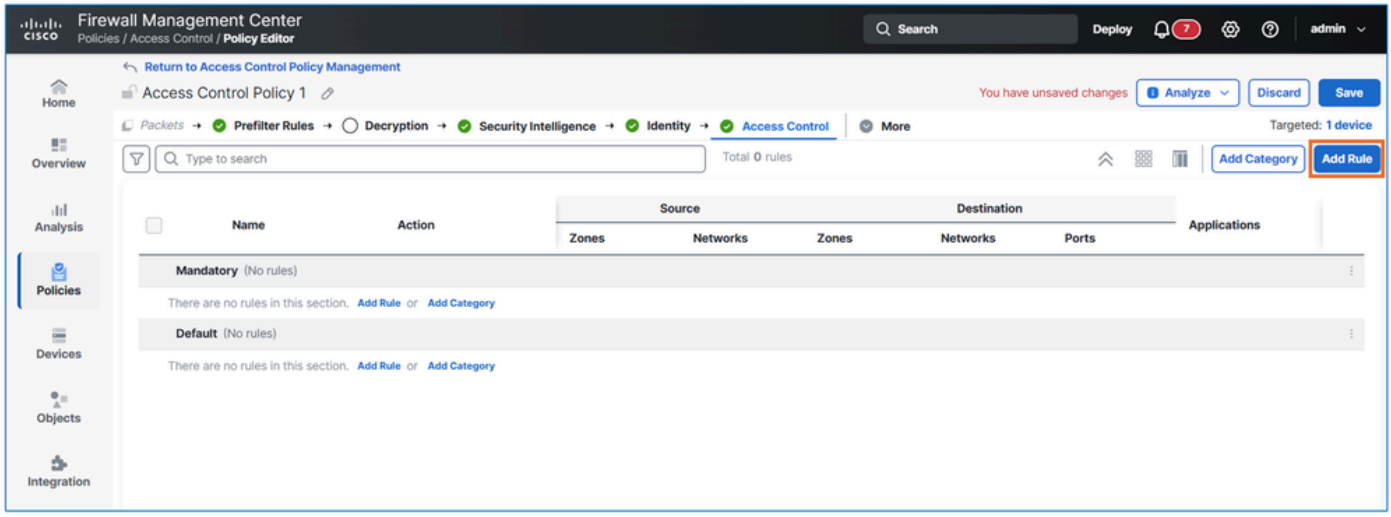
Navigieren Sie zum Abschnitt Identitätund verknüpfen Sie die mit der vorherigen Aufgabe erstellte Identitätsrichtlinie.



Identitätsrichtlinie hinzufügen

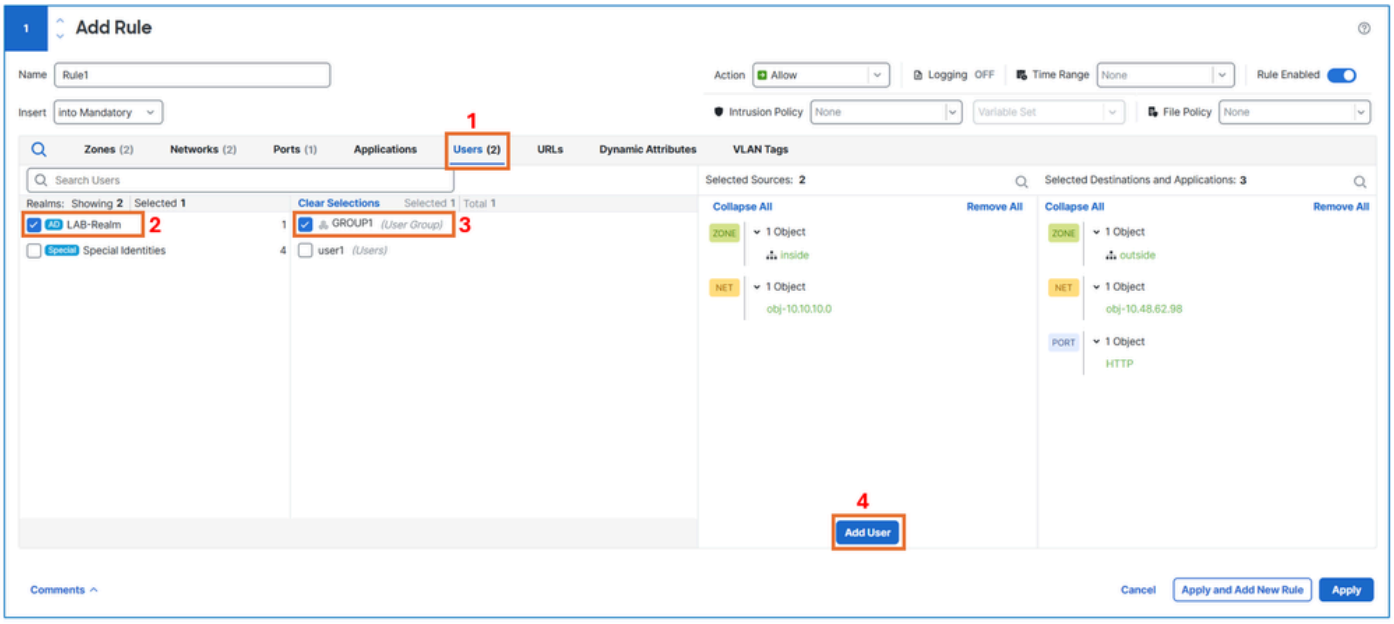
Klicken Sie auf die Schaltfläche Anwenden.

Schritt 2: Erstellen Sie die Zugriffskontrollregel (Access Control Rule).



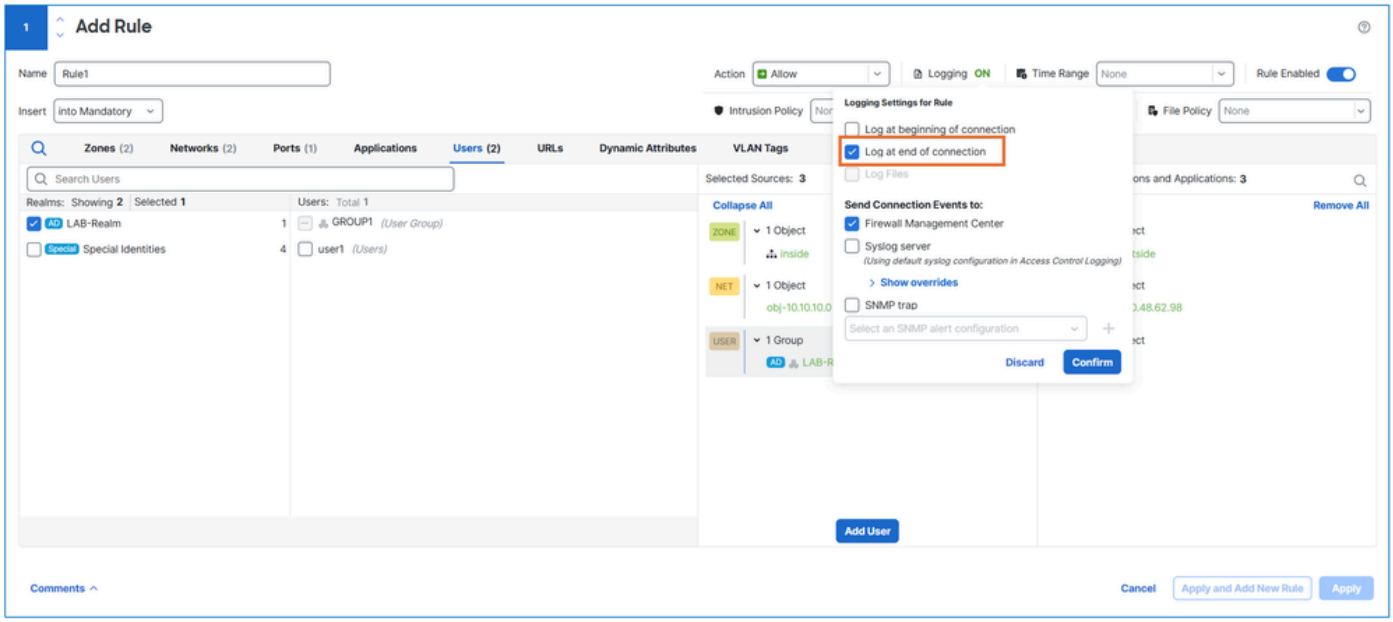
AKP erstellen

Geben Sie die Details gemäß den Aufgabenanforderungen ein, und vor allem addGROUP1 fromLAB-Realm unter derBenutzertabelle.



Benutzer zur Regel hinzufügen

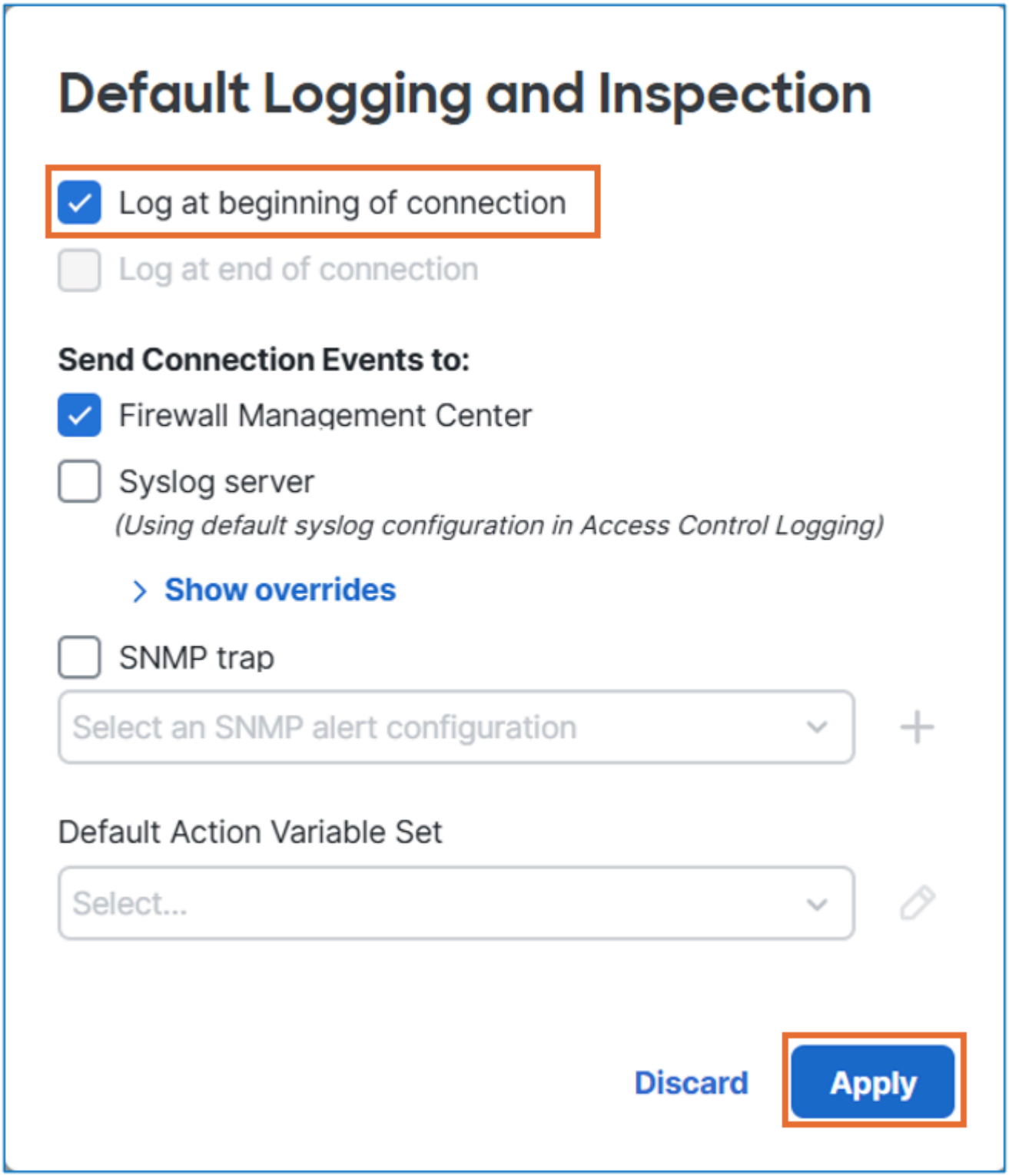
Aktivieren Sie die Protokollierung für die Regel, indem Sie am Ende der Verbindung die OptionLog auswählen.



Protokollierung aktivieren

Schritt 3: Aktivieren Sie die Protokollierung für die Standardaktion.

Klicken Sie auf dasEinstellungssymbol, um dieStandardaktionsprotokolleinstellungen zu ändern.



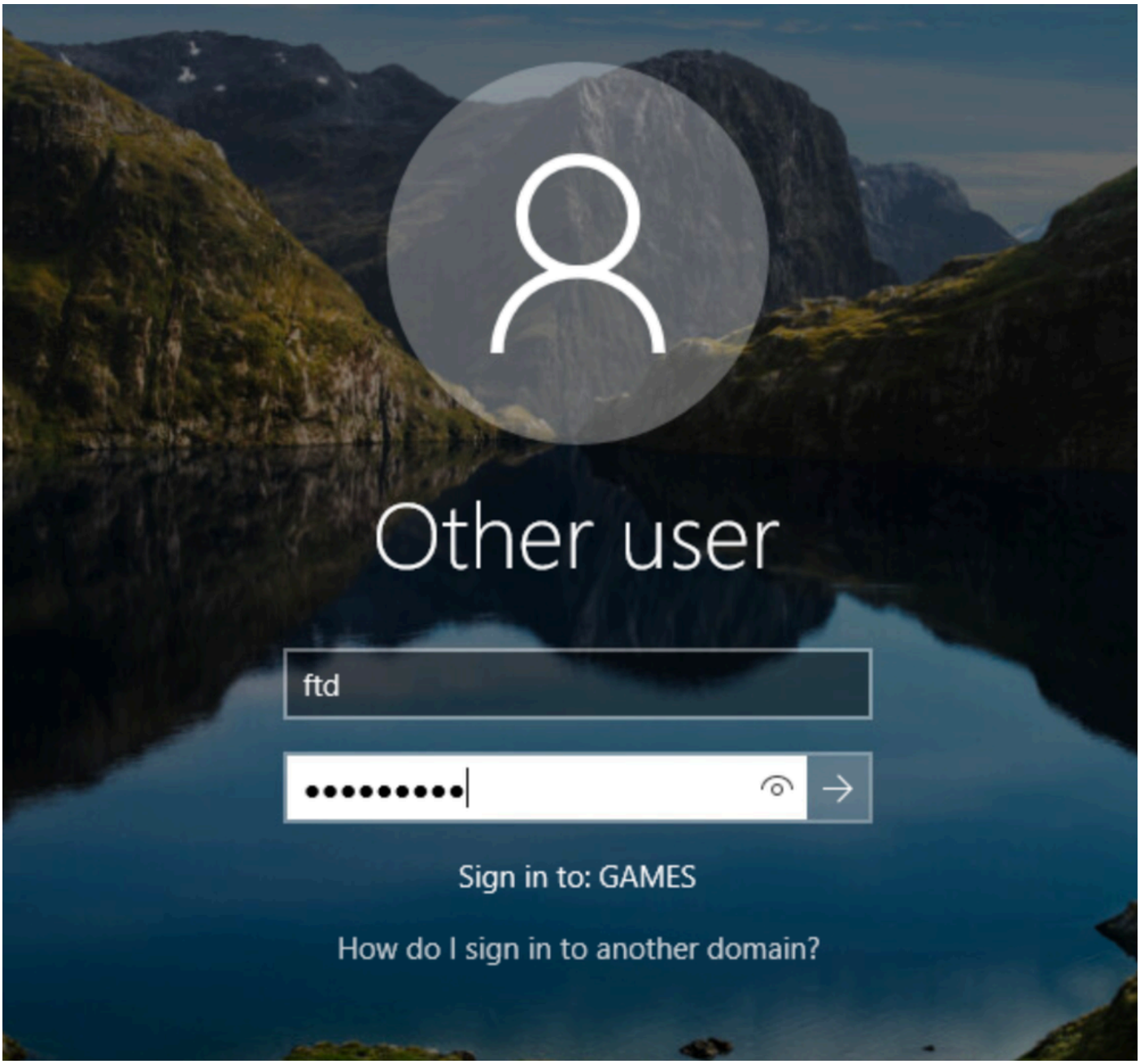
Protokollierung aktivieren

Speichern undBereitstellen der Konfiguration auf dem FTD

Verifizierung

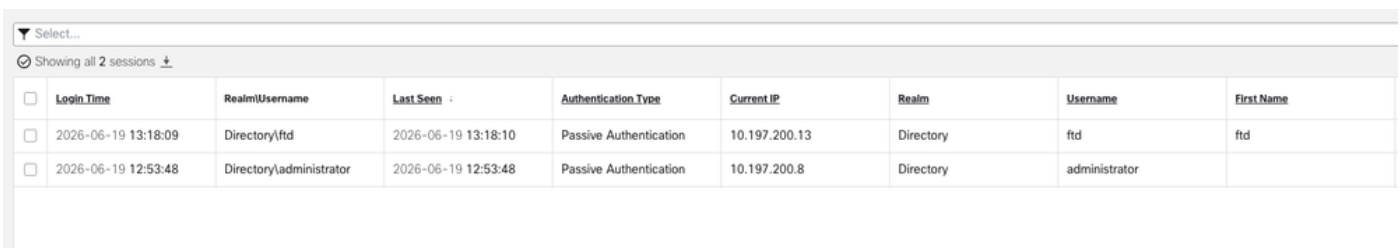
Überprüfen Sie den Vorgang der passiven Identität, indem Sie bestätigen, dass der Datenverkehr ausschließlich für ftd zulässig ist.

Melden Sie sich beim Domänenbenutzer vom Benutzercomputer an.



Benutzeranmeldung

Wenn sich ein Benutzer erfolgreich angemeldet hat, überprüfen Sie dies vom FMC unter Analysis> user >active session, um die Details des aktiven Benutzers anzuzeigen.



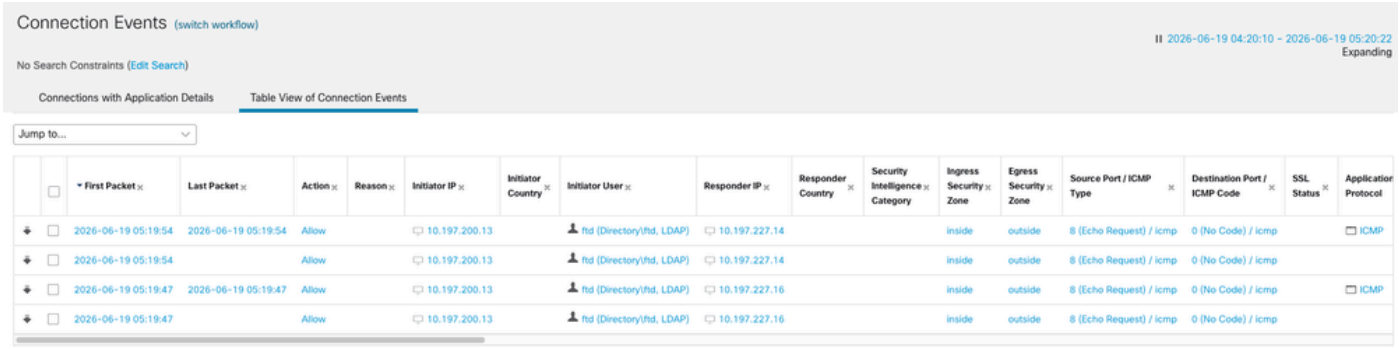
Select...

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	

Aktive Sitzungen

Nachdem Sie die Überprüfung des Datenverkehrs über die Verbindungsereignisse initiiert haben, lesen Sie die Benutzerdetails in den Verbindungsereignissen.

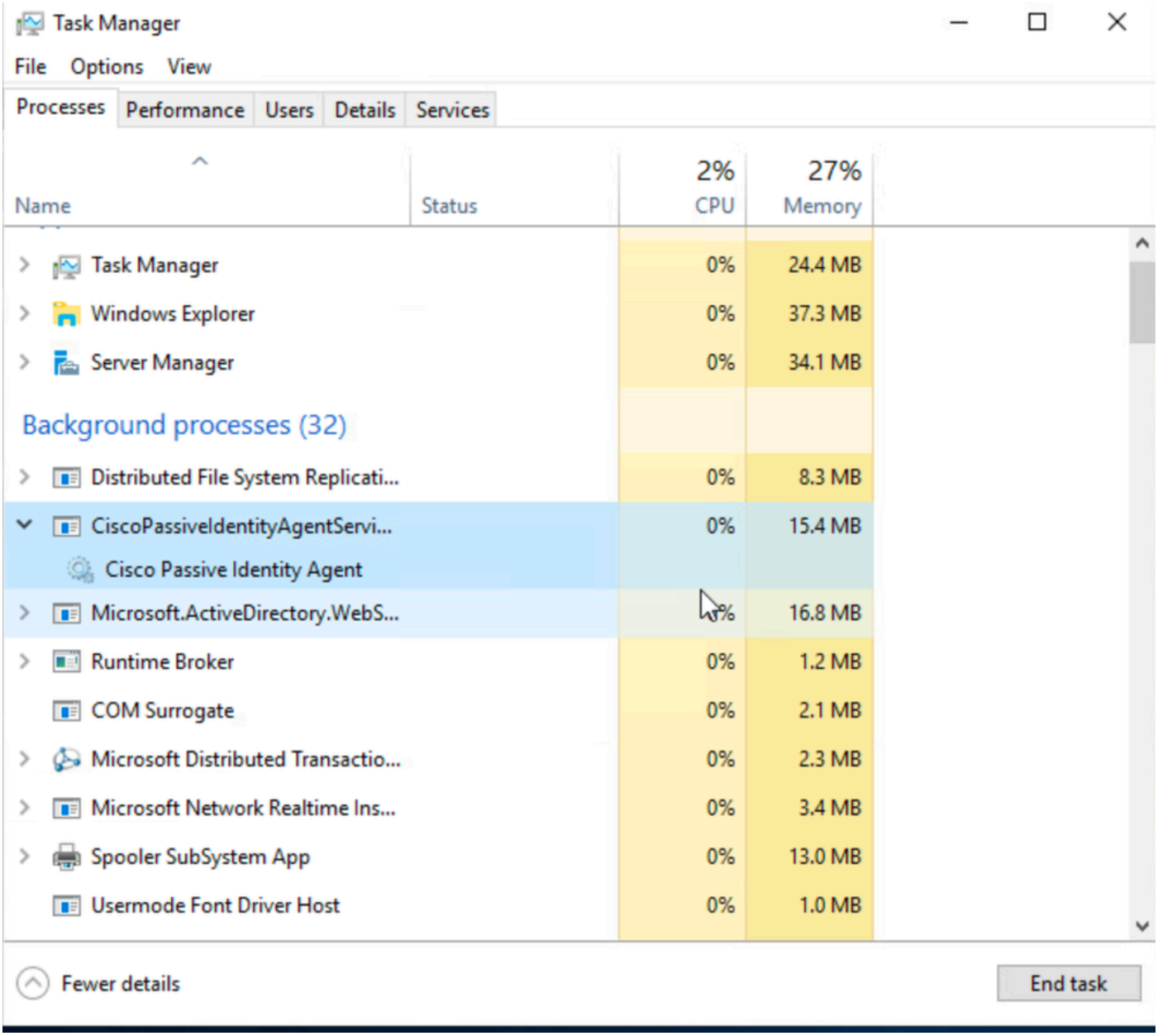


Aktive Sitzungen

Fehlerbehebung

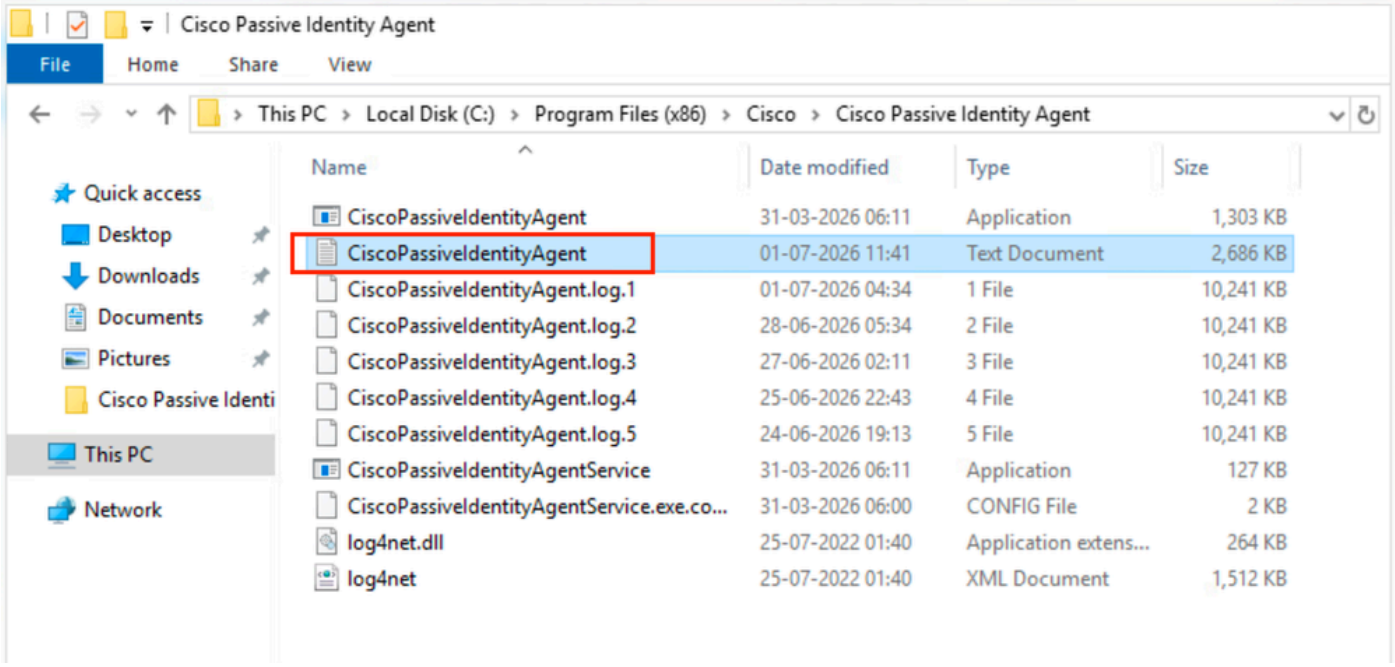
Agent-Protokolle überprüfen

Öffnen Sie auf dem Windows-Computer, auf dem der Agent gehostet wird, den Task-Manager, und überprüfen Sie, ob der Hintergrundprozess "CiscoPassiveIdentityAgentServices" ausgeführt wird.



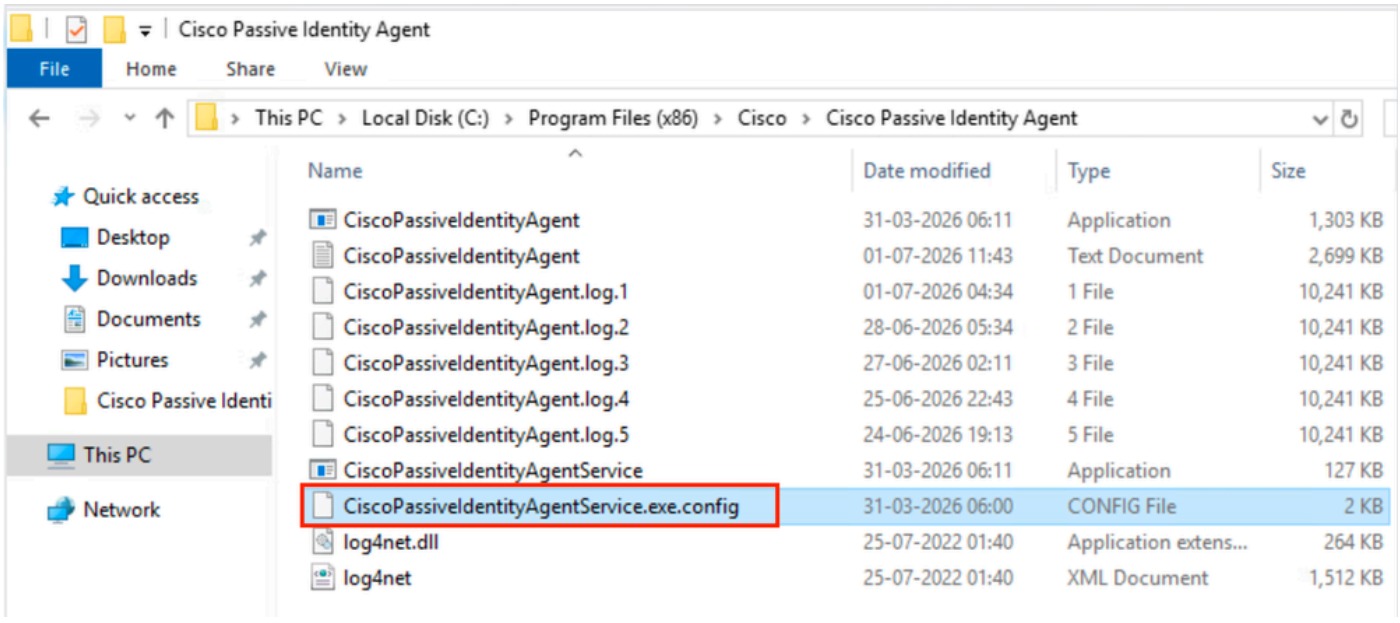
Task wird ausgeführt

Agentenprotokolle finden Sie in den CiscoPassiveIdentityAgent-Dateien, die sich standardmäßig unter folgender Adresse befinden: "C:\Program Files (x86)\Cisco\Cisco Passive Identity Agent\".



Agent

Standardmäßig werden die Agentenprotokolle auf dieINFOlevel gesetzt. Um die Protokollierung auf DEBUG-Ebene zu aktivieren, ändern Sie die Datei "CiscoPassiveIdentityAgentService.exe.configfile", und legen Sie die Protokollierungsebene auf "ALL" oder "DEBUG" fest.



Agentenkonfiguration

Informationsprotokoll

Aktivieren von Agent-Protokollen - Agent-Konfiguration abrufen.

INFO-REST-Client, Massenereignisse: [f"domain":"games.cisco.com", "srcIpAddress": "X.X.X.X", "Benutzer": "fdm", "timestamp": "01.07.2026

INFO-REST-Client, Zuordnungsstatus: OK

INFO Rest Client, REST-Beitrag erfolgreich für userBatch fdm, Latenz = 0, aktuelle DC TIME in UTC: 01.07.2026 19:47:34 ANWENDER angemeldet am

INFO Rest Client, Anfordern der Agentenkonfiguration

FMC-Protokolle

Führen Sie diesen Befehl aus, um festzustellen, ob die Zuordnung von Benutzer zu IP vom Agenten empfangen wurde.

```
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-Ausgang

Wenn der vorherige Befehl keine Zuordnung anzeigt, sammeln Sie diese Protokolle, und wenden Sie sich an das Cisco TAC.

Dies ist eine Liste der relevanten Protokolle für die FMC-API. Das Pigtail Log umfasst alle von ihnen.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.