

Konfigurieren des passiven Identitätsagenten mit FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationen](#)

[Konfigurieren einer passiven Identity Agent-Quelle](#)

[Erstellen eines passiven Identity Agent-Benutzers im Secure Firewall Management Center](#)

[Installation und Konfiguration der Software für den passiven Identitätsagent](#)

[Identitätsrichtlinien konfigurieren](#)

[Zugriffskontrollrichtlinien konfigurieren](#)

[Verifizierung](#)

[Fehlerbehebung](#)

[Agent-Protokolle überprüfen](#)

[FMC-Protokolle](#)

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.

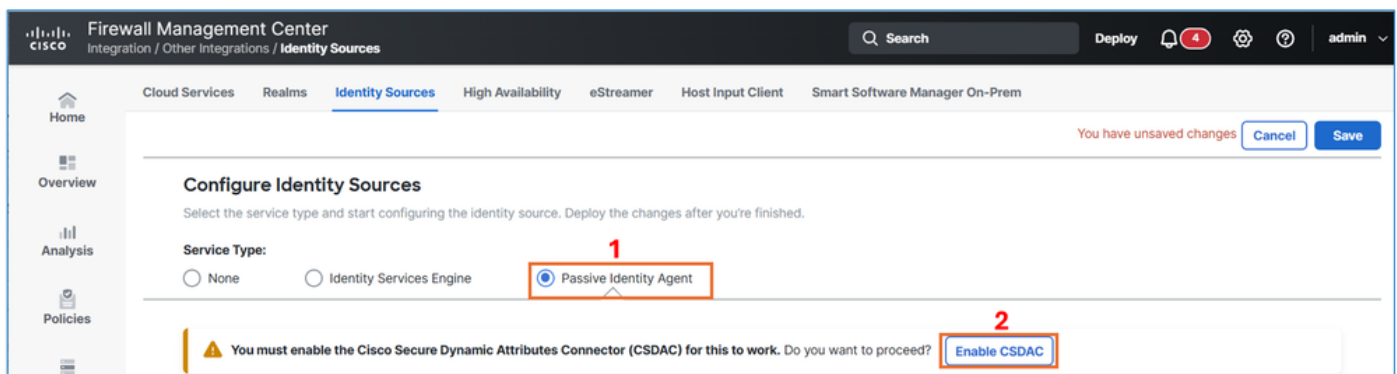
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Enable Cisco Secure Dynamic Attributes Connector?



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

Cancel

Enable

CSDAC aktivieren

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

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 aktiviert

Klicken Sie auf die Schaltfläche Agent erstellen.

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

Agent erstellen

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

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

Agent konfigurieren

Klicken Sie auf die Schaltfläche Speichern.

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**

You have unsaved changes [Cancel](#) [Save](#)

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			

Speichern Sie die Konfiguration.

Ergebnis.

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**

[Cancel](#) [Save](#)

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	

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.

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

Benutzer erstellen

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

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
 - ☒ Passive Identity User
- Custom User Roles
- ☐ REST VDI

Cancel

Save

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 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

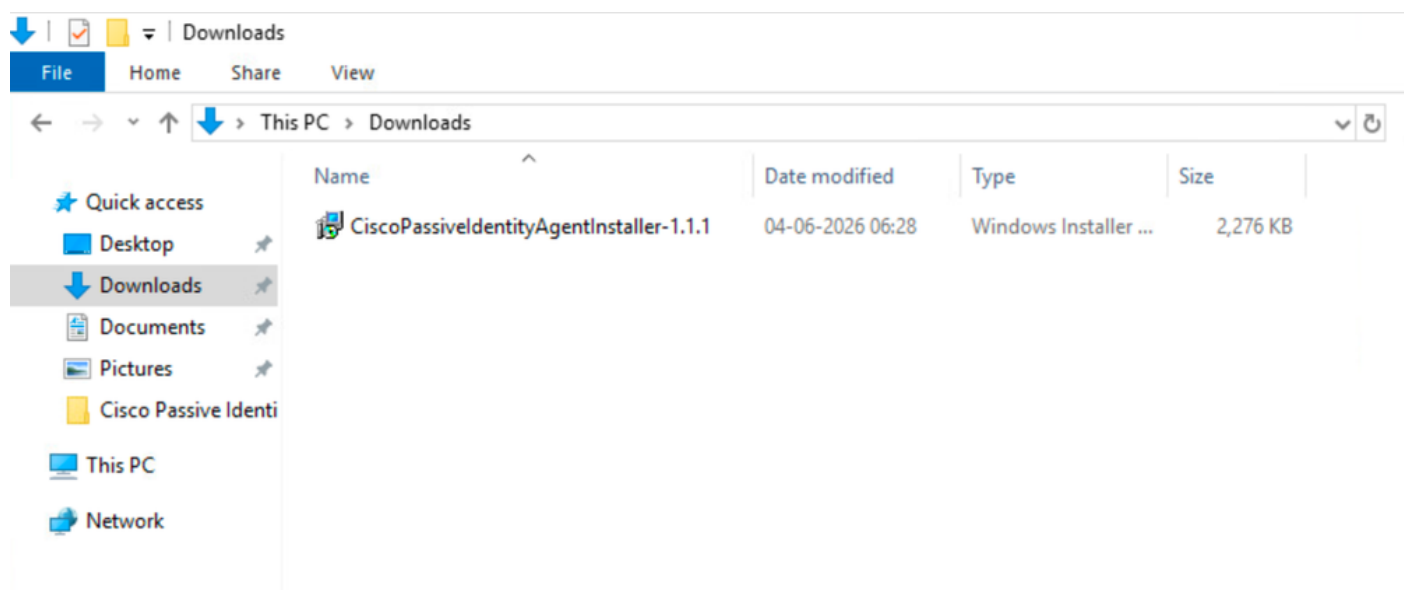
Release Notes for Passive Identity Agt

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

Software herunterladen

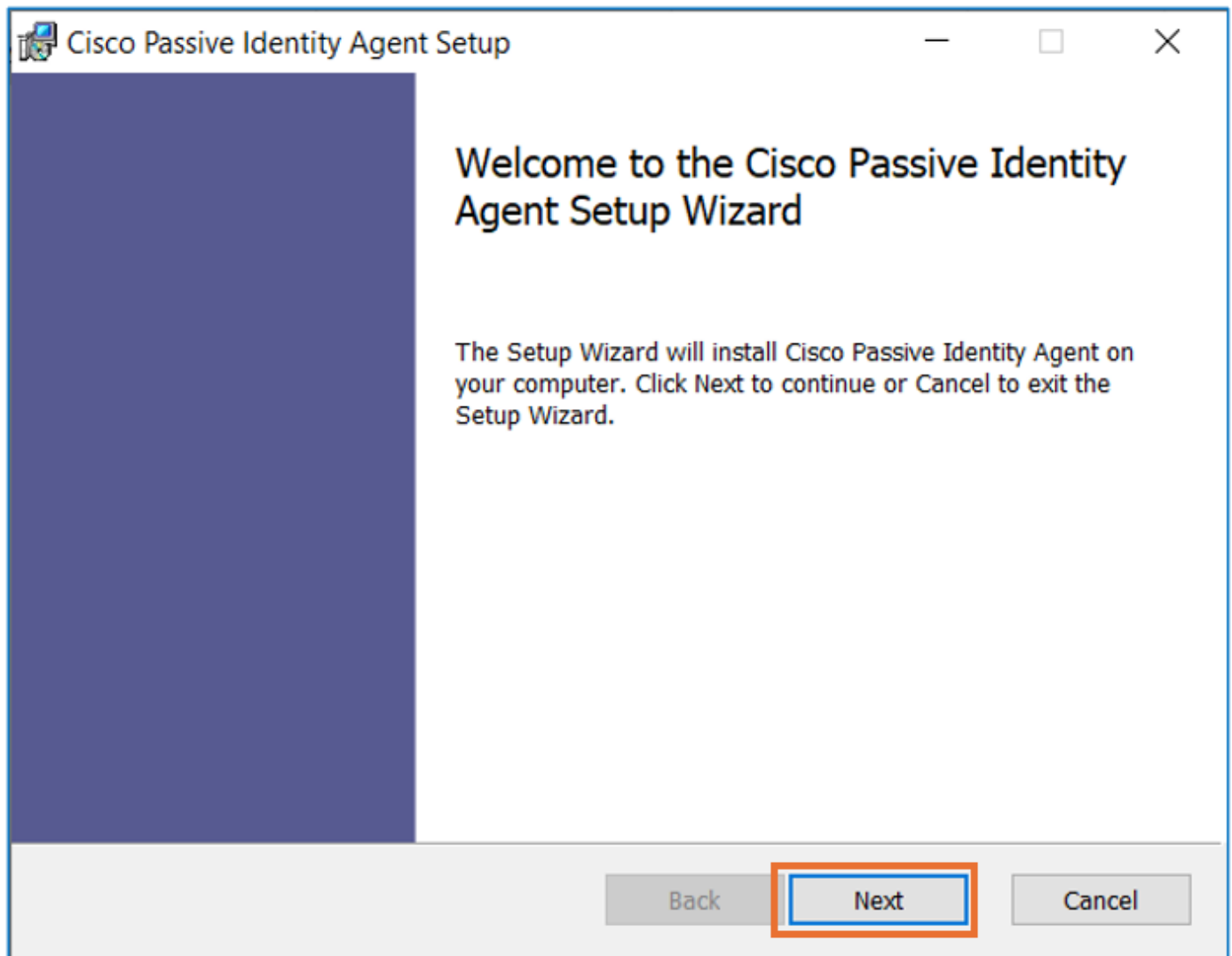
Starten Sie nach dem Herunterladen des Agenten den Installationsvorgang auf dem Domänencontroller.



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.

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

Search

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

Konfigurieren Sie den Agenten.

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

 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

Klicken Sie auf OK, um die Agentenkonfiguration abzuschließen.

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

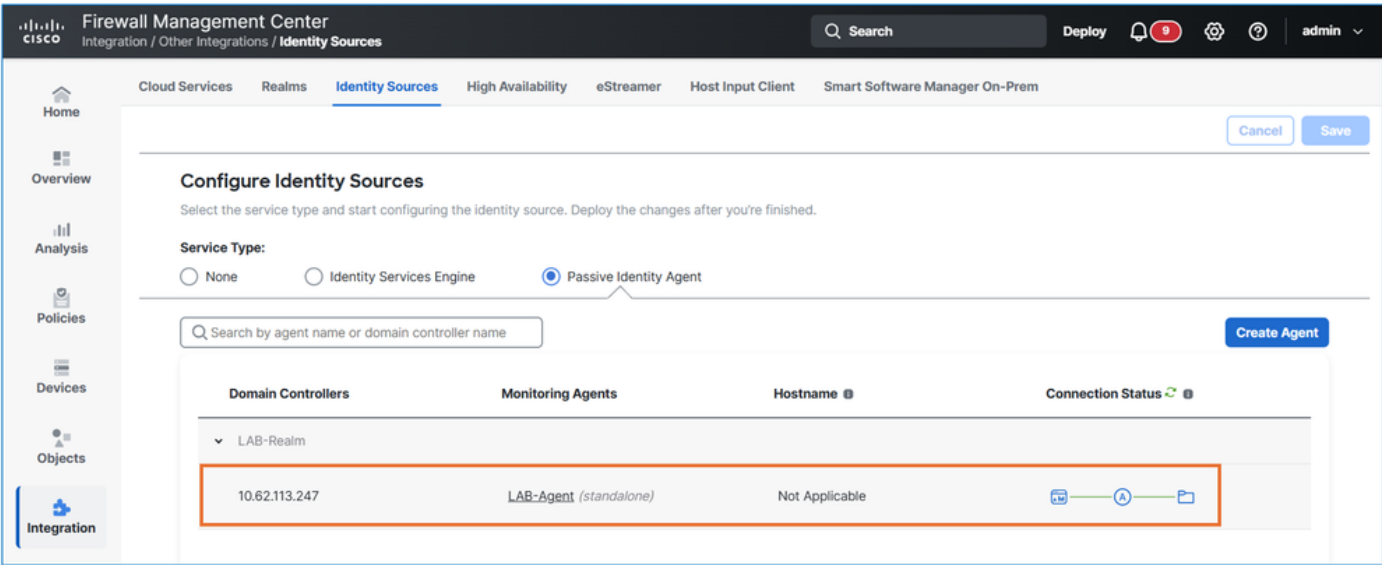
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

Agent wird ausgeführt

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



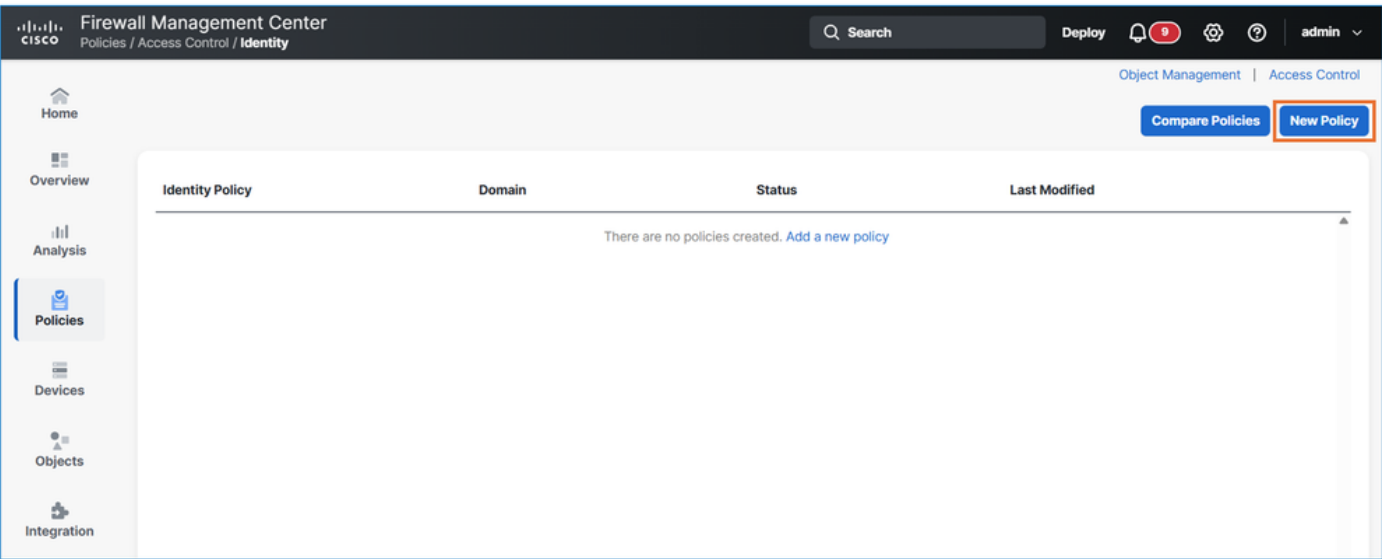
die Kommunikation von fmc überprüfen

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.

New Identity policy

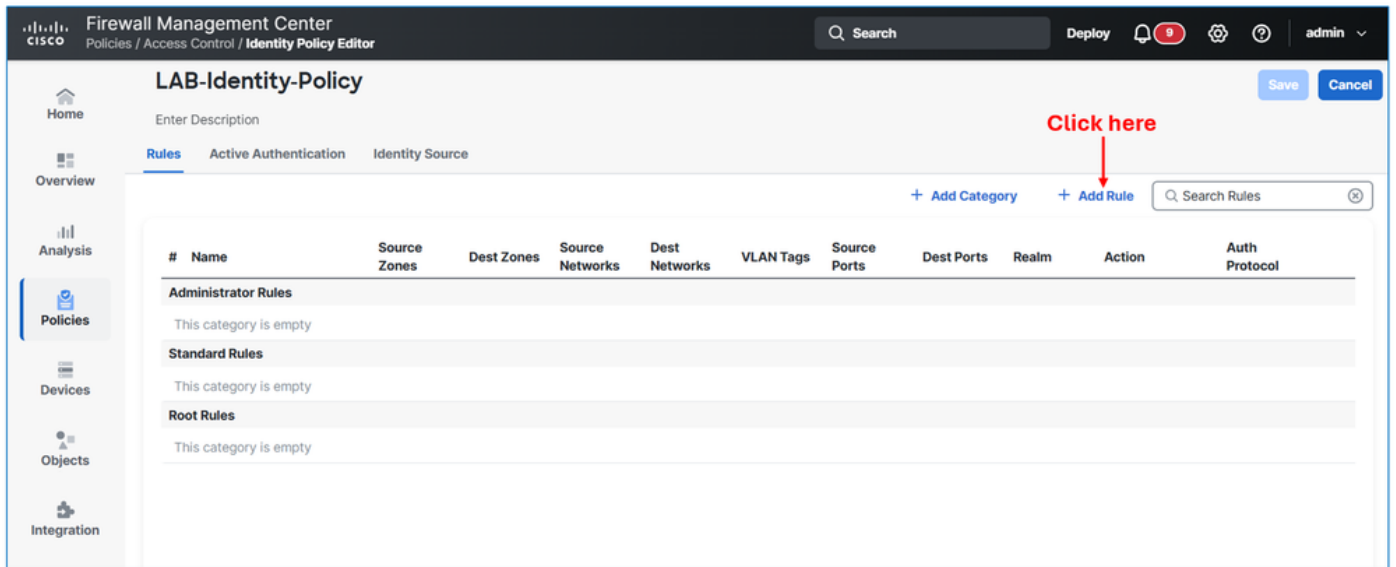
Name

Description

[Cancel](#) [Save](#)

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.

Add Rule

Name
☒ 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

1

Realm & Settings

Authentication Realm *

2

LAB-Realm (AD)

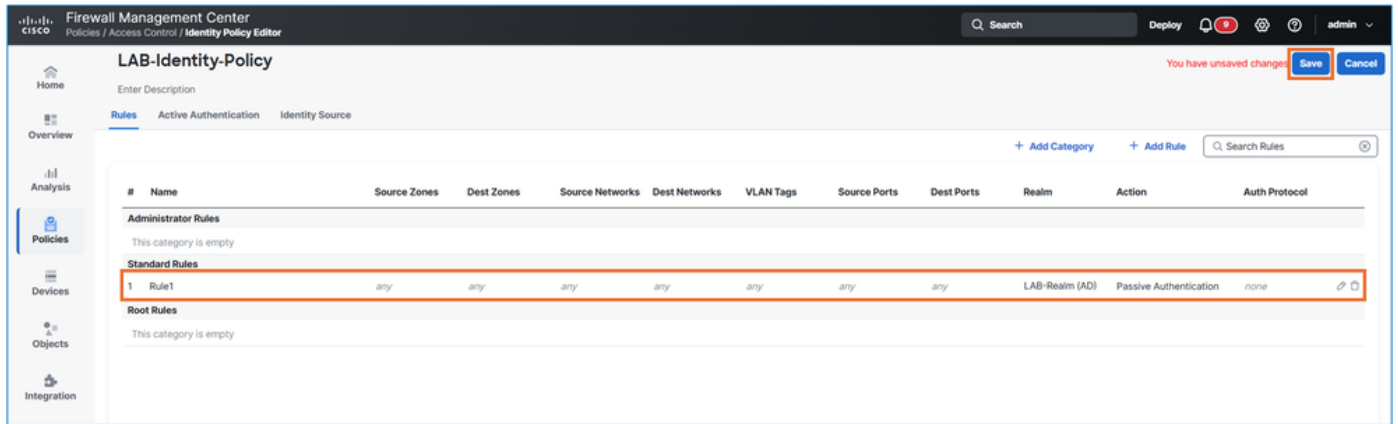
☐ Use active authentication if passive or VPN identity cannot be established

3

Cancel
Add

Bereichseinstellung

Klicken Sie auf die Schaltfläche Speichern.



Konfig. speichern

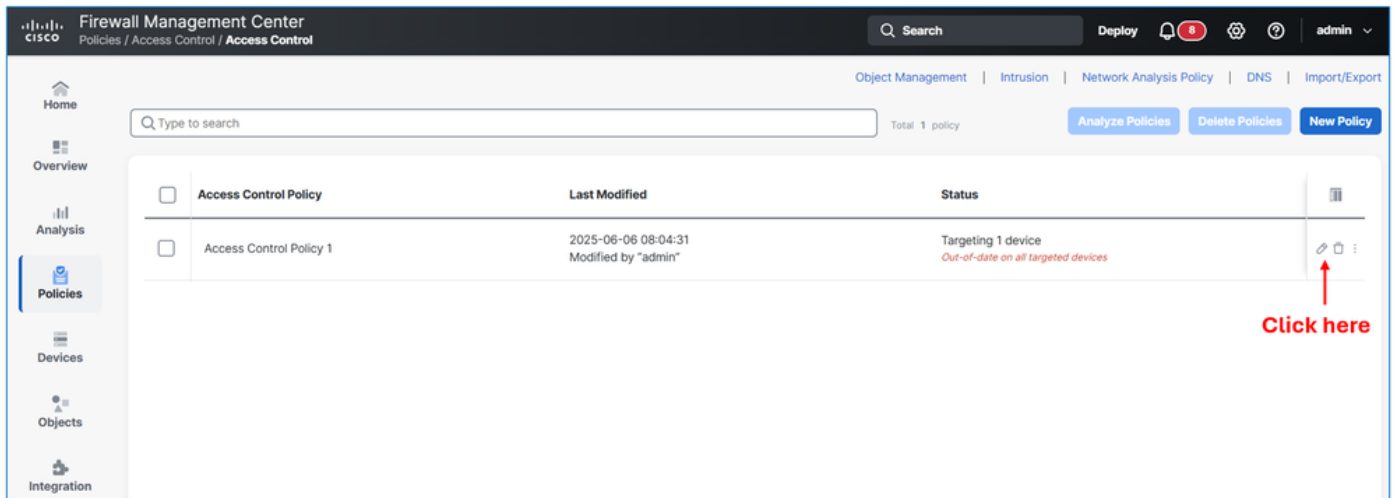
Zugriffskontrollrichtlinien konfigurieren

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

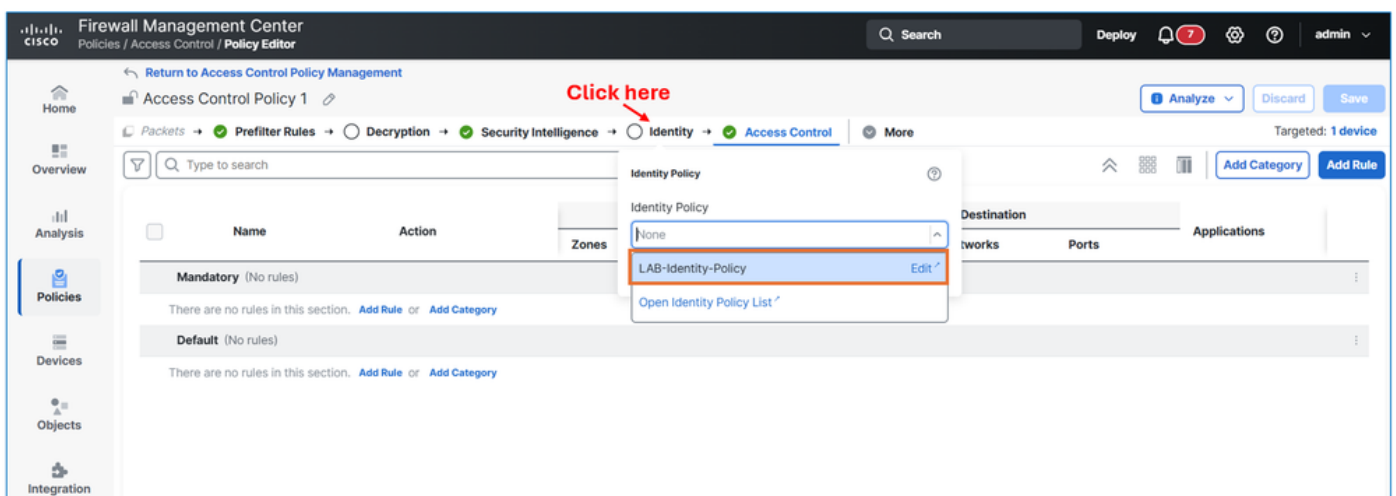
Schritt 1: Verknüpfen der Identitätsrichtlinie mit der Richtlinie für die Zugriffskontrolle

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



Richtlinie bearbeiten

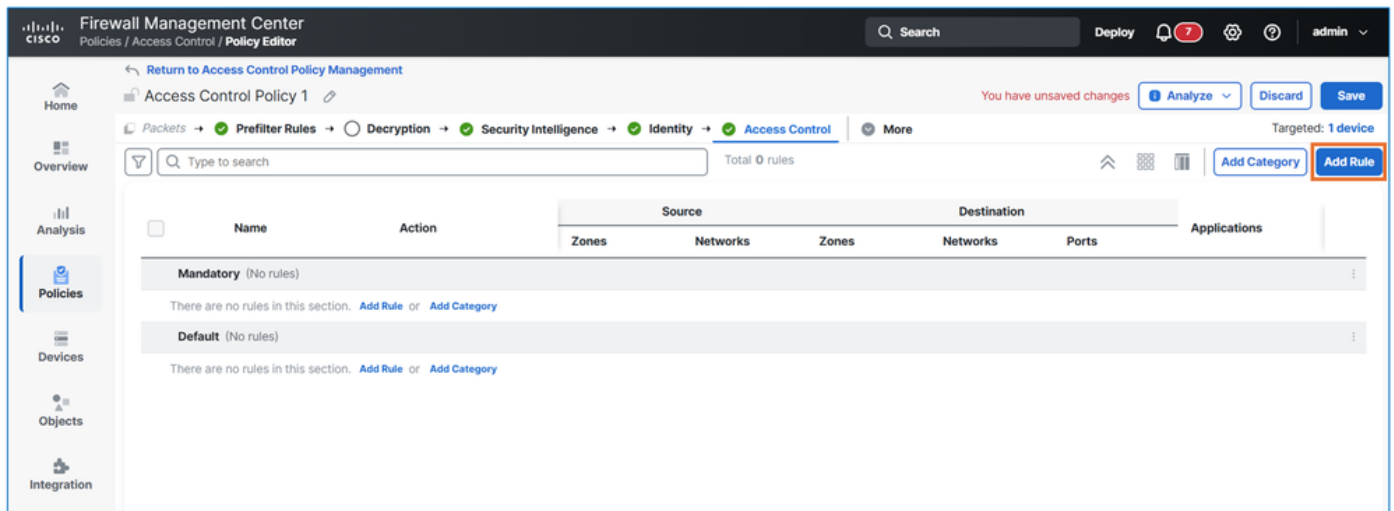
Navigieren Sie zum Abschnitt **Identität** und verknüpfen Sie die mit der vorherigen Aufgabe erstellte Identitätsrichtlinie.



Identitätsrichtlinie hinzufügen

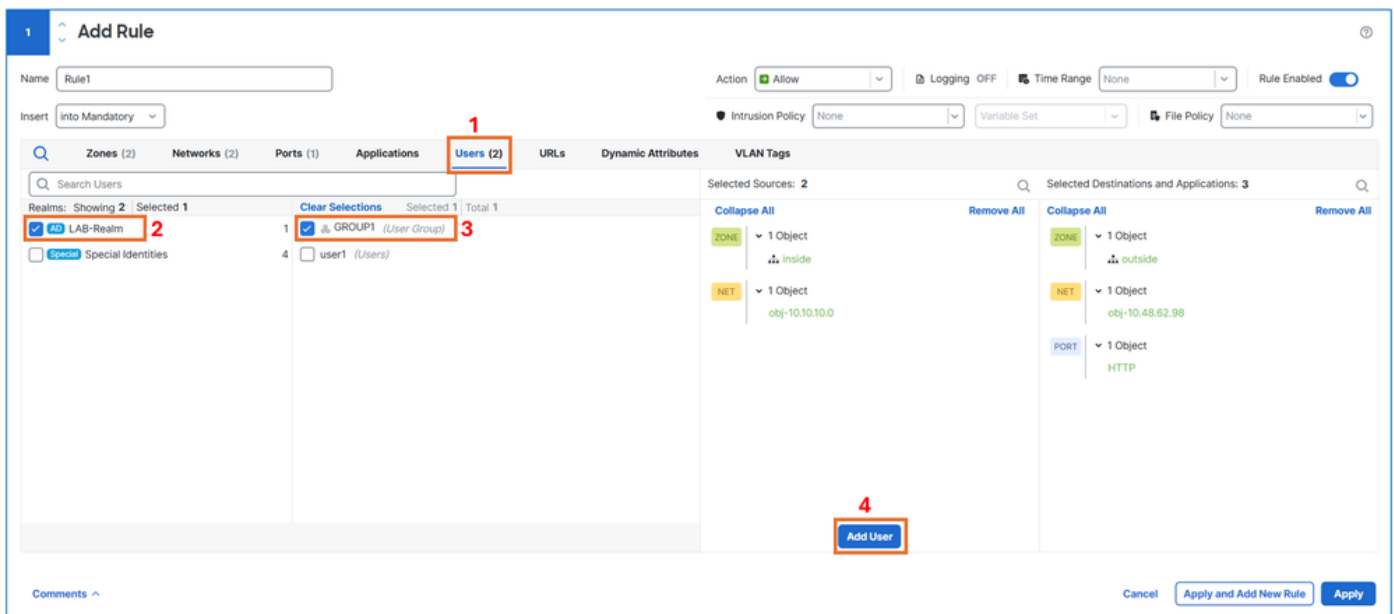
Klicken Sie auf die Schaltfläche **Anwenden**.

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



AKP erstellen

Geben Sie die Details gemäß den Aufgabenanforderungen ein, und vor allem addGROUP1 from LAB-Realm unter der Benutzertabelle.



Benutzer zur Regel hinzufügen

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

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

☒ LAB-Realm

☐ 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

Comments ^

Protokollierung aktivieren

Schritt 3: Aktivieren Sie die Protokollierung für die Standardaktion.

Klicken Sie auf das Einstellungssymbol, um die Standardaktionsprotokolleinstellungen zu ändern.

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

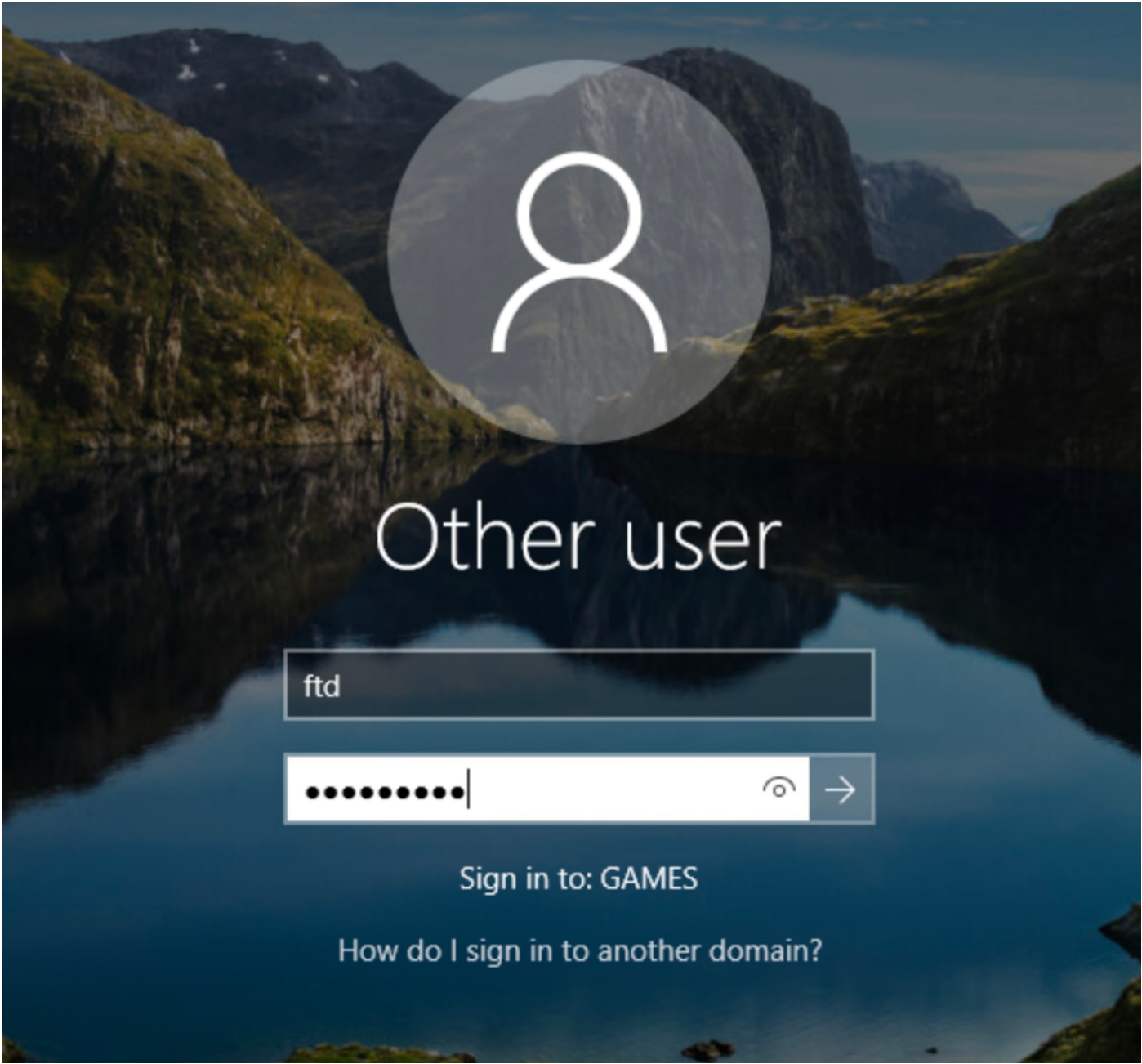
Protokollierung aktivieren

Speichern und Bereitstellen 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.

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

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 Manager

File Options View

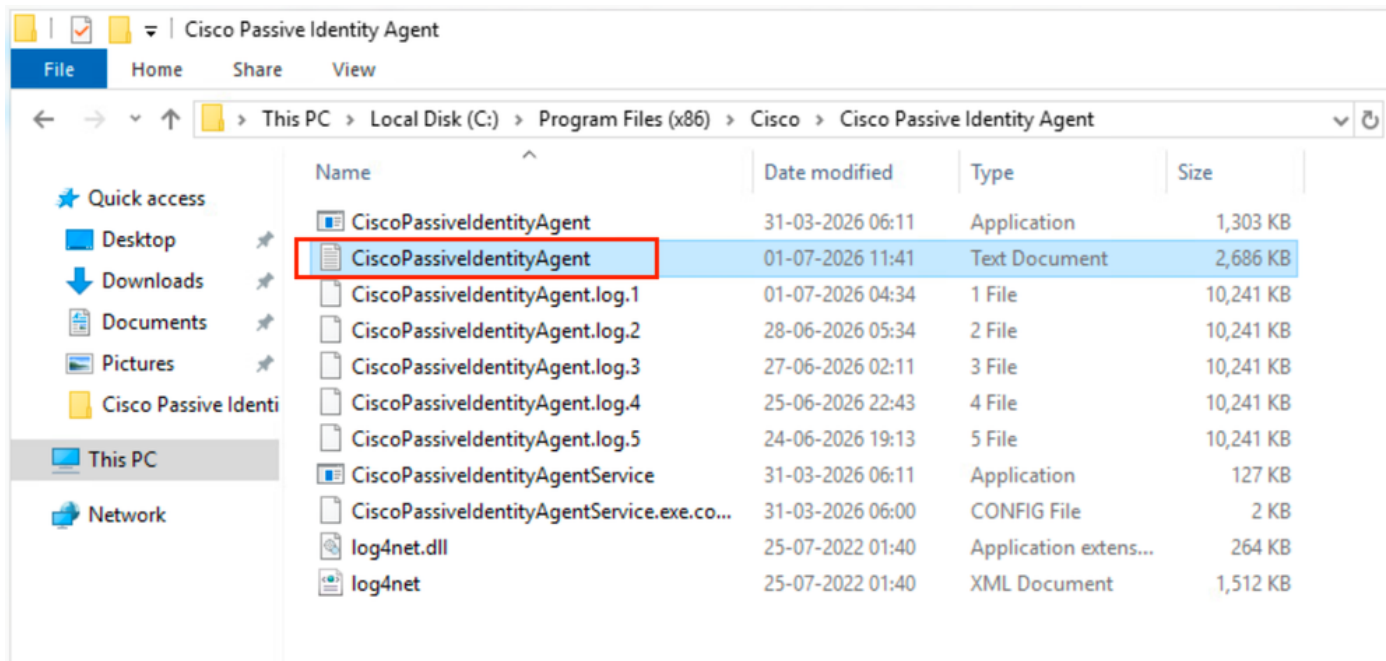
Processes Performance Users Details Services

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			
> 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

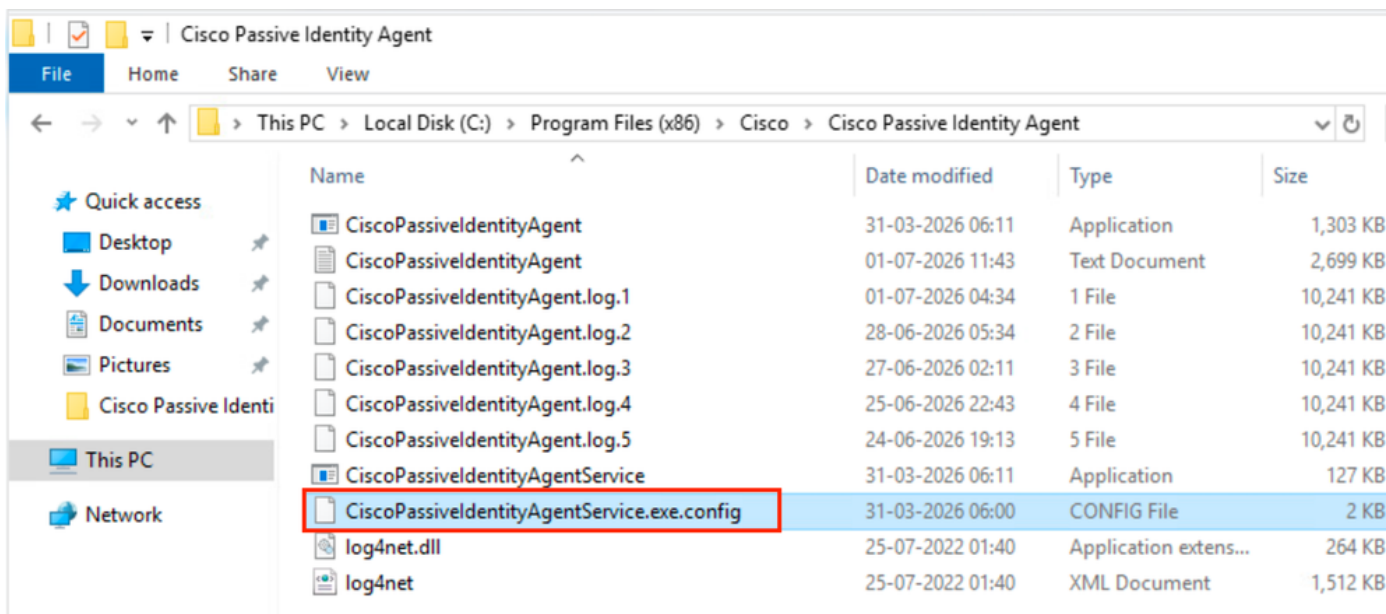
Task wird ausgeführt

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 die INFO-Ebene gesetzt. Um die Protokollierung auf DEBUG-Ebene zu aktivieren, ändern Sie die Datei "CiscoPassiveIdentityAgentService.exe.config", und legen Sie die Protokollierungsebene auf "ALL" oder "DEBUG" fest.



Agentenkonfiguration



```
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>
```

Informationsprotokoll

Aktivieren von Agent-Protokollen - Agent-Konfiguration abrufen.

INFO-REST-Client, Massenereignisse: [{"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.