

FMCを使用したパッシブIDエージェントの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーション](#)

[パッシブIDエージェントソースの設定](#)

[Secure Firewall Management CenterでのパッシブIDエージェントユーザの作成](#)

[Passive Identity Agentソフトウェアのインストールと設定](#)

[アイデンティティポリシーの設定](#)

[アクセスコントロールポリシーの設定](#)

[検証](#)

[トラブルシューティング](#)

[エージェントログの確認](#)

[FMCログ](#)

はじめに

このドキュメントでは、セッションデータをFMCに送信するパッシブIDエージェントソース (PID)を設定する方法について説明します

前提条件

要件

- バージョン7.6以降を実行しているCisco Secure Firewall Management Center
- バージョン7.6以降を実行しているCisco Secure Firewall
- Windows Active Directoryサーバの場合、サーバはWindows Server 2008以降を実行する必要があります。
- セキュアファイアウォール脅威対策デバイスでSnort 3を有効にする必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall Management Center 7.6.5
- Cisco Secureファイアウォール7.6.5
- Windows Server 2022上で動作するMicrosoft Active Directory

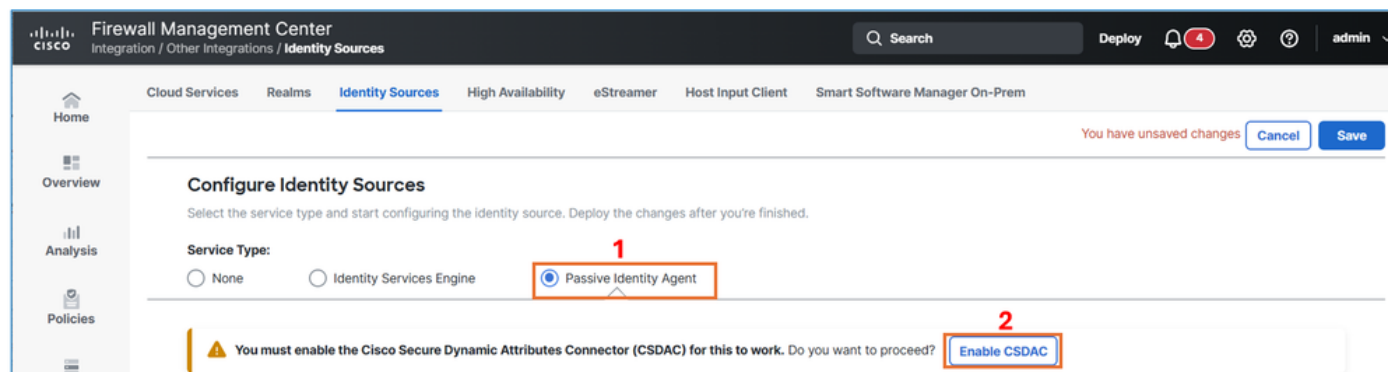
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

コンフィギュレーション

エージェントを設定する前に、ADとFMCの統合を完了してください。

パッシブIDエージェントソースの設定

FMC UIで、Integration > Other Integrations > Identity Sourcesの順に移動し、Passive Identity Agentをクリックします。Cisco Secure Dynamic Attributes Connectorがまだ有効になっていない場合は、Enable CSDACをクリックして有効にするように求められます。



パッシブIDエージェント

CSDACを有効にするには、[有効]ボタンをクリックします。

Enable Cisco Secure Dynamic Attributes Connector?



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

Cancel

Enable

CSDACを有効にする

このステップには約10分かかります。CSDACが正しく有効化されたら、「Donebutton」をクリックして続行します。

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有効

Create Agentbuttonをクリックします。

Firewall Management Center
Integration / Other Integrations / Identity Sources

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?

```
graph LR
    FMC[Firewall Management Center] -- 1 --> Agents[Primary Agent / Secondary Agent]
    Agents -- 2 --> DC[Domain Controllers]
    DC -- 3 --> Agents
    Agents -- 4 --> FMC
    Agents -- 5 --> Agents
```

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](#)

エージェントの作成

エージェントの名前を定義し、Standaloneoptionを選択して、前のタスクで作成した適切なDomainコントローラに関連付けます。

Configure Agent



Name *

LAB-Agent

Description

Role ⓘ



Primary



Secondary



Standalone

[Learn more](#) about the agent role.

Domain Controller *

10.62.113.247 ×



Agent will monitor this domain controller.

Important:

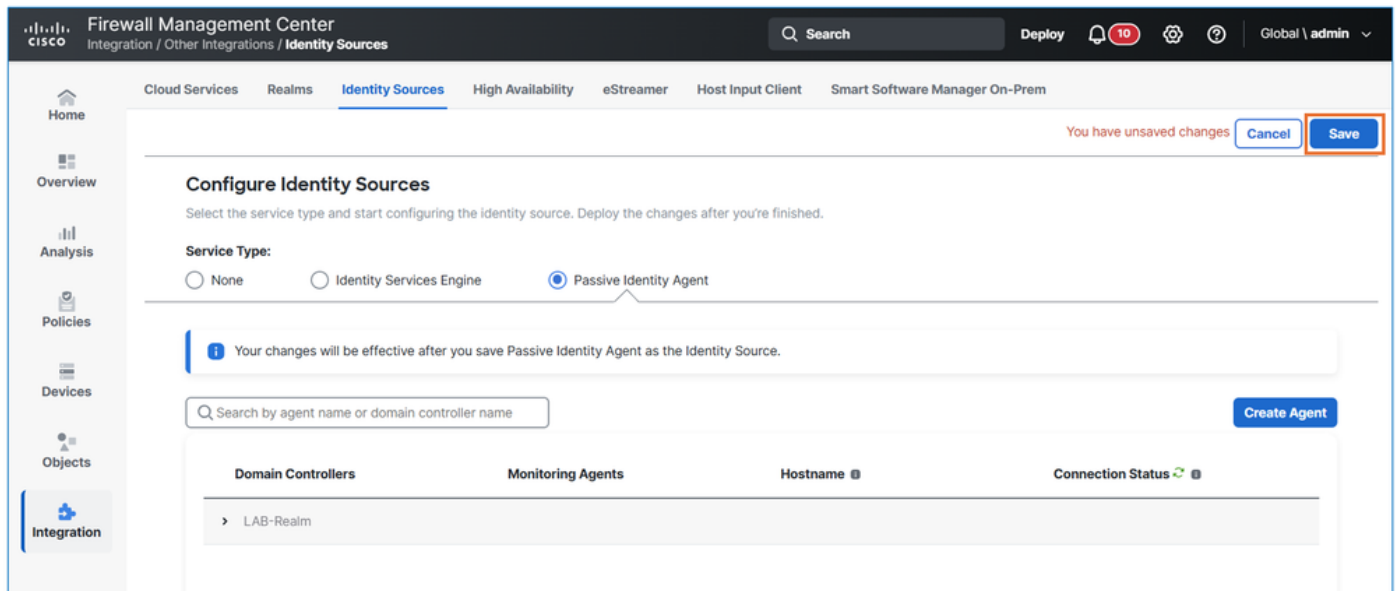
This agent will be created and assigned to the selected domain controller. Install it on the domain controller (or on its member machine) to start the tracking.

Cancel

Save

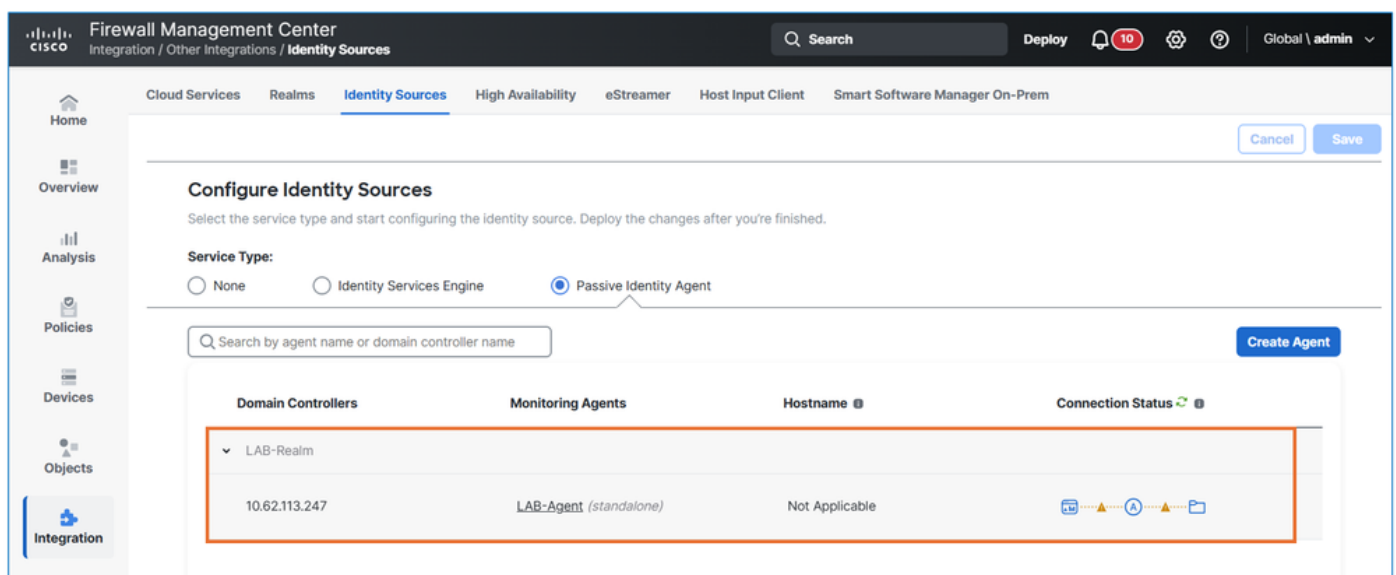
エージェントの設定

「保存」ボタンをクリックします。



設定の保存

結果です。



ステータスの確認



注：パッシブIDエージェントは回線を使用してステータスを示します。オレンジ色の場合、エージェントがSecure Firewall Management Centerと正常に通信していないことを示します。新しく作成されたエージェント回線はオレンジ色で、設定が完了するまでオレンジ色のままです。

Secure Firewall Management CenterでのパッシブIDエージェントユーザの作成

パッシブIDエージェントと通信するために十分な権限を持つセキュアファイアウォール管理センター(FMC)ユーザを作成します。このユーザには、他のタスクを実行する権限が制限されています。ユーザは、パッシブIDエージェントとの通信のみを有効にすることが想定されています。

FMCのUIで、System > Usersに移動し、Create Userをクリックします。タスクの要件に従って、ユーザの詳細を入力します。

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

ユーザーの作成

パッシブIDユーザロールのみを割り当てます。「保存」ボタンをクリックします。

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

パッシブidユーザの選択

Passive Identity Agentソフトウェアのインストールと設定

指定されたドメインコントローラにPassive Identity Agentソフトウェアをインストールして設定します。

software.cisco.comからpassive identity agentをダウンロードします。

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

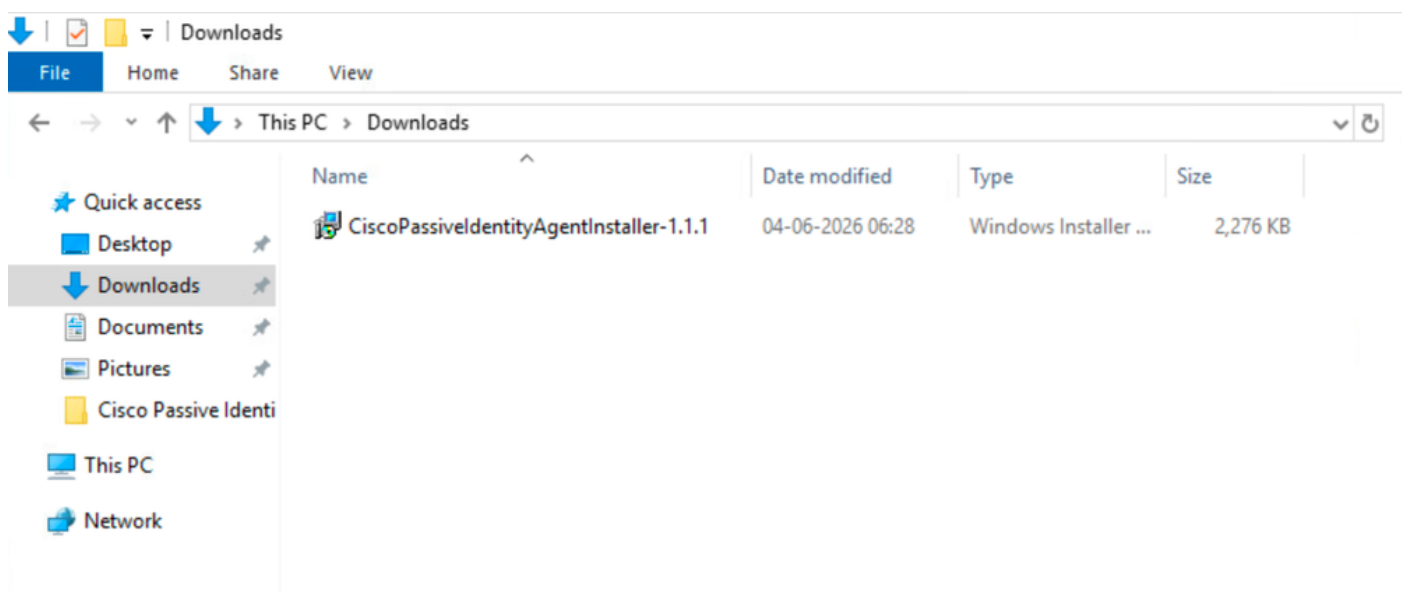
Release Passive Identity Agt
[My Notifications](#)

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

ソフトウェアのダウンロード

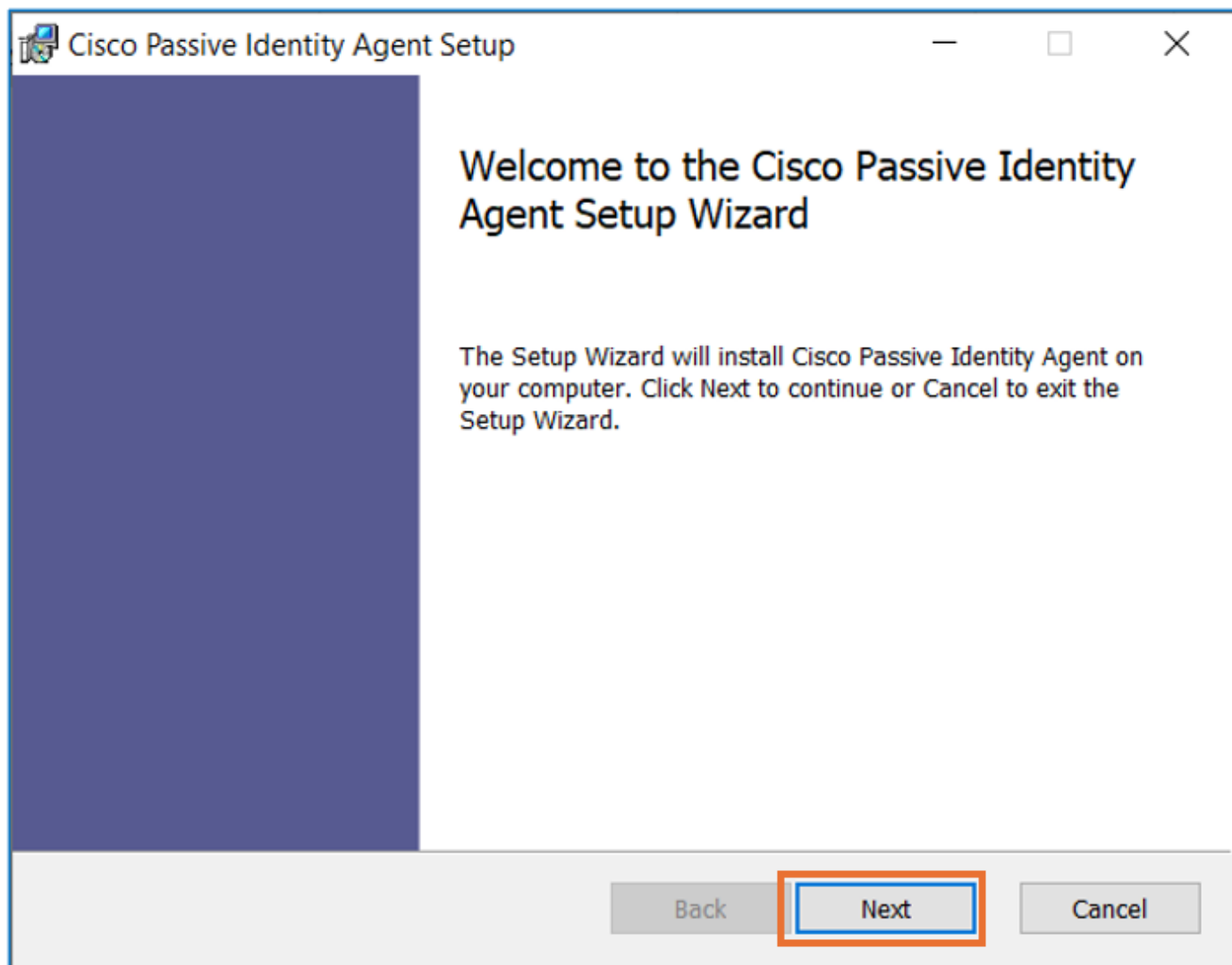
エージェントをダウンロードしたら、ドメインコントローラでインストールプロセスを開始します。



エージェント

]

セットアップを完了するには、付属のインストール手順を参照してください。



インストールするもの

インストールが完了したら、Passive Identity Agentソフトウェアを開き、タスク要件で指定されている必要な情報を入力します。Testボタンをクリックして、FMCとの接続を確認します。

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 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

I have **Secondary** FMC ▾

Username/Password created in previous task

Click here to test the connectivity

エージェントを設定します。

接続のテストが正常に終了したら、「保存」ボタンをクリックします。

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

テスト

OKボタンをクリックして、エージェントの設定を完了します。

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

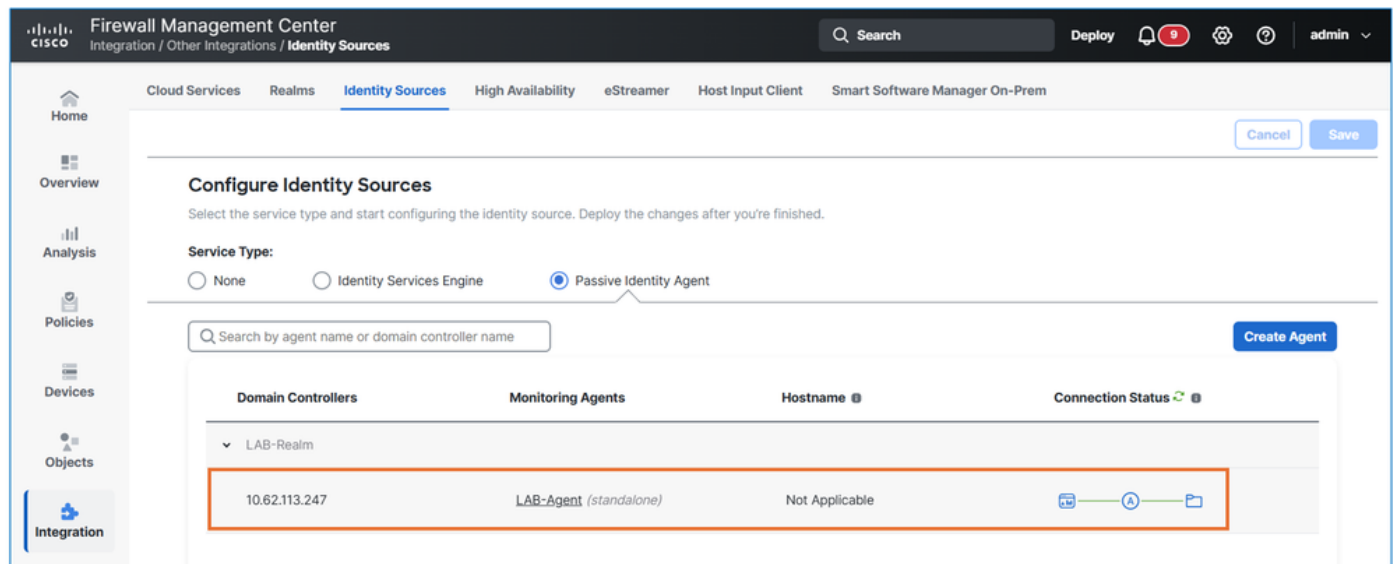
Primary FMC FQDN / IP Address:	10.62.184.97
Port:	443
Username:	passiveidentity
Password:	*****
Agent Name:	LAB-Agent
Agent Domain Controllers:	10.62.113.247

Edit..

OK

エージェントは実行中です

FMCのUIで、Integration > Other Integrations > Identity Sources > Passive Identity Agentの順に移動します。パッシブIDエージェントが緑色のステータスを表示していることを確認します。



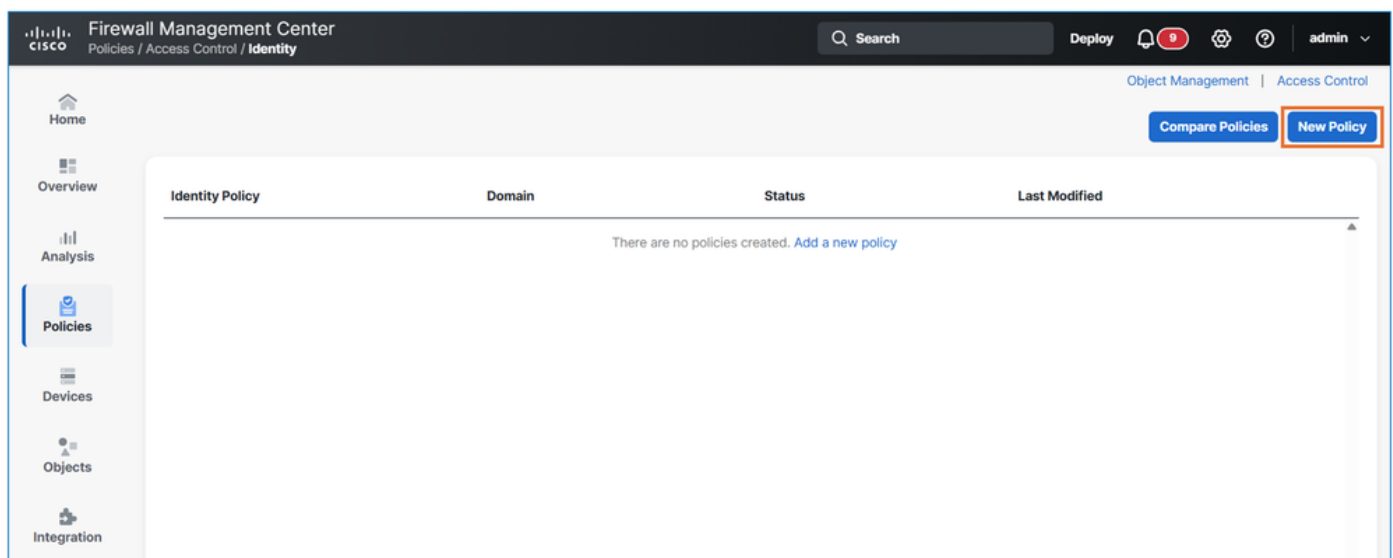
fmcからの通信の確認

アイデンティティポリシーの設定

提供されたテーブルに基づいてアイデンティティポリシーを作成します。

ポリシー名	ルール名	認証レム	残りの設定
ラボIDポリシー	ルール1	ラボ領域	デフォルトのままにする

FMCのUIで、Policies > Access Control > Identityの順に移動します。New Policybuttonをクリックします。



新しいポリシー

タスクの要件に従ってポリシー名を入力します。

New Identity policy

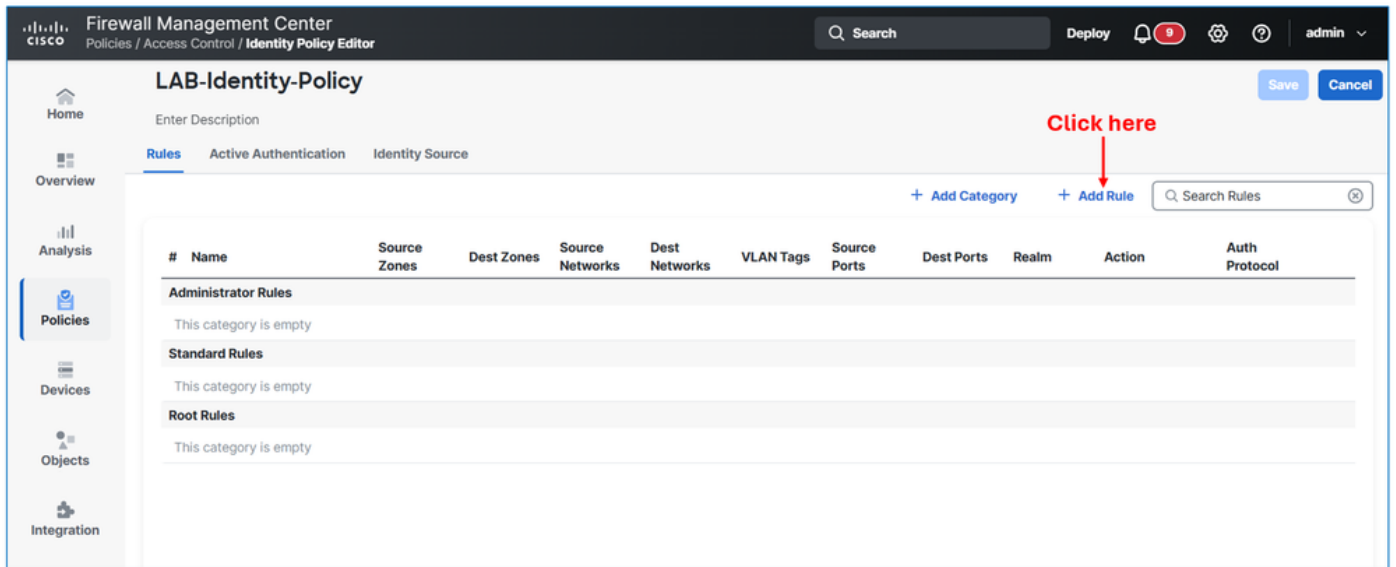
Name

Description

CancelSave

新しいポリシー

Add Rulebuttonをクリックします。

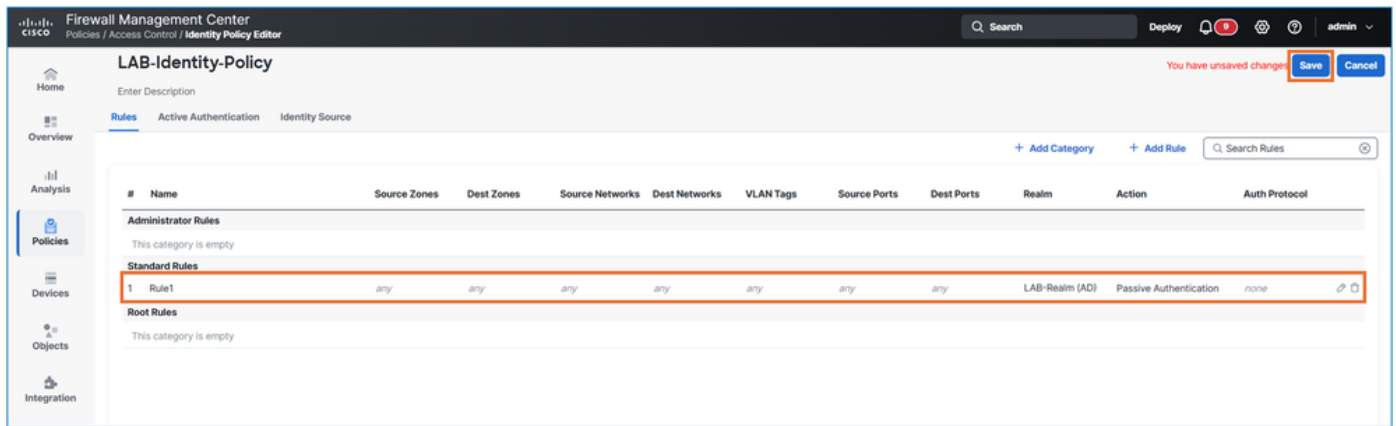


ルールの作成

Realm & Settingstabに移動し、タスク要件に基づいてAuthentication Realmbasedを選択します。最後に、Addbuttonをクリックします。

レールの設定

「保存」ボタンをクリックします。



設定を保存します

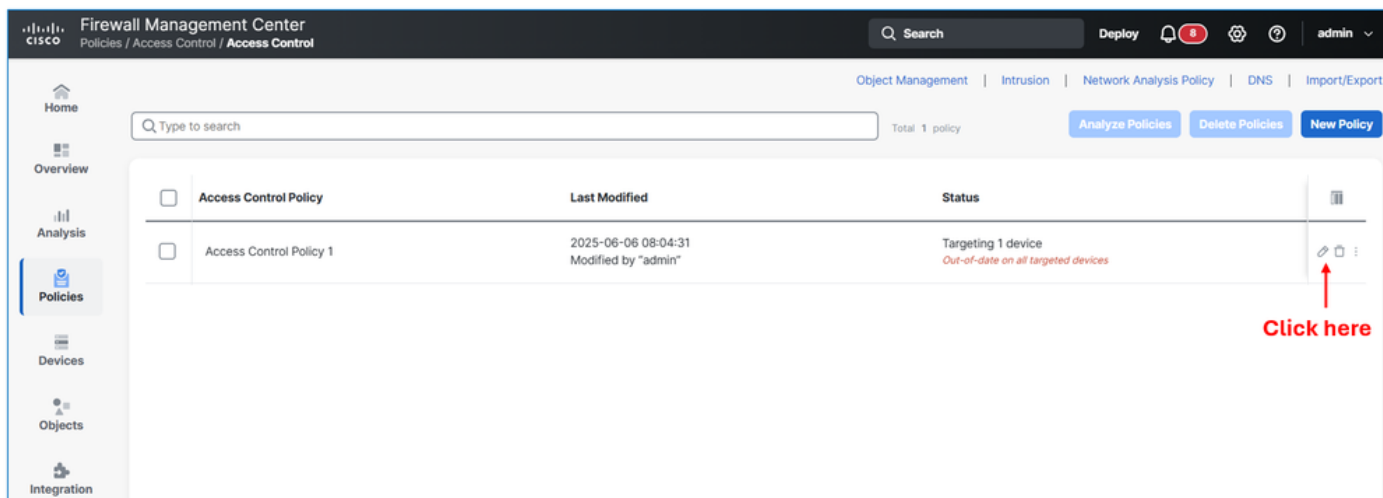
アクセスコントロールポリシーの設定

アイデンティティポリシーをアクセスコントロールポリシーにリンクさせ、次の属性を持つアクセスポリシールールを作成します。

属性名	値
ルール名	ルール1
アクション	プライベート ネットワーク間で
ソースゾーン	INSIDE
宛先ゾーン	OUTSIDE
送信元ネットワーク	10.10.10.0/24
宛先ネットワーク	10.48.62.98/32
サービス	宛先ポートTCP 80(HTTP)
ユーザ	ラボ領域/グループ1
Logging	接続の最後

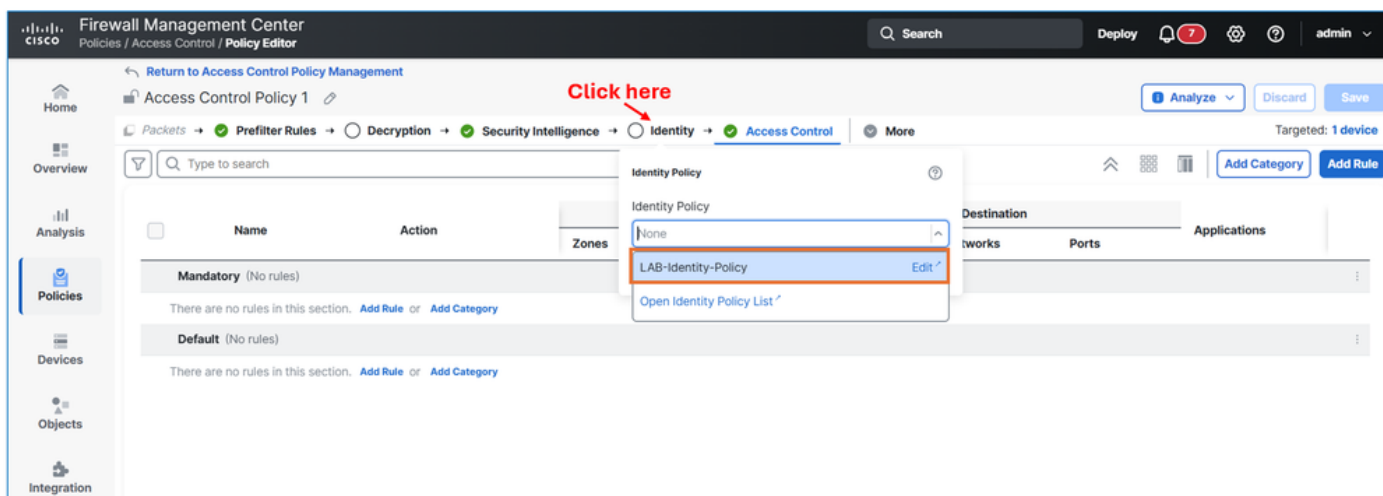
ステップ 1：アイデンティティポリシーをアクセスコントロールポリシーにリンクする

FMCのUIで、Policies > Access Control > Access Controlの順に移動します。ポリシーのEditbuttonをクリックします。



ポリシーの編集

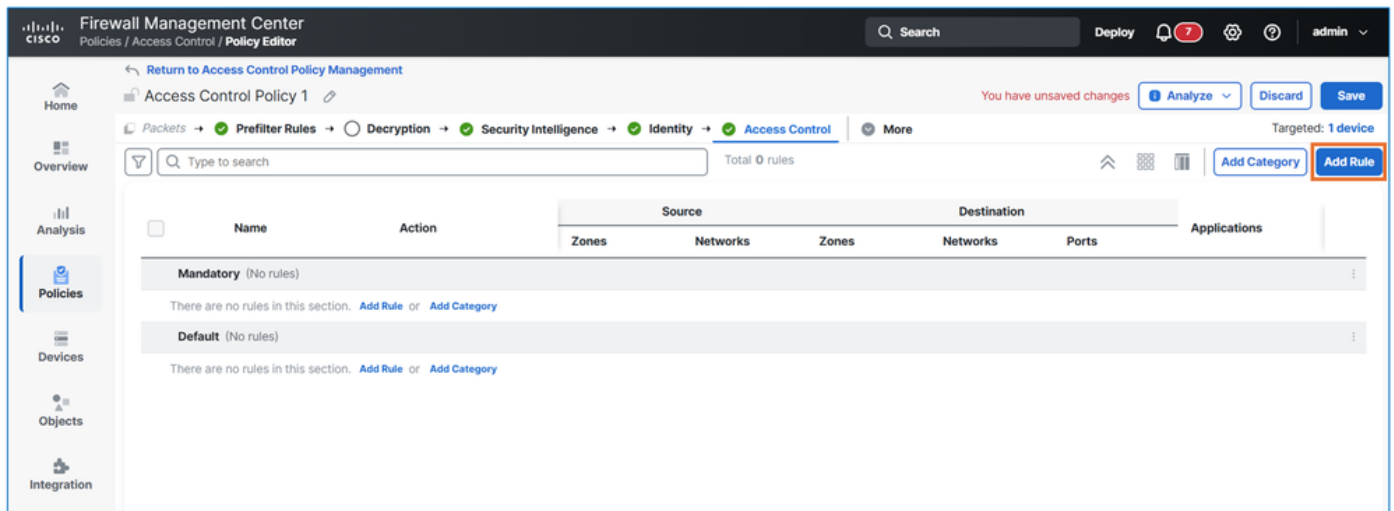
identitysectionに移動し、前のタスクで作成したID Policyをリンクします。



アイデンティティポリシーの追加

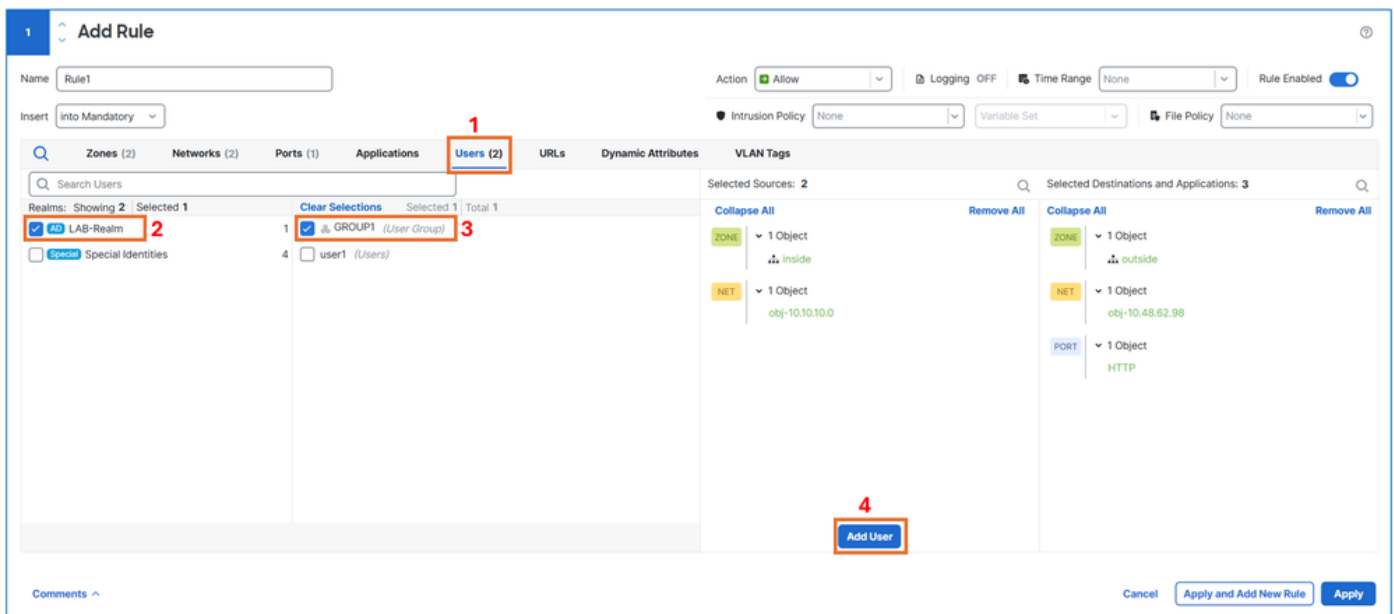
Applybuttonをクリックします。

ステップ 2アクセスコントロールルールを作成します。



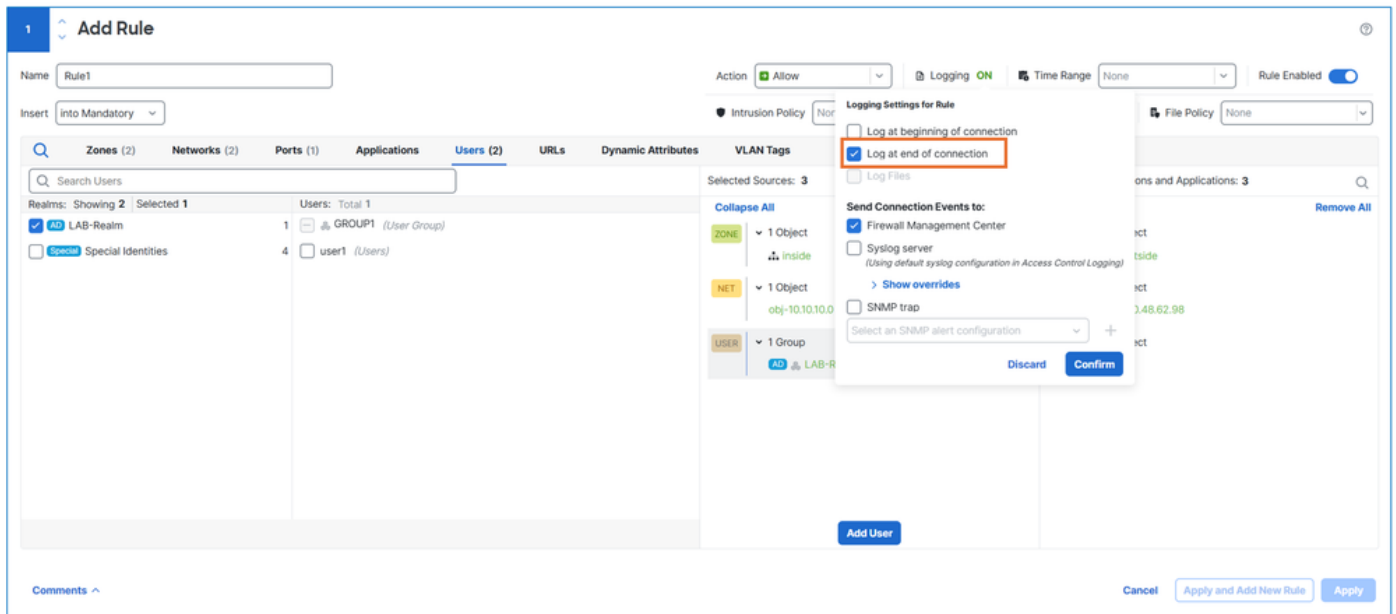
acpの作成

タスク要件に従って詳細を入力します。最も重要なことは、Userstabの下でaddGROUP1 fromLAB-Realmを入力することです。



ルールにユーザーを追加する

接続の最後でselectingLogを使用して、ルールのロギングを有効にします。



enable logging

ステップ 3デフォルトアクションのロギングを有効にします。

デフォルトのActionlogging設定を変更するには、設定アイコンをクリックします。

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

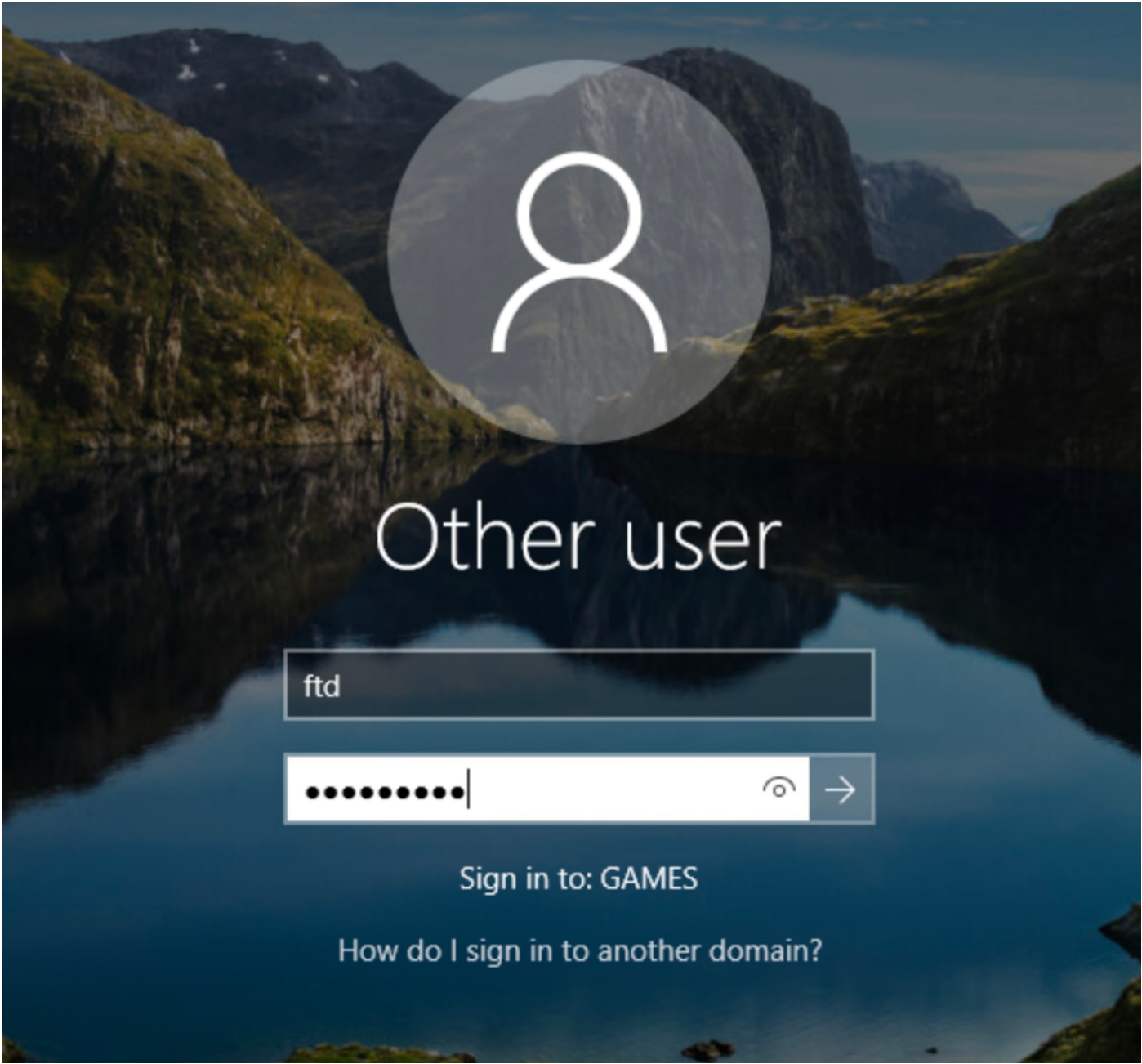
ロギングを有効にします。

FTDに設定を保存して展開します。

検証

トラフィックがftdに対してのみ許可されていることを確認して、パッシブIDの動作を確認します。

ユーザマシンからドメインユーザにログインします。



ユーザログイン

ユーザが正常にログインしたら、FMCのAnalysis > user > active sessionで、アクティブユーザの詳細を確認します。

▼ 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	

アクティブセッション

接続イベントからトラフィックの検証を開始した後、接続イベントのユーザの詳細を確認します。

Connection Events (switch workflow)

No Search Constraints (Edit Search)

Connections with Application Details

Table View of Connection Events

II 2026-06-19 04:20:10 - 2026-06-19 05:20:22

Expanding

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		

アクティブセッション

トラブルシューティング

エージェントログの確認

エージェントをホストしているWindowsマシンでTask Managerを開き、バックグラウンド processCiscoPassiveIdentityAgentServiceisが実行されていることを確認します。

Task Manager

File Options View

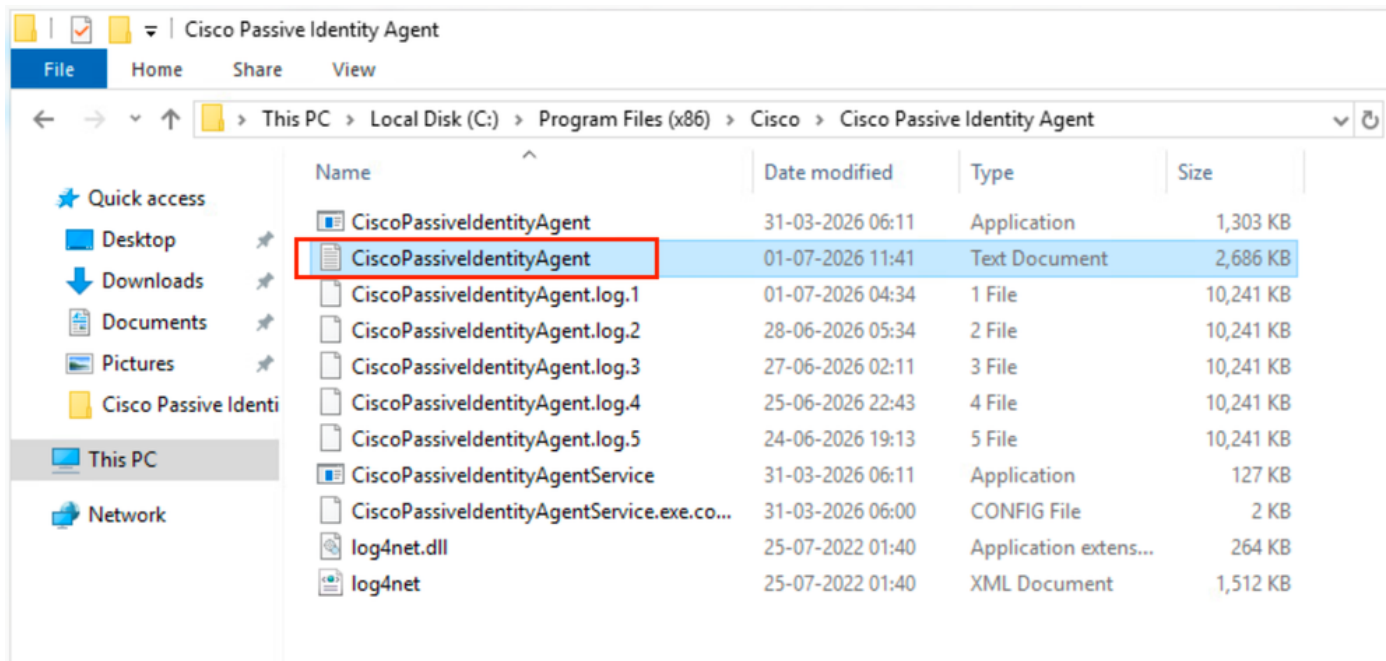
Processes Performance Users Details Services

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

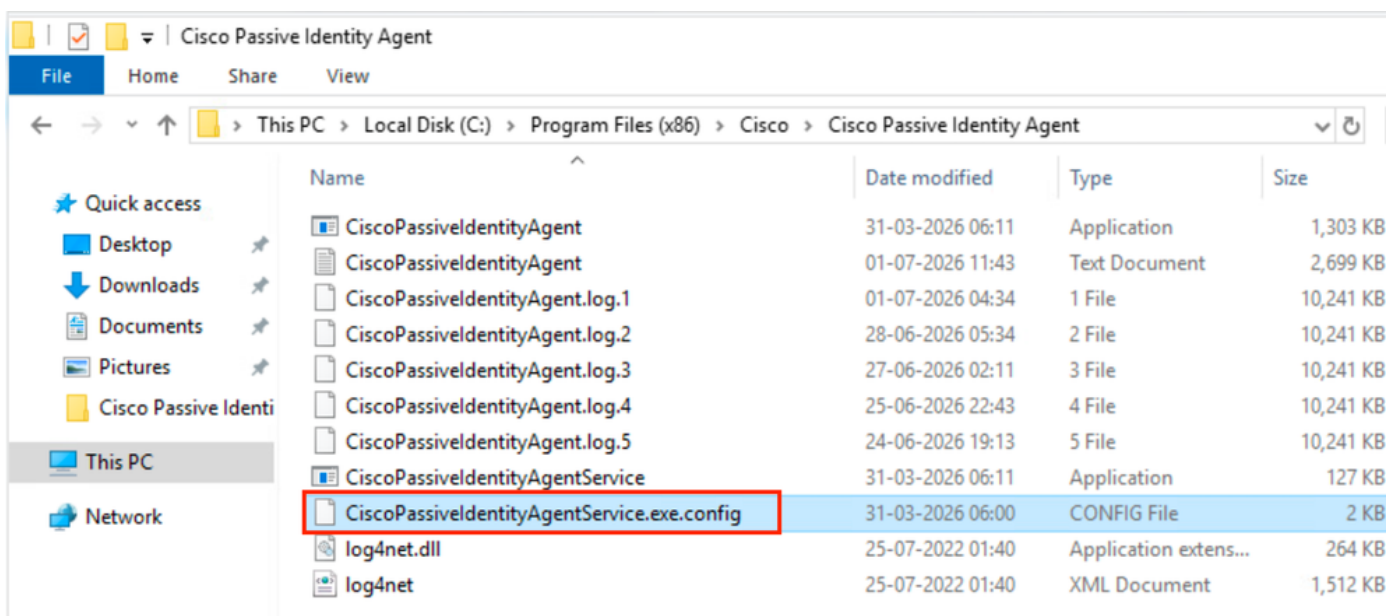
実行中のタスク

エージェントログは、CiscoPassiveIdentityAgentファイルに含まれています。デフォルトの場所は、「C:\Program Files (x86)\Cisco\Cisco Passive Identity Agent\」です。



エージェント

デフォルトでは、エージェントログはINFOlevelに設定されます。DEBUGレベルのロギングを有効にするには、CiscoPassiveIdentityAgentService.exe.exeコンフィギュレーションファイルを変更し、ログレベルをALLorDEBUGに設定します。



エージェント設定



```
<?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>
```

情報ログ

エージェントログのチェック：エージェント設定のフェッチ。

INFO Restクライアント、バルクイベント：[{"domain":"games.cisco.com", "srcIpAddress":
"X.X.X.X", "user": "fdm", "timestamp": "2026-07-01T19

情報：Restクライアント、マッピングステータス：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クライアント、エージェント構成の要求

FMCログ

このコマンドを実行して、エージェントからユーザとIPのマッピングを受信したかどうかを確認
します。

```
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出力

上記のコマンドでマッピングが表示されない場合は、これらのログを収集して、Cisco TACに連絡してください。

FMC APIに関連するログの一覧を以下に示します。ピッグテールログは、それらすべてを包含する。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。