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

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

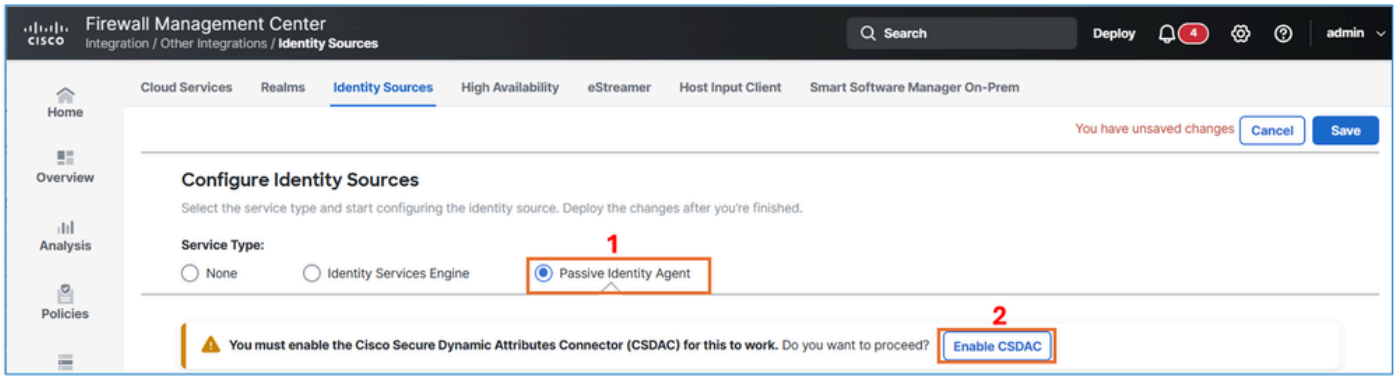
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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。

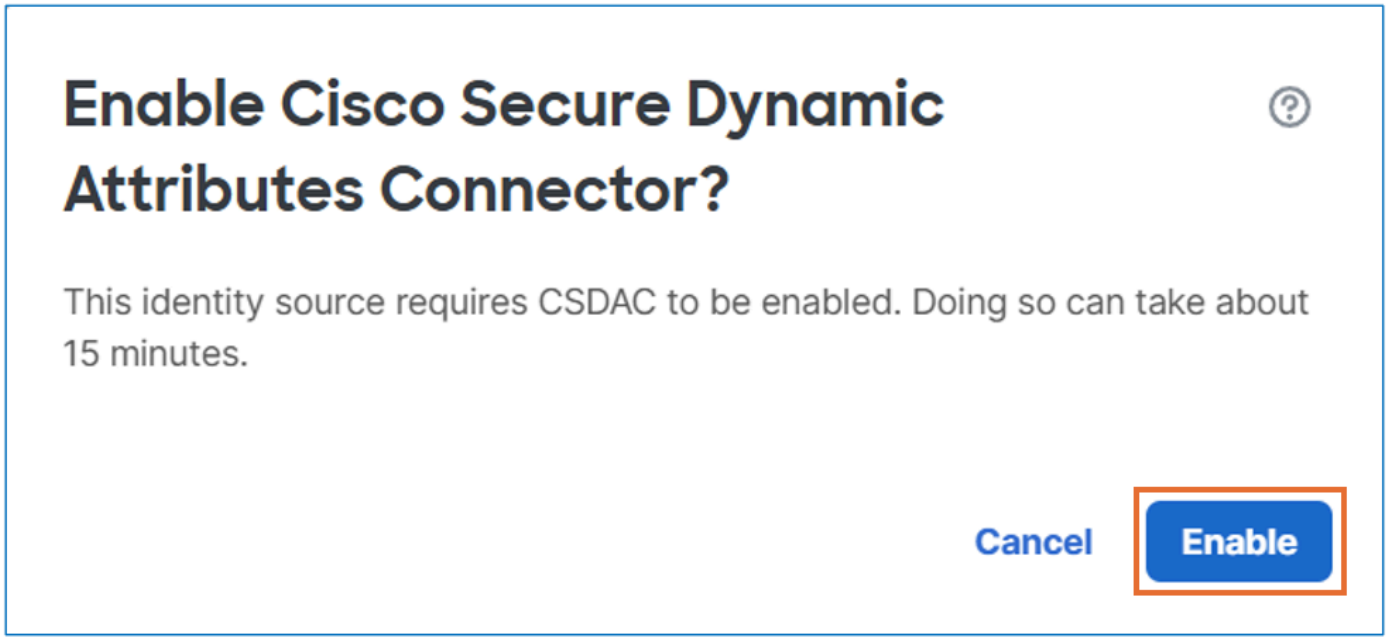
パッシブIDエージェントソースの設定

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。



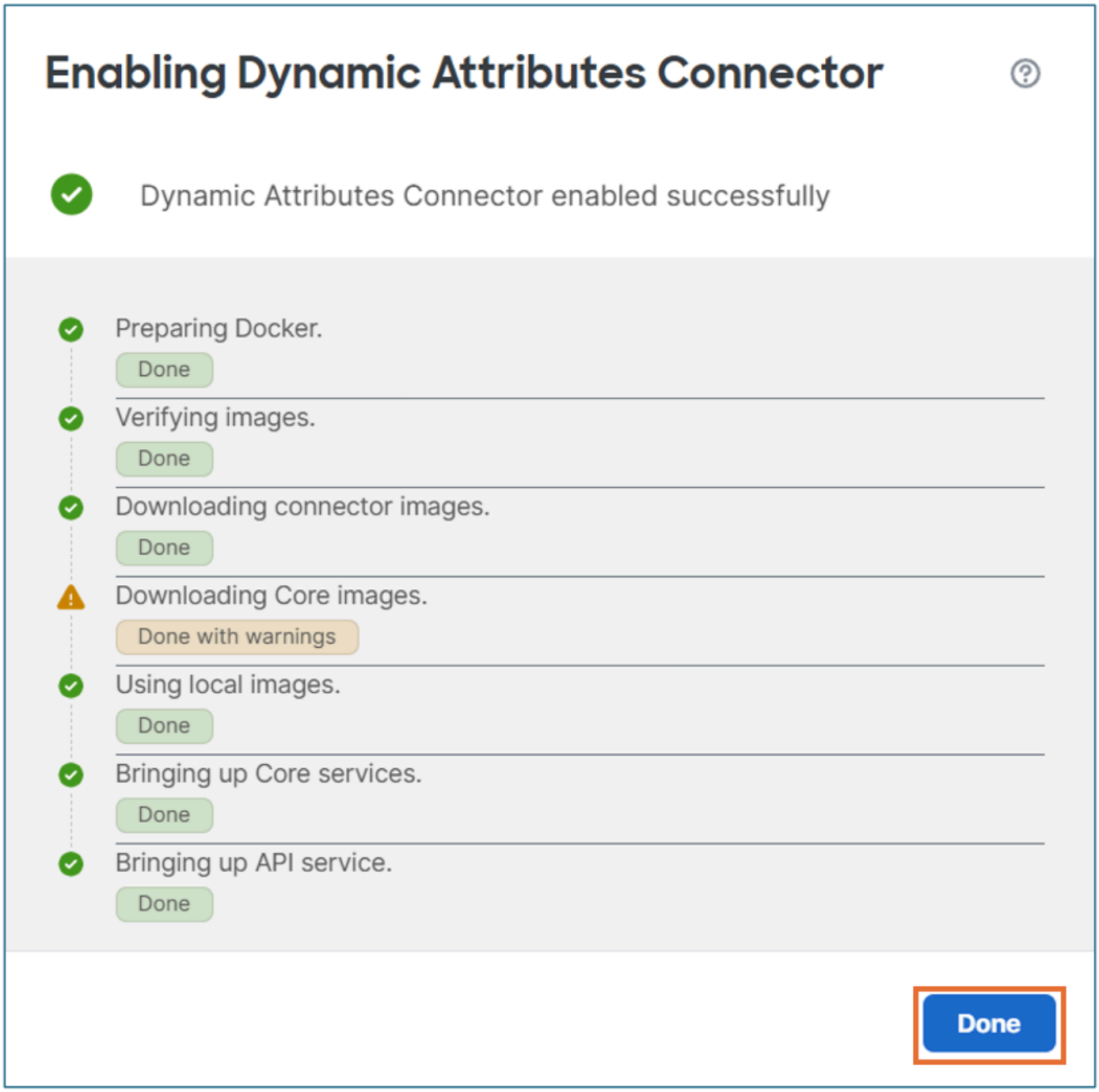
パッシブIDエージェント

CSDACを有効にするには、[有効]ボタンをクリックします。



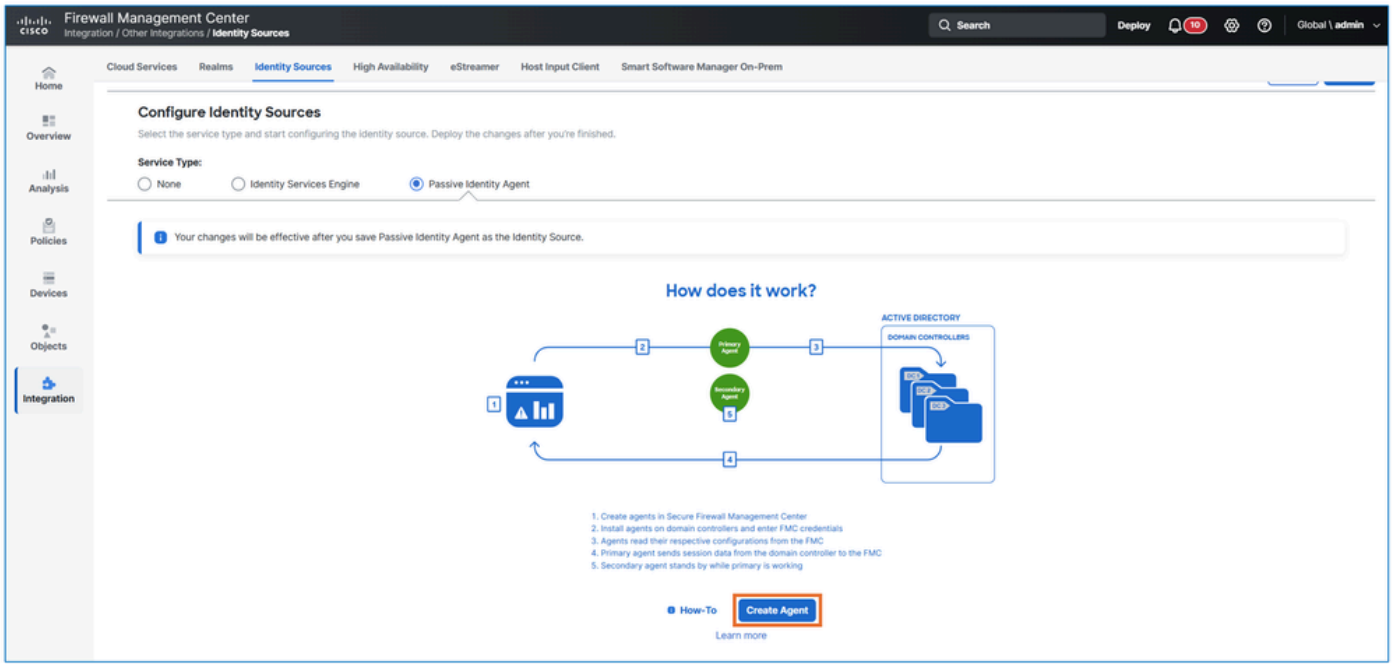
CSDACを有効にする

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。



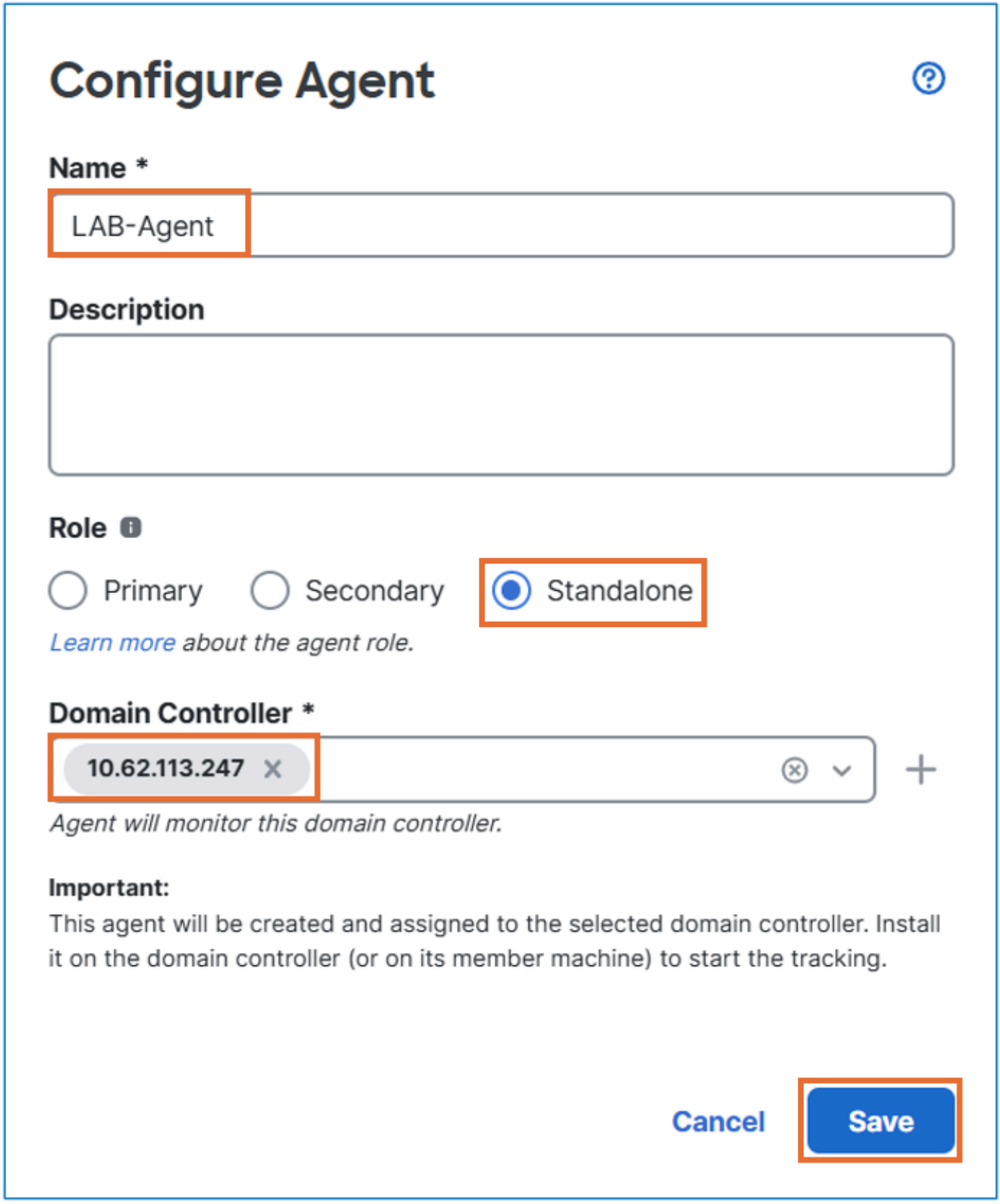
CSDAC有効

Create Agentbuttonをクリックします。



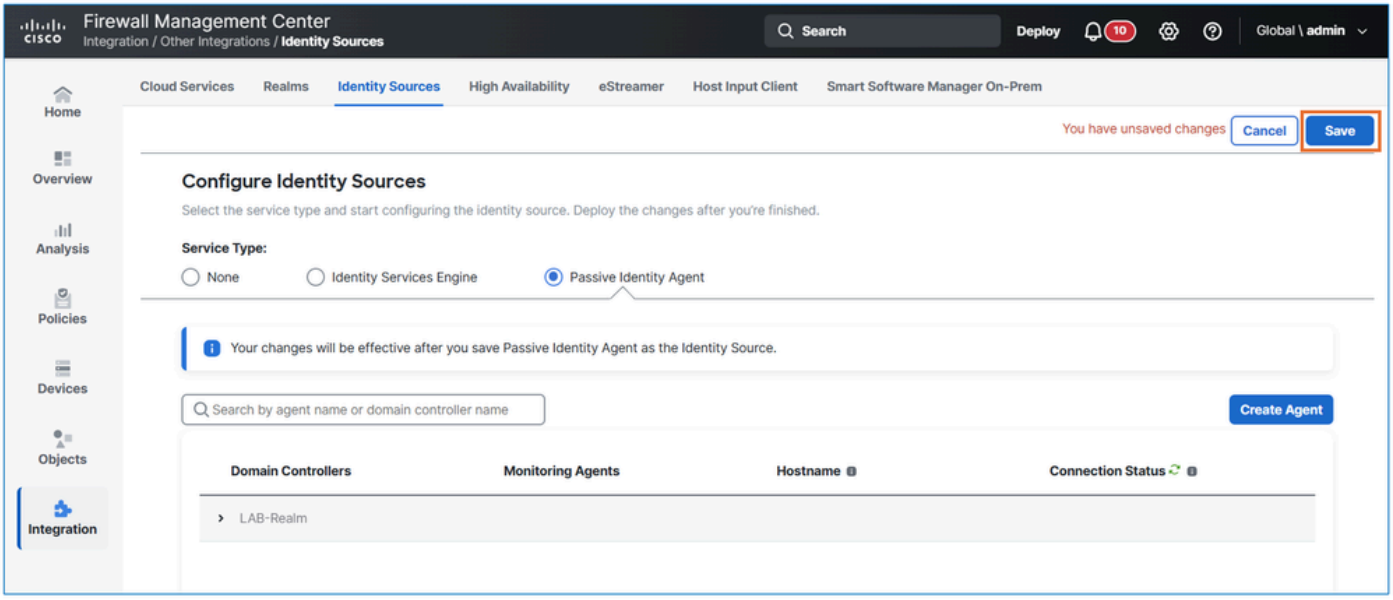
エージェントの作成

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。



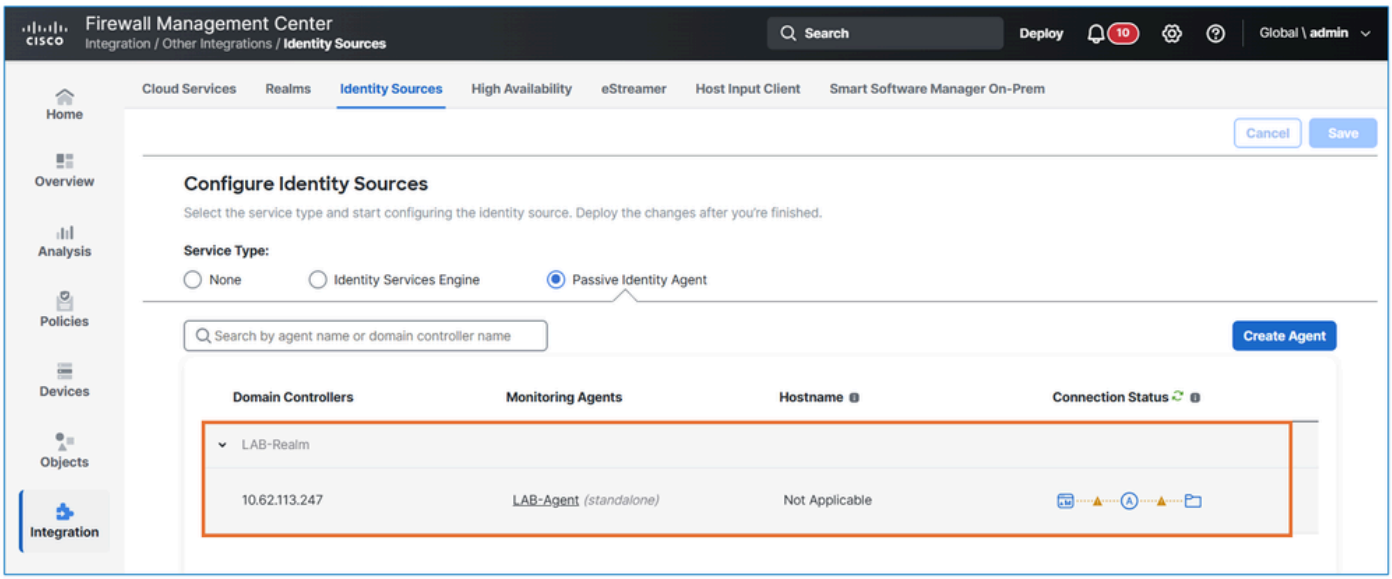
エージェントの設定

「保存」ボタンをクリックします。



設定の保存

結果です。



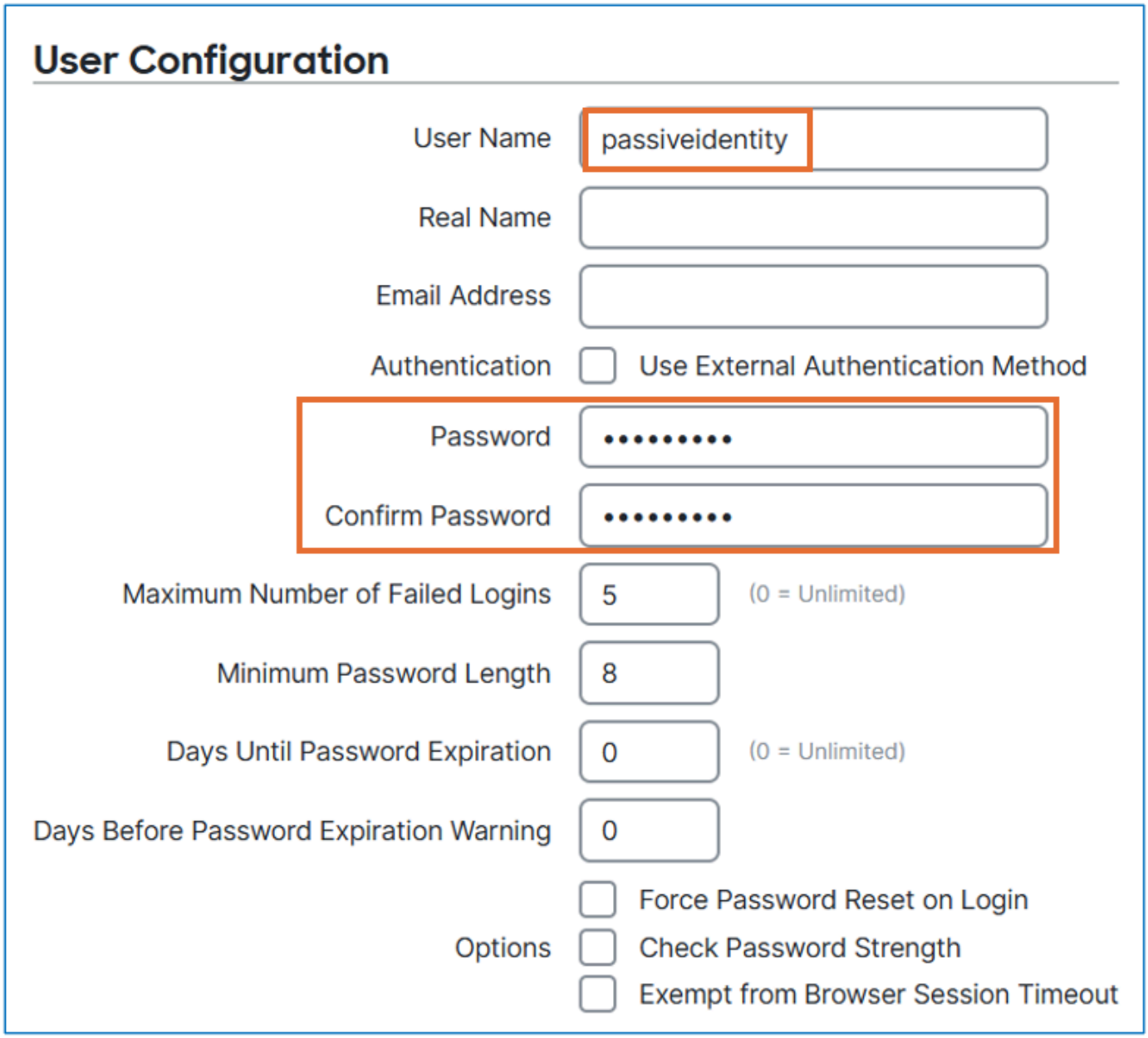
ステータスの確認

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

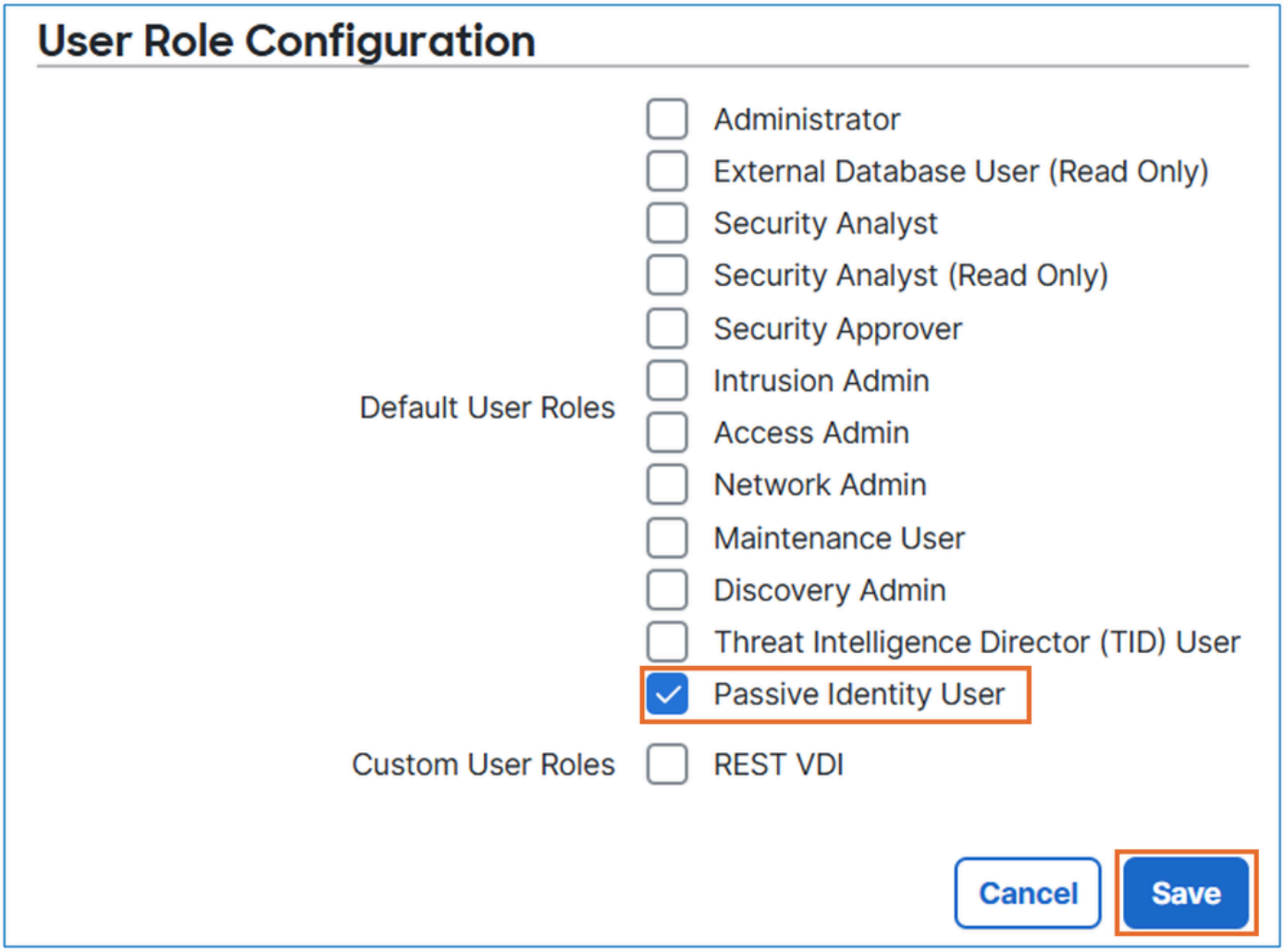
パッシブIDエージェントと通信するために十分な権限を持つセキュアファイアウォール管理センター(FMC)ユーザを作成します。 このユーザには、他のタスクを実行する権限が制限されています。ユーザは、パッシブIDエージェントとの通信のみを有効にすることが想定されています。

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。



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。

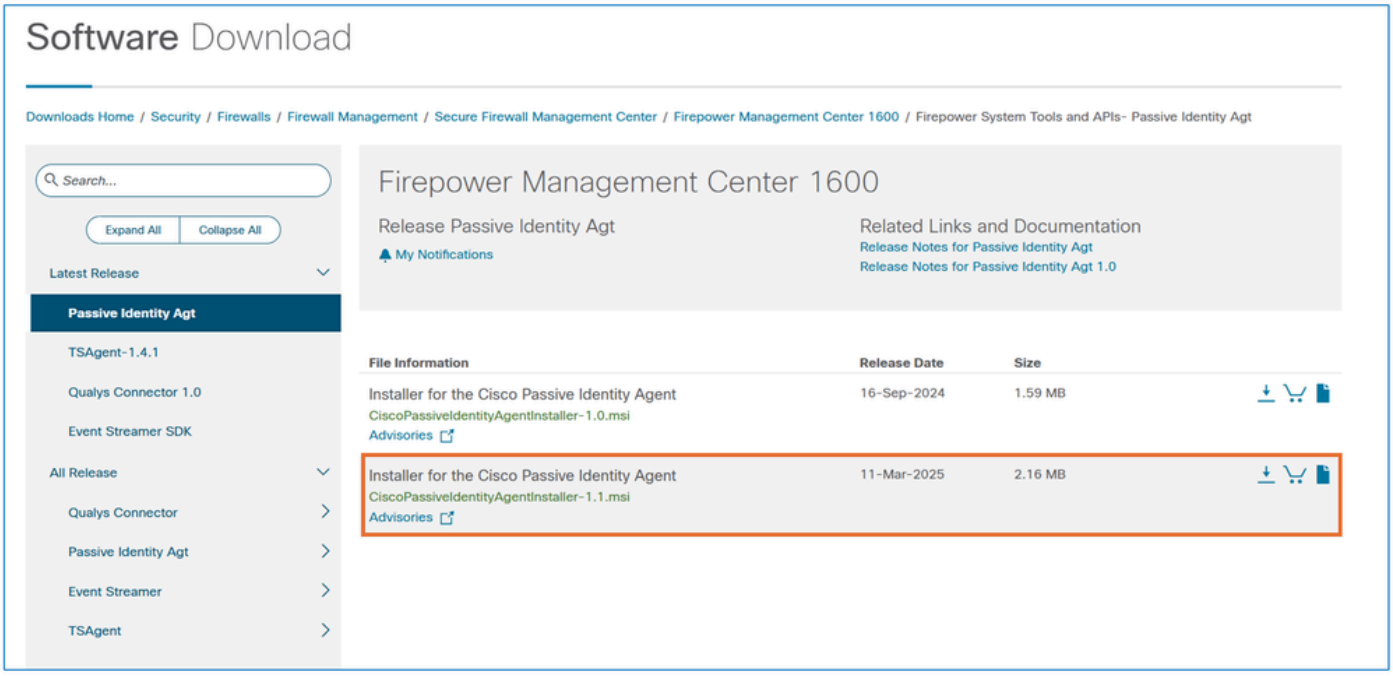


パッシブidユーザの選択

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

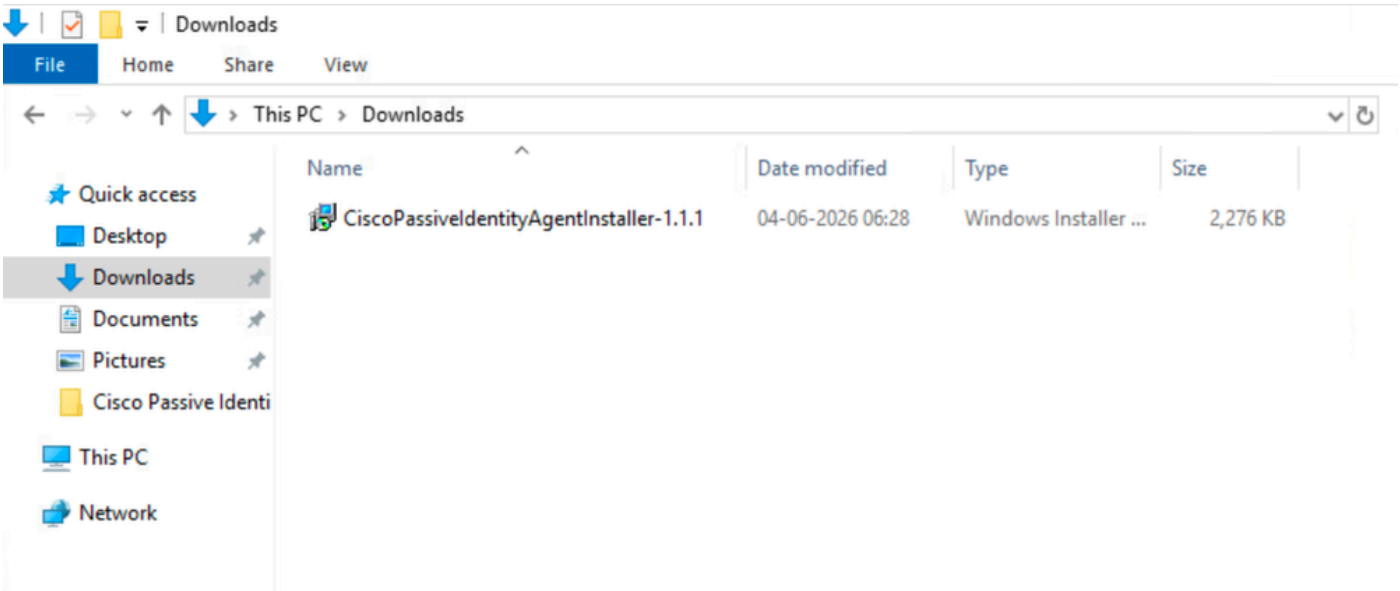
指定されたドメインコントローラにPassive Identity Agentソフトウェアをインストールして設定します。

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



ソフトウェアのダウンロード

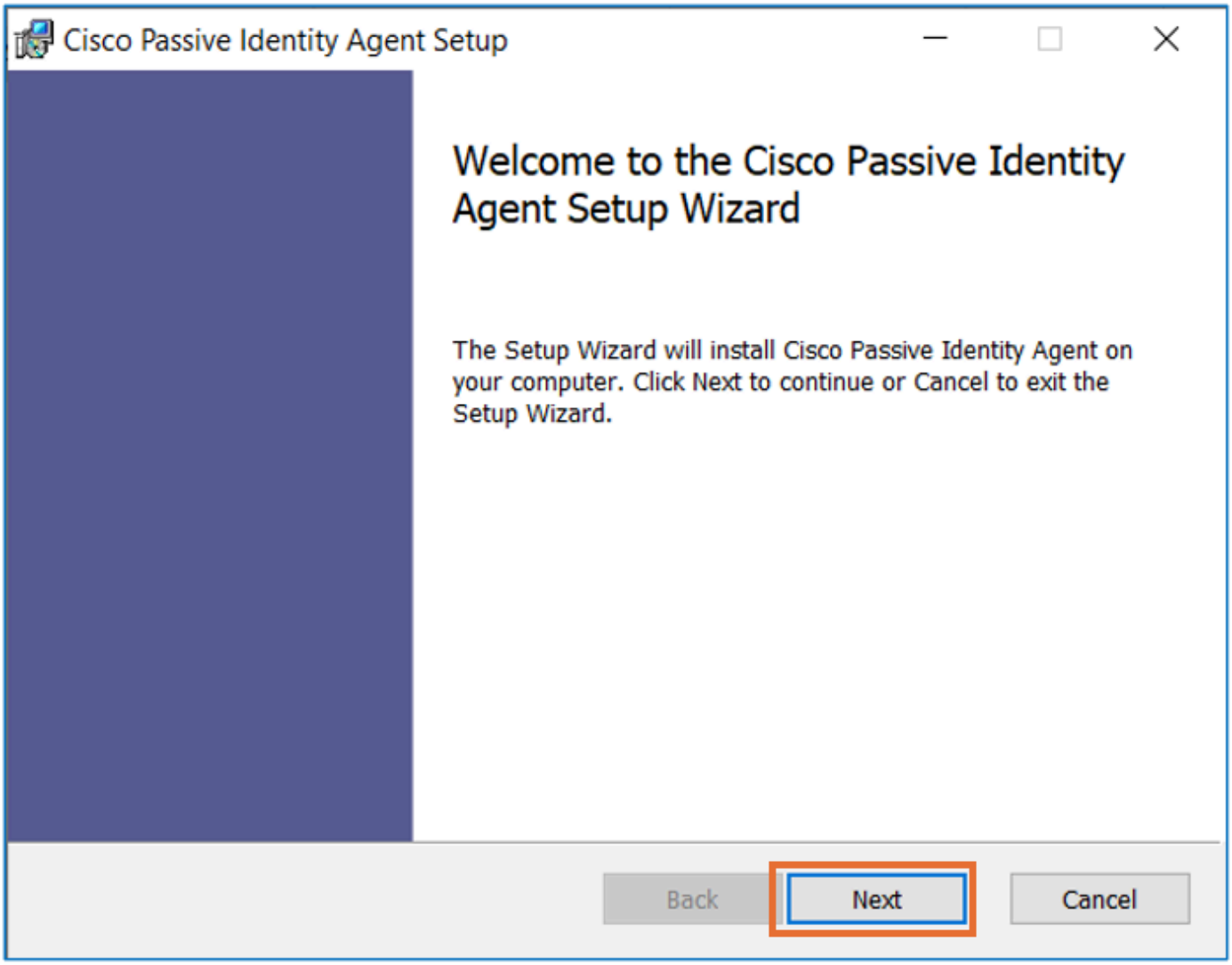
エージェントをダウンロードしたら、ドメインコントローラでインストールプロセスを開始します。



エージェント

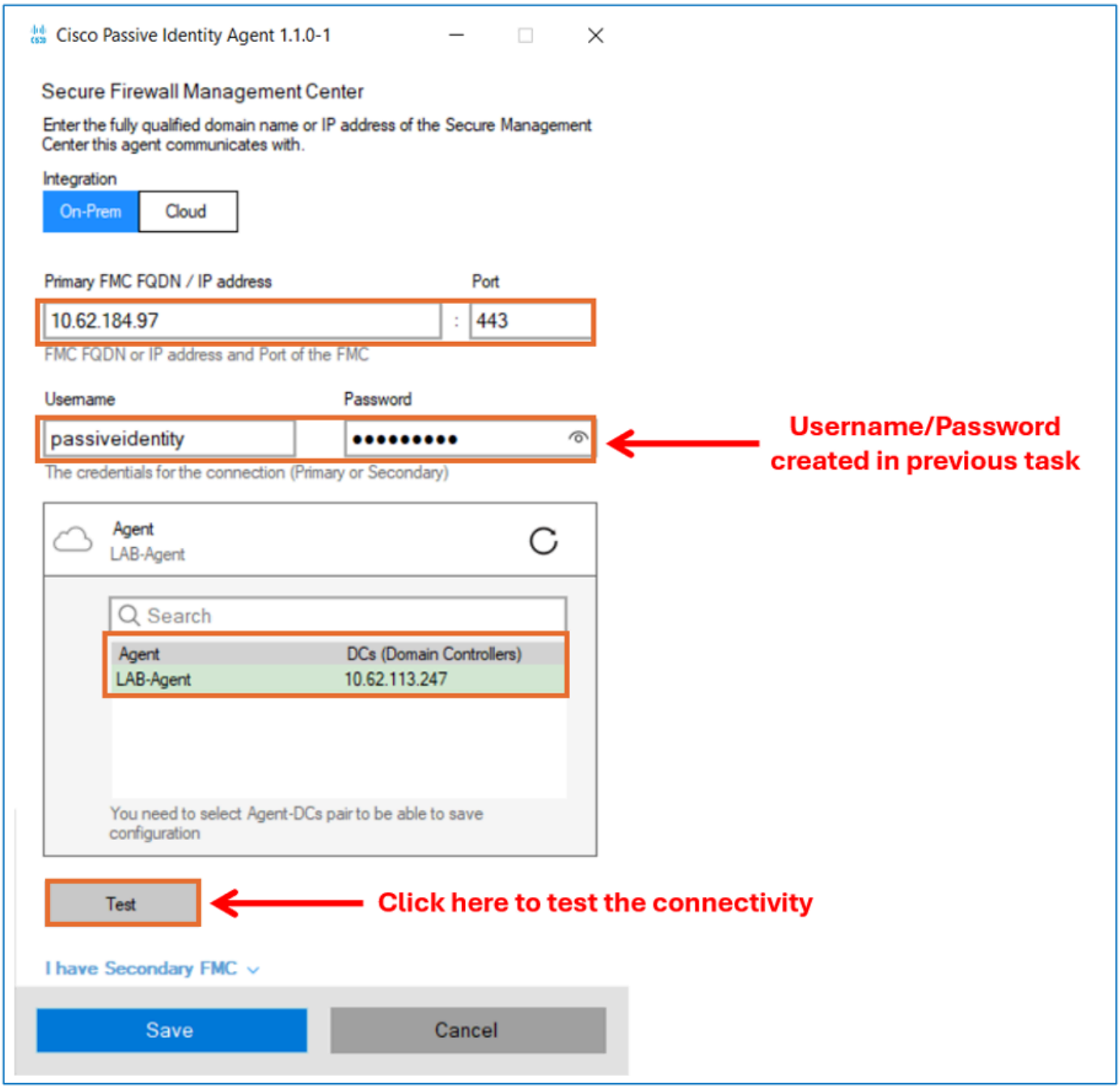
]

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。



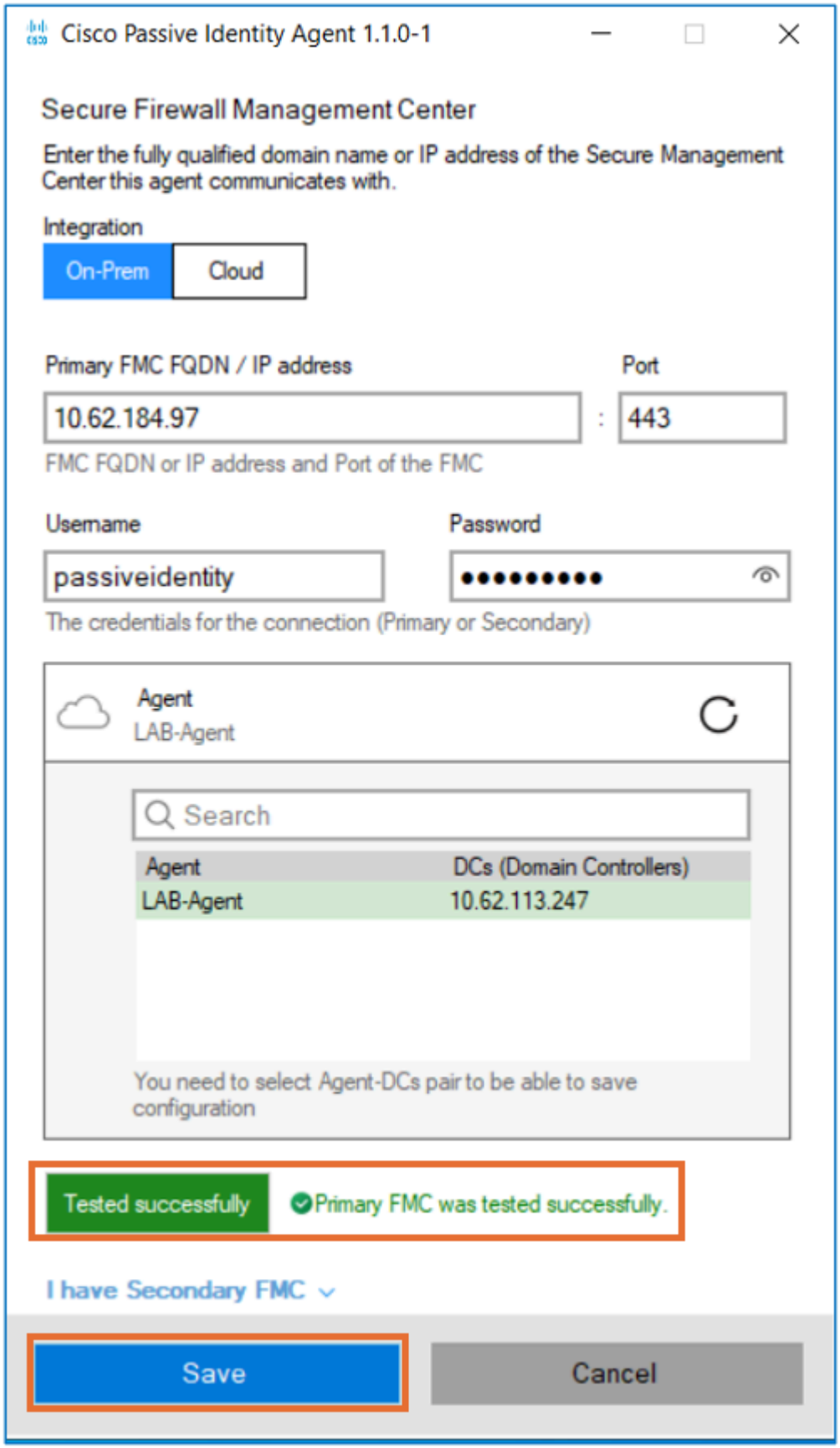
インストールするもの

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。



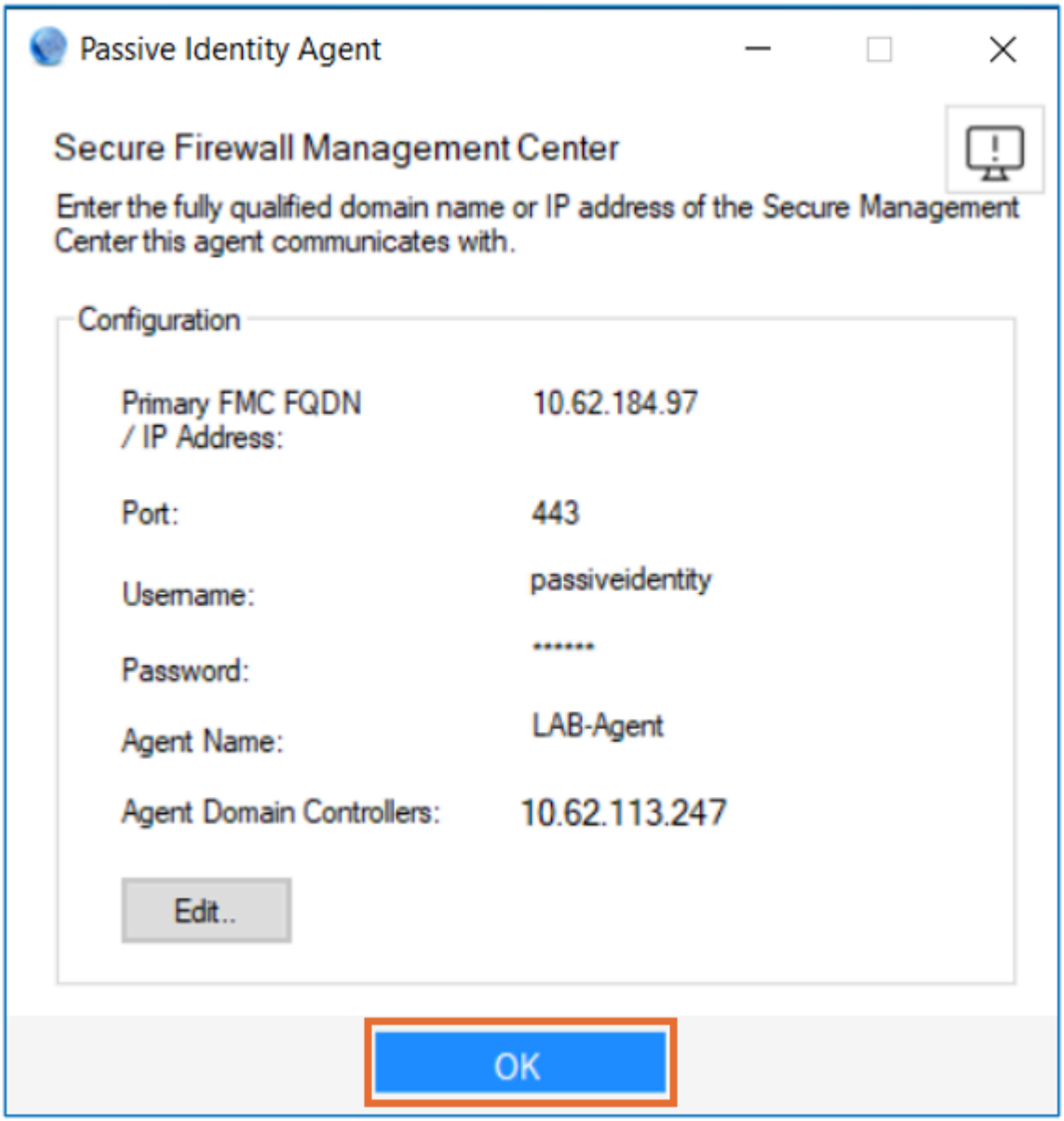
エージェントを設定します。

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。



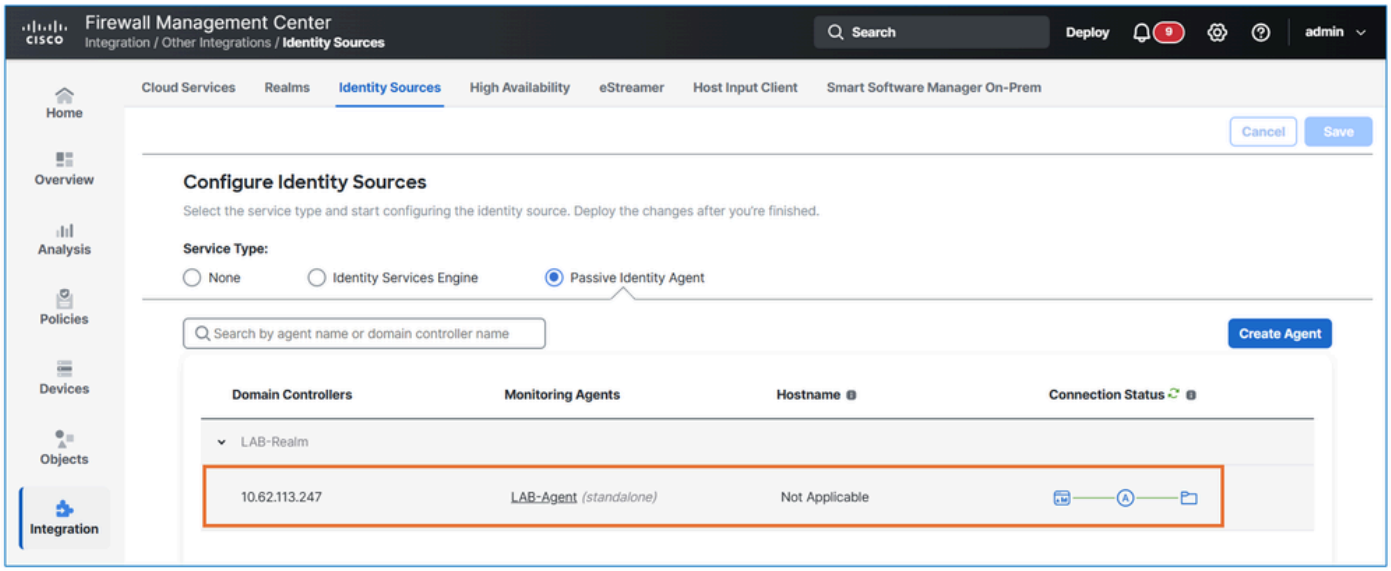
テスト

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。



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。



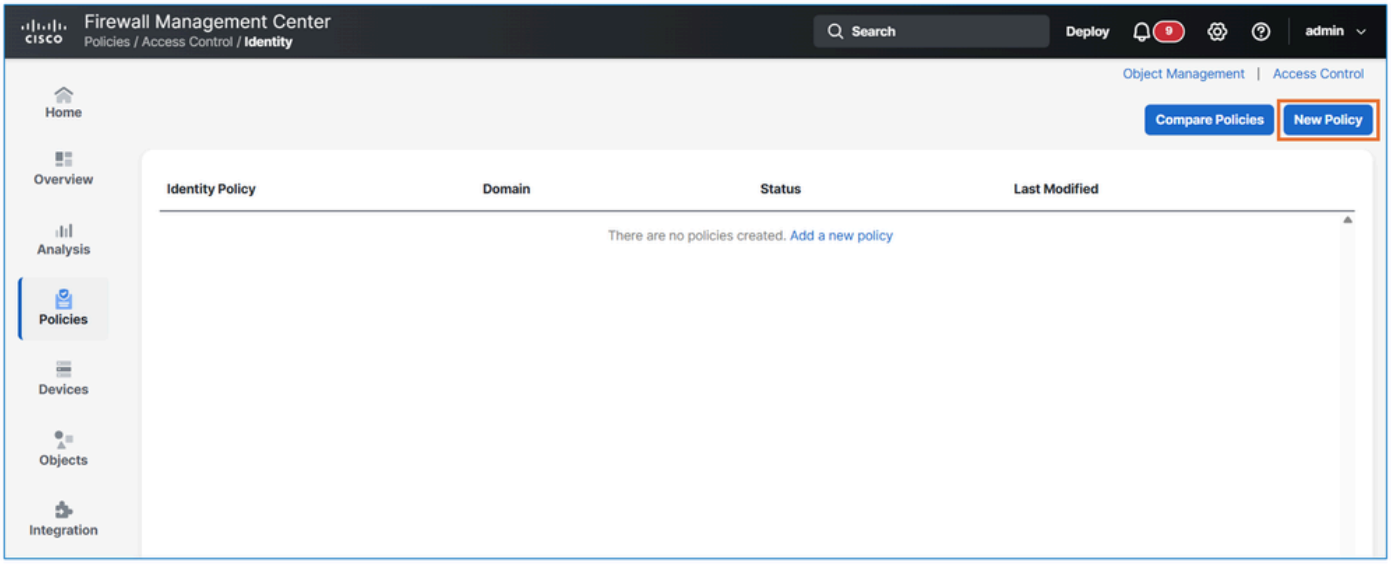
fmcからの通信の確認

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。

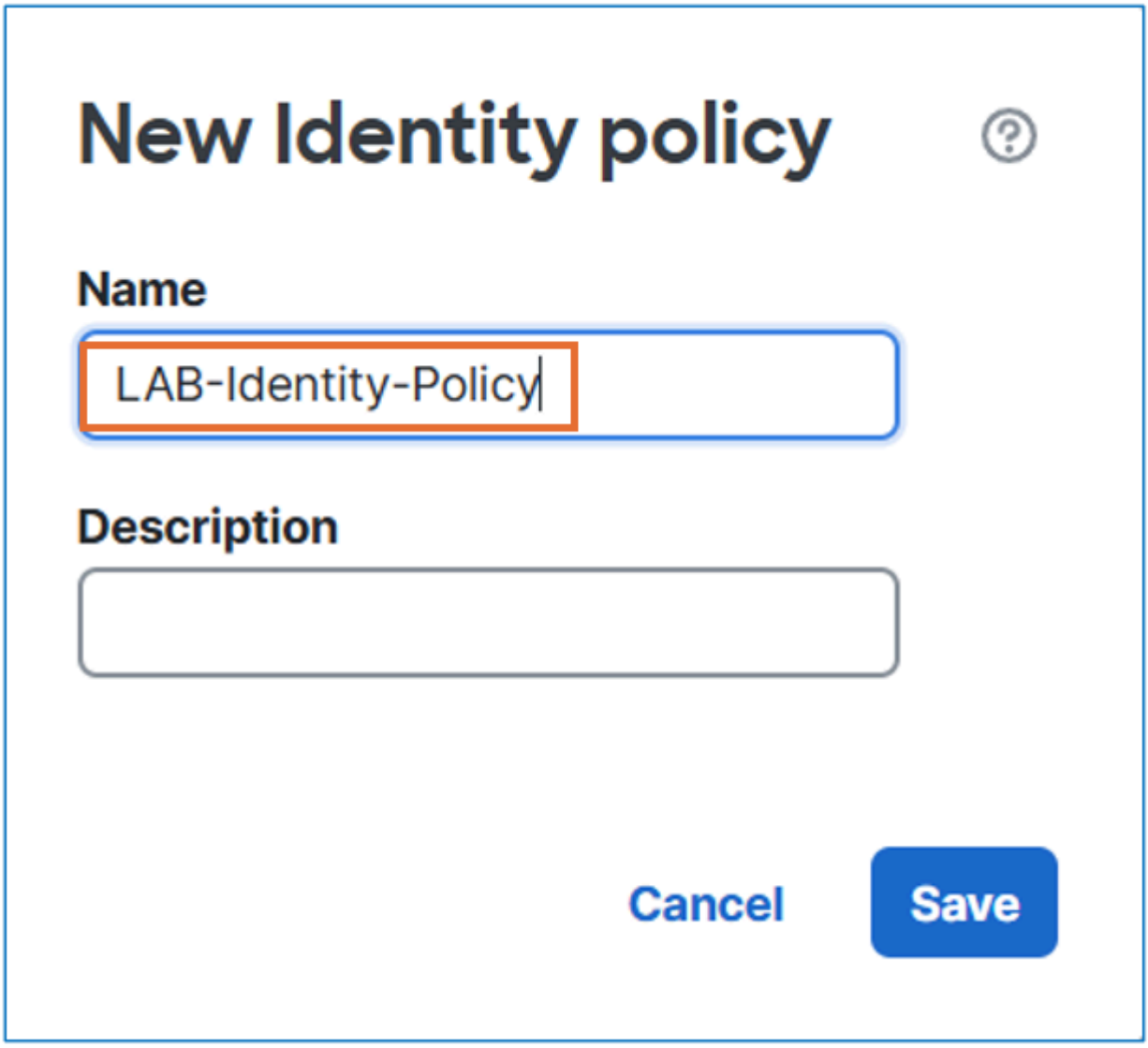
ポリシー名	ルール名	認証レルム	残りの設定
ラボIDポリシー	ルール1	ラボ領域	デフォルトのままにする

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。



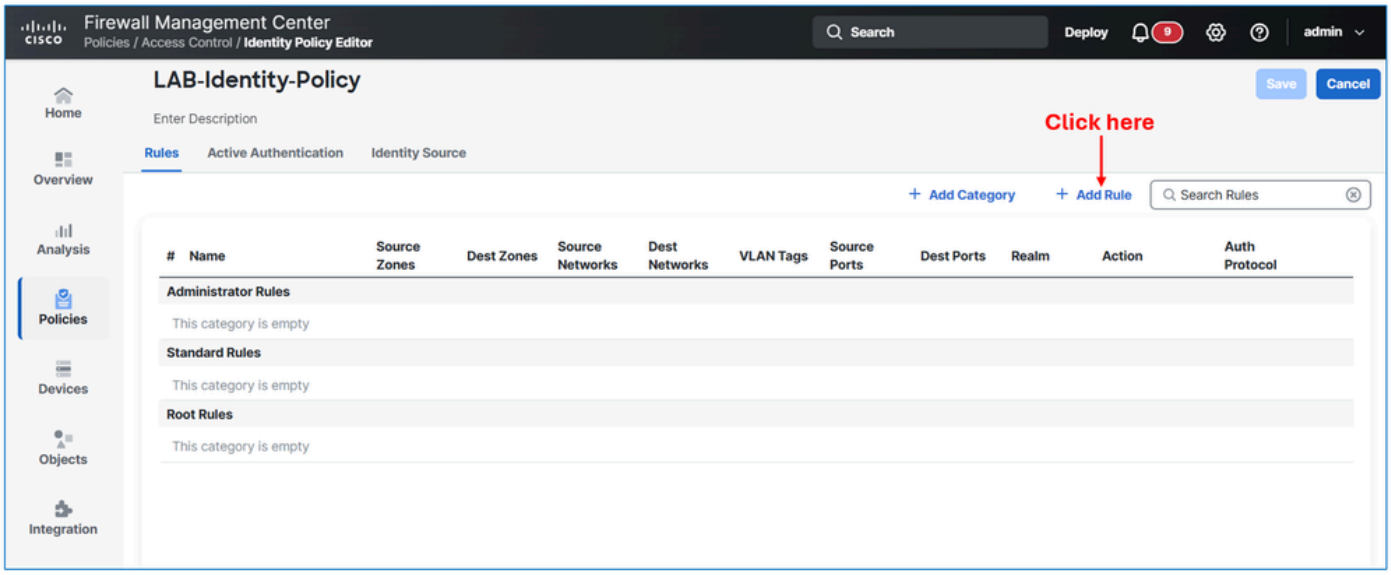
新しいポリシー

タスクの要件に従ってポリシー名を入力します。



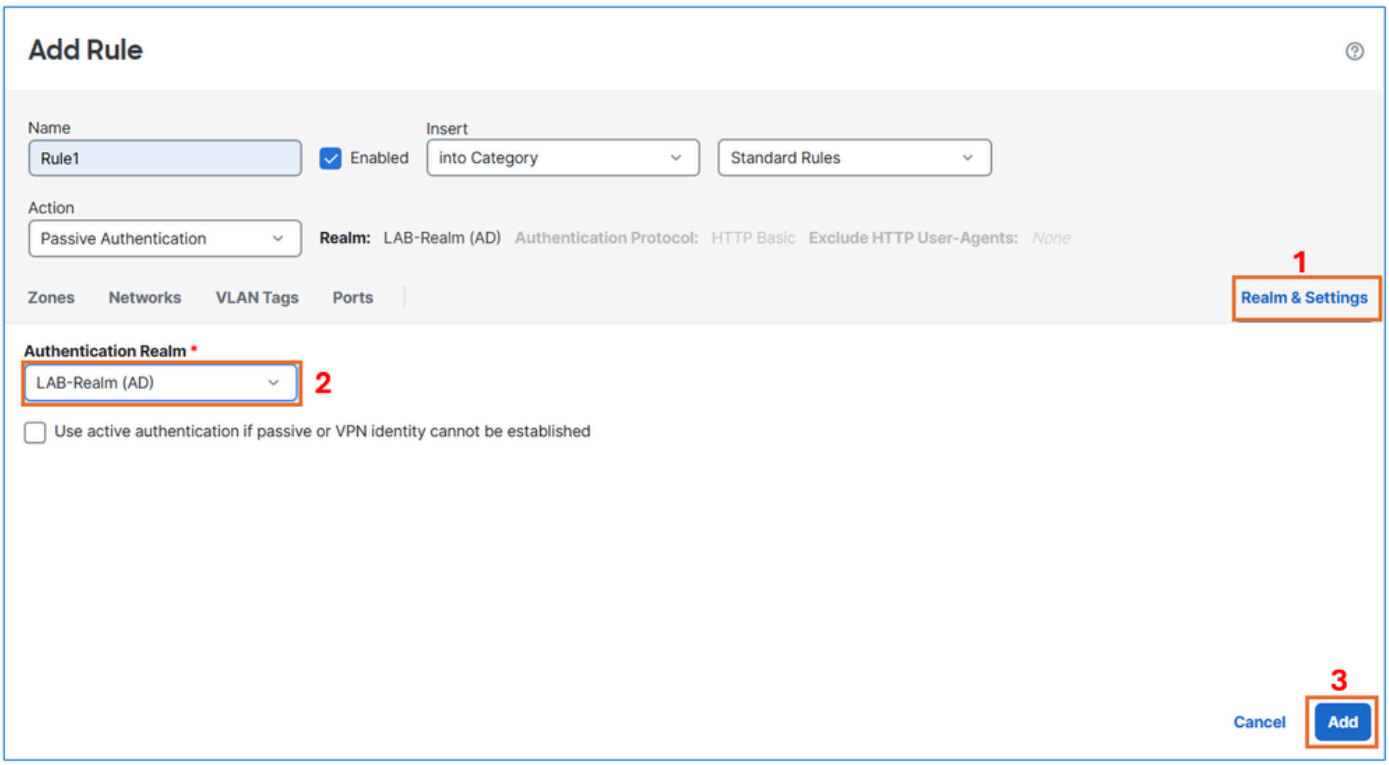
新しいポリシー

Add Rulebuttonをクリックします。



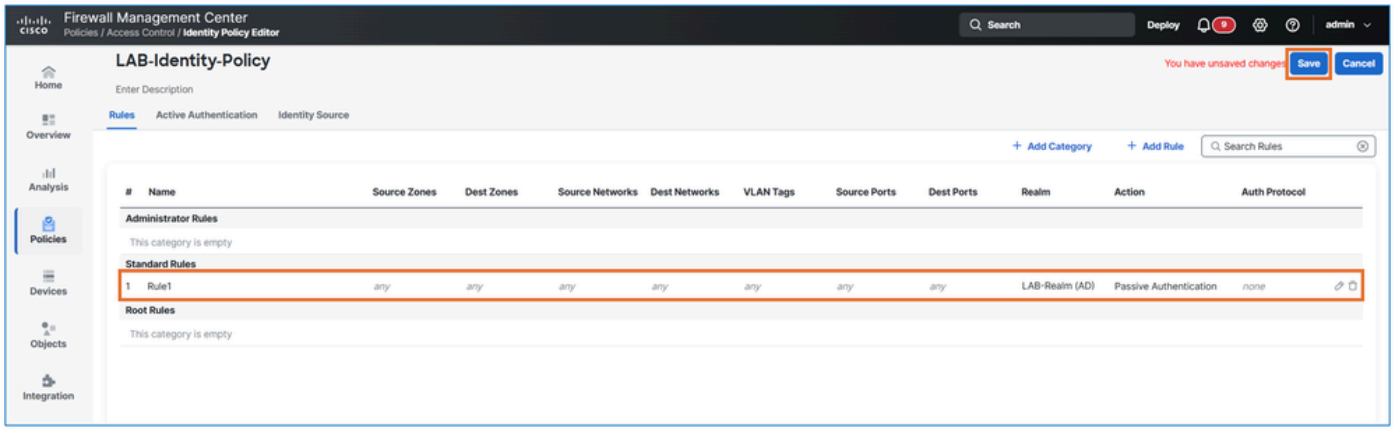
ルールの作成

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。



レルムの設定

「保存」ボタンをクリックします。



設定を保存します

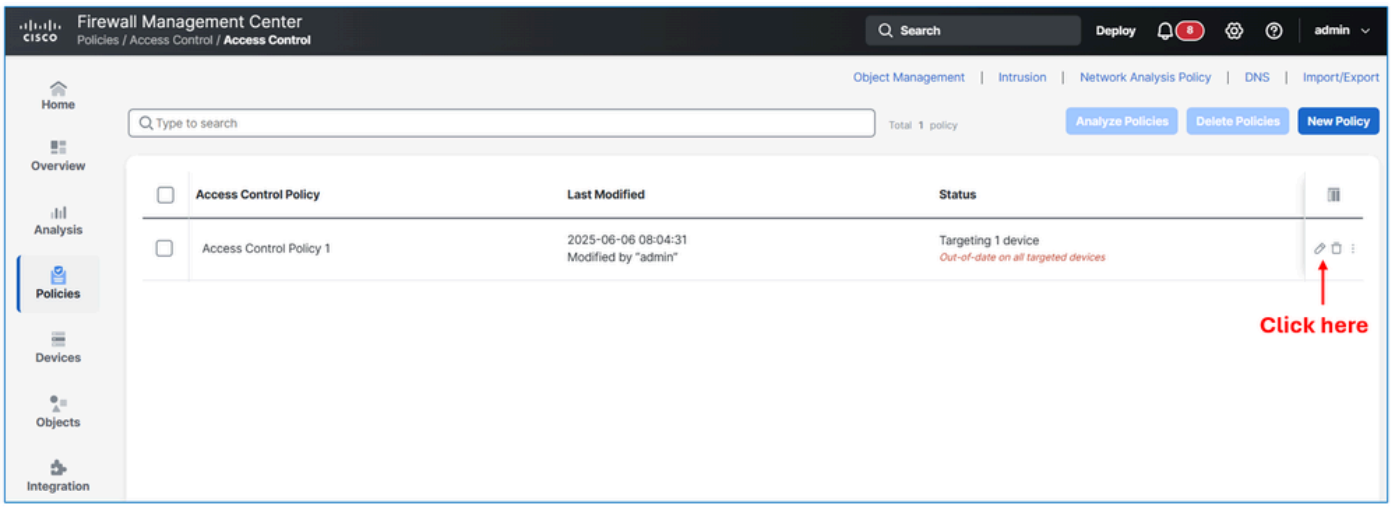
アクセスコントロールポリシーの設定

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

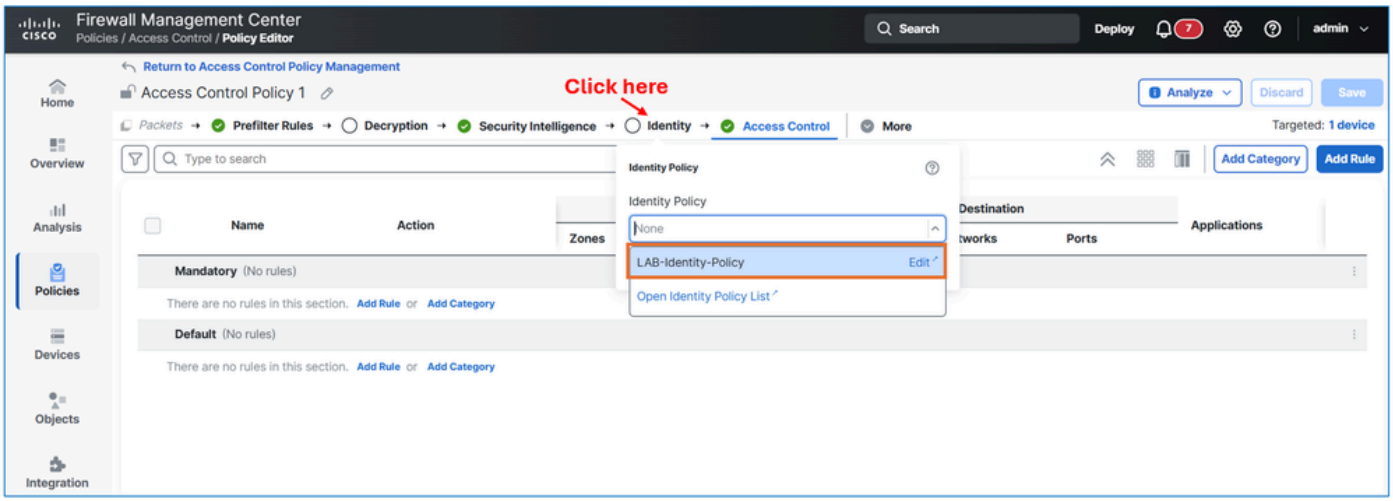
ステップ 1：アイデンティティポリシーをアクセスコントロールポリシーにリンクする

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

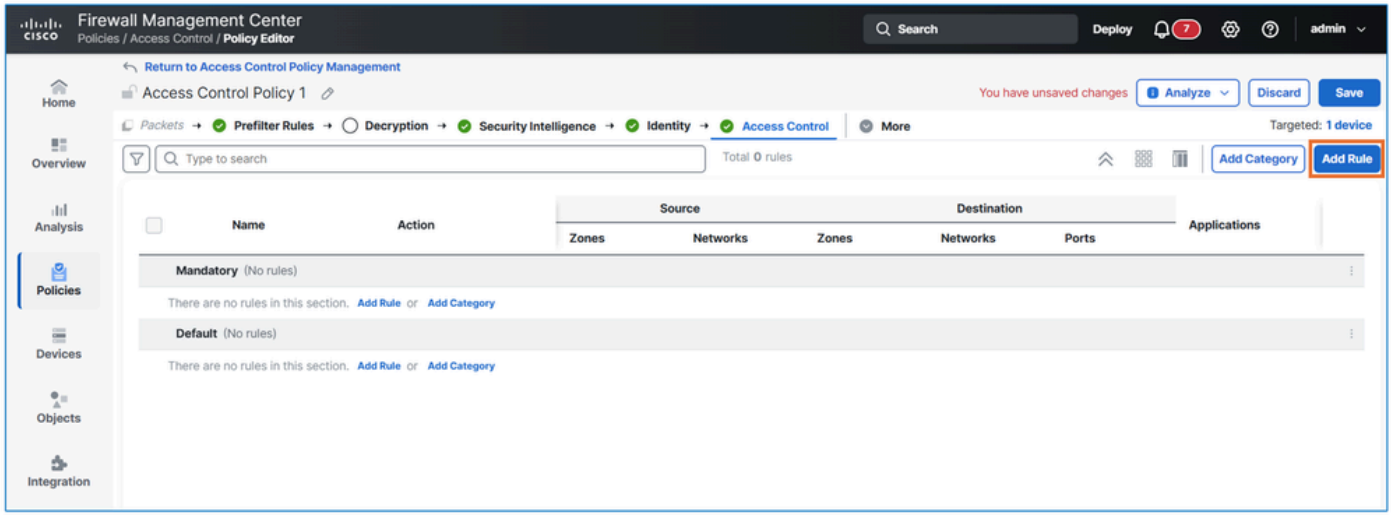
identitysectionに移動し、前のタスクで作成したID Policyをリンクします。



アイデンティティポリシーの追加

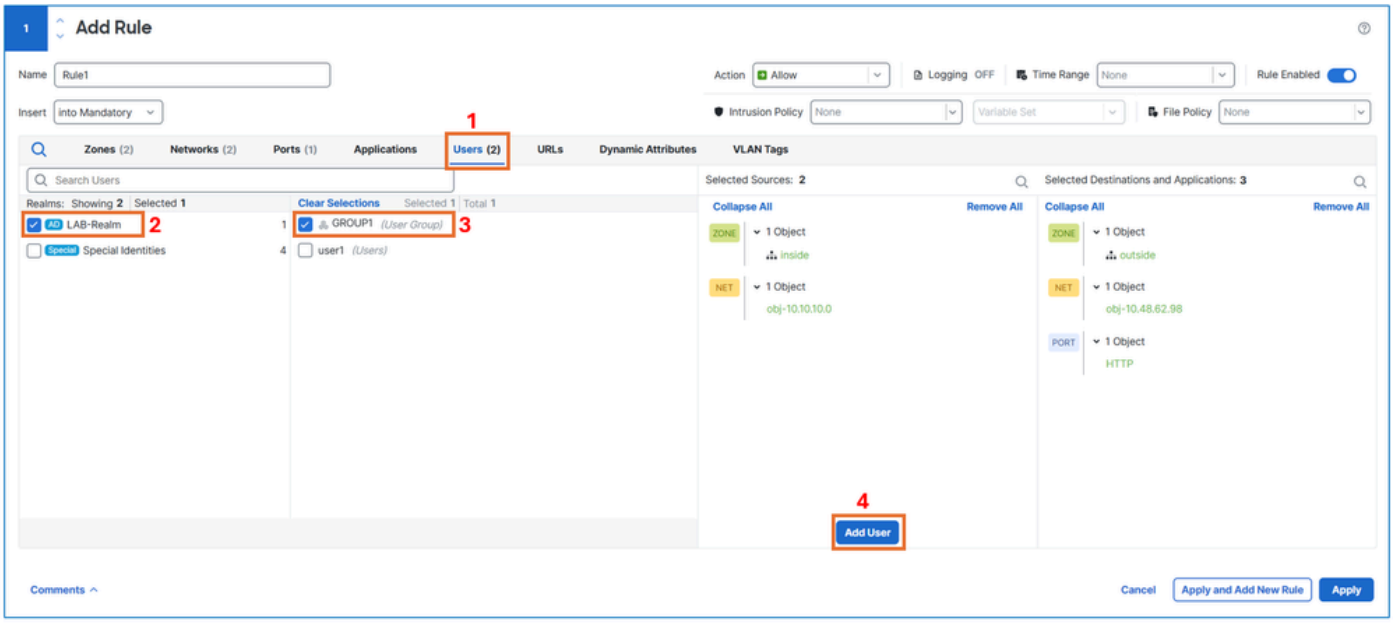
Applybuttonをクリックします。

ステップ 2アクセスコントロールルールを作成します。



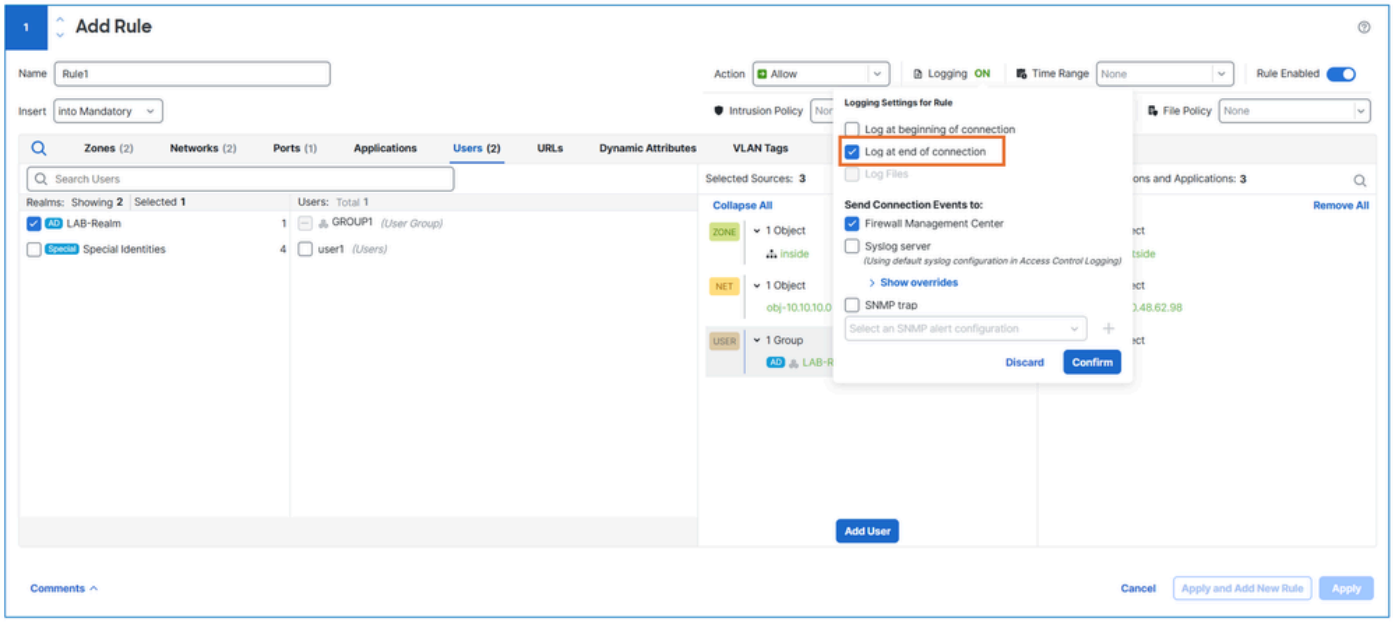
acpの作成

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

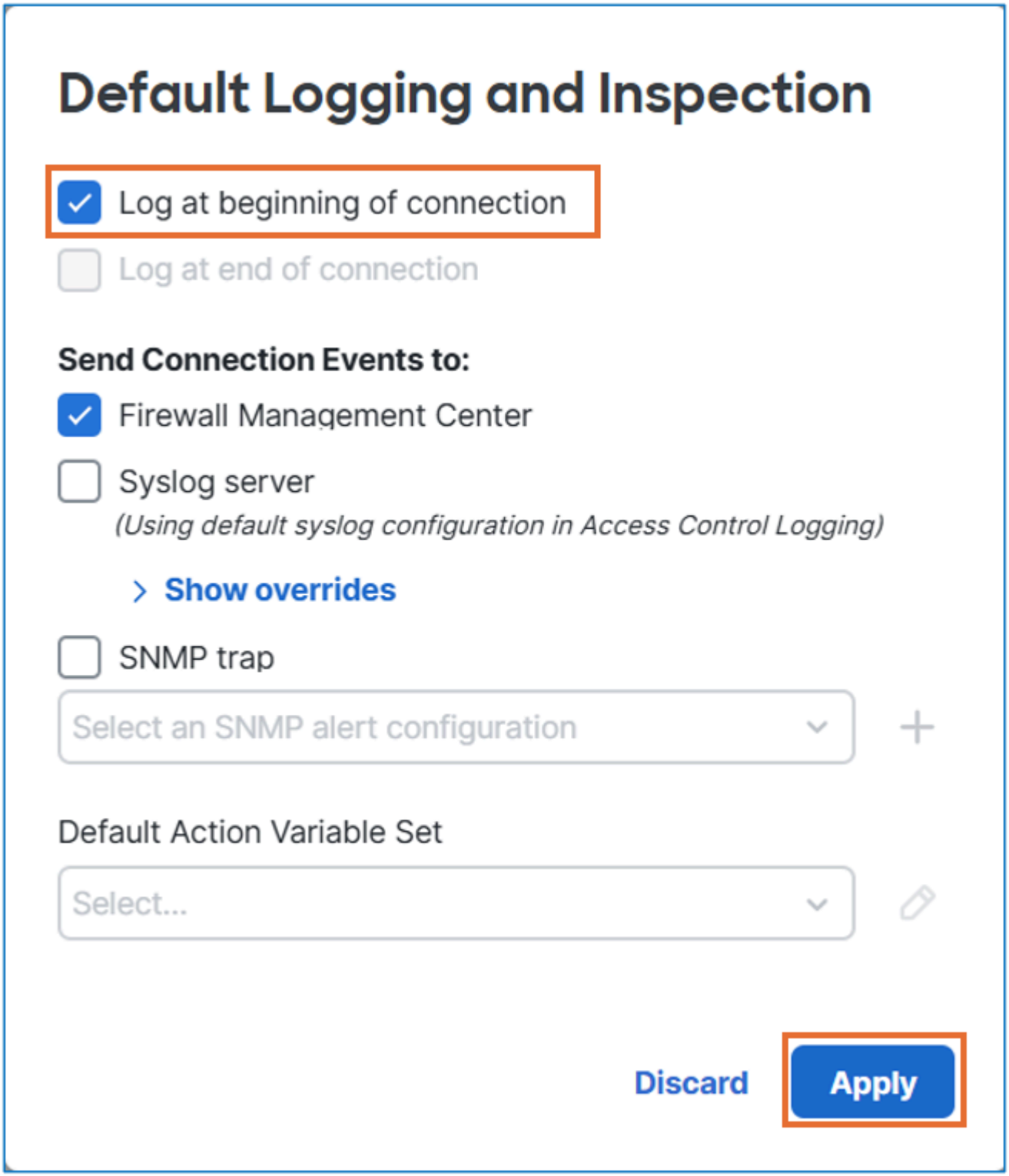
接続の最後でselectingLogを使用して、ルールのロギングを有効にします。



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。



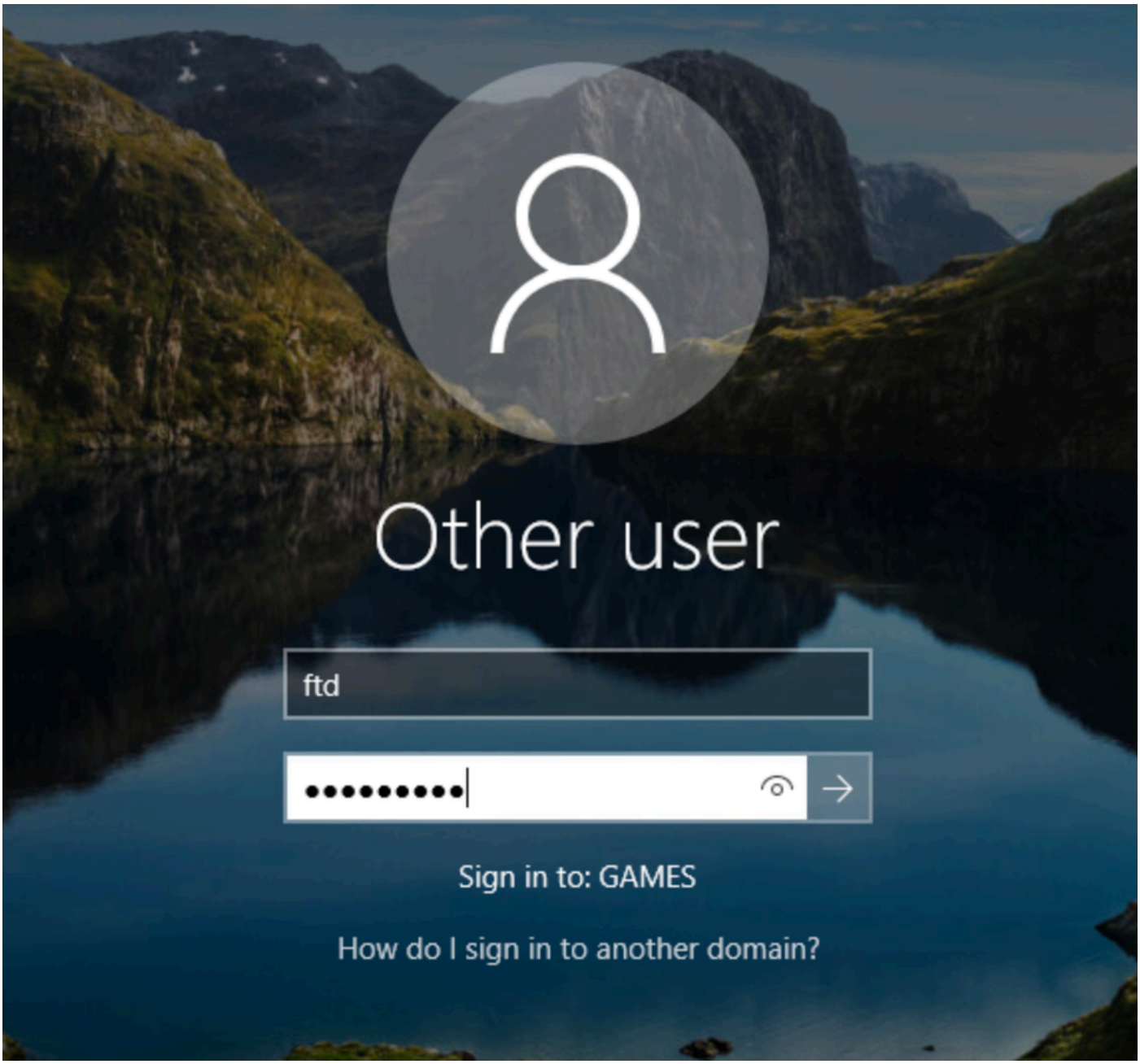
ロギングを有効にします。

FTDに設定を保存して展開します。

検証

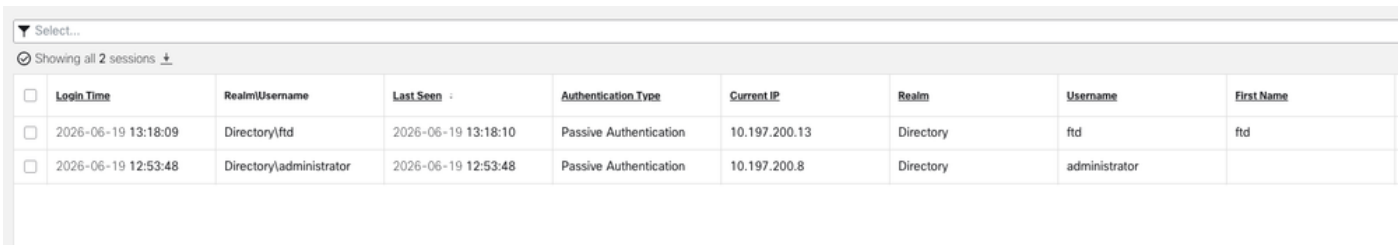
トラフィックがftdに対してのみ許可されていることを確認して、パッシブIDの動作を確認します。

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。



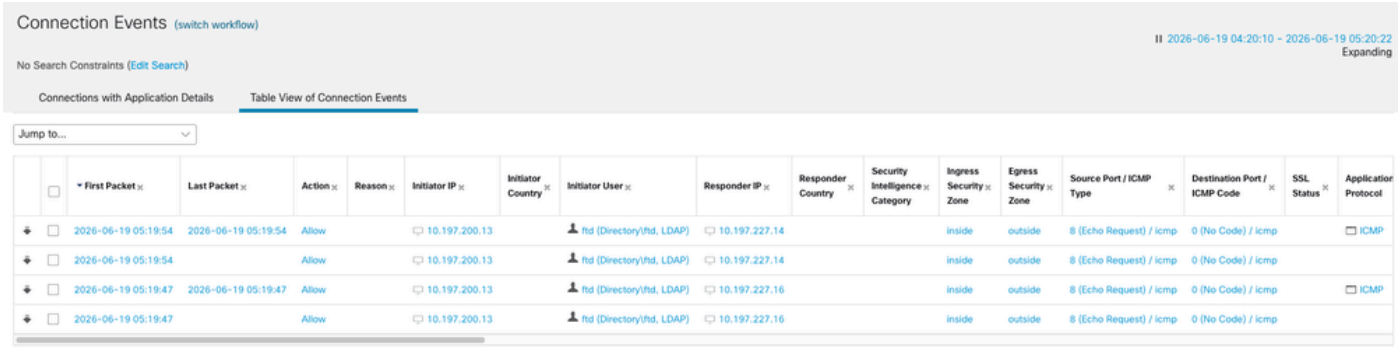
Select...

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。

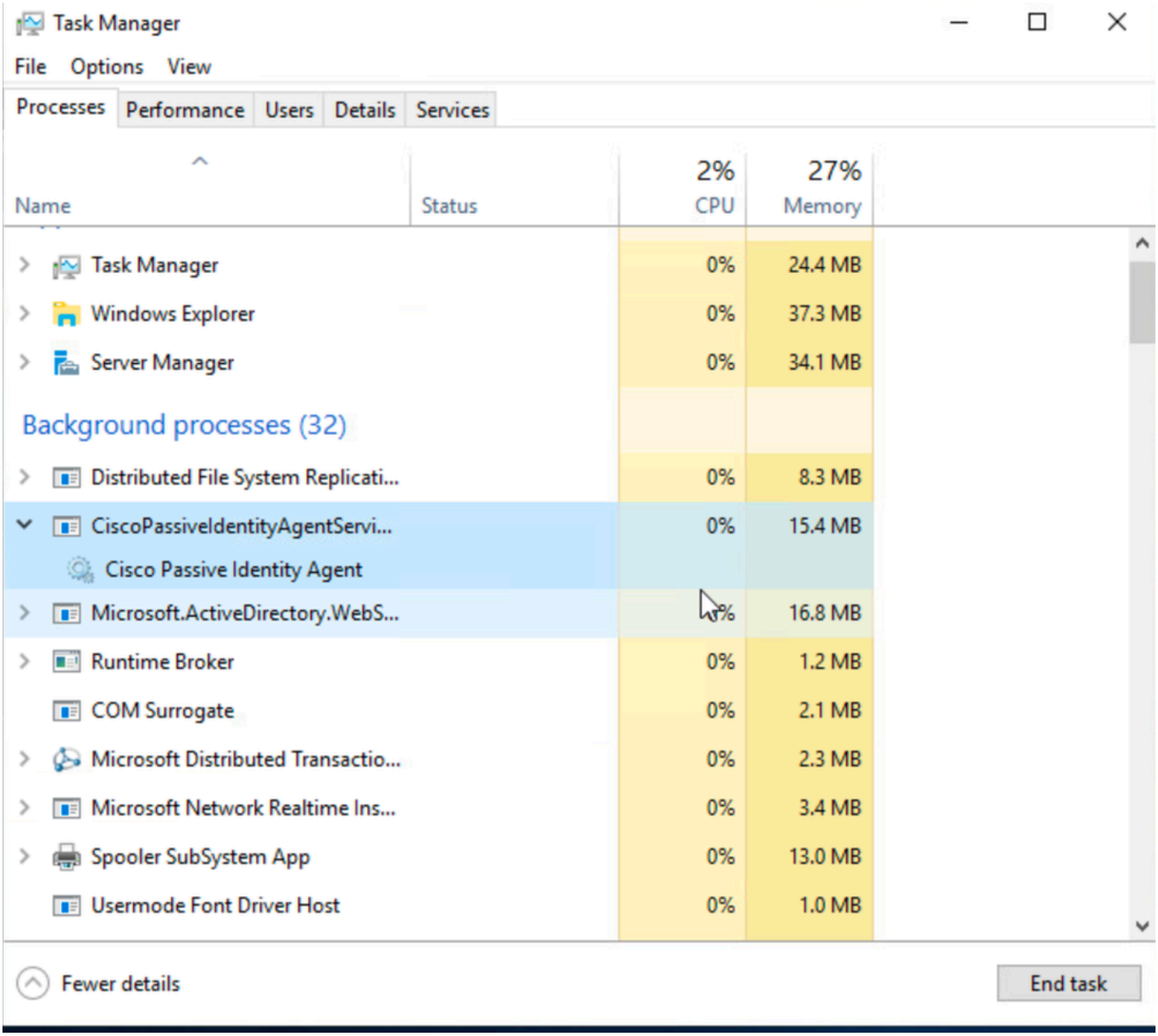


アクティブセッション

トラブルシューティング

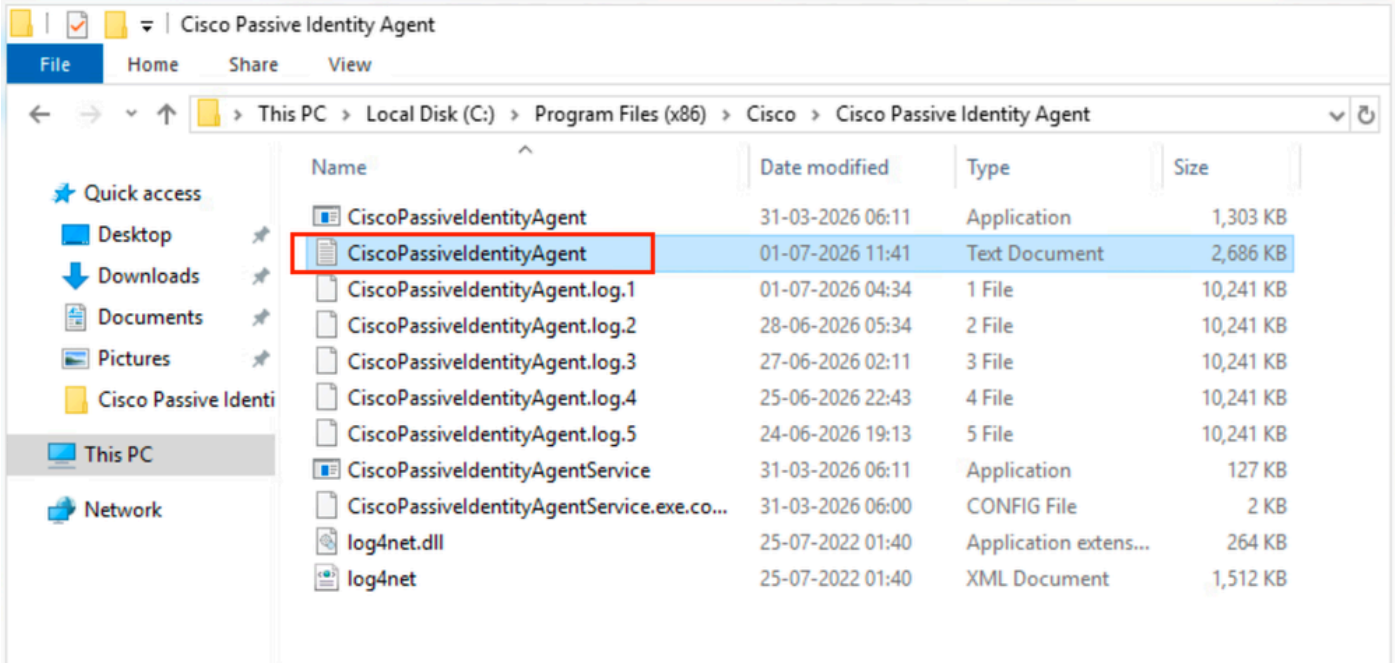
エージェントログの確認

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。



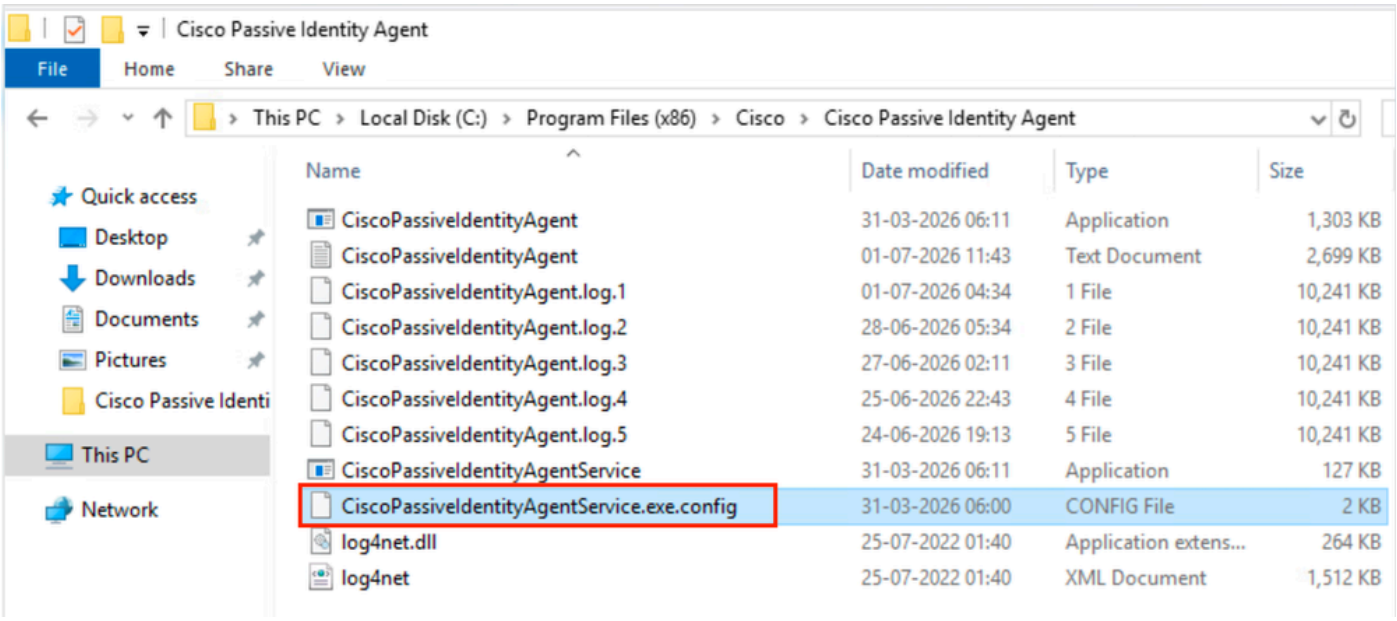
実行中のタスク

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

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： [f"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。