Configuration de Passive Identity Agent à l'aide de FMC

Table des matières

Introduction

Ce document décrit comment configurer l'agent d'identité passif Source qui envoie des données de session à FMC

Conditions préalables

Exigences

- Cisco Secure Firewall Management Center version 7.6+
- Cisco Secure Firewall version 7.6+
- Serveur Windows Active Directory, le serveur doit exécuter Windows Server 2008 ou version ultérieure.
- Vous devez activer Snort 3 sur les périphériques Secure Firewall Threat Defense.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

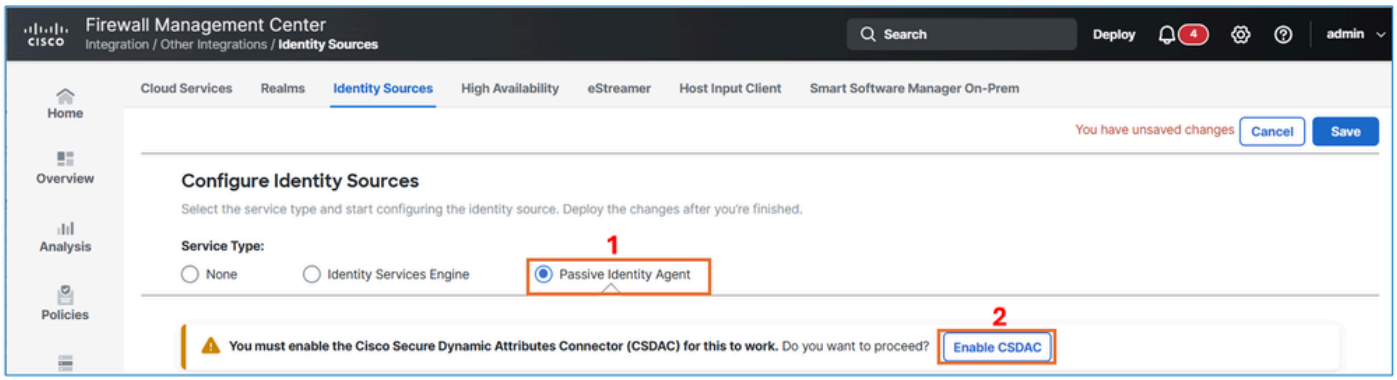
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurations

Avant de configurer l'agent, veuillez terminer l'intégration d'AD et de FMC.

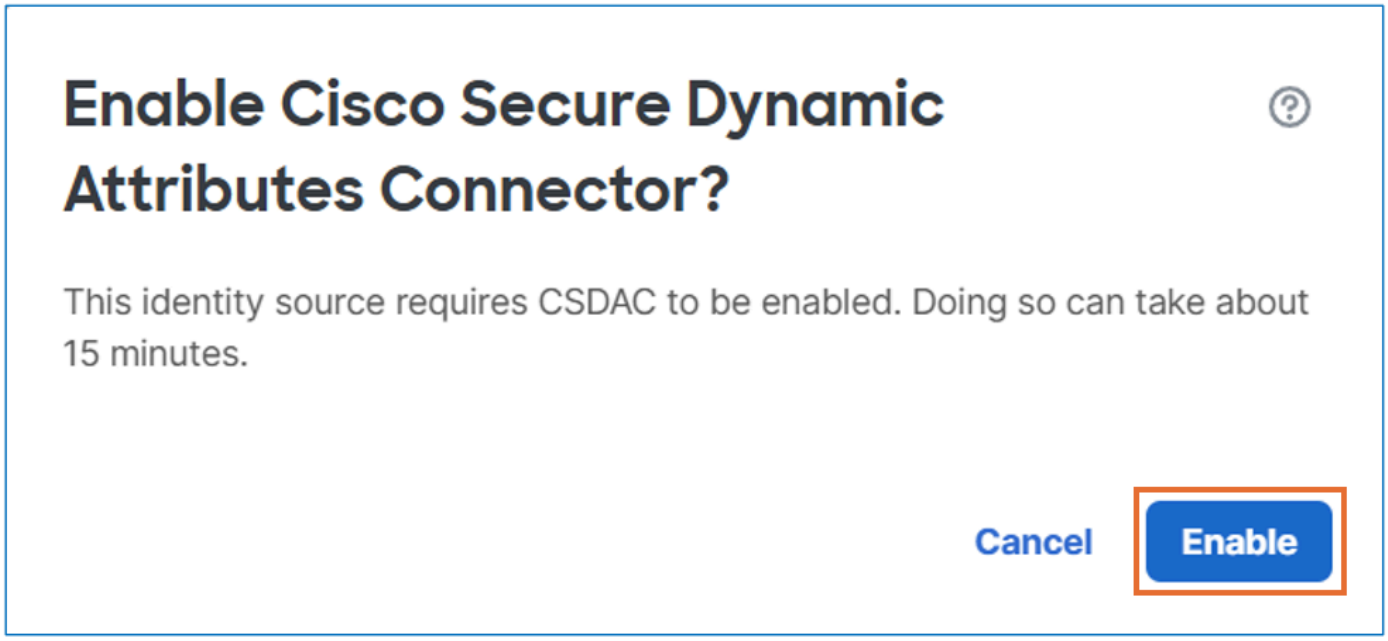
Configuration d'une source d'agent d'identité passive

Dans l'interface utilisateur de FMC, accédez à Intégration > Autres intégrations > Sources d'identité, cliquez sur Agent d'identité passif. Si le connecteur d'attributs dynamiques sécurisés Cisco n'a pas encore été activé, vous êtes invité à le faire en cliquant sur Activer CSDAC.



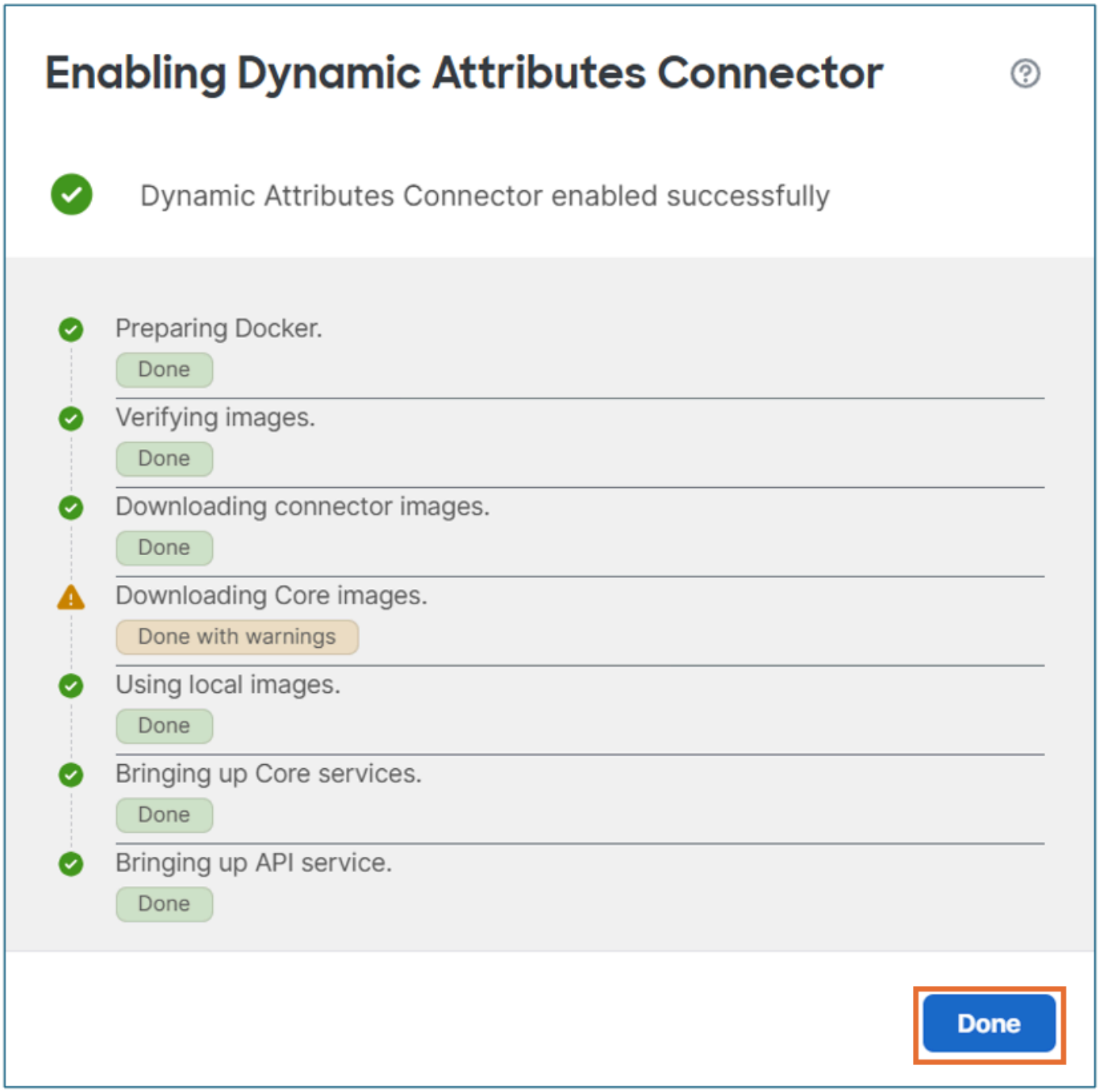
Agent d'identité passif

Cliquez sur le bouton Activer pour activer le CSDAC.



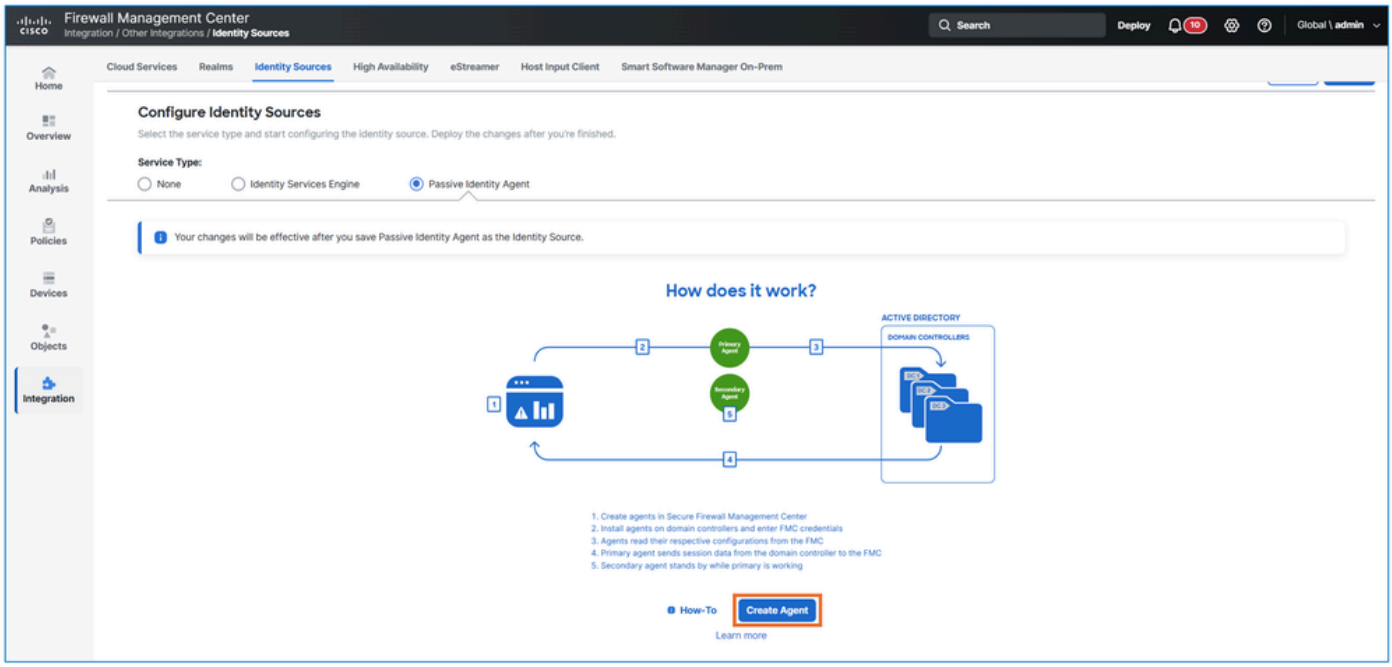
Activer CSDAC

Cette étape prend environ 10 minutes. Une fois que le CSDAC est correctement activé, cliquez sur le bouton Terminer pour continuer.



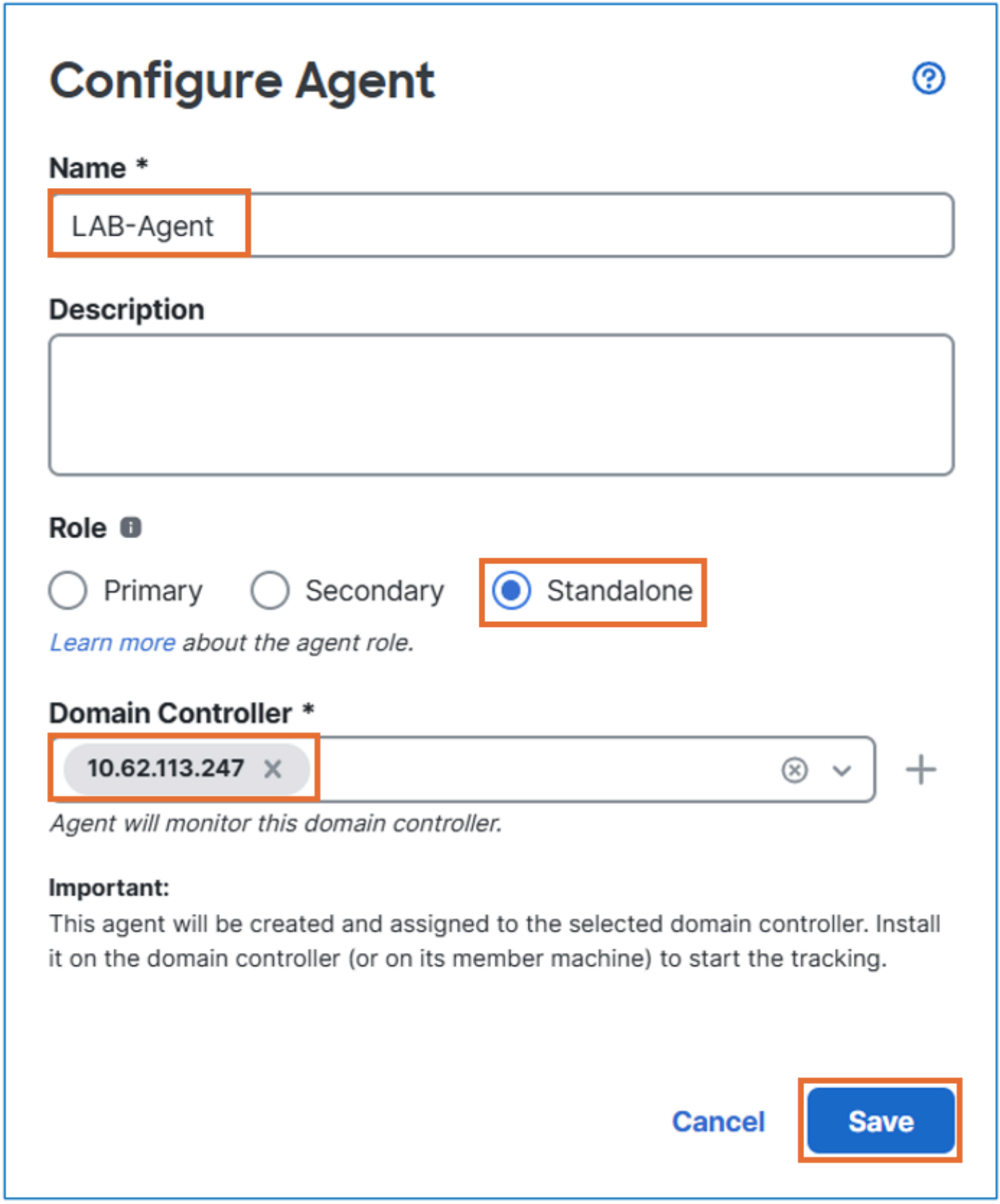
CSDAC activé

Cliquez sur le bouton Créer un agent.



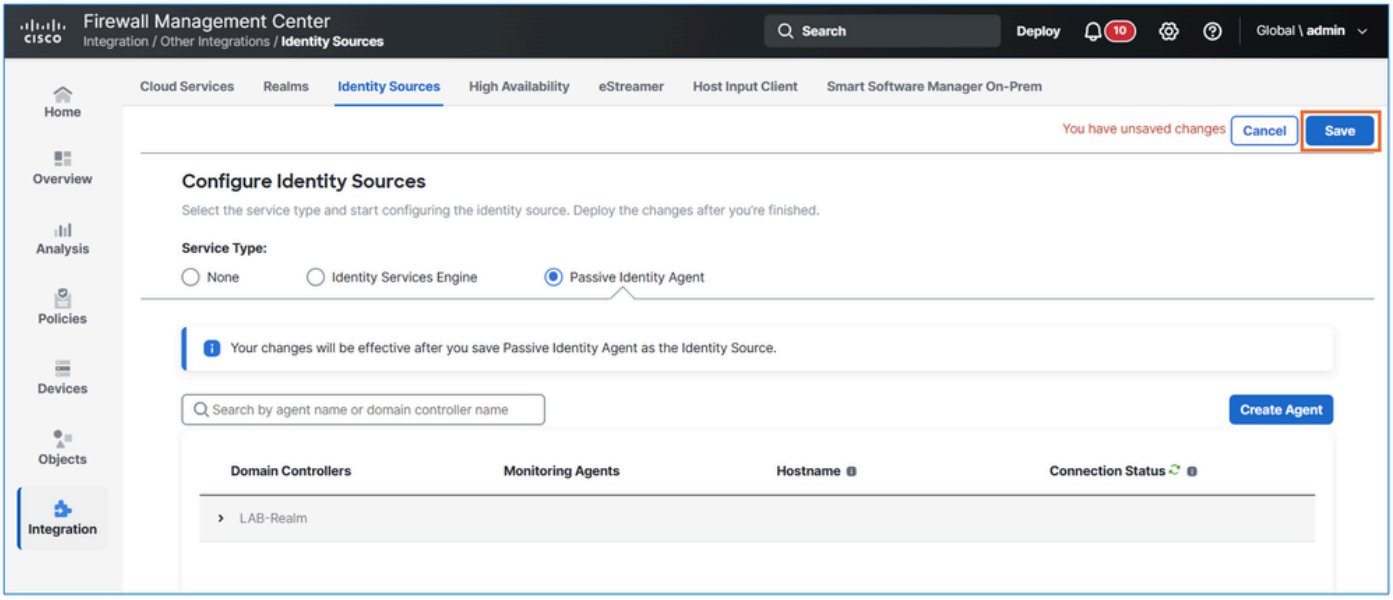
Créer un agent

Définissez un nom pour l'agent, sélectionnez l'option Autonome et associez-la au contrôleur de domaine approprié créé dans la tâche précédente.



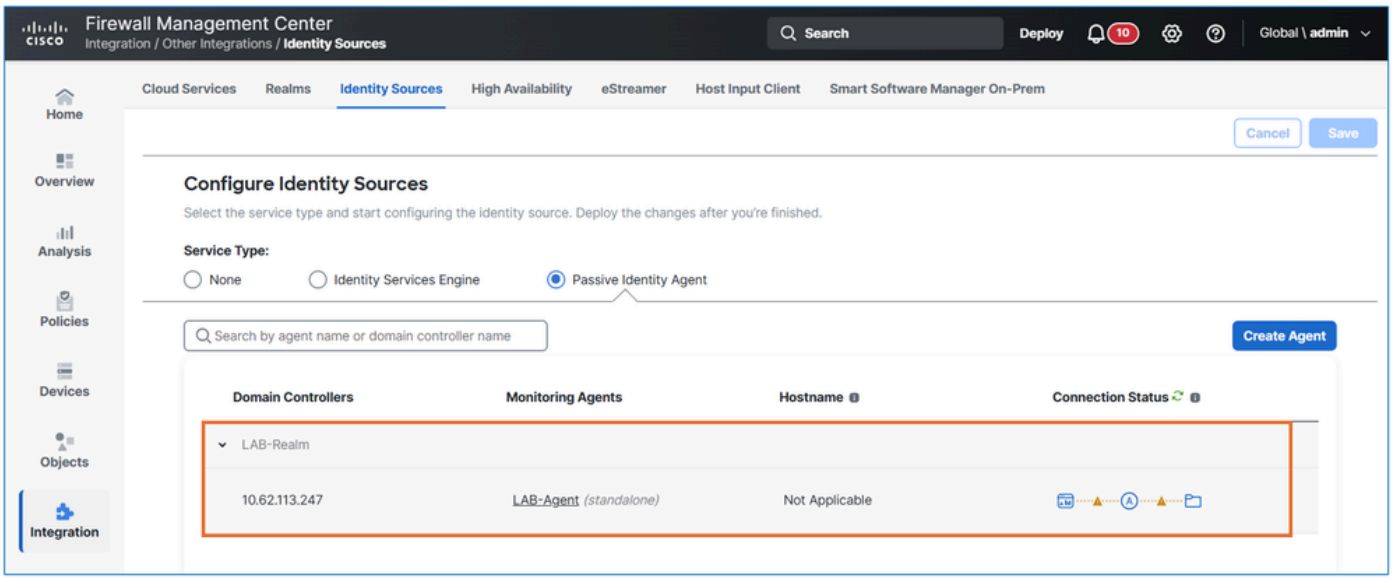
Configurer l'agent

Cliquez sur le bouton Enregistrer.



Enregistrez la configuration

Le résultat .



Vérifier l'état

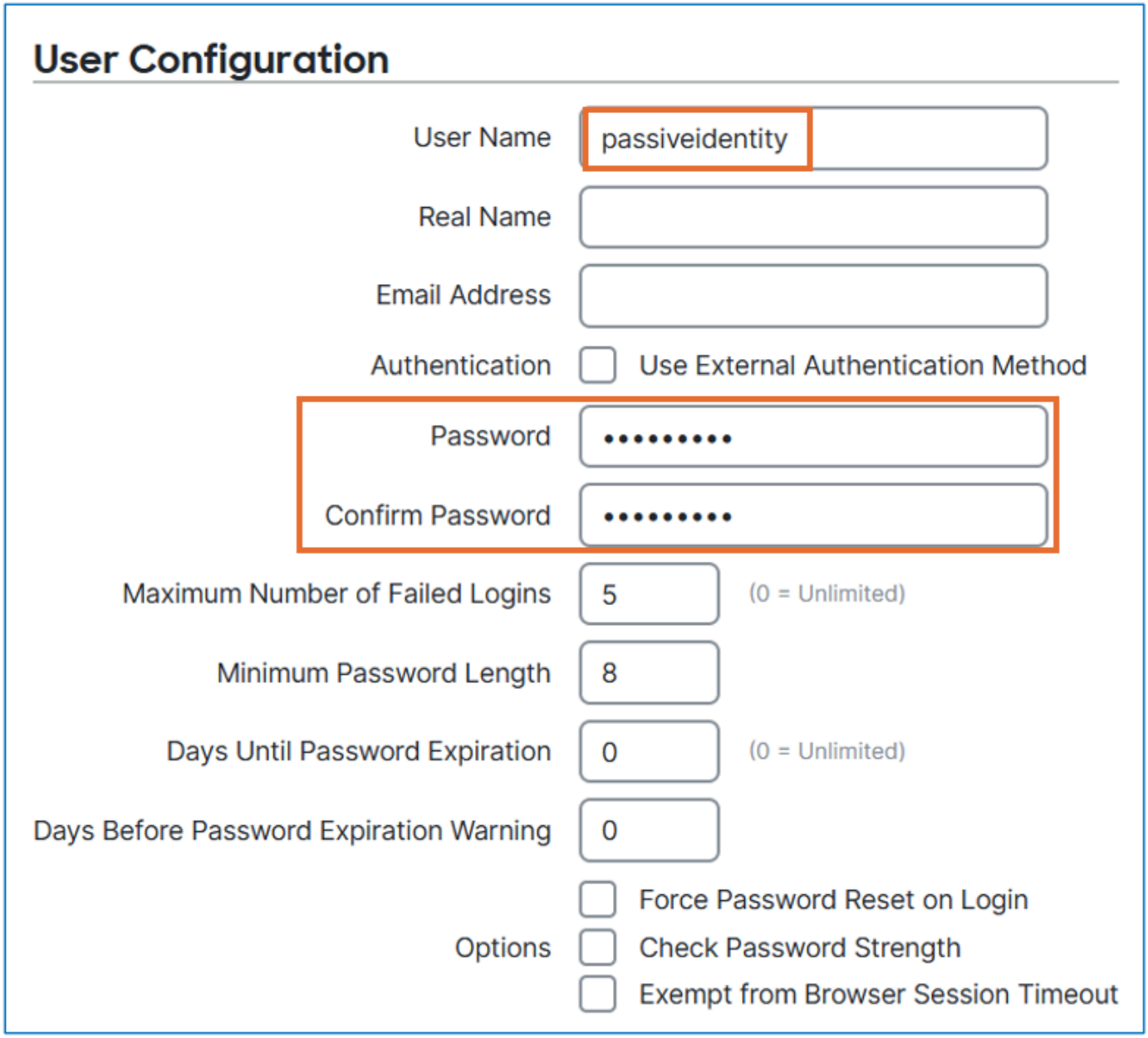
Remarque : L'agent d'identité passif indique l'état à l'aide de lignes, l'orange signifie que l'agent n'a jamais communiqué avec le Centre de gestion du pare-feu sécurisé. Une ligne d'agent nouvellement créée est orange et le reste jusqu'à ce que la configuration soit terminée.

Création d'un utilisateur d'Identity Agent passif sur le Secure Firewall Management

Center

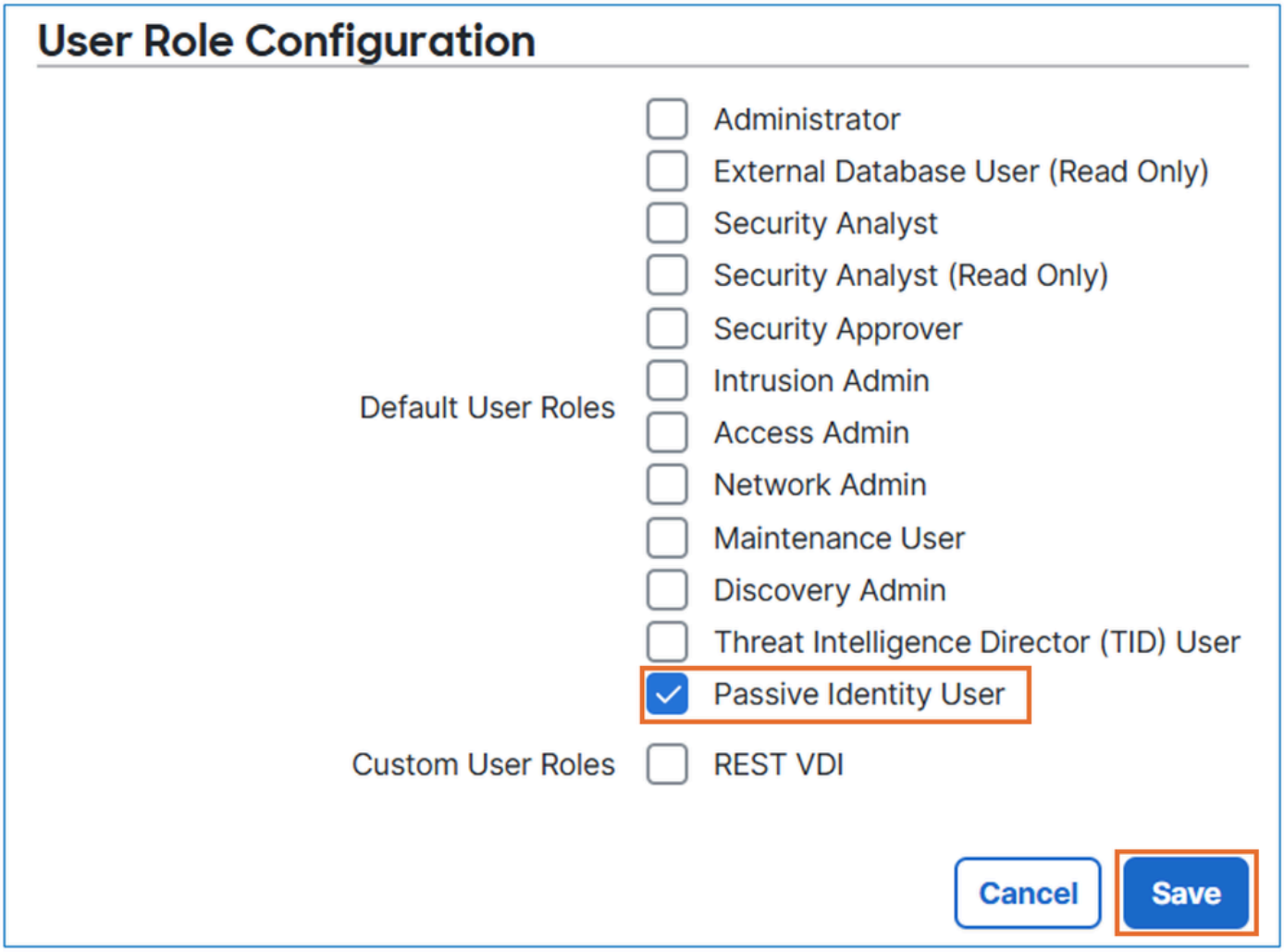
Créez un utilisateur Secure Firewall Management Center disposant des autorisations suffisantes pour communiquer avec l'agent d'identité passif. Cet utilisateur dispose de privilèges limités pour effectuer d'autres tâches ; l'utilisateur doit uniquement activer la communication avec l'agent d'identité passif.

Dans l'interface utilisateur de FMC, accédez à Système > Utilisateurs et cliquez sur Créer un utilisateur. Renseignez les détails de l'utilisateur en fonction des exigences de la tâche.



Créer un utilisateur

Attribuez uniquement le rôle d'utilisateur Identité passive. Cliquez sur le bouton Enregistrer.

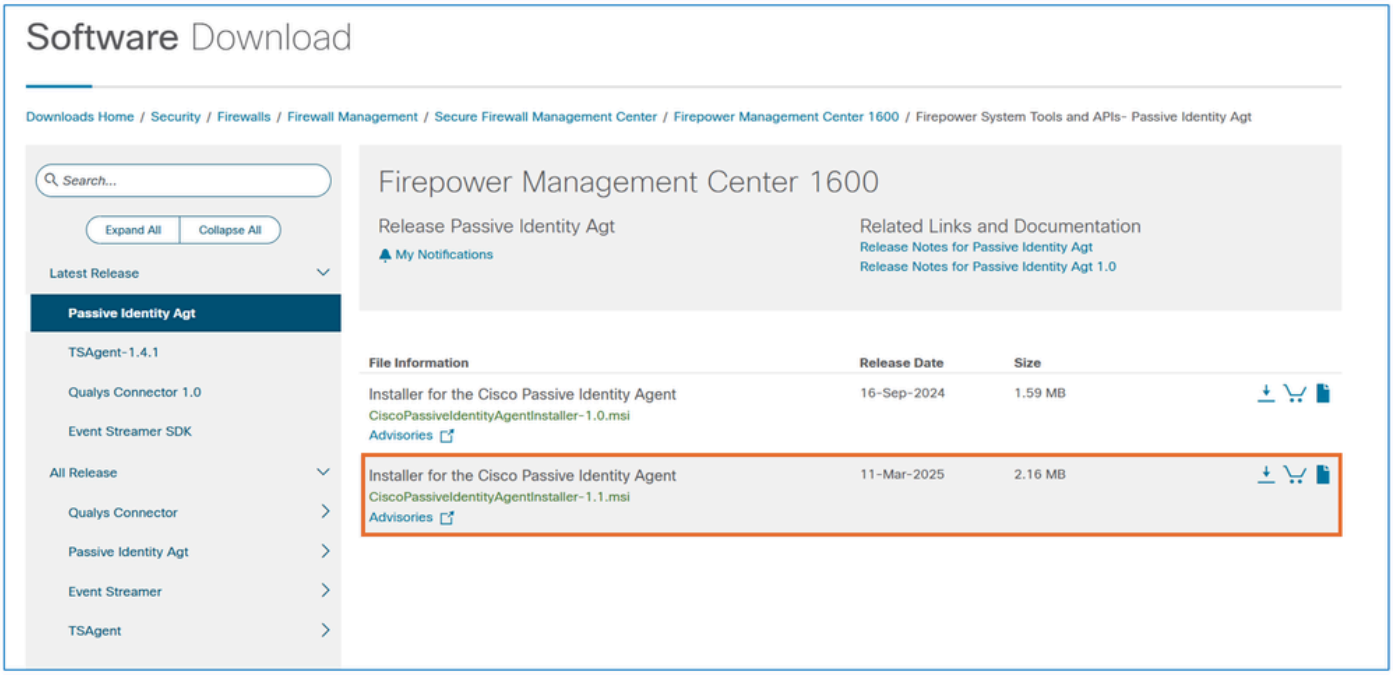


sélectionnez l'utilisateur d'identité passive

Installation et configuration du logiciel Passive Identity Agent

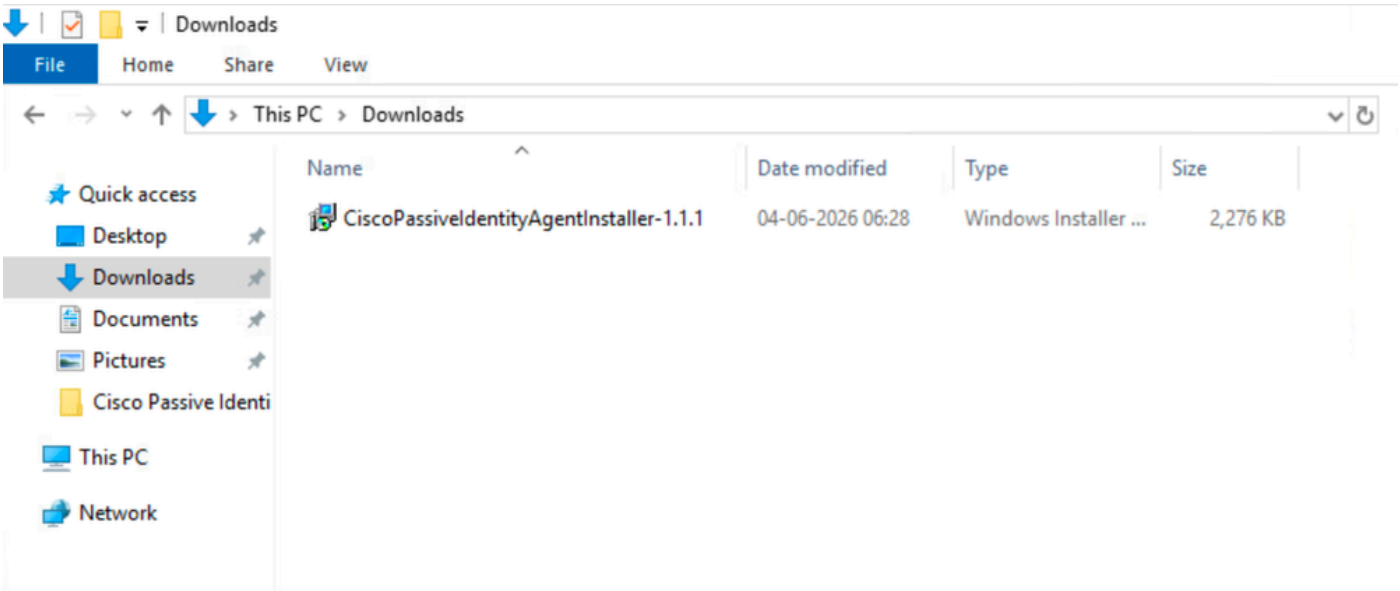
Installez et configurez le logiciel Passive Identity Agent sur le contrôleur de domaine désigné.

Téléchargez l'agent d'identité passif depuis software.cisco.com.



télécharger le logiciel

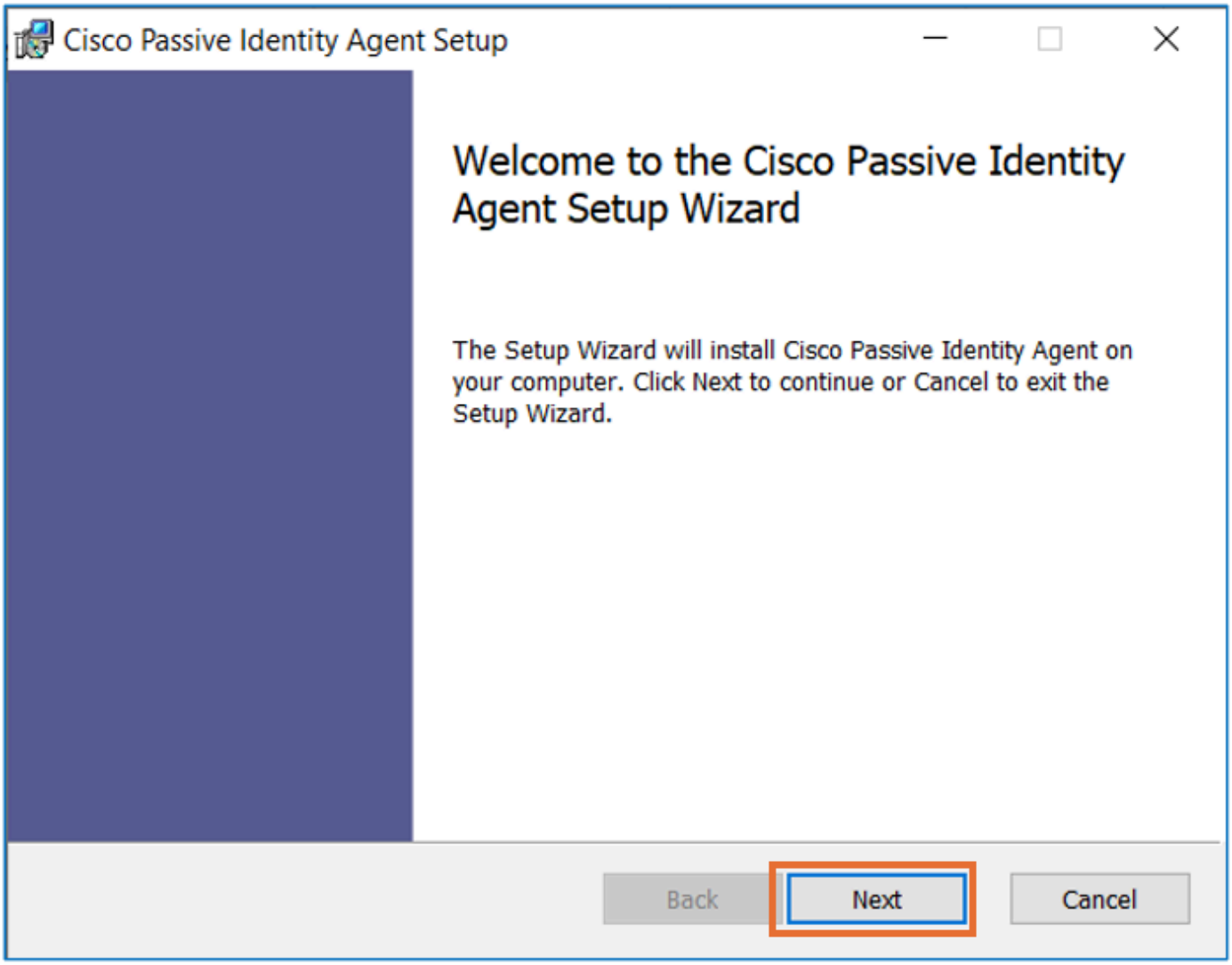
Après avoir téléchargé l'agent, commencez le processus d'installation sur le contrôleur de domaine.



préposé

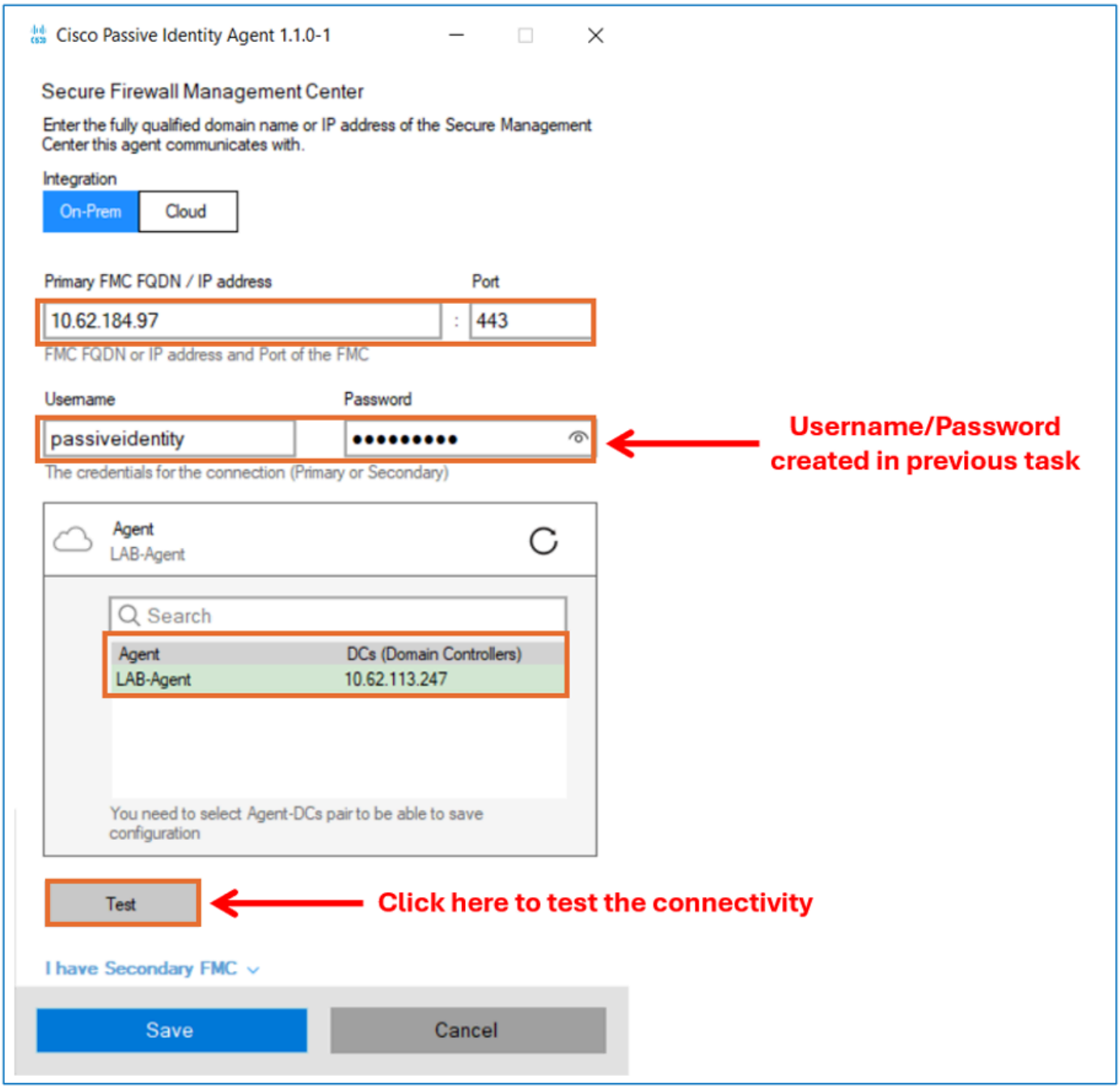
]

Reportez-vous aux instructions d'installation fournies pour terminer la configuration.



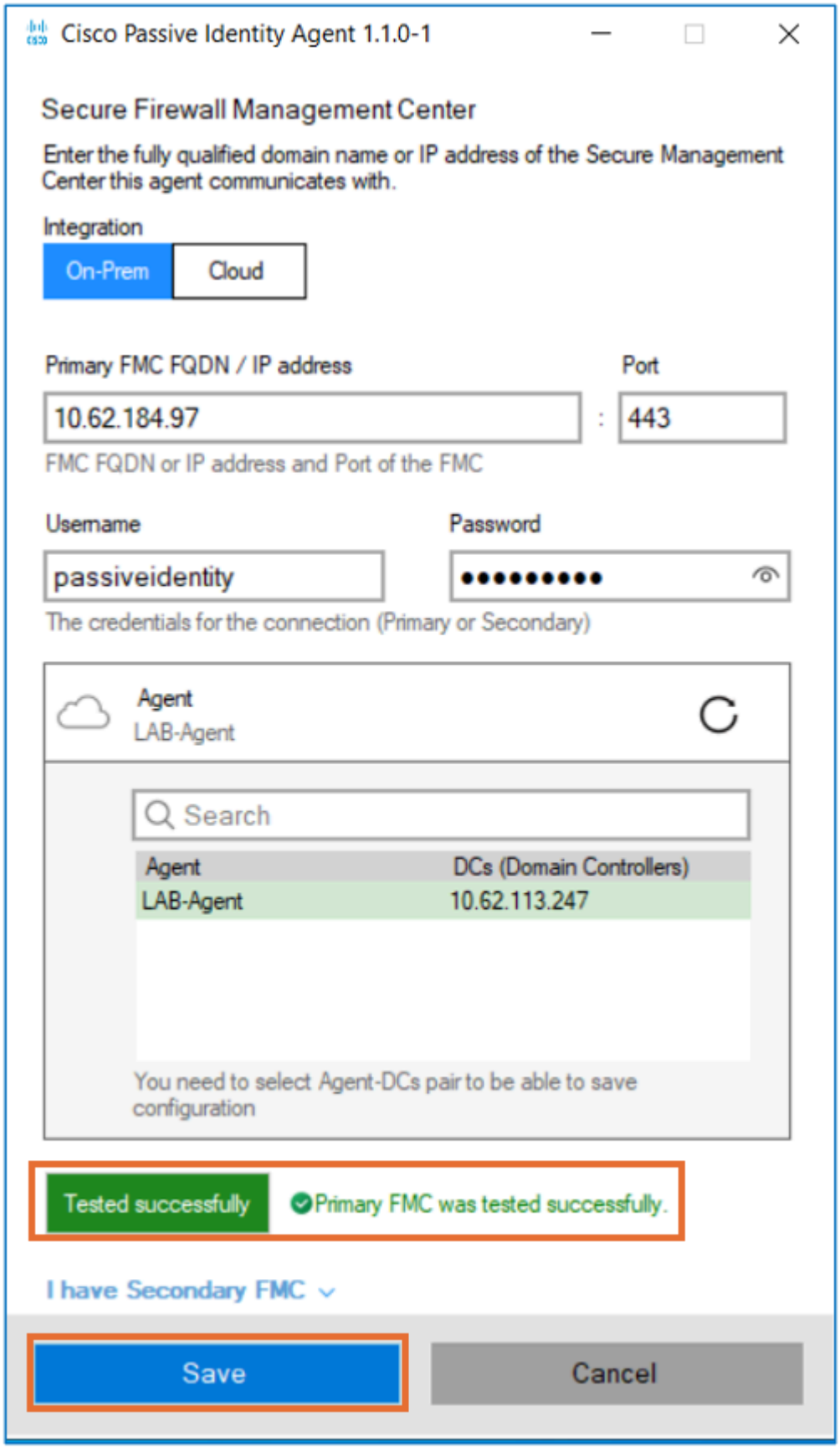
Install

Une fois l'installation terminée, ouvrez le logiciel Passive Identity Agent et entrez les informations requises comme indiqué dans les exigences de la tâche. Cliquez sur le bouton Test pour vérifier la connectivité avec le FMC.



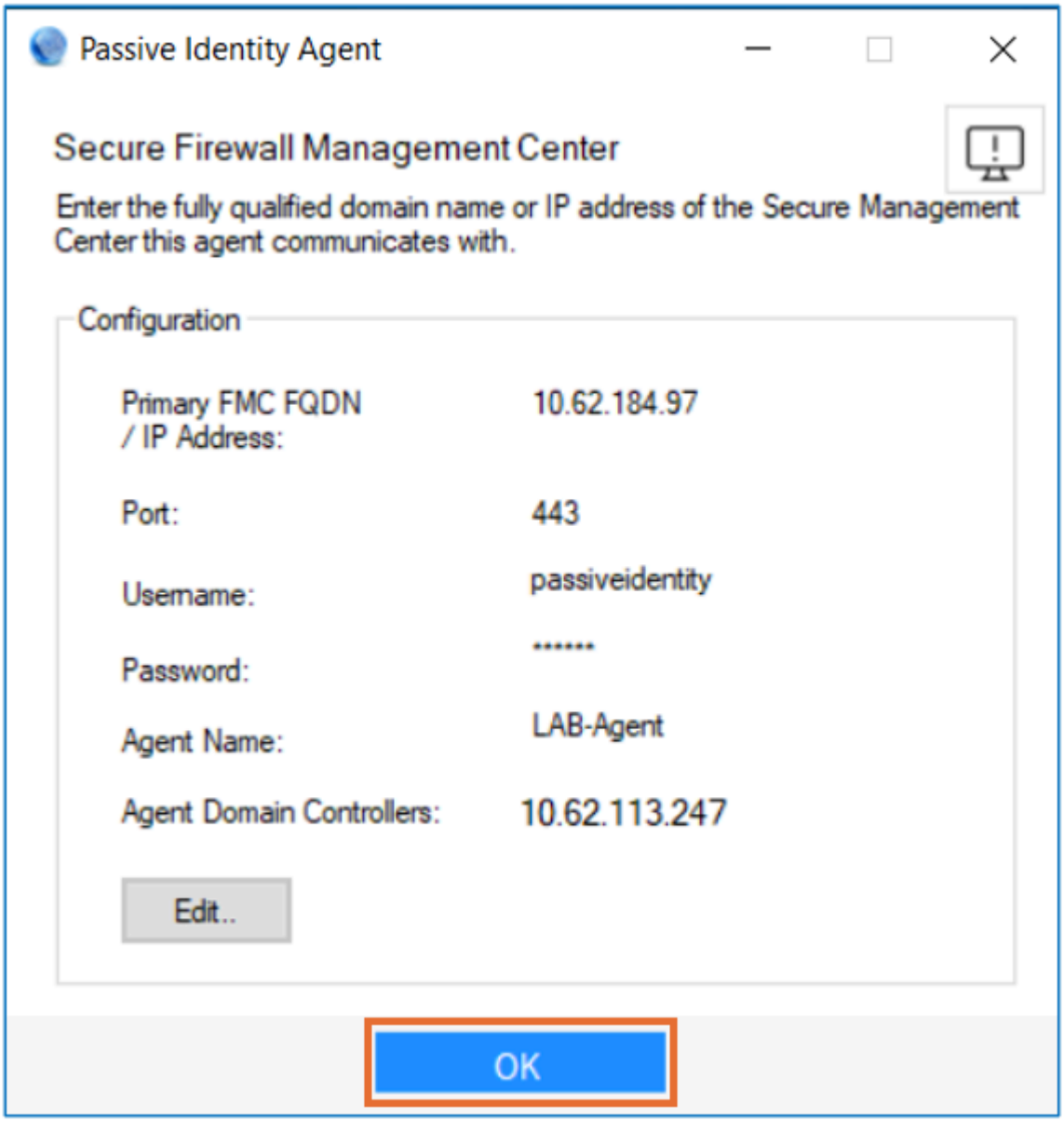
configurez l'agent.

Après avoir testé la connectivité, cliquez sur le bouton Enregistrer.



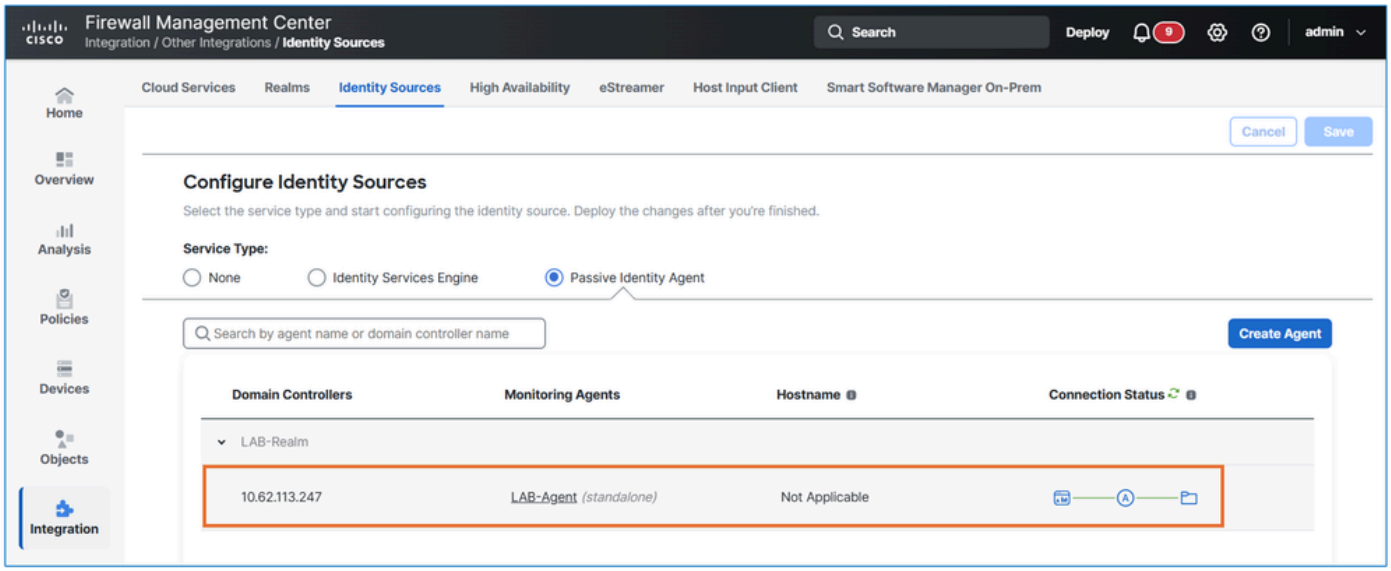
épreuve

Cliquez sur le bouton OK pour terminer la configuration de l'agent.



l'agent est en cours

Dans l'interface utilisateur de FMC, accédez à Intégration > Autres intégrations > Sources d'identité > Agent d'identité passif. Vérifiez que l'agent d'identité passif affiche un état vert.



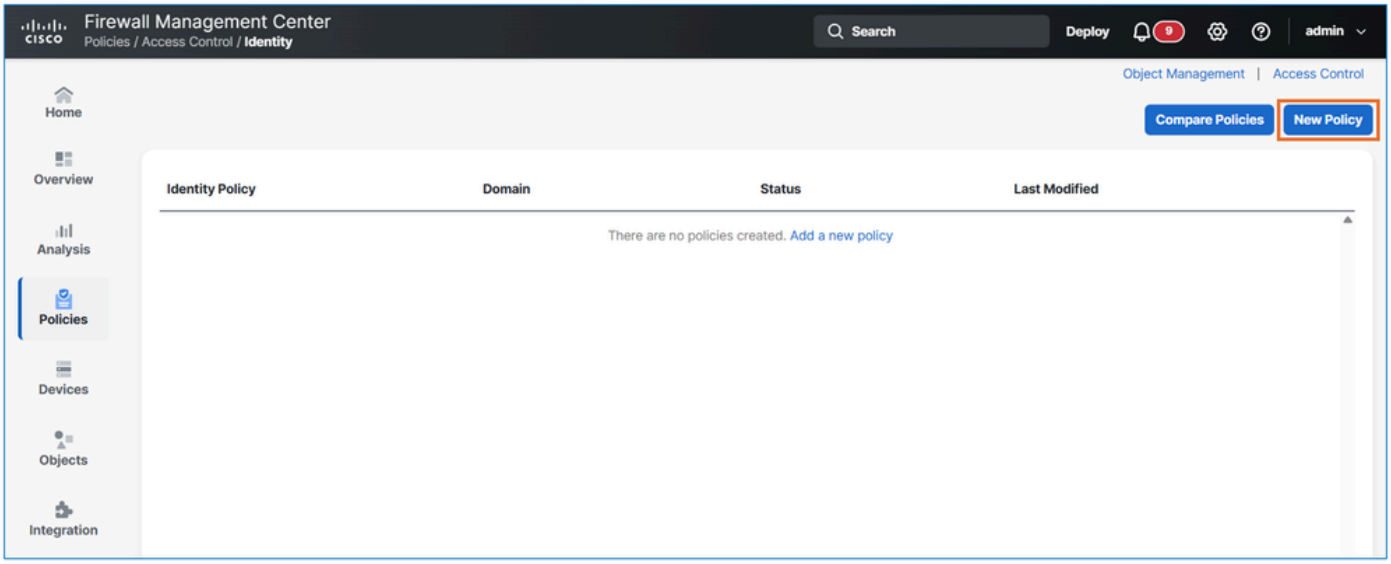
vérification de la communication de fmc

Configurer les stratégies d'identité

Créez une politique d'identité basée sur la table fournie.

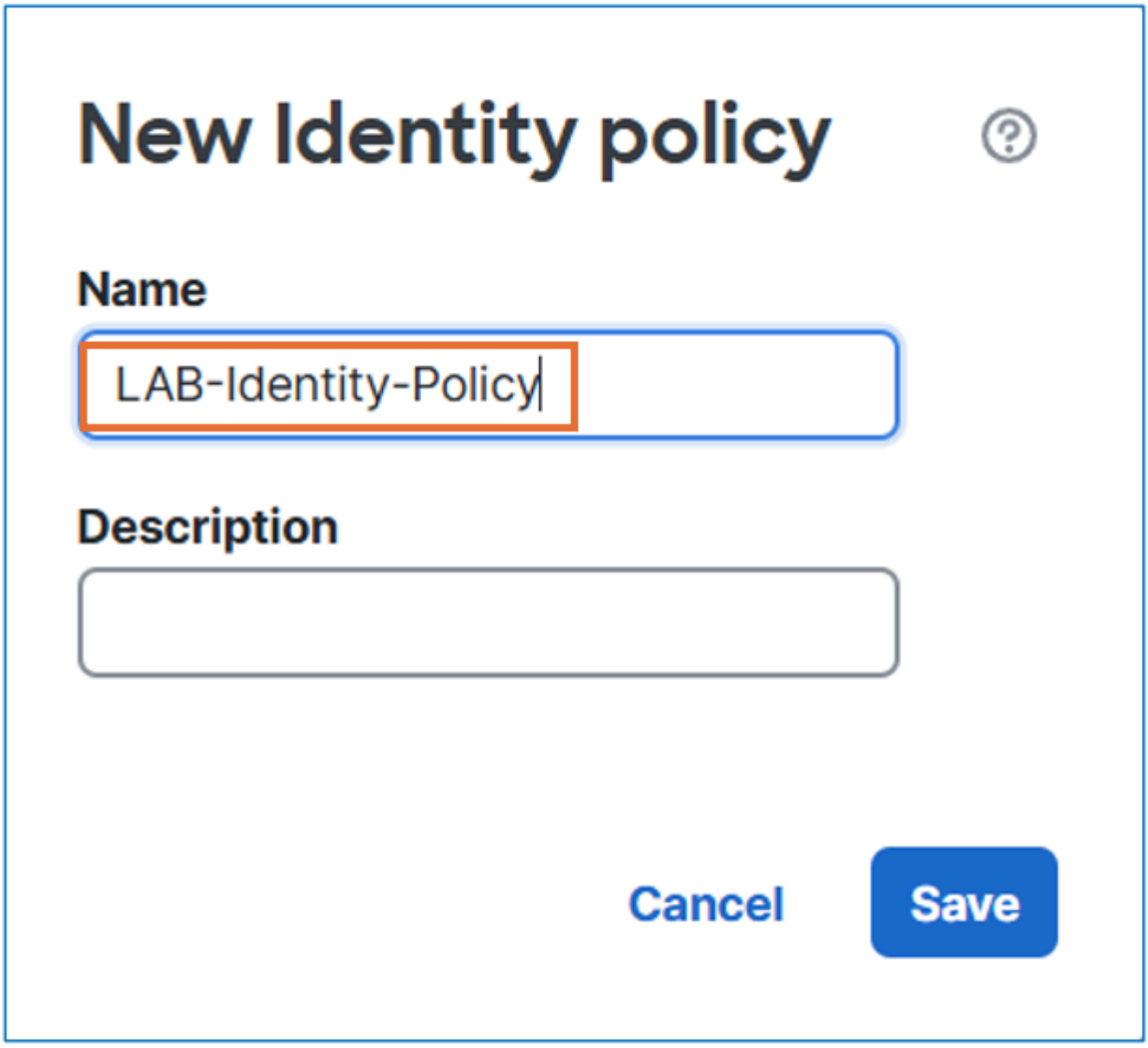
Nom de stratégie	Nom de règle	Domaine d'authentification	Paramètres restants
LAB-Identity-Policy	Règle1	Domaine de travaux pratiques	Laisser par défaut

Dans l'interface utilisateur de FMC, accédez à Politiques > Contrôle d'accès > Identité. Cliquez sur le bouton Nouvelle stratégie.



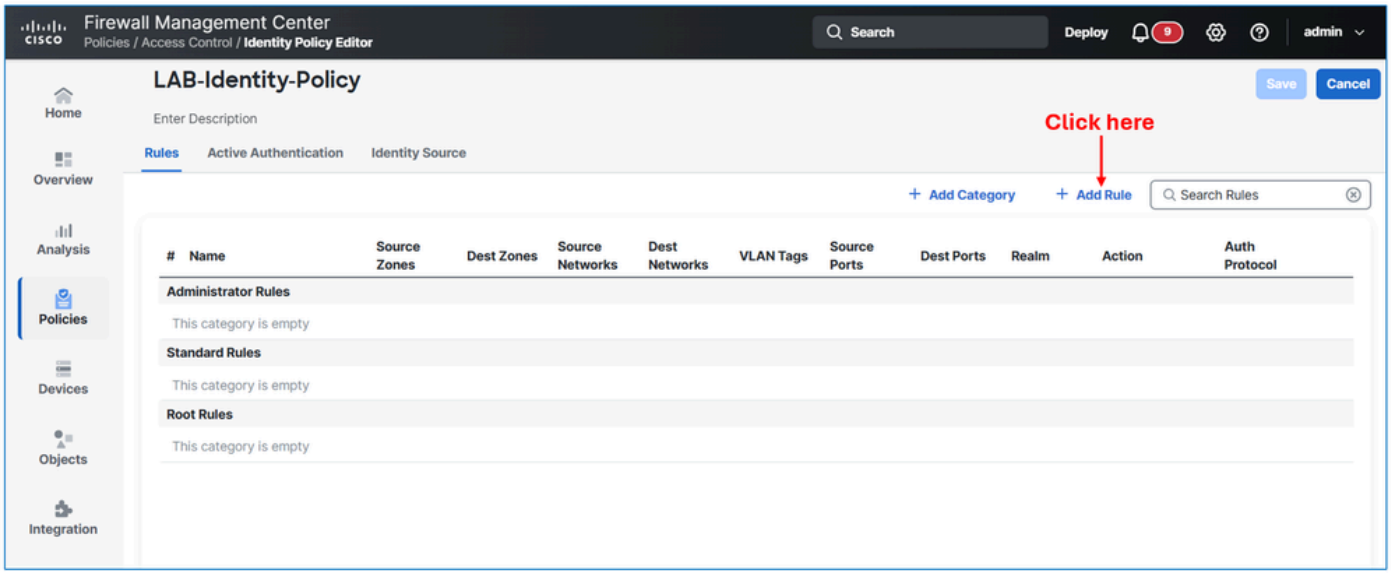
nouvelle police

Entrez le nom de la stratégie en fonction des exigences de la tâche.



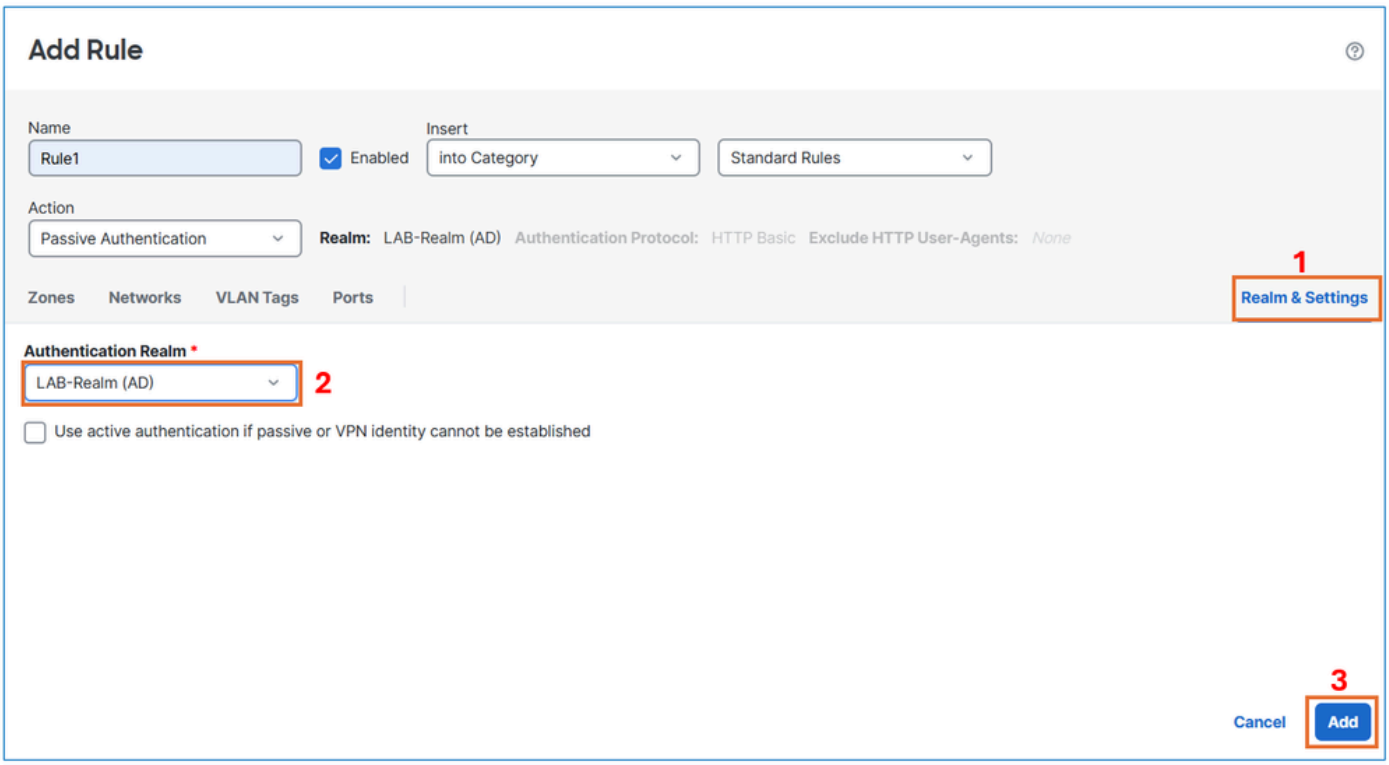
nouvelle police

Cliquez sur le bouton Ajouter une règle.



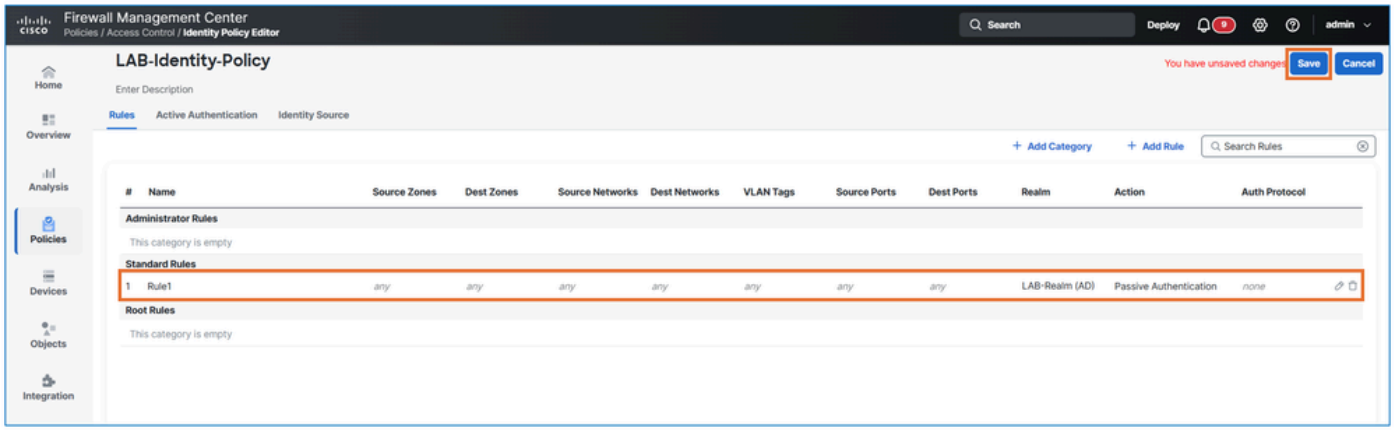
créer une règle

Accédez à l'ongletDomaine et paramètres et sélectionnez le domaine d'authentification en fonction des exigences de tâche. Enfin, cliquez sur le bouton Ajouter.



Paramètre du domaine

Cliquez sur le bouton Enregistrer.



enregistrez la configuration

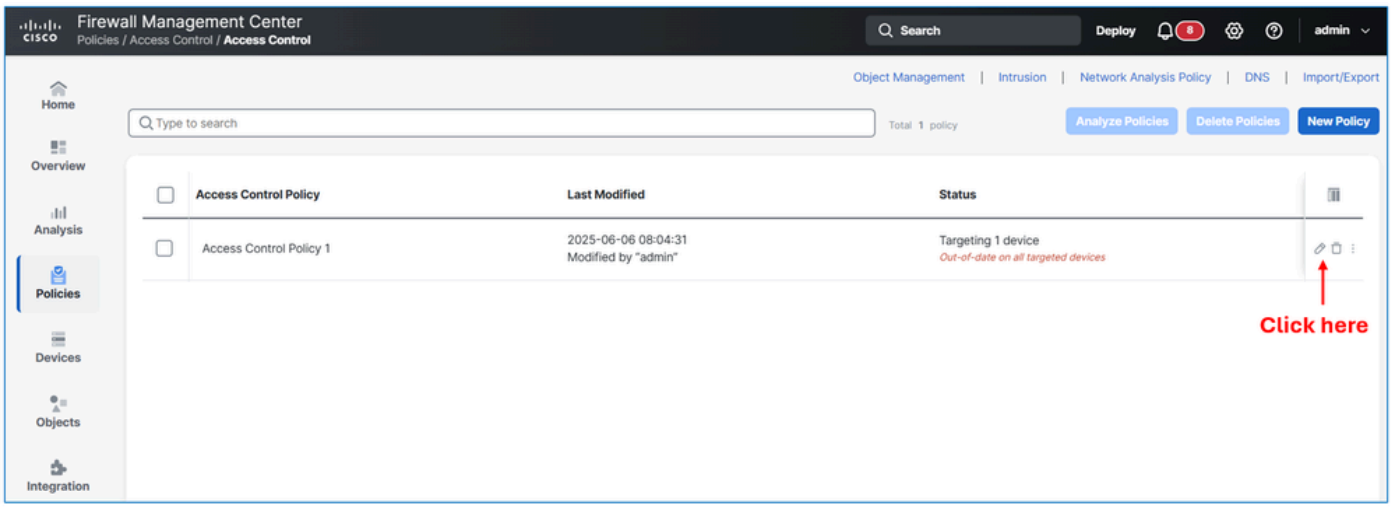
Configurer les stratégies de contrôle d'accès

Liez la stratégie d'identité à la stratégie de contrôle d'accès et créez une règle de stratégie d'accès avec les attributs suivants :

Nom d'attribut	Valeur
Nom de règle	Règle1
Action	Allow
Zone source	Intérieur
Zone de destination	Extérieur
Réseaux sources	10.10.10.0/24
Réseaux de destination	10.48.62.98/32
Service	Port de destination TCP 80 (HTTP)
Utilisateurs	LAB-Realm/GROUPE1
Journalisation	À la fin de la connexion

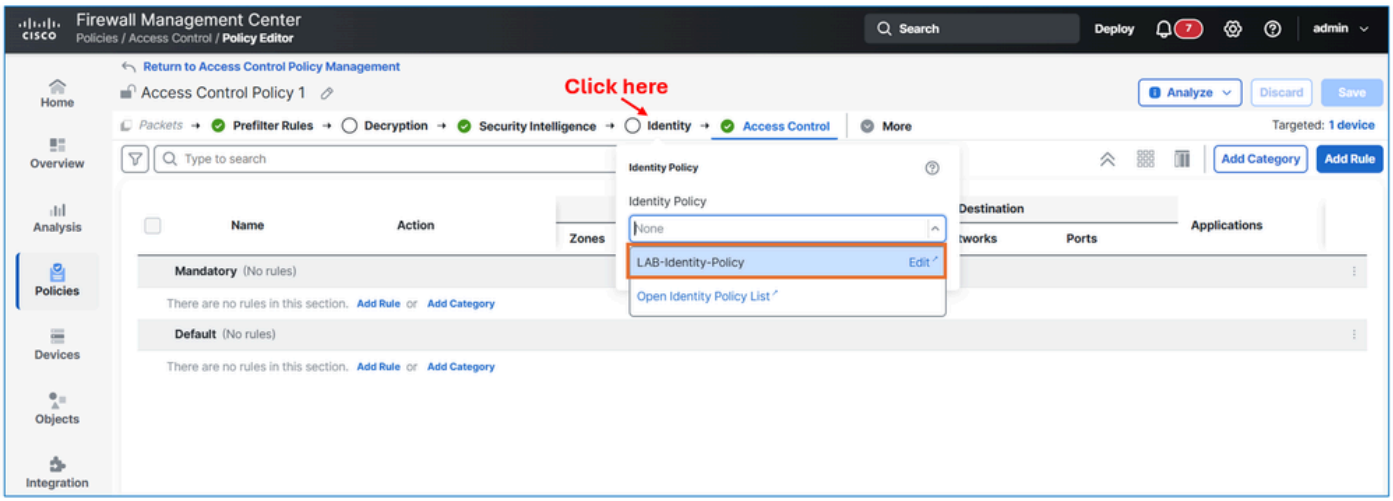
Étape 1. Lier la stratégie d’identité à la stratégie de contrôle d’accès

Dans l'interface utilisateur de FMC, accédez à Politiques > Contrôle d'accès > Contrôle d'accès. Cliquez sur le bouton Modifier correspondant à votre stratégie.



Modifier la stratégie

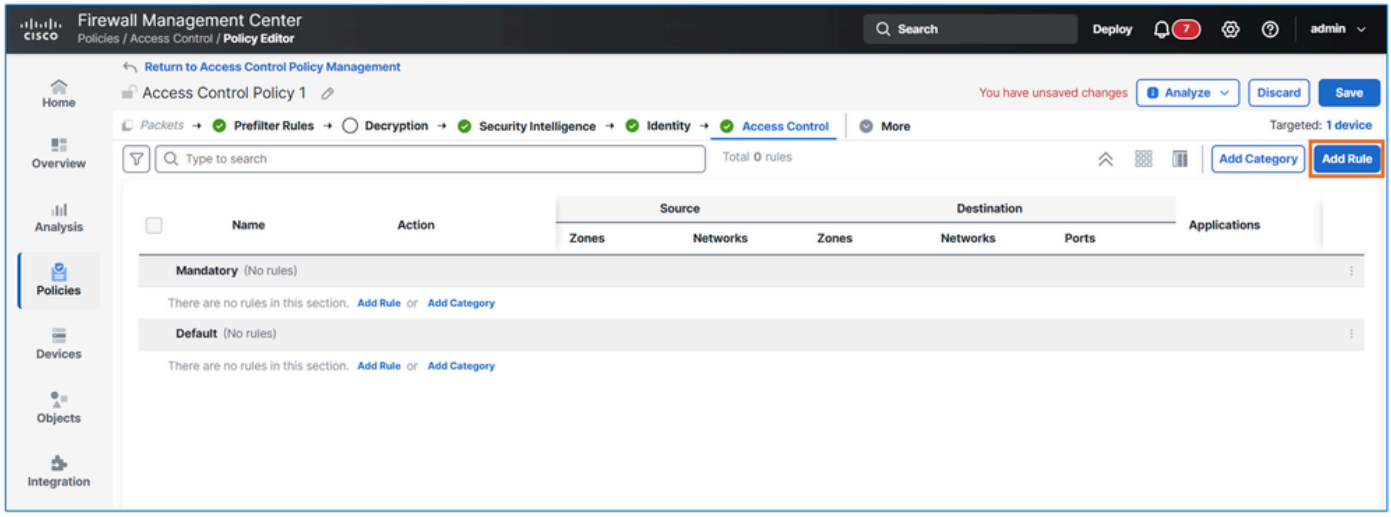
Accédez à la section Identité et liez la politique d'identité créée dans la tâche précédente.



ajouter une stratégie d'identité

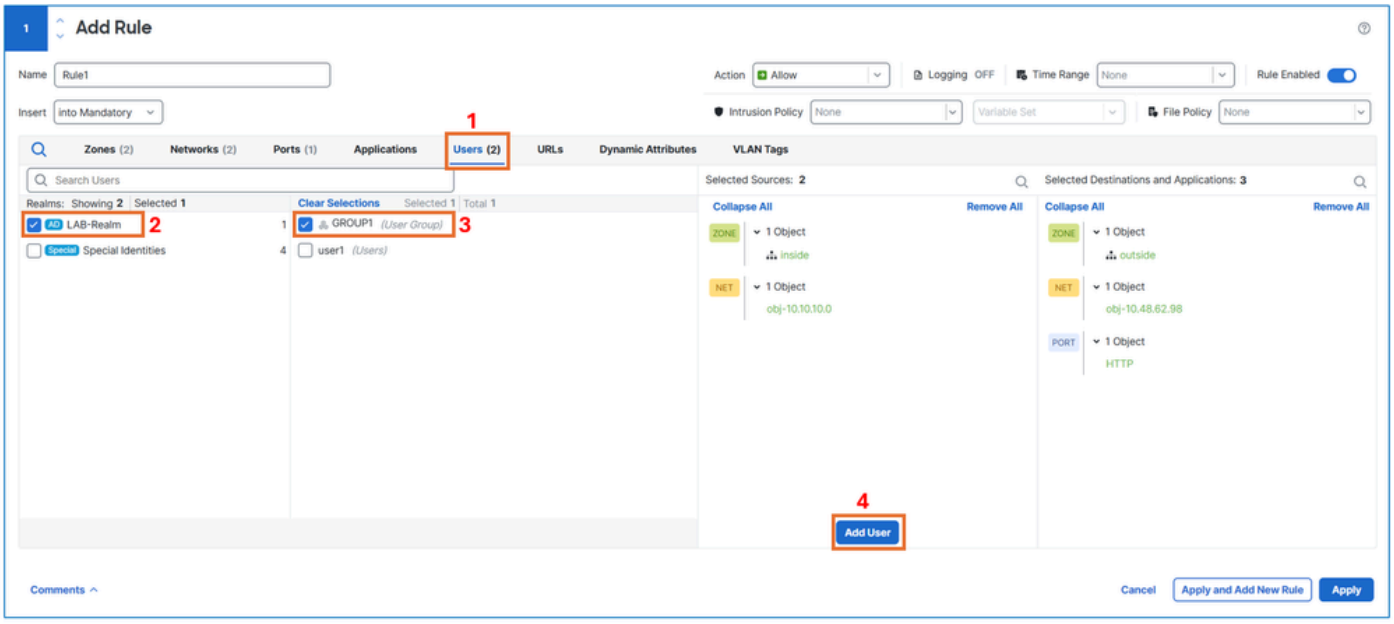
Cliquez sur le bouton Appliquer

Étape 2 : création de la règle de contrôle d’accès.



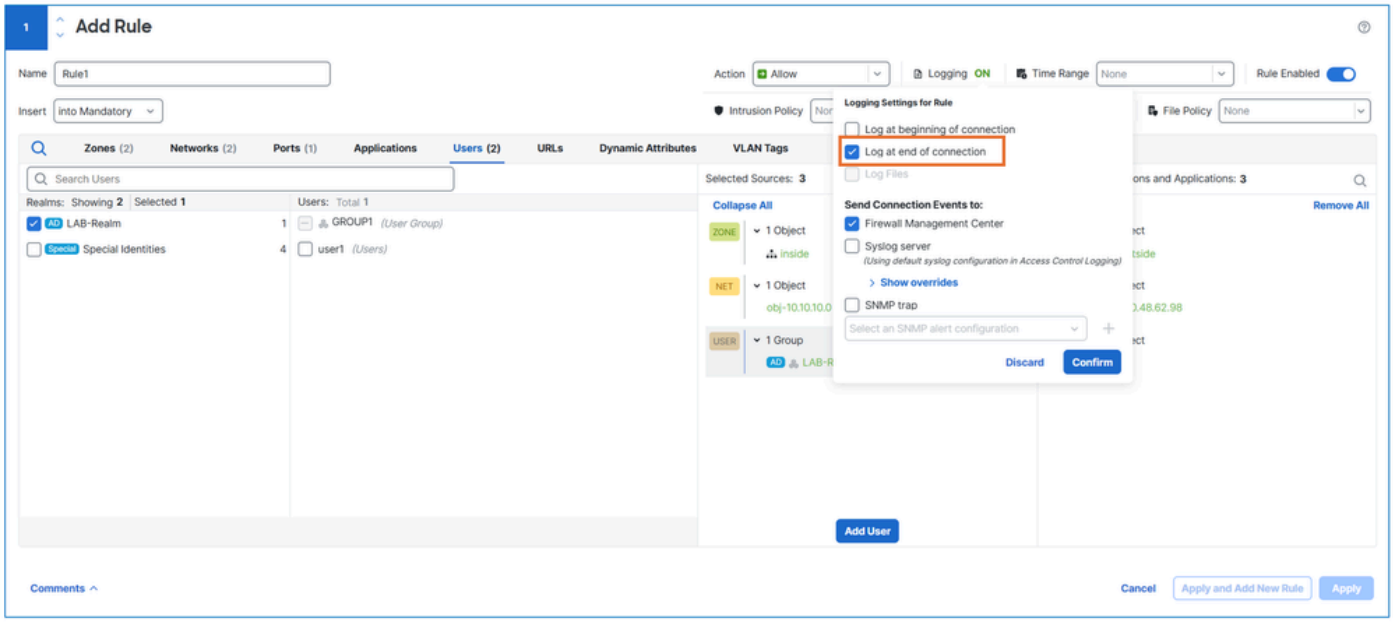
créer ACP

Entrez les détails en fonction des exigences de la tâche et, plus important encore, sous l'onglet Utilisateurs, addGROUP1fromLAB-Realm.



ajouter des utilisateurs à la règle

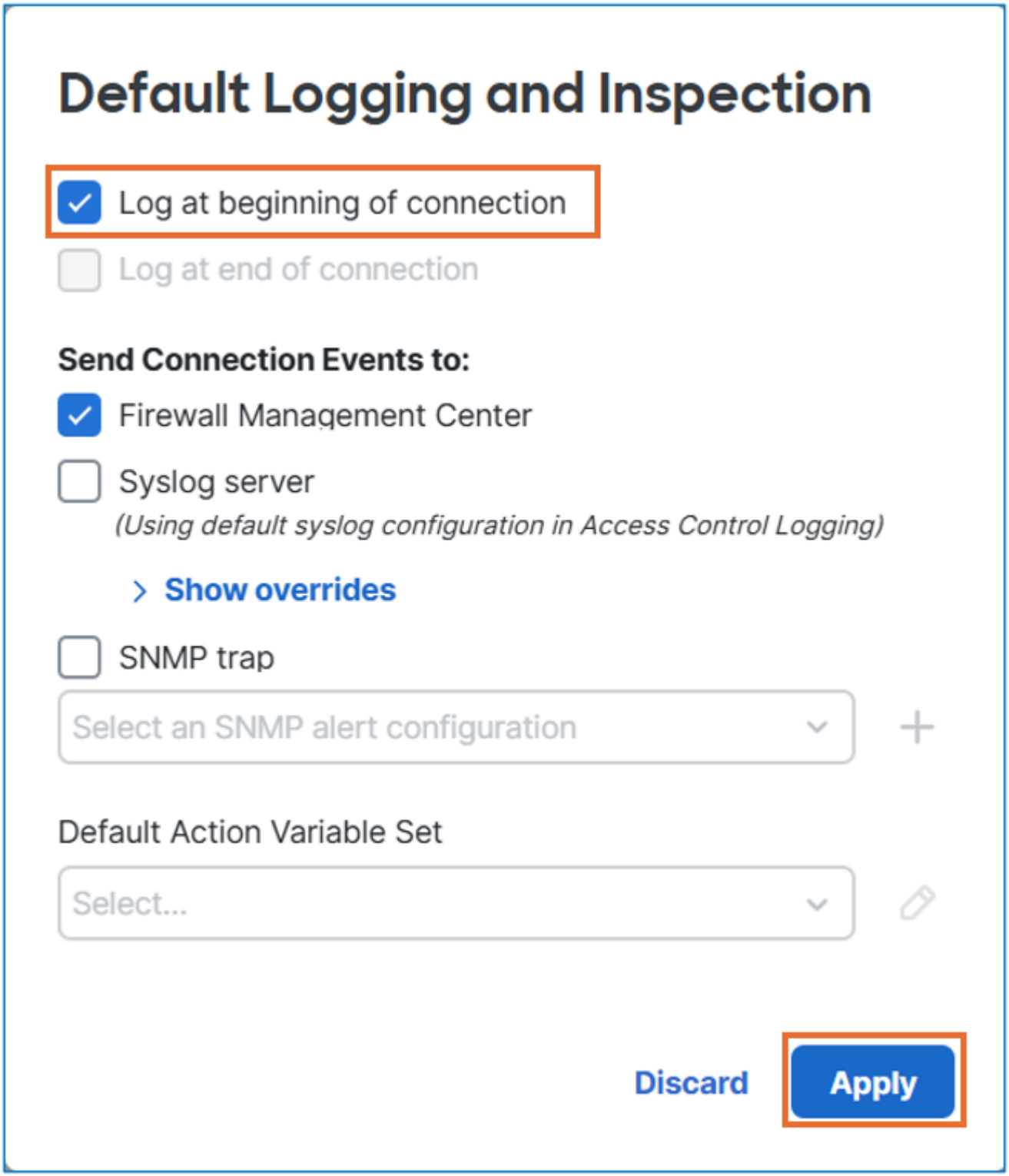
Activez la journalisation pour la règle en sélectionnant Log à la fin de la connexion.



activer la journalisation

Étape 3 : activation de la journalisation de l'action par défaut

Cliquez sur cette icône pour modifier les paramètres de consignation des actions par défaut.



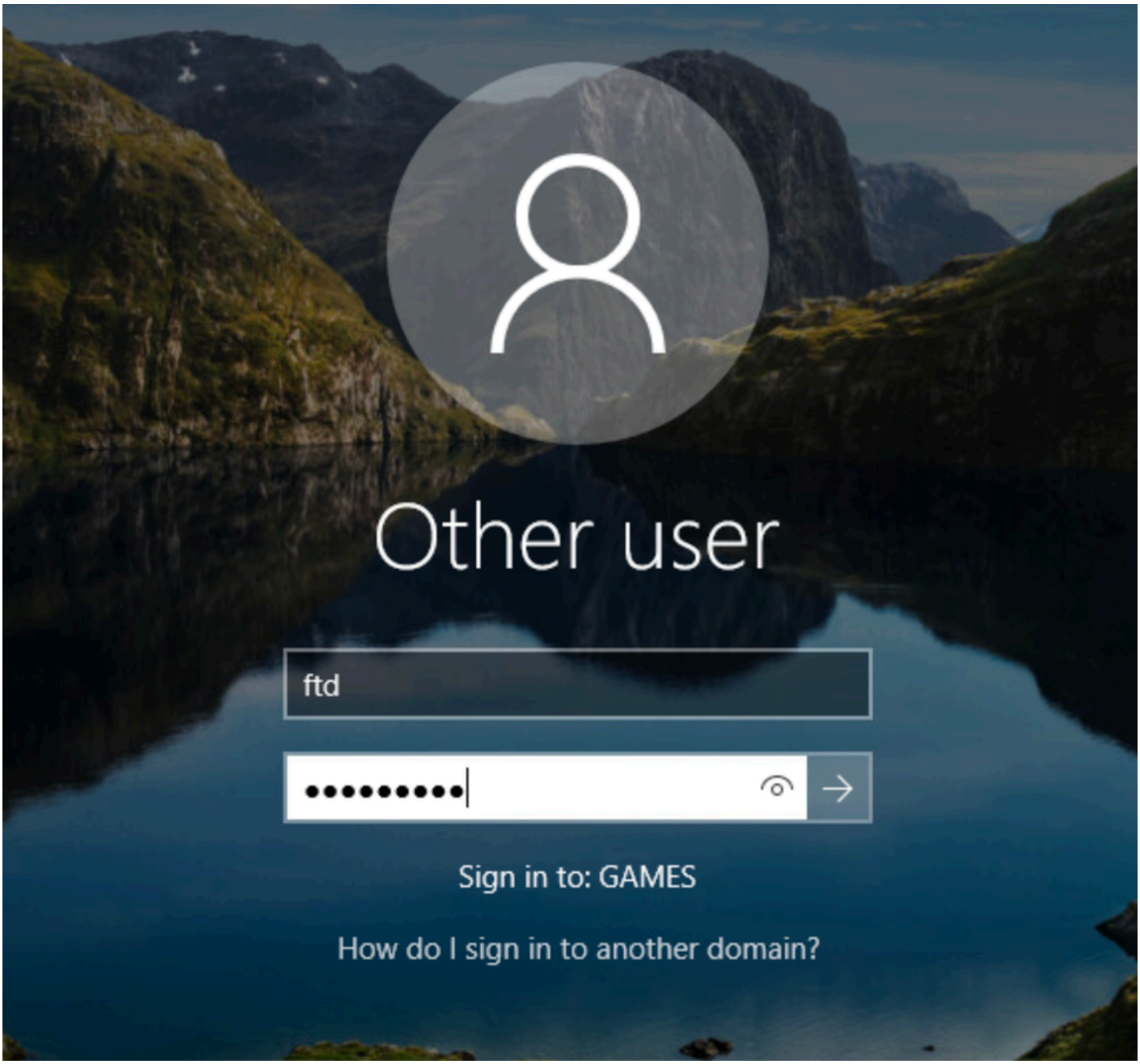
Activer la journalisation

Enregistrer et déployer la configuration sur le FTD.

Vérification

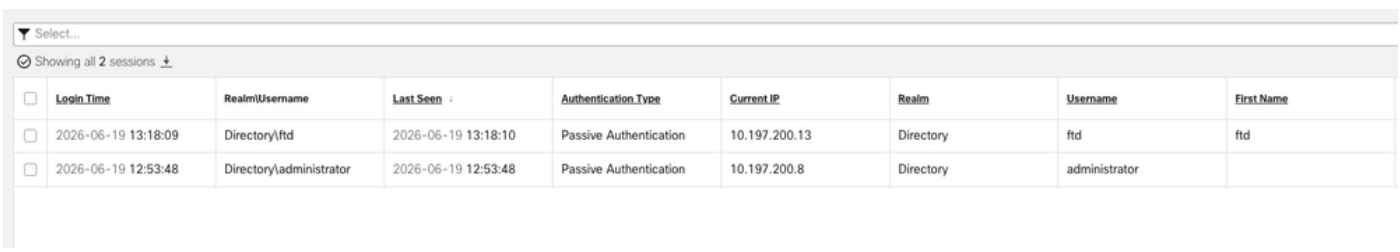
Vérifiez l'opération d'identité passive en confirmant que le trafic est autorisé exclusivement pour ftd.

Connectez-vous à l'utilisateur du domaine à partir de l'ordinateur utilisateur.



login utilisateur

Une fois qu'un utilisateur s'est connecté avec succès, vérifiez à partir de FMC sous Analysis> user >active session pour afficher les détails de l'utilisateur actif.



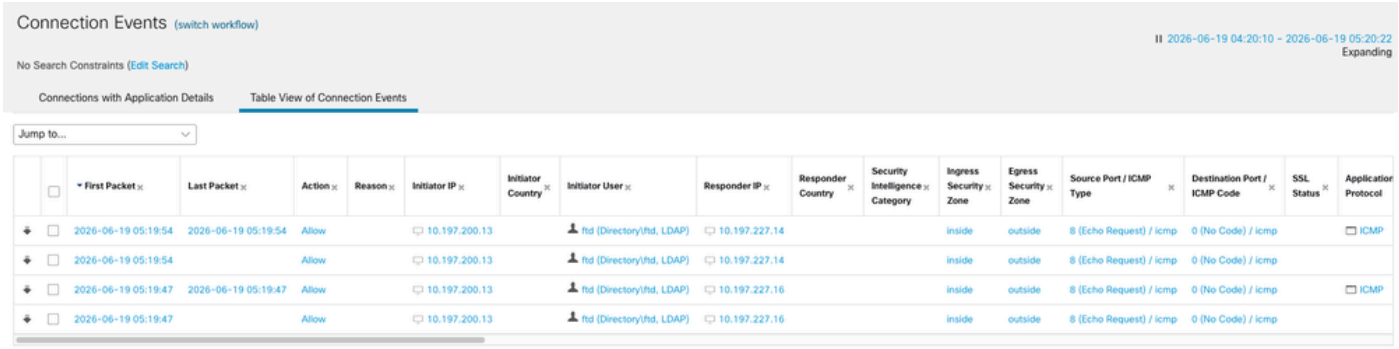
Select...

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	

Sessions actives

Après avoir initié une vérification du trafic à partir des événements de connexion, consultez les détails de l'utilisateur dans les événements de connexion.

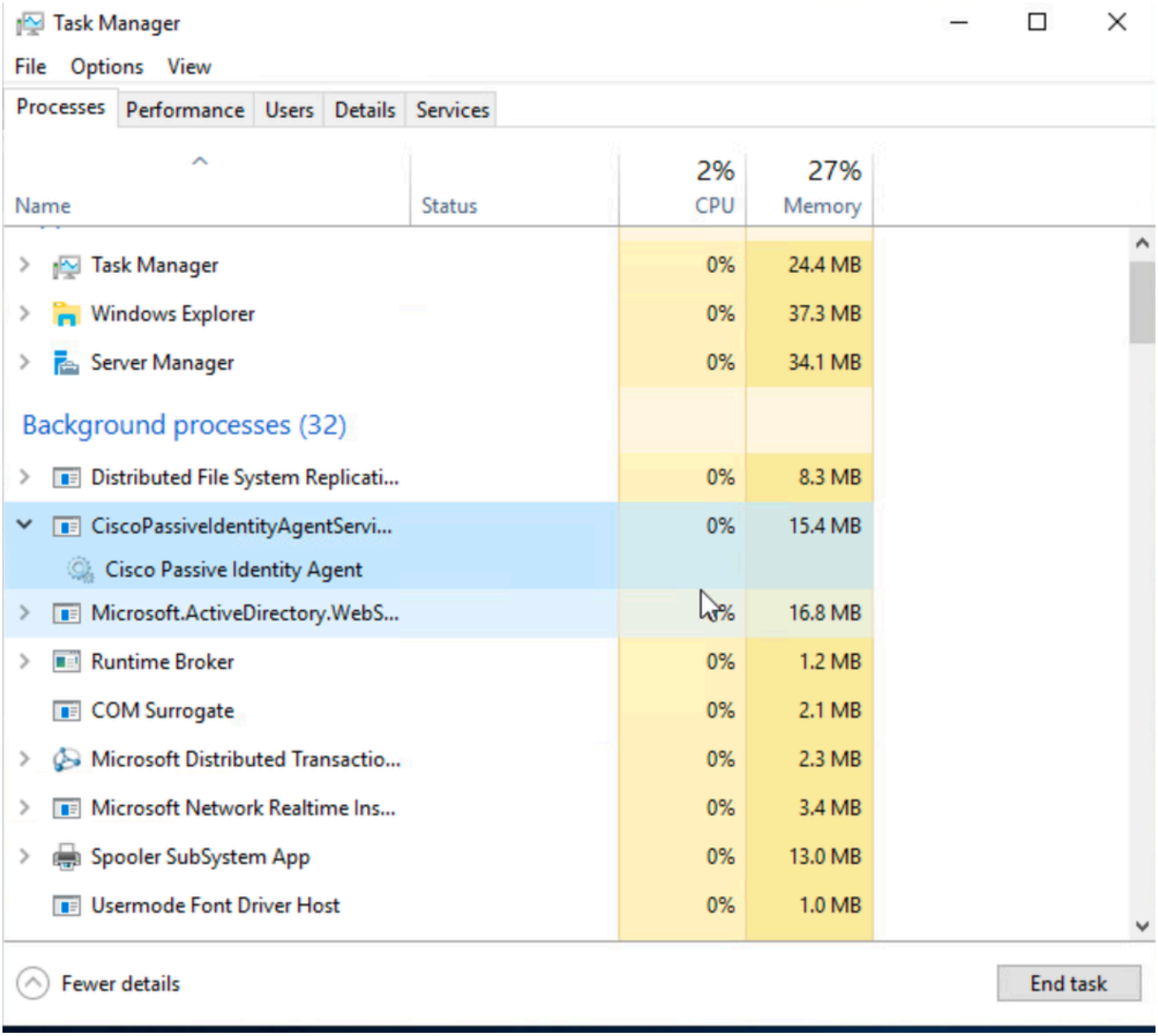


Sessions actives

Dépannage

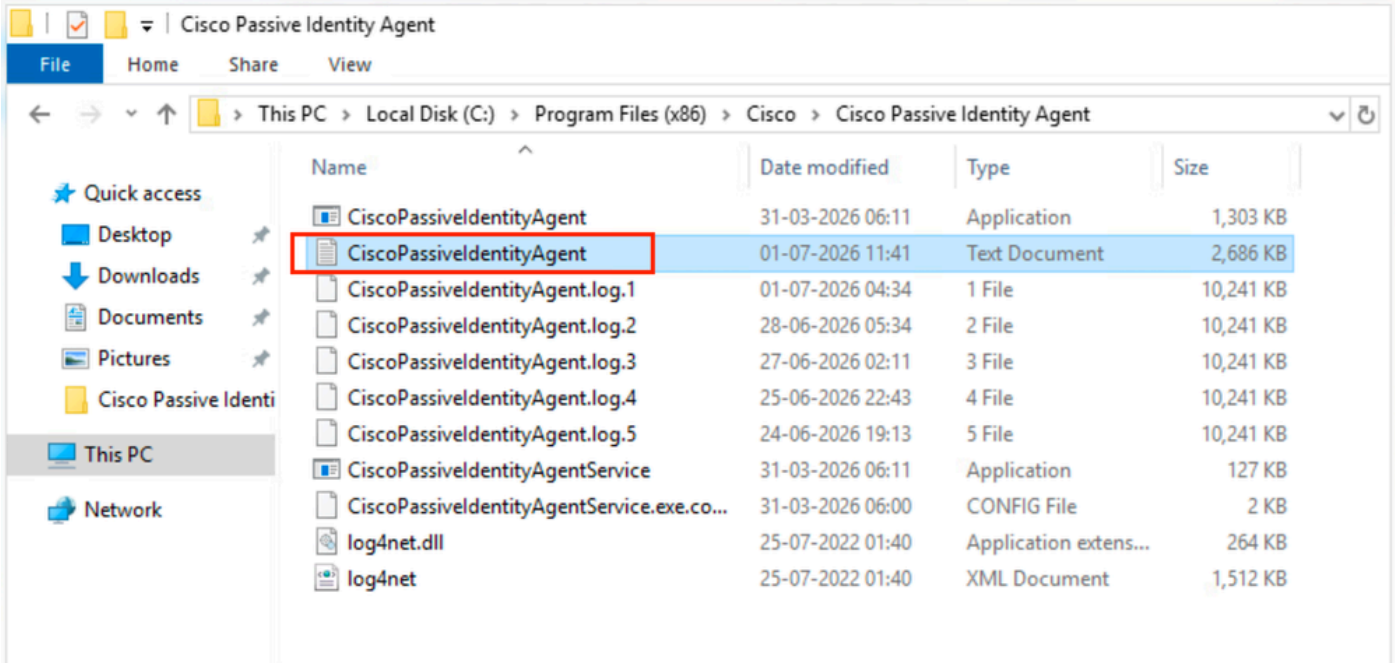
Vérification des journaux des agents

Sur l'ordinateur Windows hébergeant l'agent, ouvrez Task Manager et vérifiez que le processus en arrière-planCiscoPassiveIdentityAgentService est en cours d'exécution.



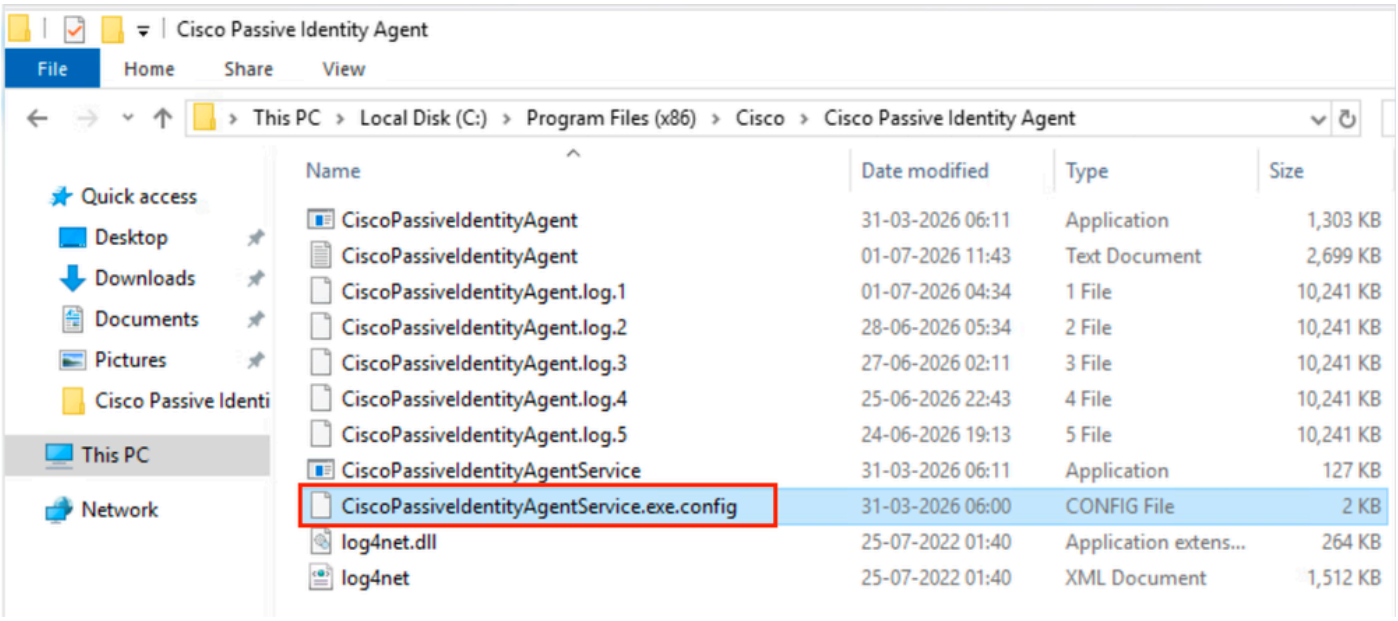
Tâche en cours

Les journaux de l'agent se trouvent dans les fichiers CiscoPassiveIdentityAgent, situés par défaut à l'adresse suivante : "C:\Program Fichiers (x86)\Cisco\Cisco Passive Identity Agent\".



préposé

Par défaut, les journaux de l'agent sont définis sur le niveauINFO. Pour activer la journalisation de niveau DEBUG, modifiez le fichierCiscoPassiveIdentityAgentService.exe.configfile et définissez le niveau de journalisation sur ALLouDEBUG.



configuration de l'agent

journal d'information

Vérification des journaux des agents - Récupérer la configuration des agents.

INFO Rest Client, Bulk Events : [f"domain":"games.cisco.com", "srcIpAddress": "X.X.X.X", "utilisateur" : "fdm", "timestamp" : "01/07/2026

INFO Rest Client, état du mappage : OK

INFO Rest Client, REST post successful for userBatch fdm, latency = 0, current DC TIME in UTC : 01/07/2026 19:47:34 UTILISATEUR connecté

INFO Rest Client, Demande de configuration de l'agent

Journaux FMC

Exécutez cette commande pour vérifier si le mappage utilisateur-IP a été reçu de l'agent.

```
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#
```

sortie fmc

Si la commande précédente n'affiche aucun mappage, collectez ces journaux et contactez le centre d'assistance technique Cisco.

Il s’agit d’une liste de journaux pertinents pour l’API FMC. La grue de quenouilles les englobe toutes.

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.