Déployer le module de sécurité d'itinérance AnyConnect Umbrella avec FMC

Table des matières

Introduction

Ce document décrit comment déployer le module de sécurité d'itinérance AnyConnect Umbrella à l'aide de Cisco Firewall Management Console (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès au tableau de bord Cisco Umbrella
- Accès à Cisco Firewall Management Console (FMC), version 6.7 ou ultérieure, car cette version ajoute la prise en charge de modules AnyConnect supplémentaires. Pour les versions antérieures à 6.7, FlexConfig peut être utilisé pour déployer le module, vous pouvez vous référer à la documentation Cisco pour plus de détails.
- Profil de module AnyConnect Umbrella (orginfo.json)
- La configuration VPN AnyConnect est déjà terminée et fonctionne sur le FMC/FTD

Composants utilisés

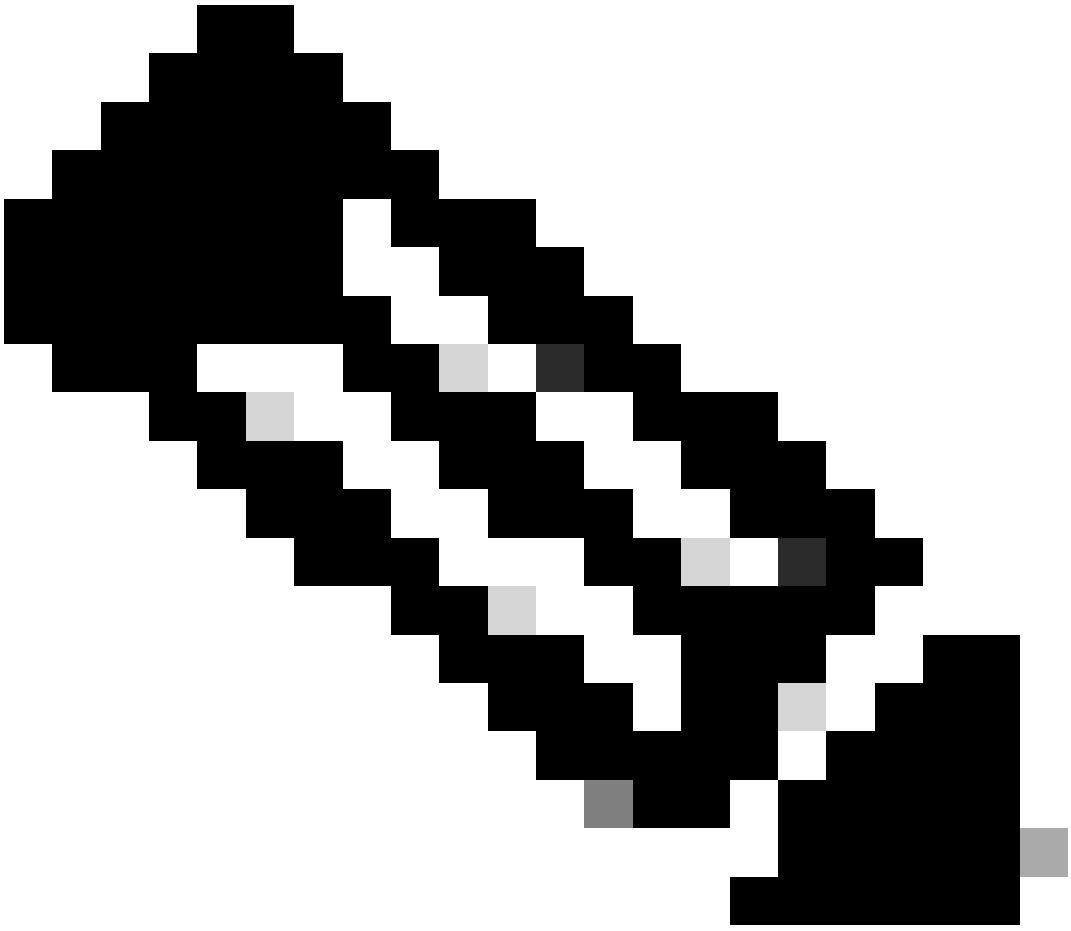
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Module de sécurité AnyConnect Umbrella Roaming
- Cisco Firewall Management Console (FMC) pour versions 6.7 ou ultérieures

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.

Aperçu



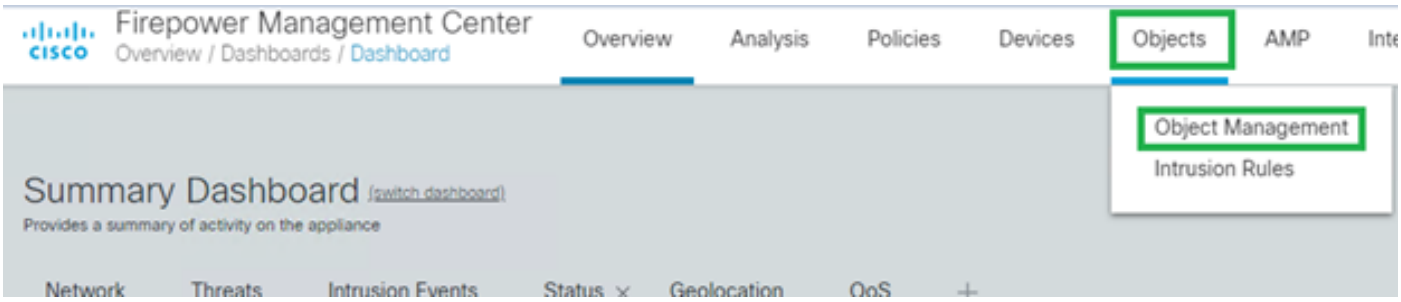
> Remarque : Cisco a annoncé la fin de vie de Cisco AnyConnect en 2023. Cisco a annoncé la fin de vie d'Umbrella Roaming Client le 2 avril 2024 et la dernière date d'assistance était le 2 avril 2025. De nombreux clients Cisco Umbrella bénéficient déjà de la migration vers Cisco Secure Client et nous vous encourageons à commencer la migration dès que possible pour bénéficier d'une meilleure expérience d'itinérance. Pour en savoir plus, lisez cet article de la Base de connaissances : Comment puis-je installer Cisco Secure Client avec le module Umbrella ?

Ce guide de configuration présente les étapes de mise en service du module de sécurité d'itinérance AnyConnect Umbrella via Cisco Firewall Management Console (FMC) pour les versions 6.7 ou ultérieures.

Installation et téléchargement du module AnyConnect Umbrella à partir du FMC :

Suivez ces étapes pour activer l'installation/le téléchargement du module AnyConnect Umbrella à partir du FMC :

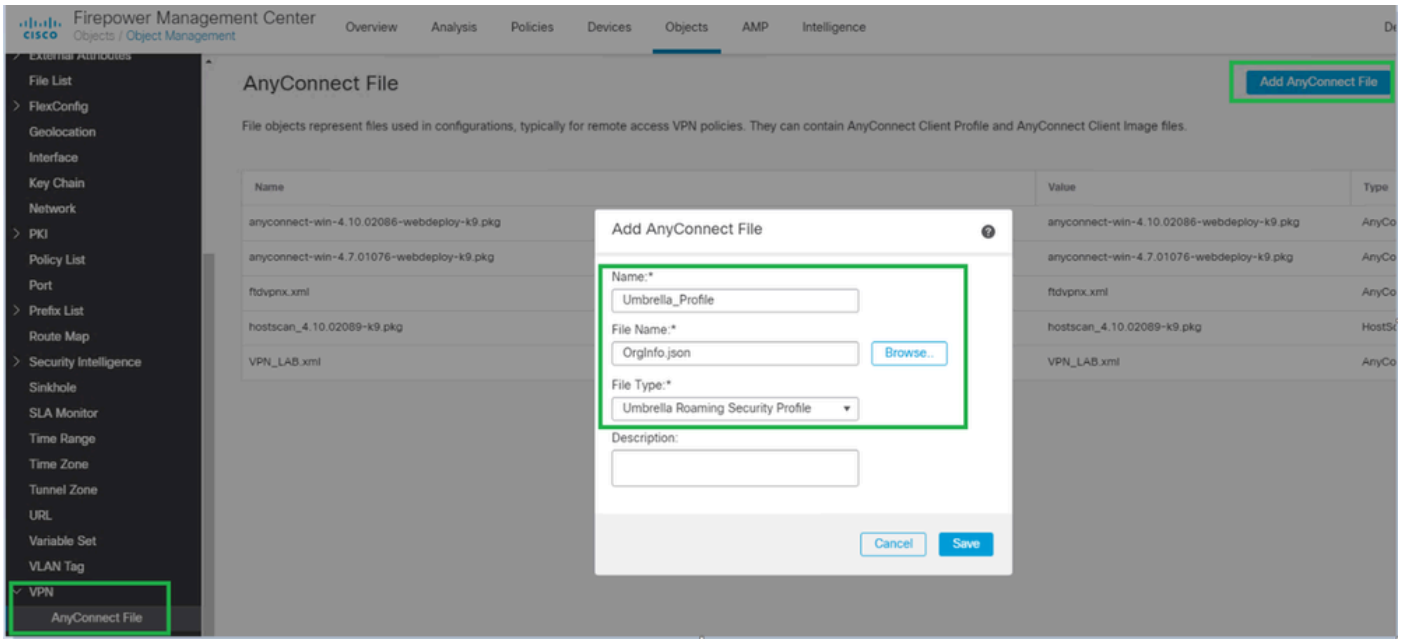
1. Accédez à Objets > Gestion des objets :



8178144512532

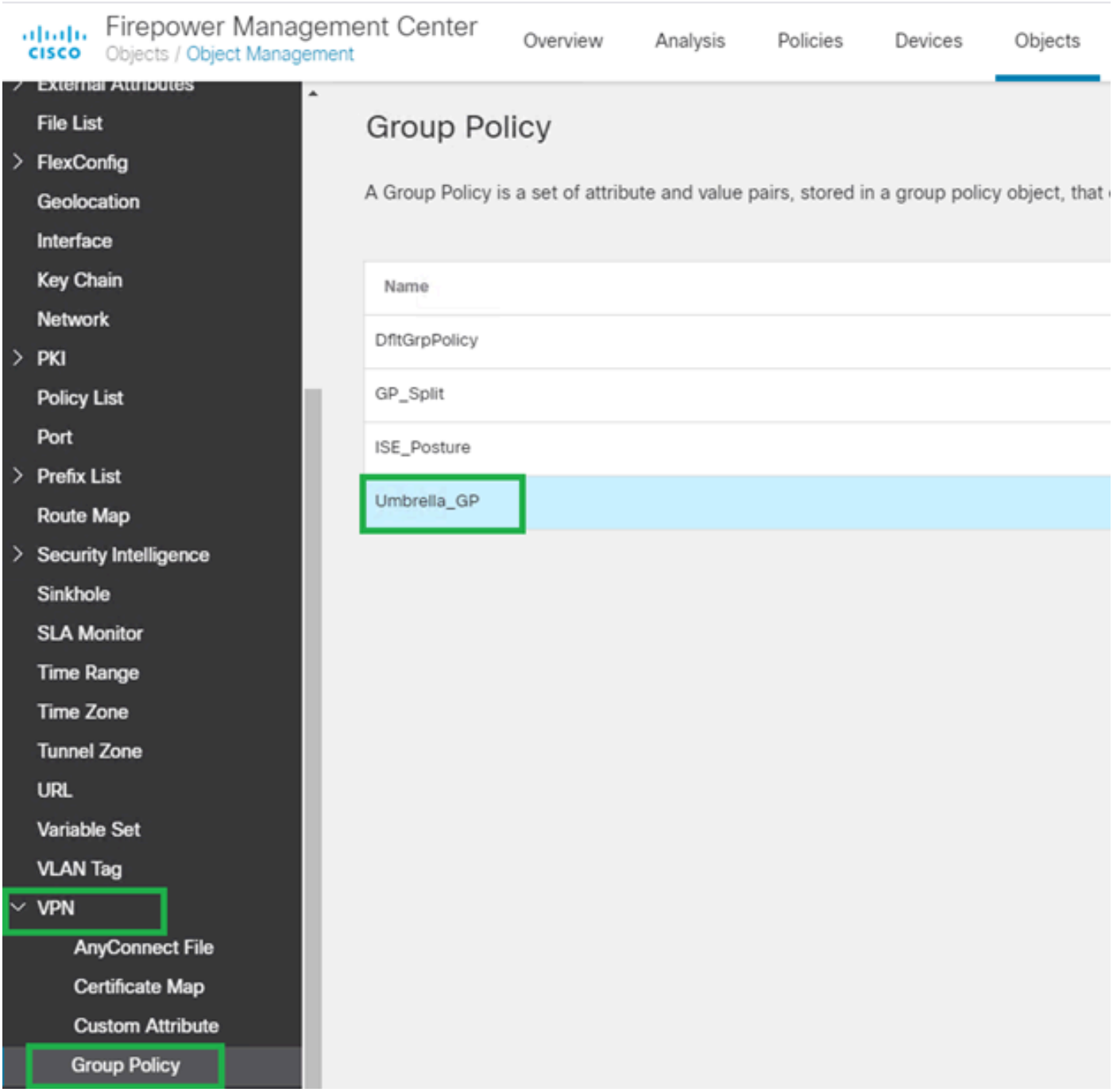
2. Accédez à VPN > AnyConnect File > Add AnyConnect File. Définissez un nom pour le profil (significatif localement).

- Recherchez le fichier JSON téléchargé à partir de votre tableau de bord Cisco Umbrella.
- Sous Type de fichier, sélectionnez Umbrella Roaming Security Profile, puis Enregistrer.



8178144531860

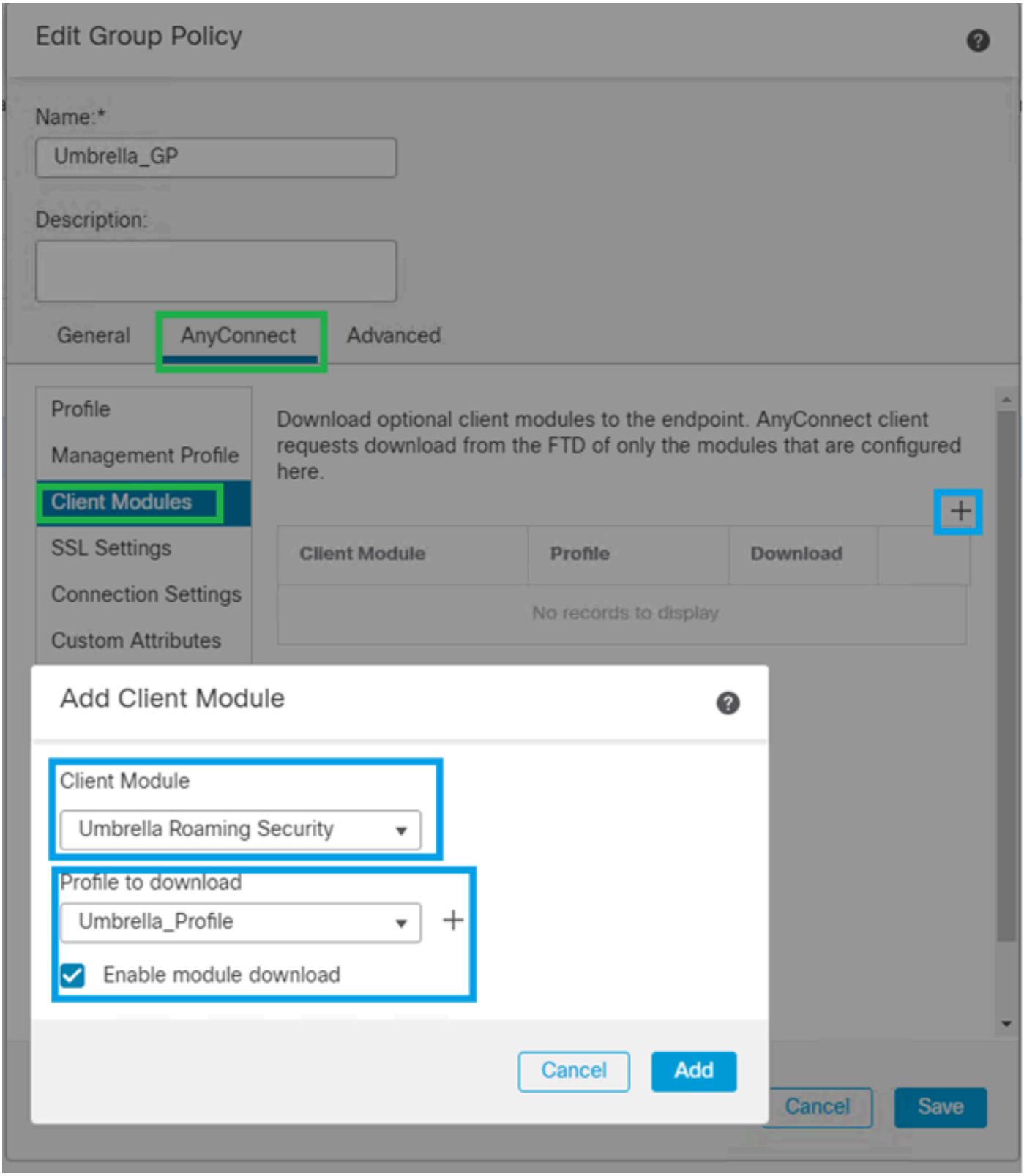
3. Une fois là, sélectionnez Group Policy, puis sélectionnez la stratégie de groupe que vous utilisez pour déployer Umbrella ("Umbrella_GP" dans ce cas) :



8178147609492

4. Sélectionnez AnyConnect > Client Modules > Add Client Module.

- Sous Client Module, sélectionnez Umbrella Roaming Client, puis Profile pour télécharger le profil que nous avons défini à l'étape 2.
- Assurez-vous que le module Enabled download est sélectionné afin que les utilisateurs se connectant via AnyConnect puissent télécharger automatiquement le profil Umbrella JSON.



8178147636628

Facultatif: Authentification locale VPN (FMC 7.0 ou ultérieure requise)

Si vous souhaitez tester un profil distinct avec l'authentification locale sur le FMC/FTD, vous pouvez effectuer les étapes suivantes (FMC 7.0 ou version ultérieure est requis) :

1. Créez un domaine local.

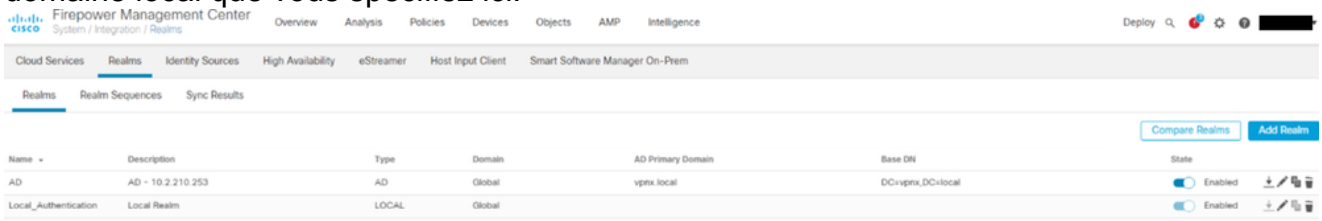
- Les noms d'utilisateur et mots de passe locaux sont stockés dans les domaines locaux.
- Lorsque vous créez un domaine (**Système > Intégration > Domaines**) et sélectionnez le nouveau type de domaine **LOCAL**, le système vous invite à ajouter un ou plusieurs utilisateurs locaux.

2. Configurez le VPN RA pour utiliser l'authentification locale.

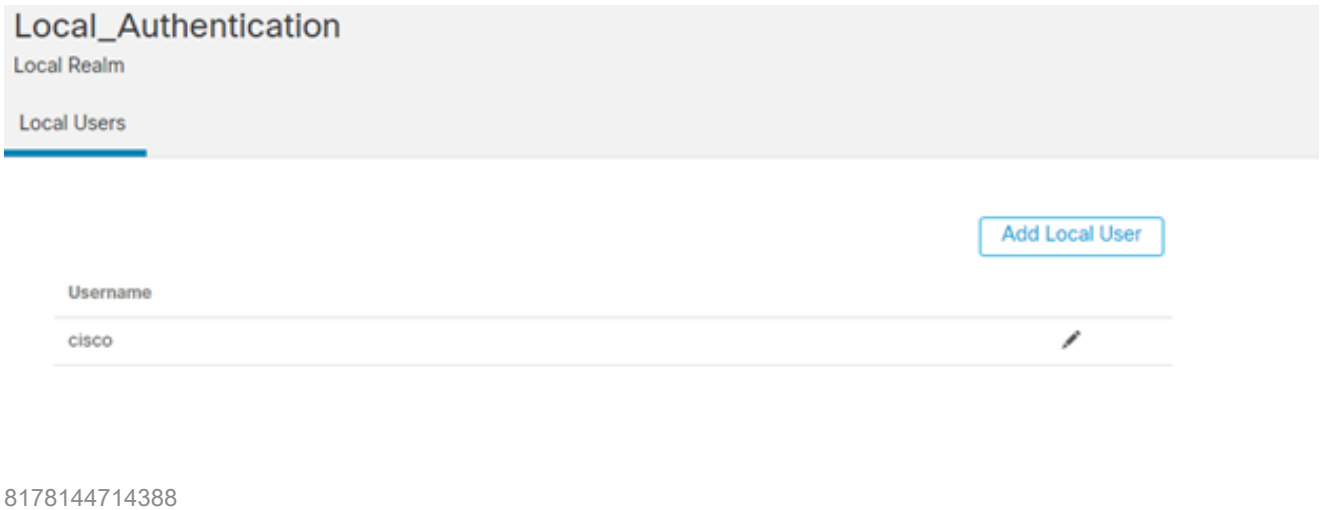
- Créez ou modifiez une stratégie VPN RA (**Périphériques > VPN > Accès à distance**).
- Créez un profil de connexion dans cette stratégie.
- Spécifiez **LOCAL** comme serveur d'authentification principal, secondaire ou de secours dans ce profil de connexion.

3. Associez le domaine local que vous avez créé à une stratégie VPN RA.

- Dans l'éditeur de stratégie VPN RA, utilisez le nouveau paramètre **Local Realm**. Chaque profil de connexion de la stratégie VPN RA qui utilise l'authentification locale peut utiliser le domaine local que vous spécifiez ici.



8178273923732



8178144714388

Additional Information

[Notes de version de Cisco Firewall (anciennement Firepower), version 7.0.x]

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.