Configuration du client sécurisé SSL avec authentification locale sur FTD

Table des matières

Introduction

Ce document décrit comment configurer Cisco Secure Client (y compris Anyconnect) avec l'authentification locale sur Cisco FTD géré par Cisco FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration du client sécurisé SSL via Firepower Management Center (FMC)
- Configuration des objets Firepower via FMC
- Certificats SSL sur Firepower

Composants utilisés

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

- Cisco Firepower Threat Defense (FTD) version 7.0.0 (build 94)
- Cisco FMC version 7.0.0 (build 94)
- Client Cisco Secure Mobility 4.10.01075

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.

Informations générales

Dans cet exemple, SSL (Secure Sockets Layer) est utilisé pour créer un réseau privé virtuel (VPN) entre FTD et un client Windows 10.

À partir de la version 7.0.0, FTD géré par FMC prend en charge l'authentification locale pour les clients sécurisés Cisco. Cette méthode peut être définie comme méthode d'authentification principale ou comme méthode de secours en cas d'échec de la méthode principale. Dans cet exemple, l'authentification locale est configurée comme authentification principale.

Avant cette version logicielle, l'authentification locale du client sécurisé Cisco sur FTD était uniquement disponible sur Cisco Firepower Device Manager (FDM).

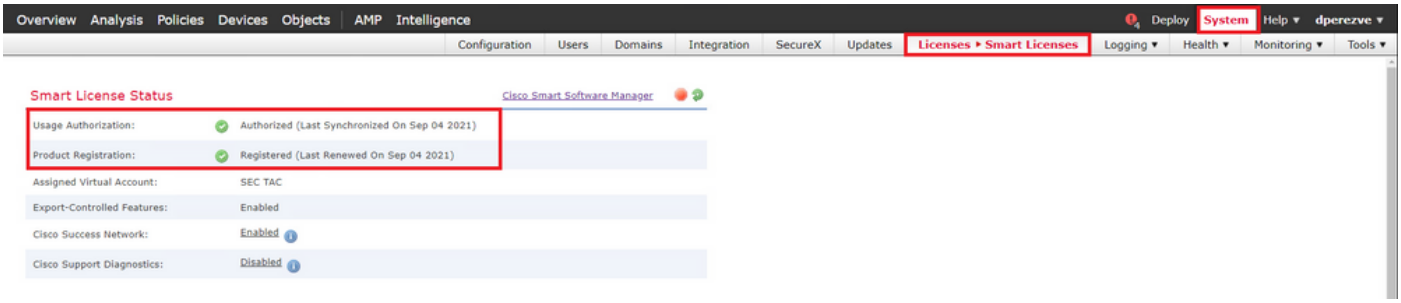
Configurer

Configurations

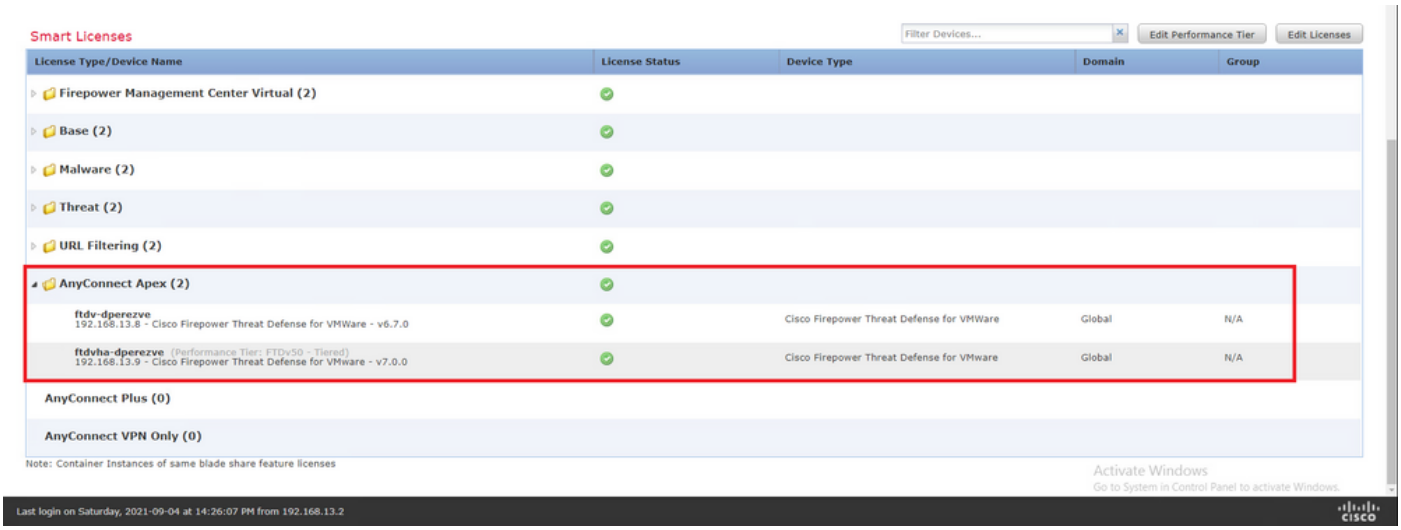
Étape 1. Vérifier les licences

Avant de configurer Cisco Secure Client, le FMC doit être enregistré et conforme au portail de gestion des licences Smart. Vous ne pouvez pas déployer Cisco Secure Client si FTD ne possède pas de licence Plus, Apex ou VPN Only valide.

Accédez à System > Licenses > Smart Licenses afin de valider que le FMC est enregistré et conforme à Smart Licensing Portal.



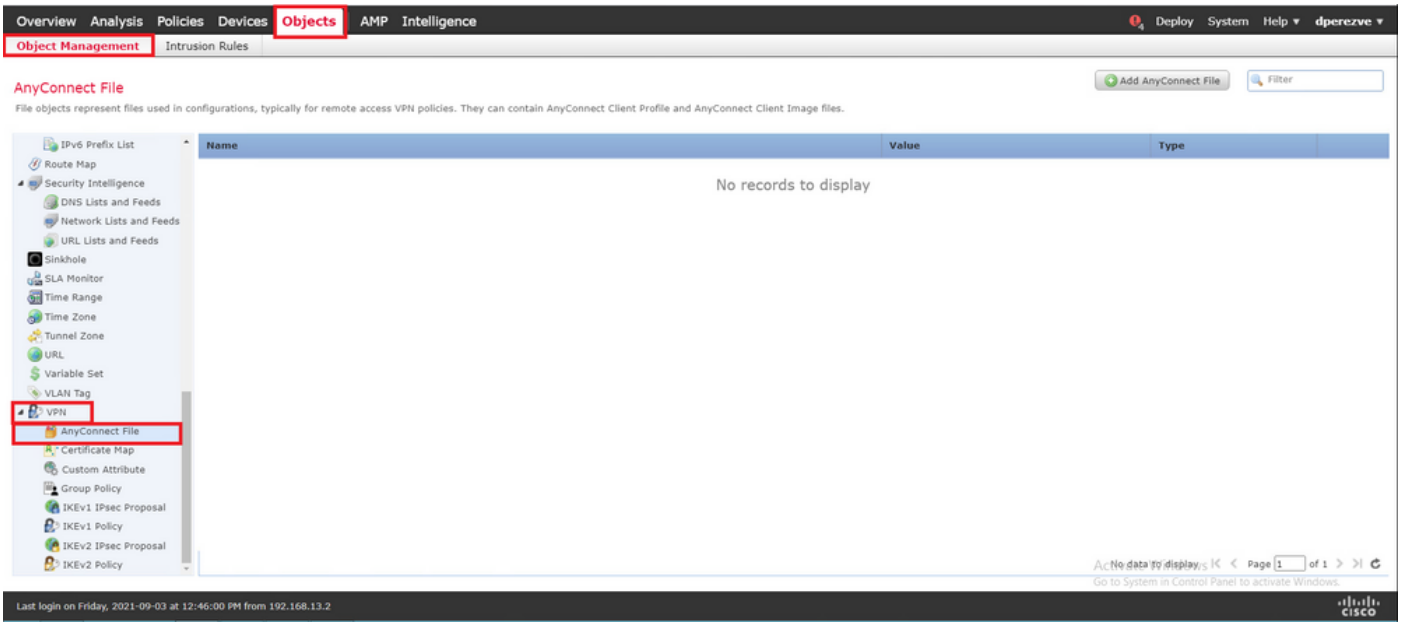
Dans la même page, au bas du tableau Licences Smart, vous pouvez voir les différents types de licences Cisco Secure Client (AnyConnect) disponibles et les périphériques abonnés à chacune d'elles. Valider le FTD disponible est enregistré dans l'une de ces catégories.



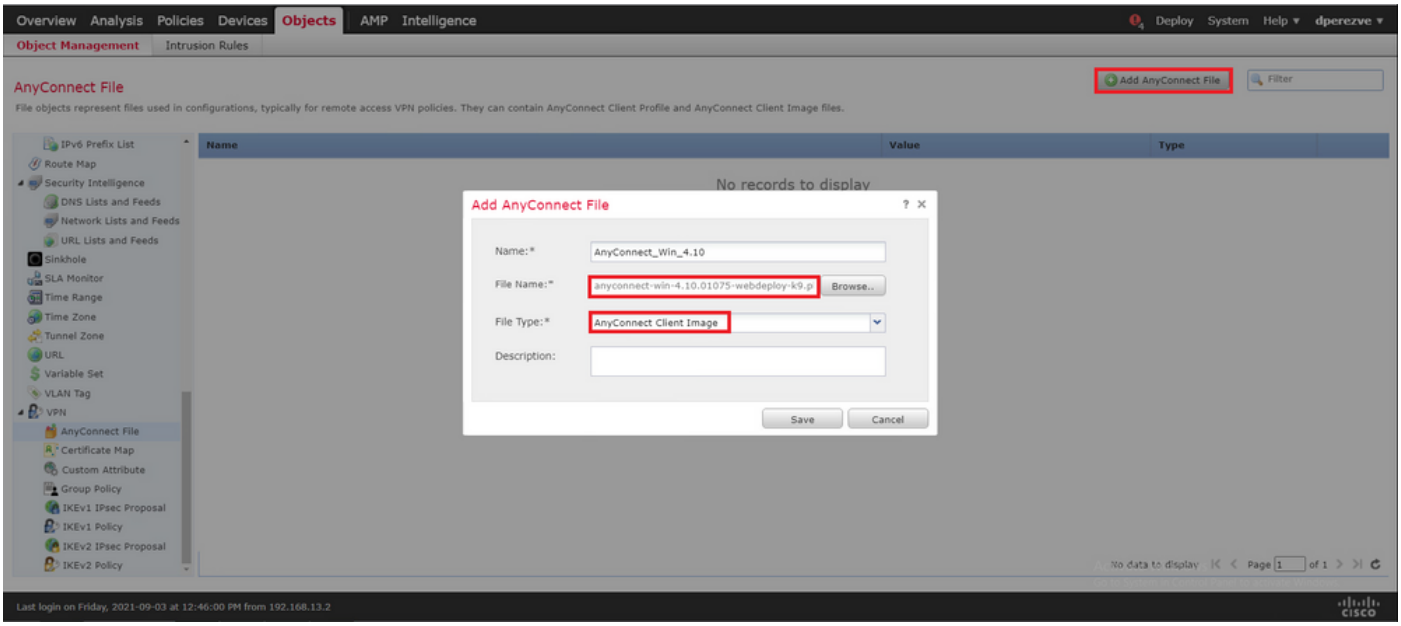
Étape 2. Télécharger le package Cisco Secure Client vers FMC

Téléchargez le package de déploiement de tête de réseau Cisco Secure Client (AnyConnect) pour Windows depuis le site cisco.com.

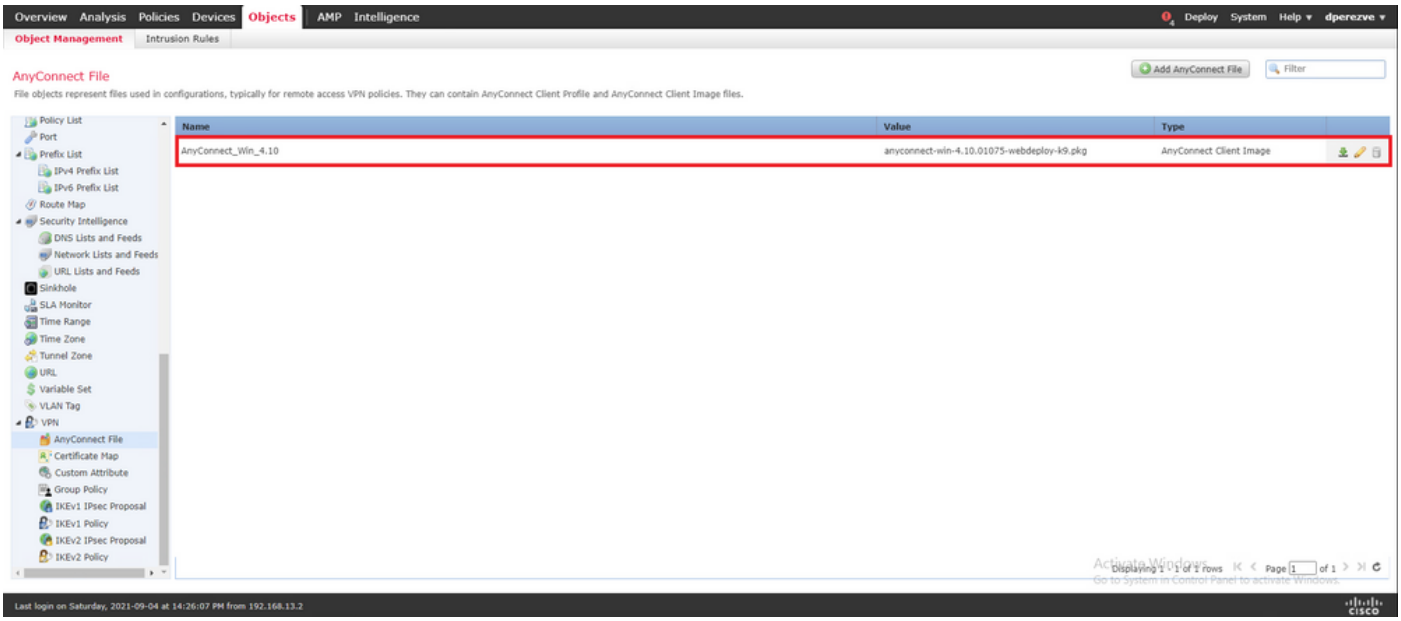
Afin de télécharger l'image de Cisco Secure Client, naviguez vers Objects > Object Management et choisissez Cisco Secure Client File sous la catégorie VPN dans la table des matières.



Cliquez sur le bouton Ajouter un fichier AnyConnect. Dans la fenêtre Add AnyConnect Secure Client File, attribuez un nom à l'objet, puis choisissez Browse.. afin de choisir le package Cisco Secure Client et enfin choisissez AnyConnect Client Image comme type de fichier dans le menu déroulant.



Cliquez sur le bouton Enregistrer. L'objet doit être ajouté à la liste des objets.



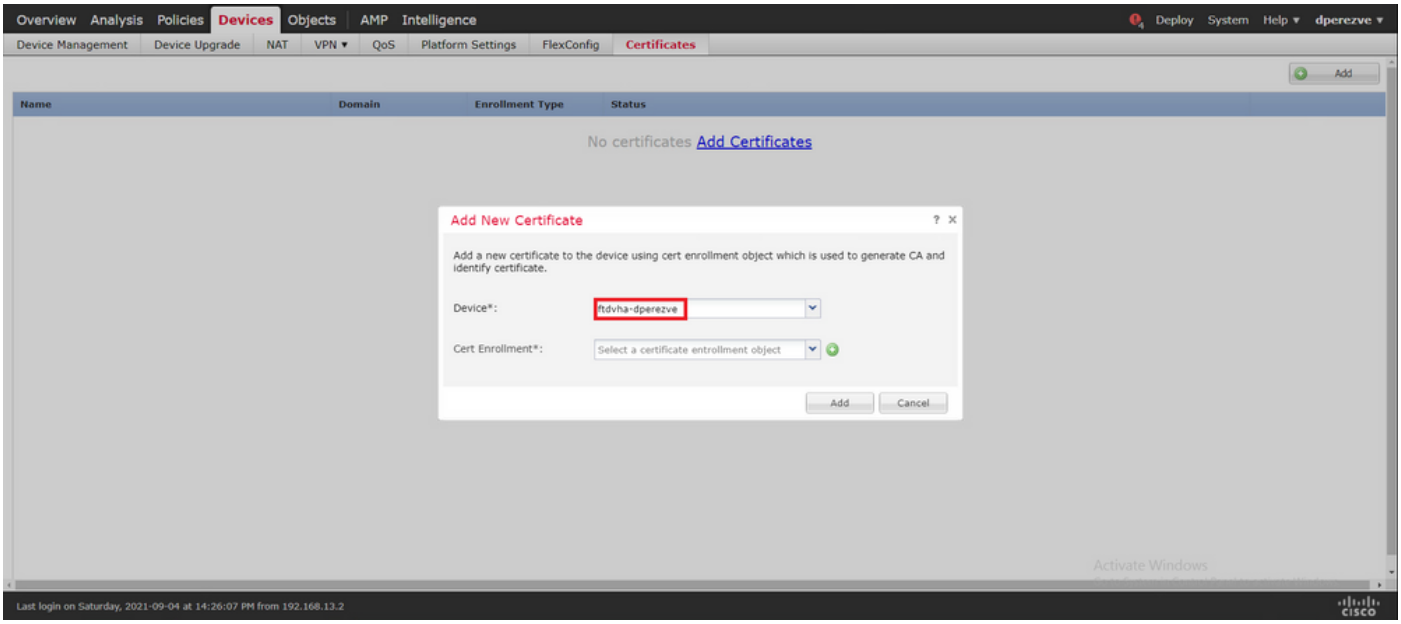
Étape 3. Générer un certificat auto-signé

SSL Cisco Secure Client (AnyConnect) nécessite l'utilisation d'un certificat valide dans la connexion SSL entre la tête de réseau VPN et le client.

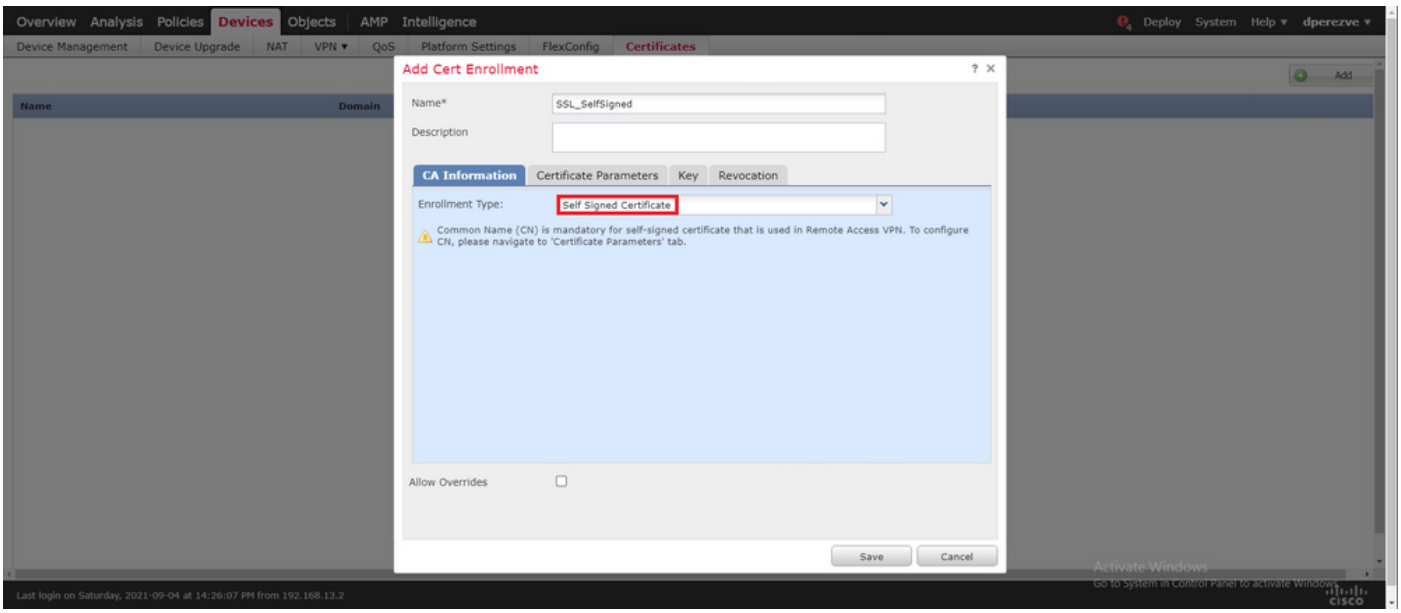
Remarque : dans cet exemple, un certificat auto-signé est généré à cette fin. Cependant, en plus des certificats auto-signés, il est possible de télécharger un certificat signé par une autorité de certification interne ou par une autorité de certification bien connue.

Afin de créer le certificat auto-signé naviguez à Périphériques > Certificats.

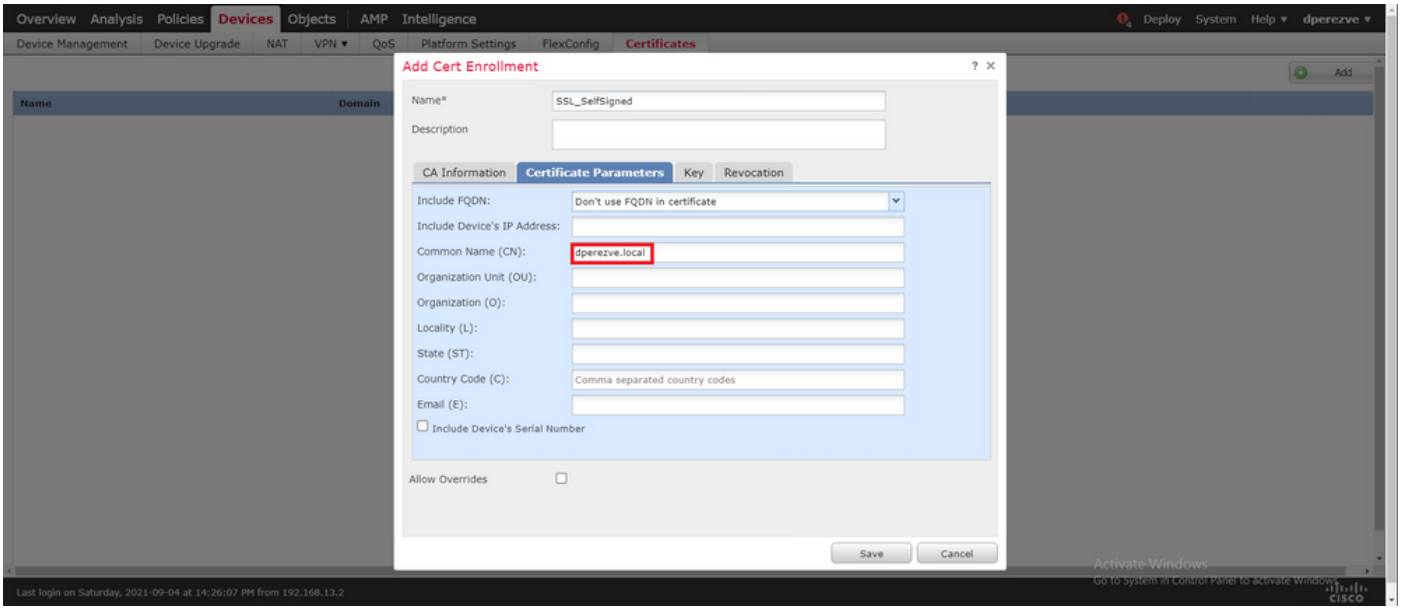
Cliquez sur le bouton Ajouter. Ensuite, choisissez le FTD disponible dans le menu déroulant Device de la fenêtre Add New Certificate.



Cliquez sur le bouton Add Cert Enrollment (vert + symbole) pour créer un nouvel objet d'inscription. À présent, dans la fenêtre Ajouter une inscription de certificat, attribuez un nom à l'objet et choisissez Certificat auto-signé dans le menu déroulant Type d'inscription.



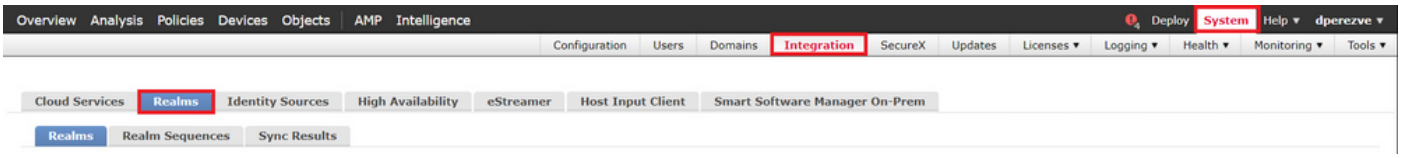
Enfin, pour les certificats auto-signés, il est obligatoire d'avoir un nom commun (NC). Accédez à l'onglet Certificate Parameters afin de définir un CN.



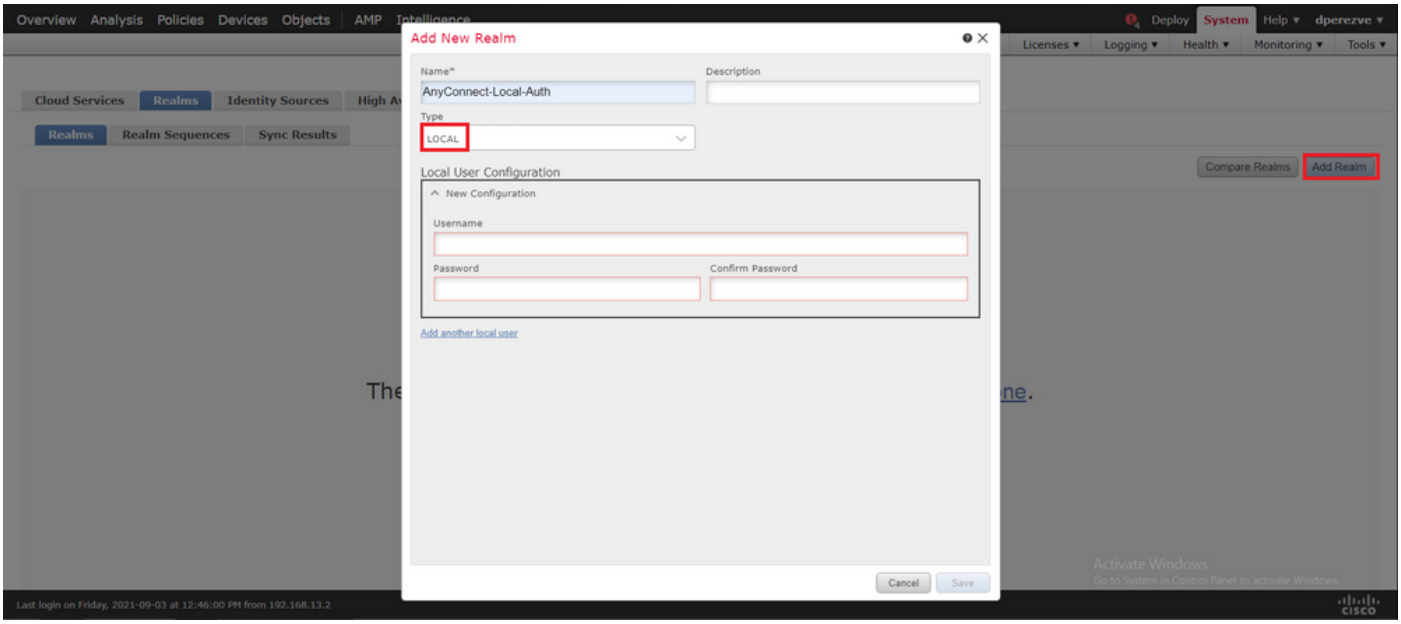
Choisissez Save and Add button. Après quelques secondes, le nouveau certificat doit être ajouté à la liste des certificats.

Étape 4. Créer un domaine local sur FMC

La base de données d'utilisateur locale et les mots de passe respectifs sont stockés dans un domaine local. Pour créer le domaine local, accédez à Système > Intégration > Domaines.

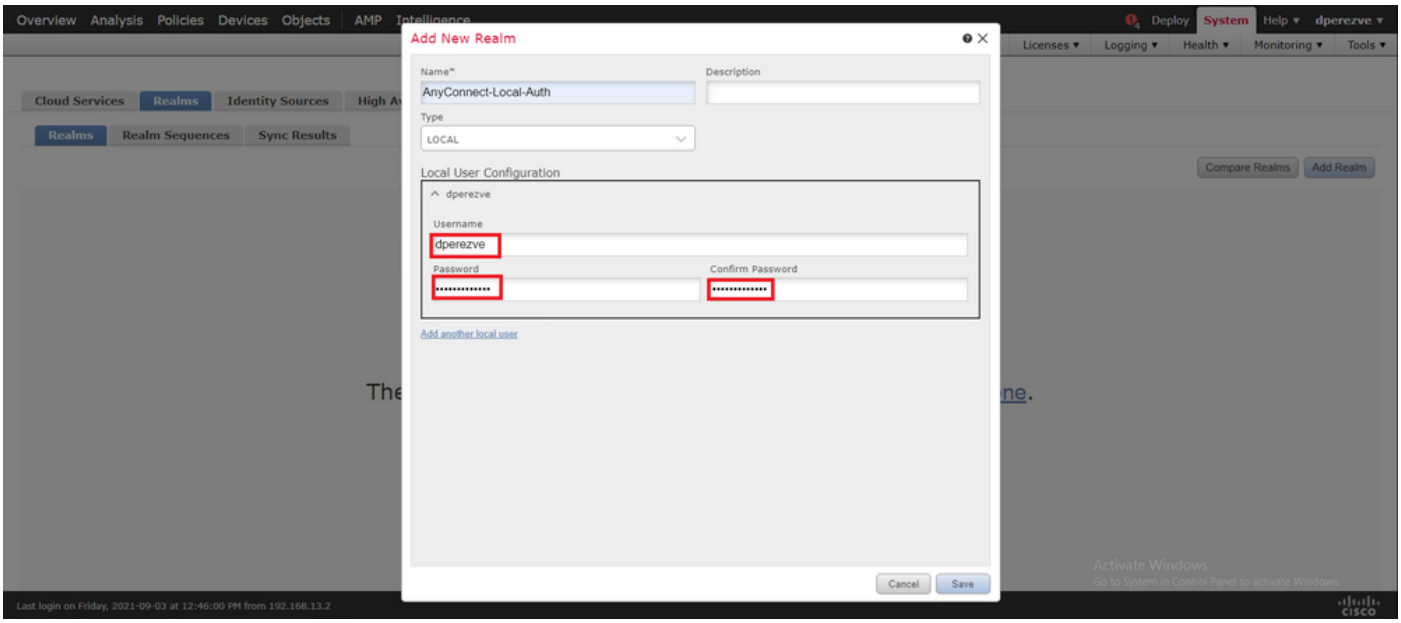


Cliquez sur le bouton Ajouter un domaine. Dans la fenêtre Ajouter un nouveau domaine, attribuez un nom et choisissez l'option LOCAL dans le menu déroulant Type.

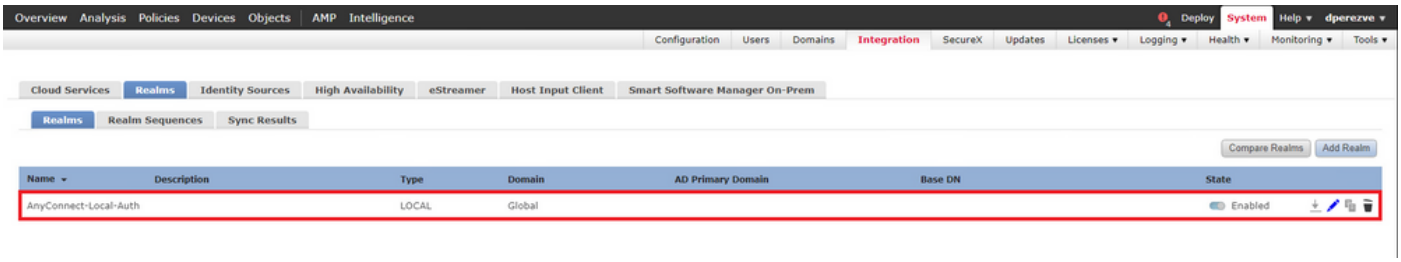


Les comptes d'utilisateurs et les mots de passe sont créés dans la section Configuration utilisateur locale.

Remarque : les mots de passe doivent comporter au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

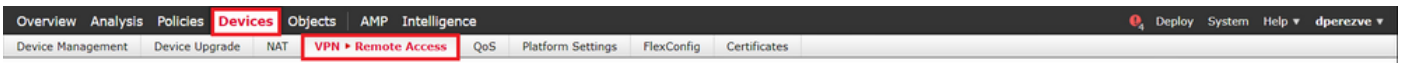


Enregistrez les modifications et ajoutez un nouveau domaine (realm) à la liste des domaines existants.

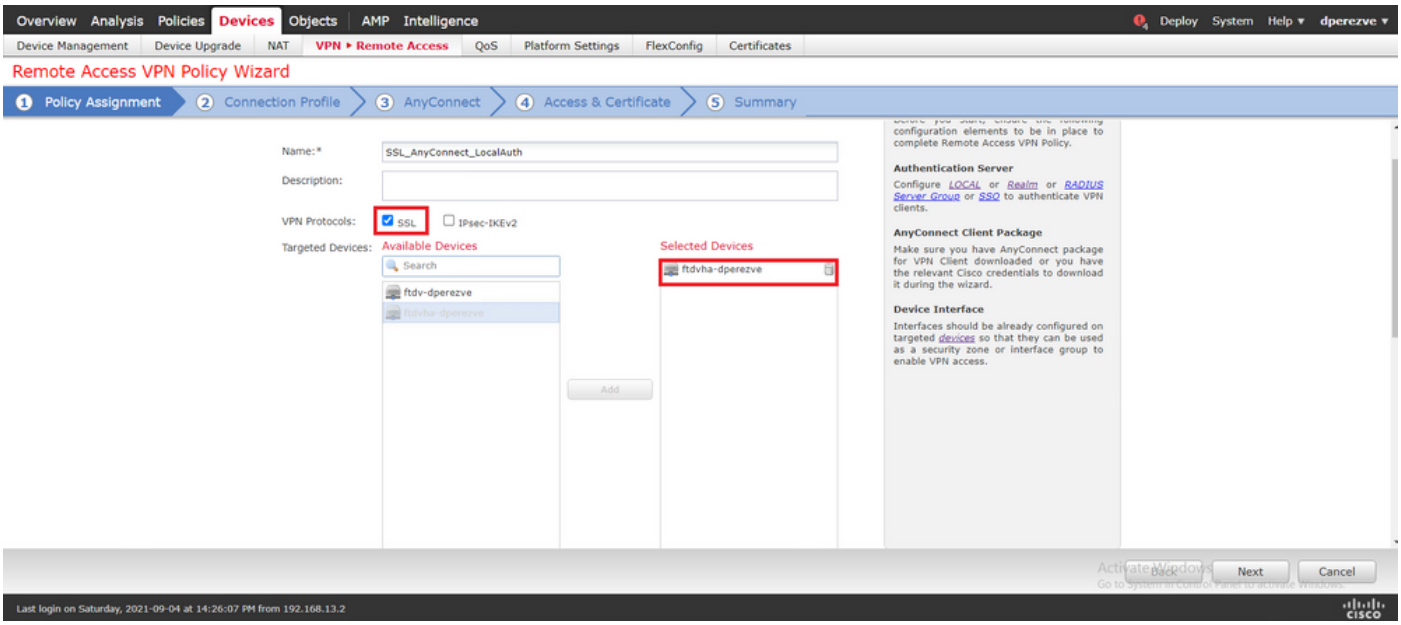


Étape 5. Configurer le client sécurisé Cisco SSL

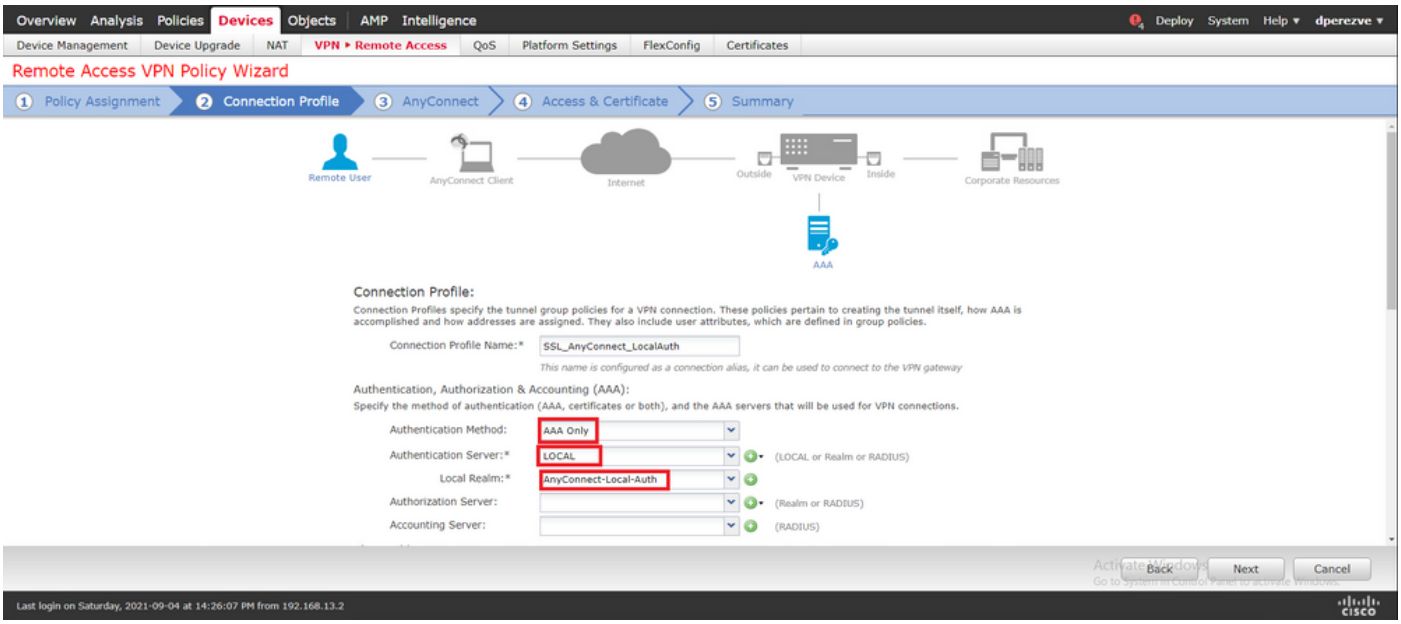
Afin de configurer SSL Cisco Secure Client, naviguez vers Devices > VPN > Remote Access.



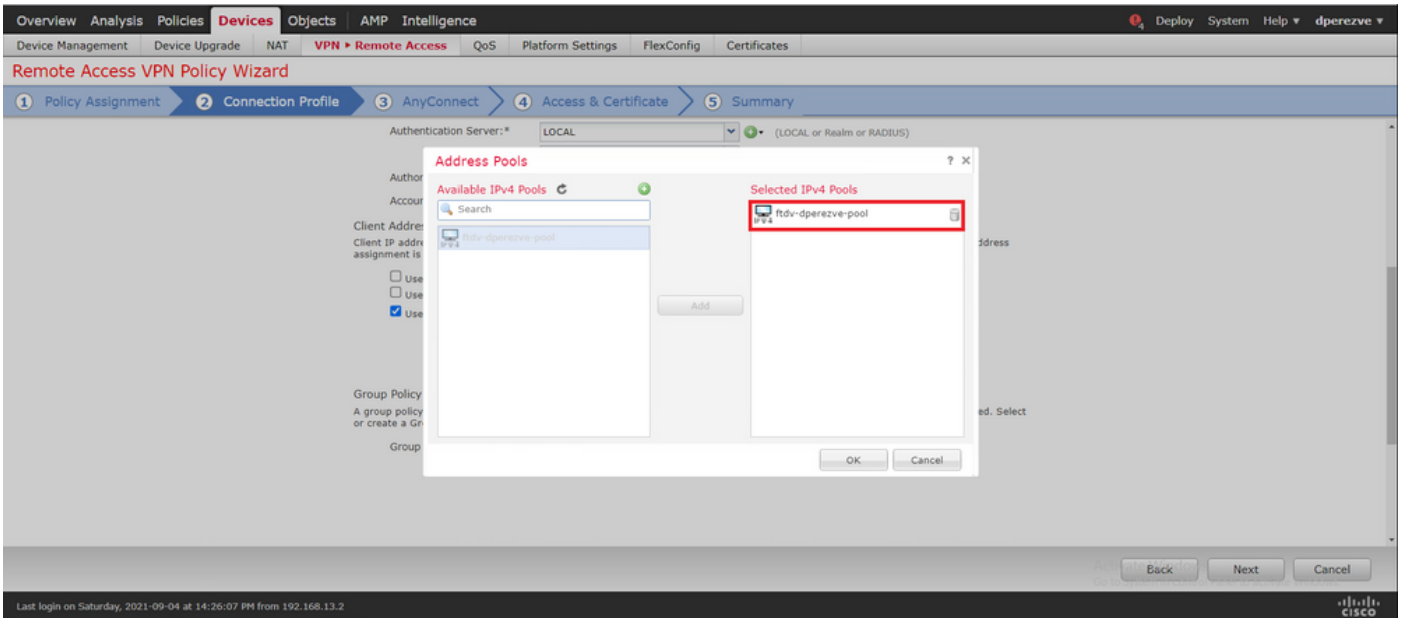
Cliquez sur le bouton Add afin de créer une nouvelle stratégie VPN. Définissez un nom pour le profil de connexion, cochez la case SSL et choisissez le FTD disponible comme périphérique cible. Tout doit être configuré dans la section Affectation de stratégie de l'Assistant Stratégie VPN d'accès à distance.



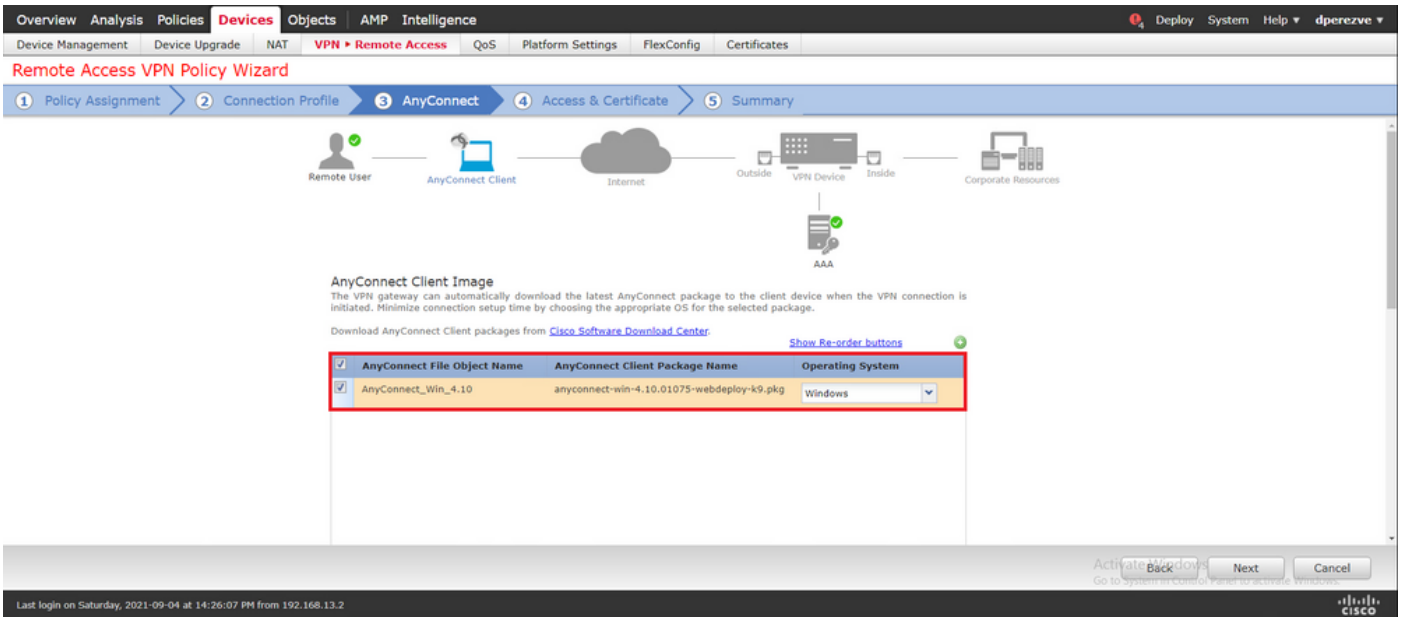
Choisissez Next afin de passer à la configuration Connection Profile. Définissez un nom pour le profil de connexion et choisissez AAA Only comme méthode d'authentification. Ensuite, dans le menu déroulant Authentication Server, choisissez LOCAL, et enfin, choisissez le domaine local créé à l'étape 4 dans le menu déroulant Local Realm.



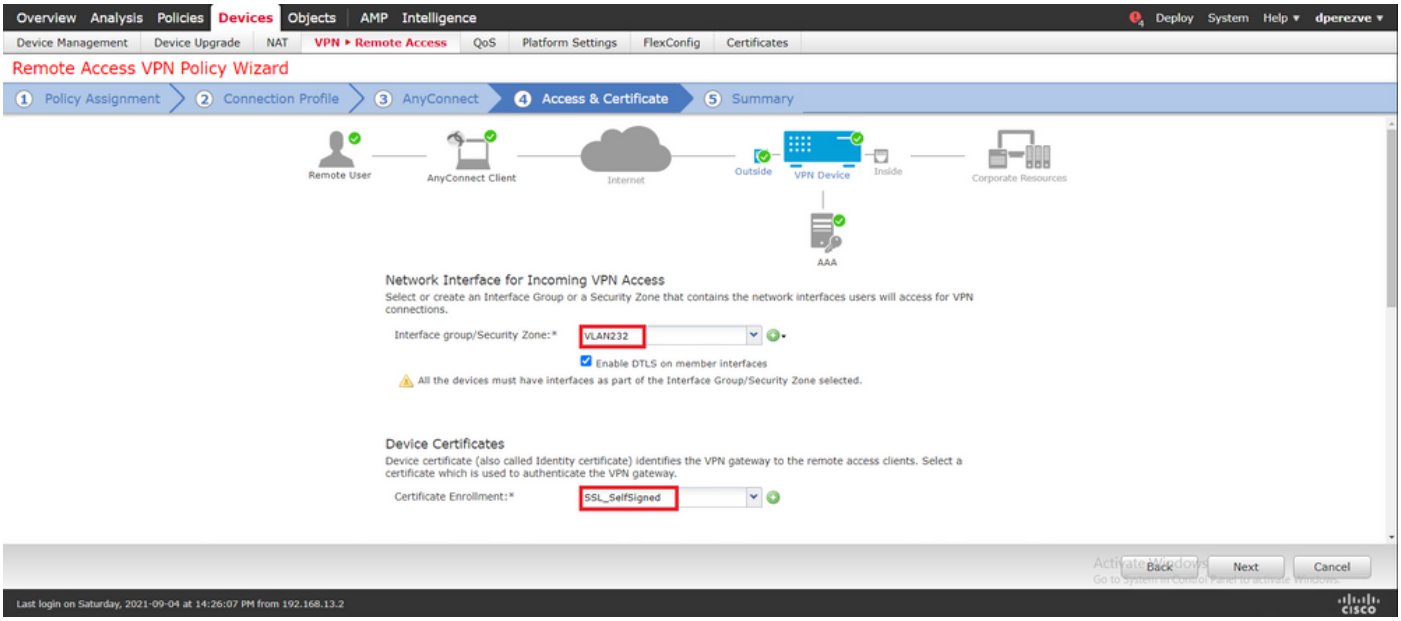
Faites défiler la page vers le bas, puis choisissez l'icône de crayon dans la section IPv4 Address Pool afin de définir le pool d'adresses IP utilisé par les clients sécurisés Cisco.



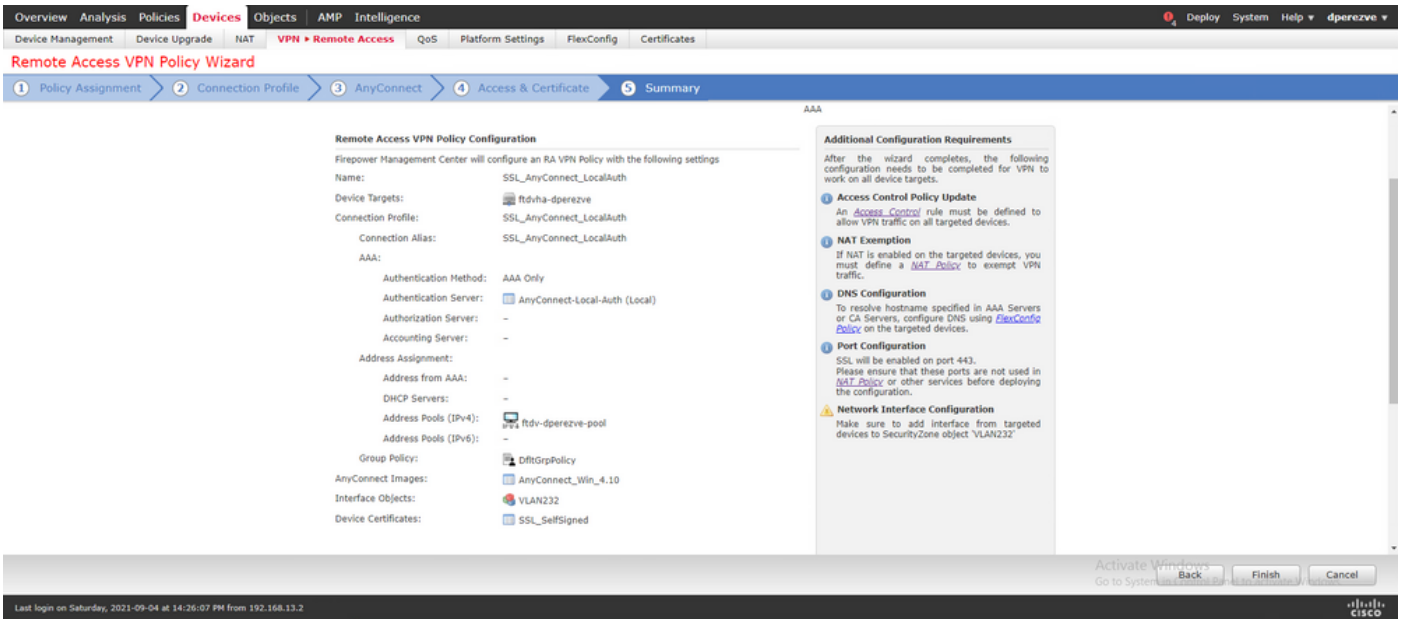
Choisissez Next afin de passer à la section AnyConnect. Sélectionnez maintenant l'image du client sécurisé Cisco téléchargée à l'étape 2.



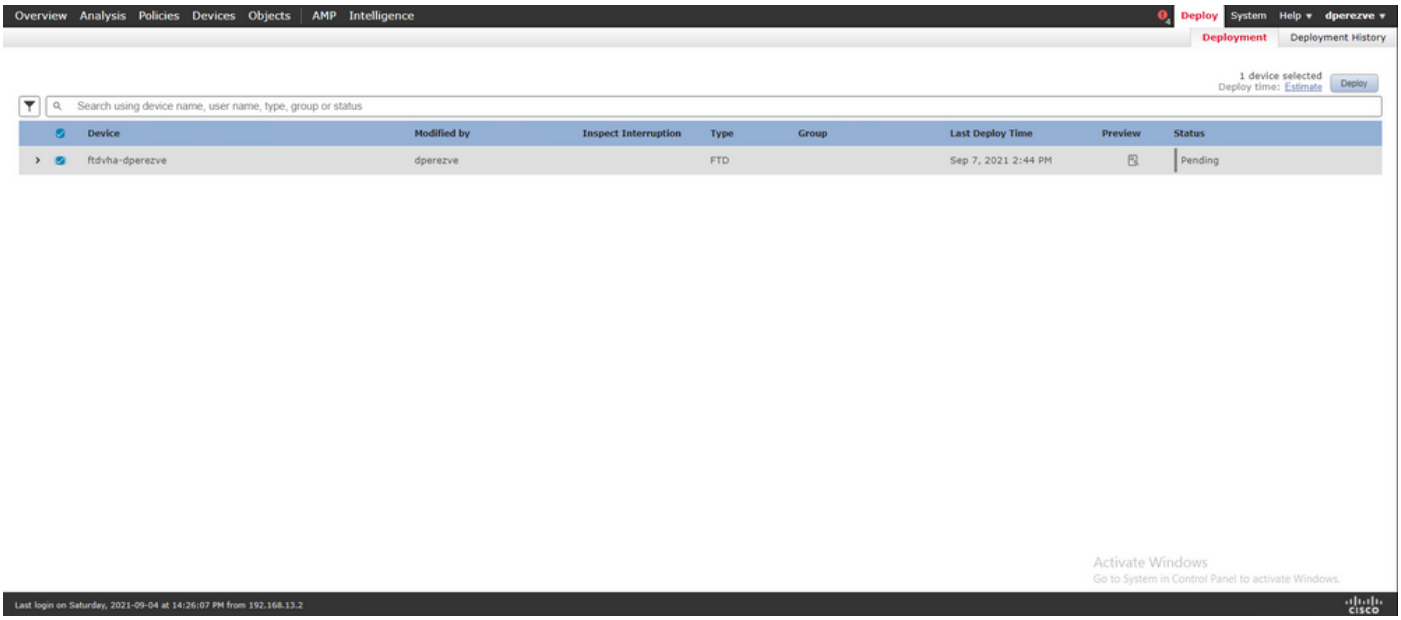
Choisissez Next afin de passer à la section Access & Certificate. Dans le menu déroulant Interface group/Security Zone, choisissez l'interface sur laquelle Cisco Secure Client (AnyConnect) doit être activé. Ensuite, dans le menu déroulant Certificate Enrollment, choisissez le certificat créé à l'étape 3.



Enfin, choisissez Next afin d'afficher un résumé de la configuration de Cisco Secure Client.

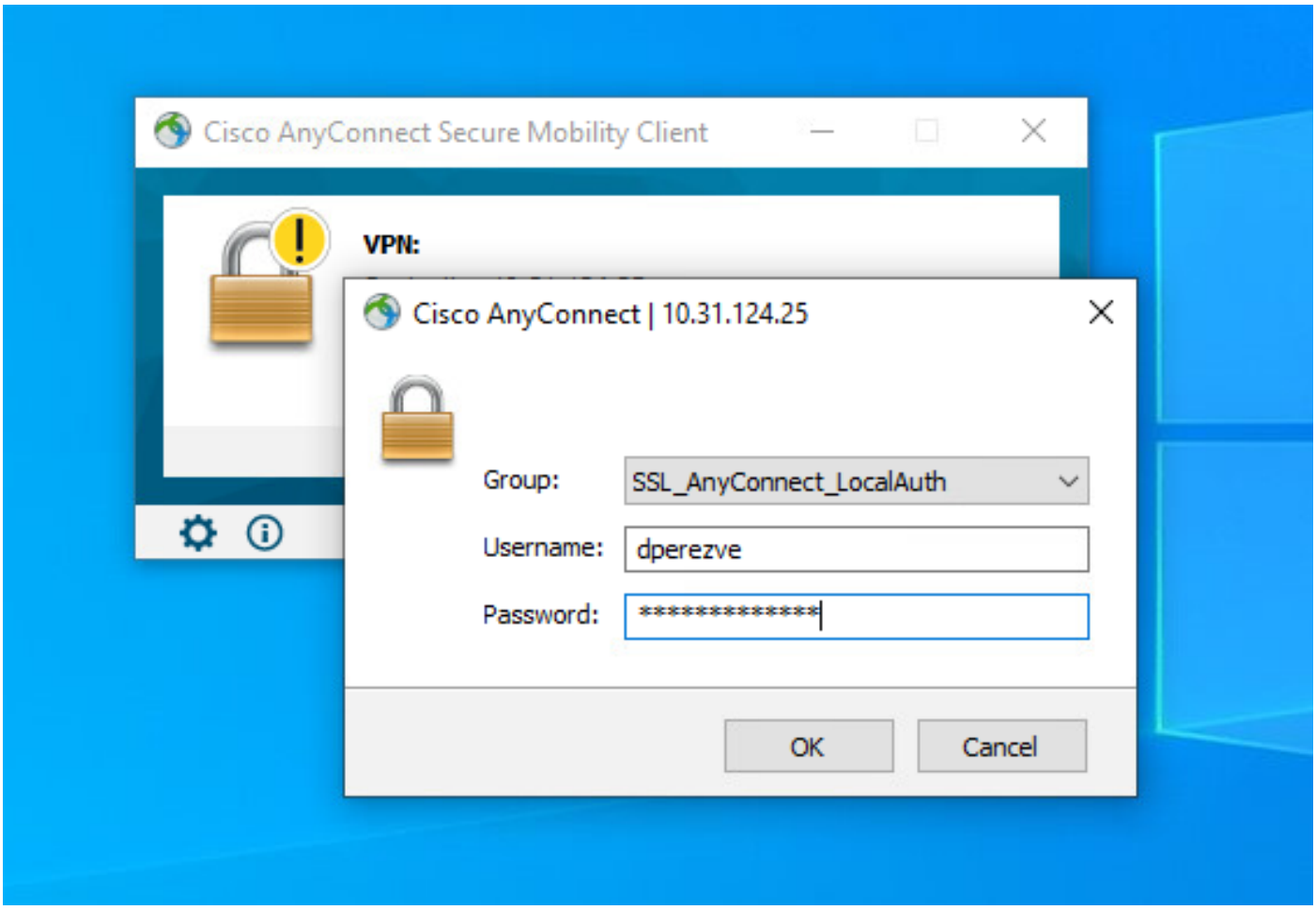


Si tous les paramètres sont corrects, choisissez Finish et déployez les modifications sur FTD.

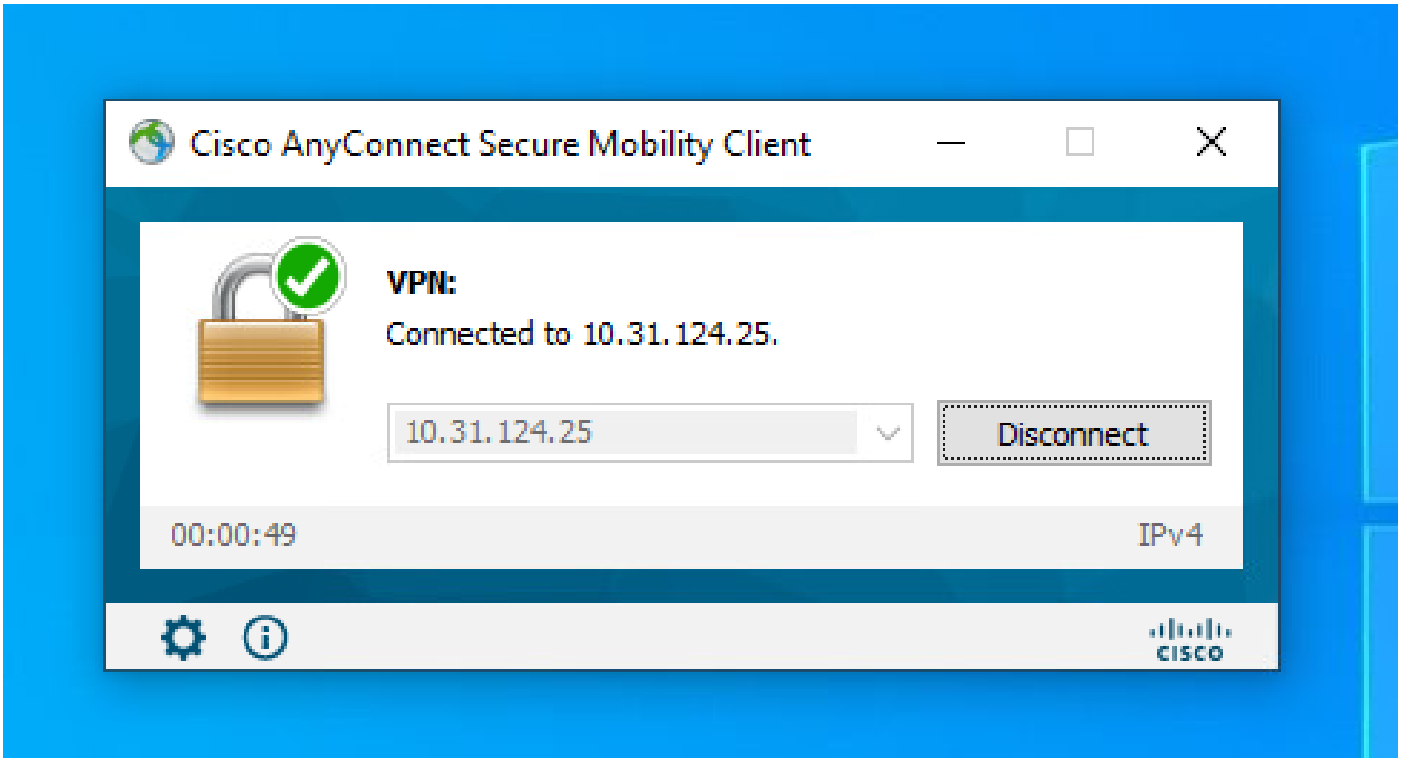


Vérifier

Une fois le déploiement réussi, initiez une connexion Cisco AnyConnect Secure Mobility Client du client Windows au FTD. Le nom d'utilisateur et le mot de passe utilisés dans l'invite d'authentification doivent être identiques à ceux créés à l'étape 4.



Une fois les informations d'identification approuvées par le FTD, l'application Cisco AnyConnect Secure Mobility Client doit afficher l'état connecté.



À partir de FTD, vous pouvez exécuter la commande show vpn-sessiondb anyconnect afin

d'afficher les sessions Cisco Secure Client actuellement actives sur le pare-feu.

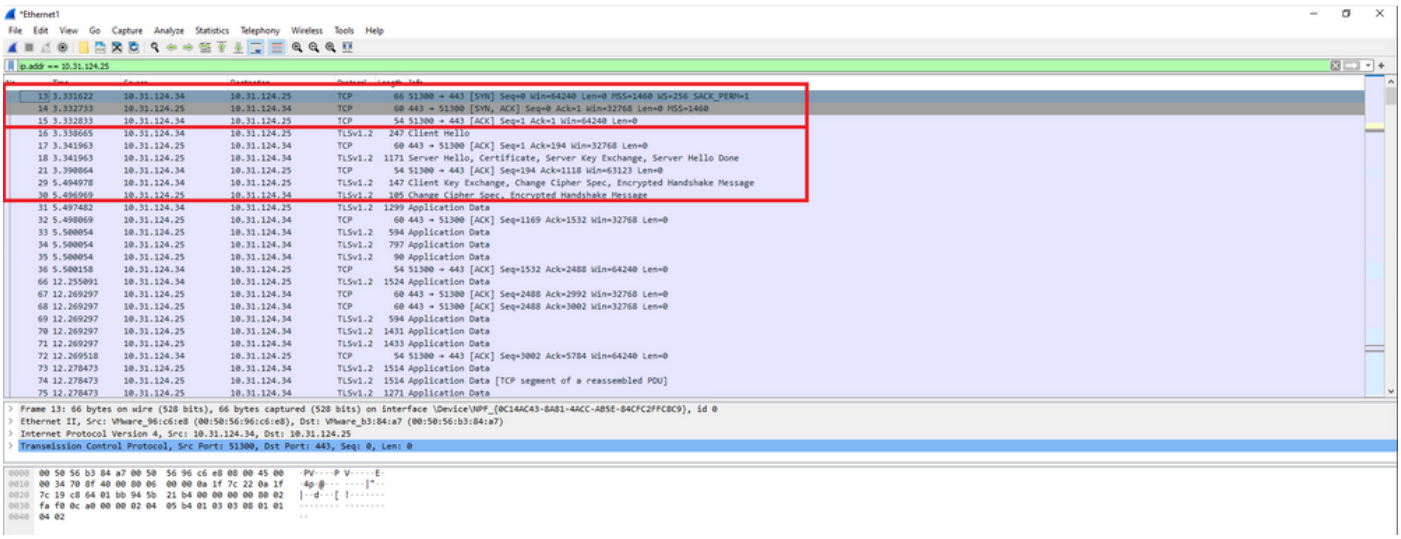
```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dperezve               Index        : 8
Assigned IP  : 172.16.13.1            Public IP    : 10.31.124.34
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 15756                  Bytes Rx     : 14606
Group Policy : DfltGrpPolicy
Tunnel Group : SSL_AnyConnect_LocalAuth
Login Time   : 21:42:33 UTC Tue Sep 7 2021
Duration     : 0h:00m:30s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 00000000000080006137dcc9
Security Grp : none                   Tunnel Zone  : 0
```

Dépannage

Exécutez la commande debug webvpn anyconnect 255 sur FTD afin de voir le flux de connexion SSL sur FTD.

```
firepower# debug webvpn anyconnect 255
```

Outre les débogages du client sécurisé Cisco, le flux de connexion peut également être observé avec les captures de paquets TCP. Il s'agit d'un exemple de connexion réussie, une connexion normale de trois mois entre le client Windows et FTD est terminée, suivie d'une connexion SSL utilisée pour accepter les chiffrements.



Après les échanges de protocole, FTD doit valider les informations d'identification avec les informations stockées dans le domaine local.

Collectez le bundle DART et contactez le TAC Cisco pour plus d'informations.

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.