

Configuration du client sécurisé SSL avec authentification locale sur FTD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configurations](#)

[Étape 1. Vérifier les licences](#)

[Étape 2. Télécharger le package Cisco Secure Client vers FMC](#)

[Étape 3. Générer un certificat auto-signé](#)

[Étape 4. Créer un domaine local sur FMC](#)

[Étape 5. Configurer le client sécurisé Cisco SSL](#)

[Vérifier](#)

[Dépannage](#)

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).

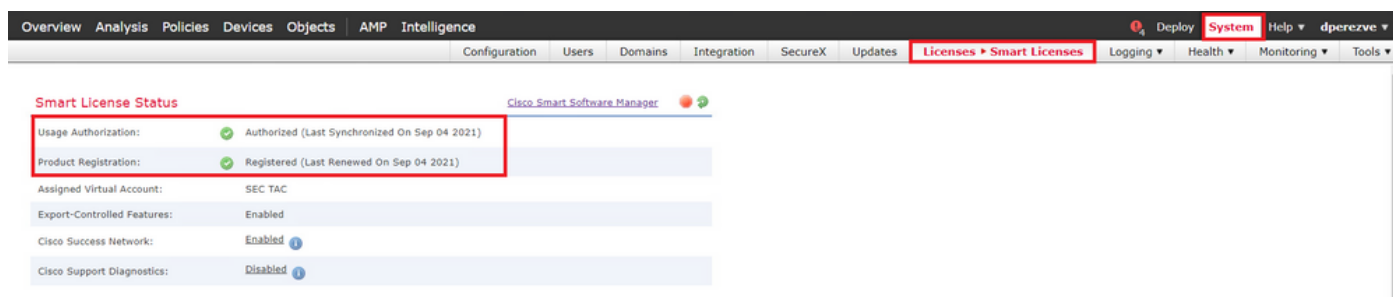
Configurer

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.

Smart Licenses

Filter Devices... Edit Performance Tier Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	✓			
Base (2)	✓			
Malware (2)	✓			
Threat (2)	✓			
URL Filtering (2)	✓			
AnyConnect Apex (2)	✓			
ftdv-dperevze 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
ftdvha-dperevze (Performance Tier: FTDv50 - Tiered) 192.168.13.9 - Cisco Firepower Threat Defense for VMWare - v7.0.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				






















Note: Container Instances of same blade share feature licenses

Activate Windows
Go to System in Control Panel to activate Windows.

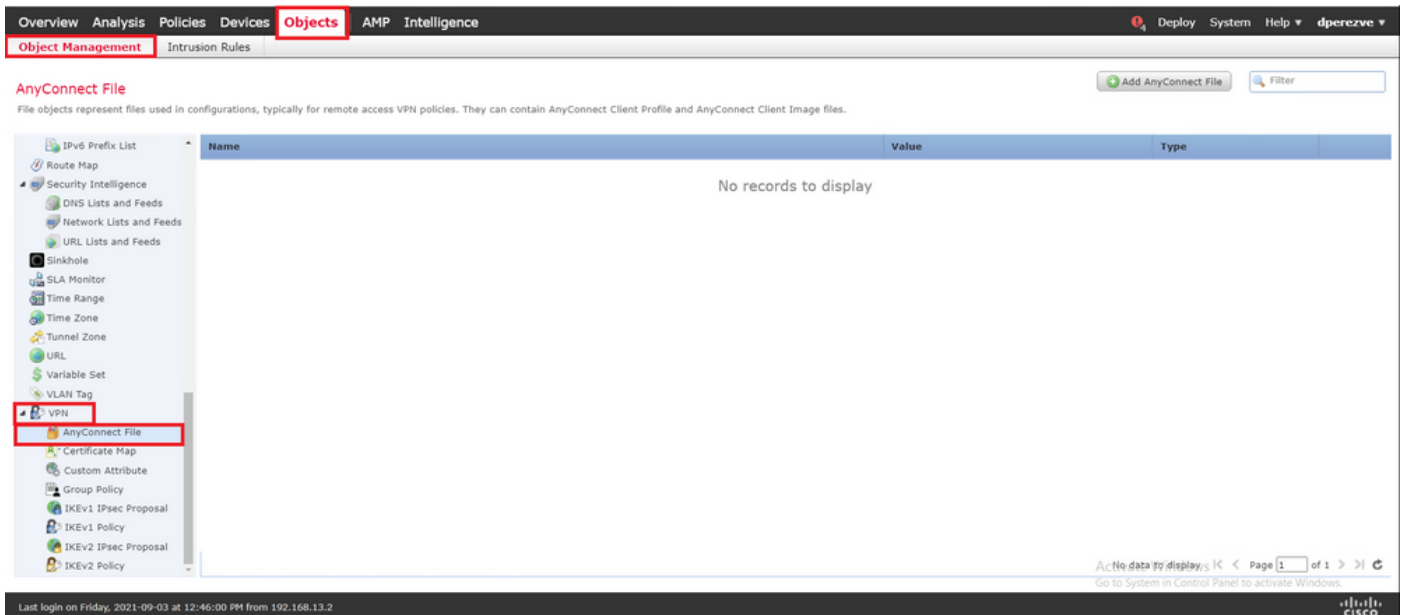
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Étape 2. Télécharger le package Cisco Secure Client vers FMC

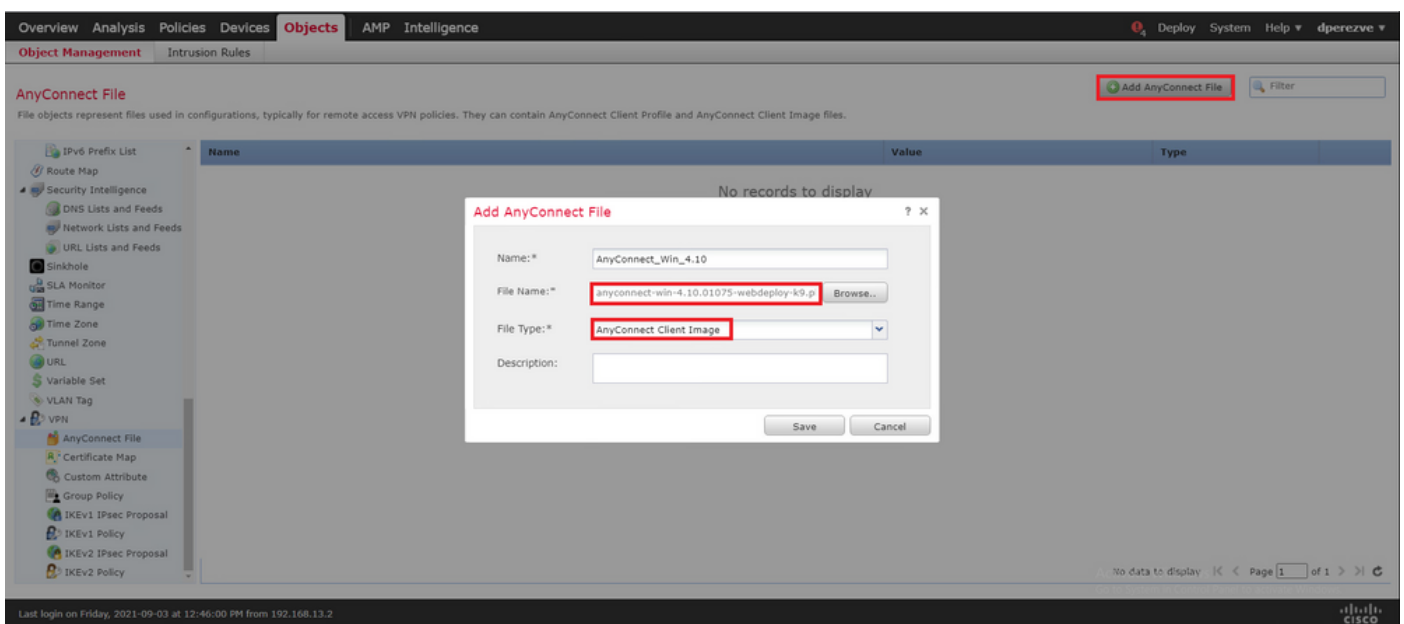
Téléchargez le package de déploiement de tête de réseau Cisco Secure Client (AnyConnect) pour Windows depuis le site cisco.com.

Application Programming Interface [API] (Windows)   anyconnect-win-4.10.01075-vpnapi.zip Advisories 	21-May-2021	141.72 MB	 
AnyConnect Headend Deployment Package (Windows)   anyconnect-win-4.10.01075-webdeploy-k9.pkg Advisories 	21-May-2021	77.81 MB	 
AnyConnect Pre-Deployment Package (Windows 10 ARM64) - includes individual MSI files   anyconnect-win-arm64-4.10.01075-predeploy-k9.zip Advisories 	21-May-2021	34.78 MB	 
AnyConnect Headend Deployment Package (Windows 10 ARM64)    anyconnect-win-arm64-4.10.01075-webdeploy-k9.pkg Advisories 	21-May-2021	44.76 MB	 
Profile Editor (Windows)   tools-anyconnect-win-4.10.01075-profileeditor-k9.msi Advisories 	21-May-2021	10.90 MB	 
AnyConnect Installer Transforms (Windows)   tools-anyconnect-win-4.10.01075-transforms.zip Advisories 	21-May-2021	0.05 MB	 

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.

Overview Analysis Policies Devices **Objects** AMP Intelligence

Object Management Intrusion Rules

AnyConnect File

File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files.

Name	Value	Type
AnyConnect_Win_4.10	anyconnect-win-4.10.01075-webdeploy-k9.pkg	AnyConnect Client Image

Policy List


- Port
- Prefix List
 - IPV4 Prefix List
 - IPV6 Prefix List
- Route Map
- Security Intelligence
 - DNS Lists and Feeds
 - Network Lists and Feeds
 - URL Lists and Feeds
- Sinkhole
- SLA Monitor
- Time Range
- Time Zone
- Tunnel Zone
- URL
- Variable Set
- VLAN Tag
- VPN
 - AnyConnect File**
 - Certificate Map
 - Custom Attribute
 - Group Policy
 - IKEv1 IPsec Proposal
 - IKEv1 Policy
 - IKEv2 IPsec Proposal
 - IKEv2 Policy

Activate Windows
Go to Settings to activate Windows.

Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

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.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management Device Upgrade NAT VPN QoS Platform Settings FlexConfig **Certificates**

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

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management Device Upgrade NAT VPN QoS Platform Settings FlexConfig **Certificates**

No certificates [Add Certificates](#)

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

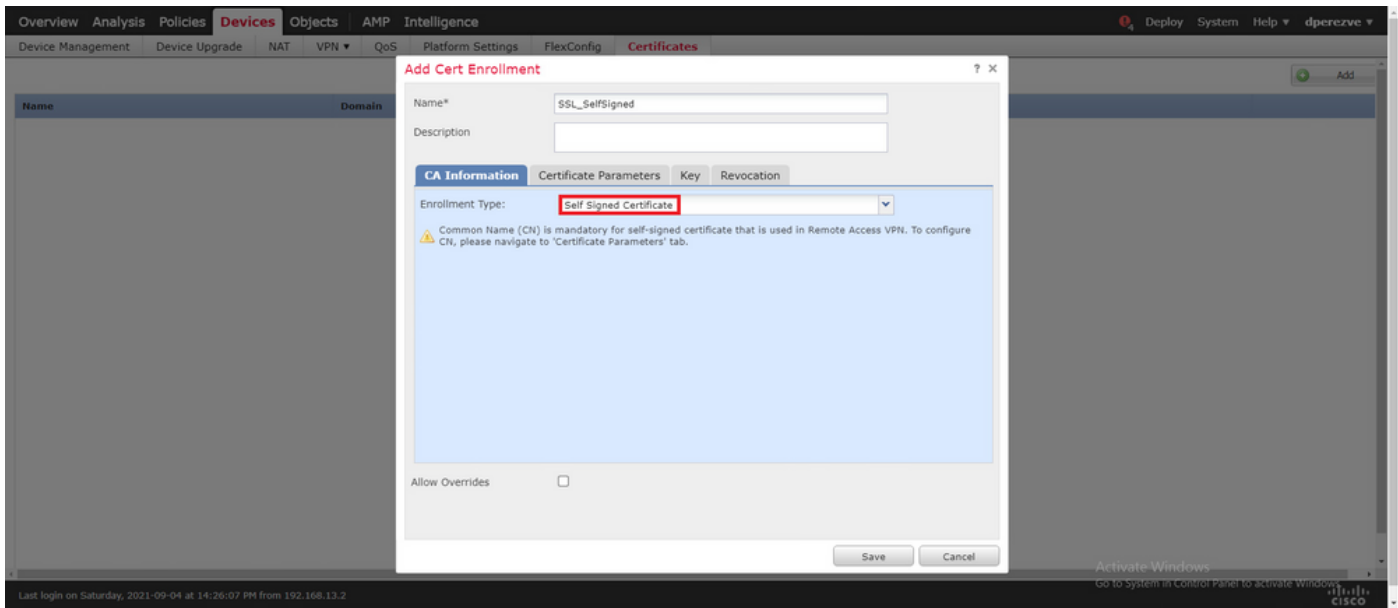
Device*:

Cert Enrollment*:

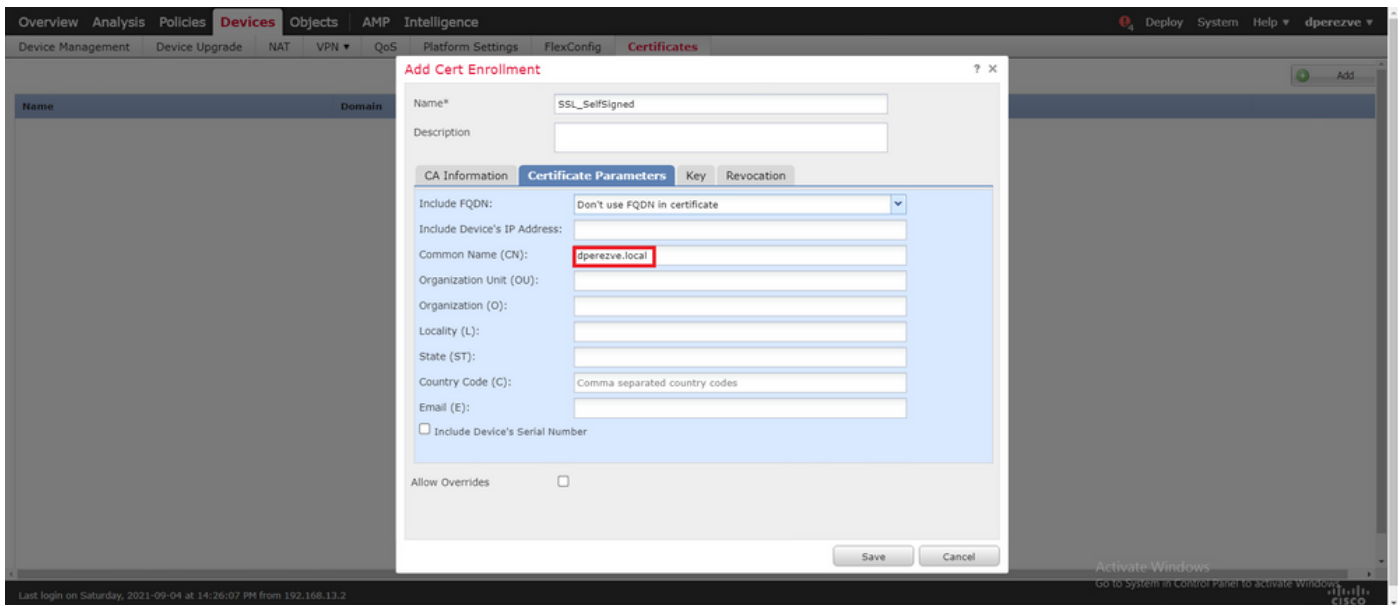
Activate Windows
Go to Settings to activate Windows.

Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

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.

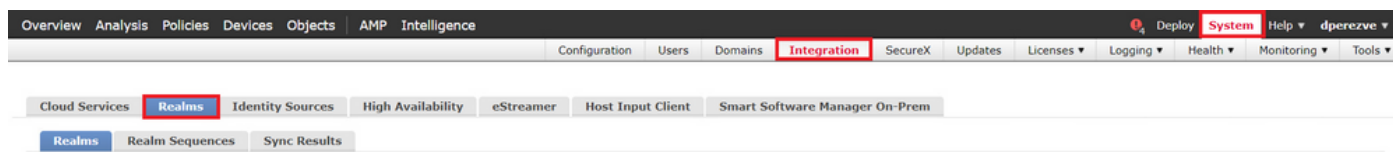


Choisissez Save and Add button. Après quelques secondes, le nouveau certificat doit être ajouté à la liste des certificats.

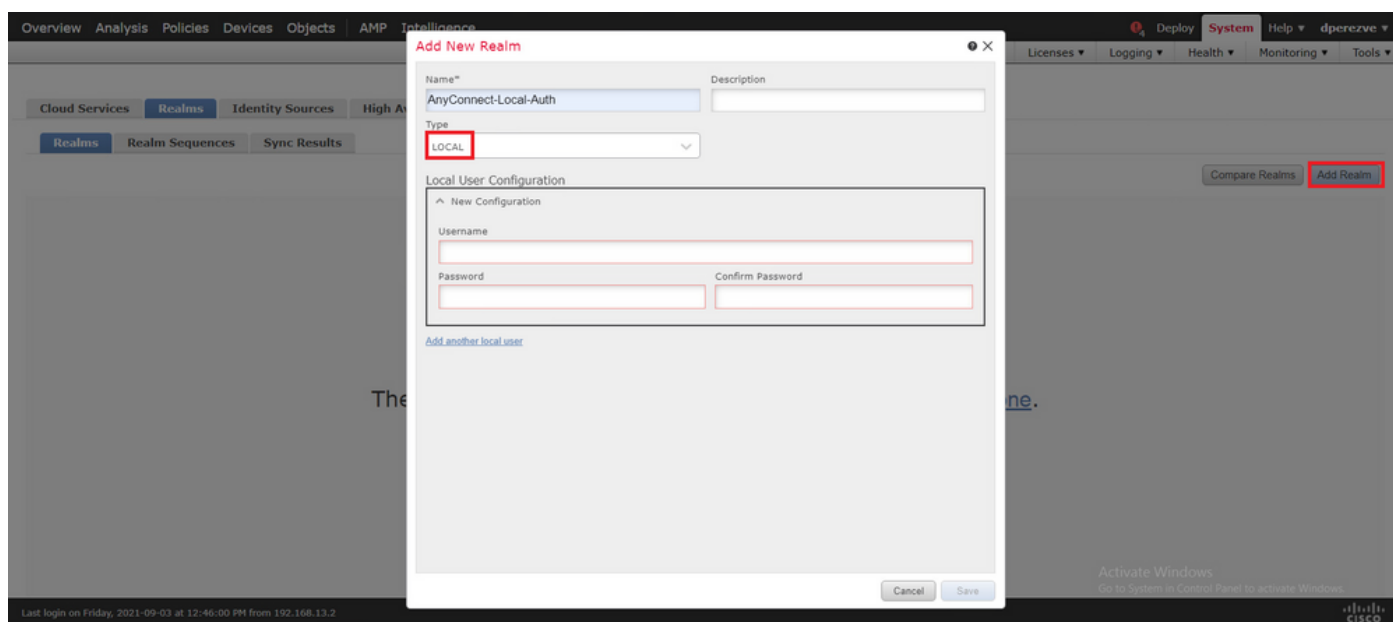


Étape 4. Créer un domaine local sur FMC


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.

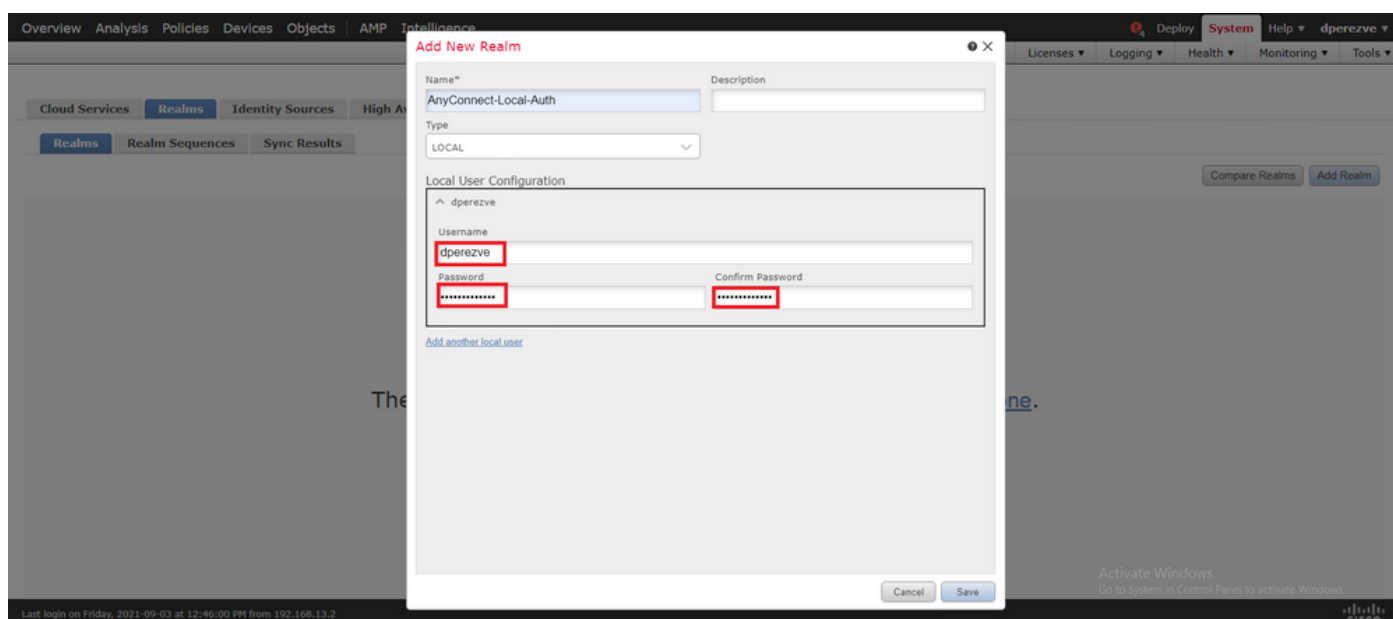


Cliquez sur le bouton Ajouter un domaine. Dans la fenêtre Ajouter un nouveau domaine, attribuez un nom et choisissez l'option LOCAL dans le menu déroulant Type.

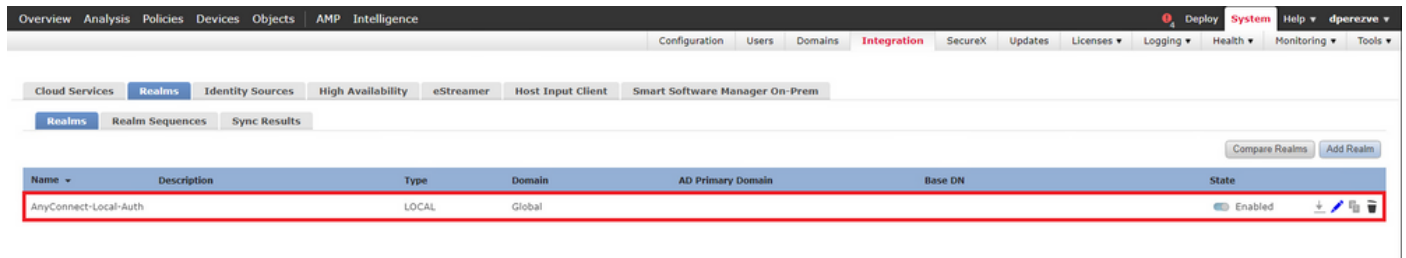


Les comptes d'utilisateurs et les mots de passe sont créés dans la section Configuration utilisateur locale.

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

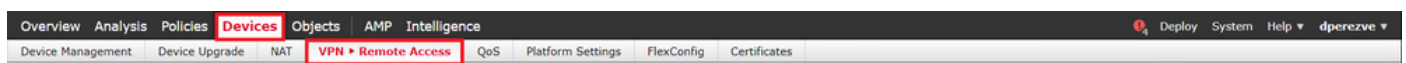


Enregistrez les modifications et ajoutez un nouveau domaine (realm) à la liste des domaines existants.

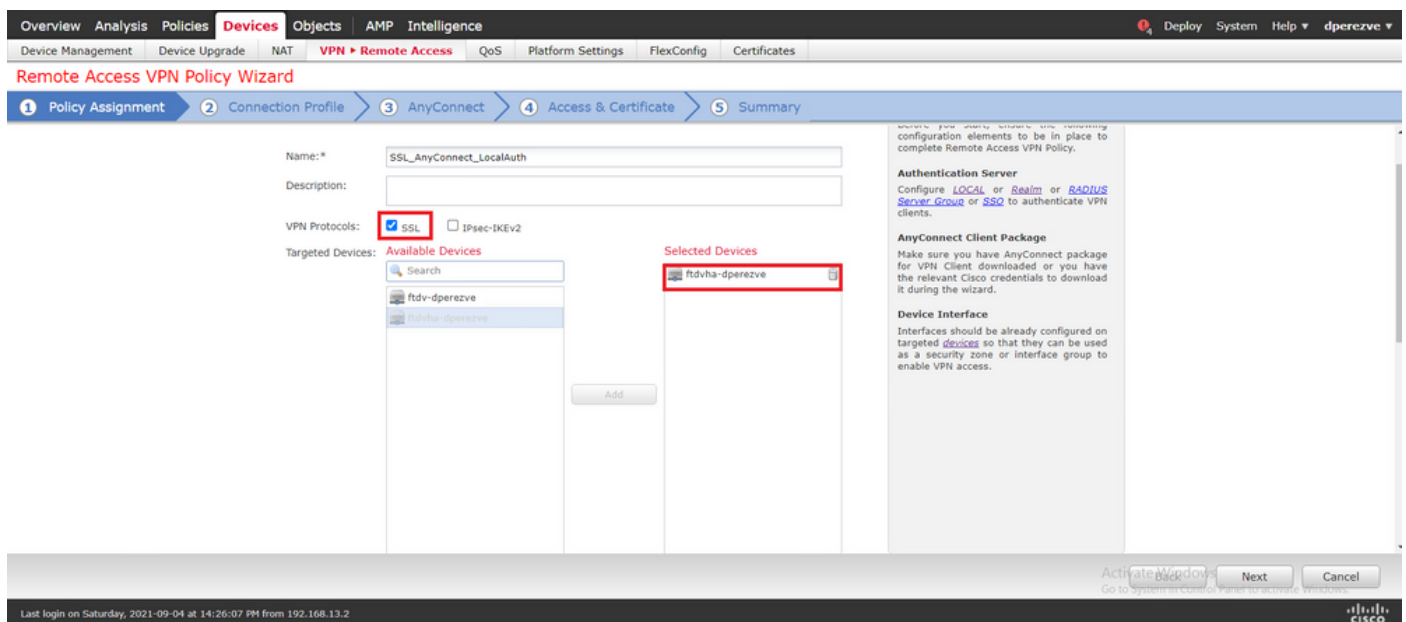


Étape 5. Configurer le client sécurisé Cisco SSL

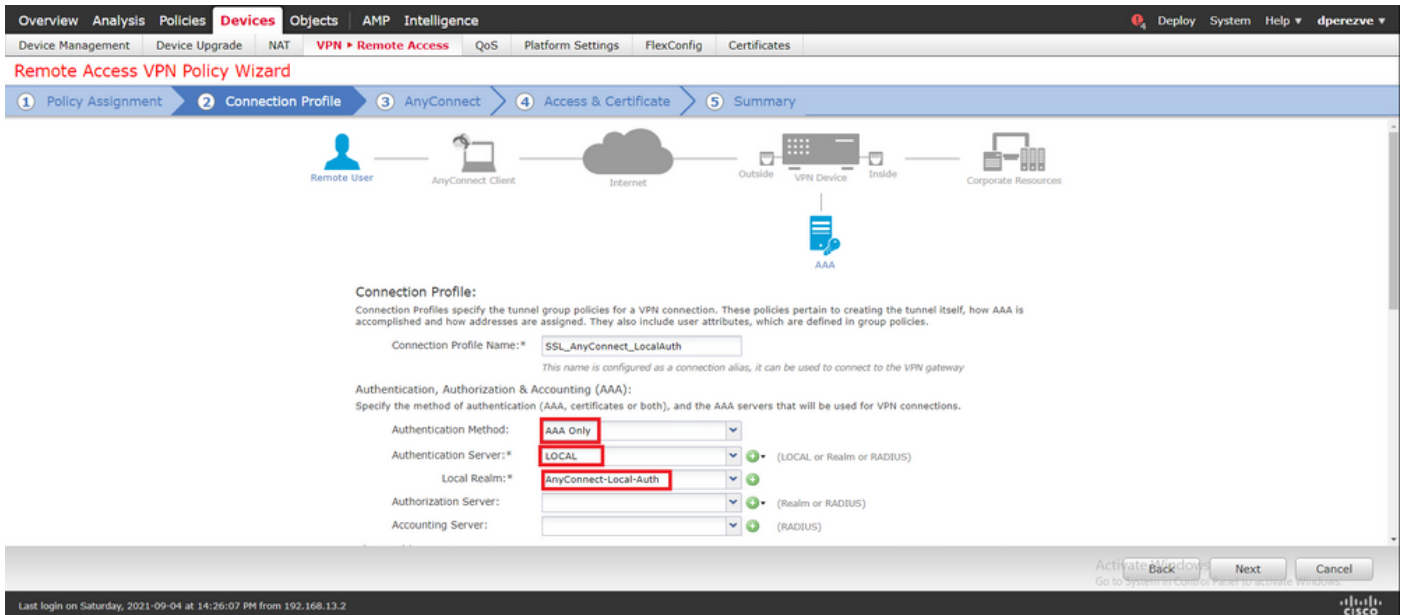
Afin de configurer SSL Cisco Secure Client, naviguez vers Devices > VPN > Remote Access.



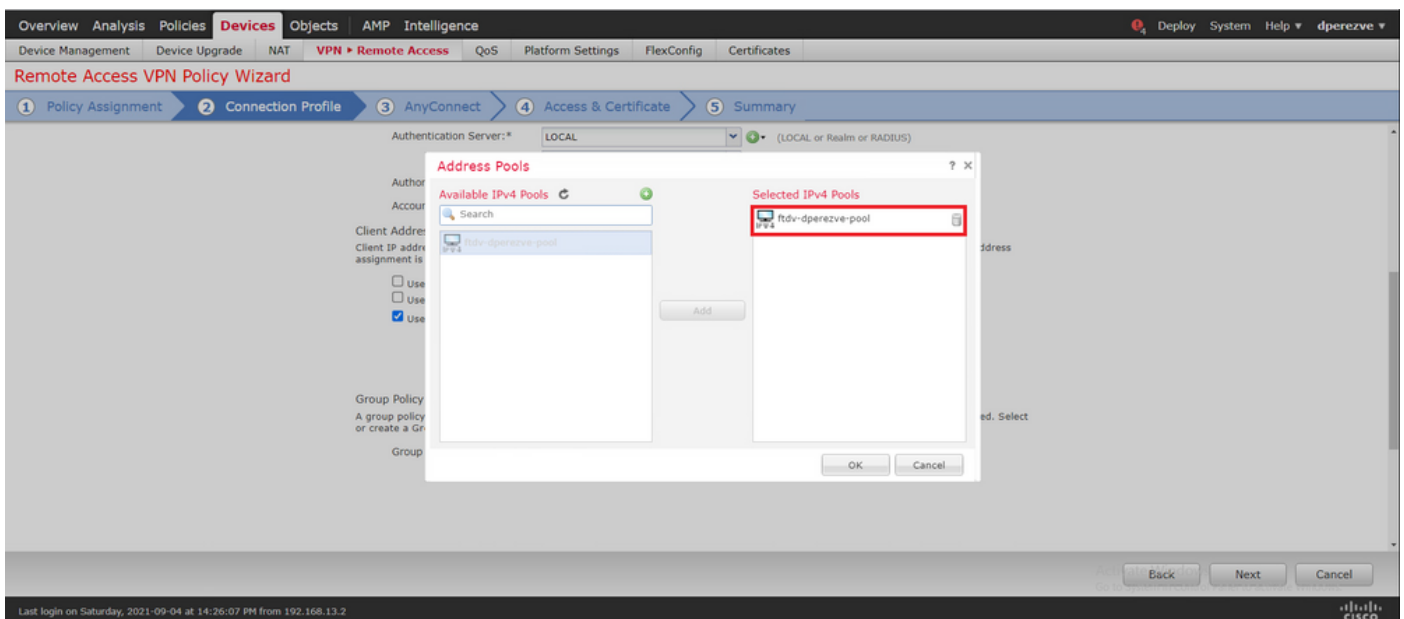
Cliquez sur le bouton Add afin de créer une nouvelle stratégie VPN. Définissez un nom pour le profil de connexion, cochez la case SSL et choisissez le FTD disponible comme périphérique cible. Tout doit être configuré dans la section Affectation de stratégie de l'Assistant Stratégie VPN d'accès à distance.



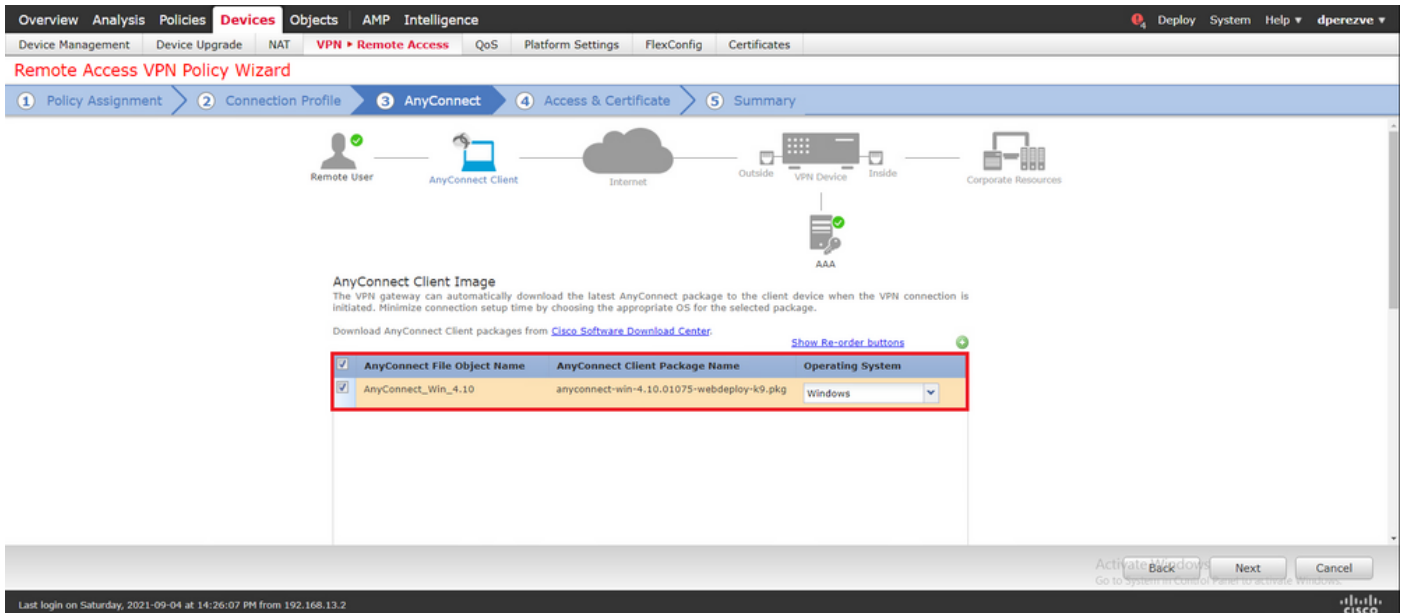
Choisissez Next afin de passer à la configuration Connection Profile. Définissez un nom pour le profil de connexion et choisissez AAA Only comme méthode d'authentification. Ensuite, dans le menu déroulant Authentication Server, choisissez LOCAL, et enfin, choisissez le domaine local créé à l'étape 4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



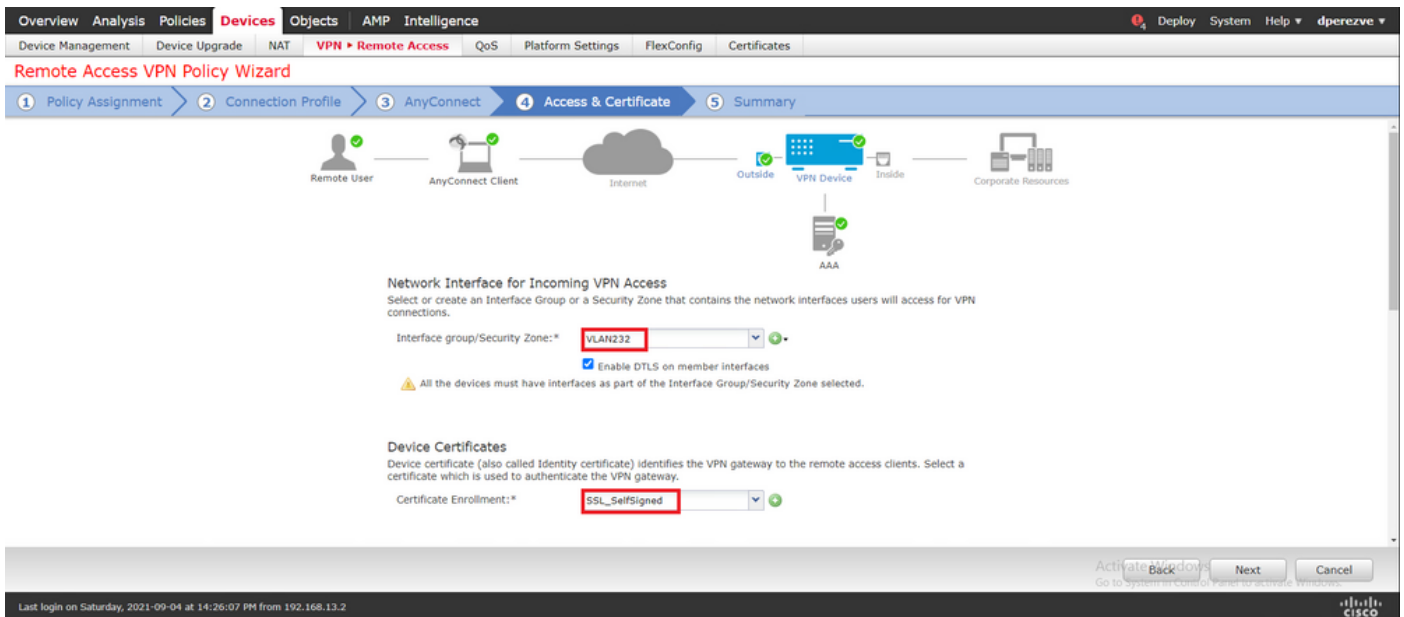
Faites défiler la page vers le bas, puis choisissez l'icône de crayon dans la section IPv4 Address Pool afin de définir le pool d'adresses IP utilisé par les clients sécurisés Cisco.



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.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management Device Upgrade NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment > 2 Connection Profile > 3 AnyConnect > 4 Access & Certificate > 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: SSL_AnyConnect_LocalAuth

Device Targets: ftdvha-dpereze

Connection Profile: SSL_AnyConnect_LocalAuth

Connection Alias: SSL_AnyConnect_LocalAuth

AAA:

- Authentication Method: AAA Only
- Authentication Server: AnyConnect-Local-Auth (Local)
- Authorization Server: -
- Accounting Server: -

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): ftdvha-dpereze-pool
- Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images: AnyConnect_Win_4.10

Interface Objects: VLAN232

Device Certificates: SSL_SelfSigned

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- Network Interface Configuration**
Make sure to add interface from targeted devices to SecurityZone object 'VLAN232'

Activate Windows
Go to System in Control Panel to activate Windows.

Back Finish Cancel

Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

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

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy System Help dpereze

Deployment Deployment History

1 device selected
Deploy time: Estimate Deploy

Search using device name, user name, type, group or status

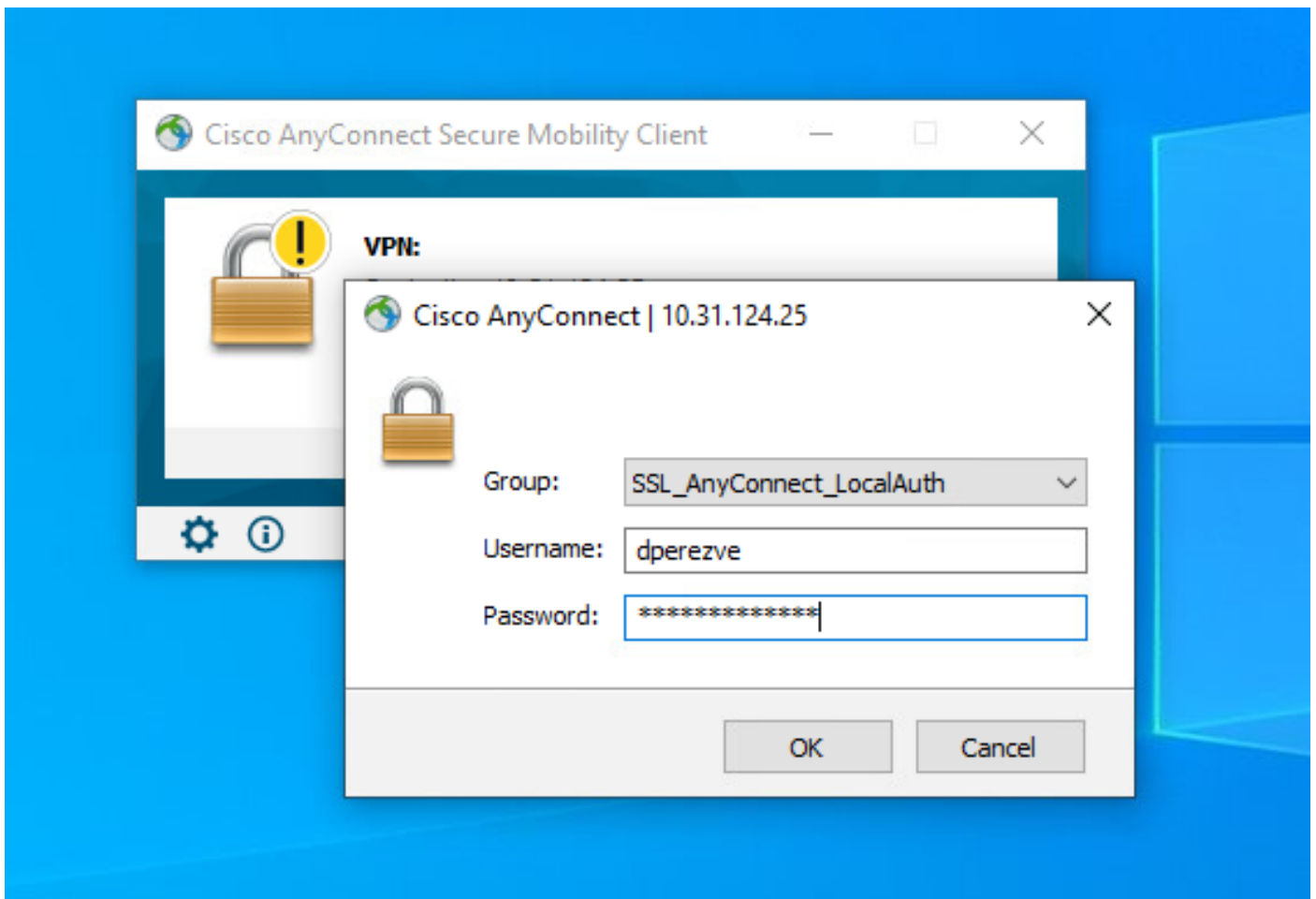
Device	Modified by	Inspect	Interruption	Type	Group	Last Deploy Time	Preview	Status
ftdvha-dpereze	dpereze			FTD		Sep 7, 2021 2:44 PM		Pending

Activate Windows
Go to System in Control Panel to activate Windows.

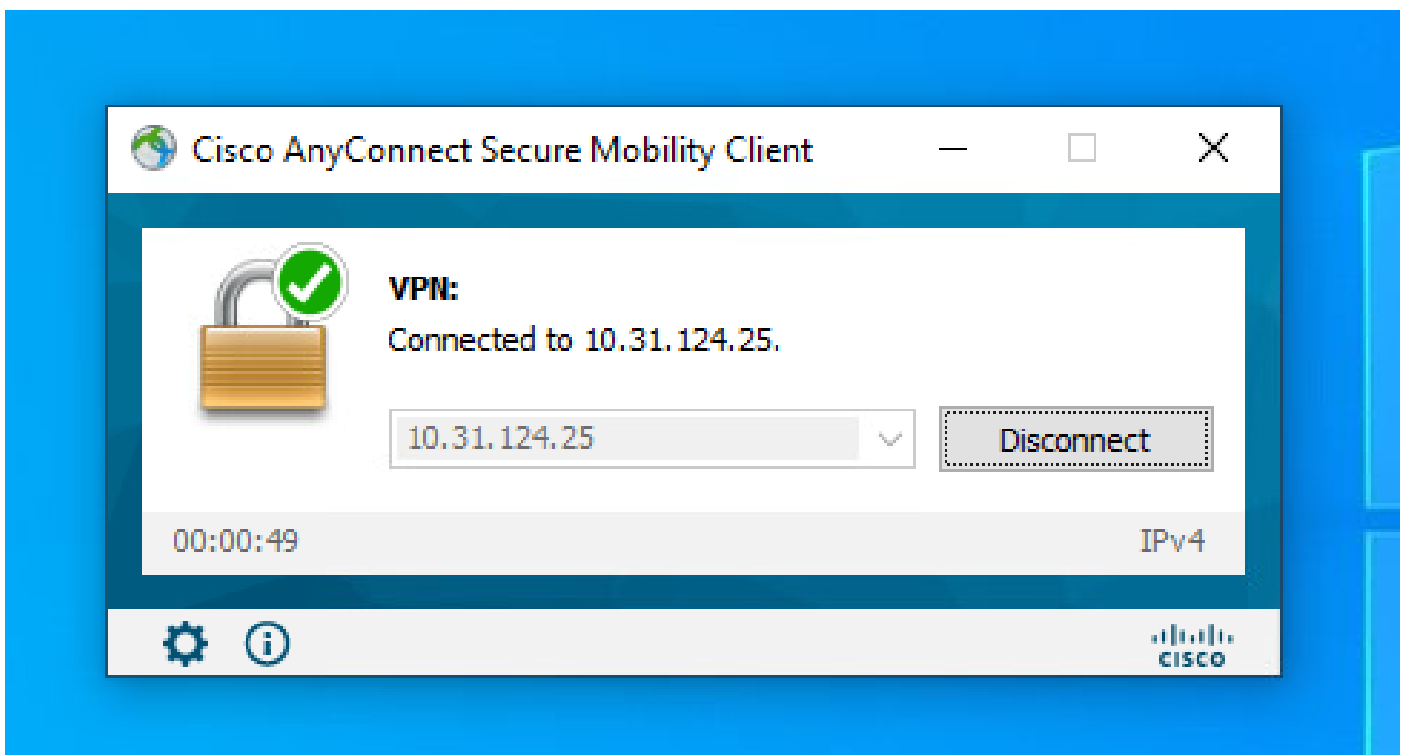
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

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.

The image shows a Wireshark capture of a TLS handshake. The packet list pane shows the following key packets:

- 13: 3.331222 10.31.124.34 → 10.31.124.25 TCP 66 51300 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
- 14: 3.332733 10.31.124.25 → 10.31.124.34 TCP 60 443 → 51300 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
- 15: 3.332833 10.31.124.34 → 10.31.124.25 TCP 56 51300 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
- 16: 3.336655 10.31.124.34 → 10.31.124.25 TLSv1.2 247 Client Hello
- 17: 3.341963 10.31.124.25 → 10.31.124.34 TCP 60 443 → 51300 [ACK] Seq=1 Ack=194 Win=32768 Len=0
- 18: 3.341963 10.31.124.25 → 10.31.124.34 TLSv1.2 1171 Server Hello, Certificate, Server Key Exchange, Server Hello Done
- 21: 3.390864 10.31.124.34 → 10.31.124.25 TCP 54 51300 → 443 [ACK] Seq=194 Ack=1118 Win=63123 Len=0
- 29: 5.494978 10.31.124.34 → 10.31.124.25 TLSv1.2 147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
- 30: 5.496969 10.31.124.25 → 10.31.124.34 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message

The packet details pane for the selected packet (Frame 13) shows:

```

> Internet Protocol Version 4, Src: 10.31.124.34, Dst: 10.31.124.25
> Transmission Control Protocol, Src Port: 51300, Dst Port: 443, Seq: 0, Len: 0
  
```

The packet bytes pane shows the raw hex and ASCII data for the captured frame.

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.