

SSL AnyConnect met lokale verificatie op FTD beheerde door FMC configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuraties](#)

[Stap 1. Controleer de licenties](#)

[Stap 2. Upload AnyConnect met FMC](#)

[Stap 3. Een zelfondertekend certificaat genereren](#)

[Stap 4. Lokaal antwoord op FMC maken](#)

[Stap 5. Het configureren van SSL AnyConnect](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u Cisco AnyConnect met lokale verificatie kunt configureren op een Cisco Firepower Threat Defense (FTD) die wordt beheerd door Cisco Firepower Management Center (FMC). In het voorbeeld onder Secure Socket Layer (SSL) wordt gebruikt om Virtual Private Network (VPN) tussen FTD en een Windows 10-client te maken.

Bijgedragen door Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SSL AnyConnect-configuratie via FMC
- Configuratie van FireSIGHT-objecten via FMC
- SSL-certificaten op Firepower

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTD versie 7.0.0 (gebouwd 94)

- Cisco FMC versie 7.0.0 (gebouwd 94)
- Cisco AnyConnect beveiligde mobiliteit-client 4.10.01075

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Vanaf release 7.0.0 ondersteunt FTD die wordt beheerd door FMC lokale authenticatie voor AnyConnect-klanten. Dit kan worden gedefinieerd als de primaire authenticatiemethode of als reserve voor het geval de primaire methode faalt. In dit voorbeeld wordt lokale authenticatie ingesteld als de primaire authenticatie.

Voor deze softwareversie was AnyConnect lokale verificatie op FTD alleen beschikbaar op Cisco Firepower Apparaatbeheer (FDM).

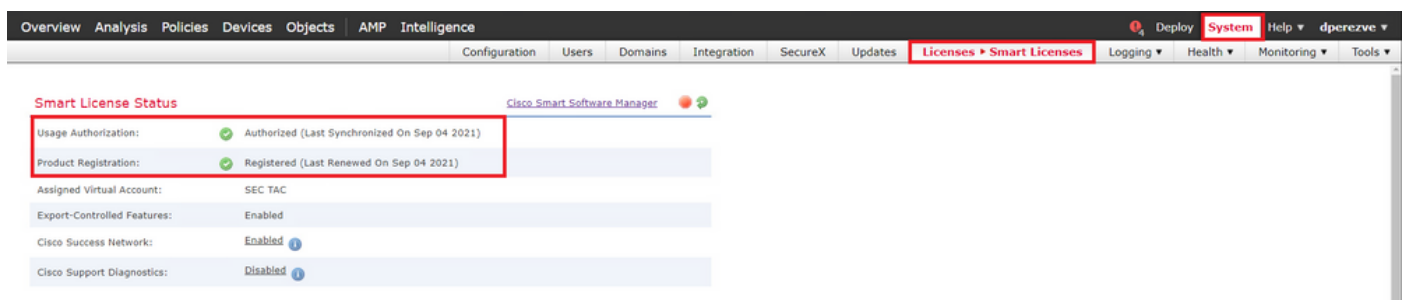
Configureren

Configuraties

Stap 1. Controleer de licenties

Voordat u AnyConnect kunt configureren moet de FMC worden geregistreerd en in overeenstemming zijn met Smart Licensing Portal. U kunt AnyConnect niet implementeren als FTD geen geldige Plus-, Apex- of VPN-licentie heeft.

Navigeer naar **Systeem > Licenties > Smart Licenties** om het FMC te valideren en is deze compatibel met Smart Licensing Portal.



Scroll-down op dezelfde pagina, onder in het schema van **slimme licenties**, u kunt de verschillende soorten AnyConnect-licenties zien die beschikbaar zijn en de apparaten die op elke licentie zijn geabonneerd. De geldigheid van de FTD in kwestie is geregistreerd onder één van deze categorieën.

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-dperezve 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
ftdvha-dperezve (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.

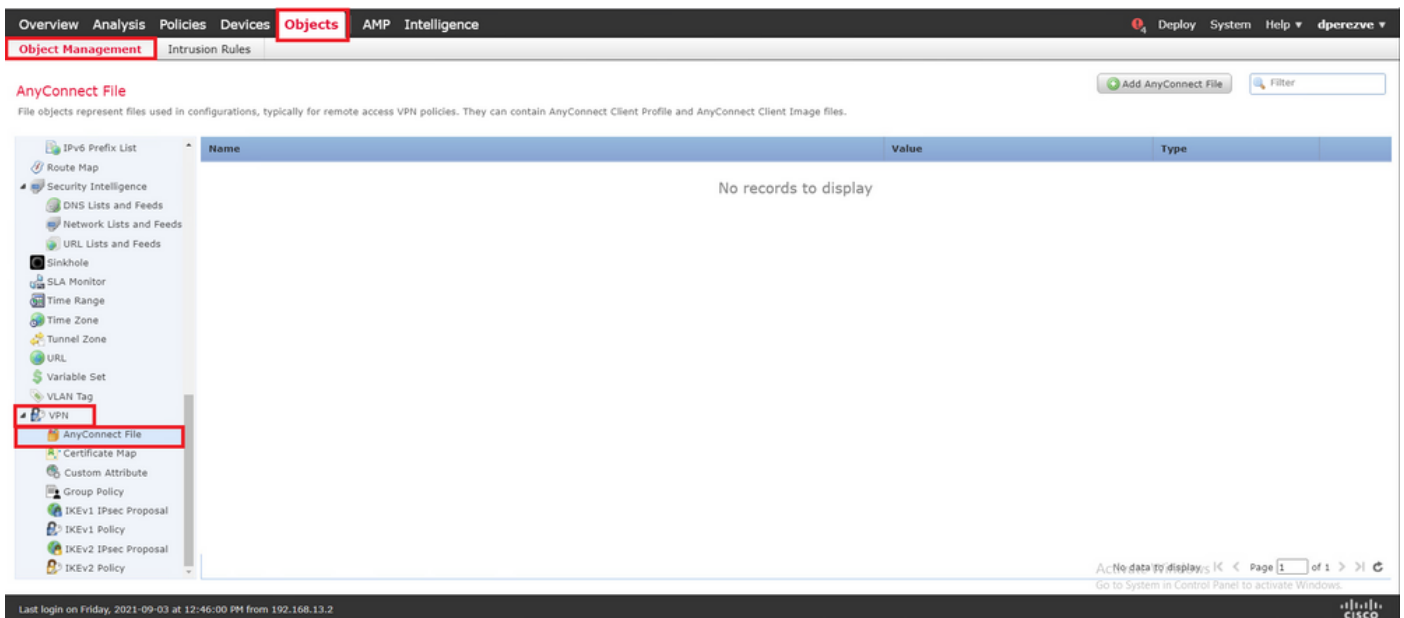
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Stap 2. Upload AnyConnect met FMC

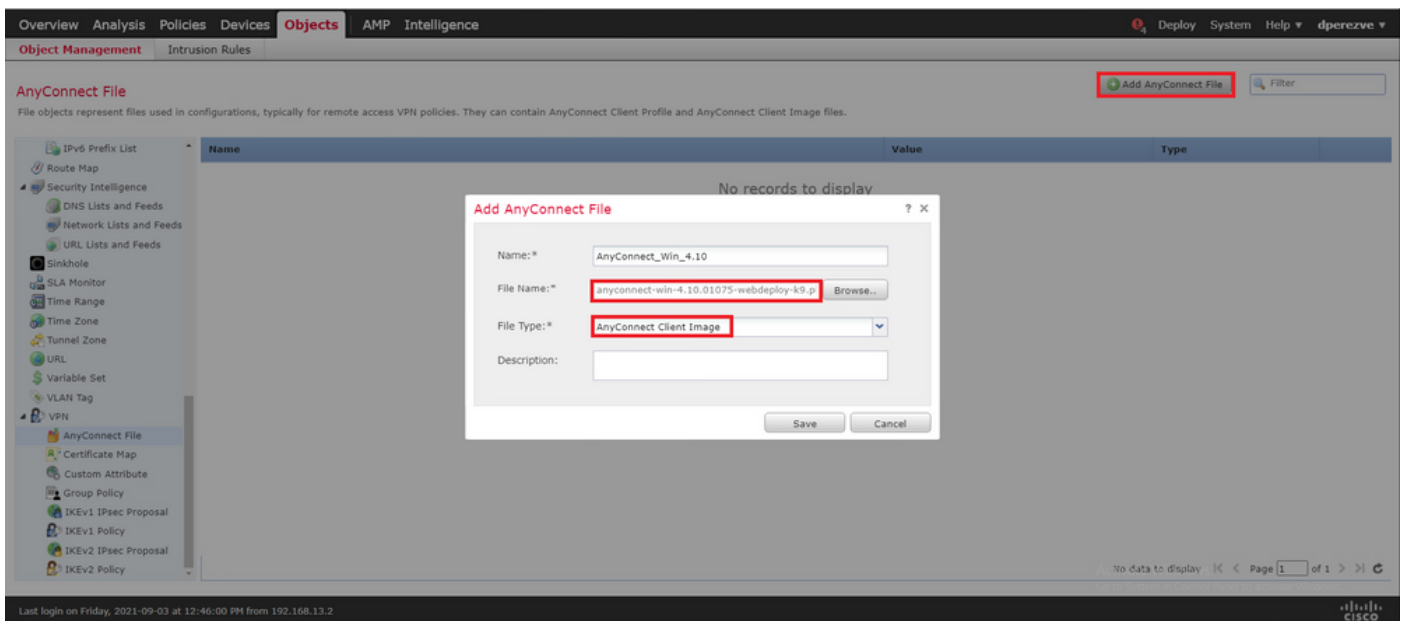
Download het AnyConnect Head-end implementatiepakket voor Windows van [cisco.com](https://www.cisco.com).

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	 

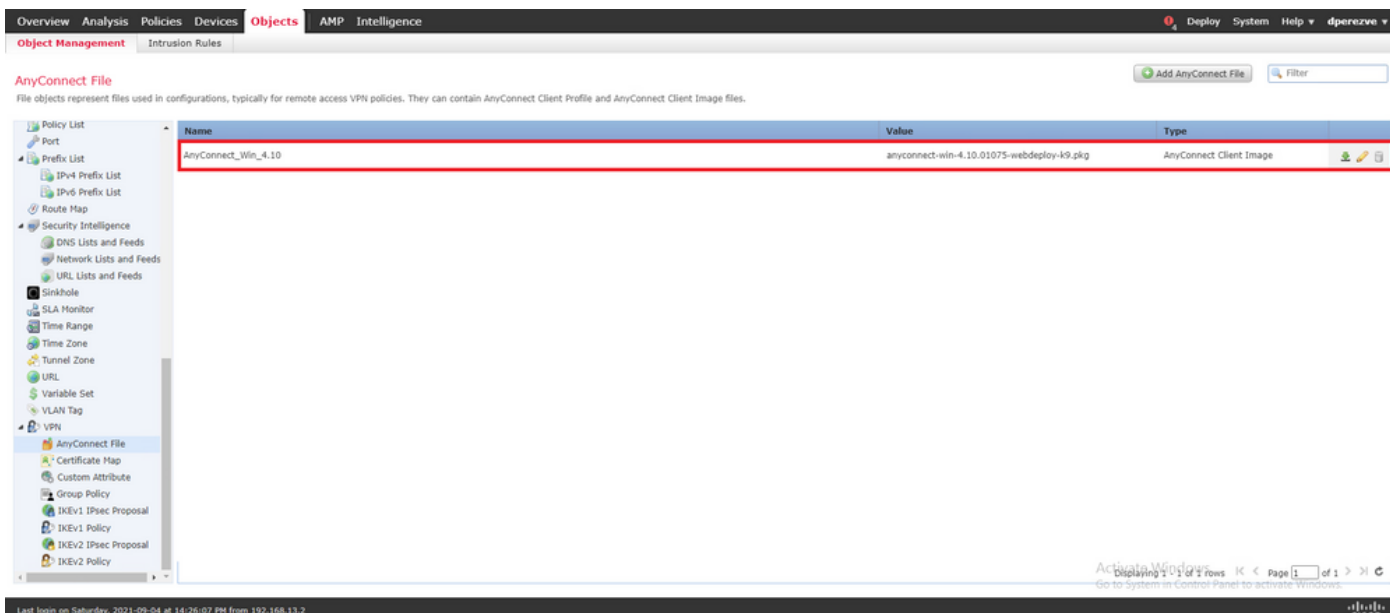
Als u de AnyConnect-afbeelding wilt uploaden, navigeer dan naar **Objecten > Objectbeheer** en selecteer **AnyConnect File** onder de **VPN**-categorie in de inhoudsopgave.



Selecteer de knop **Add AnyConnect File**. In het venster **Add AnyConnect File** toewijzen u een naam voor het object en selecteert u **Bladeren**. Om het AnyConnect-pakket te kiezen en uiteindelijk **AnyConnect-clientafbeelding** als het bestandstype in het vervolgkeuzemenu te kiezen.



Selecteer de knop **Opslaan** en het object moet aan de lijst met objecten worden toegevoegd.



Stap 3. Een zelfondertekend certificaat genereren

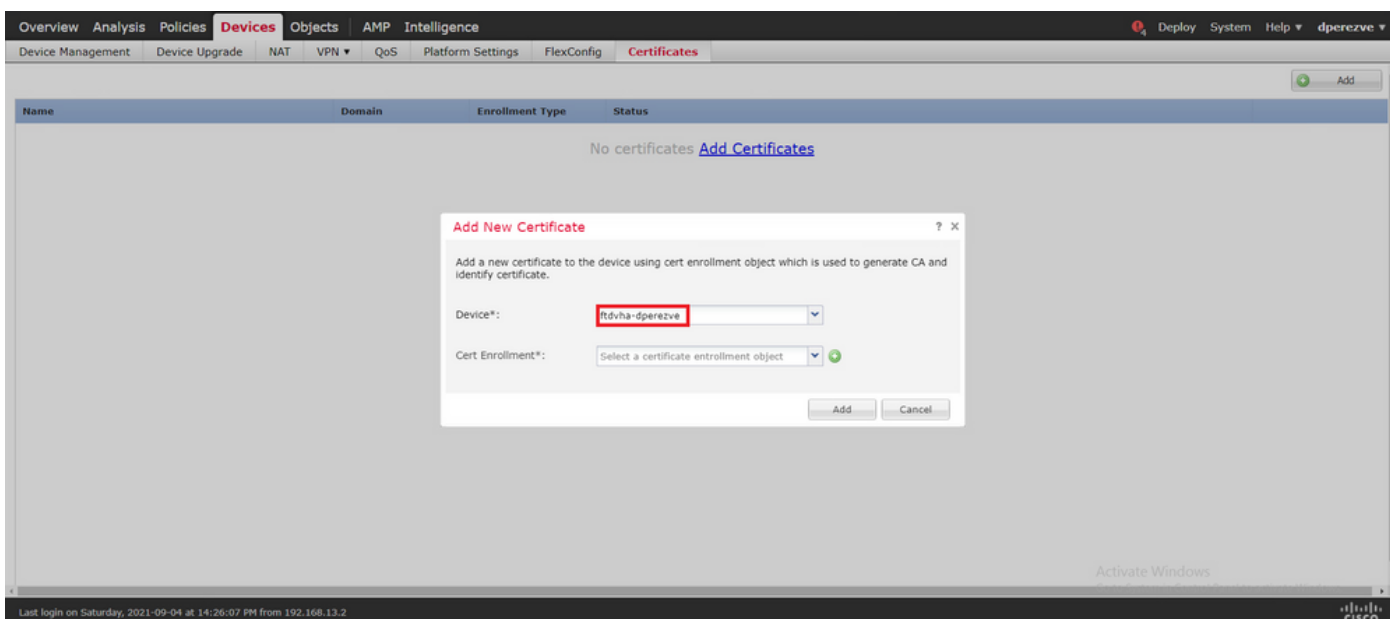
SSL AnyConnect vereist dat één geldig certificaat in de SSL-handdruk tussen VPN-head-end en -client wordt gebruikt.

Opmerking: In dit voorbeeld wordt hiervoor een zelfondertekend certificaat gegenereerd. Naast de zelf ondertekende certificaten is het echter mogelijk om een certificaat te uploaden dat is ondertekend door een interne certificeringsinstantie (CA) of een bekende CA.

Om het zelf-ondertekende certificaat te maken, navigeer naar **Apparaten > Certificaten**.

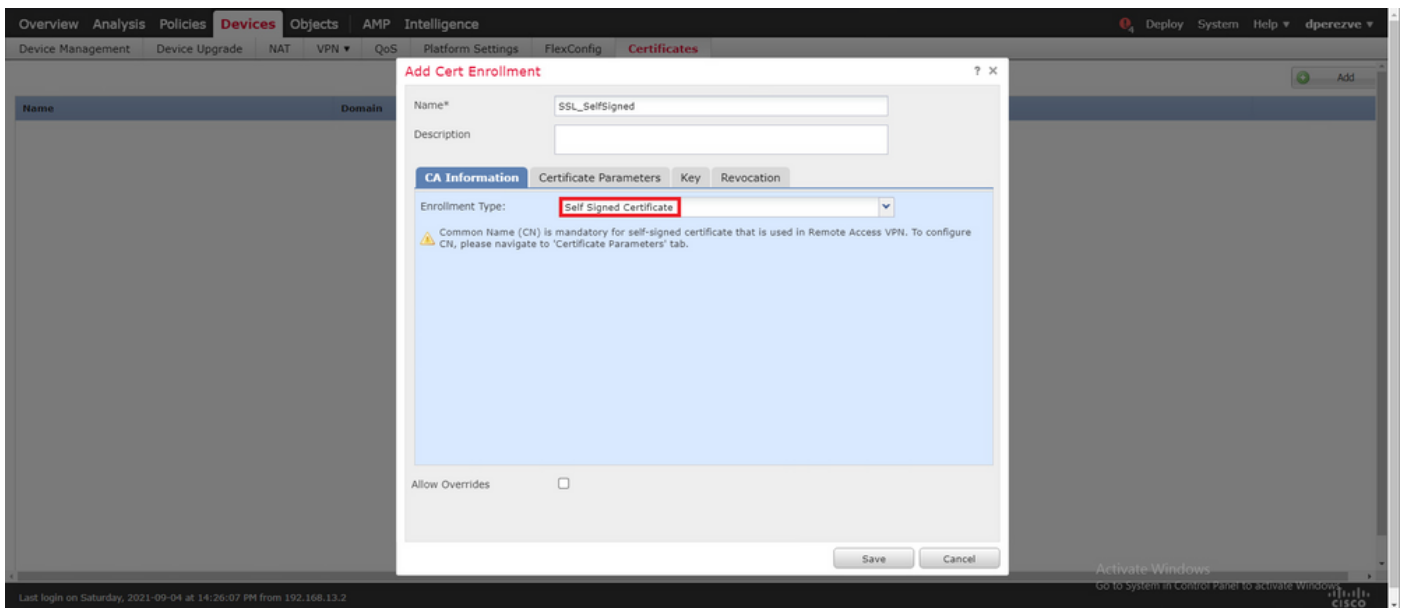


Selecteer de knop **Add** en kies vervolgens de FTD die in het vervolgkeuzemenu **Apparaat** in het venster **Add New Certificate (Nieuw certificaat toevoegen)** wordt gebruikt.

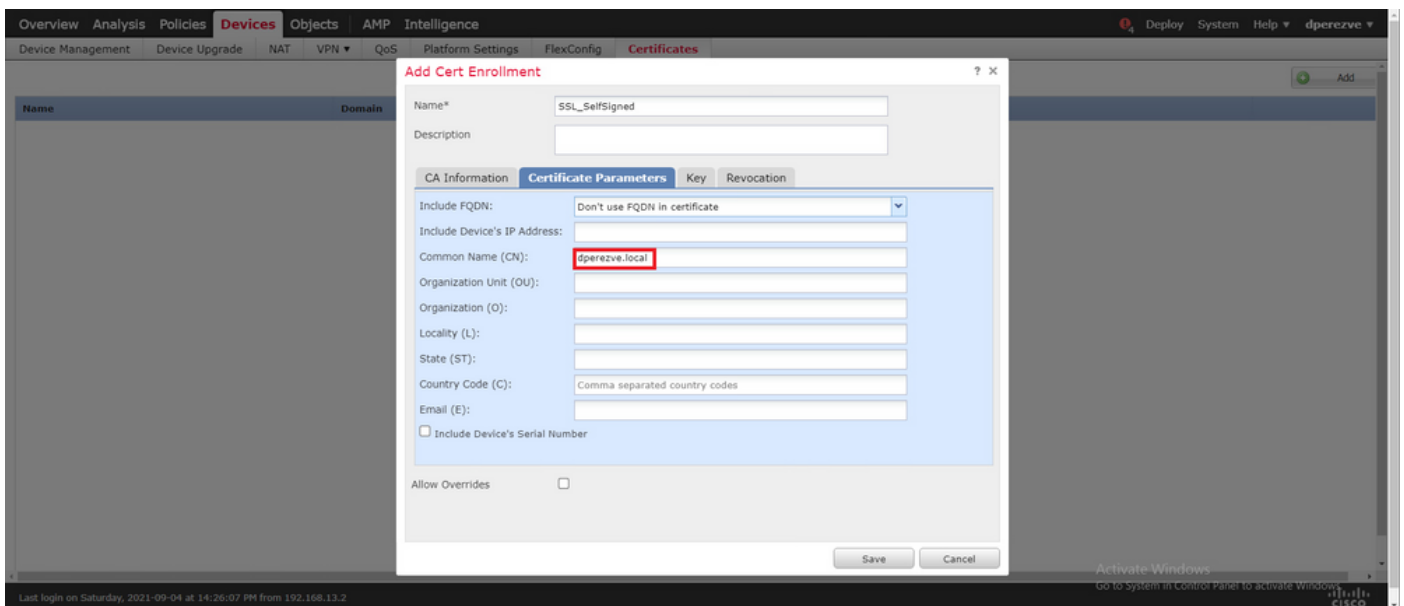


Selecteer de knop **Toegang toevoegen** (groen + symbool) om een nieuw inschrijvingsobject te maken. Nu, in het venster **Add Cert Enrollment**, geef een naam voor het object toe en kies

Zelfgetekend Certificaat in het vervolgkeuzemenu Invoertype.



Ten slotte is het voor zelf ondertekende certificaten verplicht een gemeenschappelijke naam (GN) te hebben. Navigeer naar het tabblad **certificaatparameters** om een GN te definiëren.



Selecteer de knoppen **Opslaan** en **Toevoegen** na een paar seconden. Het nieuwe certificaat moet aan de certificaatlijst worden toegevoegd.

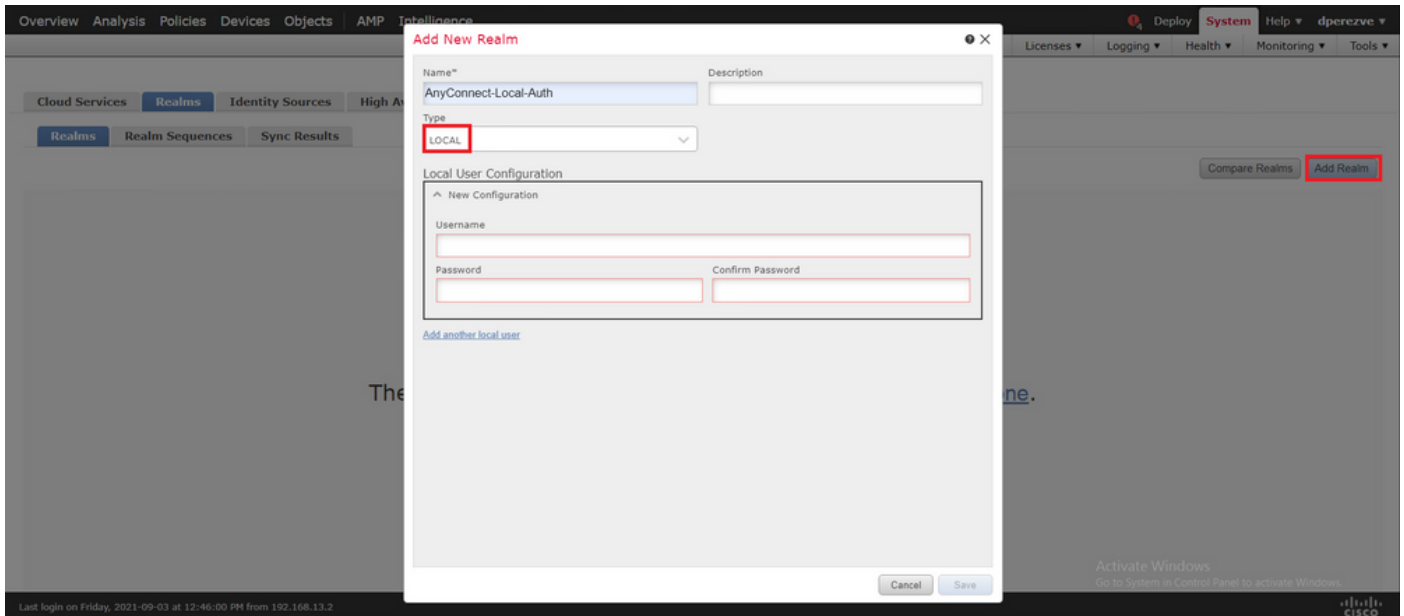


Stap 4. Lokaal antwoord op FMC maken

De lokale gebruikersdatabse en de respectievelijke wachtwoorden worden in een lokaal veld opgeslagen. Om het lokale rijk te maken navigeer naar **Systeem > Integratie > Realms**.

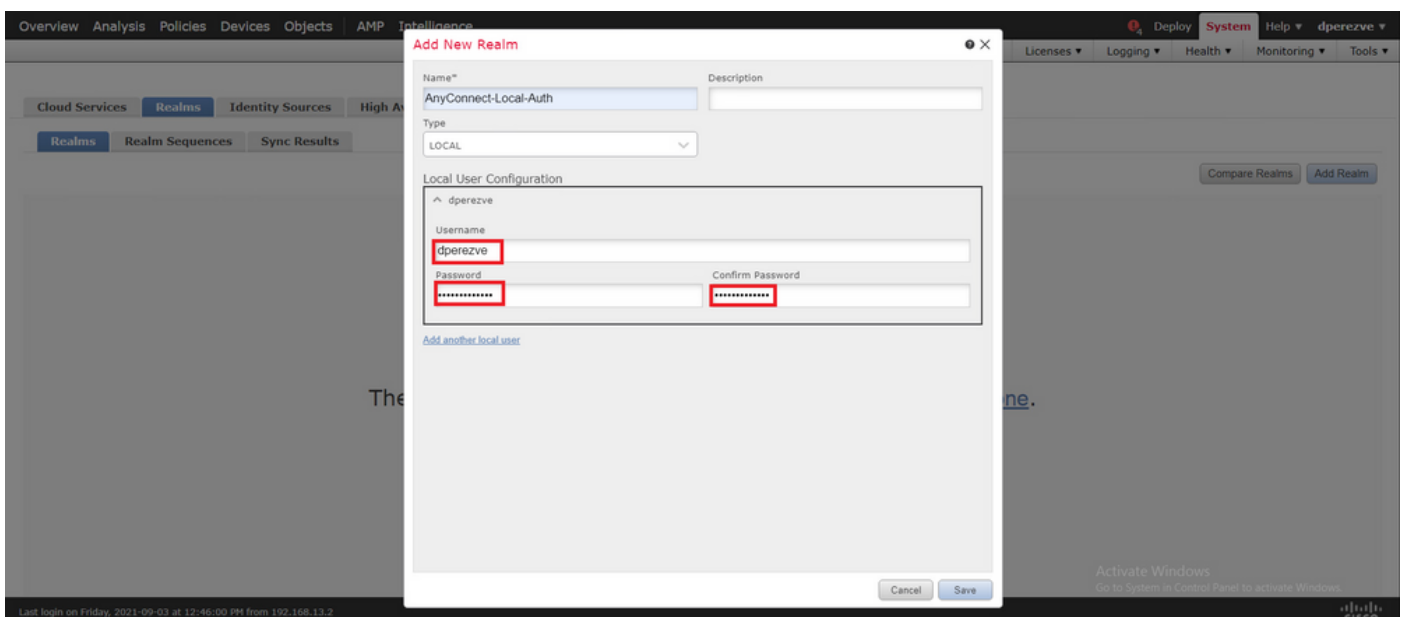


Selecteer de knop **Opnieuw toevoegen**. In het venster **Add New Realm** toewijzen een naam en selecteer **LOCAL** optie in het vervolgkeuzemenu **Type**.



Gebruikersrekeningen en wachtwoorden die in het gedeelte **Local User Configuration** zijn gemaakt.

Opmerking: Wachtwoorden moeten ten minste één hoofdletter, één kleine letter, één nummer en één speciaal teken hebben.



Veranderingen opslaan en een nieuw gebied moeten aan de lijst met bestaande gebieden worden toegevoegd.

Name	Description	Type	Domain	AD Primary Domain	Base DN	State
AnyConnect-Local-Auth		LOCAL	Global			Enabled

Stap 5. Het configureren van SSL AnyConnect

Om SSL AnyConnect te configureren navigeer naar **Apparaten > VPN > Externe toegang**.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	
Device Management	Device Upgrade	NAT	VPN > Remote Access	QoS	Platform Settings	FlexConfig	Certificates

Selecteer de knop **Toevoegen** om een nieuw VPN-beleid te maken. Definieer een naam voor het verbindingsprofiel, selecteer SSL selectieteken en kies de FTD in hand als het beoogde apparaat, alles moet in de sectie **Beleidsstowijzing** in de wizard **Afstandsbeleid van VPN** worden geconfigureerd.

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

Name: *

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices: Available Devices

- ftdv-dpereze
- ftdva-dpereze

Selected Devices

- ftdva-dpereze

Authentication Server
Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.

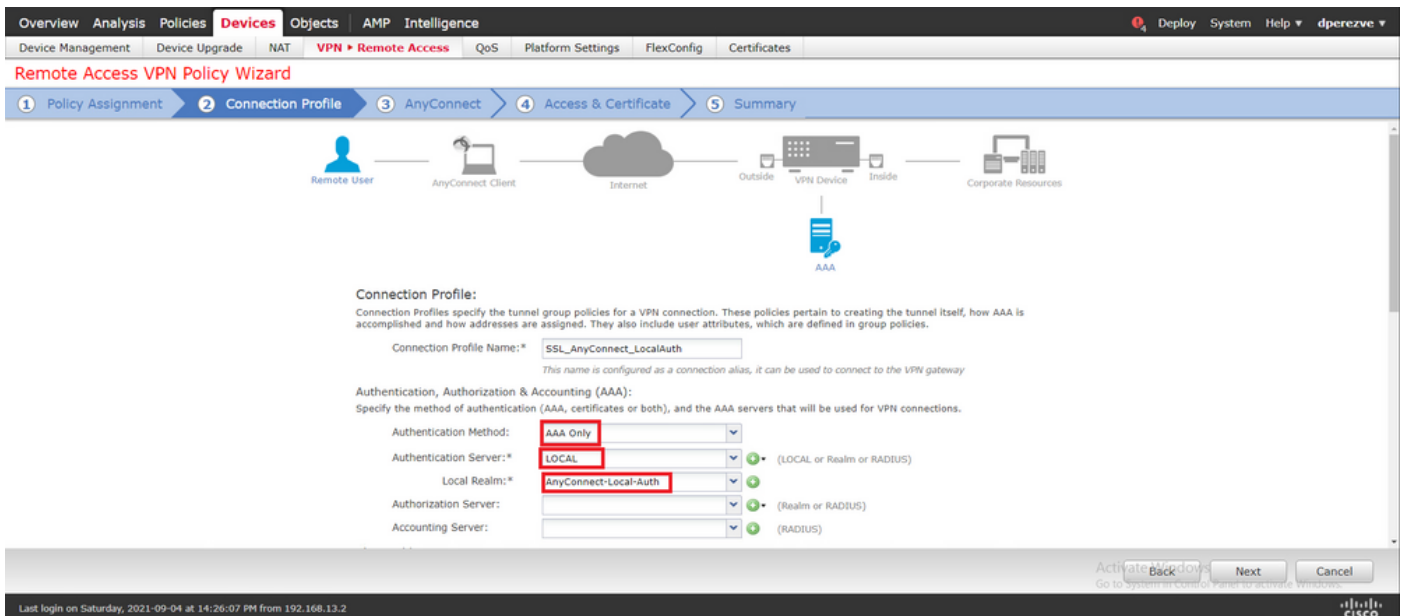
AnyConnect Client Package
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface
Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

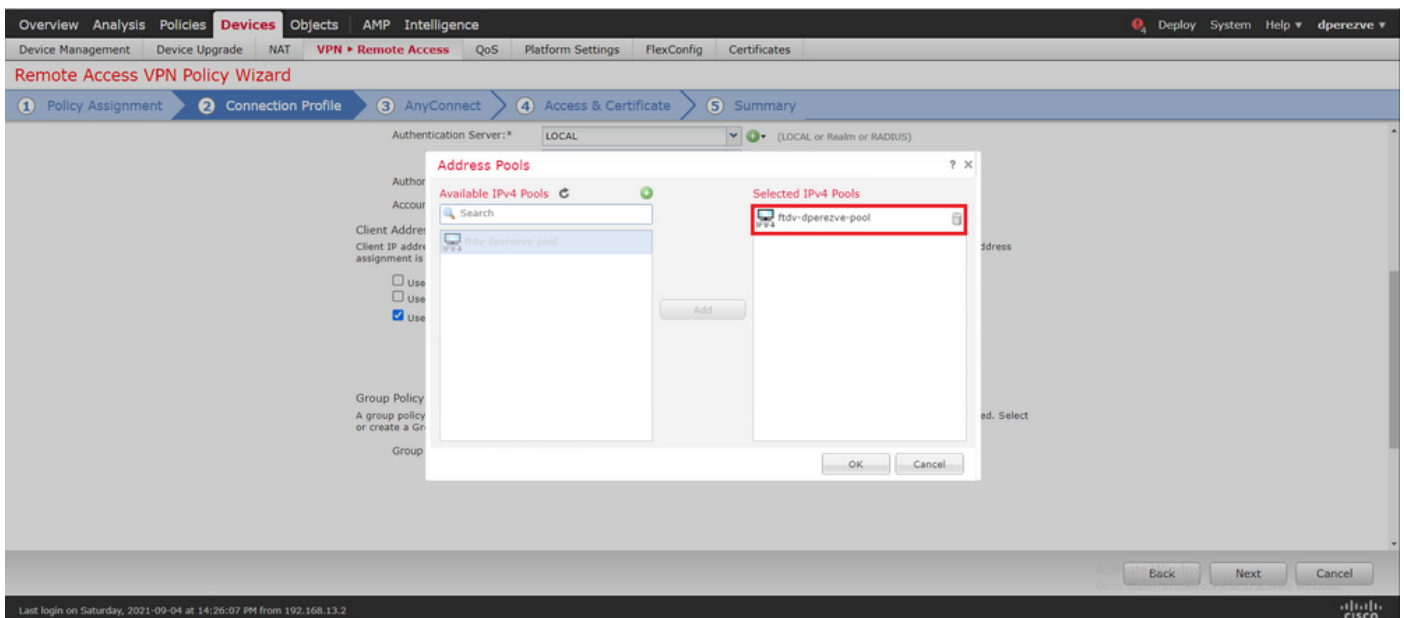
Activate Wizard | Back | Next | Cancel

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

Selecteer **Volgende** om naar de configuratie van het **verbindingsprofiel** te gaan. Definieer een naam voor het verbindingsprofiel en selecteer **AAA Alleen** als de authenticatiemethode, en selecteer vervolgens in het vervolgkeuzemenu **Verificatieserver LOCAL** en selecteer vervolgens het lokale veld dat is gemaakt in Stap 4 in het vervolgkeuzemenu Local Real.



Scroll-down op dezelfde pagina, selecteer vervolgens het potlood pictogram in het gedeelte IPv4-adresgroep om de IP pool te definiëren die door AnyConnect-klanten wordt gebruikt.



Selecteer **Volgende** om naar het gedeelte **AnyConnect** te gaan. Selecteer nu de AnyConnect-afbeelding die in Stap 2 is geüpload.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

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

AnyConnect Client Image
The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#) [Show Re-order buttons](#)

AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/> AnyConnect_Win_4.10	anyconnect-win-4.10.01075-webdeploy-k9.pkg	Windows

Activate Windows Go to Settings to activate Windows. Back Next Cancel

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

Selecteer **Volgende** om naar het gedeelte **Toegang en certificaat** te gaan. Selecteer in het vervolkeuzemenu **Interfacegroep/Security Zone** de interface waar AnyConnect moet worden ingeschakeld en selecteer vervolgens in het vervolkeuzemenu **certificaatschrijving** het certificaat dat in Stap 3 is gemaakt.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

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

Network Interface for Incoming VPN Access
Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Activate Windows Go to Settings to activate Windows. Back Next Cancel

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

Selecteer ten slotte **Volgende** om een samenvatting van de AnyConnect-configuratie te zien.

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-dperezve

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): ftdv-dperezve-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'

Buttons: Back, Finish, Cancel

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

Als alle instellingen correct zijn, selecteert u **Voltooien** en implementeert u wijzigingen in FTD.

Deployment | Deployment History

1 device selected
Deploy time: Estimate

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

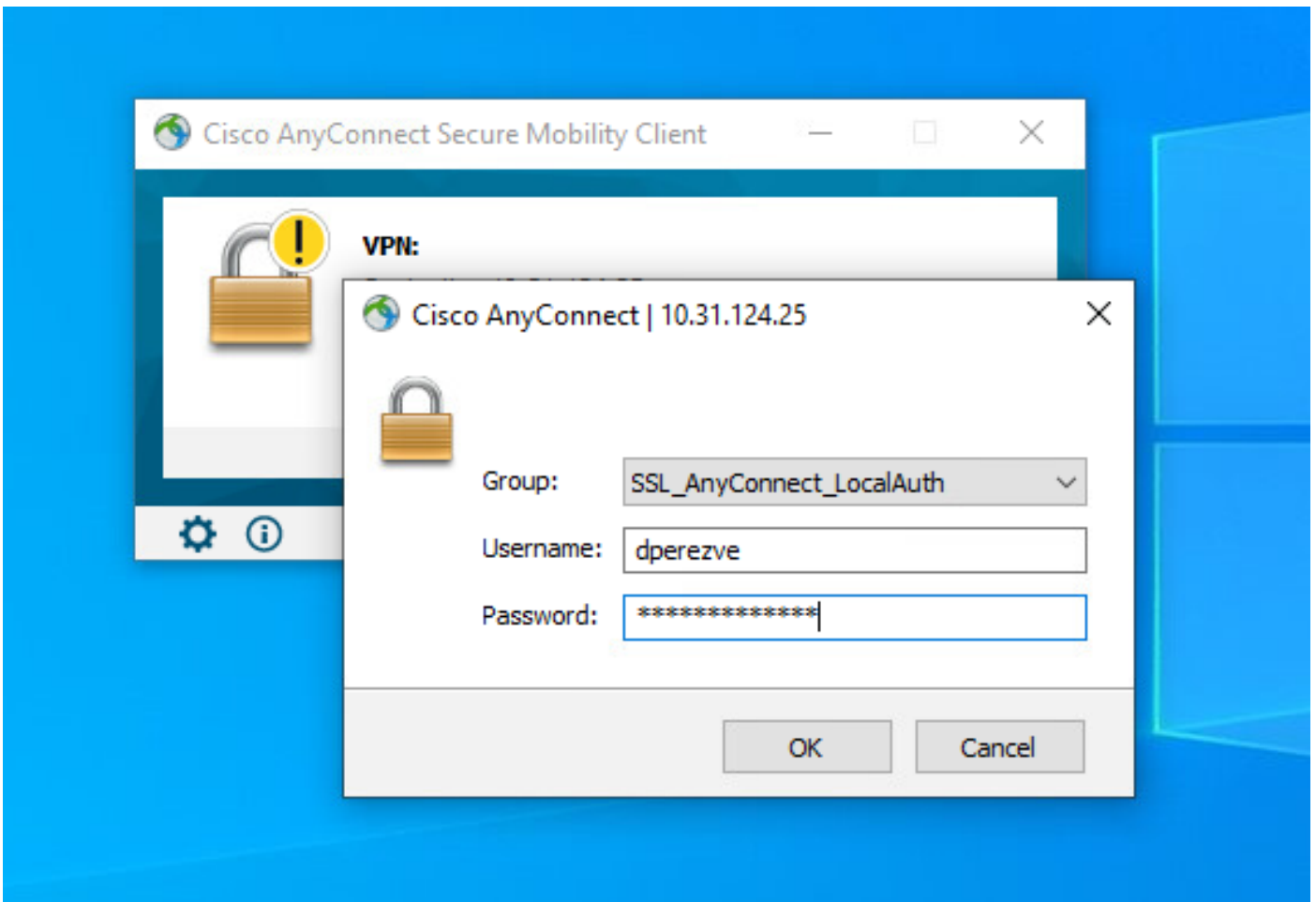
Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
ftdvha-dperezve	dperezve		FTD		Sep 7, 2021 2:44 PM		Pending

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

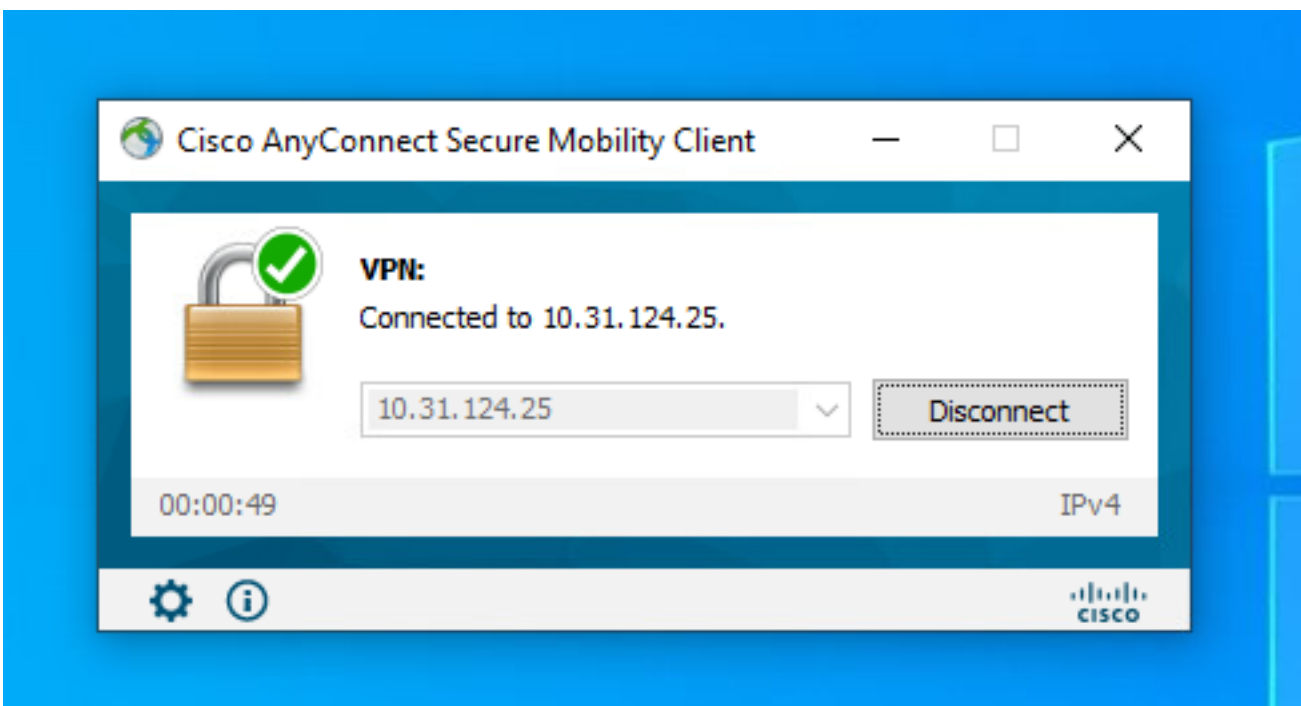
Footer: Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Verifiëren

Nadat de implementatie met succes is voltooid, kunt u een AnyConnect-verbinding van Windows client naar FTD starten. De gebruikersnaam en het wachtwoord die gebruikt worden in de authenticatie-prompt moeten hetzelfde zijn als in Stap 4.



Zodra de aanmeldingsgegevens door FTD zijn goedgekeurd, moet AnyConnect-app de aangesloten status weergeven.



Vanaf FTD kunt u **show vpn-sessiondb** uitvoeren om de opdracht **aan te sluiten** om de AnyConnect-sessies weer te geven die momenteel actief zijn in de Firewall.

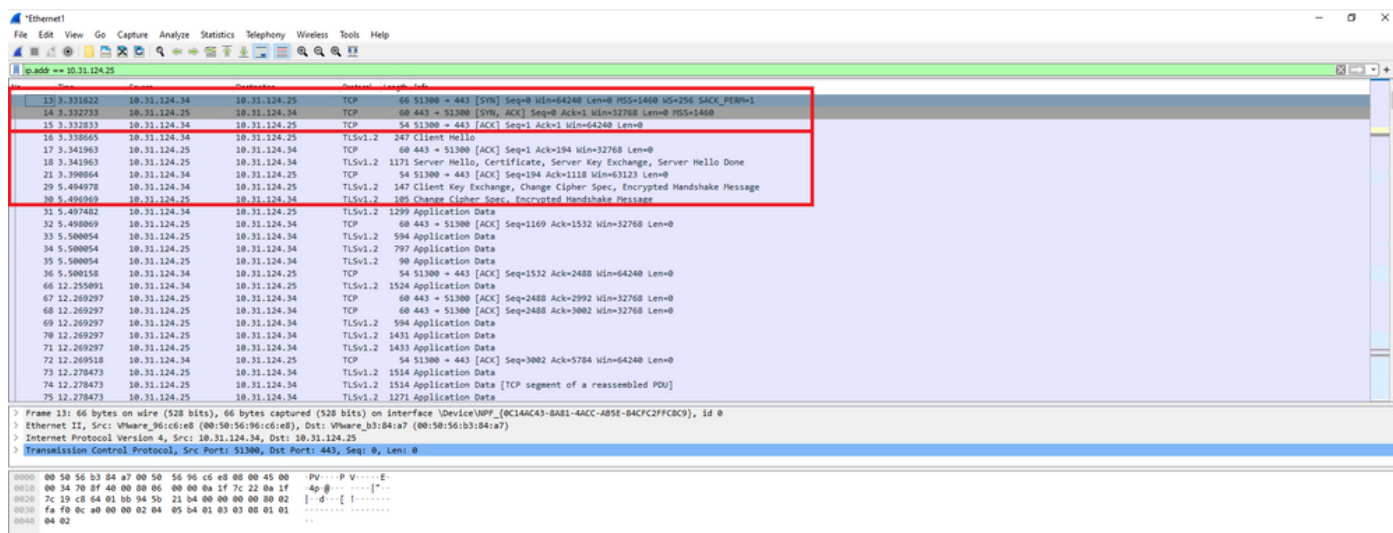
Assigned IP : 172.16.13.1 Public IP : 10.31.124.34 Protocol : AnyConnect-Parent SSL-Tunnel DTLs-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLs-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLs-Tunnel: (1)SHA384 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

Problemen oplossen

Start debug webVPN anyconnect 255 opdracht op FTD om SSL-verbindingsstroom op FTD te zien.

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

Naast AnyConnect debugs kan ook de verbindingstroom met TCP-pakketvastlegging worden waargenomen. Hieronder zie je een voorbeeld van een succesvolle verbinding. Er wordt een regelmatige drie handdruk tussen Windows client en FTD voltooid, gevolgd door een SSL-handdruk die wordt gebruikt om ciphers goed te keuren.



Nadat de protocol handtekeningen zijn gemaakt, moet FTD geloofsbriefen valideren met informatie die in lokaal gebied is opgeslagen.

Verzamel de DART-bundel en neem contact op met Cisco TAC voor verder onderzoek.