

Konfigurieren von SSL AnyConnect mit lokaler Authentifizierung auf von FMC verwaltetem FTD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurationen](#)

[Schritt 1: Lizenzierung überprüfen](#)

[Schritt 2: AnyConnect-Paket auf FMC hochladen](#)

[Schritt 3: Erstellen eines selbstsignierten Zertifikats](#)

[Schritt 4: Lokalen Bereich auf FMC erstellen](#)

[Schritt 5: Konfigurieren von SSL AnyConnect](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Cisco AnyConnect mit lokaler Authentifizierung auf einer Cisco FirePOWER Threat Defense (FTD) konfiguriert wird, die vom Cisco FirePOWER Management Center (FMC) verwaltet wird. Im Beispiel unten wird Secure Sockets Layer (SSL) zum Erstellen eines Virtual Private Network (VPN) zwischen FTD und einem Windows 10-Client verwendet.

Mitarbeiter: Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SSL AnyConnect-Konfiguration über FMC
- Konfiguration von FirePOWER-Objekten über FMC
- SSL-Zertifikate für FirePOWER

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FTD Version 7.0.0 (Build 94)
- Cisco FMC Version 7.0.0 (Build 94)
- Cisco AnyConnect Secure Mobility Client 4.10.01075

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ab Version 7.0.0 unterstützt von FMC verwaltetes FTD die lokale Authentifizierung für AnyConnect-Clients. Dies kann entweder als primäre Authentifizierungsmethode oder als Fallback definiert werden, falls die primäre Methode fehlschlägt. In diesem Beispiel wird die lokale Authentifizierung als primäre Authentifizierung konfiguriert.

Vor dieser Softwareversion war die lokale AnyConnect-Authentifizierung auf FTD nur auf dem Cisco FirePOWER Device Manager (FDM) verfügbar.

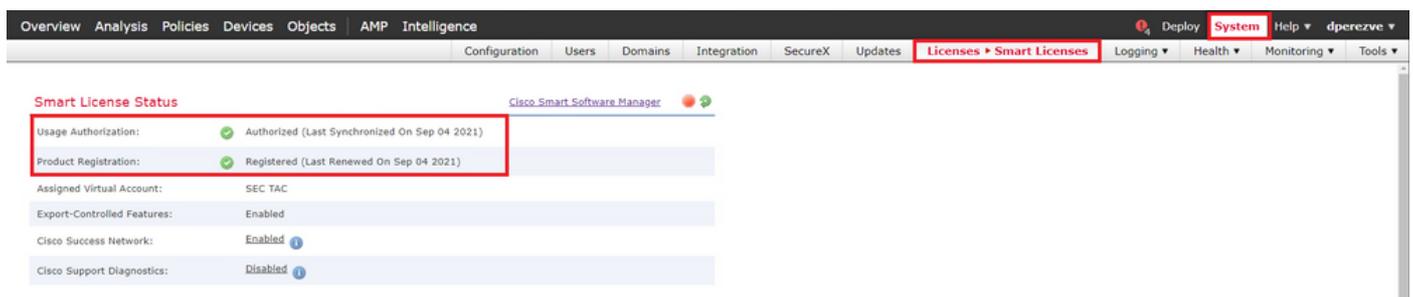
Konfigurieren

Konfigurationen

Schritt 1: Lizenzierung überprüfen

Bevor AnyConnect konfiguriert werden kann, muss das FMC registriert und mit dem Smart Licensing Portal kompatibel sein. AnyConnect kann nicht bereitgestellt werden, wenn FTD keine gültige Plus-, Apex- oder VPN Only-Lizenz besitzt.

Navigieren Sie zu **System > Licenses > Smart Licenses (System > Lizenzen > Smart Licenses)**, um zu überprüfen, ob das FMC registriert ist und dem Smart Licensing Portal entspricht.



Scrollen Sie auf derselben Seite unten im **Smart Licenses**-Diagramm nach unten, um die verschiedenen verfügbaren AnyConnect-Lizenzen und die jeweils abonnierten Geräte anzuzeigen. Validieren Sie, ob die jeweilige FTD in einer dieser Kategorien registriert ist.

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.

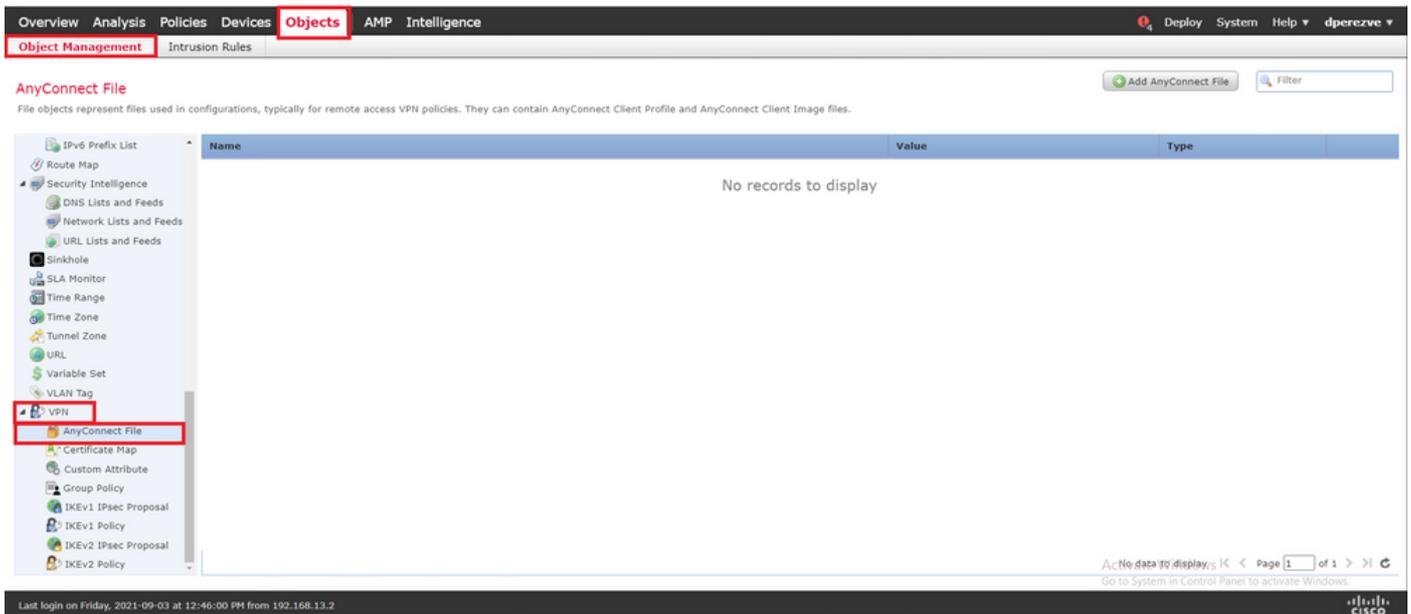
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Schritt 2: AnyConnect-Paket auf FMC hochladen

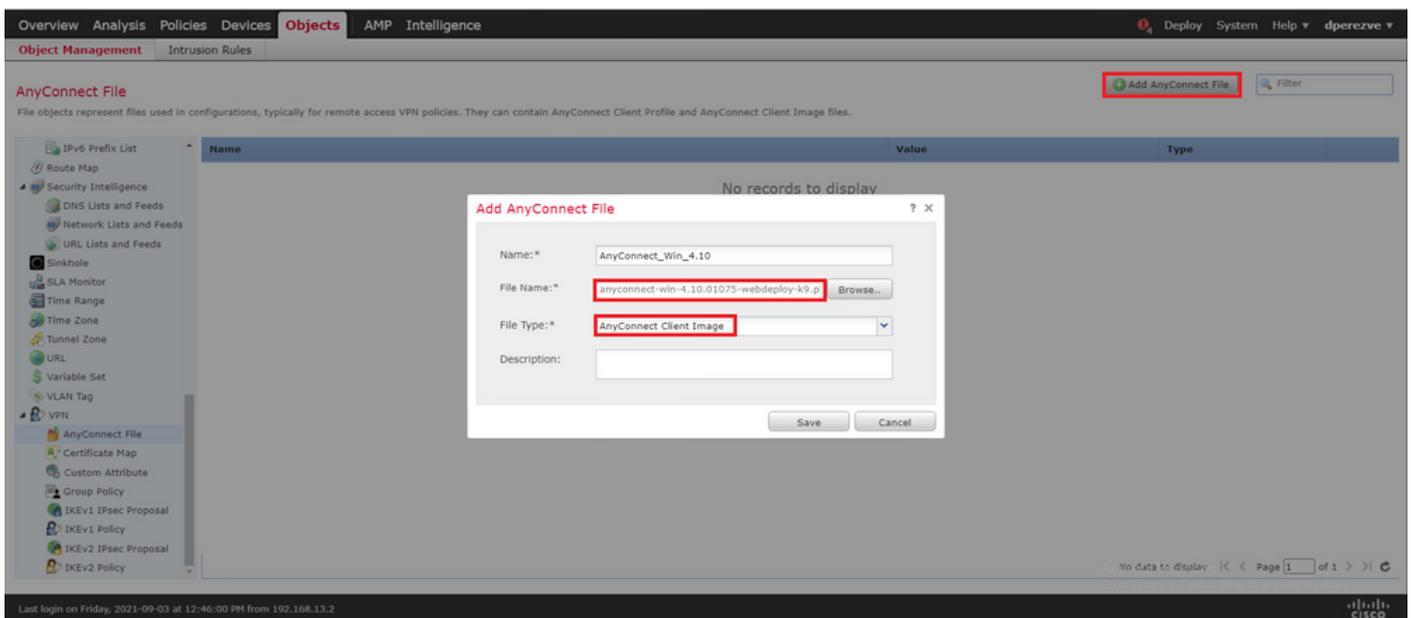
Laden Sie das AnyConnect Headend-Bereitstellungspaket für Windows von cisco.com herunter.

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	 

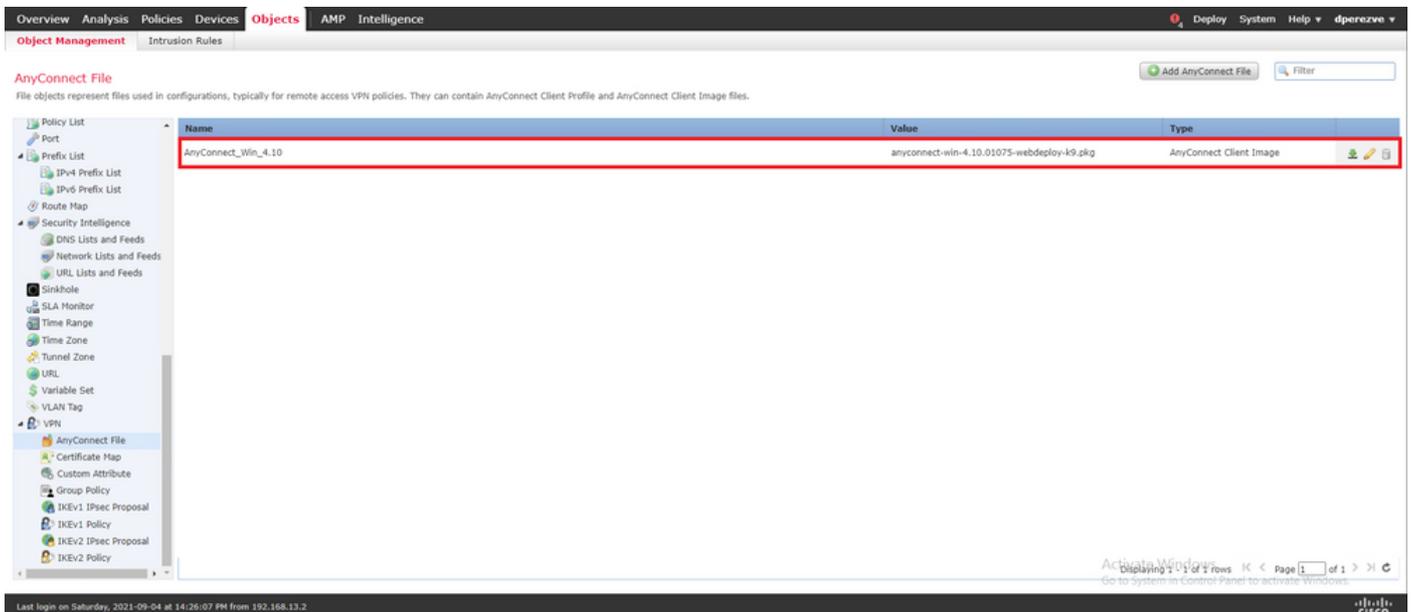
Um das AnyConnect-Image hochzuladen, navigieren Sie zu **Objects > Object Management** und wählen Sie **AnyConnect File** unter der **VPN-Kategorie** im Inhaltsverzeichnis aus.



Wählen Sie die Schaltfläche **AnyConnect-Datei hinzufügen** aus. Weisen Sie im Fenster **AnyConnect-Datei hinzufügen** einen Namen für das Objekt zu, und wählen Sie dann **Durchsuchen** aus, um das AnyConnect-Paket auszuwählen und schließlich **AnyConnect Client Image** im Dropdown-Menü als Dateityp auszuwählen.



Wählen Sie die Schaltfläche **Speichern**, das Objekt muss der Objektliste hinzugefügt werden.



Schritt 3: Erstellen eines selbstsignierten Zertifikats

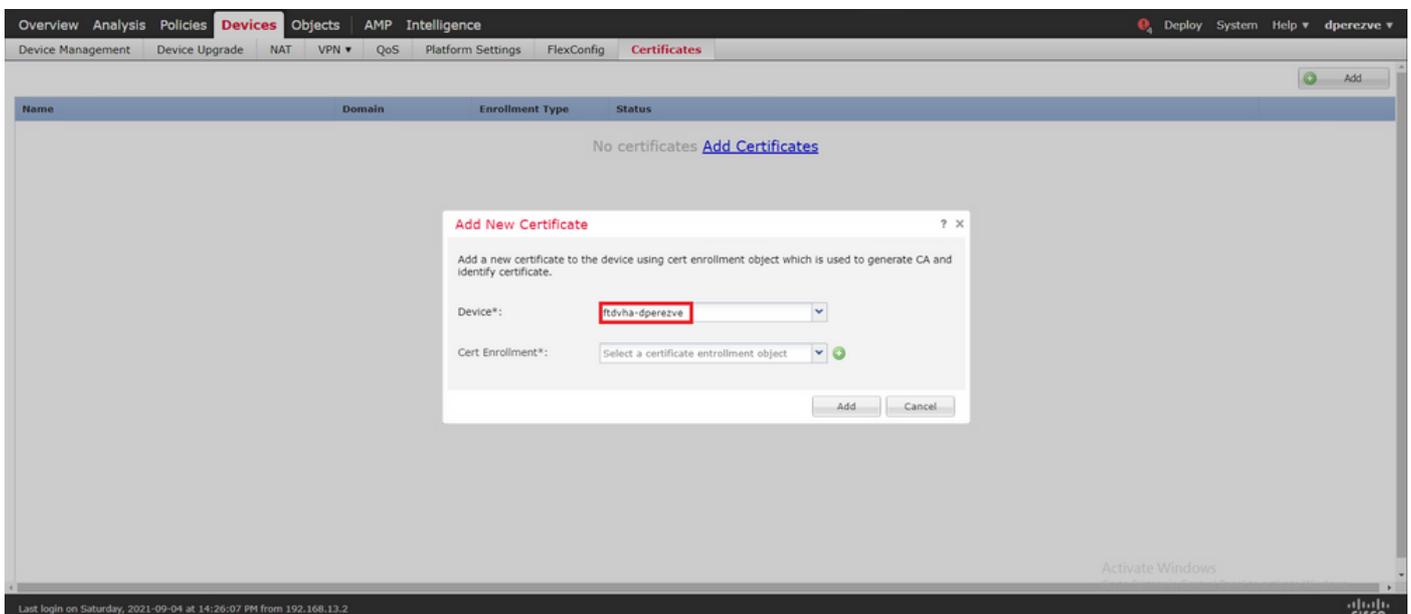
Für SSL AnyConnect ist die Verwendung eines gültigen Zertifikats im SSL-Handshake zwischen VPN-Headend und Client erforderlich.

Anmerkung: In diesem Beispiel wird zu diesem Zweck ein selbstsigniertes Zertifikat generiert. Neben selbstsignierten Zertifikaten ist es jedoch möglich, ein Zertifikat hochzuladen, das entweder von einer internen Zertifizierungsstelle (Certificate Authority, CA) oder einer bekannten Zertifizierungsstelle signiert wurde.

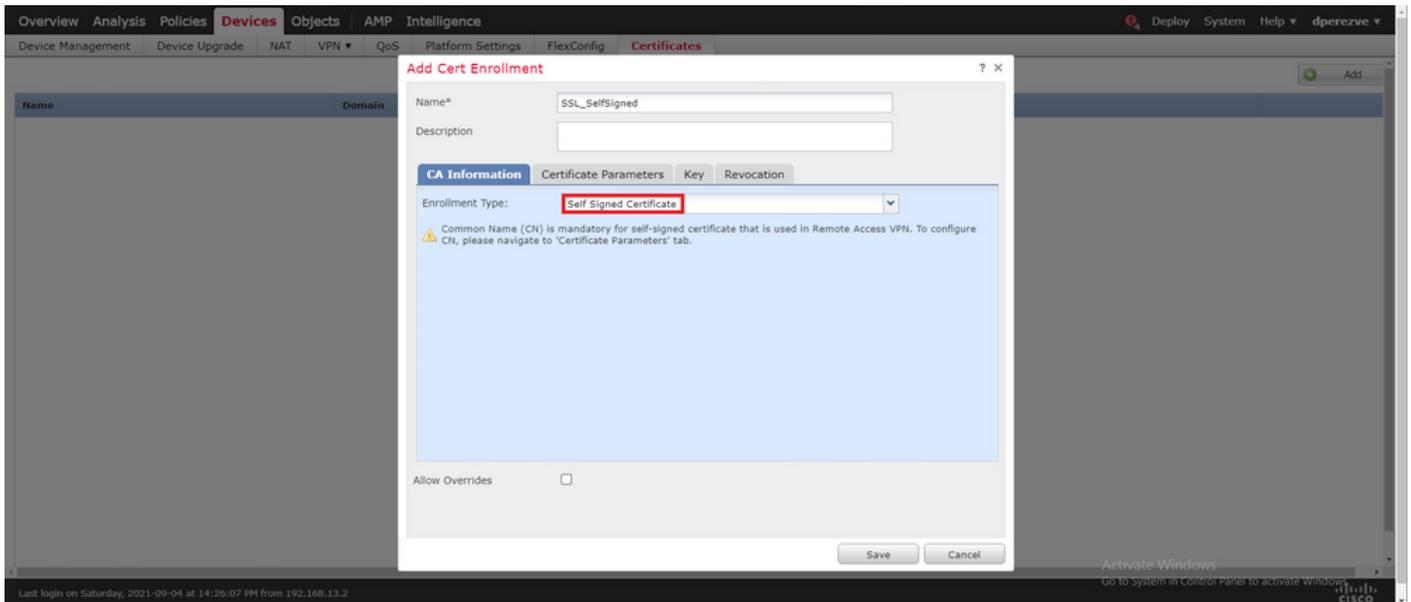
Um ein selbstsigniertes Zertifikat zu erstellen, navigieren Sie zu **Devices > Certificates (Geräte > Zertifikate)**.



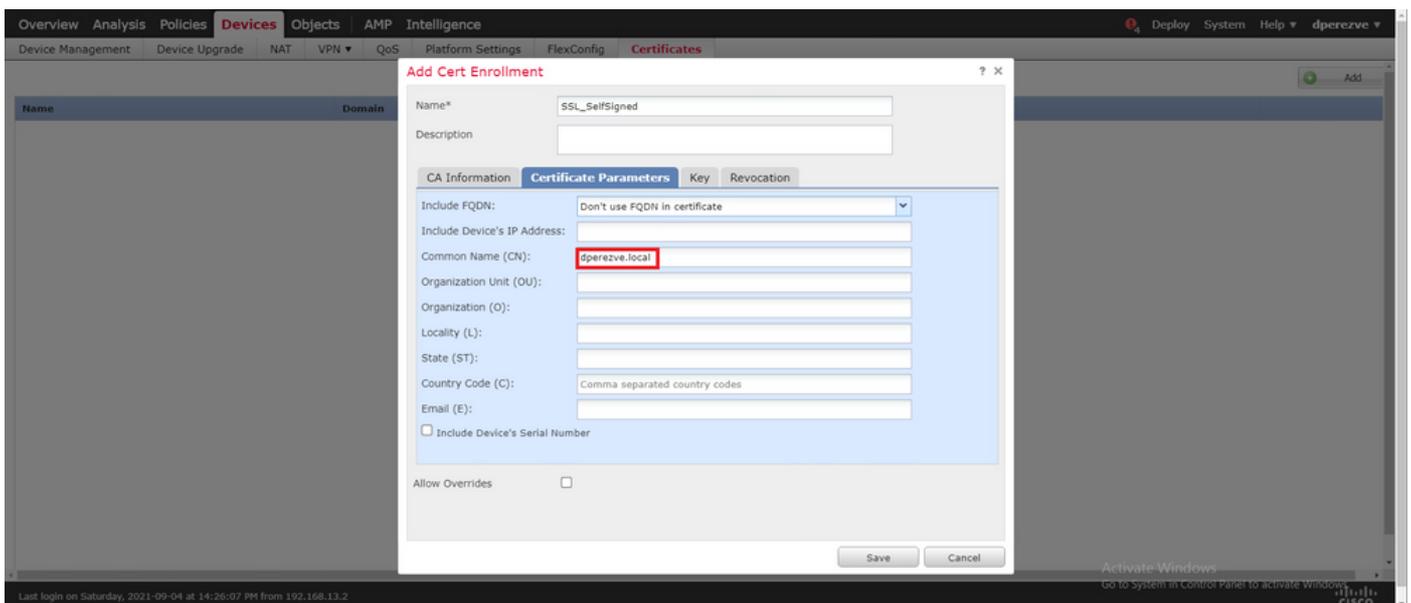
Wählen Sie die Schaltfläche **Hinzufügen** und anschließend im Dropdown-Menü **Gerät** im Fenster **Neues Zertifikat hinzufügen** die entsprechende FTD aus.



Wählen Sie die Schaltfläche **Add Cert Enrollment** (grünes + Symbol), um ein neues Anmeldeobjekt zu erstellen. Weisen Sie nun im Fenster **Add Cert Enrollment (Registrierung hinzufügen)** einen Namen für das Objekt zu, und wählen Sie im Dropdown-Menü **Anmeldungstyp** die Option **Self Signed Certificate (selbstsigniertes Zertifikat)** aus.



Bei selbstsignierten Zertifikaten ist es schließlich erforderlich, einen gemeinsamen Namen (CN) zu haben. Navigieren Sie zur Registerkarte **Zertifikatsparameter**, um einen CN zu definieren.



Wählen Sie die Schaltflächen **Speichern** und **Hinzufügen**, und nach einigen Sekunden muss das neue Zertifikat der Zertifikatsliste hinzugefügt werden.



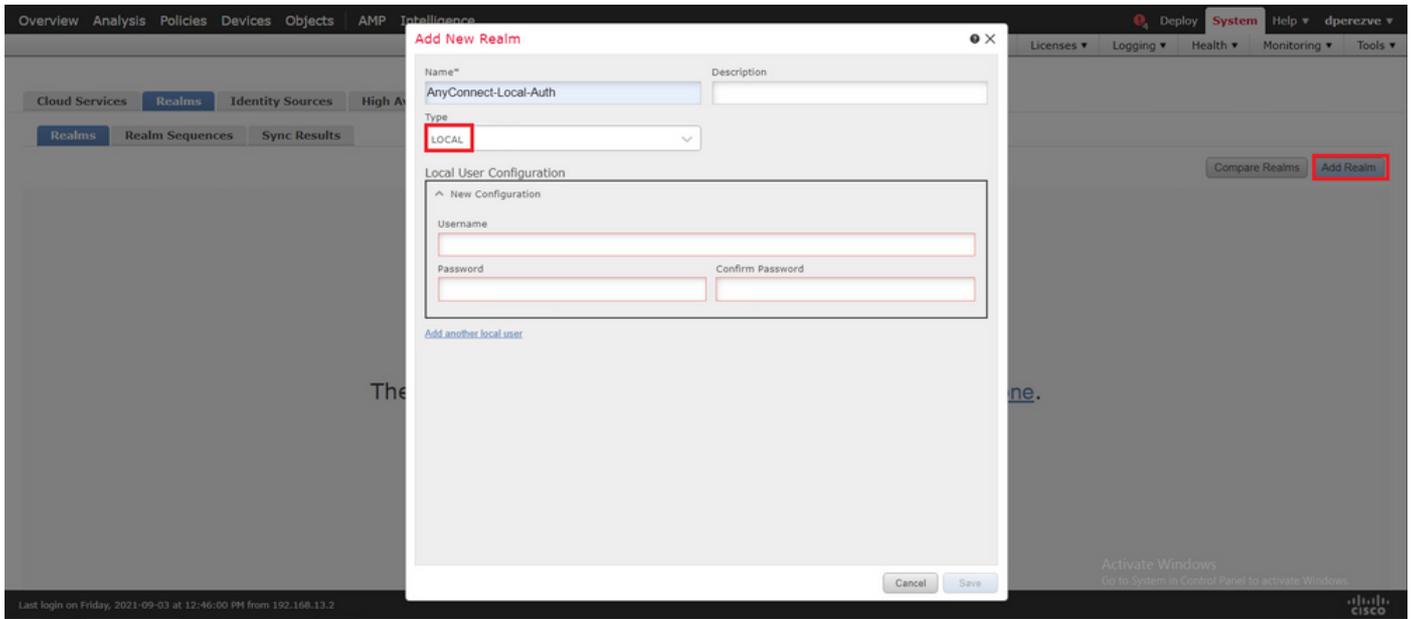
Schritt 4: Lokalen Bereich auf FMC erstellen

Die lokale Benutzerdatenbank und die entsprechenden Kennwörter werden in einem lokalen

Bereich gespeichert. Um den lokalen Bereich zu erstellen, navigieren Sie zu **System > Integration > Realms**.

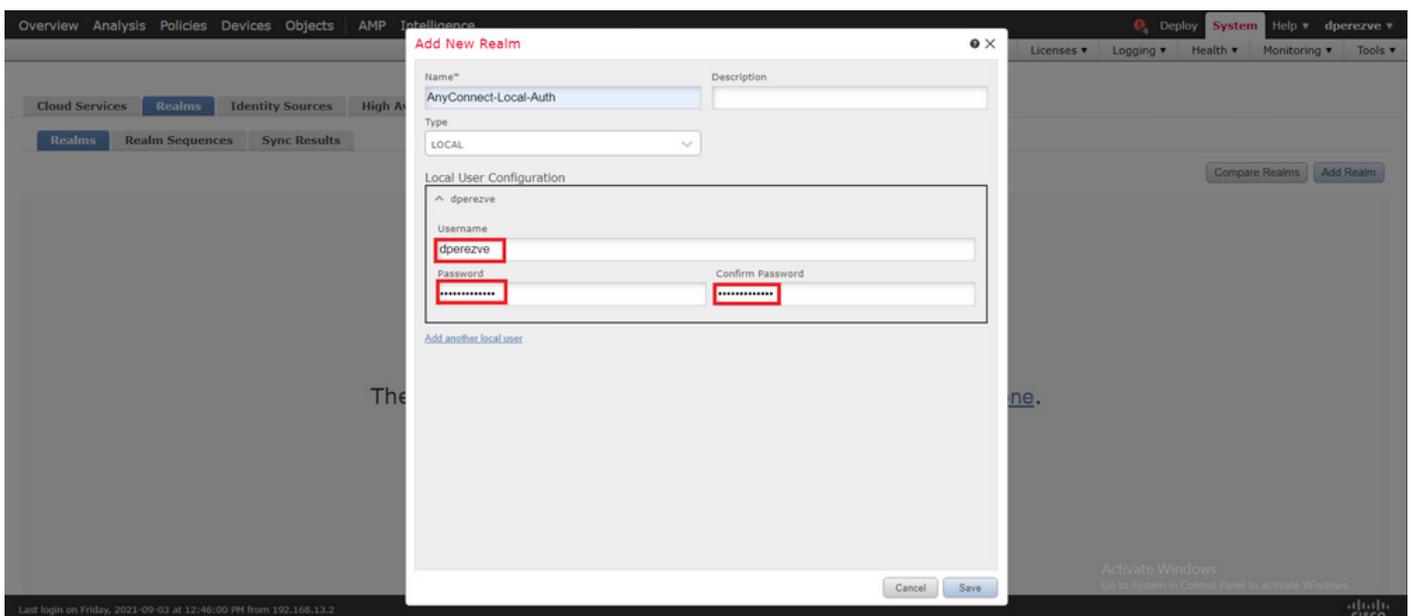


Wählen Sie die Schaltfläche **Bereich hinzufügen aus**. Weisen Sie im Fenster **Neuen Bereich hinzufügen** einen Namen zu, und wählen Sie im Dropdown-Menü **Typ** die Option **LOCAL** aus.

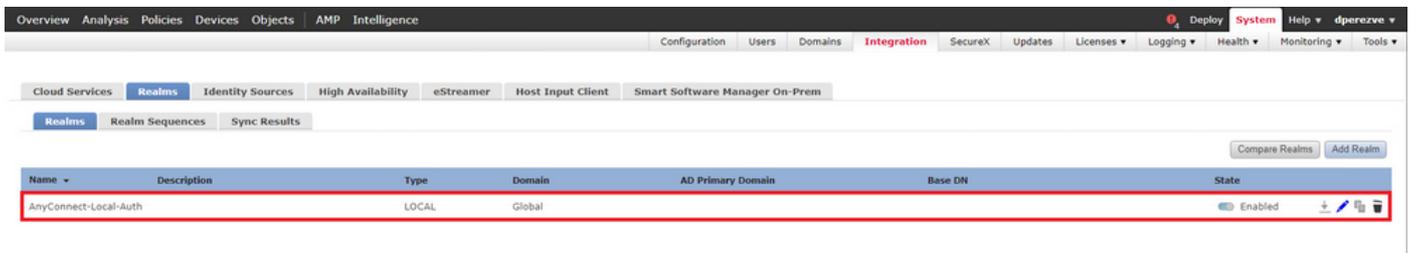


Benutzerkonten und Kennwörter, die im Abschnitt **"Lokale Benutzerkonfiguration"** erstellt wurden.

Hinweis: Kennwörter müssen aus mindestens einem Großbuchstaben, einem Kleinbuchstaben, einer Zahl und einem Sonderzeichen bestehen.



Änderungen speichern und neuer Bereich muss der Liste der vorhandenen Bereiche hinzugefügt werden.

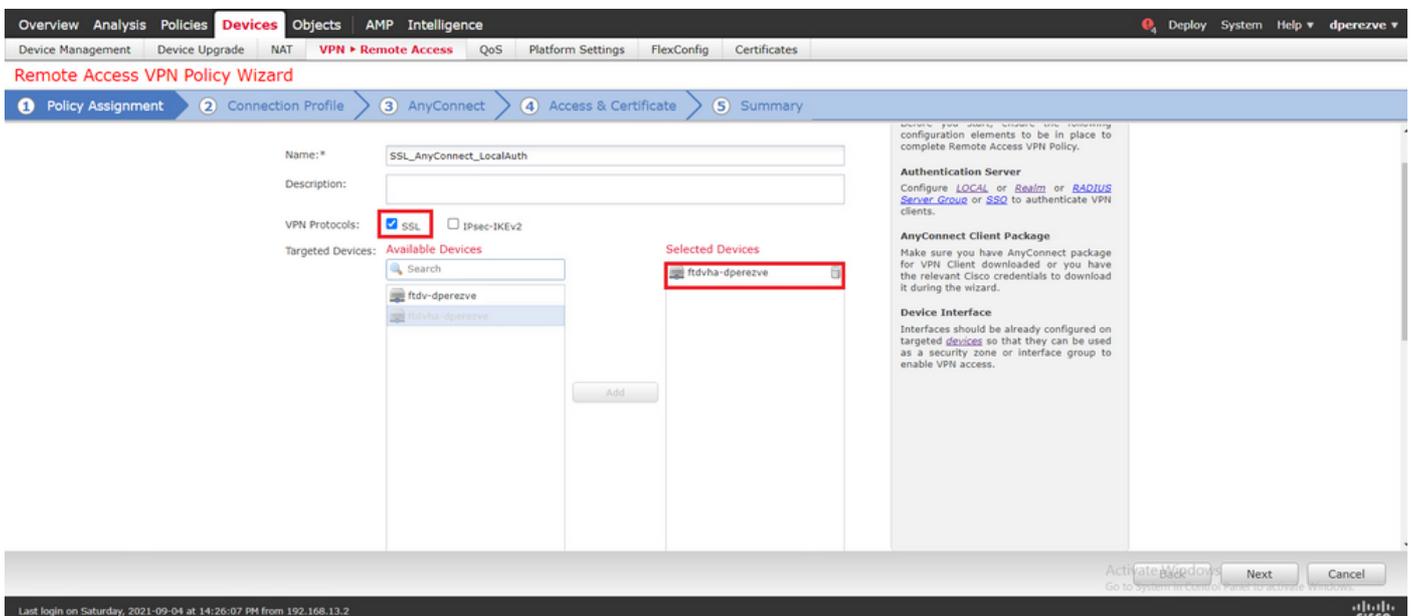


Schritt 5: Konfigurieren von SSL AnyConnect

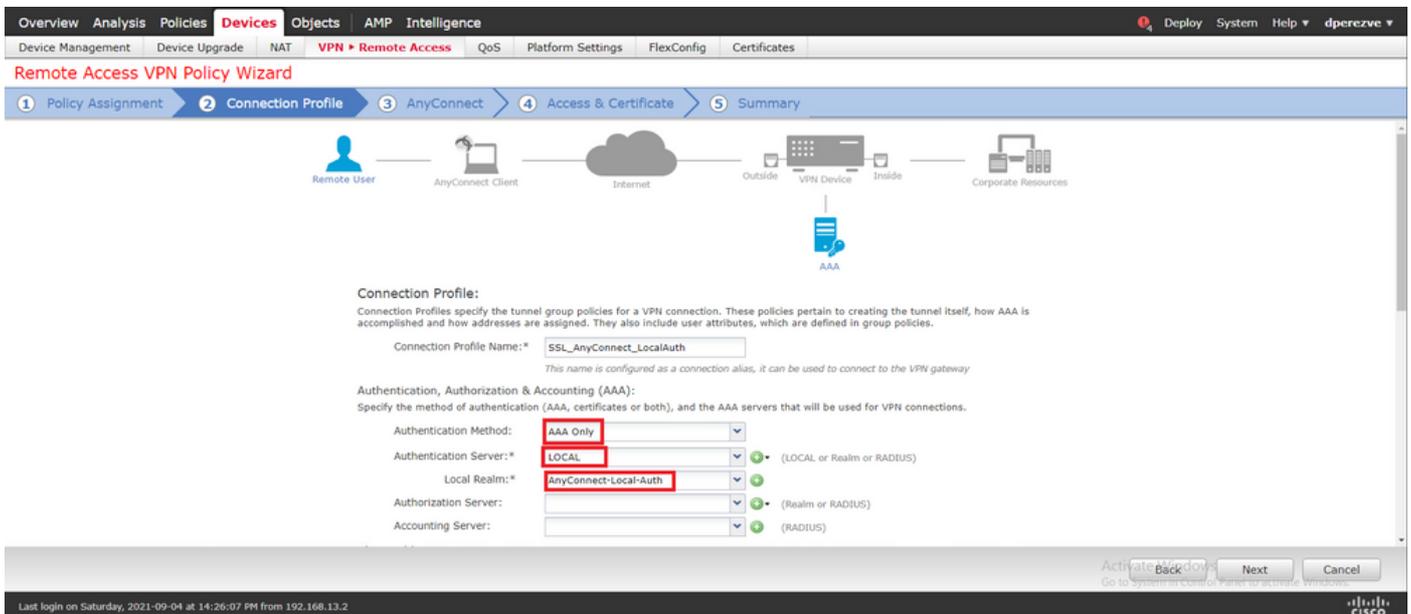
Um SSL AnyConnect zu konfigurieren, navigieren Sie zu **Devices > VPN > Remote Access**.



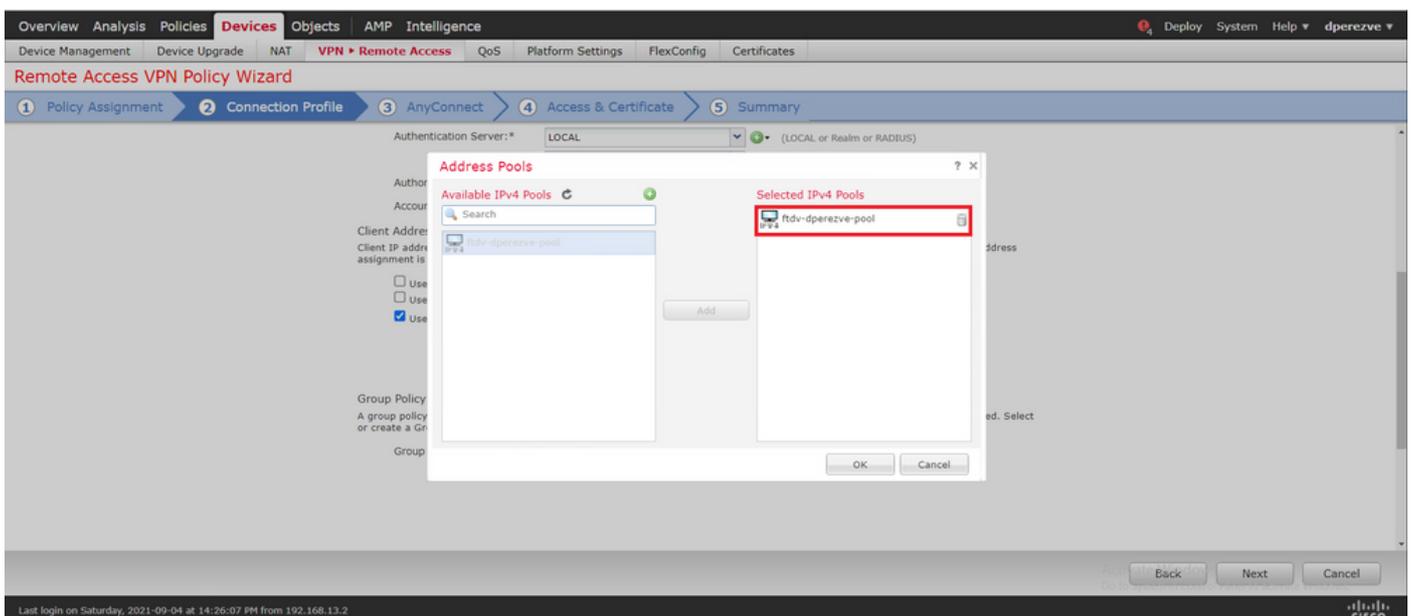
Wählen Sie die Schaltfläche **Hinzufügen**, um eine neue VPN-Richtlinie zu erstellen. Legen Sie einen Namen für das Verbindungsprofil fest, aktivieren Sie das Kontrollkästchen **SSL**, und wählen Sie das jeweilige FTD als Zielgerät aus. Im Abschnitt **Richtlinienzuweisung** im Assistenten für **VPN-Remotezugriffsrichtlinien** muss alles konfiguriert werden.



Wählen Sie **Weiter**, um zur **Verbindungsprofilkonfiguration** zu wechseln. Definieren Sie einen Namen für das Verbindungsprofil, und wählen Sie **AAA Only** als Authentifizierungsmethode aus. Wählen Sie dann im **Authentication Server**-Dropdown-Menü die Option **LOCAL** aus, und wählen Sie schließlich im Dropdown-Menü Local Realm (Lokaler Bereich) den in Schritt 4 erstellten lokalen Bereich aus.



Scrollen Sie auf derselben Seite nach unten, und wählen Sie dann das Bleistiftsymbol im Abschnitt **IPv4-Adresspool** aus, um den von AnyConnect-Clients verwendeten IP-Pool zu definieren.



Wählen Sie **Weiter**, um zum Abschnitt **AnyConnect** zu wechseln. Wählen Sie jetzt das in Schritt 2 hochgeladene AnyConnect-Image aus.

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 Cisco

Wählen Sie **Weiter**, um zum Abschnitt **"Zugriff und Zertifikat"** zu wechseln. Wählen Sie im Dropdown-Menü **Schnittstellengruppe/Sicherheitszone** die Schnittstelle aus, für die AnyConnect aktiviert werden soll. Wählen Sie anschließend im Dropdown-Menü **Zertifikatregistrierung** das in Schritt 3 erstellte Zertifikat aus.

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 Cisco

Wählen Sie abschließend **Weiter**, um eine Zusammenfassung der AnyConnect-Konfiguration anzuzeigen.

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

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.

- 1 **Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- 1 **NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- 1 **DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- 1 **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.
- 1 **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 Cisco

Wenn alle Einstellungen korrekt sind, wählen Sie **Fertig stellen** und geben Sie die Änderungen an FTD weiter.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help dperezve

Deployment Deployment History

1 device selected
Deploy time: Estimate Deploy

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

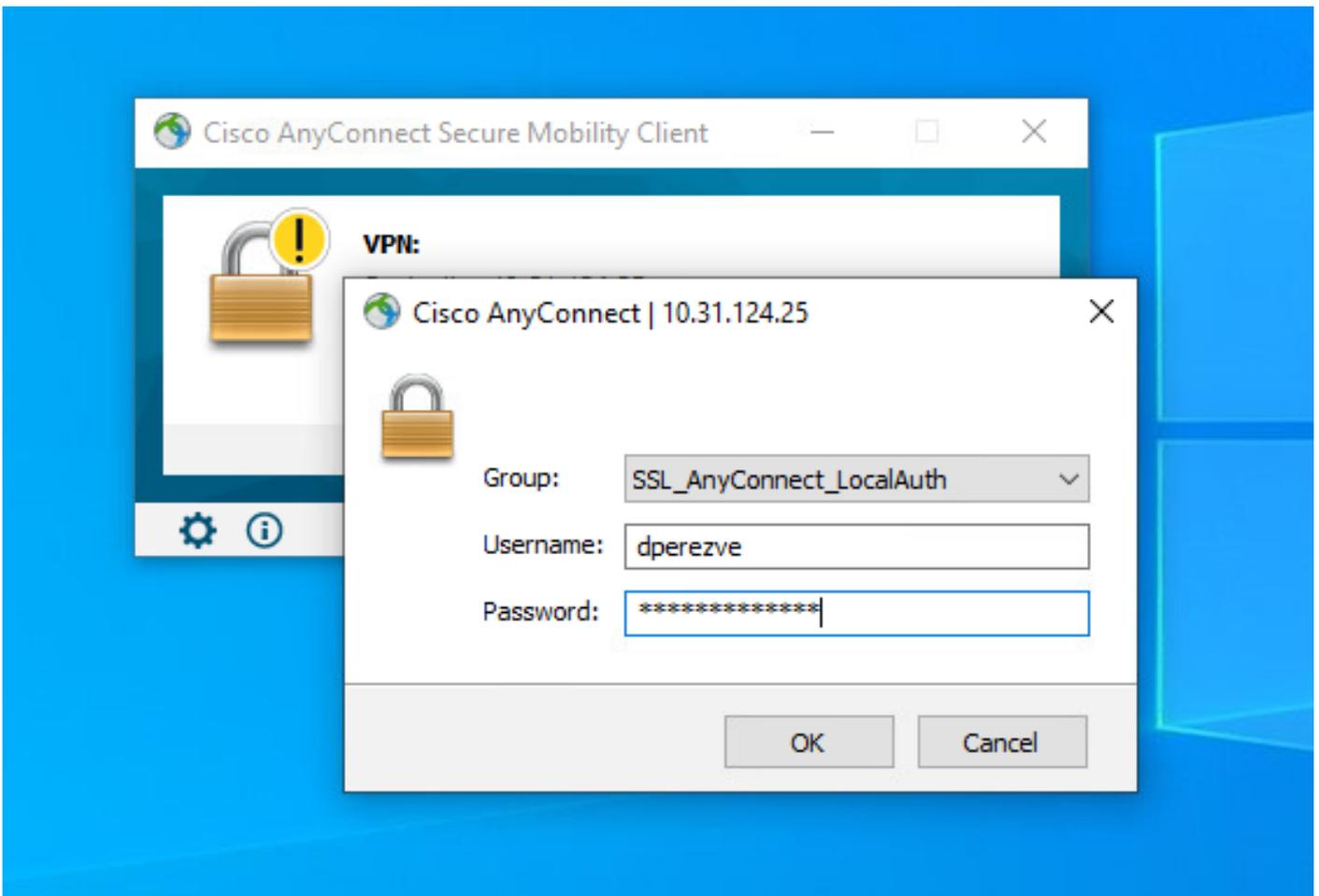
Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
ftdvha-dperezve	dperezve		FTD		Sep 7, 2021 2:44 PM		Pending

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

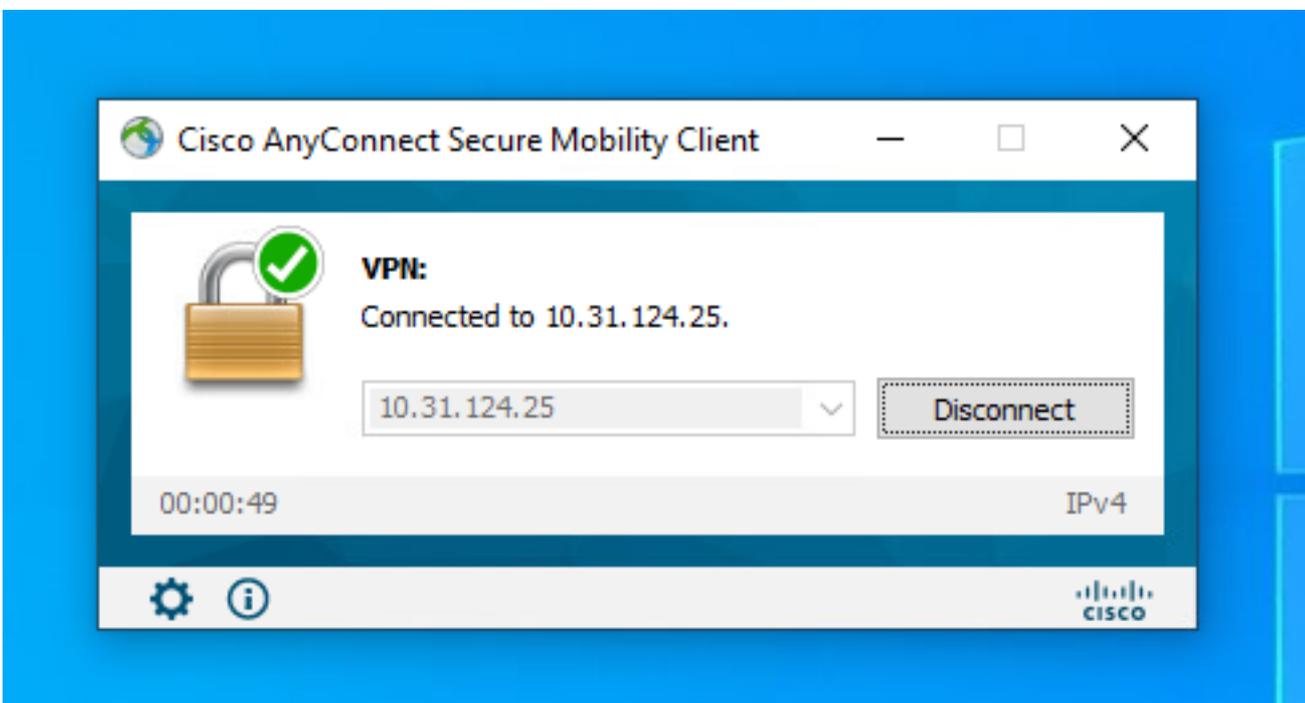
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2 Cisco

Überprüfung

Sobald die Bereitstellung erfolgreich war, starten Sie eine AnyConnect-Verbindung vom Windows-Client zu FTD. Der Benutzername und das Kennwort, die bei der Authentifizierungsaufforderung verwendet werden, müssen mit denen übereinstimmen, die in Schritt 4 erstellt wurden.



Sobald die Anmeldeinformationen von FTD genehmigt wurden, muss die AnyConnect-App den Status "Verbunden" anzeigen.



Von FTD aus können Sie den Befehl **show vpn-sessiondb anyconnect** ausführen, um die derzeit aktiven AnyConnect-Sitzungen auf der Firewall anzuzeigen.

```
firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dperezve Index : 8
```

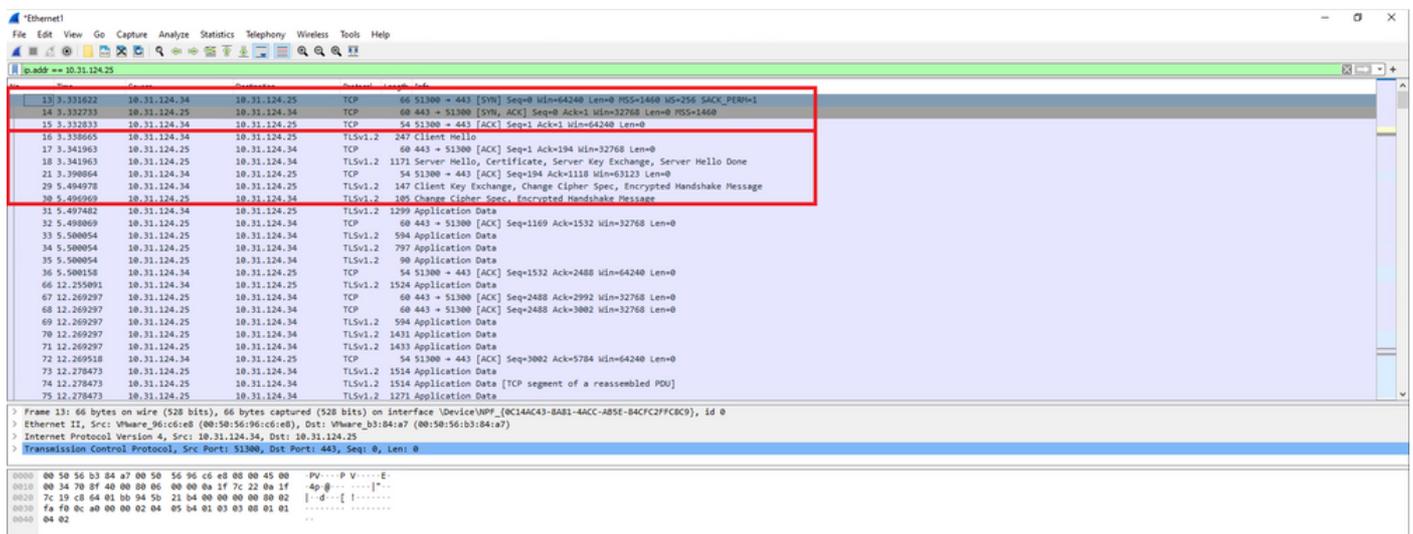
Assigned IP : 172.16.13.1 Public IP : 10.31.124.34 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384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

Fehlerbehebung

Führen Sie den Befehl **debug webvpn anyconnect 255** auf FTD aus, um den SSL-Verbindungsfluss bei FTD anzuzeigen.

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

Neben den AnyConnect-Debuggen kann der Verbindungsfluss auch bei der TCP-Paketerfassung beobachtet werden. Unten sehen Sie ein Beispiel für eine erfolgreiche Verbindung. Ein regulärer Drei-Handshake zwischen Windows-Client und FTD ist abgeschlossen, gefolgt von einem SSL-Handshake, der verwendet wird, um Verschlüsselungen zu akzeptieren.



Nach dem Handshake des Protokolls muss FTD Anmeldeinformationen mit Informationen validieren, die im lokalen Bereich gespeichert sind.

Sammeln Sie ein DART-Paket, und wenden Sie sich für weitere Recherchen an das Cisco TAC.