

Konfiguration eines SSL Secure Client mit lokaler Authentifizierung auf FTD

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [Konfigurieren](#)
- [Konfigurationen](#)
- [Schritt 1: Lizenzierung überprüfen](#)
- [Schritt 2: Cisco Secure ClientPackage auf FMC hochladen](#)
- [Schritt 3: Selbstsigniertes Zertifikat generieren](#)
- [Schritt 4: Lokalen Bereich auf FMC erstellen](#)
- [Schritt 5: SSL Cisco Secure Client konfigurieren](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration des Cisco Secure Client (einschließlich AnyConnect) mit lokaler Authentifizierung auf dem von Cisco FMC verwalteten Cisco FTD.

Voraussetzungen

Anforderungen

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

- SSL Secure Client-Konfiguration über FirePOWER Management Center (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 Firepower Threat Defense (FTD) Version 7.0.0 (Build 94)
- Cisco FMC Version 7.0.0 (Build 94)
- Cisco 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 möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Beispiel wird Secure Sockets Layer (SSL) verwendet, um ein Virtual Private Network (VPN) zwischen FTD und einem Windows 10-Client zu erstellen.

Ab Version 7.0.0 unterstützt die von FMC verwaltete FTD die lokale Authentifizierung für Cisco Secure 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 Authentifizierung über FTD mit Cisco Secure Client nur über den Cisco FirePOWER Device Manager (FDM) möglich.

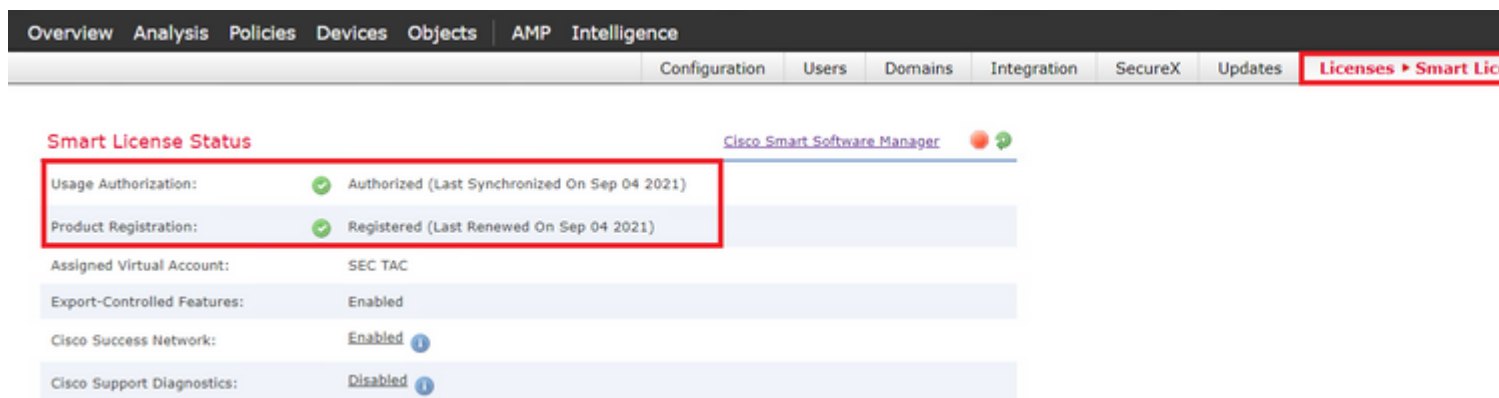
Konfigurieren

Konfigurationen

Schritt 1: Lizenzierung überprüfen

Vor der Konfiguration des Cisco Secure Client muss das FMC registriert sein und mit dem Smart Licensing-Portal übereinstimmen. Sie können Cisco Secure Client nicht bereitstellen, wenn FTD nicht über eine gültige Plus-, Apex- oder VPN Only-Lizenz verfügt.

Navigieren Sie zu **System > Licenses > Smart Licenses**, um zu überprüfen, ob das FMC registriert ist und mit dem Smart Licensing-Portal übereinstimmt.



The screenshot shows the 'Smart License Status' page in the Cisco FMC interface. The page is titled 'Smart License Status' and includes a 'Cisco Smart Software Manager' status indicator. The main content is a table with the following rows:

Component	Status
Usage Authorization:	Authorized (Last Synchronized On Sep 04 2021)
Product Registration:	Registered (Last Renewed On Sep 04 2021)
Assigned Virtual Account:	SEC TAC
Export-Controlled Features:	Enabled
Cisco Success Network:	Enabled ⓘ
Cisco Support Diagnostics:	Disabled ⓘ

Blättern Sie auf derselben Seite nach unten. Unten im Diagramm für **Smart Licenses** sehen Sie die verschiedenen verfügbaren Typen von Cisco Secure Client (AnyConnect)-Lizenzen und die jeweils abonnierten Geräte. Validieren Sie, dass das vorliegende FTD in einer dieser Kategorien registriert ist.

Smart Licenses













License Type/Device Name	License Status	Device Type
▶ 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
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
AnyConnect Plus (0)		
AnyConnect VPN Only (0)		

Note: Container Instances of same blade share feature licenses

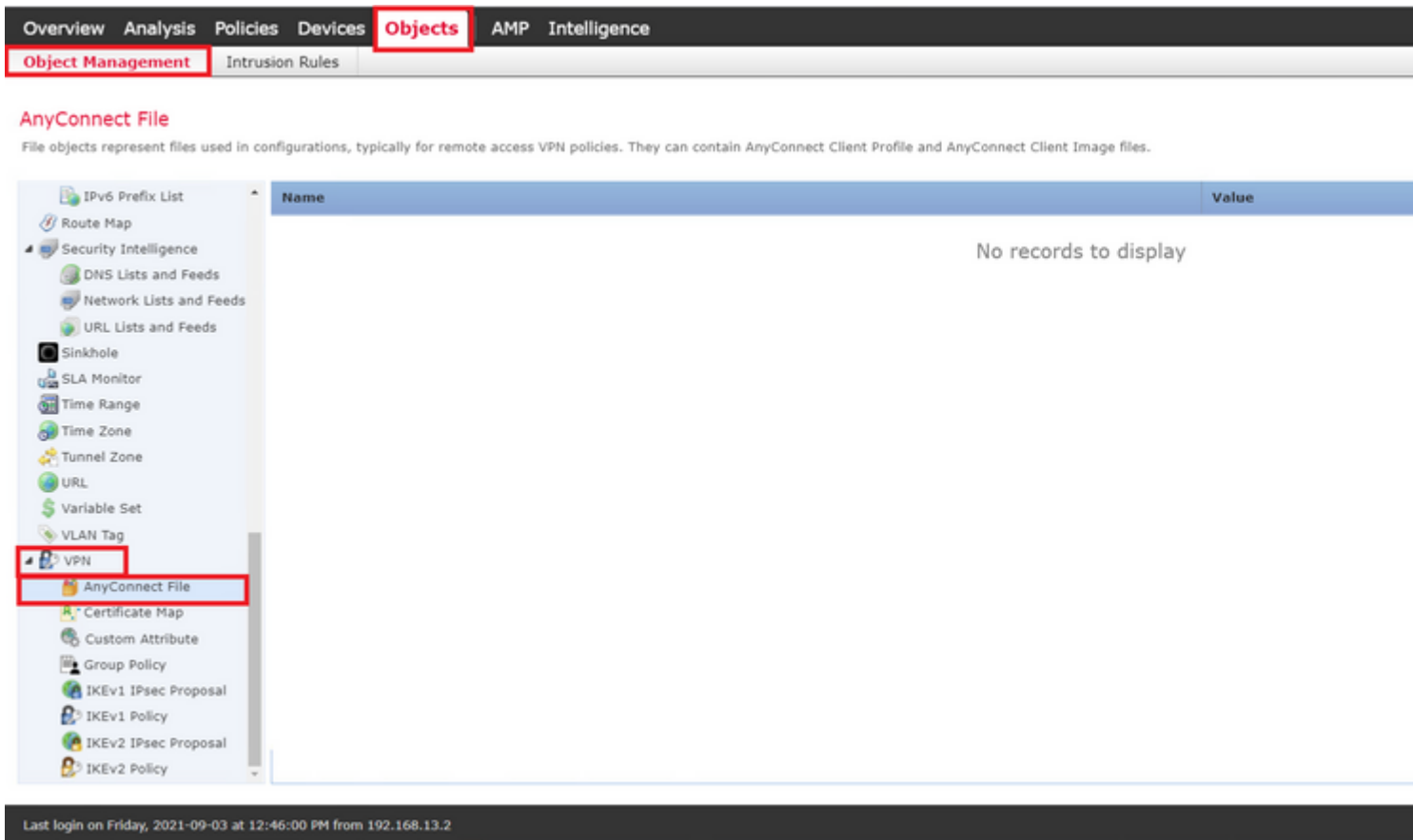
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Schritt 2: Hochladen des Cisco Secure Client-Pakets auf FMC

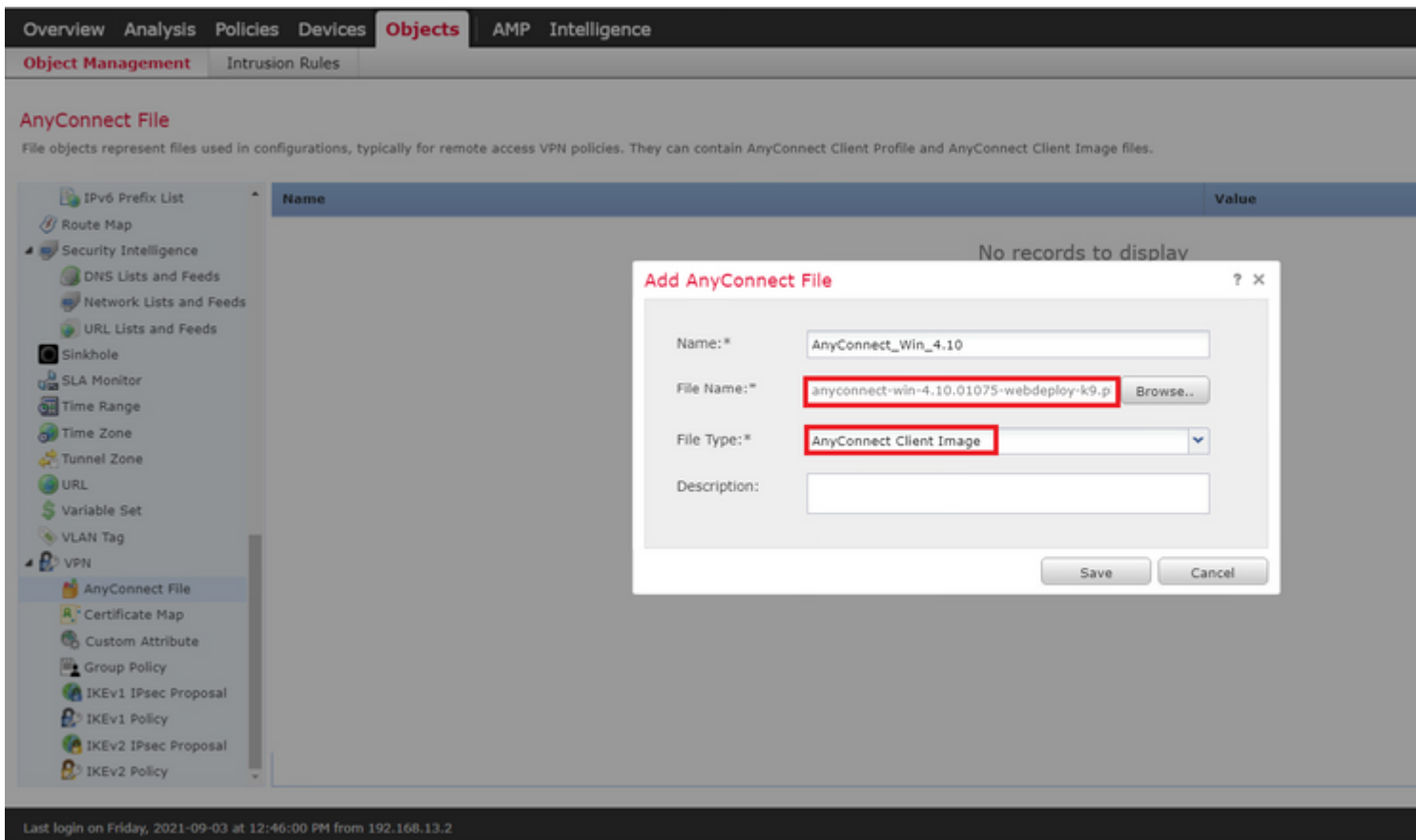
Laden Sie das Cisco Secure Client (AnyConnect) Headend Deployment Package für Windows von [cisco.com](https://www.cisco.com) herunter.

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 Cisco Secure Client-Image hochzuladen, navigieren Sie zu **Objects > Object Management (Objekte > Objektverwaltung)** und wählen Sie **Cisco Secure Client File** in der **VPN**-Kategorie im Inhaltsverzeichnis aus.



Wählen Sie die Schaltfläche **AnyConnect-Datei hinzufügen**. Weisen Sie im Fenster **Add AnyConnect Secure Client File (AnyConnect-Sicherheitsclientdatei hinzufügen)** einen Namen für das Objekt zu, und wählen Sie dann **Browse...** (**Durchsuchen**), um das Cisco Secure Client-Paket auszuwählen und schließlich **AnyConnect Client Image** als Dateityp im Dropdown-Menü auszuwählen.



Wählen Sie **Speichern**. Das Objekt muss der Objektliste hinzugefügt werden.

The screenshot shows the Cisco ASA configuration interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP Intelligence'. The 'Objects' tab is active, and the 'Object Management' sub-tab is selected. The main content area displays the 'AnyConnect File' object configuration. A table lists the object details:

Name	Value
AnyConnect_Win_4.10	anyconnect-win-4.10.01075-webdep

The left sidebar shows a tree view of configuration objects, with 'AnyConnect File' selected under the 'VPN' category. At the bottom, a status bar indicates the last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2.

Schritt 3: Selbstsigniertes Zertifikat generieren

Für den SSL Cisco Secure Client (AnyConnect) ist ein gültiges Zertifikat erforderlich, damit der SSL-Handshake zwischen VPN-Headend und Client durchgeführt werden kann.

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

Um das selbstsignierte Zertifikat zu erstellen, navigieren Sie zu **Geräte > Zertifikate**.

The screenshot shows the Cisco ASA configuration interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP Intelligence'. The 'Devices' tab is active, and the 'Certificates' sub-tab is selected. The main content area displays the 'Certificates' configuration page.

Wählen Sie die Schaltfläche **Hinzufügen**. Wählen Sie dann im Dropdown-Menü **Gerät** im Fenster **Neues Zertifikat hinzufügen** die aktuell verfügbare FTD aus.

Overview Analysis Policies **Devices** Objects AMP Intelligence


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

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

Add New Certificate ? x

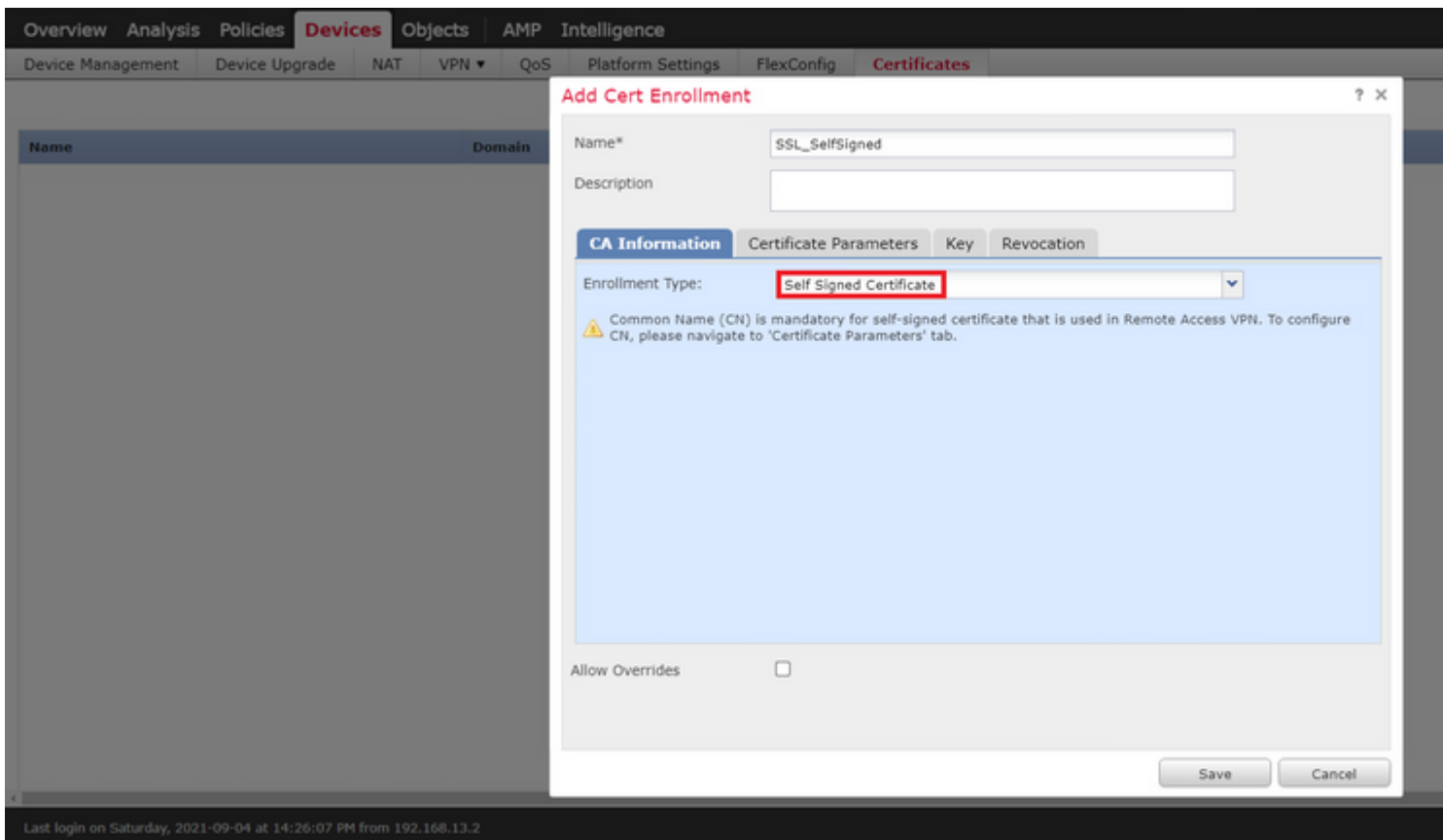
Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

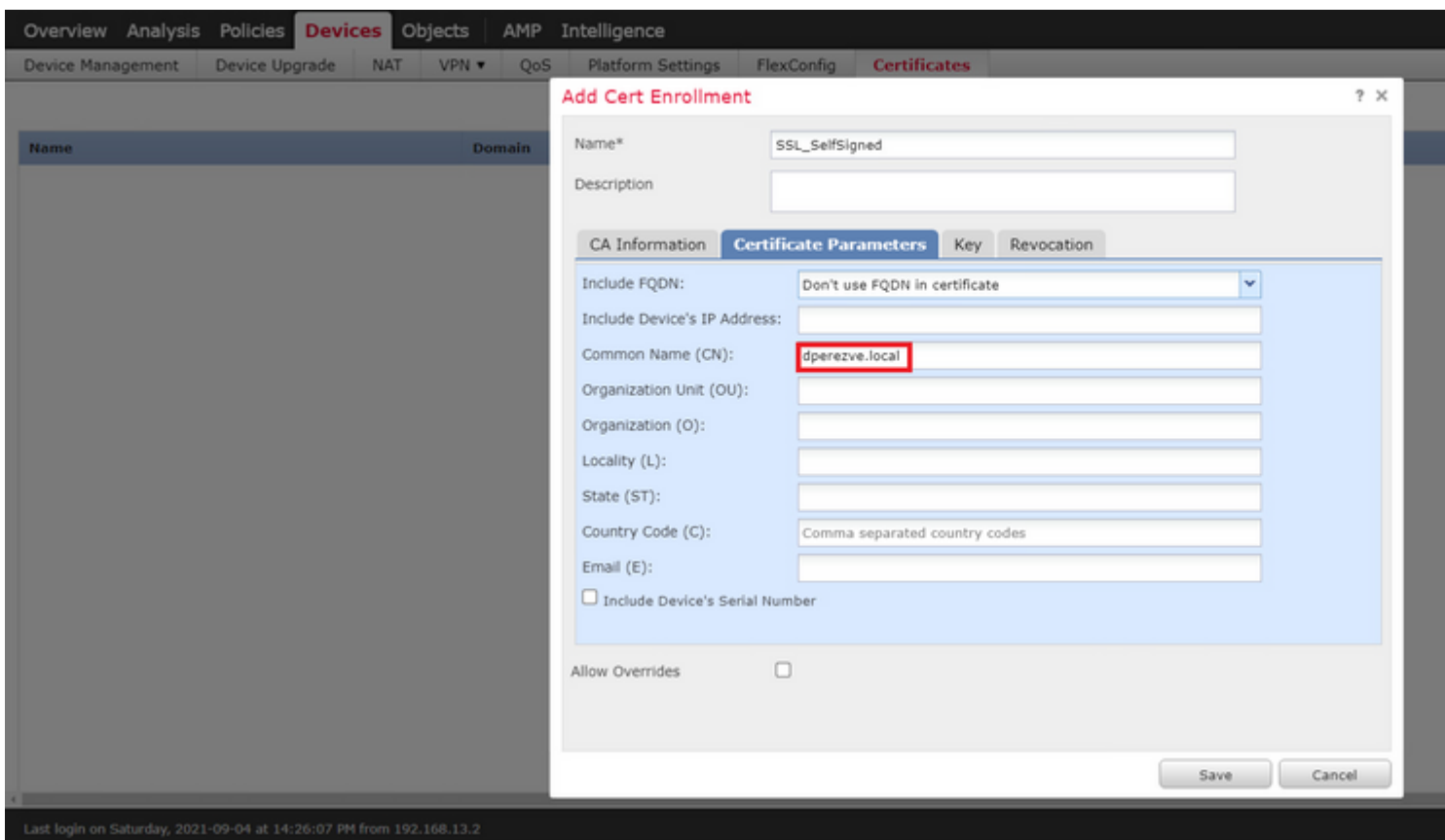
Cert Enrollment*: 

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

Wählen Sie die Schaltfläche **Add Certificate Enrollment (Zertifizierungsanmeldung hinzufügen)** (grün + Symbol), um ein neues Registrierungsobjekt zu erstellen. Weisen Sie nun im Fenster **Add Certificate Enrollment (Zertifikatregistrierung hinzufügen)** einen Namen für das Objekt zu, und wählen Sie im Dropdown-Menü **Enrollment Type (Registrierungstyp)** die Option **Self Signed Certificate (Selbstsigniertes Zertifikat)** aus.



Für selbstsignierte Zertifikate ist ein Common Name (CN) erforderlich. Navigieren Sie zur Registerkarte **Zertifikatparameter**, um eine CN zu definieren.

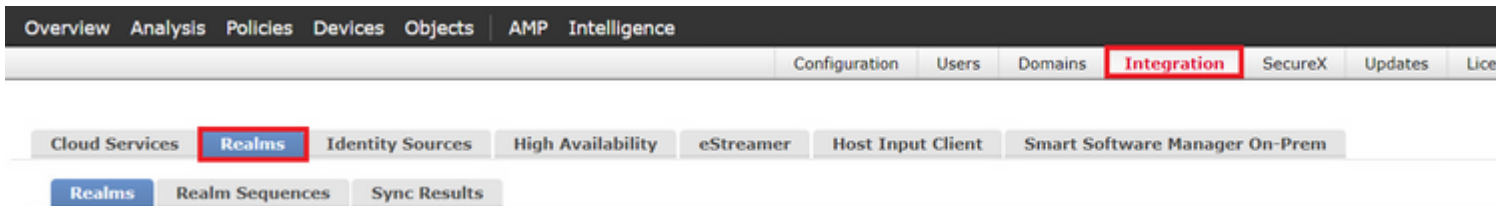


Wählen Sie **Speichern** und **Hinzufügen** Schaltflächen. Nach einigen Sekunden muss das neue Zertifikat der Zertifikatsliste hinzugefügt werden.

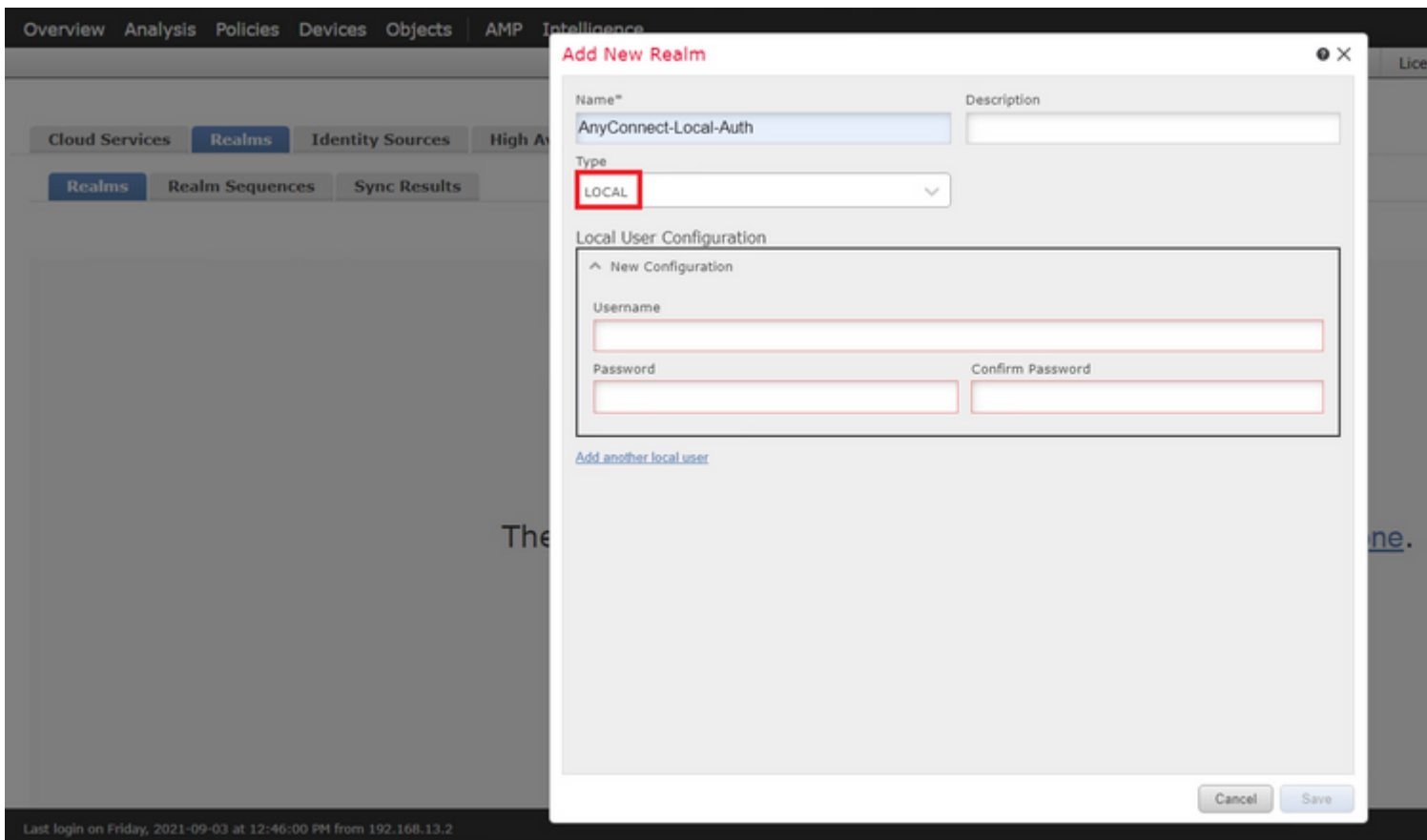
Name	Domain	Enrollment Type	Status
ftdvha-dperezve			
SSL_SelfSigned	Global	Self-Signed	CA ID

Schritt 4: Lokalen Bereich auf FMC erstellen

Die lokale Benutzerdatenbank und die jeweiligen Passwörter werden in einem lokalen Bereich gespeichert. Um den lokalen Bereich zu erstellen, navigieren Sie zu **System > Integration > Realms**.

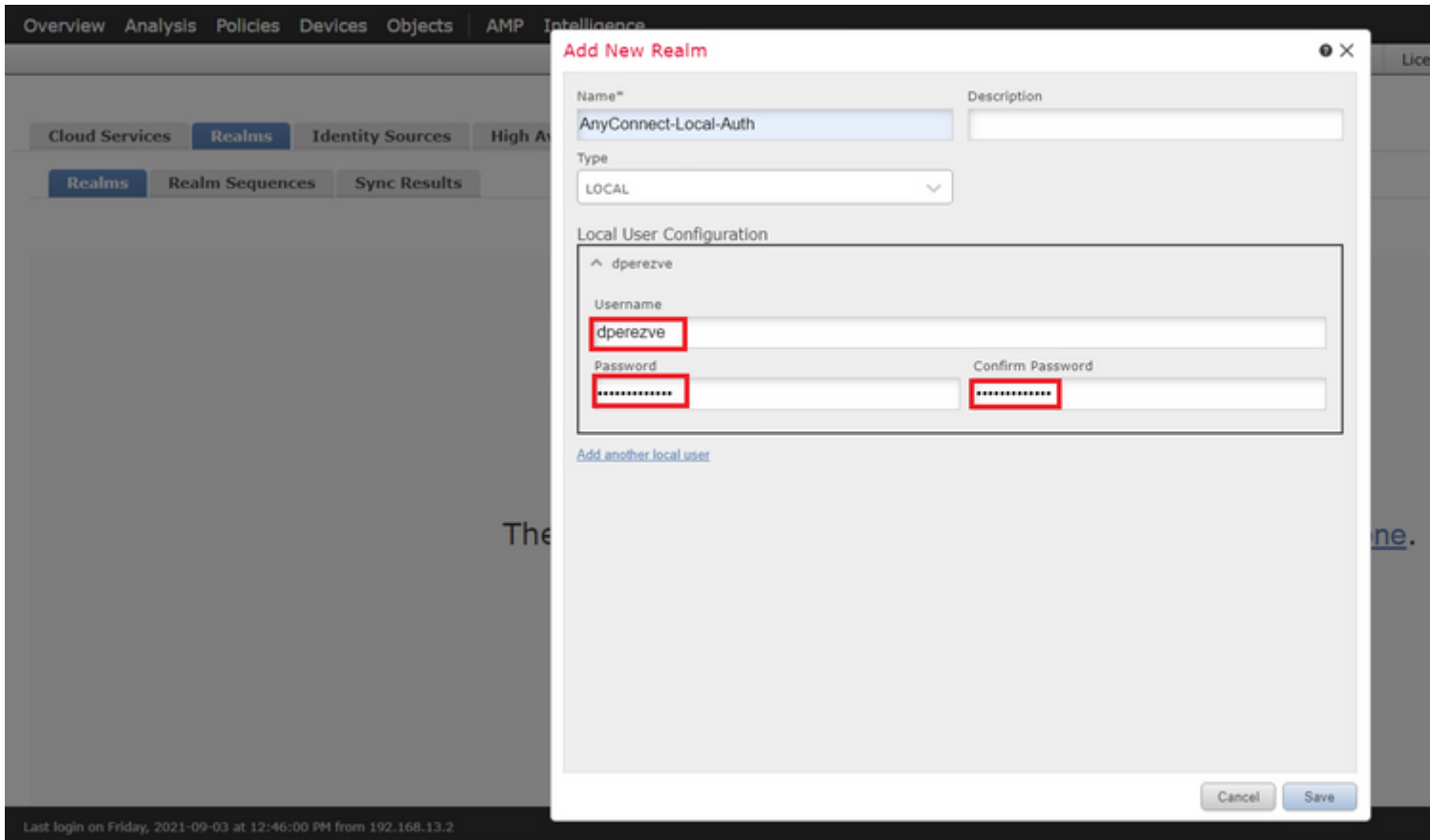


Wählen Sie die Schaltfläche **Bereich hinzufügen**. Weisen Sie im Fenster **Neuen Bereich hinzufügen** einen Namen zu, und wählen Sie im Dropdown-Menü **Typ** die Option **LOKAL**.

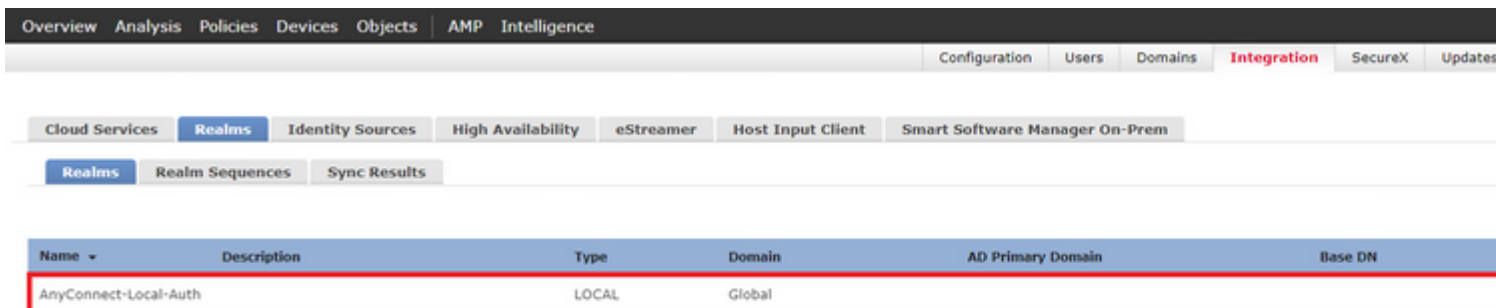


Benutzerkonten und Kennwörter werden im Abschnitt "Lokale Benutzerkonfiguration" erstellt.

Hinweis: Kennwörter müssen mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten.



Die Änderungen **speichern** und der neue Bereich muss zur Liste der vorhandenen Bereiche hinzugefügt werden.



Schritt 5: SSL Cisco Secure Client konfigurieren

Um SSL Cisco Secure Client zu konfigurieren, navigieren Sie zu **Devices > VPN > Remote Access**.



Wählen Sie **Hinzufügen** aus, um eine neue VPN-Richtlinie zu erstellen. Definieren Sie einen Namen für das Verbindungsprofil, aktivieren Sie das Kontrollkästchen **SSL**, und wählen Sie die verfügbare FTD als Zielgerät aus. Alle Einstellungen müssen im Abschnitt **Richtlinienzuweisung** im **Assistenten für VPN-Richtlinien für den Remotezugriff** konfiguriert werden.

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: * SSL_AnyConnect_LocalAuth

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices:

Available Devices

- Search
- ftdv-dperezve
- ftdvha-dperezve

Selected Devices

- ftdvha-dperezve

Add

Authentication Server
Configure [LOCAL](#) or [Realm Server Group](#) or [SSO](#) to authenticate clients.

AnyConnect Client Package
Make sure you have AnyConnect for VPN Client downloaded on the relevant Cisco credentials it during the wizard.

Device Interface
Interfaces should be already configured on targeted [devices](#) so that they are in a security zone or interface to enable VPN access.

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

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

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

Connection Profile:
Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name: * SSL_AnyConnect_LocalAuth
This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):
Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only
Authentication Server: * LOCAL (LOCAL or Realm or RADIUS)
Local Realm: * AnyConnect-Local-Auth
Authorization Server: (Realm or RADIUS)
Accounting Server: (RADIUS)

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

Führen Sie auf derselben Seite einen Bildlauf nach unten durch, und wählen Sie dann das Bleistiftsymbol im Abschnitt **IPv4-Adresspool** aus, um den von Cisco Secure Clients verwendeten IP-Pool zu definieren.

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

Authentication Server: * LOCAL (LOCAL or Realm or RADIUS)

Client Address: Client IP address assignment is

Use
 Use
 Use

Group Policy: A group policy or create a Gr
Group

Address Pools

Available IPv4 Pools

Search

ftdv-dperezve-pool

Selected IPv4 Pools

ftdv-dperezve-pool

Add

OK Cancel

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

Wählen Sie **Weiter** aus, um zum Abschnitt **AnyConnect** zu wechseln. Wählen Sie nun das in Schritt 2

hochgeladene Cisco Secure Client-Image aus.

The screenshot shows the 'Remote Access VPN Policy Wizard' in step 3, 'AnyConnect'. The navigation bar includes: Overview, Analysis, Policies, **Devices**, Objects, AMP, Intelligence, Device Management, Device Upgrade, NAT, **VPN > Remote Access**, QoS, Platform Settings, FlexConfig, Certificates.

The wizard steps are: 1 Policy Assignment, 2 Connection Profile, 3 **AnyConnect**, 4 Access & Certificate, 5 Summary.

The network diagram shows: Remote User (with a green checkmark) connected to an AnyConnect Client, which connects to the Internet. The Internet connects to a VPN Device (with a green checkmark) via an Outside interface. The VPN Device has an Inside interface connected to Corporate Resources. An AAA server is also connected to the VPN Device.

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](#)

<input checked="" type="checkbox"/>	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

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

Wählen Sie **Weiter** aus, um zum Abschnitt **Zugriff und Zertifikat** zu wechseln. Wählen Sie im Dropdown-Menü **Interface group/Security Zone** (Schnittstellengruppe/Sicherheitszone) die Schnittstelle aus, auf der Cisco Secure Client (AnyConnect) aktiviert werden soll. Wählen Sie dann im Dropdown-Menü **Certificate Enrollment** (Zertifikatregistrierung) das in Schritt 3 erstellte Zertifikat aus.

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

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:* **VLAN232**

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:* **SSL_SelfSigned**

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

Wählen Sie anschließend **Weiter**, um eine Zusammenfassung der Cisco Secure Client-Konfiguration anzuzeigen.

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

AAA

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):	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.

⚠ **Network Interface Configuration**
Make sure to add interface from targeted devices to SecurityZone object 'VLAN232'

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

Wenn alle Einstellungen korrekt sind, wählen Sie **Beenden** und stellen Sie Änderungen in FTD bereit.

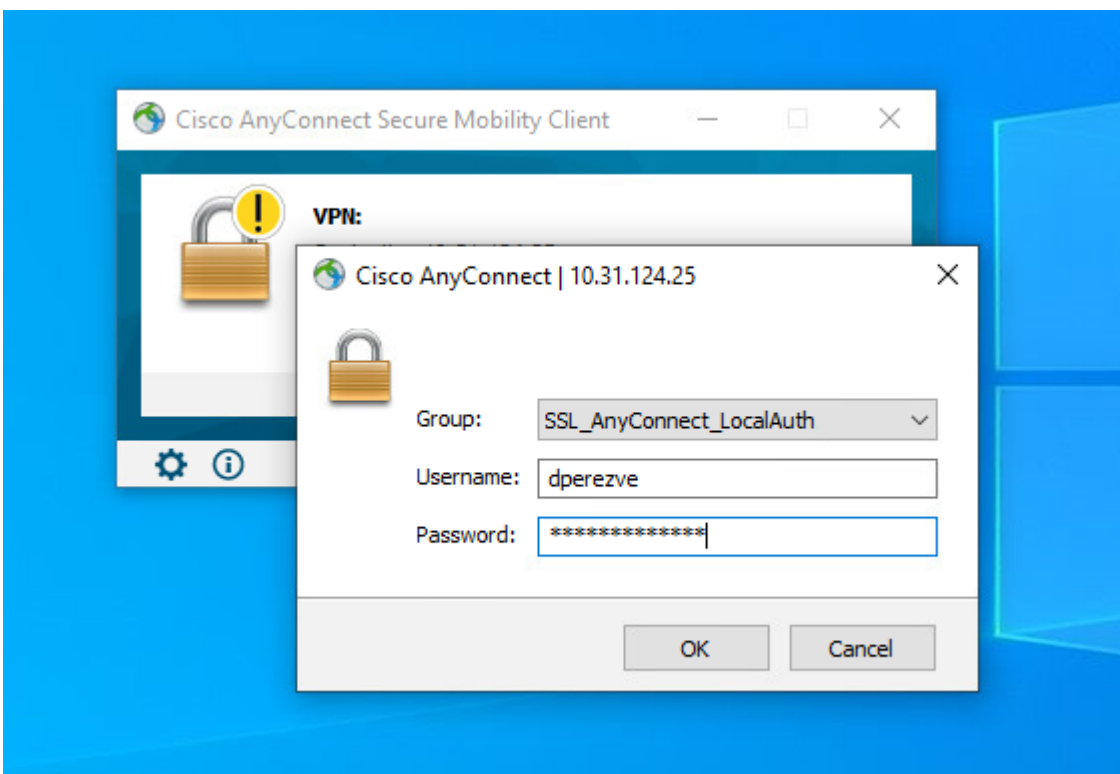
Search using device name, user name, type, group or status

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

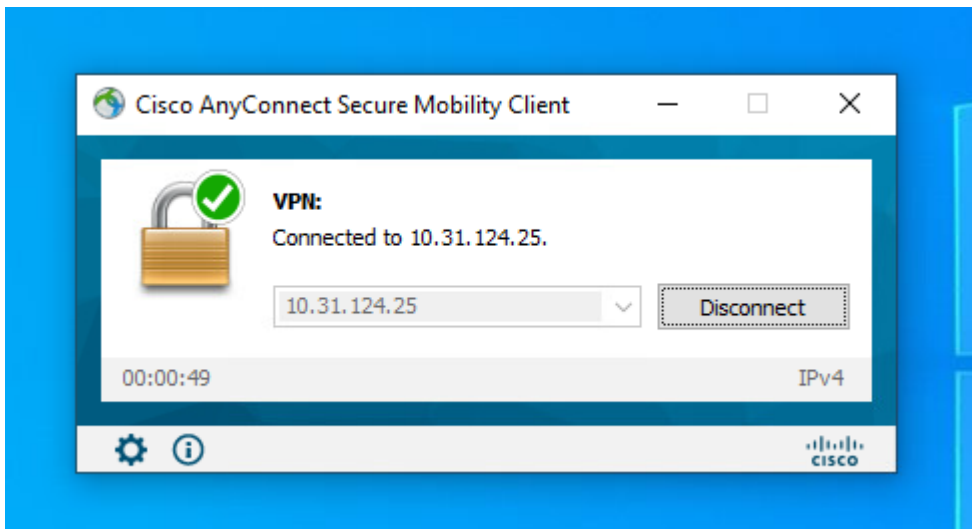
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Überprüfung

Sobald die Bereitstellung erfolgreich war, initiieren Sie eine Verbindung des Cisco AnyConnect Secure Mobility Client vom Windows-Client zum FTD. Der Benutzername und das Kennwort für die Authentifizierungsaufforderung müssen mit den Angaben in Schritt 4 übereinstimmen.



Sobald die Anmeldedaten von FTD genehmigt wurden, muss die Cisco AnyConnect Secure Mobility Client-App den Verbindungsstatus anzeigen.



Über FTD können Sie den Befehl **show vpn-sessiondb anyconnect** ausführen, um die derzeit auf der Firewall aktiven Cisco Secure Client-Sitzungen 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
```

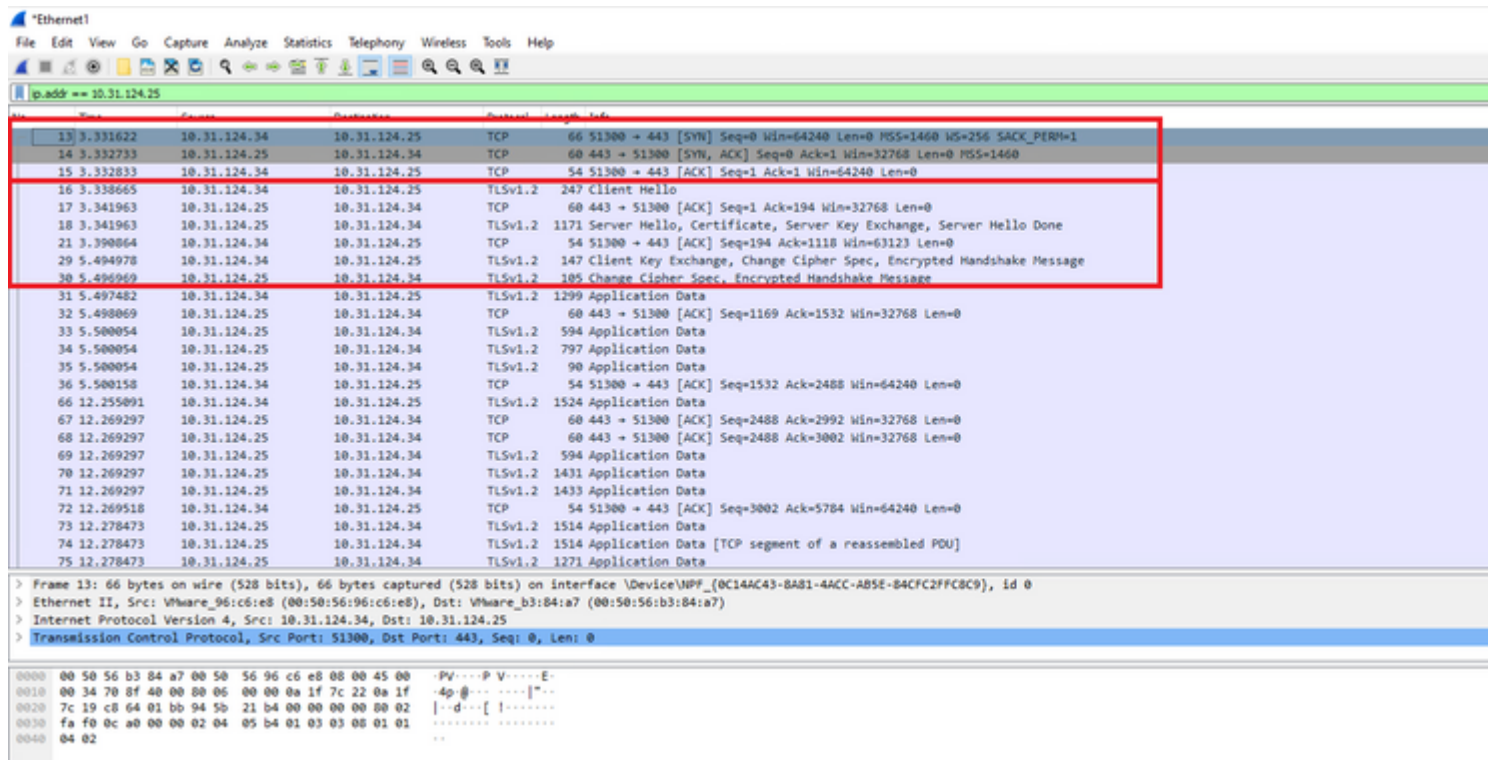
Fehlerbehebung

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

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

Neben den Cisco Secure Client-Debugging-Vorgängen kann der Verbindungsfluss auch bei der TCP-

Paketerfassung beobachtet werden. Dies ist ein Beispiel für eine erfolgreiche Verbindung. Ein regulärer Drei-Handshake zwischen dem Windows-Client und FTD wird durchgeführt, gefolgt von einem SSL-Handshake, der verwendet wird, um Chiffren zu vereinbaren.



Nach einem Protokoll-Handshake muss FTD die Anmeldeinformationen anhand der im lokalen Bereich gespeicherten Informationen validieren.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.