Konfiguration eines SSL Secure Client mit lokaler Authentifizierung auf FTD

Inhalt

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.

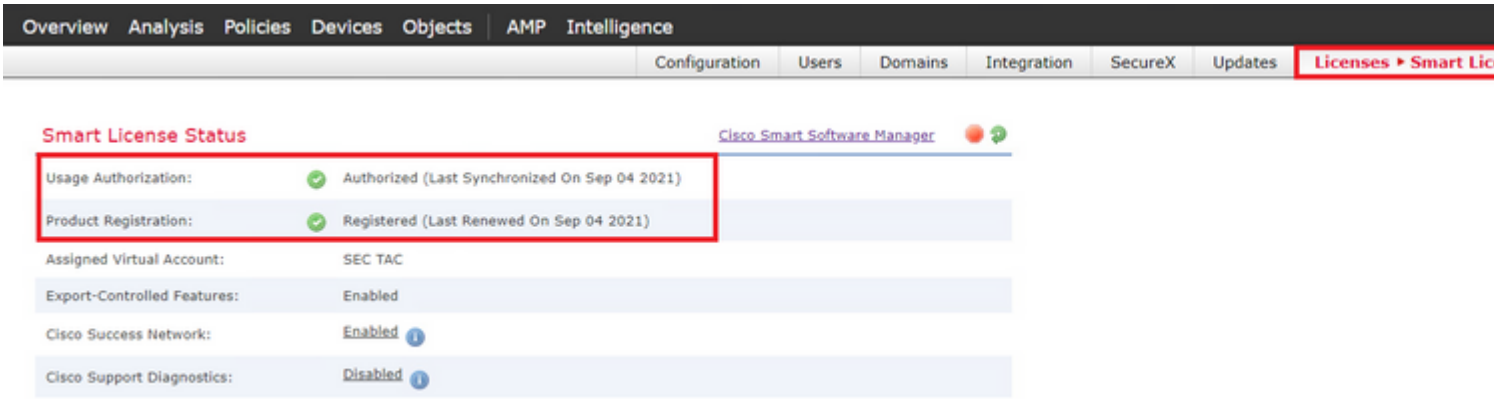
Konfigurieren

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.



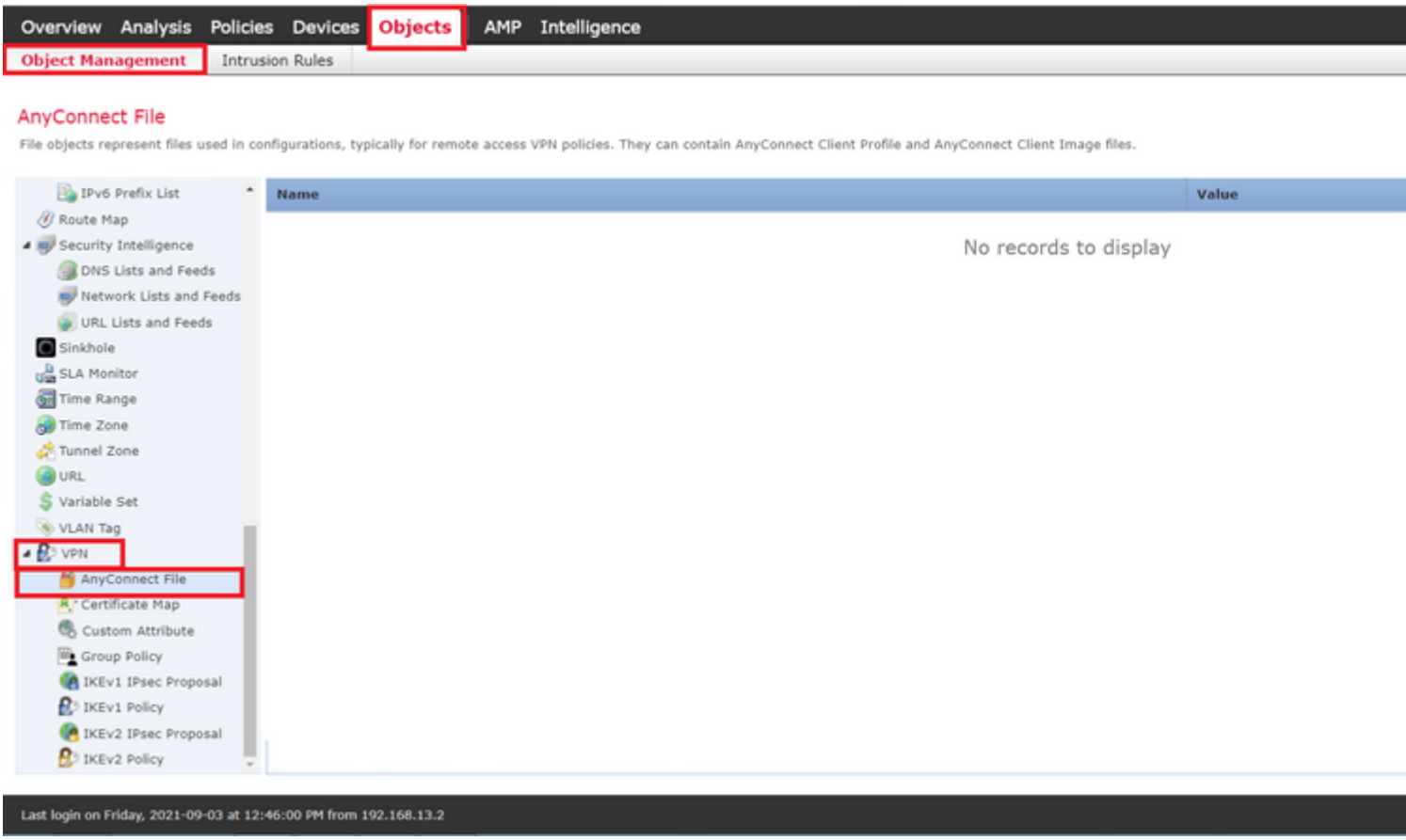
Blättern Sie auf derselben Seite nach unten. Unten im Diagramm für **Smart Licenses** sehen Sie die verschiedenen verfügbaren Typen von Cisco Secure Client (AnyConnect)-Lizenzen und die jeweils abonnierten Geräte. Validieren Sie, dass das vorliegende FTD in einer dieser Kategorien registriert ist.

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

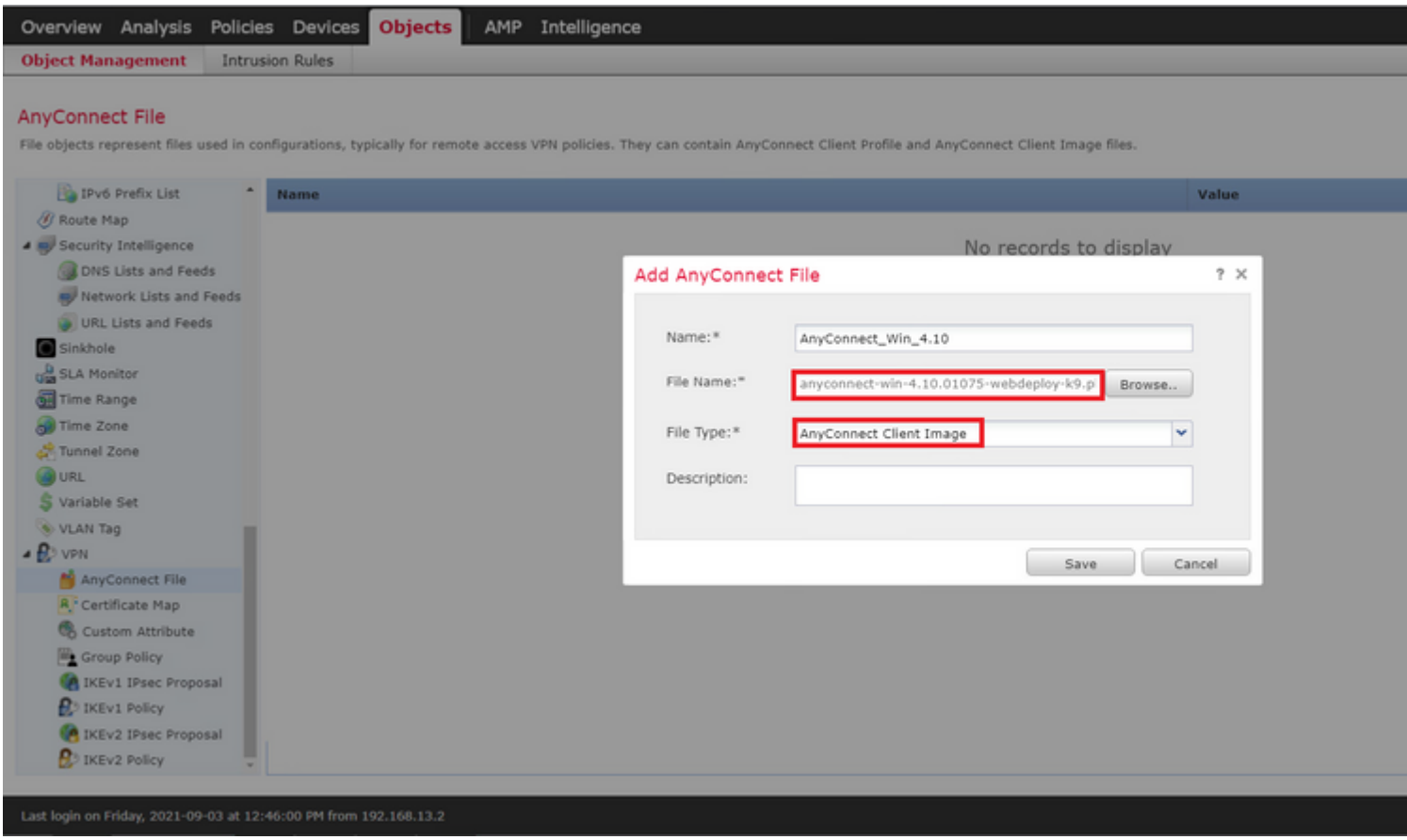
Laden Sie das Cisco Secure Client (AnyConnect) Headend Deployment Package für Windows von cisco.com herunter.

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

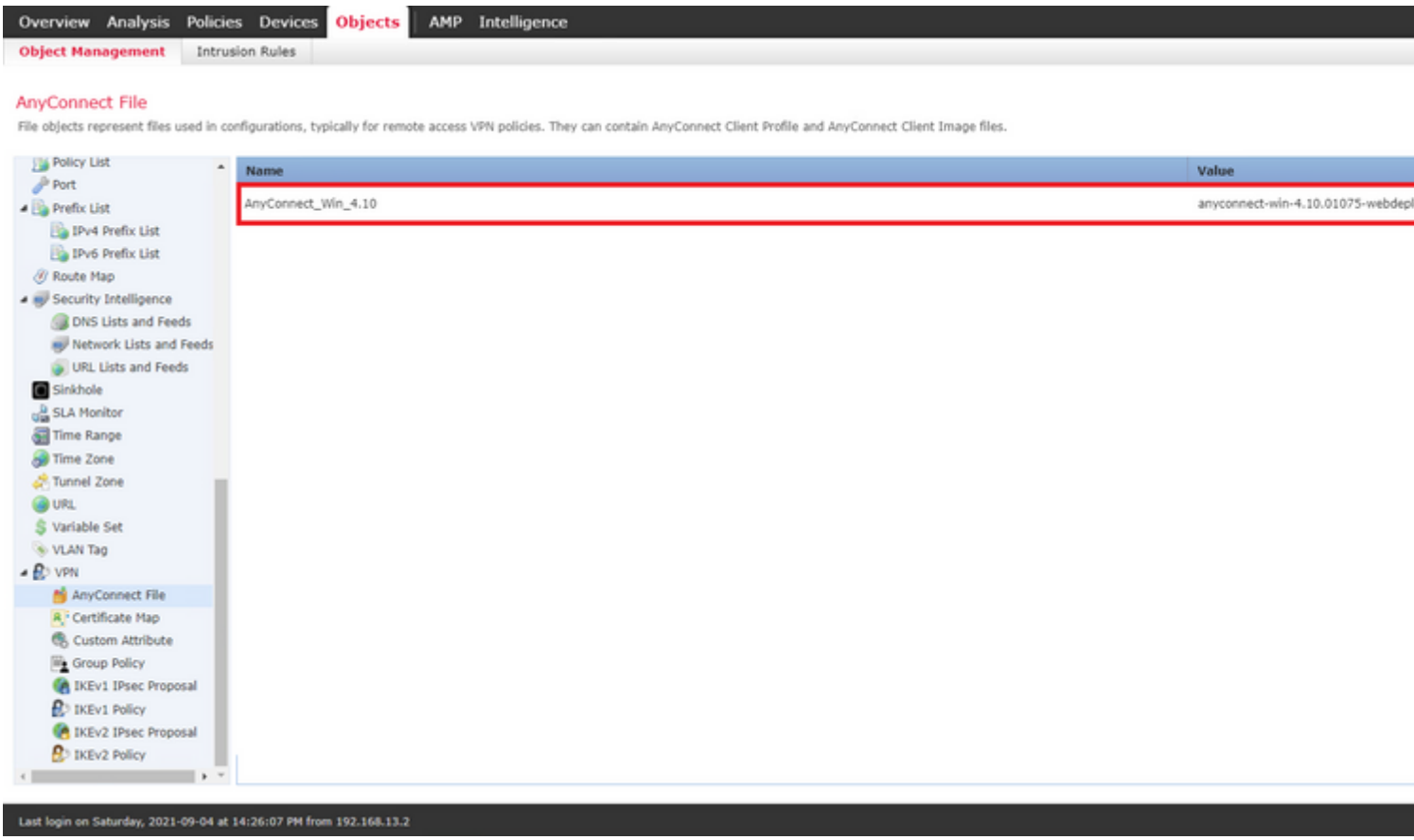
Um das Cisco Secure Client-Image hochzuladen, navigieren Sie zu **Objects > Object Management (Objekte > Objektverwaltung)** und wählen Sie **Cisco Secure Client File** in der **VPN-**Kategorie im Inhaltsverzeichnis aus.



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.

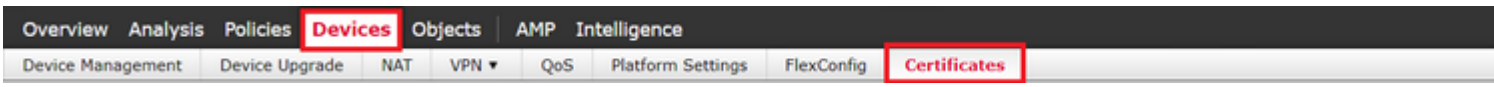


Schritt 3: Selbstsigniertes Zertifikat generieren

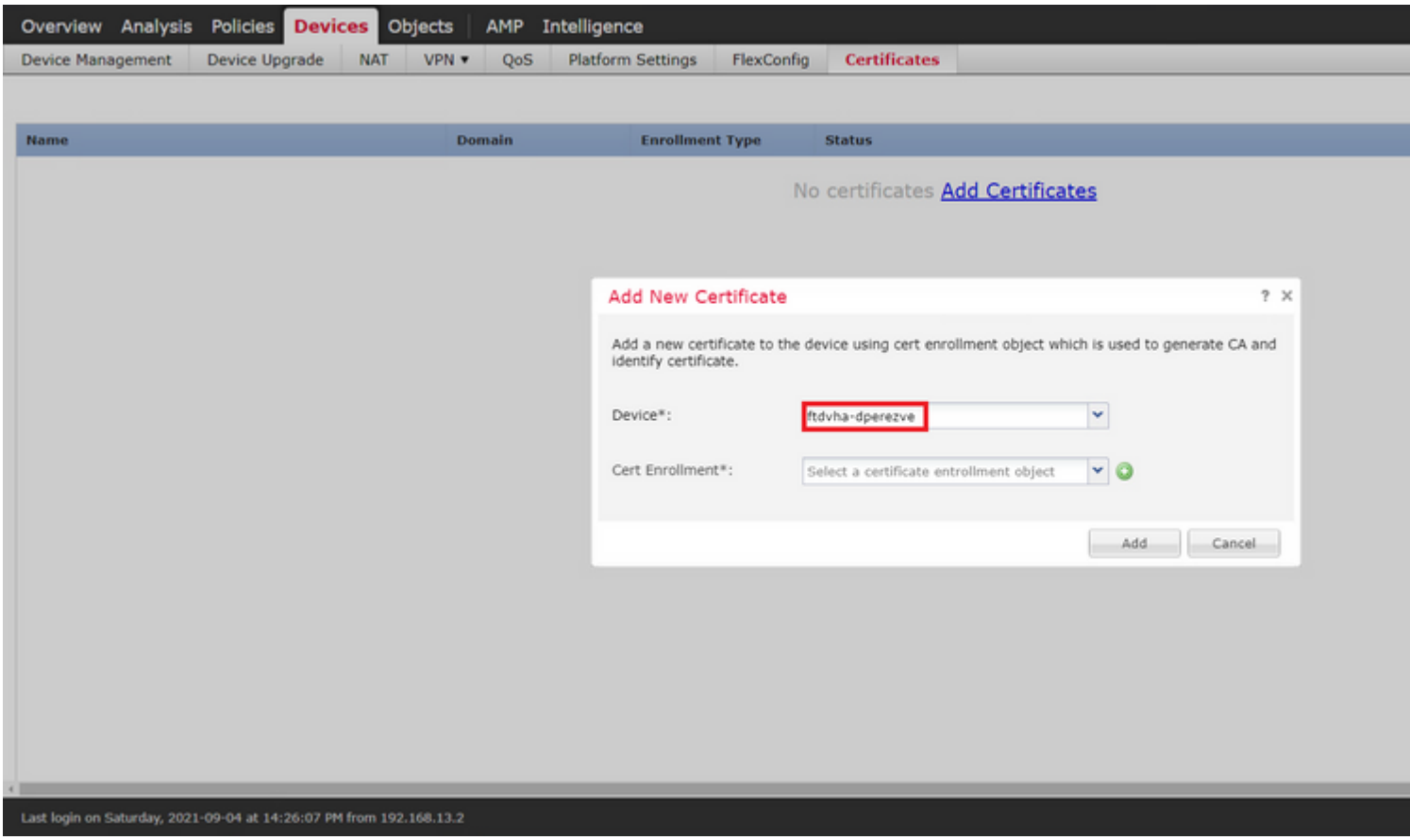
Für den SSL Cisco Secure Client (AnyConnect) ist ein gültiges Zertifikat erforderlich, damit der SSL-Handshake zwischen VPN-Headend und Client durchgeführt werden kann.

> **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.

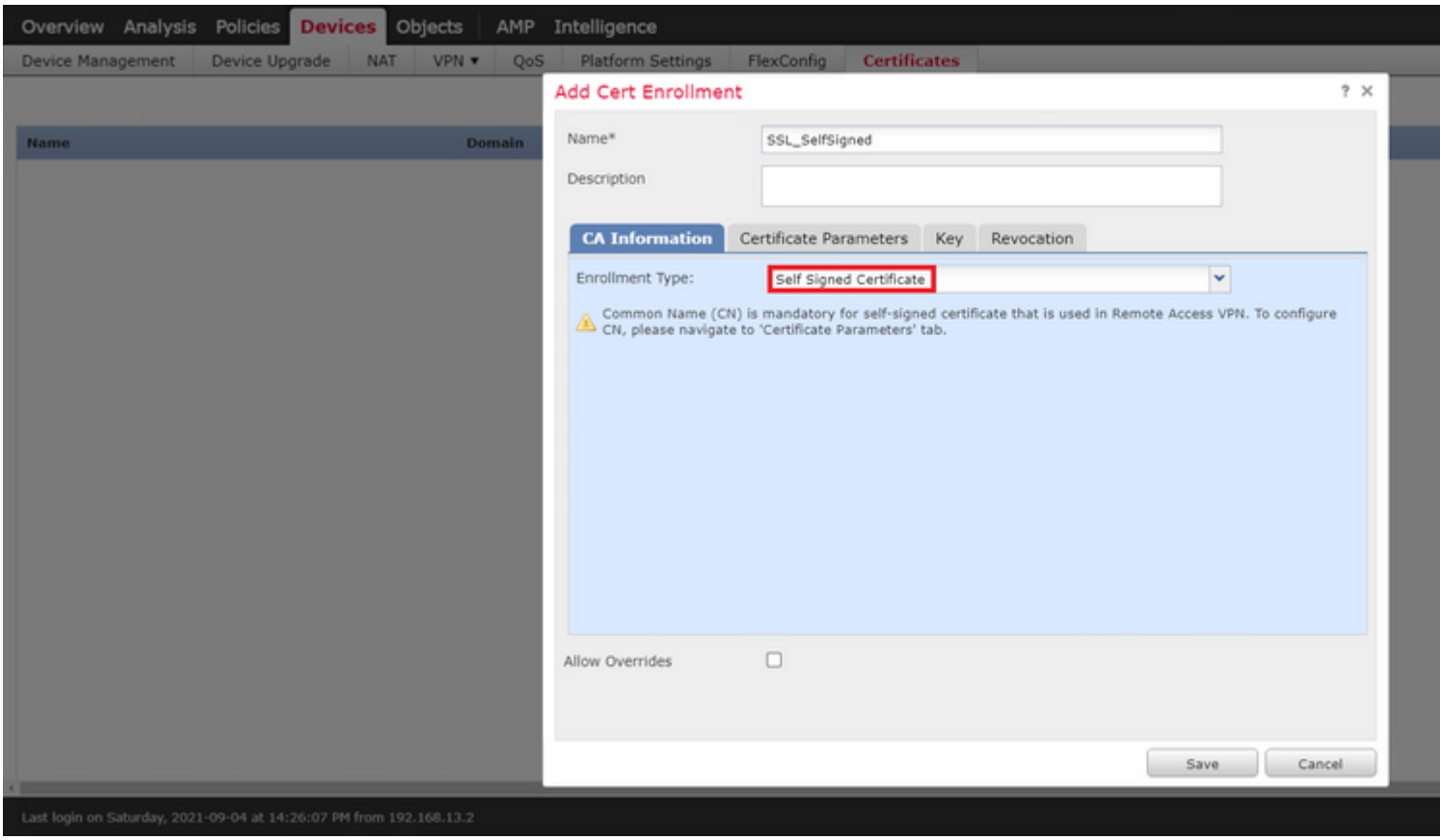
Um das selbstsignierte Zertifikat zu erstellen, navigieren Sie zu **Geräte > Zertifikate**.



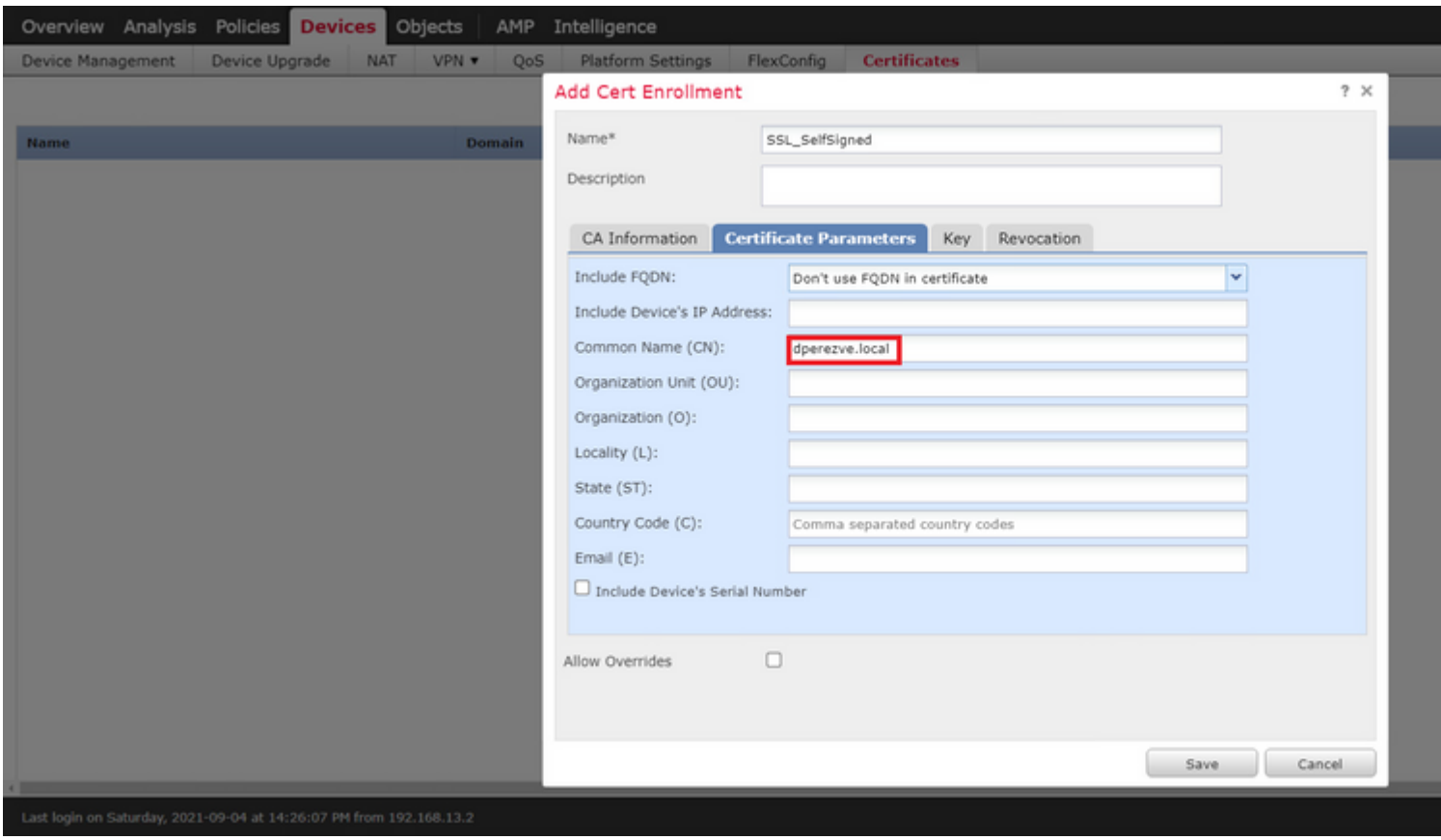
Wählen Sie die Schaltfläche **Hinzufügen**. Wählen Sie dann im Dropdown-Menü **Gerät** im Fenster **Neues Zertifikat hinzufügen** die aktuell verfügbare FTD aus.



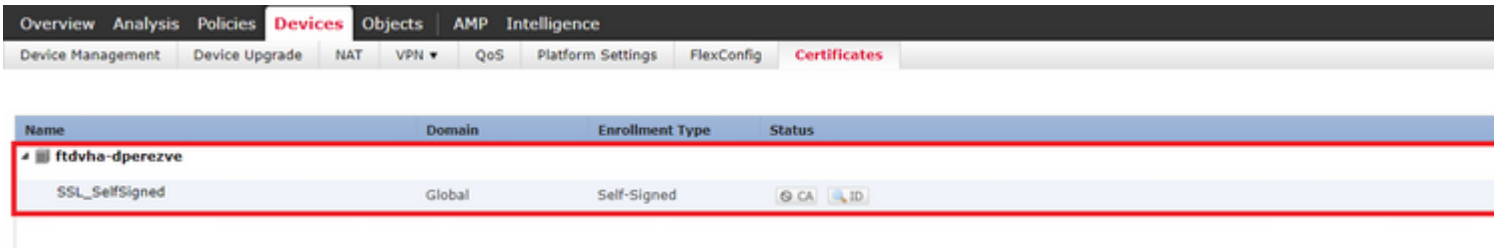
Wählen Sie die Schaltfläche **Add Certificate Enrollment (Zertifizierungsanmeldung hinzufügen**) (grün + Symbol), um ein neues Registrierungsobjekt zu erstellen. Weisen Sie nun im Fenster **Add Certificate Enrollment (Zertifikatregistrierung hinzufügen)** einen Namen für das Objekt zu, und wählen Sie 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.

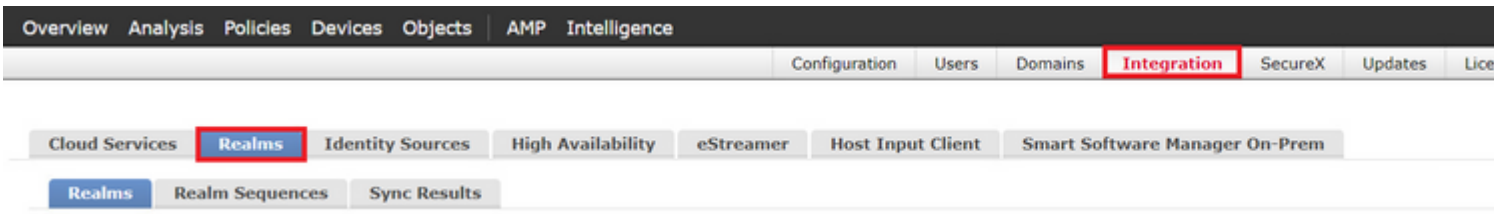


Wählen Sie **Speichern** und **Hinzufügen** Schaltflächen. Nach einigen Sekunden muss das neue Zertifikat der Zertifikatsliste hinzugefügt werden.

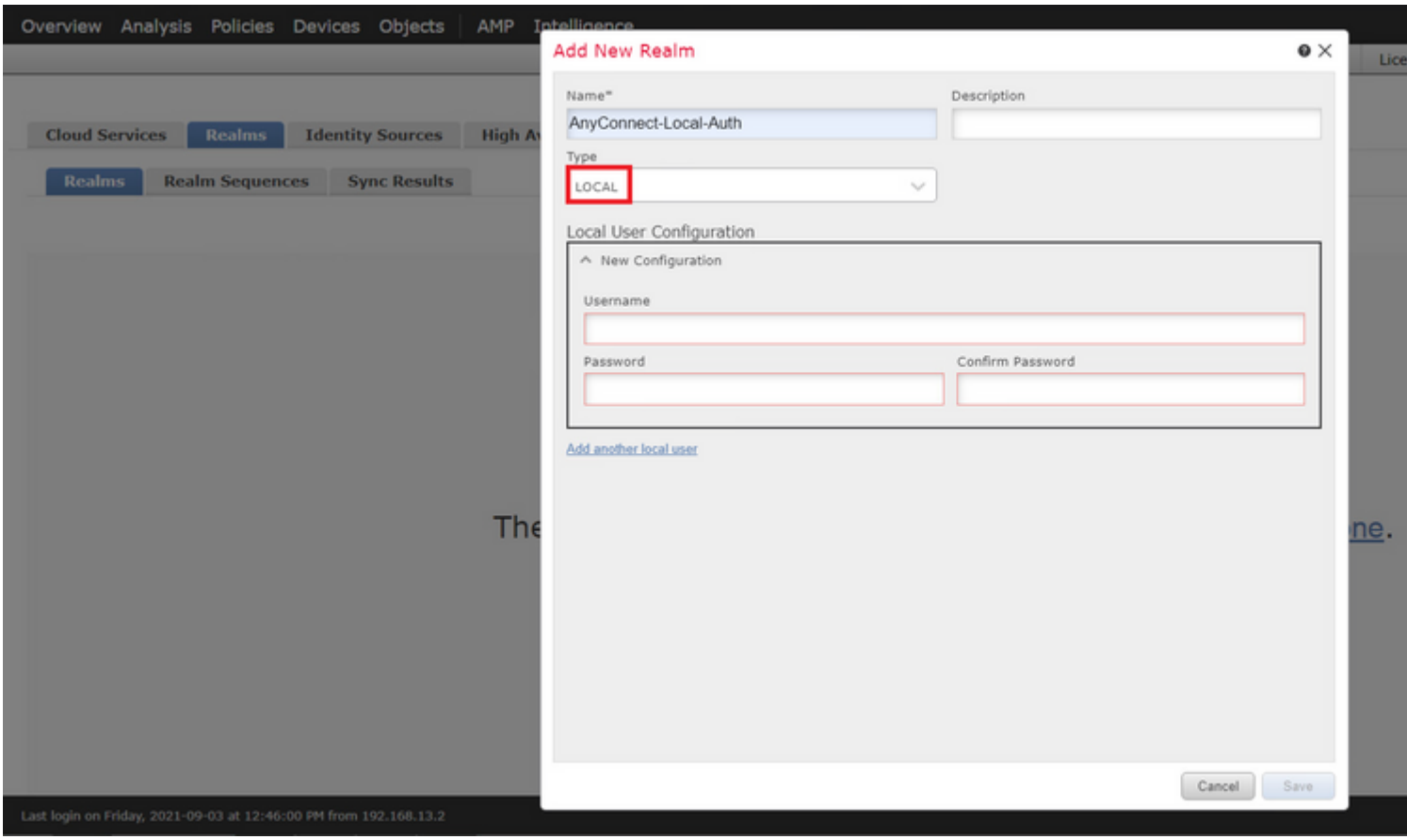


Schritt 4: Lokalen Bereich auf FMC erstellen

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**.

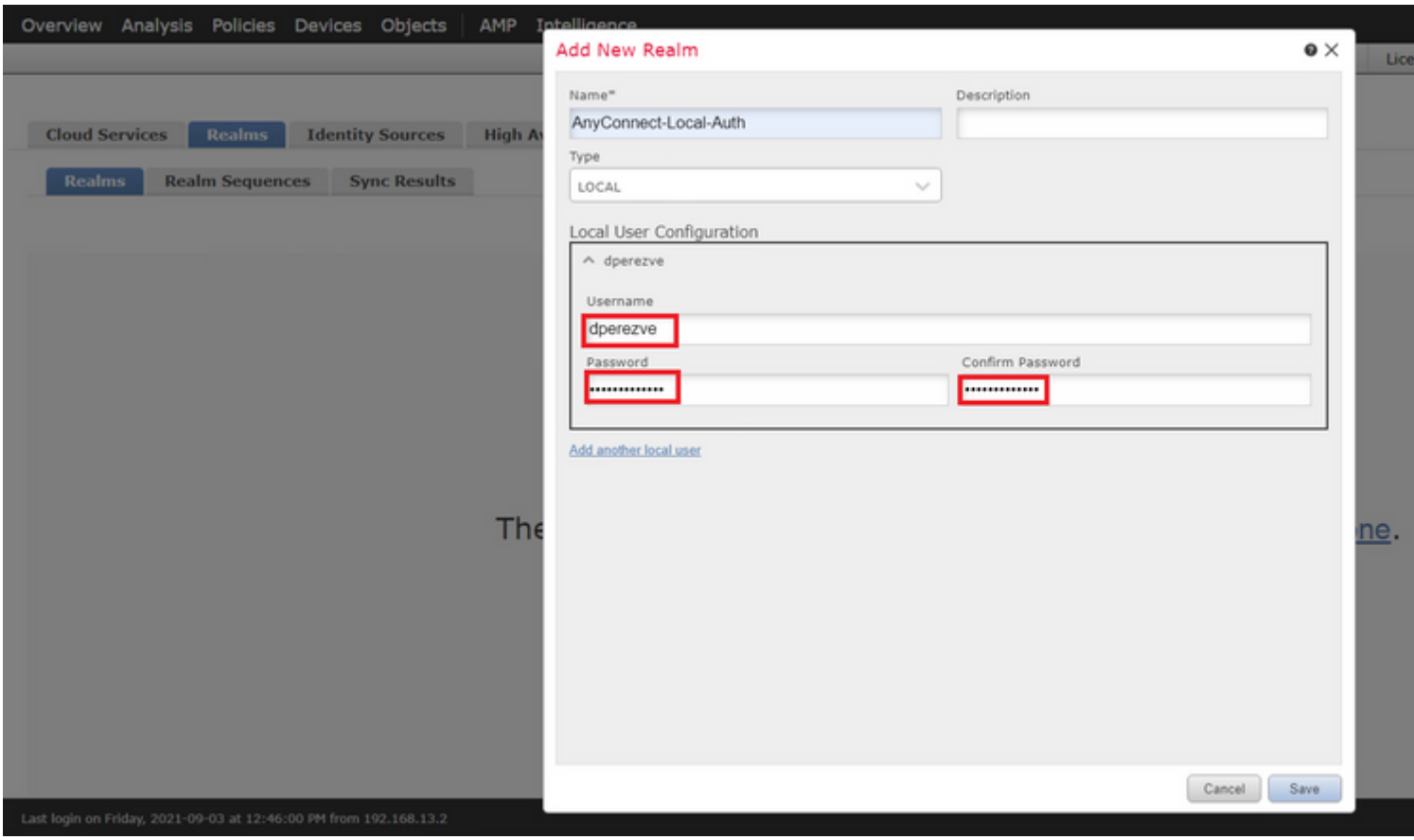


Wählen Sie die Schaltfläche **Bereich hinzufügen**. Weisen Sie im Fenster **Neuen Bereich hinzufügen** einen Namen zu, und wählen Sie im Dropdown-Menü **Typ** die Option **LOKAL**.

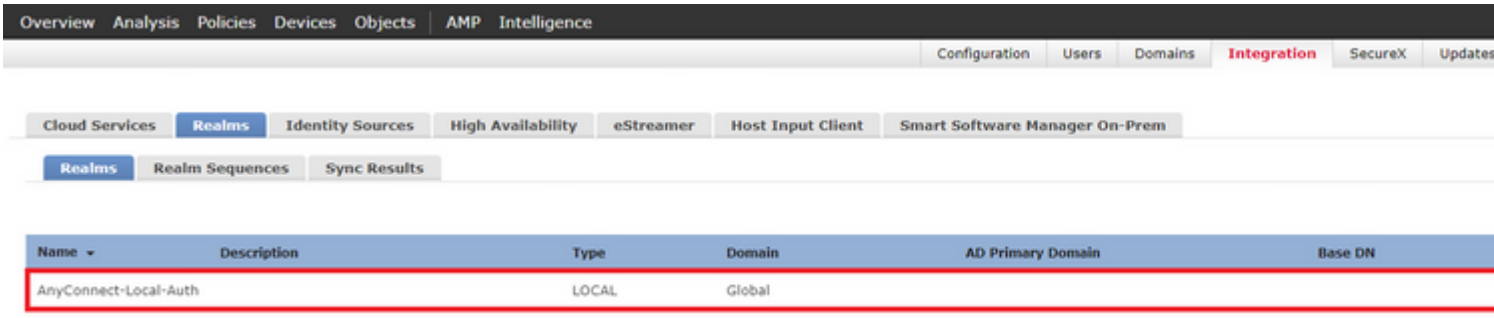


Benutzerkonten und Kennwörter werden im Abschnitt "Lokale Benutzerkonfiguration" erstellt.

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



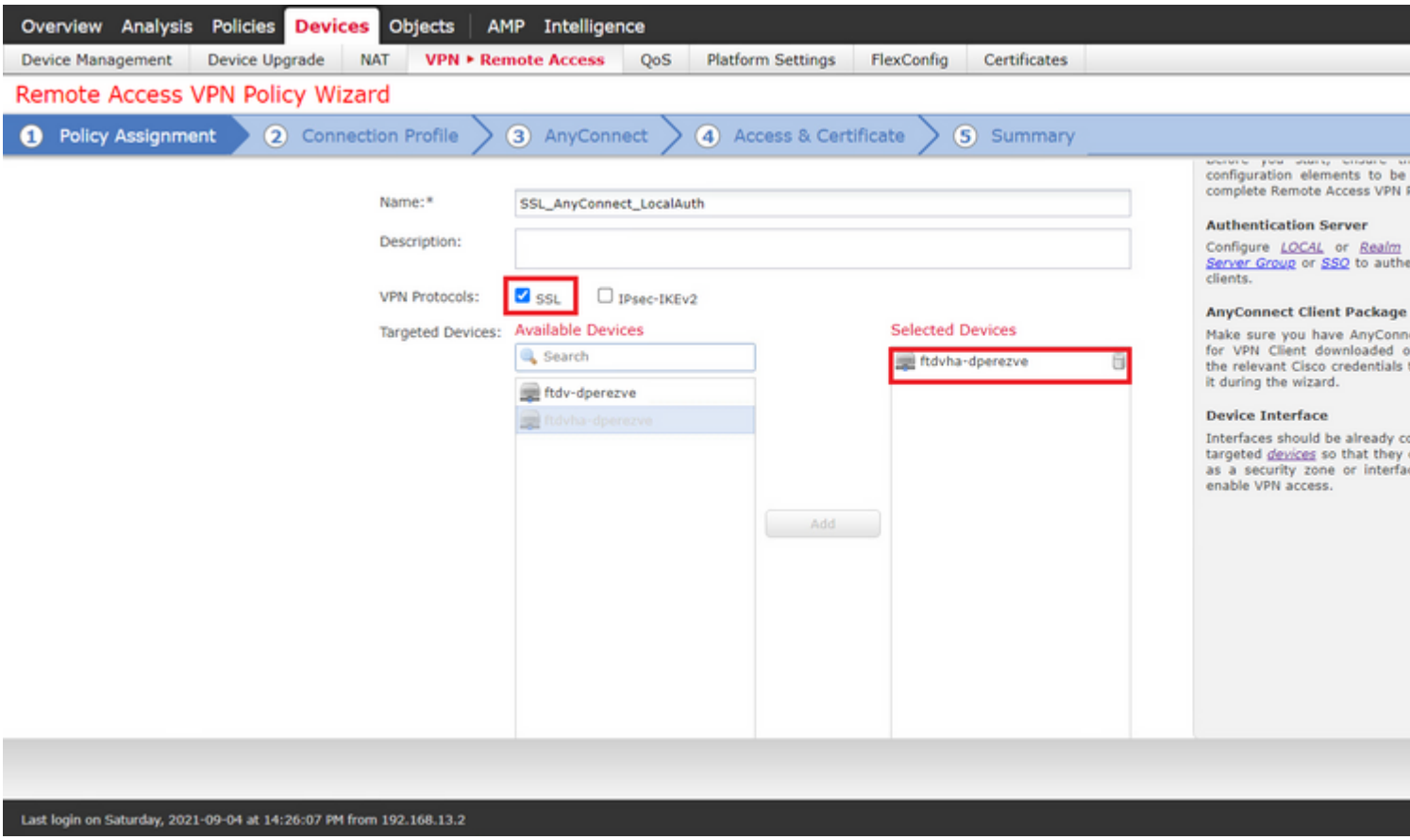
Die Änderungen **speichern** und der neue Bereich muss zur Liste der vorhandenen Bereiche hinzugefügt werden.



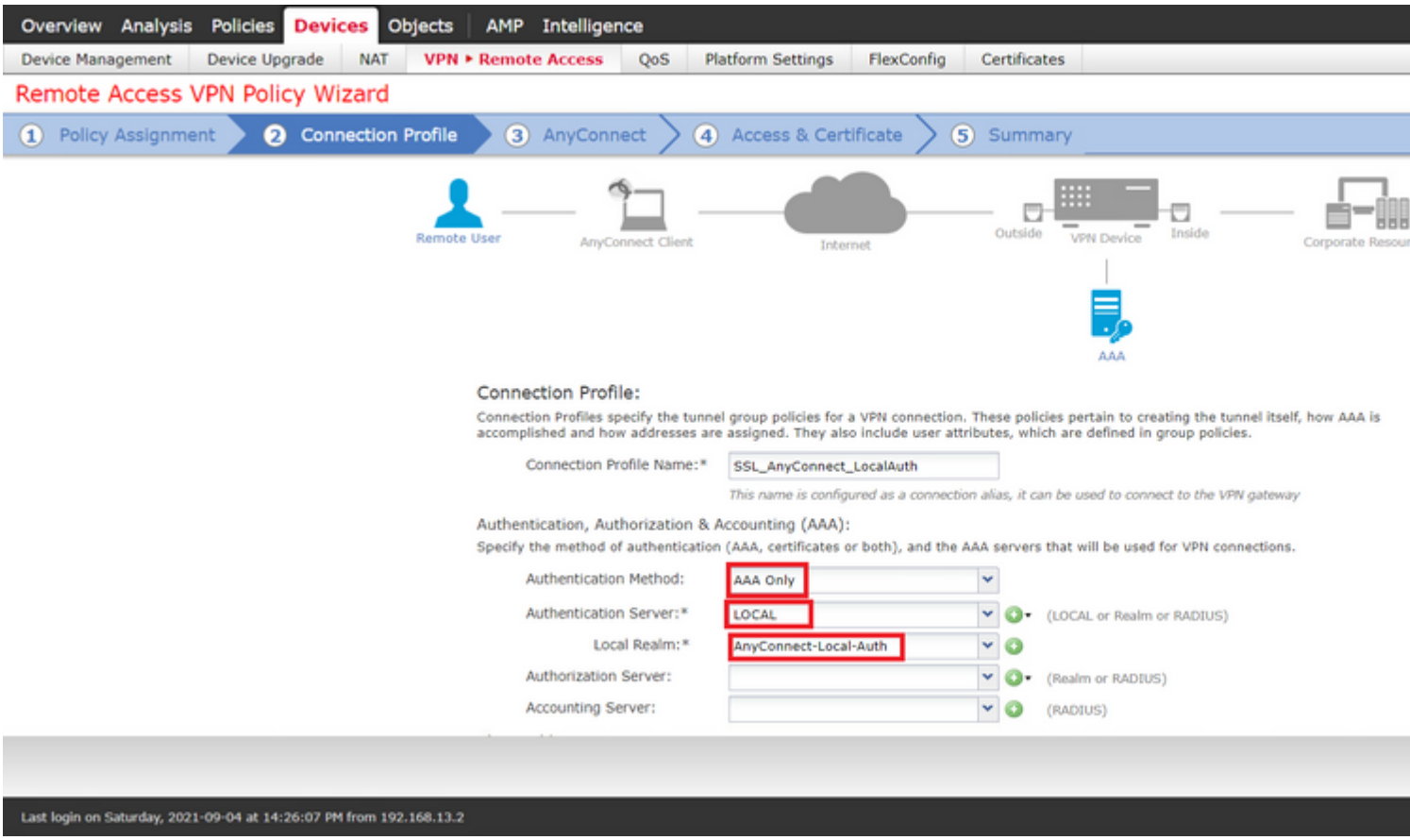
Schritt 5: SSL Cisco Secure Client konfigurieren

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

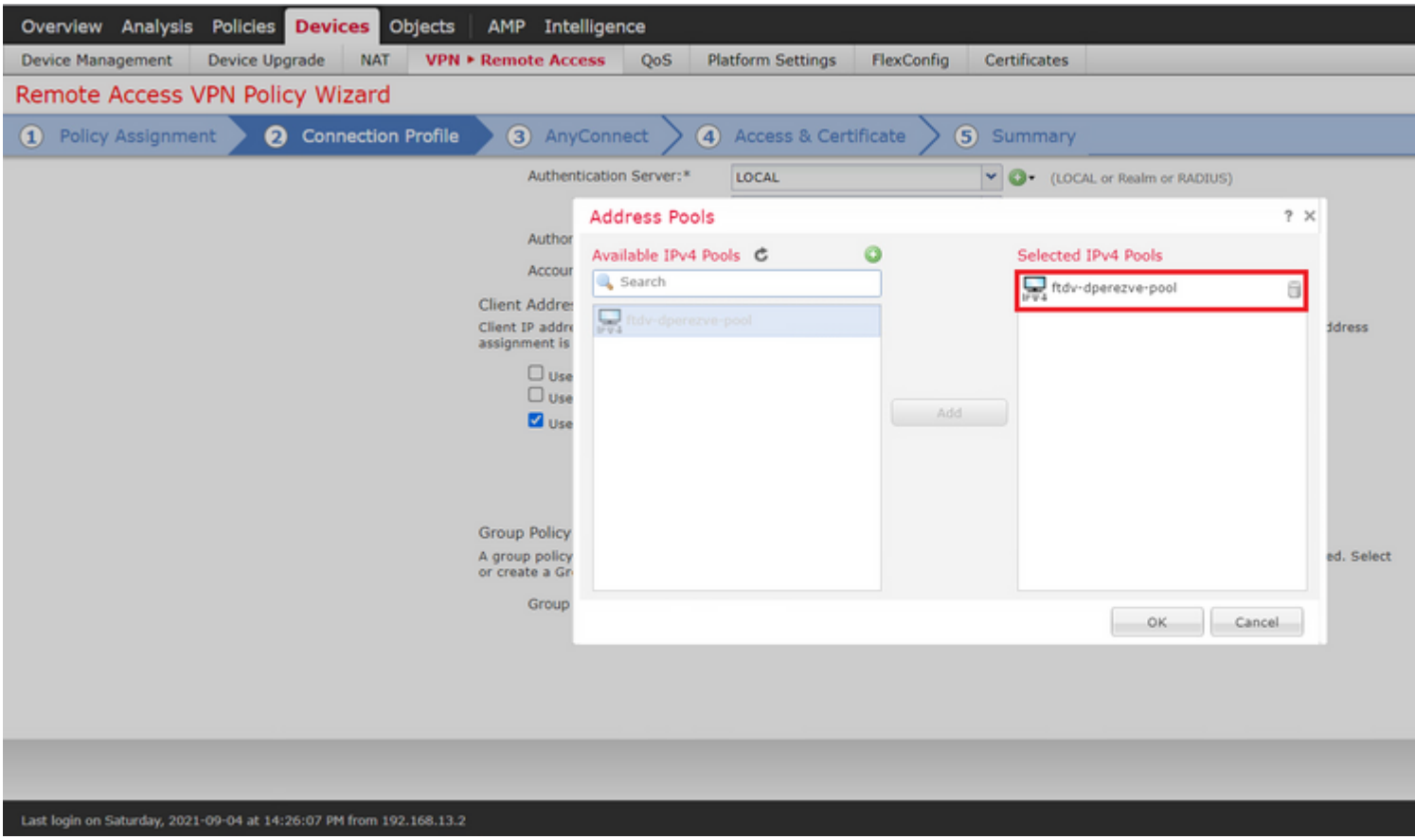
Wählen Sie **Hinzufügen** aus, um eine neue VPN-Richtlinie zu erstellen. Definieren Sie einen Namen für das Verbindungsprofil, aktivieren Sie das Kontrollkästchen SSL, und wählen Sie die verfügbare FTD als Zielgerät aus. Alle Einstellungen müssen im Abschnitt **Richtlinienzuweisung** im **Assistenten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



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.

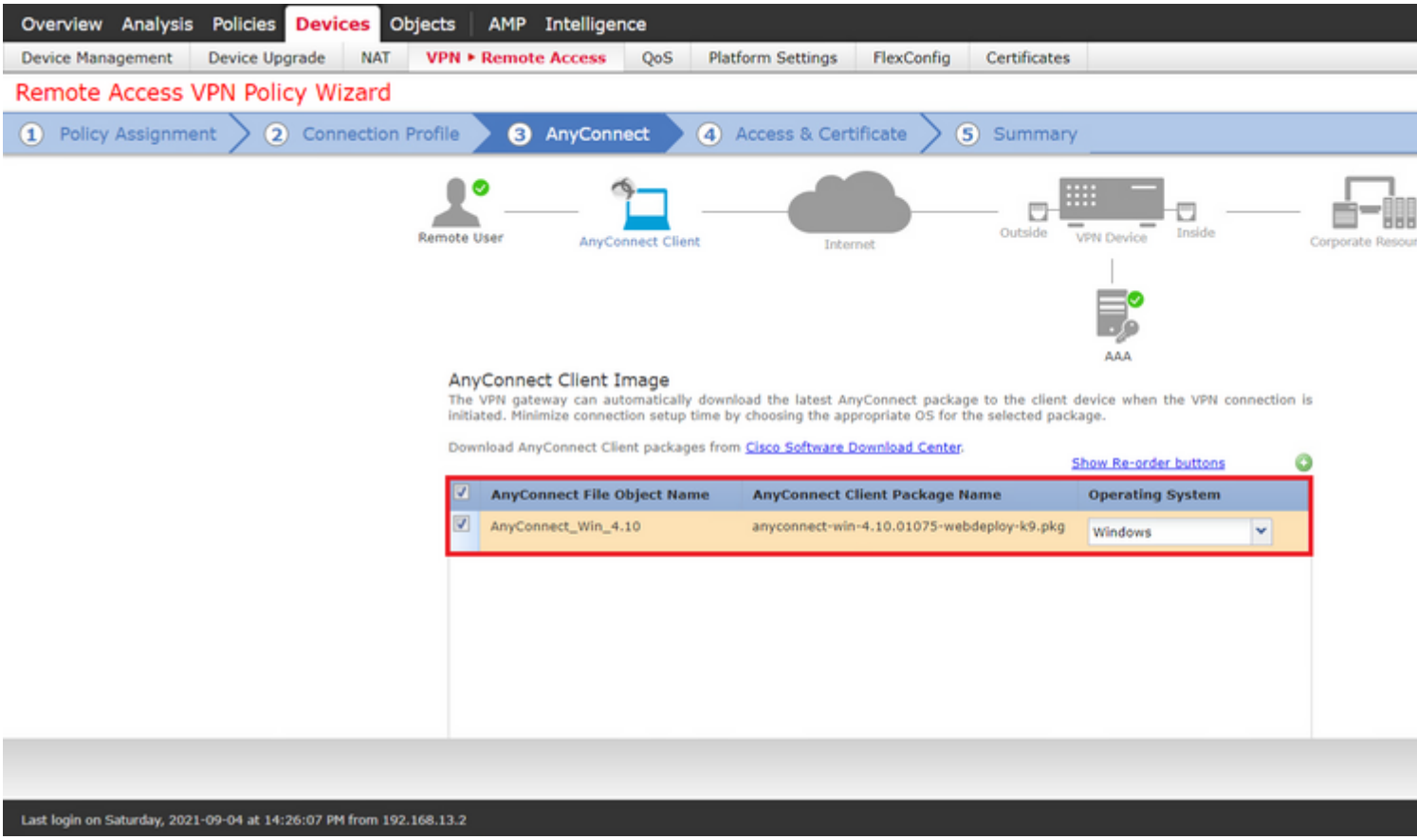


Führen Sie auf derselben Seite einen Bildlauf nach unten durch, und wählen Sie dann das Bleistiftsymbol im Abschnitt **IPv4-Adresspool aus,** um den von Cisco Secure Clients verwendeten IP-Pool zu definieren.

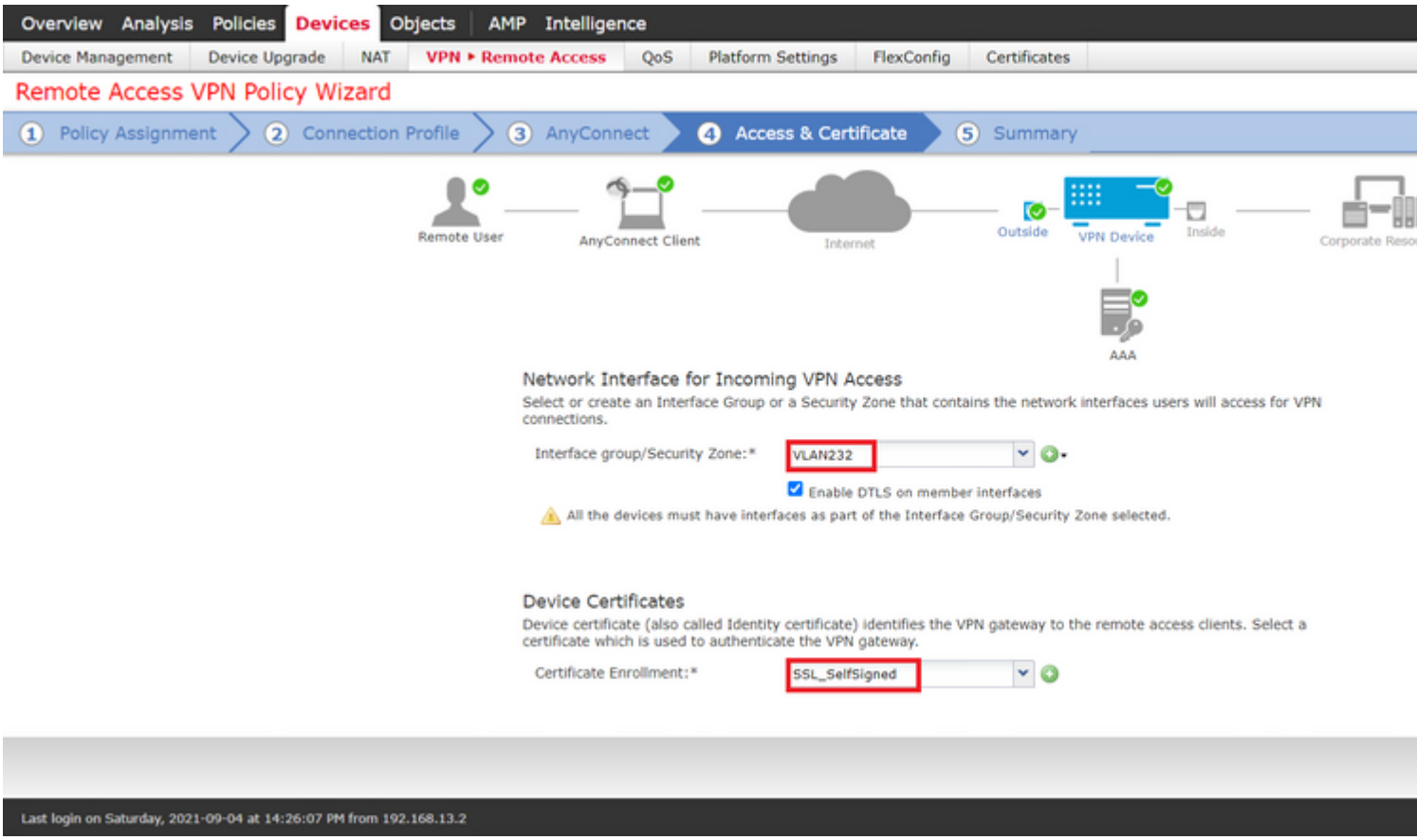


Wählen Sie **Weiter** aus, um zum Abschnitt **AnyConnect** zu wechseln. Wählen Sie nun das in Schritt 2

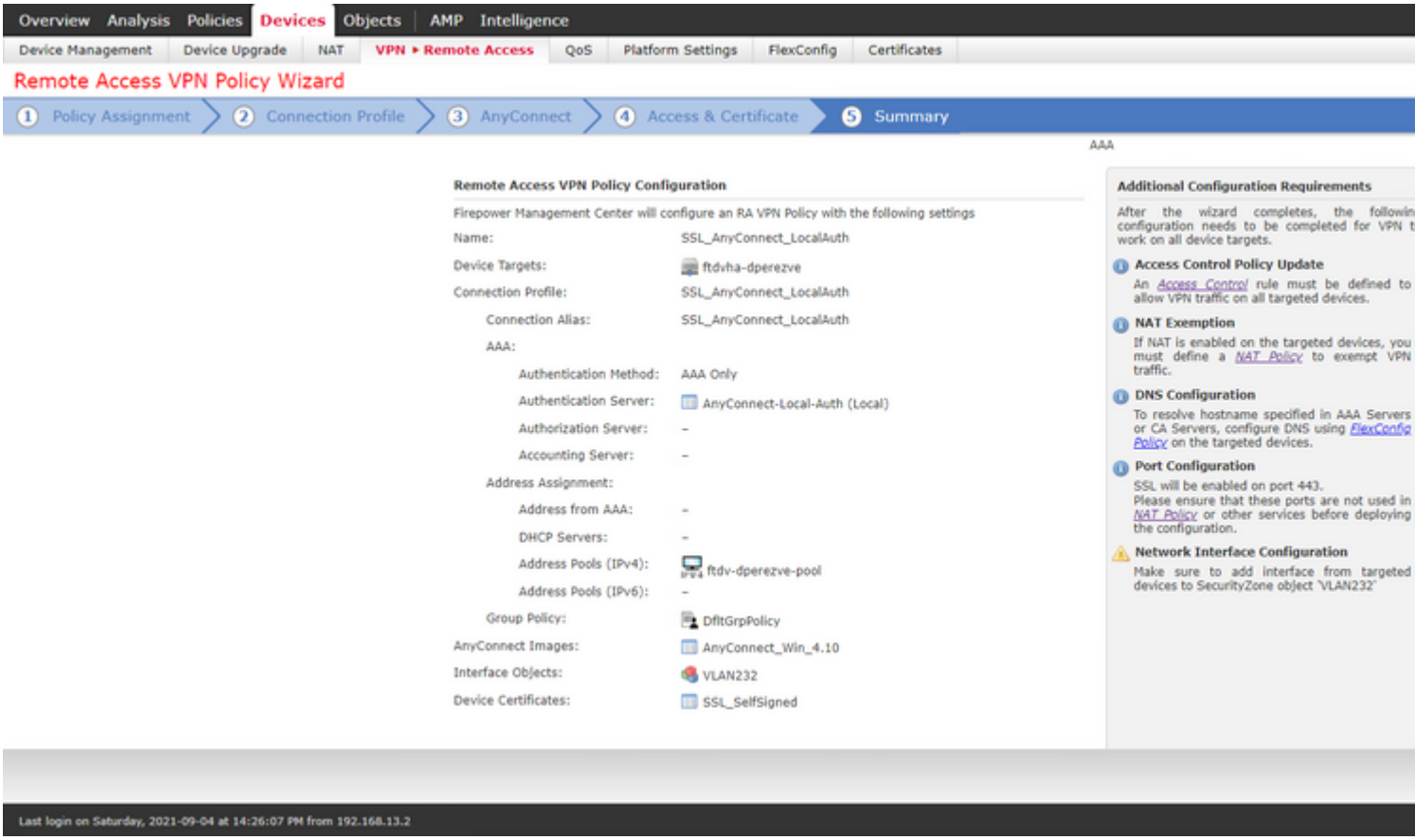
hochgeladene Cisco Secure Client-Image aus.



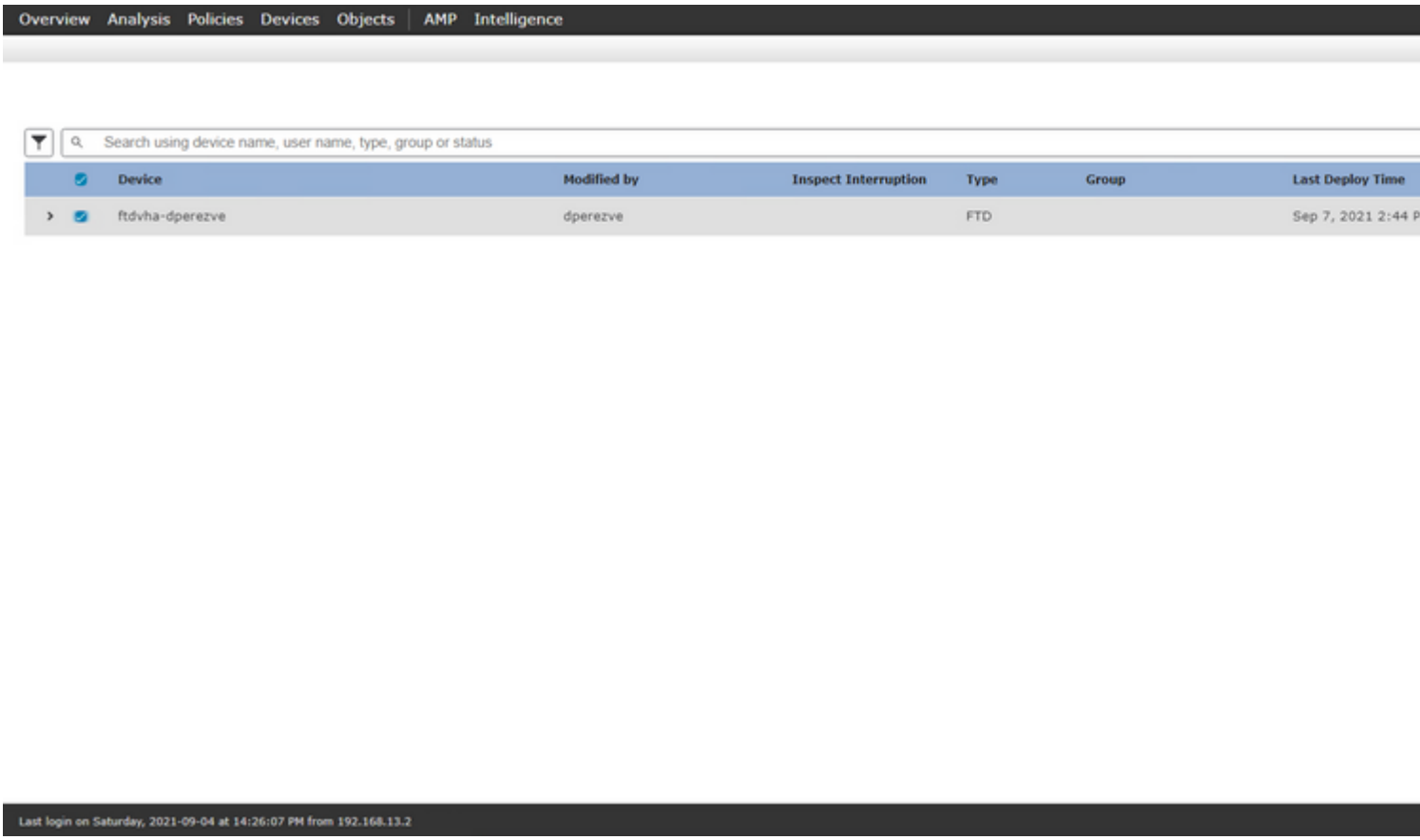
Wählen Sie **Weiter** aus, um zum Abschnitt **Zugriff und Zertifikat** zu wechseln. Wählen Sie im Dropdown-Menü **Interface group/Security Zone** (Schnittstellengruppe/Sicherheitszone) die Schnittstelle aus, auf der Cisco Secure Client (AnyConnect) aktiviert werden soll. Wählen Sie dann im Dropdown-Menü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



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

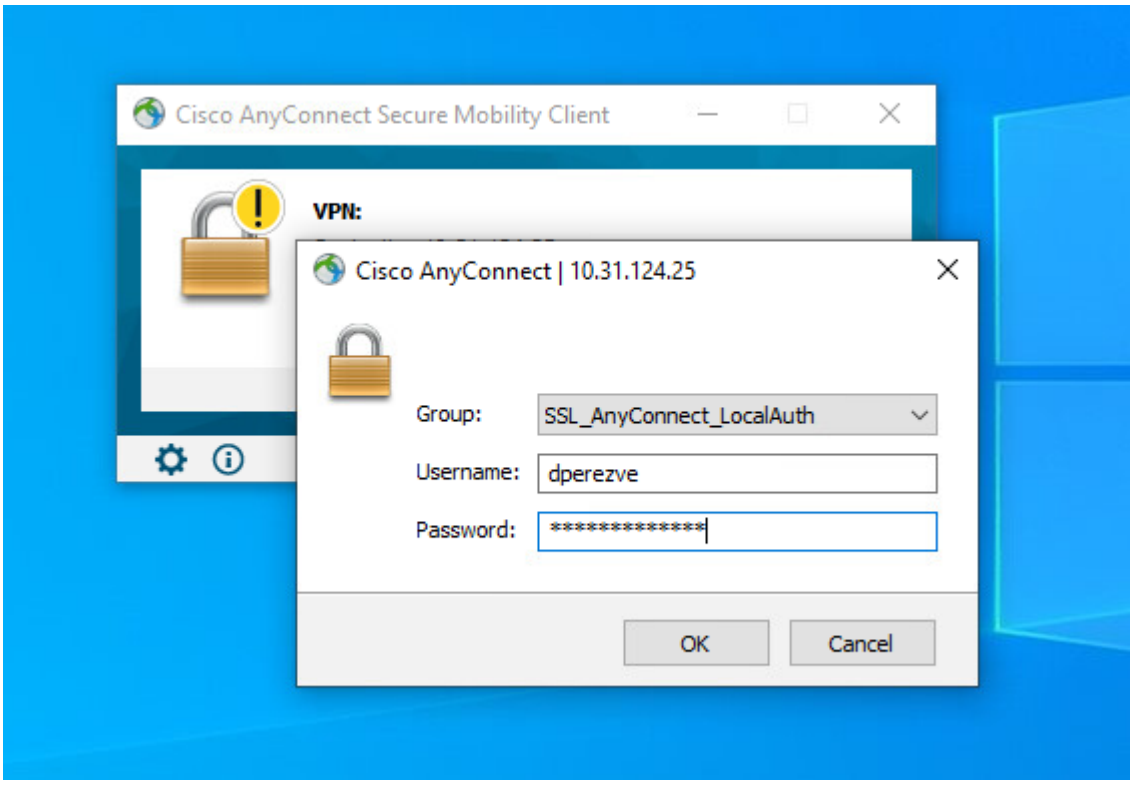


Wenn alle Einstellungen korrekt sind, wählen Sie **Beenden** und stellen Sie Änderungen in FTD bereit.

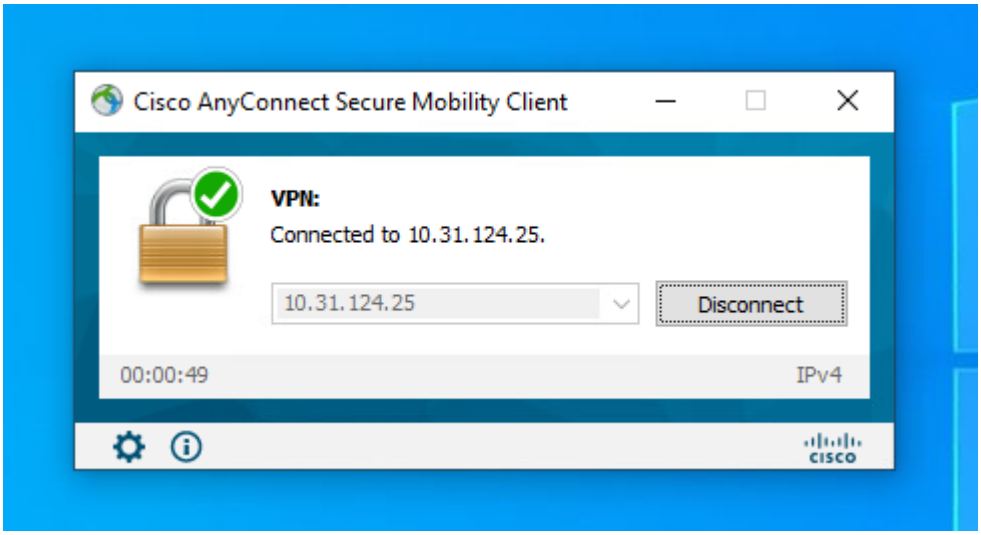


Überprüfung

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
```

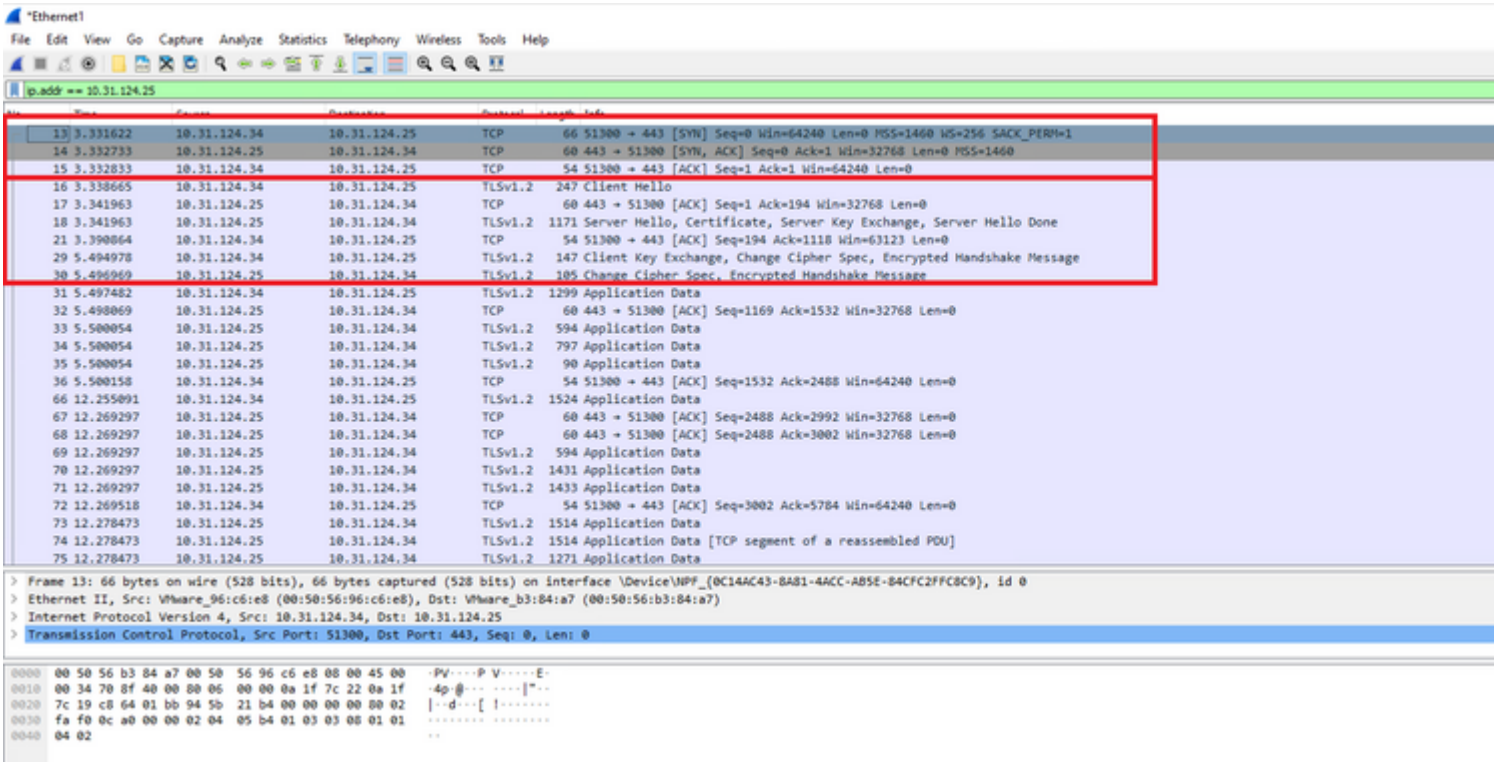
Fehlerbehebung

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.