# Konfigurieren der Authentifizierung von sicheren Client-Zertifikaten auf von FMC verwaltetem FTD

## Inhalt



## Einleitung

Dieses Dokument beschreibt den Prozess der Konfiguration eines Remote Access VPN auf Firepower Threat Defense (FTD), das vom Firepower Management Center (FMC) mit Zertifikatsauthentifizierung verwaltet wird.

Beitrag von Dolly Jain und Rishabh Aggarwal, Cisco TAC Engineer.

## Voraussetzungen

### Anforderungen

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

- Manuelle Zertifikatsregistrierung und Grundlagen von SSL
FMC
- Grundlegende Authentifizierungskenntnisse für Remote Access VPN
- Zertifizierungsstelle eines Drittanbieters (Certificate Authority, CA) wie Entrust, Geotrust, GoDaddy, Thawte und VeriSign

### Verwendete Komponenten

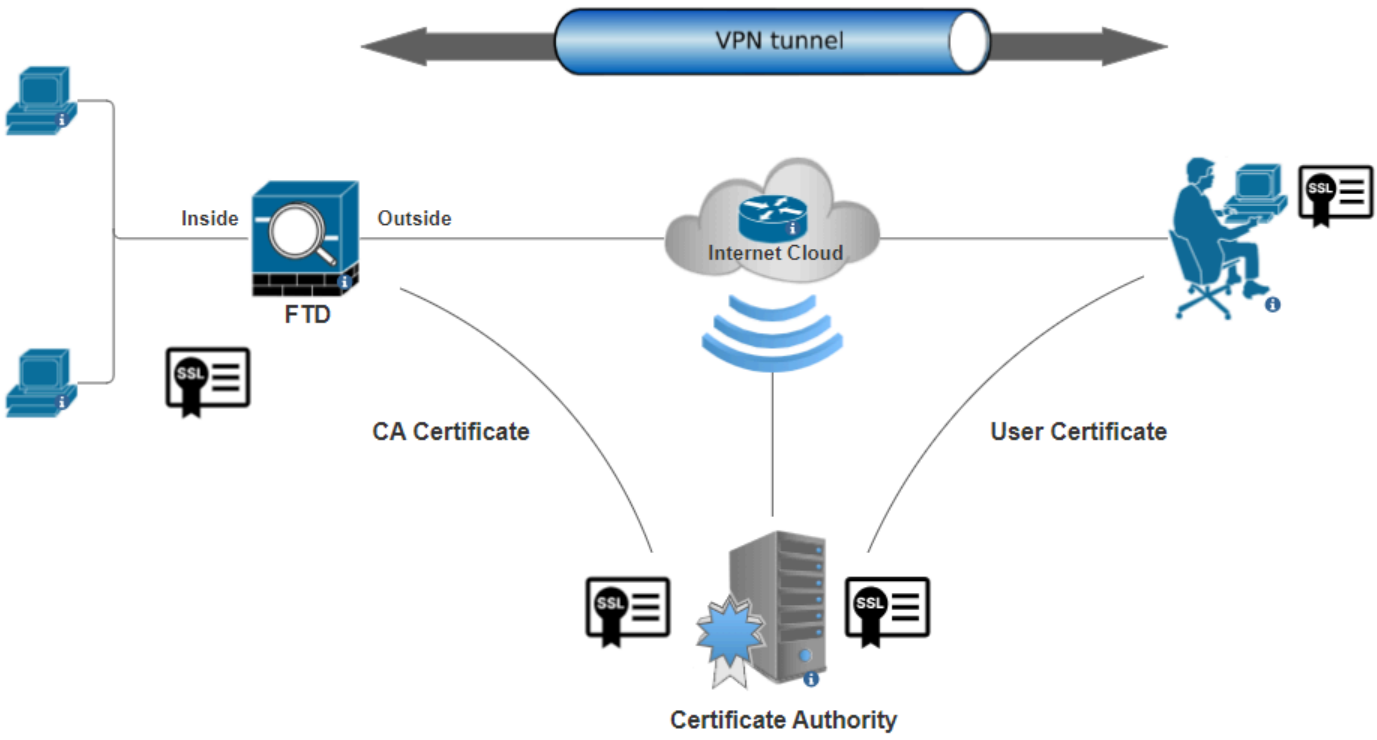
Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Sichere Firepower Threat Defense Version 7.4.1
- FirePOWER Management Center (FMC) Version 7.4.1
- Secure Client Version 5.0.05040
- Microsoft Windows Server 2019 als CA-Server

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.

# Konfigurieren

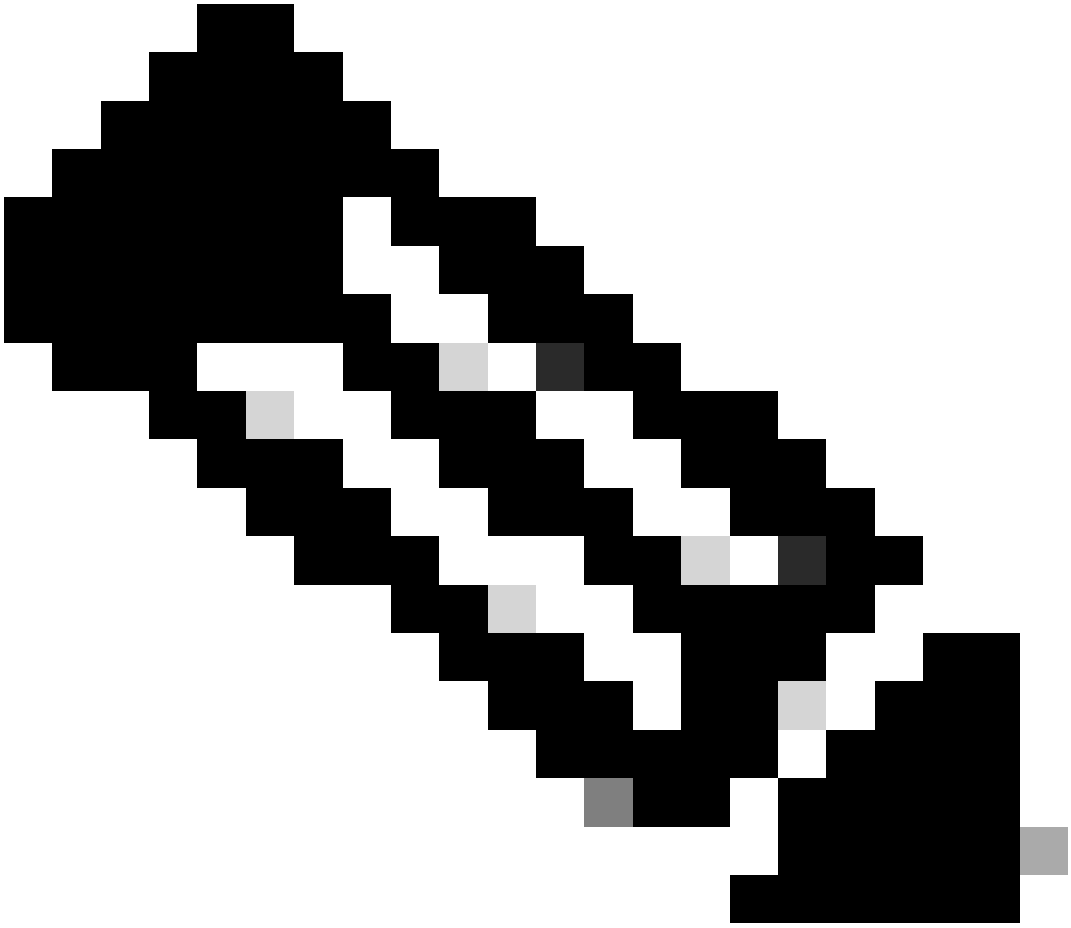
## Netzwerkdiagramm




Netzwerkdiagramm

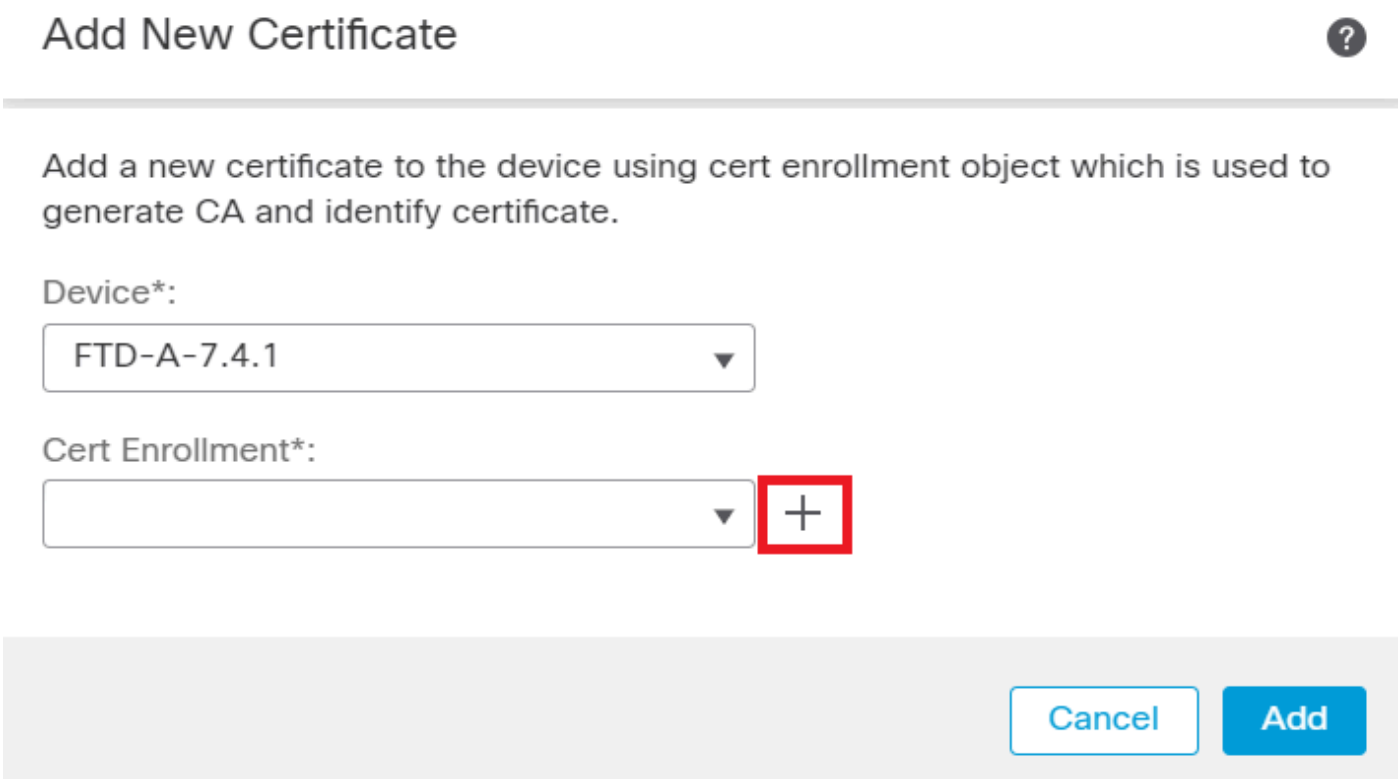
## Konfigurationen

a. Erstellen/Importieren eines Zertifikats für die Serverauthentifizierung



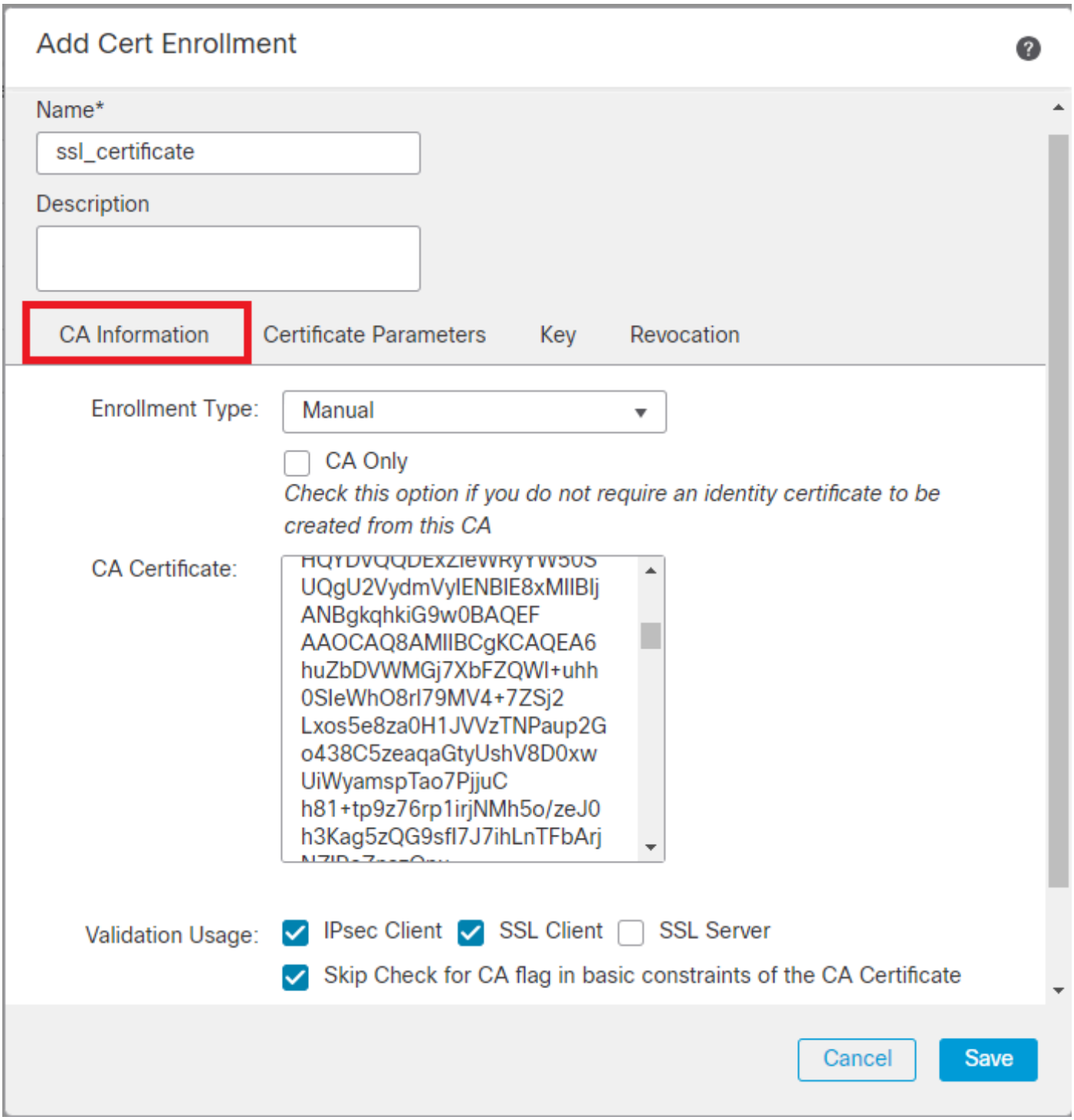
Hinweis: Auf FMC ist ein CA-Zertifikat erforderlich, bevor Sie den CSR generieren können. Wenn der CSR von einer externen Quelle (OpenSSL oder einem Drittanbieter) generiert wird, schlägt die manuelle Methode fehl, und das PKCS12-Zertifikatformat muss verwendet werden.

Schritt 1: Navigieren Sie zu, Devices > Certificatesund klicken Sie auf Add. Wählen Sie Gerät aus, und klicken Sie unter Zertifikatregistrierung auf das Pluszeichen (+).




*Zertifikatregistrierung hinzufügen*

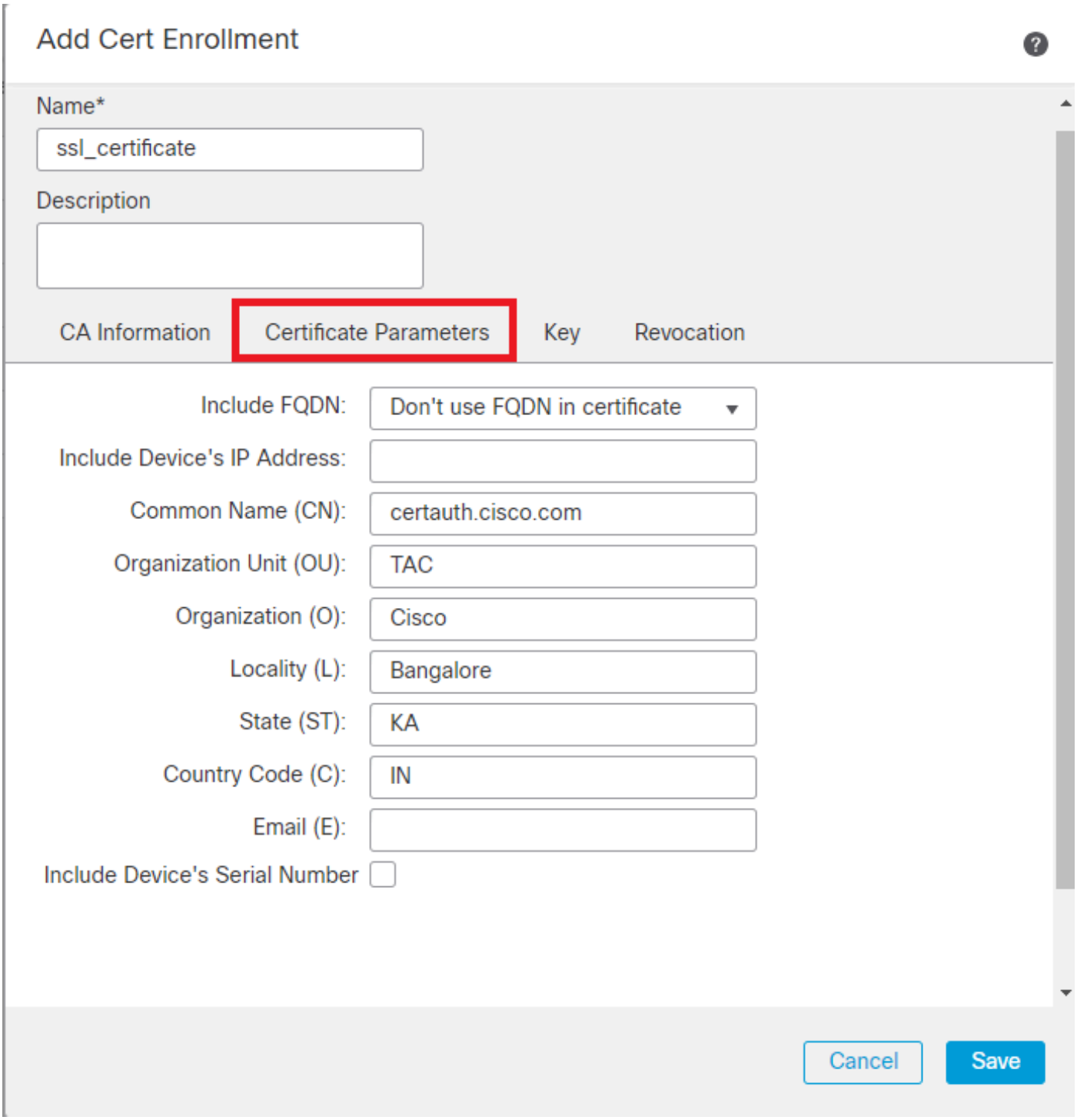
Schritt 2: Wählen Sie unterCA Information den Registrierungstyp als aus, und fügen Sie das Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) ein, das zum Signieren des CSR verwendet wirdManual.




*CA-Informationen hinzufügen*

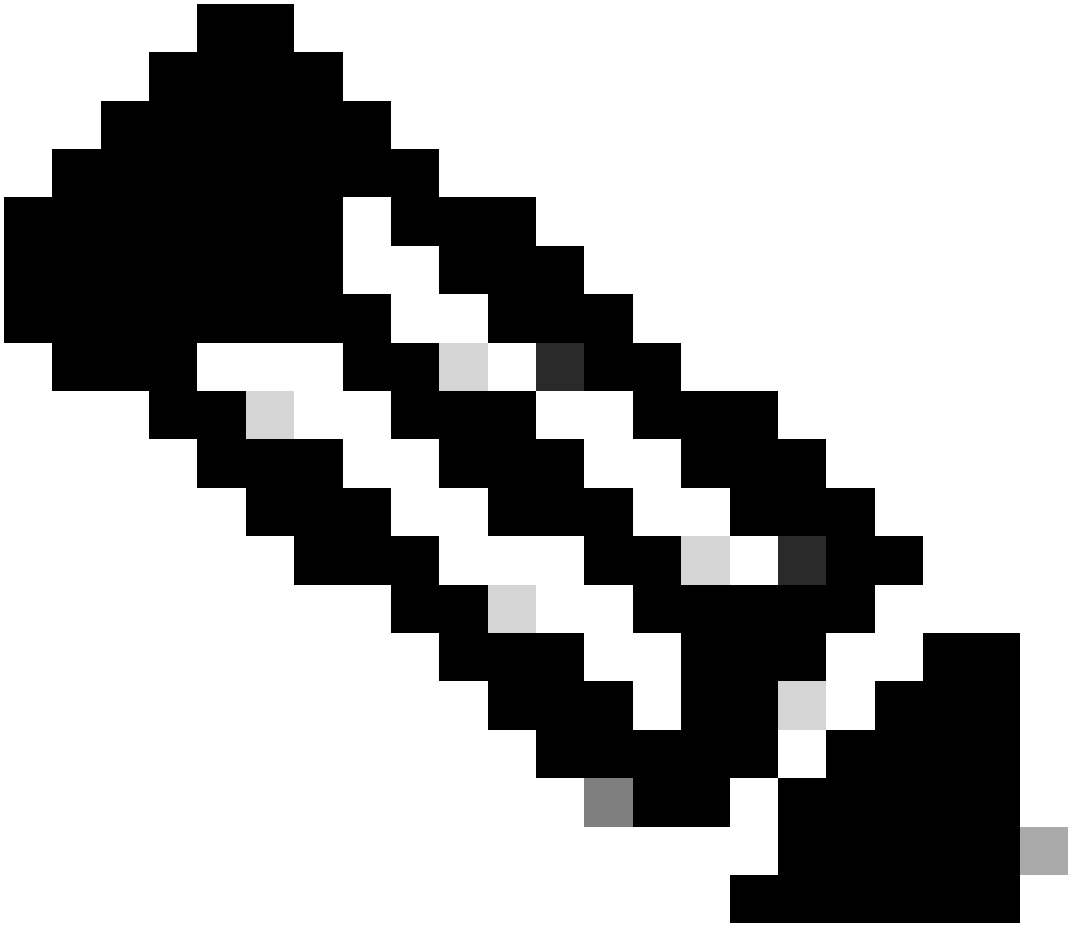
Schritt 3: Wählen Sie für die Validierungsverwendung IPsec Client, SSL Client und Skip Check for CA flag in basic constraints of the CA Certificate.

Schritt 4: Geben Sie unter Certificate Parameters die Details zum Betreff ein.

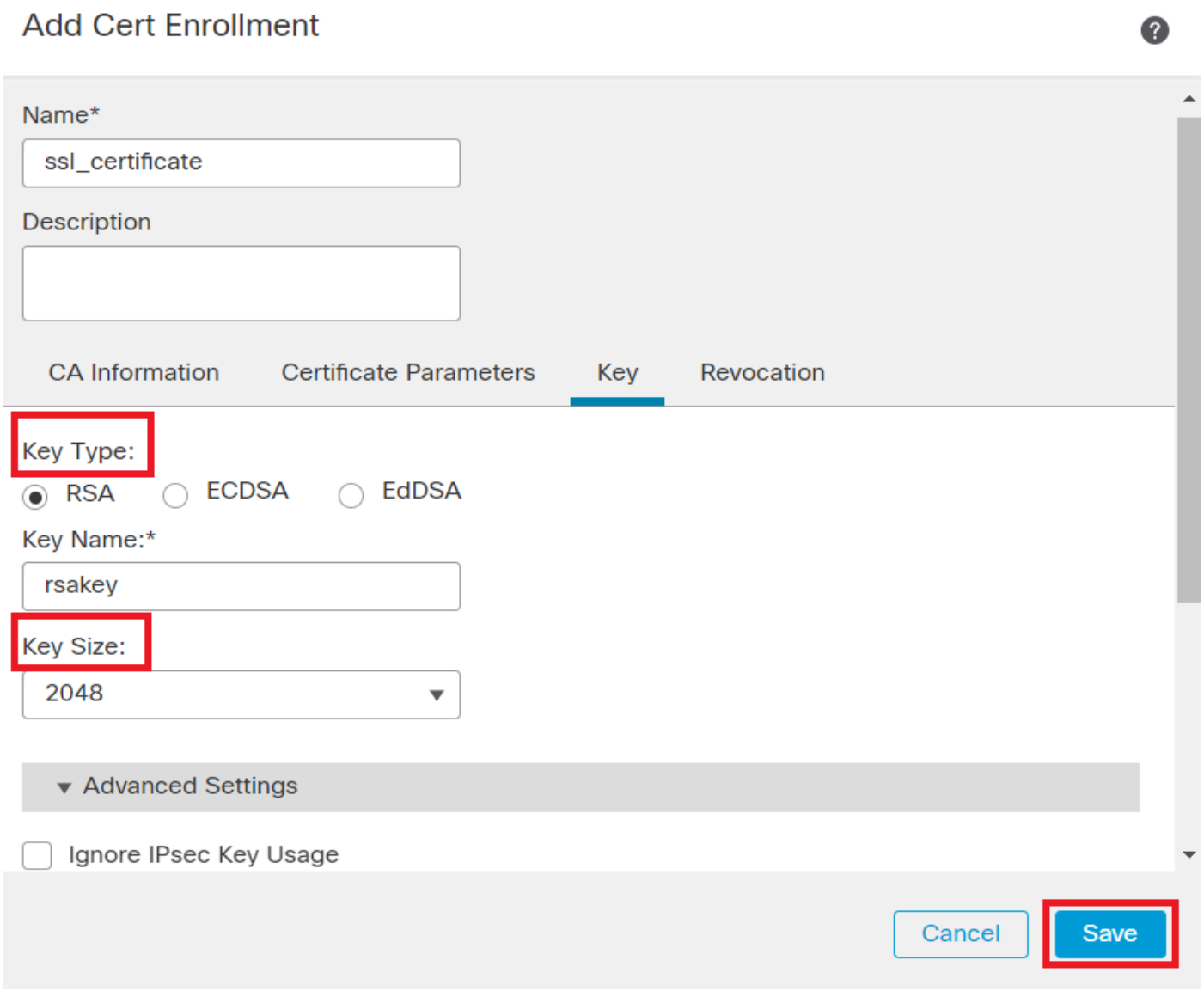



*Zertifikatsparameter hinzufügen*

Schritt 5: Wählen KeySie unter den Schlüsseltyp RSA mit einem Schlüsselnamen und einer Schlüsselgröße aus. Klicken Sie auf Save.

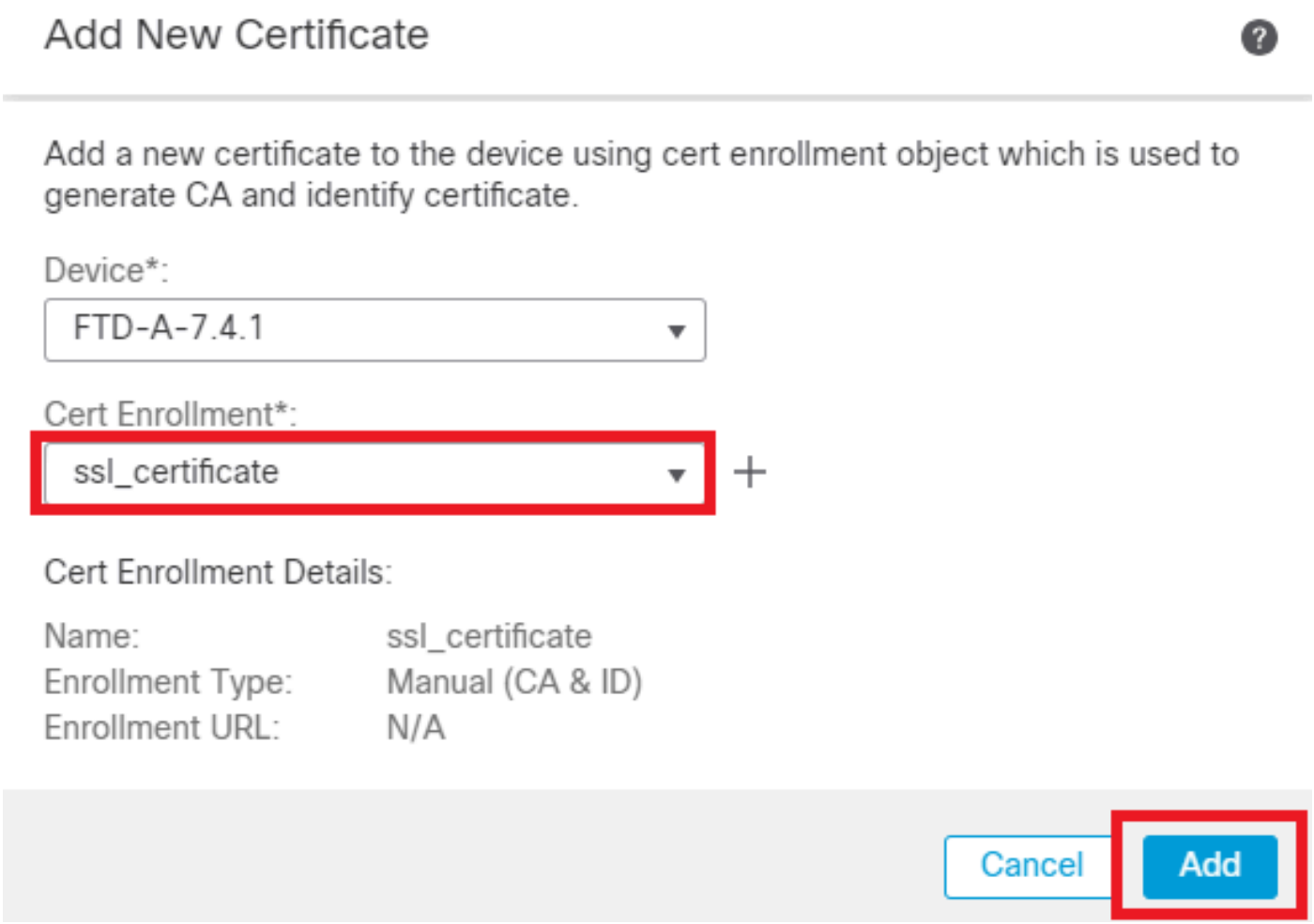


**Hinweis**: Für den RSA-Schlüsseltyp beträgt die minimale Schlüsselgröße 2048 Bit.



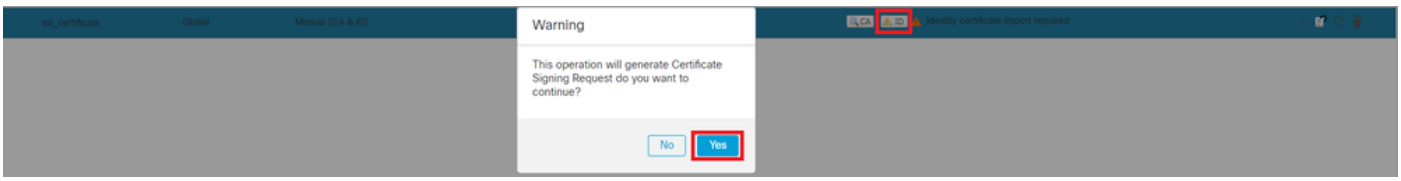

*RSA-Schlüssel hinzufügen*

Schritt 6: Wählen Sie unter Cert Enrollment den Vertrauenspunkt aus der Dropdown-Liste aus, die gerade erstellt wurde, und klicken Sie auf Add.



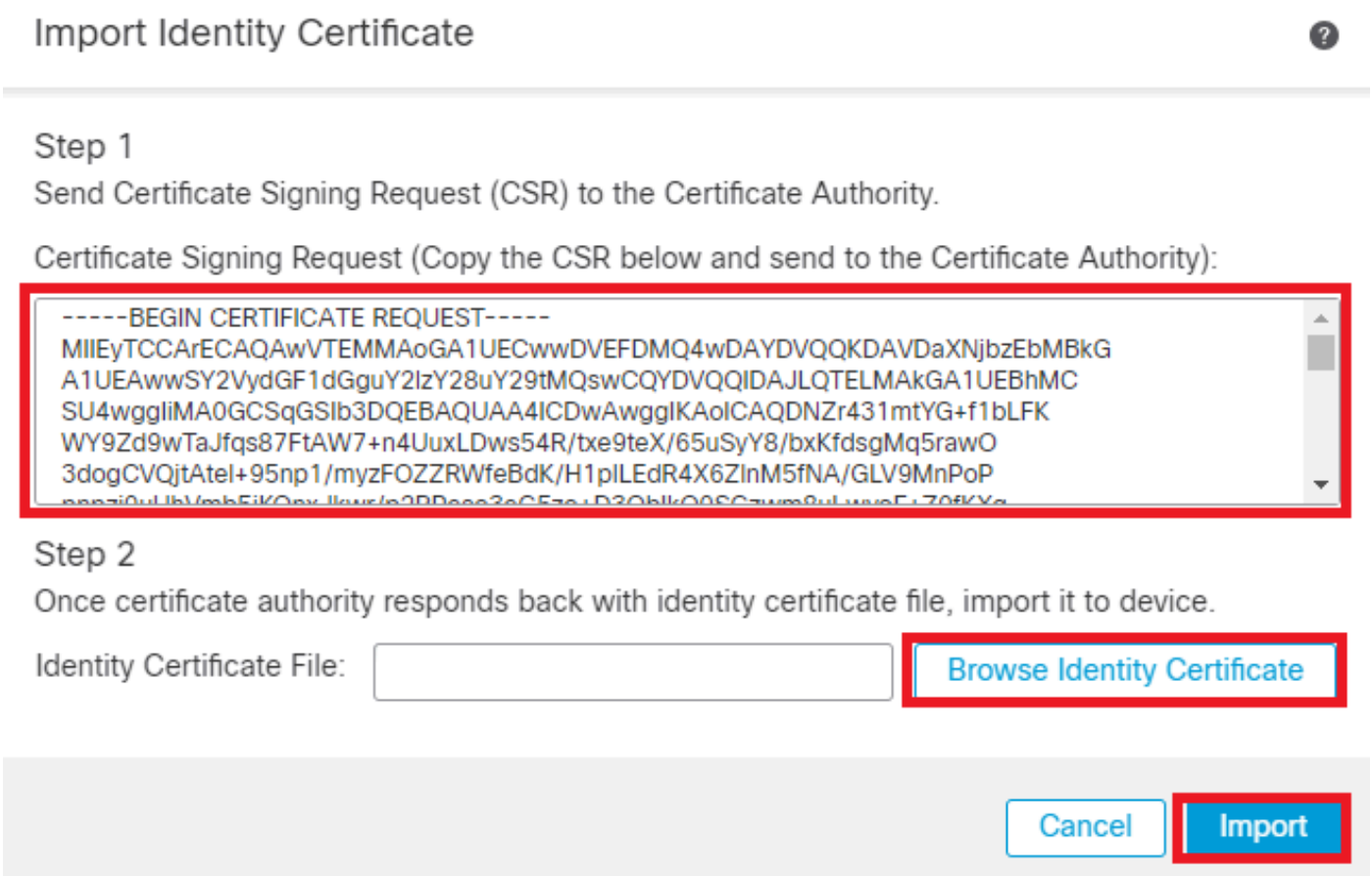

*Neues Zertifikat hinzufügen*

Schritt 7. Klicken Sie auf ID und anschließend auf dieYes weitere Eingabeaufforderung, um die CSR-Anfrage zu erstellen.

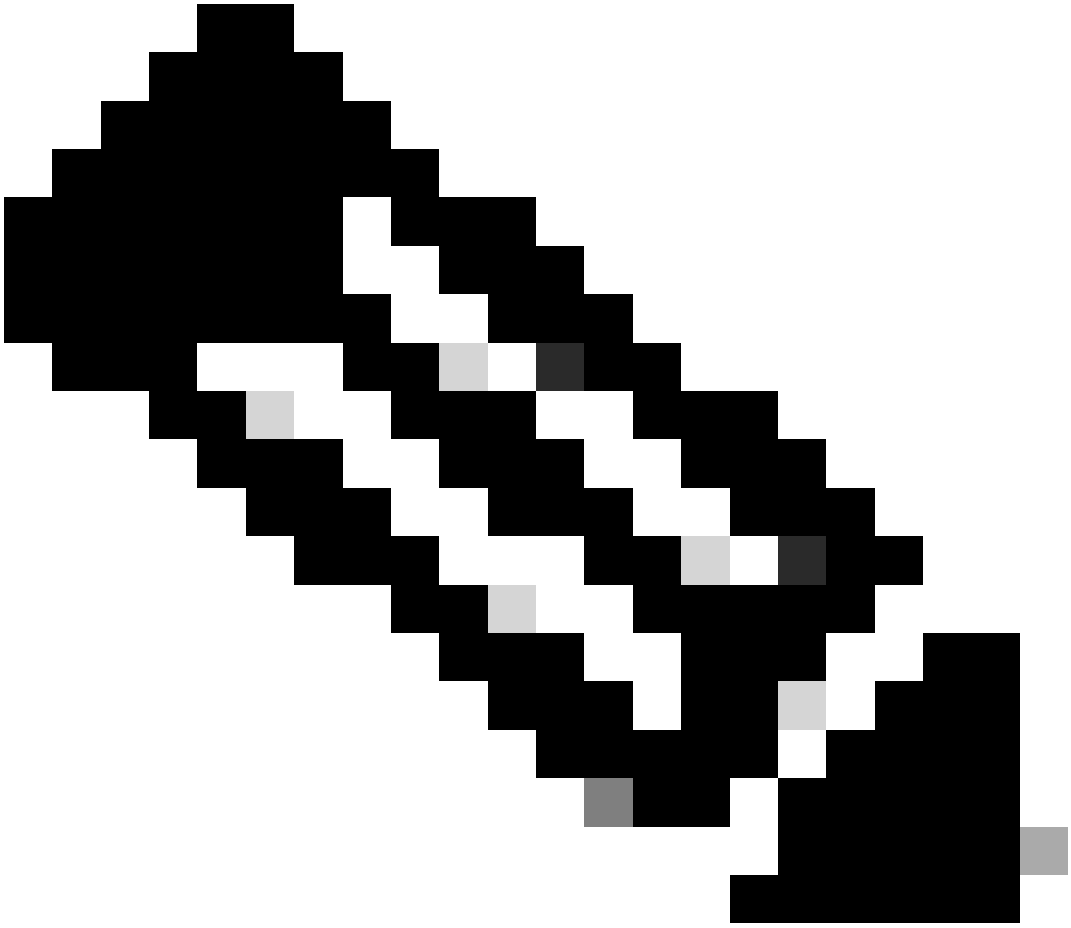



*CSR erstellen*

Schritt 8: Kopieren Sie die CSR-Datei, und lassen Sie sie von der Zertifizierungsstelle signieren. Sobald das Identitätszertifikat von der Zertifizierungsstelle ausgestellt wurde, importieren Sie es, indem Sie auf klicken Browse Identity Certificate und dann auf klickenImport.



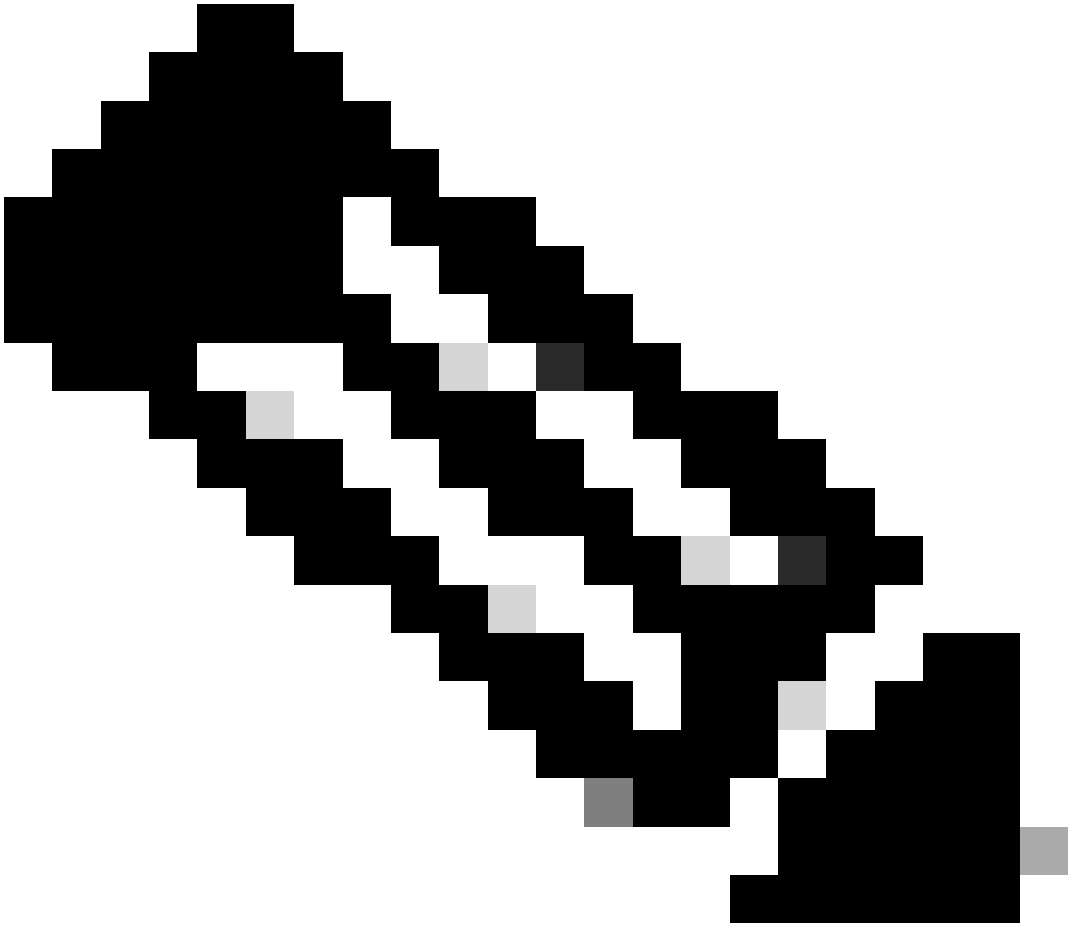

*ID-Zertifikat importieren*



**Hinweis**: Wenn die Ausstellung des ID-Zertifikats Zeit in Anspruch nimmt, können Sie Schritt 7 später wiederholen. Dadurch wird derselbe CSR generiert, und wir können das ID-Zertifikat importieren.

---

**b. Hinzufügen eines Zertifikats einer vertrauenswürdigen/internen Zertifizierungsstelle**



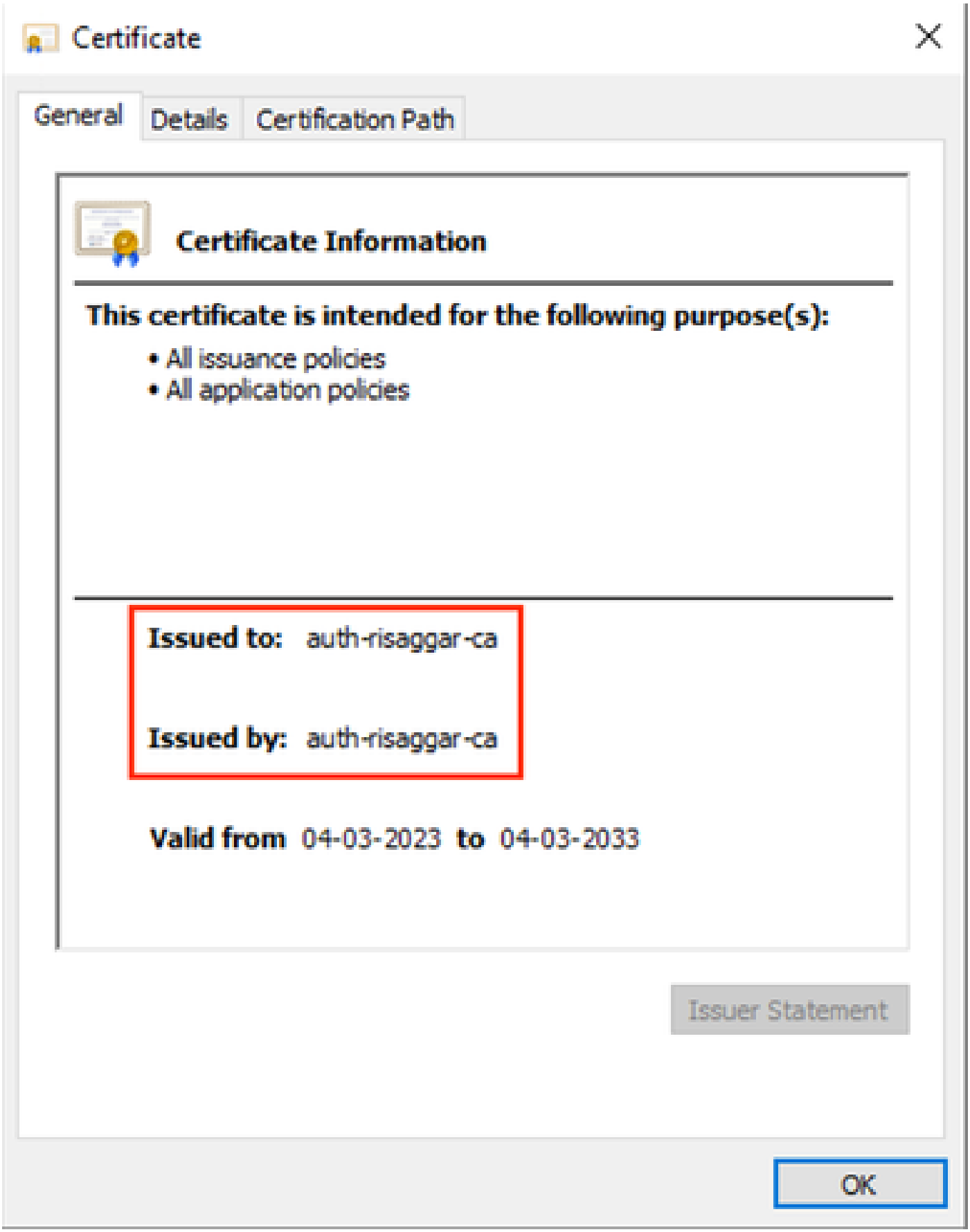
**Hinweis:** Wenn die in Schritt (a), **"Erstellen/Importieren eines für die Serverauthentifizierung verwendeten Zertifikats" verwendete Zertifizierungsstelle (Certificate Authority, CA) auch** Benutzerzertifikate ausstellt, können Sie **Schritt (b)**, "Hinzufügen eines vertrauenswürdigen/internen Zertifizierungsstellenzertifikats", überspringen. Es ist nicht erforderlich, dasselbe Zertifizierungsstellenzertifikat erneut hinzuzufügen, und es muss ebenfalls vermieden werden. Wenn dasselbe CA-Zertifikat erneut hinzugefügt wird, wird "trustpoint" mit "validation-usage none" konfiguriert, was sich auf die Zertifikatsauthentifizierung für RAVPN auswirken kann.

---

Schritt 1: Navigieren Sie zu, Devices > Certificates und klicken Sie auf Add.

Wählen Sie Gerät aus, und klicken Sie unter Zertifikatregistrierung auf das Pluszeichen (+).

Hier wird "auth-risaggar-ca" verwendet, um Identitäts-/Benutzerzertifikate auszustellen.

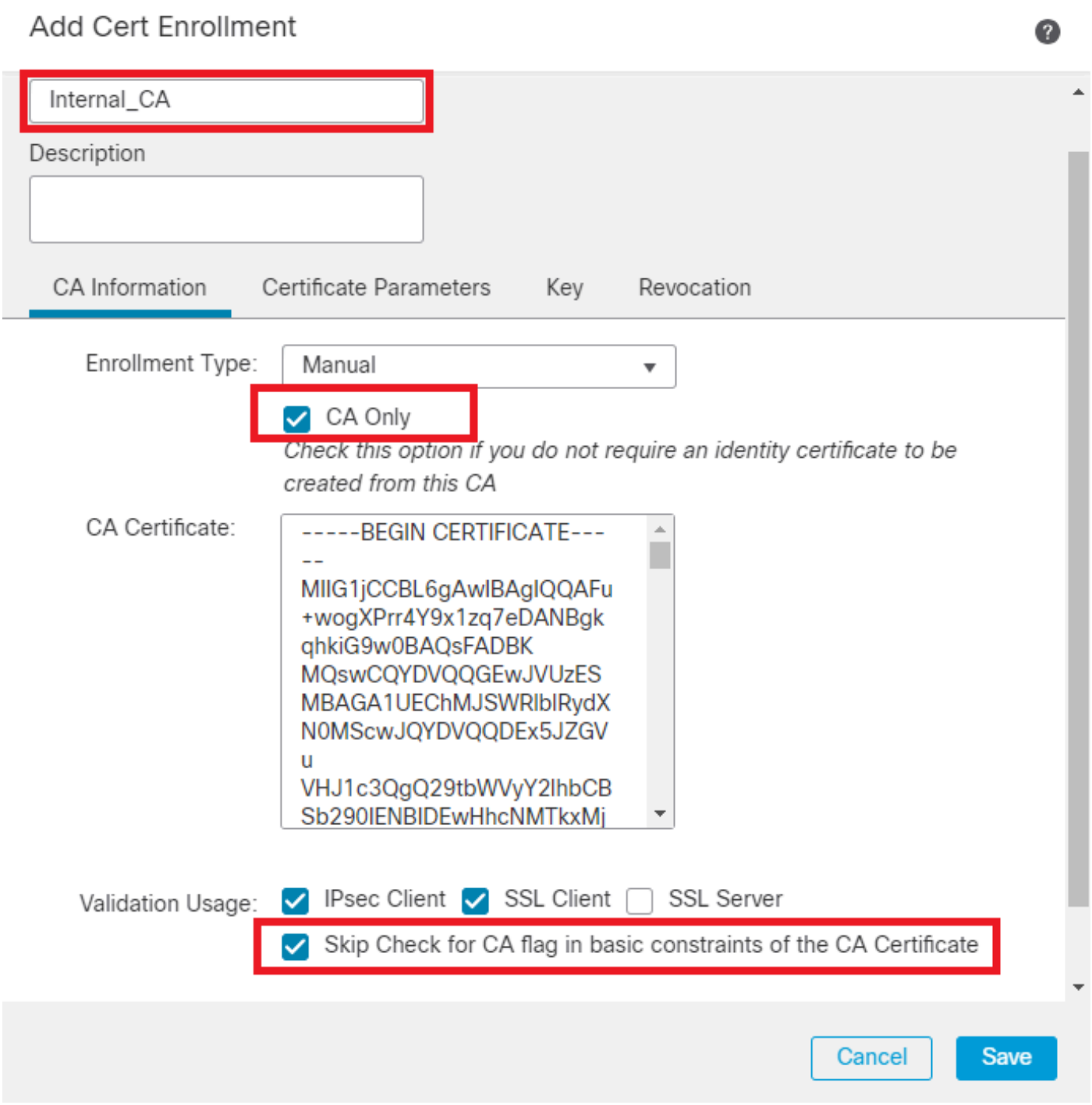



*auth-risaggar-ca*

Schritt 2: Geben Sie einen Namen für einen Vertrauenspunkt ein, und wählen SieManual unter CA information den Registrierungstyp aus.

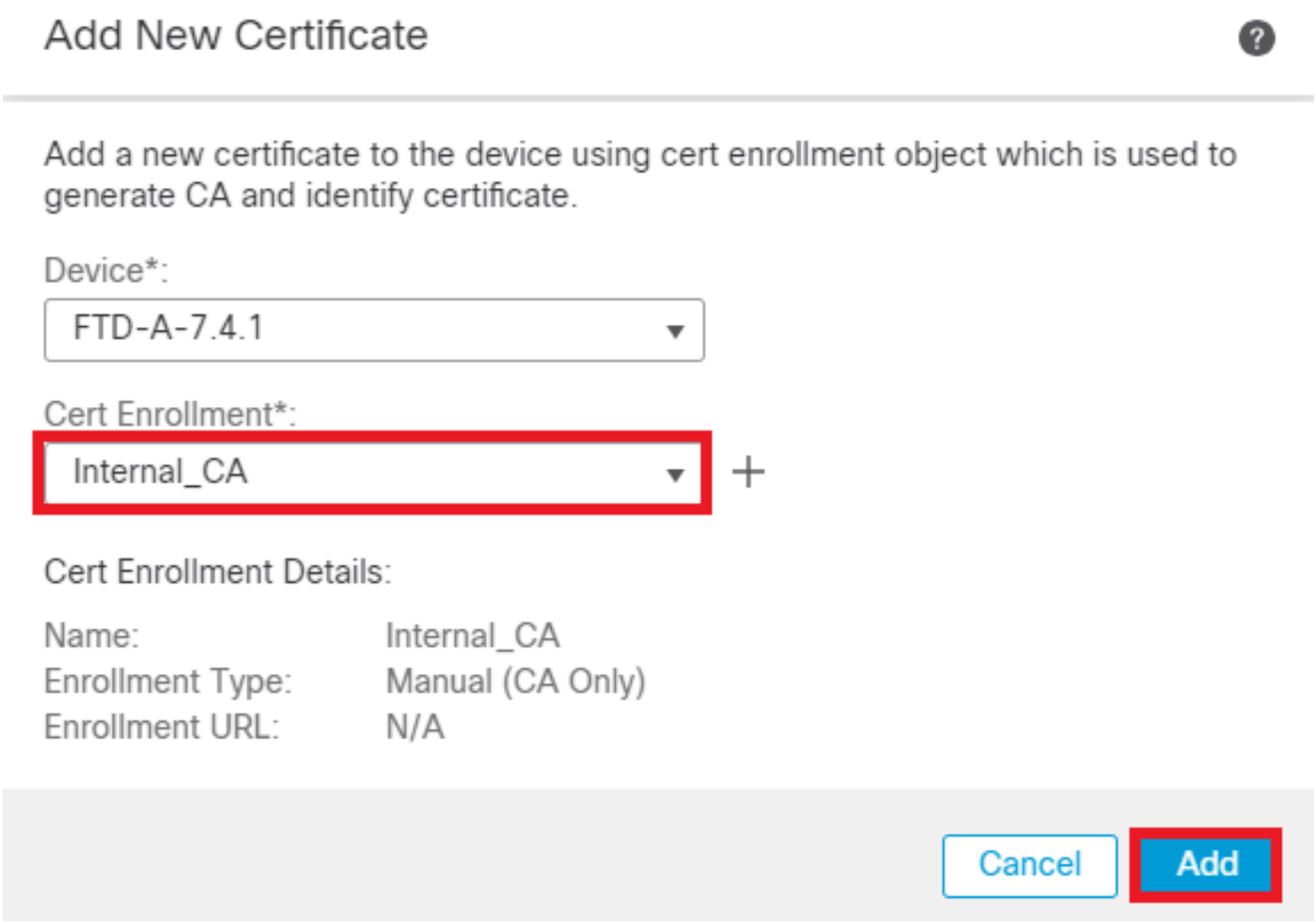
Schritt 3: Aktivieren CA Onlyund fügen Sie das Zertifikat der vertrauenswürdigen/internen Zertifizierungsstelle im PEM-Format ein.

Schritt 4: Aktivieren Sie das Kontrollkästchen, **Skip Check for CA flag in basic constraints of the CA Certificate**und klicken Sie auf Save.



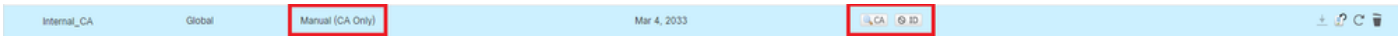

*Vertrauenspunkt hinzufügen*

Schritt 5: Wählen Sie unter Cert Enrollment den Vertrauenspunkt aus dem Dropdown-Menü aus, das gerade erstellt wurde, und klicken Sie auf Add.




*Interne Zertifizierungsstelle hinzufügen*

Schritt 6: Das zuvor hinzugefügte Zertifikat wird angezeigt als:

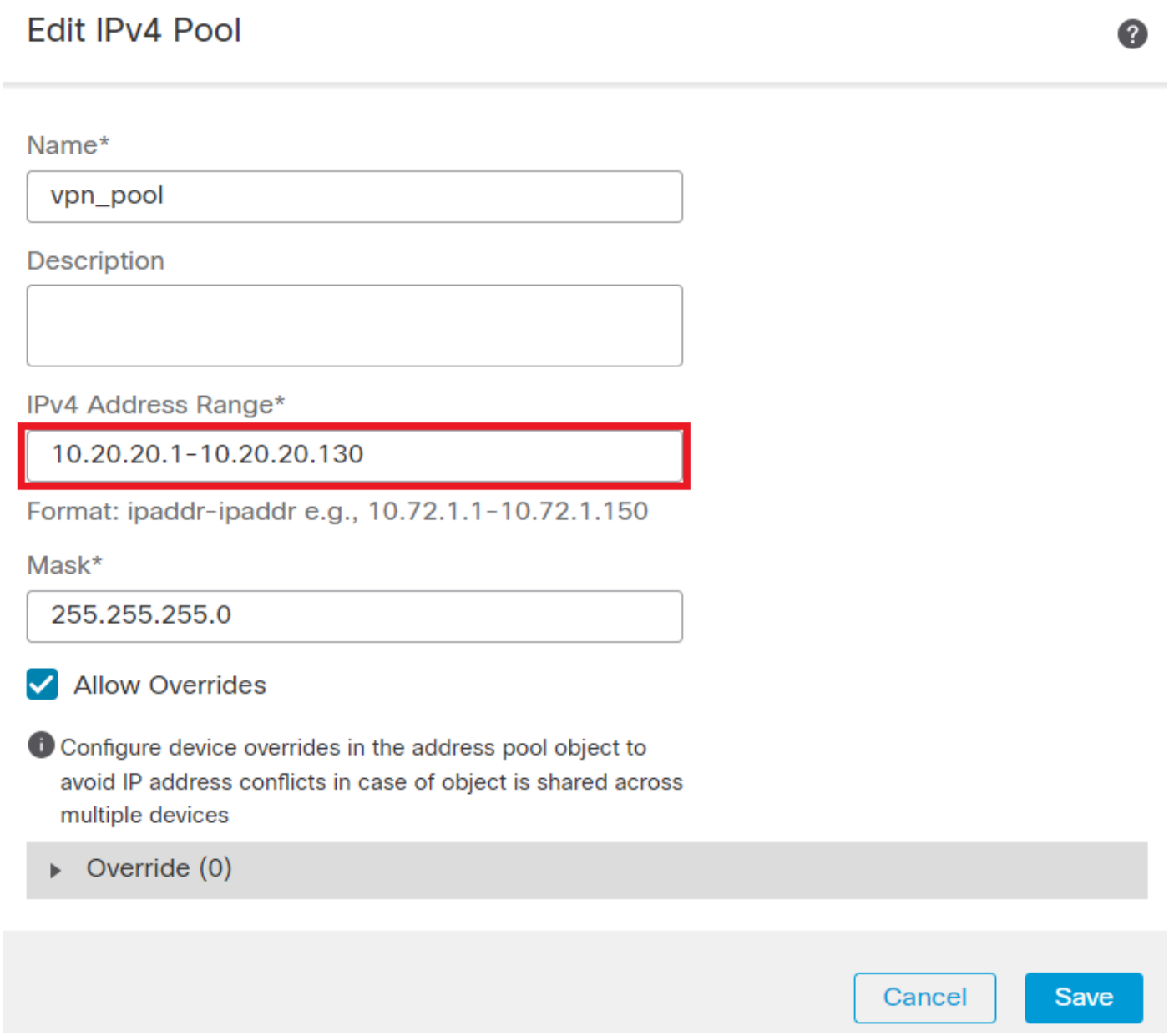



*Zertifikat hinzugefügt*

**c. Konfigurieren des Adresspools für VPN-Benutzer**

Schritt 1: Navigieren Sie zu Objects > Object Management > Address Pools > IPv4 Pools .

Schritt 2: Geben Sie den Namen und den IPv4-Adressbereich mit einer Maske ein.




*IPv4-Pool hinzufügen*

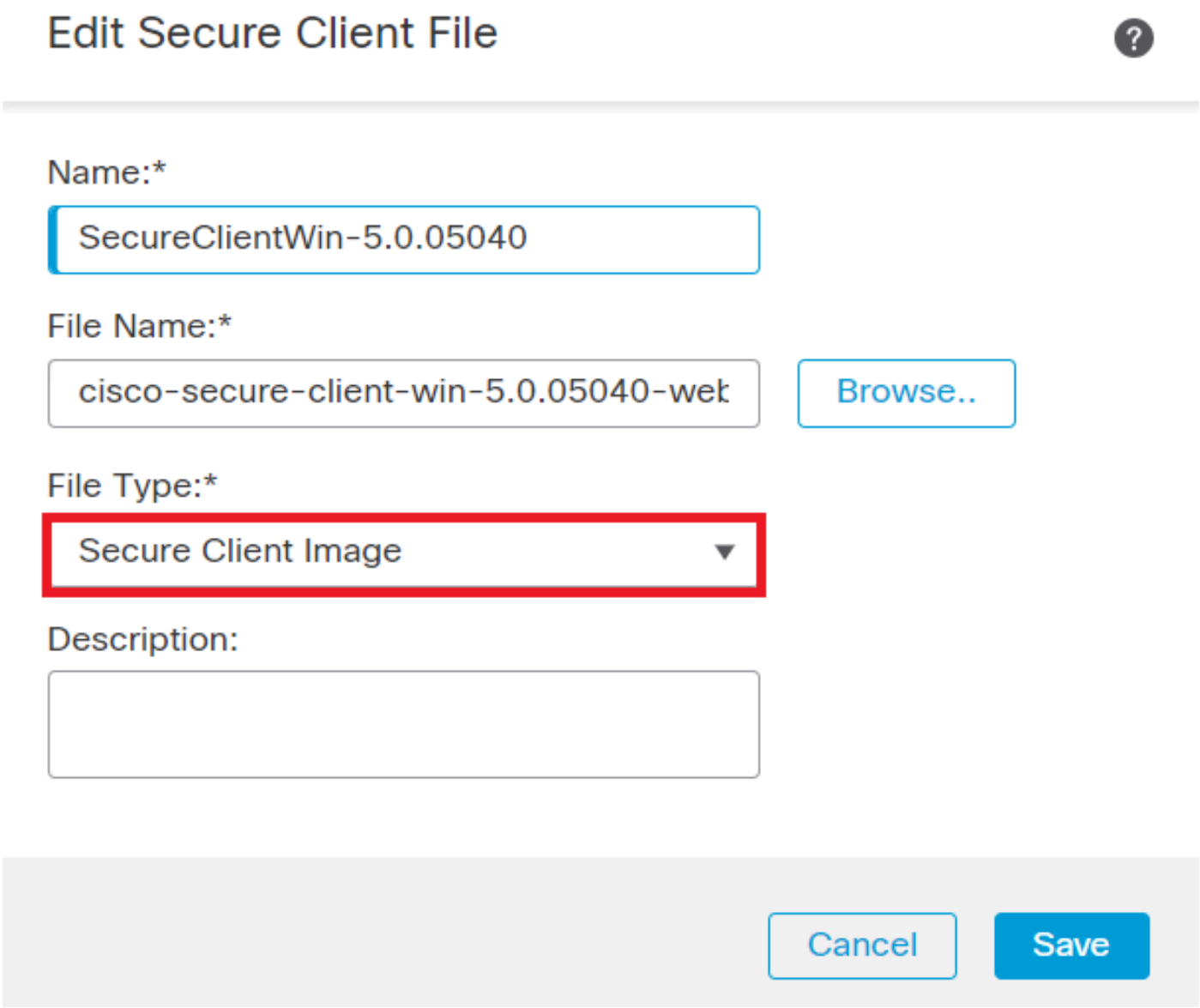
**d. Hochladen sicherer Client-Images**

Schritt 1: Laden Sie über die Cisco Software-Website WebDeployment sichere Client-Images nach Betriebssystem herunter.

Schritt 2: Navigieren Sie zu Objects > Object Management > VPN > Secure Client File > Add Secure Client File .

Schritt 3: Geben Sie den Namen ein, und wählen Sie die Datei Secure Client von der Festplatte aus.

Schritt 4: Wählen Sie den Dateityp aus, Secure Client Image und klicken Sie auf Save.




*Sicheres Client-Image hinzufügen*

**e. Erstellen und Hochladen eines XML-Profils**

Schritt 1: Laden Sie den Secure Client Profile Editor von der Cisco Software-Website herunter, und installieren Sie ihn.

Schritt 2: Erstellen Sie ein neues Profil, und wählen Sie im Dropdown-Menü "Clientzertifikatauswahl" die OptionAll aus. Es steuert hauptsächlich, welche Zertifikatspeicher(s) Secure Client zum Speichern und Lesen von Zertifikaten verwenden kann.

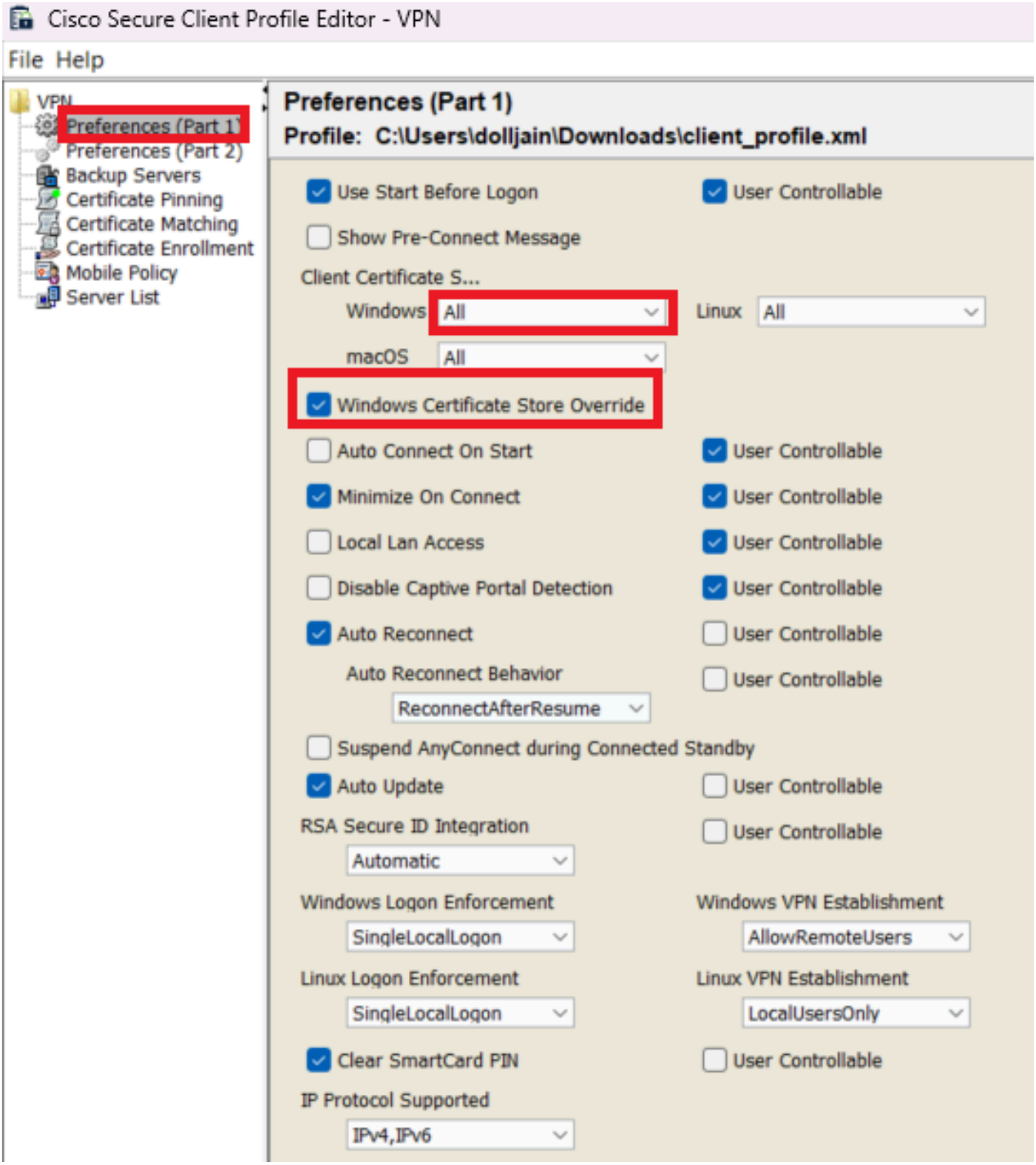
Zwei weitere Optionen sind:

- **Computer** - Der sichere Client ist auf die Zertifikatssuche im Zertifikatspeicher des lokalen Windows-Computers beschränkt.
- **Benutzer** - Der sichere Client ist auf die Zertifikatsuche im lokalen Windows-Benutzerzertifikatsspeicher beschränkt.

Überschreiben des Zertifikatspeichers als True festlegen**.**

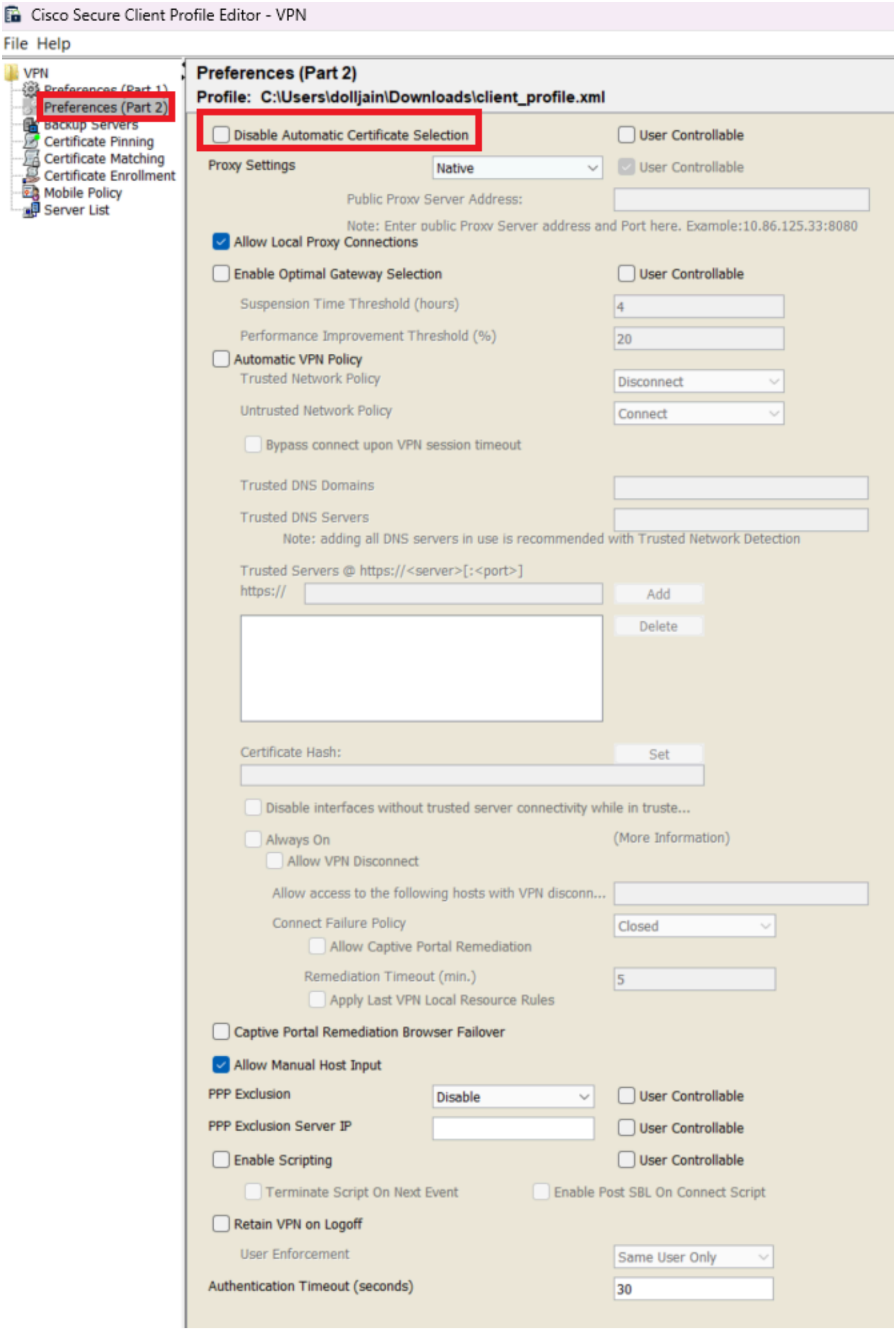
Dadurch kann ein Administrator Secure Client anweisen, Zertifikate im Zertifikatspeicher des Windows-Computers (lokales System) für die

Clientzertifikatauthentifizierung zu verwenden. Die Aufhebung des Zertifikatsspeichers gilt nur für SSL, bei dem die Verbindung standardmäßig vom Benutzeroberflächenprozess initiiert wird. Bei Verwendung von IPSec/IKEv2 kann diese Funktion im Profil für sichere Clients nicht verwendet werden.



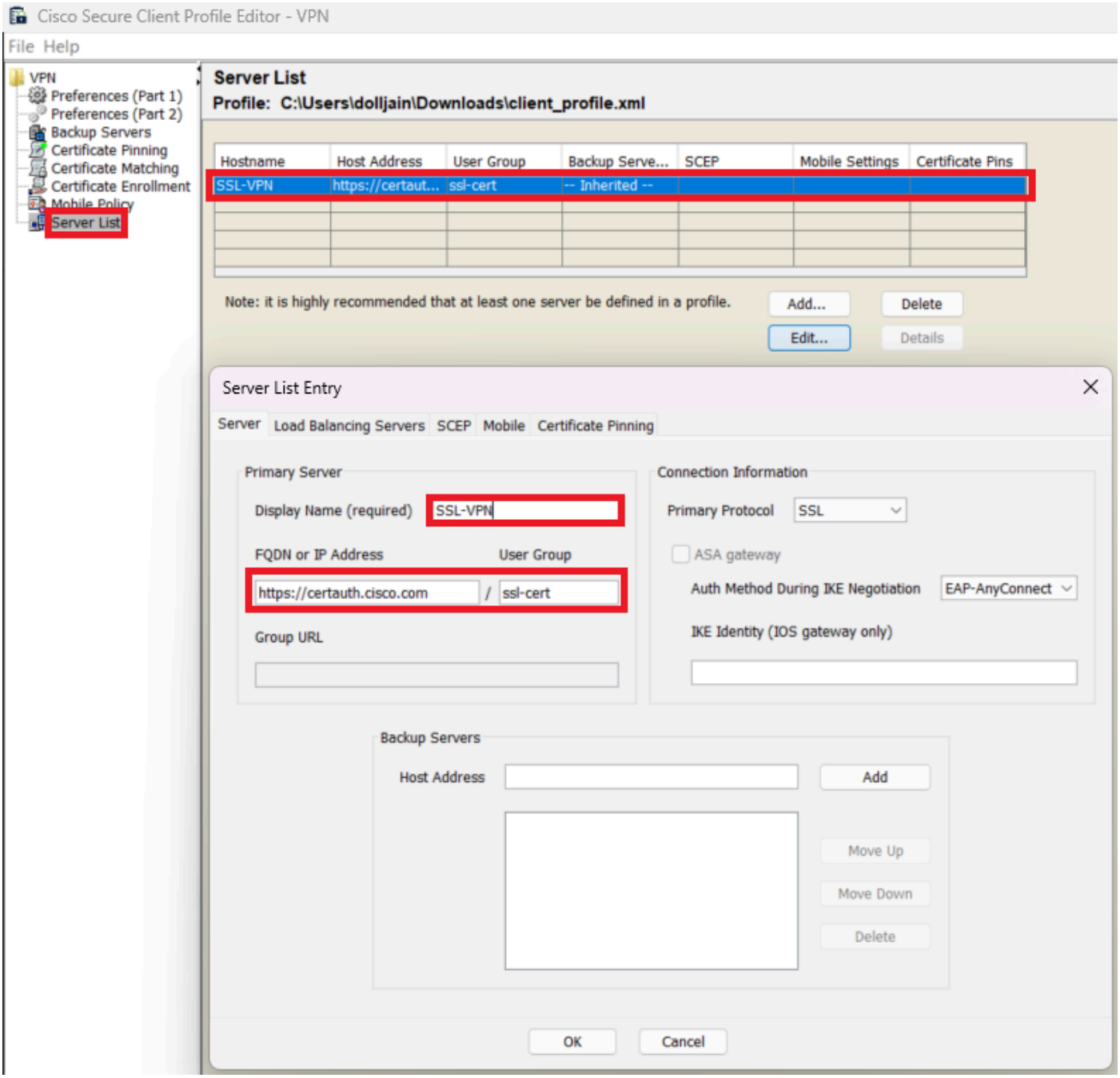

*Voreinstellungen hinzufügen (Teil 1)*

Schritt 3. (Optional) Deaktivieren Sie die OptionDisable Automatic Certificate Selection, da der Benutzer nicht aufgefordert wird, das Authentifizierungszertifikat auszuwählen.




*Voreinstellungen hinzufügen (Teil 2)*

Server List Entry zum Einrichten eines Profils in Secure Client VPN, indem Sie in der Serverliste die Gruppen-Alias- und Gruppen-URL angeben und das XML-Profil speichern.




*Serverliste hinzufügen*

Schritt 5: Schließlich ist das XML-Profil einsatzbereit.

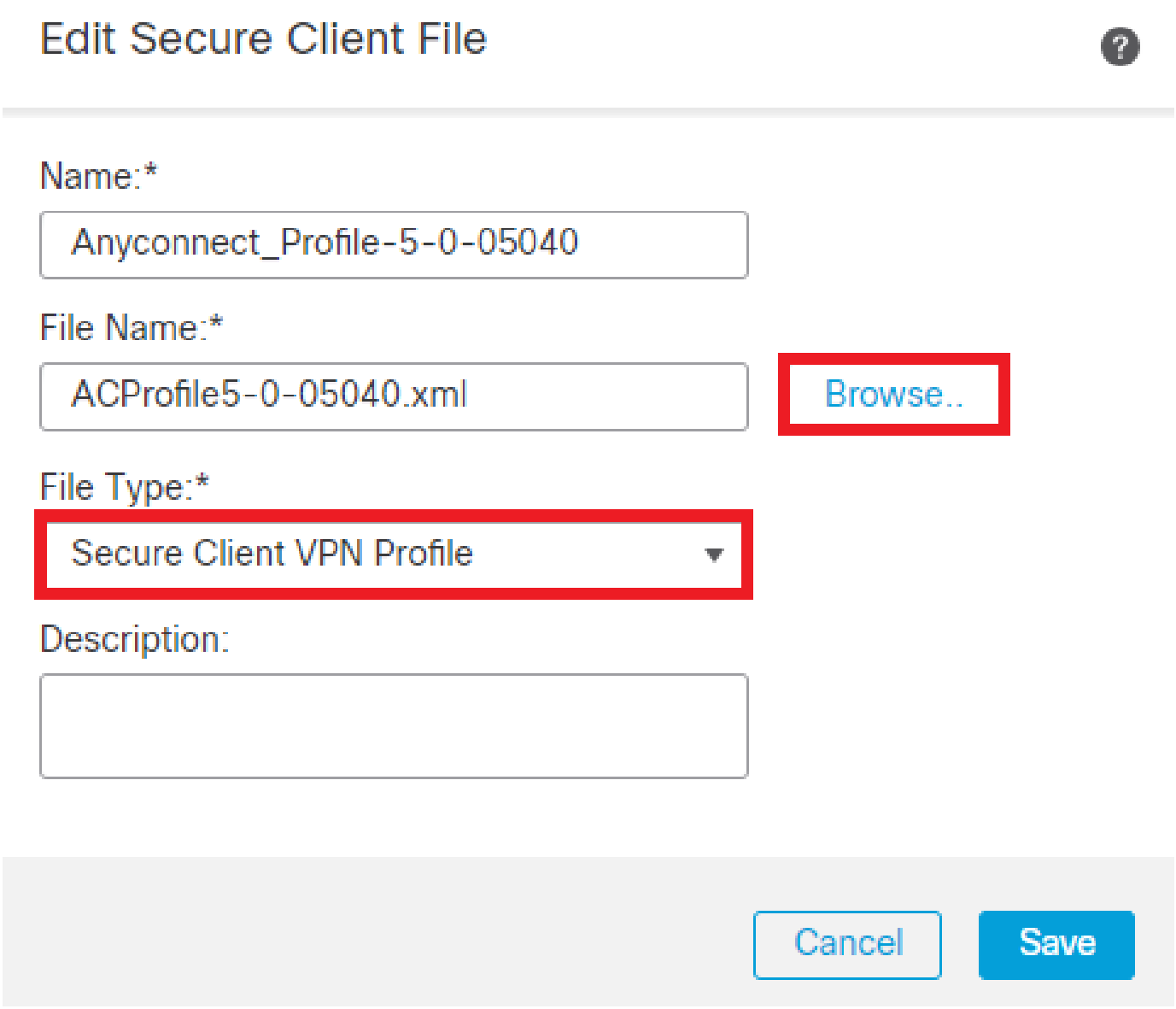

*XML-Profil*

Speicherort von XML-Profilen für verschiedene Betriebssysteme:

- **Windows** - C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile
- **MacOS** - /opt/cisco/anyconnect/profile
- **Linux** - /opt/cisco/anyconnect/profile

Schritt 6: Navigieren Sie zu Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile .

Geben Sie den Namen für die Datei ein, und klicken Sie auf Browse, um das XML-Profil auszuwählen. Klicken Sie auf .Save

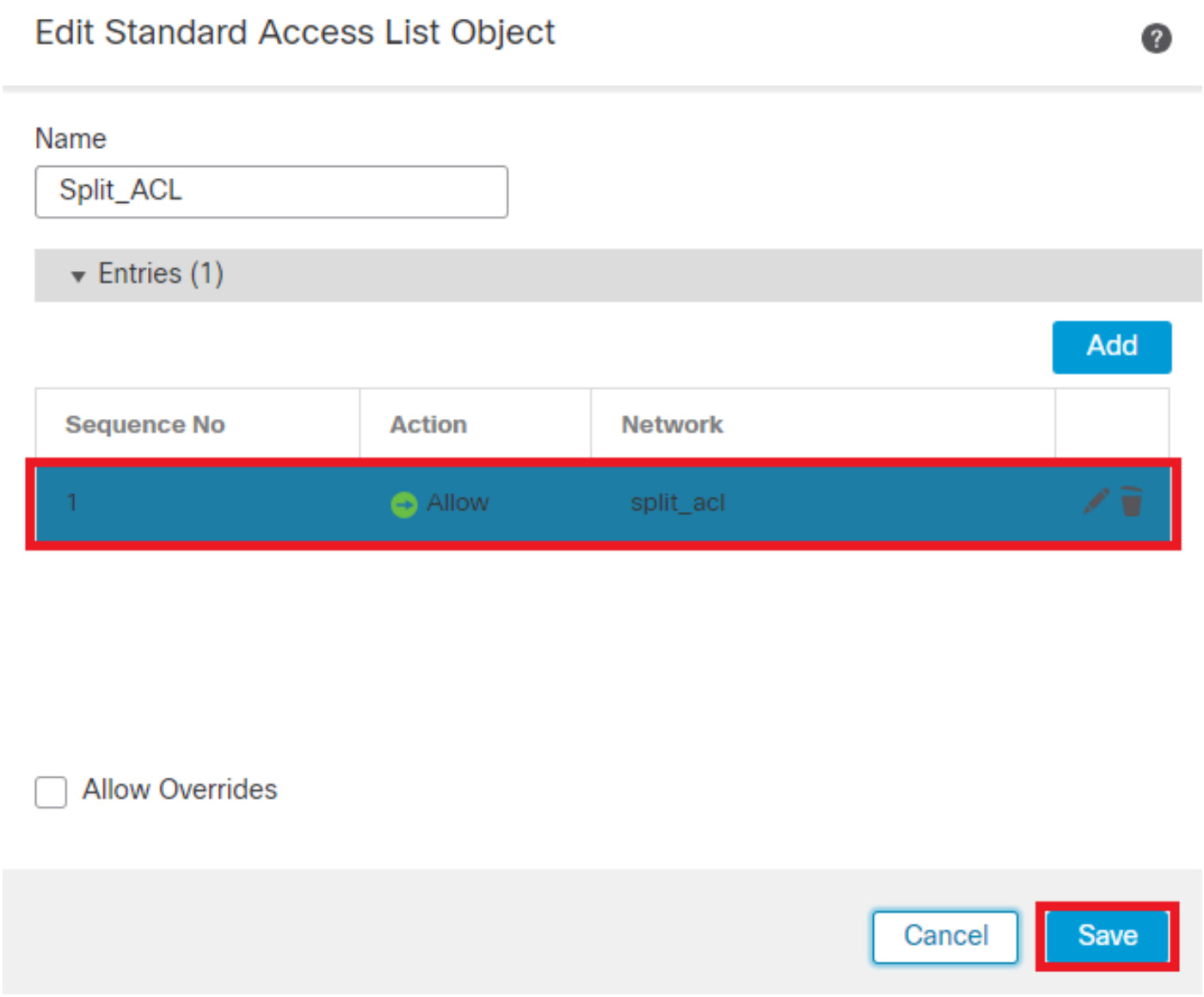



*Secure Client VPN-Profil hinzufügen*

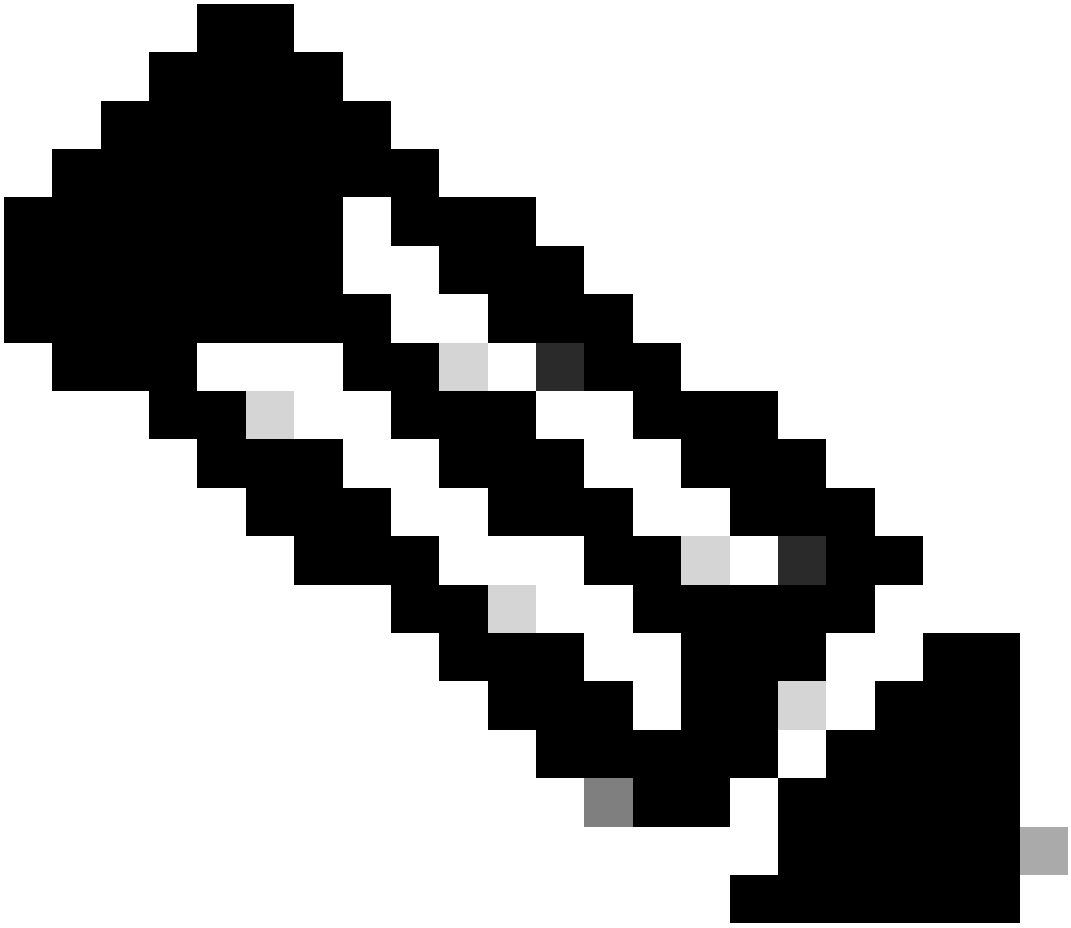
Konfiguration des Remotezugriff-VPNs

Schritt 1: Erstellen Sie eine Zugriffskontrollliste entsprechend der Anforderung, um den Zugriff auf interne Ressourcen zu ermöglichen.

Navigieren Sie zu, Objects > Object Management > Access List > Standard und klicken Sie auf Add Standard Access List.




*Standard-ACL hinzufügen*

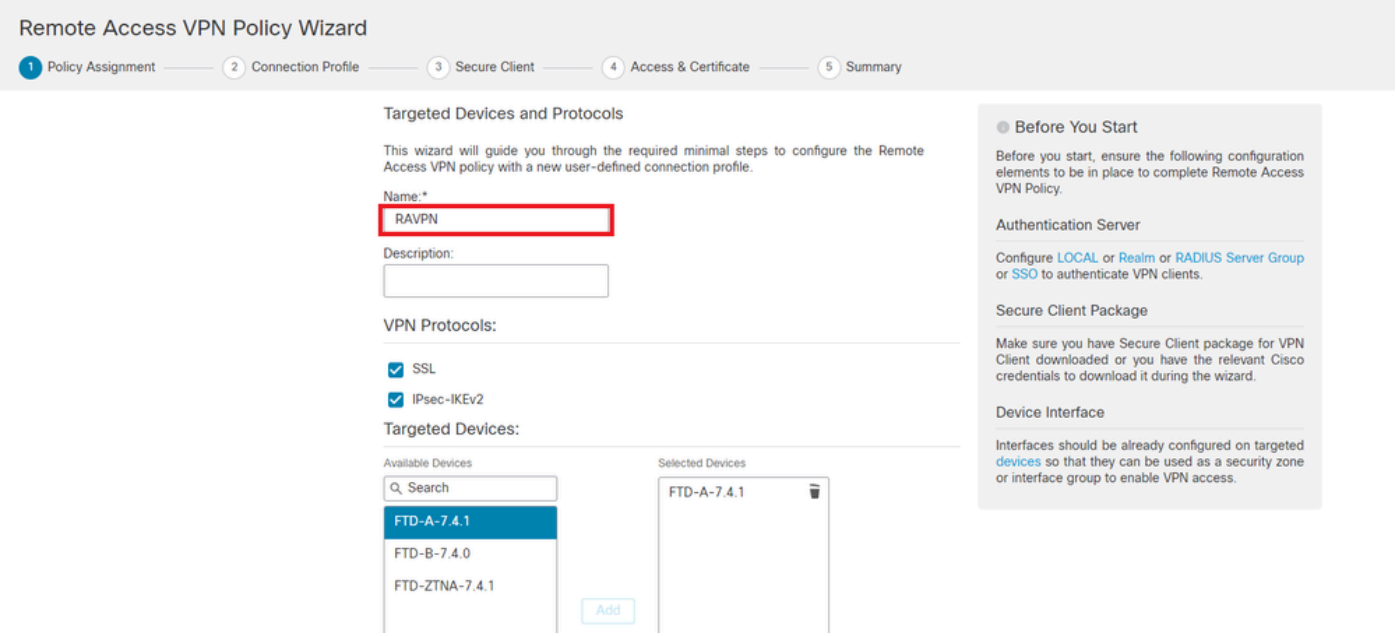


**Hinweis**: Diese ACL wird von Secure Client verwendet, um sichere Routen zu internen Ressourcen hinzuzufügen.

---

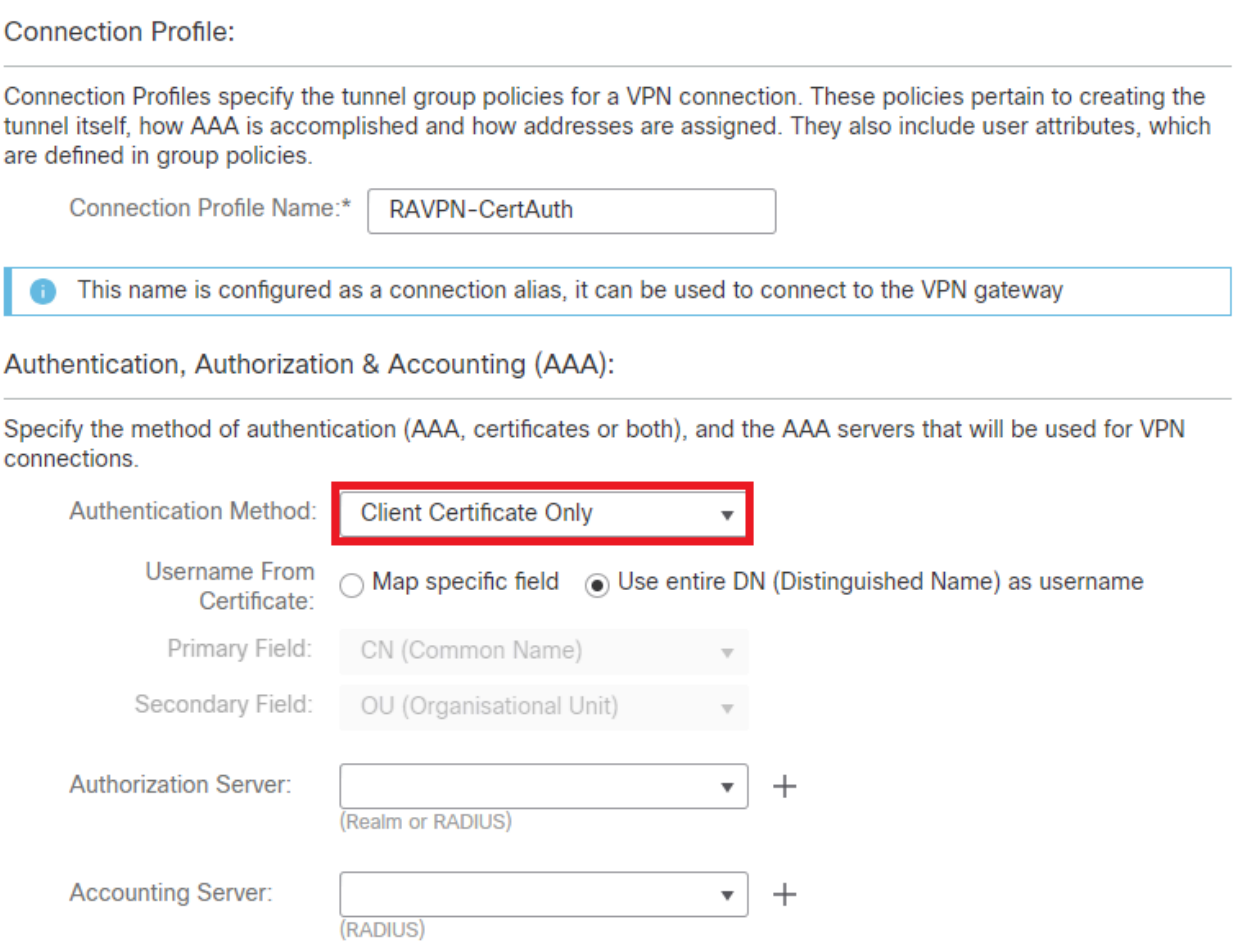
Schritt 2: Navigieren Sie zu, Devices > VPN > Remote Access und klicken Sie auf Add.

Schritt 3: Geben Sie den Namen des Profils ein, wählen Sie das FTD-Gerät aus, und klicken Sie auf "Weiter".



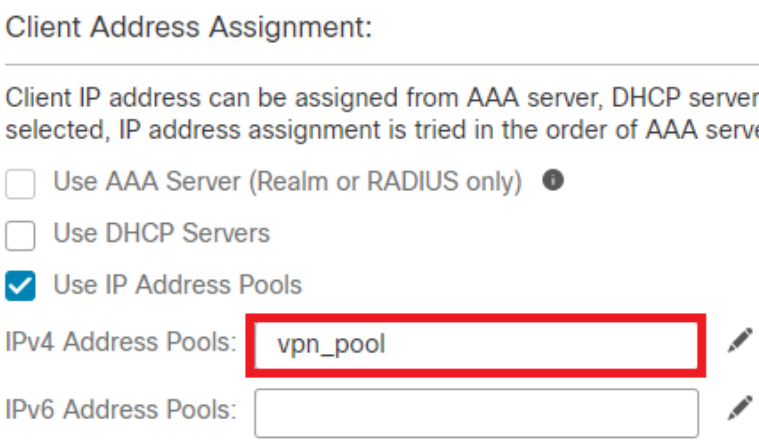

*Profilnamen hinzufügen*

Schritt 4: Geben Sie den Befehl ein, Connection Profile Nameund wählen Sie die Authentifizierungsmethode Client Certificate Only wie unter Authentifizierung, Autorisierung und Abrechnung (AAA) aus.



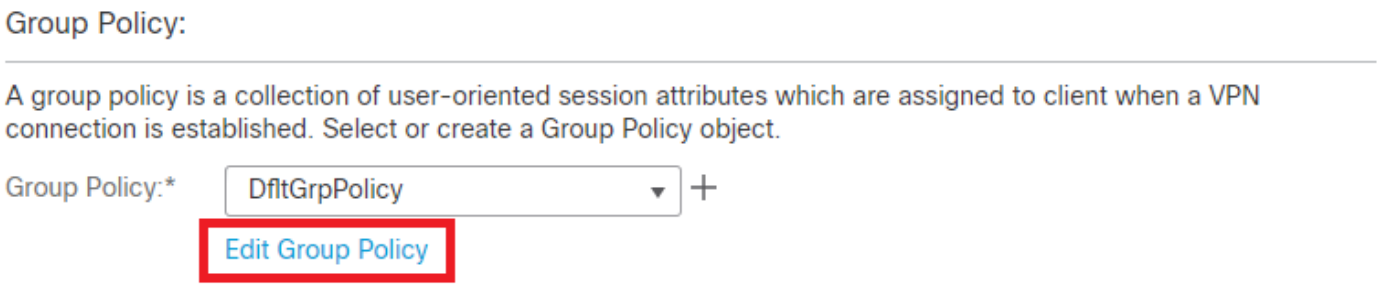

*Authentifizierungsmethode auswählen*

Schritt 5: Klicken Sie Use IP Address Pools unter Client Address Assignment (Client-Adressenzuweisung) auf und wählen Sie den zuvor erstellten IPv4-Adresspool aus.




*Client-Adressenzuweisung auswählen*

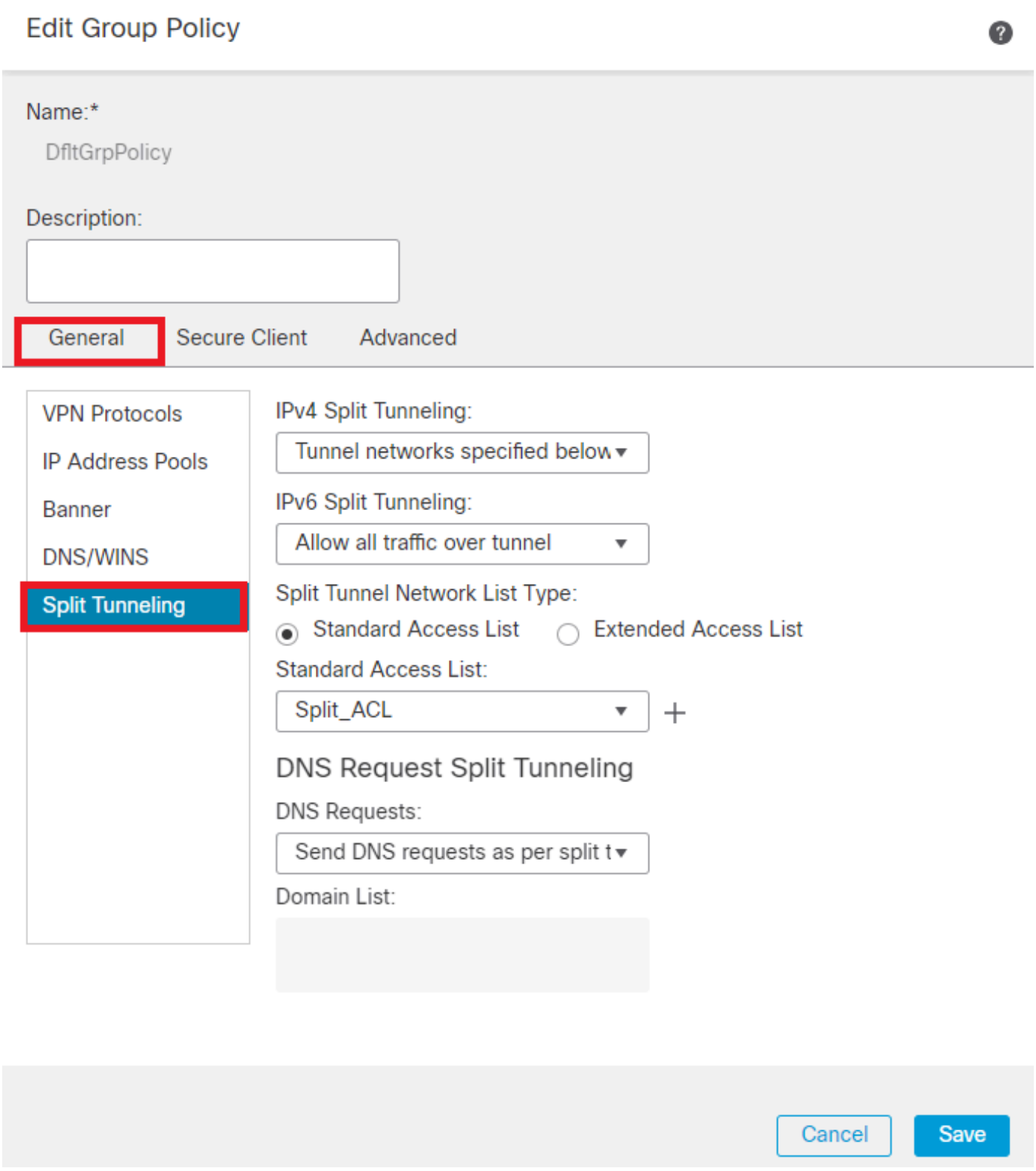
Schritt 6: Bearbeiten Sie die Gruppenrichtlinie.




*Gruppenrichtlinie bearbeiten*

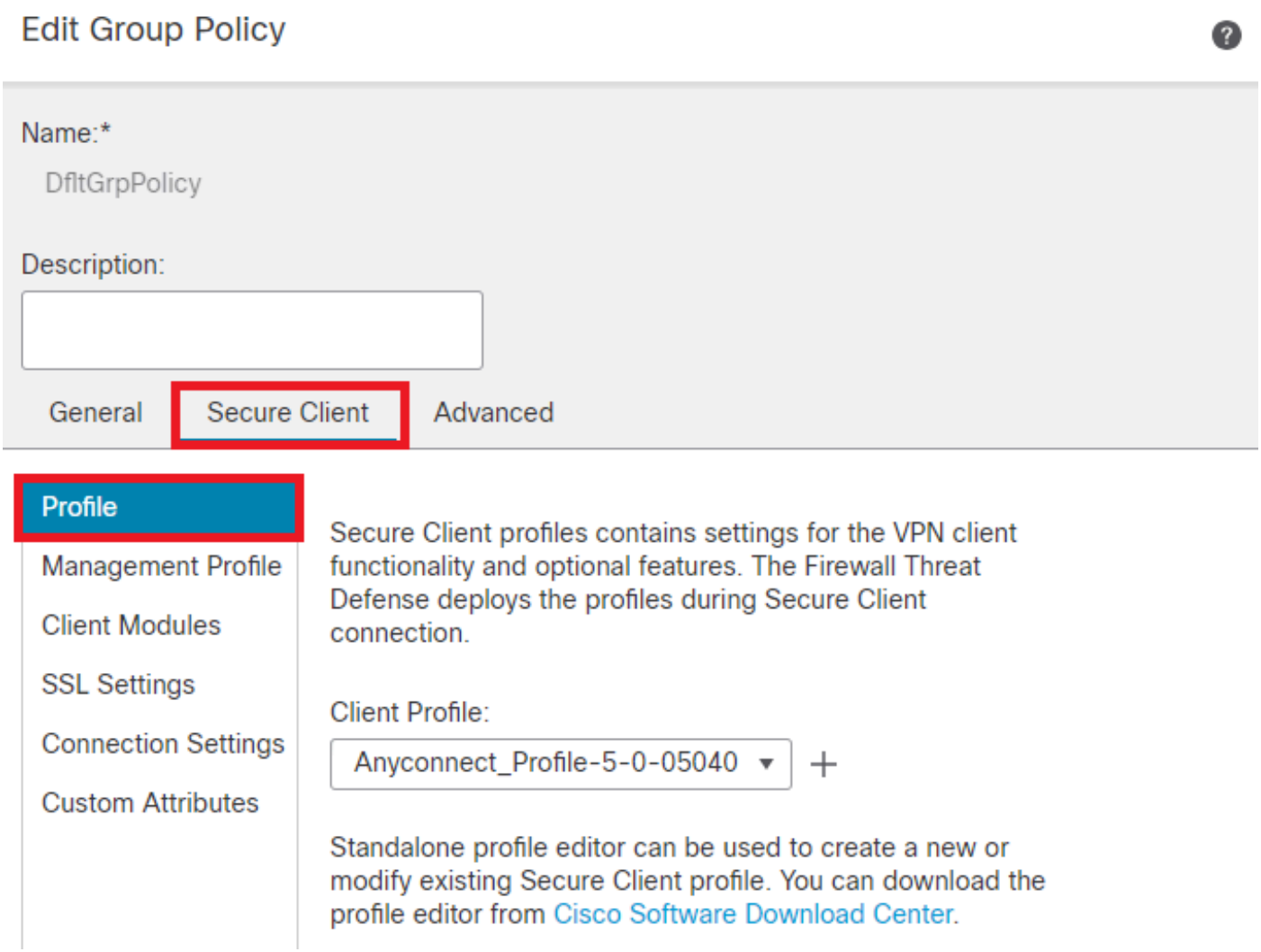
Schritt 7. Navigieren Sie zu General > Split Tunneling , wählen Sie unter Netzwerklistentyp für Split Tunnel ausTunnel networks specified below, und wählen SieStandard Access List diese aus.

Wählen Sie die zuvor erstellte ACL aus.



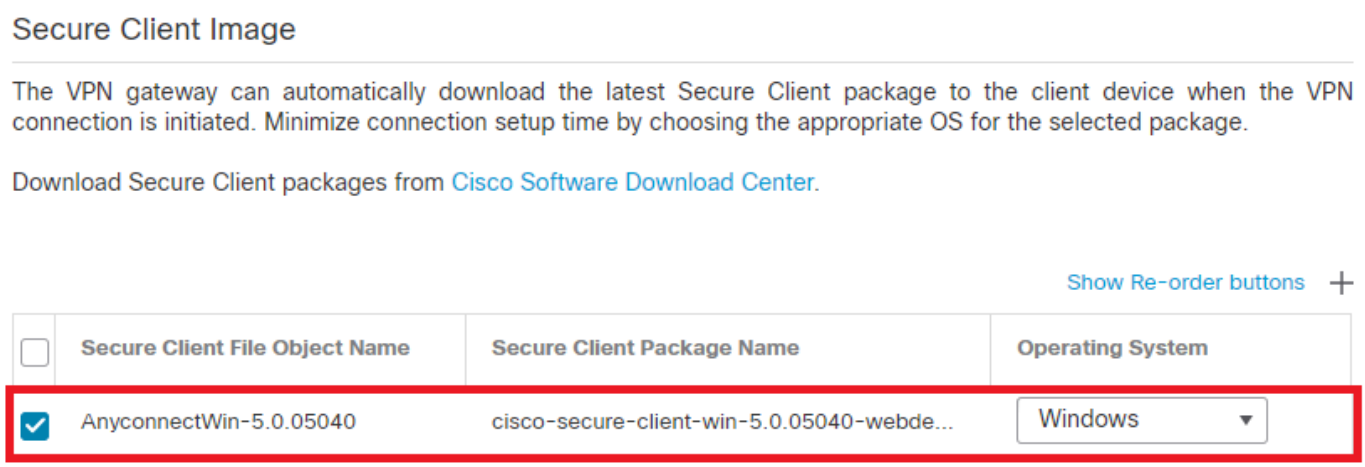

*Split-Tunneling hinzufügen*

Schritt 8: Navigieren Sie zu Secure Client > Profile , wählen Sie die aus, Client Profile und klicken Sie auf Save.



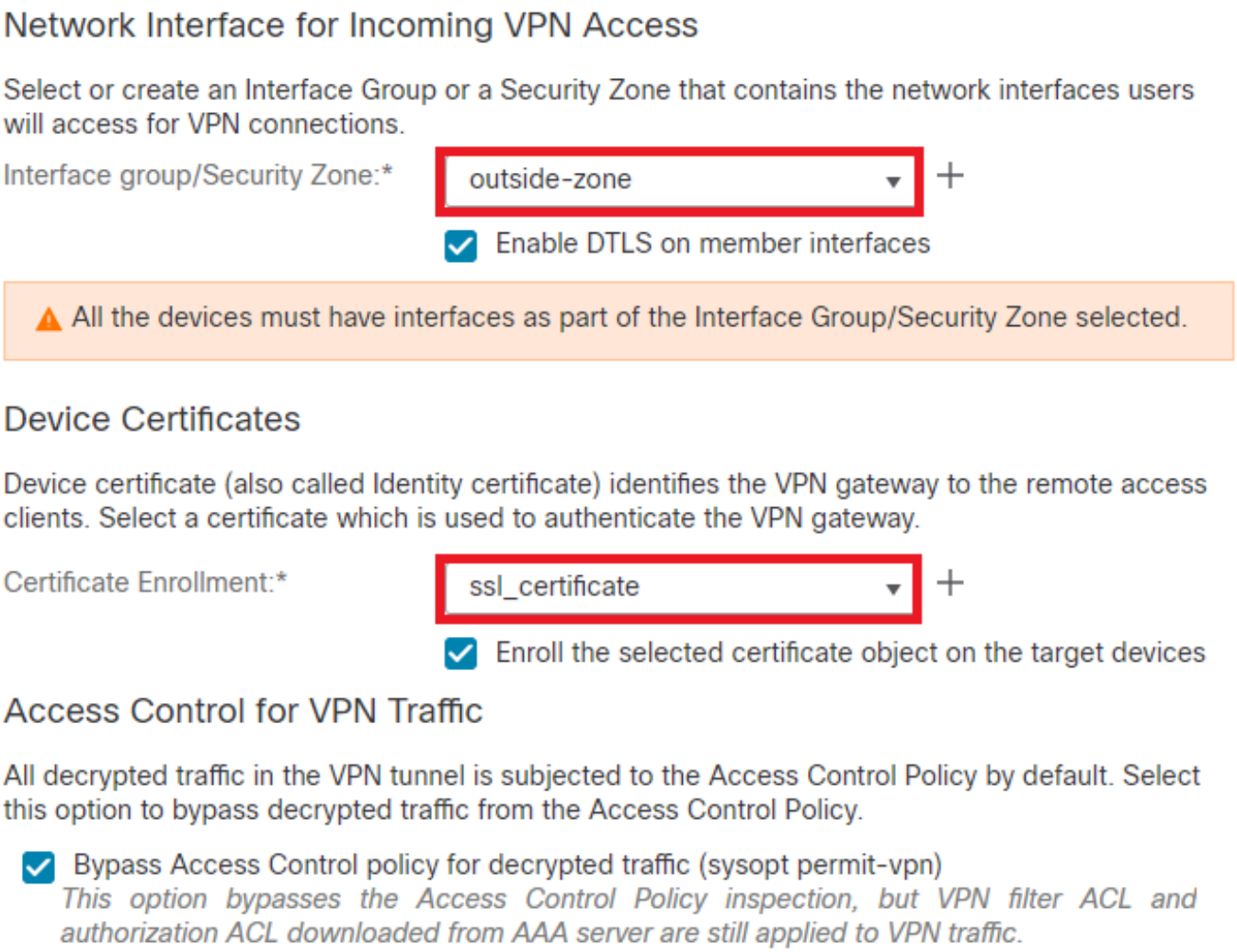

*Sicheres Clientprofil hinzufügen*

Schritt 9. Klicken Sie auf Next, wählen Sie die aus, und klicken SieSecure Client Image auf Next.



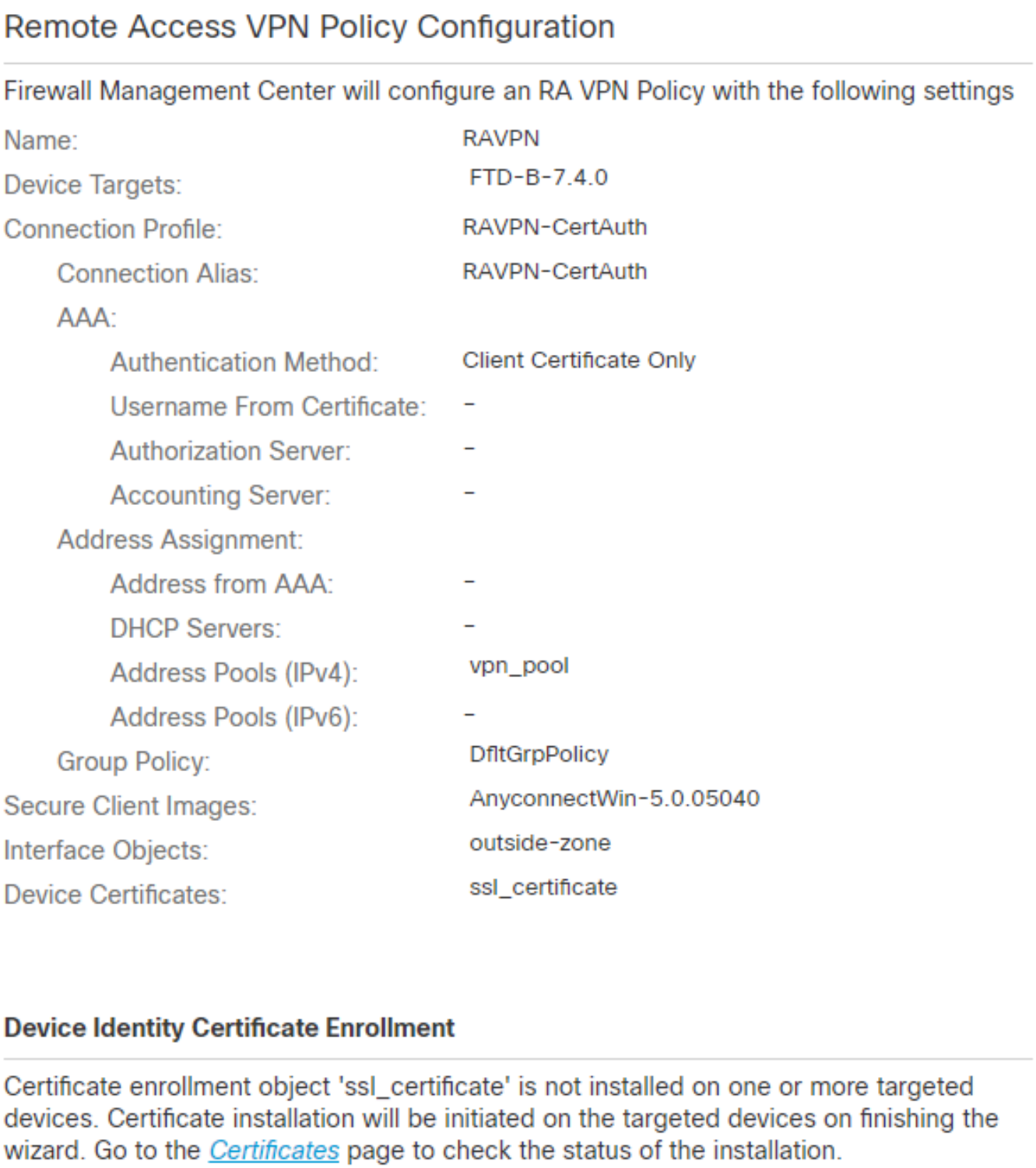

*Sicheres Client-Image hinzufügen*

Schritt 10. Wählen Sie die Netzwerkschnittstelle für den VPN-Zugriff aus, wählen Sie die aus Device Certificates, aktivieren Sie sysopt permit-vpn, und klicken Sie auf Next.




*Zugriffskontrolle für VPN-Datenverkehr hinzufügen*

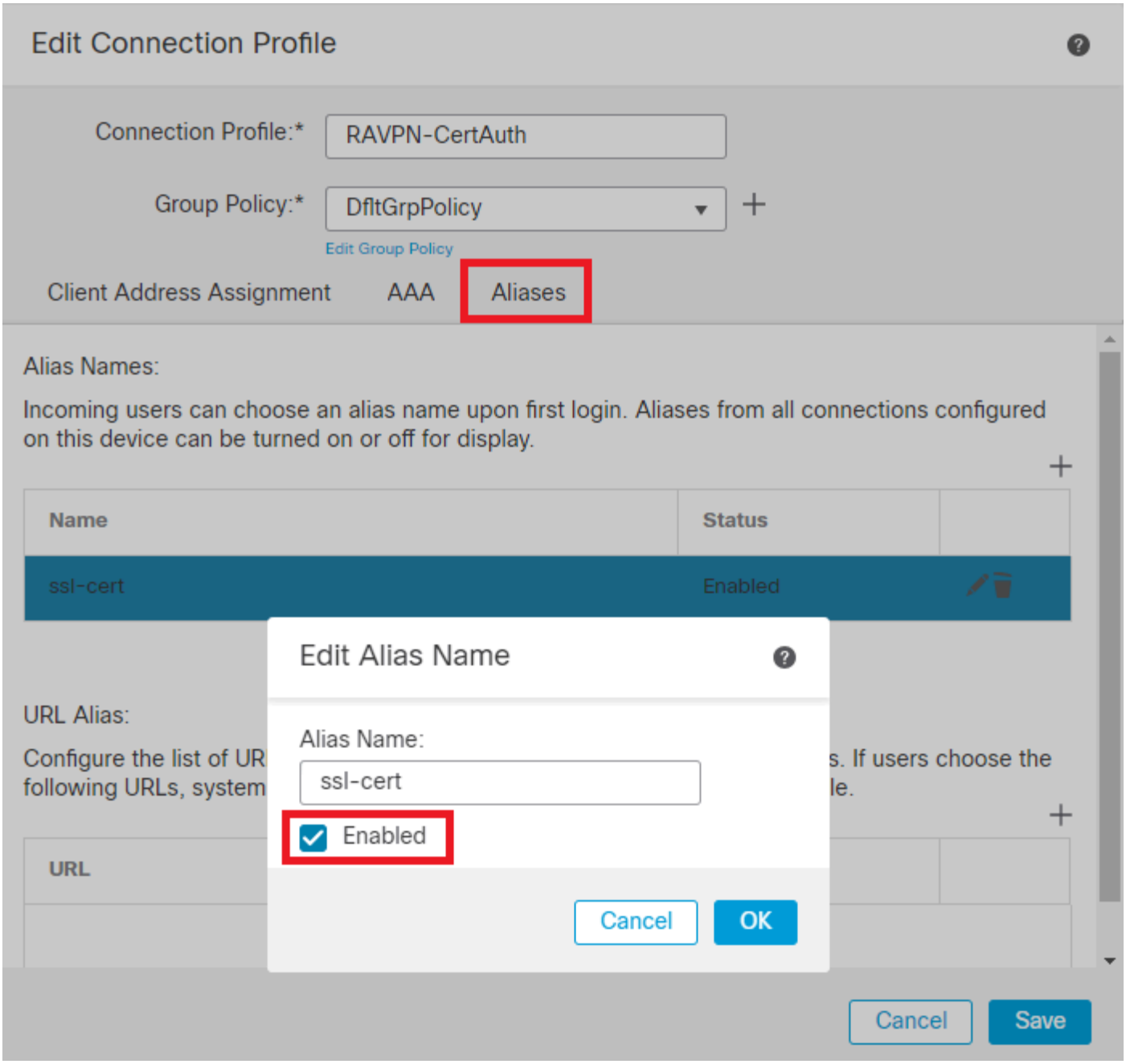
Schritt 11. Überprüfen Sie abschließend alle Konfigurationen, und klicken Sie auf Finish.




*Konfiguration der VPN-Richtlinie für den Remote-Zugriff*

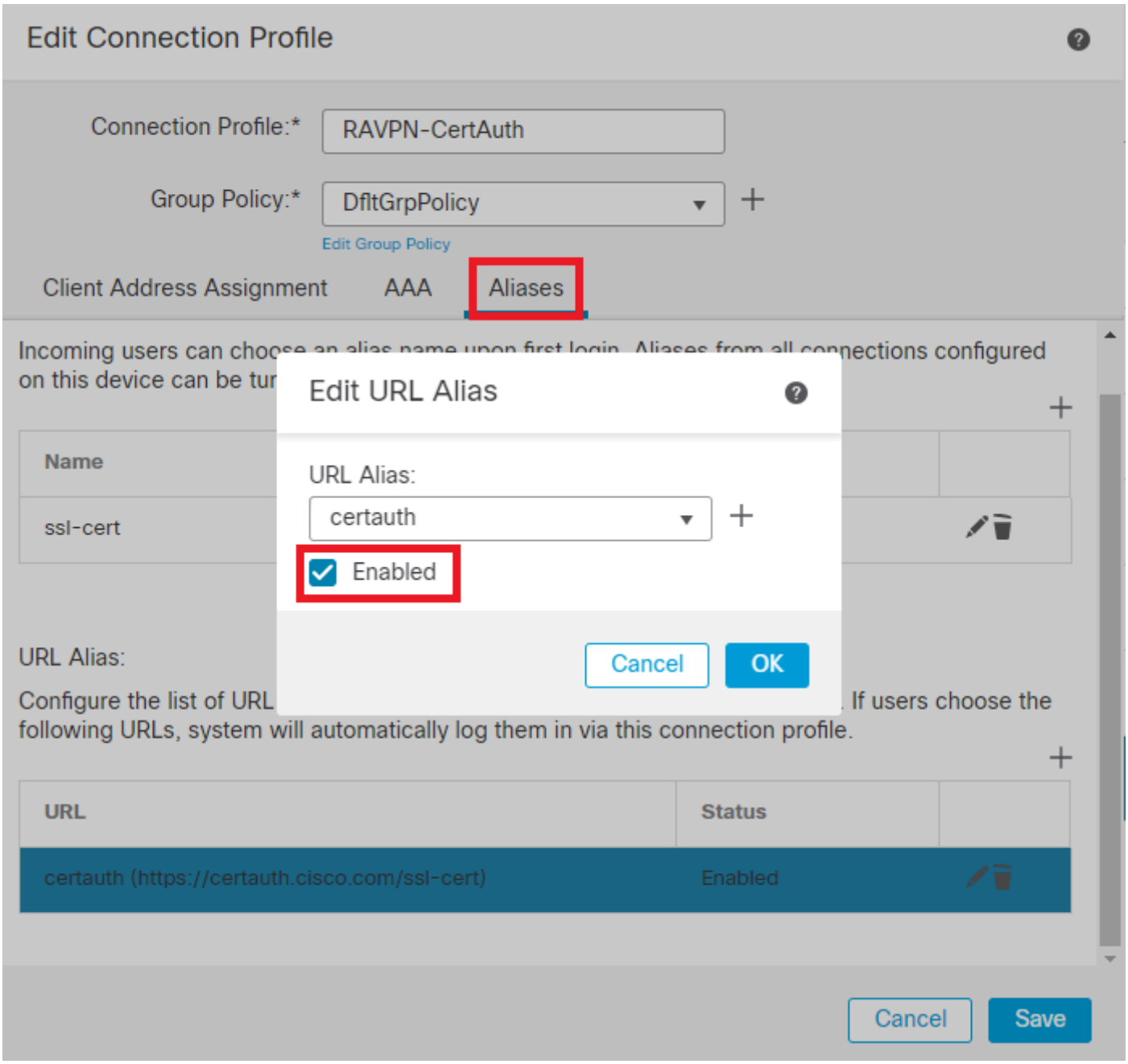
Schritt 12: Nachdem Sie die Ersteinrichtung des Remote Access VPN abgeschlossen haben, bearbeiten Sie das erstellte Verbindungsprofil und wechseln Sie zu Aliases.

Schritt 13: group-alias Konfigurieren Sie Ihre Konfiguration, indem Sie auf das Plussymbol (+) klicken.



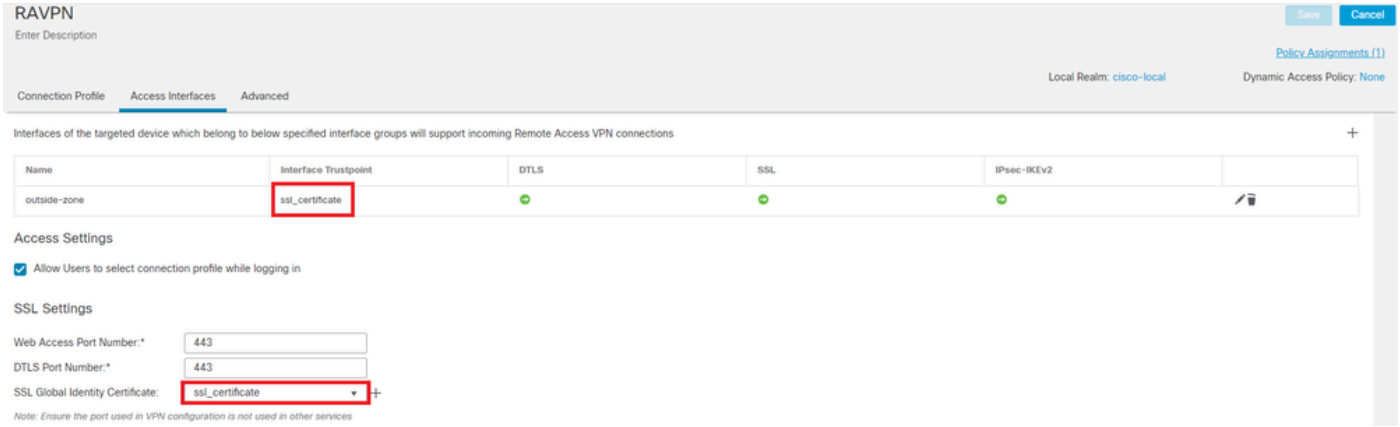

*Gruppenalias bearbeiten*

Schritt 14: group-url Konfigurieren Sie Ihre Konfiguration, indem Sie auf das Plussymbol (+) klicken. Verwenden Sie dieselbe Gruppen-URL, die zuvor im Clientprofil konfiguriert wurde.




*Gruppen-URL bearbeiten*

Schritt 15: Navigieren Sie zu Access Interfaces (Zugriffsschnittstellen). Wählen Sie unter den SSL-Einstellungen die Interface Truspoint undSSL Global Identity Certificate aus.



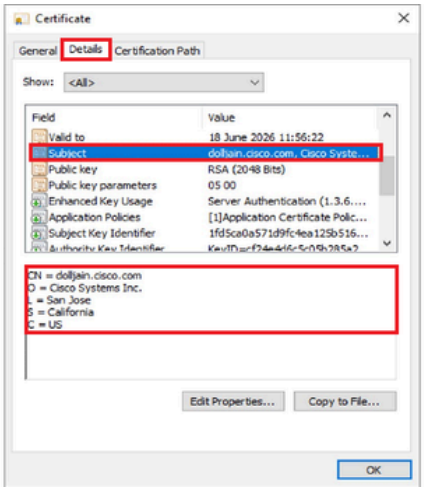
*Zugriffsschnittstellen bearbeiten*

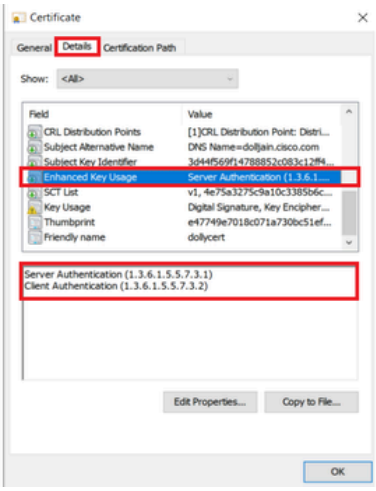
Schritt 16: KlickenSave Sie, und stellen Sie diese Änderungen bereit.

Überprüfung

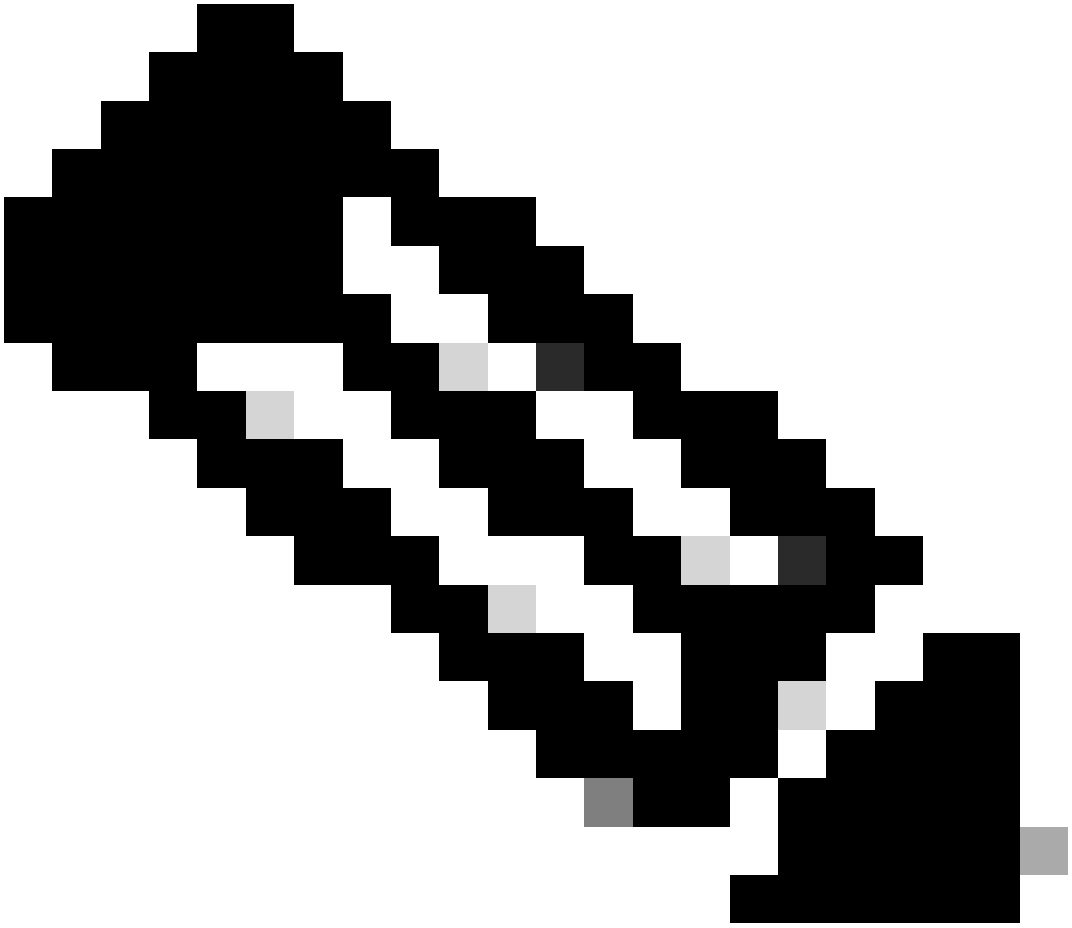
Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Auf dem sicheren Client-PC muss das Zertifikat mit einem gültigen Datum, einem gültigen Betreff und einer gültigen EKU auf dem PC des Benutzers installiert sein. Dieses Zertifikat muss von der Zertifizierungsstelle ausgestellt werden, deren Zertifikat, wie zuvor gezeigt, auf FTD installiert ist. Hier wird die Identität bzw. das Benutzerzertifikat von "auth-risaggar-ca" ausgestellt.

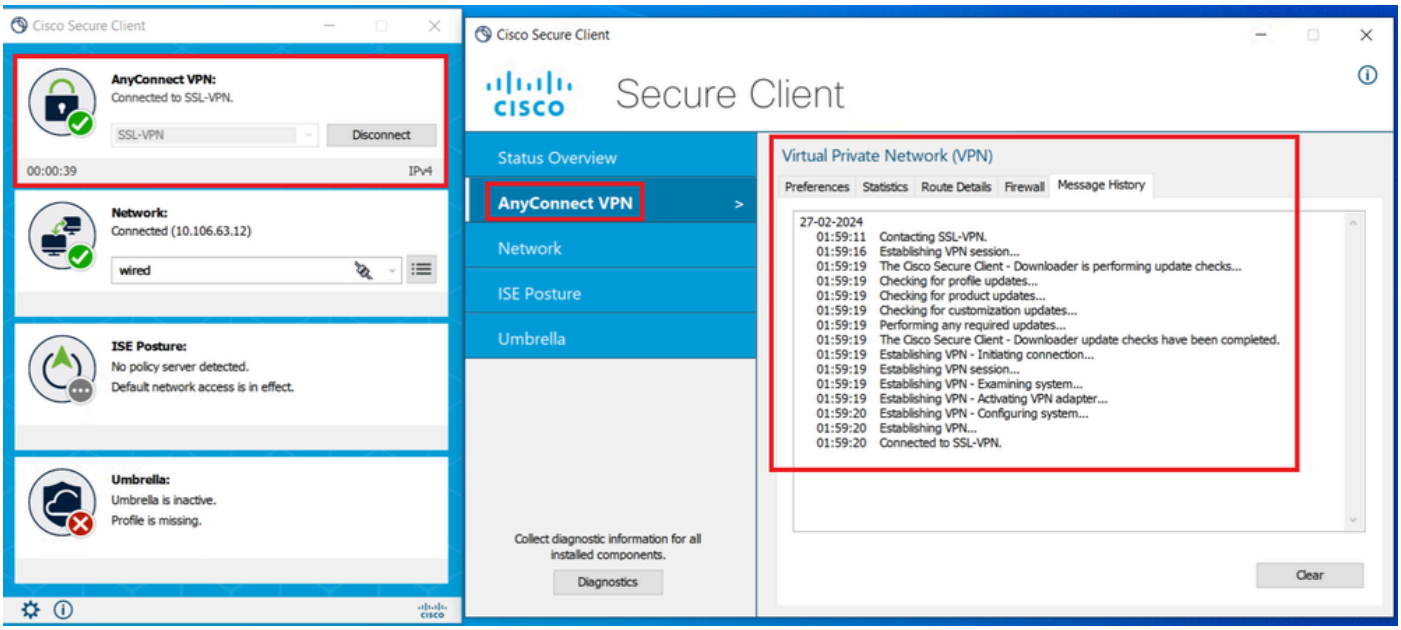




*Zertifikat-Highlights*



**Hinweis**: Das Client-Zertifikat muss über die erweiterte Schlüsselverwendung (Enhanced Key Usage, EKU) für die "Client-Authentifizierung" verfügen.

2. Der Secure Client muss die Verbindung herstellen.




*Erfolgreiche sichere Clientverbindung*

3. Führen Sie show vpn-sessiondb anyconnect aus, um die Verbindungsdetails des aktiven Benutzers unter der verwendeten Tunnelgruppe zu bestätigen.

```
firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dolljain.cisco.com Index :
```

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

1. Die Fehlerbehebungen können über die Diagnose-CLI des FTD ausgeführt werden:

debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255

2. Lesen Sie dieses Handbuch für häufige Probleme.

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.