Zertifikatsauthentifizierung konfigurieren & DUO SAML-Authentifizierung

Inhalt

Einleitung

In diesem Dokument wird ein Beispiel für die Implementierung einer zertifikatbasierten Authentifizierung und einer dualen SAML-Authentifizierung beschrieben.

Voraussetzungen

In diesem Leitfaden werden folgende Tools und Geräte verwendet:

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Interne Zertifizierungsstelle
- Cisco DUO Premier-Konto
- Cisco DUO-Authentifizierungsproxy
- Cisco Secure Client (CSC)

Anforderungen

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

- Basis-VPN,
- SSL/TLS
- Public-Key-Infrastruktur
- Erfahrungen mit FMC
- Cisco Secure Client
- FTD-Code 7.2.0 oder höher
- Cisco DUO-Authentifizierungsproxy

Verwendete Komponenten

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

- Cisco FTD (7.3.1)
- Cisco FMC (7.3.1)
- Cisco Secure Client (5.0.02075)
- Cisco DUO-Authentifizierungsproxy (6.0.1)
- Mac OS (13.4.1)
- Active Directory

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.

Schritte für DUO konfigurieren

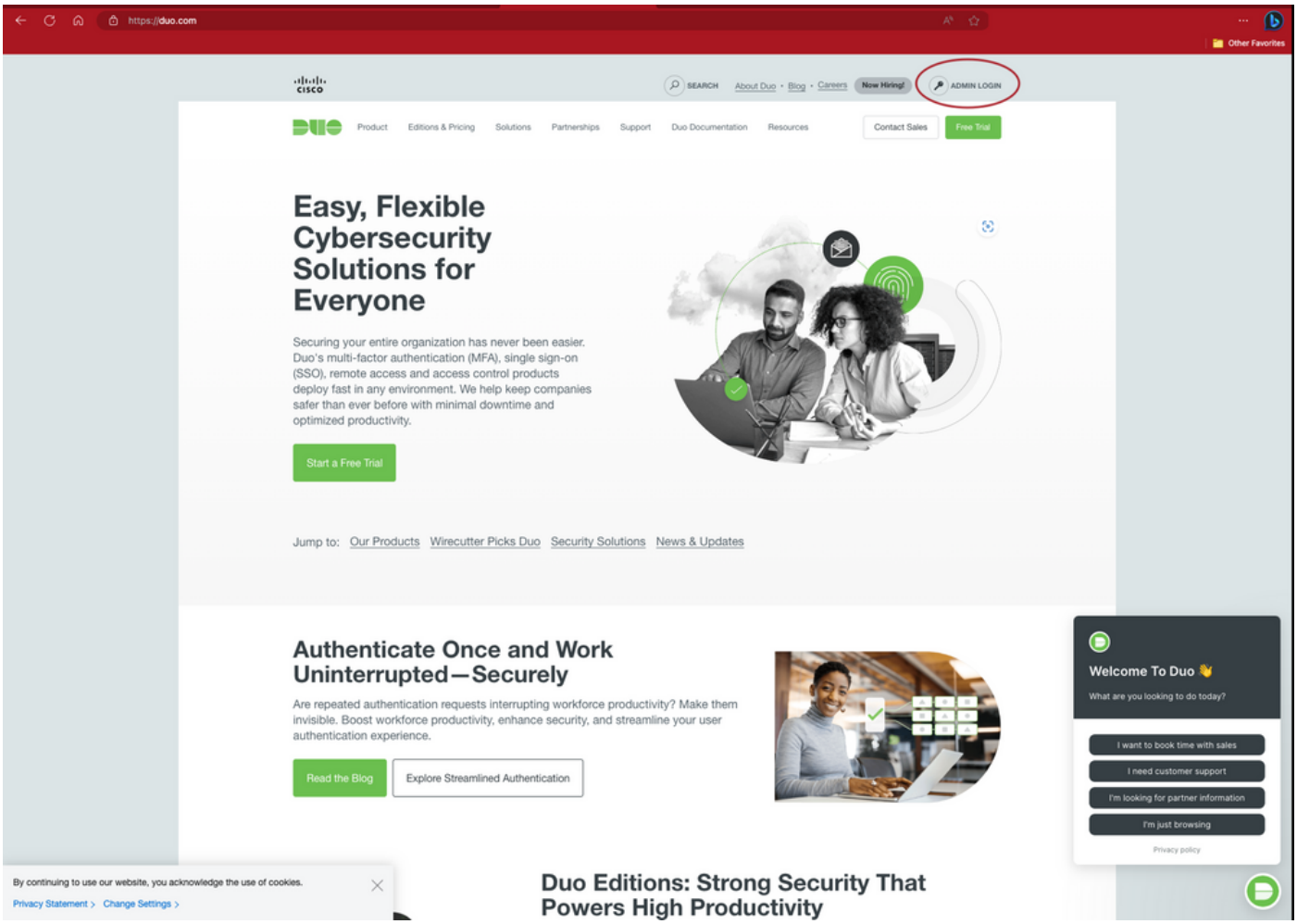
In diesem Abschnitt werden die Schritte zur Konfiguration von Cisco DUO Single Sign-on (SSO) beschrieben. Stellen Sie vor dem Start sicher, dass der Authentifizierungsproxy implementiert ist.

Warnung: Wenn kein Authentifizierungsproxy implementiert wurde, enthält dieser Link den Leitfaden für diese Aufgabe. DUO Authentication Proxy Guide

---

Erstellen einer Anwendungsschutzrichtlinie

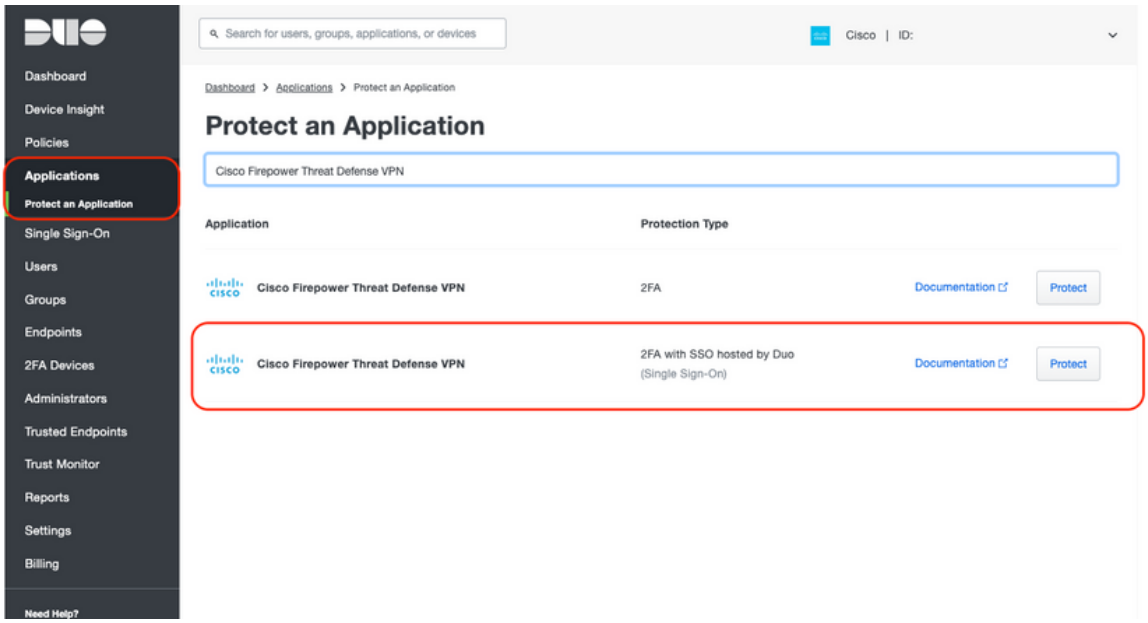
Schritt 1: Melden Sie sich über diesen Link beim Admin-Panel an Cisco Duo



Cisco DUO-Startseite

Schritt 2: Navigieren Sie zu Dashboard > Anwendungen > Eine Anwendung schützen.

Geben Sie in der Suchleiste "Cisco Firepower Threat Defense VPN" ein, und wählen Sie "Schützen".



Schützen eines Anwendungs-Screenshots

Wählen Sie die Option mit nur Schutzart "2FA mit SSO gehostet von Duo".

Schritt 3: Kopieren Sie diese URL-Informationen unter Metadaten.

- Element-ID des Identitätsanbieters
- SSO-URL
- Abmelde-URL

Beispiel für zu kopierende Informationen

Anmerkung: Die Links wurden im Screenshot weggelassen.

Schritt 4: Wählen Sie "Zertifikat herunterladen", um das Identitätsanbieter-Zertifikat unter "Downloads" herunterzuladen.

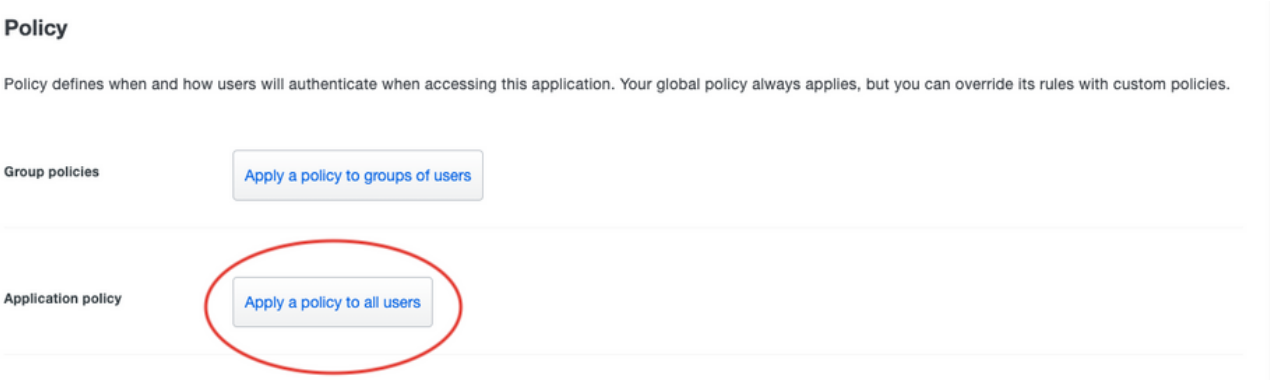
Schritt 5: Geben Sie die Informationen zum Service Provider ein.

Cisco FirePOWER Base-URL - Der FQDN zum Erreichen des FTD

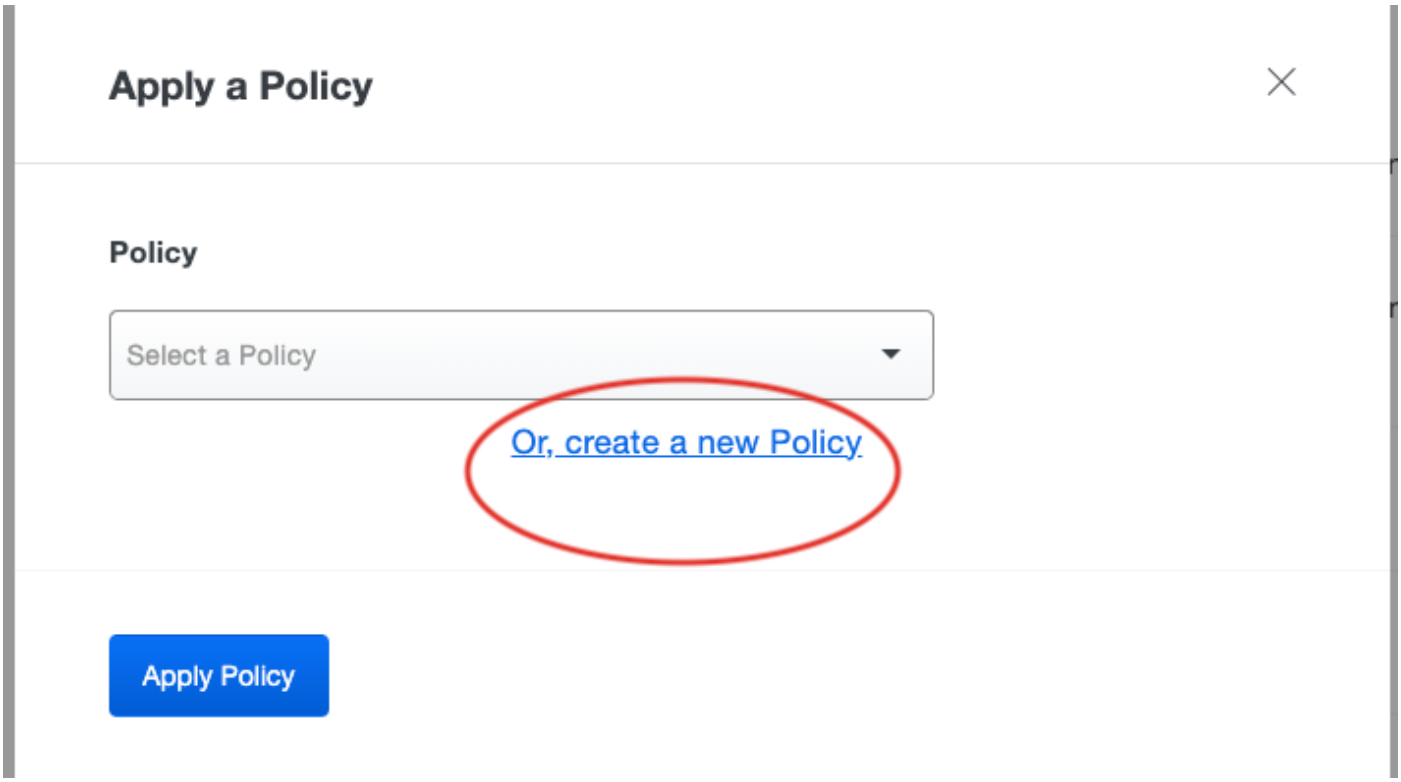
Name des Verbindungsprofils - Name der Tunnelgruppe

Anwendungsrichtlinie erstellen

Schritt 1: So erstellen Sie eine Anwendungsrichtlinie unter Richtlinie Wählen Sie "Eine Richtlinie auf alle Benutzer anwenden", und wählen Sie dann "Oder, eine neue Richtlinie erstellen", wie im Bild gezeigt.

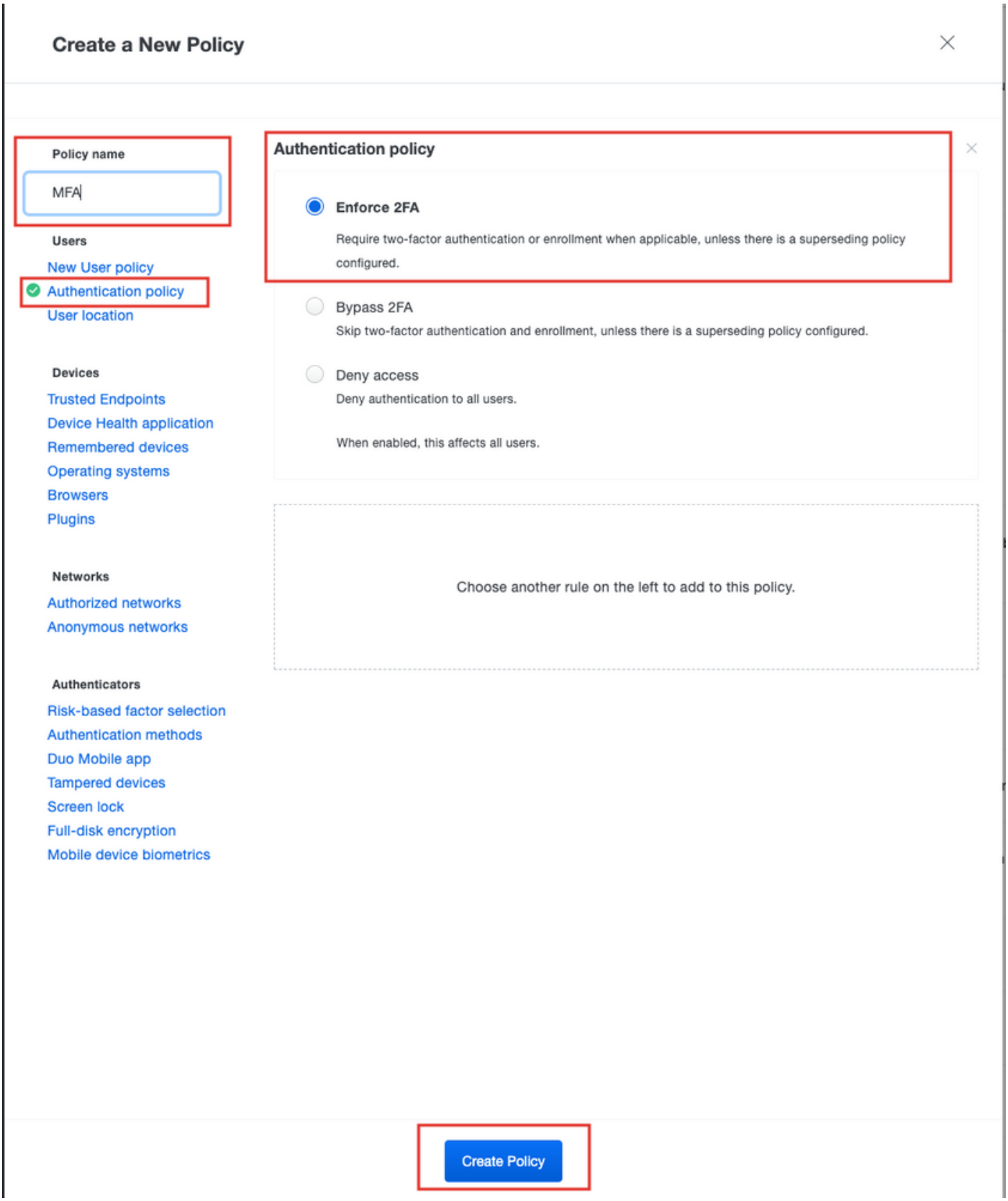


Beispiel für das Erstellen einer Anwendungsrichtlinie



Beispiel für das Erstellen einer Anwendungsrichtlinie

Schritt 2: Geben Sie unter Richtlinienname den gewünschten Namen ein, wählen Sie unter Benutzer die Option "Authentifizierungsrichtlinie" und anschließend die Option "Durchsetzen von 2FA." Speichern Sie dann mit "Richtlinie erstellen".



Beispiel für das Erstellen einer Anwendungsrichtlinie

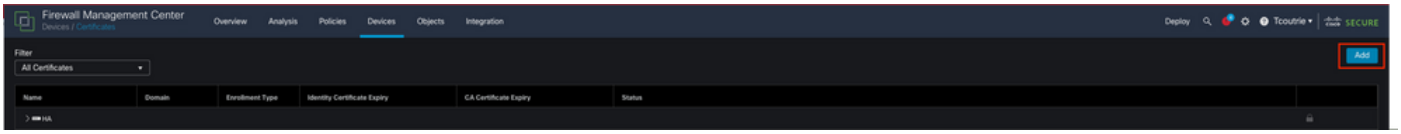
Schritt 3: Wenden Sie die Richtlinie mit "Apply Policy" (Richtlinie anwenden) im nächsten Fenster an. Führen Sie dann einen Bildlauf nach unten durch, und wählen Sie "Speichern" aus, um die DUO-Konfigurationen abzuschließen.

Konfigurationsschritte für FMC

Bereitstellung des Identitätszertifikats für die FTD

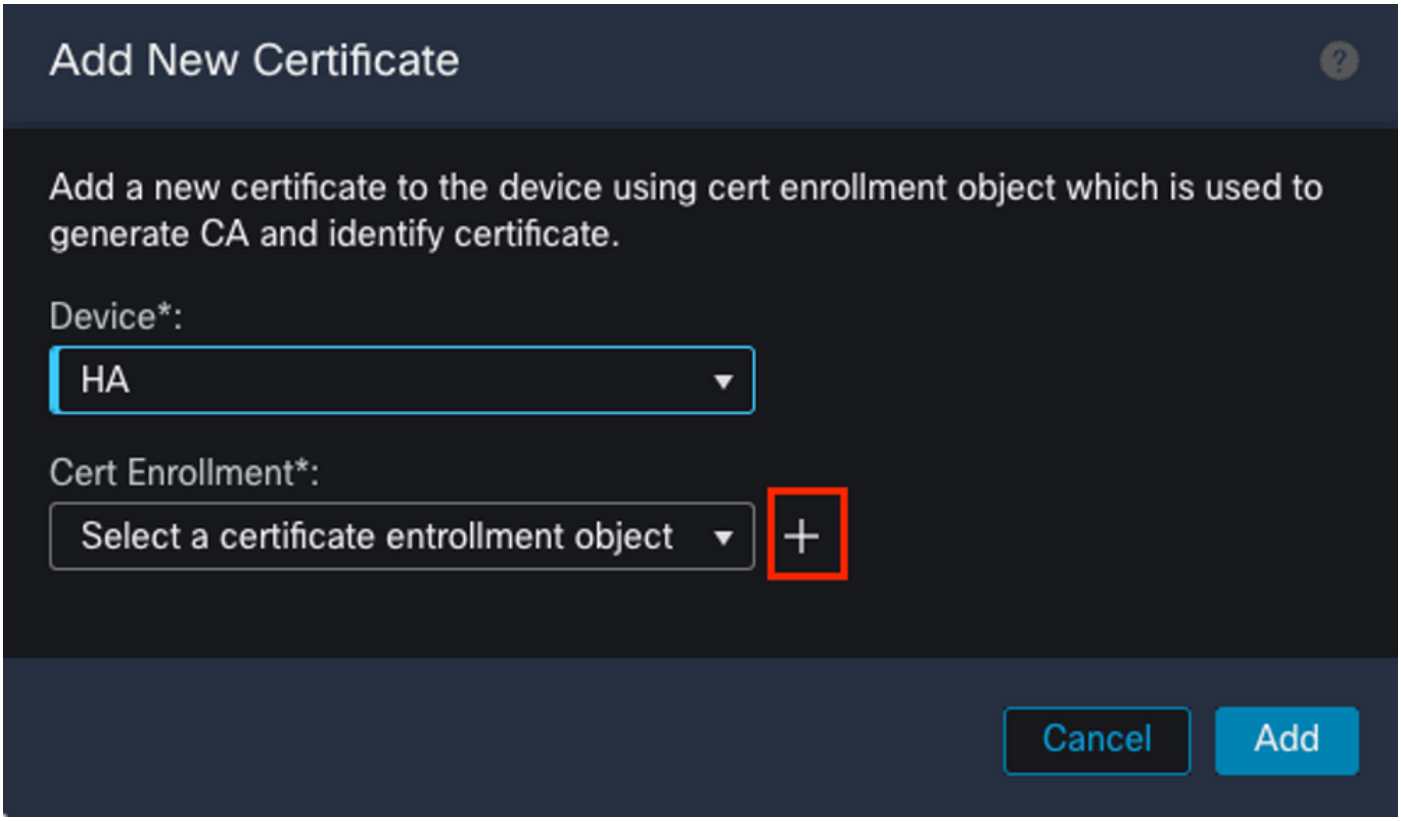
In diesem Abschnitt wird die Konfiguration und Bereitstellung des Identitätszertifikats für die FTD beschrieben, die für die Zertifikatsauthentifizierung erforderlich ist. Stellen Sie vor dem Start sicher, dass Sie alle Konfigurationen bereitstellen.

Schritt 1: Navigieren Sie zuGeräte > Zertifikat, und wählen SieHinzufügen aus, wie im Bild dargestellt.



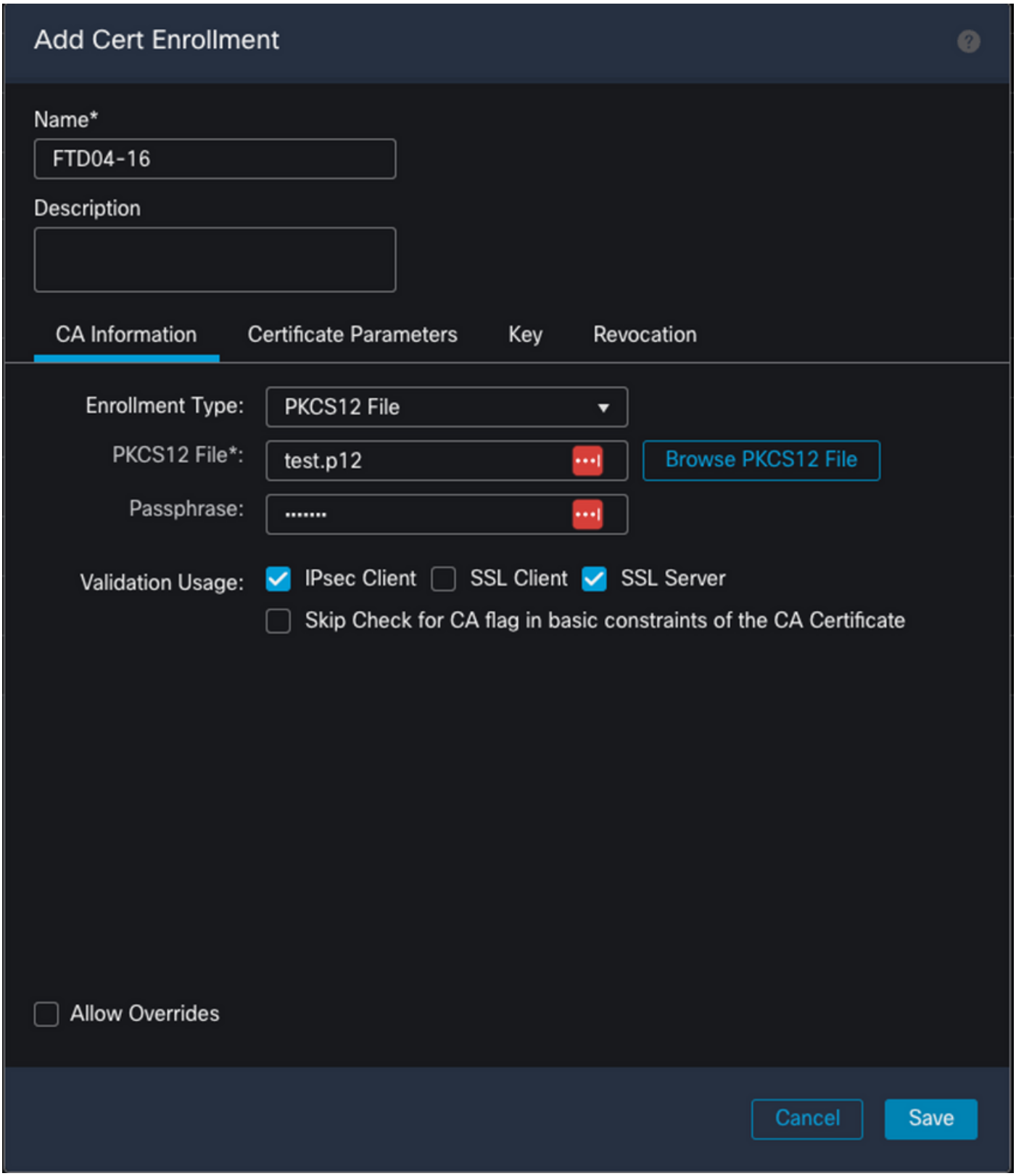
Screenshot der Geräte/Zertifikate

Phase 2: Wählen Sie die FTD-Appliance aus der Dropdown-Liste aus. Klicken Sie auf das Symbol +, um eine neue Zertifikatregistrierungsmethode hinzuzufügen.



Screenshot des neuen Zertifikats hinzufügen

Schritt 3: Wählen Sie die bevorzugte Methode zum Abrufen von Zertifikaten in der Umgebung über den "Anmeldungstyp" aus, wie im Bild gezeigt.



Screenshot der neuen Seite für die Zertifikatsregistrierung

Tipp: Es stehen folgende Optionen zur Verfügung: Selbstsigniertes Zertifikat - Lokales Erstellen eines neuen Zertifikats, SCEP - Verwenden des einfachen Zertifikatregistrierungsprotokolls, um ein Zertifikat von einer Zertifizierungsstelle zu erhalten, Manuell - Manuelles Installieren des Stamm- und Identitätszertifikats, PKCS12 -

Hochladen des verschlüsselten Zertifikatpakets mit Stamm, Identität und privatem Schlüssel.

Bereitstellung des IDP-Zertifikats für das FTD

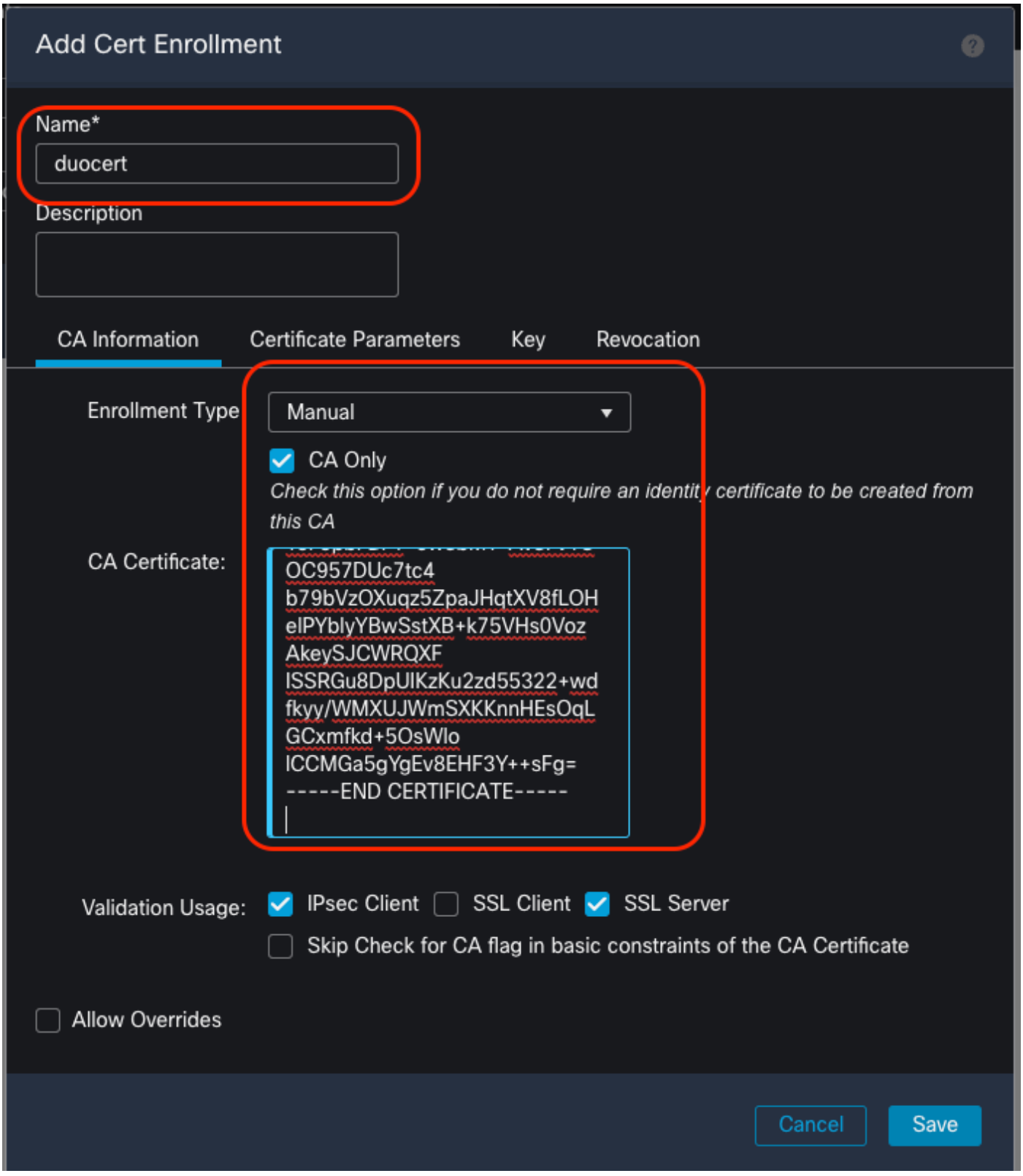
In diesem Abschnitt wird die Konfiguration und Bereitstellung des IDP-Zertifikats für das FTD beschrieben. Stellen Sie sicher, dass Sie alle Konfigurationen bereitstellen, bevor Sie beginnen.

Schritt 1: Navigieren Sie zu Geräte > Zertifikat, und wählen Sie Hinzufügen."

Phase 2: Wählen Sie die FTD-Appliance aus der Dropdown-Liste aus. Klicken Sie auf das Symbol +, um eine neue Zertifikatregistrierungsmethode hinzuzufügen.

Schritt 3: Geben Sie im Fenster "Add Cert Enrollment" (Zertifikatsregistrierung hinzufügen) die erforderlichen Informationen ein, wie im Bild dargestellt, und klicken Sie dann auf "Save" (Speichern), wie im Bild dargestellt.

- Name: Name des Objekts
- Anmeldungstyp: Manuell
- Kontrollkästchen aktiviert: Nur CA
- Zertifizierungsstellenzertifikat: Pem Format des Zertifikats

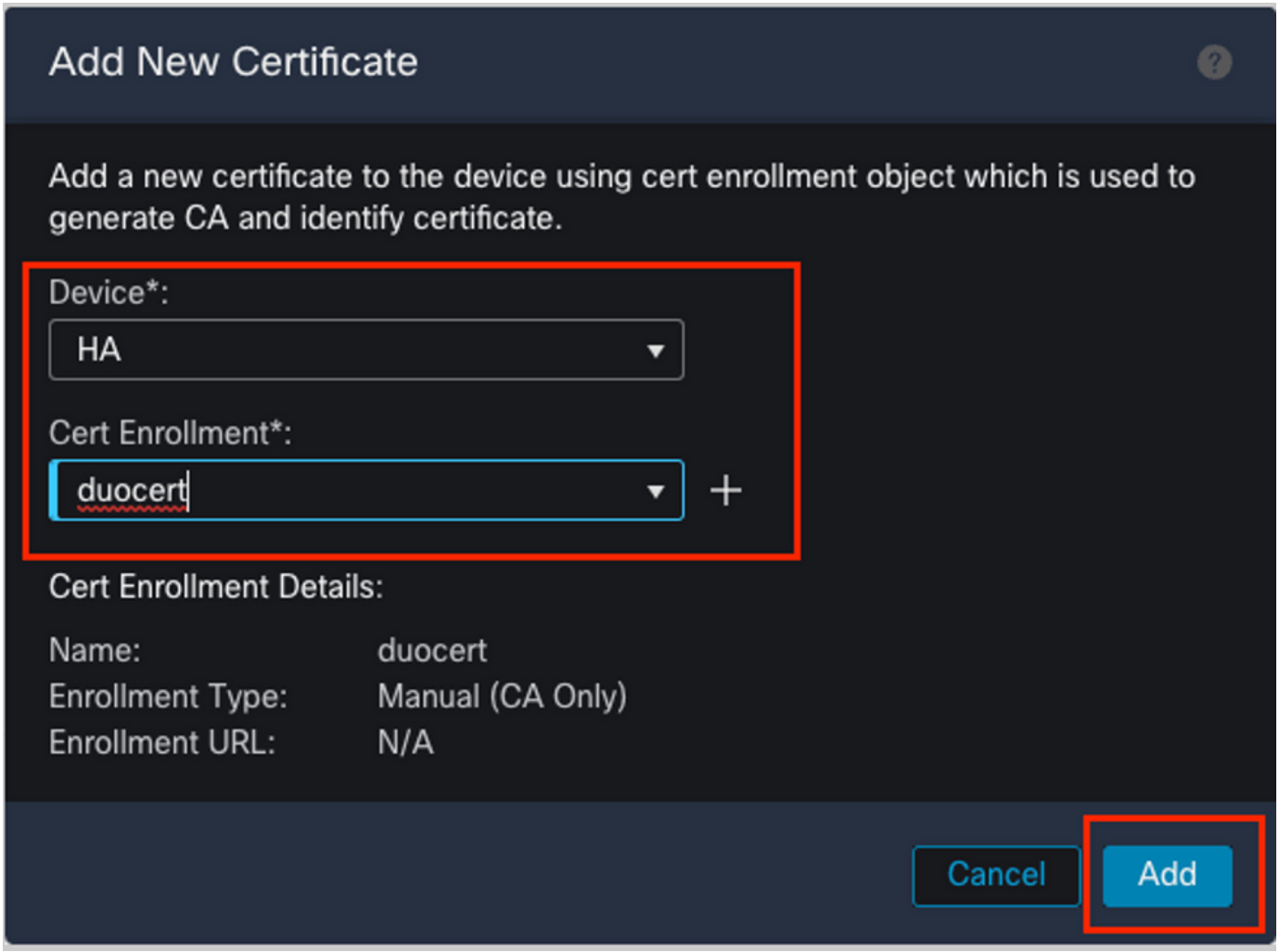


Beispiel zum Erstellen eines Zertifikatregistrierungsobjekts

⚠ Vorsicht: Bei Bedarf kann "Prüfung auf CA-Flag in grundlegenden Einschränkungen des CA-Zertifikats überspringen" verwendet werden. Verwenden Sie diese Option mit Vorsicht.

Schritt 4: Wählen Sie das neu erstellte Zertifikatregistrierungsobjekt unter "Zertifikatregistrierung*:"

und wählen Sie dann "Hinzufügen" aus, wie im Bild gezeigt.



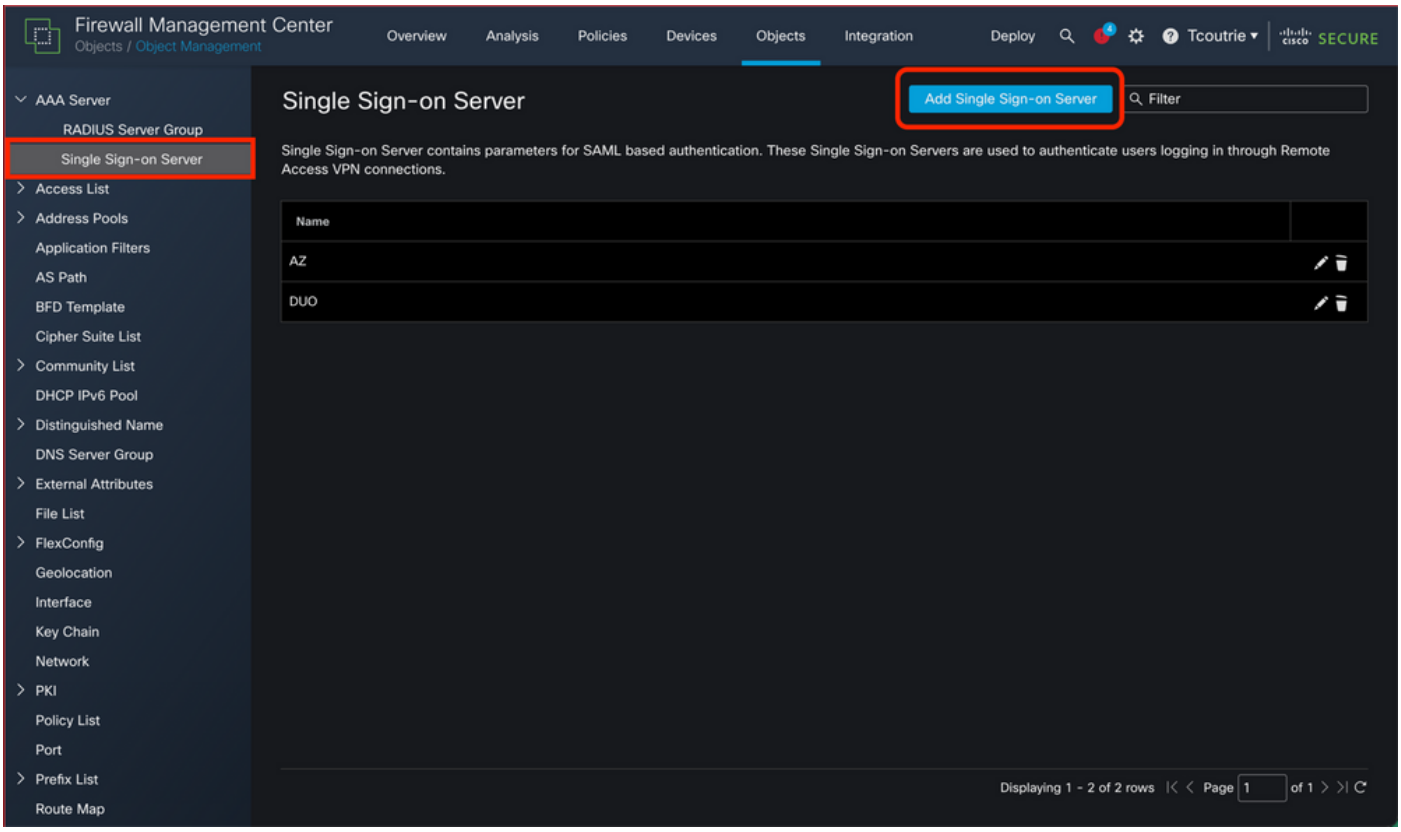
Screenshot des hinzugefügten Zertifikatregistrierungsobjekts und des Geräts

Anmerkung: Nach dem Hinzufügen wird das Zertifikat sofort bereitgestellt.

Erstellen des SAML-SSO-Objekts

In diesem Abschnitt werden die Schritte zur Konfiguration von SAML SSO über FMC beschrieben. Stellen Sie vor dem Start sicher, dass Sie alle Konfigurationen bereitstellen.

Schritt 1: Navigieren Sie zu Objekte > AAA-Server > Single Sign-on-Server, und wählen Sie "Single Sign-on-Server hinzufügen".

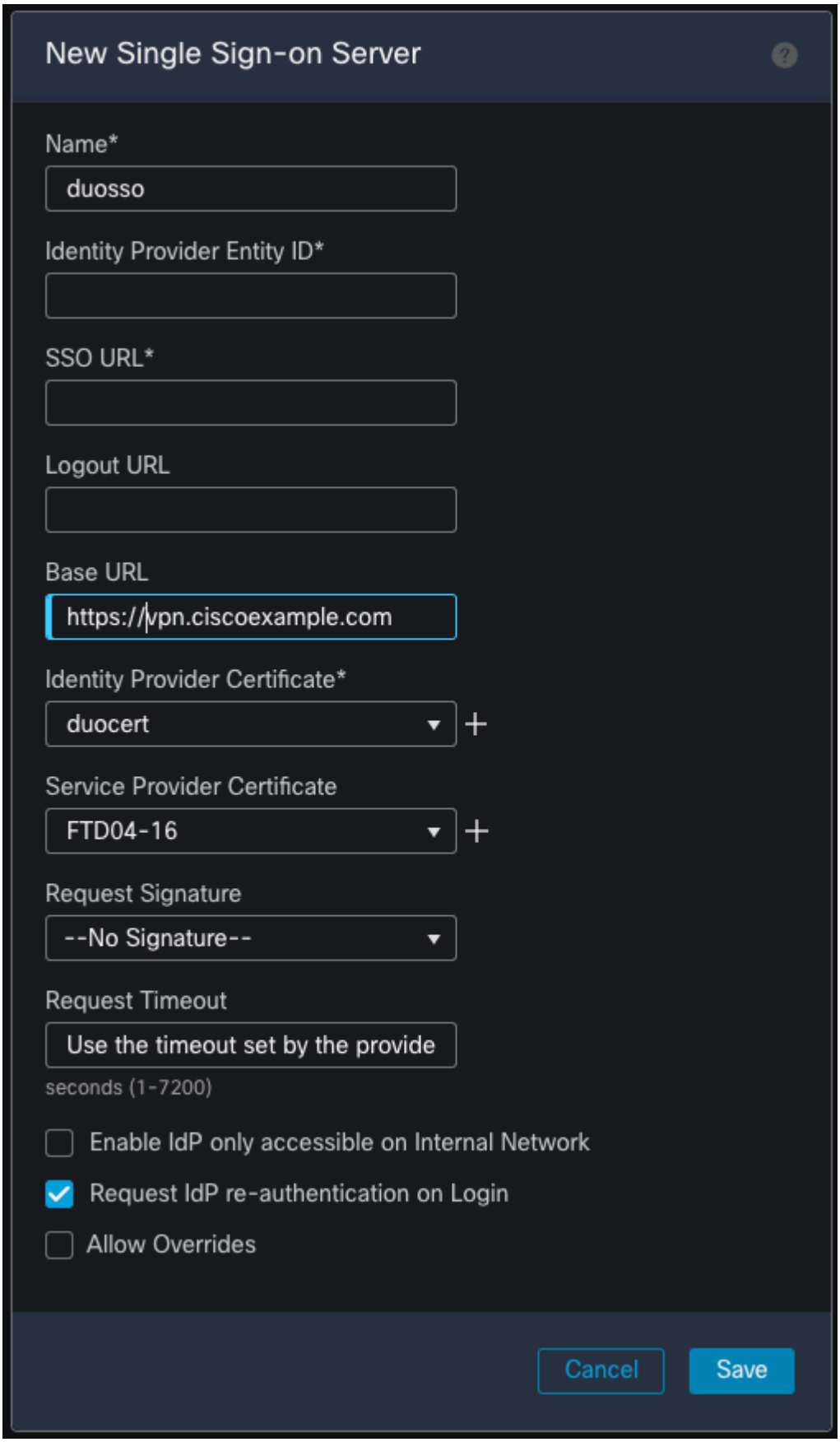


Beispiel zum Erstellen eines neuen SSO-Objekts

Schritt 2: Geben Sie die erforderlichen Informationen aus "Create an Application Protection Policy" (Anwendungsschutzrichtlinie erstellen) ein

". Um fortzufahren, nachdem Sie fertig sind, wählen Sie "Speichern".

- Name*: Name des Objekts
- Element-ID des Identitätsanbieters*: Element-ID aus Schritt 3
- SSO-URL*: Anmelde-URL aus Schritt 3 kopiert
- Abmelden-URL: Abmelden-URL aus Schritt 3 kopiert
- Basis-URL: Verwenden desselben FQDN wie "Cisco FirePOWER Base URL" in Schritt 5
- Zertifikat des Identitätsanbieters*: bereitgestelltes IDP-Zertifikat
- Dienstanbieterzertifikat: Zertifikat auf der externen Schnittstelle des FTD



Beispiel für ein neues SSO-Objekt.

Anmerkung: Die Links für die Element-ID, die SSO-URL und die Abmelde-URL wurden im

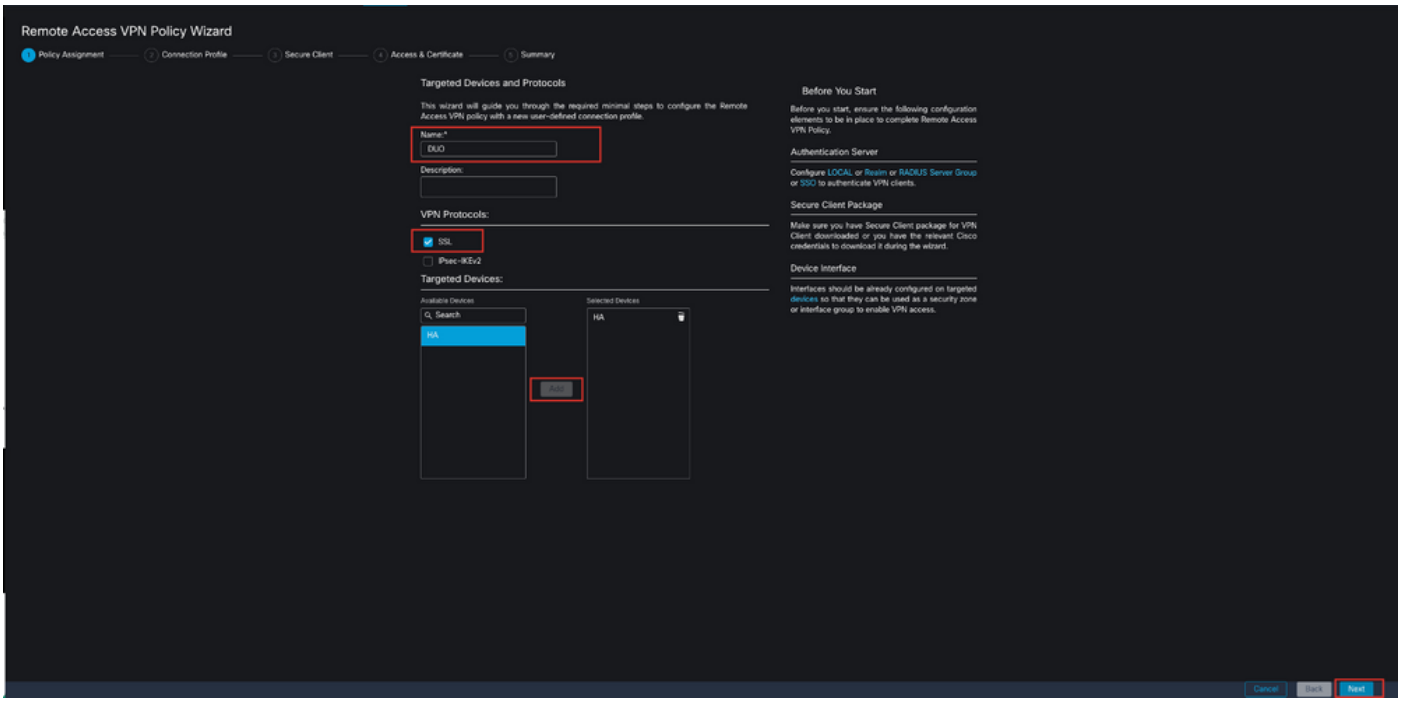
Screenshot weggelassen.

Erstellen einer RAVPN-Konfiguration (Virtual Private Network) für Remote-Zugriff

In diesem Abschnitt werden die Schritte zur RAVPN-Konfiguration mithilfe des Assistenten beschrieben.

Schritt 1: Navigieren Sie zu Geräte > Remotezugriff Wählen Sie "Hinzufügen" aus.

Schritt 2. Geben Sie im Assistenten den Namen des neuen RAVPN Policy Wizard ein, und wählen Sie unter VPN Protocols: Add the Targeted Devices (VPN-Protokolle: Zielgeräte hinzufügen) die Option SSL aus, wie im Bild dargestellt. Wählen Sie nach Abschluss der Aktion "Weiter" aus.



Schritt 1 des RAVPN-Assistenten

Schritt 2: Stellen Sie für das Verbindungsprofil die hier gezeigten Optionen ein: Wählen Sie nach Abschluss "Weiter" aus.

- Verbindungsprofilname: Verwenden Sie den Namen der Tunnelgruppe in Schritt 5 von "Erstellen einer Anwendungsschutzrichtlinie".

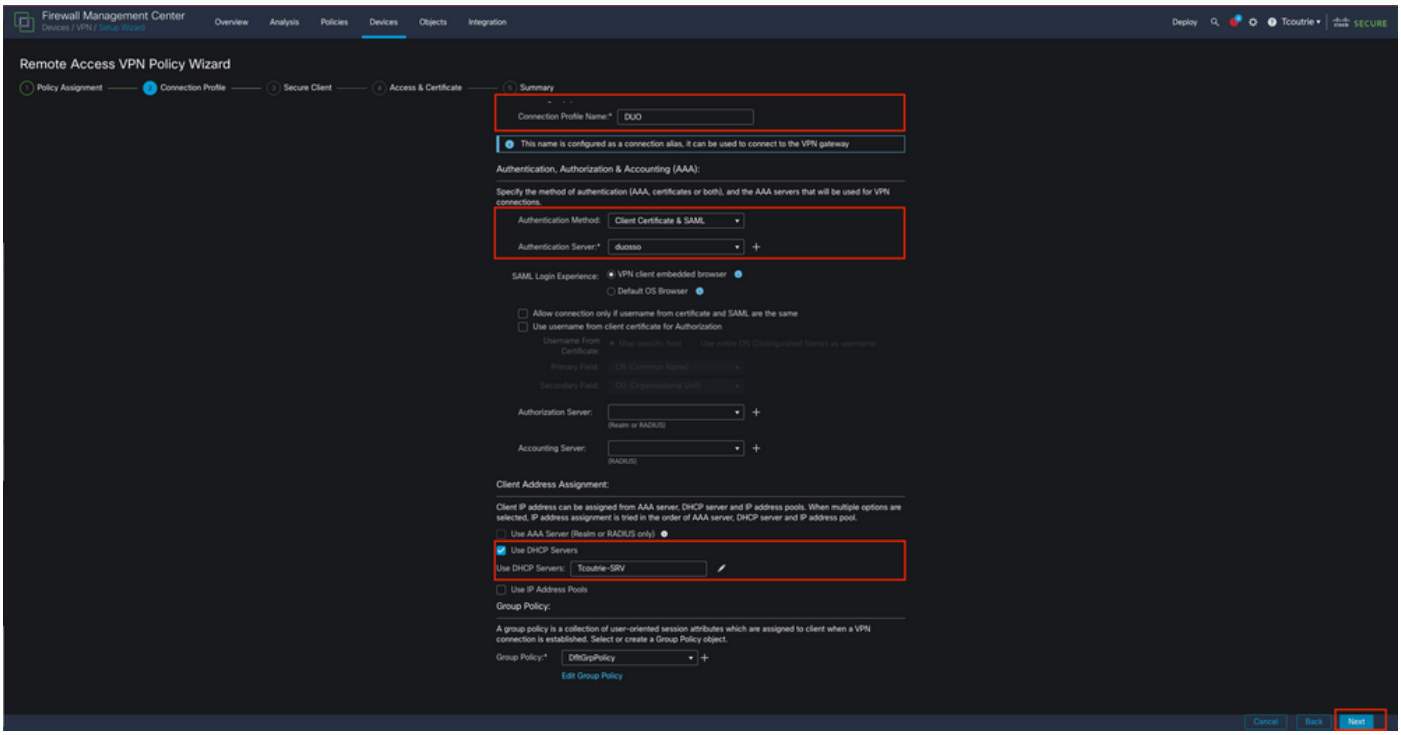
Authentifizierung, Autorisierung und Abrechnung (AAA):

- Authentifizierungsmethode: Client-Zertifikat und SAML
- Authentifizierungsserver:* Wählen Sie das SSO-Objekt aus, das während der Erstellung des SAML-SSO-Objekts erstellt wurde.

Client-Adressenzuweisung:

- AAA-Server verwenden (nur Bereich oder RADIUS) - Radius oder LDAP

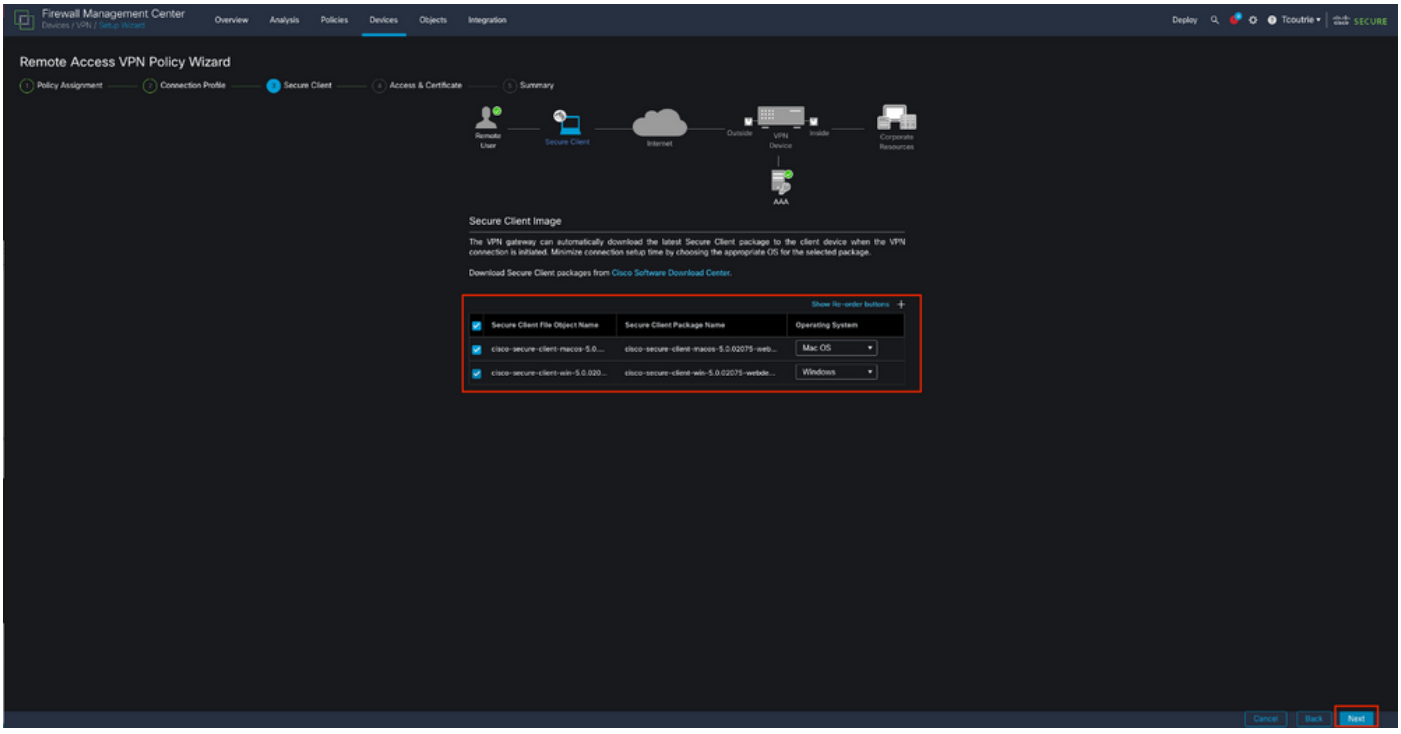
- DHCP-Server verwenden - DHCP-Server
- IP-Adresspools verwenden - Lokaler Pool auf dem FTD



Schritt 2 des RAVPN-Assistenten

Tipp: Für diese Übung wird ein DHCP-Server verwendet.

Schritt 3: Wählen Sie "+", um ein Web-Bereitstellungs-Image des bereitzustellenden Cisco Secure Client hochzuladen. Aktivieren Sie dann das Kontrollkästchen für das bereitzustellende CSC-Image. wie im Bild dargestellt. Wählen Sie "Weiter" nach Abschluss.

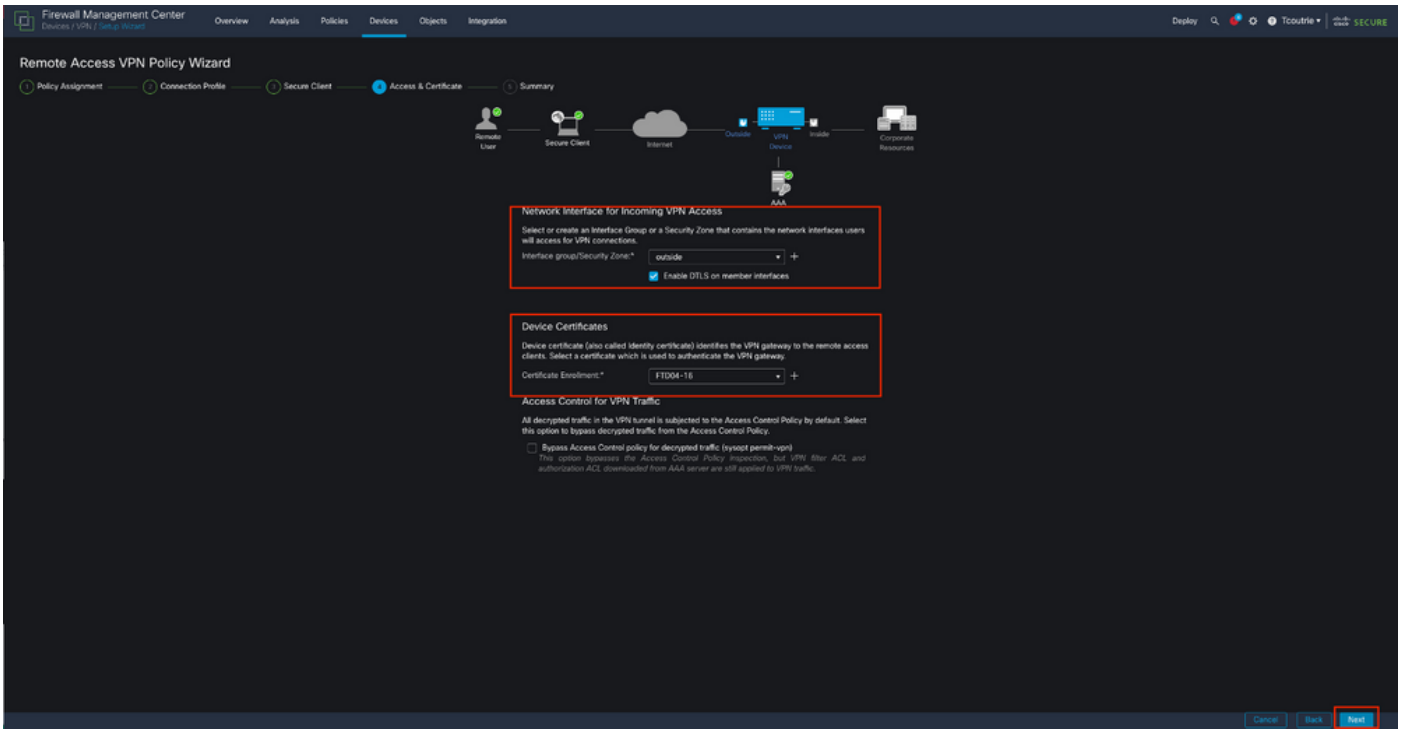


Schritt 3 RAVPN-Assistent

Schritt 4. Setzen Sie diese Objekte (wie im Bild zu sehen): Wählen Sie "Weiter" einmal abgeschlossen.

Schnittstellengruppe/Sicherheitszone:*: Externe Schnittstelle

"Zertifikatregistrierung:*": Identitätszertifikat, das während des Abschnitts "Bereitstellung des Identitätszertifikats für das FTD" dieses Leitfadens erstellt wurde

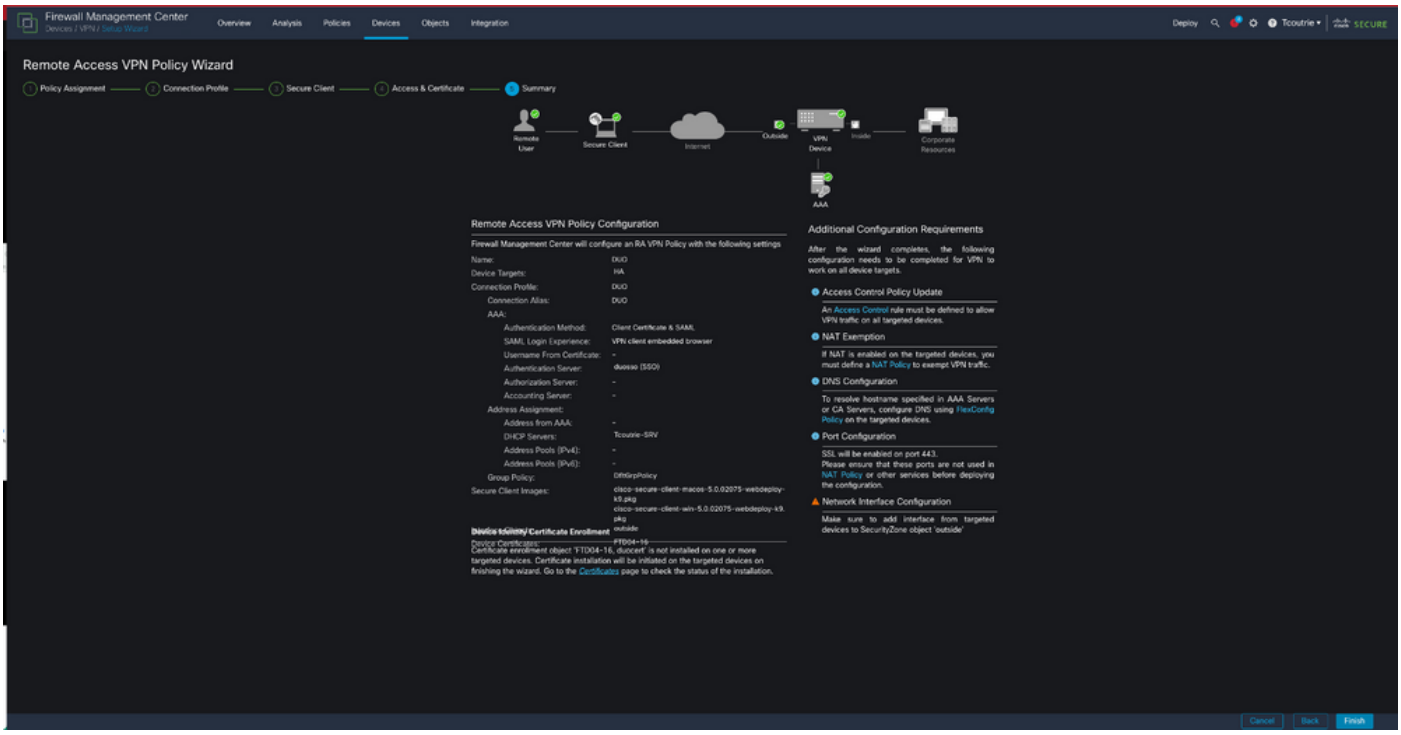


Schritt 4 des RAVPN-Assistenten

Tipp: Wenn dies nicht erstellt wurde, fügen Sie ein neues Zertifikatregistrierungsobjekt hinzu, indem Sie auf "+" klicken.

Schritt 6: Übersicht

Überprüfen Sie alle Informationen. Wenn alles korrekt ist, fahren Sie mit 'Beenden."



Übersichtsseite

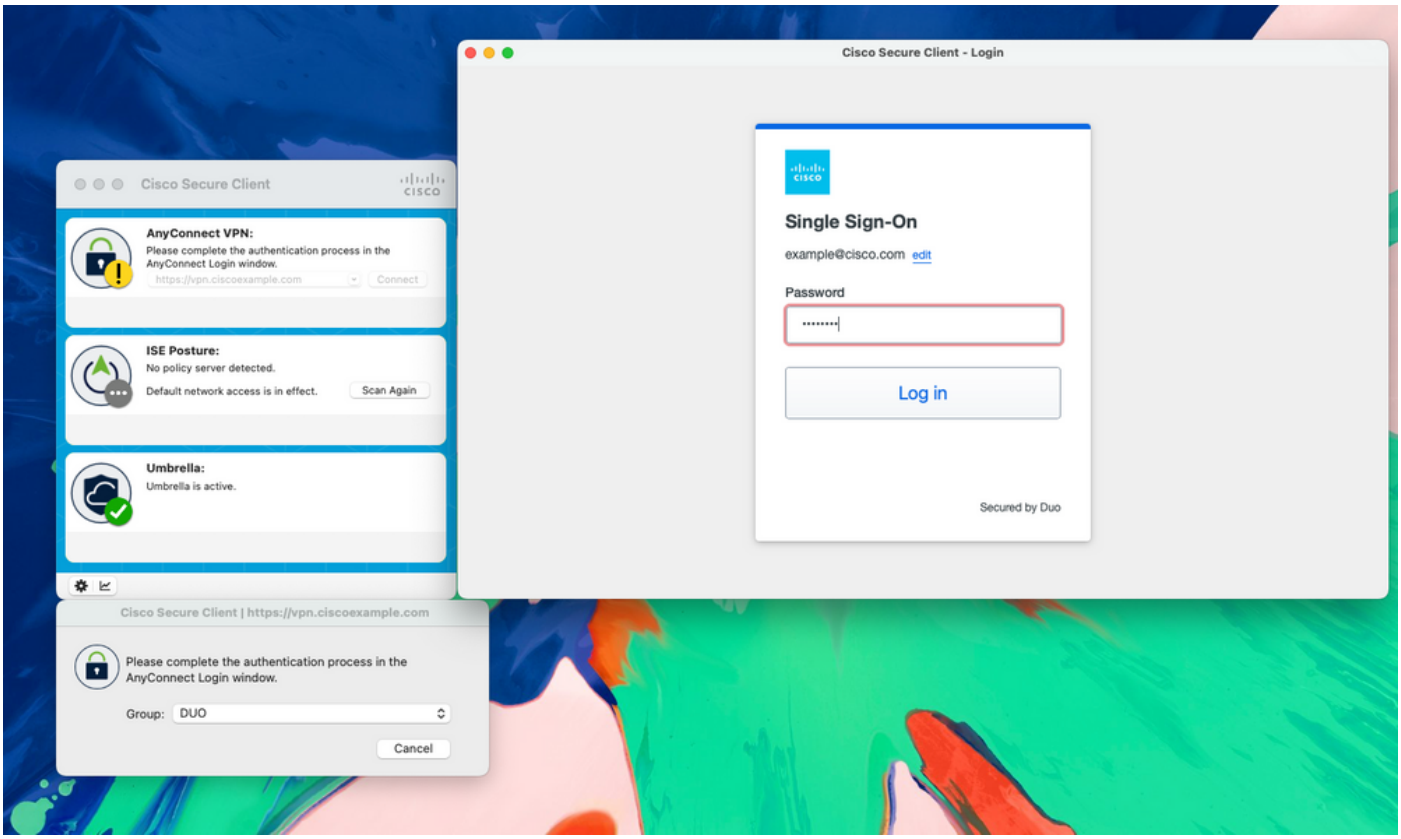
Schritt 7: Bereitstellen der neu hinzugefügten Konfigurationen

Überprüfung

In diesem Abschnitt wird beschrieben, wie Sie einen erfolgreichen Verbindungsversuch überprüfen.

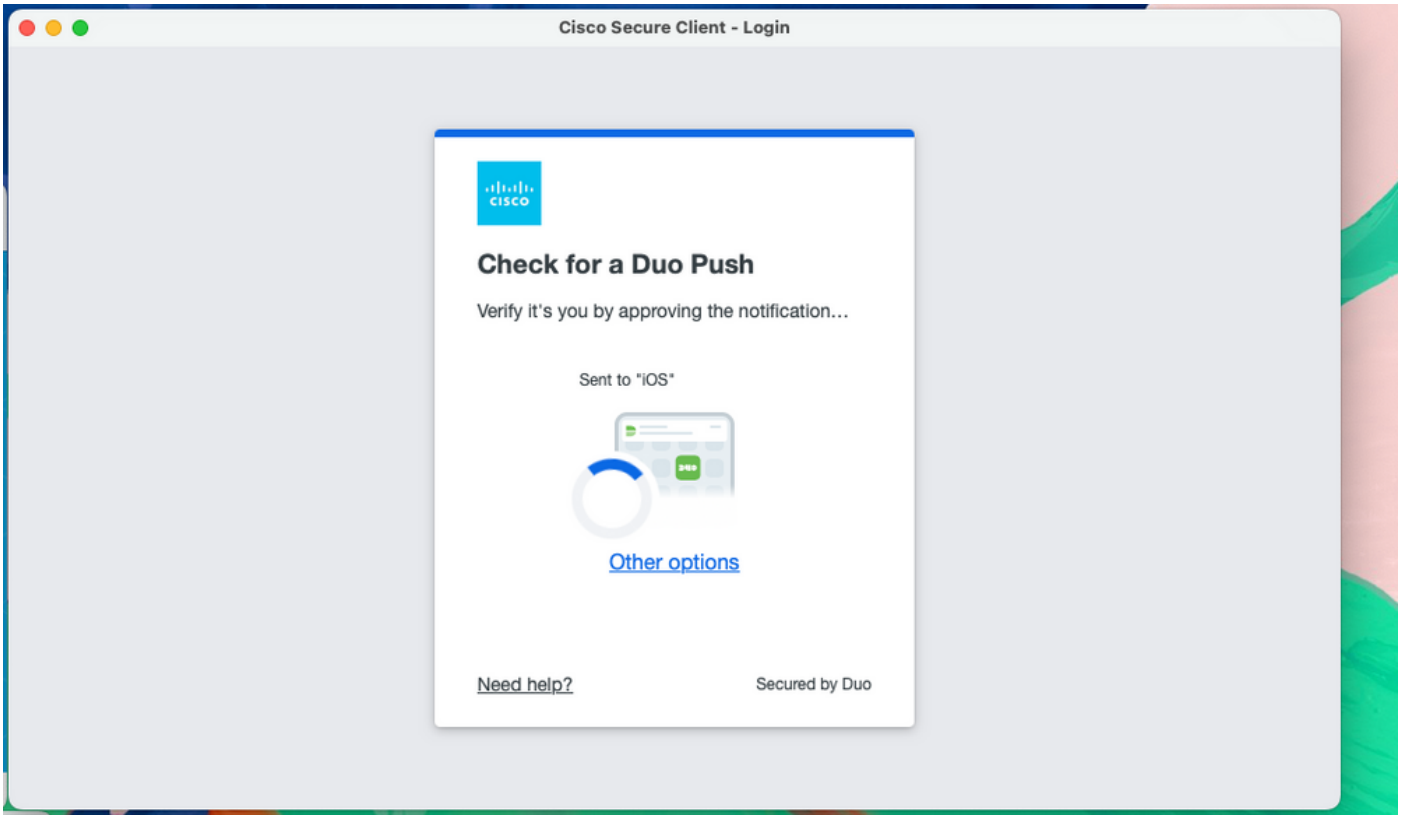
Öffnen Sie den Cisco Secure Client, geben Sie den FQDN des FTD ein, und stellen Sie die Verbindung her.

Geben Sie die Anmeldeinformationen auf der Seite SSO ein.



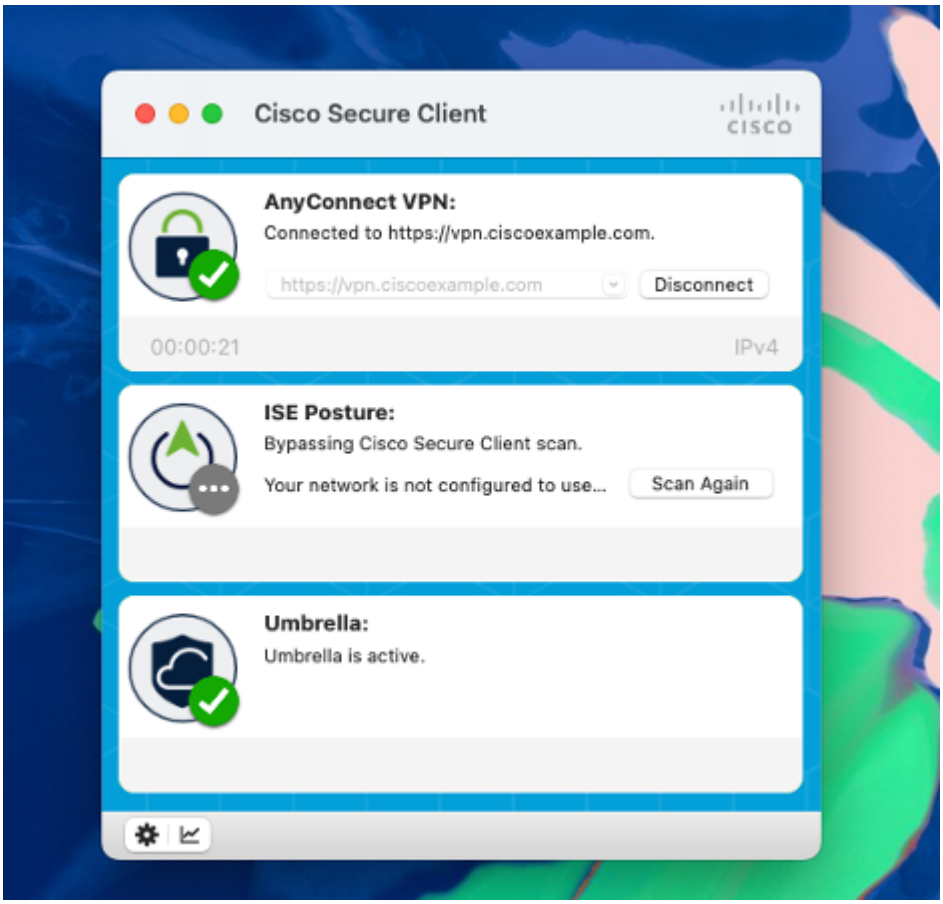
SSO-Seite über Cisco Secure Client

Akzeptieren Sie die DUO-Übertragung auf das registrierte Gerät.



DUO-Push

Verbindung erfolgreich hergestellt.



Mit FTD verbunden

Überprüfen Sie mit dem folgenden Befehl die FTD-Verbindung: show vpn-sessiondb detail anyconnect

```
tcoutrie-ftd2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     :                       Index        : 1916
Assigned IP  :                       Public IP    :
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel:
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SH
Bytes Tx     : 390964                Bytes Rx     : 124114
Pkts Tx      : 1216                  Pkts Rx      : 1223
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy :                       Tunnel Group :
Login Time   : 23:54:41 UTC Tue Jul 18 2023
Duration     : 0h:11m:28s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : 0a7aa95d0077c00064b72641
Security Grp : none                  Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 1916.1
  Public IP    :
  Encryption   : none                  Hashing      : none
  TCP Src Port : 53859                 TCP Dst Port : 443
  Auth Mode    : Certificate and SAML
  Idle Time Out: 30 Minutes            Idle TO Left : 18 Minutes
  Client OS    : mac-intel
```

Im Ausgabebeispiel wurden einige Informationen ausgelassen.

Fehlerbehebung

Dies sind mögliche Probleme, die nach der Implementierung auftreten.

Ausgabe 1: Die Zertifikatauthentifizierung ist fehlgeschlagen.

Stellen Sie sicher, dass das Stammzertifikat auf dem FTD installiert ist.

Verwenden Sie folgende Debugging-Optionen:

debug crypto ca 14

debug aaa shim 128

debuggen aaa häufig 128

Ausgabe 2: SAML-Fehler

Diese Fehlerbehebungen können aktiviert werden, um:

debug aaa shim 128

debuggen aaa häufig 128

debug webvpn anyconnect 128

debug webvpn saml 255

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.