

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

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

- [a. Erstellen/Importieren eines Zertifikats für die Serverauthentifizierung](#)
- [b. Hinzufügen eines Zertifikats einer vertrauenswürdigen/internen Zertifizierungsstelle](#)
- [c. Konfigurieren des Adresspools für VPN-Benutzer](#)
- [d. Hochladen sicherer Client-Images](#)
- [e. Erstellen und Hochladen eines XML-Profiles](#)

[Konfiguration des Remotezugriff-VPNs](#)

[Überprüfung](#)

[Fehlerbehebung](#)

---

## 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 Authentifizierungskennnisse für Remote Access VPN
  - Zertifizierungsstelle eines Drittanbieters (Certificate Authority, CA) wie Entrust, Geotrust, GoDaddy, Thawte und VeriSign

### Verwendete Komponenten

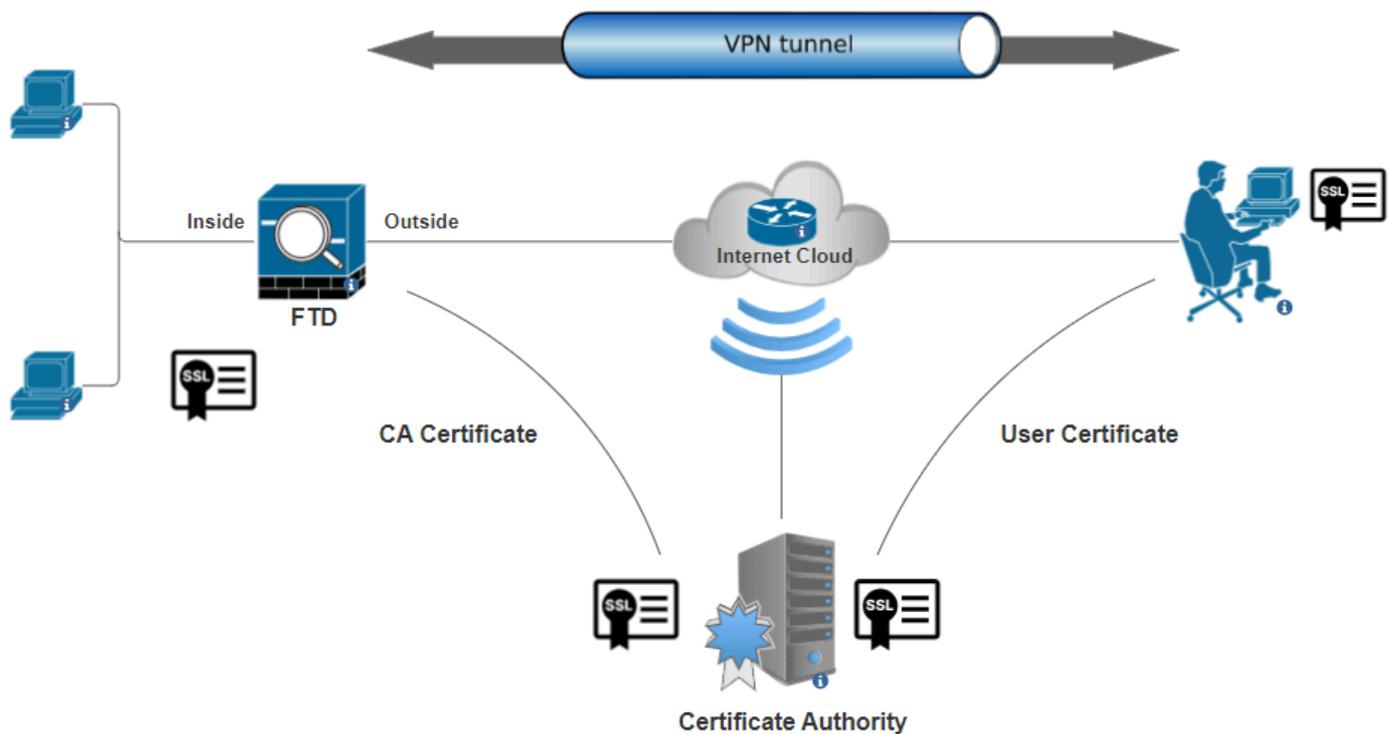
Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- 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 > Certificates](#) und klicken Sie auf Add. Wählen Sie Gerät aus, und klicken Sie unter Zertifikatregistrierung auf das Pluszeichen (+).

## Add New Certificate



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

Device\*:

Cert Enrollment\*:

Cancel

Add

*Zertifikatregistrierung hinzufügen*

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

## Add Cert Enrollment



Name\*

ssl\_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

*Check this option if you do not require an identity certificate to be created from this CA*

CA Certificate:

```
HQYDVQQDEZXIEWRYRW50S
UQgU2VydmVylENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID=Z...
```

Validation Usage:



IPsec Client



SSL Client



SSL Server



Skip Check for CA flag in basic constraints of the CA Certificate

Cancel

Save

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.

## Add Cert Enrollment



Name\*

ssl\_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN: Don't use FQDN in certificate ▼

Include Device's IP Address:

Common Name (CN): certauth.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): Bangalore

State (ST): KA

Country Code (C): IN

Email (E):

Include Device's Serial Number

Cancel

Save

*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.

---

## Add Cert Enrollment



Name\*

Description

CA Information   Certificate Parameters   **Key**   Revocation

**Key Type:**

RSA    ECDSA    EdDSA

Key Name:\*

**Key Size:**

▼ Advanced Settings

Ignore IPsec Key Usage

*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.

## Add New Certificate



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

Device\*:

Cert Enrollment\*:

 +

Cert Enrollment Details:

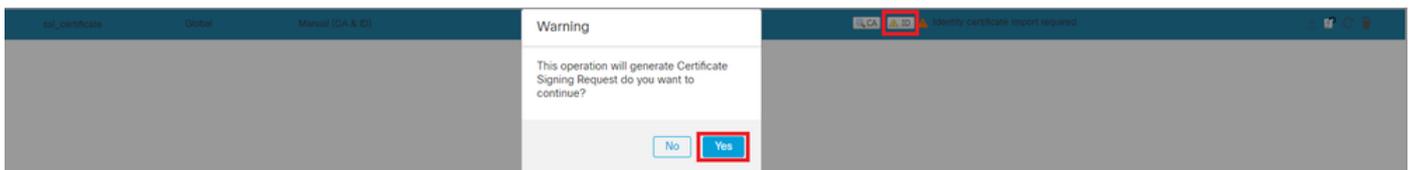
Name: ssl\_certificate  
Enrollment Type: Manual (CA & ID)  
Enrollment URL: N/A

Cancel

Add

*Neues Zertifikat hinzufügen*

Schritt 7. Klicken Sie auf ID und anschließend auf die Yes 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 klicken Import.

# Import Identity Certificate



## Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMakGA1UEBhMC
SU4wgglIIMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1pLEdR4X6ZlnM5fNA/GLV9MnPoP
ppzi0uLlbVmb5iKQexllaur/e3PDccc3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

## Step 2

Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

[Import](#)



**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.

General Details Certification Path



### Certificate Information

**This certificate is intended for the following purpose(s):**

- All issuance policies
- All application policies

**Issued to:** auth-risaggar-ca

**Issued by:** auth-risaggar-ca

**Valid from** 04-03-2023 **to** 04-03-2033

Issuer Statement

OK

*auth-risaggar-ca*

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

Schritt 3: Aktivieren CA Only und 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.

### Add Cert Enrollment ?

Description

CA InformationCertificate ParametersKeyRevocation

Enrollment Type: Manual

CA Only

*Check this option if you do not require an identity certificate to be created from this CA*

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
--  
MIIG1jCCBL6gAwIBAgIQQAFu  
+wogXPrr4Y9x1zq7eDANBgk  
qhkiG9w0BAQsFADBK  
MQswCQYDVQQGEwJVUzES  
MBAGA1UEChMJSWRlbiRydX  
N0MScwJQYDVQQDEx5JZGV  
u  
VHJ1c3QgQ29tbWVyY2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage:  IPsec Client  SSL Client  SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

CancelSave

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

# Add New Certificate



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

Device\*:

Cert Enrollment\*:

 +

Cert Enrollment Details:

Name: Internal\_CA  
Enrollment Type: Manual (CA Only)  
Enrollment URL: N/A

*Interne Zertifizierungsstelle hinzufügen*

Schritt 6: Das zuvor hinzugefügte Zertifikat wird angezeigt als:

Internal_CA	Global	Manual (CA Only)	Mar 4, 2033	CA ID	⌵ ⌵ ⌵ ⌵
-------------	--------	------------------	-------------	-------	---------

*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.

## Edit IPv4 Pool



Name\*

vpn\_pool

Description

IPv4 Address Range\*

10.20.20.1-10.20.20.130

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask\*

255.255.255.0

Allow Overrides

**i** Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▶ Override (0)

Cancel

Save

*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.

# Edit Secure Client File



Name:\*

File Name:\*

File Type:\*

Description:

*Sicheres Client-Image hinzufügen*

## e. Erstellen und Hochladen eines XML-Profiles

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 Option All aus. Es steuert hauptsächlich, welche Zertifikatspeicher(s) Secure Client zum Speichern und Lesen von Zertifikaten verwenden kann.

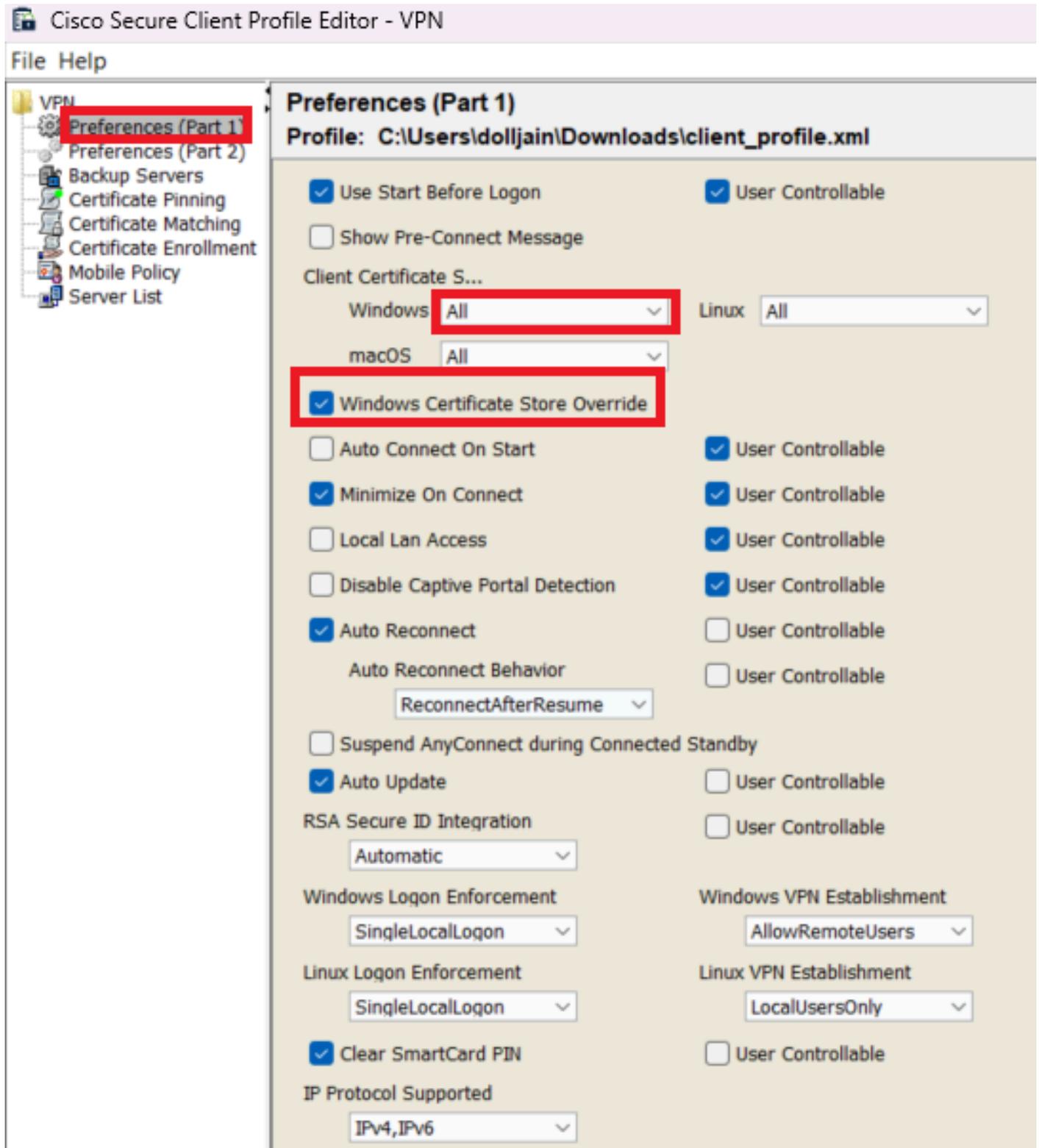
Zwei weitere Optionen sind:

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

Überschreiben des Zertifikatspeichers als True festlegen.

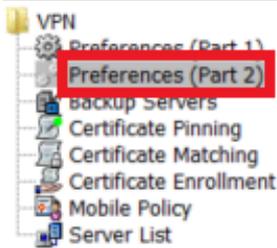
Dadurch kann ein Administrator Secure Client anweisen, Zertifikate im Zertifikatspeicher des Windows-Computers (lokales System) für die

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 Option `Disable Automatic Certificate Selection`, da der Benutzer nicht aufgefordert wird, das Authentifizierungszertifikat auszuwählen.



## Preferences (Part 2)

Profile: C:\Users\dolljain\Downloads\client\_profile.xml

Disable Automatic Certificate Selection

User Controllable

### Proxy Settings

Native

User Controllable

Public Proxy Server Address:

Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080

Allow Local Proxy Connections

Enable Optimal Gateway Selection

User Controllable

Suspension Time Threshold (hours)

Performance Improvement Threshold (%)

Automatic VPN Policy

Trusted Network Policy

Disconnect

Untrusted Network Policy

Connect

Bypass connect upon VPN session timeout

Trusted DNS Domains

Trusted DNS Servers

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Trusted Servers @ https://<server>[:<port>]

https://

Add

Delete

Certificate Hash:

Set

Disable interfaces without trusted server connectivity while in truste...

Always On

(More Information)

Allow VPN Disconnect

Allow access to the following hosts with VPN disconn...

Connect Failure Policy

Closed

Allow Captive Portal Remediation

Remediation Timeout (min.)

Apply Last VPN Local Resource Rules

Captive Portal Remediation Browser Failover

Allow Manual Host Input

PPP Exclusion

Disable

User Controllable

PPP Exclusion Server IP

User Controllable

Enable Scripting

User Controllable

Terminate Script On Next Event

Enable Post SBL On Connect Script

Retain VPN on Logoff

User Enforcement

Same User Only

Authentication Timeout (seconds)

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.

The screenshot shows the Cisco Secure Client Profile Editor - VPN interface. The main window displays the 'Server List' for a profile named 'C:\Users\dolljain\Downloads\client\_profile.xml'. The table below shows the current server entry:

Hostname	Host Address	User Group	Backup Serve...	SCEP	Mobile Settings	Certificate Pins
SSL-VPN	https://certaut...	ssl-cert	-- Inherited --			

Below the table, there is a note: "Note: it is highly recommended that at least one server be defined in a profile." and buttons for 'Add...', 'Delete', 'Edit...', and 'Details'.

The 'Server List Entry' dialog box is open, showing the configuration for the selected server. The 'Primary Server' section includes:

- Display Name (required): SSL-VPN
- FQDN or IP Address: https://certauth.cisco.com
- User Group: ssl-cert
- Group URL: (empty field)

The 'Connection Information' section includes:

- Primary Protocol: SSL
- ASA gateway: (unchecked)
- Auth Method During IKE Negotiation: EAP-AnyConnect
- IKE Identity (IOS gateway only): (empty field)

The 'Backup Servers' section includes a table for adding backup servers:

Host Address	Action
	Add
	Move Up
	Move Down
	Delete

Buttons for 'OK' and 'Cancel' are at the bottom of the dialog.

*Serverliste hinzufügen*

Schritt 5: Schließlich ist das XML-Profil einsatzbereit.

```

<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStoreAll</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreLinuxAll</CertificateStoreLinux>
    <CertificateStoreOverride>true</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>30</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
    <ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
    <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
    <AutoReconnect UserControllable="false">true
      <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
    </AutoReconnect>
    <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
    <AutoUpdate UserControllable="false">true</AutoUpdate>
    <RSA SecurIDIntegration UserControllable="false">Automatic</RSA SecurIDIntegration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVFNEstablishment>AllowRemoteUsers</WindowsVFNEstablishment>
    <LinuxVFNEstablishment>LocalUsersOnly</LinuxVFNEstablishment>
    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
    <PFPEExclusion UserControllable="false">Disable
      <PFPEExclusionServerIP UserControllable="false"></PFPEExclusionServerIP>
    </PFPEExclusion>
    <EnableScripting UserControllable="false">false</EnableScripting>
    <EnableAutomaticServerSelection UserControllable="false">false
      <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
      <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
    </EnableAutomaticServerSelection>
    <RetainVpnOnLogoff>false
      </RetainVpnOnLogoff>
    <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
    <AllowManualHostInput>true</AllowManualHostInput>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>SSL-VPN</HostName>
      <HostAddress>https://certauth.cisco.com</HostAddress>
      <UserGroup>ssl-cert</UserGroup>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>

```

## 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

# Edit Secure Client File



Name:\*

File Name:\*

File Type:\*

Description:

*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.

# Edit Standard Access List Object



Name

Split\_ACL

▼ Entries (1)

Add

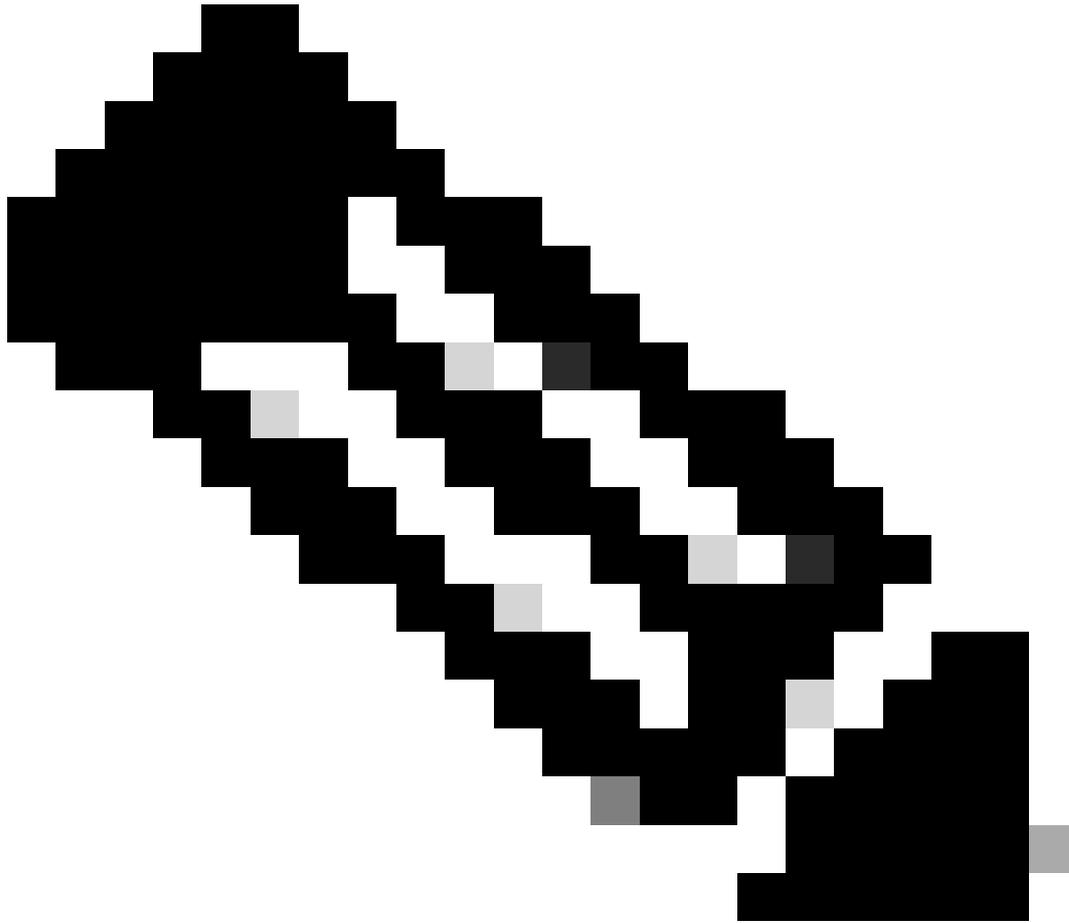
Sequence No	Action	Network	
1	Allow	split_acl	

Allow Overrides

Cancel

Save

*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".

## Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

### Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:\*

RAVPN

Description:

VPN Protocols:

- SSL  
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Q Search"/>	FTD-A-7.4.1
FTD-A-7.4.1	
FTD-B-7.4.0	
FTD-ZTNA-7.4.1	
<input type="button" value="Add"/>	

### Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

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

Secure Client Package

Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

*Profilnamen hinzufügen*

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

### 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:\* RAVPN-CertAuth

**i** 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: Client Certificate Only

Username From Certificate:  Map specific field  Use entire DN (Distinguished Name) as username

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Authorization Server:  +  
(Realm or RADIUS)

Accounting Server:  +  
(RADIUS)

*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 Address Assignment:

---

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:  

IPv6 Address Pools:  

*Client-Adressenzuweisung auswählen*

Schritt 6: Bearbeiten Sie die Gruppenrichtlinie.

## Group Policy:

---

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:\*  ▼ +

[Edit Group Policy](#)

*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.

# Edit Group Policy



Name:\*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

Tunnel networks specified below ▼

IPv6 Split Tunneling:

Allow all traffic over tunnel ▼

Split Tunnel Network List Type:

Standard Access List  Extended Access List

Standard Access List:

Split\_ACL ▼ +

DNS Request Split Tunneling

DNS Requests:

Send DNS requests as per split t ▼

Domain List:

Cancel

Save

*Split-Tunneling hinzufügen*

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

# Edit Group Policy



Name:\*

DfltGrpPolicy

Description:

General

**Secure Client**

Advanced

## Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

Secure Client profiles contains settings for the VPN client functionality and optional features. The Firewall Threat Defense deploys the profiles during Secure Client connection.

Client Profile:

Anyconnect\_Profile-5-0-05040

Standalone profile editor can be used to create a new or modify existing Secure Client profile. You can download the profile editor from [Cisco Software Download Center](#).

*Sicheres Clientprofil hinzufügen*

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

## Secure Client Image

The VPN gateway can automatically download the latest Secure Client 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 Secure Client packages from [Cisco Software Download Center](#).

Show Re-order buttons

<input type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyconnectWin-5.0.05040	cisco-secure-client-win-5.0.05040-webde...	Windows <input type="button" value="v"/>

*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.

## 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:\*  +  
 Enroll the selected certificate object on the target devices

## Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)  
*This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

*Zugriffskontrolle für VPN-Datenverkehr hinzufügen*

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

## Remote Access VPN Policy Configuration

---

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	FTD-B-7.4.0
Connection Profile:	RAVPN-CertAuth
Connection Alias:	RAVPN-CertAuth
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
Secure Client Images:	AnyconnectWin-5.0.05040
Interface Objects:	outside-zone
Device Certificates:	ssl_certificate

### Device Identity Certificate Enrollment

---

Certificate enrollment object 'ssl\_certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

*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 Plusymbol (+) klicken.

## Edit Connection Profile

Connection Profile:\*

Group Policy:\*  +

[Edit Group Policy](#)

Client Address Assignment   AAA   **Aliases**

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
ssl-cert	Enabled	

URL Alias:

Configure the list of UR following URLs, system

URL	
-----	--

### Edit Alias Name

Alias Name:

  
 Enabled

*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.

## Edit Connection Profile

Connection Profile:\* RAVPN-CertAuth

Group Policy:\* DfltGrpPolicy

Client Address Assignment   AAA   **Aliases**

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off.

### Edit URL Alias

URL Alias:

certauth

Enabled

Cancel   OK

URL Alias:

Configure the list of URL Aliases. If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status
certauth (https://certauth.cisco.com/ssl-cert)	Enabled

Cancel   Save

### Gruppen-URL bearbeiten

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

## RAVPN

Enter Description

Connection Profile   **Access Interfaces**   Advanced

Local Realm: cisco-local   Dynamic Access Policy: None

Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2
outside-zone	ssl_certificate	●	●	●

Access Settings

Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:\* 443

DTLS Port Number:\* 443

SSL Global Identity Certificate: ssl\_certificate

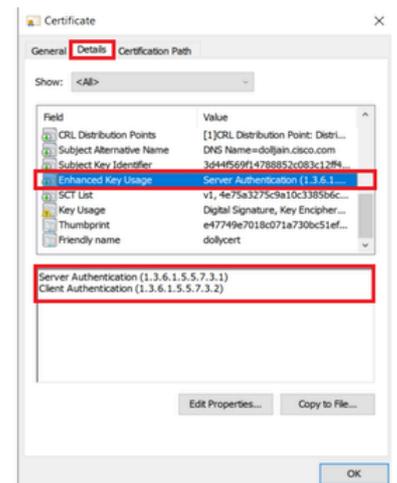
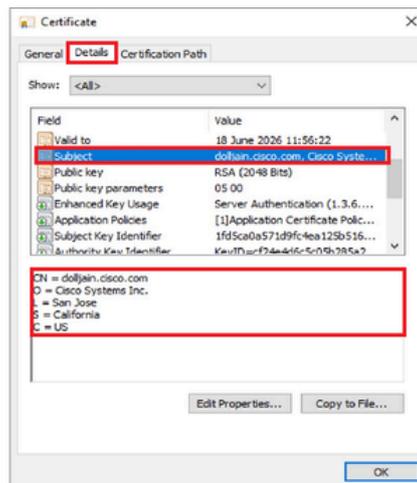
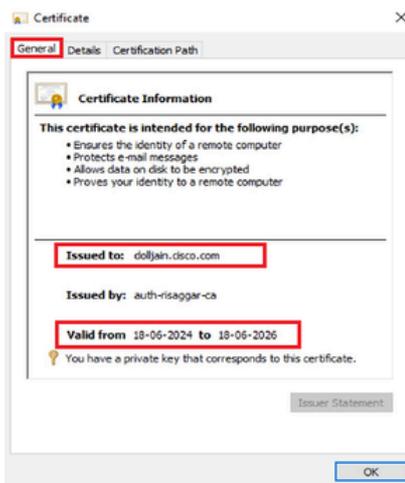
Note: Ensure the port used in VPN configuration is not used in other services

Schritt 16: Klicken Sie auf Save, und stellen Sie diese Änderungen bereit.

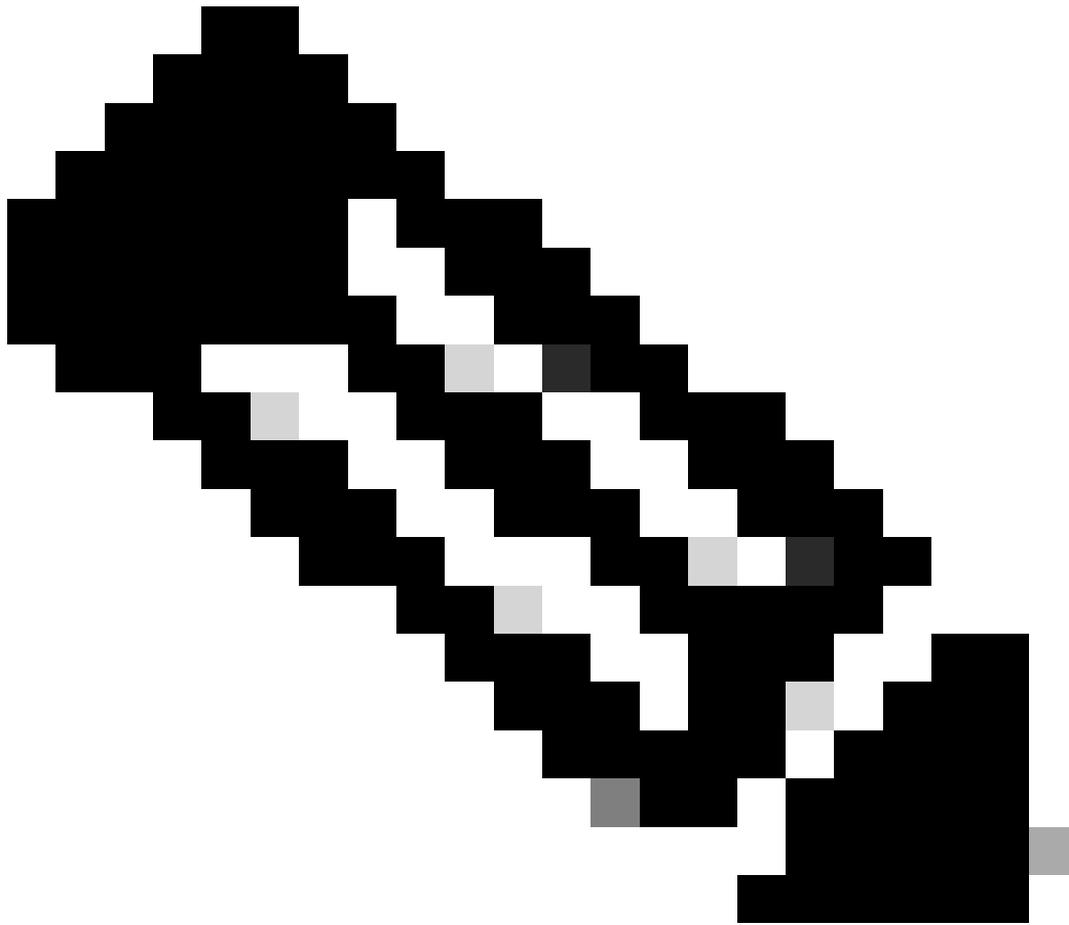
### Überprüfung

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.



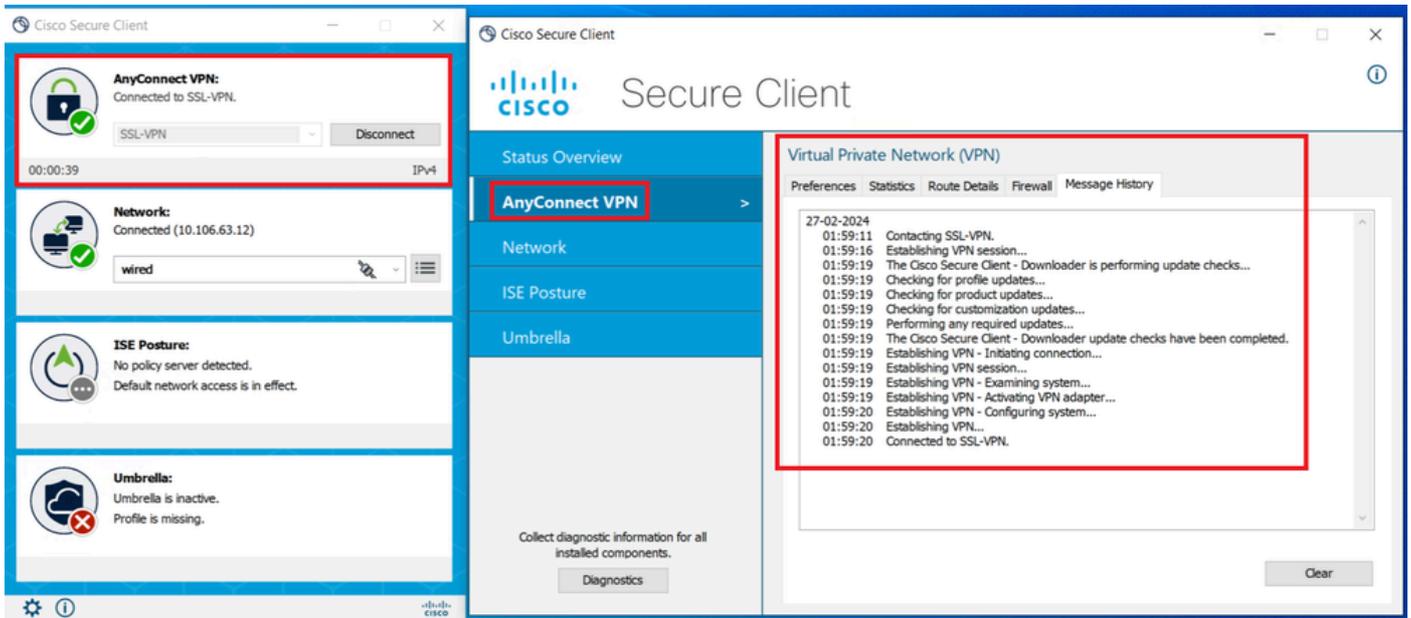
### Zertifikat-Highlights



**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.