

# Konfigurieren der Zertifikatuordnung für die sichere Client-Authentifizierung auf FTD über FDM

## Inhalt

---

### [Einleitung](#)

### [Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

### [Hintergrundinformationen](#)

### [Netzwerkdiagramm](#)

### [Konfigurationen](#)

#### [Konfiguration in FDM](#)

[Schritt 1: FTD-Schnittstelle konfigurieren](#)

[Schritt 2: Cisco Secure Client-Lizenz bestätigen](#)

[Schritt 3: Adresspool hinzufügen](#)

[Schritt 4: Sicheres Clientprofil erstellen](#)

[Schritt 5: Hochladen eines sicheren Client-Profiles an FDM](#)

[Schritt 6: Gruppenrichtlinie hinzufügen](#)

[Schritt 7: FTD-Zertifikat hinzufügen](#)

[Schritt 8: CA zu FTD hinzufügen](#)

[Schritt 9: VPN-Verbindungsprofil für Remote-Zugriff hinzufügen](#)

[Schritt 10: Zusammenfassung für Verbindungsprofil bestätigen](#)

#### [In FTD-CLI bestätigen](#)

#### [Bestätigung in VPN-Client](#)

[Schritt 1: Kopieren des sicheren Clientprofils auf den VPN-Client](#)

[Schritt 2: Clientzertifikat bestätigen](#)

[Schritt 3: Zertifizierungsstelle bestätigen](#)

### [Überprüfung](#)

[Schritt 1: VPN-Verbindung initiieren](#)

[Schritt 2: VPN-Sitzungen in FTD CLI bestätigen](#)

### [Fehlerbehebung](#)

### [Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie der Cisco Secure Client mit SSL auf FTD über FDM mithilfe der Zertifikatuordnung für die Authentifizierung eingerichtet wird.

## Voraussetzungen

## Anforderungen

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

- Cisco FirePOWER Gerätemanager (FDM) - virtuell
- Firewall Threat Defense (FTD) - virtuell
- VPN-Authentifizierungsablauf

## Verwendete Komponenten

- Cisco FirePOWER Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8
  
- Cisco Secure Client 5.1.4.74
- Profil-Editor (Windows) 5.1.4.74

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

CertificateMatch ist eine Funktion, mit der Administratoren Kriterien konfigurieren können, die der Client verwenden muss, um ein Clientzertifikat für die Authentifizierung mit dem VPN-Server auszuwählen. Diese Konfiguration wird im Clientprofil angegeben. Dabei handelt es sich um eine XML-Datei, die mit dem Profil-Editor verwaltet oder manuell bearbeitet werden kann. Die CertificateMatch-Funktion kann verwendet werden, um die Sicherheit von VPN-Verbindungen zu verbessern, indem sichergestellt wird, dass nur ein Zertifikat mit spezifischen Attributen für die VPN-Verbindung verwendet wird.

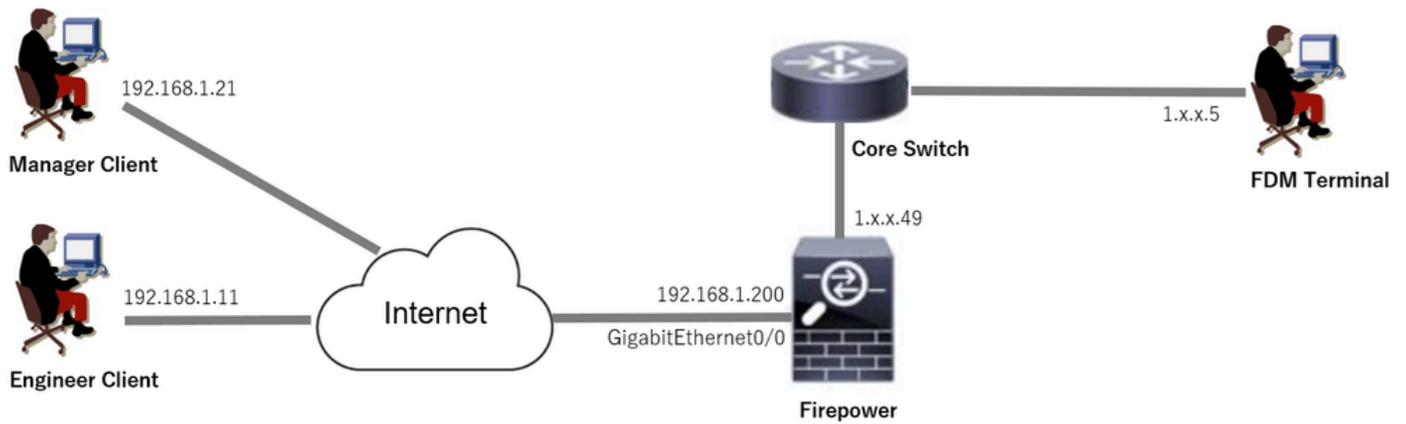
In diesem Dokument wird beschrieben, wie der Cisco Secure Client mithilfe des allgemeinen Namens eines SSL-Zertifikats authentifiziert wird.

Diese Zertifikate enthalten einen gemeinsamen Namen, der für Autorisierungszwecke verwendet wird.

- CA: ftd-ra-ca-common-name
- Techniker-VPN-Client-Zertifikat: vpnEngineerClientCN
- Manager VPN Client-Zertifikat: vpnManagerClientCN
- Serverzertifikat: 192.168.1.200

## Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für das Beispiel dieses Dokuments verwendet wird.



Netzwerkdiagramm

## Konfigurationen

### Konfiguration in FDM

#### Schritt 1: FTD-Schnittstelle konfigurieren

Navigieren Sie zu Device > Interfaces > View All Interfaces (Gerät > Schnittstellen), konfigurieren Sie die interne und externe Schnittstelle für FTD auf der Registerkarte Interfaces (Schnittstellen).

Bei GigabitEthernet0/0

- Name: außen
- IP-Adresse: 192.168.1.200/24

Firewall Device Manager | Monitoring | Policies | Objects | Device: firepower

Device Summary  
Interfaces

Cisco Firepower Threat Defense for VMware

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7

MGMT  
CONSOLE

Interfaces | Virtual Tunnel Interfaces

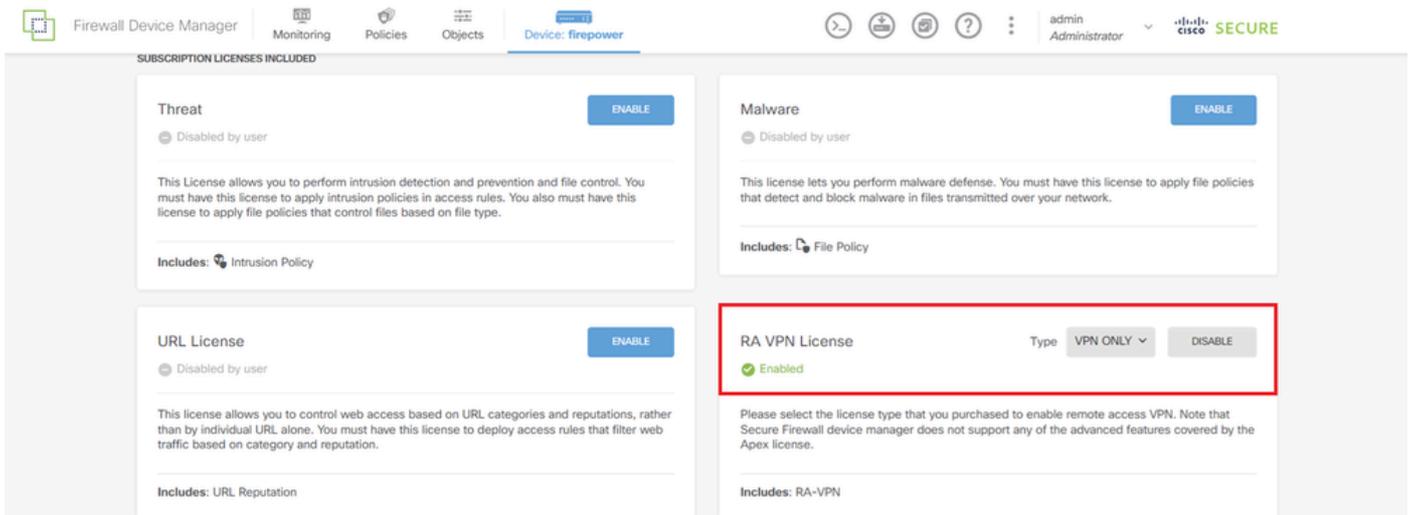
9 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ GigabitEthernet0/0	outside	Enabled	Routed	192.168.1.200		Enabled	

FTD-Schnittstelle

#### Schritt 2: Cisco Secure Client-Lizenz bestätigen

Navigieren Sie zu Device > Smart License > View Configuration, und bestätigen Sie den Artikel Cisco Secure Client License in RA VPN License.



Secure Client-Lizenz

### Schritt 3: Adresspool hinzufügen

Navigieren Sie zu Objekte > Netzwerke, und klicken Sie auf + Schaltfläche.



Adresspool hinzufügen

Geben Sie die erforderlichen Informationen ein, um einen neuen IPv4-Adresspool hinzuzufügen. Klicken Sie auf die Schaltfläche OK.

- Name: ftd-cert-match-pool
- Typ: Bereich
- IP-Bereich: 172.16.1.150-172.16.1.160

## Add Network Object



Name

ftd-cert-match-pool

Description

Type



Network



Host



FQDN



Range

IP Range

172.16.1.150-172.16.1.160

*e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100*

CANCEL

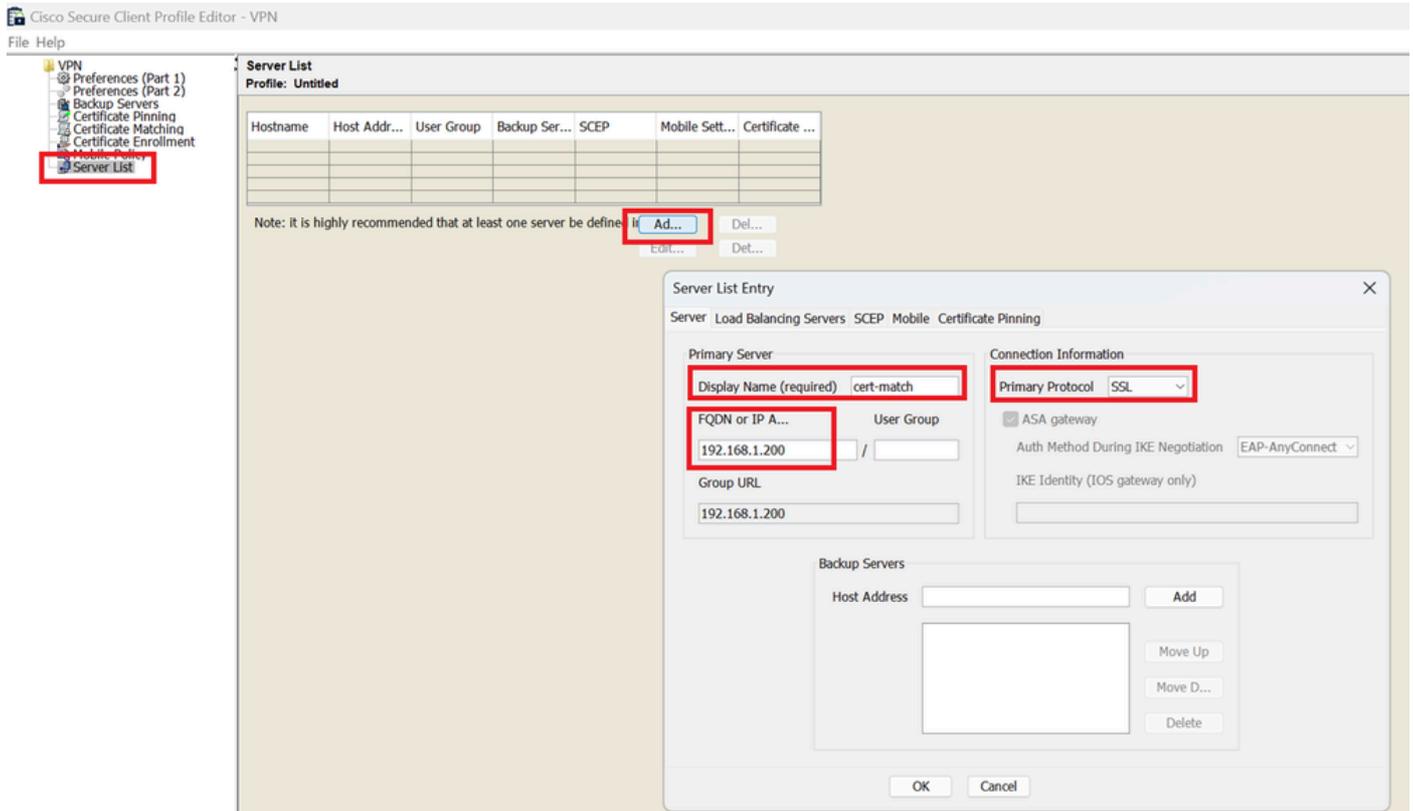
OK

Details zum IPv4-Adresspool

### Schritt 4: Sicheres Clientprofil erstellen

Laden Sie den Secure Client Profile Editor von der [Cisco Software](#)-Website herunter, und installieren Sie ihn. Navigieren Sie zur Serverliste, und klicken Sie auf die Schaltfläche Hinzufügen. Geben Sie die erforderlichen Informationen ein, um einen Server-Listeneintrag hinzuzufügen, und klicken Sie auf die Schaltfläche OK.

- Anzeigenname: Zertifikatübereinstimmung
- FQDN oder IP-Adresse: 192.168.1.200
- Primäres Protokoll: SSL



Server-Listeneintrag

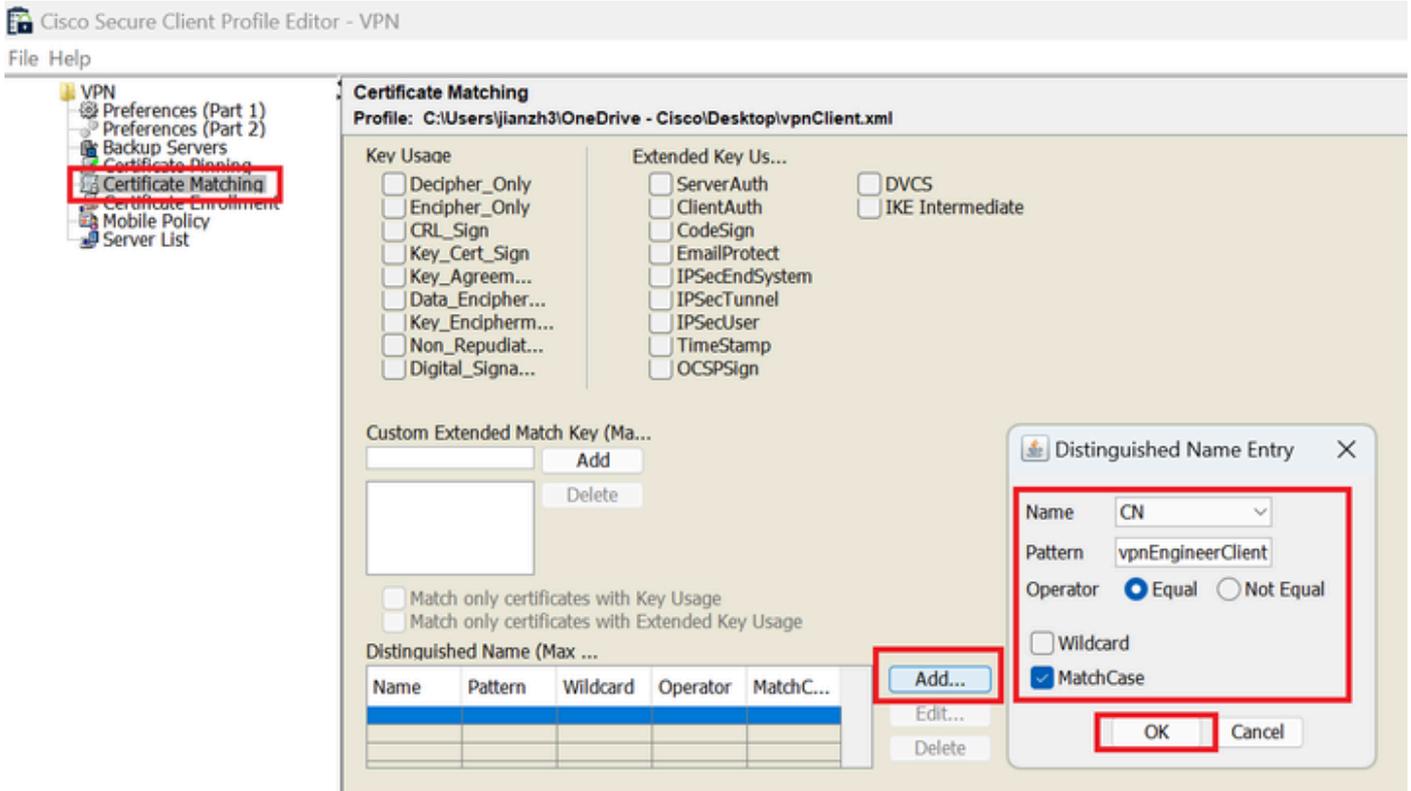
Navigieren Sie zu Zertifikatzuordnung, und klicken Sie auf die Schaltfläche Hinzufügen. Geben Sie die erforderlichen Informationen ein, um einen Distinguished Name Entry hinzuzufügen, und klicken Sie auf die Schaltfläche OK.

- Name: KN
- Muster: vpnEngineerClientCN
- Operator: Gleich



Hinweis: Aktivieren Sie in diesem Dokument die Option MatchCase.

---



Distinguished Name-Eintrag

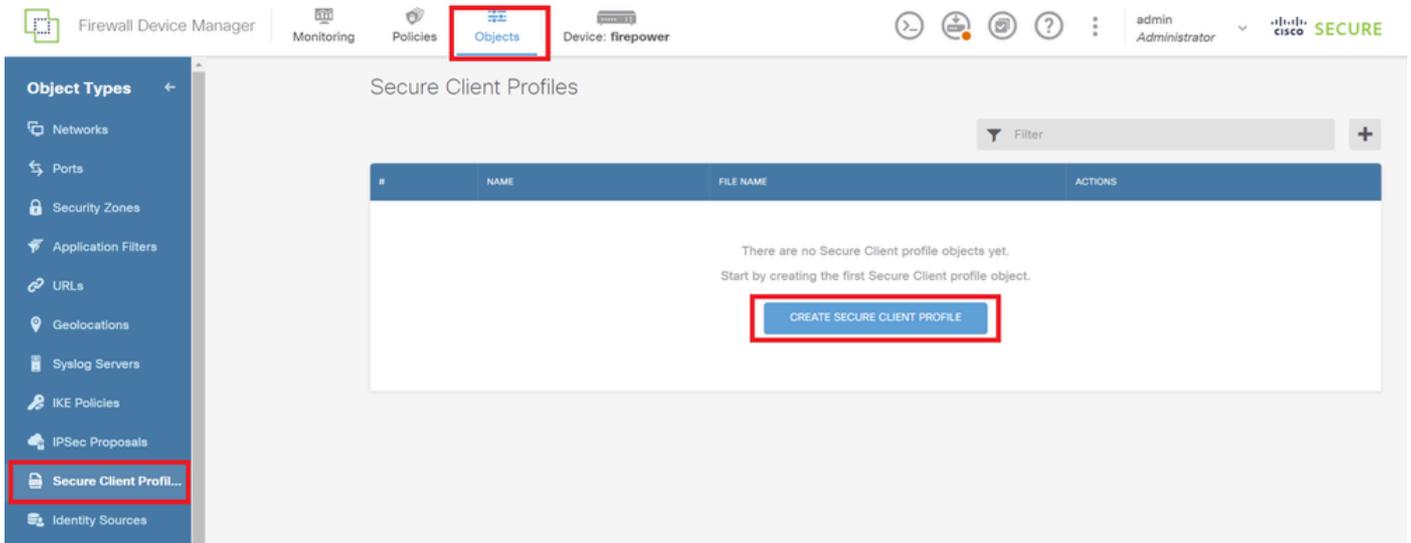
Speichern Sie das sichere Clientprofil auf dem lokalen Computer, und bestätigen Sie die Profildetails.



Sicheres Client-Profil

Schritt 5: Hochladen eines sicheren Client-Profiles an FDM

Navigieren Sie zu Objekte > Secure Client Profile, und klicken Sie auf CREATE SECURE CLIENT PROFILE (SICHERES CLIENT-PROFIL ERSTELLEN).



Sicheres Clientprofil erstellen

Geben Sie die erforderlichen Informationen ein, um ein sicheres Clientprofil hinzuzufügen, und klicken Sie auf die Schaltfläche OK.

- Name: secureClientProfile
- Sicheres Clientprofil: secureClientProfile.xml (Hochladen vom lokalen Computer)

## Add Secure Client Profile

Name

secureClientProfile

Description

Secure Client Profile

UPLOAD secureClientProfile.xml

CANCEL OK

Sicheres Clientprofil hinzufügen

## Schritt 6: Gruppenrichtlinie hinzufügen

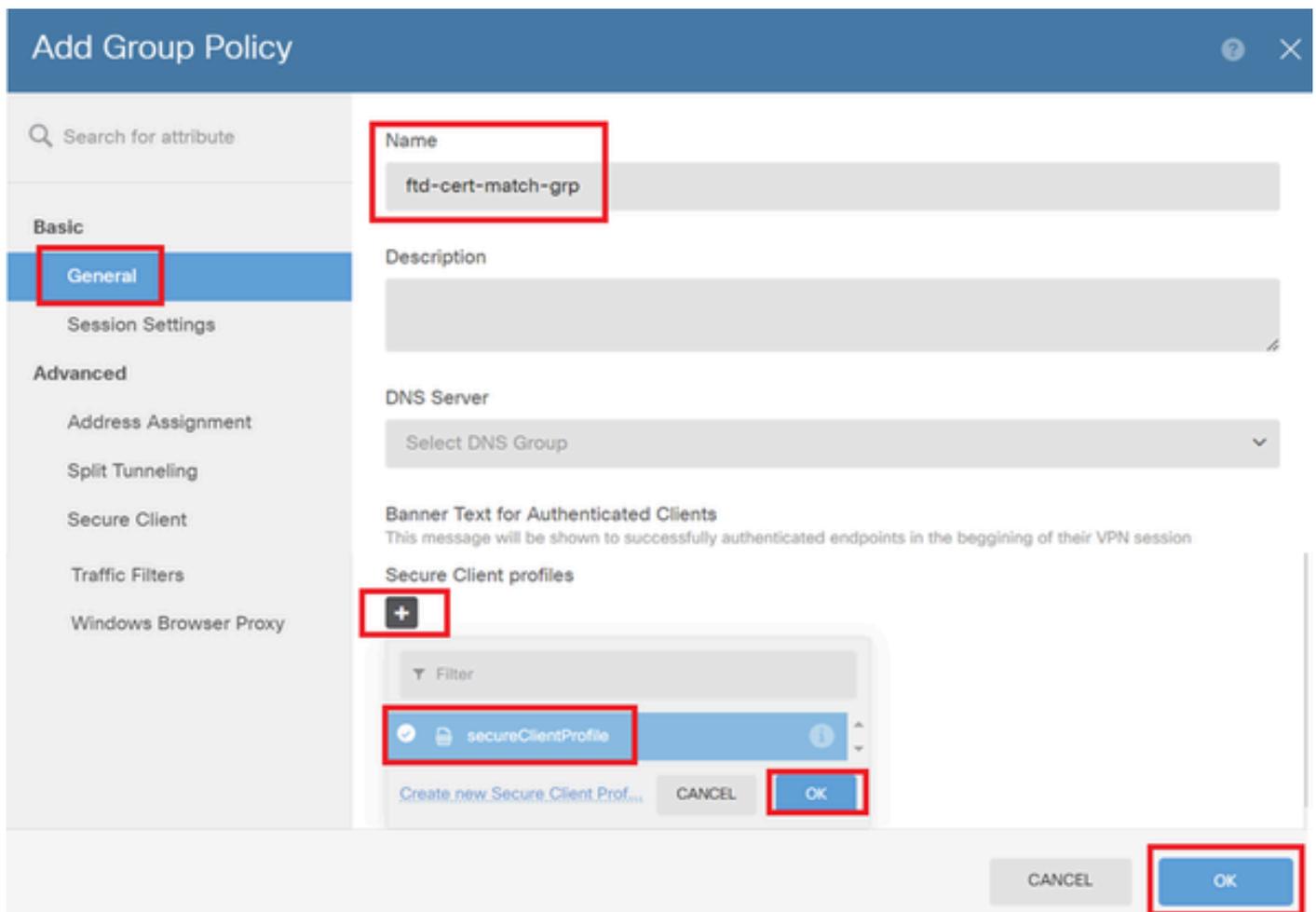
Navigieren Sie zu Gerät > Remotezugriff-VPN > Konfiguration anzeigen > Gruppenrichtlinien, und klicken Sie auf +.



Gruppenrichtlinie hinzufügen

Geben Sie die erforderlichen Informationen ein, um eine Gruppenrichtlinie hinzuzufügen, und klicken Sie auf die Schaltfläche OK.

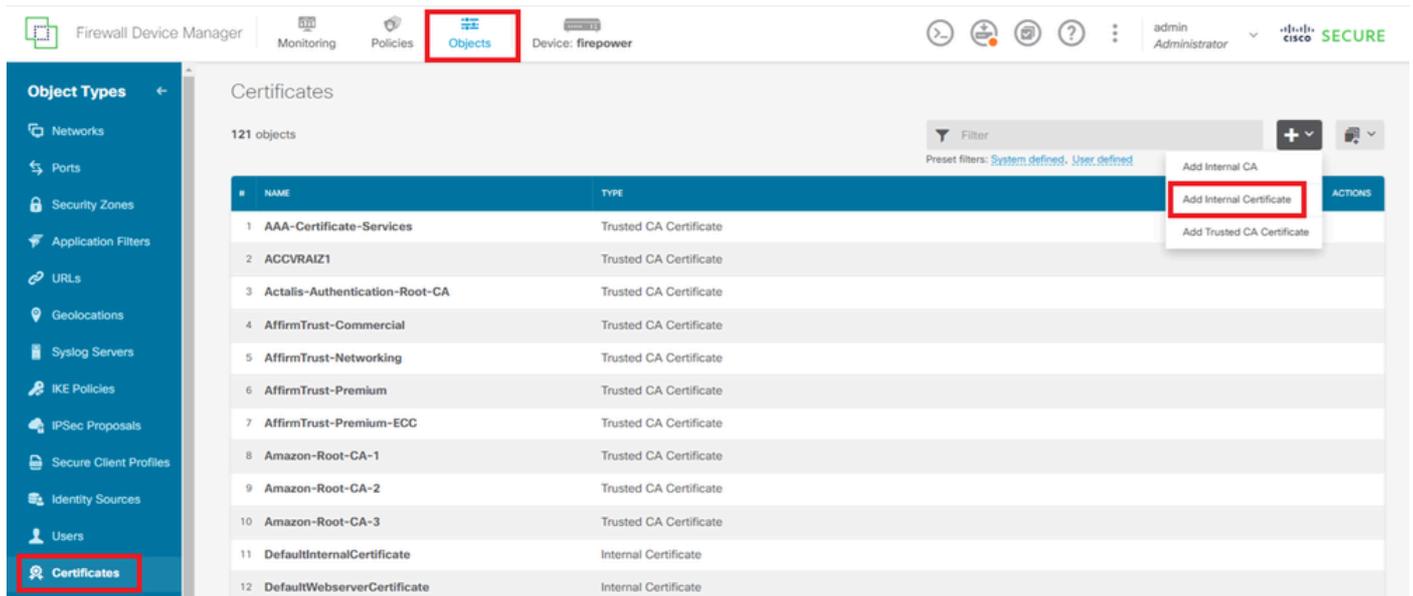
- Name: ftd-cert-match-grp
- Profile für sichere Clients: secureClientProfile



Details zur Gruppenrichtlinie

## Schritt 7. FTD-Zertifikat hinzufügen

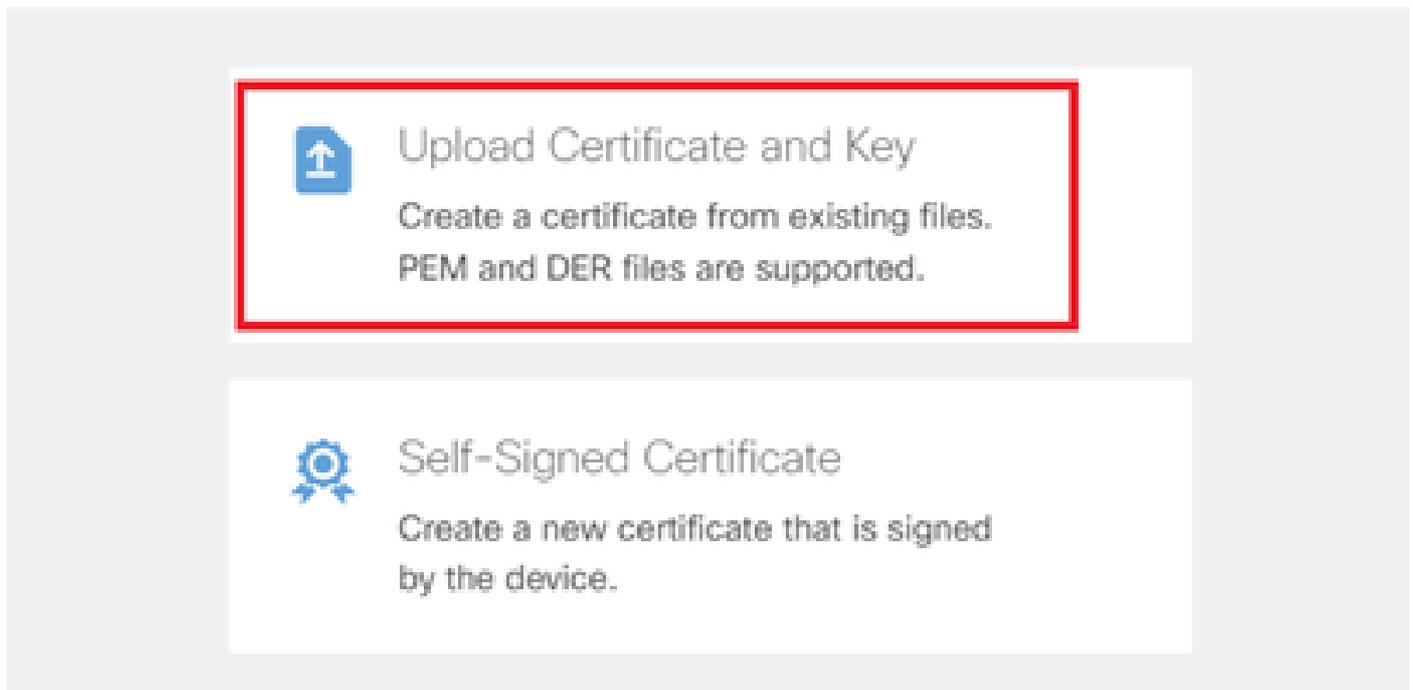
Navigieren Sie zu Objekte > Zertifikate, und klicken Sie auf Internes Zertifikat hinzufügen aus + Element.



Internes Zertifikat hinzufügen

Klicken Sie auf Zertifikat und Schlüssel hochladen.

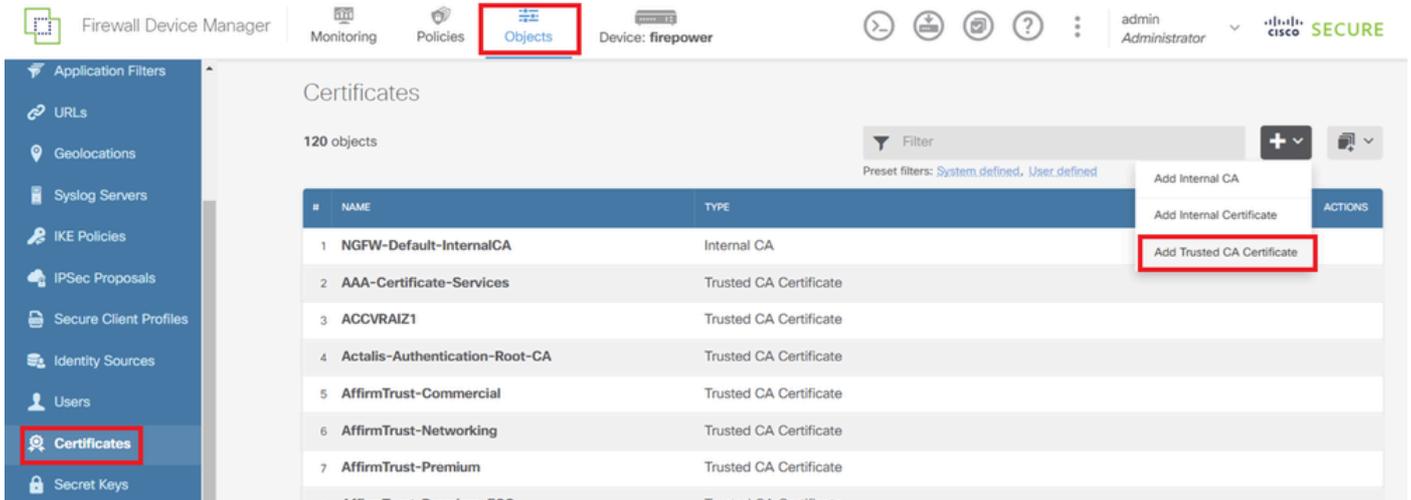
Choose the type of internal certificate you want to create



Zertifikat und Schlüssel hochladen

Geben Sie die erforderlichen Informationen für das FTD-Zertifikat ein, importieren Sie ein Zertifikat und einen Zertifikatschlüssel vom lokalen Computer, und klicken Sie dann auf die Schaltfläche





Vertrauenswürdigen Zertifizierungsstellenzertifikat hinzufügen

Geben Sie die erforderlichen Informationen für die Zertifizierungsstelle ein, und importieren Sie ein Zertifikat vom lokalen Computer.

- Name: ftdvpn-ca-cert
- Validierung und Verwendung für spezielle Services: SSL-Client

# Add Trusted CA Certificate



Name

ftdvpn-ca-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

ftd-ra-ca.crt

Upload Certificate

```
-----BEGIN CERTIFICATE-----
MIIDbDCCA1SgAwIBAgIIUkKgLG229/0wDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE
BHMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUub2t5bzEOMAwGA1UEChMF
O31vMQ4wDAYDVQQDEwTBVRva31vMQ4wDAYDVRQDEwVUub2t5bzEOMAwGA1UEChMF
-----
```

Skip CA Certificate Check

Validation Usage for Special Services

SSL Client

CANCEL

OK

Details zum vertrauenswürdigen Zertifizierungsstellenzertifikat

## Schritt 9. VPN-Verbindungsprofil für Remote-Zugriff hinzufügen

Navigieren Sie zu Gerät > Remotezugriff-VPN > Konfiguration anzeigen > Verbindungsprofile, und klicken Sie auf die Schaltfläche VERBINDUNGSPROFIL ERSTELLEN.

Firewall Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator | cisco SECURE

RA VPN

Connection Profiles

Group Policies

SAML Server

Device Summary

Remote Access VPN Connection Profiles

#	NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.				

CREATE CONNECTION PROFILE

VPN-Verbindungsprofil für Remote-Zugriff hinzufügen

Geben Sie die erforderlichen Informationen für das Verbindungsprofil ein, und klicken Sie auf die

Schaltfläche Weiter.

- Name des Verbindungsprofils: ftd-cert-match-vpn
- Authentifizierungstyp: Nur Client-Zertifikat
- Benutzername vom Zertifikat: Zuordnungsspezifisches Feld
- Primärfeld: CN (Common Name)
- Sekundäres Feld: OU (Organisationseinheit)
- IPv4-Adresspools: ftd-cert-match-pool

Firewall Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator | CISCO SECURE

Remote Access VPN | 1 Connection and Client Configuration | 2 Remote User Experience | 3 Global Settings | 4 Summary

Remote Users | Secure Clients | Internet | Client Certificate | FIREPOWER | OUTSIDE INTERFACE | INSIDE INTERFACES | Corporate Resources | Identity Source for User Authentication

### Connection and Client Configuration

Specify how to authenticate remote users and the secure clients they can use to connect to the inside network.

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

ftd-cert-match-vpn

Group Alias (one per line, up to 5) | Group URL (one per line, up to 5)

ftd-cert-match-vpn

Primary Identity Source

Authentication Type  
Client Certificate Only

Username from Certificate

Map Specific Field

Primary Field | Secondary Field

CN (Common Name) | OU (Organisational Unit)

Use entire DN (distinguished name) as username

Advanced

Authorization Server | Accounting Server

Please select | Please select

Client Address Pool Assignment

IPv4 Address Pool | IPv6 Address Pool

Endpoints are provided an address from this pool | Endpoints are provided an address from this pool

ftd-cert-match-pool

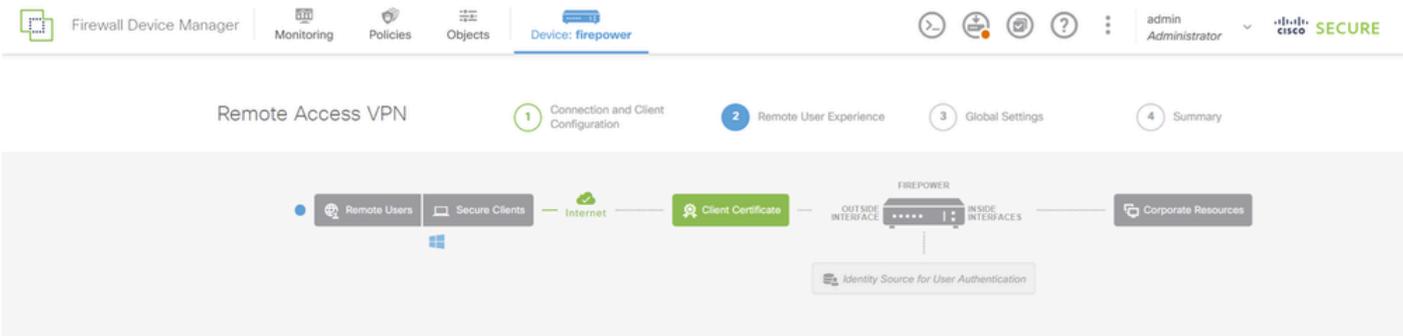
DHCP Servers

CANCEL | NEXT

Details zum VPN-Verbindungsprofil

Geben Sie die erforderlichen Informationen für die Gruppenrichtlinie ein, und klicken Sie auf die Schaltfläche Weiter.

- Gruppenrichtlinie anzeigen: ftd-cert-match-grp



### Remote User Experience

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.

View Group Policy

ftd-cert-match-grp

Policy Group Brief Details

DNS + BANNER Edit

DNS Server None

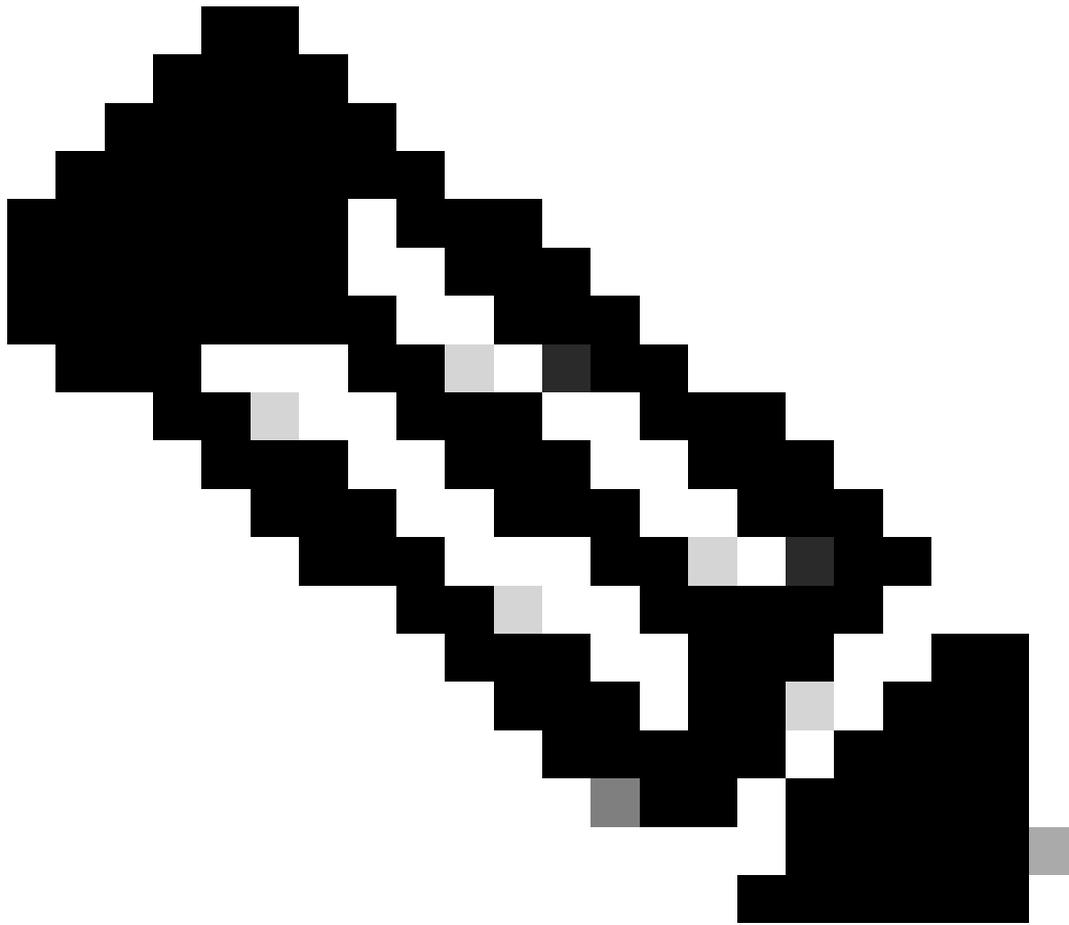
Banner Text for Authentication

BACK NEXT

Gruppenrichtlinie auswählen

Wählen Sie Certificate of Device Identity, Outside Interface, Secure Client Package für die VPN-Verbindung aus.

- Zertifikat für die Geräteidentität: ftd-vpn-cert
- Externe Schnittstelle: außen (GigabitEthernet0/0)
- Secure Client-Paket: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



Hinweis: Deaktivieren der Funktion zum Ausschließen von NAT in diesem Dokument.

---



### Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

**Certificate of Device Identity**  
ftd-vpn-cert (Validation Usage: SSL Se...)

**Outside Interface**  
outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface  
Port  
443  
e.g. ravn.example.com e.g. 8080

**Access Control for VPN Traffic**  
Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic.  
 Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

**NAT Exempt**

**Secure Client Package**  
If a user does not already have the right secure client package installed, the system will launch the secure client installer when the client authenticates for the first time. The user can then install the package from the system.  
You can download secure client packages from [software.cisco.com](https://software.cisco.com).  
You must have the necessary secure client software license.

**Packages**  
UPLOAD PACKAGE  
Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK NEXT

Details der globalen Einstellungen

## Schritt 10. Zusammenfassung für Verbindungsprofil bestätigen

Bestätigen Sie die für die VPN-Verbindung eingegebenen Informationen, und klicken Sie auf die Schaltfläche FERTIG stellen.

^ Summary

Review the summary of the Remote Access VPN configuration.

**Ftd-Cert-Match-Vpn**

**STEP 1: CONNECTION AND CLIENT CONFIGURATION**

Primary Identity Source

Authentication Type: Client Certificate Only

Primary Identity Source: -

Fallback Local Identity Source: -

Username from Certificate: Map Specific Field

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Advanced

Authorization Server

Accounting Server

Client Address Pool Assignment

IPv4 Address Pool: ftd-cert-match-pool

IPv6 Address Pool: -

DHCP Servers: -

**STEP 2: GROUP POLICY**

Group Policy Name: ftd-cert-match-grp

Banner + DNS Server

DNS Server: -

Banner text for authenticated clients: -

Session Settings

Maximum Connection Time / Alert Interval: Unlimited / 1 minutes

Idle Timeout / Alert Interval: 30 / 1 minutes

Simultaneous Login per User: 3

Split Tunneling

IPv4 Split Tunneling: Allow all traffic over tunnel

IPv6 Split Tunneling: Allow all traffic over tunnel

Secure Client

Secure Client Profiles: secureClientProfile

**STEP 3: GLOBAL SETTINGS**

Certificate of Device Identity: ftd-vpn-cert

Outside Interface: GigabitEthernet0/0 (outside)

Fully-qualified Domain Name for the Outside Interface: -

Port: 443

Access Control for VPN Traffic: No

NAT Exempt

NAT Exempt: No

Inside Interfaces: -

Inside Networks: -

Secure Client Package

Packages: Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK FINISH

Zusammenfassung für Verbindungsprofil bestätigen

### In FTD-CLI bestätigen

Bestätigen Sie die VPN-Verbindungseinstellungen in der FTD-CLI nach der Bereitstellung vom FDM.

```
// Defines IP of interface
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftd-vpn-cert
enrollment terminal
keypair ftd-vpn-cert
crl configure

// Server Certificate
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client
crl configure

// CA
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect profiles secureClientProfile disk0:/anyconnprofs/secureClientProfile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable
```

```
// Configures the group-policy to allow SSL connections
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles value secureClientProfile type user
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting
```

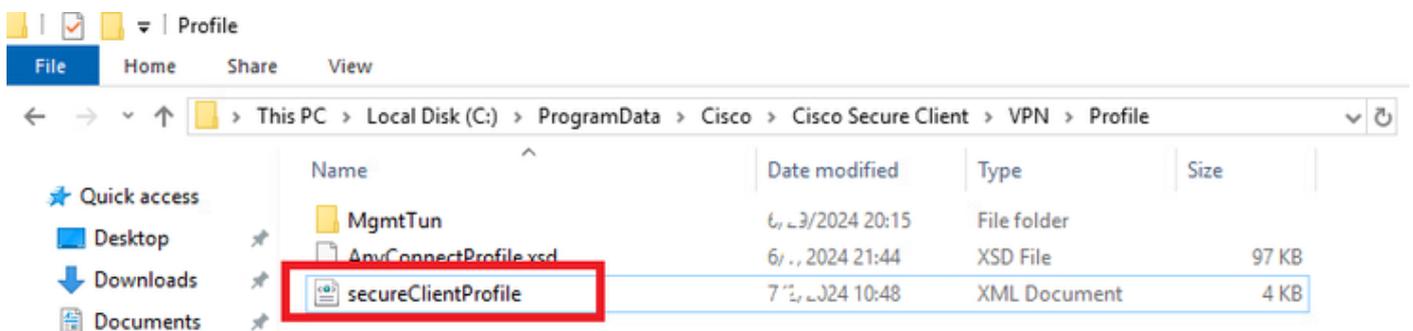
```
// Configures the tunnel-group to use the certificate authentication
tunnel-group ftd-cert-match-vpn type remote-access
tunnel-group ftd-cert-match-vpn general-attributes
address-pool ftd-cert-match-pool
default-group-policy ftd-cert-match-grp
tunnel-group ftd-cert-match-vpn webvpn-attributes
authentication certificate
group-alias ftd-cert-match-vpn enable
```

## Bestätigung in VPN-Client

Schritt 1: Kopieren des sicheren Clientprofils auf den VPN-Client

Kopieren Sie ein sicheres Client-Profil in einen technischen VPN-Client und einen Manager-VPN-Client.

Hinweis: Verzeichnis des sicheren Clientprofils auf dem Windows-Computer:  
C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



Kopieren des sicheren Clientprofils auf den VPN-Client

## Schritt 2: Clientzertifikat bestätigen

Navigieren Sie im VPN-Client des Technikers zu Certificates - Current User > Personal > Certificates (Zertifikate - Aktueller Benutzer > Persönlich), und überprüfen Sie das Client-Zertifikat,

das für die Authentifizierung verwendet wird.



Zertifikat für Techniker-VPN-Client bestätigen

Doppelklicken Sie auf das Client-Zertifikat, navigieren Sie zu Details, überprüfen Sie die Details des Betreffs.

- Betreff: CN = vpnEngineerClientCN

# Certificate



General Details Certification Path

Show: <All>

Field	Value
Valid to	Wednesday, June 18, 2025 5:...
Subject	vpnEngineerClientCN, vpnEngl...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Comment	xca certificate
Thumbprint algorithm	sha1

CN = vpnEngineerClientCN

O = Cisco  
L = Tokyo  
S = Tokyo  
C = JP

Edit Properties...

Copy to File...

OK

Details zum Techniker-Client-Zertifikat

Navigieren Sie im VPN-Client des Managers zu Certificates - Current User > Personal > Certificates, und überprüfen Sie das Client-Zertifikat, das für die Authentifizierung verwendet wird.



Zertifikat für Manager VPN Client bestätigen

Doppelklicken Sie auf das Client-Zertifikat, navigieren Sie zu Details, überprüfen Sie die Details des Betreffs.

- Betreff: CN = vpnManagerClientCN

# Certificate



General Details Certification Path

Show: <All>

Field	Value
Issued	Thursday, June 19, 2025 9:41...
Subject	vpnManagerClientCN, vpnMan...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Comment	xca certificate
Thumbprint algorithm	sha1

CN = vpnManagerClientCN

O = Cisco  
L = Tokyo  
S = Tokyo  
C = JP

Edit Properties...

Copy to File...

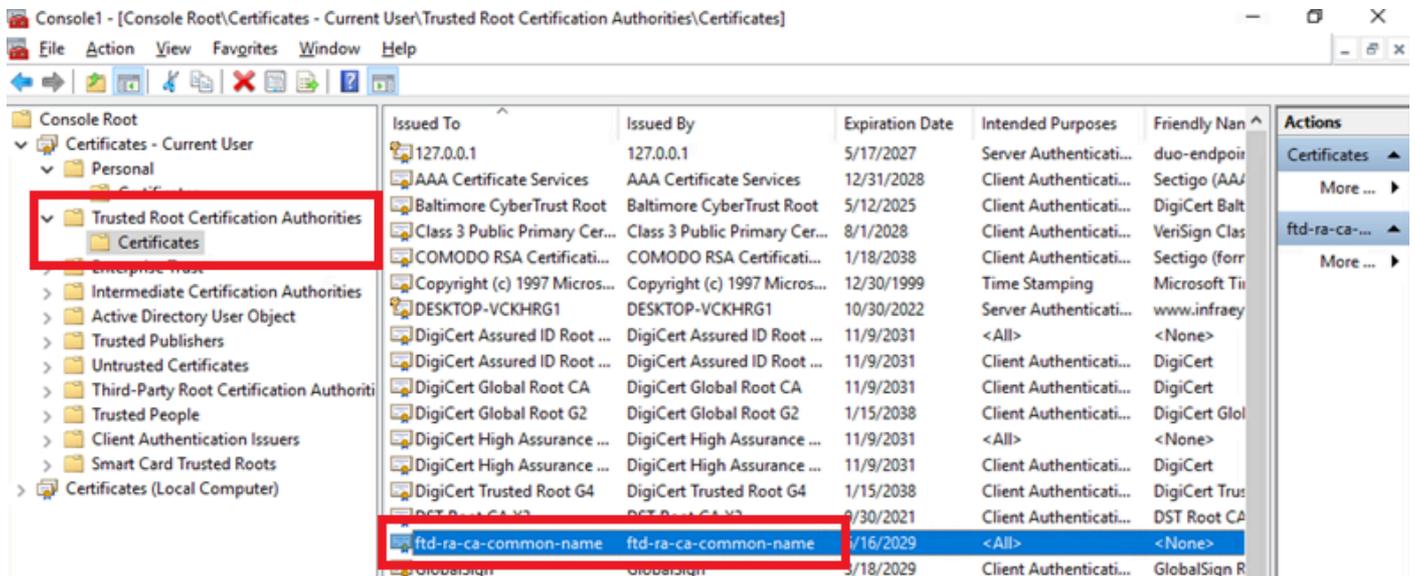
OK

Details zum Manager-Clientzertifikat

Schritt 3: Zertifizierungsstelle bestätigen

Navigieren Sie im VPN-Client des Technikers und im VPN-Client des Managers zu Certificates - Current User > Trusted Root Certification Authorities > Certificates, und überprüfen Sie die für die Authentifizierung verwendete Zertifizierungsstelle.

- Ausgestellt von: ftd-ra-ca-common-name

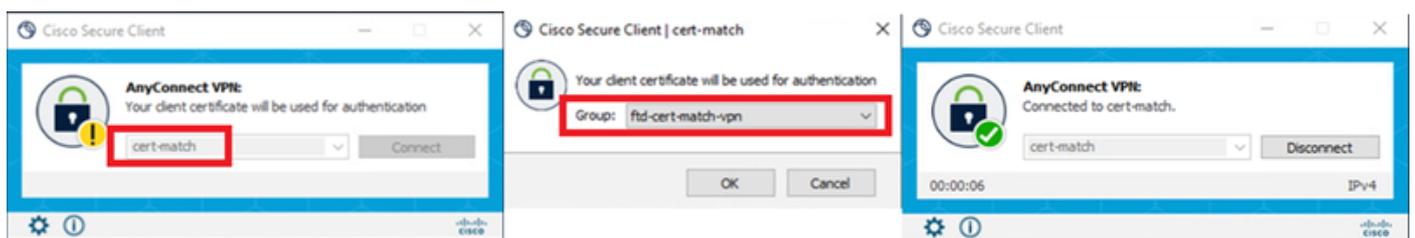


Zertifizierungsstelle bestätigen

## Überprüfung

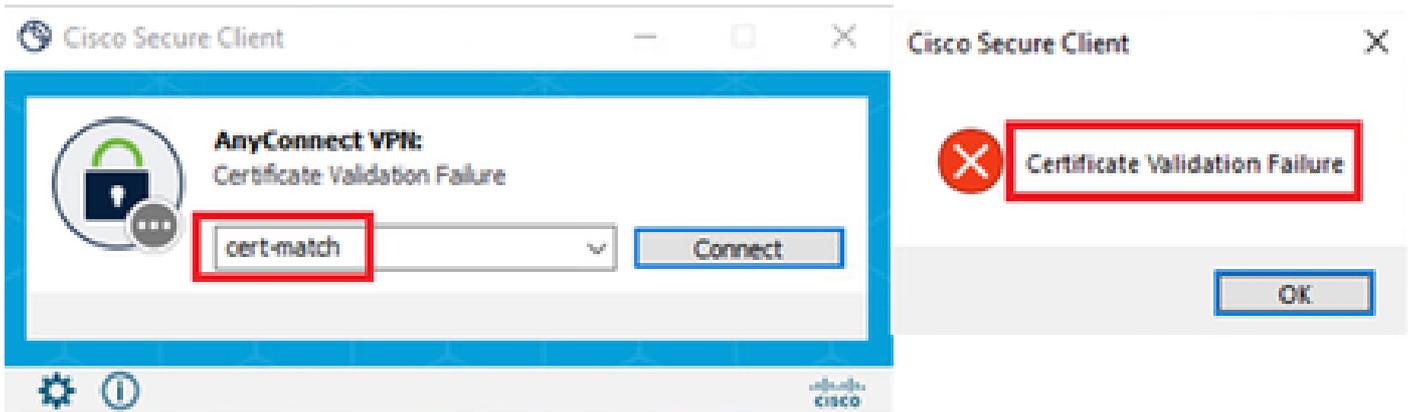
Schritt 1: VPN-Verbindung initiieren

Initiieren Sie im Techniker-VPN-Client die Verbindung zum Cisco Secure Client. Der Benutzername und das Kennwort müssen nicht eingegeben werden, da die VPN-Verbindung erfolgreich hergestellt wurde.



VPN-Verbindung für Techniker-VPN-Client erfolgreich

Initiieren Sie im Manager-VPN-Client die Verbindung mit dem Cisco Secure Client. Die Verbindung mit dem VPN ist aufgrund eines Fehlers bei der Zertifikatsvalidierung fehlgeschlagen.



Fehler bei der VPN-Verbindung für Manager VPN-Client

## Schritt 2: VPN-Sitzungen in FTD CLI bestätigen

Führen Sie in der FTD (Lina) CLI den Befehl `show vpn-sessiondb detail anyconnect`, um die VPN-Sitzungen des Technikers zu bestätigen.

```
firepower# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username : vpnEngineerClientCN Index : 32
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx : 14718 Bytes Rx : 12919
Pkts Tx : 2 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn
Login Time : 05:42:03 UTC Tue Jul 2 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0000000000200006683932b
Security Grp : none Tunnel Zone : 0
```

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

AnyConnect-Parent:

```
Tunnel ID : 32.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50170 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
```

Bytes Tx : 7359 Bytes Rx : 0  
Pkts Tx : 1 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

#### SSL-Tunnel:

Tunnel ID : 32.2  
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384  
Encapsulation: TLSv1.2 TCP Src Port : 50177  
TCP Dst Port : 443 Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74  
Bytes Tx : 7359 Bytes Rx : 12919  
Pkts Tx : 1 Pkts Rx : 51  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

#### Fehlerbehebung

Informationen zur VPN-Authentifizierung finden Sie im Debug-Syslog des Lina-Moduls und in der DART-Datei auf dem Windows-Computer.

Dies ist ein Beispiel für Debug-Protokolle in der Lina-Engine während der VPN-Verbindung vom Engineering-Client.

```
Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN
Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN
Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN
Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 session
```

#### Zugehörige Informationen

[Konfiguration des FDM On-Box Management Service für FirePOWER 2100](#)

[Konfiguration eines Remote-Access-VPN auf einem von FDM verwalteten FTD](#)

[Konfiguration und Überprüfung des Syslog im FirePOWER Geräte-Manager](#)

## 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.