

Konfigurieren der Zertifikatzuordnung für sichere Client-Authentifizierung auf FTD über FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Konfiguration in FMC](#)

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

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

[Schritt 3: IPv4-Adresspool hinzufügen](#)

[Schritt 4: Gruppenrichtlinie hinzufügen](#)

[Schritt 5: FTD-Zertifikat hinzufügen](#)

[Schritt 6: Richtlinienzuweisung für Techniker-Verbindungsprofil hinzufügen](#)

[Schritt 7: Konfigurieren von Details für das Verbindungsprofil eines Technikers](#)

[Schritt 8: Konfigurieren von sicherem Client-Image für Techniker-Verbindungsprofil](#)

[Schritt 9: Konfigurieren des Zugriffs und des Zertifikats für das Techniker-Verbindungsprofil](#)

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

[Schritt 11: Hinzufügen eines Verbindungsprofils für den Manager-VPN-Client](#)

[Schritt 12: Zertifikatzuordnung hinzufügen](#)

[Schritt 13: Binden der Zertifikatzuordnung an das Verbindungsprofil](#)

[In FTD-CLI bestätigen](#)

[Bestätigung in VPN-Client](#)

[Schritt 1: Clientzertifikat bestätigen](#)

[Schritt 2: Zertifizierungsstelle bestätigen](#)

[Überprüfung](#)

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

[Schritt 2: Aktive Sitzungen in FMC bestätigen](#)

[Schritt 3: 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 FMC mithilfe der Zertifikatzuordnung für die Authentifizierung eingerichtet wird.

Voraussetzungen

Anforderungen

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

- Cisco FirePOWER Management Center (FMC)
- Firewall Threat Defense (FTD) - virtuell
- VPN-Authentifizierungsablauf

Verwendete Komponenten

- Cisco FirePOWER Management Center für VMware 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1

- Cisco Secure Client 5.1.3.62

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

Die Zertifikatszuordnung ist eine Methode, die in VPN-Verbindungen verwendet wird, bei denen ein Clientzertifikat einem lokalen Benutzerkonto zugeordnet wird oder Attribute innerhalb des Zertifikats für Autorisierungszwecke verwendet werden. Hierbei wird ein digitales Zertifikat als Mittel zur Identifizierung eines Benutzers oder Geräts verwendet. Durch die Verwendung der Zertifikatszuordnung wird das SSL-Protokoll zur Authentifizierung von Benutzern verwendet, ohne dass diese Anmeldeinformationen eingeben müssen.

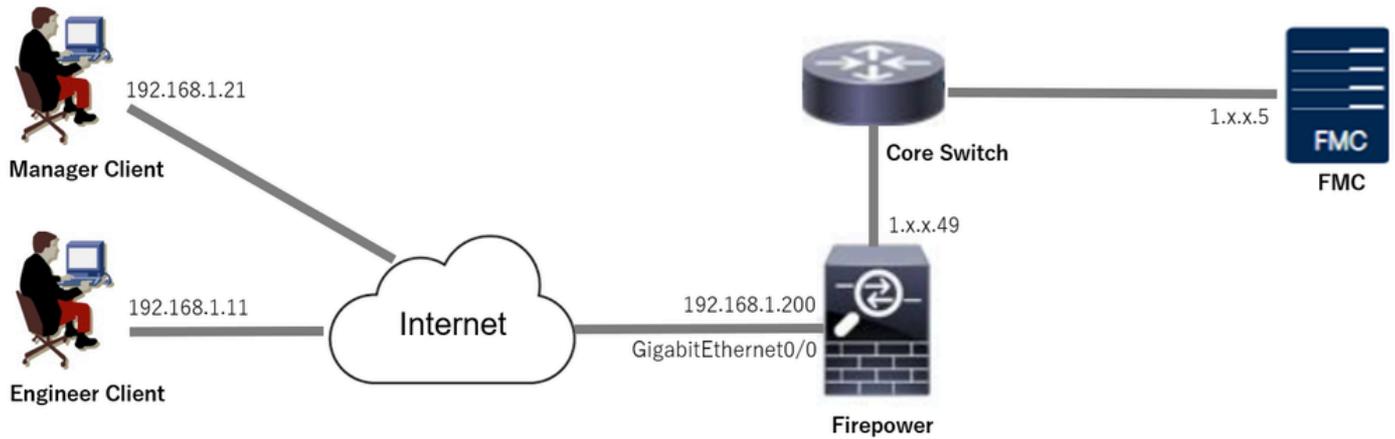
In diesem Dokument wird beschrieben, wie der Cisco Secure Client mithilfe des allgemeinen Namens eines SSL-Zertifikats authentifiziert wird.

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 FMC

Schritt 1: FTD-Schnittstelle konfigurieren

Navigieren Sie zu **Devices > Device Management**, bearbeiten Sie das FTD-Zielgerät, und konfigurieren Sie die externe Schnittstelle für FTD in **Interface** tab.

Bei **GigabitEthernet0/0**

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

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒 **SECURE**

1.1.1.1.49 Save Cancel

Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

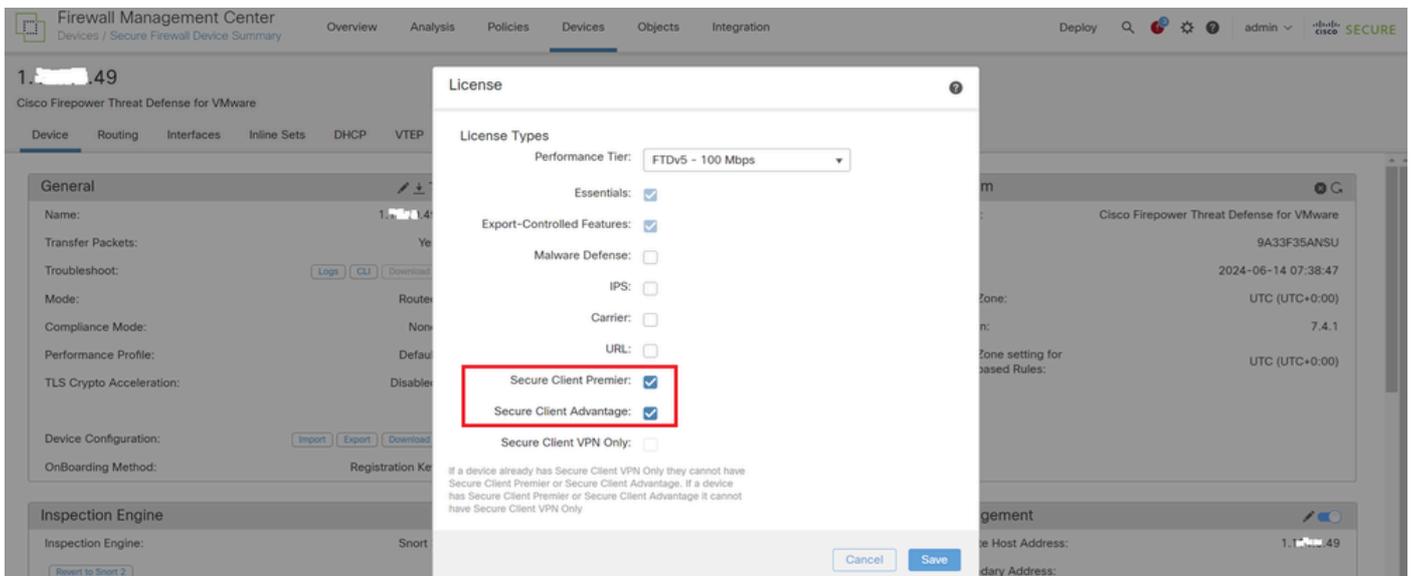
All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical	outsideZone		192.168.1.200/24(Static)	Disabled	Global

FTD-Schnittstelle

Schritt 2: Cisco Secure Client-Lizenz bestätigen

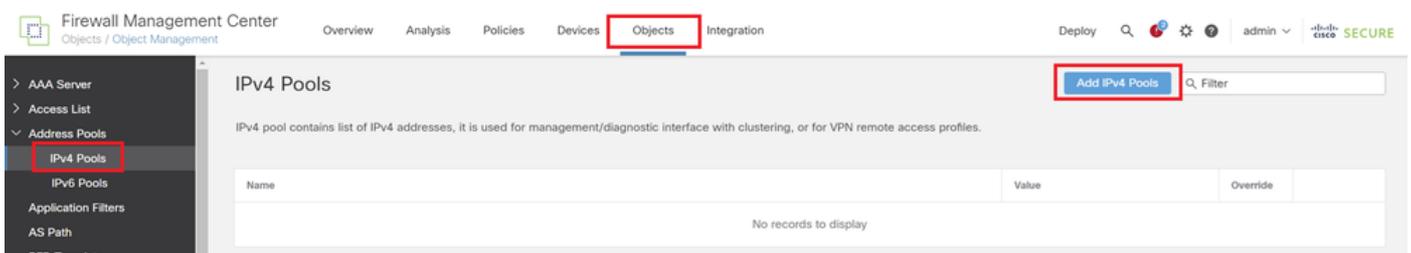
Navigieren Sie zu **Geräte > Geräteverwaltung**, bearbeiten Sie das FTD-Zielgerät, und bestätigen Sie die Cisco Secure Client-Lizenz auf der Registerkarte **Gerät**.



Secure Client-Lizenz

Schritt 3: IPv4-Adresspool hinzufügen

Navigieren Sie zu **Object > Object Management > Address Pools > IPv4 Pools**, und klicken Sie auf **Add IPv4 Pools** (IPv4-Pools hinzufügen).



IPv4-Adresspool hinzufügen

Geben Sie die erforderlichen Informationen ein, um einen IPv4-Adresspool für den VPN-Client des Technikers zu erstellen.

- Name: ftd-vpn-engineer-pool
- IPv4-Adressbereich: 172.16.1.100-172.16.1.110
- Maske: 255.255.255.0

Edit IPv4 Pool



Name*
ftd-vpn-engineer-pool

Description

IPv4 Address Range*
172.16.1.100-172.16.1.110

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-Adresspool für Techniker-VPN-Client

Geben Sie die erforderlichen Informationen ein, um einen IPv4-Adresspool für den Manager-VPN-Client zu erstellen.

- Name: ftd-vpn-manager-pool
- IPv4-Adressbereich: 172.16.1.120-172.16.1.130
- Maske: 255.255.255.0

Add IPv4 Pool



Name*
ftd-vpn-manager-pool

Description

IPv4 Address Range*
172.16.1.120-172.16.1.130

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-Adresspool für Manager-VPN-Client

Bestätigen Sie die neuen IPv4-Adresspools.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ ? admin | **SECURE**

IPv4 Pools Add IPv4 Pools 🔍 Filter

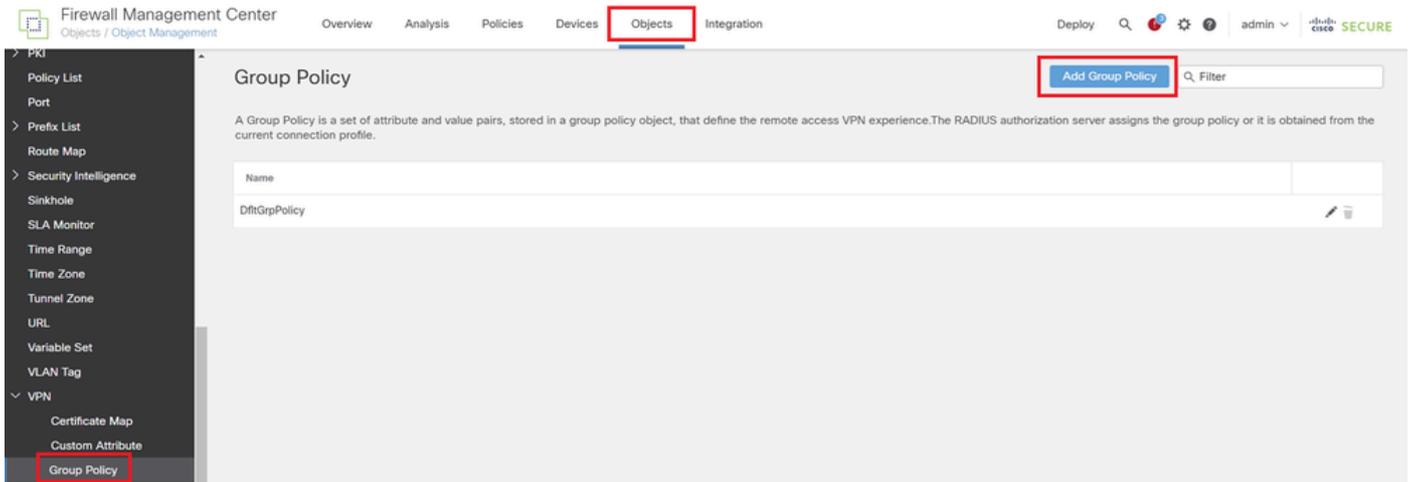
IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.

Name	Value	Override	
ftd-vpn-engineer-pool	172.16.1.100-172.16.1.110	●	✎ 🗑
ftd-vpn-manager-pool	172.16.1.120-172.16.1.130	●	✎ 🗑

Neue IPv4-Adresspools

Schritt 4: Gruppenrichtlinie hinzufügen

Navigieren Sie zu **Object > Object Management > VPN > Group Policy**, und klicken Sie auf **Add Group Policy** (Gruppenrichtlinie hinzufügen).



Gruppenrichtlinie hinzufügen

Geben Sie die erforderlichen Informationen ein, um eine Gruppenrichtlinie für den Techniker-VPN-Client zu erstellen.

- Name: ftd-vpn-engineer-grp
- VPN-Protokolle: SSL

Add Group Policy

Name:*

ftd-vpn-engineer-grp

Description:

General Secure Client Advanced

VPN Protocols

VPN Tunnel Protocol:
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Gruppenrichtlinie für Techniker-VPN-Client

Geben Sie die erforderlichen Informationen ein, um eine Gruppenrichtlinie für den Manager-VPN-Client zu erstellen.

- Name: ftd-vpn-manager-grp
- VPN-Protokolle: SSL

Add Group Policy



Name:*

ftd-vpn-manager-grp

Description:

General Secure Client Advanced

VPN Protocols

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Gruppenrichtlinie für Manager-VPN-Client

Die neuen Gruppenrichtlinien bestätigen.

Firewall Management Center

Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒

PKI

Policy List

Port

Prefix List

Route Map

Security Intelligence

Sinkhole

SLA Monitor

Time Range

Time Zone

Tunnel Zone

Group Policy

Add Group Policy 🔍 Filter

A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

Name	
DfltGrpPolicy	✎ 🗑
ftd-vpn-engineer-grp	✎ 🗑
ftd-vpn-manager-grp	✎ 🗑

Neue Gruppenrichtlinien

Schritt 5: FTD-Zertifikat hinzufügen

Navigieren Sie zu Object > Object Management > PKI > Cert Enrollment, und klicken Sie auf Add Cert Enrollment (Zertifikatregistrierung hinzufügen).

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ ⓘ admin 🔽

Cipher Suite List
> Community List
DHCP IPv6 Pool
> Distinguished Name
> DNS Server Group
> External Attributes
File List
> FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
 Cert Enrollment
 External Cert Groups

Cert Enrollment

Add Cert Enrollment 🔍

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Name	Type	Override
No records to display		

Zertifikatregistrierung hinzufügen

Geben Sie die erforderlichen Informationen für das FTD-Zertifikat ein, und importieren Sie eine PKCS12-Datei vom lokalen Computer.

- Name: ftd-vpn-Zertifikat
- Registrierungstyp: PKCS12-Datei

Add Cert Enrollment



Name*
ftd-vpn-cert

Description

This certificate is already enrolled on devices. Remove the enrolment from Device>Certificate page to edit/delete this Certificate.

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: ftdCert.pfx [Browse PKCS12 File](#)

Passphrase*:

Validation Usage: IPsec Client SSL Client SSL Server

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

Cancel

Save

Details zur Zertifikatregistrierung

Bestätigen Sie die neue Zertifikatregistrierung.

Firewall Management Center

Overview Analysis Policies Devices **Objects** Integration

Deploy Search Settings Help admin Cisco SECURE

Cipher Suite List
Community List
DHCP IPv6 Pool
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig

Cert Enrollment

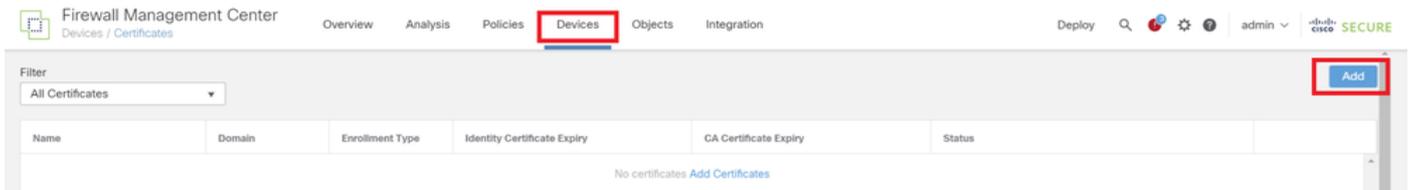
Add Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Name	Type	Override
ftd-vpn-cert	PKCS12 File	

Neue Zertifikatregistrierung

Navigieren Sie zu Geräte > Zertifikate, und klicken Sie auf die Schaltfläche Hinzufügen.



FTD-Zertifikat hinzufügen

Geben Sie die erforderlichen Informationen ein, um die neue Zertifikatsregistrierung an FTD zu binden.

- Gerät: 1.x.x.49
- Zertifikatsregistrierung: ftd-vpn-cert

Add New Certificate



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

Device*:
1.x.x.49

Cert Enrollment*:
ftd-vpn-cert

+

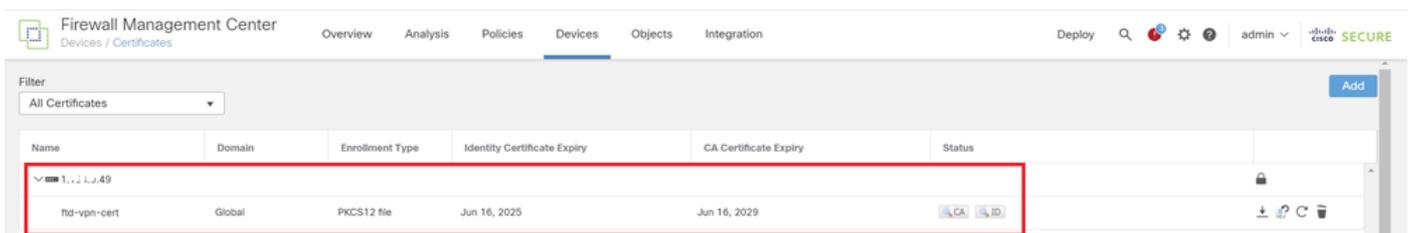
Cert Enrollment Details:

Name: ftd-vpn-cert
Enrollment Type: PKCS12 file
Enrollment URL: N/A

Cancel Add

Zertifikat an FTD binden

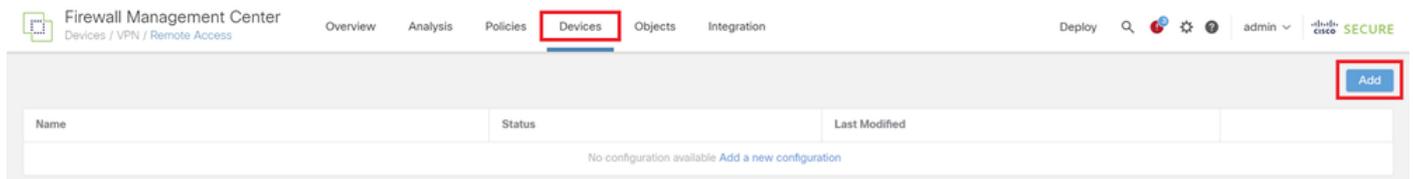
Bestätigen Sie den Status der Zertifikatsbindung.



Status der Zertifikatsbindung

Schritt 6: Richtlinienzuweisung für Techniker-Verbindungsprofil hinzufügen

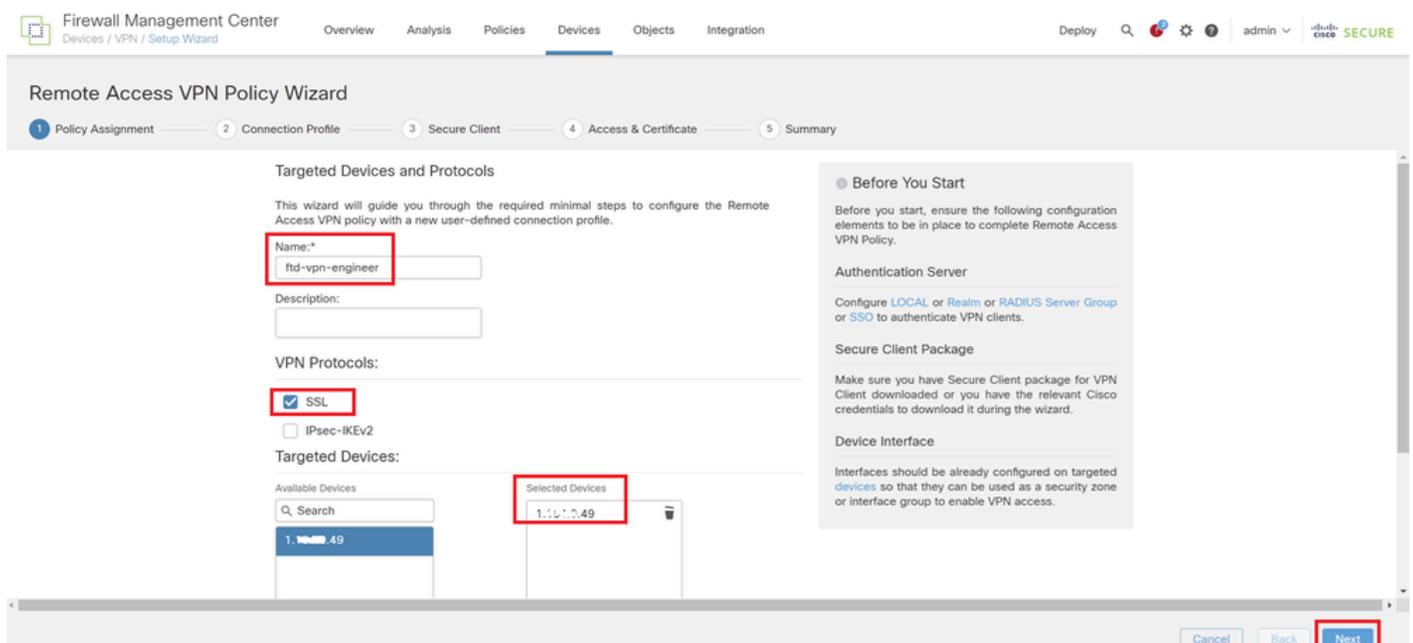
Navigieren Sie zu Geräte > VPN > Remotezugriff, und klicken Sie auf Hinzufügen.



Remote Access-VPN hinzufügen

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

- Name: ftd-vpn-engineer
- VPN-Protokolle: SSL
- Zielgeräte: 1.x.x.49



Richtlinienzuweisung

Schritt 7. Konfigurieren von Details für das Verbindungsprofil eines Technikers

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

- Authentifizierungsmethode: Nur Client-Zertifikat
- Benutzername vom Zertifikat: Zuordnungsspezifisches Feld
- Primärfeld: CN (Common Name)
- Sekundäres Feld: OU (Organisationseinheit)

- IPv4-Adresspools: ftd-vpn-engineer-pool
- Gruppenrichtlinie: ftd-vpn-engineer-grp

Remote Access VPN Policy Wizard

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

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:*

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:

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

Primary Field:

Secondary Field:

Authorization Server: +

Accounting Server: +

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:

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](#)

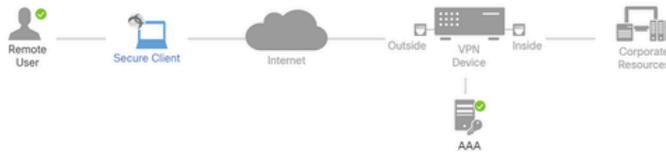
Details zum Verbindungsprofil

Schritt 8: Konfigurieren von sicherem Client-Image für Techniker-Verbindungsprofil

Wählen Sie sichere Client-Abbilddatei 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



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 checked="" type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	cisco-secure-client-win-5.1.3.6...	cisco-secure-client-win-5.1.3.62-webdepl...	Windows

Sicheren Client auswählen

Schritt 9. Konfigurieren des Zugriffs und des Zertifikats für das Techniker-Verbindungsprofil

Wählen Sie einen Wert für Schnittstellengruppe/Sicherheitszone und Zertifikatregistrierungselemente aus, und klicken Sie auf die Schaltfläche Weiter.

- Schnittstellengruppe/Sicherheitszone: outsideZone
- Zertifikatregistrierung: ftd-vpn-cert

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⚙️ admin 🔒 CISCO SECURE

Remote Access VPN Policy Wizard

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

AAA

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:* +

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

Cancel Back **Next**

Details zum Zugriff und Zertifikat

Schritt 10. Zusammenfassung für Techniker-Verbindungsprofil bestätigen

Bestätigen Sie die für die VPN-Richtlinie für den Remotezugriff eingegebenen Informationen, und klicken Sie auf die Schaltfläche Fertig stellen.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⚙️ admin 🔒 CISCO SECURE

Remote Access VPN Policy Wizard

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

Remote Access VPN Policy Configuration

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

Name:	ftd-vpn-engineer
Device Targets:	1.1.1.1-1.1.1.49
Connection Profile:	ftd-vpn-engineer
Connection Alias:	ftd-vpn-engineer
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	ftd-vpn-engineer-pool
Address Pools (IPv6):	-
Group Policy:	ftd-vpn-engineer-grp
Secure Client Images:	cisco-secure-client-win-5.1.3.62-webdeploy-k9.pk.g
Interface Objects:	outsideZone
Device Certificates:	ftd-vpn-cert

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

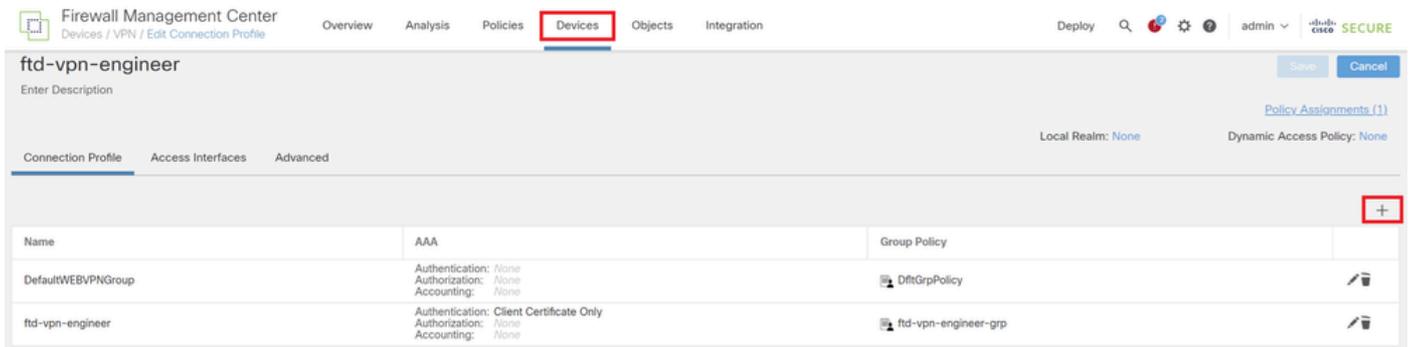
- Access Control Policy Update
An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.
- DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.
- Port Configuration
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Secure Client image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in NAT Policy or other services before deploying.

Cancel Back **Finish**

Details zur VPN-Richtlinie für den Remote-Zugriff

Schritt 11. Hinzufügen eines Verbindungsprofils für den Manager-VPN-Client

Navigieren Sie zu Geräte > VPN > Remotezugriff > Verbindungsprofil, und klicken Sie auf +.



The screenshot shows the 'Firewall Management Center' interface. The 'Devices' tab is selected and highlighted with a red box. The page title is 'ftd-vpn-engineer'. Below the title, there are tabs for 'Connection Profile', 'Access Interfaces', and 'Advanced'. The 'Connection Profile' tab is active. A table lists existing connection profiles. A red box highlights a plus sign (+) in the top right corner of the table, indicating where to click to add a new profile.

Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy	 
ftd-vpn-engineer	Authentication: Client Certificate Only Authorization: None Accounting: None	ftd-vpn-engineer-grp	 

Hinzufügen eines Verbindungsprofils für den Manager-VPN-Client

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

- Name: ftd-vpn-manager
- Gruppenrichtlinie: ftd-vpn-manager-grp
- IPv4-Adresspools: ftd-vpn-manager-pool

Add Connection Profile



Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

Client Address Assignment AAA Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
ftd-vpn-manager-pool	172.16.1.120-172.16.1.130	ftd-vpn-manager-pool

DHCP Servers: +

Name	DHCP Server IP Address	
------	------------------------	--

Details zum Verbindungsprofil für den Manager-VPN-Client

Neue hinzugefügte Verbindungsprofile bestätigen

Firewall Management Center
Devices / VPN / Edit Connection Profile

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⚙️ admin **SECURE**

ftd-vpn-engineer You have unsaved changes

Enter Description [Policy Assignments \(1\)](#)

Local Realm: None Dynamic Access Policy: None

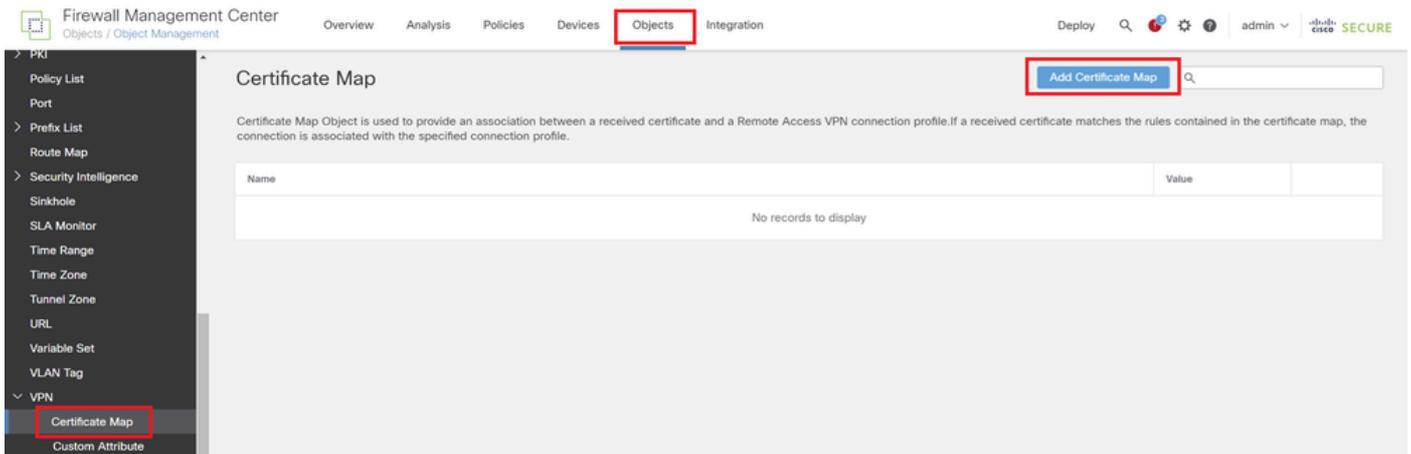
Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy	
DefaultWEBVPGGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy	🗑️
ftd-vpn-engineer	Authentication: Client Certificate Only Authorization: None Accounting: None	ftd-vpn-engineer-grp	🗑️
ftd-vpn-manager	Authentication: Client Certificate Only Authorization: None Accounting: None	ftd-vpn-manager-grp	🗑️

Hinzufügen von Verbindungsprofilen bestätigen

Schritt 12: Zertifikatzuordnung hinzufügen

Navigieren Sie zu Objekte > Objektverwaltung > VPN > Zertifikatzuordnung, und klicken Sie auf die Schaltfläche Zertifikatzuordnung hinzufügen.



Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ ⚠️ admin ▾ 

PKI
Policy List
Port
Prefix List
Route Map
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable Set
VLAN Tag
VPN
Certificate Map
Custom Attribute

Certificate Map

Add Certificate Map 🔍

Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile. If a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile.

Name	Value
No records to display	

Zertifikatzuordnung hinzufügen

Geben Sie die erforderlichen Informationen für die Zertifikatzuordnung des VPN-Clients des Technikers ein, und klicken Sie auf die Schaltfläche Speichern.

- Name der Karte: cert-map-engineer
- Zuordnungsregel: CN (Common Name) Equals vpnEngineerClientCN

Add Certificate Map



Map Name*:

cert-map-engineer

Mapping Rule

Configure the certificate matching rule

Add Rule

#	Field	Component	Operator	Value		
1	Subject	CN (Common Name)	Equals	vpnEngineerCie...		

Cancel

Save

Zertifikatszuordnung für Techniker-Client

Geben Sie die erforderlichen Informationen für die Zertifikatszuordnung des VPN-Clients des Managers ein, und klicken Sie auf die Schaltfläche Speichern.

- Kartenname: cert-map-manager
- Zuordnungsregel: CN (Common Name) Equals vpnManagerClientCN

Add Certificate Map



Map Name*:

Mapping Rule
Configure the certificate matching rule

Add Rule

#	Field	Component	Operator	Value		
1	Subject	CN (Common Name)	Equals	vpnManagerClie...		

Cancel

Save

Zertifikatszuordnung für Manager-Client

Neue hinzugefügte Zertifikatszuordnungen bestätigen.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ? admin ▾ SECURE

Certificate Map

Add Certificate Map 🔍

Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile. If a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile.

Name	Value		
cert-map-engineer	1 Criteria		
cert-map-manager	1 Criteria		

Neue Zertifikatszuordnungen

Schritt 13: Binden der Zertifikatszuordnung an das Verbindungsprofil

Navigieren Sie zu Devices > VPN > Remote Access, und bearbeiten Sie ftd-vpn-engineer. Navigieren Sie anschließend zu Erweitert > Zertifikatszuordnungen, und klicken Sie auf die Schaltfläche Zuordnung hinzufügen.

Zertifikatzuordnung binden

Bindende Zertifikatzuordnung zum Verbindungsprofil für VPN-Client des Technikers.

- Name der Zertifikatzuordnung: cert-map-engineer
- Connection Profile: ftd-vpn-engineer

Add Connection Profile to Certificate Map ?

Choose a Certificate Map and associate Connection Profiles to selected Certificate Map.

Certificate Map Name*:

cert-map-engineer
▼

+

Connection Profile*:

ftd-vpn-engineer
▼

Cancel
OK

Bindende Zertifikatzuordnung für Techniker-VPN-Client

Bindende Zertifikatzuordnung zum Verbindungsprofil für Manager-VPN-Client.

- Name der Zertifikatzuordnung: cert-map-manager
- Verbindungsprofil: ftd-vpn-manager

Add Connection Profile to Certificate Map



Choose a Certificate Map and associate Connection Profiles to selected Certificate Map.

Certificate Map Name*:
cert-map-manager

+

Connection Profile*:
ftd-vpn-manager

Cancel OK

Bindende Zertifikatzuordnung für Manager VPN Client

Bestätigen Sie die Einstellung der Zertifikatbindung.

Firewall Management Center
Devices / VPN / Edit Advanced

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾ 🔒 Cisco SECURE

ftd-vpn-engineer You have unsaved changes Save Cancel

Enter Description Policy Assignments (1)

Connection Profile Access Interfaces **Advanced** Local Realm: None Dynamic Access Policy: None

Secure Client Images
Secure Client Customization
GUI Text and Messages
Icons and Images
Scripts
Binaries
Custom Installer Transforms
Localized Installer Transforms
Address Assignment Policy
Certificate Maps
Group Policies

General Settings for Connection Profile Mapping
The device processes the policies in the order listed below until it finds a match

- Use group URL if group URL and Certificate Map match different Connection Profiles
- Use the configured rules to match a certificate to a Connection Profile

Certificate to Connection Profile Mapping
Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are matched. If none of the Certificate Map is matched, default connection profile will be chosen.

Certificate Map	Connection Profile	
cert-map-engineer	ftd-vpn-engineer	🗑️
cert-map-manager	ftd-vpn-manager	🗑️

Add Mapping

Zertifikatbindung bestätigen

In FTD-CLI bestätigen

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

```
// Defines IP of interface
```

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-vpn-engineer-pool 172.16.1.100-172.16.1.110 mask 255.255.255.0
ip local pool ftd-vpn-manager-pool 172.16.1.120-172.16.1.130 mask 255.255.255.0

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

// Server Certificate Chain
crypto ca certificate chain ftd-vpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
.....
quit

certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit

// Defines Certificate Map for Engineer VPN Clients
crypto ca certificate map cert-map-engineer 10
subject-name attr cn eq vpnEngineerClientCN

// Defines Certificate Map for Manager VPN Clients
crypto ca certificate map cert-map-manager 10
subject-name attr cn eq vpnManagerClientCN

// 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:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert-map-engineer 10 ftd-vpn-engineer
certificate-group-map cert-map-manager 10 ftd-vpn-manager
error-recovery disable

// Configures the group-policy to allow SSL connections from manager VPN clients
group-policy ftd-vpn-manager-grp internal
group-policy ftd-vpn-manager-grp attributes
banner none
wins-server none
```

```
dns-server none
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 ikev2 ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable
```

```
// Configures the group-policy to allow SSL connections from engineer VPN clients
group-policy ftd-vpn-engineer-grp internal
group-policy ftd-vpn-engineer-grp attributes
banner none
wins-server none
dns-server none
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-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
```

```
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable
```

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

```
// Configures the tunnel-group to use the certificate authentication for manager VPN clients
tunnel-group ftd-vpn-manager type remote-access
tunnel-group ftd-vpn-manager general-attributes
address-pool ftd-vpn-manager-pool
default-group-policy ftd-vpn-manager-grp
tunnel-group ftd-vpn-manager webvpn-attributes
authentication certificate
```

Bestätigung in VPN-Client

Schritt 1: Clientzertifikat bestätigen

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



Zertifikat für Techniker-VPN-Client bestätigen

Doppelklicken Sie auf das Clientzertifikat, navigieren Sie zu Details, und überprüfen Sie die Details von Subject.

- 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 Clientzertifikat, navigieren Sie zu Details, und überprüfen Sie die Details von Subject.

- 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...

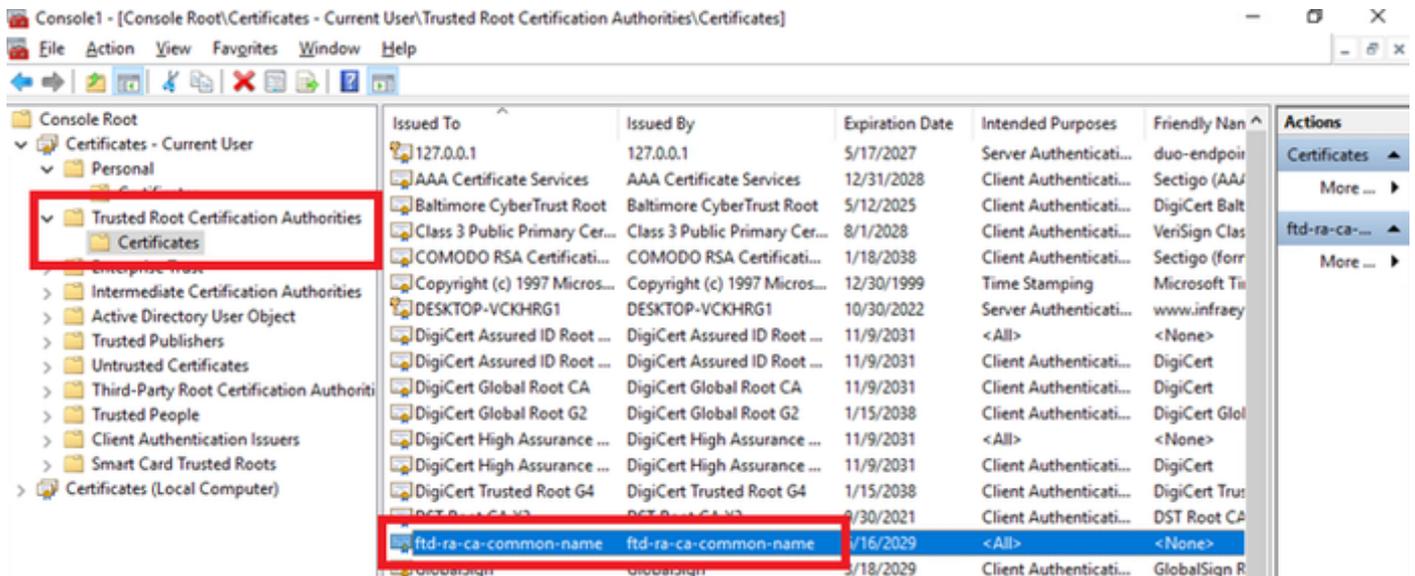
OK

Details zum Manager-Clientzertifikat

Schritt 2: 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

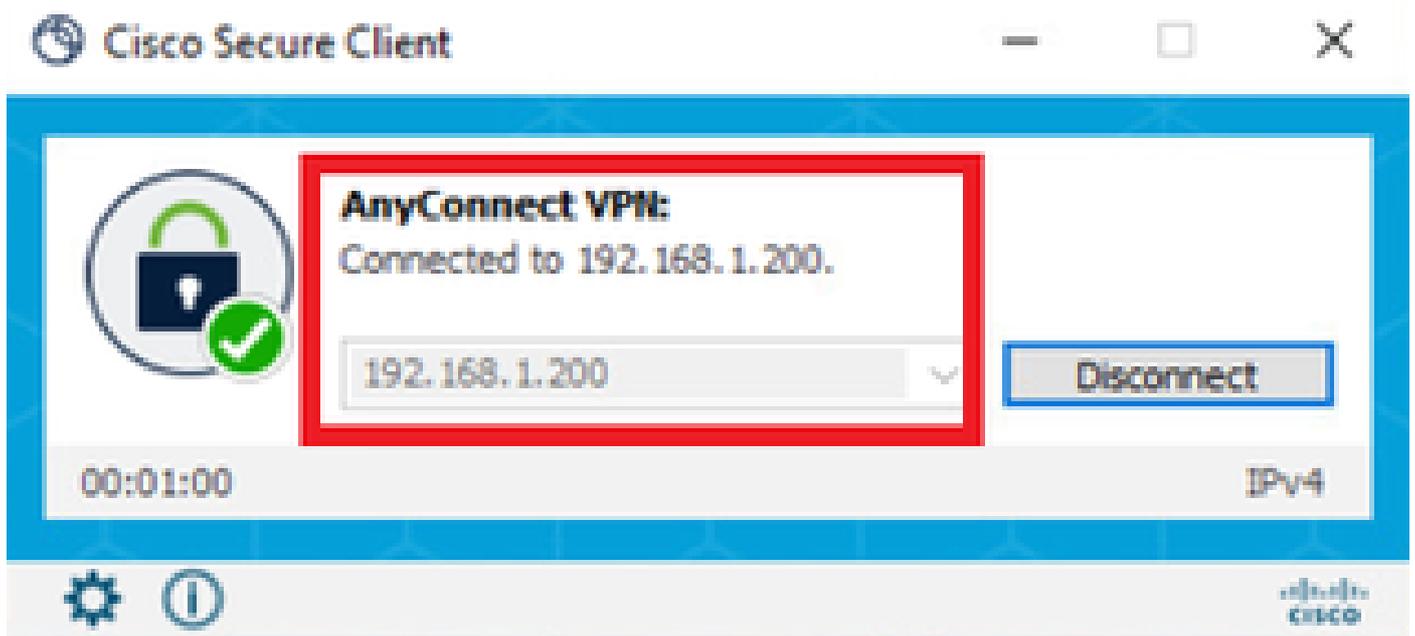


Zertifizierungsstelle bestätigen

Überprüfung

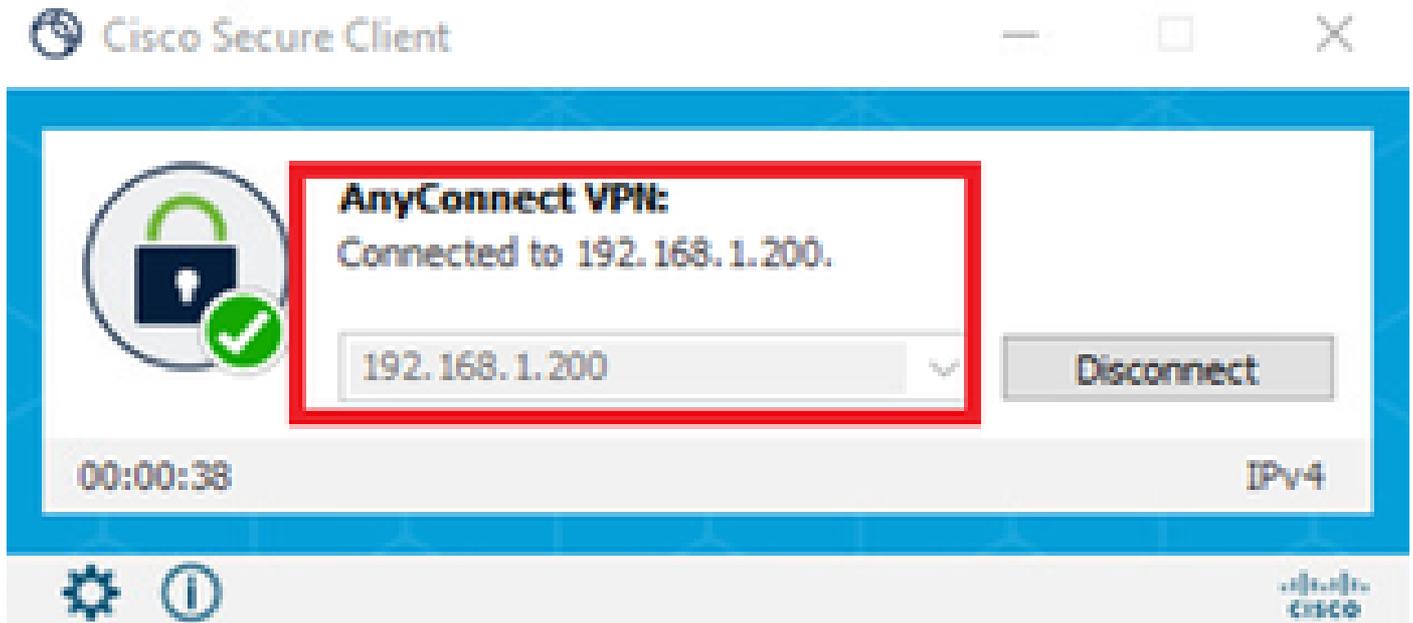
Schritt 1: VPN-Verbindung initiieren

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 vom Techniker-Client initiieren

Initiieren Sie im Manager 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 vom Manager-Client initiieren

Schritt 2: Aktive Sitzungen in FMC bestätigen

Navigieren Sie zu Analyse > Benutzer > Aktive Sitzungen, und überprüfen Sie die aktive Sitzung auf VPN-Authentifizierung.

<input type="checkbox"/>	Login Time	Realm/Username	Last Seen	Authentication Type	Current IP	Realm	Username ↓	First Name	Last Name
<input type="checkbox"/>	2024-06-19 11:01:19	Discovered Identities\vpnManagerClientCN	2024-06-19 11:01:19	VPN Authentication	172.16.1.120	Discovered Identities	vpnManagerClientCN		
<input type="checkbox"/>	2024-06-19 11:00:35	Discovered Identities\vpnEngineerClientCN	2024-06-19 11:00:35	VPN Authentication	172.16.1.101	Discovered Identities	vpnEngineerClientCN		

Aktive Sitzung bestätigen

Schritt 3: VPN-Sitzungen in FTD CLI bestätigen

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

```
ftd702# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : vpnEngineerClientCN Index : 13
```

```
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14782 Bytes Rx : 12714
Pkts Tx : 2 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-engineer-grp Tunnel Group : ftd-vpn-engineer
Login Time : 02:00:35 UTC Wed Jun 19 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000d00066723bc3
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 13.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50225 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 13.2
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50232
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 1775
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 13.3
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 50825
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62

Bytes Tx : 0 Bytes Rx : 10939
Pkts Tx : 0 Pkts Rx : 30
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Username : vpnManagerClientCN Index : 14
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14782 Bytes Rx : 13521
Pkts Tx : 2 Pkts Rx : 57
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-manager-grp Tunnel Group : ftd-vpn-manager
Login Time : 02:01:19 UTC Wed Jun 19 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000e00066723bef
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 14.1
Public IP : 192.168.1.21
Encryption : none Hashing : none
TCP Src Port : 49809 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 14.2
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 49816
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 3848
Pkts Tx : 1 Pkts Rx : 25
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 14.3
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-256 Hashing : SHA384

Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 65501
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 0 Bytes Rx : 9673
Pkts Tx : 0 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Fehlerbehebung

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

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

<#root>

```
Jun 19 2024 02:00:35: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN
Jun 19 2024 02:00:35: %FTD-6-717022:
```

Certificate was successfully validated

```
. serial number: 7AF1C78ADCC8F941, subject name:
```

```
CN=vpnEngineerClientCN
```

```
,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
```

```
Jun 19 2024 02:00:35: %FTD-7-717038: Tunnel group match found.
```

Tunnel Group: ftd-vpn-engineer

```
, Peer certificate: serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
```

```
Jun 19 2024 02:00:35: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-engineer-grp) for user
```

```
Jun 19 2024 02:00:46: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50
```

Dies ist ein Beispiel für Debug-Protokolle im Lina-Modul während der VPN-Verbindung vom Manager-Client.

<#root>

```
Jun 19 2024 02:01:19: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN
Jun 19 2024 02:01:19: %FTD-6-717022:
```

Certificate was successfully validated

```
. serial number: 1AD1B5EAE28C6D3C, subject name:
```

```
CN=vpnManagerClientCN
```

```
,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
```

```
Jun 19 2024 02:01:19: %FTD-7-717038: Tunnel group match found.
```

Tunnel Group: ftd-vpn-manager

, Peer certificate: serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN,OU=vpnManagerC
Jun 19 2024 02:01:19: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-manager-grp) for user :
Jun 19 2024 02:01:25: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.21/65

Zugehörige Informationen

[Konfigurieren der zertifikatbasierten AnyConnect-Authentifizierung für den mobilen Zugriff](#)

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.