

# FMCを介したFTDでのセキュアクライアント認証の証明書マッピングの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[FMCでの設定](#)

[ステップ 1: FTDインターフェイスの設定](#)

[ステップ 2: Cisco Secure Clientライセンスの確認](#)

[ステップ 3: IPv4アドレスプールの追加](#)

[ステップ 4: グループポリシーの追加](#)

[ステップ 5: FTD証明書の追加](#)

[手順 6: エンジニア接続プロファイルのポリシー割り当ての追加](#)

[手順 7: エンジニア接続プロファイルの詳細の設定](#)

[ステップ 8: エンジニア接続プロファイル用のセキュアクライアントイメージの設定](#)

[ステップ 9: エンジニア接続プロファイルのアクセスと証明書の設定](#)

[ステップ 10: エンジニアの接続プロファイルの要約の確認](#)

[ステップ 11: Manager VPN Client用の接続プロファイルの追加](#)

[ステップ 12: 証明書マップの追加](#)

[ステップ 13: 接続プロファイルへの証明書マップのバインド](#)

[FTD CLIで確認](#)

[VPNクライアントでの確認](#)

[ステップ 1: クライアント証明書の確認](#)

[ステップ 2: CAの確認](#)

[確認](#)

[ステップ 1: VPN接続の開始](#)

[ステップ 2: FMCでのアクティブセッションの確認](#)

[ステップ 3: FTD CLIでのVPNセッションの確認](#)

[トラブルシューティング](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、認証に証明書マッピングを使用して、FMC経由でFTD上のSSLを使用してCisco Secure Client(CSC)を設定する方法について説明します。

## 前提条件

## 要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Management Center ( FMC )
- ファイアウォール脅威対策(FTD)仮想
- VPN認証のフロー

## 使用するコンポーネント

- VMWare 7.4.1向けCisco Firepower Management Center
- シスコファイアウォール脅威対策の仮想7.4.1
  
- Cisco Secureクライアント5.1.3.62

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

証明書マッピングは、クライアント証明書がローカルユーザアカウントにマッピングされるVPN接続で使用される方法、または証明書内の属性が認可の目的で使用される方法です。これは、ユーザまたはデバイスを識別する手段としてデジタル証明書が使用されるプロセスです。証明書マッピングを使用することで、SSLプロトコルを利用して、クレデンシャルを入力せずにユーザを認証します。

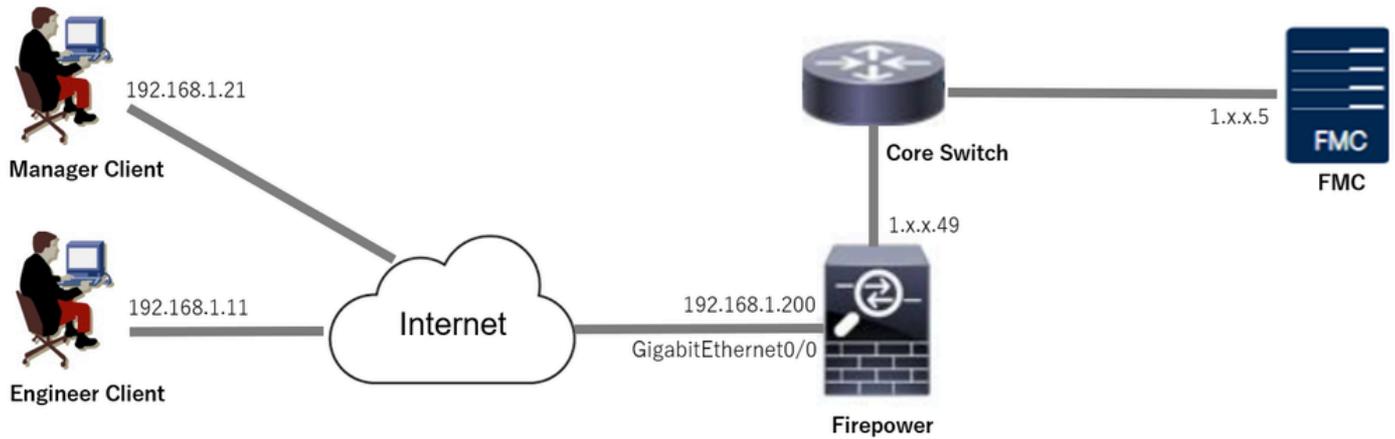
このドキュメントでは、SSL証明書の共通名を使用してCisco Secure Client(CSA)を認証する方法について説明します。

これらの証明書には共通の名前が含まれており、認証の目的で使用されます。

- CA:ftd-ra-ca-common-name
- エンジニアVPNクライアント証明書：vpnEngineerClientCN
- マネージャVPNクライアント証明書：vpnManagerClientCN
- サーバ証明書：192.168.1.200

## ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。



ネットワーク図

## コンフィギュレーション

### FMCでの設定

#### ステップ 1 : FTDインターフェイスの設定

Devices > Device Managementの順に移動し、ターゲットFTDデバイスを編集して、FTD inInterfacestabの外部インターフェイスを設定します。

GigabitEthernet0/0の場合、

- 名前 : outside
- セキュリティゾーン : outsideZone
- IPアドレス : 192.168.1.200/24

Firewall Management Center  
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒 **SECURE**

1.17.1.49 Save Cancel

Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

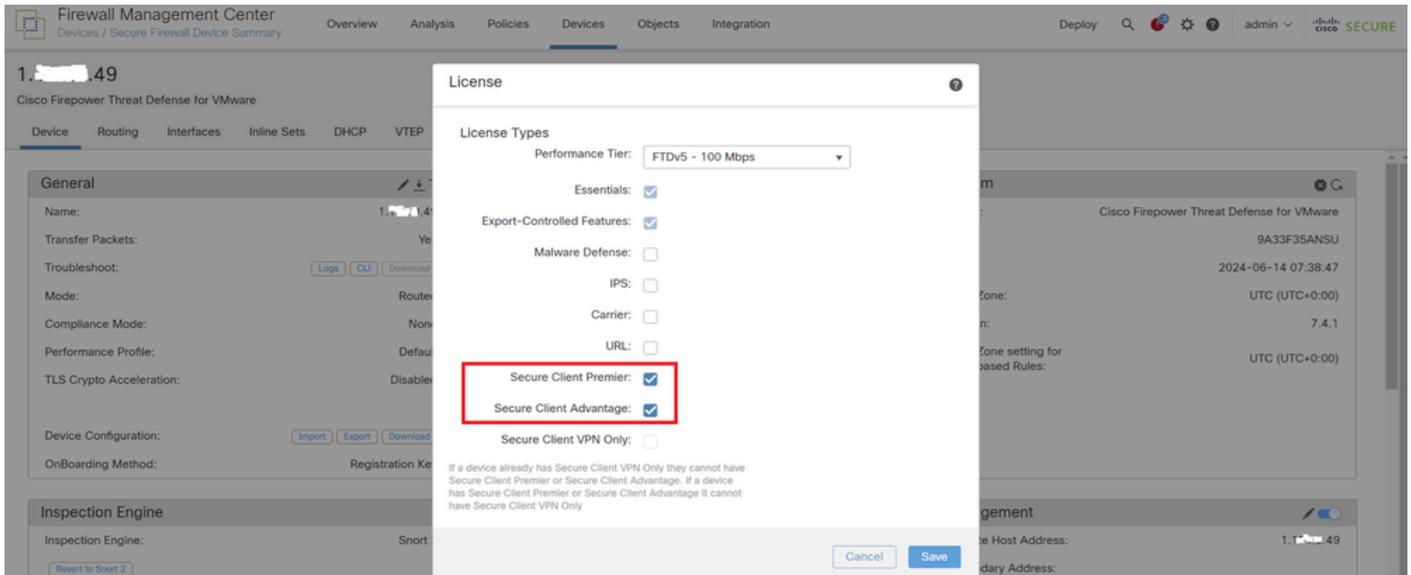
All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces

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インターフェイス

#### ステップ 2 : Cisco Secure Clientライセンスの確認

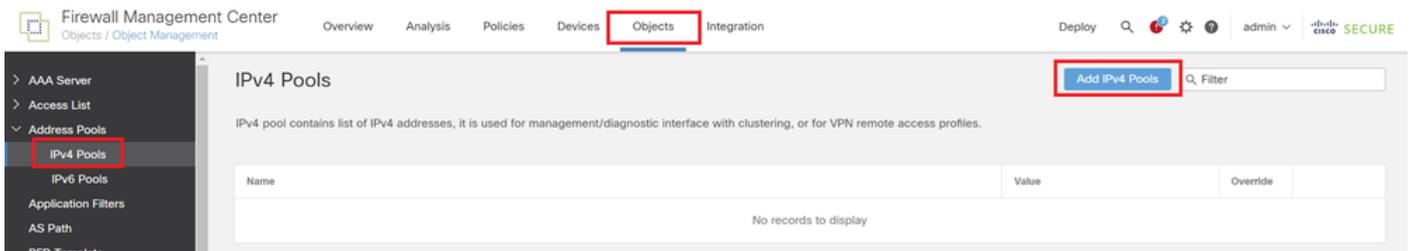
Devices > Device Managementの順に移動し、ターゲットFTDデバイスを編集し、DeviceタブでCisco Secure Clientライセンスを確認します。



セキュアクライアントライセンス

### ステップ 3 : IPv4アドレスプールの追加

Object > Object Management > Address Pools > IPv4 Poolsの順に選択し、Add IPv4 Poolsボタンをクリックします。



IPv4アドレスプールの追加

エンジニアのVPNクライアント用のIPv4アドレスプールを作成するために必要な情報を入力します。

- 名前 : ftd-vpn-engineer-pool
- IPv4アドレス範囲 : 172.16.1.100 ~ 172.16.1.110
- マスク : 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

エンジニアVPNクライアント用のIPv4アドレスプール

マネージャVPNクライアント用のIPv4アドレスプールを作成するために必要な情報を入力します

。

- 名前 : ftd-vpn-manager-pool
- IPv4アドレス範囲 : 172.16.1.120 ~ 172.16.1.130
- マスク : 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

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

Manager VPN Client用のIPv4アドレスプール

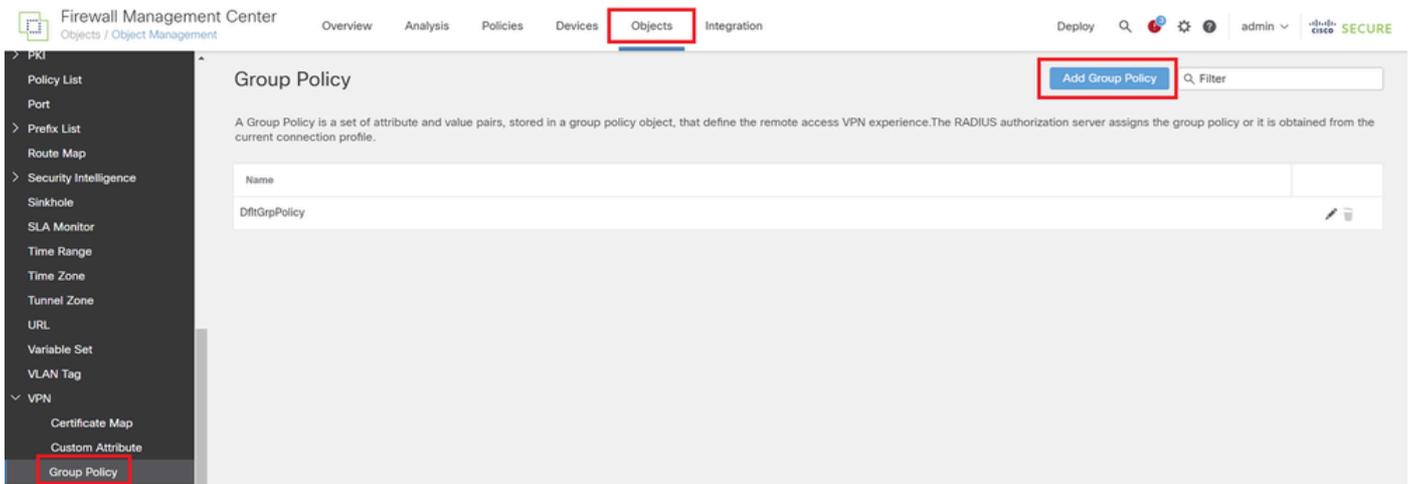
新しいIPv4アドレスプールを確認します。

Name	Value	Override	
ftd-vpn-engineer-pool	172.16.1.100-172.16.1.110	<span style="color: green;">●</span>	
ftd-vpn-manager-pool	172.16.1.120-172.16.1.130	<span style="color: green;">●</span>	

新しいIPv4アドレスプール

ステップ 4 : グループポリシーの追加

Object > Object Management > VPN > Group Policyの順に移動し、Add Group Policybuttonをクリックします。



グループポリシーの追加

エンジニアのVPNクライアントのグループポリシーを作成するために必要な情報を入力します。

- 名前 : ftd-vpn-engineer-grp
- VPNプロトコル : 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

IP Address Pools  
Banner  
DNS/WINS  
Split Tunneling

エンジニアVPNクライアントのグループポリシー

マネージャVPNクライアントのグループポリシーを作成するために必要な情報を入力します。

- 名前 : ftd-vpn-manager-grp
- VPNプロトコル : 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

マネージャVPNクライアントのグループポリシー

新しいグループポリシーを確認します。

Firewall Management Center

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

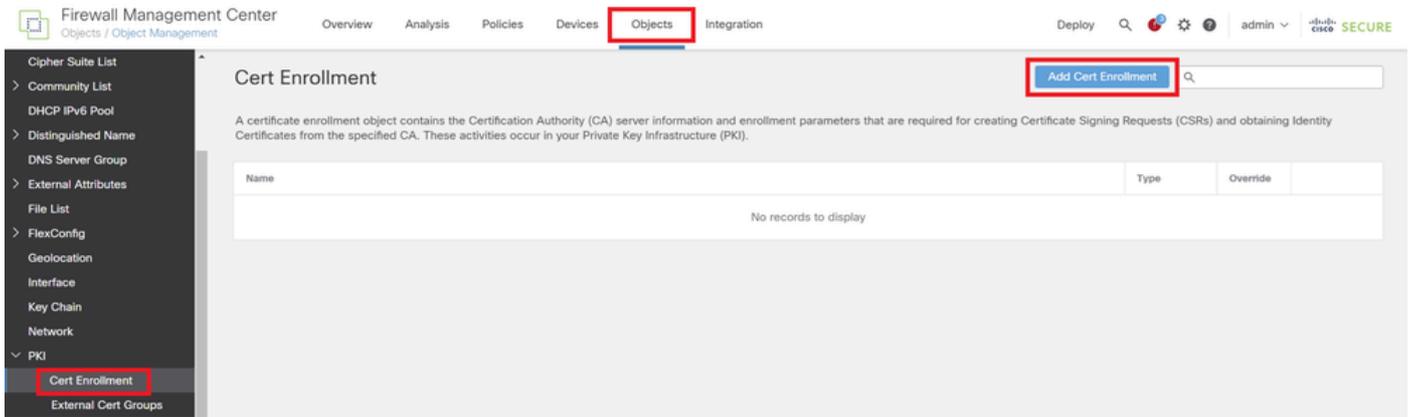
A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

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

新しいグループポリシー

### ステップ 5 : FTD証明書の追加

Object > Object Management > PKI > Cert Enrollmentの順に移動し、Add Cert Enrollmentbuttonをクリックします。



証明書の登録の追加

FTD証明書に必要な情報を入力し、ローカルコンピュータからPKCS12ファイルをインポートします。

- 名前 : ftd-vpn-cert
- 登録タイプ : PKCS12ファイル

## 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

証明書登録の詳細

新しい証明書の登録を確認します。

Firewall Management Center

Overview   Analysis   Policies   Devices   **Objects**   Integration

Deploy   Search   Settings   Help   admin   **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	

新しい証明書の登録

Devices > Certificatesの順に移動し、Addボタンをクリックします。

Firewall Management Center  
Devices / Certificates

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin 🔒 cisco **SECURE**

Filter: All Certificates Add

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
No certificates <a href="#">Add Certificates</a>					

FTD証明書の追加

新しい証明書の登録をFTDにバインドするために必要な情報を入力します。

- デバイス : 1.x.x.49
- 証明書登録: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\*:

Cert Enrollment\*:  +

Cert Enrollment Details:

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

Cancel Add

FTDへの証明書のバインド

証明書バインドの状態を確認します。

Firewall Management Center  
Devices / Certificates

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin 🔒 cisco **SECURE**

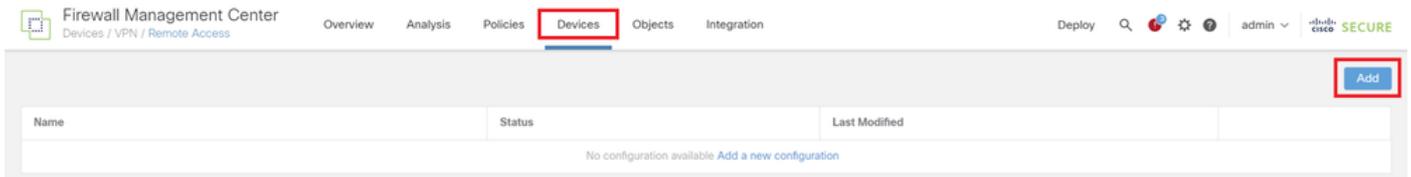
Filter: All Certificates Add

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
1.1.1.49					
ftd-vpn-cert	Global	PKCS12 file	Jun 16, 2025	Jun 16, 2029	CA ID

証明書バインドの状態

## 手順 6 : エンジニア接続プロファイルのポリシー割り当ての追加

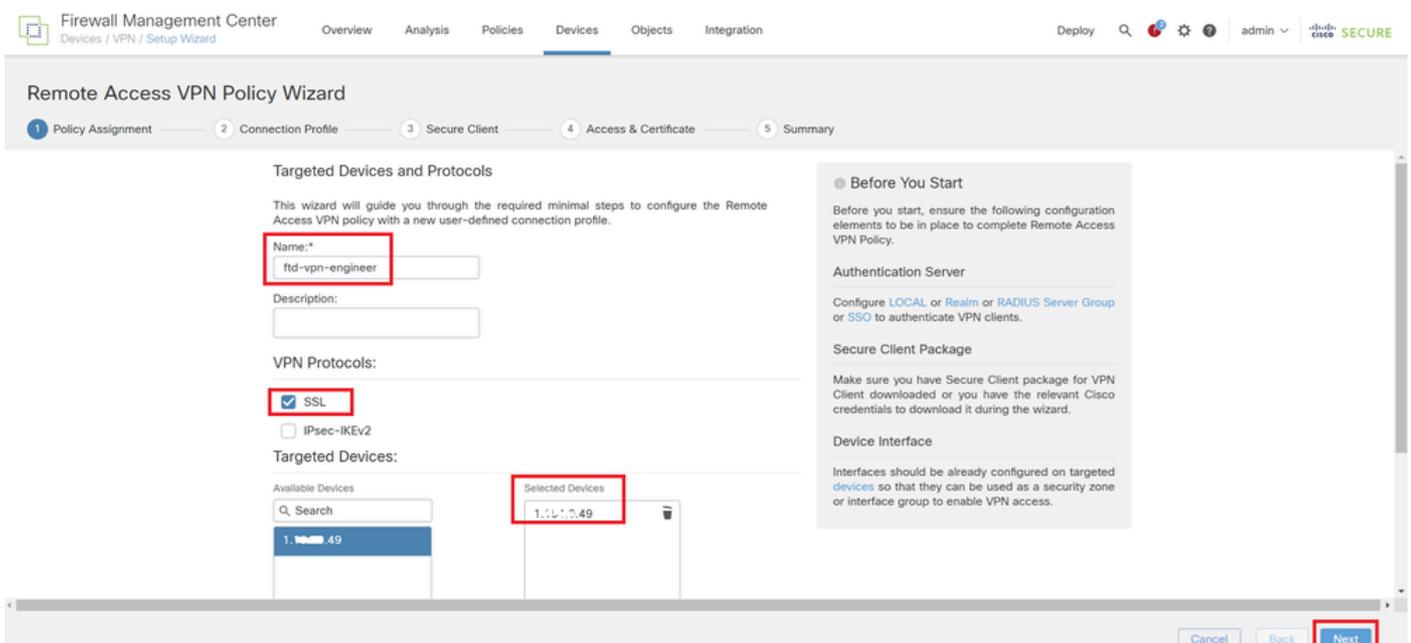
Devices > VPN > Remote Accessの順に移動し、Addbuttonをクリックします。



リモートアクセスVPNの追加

必要な情報を入力し、Nextbuttonをクリックします。

- 名前 : ftd-vpn-engineer
- VPNプロトコル : SSL
- ターゲットデバイス : 1.x.x.49



ポリシーの割り当て

## 手順 7 : エンジニア接続プロファイルの詳細の設定

必要な情報を入力し、Nextbuttonをクリックします。

- 認証方法 : クライアント証明書のみ
- 証明書からのユーザ名 : 特定のフィールドのマッピング
- 主フィールド : CN ( 共通名 )
- セカンダリフィールド : OU(Organizational Unit)
  
- IPv4アドレスプール : ftd-vpn-engineer-pool
- グループポリシー : ftd-vpn-engineer-grp

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

**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:\*

**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:  +  
(Realm or RADIUS)

Accounting Server:  +  
(RADIUS)

**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](#)

接続プロファイルの詳細

## ステップ 8 : エンジニア接続プロファイル用のセキュアクライアントイメージの設定

secure client image fileを選択し、Nextbuttonをクリックします。

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 User — Secure Client — Internet — Outside — VPN Device — Inside — Corporate Resources

AAA

**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

セキュアクライアントの選択

## ステップ 9 : エンジニア接続プロファイルのアクセスと証明書の設定

Interface group/Security ZoneおよびCertificate Enrollment項目の値を選択し、Nextボタンをクリックします。

- インターフェイスグループ/セキュリティゾーン : outsideZone
- 証明書の登録 : 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:\* outsideZone +

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:\* ftd-vpn-cert +

#### 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**

アクセスおよび証明書の詳細

## ステップ 10 : エンジニアの接続プロファイルの要約の確認

リモートアクセスVPNポリシーに入力した情報を確認し、Finishボタンをクリックします。

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:	1,1,1,1:49
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.

- 1 Access Control Policy Update  
An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- 1 NAT Exemption  
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.
- 1 DNS Configuration  
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.
- 1 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.

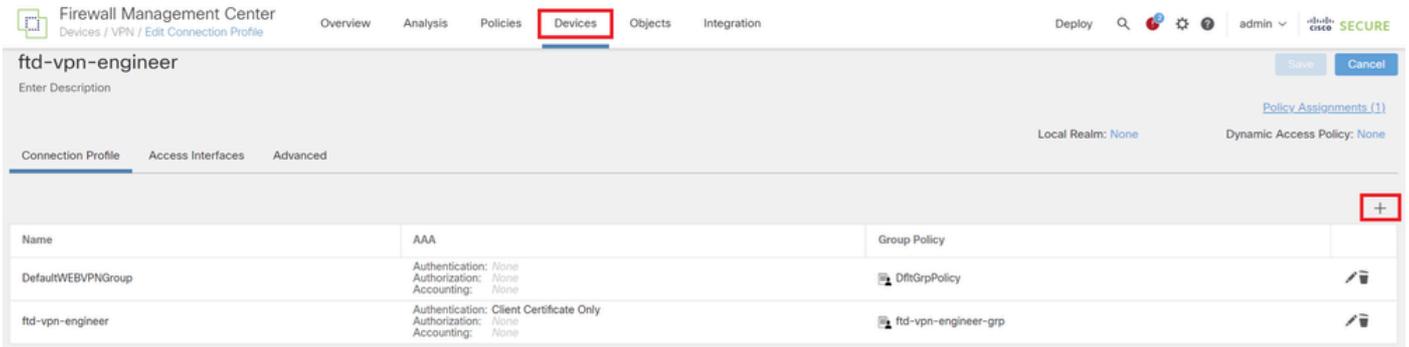
Cancel Back **Finish**

リモートアクセスVPNポリシーの詳細

## ステップ 11 Manager VPN Client用の接続プロファイルの追加

Devices > VPN > Remote Access > Connection Profileの順に移動し、+ボタンをクリックします

o



Manager VPN Client用の接続プロファイルの追加

接続プロファイルに必要な情報を入力し、Saveボタンをクリックします。

- 名前 : ftd-vpn-manager
- グループポリシー : ftd-vpn-manager-grp
- IPv4アドレスプール : 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	
<b>ftd-vpn-manager-pool</b>	172.16.1.120-172.16.1.130	ftd-vpn-manager-pool

DHCP Servers: +

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

マネージャVPNクライアントの接続プロファイルの詳細

新しく追加された接続プロファイルを確認します。

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

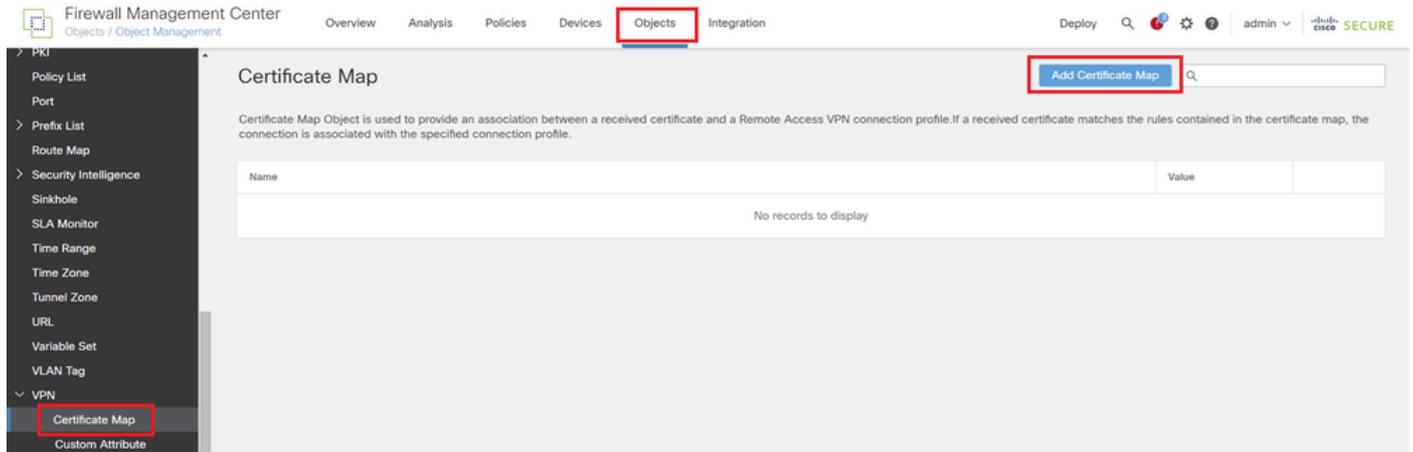
Connection Profile   Access Interfaces   Advanced

Name	AAA	Group Policy	
DefaultWEBVpnGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy	🗑️
<b>ftd-vpn-engineer</b>	Authentication: Client Certificate Only Authorization: None Accounting: None	<b>ftd-vpn-engineer-grp</b>	🗑️
<b>ftd-vpn-manager</b>	Authentication: Client Certificate Only Authorization: None Accounting: None	<b>ftd-vpn-manager-grp</b>	🗑️

追加された接続プロファイルの確認

## ステップ 12 証明書マップの追加

Objects > Object Management > VPN > Certificate Mapの順に選択し、AddCertificate Mapボタンをクリックします。



### 証明書マップの追加

エンジニアのVPN Clientの証明書マップに必要な情報を入力し、Saveボタンをクリックします。

- マップ名 : cert-map-engineer
- マッピングルール : CN ( 共通名 ) はvpnEngineerClientCNと同じ

## 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

エンジニアクライアントの証明書マップ

Manager VPN Clientの証明書マップに必要な情報を入力し、Saveボタンをクリックします。

- マップ名 : cert-map-manager
- マッピングルール : CN ( 共通名 ) はvpnManagerClientCNと同じ

## Add Certificate Map



Map Name\*:

cert-map-manager

Mapping Rule

Configure the certificate matching rule

Add Rule

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

Cancel

Save

Manager Clientの証明書マップ

新しく追加された証明書マップを確認します。

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		

新しい証明書マップ

ステップ 13 接続プロファイルへの証明書マップのバインド

Devices > VPN > Remote Accessの順に移動し、ftd-vpn-engineerを編集します。次に、Advanced > Certificate Mapsの順に移動し、Add Mappingボタンをクリックします。

Firewall Management Center  
Devices / VPN / Edit Advanced

Overview Analysis Policies **Devices** Objects Integration

ftd-vpn-engineer

Enter Description

Connection Profile Access Interfaces **Advanced**

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.

Please provide at least one Certificate Mapping.

Add Mapping

Certificate Map	Connection Profile
No Records Found	

証明書マップのバインド

エンジニアのVPNクライアントの接続プロファイルに証明書マップをバインドしています。

- Certificate Map Name ( 証明書マップ名 ) : cert-map-engineer
- コネクションプロファイル: 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

エンジニアVPNクライアントのバインディング証明書マップ

マネージャーVPNクライアントの接続プロファイルに証明書マップをバインドしています。

- Certificate Map Name ( 証明書マップ名 ) : cert-map-manager
- 接続プロファイル : 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

Manager VPN Clientのバインディング証明書マップ

証明書バインドの設定を確認します。

Firewall Management Center  
Devices / VPN / Edit Advanced

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Help admin | Cisco SECURE

ftd-vpn-engineer  
Enter Description

You have unsaved changes Save Cancel

Policy Assignments (1)

Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

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

証明書バインドの確認

FTD CLIで確認

FMCからの展開後に、FTD CLIでVPN接続設定を確認します。

```
// 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
```

## VPNクライアントでの確認

### ステップ 1：クライアント証明書の確認

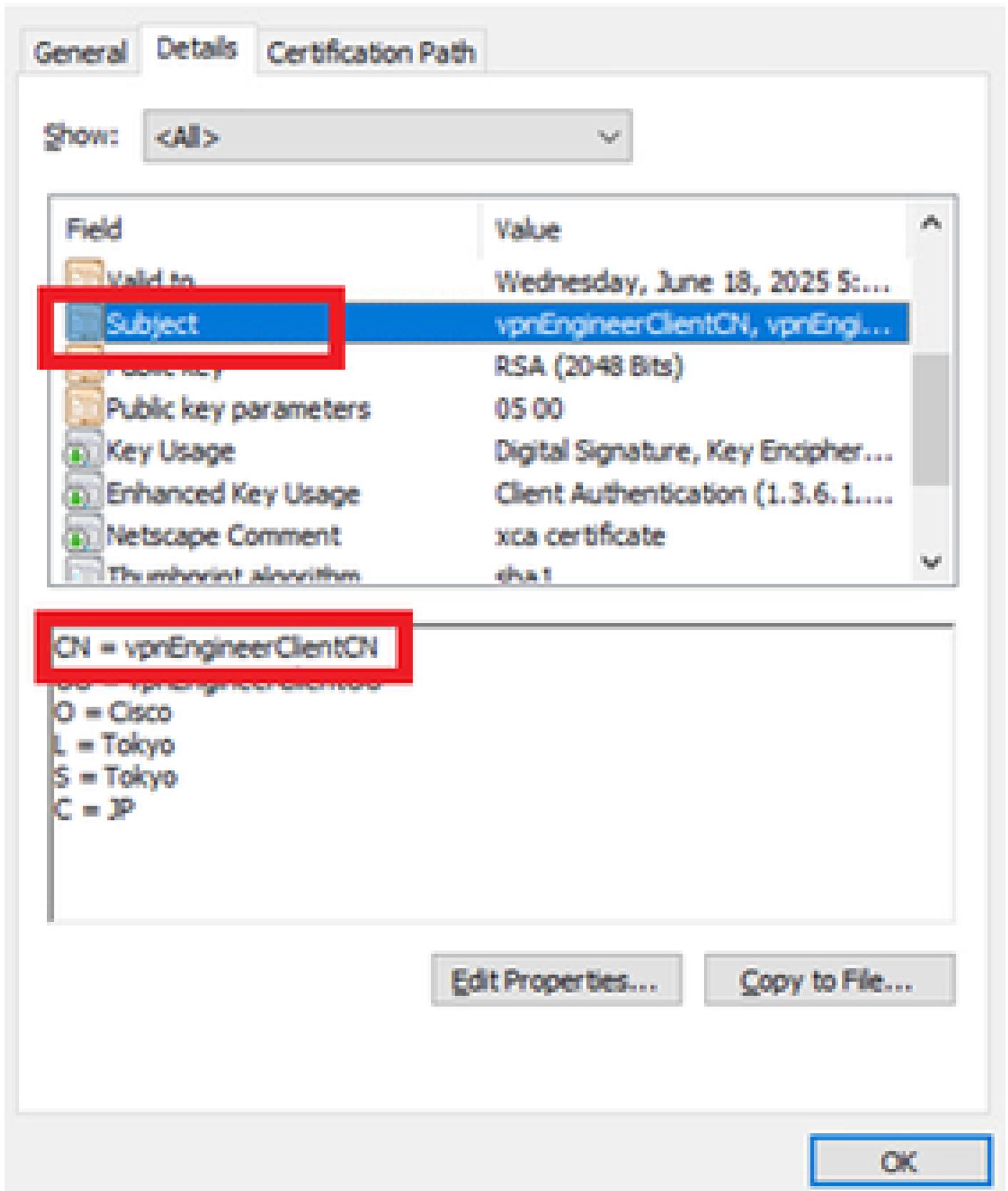
VPN Clientエンジニアで、Certificates - Current User > Personal > Certificatesの順に移動し、認証に使用するクライアント証明書を確認します。



エンジニア用VPN Clientの証明書の確認

クライアント証明書をダブルクリックし、Detailsに移動して、Subjectの詳細を確認します。

- 件名：CN = vpnEngineerClientCN



技術士免状の内容

マネージャのVPN Clientで、Certificates - Current User > Personal > Certificatesの順に移動し、認証に使用するクライアント証明書を確認します。



Manager VPN Clientの証明書の確認

クライアント証明書をダブルクリックし、Detailsに移動して、Subjectの詳細を確認します。

- 件名 : 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...

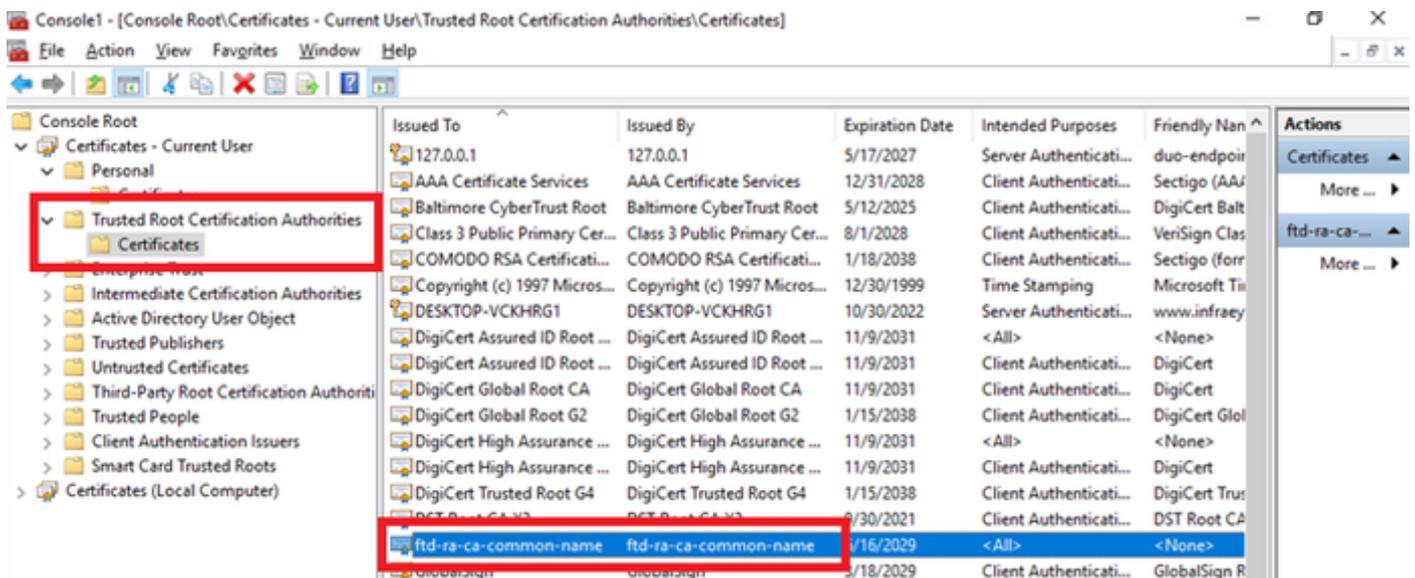
OK

マネージャクライアント証明書の詳細

ステップ 2 : CAの確認

エンジニアのVPNクライアントとマネージャのVPNクライアントの両方で、Certificates - Current User > Trusted Root Certification Authorities > Certificatesの順に移動し、認証に使用するCAを確認します。

- 発行元 : ftd-ra-ca-common-name

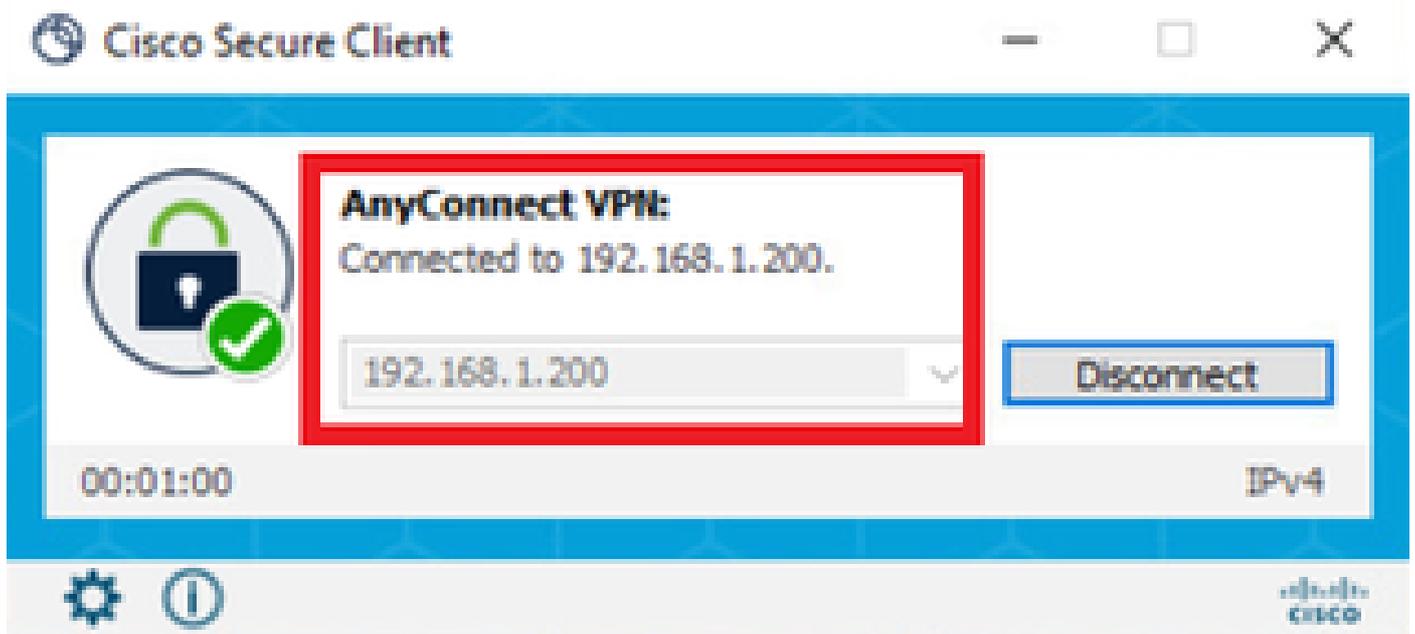


CAの確認

## 確認

### ステップ 1 : VPN接続の開始

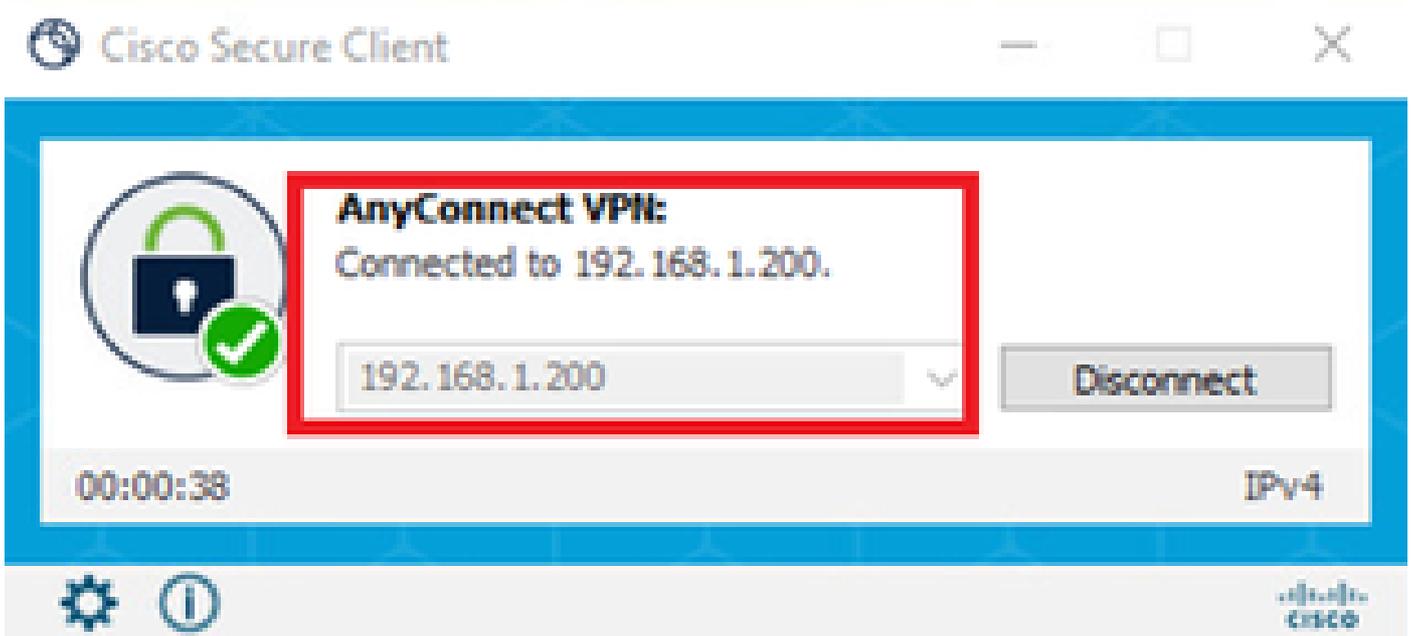
エンジニアのVPNクライアントで、Cisco Secure Client接続を開始します。ユーザ名とパスワードを入力する必要はなく、VPNは正常に接続されました。



エンジニアクライアントからのVPN接続の開始

マネージャのVPNクライアントで、Cisco Secure Client接続を開始します。ユーザ名とパスワー

ドを入力する必要はなく、VPNは正常に接続されました。



Manager ClientからのVPN接続の開始

## ステップ 2 : FMCでのアクティブセッションの確認

Analysis > Users > Active Sessionsの順に移動し、VPN認証のアクティブセッションを確認します。

The image shows the Firewall Management Center (FMC) interface. The breadcrumb navigation is "Analysis / Users / Active Sessions". The table displays active sessions with columns for Login Time, Realm/Username, Last Seen, Authentication Type, Current IP, Realm, Username, First Name, and Last Name. Two sessions are listed, both with "VPN Authentication" as the authentication type, highlighted with red boxes. The first session is for "vpnManagerClientCN" with IP 172.16.1.120, and the second is for "vpnEngineerClientCN" with IP 172.16.1.101.

	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		

アクティブセッションの確認

## ステップ 3 : FTD CLIでのVPNセッションの確認

FTD(Lina)CLIでshow vpn-sessiondb detail anyconnectコマンドを実行し、エンジニアとマネージャのVPNセッションを確認します。

```
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

## トラブルシュート

VPN認証に関する情報は、Linaエンジンのdebug syslogおよびWindows PCのDARTファイルに記載されています。

次に、エンジニアクライアントからのVPN接続中のLinaエンジンのデバッグログの例を示します。

### <#root>

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

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=vpnEngineerClientCN,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

次に、マネージャクライアントからのVPN接続中のLinaエンジンのデバッグログの例を示します。

### <#root>

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

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=vpnManagerClientCN,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.

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:192.168.1.21/50

関連情報

[モバイルアクセス用のAnyconnect証明書ベース認証の設定](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。