Configure Cert Mapping for Secure Client Auth on FTD via FMC

Contents

Introduction

This document describes how to set up Cisco Secure Client with SSL on FTD via FMC using certificate mapping for authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defense (FTD) Virtual
- VPN Authentication Flow

Components Used

- Cisco Firepower Management Center for VMWare 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1

- Cisco Secure Client 5.1.3.62

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Certificate mapping is a method used in VPN connections where a client certificate is mapped to a local user account, or attributes within the certificate are used for authorization purposes.This is a process where a digital certificate is used as a means of identifying a user or device. By using certificate mapping, it leverages the SSL protocol to authenticate users without the need for them to input credentials.

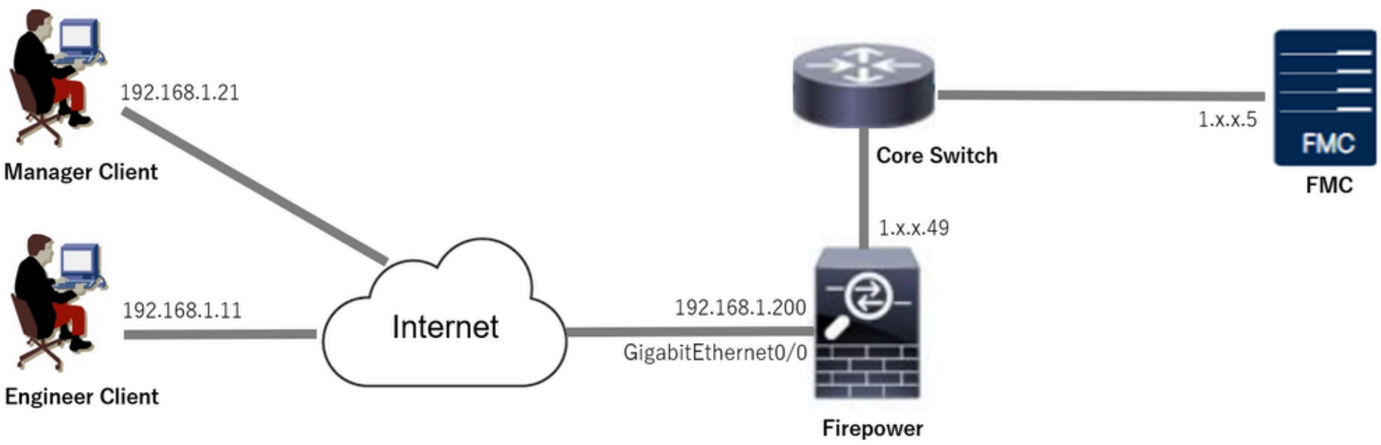
This document describes how to authenticate the Cisco Secure Client using the common name from an SSL certificate.

These certificates contain a common name within them, which is used for authorization purposes.

- CA : ftd-ra-ca-common-name
- Engineer VPN Client Certificate: vpnEngineerClientCN
- Manager VPN Client Certificate: vpnManagerClientCN
- Server Certificate: 192.168.1.200

Network Diagram

This image shows the topology that is used for the example of this document.



Network Diagram

Configurations

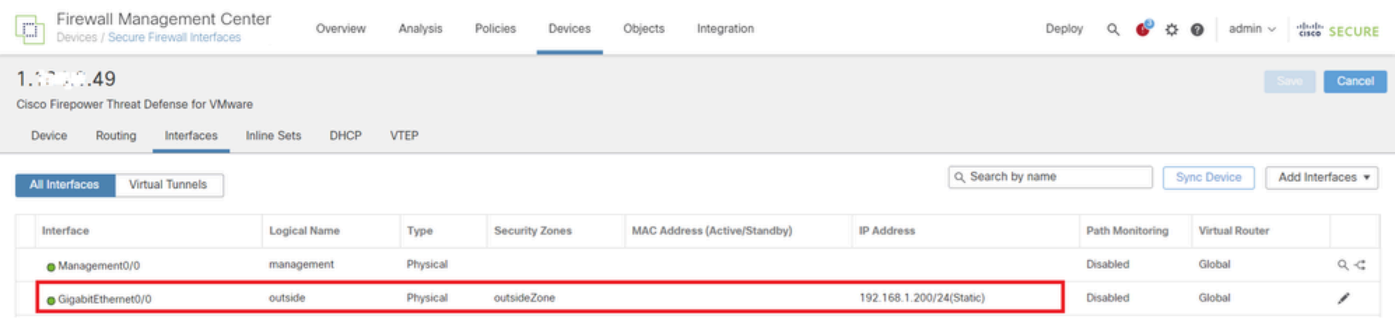
Configuration in FMC

Step 1. Configure FTD Interface

Navigate to**Devices > Device Management**, edit the target FTD device, config outside interface for FTD in**Interfaces**tab.

For GigabitEthernet0/0,

- Name: outside
- Security Zone: outsideZone
- IP Address: 192.168.1.200/24



1.[redacted].49

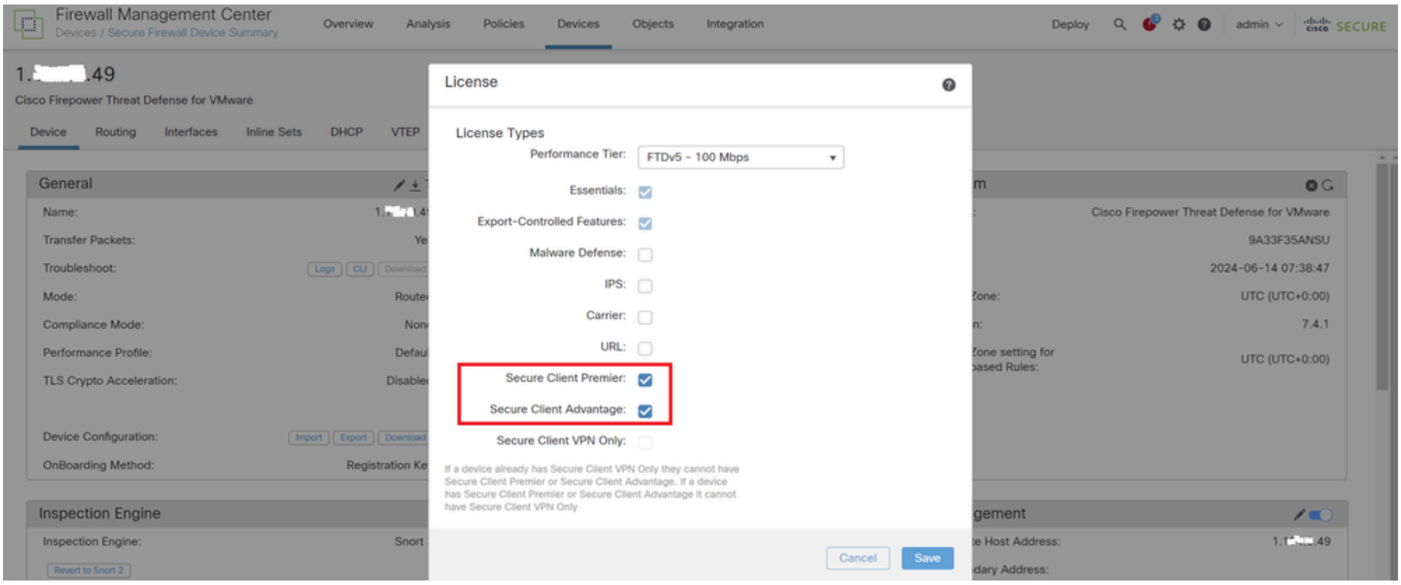
Cisco Firepower Threat Defense for VMware

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 Interface

Step 2. Confirm Cisco Secure Client License

Navigate to**Devices > Device Management**, edit the target FTD device, confirm the Cisco Secure Client license in**Device**tab.



1.[redacted].49

Cisco Firepower Threat Defense for VMware

License

License Types

Performance Tier: FTDv5 - 100 Mbps

Essentials: ☑

Export-Controlled Features: ☑

Malware Defense: □

IPS: □

Carrier: □

URL: □

Secure Client Premier: ☑

Secure Client Advantage: ☑

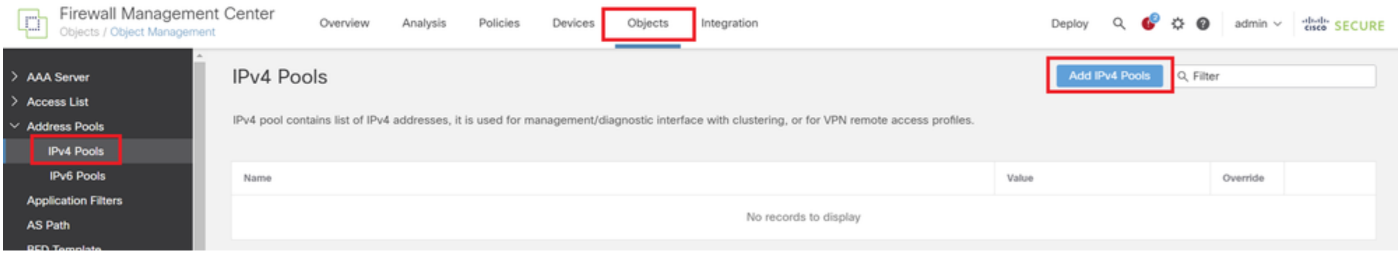
Secure Client VPN Only: □

If a device already has Secure Client VPN Only they cannot have Secure Client Premier or Secure Client Advantage. If a device has Secure Client Premier or Secure Client Advantage it cannot have Secure Client VPN Only

Secure Client License

Step 3. Add IPv4 Address Pool

Navigate to**Object > Object Management > Address Pools > IPv4 Pools**, click**Add IPv4 Pools**button.



IPv4 Pools

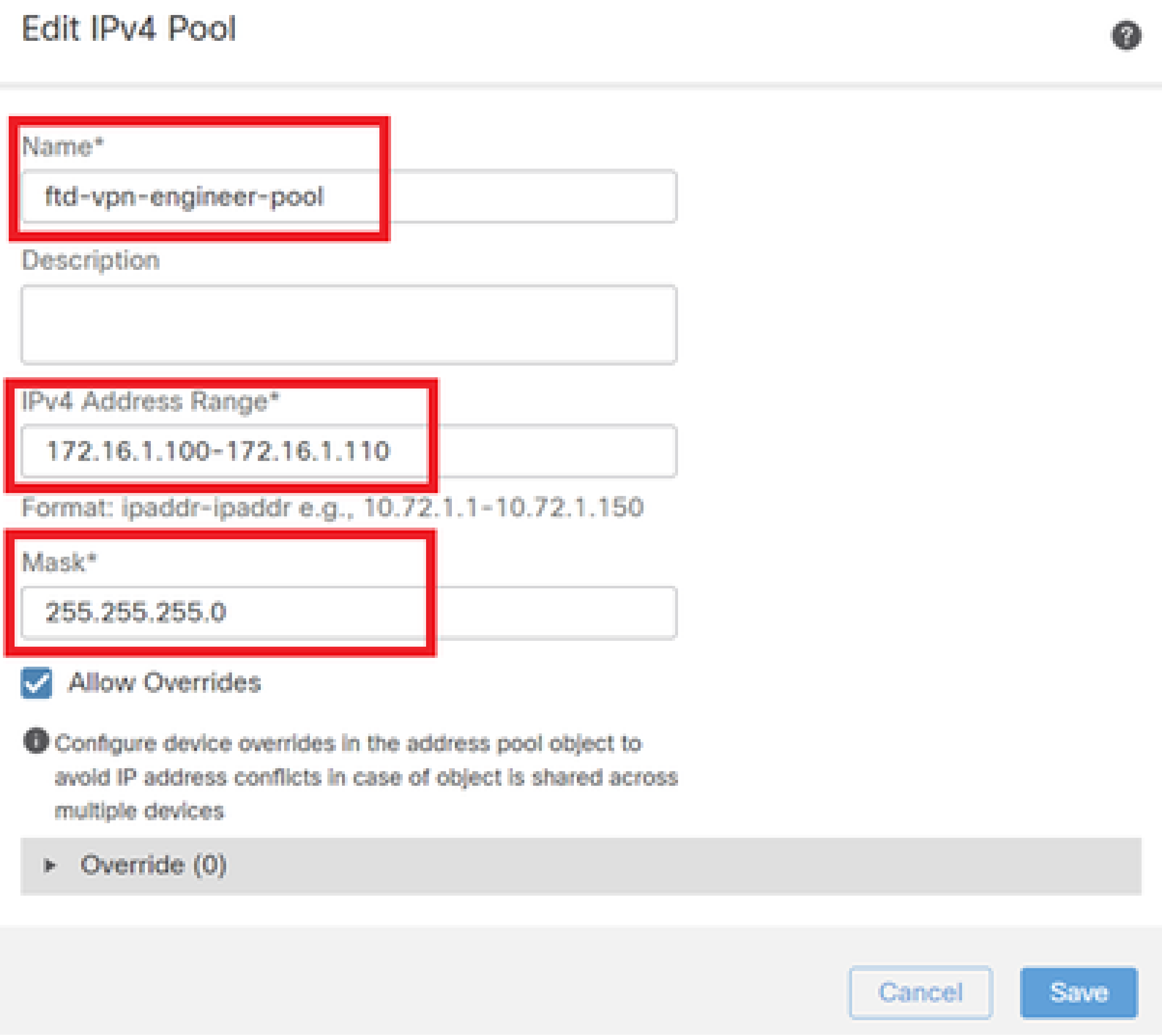
IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.

Name	Value	Override
No records to display		

Add IPv4 Address Pool

Input necessary information to create an IPv4 address pool for engineer VPN client.

- Name: ftd-vpn-engineer-pool
- IPv4 Address Range: 172.16.1.100-172.16.1.110
- Mask: 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

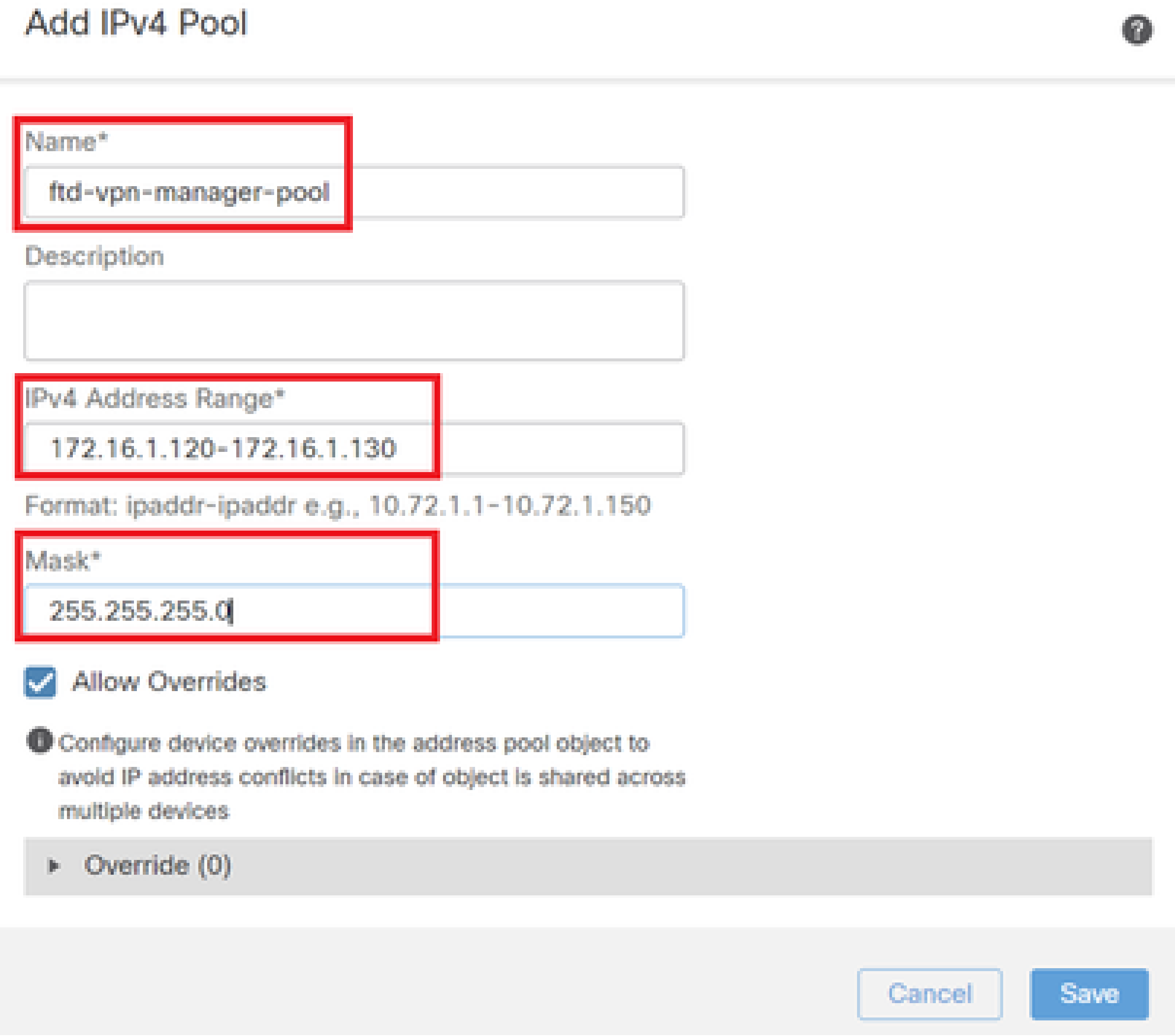
☑ Allow Overrides

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

IPv4 Address Pool for Engineer VPN Client

Input necessary information to create an IPv4 address pool for manager VPN client.

- Name: ftd-vpn-manager-pool
- IPv4 Address Range: 172.16.1.120-172.16.1.130
- Mask: 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

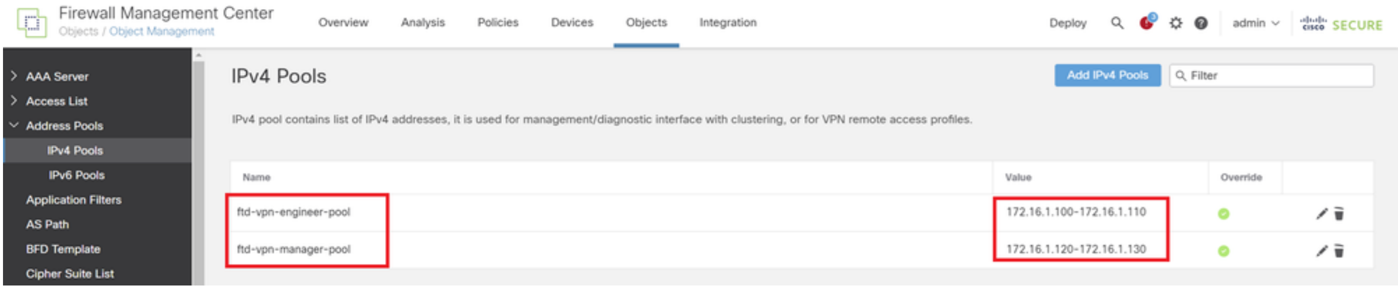
Mask*
255.255.255.0

☑ Allow Overrides

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

IPv4 Address Pool for Manager VPN Client

Confirm the new IPv4 address pools.



IPv4 Pools

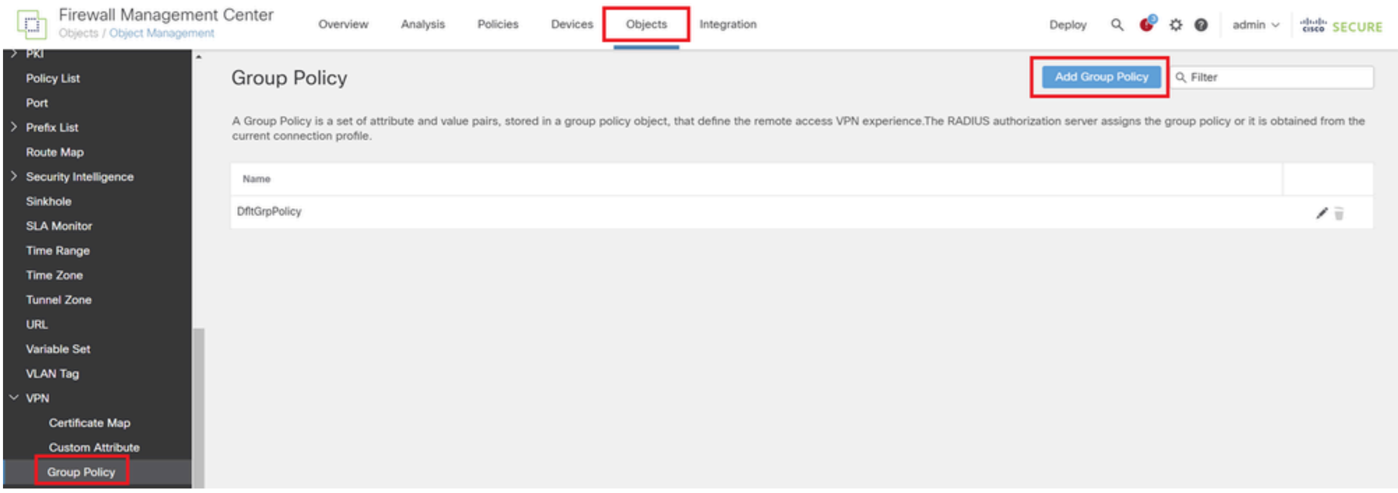
IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.

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	●

New IPv4 Address Pools

Step 4. Add Group Policy

Navigate to**Object > Object Management > VPN > Group Policy**, click**Add Group Policy**button.



Group Policy

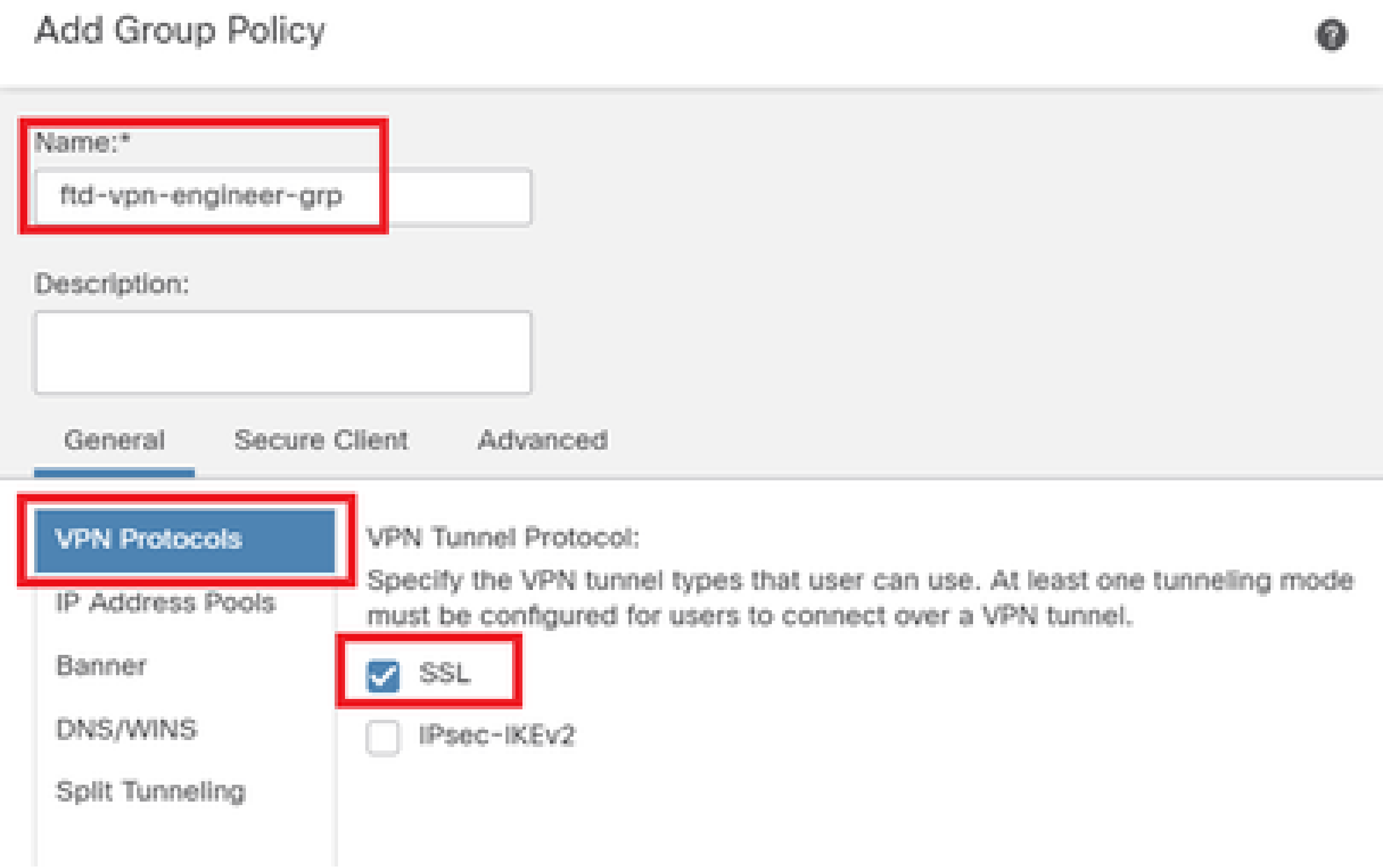
A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience.The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

Name
DfltGrpPolicy

Add Group Policy

Input necessary information to create a group policy for the engineer VPN client.

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



Add Group Policy

Name:* ftd-vpn-engineer-grp

Description:

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.

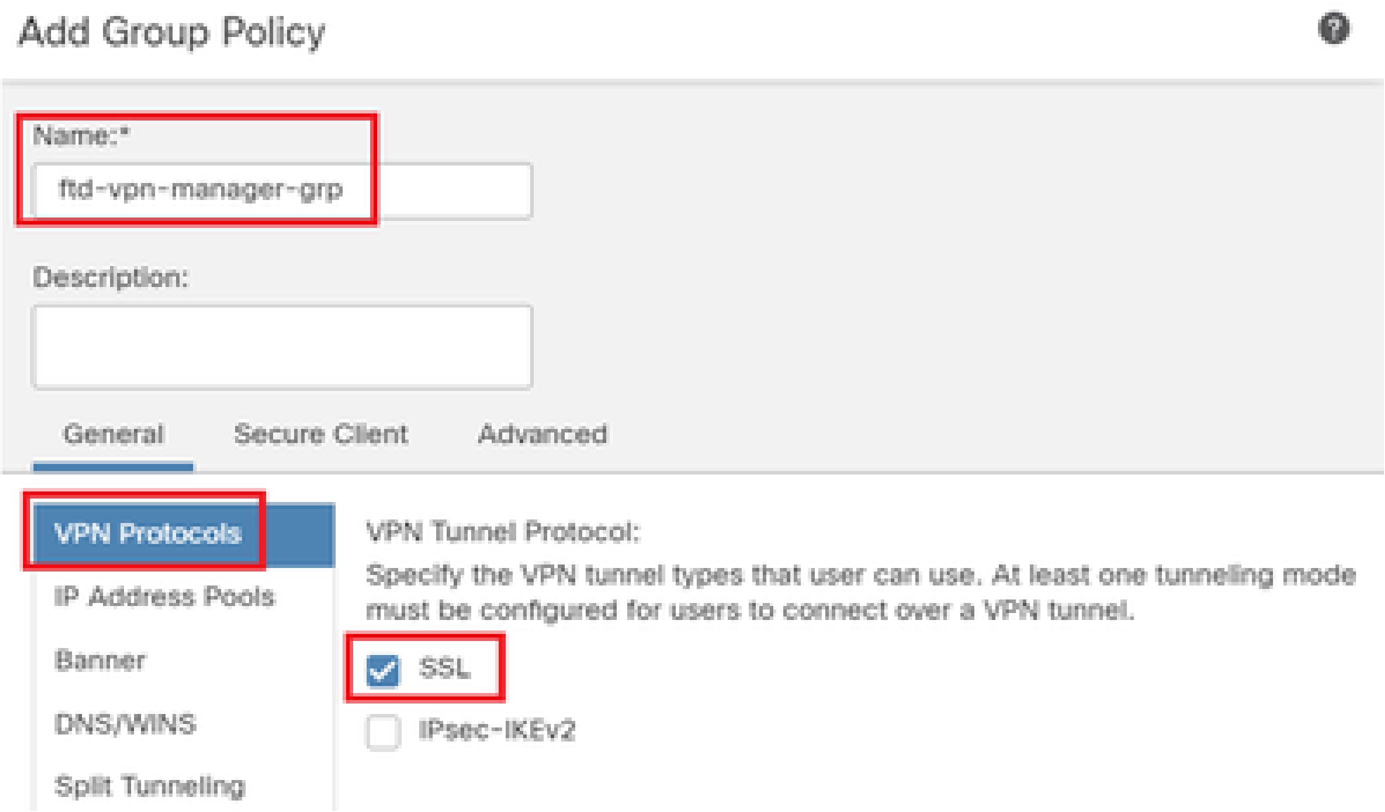
☑ SSL

□ IPsec-IKEv2

Group Policy for Engineer VPN Client

Input necessary information to create a group policy for manager VPN client.

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



Add Group Policy

Name:* ftd-vpn-manager-grp

Description:

VPN Tunnel Protocol:

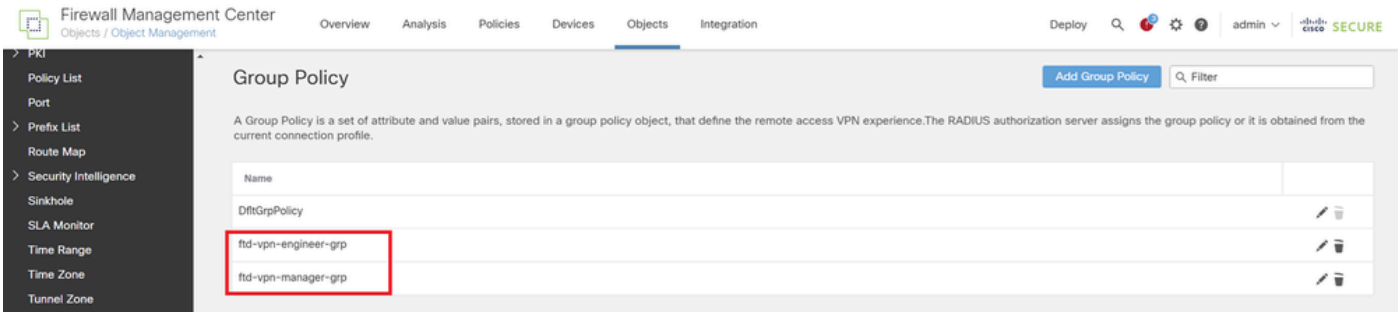
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

☑ SSL

□ IPsec-IKEv2

Group Policy for Manager VPN Client

Confirm the new group policies.



Group Policy

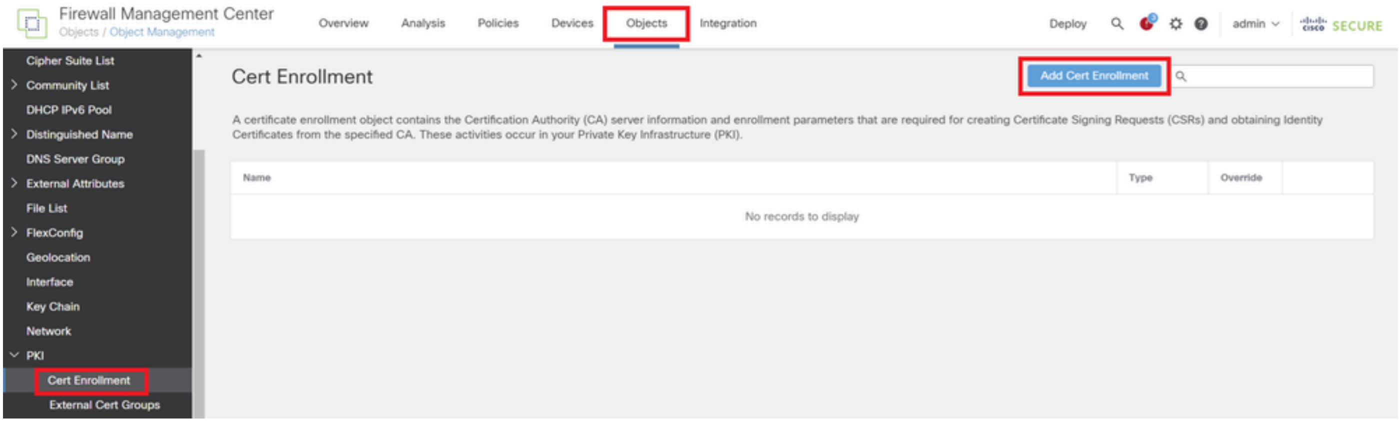
A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience.The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

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

New Group Policies

Step 5. Add FTD Certificate

Navigate to**Object > Object Management > PKI > Cert Enrollment**, click**Add Cert Enrollment**button.



Cert Enrollment

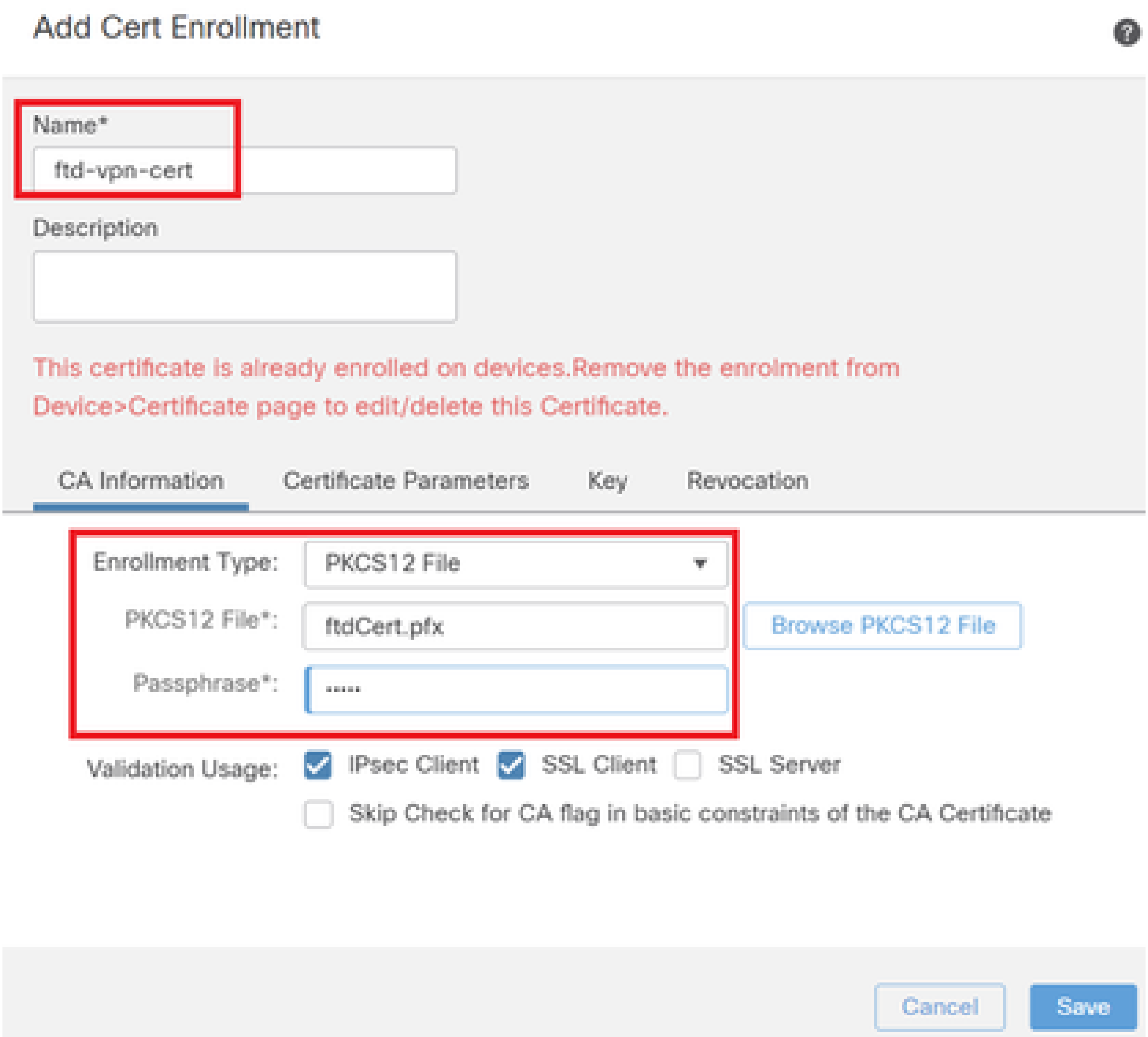
A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure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

Name	Type	Override
No records to display		

Add Certificate Enrollment

Input necessary information for FTD certificate and import a PKCS12 file from local computer.

- Name: ftd-vpn-cert
- Enrollment Type: PKCS12 File



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.

Enrollment Type: PKCS12 File

PKCS12 File*: ftdCert.pfx

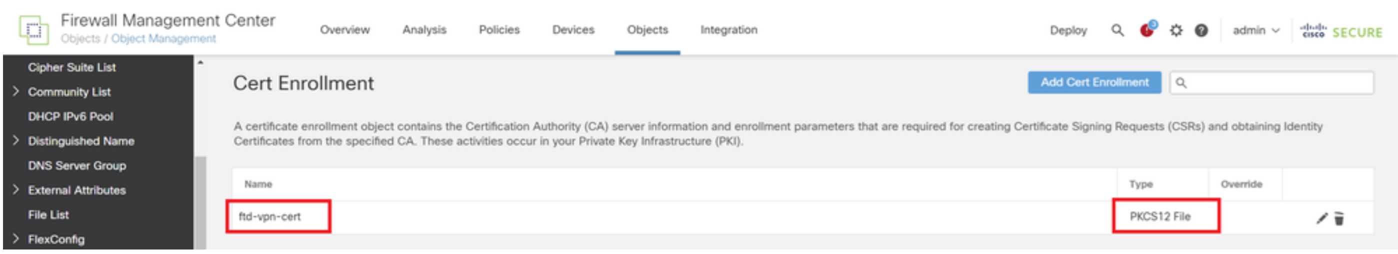
Passphrase*: •••••

Validation Usage: ☑ IPsec Client ☑ SSL Client □ SSL Server

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

Details of Certificate Enrollment

Confirm the new certificate enrollment.



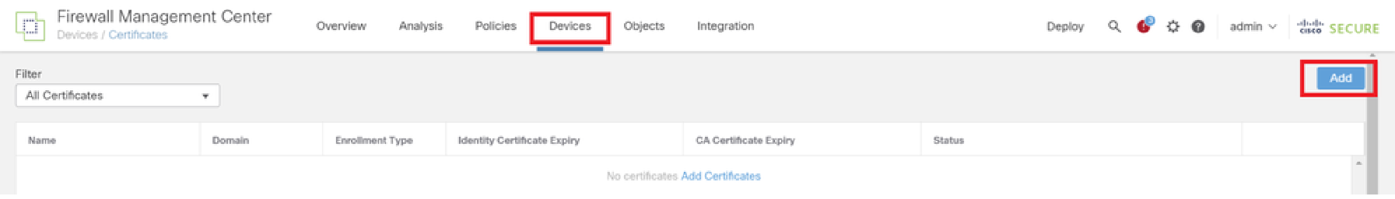
Cert Enrollment

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	

New Certificate Enrollment

Navigate to**Devices** > **Certificates**, click**Add** button.



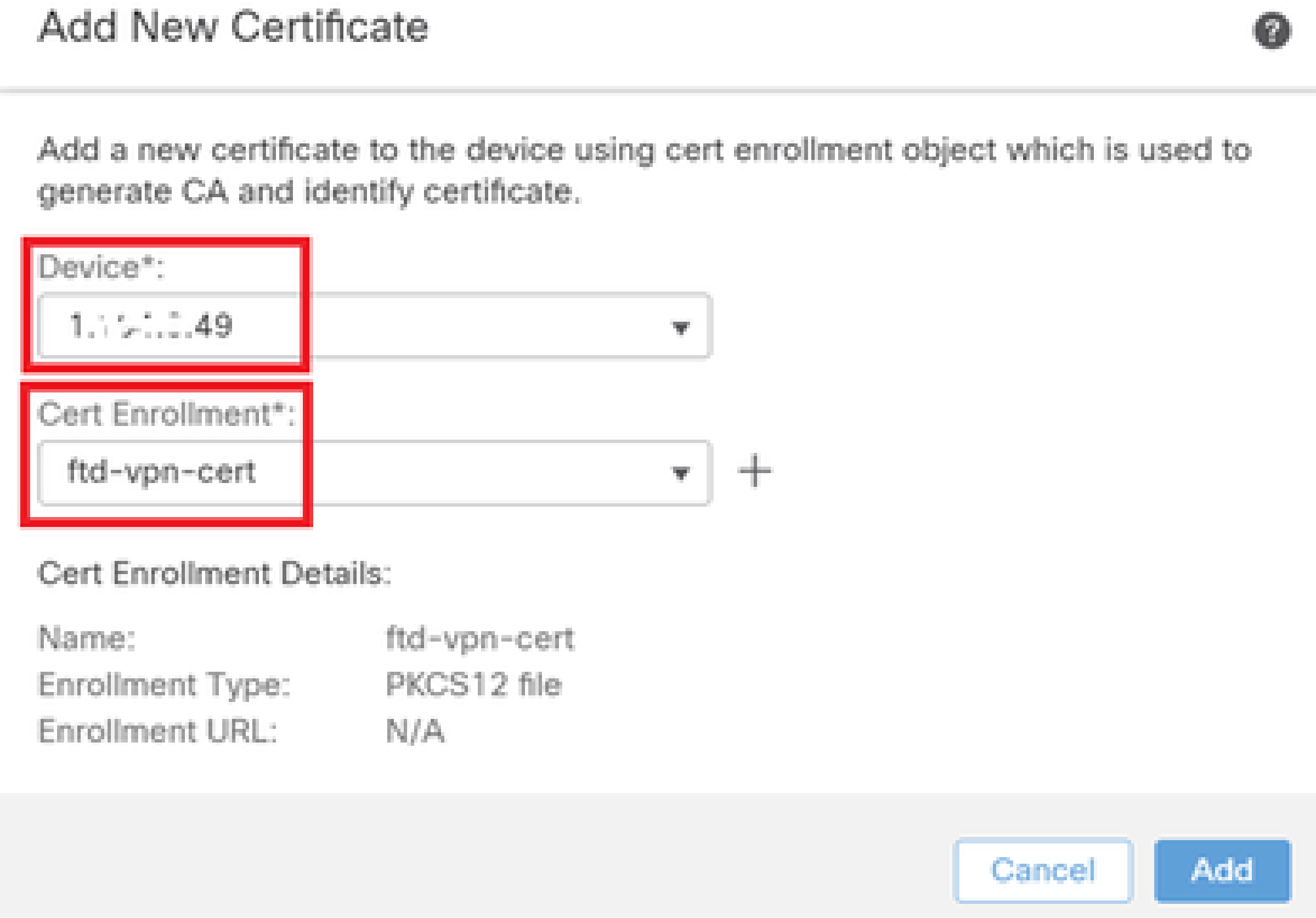
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status

No certificates Add Certificates

Add FTD Certificate

Input necessary information to bind the new certificate enrollment to FTD.

- Device: 1.x.x.49
- Cert Enrollment: 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.[redacted].49

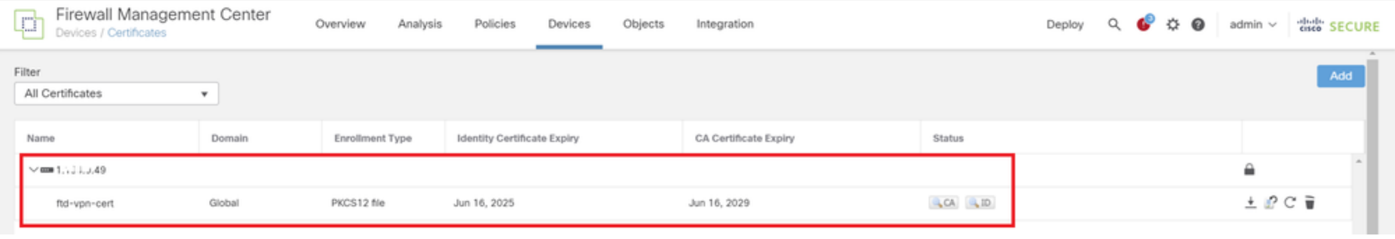
Cert Enrollment*: ftd-vpn-cert

Cert Enrollment Details:

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

Bind Certificate to FTD

Confirm the status of the certificate binding.

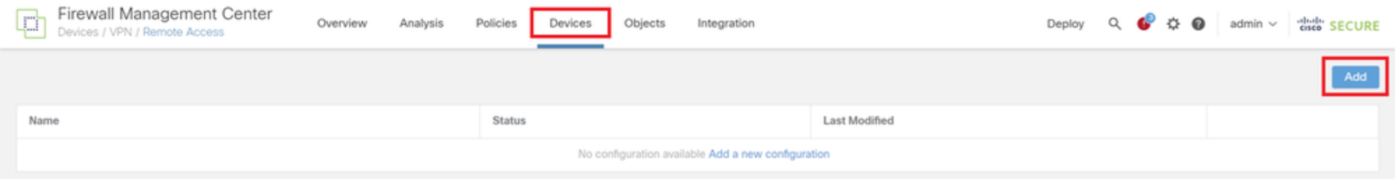


Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
1.[redacted].49					
ftd-vpn-cert	Global	PKCS12 file	Jun 16, 2025	Jun 16, 2029	CA ID

Status of Certificate Binding

Step 6. Add Policy Assignment for Engineer Connection Profile

Navigate to**Devices > VPN > Remote Access**, click**Add**button.


Firewall Management Center
Devices / VPN / Remote Access

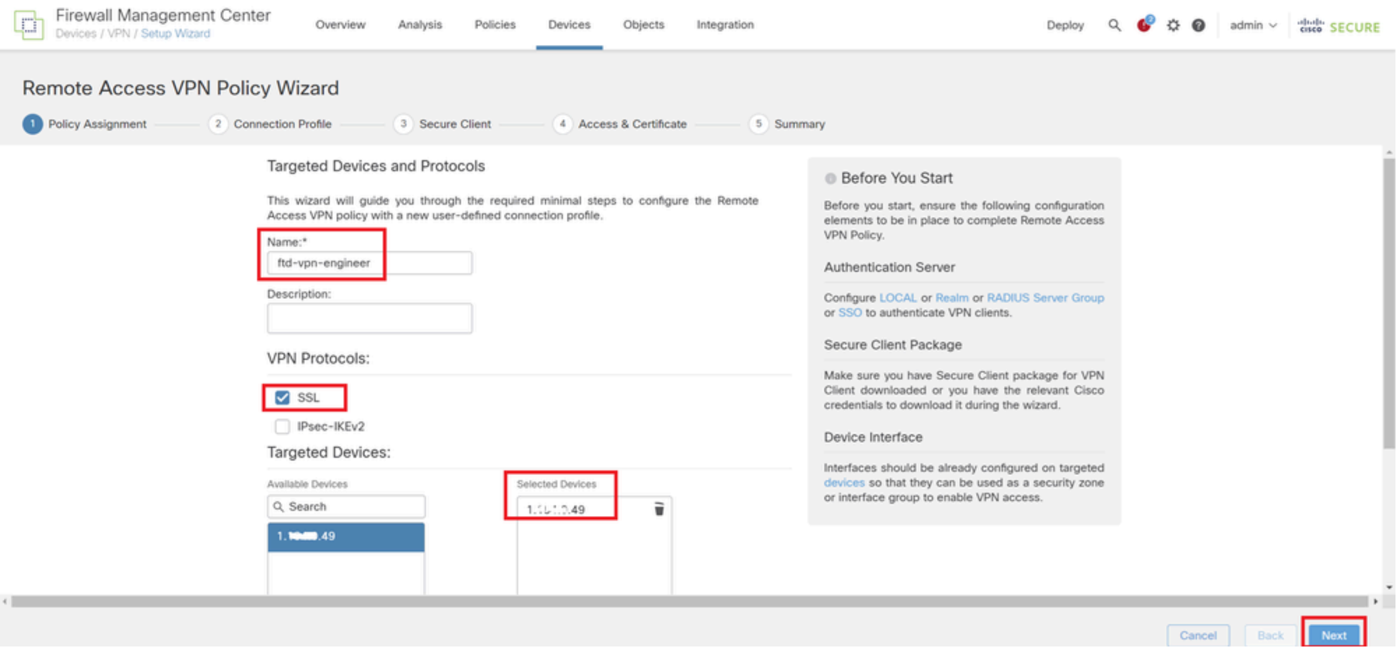
Name	Status	Last Modified

No configuration available Add a new configuration

Add Remote Access VPN

Input necessary information and click**Next**button.

- Name: ftd-vpn-engineer
- VPN Protocols: SSL
- Targeted Devices: 1.x.x.49


Firewall Management Center
Devices / VPN / Setup Wizard

Remote Access VPN Policy Wizard

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

Targeted Devices and Protocols

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

Name:* ftd-vpn-engineer

Description:

VPN Protocols:

☑ SSL

□ IPsec-IKEv2

Targeted Devices:

Available Devices

Search

1.[redacted].49

Selected Devices

1.[redacted].49

Before You Start

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

Authentication Server

Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.

Secure Client Package

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

Device Interface

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

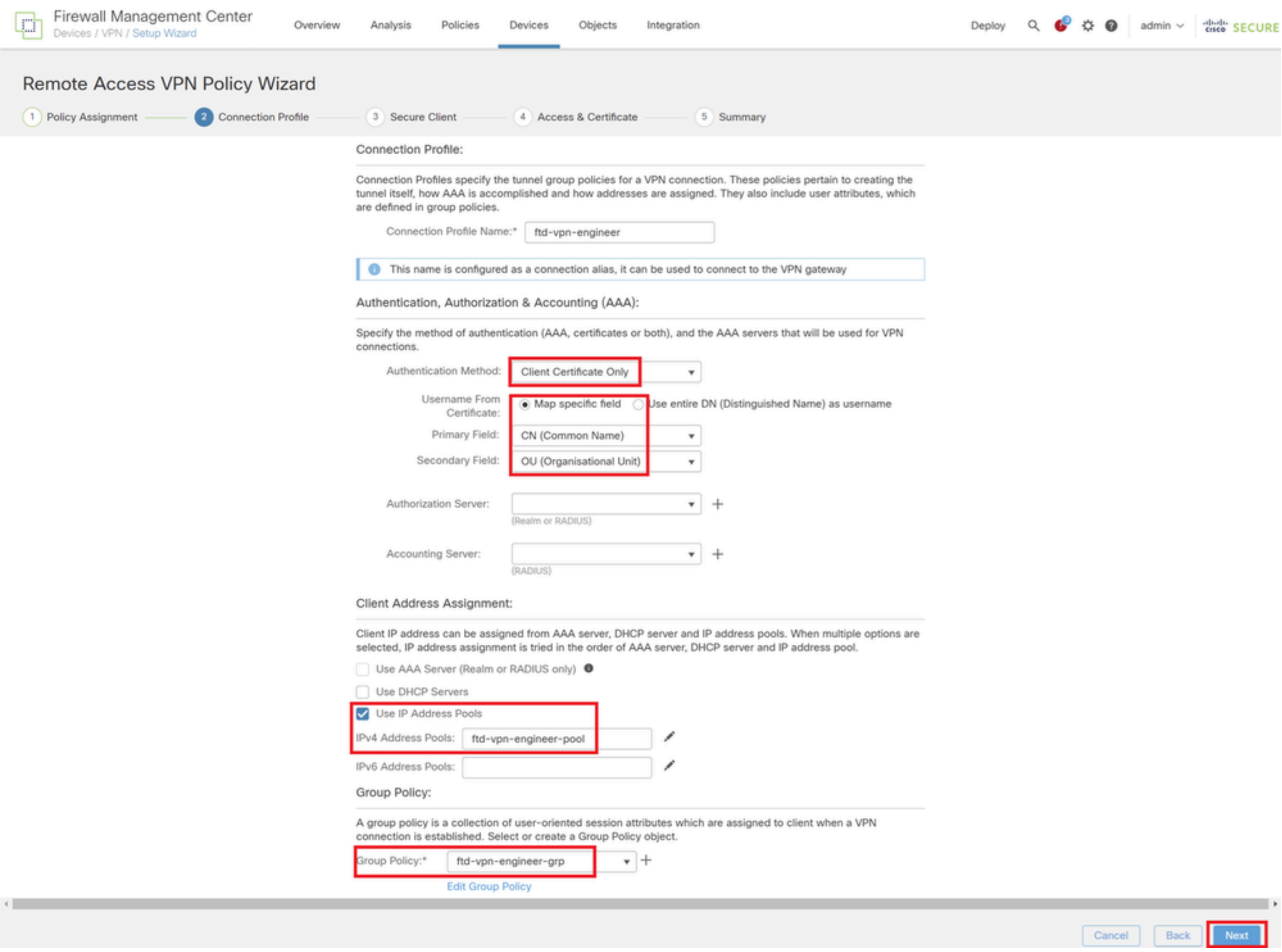
Policy Assignment

Step 7. Configure Details for Engineer Connection Profile

Input necessary information and click**Next**button.

- Authentication Method: Client Certificate Only
- Username From Certificate: Map specific field
- Primary Field: CN (Common Name)
- Secondary Field: OU (Organizational Unit)

- IPv4 Address Pools: ftd-vpn-engineer-pool
- Group Policy: 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:* ftd-vpn-engineer

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

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: Client Certificate Only

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

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Authorization Server: (Realm or RADIUS) +

Accounting Server: (RADIUS) +

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: ftd-vpn-engineer-pool

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:* ftd-vpn-engineer-grp +

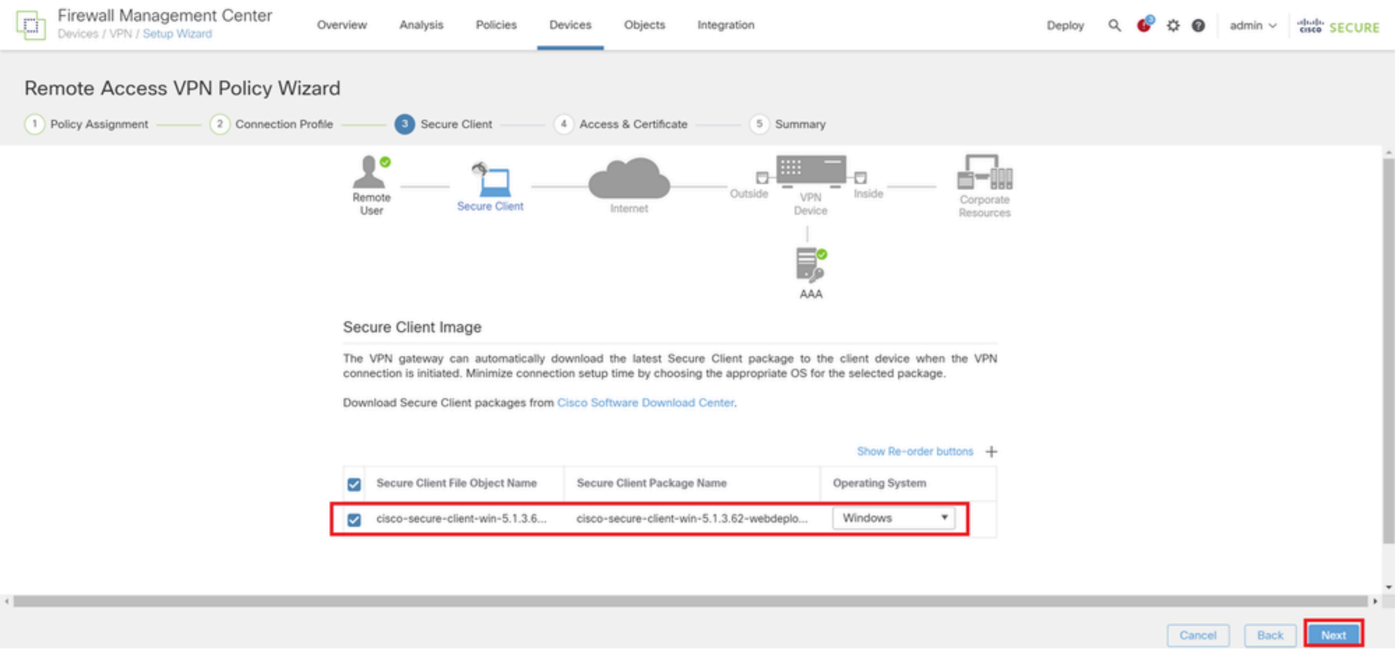
Edit Group Policy

Cancel Back Next

Details of Connection Profile

Step 8. Configure Secure Client Image for Engineer Connection Profile

Select **secure client image file** and click**Next**button.



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 +

☑	Secure Client File Object Name	Secure Client Package Name	Operating System
☑	cisco-secure-client-win-5.1.3.6...	cisco-secure-client-win-5.1.3.62-webdeplo...	Windows

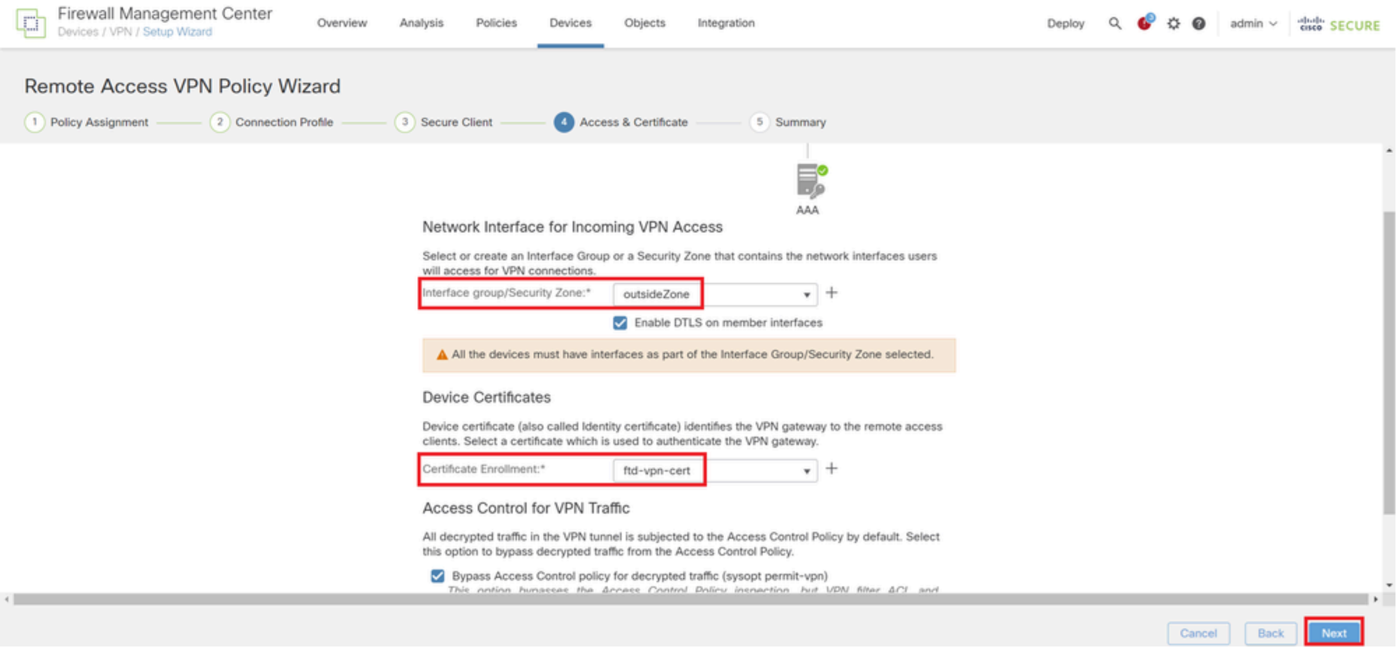
Cancel Back Next

Select Secure Client

Step 9. Configure Access and Certificate for Engineer Connection Profile

Select value for **Interface group/Security Zone** and **Certificate Enrollment** items, click **Next** button.

- Interface group/Security Zone: outsideZone
- Certificate Enrollment: ftd-vpn-cert



Remote Access VPN Policy Wizard

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

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.

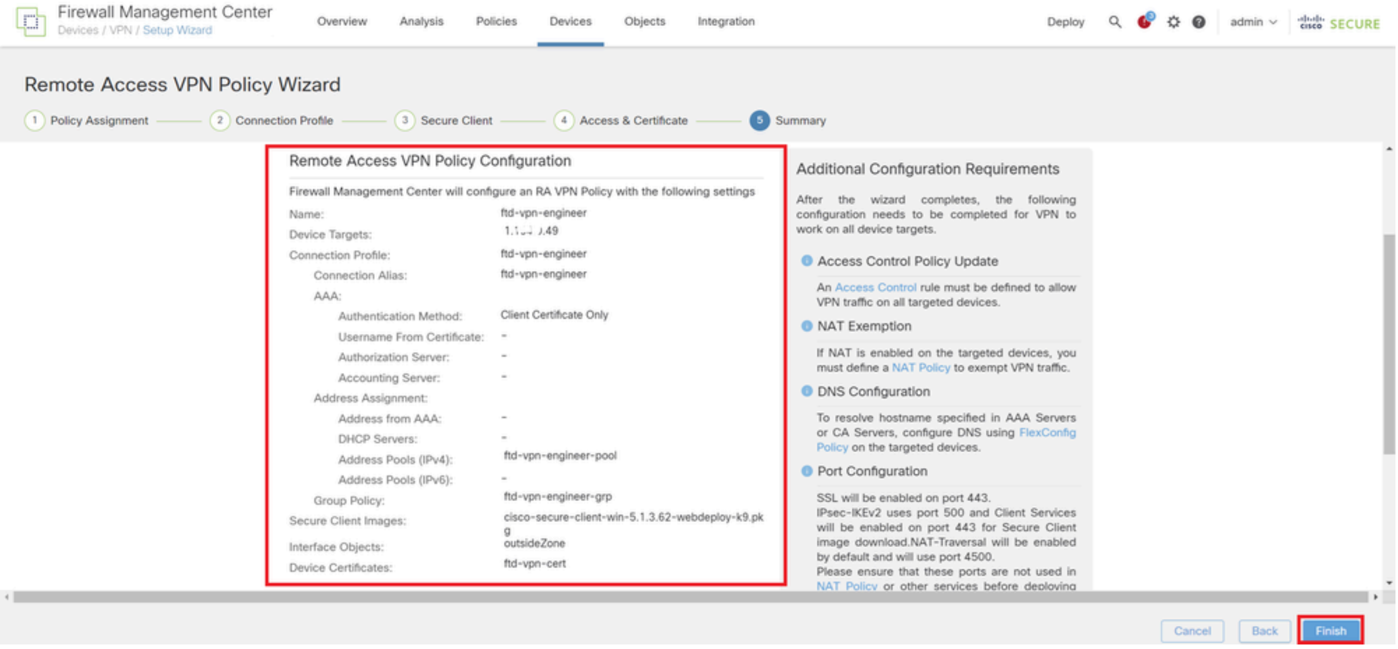
☑ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

This option bypasses the Access Control Policy inspection, but VPN filter ACL and

Details of Access and Certificate

Step 10. Confirm Summary for Engineer Connection Profile

Confirm the information entered for remote access VPN policy and click **Finish** button.



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[redacted].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.pkg
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.

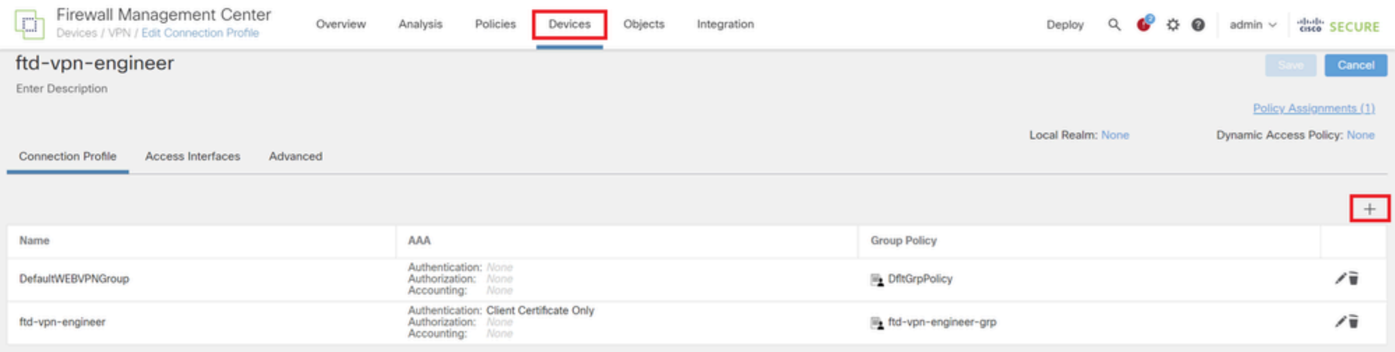
Port Configuration

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

Details of Remote Access VPN Policy

Step 11. Add Connection Profile for Manager VPN Client

Navigate to **Devices > VPN > Remote Access > Connection Profile**, click **+** button.



ftd-vpn-engineer

Enter Description

Policy Assignments (1)

Local Realm: None

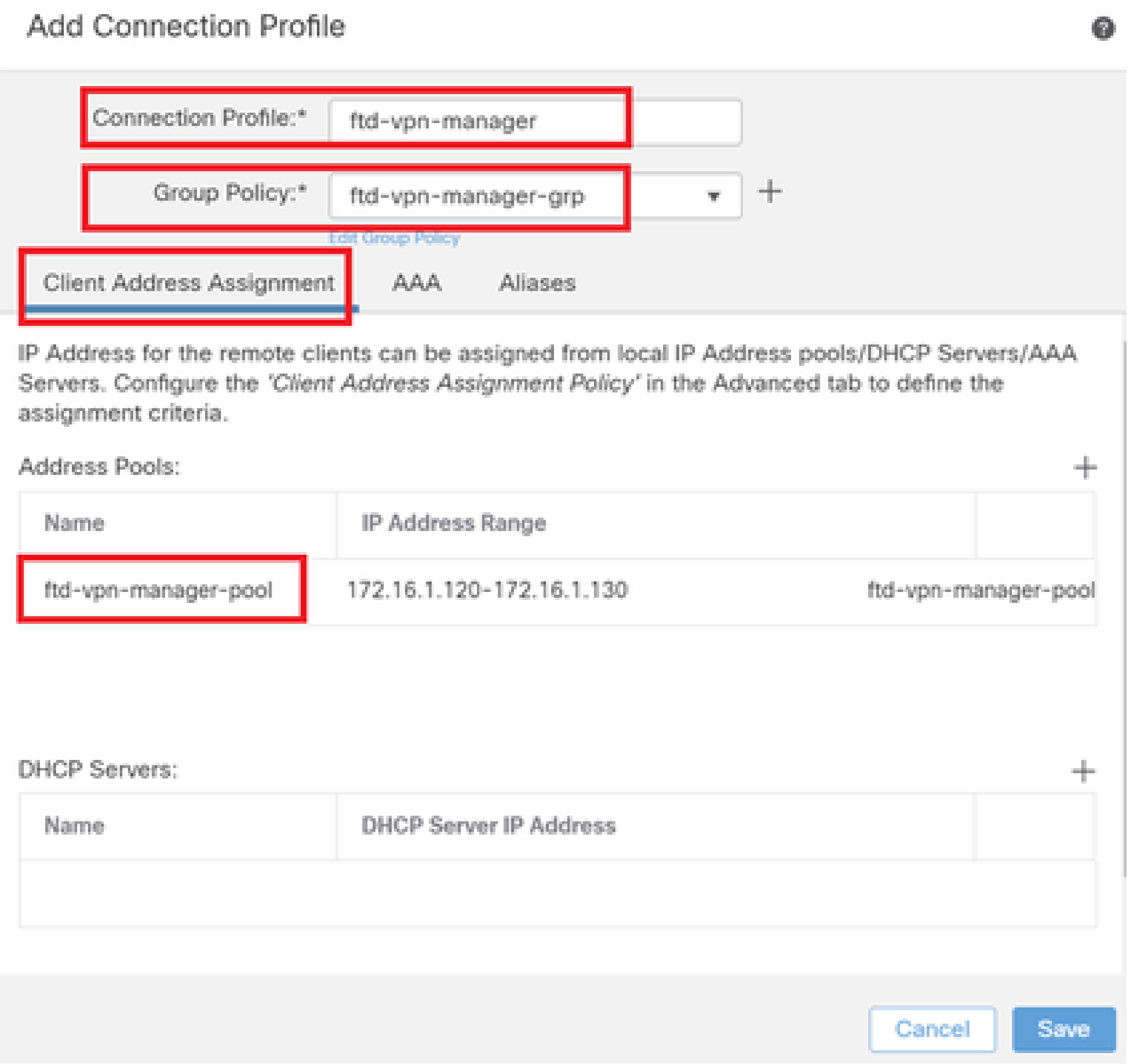
Dynamic Access Policy: None

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

Add Connection Profile for Manager VPN Client

Input necessary information for connection profile and click **Save** button.

- Name: ftd-vpn-manager
- Group Policy: ftd-vpn-manager-grp
- IPv4 Address Pools: ftd-vpn-manager-pool



Connection Profile:* ftd-vpn-manager

Group Policy:* ftd-vpn-manager-grp

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:

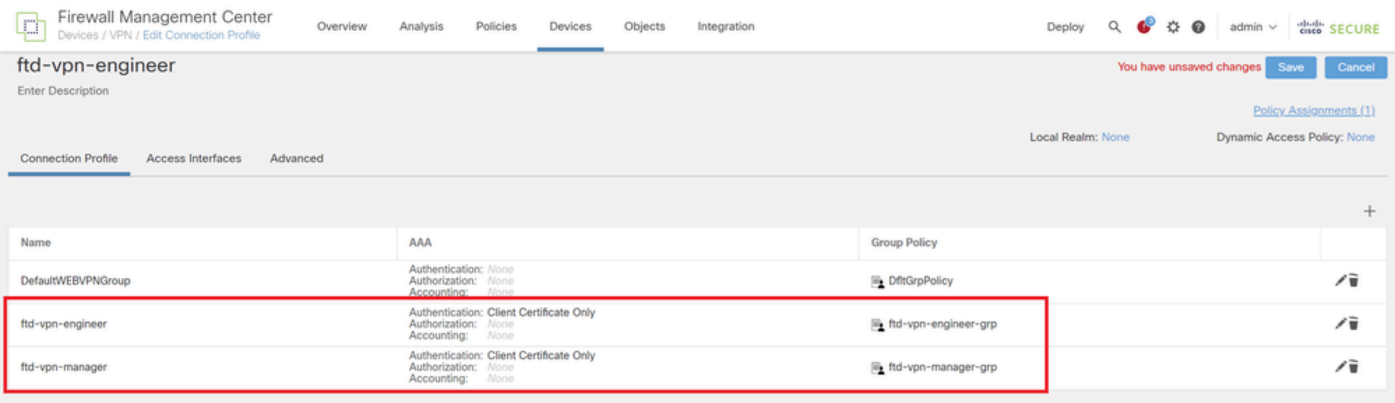
Name	IP Address Range	
ftd-vpn-manager-pool	172.16.1.120-172.16.1.130	ftd-vpn-manager-pool

DHCP Servers:

Name	DHCP Server IP Address	

Details of Connection Profile for Manager VPN Client

Confirm new added connection profiles.



ftd-vpn-engineer

Enter Description

Local Realm: None

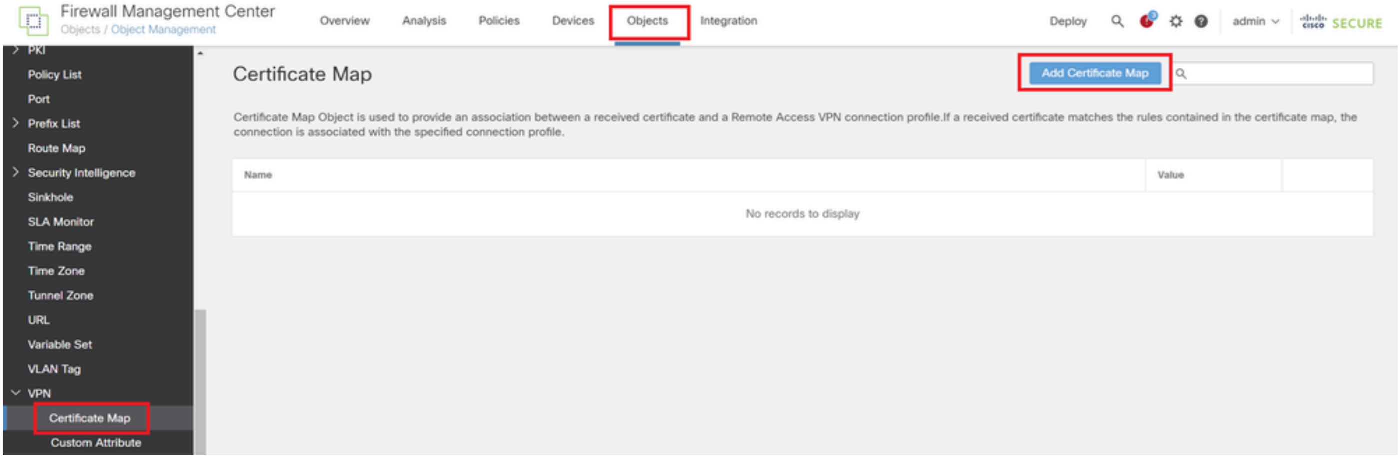
Dynamic Access Policy: None

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	
ftd-vpn-manager	Authentication: Client Certificate Only Authorization: None Accounting: None	ftd-vpn-manager-grp	

Confirm Added Connection Profiles

Step 12. Add Certificate Map

Navigate to **Objects** > **Object Management** > **VPN** > **Certificate Map**, click **AddCertificate Map** button.



Certificate Map

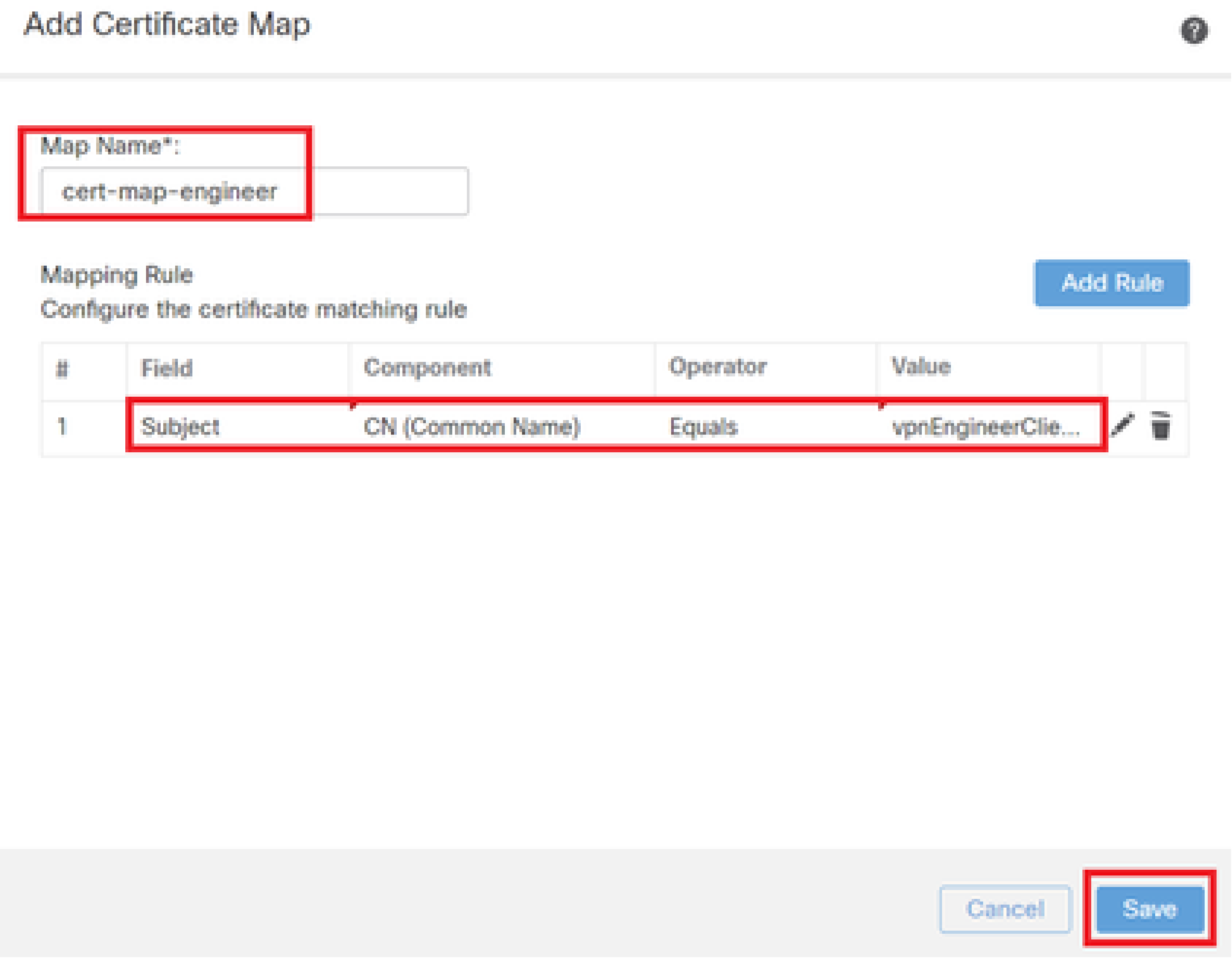
Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile.If a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile.

Name	Value
No records to display	

Add Certificate Map

Input necessary information for the certificate map of the engineer VPN client and click **Save** button.

- Map Name: cert-map-engineer
- Mapping Rule: CN (Common Name) Equals vpnEngineerClientCN



Add Certificate Map

Map Name*: cert-map-engineer

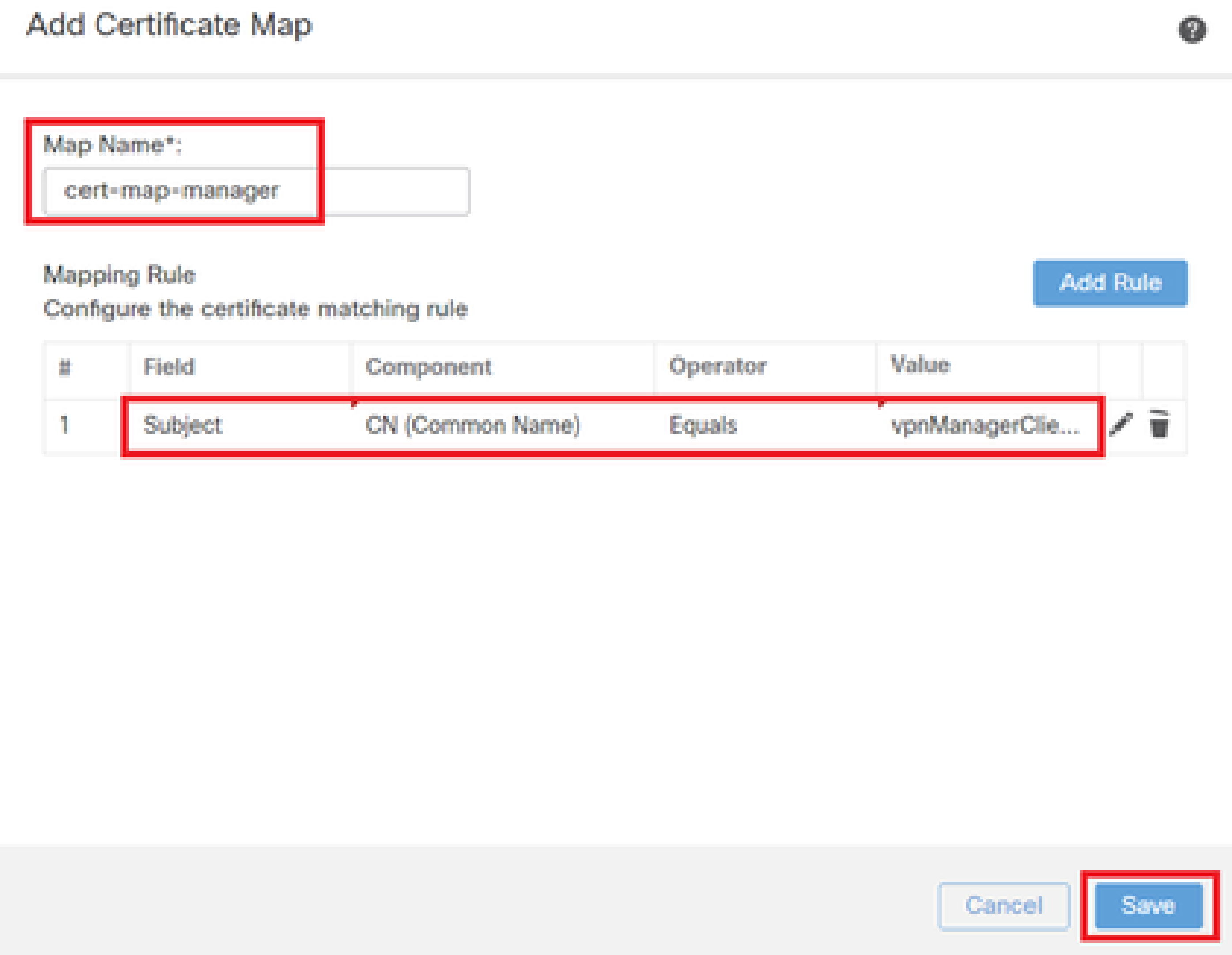
Mapping Rule
Configure the certificate matching rule

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

Certificate Map for Engineer Client

Input necessary information for the certificate map of the manager VPN client and click **Save** button.

- Map Name: cert-map-manager
- Mapping Rule: CN (Common Name) Equals vpnManagerClientCN



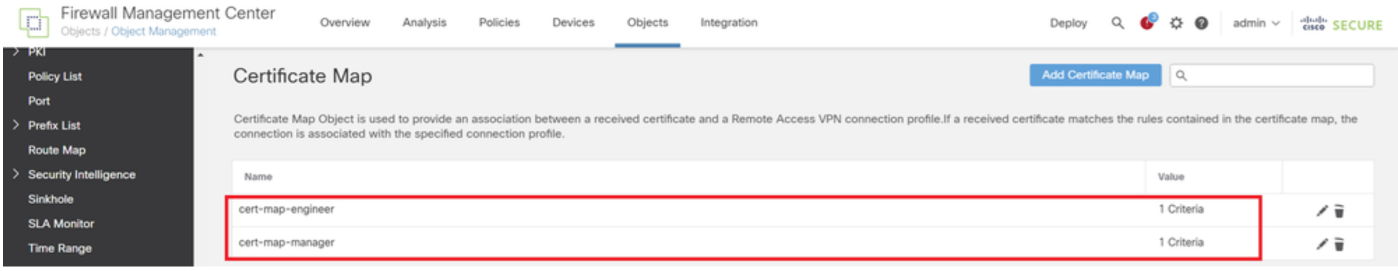
Map Name*: cert-map-manager

Mapping Rule
Configure the certificate matching rule

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

Certificate Map for Manager Client

Confirm new added certificate maps.



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.

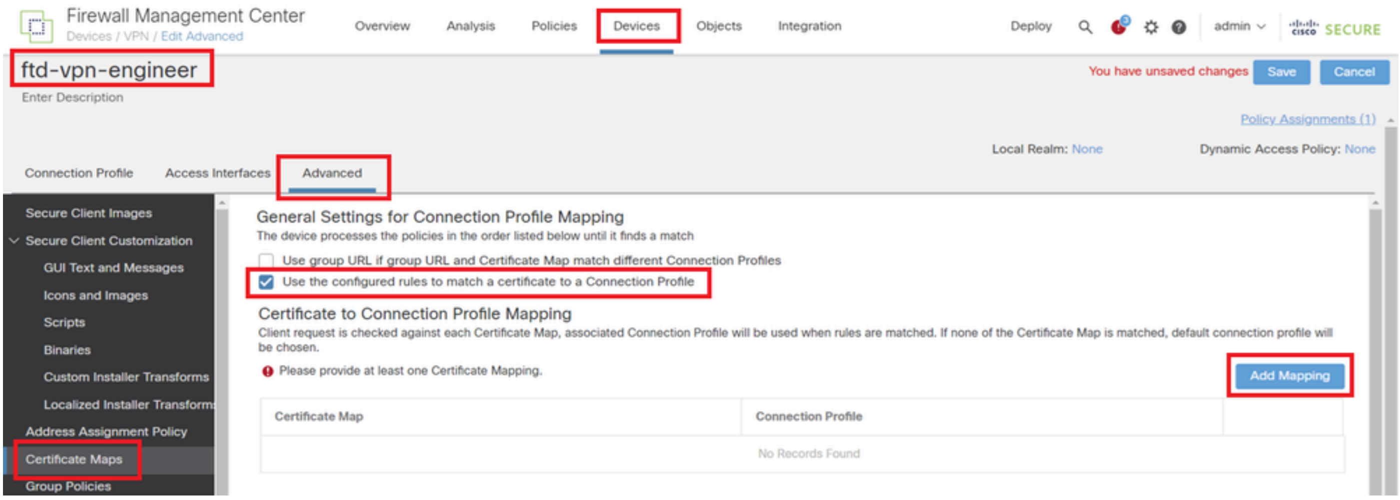
Name	Value
cert-map-engineer	1 Criteria
cert-map-manager	1 Criteria

New Certificate Maps

Step 13. Bind Certificate Map to Connection Profile

Navigate to **Devices > VPN > Remote Access**, edit **ftd-vpn-engineer**. Then, navigate to **Advanced**

> **Certificate Maps**, click **Add Mapping** button.



ftd-vpn-engineer

Enter Description

You have unsaved changes

Local Realm: None

Dynamic Access Policy: None

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.

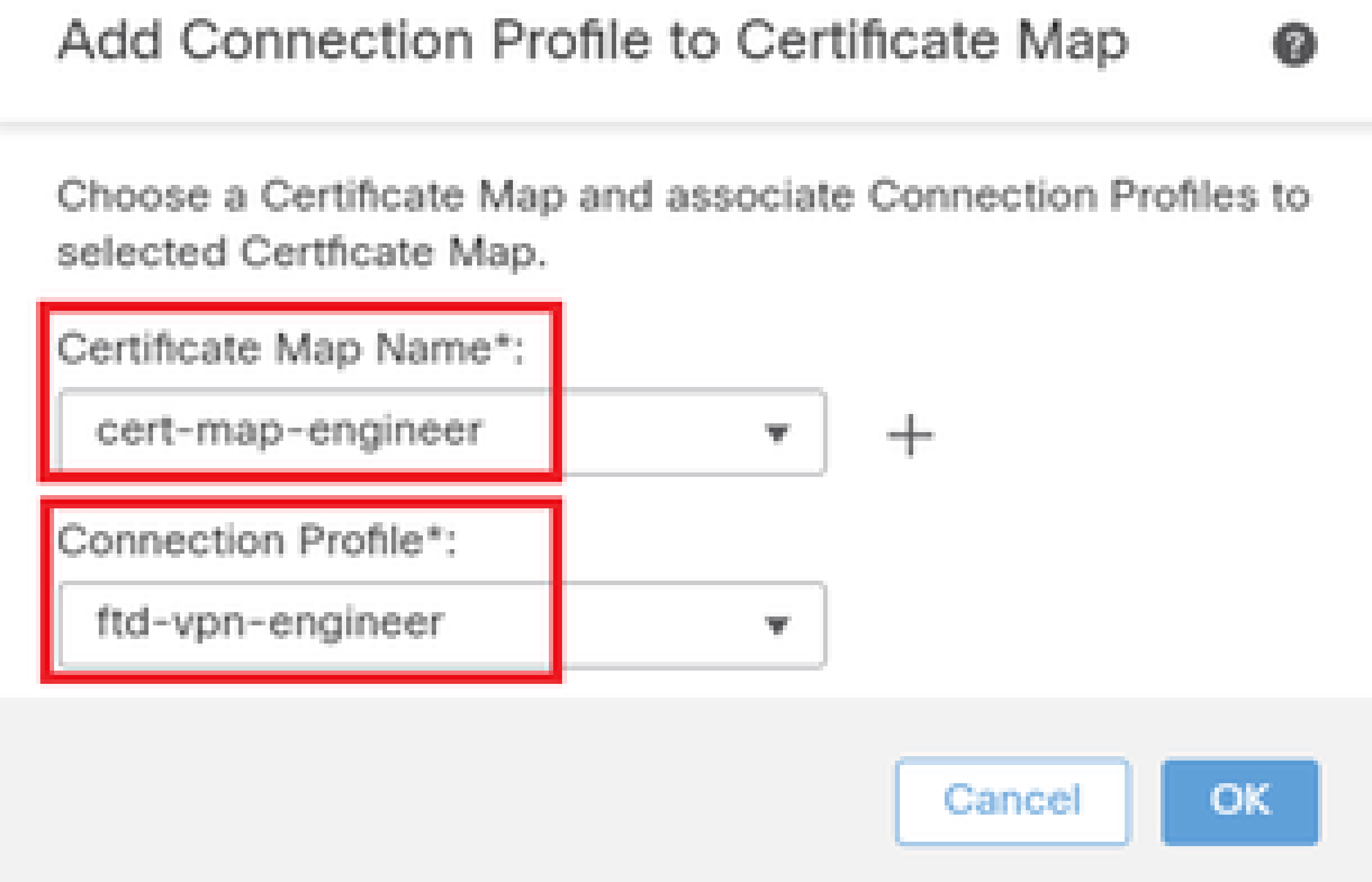
Please provide at least one Certificate Mapping.

Certificate Map	Connection Profile	
No Records Found		

Bind Certificate Map

Binding certificate map to connection profile for engineer VPN client.

- Certificate Map Name: cert-map-engineer
- Connection Profile: ftd-vpn-engineer



Add Connection Profile to Certificate Map

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

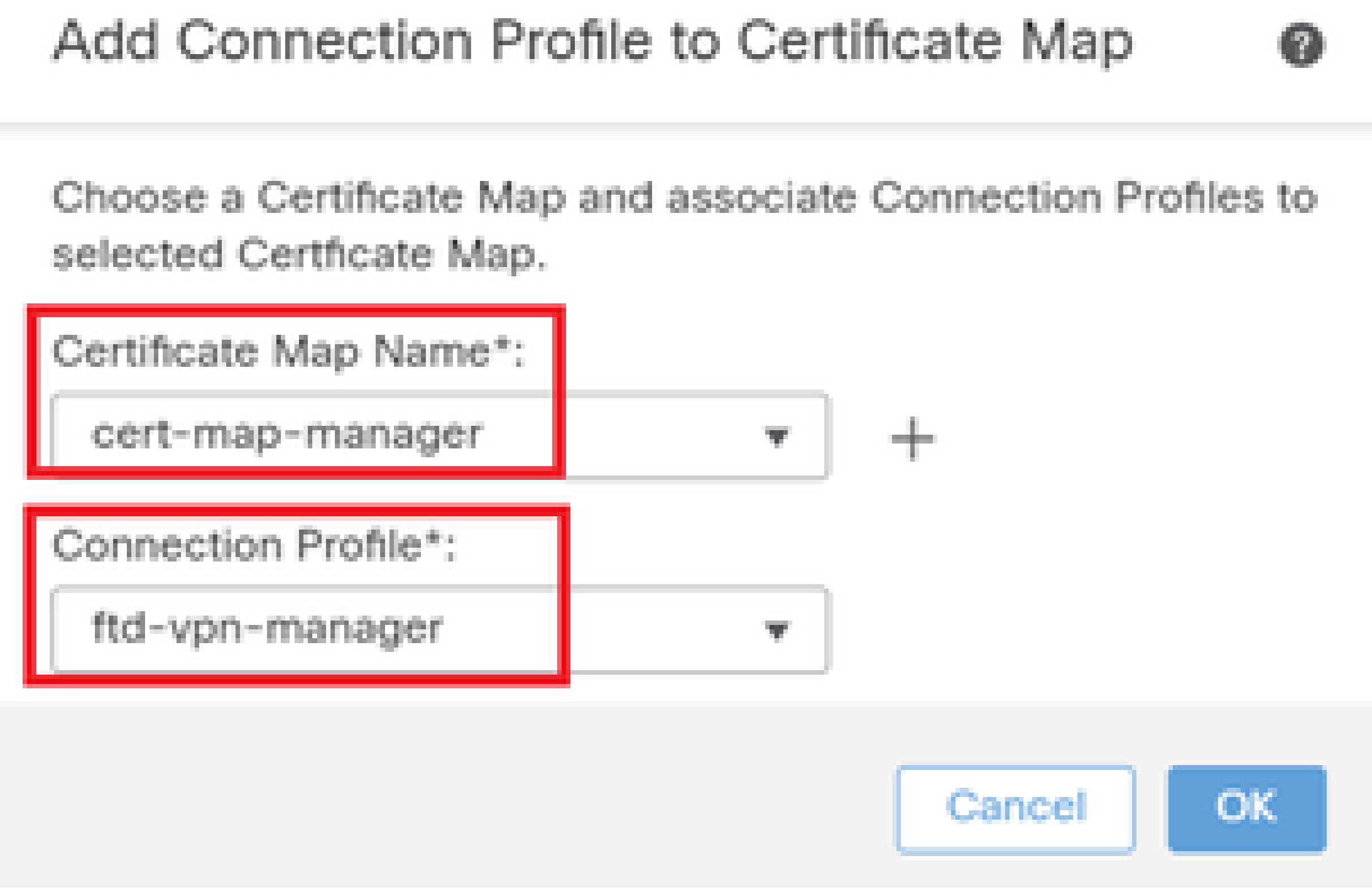
Certificate Map Name*: cert-map-engineer

Connection Profile*: ftd-vpn-engineer

Binding Certificate Map for Engineer VPN Client

Binding certificate map to connection profile for manager VPN client.

- Certificate Map Name: cert-map-manager
- Connection Profile: ftd-vpn-manager



Add Connection Profile to Certificate Map

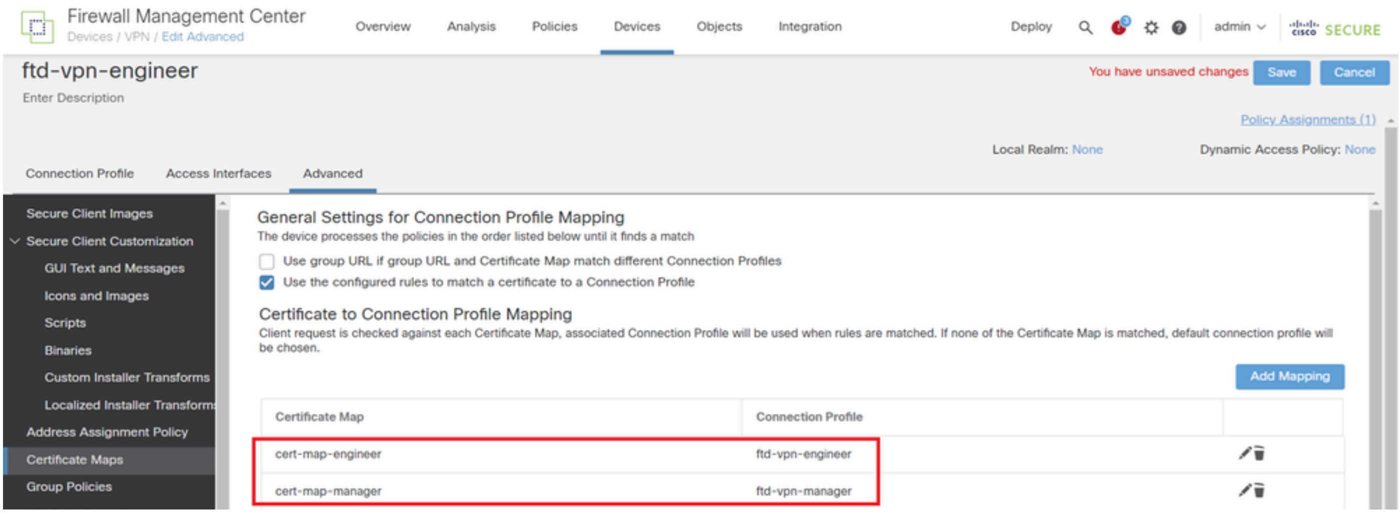
Choose a Certificate Map and associate Connection Profiles to selected Certficate Map.

Certificate Map Name*: cert-map-manager

Connection Profile*: ftd-vpn-manager

Binding Certificate Map for Manager VPN Client

Confirm the setting of certificate binding.



ftd-vpn-engineer

Enter Description

You have unsaved changes

Policy Assignments (1)

Local Realm: None

Dynamic Access Policy: None

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

Confirm Certificate Binding

Confirm in FTD CLI

Confirm the VPN connection settings in the FTD CLI after deployment from the FMC.

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
```

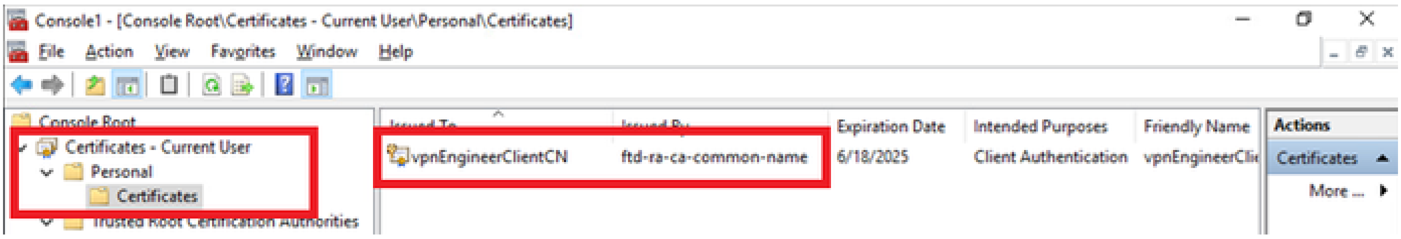
```
security-level 0
ip address 192.168.1.200 255.255.255.0

// 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
```

Confirm in VPN Client

Step 1. Confirm Client Certificate

In engineer VPN client, navigate to**Certificates - Current User** > **Personal** > **Certificates**, check the client certificate used for authentication.



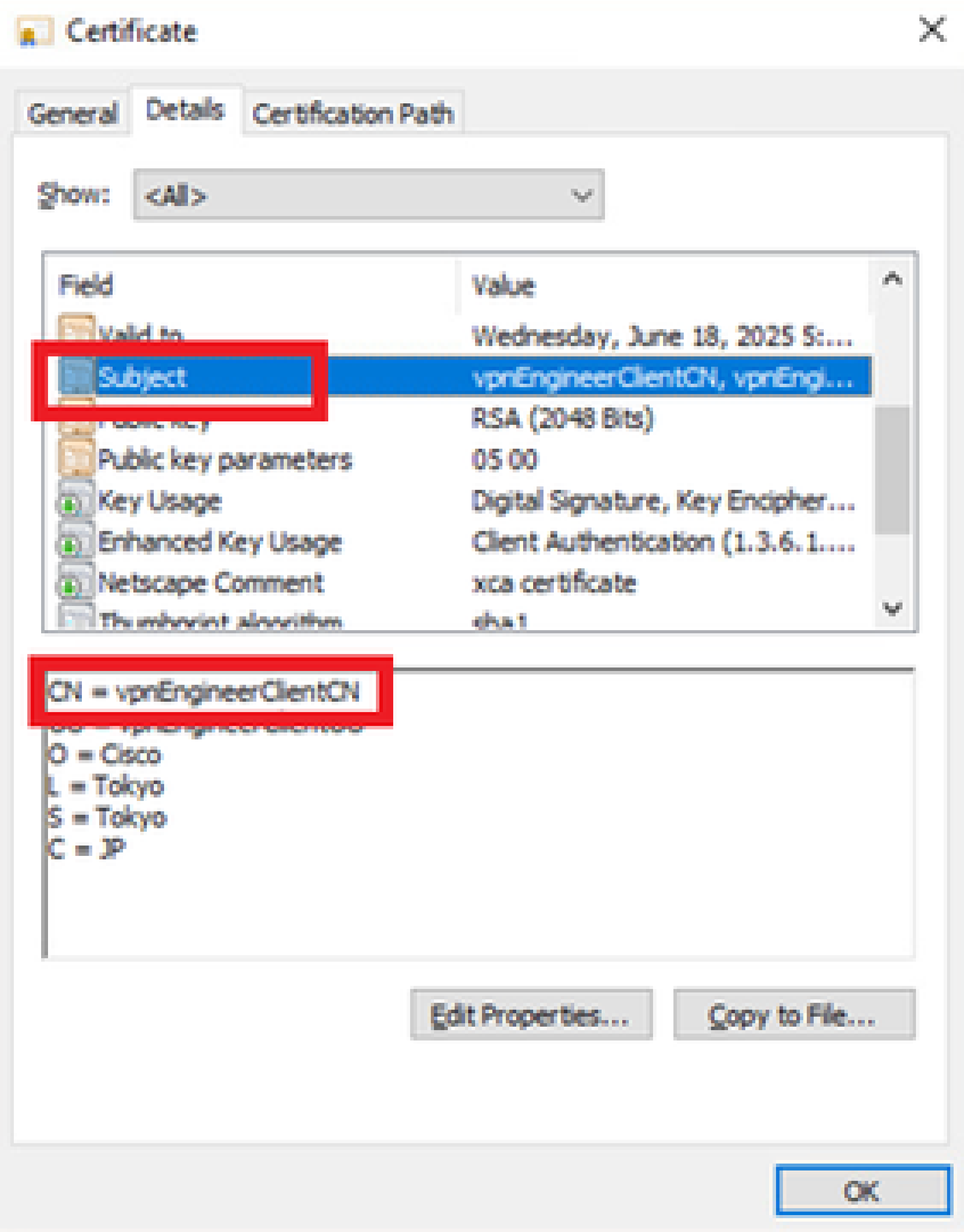
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
vpnEngineerClientCN	ftd-ra-ca-common-name	6/18/2025	Client Authentication	vpnEngineerCli

Confirm Certificate for Engineer VPN Client

Double click the client certificate, navigate to**Details**, check the detail of**Subject**.

- Subject: CN = vpnEngineerClientCN



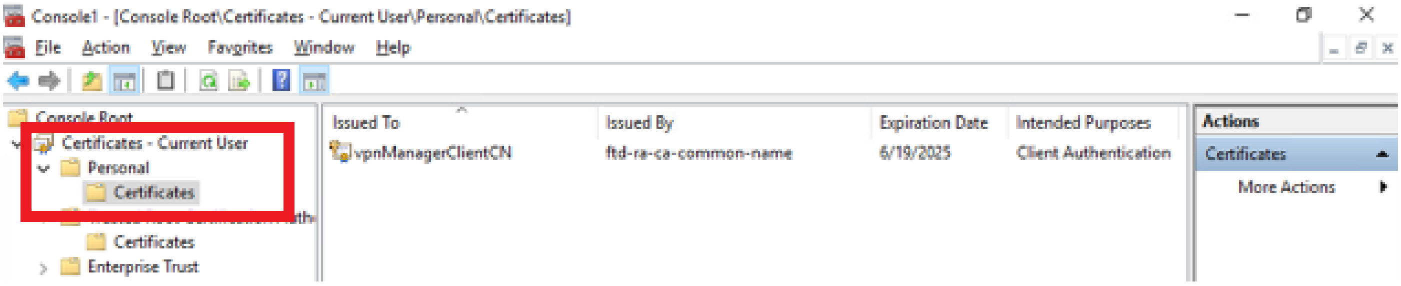
Certificate

Field	Value
Valid to	Wednesday, June 18, 2025 5:...
Subject	vpnEngineerClientCN, vpnEngi...
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
OU = vpnEngineerClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP
```

Details of Engineer Client Certificate

In manager VPN client, navigate to**Certificates - Current User > Personal > Certificates**, check the client certificate used for authentication.

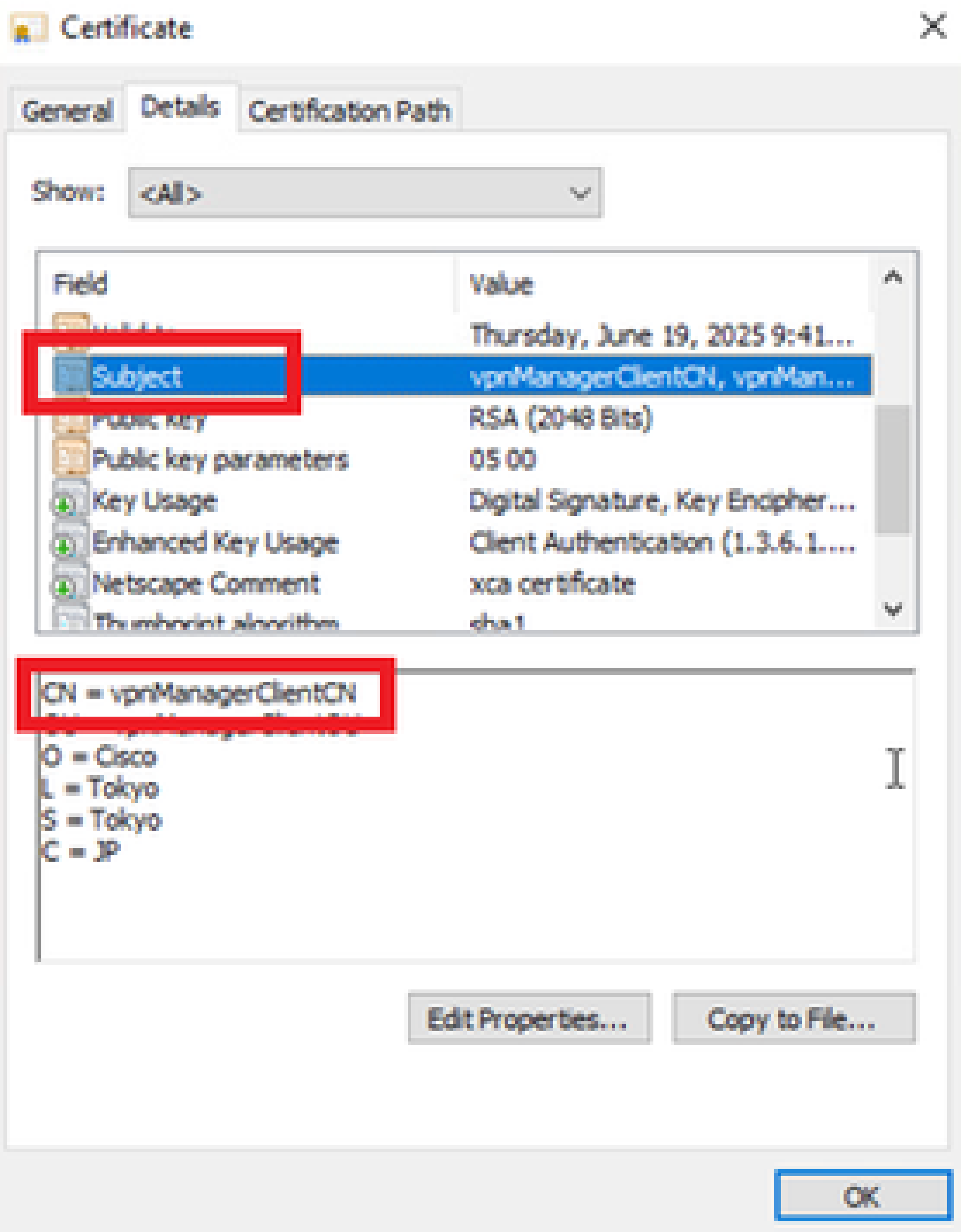

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Certificates
Enterprise Trust
Actions
Certificates
More Actions

Issued To	Issued By	Expiration Date	Intended Purposes
vpnManagerClientCN	ftd-ra-ca-common-name	6/19/2025	Client Authentication

Confirm Certificate for Manager VPN Client

Double click the client certificate, navigate to**Details**, check the detail of**Subject**.

- Subject: CN = vpnManagerClientCN



Show: <All>

Field	Value
Valid to	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

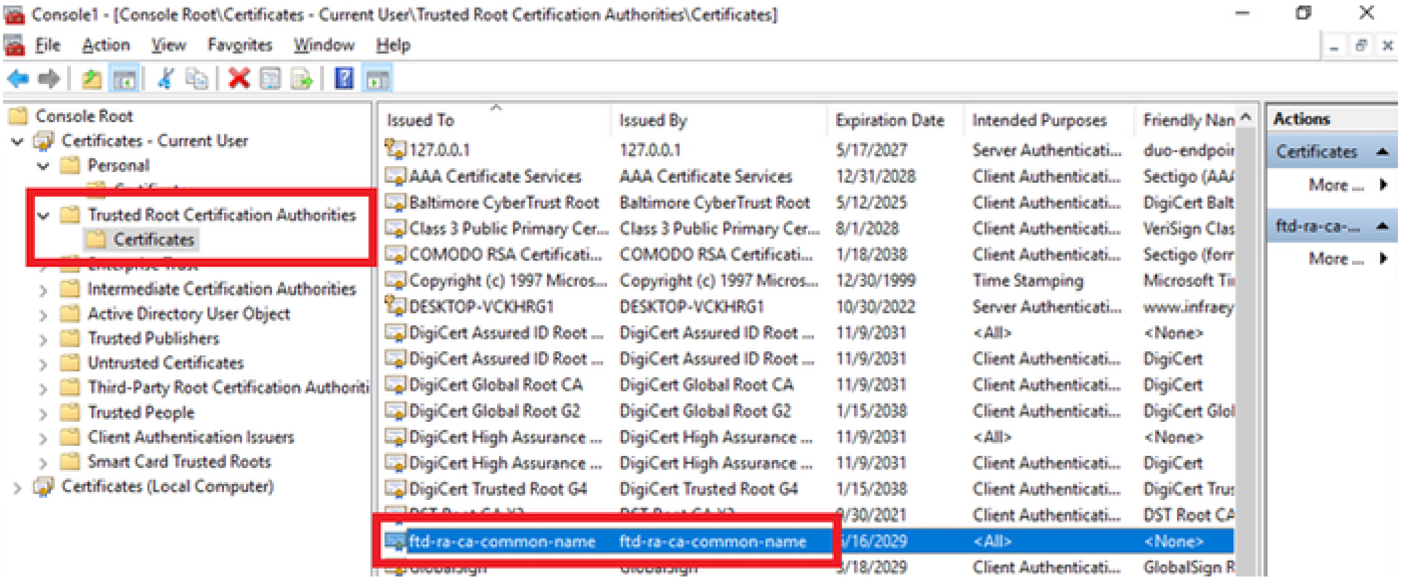
```
CN = vpnManagerClientCN
OU = vpnManagerClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP
```

Details of Manager Client Certificate

Step 2. Confirm CA

In both engineer VPN client and manager VPN client, navigate to**Certificates - Current User > Trusted Root Certification Authorities > Certificates**, check the CA used for authentication.

- Issued By: ftd-ra-ca-common-name



Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots
Certificates (Local Computer)
Actions
Certificates
More ...
ftd-ra-ca-...
More ...

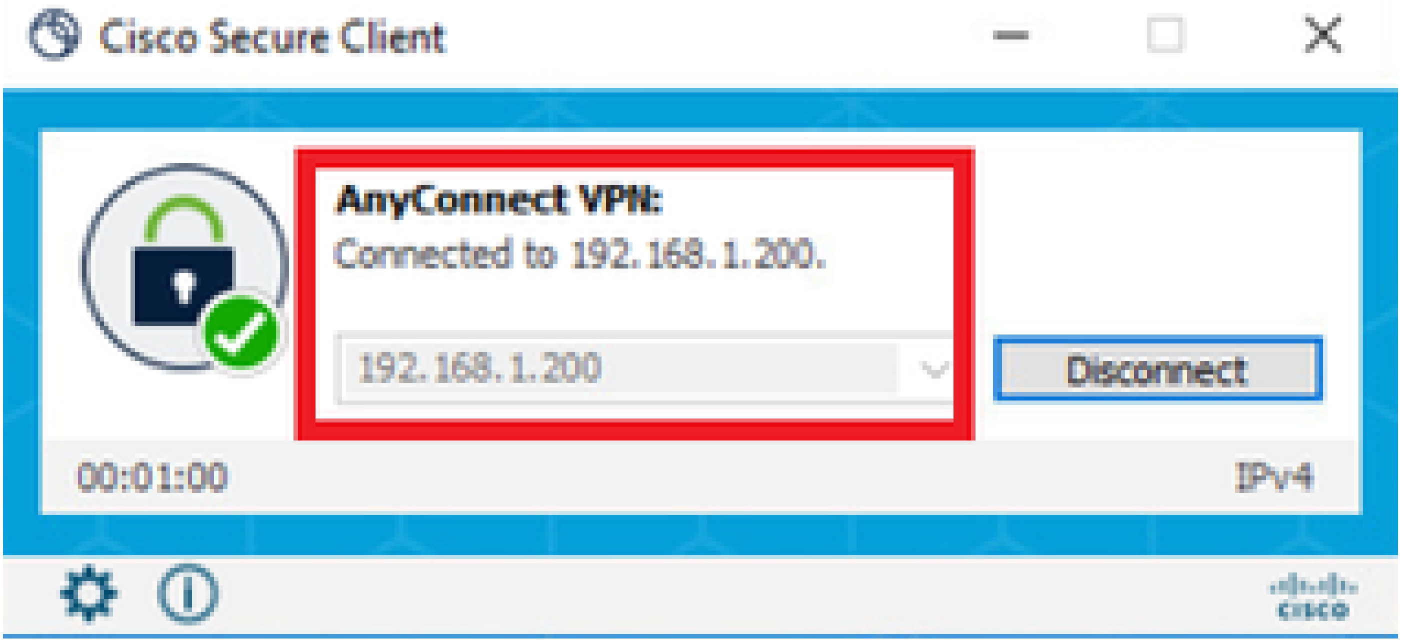
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan
127.0.0.1	127.0.0.1	5/17/2027	Server Authenticati...	duo-endpoi
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati...	Sectigo (AA/
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati...	DigiCert Balt
Class 3 Public Primary Cer...	Class 3 Public Primary Cer...	8/1/2028	Client Authenticati...	VeriSign Clas
COMODO RSA Certificati...	COMODO RSA Certificati...	1/18/2038	Client Authenticati...	Sectigo (forr
Copyright (c) 1997 Micros...	Copyright (c) 1997 Micros...	12/30/1999	Time Stamping	Microsoft Ti
DESKTOP-VCKHRG1	DESKTOP-VCKHRG1	10/30/2022	Server Authenticati...	www.infraey
DigiCert Assured ID Root ...	DigiCert Assured ID Root ...	11/9/2031	<All>	<None>
DigiCert Assured ID Root ...	DigiCert Assured ID Root ...	11/9/2031	Client Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Glol
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	<All>	<None>
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	Client Authenticati...	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati...	DigiCert Trus
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...	DST Root CA
ftd-ra-ca-common-name	ftd-ra-ca-common-name	/16/2029	<All>	<None>
GlobalSign	GlobalSign	/18/2029	Client Authenticati...	GlobalSign R

Confirm CA

Verify

Step 1. Initiate VPN Connection

In engineer VPN client, initiate the Cisco Secure Client connection. No need to input the username and password, the VPN connected successfully.

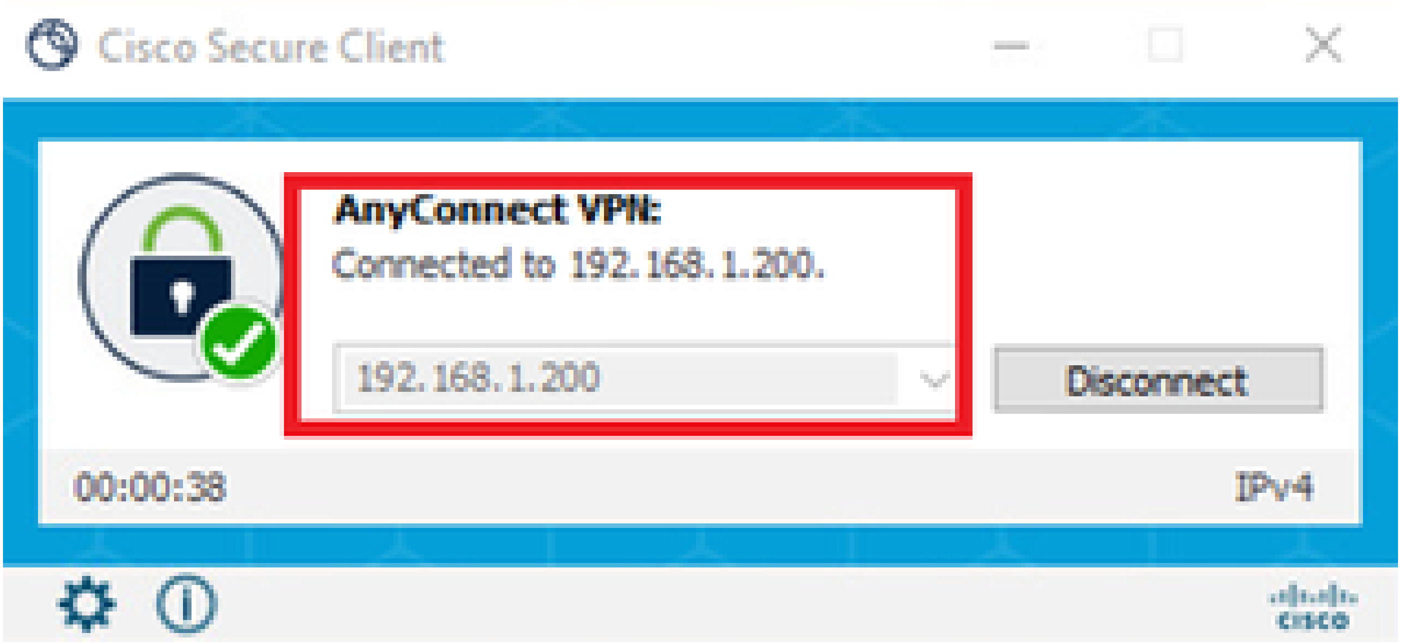


AnyConnect VPN:
Connected to 192.168.1.200.

192.168.1.200

Initiate VPN Connection from Engineer Client

In manager VPN client, initiate the Cisco Secure Client connection. No need to input the username and password, the VPN connected successfully.



AnyConnect VPN:
Connected to 192.168.1.200.

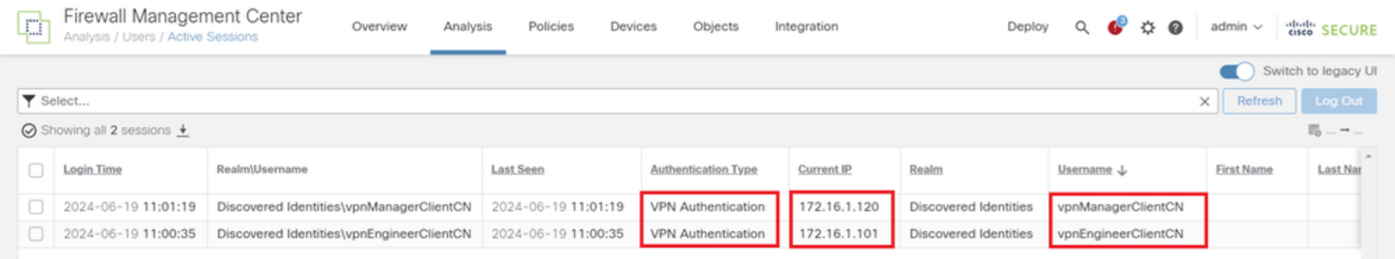
192.168.1.200

00:00:38

Initiate VPN Connection from Manager Client

Step 2. Confirm Active Sessions in FMC

Navigate to**Analysis** > **Users** > **Active Sessions**, check the active session for VPN authentication.



Showing all 2 sessions

□	Login Time	Realm\Username	Last Seen	Authentication Type	Current IP	Realm	Username ↓	First Name	Last Nar
□	2024-06-19 11:01:19	Discovered Identities\vpnManagerClientCN	2024-06-19 11:01:19	VPN Authentication	172.16.1.120	Discovered Identities	vpnManagerClientCN		
□	2024-06-19 11:00:35	Discovered Identities\vpnEngineerClientCN	2024-06-19 11:00:35	VPN Authentication	172.16.1.101	Discovered Identities	vpnEngineerClientCN		

Confirm Active Session

Step 3. Confirm VPN Sessions in FTD CLI

Run`show vpn-sessiondb detail anyconnect` command in FTD (Lina) CLI to confirm the VPN sessions of engineer and manager.

```
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
```

Troubleshoot

You can expect to find information about VPN authentication in the debug syslog of Lina engine and in the DART file on Windows PC.

This is an example of debug logs in the Lina engine during VPN connection from engineer client.

```
<#root>

Jun 19 2024 02:00:35: %FTD-7-717029: Identified client certificate within certificate chain. serial num
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=vpnEnginee
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
```

This is an example of debug logs in the Lina engine during VPN connection from manager client.

```
<#root>

Jun 19 2024 02:01:19: %FTD-7-717029: Identified client certificate within certificate chain. serial num
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
```

Related Information

[Configure Anyconnect Certificate Based Authentication for Mobile Access]()