Configure AAA and Cert Auth for Secure Client on FTD via FMC

Contents

Introduction

This document describes the steps for configuring Cisco Secure Client over SSL on FTD managed by FMC with AAA and certificate authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

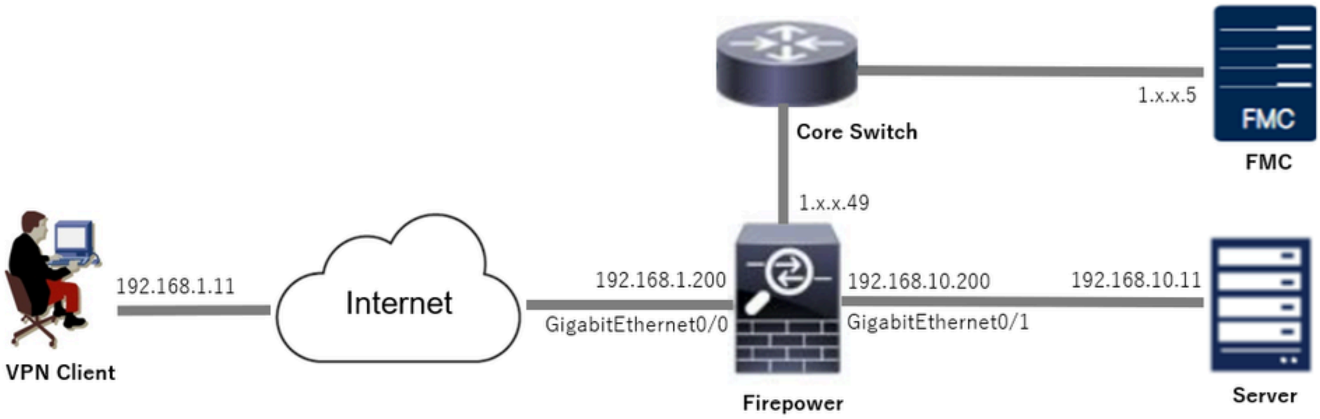
As organizations adopt more stringent security measures, combining two-factor authentication (2FA) with certificate-based authentication has become a common practice to enhance security and protect against unauthorized access. One of the features that can significantly improve user experience and security is the ability to pre-fill the username in the Cisco Secure Client. This feature simplifies the login process and enhances the overall efficiency of remote access.
This document describes how to integrate pre-filled username with Cisco Secure Client on FTD, ensuring that users can quickly and securely connect to the network.

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

- **CA** : ftd-ra-ca-common-name
- **Client Certificate** : sslVPNClientCN
- **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

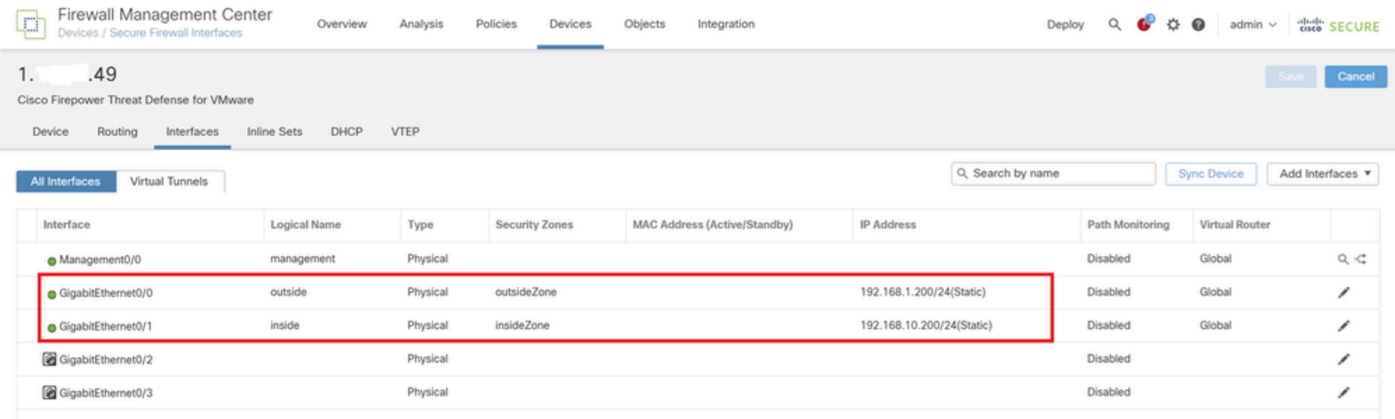
Navigate to **Devices > Device Management**, edit the target FTD device, config inside and outside interface for FTD in **Interfaces** tab.

For GigabitEthernet0/0,

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

For GigabitEthernet0/1,

- **Name** : inside
- **Security Zone** : insideZone
- **IP Address** : 192.168.10.200/24



1.[redacted].49

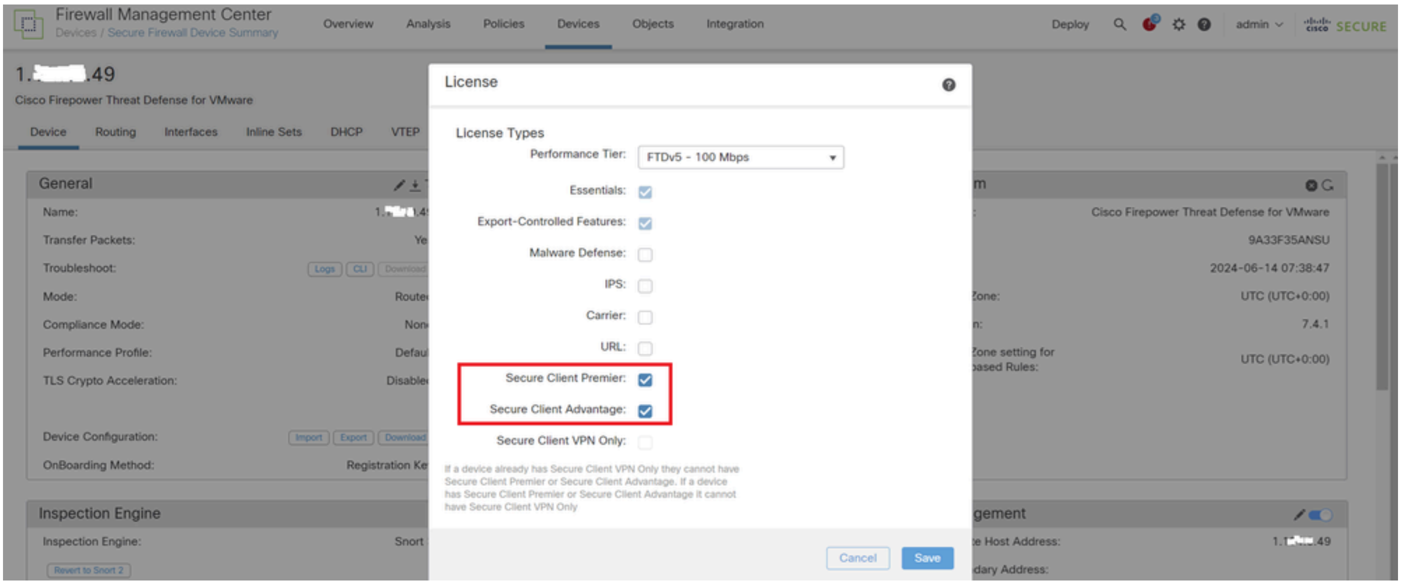
Cisco Firepower Threat Defense for VMware

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
GigabitEthernet0/1	inside	Physical	insideZone		192.168.10.200/24(Static)	Disabled	Global
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	

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

General

Name: 1.[redacted].4
Transfer Packets: Ye
Troubleshoot:
Mode: Route
Compliance Mode: Non
Performance Profile: Defau
TLS Crypto Acceleration: Disable
Device Configuration:
OnBoarding Method: Registration Ke

Inspection Engine

Inspection Engine: Snort

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

m

: Cisco Firepower Threat Defense for VMware
9A33F35ANSU
2024-06-14 07:38:47
Zone: UTC (UTC+0:00)
n: 7.4.1
Zone setting for
based Rules: UTC (UTC+0:00)

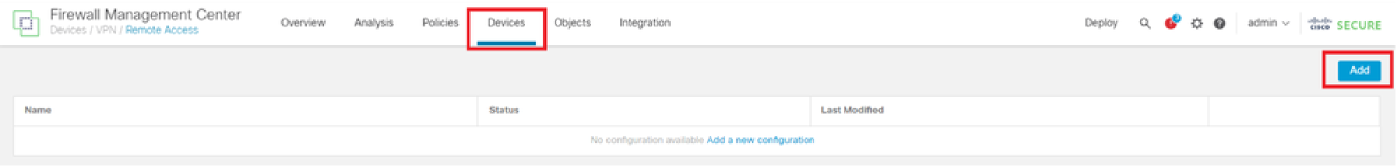
gement

e Host Address: 1.[redacted].49
dary Address:

Secure Client License

Step 3. Add Policy Assignment

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

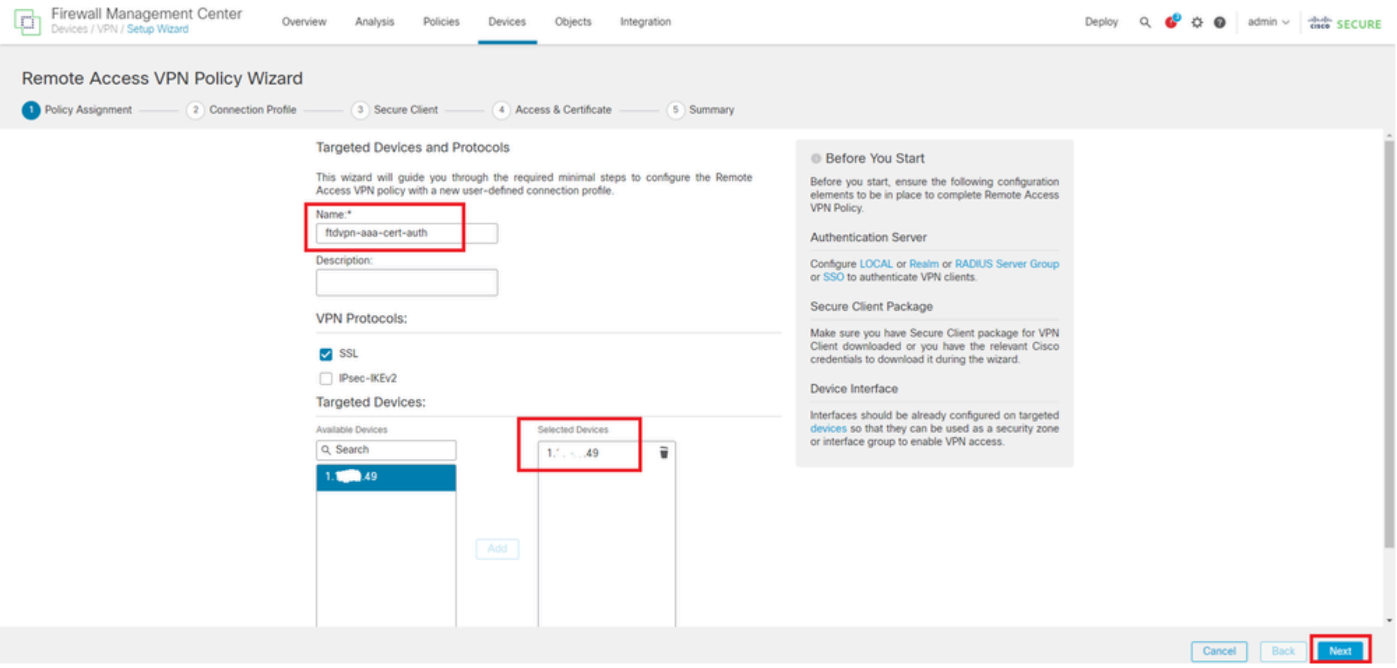


No configuration available Add a new configuration

Add Remote Access VPN

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

- **Name** : ftdvpn-aaa-cert-auth
- **VPN Protocols** : SSL
- **Targeted Devices** : 1.x.x.49



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:* ftdvpn-aaa-cert-auth

Description:

VPN Protocols:

☑ SSL

□ IPsec-IKEv2

Targeted Devices:

Available Devices: 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

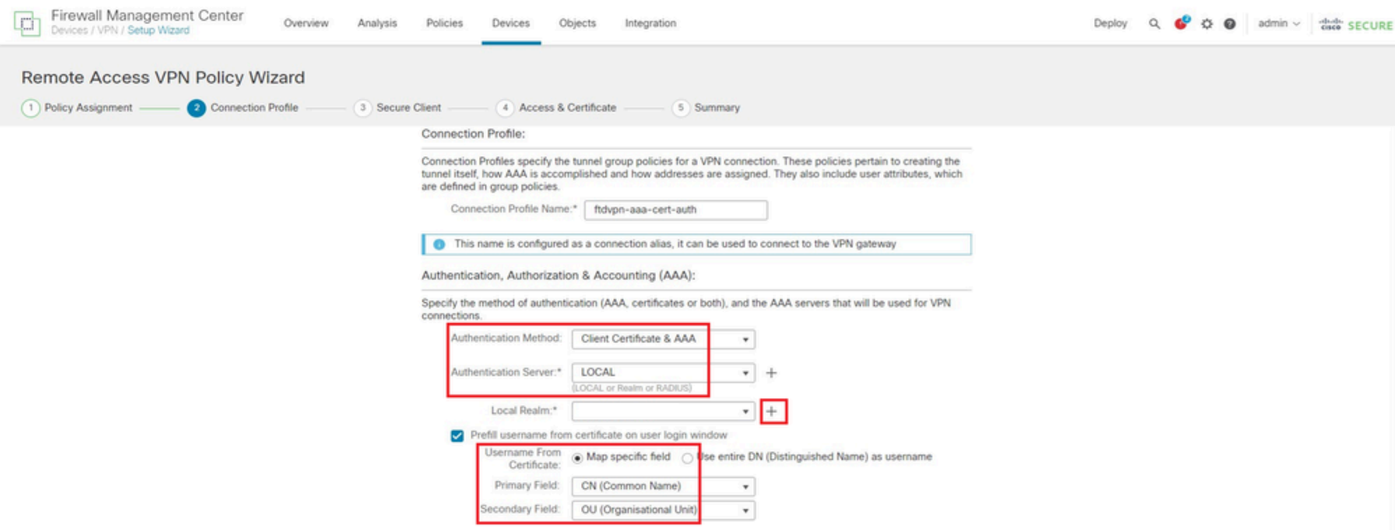
Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

Policy Assignment

Step 4. Config Details for Connection Profile

Input necessary information for connection profile and click **+** button next to the **Local Realm** item.

- **Authentication Method** : Client Certificate & AAA
- **Authentication Server** : LOCAL
- **Username From Certificate** : Map specific field
- **Primary Field** : CN (Common Name)
- **Secondary Field** : OU (Organizational Unit)



Remote Access VPN Policy Wizard

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:* ftdvpn-aaa-cert-auth

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 & AAA

Authentication Server:* LOCAL
(LOCAL or Realm or RADIUS)

Local Realm:* +

☑ Prefill username from certificate on user login window

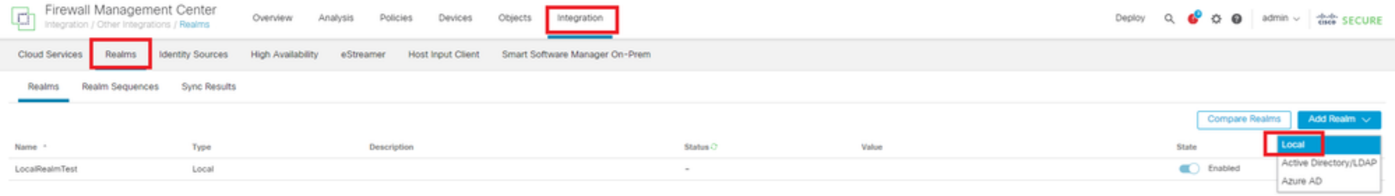
Username From Certificate: ● Map specific field ○ Use entire DN (Distinguished Name) as username

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Details of Connection Profile

Click **Local** from **Add Realm** drop-down list to add a new local realm.



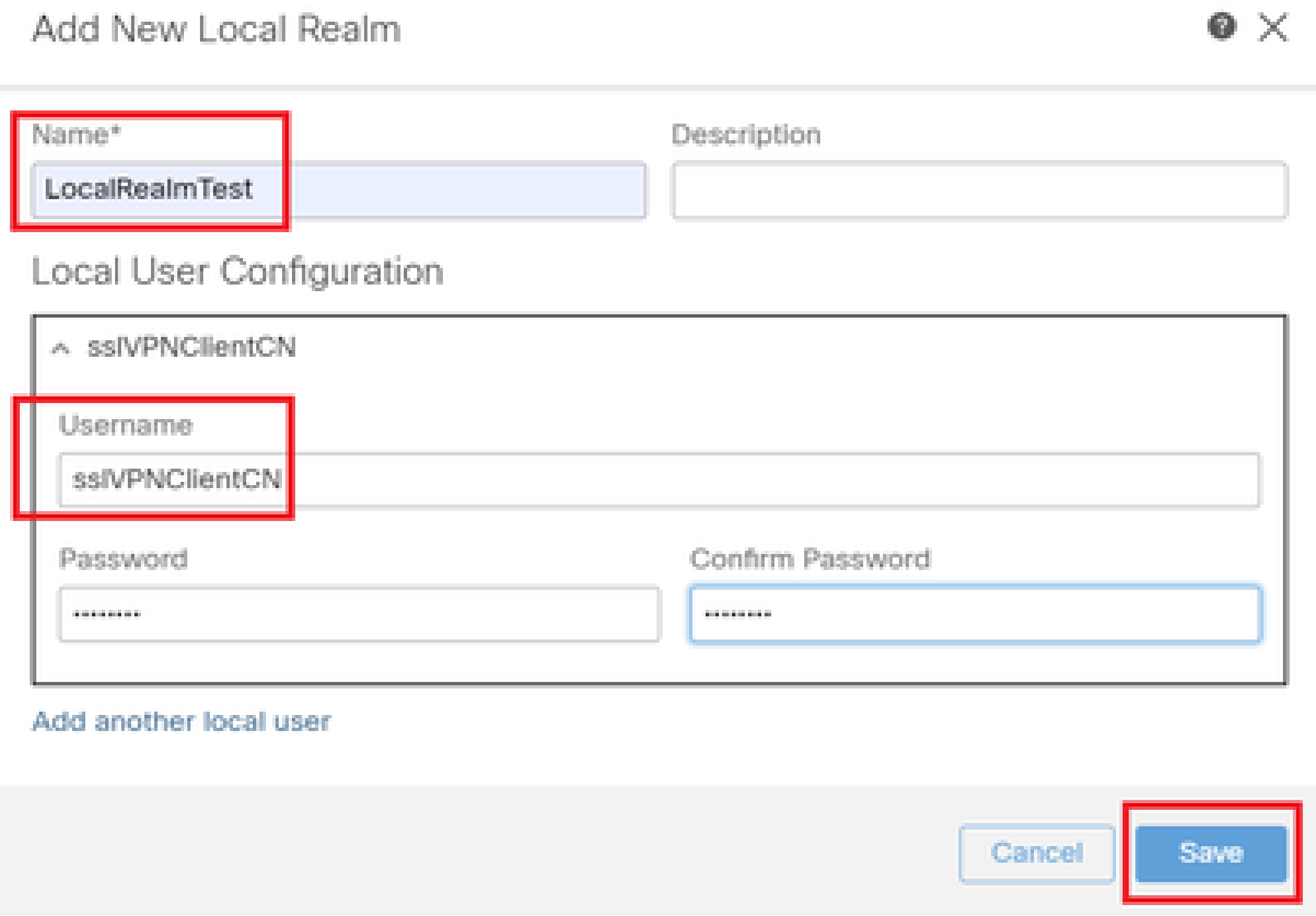
Name	Type	Description	Status	Value	State
LocalRealmTest	Local		-		Enabled

Add Local Realm

Input necessary information for local realm and click **Save** button.

- **Name** : LocalRealmTest
- **Username** : sslVPNClientCN

Note: The username equals the common name within the client certificate



Add New Local Realm

Name*: LocalRealmTest

Description:

Local User Configuration

sslVPNClientCN

Username: sslVPNClientCN

Password: ••••••••

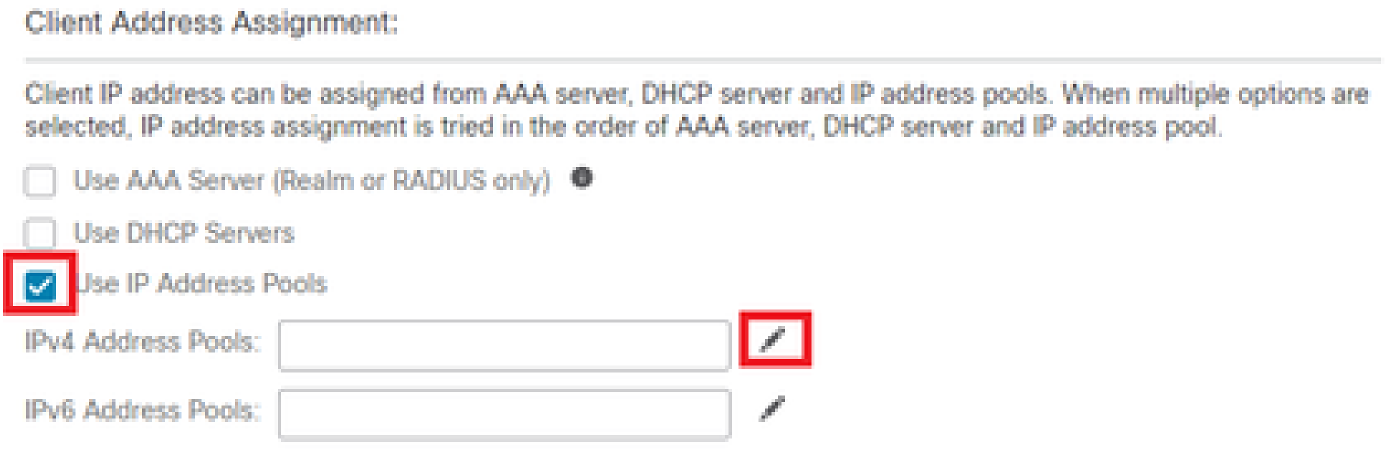
Confirm Password: ••••••••

Add another local user

Details of Local Realm

Step 5. Add Address Pool for Connection Profile

Click **edit** button next to the **IPv4 Address Pools** item.



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:

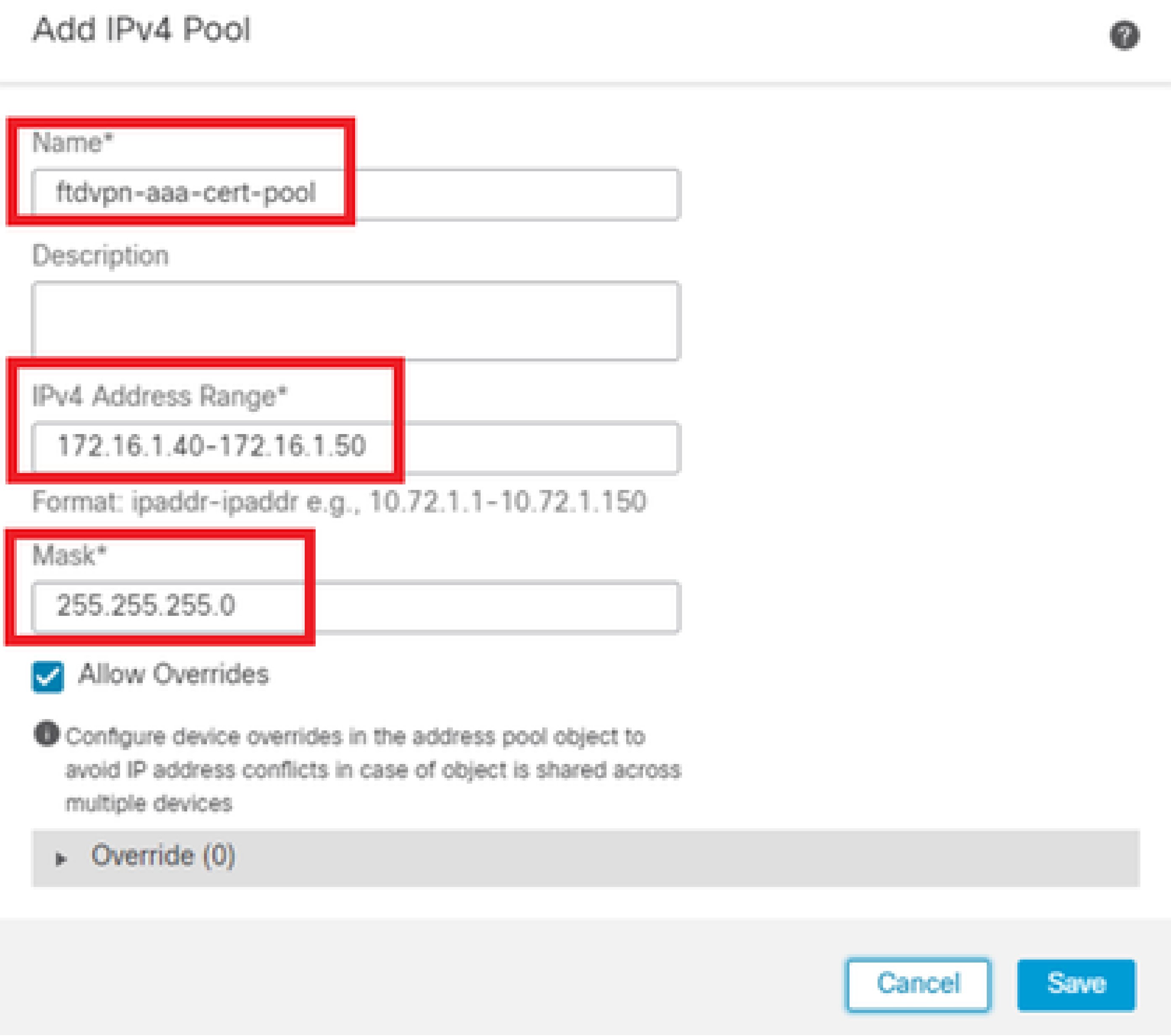
IPv6 Address Pools:

Add IPv4 Address Pool

Input necessary information to add a new IPv4 address pool. Select the new IPv4 address pool for connection profile.

- **Name** : ftdvpn-aaa-cert-pool
- **IPv4 Address Range** : 172.16.1.40-172.16.1.50

- **Mask** : 255.255.255.0



Add IPv4 Pool

Name*: ftdvpn-aaa-cert-pool

Description:

IPv4 Address Range*: 172.16.1.40-172.16.1.50

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

Mask*: 255.255.255.0

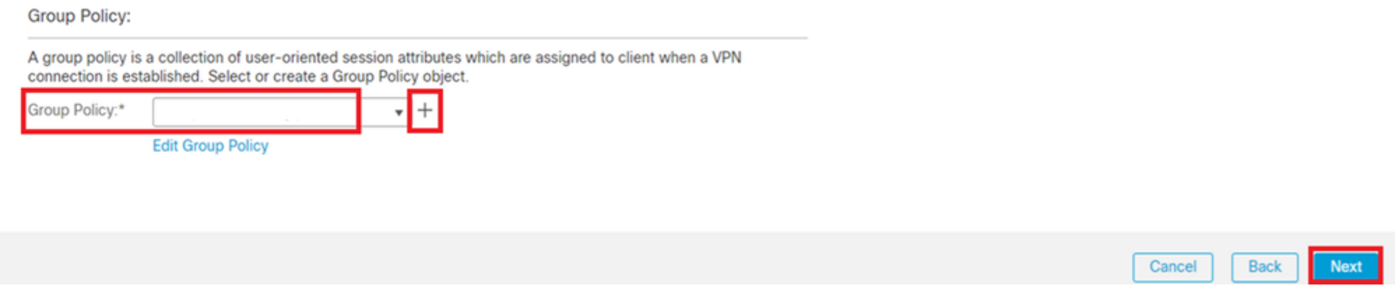
☑ Allow Overrides

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

Details of IPv4 Address Pool

Step 6. Add Group Policy for Connection Profile

Click + button next to the **Group Policy** item.



Group Policy:

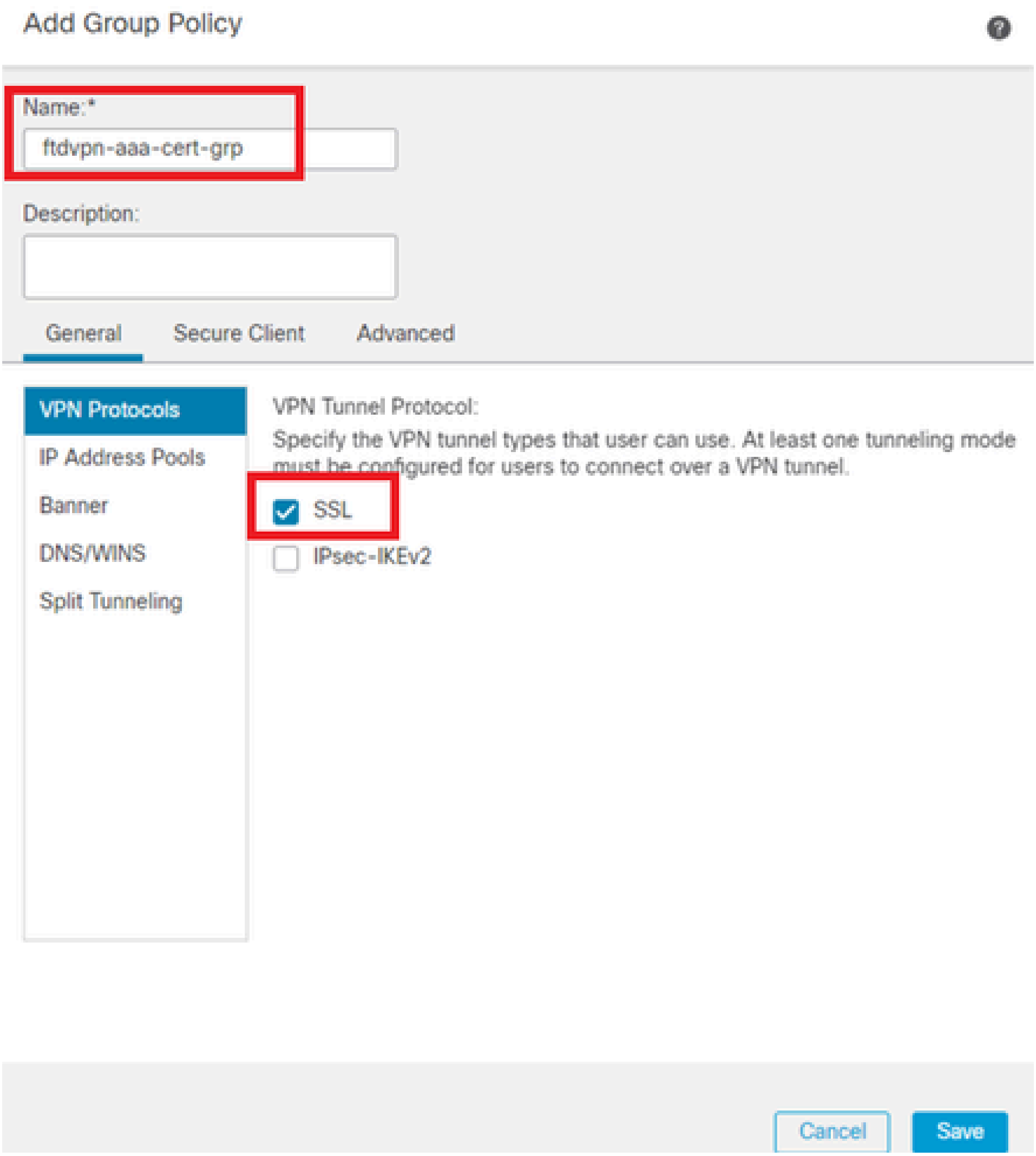
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:*

Add Group Policy

Input necessary information to add a new group policy. Select the new group policy for connection profile.

- **Name** : ftdvpn-aaa-cert-grp
- **VPN Protocols** : SSL



Add Group Policy

Name:*

ftdvpn-aaa-cert-grp

Description:

General | Secure Client | Advanced

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.

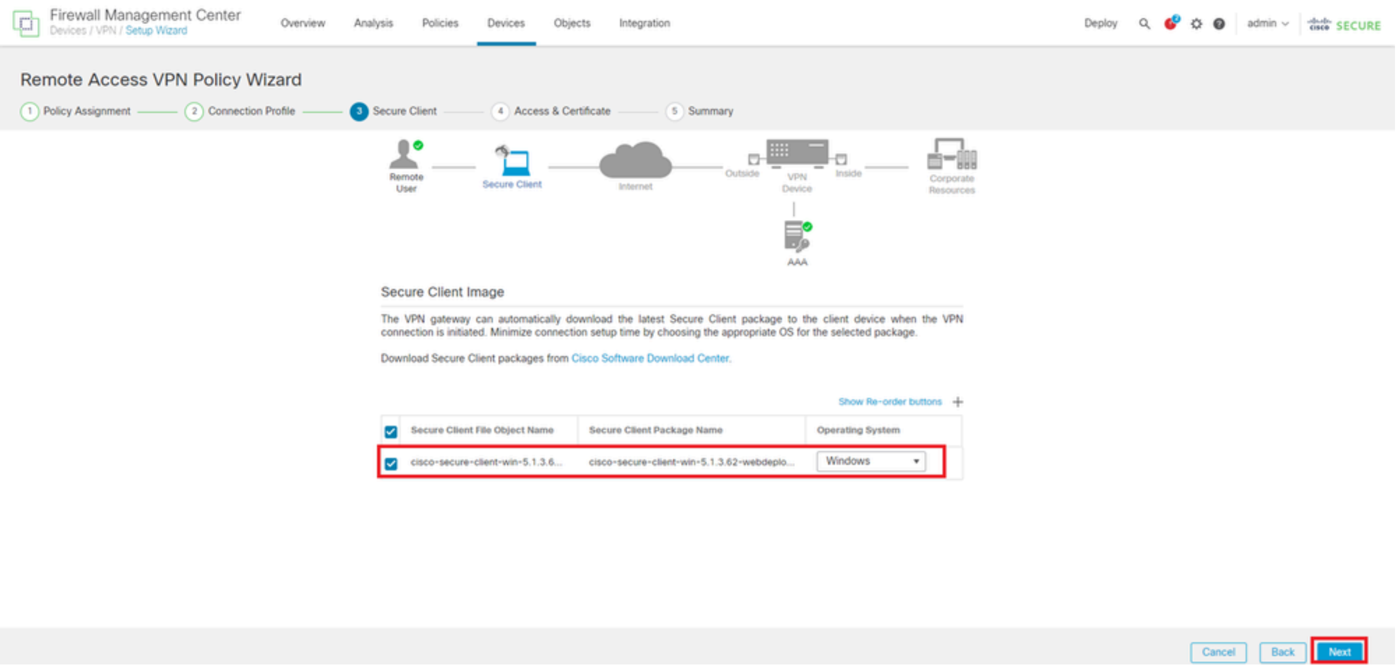
☑ SSL

□ IPsec-IKEv2

Details of Group Policy

Step 7. Config Secure Client Image for Connection Profile

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



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 +

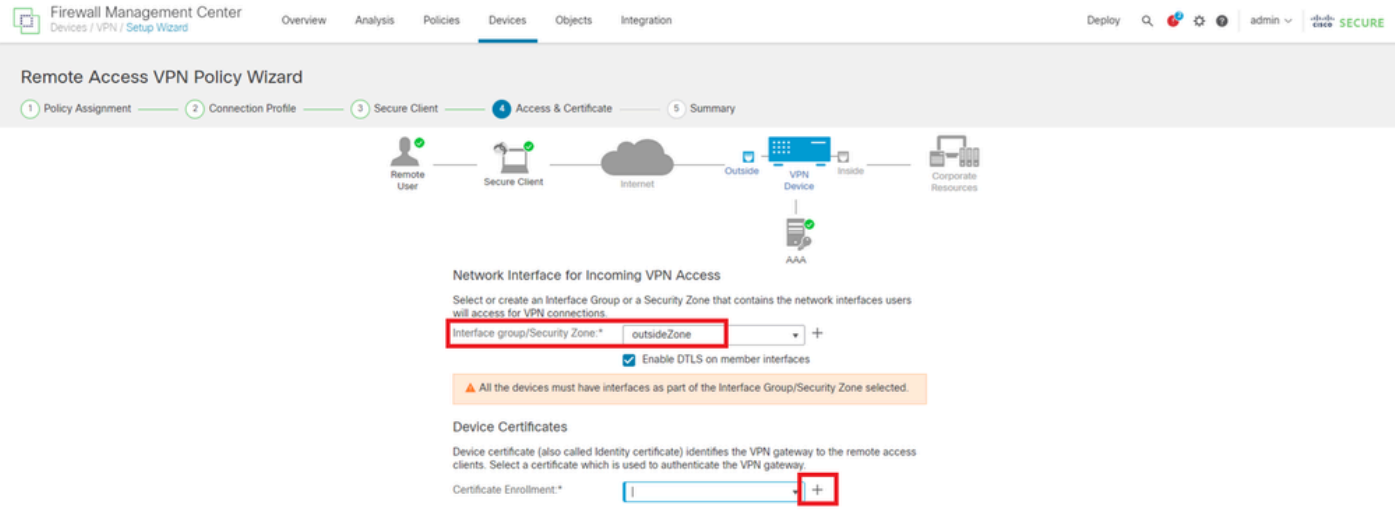
☑	Secure Client File Object Name	Secure Client Package Name	Operating System
☑	cisco-secure-client-win-5.1.3.6...	cisco-secure-client-win-5.1.3.62-webdeplo...	Windows

Select Secure Client Image

Step 8. Config Access & Certificate for Connection Profile

Select **Security Zone** for VPN connection and click **+** button next to **Certificate Enrollment** item.

- **Interface group/Security Zone** : outsideZone



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

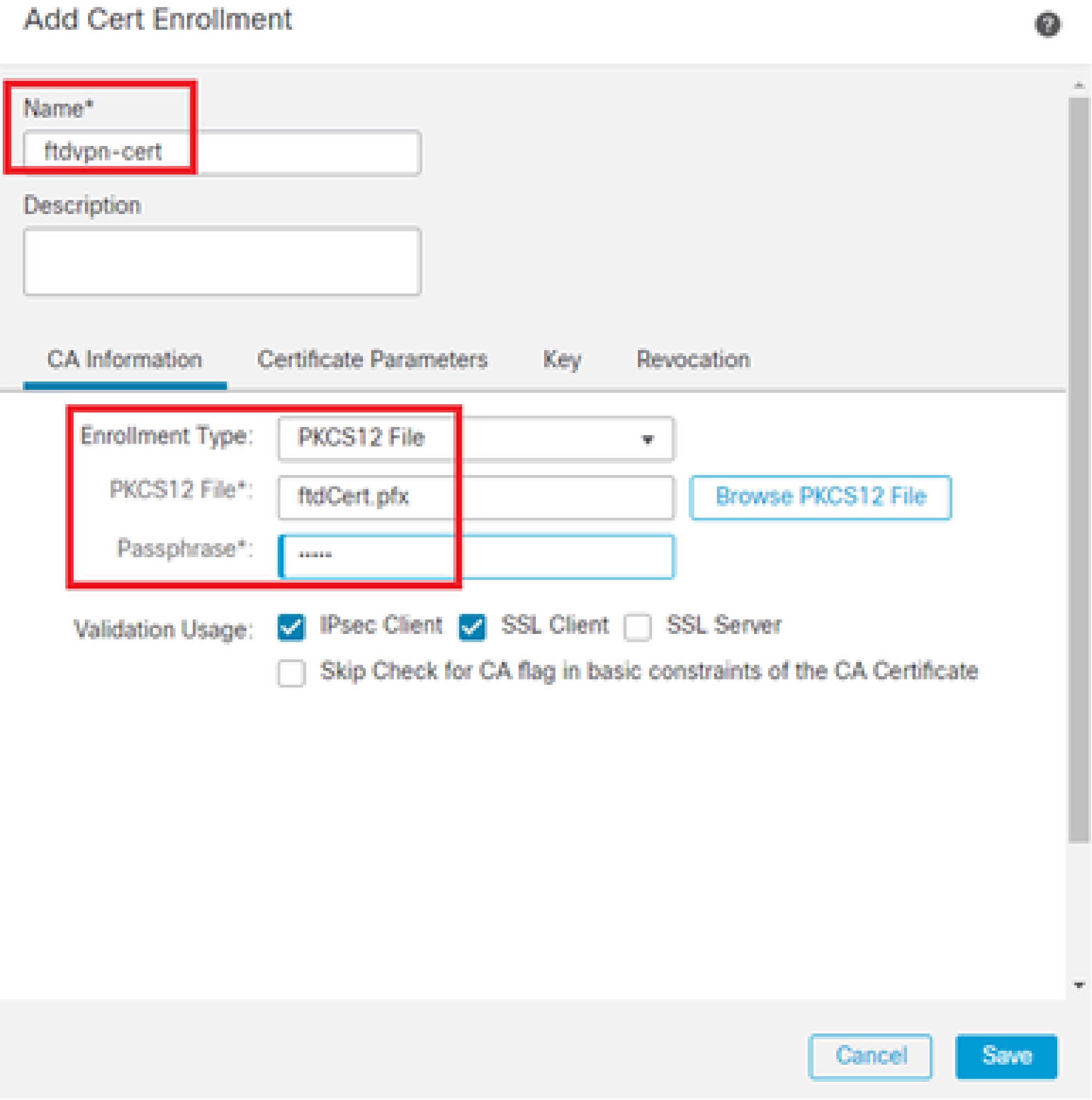
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Select Security Zone

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

- **Name** : ftdvpn-cert
- **Enrollment Type** : PKCS12 File



Add Cert Enrollment

Name*: ftdvpn-cert

Description:

Enrollment Type: PKCS12 File

PKCS12 File*: ftdCert.pfx

Passphrase*: ••••••

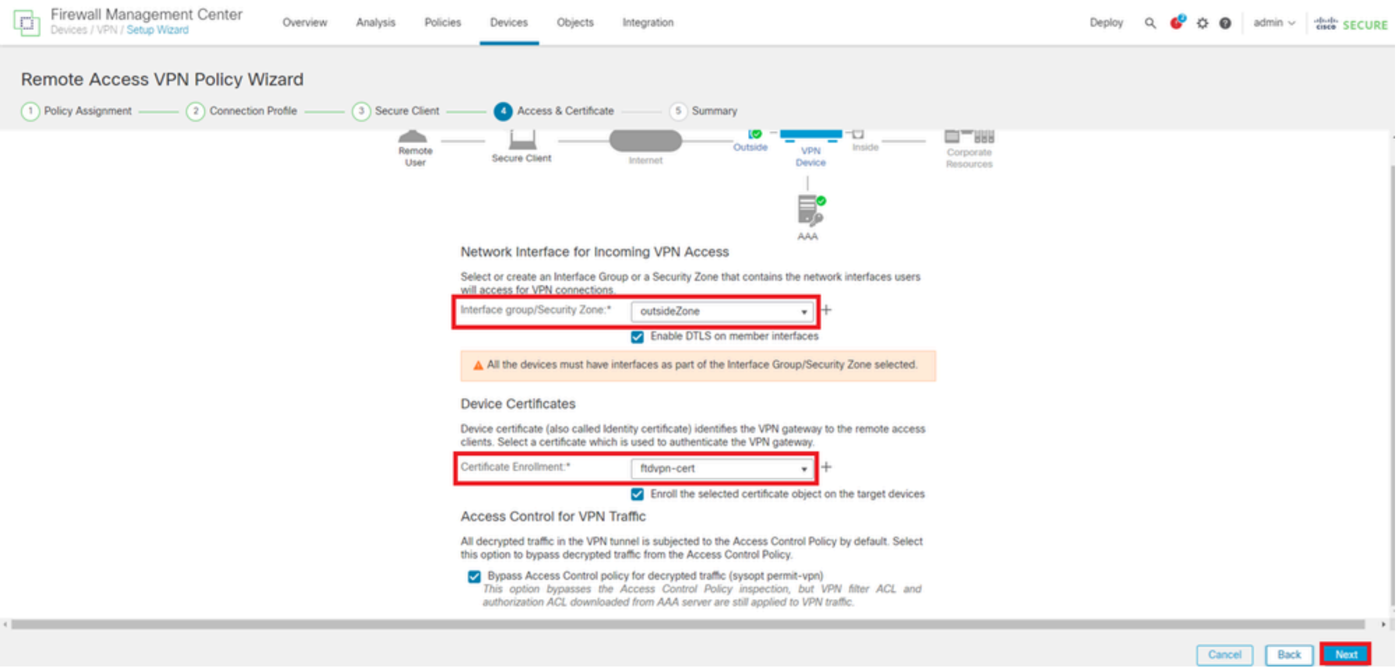
Validation Usage: ☑ IPsec Client ☑ SSL Client □ SSL Server

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

Add FTD Certificate

Confirm the information entered in **Access & Certificate** wizard and click **Next** button.

Note: Enable **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**, so that decrypted VPN traffic is not subjected to access control policy inspection.



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:* ftdvpn-cert

☑ Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

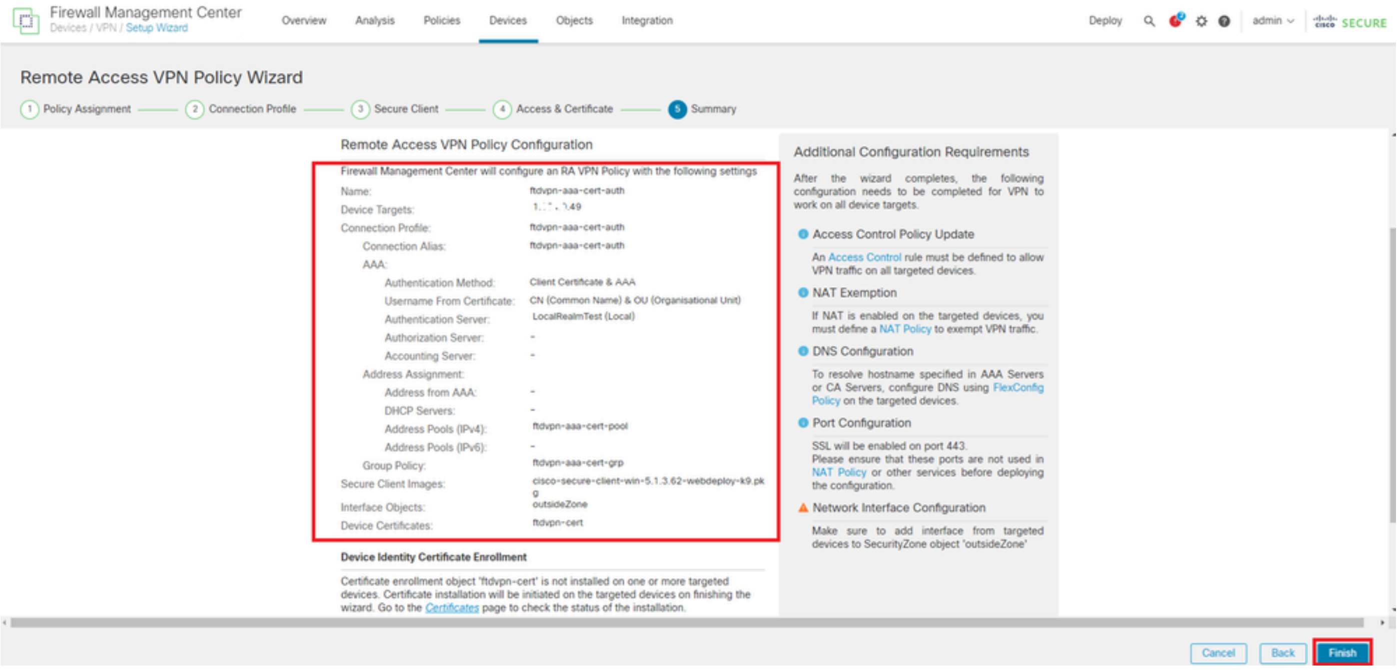
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

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

Confirm Settings in Access & Certificate

Step 9. Confirm Summary for Connection Profile

Confirm the information entered for VPN connection 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:	ftdvpn-aaa-cert-auth
Device Targets:	1.[redacted].49
Connection Profile:	ftdvpn-aaa-cert-auth
Connection Alias:	ftdvpn-aaa-cert-auth
AAA:	
Authentication Method:	Client Certificate & AAA
Username From Certificate:	CN (Common Name) & OU (Organisational Unit)
Authentication Server:	LocalRealmTest (Local)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	ftdvpn-aaa-cert-pool
Address Pools (IPv6):	-
Group Policy:	ftdvpn-aaa-cert-grp
Secure Client Images:	cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg
Interface Objects:	outsideZone
Device Certificates:	ftdvpn-cert

Device Identity Certificate Enrollment

Certificate enrollment object 'ftdvpn-cert' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the Certificates page to check the status of the installation.

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

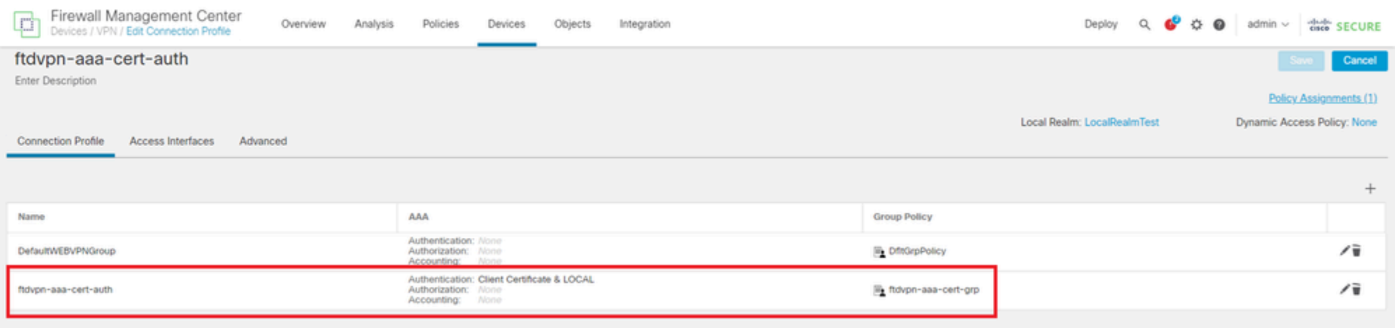
SSL will be enabled on port 443.
Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

Network Interface Configuration

Make sure to add interface from targeted devices to SecurityZone object 'outsideZone'

Confirm Settings for VPN Connection

Confirm the summary of remote access VPN policy and deploy the settings to FTD.



ftdvpn-aaa-cert-auth

Enter Description

Local Realm: LocalRealmTest

Dynamic Access Policy: None

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
ftdvpn-aaa-cert-auth	Authentication: Client Certificate & LOCAL Authorization: None Accounting: None	ftdvpn-aaa-cert-grp

Summary of Remote Access VPN Policy

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
interface GigabitEthernet0/1
nameif inside
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0

// Defines a local user
username sslVPNClientCN password ***** encrypted

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

// Server Certificate Chain
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
......
quit
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
```

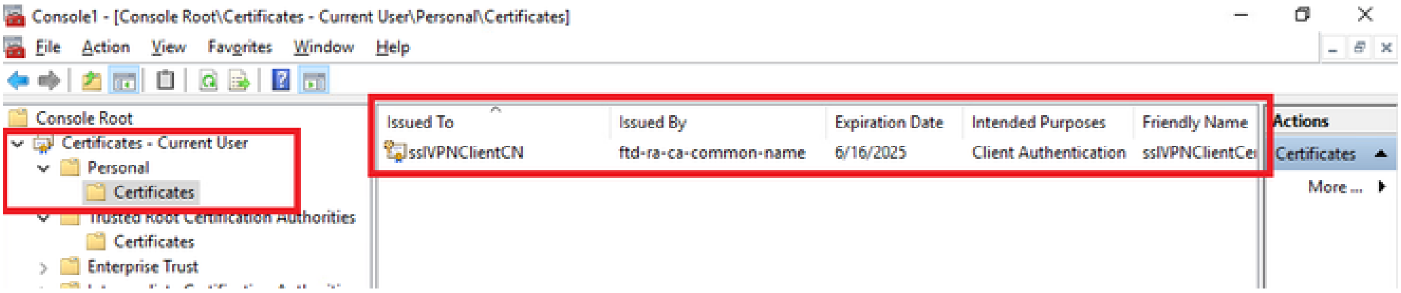
```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-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 aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
```

```
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

Confirm in VPN Client

Step 1. Confirm Client Certificate

Navigate to **Certificates - Current User** > **Personal** > **Certificates**, check the client certificate used for authentication.



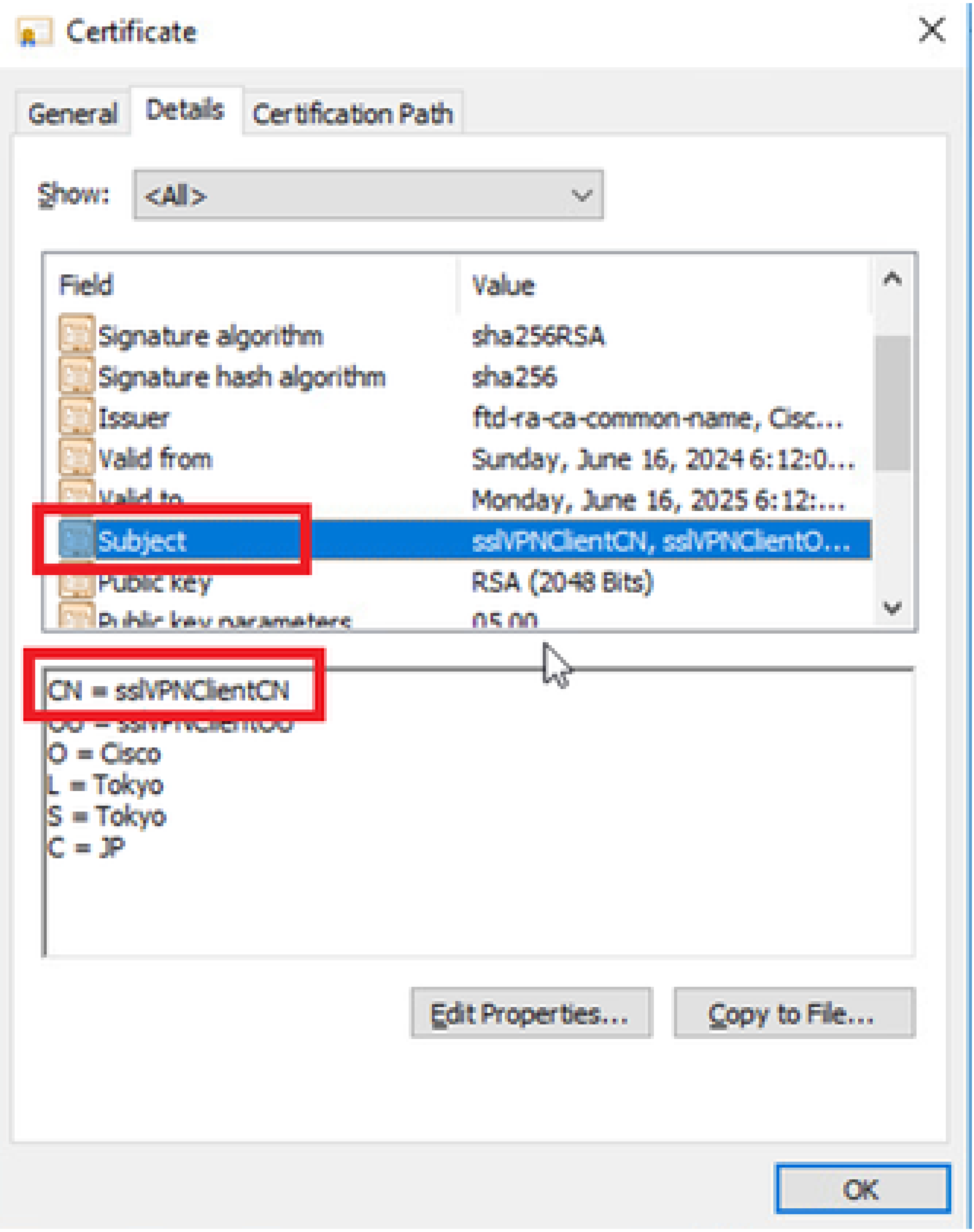
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Actions
Certificates
More ...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
sslVPNClientCN	ftd-ra-ca-common-name	6/16/2025	Client Authentication	sslVPNClientCe

Confirm Client Certificate

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

- **Subject** : CN = sslVPNClientCN



Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ftd-ra-ca-common-name, Cisc...
Valid from	Sunday, June 16, 2024 6:12:0...
Valid to	Monday, June 16, 2025 6:12:...
Subject	sslVPNClientCN, sslVPNClientO...
Public key	RSA (2048 Bits)
Public key parameters	05 00

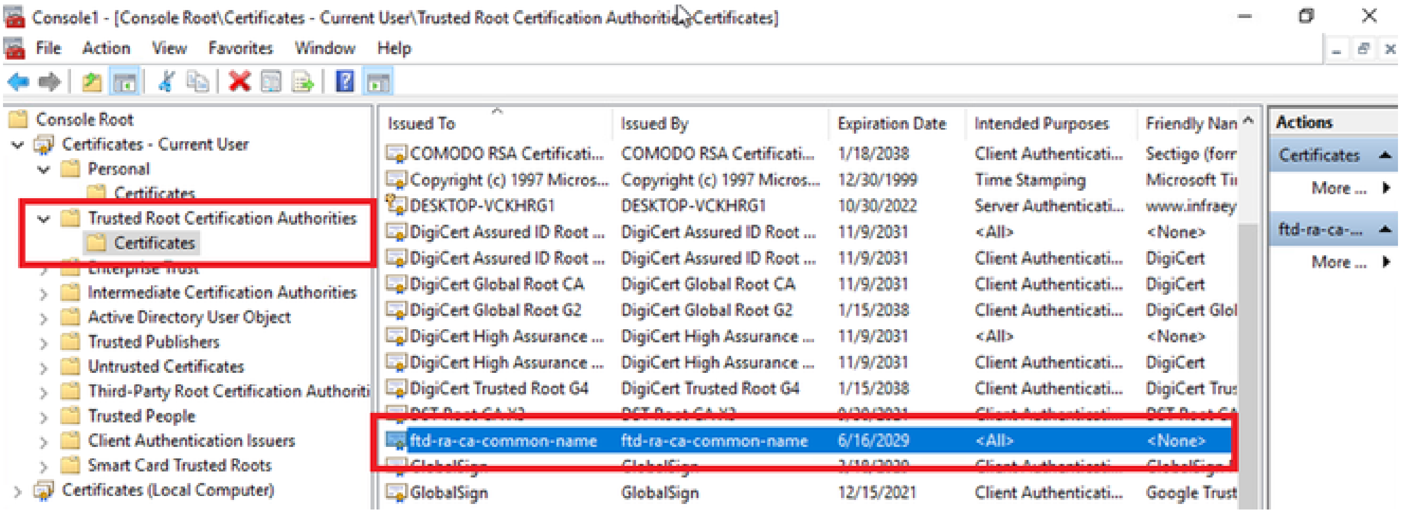
```
CN = sslVPNClientCN
OU = sslVPNClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP
```

Details of Client Certificate

Step 2. Confirm CA

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
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	6/16/2029	<All>	<None>
GlobalSign	GlobalSign	3/18/2029	Client Authenticati...	GlobalSign
GlobalSign	GlobalSign	12/15/2021	Client Authenticati...	Google Trust

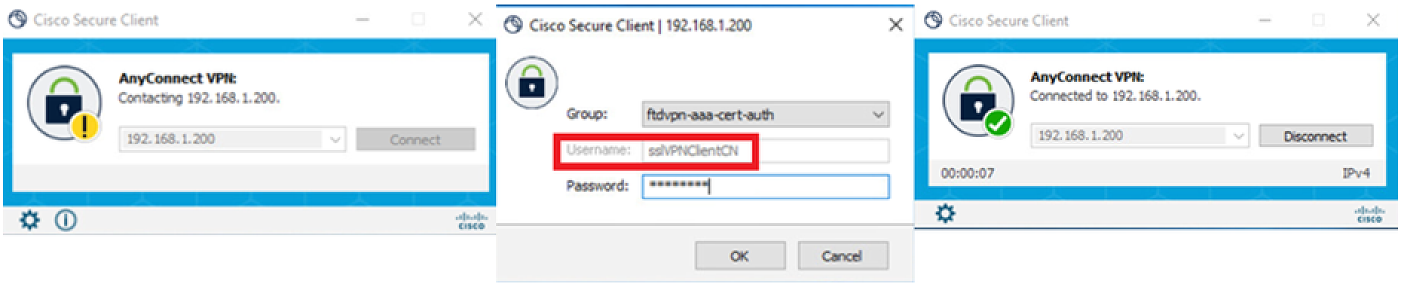
Confirm CA

Verify

Step 1. Initiate VPN Connection

On the endpoint, initiate the Cisco Secure Client connection. The username is extracted from the client certificate, you need to input the password for VPN authentication.

Note: The username is extracted from the CN (Common Name) field of the client certificate in this document.



Cisco Secure Client

AnyConnect VPN:
Contacting 192.168.1.200.

192.168.1.200

Cisco Secure Client | 192.168.1.200

Group: ftdvpn-aaa-cert-auth

Username: sslVPNClientCN

Password: ********

Cisco Secure Client

AnyConnect VPN:
Connected to 192.168.1.200.

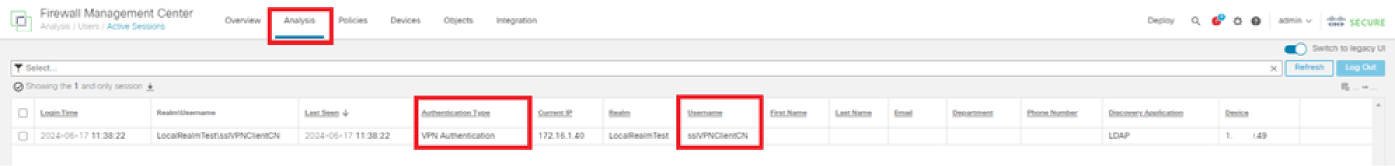
192.168.1.200

00:00:07 IPv4

Initiate VPN Connection

Step 2. Confirm Active Sessions in FMC

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



	Login Time	Realm\Username	Last Seen	Authentication Type	Current IP	Realm	Username	First Name	Last Name	Email	Department	Phone Number	Discovery Application	Device
□	2024-06-17 11:38:22	LocalRealmTest\sslVPNClientCN	2024-06-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	sslVPNClientCN						LDAP	1. 149

Confirm Active Session

Step 3. Confirm VPN Session in FTD CLI

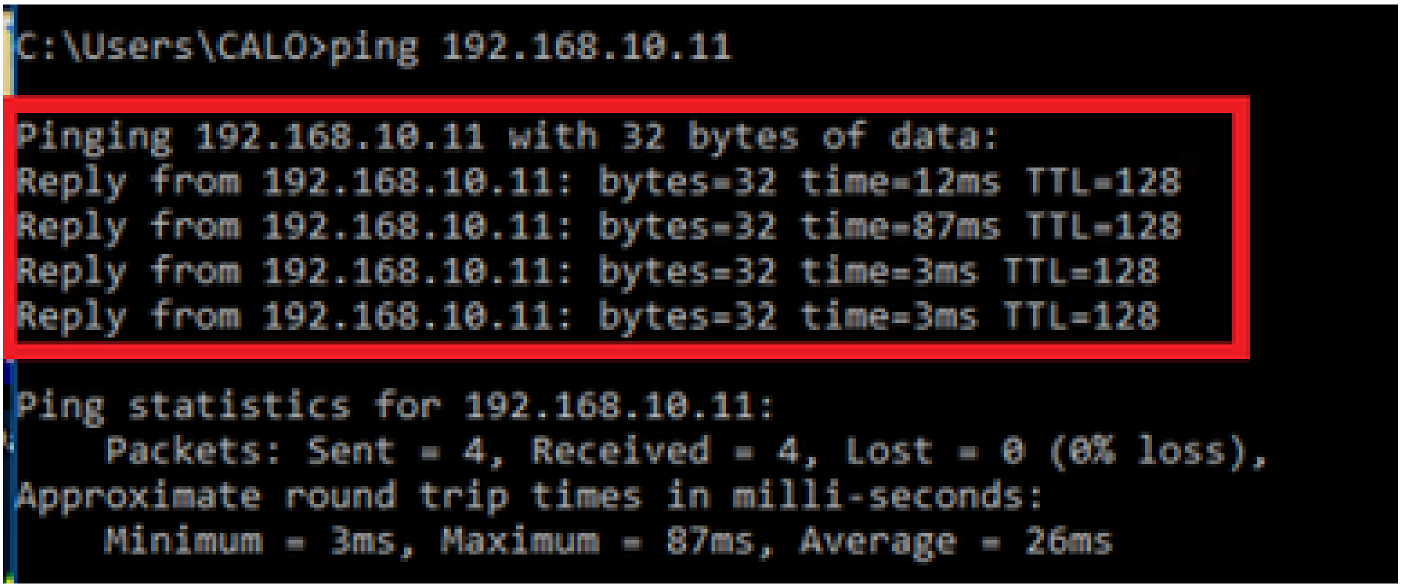
Runshow vpn-sessiondb detail anyconnect command in FTD (Lina) CLI to confirm the VPN session.

```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 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 : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb00718200007000666fa19e
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 7.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50035 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 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 : 7390 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
```

```
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 2292
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 7.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56382
UDP Dst Port : 443 Auth Mode : Certificate and userPassword
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 : 13094
Pkts Tx : 0 Pkts Rx : 34
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Step 4. Confirm Communication with Server

Initiate ping from VPN client to the Server, confirm that communication between the VPN client and the server is successful.



```
C:\Users\CALO>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=12ms TTL=128
Reply from 192.168.10.11: bytes=32 time=87ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 87ms, Average = 26ms
```

Ping succeeded

Run `capture in interface inside real-time` command in FTD (Lina) CLI to confirm packet capture.

<#root>

```
ftd702#
```

`capture in interface inside real-time`

```
Use ctrl-c to terminate real-time capture
```

```
1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo reply
```

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.

```
// Certificate Authentication
Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial numb
Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocat
Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B23

// Extract username from the CN (Common Name) field
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been reques
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed.

// AAA Authentication
Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVP
Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user =
Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN
```

These debugs can be run from the diagnostic CLI of the FTD, which provides information you can use in order to troubleshoot your configuration.

- debug crypto ca 14
- debug webvpn anyconnect 255
- debug crypto ike-common 255

Reference

Configure AnyConnect Remote Access VPN on FTD

Configure Anyconnect Certificate Based Authentication for Mobile Access