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

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Network Diagram

Configurations

- Configuration in FMC
  - Step 1. Configure FTD Interface
  - Step 2. Confirm Cisco Secure Client License
  - Step 3. Add Policy Assignment
  - Step 4. Config Details for Connection Profile
  - Step 5. Add Address Pool for Connection Profile
  - Step 6. Add Group Policy for Connection Profile
  - Step 7. Config Secure Client Image for Connection Profile
  - Step 8. Config Access & Certificate for Connection Profile
  - Step 9. Confirm Summary for Connection Profile
- Confirm in FTD CLI
- Confirm in VPN Client
  - Step 1. Confirm Client Certificate
  - Step 2. Confirm CA

Verify

- Step 1. Initiate VPN Connection
- Step 2. Confirm Active Sessions in FMC
- Step 3. Confirm VPN Session in FTD CLI
- Step 4. Confirm Communication with Server

Troubleshoot

Reference

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

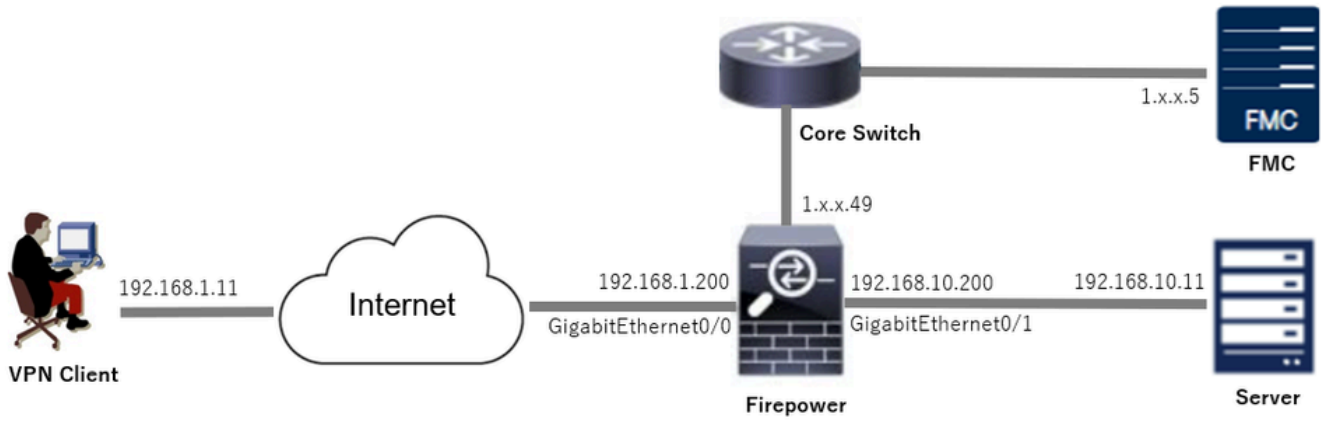
As organizations adopt more stringent security measures, combining two-factor authentication (2FA) with certificate-based authentication has become a common practice to enhance security and protect against unauthorized access. One of the features that can significantly improve user experience and security 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

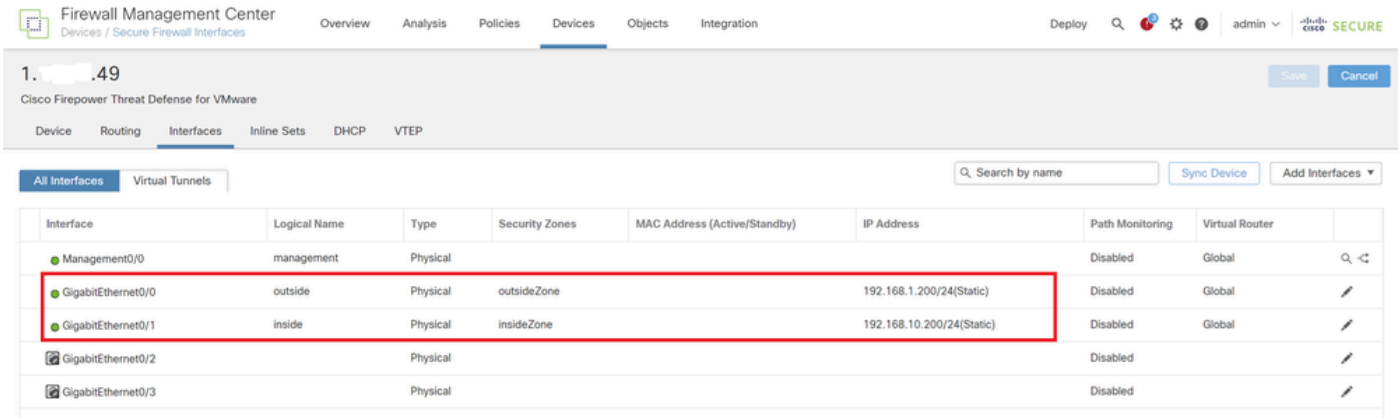
Navigate to **Devices > Device Management**, edit the target FTD device, config inside and outside interface for FTD in **Interfaces** tab.

For GigabitEthernet0/0,

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

For GigabitEthernet0/1,

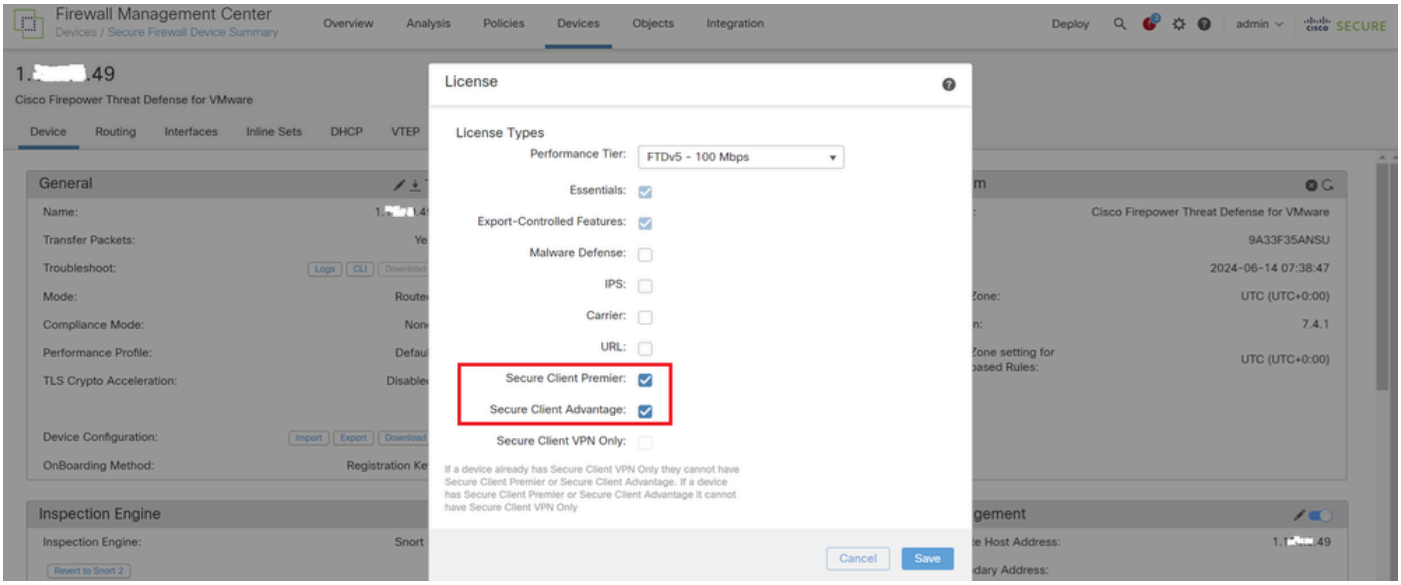
- **Name** : inside
- **Security Zone** : insideZone
- **IP Address** : 192.168.10.200/24



FTD Interface

Step 2. Confirm Cisco Secure Client License

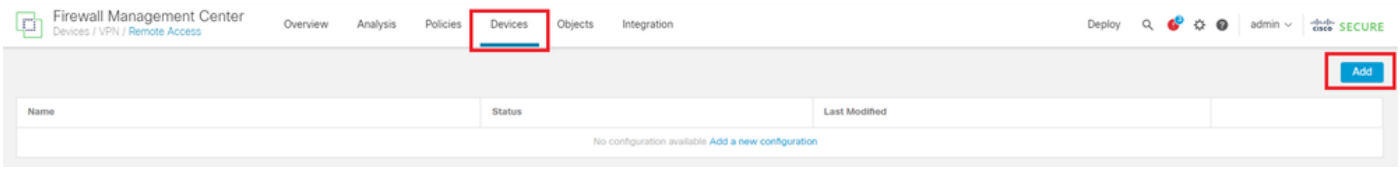
Navigate to **Devices > Device Management**, edit the target FTD device, confirm the Cisco Secure Client license in **Device** tab.



Secure Client License

Step 3. Add Policy Assignment

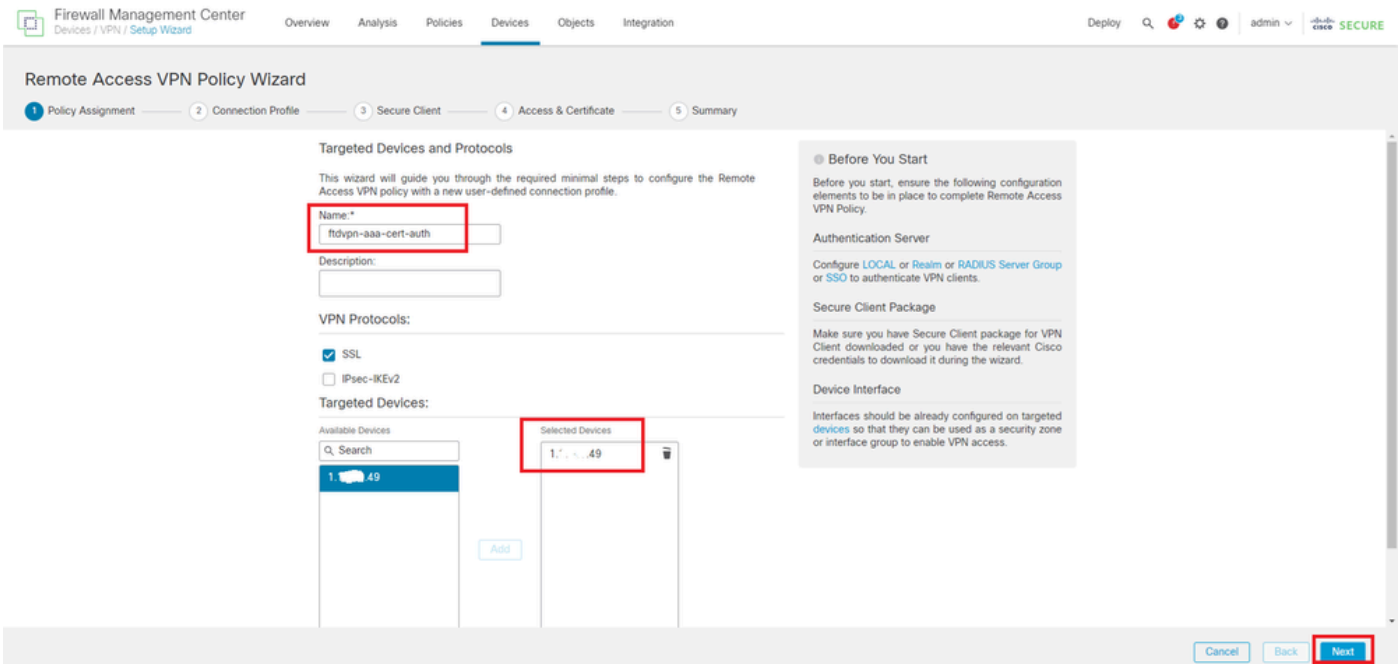
Navigate to **Devices > VPN > Remote Access**, click **Add** button.



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

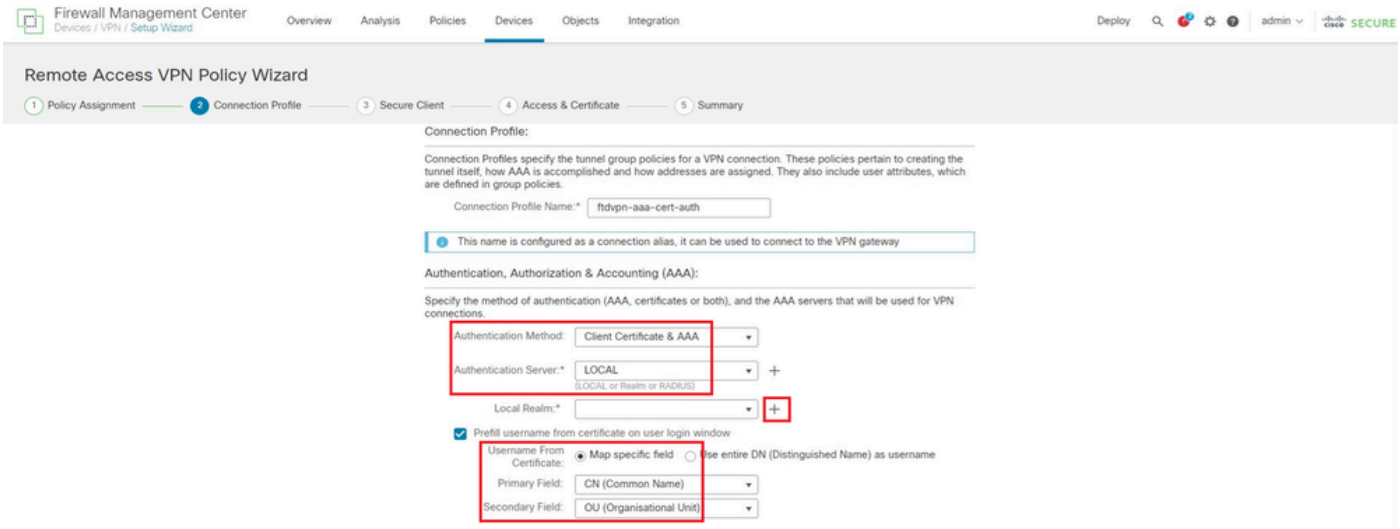


Policy Assignment

Step 4. Config Details for Connection Profile

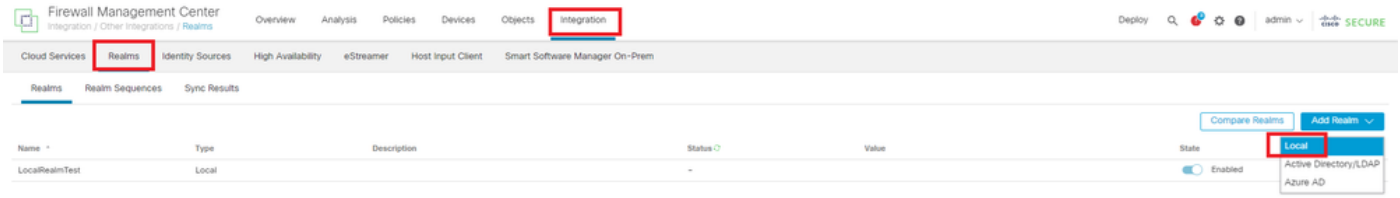
Input necessary information for connection profile and click + button next to the **Local Realm** item.

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



Details of Connection Profile

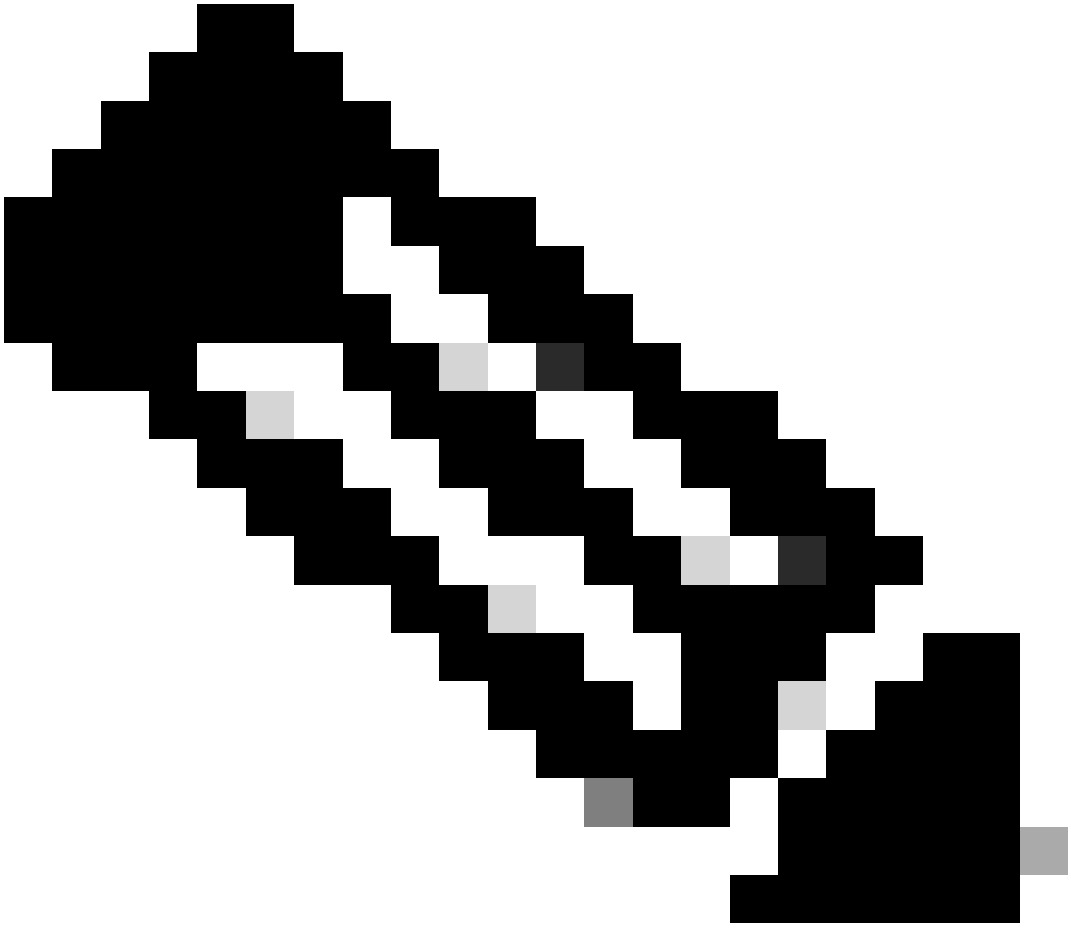
Click **Local** from **Add Realm** drop-down list to add a new local realm.



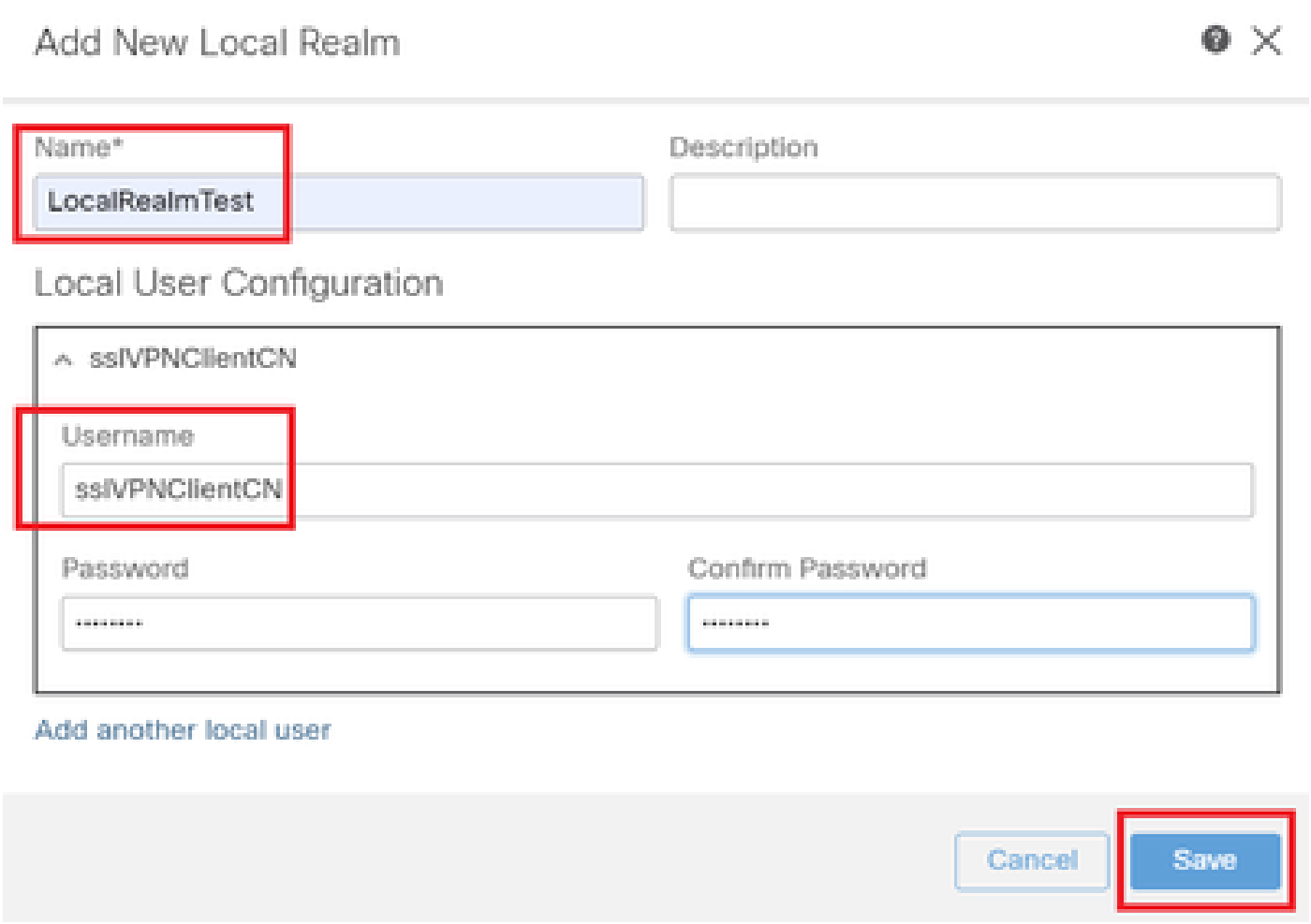
Add Local Realm

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

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



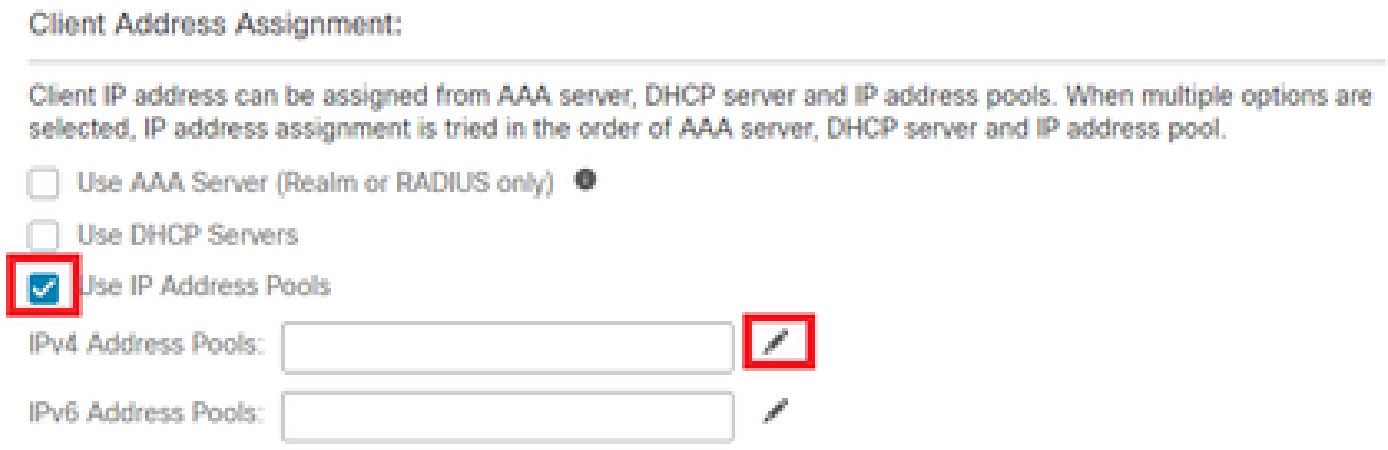
Note: The username equals the common name within the client certificate



Details of Local Realm

Step 5. Add Address Pool for Connection Profile

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

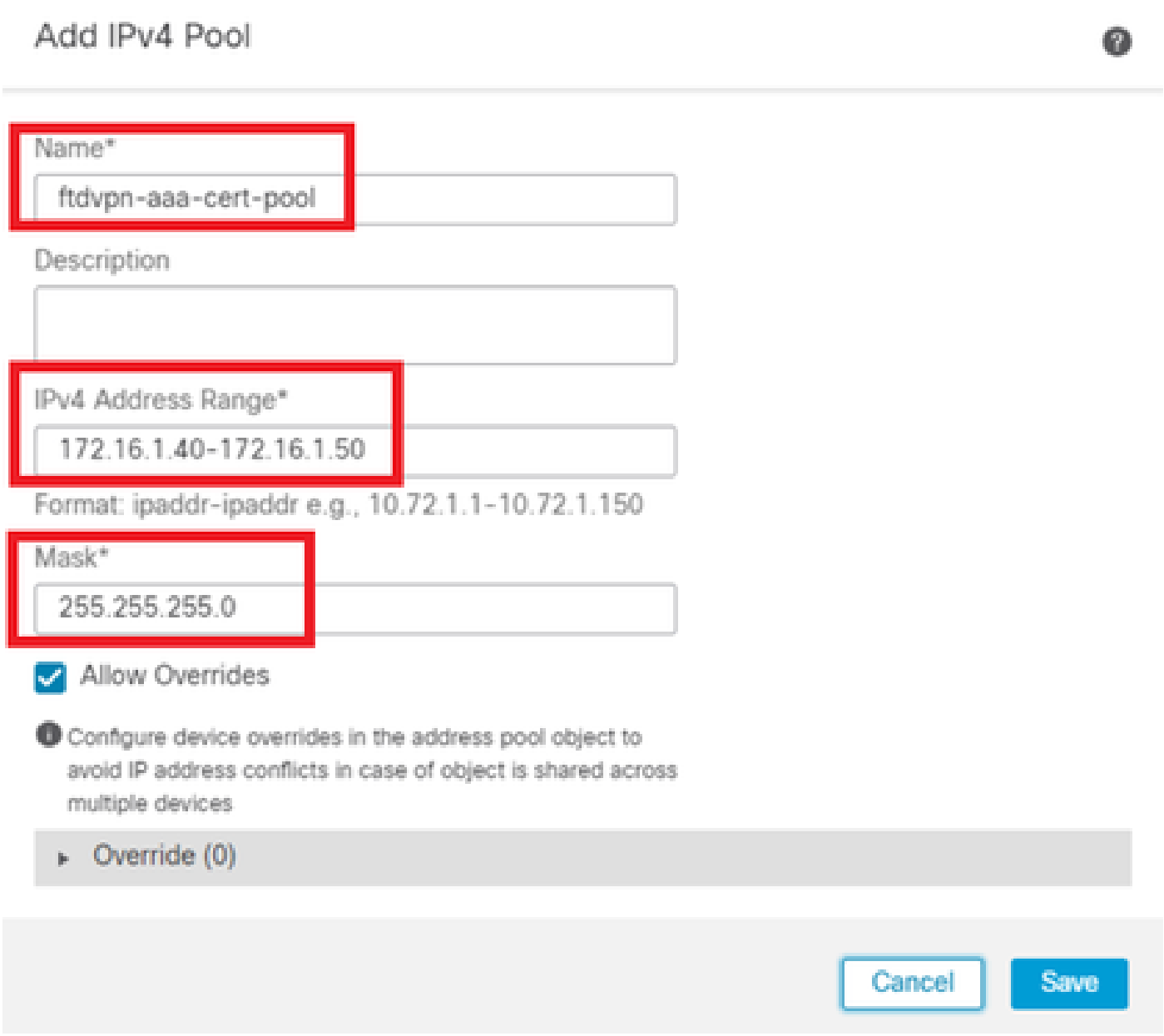


Add IPv4 Address Pool

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

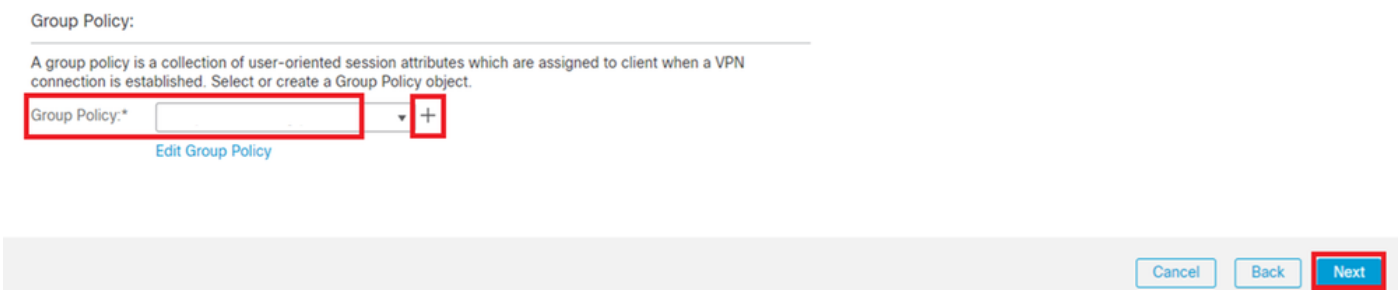
- **Mask** : 255.255.255.0



Details of IPv4 Address Pool

Step 6. Add Group Policy for Connection Profile

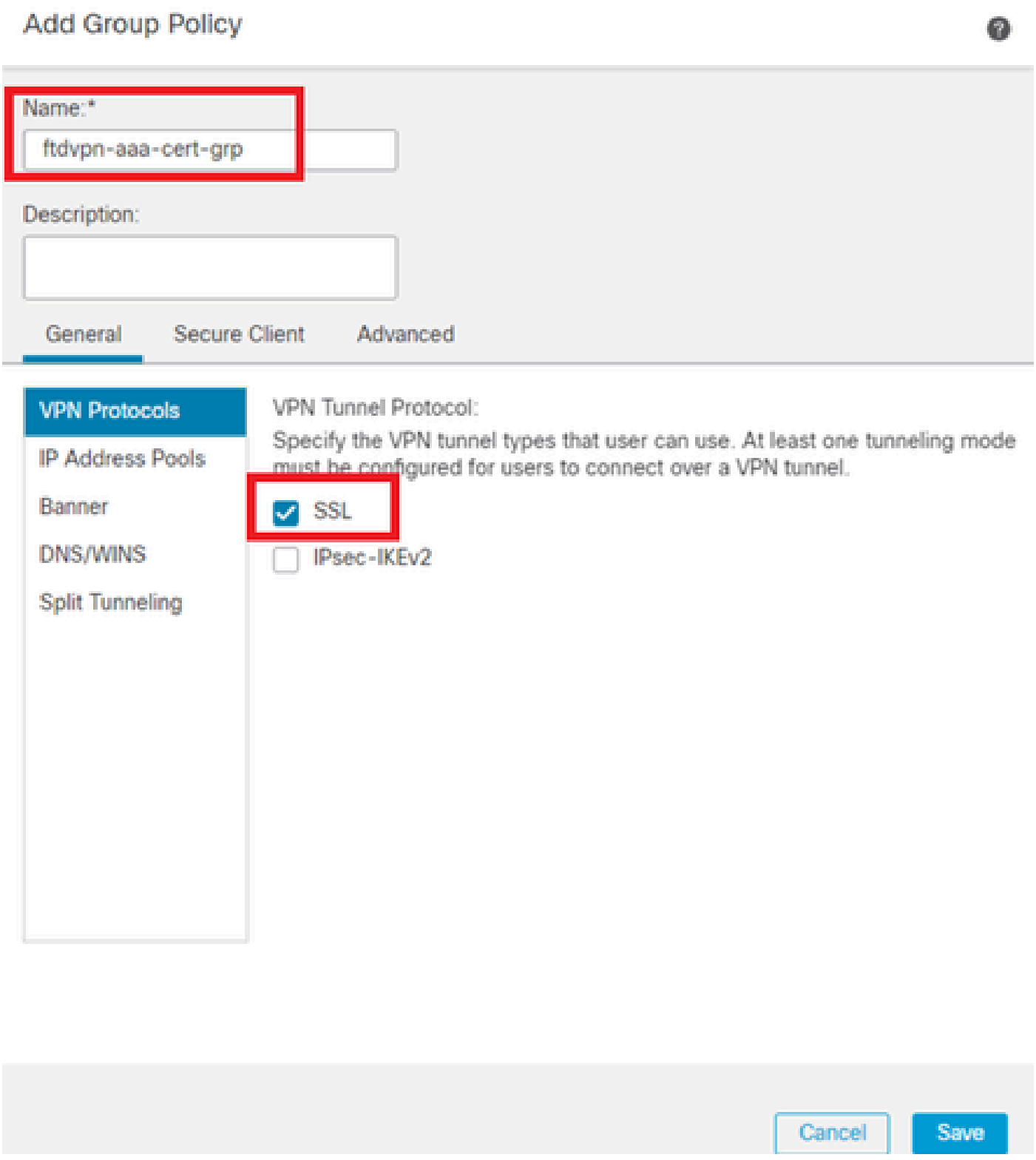
Click + button next to the **Group Policy** item.



Add Group Policy

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

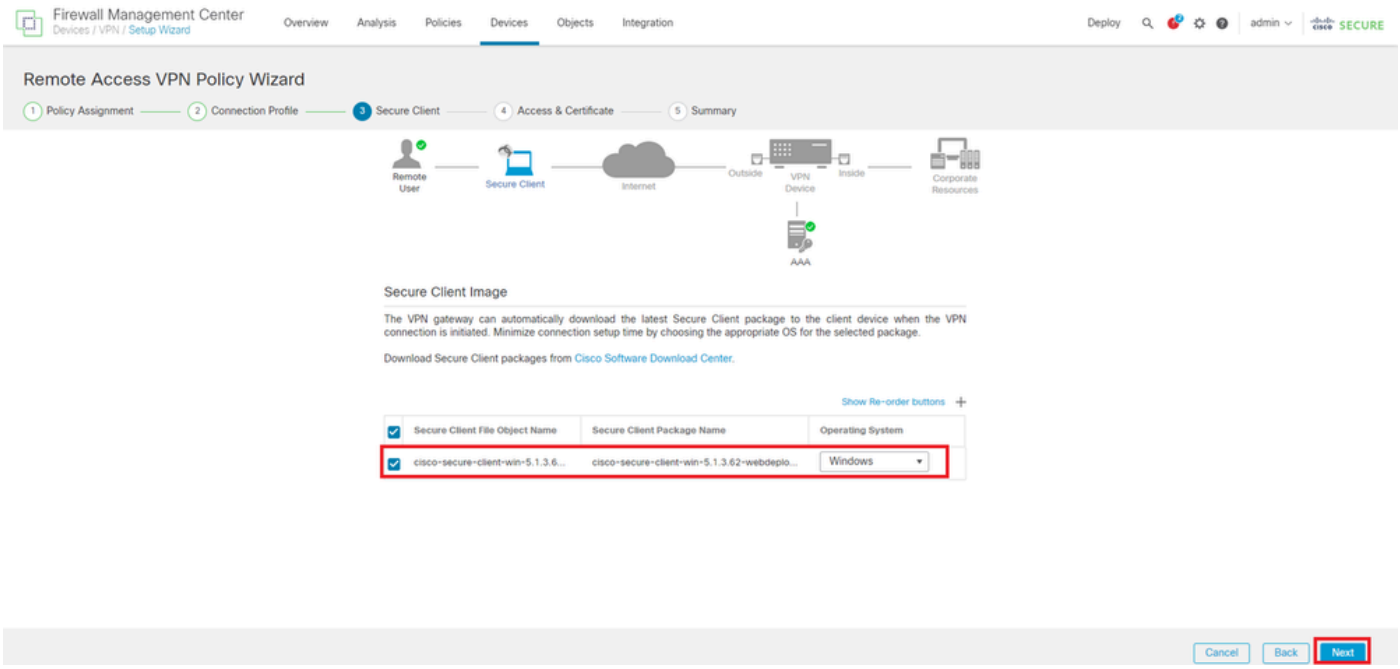
- **Name** : ftdvpn-aaa-cert-grp
- **VPN Protocols** : SSL



Details of Group Policy

Step 7. Config Secure Client Image for Connection Profile

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

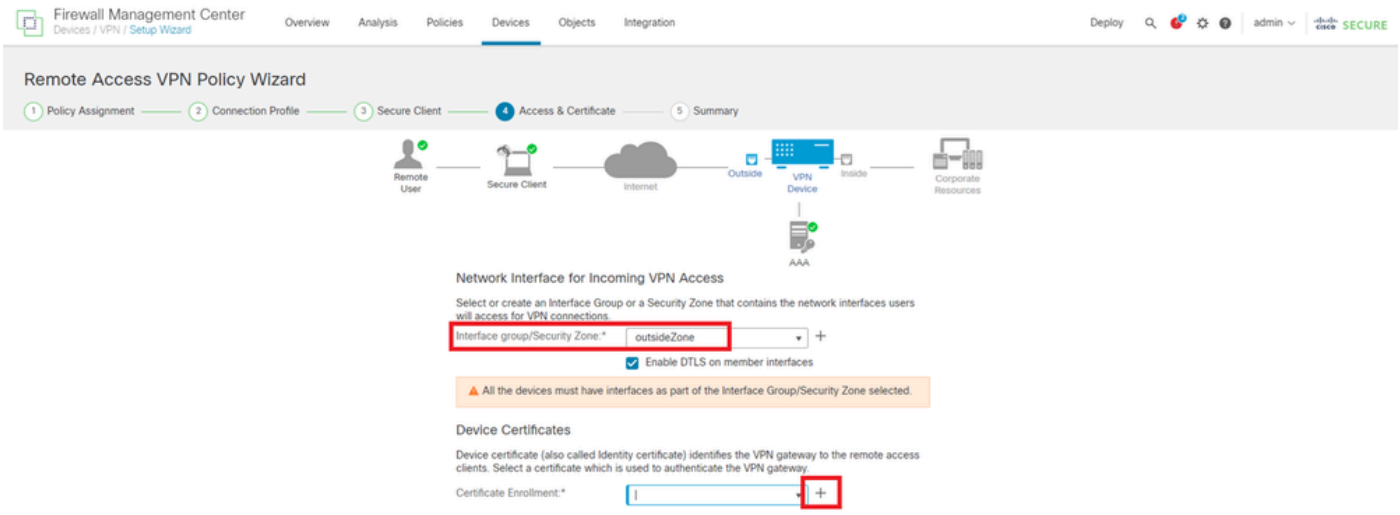


Select Secure Client Image

Step 8. Config Access & Certificate for Connection Profile

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

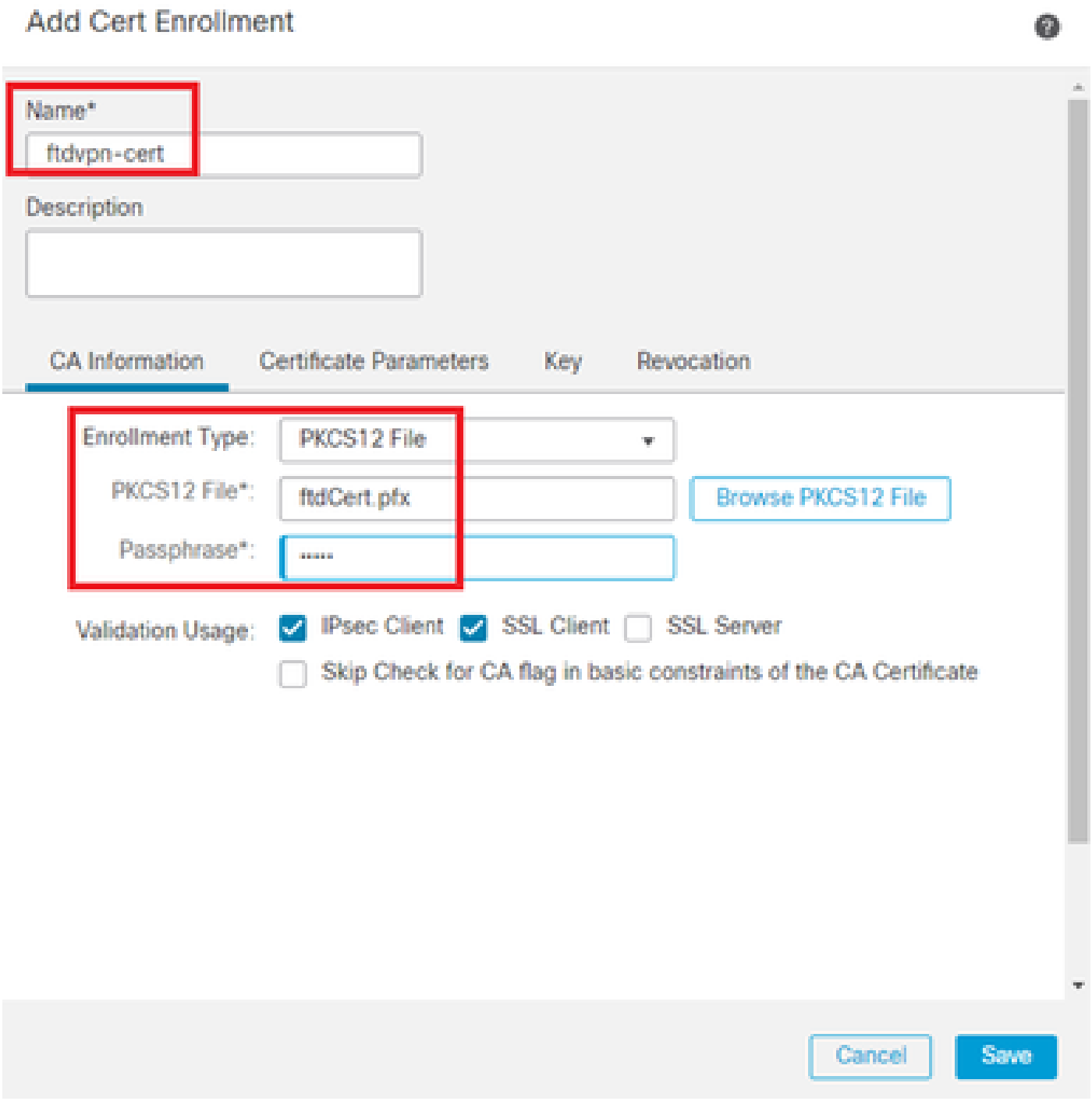
- **Interface group/Security Zone** : outsideZone



Select Security Zone

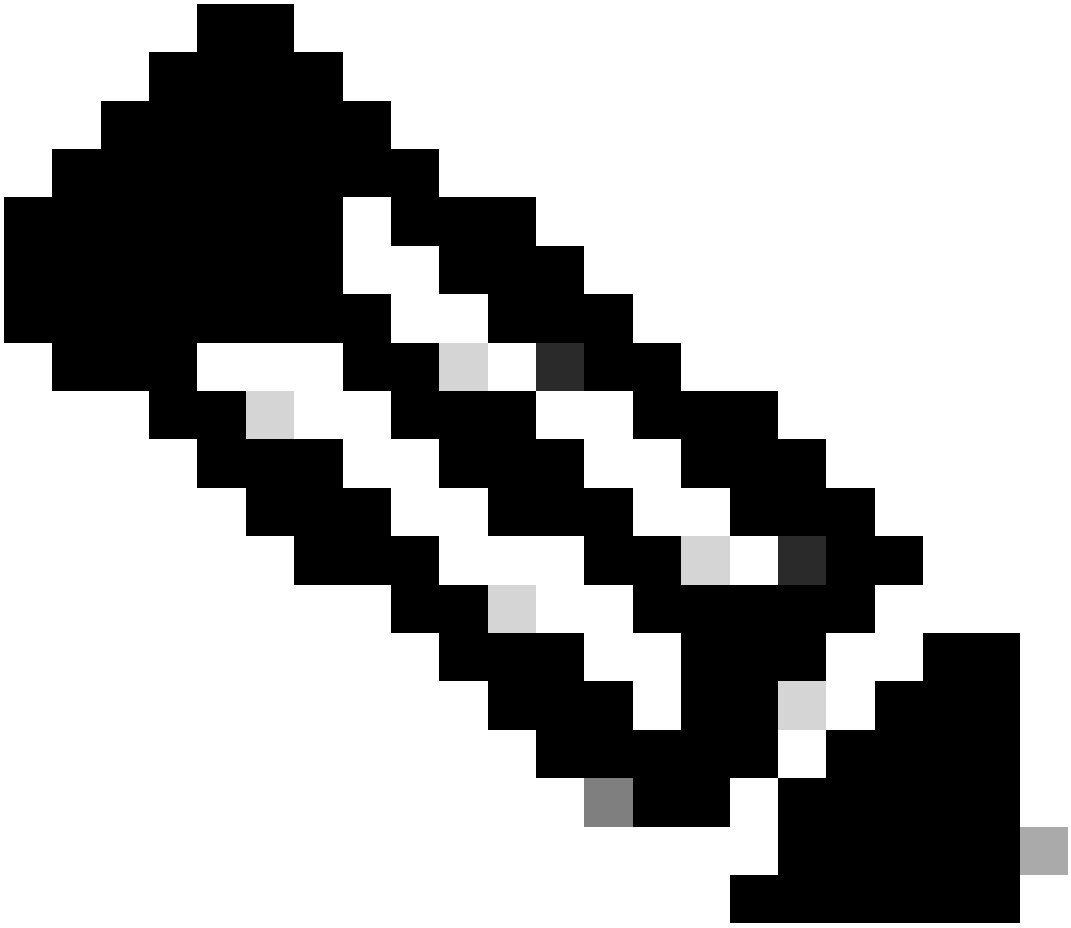
Input necessary information for FTD certificate and import a PKCS12 file from local computer.

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

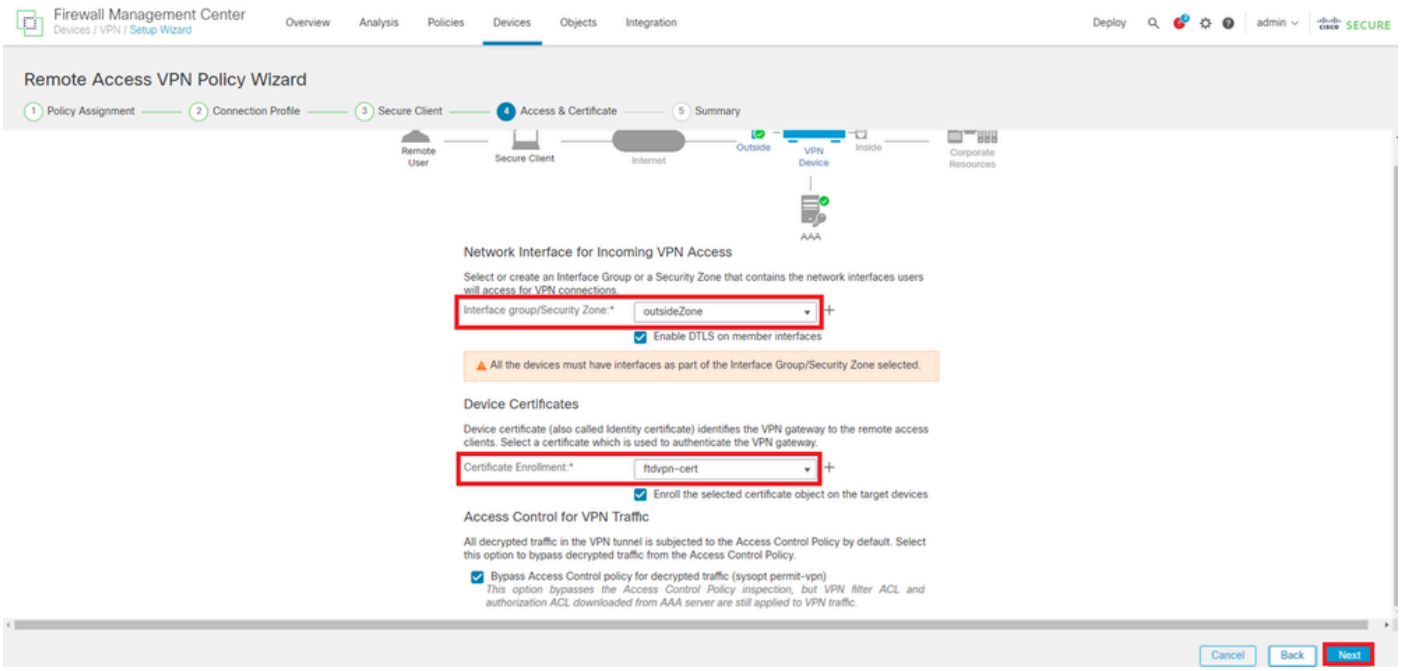


Add FTD Certificate

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



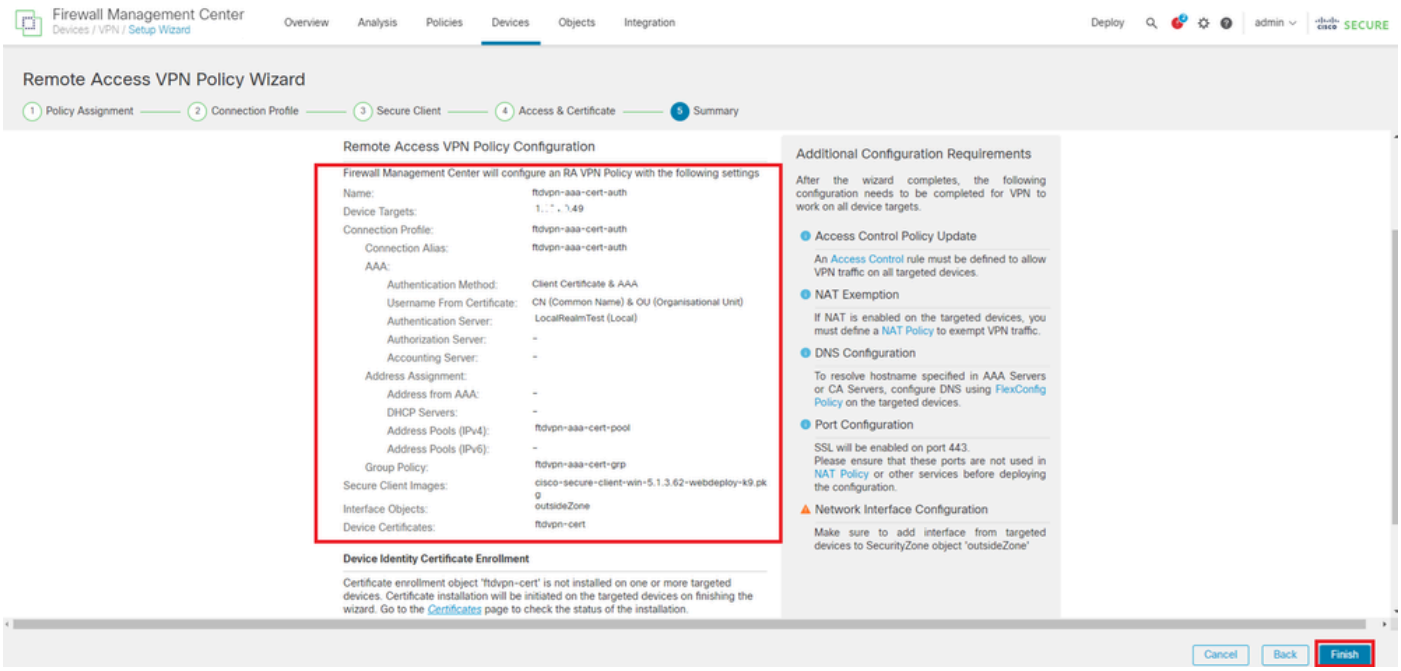
Note: Enable **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**, so that decrypted VPN traffic is not subjected to access control policy inspection.



Confirm Settings in Access & Certificate

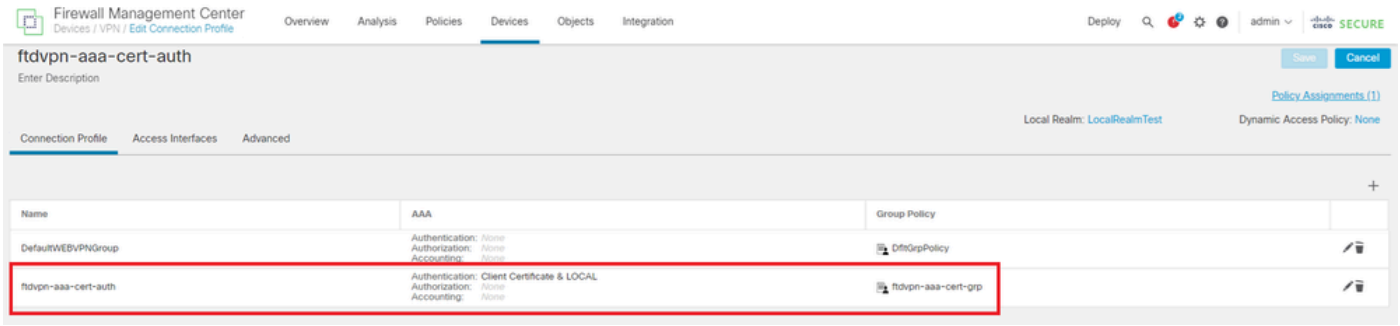
Step 9. Confirm Summary for Connection Profile

Confirm the information entered for VPN connection and click **Finish** button.



Confirm Settings for VPN Connection

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



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

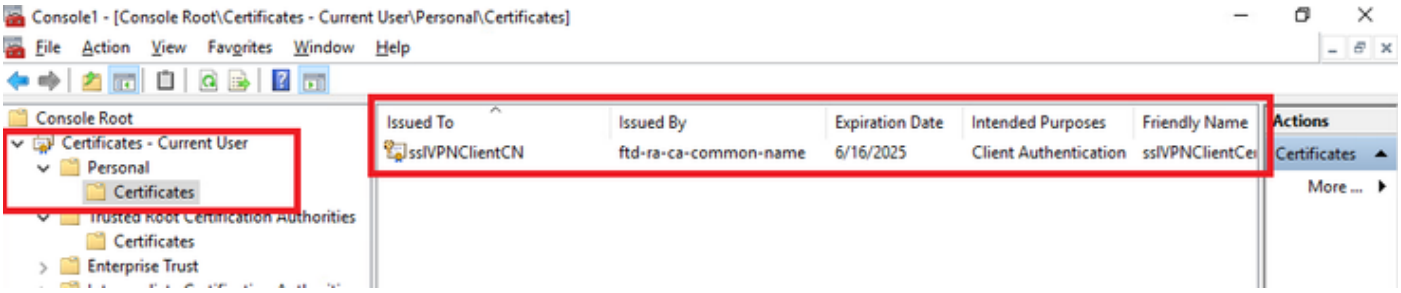
// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show 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

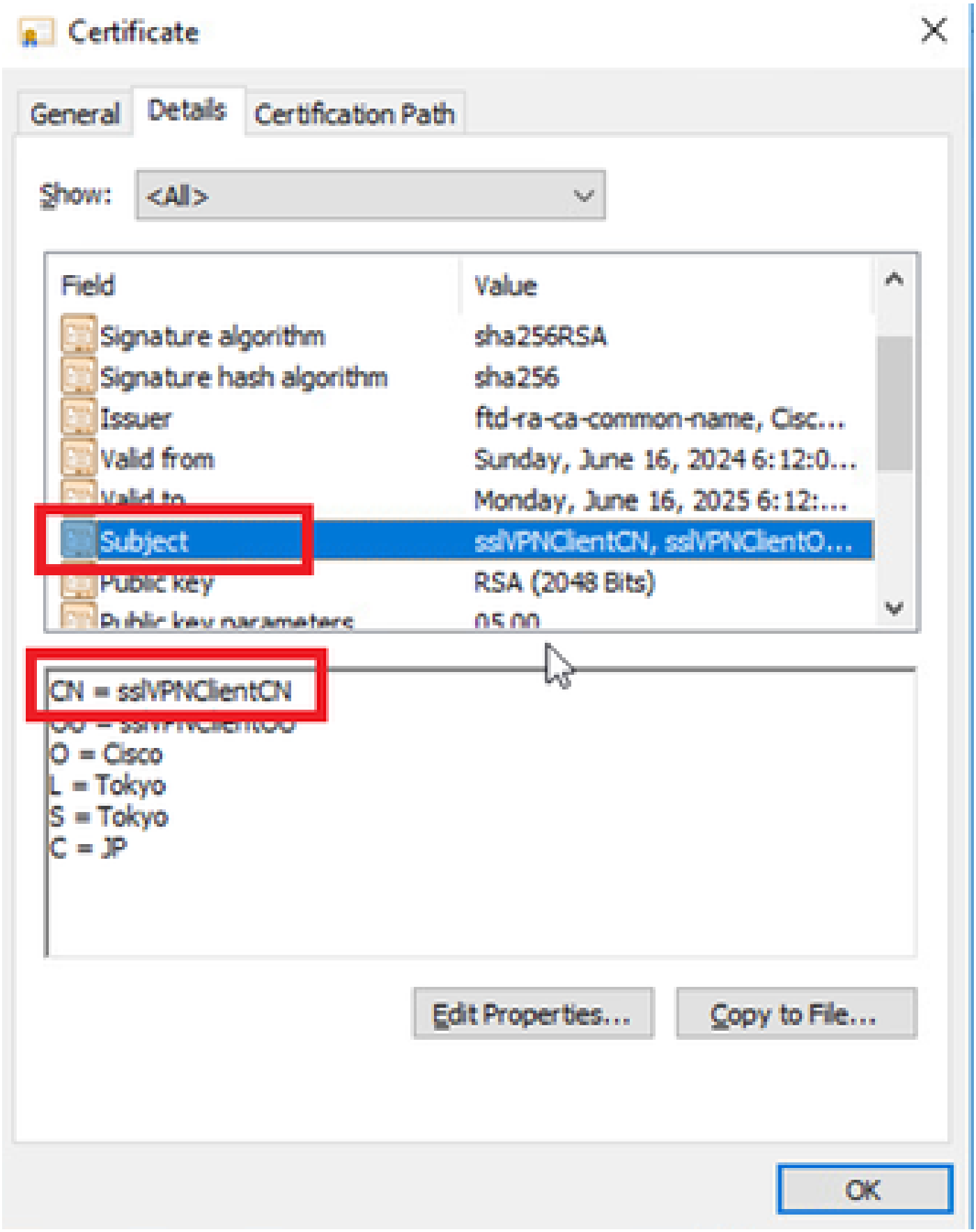
Navigate to **Certificates - Current User > Personal > Certificates**, check the client certificate used for authentication.



Confirm Client Certificate

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

- **Subject** : CN = sslVPNClientCN



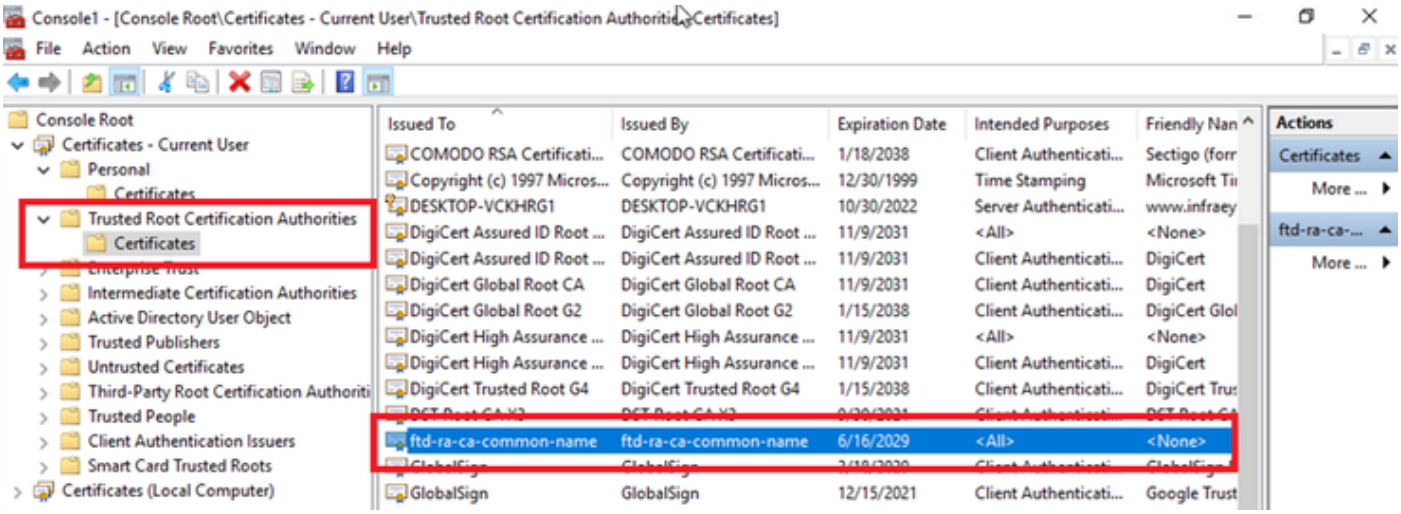
Details of Client Certificate

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

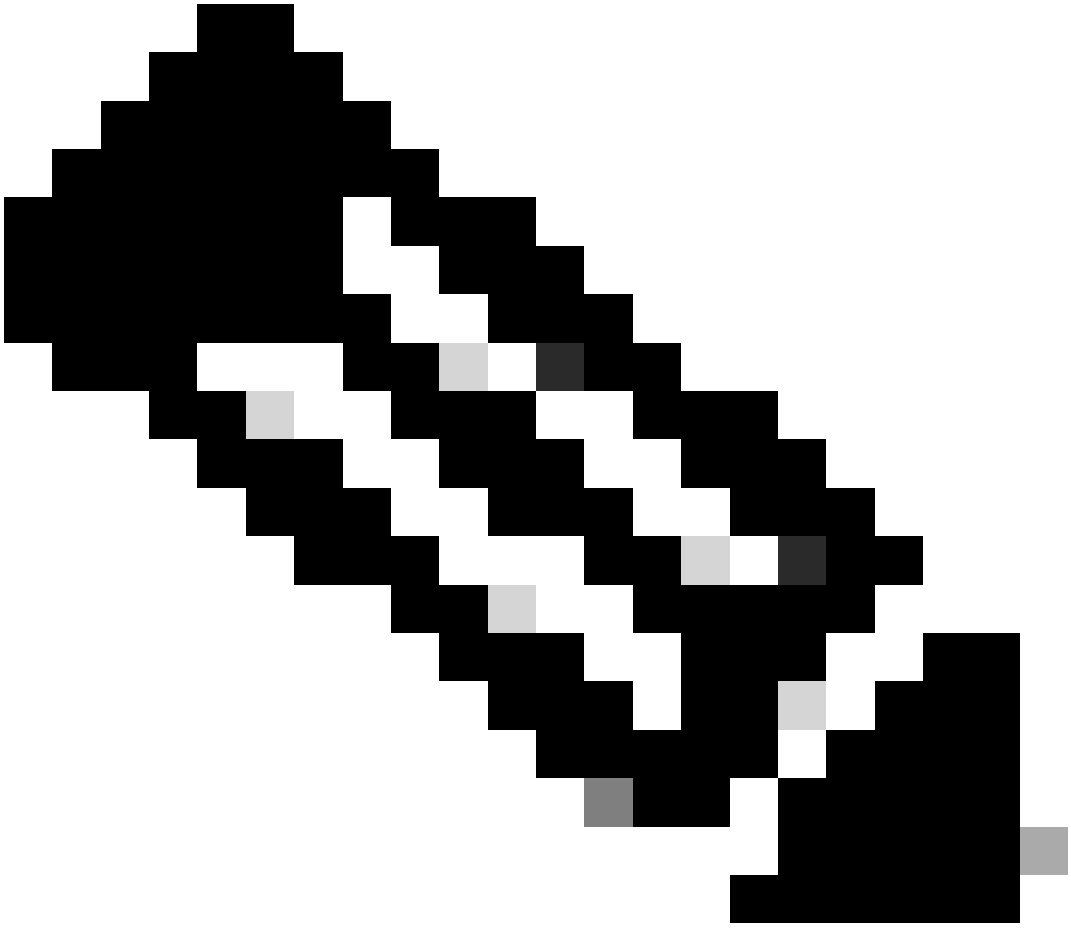


Confirm CA

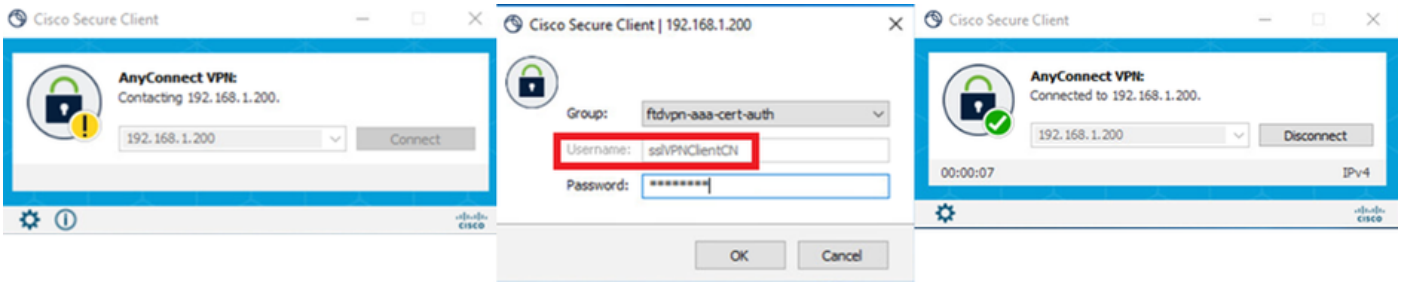
Verify

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.



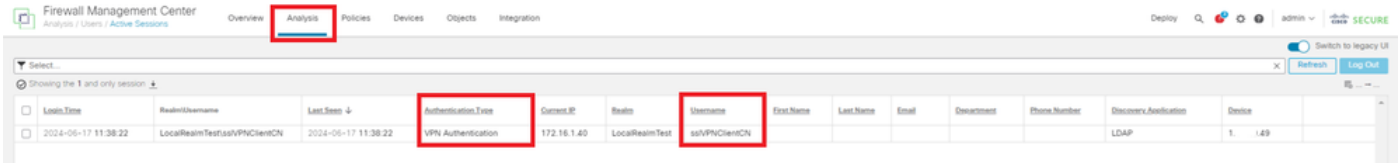
Note: The username is extracted from the CN (Common Name) field of the client certificate in this document.



Initiate VPN Connection

Step 2. Confirm Active Sessions in FMC

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



Confirm Active Session

Step 3. Confirm VPN Session in FTD CLI

Run`show 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 : cb007182000070000666fa19e
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

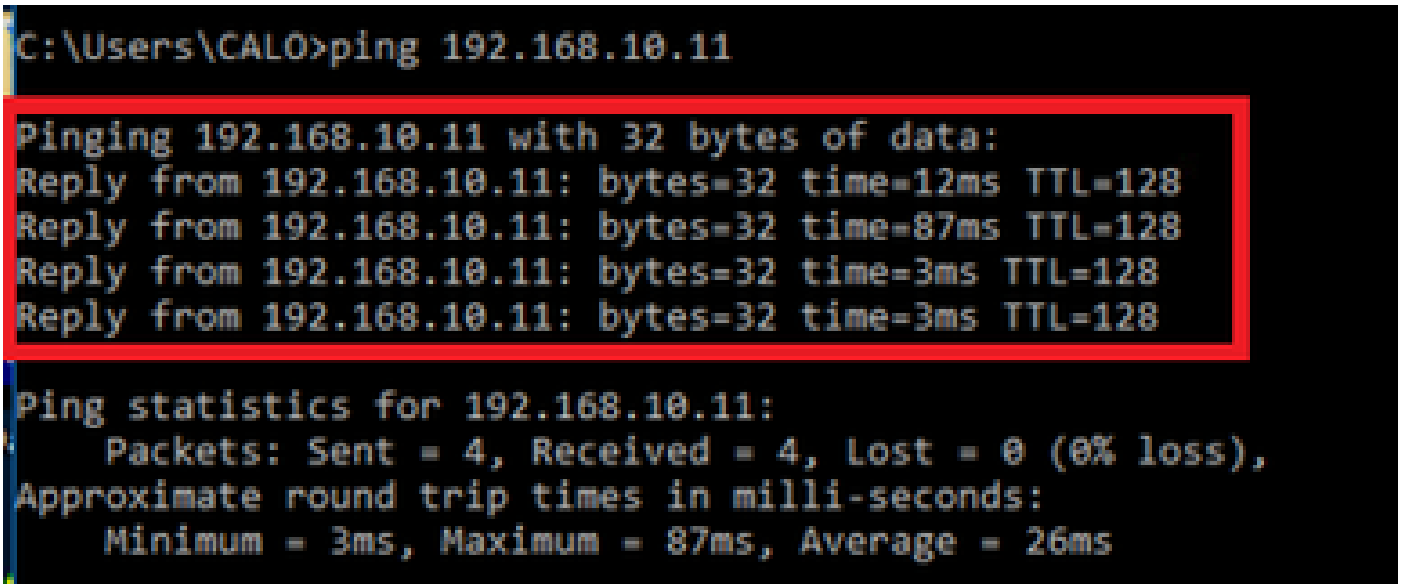
SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
```

```
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.



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 = sslVPN
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