Configure Secure Client Certificate Auth on FTD Managed by FMC

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Network Diagram
- Configurations
  - Create/Import a Certificate Used for Server Authentication
  - Add a Trusted/Internal CA Certificate
  - Configure Address Pool for VPN Users
  - Upload Secure Client Images
  - Create and Upload XML Profile
- Remote Access VPN Configuration

Verify

Troubleshoot

Introduction

This document describes configuring remote access VPN on FTD managed by FMC with certificate authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FMC
- Basic Authentication Knowledge for Remote Access VPN
- Manual Certificate Enrollment and Basic Knowledge of Secure Sockets Layer (SSL)
- Third-party Certificate Authority (CA) such as Entrust, Geotrust, GoDaddy, Thawte, and VeriSign

---

Components Used

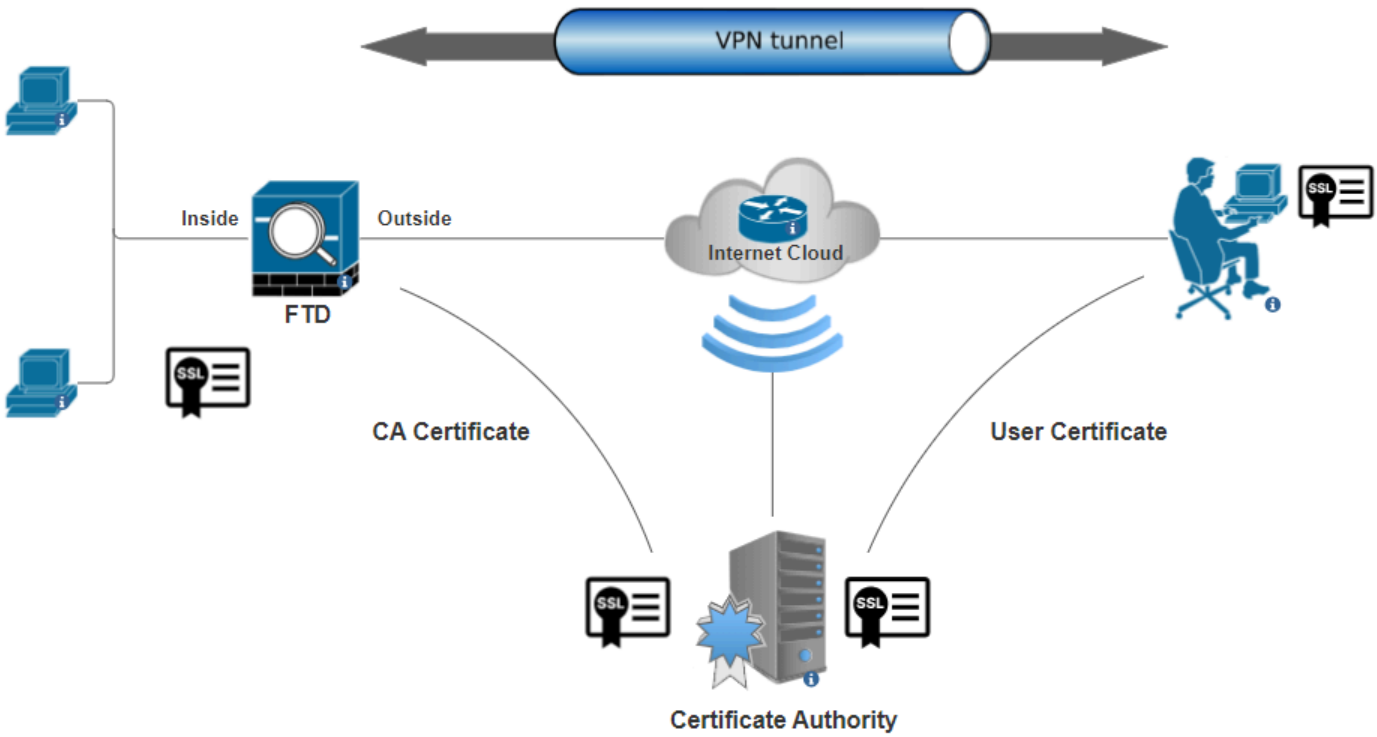
The information in this document is based on these software versions:

- FMC version 7.4.1
- Secure Client Version 5.0.05040
- Secure Firepower Threat Defense Version 7.4.1
- Microsoft Windows Server 2019 as the CA Server

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.

Configure

Network Diagram



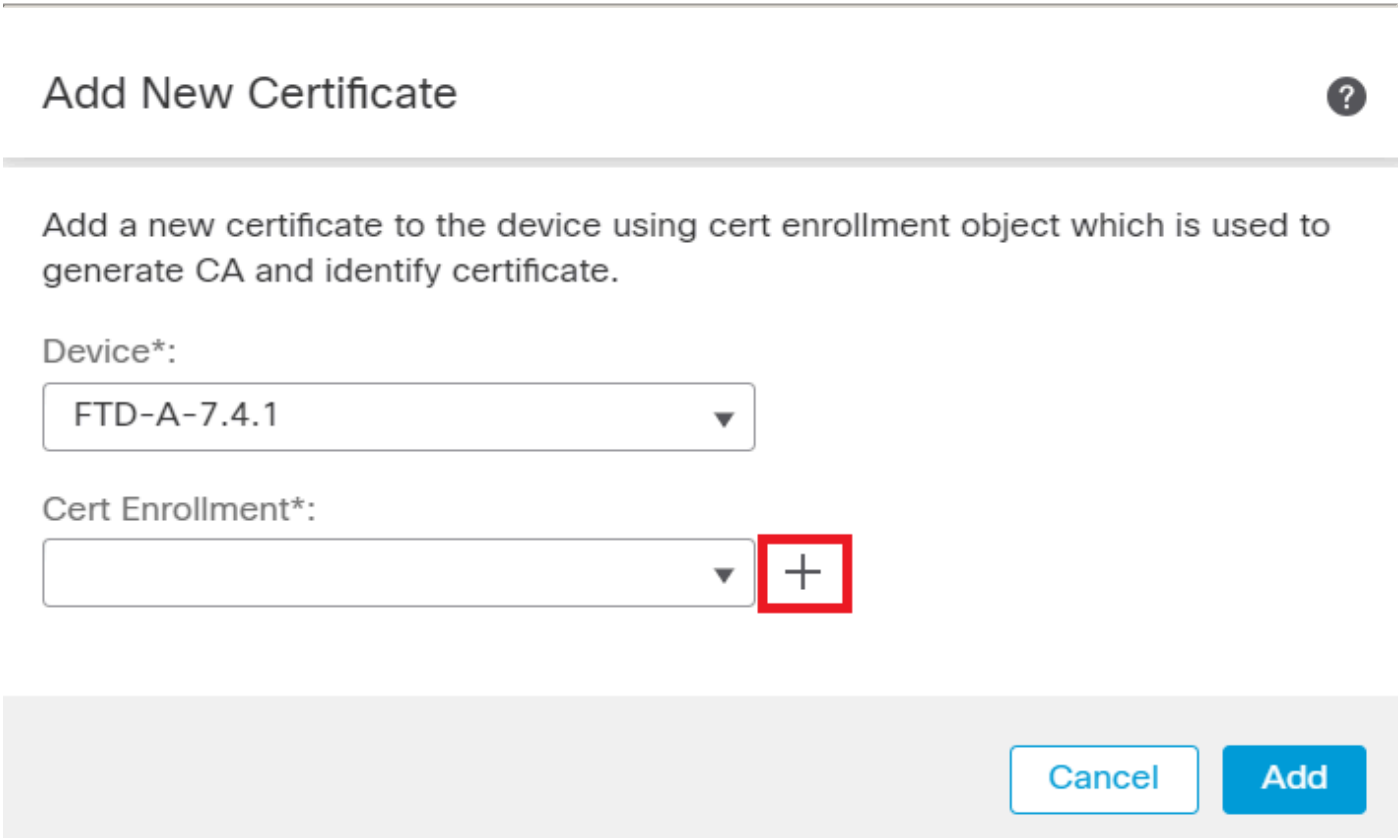
Network Diagram

Configurations

Create/Import a Certificate Used for Server Authentication

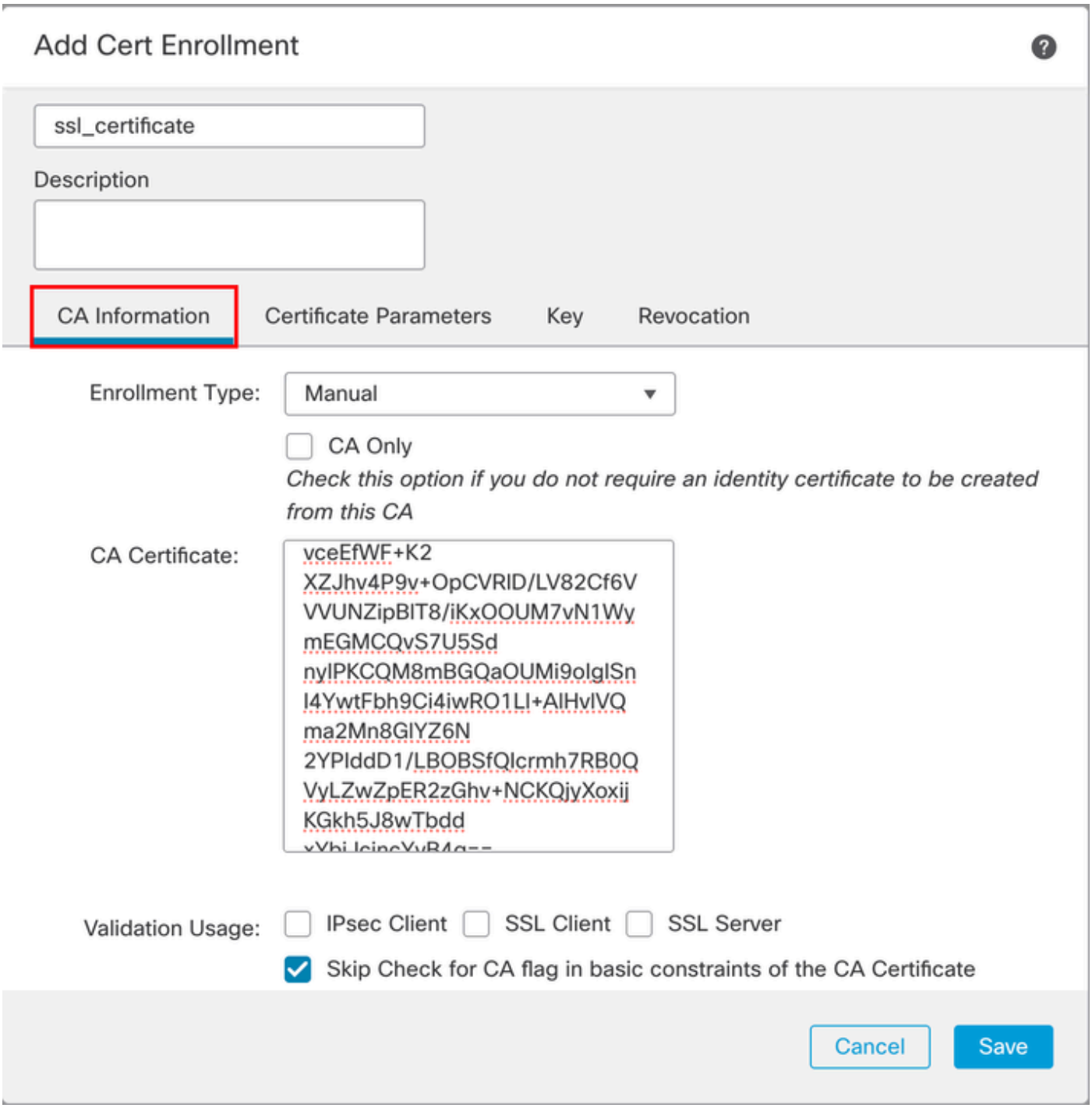
Note: On FMC, a Certificate Authority (CA) is required before you can generate the CSR. If the CSR is generated from an external source (OpenSSL or third-party party), the manual method fails and the PKCS12 certificate format must be used.

1. Navigate to **Devices** > **Certificates** and click **Add**. Choose **Device** and click the plus sign (+) under Cert Enrollment.



Add Cert Enrollment

2. Under **CA Information**, choose the Enrollment Type as **Manual** and paste the CA certificate used to sign the CSR.



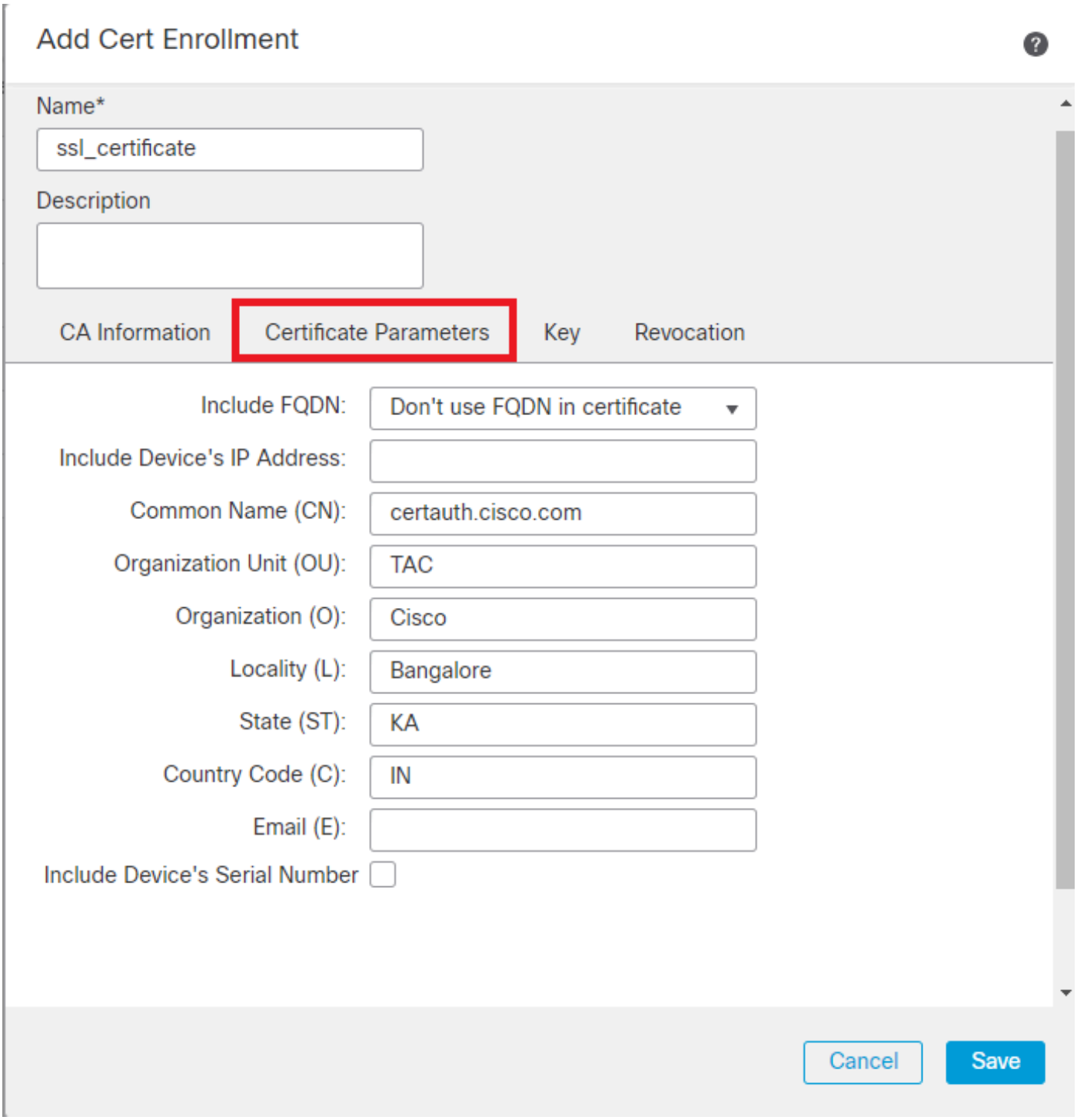
Add CA Information

---

3. Choose **Skip Check for CA flag in basic constraints of the CA Certificate** as shown in the prior image.

---

4. Under **Certificate Parameters**, complete the subject name details.

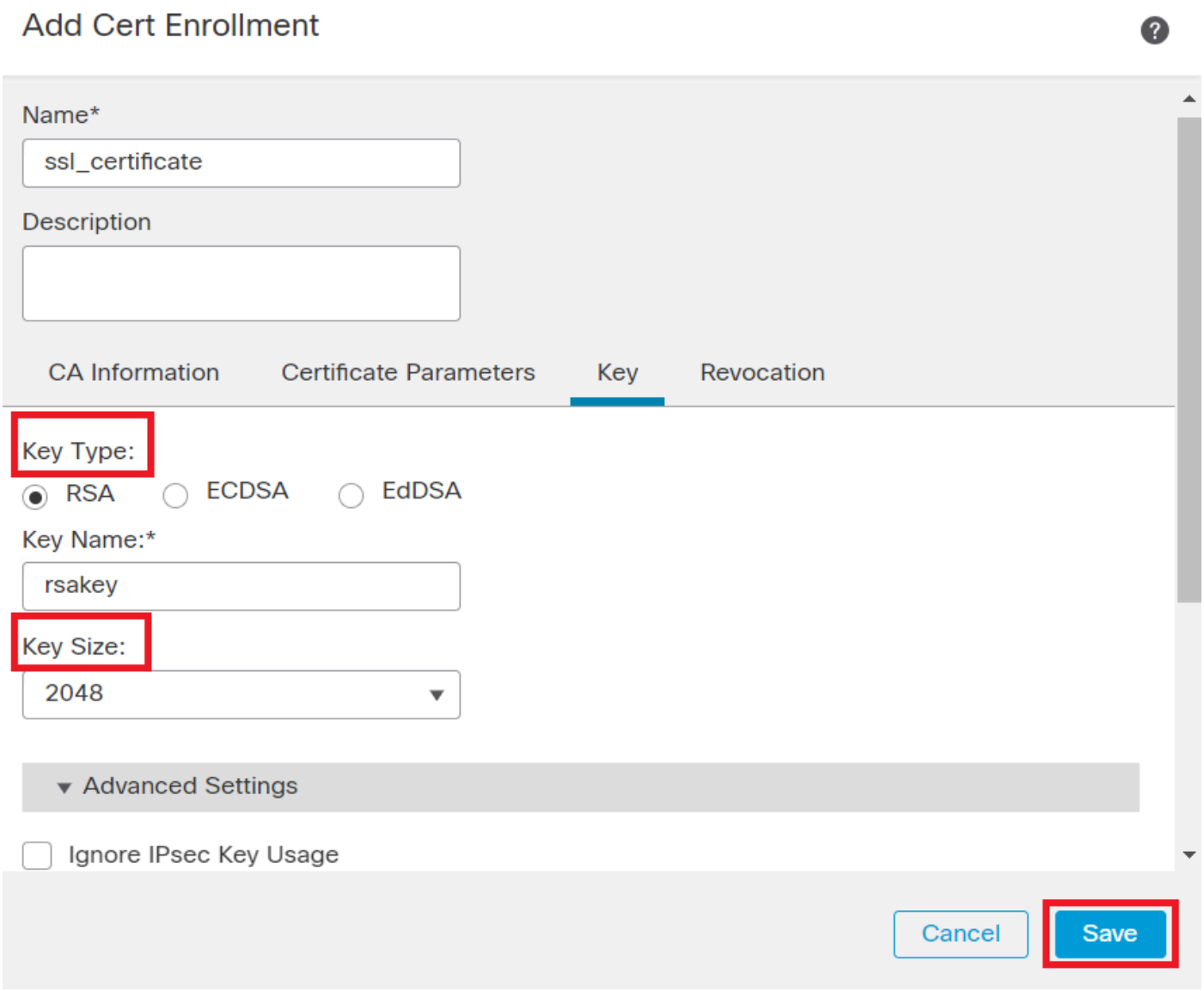


Add Certificate Parameters

---

5. Under **Key**, choose the key type as **RSA** with a key name and size. Click Save.

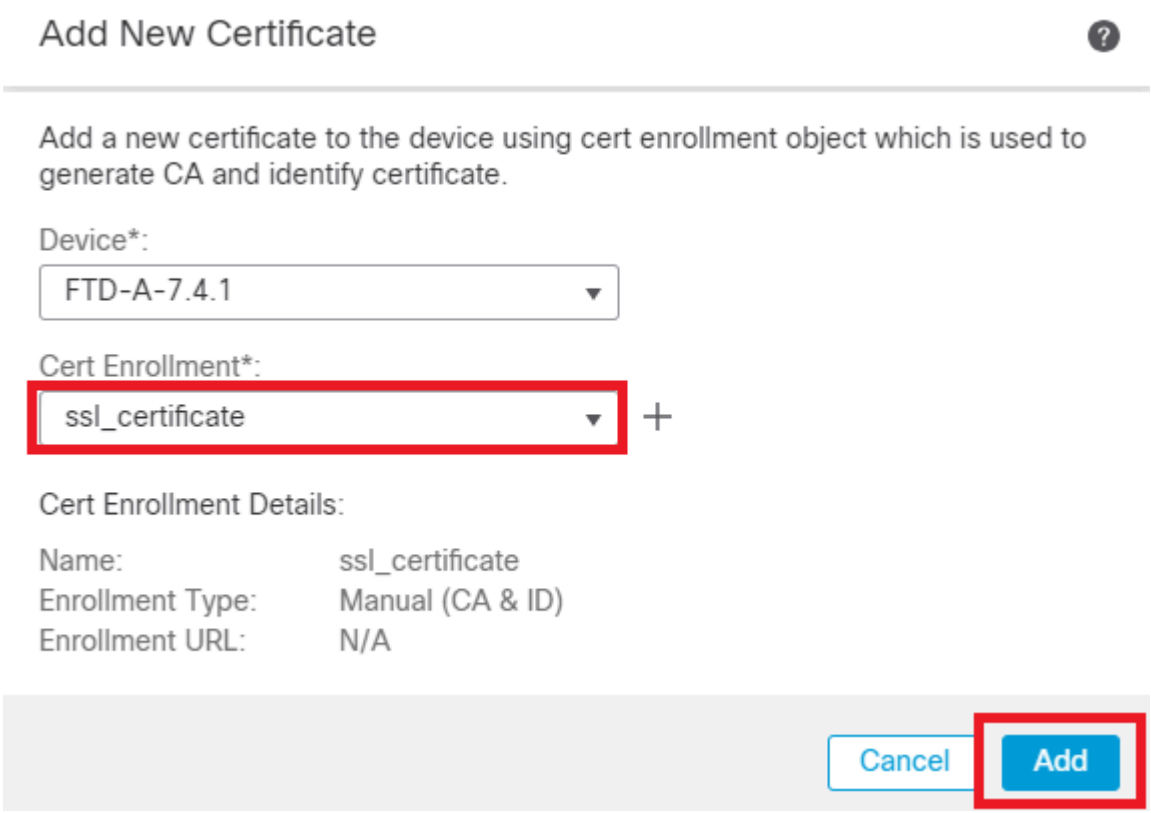
Note: For the RSA key type, the minimum key size is 2048 bits.



Add RSA key

---

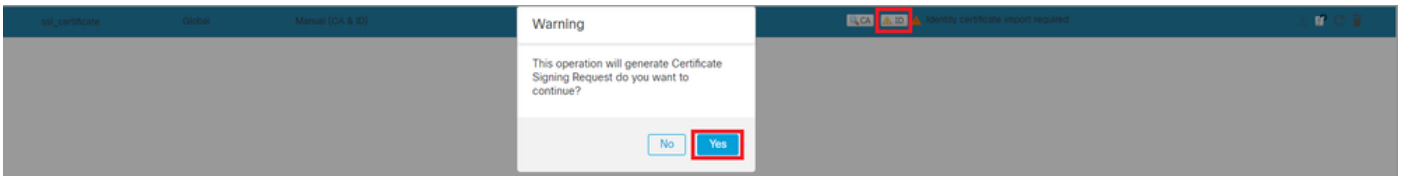
6. Under **Cert Enrollment**, choose the trust point from the drop-down menu, which was just created and click **Add**.



Add new Certificate

---

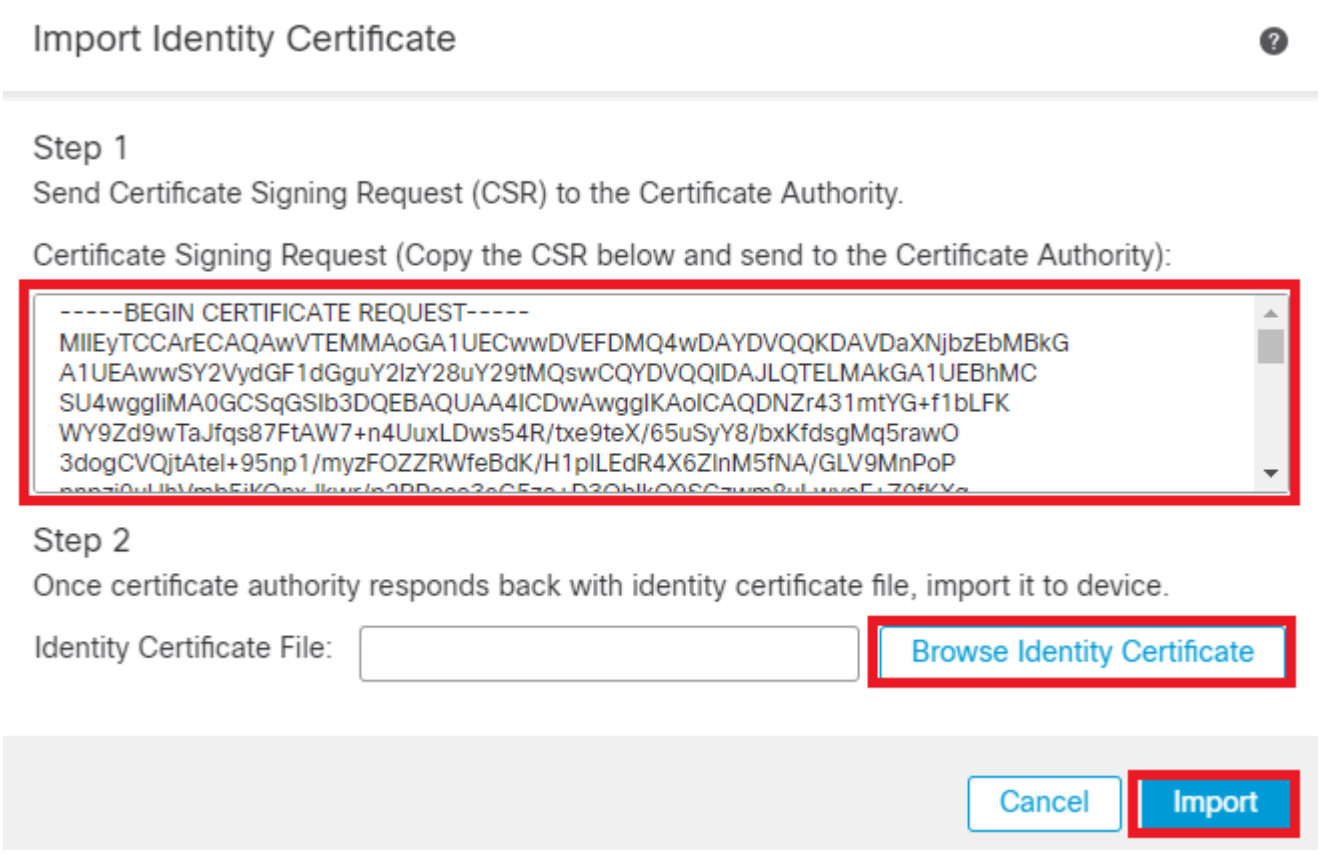
7. Click **ID**, then click **Yes**, to generate the CSR.



Generate CSR

---

8. Copy the CSR and ensure it is signed by the CA. Once the Identity certificate is issued by the CA, import it by clicking **Browse Identity Certificate** and click **Import**.



Import ID Certificate

Note: If the issuance of the ID certificate takes time, you can repeat Step 7. later. This generates the same CSR and you can import the ID certificate.

Add a Trusted/Internal CA Certificate

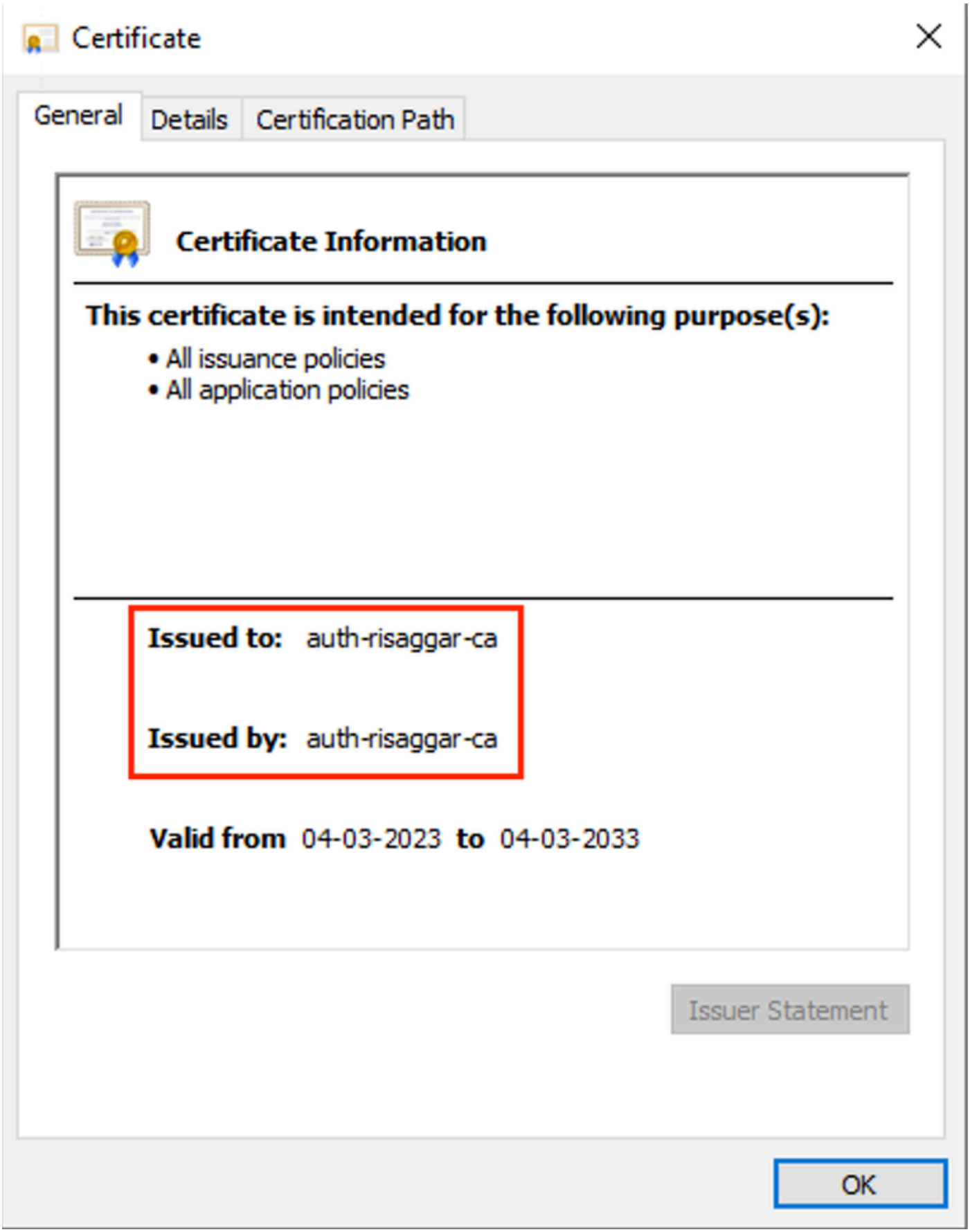
1. Navigate to **Devices > Certificates** and click **Add**.

---

2. Choose **Device** and click the plus sign (+) under Cert Enrollment.

---

3. In this example, **auth-risaggar-ca** is used to issue the identity/user certificates.



auth-risaggar-ca

---

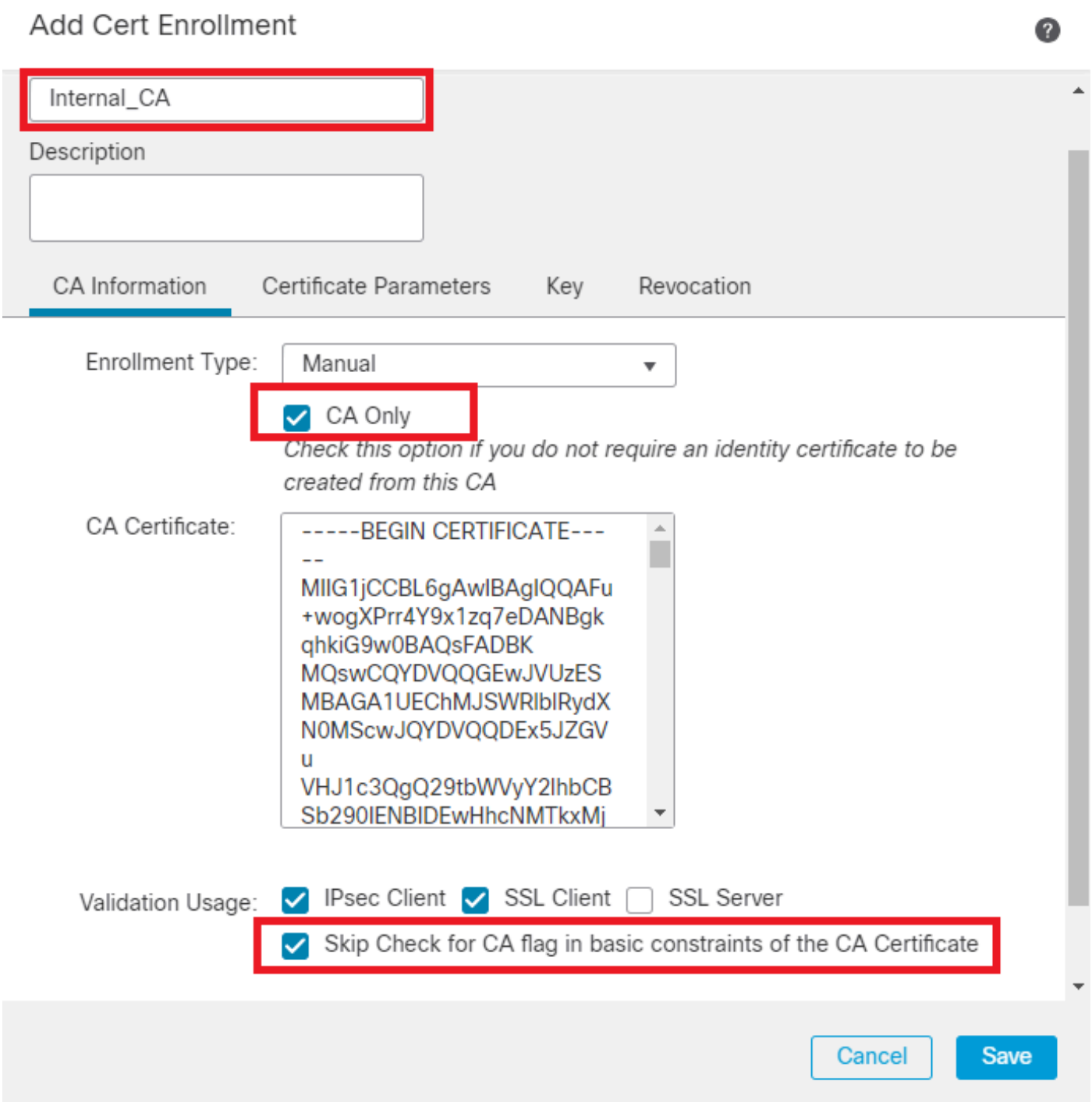
4. Enter a trustpoint name and choose **Manual** as the enrollment type under **CA information**.

---

5. Check **CA Only** and paste the trusted/internal CA certificate in **pem** format.

---

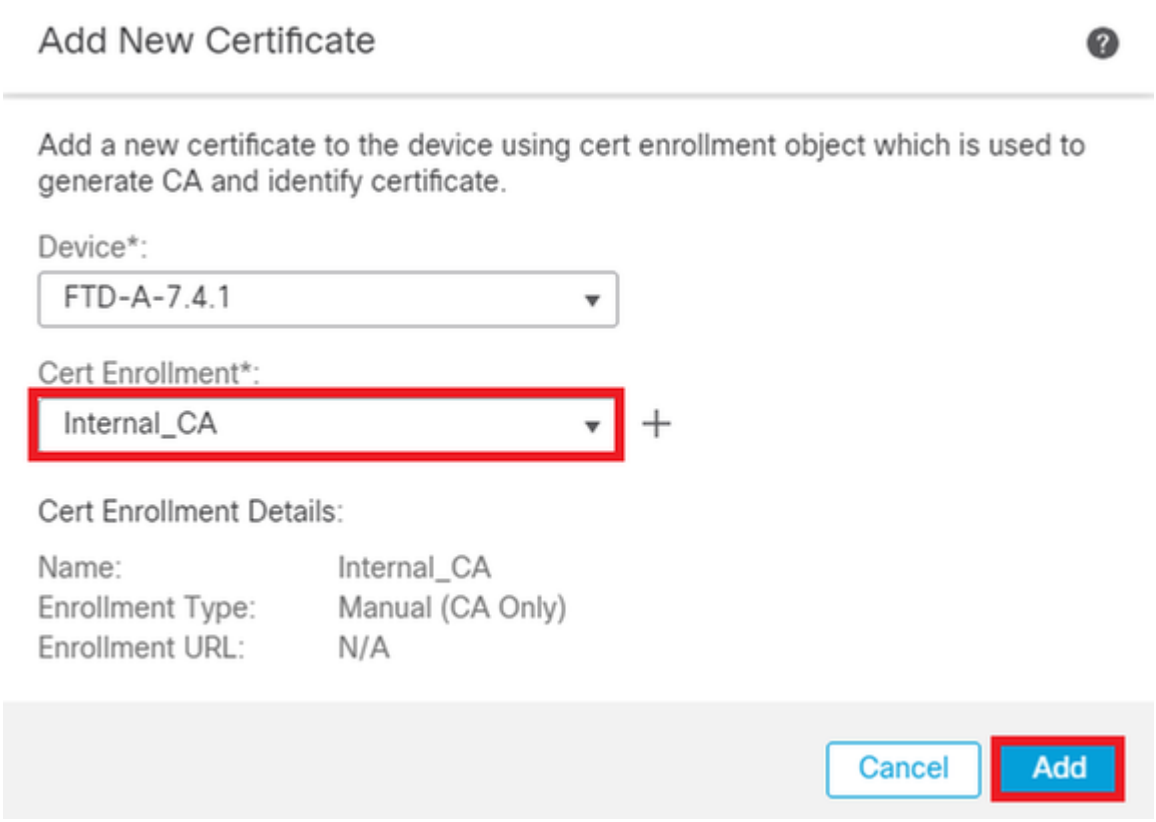
6. Check **Skip Check for CA flag in basic constraints of the CA Certificate** and click Save.



Add Trustpoint

---

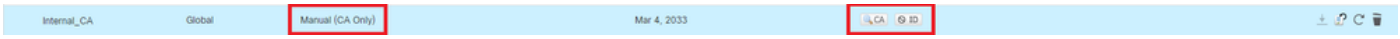
7. Under **Cert Enrollment**, choose the trustpoint from the drop-down menu, which was just created and click Add.



Add Internal CA

---

8. The certificate added earlier is displayed as:



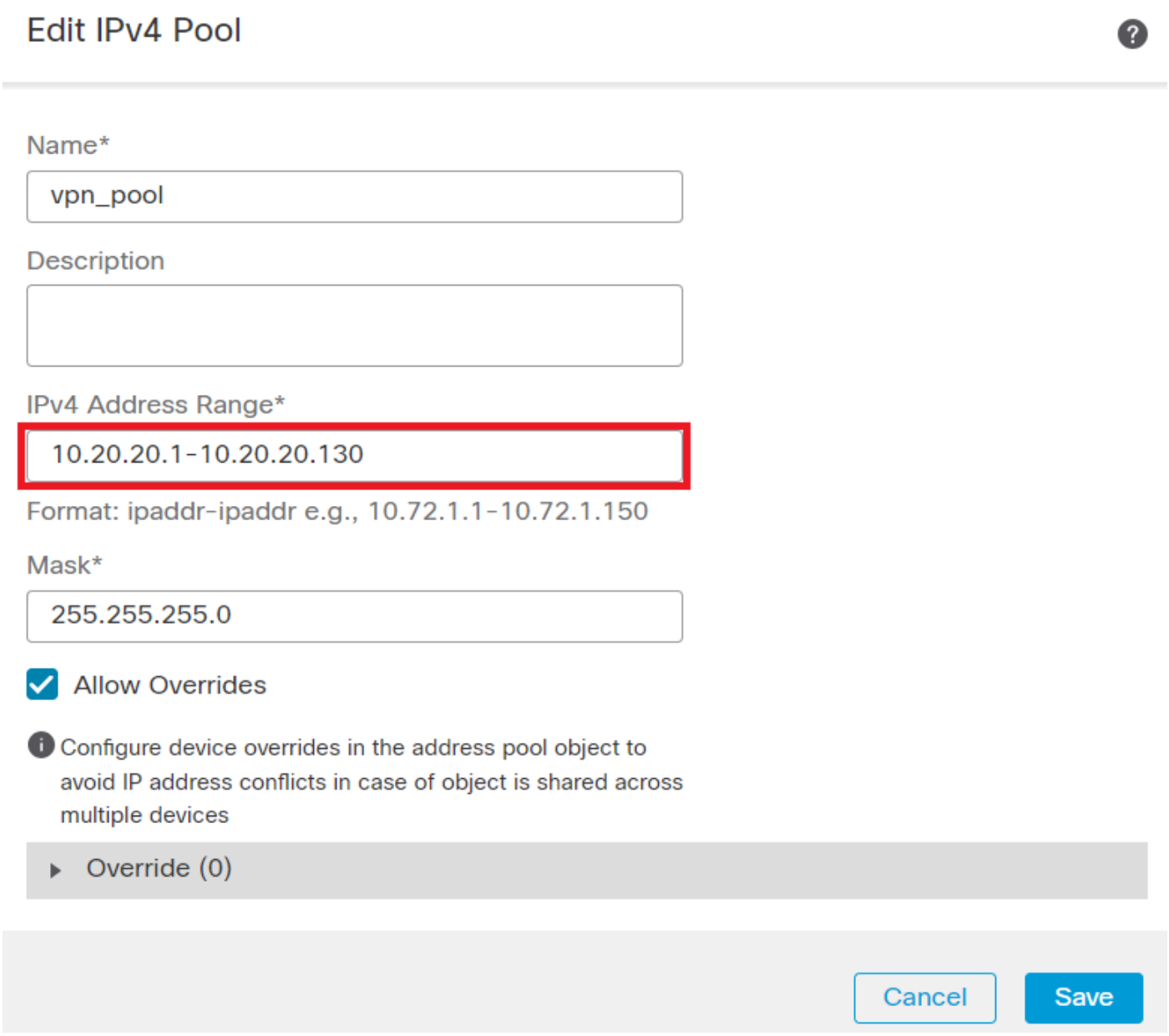
Added Certificate

Configure Address Pool for VPN Users

1. Navigate to **Objects > Object Management > Address Pools > IPv4 Pools**.

---

2. Enter the name and IPv4 address range with a mask.



Add IPv4 Pool

Upload Secure Client Images

1. Download web deploy secure client images per the OS from the Cisco Software site.

---

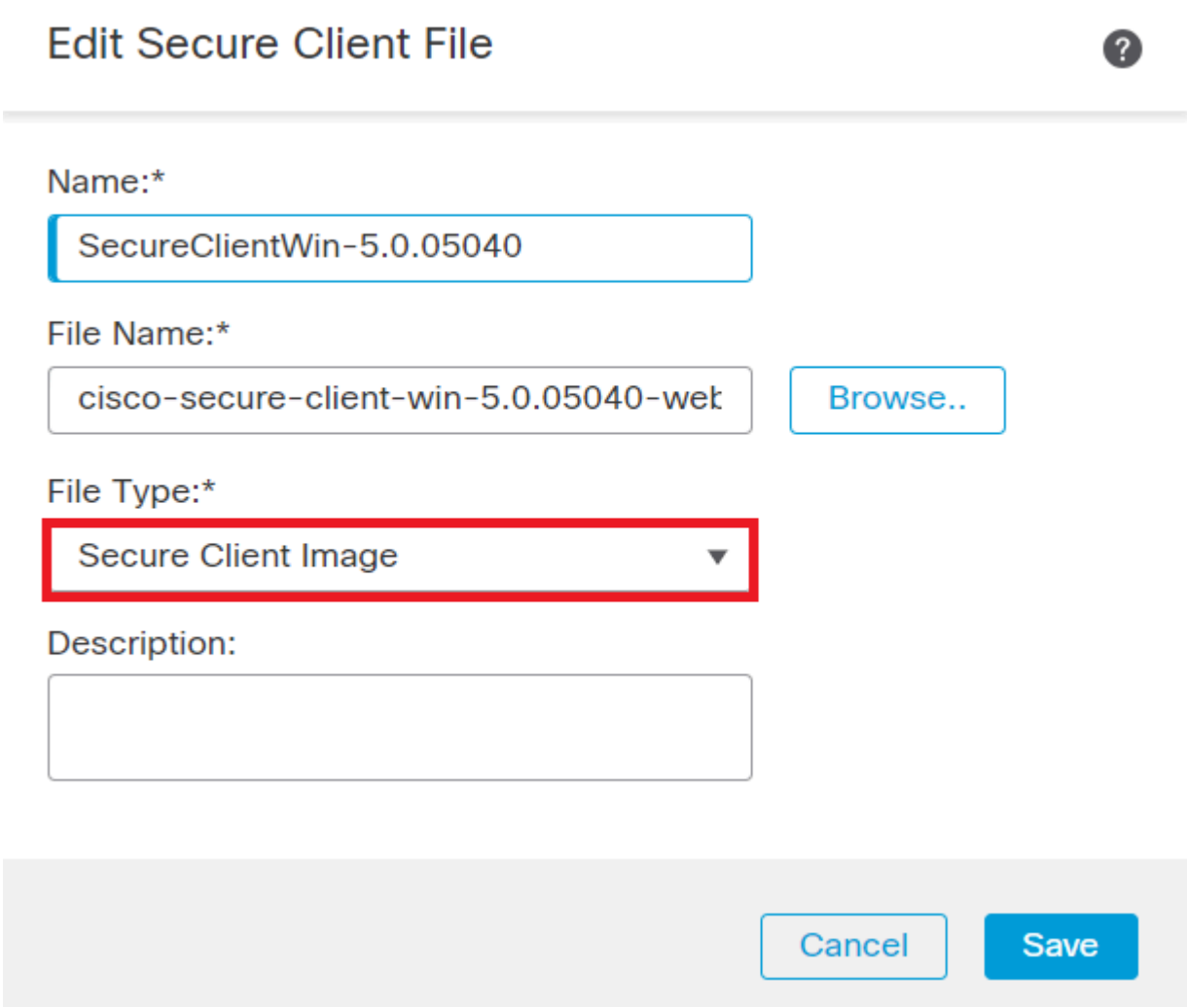
2. Navigate to **Objects > Object Management > VPN > Secure Client File > Add Secure Client File**.

---

3. Enter the name and choose the Secure Client file from the disk.

---

4. Choose the file type as **Secure Client Image** and click **Save**.



Add Secure Client Image

Create and Upload XML Profile

1. Download and install the Secure Client **Profile Editor** from the Cisco Software site.

---

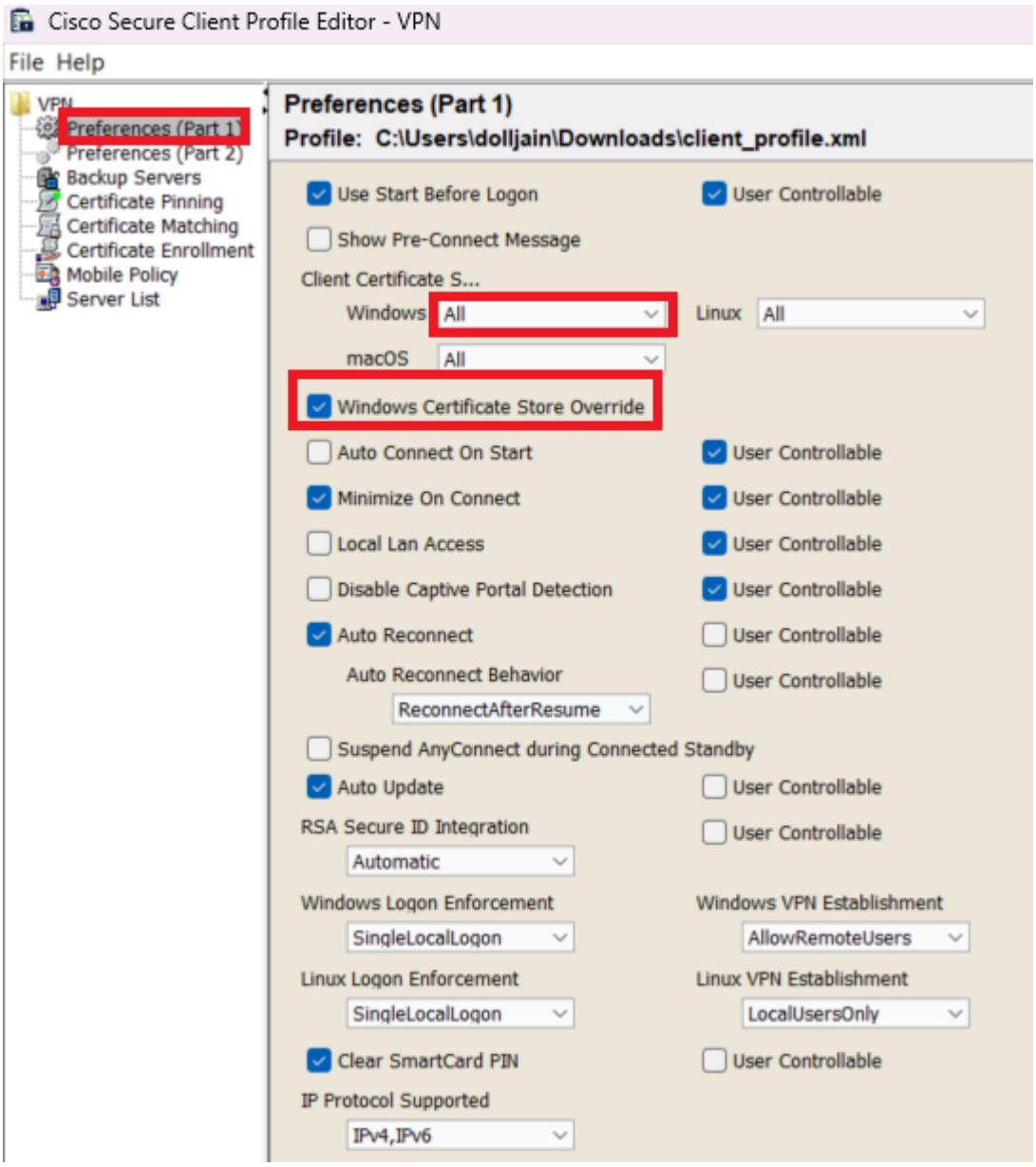
2. Create a new profile and choose **All** from the Client Certificate Selection drop down menu. This mainly controls which certificate are stored and which certificate Secure Client can use to based on what has been stored and to read certificates.

Two other available options are:

i. **Machine**: Secure Client is restricted to certificate lookup on the Windows local machine certificate store.
ii. **User**: Secure Client is restricted to certificate lookup on the local Windows user certificate store.

Set Certificate Store Override as **True**.

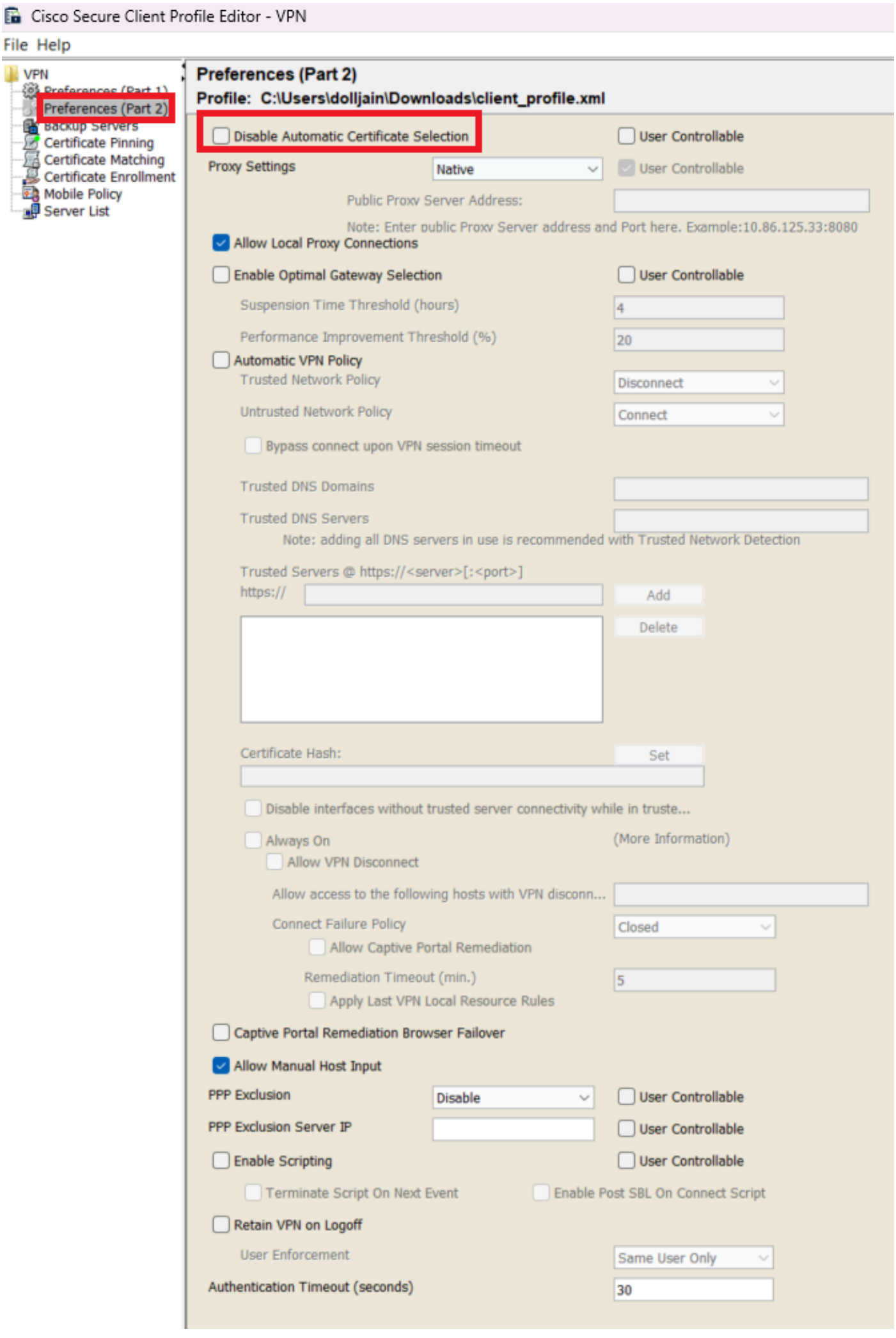
This allows an administrator to direct Secure Client to utilize certificates in the Windows machine (Local System) certificate store for client certificate authentication. Certificate Store Override only applies to SSL, where the connection is initiated, by default in the UI process. When using IPSec/IKEv2, this feature in the Secure Client Profile is not applicable.



Add Preferences (Part1)

---

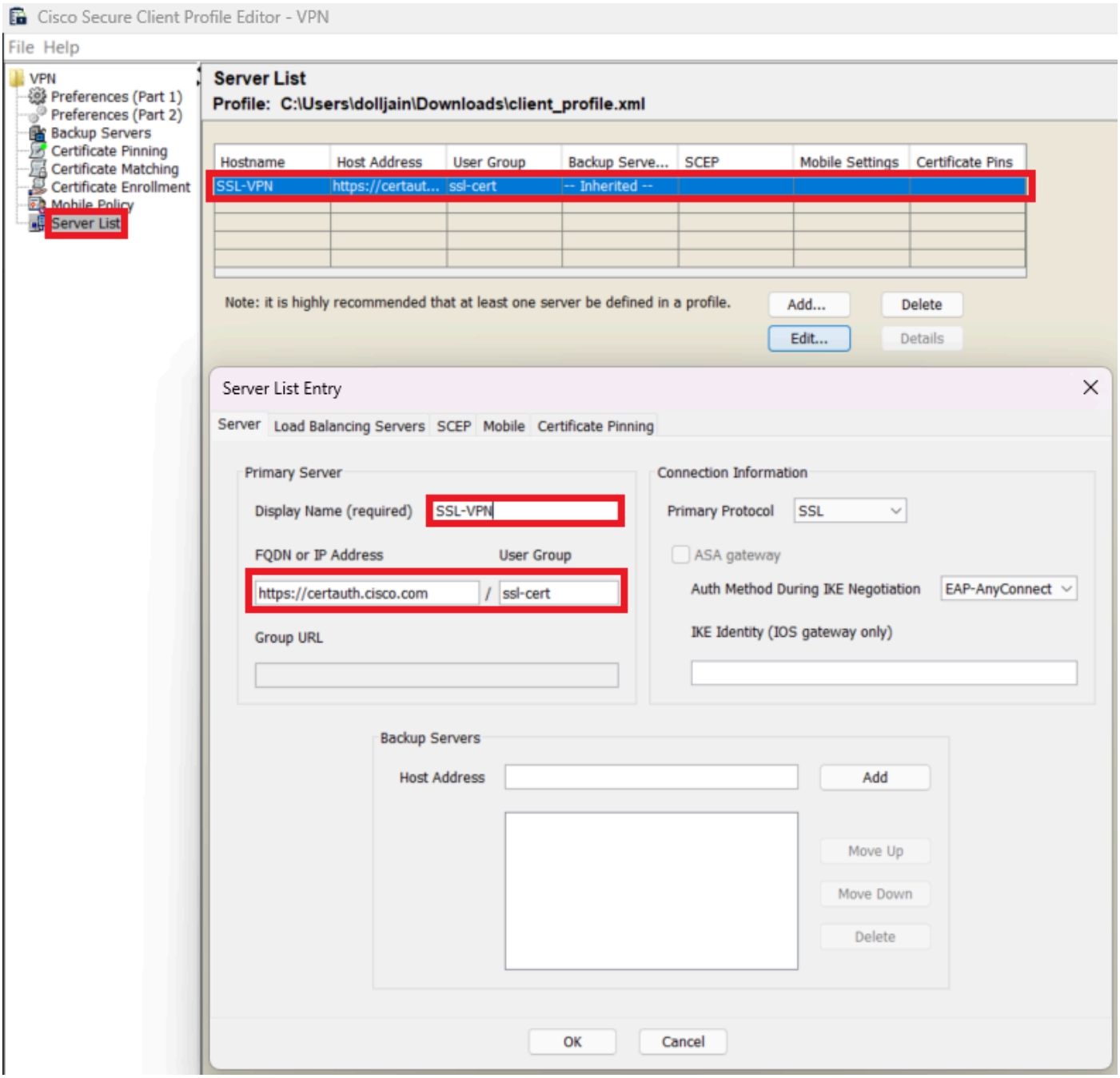
3. (**Optional**) Uncheck the **Disable Automatic Certificate Selection**, as it avoids the prompt to choose the authentication certificate.


Cisco Secure Client Profile Editor - VPN
File Help
VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Pinning
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
Preferences (Part 2)
Profile: C:\Users\dolljain\Downloads\client_profile.xml
Disable Automatic Certificate Selection
User Controllable
Proxy Settings
Native
User Controllable
Public Proxy Server Address:
Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080
Allow Local Proxy Connections
Enable Optimal Gateway Selection
User Controllable
Suspension Time Threshold (hours)
4
Performance Improvement Threshold (%)
20
Automatic VPN Policy
Trusted Network Policy
Disconnect
Untrusted Network Policy
Connect
Bypass connect upon VPN session timeout
Trusted DNS Domains
Trusted DNS Servers
Note: adding all DNS servers in use is recommended with Trusted Network Detection
Trusted Servers @ https://<server>[:<port>]
https://
Add
Delete
Certificate Hash:
Set
Disable interfaces without trusted server connectivity while in truste...
Always On
(More Information)
Allow VPN Disconnect
Allow access to the following hosts with VPN disconn...
Connect Failure Policy
Closed
Allow Captive Portal Remediation
Remediation Timeout (min.)
5
Apply Last VPN Local Resource Rules
Captive Portal Remediation Browser Failover
Allow Manual Host Input
PPP Exclusion
Disable
User Controllable
PPP Exclusion Server IP
User Controllable
Enable Scripting
User Controllable
Terminate Script On Next Event
Enable Post SBL On Connect Script
Retain VPN on Logoff
User Enforcement
Same User Only
Authentication Timeout (seconds)
30

Add Preferences (Part2)

---

4. Create a Server List Entry for setting up a profile in Secure Client VPN by providing group-alias and group-url under the Server List and save the XML profile.



Add Server List

---

5. The XML profile is ready to use.



```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
    <ClientInitialization>
        <UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
        <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
        <ShowPreConnectMessage>false</ShowPreConnectMessage>
        <CertificateStore>All</CertificateStore>
        <CertificateStoreMac>All</CertificateStoreMac>
        <CertificateStoreLinux>All</CertificateStoreLinux>
        <CertificateStoreOverride>true</CertificateStoreOverride>
        <ProxySettings>Native</ProxySettings>
        <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
        <AuthenticationTimeout>30</AuthenticationTimeout>
        <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
        <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
        <LocalLanAccess UserControllable="true">false</LocalLanAccess>
        <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
        <ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
        <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
        <AutoReconnect UserControllable="false">true
            <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
        </AutoReconnect>
        <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
        <AutoUpdate UserControllable="false">true</AutoUpdate>
        <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
        <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
        <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
        <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
        <LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
        <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
        <PPPExclusion UserControllable="false">Disable
            <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
        </PPPExclusion>
        <EnableScripting UserControllable="false">false</EnableScripting>
        <EnableAutomaticServerSelection UserControllable="false">false
            <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
            <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
        </EnableAutomaticServerSelection>
        <RetainVpnOnLogoff>false
        </RetainVpnOnLogoff>
        <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
        <AllowManualHostInput>true</AllowManualHostInput>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>SSL-VPN</HostName>
            <HostAddress>https://certauth.cisco.com</HostAddress>
            <UserGroup>ssl-cert</UserGroup>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

XML Profile

The location of XML profiles for various operating systems:

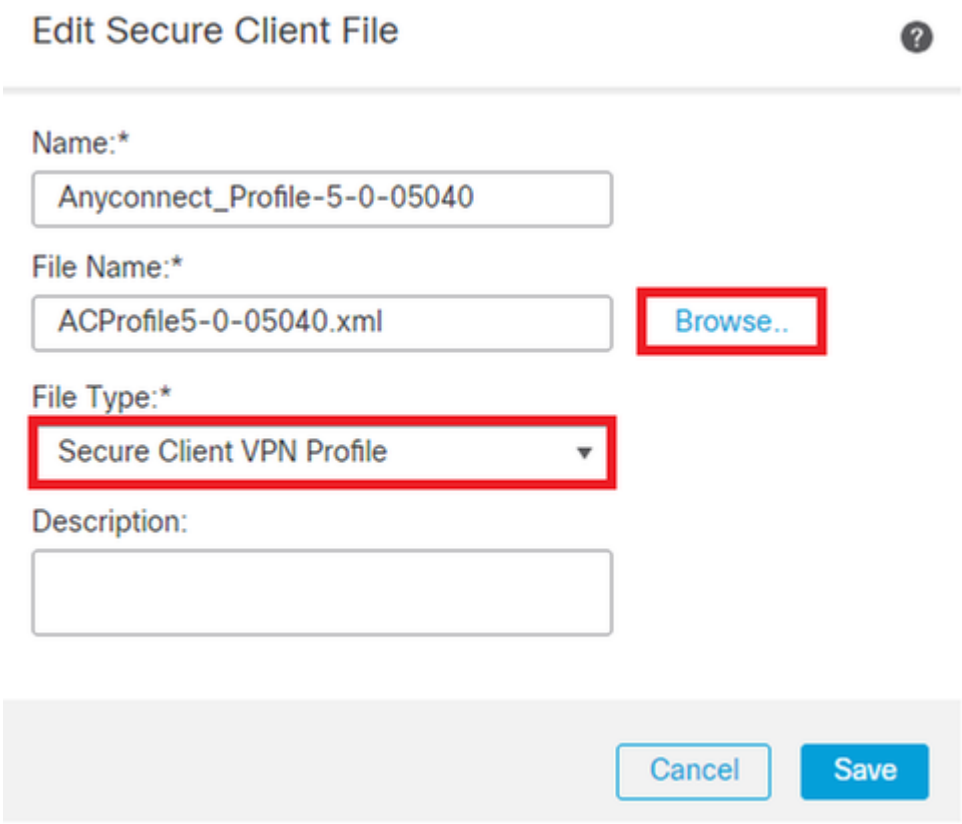
- Linux - /opt/cisco/anyconnect/profile
- MacOS - /opt/cisco/anyconnect/profile
- Windows - C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

---

6. Navigate to **Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile**.

---

7. Enter the name for the file and click **Browse** to choose the XML profile. Click Save.



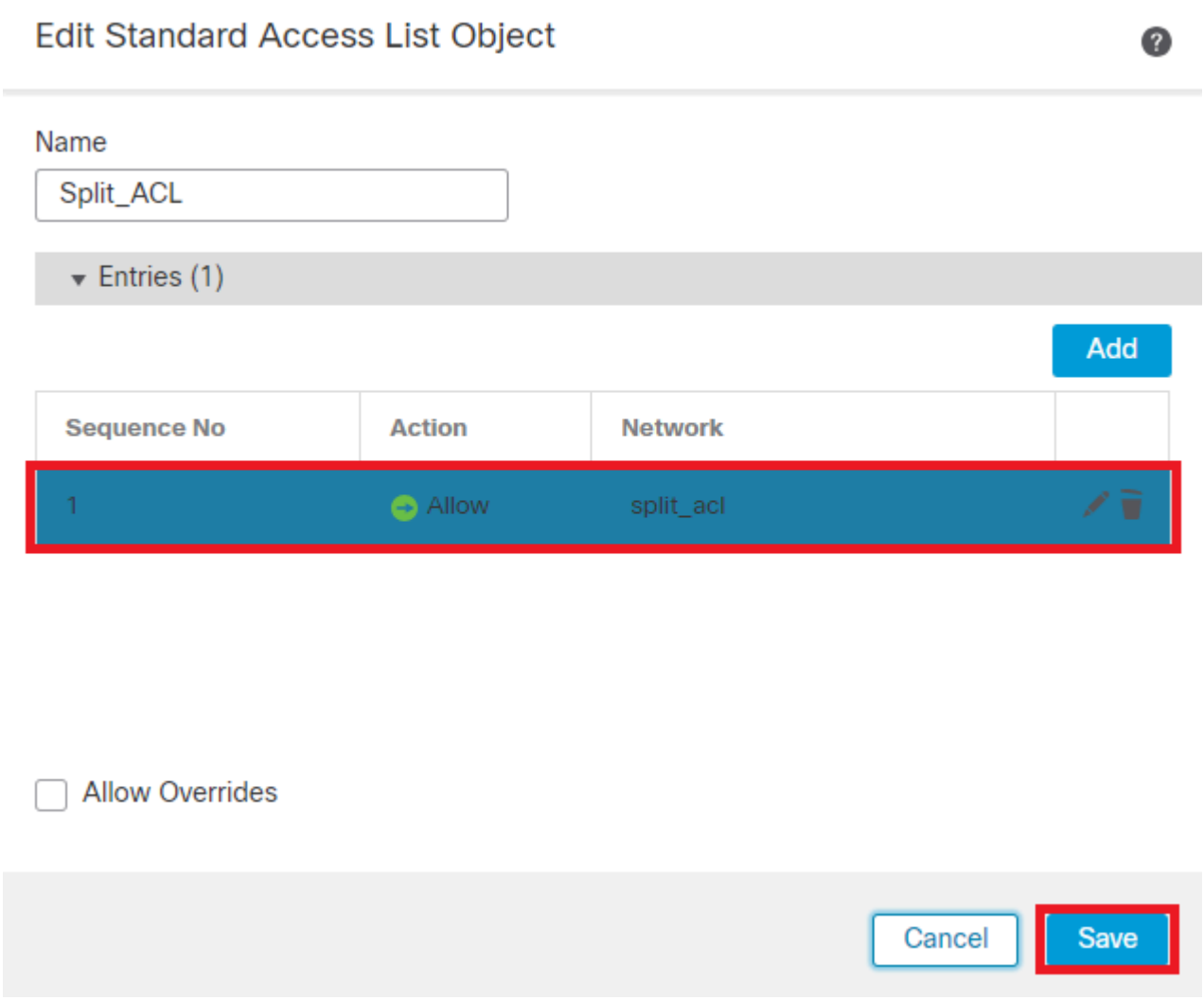
Add Secure Client VPN Profile

Remote Access VPN Configuration

1. Create an ACL to allow access to internal resources.

---

2. Navigate to **Objects > Object Management > Access List > Standard** and click **Add Standard Access List**.



Add Standard ACL

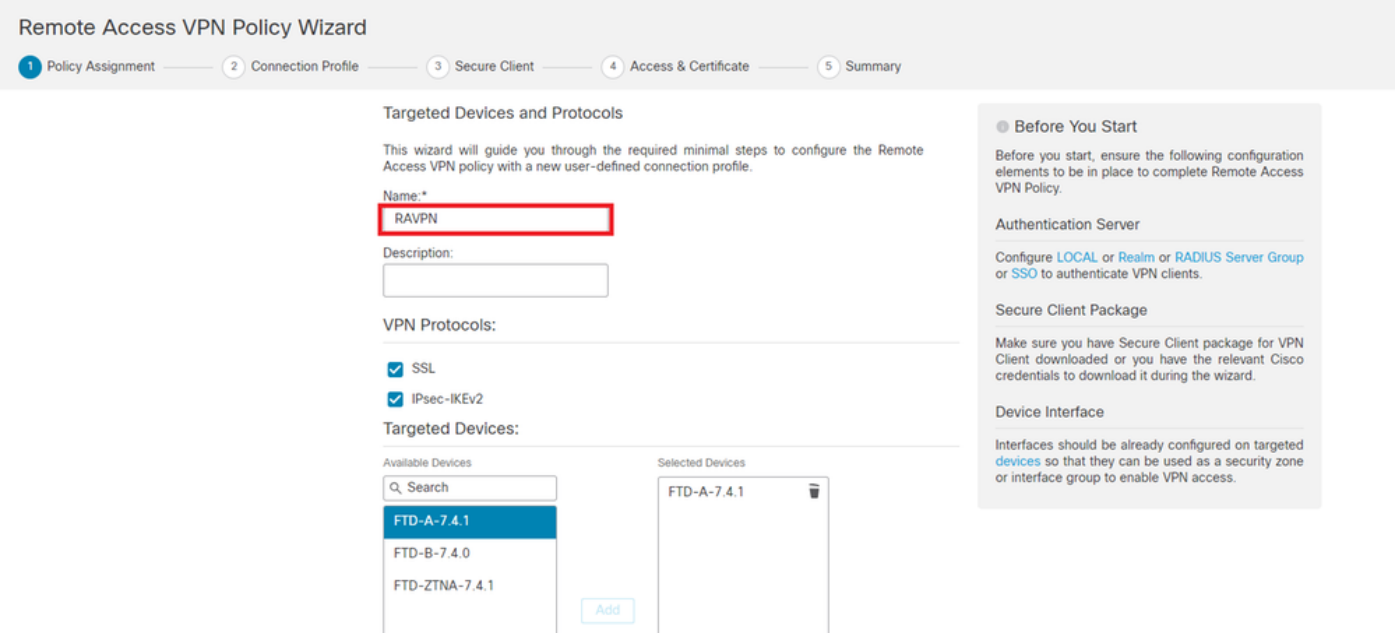
Note: This ACL is used by Secure Client to add secure routes to internal resources.

---

3. Navigate to **Devices > VPN > Remote Access** and click **Add**.

---

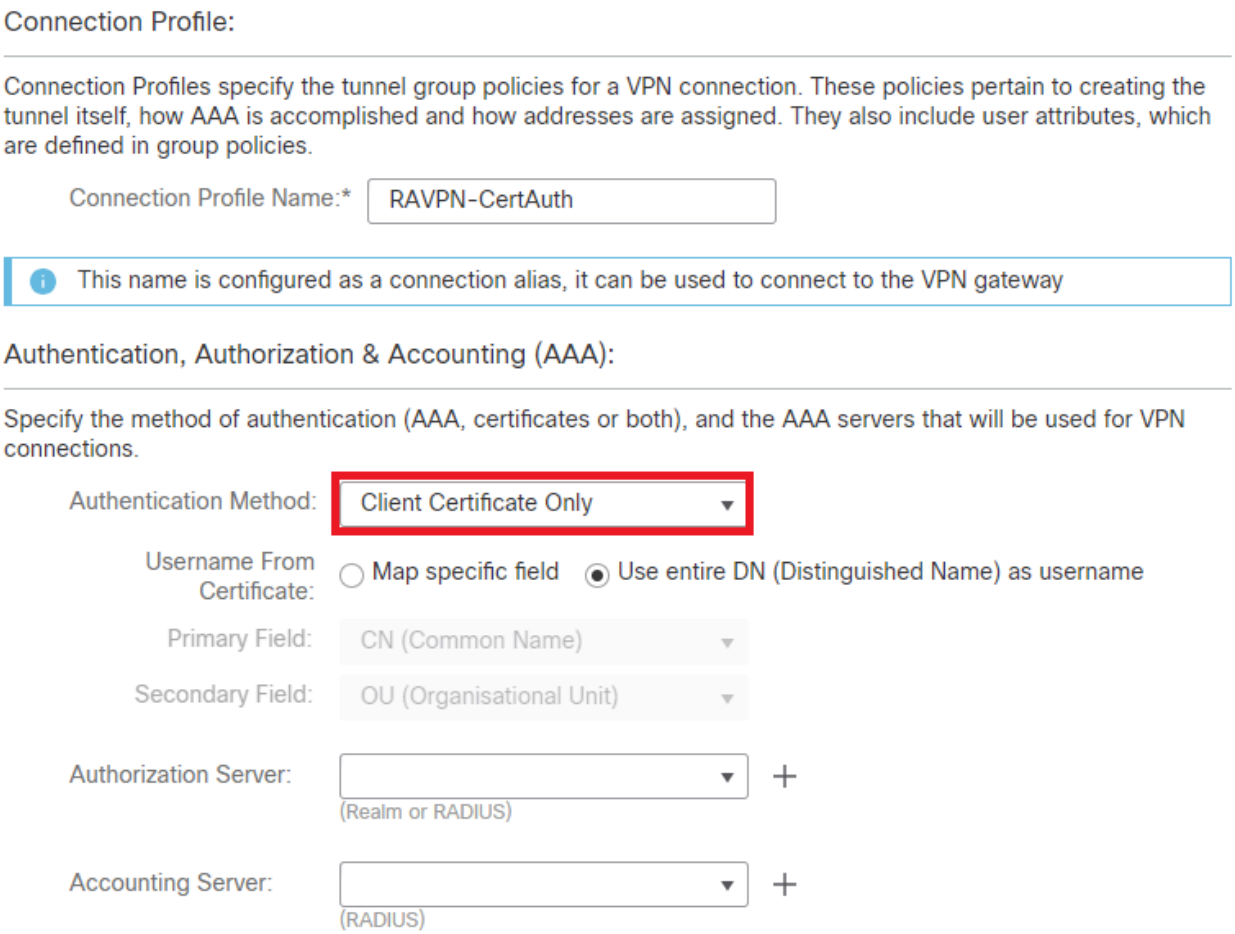
4. Enter the name of the profile, then choose the FTD device and click **Next**.



Add Profile Name

---

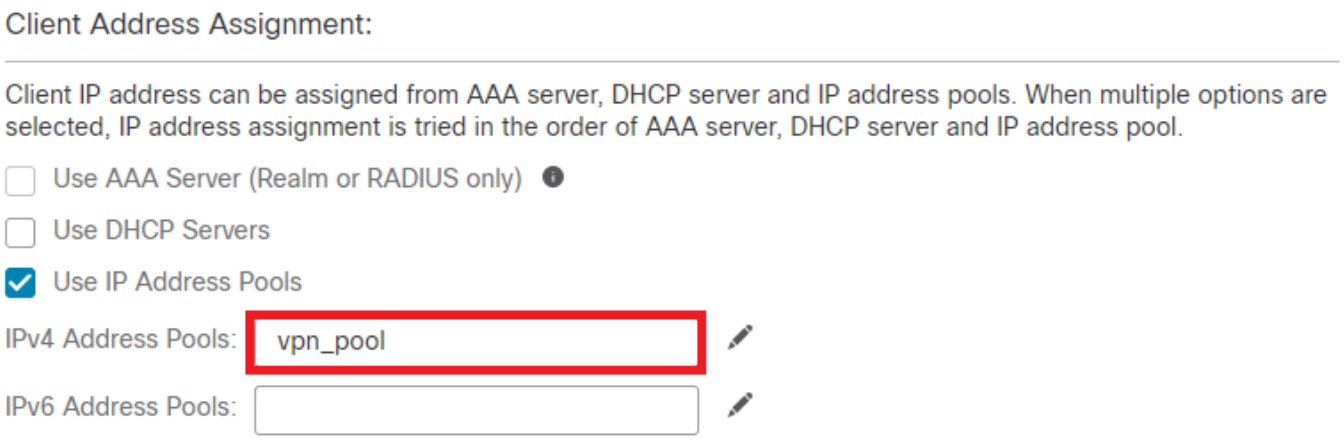
5. Enter the **Connection Profile Name** and choose the Authentication Method as **Client Certificate Only** under Authentication, Authorization, and Accounting (AAA).



Select Authentication Method

---

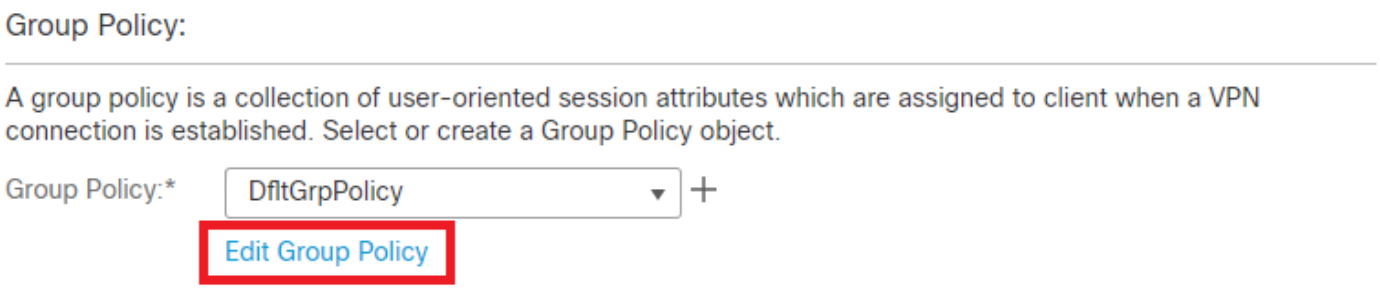
6. Click **Use IP Address Pools** under Client Address Assignment, and choose the IPv4 Address Pool created earlier.



Select Client Address Assignment

---

7. Edit the Group Policy.



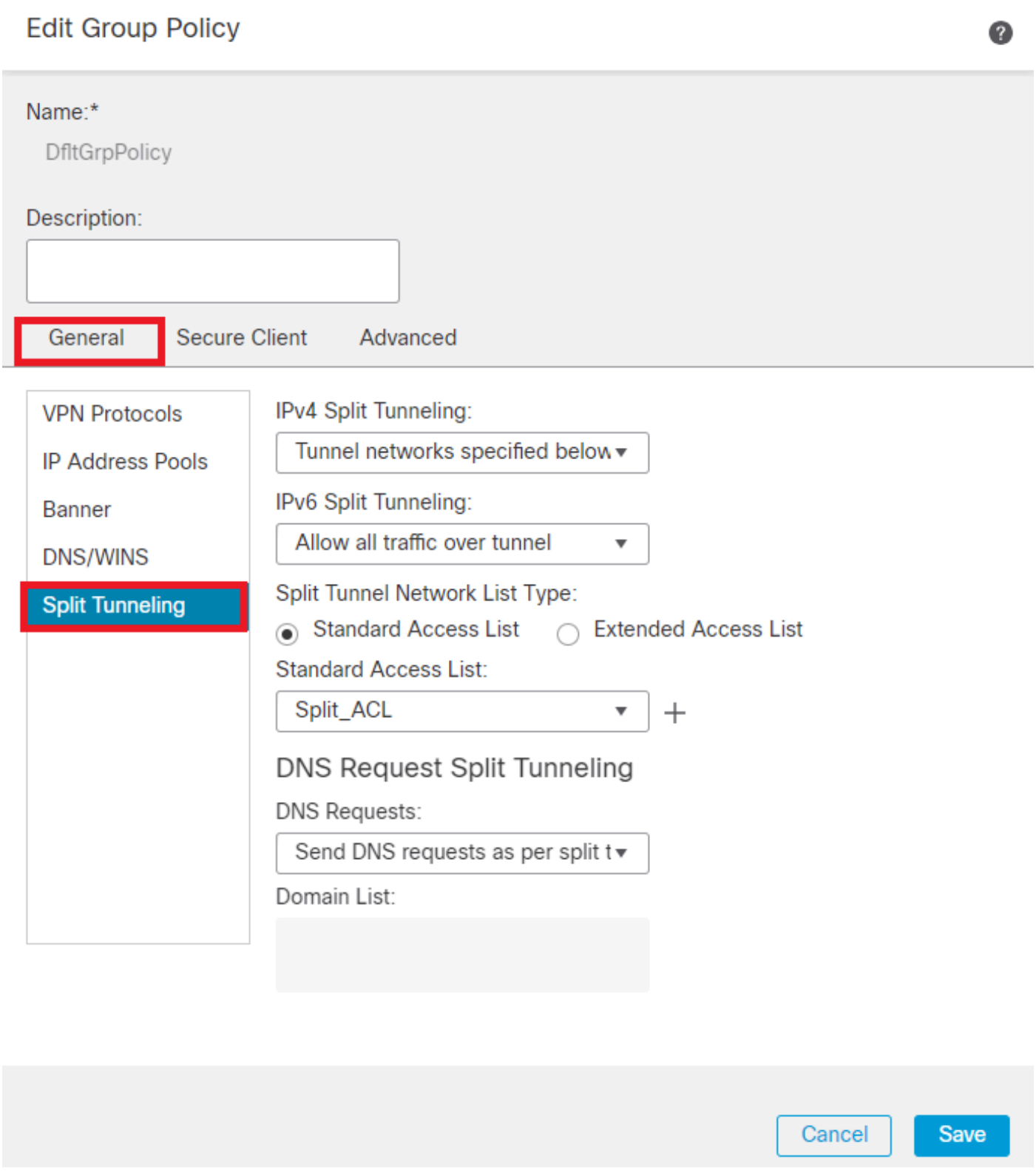
Edit Group Policy

---

8. Navigate to **General > Split Tunneling**, choose **Tunnel networks specified below** and then **Standard Access List** under **Split Tunnel Network List Type**.

---

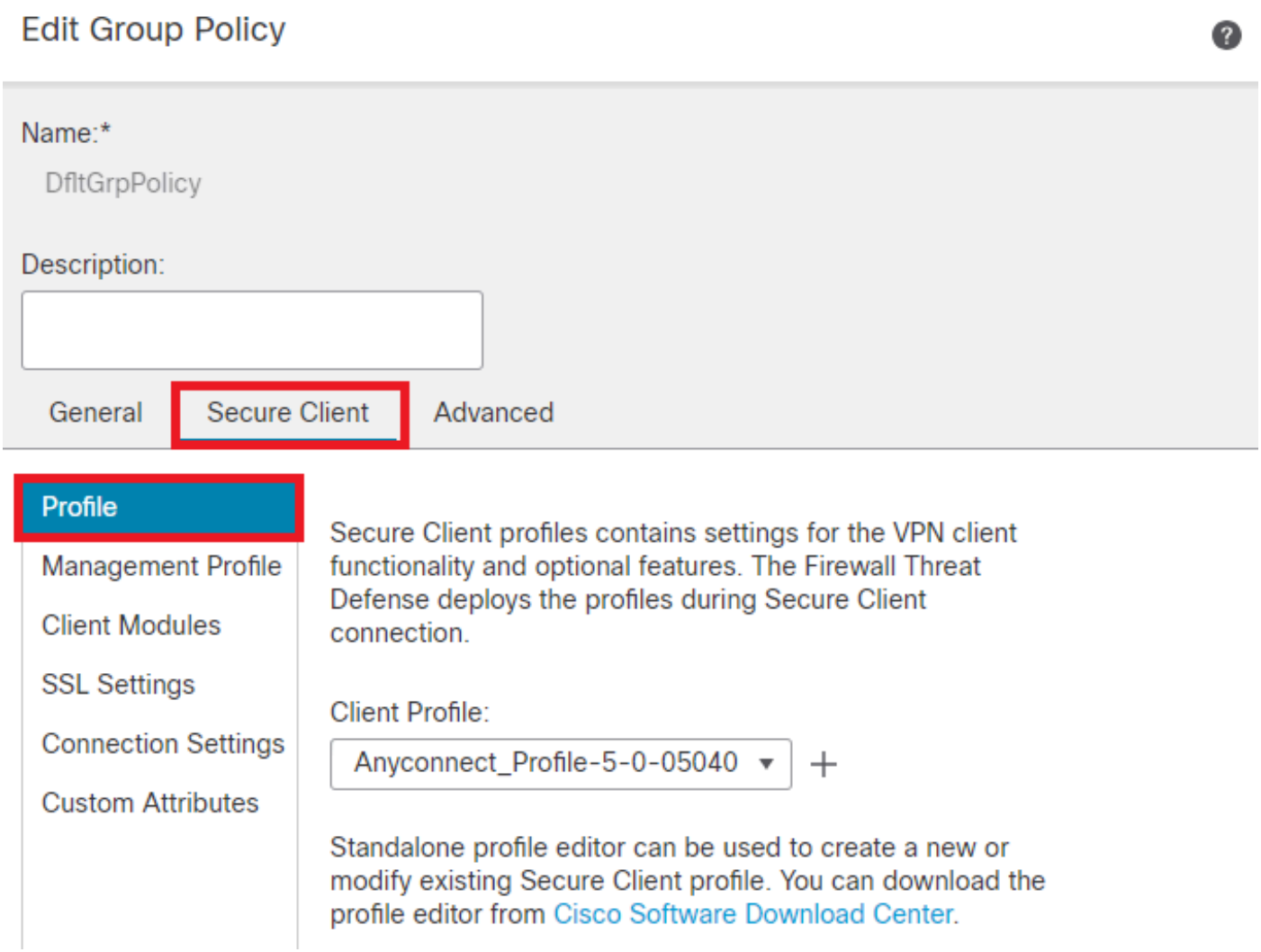
9. Choose the ACL created earlier.



Add Split Tunneling

---

10. Navigate to **Secure Client > Profile**, choose the **Client Profile** and click **Save**.



Add Secure Client Profile

---

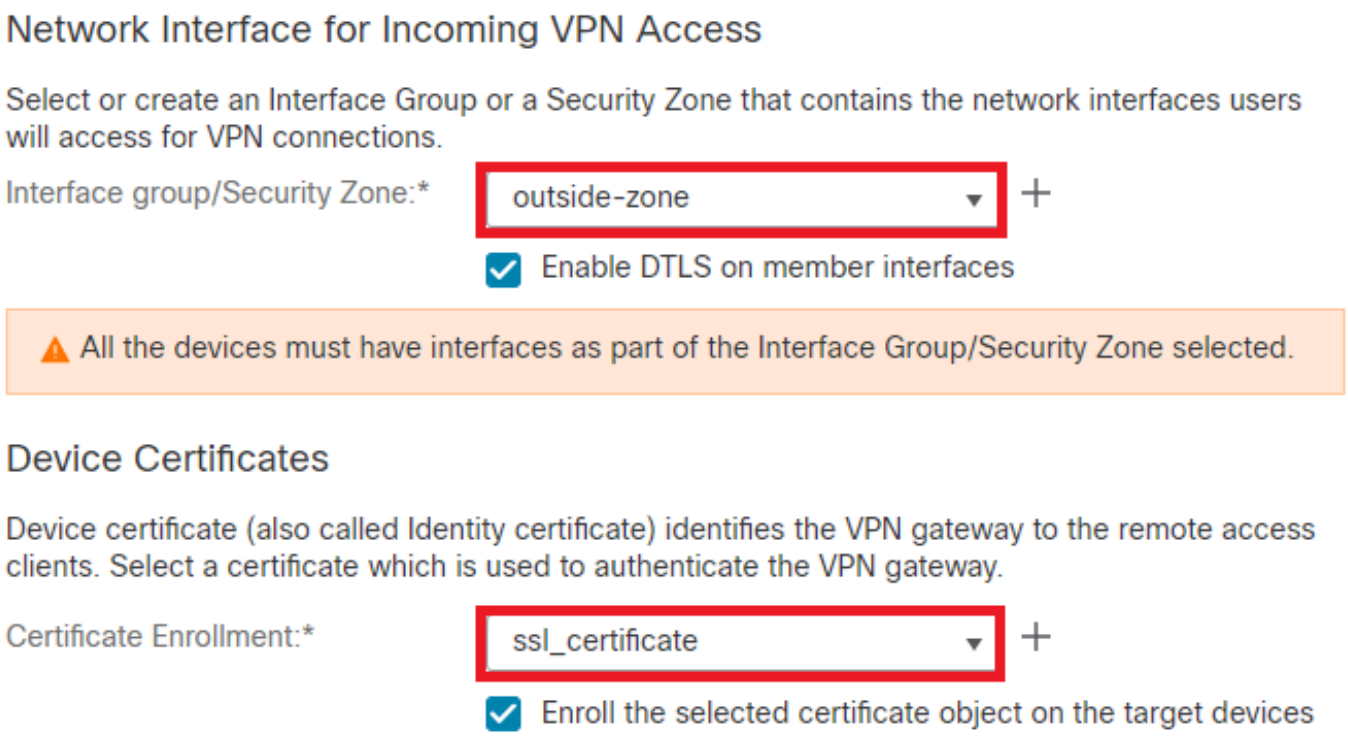
11. Click Next, then select **Secure Client Image** and click Next.



Add Secure Client Image

---

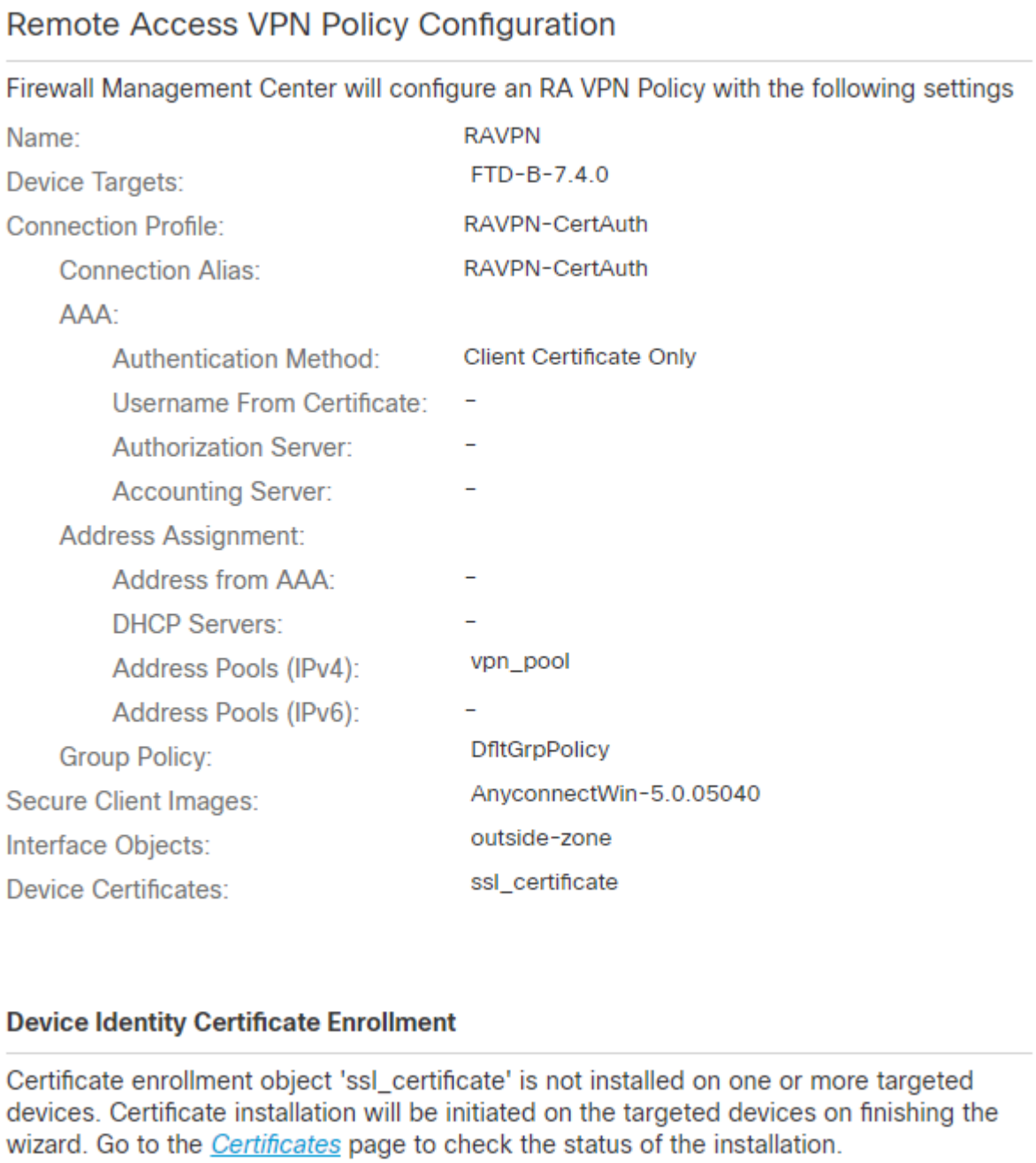
12. Choose the Network Interface for VPN Access, choose the Device Certificates and check sysopt permit-vpn and click Next.



Add Access Control for VPN Traffic

---

13. Review all the configurations and click **Finish**.



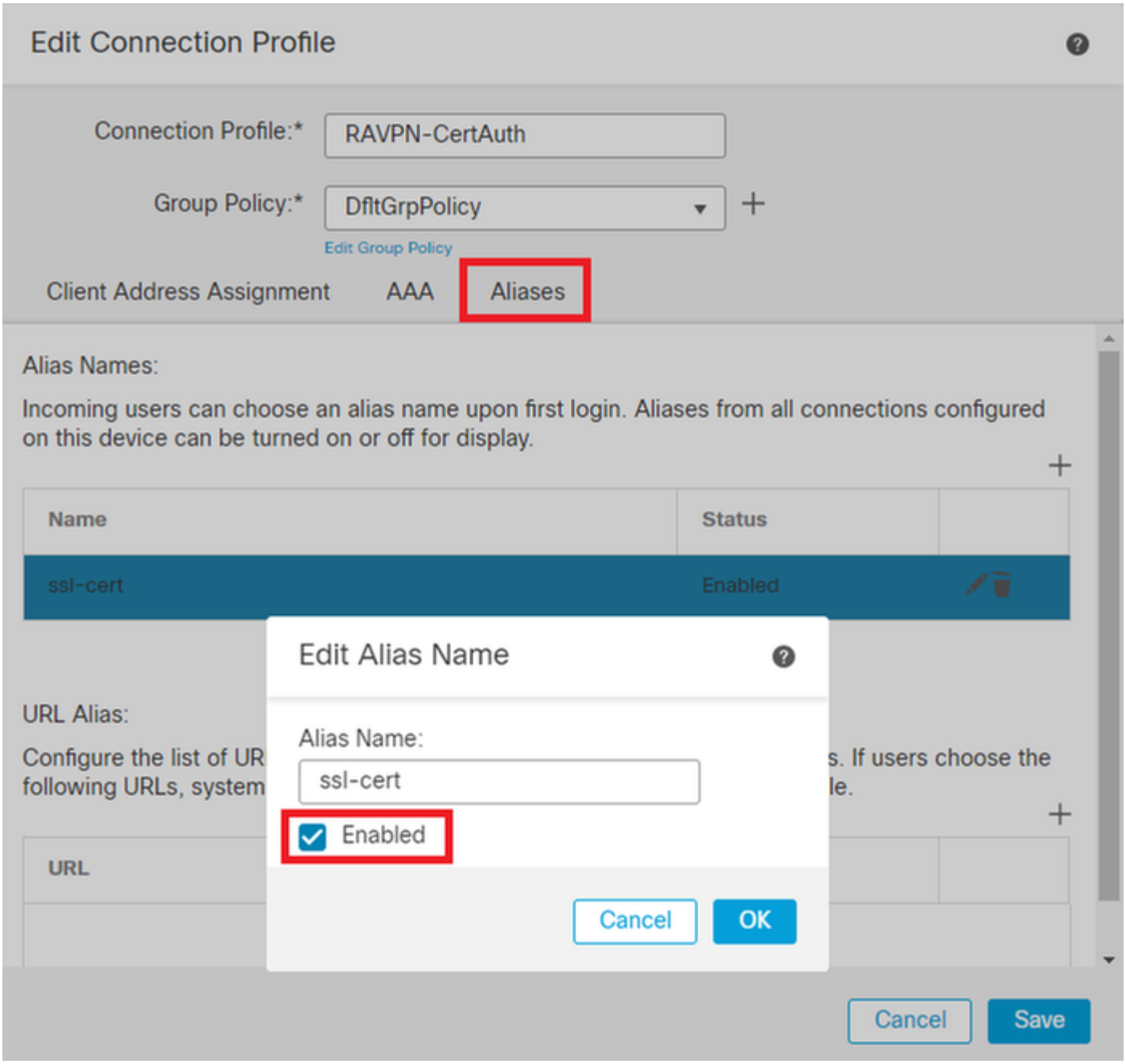
Remote Access VPN Policy Configuration

---

14. Once the initial setup of Remote Access VPN is complete, edit the Connection Profile created and navigate to **Aliases**.

---

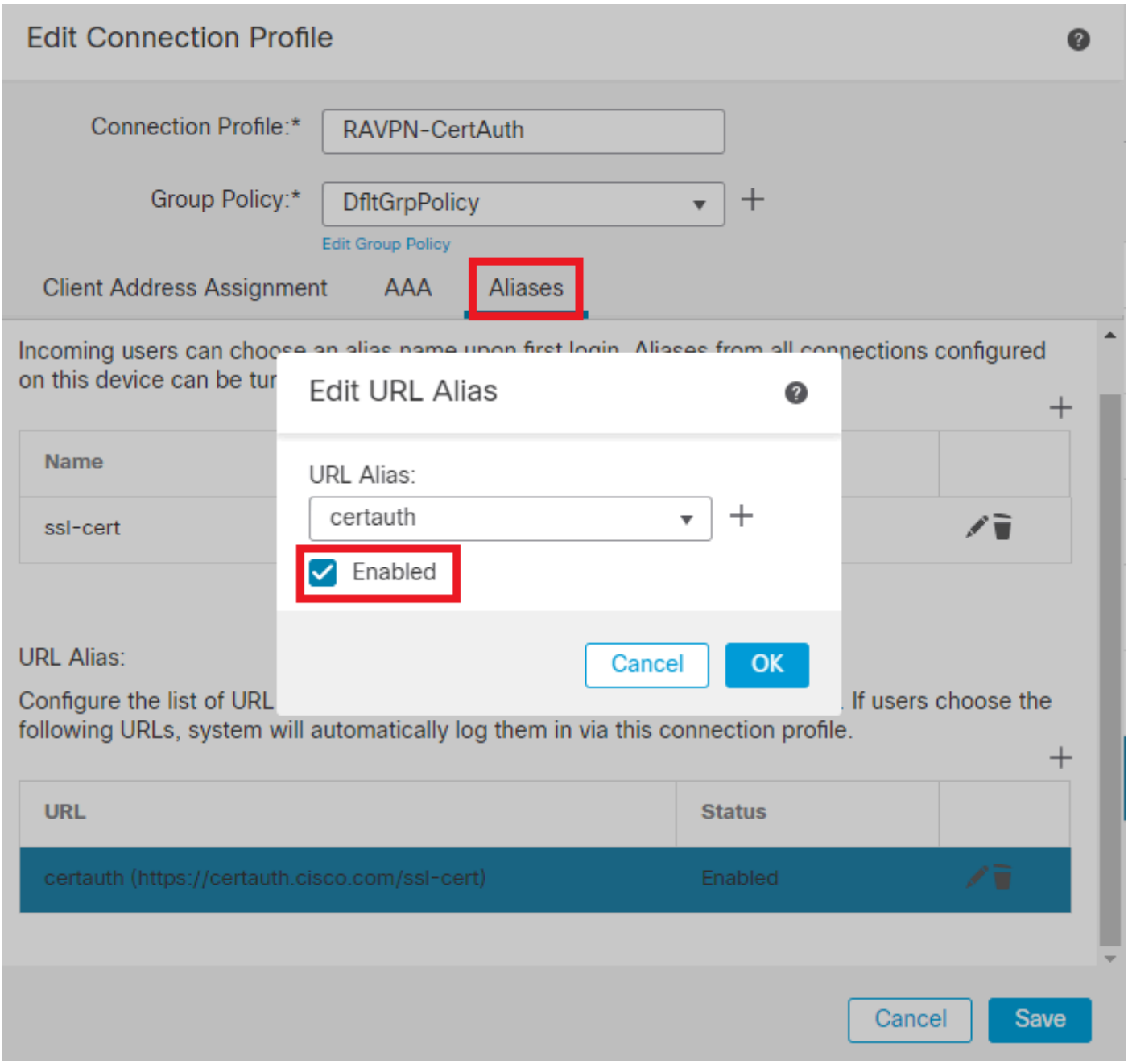
15. Configure **group-alias** by clicking the plus icon (+).



Edit Group Alias

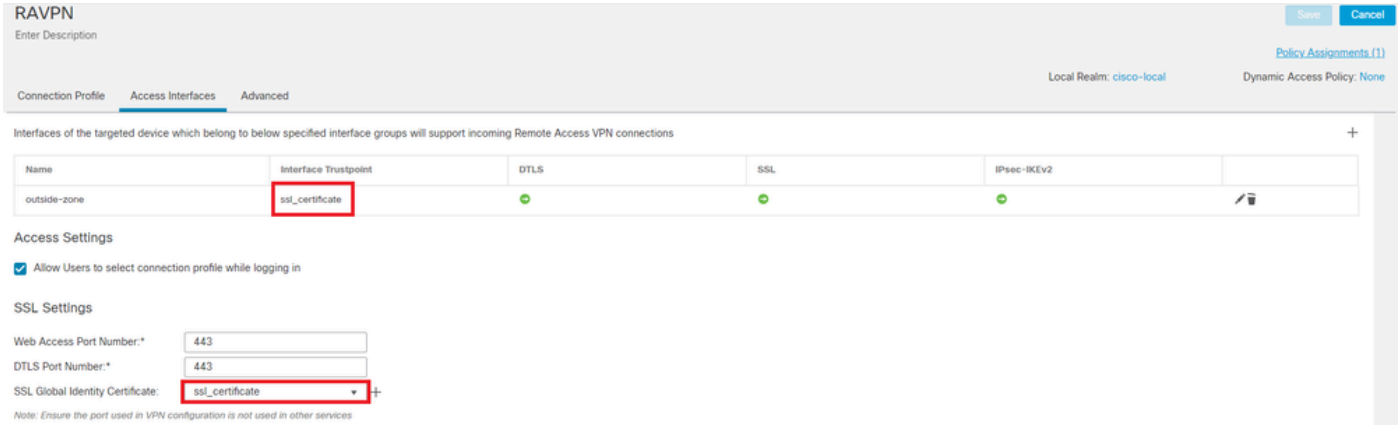
---

16. Configure the group-url by clicking the plus icon (+). Use the same Group URL configured earlier in the Client Profile.



Edit Group URL

Step 17. Navigate to Access Interfaces. Choose the **Interface Trustpoint** and the **SSL Global Identity Certificate** under the SSL settings.



Edit Access Interfaces

---

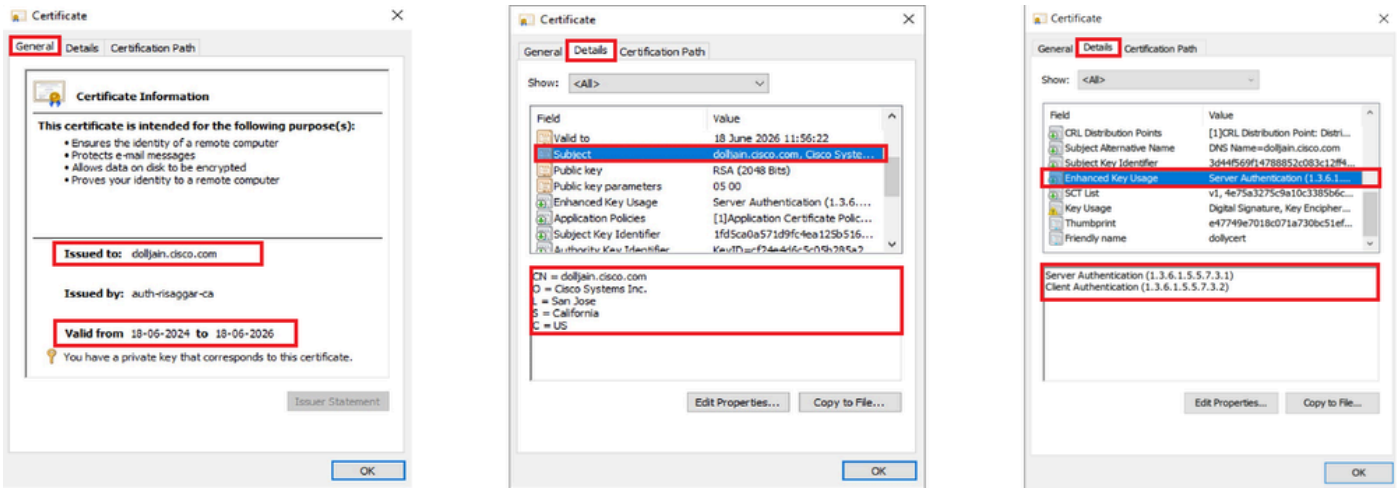
18. Click **Save** and deploy the changes.

Verify

Use this section to confirm your configuration works properly.

---

1. The secure client PC must have the certificate installed with a valid date, subject, and Enhanced Key Usage (EKU) on the PC of the user. This certificate must be issued by the CA whose certificate is installed on FTD as shown previously. In the next example, the identity or user certificate is issued by **auth-risaggar-ca**.

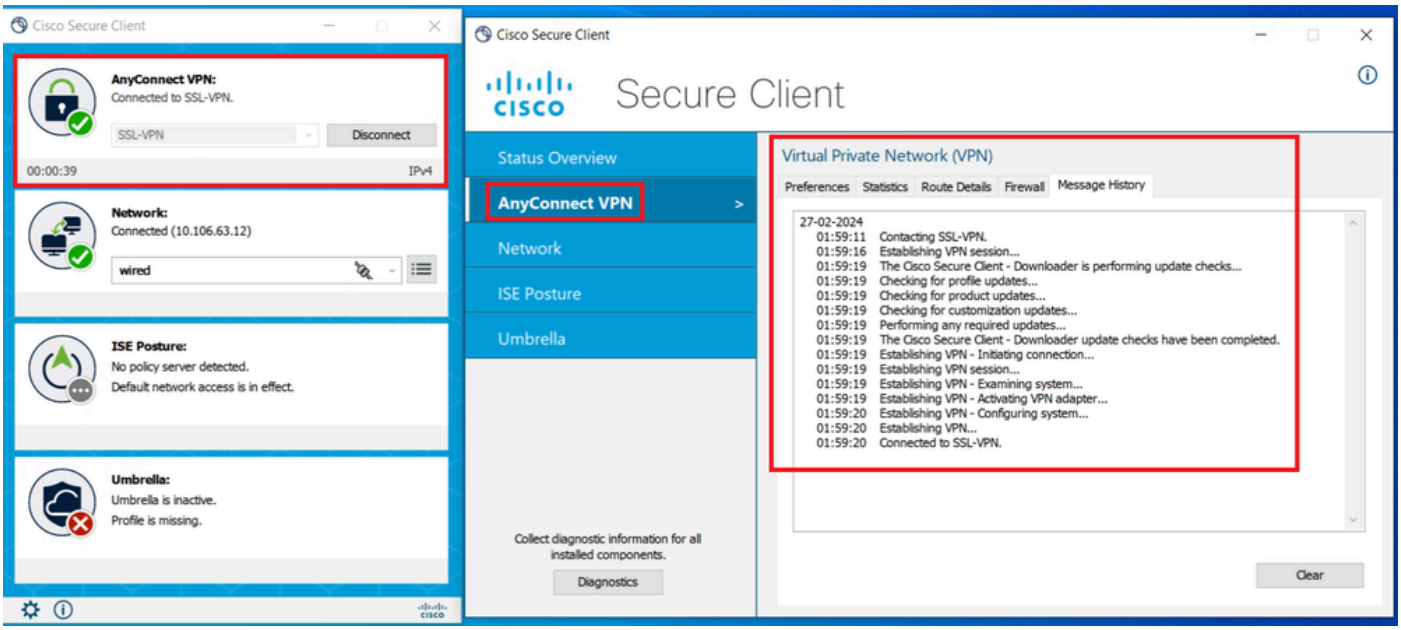


Certificate Highlights



Note: The client certificate must have the Client Authentication EKU.

2. Secure Client must establish the connection.



Successful Secure Client Connection

3. Run the **show vpn-sessiondb anyconnect** command to confirm the connection details of the active user under the used tunnel group.

```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dolljain.cisco.com     Index        : 8
Assigned IP  : 10.20.20.1             Public IP    : 72.163.X.X
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256
Bytes Tx     : 14402                  Bytes Rx     : 9652
Group Policy : DfltGrpPolicy          Tunnel Group : RAVPN-CertAuth
Login Time   : 08:32:22 UTC Mon Mar 18 2024
Duration     : 0h:03m:59s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0ac5de050000800065f7fc16
Security Grp : none                   Tunnel Zone  : 0
```

Troubleshoot

This section provides information to troubleshoot your configuration.

---

1. Debugs can be run from the diagnostic CLI of the FTD:

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

---

2. Refer to the Troubleshoot Cisco Secure Client VPN Common Problems guide for additional assistance.