Configure Secure Client Certificate Authentication on FTD Managed by FMC

Contents

Introduction

This document describes the process of configuring remote access VPN on Firepower Threat Defense (FTD) managed by Firepower Management Center (FMC) with certificate authentication.

Contributed by Dolly Jain and Rishabh Aggarwal, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Manual certificate enrollment and basics of SSL
- FMC
- Basic Authentication knowledge for Remote Access VPN
- Third-party Certificate Authority (CA) like Entrust, Geotrust, GoDaddy, Thawte, and VeriSign.

Components Used

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

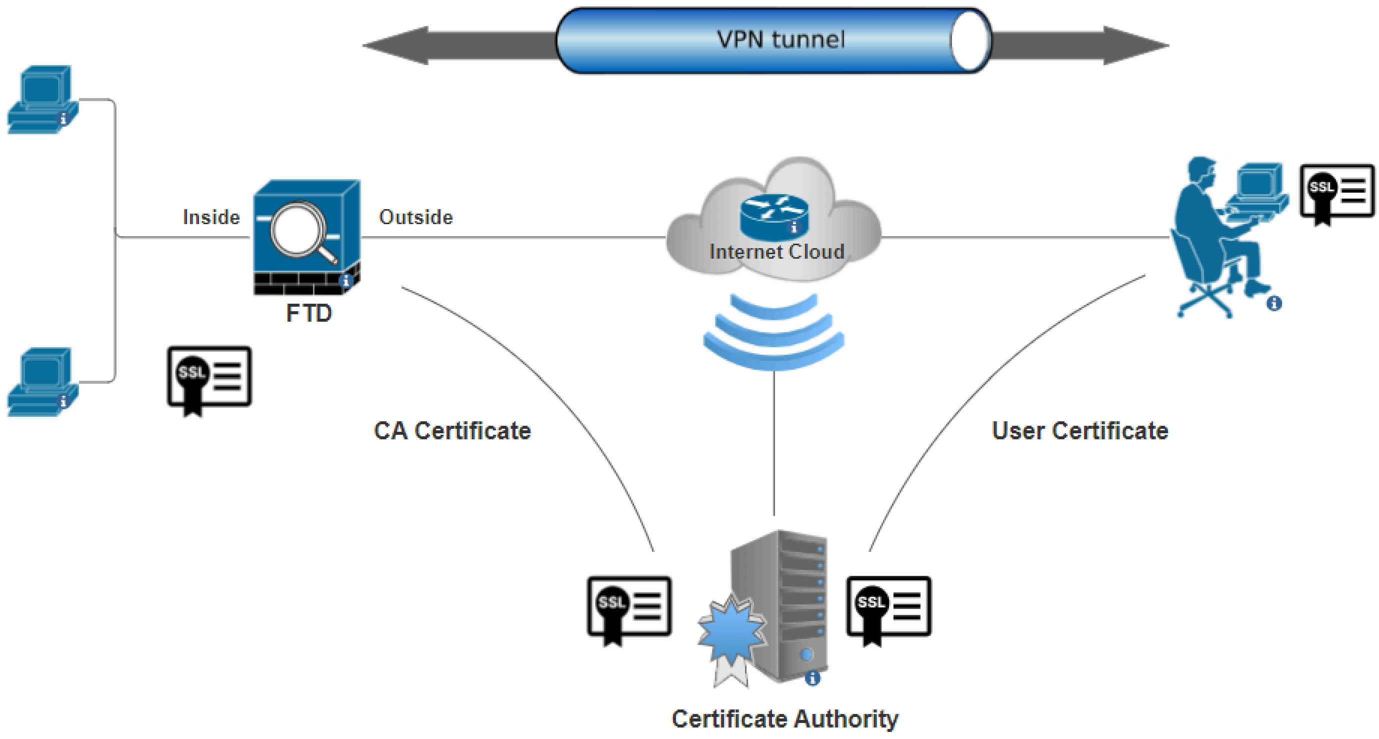
- Secure Firepower Threat Defense version 7.4.1

- Firepower Management Center (FMC) version 7.4.1
- Secure Client version 5.0.05040
- Hydrant / IdentTrust 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

To configure Remote Access VPN with Certificate Authentication in FMC, you need to:

- Create a certificate used for server authentication.

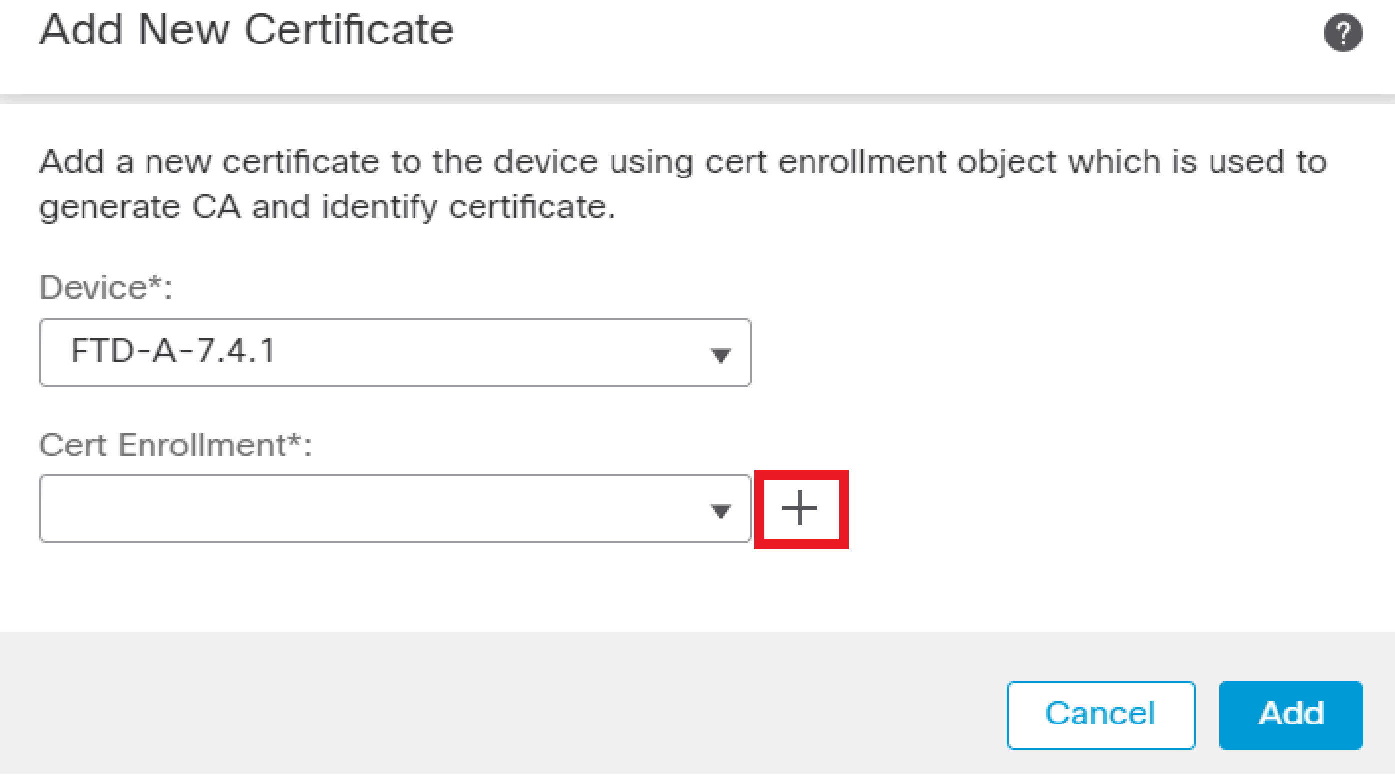
- Add a Trusted or Internal CA certificate on FTD via FMC for authenticating the user certificate.
- Create a pool of addresses for VPN users.
- Upload Secure Client images for different platforms.

- Create and upload XML Profile.

1. Import a Certificate Used for Server Authentication

Note: On FMC, CA certificate is needed before you can generate the CSR. If CSR is generated from an external source (openssl or 3rd party), the manual method fails and PKCS12 certificate format must be used.

Step 1. Navigate to Devices > Certificatesand click Add Cert Enrollment. Select Device and click on plus sign (+) under Cert Enrollment.



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

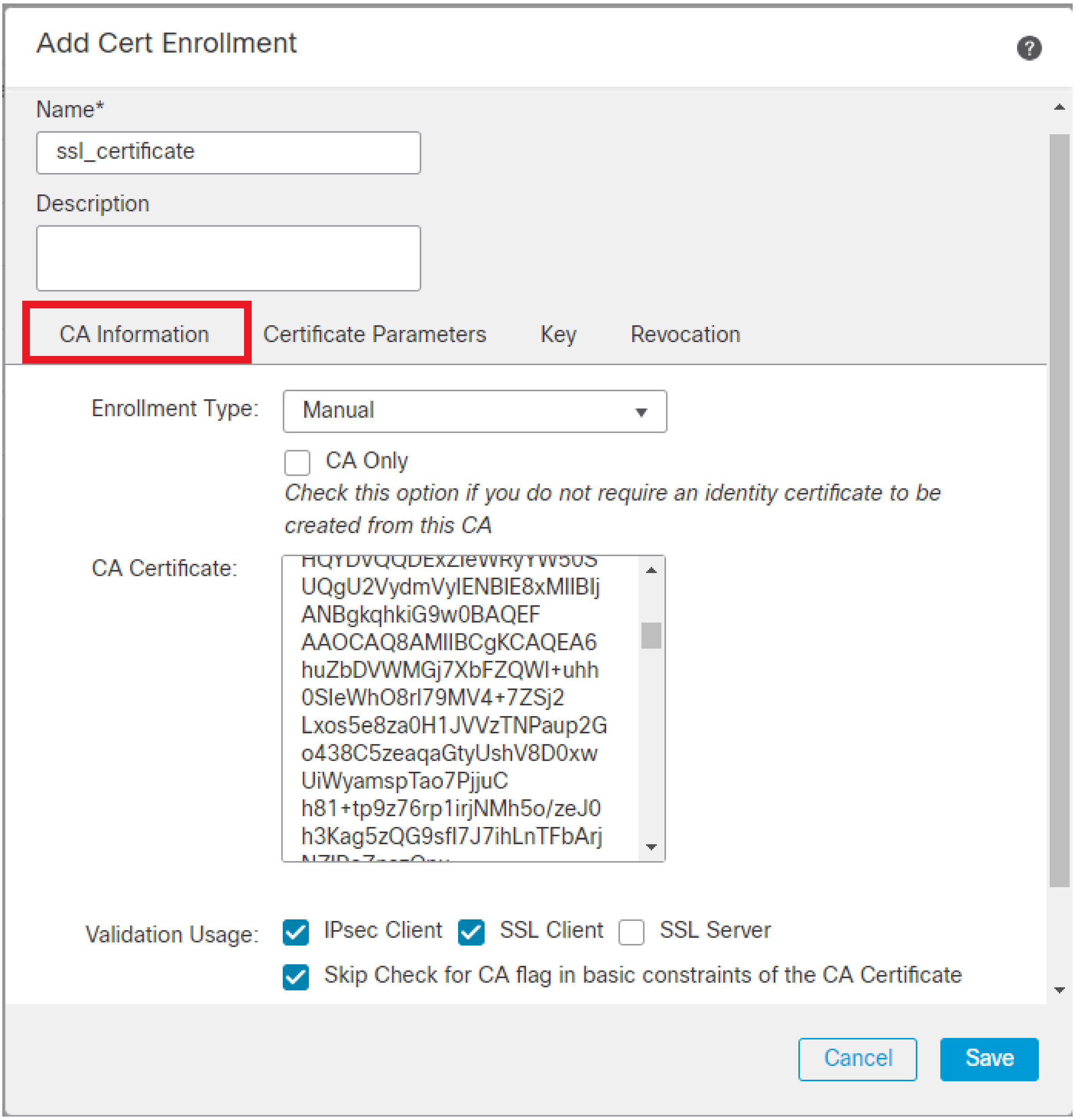
Device*:

FTD-A-7.4.1

Cert Enrollment*:

Add Cert Enrollment

Step 2. Under the CA Information, select the Enrollment Type as Manual and paste the Certificate Authority (CA) certificate that is used to sign the CSR.



Add Cert Enrollment

Name*

ssl_certificate

Description

Enrollment Type: Manual

□ CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
HQYDVQQDExZieWRyYW50S
UQgU2VydmVyIENBIE8xMIIBIj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWMGj7XbFZQWl+uhh
0SleWhO8rl79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
```

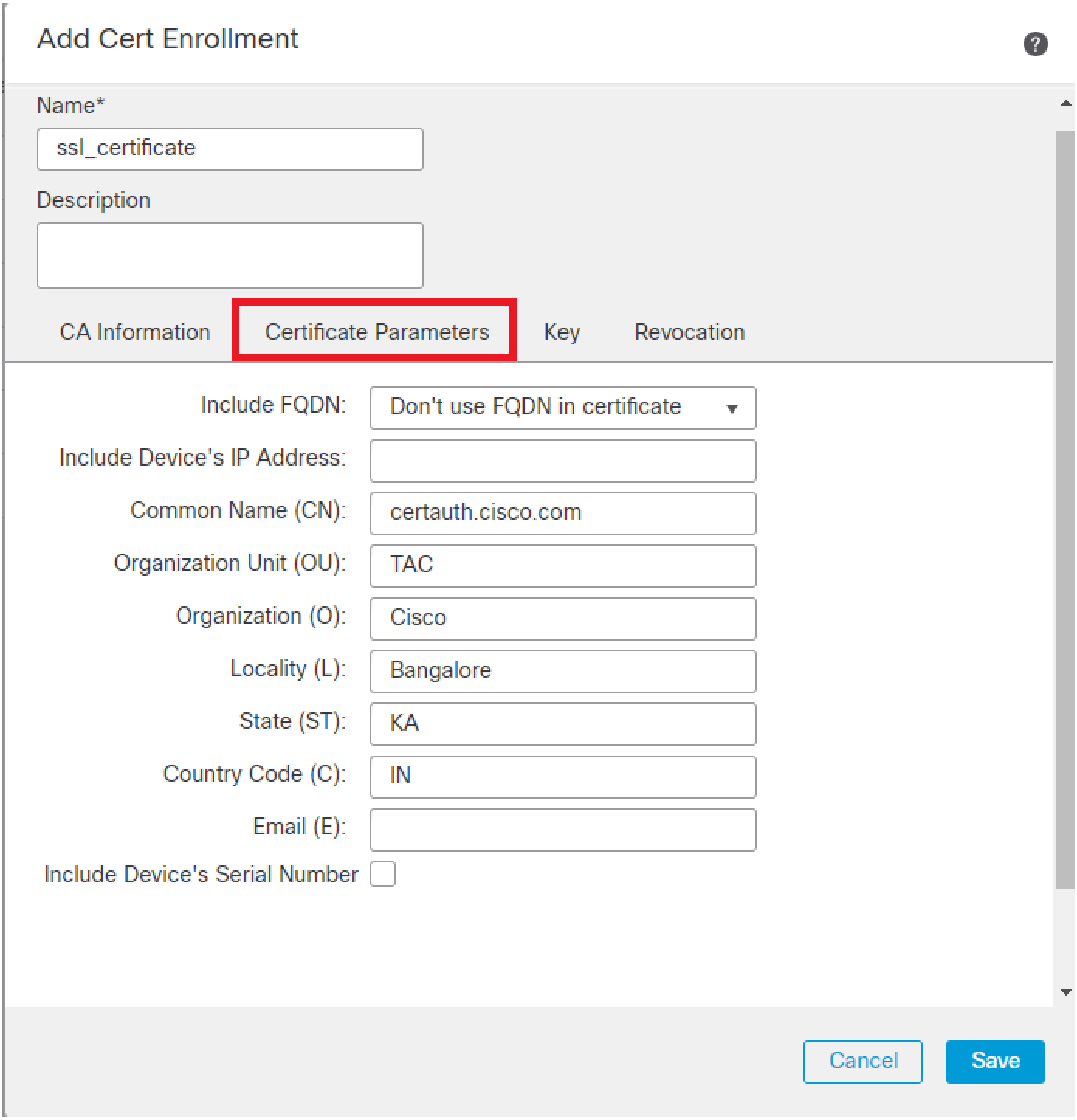
Validation Usage: ☑ IPsec Client ☑ SSL Client □ SSL Server

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

Add CA Information

Step 3. For Validation Usage, select IPsec Client, SSL Client and Skip Check for CA flag in basic constraints of the CA Certificate.

Step 4. Under Certificate Parameters, fill in the subject name details.



Add Cert Enrollment

Name*: ssl_certificate

Description:

Include FQDN: Don't use FQDN in certificate

Include Device's IP Address:

Common Name (CN): certauth.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): Bangalore

State (ST): KA

Country Code (C): IN

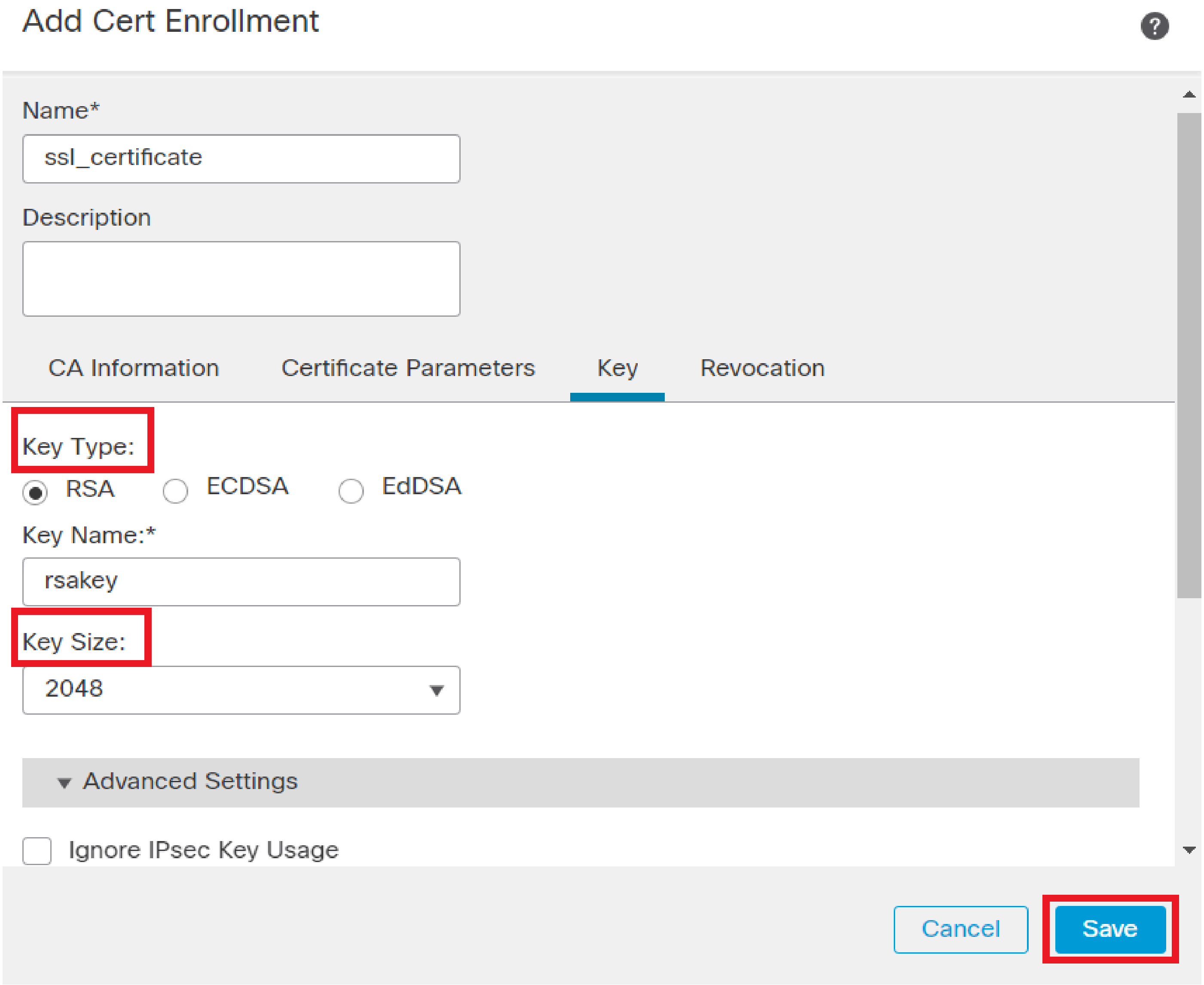
Email (E):

Include Device's Serial Number □

Add Certificate Parameters

Step 5. Under Keyselect the key type as RSA with a key name and size. Click on Save.

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



Add Cert Enrollment

Name*

ssl_certificate

Description

Key Type:

● RSA ○ ECDSA ○ EdDSA

Key Name:*

rsakey

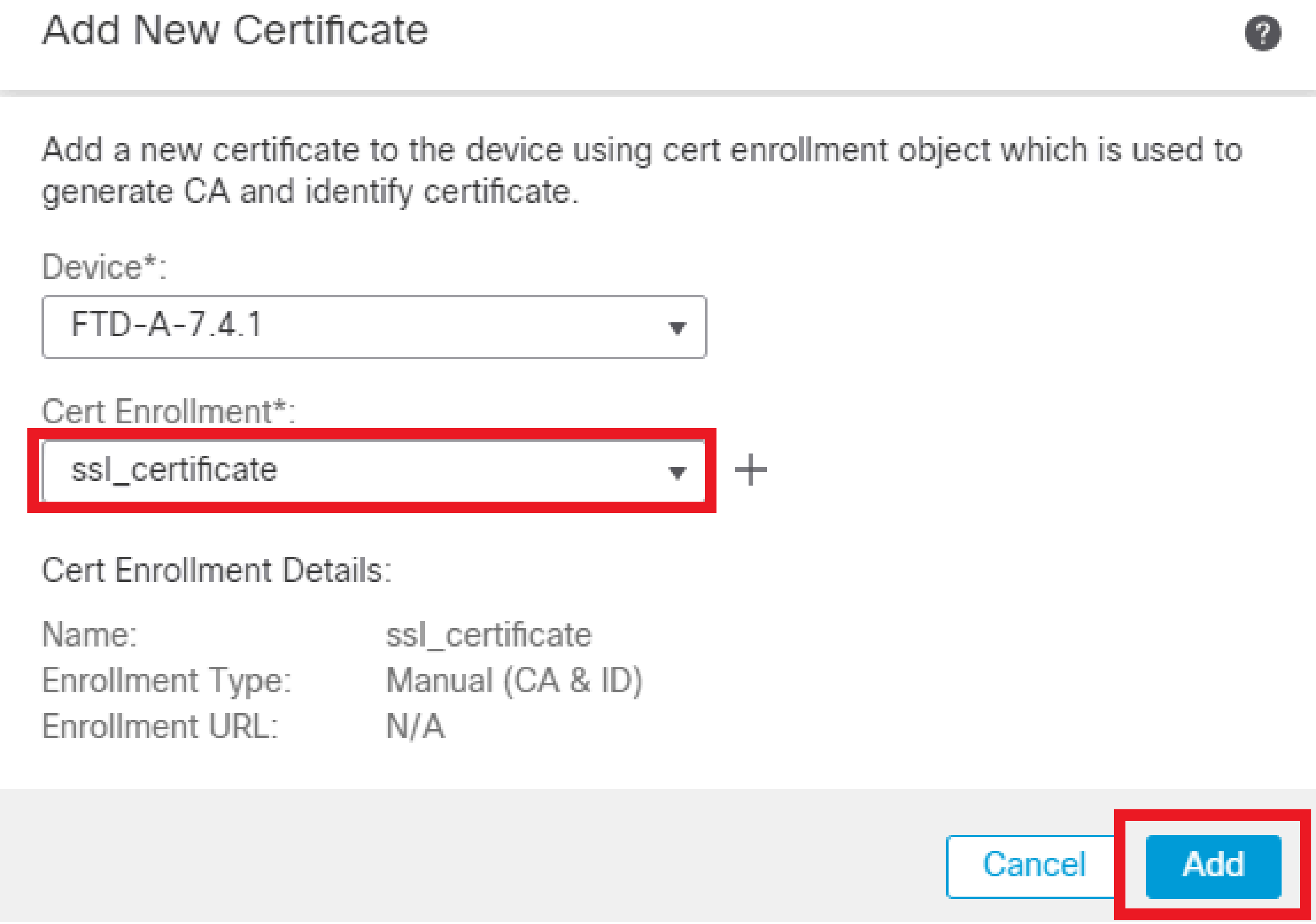
Key Size:

2048

□ Ignore IPsec Key Usage

Add RSA key

Step 6. Under Cert Enrollment, select the trust point from the dropdown which was just created and click Add.



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD-A-7.4.1

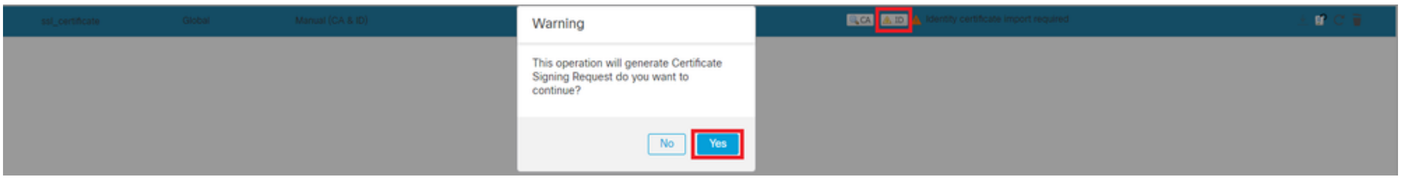
Cert Enrollment*: ssl_certificate

Cert Enrollment Details:

Name: ssl_certificate
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Add new Certificate

Step 7. Click on ID, then click on Yes on further prompt to generate the CSR.



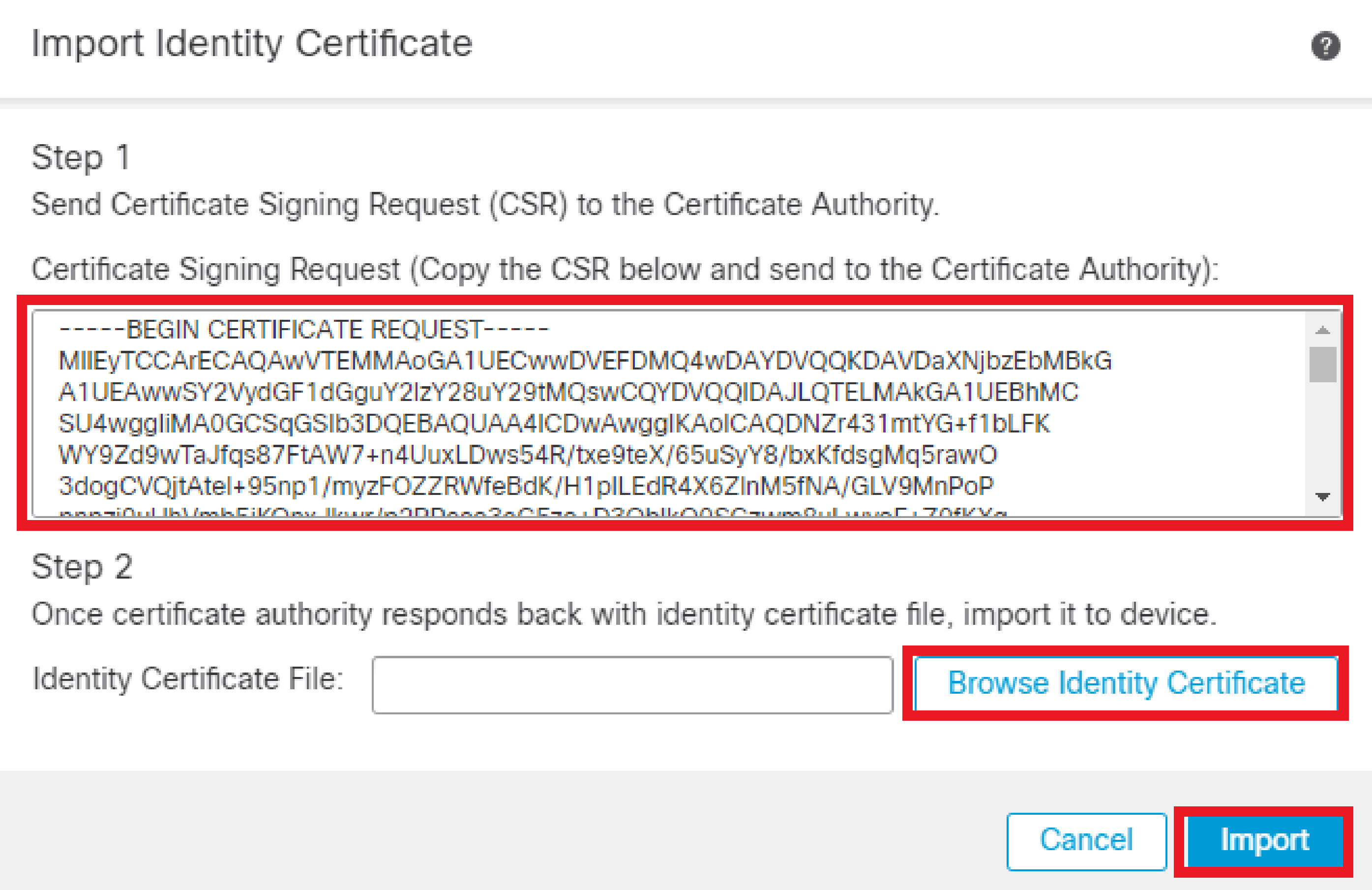
ssl_certificate Global Manual (CA & ID) CA ID Identity certificate import required

Warning

This operation will generate Certificate Signing Request do you want to continue?

Generate CSR

Step 8. Copy the CSR and get it signed by the Certificate authority. Once, the Identity certificate is issued by CA, import it by clicking on Browse Identity Certificate and click Import .



Import Identity Certificate

Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMAkGA1UEBhMC
SU4wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1plLEdR4X6ZlnM5fNA/GLV9MnPoP
```

Step 2

Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:

Import ID Certificate

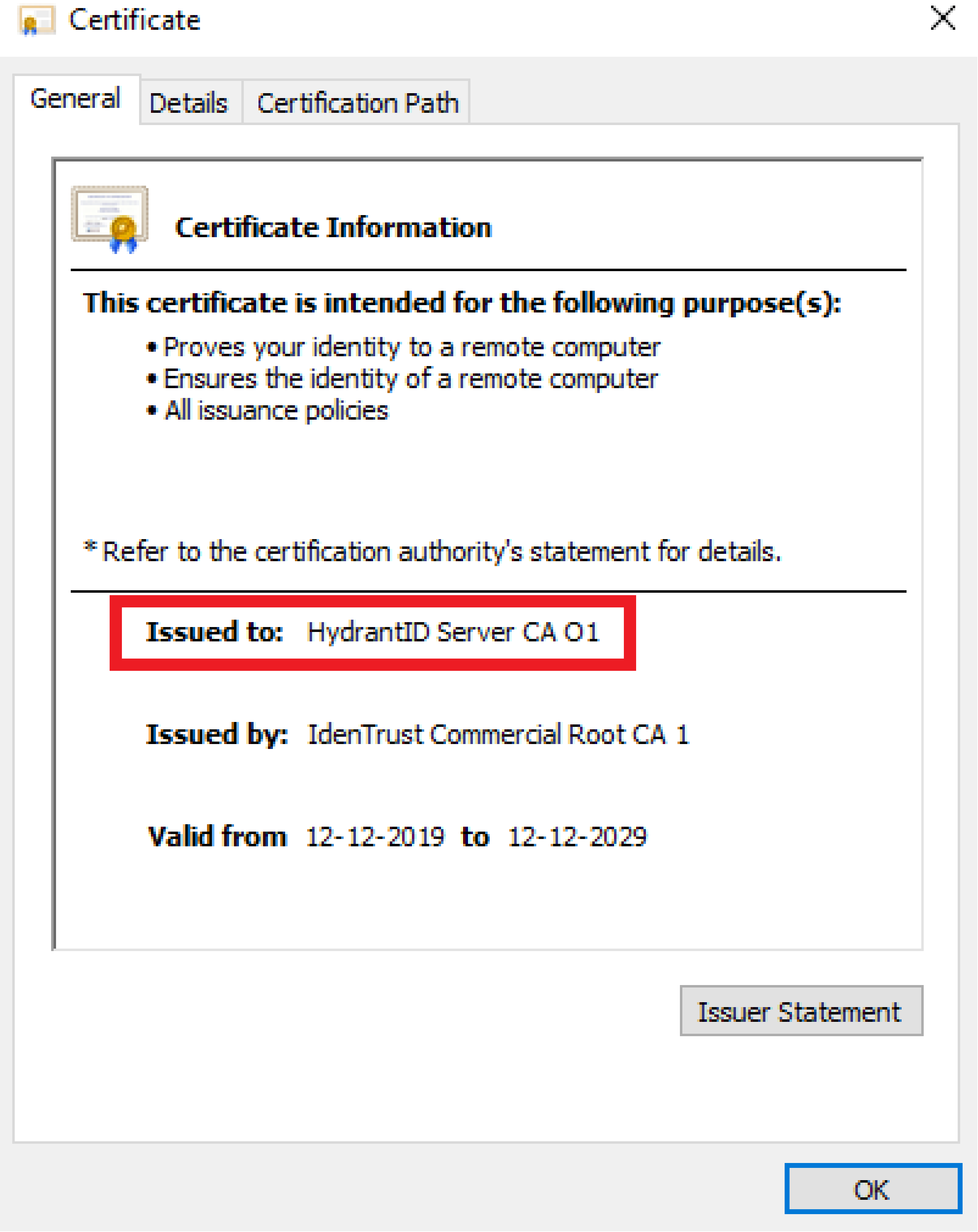
2. Add a Trusted/Internal CA Certificate

Note: If the trusted/internal Certificate Authority used in Step (a) also issues certificates to users then skip Step (b). There is no need to add the same CA certificate again and it must be avoided as well. If the same CA certificate is added again, trustpoint is configured with "validation-usage none" which can impact certificate authentication for RAVPN.

Step 1. Navigate to Devices > Certificates and click Add Cert Enrollment .

Select Device and click on plus sign (+) under Cert Enrollment.

Here, HydrantID Server CA 01 is used to issue identity/user certificates.



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- All issuance policies

* Refer to the certification authority's statement for details.

Issued to: HydrantID Server CA O1

Issued by: IdenTrust Commercial Root CA 1

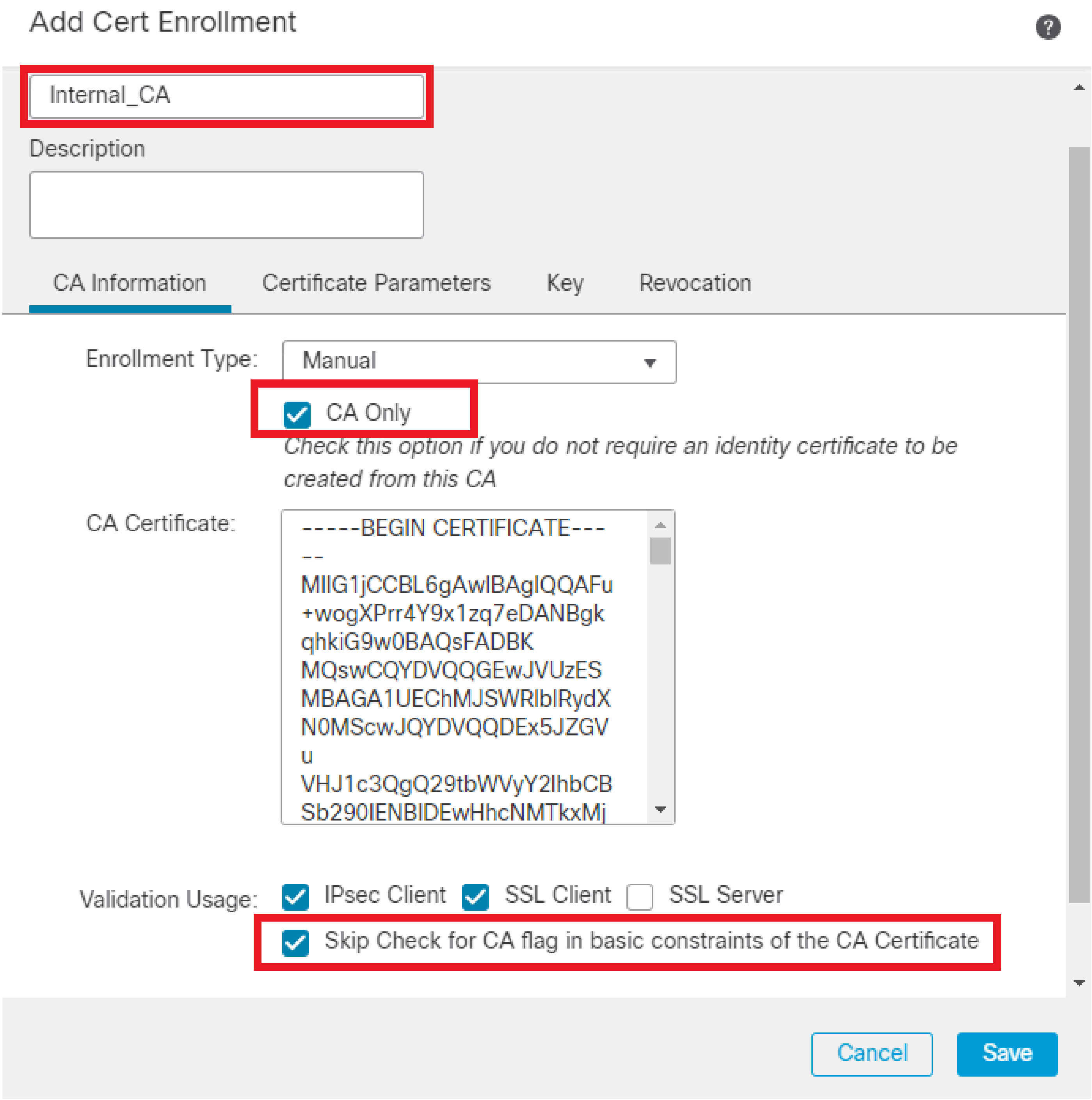
Valid from 12-12-2019 **to** 12-12-2029

HydrantID Server CA 01

Step 2. Enter a trustpoint name and selectManual as the enrollment type under CA information.

Step 3. Check CA Onlyand paste the trusted/internal CA certificate in pem format.

Step 4. Check **Skip Check for CA flag in basic constraints of the CA Certificate**and click Save.



Add Cert Enrollment

Internal_CA

Description

Enrollment Type: Manual

☑ CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

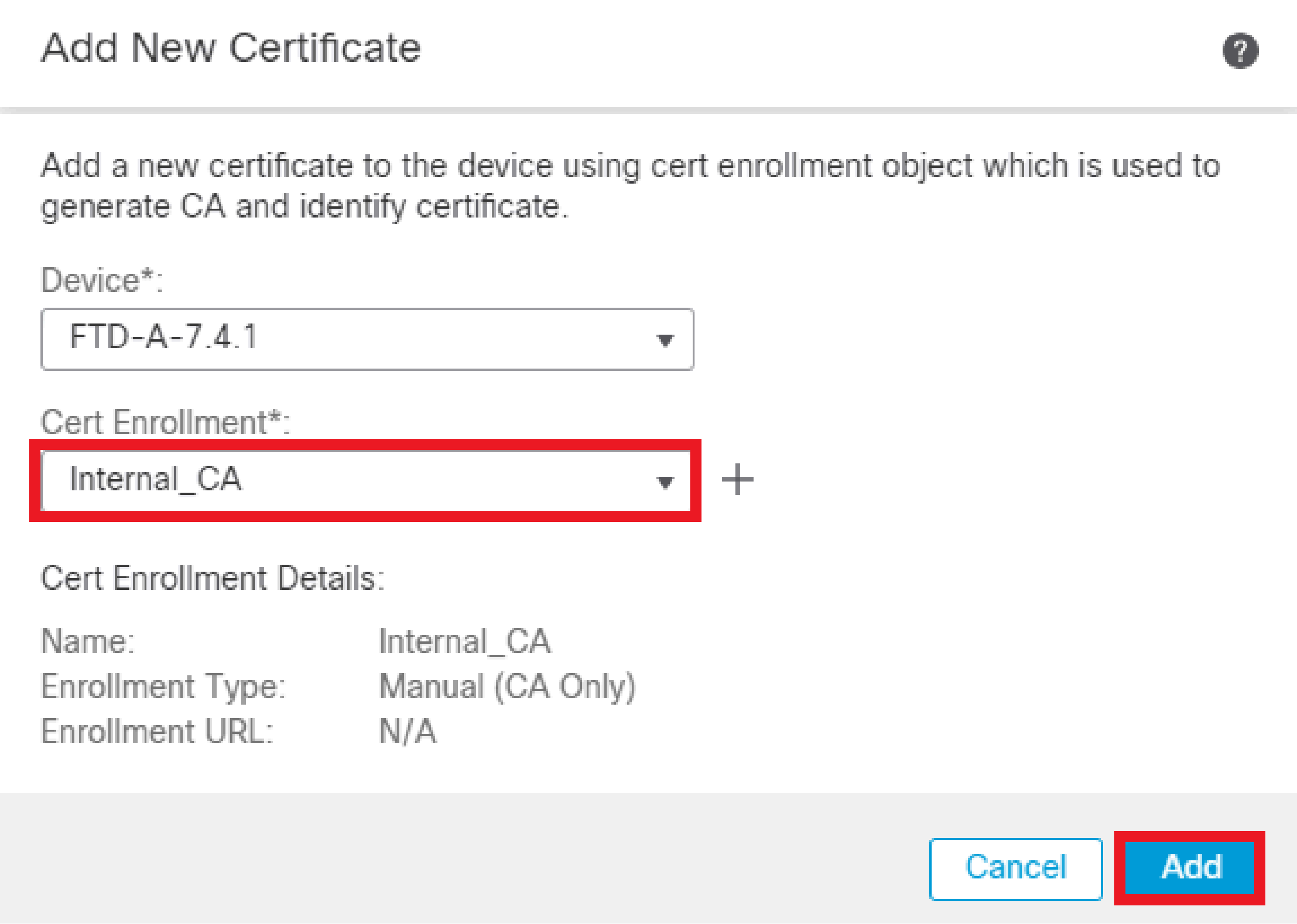
```
-----BEGIN CERTIFICATE---
--
MIIG1jCCBL6gAwIBAgIQQAFu
+wogXPrr4Y9x1zq7eDANBgk
qhkiG9w0BAQsFADBK
MQswCQYDVQQGEwJVUzES
MBAGA1UEChMJSWRlbIRydX
N0MScwJQYDVQQDEx5JZGV
u
VHJ1c3QgQ29tbWVyY2lhbCB
Sb290IENBIDEwHhcNMTkxMj
```

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

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

Add Trustpoint

Step 5. Under Cert Enrollment, select the trustpoint from the dropdown which was just created and click Add.



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD-A-7.4.1

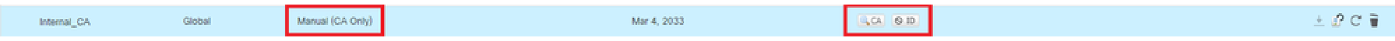
Cert Enrollment*: Internal_CA

Cert Enrollment Details:

Name: Internal_CA
Enrollment Type: Manual (CA Only)
Enrollment URL: N/A

Add Internal CA

Step 6. The certificate added earlier is shown as:



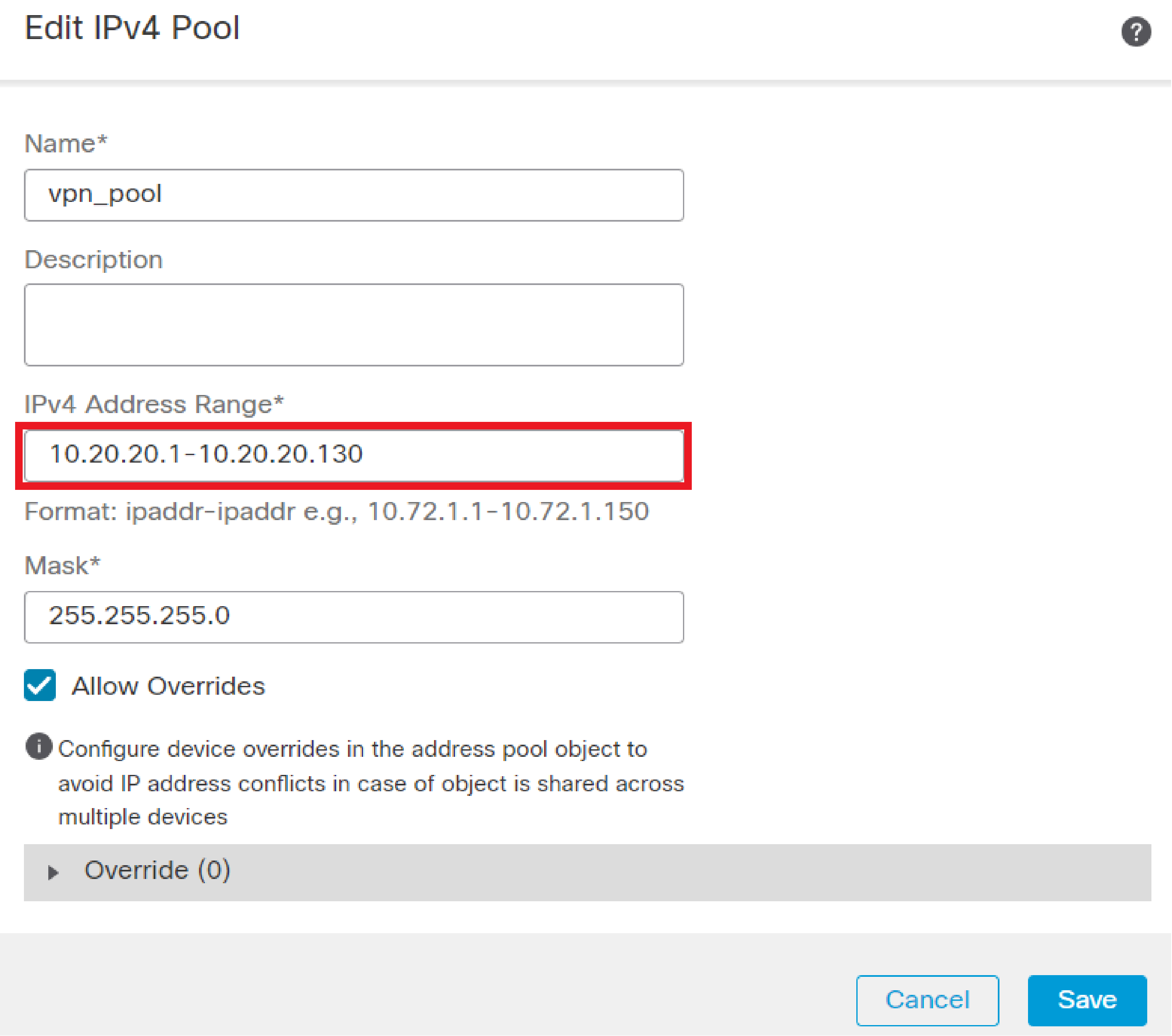
Internal_CA Global Manual (CA Only) Mar 4, 2033

Added Certificate

3. Configure Address Pool for VPN Users

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

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



Edit IPv4 Pool

Name*

vpn_pool

Description

IPv4 Address Range*

10.20.20.1-10.20.20.130

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

Add IPv4 Pool

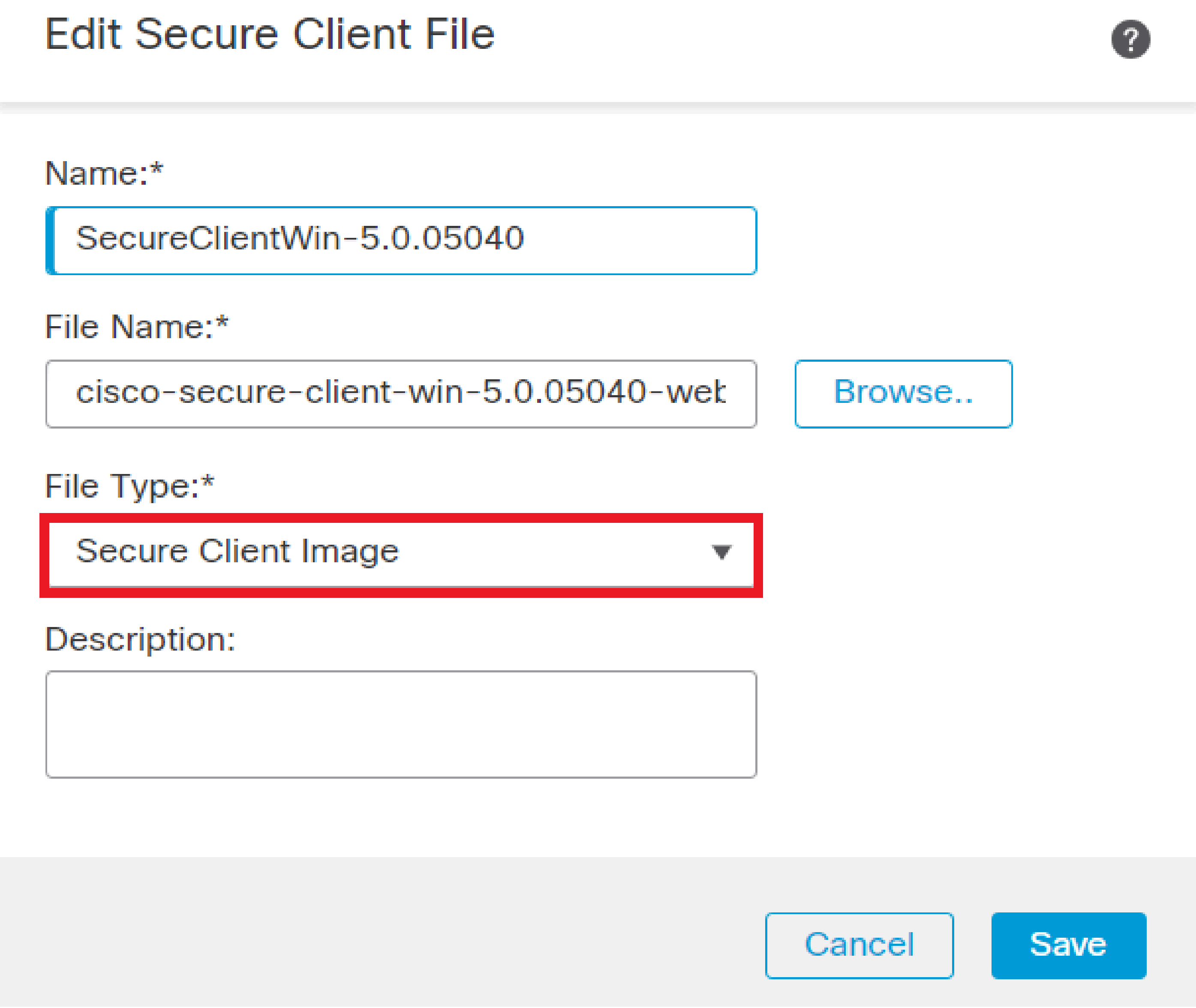
4. Upload Secure Client Images

Step 1. Download webdeploy secure client images as per OS from Cisco Software site.

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

Step 3. Enter the name and select the Secure Client file from the disk.

Step 4. Select the file type as Secure Client Image and click on Save.



Edit Secure Client File

Name:* SecureClientWin-5.0.05040

File Name:* cisco-secure-client-win-5.0.05040-wel

File Type:* Secure Client Image

Description:

Add Secure Client Image

5. Create and Upload XML Profile

Step 1. Download and install the Secure Client `Profile Editor` from [Cisco Software](https://software.cisco.com) site.

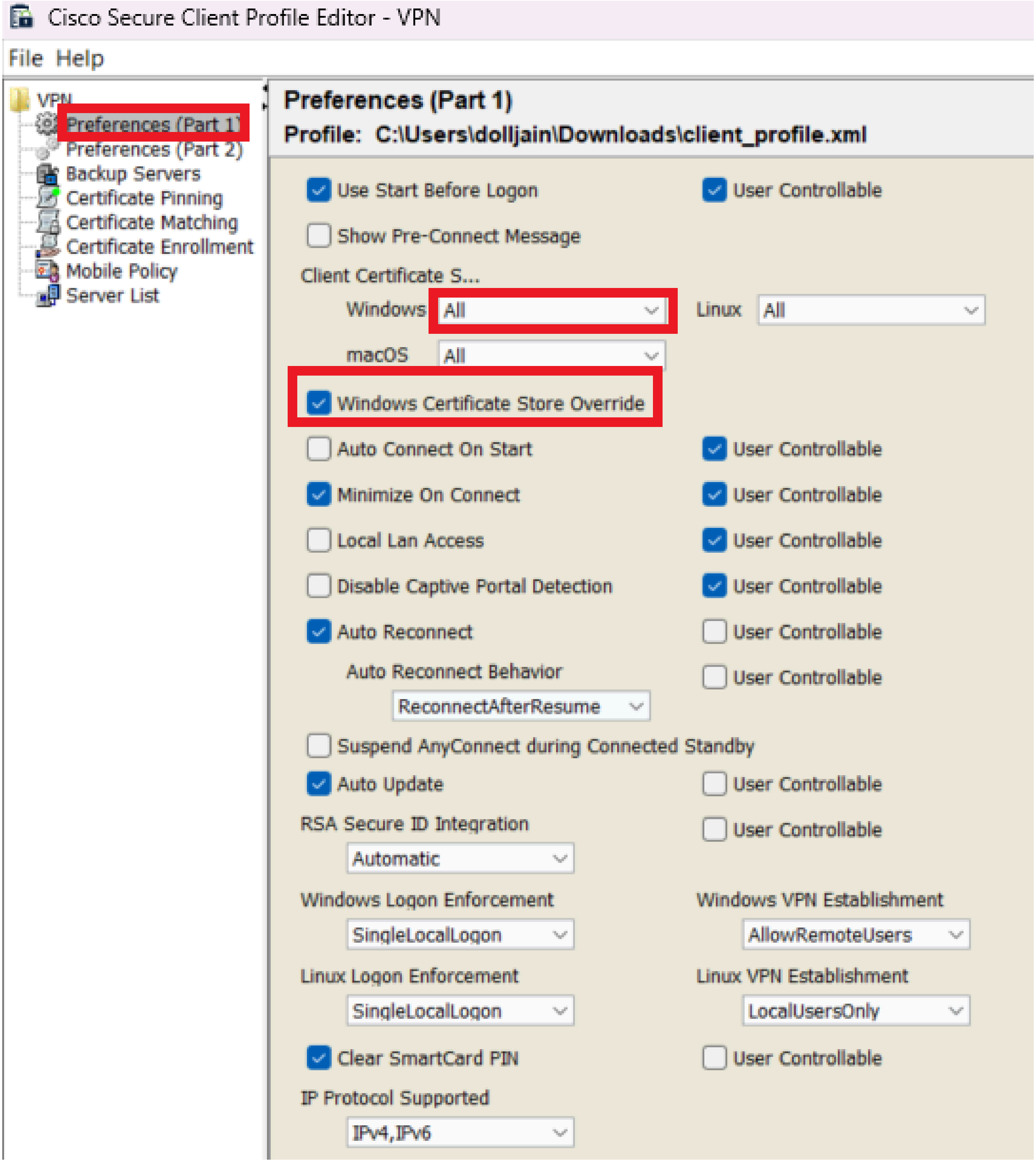
Step 2. Create a new profile and select `All` from the Client Certificate Selection dropdown. It mainly controls which certificate store(s) Secure Client can use to store and read certificates.

Two other available options are:

1. **Machine** - Secure Client is restricted to certificate lookup on the Windows local machine certificate store.
2. **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, by the UI process. When using IPSec/IKEv2, this feature in the Secure Client Profile is not applicable.



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 1)

Profile: C:\Users\dolljain\Downloads\client_profile.xml

☑ Use Start Before Logon ☑ User Controllable

□ Show Pre-Connect Message

Client Certificate S...

Windows: All — Linux: All

macOS: All

☑ Windows Certificate Store Override

□ Auto Connect On Start ☑ User Controllable

☑ Minimize On Connect ☑ User Controllable

□ Local Lan Access ☑ User Controllable

□ Disable Captive Portal Detection ☑ User Controllable

☑ Auto Reconnect □ User Controllable

Auto Reconnect Behavior: ReconnectAfterResume □ User Controllable

□ Suspend AnyConnect during Connected Standby

☑ Auto Update □ User Controllable

RSA Secure ID Integration: Automatic □ User Controllable

Windows Logon Enforcement: SingleLocalLogon

Windows VPN Establishment: AllowRemoteUsers

Linux Logon Enforcement: SingleLocalLogon

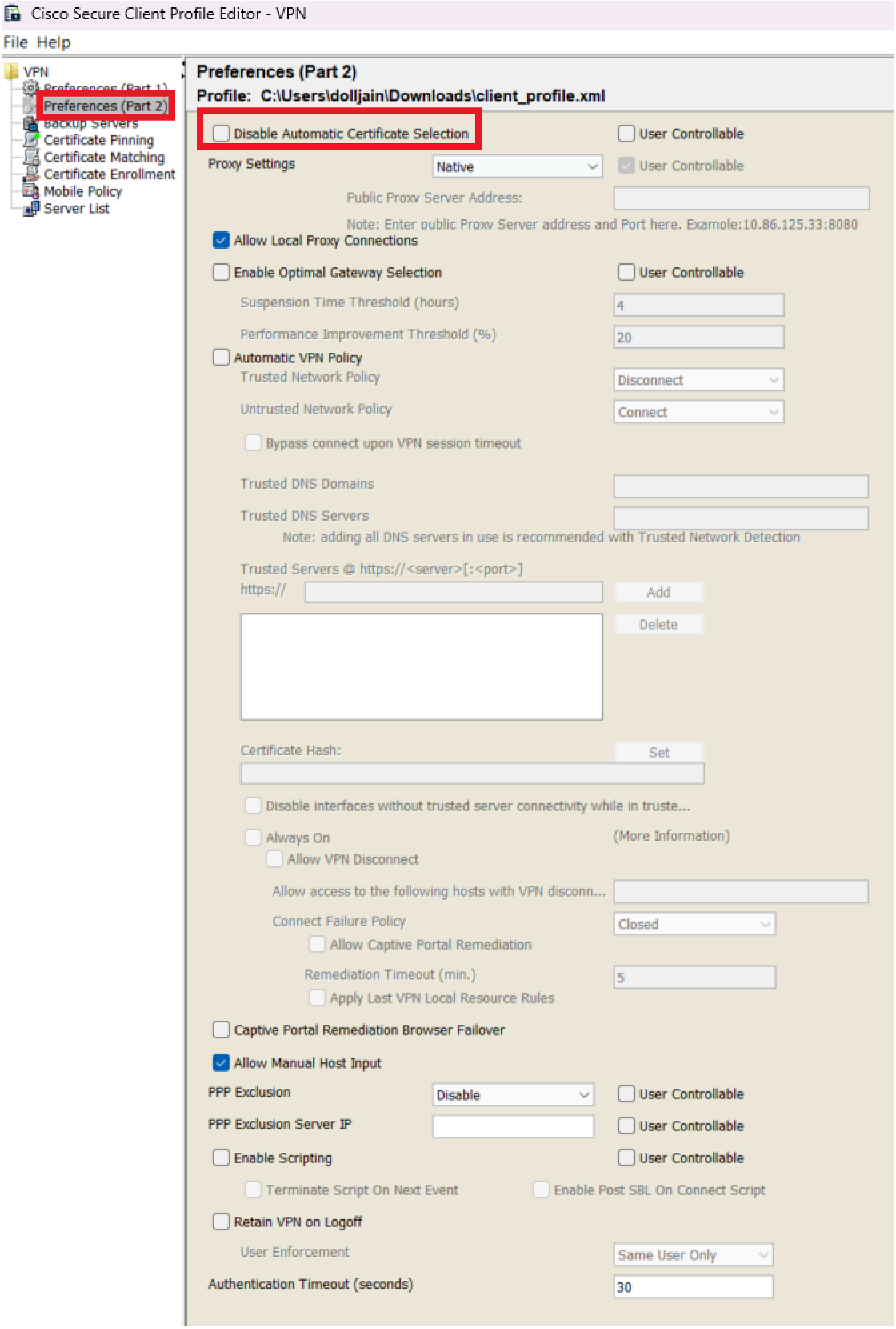
Linux VPN Establishment: LocalUsersOnly

☑ Clear SmartCard PIN □ User Controllable

IP Protocol Supported: IPv4,IPv6

Add Preferences (Part1)

Step 3. Uncheck the Disable Automatic Certificate Selection as it avoids the prompt for the user to select the authentication certificate.



Cisco Secure Client Profile Editor - VPN

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://

Certificate Hash:

□ 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

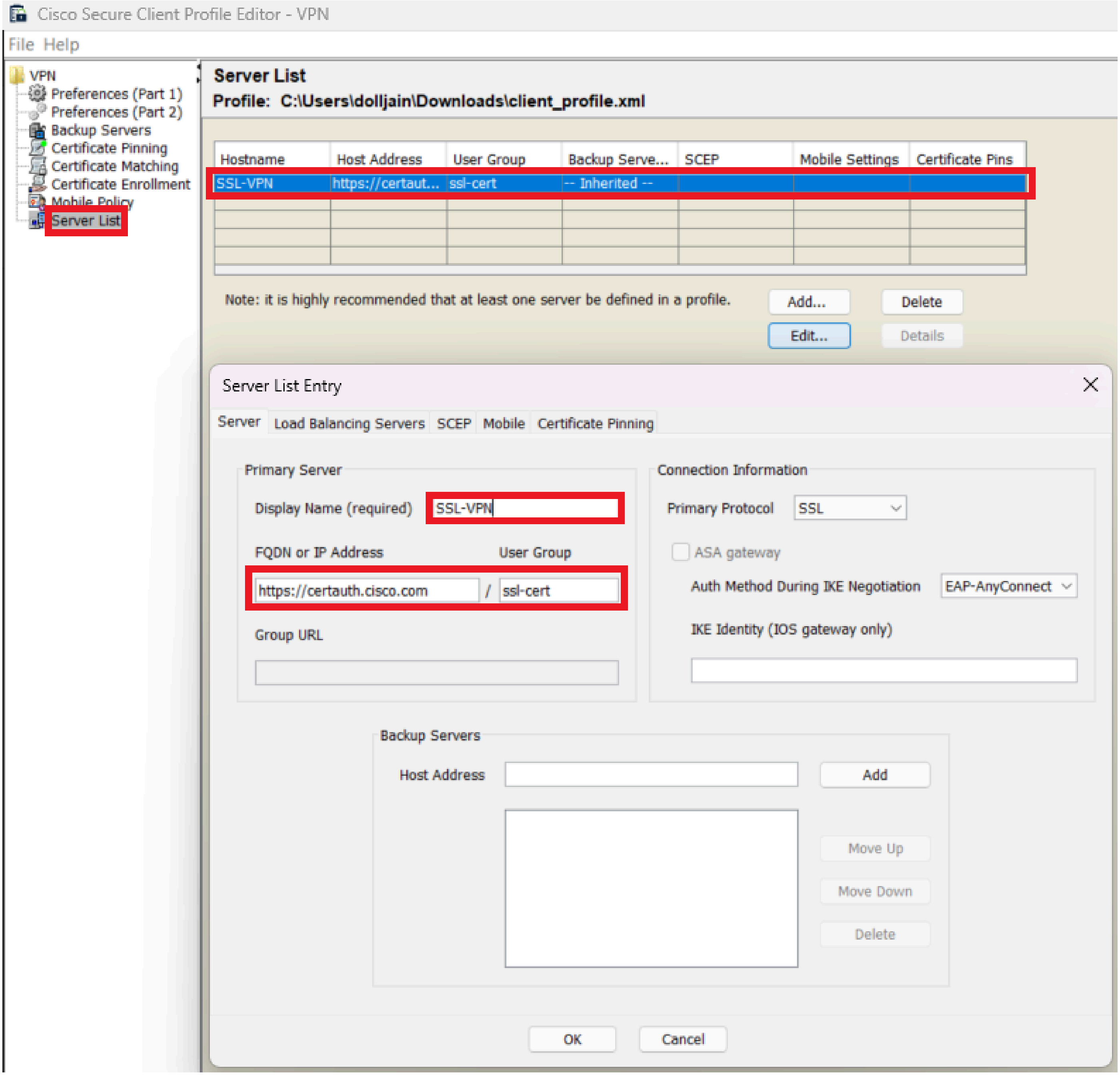
□ Retain VPN on Logoff

User Enforcement: Same User Only

Authentication Timeout (seconds): 30

Add Preferences (Part2)

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.



Cisco Secure Client Profile Editor - VPN

Server List

Profile: C:\Users\dolljain\Downloads\client_profile.xml

Hostname	Host Address	User Group	Backup Serve...	SCEP	Mobile Settings	Certificate Pins
SSL-VPN	https://certaut...	ssl-cert	-- Inherited --			

Note: it is highly recommended that at least one server be defined in a profile.

Server List Entry

Primary Server

Display Name (required): SSL-VPN

FQDN or IP Address / User Group: https://certauth.cisco.com / ssl-cert

Group URL:

Connection Information

Primary Protocol: SSL

□ ASA gateway

Auth Method During IKE Negotiation: EAP-AnyConnect

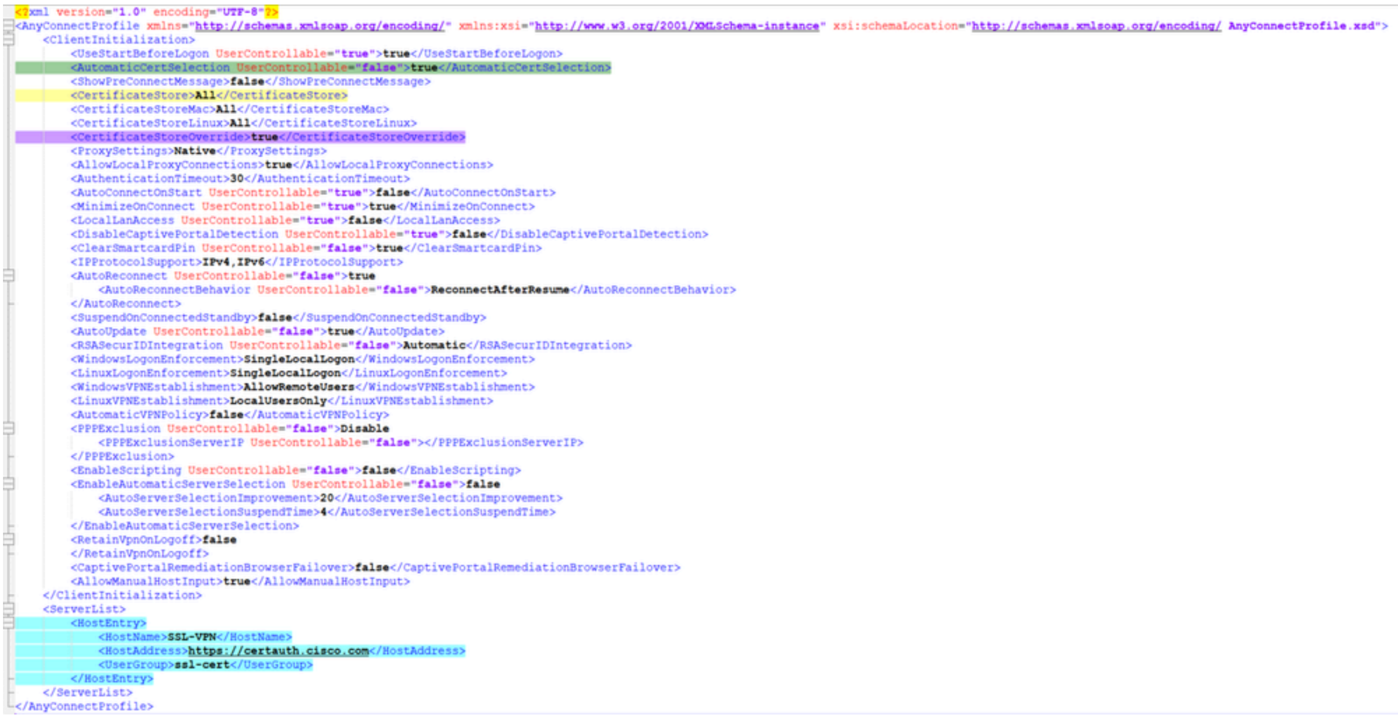
IKE Identity (IOS gateway only):

Backup Servers

Host Address:

Add Server List

Step 5. Finally, the XML profile is ready for use.



```xml
<?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>
```

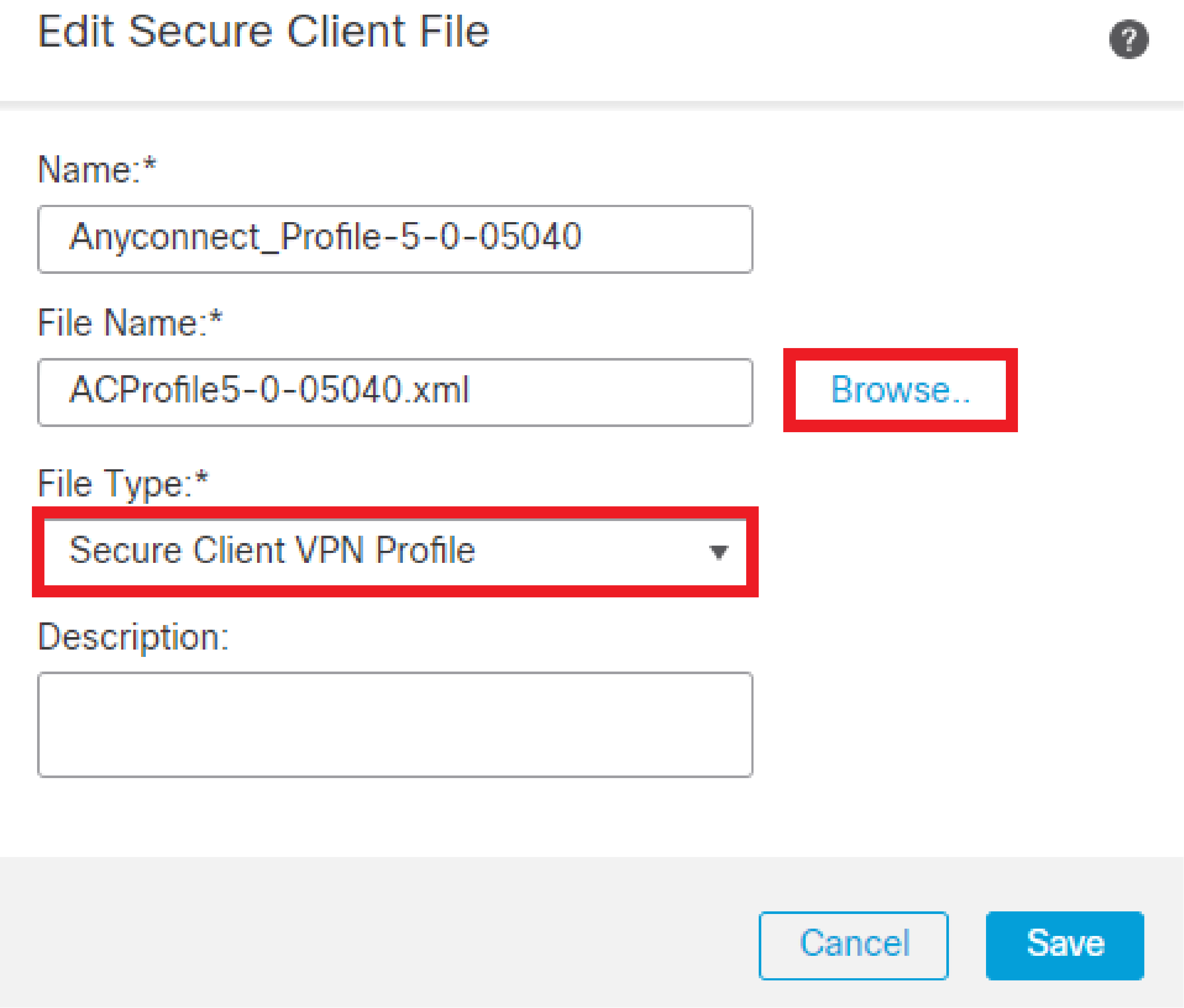
XML Profile

Location of XML profiles for various operating systems:

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

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

Enter the name for the file and click on Browse to select the XML profile. Click Save.



Edit Secure Client File

Name:* Anyconnect_Profile-5-0-05040

File Name:* ACProfile5-0-05040.xml

File Type:* Secure Client VPN Profile

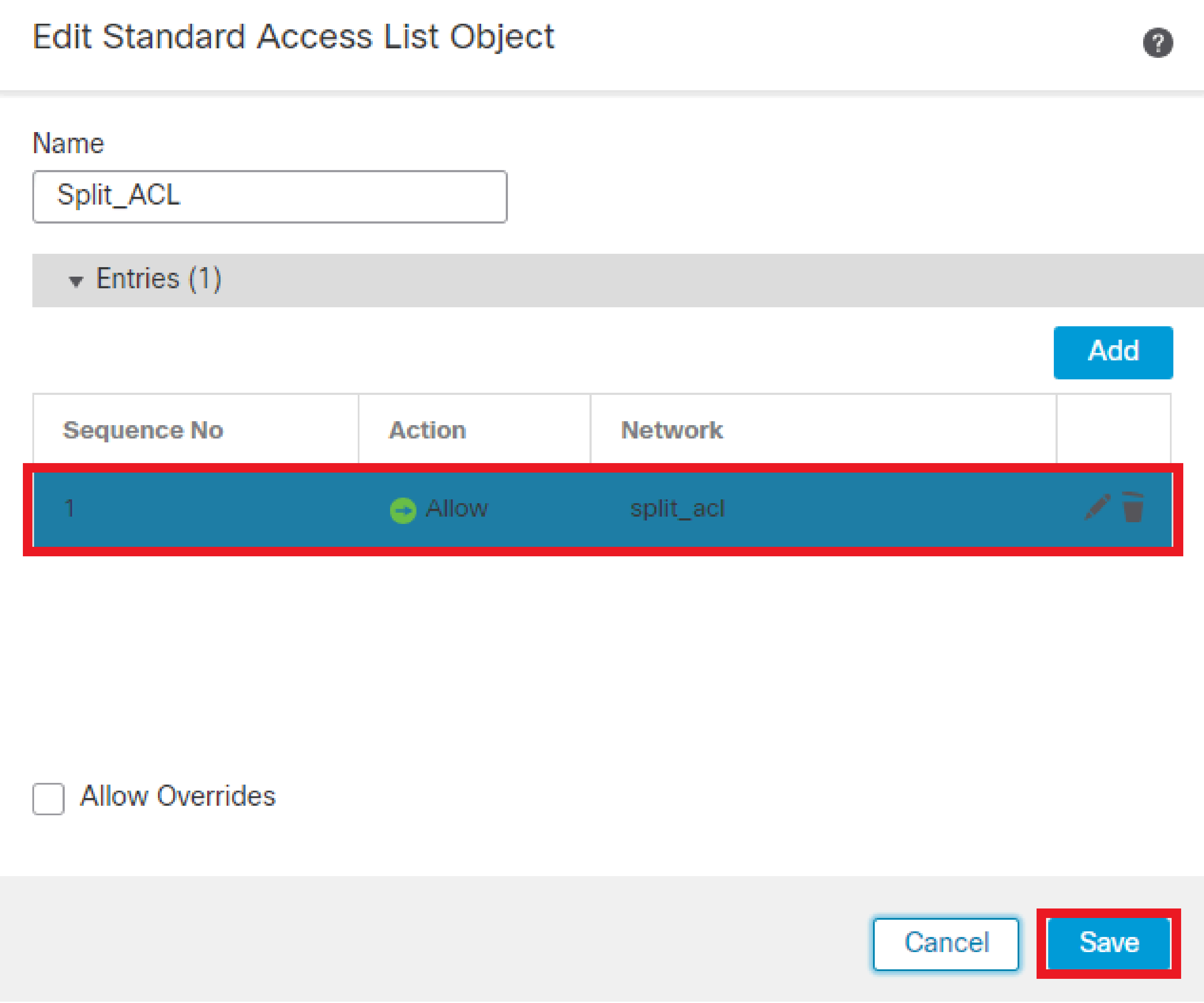
Description:

Add Secure Client VPN Profile

Remote Access VPN Configuration

Step 1. Create an ACL as per requirement to allow access to internal resources.

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



Edit Standard Access List Object

Name

Split_ACL

▾ Entries (1)

Sequence No	Action	Network	
1	● Allow	split_acl	

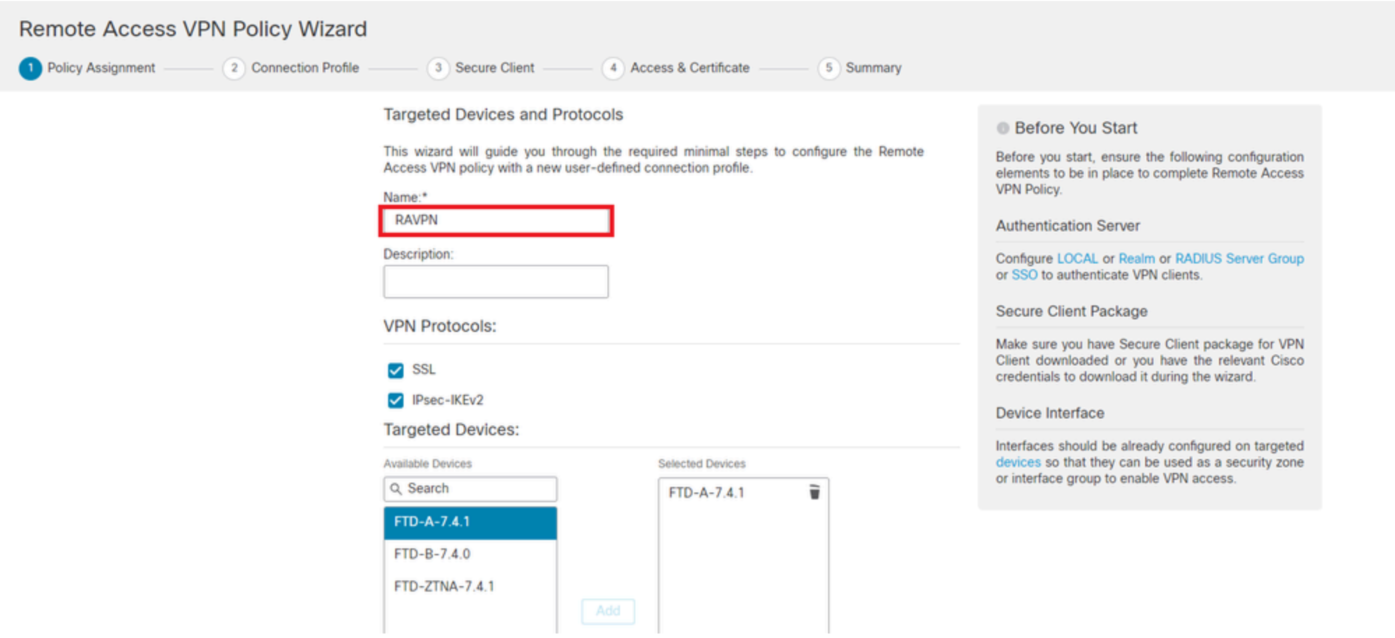
□ Allow Overrides

Add Standard ACL

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

Step 2. Navigate to Devices > VPN > Remote Access and click Add.

Step 3. Enter the name of the profile, then select the FTD device and click on Next.



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:* RAVPN

Description:

VPN Protocols:

☑ SSL

☑ IPsec-IKEv2

Targeted Devices:

Available Devices: FTD-A-7.4.1, FTD-B-7.4.0, FTD-ZTNA-7.4.1

Selected Devices: FTD-A-7.4.1

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

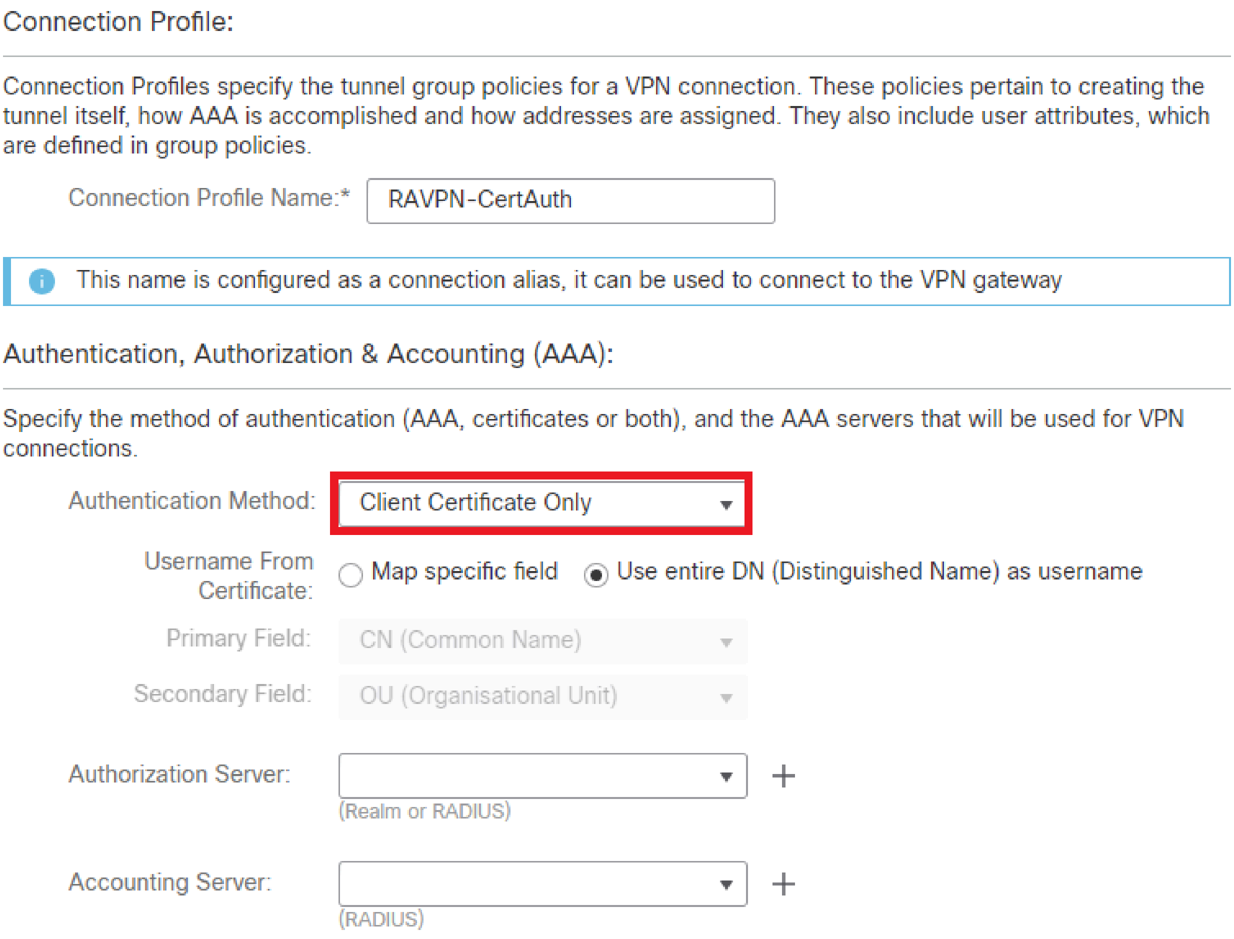
Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

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.

Add Profile Name

Step 4. Enter the Connection Profile Nameand select the Authentication Method as Client Certificate Only under Authentication, Authorization and Accounting (AAA).



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:* RAVPN-CertAuth

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)

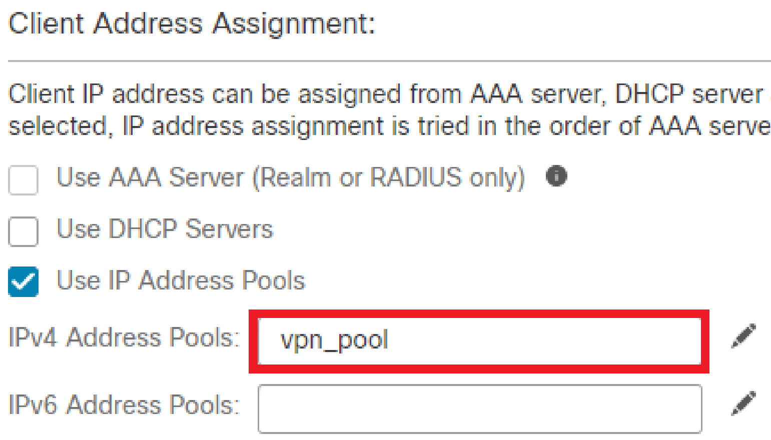
Secondary Field: OU (Organisational Unit)

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

Select Authentication Method

Step 5. Click on Use IP Address Pools under Client Address Assignment and select the IPv4 Address Pool created earlier.



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

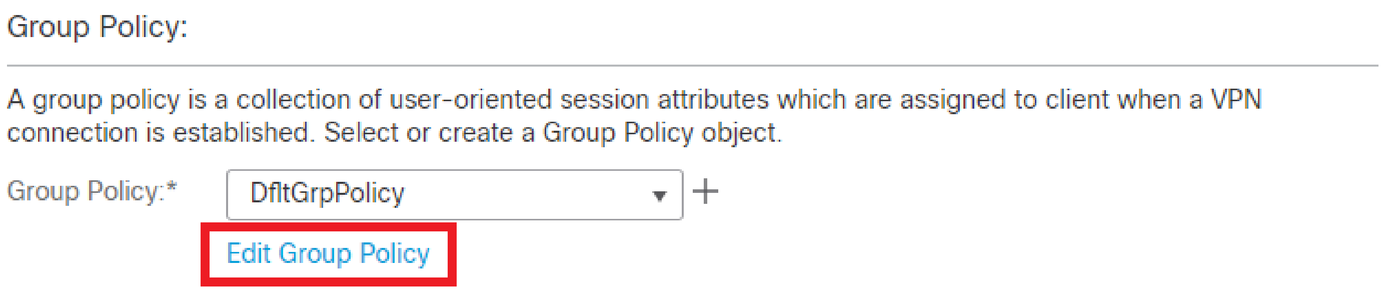
☑ Use IP Address Pools

IPv4 Address Pools: vpn_pool

IPv6 Address Pools:

Select Client Address Assignment

Step 6. Edit the Group Policy.



Group Policy:

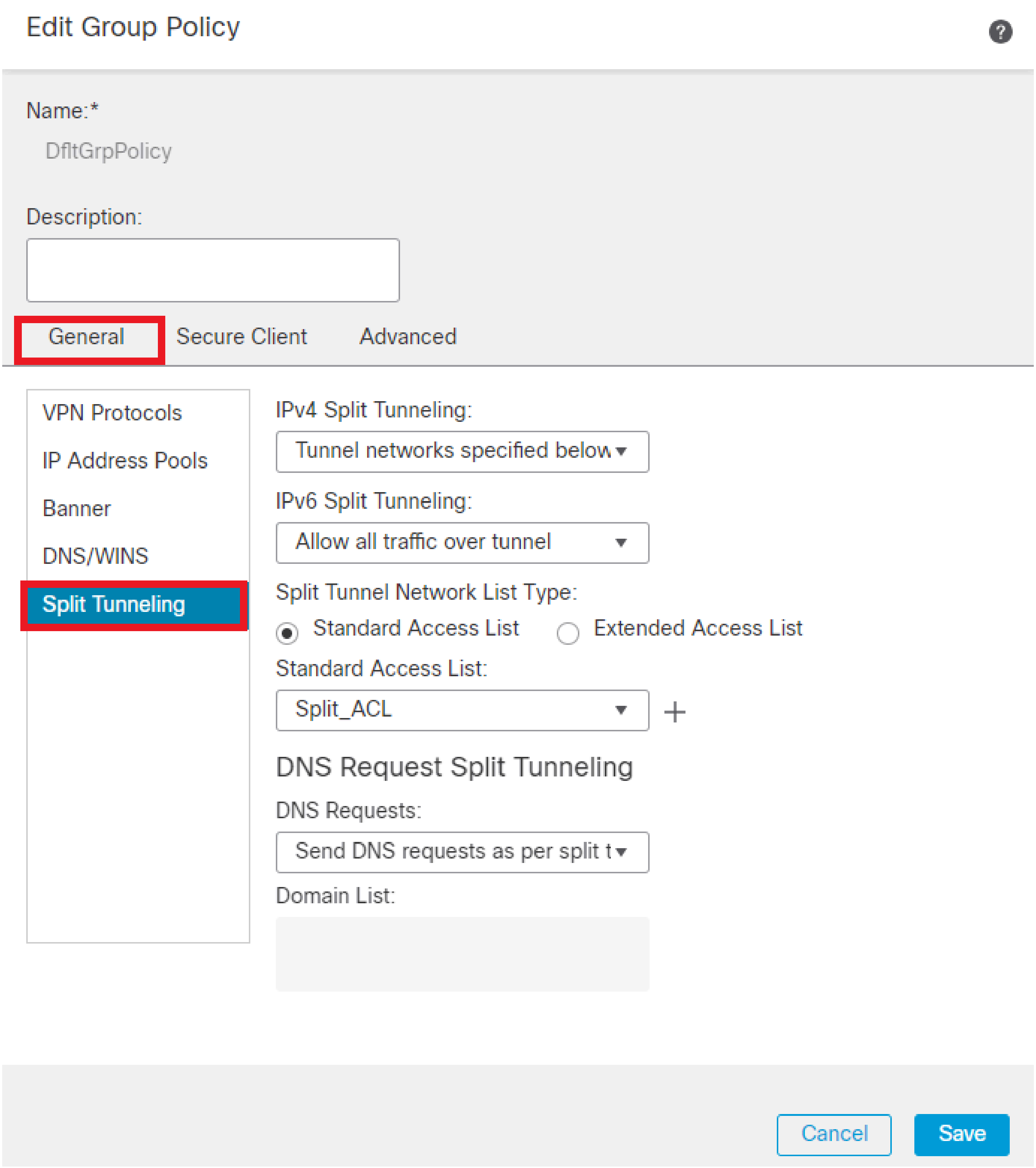
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* DfltGrpPolicy

Edit Group Policy

Step 7. Navigate to General > Split Tunneling , select Tunnel networks specified below and select Standard Access List under Split Tunnel Network List Type.

Select the ACL created earlier.



Edit Group Policy

Name:*

DfltGrpPolicy

Description:

General | Secure Client | Advanced

IPv4 Split Tunneling: Tunnel networks specified below

IPv6 Split Tunneling: Allow all traffic over tunnel

Split Tunnel Network List Type: ● Standard Access List ○ Extended Access List

Standard Access List: Split_ACL

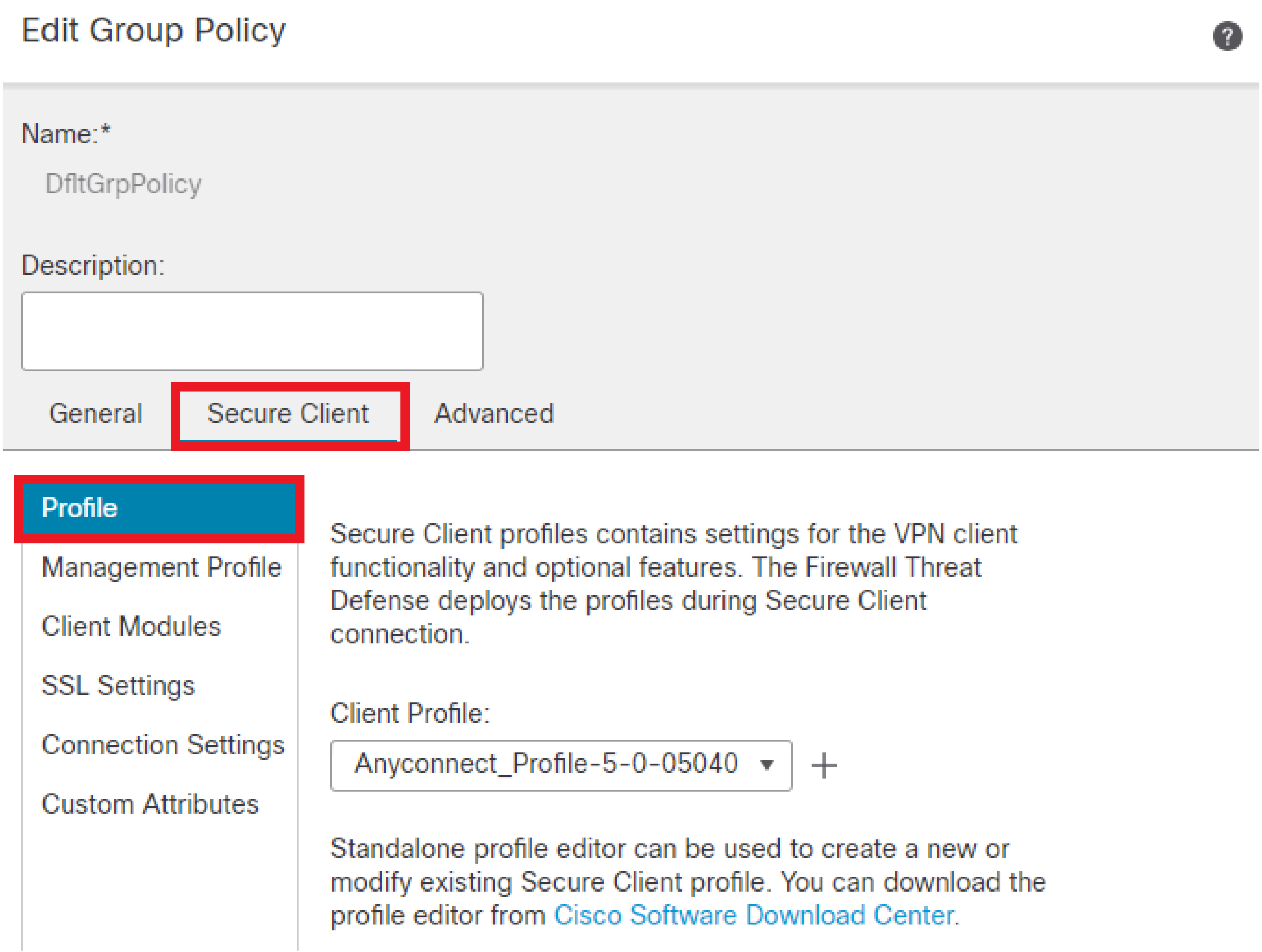
DNS Request Split Tunneling

DNS Requests: Send DNS requests as per split t

Domain List:

Add Split Tunneling

Step 8. Navigate to Secure Client > Profile , select the Client Profile and click Save.



Edit Group Policy

Name:*

DfltGrpPolicy

Description:

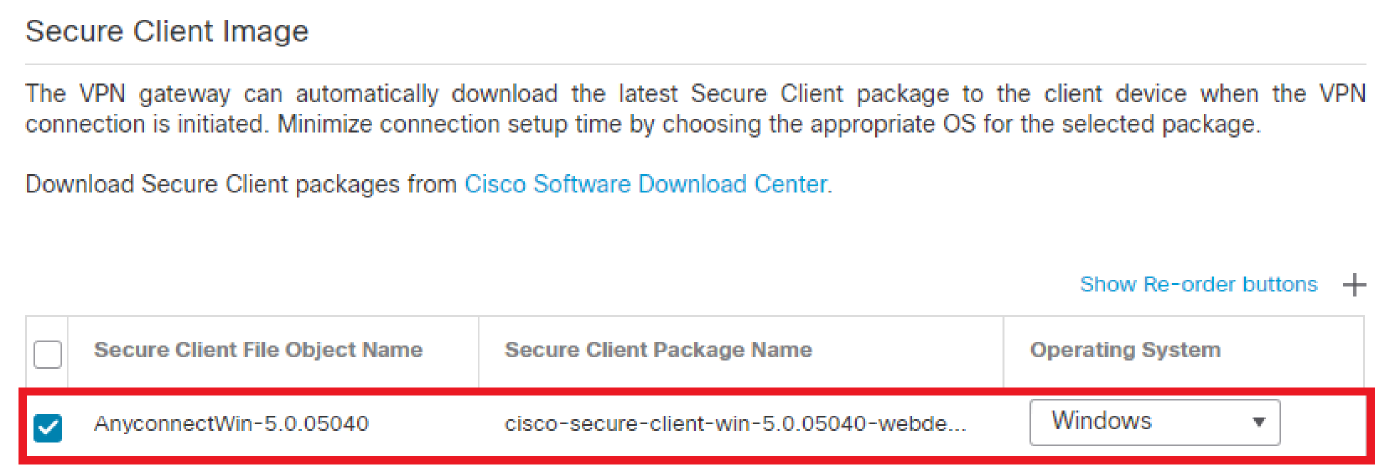
Secure Client profiles contains settings for the VPN client functionality and optional features. The Firewall Threat Defense deploys the profiles during Secure Client connection.

Client Profile: Anyconnect_Profile-5-0-05040

Standalone profile editor can be used to create a new or modify existing Secure Client profile. You can download the profile editor from Cisco Software Download Center.

Add Secure Client Profile

Step 9. Click on Next, then select the Secure Client Image and click Next.



Secure Client Image

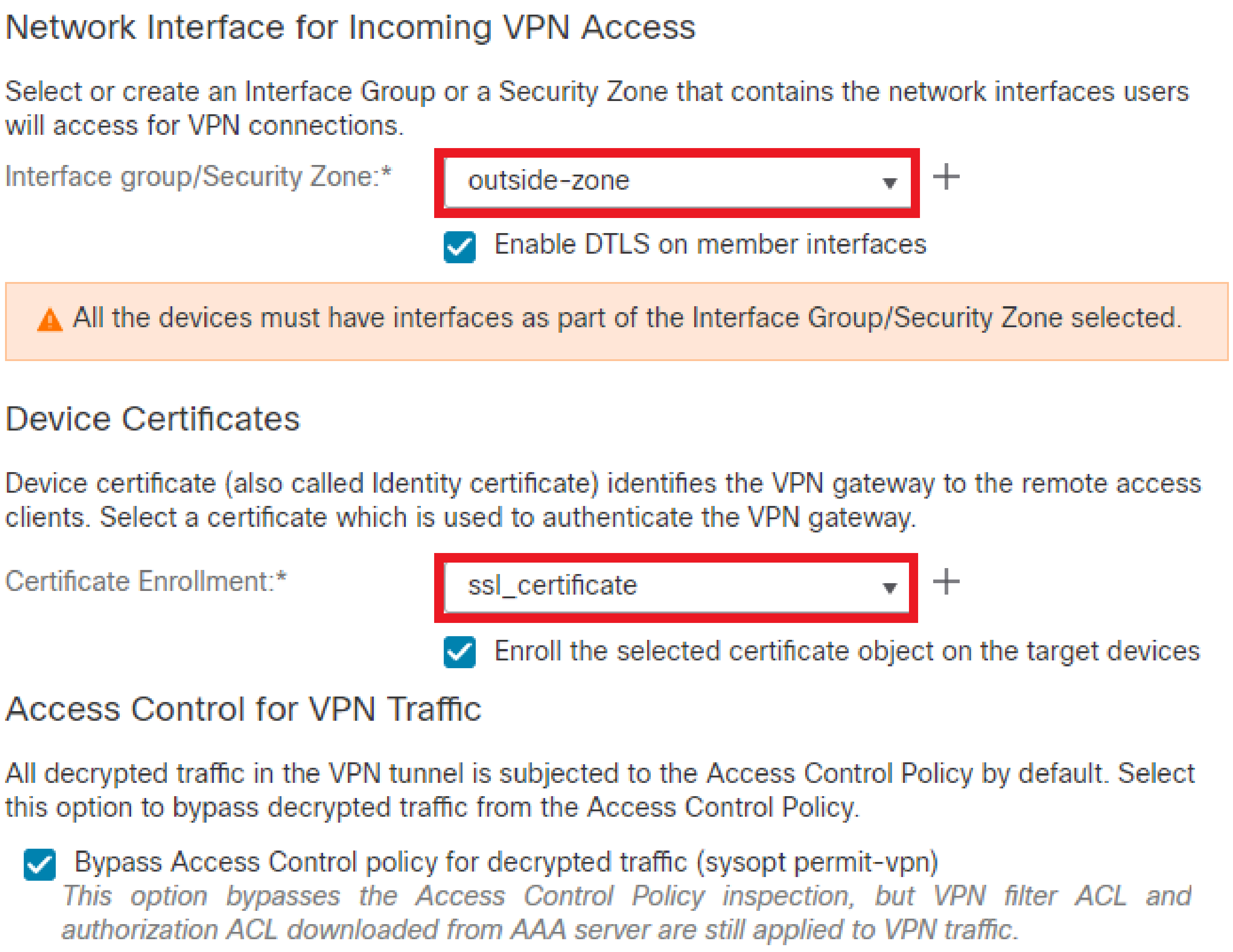
The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from Cisco Software Download Center.

□	Secure Client File Object Name	Secure Client Package Name	Operating System
☑	AnyconnectWin-5.0.05040	cisco-secure-client-win-5.0.05040-webde...	Windows

Add Secure Client Image

Step 10. Select the Network Interface for VPN Access, choose the Device Certificates and check sysopt permit-vpn and click Next.



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:* outside-zone

☑ 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:* ssl_certificate

☑ Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

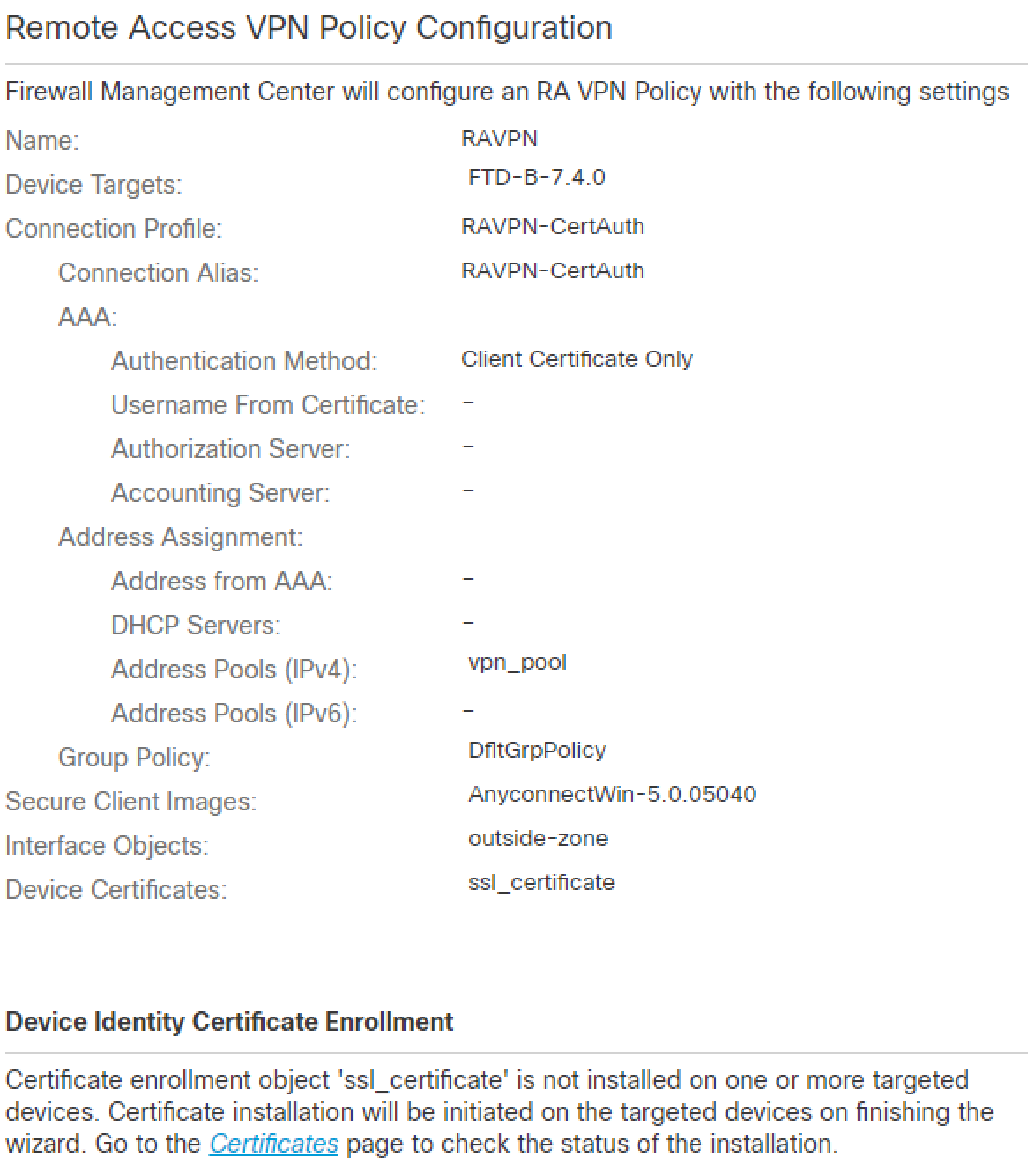
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

☑ 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.

Add Access Control for VPN Traffic

Step 11. Finally, review all the configurations and click Finish.



Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	FTD-B-7.4.0
Connection Profile:	RAVPN-CertAuth
Connection Alias:	RAVPN-CertAuth
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
Secure Client Images:	AnyconnectWin-5.0.05040
Interface Objects:	outside-zone
Device Certificates:	ssl_certificate

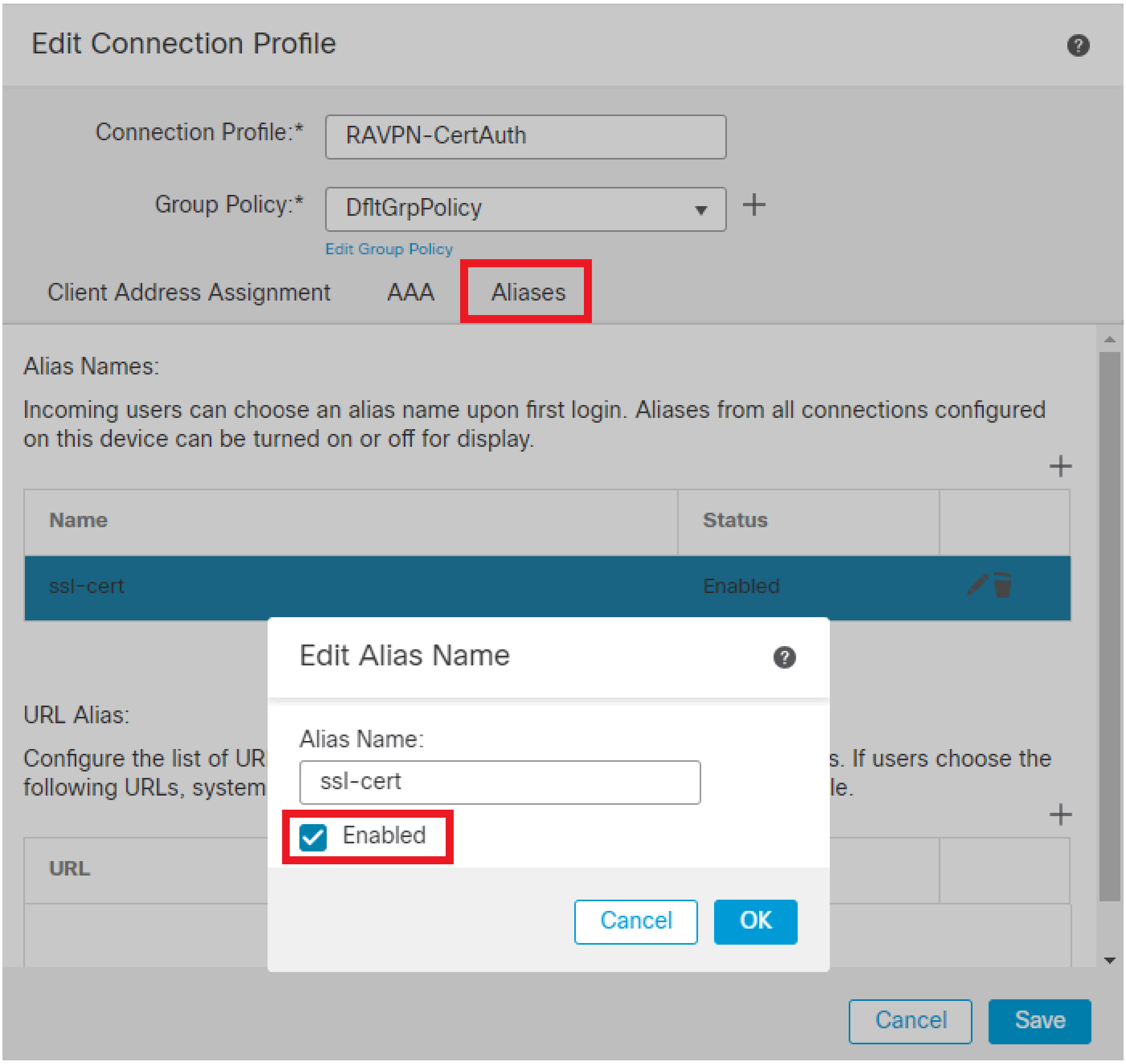
Device Identity Certificate Enrollment

Certificate enrollment object 'ssl_certificate' 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.

Remote Access VPN Policy Configuration

Step 12. Once the initial setup of Remote Access VPN is complete, edit the Connection Profile created and go to Aliases.

Step 13. Configure group-alias by clicking on the plus icon (+).



Edit Connection Profile

Connection Profile:* RAVPN-CertAuth

Group Policy:* DfltGrpPolicy

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
ssl-cert	Enabled	

URL Alias:

Configure the list of UR... s. If users choose the following URLs, system ... le.

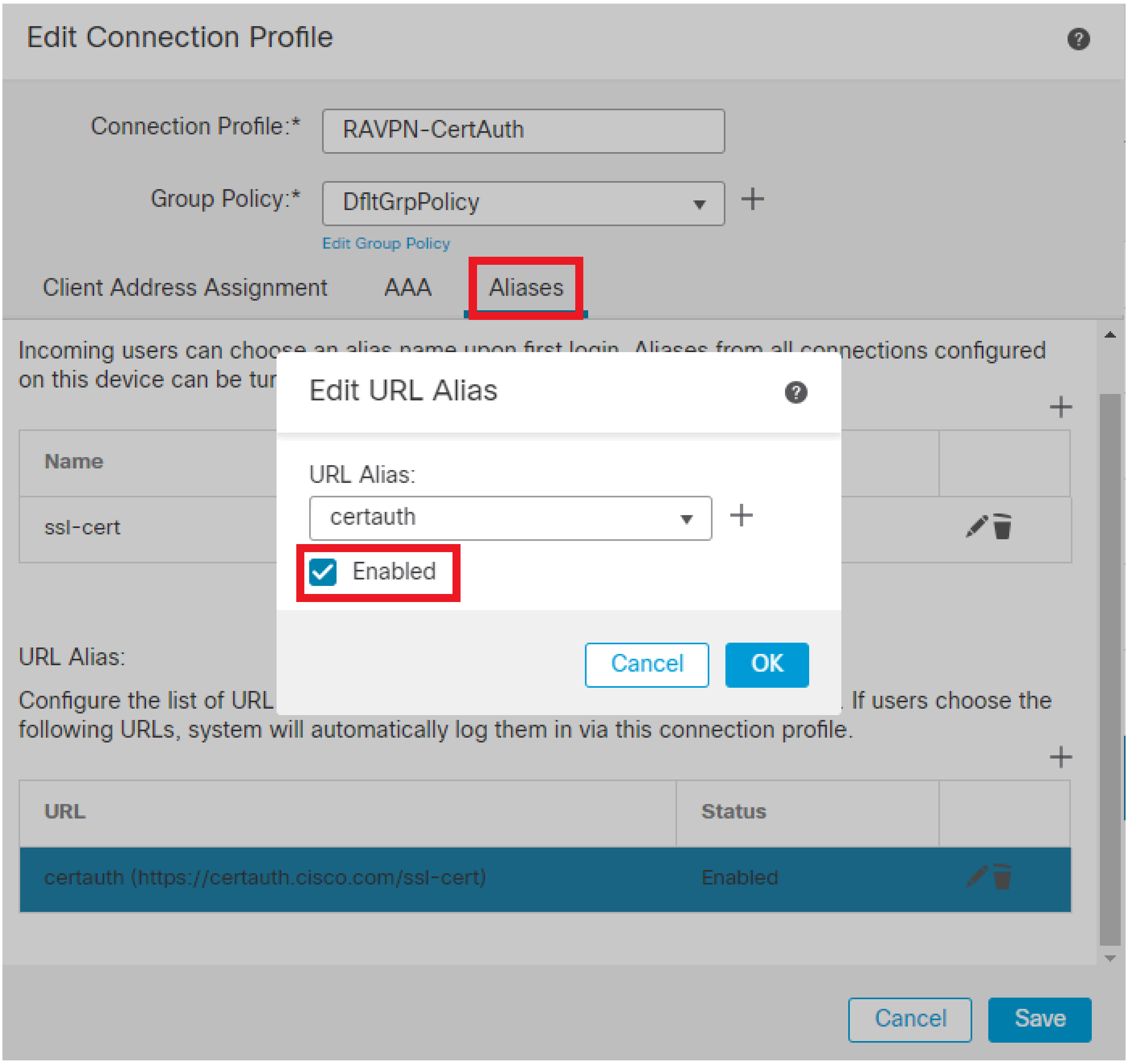
Edit Alias Name

Alias Name: ssl-cert

☑ Enabled

Edit Group Alias

Step 14. Configure group-url by clicking on the plus icon (+). Use the same Group URL configured earlier in the Client Profile.



Edit Connection Profile

Connection Profile:* RAVPN-CertAuth

Group Policy:* DfltGrpPolicy

Edit Group Policy

Client Address Assignment | AAA | Aliases

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be tur

Name		
ssl-cert		

Edit URL Alias

URL Alias: certauth

☑ Enabled

Cancel | OK

URL Alias:

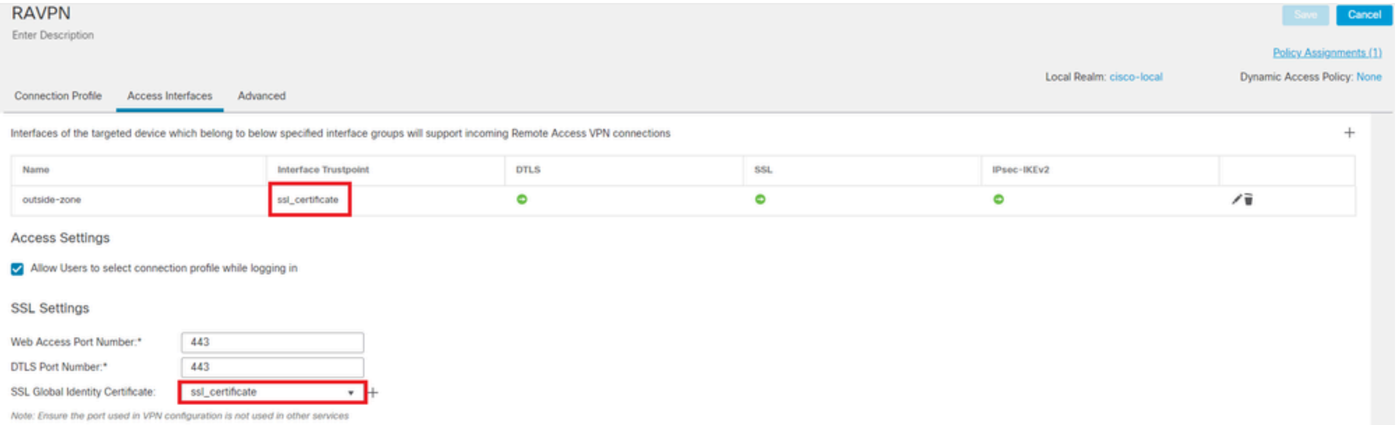
Configure the list of URL . If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status	
certauth (https://certauth.cisco.com/ssl-cert)	Enabled	

Cancel | Save

Edit Group URL

Step 15. Navigate to Access Interfaces. Select the Interface Truspoint and the SSL Global Identity Certificate under the SSL settings.



RAVPN

Enter Description

Save | Cancel

Policy Assignments (1)

Local Realm: cisco-local

Dynamic Access Policy: None

Connection Profile | Access Interfaces | Advanced

Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2	
outside-zone	ssl_certificate	●	●	●	

Access Settings

☑ Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:* 443

DTLS Port Number:* 443

SSL Global Identity Certificate: ssl_certificate

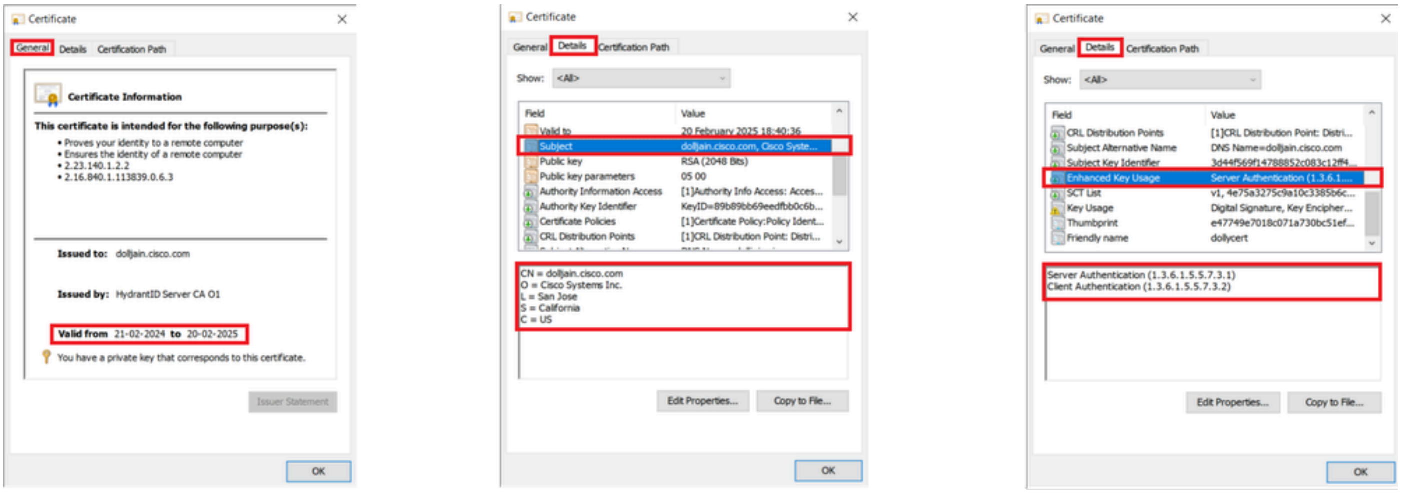
Note: Ensure the port used in VPN configuration is not used in other services

Edit Access Interfaces

Step 16. ClickSave and deploy these changes.

Verify

1. Secure Client PC must have the certificate installed with a valid date, subject and EKU on the user PC. This certificate must be issued by the CA whose certificate is installed on FTD as shown earlier. Here, the identity or user certificate is issued by "HydrantID Server CA 01".



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.2
- 2.16.840.1.113839.0.6.3

Issued to: doljain.cisco.com

Issued by: HydrantID Server CA 01

Valid from 21-02-2024 **to** 20-02-2025

You have a private key that corresponds to this certificate.

Show: <All>

Field	Value
Valid to	20 February 2025 18:40:36
Subject	doljain.cisco.com, Cisco Syste...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Information Access	[1]Authority Info Access: Acces...
Authority Key Identifier	KeyID=89b89bb69eedfbb0c6b...
Certificate Policies	[1]Certificate Policy:Policy Ident...
CRL Distribution Points	[1]CRL Distribution Point: Distri...

```
CN = doljain.cisco.com
O = Cisco Systems Inc.
L = San Jose
S = California
C = US
```

Show: <All>

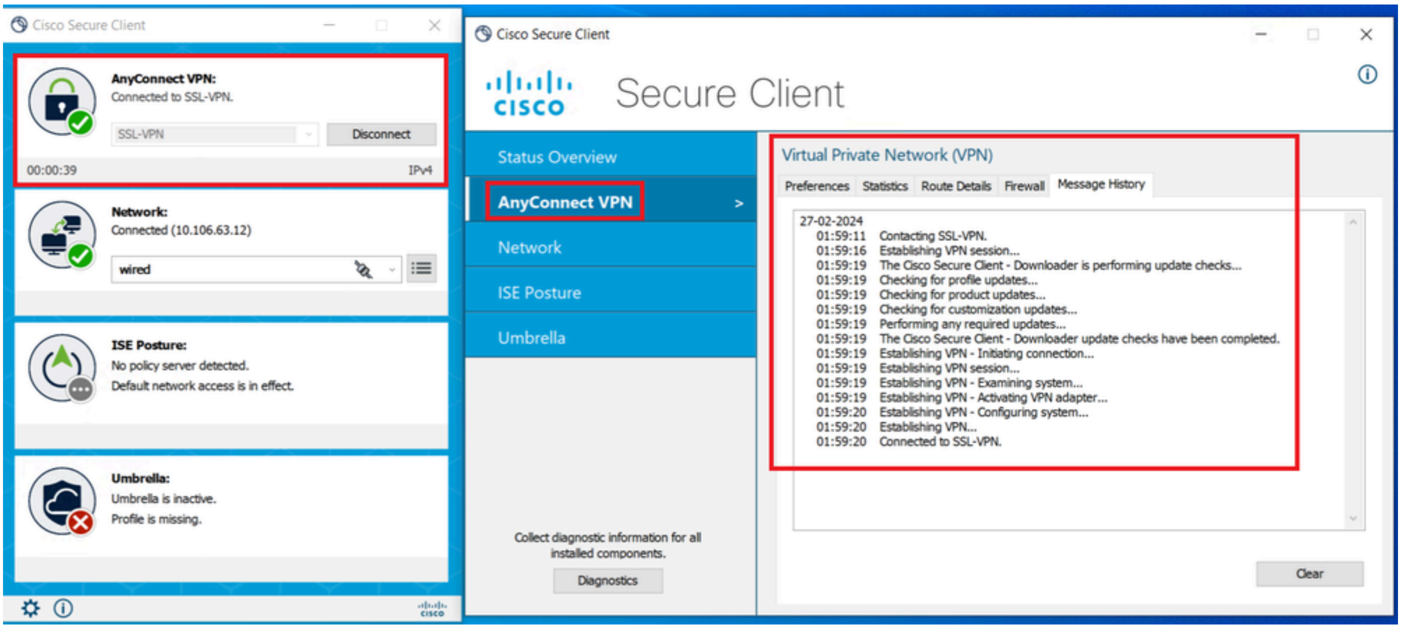
Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distri...
Subject Alternative Name	DNS Name=doljain.cisco.com
Subject Key Identifier	3d44f569f14788852c083c12ff4...
Enhanced Key Usage	Server Authentication (1.3.6.1....
SCT List	v1, 4e75a3275c9a10c3385b6c...
Key Usage	Digital Signature, Key Encipher...
Thumbprint	e47749e7018c071a730bc51ef...
Friendly name	dollycert

```
Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)
```

Certificate Highlights

Note: The client certificate must have the "Client Authentication" Enhanced Key Usage (EKU).

2. Secure Client must establish the connection.



```
27-02-2024
    01:59:11   Contacting SSL-VPN.
    01:59:16   Establishing VPN session...
    01:59:19   The Cisco Secure Client - Downloader is performing update checks...
    01:59:19   Checking for profile updates...
    01:59:19   Checking for product updates...
    01:59:19   Checking for customization updates...
    01:59:19   Performing any required updates...
    01:59:19   The Cisco Secure Client - Downloader update checks have been completed.
    01:59:19   Establishing VPN - Initiating connection...
    01:59:19   Establishing VPN session...
    01:59:19   Establishing VPN - Examining system...
    01:59:19   Establishing VPN - Activating VPN adapter...
    01:59:20   Establishing VPN - Configuring system...
    01:59:20   Establishing VPN...
    01:59:20   Connected to SSL-VPN.
```

Successful Secure Client Connection

3. Run show vpn-sessiondb anyconnect 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

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 this guide for common problems.