

Beveiligde verificatie van clientcertificaat configureren op FTD die wordt beheerd door FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[a. Een certificaat maken/importeren dat wordt gebruikt voor serververificatie](#)

[b. Een betrouwbaar/intern CA-certificaat toevoegen](#)

[c. Adresgroep voor VPN-gebruikers configureren](#)

[d. Beveiligde clientafbeeldingen uploaden](#)

[e. XML-profiel maken en uploaden](#)

[Configuratie van VPN voor externe toegang](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft het proces van het configureren van externe toegang tot VPN op Firepower Threat Defence (FTD), beheerd door Firepower Management Center (FMC) met certificaatverificatie.

Bijgedragen door Dolly Jain en Rishabh Aggarwal, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Handmatige inschrijving van certificaten en basisgegevens van SSL VCC
- Basiskennis van verificatie voor externe toegang via VPN
- Certificaat Autoriteit van derden (CA) zoals Entrust, Geotrust, GoDaddy, Thawte en VeriSign

Gebruikte componenten

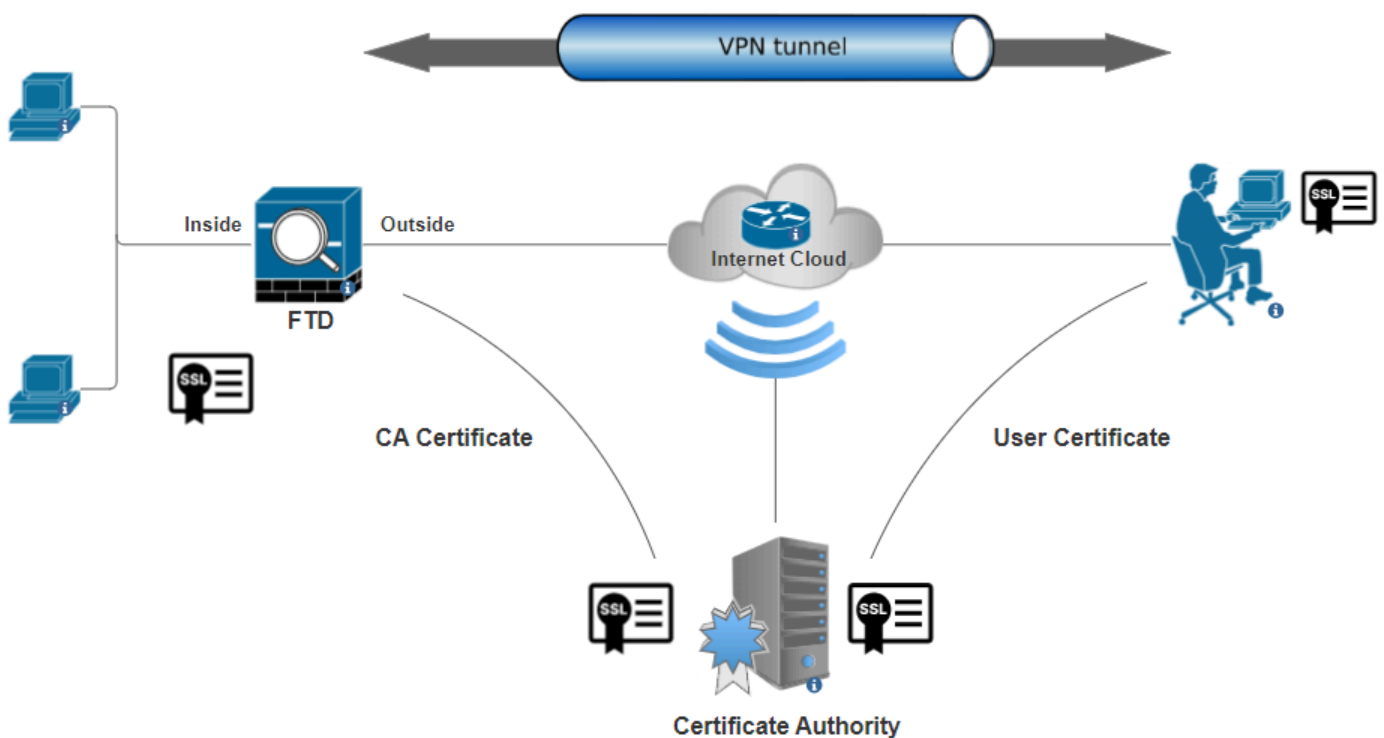
De informatie in dit document is gebaseerd op de volgende softwareversies:

- Secure Firepower Threat Defense versie 7.4.1
- Firepower Management Center (FMC) versie 7.4.1
- Secure Client versie 5.0.05040
- Microsoft Windows Server 2019 als CA-server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdigram



Netwerkdigram

Configuraties

- a. Een certificaat maken/importeren dat wordt gebruikt voor serververificatie



Opmerking: op VCC is een CA-certificaat nodig voordat u de CSR kunt genereren. Als MVO wordt gegenereerd vanuit een externe bron (OpenSSL of een derde partij), mislukt de handmatige methode en moet het PKCS12-certificaatformaat worden gebruikt.

Stap 1. Navigeer naar Devices > Certificaten klik op Add. Selecteer Apparaat en klik op plusteken (+) onder Volledige inschrijving.

Add New Certificate



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

Device*:

Cert Enrollment*:

Cancel

Add

Registratie toevoegen

Stap 2. Selecteer onder het CA Information de optie Inschrijftype als Manual en plak het certificaat van de certificeringsinstantie (CA) dat wordt gebruikt om de CSR te ondertekenen.

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

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

CA Certificate:

```
HQYDVQQDEZXIEWRyYw50S
UQgU2VydMvYlENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID-7...
```

Validation Usage:

IPsec Client SSL Client SSL Server

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

Cancel

Save

CA-informatie toevoegen

Step 3. Selecteer IPsec Client, SSL Client en Skip Check for CA flag in basic constraints of the CA Certificate voor validatiegebruik.

Step 4. Vul onder Certificate Parameters dit punt de onderwerpnaam in.

Add Cert Enrollment



Name*

ssl_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

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):

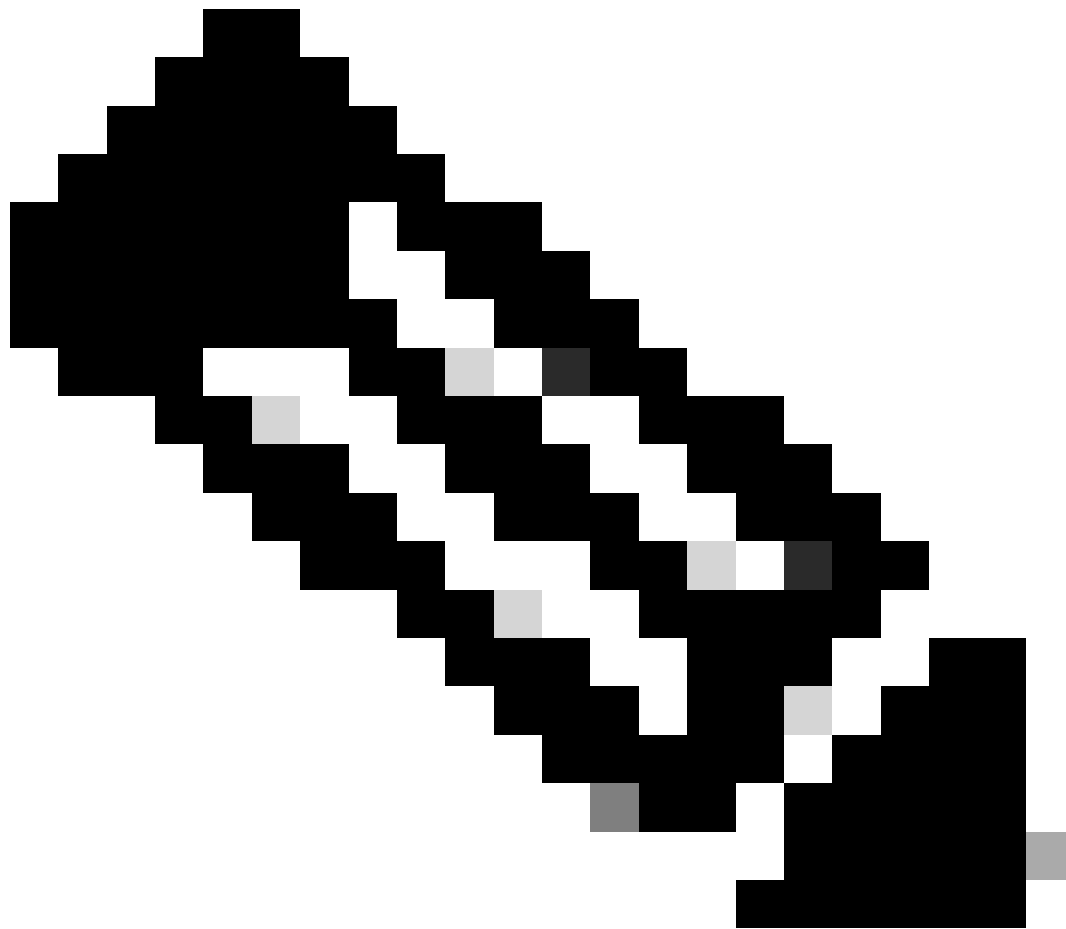
Include Device's Serial Number

Cancel

Save

Certificaatparameters toevoegen

Stap 5. Selecteer onder Keyhet sleuteltype RSA met een toetsnaam en -grootte. Klik op Save.



Opmerking: voor RSA-sleuteltype is de minimale sleutelgrootte 2048 bits.

Add Cert Enrollment



Name*
ssl_certificate

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:
 RSA ECDSA EdDSA

Key Name:*
rsakey

Key Size:
2048 ▼

▼ Advanced Settings

Ignore IPsec Key Usage

Cancel **Save**

RSA-toets toevoegen

Stap 6. Selecteer onder Cert Enrollment het vertrouwenspunt uit de vervolgkeuzelijst die zojuist is gemaakt en klik op 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*:

Cert Enrollment*:

 +

Cert Enrollment Details:

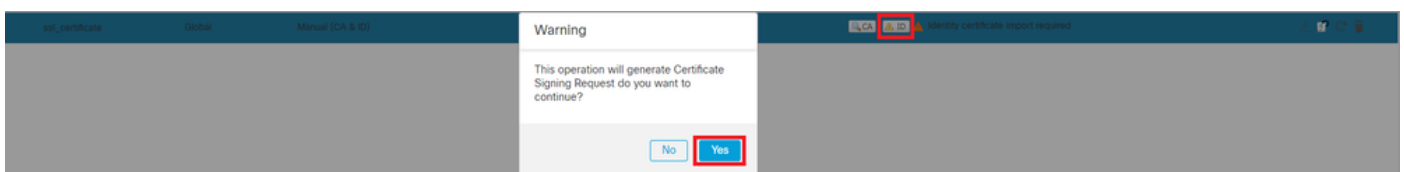
Name: ssl_certificate
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Cancel

Add

Nieuw certificaat toevoegen

Stap 7. Klik op ID en klik op Yes op verdere prompt om de MVO te genereren.



MVO genereren

Stap 8. Kopieer de MVO en laat deze ondertekenen door de Certificaatinstantie. Zodra het Identiteitscertificaat door CA is afgegeven, importeert u het door op te klikken Browse Identity Certificate en vervolgens te klikken 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-----  
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG  
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMakGA1UEBhMC  
SU4wgglIIMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK  
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO  
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1pLEdR4X6ZlnM5fNA/GLV9MnPoP  
ppzi0uLlbVmb5iKQexllaur/e3PDee3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

Step 2

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

Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

[Import](#)



Opmerking: als de uitgifte van het ID-certificaat tijd in beslag neemt, kunt u stap 7 later herhalen. Dit zal hetzelfde MVO genereren en we kunnen het ID-certificaat importeren.

b. Een betrouwbaar/intern CA-certificaat toevoegen



Opmerking: Als de certificeringsinstantie (CA) gebruikt in stap a), "**Maak/importeer een certificaat dat gebruikt wordt voor serververificatie**" ook gebruikerscertificaten afgeeft, kunt u **stap b)**, "**Voeg een betrouwbaar/intern CA-certificaat toe**". Het is niet nodig om hetzelfde CA certificaat opnieuw toe te voegen en het moet ook worden vermeden. Als hetzelfde CA-certificaat opnieuw wordt toegevoegd, is trustpoint geconfigureerd met "validatie-gebruik geen" wat invloed kan hebben op de certificaatverificatie voor RAVPN.

Stap 1. Navigeer naar Devices > Certificates en klik op Add.

Selecteer Apparaat en klik op plusteken (+) onder Volledige inschrijving.

Hier wordt "auth-risaggar-ca" gebruikt om identiteits-/gebruikerscertificaten af te geven.

General

Details

Certification Path



Certificate Information

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

- All issuance policies
- All application policies

Issued to: auth-risaggar-ca

Issued by: auth-risaggar-ca

Valid from 04-03-2023 **to** 04-03-2033

Issuer Statement

OK

auth-risaggar-ca

Stap 2. Voer een trustpoint naam in en selecteer Manual als het inschrijvingstype onder CA information.

Stap 3. Controleer CA Onlyen plak het vertrouwde/interne CA-certificaat in pem-indeling.

Stap 4. Controleer **Skip Check for CA flag in basic constraints of the CA Certificate** en klik op Save.

Add Cert Enrollment ?

Internal_CA

Description

CA Information | Certificate Parameters | Key | Revocation

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  
VHJ1c3QgQ29tbWV5Y2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage: IPsec Client SSL Client SSL Server

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

Cancel Save

Trustpoint toevoegen

Stap 5. Onder Cert Enrollment, selecteer het trustpoint van dropdown die net werd gecreëerd en klik 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*:

Cert Enrollment*:

 +

Cert Enrollment Details:

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

Cancel

Add

Interne CA toevoegen

Stap 6. Het eerder toegevoegde certificaat wordt weergegeven als:

Internal_CA	Global	Manual (CA Only)	Mar 4, 2033	CA ID	⌵ ⌵ ⌵ ⌵
-------------	--------	------------------	-------------	-------	---------

Toegevoegd certificaat

c. Adresgroep voor VPN-gebruikers configureren

Stap 1. Navigeer naar Objects > Object Management > Address Pools > IPv4 Pools .

Stap 2. Voer de naam en het IPv4-adresbereik in met een masker.

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

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

► Override (0)

Cancel

Save

IPv4-pool toevoegen

d. Beveiligde clientafbeeldingen uploaden

Stap 1. Download webimplementeer beveiligde client-afbeeldingen volgens het besturingssysteem van de [Cisco](#)-softwaresite.

Stap 2. Navigeer naar Objects > Object Management > VPN > Secure Client File > Add Secure Client File .

Stap 3. Voer de naam in en selecteer het bestand Secure Client (Beveiligde client) op de schijf.

Stap 4. Selecteer het bestandstype als Secure Client Image en klik op Save.

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

Een beveiligde clientafbeelding toevoegen

e. XML-profiel maken en uploaden

Stap 1. Download en installeer de Secure Client Profile Editor vanaf de [Cisco-software](#)site.

Stap 2. Maak een nieuw profiel en selecteer All uit de vervolgkeuzelijst Clientcertificaat. Het regelt voornamelijk welke certificaatopslag(en) Secure Client kan gebruiken om certificaten op te slaan en te lezen.

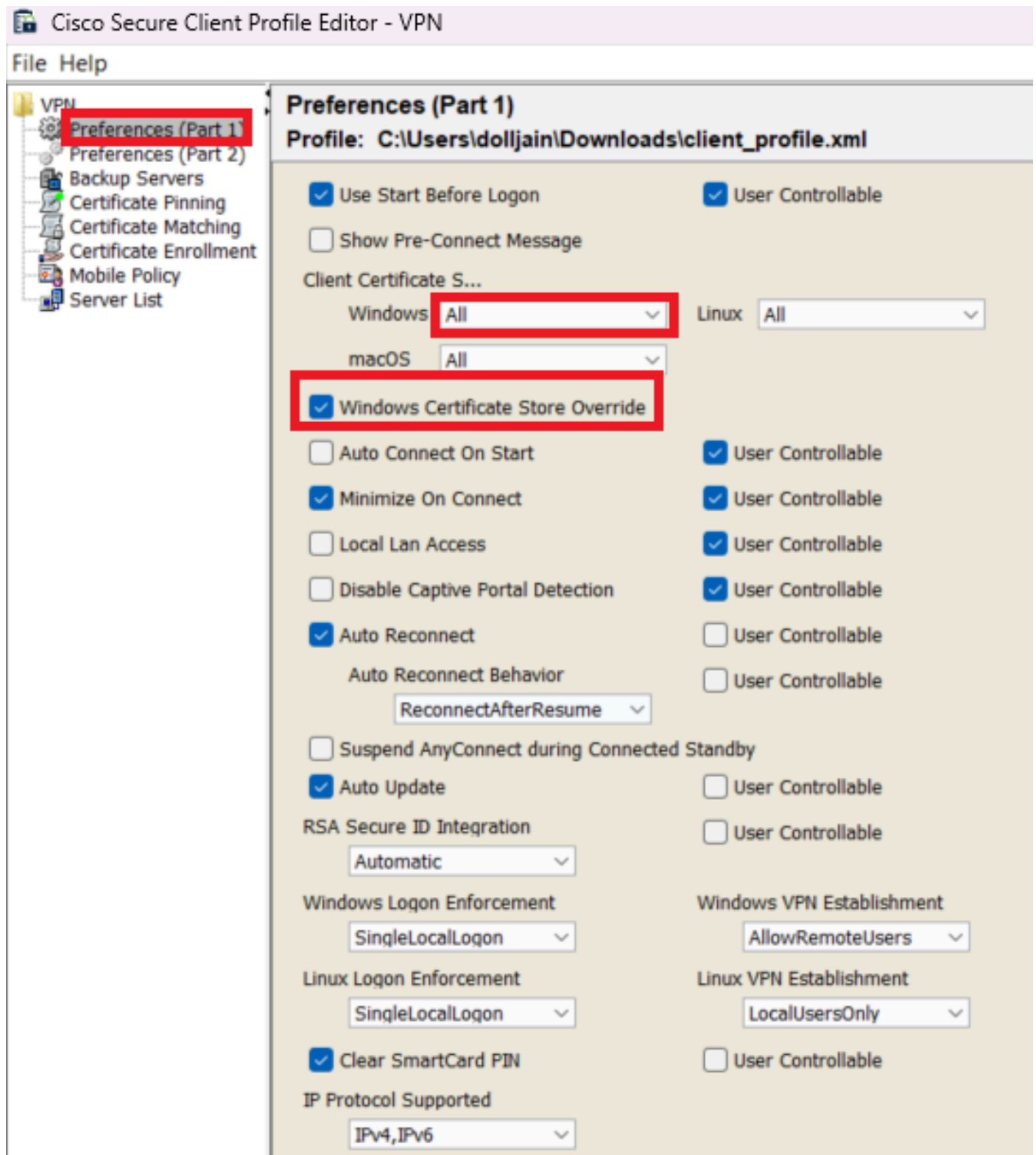
Twee andere beschikbare opties zijn:

- **Machine** - Secure Client is beperkt tot het opzoeken van certificaten in het lokale Windows-certificaatarchief.
- **Gebruiker** - Secure Client is beperkt tot het opzoeken van certificaten in het lokale Windows-gebruikerscertificaatarchief.

certificaatarchief instellen op True .

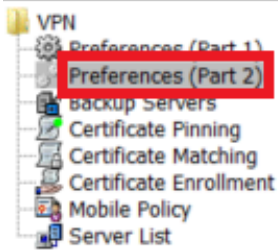
Hiermee kan een beheerder beveiligde client opdracht geven om certificaten te gebruiken in het certificeringsarchief van het Windows-systeem

(lokaal systeem) voor de verificatie van clientcertificaten. Certificate Store Override is alleen van toepassing op SSL, waar de verbinding standaard wordt geïnitieerd door het UI-proces. Wanneer u IPSec/IKEv2 gebruikt, is deze voorziening in het beveiligde clientprofiel niet van toepassing.



Voorkeuren toevoegen (Deel 1)

Stap 3. (Optioneel) Schakel de optie uit omdat de gebruiker niet wordt gevraagd het Disable Automatic Certificate Selection verificatiecertificaat te selecteren.



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

Server List Entry voor het instellen van een profiel in Secure Client VPN door groep-alias en groep-url te bieden onder de Serverlijst en sla het XML-profiel op.

The screenshot shows the Cisco Secure Client Profile Editor - VPN interface. The left sidebar contains a tree view with 'Server List' selected. The main window displays the 'Server List' configuration for a profile named 'C:\Users\dolljain\Downloads\client_profile.xml'. A table lists the server entries, with the first entry 'SSL-VPN' highlighted in red. Below the table, a note states: 'Note: it is highly recommended that at least one server be defined in a profile.' Buttons for 'Add...', 'Delete', 'Edit...', and 'Details' are visible.

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

Server List Entry dialog box details:

- Primary Server: Display Name (required) is 'SSL-VPN'.
- FQDN or IP Address: 'https://certauth.cisco.com'.
- User Group: 'ssl-cert'.
- Group URL: (empty field).
- Connection Information: Primary Protocol is 'SSL'.
- Auth Method During IKE Negotiation: 'EAP-AnyConnect'.
- IKE Identity (IOS gateway only): (empty field).
- Backup Servers: (empty list with 'Add', 'Move Up', 'Move Down', 'Delete' buttons).

Serverlijst toevoegen

Stap 5. Tot slot is het XML profiel klaar voor gebruik.

```

<?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>
    <CertificateStoreAll>All</CertificateStoreAll>
    <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>
    <RSA SecurID Integration UserControllable="false">Automatic</RSA SecurID Integration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVFNEstablishment>AllowRemoteUsers</WindowsVFNEstablishment>
    <LinuxVFNEstablishment>LocalUsersOnly</LinuxVFNEstablishment>
    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
    <PFPEExclusion UserControllable="false">Disable
      <PFPEExclusionServerIP UserControllable="false"></PFPEExclusionServerIP>
    </PFPEExclusion>
    <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-profiel

Locatie van XML profielen voor verschillende besturingssystemen:

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

Stap 6. Navigeer naar Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile .

Voer de naam voor het bestand in en klik op Browse om het XML-profiel te selecteren. Klik op de knop .Save

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

VPN-profiel voor beveiligde client toevoegen

Configuratie van VPN voor externe toegang

Stap 1. Maak een ACL per vereiste om toegang tot interne bronnen te verlenen.

Navigeer naar Objects > Object Management > Access List > Standard en klik op Add Standard Access List.

Edit Standard Access List Object



Name

Split_ACL

▼ Entries (1)

Add

Sequence No	Action	Network	
1	Allow	split_acl	

Allow Overrides

Cancel

Save

Standaard ACL toevoegen



Opmerking: deze ACL wordt gebruikt door beveiligde client om beveiligde routes aan interne bronnen toe te voegen.

Stap 2. Navigeer naar `Devices > VPN > Remote Access` en klik op `Add`.

Stap 3. Typ de naam van het profiel, selecteer vervolgens het FTD-apparaat en klik op `Volgende`.

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	Selected Devices
<input type="text" value="Q Search"/>	FTD-A-7.4.1
FTD-A-7.4.1	
FTD-B-7.4.0	
FTD-ZTNA-7.4.1	
<input type="button" value="Add"/>	

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.

Profielnaam toevoegen

Stap 4. Voer de gegevens in Connection Profile Name en selecteer de verificatiemethode zoals Client Certificate Only onder Verificatie, autorisatie en 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

i 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)

Selecteer een verificatiemethode

Stap 5. Klik op Use IP Address Pools onder Toewijzing clientadres en selecteer de IPv4-adresgroep die eerder is gemaakt.


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: 

Selecteer Toewijzing van clientadres

Stap 6. Bewerk het groepsbeleid.

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:* ▼ +

[Edit Group Policy](#)

Groepsbeleid bewerken

Stap 7. Navigeer naar General > Split Tunneling , selecteer Tunnel networks specified below en selecteer Standard Access List onder Netwerkljsttype splitter tunnel.

Selecteer de ACL die eerder is gemaakt.

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

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:

Cancel

Save

Split-tunneling toevoegen

Stap 8. Navigeer naar Secure Client > Profile , selecteer de Client Profile en klik Save.

Edit Group Policy



Name:*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

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](#).

Beveiligd clientprofiel toevoegen

Stap 9. Klik op Next, selecteer vervolgens de knop Secure Client Image en klik op 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](#).

Show Re-order buttons +

<input type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyconnectWin-5.0.05040	cisco-secure-client-win-5.0.05040-webde...	Windows


Een beveiligde clientafbeelding toevoegen

Stap 10. Selecteer de Netwerkinterface voor VPN-toegang, kies de Device Certificates en controleer sysopt license-vpn en klik op 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:* +
 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:* +
 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 voor VPN-verkeer

Stap 11. Controleer tot slot alle configuraties en klik op 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.

Configuratie van VPN-beleid voor externe toegang

Stap 12. Nadat de eerste configuratie van Remote Access VPN is voltooid, bewerk je het verbindingsprofiel dat is gemaakt en ga je naar Aliases.

Stap 13. Configureer group-alias door op het plus-pictogram (+) te klikken.

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth


Group Policy:* DfltGrpPolicy +

[Edit Group Policy](#)

Client Address Assignment AAA **Aliases**

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 following URLs, system

URL

Edit Alias Name

Alias Name:

 Enabled

Cancel OK

Cancel Save

Groepsalias bewerken

Stap 14. Configureer group-url door op het plus-pictogram (+) te klikken. Gebruik dezelfde URL voor groep die eerder in het clientprofiel is geconfigureerd.

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 turned on or off.

Edit URL Alias

URL Alias:

certauth

Enabled

[Cancel](#) [OK](#)

URL Alias:

Configure the list of URL Aliases for this connection profile. 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](#)

URL voor groep bewerken

Stap 15. Navigeren naar toegangsiinterfaces. Selecteer de Interface Trustpoint en de SSL Global Identity Certificate onder de SSL-instellingen.

RAVPN

Enter Description

Local Realm: cisco-local Policy Assignments (1) 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

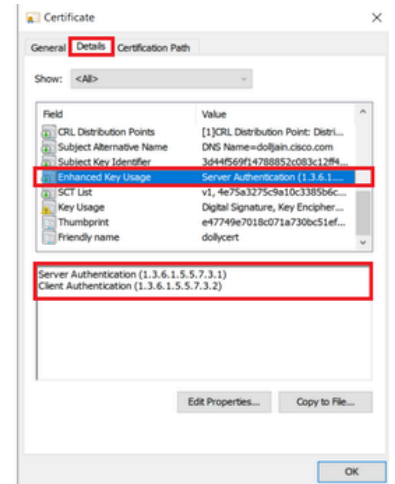
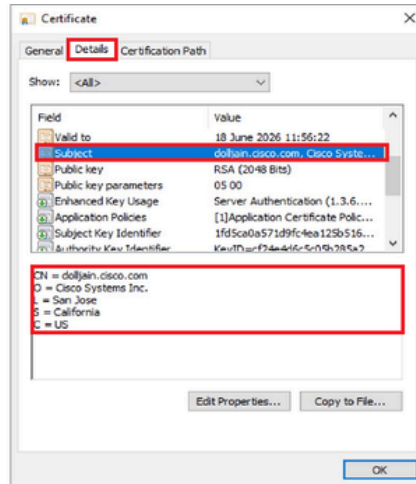
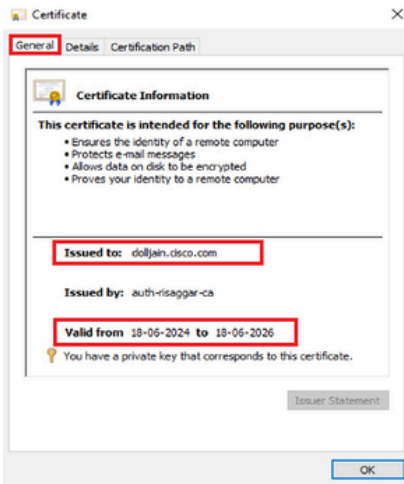
Toegangsiinterfaces bewerken

Stap 16. KlikSave en implementeer deze wijzigingen.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

1. Op de beveiligde client-pc moet het certificaat met een geldige datum, onderwerp en EKU op de pc van de gebruiker zijn geïnstalleerd. Dit certificaat moet worden afgegeven door de bevoegde instantie waarvan het certificaat op het FTD is geïnstalleerd, zoals eerder is aangegeven. Hier wordt het identiteits- of gebruikerscertificaat afgegeven door "auth-risaggar-ca".

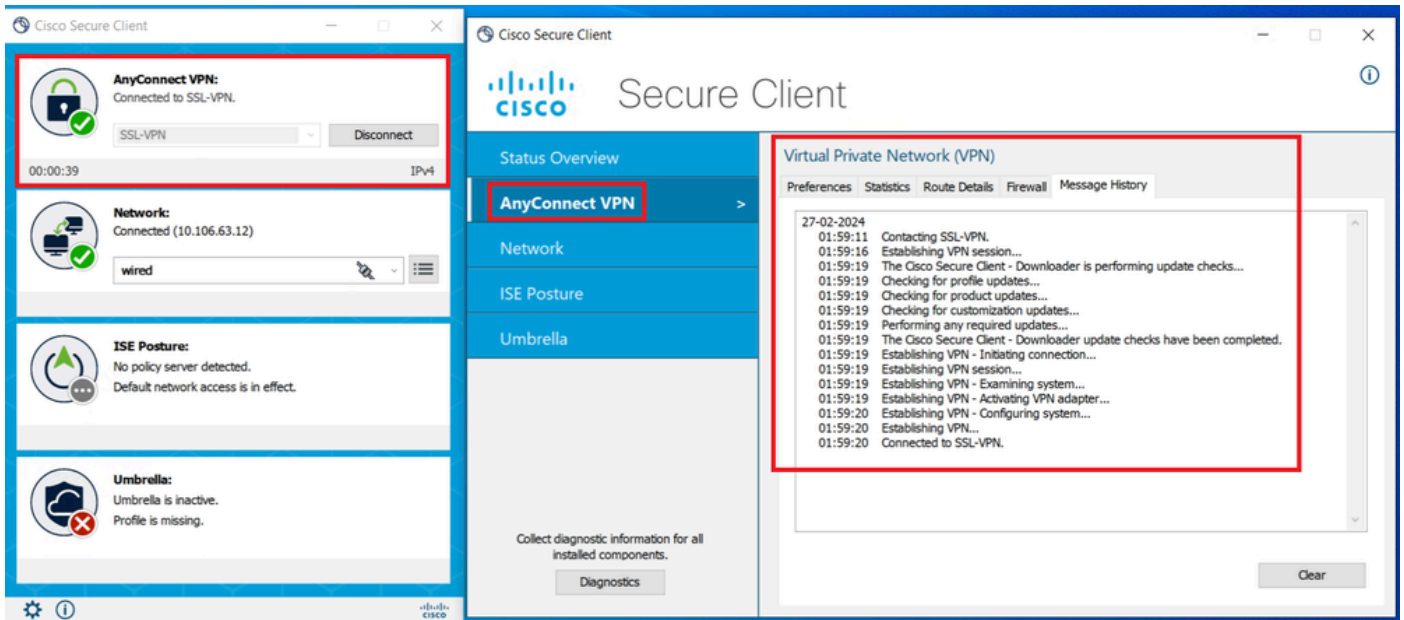


Kenmerken certificaat



Opmerking: voor het clientcertificaat moet de ECU (Enhanced Key Usage) voor clientverificatie zijn ingevoerd.

2. Secure Client moet de verbinding tot stand brengen.



Succesvolle beveiligde clientverbinding

3. Uitvoeren show vpn-sessiondb anyconnect om de verbindinggegevens van de actieve gebruiker in de gebruikte tunnelgroep te bevestigen.

```
firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dolljain.cisco.com Index :
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

1. Debugs kunnen worden uitgevoerd vanaf de diagnostische CLI van de FTD:

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

2. Raadpleeg deze [handleiding](#) voor algemene problemen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.