

Configurer l'authentification de certificat client sécurisé sur FTD géré par FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[a. Créer/importer un certificat utilisé pour l'authentification du serveur](#)

[b. Ajouter un certificat CA approuvé/interne](#)

[c. Configurer le pool d'adresses pour les utilisateurs VPN](#)

[d. Télécharger des images client sécurisées](#)

[e. Créer et télécharger un profil XML](#)

[Configuration VPN d'accès à distance](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit le processus de configuration du VPN d'accès à distance sur Firepower Threat Defense (FTD) géré par Firepower Management Center (FMC) avec l'authentification de certificat.

Contribution de Dolly Jain et Rishabh Aggarwal, Ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Inscription manuelle des certificats et notions de base de SSL
- FMC
- Connaissances de base en authentification pour VPN d'accès à distance
- Autorité de certification (AC) tierce comme Entrust, Geotrust, GoDaddy, Thawte et VeriSign

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Défense contre les menaces Secure Firepower version 7.4.1
- Firepower Management Center (FMC) version 7.4.1
- Client sécurisé version 5.0.05040
- Microsoft Windows Server 2019 en tant que serveur AC

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau

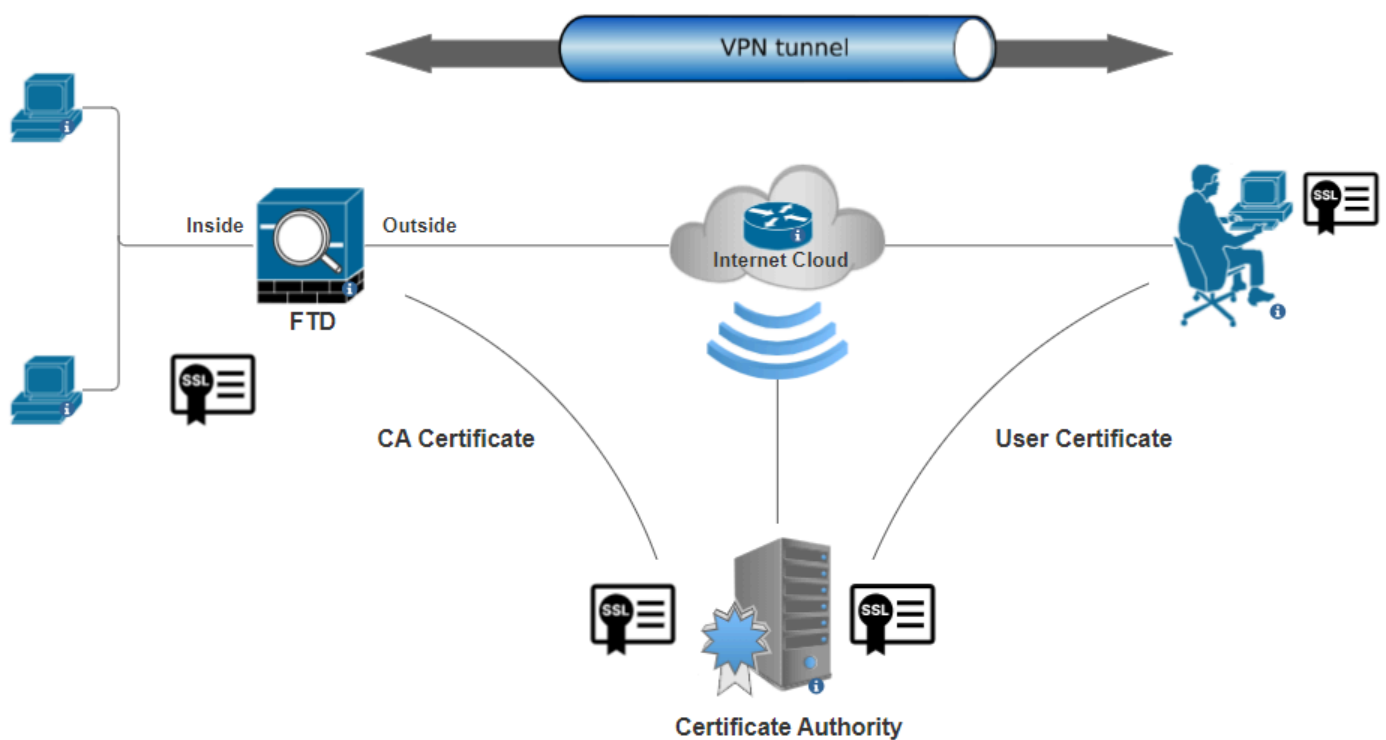
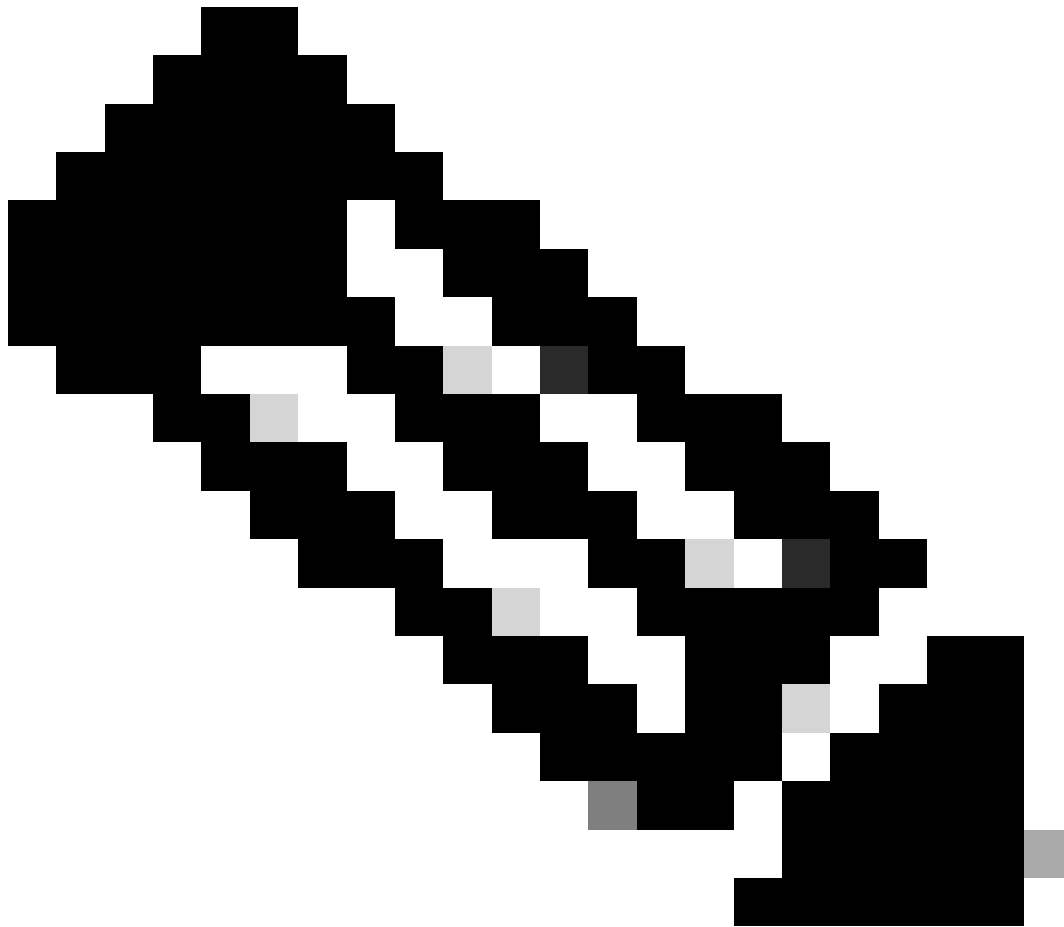


Diagramme du réseau

Configurations

- a. Créer/importer un certificat utilisé pour l'authentification du serveur



Remarque : sur FMC, un certificat CA est nécessaire avant de pouvoir générer le CSR. Si CSR est généré à partir d'une source externe (OpenSSL ou tierce partie), la méthode manuelle échoue et le format de certificat PKCS12 doit être utilisé.

Étape 1. Accédez à `Devices > Certificates` et cliquez sur `Add`. Sélectionnez `Périphérique` et cliquez sur le signe plus (+) sous `Inscription au certificat`.

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

Ajouter une inscription de certificat

Étape 2. Sous l'CA Information, sélectionnez le type d'inscription comme Manual et collez le certificat d'autorité de certification (CA) utilisé pour signer le CSR.

Add Cert Enrollment ?

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

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

CA Certificate:

```
HQYDVQQDEZXIEWRYRW50S
UQgU2VydMvYlENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID=Z...
```

Validation Usage: IPsec Client SSL Client SSL Server
 Skip Check for CA flag in basic constraints of the CA Certificate

Ajouter des informations CA

Étape 3. Pour Utilisation de la validation, sélectionnez IPsec Client, SSL Client et Skip Check for CA flag in basic constraints of the CA Certificate.

Étape 4. SousCertificate Parameters, renseignez les détails du nom de l'objet.

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):

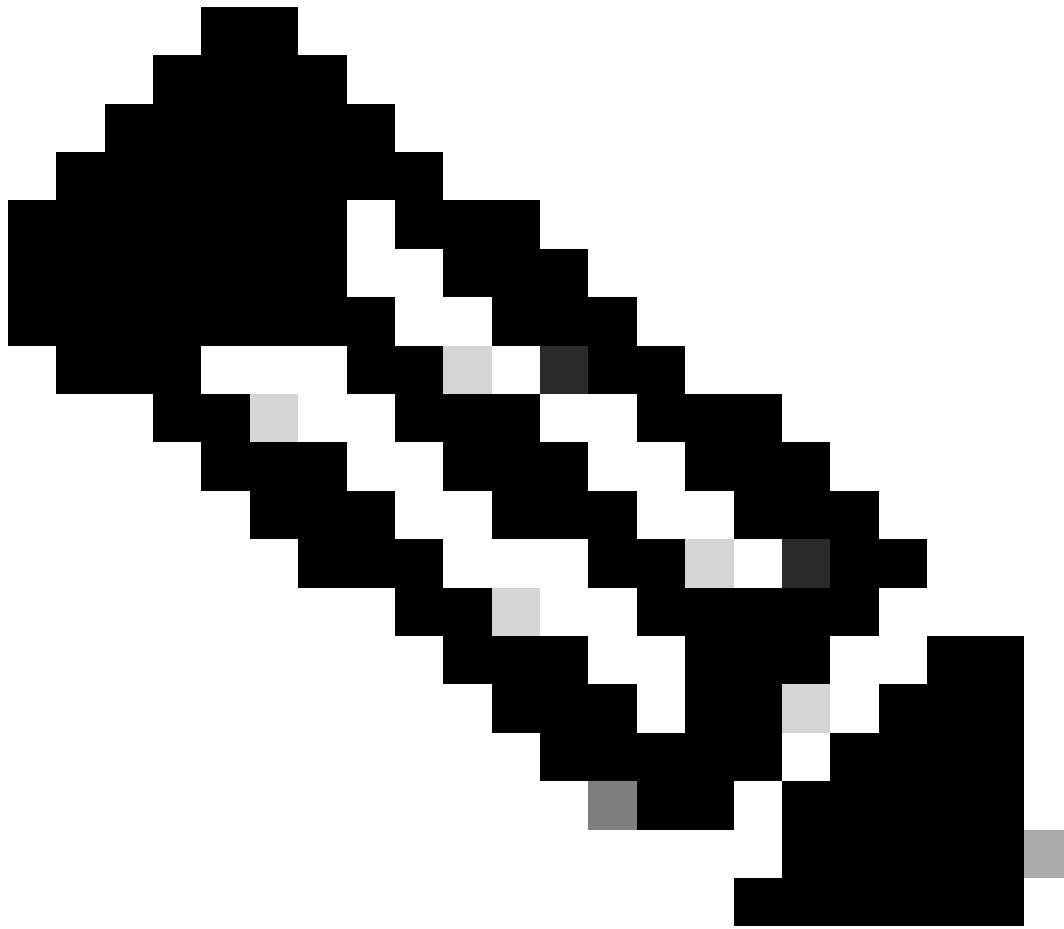
Include Device's Serial Number

Cancel

Save

Ajouter des paramètres de certificat

Étape 5. Sous Keysélectionnez le type de clé RSA avec un nom et une taille de clé. Cliquez sur Save.



Remarque : pour le type de clé RSA, la taille de clé minimale est de 2 048 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

Ajouter une clé RSA

Étape 6. SousCert Enrollment, sélectionnez le point de confiance dans la liste déroulante qui vient d'être créé et cliquez sur 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:

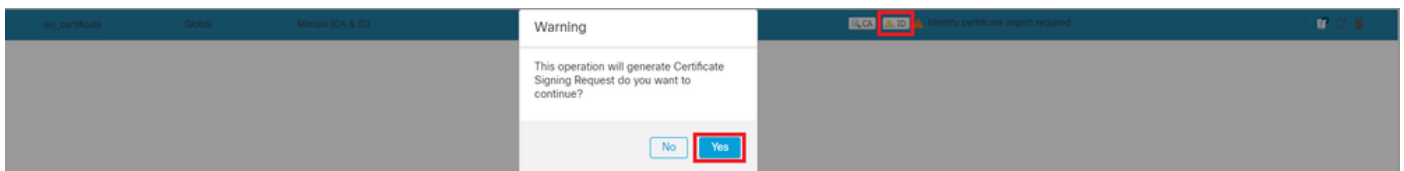
Name: ssl_certificate
Enrollment Type: Manual (CA & ID)
Enrollment URL: N/A

Cancel

Add

Ajouter un nouveau certificat

Étape 7. Cliquez sur ID, puis sur Yes une autre invite pour générer le CSR.



Générer CSR

Étape 8. Copiez le CSR et faites-le signer par l'autorité de certification. Une fois le certificat d'identité émis par l'autorité de certification, importez-le en cliquant sur Browse Identity Certificate et cliquez sur 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/e3PDeee3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

Step 2

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

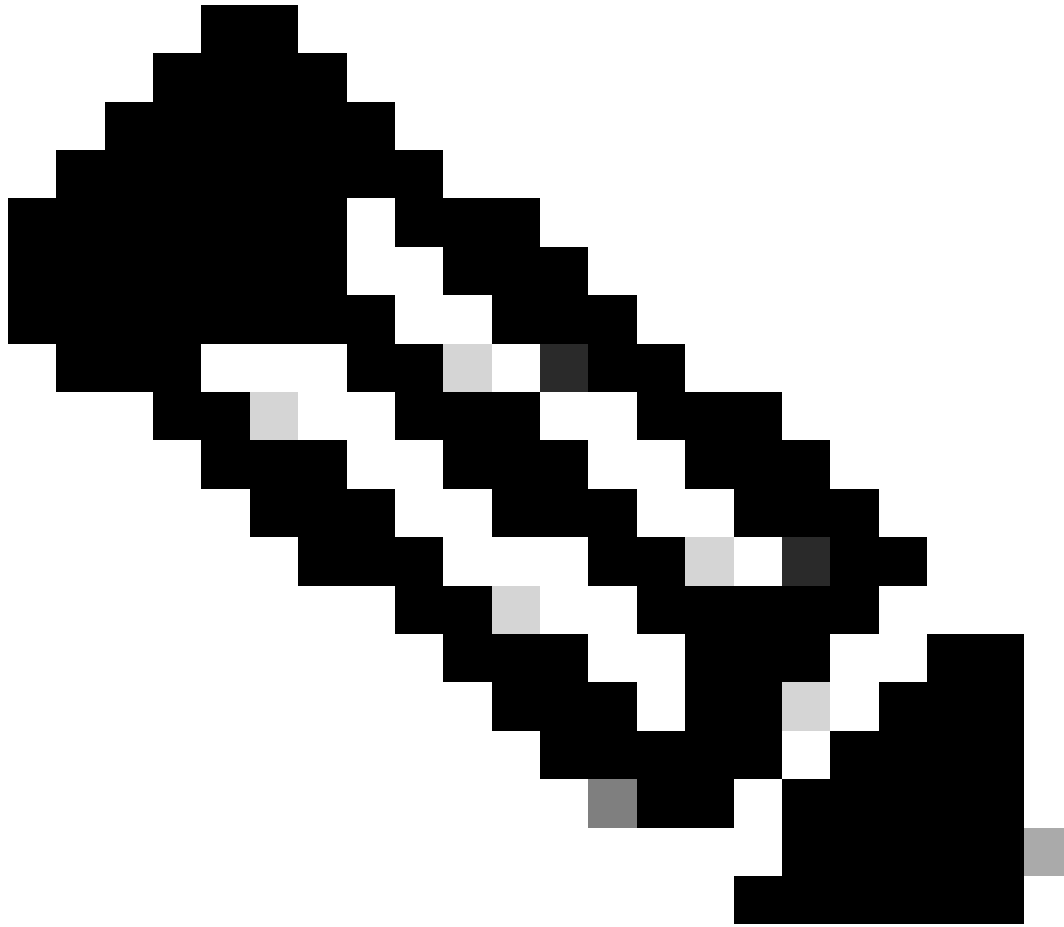
Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

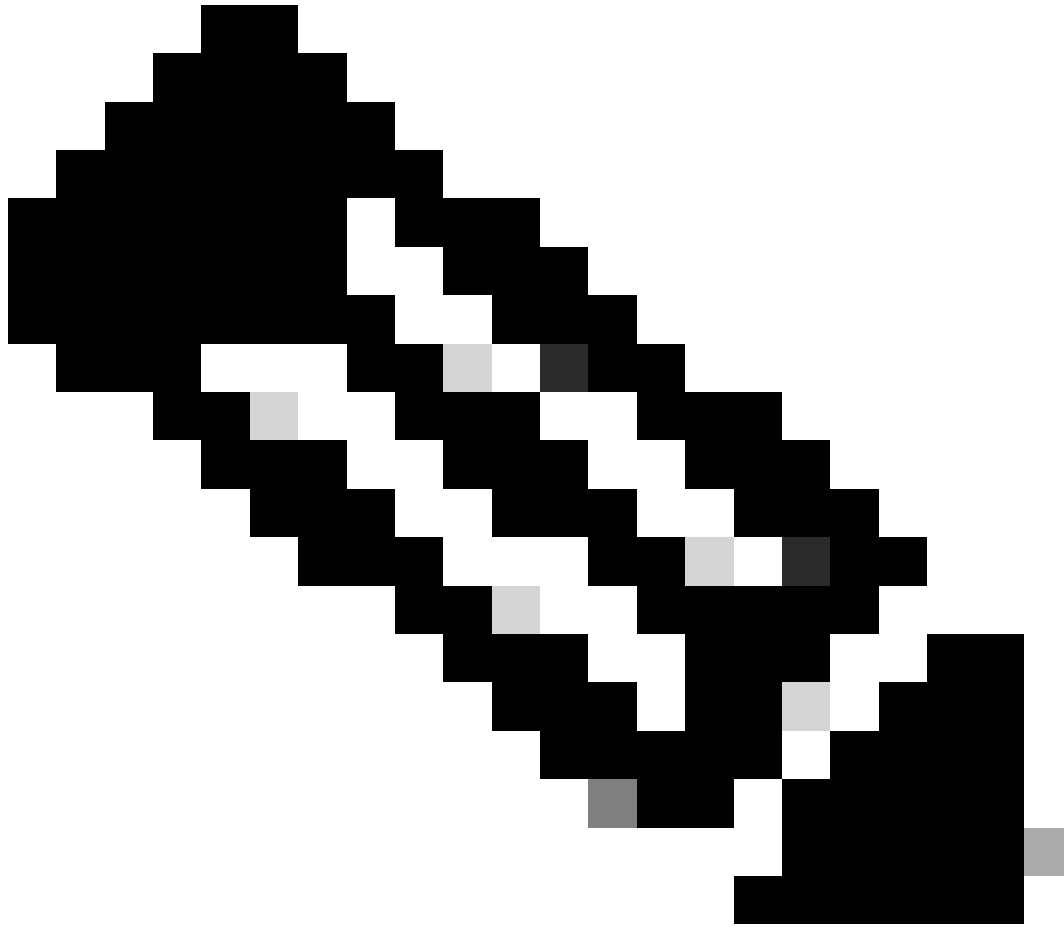
[Import](#)

Importer le certificat ID



Remarque : si l'émission du certificat d'ID prend du temps, vous pouvez répéter l'étape 7 ultérieurement. Cela générera le même CSR et nous pourrons importer le certificat d'ID.

b. Ajouter un certificat CA approuvé/interne



Remarque : si l'autorité de certification utilisée à l'étape (a), « **Créer/importer un certificat utilisé pour l'authentification du serveur** » émet également des certificats utilisateur, vous pouvez ignorer l'étape (b), « **Ajouter un certificat CA approuvé/interne** ». Il n'est pas nécessaire d'ajouter à nouveau le même certificat d'autorité de certification et il doit également être évité. Si le même certificat CA est ajouté à nouveau, trustpoint est configuré avec « validation-usage none », ce qui peut avoir un impact sur l'authentification de certificat pour RAVPN.

Étape 1. Accédez à Devices > Certificates et cliquez sur Add.

Sélectionnez Périphérique et cliquez sur le signe plus (+) sous Inscription au certificat.

Ici, « auth-risaggar-ca » est utilisé pour émettre des certificats d'identité/d'utilisateur.

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

Étape 2. Entrez un nom de point de confiance et sélectionnez Manual comme type d'inscription sous CA information.

Étape 3. Vérifiez CA Only et collez le certificat CA approuvé/interne au format pem.

Étape 4. Cochez **Skip Check for CA flag in basic constraints of the CA Certificate** et cliquez sur Save.

Add Cert Enrollment ?

Internal_CA

Description

CA InformationCertificate ParametersKeyRevocation

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  
N0MScwJQYDVQQDEw5JZGV  
u  
VHJ1c3QgQ29tbWV5Y2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage: IPsec Client SSL Client SSL Server

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

CancelSave

Ajouter un point de confiance

Étape 5. Sous Cert Enrollment, sélectionnez le point de confiance dans la liste déroulante qui vient d'être créée et cliquez sur 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

Ajouter une autorité de certification interne

Étape 6. Le certificat ajouté précédemment s'affiche comme suit :

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

Certificat ajouté

c. Configurer le pool d'adresses pour les utilisateurs VPN

Étape 1. Accédez à Objects > Object Management > Address Pools > IPv4 Pools .

Étape 2. Entrez le nom et la plage d'adresses IPv4 avec un masque.

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

Ajouter un pool IPv4

d. Télécharger des images client sécurisées

Étape 1. Téléchargez des images client sécurisées WebDéploiement conformément au système d'exploitation à partir du site [Cisco Software](#).

Étape 2. Accédez à Objects > Object Management > VPN > Secure Client File > Add Secure Client File .

Étape 3. Entrez le nom et sélectionnez le fichier Secure Client sur le disque.

Étape 4. Sélectionnez le type de fichier comme Secure Client Image et cliquez sur Save.

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

Ajouter une image de client sécurisé

e. Créer et télécharger un profil XML

Étape 1. Téléchargez et installez le client sécurisé Profile Editor à partir du site [Cisco Software](#).

Étape 2. Créez un nouveau profil et sélectionnez-leAll dans la liste déroulante Sélection de certificat client. Il contrôle principalement quel(s) magasin(s) de certificats Secure Client peut utiliser pour stocker et lire des certificats.

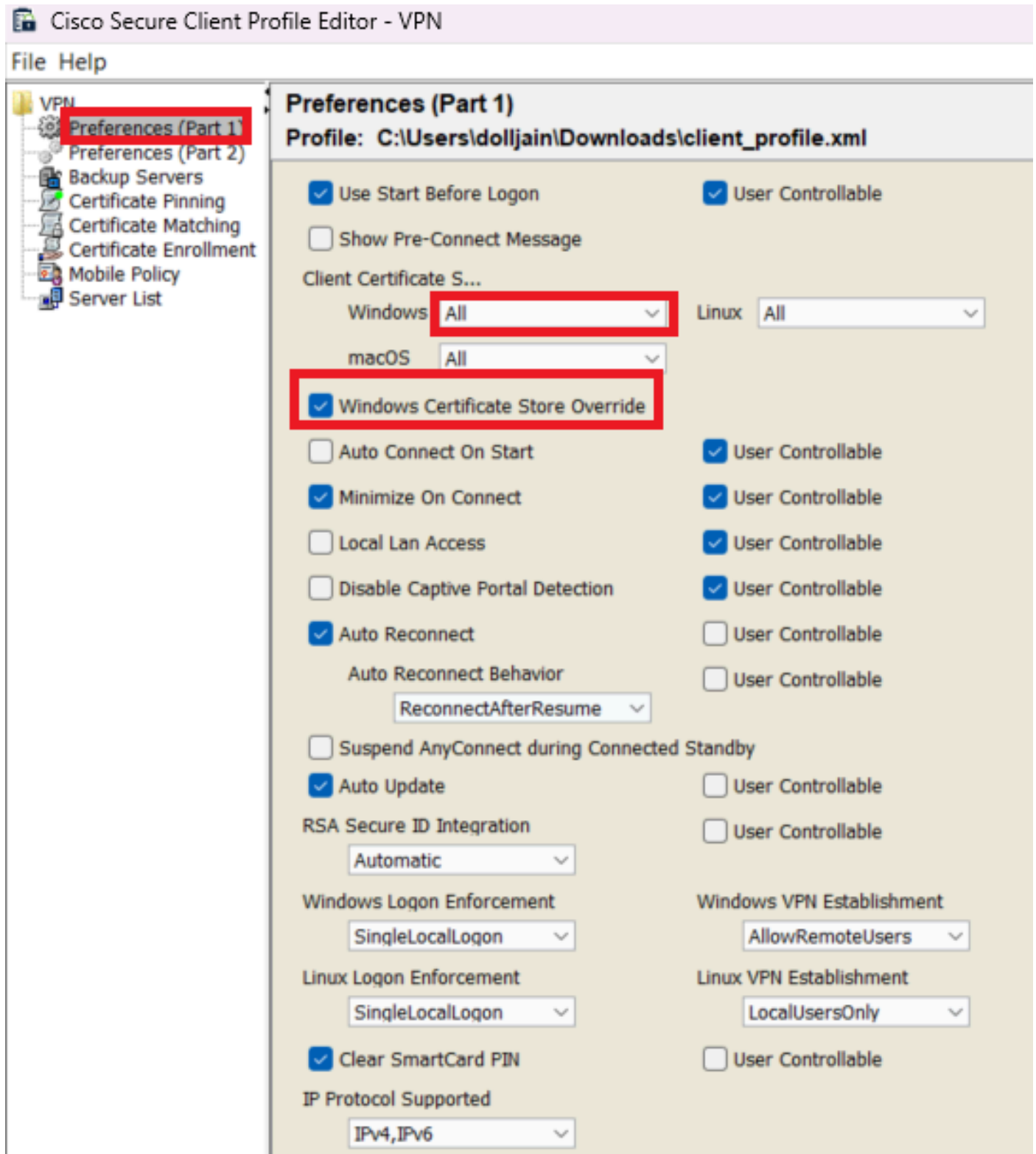
Deux autres options sont disponibles :

- **Ordinateur** - Le client sécurisé est limité à la recherche de certificats sur le magasin de certificats de l'ordinateur local Windows.
- **Utilisateur** - Le client sécurisé est limité à la recherche de certificats sur le magasin de certificats d'utilisateur Windows local.

Définir le remplacement du magasin de certificats comme True .

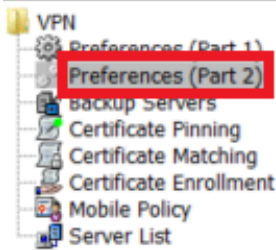
Cela permet à un administrateur d'indiquer au client sécurisé d'utiliser les certificats dans le magasin de certificats de l'ordinateur Windows

(système local) pour l'authentification du certificat client. Le remplacement du magasin de certificats s'applique uniquement à SSL, où la connexion est initiée, par défaut, par le processus de l'interface utilisateur. Lorsque vous utilisez IPSec/IKEv2, cette fonctionnalité du profil client sécurisé n'est pas applicable.



Ajouter des préférences (Partie 1)

Étape 3. (Facultatif) Désactivez la case à cocher Disable Automatic Certificate Selection, car l'utilisateur n'est pas invité à sélectionner le certificat d'authentification.



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)

Performance Improvement Threshold (%)

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.)

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)

Server List Entry pour configurer un profil dans Secure Client VPN en fournissant group-alias et group-url sous la Liste des serveurs et enregistrez le profil XML.

The screenshot shows the Cisco Secure Client Profile Editor - VPN interface. 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 highlighted in red:

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

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.

The 'Server List Entry' dialog box is open, showing the configuration for the selected server. The 'Primary Server' section includes:

- Display Name (required): SSL-VPN
- FQDN or IP Address: https://certauth.cisco.com
- User Group: ssl-cert
- Group URL: (empty field)

The 'Connection Information' section includes:

- Primary Protocol: SSL
- ASA gateway: (unchecked)
- Auth Method During IKE Negotiation: EAP-AnyConnect
- IKE Identity (IOS gateway only): (empty field)

The 'Backup Servers' section includes a table for adding backup servers:

Host Address	Action
	Add
	Move Up
	Move Down
	Delete

Buttons for 'OK' and 'Cancel' are at the bottom of the dialog.

Ajouter une liste de serveurs

Étape 5. Enfin, le profil XML est prêt à être utilisé.

```

<?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 SecurIDIntegration UserControllable="false">Automatic</RSA SecurIDIntegration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVFNEstablishment>AllowRemoteUsers</WindowsVFNEstablishment>
    <LinuxVFNEstablishment>LocalUsersOnly</LinuxVFNEstablishment>
    <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>

```

Profil XML

Emplacement des profils XML pour différents systèmes d'exploitation :

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

Étape 6. Accédez à **Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile** .

Entrez le nom du fichier et cliquez sur **Browse** pour sélectionner le profil XML. Cliquez sur **Save**.

Edit Secure Client File



Name:*

File Name:*

File Type:*

Description:

Ajouter un profil VPN client sécurisé

Configuration VPN d'accès à distance

Étape 1. Créez une liste de contrôle d'accès en fonction des besoins pour autoriser l'accès aux ressources internes.

Accédez à Objects > Object Management > Access List > Standard et cliquez sur Add Standard Access List.

Edit Standard Access List Object



Name

Split_ACL

▼ Entries (1)

Add

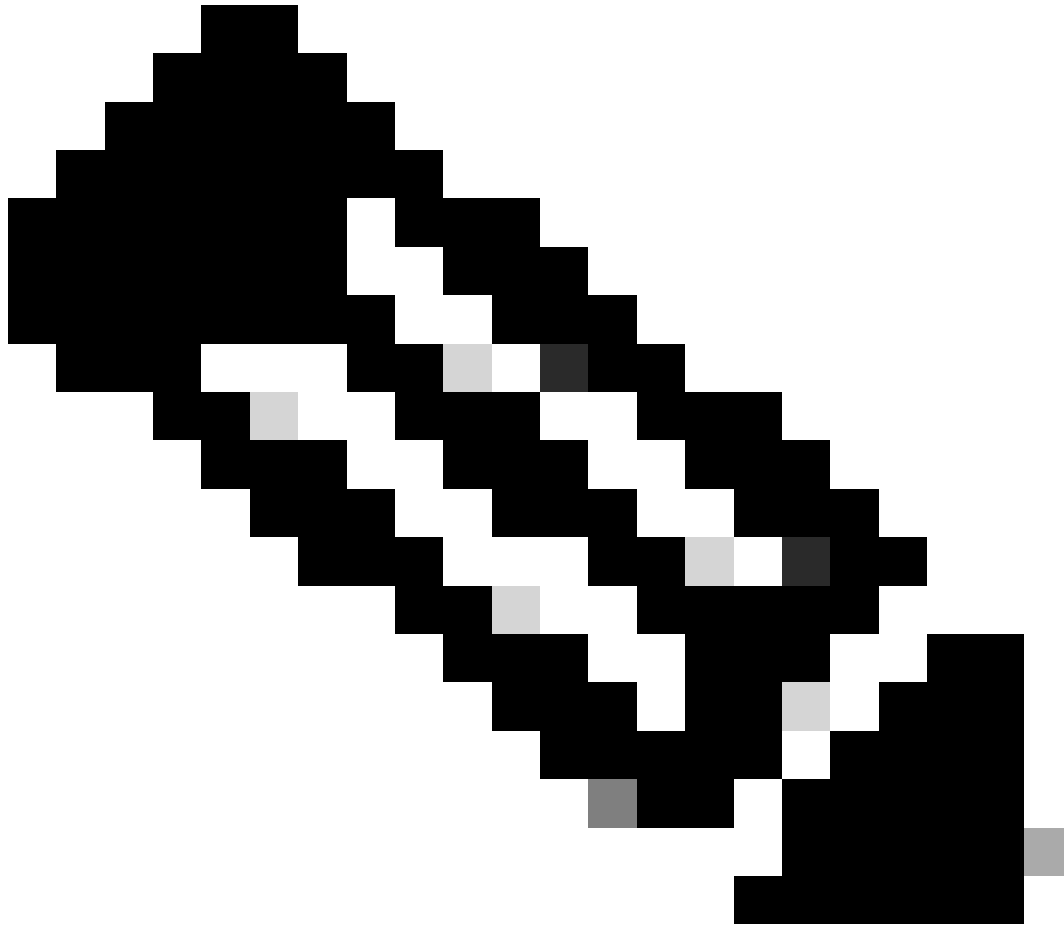
Sequence No	Action	Network	
1	Allow	split_acl	

Allow Overrides

Cancel

Save

Ajouter une ACL standard



Remarque : cette liste de contrôle d'accès est utilisée par le client sécurisé pour ajouter des routes sécurisées aux ressources internes.

Étape 2. Accédez à [Devices > VPN > Remote Access](#) et cliquez sur [Add](#).

Étape 3. Saisissez le nom du profil, puis sélectionnez le périphérique FTD et cliquez sur [Next \(Suivant\)](#).

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.

Ajouter un nom de profil

Étape 4. Saisissez le Connection Profile Name et sélectionnez la méthode d'authentification comme Client Certificate Only sous 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

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)

Sélectionner une méthode d'authentification

Étape 5. Cliquez sur Use IP Address Pools sous Client Address Assignment et sélectionnez le pool d'adresses IPv4 créé précédemment.


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: 

Sélectionner l'affectation d'adresses client

Étape 6. Modifiez la stratégie de groupe.

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](#)

Modifier la stratégie de groupe

Étape 7. Accédez à General > Split Tunneling , sélectionnez Tunnel networks specified below et sélectionnez Standard Access List sous Split Tunnel Network List Type.

Sélectionnez la liste de contrôle d'accès créée précédemment.

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

Ajouter une tunnellation partagée

Étape 8. Accédez à Secure Client > Profile , sélectionnez le Client Profile et cliquez sur 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](#).

Ajouter un profil client sécurisé

Étape 9. Cliquez sur Next, puis sélectionnez le Secure Client Image et cliquez sur 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 ▾

Ajouter une image de client sécurisé

Étape 10. Sélectionnez l'interface réseau pour l'accès VPN, choisissez le Device Certificates et cochez sysopt permit-vpn et cliquez sur 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.

Ajouter un contrôle d'accès pour le trafic VPN

Étape 11. Enfin, passez en revue toutes les configurations et cliquez sur 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.

Configuration de la stratégie VPN d'accès à distance

Étape 12. Une fois la configuration initiale du VPN d'accès à distance terminée, modifiez le profil de connexion créé et accédez à Aliases.

Étape 13. Configurez group-alias en cliquant sur l'icône plus (+).

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

Modifier un alias de groupe

Étape 14. Configurez group-url en cliquant sur l'icône plus (+). Utilisez la même URL de groupe que celle configurée précédemment dans le profil client.

Edit Connection Profile

Connection Profile:* RAVPN-CertAuth

Group Policy:* DfltGrpPolicy

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. 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

Modifier l'URL du groupe

Étape 15. Accédez à Access Interfaces. Sélectionnez les Interface Trustpoint et les SSL Global Identity Certificate sous les paramètres SSL.

RAVPN

Enter Description

Connection Profile **Access Interfaces** Advanced

Local Realm: cisco-local Policy Assignments (1) Dynamic Access Policy: None

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

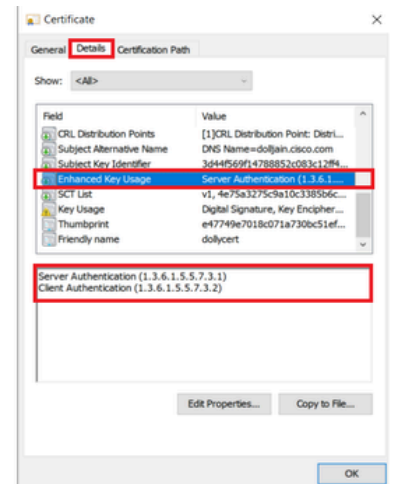
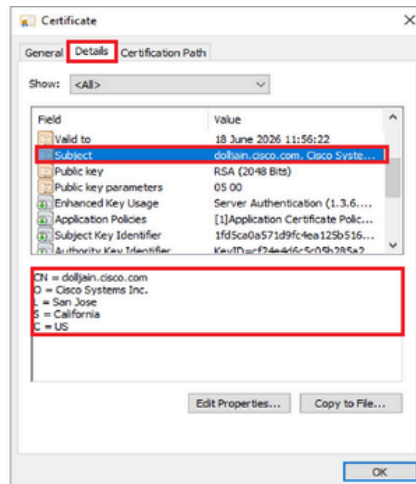
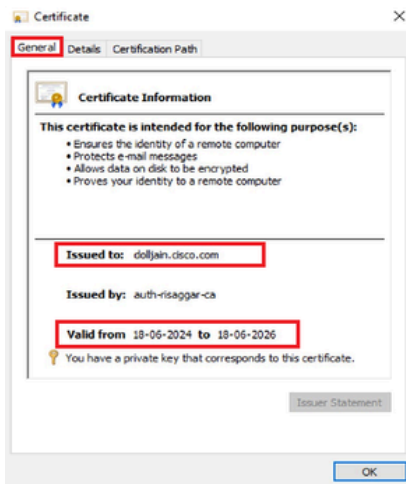
Modifier les interfaces d'accès

Étape 16. Cliquez Save sur et déployez ces modifications.

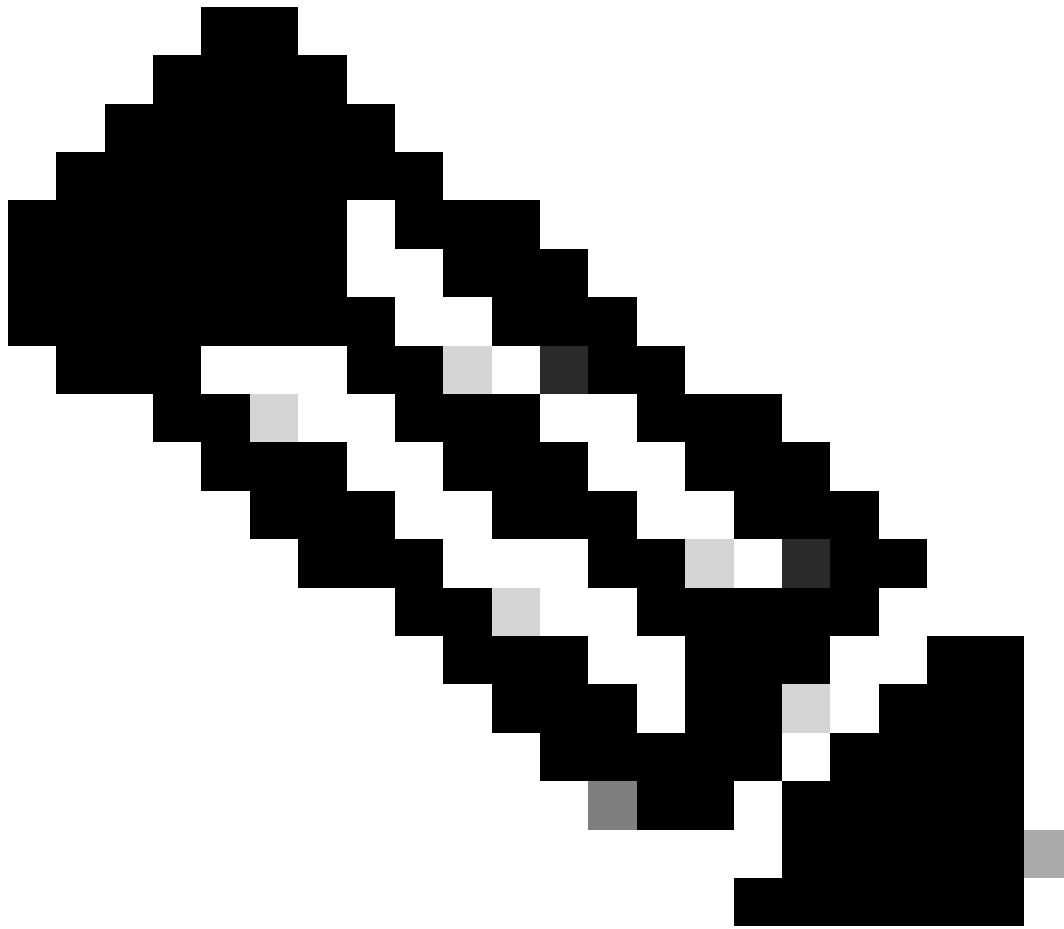
Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Le certificat doit être installé sur le PC client sécurisé avec une date, un objet et une UKE valides sur le PC de l'utilisateur. Ce certificat doit être émis par l'autorité de certification dont le certificat est installé sur le FTD, comme indiqué précédemment. Ici, le certificat d'identité ou d'utilisateur est émis par "auth-risaggar-ca".

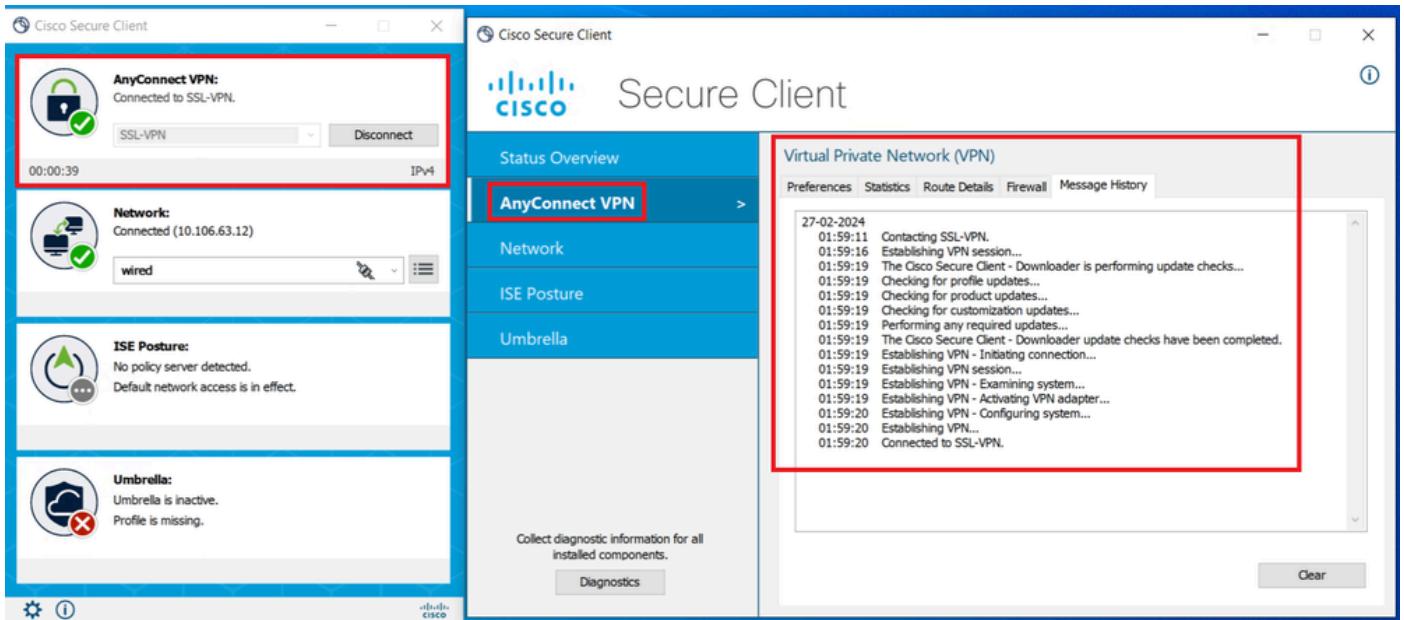


Points saillants du certificat



Remarque : le certificat client doit avoir l'utilisation améliorée de la clé (EKU) « Authentification client ».

2. Le client sécurisé doit établir la connexion.



Connexion client sécurisée réussie

3. Exécutez `show vpn-sessiondb anyconnect` pour confirmer les détails de connexion de l'utilisateur actif dans le groupe de tunnels utilisé.

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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

1. Les débogages peuvent être exécutés à partir de l'interface de ligne de commande de diagnostic du FTD :

```
debug crypto ca 14
```

```
debug webvpn anyconnect 255
```

```
debug crypto ike-common 255
```

2. Reportez-vous à ce [guide](#) pour les problèmes courants.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.