# Configurer la correspondance de certificat pour l'authentification client sécurisée sur FTD via FDM

## Table des matières

## Introduction

Ce document décrit comment configurer Cisco Secure Client avec SSL sur FTD via FDM en utilisant la correspondance de certificat pour l'authentification.

## Conditions préalables

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Device Manager (FDM) virtuel
- Défense contre les menaces de pare-feu (FTD) virtuelle
- Flux d'authentification VPN

### Composants utilisés

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8
- Cisco Secure Client 5.1.4.74
- Éditeur de profil (Windows) 5.1.4.74

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.

## Informations générales

CertificateMatch est une fonctionnalité qui permet aux administrateurs de configurer des critères que le client doit utiliser pour sélectionner un certificat client pour l'authentification avec le serveur VPN. Cette configuration est spécifiée dans le profil client, qui est un fichier XML pouvant être géré à l'aide de l'Éditeur de profil ou modifié manuellement. La fonctionnalité CertificateMatch peut être utilisée pour améliorer la sécurité des connexions VPN en s'assurant que seul un certificat avec des attributs spécifiques est utilisé pour la connexion VPN.

Ce document décrit comment authentifier le client sécurisé Cisco en utilisant le nom commun d'un certificat SSL.

Ces certificats contiennent un nom commun qui est utilisé à des fins d'autorisation.

- CA : ftd-ra-ca-common-name
- Certificat du client VPN de l'ingénieur : vpnEngineerClientCN
- Certificat du client VPN du gestionnaire : vpnManagerClientCN
- Certificat du serveur : 192.168.1.200

## Diagramme du réseau

Cette image présente la topologie utilisée pour l'exemple de ce document.



Diagramme du réseau

## Configurations

Configuration dans FDM

Étape 1. Configurer l'interface FTD

Accédez à Device > Interfaces > View All Interfaces, configurez l'interface interne et externe pour FTD dans l'onglet Interfaces.

Pour GigabitEthernet0/0,

- Nom : extérieur
- Adresse IP : 192.168.1.200/24

Firewall Device Manager	mitoring Policies	Objects Device: fi	repower	$(\Sigma)$		) ? :	admin Administrator	<ul> <li>cisco SECURE</li> </ul>
Device Summary Interfaces								
Cisco Firepower Threat Defe 0/0 0/1 0/2 0/3 0/1 0/2 0/3 0/1 0/2 0/3 0/1 0/2 0/3	nse for VMware	MGMT CONSOLE						
Interfaces Virtual Tunnel	Interfaces							
9 Interfaces				-	, Τ	Filter		+
NAME		LOGICAL NAME	STATUS MC	DE IP ADDRESS		STANDBY ADDRES	SS MONITOR FO	IR HA ACTIONS
> 🗸 GigabitEthernet0/0		outside	Ro	uted 192.168.1.200 500	3		Enabled	

Interface FTD

Étape 2. Confirmer la licence Cisco Secure Client

Accédez à Device > Smart License > View Configuration, confirmez la licence Cisco Secure Client dans l'élément RA VPN License.



Licence client sécurisée

### Étape 3. Ajouter un pool d'adresses

Accédez à Objets > Réseaux, cliquez sur + bouton.

Firewall Device Manag	er Monitoring Policies Objects Device:	firepower		cisco SECURE
Object Types ←	Network Objects and Groups			
C Networks	7 objects		<b>Y</b> Filter	+ 🕫
S Ports			Preset filters: System defined, User defined	
Security Zones	# NAME	TYPE VALUE		ACTIONS
<ul> <li>Application Elitere</li> </ul>	1 IPv4-Private-10.0.0.0-8	NETWORK 10.0.0/8		

Ajouter un pool d'adresses

Entrez les informations nécessaires pour ajouter un nouveau pool d'adresses IPv4. Cliquez sur le bouton OK.

- Nom : ftd-cert-match-pool
- Type : Plage
- Plage IP : 172.16.1.150-172.16.1.160

## Add Network Object

Name	
ftd-cert-match-pool	
Description	
O Network ○ Host ○ FQDN ● R	Range
IP Range	
172.16.1.150-172.16.1.160	
e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-	2001:DB8:0:CD30::100
	CANCEL OK

Ø

Х

Détail du pool d'adresses IPv4

Étape 4. Créer un profil client sécurisé

Téléchargez et installez Secure Client Profile Editor à partir du site <u>Cisco Software</u>. Accédez à Server List, cliquez sur Add button. Entrez les informations nécessaires pour ajouter une entrée de liste de serveurs et cliquez sur le bouton OK.

- Nom d'affichage : cert-match
- Nom de domaine complet ou adresse IP : 192.168.1.200
- Protocole principal : SSL

PN Preferences (Part 1) Preferences (Part 2) Packup Secure	Server List Profile: Untitled								
Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment	Hostname Host Addr Note: it is highly recommend	User Group Bad	okup Ser SCE	Ma	bile Sett Certific	đe			
					Server List Entry	a Caputer CCED Mak	ile Cestificate Disping		
					Primary Server Display Name ( FQDN or IP A 192.168.1.200 Group URL 192.168.1.200	cert-match User Gr	Connection Info Primary Proto Oup	rmation col SSL var way ad During IKE Negotiation EAP-Any y (IOS gateway only)	yConnect 🗸
						Backup Servers Host Address		Add Move Up Move D Delete	
							DK Cancel	Delete	

Entrée de liste de serveurs

Accédez à Certificate Matching, cliquez sur Add button. Entrez les informations nécessaires pour ajouter une entrée de nom unique et cliquez sur le bouton OK.

- Nom : CN
- Modèle : vpnEngineerClientCN
- Opérateur : égal



Remarque : cochez l'option MatchCase dans ce document.

File Help											
VPN Preferences (Part 1) Preferences (Part 2)	Certificate Profile: C:	Certificate Matching Profile: C:\Users\jianzh3\OneDrive - Cisco\Desktop\vpnClient.xml									
Backup Servers	Kev Usag Deci Enci CRL Key Data Key Non Digi	Kev Usage       Extended Key Us         Decipher_Only       ServerAuth       DVCS         Encipher_Only       ClientAuth       IKE Interme         CRL_Sign       CodeSign         Key_Cert_Sign       EmailProtect         Data_Encipher       IPSecEndSystem         Data_Encipher       IPSecTunnel         Key_Encipherm       IPSecUser         Non_Repudiat       TimeStamp         Digital_Signa       OCSPSign		DVCS	ste						
	Custom Extended Match Key (Ma Add Delete						Distinguished Name Entry X     Name CN				
	Mate Mate Distinguis	ch only certii ch only certii shed Name ( Pattern	ficates with F ficates with E Max Wildcard	Gey Usage Extended Ke	y Usage MatchC	Add	Pattern vpnEngineerClient Operator O Equal Not Equal Wildcard MatchCase				
						Edit Delete	OK Cancel				

Entrée de nom distinctif

Enregistrez le profil client sécurisé sur l'ordinateur local et confirmez les détails du profil.

▼ <certificatematch> <matchonlycertswithku>false</matchonlycertswithku></certificatematch>	sWithKU>
▼ <distinguishedname> ▼<distinguishednamedefinition matchcase="Enabled" operator="Ec&lt;br&gt;&lt;Name&gt;CN&lt;/Name&gt;&lt;br&gt;&lt;Pattern&gt;vpnEngineerClientCN&lt;/Pattern&gt;&lt;br&gt;&lt;/DistinguishedNameDefinition&gt;&lt;br&gt;&lt;/DistinguishedName&gt;&lt;/pre&gt;&lt;/td&gt;&lt;th&gt;qual" wildcard="Disabled"></distinguishednamedefinition></distinguishedname>	
	h   " f -   " >
EnableAutomaticServerSelection UserControlla false	able= false >
<pre><autoserverselectionimprovement>20<autoserverselectionsuspendtime>4</autoserverselectionsuspendtime>4  <retainvpnonlogoff>false </retainvpnonlogoff> <captiveportalremediationbrowserfailover>fals <allowmanualhostinput>true </allowmanualhostinput></captiveportalremediationbrowserfailover></autoserverselectionimprovement></pre>	rverSelectionImprovement> verSelectionSuspendTime> se hput>
<pre></pre>	

Profil client sécurisé

Étape 5. Télécharger le profil client sécurisé vers FDM

Accédez à Objets > Profil client sécurisé, cliquez sur le bouton CREATE SECURE CLIENT PROFILE.

Firewall Device Manager Monitoring	Policies Objects Device: firepower	S (admin definition) → administrator	SECURE
Object Types ←	Secure Client Profiles		
C Networks		<b>Filter</b>	+
S Ports	# NAME	FILE NAME ACTIONS	
🔒 Security Zones			
🐬 Application Filters		There are no Secure Client profile objects yet.	
C <sup>2</sup> URLs		Start by creating the first Secure Client profile object.	
Geolocations		CREATE SECURE CUENT PROFILE	
Syslog Servers			
🔎 IKE Policies			
🐴 IPSec Proposals			
Secure Client Profil			
Statity Sources			

Créer un profil client sécurisé

Entrez les informations nécessaires pour ajouter un profil client sécurisé et cliquez sur le bouton OK.

- Nom : secureClientProfile
- Profil client sécurisé : secureClientProfile.xml (téléchargement à partir de l'ordinateur local)

Add Secure Client Profile	0	×
Name secureClientProfile		
Description		
		4
UPLOAD secureClientProfile.xml		
CANCEL	ОК	

Ajouter un profil client sécurisé

### Étape 6. Ajouter une stratégie de groupe

Accédez à Device > Remote Access VPN > View Configuration > Group Policies, cliquez sur + button.

Firewall Device Ma	inager Monitoring Policies Objects	Device: firepower	$(\Sigma_{-})$	۵ 🤃 🗄	admin Administrator	cisco SECURE
RA VPN ←	Device Summary Group Policies					
Connection Profiles	2 objects			<b>T</b> Filter		+
SAML Server	# NAME	DNS SERVER	IPV4 SPLIT TUNNELING	IPV6 SPLIT TUNNELING	SECURE CLIENT PROFILES	ACTIONS
	1 DfltGrpPolicy		Allow all traffic	Allow all traffic		

Ajouter une stratégie de groupe

Entrez les informations nécessaires pour ajouter une stratégie de groupe et cliquez sur OK.

- Nom : ftd-cert-match-grp
- · Profils clients sécurisés : secureClientProfile

Add Group Policy		0	×
Q Search for attribute	Name		
Basic	ftd-cert-match-grp Description		
General Session Settings			4
Advanced	DNS Server		
Address Assignment	Select DNS Group	~	,
Split Tunneling			
Secure Client	Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session		
Traffic Filters	Secure Client profiles		
Windows Browser Proxy	+		
	▼ Filter		
	secureClientProfile		
	Create new Secure Client Prof. CANCEL		
	CANCEL	ОК	

Détails de la stratégie de groupe

Étape 7. Ajouter un certificat FTD

Accédez à Objets > Certificats, cliquez sur Ajouter un certificat interne à partir de l'élément +.

Firewall Device Man	ager Monitoring Policies Objects Device: fi	repower	▷ ♣ @ ? : A	dmin dministrator
Ôbject Types ←	Certificates			
C Networks	121 objects		<b>T</b> Filter	+ · @ ·
S Ports			Preset filters: System defined. User defined	Add Internal CA
Security Zones	II NAME	туре		Add Internal Certificate ACTIONS
Application Filters	1 AAA-Certificate-Services	Trusted CA Certificate		Add Trusted CA Certificate
	2 ACCVRAIZ1	Trusted CA Certificate		
	3 Actalis-Authentication-Root-CA	Trusted CA Certificate		
Geolocations	4 AffirmTrust-Commercial	Trusted CA Certificate		
Syslog Servers	5 AffirmTrust-Networking	Trusted CA Certificate		
🔏 IKE Policies	6 AffirmTrust-Premium	Trusted CA Certificate		
🛖 IPSec Proposals	7 AffirmTrust-Premium-ECC	Trusted CA Certificate		
Secure Client Profiles	8 Amazon-Root-CA-1	Trusted CA Certificate		
Identity Sources	9 Amazon-Root-CA-2	Trusted CA Certificate		
Users	10 Amazon-Root-CA-3	Trusted CA Certificate		
	11 DefaultInternalCertificate	Internal Certificate		
2 Certificatés	12 DefaultWebserverCertificate	Internal Certificate		

Ajouter un certificat interne

Cliquez sur Télécharger le certificat et la clé.



Télécharger le certificat et la clé

Entrez les informations nécessaires pour le certificat FTD, importez un certificat et une clé de certificat depuis l'ordinateur local, puis cliquez sur le bouton OK.

- Nom : ftd-vpn-cert
- Utilisation de la validation pour les services spéciaux : serveur SSL

Add Internal Certificate	0 ×
Name ftd-vpn-cert	
Certificate Paste certificate, or choose a file (DER, PEM, CRT, CER)BEGIN CERTIFICATE MIIDfDCCAmSgAwIBAgIIIkE99YS2cmwwDQYJKoZIhvcNAQELBQAwbTELMAkGA BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAyDVQQHEwVUb2tSbzE0MAwGA1UE0 021+v28+v28+v28+v28+v28+v28+v28+v28+v28+v28	AIUE
Certificate Key Paste certificate key, or choose a file (KEY, PEM) BEGIN RSA PRIVATE KEY MIIEogIBAAKCAQEAxdn5eTUmgo5+GUG2Ng2FjI/+xHRkRrf6o2OccGdzLYK1t 98WPu1YP0T/qwCffKXuMQ9DEVGWIjLRX9nvXdBNoaKUb2Vzc03qW3AjE87p0t	ftdCertKey.pem Upload.Certificate.Key tzw8 +0t0
Validation Usage for Special Services SSL Server ×	~
CANCEL	ОК

Détails du certificat interne

Étape 8. Ajouter une AC au FTD

Accédez à Objets > Certificats, cliquez sur Ajouter un certificat CA approuvé à partir de l'élément +.

Firewall Device Manager	Monitoring Policies Objects Device: firepo	wer $(b_{-})$ (a) (b) $(c_{-})$ (c) $(c_{-})$	dmin dministrator
🐬 Application Filters	Cartificateo		
🖉 URLs	Certificates		
Geolocations	120 objects	<b>T</b> Filter	+ ~ 🗊 ~
		Preset filters: System defined, User defined	Add Internal CA
Sysiog Servers	# NAME	туре	Add Internal Certificate ACTIONS
🔏 IKE Policies	1 NGFW-Default-InternalCA	Internal CA	Add Trusted CA Certificate
🔺 IPSec Proposals	2 AAA-Certificate-Services	Trusted CA Certificate	
Secure Client Profiles	3 ACCVRAIZ1	Trusted CA Certificate	
s Identity Sources	4 Actalis-Authentication-Root-CA	Trusted CA Certificate	
1 Users	5 AffirmTrust-Commercial	Trusted CA Certificate	
<b>Q</b> Certificates	6 AffirmTrust-Networking	Trusted CA Certificate	
	7 AffirmTrust-Premium	Trusted CA Certificate	
Secret Keys	Alfantan Device FOO	T	

Ajouter un certificat CA approuvé

Entrez les informations nécessaires pour l'autorité de certification, importez un certificat depuis l'ordinateur local.

- Nom : ftdvpn-ca-cert
- Utilisation de la validation pour les services spéciaux : client SSL

## Add Trusted CA Certificate

Name	
ftdvpn-ca-cert	
Certificate	ftd-ra-ca.crt
Paste certificate, or choose a file (DER, PEM, CRT, CER)	Upload Certificate
BEGIN CERTIFICATE MIIDbDCCA1SgAwIBAgIIUkKgLg229/0wDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUb2t5bzEOMAwGA1UEChMF	Î.
Skip CA Certificate Check	
SSL Client ×	~
CANCEL	ок
étails du certificat CA approuvé	

2

Étape 9. Ajouter un profil de connexion VPN d'accès à distance

Accédez à Device > Remote Access VPN > View Configuration > Connection Profiles, cliquez sur le bouton CREATE CONNECTION PROFILE.

Firewall Device Ma	anager Monitoring	Policies Objects	Device: firepower	۵. 🖨	Ø ? :	admin Administrator
RA VPN ←		Device Summary Remote Access	VPN Connection Profiles			
Group Policies					<b>T</b> Filter	+
SAML Server		# NAME	АЛА	GROUP POLICY		ACTIONS
			There	are no Remote Access Connection	ns yet.	
				tart by creating the first Connectio		

Ajouter un profil de connexion VPN d'accès à distance

Entrez les informations nécessaires pour le profil de connexion et cliquez sur Next .

- Nom du profil de connexion : ftd-cert-match-vpn
- Type d'authentification : certificat client uniquement
- Nom d'utilisateur du certificat : champ spécifique au mappage
- Champ principal : CN (nom commun)
- Champ secondaire : OU (Unité organisationnelle)
- Pools d'adresses IPv4 : ftd-cert-match-pool

Firewall Device Manager Monitoring Policies	Objects Device: firepower	(c)
Remote Access VPN	Connection and Client     Configuration     Configuration     Configuration	3 Global Settings 4 Summary
Remote Users	ients — Internet	FREPOWER  SISCE  Corporate Resources  urce for User Authentication
	Connection and Client Confe Specify how to authenticate remote users and the secure clients inside network.	guration they can use to connect to the
	Connection Profile Name This name is configured as a connection alias, it can be used to connect to the ftd-cert-match-vpn	VPN gateway
	Group Alias (one per line, up to 5) Group URL (on ftd-cert-match-vpn	e per line, up to 5)
	Primary Identity Source Authentication Type Client Certificate Only	
	Username from Certificate  Map Specific Field  Primary Field  CN (Common Name)  V (Ufformation	d Konal (bit)
	Use entire DN (distinguished name) as username Advanced	
	Authorization Server Accounting Server Please select Y Please select	и ~
	Client Address Pool Assignment IPv6 Address Pool Endpoints are provided an address from this pool + +	X Ied an address from this pool
	10 ftd-cert-match-pool DHCP Servers +	
	CANCEL	

Détails du profil de connexion VPN

Entrez les informations nécessaires à la stratégie de groupe et cliquez sur Next .

• Afficher la stratégie de groupe : ftd-cert-match-grp

Firewall Device Manager Monitoring Policies Objects	Device: firepower	> 🖨 🔊 ?	admin Administrator
Remote Access VPN	Connection and Client     Configuration     Remote User Experience	3 Global Settings	(4) Summary
Remote Users     E     Secure Cli	ierts — Internet — Q Clent Certificate — STERACE	FREPOWER INSCE INTERFACES	Corporate Resources
	Remote User Experience A group policy is a collection of user-oriented session attributes will VPN connection is established. Select or create a Gre View Group Policy ftd-cert-match-grp Policy Group Brief Details  DNS = BANNER	Ce Ich are assigned to client when a oup Policy object.	
	Barrier Text for Authentice BACK NEXT		

Sélectionner une stratégie de groupe

Sélectionnez Certificate of Device Identity, Outside Interface, Secure Client Package pour la connexion VPN.

- Certificat d'identité du périphérique : ftd-vpn-cert
- Interface externe : externe (GigabitEthernet0/0)
- Package client sécurisé : cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



Remarque : fonction NAT Exempt désactivée dans ce document.

Firewall Device Manager Monitoring Policies Objects Device: firepow	er
Remote Users 🖵 Secure Clients 💽 Internet	Client Certificate
These settings control the bas apply to all connection prof	Global Settings ic functioning of the connection. Changes to any of these options iles; you cannot configure different settings in different profiles.
Certificate of Device Identity ftd-vpn-cert (Validation Utage	Outside Interface :: SSL Se V outside (GigabitEthernet0/0)
Fully-qualified Domain Name for e.g. ravpn.example.com	Port 443 e.g. 8080
Access Control for VPN Traffic Decrypted VPN traffic is subjected to 1 policy for decrypted traffic option byp and the authorization ACL downloaded Bypass Access Control polic	Incess control policy inspection by default. Enabling the Bypass Access Control Isses the access control policy, but for remote access VPN, the VPN Filter ACL I from the AAA server are still applied to VPN traffic Y for decrypted traffic (sysopt permit-vpn)
NAT Exempt	
Secure Client Package If a user does not already have the rigil installer when the client authenticates You can download secure client packa You must have the necessary secure c	It secure client package installed, the system will launch the secure client for the first time. The user can then install the package from the system. ges from software.cisco.com (Z. lient software iconse.
Packages UPLOAD PACKAGE V	
Windows: cisco-secure-client	BACK NEXT

Détails des paramètres globaux

Étape 10. Confirmer le résumé du profil de connexion

Confirmez les informations entrées pour la connexion VPN et cliquez sur le bouton FINISH.

þ	Firewall Device Manager	1回 Monitoring	Policies	Dbjects	Device: firepower	$\odot$	٢	۲	?	÷	admin Administrator	Ŷ	cisco SECURE

#### Summary

Review the summary of the Remote Access VPN configuration.

STEP 1: CONNECTION AND CLIENT CONFIGURATION		
Primary Identity Source		
Authentication Type	Client Certificate Only	
Primary Identity Source	-	
Fallback Local Identity Source	-	
Username from Certificate	Map Specific Field	
Primary Field	CN (Common Name)	
Secondary Field	OU (Organisational Unit)	
V Advanced		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		
IPv4 Address Pool	-C πα-cert-match-pool	
IPv6 Address Pool	'0 =	
DHCP Servers	-	
	a beret mathing	
Banner + DNS Server	De un-cert-match-Bib	
DNS Server	i -	
Banner text for authenticated clients	-	
Session Settings		
Maximum Connection Time / Alert Interval	Unlimited / 1 minutes	
Idle Timeout / Alert Interval	30 / 1 minutes	
Simultaneous Login per User	3	
Split Tunneling		
IPv4 Split Tunneling	Allow all traffic over tunnel	
IPv6 Split Tunneling	Allow all traffic over tunnel	
Secure Client		
Secure Client Profiles	e secureClientProfile	
STEP 3: GLOBAL SETTINGS		
Certificate of Device Identity	भूद no-vpn-cen	
Outside Interface	GigabitEthemeto/0 (outside)	
Fully-qualified Domain Name for the Outside Interface	-	
Port	443	
Access Control for VPN Traffic	No	
NAT Exempt		
NAT Exempt	No	
Inside Interfaces	-	
Inside Networks	-	
Secure Client Package		
Packages	III Windows: cisco-secure-client-win-5,1,4,74-webdeploy-k9,pkg	

Confirmer le résumé du profil de connexion

## Confirmer dans FTD CLI

Confirmez les paramètres de connexion VPN dans l'interface de ligne de commande du FTD après le déploiement à partir du FDM.

// Defines IP of interface interface GigabitEthernet0/0 speed auto nameif outside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.1.200 255.255.255.0 // Defines a pool of addresses ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160 // Defines Trustpoint for Server Certificate crypto ca trustpoint ftd-vpn-cert enrollment terminal keypair ftd-vpn-cert crl configure // Server Certificate crypto ca certificate chain ftdvpn-ca-cert certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 . . . . . . quit // Defines Trustpoint for CA crypto ca trustpoint ftdvpn-ca-cert enrollment terminal validation-usage ssl-client crl configure // CA crypto ca certificate chain ftdvpn-ca-cert certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 . . . . . . quit // Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2 anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml anyconnect enable tunnel-group-list enable cache disable error-recovery disable

// Configures the group-policy to allow SSL connections group-policy ftd-cert-match-grp internal group-policy ftd-cert-match-grp attributes dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-dns none split-tunnel-all-dns disable client-bypass-protocol disable msie-proxy method no-modify vlan none address-pools none ipv6-address-pools none webvpn anyconnect ssl dtls none anyconnect mtu 1406 anyconnect ssl keepalive none anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client none anyconnect dpd-interval gateway none anyconnect ssl compression none anyconnect dtls compression none anyconnect modules none anyconnect profiles value secureClientProfile type user anyconnect ssl df-bit-ignore disable always-on-vpn profile-setting

// Configures the tunnel-group to use the certificate authentication tunnel-group ftd-cert-match-vpn type remote-access tunnel-group ftd-cert-match-vpn general-attributes address-pool ftd-cert-match-pool default-group-policy ftd-cert-match-grp tunnel-group ftd-cert-match-vpn webvpn-attributes authentication certificate group-alias ftd-cert-match-vpn enable

### Confirmer dans le client VPN

Étape 1. Copier le profil de client sécurisé vers le client VPN

Copiez le profil client sécurisé pour concevoir le client VPN et le client VPN du manager.



Remarque : le répertoire du profil client sécurisé sur l'ordinateur Windows : C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

📙 📝 📑 🖛 🕴 Profil	e				
File Home	Share	View			
← → • ↑ 📙	> Thi	s PC > Local Disk (C:) > ProgramD	ata > Cisco > Cisco Secure Clie	nt > VPN > Profile	ڻ ~
		Name	Date modified	Туре	Size
Quick access	*	MgmtTun	€, ∠3/2024 20:15	File folder	
Downloads		AnvConnectProfile vsd	6/., 2024 21:44	XSD File	97 KB
Documents	*	🖆 secureClientProfile	7 1, 2024 10:48	XML Document	4 KB



### Étape 2. Confirmer le certificat client

Dans Engineer VPN Client, accédez à Certificates - Current User > Personal > Certificates, vérifiez le certificat client utilisé pour l'authentification.



Confirmer le certificat du client VPN de l'ingénieur

Double-cliquez sur le certificat client, accédez à Détails, vérifiez les détails de Objet.

• Objet : CN = vpnEngineerClientCN

Certificate	×
General Details Certification P	ath
Show: <all></all>	$\sim$
Field	Value ^ Wednesday, June 18, 2025 5:
Subject	vpnEngineerClientCN, vpnEngi RSA (2048 Bits)
Key Usage     Enhanced Key Usage	Digital Signature, Key Encipher Client Authentication (1.3.6.1
Thumboriot algorithm	sha1
CN = vpnEngineerClientCN O = Cisco L = Tokyo S = Tokyo C = JP	
	Edit Properties
	OK

Détails du certificat du client ingénieur

Dans le client VPN du gestionnaire, naviguez vers Certificates - Current User > Personal > Certificates, vérifiez le certificat client utilisé pour l'authentification.



Confirmer le certificat pour le client VPN Manager

Double-cliquez sur le certificat client, accédez à Détails, vérifiez les détails de Objet.

• Objet : CN = vpnManagerClientCN

General Details Certification	Path	
Show: <all></all>	$\sim$	
Field	Value	^
Served at a	Thursday, June 19, 2025 9:41	
j Subject	vpnManagerClientCN, vpnMan	
PUDIC KEY	RSA (2048 Bits)	
Public key parameters	05 00	
🔊 Key Usage	Digital Signature, Key Encipher	
Enhanced Key Usage	Client Authentication (1.3.6.1	
Netscape Comment	xca certificate	
Thumborint algorithm	cha 1	Y
CN = vpnManagerClientCN O = Cisco L = Tokyo S = Tokyo C = JP		I
	Edit Properties Copy to File	
	OK	

×

## Étape 3. Confirmer CA

🔊 Certificate

Détails du certificat client du manager

Dans le client VPN ingénieur et le client VPN gestionnaire, naviguez vers Certificates - Current User > Trusted Root Certification Authorities > Certificates, vérifiez l'autorité de certification utilisée pour l'authentification.

• Émis par : ftd-ra-ca-common-name

🖀 Console1 - [Console Root\Certificates - Current	t User\Trusted Root Certification A	Authorities\Certificates]				o ×
🚘 File Action View Favorites Window	Help					- 8 ×
🗢 🔿 🙍 📷 🤞 💫 🗟 🖉						
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Actions
✓ ☑ Certificates - Current User	2127.0.0.1	127.0.0.1	5/17/2027	Server Authenticati	duo-endpoir	Certificates 🔺
V Personal	AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati	Sectigo (AAJ	More >
ve 🥽 Touted Poot Cartification Authorities	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati	DigiCert Balt	
Certificates	🔄 Class 3 Public Primary Cer	Class 3 Public Primary Cer	8/1/2028	Client Authenticati	VeriSign Clas	ftd-ra-ca 🔺
Centrates	COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	More >
> Intermediate Certification Authorities	Copyright (c) 1997 Micros	Copyright (c) 1997 Micros	12/30/1999	Time Stamping	Microsoft Tii	
> Active Directory User Object	STATEST DESKTOP-VCKHRG1	DESKTOP-VCKHRG1	10/30/2022	Server Authenticati	www.infraey	
> 🛄 Trusted Publishers	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	<all></all>	<none></none>	
> Intrusted Certificates	🔄 🔄 DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	Client Authenticati	DigiCert	
> Chird-Party Root Certification Authoriti	🔄 DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati	DigiCert	
> Constant Second Se	🔄 DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati	DigiCert Glol	
> Client Authentication Issuers	🔄 DigiCert High Assurance	DigiCert High Assurance	11/9/2031	<all></all>	<none></none>	
> Smart Card Trusted Roots	🔄 DigiCert High Assurance	DigiCert High Assurance	11/9/2031	Client Authenticati	DigiCert	
> 🙀 Certificates (Local Computer)	DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati	DigiCert Trus	
		DCT D CA YO	9/30/2021	Client Authenticati	DST Root CA	
	🙀 ftd-ra-ca-common-name	ftd-ra-ca-common-name	/16/2029	<all></all>	<none></none>	
		olooabign	3/18/2029	Client Authenticati	GlobalSign R	
Confirmer CA						

\_

## Vérifier

### Étape 1. Initiation de la connexion VPN

Dans Engineer VPN Client, initiez la connexion Cisco Secure Client. Pas besoin d'entrer le nom d'utilisateur et le mot de passe, le VPN s'est connecté avec succès.

S Cisco Secure Client − □ ×	S Cisco Secure Client   cert-match X	Sisco Secure Client	– 🗆 X
AnyConnect VPI: Your clent certificate will be used for authentication cert-match Connect	Your clent certificate will be used for authentication Group: ftd-cert-match-upn	AnyConnect VPIE Connected to cert-match. cert-match	Disconnect
	OK Cancel	00:00:06	IPv4
🔅 🕕 🕴		<b>♀</b> ①	utinada. Cisco

Connexion VPN réussie pour le client VPN de l'ingénieur

Dans le client VPN du gestionnaire, initiez la connexion du client sécurisé Cisco. Le VPN connecté a échoué en raison d'un échec de validation du certificat.



Échec de la connexion VPN pour le client VPN Manager

### Étape 2. Confirmer les sessions VPN dans FTD CLI

**Exécutez la commande**show vpn-sessiondb detail anyconnect dans l'interface de ligne de commande FTD (Lina) pour confirmer les sessions VPN de l'ingénieur.

firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32 Assigned IP: 172.16.1.150 Public IP: 192.168.1.11 Protocol : AnyConnect-Parent SSL-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 Bytes Tx : 14718 Bytes Rx : 12919 Pkts Tx : 2 Pkts Rx : 51 Pkts Tx Drop: 0 Pkts Rx Drop: 0 Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn Login Time : 05:42:03 UTC Tue Jul 2 2024 Duration: 0h:00m:11s Inactivity: 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000200006683932b Security Grp: none Tunnel Zone: 0

AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1

AnyConnect-Parent: Tunnel ID : 32.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 50170 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.17763 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7359 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 32.2 Assigned IP : 172.16.1.150 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 50177 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7359 Bytes Rx : 12919 Pkts Tx : 1 Pkts Rx : 51 Pkts Tx Drop : 0 Pkts Rx Drop : 0

#### Dépannage

Vous pouvez vous attendre à trouver des informations sur l'authentification VPN dans le syslog de débogage du moteur Lina et dans le fichier DART sur l'ordinateur Windows.

Ceci est un exemple de journaux de débogage dans le moteur Lina pendant la connexion VPN du client ingénieur.

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClient Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi

#### Informations connexes

Configuration du service de gestion prêt à l'emploi FDM pour Firepower 2100 Configurer un VPN d'accès à distance sur FTD géré par FDM Configuration et vérification de Syslog dans le Gestionnaire de périphériques Firepower

### 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.