# Wachtwoordbeheer configureren met LDAP's voor RA VPN op FTD beheerde via FMC

# Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Configuratie Netwerkdiagram en -scenario Bepaal LDAP-basis DN en groep DN Kopieert de SSL-certificaatsleuf van LDAPS In het geval van meerdere certificaten die zijn geïnstalleerd in de lokale machineopslag op de LDAP-server (optioneel) **FMC-configuraties** Licentie controleren Instellingsgebied AnyConnect configureren voor wachtwoordbeheer **Implementeren** Laatste configuratie **AAA-configuratie Configuratie AnyConnect** Verificatie Verbinding maken met AnyConnect en wachtwoordbeheer voor de gebruikersverbinding controleren Problemen oplossen Debugs Debugs voor werkwachtwoordbeheer Veelvoorkomende fouten die tijdens het wachtwoordbeheer worden aangetroffen

# Inleiding

Dit document beschrijft het configureren van wachtwoordbeheer met LDAP's voor AnyConnect Clients die verbinding maken met Cisco Firepower Threat Defence (FTD).

# Voorwaarden

# Vereisten

Cisco raadt u aan een basiskennis te hebben van deze onderwerpen:

- Basiskennis van de configuratie van RA VPN (Remote Access Virtual Private Network) op FMC
- Basiskennis van de LDAP-serverconfiguratie op het VCC
- Basiskennis van Active Directory

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft 2012 R2-server
- FMCv met 7.3.0
- FTDv met 7.3.0

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.

# Configuratie

# Netwerkdiagram en -scenario



Windows-server is vooraf geconfigureerd met ADDS en ADCS om het wachtwoordbeheerproces van de gebruiker te testen. In deze configuratiehandleiding worden deze gebruikersaccounts gemaakt.

Gebruikersaccounts:

- Beheerder: Dit wordt gebruikt als de directory account om de FTD te kunnen binden aan de Active Directory-server.
- admin: Een account van een testbeheerder waarmee de gebruikersidentiteit wordt aangetoond.

# Bepaal LDAP-basis DN en groep DN

1. Open (Openstaand) Active Directory Users and Computers via het Dashboard van Server Manager.

Server Ma	anager • Dashboard			C     Active Directory Add	nage Tools View Help ministrative Center
III Dathboard	WELCOME TO SERVER MANAGER			Active Directory Do	mains and Trusts
Lossi Casara				Active Directory Mo	dule for Windows PowerShell
Local Server				Active Directory Site	is and Services
All Servers	1 Confi	gure this local server		AD ES Mananement	is and computers
R AD CS				ADSI Edit	
iii AD DS	QUICK START			Certification Author	ity
AD FS	2 Ad	d roles and features		Component Service	
DNS DNS	3 Ad	other servers to manage		Computer Manager	nent
■ File and Storage Services ▷	5 Ad	outer servers to manage		Defragment and Op	timize Drives
ED IIS	4 Cre	ate a server group		DNS	
PL NAP				Event Viewer	
				Group Policy Manag	jement
	15101110005			Health Registration	Authority
	LEARN MURE			Internet Information	Services (IIS) Manager
				ISCSI Initiator	
	ROLES AND SERVER GROUPS			Local Security Policy	
	Roles: 7   Server groups: 1   Servers total:	1		ODBC Data Sauran	(22.164)
		[H]		File ODEC Data Sources	(52-50)
	™ā AD CS 1	I AD DS 1 AD FS	1 🗄 DNS 1	Serv Performance Monit	(04-010)
	Manageability	Manageability     Manageability	ty Manageability	Mana Resource Monitor	
	Events	Events Events	Events	Security Configurati	on Wizard
	Events	Events Events	cvents	Services	
	Services	Services Services	Services	Servi System Configuratio	in
	Performance	Performance Performance	Performance	Perfo System Information	
	BPA results	BPA results BPA results	BPA results	BPA Task Scheduler	
				Windows Firewall w	ith Advanced Security
				Windows Memory 8	liagnostic
				Windows PowerShe	
				Windows PowerShe	II (x86)
	1 IS 1	NAP 1 Local Serve	r 1 All Servers 1	Windows PowerShe	I ISE
	Manageability	Manageability     Manageability	ty Manageability	Windows PowerShe Windows Server Bac	li ISE (x86) kup
	Events	Events Events	Events		
	Coniese	Capitan Capitan	Contract		
	Services	Services Services	Services		
	Performance	Performance Performance	Performance	Activate Windo	ws
	BPA results	BPA results BPA results	BPA results	Go to Action Center	to activate Windows.
					~

2. Open de View Option op het bovenpaneel, en laat toe Advanced Features, zoals aangegeven op de afbeelding:

	Active Directory U	lsers and Computers	_ <b>_</b> ×
File Action View	/ Help		
( <del>-</del>	Add/Remove Columns		
📃 Active Direc	Large Icons	n	
▷ Saved Q	Small Icons		
⊿ main razor.loc ▷ 📫 Built	List	ntainer for up	
D 🖺 Com 🔍	Com     Detail     Dom     Users, Contacts, Groups, and Computers as containers     Eore	ntainer for sec	
▷ Dom		ntainer for or	
▷ 📫 Lost	Advanced Features	ntainer for ma	
⊳ 🧰 Man	Contractions	tem settings	
▷ Prog ▷ System	Customize	ntainer for up	
<ul> <li>Delta Sers</li> <li>MTDS Que</li> <li>MTDS Que</li> <li>TPM Devi</li> </ul>	atas TPM Devices msTPM-Infor ees infrastructure infrastructureU		
<	>		
Displays items in a list			

3. Hierdoor kunnen extra eigenschappen worden weergegeven onder de AD-objecten. Bijvoorbeeld om de DN voor de root te vinden razor.local, klik met de rechtermuisknop razor.localen kies vervolgens Properties, zoals getoond in deze afbeelding:

A	Active Directory Users and Computers	_ 🗆 X
File Action View Help		
🗢 🔿 📶 🗂 🖾 🍳 📾	🝸 📴 🕱	
Active Directory Users and Com Saved Queries  Active Directory Users and Com Saved Queries  Active Directory Users and Com Builtin builtin  Delegate Control Find  Delegate Controller Find  Change Domain Controller Change Domain functional level Delegate Source All Tasks View All Tasks View Properties Help	Description Domain ner Default container for up zational Default container for sec dFound Default container for or ner Default container for ma ner Default location for stor ner Builtin system settings ner Default container for up QuotaC Quota specifications co A-Infor uctureU	
Opens the properties dialog box for the current selection.		

4. Onder Properties, kiest u de Attribute Editor tabblad. Zoeken distinguishedName Klik onder de kenmerken op View, zoals aangegeven in de afbeelding.

Dit opent een nieuw venster waar de DN kan worden gekopieerd en later in FMC kan worden geplakt.

In dit voorbeeld, de wortel DN is  $_{DC=razor, DC=local}$ . Kopieert de waarde en sla deze op voor later gebruik. Klik op de knop  $_{OK}$  om het venster String Attribute Editor te verlaten en op te klikken  $_{OK}$  om de Eigenschappen te verlaten.

raz	zor.local Properties ?	x				
General Managed By Ob	oject Security Attribute Editor					
Attributes:						
Attribute	Value	~				
defaultLocalPolicyObj	<not set=""></not>					
description	<not set=""></not>					
desktopProfile	<not set=""></not>	=				
displayName	<not set=""></not>					
displayNamePrintable	<not set=""></not>					
distinguishedName	DC=razor,DC=local					
domainPolicyObject	<not set=""></not>					
domainReplica	<not set=""></not>					
dSASignature	{ V1: Flags = 0x0; LatencySecs = 0; DsaGuid					
dSCorePropagationD	0x0 = ( )					
eFSPolicy	<not set=""></not>					
extensionName	<not set=""></not>					
flags	<not set=""></not>					
forceLogoff	(never)	~				
< 111	>					
View	View					
Stri	ng Attribute Editor	x				
Attribute: distinguish	edName					
Value:						
DC=razor,DC=local						
Clear	OK Cano	el				

## Kopieert de SSL-certificaatsleuf van LDAPS

1. Druk Win+R en mmc.exeklikt u vervolgens op OK, zoals in deze afbeelding wordt getoond.



2. Naar navigeren File > Add/Remove Snap-in..., zoals in deze afbeelding getoond:

	Console1 - [Console Root]	_ <b>□</b> ×
File Action View Favorites Window Help		_ 8 ×
Mew Ctrl+N		
Open Ctrl+O	Actions	
Save Ctrl+S	There are no items to show in this view. Console F	Root 🔺
Save As	More A	Actions +
Add/Remove Snap-in Ctrl+M	4	
Options	-	
1 C:\Windows\system32\dsa		
2 C:\Windows\system32\eventvwr		
4 C:\Windows\system32\certsry		
Fvit	-	
Enables you to add snap-ins to or remove them from the sn	ap-in console.	

3. Kies onder beschikbare snap-ins Certificates en klik vervolgens op Add, zoals getoond in deze afbeelding:

ap-in	Vendor	^	<u></u>	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor				Remove
Active Directory Site	Microsoft Cor				Demove
Active Directory Use	Microsoft Cor				
ActiveX Control	Microsoft Cor				Move Up
ADSI Edit	Microsoft Cor				Move Down
Authorization Manager	Microsoft Cor		Add >		Hove Boun
Certificate Templates	Microsoft Cor				
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Mcrosoft Cor				
Disk Management	Microsoft and				Advanced

4. Kiezen Computer account en klik vervolgens op Next, zoals getoond in deze afbeelding:

Certificates snap-in	×
This snap-in will always manage certificates for: <u>Service account</u> <u>Computer account</u>	
< <u>B</u> ack <u>N</u> ext > Canc	el:

Zoals hier getoond, klik Finish.

Select Computer	$\times$
Select the computer you want this snap in to manage.         This snap in will always manage: <ul> <li>Local computer: (the computer this console is running on)</li> <li>Another computer:</li> <li>Prowse</li> </ul> Another computer:       Prowse         Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cance	I

5. Klik nu op  $_{\rm OK}$ , zoals in deze afbeelding wordt getoond.

inap-in	Vendor	^		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			uge Certificates (Local Computer)	Bemove
Active Directory Site	Microsoft Cor				
Active Directory Use	Microsoft Cor				Maura Lin
ActiveX Control	Microsoft Cor				move <u>up</u>
ADSI Edit	Microsoft Cor				Move Down
Contificate Templates	Microsoft Cor		<u>A</u> dd >		
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
Piele Management	Microsoft and				Advanta

- 6. Breid de Personal map aan en klik vervolgens op Certificates. Het certificaat dat door LDAP's wordt gebruikt, moet worden afgegeven aan de FQDN (Fully Qualified Domain Name) van de Windows-server. Op deze server staan drie certificaten vermeld:
- Er is een CA-certificaat afgegeven aan en door razor-WIN-E3SKFJQD6J7-CA.
- Een CA-certificaat afgegeven aan en door supinfo-WIN-FNJVP9QUEH9-CA.
- Er is een identiteitsbewijs afgegeven aan WIN-E3SKFJQD6J7.razor.local door razor-WIN-E3SKFJQD6J7-CA.

In deze configuratiehandleiding is de FQDN WIN-E3SKFJQD6J7.razor.local en dus zijn de eerste twee certificaten niet geldig voor gebruik als het LDAPs SSL certificaat. Het aan WIN-E3SKFJQD6J7.razor.local is een certificaat dat automatisch is afgegeven door de Windows Server CA-service. Dubbelklik op het certificaat om de gegevens te controleren.



- 7. Om als het LDAPs SSL-certificaat te worden gebruikt, moet het certificaat aan de volgende vereisten voldoen:
- De algemene naam of DNS-onderwerpalternatieve naam komt overeen met de FQDN van de Windows-server.
- Het certificaat heeft serververificatie in het veld Uitgebreid sleutelgebruik.

In het Details tabblad voor het certificaat, kies Subject Alternative Name, waarbij de FQDN WIN-E3SKFJQD6J7.razor.local aanwezig is.

Cer	tificate ×					
General Details Certification Path						
Show: <all></all>	✓					
Field	Value					
Enhanced Key Usage	Client Authentication (1.3.6.1					
Application Policies	[1]Application Certificate Polic					
Subject Key Identifier	1b 34 75 f8 c4 3e ef 58 fb 43					
Authority Key Identifier	KeyID=cf 83 92 a4 14 00 e7 5					
CRL Distribution Points	[1]CRL Distribution Point: Distr					
Authority Information Access	[1]Authority Info Access: Acc					
🖳 Key Usage	Digital Signature, Key Encipher					
Subject Alternative Name	DNS Name=WIN-E3SKFJQD6J 🗸					
DNS Name=WIN-E3SKFJQD6J7.razor.local						
DNS Name=RAZOR						
I						
E	dit Properties Copy to File					
Learn more about certificate details						
Learn more about <u>ceruncate details</u>						
	ОК					

Onder Enhanced Key Usage, Server Authentication aanwezig is.

Cer	tificate	x			
General Details Certification Path					
Show: <all></all>	*				
Field	Value	~			
Certificate Template Inform	Template = LDAPoverSSL(1.3.6				
🛐 Enhanced Key Usage	Client Authentication (1.3.6.1				
Application Policies	[1]Application Certificate Polic				
🗊 Subject Key Identifier	1b 34 75 f8 c4 3e ef 58 fb 43				
authority Key Identifier	KeyID=cf 83 92 a4 14 00 e7 5	=			
CRL Distribution Points	[1]CRL Distribution Point: Distr				
Authority Information Access	[1]Authority Info Access: Acc				
💦 Key Usage	Digital Signature, Key Encipher	~			
Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) KDC Authentication (1.3.6.1.5.2.3.5)					
Edit Properties Copy to File Learn more about <u>certificate details</u>					
	OK				

8. Zodra dit is bevestigd, wordt onder de Certification Path tabblad kiest u het certificaat op het hoogste niveau dat het basiscertificaat van CA is, en klikt u vervolgens op View Certificate. Hierdoor worden de certificaatgegevens voor het basiscertificaat van de CA geopend, zoals in de afbeelding wordt getoond:

Certificate	🗶 Certificate	٢
General Details Certification Path	General       Details       Certification Path         Image: Certificate Information         This certificate is intended for the following purpose(s):         • All issuance policies         • All application policies	
View Certificate	Issued to: razor-WIN-E3SKFJQD6J7-CA Issued by: razor-WIN-E3SKFJQD6J7-CA	
Certificate status: This certificate is OK.	Valid from 3/22/2021 to 3/22/2026	
Learn more about <u>certification paths</u>	Learn more about <u>certificates</u>	

9. In het Details tabblad van het basiscertificaat van CA, klikt u op Copy to File en navigeer door deCertificate Export Wizard die de root-CA in PEM-formaat exporteert.

Kiezen Base-64 encoded X.509 als bestandsindeling.

e 🦻	Certificate Export Wizard		
	Completing the Certificate Exp	oort Wizard	
	You have successfully completed the Certificate	Export wizard.	
	You have specified the following settings:		
	File Name	C:\Users\Administrator\Downloads\rod	
	Export Keys Include all certificates in the certification path	No	
	File Format	Base64 Encoded X.509 (*.cer)	
	< 111	>	
		Finish Can	cel

10. Open het Root CA-certificaat dat is opgeslagen op de geselecteerde locatie op de machine met een blocnote of een andere teksteditor.

Dit is het certificaat in PEM-indeling. Bewaar dit voor later.

----BEGIN CERTIFICATE-----

MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgovcjEhMB8GA1UEAxMYcmF6b3ItV010LUUzU0tGS1FENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCguBWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvcGCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnb1xwtX0B2G4UxZ3LRrWznjXaS02Rc3qVw41n0AziGs4ZMNM1X8UWeKuwi8W9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU30aiiI/tp422ydy3Kg17Iqt1s4XqpZmTezykWra7dUyXfkuESk61E0AVCCSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhuj1x4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwEDDagGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00BBYEFM+DkqQUA0dY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIAA41BAQCiSm5U7U6Y7zXdx+d1eJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7Bn06f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q4sMZffbVrG1Rz7twW36J5G5vhNUhzZ1N20Lw6wtHg2S08X1vpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nry1bGuDsepY7/u2uWfy/vpTJigeok2DH6HFf0ET3sE+7rsIAY+of0kWW5gNwQ4h0wv4Goqj+YQRAXXi2OZy1tHR1dfUUbwVENSFQtDnFA7X

In het geval van meerdere certificaten die zijn geïnstalleerd in de lokale machineopslag op de LDAP-server (optioneel)

1. In een situatie waarin meerdere identiteitscertificaten door LDAPS kunnen worden gebruikt en er onzekerheid is over de vraag welke certificaten worden gebruikt of wanneer er geen toegang tot de LDAPS-server is, is het nog steeds mogelijk de wortel CA uit een pakketopname op de FTD te halen.

2. Wanneer u meerdere certificaten hebt die geldig zijn voor serververificatie in de lokale computercertificaatopslag van de LDAP-server (zoals AD DS-domeincontroller), kan worden opgemerkt dat een ander certificaat wordt gebruikt voor LDAPS-communicatie. De beste oplossing voor een dergelijk probleem is om alle overbodige certificaten uit het lokale computercertificaatarchief te verwijderen en slechts één certificaat te hebben dat geldig is voor serververificatie.

Als er echter een legitieme reden is dat u twee of meer certificaten vereist en ten minste een Windows Server 2008 LDAP-server hebt, kan de Active Directory Domain Services (NTDS\Personal) certificaatopslag worden gebruikt voor LDAP-communicatie.

Deze stappen tonen aan hoe u een LDAPS-enabled certificaat kunt exporteren van een domeincontroller lokale computer certificaatopslag naar de Active Directory Domain Services servicecertificaatopslag (NTDS\Personal).

- Navigeer naar de MMC-console op de Active Directory Server, kies Bestand en klik vervolgens op Add/Remove Snap-in.
- Klik op de knop Certificates en klik vervolgens op Add.
- In het Certificates snap-in, kiezen Computer account en klik vervolgens op Next.
- In Select Computer, kiezen Local Computer, klik op de knop OKen klik vervolgens op Finish. In Add or Remove Snap-ins, klik op de knop OK.
- Klik met de rechtermuisknop op de certificaatconsole van een computer met een certificaat dat wordt gebruikt voor de serververificatie. certificate,klik op de knop All Tasksen klik vervolgens op Export.

<b>a</b>	Console1 - [Console Root\Certifie	cates (Local Computer)\Per	rsonal\Certificates]	_ <b>D</b> X
🖀 File Action View Favorites Windo	ow Help			_ 8 ×
🗢 🔿 🙋 🐻 🐇 🖬 🖒 📘	? 🖬			
Console Root	Issued To	Issued By	Expiration Date	Actions
∠ Gertificates (Local Computer)	azor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates
⊿ Personal	supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	A 2/23/2025	More Actions
Certificates	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD617_CA	A / 25 / 2022	More Actions 7
Foterprise Trust		Oper	n	WIN-E3SKEIOD617 razor local
Enterprise Trust	•	All T	Tasks ► Op	en 🕨
Trusted Publishers		Cut	Rec	quest Certificate with New Key
Untrusted Certificates		Сору	v Rer	new Certificate with New Key
Third-Party Root Certification Au		Delet	te No.	
Trusted People	-		Ma	inage Private Keys
Client Authentication Issuers		Prop	perties Ad	vanced Operations
Other People		Help	p Exp	port
Remote Desktop				
Certificate Enrollment Requests				
Smart Card Trusted Roots				
Irusted Devices	-			
< III >			>	
Export a certificate				,

• Exporteer het certificaat in de pfx in de volgende delen. Verwijs naar dit artikel over hoe een certificaat uit te voeren in de pfx formaat vanaf MMC:

https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html.

- Nadat het certificaat is geëxporteerd, navigeert u naar Add/Remove Snap-in ON MMC console. Klik op de knop Certificates en klik vervolgens op Add.
- Kiezen Service account en klik vervolgens op Next.

Certificates snap-ir	n <b>X</b>
This snap-in will always manage certificates for: O My user account Service account Computer account	

- In het Select Computer dialoogvenster kiest u Local Computer en klik op Next.
- Kiezen Active Directory Domain Services en klik vervolgens op Finish.

Certificate	es snap-in 🗙
Select a service account to manage on the local c	:omputer.
Active Directory Certificate Services Active Directory Domain Services Active Directory Web Services AD FS Windows Service Application Experience Application Host Helper Service Application Identity Application Information Application Layer Gateway Service Application Management ASP.NET State Service Background Intelligent Transfer Service Background Tasks Infrastructure Service Base Filtering Engine	
	< Back Finish Cancel

- Op de Add/Remove Snap-ins dialoogvenster klikt u op OK.
- Uitbreiden Certificates Services (Active Directory Domain Services) en klik vervolgens op NTDS\Personal.
- Rechtsklik NTDS\Personal,klik op de knop All Tasksen klik vervolgens op Import.

Console1 - [Console Root	Certificates - Service (Active Directory Domain Services) on Local Compu	ter\NTDS\Personal]
🖀 File Action View Favorites Window He	elp	_ 8 ×
🗢 🔿 🙍 🖬 📋 🧟 🕞 🚺		
Console Root Obje	ect Type	Actions
▷ Gertificates (Local Computer)	Certificates	NTDS\Personal
Certificates - Service (Active Directory D		More Actions
▷ Int Find Certificates		
D 🖾 NT 🛛 All Tasks 🕨	Find Certificates	
⊳ INI View ►	Import	
NT New Window from Here	Advanced Operations	
NT     New Taskpad View		
NT Refresh		
Export List		
Help		
< III >		][
Add a certificate to a store		

- Op de Certificate Import Wizard welkomstscherm, klik op Next.
- Klik in het scherm Bestand om te importeren op Browse, en lokaliseer het certificaatbestand dat u eerder hebt geëxporteerd.
- Zorg er in het Open scherm voor dat de uitwisseling van persoonlijke informatie (\*pfx,\*.p12) is geselecteerd als het bestandstype en navigeer vervolgens in het bestandssysteem om het eerder geëxporteerde certificaat te vinden. Klik vervolgens op dat certificaat.

-	Оре	n			x
Organize 👻 New folder				•	
☆ Favorites	Name	Date modified	Туре	Size	
Desktop	😼 Idapcert	4/25/2022 12:01	Personal Informati	5 KB	
ik Downloads E Recent places					
🕞 Libraries					
Documents     Music					
E Pictures					
Videos					
1툪 Computer					
👽 Network					
File na	me: Idapcert		✓ Personal	Information Exch	nange 🗸
			Оре	n Ca	ncel

- Klik op de knop Open en klik vervolgens op Next.
- Voer in het wachtwoordscherm het wachtwoord in dat u voor het bestand hebt ingesteld en klik vervolgens op Next.
- Zorg er op de pagina Certificaatopslag voor dat Alle certificaten plaatsen zijn geselecteerd en lees Certificaatopslag: NTDS\Personal en klik vervolgens op Next.

€	Ø Certificate Import Wizard						
	Certificate Store						
	Certificate stores are system areas where certificates are kept.						
	Windows can automatically select a certificate store, or you can specify a location for the certificate.						
	$\bigcirc$ Automatically select the certificate store based on the type of certificate						
	Place all certificates in the following store						
	Certificate store:						
	NTDS\Personal Browse						
	Learn more about <u>certificate stores</u>						
	Next Cancel						

х

• Op de Certificate Import Wizard scherm voltooien, klikt u op Finish. U ziet dan een bericht dat de import succesvol was. Klik op de knop ok. Het certificaat is ingevoerd in het certificaatarchief: NTDS\Personal.

Console1 - [Console Root\Certific	ates - Service (Active Directory	Domain Services) on Local C	Computer\NTDS\Pe	ersonal\Certificates]	_ 🗆 X		
🚡 File Action View Favorites Window Help							
🗢 🤿 🖄 📰 🔏 🐁 🔛 📓							
Console Root	Issued To 📩	Issued By	Expiration Date	Actions			
Certificates (Local Computer)	razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates			
Certificates - Service (Active Directory D     Image: A Image: Active Directory D     Image: A Image: Active Directory D     Image: Active D     Image: Actined D     Image: Active D     Image: Active D     Image: Active D	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	•		
Certificates				WIN-E3SKFJQD6J7.r	azor.local 🔺		
NIDS\Irusted Koot Certification Au     MTDS\Enterprise Trust     MTDS\Intermediate Certification Au     MTDS\Intermediate Certificates     MTDS\Untrusted Publishers     MTDS\Third-Party Root Certification     MTDS\Trusted People     MTDS\Client Authentication Issuers				More Actions	,		
< <u> </u>	< III		>				
NTDS\Personal store contains 2 certificates.	VTDS\Personal store contains 2 certificates.						

## **FMC-configuraties**

#### Licentie controleren

Om de AnyConnect-configuratie te kunnen implementeren, moet de FTD worden geregistreerd bij de slimme licentieserver en moet een geldige Plus-, Apex- of VPN-licentie alleen op het apparaat worden toegepast.

#### Instellingsgebied

1. Naar navigeren System > Integration. Naar navigeren Realmsklikt u vervolgens op Add Realm, zoals getoond in deze afbeelding:

Overview Analys	is Policies Devices Objects	AMP Intelligence							<b>e</b>	Deploy System Help	admin v
				Configuration U	Jsers Domains	Integration	Updates	Licenses v	Logging •	Health • <sup>1</sup> Monitoring	<ul> <li>Tools •</li> </ul>
	3					2					
Cloud Services	Realms Identity Sources	High Availability	eStreamer Host Input Client	Smart Software Manage	er On-Prem						
Realms R	ealm Sequences Sync Results										4
										Compare Realms	idd Realm
Name -	Description	Tune	Domain	AD Brimany Domain		Base DN				State	

 Vul de weergegeven velden in op basis van de informatie die bij de Microsoft-server voor LDAP's is verzameld. Hiervoor moet u het Root CA-certificaat importeren dat het LDAPservicecertificaat op de Windows-server heeft ondertekend onder Objects > PKI > Trusted CAs > Add Trusted CA, aangezien dit in het kader van deDirectory Server Configuration van het rijk. Klik op de knop ок.

Firepower Manag Objects / Object Manage	ement Center Overview Analy	sis Policies Devices Objects AMP Intelligence		Deploy Q 🚱 🔅 (	admin 🔹
AAA Server     Access List     Address Pools     Application Elitere	Trusted CAs Trusted certificate authority (CA) object	represents a CA public key certificate belonging to a trusted CA. You can use e	xternal CA objects in	Add Trusted CA Q. Filter SSL policy, realm configurations and ISE/ISE-PIC connection	on.
AS Path Cipher Suite List Community List	Name ISRG-Root-X1 Izence.com			Value CN=ISRG Root X1, ORG=Internet Security Research G CN=Izenoe.com, ORG=IZENPE S.A., C=ES	11
DNS Server Group     External Attributes     Eile List	LDAPS-ROOT-CERT Microsec-e-Szigno-Root-CA-2009	Edit Trusted Certificate Authority	0	CN=razor-WIN-E3SKFJQD6J7-CA CN=Microsec e-Szigno Root CA 2009, ORG=Microse	11
FlexConfig     Geolocation     Interface	NetLock-Arany-Class-Gold-FAtanAosAtv OISTE-WISeKey-Global-Root-GA-CA	Name: LDAPS-ROOT-CERT		CN=NetLock Arany (Class Gold) FA tanA2sÅtvÅjny, CN=OISTE WISeKey Global Root GA CA, ORG=WISeK	/1
Key Chain Network	OISTE-WISeKey-Global-Root-GB-CA OISTE-WISeKey-Global-Root-GC-CA	Subject: Common Name: razor-WIN-E3SKFJQD6J7-CA Organization:		CN=OISTE WISeKey Global Root GB CA, ORG=WISeK CN=OISTE WISeKey Global Root GC CA, ORG=WISeK	/1
Cert Enrollment External Cert Groups External Certs	QuoVadis-Root-CA-1-G3 QuoVadis-Root-CA-2	Organization Unit: Issuer: Common Name: razor-WIN-E3SKFJQD6J7-CA		CN=QuoVadis Root CA 1 G3, ORG=QuoVadis Limited, CN=QuoVadis Root CA 2, ORG=QuoVadis Limited, C=	/1
Internal CA Groups Internal CAs Internal Cert Groups	QuoVadis-Root-CA-3 QuoVadis-Root-CA-3-G3	Organization: Organization Unit: Not Valid Before:		CN=QuoVadis Root CA 3, ORG=QuoVadis Limited, C= CN=QuoVadis Root CA 3 G3, ORG=QuoVadis Limited,	11
Internal Certs Trusted CA Groups Trusted CAs	QuoVadis-Root-Certification-Authority Secure-Global-CA	Mar 22 14:33:15 2021 GMT Not Valid After: Mar 22 14:43:15 2026 GMT		CN=QueVadis Root Certification Authority, ORG=QueV CN=Secure Global CA, ORG=SecureTrust Corporation	11
Policy List Port	SecureTrust-CA	Install Certificate Cance	el Save	CN*SecureTrust CA, ORG*SecureTrust Corporation, Displaying 81 - 100 of 125 rows  < < Page 5	/ ⊒ 017 > >  C

#### Add New Realm

Name*	Description
LDAP-Server	
Туре	
LDAP ~	
Directory Username*	Directory Password*
Administrator@razor.local	
E.g. user@domain.com	
Base DN*	Group DN*
DC=razor,DC=local	DC=razor,DC=local
E.g. ou=group,dc=cisco,dc=com	E.g. ou=group,dc=cisco,dc=com
Directory Server Configuration	
<ul> <li>WIN-E3SKFJQD6J7.razor.local:636</li> </ul>	
Hostname/IP Address*	Port*
WIN-E3SKE IOD6 I7 razor local	636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT +
Interface used to connect to Directory server (i)	
Resolve via route lookup	
<ul> <li>Choose an interface</li> </ul>	
Default: Management/Diagnostic Interface	$\sim$
Test	
Add another directory	

0 ×

3. Klik op de knop Test om ervoor te zorgen dat het VCC met succes kan verbinden met de Directory Gebruikersnaam en het wachtwoord dat in de eerdere stap is opgegeven. Aangezien deze tests worden geïnitieerd vanuit het FMC en niet via een van de routeerbare interfaces die op de FTD zijn geconfigureerd (zoals binnenkant, buitenkant, dmz), garandeert een succesvolle (of mislukte) verbinding niet hetzelfde resultaat voor AnyConnect-verificatie, aangezien AnyConnect LDAP-verificatieverzoeken worden geïnitieerd vanuit een van de FTD routable interfaces.

Add Directory	@ ×
Hostname/IP Address* WIN-E3SKFJQD6J7.razor.loc Encryption	Port* 636 CA Certificate*
Interface used to connect to Dire	ctory server
Test Test Choose an interface	gnostic Interface
	Cancel OK

4. Schakel het nieuwe domein in.

Overview Anal	lysis Policies Devices Objects	AMP Intelligence					•	Deploy System	Help v admin v
				Configuration Users	Domains Inte	egration Updates	Licenses • Logging •	Health • Mor	nitoring • Tools •
Cloud Service	Realms Identity Sources	High Availability eStreame	r Host Input Client	Smart Software Manager On-F	rem				
Realms	Realm Sequences Sync Results								
								Compare Rea	Add Realm
Name +	Description	Туре	Domain	AD Primary Domain		Base DN		State	
AC-Local		LOCAL	Global					Enabled	🛓 🖊 🖥 🗑
LDAP		AD	Global	cisco01.com	0	OU=Users,OU=CISCO,DC	=cisco01,DC=com	Enabled	<u>* / %</u> ¥
LDAP-Server		AD	Global	razor.local		DC=razor,DC=local		C Enabled	±∕¶∎ ¥

AnyConnect configureren voor wachtwoordbeheer

1. Kies het bestaande verbindingsprofiel of maak een nieuw profiel aan als AnyConnect voor het eerst is ingesteld. Hier wordt een bestaand verbindingsprofiel met de naam 'AnyConnectAD' gebruikt dat is toegewezen aan de lokale verificatie.

Overview Analysis Policies Devices Objects AMP Intel	ligence		🎨 Deploy System Help 🕶 admin 🕶
Device Management Device Upgrade NAT VPN • Remote Acce	SS QoS Platform Settings FlexConfig Certif	cates	
AnyConnect Enter Description			Save Cancel
			Policy Assignments (1)
		Local Realm: asa	Dynamic Access Policy: Hostscan
Connection Profile Access Interfaces Advanced			
			0
Name	ААА	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy	/ 5
AnyConnect	Authentication: Radius (RADIUS) Authorization: Radius (RADIUS) Accounting: None	DfttGrpPolicy	/ 6
AnyConnect-AD	Authentication: LOCAL Authorization: None Accounting: None	AnyConnect-Group	/ 6

2. Bewerk het verbindingsprofiel en wijs de nieuwe LDAPs-server toe die in de eerdere stappen is geconfigureerd, onder de AAA-instellingen van het verbindingsprofiel. Klik op de knop save in de rechterbovenhoek

Firepower Management Center Devices / VPN / Edit Connection Profile	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🙆 admin 🔻
AnyConnect		Save
Enter Description		Policy Assignments (1)
Connection Profile Access Interfaces Advanced	Edit Connection Profile	Local Realm: None Dynamic Access Policy: Hostscan
	Connection Profile:* AnyConnect-AD	
	Group Policy:* AnyConnect-Group +	+
Name	Edit Group Policy Client Address Assignment AAA Aliases	
DefaultWEBVPNGroup	Authentication	/1
AnyConnect	Authentication Method: AAA Only 💌	/1
AnvConnect-AD	Authentication Server: LDAP-Server (AD)	11
	Fallback to LOCAL Authentication	
	Use secondary authentication	
	Authorization	
	Authorization Server: Use same authentication server 🔻	
	Allow connection only if user exists in authorization database Configure LDAP Attribute Map	
	Accounting	
	Accounting Server:	
	<ul> <li>Advanced Settings</li> </ul>	
	Strip Realm from username	
	Cancel Save	

3. Wachtwoordbeheer inschakelen onder de AAA > Advanced Settings en slaat de configuratie op.

Overview Analysis Policies Devices Objects AMP Intellig	nce	🇛 Deploy System Help 🕶 admin 🕶
Device Management Device Upgrade NAT VPN + Remote Access AnyConnect Enter Description	QoS Platform Settings FlexConfig Certificates	Save Cancel
		Policy Assignments (1) Local Realm: asa Dynamic Access Policy: <u>Hostscan</u>
Connection Profile Access Interfaces Advanced	Connection Profile 7 × Connection Profile: AnyConnect-AD Group Policy: AnyConnect-Oropo Fill Croup Policy: Connect-Oropo	0
DefaultWEBVPNGroup	Client Address Assignment AAA Aliases	/8
AnvConnect	LDAP-Server (AD)	19
;	Fallback to LOCAL Authentication	
AnyConnect-AD	Use secondary authentication Authorization	<i>2</i> 8
sjobs	Authorization Server: Use same sufferintiation server  Authorization Server Configure LDAP Attribute Map	∕8
	Accounting Accounting Server: Accounting Server: Accounting Server: Accounting Server: Accounting Server: Accounting Server: Accounting Server: Accounting Server: Accounting Server: Accounting Server: Strip Realm from username Finable Password Management Notify user on the day of password expiration Serve Cancel	

#### Implementeren

1. Als u klaar bent met de configuratie, klikt u op deDeploy knop aan de rechterbovenkant.

Overview Analysis Policies	Devices	Objects	AMP	Intelligence
----------------------------	---------	---------	-----	--------------

2. Klik op het selectievakje naast de FTD-configuratie die erop is toegepast en klik vervolgens op Deploy, zoals getoond in deze afbeelding:

Overview	Analysis	olicies Devices Objects	AMP Intelligence						🎨 Deploy System Help 🔻 admin 🕶
									Deployment Deployment History
<b>\</b>	Search usir	device name, user name, type, gr	oup or status						1 device selected Deploy time: Estimate
•	Device		Modified by	Inspect Interruption	Туре	Group	Last Deploy Time	Preview	Status
> 🛛	10.197.22	.190_FTD1	admin		FTD		May 30, 2022 7:34 AM	8.	Pending

## Laatste configuratie

Dit is de configuratie in de FTD CLI na de succesvolle implementatie.

AAA-configuratie

#### <#root>

> show running-config aaa-server

```
aaa-server LDAP-Server protocol ldap
```

Note the second state of t

```
max-failed-attempts 4
```

```
realm-id 8
```

aaa-server LDAP-Server host WIN-E3SKFJQD6J7.razor.local

<----- LDAPs Server to which the queries are sent

```
server-port 636
```

- ldap-base-dn DC=razor,DC=local
- ldap-group-base-dn DC=razor,DC=local
- ldap-scope subtree
- ldap-naming-attribute sAMAccountName
- ldap-login-password \*\*\*\*\*
- ldap-login-dn \*\*\*\*\*@razor.local
- ldap-over-ssl enable
- server-type microsoft

# Configuratie AnyConnect

#### <#root>

> show running-config webvpn

#### webvpn

```
enable Outside
```

anyconnect image disk0:/csm/anyconnect-win-4.10.01075-webdeploy-k9.pkg 1 regex "Windows"

```
anyconnect profiles FTD-Client-Prof disk0:/csm/ftd.xml
```

anyconnect enable

tunnel-group-list enable

- cache
- no disable
- error-recovery disable

```
> show running-config tunnel-group
```

tunnel-group AnyConnect-AD type remote-access tunnel-group AnyConnect-AD general-attributes address-pool Pool-1

authentication-server-group LDAP-Server

default-group-policy AnyConnect-Group

password-management password-expire-in-days 1

tunnel-group AnyConnect-AD webvpn-attributes
group-alias Dev enable

> show running-config group-policy AnyConnect-Group

group-policy

AnyConnect-Group

internal

<----- Group-Policy configuration that is mapped once the user is authenticated</pre>

group-policy AnyConnect-Group attributes

vpn-simultaneous-logins 3

vpn-idle-timeout 35791394

vpn-idle-timeout alert-interval 1

vpn-session-timeout none

vpn-session-timeout alert-interval 1

vpn-filter none

vpn-tunnel-protocol ikev2 ssl-client

```
split-tunnel-policy tunnelspecified
```

split-tunnel-network-list value Remote-Access-Allow

<----- LDAPs Serve

<---- Password-management

<---- Protocol

default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect profiles value FTD-Client-Prof type user anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable

> show running-config ssl

ssl trust-point ID-New-Cert Outside

<----- FTD ID-cert trustpoint name mapped to the outside interface on which AnyConnect Connections

# Verificatie

Verbinding maken met AnyConnect en wachtwoordbeheer voor de gebruikersverbinding controleren

1. Start een verbinding met het betreffende verbindingsprofiel. Zodra bij de eerste aanmelding is bepaald dat het wachtwoord moet worden gewijzigd omdat het eerdere wachtwoord door de Microsoft Server is geweigerd omdat het is verlopen, wordt de gebruiker gevraagd het wachtwoord te wijzigen.

S Cisco AnyConnect   FTD-Hostname X		
Group: Dev v Username: admin Passinord: [	G Cisco AnyConnect Secure Mobility Client - X      Viii:     Contacting FTD-Hostname.      FTD-Hostname     Connect	
OK Cancel	C C C C C C C C C C C C C C C C C C C	
Sisco AnyConnect   FTD-Hostname	×	
New Password:	a new brue: S Cisco AnyConnect Secure Mobility Client — X VPRE Contacting FTD-Hostname.	
Continue	Cancel	

2. Zodra de gebruiker het nieuwe wachtwoord voor aanmelding invoert, is de verbinding tot stand gebracht.

🚳 Cisco AnyC	onnect Secure Mobility Client		_		×
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconnec	t
00:02:43					IPv4
<b>۞</b> ()					ditalia cisco

3. Controleer de gebruikersverbinding op de FTD CLI:

#### <#root>

FTD\_2# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

 Username
 : admin

 Index
 : 7

 <------ Username, IP address assigned information of the client</td>

 Assigned IP
 : 10.1.x.x

 Public IP
 : 10.106.xx.xx

 Protocol
 :

 AnyConnect-Username, USERNAME

License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384

Bytes Tx	:	16316	Bytes Rx	:	2109
Group Policy	:	AnyConnect-Group	Tunnel Group	:	AnyConnect-AD
Login Time	:	13:22:24 UTC Mon Apr 2	5 2022		
Duration	:	Oh:00m:51s			
Inactivity	:	Oh:00m:00s			
VLAN Mapping	:	N/A	VLAN	:	none
Audt Sess ID	:	0ac5e0fa000070006266a09	90		
Security Grp	:	none	Tunnel Zone	:	0

# Problemen oplossen

### Debugs

Dit debug kan worden uitgevoerd in diagnostische CLI om problemen op te lossen met wachtwoordbeheer: debug ladp 255.

Debugs voor werkwachtwoordbeheer

#### <#root>

- [24] Session Start
- [24] New request Session, context 0x0000148f3c271830, reqType = Authentication
- [24] Fiber started
- [24] Creating LDAP context with uri=ldaps://10.106.71.234:636
- [24] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful
- [24] supportedLDAPVersion: value = 3
- [24] supportedLDAPVersion: value = 2
- [24] Binding as \*\*\*\*\*@razor.local
- [24] Performing Simple authentication for \*\*\*\*\*@razor.local to 10.106.71.234
- [24] LDAP Search:

Base DN = [DC=razor,DC=local]

Filter = [sAMAccountName=admin]

Scope = [SUBTREE]

[24] User DN = [CN=admin,CN=Users,DC=razor,DC=local]

[24] Talking to Active Directory server 10.106.71.234

[24] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[24] Read bad password count 3

[24] Binding as admin

[24] Performing Simple authentication for admin to 10.106.71.234

[24] Simple authentication for admin returned code (49) Invalid credentials

[24] Message (admin): 80090308: LdapErr: DSID-0C0903C5, comment: AcceptSecurityContext error, data 773,

[24] Checking password policy

[24] New password is required for admin

[24] Fiber exit Tx=622 bytes Rx=2771 bytes, status=-1

[24] Session End

[25] Session Start

[25] New request Session, context 0x0000148f3c271830, reqType = Modify Password

[25] Fiber started

[25] Creating LDAP context with uri=ldaps://10.106.71.234:636

[25] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful

- [25] supportedLDAPVersion: value = 3
- [25] supportedLDAPVersion: value = 2
- [25] Binding as \*\*\*\*\*@razor.local
- [25] Performing Simple authentication for \*\*\*\*\*@razor.local to 10.106.71.234
- [25] LDAP Search:

Base DN = [DC=razor, DC=local]

Filter = [sAMAccountName=admin]

Scope = [SUBTREE]

- [25] User DN = [CN=admin,CN=Users,DC=razor,DC=local]
- [25] Talking to Active Directory server 10.106.71.234
- [25] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[25] Read bad password count 3

[25] Change Password for admin successfully converted old password to unicode

[25] Change Password for admin successfully converted new password to unicode

[25] Password for admin successfully changed

[25] Retrieved User Attributes:

- [25] objectClass: value = top
- [25] objectClass: value = person
- [25] objectClass: value = organizationalPerson
- [25] objectClass: value = user
- [25] cn: value = admin
- [25] givenName: value = admin
- [25] distinguishedName: value = CN=admin,CN=Users,DC=razor,DC=local
- [25] instanceType: value = 4
- [25] whenCreated: value = 20201029053516.0Z

[25]	whenChanged: value = 20220426032127.0Z
[25]	displayName: value = admin
[25]	uSNCreated: value = 16710
[25]	uSNChanged: value = 98431
[25]	name: value = admin
[25]	objectGUID: value =0.].LH9.4
[25]	userAccountControl: value = 512
[25]	<pre>badPwdCount: value = 3</pre>
[25]	codePage: value = 0
[25]	countryCode: value = 0
[25]	badPasswordTime: value = 132610388348662803
[25]	lastLogoff: value = 0
[25]	lastLogon: value = 132484577284881837
[25]	<pre>pwdLastSet: value = 0</pre>
[25]	primaryGroupID: value = 513
[25]	objectSid: value =7Z RQ
[25]	accountExpires: value = 9223372036854775807
[25]	logonCount: value = 0
[25]	sAMAccountName: value = admin
[25]	sAMAccountType: value = 805306368
[25]	userPrincipalName: value = *****@razor.local
[25]	<pre>objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=razor,DC=local</pre>
[25]	dSCorePropagationData: value = 20220425125800.0Z
[25]	dSCorePropagationData: value = 20201029053516.0Z
[25]	dSCorePropagationData: value = 16010101000000.0Z
[25]	lastLogonTimestamp: value = 132953506361126701
[25]	<pre>msDS-SupportedEncryptionTypes: value = 0</pre>
[25]	uid: value = *****@razor.local
[25] F	Fiber exit Tx=714 bytes Rx=2683 bytes, status=1

[25] Session End

## Veelvoorkomende fouten die tijdens het wachtwoordbeheer worden aangetroffen

Als het wachtwoordbeleid dat door de Microsoft Server is ingesteld niet wordt nageleefd wanneer de gebruiker het nieuwe wachtwoord invoert, wordt de verbinding verbroken met de fout "Wachtwoord voldoet niet aan de Wachtwoordbeleidsvereisten". Zorg er dus voor dat het nieuwe wachtwoord voldoet aan het beleid dat door de Microsoft Server voor LDAP's is ingesteld.

😚 Cisco	o AnyConnec	t   FTD-Hostname	×			
	Cannot comp password pol complexity, a	Nete password change because the password does not meet the licy requirements. Check the minimum password length, password and password history requirements.				
	Group:	Dev 🗸	Cisco /	AnyConnect Secure Mobility Client - 🗆 🗙		
	Username: [	admin				
	Password:		] 🛛 🕰	VPN: Cannot complete password change because the password		
		OK Cancel		does not meet the password policy requirements. Check FTD-Hostname Connect		
			<b>0</b> ()	altaba cisco		
			Cisco A	nyConnect	×	
			8	Cannot complete password change because the password does not meet the password policy requirements. Check the minimum password length, password complexity, and password history requirements.		
				ОК		

#### 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.