Kennwortverwaltung mit LDAPs für RA VPN auf FTD konfiguriert, von FMC verwaltet

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten **Konfiguration** Netzwerkdiagramm und -szenario Ermitteln der LDAP-Basis-DN und Gruppen-DN LDAP SSL-Zertifikatstamm kopieren Wenn mehrere Zertifikate im lokalen Computerspeicher auf dem LDAP-Server installiert sind (optional) **FMC-Konfigurationen** Lizenzierung überprüfen Setup-Bereich AnyConnect für die Passwortverwaltung konfigurieren **Bereitstellung** Abschließende Konfiguration **AAA-Konfiguration** AnyConnect-Konfiguration Verifizierung Stellen Sie eine Verbindung mit AnyConnect her, und überprüfen Sie den Kennwortverwaltungsprozess für die Benutzerverbindung. Fehlerbehebung Fehlerbehebung Arbeiten mit Kennwortverwaltungsdebugs Häufige Fehler bei der Kennwortverwaltung

Einleitung

In diesem Dokument wird die Konfiguration der Kennwortverwaltung mithilfe von LDAPs für AnyConnect-Clients beschrieben, die eine Verbindung mit Cisco FirePOWER Threat Defense (FTD) herstellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- Grundkenntnisse der RA VPN-Konfiguration (Remote Access Virtual Private Network) auf FMC
- Grundkenntnisse der LDAP-Serverkonfiguration auf FMC
- Grundkenntnisse von Active Directory

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Microsoft 2012 R2-Server
- FMCv mit 7.3.0
- FTDv mit 7.3.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfiguration

Netzwerkdiagramm und -szenario



Der Windows-Server ist mit ADDS und ADCS vorkonfiguriert, um die Verwaltung des Benutzerkennworts zu testen. In dieser Konfigurationsanleitung werden diese Benutzerkonten erstellt.

Benutzerkonten:

- Administrator: Dieser Parameter wird als Verzeichniskonto verwendet, damit die FTD eine Bindung zum Active Directory-Server herstellen kann.
- admin: Ein Test-Administratorkonto, mit dem die Benutzeridentität veranschaulicht wird.

Ermitteln der LDAP-Basis-DN und Gruppen-DN

1. Offen Active Directory Users and Computers über das Server Manager-Dashboard.

Server Ma	mager • Dashboard			CO Active Directory Administrative Center Active Directory Administrative Center Active Directory Module for Windows PowerShell Active Directory Module for Windows PowerShell
I Local Server III All Servers III AD CS III AD DS AP AD DS AP AD DS AP AD DS AP AD S III S IIIS 『Local Services ▷ IIIS 『Local Services ▷ IIIS 『Local Services ▷ IIIS	CUICK START CUICK START CUICK START C Add A Add A Add A Add Create CLEARN MORE ROLES AND SERVER GROUPS	igure this local server id roles and features id other servers to manage eate a server group		Active Directory Uses and Computes Active Directory Uses and Computes ADF 5 Management ADF 16 for Authority Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer Group Policy Management Health Registration Authority Internet Information Services (IIS) Manager ISCS Initiator Local Security Policy
	Roles 7 Server groups 1 Servers total AD CS 1 Manageability Events Services Performance BPA results	AD DS 1 Manageability Events Services Performance BPA results	AD FS 1 Manageability Manageability Events Manageability Events Services Performance Performance BPA results BPA results	File ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) Performance Monitor Even Servi Services Services Services System Information BPA Windows Firewall with Advanced Security Windows Memory Diagnostic Windows Memory Diagnostic
	IIS 1 ① Manageability Events Services Performance BPA results	NAP 1 Manageability Events Services Performance BPA results	Image Local Server 1 Image ability Events Services Performance PPA results Performance	Windows PowerShell (s66) Windows PowerShell (sE Windows Server Backup Windows Server Backup Contract Windows Go to Action Center to activate Windows.

2. Öffnen Sie View Option oben an, und aktivieren Sie die Advanced Features, wie in der Abbildung dargestellt:

	Active Directory U	sers and Computers	_ _ ×
File Action View	/ Help		
🗢 🔿 🙍	Add/Remove Columns		
Active Direc Large Icons		n	
▷ Saved Q	Small Icons		
≥ inazor.iot	List	ntainer for up	
⊳ 🚞 Com 🎴	▷ Com ● Detail	ntainer for sec	
	ntainer for or		
	ntainer for ma tation for stor		
▷ Man	▷ Man Customize	em settings	
 Lost Filter Options Prog System Users NTDS Quotas TPM Devices TPM Devices Infrastructure infrastructureU 		vecifications co	
Displays items is a list			
Displays items in a list	•		

 Dies ermöglicht die Anzeige zusätzlicher Eigenschaften unter den AD-Objekten. Um z. B. den DN f
ür den Root zu finden, razor.local, Rechtsklick razor.local, und w
ählen Sie Properties, wie in diesem Bild gezeigt:

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com Name Type Description Image: Source Queries Image: Directory Users and Com Delegate Control Default container for up Image: Dorn Change Dornain Default container for or co Default container for or co Image: Dorn Change Dornain Controller ner Default container for or co Image: Dorn Change Dornain Controller ner Default container for or co Image: Dorn Change Dornain functional level ner Default container for stor Image: Dorn Change Dornain functional level ner Default container for stor Image: Dorn Change Dornain functional level ner Default container for stor Image: Dorn Change Dornain functional level ner Default container for stor Image: Dorn Change Dornain functional level ner Default container for stor Image: Dorn Change Dornain functional level ner Default container for stor Image: Dornain functional for poperior Quota specifications co Quota specifications co Image: Dornain functional for poperior Image: Dornain functional for poperinformal functin
Opens the properties dialog box for the current selection.

4. Unter Properties, wählen Sie Attribute Editor aus. Suchen distinguishedName klicken Sie unter den Attributen auf View, wie im Bild dargestellt.

Daraufhin wird ein neues Fenster geöffnet, in das die DN kopiert und später in FMC eingefügt werden kann.

In diesem Beispiel ist der Stamm-DN _{DC=razor}, _{DC=local}. Kopieren Sie den Wert, und speichern Sie ihn für einen späteren Zeitpunkt. Klicken Sie auf _{OK} um das Fenster String Attribute Editor zu verlassen und auf _{OK} um die Eigenschaften zu beenden.

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	Filter	
Stri	ng Attribute Editor	x
Attribute: distinguish	edName	
Value:		
DC=razor,DC=local		
Clear	OK Cano	el

LDAP SSL-Zertifikatstamm kopieren

1. Presse Win+R und geben mmc.exe, und klicken Sie dann auf OK, wie in diesem Bild dargestellt.



2. Navigieren Sie zu File > Add/Remove Snap-in..., wie in diesem Bild gezeigt:

a	Console1 - [Console Root]	_ _ ×
File Action View Favorites Window Help		_ <i>8</i> ×
New Ctrl+N		
Open Ctrl+O		Actions
Save Ctrl+S	There are no items to show in this view.	Console Root
Save As		More Actions
Add/Remove Snap-in Ctrl+M		
C:\Windows\system32\dsa		
3 C:\Windows\system32\certmar		
4 C:\Windows\system32\certsrv		
Exit		
Enables you to add snap-ins to or remove them from the snap	o-in console.	

3. Wählen Sie unter Verfügbare Snap-Ins die Option Certificates und dann auf Add, wie in diesem Bild gezeigt:

	Venuor	^		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor				Remove
Active Directory Site	. Microsoft Cor				Demote
Active Directory Use	Microsoft Cor				
ActiveX Control	Microsoft Cor				Move Up
ADSI Edit	Microsoft Cor				Move Down
Authorization Manager	Microsoft Cor		<u>A</u> dd >		nore gomi
Certificate Templates	Microsoft Cor				
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
Disk Management	Microsoft and	¥			Ad <u>v</u> anced

4. Auswählen Computer account und dann auf Next, wie in diesem Bild gezeigt:

Certificates snap-in	×
This snap-in will always manage certificates for: <u>Service account</u> <u>Computer account</u>	
< <u>B</u> a	ck <u>N</u> ext > Cancel

Klicken Sie wie hier gezeigt auf Finish.

Select Computer	Х
Select the computer you want this snap-in to manage. This snap-in will always manage: Local computer: (the computer this console is running on) Another computer: Browse Another computer: Browse Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

5. Klicken Sie jetzt auf $_{\rm OK}$, wie in diesem Bild dargestellt.

Active Directory Do Microsoft Cor Active Directory Site Microsoft Cor Active Directory Use Microsoft Cor Active Directory Use Microsoft Cor Active Directory Use Microsoft Cor	<u>R</u> emove
Active Directory Site Microsoft Cor Active Directory Use Microsoft Cor ActiveX Control Microsoft Cor ADSI Edit Microsoft Cor	
Active Directory Use Microsoft Cor ActiveX Control Microsoft Cor ADSI Edit Microsoft Cor	
ActiveX Control Microsoft Cor ADSI Edit Microsoft Cor Authorization Manager Microsoft Cor	
ADSI Edit Microsoft Cor	Move Up
A URACAS BAD MADA MADA MADA MADA MADA MADA MADA	Move Down
Autoinization Manager Microsoft Cor Add >	-
Certificates Microsoft Cor	
Certification Authority Microsoft Cor	
Component Services Microsoft Cor	
Computer Managem Microsoft Cor	
Device Manager Microsoft Cor	
Disk Management Microsoft and	Advanced
· · · · · · · · · · · · · · · · · · ·	

- 6. Erweitern Sie die Personal Ordner, und klicken Sie auf Certificates. Das von LDAPs verwendete Zertifikat muss f
 ür den vollqualifizierten Dom
 änennamen (Fully Qualified Domain Name, FQDN) des Windows-Servers ausgestellt werden. Auf diesem Server sind drei Zertifikate aufgelistet:
- Ein Zertifizierungsstellenzertifikat wurde ausgestellt von und an razor-WIN-E3SKFJQD6J7-CA.
- Ein Zertifizierungsstellenzertifikat, das an und von supinfo-WIN-FNJVP9QUEH9-CA.
- Ein Identitätszertifikat wurde ausgestellt für WIN-E3SKFJQD6J7.razor.local von razor-WIN-E3SKFJQD6J7-CA.

In diesem Konfigurationsleitfaden wird der FQDN WIN-E3SKFJQD6J7.razor.local Daher sind die ersten beiden Zertifikate nicht als LDAP SSL-Zertifikat gültig. Das Identitätszertifikat, das ausgestellt wurde an WIN-E3SKFJQD6J7.razor.local ist ein Zertifikat, das automatisch vom Windows Server-Zertifizierungsstellendienst ausgestellt wurde. Doppelklicken Sie auf das Zertifikat, um die Details zu überprüfen.



- 7. Um als LDAP SSL-Zertifikat verwendet werden zu können, muss das Zertifikat folgende Anforderungen erfüllen:
- Der allgemeine Name oder alternative DNS-Betreffname stimmt mit dem FQDN des Windows Servers überein.
- Das Zertifikat weist im Feld "Enhanced Key Usage" (Erweiterte Schlüsselverwendung) eine Serverauthentifizierung auf.

Im Details Registerkarte für das Zertifikat, wählen Sie Subject Alternative Name, wobei der FQDN WIN-E3SKFJQD6J7.razor.local vorhanden ist.

Ce Ce	rtificate ×				
General Details Certification Path	1				
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					
F	dit Properties Copy to File				
	copy which				
Learn more about <u>certificate details</u>					
	OK				
	UK				

Unter Enhanced Key Usage, Server Authentication vorhanden ist.

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. Sobald dies bestätigt ist, wird im Rahmen des Certification Path auf, wählen Sie das Zertifikat der obersten Ebene aus, das das Root-Zertifizierungsstellenzertifikat darstellt, und klicken Sie dann auf View Certificate. Dadurch werden die Zertifikatdetails für das Stammzertifikat der Zertifizierungsstelle geöffnet, wie im Bild gezeigt:

Certificate	x Certificate	x
General Details Certification Path Certification path Tazor-WIN-E3SKFJQD6J7-CA WIN-E3SKFJQD6J7.razor.local	General Details Certification Path 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.		
Learn more about <u>certification paths</u>	Learn more about <u>certificates</u>	t
OK	ОК	

9. Im Details Registerkarte des Stammzertifikats der Zertifizierungsstelle klicken Sie auf Copy to File und navigieren Sie durch dieCertificate Export Wizard der die Stammzertifizierungsstelle im PEM-Format exportiert.

Auswählen Base-64 encoded X.509 als Dateiformat.

e 🦻	Certificate Export Wizard		
	Completing the Certificate Exp	port Wizard	
	You have successfully completed the Certificate	Export wizard.	
	You have specified the following settings:		
	File Name	C:\Users\Administrator\Downloads\roo	
	Export Keys	No	
	Include all certificates in the certification path	No	
	File Format	Base64 Encoded X.509 (*.cer)	
		2	
		Finish C	ancel

10. Öffnen Sie das Zertifikat der Stammzertifizierungsstelle, das am ausgewählten Speicherort auf dem Computer gespeichert ist, mit einem Notizblock oder einem anderen Texteditor.

Zeigt das Zertifikat im PEM-Format an. Speichern Sie das für später.

----BEGIN CERTIFICATE-----

MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgovcjEhMB8GA1UEAxMYcmF6b3ItV010LUUzU0tGS1FENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCguBWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvcGCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnb1xwtX0B2G4UxZ3LRrWznjXaS02Rc3qVw41n0AziGs4ZMNM1X8UWeKuwi8W9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU30aiiI/tp422ydy3Kg17Iqt1s4XqpZmTezykWra7dUyXfkuESk61E0AVCCSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhuj1x4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwEDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00BBYEFM+DkqQUA0dY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIAA41BAQCiSm5U7U6Y7zXdx+d1eJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7Bn06f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q4sMZffbVrG1Rz7twW36J5G5vhNUhzZ1N20Lw6wtHg2S08X1vpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nry1bGuDsepY7/u2uWfy/vpTJigeok2DH6HFf0ET3sE+7rsIAY+of0kWW5gNwQ4h0wv4Goqj+YQRAXXi2OZy1tHR1dfUUbwVENSFQtDnFA7X

Wenn mehrere Zertifikate im lokalen Computerspeicher auf dem LDAP-Server installiert sind (optional)

1. Bei mehreren Identitätszertifikaten, die von LDAPS verwendet werden können und bei Unsicherheit darüber, welche verwendet werden, oder wenn kein Zugriff auf den LDAPS-Server besteht, ist es weiterhin möglich, die Stammzertifizierungsstelle aus einer Paketerfassung auf dem FTD zu extrahieren.

2. Wenn Sie im lokalen Computer-Zertifikatspeicher des LDAP-Servers (z. B. AD DS-Domänencontroller) mehrere Zertifikate haben, die für die Serverauthentifizierung gültig sind, kann festgestellt werden, dass für die LDAPS-Kommunikation ein anderes Zertifikat verwendet wird. Die beste Lösung für ein solches Problem besteht darin, alle nicht benötigten Zertifikate aus dem Zertifikatspeicher des lokalen Computers zu entfernen und nur ein Zertifikat zu haben, das für die Serverauthentifizierung gültig ist.

Wenn jedoch ein legitimer Grund vorliegt, dass Sie zwei oder mehr Zertifikate benötigen und mindestens über einen Windows Server 2008 LDAP-Server verfügen, kann der Active Directory Domain Services (NTDS\Personal)-Zertifikatspeicher für die LDAP-Kommunikation verwendet werden.

Diese Schritte zeigen, wie ein LDAPS-aktiviertes Zertifikat aus einem Zertifikatspeicher des lokalen Domänencontrollers in den Zertifikatspeicher des Active Directory-Domänendiensts (NTDS\Personal) exportiert wird.

- Navigieren Sie zur MMC-Konsole auf dem Active Directory-Server, wählen Sie Datei aus, und klicken Sie dann auf Add/Remove Snap-in.
- Klicken Sie auf Certificates und dann auf Add.
- Im Certificates snap-in, wählen Computer account und dann auf Next.
- In Select Computer, wählen Local Computer, Klicken Sie auf OK, und klicken Sie dann auf Finish. In Add or Remove Snap-ins, Klicken Sie auf OK.
- Klicken Sie in der Zertifikatskonsole eines Computers, der ein für die Serverauthentifizierung verwendetes Zertifikat enthält, mit der rechten Maustaste auf den certificate, Klicken Sie auf All Tasks, und klicken Sie dann auf Export.

a	Console1 - [Console Root\Certif	icates (Local Computer)\Perso	nal\Certificates]	_ D X
🚟 File Action View Favorites Windo	ow Help			_ 8 ×
🗢 🔿 🚈 🔣 🖬 🗶 🖬 😖	? 🖬			
Console Root	Issued To	Issued By	Expiration Date	Actions
⊿ G Certificates (Local Computer)	🛱 razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates
⊿ Personal	supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	2/23/2025	More Actions
Certificates	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD617_CA	A/25/2022	more Actions 7
Forterprise Trust =	_	Open		WIN-E3SKEIOD617 razor local
Intermediate Certification Autho		All Tasks	; • Op	en 🕨
Trusted Publishers		Cut	Re	quest Certificate with New Key
Untrusted Certificates		Сору	Rei	new Certificate with New Key
Third-Party Root Certification Au		Delete	M	nage Drivate Kevr
Trusted People	1	Descet		and Operations
Client Authentication Issuers		Propertie	Ad	vanced Operations
Other People		Help	Exp	port
Certificate Enrollment Requests				
Smart Card Trusted Roots				
Trusted Devices				
▷ I Web Hosting	-			
< III >	<		>	
Export a certificate				

• Exportieren Sie das Zertifikat im pfx in den nachfolgenden Abschnitten formatieren. Verweisen Sie in diesem Artikel darauf, wie ein Zertifikat im pfx Format aus MMC:

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

- Sobald der Export des Zertifikats abgeschlossen ist, navigieren Sie zu Add/Remove Snap-in on MMC console. Klicken Sie auf Certificates und dann auf Add.
- Auswählen Service account und dann auf Next.

Certificates snap-in This snap-in will always manage certificates for: My user account Service account Computer account

- Im Select Computer Dialogfeld auswählen, Local Computer und klicke auf Next.
- Auswählen Active Directory Domain Services und dann auf Finish.

Certificat	tes snap-in
Select a service account to manage on the local	computer.
Service account:	
Active Directory Certificate Services	<u>^</u>
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

- Auf dem Add/Remove Snap-ins auf OK.
- Erweitern Certificates Services (Active Directory Domain Services) und dann auf NTDS\Personal.
- Rechtsklick NTDS\Personal,Klicken Sie auf All Tasks, und klicken Sie dann auf 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		

- Auf dem Certificate Import Wizard Willkommensbildschirm, auf Next.
- Klicken Sie im Bildschirm Zu importierende Datei auf Browse, und suchen Sie die Zertifikatsdatei, die Sie zuvor exportiert haben.
- Stellen Sie auf dem Bildschirm Öffnen sicher, dass Persönliche Informationen ausgetauscht werden (*pfx,*.p12) als Dateityp ausgewählt ist, und navigieren Sie dann im Dateisystem, um das zuvor exportierte Zertifikat zu suchen. Klicken Sie dann auf das Zertifikat.

	Oper	ı			x
€ 🗇 ▼ ↑ 📑 ▶ Lik	oraries + Documents		✓ 🖒 Search Do	cuments	Q
Organize 👻 New folder				•== •	
🔆 Favorites	Name	Date modified	Туре	Size	
Desktop	😼 ldapcert	4/25/2022 12:01	Personal Informati	5 KB	
🚺 Downloads 🖳 Recent places					
🥽 Libraries					
Documents					
J Music					
Pictures					
🖳 Videos					
File na	ame: Idapcert		✓ Personal	Information Exc	hange ∨
			Оре	n C	ancel

- Klicken Sie auf Open und dann auf Next.
- Geben Sie im Bildschirm Password (Kennwort) das Kennwort ein, das Sie für die Datei festgelegt haben, und klicken Sie dann auf Next.
- Stellen Sie auf der Seite Zertifikatspeicher sicher, dass Alle Zertifikate platzieren ausgewählt ist, und lesen Sie den Zertifikatspeicher: NTDS\Personal und dann auf Next.

€	Sertificate 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.
	O Automatically select the certificate store based on the type of certificate
	Iace all certificates in the following store
	Certificate store:
	NTDS\/Personal Browse
	Learn more about certificate stores
	Next Cancel

х

• Auf dem Certificate Import Wizard Vervollständigungsbildschirm, klicken Sie auf Finish. Daraufhin wird die Meldung angezeigt, dass der Import erfolgreich war. Klicken Sie auf OK. Es wird angezeigt, dass das Zertifikat unter dem Zertifikatspeicher importiert wurde: NTDS\Personal.

Console1 - [Console Root\Certific	ates - Service (Active Directory	Domain Services) on Local C	Computer\NTDS\Pe	ersonal\Certificates]	_ 🗆 X
藩 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.					

FMC-Konfigurationen

Lizenzierung überprüfen

Um die AnyConnect-Konfiguration bereitzustellen, muss der FTD beim Smart Licensing-Server registriert sein und eine gültige Plus-, Apex- oder VPN Only-Lizenz auf das Gerät angewendet werden.

Setup-Bereich

1. Navigieren Sie zu System > Integration. Navigieren Sie zu Realms, und klicken Sie dann auf Add Realm, wie in diesem Bild gezeigt:

Overview Analys	sis Policies Devices Obj	ects AMP Intelligence								%	Deploy Sy	stem Help 🔻	admin v
				Configuration	Users D	Domains	Integration	Updates	Licenses v	Logging v	Health •	¹ Monitoring *	Tools •
	3						2						
Cloud Services	Realms Identity Sou	ces High Availability	eStreamer Host Input 0	Client Smart Software Man	ager On-Pren	m							
Realms R	Realm Sequences Sync Re	sults											4
											Compa	re Realms Ad	d Realm
Name +	Description	Type	Domain	AD Primary Domai	0		Base DN				State		

 Füllen Sie die angezeigten Felder basierend auf den Informationen aus, die vom Microsoft-Server für LDAPs erfasst wurden. Importieren Sie zuvor das Zertifikat der Stammzertifizierungsstelle, das das LDAP-Dienstzertifikat auf dem Windows Server signiert hat unter Objects > PKI > Trusted CAs > Add Trusted CA, wie dies imDirectory Server Configuration des Bereichs. Klicken Sie abschließend auf OK.

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 V PKI	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	
 WIN-E3SKFJQD6J7.razor.local:636 	
Hostname/IP Address*	Port*
WIN-E3SKFJQD6J7.razor.local	636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT V +
Interface used to connect to Directory server (
Resolve via route lookup	
 Choose an interface 	
Default: Management/Diagnostic Interface	~
Test	

0 ×

3. Klicken Sie auf Test um sicherzustellen, dass FMC eine erfolgreiche Bindung mit dem im vorherigen Schritt angegebenen Benutzernamen und Kennwort für das Verzeichnis herstellen kann. Da diese Tests vom FMC und nicht über eine der im FTD konfigurierten routingfähigen Schnittstellen (z. B. intern, extern, dmz) initiiert werden, garantiert eine

erfolgreiche (oder fehlgeschlagene) Verbindung nicht dasselbe Ergebnis für die AnyConnect-Authentifizierung, da AnyConnect LDAP-Authentifizierungsanforderungen von einer der FTD-routingfähigen Schnittstellen initiiert werden.

Add Directory	@ ×
Hostname/IP Address* WIN-E3SKFJQD6J7.razor.loc	Port* 636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT V +
Interface used to connect to Dire	ctory server 👔
 Choose an interface 	
Default: Management/Diag	succeeded
	Cancel OK

4. Aktivieren des neuen Bereichs.

Overview Analy	ysis Policies Devices Objects	AMP Intelligence				n Deploy System Help + admir
				Configuration Users Domains	Integration Updates Licenses • Loggin	ng • Health • Monitoring • Too
Cloud Services	Realms Identity Sources	High Availability eStreame	r Host Input Client	Smart Software Manager On-Prem		
Realms	Realm Sequences Sync Results					
						Compare Realms Add Realm
Name +	Description	Туре	Domain	AD Primary Domain	Base DN	State
AC-Local		LOCAL	Global			🃼 Enabled 🛛 🛓 🖍 🖥 🖥
LDAP		AD	Global	cisco01.com	OU=Users,OU=CISCO,DC=cisco01,DC=com	🐑 Enabled 🛛 🛓 🖍 🖥 🖥
LDAP-Server		AD	Global	razor.local	DC=razor,DC=local	🐑 Enabled 🛛 🛓 🖍 🖥 🗑

AnyConnect für die Passwortverwaltung konfigurieren

1. Wählen Sie das vorhandene Verbindungsprofil aus, oder erstellen Sie ein neues, wenn es sich um eine Ersteinrichtung von AnyConnect handelt. Hier wird ein vorhandenes

Verbindungsprofil mit dem Namen "AnyConnect-AD" verwendet, das der lokalen Authentifizierung zugeordnet ist.

Overview Analysis Policies Devices Objects AMP Inte	lligence		🚹 Deploy System Help 🕶 admin 🕶
Device Management Device Upgrade NAT VPN > Remote Acc	QoS Platform Settings FlexConfig	Certificates	
AnyConnect Enter Description			Save Save
			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	/ 6
AnyConnect	Authentication: Radius (RADIUS) Authorization: Radius (RADIUS) Accounting: None	ChttGrpPolicy	/ 6
AnyConnect-AD	Authentication: LOCAL Authorization: None Accounting: None	🛅 AnyConnect-Group	/ 0

2. Bearbeiten Sie das Verbindungsprofil, und ordnen Sie den neuen LDAP-Server zu, der in den vorherigen Schritten unter den AAA-Einstellungen des Verbindungsprofils konfiguriert wurde. Klicken Sie abschließend auf Save in der rechten oberen Ecke.

CISCO Firepower Management Center Devices / VPN / Edit Connection Profile Overview	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🕥 admin 🔻
AnyConnect		Save Cancel
Enter Description		
Connection Dealer Assess Interfaces Advanced	Edit Connection Profile	Policy Assignments (1) Local Realm: None Dynamic Access Policy: Hostscan
Connection Prome Access intenaces Advanced	Connection Profile:* AnyConnect-AD	
	Group Policy:* AnyConnect-Group + +	+
Name	Edit Group Policy Client Address Assignment AAA Aliases	
DefaultWEBVPNGroup	Citerit Address Assignment Add Alases	11
	Authentication	
AnyConnect	Authentication Method: AAA Only	/1
AnyConnect-AD	Authentication Server: LDAP-Server (AD)	/i
	Fallback to LOCAL Authentication	
	Authorization	
	Authorization Server: Use same authentication server V	
	Allow connection only if user exists in authorization database	
	Accounting	
	Accounting Server:	
	 Advanced Settings 	
	Strip Realm from username	
	Cancel Save	

3. Passwortverwaltung unter dem AAA > Advanced Settings und speichert die Konfiguration.

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 X	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	

Bereitstellung

1. Klicken Sie nach Abschluss der Konfiguration aufDeploy -Taste oben rechts.

Overview Analysis Policies Devices Objects AMP Intelligence 🍕 Deploy System Help 🕶 admin 🔻			
	Overview Analysis Policies Devices Objects	5 AMP Intelligence	🗛 Deploy System Help 🕶 admin 💌

2. Klicken Sie auf das Kontrollkästchen neben der FTD-Konfiguration, die darauf angewendet wurde, und klicken Sie dann auf Deploy, wie in diesem Bild gezeigt:

Overview	Analysis Policies De	evices Objects	AMP Intelligence						Poploy System	Help 🔻 admin 🔻
									Deployment	Deployment History
२ वि	Search using device name	e, user name, type, gro	up or status						1 device s Deploy time:	Essimate Deploy
•	Device		Modified by	Inspect Interruption	Туре	Group	Last Deploy Time	Preview	Status	
> 🛛	10.197.224.190_FTD1		admin		FTD		May 30, 2022 7:34 AM	12	Pending	

Abschließende Konfiguration

Dies ist die Konfiguration, die Sie nach der erfolgreichen Bereitstellung in der FTD-CLI sehen.

AAA-Konfiguration

<#root>

> show running-config aaa-server

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

```
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

AnyConnect-Konfiguration

<#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

Verifizierung

Stellen Sie eine Verbindung mit AnyConnect her, und überprüfen Sie den Kennwortverwaltungsprozess für die Benutzerverbindung.

1. Stellen Sie eine Verbindung mit dem betreffenden Verbindungsprofil her. Sobald bei der erstmaligen Anmeldung festgestellt wird, dass das Kennwort geändert werden muss, da das frühere Kennwort vom Microsoft Server nach Ablauf zurückgewiesen wurde, wird der Benutzer aufgefordert, das Kennwort zu ändern.

S Cisco AnyConnect FTD-Hostname	×	
Group: Dev Utername: admin Password: [Cisco AnyConnect Secure Mobility Client - Vitie Contacting FTD Hostname. FTD Hostname Connect	
OK Canad		
Cisco AnyConnect FTD-Hostname	There a new Cisco AnyConnect Secure Mobility Client Cisco AnyConnect Secure Mobility Client VPIt Contacting FTD Hostname. FTD Hostname Contoue Contoue Contoue	
	Carlo Carlos Car	

2. Sobald der Benutzer das neue Kennwort für die Anmeldung eingegeben hat, wird die Verbindung erfolgreich hergestellt.

🚳 Cisco AnyC	onnect Secure Mobility Client		_		×
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconnec	t
00:02:43					IPv4
\$ (i)					altalta cisco

3. Überprüfen Sie die Benutzerverbindung der FTD-CLI:

<#root>

FTD_2# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : admin Index : 7 <----- Username, IP address assigned information of the client

Assigned IP : 10.1.x.x

:

Public IP : 10.106.xx.xx

Protocol

AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

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 25	5 2022		
Duration	:	Oh:00m:51s			
Inactivity	:	0h:00m:00s			
VLAN Mapping	:	N/A	VLAN	:	none
Audt Sess ID	:	0ac5e0fa000070006266a09	90		
Security Grp	:	none	Tunnel Zone	:	0

Fehlerbehebung

Fehlerbehebung

Dieses Debugging kann in der Diagnose-CLI ausgeführt werden, um Probleme im Zusammenhang mit der Kennwortverwaltung zu beheben: debug Idap 255.

Arbeiten mit Kennwortverwaltungsdebugs

```
<#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

Häufige Fehler bei der Kennwortverwaltung

Wenn die vom Microsoft Server festgelegte Kennwortrichtlinie während der Bereitstellung des neuen Kennworts durch den Benutzer nicht erfüllt wird, wird die Verbindung in der Regel mit der Fehlermeldung "Kennwort erfüllt nicht die Anforderungen der Kennwortrichtlinie" beendet. Stellen Sie daher sicher, dass das neue Kennwort der vom Microsoft Server für LDAPs festgelegten Richtlinie entspricht.

S Cisco AnyConn	ect FTD-Hostname	×			
Cannot con password p complexity,	mplete password change because the password does not meet the policy requirements. Check the minimum password length, password , and password history requirements.				
Group:	Dev 🗸	S Cisco Ar	nyConnect Secure Mobility Client - 🛛 🗙		
Username:	admin				
Password:			VPN: Cannot complete password change because the password does not meet the password policy requirements. Check		
	OK Cancel	_	FTD-Hostname V Connect		
		\$ ()	alada Cisco		
		Cisco Any	Connect	×	
		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		

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.