# FMC에서 관리하는 FTD의 RA VPN에 대해 LDAP를 사용하여 비밀번호 관리 구성

## 목차

<u>소개</u> 사전 요구 <u>사항</u> 요구 사항 사용되는 구성 요소 설정 네트워크 다이어그램 및 시나리오 LDAP 기본 DN 및 그룹 DN 결정 LDAPS SSL 인증서 루트 복사 LDAP 서버의 로컬 컴퓨터 저장소에 여러 인증서가 설치된 경우(선택 사항) FMC 컨피그레이션 라이센싱 확인 영역 설정 비밀번호 관리를 위한 AnyConnect 구성 구축 최종 컨피그레이션 AAA 컨피그레이션 AnyConnect 컨피그레이션 확인 AnyConnect에 연결하고 사용자 연결에 대한 비밀번호 관리 프로세스 확인 문제 해결 디버그 작동 중인 비밀번호 관리 디버그 비밀번호 관리 중에 발생하는 일반적인 오류

## 소개

이 문서에서는 Cisco FTD(Firepower Threat Defense)에 연결하는 AnyConnect 클라이언트에 대해 LDAP를 사용하여 비밀번호 관리를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

## 요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- FMC의 RA VPN(Remote Access Virtual Private Network) 구성에 대한 기본 지식
- FMC의 LDAP 서버 컨피그레이션에 대한 기본 지식

• Active Directory에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft 2012 R2 서버
- 7.3.0을 실행하는 FMCv
- 7.3.0을 실행하는 FTDv

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 설정

네트워크 다이어그램 및 시나리오



Windows 서버는 사용자 암호 관리 프로세스를 테스트하기 위해 ADDS 및 ADCS로 미리 구성되어 있습니다. 이 컨피그레이션 가이드에서는 이러한 사용자 계정을 생성합니다.

사용자 계정:

- 관리자: FTD가 Active Directory 서버에 바인딩될 수 있도록 디렉토리 계정으로 사용됩니다.
- admin: 사용자 ID를 시연하는 데 사용되는 테스트 관리자 계정입니다.

#### LDAP 기본 DN 및 그룹 DN 결정

1. 열기 Active Directory Users and Computers Server Manager Dashboard(서버 관리자 대시보드)를 클릭 합니다.

It Dashboard       WELCOME TO SERVER MANAGER         It Local Server       All Servers         AD CS       Image: Configure this local server         AD DS       Image: Configure this local server         Image: Configure this local server       Image: Configure this local server         Image: Configure this local server       Image: Configure this local server         Image: Configure this local server       Image: Configure this local server         Image: Configure this local server       Image: Configure this local server         Image: Configure this local server       Image: Configure this local server         Image: Configure this local server       Image: Configure this local server         Image: Configure this local server       Image: Configure this local server         Image: Configure this local server       Image: Configure this local server         Image: Configure this local server	igure this local server Id roles and features Id other servers to manage eate a server group E1 Image AD DS 1 Omega AD FS 1 Omega AD F	DNS 1 Manageability Events Services	Manage         Yow         Help           Active Directory Administrative Center         Active Directory Domains and Trusts         Active Directory Domains and Trusts           Active Directory Densins and Trusts         Active Directory Stells and Services         Active Directory Stells and Services           Active Directory Stells and Services         Active Directory Stells and Computers         AD FS Management           ADSI Edit         Component Services         Computers Services           Component Services         Dristication Authority           Component Services         Directory Management           Health Registration Authority         Internet Information Services (IIS) Manager           IGSI Initiator         Local Security Policy           Network Policy Server         ODBC Data Sources (32-bit)           ODBC Data Sources (32-bit)         ODBC Data Sources (34-bit)           Persource Monitor         Resource Monitor           Resource Monitor         Services           Seventy Configuration Wizard         Services
Services Performance BPA results	Events     Cvents       Services     Performance       BPA results     Services       Performance     BPA results       Image ability     Image ability       Events     Services       Performance     Performance       BPA results     Image ability       Events     Services       Performance     Performance       BPA results     BPA results	Cventa Cventa Services Performance BPA results All Servers 1 All Servers 1 Manageability Events Services Performance BPA results	Services System Configuration System Information Task Scheduler Windows Freenall with Advanced Security Windows PowerShell Windows PowerShell (80) Windows PowerShell (88) Windows PowerShell (88) Windows Server Backup
BPA results	BPA results BPA results	BPA results	to to Action Center to activate Windows.

2. 열기 View Option 을 활성화하여 Advanced Features, 이미지에 표시된 대로

	Active Dire	ectory Users and Computers	_ <b>□</b> X
File Action View	v Help		
🗢 🔿 🖄 [	Add/Remove Columns		
File     Action     View       Active Direc     Saved Q       Saved Q       Built       Built       Com       Built       Com       Man       Prog       System       Users       NTDS Que       TPM Devi	V Help Add/Remove Columns Large Icons Small Icons List Detail Users, Contacts, Groups, and Computers as containers Advanced Features Filter Options Customize Customize TPM Devices msTPM-Infor msTPM-Infor msTPM-Infor	ntainer for up ntainer for do ntainer for sec s ntainer for or ma ation for stor em settings 	
<	>		
Displays items in a list	t.		

3. 이렇게 하면 AD 개체 아래의 추가 속성을 볼 수 있습니다.

예를 들어, 루트에 대한 DN을 찾으려면 razor.local 마우스 오른쪽 버튼으로 클릭 razor.local을 선택 한 다음 Properties, 이 이미지에 표시된 대로

3	Active Directory Users and Computers	_ 🗆 X
File Action View Help		
🗢 🔿 📶 🔲 🖾 🔂 🖬 🖏 📚 🝃	i 7 🧕 🤽	
Active Directory Users and Com Saved Queries Saved Queries Built Saved Queries Delegate Control Built Delegate Control Delegate Control Delegate Control Delegate Control Change Domain Controller Delegate Control Find Change Domain Controller Delegate Control Find Change Domain Controller Derations Masters Derations	e Description tinDomain ner Default container for up zational Default container for od ner Default container for or sec JFound Default container for ma ner Default location for stor ner Builtin system settings ner Default container for up Quota Specifications co I-Infor uctureU	
Opens the properties dialog box for the current selection.		

4. 아래 Properties을 선택합니다. Attribute Editor 탭을 클릭합니다. 찾기 distinguishedName 속성 아래에서 View에 나와 있는 것처럼.

이렇게 하면 나중에 DN을 복사하여 FMC에 붙여넣을 수 있는 새 창이 열립니다.

이 예에서 루트 DN은 <sub>DC=razor</sub>, <sub>DC=local</sub>. 값을 복사하여 나중에 저장할 수 있습니다. 클릭 OK string Attribute Editor 창을 종료하고 OK 등록 정보를 종료하려면 다시 시도하십시오.

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	Attribute: distinguishedName				
Value:					
DC=razor,DC=local					
Clear	OK Cano	el			

## LDAPS SSL 인증서 루트 복사

1. 누르기 Win+R 및 입력 mmc.exe를 클릭한 다음 OK이 그림에 나와 있는 것처럼.



2. 탐색 File > Add/Remove Snap-in..., 이 이미지에 표시된 ss:

<b>a</b>	Console1 - [Console Root]	_ <b>_</b> ×
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		
1 C/Windows/outem22/dea		
2 C:\Windows\system32\eventywr		
3 C:\Windows\system32\certmgr		
4 C:\Windows\system32\certsrv		
Exit		
Enables you to add snap-ins to or remove them from the snap	p-in console.	

## 3. 사용 가능한 스냅인에서 Certificates 다음을 클릭합니다. Add, 이 이미지에 표시된 대로

ap-in	Vendor	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			Remove
Active Directory Site	Microsoft Cor			Genere
Active Directory Use	Microsoft Cor			
ActiveX Control	Microsoft Cor			Move Up
ADSI Edit	Microsoft Cor			Move Down
Authorization Manager	Microsoft Cor		Add >	Hove Bown
Certificate Templates	Microsoft Cor			
Certificates	Microsoft Cor			
ICertification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
"Disk Management	Mcrosoft and	~		Advanced

4. 선택 Computer account 다음을 클릭합니다. Next, 이 이미지에 표시된 대로

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

여기에 표시된 대로 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>Another computer:</li> <li>Browse</li> </ul> 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. 이제 oк이 그림에 나와 있는 것처럼.

Active Directory Do Mic Active Directory Site Mic Active Directory Use Mic	icrosoft Cor icrosoft Cor			LaP Certificates (Local Computer)	
Active Directory Site Mic Active Directory Use Mic	icrosoft Cor				Remove
Active Directory Use Mic					Genere
	icrosoft Cor				
ActiveX Control Mic	icrosoft Cor				Move Up
ADSI Edit Mic	icrosoft Cor				Move Down
Authorization Manager Mic	icrosoft Cor		<u>A</u> dd >		there goint
Certificate Templates Mic	icrosoft Cor		Provide statements		
Certificates Mic	crosoft Cor				
Certification Authority Mic	crosoft Cor				
Component Services Mic	crosoft Cor				
Device Managem Mic	crosoft Cor				
Disk Management Mic	icrosoft and	~			Ad <u>v</u> anced

- 6. 를 펼칩니다. Personal 폴더를 클릭한 다음 Certificates. LDAP에서 사용하는 인증서는 Windows 서 버의 FQDN(Fully Qualified Domain Name)에 발급해야 합니다. 이 서버에는 세 가지 인증서가 나열됩니다.
- CA 인증서는 razor-WIN-E3SKFJQD6J7-CA.
- 에 의해 발급된 CA 인증서 supinfo-WIN-FNJVP9QUEH9-CA.
- ID 인증서가 WIN-E3SKFJQD6J7.razor.local 에 의해 razor-WIN-E3SKFJQD6J7-CA.

이 컨피그레이션 가이드에서 FQDN은 WIN-E3SKFJQD6J7.razor.local 따라서 처음 두 인증서는 LDAPs SSL 인증서로 사용할 수 없습니다. 발급된 ID 인증서 WIN-E3SKFJQD6J7.razor.local 은(는) Windows Server CA 서비스에서 자동으로 발급한 인증서입니다. 세부 정보를 확인하려면 인증서를 두 번 클릭합니다.



- 7. LDAPs SSL 인증서로 사용하려면 인증서가 다음 요구 사항을 충족해야 합니다.
- 공용 이름 또는 DNS 주체 대체 이름이 Windows Server의 FQDN과 일치합니다.
- 인증서에는 Enhanced Key Usage(고급 키 사용) 필드 아래에 서버 인증이 있습니다.

아래 Details 인증서의 탭에서 Subject Alternative Name여기서 FQDN은 WIN-E3SKFJQD6J7.razor.local 이(가) 있습니다.

Cer	tificate ×				
General Details Certification Path					
Show (All)					
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 V				
DNS Name = WIN-E3SKFJQD6J7.razor.local DNS Name = razor.local DNS Name = RAZOR					
Ec Learn more about <u>certificate details</u>	dit Properties Copy to File				
	ОК				

아래 Enhanced Key Usage, Server Authentication 이(가) 있습니다.

📃 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)				
Ec Learn more about <u>certificate details</u>	dit Properties Copy to File			
	ОК			

8. 확인되시면, Certification Path 탭에서 루트 CA 인증서인 최상위 인증서를 선택한 다음 View Certificate. 그러면 이미지에 표시된 것처럼 루트 CA 인증서에 대한 인증서 세부사항이 열립니다.

R Certificate	x	Certificate X
General Details Certification Path Certification path arazor-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.		Valid from 3/22/2021 to 3/22/2026
Learn more about <u>certification paths</u>		Learn more about <u>certificates</u>
ОК		OK

9. 아래 Details 루트 CA 인증서의 탭에서 Copy to File Cisco의Certificate Export Wizard PEM 형식으로 루트 CA를 내보냅니다.

선택 Base-64 encoded X.509 파일 형식으로

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\roc	
	Export Keys	No	
	Include all certificates in the certification path	No	
	File Format	Base64 Encoded X.509 (*.cer)	
	< 111	>	
_			
		Finish Can	cel

10. 메모장이나 다른 텍스트 편집기를 사용하여 시스템의 선택한 위치에 저장된 루트 CA 인증서 를 엽니다.

PEM 형식 인증서가 표시됩니다. 나중에 사용할 수 있도록 저장하십시오.

----BEGIN CERTIFICATE-----

MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgo vcjEhMB8GA1UEAxMYcmF6b3ItV010LUUzU0tGS1FENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCgr BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvc CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnb1xwtX0B2G4UxZ3LRrWznjXaS02Rc3qVw41nOAziGs4ZMNM1X8UWeKuwi8 9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU30aiiI/tp422ydy3Kg17Iqt1s4XqpZmTezykWra7dUyXfkuESk61E0AV CSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhuj1x4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwE DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00BBYEFM+DkqQUA0dY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSI AA4IBAQCiSm5U7U6Y7zXdx+d1eJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7Bn06f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q 4sMZffbVrG1Rz7twWY36J5G5vhNUhzZ1N20Lw6wtHg2S08X1vpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nry1b GuDsepY7/u2uWfy/vpTJigeok2DH6HFf0ET3sE+7rsIAY+of0kWW5gNwQ4h0wv4Goqj+YQRAXXi2OZy1tHR1dfUUbwVENSFQtDnFA7X

#### LDAP 서버의 로컬 컴퓨터 저장소에 여러 인증서가 설치된 경우(선택 사항)

1. LDAPS에서 사용 할 수 있는 여러 ID 인증서의 경우 및 사용 할 수 있는 불확실성이 있거나 LDAPS 서버에 액세스 할 수 없는 경우, FTD에서 수행 한 패킷 캡처에서 루트 CA를 추출 할 수 있 습니다.

2. LDAP 서버(예: AD DS 도메인 컨트롤러) 로컬 컴퓨터 인증서 저장소에 서버 인증에 유효한 인증 서가 여러 개 있는 경우 LDAPS 통신에 다른 인증서가 사용된다는 것을 알 수 있습니다. 이러한 문 제의 가장 좋은 해결책은 로컬 컴퓨터 인증서 저장소에서 불필요한 인증서를 모두 제거하고 서버 인증에 유효한 인증서를 하나만 갖는 것입니다.

그러나 둘 이상의 인증서가 필요하고 Windows Server 2008 LDAP 서버가 하나 이상 있는 합당한 이유가 있는 경우 LDAP 통신에 Active Directory 도메인 서비스(NTDS\개인) 인증서 저장소를 사용 할 수 있습니다.

이 단계에서는 도메인 컨트롤러 로컬 컴퓨터 인증서 저장소에서 Active Directory 도메인 서비스 서비스 인증서 저장소(NTDS\Personal)로 LDAPS 지원 인증서를 내보내는 방법을 보여 줍니다.

- Active Directory 서버에서 MMC 콘솔로 이동하여 파일을 선택한 다음 Add/Remove Snap-in.
- 클릭 Certificates 다음을 클릭합니다. Add.
- 의 Certificates snap-in, 선택 Computer account 다음을 클릭합니다. Next.
- 수신 Select Computer, 선택 Local Computer, 클릭 OK을 클릭한 다음 Finish. 수신 Add or Remove Snap-ins, 클릭 OK.
- 서버 인증에 사용되는 인증서가 들어 있는 컴퓨터의 인증서 콘솔에서 certificate, 클릭 All Tasks을 클릭한 다음 Export.

<b>a</b> (	Console1 - [Console Root\Certifi	cates (Local Computer)\Pers	onal\Certificates]	_ <b>D</b> X
🖀 File Action View Favorites Window	v 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 Certificates	supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	2/23/2025	More Actions
Trusted Root Certification Autho		Open		WINI-E3SKEIOD617 razor local
▷ Control Enterprise Trust		All Tas	ks 🕨 Op	ben
Intermediate Certification Autno Trusted Publishers		Cut	Re	quest Certificate with New Key
Untrusted Certificates		Сору	Re	new Certificate with New Key
Third-Party Root Certification Au		Delete	M	anage Private Kevs
Trusted People		Proper	ties Ad	Ivanced Operations
Other People		Help	Ev	nort
Remote Desktop		( indep		
Certificate Enrollment Requests				
Smart Card Trusted Roots Trusted Devices				
▷ I Web Hosting ✓				
< III >	< III		>	
Export a certificate				

• 에서 인증서 내보내기 pfx 다음 섹션에서 형식을 지정합니다. 에서 인증서를 내보내는 방법에 대한 이 문서를 참조하십시오. pfx MMC에서 형식:

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

- 인증서 내보내기가 완료되면 Add/Remove Snap-in **ON** MMC console. 클릭 Certificates 다음을 클릭합니다. Add.
- 선택 Service account 다음을 클릭합니다. Next.

## Certificates snap-in

х

This snap-in will always manage certificates for:

- My user account
- Service account
- Computer account
- 의 Select Computer 대화 상자에서 Local Computer 을 클릭하고 Next.
- 선택 Active Directory Domain Services 다음을 클릭합니다. Finish.

Certificates sn	ap-in 🗙
Select a service account to manage on the local comput	er.
Service account: 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 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

- 에 Add/Remove Snap-ins 대화 상자에서 OK.
- Expand Certificates Services (Active Directory Domain Services) 다음을 클릭합니다. NTDS\Personal.
- 마우스 오른쪽 단추 클릭 NTDS\Personal, 클릭 All Tasks을 클릭한 다음 Import.

Console1 - [Console I	oot\Certificates - Service (Active Directory Domain Services) on Local Comp	uter\NTDS\Personal] 🔄 🗖 🗙
🚟 File Action View Favorites Windov	Help	_ 8 ×
🗢 🄿 🗖 🖬 📋 🗟 🖬		
Console Root	Object Type	Actions
Certificates (Local Computer)	Certificates	NTDS\Personal
Certificates - Service (Active Directory D		More Actions
▷ I NT Find Certificates		
▷ 🛄 NT All Tasks	Find Certificates	
D NT View	Import	
▷ 🖺 NT New Window from Here	Advanced Operations	
New Taskpad View		
NT Refresh		
Export List		
Help		
Add a certificate to a store		

- 에 Certificate Import Wizard 시작 화면에서 Next.
- 가져올 파일 화면에서 Browse을 누르고 이전에 내보낸 인증서 파일을 찾습니다.
- Open(열기) 화면에서 개인 정보 교환(\*pfx,\*.p12)가 파일 유형으로 선택된 다음 파일 시스템을 탐색하여 이전에 내보낸 인증서를 찾습니다. 그런 다음 해당 인증서를 클릭합니다.

-	Oper	n			x
€ 💿 ▾ ↑ 📑 ኑ Libr	raries + Documents	✓ ♂ Search D	ocuments	Q	
Organize 🔻 New folder				•	
🔆 Favorites	Name	Date modified	Туре	Size	
Desktop	😼 Idapcert	4/25/2022 12:01	Personal Informati	5 KB	
i Downloads					
🥽 Libraries					
Documents					
J Music					
Pictures					
M Videos					
🗣 Network					
File na	me: Idapcert		✓ Persona	I Information Exchan	ge 🗸
			Ор	en Cance	el 🛛

- 클릭 Open 다음을 클릭합니다. Next.
- 암호 화면에서 파일에 대해 설정한 암호를 입력한 다음 Next.
- Certificate Store(인증서 저장소) 페이지에서 Place all certificates(모든 인증서 가져오기)가 선 택되어 있는지 확인하고 Certificate Store(인증서 저장소)를 읽습니다. NTDS\Personal 다음을 클릭 합니다. Next.

€	🔗 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.						
	O 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

• 에 Certificate Import Wizard 완료 화면에서 Finish. 그러면 가져오기가 성공했다는 메시지가 표시됩니다. 클릭 OK. 다음과 같이 인증서 저장소 아래에서 인증서를 가져왔습니다. NTDS\Personal.

Console1 - [Console Root\Certific	ates - Service (Active Directory	Domain Services) on Local C	omputer\NTDS\P	ersonal\Certificates]	- 🗆 X
藩 File Action View Favorites Window	v 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)	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	•
⊿ NIDS\Personal				More Actions	,
NTDS\Trusted Boot Certification Au				WIN-E3SKFJQD6J7.r	azor.local 🔺
NTDS\Enterprise Trust				More Actions	•
NTDS\Intermediate Certification Au					
NTDS\Trusted Publishers					
NTDS\Untrusted Certificates					
NTDS\Third-Party Root Certification					
INTDS\Trusted People					
NIDS\Client Authentication Issuers					
< III >	<		>		
NTDS\Personal store contains 2 certificates.					

### FMC 컨피그레이션

#### 라이센싱 확인

AnyConnect 컨피그레이션을 구축하려면 FTD를 Smart Licensing Server에 등록하고 유효한 Plus, Apex 또는 VPN Only 라이센스를 디바이스에 적용해야 합니다.

#### 영역 설정

1. 탐색 System > Integration. 탐색 Realms를 클릭한 다음 Add Realm, 이 이미지에 표시된 대로

Overview Analys	sis Policies Devices Objects	AMP Intelligence								<u>e</u> 1	Deploy Syst	em Help 🔻	admin 🔻
				Configuration	Users	Domains	Integration	Updates	Licenses <b>v</b>	Logging •	Health v 1	Monitoring •	Tools •
	3						2						
Cloud Services	Realms Identity Sources	High Availability eStre	eamer Host Input Client	Smart Software Mana	ger On-Pro	em							
Realms R	Realm Sequences Sync Results												4
											Compare	Realms	I Realm
Name +	Description	Туре	Domain	AD Primary Domain	1		Base DN				State		

2. LDAP용 Microsoft 서버에서 수집된 정보를 기반으로 표시된 필드를 입력합니다. 이 전에 Windows Server의 LDAP 서비스 인증서에 서명한 루트 CA 인증서를 Objects > PKI > Trusted CAs > Add Trusted CA에서 참조되는 대로Directory Server Configuration Realm의 약어입니다 작업을 마치면 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 V						
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-E3SKFJQD6J7.razor.local	636					
Encryption	CA Certificate*					
LDAPS	LDAPS-ROOT-CERT V +					
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						

 $0 \times$ 

3. 클릭 Test FMC가 이전 단계에서 제공한 디렉토리 사용자 이름 및 비밀번호로 성공적으로 바인 딩할 수 있도록 하려면 다음을 수행합니다. 이러한 테스트는 FTD에 구성된 라우팅 가능한 인 터페이스(예: 내부, 외부, dmz)를 통하지 않고 FMC에서 시작되므로, AnyConnect LDAP 인증 요청이 FTD 라우팅 가능한 인터페이스 중 하나에서 시작되므로 연결에 성공하거나 실패하더 라도 AnyConnect 인증에 대한 동일한 결과가 보장되지 않습니다.

Add Directory	@ ×
Hostname/IP Address* WIN-E3SKFJQD6J7.razor.loc	Port* 636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT V +
<ul> <li>Interface used to connect to Dire</li> <li>Resolve via route lookup</li> <li>Choose an interface</li> <li>Default: Management/Diag</li> <li>Test</li> </ul>	ectory server i
	Cancel OK

#### 4. 새 영역을 활성화합니다.

Overview Anal	lysis Policies Devices Objects	AMP Intelligence					<b>%</b>	Deploy System	Help v admin v
				Configuration Users	Domains In	ntegration Updates	Licenses • Logging •	Health • M	Ionitoring • Tools •
Cloud Service	es Realms Identity Sources	High Availability eStreame	r Host Input Client	Smart Software Manager On-F	Prem				
Realms	Realm Sequences Sync Results								
								Compare R	ealms Add Realm
Name +	Description	Туре	Domain	AD Primary Domain		Base DN		State	
AC-Local		LOCAL	Global					Enabled	土 🦯 🖬 🗑
LDAP		AD	Global	cisco01.com		OU=Users,OU=CISCO,DO	C=cisco01,DC=com	Enabled	<u>+ / %</u> ¥
LDAP-Server		AD	Global	razor.local		DC=razor,DC=local		Enabled	±/5

비밀번호 관리를 위한 AnyConnect 구성

1. AnyConnect의 초기 설정인 경우 기존 연결 프로파일을 선택하거나 새 프로파일을 생성합니 다. 여기서는 로컬 인증과 매핑된 'AnyConnect-AD'라는 기존 연결 프로파일을 사용합니다.

Overview Analysis Policies Devices Objects AMP Inte	elligence		🇛 Deploy System Help 🕶 admin 🕶
Device Management Device Upgrade NAT VPN > Remote Acc	Cess 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	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy	/ 5
AnyConnect	Authentication: Radius (RADIUS) Authorization: Radius (RADIUS) Accounting: Mone	DftGrpPolicy	/ 5
AnyConnect-AD	Authentication: LOCAL Authorization: Mone Accounting: Mone	AnyConnect-Group	/ 0

2. 연결 프로파일을 편집하고 이전 단계에서 구성한 새 LDAP 서버를 연결 프로파일의 AAA 설정 에서 매핑합니다. 작업을 마치면 Save 오른쪽 상단 구석에 있습니다

High: Firepower Management Center Devices / VPN / Edit Connection Profile	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🙆 admin 🔻
AnyConnect Enter Description		Save Cancel 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 Circup Palicy Client Address Assignment AAA Aliases	
DefaultWEBVPNGroup	Authentication	/1
AnyConnect	Authentication Method: AAA Only	/1
AnyConnect-AD	Authentication Server: LDAP-Server (AD)   Fallback to LOCAL Authentication	×1
	Use secondary authentication	
	Authorization	
	Authorization Server: Use same authentication server	
	Accounting	
	Accounting Server:	
	Strip Realm from username	
	Cancel Save	

3. 비밀번호 관리 활성화 AAA > Advanced Settings 구성을 저장합니다.

Overview Analysis Policies Devices Objects   AMP Intellig	ence	🍕 Deploy System Help 🕶 admin 🕶
AnyConnect Enter Description	Qos Platform Settings Plex.comg Certificates	Save Cancel
		Policy Assignments (1) Local Realm: asa Dynamic Access Policy: <u>Hostscan</u>
Connection Profile Access Interfaces Advanced	Edit Connection Profile ? ×	
Name	Connection Profile:* AnyConnect-AD Group Policy:* AnyConnect-Group Idit Group Policy: ©	0
DefaultWEBVPNGroup	Client Address Assignment	/ 9
	Circle Address Assignment Addr. Anases	
AnyConnect	EDAP-Server (AD)     Fallback to LOCAL Authentication	/ 6
Inclusion 4D	Use secondary authentication	25
AnyConnectWD	Authorization	~0
sjobs	Authorization Server: Use same authentication server  Childrew connection only if user exists in authorization database Configure LDAP Attribute Hap	/8
	Accounting	
	Accounting Server:	
	Advanced Settings	
	Strip Realm from username	
	Stip Group from username     Zenable Password Management	
	Notify User     days prior to password expiration	
	O Notify user on the day of password expiration	
	Save Cancel	

#### 구축

1. 모든 컨피그레이션이 완료되면<sub>Deploy</sub> 버튼을 누르시면 됩니다.

## Overview Analysis Policies Devices Objects AMP Intelligence 🍨 🖓 Deploy System Help \* admin \*

2. 적용된 FTD 컨피그레이션 옆의 확인란을 클릭한 다음 Deploy, 이 이미지에 표시된 대로

Overview Analysis	olicies Devices Objects AM	P Intelligence						艂 Deploy System Help 🔻 admin 🕶
								Deployment Deployment History
♥ Q Search usin	device name, user name, type, group (	or status						1 device selected Deploy time: Estimato
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

## 최종 컨피그레이션

성공적인 구축 후 FTD CLI에 표시되는 컨피그레이션입니다.

AAA 컨피그레이션

#### <#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 컨피그레이션

#### <#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

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>

<---- LDAPs Serve

<---- Protocol

<---- Password-management

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

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

## 확인

## AnyConnect에 연결하고 사용자 연결에 대한 비밀번호 관리 프로세스 확인

1. 관련 연결 프로파일에 대한 연결을 시작합니다. 최초 로그인 시 이전 비밀번호가 만료되어 Microsoft Server에서 거부되었으므로 비밀번호를 변경해야 한다고 판단되면 사용자에게 비밀번호 변경 프롬프트가 표시됩니다.



New Password:		
Verify Password:		
Password change required, you must enter a new password with a minimum length of 7 to continue.	😚 Cisco AnyConnect Secure Mobility Client — 🛛 🗙	
	Contacting FTD-Hostname.	
Continue Cancel	FTD-Hostname V Continue	
	to 🛈 esco	
a second s		

2. 사용자가 로그인을 위해 새 비밀번호를 입력하면 연결이 성공적으로 설정됩니다.

S Cisco AnyConnect Secure Mobility Client			-		×
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconnec	t
00:02:43					IPv4
<b>¢</b> ()					diala cisco

3. FTD CLI에서 사용자 연결을 확인합니다.

#### <#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 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Hashing Bytes Rx Bytes Tx : 16316 : 2109 Group Policy : AnyConnect-Group Tunnel Group : AnyConnect-AD Login Time : 13:22:24 UTC Mon Apr 25 2022 Duration : 0h:00m:51s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0ac5e0fa000070006266a090 Security Grp : none Tunnel Zone : 0

## 문제 해결

#### 디버그

이 디버그는 진단 CLI에서 실행하여 비밀번호 관리 관련 문제를 해결할 수 있습니다. debug ldap 255.

#### 작동 중인 비밀번호 관리 디버그

#### <#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.].LH.....9.4
- [25] userAccountControl: value = 512
- [25] badPwdCount: value = 3
- [25] codePage: value = 0
- [25] countryCode: value = 0
- [25] badPasswordTime: value = 132610388348662803
- [25] lastLogoff: value = 0

- [25] lastLogon: value = 132484577284881837
- [25] pwdLastSet: value = 0
- [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] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=razor,DC=local
- [25] dSCorePropagationData: value = 20220425125800.0Z
- [25] dSCorePropagationData: value = 20201029053516.0Z
- [25] dSCorePropagationData: value = 16010101000000.0Z
- [25] lastLogonTimestamp: value = 132953506361126701
- [25] msDS-SupportedEncryptionTypes: value = 0
- [25] uid: value = \*\*\*\*\*@razor.local
- [25] Fiber exit Tx=714 bytes Rx=2683 bytes, status=1
- [25] Session End

#### 비밀번호 관리 중에 발생하는 일반적인 오류

일반적으로 사용자가 새 암호를 제공하는 동안 Microsoft Server에서 설정한 암호 정책이 충족되지 않으면 "암호가 암호 정책 요구 사항을 충족하지 않습니다."라는 오류 메시지와 함께 연결이 종료됩 니다. 따라서 새 비밀번호가 LDAP에 대해 Microsoft Server에서 설정한 정책에 부합하는지 확인합 니다.

Sisco AnyConne	ect I FTD-Hostname X		
Cannot com password p complexity,	inglet password change because the password does not meet the olicy requirements. Check the minimum password length, password , and password history requirements.		
Group:	Dev 🗸	🕙 Cisco AnyConnect Secure Mobility Client — 🗆 🗙	
Username:	admin		
Password:		Cannot complete password change because the password does not meet the password policy requirements. Check	
	OK Cancel	FTD-Hostname v Connect	
		O este	
		Cisco AnyConnect X	
		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	

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.