# AnyConnect 클라이언트에 대해 FMC에서 관리하 는 FTD에서 AD(LDAP) 인증 및 사용자 ID 설정

## 목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 구성 네트워크 다이어그램 및 시나리오 Active Directory 구성 LDAP 기본 DN 및 그룹 DN 결정 FTD 어카운트 생성 AD 그룹 생성 및 AD 그룹에 사용자 추가(선택 사항) LDAPS SSL 인증서 루트 복사(LDAPS 또는 STARTTLS에만 필요) FMC 컨피그레이션 라이센싱 확인 영역 설정 AD 인증을 위해 AnyConnect 구성 ID 정책 활성화 및 사용자 ID에 대한 보안 정책 구성 NAT 예외 구성 구축 다음을 확인합니다. 최종 컨피그레이션 AAA 컨피그레이션 AnyConnect 컨피그레이션 AnyConnect로 연결 및 액세스 제어 정책 규칙 확인 FMC 연결 이벤트로 확인 문제 해결 디버그 LDAP 디버깅 작업 LDAP 서버와의 연결을 설정할 수 없음 로그인 DN 및/또는 비밀번호 바인딩이 잘못되었습니다. LDAP 서버가 사용자 이름을 찾을 수 없음 사용자 이름에 대한 잘못된 비밀번호 테스트 AAA 패킷 캡처 Windows Server 이벤트 뷰어 로그

소개

이 문서에서는 Cisco FTD(Firepower Threat Defense)에 연결하는 AnyConnect 클라이언트에 대해 AD 인증을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC의 RA VPN 구성에 대한 기본 지식
- FMC의 LDAP 서버 컨피그레이션에 대한 기본 지식
- AD(Active Directory)에 대한 기본 지식

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft 2016 서버
- 6.5.0을 실행하는 FMCv
- 6.5.0을 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.

#### 배경 정보

이 문서에서는 FMC(Firepower **Management Center**)에서 관리하는 **Cisco FTD(Firepower Threat Defense)에 연결하**는 AnyConnect 클라이언트에 대해 **AD(Active Directory) 인증**을 구성하는 방법 에 대해 설명합니다.

사용자 ID는 액세스 정책에서 AnyConnect 사용자를 특정 IP 주소 및 포트로 제한하는 데 사용됩니 다.

## 구성

### 네트워크 다이어그램 및 시나리오



Windows 서버는 사용자 ID를 테스트하기 위해 IIS 및 RDP로 미리 구성되어 있습니다. 이 컨피그레 이션 가이드에서는 3개의 사용자 계정과 2개의 그룹이 생성됩니다.

사용자 계정:

• FTD 관리: FTD가 Active Directory 서버에 바인딩될 수 있도록 디렉토리 계정으로 사용됩니다.

- IT 관리자: 사용자 ID를 시연하는 데 사용되는 테스트 관리자 계정입니다.
- 테스트 사용자: 사용자 ID를 시연하는 데 사용되는 테스트 사용자 계정입니다.

#### 그룹:

- AnyConnect 관리자: 사용자 ID를 시연하기 위해 IT 관리자가 추가하는 테스트 그룹입니다. 이 그룹에는 Windows Server에 대한 RDP 액세스만 있습니다.
- AnyConnect Users(AnyConnect 사용자): 사용자 ID를 입증하기 위해 Test User(사용자 테스트)가 추가된 테스트 그룹입니다. 이 그룹에는 Windows Server에 대한 HTTP 액세스만 있습니다.

#### Active Directory 구성

FTD에서 AD 인증 및 사용자 ID를 적절하게 구성하려면 몇 가지 값이 필요합니다.

FMC에서 컨피그레이션을 수행하려면 먼저 Microsoft Server에서 이 모든 세부 정보를 만들거나 수 집해야 합니다. 주요 값은 다음과 같습니다.

#### • 도메인 이름:

서버의 도메인 이름입니다. 이 컨피그레이션 가이드에서 example.com은 도메인 이름입니다.

#### • 서버 IP/FQDN 주소:

Microsoft 서버에 연결하는 데 사용되는 IP 주소 또는 FQDN. FQDN을 사용하는 경우 FQDN을 확인 하려면 FMC 및 FTD 내에서 DNS 서버를 구성해야 합니다.

이 컨피그레이션 가이드에서 이 값은 win2016.example.com(192.168.1.1로 확인됨)입니다.

#### • 서버 포트:

LDAP 서비스에서 사용하는 포트. 기본적으로 LDAP 및 STARTTLS는 LDAP에 TCP 포트 389를 사용하고 LDAP over SSL(LDAPS)은 TCP 포트 636을 사용합니다.

#### • 루트 CA:

LDAPS 또는 STARTTLS를 사용하는 경우 LDAPS에서 사용하는 SSL 인증서에 서명하는 데 사용 되는 루트 CA가 필요합니다.

#### • 디렉토리 사용자 이름 및 비밀번호:

FMC 및 FTD가 LDAP 서버에 바인딩하고 사용자를 인증하며 사용자 및 그룹을 검색하는 데 사용하 는 계정입니다.

FTD Admin이라는 이름의 어카운트가 이 용도로 생성됩니다.

#### • 기본 및 그룹 DN(고유 이름):

기본 DN은 FMC의 시작점이며 FTD는 Active Directory에 사용자 검색을 시작하고 인증하도록 지시 합니다.

마찬가지로, 그룹 DN은 FMC가 Active Directory에 사용자 ID에 대한 그룹 검색을 시작할 위치를 알 려주는 시작점입니다.

이 컨피그레이션 가이드에서는 루트 도메인 example.com이 Base DN 및 Group DN으로 사용됩니다.

그러나 프로덕션 환경에서는 LDAP 계층 내에서 Base DN 및 Group DN을 더 많이 사용하는 것이 좋습니다.

예를 들어, 이 LDAP 계층 구조는 다음과 같습니다.



관리자가 Marketing 조직 단위의 사용자가 기본 DN을 인증할 수 있도록 하려는 경우 루트 (example.com)로 설정할 수 있습니다.

그러나 Finance 조직 단위의 User1도 로그인할 수 있습니다. 사용자 검색이 루트에서 시작되어 Finance, Marketing 및 Research로 내려가기 때문입니다.

기본 DN이 example.com으로 설정됩니다.



**Marketing** 조직 단위 이하의 유일한 사용자에 대한 로그인을 제한하기 위해, 관리자는 대신 기본 DN을 Marketing으로 설정할 수 **있습니다**.

이제 Marketing에서 검색이 시작되므로 User2 및 User3만 인증할 수 **있습니다**.

기본 DN을 마케팅으로 설정



사용자가 연결할 수 있는 FTD 내에서 보다 세분화된 제어를 수행하거나 AD 특성에 따라 다른 권한 부여를 할당하려면 LDAP 권한 부여 맵을 구성해야 합니다. 이에 대한 자세한 내용은 FTD(Firepower <u>Threat Defense)에서 AnyConnect LDAP 매핑을 구성하십</u> <u>시오</u>.

이 간소화된 LDAP 계층 구조는 이 컨피그레이션 가이드에서 사용되며 루트 example.com의 DN은 Base DN 및 Group DN 모두에 사용됩니다.



LDAP 기본 DN 및 그룹 DN 결정

1. Active Directory 사용자 및 컴퓨터를 엽니다.

=	Best match
ŵ	Active Directory Users and Computers Desktop app
	Settings >
	8 Edit local users and groups
	陀 Change User Account Control settings
	8 User Accounts
	Select users who can use remote desktop
۲	
	users
-	ዶ 🗆 🧀 🔚 🛽

2. **루트 도메인**을 마우스 왼쪽 단추로 클릭하고(컨테이너를 열려면) **루트 도메인**을 마우스 오른쪽 단추로 클릭한 다음 **보기**에서 **고급** 기능을 **클릭합니다**.



3. 이렇게 하면 AD 개체 아래의 추가 속성을 볼 수 있습니다. 예를 들어, 루트 example.com에 대한 DN을 찾으려면 example.com을 마우스 오른쪽 버튼으로 클릭한 다음 Properties(속성)를 **선택합니 다**.



4. 등록 **정보**에서 속성 편집기 **탭을** 선택합니다. Attributes(**특성)** 아래에서 **distinguishedName**을 찾 은 다음 View(**보기)를 클릭합니다**.

example.com Properties		?	х
General Managed By O	bject Security Attribute Editor		
Attributes:			
Attribute	Value		^
dc	example		
defaultLocalPolicyObj	<not set=""></not>		
description	<not set=""></not>		
desktopProfile	<not set=""></not>		
displayName	<not set=""></not>		
displayNamePrintable	(not set)		
distinguishedName	DC=example.DC=com		
domainPolicyObject	<not set=""></not>		
domainReplica	<not set=""></not>		
dSASignature	{ V1: Flags = 0x0; LatencySecs =	0; DsaGui	c
dSCorePropagationD	0x0 = ( )		
eFSPolicy	<not set=""></not>		
extensionName	<not set=""></not>		
flags	<not set=""></not>		~
<		>	
View	[	Filter	
ОК	Cancel Apply	He	þ

5. 이렇게 하면 나중에 DN을 복사하여 FMC에 붙여넣을 수 있는 새 창이 열립니다. 이 예에서 루트 DN은 DC=example,DC=com입니다.

값을 복사하여 나중에 저장할 수 있습니다. OK(**확인**)를 클릭하여 String Attribute Editor(문자열 특 성 편집기) 창을 종료하고 OK(확인)를 다시 클릭하여 Properties(**속성)를 종료합니다**.

tring Attribute Editor		×		
ttribute: distingui	shedName			
alue: DC=example,DC=com Clear	ок	Cancel	Undo Cut Copy	
			Paste Delete Select All	
			Right to left Reading order Show Unicode control characters Insert Unicode control character	;
ample.com Properties Seneral Managed By O Attributes:	bject Security Attribute Edit	? ×		
Attribute cn controlAccessRights creationTime dc defautLocalPolicyObj description desktopProfile displayName d	Value (not set> 4/29/2020 2:43:49 PM Easter example (not set> (not set> (not set> (not set> (not set> DC=example,DC=com (not set> (not set> (N	m Daylight Tim :s = 0; DsaGuic >		
Vew	Cancel Apply	Filter		

Active Directory 내의 여러 개체에 대해 이 작업을 수행할 수 **있습니다**. 예를 들어, 다음 단계는 **사용 자** 컨테이너의 DN을 찾는 데 사용됩니다.



6. Advanced Features(고급 기능) 보기는 루트 DN을 마우스 오른쪽 단추로 다시 누른 다음 보기 아 래에서 Advanced Features(고급 기능)를 한 번 더 눌러 제거할 수 있습니다.



#### FTD 어카운트 생성

이 사용자 계정은 FMC 및 FTD가 사용자 및 그룹을 검색하고 사용자를 인증하기 위해 Active Directory에 바인딩할 수 있도록 합니다.

별도의 FTD 어카운트를 만드는 목적은 바인딩에 사용된 자격 증명이 손상된 경우 네트워크 내의 다 른 위치에서 무단 액세스를 방지하기 위한 것입니다.

이 계정은 기본 DN 또는 그룹 DN의 범위에 속할 필요가 없습니다.

1. Active Directory 사용자 및 컴퓨터에서 FTD 계정이 추가된 컨테이너/조직을 마우스 오른쪽 단추 로 클릭합니다.

이 컨피그레이션에서 FTD 어카운트는 사용자 이름 ftd.admin@example.com**의 Users** 컨테이너 아 래에 <u>추가됩니다.</u>

사용자를 마우스 오른쪽 **버튼**으로 클릭한 다음 **새로 만들기 > 사용자**로 **이동합니다**.

Active Directory	Users and Com	puters				-	×
File Action View	w Help						
🗢 🔿 📶	1 🖬 🗙 🛛	0 🔒 🛛	Þ	1 🗏 🐮 🕅 🦷	r 🗾 🔍		
Active Directory	Users and Com is Controllers ecurityPrincipal: Service Accour Delegate Con Find New All Tasks View Refresh Export List Properties Help	Name DefaultAcc DefaultAcc Donsdmin DosUpdate Domain Ac Domain Co trol	:0 D s :P d 0 e ers	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs	Description A user account manage. Members in this group of DNS Administrators Gro. DNS clients who are per. Designated administrato All workstations and ser. All domain controllers i All domain guests All domain users All domain users		~
<	>	WseAllow WseAllow		Printer User Shared Folder			v
creates a new item in	runs container.						

## 2. **새 개체 - 사용자 마법사를** 진행합니다.

lew Object - User		×
🤱 Create in	example.com/Users	
First name:	FTD [nitials:	
Last name:	Admin	
Full name:	FTD Admin	
User logon name:		
ftd.admin	@example.com ~	
User logon name (pre	Windows 2000):	
EXAMPLE\	ftd.admin	
	< Back Next > Cancel	1
	No. of Concession, Name	

New Object - User	×
Create in: example.com/Users	
Password:	
User must change password at next logon User cannot change password Password never expires Account is disabled	
< Back	Next > Cancel
New Object - User	×
New Object - User Create in: example.com/Users When you click Finish, the following object will be c	× zeated:
New Object - User Create in: example.com/Users When you click Finish, the following object will be c Full name: FTD Admin User logon name: ftd.admin@example.com The password never expires.	xeated:

3. FTD 계정**이 생성되었는지** 확인합니다. IT 관리자와 **테스트 사용자**, 두 **개의** 추가 **어카운트가 생** 성됩니다.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🙍 📷 🔏 🗈  🛠 🛙	i 🗟 📑 🔽 🖬	1 🙎 🔌 🛍 🤋	r 🔟 🗽		
Active Directory Users and Com Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Domain Controllers Saved Queries Saved Queries	Name DefaultAcco Denied ROD Denied ROD Domain Rom Domain Ad Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Comain Gue	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group User User User User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue Members of this group Members of this group Designated administrato		^
< >			n si e .		~

#### AD 그룹 생성 및 AD 그룹에 사용자 추가(선택 사항)

인증에는 필요하지 않지만 그룹을 사용하여 여러 사용자에게 액세스 정책을 더 쉽게 적용하고 LDAP 권한 부여를 수행할 수 있습니다.

이 컨피그레이션 가이드에서는 나중에 FMC 내에서 사용자 ID를 통해 액세스 제어 정책 설정을 적 용하는 데 그룹을 사용합니다.

1. Active Directory 사용자 및 컴퓨터에서 새 그룹이 추가된 컨테이너 또는 조직 구성 단위를 마우스 오른쪽 단추로 클릭합니다.

이 예에서는 그룹 AnyConnect Admins가 Users(사용자) 컨테이너 **아래에** 추가됩니다. Users(사용 자)를 마우스 오른쪽 **버튼**으로 클릭한 다음 **New(새로 만들기) > Group(그룹)으로 이동합니다**.

Active Directory Users and Con	puters			-	х
File Action View Help					
🗢 🔿 🙍 🚾 🔏 🗈  🗙 🛛	🗉 🖬 📑 🖬	1 🗏 🐮 🛯	r 🗾 🍇		
Active Directory Users and Com Saved Queries Saved Queries Save	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co ntrol ers	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		~
All Tasks View Refresh Export List Properties Help	> > A Read-only A Schema A	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceF msDS-ShadowPr msImaging-PSPs MSMQ Queue Al Printer User	itial ropertyList incipalContainer ias		
Creates a new item in this container.	(m	Shared Folder			v

## 2. **새 개체 - 그룹 마법사를** 진행합니다.

Create in: example.com/U name: onnect Admins name (pre-Windows 2000): onnect Admins	sers
name: onnect Admins name (pre-Windows 2000): onnect Admins	
onnect Admins name (pre-Windows 2000): onnect Admins	
name (pre-Windows 2000): onnect Admins	
onnect Admins	
p scope	Group type
omain local	Security
lobal	Obstribution
niversal	-
	OK Cancel

3. 그룹이 생성되었는지 확인합니다. AnyConnect **사용자** 그룹도 생성됩니다.

Active Directory Users and Comp	uters			-	×
File Action View Help					
🗢 🔿 🙍 📰 🔏 🗙 🖼 🖻	🛛 🖬 🗏 🐮 🖬 '	7 🗕 🔕			
Active Directory Users and Com Saved Queries Example.com Builtin Computers Domain Controllers Solution ForeignSecurityPrincipal: Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount Denied RODC Passw Domain RODC Passw Domain GODC Passw Domain GODC Passw Domain GODC Passw Domain GODC Passw Domain Computers Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin	Type Security Group Security Group User User User	Description Built-in account for ad Members of this group A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue		
< >	(h.s				¥

4. 사용자 그룹을 마우스 오른쪽 단추로 클릭한 다음 등록 정보**를 선택합니다**. 이 컨피그레이션에서 는 사용자 IT 관리자가 AnyConnect 관리자 그룹에 추가되고 사용자 **테스트 사용자**가 AnyConnect 사용자 그룹에 **추가됩니다**.

Active Directory Users and Computers					×
File Action View Help					
🗢 🔿 🖄 📰 🔏 🗈  🗙 🛙	i 🧟 🖻 🛛 🖬 🕇	2 🛙 🔻 🖻	6		
Active Directory Users and Com Saved Queries	Name	Туре	Description		^
<ul> <li>Saved Queries</li> <li>Rample.com</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>Managed Service Accour</li> <li>Users</li> </ul>	AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount DonsAdmins DonsUpdateProxy DonsUpdateProxy Domain Admins Domain Computers Domain Controllers Domain Guests Domain Guests Domain Guests Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin Group Policy Creator	Security Group User Security Group Security Group User Security Group Security Group	Add to a group Buil Move Mer Send Mail Mer All Tasks Au: Mer Cut DN: Delete DN: Rename Des All Cut Help All communications All communications Designated administrato Members of this group Members in this group c	>	
	Guest	User	Built-in account for gue		
	Key Admins	Security Group	Members of this group		
< >>	da	· · ·			~
Renames the current selection.					

## 5. **구성원** 탭에서 추가를 **클릭합니다**.

AnyConnect Admins Properties	?	×
General Members Member Of Managed By		
Members:		
Name Active Directory Domain Services Folder		
Add Remove		
OK Cancel	Apr	ply

필드에 사용자를 입력하고 이름 **확인**을 클릭하여 사용자를 확인합니다. 확인했으면 확인을 **클릭합** 니다.

Select Users, Contacts, Computers, Service Accounts, or Groups	×
Select this object type:	
Users, Service Accounts, Groups, or Other objects	Qbject Types
From this location:	
example.com	Locations
Enter the object names to select (examples):	
IT Admin (it.admin@example.com)	Check Names
Advanced OK	Cancel

올바른 사용자가 추가되었는지 확인한 다음 OK(확인) 버튼을 클릭합니다. 사용자 **테스트 사용자**는 동일한 단계를 사용하여 **AnyConnect 사용자** 그룹에도 추가됩니다.

AnyConnect Admin	s Properties	?	×
General Members	Member Of Managed By		
Members:			
Name	Active Directory Domain Services Folder example.com/Users		
Add	Remove OK Cancel	Ар	ply

LDAPS SSL 인증서 루트 복사(LDAPS 또는 STARTTLS에만 필요)

1. Win+R을 누르고 mmc.exe를 입력한 다음 확인을 클릭합니다.

-

Ø	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.								
<u>O</u> pen:	mmc.exe	~							
	OK Cancel	Browse							

2. 파일 > 스냅인 추가/제거로 이동합니다.

ᡖ Cor	nsole1 - [Console Ro	oot]		-	- 0 X
🚡 File	Action View	Favorites	Window	Help	_ 8 ×
4	New		Ctrl+N		
	Open		Ctrl+0	Actions	
	Save		Ctrl+S	There are no items to show in this view. Console Root	<b>^</b>
	Save As		_	More Actions	+
	Add/Remove Snap	p-in	Ctrl+M		
	Options				
	1 dnsmgmt				
	2 dsa				
	Exit				
Enables	you to add snap-ins	to or remo	we them fro	m the snap-in console.	

3. Available 스냅인에서 Certificates를 선택한 다음 Add를 클릭합니다.

Add or Remove Snap-ins				×
You can select snap-ins for t extensible snap-ins, you car	this console from th configure which e	iose xter	available on your computer and configure the selected set of snap-ins. For sions are enabled.	
Available snap-ins:			Selected snap-ins:	
Snap-in	Vendor	^	Console Root Edit Extensions	
Active Directory Do	Microsoft Cor Microsoft Cor		Bemove	
Active Directory Use	Microsoft Cor Microsoft Cor		Move <u>U</u> p	
Authorization Manager	Microsoft Cor Microsoft Cor		Add >	
Certificates	Microsoft Cor Microsoft Cor			
Component Services	Microsoft Cor Microsoft Cor			
Device Manager	Microsoft Cor Microsoft and	Ļ	Ad <u>v</u> anced	
Description:				
The Certificates snap-in all	ows you to browse	the	contents of the certificate stores for yourself, a service, or a computer.	
			OK Cancel	

## 4. **컴퓨터** 계정**을 선택한** 후 다음을 **클릭합니다**.

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

## Finish(마침)를 클릭합니다.

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>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 확인을 **클릭합니다**.

Add or Remove Snap-ins							х
You can select snap-ins for t extensible snap-ins, you can	his console from th configure which e	nose xter	available on you nsions are enable	ur computer and cor ed.	nfigure the selected se	et of snap-ins. For	
Available snap-ins:				Selected snap-ins:			
Snap-in Active Directory Do Active Directory Site Active Directory Use ActiveX Control ADSI Edit Authorization Manager Certificate Templates Certificates	Vendor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	^	<u>A</u> dd >	Console Root	(Local Computer)	Edit E <u>x</u> tensions Remove Move Up Move Down	
Component Services Computer Managem Device Manager Disk Management Description:	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	Ŷ				Ad <u>v</u> anced	
The Certificates snap-in allo	ws you to browse	the	contents of the	certificate stores fo	r yourself, a service,	OK Cancel	

6. **개인** 폴더를 **확장한** 다음 인증서를 **클릭합니다**. LDAPS에서 사용하는 인증서가 Windows 서버의 **FQDN(Fully Qualified Domain Name)**에 발급됩니다. 이 서버에는 3개의 인증서가 나열됩니다.

• example-WIN2016-CA에서 발급한 CA 인증서.

- example-WIN2016-CA가 WIN2016에 발급한 ID 인증서입니다.
- example-WIN2016-CA가 win2016.example.com에 발급한 ID 인증서

이 컨피그레이션 가이드에서 FQDN은 win2016.example.com이므로 처음 2개의 인증서는 LDAPS SSL 인증서로 사용할 수 없습니다. win2016.example.com에 발급된 ID 인증서는 Windows Server CA 서비스에서 자동으로 발급된 인증서입니다. 세부 정보를 확인하려면 인증서를 두 번 클릭합니 다.

🜇 Console1 - [Console Root\Certific	ates (Local Computer)\Personal\Certi	ficates]			_	o x
🚟 File Action View Favorites	Window Help					- 8 ×
🗢 🏟 🖄 🚾 🗎 🗖 🕞 🚺						
Console Root Certificates (Local Computer) Personal Certificates Trusted Root Certification Certificates Intermediate Certification Intermediate Certificates Intrusted Publishers Untrusted Certificates Intrusted Certificates Intrusted People Client Authentication Issue Client Authentication Issue Client Authentication Issue Client Authentication Issue Remote Desktop	Issued To Caracterization of the second sec	Issued By example-WIN2016-CA example-WIN2016-CA example-WIN2016-CA	Expiration Da 4/19/2060 4/27/2025 4/28/2021	Actions Certificates More Actions		•
Certificate Enrollment Req     Certificate Enrollment Req     Smart Card Trusted Roots     Web Hosting     Windows Live ID Token Iss	٢.		>			
Personal store contains 3 certificates.						

7. LDAPS SSL 인증서로 사용하려면 인증서가 다음 요구 사항을 충족해야 합니다.

• 공용 이름 또는 DNS 주체 대체 이름은 Windows Server의 FQDN과 일치합니다.

• 인증서에는 Enhanced Key Usage(고급 키 사용) 필드 아래에 서버 인증이 있습니다.

인증서의 **Details**(세부사항) 탭에서 **Subject(주체)** 및 **Subject Alternative Name(주체 대체 이름)을** 선택합니다. FQDN win2016.example.com이 있습니다.

🙀 Certif	ficate				×
General	Details	Certification Pa	1th		
Show:	<al></al>		~		
Field			Value		^
<u>詞</u> Sut	bject		win2016.examp	le.com	
📋 Put	blic key		RSA (2048 Bits)		
Put	blic key pa	arameters	05 00		
Ce	rtificate T	emplate Name	DomainControlle	r	
Ent Contraction	hanced Ke	ey Usage	Client Authentic	ation (1.3.6.1	
() () () () () () () () () () () () () (	IME Capa	Dilities	[1]SMIME Capat	olity: Object I	
	bject Key Iboritu Ka	Identifier	30 D7 20 He H8 0	27 fb 11 16	¥
CN = w	in2016.e:	<pre>kample.com</pre>			
		[	Edit Properties	Copy to File	
				O	¢

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al)></al)>		$\sim$	
Field Sul Au Au Au Au Au	bject Key thority Ke I. Distribu thority In	Identifier y Identifier tion Points formation Access	Value 30 b7 2b 4e 48 0f 2f 17 17 e6 KeyID=3d 9f 26 37 fb 11 1f 4 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc	^
Ke Th Th	oject Alte y Usage umbprint umborint	native Name	Other Name:DS Object Guid= Digital Signature, Key Encipher sha1 ca 8e 11 3d eb bc 0f 6e 4a 00	~
Other N DS ( 18 DNS Na	Name: Object Gu me=win2	id=04 10 90 99 a9. 016.example.com	a2 38 24 65 47 84 74 64 26 cd c6 8	D
		Ed	It Properties Copy to File	
			0	¢

Enhanced Key Usage(고급 키 사용) 아래에 Server Authentication(서버 인증)이 있습니다.

🙀 Certi	ficate			×			
General	Details	Certification Path					
Show:	<ai></ai>		~				
Field			Value	^			
E Su E Pu E Pu	bject blic key blic key pa rtificate T	arameters emplate Name	win2016.example.com RSA (2048 Bits) 05 00 DomainController				
5 En	hanced Ke	ey Usage	Client Authentication (1.3.6.1				
E SM E Su Fr Au	IIME Capa bject Key thority Ke	bilities Identifier v Identifier	[1]SMIME Capability: Object I 30 b7 2b 4e 48 0f 2f 17 17 e6 KevID=3d 9f 26 37 fb 11 1f 4				
Client / Server	Authentic	tion (1.3.6.1.5.5.) ation (1.3.6.1.5.5	(1.3.2) (7.3.1)				
		Ed	It Properties Copy to File				

8. 확인이 완료되면 **Certification Path(인증 경로**) 탭에서 루트 CA 인증서인 최상위 인증서를 선택한 다음 View Certificate(**인증서 보기)**를 클릭합니다.

Certificate	×
General Details Certification Path	
Certification path	
win2016.example.com	
View Certificate	ווכ
Certificate status:	_
This certificate is OK.	
0	ĸ

9. 루트 CA 인증서에 대한 인증서 세부사항이 열립니다.

R Certificate	$\times$
General Details Certification Path	
Certificate Information This certificate is intended for the following purpose(s): • Al issuance policies • Al application policies	
Issued to: example-WIN2016-CA	
Issued by: example-WIN2016-CA	
Valid from 4/27/2020 to 4/19/2060	
Issuer Statement	
ОК	

Details 탭에서 Copy to File...(파일에 복사...)을 클릭합니다.

Certificate		×
General Details Certification Path		
Show: <all></all>	~	
Field	Value ^	
Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Valid from Valid from Valid to Subject	V3 13 86 46 e5 9d 70 4f a9 4e 35 sha256RSA sha256 example-WIN2016-CA Monday, April 27, 2020 10:50: Monday, April 19, 2060 10:50: example-WIN2016-CA	
Ec	It Properties Copy to File	1
	ОК	

10. 루트 CA를 **PEM** 형식으로 내보내는 인증서 내보내기 마법사를 진행합니다.

÷	🐉 Certificate Export Wizard	×
	Welcome to the Certificate Export Wizard	
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, dick Next.	
	<u>N</u> ext Cance	

Base-64 인코딩 X.509를 선택합니다.

Certifica	rmat tes can be exported in a variety of file formats.
Select th	e format you want to use:
OD	ER encoded binary X.509 (.CER)
ØВ	ase-64 encoded X-509 (.CER)
00	ryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
0	Include all certificates in the certification path if possible
() P	ersonal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
E	Enable certificate privacy
<u>О</u> м	icrosoft Serialized Certificate Store (.SST)

파일의 이름과 내보낼 위치를 선택합니다.

Erile to Export     Specify the name of the file you want to export     File name:	Browse	
	Next Cancel	
save As		×
← → ~ ↑ ■ > This PC > Desktop	∨ Ö Si	arch Desktop 🔎
Organize 🔻 New folder		III 🕶 😮
Image: Point of the second	Date modified Type No items match your search.	Size
File name: root		~
Save as type: Base64 Encoded X.509 (*.cer)		v
∧ Hide Folders	[	Save Cancel

÷	🚰 Certificate Export Wizard	×
	File to Export	
	Specify the name of the file you want to export	_
	File name:	
	C:\Users\admin\Desktop\root.cer Browse	
	Next Cancel	

이제 Finish(마침)**를 클릭합니다**.

	Â											
Completing the Certificate Export Wizard												
o'root.cer												
(*.cer)												
ish Ca	ncel											
	ish Ca											

11. 이제 위치로 이동하여 메모장이나 다른 텍스트 편집기로 인증서를 엽니다. PEM 형식 인증서가 표시됩니다. 나중에 사용할 수 있도록 저장하십시오.

#### ----BEGIN CERTIFICATE-----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExjleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
BBYEFD2fjjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
```

----END CERTIFICATE-----

12. (선택 사항) LDAPS에서 사용할 수 있는 ID 인증서가 여러 개 있고 사용 여부가 불확실하거나 LDAPS 서버에 대한 액세스 권한이 없는 경우 Windows 서버 또는 FTD에서 수행한 패킷 캡처에서 루트 ca를 추출할 수 있습니다.

### FMC 컨피그레이션

#### 라이센싱 확인

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

1. System > Licenses > Smart Licensing으로 이동합니다.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence					Deplo	7 🔍 s	ystem Help	▼ admin ▼
						Configuration	Users	Domains	Integration	Updates	Licenses •	Health 🔻	Monitoring	<ul> <li>Tools •</li> </ul>
										Sm	art Licenses			
										Cla	ssic Licenses			

2. 장치가 규정을 준수하고 성공적으로 등록되었는지 확인합니다. 디바이스가 AnyConnect **Apex**, **Plus** 또는 **VPN 전용** 라이센스에 등록되어 **있는지 확인합니다**.

	De	vices Objects   AMP Int	elligence						Deploy 🛛 🔩 Sy	stem Help 🔻	admin
		Configuration	Users	Domains	Integration	Updates	Licenses + Sm	art Licen:	ses Health *	Monitoring •	Tools
Smart License Status				<u>Cisco Sma</u>	ert. Software Me	neast 👋 🦻					
Usage Authorization:	0	Authorized (Last Synchronized On N	ay 03 2020)	)							
Product Registration:	0	Registered (Last Renewed On Mar 0	3 2020)								
Assigned Virtual Account:		SEC TAC									
Export-Controlled Features:		Enabled									
Cisco Success Network:		Disabled 🕕									
Cisco Support Diagnostics:		Disabled 0									
Smart Licenses							Filter	Devices		× EdR	Licenses
License Type/Device Name				License State	IS	Device Type			Domain	Group	
Firepower Management Control	ent	er Virtual (2)		0							
Þ 🟳 Base (2)				0							
🖻 🟳 Malware (1)				0							
🖻 📁 Threat (2)				0							
🖹 🟳 URL Filtering (2)				0							
🗸 📁 AnyConnect Apex (1)				0							
FTD-2 192.168.1.17 · Cisco Firepow	ver T	Threat Defense for VMWare - v6.3.0		0		Cisco Firepower	Threat Defense for \	MWare	Global	N/A	
AnyConnect Plus (0)											
AnyConnect VPN Only (0)											

#### 영역 설정

#### 1. 시스템 > 통합으로 이동합니다.

Overview Analysis Policies Devices Objects AMP	Intelligence	Intelligence Deploy 🔍 Sy							admin 🔻
	Configuration	Users	Domains	Integration	Updates	Licenses •	Health *	Monitoring •	Tools *

2. 영역 **아래**에서 **새** 영역을 누릅니다.

Overview Analysis Policie	s Devices Objects	AMP I	ntelligence					Deploy	0 Sys	stem Help v	≠ admin <del>v</del>
			Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring	<ul> <li>Tools *</li> </ul>
Cloud Services Realms	Identity Sources	eStreamer	Host Input Clien	t Sma	rt Software S	atellite					
									M Comp	are realms	New realm
Name	Description	Domain	Туре		Base DN	Group	DN	Group Attr	ibute	State	

3. Microsoft 서버에서 수집한 정보를 바탕으로 적절한 필드를 입력합니다. 완료되면 확인을 **클릭합** 니다.

lame *	LAB-AD		
Description			
Type *	AD	~	
AD Primary Domain *	example.com		ex: domain.com
AD Join Username			ex: user@domain
AD Join Password			Test AD Join
Directory Username *	ftd.admin@example.com		ex: user@domain
Directory Password *	•••••		
Base DN *	DC=example,DC=com		ex: ou=user,dc=cisco,dc=com
Group DN *	DC=example,DC=com		ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	~	

4. 신규 창에서 디렉토리를 선택하고 아직 선택하지 않은 경우 디렉토리 추가를 누릅니다.

Overview	Analysis	Policies	Devices	Objects	AMP	Intellige	ence			Deploy	🖉 🍕 Sy:	stem Help 🔻	admin <del>v</del>
				Configu	uration	Users	Domains	Integration	Updates	Licenses 🔻	Health •	Monitoring •	Tools •
LAB-AD	) tion											Save	Cancel
Directory	Realm Conf	iguration	User Dowr	load									
													dd directory

AD 서버에 대한 세부 정보를 입력합니다. FQDN을 사용하는 경우 FQDN을 확인하도록 DNS를 구 성하지 않으면 FMC 및 FTD를 성공적으로 바인딩할 수 없습니다.

FMC에 대한 DNS를 설정하려면 **System > Configuration**으로 이동하고 **Management** Interfaces를 **선택합니다**.

FTD에 대한 DNS를 설정하려면 Devices(디바이스) > Platform Settings(플랫폼 설정)로 이동하고, 새 정책을 생성하거나, 현재 정책을 수정한 다음 DNS로 이동합니다.

Add directory	? ×
Hostname / IP Address	win2016.example.com
Port	389
Encryption	○ STARTTLS ○ LDAPS ④ None
SSL Certificate	✓ ③
	OK Test Cancel

#### LDAPS 또는 STARTTLS를 사용하는 경우 녹색 + 기호를 클릭하고 인증서에 이름을 지정한 다음 PEM 형식의 루트 CA 인증서를 복사합니다. 완료되면 **Save**(저장)를 클릭합니다.

Import Trusted Certificate Authority	? ×
Name:     LDAPS_ROOT       Certificate Data or, choose a file:     Browse	
<ul> <li>BEGIN CERTIFICATE</li> <li>MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOITTaVsgHwPBfd++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU Cjyeub3CO+meJUuKom2R47C0D35TUv0/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBUaLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKq0L7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBcwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW10FmTOvdNVIb7Xpl1IVa 6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRI+D dLEFKQqmMeYvKvf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96 9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PpIW6E END CERTIFICATE</li> </ul>	< · · · · · · · · · · · · · · · · · · ·
Encrypted, and the password is:	
Save	Cancel

SSL Certificate(SSL 인증서) 옆의 드롭다운에서 새로 추가된 루트 CA를 선택하고 STARTTLS(STARTTLS) 또는 LDAPS를 클릭합니다.
Edit directory		?	×
Hostname / IP Address	win2016.example.com		
Port	636		
Encryption	○ STARTTLS		
SSL Certificate	LDAPS_ROOT 💌 📀		
	OK Test Cancel		

Test(테스트)를 클릭하여 FMC가 이전 단계에서 제공한 디렉토리 사용자 이름 및 비밀번호로 성공 적으로 바인딩할 수 있는지 확인합니다.

이러한 테스트는 FTD에 구성된 라우팅 가능한 인터페이스(예: 내부, 외부, dmz)를 통하지 않고 FMC에서 시작되므로, AnyConnect LDAP 인증 요청이 FTD 라우팅 가능한 인터페이스 중 하나에서 시작되므로 연결에 성공하거나 실패하더라도 AnyConnect 인증에 대한 동일한 결과가 보장되지 않 습니다.

FTD에서 LDAP 연결을 테스트하는 방법에 대한 자세한 내용은 Troubleshooting(문제 해결) 영역의 Test AAA and Packet Capture(AAA 및 패킷 캡처 테스트) 섹션을 참조하십시오.

Status	
$(\mathbf{i})$	Test connection succeeded
	OK

5. User Download(사용자 다운로드) 아래에서 이후 단계에서 사용자 ID에 사용되는 그룹을 다운로 드합니다.

**사용자 및 그룹 다운로드** 확인란을 선택하고 **사용 가능한** 그룹의 **열이** Active Directory 내에 구성된 그룹으로 채워집니다.

그룹은 Include(포함) 또는 Excluded(제외됨)일 수 있지만, 기본적으로 Group DN(그룹 DN) 아래에 있는 모든 그룹이 포함됩니다.

특정 사용자를 포함하거나 제외할 수도 있습니다. 포함된 모든 그룹 및 사용자를 나중에 사용자 ID에 대해 선택할 수 있습니다.

완료되면 저장을 클릭합니다.

Overview Analysis Policies Devices Objects AMP Intel	ligence			Deploy	🕘 🕘 Syste	m Help 🔻	admin 🔻
	Configuration Users	Domains Integration	Upd	ates Licenses •	Health <b>*</b>	Monitoring •	Tools 🔻
LAB-AD Enter Description				You have un	saved changes	🔚 Save	8 Cancel
Directory Realm Configuration User Download							
Download users and groups							
Begin automatic download at 8 V PM V America/New York Repeat Every	24 V Hours						
Available Groups 😋	Groups to Include (2)			Groups to Exclude (	0)		
Search by name	🚔 AnyConnect Admins		- 8	None			
AnyConnect Admins	AnyConnect Users		8				
A DnsUpdateProxy							
A WseRemoteAccessUsers							
A WseInvisibleToDashboard							
Allowed RODC Password Replication Group Add to							
A Enterprise Key Admins Include							
🝰 Domain Admine Add to							
A WseAlertAdministrators							
A Event Log Readers							
A Replicator							
A Domain Guests							
A Windows Authorization Access Group							
Account Operators							
🝰 Hyper-V Administrators 🗸 🗸	Patro Hara ta during			Colora Unio Custinalisa			
👶 System Managed Accounts Group	Enter User Indusion		Add	Enter User Exclusion			Add

## 6. 새 영역을 사용으로 설정합니다.

Overview Analysis Policies Devices Object	cts AMP In	ntelligence				Deploy 04	System He	lp <del>v</del> admin <del>v</del>
		Configuration	Users Domains	Integration	Updates Lice	enses • Health	• Monitori	ng 🔻 Tools 🔻
Cloud Services Realms Identity Sources	eStreamer	Host Input Client	Smart Software	Satellite				
						10	Compare realms	New realm
Name Description	Domain	Туре	Base DN	Group	DN (	Group Attribute	State	
LAB-AD	Global	AD	DC=example.D0	C-com DC-exa	ample.DC=com r	member		4 / D B

7. LDAPS 또는 STARTTLS를 사용하는 경우 FTD에서 루트 CA도 신뢰해야 합니다. 이 작업을 수행 하려면 먼저 Devices(디바이스) **> Certificates(인증서)로 이동합니다**.

Overview Analysis	Policie	s Device	s (	Objects AMP	Intelligence		Deploy	) <b>e</b> ,	System	Help 🔻	admin 🔻
Device Management	NAT	VPN v (	QoS	Platform Setting	s FlexConfig	Certificates					

# 오른쪽 상단의 Add(추가)를 클릭합니다.

Overview Analysis	Polici	es Dev	ices 0	bjects	AMP	Intelligence		Deploy	0,	System	Help 🔻	admin	
Device Management	NAT	VPN •	QoS	Platform	Settings	FlexConfig	Certificates						
											0	Add	

# FTD를 선택하고 LDAP 컨피그레이션이 추가된 다음 녹색 + 기호를 클릭합니다.

Add New Certificate	1	? ×
Add a new certificate to t identify certificate.	he device using cert enrollment object whi	ch is used to generate CA and
Device":	FTD-2	¥
Cert Enrollment*:	Select a certificate entrollment object	¥ 🙆
		Add Cancel

신뢰 지점에 이름을 **지정한** 다음 Enrollment Type(**등록 유형) 드롭다운**에서 Manual enrollment(수 동 등록)**를** 선택합니다. 여기에 PEM 루트 ca 인증서를 붙여넣은 다음 Save를 **클릭합니다**.

Add Cert Enrollme	nt	? ×
Name* Description	LDAPS_ROOT	
CA Information	Certificate Parameters Key Revocation	
Enrollment Type: CA Certificate:*	Manual  Manual  Manual  Manual  Second Stress Stres	•
Allow Overrides	Save	Cancel

생성된 신뢰 지점이 선택되었는지 확인한 후 Add(추가)를 클릭합니다.

Add New Certificate		? ×
Add a new certificate to th identify certificate.	e device using cert enrollment object whic	h is used to generate CA and
Device*:	FTD-2	*
Cert Enrollment*:	LDAPS_ROOT	<b>~</b> ©
Cert Enrollment Details:		
Name:	LDAPS_ROOT	
Enrollment Type:	Manual	
SCEP URL:	NA	
		Add Cancel

새 신뢰 지점이 FTD 아래에 나타납니다. ID 인증서 가져오기가 필요하다고 언급하지만 LDAPS 서 버에서 보낸 SSL 인증서를 FTD에서 인증할 필요가 없으므로 이 메시지를 무시할 수 있습니다.

Overview Analysis	Policies Devices	Objects AMP Int	elligence	Deploy 🔍	System He	lp <del>v</del> a	admin 🔻
Device Management	NAT VPN • QoS	Platform Settings	FlexConfig Certificates				
						0	Add
Name	Domain	Enrollment Typ	e Status				
4 🗐 FTD-1							
FTD-1-PKCS12	Global	PKCS12 file	CA D			£ 🗘	6
4 🗐 FTD-2							
FTD-2-PKCS12	Global	PKCS12 file	a, ca			<i>?</i> ¢	6
FTD-2-Selfsigned	Global	Self-Signed	S CA LD			¢ 2	6
LDAPS_ROOT	Global	Manual	🔍 CA 🔺 🔬 Ide	ntity certificate import requ	ired	Ŷ¢	8

#### AD 인증을 위해 AnyConnect 구성

1. 이 단계에서는 원격 액세스 vpn 정책이 아직 생성되지 않았다고 가정합니다. 정책을 생성한 경우 해당 정책의 수정 버튼을 클릭하고 3단계로 건너뜁니다.

Devices(디바이스) > VPN > Remote Access(원격 액세스)로 이동합니다.

Overview Analysis	Policies	Device	Devices Objects AMP Intelligence									Help 🔻	admin <del>v</del>
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates							
		Site To S	ite										
		Remote A	Access										
		Troublest	hooting	]									

## Add(추가)를 클릭하여 새 원격 액세스 VPN 정책을 생성합니다

Overview Analysis	Policies Devices Obje	ts AMP	Intelligence			Deploy	<b>e</b> , s	System	Help 🔻	admin <del>v</del>
Device Management	NAT VPN + Remote Acce	as QoS	Platform Settings	FlexConfig	Certificates					
									0	Add
Name			Status		Last Modified					

No configuration available Add a new configuration

2. 원격 액세스 VPN 정책 마법사를 완료합니다. Policy Assignment(정책 할당)에서 정책 및 정책이 적용되는 디바이스의 이름을 지정합니다.



Connection **Profile(연결 프로파일**)에서 AnyConnect 사용자가 **연결될** 때 표시되는 그룹 별칭으로도 사용되는 연결 프로파일의 이름을 지정합니다.

인증 서버에서 이전에 생성한 영역을 지정합니다.

AnyConnect 클라이언트에 IP 주소를 할당하는 방법을 지정합니다.

이 연결 프로파일에 사용되는 기본 그룹 정책을 지정합니다.

Overview Analysis Policies Devices Objects   AMP	Intelligence		Deploy 🔒 System	Help 🔻	admin 🔻
Device Management NAT VPN + Remote Access QoS	Platform Settings FlexConfig	Certificates			
Remote Access VPN Policy Wizard					
Policy Assignment     2 Connection Profile     3	AnyConnect > ④ Access &	Certificate > (5) Summary			
Connection Profile:					^
Connection Profiles specify the tunne accomplished and how addresses are	I group policies for a VPN connection. These assigned. They also include user attributes	policies pertain to creating the tunnel itself, how , which are defined in group policies.	v AAA is		
Connection Profile Name:*	General				
	This name is configured as a connection alias	, it can be used to connect to the VTN gateway			
Authentication, Authorization & A	ccounting (AAA):				
Specify the method of authentication	(AAA, certificates or both), and the AAA set	rvers that will be used for VPN connections.			
Authentication Method:	AAA Only ~				
Authentication Server:*	LAB-AD 🛩 (	<ul> <li>(Realm or RADJUS)</li> </ul>			
Authorization Server:		(RADIUS)			
Accounting Server:		(RADIUS)			
Client Address Assignment:					
Client IP address can be assigned fro assignment is tried in the order of A/	m AAA server, DHCP server and IP address A server, DHCP server and IP address pool.	pools. When multiple options are selected, IP ad	dress		
Use AAA Server (RADIUS	nly) 🕕				
Use DHCP Servers					
Use IP Address Pools					
IPv4 Address Pools:	AnyConnect-Pool	<i>i</i>			
IPv6 Address Pools:		0			
Group Policy: A group policy is a collection of user- or create a Group Policy object.	oriented session attributes which are assign	ed to client when a VPN connection is establishe	d. Select		
Group Policy:*	DfltGrpPolicy 👻 (	8			
	Edit Group Policy				~
			Back Next	Ca	ancel

## AnyConnect에서 사용되는 AnyConnect 패키지를 업로드하고 지정합니다.

Overview Analysis Polici	s Devices Objects AMP Intelligence	Deploy 🔒 System	Help 🔻 admin 🔻
Device Management NAT	VPN • Remote Access QoS Platform Settings FlexConfig Certificates		
Remote Access VPN P	blicy Wizard		
1 Policy Assignment	2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary		
	vnyConnect Client Image hv VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is stilated. Minimize connection setup time by choosing the appropriate OS for the selected package.	1	^
	ownload AnyConnect Client packages from Cisco Software Download Center.		
	Show Re-order buttons		
	AnyConnect File Object Name AnyConnect Client Package Name Operating System		
	anyconnect-linux64-4.7.03052-we anyconnect-linux64-4.7.03052-webdeploy-k9		
	anyconnect-win-4.7.00136-webde anyconnect-win-4.7.00136-webdeploy-k9.pkg Windows v		~
		Back Next	Cancel

Access & Certificate(액세스 및 인증서)에서 AnyConnect 사용자가 AnyConnect에 액세스할 인터페 이스를 지정합니다.

SSL 핸드셰이크 중에 FTD에서 사용하는 인증서를 만들거나 지정합니다.

암호 해독된 트래픽에 대한 **액세스 제어 정책 우회**(sysopt permit-vpn) 확인란이 선택되지 않은 상 태로 유지되어 나중에 생성된 사용자 ID가 RAVPN 연결에 적용되는지 확인합니다.

Overview Analysis Policies Devices Objects AMP Intelligence		Deploy	0 <sub>5</sub> System	Help 🔻	admin v
Device Management NAT VPN > Remote Access QoS Platform Settings	FlexConfig Certificates				
Remote Access VPN Policy Wizard					
Policy Assignment     O     Connection Profile     O     AnyConnect	Access & Certificate     Summary				
Network Interface for Incoming VPN Acc Select or create an Interface Group or a Security Z connections.	255 ne that contains the network interfaces users will access for VPN				
Interface group/Security Zone:* outside-zone	× 0-				
S Enable DT	LS on member interfaces				
Device Certificates Device certificate (also called Identity certificate) id certificate which is used to authenticate the VPN ga	entifies the VPN gateway to the remote access clients. Select a away.				
Certificate Enrollment:* FTD-2-Selfs	aned 👻 🕄				
Corroll the	selected certificate object on the target devices				
Access Control for VPN Traffic					
All decrypted traffic in the VPN tunnel is subjected bypass decrypted traffic from the Access Control Po	o the Access Control Policy by default. Select this option to licy.				
Bypass Access Control policy for decrypted traff This option bypasses the Access Control Policy ins AAA server are still applied to VPW traffic.	c (sysopt permit-upn) ecctor, but VPN filter ACL and authorization ACL downloaded from				
		Back	Next	) <b>C</b> a	ancel

## Summary(요약)에서 컨피그레이션을 검토하고 Finish(마침)를 클릭합니다.



3. **Remote Access VPN Policy(원격 액세스 VPN 정책)** 아래에서 **edit**(수정)를 클릭하여 알맞은 **연** 결 프로필을 **선택합니다**.

Overview Analysis Policies Devices Objects	AMP Intelligence	Deploy 🔍 System Help 🔻 admin 🔻
Device Management NAT VPN • Remote Access	QoS Platform Settings FlexConfig Certificates	
FTD-2-RA-Policy Enter Description		Save Cancel
		Policy Assignments (1)
Connection Profile Access Interfaces Advanced		
		0
Name	AAA Group Policy	
DefaultWEBVPWGroup	Authentication: None DfkGrpPolicy Authorization: None Accounting: None	/ 0
General	Authentication: LAB-AD (AD)	28 - C

인증 서버가 이전에 생성한 영역으로 설정되어 있는지 확인합니다.

고급 설정에서 비밀번호 관리 사용을 선택하여 비밀번호가 만료되기 전에 사용자가 비밀번호를 변 경할 수 있도록 할 수 있습니다.

그러나 이 설정에서는 영역이 LDAPS를 사용해야 합니다. 변경 사항이 있으면 저장을 클릭합니다.

Edit Connection Pr	ofile			? ×
Connection Profile:*	General			
Group Policy:	Edit Group Po	y licy	· •	
Client Address Assign	ment AA	A Aliases		
Authentication				
Authentication Meth	iod:	AAA Only		*
Authentication Serv	er:	LAB-AD (AD)		¥
Authorization Authorization Serve	r:	Allow connection only	if user exists in authorizati	✓ on database
Accounting Accounting Server:				~
Advanced Settin  Advanced Settin  Strip Realm from Strip Group from Enable Password Notify User Notify user on th	gs username Management days pric he day of passy	t or to password expiration vord expiration		•
				Save Cancel

완료되면 오른쪽 상단에서 Save(저장)를 클릭합니다.

Overview Analysis	Polici	es Devices O	bjects	AMP	Intelligence				Deploy	<b>e</b> ,	System	Help 🔻	admin 🔻
Device Management	NAT	VPN + Remote /	Access	QoS	Platform Settings	FlexConfig	Certificates						
FTD-2-RA-Pol	cy							Yo	u have unsav	ed char	nges 📔	Save	😫 Cancel

# ID 정책 활성화 및 사용자 ID에 대한 보안 정책 구성

1. Policies(정책) > Access Control(액세스 제어) > Identity(ID)로 이동합니다.

Overview Anal	ysis Policies Devic	es Objects AMP	Intelligence			Deploy	0 <sub>5</sub> System	Help 🔻	admin 🔻
Access Control 🔻	Network Discovery	Application Detectors	Correlation	Actions 🔻					
Access Control									
Intrusion									
Malware & File									
DNS									
Identity									
SSL									
Prefilter									

#### 새 ID 정책을 만듭니다.

Overview Analysis Policies Devices Object	ts AMP Intelligence	•	Deploy 0	System Help <del>v</del> admin <del>v</del>
Access Control + Identity Network Discovery	Application Detectors Co	Correlation Actions •		
			0	oject Management Access Control
			() K c	ompare Policies 🔍 New Policy
Identity Policy	Domain		Status	Last Modified
		There are no policies cre	ated. Add a new policy	

## 새 ID **정책**의 이름을 **지정합니다**.

Name P	TD-2 Identity Policy
Description	
Description	

## 2. 규칙 추가**를 클릭합니다**.



3. 새 규칙의 이름을 지정합니다. 활성화되었고 작업이 수동 인증으로 설정되어 있는지 확인합니다.

Realm & Settings(영역 및 설정) 탭을 클릭하고 이전에 생성한 영역을 선택합니다. 완료되면 Add(추가)를 클릭합니다.

Add Rule

Name RAVPN		🖌 Enable	d Insert	into Category	~	Standard Rules	~
Action Passive Authentical	tion	▼ Realm: LAB-AD (AD)	Authentication Protocol:	HTTP Basic Exclude H	ITTP User-	Agents: None	
Remote access VPN	sessions are actively auth	henticated by VPN. Other session	ns use the rule Action.				
Zones Networks	VLAN Tags Ports					Realm & S	ettings
Realm *	LAB-AD (AD)		V 2				
Use active authentication	on if passive or VPN ident	ity cannot be established					
* Required Field							
						Add C	ancel

# 4. 저장을 **클릭합니다**.

Overview Analysis Pol	icies Device	es Objects	AMP Intellig	gence				Dep	xloy 🧛 Syster	n Help <b>⊤ ad</b>	min <del>v</del>
Access Control + Identity	Network Disc	covery Appli	cation Detectors	Correlation	Actions <b>*</b>						
FTD-2 Identity Pol	icy							You have	unsaved changes	Save 🔞	Cancel
Rules Active Authentication	1										
							Add Category	y ( 🔾 Add Rule	Search Rules		×
# Name	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol	
Administrator Rules											
This category is empty											
Standard Rules											
1 RAVPN	any	any	any	any	any	any	any	LAB-AD	Passive Authenticatio	n none	/8
Root Rules											
This category is empty											

Displaying 1 - 1 of 1 rules  $|\langle \langle | \langle | Page | \overline{1 - 0} | of 1 \rangle \rangle | c$ 

## 5. 정책 > 액세스 제어 > 액세스 제어로 이동합니다.

Overview Analysis Policies Devices Objects AMP Intelligence	Deploy	🧛 System	Help 🔻 admin 🔻
Access Control > Identity Network Discovery Application Detectors Correlation Actions •			
Access Control			
Intrusion			
Malware & File			
DNS			
Identity			
SSL			
Prefilter			

# 6. FTD가 구성된 **액세스 제어** 정책을 편집합니다.

Overview Analysis Policies	Devices Objects	AMP Intelligence				Deploy	🔒 System	Help 🔻 adm	nin T
Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions <b>*</b>					
					Object Management 1	ntrusion Netwo	rk Analysis Policy	DNS Import/Ex	xport
								New Policy	,
Access Control Policy		Status			Last Modified				
Default-Policy		Targeting 1 de Up-to-date on	evices all targeted devic	es	2020-05-04 09:15:56 Modified by "admin"			Pa 🛛 🖉 a	j –

## 7. ID **정책** 옆의 값을 **클릭합니다.**



## 앞서 생성한 ID 정책을 선택한 다음 OK(확인)를 클릭합니다.

Identity Policy		
FTD-2 Identity Policy		• 🥒
Revert to Defaults	ОК Са	ncel

8. 새 ACP 규칙을 생성하려면 규칙 추가를 누릅니다. 이러한 단계에서는 AnyConnect Admins 그룹 내의 사용자가 RDP를 사용하여 내부 네트워크 내의 장치에 연결할 수 있도록 허용하는 규칙을 만 듭니다.

Overview Analysis Policies Devi	ices Objects AMP Intelligen	œ	Deploy 0	System Help <b>v admin v</b>
Access Control > Access Control Net	twork Discovery Application Detects	tors Correlation Actions •		
Default-Policy Enter Description			You have unsaved changes Analyze Hit Co	unts 🔚 Save 🛛 😮 Cancel
Prefilter Policy: Default Prefilter Policy		SSL Policy: None	Identity Policy:	FTD-2 Identity Policy
			Theritance Se	ettings   🛐 Policy Assignments (1)
Rules Security Intelligence HTTP Res	sponses Logging Advanced			
曲 Filter by Device		Show Rule Conflicts 🥹	🔾 Add Category 🛛 Add Rule 🚔 Se	arch Rules 🛛 💢
# Name Sourc Dest Z	Sourc Dest N VLAN Use	ers Applic Sourc Dest P	URLs Sourc Dest S Action	• • .a 🕁 + 🧶
<ul> <li>Mandatory - Default-Policy (-)</li> </ul>				
There are no rules in this section. Add Rule or A	idd Category			
➡ Default - Default-Policy (-)				
There are no rules in this section. Add Rule or A	dd Category			
Default Action			Access Control: Block All Traffic	¥ 🛽

Displaying 0 - 0 of 0 rules  $|\langle \langle Page | \underline{1}$  of  $1 > \rangle| \subset C | Rules per page: 100 -$ 

#### 규칙의 Name을 지정합니다. 규칙이 활성화되어 있고 적절한 Action이 있는지 확인합니다.

Zones(영역) 탭에서 관심 트래픽에 적합한 영역을 지정합니다.

사용자가 시작한 RDP 트래픽은 외부 영역 인터페이스에서 제공된 FTD로 유입되어 내부 영역으로 이그레스(egress)됩니다.

Add Rule											? >
Name AC RDP Access				<b>V</b> (	Enabled	Insert	into Manda	story 👻			
Action 🖌 Allow			▼ 0 0 %	8 4 5							
Zones Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attributes		Insp	ection	Logging	Comments
Available Zones 🛭 🗯				Sour	rce Zones	(1)		Destination Zo	nes (1)		
🔍 side		×	)		outside-zo	ne	6	🍰 inside-zone			ij
👍 inside-zone			Add to Source Add to Destination								
										Add	Cancel

Networks(네트워크)에서 소스 및 목적지 네트워크를 정의합니다.

개체 AnyConnect\_Pool에는 AnyConnect 클라이언트에 할당된 IP 주소가 포함됩니다.

Object Inside Net에는 내부 네트워크 서브넷이 포함됩니다.

Add Ru	le												
Name	AC RDP Access				🗹 En	abled		Insert	into Manda	tory			~
Action	Allow			V 0 0.8	t I								
Zone	s Networks VLA	N Tags	Users	Applications	Ports	URLs	SGT/ISE	Attributes			Inspection	Logging	Comments
Availab	le Networks 🖸		0		Sourc	e Netwo	rks (1)			Destinati	ion Networks	(1)	
🔍 Sea	rch by name or value					Source		Original (	Client	📰 Insid	e_Net		ū
	Networks	Geolocation	n		🚍 Ar	nyConnect	_Pool		6				
Insi IPv4 IPv4 IPv4 IPv4 IPv4 IPv4 IPv4 IPv4	de_Net I-Benchmark-Tests I-Multicast I-Private-10.0.0.0-8 I-Private-172.16.0.0-12 I-Private-192.168.0.0-16 I-Private-All-RFC1918			Add To Source Networks Add to Destination	Enter	an IP add	frace		Add				
IPv6	i-IPv4-Mapped				Critter	an IP add	ress		Add	Enter an	IP address		Add
												Add	Cancel

Users(**사용자**)의 Available Realms(사용 가능한 영역) 아래에서 이전에 생성한 영역을 클릭하고 Available Users(**사용 가능한 사용자**)에서 적절한 그룹/사용자를 클릭한 다음 Add to Rule(규칙에 추가)을 클릭합니다.

Available Users 섹션 아래에서 사용 가능한 사용자 또는 그룹이 없는 경우, FMC가 영역 섹션 아래 에서 Users 및 Groups를 다운로드할 수 있는지, 그리고 적절한 Groups/User가 포함되어 있는지 확 인하십시오.

여기에 지정된 사용자/그룹이 소스 관점에서 선택됩니다.

예를 들어, 지금까지 이 규칙에 정의된 대로 FTD는 트래픽이 외부 영역에서 시작되어 내부 영역으 로 향하고, AnyConnect Pools 개체의 네트워크에서 시작되어 Inside Net 개체의 네트워크로 향하 며, AnyConnect Admins 그룹의 사용자로부터 시작되었다고 평가합니다.

Add Ri	ile											? ×
Name	AC RDP Access			<b>√</b> E	nabled	1	Insert	into Mandate	ory Y	-		
Action	Allow		N 0 0 💌	105								
Zone	Networks VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attrib	utes			Inspection	Logging	Comments
Availab	le Realms 🖸		Available Users	Ċ					Selected	Users (1)		
🔍 Sea	rch by name or value		🔍 Search by n	ame or va	lue				🝰 LAB-A	D/AnyConnect	: Admins	6
📑 Spe	cial Identities		HAB-AD/*									
🌐 LAB	i-AD		📣 AnyConnect	Admins								
			🝰 AnyConnect	Users								
			ait.admin 🚨				A	dd to Rule				
			atest.user				_					
											Add	Cancel

? X

Ports(포트)에서 TCP 및 UDP 포트 3389를 허용하기 위해 사용자 지정 RDP 객체가 생성 및 추가되 었습니다. RDP는 Applications(애플리케이션) 섹션에 추가되었을 수 있지만, 간소화를 위해 포트만 확인합니다.

Add Rule					? ×
Name AC RDP Access		Enabled	Insert into I	Mandatory 👻	
Action 🖌 Allow	• 00.	8 to J			
Zones Networks VLAN Tags	Users Applications	Ports URLs S	GT/ISE Attributes	Inspection	Logging Comments
Available Ports 🖒	0	Selected Source	Ports (0)	Selected Destination P	orts (2)
Search by name or value  AOL  DNS_over_TCP  DNS_over_UDP  Proc-HTTPS  FMC-SSH  FTD-3-FDM  FTD-3-SSH  FTD-3-SS	Add to Source Add to Destination	any		₩ RDP-TCP ₩ RDP-UDP	5 5
<i>/</i> нттр	~			Vdd Protocol TCP (6)	Port Enter a Add
					Add Cancel

마지막으로 Logging(**로깅**)에서 Log at End of Connection(연결 종료 시 로깅)을 선택하면 나중에 추 가 확인이 이루어집니다. 완료되면 Add(추가)를 클릭합니다.

Add Rule

Name	AC RDP Access				🖌 Enab	oled	Insert	into Mandatory	~		
Action	Allow			• 002	8 🖆 🗾						
Zone	s Networks	VLAN Tags	Users	Applications	Ports UI	RLs	SGT/ISE Attributes		Inspection	Logging	Comments
🗆 Log	at Beginning of C	onnection									
🗹 Log	at End of Connect	ion									
File Ever	n <b>ts:</b> Files										
Send Co V Ever	nnection Events to it Viewer	D:									
🗌 Sysl	og Server (Using	default syslog co	onfiguratio	n in Access Contr	ol Logging) Sh	iow Ov	errides				
	IP Trap Select an	SNMP Alert Con	figuration.			*	0				
									E 1	Add	Cancel

9. 그룹 AnyConnect 사용자 내의 사용자가 **Windows Server** IIS 웹 사이트에 액세스할 수 있도록 HTTP **액세스**에 대한 추가 **규칙이** 생성됩니다. 저장을 **클릭합니다**.

Overview Analysis Policies	Devices Objects	AMP Intelligence						eploy (	🔍 System Help 🔻	admin v
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions •						
Default-Policy Enter Description						You have uns	aved changes A	nalyze Hit (	Counts 📄 Save	🙁 Cancel
Prefilter Policy: <u>Default Prefilter Policy</u>		5	SL Policy: <u>None</u>			Ident	ity Policy: <u>PTD-2.1</u>	dentity Poli	isz.	
							Te 1	heritance	Settings   🥂 Policy Assi	gnmenta (1)
Rules Security Intelligence H	TTP Responses Loggin	ng Advanced								
# Filter by Device				Show Rule Con	ficta 😣	Add Category	y 🔷 Add Rule	- e - s	Search Rules	×
a Name Source Zo	Dest Zones Sour	rce Networks Dest No	two V Use	rs	A S	Dest Ports	U S D	Action	0.860	. °
w Mandatory - Default-Policy (1-2)										
1 AC RDP Access A outside-zo	ne 👍 inside-zone 🛛 🚍 J	AnyConnect_Pool 🛛 👼 Insi	Se_Net Arc af t	AB-AD/AnyConnect Admins	Any An	RDP-TCP	Any Any Any	Allow 🗸	00,8±1	• 🥒 6
2 AC HTTP Access do outside-zo	ne 🗄 inside-zone 🛛 🚊 A	AnyConnect_Pool 🛛 👼 Insi	de_Net 🛛 🗛 🦽 l	AB-AD/AnyConnect Users	Any An	у 🥜 НТТР	Any Any Any	Allow	00.801	• 🥒 🖯
▼ Default - Default-Policy (-)										
There are no rules in this section. Add R	ule or Add Category									
Default Action						Access Con	trol: Block All Traff	c		× 🔳

Displaying 1 - 2 of 2 rules |< < Page 1 of 1 > >| C | Rules per page: 100 \*

#### NAT 예외 구성

인터넷 PAT 규칙과 같이 AnyConnect 트래픽에 영향을 주는 NAT 규칙이 있는 경우, AnyConnect 트래픽이 NAT에 영향을 받지 않도록 NAT 예외 규칙을 구성하는 것이 중요합니다.

#### 1. Devices(디바이스) > NAT로 이동합니다.

Overview Analysis	e Polici	es Devi	ices 0	bjects AMP Int	elligence		Deploy	<b>e</b> ,	System	Help 🔻	admin v
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates					

## FTD에 적용되는 NAT 정책을 선택합니다.

0	verview	Analysis	Policie	es Devi	ices	Objects	AMP	Inte	elligence		(	Deploy	<b>e</b> ,	System	Help 🔻	admin 🔻
D	evice Mana	agement	NAT	VPN *	QoS	Platfo	rm Settin	gs	FlexConfig	Certificates						
															🔾 Nev	Policy
	NAT Pol	icy						Devic	се Туре		Status					
	FTD-2-	NAT-Policy						Threat	t Defense		Targeting 1 devices Up-to-date on all target	ted devices			<b>D</b> E	/ 6

? ×

2. 이 NAT 정책에는 외부 인터페이스를 외부 인터페이스로 이그레스(egress)하는 모든 트래픽 (AnyConnect 트래픽 포함)에 PAT가 영향을 주는 동적 PAT가 마지막에 있습니다.

AnyConnect 트래픽이 NAT에 영향을 받지 않도록 하려면 오른쪽 상단에서 Add Rule(규칙 추가)을 클릭합니다.



Displaying 1-1 of 1 rows |< < Page 1 of 1 > >| C Rows per page: 100 -

3. NAT 예외 규칙을 구성하고, 규칙이 유형이 고정인 수동 NAT 규칙인지 확인합니다. AnyConnect 트래픽에 적용되는 양방향 NAT 규칙입니다.

이러한 설정을 통해 FTD가 Inside\_Net에서 시작하고 AnyConnect IP 주소(AnyConnect\_Pool로 정 의됨)로 향하는 트래픽을 탐지하면, 트래픽이 inside\_zone을 인그레스하고 outside\_zone을 이그레 스할 때 소스가 동일한 값(Inside\_Net)으로 변환되고 목적지가 동일한 값(AnyConnect\_Pool)으로 변 환됩니다. 이는 기본적으로 이러한 조건이 충족될 때 NAT를 우회합니다.

Add NAT Rule									? X
NAT Rule:	Manual NAT Rul	e 👻	Ir	isert:	In Category	~	NAT Rules Before	*	
Type:	Static	~	C Enable						
Description:									0
Interface Objects	Translation	PAT Pool	Advance	d					
Available Interface Ob	ojects 🖒			Source Interface Object	ts (1)	Destina	ation Interface Ob	jects (1)	
🔍 zone		×		🚔 inside-zone	6	🚠 out	tside-zone	l	
📩 inside-zone									
🚠 outside-zone		A	dd to						
			dd to						
		Dest	tination						
							OF	Cano	el

Add NAT Rule					?
NAT Rule:	Manual NAT Rule 💙	Insert:	In Category	V NAT Rules Before	
Type:	Static 💌	Enable			
Description:					0
Interface Objects	ranslation PAT Pool	Advanced			
Original Packet			Translated Packet		
Original Source:*	Inside_Net	<b>~</b> O	Translated Source:	Address	~
Original Destination:	Address	*		Inside_Net	<b>Y</b> ()
	AnyConnect_Pool	<b>~</b> ()	Translated Destination:	AnyConnect_Pool	<b>~</b> 0
Original Source Port:		¥ 0	Translated Source Port:		<b>~</b> O
Original Destination Por	t:	¥ ()	Translated Destination Port:		<b>~</b> 🔾
				ок	Cancel

또한 FTD는 프록시 ARP가 아니라 이 트래픽에 대해 경로 조회를 수행하도록 설정됩니다. 완료되 면 **OK(확인**)를 클릭합니다.

Add NAT Rule					? ×
NAT Rule:	Manual NAT Rule	Insert:	In Category	▼ NAT Rules Before ▼	
Type:	Static 🗸	Enable			
Description:					$\hat{\mathbf{C}}$
Interface Objects	Translation PAT Pool	Advanced			
Translate DNS repli	es that match this rule				
Fallthrough to Inter	face PAT(Destination Interfac	c)			
IPv6					
Net to Net Mapping					
🗹 Do not proxy ARP o	n Destination Interface				
Perform Route Look	up for Destination Interface				
Unidirectional					
				ок	Cancel

4. 저장을 **클릭합니다**.

	Overview /	unalysis	Policies De	vices Obj	ects AMP	Intelligence			Deplo	y 🔒	System H	ielp 🔻	admin 🔻
	Device Manage	ement	NAT VPN -	QoS	Platform Setting	s FlexConfig	Certificates						
	FTD-2-N/ Enter Description	AT-Poli	су					You have	unsaved changes [ 🖄 Sh	ow Warning	js 🔡 Sa	ive	😫 Cancel
	Rules										<u>E</u> P	olicy As	signments (1)
đ	Pilter by Device											0	Add Rule
						Original Pack	et		Translated Packet				
4	Direction	Туре	Source Interface Ob	Destinatio	on Original Object Sources	Original Destinatio	Orig Service	Translated s Sources	Translated Destinations	Trans Services	Options		
•	NAT Rules Bef	one											
1	49	Static	🐴 inside-zon	e 🚠 outside	-zone 🚃 Insid	e_Net 📑 AnyCor	nnect_Pool	📰 Inside_Net	👼 AnyConnect_Pool		🥵 Dossfal 🥵 route-k 🍕 no-pro	ise ookup xy-arp	/ 6
•	Auto NAT Rule	s											
3	• •	Dynamic	🥞 any	🚠 outside	-zone 🕋 obj-a	ny		🍓 Interface			🍓 Dns:fal	se	Ø 6
٠	NAT Rules Afte	r											
							Displayir	to 1-2 of 2 rows	K < Page 1 of 1	> >	C Rowe	s per pa	ige: 100 •

#### 구축

1. 컨피그레이션이 완료되면 오른쪽 상단에서 Deploy(구축) 버튼을 클릭합니다.



2. 구성이 적용되는 FTD 옆에 있는 확인란을 클릭하고 구축을 **클릭합니다**.

Dep	loy Policies Version:2020-05-04 09:40 AM					>
V	Device	Inspect Interruption	Туре	Group	Current Version	٢
▼ ⊞	=/FTD-2	No	FTD		2020-05-04 09:16 AM	
Selec	ted devices: 1				Deploy Car	ncel



# 최종 컨피그레이션

#### AAA 컨피그레이션

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
max-failed-attempts 4
realm-id 5
aaa-server LAB-AD host win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-group-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute samaccountname
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type microsoft
```

#### AnyConnect 컨피그레이션

```
> show running-config webvpn
webvpn
enable Outside
anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
anyconnect profiles Lab disk0:/csm/lab.xml
anyconnect enable
tunnel-group-list enable
cache
 no disable
error-recovery disable
> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
address-pool AnyConnect-Pool
authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
group-alias General enable
> show running-config group-policy
group-policy DfltGrpPolicy attributes
vpn-simultaneous-logins 10
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Lab
user-authentication-idle-timeout none
webvpn
 anyconnect keep-installer none
 anyconnect modules value dart
 anyconnect ask none default anyconnect
 http-comp none
 activex-relay disable
 file-entry disable
 file-browsing disable
 url-entry disable
 deny-message none
 anyconnect ssl df-bit-ignore enable
```

> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside

# AnyConnect로 연결 및 액세스 제어 정책 규칙 확인

🚳 Cisco AnyCo	onnect Secu	ure Mobili	ty Client	—		×		
	VPN: Contacting ftd2.exam	ftd2.exam	ple.com.	~	Connect			
<b>¢</b> ()		S Cisc	o AnyConne Group: Username:	ect   ftd2 Genera it.admi	example.co	om	~	×
			Password:	*****	⊧**		Cancel	
🔇 Cisco AnyCo	onnect Secu	ure Mobili	ty Client	-		×		
	VPN: Connected ftd2.exam	to ftd2.ex	ample.com.	~ <b>_</b>	Disconnect			
00:00:12					IP	v4		
<b>Ö</b> ()								

사용자 IT 관리자는 Windows Server에 대한 RDP 액세스 권한이 있지만 HTTP에 대한 액세스 권한 이 없는 AnyConnect 관리자 그룹에 있습니다.

이 서버에 대한 RDP 및 Firefox 세션을 열면 이 사용자가 RDP를 통해서만 서버에 액세스할 수 있는 지 확인합니다.



HTTP 액세스이지만 RDP 액세스는 아닌 AnyConnect 사용자 그룹에 있는 사용자 테스트 사용자로 로그인한 경우 액세스 제어 정책 규칙이 적용되는지 확인할 수 있습니다.



# FMC 연결 이벤트로 확인

로깅이 액세스 제어 정책 규칙에서 활성화되었으므로, 해당 규칙과 일치하는 모든 트래픽에 대해 연결 이벤트를 확인할 수 있습니다

Analysis(분석) > Connections(연결) > Events(이벤트)로 이동합니다.

Overview Analys	sis Policies D	Devices Object	ts AMF	P Intellige	ence	L C	eploy 🔒 S	System Help	• admin •
Context Explorer	Connections <b>v</b>	Intrusions 🔻	Files 🔻	Hosts 🔻	Users v	Correlation <b>v</b>	Advanced 🔻	Search	
	Events								
	Security Intellig	ence Events							

연결 이벤트의 테이블 보기에서 로그는 IT 관리자에 대한 연결 이벤트만 표시하도록 필터링됩니다.

여기서 서버에 대한 RDP 트래픽(TCP 및 UDP 3389)이 허용되는지 확인할 수 있지만 포트 80 트래 픽은 차단됩니다.

Ove	rview	Analysi	s Policies I	Devices Objects AMP Int	elligence		Depl	oy 🔍 System	Help 🔻 admin 🔻	
Con	text E	cplorer C	onnections • I	Events Intrusions • Files •	Hosts V U	sers • Correlation	n • Advanced •	Search		
						Bookmark This	Page Report Designe	r Dashboard View B	lookmarks Search •	
Con Con	Connection Events (switch workflow) Connections with Application Details > Table View of Connection Events Expanding Search Constraints (Edit Search Save Search) Disabled Columns									
► Se	arch Co	onstraints ( <u>Edi</u>	t Search Save Sea	arch)					Disabled Columns	
3.	imp to.									
		Action ×	Initiator × IP	Initiator User ×	Responder × IP	Ingress × Security Zone	Egress Security Zone	Source Port / × ICMP Type	Destination Port / × ICMP Code	
4		Allow	iii <u>10.10.10.1</u>	📇 it admin (LAB-AD\it.admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62473 / tcp	3389 / tcp	
4		Block	<u>10.10.10.1</u>	📇 it admin (LAB-AD\it.admin, LDAP)	<u>192.168.1.1</u>	outside-zone	inside-zone	62474 / tcp	80 (http) / tcp	
4		Block	10.10.10.1	R it admin (LAB-AD\it.admin, LDAP)	192.168 1 1	outside-zone	inside-zone	62475 / tcp	80 (http) / tcp	

사용자 **테스트 사용자**의 경우 서버에 대한 RDP 트래픽이 차단되고 포트 80 트래픽이 허용되는지 확인할 수 있습니다.

Overview	Analysi	is Policies I	Devices O	)bjects   /	AMP Inte	elligence				Deploy	, <b>Q</b>	System	Help 🔻	admin 🔻	
Context E	xplorer C	onnections + E	Events I	ntrusions 🔻	Files 🔻	Hosts •	Users v	Correlation	n 🔻 🛛 Advan	nced 🔻	Search				
								Bookmark This	Page Report	Designer	Dashboan	d View B	ookmarks	Search +	
Connection Events (switch workflow)         Connections with Application Details > Table View of Connection Events         • Search Constraints (Edit Search Save Search)         Jump to															
	Action ×	Initiator × IP	Initiator Us	ser ×		Responder IP	× Ing Sec	ress × arity Zone	Egress Security Z	one×	Source P ICMP Ty	<u>Port /</u> × pe	Destina ICMP (	ation Port / ode	3
1	Block	10.10.10.1	📇 <u>test user</u>	(LAB-AD\test	user, LDAP)	192.168	L <u>1 outs</u> i	de-zone	inside-zone		<u>62493 / t</u>	50	3389 / t	50	
4	Allow	10.10.10.1	📇 <u>test user</u>	(LAB-AD\test	user, LDAP)	192.168	L <u>1</u> outsi	de-zone	inside-zone		62494 / to	CD.	80 (http	) / tcp	

# 문제 해결

# 디버그

이 디버그는 진단 CLI에서 LDAP 인증 관련 문제를 해결하기 위해 실행할 수 있습니다. debug Idap 255

#### 사용자 ID 액세스 제어 정책 문제를 해결하기 위해 **시스템 지원 firewall-engine-debug를 클라이언 트로 실행하여 트래픽**이 예기치 않게 허용되거나 차단되는 이유를 확인할 수 있습니다.

#### LDAP 디버깅 작업

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
       Base DN = [DC=example,DC=com]
       Filter = [sAMAccountName=it.admin]
        Scope = [SUBTREE]
[53] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53] objectClass: value = top
[53]
      objectClass: value = person
[53]
       objectClass: value = organizationalPerson
[53]
       objectClass: value = user
       cn: value = IT Admin
[53]
       sn: value = Admin
[53]
      givenName: value = IT
[53]
[53]
      distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]
      instanceType: value = 4
      whenCreated: value = 20200421025811.0Z
[53]
       whenChanged: value = 20200421204622.0Z
[53]
       displayName: value = IT Admin
[53]
[53]
       uSNCreated: value = 25896
[53]
       memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
       uSNChanged: value = 26119
[53]
[53]
      name: value = IT Admin
       objectGUID: value = &...J..O..2w...c
[53]
       userAccountControl: value = 512
[53]
[53]
      badPwdCount: value = 6
[53]
       codePage: value = 0
[53]
       countryCode: value = 0
       badPasswordTime: value = 132320354378176394
[53]
[53]
      lastLogoff: value = 0
[53]
      lastLogon: value = 0
[53]
      pwdLastSet: value = 132319114917186142
       primaryGroupID: value = 513
[53]
[53]
       objectSid: value = ......{I...;....j...
       accountExpires: value = 9223372036854775807
[53]
[53]
       logonCount: value = 0
      sAMAccountName: value = it.admin
[53]
[53]
      sAMAccountType: value = 805306368
[53]
       userPrincipalName: value = it.admin@example.com
```

[53] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com [53] dSCorePropagationData: value = 16010101000000.0Z [53] lastLogonTimestamp: value = 132319755825875876 [53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1 [53] Session End

#### LDAP 서버와의 연결을 설정할 수 없음

[-2147483611] Session Start [-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication [-2147483611] Fiber started [-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389 [-2147483611] Connect to LDAP server: ldap://172.16.1.1:389, status = Failed [-2147483611] Unable to read rootDSE. Can't contact LDAP server. [-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2 [-2147483611] Session End

잠재적 솔루션:

- 라우팅을 확인하고 FTD가 LDAP 서버로부터 응답을 수신하는지 확인합니다.
- LDAPS 또는 STARTTLS를 사용하는 경우 SSL 핸드셰이크가 성공적으로 완료될 수 있도록 올 바른 루트 CA 인증서를 신뢰해야 합니다.
- 올바른 IP 주소 및 포트가 사용되었는지 확인합니다. 호스트 이름을 사용하는 경우 DNS에서 올 바른 IP 주소로 확인할 수 있는지 확인합니다.

#### 로그인 DN 및/또는 비밀번호 바인딩이 잘못되었습니다.

```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid
credentials
[-2147483615] Failed to bind as administrator returned code (-1) Can't contact LDAP server
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

잠재적 솔루션: 로그인 DN과 로그인 비밀번호가 적절하게 구성되었는지 확인합니다. 이는 AD 서버 에서 ldp.exe를 사용하여 확인할 수 있습니다. 계정이 ldp를 사용하여 성공적으로 바인딩할 수 있는 지 확인하려면 다음 단계를 수행하십시오.

1. AD 서버에서 Win+R을 누르고 ldp.exe를 검색합니다.

🖅 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	ldp.exe ~
	OK Cancel <u>B</u> rowse

2. 연결 아래에서 연결...을 선택합니다.



3. 서버의 localhost 및 적절한 포트를 지정한 다음 확인을 **클릭합니다**.

Connect		×
Server:	localhost	
Port:	389	Connectionless
<u>O</u> K		<u>C</u> ancel

4. 오른쪽 열에는 성공적인 연결을 나타내는 텍스트가 표시됩니다. Connection(**연결) > Bind...(바인** 딩...)로 이동합니다.

<u>6</u>	ldap://wir	n2016.exa	mple.co	om/DC:	example,DC=	=com		—		$\times$
Con	nection	Browse	View	Optio	ns Utilities	Help				
	Connect				ld = ldap_op Established	en("localh connectio	iost", 389); n to localhost.			^
	Bind		Ctrl+B		Retrieving b	ase DSA i	information			
	Disconne	ect			Getting 1 en	tries:				
			~	_	configu	ac) rationNami	inaContext:			
	New		Ctrl+N		CN=	Configura	ation,DC=examp	le,DC=c	om;	
	Save				current	Fime: 5/1/2	2020 4:16:55 PM	Easter	n Daylight	
	Save As				Tim	e; Iamia e Car	1	In DO		
					defaulti	tamingCon tName: wi	in 2016 example	com:	com;	
	Exit				domain(	ControllerF	unctionality: 7 =	( WIN2	016 );	
					domainF	unctionali	ity: 7 = ( WIN201	6);		
					dsServi	ceName: (	CN=NTDS			
					Set Firs	tings,CN=\ t-Site-	WIN2016,CN=Se	rvers,C	N=Default	-
					Nan con	ne,CN=Site n:	es,CN=Configura	ation,DC	=example	,DC=
					forestFi	unctionality	y: 7 = ( WIN2016	5);		
					highest	Committed	USN: 13410;			
					isGloba	CatalogRe	eady: TRUE;			
					isSynch	ronized: T	TRUE;			
l					IdanSer	viceName	example comit	vin2016	i	~

5. **단순 바인드를** 선택한 다음 **디렉토리 계정 사용자 이름**과 **비밀번호를 지정합니다**. OK(확인)를 클 릭합니다.

Bind	×					
<u>U</u> ser: Password:	ftd.admin@example.com					
Domain: Bind type Bind as <u>c</u> ur Bind with c Simple bind	Domain: Bind type Bind as currently logged on user Bind with credentials Simple bind Advanced (DIGEST)					
✓ <u>Encrypt</u> tra Ad <u>v</u> anced	affic after bind Cancel OK					

바인딩이 성공하면 ldp는 Authenticated as: DOMAIN\username(DOMAIN\username으로 인증됨)을 **표시합니다.** 

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		—		×
Connection	Browse	View	Options	Utilities	Help				
				1.2. 1.2. 1.2. supporte Max Max Max Max Max Max Max Max	840.113 840.113 840.113 edLDAPF Percentl Receive Connect BatchRe DirSyncl ResultSe ResultSe ResultSe ValRang edLDAPV edSASLI IEGO; EX	556.1.4.2255 556.1.4.2256 556.1.4.2309 Policies (20): DirSyncRequ Buffer; InitRe tions; MaxCo eturnMessag Duration; Max etSize; MinRe etSize; MinRe etSize; MinRe etSize; MinRe etSize; MinRe etSize; MinRe tions; MaxCo eturnMessag Duration; Max coryLimit; Sys Version (2): 3 Mechanisms (TERNAL; DK	admin".	hreads; Datagramf t; ; MaxPage leryDuratio leSize; ationPerC ationPerC itive; yLimitPerc ,PI; GSS- ; ample.com	Recv; eSize; on; onn; ent;
Ready									

유효하지 않은 사용자 이름 또는 비밀번호로 바인딩을 시도하면 여기에 표시된 2와 같은 실패가 발 생합니다.

🔝 Idap://wi	in2016.exa	mple.co	om/DC=ex	ample,DC:	=com		_		×
Connection	Browse	View	Options	Utilities	Help				
			r A E S C E in	Max Max Max Three supporte supporte SPN es = Idap_s unavailable tuthenticate es = Idap_s unavailable rror <49>: I server error comment: Ac rror 0x8009 tvalid	ResultSets ResultSets ValRange; adMemory edLDAPVer edSASLMer EGO; EXTE imple_bind_ >); // v.3 ed as: 'EXAl imple_bind_ >); // v.3 dap_simple : 80090308 cceptSecur 90308 The f	ize; MinResu PerConn; Ma MaxValRang Limit; Syster sion (2): 3; 3 chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad MPLE\ftd.adr _s(Id, 'wrong _bind_s() fa : LdapErr: D ityContext e token supplie	ultSets; axNotificat geTransition MemoryL 2; ): GSSAP ST-MD5; min@exar min@exar min/. g@examp ailed: Invali SID-0C09 rror, data ed to the f	ionPerConn ve; imitPercent; i; GSS- mple.com', id Credentia 042A, 52e, v3839 unction is	ls
Ready			ļ						<ul> <li>✓</li> </ul>

#### LDAP 서버가 사용자 이름을 찾을 수 없음

```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
       Base DN = [dc=example,dc=com]
       Filter = [samaccountname=it.admi]
       Scope
              = [SUBTREE]
[-2147483612] Search result parsing returned failure status
[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End
잠재적 솔루션: AD가 FTD에서 검색한 사용자를 찾을 수 있는지 확인합니다. 이 작업은 ldp.exe로도
가능합니다.
```

```
1. 위에 표시된 대로 성공적으로 바인딩한 후 보기 > 트리로 이동합니다.
```

2. FTD에 구성된 기본 DN을 지정한 다음 확인을 클릭합니다.

Tree View	×
BaseDN: DC=example,DC=com	~
Cancel	ОК

3. 기본 DN을 마우스 오른쪽 버튼으로 클릭한 다음 검색**을 클릭합니다**.

🔝 Idap://win2016.	example.co	om/DC=ex	ample,DC	=com	- D >	<
Connection Brows	e View	Options	Utilities	Help		
■ DC = example, DC	=com	Search Virtual L Delete Modify Modify Add chil Compar Advance	ist View DN Id re ed	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ple,DC=com; 11D1AA4B00C04FD7D83A:O s,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com;	^
		Copy Copy Select al Clear ou	N I Itput	Ctrl+C Ctrl+N	311D1ADED00C04FD8D5CD:C e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	t v
Create a new docum	ent					

4. 디버그에 표시된 것과 동일한 **기본 DB**, **필터** 및 **범위** 값을 지정합니다.

이 예에서는 다음과 같습니다.

- 기본 DN: dc=example,dc=com
- 필터: samaccountname=it.admi
- 범위:하위 트리

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 X
Connection	Browse View Options Utilities Help	
Search	×	C=example,DC=com; \$8811D1ADED00C04FD8D5CD:C
Base DN:	DC=example,DC=com ~	58811D1ADED00C04FD8D5CD:C
Filter:	sAMAccountName=it.admi ~	ample,DC=com; D211D1AA4B00C04FD7D83A:O
Scope O Base	○ One Level	lers,DC=example,DC=com; \$8811D1ADED00C04FD8D5CD:C =example,DC=com;
Attributes:	objectClass;name;description;canonicalName $\sim$	68811D1ADED00C04FD8D5CD:C mple,DC=com;
Options	Run Close	2020 3:43:59 PM Eastern Daylight 20 2:41:57 PM Eastern Daylight
	 ***Searching Idap_search_s(Id, "DC= "sAMAccountName=it.a Getting 0 entries:	=example,DC=com", 2, admi", attrList, 0, &msg)
Ready		

기본 DN dc=example,dc=com 아래에 samaccountname **it.admi**를 가진 사용자 계정이 없기 때문에 ldp는 0개의 항목을 찾습니다

올바른 samaccountname **it.admin**을 사용한 또 다른 시도로 다른 결과가 표시됩니다. ldp는 기본 DN dc=example,dc=com 아래에서 1개의 항목을 찾고 해당 사용자 DN을 인쇄합니다.

🔝 Idap://w	in2016.example.com/l	DC=example,DC	=com		_		×
Connection	Browse View Op	tions Utilities	Help				
Search			2	× 58 D	811D1ADED000 C=example,DC= 811D1ADED000	C04FD8D50 com; C04FD8D50	
Base <u>D</u> N:	DC=example,DC=com	1	· · · ·	⊿ an	nple,DC=com;		
<u>F</u> ilter:	sAMAccountName=it.a	admin	```		s,DC=example,	DC=com;	3A:0
Scope O <u>B</u> ase	O <u>O</u> ne Level	Subtree		58 =e: 68	811D1ADED000 xample,DC=com 811D1ADED00 ble.DC=com:	C04FD8D50 1; C04FD8D50	D:C CD:C
<u>A</u> ttributes:	objectClass;name;des	cription;canonical	Name 🕓	- 0.	20 3:43:59 PM E	astern Day	/light
Options		<u>R</u> un	<u>C</u> lose	)2	0 2:41:57 PM Ea	istern Dayl	ight
		***Searching Idap_search "sAMAccou Getting 1 en Dn: CN=IT / canonic name: fi objectC use	g n_s(ld, "DC intName=it. itries: Admin,CN calName: e: F Admin; lass (4): to er;	C=exar .admin I=Use xample op; per	nple,DC=com", 2 ", attrList, 0, &r <b>rs,DC=exampl</b> e.com/Users/IT son; organizatio	2, msg) l <b>e,DC=con</b> Admin; onalPerson	n ;
Ready							

#### 사용자 이름에 대한 잘못된 비밀번호

```
[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter = [samaccountname=it.admin]
               = [SUBTREE]
        Scope
[-2147483613] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
```

[-2147483613] Simple authentication for it.admin returned code (49) Invalid credentials
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment:
AcceptSecurityContext error, data 52e, v3839
[-2147483613] Invalid password for it.admin
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
Arm적 해결 방법: 사용자 비밀번호가 적절하게 구성되어 있고 만료되지 않았는지 확인하십시오.

로그인 DN과 마찬가지로 FTD는 사용자 자격 증명을 사용하여 AD에 바인딩합니다.

이 바인딩은 AD가 동일한 사용자 이름 및 비밀번호 자격 증명을 인식할 수 있는지 확인하기 위해 ldp에서도 수행할 수 있습니다. ldp의 단계는 Binding Login **DN and/or password incorrect 섹션에 나와 있습니다**.

또한 Microsoft server Event Viewer 로그를 검토할 수 있습니다.

#### 테스트 AAA

test aaa-server 명령을 사용하여 특정 사용자 이름 및 비밀번호로 FTD에서 인증 시도를 시뮬레이 션할 수 있습니다. 연결 또는 인증 실패를 테스트하는 데 사용할 수 있습니다. 이 명령은 test aaaserver authentication [AAA-server] host [AD IP/hostname](aaa-server 인증[AAA-server] 호스트 테 스트)입니다.

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
realm-id 7
aaa-server LAB-AD host win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type auto-detect
```

> test aaa-server authentication LAB-AD host win2016.example.com Username: it.admin Password: \*\*\*\*\*\*\* INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds) INFO: Authentication Successful

## 패킷 캡처

패킷 캡처를 사용하여 AD 서버에 대한 연결성을 확인할 수 있습니다. LDAP 패킷이 FTD를 떠났지 만 응답이 없는 경우 라우팅 문제를 나타낼 수 있습니다.

Capture(캡처)는 양방향 LDAP 트래픽을 표시합니다.

> show route 192.168.1.1

```
Routing entry for 192.168.1.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
 * directly connected, via inside
    Route metric is 0, traffic share count is 1
```

> capture AD interface inside match tcp any host 192.168.1.1 eq 389

```
> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
 match tcp any host 192.168.1.1 eq ldap
> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password
*****
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
 match tcp any host 192.168.1.1 eq ldap
> show capture AD
54 packets captured
   1: 23:02:16.770712
                            192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
                            192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
   2: 23:02:16.772009
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
   3: 23:02:16.772039
                            192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768
<nop,nop,timestamp 1061373058 762393884>
   4: 23:02:16.772482
                           192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145)
ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0>
                           192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
   5: 23:02:16.772924
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
   6: 23:02:16.772955
                           192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
<nop,nop,timestamp 1061373059 762393885>
   7: 23:02:16.773428
                           192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
                           192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
  8: 23:02:16.775030
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
   9: 23:02:16.775075
                           192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop,nop,timestamp 1061373061 762393887>
[...]
54 packets shown
```

#### Windows Server 이벤트 뷰어 로그

AD 서버에 대한 이벤트 뷰어 로그는 장애가 발생한 이유에 대한 자세한 정보를 제공할 수 있습니다. 1. 이벤트 뷰어를 검색하여 엽니다.

=	Best match							
ŵ	01	Event \ Desktop	<b>/iewer</b> app					
	Setting	5					>	
	🖄 Vie	ew ever	nt logs					
٢	10	۲	ß			₽	1 <sub>11</sub>	
	event							
-	Q	([])	e		1	2	8	

2. Windows 로그**를 확장하고 보안** 을 클릭합니다. 사용자 계정 **이름**으로 **감사** 실패를 검색하고 실 패 정보를 검토합니다.



An account failed to log on.

Subject: Security ID:SYSTEM Account Name:WIN2016\$ Account Domain:EXAMPLE Logon ID:0x3E7

Logon Type:3

Account For Which Logon Failed: Security ID:NULL SID Account Name:it.admin Account Domain:EXAMPLE

Failure Information:

Failure Reason: The specified user account has expired. Status: 0xC0000193 Sub Status: 0x0

Process Information: Caller Process ID:0x25c Caller Process Name:C:\Windows\System32\lsass.exe

Network Information: Workstation Name:WIN2016 Source Network Address:192.168.1.17 Source Port:56321 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.