# Konfigurieren der AD-Authentifizierung (LDAP) und Benutzeridentität auf dem vom FDM verwalteten FTD für AnyConnect-Clients

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfiguration Netzwerkdiagramm und Szenario **AD-Konfigurationen** LDAP-Basis-DN ermitteln **FTD-Konto erstellen** AD-Gruppen erstellen und AD-Gruppen Benutzer hinzufügen (optional) Kopieren Sie die LDAS SSL-Zertifikatsroot (nur für LDAPS oder STARTTLS erforderlich). **FDM-Konfigurationen** Lizenzierung überprüfen AD-Identitätsquelle einrichten Konfigurieren von AnyConnect für die AD-Authentifizierung Identitätsrichtlinie aktivieren und Sicherheitsrichtlinien für Benutzeridentität konfigurieren Überprüfung Endqültige Konfiguration Herstellen einer Verbindung mit AnyConnect und Überprüfen der Zugriffskontrollrichtlinien Fehlerbehebung Debugger Arbeiten mit LDAP-Debuggern Verbindung mit LDAP-Server kann nicht hergestellt werden Binden der Anmelde-DN und/oder des Kennworts falsch LDAP-Server kann Benutzernamen nicht finden Falsches Kennwort für Benutzername AAA testen Paketerfassung

Windows Server Event Viewer-Protokolle

# Einführung

In diesem Dokument wird erläutert, wie die Active Directory-Authentifizierung (AD) für AnyConnect-Clients konfiguriert wird, die mit einer Cisco FirePOWER Threat Defense (FTD) verbunden sind, die von FirePOWER Device Management (FDM) verwaltet wird. Die Benutzeridentität wird in den Zugriffsrichtlinien verwendet, um AnyConnect-Benutzer auf bestimmte IP-Adressen und Ports zu beschränken.

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der RA VPN-Konfiguration für FDM
- Grundkenntnisse der LDAP-Serverkonfiguration auf FDM
- Grundkenntnisse von AD

### Verwendete Komponenten

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

- Microsoft 2016-Server
- FTDv läuft 6.5.0

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

## Konfiguration

## Netzwerkdiagramm und Szenario



Windows-Server ist mit Internetinformationsdienste (IIS) und Remote Desktop Protocol (RDP) vorkonfiguriert, um die Benutzeridentität zu testen. In diesem Konfigurationsleitfaden werden drei Benutzerkonten und zwei Gruppen erstellt.

Benutzerkonten:

- FTD-Administrator: Diese wird als Verzeichniskonto verwendet, damit die FTD an den AD-Server gebunden werden kann.
- IT-Administrator: Ein Testadministrator-Konto, das zum Demonstrieren der Benutzeridentität verwendet wird.
- Testbenutzer: Ein Testbenutzerkonto, das zum Demonstrieren der Benutzeridentität verwendet wird.

Gruppen:

• AnyConnect-Administratoren: Eine Testgruppe, der IT-Administrator hinzugefügt wird, um die

Benutzeridentität nachzuweisen. Diese Gruppe hat nur RDP-Zugriff auf Windows Server.

• AnyConnect-Benutzer: Eine Testgruppe, der Testbenutzer hinzugefügt wird, um die Benutzeridentität zu demonstrieren. Diese Gruppe hat nur HTTP-Zugriff auf Windows Server.

### **AD-Konfigurationen**

Um die AD-Authentifizierung und die Benutzeridentität auf FTD korrekt konfigurieren zu können, sind einige Werte erforderlich. Alle diese Details müssen auf dem Microsoft Server erstellt oder gesammelt werden, bevor die Konfiguration auf dem FDM erfolgen kann. Die wichtigsten Werte sind:

- Domänenname: Dies ist der Domänenname des Servers. In diesem Konfigurationsleitfaden ist example.com der Domänenname.
- Server-IP/FQDN-Adresse: Die IP-Adresse oder der FQDN, die zum Erreichen des Microsoft-Servers verwendet wird. Wenn ein FQDN verwendet wird, muss ein DNS-Server innerhalb von FDM und FTD konfiguriert werden, um den FQDN aufzulösen. In diesem Konfigurationsleitfaden sind diese Werte win2016.example.com, die zu 192.168.1.1 aufgelöst wird.
- Server-Port: Der vom LDAP-Dienst verwendete Port. Standardmäßig verwenden LDAP und STARTTLS den TCP-Port 389 für LDAP und LDAP über SSL (LDAPS) den TCP-Port 636.
- Stammzertifizierungsstelle: Wenn LDAPS oder STARTTLS verwendet wird, ist die Root-CA zum Signieren des SSL-Zertifikats erforderlich, das von LDAPS verwendet wird.
- Benutzername und Kennwort des Verzeichnisses: Dies ist das Konto, das von FDM und FTD verwendet wird, um eine Verbindung zum LDAP-Server herzustellen, Benutzer zu authentifizieren und nach Benutzern und Gruppen zu suchen. Zu diesem Zweck wird ein Konto mit dem Namen FTD Admin erstellt.
- DN (Base Distinguished Name): Die Basis-DN ist der Ausgangspunkt f
  ür FDM, und die FTD weist Active Directory an, bei der Suche nach Benutzern anzufangen. In diesem Konfigurationsleitfaden wird die Stammdom
  äne example.com als Basis-DN verwendet. In einer Produktionsumgebung kann es jedoch besser sein, einen Basis-DN weiter in der LDAP-Hierarchie zu verwenden. Nehmen wir zum Beispiel die folgende LDAP-Hierarchie:



Wenn ein Administrator möchte, dass Benutzer innerhalb der Marketing-Organisationseinheit die Basis-DN auf den Root (example.com) authentifizieren können, kann sich User1 unter der Abteilung Finance organizational ebenfalls anmelden, da die Benutzersuche am Root beginnt und zu Finanzen, Marketing und Forschung führt.

Basis-DN auf beispiel.com festgelegt.



Um Anmeldungen auf Benutzer in der Organisationseinheit Marketing und darunter zu beschränken, kann der Administrator stattdessen die Basis-DN auf Marketing festlegen. Jetzt können sich nur Benutzer2 und User3 authentifizieren, da die Suche bei Marketing beginnt.

Basis-DN auf Marketing eingestellt:



Beachten Sie, dass für eine detailliertere Steuerung innerhalb der FTD, für die Benutzer Verbindungen herstellen oder Benutzern unterschiedliche Autorisierungen basierend auf ihren AD-Attributen zuweisen dürfen, eine LDAP-Autorisierungszuordnung konfiguriert werden muss.

Diese vereinfachte LDAP-Hierarchie wird in diesem Konfigurationsleitfaden verwendet, und der DN für die root example.com wird für die Basis-DN verwendet.



#### LDAP-Basis-DN ermitteln

1. Öffnen Sie AD-Benutzer und -Computer.

=	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. Klicken Sie mit der linken Maustaste auf die Stammdomäne (um den Container zu öffnen), klicken Sie mit der rechten Maustaste auf die Stammdomäne, navigieren Sie dann zu **Ansicht**, und klicken Sie auf **Erweiterte Funktionen**.



3. Dadurch wird die Ansicht zusätzlicher Eigenschaften unter den AD-Objekten aktiviert. Um z. B. den DN für die root example.com zu suchen, klicken Sie mit der rechten Maustaste auf **example.com** und navigieren Sie dann zu **Properties**.

Active Directory Users and Computers			-	х
File Action View Help				
🗢 🔶 📶 🗖 🖾 🧟 🖓 🖓 🖓	2 %			
Active Directory Users and Com Saved Queries  Saved Queries  Saved Queries  Sultin  Sultin  Delegate Control  Find  Change Domain  Change Domain Controller  SubstAndFc  Subs	ain 1al 1d 1C 1r eU	Description Default container for up Default container for do Default container for sec Default container for or Default location for stor Builtin system settings Default container for up Quota specifications co		
and the second se	_			

4. Klicken Sie unter **Eigenschaften** auf die Registerkarte **Attributeditor**. Suchen Sie **DistinguishedName** unter Attributes, und klicken Sie dann auf **Anzeigen**.

example.	com Propertie	5			?	×
General	Managed By	Object	Security	Attribute E	dtor	
Attribute	88:					
Attribu	te	Valu	e			^
dc		exar	nple			
defau	tLocalPolicyOb	j knot	set>			
descri	ption	knot	set>			
deskt	op Profile	knot	set>			
displa	yName	knot	set>			
displa	vNamePrintable	e knot	set>	_		_
disting	uishedName	DC=	example.D	C=com		
domai	nPolicyObject	<not< td=""><th>set&gt;</th><td></td><td></td><td></td></not<>	set>			
domai	nReplica	<not< td=""><th>set&gt;</th><td></td><td></td><td></td></not<>	set>			
dSAS	ignature	{V1	: Flags = Ox	0; Latency:	Secs = 0; Ds	aGuic
dSCo	rePropagationD	0x0	=()			
eFSP	olicy	snot	set>			
exten	sionName	<not< td=""><th>set&gt;</th><td></td><td></td><td></td></not<>	set>			
flags		<not< td=""><th>set&gt;</th><td></td><td></td><td>~</td></not<>	set>			~
<						>
V	ew				ł	Filter
	OK		Cancel	Apr	bly	Help

5. Dadurch wird ein neues Fenster geöffnet, in das die DN kopiert und später in FDM eingefügt werden kann. In diesem Beispiel lautet die Root-DN DC=example, DC=com. Kopieren Sie den Wert. Klicken Sie auf **OK**, um das Fenster Zeichenfolgen-Editor zu verlassen, und klicken Sie erneut auf **OK**, um die Eigenschaften zu verlassen.

tring Attribute Editor		×		
ttribute: distingu	ishedName			
/alue:				
DC=example,DC=com			Undo	
Clear	OK	Cancel	Cr4	
			Conv	
			Deste	
			Paste	
			Delete	
			Select All	
			Right to left Reading order	
			Show Unicode control characters	
			Insert Unicode control character	>
Attributes:	Value	^		
Autobules.				
Attribute	Value	^		
cn controlAccess Dishte	<not set=""></not>			
creation Time	4/29/2020 2:43:49 PM Fastern Davis	aht Tim		
de	example	<u>, , , , , , , , , , , , , , , , , , , </u>		
defaultLocalPolicyObj	<not set=""></not>			
description	<not set=""></not>			
desktopProfile	<not set=""></not>			
displayName	<not set=""></not>			
displayNamePrintable	<not set=""></not>	_		
distinguishedName	DC=example,DC=com			
domainPoicyObject	shot sets			
dSASionature	{ V1: Base = 0x0: Latency Sace = 0: (	lea Grée		
dSCorePropagationD	(v), hags - axo, Latency secs = 0, L (v) = ()	~		
<	0.0 - 1 /	>		
View		Filter		
OK	Cancel Apply	Help		

Dies kann für mehrere Objekte in AD erfolgen. Diese Schritte werden beispielsweise verwendet, um die DN des Benutzercontainers zu finden:

Active Directory Users and C	omputers	-	$\times$
File Action View Help			
🗢 🔿 🙍 🚾 🖌 🗈 👂	Users Properties ? ×		
<ul> <li>Active Directory Users and Q</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrinc</li> <li>LostAndFound</li> <li>Hongram Data</li> <li>System</li> <li>Users</li> <li>NTDS Quotas</li> <li>TPM Devices</li> </ul>	Users Properties ? X General Object Security Attribute Editor Attributes: Attribute Value ^ ^ adminDescription <not set=""> adminDisplayName <not set=""> on Users defaultClassStore <not set=""> defaultClassStore <not set=""> defaultClassStore <not set=""> defaultClassStore <not set=""> displayName <not set=""> fSMORoleOwner <not set=""> instanceType Qx4 = (WRITE) <v </v </not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>		*
	OK Cancel Apply Help		
<			~

6. Die Ansicht Erweiterte Funktionen kann entfernt werden. Klicken Sie mit der rechten Maustaste auf die Root-DN, navigieren Sie zur **Ansicht**, und klicken Sie erneut auf **Erweiterte Funktionen**.



#### FTD-Konto erstellen

Dieses Benutzerkonto ermöglicht es dem FDM und der FTD, sich mit dem AD zu verbinden, um Benutzer und Gruppen zu suchen und zu authentifizieren. Der Zweck der Erstellung eines separaten FTD-Kontos besteht darin, den unbefugten Zugriff an anderen Stellen im Netzwerk zu verhindern, wenn die für die Bindung verwendeten Anmeldeinformationen beeinträchtigt werden. Dieses Konto muss nicht im Rahmen der Basis-DN liegen.

1. Klicken Sie in Active Directory-Benutzer und -Computer mit der rechten Maustaste auf den Container/die Organisation, dem das FTD-Konto hinzugefügt wird. In dieser Konfiguration wird das FTD-Konto unter dem Benutzercontainer unter dem Benutzernamen ftd.admin@example.com hinzugefügt. Klicken Sie mit der rechten Maustaste auf Benutzer, und klicken Sie dann auf Neu > Benutzer.

Active Directory	Users and Comp	puters				-	×
File Action View	w Help						
🗢 🔿 🔁 📆	X 🗈 🗙 🛙	i 🧟 🗟 🛛	Þ	1 🗏 🐮 🛯	r 🗾 🔍		
Active Directory I Active Directory I Saved Queries Saved Queri	Users and Com s rs Controllers curityPrincipal: Service Accour Delegate Con Find	Name DefaultAcc Denied ROI DonsAdmins DonsUpdate Domain Ad Domain Co trol	o D s P i n	Type User Security Group Security Group Security Group Security Group Security Group Security Group	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		^
	New All Tasks View Refresh Export List Properties	>	ers	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr	ntial PropertyList incipalContainer		
< Creates a new item in	Help	WseAlertA WseAllow WseAllow		msImaging-PSP: MSMQ Queue Al Printer User Shared Folder	ias		~

2. Navigieren Sie durch den Assistenten New Object - User.

New Object - User		х			
🤱 Create in:	example.com/Users				
First name:	FTD Initials:				
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 > Cance	1			

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. Überprüfen Sie, ob das FTD-Konto erstellt wurde. Darüber hinaus wurden zwei zusätzliche Konten erstellt: **IT-Administrator** und **Testbenutzer**.

Active Directory Users and Composite	uters			-	×
File Action View Help					
🗢 🔿 🙍 📷 🖌 🗈  🗶 📴	a 🔒 🛛 🖬	1 % 🔌 🛍 🖷	r 🧕 🗽		
Active Directory Users and Com Saved Queries Saved Com	Name	Type User	Description A user account manage		^
<ul> <li>example.com</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>Managed Service Accour</li> <li>Users</li> </ul>	Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co Domain Con Domain Gue Domain Users	Security Group Security Group Security Group Security Group Security Group Security Group Security Group	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		
	Kenterprise A Enterprise K Enterprise R FTD Admin Group Polic	Security Group Security Group Security Group User Security Group User	Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue		
<	LT Admin Key Admins Protected Us RAS and IAS Read-only D Schema Ad Test User	User Security Group Security Group Security Group Security Group User	Members of this group Members of this group Servers in this group can Members of this group Designated administrato		~

#### AD-Gruppen erstellen und AD-Gruppen Benutzer hinzufügen (optional)

Obwohl die Authentifizierung nicht erforderlich ist, können Gruppen verwendet werden, um die Anwendung von Zugriffsrichtlinien auf mehrere Benutzer sowie die LDAP-Autorisierung zu vereinfachen. In diesem Konfigurationsleitfaden werden Gruppen verwendet, um die Richtlinieneinstellungen für die Zugriffskontrolle später über die Benutzeridentität innerhalb des FDM anzuwenden.

1. Klicken Sie in **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf den Container bzw. die Organisation, der bzw. der die neue Gruppe hinzugefügt wird. In diesem Beispiel wird die Gruppe **AnyConnect-Administratoren** unter dem Benutzercontainer hinzugefügt. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und klicken Sie dann auf **Neu > Gruppe**.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🙇 📰 🔏 🖬 🗙 🛙	3 🙆 📑 🚺 🖬	1 🗏 🐮 🛯	r 🔟 🕱		
Active Directory Users and Com Saved Queries Saved Queries Save	Name DefaultAcco Denied ROD DisAdmins DisUpdateP Domain Ad Domain Co	Type User 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 Tasks View Refresh	> > >	Computer Contact Group InetOrgPerson msDS-KevCreder	ntial		
Export List Properties Help	Read-only	msDS-ResourceP msDS-ShadowPr msImaging-PSP: MSMQ Queue Al Drinter	PropertyList incipalContainer s lias		
< >> Creates a new item in this container.	Schema A	User Shared Folder			Ŷ

2. Navigieren Sie durch den Assistenten **New Object - Group** (Neues Objekt - Gruppe), wie im Bild gezeigt.

New Object - Group		×
Create in: example.com	n/Users	
Group name:		
AnyConnect Admins		
Group name (pre-Windows 2000):		
AnyConnect Admins		
Group scope	Group type	
O Domain local	Security	
Global	ODistribution	
OUniversal		
	OK Cancel	

3. Überprüfen Sie, ob die Gruppe erstellt wurde. Die Gruppe **AnyConnect-Benutzer** wurde ebenfalls erstellt.

Active Directory Users and Com	puters			_	×
File Action View Help					
🗢 🔿 🙇 📰 🐇 🗶 🔛 🛙	è   🛛 🖬   🐍 🔌 🛍 '	7 🗾 🐍			
Active Directory Users and Com Saved Queries Saved Queries Builtin Sign Computers Sign Domain Controllers Sign ForeignSecurityPrincipals Sign Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount Domain RODC Passw DnsUpdateProxy Domain Admins DosUpdateProxy Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Domain Guests Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Type Security Group Security Group User Security Group User Security Group Security Group User User User Security Group	Description Built-in account for ad Members of this group Members of this group t 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 guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue		
,	(m.s		11 1 2.1. <sup>2</sup>		

4. Klicken Sie mit der rechten Maustaste auf die Gruppe, der der Benutzer hinzugefügt wird, und wählen Sie dann **Eigenschaften aus**. In dieser Konfiguration wird der Benutzer **IT-Administrator** der Gruppe **AnyConnect-Administratoren** hinzugefügt, und der Benutzer **Test-Benutzer** wird der Gruppe **AnyConnect-Benutzer** hinzugefügt.

Active Directory Users and Composite	Active Directory Users and Computers							
File Action View Help								
🗢 🔿 🙍 📰 🔏 🗈  🖾	🖻 🗟 📲 🚮 🖏	k 🛙 🔻 🧕 🕯	5					
Active Directory Users and Com	Name	Type Security Group	Description			^		
<ul> <li>✓ math with a second se</li></ul>	AnyConnect Users Calo Cert Publishers	Security Group User Security Group Security Group	Add to a group Buil Move Mer Send Mail Mer All Tasks	>				
> Ganaged Service Accour	DefaultAccount Controllers Consult RODC Passw Consult RODC Pas	User Security Group Security Group Security Group Security Group Security Group	A u: Mer Cut DNS Delete DNS Rename Des All v Properties All v Help					
	Domain Guests Domain Users Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Security Group Security Group Security Group Security Group User User User User Security Group	All domain users Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue					
Renames the current selection.	(h.s					Ŷ		

5. Klicken Sie auf die Registerkarte **Members** und anschließend auf **Add** (Hinzufügen), wie im Bild gezeigt.

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

Geben Sie den Benutzer in das Feld ein, und klicken Sie auf die Schaltfläche **Namen überprüfen**, um zu überprüfen, ob der Benutzer gefunden wurde. Klicken Sie nach der Überprüfung auf **OK**.

Select Users, Contacts, Computers, Service Accounts, or O	Groups X
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

Überprüfen Sie, ob der richtige Benutzer hinzugefügt wurde, und klicken Sie dann auf die Schaltfläche **OK**. Der Benutzer Testbenutzer wird auch zur Gruppe AnyConnect-Benutzer hinzugefügt, wobei dieselben Schritte verwendet werden.

AnyConn	ect Admin	s Properties		?	×
General	Members	Member Of	Managed By		
Membe	rs:				
Name & IT	Admin	Active Dir example.c	ectory Domain Services Folde xom/Users	H.	
	_				
Ad	d	Remove			
			OK Cancel	Ą	oply

Kopieren Sie die LDAS SSL-Zertifikatsroot (nur für LDAPS oder STARTTLS erforderlich).

1. Drücken Sie Win+R, und geben Sie mmc.exe ein. Klicken Sie auf OK.

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

2. Navigieren Sie zu Datei > Snap-In hinzufügen/entfernen... wie im Bild gezeigt.

🚡 Co	nsole1 - [C	onsole F	Root]		-	×
🚡 File	Action	View	Favorites	Window	Help	- 8 >
4	New			Ctrl+N		
	Open			Ctrl+O	Actions	
	Save Save Ar			Ctrl+S	There are no items to show in this view. Console Root	-
	Add/Rem Options 1 dnsmgu 2 dsa Exit	nove Sna mt	ıp-in	Ctrl+M	More Actions	•
Enables	you to add	snap-in	is to or remo	ove them fro	om the snap-in console.	

3. Klicken Sie unter Verfügbare Snap-Ins auf Zertifikate und dann auf Hinzufügen.

Add or Remove Snap-ins				×
You can select snap-ins for t extensible snap-ins, you can	his console from the configure which e	iose xter	e available on your computer and configure the selected set of snap-ins. For ensions are enabled.	
Available snap-ins:			Selected snap-ins:	
Snap-in	Vendor	^	Console Root Edit Extensions	
Active Directory Do	Microsoft Cor		Remove	1
Active Directory Site	Microsoft Cor			
Active Directory Use	Microsoft Cor		Maua Lia	
ActiveX Control	Microsoft Cor		Hove gp	
Authorization Manager	Microsoft Cor		Move Down	
Certificate Templates	Microsoft Cor		<u>A</u> dd >	
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			_
Disk Management	Microsoft and	¥	Ad <u>v</u> anced	
Description				
The Certificates enancie alle	we way to become	the	a contante of the cartificate stores for varicality a carvical or a computer	
The Cerdicates shap in all	ms you to bromse	uie	e contents of the certificate stores for yoursen, a service, or a computer.	
L				_
			OK Cancel	
		_		

4. Wählen Sie Computerkonto aus, und klicken Sie dann wie im Bild gezeigt auf Weiter.

Certificates snap-in	$\times$
This snap-in will always manage certificates for: My user account Service account Computer account	
< Back Next > Cancel	

Klicken Sie auf Fertig stellen.

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

### 5. Klicken Sie auf OK.

Add or Remove Snap-ins							×
You can select snap-ins for t extensible snap-ins, you can	his console from the configure which e	nose xter	available on you nsions are enable	ur computer and cor ed.	figure the selected s	et of snap-ins. For	
Available snap-ins:				Selected snap-ins:			
Snap-in	Vendor	^		Console Root		Edit Extensions	
Active Directory Do	Microsoft Cor			Q Certificates	(Local Computer)	<u>R</u> emove	
Active Directory Use	Microsoft Cor						
ActiveX Control	Microsoft Cor					Move <u>U</u> p	
ADSI Edit	Microsoft Cor					Move Down	
Authorization Manager	Microsoft Cor		<u>A</u> dd >				-
Certificates	Mcrosoft Cor						
Certification Authority	Microsoft Cor						
Component Services	Microsoft Cor						
Computer Managem	Microsoft Cor						
Device Manager	Microsoft Cor						
T Disk Management	Microsoft and	v				Advanced	
Descriptions			1				
The Certificates energie all	un un te brouge	the	contrate of the	contificate stores fo	r un realf a convice	or a computer	
The Certificates shap-in all	ws you to browse	uie	contents of the	ceruncate stores ro	r yourself, a service,	or a computer.	
						OK Cancel	

6. Erweitern Sie den **persönlichen** Ordner, und klicken Sie dann auf **Zertifikate**. Das von LDAPS verwendete Zertifikat muss an den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Windows-Servers ausgestellt werden. Auf diesem Server sind drei Zertifikate aufgelistet.

- Ein Zertifizierungsstellenzertifikat, das an und von Beispiel-WIN2016-CA ausgestellt wird.
- Ein Identitätszertifikat, das WIN2016 vom Beispiel-WIN2016-CA ausgestellt wurde.
- Ein Identitätszertifikat, das von example-WIN2016-CA für win2016.example.com ausgestellt wurde.

In diesem Konfigurationsleitfaden lautet der FQDN "win2016.example.com", daher sind die ersten beiden Zertifikate nicht für die Verwendung als LDAPS SSL-Zertifikat gültig. Das für win2016.example.com ausgestellte Identitätszertifikat ist ein Zertifikat, das automatisch vom Zertifizierungsstellendienst für Windows Server ausgestellt wurde. Doppelklicken Sie auf das Zertifikat, um die Details zu überprüfen.



7. Um als LDAPS SSL-Zertifikat verwendet zu werden, muss das Zertifikat die folgenden Anforderungen erfüllen:

- Der allgemeine Name oder der alternative DNS-Betreff-Name entspricht dem FQDN des Windows-Servers.
- Das Zertifikat verfügt über eine Serverauthentifizierung im Feld Verwendung des erweiterten Schlüssels.

Auf der Registerkarte Details des Zertifikats unter dem **Betreff** und dem **Betreff Alternative Name** ist FQDN **win2016.example.com** vorhanden.

🙀 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>		~	
Field	bject Key thority Ke L Distribu thority In	Identifier ty 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 Other Name:DS Object Guid=	^
Ke Th Th	y Usage umbprint umborint	algorithm	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	
			O	ĸ

Unter Erweiterte Schlüsselverwendung ist Serverauthentifizierung vorhanden.

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<a<b>I&gt;</a<b>		~	
Field			Value	^
E Su E Pu E Pu	bject blic key blic key p	arameters	win2016.example.com RSA (2048 Bits) 05 00	
Ce	rtificate T	emplate Name	DomainController	
Client J	IIME Capa bject Key thority Ka Authentic Authentic	bilities Identifier v Identifier tion (1.3.6.1.5.5.) ation (1.3.6.1.5.5.)	[1]SMIME Capability: Object I 30 b7 2b 4e 48 0f 2f 17 17 e6 KevID=3d 9f 26 37 fb 11 1f 4 7.3.2) .7.3.1]	*
		Ed	It Properties Copy to File	
			0	ĸ

8. Navigieren Sie nach der Bestätigung zur Registerkarte **Zertifizierungspfad**. Klicken Sie auf das oberste Zertifikat, das das Stammzertifikat der Zertifizierungsstelle sein soll, und klicken Sie dann auf die Schaltfläche **Zertifikat anzeigen**.

Certificate	×
General Details Certification Path	
Certification path	
example-WIN2016-CA	
View Certificate	
Certificate status:	
This certificate is OK.	
ок	

9. Dadurch werden die Zertifikatdetails für das Stammzertifikat der CA geöffnet.

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

10. Öffnen Sie die Registerkarte **Details**, und klicken Sie dann auf **In Datei kopieren...** wie im Bild gezeigt.

📰 Certificate	×
General Details Certification Path	
Show: <all></all>	$\checkmark$
Field	Value ^
Version Serial number Signature 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:
E	It Properties Copy to File
	ОК

11. Navigieren Sie durch den Assistenten für den Zertifikatsexport, der die Stammzertifizierungsstelle im PEM-Format exportiert.

÷	🛃 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, click Next.	
	<u>Next</u> Cance	

12. Wählen Sie Base-64-verschlüsseltes X.509 aus.

rt File Format Certificates can be	exported in a variety of file formats.
Select the format y	ou want to use:
O DER encode	d binary X.509 (.CER)
Base-64 enc	oded X.509 (.CER)
○ Cryptograph	ic Message Syntax Standard - PKCS #7 Certificates (,P78
Include a	all certificates in the certification path if possible
O Personal Infe	ormation Exchange - PKCS #12 (.PFX)
Indude a	all certificates in the certification path if possible
Delete t	he private key if the export is successful
Export a	Il extended properties
Enable o	ertificate privacy
O Microsoft Se	rialized Certificate Store (.SST)

13. Wählen Sie den Namen der Datei und den Speicherort aus, in den die Datei exportiert werden soll.

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	

14. Klicken Sie auf Fertig stellen.

÷	Ş	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\admin\Desktop\root.cer	
		Export Keys	No	
		Include all certificates in the certification path	No	
		File Format	Base64 Encoded X.509 (*.cer)	
			Finish Canc	el

15. Navigieren Sie jetzt zum Speicherort, und öffnen Sie das Zertifikat mit einem Notizblock oder einem anderen Texteditor. Es wird das PEM-Formatzertifikat angezeigt. Speichern Sie diese Datei später.

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

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S23161zdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
```

----END CERTIFICATE----

## FDM-Konfigurationen

#### Lizenzierung überprüfen

Um AnyConnect auf FDM zu konfigurieren, muss die FTD beim Smart Licensing-Server registriert und eine gültige Plus-, Apex- oder VPN Only-Lizenz auf das Gerät angewendet werden.

#### 1. Navigieren Sie zu Gerät > Smart License wie im Bild gezeigt.

cisco. Firepower Devic	e Manager	Monitoring	Ø Policies	₩E Objects	Device: FTD-3		$\bigcirc$	٢	0	?	:	admin Administrator
	Fig. Inside Netwo	Ciaco Firapo	ower Threat Defe	0/1 0/2 0/2 0/2	MGAT	ISP/WAN/Geter	way	Constant	tormot S Server			
			1	•v•]	console			that Se	iart Licen	150		
Interfaces Connected Erabled 3 of 4 View All Interfaces	>	Routing 2 routes View Configura	ntion	>	Updates Geolocation, Ru Security Intellige View Configura	le, VDB, System Up ance Feeds ttion	igrade, <b>&gt;</b>		Syst Mana Loggi DHCP DNS S	gement / ing Settin Server Server	ettings Access ags	
Smart License Registered View Configuration	>	Backup and	I Restore	>	Troubleshoo No files created REQUEST FIL	DÎ yet E TO BE CREATED			Hostn NTP Cloud Rebox Traffi	ame I Service ot/Shutd ic Setting	s own gs	-

2. Überprüfen Sie, ob die FTD beim Smart Licensing Server registriert ist und die AnyConnect Plus-, Apex- oder VPN Only-Lizenz aktiviert ist.



#### AD-Identitätsquelle einrichten

1. Navigieren Sie zu **Objekte > Identitätsquellen**, klicken Sie dann auf das **+**-Symbol, und wählen Sie **AD** wie im Bild dargestellt aus.

cisco. Firepower Devic	ce Manager Monitoring Policie	s Objects Device: FTD-3	: ? @ 🦂 🔇	admin Administrator
Object Types 🔶 ^	Identity Sources			
Networks	1 object		Q Search	+ ~
와 Ports	a NAME	THE	VALUE	RADIUS Server
🔒 Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
🐔 Application Filters				AD
🖉 URLs				Identity Services Engine
Geolocations				
🥈 Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
🔒 AnyConnect Client				
E Identity Sources				
1 Users				
R Certificates				
🔒 Secret Keys				
DNS Groups				
Event List Filters				

2. Füllen Sie die entsprechenden Einstellungen für den Active Directory-Server mit den zuvor gesammelten Informationen aus. Wenn für den Microsoft-Server anstelle einer IP-Adresse ein Hostname (FQDN) verwendet wird, stellen Sie sicher, dass unter Objects > DNS Group (Objekte > DNS-Gruppe) eine entsprechende DNS-Gruppe erstellt wird. Wenden Sie dann diese DNS-Gruppe auf die FTD an, indem Sie zu Device > System Settings > DNS Server navigieren, die DNS-Gruppe unter der Management Interface (Verwaltungsschnittstelle) und Data Interface (Datenschnittstelle) anwenden und dann die entsprechende Ausgangsschnittstelle für DNS-Abfragen angeben. Klicken Sie auf die Test-Schaltfläche, um die erfolgreiche Konfiguration und Erreichbarkeit über die Verwaltungsoberfläche der FTD zu überprüfen. Da diese Tests von der Verwaltungsschnittstelle der FTD und nicht über eine der im FTD konfigurierten routingfähigen Schnittstellen (z. B. innen, außen, dmz) initiiert werden, gewährleistet eine erfolgreiche (oder fehlgeschlagene) Verbindung nicht das gleiche Ergebnis für die AnyConnect-Authentifizierung, da AnyConnect LDAP-Authentifizierungsanforderungen von einer der routingfähigen Schnittstellen der FTD initiiert werden. Weitere Informationen zum Testen von LDAP-Verbindungen vom FTD finden Sie in den Abschnitten Test AAA und Packet Capture im Bereich Troubleshooting (Fehlerbehebung).

Add Identity Realm

Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name	Туре
LAB-AD	Active Directory (AD)
Directory Username	Directory Password
ftd.admin@example.com	******
e.g. user@example.com	
Base DN	AD Primary Domain
DC=example,DC=com	example.com
e.g. ou=user, dc=example, dc=com	e.g. example.com
Directory Server Configuration	
win2016.example.com:389	*
Hostname / IP Address	Port
win2016.example.com	389
e.g. ad.example.com	
Encryption	Trusted CA certificate
NONE ~	Please select a certificate ~
TEST ✓ Connection to realm is successful	
Add another configuration	
	CANCEL
	CAINGEL OK

Wenn LDAPS oder STARTTLS verwendet wird, wählen Sie die entsprechende Verschlüsselung aus, und wählen Sie dann das Zertifikat der vertrauenswürdigen Zertifizierungsstelle aus. Wenn die Stammzertifizierungsstelle nicht bereits hinzugefügt wurde, klicken Sie auf **Neues Zertifikat für vertrauenswürdige CA erstellen**. Geben Sie einen Namen für das Stammzertifikat der Zertifizierungsstelle ein, und fügen Sie dann das zuvor erfasste Root-Zertifizierungsstellenzertifikat im PEM-Format ein.

## Add Trusted CA Certificate

Name LDAPS_ROOT	
Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.	
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjlwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC ASlwDOX IKoZlbycNAOEBBOADgoEPADCCAOoCggEBAl8gbTZ19NzSOpgOPb0YT67b	
CANCEL	ок
Directory Server Configuration	
win2016.example.com:636	•

Port

636

Trusted CA certificate

LDAPS\_ROOT

8 X

```
TEST
```

Hostname / IP Address

e.g. ad.example.com

Encryption

LDAPS

win2016.example.com

✓ Connection to realm is successful

In dieser Konfiguration wurden folgende Werte verwendet:

- Name: LAB-AD
- Verzeichnisbenutzername: ftd.admin@example.com
- Basis-DN: DC=Beispiel, DC=com
- Primäre AD-Domäne: example.com
- Hostname/IP-Adresse: win2016.example.com
- Anschluss: 389
- 3. Klicken Sie oben rechts auf die Schaltfläche Ausstehende Änderungen, wie im Bild gezeigt.

cisco. Firepower De	vice Manager Monitoring Po	Cies Objects Device: FTD-3	٥ 🕲 🔄	admin Administrator
Object Types 🛛 🗧 🗧	Identity Sources			
C Networks	2 objects		Q Search	+ ~
S Ports	H NAME	TYPE	VALUE	ACTIONS
Security Zones	1 LocalIdentitySource	LOCAL		
Application Filters	2 LAB-AD	AD	win2016.example.com	

4. Klicken Sie auf die Schaltfläche Jetzt bereitstellen.

Pe	ending Changes	0 ×	<
0	Last Deployment Completed Successfully 01 May 2020 12:54 PM. See Deployment History		
	Deployed Version (01 May 2020 12:54 PM)	Pending Version       LEGEND Removed Added Edit	ted
0	Active Directory Realm Added: LAB-AD		^
	- - - - - - -	<pre>dirPassword.masked: false dirPassword.encryptedString: *** directoryConfigurations[0].port: 389 directoryConfigurations[0].hostname: win2016.example.com directoryConfigurations[0].encryptionProtocol: NONE adPrimaryDomain: example.com dirUsername: ftd.admin@example.com baseDN: DC=example,DC=com enabled: true realmId: 9 name: LAB-AD</pre>	~
м	ORE ACTIONS Y	CANCEL DEPLOY NOW	]

#### Konfigurieren von AnyConnect für die AD-Authentifizierung

Um die konfigurierte AD-Identitätsquelle zu verwenden, muss sie auf die AnyConnect-Konfiguration angewendet werden.

1. Navigieren Sie zu **Device > Remote Access VPN** wie im Bild gezeigt.

CISCO. Firepower Device Manager	Monitoring Policies Objects	Device: FTD-3	admin
	[000] [		
Interfaces Connected Enabled 3 of 4 View All Interfaces	Routing 2 routes View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server DNS Server
Smart License Registered View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Hostname NTP Cloud Services Reboot/Shutdown Traffic Settings URL Filtering Preferences
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Configured 1 connection   2 Group Policies View Configuration	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	Device Administration Audit Events, Deployment History, Download Configuration View Configuration

2. Klicken Sie auf das + Symbol oder die Schaltfläche Verbindungsprofil erstellen, wie im Bild gezeigt.



3. Wählen Sie im Abschnitt "Connection and Client Configuration" (Verbindung und Client-Konfiguration) die zuvor erstellte AD-Identitätsquelle aus. Richten Sie die entsprechenden Werte für die anderen Abschnitte ein, einschließlich Verbindungsprofilname und Client-Adresspoolzuweisung. Klicken Sie abschließend auf **Abfrage senden**.

## Connection and Client Configuration

specify now to authenticate remote users a	nd the AnyConnect clients they can use to connect to the nside network.
Connection Profile Name This name is configured as a connection alias, it ca	n be used to connect to the VPN gateway
General	
Group Alias	Group URL
General	
Add Group Alias	Add Group URL
Primary Identity Source	
Authentication Type	
AAA Only Client Certificate Only	AAA and Client Certificate
Primary Identity Source for User Authenticat	ion Fallback Local Identity Source 🔥
Filter	✓ Please Select Local Identity Source ✓
1 LocalidentitySource	^
<u></u> LAB-AD	0
1 Special-Identities-Realm	$\sim$
Create new M	

#### Client Address Pool Assignment

IPv4 Address Pool Endpoints are provided an address from this pool	IPv6 Address Pool Endpoints are provided an address from this pool
C AnyConnect-Pool	
+	
CANCEL	SUBMIT QUERY

4. Wählen Sie im Abschnitt Remote User Experience (Remote-Benutzererfahrung) die entsprechende Gruppenrichtlinie aus. Standardmäßig wird **DfltGrpPolicy** verwendet. Es kann jedoch ein anderer erstellt werden.

```
View Group Policy
```

DfltGrpPolicy

Policy Group Brief Details

DNS + BANNER	Edi
DNS Server	None
Banner Text for Authenticated Clients	None
SESSION SETTINGS	
Maximum Connection Time / Alert Interval	Unlimited / 1 Minutes
Idle Time / Alert Interval	30 / 1 Minutes
Simultaneous Login per User	3
SPLIT TUNNELING	
IPv4 Split Tunneling	Allow all traffic over tunnel
IPv6 Split Tunneling	Allow all traffic over tunnel
ANYCONNECT CLIENT	
AnyConnect Client Profiles	None

5. Geben Sie im Abschnitt Global Settings (Globale Einstellungen) mindestens das SSL-Zertifikat, die externe Schnittstelle und die AnyConnect-Pakete an. Wenn zuvor kein Zertifikat erstellt wurde, kann ein selbstsigniertes Standardzertifikat (DefaultInternalCertificate) ausgewählt werden, jedoch wird eine nicht vertrauenswürdige Serverzertifikatmeldung angezeigt. Zugriffskontrollrichtlinien für entschlüsselten Datenverkehr umgehen (sysopt permit-vpn) sollte deaktiviert werden, damit die Benutzeridentitätszugriffsrichtlinien zu einem späteren Zeitpunkt wirksam werden. NAT-Freistellung kann auch hier konfiguriert werden. In dieser Konfiguration ist der gesamte IPv4-Datenverkehr von der internen Schnittstelle, der zu den AnyConnect-Client-IP-Adressen führt, außer von NAT. Für komplexere Konfigurationen, wie z. B. externe Hairpinning, müssen im Rahmen der NAT-Richtlinie zusätzliche NAT-Regeln erstellt werden. AnyConnect-Pakete finden Sie auf der Cisco Support-Website unter <u>https://software.cisco.com/download/home</u>. Zum Herunterladen des AnyConnect-Pakets ist eine gültige Plus- oder Apex-Lizenz erforderlich.

## **Global Settings**

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity	Outside Interface
FTD-3-Manual	outside (GigabitEthernet0/0)
Fully-qualified Domain Name for the Outside Interf	face
ftd3.example.com	
e.g. ravpn.example.com	
Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy policy for decrypted traffic option bypasses the access con and the authorization ACL downloaded from the AAA server Bypass Access Control policy for decrypted to	/ inspection by default. Enabling the Bypass Access Control ntrol policy, but for remote access VPN, the VPN Filter ACL er are still applied to VPN traffic raffic (sysopt permit-vpn)
NAT Exempt	
Inside Interfaces The interfaces through which remote access VPN users can connect to the internal networks +	Inside Networks The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.
inside (GigabitEthernet0/1)	+
	اتے any-ipv4
AnyConnect Package	
If a user does not already have the right AnyConnect packa installer when the client authenticates for the first time. The	ge installed, the system will launch the AnyConnect user can then install the package from the system.
You can download AnyConnect packages from software.cls You must have the necessary AnyConnect software license	ico.com.
Packages	



6. Überprüfen Sie im Abschnitt Zusammenfassung, ob AnyConnect korrekt eingerichtet ist, und klicken Sie dann auf Abfrage senden.

#### Summary

Review the summary of the Remote Access VPN configuration.

General		
STEP 1: CONNECTION AND CLIENT CONFIGURATIO	ON	
Primary Identity Source	—	
Authentication Type	AAA Only	
Primary Identity Source	赴 LAB-AD	
Fallback Local Identity Source	-	
Strip Identity Source server from username	No	
Strip Group from Username	No	
Secondary Identity Source		
Secondary Identity Source for User Authentication	n –	
Fallback Local Identity Source	-	
Advanced		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		

7. Klicken Sie oben rechts auf die Schaltfläche Ausstehende Änderungen, wie im Bild gezeigt.

cisco. Firepower Dev	ce Manager 颐 资 宗王 Monitoring Policies Objects	Device: FTD-3	∑ 😥 @ ? ÷ admin Administrator ˘			
RA VPN ←	Device Summary Remote Access VPN Connection Profiles					
Connection Profiles	1 object	Q. %	earch 🕂			
	a NAME	***	GROUP POLICY ACTIONS			
	1 General	Authentication: AAA Only Authentization: None Accounting: None	DftGrpPolicy			

8. Klicken Sie auf Jetzt bereitstellen.



#### Identitätsrichtlinie aktivieren und Sicherheitsrichtlinien für Benutzeridentität konfigurieren

An diesem Punkt sollten AnyConnect-Benutzer erfolgreich eine Verbindung herstellen können, aber möglicherweise nicht auf bestimmte Ressourcen zugreifen können. In diesem Schritt wird die Benutzeridentität aktiviert, sodass nur Benutzer innerhalb von AnyConnect Admins mit RDP eine Verbindung zu internen Ressourcen herstellen können und nur Benutzer innerhalb der Gruppe AnyConnect-Benutzer mit HTTP eine Verbindung zu internen Ressourcen herstellen können.

1. Navigieren Sie zu Richtlinien > Identität, und klicken Sie auf Identitätsrichtlinie aktivieren.



Für diese Konfiguration ist keine weitere Konfiguration erforderlich, und die Standardaktion ist ausreichend.

cisco. Firepo	wer Device Manage	r Mo	nitoring Policies	部王 Objects	Device: FTD-3		o 🔒 🛛	? :	admin Administrator	×
🛷 Security P	olicies									
□ → ○ s	SL Decryption $\rightarrow$	Identity $\Rightarrow$	O Security Intellige	ence -> 📀 M	NAT $ ightarrow$ 📀 Acc	ess Control 🚽 🐐	Intrusion			
Identity Policy	D					Q Search			¢ <u>s</u>	+
			SOURCE			DESTINATION				
H NAME	AUTHENTICATION	AUTH, TYPE	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	ACTION	8
				There are no	Identity rules yet.					
				Start by creating	the first identity rule					
CREATE IDENTITY RULE										
Default Action	Passive Auth Any	Identity Source	~ <b>0</b>							

2. Navigieren Sie zu **Richtlinien > NAT**, und stellen Sie sicher, dass NAT korrekt konfiguriert ist. Wenn die in den AnyConnect-Einstellungen konfigurierte NAT-Ausnahme ausreicht, ist hier keine zusätzliche Konfiguration erforderlich.

cisco. Firepow	er Device M	Manager	Monitori	ng Policies	i≣≣ Objects	Device: FTD-3		۵ 🔮	۲	admin Admini	strator
🛷 Security Po	licies										
□ → ○ SSI	Decryption	-> 📀 Id	entity $\rightarrow$ (	Security Intelligen	ce $ ightarrow$ NM	T $ ightarrow$ 🕗 Acce	ess Control $\Rightarrow$	S Intrusion			
1 rule								Q Search			+
			OFFICINAL PACKET				TRANSLATED PACK	ŧT			
a NAME	TYPE	INTERFACES	SOURCE AD	DESTINATIO	SOUNCE PORT	DESTINATIO	SOUNCE AD	DESTINATIO	SOURCE PORT	DESTINATIO	ACTIONS
Auto NAT Rules											
> # Internet_PAT	DYNAMIC	J ANY outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

3. Navigieren Sie zu **Richtlinien > Zugriffskontrolle**. In diesem Abschnitt ist die Standardaktion auf "Blockieren" gesetzt. Es wurden keine Zugriffsregeln erstellt, sodass ein AnyConnect-Benutzer nach der Verbindung auf nichts zugreifen kann. Klicken Sie auf das + Symbol oder auf Zugriffsregel erstellen, um eine neue Regel hinzuzufügen.

cisco. Firepo	ower Device Manager	题 Monitoring	Ø Policies	前面 Objects	Device: FTD-3		۵ 🗳	:	* ad * Ad	imin Iministrator		
🕫 Security i	Policies											
$\square \rightarrow \bigcirc$	$\square \rightarrow \bigcirc$ SSL Decryption $\rightarrow \oslash$ identity $\rightarrow \bigcirc$ Security Intelligence $\rightarrow \oslash$ NAT $\rightarrow \oslash$ Access Control $\rightarrow \circledast$ Intrusion											
						Q Search				®. +		
	sounce			DESTINATION								
N NAME	ACTION ZONES	METWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS		
				There are no a	ocess rules yet.							
				Start by creating t	the first access rule.							
				CREATE A	CCESS RULE							
Default Action	Access Control 🤤 Block	9, E. 🗸										

4. Füllen Sie die Felder mit den entsprechenden Werten aus. Bei dieser Konfiguration sollten Benutzer innerhalb der AnyConnect-Administratorgruppe über RDP-Zugriff auf den Windows-Server im internen Netzwerk verfügen. Für die Quelle wird die Zone als outside\_zone konfiguriert. Dies ist die externe Schnittstelle, mit der die AnyConnect-Benutzer eine Verbindung herstellen, und das Netzwerk wird als AnyConnect-Pool-Objekt konfiguriert, das zuvor konfiguriert wurde, um AnyConnect-Clients IP-Adressen zuzuweisen. Für die Benutzeridentität im FDM muss die Quelle die Zone sein, von der der Benutzer die Verbindung initiiert. Für das Ziel wird die Zone als inside\_zone konfiguriert, d. h. als interne Schnittstelle, die sich der Windows Server befindet, das Netzwerk wird als Inside\_Net-Objekt konfiguriert. Dies ist ein Objekt, das das Subnetz definiert, in dem sich der Windows Server befindet, und Ports/Protokolle werden auf zwei benutzerdefinierte Port-Objekte festgelegt, um den RDP-Zugriff über TCP 3389 und UDP 3389 zu ermöglichen.

Edit Access	Rul	e										×
Order Title 1  AC R Source/Destination	DP Ac	plications URLs	Use	rs Intru	Action Allow sion Policy	File policy <sup>9</sup> Log	ging					
SOURCE						DESTINATION						
Zones	+	Networks	+	Ports	+	Zones	+	Networks	+	Ports/Protocols		+
outside_zone		C AnyConnect-Pool		ANY		inside_zone		Dinside_Net		$rac{l}{l}$ RDP-TCP		
Show Diagram	$\supset$	Not hit yet							CA	INCEL	ок	

Im Abschnitt "Benutzer" wird die Gruppe "AnyConnect-Administratoren" hinzugefügt, sodass Benutzer außerhalb dieser Gruppe RDP-Zugriff auf den Windows-Server erhalten. Klicken Sie auf das + Symbol, klicken Sie auf die Registerkarte Gruppen, klicken Sie auf die entsprechende Gruppe und dann auf **OK**. Beachten Sie, dass auch einzelne Benutzer und die Identitätsquelle ausgewählt werden können.

Add Access Rule	@ ×	
Order Title 1  AC RDP Access Source/Destination Applications URLs Users	Action       Allow           Intrusion Policy        File policy	
AVAILABLE USERS         Y Filter         Identity Sources         It         LAB-AD \ Account Operators         It         LAB-AD \ Administrators         It         LAB-AD \ Allowed RODC Password Replication Group         It         It         LAB-AD \ Allowed RODC Password Replication Group         It         LAB-AD \ AnyConnect Users         It         LAB-AD \ AnyConnect Users         Create new Identity Realm	CONTROLLING ACCESS FOR USERS AND USER GROUPS  If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.	
Show Diagram	CANCEL OK	

## Klicken Sie nach Auswahl der entsprechenden Optionen auf OK.

Add Access Rule	0 ×
Order Title Action	
1 V AC RDP Access	llow V
Source/Destination Applications URLs Users Intrusion Pol	icy <sup>0</sup> File policy <sup>0</sup> Logging
AVAILABLE USERS	+ Lt CONTROLLING ACCESS FOR USERS AND USER GROUPS
148-AD \ AnyConnect Admins	If you configure identity policies to establish user identity based on source IP address, you can control access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.
Show Diagram	CANCEL

5. Erstellen Sie bei Bedarf weitere Zugriffsregeln. In dieser Konfiguration wird eine weitere

Zugriffsregel erstellt, um Benutzern innerhalb der AnyConnect-Benutzergruppe HTTP-Zugriff auf den Windows-Server zu ermöglichen.

Edit Access Rule	0 ×
Order Title	Action
2 Y AC HTTP Access	🔁 Allow 👻
Source/Destination Applications URLs Users Intru	trusion Policy <sup>9</sup> File policy <sup>9</sup> Logging
SOURCE	DESTINATION
Zones + Networks + Ports	+ Zones + Networks + Ports/Protocols +
avy outside_zone C AnyConnect-Pool ANY	G inside_zone ☐ Inside_Net ⊆ HTTP
Show Diagram	CANCEL
Edit Access Rule	0 ×
Order Title	Action
2 V AC HTTP Access	Allow 👻
Source/Destination Applications URLs Users Intru	trusion Policy <sup>0</sup> File policy <sup>0</sup> Logging
AVAILABLE USERS	+ 12 CONTROLLING ACCESS FOR USERS AND USER GROUPS
武 LAB-AD \ AnyConnect Users	If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.
Show Diagram	CANCEL OK

6. Überprüfen Sie die Konfiguration der Zugriffsregel, und klicken Sie dann oben rechts auf die

Schaltfläche Ausstehende Änderungen, wie im Bild gezeigt.

	list	Firepowe	er Devic	e Manager	Monitoring	Policies	Ubjects D	Device: FTD-3		0	0?	): [;	idmin Idministra	tor
đ	🕫 Security Policies													
	9	$\rightarrow$ () SSL	Decryptio	o 🔶 🥑 Iden	tity → 🔘 Se	curity Intelligence	ightarrow 📀 NAT	→ <table-cell> Access</table-cell>	Control 🔿 🍕	Intrusion				
2	ules								Q Search				0	+
				SOURCE			DESTINATION							
	•	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO_	APPLICATIONS	UNLS	USERS		ACTIONS
;	• 1	AC RDP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP	ANY	ANY	AnyConne	Ф.С.	
;	2	AC HTTP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne	Ф.С.	
	Pefaul	It Action Acc	ess Control	😑 Block 🛛 🖏	E. V									

7. Überprüfen Sie die Änderungen, und klicken Sie dann auf Jetzt bereitstellen.

Pe	nding Changes			0	×
<ul> <li>■</li> <li>2</li> </ul>	Last Deployment Completed Successfully 8 Apr 2020 01:35 PM. See Deployment History				
	Deployed Version (28 Apr 2020 01:35 PM)	Pending Version	LEGEND Removed	Added	Edited
0	Access Rule Added: AC HTTP Access				~
		users[0].name: AnyConnect Use logFiles: false eventLogAction: LOG_NONE ruleId: 268435467 name: AC HTTP Access	irs		
	sourceZones:				
	- destinationZones:	outside_zone			
	-	inside_zone			
	sourceNetworks:				
	-	AnyConnect-Pool			
	destinationNetworks:				
	-	Inside_Net			
	destinationPorts:	UTTD			
	users[0].identitySource:	niir			
	-	LAB-AD			
0	Access Pula Added: AC PDP Access				~
0	ALLESS NUE AUGEL AU RUF ALLESS				
м	DRE ACTIONS Y	CANCEL	DEPLOY NO	ow	~

# Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Endgültige Konfiguration

#### AAA-Konfiguration

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

#### Konfigurieren von AnyConnect

```
> show running-config webvpn
webvpn
enable outside
http-headers
 hsts-server
  enable
  max-age 31536000
  include-sub-domains
  no preload
 hsts-client
  enable
 x-content-type-options
 x-xss-protection
 content-security-policy
anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
 cache
 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-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
 anyconnect ssl dtls none
> show running-config ssl
```

ssl trust-point FTD-3-Manual outside

Herstellen einer Verbindung mit AnyConnect und Überprüfen der Zugriffskontrollrichtlinien

Cisco AnyConnect Se	g ftd3.example.com.
	Cisco AnyConnect   ftd3.example.com     Group:   General   Username:   it.admin   Password:     ********
	OK Cancel
🚳 Cisco AnyConnect Se	cure Mobility Client — 🗆 🗙
Connecte ftd3.exa	d to ftd3.example.com. ample.com v Disconnect
00:00:14	IPv4
<b>Q</b> (i)	

Benutzer-IT-Admin ist in der Gruppe AnyConnect-Administratoren, die über RDP-Zugriff auf den Windows-Server verfügt, jedoch keinen Zugriff auf HTTP hat. Durch das Öffnen einer RDP- und Firefox-Sitzung mit diesem Server wird überprüft, ob dieser Benutzer nur über RDP auf den Server zugreifen kann.



Wenn Sie bei einem Testbenutzer angemeldet sind, der zur Gruppe AnyConnect-Benutzer gehört, die über HTTP-Zugriff, aber keinen RDP-Zugriff verfügen, können Sie überprüfen, ob die Zugriffskontrollrichtlinien wirksam werden.



## Fehlerbehebung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

## Debugger

Dieser Debugger kann in der CLI der Diagnose ausgeführt werden, um Probleme mit der LDAP-Authentifizierung zu beheben: **debug Idap 255**.

Um Probleme mit der Zugriffskontrollrichtlinie für die Benutzeridentität zu beheben, kann die **Firewall-Engine-Debugging-**Funktion **des Systems** in clish ausgeführt werden, um zu ermitteln, warum Datenverkehr unerwartet zugelassen oder blockiert wird.

#### Arbeiten mit LDAP-Debuggern

```
[53] Session Start
[53] New request Session, context 0x00002bldl3f4bbf0, 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]
[53]
      sn: value = Admin
[53]
      givenName: value = IT
[53]
      distinguishedName: value = CN=IT Admin, CN=Users, DC=example, DC=com
      instanceType: value = 4
[53]
       whenCreated: value = 20200421025811.0Z
[53]
       whenChanged: value = 20200421204622.0Z
[53]
       displayName: value = IT Admin
[53]
      uSNCreated: value = 25896
[53]
[53]
      memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
      uSNChanged: value = 26119
[53]
      name: value = IT Admin
[53]
       objectGUID: value = &...J..O...2w...c
[53]
[53]
       userAccountControl: value = 512
[53]
      badPwdCount: value = 6
      codePage: value = 0
[53]
[53]
      countryCode: value = 0
      badPasswordTime: value = 132320354378176394
[53]
[53]
      lastLogoff: value = 0
[53]
      lastLogon: value = 0
[53]
       pwdLastSet: value = 132319114917186142
      primaryGroupID: value = 513
[53]
      objectSid: value = .....{I...;....j...
[53]
[53]
      accountExpires: value = 9223372036854775807
[53]
      logonCount: value = 0
[53]
      sAMAccountName: value = it.admin
      sAMAccountType: value = 805306368
[53]
[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
```

#### Verbindung mit LDAP-Server kann nicht hergestellt werden

```
[-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
```

Potenzielle Lösungen:

- Überprüfen Sie das Routing, und stellen Sie sicher, dass die FTD eine Antwort vom LDAP-Server erhält.
- Wenn LDAPS oder STARTTLS verwendet wird, stellen Sie sicher, dass das richtige Root-Zertifizierungsstellenzertifikat vertrauenswürdig ist, damit der SSL-Handshake erfolgreich abgeschlossen werden kann.
- Überprüfen Sie, ob die richtige IP-Adresse und der richtige Port verwendet werden. Wenn ein Hostname verwendet wird, überprüfen Sie, ob der DNS in der Lage ist, diesen auf die richtige IP-Adresse aufzulösen.

#### Binden der Anmelde-DN und/oder des Kennworts falsch

```
[-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
```

Mögliche Lösung: Überprüfen Sie, ob die Anmelde-DN und das Anmeldekennwort entsprechend konfiguriert sind. Dies kann auf dem AD-Server mit **Idp.exe** überprüft werden. Um zu überprüfen, ob ein Konto erfolgreich mit der Verwendung von Idp verknüpft werden kann, gehen Sie durch die folgenden Schritte:

1. Drücken Sie auf dem AD-Server Win+R und suchen Sie nach Idp.exe.

🗐 Run	×
Ø	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. Klicken Sie auf Verbindung > Verbindung herstellen... wie im Bild gezeigt.



3. Geben Sie localhost für den Server und den entsprechenden Port an, und klicken Sie dann auf OK.

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

4. Die rechte Spalte zeigt den Text an, der auf eine erfolgreiche Verbindung hinweist. Klicken Sie auf **Verbindung > Bind..** wie im Bild gezeigt.

🟠 Idap://wi	in2016.exa	mple.co	om/DC:	= example, DC	=com		—		$\times$
Connection	Browse	View	Optio	ns Utilities	Help				
Connection Connection Bind Disconn New Save Save Save As Exit	Browse t	View Ctrl+B Ctrl+N	Optio	ns Utilities Id = Idap_op Established Retrieving b Getting 1 en Dn: (RootD) configur CN= current Time defaultM dnsHos domain domain dsServi	Help en("localhos connection ase DSA inf ase DSA inf tries: <b>SE)</b> rationNaming Configuration Time: 5/1/20 e; NamingConte tName: win2 ControllerFun Functionality iceName: CN-Withow CN-Withow CN-Withow tingen CN-Withow	st", 389); to localhost. formation gContext: on,DC=examp 20 4:16:55 PM ext: DC=examp 2016.example nctionality: 7 = : 7 = ( WIN201 I=NTDS	le,DC=c 1 Eastern ple,DC=c .com; = ( WIN2 16 );	om; n Daylight com; 016 ); N=Default	-
				Firs Nan com forestFu highest( isGlobal isSynch IdanSer	it-Site- ne,CN=Sites n; unctionality: CommittedUS ICatalogRea Ironized: TR viceName: e	,CN=Configur 7 = ( WIN2010 SN: 13410; dy: TRUE; UE; example.com;	ation,DC 6 ); win2016	=example,I	DC=

5. Wählen Sie **Einfache Bindung**, und geben Sie dann Benutzername und Kennwort des Verzeichniskontos an. Klicken Sie auf **OK**.

Bind	×						
<u>U</u> ser: Password:	User: ftd.admin@example.com Password:						
<u>D</u> omain:	Domain:						
User:       ftd.admin@example.com         Password:       ••••••         Domain:       ••••••         Bind type       Bind as currently logged on user         Bind with credentials       Bind with credentials         Simple bind       Advanced (DIGEST)         Encrypt traffic after bind       OK							
User:       ftd.admin@example.com         Password:       ••••••         Domain:       ••••••         Bind type       •         Bind type       •         Bind as currently logged on user       •         Bind with credentials       •         Simple bind       •         Advanced (DIGEST)       •         Advanced       Cancel       OK							

Bei erfolgreicher Bindung wird ldp als DOMÄNE\Benutzername authentifiziert angezeigt.

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		_		×	<
Connection	Browse	View	Options	Utilities	Help					
				1.2. 1.2. 1.2. supporti Max Max Max Max Max Max Max Max	840.113556 840.113556 840.113556 edLDAPPoli (PercentDirs (ReceiveBu (Connection (BatchRetur (DirSyncDur (ResultSets (ResultSets (ValRange; eadMemory edLDAPVer edSASLMer IEGO; EXTE	5.1.4.2255; 5.1.4.2256; 5.1.4.2309; cies (20): M SyncReques ffer; InitRec is; MaxConn mMessages ration; MaxT ize; MinRes PerConn; MaxT ize; MinRes PerConn; MaxT ize; MinRes PerConn; MaxT ize; MinRes PerConn; MaxT ize; MinRes PerConn; MaxT chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad	axPooIThr sts; MaxDa vTimeout; IdleTime; I ; MaxQue empTable ultSets; axNotifical geTransiti mMemoryL 2; ): GSSAP :ST-MD5; Imin@exa	reads; atagramR MaxPage! ryDuratio Size; tionPerCo ve; LimitPerce I; GSS-	ecv; Size; n; mn; mt;	^
			-							¥
Ready										

Wenn Sie versuchen, eine Bindung mit einem ungültigen Benutzernamen oder Kennwort zu erstellen, führt dies zu einem solchen Fehler.

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC:	=com		_		×
Connection	Browse	View	Options	Utilities	Help				
			r A E S C E ir	Max Max Max Three supporte supporte SPN es = Idap_s unavailable cuthenticate es = Idap_s unavailable rror <49>: I server error comment: Ac rror 0x8009 ivalid	ResultSets ResultSets ValRange; adMemoryl edLDAPVer edSASLMed EGO; EXTE imple_bind_ >); // v.3 ed as: 'EXAI imple_bind_ >); // v.3 dap_simple : 80090308 cceptSecur 90308 The t	ize; MinResi PerConn; Ma MaxValRang Limit; Syster sion (2): 3; 2 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; ): GSSAPI ST-MD5; min@exar min@exar min". g@examp ailed: Invali SID-0C09 rror, data ed to the f	ionPerConn ve; imitPercent ; GSS- mple.com', le.com', id Credentia 042A, 52e, v3839 unction is	ls
Ready			ļ						¥

#### LDAP-Server kann Benutzernamen nicht finden

```
[-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
```

Mögliche Lösung: Vergewissern Sie sich, dass AD den Benutzer mit der Suche durch die FTD finden kann. Dies kann auch mit Idp.exe durchgeführt werden.

1. Navigieren Sie nach der erfolgreichen Bindung zu Ansicht > Struktur wie im Bild gezeigt.

🔝 Idap://w	Idap://win2016.example.com/DC=example,DC=com							_		$\times$		
Connection	Browse	View	/ Option	s Utilities	Help							
			Tree			Ctrl+T				^		
			Enterprise	e Configurat	ion		/axP	PoolThr	eads;			
		$\checkmark$	Status Ba	n/DC= example,DC= com Options Utilities Help ee Ctrl+T terprise Configuration atus Bar t Font MaxDirSyncDuration; Ma MaxResultSetSize; MinR MaxResultSetSize; MinR MaxResultSetSize; MinR MaxResultSetSPerConn; MaxValRange; MaxValR ThreadMemoryLimit; Sys supportedLDAPVersion (2): supportedSASLMechanisms SPNEGO; EXTERNAL; D 			sts; vTin	maxDa neout;	itagramR	ecv;		
			Set Font	t Font MaxDirSvncDuration: Max				nldleTime; MaxPageSize s: MaxQueryDuration;				
				Max Max Max Thre support support SPN	DirSync ResultS ResultS ValRang adMem edLDAP edSASL EGO; E)	Duration; Ma etSize; MinF etsPerConn ge; MaxVaF oryLimit; Sy Version (2): Mechanisms (TERNAL; D	axTem ResultS ; MaxN RangeT stemMe : 3; 2; s (4): G NGEST-	pTable ets; iotificat ransitiv emoryL SSSAPI -MD5;	Size; ionPerCo /e; imitPerce ; GSS-	nn; :nt;		
				res = ldap_s <unavailable Authenticate</unavailable 	imple_bi ≫); // v.3 ed as: 'E)	ind_s(ld, 'ftd } XAMPLE\ftd	1.admin I.admin'	@exar	nple.com	,		
				I						~		

2. Geben Sie die für FTD konfigurierte Basis-DN an, und klicken Sie dann auf OK.

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

3. Klicken Sie mit der rechten Maustaste auf die Basis-DN, und klicken Sie dann auf Suchen, wie im Bild gezeigt.

Idap://win2016.exampl Connection Browse Vie		mple.co	om/DC=ex		_		×				
Connection	Browse	View	Options	Utilities	Help						
<b>€</b> DC=exam	iple,DC=c	om	Search Virtual L Delete Modify Modify Add chil Compar Advance Copy DN Copy Select al Clear ou	ist View DN Id e ed N	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A Ctrl+A Ctrl+C	>	cipals,DC 11D2B9A =example E11D297( example, 11D1ADE eexample 11D1ADE ole,DC=co 11D1AA s,DC=exa 11D1ADE ample,DC 311D1ADE e,DC=cor 0 3:43:59 2:41:57 I	=examp A00C0 ,DC=co C400C0 ,DC=cor ED00C0 e,DC=cc ED00C0 om; 4B00C0 mple,D0 ED00C0 =com; ED00C0 =com; ED00C0 m; PM East	ole,DC=co 4F79F805 m; 4FD8D5C n; 4FD8D5C om; 4FD8D5C 4FD7D83 C=com; 4FD8D5C 4FD8D5C 04FD8D5C 04FD8D5C	om; 5:CN D:C D:C D:C A:O D:C D:C D:C ight ght	~
Create a new o	locument										-

4. Geben Sie die Werte für Basisdatenbank, Filter und Bereich an, die im Debuggen angezeigt werden. In diesem Beispiel sind folgende Beispiele:

- Basis-DN: dc=beispiel,dc=com
- Filtern: samaccountName=it.admi
- Geltungsbereich:SUBTREE

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 ×	
Connection	Browse View Options Utilities Help		
Search	×	C=example,DC=com; 68811D1ADED00C04FD8D5CD:C	^
Base DN:	DC=example,DC=com ~	58811D1ADED00C04FD8D5CD:C	
Filter:	sAMAccountName=it.admi ~	ample,DC=com; D211D1AA4B00C04FD7D83A:O	
Scope O Base	One Level Subtree	lers,DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C example,DC=com;	
Attributes:	objectClass;name;description;canonicalName ~	68811D1ADED00C04FD8D5CD:C nple,DC=com; 1020 3:43:59 PM Eastern Daylight	
Options	Run Close	)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			

ldp findet 0 Einträge, da kein Benutzerkonto mit dem **gleichenAccountName=it.admi** unter Basis-DN dc=beispiel,dc=com vorhanden ist.

Bei einem erneuten Versuch mit dem richtigen **samaccountName=it.admin** wird ein anderes Ergebnis angezeigt. Idp sucht 1 Eintrag unter der Basis-DN dc=beispiel,dc=com und gibt die DN des Benutzers aus.

🔐 Idap://w	in2016.example.	com/DC=ex	ample,DC:	=com		- □ >	<
Connection	Browse View	Options	Utilities	Help			
Search					$\times$	58811D1ADED00C04FD8D5CD:C DC=example,DC=com;	^
Base <u>D</u> N: Filter:	DC=example,DC	C=com ne=it.admin			~	58811D1ADED00C04FD8D5CD:C ample,DC=com; D211D1AA4B00C04FD7D83A:C lers DC=example DC=com;	) )
Scope	O <u>O</u> ne Level	● <u>S</u> ubtree	e			58811D1ADED00C04FD8D5CD:C example,DC=com; 68811D1ADED00C04FD8D5CD:C mple DC=com;	2
<u>A</u> ttributes:	objectClass;nam	e;descriptior	n;canonicalN	lame	$\sim$	020 3:43:59 PM Eastern Dayligh	t
Options		<u>R</u> un		<u>C</u> lose		)20 2:41:57 PM Eastern Daylight	
		k G D	**Searching dap_search sAMAccour Setting 1 ent On: CN=IT A canonica name: IT objectCla user	I _s(Id, "I ntName= tries: Admin,( alName: Admin; ass (4): r;	DC=e =it.ad C <b>N=U</b> exar top;	min", attrList, 0, &msg) <b>Isers,DC=example,DC=com</b> mple.com/Users/IT Admin; person; organizationalPerson;	
Ready							

#### Falsches Kennwort für Benutzername

```
[-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
```

Mögliche Lösung: Überprüfen Sie, ob das Kennwort des Benutzers korrekt konfiguriert wurde und nicht abgelaufen ist. Ähnlich wie bei der Anmelde-DN ist auch die FTD an AD mit den Anmeldeinformationen des Benutzers gebunden. Diese Bindung kann auch in Idp erfolgen, um zu überprüfen, ob das AD denselben Benutzernamen und dieselben Anmeldeinformationen für das Kennwort erkennen kann. Die Schritte in Idp sind im Abschnitt **Anmelde-DN und/oder Kennwort falsch** anzeigen. Darüber hinaus können die Microsoft Server Event Viewer-Protokolle aus einem potenziellen Grund überprüft werden.

#### AAA testen

Der Befehl test aaa-server kann verwendet werden, um einen Authentifizierungsversuch der FTD mit einem bestimmten Benutzernamen und Kennwort zu simulieren. Dies kann zum Testen auf Verbindungs- oder Authentifizierungsfehler verwendet werden. Der Befehl lautet **test aaa-server authentication [AAA-server] host [AD IP/hostname]**.

```
> 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
```

#### Paketerfassung

Paketerfassungen können verwendet werden, um die Erreichbarkeit zum AD-Server zu überprüfen. Wenn LDAP-Pakete die FTD verlassen, aber keine Antwort gibt, könnte dies auf ein Routing-Problem hinweisen.

Im Folgenden wird ein bidirektionaler LDAP-Datenverkehr aufgezeichnet:

```
> 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
                           192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
   1: 23:02:16.770712
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>
   5: 23:02:16.772924
                          192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
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>
                          192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
   7: 23:02:16.773428
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
  8: 23:02:16.775030
                          192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
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 Event Viewer-Protokolle

Die Ereignisanzeige meldet sich im AD-Servervan an und liefert detailliertere Informationen, warum ein Fehler aufgetreten ist.

1. Ereignisanzeige suchen und öffnen.

=	Best match	
ഹ	Event Viewer Desktop app	
	Settings >	
	Wiew event logs	
۲		
	event	
-	ዶ 🗆 🧀 🔚 💈	

2. Erweitern Sie **Windows-Protokolle**, und klicken Sie auf **Sicherheit**. Suchen Sie mit dem Kontonamen des Benutzers nach **Audit Failure (Audit-Fehler)**, und überprüfen Sie die Fehlerinformationen, wie im Bild gezeigt.



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