# AAD-verificatie (LDAP) en gebruikersidentiteit instellen op FTD beheerde door FDM voor AnyConnect-clients

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram en -scenario **AD-configuraties** LBP-basis DN bepalen Een FTD-account maken AD-groepen maken en gebruikers aan AD-groepen toevoegen (optioneel) Kopieer de LDAPS SSL-certificatieroot (alleen vereist voor LDAPS of STARTTLS) **FDM-configuraties** Controleer de licenties AD-identiteitsbron instellen AnyConnect voor AD-verificatie configureren identiteitsbeleid inschakelen en beveiligingsbeleid voor gebruikers-identiteit instellen Verifiëren Eindconfiguratie Connect met AnyConnect en controleer beleidsregels voor toegangscontrole Problemen oplossen **Debugs** Werkopbalkkaarten Kan geen verbinding met LDAP-server opzetten Vastlegging ISDN en/of wachtwoord niet correct LDAP Server kan geen gebruikersnaam vinden Onjuist wachtwoord voor gebruikersnaam **Test AAA** Packet Capture Vastlegging Windows Server Event Viewer

## Inleiding

Het doel van dit document is in detail te treden hoe u actieve directory (AD)-verificatie kunt configureren voor AnyConnect-clients die verbinding maken met een Cisco Firepower Threat Defense (FTD) dat wordt beheerd door Firepower Devices Management (FDM). De identiteit van de gebruiker wordt in het toegangsbeleid gebruikt om AnyConnect-gebruikers te beperken tot specifieke IP-adressen en -poorten.

## Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van RA VPN-configuratie op FDM
- Basiskennis van de LAN-serverconfiguratie op FDM
- Basiskennis van de AD

### Gebruikte componenten

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

- Microsoft 2016-server
- FTDv met 6,5,0

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Configureren

## Netwerkdiagram en -scenario



Windows server is vooraf ingesteld met Internet Information Services (IS) en Remote Desktop Protocol (RDP) om de gebruikersidentiteit te testen. In deze configuratiehandleiding worden drie gebruikersaccounts en twee groepen gemaakt.

Gebruikersrekeningen:

- FTD Admin: Dit wordt gebruikt als directory account om de FTD te kunnen binden aan de AD server.
- IT-beheerder: Een testbeheeraccount die wordt gebruikt om de identiteit van de gebruiker aan te tonen.
- Test gebruiker: Een testgebruikersaccount die wordt gebruikt om de identiteit van de gebruiker aan te tonen.

Groepen:

• AnyConnect wordt beheerd: Aan een testgroep die IT Admin wordt toegevoegd om de identiteit van de gebruiker aan te tonen. Deze groep heeft alleen RDP-toegang tot de

Windows-server

• AnyConnect-gebruikers: Een testgroep waaraan de testgebruiker wordt toegevoegd om de identiteit van de gebruiker aan te tonen. Deze groep heeft alleen HTTP-toegang tot de Windows-server

## **AD-configuraties**

Om de AD-verificatie en de gebruikersidentiteit op de juiste wijze te kunnen configureren, zijn een aantal waarden vereist. Al deze gegevens moeten op de Microsoft Server gemaakt of verzameld worden voordat de configuratie op FDM kan worden uitgevoerd. De belangrijkste waarden zijn:

- Domain Name: Dit is de domeinnaam van de server. In deze configuratiehandleiding is bijvoorbeeld.com de domeinnaam.
- IP/FQDN-adres van server: Het IP-adres of FQDN wordt gebruikt om de Microsoft server te bereiken. Als een FQDN wordt gebruikt, moet een DNS-server binnen FDM en FTD worden geconfigureerd om de FQDN-oplossing te vinden. In deze configuratie gids, zijn deze waarden **win2016.voorbeeld.com** die naar 192.168.1.1 **oplost**.
- serverpoort: De haven die wordt gebruikt door de LDAP-dienst. Standaard zullen LDAP en STARTTLS TCP poort 389 gebruiken voor LDAP en LDAP over SSL (LDAPS) TCP poort 636 gebruiken.
- Root CA: Als LDAPS of STARTTLS wordt gebruikt, moet de basis CA die wordt gebruikt om het SSL-certificaat te ondertekenen dat door LDAPS wordt gebruikt, worden gebruikt.
- Gebruikersnaam en wachtwoord map: Dit is de account die door FDM en FTD wordt gebruikt om zich te binden aan de LDAP server en gebruikers en groepen te controleren. Voor dit doel wordt een account met de naam FTD Admin aangemaakt.
- Basisnaam (DN): De Base DN is het beginpunt FDM en de FTD zal Actieve Map vertellen om te beginnen wanneer het zoeken naar gebruikers. In deze configuratie gids, zal het root domeinvoorbeeld.com als basis DN worden gebruikt; voor een productieomgeving kan het gebruik van een basisDNA in de LDAP-hiërarchie echter beter zijn. Bijvoorbeeld, neem deze LDAP hiërarchie:



Als een beheerder wil dat gebruikers binnen de eenheid van de organisatie voor het in de handel brengen in staat zijn om de basis DN te authenticeren kan worden ingesteld op de wortel (voorbeeld.com), dan zal dit ook Gebruiker1 onder de organisatie van Financiën toestaan om ook in te loggen aangezien de gebruikerszoektocht bij de wortel zal beginnen en naar Financiën, Marketing en Onderzoek zal gaan.

Base DN ingesteld op voorbeeld.com.



Om logins te beperken tot alleen gebruikers in de afdeling Marketingorganisatie en hieronder, kan de admin in plaats daarvan de Base DN op Marketing instellen. Alleen User2 en User3 kunnen nu voor authenticatie zorgen, omdat de zoekactie bij Marketing begint.

Base DN ingesteld op Marketing:



Merk op dat voor een meer gedetailleerde controle binnen de FTD waarvoor gebruikers op basis van hun AD-eigenschappen verschillende vergunningen mogen aansluiten of toewijzen, een LBP-vergunningskaart moet worden geconfigureerd.

Deze vereenvoudigde LDAP hiërarchie wordt gebruikt in deze configuratiehandleiding en de DN voor het basisvoorbeeld.com zal worden gebruikt voor de Base DN.



#### LBP-basis DN bepalen

1. Open AD-gebruikers en computers.

=	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	a 🖉 🖞 🗋 🕲 📾
	users
-	ዶ 🗆 🤶 🚍 🤱 📕

2. Klik met de rechtermuisknop op het basisdomein (om de container te openen), klik met de rechtermuisknop op het basisdomein en navigeer vervolgens naar **Weergave** en klik op **Geavanceerde functies**.



3. Hierdoor kan de weergave van extra eigenschappen onder de AD-objecten mogelijk worden. Bijvoorbeeld, om de DN voor het root voorbeeld.com te vinden, klik met de rechtermuisknop **op voorbeeld.com** en navigeer vervolgens naar **Properties**.



4. Klik onder **Properties** op het tabblad **Eigenschappen**. Vind **geachte naam** onder de Eigenschappen en klik vervolgens op **Weergeven**.

example.	com Propertie	5				?	×
General	Managed By	Object	Security	Attribu	te Editor		
Attribute	88:						
Attribu	te	Valu	e				^
dc		exar	nple				_
defaul	tLocalPolicyOb	j knot	set>				
descri	ption	knot	set>				
deskte	op Profile	knot	set>				
display	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><td></td></not<>	set>				
domai	nReplica	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
dSAS	ignature	{ V1	: Flags = O	0; Later	ncySecs :	= 0; DsaG	uic
dSCor	rePropagationD	0x0	=()				
eFSP	olicy	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
extens	sionName	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
flags		rnot	set>				× 1
<							>
W	ew					Fite	r
	OK		Cancel		Apply	H	lelp

5. Dit opent een nieuw venster waarin de DN later kan worden gekopieerd en geplakt naar FDM. In dit voorbeeld is de root DN DC=voorbeeld, DC=com. Kopieert de waarde. Klik op **OK** om het venster van de editor van String-kenmerken te verlaten en klik vervolgens nogmaals op **OK** om de eigenschappen te verlaten.

ang Attribute Caltor	~	
ttribute: distingu	ishedName	
alue:		
DC=example,DC=com		Undo
Clear	OK Cancel	Cut
		Conv
		Dasta
		Paste
		Delete
		Select All
		Right to left Reading order
		Show Unicode control characters
		Insert Unicode control character
Attributes: Attribute	Value ^	
Attributes:		
Attribute	Value ^	
cn	<not set=""></not>	
controlAccessHights	<not set=""> 4/29/2020 2:42:49 PM Eastern Daulight Ten</not>	
de	example	
defaultLocalPolicyObj	<not set=""></not>	
description	<not set=""></not>	
desktopProfile	(not set)	
displayName displayName Distabile	(not set)	
displayNamePrintable	<not set=""></not>	
domainPolicyObject	(not set)	
domainReplica	<not set=""></not>	
dSASignature	{ V1: Rags = 0x0; LatencySecs = 0; DsaGuic	
dSCorePropagationD	0x0 = ( )	
<	>	
View	Filter	

Dit kan worden gedaan voor meerdere objecten binnen AD. Bijvoorbeeld, deze stappen worden gebruikt om DNA van de gebruikerscontainer te vinden:



6. De weergave Geavanceerde functies kan worden verwijderd. Klik met de rechtermuisknop op de root-DN, navigeer om **geavanceerde functies** te **bekijken** en klik nogmaals **op Advanced-functies**.



#### Een FTD-account maken

Met deze gebruikersaccount kunnen FDM en de FTD aan de AD binden om naar gebruikers en groepen te zoeken en hen te authentiseren. Het doel van het creëren van een afzonderlijke FTD-account is ongeoorloofde toegang elders binnen het netwerk te voorkomen indien de voor de band gebruikte referenties worden gecompromitteerd. Deze rekening hoeft niet binnen het toepassingsgebied van de basisDN te vallen.

1. In **Active Directory Gebruikers en Computers** wordt met de rechtermuisknop op de container/organisatie de FTD-account toegevoegd. In deze configuratie zal de FTD-account worden toegevoegd onder de Gebruikersnaam **ftd.admin@example.com**. Klik met de rechtermuisknop op **Gebruikers**, dan op **Nieuw > Gebruiker**.

Active Directory Users and Con	puters			-	×
File Action View Help					
🗢 🔿 🖄 🚾 🐇 💷 🗶 [	🗊 🖸 🔒 🖬 🖬	n   🐮 🔌 în 🦷	r 🗵 🕱		
Active Directory Users and Com Saved Queries Saved Queries Saved Queries Subscript Example.com Subscript Exam	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad 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 domain users		^
All Tasks View Refresh Export List Properties Help	> > WseAlertA	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue All Printer	ntial PropertyList incipalContainer		
< >> Creates a new item in this container.	& WseAllow	User Shared Folder	-		Ŷ

2. Navigeer door de **nieuwe** wizard **van de gebruiker**.

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	<u>Wi</u> ndows 2000):	
EXAMPLE\	ftd.admin	
		_
	< Back Next > Cancel	

New Object - User		×
🤱 Create in: exar	nple.com/Users	
Password:	•••••	
Confirm password:	•••••	
User must change passw	rord at next logon	
User cannot change pas	sword	
Password never expires		
Account is disabled		
	< Back Next >	Cancel
New Object - User		×
New Object - User	mple.com/Users	×
New Object - User Create in: exam When you click Finish, the for	mple.com/Users billowing object will be created:	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin	mple.com/Users billowing object will be created:	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin	mple.com/Users billowing object will be created: @example.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin The password never expires	mple.com/Users billowing object will be created: @example.com	×
New Object - User Create in: exar When you click Finish, the for Full name: FTD Admin User logon name: ftd.adminu The password never expires	mple.com/Users billowing object will be created: @example.com 8.	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin The password never expires	mple.com/Users bilowing object will be created: @example.com 8.	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.adminu The password never expires	mple.com/Users bilowing object will be created: @example.com s.	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admine The password never expires	mple.com/Users ollowing object will be created: @example.com s.	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.adminu The password never expires	mple.com/Users pllowing object will be created: @example.com s.	×

3. Controleer dat de FTD-account is aangemaakt. Daarnaast zijn er twee extra rekeningen gecreëerd, **IT Admin** en **Test User**.

Active Directory Users and Computers					×
🖾 🗟 📑 🖬	n 🙁 📚 în 🦷	7 🗾 🗽			
Name DefaultAcco DefaultAcco DefaultAcco Donain ROD Donain Ad Domain Ad Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Comain Gue	Type User Security Group Security Group User	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 guests All domain users Designated administrato Members of this group Members of this group Members of this group			~
Key Admins Key Admins RAS and IAS Read-only D Schema Ad Test User	Security Group 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			~
	Name DefaultAcco DefaultAcco DefaultAcco Denied ROD DonsUpdateP Donain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Comain Gue Domain Gue Reat-only D Read-only D Schema Ad Test User	Imputers         Imputers	Imputers         Imputers         Imputers       Imputers         Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Imputers       Imputers       Imputers       Imputers       Imputers       Imputers       Imputers         Imputers       Im	Imputers       —         Imputers       Imputers         Imputers <td>Imputes       —       —         Imputes       Imputes       Imputes       Imputes         Imputes       Imputes       Imputes       Imputes       Imputes         Imputes       Imputes       Imputes       Imputes       Imputes       Imputes</td>	Imputes       —       —         Imputes       Imputes       Imputes       Imputes         Imputes       Imputes       Imputes       Imputes       Imputes         Imputes       Imputes       Imputes       Imputes       Imputes       Imputes

#### AD-groepen maken en gebruikers aan AD-groepen toevoegen (optioneel)

Hoewel niet vereist voor authenticatie, kunnen groepen worden gebruikt om het gemakkelijker te maken om toegangsbeleid toe te passen op meerdere gebruikers zowel als op de LDAP - autorisatie. In deze configuratiehandleiding worden groepen gebruikt om later beleidsinstellingen voor toegangscontrole toe te passen door middel van gebruikersidentiteit binnen FDM.

1. In Actieve Gebruikers en Computers van de Map, klikt u met de rechtermuisknop op de container/de organisatie waaraan de nieuwe groep wordt toegevoegd. In dit voorbeeld wordt de groep AnyConnect Admins toegevoegd onder de Gebruikers-tank. Klik met de rechtermuisknop op Gebruikers, dan op Nieuw > Groep.

Active Directory Users and Com	puters			-	х
File Action View Help					
🗢 🔿 🖄 🚾 🐇 💷 🗶 (	🗊 🖸 🔒 🚺 🖬	1 🗏 🔌 🗈 🎙	1 🗵 🔍		
Active Directory Users and Com Saved Queries Saved Queries Saved Queries Subscription Subscription Subscription Subscription Subscription Active Directory Users and Com Subscription Subsc	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co ntrol	Type User 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	ers	Computer Contact Group InetOrgPerson msDS-KeyCreder	All domain users		
Export List Properties Help	Read-only	msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue Al Printer User	PropertyList incipalContainer i ias		
Creates a new item in this container.		Shared Folder			×

2. Navigeer door de Nieuwe Object - Group Wizard zoals in de afbeelding.

	×
Create in: example.c	om/Users
oup name:	
nyConnect Admins	
wo name (ore-Windows 2000):	
nyConnect Admins	
roup scope	Group type
Domain local	Security
🖲 Global	Obstribution
Universal	
	OK Cancel

3. Controleer of de groep is aangemaakt. De AnyConnect-gebruikersgroep is ook opgericht.

Active Directory Users and Com	_	×			
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 Domain Admins Domain Computers Domain Computers Domain Controllers 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 I 2.1.		

4. Klik met de rechtermuisknop op de groep waaraan de gebruiker(s) wordt toegevoegd en selecteer **Eigenschappen**. Bij deze configuratie wordt de gebruiker **IT Admin** toegevoegd aan de groep **AnyConnect Admins** en de **testgebruiker** wordt toegevoegd aan de groep **AnyConnect-gebruikers**.

Active Directory Users and Computer	iters			-	×
File Action View Help					
🗢 🔿 🙍 📰 🤞 🖾 🔀	@ 🔒 🛛 🖬 🖏	k 🛯 🔻 🧕 🕯	5		
Active Directory Users and Com	Name AnyConnect Admins	Type Security Group	Description		^
Builtin     Computers     Some Domain Controllers	AnyConnect Users calo	Security Group User Security Group	Buil Move Mer Send Mail		
> ForeignSecurityPrincipal:	Cloneable Domain C DefaultAccount	Security Group User	Mer All Tasks A u:	>	
Users	Denied RODC Passw DnsAdmins DnsUpdateProxy Domain Admins Domain Computers Domain Controllers Domain Guests Domain Users	Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Mer Cut DNS Delete DNS Rename Des All v <b>Properties</b> All v Help All communications All domain users		
	Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Security Group Security Group User Security Group User User Security Group	Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue Members of this group		
Renames the current selection.	(h.s				Ŷ

5. Klik op het tabblad Leden en klik vervolgens op Toevoegen zoals in de afbeelding.

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

Voer de gebruiker in het veld in en klik op de knop **Namen controleren** om te controleren of de gebruiker wel gevonden is. Klik na verificatie op **OK**.

Select Users, Contacts, Computers, Service Accounts,	or 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
ådvanced	OK Cancel

Controleer of de juiste gebruiker is toegevoegd en klik vervolgens op de knop **OK**. De gebruiker Test Gebruiker is ook toegevoegd aan groep AnyConnect-gebruikers met dezelfde stappen.

AnyConn	ect Admin	s Properties			?	×
General	Members	Member Of	Managed By			
Member	na:					_
Name & IT	Admin	Active Dir example.c	ectory Domain com/Users	Services Folder		
	_					-
Ad	d	Remove				
			ОК	Cancel	Ар	ply

Kopieer de LDAPS SSL-certificatieroot (alleen vereist voor LDAPS of STARTTLS)

1. Druk op Win+R en type mmc.exe. Klik op OK.

💷 Run		×
0	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	<u>B</u> rowse

2. Navigeer naar **bestand > Magnetisch toevoegen/verwijderen...** zoals in de afbeelding wordt weergegeven.

🚡 Console1 - [Console Root]		-	ΟX
File Action View Favorites Window	Help		_ 8 ×
New Ctrl+N			
Open Ctrl+O		Actions	
Save Ctrl+S	There are no items to show in this view.	Console Root	<b>^</b>
Save As		More Actions	+
Add/Remove Snap-in Ctrl+M			
Options			
1 dnsmgmt			
2 dsa			
Exit			
Enables you to add snap-ins to or remove them fr	om the snap-in console.		

3. Klik onder beschikbare knoppen op Certificaten en vervolgens op Toevoegen.

Add or Remove Snap-ins				×				
You can select snap-ins for t extensible snap-ins, you can	You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.							
Available snap-ins:			Selected snap-ins:					
Snap-in	Vendor	^	Console Root Edit Extensions					
Active Directory Do	Microsoft Cor		Remove					
Active Directory Site	Microsoft Cor							
Active Directory Use	Microsoft Cor		Meso Lin					
ActiveX Control	Microsoft Cor		Hove Op					
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	¥	Advanced					
Description:								
The Certificates snan-in all	we you to browse	the	e contents of the certificate stores for yourself, a service, or a computer.					
The certificates shap that	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	-	e contenta or are certained to rear your service, or a comparer.					
			OK Cancel					

## 4. Selecteer Computer-account en klik vervolgens op Volgende zoals in de afbeelding.

Certificates snap-in	×
This snap-in will always manage certificates for: 	
< <u>Back</u> <u>N</u> ext > Car	ncel

Klik op Voltooien.

Select Computer	×
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>Rrowse</li> </ul> Another computer:       Browse         Alow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

### 5. Klik op **OK**.

Add or Remove Snap-ins				3	×
You can select snap-ins for t extensible snap-ins, you can	his console from the configure which e	iose xter	available on you nsions are enable	r computer and configure the selected set of snap-ins. For d.	
Available snap-ins:				Selected snap-ins:	
Snap-in	Vendor	^		Console Root Edit Extensions	
Active Directory Do	Microsoft Cor Microsoft Cor			Certificates (Local Computer)	
Active Directory Use	Microsoft Cor Microsoft Cor			Move <u>U</u> p	
ADSI Edit	Microsoft Cor Microsoft Cor		Add >	Move <u>D</u> own	
Certificate Templates	Microsoft Cor Microsoft Cor				
Component Services	Microsoft Cor Microsoft Cor				
Computer Managem	Microsoft Cor Microsoft Cor				
T Disk Management	Microsoft and	$\checkmark$		Advanced	
Description: The Certificates snap-in allo	ws you to browse	the	contents of the	certificate stores for yourself, a service, or a computer.	٦
				OK Cancel	

6. Vouw de **persoonlijke** map uit en klik vervolgens op **Certificaten**. Het certificaat dat wordt gebruikt door LDAPS moet worden afgegeven aan de FQDN-naam (Full Qualified Domain Name, FQDN) van de Windows-server. Op deze server zijn er 3 certificaten vermeld.

- Een CA-certificaat afgegeven aan en door voorbeeld-WIN2016-CA.
- Een identiteitsbewijs afgegeven aan WIN2016 door voorbeeld-WIN2016-CA.
- Een identiteitsbewijs afgegeven voor win2016.voorbeeldv.com door voorbeeld-WIN2016-CA.

In deze configuratie gids is de FQDN win2016.voorbeeldcom en dus zijn de eerste 2 certificaten niet geldig voor gebruik als het LDAPS SSL-certificaat. Het identiteitsbewijs dat is afgegeven voor win2016.voorbeeldcom is een certificaat dat automatisch is afgegeven door de CA-service van Windows Server. Dubbelklik op het certificaat om de gegevens te controleren.

🚡 Console1 - [Console Root\Certific	ates (Local Computer)\Personal\C	ertificates]		-	οx
🚟 File Action View Favorites	Window Help				- 8 ×
🗢 🔿 🙋 📆 📋 🙆 😽	2				
Console Root	Issued To	Issued By	Expiration Da	Actions	
Certificates (Local Computer)	axample-WIN2016-CA	example-WIN2016-CA	4/19/2060	Certificates	<b></b>
Contificator	20 WIN2016	example-WIN2016-CA	4/27/2025	More Actions	+
Trusted Boot Certification	win2016.example.com	example-WIN2016-CA	4/28/2021		
> Cherprise Trust					
> intermediate Certification					
> 📔 Trusted Publishers					
> Intrusted Certificates					
> iii Third-Party Root Certificat					
> iii Trusted People					
> Client Authentication Issue					
> iii Preview Build Roots					
> local NonRemovable Cert					
> 🧮 Remote Desktop					
> Certificate Enrollment Req					
Smart Card Trusted Roots					
> Trusted Devices					
> Web Hosting					
> windows Live ID Token Iss					
< >	<		>		
Personal store contains 3 certificates.					

7. Het certificaat moet aan de volgende eisen voldoen om als LGO-SSL-certificaat te kunnen worden gebruikt:

- De gezamenlijke naam of DNS Betreft Alternatieve naam komt overeen met FQDN van de Windows Server.
- Het certificaat heeft serververificatie onder het veld Uitgebreide sleutel voor gebruik.

Onder het tabblad Details voor het certificaat, onder **Onderwerp** en **Onderwerp Alternatieve Naam**, **is** FQDN **win2016.voorbeeld.com** aanwezig.

🙀 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	
Enf	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	¢

🙀 Certil	ficate			×
General	Details	Certification Path		
Show:	<al></al>		~	
Field Sul Au CR Au	bject Key thority Ke L 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 Thi Thi	y Usage umbprint	mative Name	Other Name:DS Object Guid= Digital Signature, Key Encipher sha1 ca Re 11 3d eb bc 0f 6e 4a 00	~
Other M DS 0 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	(

Onder Uitgebreid gebruik, is de serververificatie aanwezig.

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al></al>		$\sim$	
Field			Value	^
E Su E Pu Pu	bject blic key blic key pa	arameters	win2016.example.com RSA (2048 Bits) 05 00	
Ce SE SM SM	rtificate T hanced Ki IIME Capa	emplate Name ey Usage bilities	DomainController Client Authentication (1.3.6.1 [1]SMIME Capability: Object I 20.b7.2b.4e.48.0f.2f.17.17.ef.	
(金) SU 用 Au	thority Ke	uenuner v Identifier	30 07 20 He Ho UT 2T 17 17 e6 KevID=3d 9f 26 37 fb 11 1f 4	¥
Client / Server	Authentic	ation (1.3.6.1.5.5.) ation (1.3.6.1.5.5.	7.3.2) (7.3.1)	
		Ed	It Properties Copy to File	
			0	ĸ

8. Als dit eenmaal is bevestigd, navigeer dan naar het tabblad **certificeringssnijpad**. Klik op het hoogste certificaat dat het basiscertificaat moet zijn, en klik vervolgens op de knop **Certificaat bekijken**.

💼 Certificate	×
General Details Certification Path	
Certification path	
	View Certificate
Certificate status: This certificate is OK.	
	ОК

9. Hierdoor worden de certificeringsgegevens voor het basiscertificaat van CA geopend.

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. Open het tabblad **Details** en klik vervolgens op **Kopie naar bestand...** zoals in de afbeelding wordt weergegeven.

Certificate		$\times$
General Details Certification Path		
Show: <all></all>	~	
Field	Value	^
Version Serial number Signature algorithm Signature hash algorithm 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	>
E	dit Properties Copy to File	
	ОК	

11. Navigeer door de Wizard Certificaat Exporteren die de wortel CA in PEM-indeling zal uitvoeren.

÷	🐓 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	1

12. Selecteer Base-64 gecodeerd X.509.

÷	🚰 Certificate Export Wizard	^
	Export File Format Certificates can be exported in a variety of file formats.	
	Select the format you want to use:	
	O DER encoded binary X.509 (.CER)	
	Base-64 encoded X.509 (.CER)	
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
	Include all certificates in the certification path if possible	
	<ul> <li>Personal Information Exchange - PKCS #12 (.PFX)</li> </ul>	
	Include all certificates in the certification path if possible	
	Delete the private key if the export is successful	
	Export all extended properties	
	Enable certificate privacy	
	<ul> <li>Microsoft Serialized Certificate Store (.SST)</li> </ul>	
	Next Cance	I

 $\sim$ 

13. Selecteer de naam van het bestand en waar het naar geëxporteerd wordt.

Everificate Export Wizard      File 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. Klik op Voltooien.

esktop'root.cer
.509 (*.cer)
Finish Cancel

15. Ga nu naar de locatie en open het certificaat met een schrijfblok of een andere teksteditor. Dit toont het PEM-certificaat. Sla dit later op.

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

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++M+bLn3AiZnHV
00+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscbubR1+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33Pp1W6E
```

----END CERTIFICATE----

## **FDM-configuraties**

Controleer de licenties

Om AnyConnect op FDM te configureren moet de FTD worden geregistreerd met de slimme licentieserver en moet een geldige Plus-, Apex- of VPN-licentie alleen op het apparaat worden toegepast.

cisco. Firepower Devis	ce Manager	Monitoring Policies	ing Objects	Device: FTD-3	6	) 🖨 🙆	?:	admin Adm/nistrator
	Finalde Netwo	ort	637 Defense for V (0) 0 0/1 0/2 2 2 2 10 10 10 10 10 10 10 10 10 10 10 10 10 1	CONSOLE	ISPWAN/Gotoway	Internet CNS Server CNTP Server CNTP Server Cntthe Smart Licer	60	
Interfaces Connected Enabled 3 of 4 View All Interfaces	>	Routing 2 routes View Configuration	>	Updates Geolocation, Ruk Security Intelligen View Configurat	e, VDB, System Upgrad nee Feeds ion	Syst Mana Loggi DHCF DNS	tem Setting: gement Access ng Settings ? Server Server	S
Smart License Registered View Configuration	>	Backup and Restore	>	Troubleshoo No files created y REQUEST FILE	t vet TO BE CREATED	Mana Hostr NTP Cloud Rebo Traff	gement Interfac ame I Services ot/Shutdown ic Settings	×

1. Blader naar **apparaat > Smart License** zoals in de afbeelding.

2. Controleer dat de FTD bij de slimme licentieserver is geregistreerd en dat de AnyConnect Plux, Apex of VPN only licentie is ingeschakeld.



#### AD-identiteitsbron instellen

1. Navigeer naar **Exemplaren > Identiteitbronnen**, klik dan op het **+** symbool en selecteer **AD** zoals in de afbeelding.

cisco. Firepower Dev	ice Manager Monitoring Policie	s Objects Device: FTD-3	o 🔒 🙆 ? 🗄	admin Administrator
Object Types 🔶	Identity Sources			
C Networks	1 object		Q Search	+ ~
와 Ports	* NAME	THE	VALUE	RADIUS Server
Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
🐔 Application Filters				AD
Ø URLS				Identity Services Engine
Geolocations				
Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
🔒 AnyConnect Client				
Identity Sources				
1 Users				
R Certificates				
🔒 Secret Keys				
DNS Groups				
Vert List Filters				

2. Vul de juiste instellingen voor de Active Directory server in met de eerder verzamelde informatie. Als een hostname (FQDN) voor de Microsoft server in plaats van een IP-adres wordt gebruikt, zorg er dan voor dat er een geschikte DNS-groep onder **Objecten > DNS-groep** wordt gemaakt. Pas dan die DNS-groep op de FTD toe door te navigeren naar **Apparaat > Systeeminstellingen > DNS-server**, de DNS-groep toe te passen onder de **Managementinterface** en **Data Interface** en dan de juiste graafinterface voor DNS-vragen te specificeren. Klik op de knop **Test** om een succesvolle configuratie en bereikbaarheid te controleren vanuit de beheerinterface van de FTD. Aangezien deze tests worden gestart vanuit de beheerinterface van de FTD en niet via een van de routeerbare interfaces die op de FTD zijn geconfigureerd (zoals binnen, buiten, dmz), garandeert een succesvolle (of mislukte) verbinding niet hetzelfde resultaat voor AnyConnect-verificatie, aangezien AnyConnect LDAP-verificatieverzoeken zullen worden geïnitieerd vanuit een van de routekaarten van de FTD. Kijk in het gedeelte Problemen oplossen voor meer informatie over het testen van LDAP-verbindingen vanuit de FTD. Add Identity Realm

Ŀ,

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
Hostname / IP Address win2016.example.com	90rt 389
Hostname / IP Address win2016.example.com e.g. ad.example.com	Port 389
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption	Port 389 Trusted CA certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful Add another configuration	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful Add another configuration	Port 389 Trusted CA certificate Please select a certificate

Als LDAPS of STARTTLS wordt gebruikt, selecteert u de juiste encryptie en vervolgens selecteert u het Trusted CA-certificaat. Als de bron-CA niet al is toegevoegd, klikt u op **Nieuw betrouwbaar CA-certificaat maken**. Typ een naam voor het basis-CA-certificaat en plak vervolgens het PEM-formaat wortelcertificaat dat eerder is verzameld.

## Add Trusted CA Certificate

Name LDAPS_ROOT	
Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.	
BEGIN CERTIFICATE MIIDCDCCAfCgAwlBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjlwMTYtQ0EwlBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC ASlwDQY_lKoZlbwcNAQEBBQADcoCAQoCcaeEBAl8chT719NzSQpoQPb0YT67b	
CANCEL	
Directory Server Configuration	

0 X

win2016.example.com:636		4	•
Hostname / IP Address		Port	
win2016.example.com		636	
e.g. ad.example.com			
Encryption		Trusted CA certificate	
LDAPS	~	LDAPS_ROOT	~
TEST ✓ Connection to realm is suc	ccessful		

In deze configuratie werden deze waarden gebruikt:

- Name: LAB-AD
- Gebruikersnaam map: ftd.admin@example.com
- Base DN: DC=voorbeeld, DC=com
- AD Primair domein: example.com
- Hostnaam/IP-adres: win2016.example.com
- Port: 389
- 3. Klik rechtsboven op de knop Wijzigingen in de afbeelding in afwachting van verandering.

cisco. Firepower De	wice Manager 🕅 🧭	Objects Device: FTD-3	S admin Administrator ✓
Object Types 🛛 🗧	<ul> <li>Identity Sources</li> </ul>		
C Networks	2 objects	Q. Sas	** <b>+</b> *
S Ports	H NAME	TYPE VALUE	ACTIONS
Security Zones	1 LocalIdentitySource	LOCAL	
Application Filters	2 LAB-AD	AD win2016.example.	com

#### 4. Klik op de knop **Nu implementeren**.

Pe	ending Changes	0 ×	
0	Last Deployment Completed Successfully 01 May 2020 12:54 PM. <u>See Deployment History</u>		
	Deployed Version (01 May 2020 12:54 PM)	Pending Version ( LEGEND Removed Added Edited	
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 V	

#### AnyConnect voor AD-verificatie configureren

Om de geconfigureerde AD-identiteitsbron te kunnen gebruiken, moet deze op de AnyConnectconfiguratie worden toegepast.

1. Blader naar **Apparaat > Remote Access VPN** zoals in de afbeelding.

CISCO. Firepower Device Manager	Monitoring Policies Objects	Device: FTD-3	admin
	[ <u>avo</u> ]		
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	Management Interface 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. Klik op het + symbool of de knop verbindingsprofiel maken zoals in de afbeelding.



3. Selecteer onder het gedeelte Connection en Client Configuration de AD-identiteitsbron die eerder is gemaakt. Stel de juiste waarden voor de andere onderdelen in, inclusief de toewijzing van het verbindingsprofiel en de clientadrestoewijzing. Klik op **Submit Query** als u klaar bent.

## Connection and Client Configuration

Specify now to authenticate remote users	inside network.
Connection Profile Name This name is configured as a connection alias, it c	can 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 Authentica	ation Fallback Local Identity Source 🔥
Filter	✓ Please Select Local Identity Source ✓
11 LocalidentitySource	~
11 LAB-AD	0
11 Special-Identities-Realm	~
Create new 💙	

#### 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. Selecteer in het gedeelte Remote User Experience het juiste groepsbeleid. Standaard wordt het **DfltGrpPolicy** gebruikt; er kan echter een andere worden gecreëerd .

```
View Group Policy
```

DfltGrpPolicy

Policy Group Brief Details

DNS + BANNER	Ed
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. Specificeer onder het gedeelte Global Settings ten minste het SSL-certificaat, de externe interface en de AnyConnect-pakketten. Als er nog geen certificaat is gemaakt, kan er echter een standaard, zelf-ondertekend certificaat (<u>DefaultInternecertificaatbericht</u>) worden geselecteerd. U kunt het certificaat van een onvertrouwde server echter wel zien. Het beleid van toegangscontrole voor gedecrypteerd verkeer (systeemvergunning-vpn) moet ongecontroleerd zijn zodat de regels van het toegangsbeleid voor gebruikers van identiteit later van kracht worden. NAT-vrijstelling kan hier ook worden ingesteld. In deze configuratie is al het ipv4-verkeer van de interne interface naar AnyConnect client-IP-adressen behalve NAT. Voor complexere instellingen zoals buiten het afkapsel, zullen in het kader van het NAT-beleid aanvullende NAT-regels moeten worden gecreëerd. AnyConnect-pakketten zijn beschikbaar op de Cisco-ondersteuningswebsite: <u>https://software.cisco.com/download/home</u>. Er is een geldige Plus- of Apex-licentie vereist om het AnyConnect-pakket te kunnen downloaden.

## **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 V	outside (GigabitEthernet0/0)
Fully-qualified Domain Name for the Outside Inter	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 co and the authorization ACL downloaded from the AAA serv Bypass Access Control policy for decrypted	ry inspection by default. Enabling the Bypass Access Control ontrol policy, but for remote access VPN, the VPN Filter ACL ver are still applied to VPN traffic traffic (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)	+
	الله 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	age installed, the system will launch the AnyConnect e user can then install the package from the system.
You can download AnyConnect packages from software.cl You must have the necessary AnyConnect software license	isco.com. e.



6. Controleer onder het kopje of AnyConnect correct is ingesteld en klik vervolgens op Submit Query.

#### Summary

Review the summary of the Remote Access VPN configuration.

O		
General		
STEP 1: CONNECTION AND CLIENT CONFIGURATION	DN	
Primary Identity Source		
Authentication Type	AAA Only	
Primary Identity Source	北 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	-	
Fallback Local Identity Source	-	
⊘ Advanced		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		

7. Klik op de knop Wijzigingen rechts in de afbeelding.

cisco. Firepower Dev	ice Manager Monitoring Policies Objects	Device: FTD-3	(5.) 🕢 🗇 ? 🕴 admin Administrator
RA VPN ←	Device Summary Remote Access VPN Connection Prof	iles	
Connection Profiles	1 object	Q, s	tearch +
	я нама	***	SROUP POLICY ACTIONS
	1 General	Authentication: AAA Only Authorization: None Accounting: None	DfttGrpPolicy

8. Klik op Nu implementeren.



#### identiteitsbeleid inschakelen en beveiligingsbeleid voor gebruikers-identiteit instellen

Op dit punt zouden AnyConnect-gebruikers met succes moeten kunnen verbinden, maar mogelijk geen toegang hebben tot specifieke bronnen. Deze stap maakt het mogelijk de identiteit van de gebruiker te bepalen, zodat alleen gebruikers binnen AnyConnect Admins met interne bronnen kunnen verbinden met het gebruik van RDP en alleen gebruikers binnen de groep AnyConnectgebruikers met interne bronnen kunnen verbinden met het gebruik van HTTP.

1. Navigeer naar **beleid > Identity** en klik op **identiteitsbeleid inschakelen**.

cisco. Firepower De	wice Manager Monitoring	Policies Objects	Device: FTD-3	> 🖨	۵ ()	÷	admin Administrator
Security Policie     → O sst. Decry	IS gation → <mark>O kitenatiy</mark> → O Securit	Intelligence $ ightarrow$ 🔗 N	IAT $ ightarrow$ Access Control	-> 🖏 Intrusion			
	Establishing User Identity You can use identity policies to collect us identity information from connections. You can then view usage based on user identi in the dashboards, and configure access control based on user or user group. By Inking network behavior, traffic, and even directly to individual users, the system can help you identify the source of policy breaches, attacks, or network vulnerabilities.	users 🍂	How Identity polic Passive authentication Act PASSIVE AUTHENTIC PASSIVE AUTHENTIC PASSIVE AUTHENTIC MULTIPLE DENTITY SOURCE DENTITY SOURCE	cies work  five authentication  ICATION  CES  POLICY	IGE IDENTITY		

Voor deze configuratie is geen verdere configuratie nodig en is de Standaardactie voldoende.

cisco. Firepo	wer Device Manag	er Mor	itoring Policies	語 Objects	Device: FTD-3	(	> 🔒 🛛	?:	admin Administrator	~	
Security Policies											
$\Box \rightarrow \bigcirc SSL Decryption \rightarrow \bigodot Identity \rightarrow \bigcirc Security Intelligence \rightarrow \bigotimes NAT \rightarrow \bigotimes Access Control \rightarrow \circledast Intrusion$											
Identity Policy	D					Q Search			¢ <sub>2</sub>	+	
			SOURCE			DESTINATION					
H NAME	AUTHENTICATION	AUTH, TYPE	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	ACTIO	NS	
				There are no k	dentity rules yet.						
				Start by creating t	he first Identity rule						
				CREATE ID	ENTITY RULE						
Default Action	A Passive Auth Ar	v Identity Source	× 0								
L	a contraction for	.,									

2. Navigeer naar **beleid > NAT** en zorg ervoor dat NAT correct is geconfigureerd. Als de NATuitzondering die in de AnyConnect-instellingen is ingesteld, is geconfigureerd, is hier geen extra configuratie nodig.

cisco. Firepow	er Device	Manager	Monitoring	Ø Policies	₩E Objects	Device: FTD-3		۵ 🔒	Ø ?	admin Admini	strator
🛷 Security Po	licies										
□ → ○ sst	Decryption	-> 🕑 Id	entity $\rightarrow$ $\bigcirc$ S	ecurity Intelligent	20	T $ ightarrow$ 🖉 Acce	ess Control 🛛 🔿	S Intrusion			
1 rule								Q Search			+
			OFFICINAL PACKET				TRANSLATED PACK	π			
a NAME	TYPE	INTERFACES	SOURCE AD	DESTINATIO	SOUNCE PORT	DESTINATIO	SOUNCE AD	DESTINATIO	SOURCE PORT	DESTINATIO	ACTIONS
Auto NAT Rules											
> # Internet_PAT	DYNAMIC	U ANY outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

3. Navigeer naar **beleid > Toegangsbeheer**. In dit gedeelte is de Default Action (Actie) ingesteld op Blokken en er zijn geen toegangsregels gecreëerd. Zodra een AnyConnect-gebruiker zich aansluit, kunnen ze niets bereiken. Klik op het **+** symbool of **op** Toegangsregel maken om een nieuwe regel toe te voegen.

cisco. Firepor	wer Device Manager	Monitoring	Policies	前面 Objects	Device: FTD-3		۵ 🗳	0 ()	ad Ad	imin v Iministrator
🛷 Security P	olicies									
⊡ → Os	SL Decryption $ ightarrow$	Identity $\rightarrow$ ():	Security Intelligence	) -> 📀 N/	AT $ ightarrow$ Acces	s Control 🔿 🛛 🍕	Intrusion			
						Q Search				®. +
	800802			DESTINATION						
* NAME	ACTION ZONES	METWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
				There are no i	access rules yet.					
			2	tart by creating I	the first access rule.					
				CREATE A	CCESS RULE					
Default Action	Access Control 😑 Block	9. E. I -								

4. Vul de velden in met de juiste waarden. In deze configuratie moeten gebruikers binnen de groep AnyConnect Admins RDP-toegang tot de Windows Server in het interne netwerk hebben. Voor de bron wordt de zone ingesteld als buitenkant\_zone, die de externe interface is waar de AnyConnect-gebruikers een verbinding mee zullen maken en het netwerk is geconfigureerd als het AnyConnect-Pool-object dat eerder was geconfigureerd om IP-adressen toe te wijzen aan AnyConnect-klanten. Voor gebruikers-identiteit in FDM moet de bron de zone en het netwerk zijn waarvan de gebruiker de verbinding start. Voor de bestemming, wordt de zone gevormd als binnenkant\_zone die de binneninterface is de Server van Windows wordt gevestigd, wordt het netwerk gevormd als het object Inside\_Net dat een object is dat het net definieert waarin de Windows Server zich bevindt, en Port/Protocols worden ingesteld op twee aangepaste poortobjecten om RDP-toegang via TCP 3389 en UDP 3389 toe te staan.

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		$\leftrightarrows_{RDP-TCP}$		
Show Diagram	$\supset$	Not hit yet							CA	WCEL	ок	

Onder het gedeelte Gebruikers wordt de groep AnyConnect Admins toegevoegd zodat gebruikers uit deze groep RDP-toegang tot de Windows Server krijgen. Klik op het + symbool, klik op het tabblad Groepen, klik op het juiste groep en klik vervolgens op **OK**. Houd er rekening mee dat individuele gebruikers en de identiteitsbron ook kunnen worden geselecteerd.

Add Access Rule	• ×
Order Title 1 Y AC RDP Access	Action       Allow
Source/Destination Applications URLs Users	Intrusion Policy File policy Logging
▼ Filter Identity Sources Groups 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
北 LAB-AD \ Account Operators 北 LAB-AD \ Administrators	<ul> <li>network access changes as users change roles in your organization, moving from one group to another.</li> </ul>
LAB-AD \ Allowed RODC Password Replication Group     LAB-AD \ AnyConnect Admins     LAB-AD \ AnyConnect Users	Ĵ
Create new Identity Realm CANCEL OK	
Show Diagram	CANCEL OK

## Klik nadat de juiste opties zijn geselecteerd op OK.

Add Access Rule	• ×
Order Title Act 1  AC RDP Access Source/Destination Applications URLs Users Intrusion	tion       Allow     V       Policy     File policy       Logging
AVAILABLE USERS	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

5. Maak indien nodig meer toegangsregels. In deze configuratie wordt een andere toegangsregel

gecreëerd om gebruikers binnen de AnyConnect-gebruikersgroep HTTP toegang tot de Windowsserver te geven.

Edit Access Rule		0 ×
Order Title	Action	
2 V AC HTTP Access	🔁 Allow \vee	
Source/Destination Applications URLs Users Intr	usion Policy <sup>0</sup> File policy <sup>0</sup> Loggi	ing
SOURCE	DESTINATION	· •
Zones + Networks + Ports	+ Zones	+ Networks + Ports/Protocols +
AnyConnect-Pool	a inside_zone	🕤 Inside_Net 🖕 HTTP
Show Diagram		CANCEL OK
Order Title	Action	
2 Y AC HTTP Access	Allow ✓	
Source/Destination Applications URLs Users Intr	usion Policy <sup>9</sup> File policy <sup>9</sup> Loggi	ing
AVAILABLE USERS	+ the controlling ac	CCESS FOR USERS AND USER GROUPS
	address, you can co membership. By cor appropriate access- different address thu network access cha from one group to a	ontrol access based on user name or user group ntrolling access based on user identity, you can apply the controls whether the user changes workstations or obtains a rough DHCP. If you base rules on group membership, user anges as users change roles in your organization, moving another.
Show Diagram		CANCEL OK

6. Controleer de configuratie van de toegangsregel en klik vervolgens op de knop Wijzigingen

rechtsboven in de afbeelding.

cisco. Firepor	ver Devic	e Manager	Egg Monitoring	Policies	Objects 0	Device: FTD-3		0	0	) : (	admin A <i>dministra</i>	itor
🕫 Security P	olicies											
$\Box \rightarrow \bigcirc$ SSL Decryption $\rightarrow \oslash$ Identity $\rightarrow \bigcirc$ Security Intelligence $\rightarrow \oslash$ NAT $\rightarrow \oslash$ Access Control $\rightarrow \circledast$ Intrusion												
2 rules							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 Acces	n Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne	Ф.С.	
Default Action A	ccess Contro	😑 Block 🛛 🖏	₽									

7. Controleer de wijzigingen en klik vervolgens op Nu implementeren.

Pe	nding Changes		0	×
<ul> <li>↓</li> <li>↓</li></ul>	ast Deployment Completed Successfully 8 Apr 2020 01:35 PM. See Deployment History			
	Deployed Version (28 Apr 2020 01:35 PM)	Pending Version C LEGEND Removed	Added	Edited
0	Access Rule Added: AC HTTP Access			^
		users[0].name: AnyConnect Users logFiles: false eventLogAction: LOG_NONE ruleId: 268435467 name: AC HTTP Access		
	sourceZones:			
	destinationZones:	outside_zone		
	-	inside_zone		
	sourceNetworks:			
	-	AnyConnect-Pool		
	destinationNetworks:			
	-	Inside_Net		
	destinationPorts:	HTTP		
	users[0].identitySource:			
	-	LAB-AD		
0	Access Pula Added: AC PDP Access			~
0	ACCess Rule Audeu, AC RDF ACCess			
м	RE ACTIONS Y	CANCEL DEPLOY NO	w	~

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

### Eindconfiguratie

#### AAA-configuratie

show running-configuration aaa-server

dn ftd.admin@example.com server-type auto-detect

AnyConnect configureren

> 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

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-login-

Connect met AnyConnect en controleer beleidsregels voor toegangscontrole

S Cisco AnyCo	VPN: Contacting ftd3.4	example.co	ent -	Conr	nect		
¢ (i)		S Cisco	o AnyConne Group: Username: Password:	ct   ftd3.e General it.admin	example.com	~	×
					ОК	Cancel	
S Cisco AnyCo	nnect Secure M	obility Cli	ent -	-	×		
	VPN: Connected to ftd ftd3.example.co	13.example	.com.	Discor	nect		
00:00:14					IPv4		
<b>Q</b> ()							

Gebruiker IT Admin is in de groep AnyConnect Admins die RDP-toegang tot de Windows Server heeft, maar heeft geen toegang tot HTTP. Als u een RDP- en Firefox-sessie naar deze server opent, verifieert u dat deze gebruiker de server alleen kan benaderen via RDP.



Als u inlogt bij een Test-gebruiker die in de groep AnyConnect-gebruikers is die HTTP-toegang maar geen RDP-toegang hebben, kunt u controleren of de regels voor het toegangscontrolebeleid van kracht worden.



## Problemen oplossen

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

### Debugs

Dit debug kan in een diagnostische CLI worden uitgevoerd om problemen met de authenticatie aan de LMP op te lossen: **debug Idap 255**.

Om problemen met betrekking tot de identiteit van gebruikers op te lossen, **kan** het **systeem** de **ondersteuning van firewalls** en **het debug** van **firewalls** in Engels worden uitgevoerd om te bepalen waarom verkeer onverwachts is toegestaan of geblokkeerd.

#### Werkopbalkkaarten

```
[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:
      objectClass: value = top
[53]
[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]
[53]
       displayName: value = IT Admin
      uSNCreated: value = 25896
[53]
[53]
      memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]
      uSNChanged: value = 26119
      name: value = IT Admin
[53]
[53]
       objectGUID: value = &...J..O..2w...c
[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 = 1601010100000.0Z
[53]
       lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

#### Kan geen verbinding met LDAP-server opzetten

```
[-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
```

Potentiële oplossingen:

- Controleer de routing en zorg ervoor dat de FTD een antwoord van de LDAP-server ontvangt.
- Als LDAPS of STARTTLS wordt gebruikt, zorg er dan voor dat het juiste basiscertificaat van CA is vertrouwd zodat de SSL-handdruk met succes kan worden voltooid.
- Controleer dat het juiste IP-adres en de juiste poort worden gebruikt. Als een hostname wordt gebruikt, controleer of DNS in staat is om deze op het juiste IP-adres op te lossen

#### Vastlegging ISDN en/of wachtwoord niet correct

```
[-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
```

Potentiële oplossing: Controleer dat de inlognaam en het inlogwachtwoord correct zijn ingesteld. Dit kan op de AD server met **Idp.exe** worden geverifieerd. Om te verifiëren dat een account met succes kan verbinden met het gebruik van Idp, navigeer deze stappen:

1. Druk op Win+R op de AD-server en zoek naar Idp.exe.

💷 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. Klik op **Connection > Connect...** zoals in de afbeelding wordt weergegeven.

🔝 Ldp	_		×
Connection Browse View Options Utilities Help			
Connect			
Bind Ctrl+B			
Disconnect			
New Ctrl+N			
Save As			
Evit			
		NUM	

3. Specificeer localhost voor de server en de juiste poort en klik vervolgens op OK.

Connect		×
<u>S</u> erver:	localhost	
Port:	389	Connectionless
<u>0</u> K		<u>C</u> ancel

4. De rechterkolom geeft de tekst weer die een goede verbinding aangeeft. Klik op **Connection > Bind...** zoals in de afbeelding wordt weergegeven.

🔝 Idap://w	/in2016.ex	ample.co	om/DC	= example, DC	=com		_		$\times$
Connection	Browse	View	Optio	ns Utilities	Help				
Conne Bind Discon New Save Save A Exit	ct nect	Ctrl+B		Id = Idap_op Established Retrieving b Getting 1 en Dn: (RootD configu CN= current Tim defaultM dnsHos domainf dsServi Set Firs Nan con forestFo highest( isGlobal isSynch	en ("localho connection ase DSA in tries: SE) rationNamin =Configurati Time: 5/1/20 e; VamingConte tName: win ControllerFu Functionality iceName: CP tings,CN=W st-Site- me,CN=Sites n; unctionality: CommittedU ICatalogRea pronized: TF viceName: C	st", 389); <u>to localhost.</u> formation gContext: ion,DC=examp 20 4:16:55 PM ext: DC=exam 2016.example inctionality: 7 = /: 7 = ( WIN201 N=NTDS IN2016,CN=Se s,CN=Configur : 7 = ( WIN2010 SN: 13410; idy: TRUE; RUE; example.com:	le,DC=c 1 Easter ple,DC=c .com; = ( WIN2 16 ); ervers,C ation,DC 6 ); win2016	om; n Daylight com; 016 ); N=Default- 2=example,	DC=

5. Selecteer **Eenvoudig** Bind, en specificeer vervolgens de naam en het wachtwoord van de directory-account. Klik op **OK**.

Bind	×
<u>U</u> ser:	ftd.admin@example.com
<u>P</u> assword: Domain:	•••••
Bind type Bind as <u>c</u> u Bind with o Simple bind Advanced	rrently logged on user redentials (DIGEST) affic after bind Cancel OK

Met een succesvolle bind, zal ldp verklaard als gebruikersnaam DOMAIN\tonen.

🔐 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	840.11355 840.11355 840.11355 edLDAPPol PercentDir ReceiveBu Connection BatchRetu DirSyncDu ResultSets ResultSets ResultSets ValRange; edLDAPVe edSASLMe EGO; EXTE	6.1.4.2255; 6.1.4.2256; 6.1.4.2309; icies (20): Ma SyncReques offer; InitRecons; MaxConn rnMessages iration; MaxT Size; MinReso PerConn; Ma MaxValRang /Limit; Syster rsion (2): 3; echanisms (4 ERNAL; DIGE _s(Id, 'ftd.ad	axPooIThr sts; MaxDa vTimeout; IdleTime; I ; MaxQue empTable ultSets; axNotificat geTransiti mMemoryL 2; ): GSSAP ST-MD5; min@exan min'.	eads; atagramR MaxPage: ryDuratio Size; tionPerCo ve; .imitPerce I; GSS-	ecv; Size; n; nn; ent;	~
Ready										

Als u probeert een bestand te binden met een ongeldige gebruikersnaam of een ongeldig wachtwoord, dan levert dit een fout op.

Idap://win2016.example.com/DC=example,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 kan geen gebruikersnaam vinden

```
[-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
```

Potentiële oplossing: Controleer dat AD de gebruiker kan vinden met de zoekopdracht die door de FTD wordt uitgevoerd. Dit kan ook met ldp.exe worden gedaan.

1. Nadat u met succes hebt binden, navigeer dan naar **Beeld > Boom** zoals in de afbeelding.

Idap://win2016.example.com/DC=example,DC=com								· [		×
Connection	Browse	View	/ Option	s Utilities	Help					
		~	Tree Enterprise Status Ba Set Font	e Configurat r	ion	Ctrl+T	AaxPoo sts; Ma svTime nktleTin s; Max	v; re;		
				s; MaxQueryDuratio MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerCo MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPerce supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;						
 res = Idap_simple_bind_s(Id, 'ftd.admin@example.com', <unavailable>); // v.3 Authenticated as: 'EXAMPLE\ftd.admin'. </unavailable>								.com',	~	

2. Specificeer de Base DN die op de FTD is geconfigureerd en klik vervolgens op **OK**.

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

3. Klik met de rechtermuisknop op de Base DN en klik vervolgens op Zoeken zoals in de afbeelding.

🔝 Idap://win2016.examp	– 🗆 ×	<		
Connection Browse V	iew Options Utilities	Help		
DC=example,DC=com	Search Virtual List View Delete Modify Modify DN Add child Compare Advanced Copy DN Copy Select all Clear output	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A > Ctrl+C Ctrl+C	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1AAED00C04FD8D5CD:C ole,DC=com; 11D1AA4B00C04FD7D83A:O s,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com; 311D1ADED00C04FD8D5CD:C e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	~
Create a new document				

4. Specificeer dezelfde basisDB-, filter- en toepassingswaarden als in de uiteinden. In dit voorbeeld:

- Base DN: dc=voorbeeld, dc=com
- Filteren: samaccountname=it.admi
- Toepassingsgebied: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 vindt 0 items vanwege het feit dat er geen gebruikersaccount is met **samaccountname=it.admi** onder Base DN dc=voorbeeld,dc=com.

Het opnieuw proberen met de juiste **samaccountname=it.admin** toont een ander resultaat. Idp vindt 1 ingang onder Base DN dc=voorbeeld, dc=com en drukt die gebruiker DNA af.

🔐 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							

#### Onjuist wachtwoord voor gebruikersnaam

```
[-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
```

Potentiële oplossing: Controleer dat het wachtwoord van de gebruiker correct is ingesteld en dat het niet is verlopen. Overeenkomstig met de Login DN heeft de FTD een verbinding tegen AD met de geloofsbrieven van de gebruiker. Dit bindt kan ook in ldp worden gedaan om te verifiëren dat de AD dezelfde gebruikersnaam en wachtwoord kan herkennen. De stappen in ldp worden in sectie **Binding vanaf ISDN en/of Wachtwoord onjuist** weergegeven. Bovendien kunnen de logbestanden van het Microsoft Server Event Viewer om een mogelijke reden worden herzien.

#### **Test AAA**

De opdracht van de testserver kan worden gebruikt om een verificatiepoging van de FTD met een specifieke gebruikersnaam en een wachtwoord te simuleren. Dit kan worden gebruikt om te testen op aansluitings- of echtheidsfouten. De opdracht is **test a-server authenticatie [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
```

#### **Packet Capture**

> show capture

Packet Captures kunnen worden gebruikt om bereikbaarheid aan de AD server te verifiëren. Als LDAP-pakketten de FTD verlaten maar er geen respons is, kan dit een routeprobleem aangeven.

Hier volgt een opname die het bidirectionele LDAP-verkeer laat zien:

```
> 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
```

```
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>
                      192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768
   3: 23:02:16.772039
<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>
   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
```

### Vastlegging Windows Server Event Viewer

Het Event Viewer logt in de AD-serverbus en geeft meer gedetailleerde informatie over waarom er een fout is opgetreden.

1. Zoeken naar en openen het evenementenvenster.

=	Best match									
ŵ	Event Viewer Desktop app									
	Settings					>				
	🖄 View ever	nt logs								
٢	ē ô	ß		2	œ	រុជ				
	event									
	ρD	e		1	2	8				

2. Vul Windows uit en klik op Beveiliging. Zoek naar een auditfout met de accountnaam van de gebruiker en controleer de foutinformatie zoals in de afbeelding.



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