

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

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram 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

Netwerkdigram 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

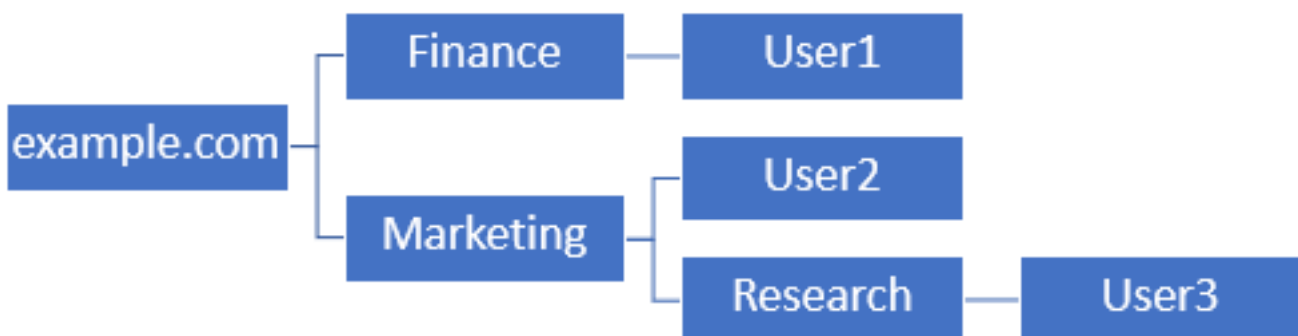
Windows-server

- 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

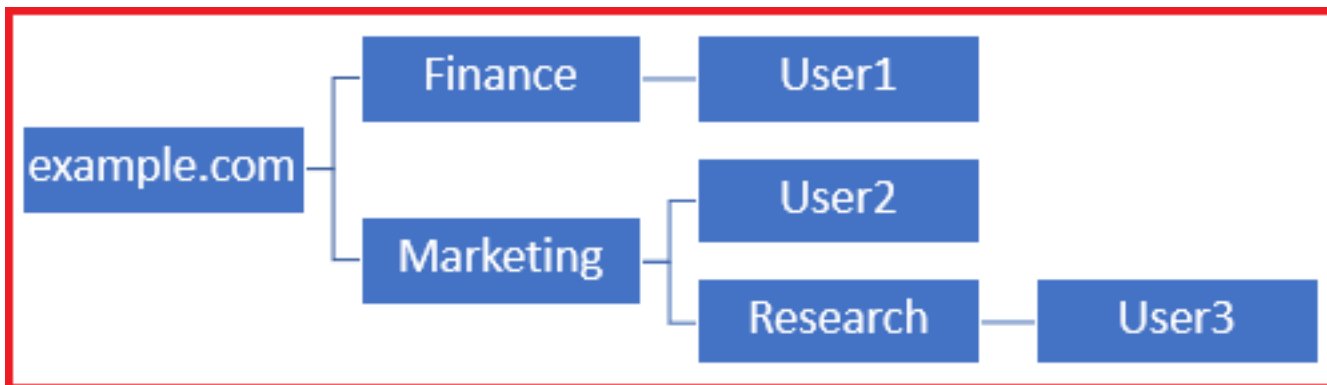
Om de AD-verificatie en de gebruikersidentiteit op de juiste wijze te kunnen configureren, zijn een aantal waarden vereist. Al deze gegevens moeten op de Microsoft Server gemaakt of verzameld worden voordat de configuratie op FDM kan worden uitgevoerd. De belangrijkste waarden zijn:

- 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:



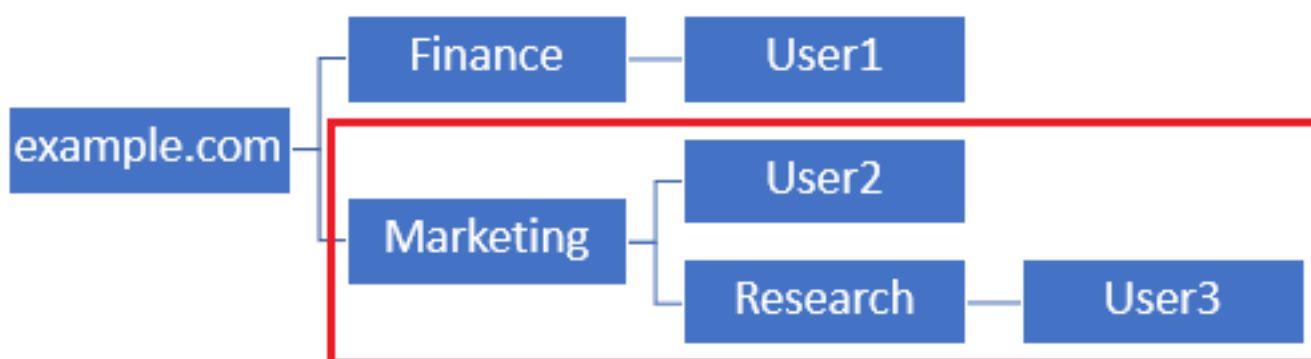
Als een beheerder wil dat gebruikers binnen de eenheid van de organisatie voor het in de handel brengen in staat zijn om de basis DN te authenticeren kan worden ingesteld op de wortel (voorbeeld.com), dan zal dit ook Gebruiker1 onder de organisatie van Financiën toestaan om ook in te loggen aangezien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

Base DN ingesteld op voorbeeld.com.



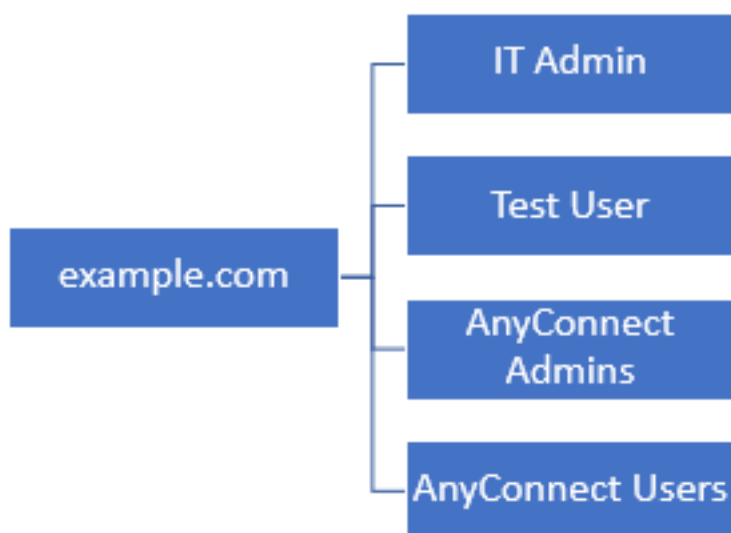
Om logins te beperken tot alleen gebruikers in de afdeling Marketingorganisatie en hieronder, kan de admin in plaats daarvan de Base DN op Marketing instellen. Alleen User2 en User3 kunnen nu voor authenticatie zorgen, omdat de zoekactie bij Marketing begint.

Base DN ingesteld op Marketing:



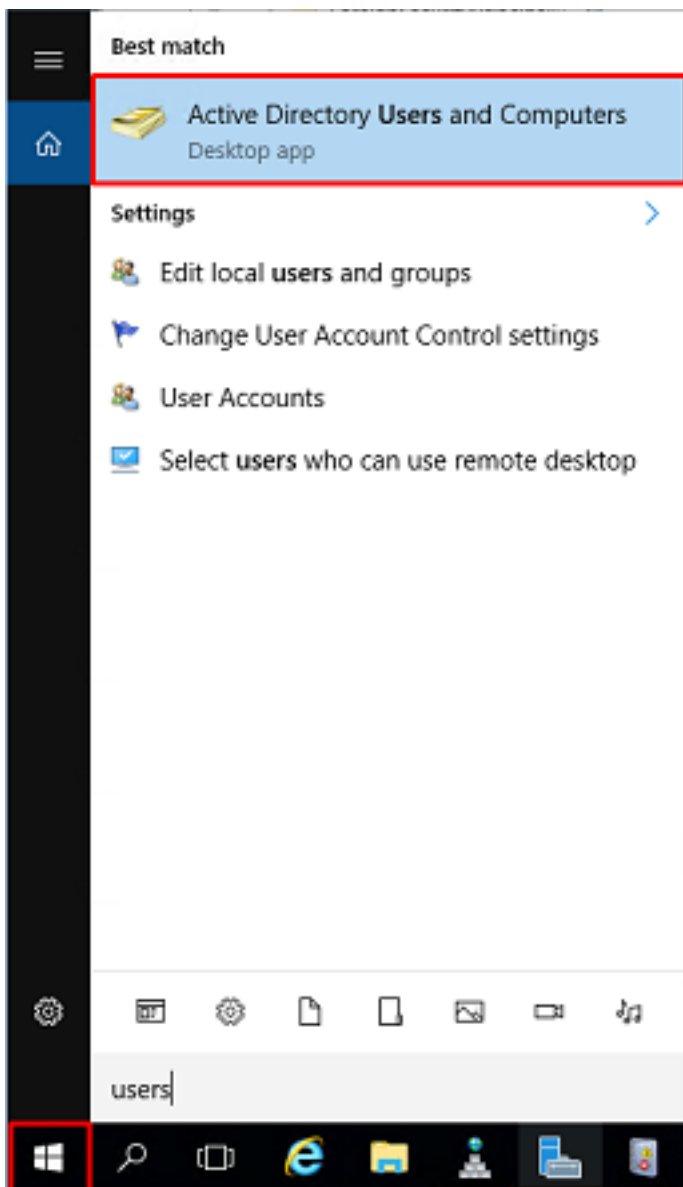
Merk op dat voor een meer gedetailleerde controle binnen de FTD waarvoor gebruikers op basis van hun AD-eigenschappen verschillende vergunningen mogen aansluiten of toewijzen, een LBP-vergunningskaart moet worden geconfigureerd.

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

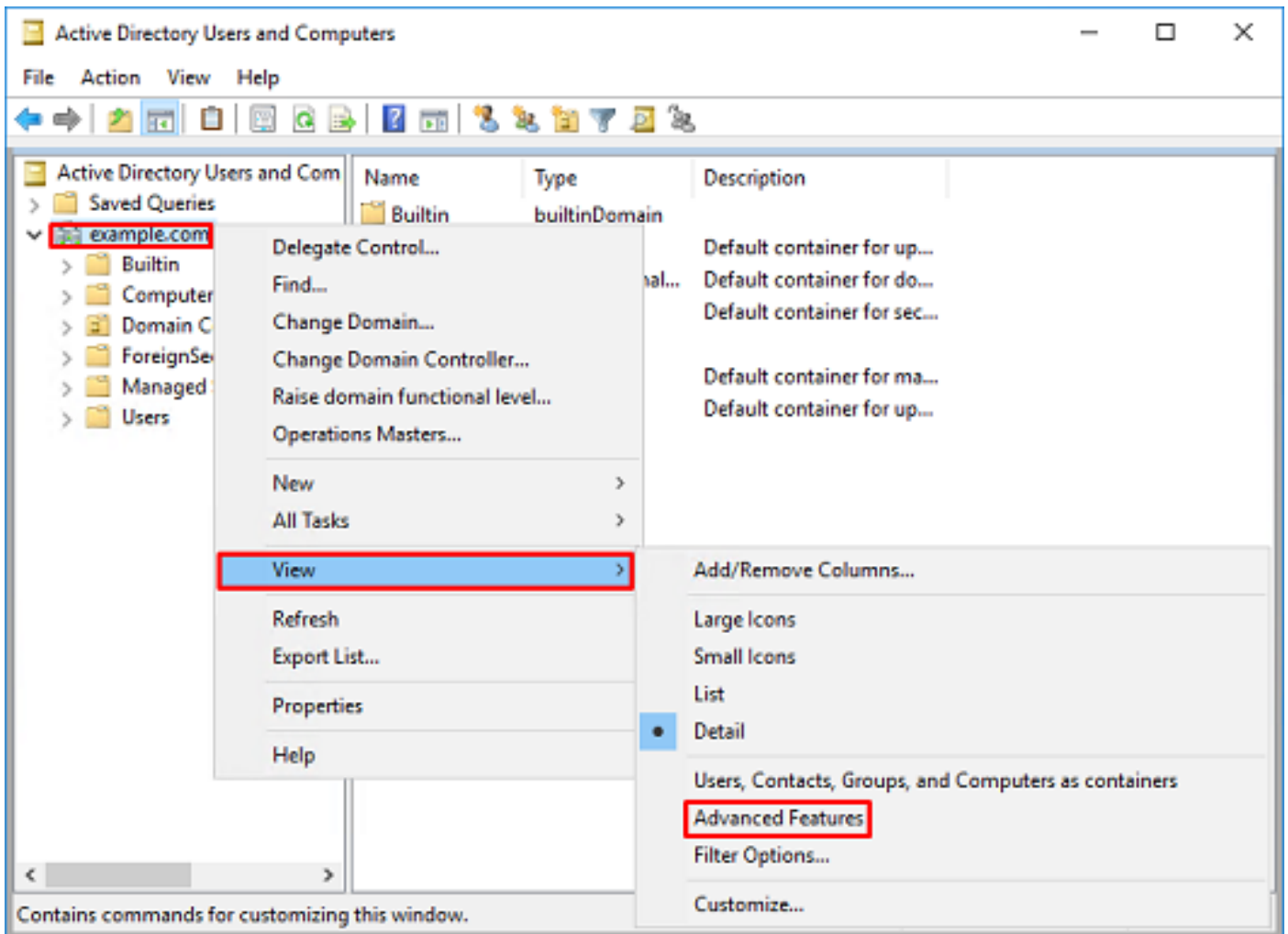


LBP-basis DN bepalen

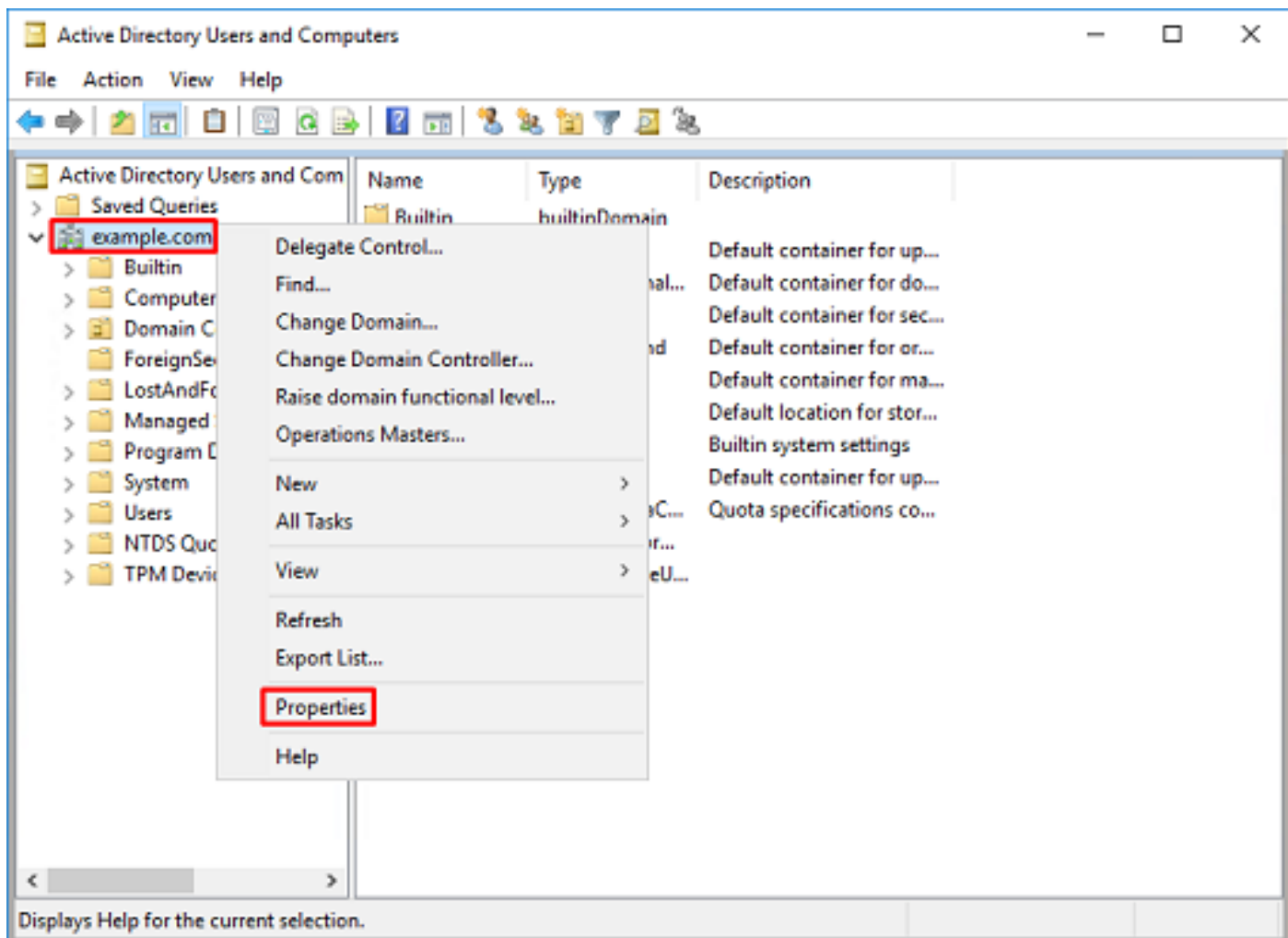
1. Open AD-gebruikers en computers.



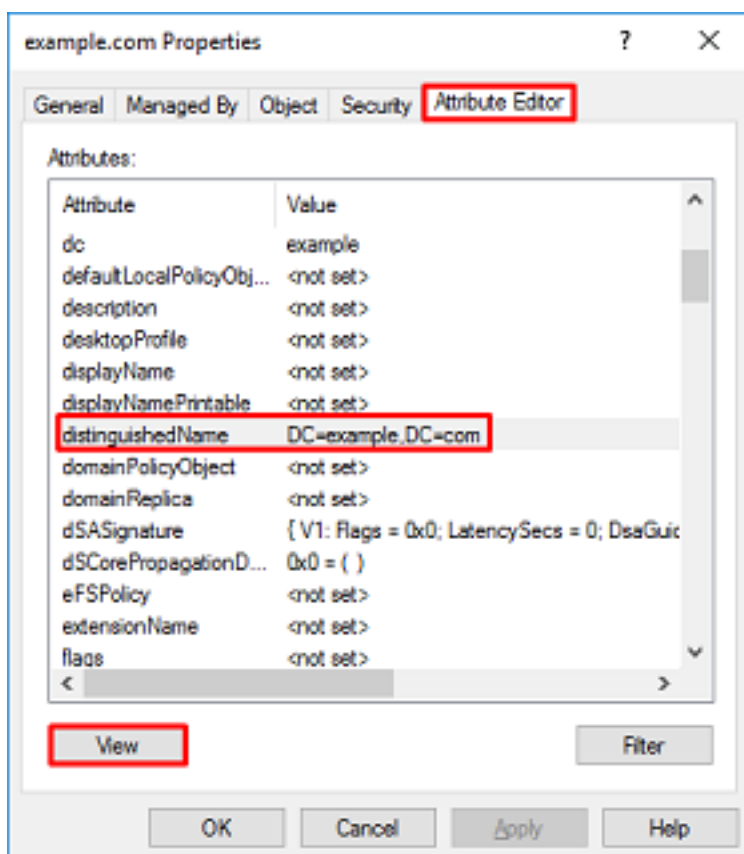
2. Klik met de rechtermuisknop op het basisdomein (om de container te openen), klik met de rechtermuisknop op het basisdomein en navigeer vervolgens naar **Weergave** en klik op **Geavanceerde functies**.



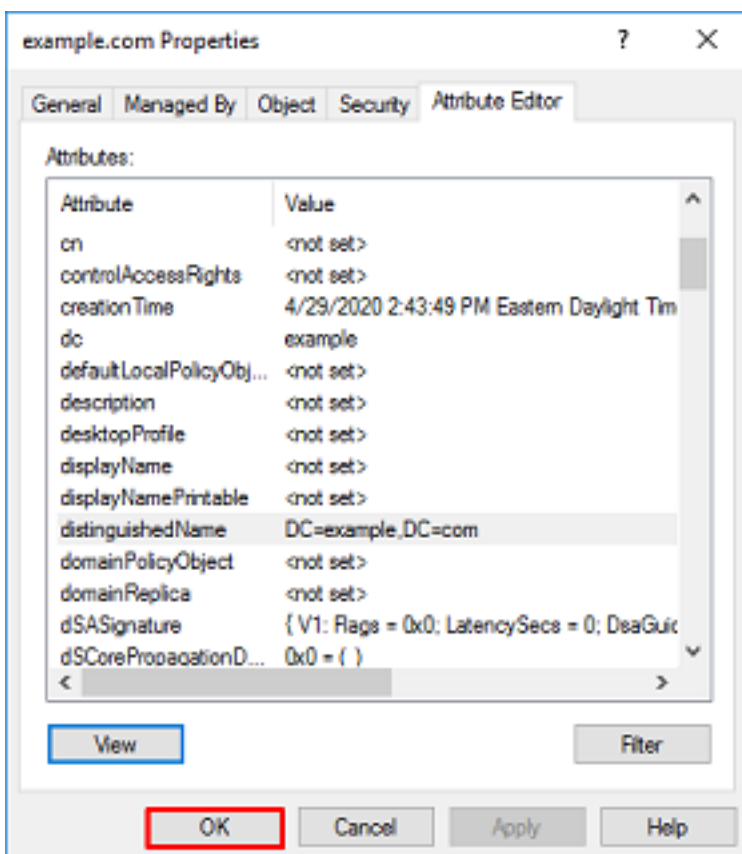
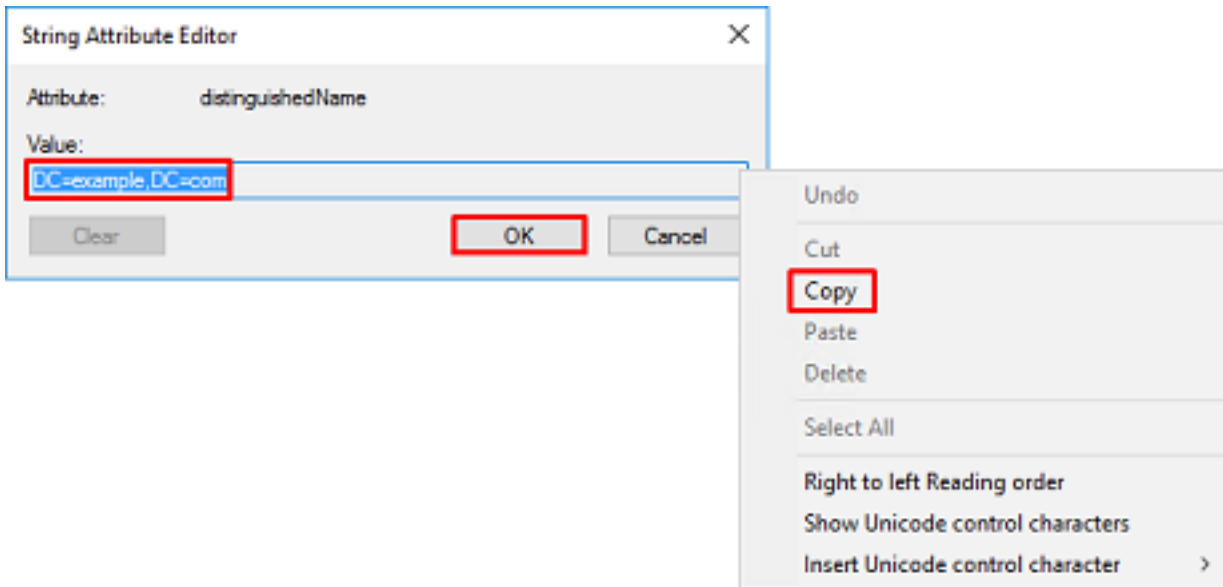
3. Hierdoor kan de weergave van extra eigenschappen onder de AD-objecten mogelijk worden. Bijvoorbeeld, om de DN voor het root voorbeeld.com te vinden, klik met de rechtermuisknop op voorbeeld.com en navigeer vervolgens naar **Properties**.



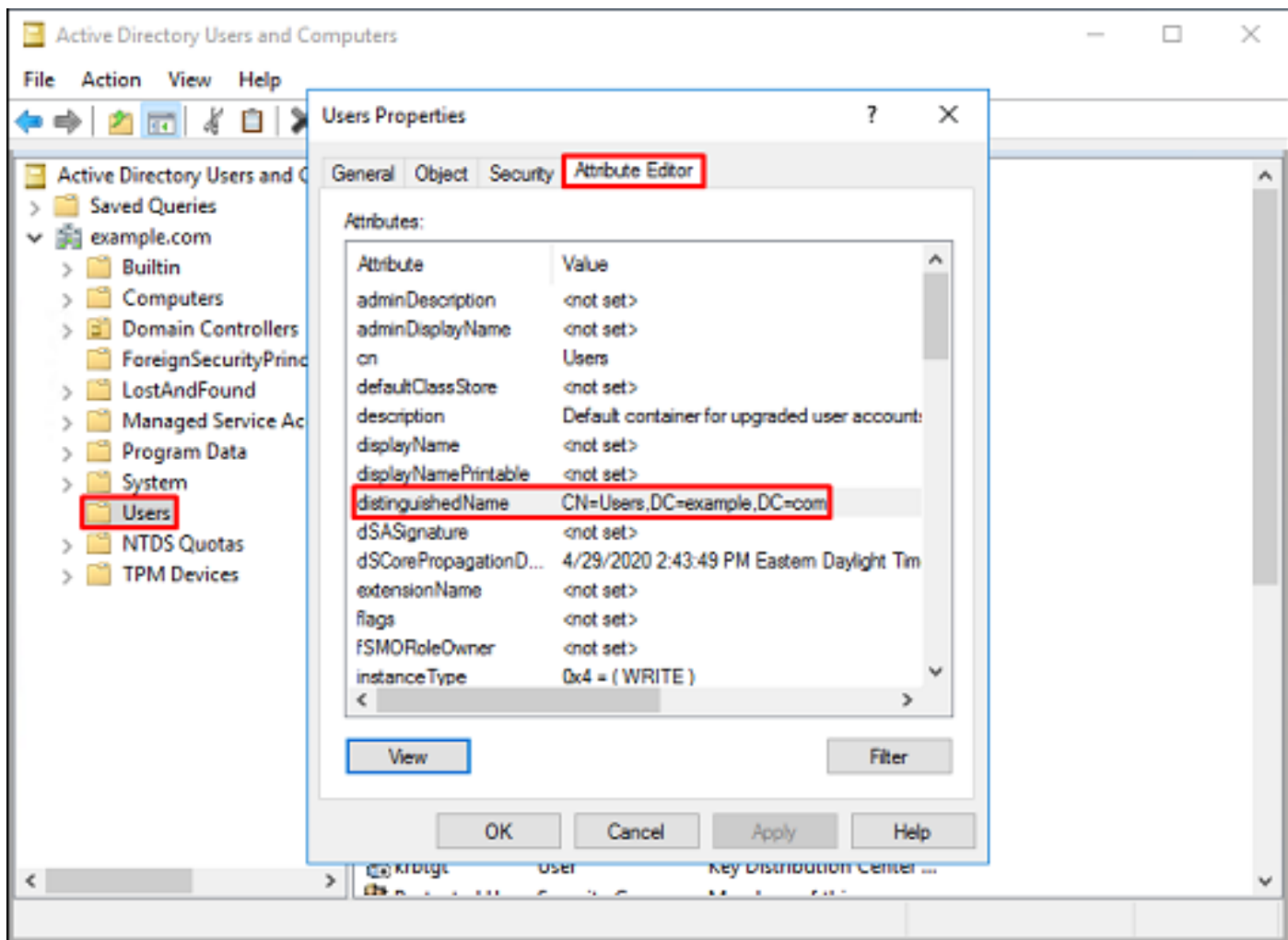
4. Klik onder **Properties** op het tabblad **Eigenschappen**. Vind **geachte naam** onder de Eigenschappen en klik vervolgens op **Weergeven**.



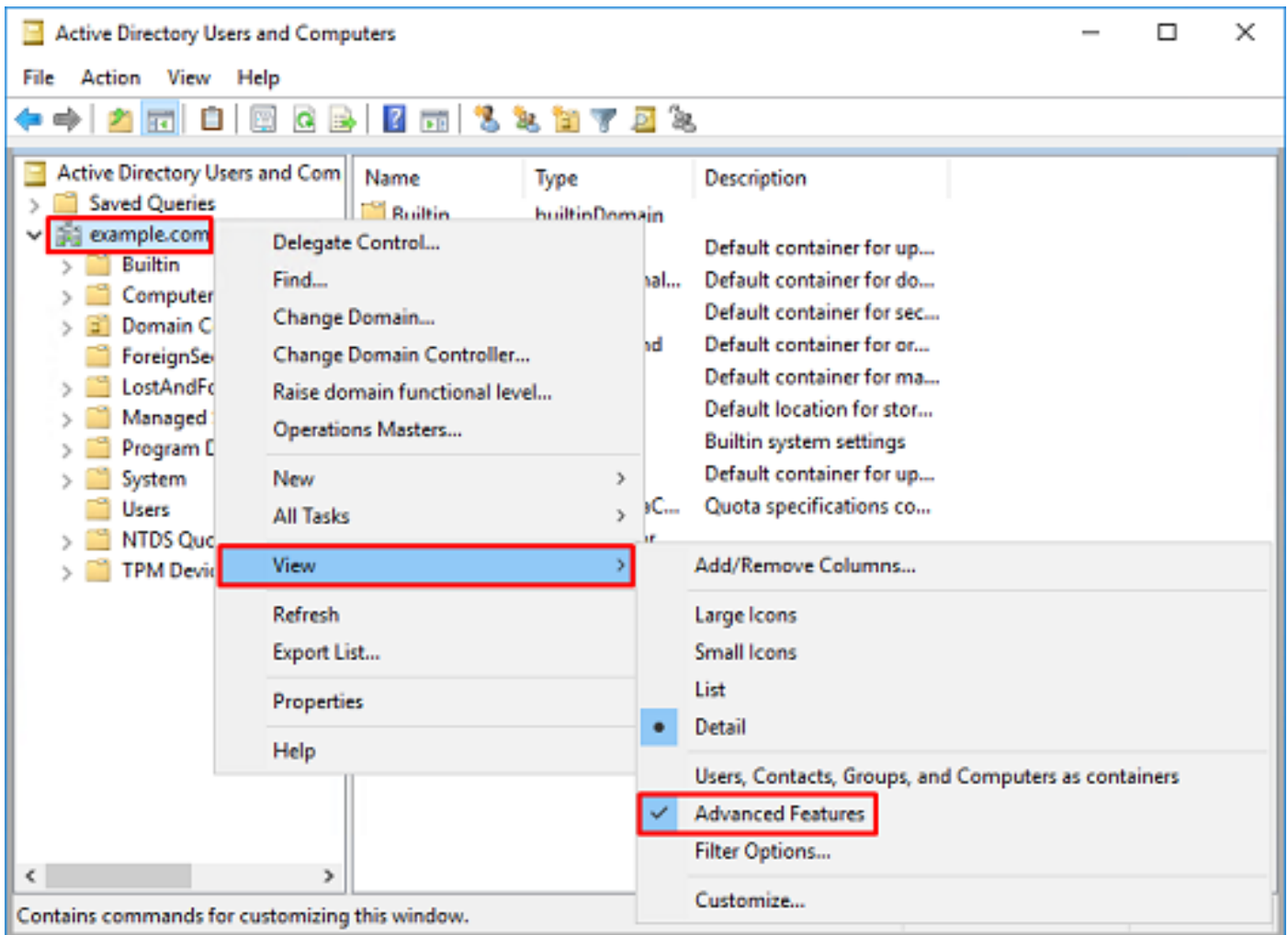
5. Dit opent een nieuw venster waarin de DN later kan worden gekopieerd en geplakt naar FDM. In dit voorbeeld is de root DN DC=voorbeeld, DC=com. Kopieert de waarde. Klik op **OK** om het venster van de editor van String-kenmerken te verlaten en klik vervolgens nogmaals op **OK** om de eigenschappen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



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 authenticeren. 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**.

New Object - User

Create in: example.com/Users

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

New Object - User

Create in: example.com/Users

When you click Finish, the following object will be created:

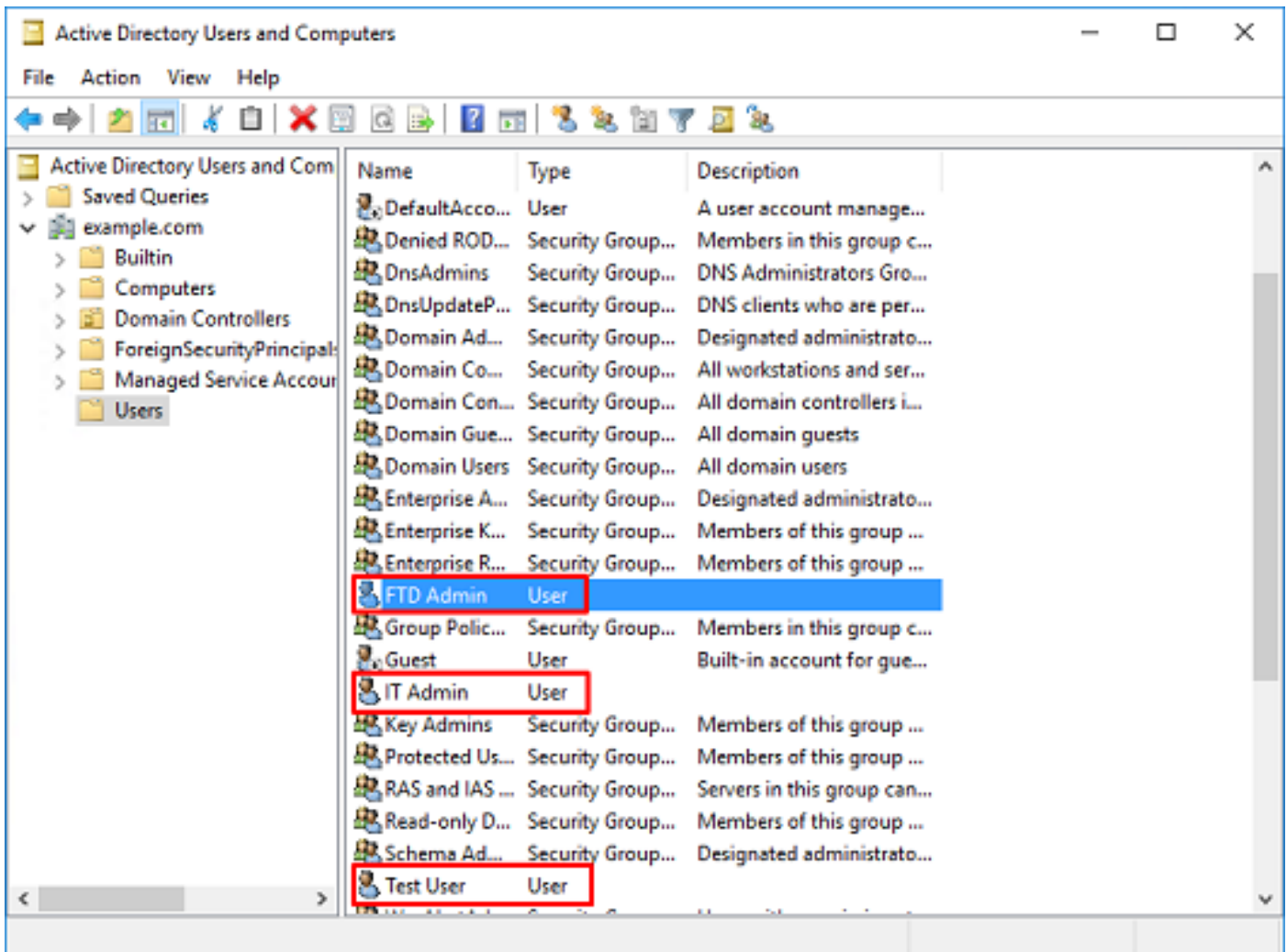
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

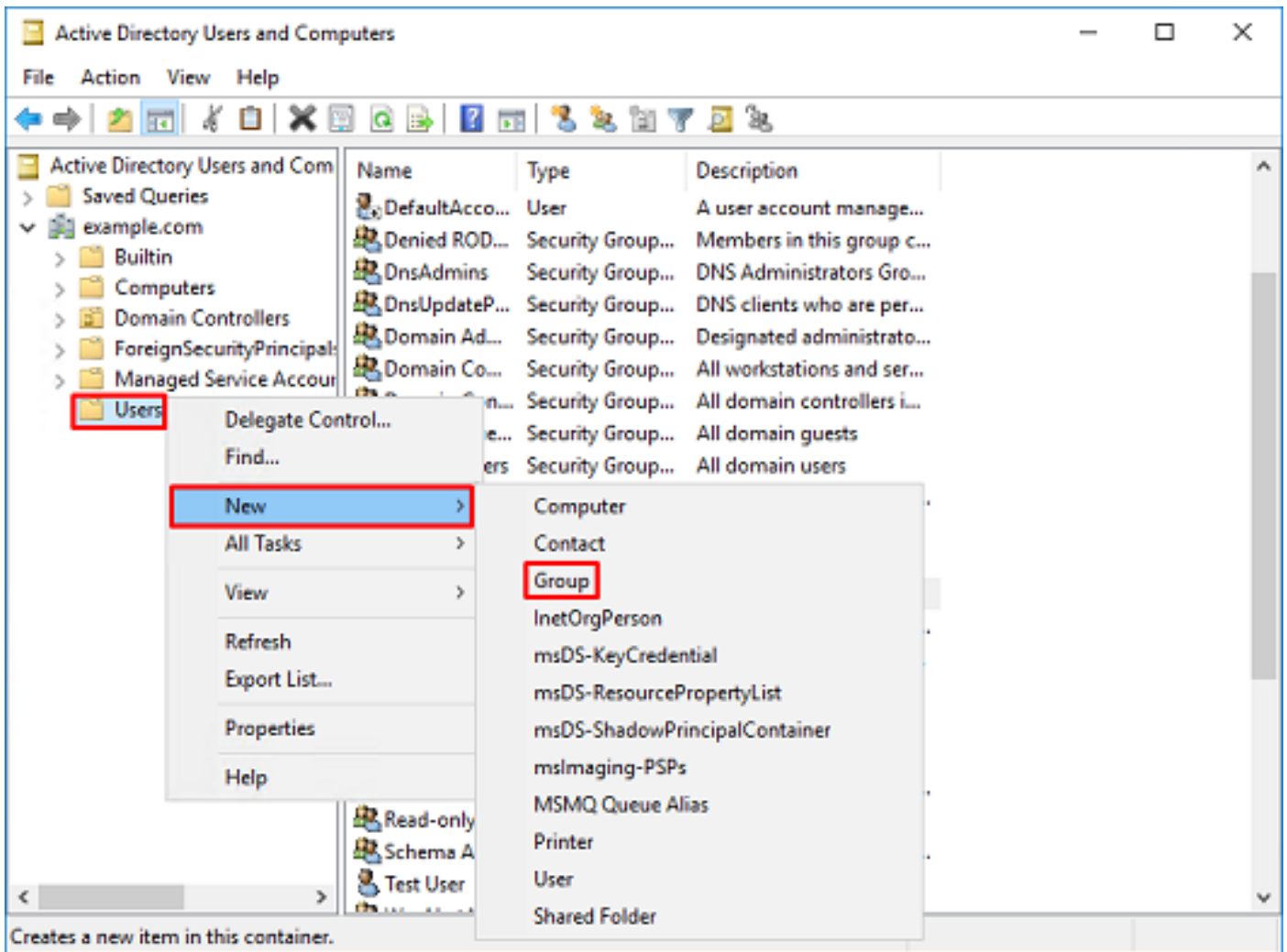
3. Controleer dat de FTD-account is aangemaakt. Daarnaast zijn er twee extra rekeningen gecreëerd, **IT Admin** en **Test User**.



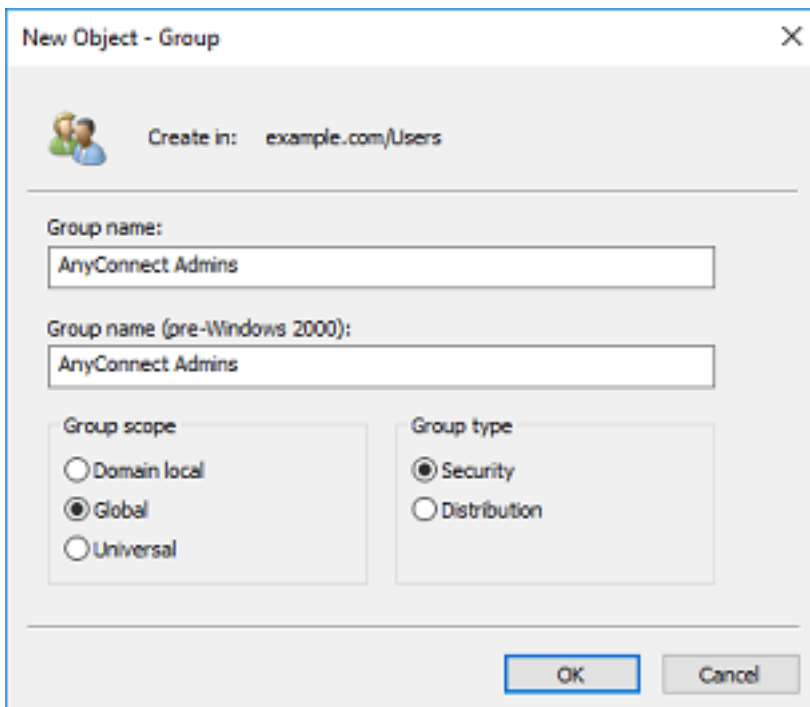
AD-groepen maken en gebruikers aan AD-groepen toevoegen (optioneel)

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.

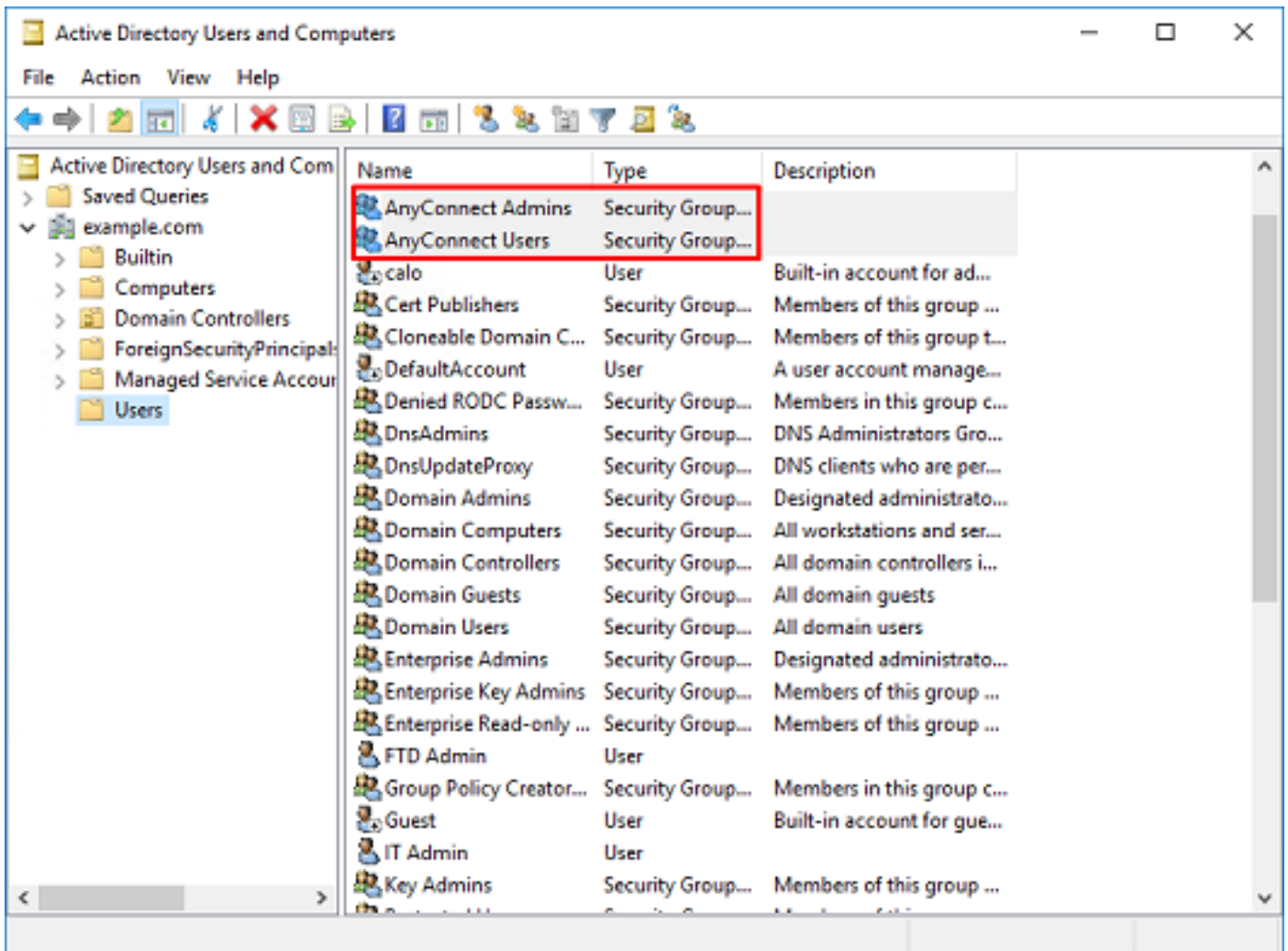
1. In **Actieve Gebruikers en Computers van de Map**, klikt u met de rechtermuisknop op de container/de organisatie waaraan de nieuwe groep wordt toegevoegd. In dit voorbeeld wordt de groep **AnyConnect Admins** toegevoegd onder de Gebruikers-tank. Klik met de rechtermuisknop op **Gebruikers**, dan op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



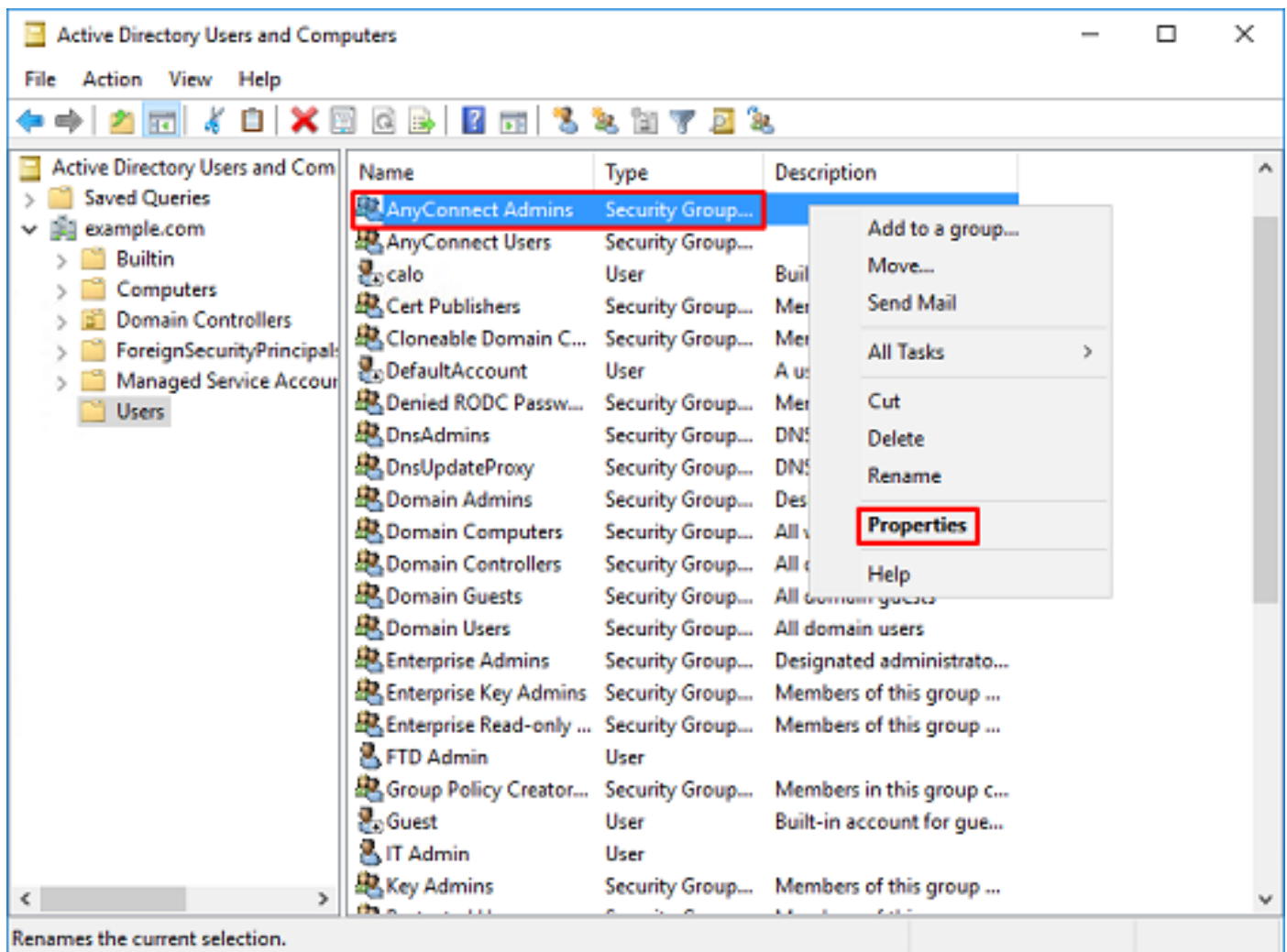
2. Navigeer door de **Nieuwe Object - Group Wizard** zoals in de afbeelding.



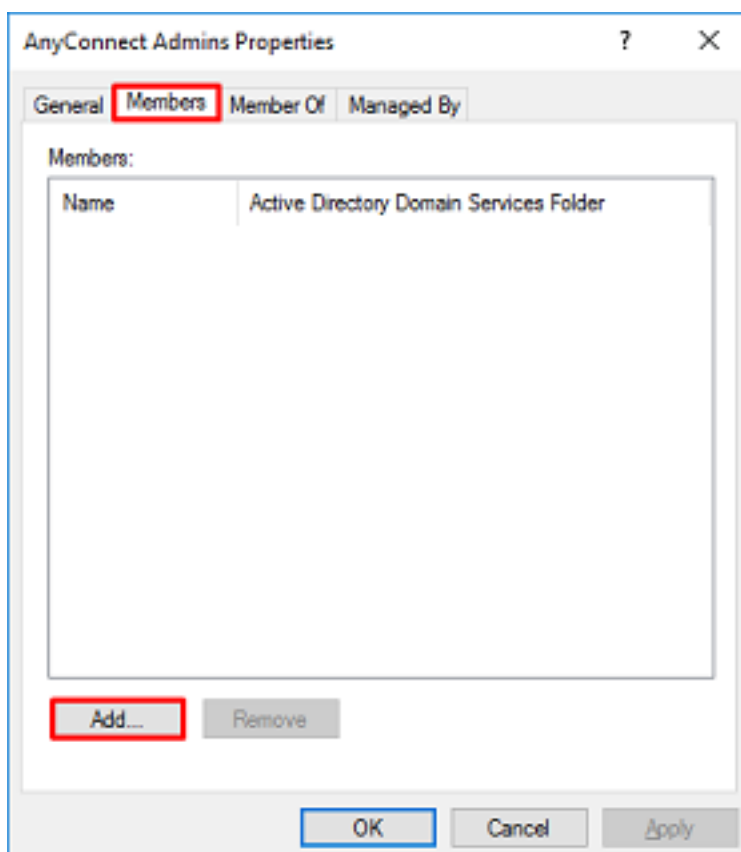
3. Controleer of de groep is aangemaakt. De **AnyConnect**-gebruikersgroep is ook opgericht.



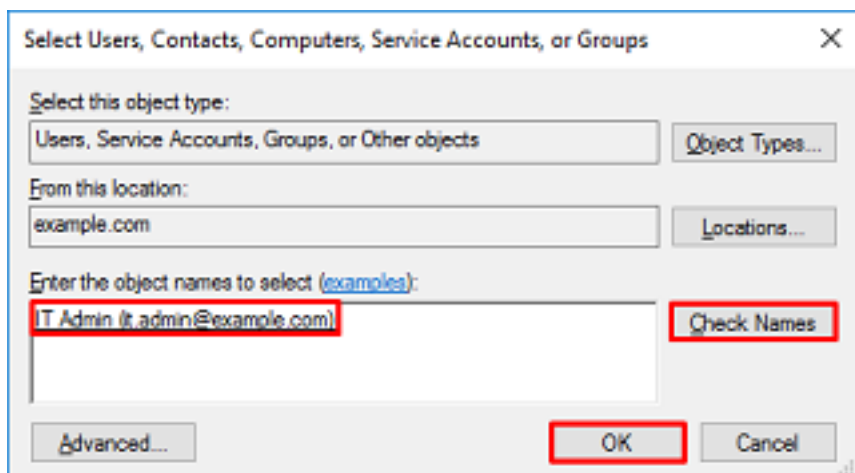
4. Klik met de rechtermuisknop op de groep waaraan de gebruiker(s) wordt toegevoegd en selecteer **Eigenschappen**. Bij deze configuratie wordt de gebruiker **IT Admin** toegevoegd aan de groep **AnyConnect Admins** en de **testgebruiker** wordt toegevoegd aan de groep **AnyConnect-gebruikers**.



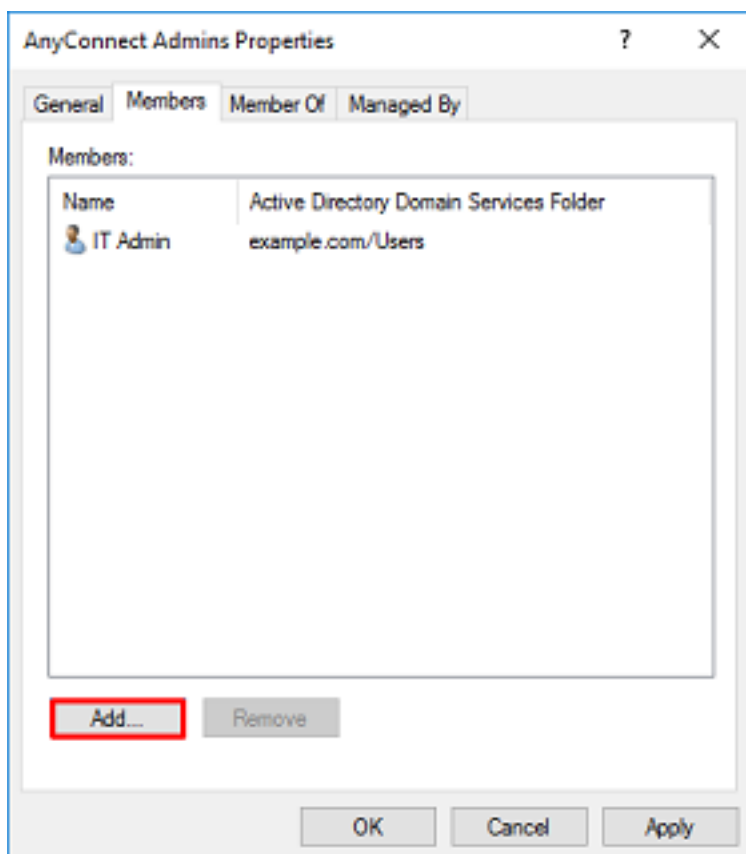
5. Klik op het tabblad **Leden** en klik vervolgens op **Toevoegen** zoals in de afbeelding.



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**.

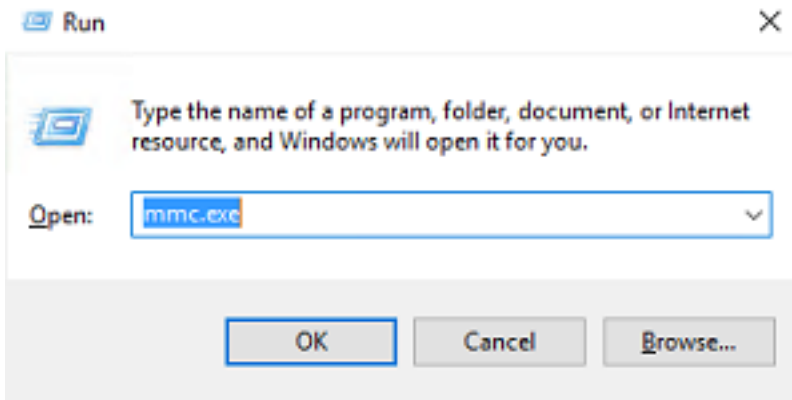


Controleer of de juiste gebruiker is toegevoegd en klik vervolgens op de knop **OK**. De gebruiker Test Gebruiker is ook toegevoegd aan groep AnyConnect-gebruikers met dezelfde stappen.

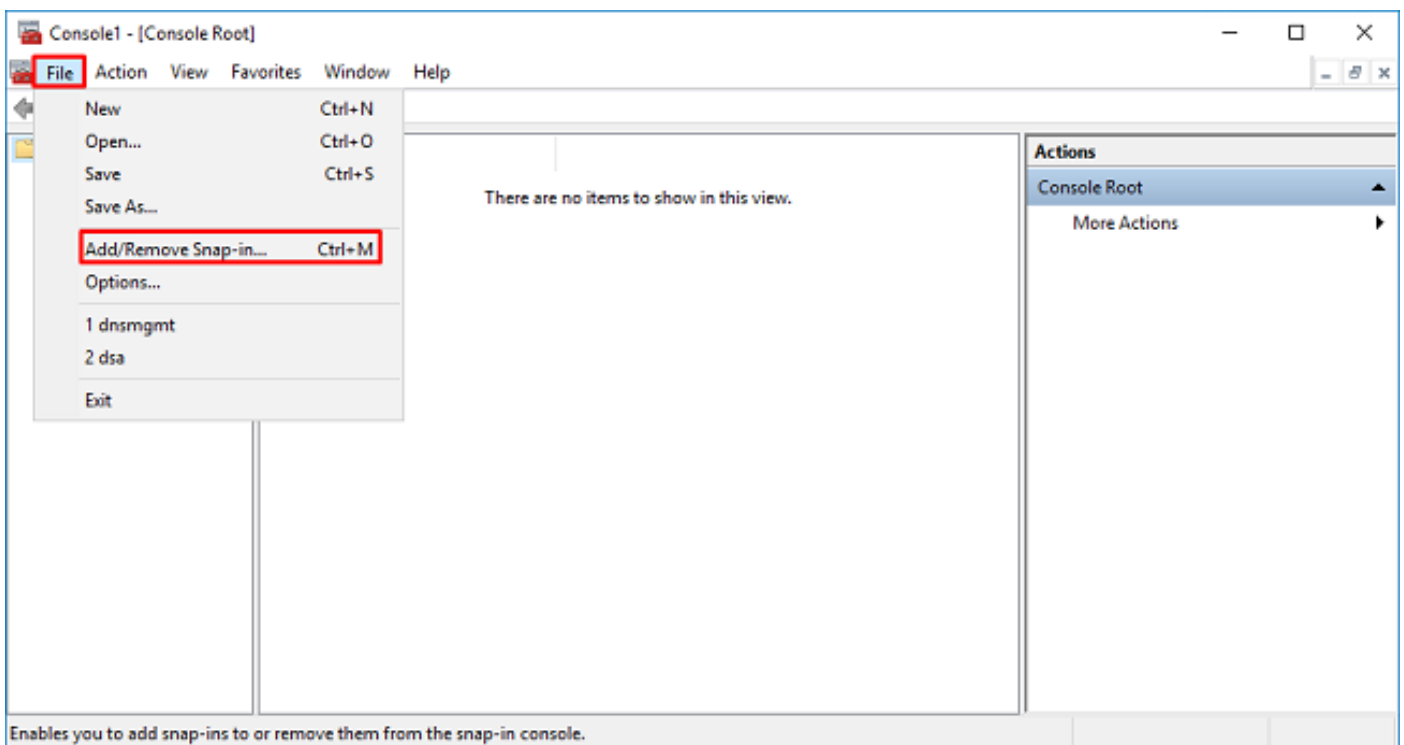


Kopieer de LDAPS SSL-certificatieroot (alleen vereist voor LDAPS of STARTTLS)

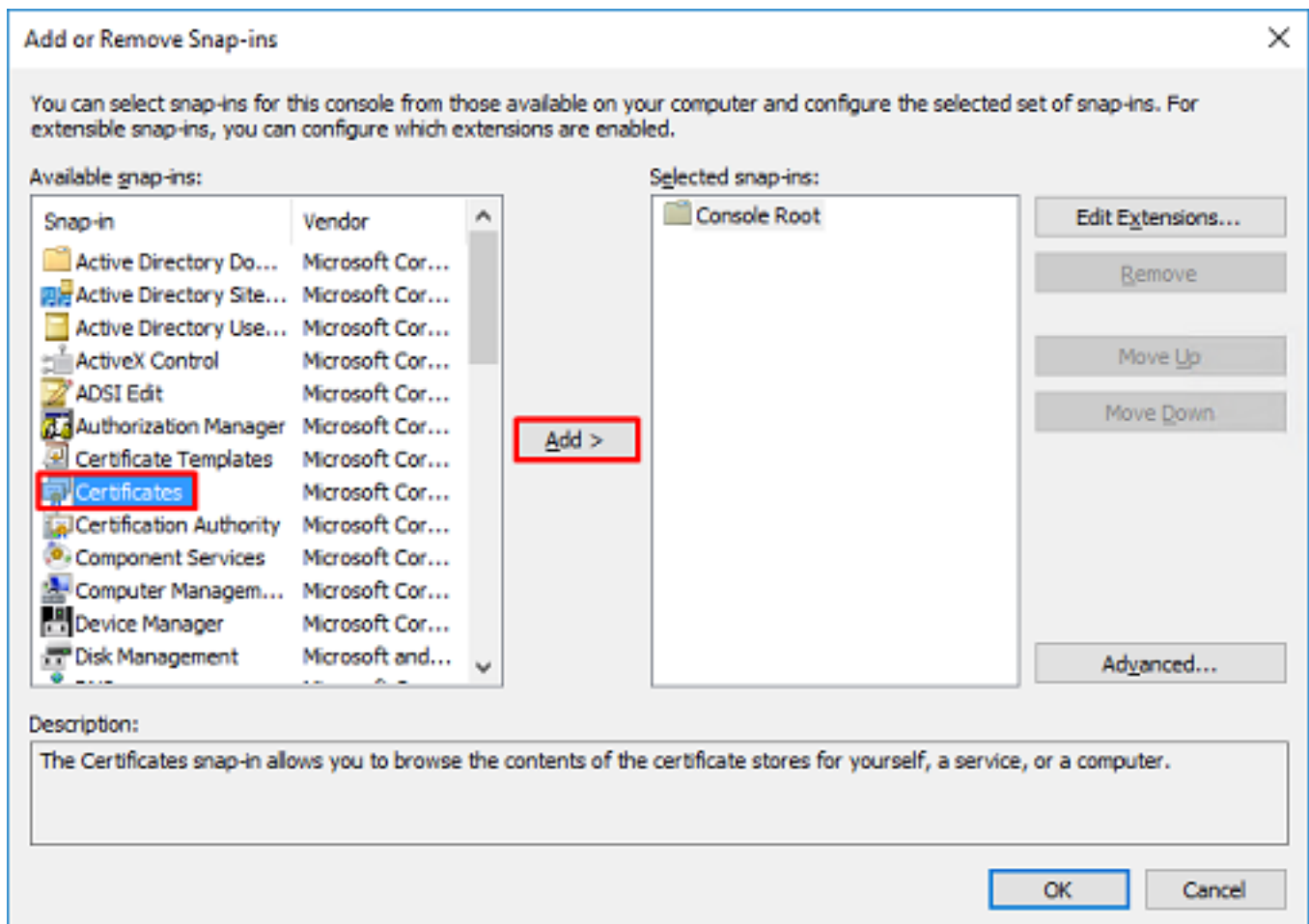
1. Druk op **Win+R** en type **mmc.exe**. Klik op **OK**.



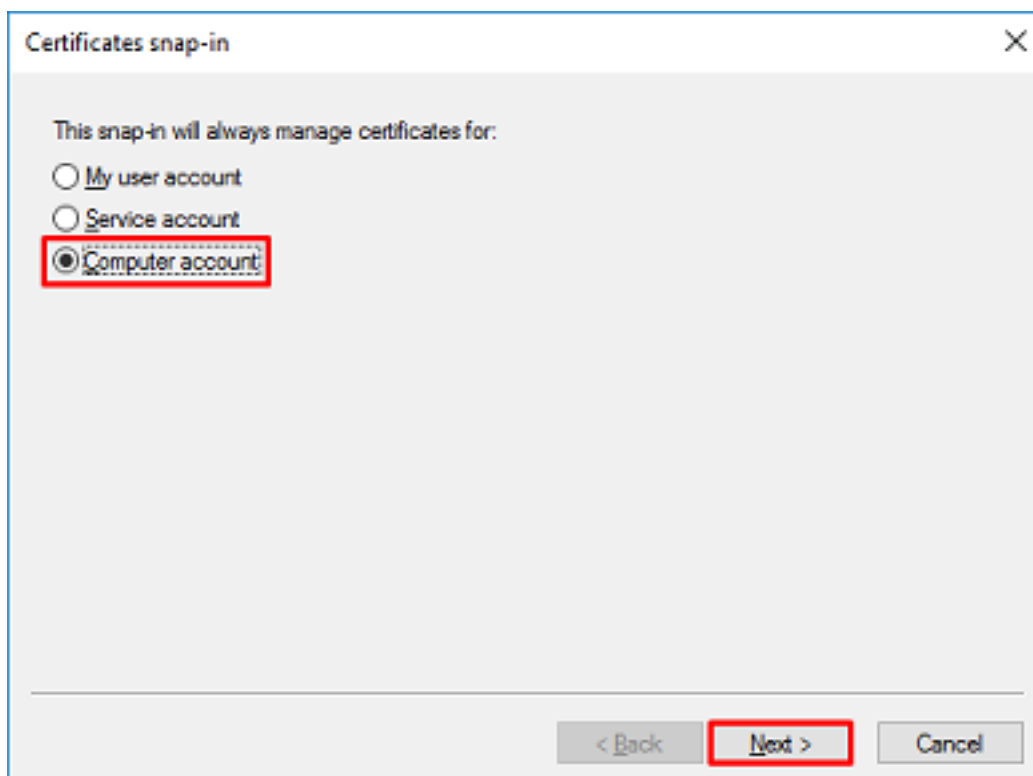
2. Navigeer naar **bestand > Magnetisch toevoegen/verwijderen...** zoals in de afbeelding wordt weergegeven.



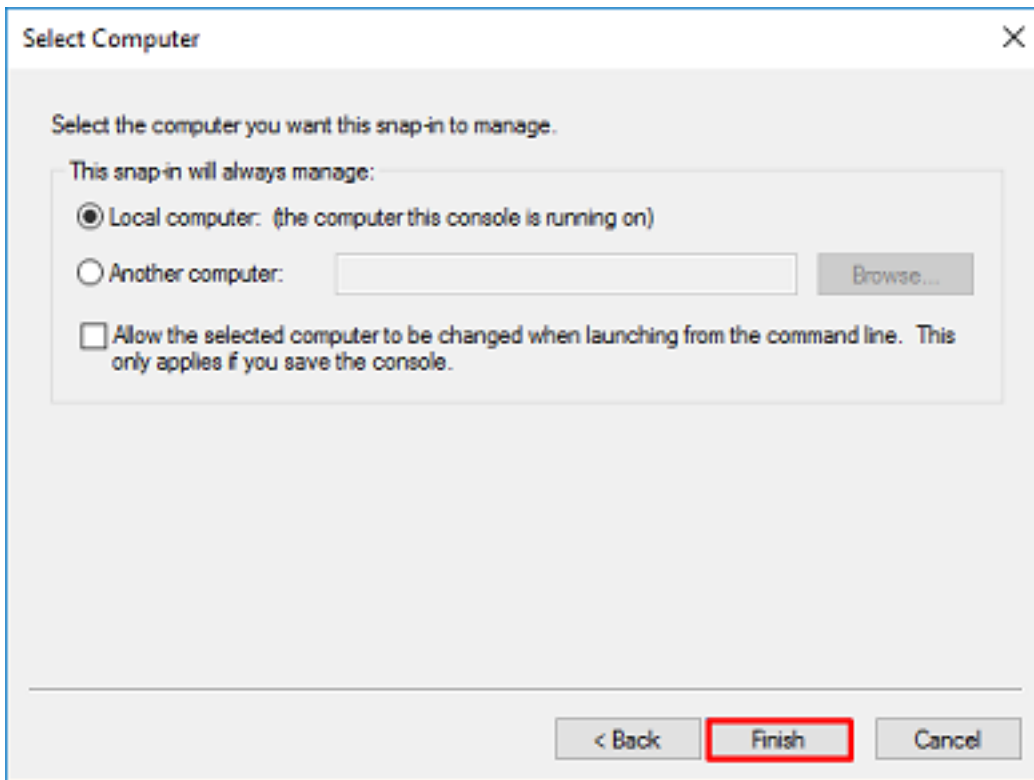
3. Klik onder beschikbare knoppen op **Certificaten** en vervolgens op **Toevoegen**.



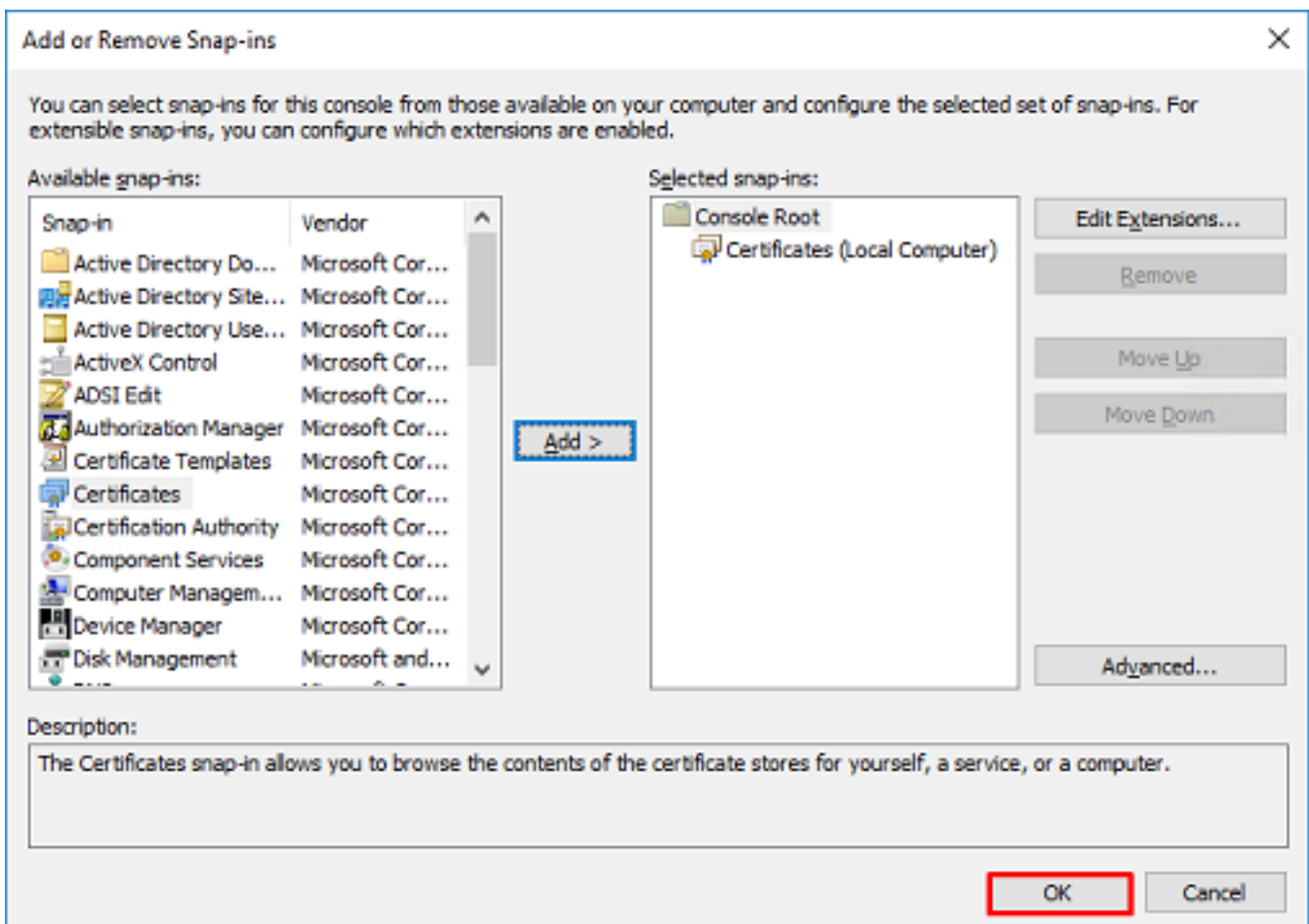
4. Selecteer **Computer-account** en klik vervolgens op **Volgende** zoals in de afbeelding.



Klik op **Voltoeien**.



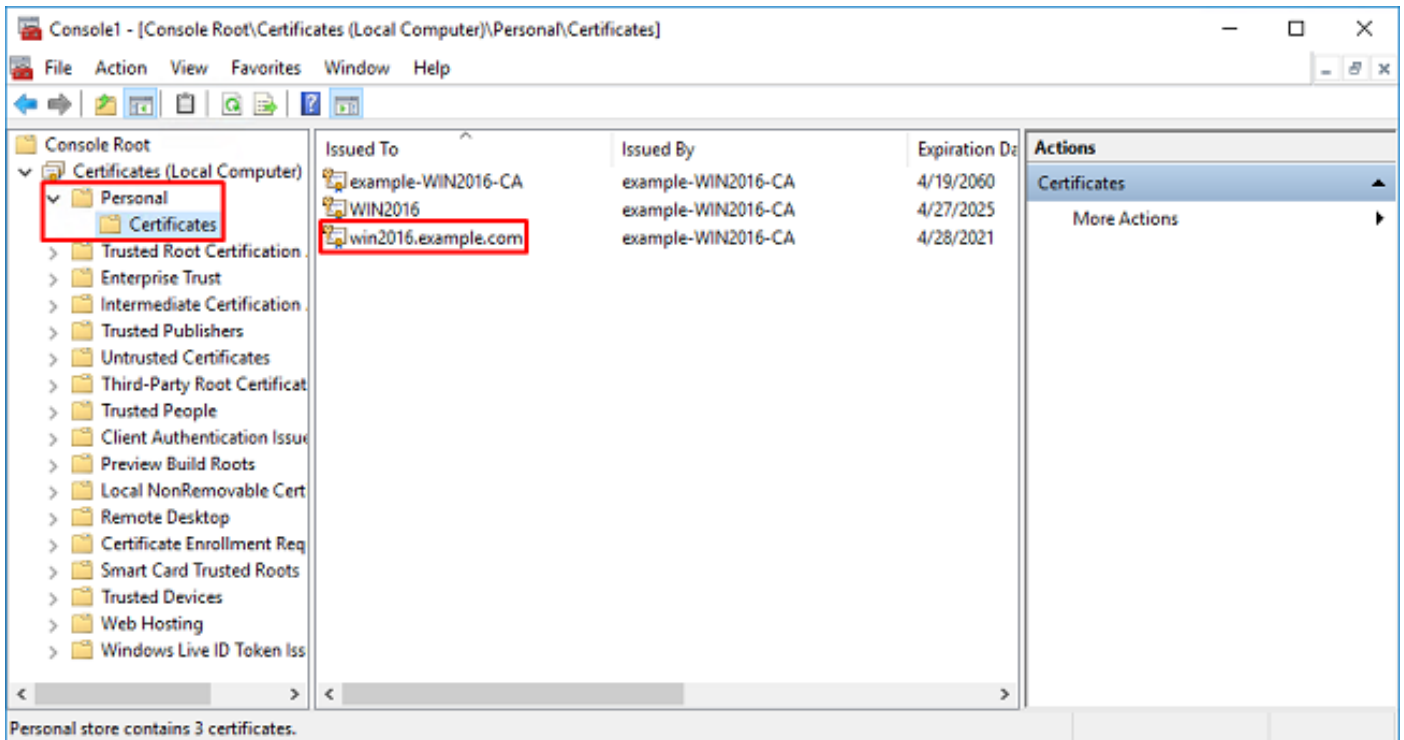
5. Klik op OK.



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.

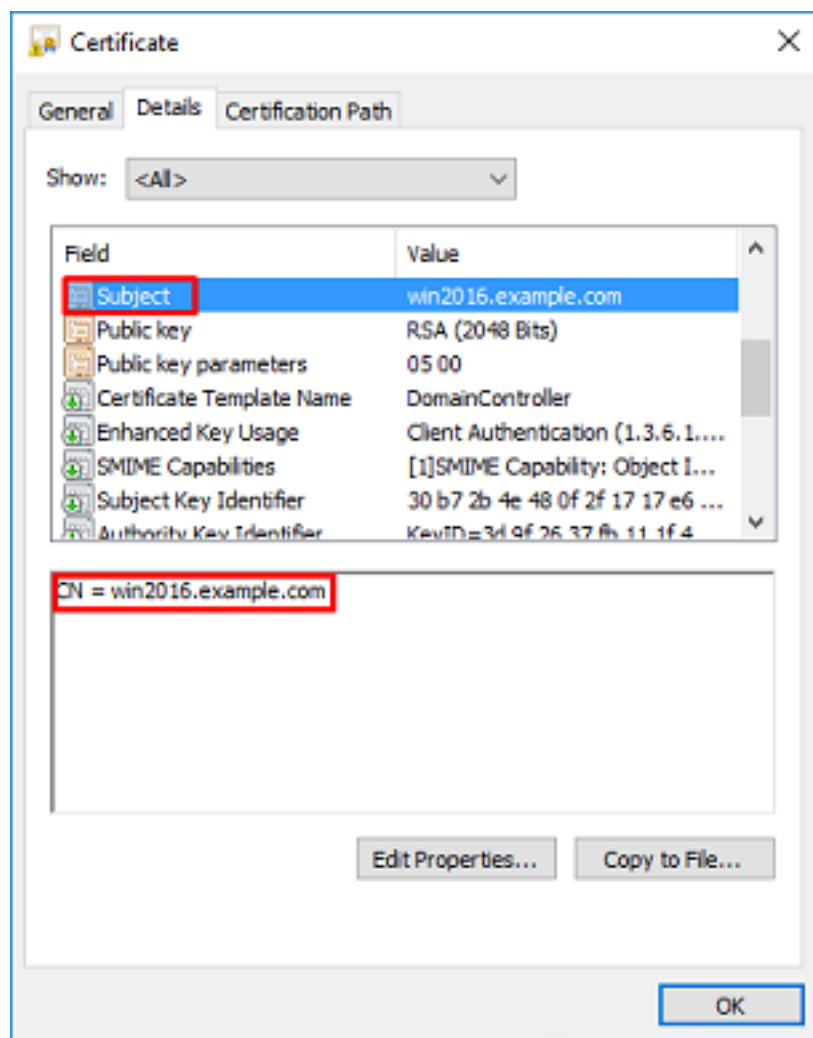
In deze configuratie gids is de FQDN win2016.voorbeeldcom en dus zijn de eerste 2 certificaten niet geldig voor gebruik als het LDAPS SSL-certificaat. Het identiteitsbewijs dat is afgegeven voor win2016.voorbeeldcom is een certificaat dat automatisch is afgegeven door de CA-service van Windows Server.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

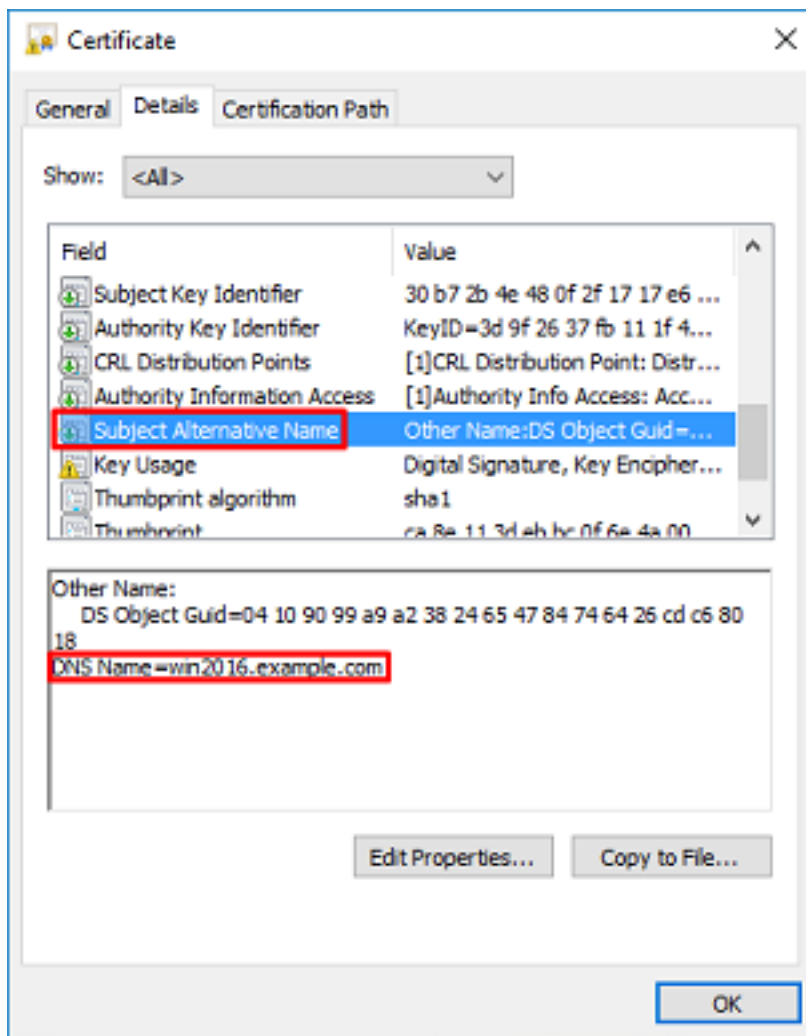


7. Het certificaat moet aan de volgende eisen voldoen om als LGO-SSL-certificaat te kunnen worden gebruikt:

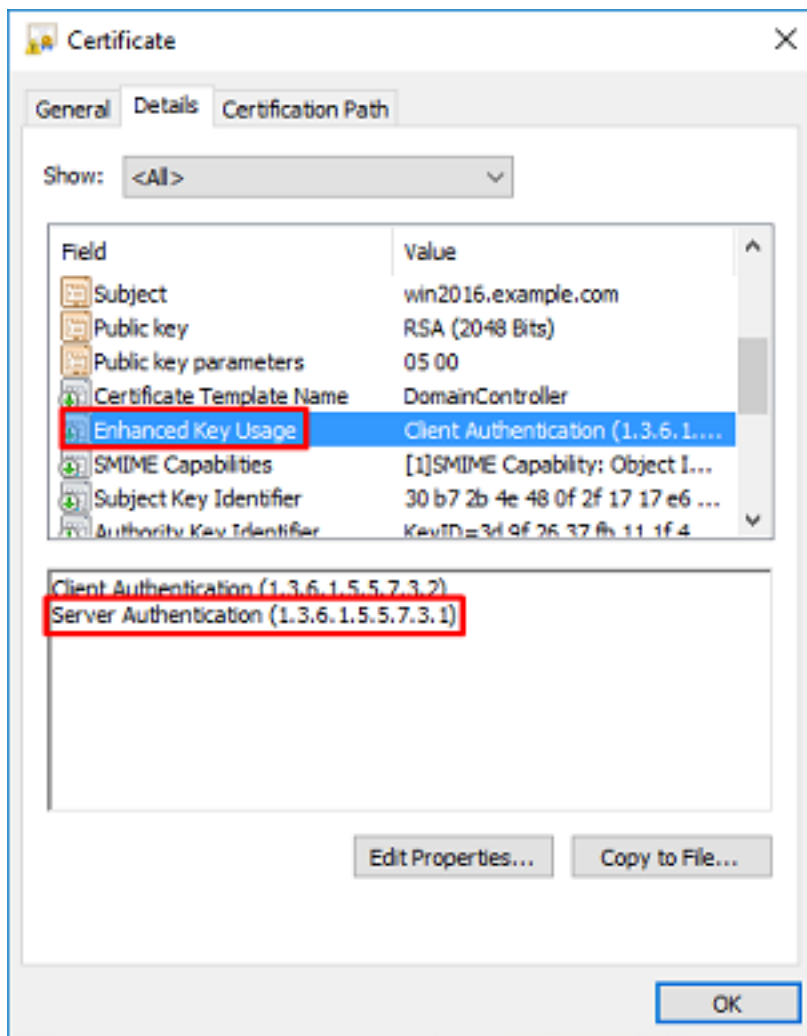
- De gezamenlijke naam of DNS Betreft Alternatieve naam komt overeen met FQDN van de Windows Server.
- Het certificaat heeft serververificatie onder het veld Uitgebreide sleutel voor gebruik.

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

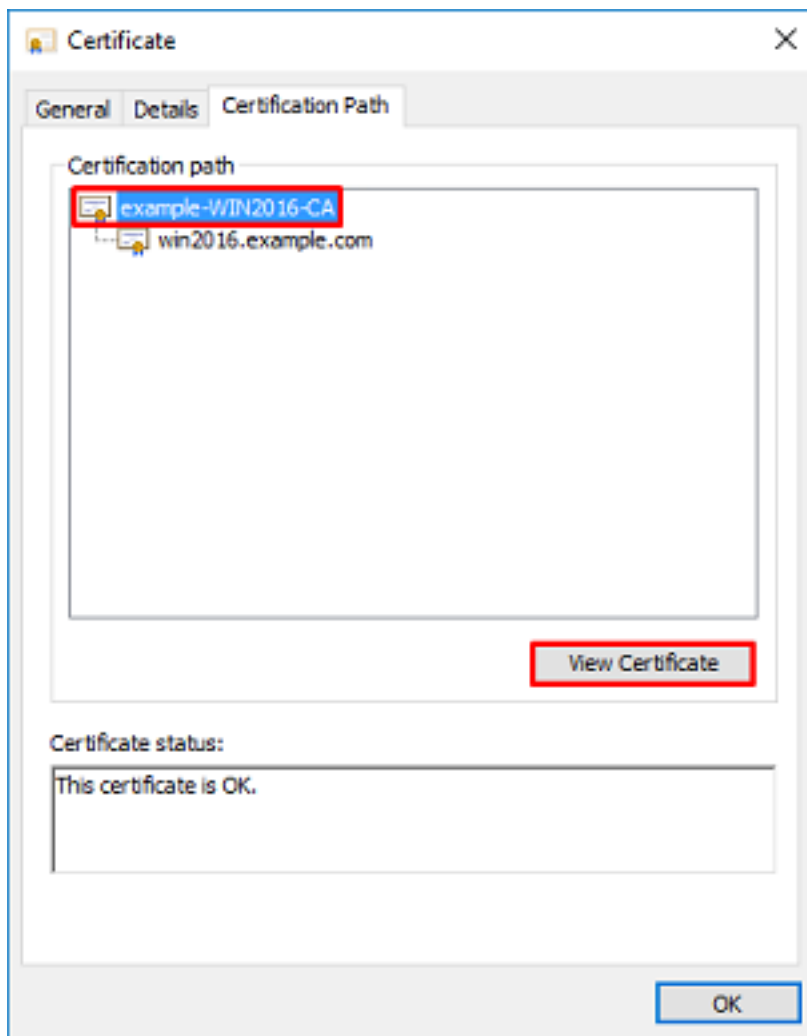




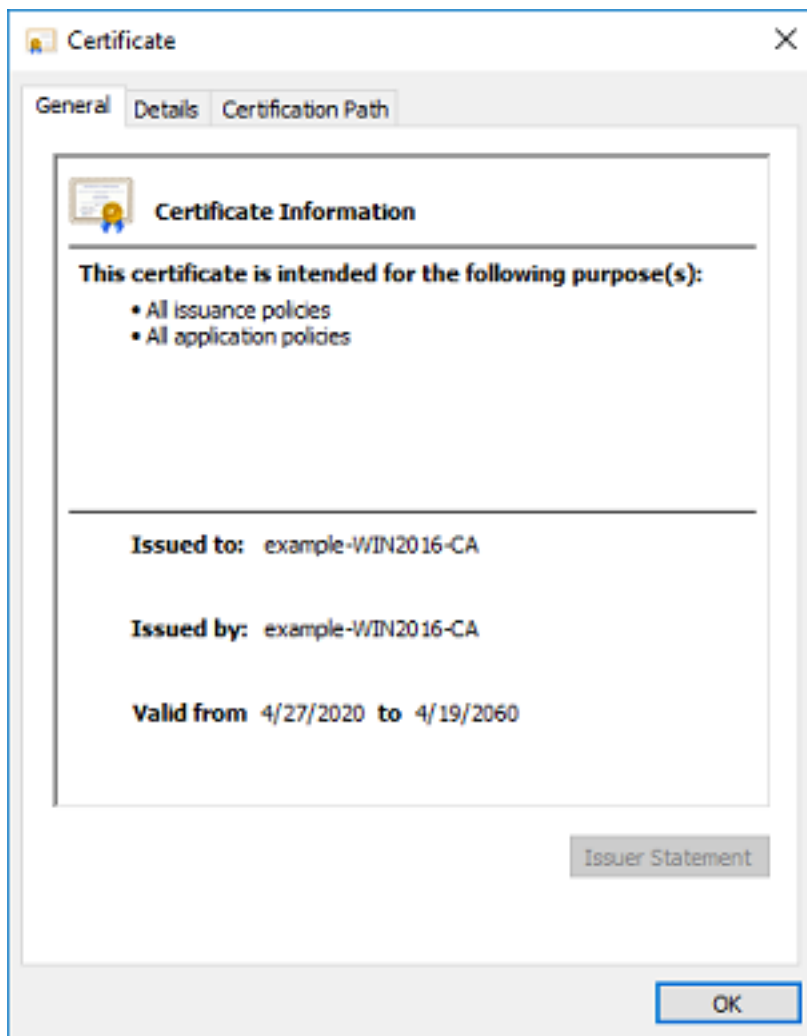
Onder **Uitgebreid gebruik**, is de serververificatie aanwezig.



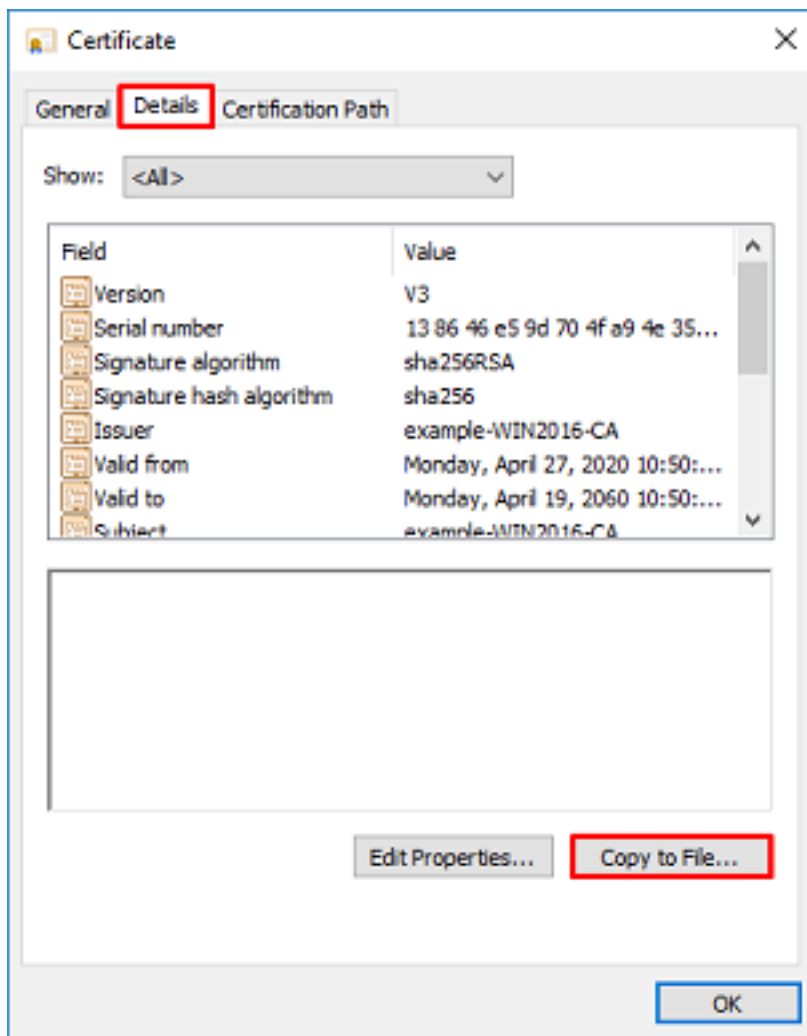
8. Als dit eenmaal is bevestigd, navigeer dan naar het tabblad **certificeringssnijpad**. Klik op het hoogste certificaat dat het basiscertificaat moet zijn, en klik vervolgens op de knop **Certificaat bekijken**.



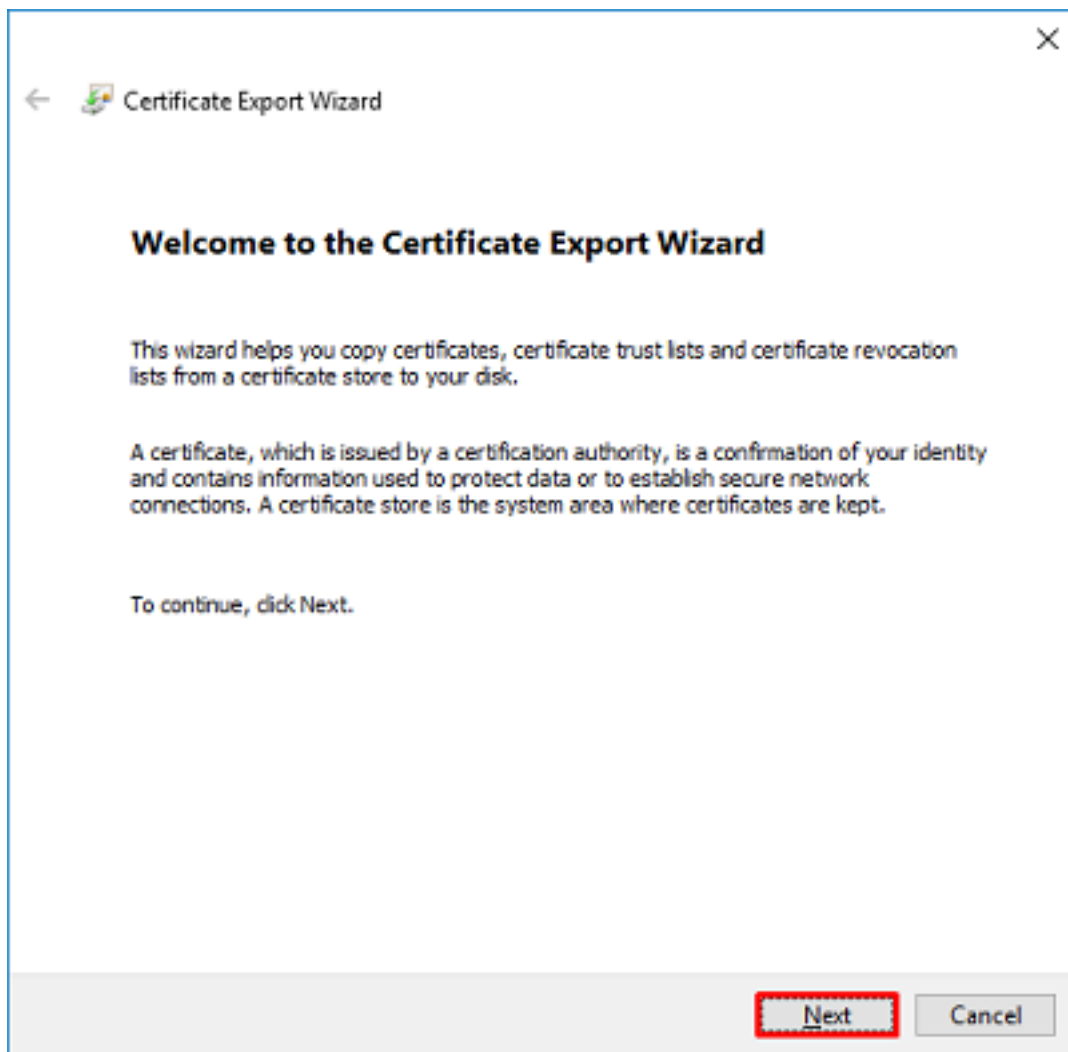
9. Hierdoor worden de certificeringsgegevens voor het basiscertificaat van CA geopend.



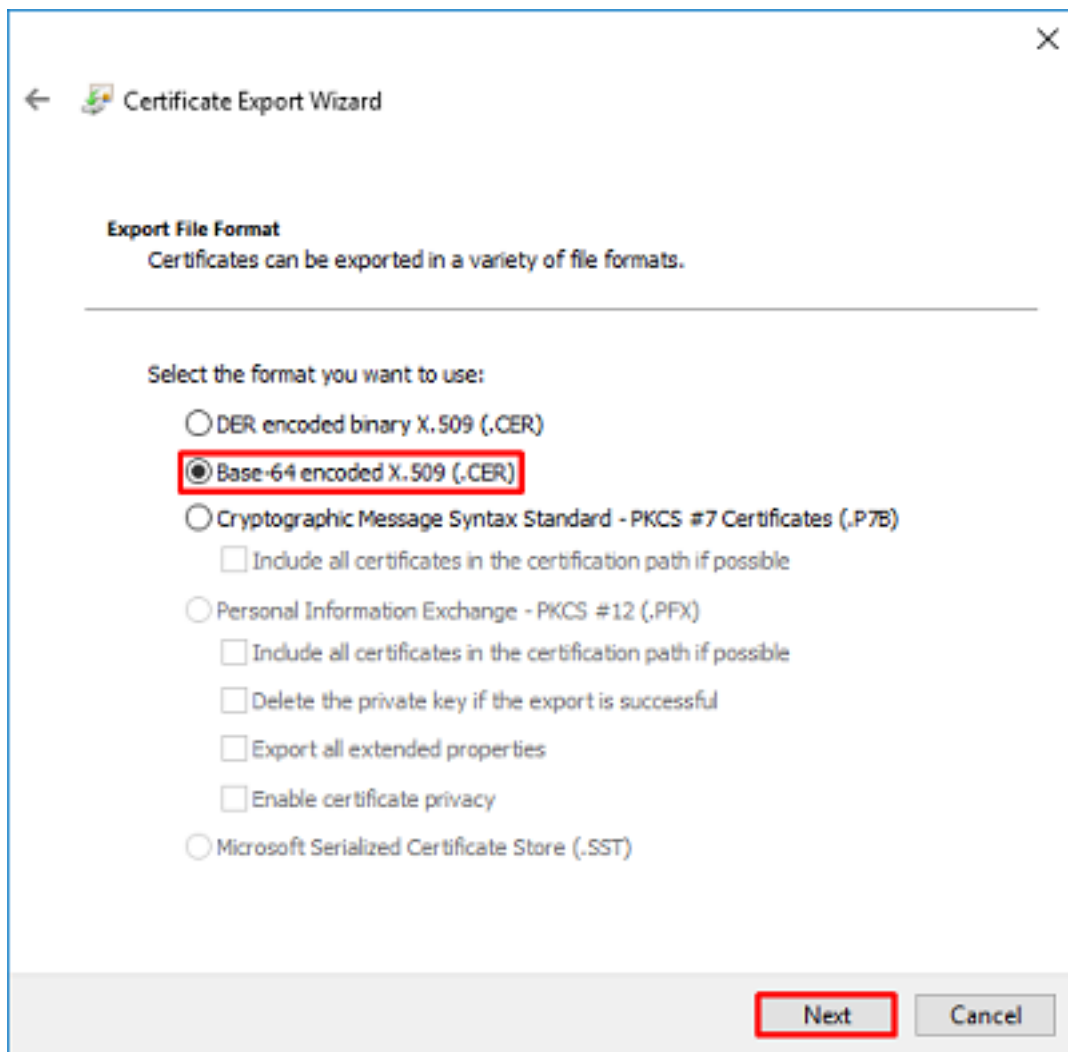
10. Open het tabblad **Details** en klik vervolgens op **Kopie naar bestand...** zoals in de afbeelding wordt weergegeven.



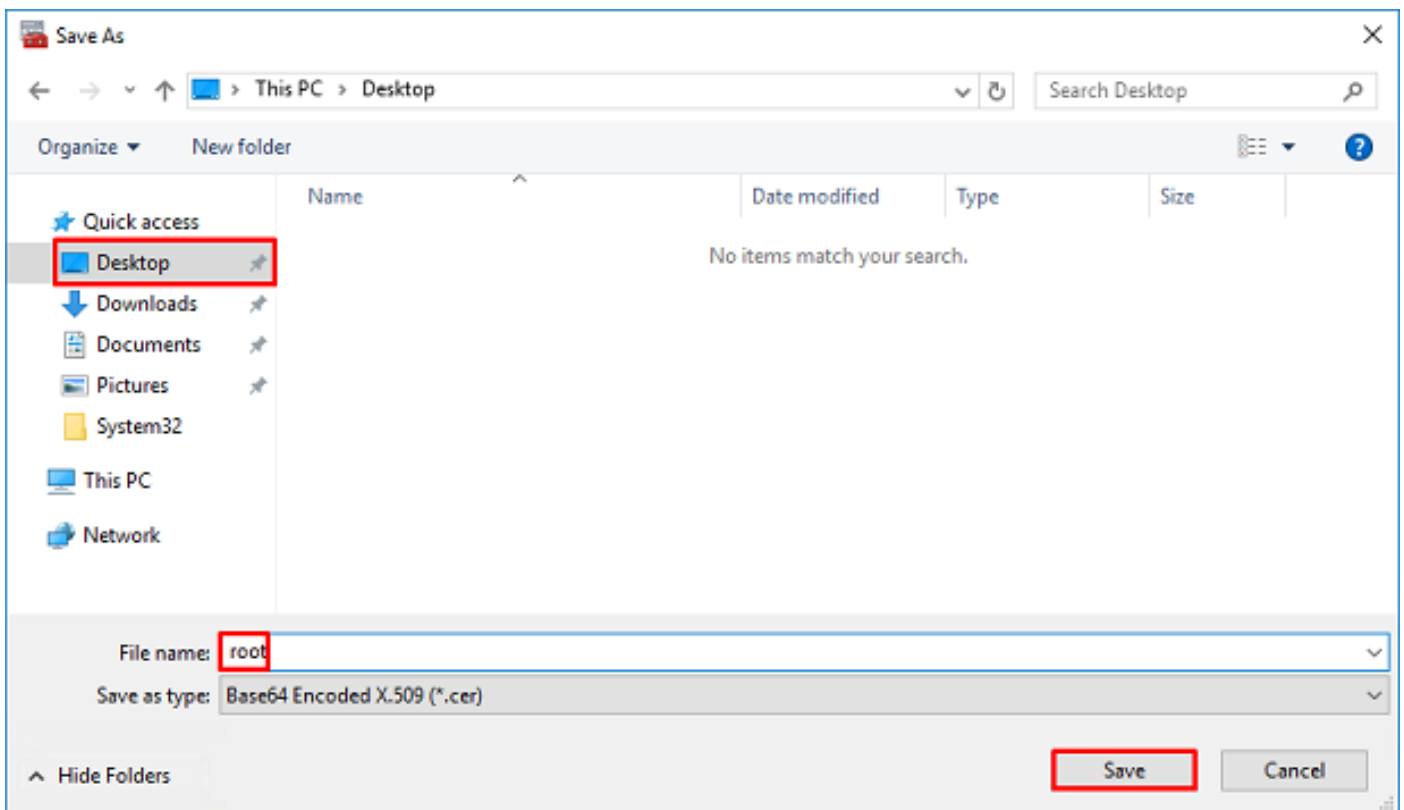
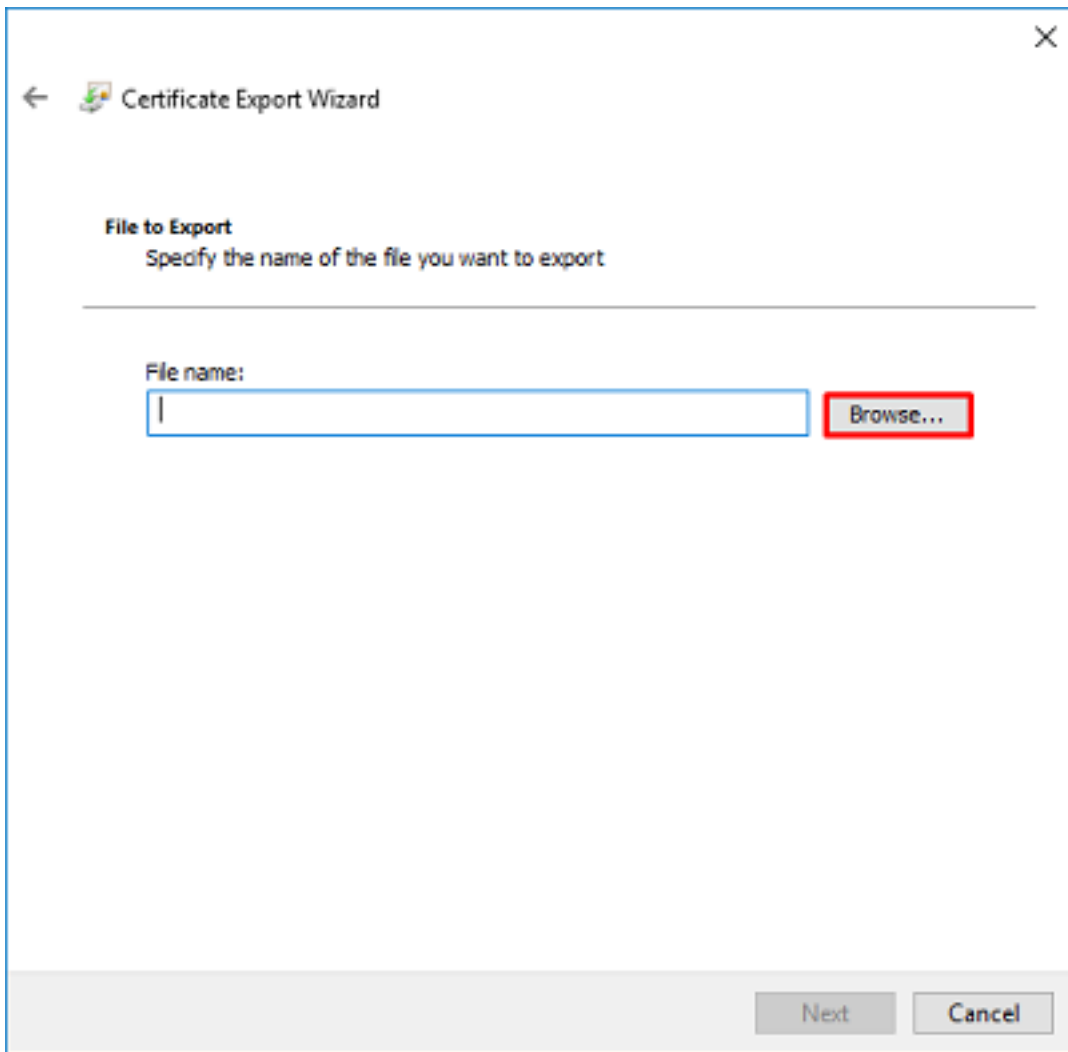
11. Navigeer door de Wizard Certificaat Exporteren die de wortel CA in PEM-indeling zal uitvoeren.

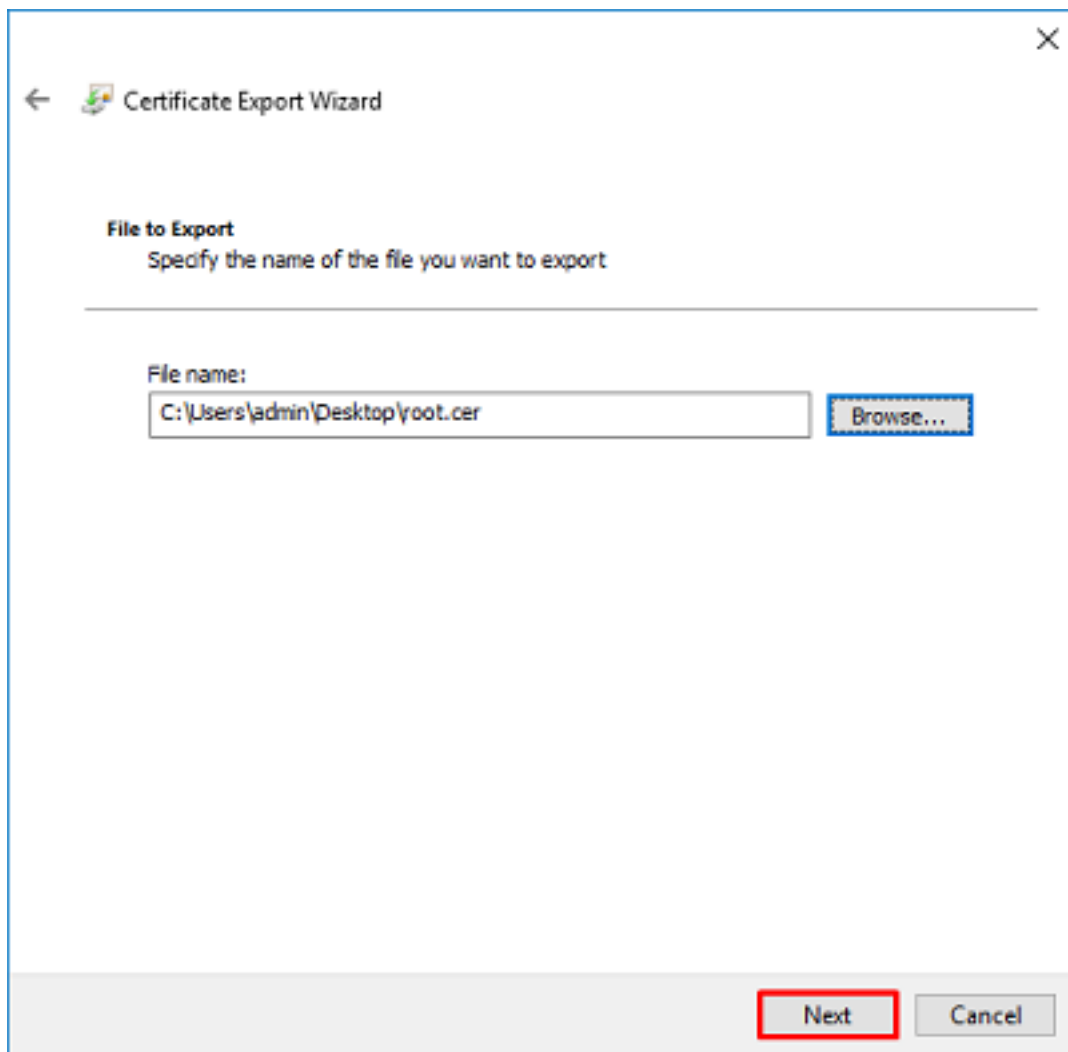


12. Selecteer **Base-64** gecodeerd X.509.

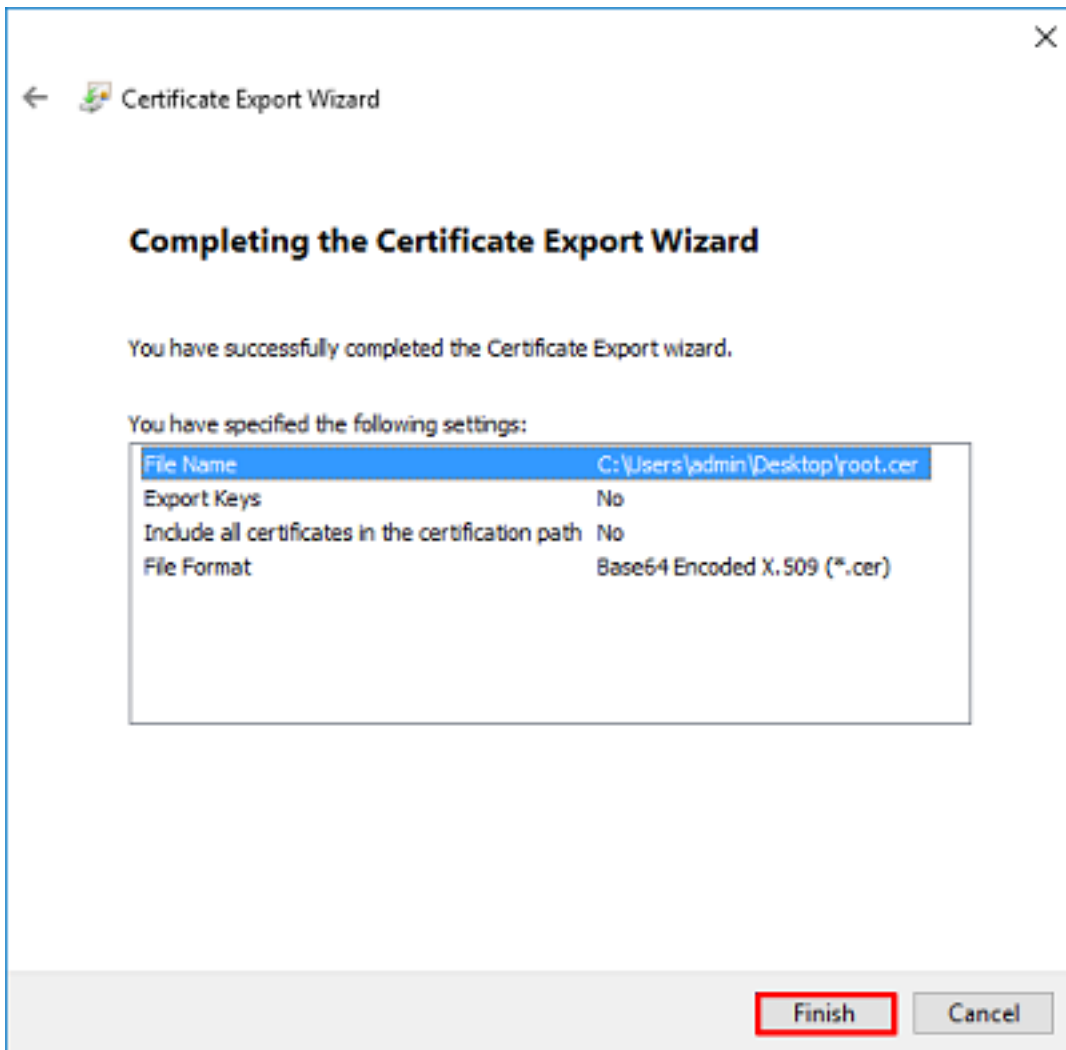


13. Selecteer de naam van het bestand en waar het naar geëxporteerd wordt.





14. Klik op **Voltoeien**.



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.

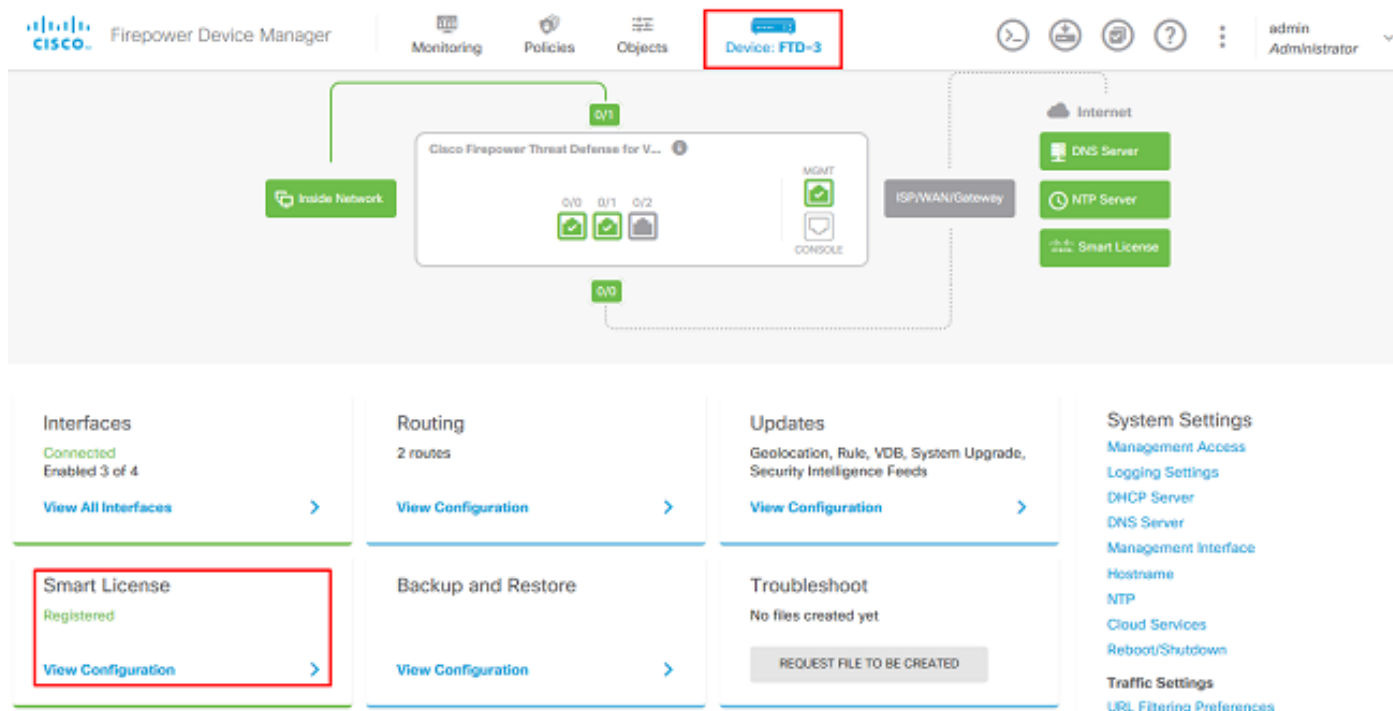
```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeJleGFtcGxlLVdJdTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlAMB0xGzAZBgNVBAMTEmV4YW1wbGUtV01OMjAxNi1lDQTC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++m+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPPkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxcVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OfpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgrEtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubR1+d
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFQV3DgZg+R96
9WLCR30big6xyo9Zu+lixcWpdrbADO6zMhbEYEHkh00jBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

FDM-configuraties

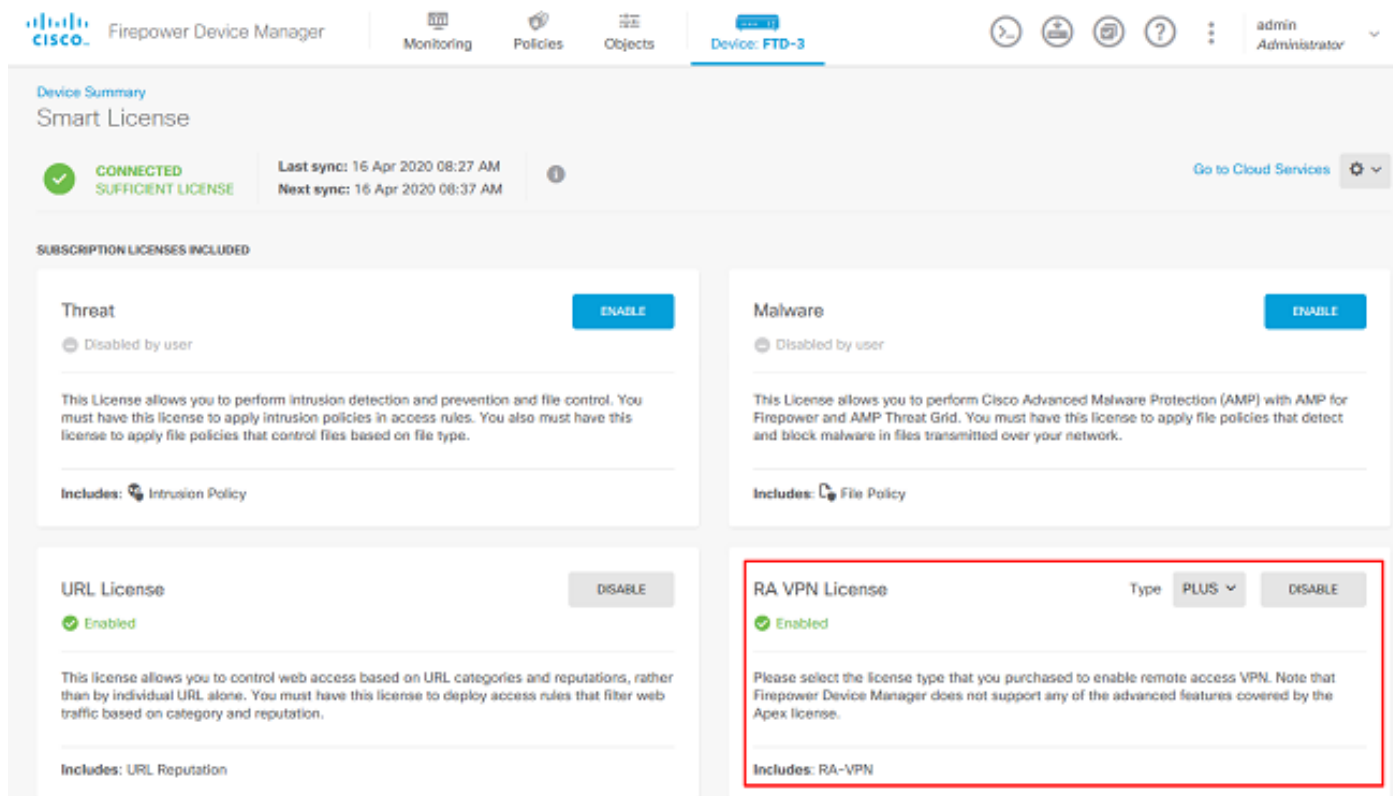
Controleer de licenties

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.

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

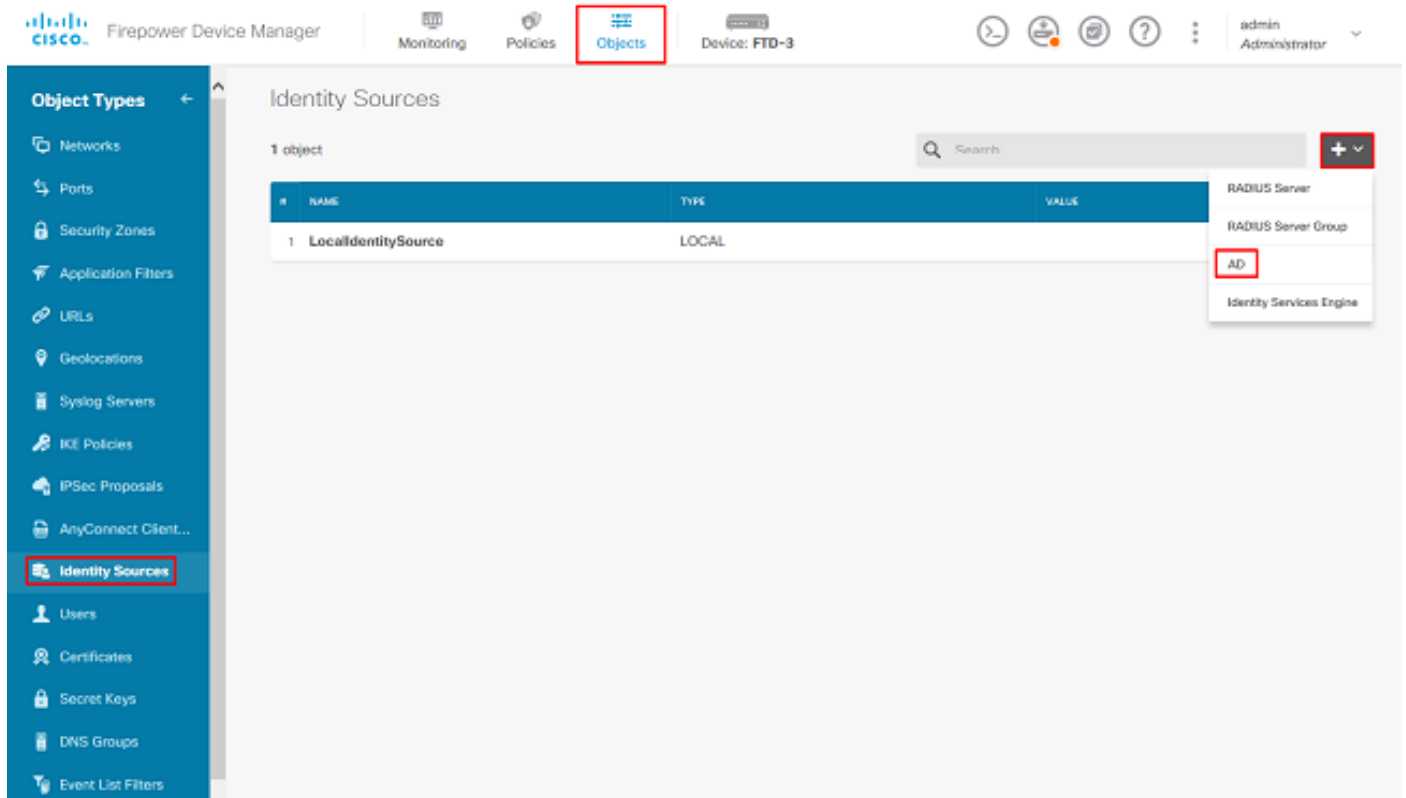


2. Controleer dat de FTD bij de slimme licentieserver is geregistreerd en dat de AnyConnect Plus, Apex of VPN only licentie is ingeschakeld.



AD-identiteitsbron instellen

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



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 > Systeminstellingen > 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



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

Name

LAB-AD

Type

Active Directory (AD)

Directory Username

ftd.admin@example.com

e.g. user@example.com

Directory Password

••••••••

Base DN

DC=example,DC=com

e.g. ou=user, dc=example, dc=com

AD Primary Domain

example.com

e.g. example.com

Directory Server Configuration

win2016.example.com:389

Hostname / IP Address

win2016.example.com

e.g. ad.example.com

Port

389

Encryption

NONE

Trusted CA certificate

Please select a certificate

TEST

✓ Connection to realm is successful

[Add another configuration](#)

CANCEL

OK

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-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExJleGFtcGxlLVdJTlJwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC
ASwDQYJKoZIhvcNAQEFBQADQgEPADCCAQoCggEFRAI8ghT719NzS0ncOPh0YT67h
```

CANCEL OK

Directory Server Configuration

win2016.example.com:636

Hostname / IP Address: win2016.example.com
e.g. ad.example.com

Port: 636

Encryption: LDAPS

Trusted CA certificate: LDAPS_ROOT

TEST ✓ Connection to realm is successful

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 Device Manager

Monitoring Policies **Objects** Device: FTD-3

admin Administrator

Object Types

- Networks
- Ports
- Security Zones
- Application Filters

Identity Sources

2 objects

#	NAME	TYPE	VALUE	ACTIONS
1	LocalIdentitySource	LOCAL		
2	LAB-AD	AD	win2016.example.com	

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

Pending Changes

✓ **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 Edited

+ **Active Directory Realm Added: LAB-AD**

```
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
```

MORE ACTIONS ▼ | CANCEL | **DEPLOY NOW** ▼

AnyConnect voor AD-verificatie configureren

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

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

Firepower Device Manager | Monitoring | Policies | Objects | **Device: FTD-3** | admin Administrator

Interfaces: Connected, Enabled 3 of 4 | View All Interfaces >

Smart License: Registered | View Configuration >

Site-to-Site VPN: There are no connections yet | View Configuration >

Remote Access VPN: Configured, 1 connection | 2 Group Policies | View Configuration >

Routing: 2 routes | View Configuration >

Backup and Restore: | View Configuration >

Updates: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds | View Configuration >

Troubleshoot: No files created yet | REQUEST FILE TO BE CREATED

Advanced Configuration: Includes: FlexConfig, Smart CLI | View Configuration >

System Settings: Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences

Device Administration: Audit Events, Deployment History, Download Configuration | View Configuration >

2. Klik op het + symbol of de knop **verbindingsprofiel maken** zoals in de afbeelding.

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

Search

+	NAME	AAA	GROUP POLICY	ACTIONS
<p>There are no Remote Access Connections yet. Start by creating the first Connection.</p> <p>CREATE CONNECTION PROFILE</p>				

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 how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

General

Group Alias

General

[Add Group Alias](#)

Group URL

[Add Group URL](#)

Primary Identity Source

Authentication Type

AAA Only

Client Certificate Only

AAA and Client Certificate

Primary Identity Source for User Authentication

Filter

LocalIdentitySource

LAB-AD

Special-Identities-Realm

[Create new](#)

Fallback Local Identity Source ⚠


Please Select Local Identity Source

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool



 AnyConnect-Pool

IPv6 Address Pool

Endpoints are provided an address from this pool



DHCP Servers



CANCEL

SUBMIT QUERY

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

Policy Group Brief Details

DNS + BANNER		Edit
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 ([DefaultInternecertificaatbericht](#)) 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: <https://software.cisco.com/download/home>. 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

FTD-3-Manual

Outside Interface

outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface

ftd3.example.com

e.g. ravpn.example.com

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks

+

inside (GigabitEthernet0/1)

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.

+

any-ipv4

AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from software.cisco.com.

You must have the necessary AnyConnect software license.

Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.03052-webdeploy-k9.pkg

Linux: anyconnect-linux64-4.7.03052-webdeploy-k9.pkg

BACK

NEXT

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.

General

STEP 1: CONNECTION AND CLIENT CONFIGURATION

Primary Identity Source

Authentication Type AAA Only

Primary Identity Source 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

IPv4 Address Pool

BACK SUBMIT QUERY

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

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

1 object

Search

#	NAME	AAA	GROUP POLICY	ACTIONS
1	General	Authentication: AAA Only Authorization: None Accounting: None	DfltGrpPolicy	

8. Klik op **Nu implementeren**.

Pending Changes

?
✕
Close

✔ Last Deployment Completed Successfully
16 Apr 2020 12:41 PM, [See Deployment History](#)

Deployed Version (16 Apr 2020 12:41 PM)	Pending Version
+ Network Object Added: <i>AnyConnect-Pool</i>	
-	subType: Network
-	value: 10.10.10.0/24
-	isSystemDefined: false
-	dnsResolution: IPV4_AND_IPV6
-	name: AnyConnect-Pool
+ RA VPN Added: <i>NGFW-Remote-Access-VPN</i>	
-	vpnGatewaySettings[0].exemptNatRule: true
-	vpnGatewaySettings[0].outsideFqdn: ftd3.example.com
-	vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t...
-	name: NGFW-Remote-Access-VPN
anyconnectPackageFiles:	
-	anyconnect-win-4.7.03052-webdeploy-k9.pkg
vpnGatewaySettings[0].serverCertificate:	
-	FTD-3-Manual
vpnGatewaySettings[0].outsideInterface:	
-	outside
vpnGatewaySettings[0].insideInterfaces:	
-	inside
vpnGatewaySettings[0].insideNetworks:	

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

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 AnyConnect-gebruikers met interne bronnen kunnen verbinden met het gebruik van HTTP.

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

Firepower Device Manager

Monitoring **Policies** Objects Device: FTD-3

Security Policies

SSL Decryption → **Identity** → Security Intelligence → NAT → Access Control → Intrusion

Establishing User Identity

You can use identity policies to collect user identity information from connections. You can then view usage based on user identity in the dashboards, and configure access control based on user or user group. By linking network behavior, traffic, and events directly to individual users, the system can help you identify the source of policy breaches, attacks, or network vulnerabilities.

How Identity policies work

Passive authentication Active authentication

ENABLE IDENTITY POLICY

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

Firepower Device Manager

Monitoring **Policies** Objects Device: FTD-3

Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion

Identity Policy

Search

#	NAME	AUTHENTICATION	AUTH. TYPE	SOURCE ZONES	NETWORKS	PORTS	DESTINATION ZONES	NETWORKS	PORTS/PROTO...	ACTIONS
<p>There are no Identity rules yet. Start by creating the first identity rule.</p> <p>CREATE IDENTITY RULE</p>										

Default Action **Passive Auth** Any Identity Source

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

Firepower Device Manager

Monitoring **Policies** Objects Device: FTD-3

Security Policies

SSL Decryption → Identity → Security Intelligence → **NAT** → Access Control → Intrusion

1 rule

Search

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET			TRANSLATED PACKET				ACTIONS	
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT		DESTINATIO...
Auto NAT Rules												
>	#	Internet_PAT	DYNAMIC	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.

The screenshot shows the Cisco Firepower Device Manager (FDM) interface. The top navigation bar includes 'Monitoring', 'Policies', and 'Objects'. The 'Policies' tab is selected. The breadcrumb trail is: SSL Decryption -> Identity -> Security Intelligence -> NAT -> Access Control -> Intrusion. The 'Access Control' tab is active. Below the breadcrumb trail is a search bar and a '+ Add' button. A table with columns for NAME, ACTION, SOURCE (ZONES, NETWORKS, PORTS), and DESTINATION (ZONES, NETWORKS, PORTS/PROTOS, APPLICATIONS, URLS, USERS, ACTIONS) is shown. The table is empty, with a message: 'There are no access rules yet. Start by creating the first access rule.' Below this message is a 'CREATE ACCESS RULE' button. At the bottom, the 'Default Action' is set to 'Access Control' with a 'Block' action selected.

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 Rule

Order	Title	Action
1	AC RDP Access	Allow

Source/Destination Applications URLs Users Intrusion Policy File policy Logging

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP

Show Diagram Not hit yet CANCEL OK

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: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

AVAILABLE USERS

Filter: []

Identity Sources: **Groups** | Users

- LAB-AD \ Account Operators
- LAB-AD \ Administrators
- LAB-AD \ Allowed RODC Password Replication Group
- LAB-AD \ AnyConnect Admins**
- LAB-AD \ AnyConnect Users

Create new Identity Realm | CANCEL | **OK**

Show Diagram:

CANCEL | **OK**

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

Add Access Rule

Order: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

AVAILABLE USERS

- LAB-AD \ AnyConnect Admins

Show Diagram:

CANCEL | **OK**

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

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

Edit Access Rule

Order: 2 | Title: AC HTTP Access | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

SOURCE

Zones	Networks	Ports
outside_zone	AnyConnect-Pool	ANY

DESTINATION

Zones	Networks	Ports/Protocols
inside_zone	Inside_Net	HTTP

Show Diagram | Not hit yet | CANCEL | OK

Edit Access Rule

Order: 2 | Title: AC HTTP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

AVAILABLE USERS

LAB-AD \ AnyConnect 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 | Not hit yet | CANCEL | OK

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

rechtsboven in de afbeelding.

The screenshot shows the Cisco Firepower Device Manager interface. At the top, there are navigation tabs for Monitoring, Policies, Objects, and Device: FTD-3. The user is logged in as admin Administrator. The main section is titled "Security Policies" and shows a breadcrumb trail: SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion. Below this, it indicates "2 rules" and provides a search bar. A table lists the rules:

#	NAME	ACTION	SOURCE ZONES	NETWORKS	PORTS	DESTINATION ZONES	NETWORKS	PORTS/PROTO...	APPLICATIONS	URLS	USERS	ACTIONS
1	AC RDP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP	ANY	ANY	AnyConne...	
2	AC HTTP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne...	

At the bottom, the "Default Action" is set to "Access Control" with a "Block" button and a dropdown menu.

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

The screenshot shows the "Pending Changes" dialog box. It features a blue header with the title "Pending Changes" and a close button. Below the header, a green checkmark indicates "Last Deployment Completed Successfully" on 28 Apr 2020 01:35 PM, with a link to "See Deployment History".

The dialog is divided into two sections: "Deployed Version (28 Apr 2020 01:35 PM)" and "Pending Version". A legend indicates that "Removed" items are in red, "Added" items are in green, and "Edited" items are in blue. Under the "Pending Version" section, two items are listed as "Access Rule Added":

- Access Rule Added: AC HTTP Access**
 - users[0].name: AnyConnect Users
 - logFiles: false
 - eventLogAction: LOG_NONE
 - ruleId: 268435467
 - name: AC HTTP Access
- Access Rule Added: AC RDP Access**

At the bottom of the dialog, there are three buttons: "MORE ACTIONS" (with a dropdown arrow), "CANCEL", and "DEPLOY NOW" (highlighted with a red box and a dropdown arrow).

Verifiëren

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

Eindconfiguratie

AAA-configuratie

```
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
```

AnyConnect configureren

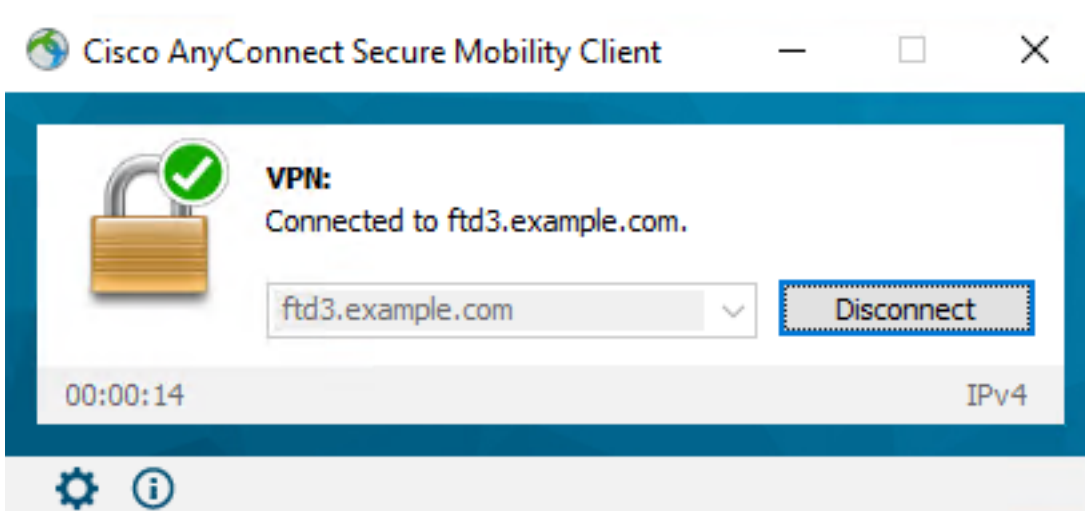
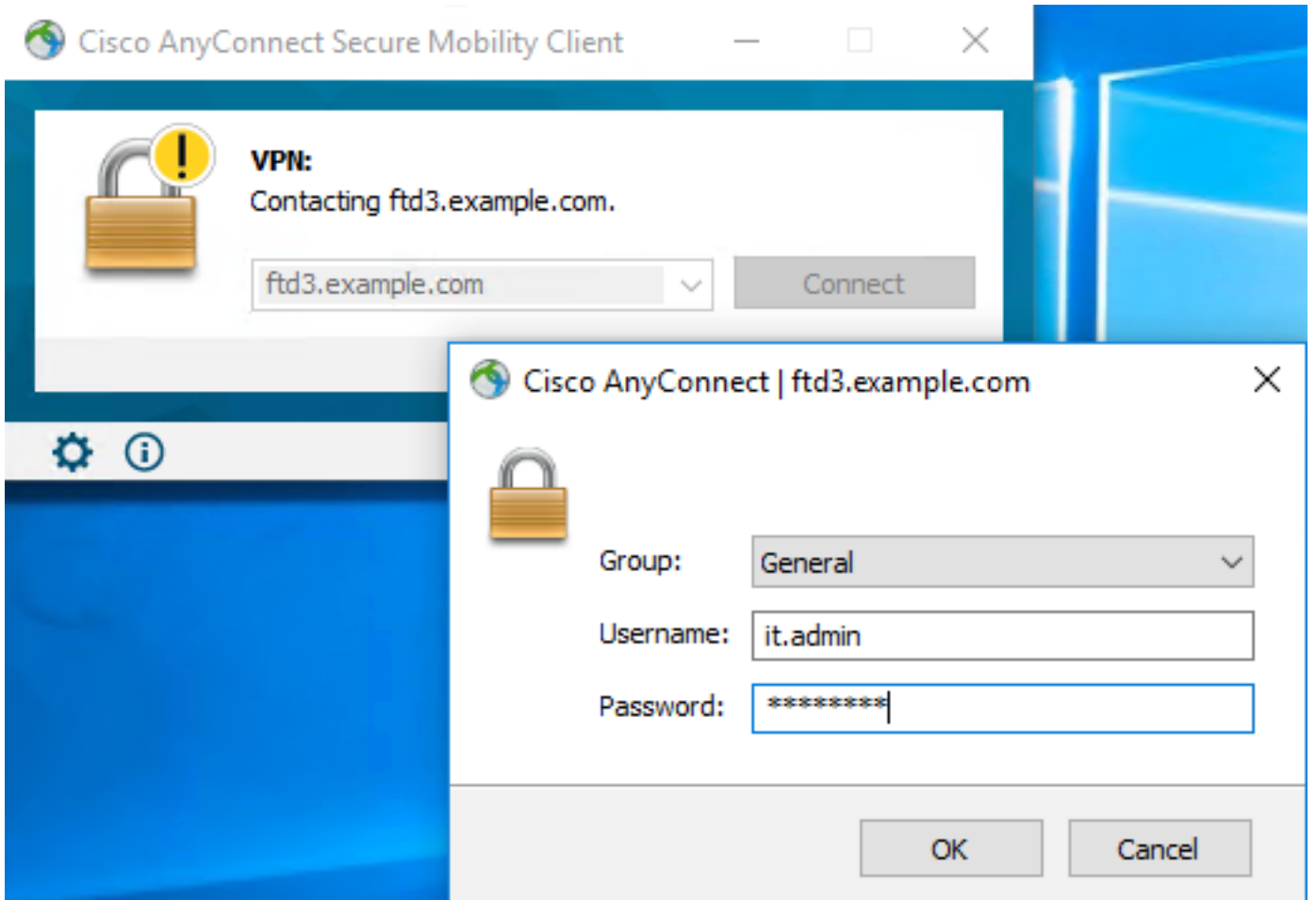
```
> show running-config webvpn
webvpn
  enable outside
  http-headers
    hsts-server
      enable
      max-age 31536000
      include-sub-domains
      no preload
    hsts-client
      enable
  x-content-type-options
  x-xss-protection
  content-security-policy
  anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 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
```

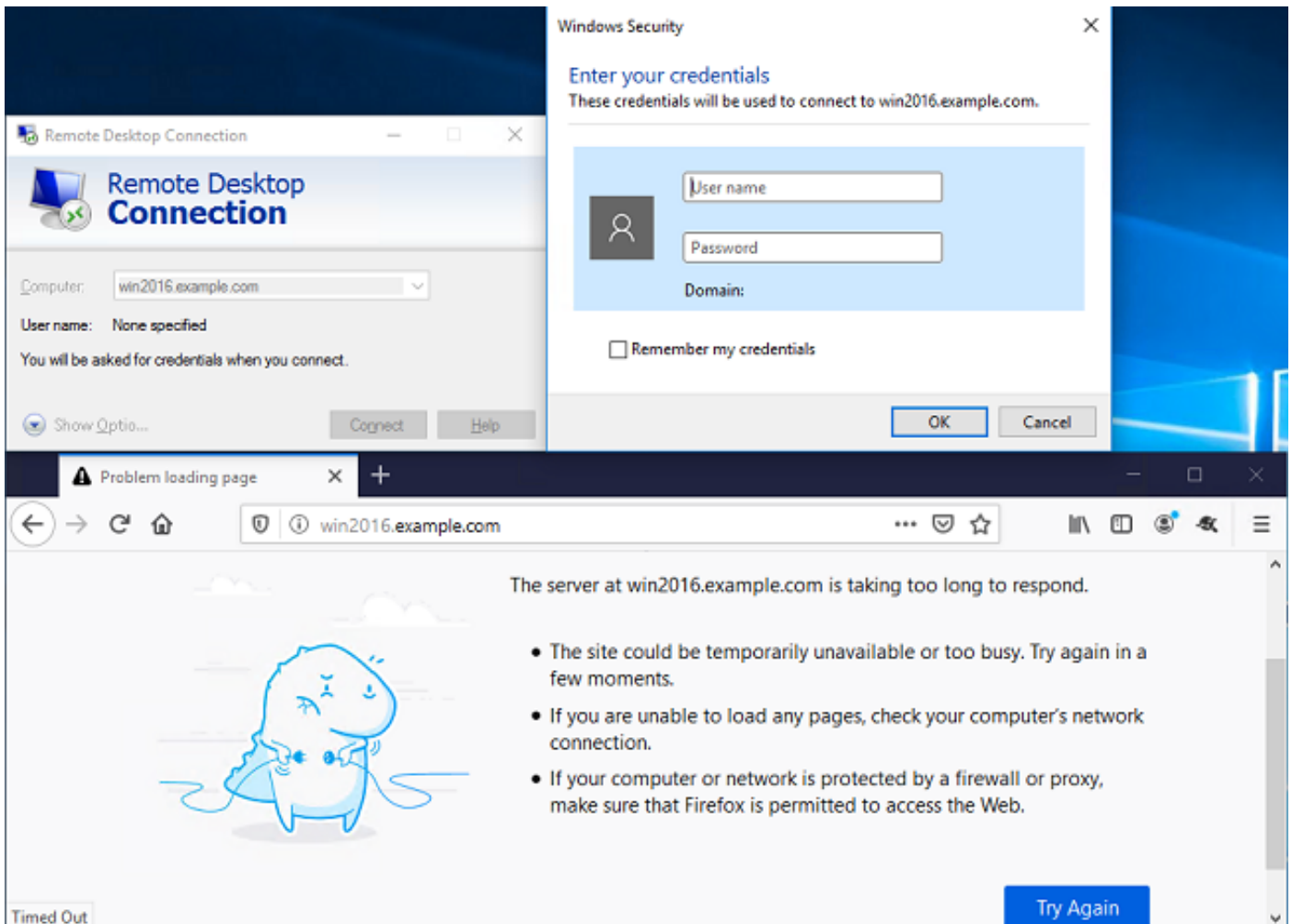
```
> show running-config group-policy
group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
  anyconnect ssl dtls none
```

```
> show running-config ssl
ssl trust-point FTD-3-Manual outside
```

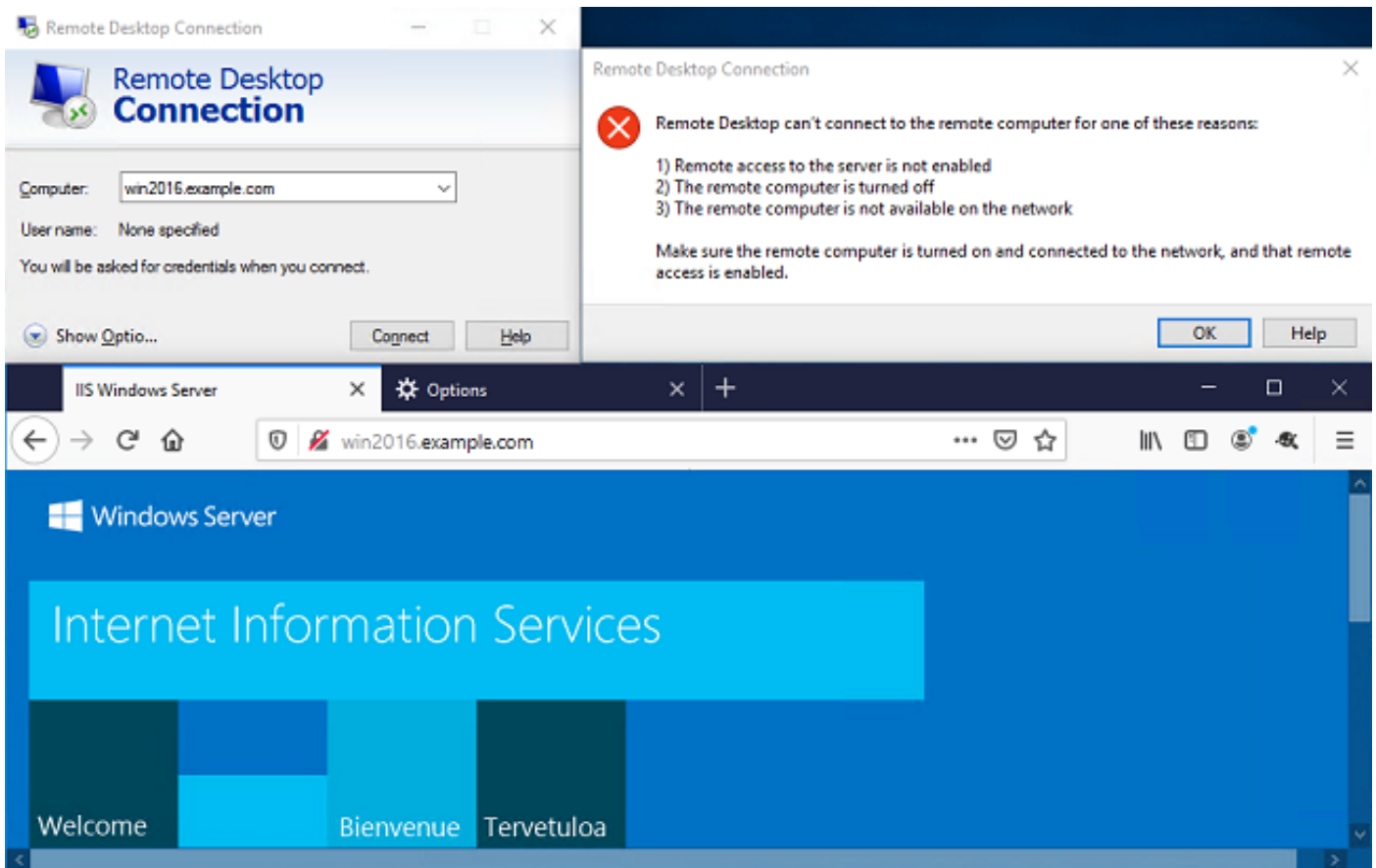
Connect met AnyConnect en controleer beleidsregels voor toegangscontrole



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 ldap 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:
[53]   objectClass: value = top
[53]   objectClass: value = person
[53]   objectClass: value = organizationalPerson
[53]   objectClass: value = user
[53]   cn: value = IT Admin
[53]   sn: value = Admin
[53]   givenName: value = IT
[53]   distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]   instanceType: value = 4
[53]   whenCreated: value = 20200421025811.0Z
[53]   whenChanged: value = 20200421204622.0Z
[53]   displayName: value = IT Admin
[53]   uSNCreated: value = 25896
[53]   memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]   uSNChanged: value = 26119
[53]   name: value = IT Admin
[53]   objectGUID: value = &...J..O..2w...c
[53]   userAccountControl: value = 512
[53]   badPwdCount: value = 6
[53]   codePage: value = 0
[53]   countryCode: value = 0
[53]   badPasswordTime: value = 132320354378176394
[53]   lastLogoff: value = 0
[53]   lastLogon: value = 0
[53]   pwdLastSet: value = 132319114917186142
[53]   primaryGroupID: value = 513
[53]   objectSid: value = .....{I...;.....j}...
[53]   accountExpires: value = 9223372036854775807
[53]   logonCount: value = 0
[53]   sAMAccountName: value = it.admin
[53]   sAMAccountType: value = 805306368
[53]   userPrincipalName: value = it.admin@example.com
[53]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
[53]   dSCorePropagationData: value = 16010101000000.0Z
[53]   lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End

```

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:

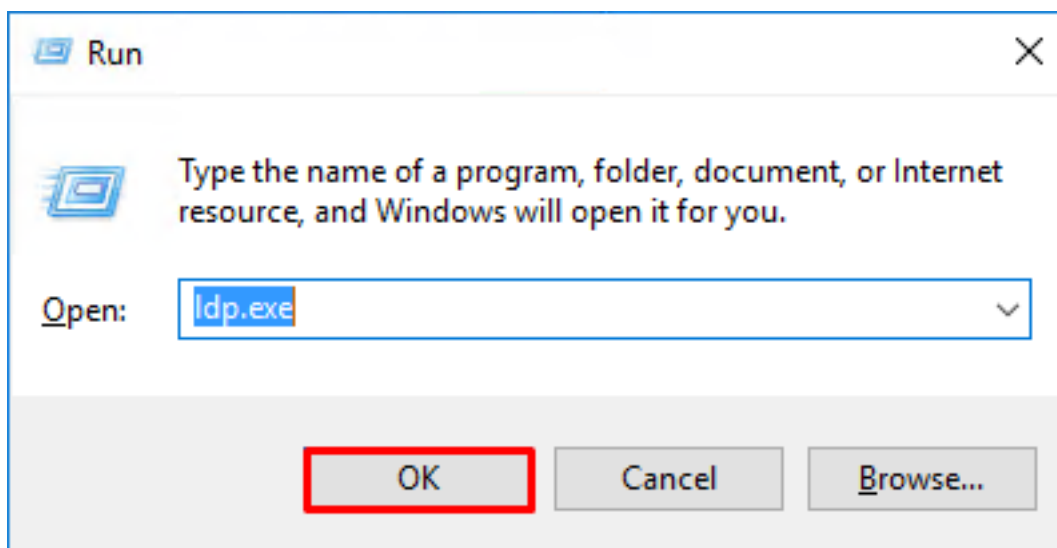
- Controleer de routing en zorg ervoor dat de FTD een antwoord van de LDAP-server ontvangt.
- Als LDAPS of STARTTLS wordt gebruikt, zorg er dan voor dat het juiste basiscertificaat van CA is vertrouwd zodat de SSL-handdruk met succes kan worden voltooid.
- Controleer dat het juiste IP-adres en de juiste 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

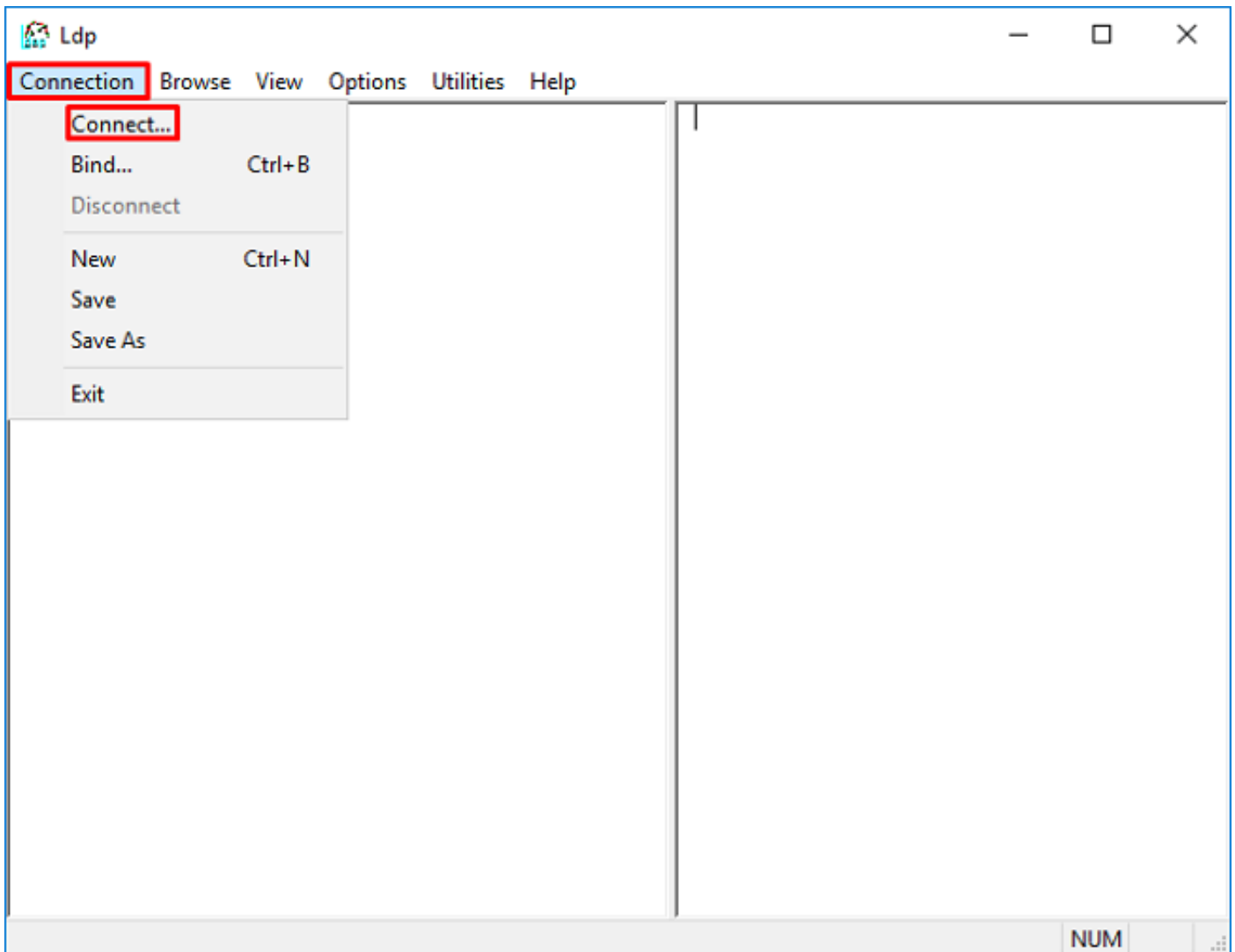
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] 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 **ldp.exe** worden geverifieerd. Om te verifiëren dat een account met succes kan verbinden met het gebruik van ldp, navigeer deze stappen:

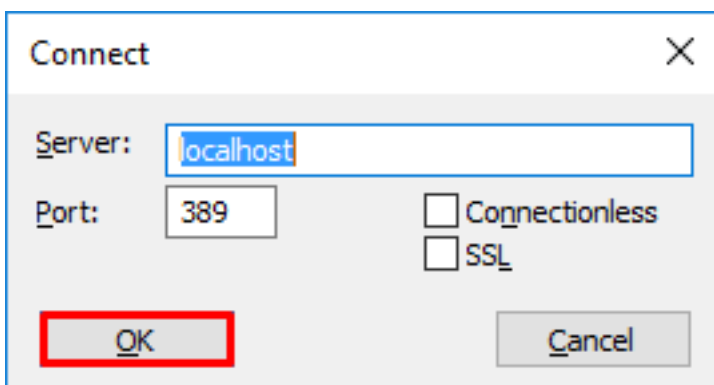
1. Druk op **Win+R** op de AD-server en zoek naar **ldp.exe**.



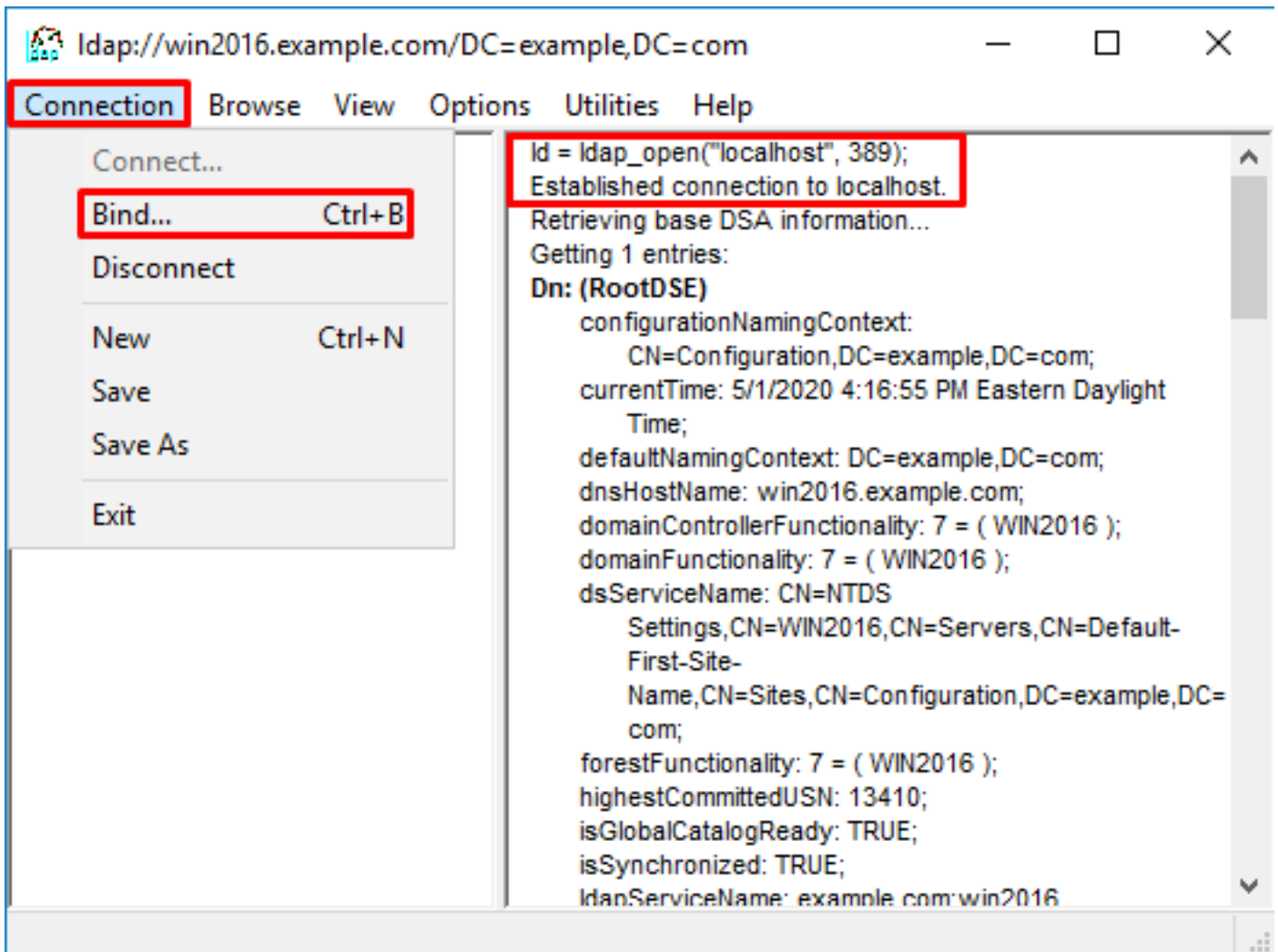
2. Klik op **Connection > Connect...** zoals in de afbeelding wordt weergegeven.



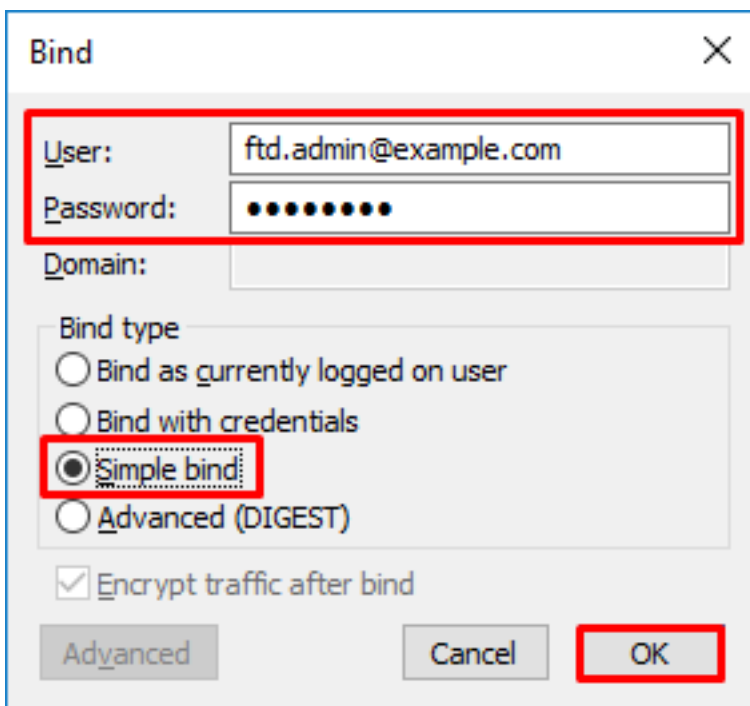
3. Specificeer localhost voor de server en de juiste poort en klik vervolgens op **OK**.



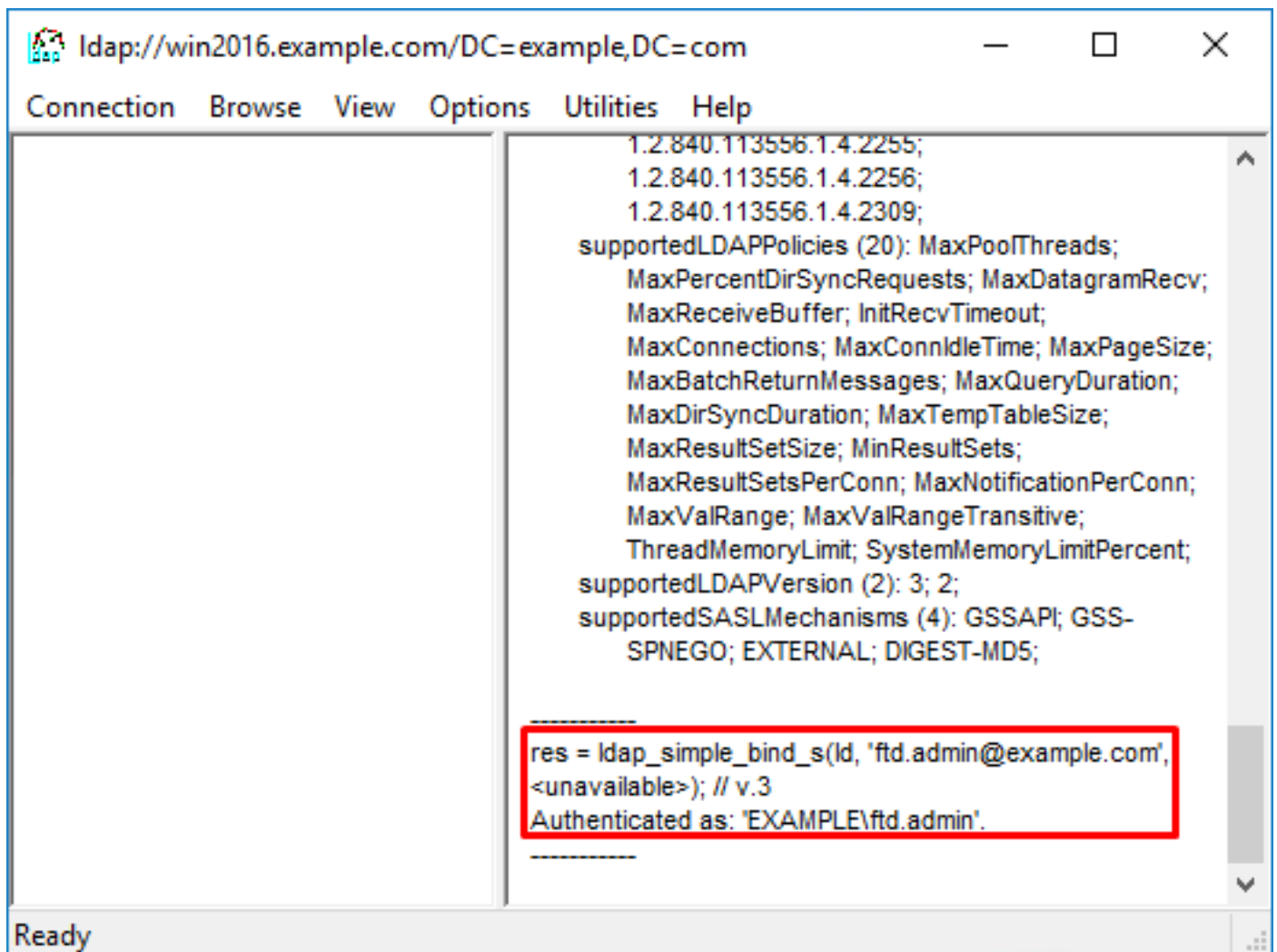
4. De rechterkolom geeft de tekst weer die een goede verbinding aangeeft. Klik op **Connection > Bind...** zoals in de afbeelding wordt weergegeven.



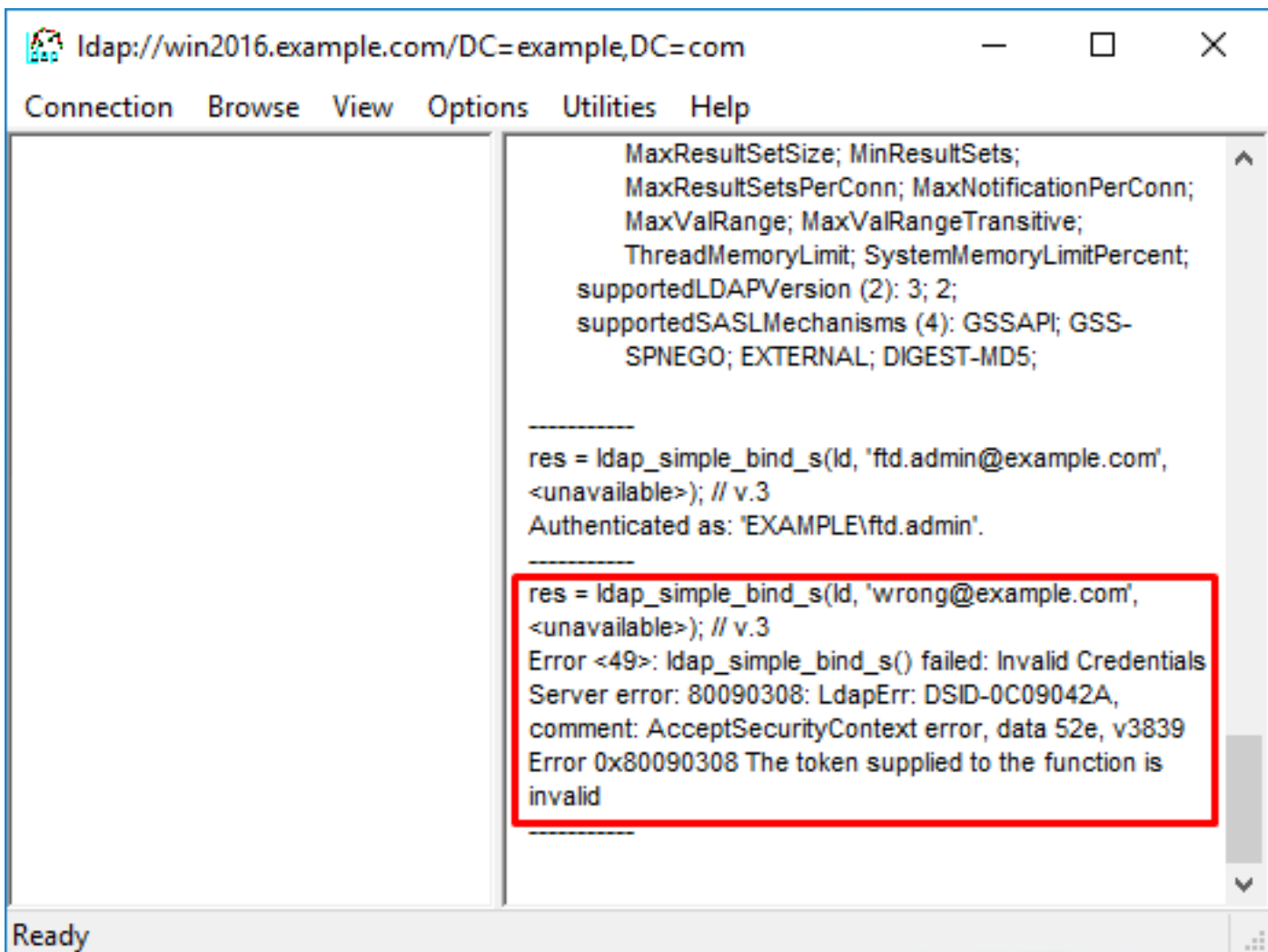
5. Selecteer **Eenvoudig Bind**, en specificeer vervolgens de naam en het wachtwoord van de directory-account. Klik op **OK**.



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



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

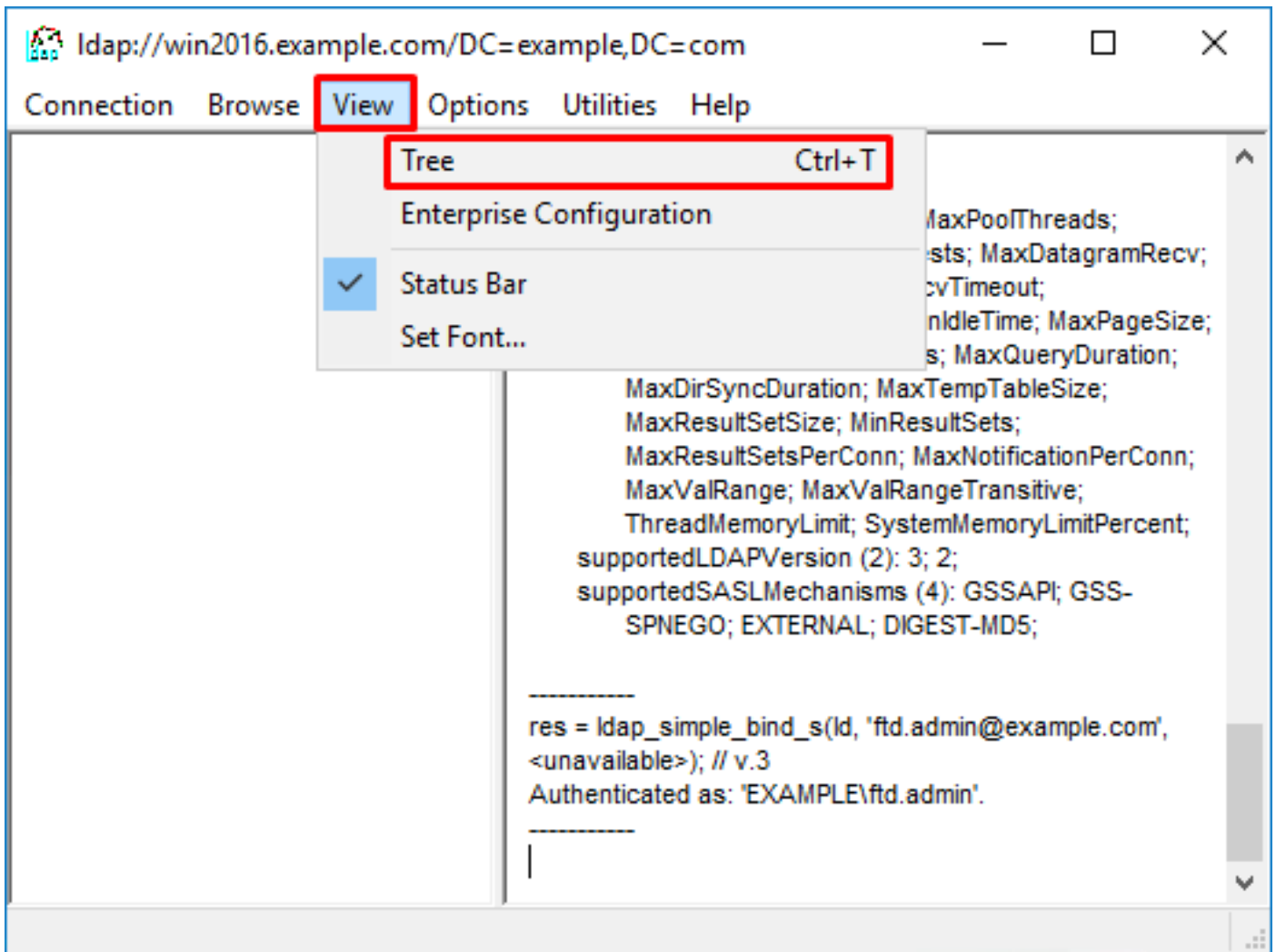


LDAP Server kan geen gebruikersnaam vinden

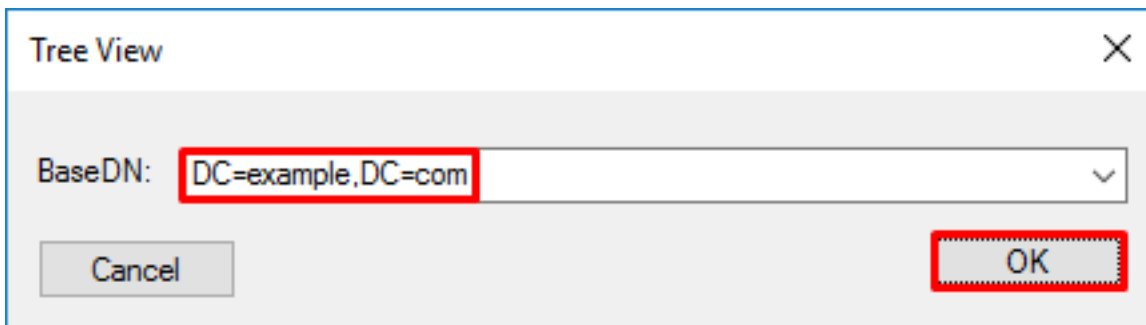
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] 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.

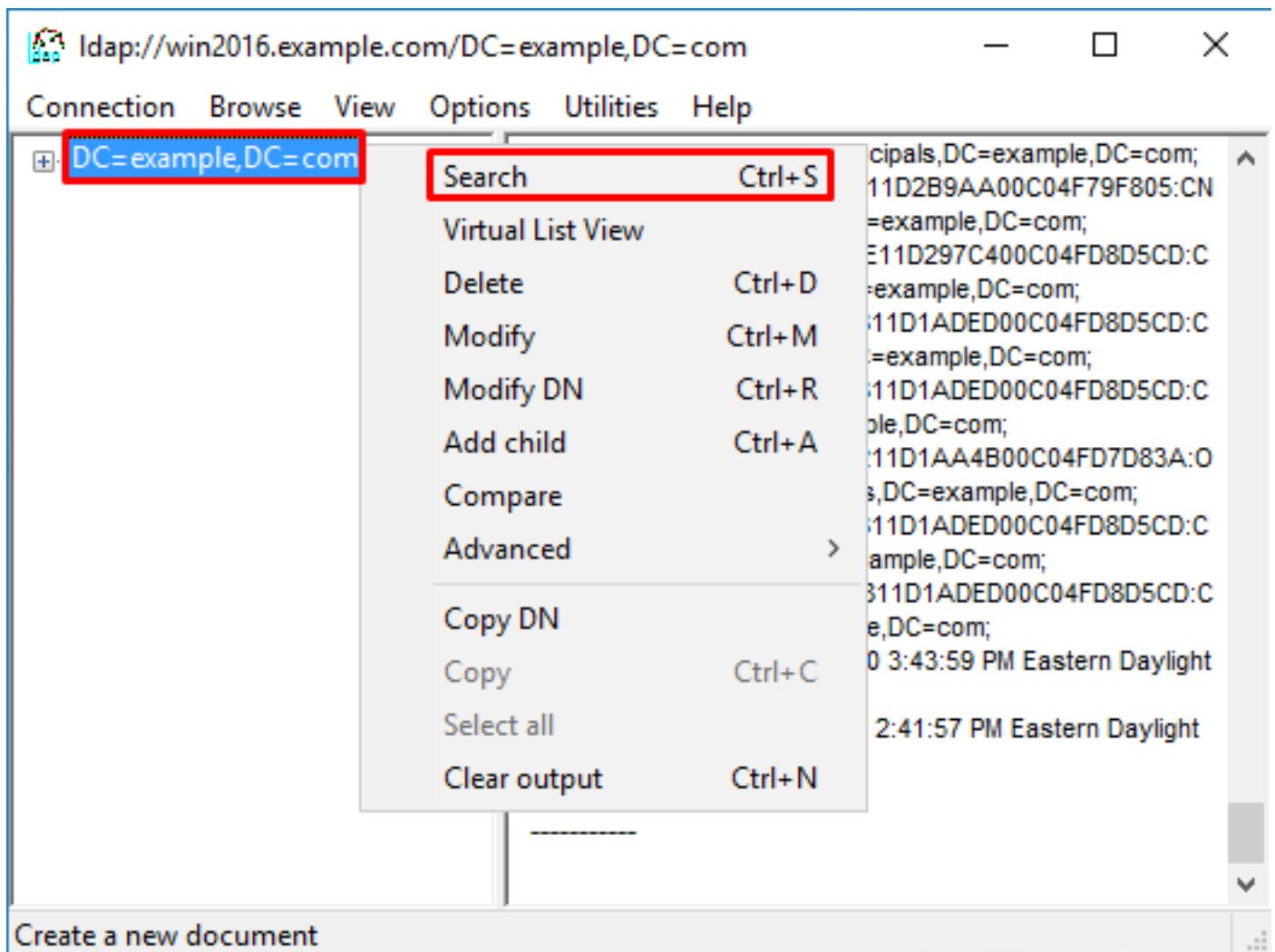
1. Nadat u met succes hebt binden, navigeer dan naar **Beeld > Boom** zoals in de afbeelding.



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

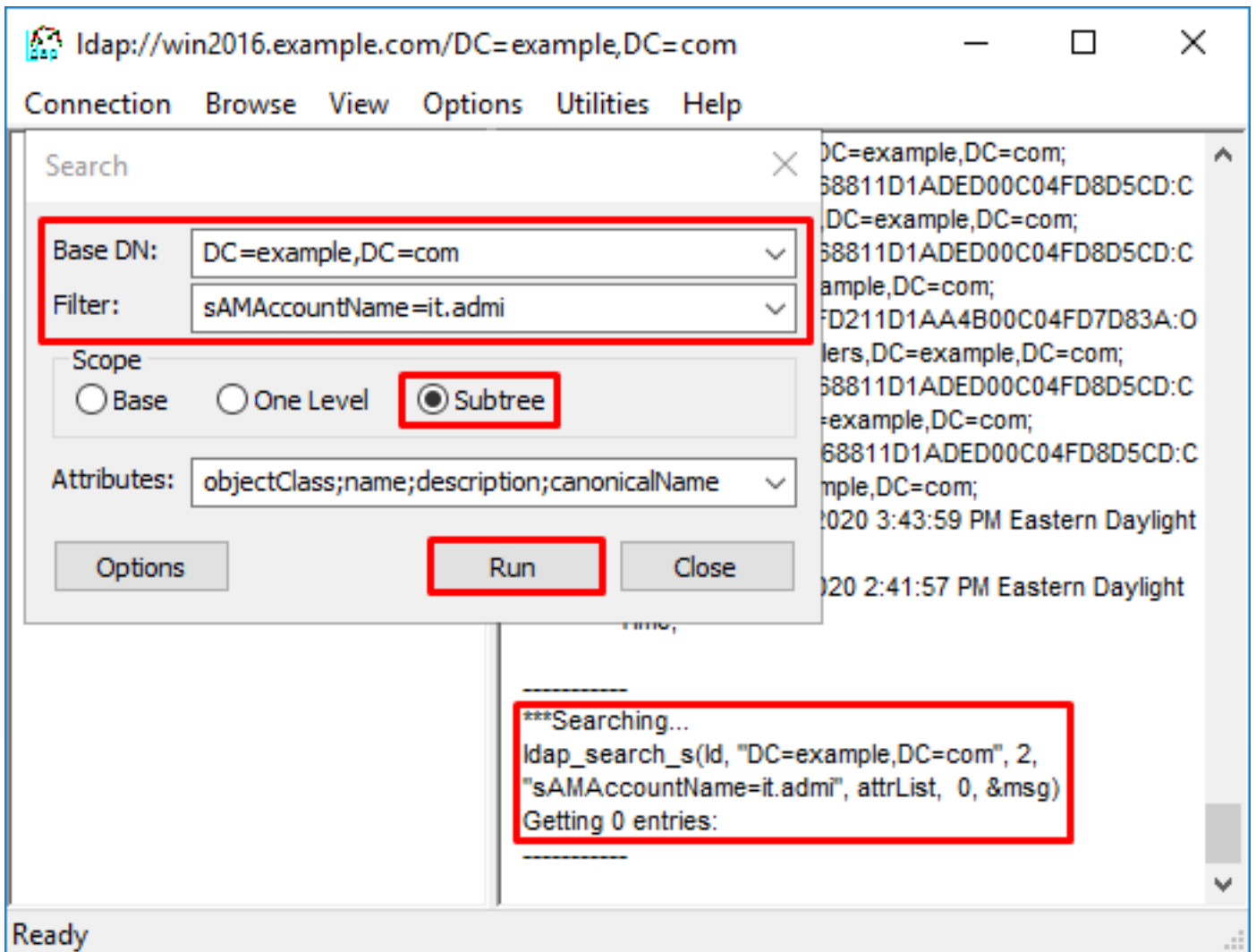


3. Klik met de rechtermuisknop op de Base DN en klik vervolgens op Zoeken zoals in de afbeelding.



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



Idp 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.

LDAP Search Tool Interface

Connection: ldap://win2016.example.com/DC=example,DC=com

Search Dialog:

- Base DN: DC=example,DC=com
- Filter: sAMAccountName=it.admin
- Scope: Subtree
- Attributes: objectClass;name;description;canonicalName
- Buttons: Options, Run, Close

Main Window Output:

```

68811D1AED00C04FD8D5CD:C
DC=example,DC=com;
68811D1AED00C04FD8D5CD:C
example,DC=com;
FD211D1AA4B00C04FD7D83A:O
lers,DC=example,DC=com;
68811D1AED00C04FD8D5CD:C
=example,DC=com;
68811D1AED00C04FD8D5CD:C
mple,DC=com;
020 3:43:59 PM Eastern Daylight
020 2:41:57 PM Eastern Daylight

```

Search Results:

```

***Searching...
ldap_search_s(ld, "DC=example,DC=com", 2,
"sAMAccountName=it.admin", attrList, 0, &msg)
Getting 1 entries:
Dn: CN=IT Admin,CN=Users,DC=example,DC=com
canonicalName: example.com/Users/IT Admin;
name: IT Admin;
objectClass (4): top; person; organizationalPerson;
user;

```

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]
      Scope = [SUBTREE]
[-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

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

> show capture
```



```
capture AD type raw-data interface inside [Capturing - 0 bytes]
  match tcp any host 192.168.1.1 eq ldap

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

> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
  match tcp any host 192.168.1.1 eq ldap

> show capture AD

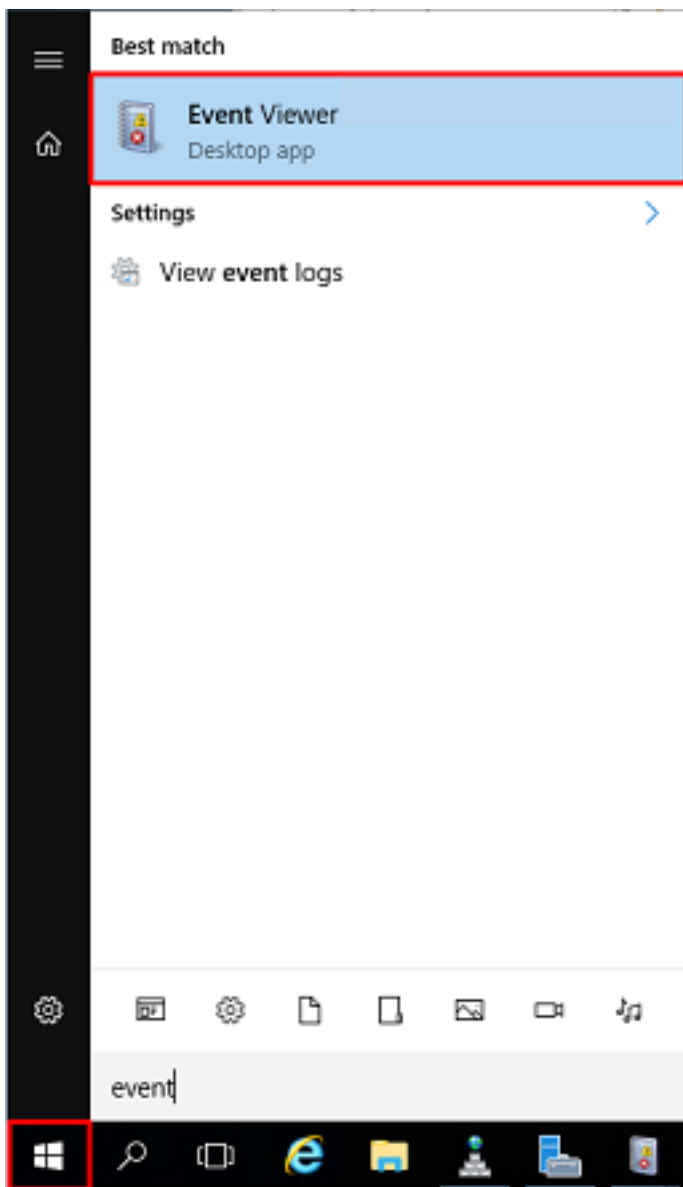
54 packets captured

  1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
  2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
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>
  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>
  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>
[...]
```

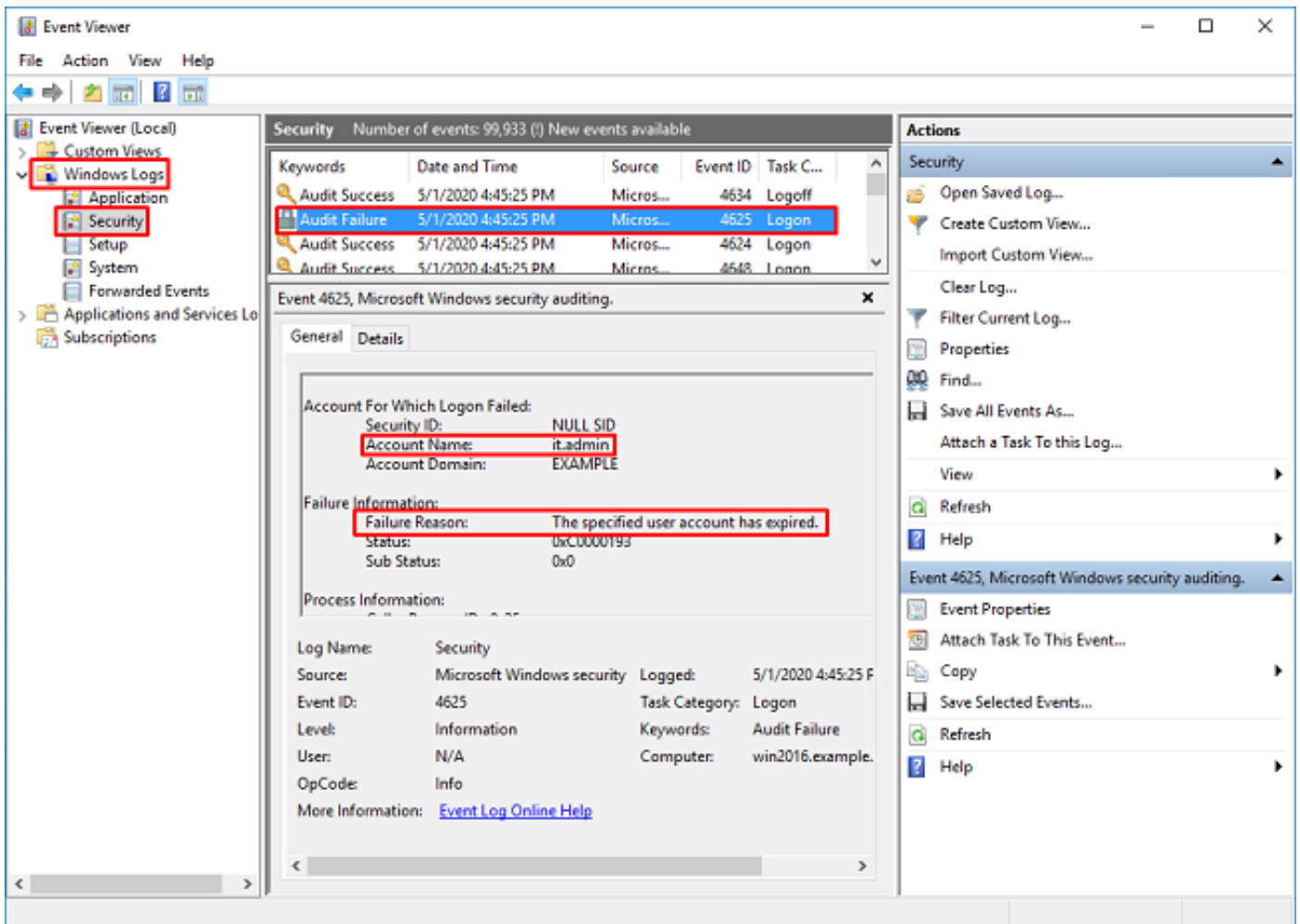
Vastlegging Windows Server Event Viewer

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.



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\$\br/>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