

AD-verificatie (LDAP) en gebruikersidentiteit op FTD beheerd door FMC configureren voor AnyConnect-clients

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram en -scenario](#)

[Active Directory-configuraties](#)

[Bepaal LDAP-basis DN en groep DN](#)

[Een FTD-account maken](#)

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

[Kopieert de SSL-certificaatroot van LDAPS \(alleen vereist voor LDAPS of STARTTLS\).](#)

[FMC-configuraties](#)

[Licentie controleren](#)

[Instellingsgebied](#)

[AnyConnect configureren voor AD-verificatie](#)

[Identiteitsbeleid inschakelen en Beveiligingsbeleid voor gebruikersidentiteit configureren](#)

[NAT-vrijstelling configureren](#)

[Implementeren](#)

[Verifiëren](#)

[Laatste configuratie](#)

[AAA-configuratie](#)

[Configuratie AnyConnect](#)

[Verbinding maken met AnyConnect en toegangscontroleregels controleren](#)

[Verifiëren met FMC Connection-gebeurtenissen](#)

[Problemen oplossen](#)

[Debugs](#)

[LDAP-debuggs werken](#)

[Kan geen verbinding maken met LDAP-server](#)

[Binding Login DN en/of wachtwoord niet correct](#)

[LDAP-server kan de gebruikersnaam niet vinden](#)

[Onjuist wachtwoord voor de gebruikersnaam](#)

[AAA testen](#)

[PacketCapture](#)

[Logbestanden van Windows Server Event Viewer](#)

Inleiding

Dit document beschrijft hoe u AD-verificatie moet configureren voor AnyConnect-clients die verbinding maken met Cisco Firepower Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van RA VPN-configuratie op FMC
- Basiskennis van de LDAP-serverconfiguratie op het VCC
- Basiskennis van **Active Directory (AD)**

Gebruikte componenten

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

- Microsoft 2016-server
- FMCv met 6.5.0
- 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 live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft hoe u **Active Directory (AD)**-verificatie kunt configureren voor **AnyConnect**-clients die verbinding maken met **Cisco Firepower Threat Defence (FTD)**, beheerd door **Firepower Management Center (FMC)**.

Gebruikersidentiteit wordt gebruikt in het toegangsbeleid om AnyConnect-gebruikers te beperken tot specifieke IP-adressen en -poorten.

Configureren

Netwerkdigram en -scenario



Windows-server is vooraf geconfigureerd met IIS en RDP om de gebruikersidentiteit te testen. In deze configuratiehandleiding worden drie gebruikersaccounts en twee groepen aangemaakt.

Gebruikersaccounts:

- **FTD Admin:** Dit wordt gebruikt als de directory account om de FTD te kunnen binden aan de Active Directory-server.
- **IT Admin:** een account van een testbeheerder die wordt gebruikt om de identiteit van de gebruiker aan te tonen.
- **Testgebruiker:** een testgebruikersaccount dat wordt gebruikt om de identiteit van de gebruiker aan te tonen.

Groepen:

- **AnyConnect Admins:** een testgroep waaraan IT-beheerder 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 die de testgebruiker toevoegt om de gebruikersidentiteit aan te tonen. Deze groep heeft alleen HTTP-toegang tot de Windows-server.

Active Directory-configuraties

Om AD-verificatie en gebruikersidentiteit op FTD correct te kunnen configureren, zijn enkele waarden vereist.

Al deze gegevens moeten worden aangemaakt of verzameld op de Microsoft Server voordat de configuratie op FMC kan worden uitgevoerd. De belangrijkste waarden zijn:

- **Domeinnaam:**

Dit is de domeinnaam van de server. In deze configuratiehandleiding is `example.com` de domeinnaam.

- **IP/FQDN-adres voor servers:**

Het IP-adres of FQDN wordt gebruikt om de Microsoft-server te bereiken. Als een FQDN wordt gebruikt, moet een DNS-server worden geconfigureerd binnen FMC en FTD om de FQDN op te lossen.

In deze configuratiehandleiding is deze waarde `win2016.example.com` (die zich oplost in `192.168.1.1`).

- **Serverpoort:**

De poort die wordt gebruikt door de LDAP-service. Standaard gebruiken LDAP en STARTTLS TCP-poort 389 voor LDAP en gebruikt LDAP over SSL (LDAPS) TCP-poort 636.

- **Root-CA:**

Als LDAPS of STARTTLS wordt gebruikt, is de wortel CA die wordt gebruikt om het SSL certificaat te ondertekenen dat door LDAPS wordt gebruikt vereist.

- **Gebruikersnaam en wachtwoord map:**

Dit is de account die door FMC en FTD wordt gebruikt om te binden aan de LDAP-server en gebruikers te verifiëren en te zoeken naar gebruikers en groepen.

Hiervoor wordt een account met de naam FTD Admin aangemaakt.

- **Voornaam (DN) van basis- en groep:**

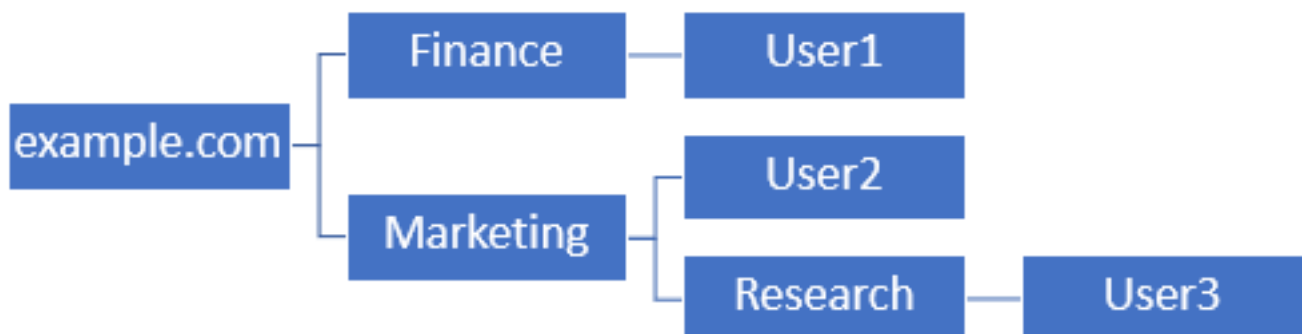
De Base DN is het startpunt FMC en de FTD vertelt de Active Directory om te beginnen met het zoeken naar en authenticeren van gebruikers.

Op dezelfde manier is de Groep DN het uitgangspunt FMC vertelt de Active Directory waar te beginnen zoeken naar groepen voor gebruikersidentiteit.

In deze configuratiegids, wordt het worteldomein example.com gebruikt als Basis DN en Groep DN.

Voor een productieomgeving is het echter beter om een **Base DN** en **Group DN** verder binnen de LDAP-hiërarchie te gebruiken.

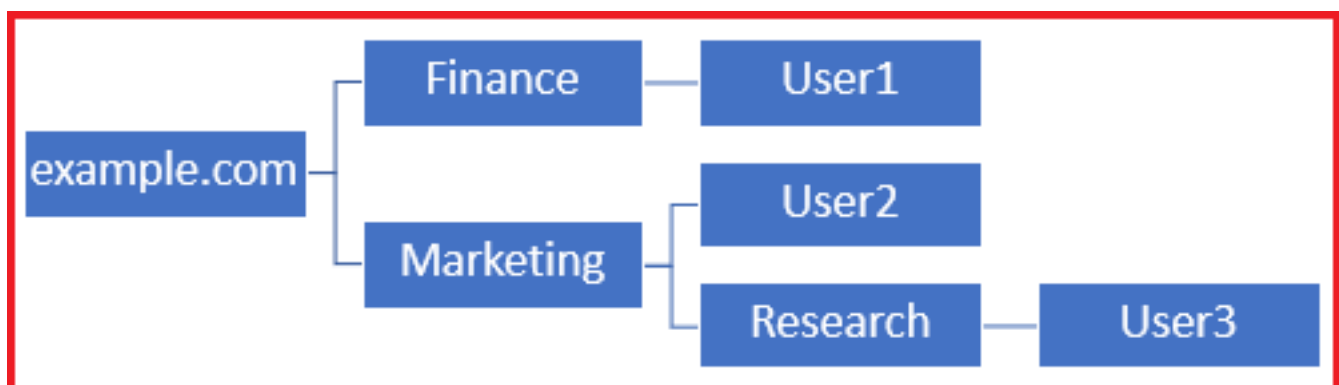
Deze LDAP-hiërarchie bijvoorbeeld:



Als een beheerder wil dat gebruikers binnen de organisatorische eenheid **Marketing** de basis-DN kunnen verifiëren kan worden ingesteld op de root (example.com).

Echter, dit maakt het ook mogelijk dat Gebruiker1 onder de **Finance** organisatieafdeling ook inlogt, aangezien het zoeken van de gebruiker begint bij de wortel en gaat naar **Finance, Marketing** en **Research**.

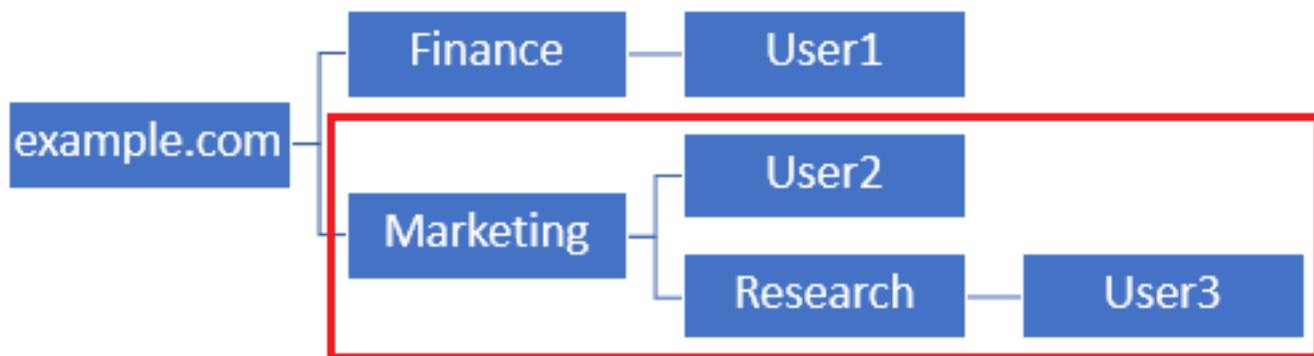
Base-DN ingesteld op example.com



Om logins te beperken tot de enige gebruiker in de **Marketing** organisatorische eenheid en hieronder, kan de beheerder in plaats daarvan de Base DN instellen op **Marketing**.

Alleen Gebruiker2 en Gebruiker3 kunnen nu authenticeren omdat de zoekactie begint bij **Marketing**.

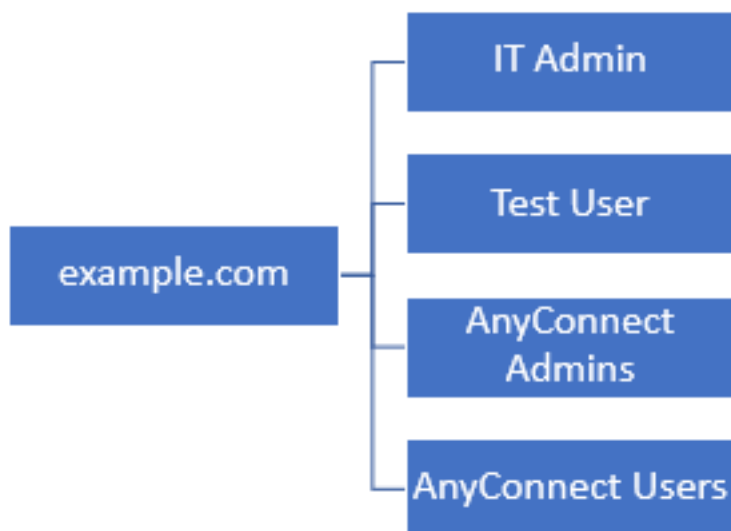
Base-DN ingesteld op Marketing



Merk op dat voor meer granulaire controle binnen de FTD waarvoor gebruikers verschillende autorisaties kunnen verbinden of toewijzen op basis van hun AD-kenmerken, een LDAP-autorisatiekaart moet worden geconfigureerd.

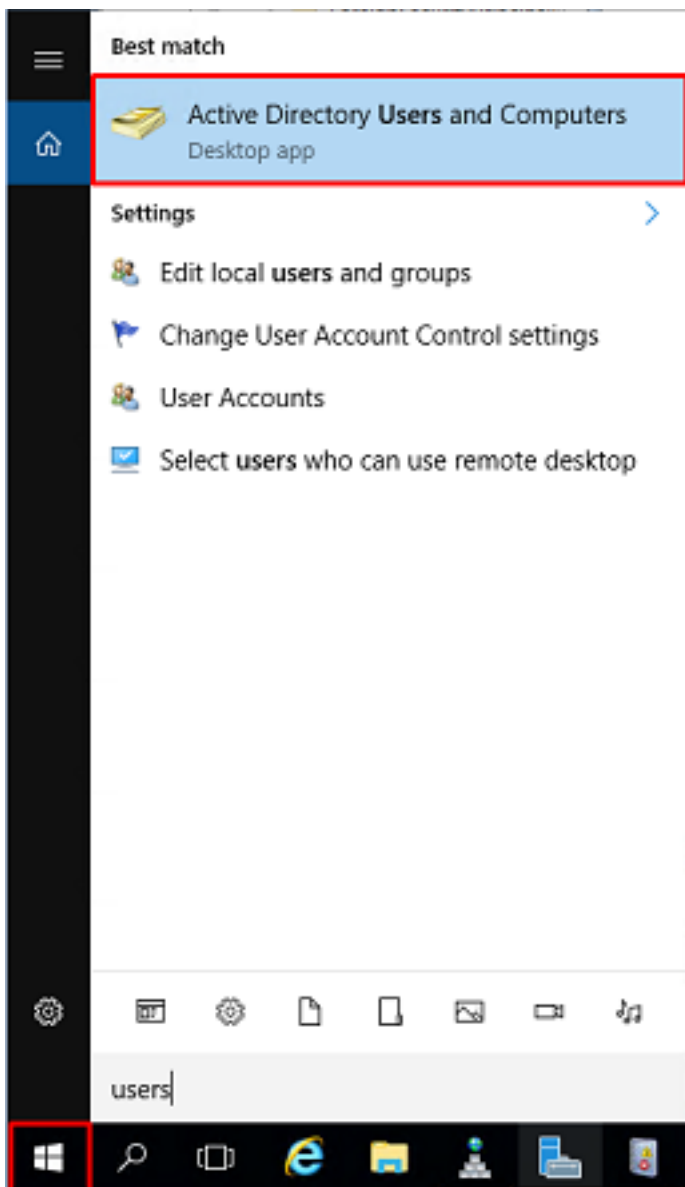
Meer informatie hierover kunt u hier vinden: [AnyConnect LDAP-mapping configureren op Firepower Threat Defence \(FTD\)](#).

Deze vereenvoudigde LDAP-hiërarchie wordt gebruikt in deze configuratiehandleiding en de DN voor de root example.com wordt gebruikt voor zowel de Base-DN als de Groep-DN.

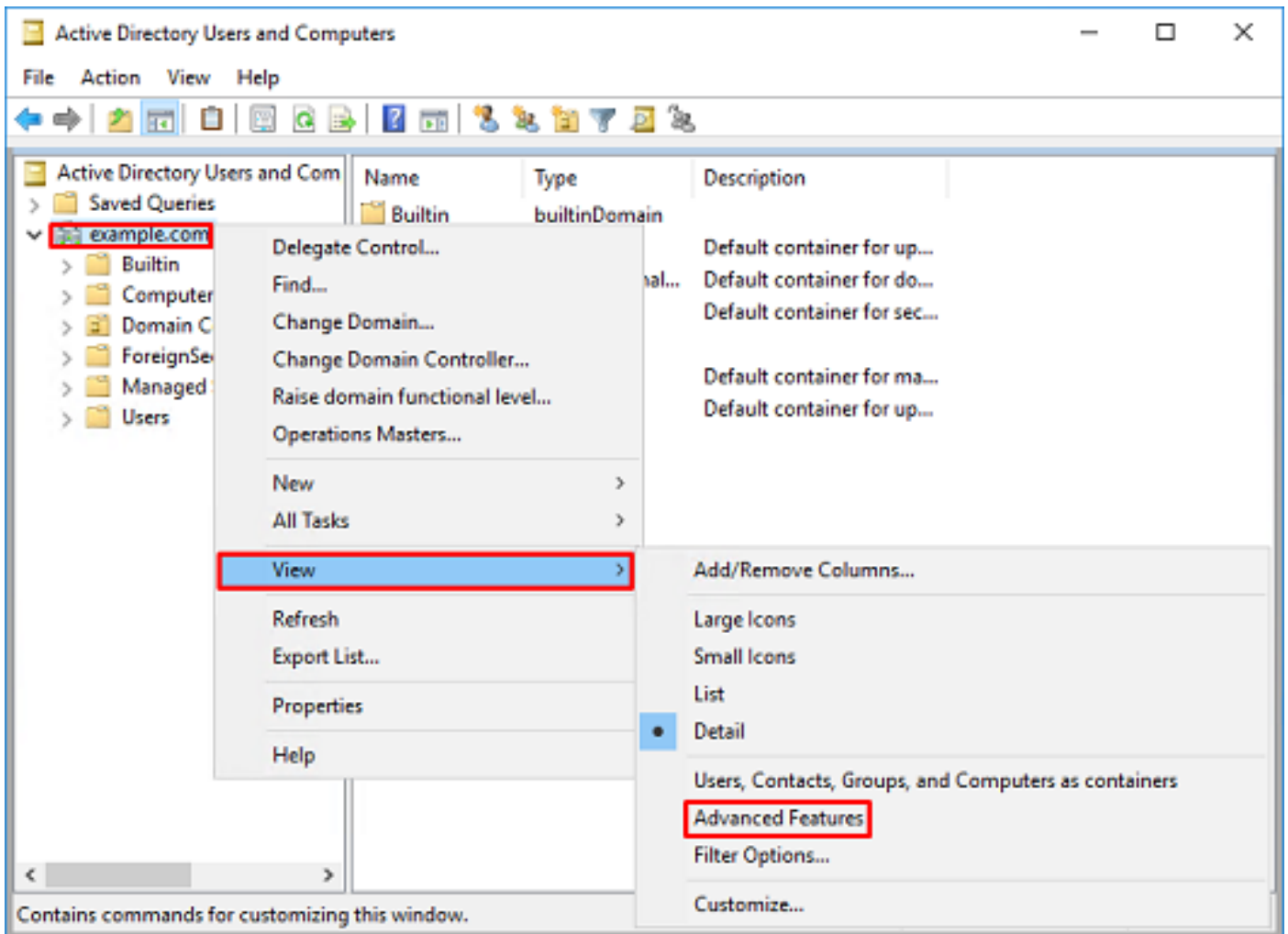


Bepaal LDAP-basis DN en groep DN

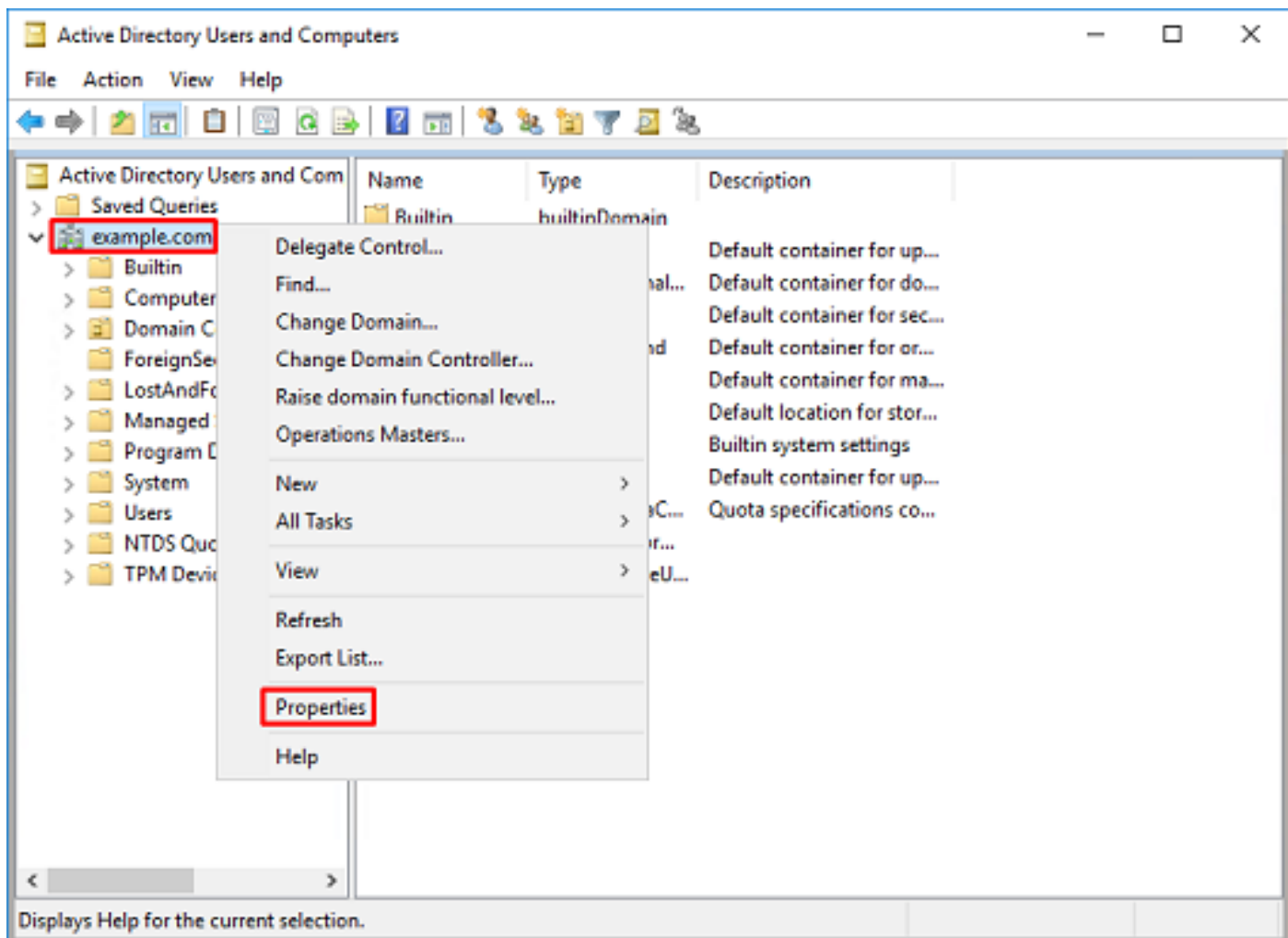
1. Open **Active Directory-gebruikers en -computers**.



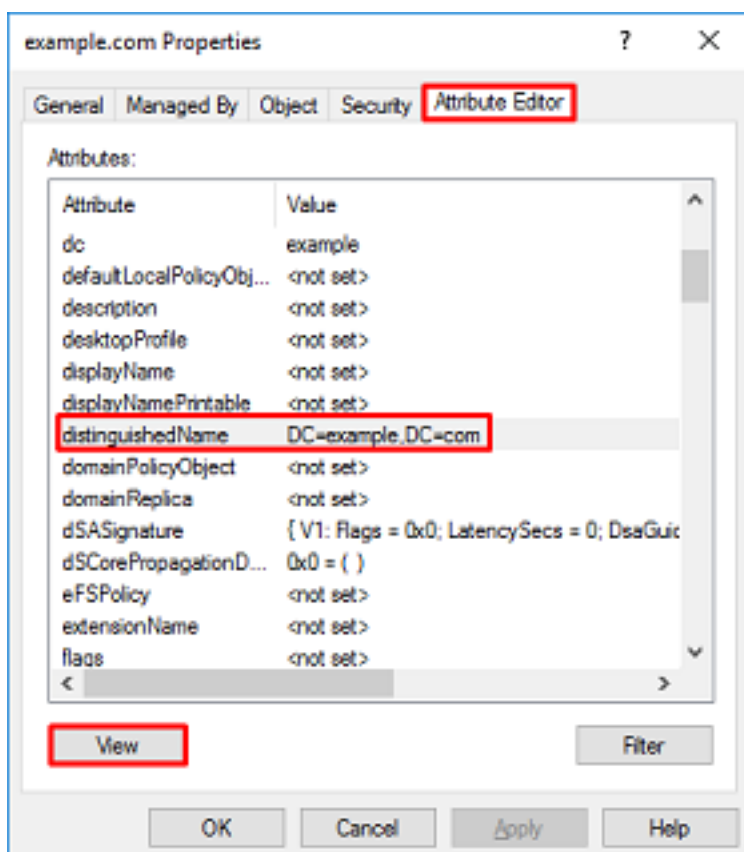
2. Klik met de linkermuisknop op **rootdomein** (om de container te openen), klik met de rechtermuisknop op het **rootdomein**, en klik vervolgens onder **Weergave**, op **Geavanceerde functies**.



3. Hierdoor kunnen extra eigenschappen worden weergegeven onder de AD-objecten. Bijvoorbeeld, om DN voor de wortel example.com te vinden, klik example.com met de rechtermuisknop en kies dan **Eigenschappen**.

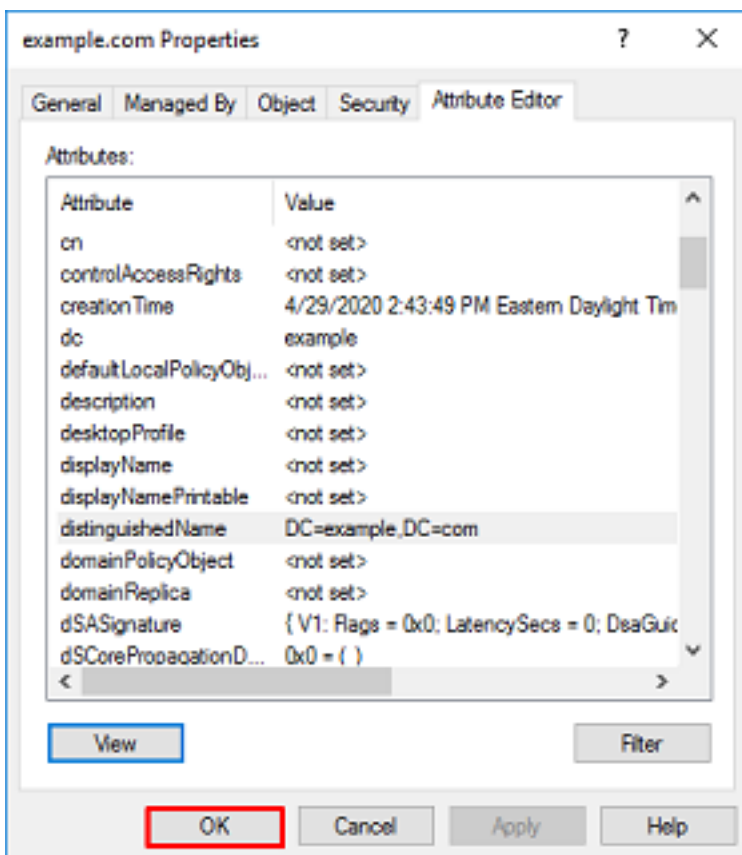
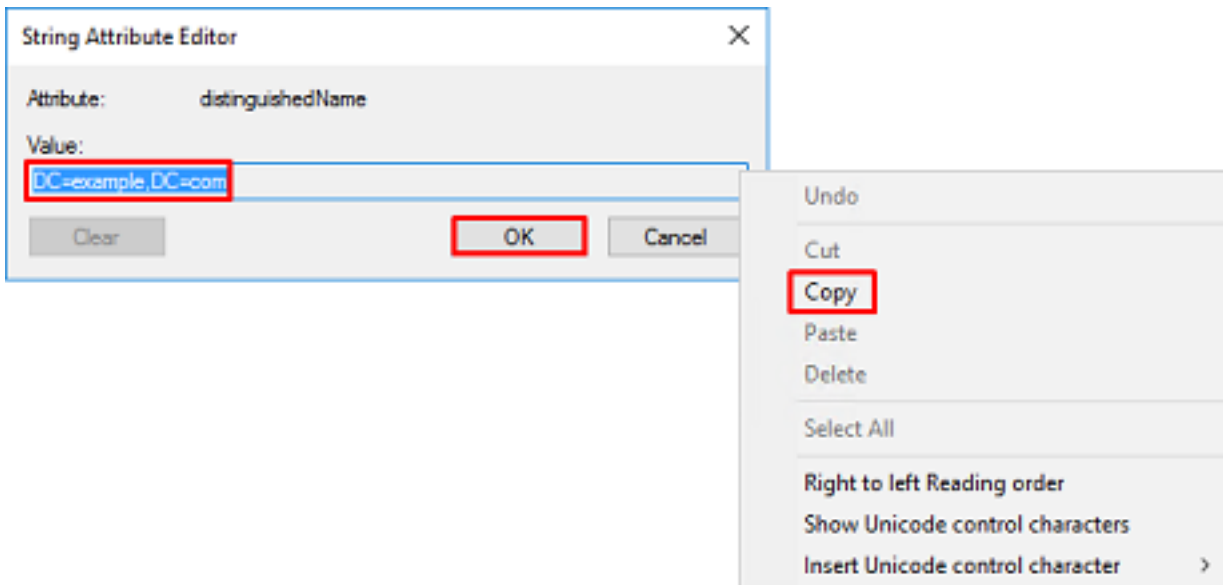


4. Selecteer onder **Proprieties** het tabblad **Attribute Editor**. Vind **voornaamNaam** onder de **Kenmerken**, dan klik op **Weergeven**.

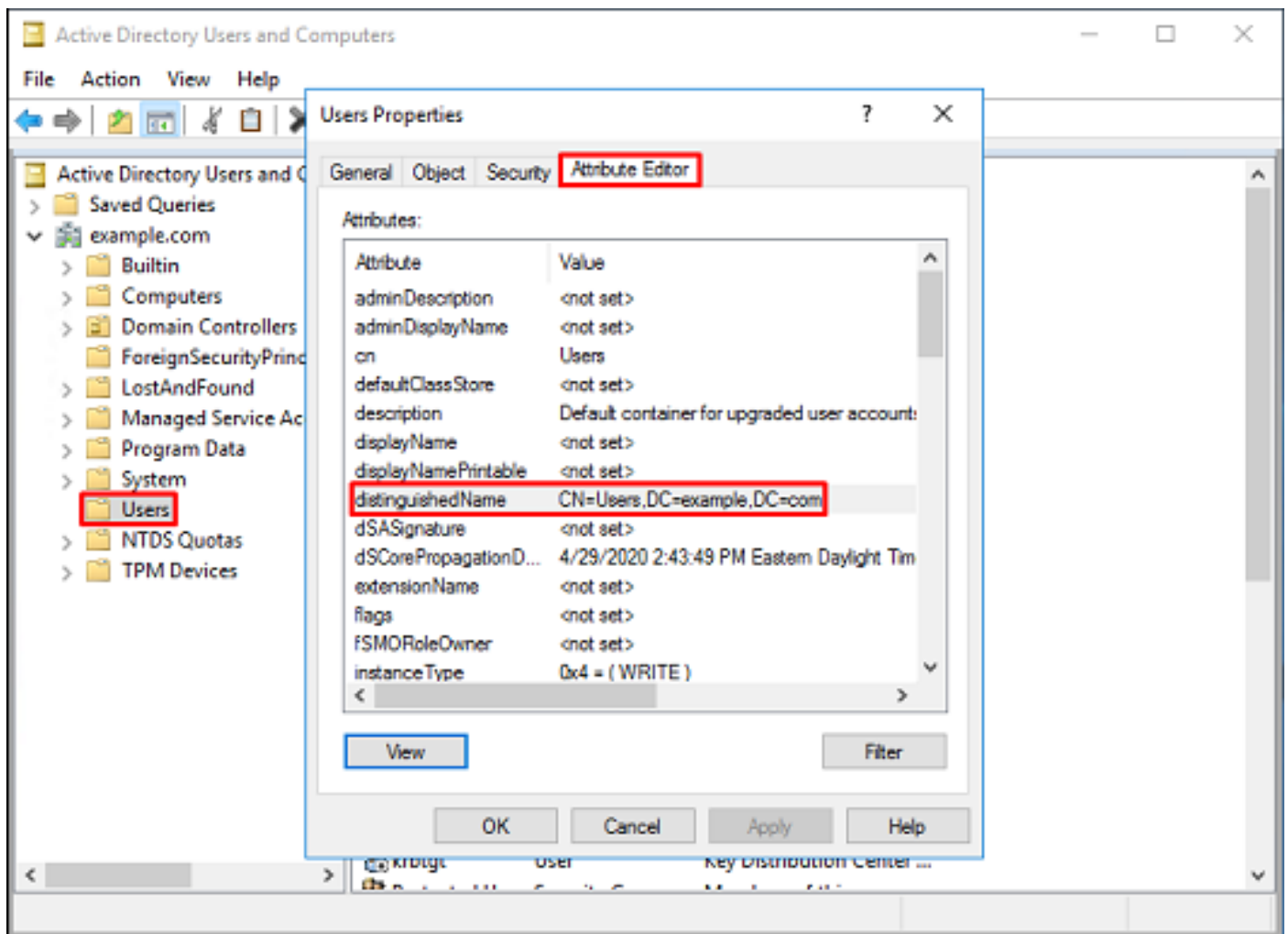


5. Hierdoor wordt een nieuw venster geopend waarin de DN kan worden gekopieerd en later in het VCC kan worden geplakt. In dit voorbeeld, de wortel DN is DC=example, DC=com.

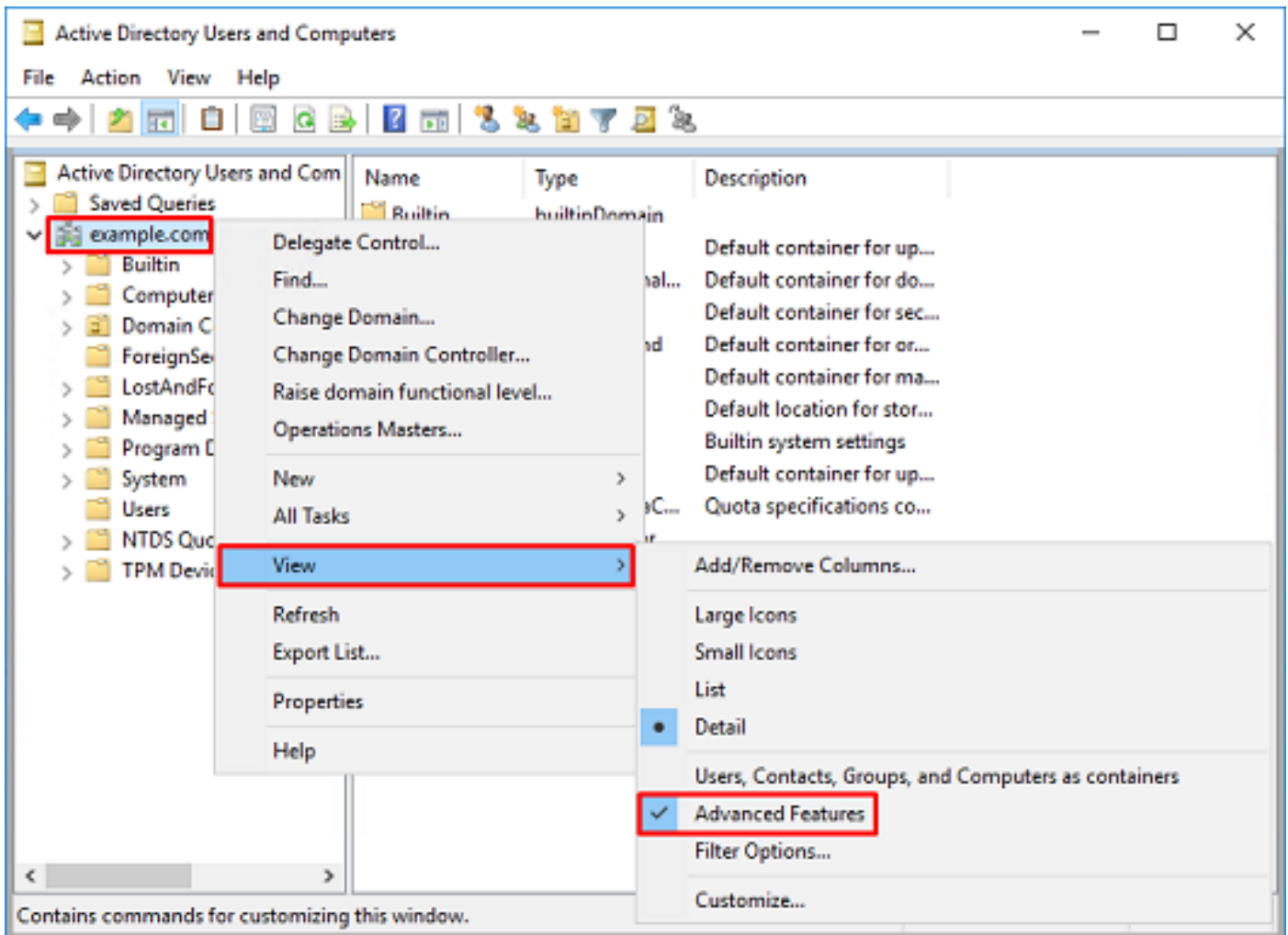
Kopieert de waarde en slaat deze op voor later. Klik op **OK** om het venster **String Attribute Editor** te verlaten en klik nogmaals op **OK** om de **Proprieties** te verlaten.



Dit kan worden gedaan voor meerdere objecten in **Active Directory**. Deze stappen worden bijvoorbeeld gebruikt om de DN van de **User**-container te vinden:



6. De weergave **Geavanceerde functies** kan worden verwijderd door nogmaals op de hoofdletter DN te klikken en vervolgens onder **Beeld**, klik nogmaals op **Geavanceerde functies**.



Een FTD-account maken

Met deze gebruikersaccount kunnen FMC en FTD met de actieve directory binden om naar gebruikers en groepen te zoeken en gebruikers te verifiëren.

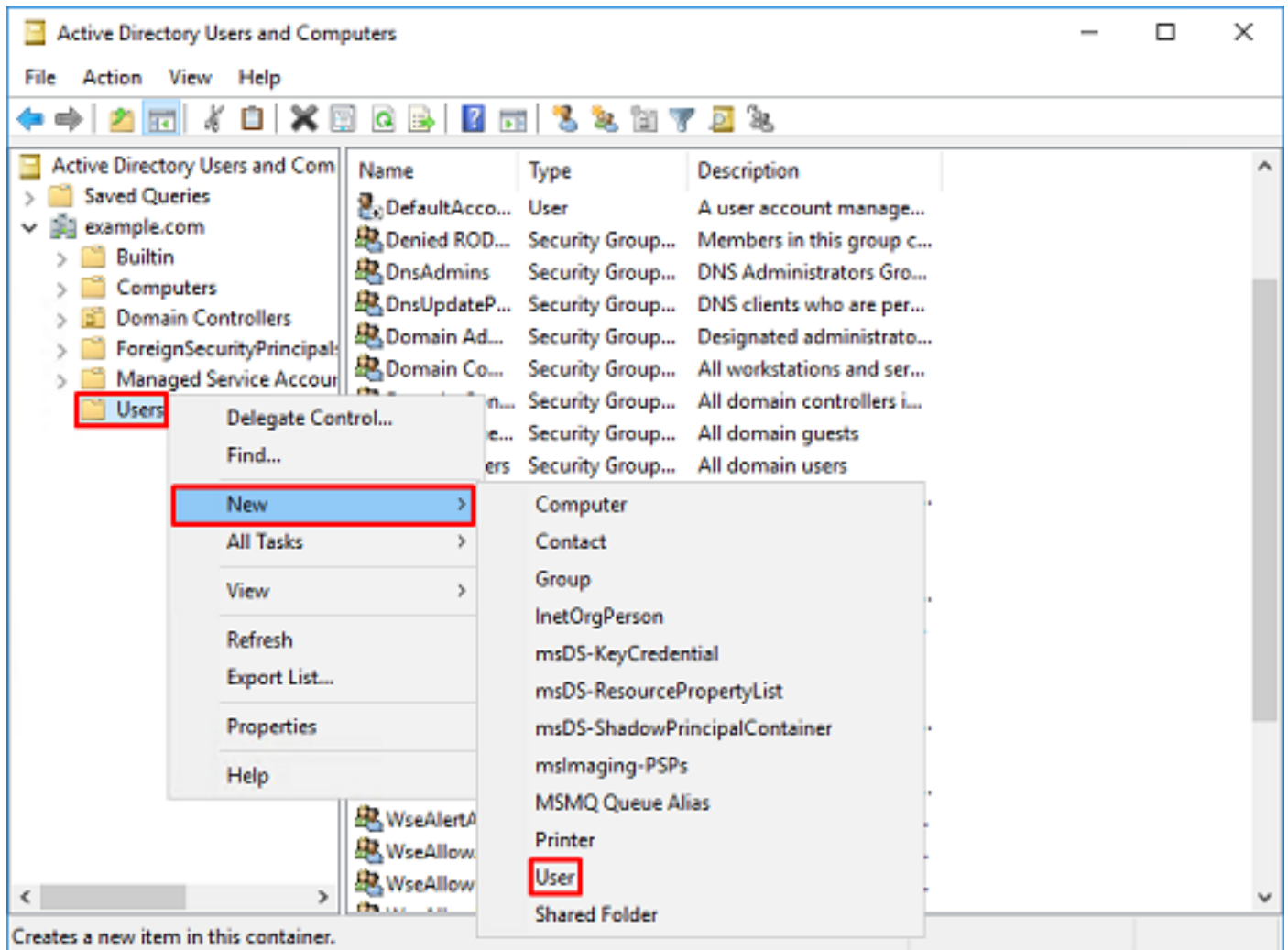
Het doel van het creëren van een afzonderlijke FTD-account is om onbevoegde toegang elders in het netwerk te voorkomen als de referenties die worden gebruikt voor de binding worden gecompromitteerd.

Deze account hoeft niet binnen het bereik van de Base DN of Group DN te vallen.

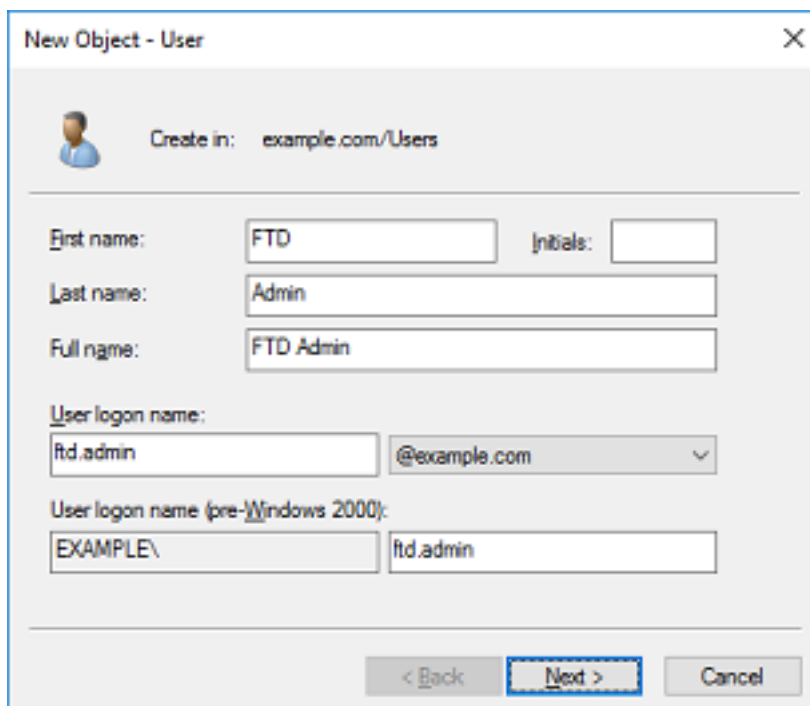
1. Klik in **Active Directory User and Computers** met de rechtermuisknop op de container/organisatie waaraan de FTD-account wordt toegevoegd.

In deze configuratie wordt de FTD-account toegevoegd onder de **User** container onder de gebruikersnaam fd.admin@example.com.

Klik met de rechtermuisknop op **Gebruikers** en navigeer vervolgens naar **Nieuw > Gebruiker**.



2. Ga door het Nieuwe Voorwerp - de Toveraar van de 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:

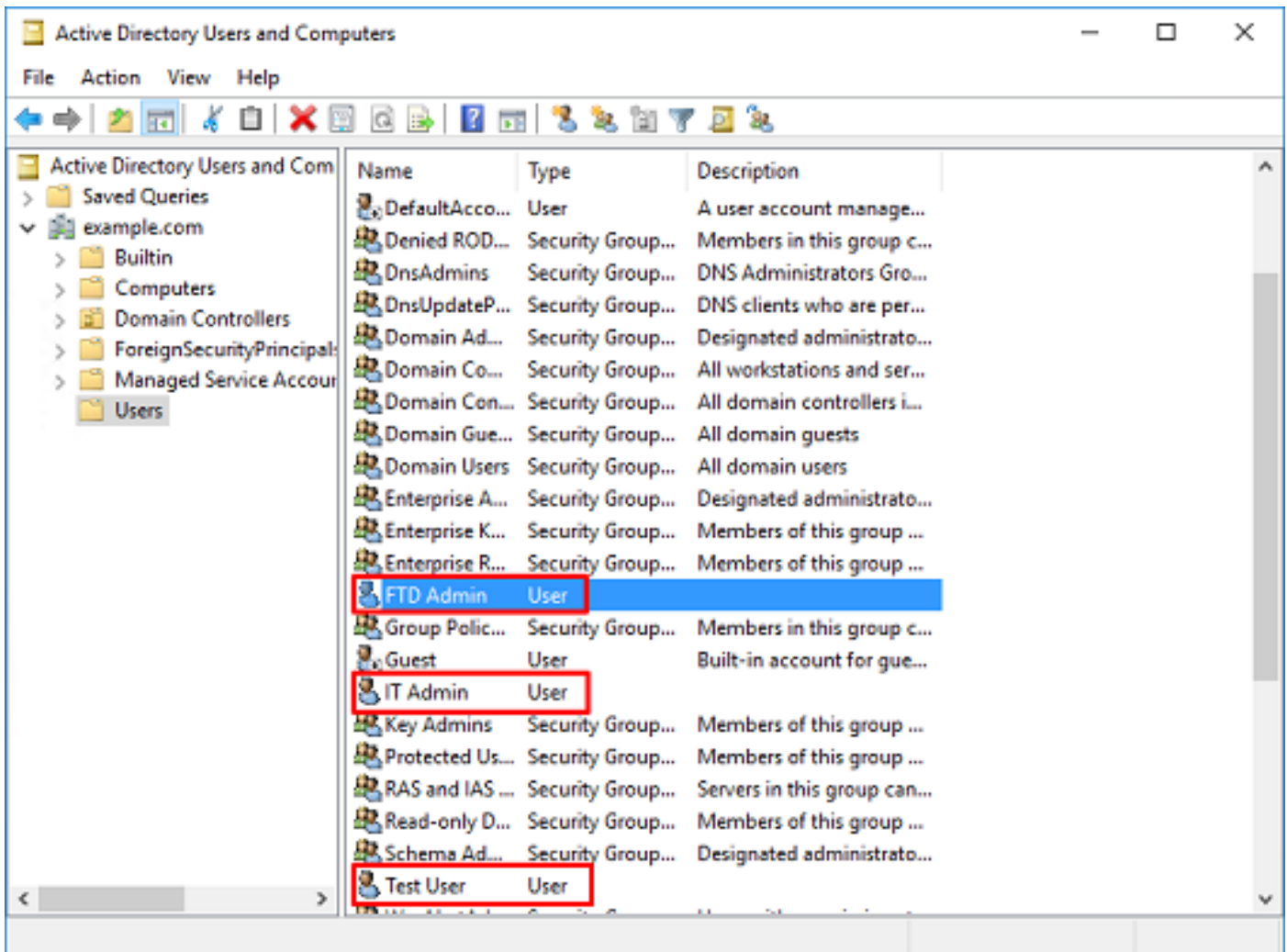
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

3. Controleer of de **FTD-account** is aangemaakt. Er worden twee extra accounts aangemaakt: **IT-beheerder** en **testgebruiker**.



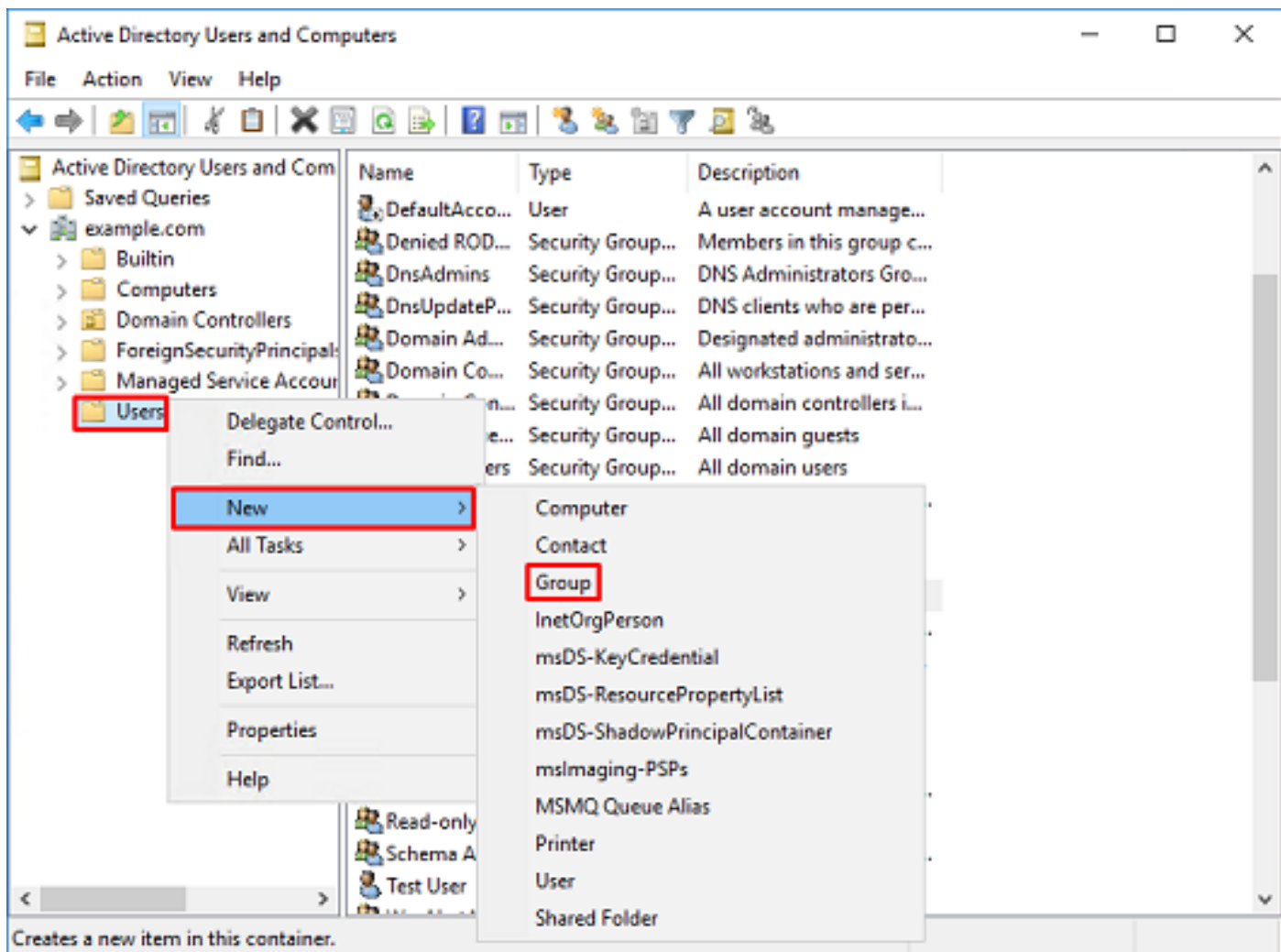
AD-groepen maken en gebruikers toevoegen aan AD-groepen (optioneel)

Hoewel dit niet nodig is voor verificatie, kunnen groepen worden gebruikt om het gemakkelijker te maken om toegangsbeleid toe te passen op meerdere gebruikers en LDAP-autorisatie.

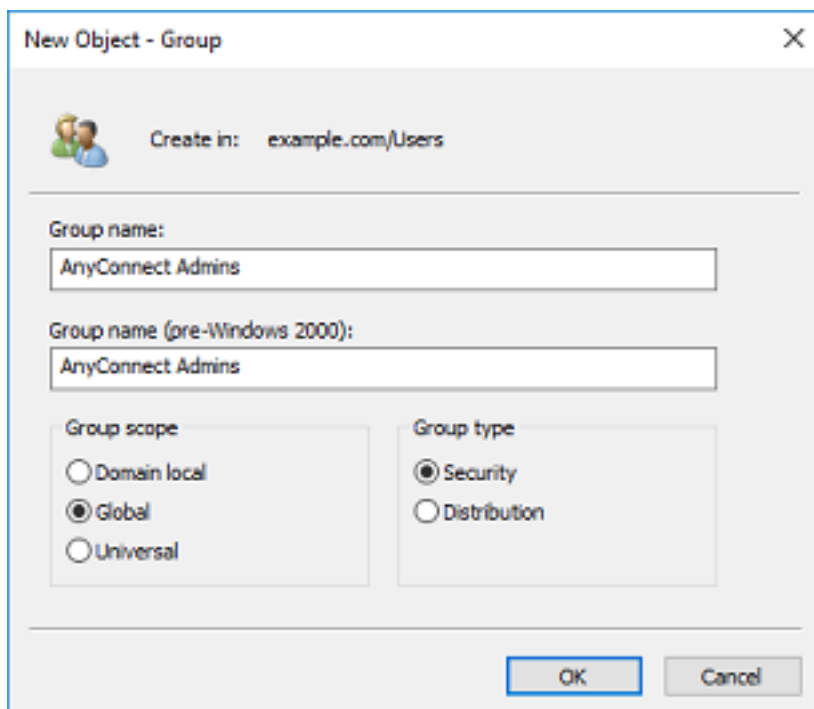
In deze configuratiegids worden groepen gebruikt om later via gebruikersidentiteit binnen FMC instellingen voor toegangscontrole toe te passen.

1. Klik in **Active Directory User and Computers** met de rechtermuisknop op de container of de organisatorische eenheid waaraan de nieuwe groep wordt toegevoegd.

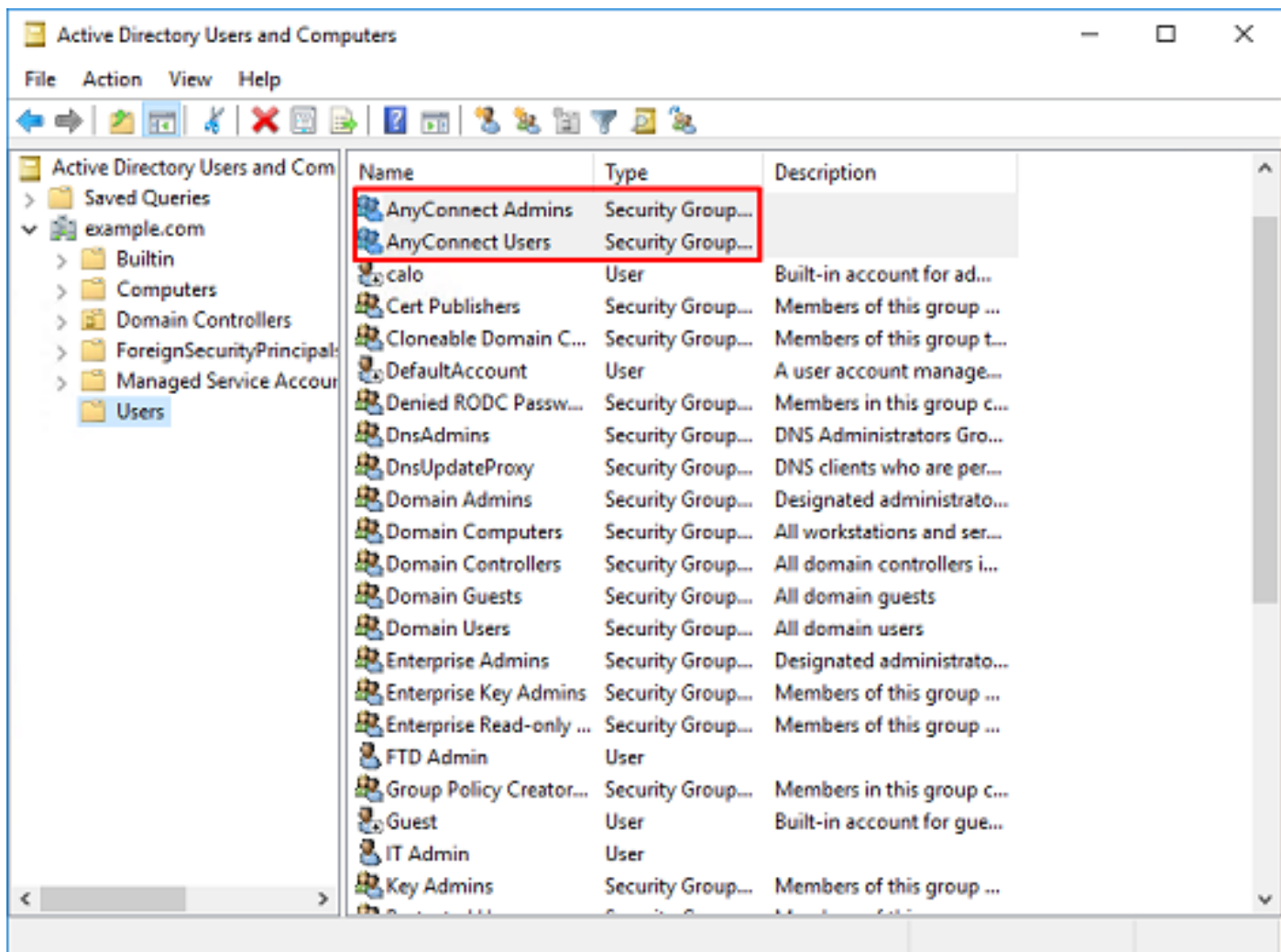
In dit voorbeeld wordt de groep AnyConnect Admins toegevoegd onder de container **Gebruikers**. Klik met de rechtermuisknop op **Gebruikers** en navigeer vervolgens naar **Nieuw > Groepen**.



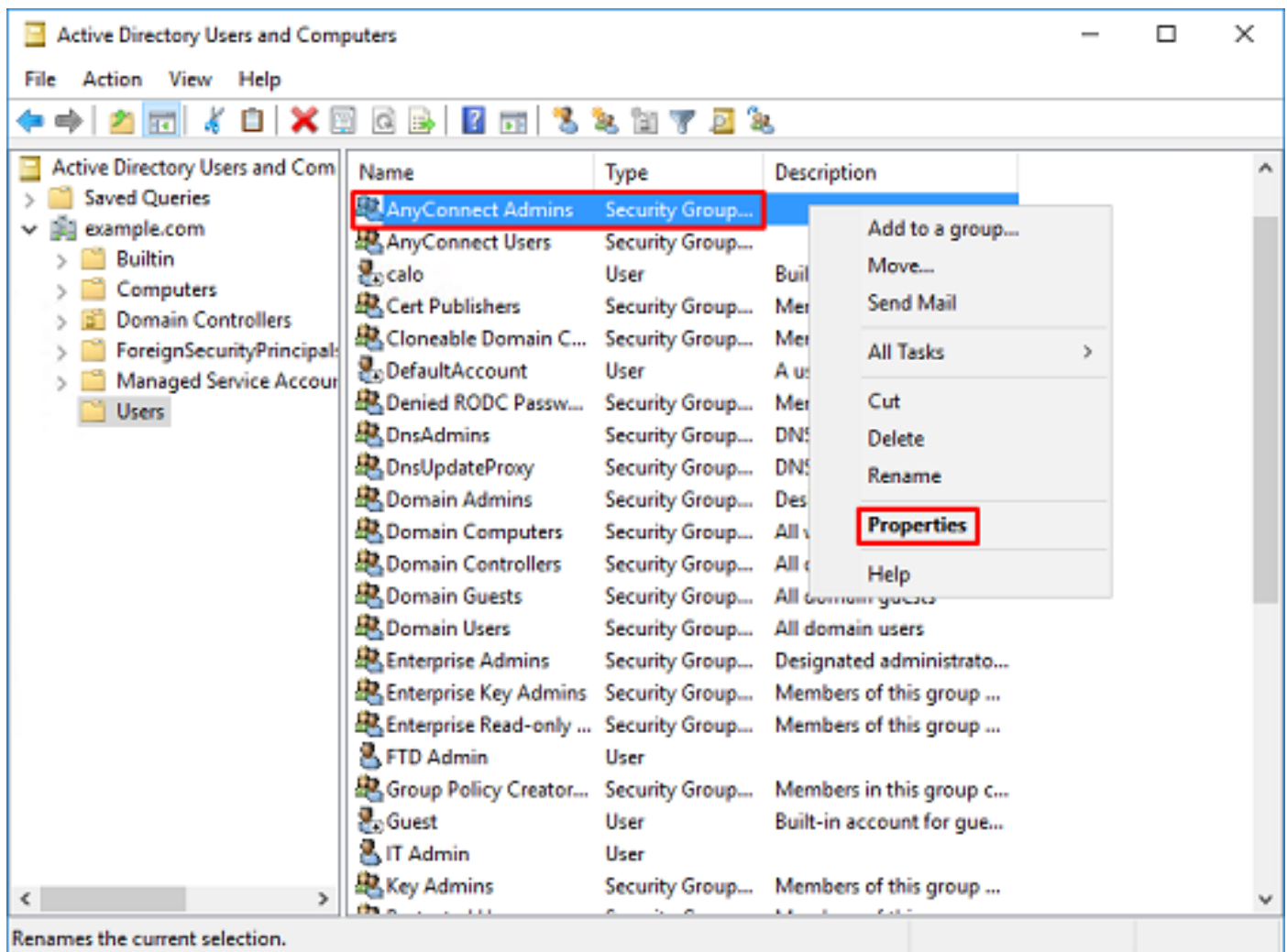
2. Ga door de Wizard Nieuw object - Groep.



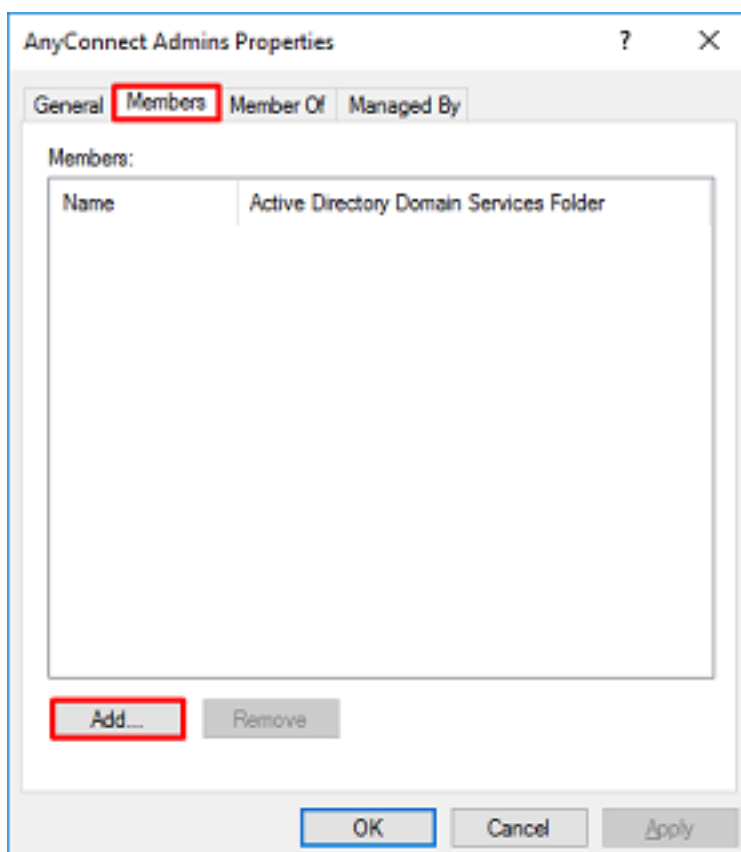
3. Controleer of de groep is gemaakt. De **AnyConnect**-gebruikersgroep is ook gemaakt.



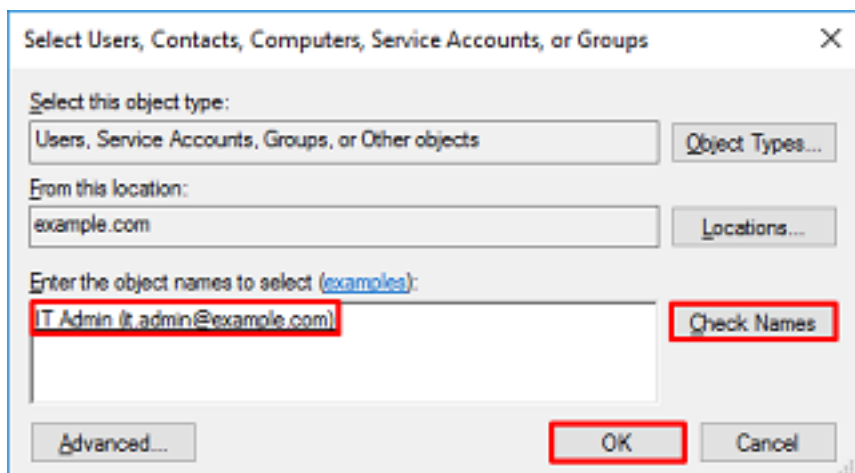
4. Klik met de rechtermuisknop op de groep van de gebruiker(s) en kies vervolgens **Eigenschappen**. In deze configuratie wordt de IT-beheerder van de gebruiker toegevoegd aan de groep AnyConnect-beheerders en wordt de **testgebruiker** toegevoegd aan de groep **AnyConnect-gebruikers**.



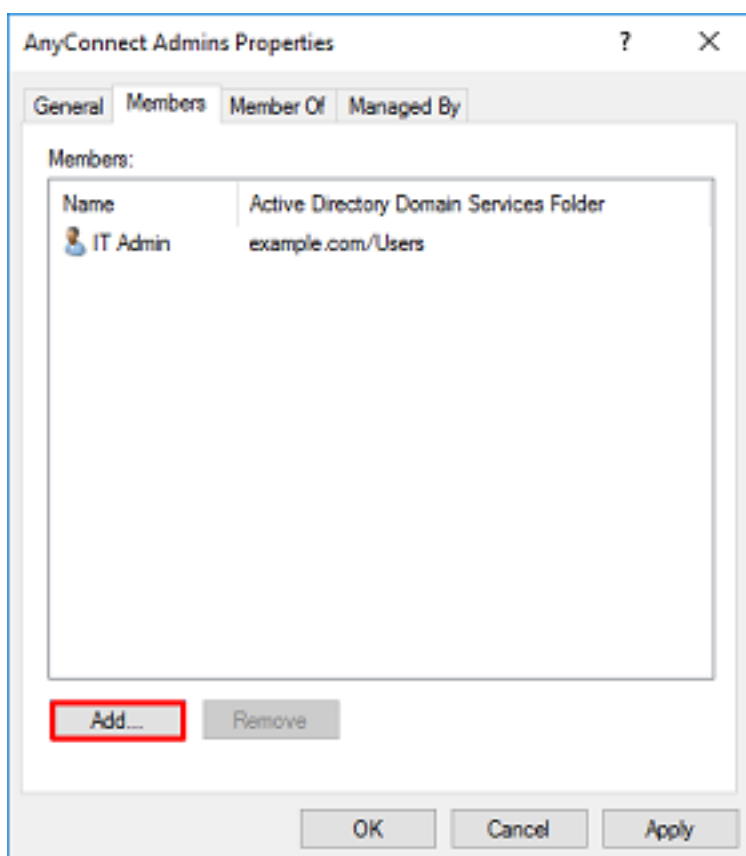
5. Klik onder het tabblad Leden op Toevoegen.



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

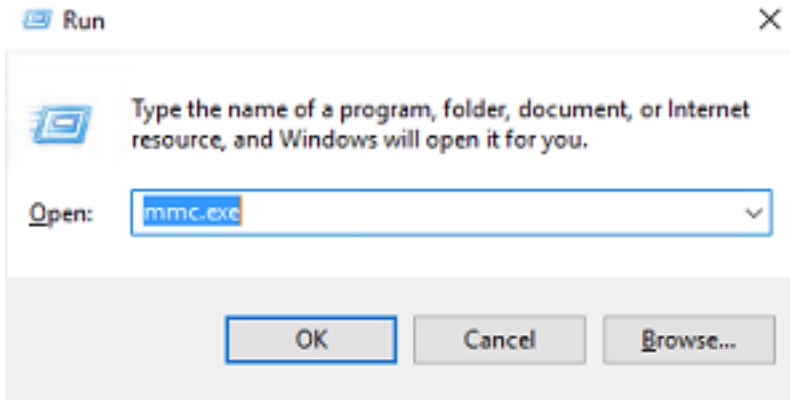


Controleer of de juiste gebruiker is toegevoegd en klik op de knop OK. De gebruiker **Test User** wordt ook toegevoegd aan de groep **AnyConnect-gebruikers** met dezelfde stappen.

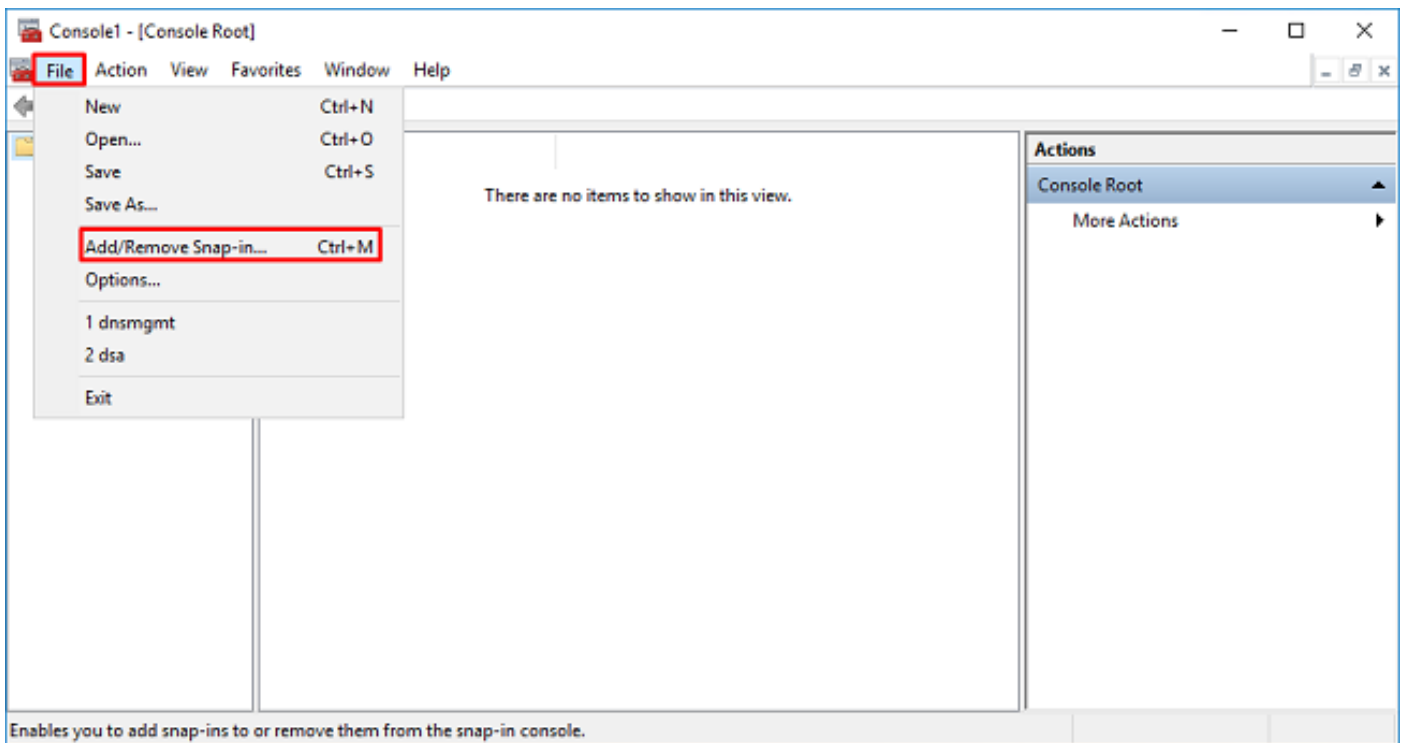


Kopieert de SSL-certificaattoet van LDAPS (alleen vereist voor LDAPS of STARTTLS).

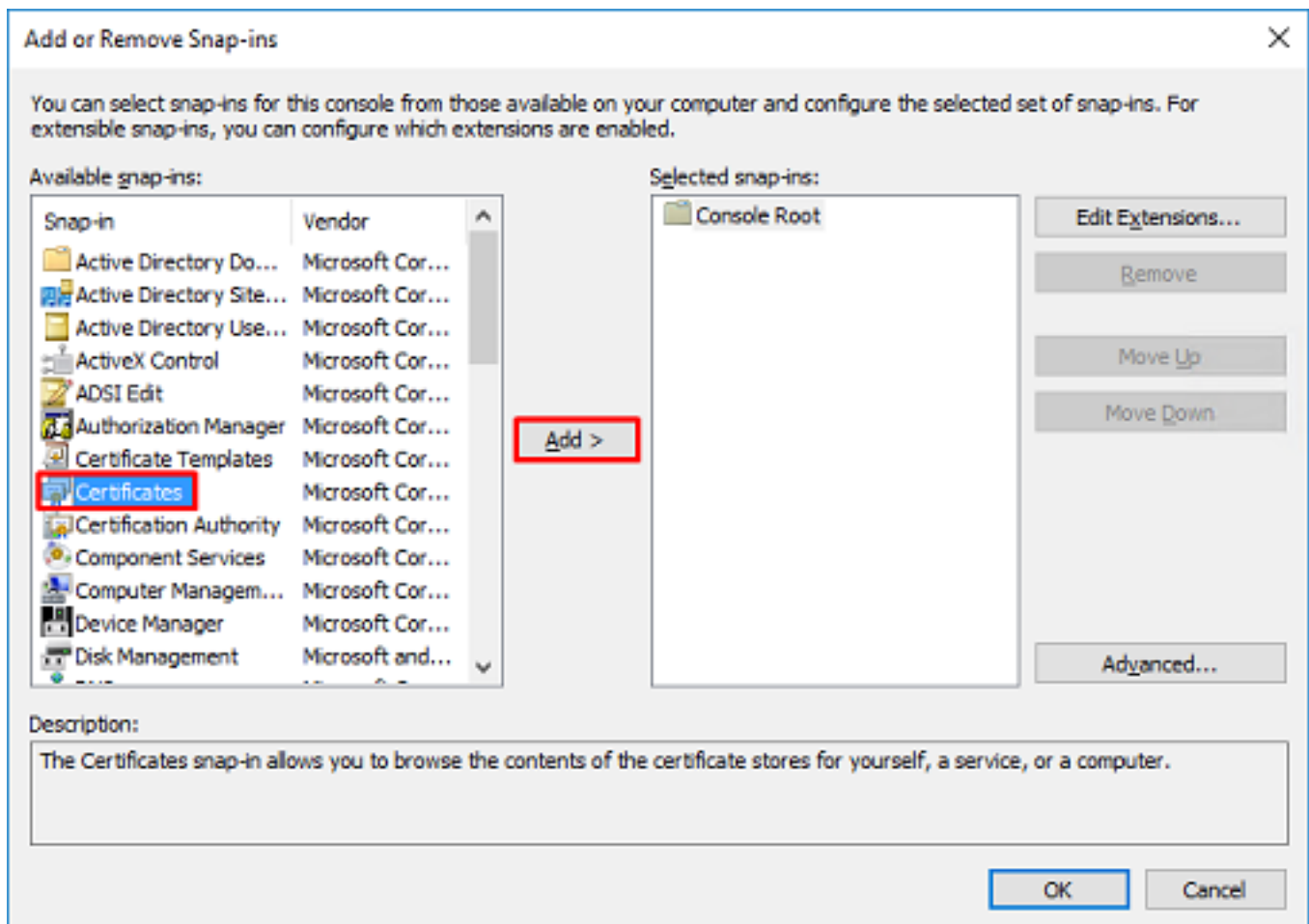
1. Druk op **Win+R** en voer **mmc.exe** in. klik vervolgens op OK.



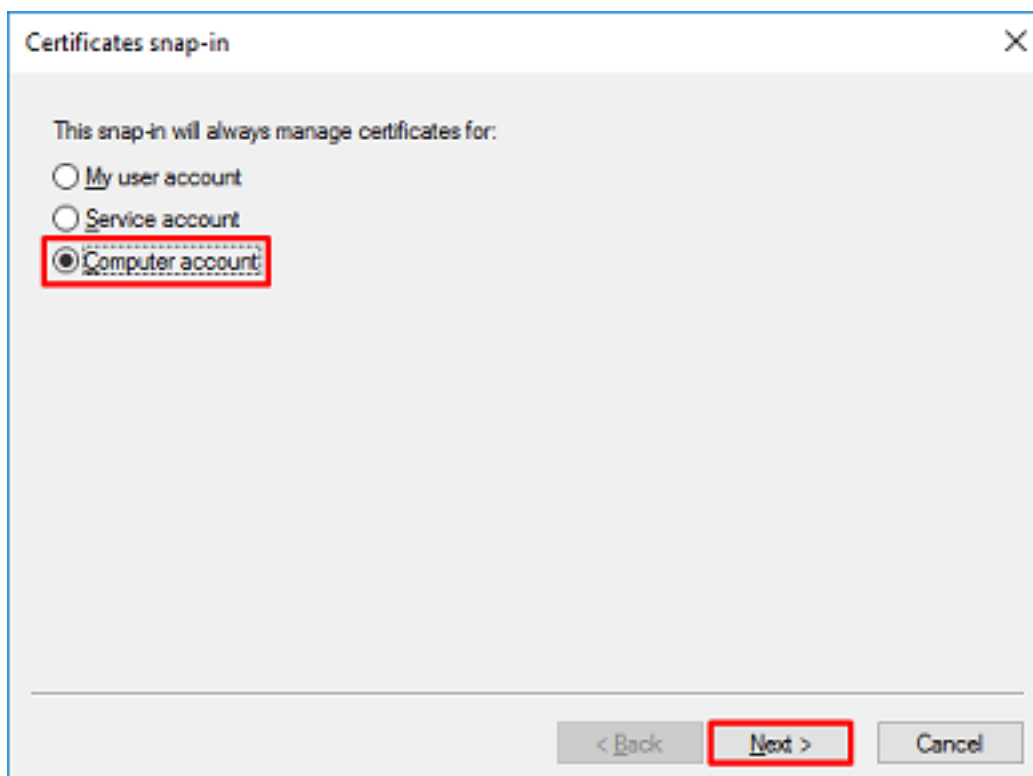
2. Navigeer naar **Bestand > Magnetisch toevoegen/verwijderen...**



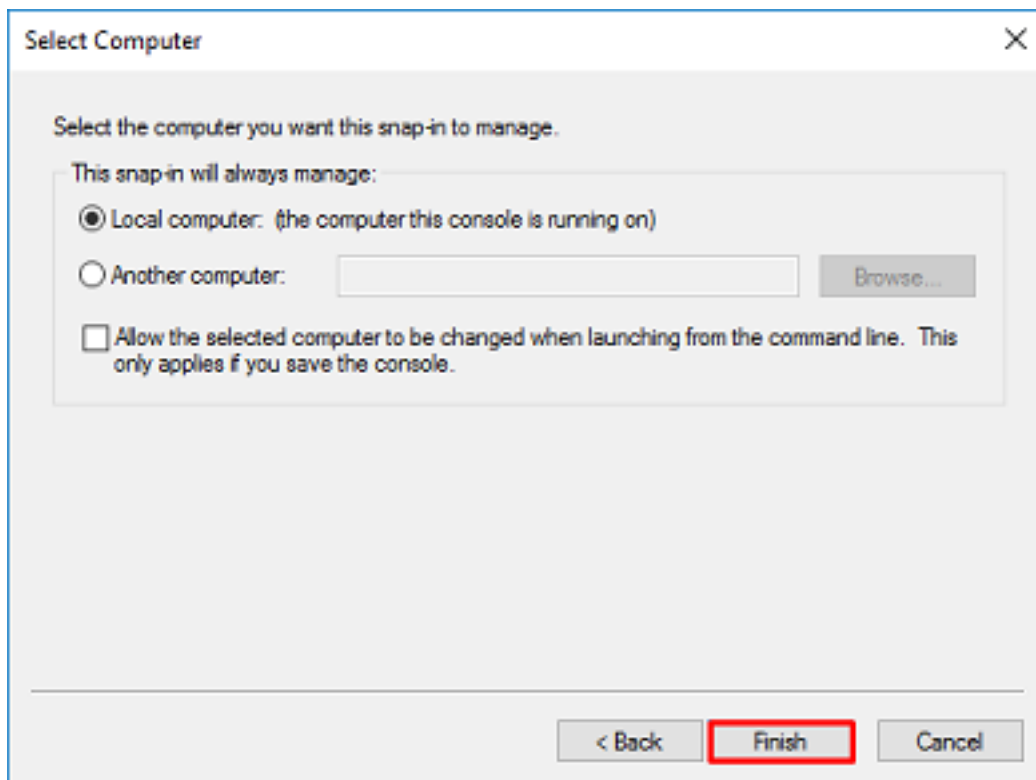
3. Selecteer onder Beschikbare invoegtoepassingen de optie **Certificaten** en klik vervolgens op **Toevoegen**.



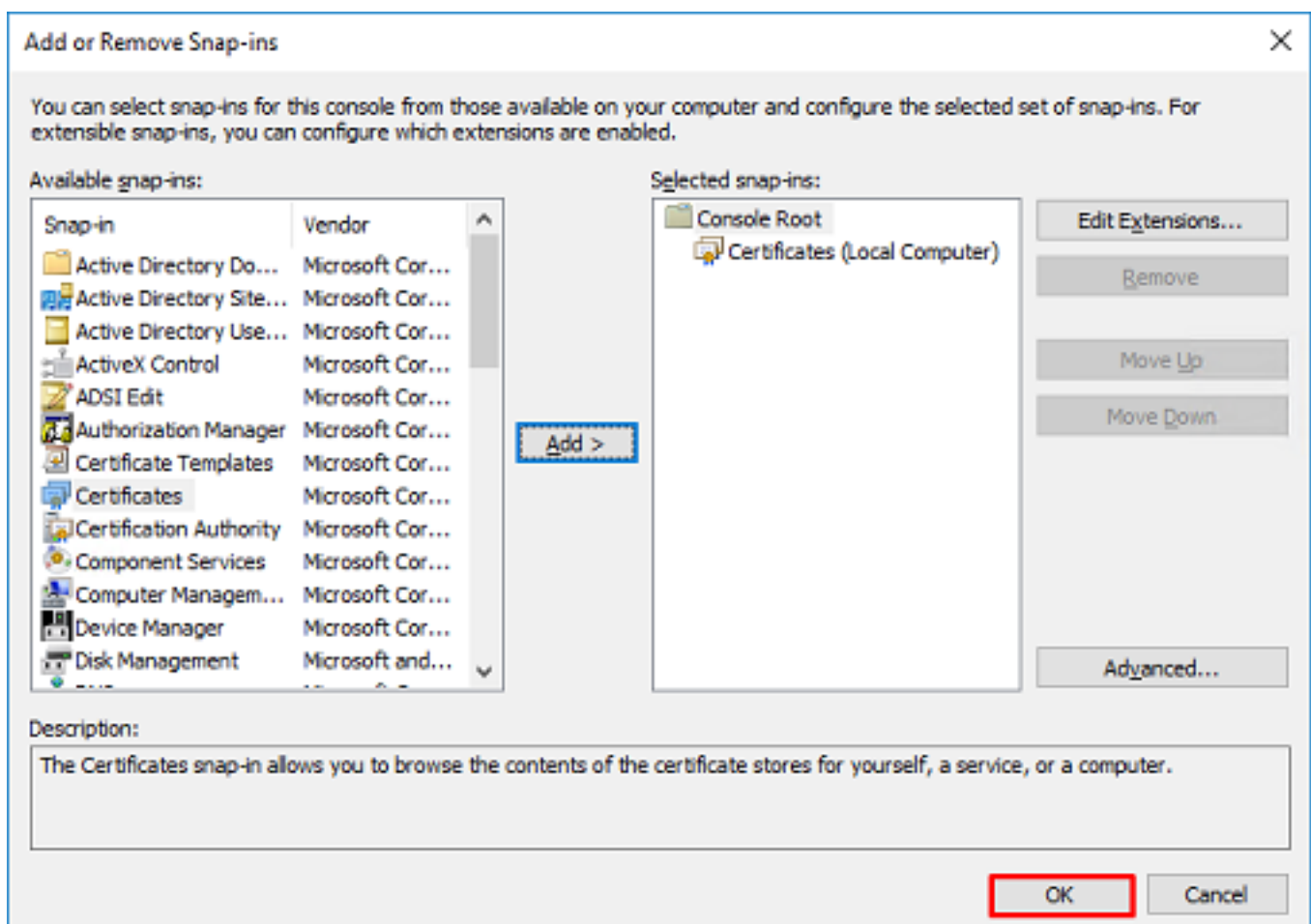
4. Selecteer **Computer-account** en klik op **Volgende**.



Klik op **Finish** (Voltooien).



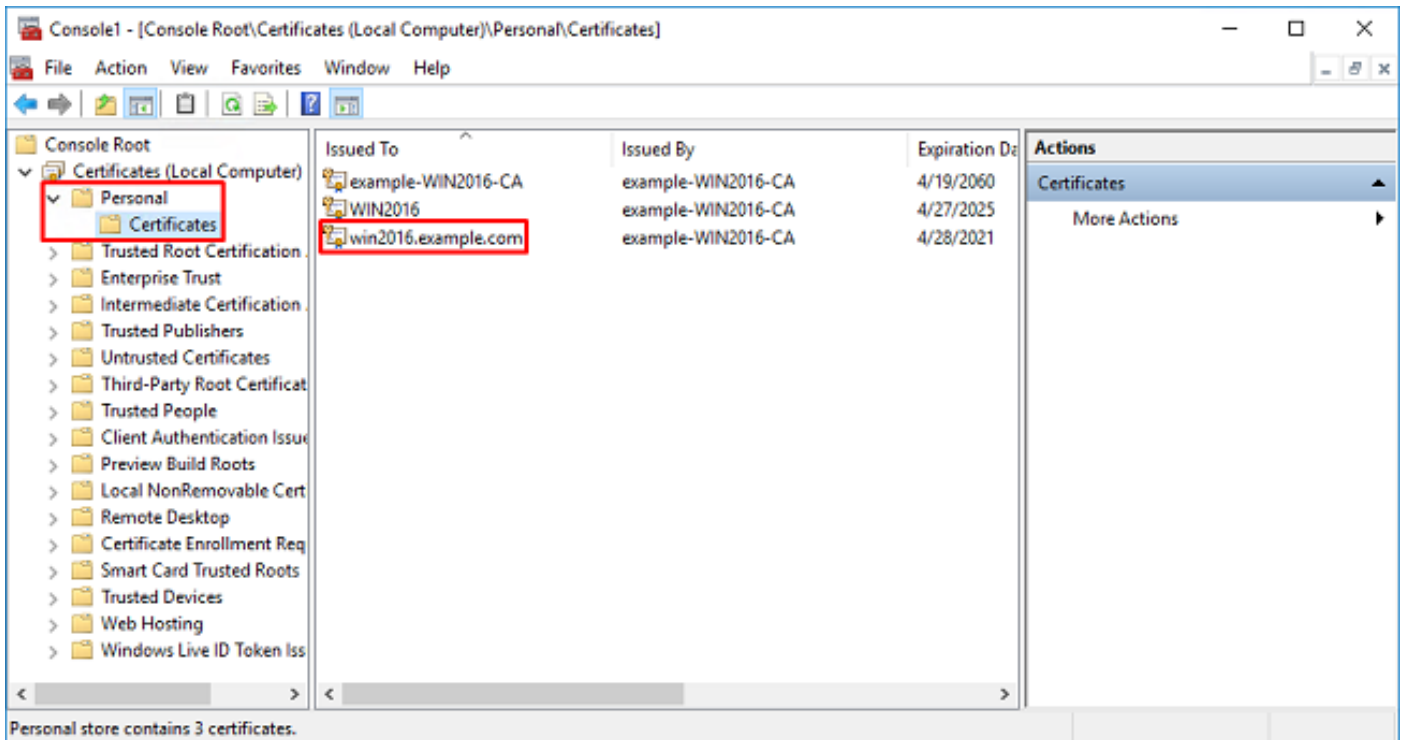
5. Klik nu op **OK**.



6. Vouw de **persoonlijke** map uit en klik vervolgens op **Certificaten**. Het door LDAPS gebruikte certificaat wordt afgegeven aan de **volledig gekwalificeerde domeinnaam (FQDN)** van de Windows-server. Op deze server staan 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 aan win2016.example.com door voorbeeld-WIN2016-CA.

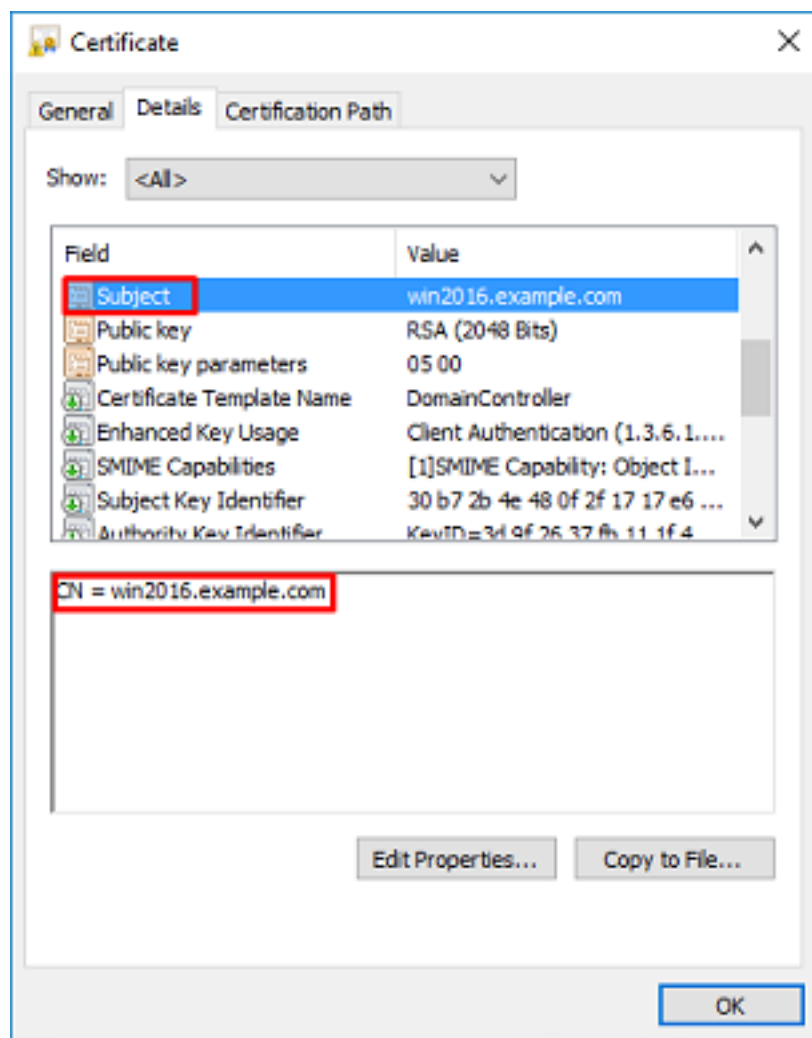
In deze configuratiehandleiding is de FQDN win2016.example.com en dus zijn de eerste 2 certificaten niet geldig voor gebruik als het LDAPS SSL-certificaat. Het identiteitscertificaat dat wordt afgegeven aan win2016.example.com is een certificaat dat automatisch is afgegeven door de Windows Server CA-service. Dubbelklik op het certificaat om de gegevens te controleren.

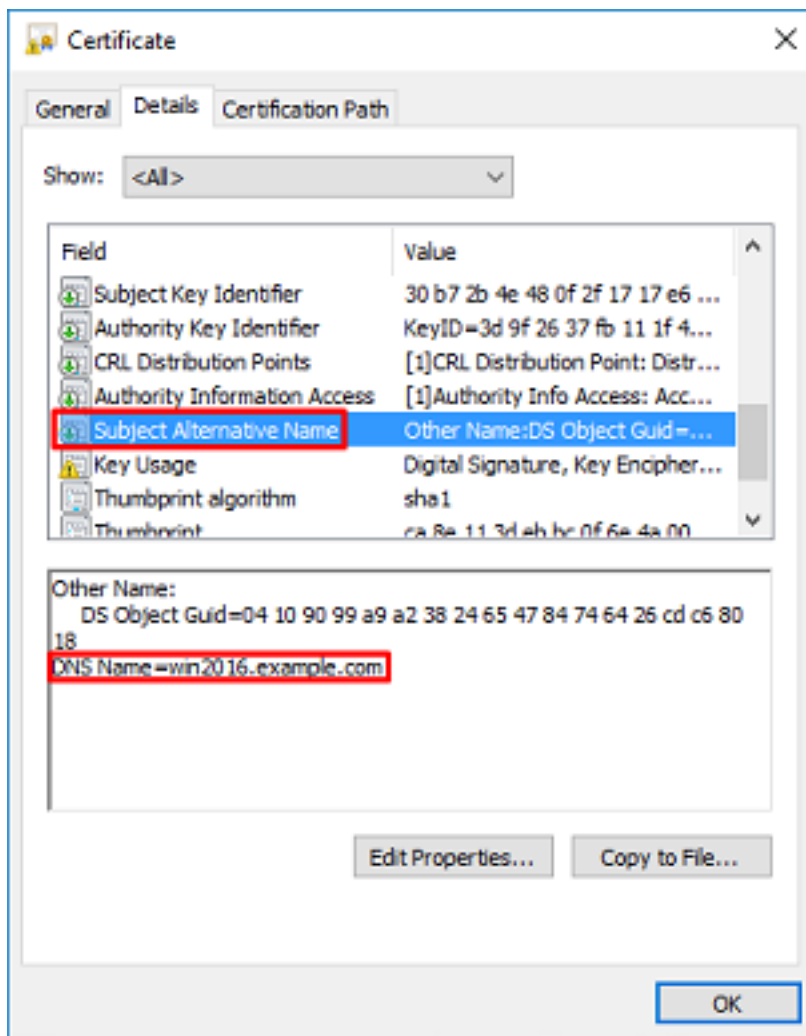


7. Om als SSL-certificaat van het LDAPS te worden gebruikt, moet het certificaat aan de volgende eisen voldoen:

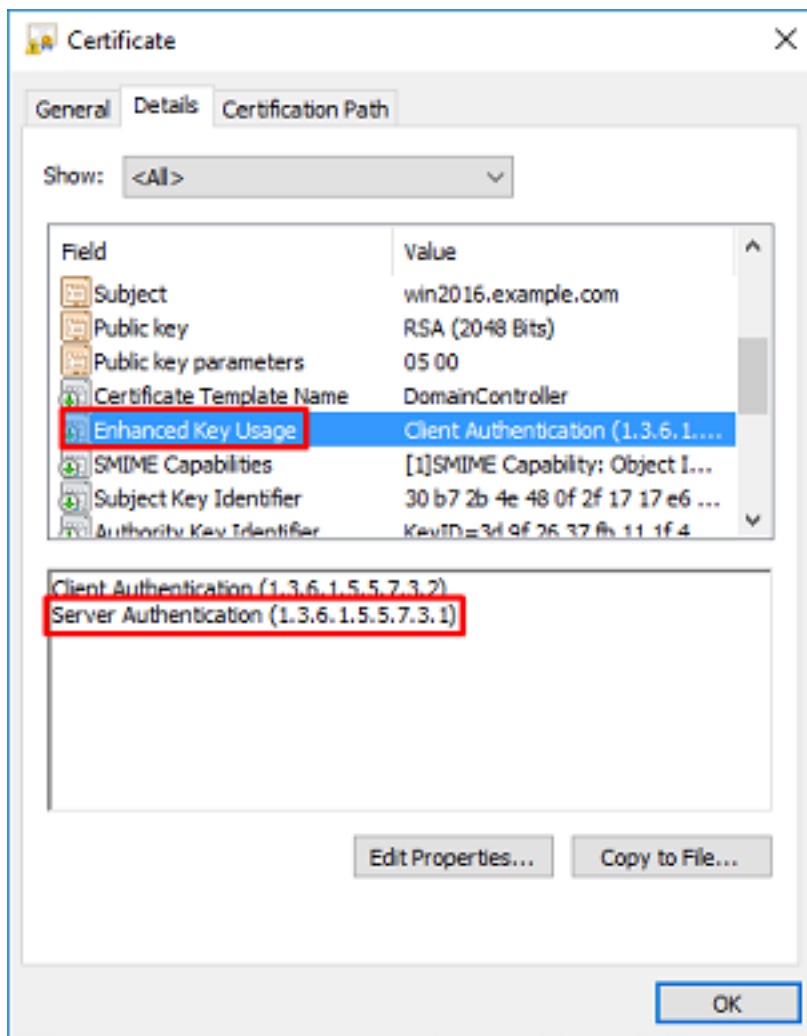
- De veelvoorkomende naam voor **DNS-onderwerp** alternatieve naam komt overeen met de FQDN-naam van de Windows-server.
- Het certificaat heeft **serververificatie** in het veld **Uitgebreid sleutelgebruik**.

Onder het tabblad **Details** voor het certificaat, selecteert u **Onderwerp** en **Onderwerp Alternatieve Naam**, de FQDN win2016.example.com is aanwezig.

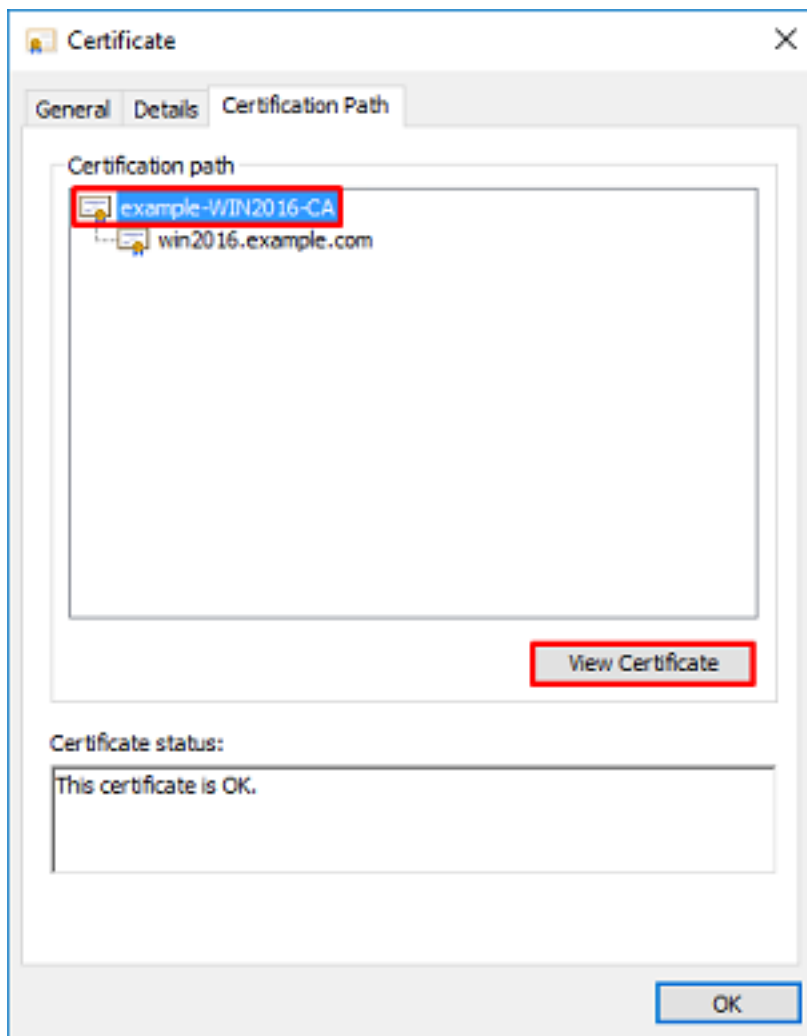




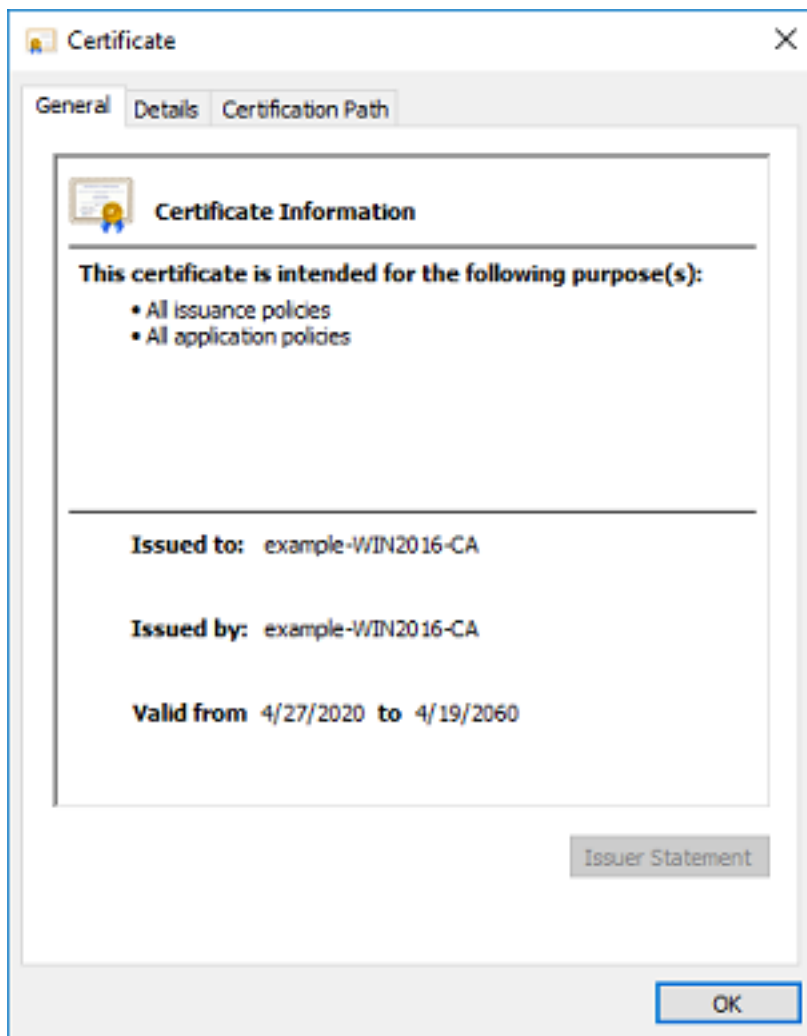
Onder Enhanced Key Usage is serververificatie aanwezig.



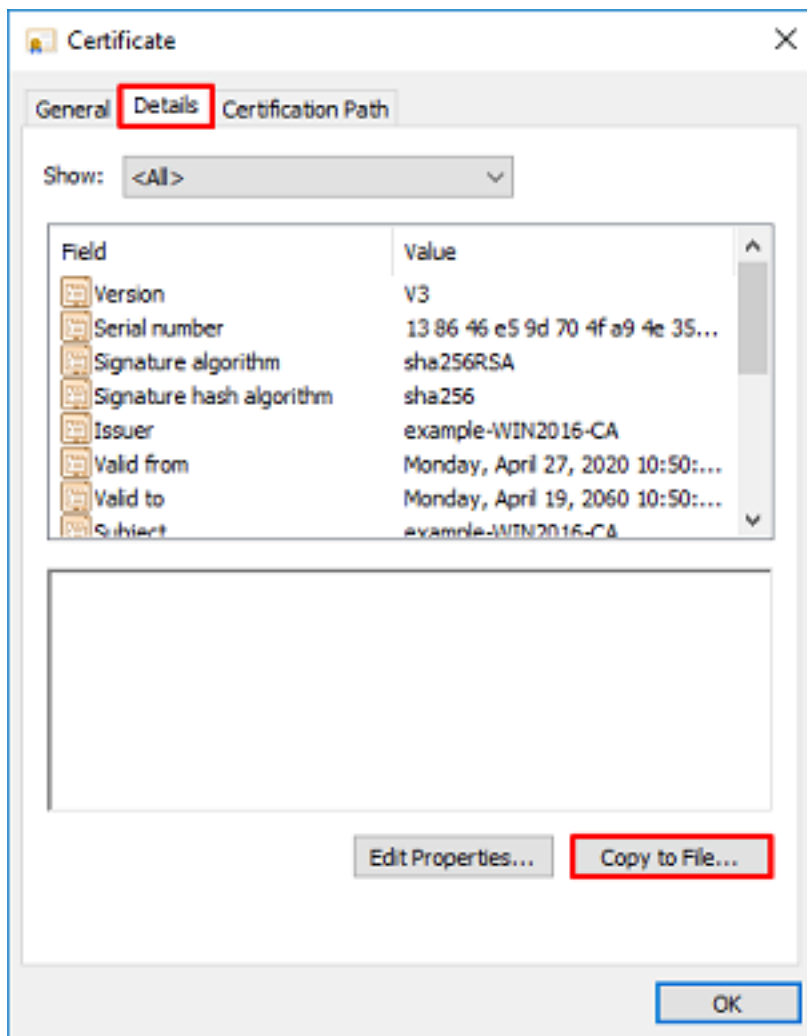
8. Zodra dat is bevestigd, selecteert u onder het tabblad **Certificeringspad** het bovenste certificaat dat het basiscertificaat van de CA is en klikt u op **Certificaat bekijken**.



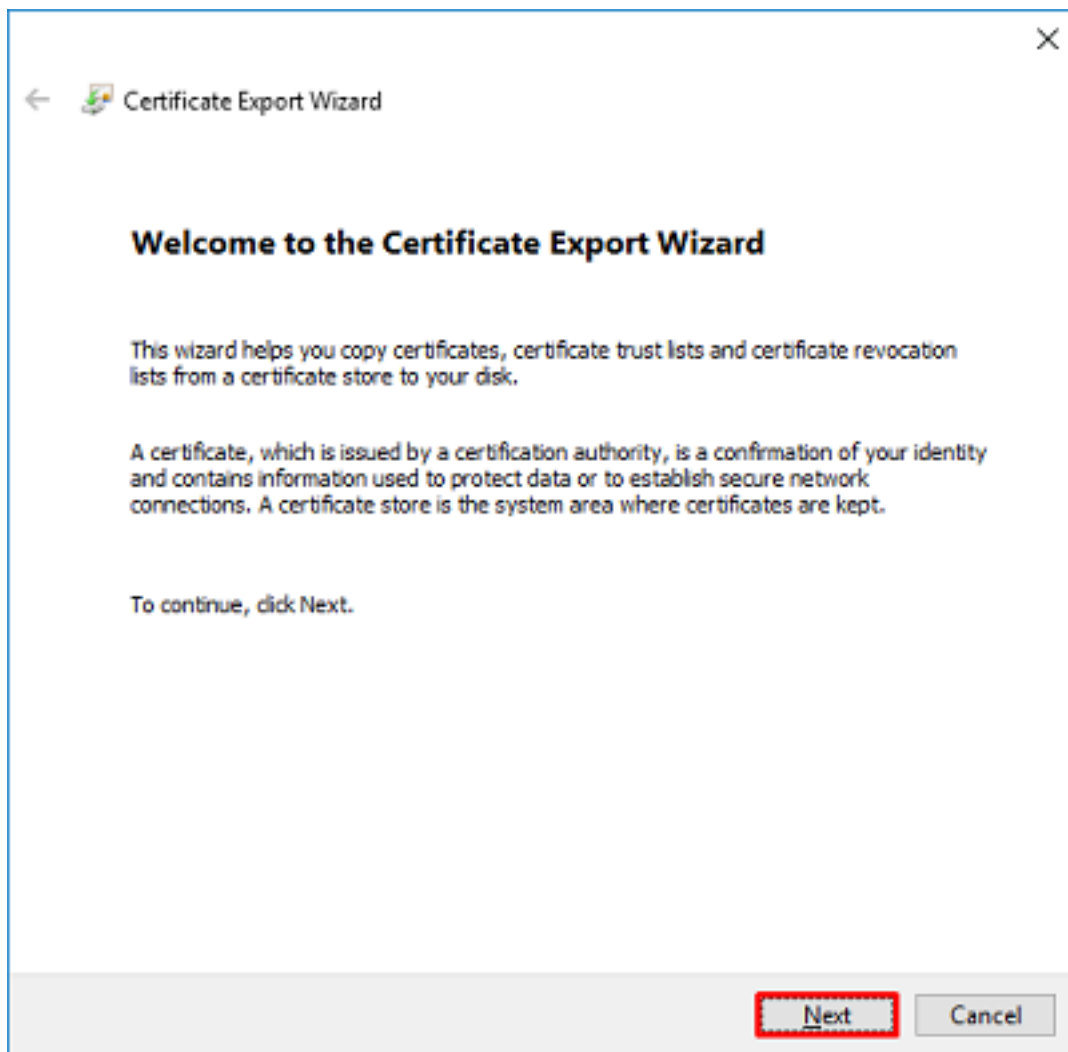
9. Hierdoor worden de certificaatgegevens voor het basiscertificaat van CA geopend.



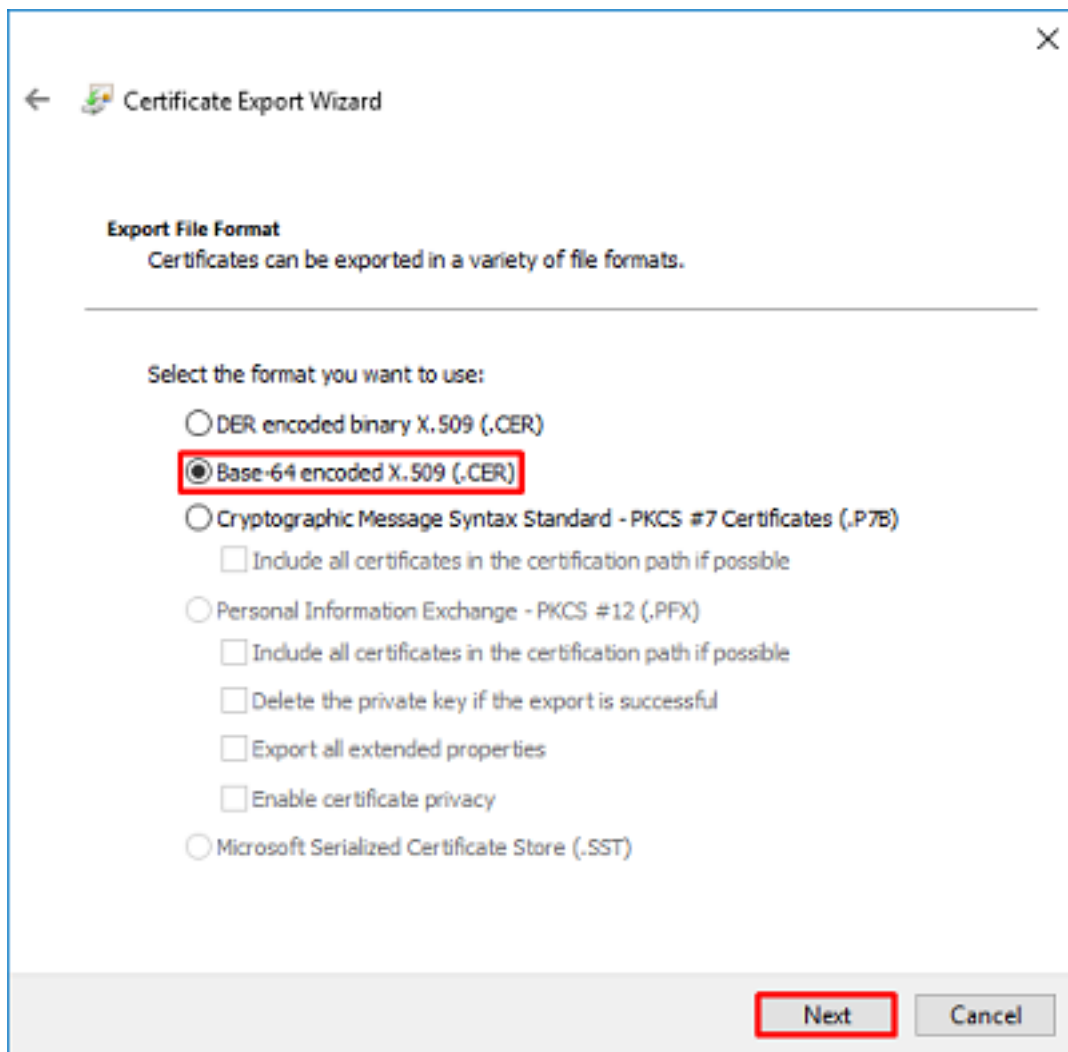
Klik onder het tabblad **Details** op **Kopiëren naar bestand...**



10. Ga door de **wizard Certificaat exporteren** en exporteer de root-CA in PEM-indeling.



Selecteer **Base-64 encoded X.509**



← Certificate Export Wizard

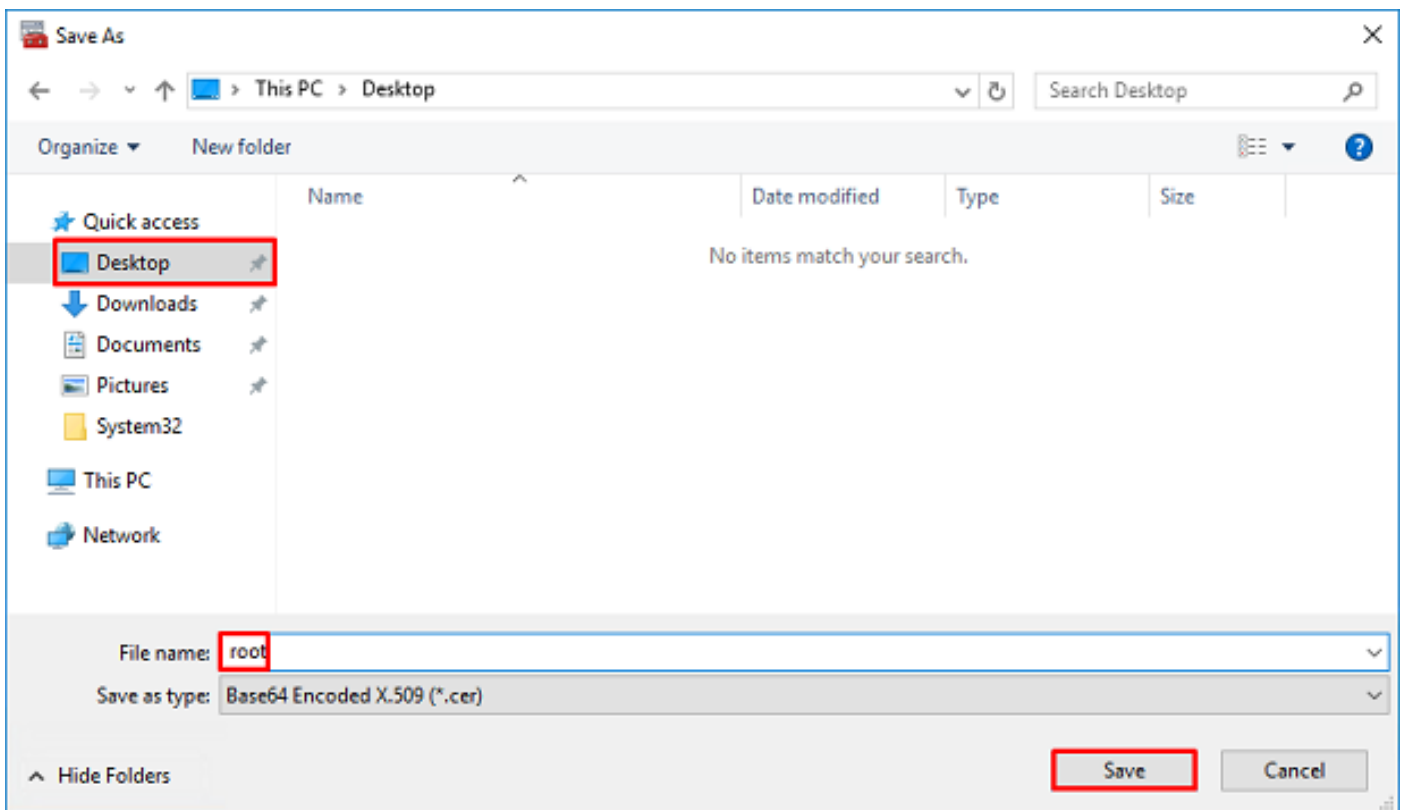
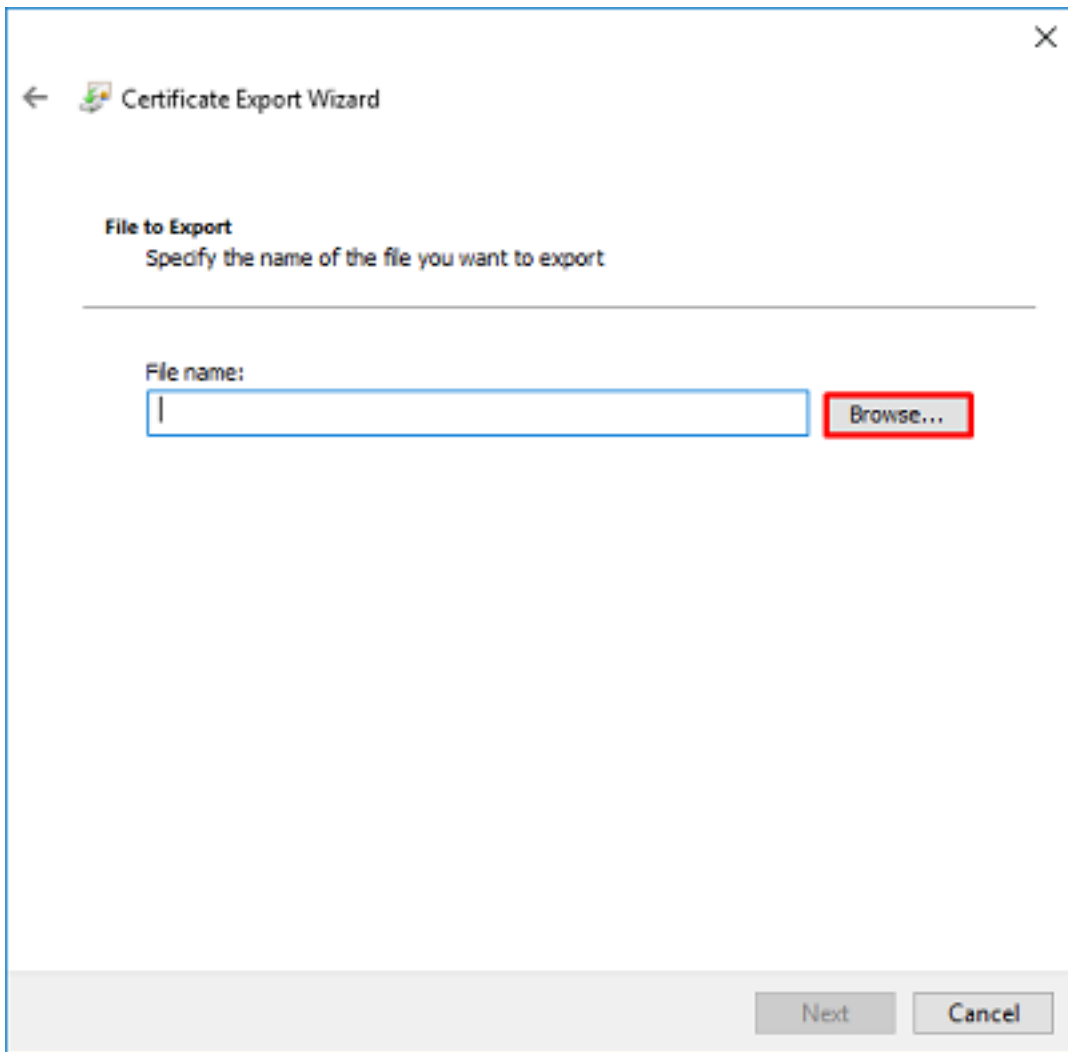
Export File Format
Certificates can be exported in a variety of file formats.

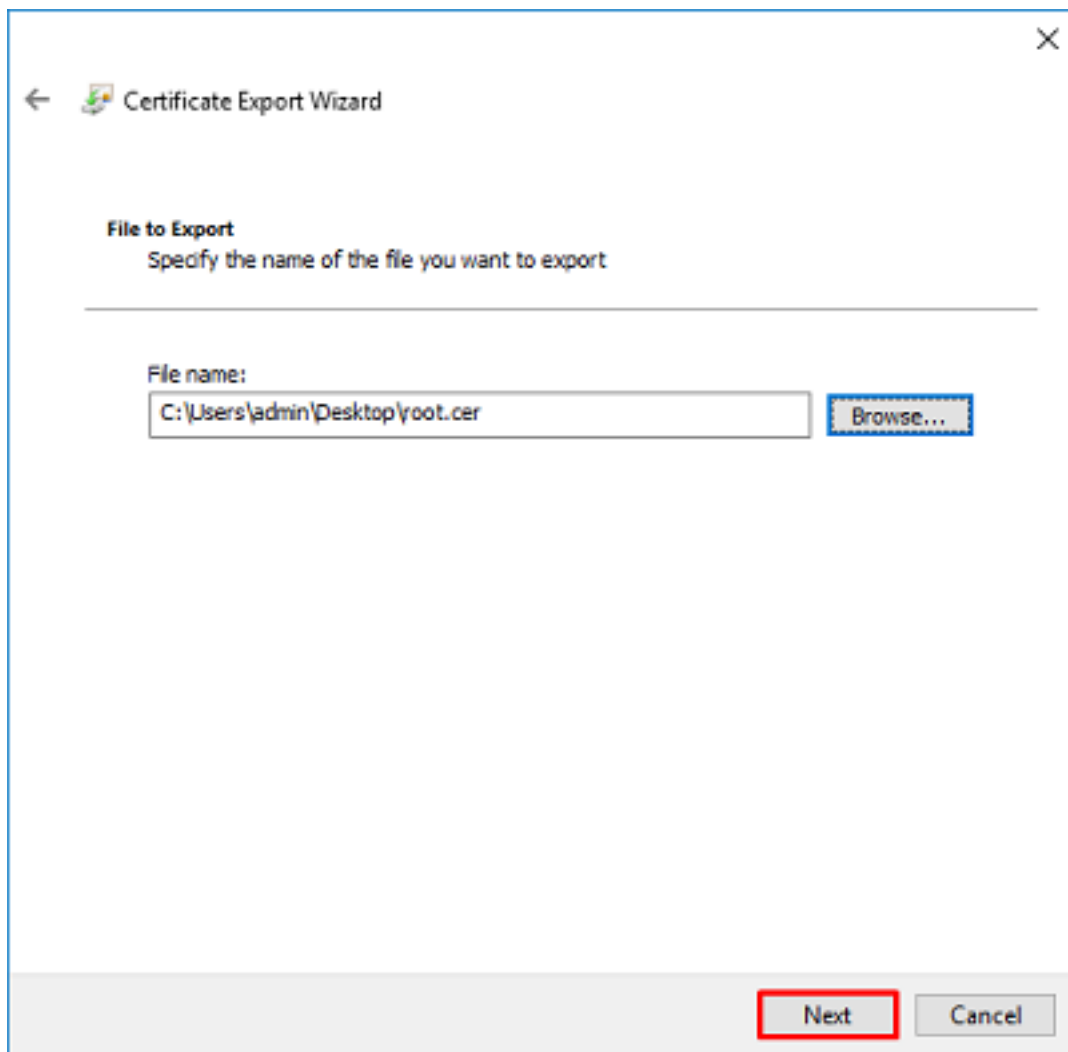
Select the format you want to use:

- 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
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Delete the private key if the export is successful
 - Export all extended properties
 - Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

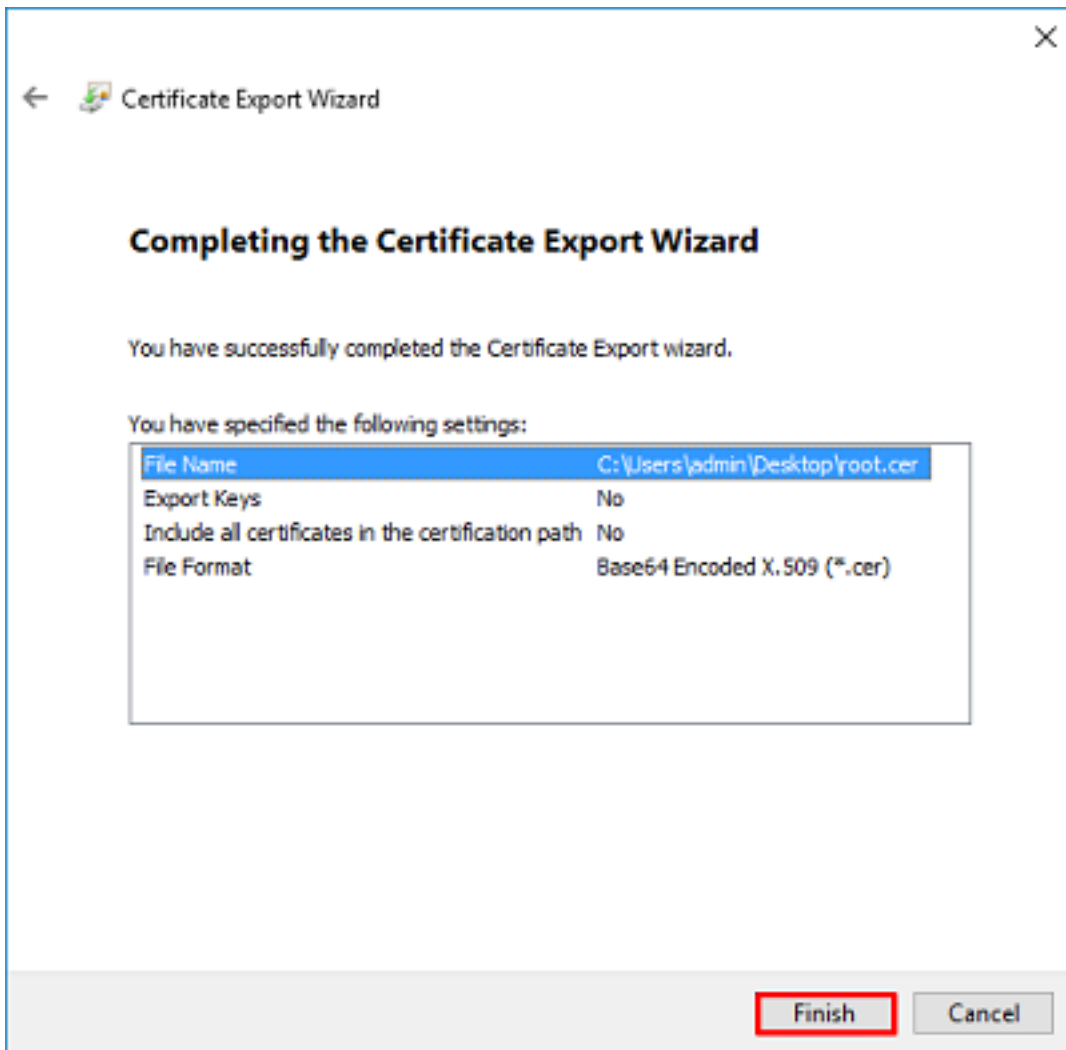
Next Cancel

Selecteer de naam van het bestand en de locatie van de export.





Klik nu op **Voltooien**.



11. Ga nu naar de locatie en open het certificaat met een blocnote of een andere teksteditor. Dit is het certificaat in PEM-indeling. Bewaar dit voor later.

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeXJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlAMB0xGzAZBgNVBAMTEmV4YW1wbGUtV01OMjAxNi1lDQTC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxcVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB3lZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAEt7r
pHFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEm0c9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgrEtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixWpdrbAD06zMHbEYEHkh00jBrUEBBI6Cy83iTZ9ejsk
KgWBJXEu33PplW6E
-----END CERTIFICATE-----
```

12. (facultatief) In het geval dat er meerdere identiteitscertificaten zijn die door LDAPS kunnen worden gebruikt en er onzekerheid is over welke certificaten worden gebruikt, of dat er geen toegang tot de LDAPS-server is, is het mogelijk om de wortelkaart te halen uit een pakketopname die op de Windows-server of FTD daarna is uitgevoerd.

FMC-configuraties

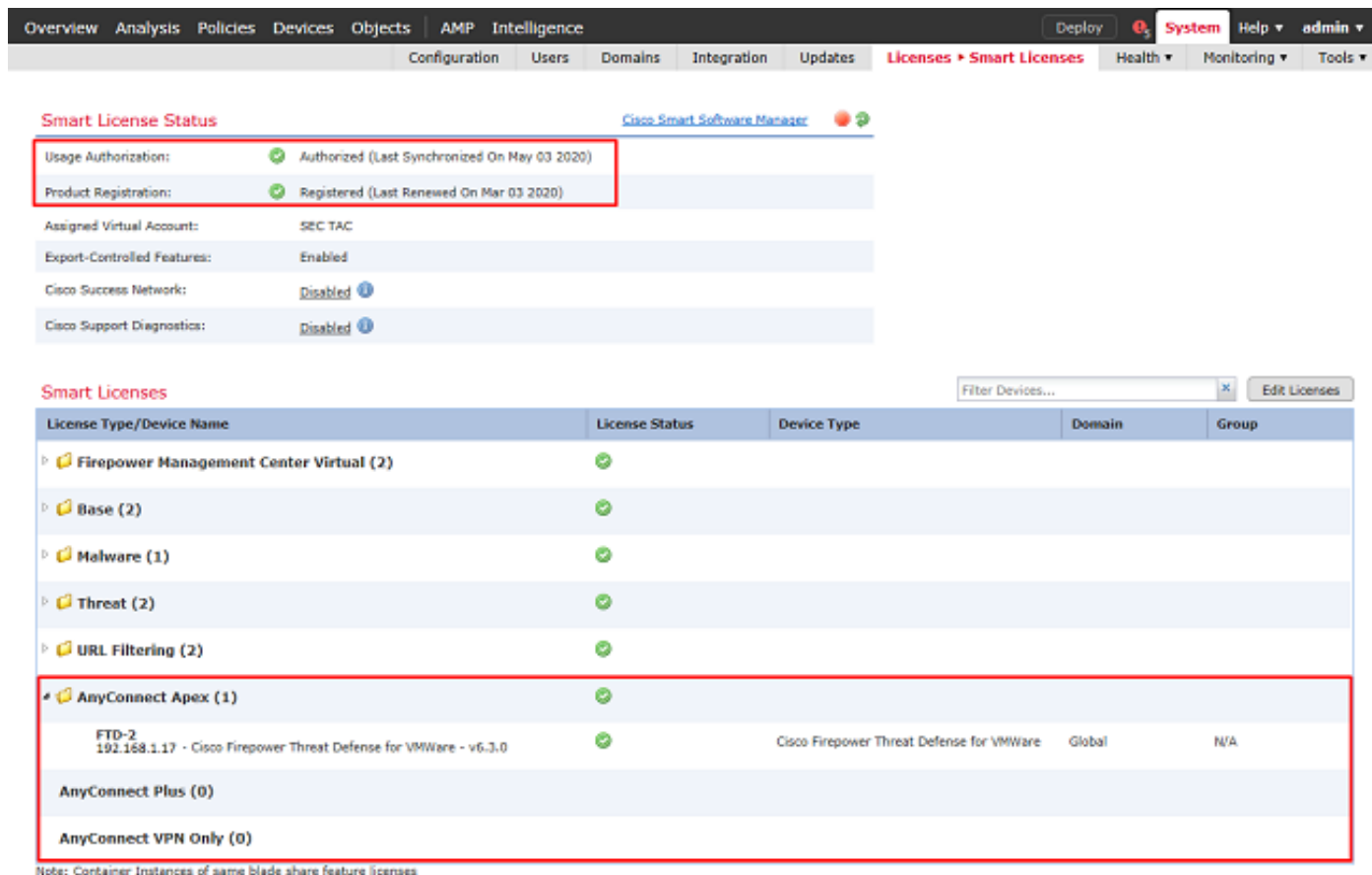
Licentie controleren

Om de AnyConnect-configuratie te kunnen implementeren, moet de FTD worden geregistreerd bij de slimme licentieserver en moet een geldige Plus-, Apex- of VPN-licentie alleen op het apparaat worden toegepast.

1. Ga naar **Systeem > Licenties > Slimme licenties**.



2. Controleer of de apparaten aan de voorschriften voldoen en met succes zijn geregistreerd. Zorg ervoor dat het apparaat is geregistreerd met een **AnyConnect Apex-, Plus- of VPN-licentie**.



Instellingsgebied

1. Ga naar **Systeem > Integratie**.



2. Klik onder **Realms** op **Nieuw domein**.



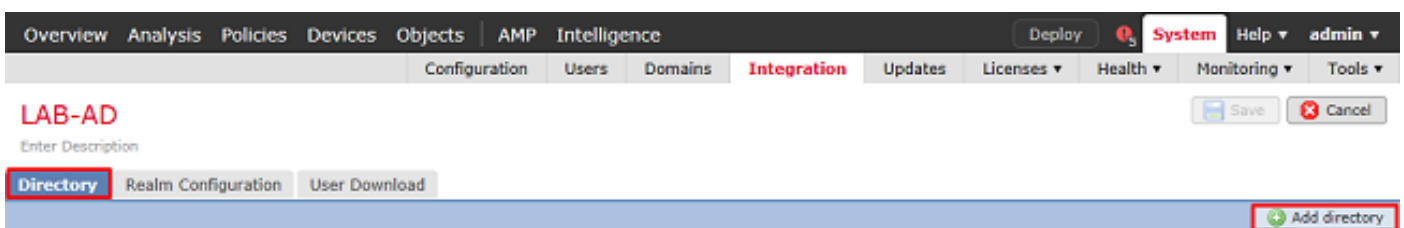
3. Vul de juiste velden in op basis van de bij de Microsoft-server verzamelde informatie. Klik op OK als u klaar bent.

Add New Realm

| | | |
|----------------------|--|---|
| Name * | <input type="text" value="LAB-AD"/> | |
| Description | <input type="text"/> | |
| Type * | <input type="text" value="AD"/> | |
| AD Primary Domain * | <input type="text" value="example.com"/> | ex: domain.com |
| AD Join Username | <input type="text"/> | ex: user@domain |
| AD Join Password | <input type="password"/> | <input type="button" value="Test AD Join"/> |
| Directory Username * | <input type="text" value="ftd.admin@example.com"/> | ex: user@domain |
| Directory Password * | <input type="password" value="*****"/> | |
| Base DN * | <input type="text" value="DC=example,DC=com"/> | ex: ou=user,dc=cisco,dc=com |
| Group DN * | <input type="text" value="DC=example,DC=com"/> | ex: ou=group,dc=cisco,dc=com |
| Group Attribute | <input type="text" value="Member"/> | |

* Required Field

4. Selecteer in het nieuwe venster **Directory** als dit nog niet is gekozen en klik op **Map toevoegen**.



Vul de gegevens van de AD-server in. Merk op dat als FQDN wordt gebruikt, FMC en FTD niet met succes kunnen binden tenzij DNS wordt gevormd om FQDN op te lossen.

Als u DNS voor FMC wilt instellen, navigeert u naar **System > Configuration** en selecteert u **Management Interfaces**.

Om DNS voor de FTD in te stellen, navigeer naar **Apparaten > Platform-instellingen**, maak een nieuw beleid, of bewerk een huidig beleid dan gaan naar DNS.

Add directory



Hostname / IP Address:

Port:

Encryption: STARTTLS LDAPS None

SSL Certificate:

OK

Test

Cancel

Als LDAPS of STARTTLS wordt gebruikt, klik op het Green **+**-symbool, geef het certificaat een naam en kopieer het PEM-formaat root CA-certificaat. Klik op **Opslaan** als u klaar bent.

Import Trusted Certificate Authority



Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExleGFtZXQxLWVudC9wcm9kdGVudC90EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOITaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVVY/E5qVKEKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQn4+SrOhHWIRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fj7ER9EM/HcXCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAET7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVib7Xp11Iva
6tALTt3ANRNqREtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjIBCxsTscubRI+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

Encrypted, and the password is:

Save

Cancel

Selecteer de nieuw toegevoegde root-CA uit de vervolgkeuzelijst naast SSL-certificaat en klik op STARTTLS of LDAPS.

Edit directory

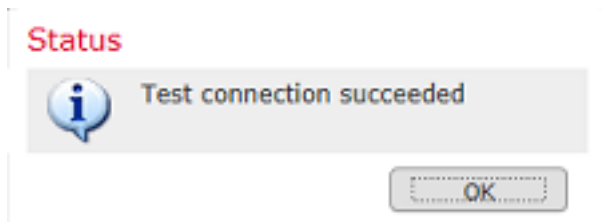


| | |
|-----------------------|--|
| Hostname / IP Address | <input type="text" value="win2016.example.com"/> |
| Port | <input type="text" value="636"/> |
| Encryption | <input type="radio"/> STARTTLS <input checked="" type="radio"/> LDAPS <input type="radio"/> None |
| SSL Certificate | <input type="text" value="LDAPS_ROOT"/> |

Klik op Test om er zeker van te zijn dat FMC met succes kan binden met de Directory Gebruikersnaam en het wachtwoord dat in de vorige stap is opgegeven.

Omdat deze tests worden geïnitieerd vanuit het FMC en niet via een van de routeerbare interfaces die op de FTD zijn geconfigureerd (zoals binnenkant, buitenkant, dmz), garandeert een succesvolle (of mislukte) verbinding niet hetzelfde resultaat voor AnyConnect-verificatie omdat AnyConnect LDAP-verificatieaanvragen worden geïnitieerd vanuit een van de FTD routable interfaces.

Zie de secties Test AAA en Packet Capture in het gedeelte Problemen oplossen voor meer informatie over het testen van LDAP-verbindingen vanuit de FTD.



5. Download onder **Gebruikersdownload** de groepen die in latere stappen worden gebruikt voor gebruikersidentiteit.

Schakel het selectievakje **Gebruikers en groepen downloaden in** en de kolom **Beschikbare groepen** wordt gevuld met groepen die zijn geconfigureerd binnen Active Directory.

Groepen kunnen worden opgenomen of uitgesloten, maar standaard zijn alle groepen die onder de Groep DN worden gevonden, inbegrepen.

Ook specifieke gebruikers kunnen worden opgenomen of uitgesloten. Alle opgenomen groepen en gebruikers zijn beschikbaar om later te worden geselecteerd voor gebruikersidentiteit.

Als u klaar bent, klikt u op **Opslaan**.

LAB-AD

Enter Description

Directory Realm Configuration **User Download**

Download users and groups

Begin automatic download at 8 AM America/New York Repeat Every 24 Hours

Download Now

Available Groups

Search by name

- AnyConnect Admins
- DnsUpdateProxy
- WseRemoteAccessUsers
- WseInvisibleToDashboard
- Allowed RODC Password Replication Group
- Enterprise Key Admins
- Domain Admins
- WseAlertAdministrators
- Event Log Readers
- Replicator
- Domain Guests
- Windows Authorization Access Group
- Account Operators
- Hyper-V Administrators
- System Managed Accounts Group

Groups to Include (2)

- AnyConnect Admins
- AnyConnect Users

Groups to Exclude (0)

None

Enter User Inclusion Add Enter User Exclusion Add

6. Schakel het nieuwe domein in.

Overview Analysis Policies Devices Objects AMP Intelligence

Configuration Users Domains **Integration** Updates Licenses Health Monitoring Tools

Cloud Services **Realms** Identity Sources eStreamer Host Input Client Smart Software Satellite

Compare realms New realm

| Name | Description | Domain | Type | Base DN | Group DN | Group Attribute | State |
|--------|-------------|--------|------|-------------------|-------------------|-----------------|-------------------------------------|
| LAB-AD | | Global | AD | DC=example,DC=com | DC=example,DC=com | member | <input checked="" type="checkbox"/> |

7. Indien LDAPS of STARTTLS wordt gebruikt, moet de oorspronkelijke CA ook door de FTD worden vertrouwd. Om dit te doen navigeer eerst naar **Apparaten > Certificaten**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Klik op Add in de rechterbovenhoek.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Add

Selecteer de FTD, de LDAP configuratie wordt toegevoegd om dan op het Groene + symbool te klikken.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*: 

Geef het trustpoint een **Naam** en kies vervolgens **Handmatige** inschrijving uit de vervolgkeuzelijst **Inschrijftype**. Plakt hier het PEM root ca certificaat en klik vervolgens op **Opslaan**.

Add Cert Enrollment

Name*:

Description:

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type:

CA Certificate*:

```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki
G9w0BAQsFADAd
MRswGQYDVQQQExJleGFtcGxlLVdJTjJlWMTYtQ0EwIBcNMjAwNDI
3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGU
tV0lOMjAxNi1DQTCC
ASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N
zSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItaVsgHwPBF
d++M+bLn3AiZnHV
OO+k6dVvY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIo
ficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN
O7KEMkfa1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBU
aLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86
```

Allow Overrides:

Controleer dat het gemaakte trustpoint is geselecteerd en klik vervolgens op **Toevoegen**.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: LDAPS_ROOT
 Enrollment Type: Manual
 SCEP URL: NA

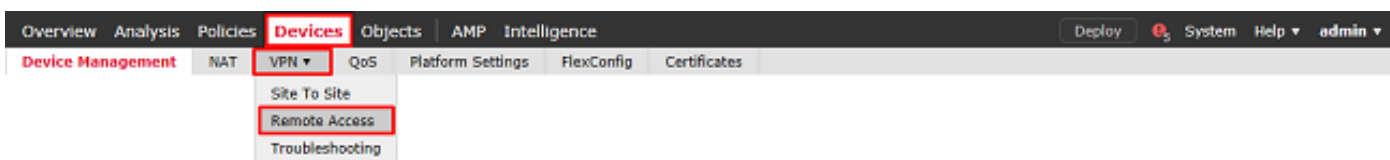
Het nieuwe trustpoint verschijnt onder het FTD. Hoewel hierin wordt vermeld dat de invoer van een identiteitscertificaat is vereist, is het voor het FTD niet nodig het SSL-certificaat te kunnen verifiëren dat door de LDAPS-server is verzonden, zodat dit bericht kan worden genegeerd.

| Name | Domain | Enrollment Type | Status |
|------------------|--------|-----------------|---|
| FTD-1 | | | |
| FTD-1-PKCS12 | Global | PKCS12 file | CA ID |
| FTD-2 | | | |
| FTD-2-PKCS12 | Global | PKCS12 file | CA ID |
| FTD-2-Selfsigned | Global | Self-Signed | CA ID |
| LDAPS_ROOT | Global | Manual | CA ID ID Identity certificate import required |

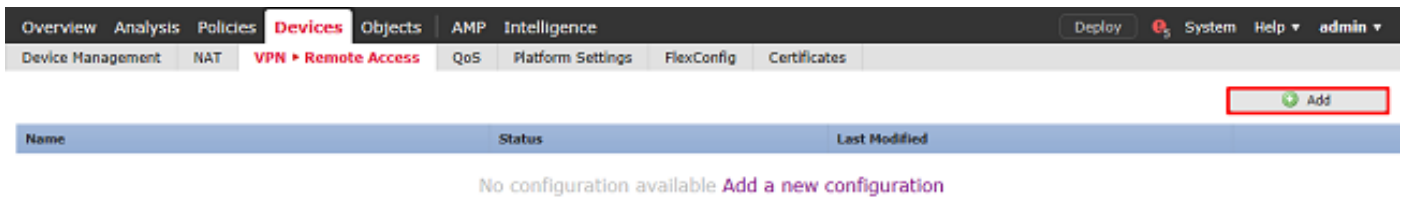
AnyConnect configureren voor AD-verificatie

1. Bij deze stappen wordt ervan uitgegaan dat er al geen VPN-beleid voor externe toegang is gemaakt. Als er een is gemaakt, klik dan op de bewerkingsknop voor dat beleid en ga naar stap 3.

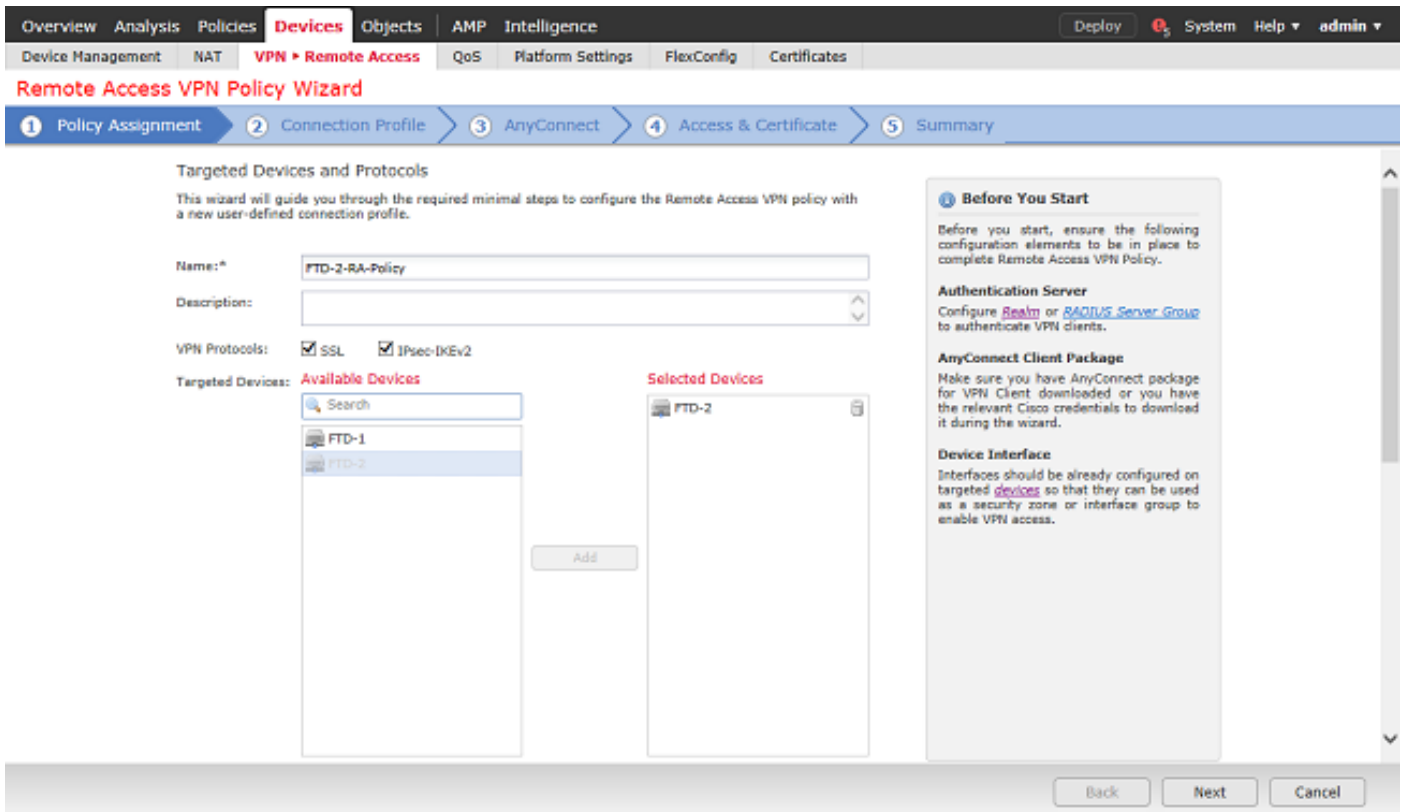
Navigeer naar **Apparaten > VPN > Externe toegang**.



Klik op **Add** om een nieuw VPN-beleid voor externe toegang te maken



2. Voltooi de **beleidswizard voor externe toegang tot VPN**. Specificeer onder **Beleidstoewijzing** een naam voor het beleid en de apparaten waarop het beleid wordt toegepast.



Specificeer onder **Verbindingsprofiel** de naam van **Verbindingsprofiel** dat ook wordt gebruikt als de groepalias die AnyConnect-gebruikers zien wanneer ze verbinding maken.

Specificeer het domein dat eerder is gemaakt onder **Verificatieserver**.

Geef op hoe AnyConnect-clients IP-adressen krijgen toegewezen.

Specificeer het standaardgroepsbeleid dat voor dit verbindingsprofiel wordt gebruikt.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 **Connection Profile** 3 AnyConnect 4 Access & Certificate 5 Summary

Connection Profile:
 Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name: *
This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):
 Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:
 Authentication Server: * (Realm or RADIUS)
 Authorization Server: (RADIUS)
 Accounting Server: (RADIUS)

Client Address Assignment:
 Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only) ⓘ
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools:
 IPv6 Address Pools:

Group Policy:
 A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy: * [Edit Group Policy](#)

Back Next Cancel

Upload en specificeer onder AnyConnect de AnyConnect-pakketten die worden gebruikt.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

AnyConnect Client Image
 The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from Cisco Software Download Center.

Show Re-order buttons

| <input checked="" type="checkbox"/> | AnyConnect File Object Name | AnyConnect Client Package Name | Operating System |
|-------------------------------------|------------------------------------|--|------------------|
| <input checked="" type="checkbox"/> | anyconnect-linux64-4.7.03052-we... | anyconnect-linux64-4.7.03052-webdeploy-k9... | Linux |
| <input checked="" type="checkbox"/> | anyconnect-win-4.7.00136-webde... | anyconnect-win-4.7.00136-webdeploy-k9.pkg | Windows |

Back Next Cancel

Specificeer onder **Access & Certificate** de interface waartoe AnyConnect-gebruikers toegang hebben voor AnyConnect.

Maak en/of specificeer het certificaat dat door de FTD wordt gebruikt tijdens de SSL-handdruk.

Zorg ervoor dat het aanvinkvakje voor **het beleid** voor **toegangscontrole** voor gedecrypteerd verkeer (sysopt license-vpn) niet is aangevinkt, zodat de gebruikersidentiteit die later wordt gemaakt, van kracht wordt voor RAVPN-verbindingen.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Network Interface for Incoming VPN Access
 Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:

Enable DTLS on member interfaces

Device Certificates
 Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:

Enroll the selected certificate object on the target devices

Access Control for VPN Traffic
 All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Back Next Cancel

Bekijk onder **Samenvatting** de configuratie en klik op **Voltoeien**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: FTD-2-RA-Policy

Device Targets: FTD-2

Connection Profile: General

Connection Alias: General

AAA:

- Authentication Method: AAA Only
- Authentication Server: LAB-AD
- Authorization Server: -
- Accounting Server: -

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): AnyConnect-Pool
- Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images:

- anyconnect-linux64-4.7.03052-webdeploy-k9.pkg
- anyconnect-win-4.7.00136-webdeploy-k9.pkg

Interface Objects: outside-zone

Device Certificates: FTD-2-Selfsigned

Device Identity Certificate Enrollment

Certificate enrollment object 'FTD-2-Selfsigned' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.

Network Interface Configuration

Make sure to add interface from targeted devices to SecurityZone object 'outside-zone'

Back Finish Cancel

3. Klik onder het **VPN-beleid** voor externe toegang op **bewerken** voor het juiste **verbindingsprofiel**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

FTD-2-RA-Policy Save Cancel

Enter Description Policy Assignments (1)

Connection Profile Access Interfaces **Advanced**

| Name | AAA | Group Policy |
|---------------------|--|---------------|
| DefaultWEB/VPNGroup | Authentication: None Authorization: None Accounting: None | DfitGrpPolicy |
| General | Authentication: LAB-AD (AD) Authorization: None Accounting: None | DfitGrpPolicy |

Zorg ervoor dat de verificatieserver is ingesteld op het domein dat eerder is gemaakt.

Onder **Advanced Settings** kan **Wachtwoordbeheer** worden ingeschakeld om gebruikers in staat te stellen hun wachtwoord te wijzigen wanneer of voordat hun wachtwoord verloopt.

Deze instelling vereist echter dat het gebied LDAPS gebruikt. Als er wijzigingen zijn aangebracht, klikt u op **Opslaan**.

Edit Connection Profile ? X

Connection Profile:* General

Group Policy:* DfitGrpPolicy [Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: LAB-AD (AD)

Use secondary authentication

Authorization

Authorization Server:

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

Advanced Settings

Strip Realm from username

Strip Group from username

Enable Password Management

Notify User 14 days prior to password expiration

Notify user on the day of password expiration

Save Cancel

Klik rechtsboven op **Opslaan**.



Identiteitsbeleid inschakelen en Beveiligingsbeleid voor gebruikersidentiteit configureren

1. Ga naar **Beleid > Toegangsbeheer > Identiteit**.



Een nieuw identiteitsbeleid maken.



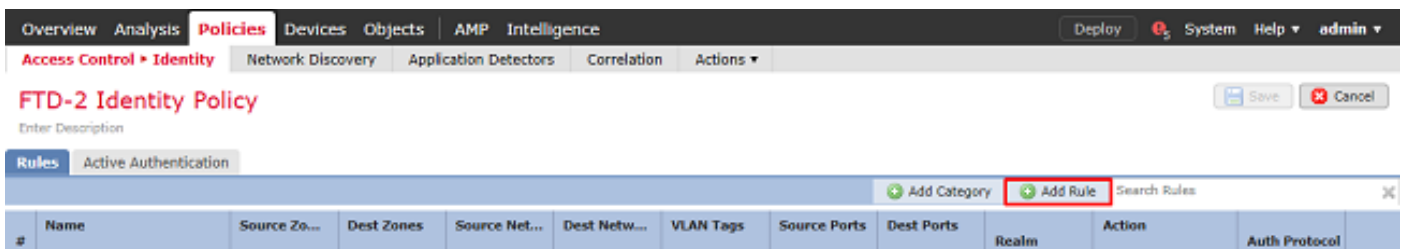
Specificeer een **naam** voor het nieuwe **identiteitsbeleid**.

New Identity policy

Name:

Description:

2. Klik op **Regel toevoegen**.



3. Geef een **naam op** voor de nieuwe regel. Zorg ervoor dat deze is ingeschakeld en dat de actie is ingesteld op Passieve verificatie.

Klik op het tabblad **Realm & Settings** en selecteer het gebied dat eerder is gemaakt. Klik op **Toevoegen** als u klaar bent.

Add Rule

Name: Enabled

Insert: into Category

Action: Realm: LAB-AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Remote access VPN sessions are actively authenticated by VPN. Other sessions use the rule Action.

Zones Networks VLAN Tags Ports **Realm & Settings**

Realm *

Use active authentication if passive or VPN identity cannot be established

* Required Field

Add Cancel

4. Klik op Opslaan.

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control > Identity Network Discovery Application Detectors Correlation Actions

FTD-2 Identity Policy You have unsaved changes **Save** Cancel

Rules Active Authentication

| # | Name | Source Zo... | Dest Zones | Source Net... | Dest Netw... | VLAN Tags | Source Ports | Dest Ports | Realm | Action | Auth Protocol |
|---|-------|--------------|------------|---------------|--------------|-----------|--------------|------------|--------|------------------------|---------------|
| Administrator Rules This category is empty | | | | | | | | | | | |
| Standard Rules | | | | | | | | | | | |
| 1 | RAVPN | any | any | any | any | any | any | any | LAB-AD | Passive Authentication | none |
| Root Rules This category is empty | | | | | | | | | | | |

Displaying 1 - 1 of 1 rules Page 1 of 1

5. Ga naar Beleid > Toegangsbeheer > Toegangsbeheer.

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control > Identity Network Discovery Application Detectors Correlation Actions

Access Control

- Intrusion
- Malware & File
- DNS
- Identity**
- SSL
- Prefilter

6. Bewerk het Toegangscontrolebeleid waarop de FTD is geconfigureerd.

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control > Access Control Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Import/Export

New Policy

| Access Control Policy | Status | Last Modified |
|-----------------------|---|--|
| Default-Policy | Targeting 1 devices Up-to-date on all targeted devices | 2020-05-04 09:15:56 Modified by "admin" |

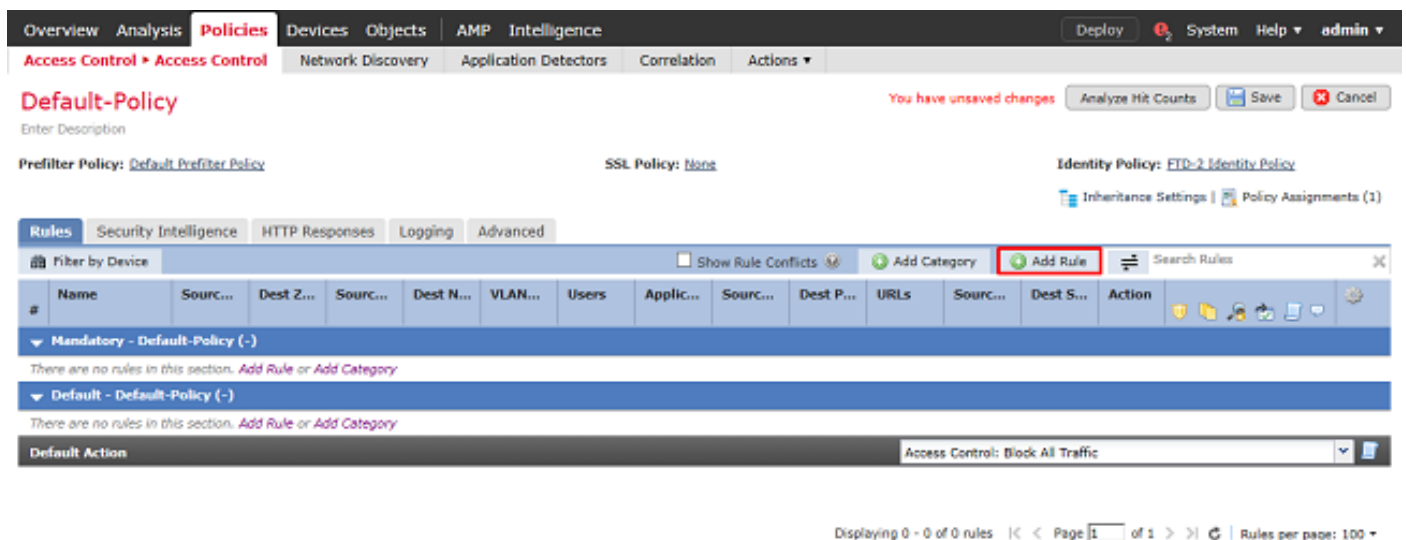
7. Klik op de waarde naast **Identiteitsbeleid**.



Selecteer het eerder gemaakte **identiteitsbeleid** en klik op **OK**.



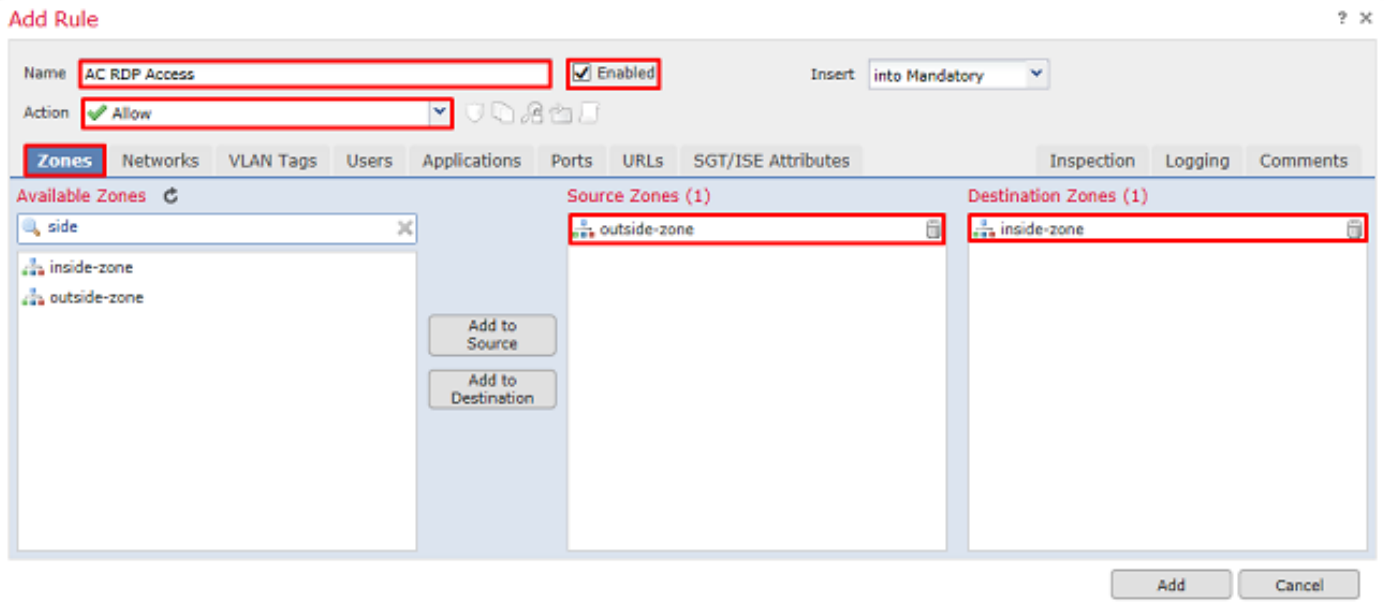
8. Klik op **Regel toevoegen** om een nieuwe ACS-regel te maken. Met deze stappen wordt een regel gemaakt op grond waarvan gebruikers in de AnyConnect Admins-groep met RDP verbinding kunnen maken met apparaten binnen het netwerk.



Geef een naam op voor de regel. Zorg ervoor dat de regel is ingeschakeld en de juiste actie onderneemt.

Specificeer onder het tabblad **Zones** de juiste zones voor het interessante verkeer.

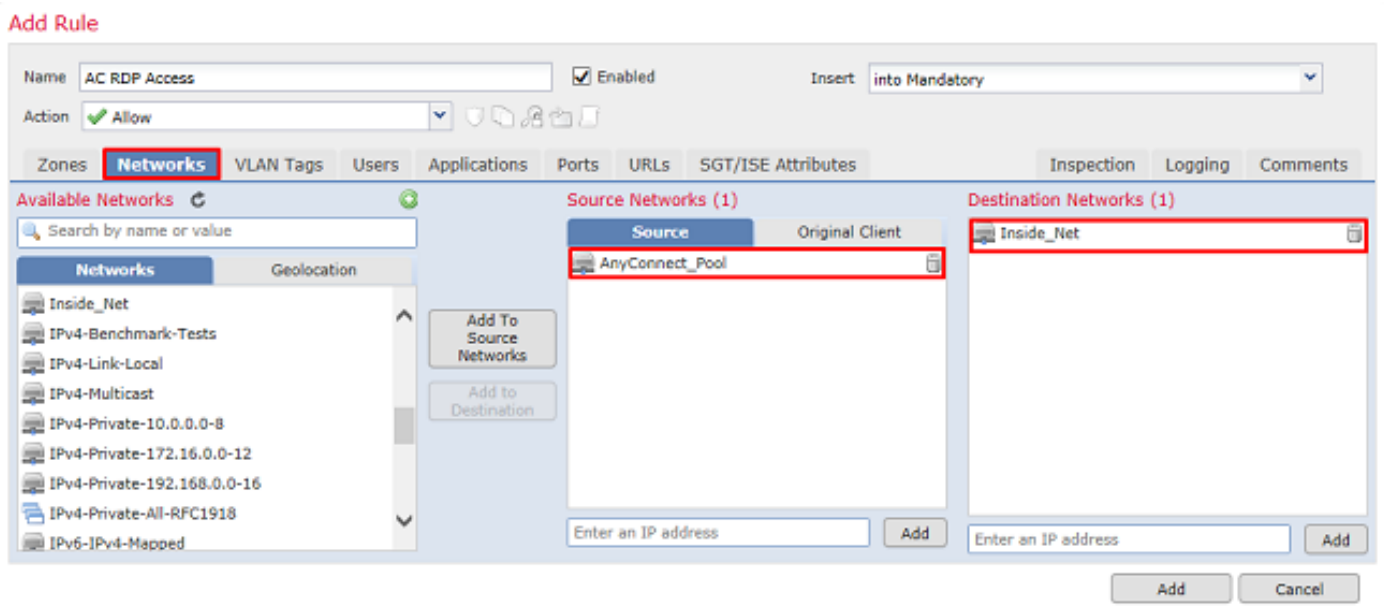
RDP-verkeer dat door gebruikers wordt geïnitieerd, komt in de FTD-bron vanuit de interface van de buitenzone en verlaat de binnenzone.



Definieer onder **Netwerken** de bron- en doelnetwerken.

Object AnyConnect_Pool bevat de IP-adressen die zijn toegewezen aan AnyConnect-clients.

Voorwerp Inside_Net omvat het binnenste netwerksubnetnet.



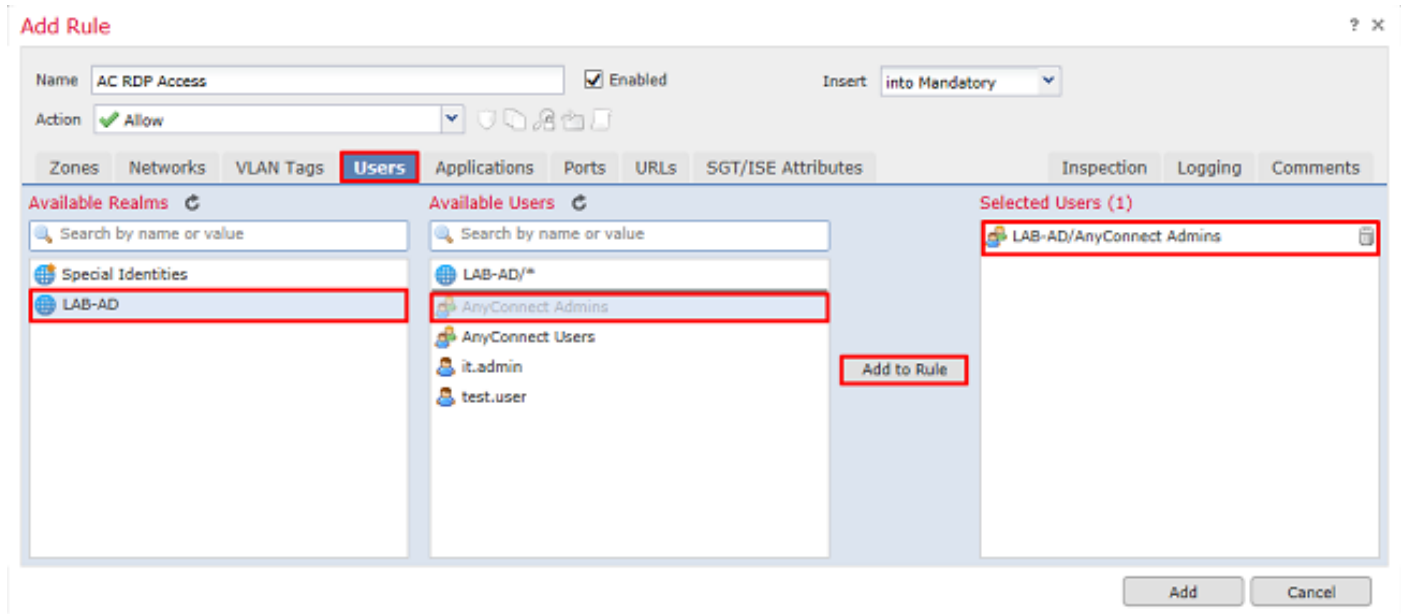
Klik onder **Gebruikers** op het gebied dat eerder is gemaakt onder **Beschikbare interfaces**, klik op de juiste groep/gebruiker onder **Beschikbare gebruikers** en klik vervolgens op **Toevoegen aan regel**.

Als er onder de sectie **Beschikbare gebruikers** geen gebruikers of groepen beschikbaar zijn, zorg er dan voor dat het VCC in staat is om de **gebruikers** en **groepen** onder de sectie Gebiedsdelen te downloaden en dat de juiste **groepen/gebruikers** worden opgenomen.

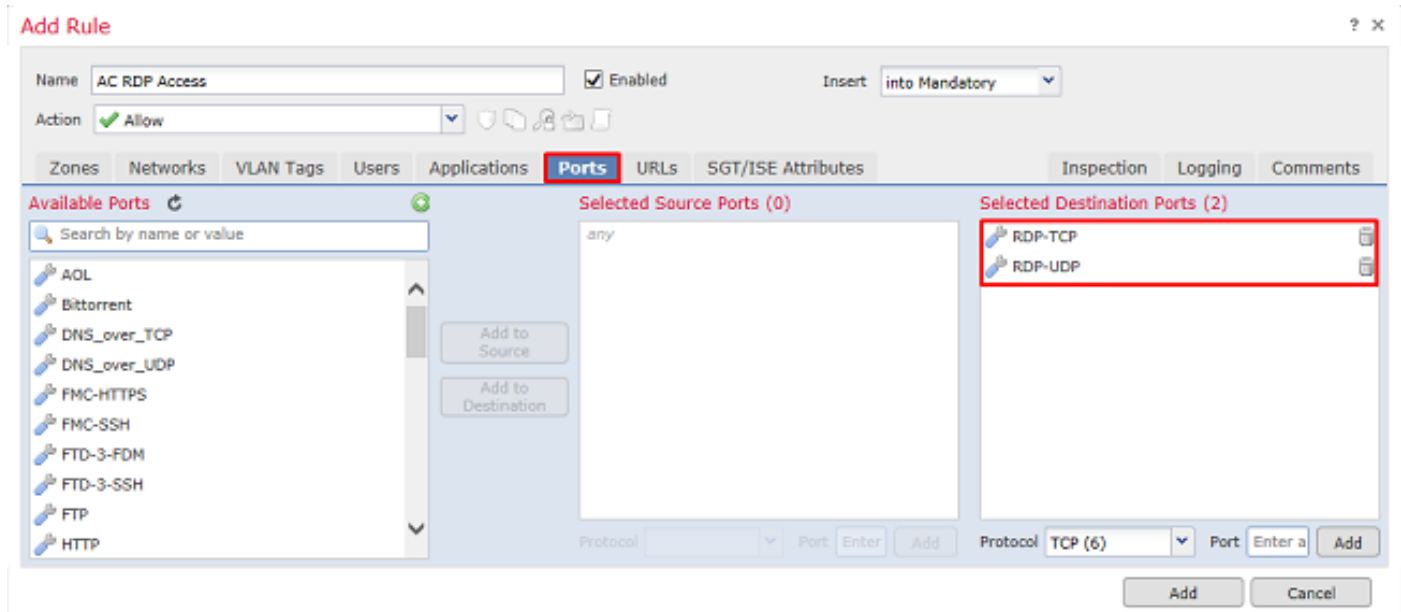
De hier gespecificeerde **gebruikers/groepen** worden vanuit bronperspectief gecontroleerd.

Met wat tot nu toe in deze regel is gedefinieerd, evalueert de FTD bijvoorbeeld dat het verkeer afkomstig is van de buitenzone en bestemd is voor de binnenzone, afkomstig is van het netwerk in het AnyConnect_Pools-object en bestemd is voor het netwerk in het Inside_Net-object, en dat het

verkeer afkomstig is van een gebruiker in de AnyConnect Admins-groep.



Onder Ports zijn aangepaste RDP-objecten gemaakt en toegevoegd om TCP- en UDP-poort 3389 toe te staan. Merk op dat RDP onder de sectie **Toepassingen** had kunnen worden toegevoegd maar voor eenvoud worden alleen de poorten gecontroleerd.



Ten slotte wordt onder **Logging**, **Log at End of Connection** later gecontroleerd voor extra verificatie. Klik op **Toevoegen** als u klaar bent.

Add Rule ? x

Name: Enabled Insert:

Action:

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection **Logging** Comments

Log at Beginning of Connection
 Log at End of Connection

File Events:
 Log Files

Send Connection Events to:
 Event Viewer
 Syslog Server (Using default syslog configuration in Access Control Logging) [Show Overrides](#)
 SNMP Trap

9. Er wordt een extra regel voor HTTP-toegang gecreëerd om gebruikers binnen de groep **AnyConnect-gebruikers** toegang tot de website van **Windows Server IIS** te geven. Klik op **Save** (Opslaan).

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control **Access Control** Network Discovery Application Detectors Correlation Actions

Default-Policy You have unsaved changes

Enter Description

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [FTD-2 Identity Policy](#)

[Rules](#) Security Intelligence HTTP Responses Logging Advanced [Inheritance Settings](#) | [Policy Assignments \(1\)](#)

Filter by Device Show Rule Conflicts

| # | Name | Source Zo... | Dest Zones | Source Networks | Dest Netwo... | V... | Users | A... | S... | Dest Ports | U... | S... | D... | Action |
|--|----------------|--------------|-------------|-----------------|---------------|------|--------------------------|------|------|--------------------|------|------|------|--------|
| Mandatory - Default-Policy (1-2) | | | | | | | | | | | | | | |
| 1 | AC RDP Access | outside-zone | inside-zone | AnyConnect_Pool | Inside_Net | Any | LAB-AD/AnyConnect Admins | Any | Any | RDP-TCP RDP-UDP | Any | Any | Any | Allow |
| 2 | AC HTTP Access | outside-zone | inside-zone | AnyConnect_Pool | Inside_Net | Any | LAB-AD/AnyConnect Users | Any | Any | HTTP | Any | Any | Any | Allow |
| Default - Default-Policy (-) | | | | | | | | | | | | | | |
| There are no rules in this section. Add Rule or Add Category | | | | | | | | | | | | | | |

Default Action

Displaying 1 - 2 of 2 rules | Page 1 of 1 | Rules per page: 100

NAT-vrijstelling configureren

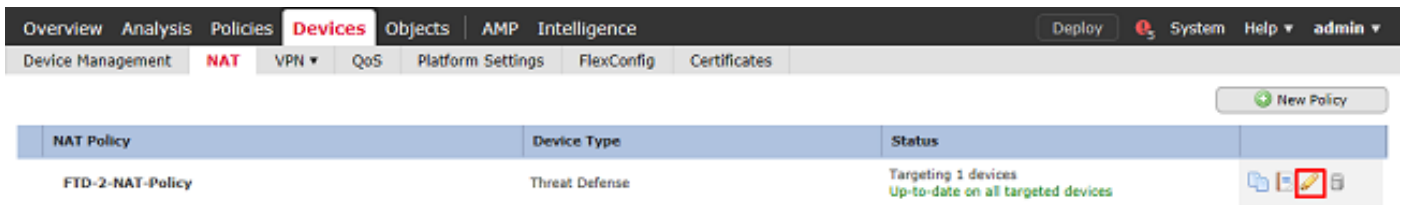
Als er NAT-regels zijn die invloed hebben op AnyConnect-verkeer, zoals Internet PAT-regels, is het belangrijk om NAT-vrijstellingsregels te configureren zodat AnyConnect-verkeer niet NAT-beïnvloed is.

1. Navigeer naar **apparaten > NAT**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

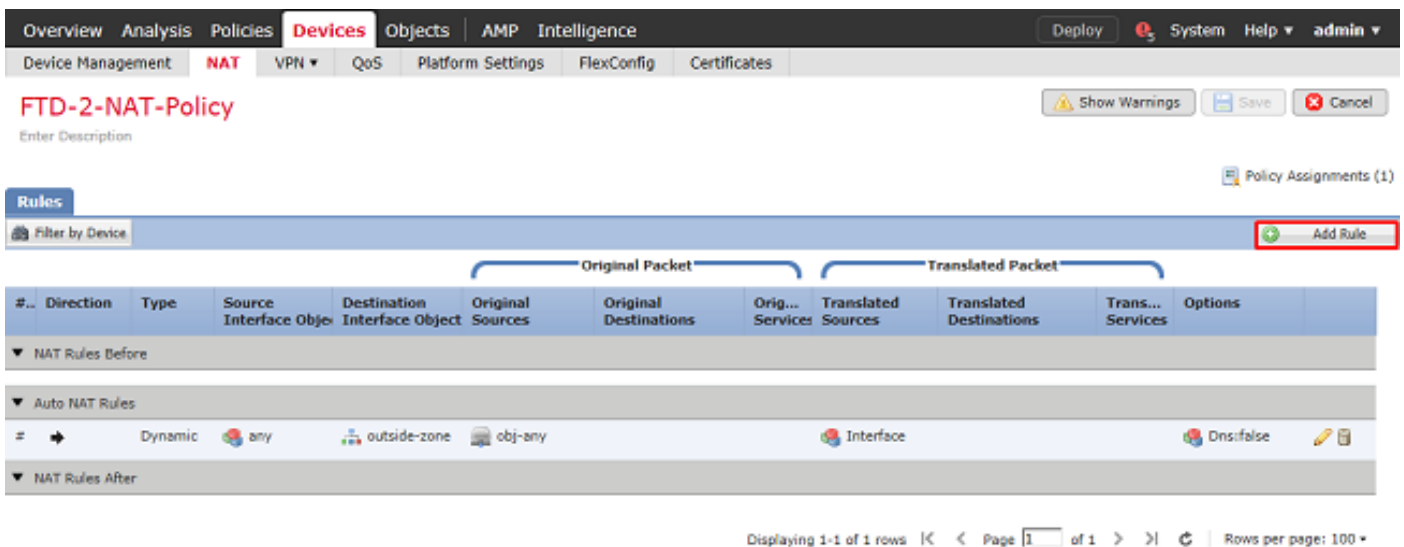
Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

Selecteer het NAT-beleid dat op de FTD wordt toegepast.



2. In dit NAT-beleid is er een Dynamisch PAT aan het einde dat PAT-invloed heeft op al het verkeer (inclusief AnyConnect-verkeer) dat de buiteninterface naar de buiteninterface perst.

Klik rechtsboven op **Regel toevoegen** om te voorkomen dat het AnyConnect-verkeer NAT-beïnvloed wordt.



3. Configureer een NAT-vrijstellingsregel en zorg ervoor dat de regel een handmatige NAT-regel is met Type Statisch. Dit is een bidirectionele NAT-regel die van toepassing is op AnyConnect-verkeer.

Met deze instellingen, wanneer de FTD verkeer detecteert afkomstig van Inside_Net en bestemd voor AnyConnect IP-adres (gedefinieerd door AnyConnect_Pool), wordt de bron vertaald naar dezelfde waarde (Inside_Net) en wordt de bestemming vertaald naar dezelfde waarde (AnyConnect_Pool) wanneer het verkeer binnendringt in de inside_zone en de buitenkant_zone betreedt. Dit passeert NAT in essentie wanneer aan deze voorwaarden wordt voldaan.

Add NAT Rule ? X

NAT Rule: **Manual NAT Rule** Insert: **In Category** NAT Rules Before

Type: **Static** Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects ↻

zone

inside-zone
outside-zone

Add to Source
Add to Destination

Source Interface Objects (1)

inside-zone

Destination Interface Objects (1)

outside-zone

OK Cancel

Add NAT Rule ? X

NAT Rule: **Manual NAT Rule** Insert: **In Category** NAT Rules Before

Type: **Static** Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* **Inside_Net**

Original Destination: **Address**

AnyConnect_Pool

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: **Address**

Inside_Net

Translated Destination: **AnyConnect_Pool**

Translated Source Port:

Translated Destination Port:

OK Cancel

Daarnaast is de FTD ingesteld om een routerraadpleging uit te voeren op dit verkeer en niet op proxy-ARP. Klik op **OK** als u klaar bent.

Add NAT Rule ? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

4. Klik op Opslaan.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates You have unsaved changes Show Warnings

FTD-2-NAT-Policy
Enter Description Policy Assignments (1)

Rules Add Rule

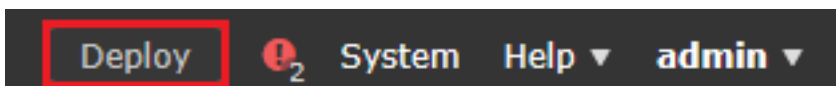
Filter by Device

| # | Direction | Type | Original Packet | | Translated Packet | | Orig... Services | Translated Sources | Translated Destinations | Trans... Services | Options |
|--------------------|-----------|---------|-------------------------|------------------------------|-------------------|-----------------------|------------------|--------------------|-------------------------|-------------------|---|
| | | | Source Interface Object | Destination Interface Object | Original Sources | Original Destinations | | | | | |
| ▼ NAT Rules Before | | | | | | | | | | | |
| 1 | ↔ | Static | inside-zone | outside-zone | Inside_Net | AnyConnect_Pool | | Inside_Net | AnyConnect_Pool | | Dns:false route-lookup no-proxy-arp |
| ▼ Auto NAT Rules | | | | | | | | | | | |
| = | → | Dynamic | any | outside-zone | obj-any | | | Interface | | | Dns:false |
| ▼ NAT Rules After | | | | | | | | | | | |

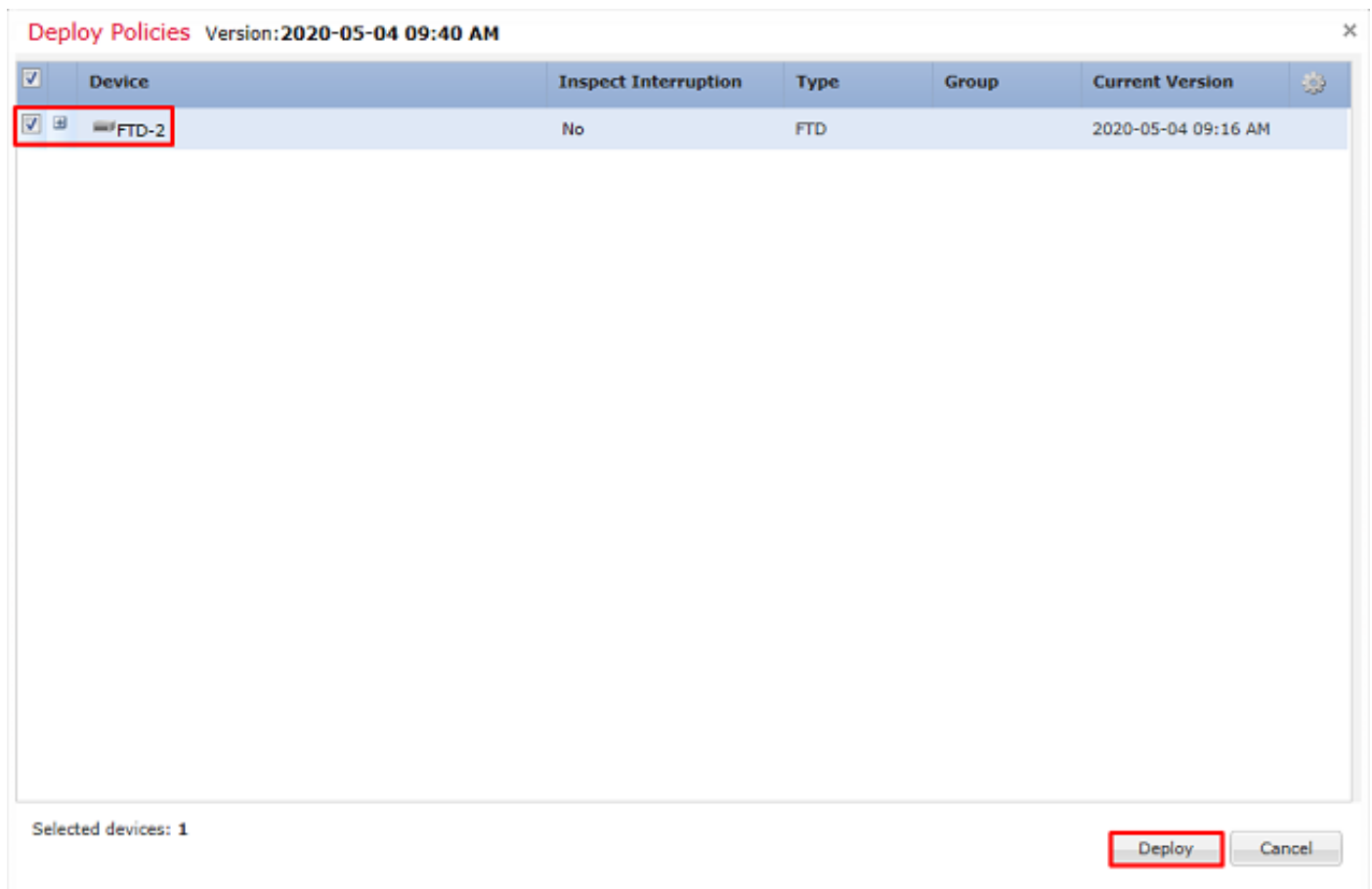
Displaying 1-2 of 2 rows | Page 1 of 1 | Rows per page: 100

Implementeren

1. Wanneer de configuratie is voltooid, klikt u op de knop **Implementeren** rechtsboven.



2. Klik op het selectievakje naast de FTD als de configuratie erop wordt toegepast en klik vervolgens op **Implementeren**.



Verifiëren

Laatste configuratie

AAA-configuratie

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

Configuratie AnyConnect

```
> show running-config webvpn
webvpn
  enable Outside
  anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
  anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
  anyconnect profiles Lab disk0:/csm/lab.xml
```

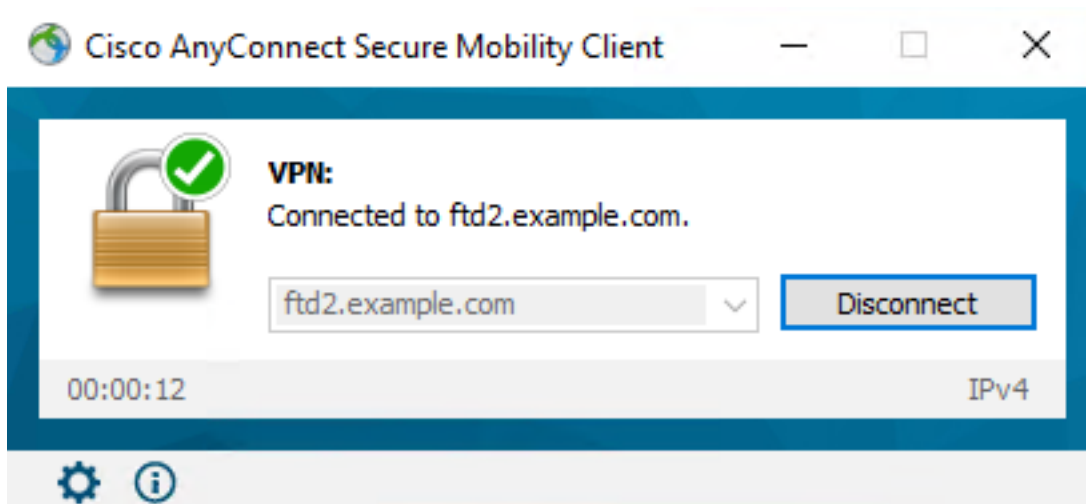
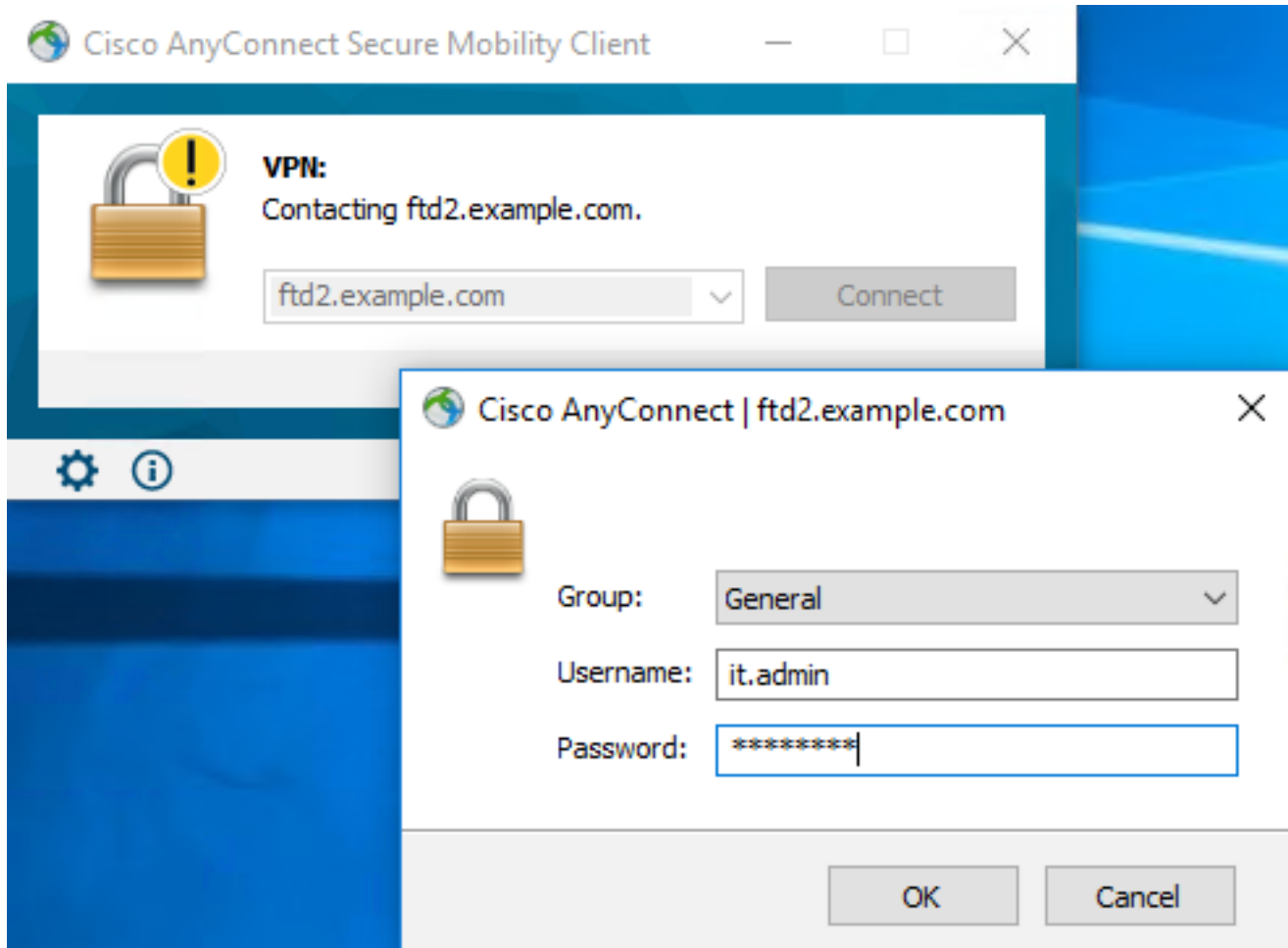
```
anyconnect enable
tunnel-group-list enable
cache
  no disable
error-recovery disable

> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
  address-pool AnyConnect-Pool
  authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
  group-alias General enable

> show running-config group-policy
group-policy DfltGrpPolicy attributes
  vpn-simultaneous-logins 10
  vpn-tunnel-protocol ikev2 ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value Lab
  user-authentication-idle-timeout none
webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
  deny-message none
  anyconnect ssl df-bit-ignore enable

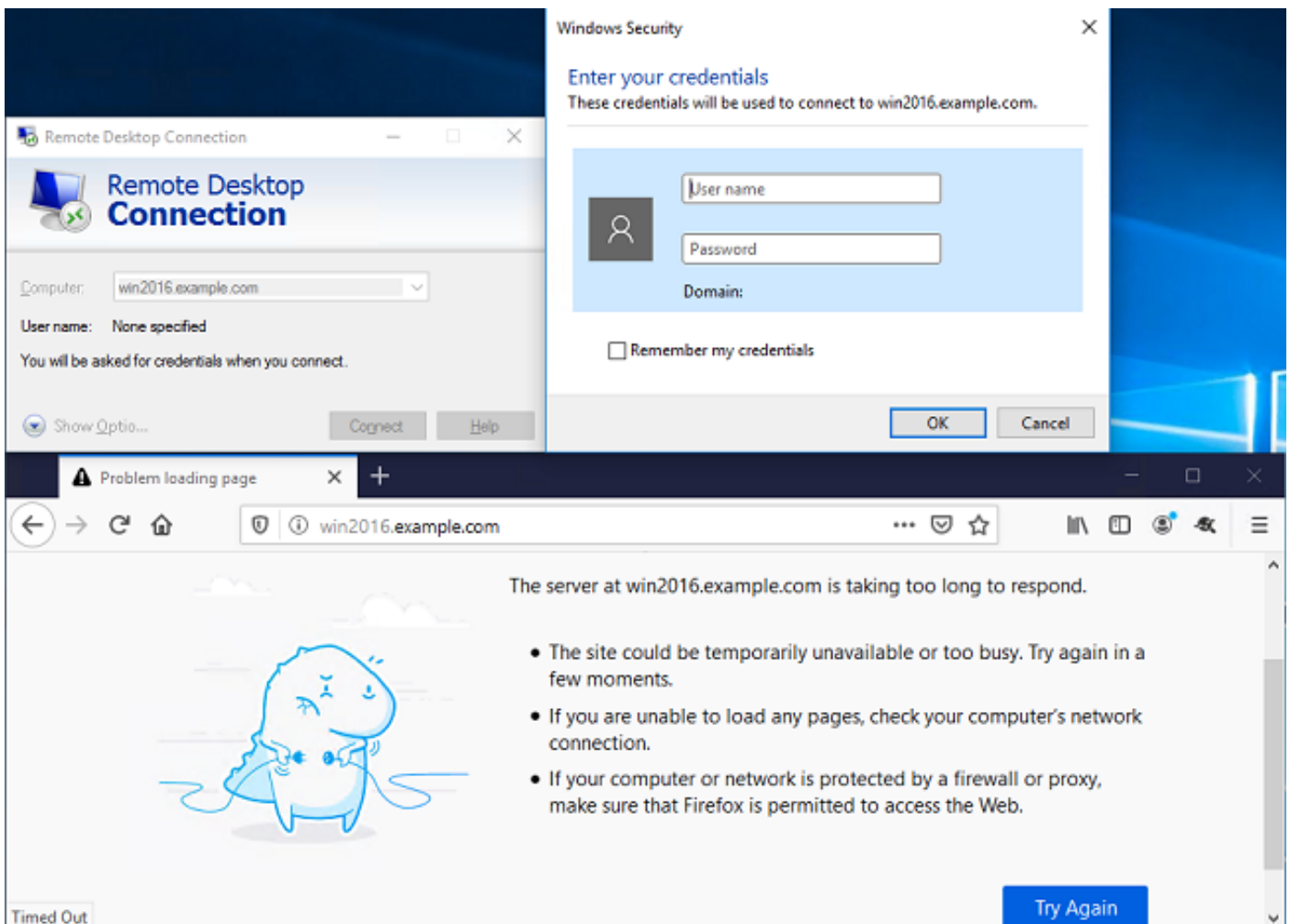
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

Verbinding maken met AnyConnect en toegangscontroleregels controleren

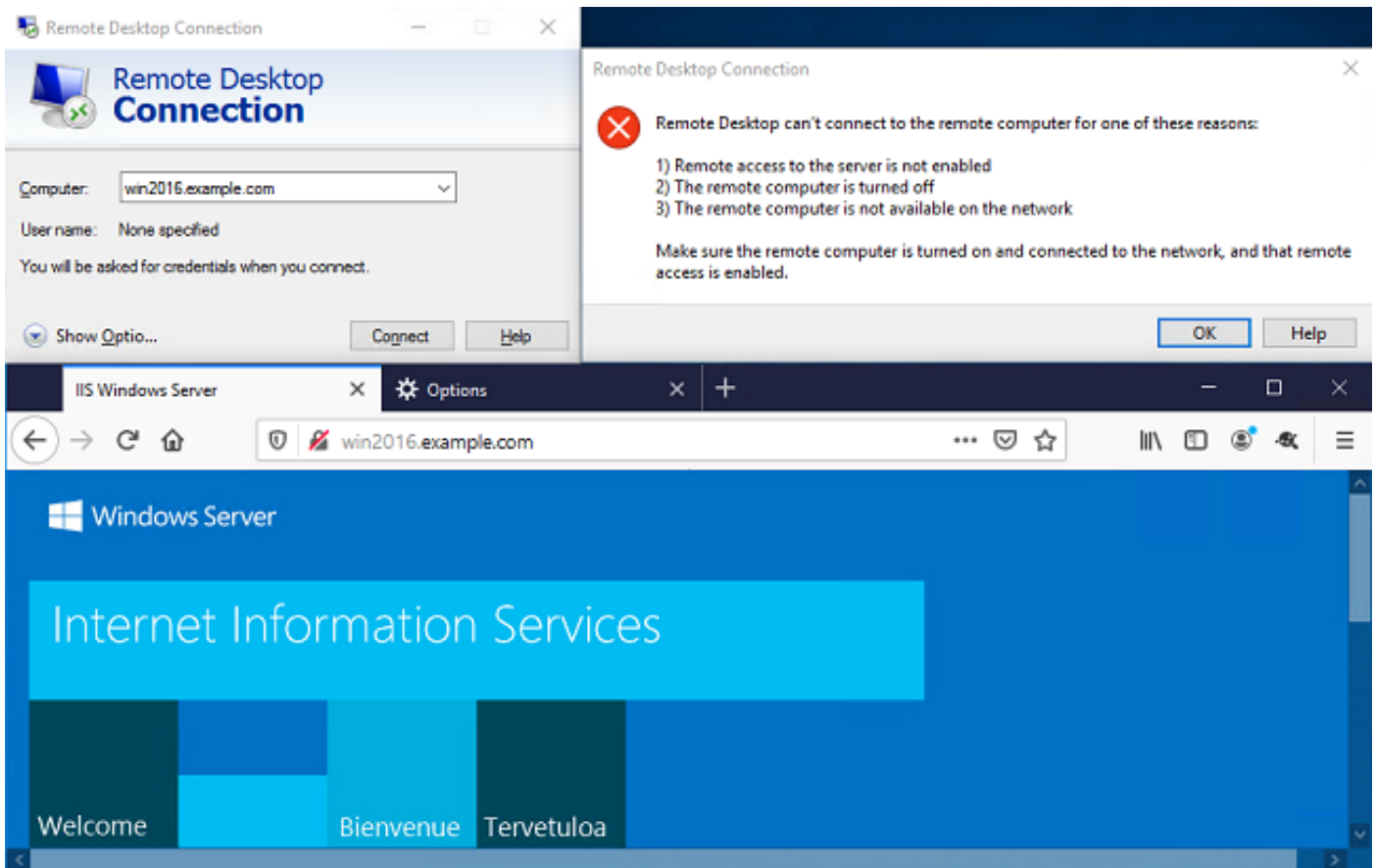


De gebruiker IT Admin bevindt zich in de groep AnyConnect Admins die RDP-toegang heeft tot de Windows-server, maar heeft geen toegang tot HTTP.

Door een RDP- en Firefox-sessie te openen voor deze server wordt geverifieerd dat deze gebruiker alleen toegang heeft tot de server via RDP.



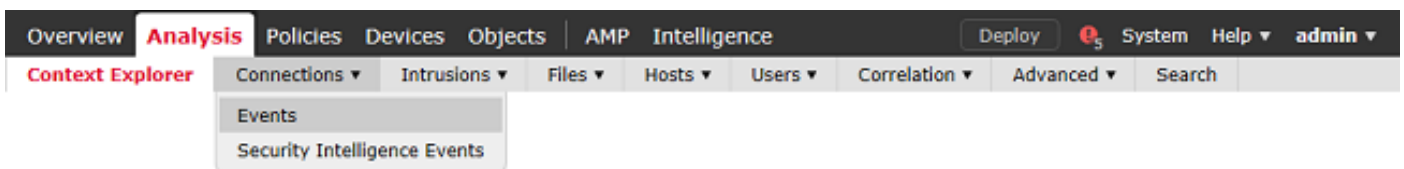
Indien ingelogd met gebruiker Test Gebruiker die in de groep AnyConnect Gebruikers die als HTTP-toegang maar niet RDP-toegang is, kunnen we verifiëren dat de regels van het toegangscontrolebeleid van kracht worden.



Verifiëren met FMC Connection-gebeurtenissen

Aangezien vastlegging is ingeschakeld in de regels voor toegangsbeleid, kunnen de gebeurtenissen van de verbinding worden gecontroleerd op elk verkeer dat aan die regels voldoet

Navigeer naar **Analyse > Verbindingen > Gebeurtenissen**.



Onder de **Tabelweergave van Verbindingsgebeurtenissen** worden de logs gefilterd om alleen verbindingengebeurtenissen voor IT-beheerder weer te geven.

Hier kunt u controleren of RDP-verkeer naar de server (TCP en UDP 389) is toegestaan, maar poort 80 wordt geblokkeerd.

| | Action | Initiator IP | Initiator User | Responder IP | Ingress Security Zone | Egress Security Zone | Source Port / ICMP Type | Destination Port / ICMP Code |
|---|--------|--------------|----------------------------------|--------------|-----------------------|----------------------|-------------------------|------------------------------|
| ↓ | Allow | 10.10.10.1 | it_admin (LAB-AD\it_admin, LDAP) | 192.168.1.1 | outside-zone | inside-zone | 62473 / tcp | 3389 / tcp |
| ↓ | Block | 10.10.10.1 | it_admin (LAB-AD\it_admin, LDAP) | 192.168.1.1 | outside-zone | inside-zone | 62474 / tcp | 80 (http) / tcp |
| ↓ | Block | 10.10.10.1 | it_admin (LAB-AD\it_admin, LDAP) | 192.168.1.1 | outside-zone | inside-zone | 62475 / tcp | 80 (http) / tcp |
| ↓ | Block | 10.10.10.1 | it_admin (LAB-AD\it_admin, LDAP) | 192.168.1.1 | outside-zone | inside-zone | 62476 / tcp | 80 (http) / tcp |

Voor gebruiker **Test Gebruiker**, kunt u verifiëren dat RDP-verkeer naar de server is geblokkeerd en poort 80-verkeer is toegestaan.

| | Action | Initiator IP | Initiator User | Responder IP | Ingress Security Zone | Egress Security Zone | Source Port / ICMP Type | Destination Port / ICMP Code |
|---|--------|--------------|------------------------------------|--------------|-----------------------|----------------------|-------------------------|------------------------------|
| ↓ | Block | 10.10.10.1 | test_user (LAB-AD\test_user, LDAP) | 192.168.1.1 | outside-zone | inside-zone | 62493 / tcp | 3389 / tcp |
| ↓ | Allow | 10.10.10.1 | test_user (LAB-AD\test_user, LDAP) | 192.168.1.1 | outside-zone | inside-zone | 62494 / tcp | 80 (http) / tcp |

Problemen oplossen

Debugs

Deze debug kan worden uitgevoerd in diagnostische CLI om problemen met LDAP-verificatie op te lossen: **debug ldap 255**

Om problemen op te lossen met het toegangsbeleid van de gebruikersidentiteit, kan de **systemondersteuning firewall-engine-debug** in clish worden uitgevoerd om te bepalen waarom verkeer onverwacht wordt toegestaan of geblokkeerd.

LDAP-debuggen werken

```
[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...i.....}...
[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 maken met LDAP-server

```

[-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

```

Mogelijke oplossingen:

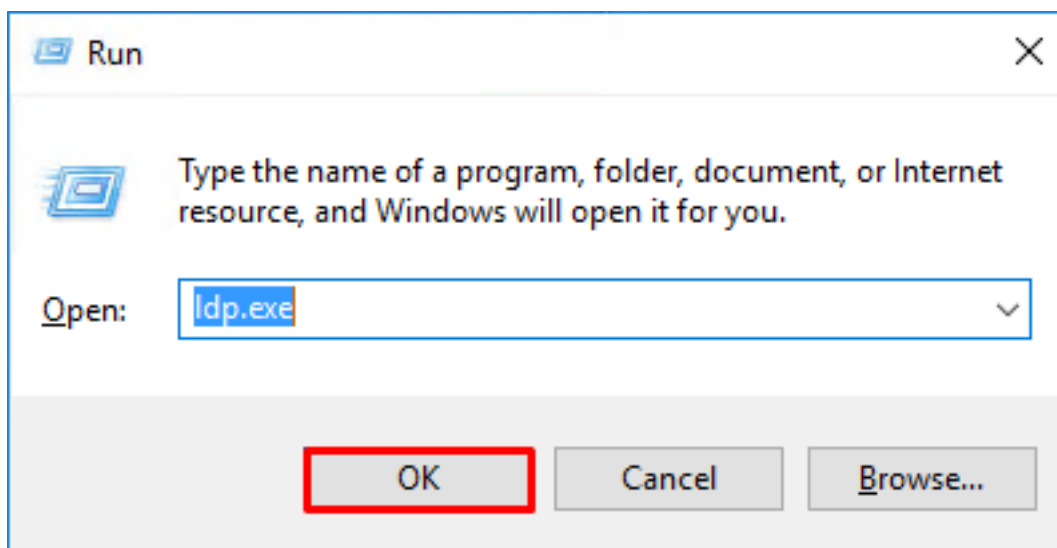
- Controleer de routing en controleer of de FTD een respons ontvangt van de LDAP-server.
- Als LDAPS of STARTTLS wordt gebruikt, zorg ervoor dat het juiste wortel CA certificaat wordt vertrouwd op zodat de SSL handdruk met succes kan voltooien.
- Controleer of het juiste IP-adres en de juiste poort worden gebruikt. Als een hostname wordt gebruikt, controleer of DNS in staat is om het op te lossen naar het juiste IP-adres.

Binding Login DN en/of wachtwoord niet correct

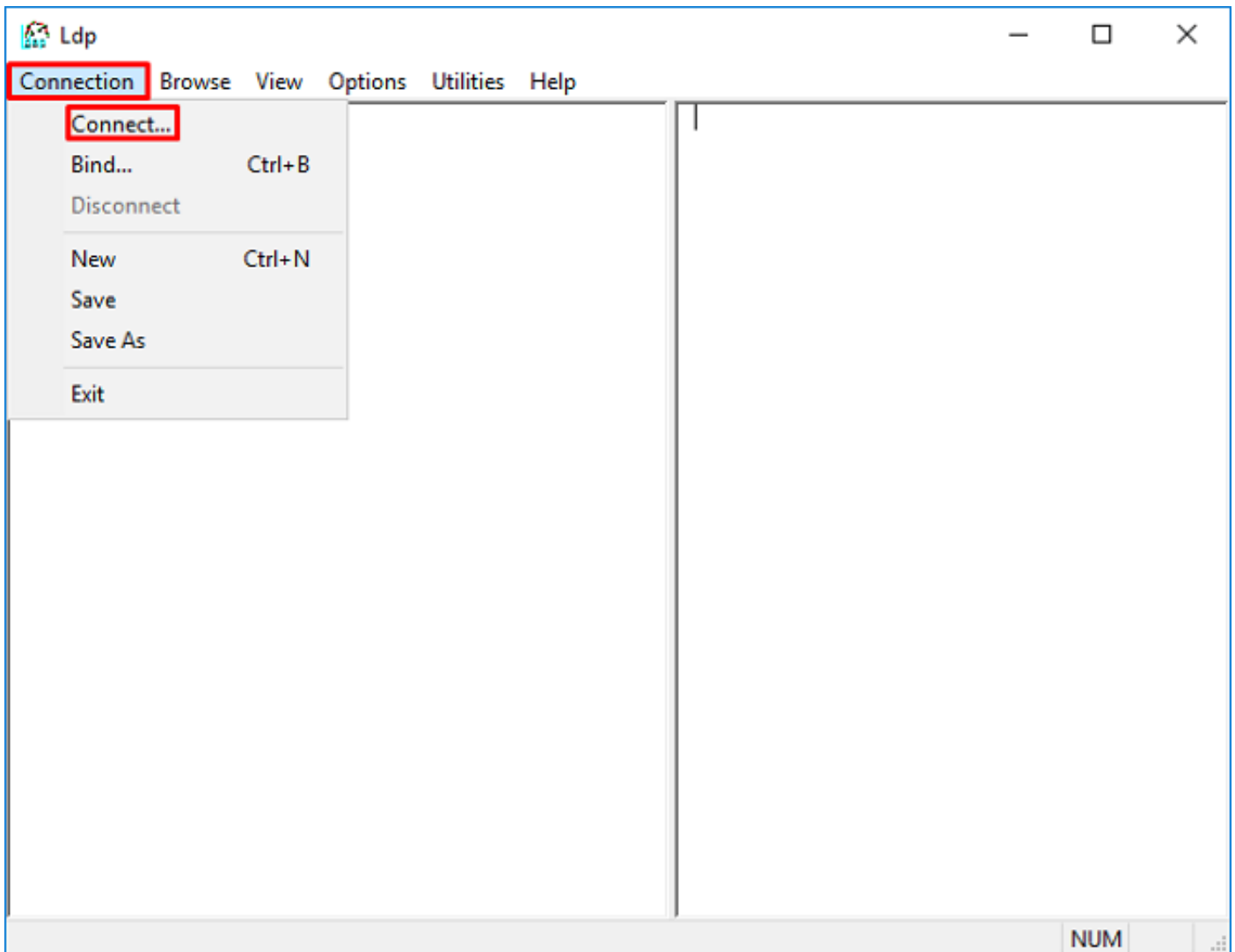
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] 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 of het aanmeldingswachtwoord en het inlogwachtwoord correct zijn ingesteld. Dit kan worden geverifieerd op de AD-server met **ldp.exe**. Ga als volgt te werk om te controleren of een account met succes bindt met behulp van ldp:

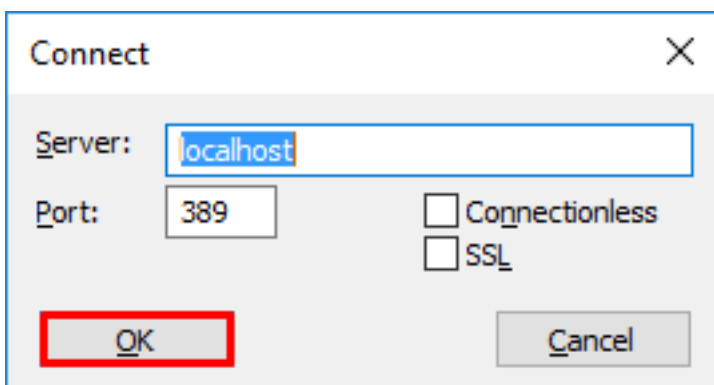
1. Druk op de AD-server op **Win+R** en zoek naar **ldp.exe**



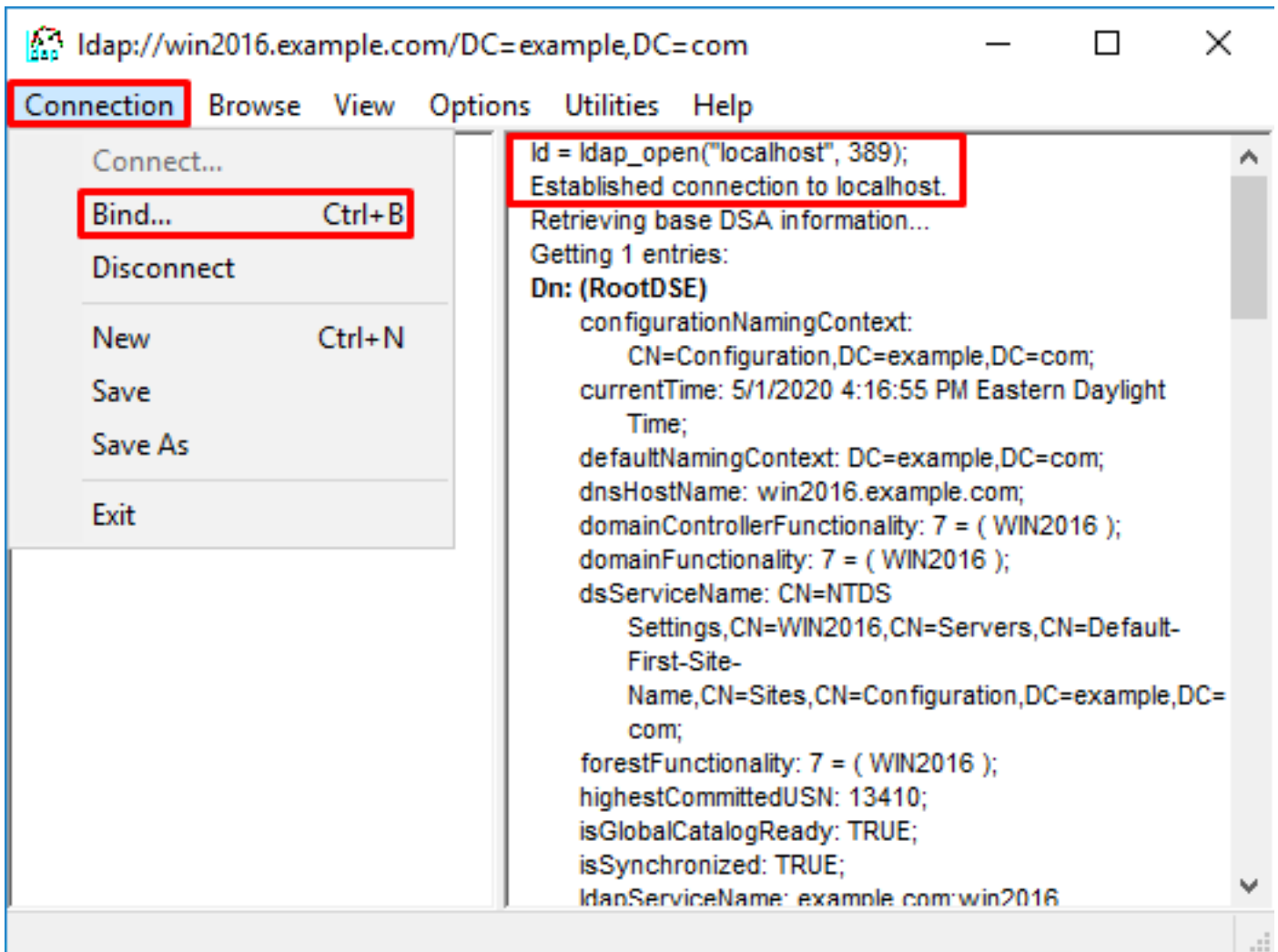
2. Kies onder **Verbinding Connect...**



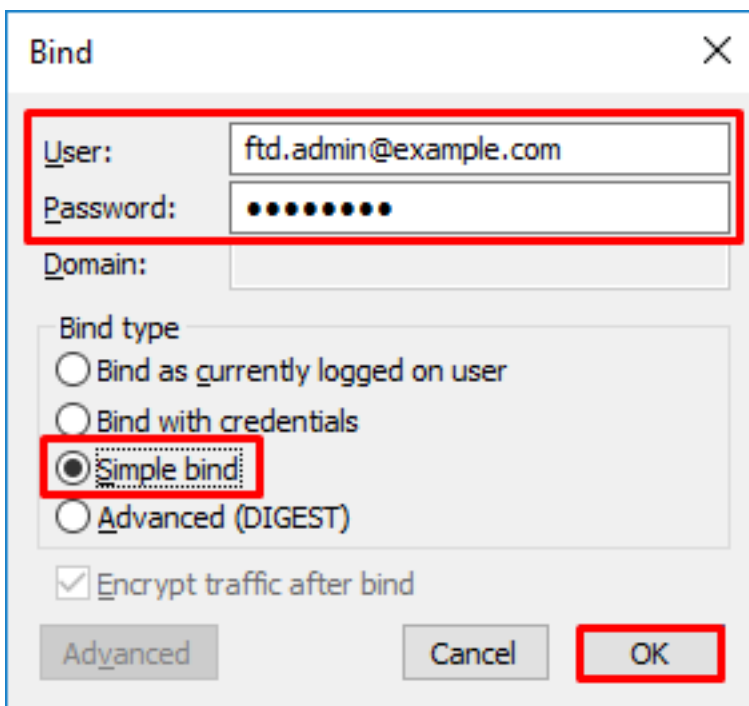
3. Specificeer localhost voor server en de juiste poort en klik vervolgens op **OK**.



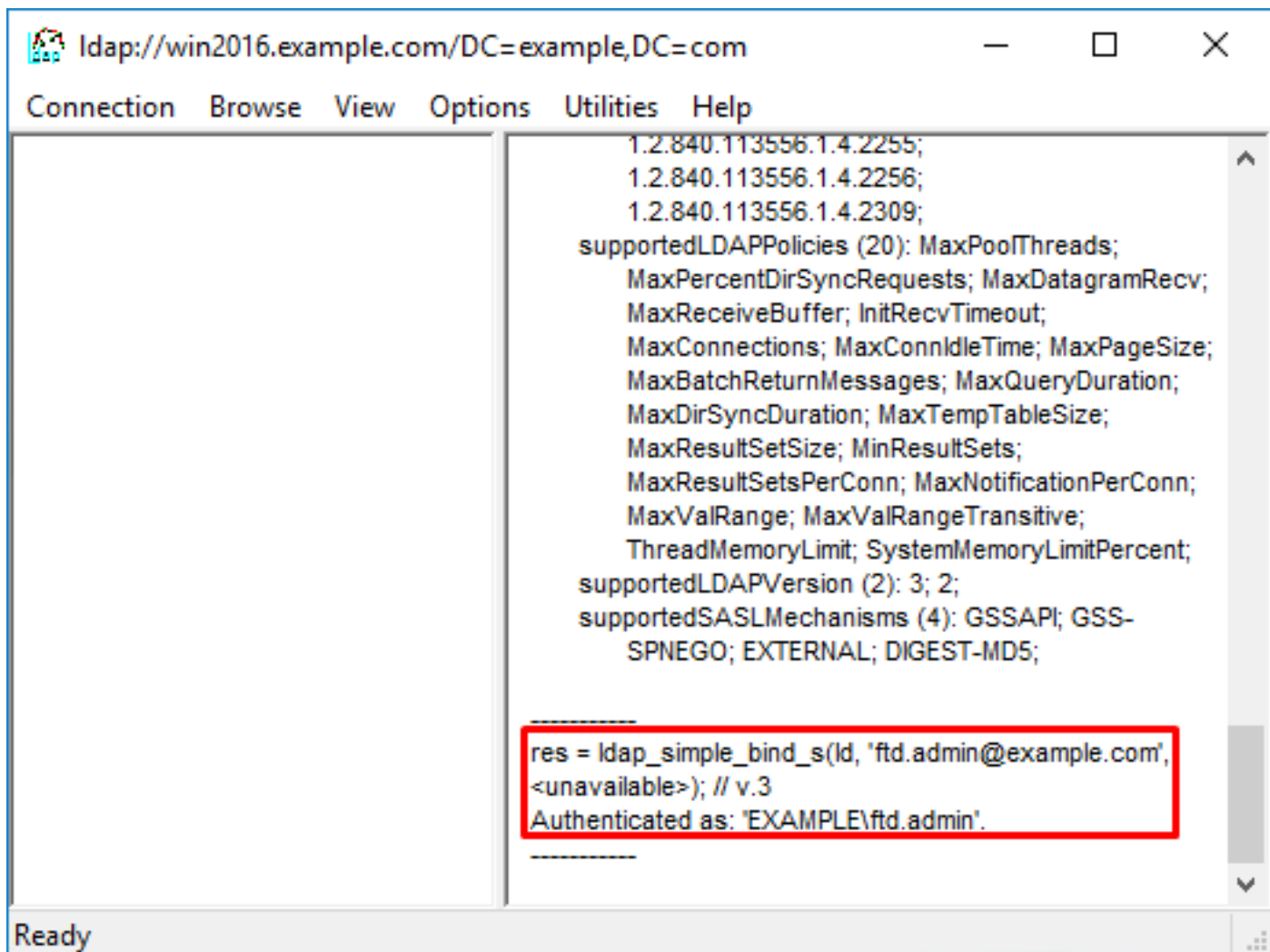
4. De rechterkolom toont tekst die een succesvolle verbinding aangeeft. Navigeren naar **verbinding > binden...**



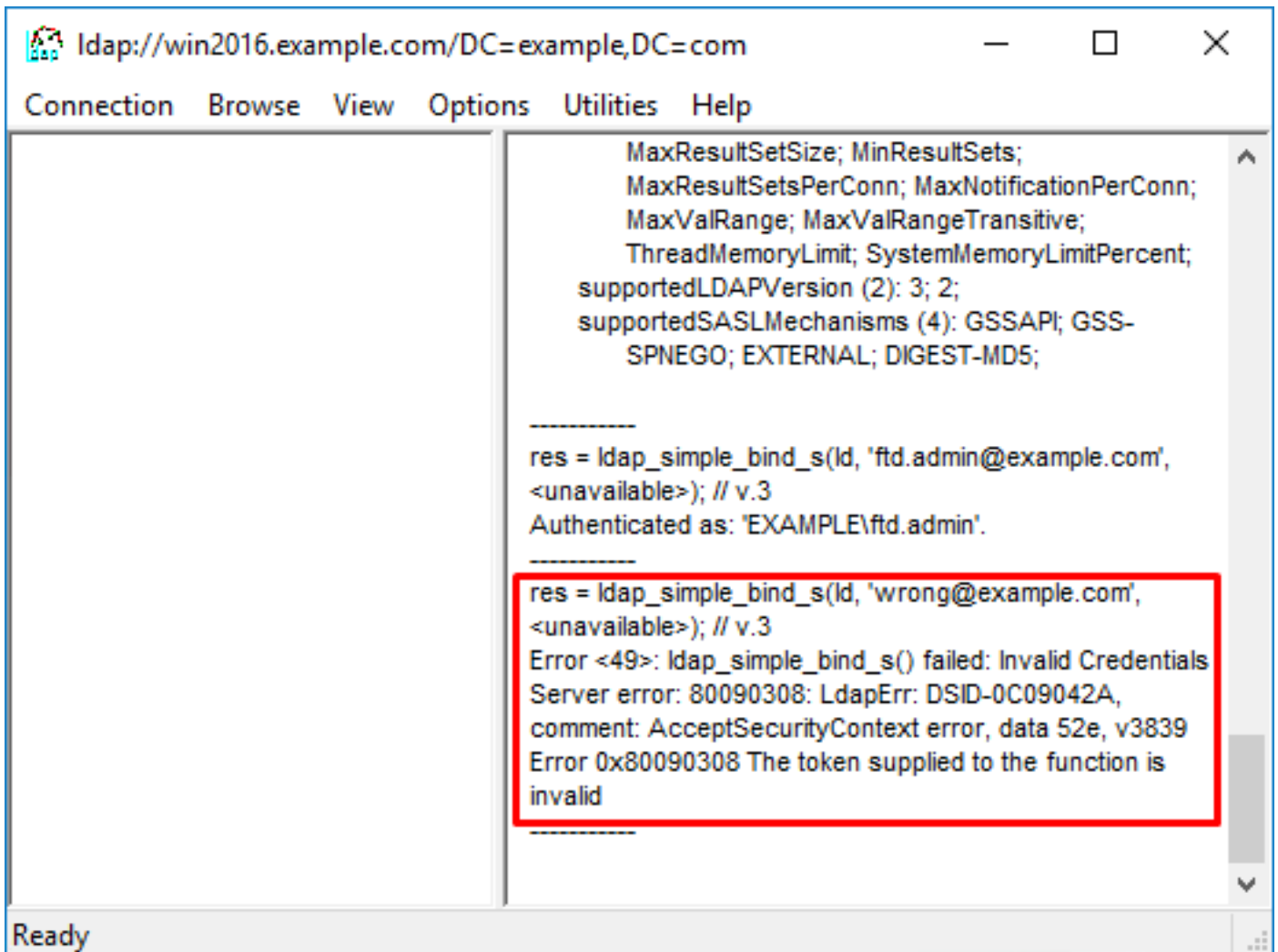
5. Selecteer **Simple Bind** en specificeer vervolgens de **Directory Account Gebruikersnaam** en **Wachtwoord**. Klik op **OK**.



Met een succesvolle bind, Idp toont Authenticated als: **DOMAINusername**



Een poging een bind met een ongeldige gebruikersnaam of wachtwoord resulteert in een mislukking zoals de twee die hier worden gezien.

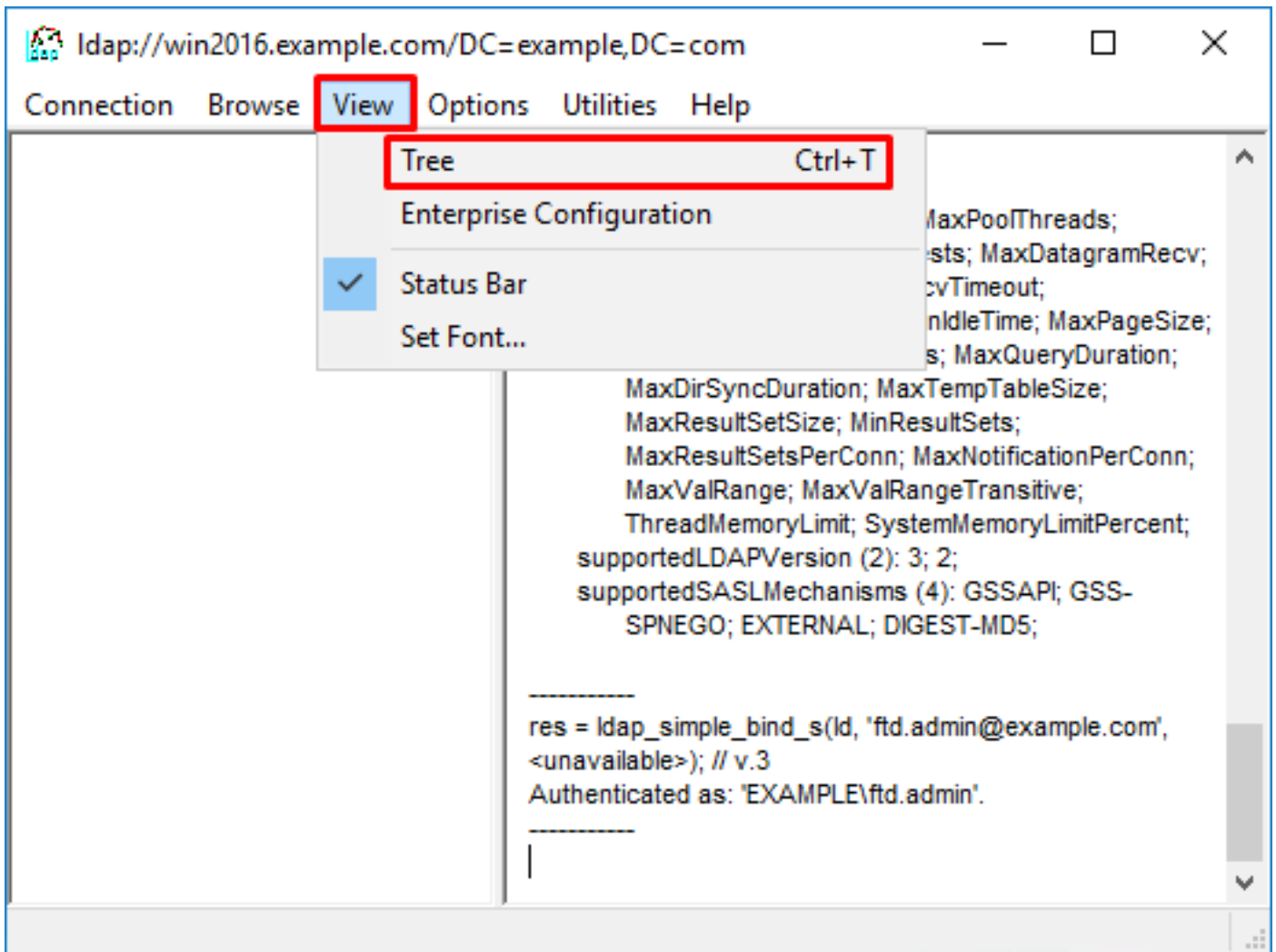


LDAP-server kan de gebruikersnaam niet vinden

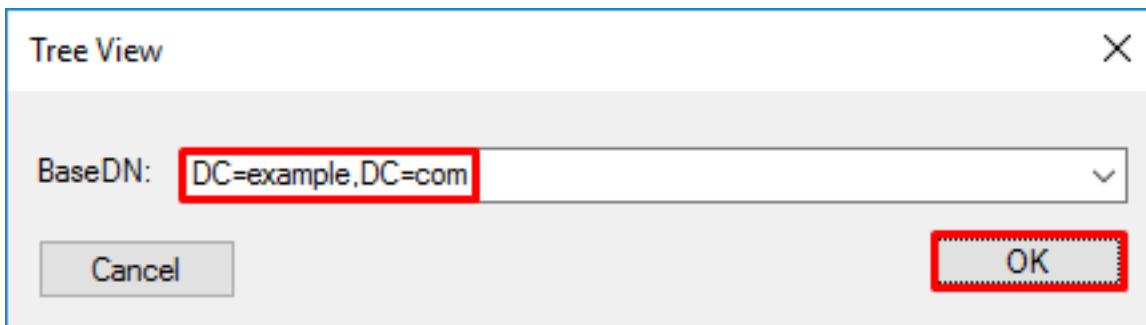
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] 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 zoekactie uitgevoerd door de FTD. Dit kan ook met **ldp.exe** worden gedaan.

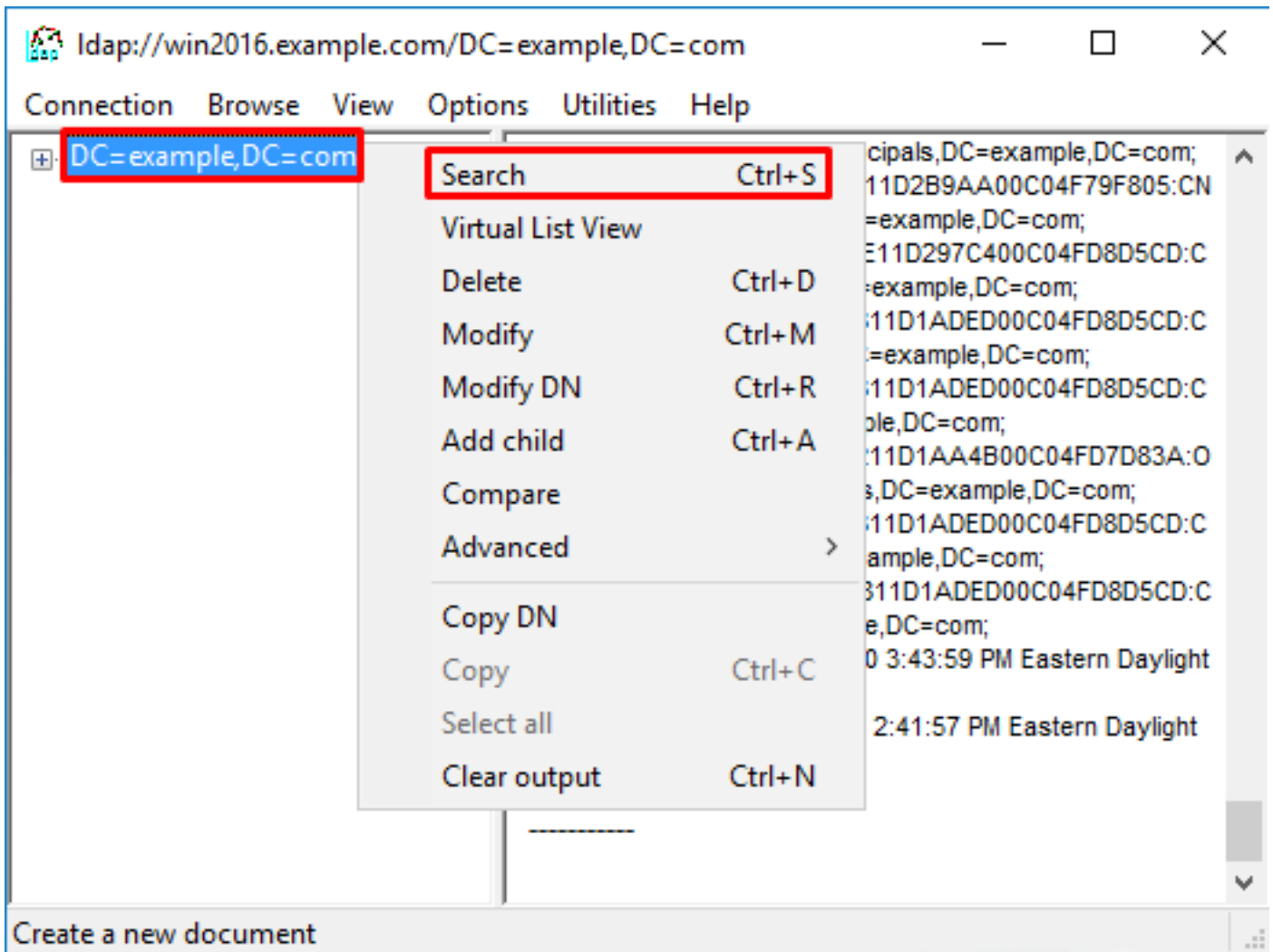
1. Nadat u met succes de bovenstaande binding hebt uitgevoerd, navigeert u naar **Beeld > Boom**.



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



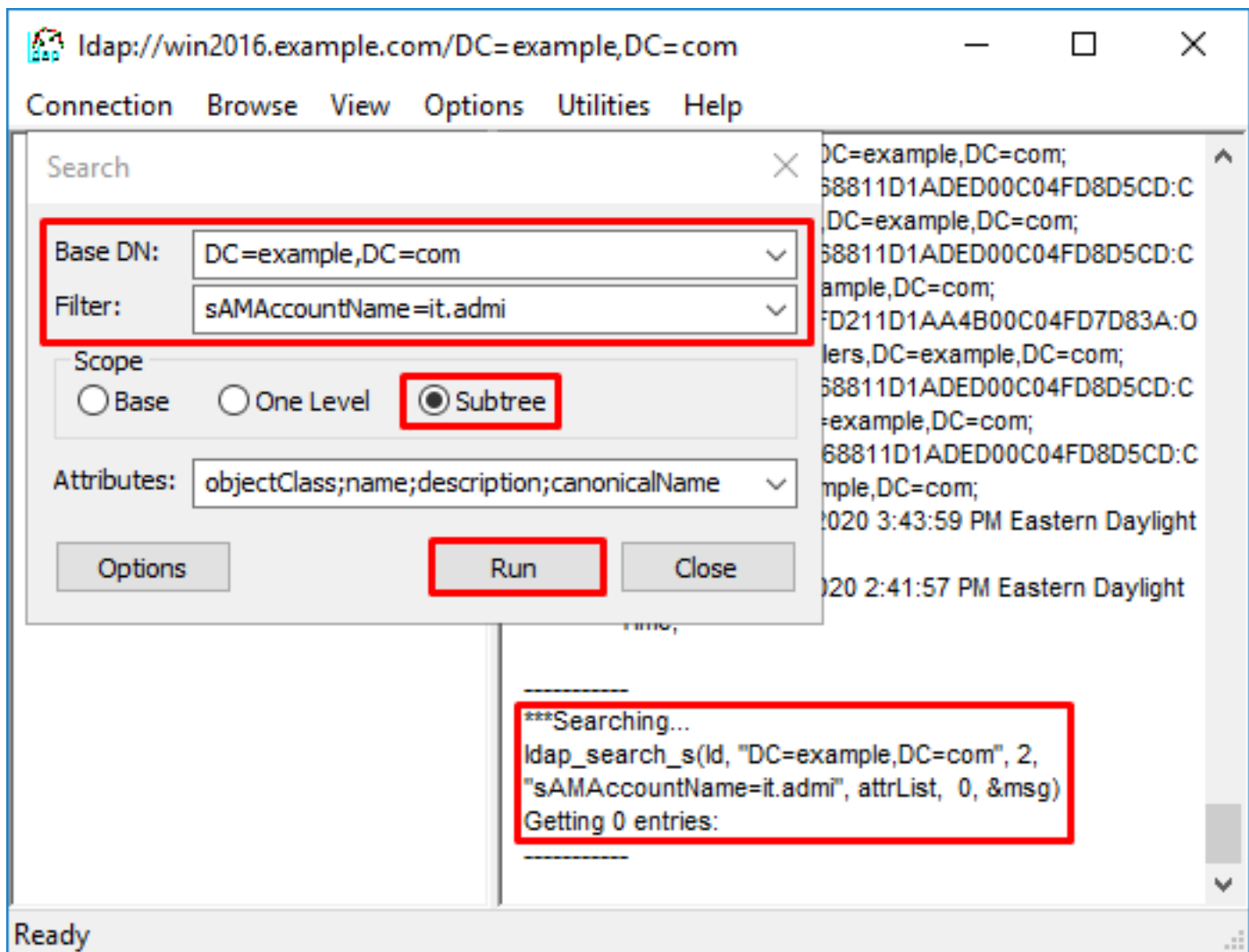
3. Klik met de rechtermuisknop op de Base-DN en klik vervolgens op **Zoeken**.



4. Specificeer dezelfde **Base DB**-, **Filter**- en **Scope**-waarden als in de debugs.

In dit voorbeeld zijn dit:

- Dc=voorbeeld, dc=com
- Filter: samaccountname=it.admi
- Toepassingsgebied:SUBTREE



Idp vindt 0 items te wijten aan er is geen gebruikersaccount met de naam **it.admi** onder de Base DN dc=example,dc=com

Een andere poging met de juiste samaccountnaam **it.admin** toont een ander resultaat. Idp vindt 1 ingang onder de Base DN dc=example, dc=com en drukt die gebruiker DN.

Idap://win2016.example.com/DC=example,DC=com

Connection Browse View Options Utilities Help

Search

Base DN: DC=example,DC=com

Filter: sAMAccountName=it.admin

Scope

Base One Level Subtree

Attributes: objectClass;name;description;canonicalName

Options Run Close

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

***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 de 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 of het gebruikerswachtwoord correct is geconfigureerd en of het niet is verlopen. Net als bij de Login DN doet de FTD een bind tegen AD met de gebruikersreferenties.

Dit bind kan ook worden gedaan in ldp om te verifiëren dat de AD in staat is om dezelfde gebruikersnaam en wachtwoordreferenties te herkennen. De stappen in ldp worden weergegeven in de sectie **Binding Login DN en/of onjuist wachtwoord**.

Daarnaast kunnen de Microsoft server **Event Viewer** logbestanden worden bekeken om een mogelijke reden.

AAA testen

De test **aaa-server** opdracht kan worden gebruikt om een verificatiepoging van de FTD met een specifieke gebruikersnaam en wachtwoord te simuleren. Hiermee kan worden getest op verbinding- of verificatiefouten. Dit commando is **test aaa-server verificatie [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
```

PacketCapture

Packet-opnamen kunnen worden gebruikt om de bereikbaarheid naar de AD-server te verifiëren. Als LDAP-pakketten de FTD verlaten, maar er is geen respons, kan dit wijzen op een routeringsprobleem.

Capture toont het tweerichtingsverkeer LDAP.

```
> 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

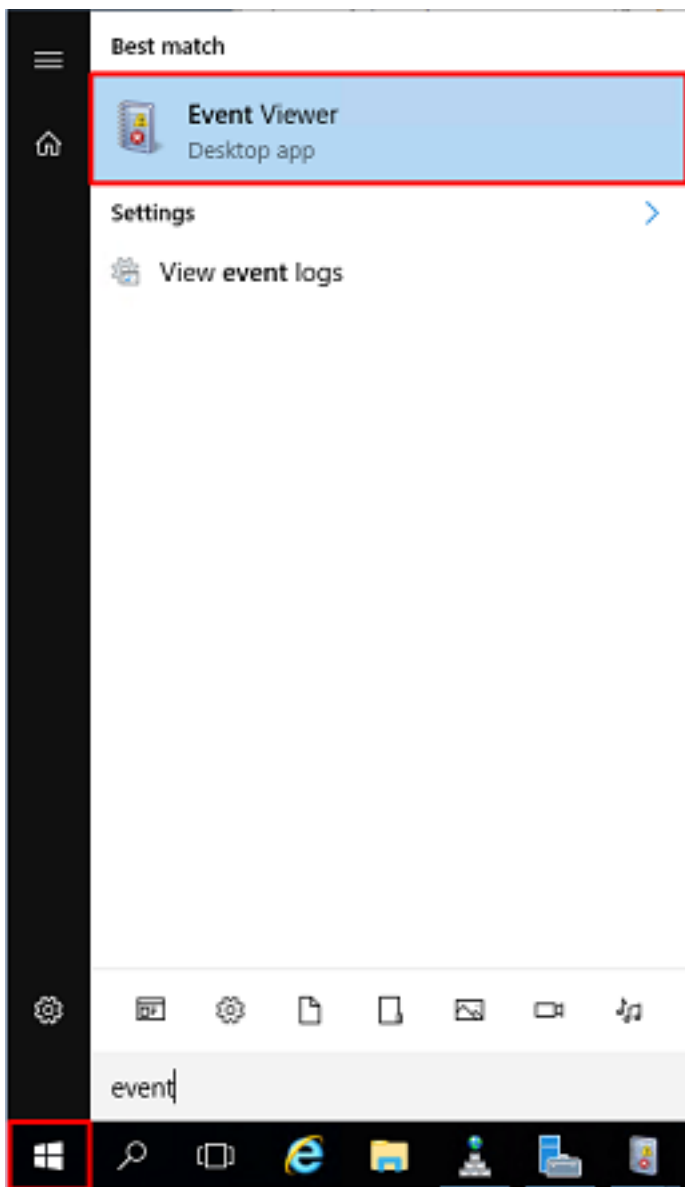
54 packets captured

  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>
[...]
```

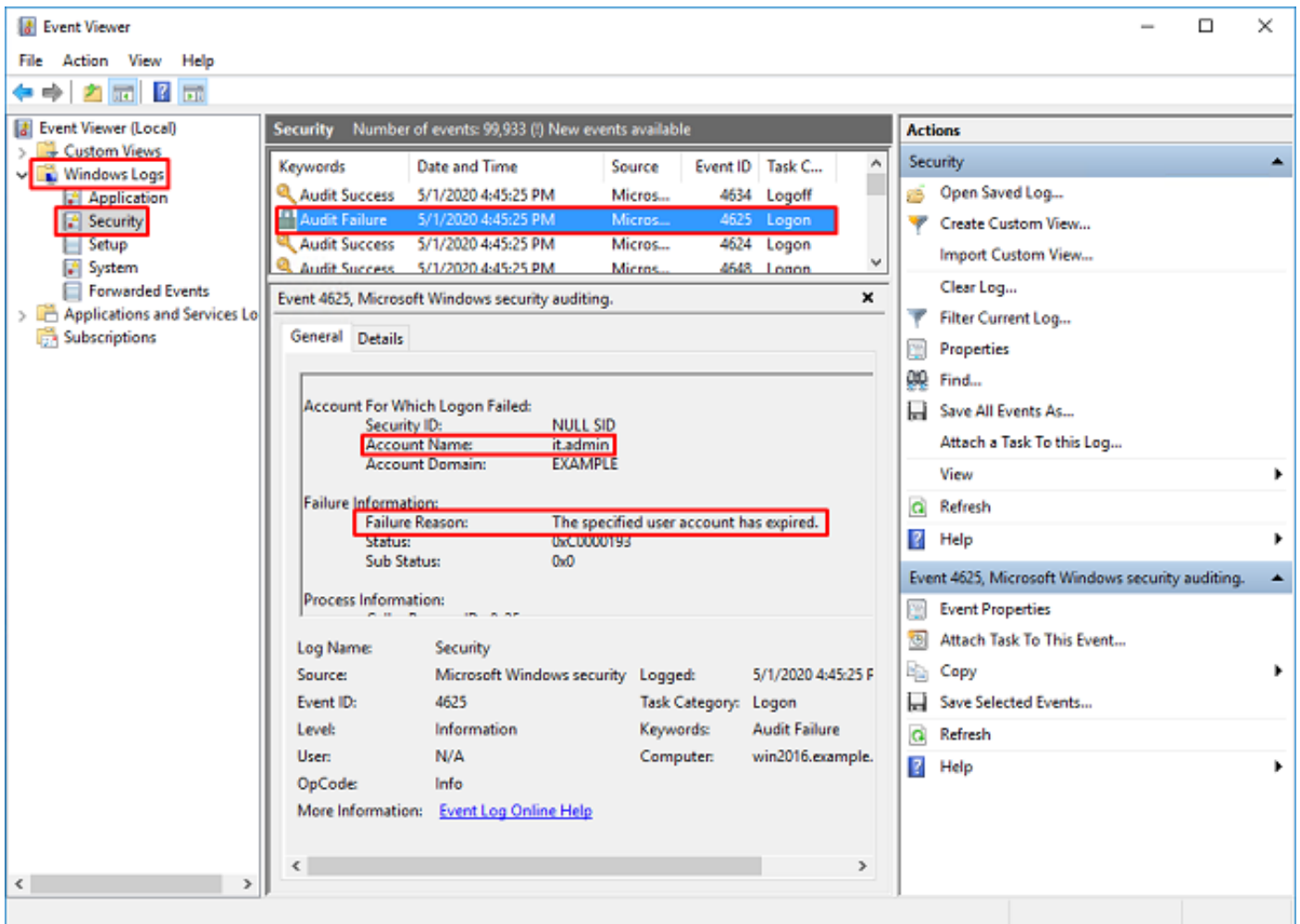
Logbestanden van Windows Server Event Viewer

De Event Viewer logt in op de AD-server en kan gedetailleerdere informatie geven over de oorzaak van een fout.

1. Zoek naar en open Event Viewer.



2. **Windows-logbestanden** uitvouwen en op **Beveiliging** klikken. Zoek naar **auditfouten** met de naam van de gebruikersaccount en bekijk de foutinformatie.



An account failed to log on.

Subject:

Security ID:SYSTEM
Account Name:WIN2016\$\nAccount 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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.