Wachtwoordbeheer configureren met LDAP's voor RA VPN op FTD beheerde via FMC

Inhoud

Inleiding

Dit document beschrijft het configureren van wachtwoordbeheer met LDAP's voor AnyConnect Clients die verbinding maken met Cisco Firepower Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis te hebben van deze onderwerpen:

- Basiskennis van de configuratie van RA VPN (Remote Access Virtual Private Network) op FMC
- Basiskennis van de LDAP-serverconfiguratie op het VCC
- Basiskennis van Active Directory

Gebruikte componenten

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

- Microsoft 2012 R2-server
- FMCv met 7.3.0
- FTDv met 7.3.0

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.

Configuratie

Netwerkdiagram en -scenario

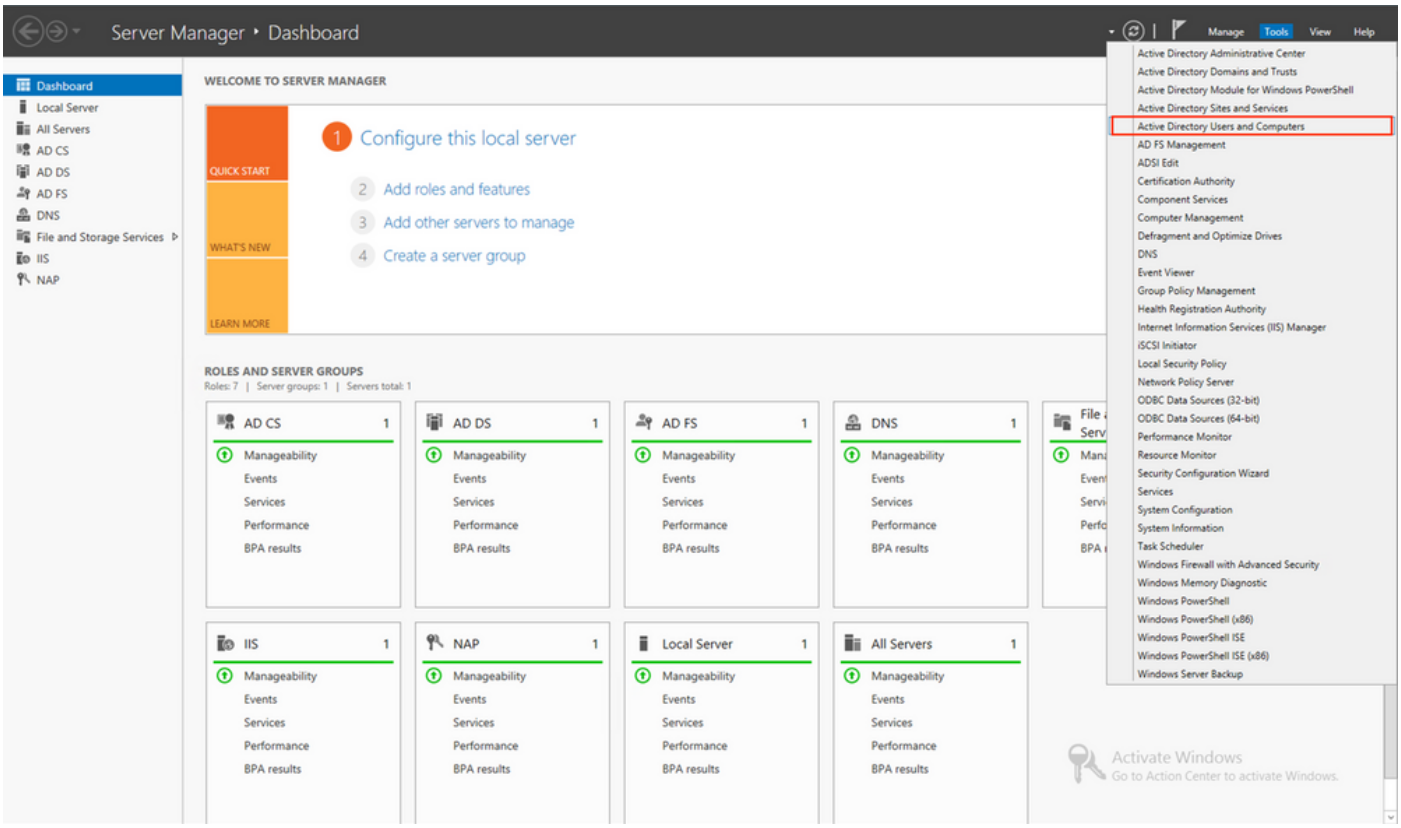
Windows-server is vooraf geconfigureerd met ADDS en ADCS om het wachtwoordbeheerproces van de gebruiker te testen. In deze configuratiehandleiding worden deze gebruikersaccounts gemaakt.

Gebruikersaccounts:

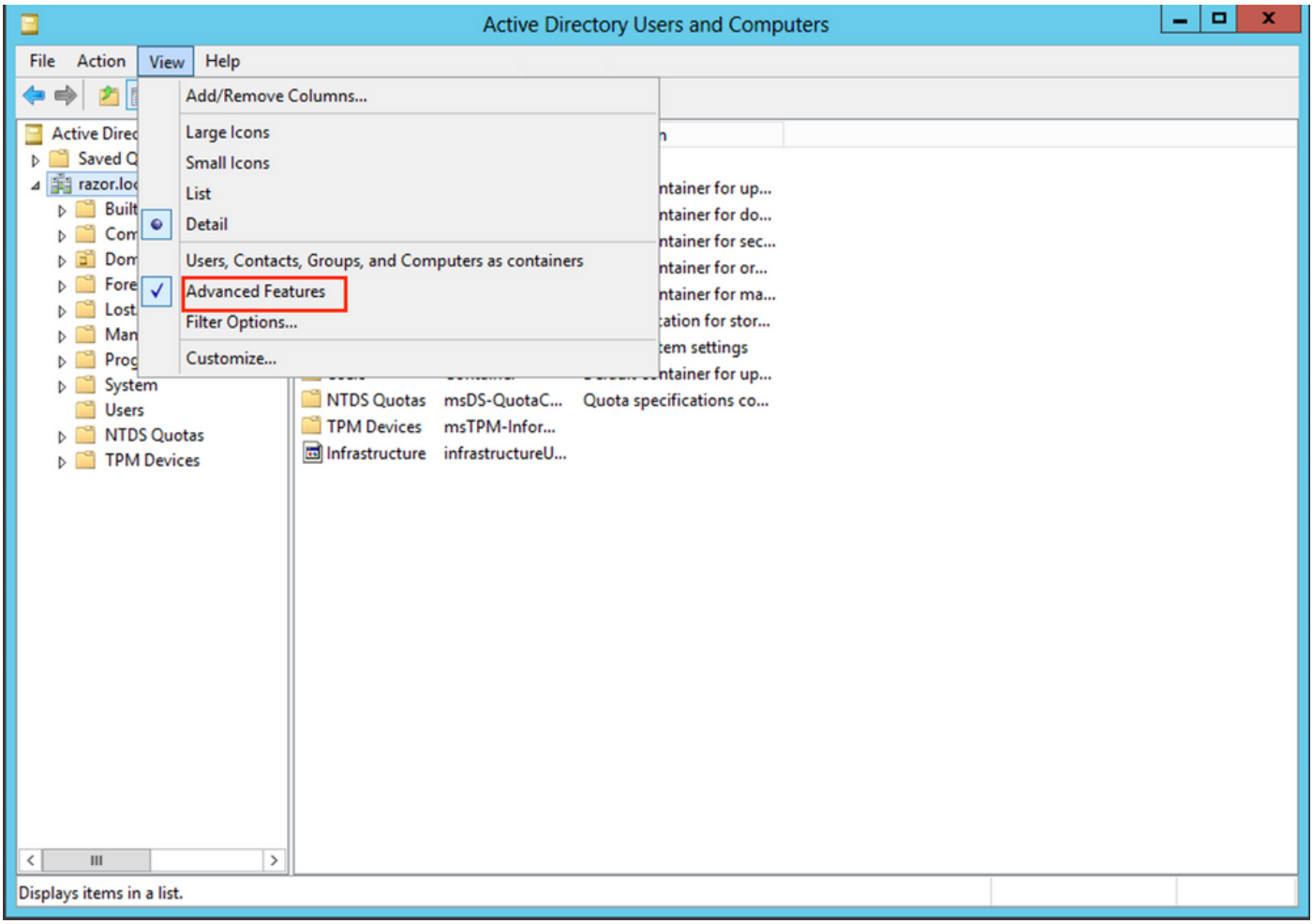
- Beheerder: Dit wordt gebruikt als de directory account om de FTD te kunnen binden aan de Active Directory-server.
- admin: Een account van een testbeheerder waarmee de gebruikersidentiteit wordt aangetoond.

Bepaal LDAP-basis DN en groep DN

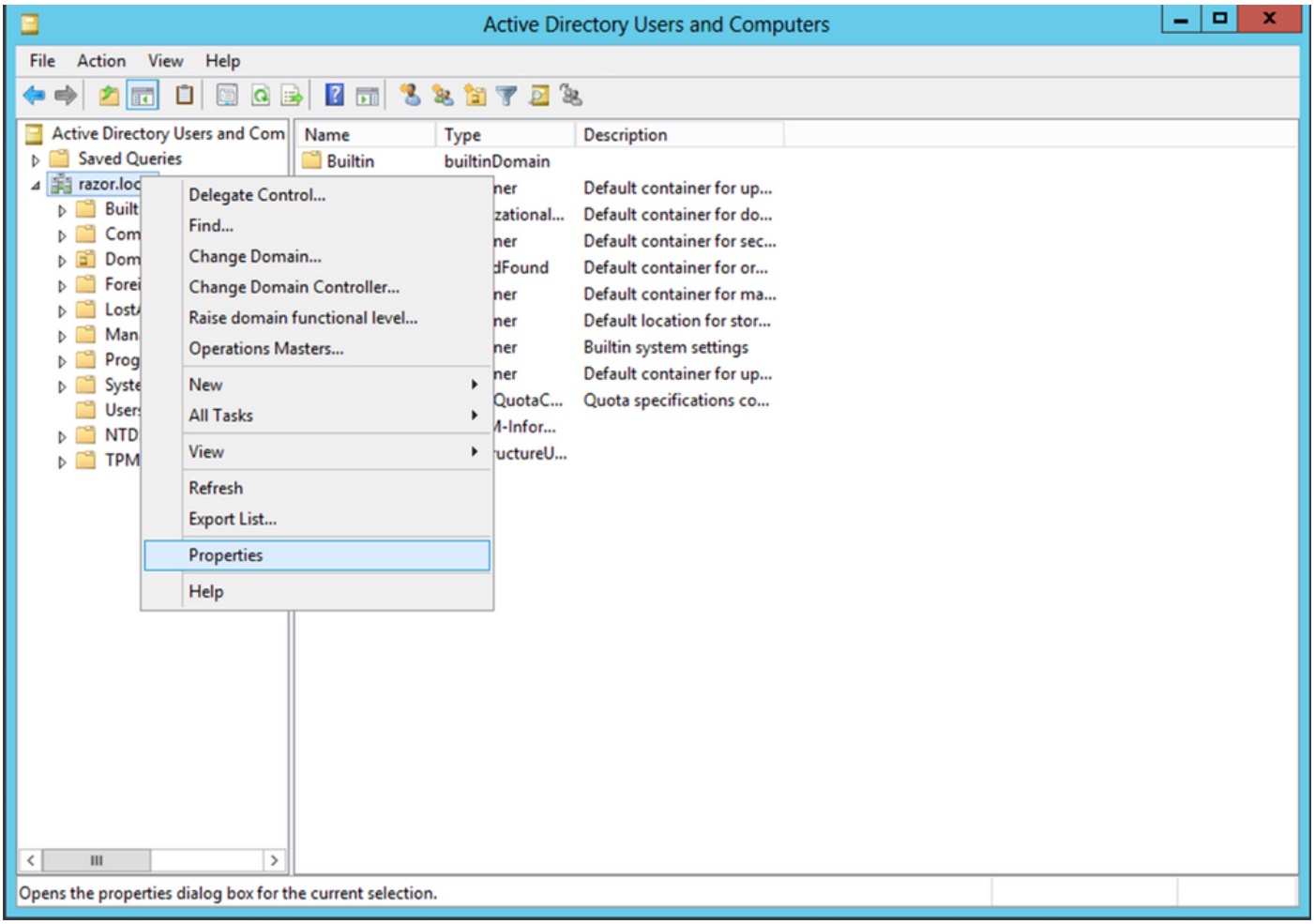
1. Open (Openstaand) Active Directory Users and Computers via het Dashboard van Server Manager.



2. Open de View Option op het bovenpaneel, en laat toe Advanced Features, zoals aangegeven op de afbeelding:



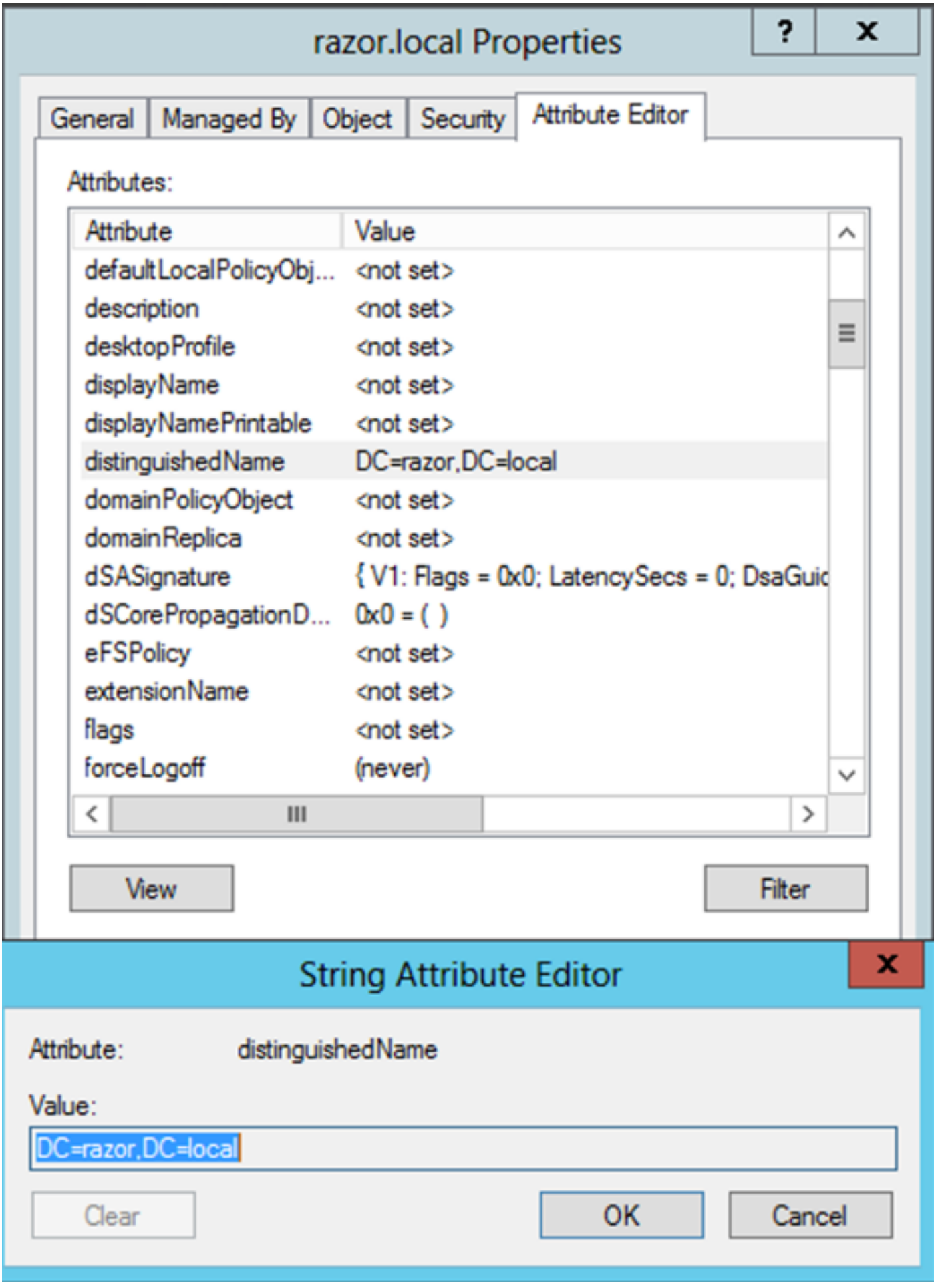
3. Hierdoor kunnen extra eigenschappen worden weergegeven onder de AD-objecten. Bijvoorbeeld om de DN voor de root te vinden razor.local, klik met de rechtermuisknop razor.localen kies vervolgens Properties, zoals getoond in deze afbeelding:



4. Onder Properties, kiest u de Attribute Editor tabblad. Zoeken distinguishedName Klik onder de kenmerken op View, zoals aangegeven in de afbeelding.

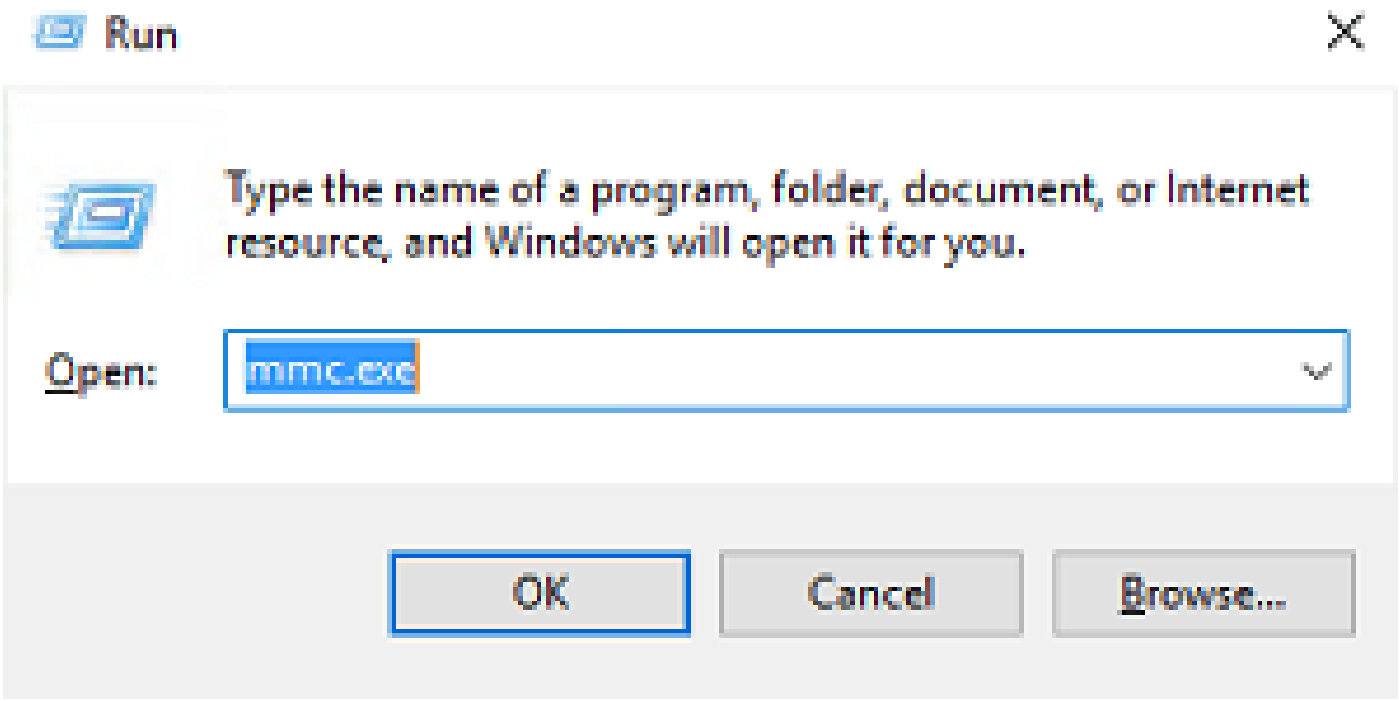
Dit opent een nieuw venster waar de DN kan worden gekopieerd en later in FMC kan worden geplakt.

In dit voorbeeld, de wortel DN is DC=razor, DC=local. Kopieert de waarde en sla deze op voor later gebruik. Klik op de knop OK om het venster String Attribute Editor te verlaten en op te klikken OK om de Eigenschappen te verlaten.

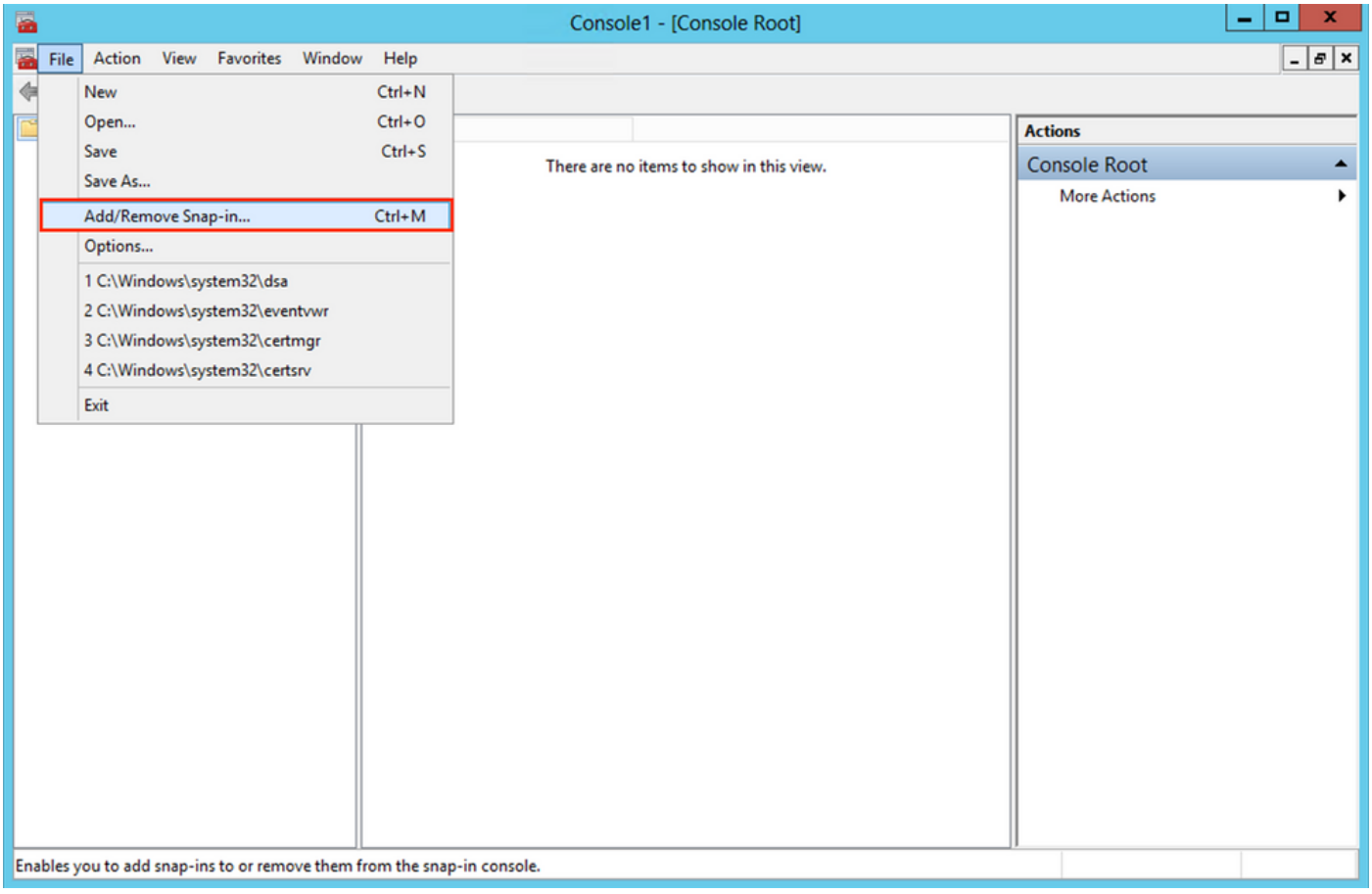

razor.local Properties
General
Managed By
Object
Security
Attribute Editor
Attributes:
Attribute
Value
defaultLocalPolicyObj...
<not set>
description
<not set>
desktopProfile
<not set>
displayName
<not set>
displayNamePrintable
<not set>
distinguishedName
DC=razor,DC=local
domainPolicyObject
<not set>
domainReplica
<not set>
dSASignature
{ V1: Flags = 0x0; LatencySecs = 0; DsaGuic
dSCorePropagationD...
0x0 = ( )
eFSPolicy
<not set>
extensionName
<not set>
flags
<not set>
forceLogoff
(never)
View
Filter
String Attribute Editor
Attribute:
distinguishedName
Value:
DC=razor,DC=local
Clear
OK
Cancel

Kopieert de SSL-certificaatsleuf van LDAPS

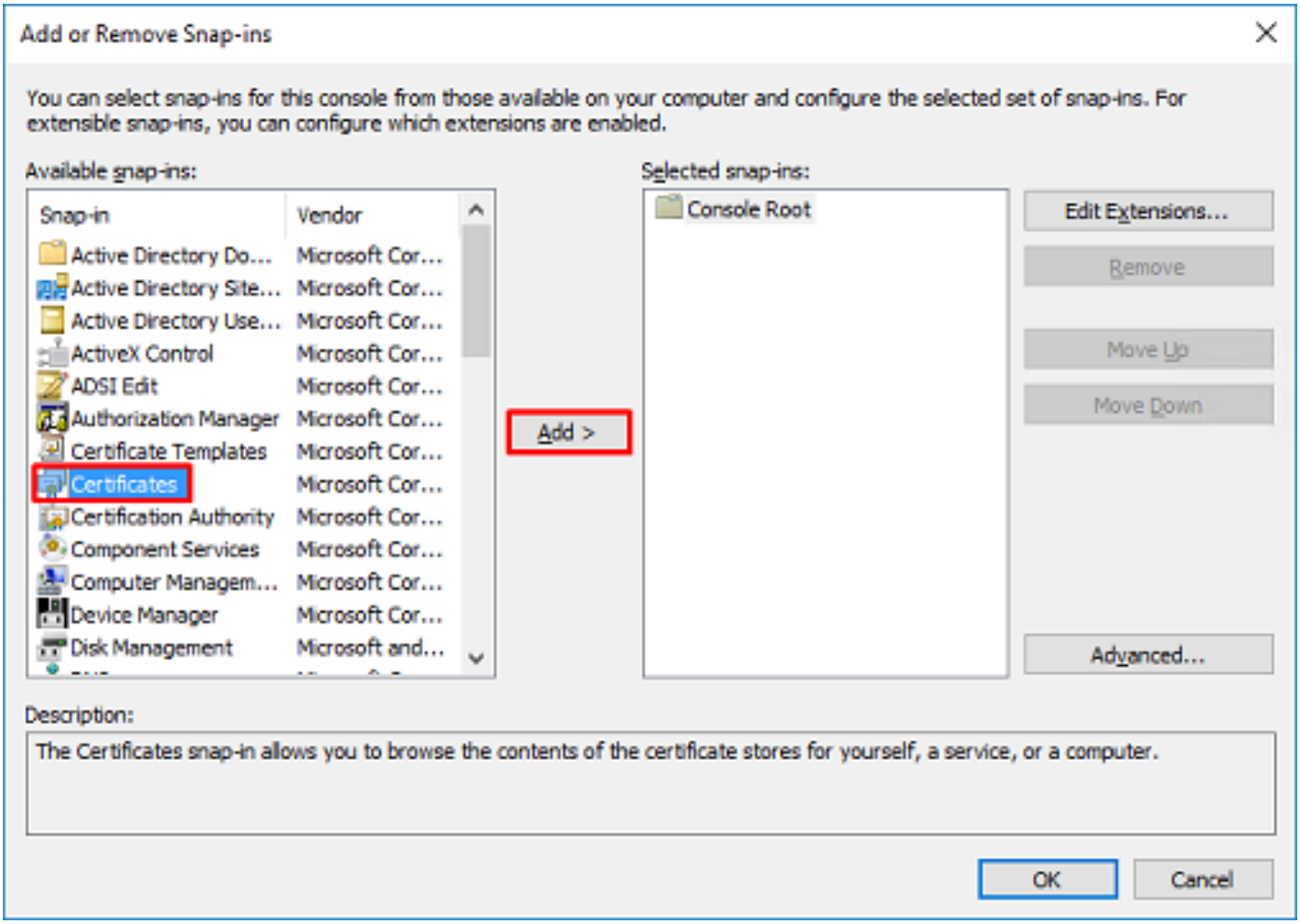
1. Druk Win+R en mmc.exeklikt u vervolgens op OK, zoals in deze afbeelding wordt getoond.



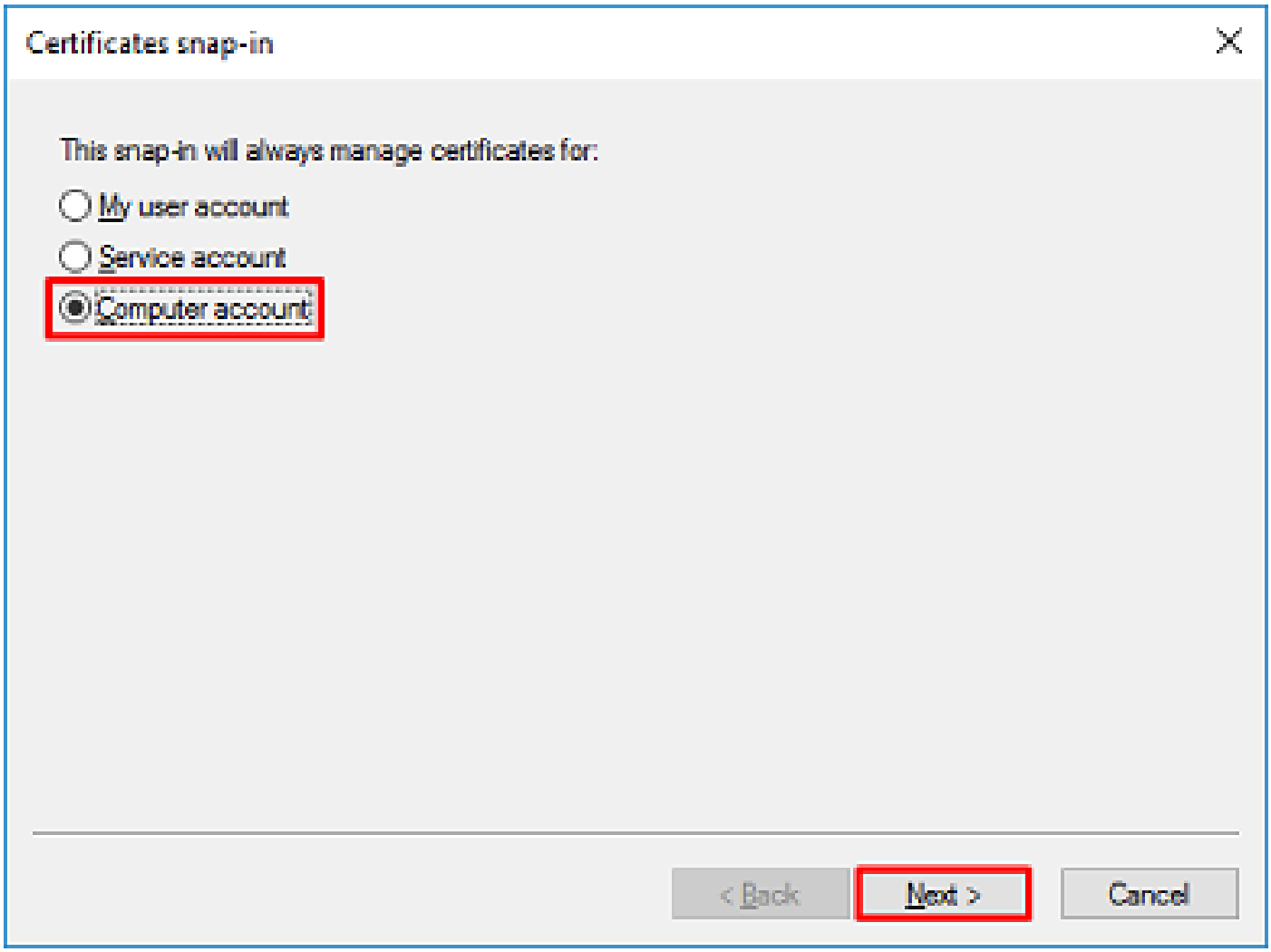
2. Naar navigeren File > Add/Remove Snap-in..., zoals in deze afbeelding getoond:



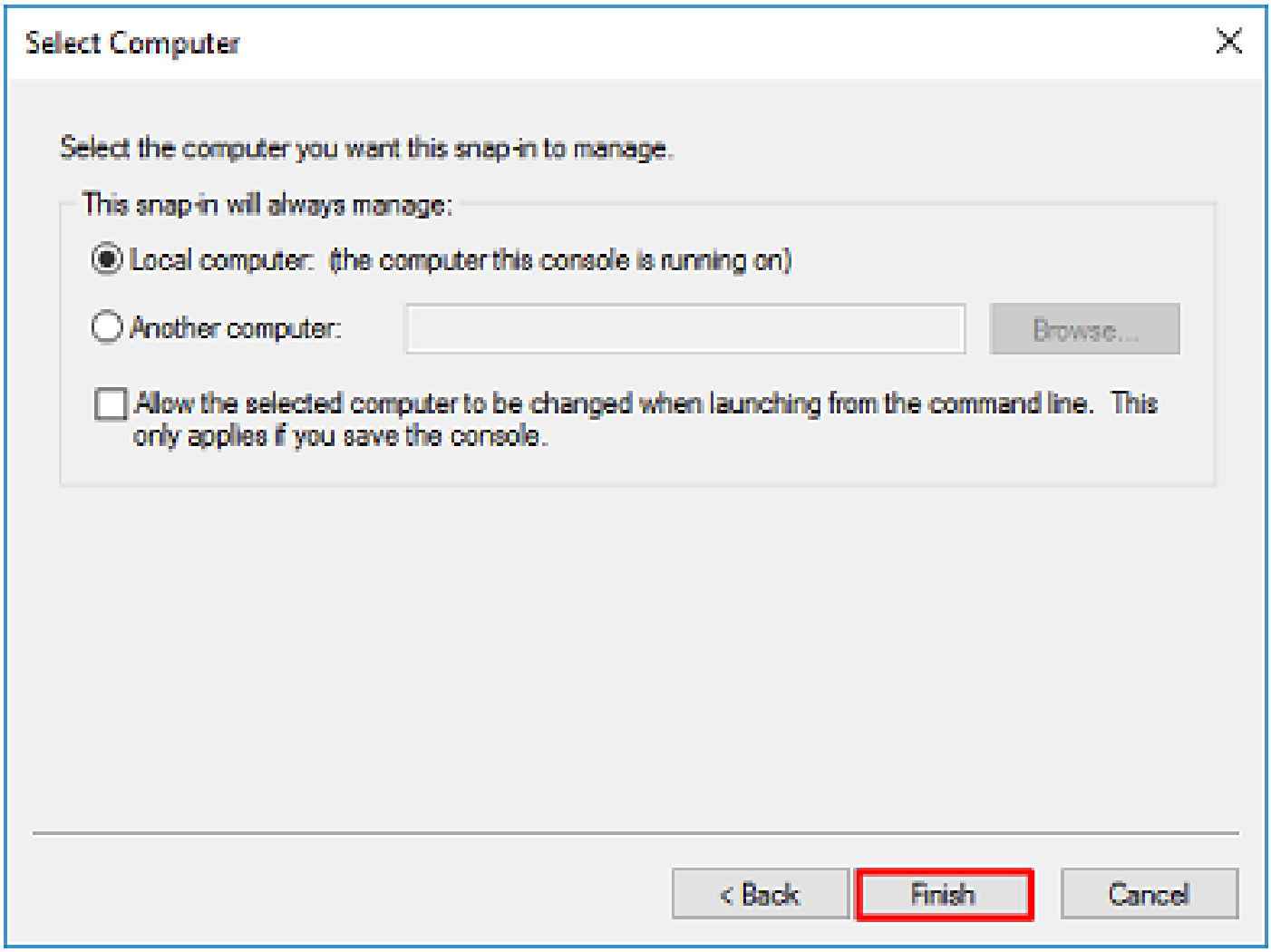
3. Kies onder beschikbare snap-ins Certificates en klik vervolgens op Add, zoals getoond in deze afbeelding:



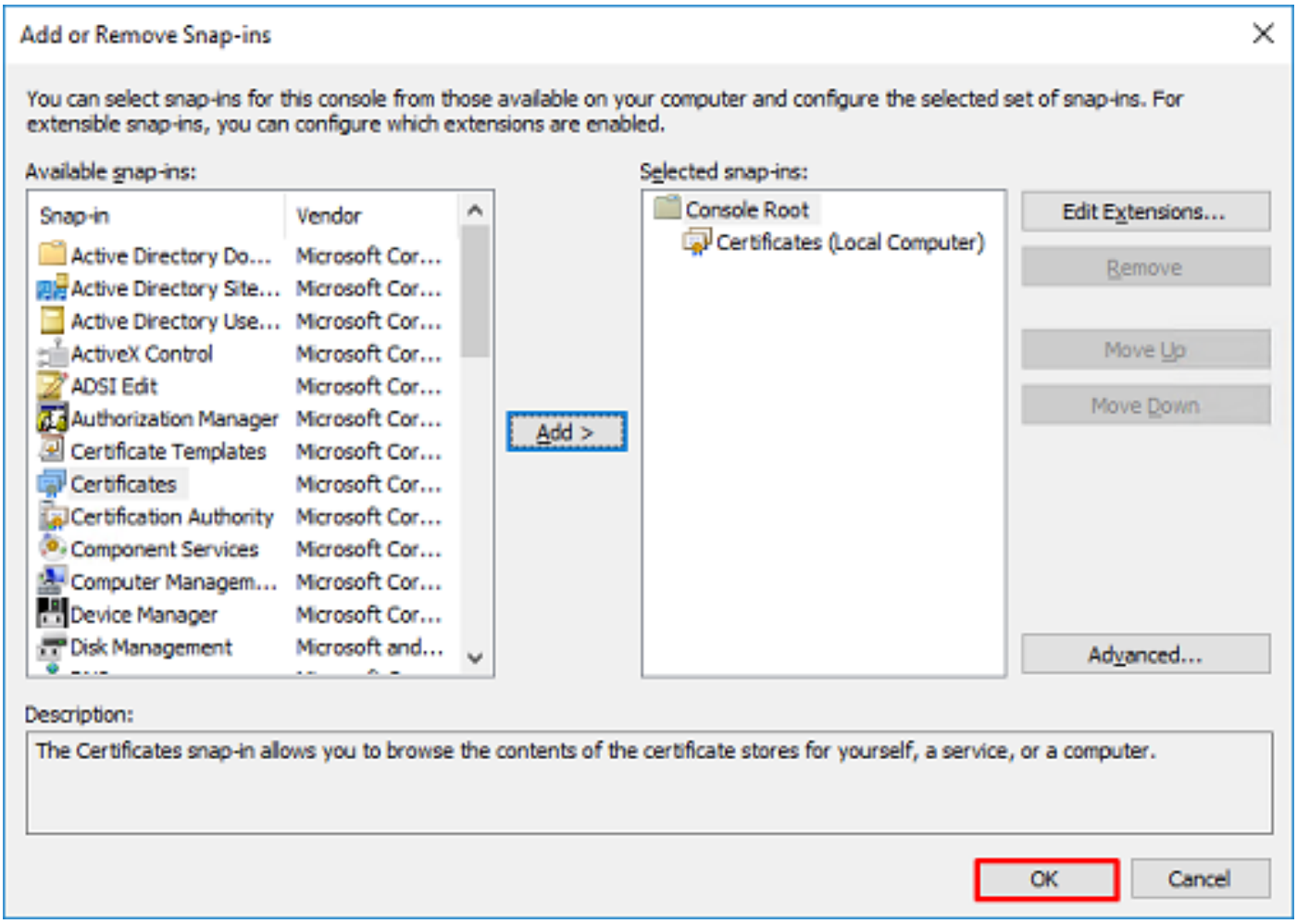
4. Kiezen Computer account en klik vervolgens op Next, zoals getoond in deze afbeelding:



Zoals hier getoond, klik Finish.



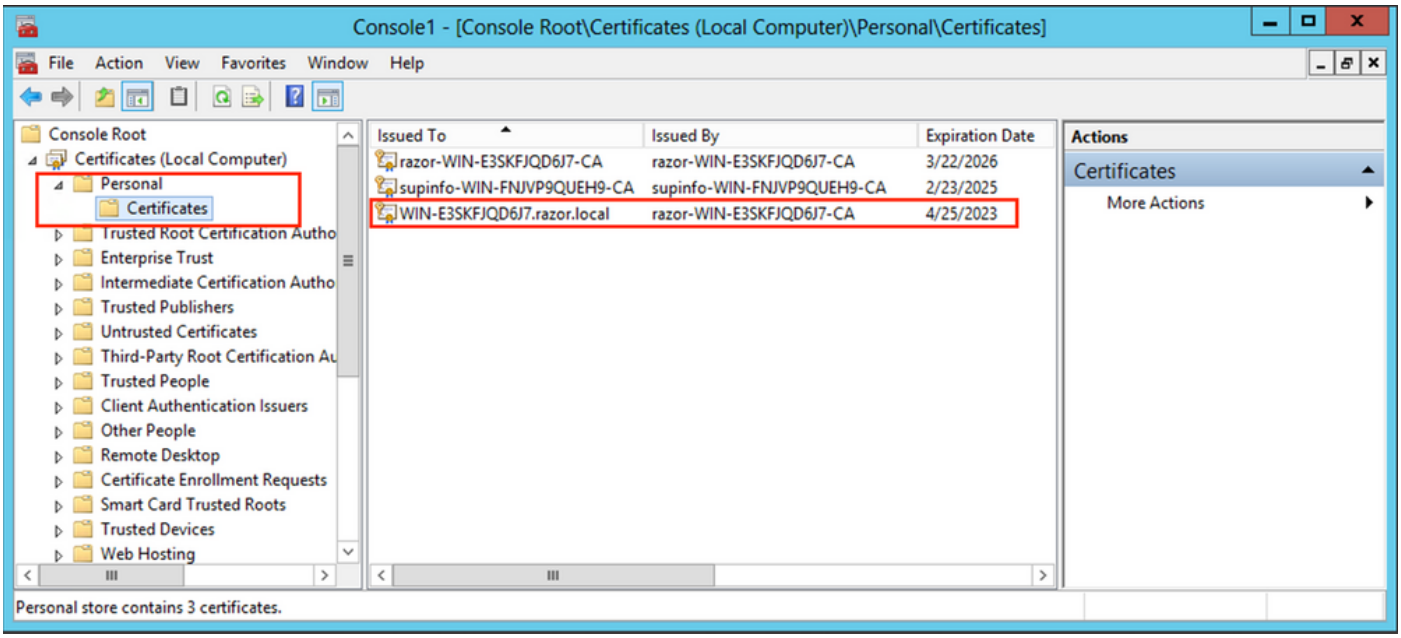
5. Klik nu op OK, zoals in deze afbeelding wordt getoond.



6. Breid de Personal map aan en klik vervolgens op Certificates. Het certificaat dat door LDAP's wordt gebruikt, moet worden afgegeven aan de FQDN (Fully Qualified Domain Name) van de Windows-server. Op deze server staan drie certificaten vermeld:

- Er is een CA-certificaat afgegeven aan en door razor-WIN-E3SKFJQD6J7-CA.
- Een CA-certificaat afgegeven aan en door supinfo-WIN-FNJVP9QUEH9-CA.
- Er is een identiteitsbewijs afgegeven aan WIN-E3SKFJQD6J7.razor.local door razor-WIN-E3SKFJQD6J7-CA.

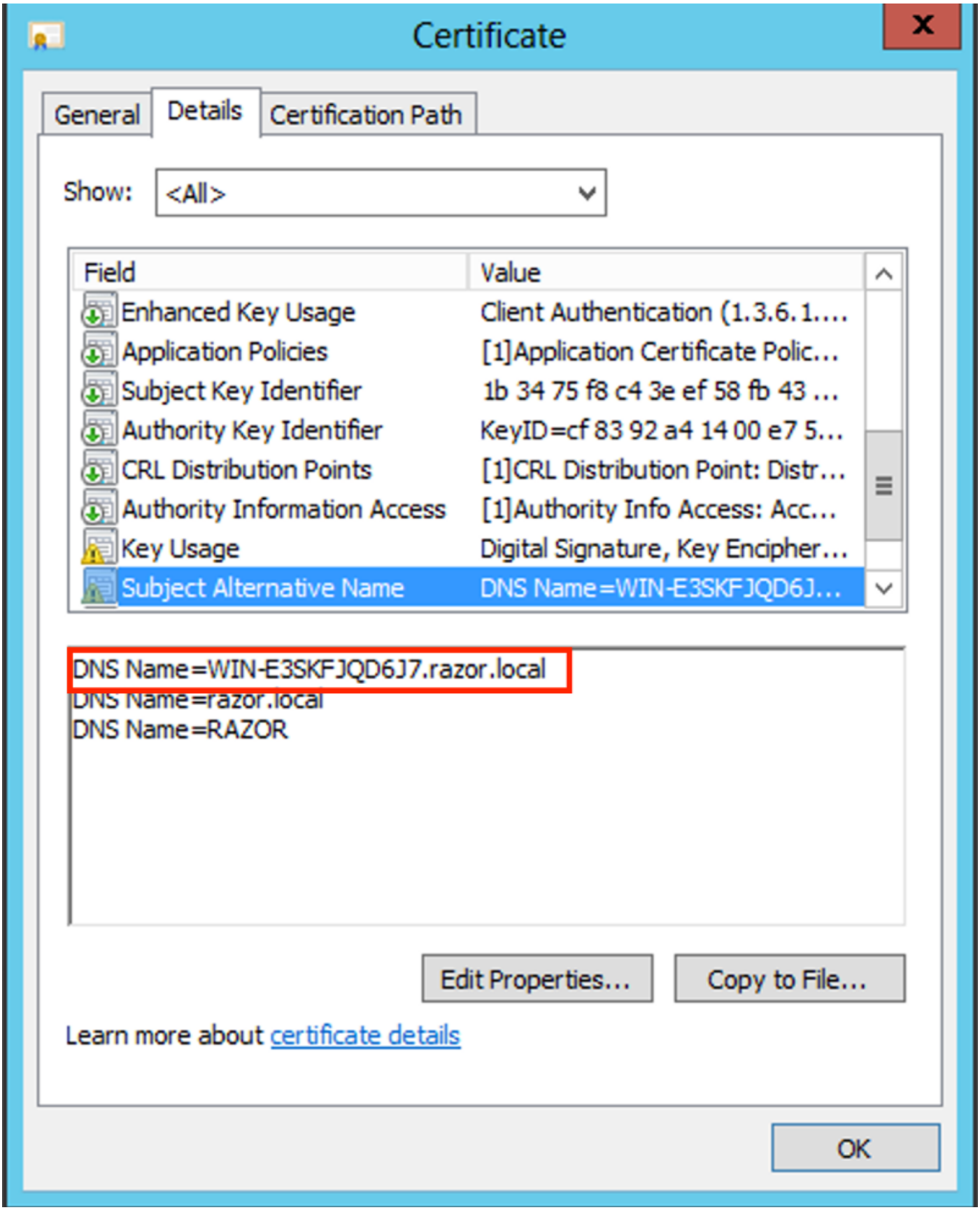
In deze configuratiehandleiding is de FQDN WIN-E3SKFJQD6J7.razor.local en dus zijn de eerste twee certificaten niet geldig voor gebruik als het LDAPs SSL certificaat. Het aan WIN-E3SKFJQD6J7.razor.local is een certificaat dat automatisch is afgegeven door de Windows Server CA-service. Dubbelklik op het certificaat om de gegevens te controleren.



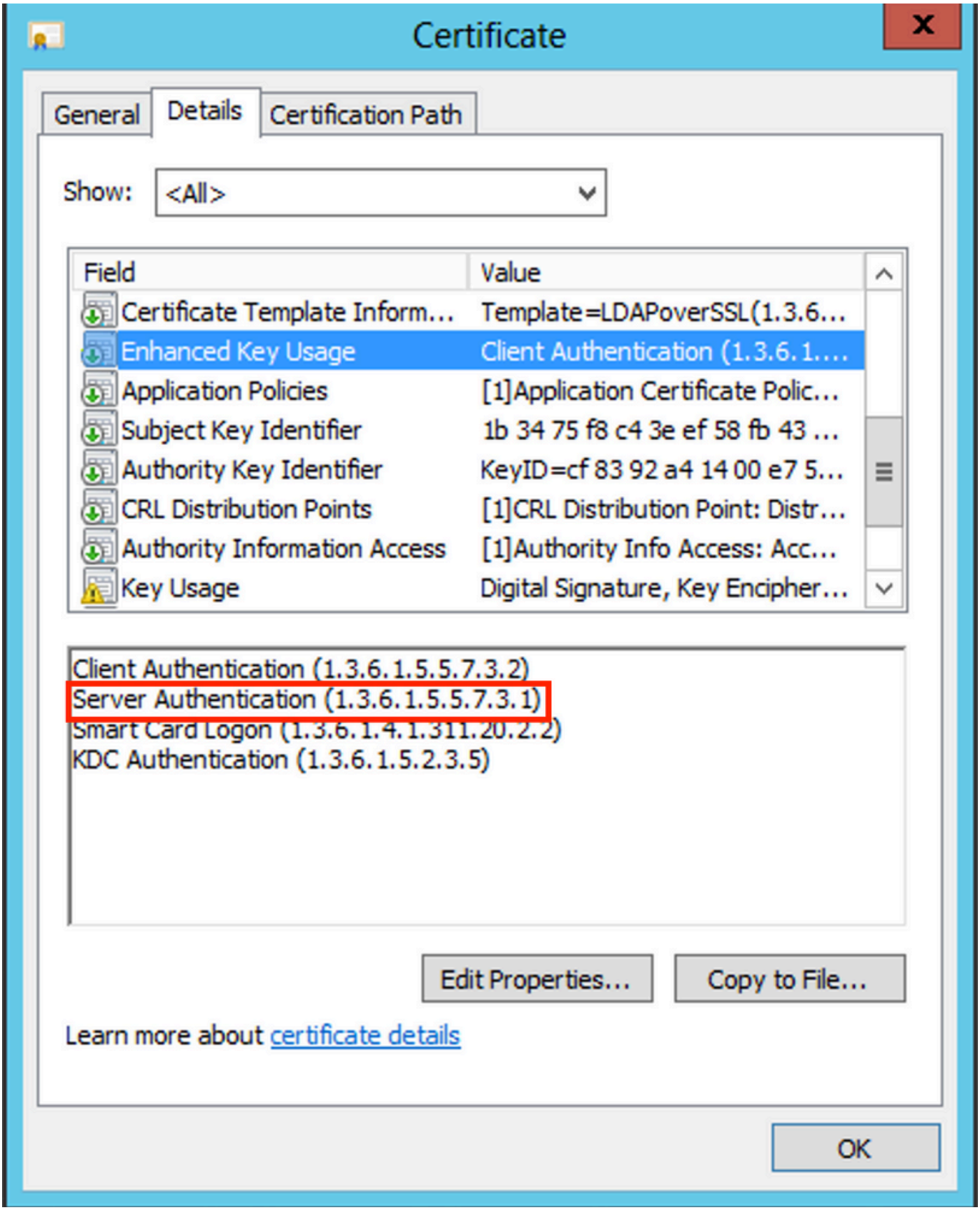
7. Om als het LDAPs SSL-certificaat te worden gebruikt, moet het certificaat aan de volgende vereisten voldoen:

- De algemene naam of DNS-onderwerpalternatieve naam komt overeen met de FQDN van de Windows-server.
- Het certificaat heeft serververificatie in het veld Uitgebreid sleutelgebruik.

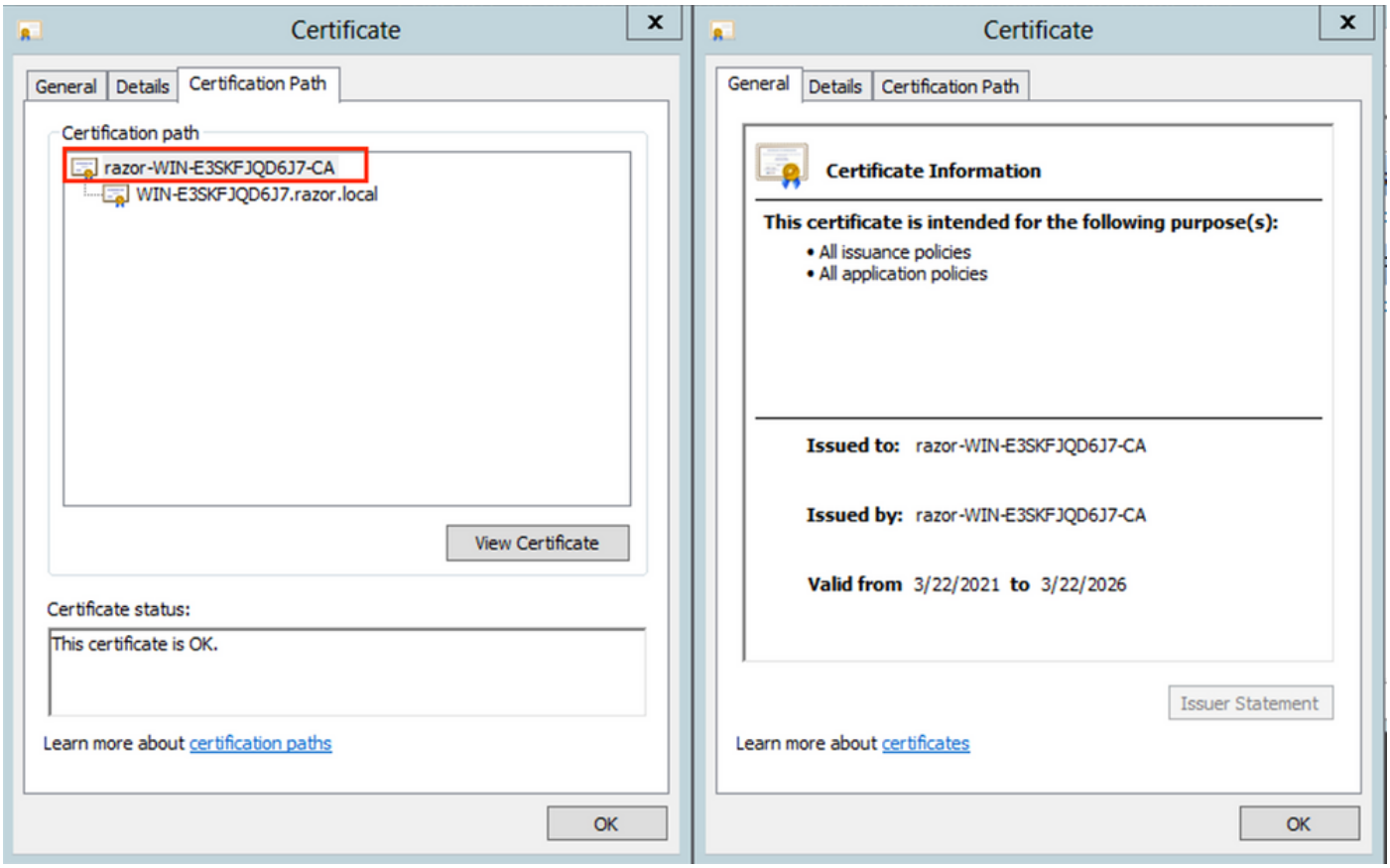
In het Details tabblad voor het certificaat, kies Subject Alternative Name, waarbij de FQDN WIN-E3SKFJQD6J7.razor.local aanwezig is.



Onder Enhanced Key Usage, Server Authentication aanwezig is.

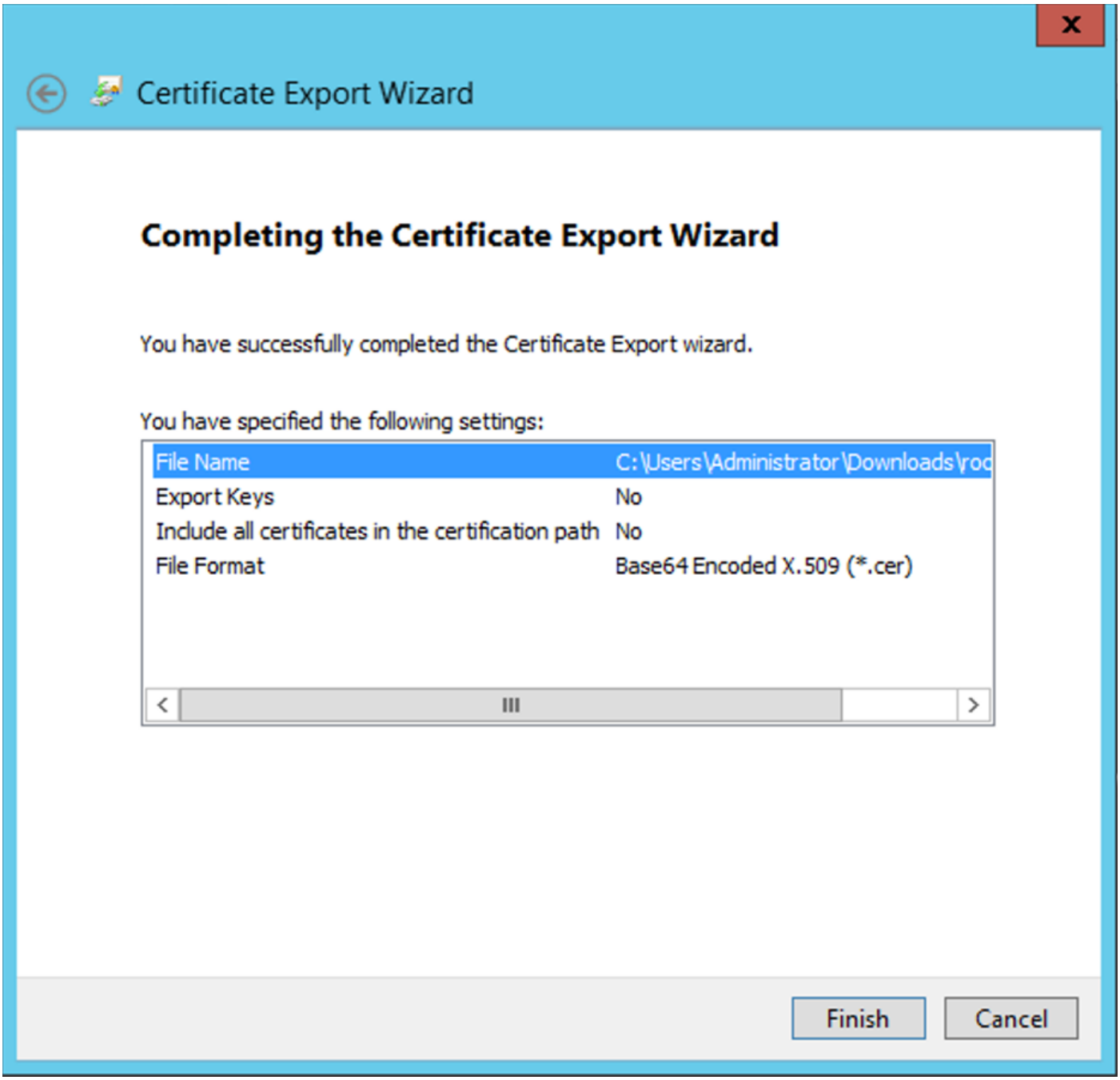


8. Zodra dit is bevestigd, wordt onder de Certification Path tabblad kiest u het certificaat op het hoogste niveau dat het basiscertificaat van CA is, en klikt u vervolgens op View Certificate. Hierdoor worden de certificaatgegevens voor het basiscertificaat van de CA geopend, zoals in de afbeelding wordt getoond:



9. In het Details tabblad van het basiscertificaat van CA, klikt u op Copy to File en navigeer door deCertificate Export Wizard die de root-CA in PEM-formaat exporteert.

Kiezen Base-64 encoded X.509 als bestandsindeling.



10. Open het Root CA-certificaat dat is opgeslagen op de geselecteerde locatie op de machine met een blocnote of een andere teksteditor.

Dit is het certificaat in PEM-indeling. Bewaar dit voor later.

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgo
vcjEhMB8GA1UEAxMYcmF6b3ItV0lOLUUzU0tGSlFENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCg
BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvc
CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnblxwtXOB2G4UxZ3LRrWznjXaSO2Rc3qVw4lnOAziGs4ZMNM1X8UWeKuwi8
9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU3OaiiI/tp422ydy3Kgl7Iqt1s4XqpZmTezykWra7dUyXfkuESk6lEOAV
CSkTQTRXYryy8dJrWjAF/n6A3VnS/l7Uhujlx4CD2OBkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwE
DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFM+DkqQUAOdY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSI
AA4IBAQCiSm5U7U6Y7zXdx+dleJdOQmGgKayAAuYAD+MWNwC4NzFD8Yr7BnO6f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q
4sMZffbVrGlRz7twWY36J5G5vhNUhzZ1N2OLw6wtHg2SO8XlvpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nrylb
GuDsepY7/u2uWfy/vpTJigeok2DH6HFfOET3sE+7rsIAY+ofOkWW5gNwQ4hOwv4Goqj+YQRAXXi2OZyltHR1dfUUbwVENSFQtDnFA7X
```

```
-----END CERTIFICATE-----
```

In het geval van meerdere certificaten die zijn geïnstalleerd in de lokale machineopslag op de LDAP-server (optioneel)

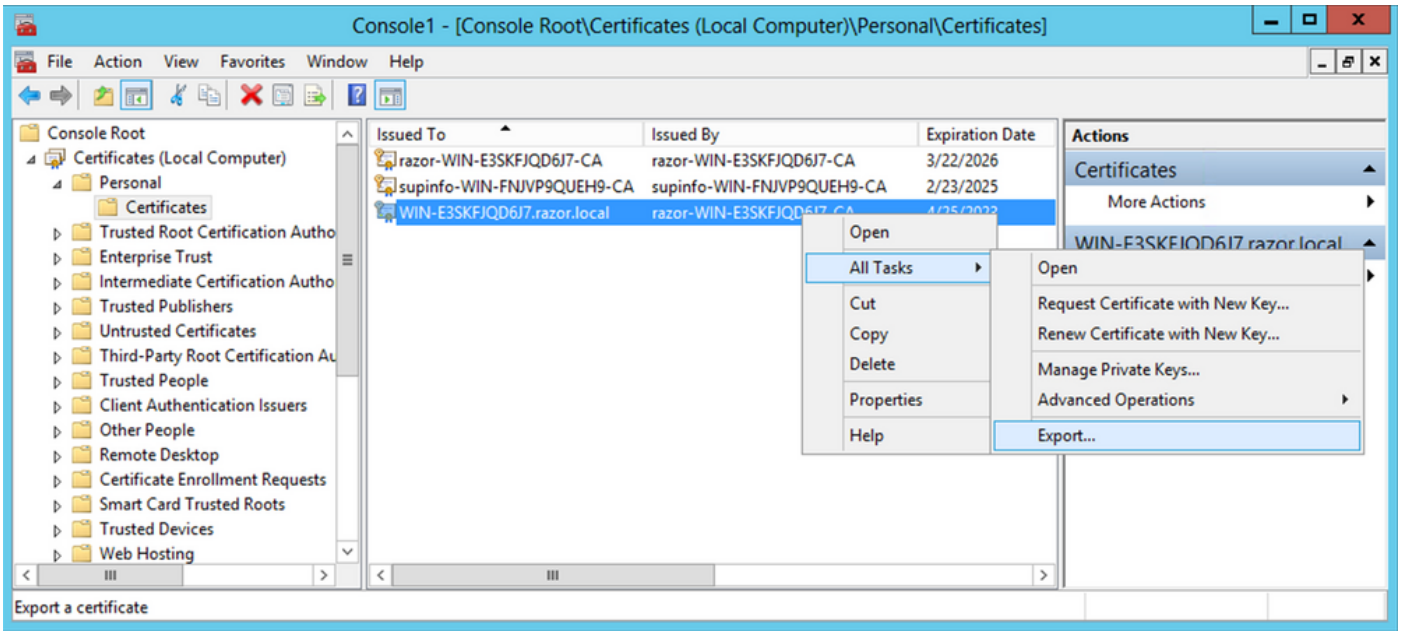
1. In een situatie waarin meerdere identiteitscertificaten door LDAPS kunnen worden gebruikt en er onzekerheid is over de vraag welke certificaten worden gebruikt of wanneer er geen toegang tot de LDAPS-server is, is het nog steeds mogelijk de wortel CA uit een pakketopname op de FTD te halen.

2. Wanneer u meerdere certificaten hebt die geldig zijn voor serververificatie in de lokale computercertificaatopslag van de LDAP-server (zoals AD DS-domeincontroller), kan worden opgemerkt dat een ander certificaat wordt gebruikt voor LDAPS-communicatie. De beste oplossing voor een dergelijk probleem is om alle overbodige certificaten uit het lokale computercertificaatarchief te verwijderen en slechts één certificaat te hebben dat geldig is voor serververificatie.

Als er echter een legitieme reden is dat u twee of meer certificaten vereist en ten minste een Windows Server 2008 LDAP-server hebt, kan de Active Directory Domain Services (NTDS\Personal) certificaatopslag worden gebruikt voor LDAP-communicatie.

Deze stappen tonen aan hoe u een LDAPS-enabled certificaat kunt exporteren van een domeincontroller lokale computer certificaatopslag naar de Active Directory Domain Services servicecertificaatopslag (NTDS\Personal).

- Navigeer naar de MMC-console op de Active Directory Server, kies Bestand en klik vervolgens op Add/Remove Snap-in.
- Klik op de knop Certificates en klik vervolgens op Add.
- In het Certificates snap-in, kiezen Computer account en klik vervolgens op Next.
- In Select Computer, kiezen Local Computer,klik op de knop OKen klik vervolgens op Finish. In Add or Remove Snap-ins,klik op de knop OK.
- Klik met de rechtermuisknop op de certificaatconsole van een computer met een certificaat dat wordt gebruikt voor de serververificatie. certificate,klik op de knop All Tasksen klik vervolgens op Export.

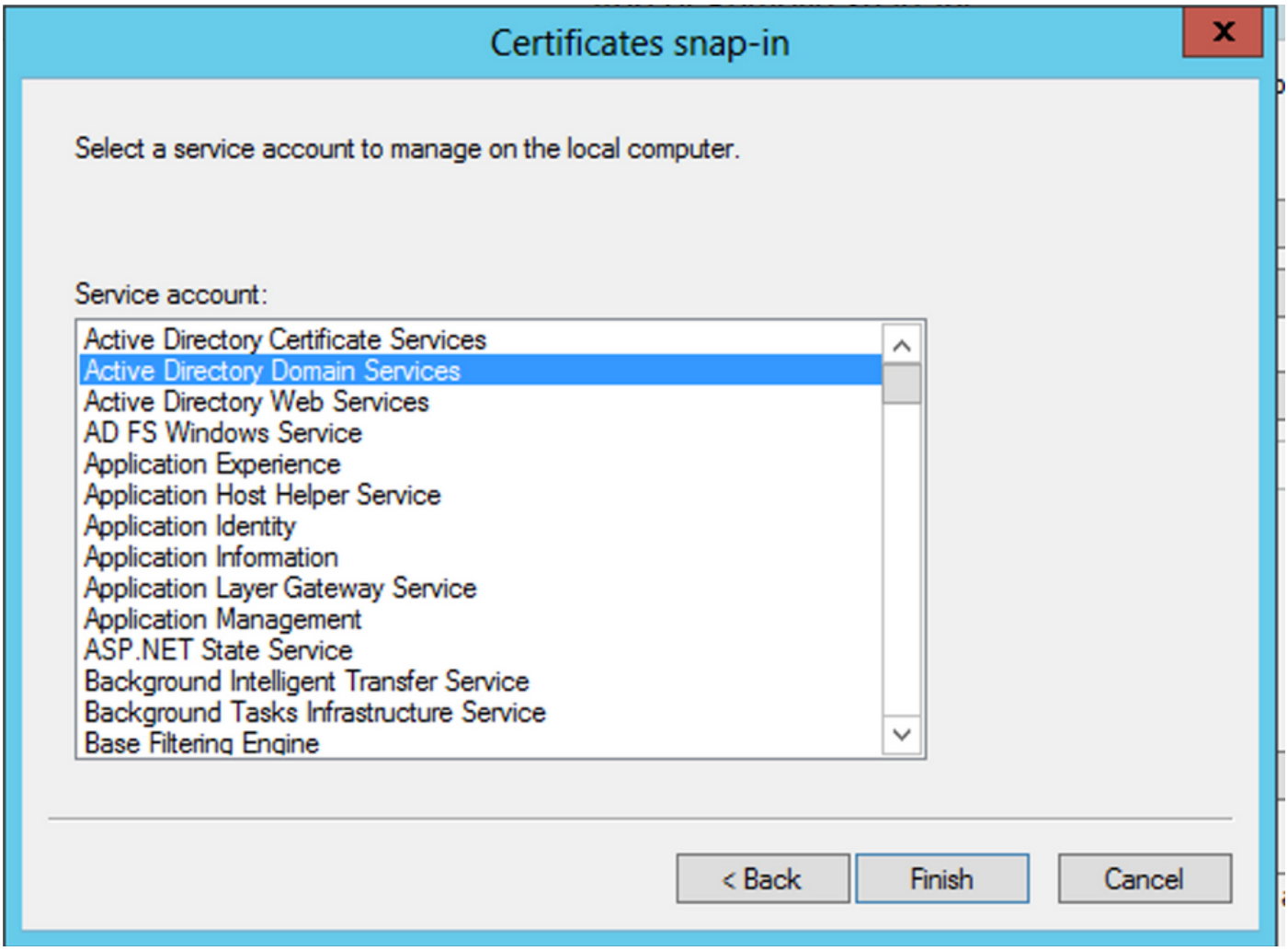


- Exporteer het certificaat in de pfx in de volgende delen. Verwijs naar dit artikel over hoe een certificaat uit te voeren in de pfx formaat vanaf MMC:

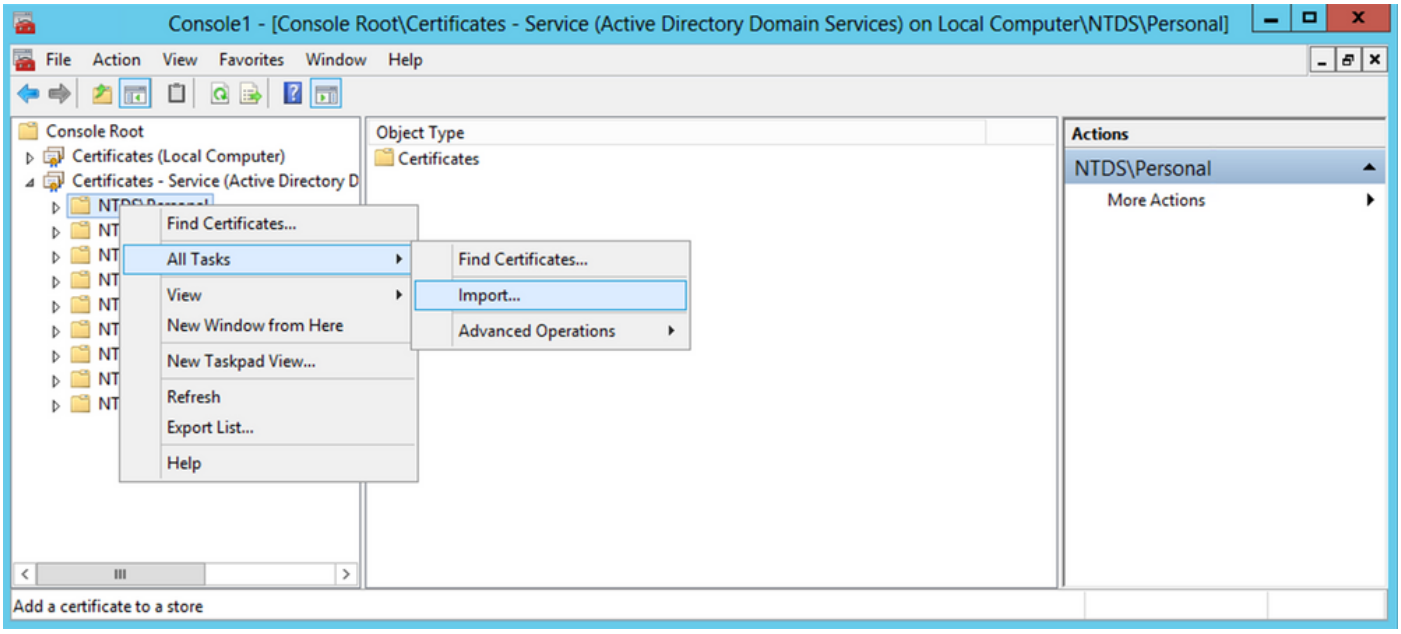
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html.

- Nadat het certificaat is geëxporteerd, navigeert u naar Add/Remove Snap-in on MMC console. Klik op de knop Certificates en klik vervolgens op Add.
- Kiezen Service account en klik vervolgens op Next.

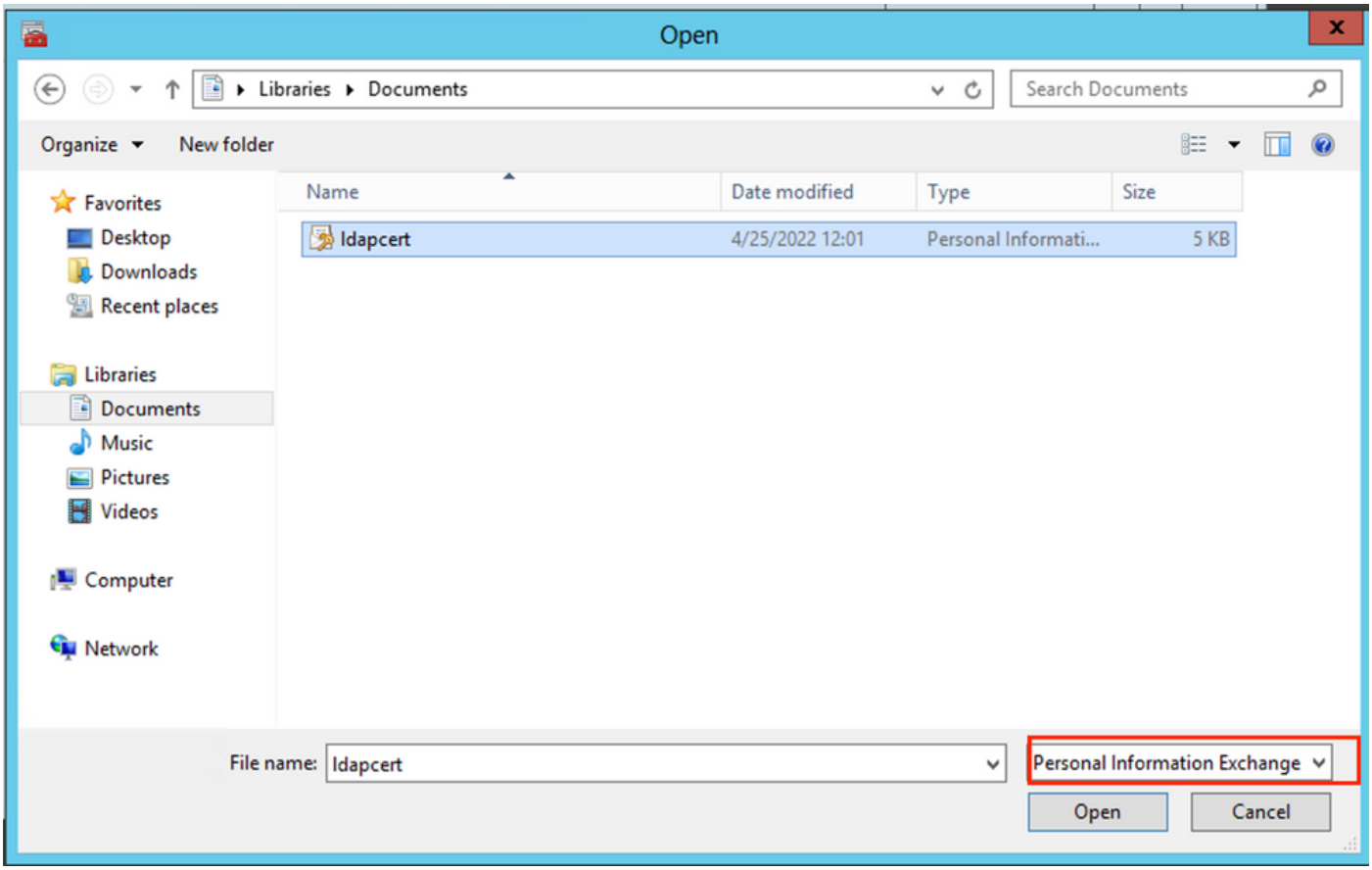
- In het Select Computer dialoogvenster kiest u Local Computer en klik op Next.
- Kiezen Active Directory Domain Services en klik vervolgens op Finish.



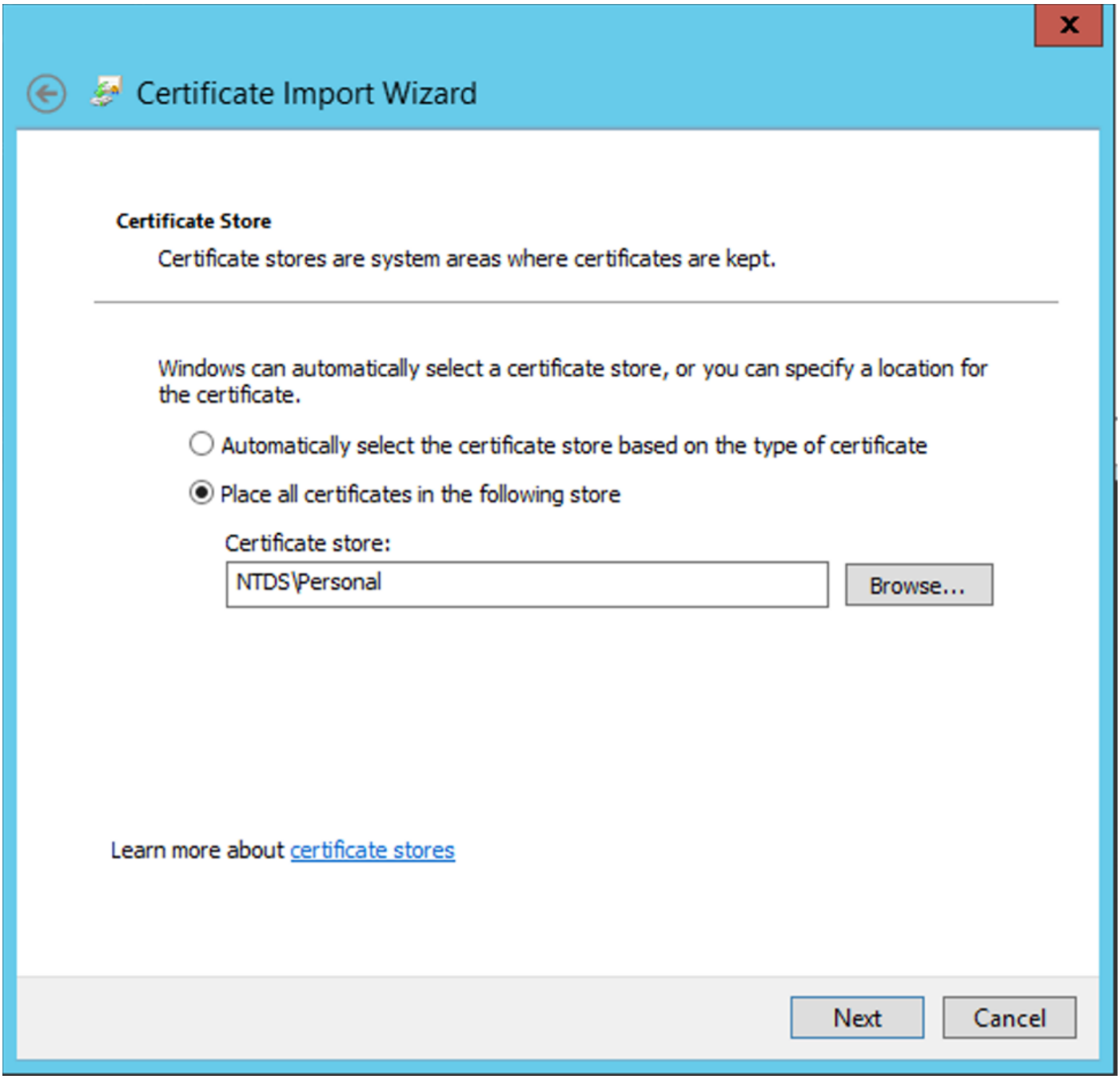
- Op de Add/Remove Snap-ins dialoogvenster klikt u op OK.
- Uitbreiden Certificates - Services (Active Directory Domain Services) en klik vervolgens op NTDS\Personal.
- Rechtsklik NTDS\Personal,klik op de knop All Tasksen klik vervolgens op Import.



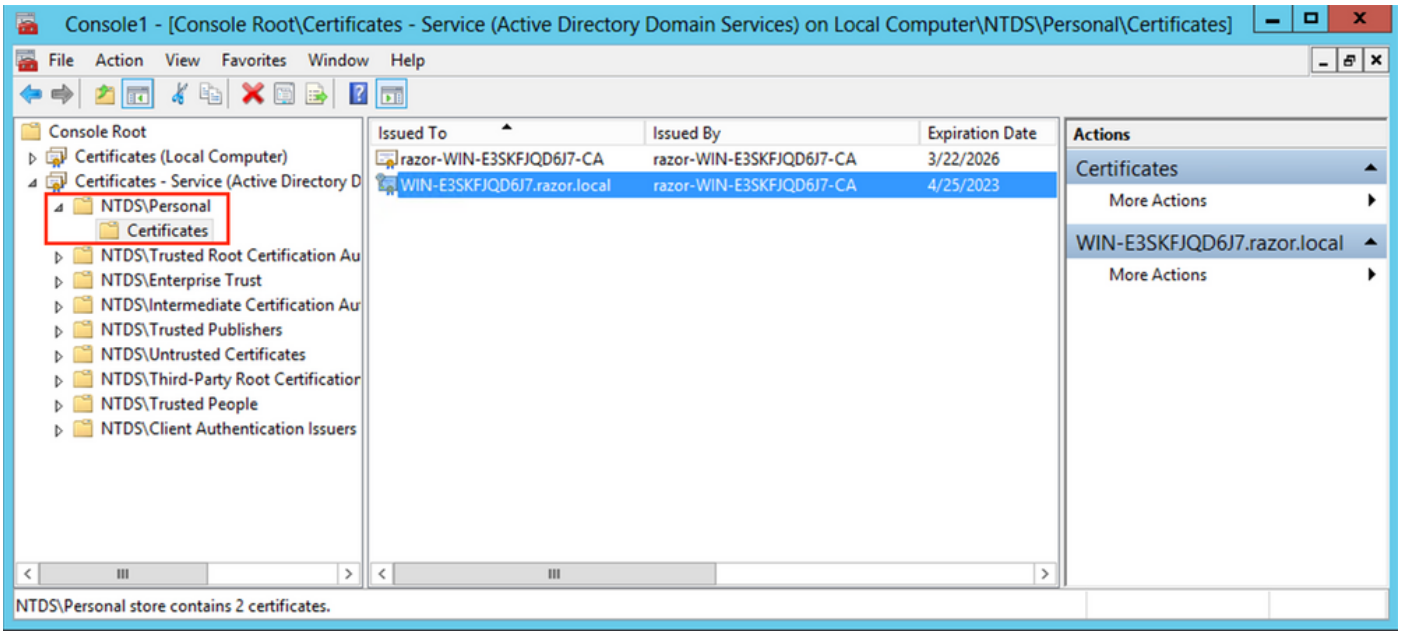
- Op de Certificate Import Wizard welkomstscherm, klik op Next.
- Klik in het scherm Bestand om te importeren op Browse, en lokaliseer het certificaatbestand dat u eerder hebt geëxporteerd.
- Zorg er in het Open scherm voor dat de uitwisseling van persoonlijke informatie (*pfx,*.p12) is geselecteerd als het bestandstype en navigeer vervolgens in het bestandssysteem om het eerder geëxporteerde certificaat te vinden. Klik vervolgens op dat certificaat.



- Klik op de knop Open en klik vervolgens op Next.
- Voer in het wachtwoordscherm het wachtwoord in dat u voor het bestand hebt ingesteld en klik vervolgens op Next.
- Zorg er op de pagina Certificaatopslag voor dat Alle certificaten plaatsen zijn geselecteerd en lees Certificaatopslag: NTDS\Personal en klik vervolgens op Next.



- Op de Certificate Import Wizard scherm voltooien, klikt u op Finish. U ziet dan een bericht dat de import succesvol was. Klik op de knop OK. Het certificaat is ingevoerd in het certificaatarchief: NTDS\Personal.



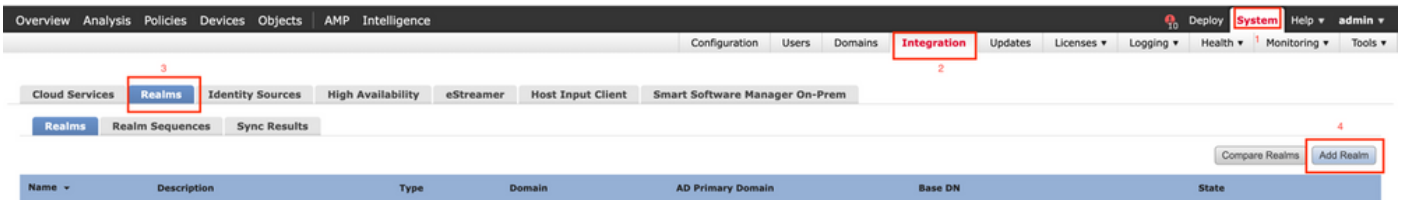
FMC-configuraties

Licentie controleren

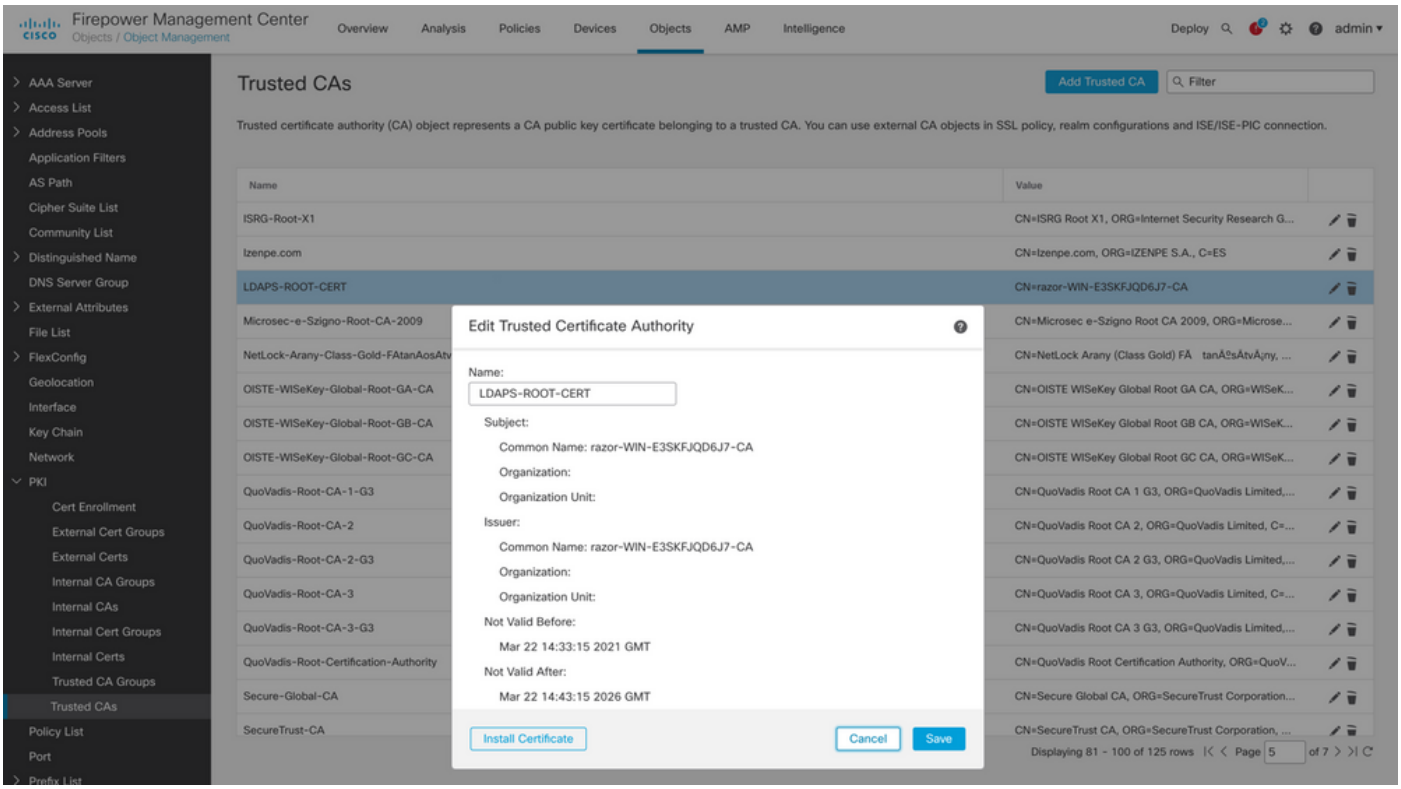
Om de AnyConnect-configuratie te kunnen implementeren, moet de FTD worden geregistreerd bij de slimme licentieserver en moet een geldige Plus-, Apex- of VPN-licentie alleen op het apparaat worden toegepast.

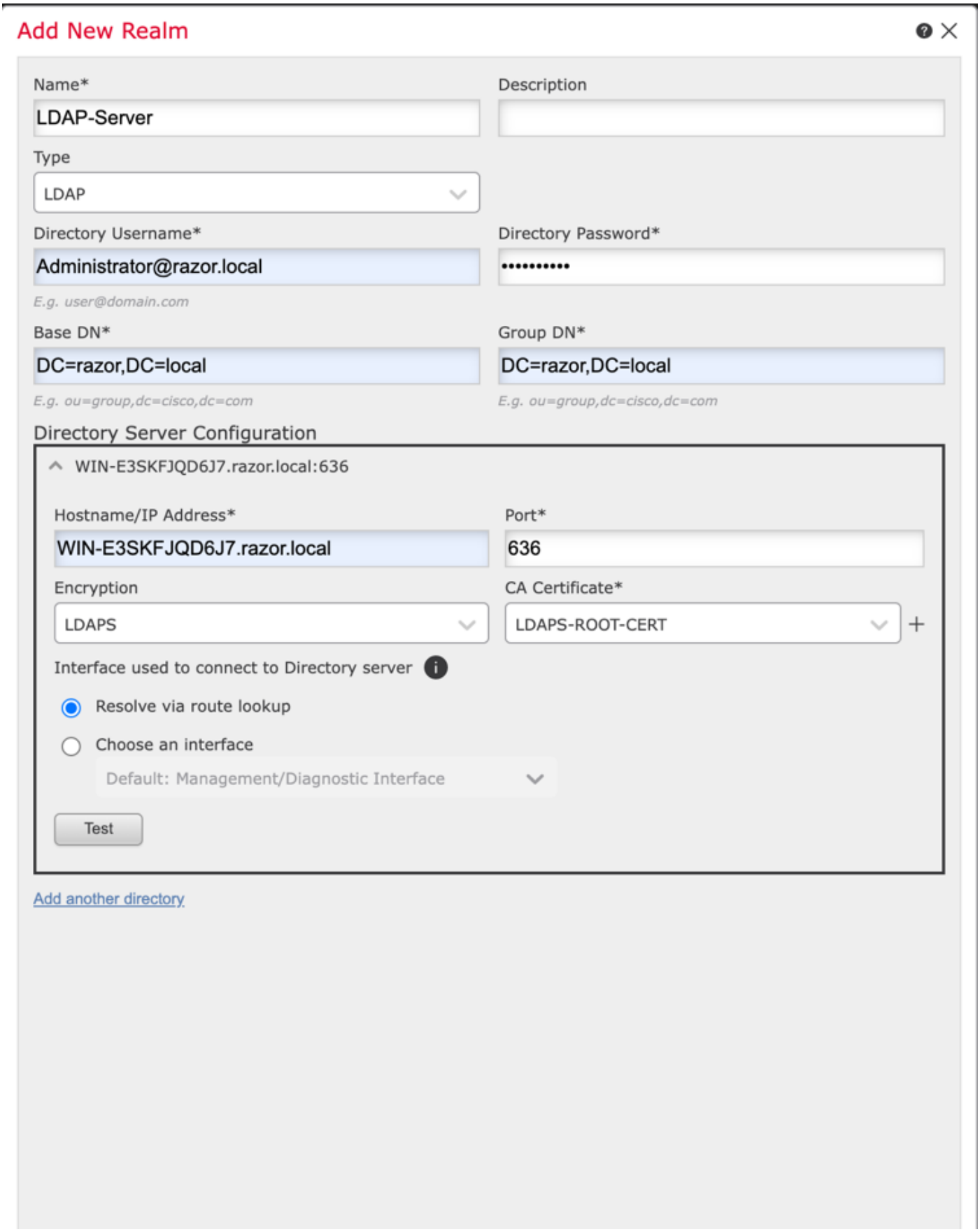
Instellingsgebied

1. Naar navigeren System > Integration. Naar navigeren Realmsklikt u vervolgens op Add Realm, zoals getoond in deze afbeelding:



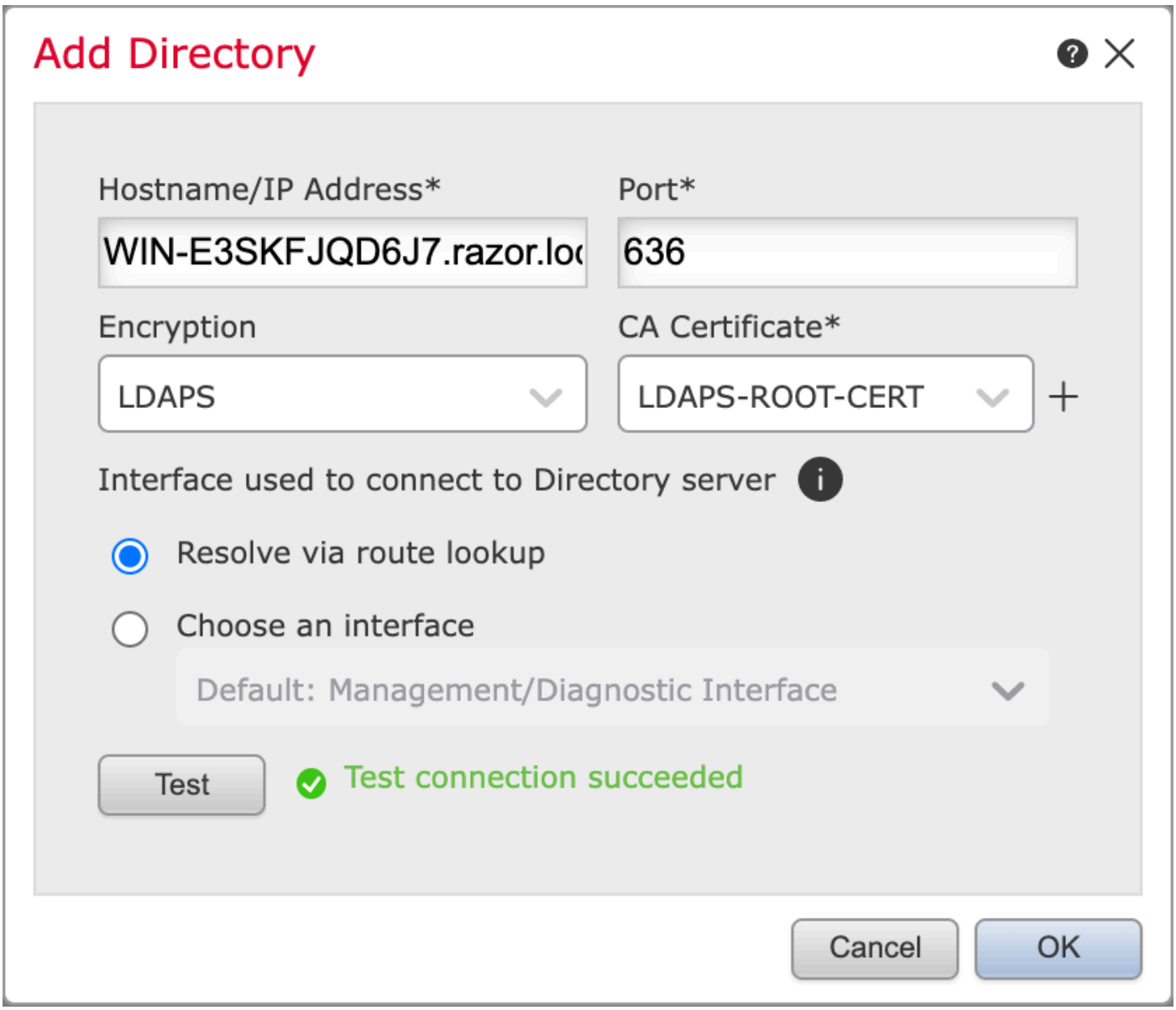
2. Vul de weergegeven velden in op basis van de informatie die bij de Microsoft-server voor LDAP's is verzameld. Hiervoor moet u het Root CA-certificaat importeren dat het LDAP-servicecertificaat op de Windows-server heeft ondertekend onder Objects > PKI > Trusted CAs > Add Trusted CA, aangezien dit in het kader van deDirectory Server Configuration van het rijk. Klik op de knop OK.


Firepower Management Center
Objects / Object Management
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Deploy
admin
AAA Server
Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Cert Enrollment
External Cert Groups
External Certs
Internal CA Groups
Internal CAs
Internal Cert Groups
Internal Certs
Trusted CA Groups
Trusted CAs
Policy List
Port
Trusted CAs
Add Trusted CA
Filter
Trusted certificate authority (CA) object represents a CA public key certificate belonging to a trusted CA. You can use external CA objects in SSL policy, realm configurations and ISE/ISE-PIC connection.
Name
Value
ISRG-Root-X1
CN=ISRG Root X1, ORG=Internet Security Research G...
Izenpe.com
CN=Izenpe.com, ORG=IZENPE S.A., C=ES
LDAPS-ROOT-CERT
CN=razor-WIN-E3SKFJQD6J7-CA
Microsec-e-Szigno-Root-CA-2009
CN=Microsec e-Szigno Root CA 2009, ORG=Microse...
NetLock-Arany-Class-Gold-FAtanAosAtv
CN=NetLock Arany (Class Gold) FÁ tanÚsÁtvÁny, ...
OISTE-WISeKey-Global-Root-GA-CA
CN=OISTE WISeKey Global Root GA CA, ORG=WISeK...
OISTE-WISeKey-Global-Root-GB-CA
CN=OISTE WISeKey Global Root GB CA, ORG=WISeK...
OISTE-WISeKey-Global-Root-GC-CA
CN=OISTE WISeKey Global Root GC CA, ORG=WISeK...
QuoVadis-Root-CA-1-G3
CN=QuoVadis Root CA 1 G3, ORG=QuoVadis Limited,...
QuoVadis-Root-CA-2
CN=QuoVadis Root CA 2, ORG=QuoVadis Limited, C=...
QuoVadis-Root-CA-2-G3
CN=QuoVadis Root CA 2 G3, ORG=QuoVadis Limited,...
QuoVadis-Root-CA-3
CN=QuoVadis Root CA 3, ORG=QuoVadis Limited, C=...
QuoVadis-Root-CA-3-G3
CN=QuoVadis Root CA 3 G3, ORG=QuoVadis Limited,...
QuoVadis-Root-Certification-Authority
CN=QuoVadis Root Certification Authority, ORG=QuoV...
Secure-Global-CA
CN=Secure Global CA, ORG=SecureTrust Corporation...
SecureTrust-CA
CN=SecureTrust CA, ORG=SecureTrust Corporation, ...
Displaying 81 - 100 of 125 rows
Page 5 of 7
Edit Trusted Certificate Authority
Name:
LDAPS-ROOT-CERT
Subject:
Common Name: razor-WIN-E3SKFJQD6J7-CA
Organization:
Organization Unit:
Issuer:
Common Name: razor-WIN-E3SKFJQD6J7-CA
Organization:
Organization Unit:
Not Valid Before:
Mar 22 14:33:15 2021 GMT
Not Valid After:
Mar 22 14:43:15 2026 GMT
Install Certificate
Cancel
Save

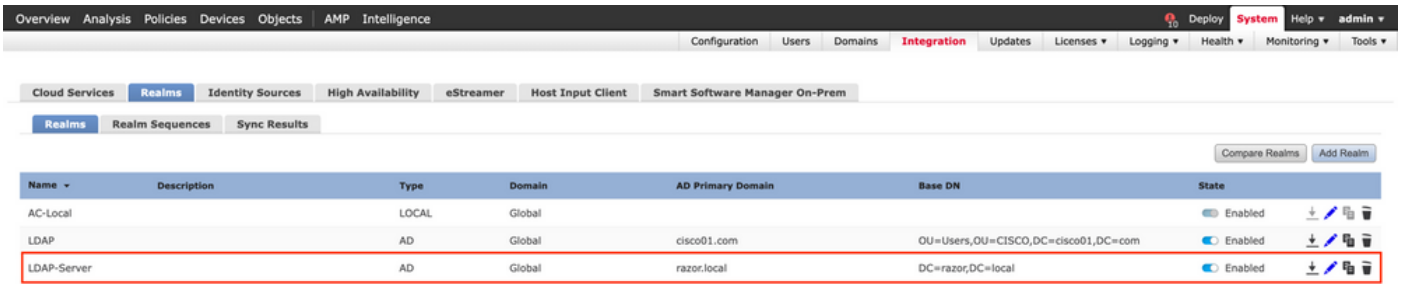


3. Klik op de knop Test om ervoor te zorgen dat het VCC met succes kan verbinden met de Directory Gebruikersnaam en het wachtwoord dat in de eerdere stap is opgegeven. Aangezien deze tests worden geïnitieerd vanuit het FMC en niet via een van de routeerbare interfaces die op de FTD zijn geconfigureerd (zoals binnenkant, buitenkant, dmz),

garandeert een succesvolle (of mislukte) verbinding niet hetzelfde resultaat voor AnyConnect-verificatie, aangezien AnyConnect LDAP-verificatieverzoeken worden geïnitieerd vanuit een van de FTD routable interfaces.



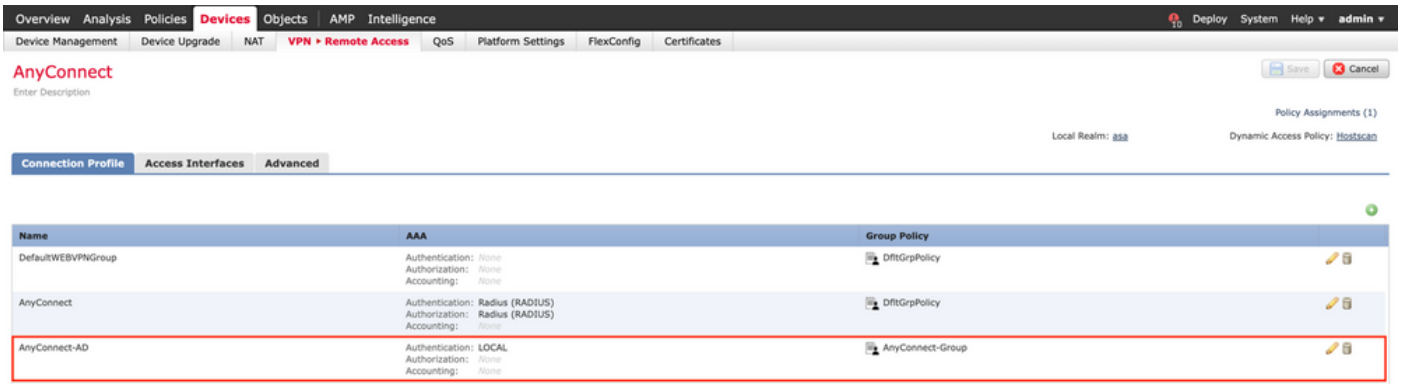
4. Schakel het nieuwe domein in.



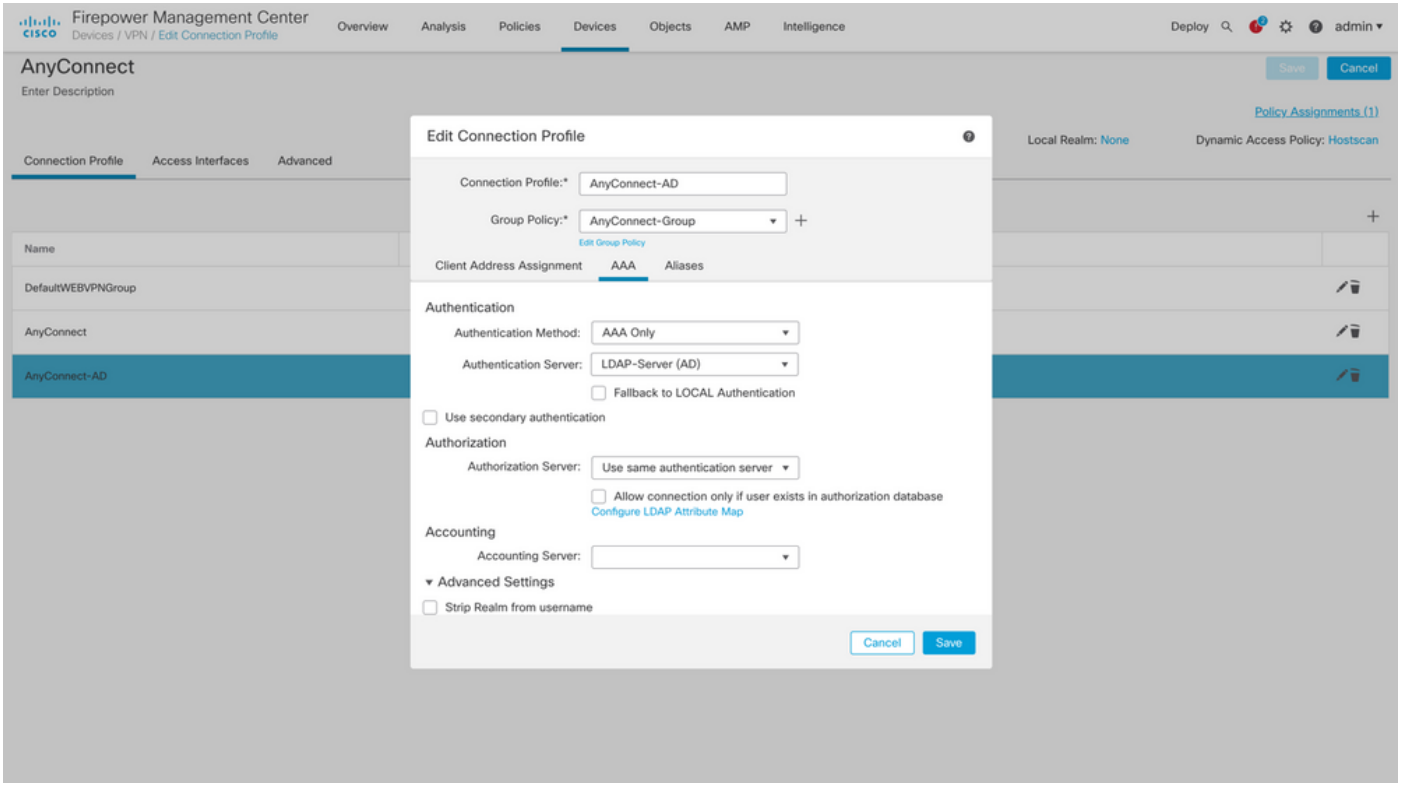
AnyConnect configureren voor wachtwoordbeheer

1. Kies het bestaande verbindingsprofiel of maak een nieuw profiel aan als AnyConnect voor het eerst is ingesteld. Hier wordt een bestaand verbindingsprofiel met de naam 'AnyConnect-

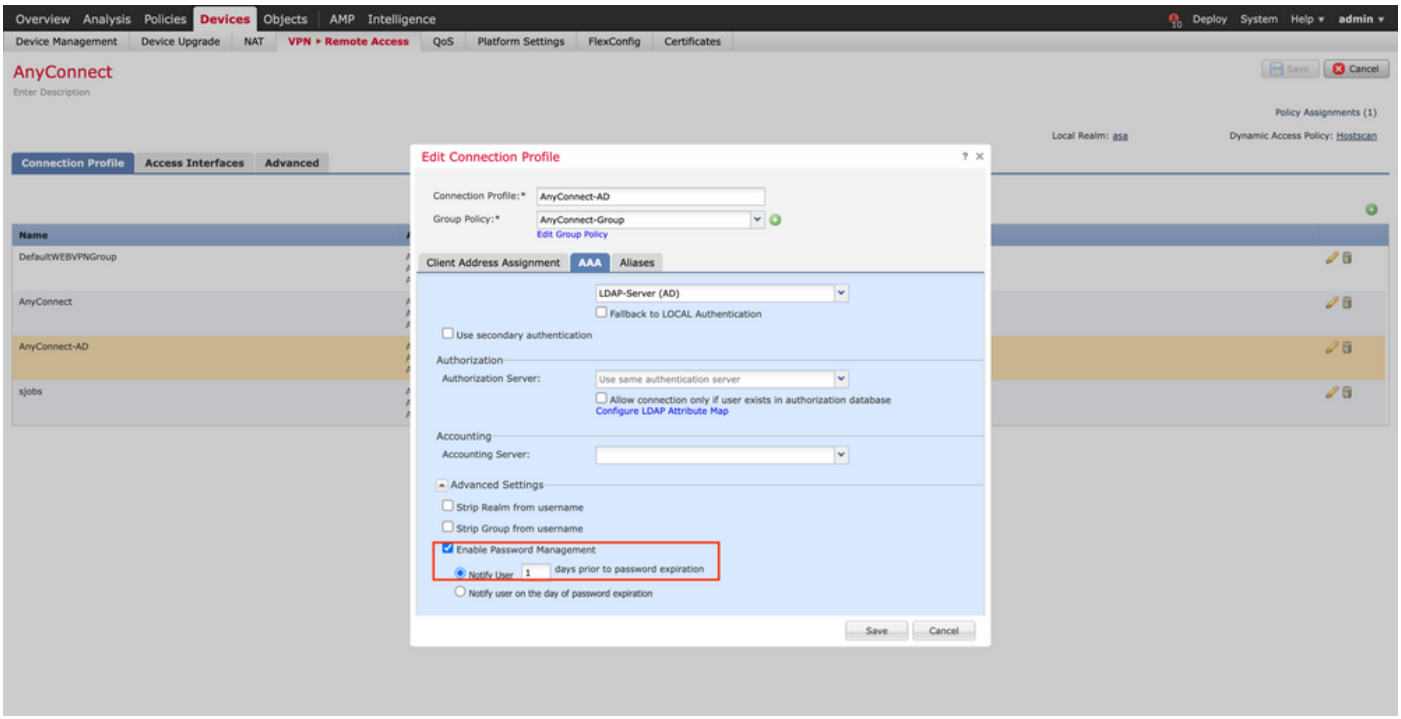
AD' gebruikt dat is toegewezen aan de lokale verificatie.



2. Bewerk het verbindingsprofiel en wijs de nieuwe LDAPs-server toe die in de eerdere stappen is geconfigureerd, onder de AAA-instellingen van het verbindingsprofiel. Klik op de knop Save in de rechterbovenhoek



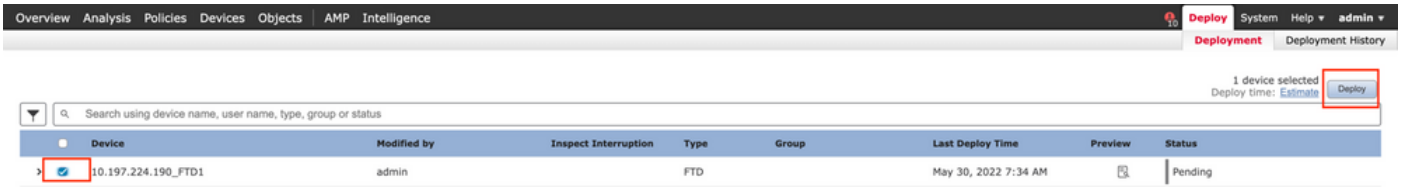
3. Wachtwoordbeheer inschakelen onder de AAA > Advanced Settings en slaat de configuratie op.



Implementeren

1. Als u klaar bent met de configuratie, klikt u op deDeploy knop aan de rechterbovenkant.

2. Klik op het selectievakje naast de FTD-configuratie die erop is toegepast en klik vervolgens op Deploy, zoals getoond in deze afbeelding:



Laatste configuratie

Dit is de configuratie in de FTD CLI na de succesvolle implementatie.

AAA-configuratie

<#root>

```
> show running-config aaa-server
```

```
aaa-server LDAP-Server protocol ldap
                                                    <------ aaa-server group configured for LDAPs
```

```
 max-failed-attempts 4
 realm-id 8
aaa-server LDAP-Server host WIN-E3SKFJQD6J7.razor.local
                          <-------- LDAPs Server to which the queries are sent

 server-port 636
 ldap-base-dn DC=razor,DC=local
 ldap-group-base-dn DC=razor,DC=local
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn *****@razor.local
 ldap-over-ssl enable
 server-type microsoft
```

Configuratie AnyConnect

<#root>

```
> show running-config webvpn

webvpn
 enable Outside
 anyconnect image disk0:/csm/anyconnect-win-4.10.01075-webdeploy-k9.pkg 1 regex "Windows"
 anyconnect profiles FTD-Client-Prof disk0:/csm/ftd.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  no disable
error-recovery disable
```

```
> show running-config tunnel-group

tunnel-group AnyConnect-AD type remote-access
tunnel-group AnyConnect-AD general-attributes
 address-pool Pool-1
authentication-server-group LDAP-Server                                    <-------- LDAPs Serve

 default-group-policy AnyConnect-Group
 password-management password-expire-in-days 1                          <-------- Password-management

tunnel-group AnyConnect-AD webvpn-attributes
 group-alias Dev enable


> show running-config group-policy AnyConnect-Group

group-policy
AnyConnect-Group
 internal
<--------- Group-Policy configuration that is mapped once the user is authenticated

group-policy AnyConnect-Group attributes
 vpn-simultaneous-logins 3
 vpn-idle-timeout 35791394
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
vpn-tunnel-protocol ikev2 ssl-client                                       <-------- Protocol

 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Remote-Access-Allow
```

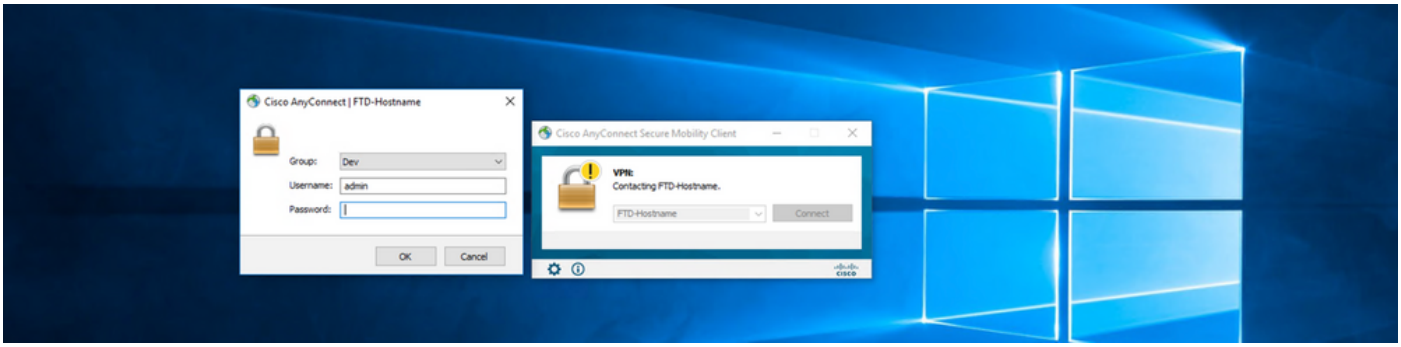
```
 default-domain none
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private none
  anyconnect ssl keepalive 20
  anyconnect ssl rekey time none
  anyconnect ssl rekey method none
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression none
  anyconnect modules value none
  anyconnect profiles value FTD-Client-Prof type user
  anyconnect ask none default anyconnect
  anyconnect ssl df-bit-ignore disable
```

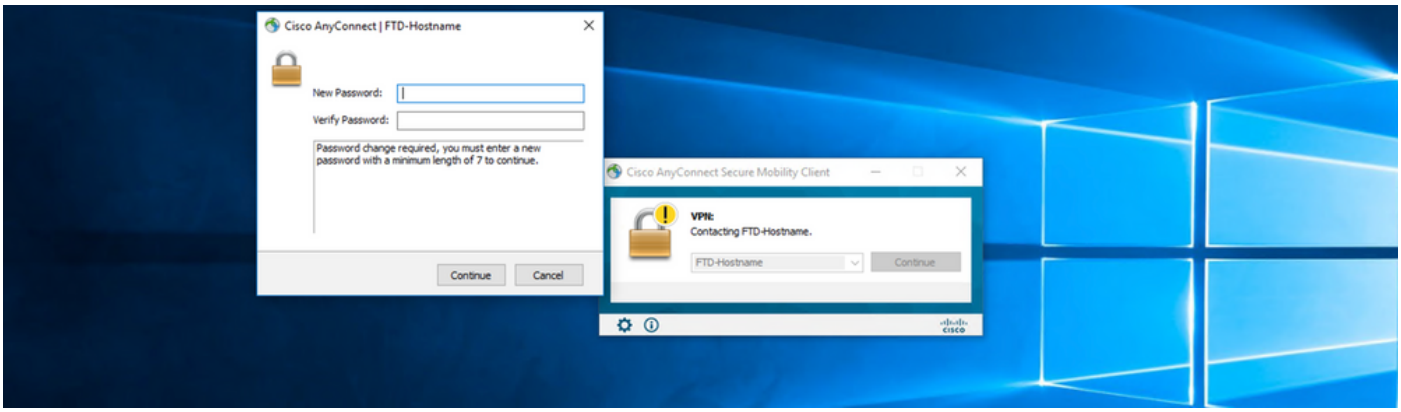
```
> show running-config ssl

ssl trust-point ID-New-Cert Outside
  <-------- FTD ID-cert trustpoint name mapped to the outside interface on which AnyConnect Connections
```

Verificatie

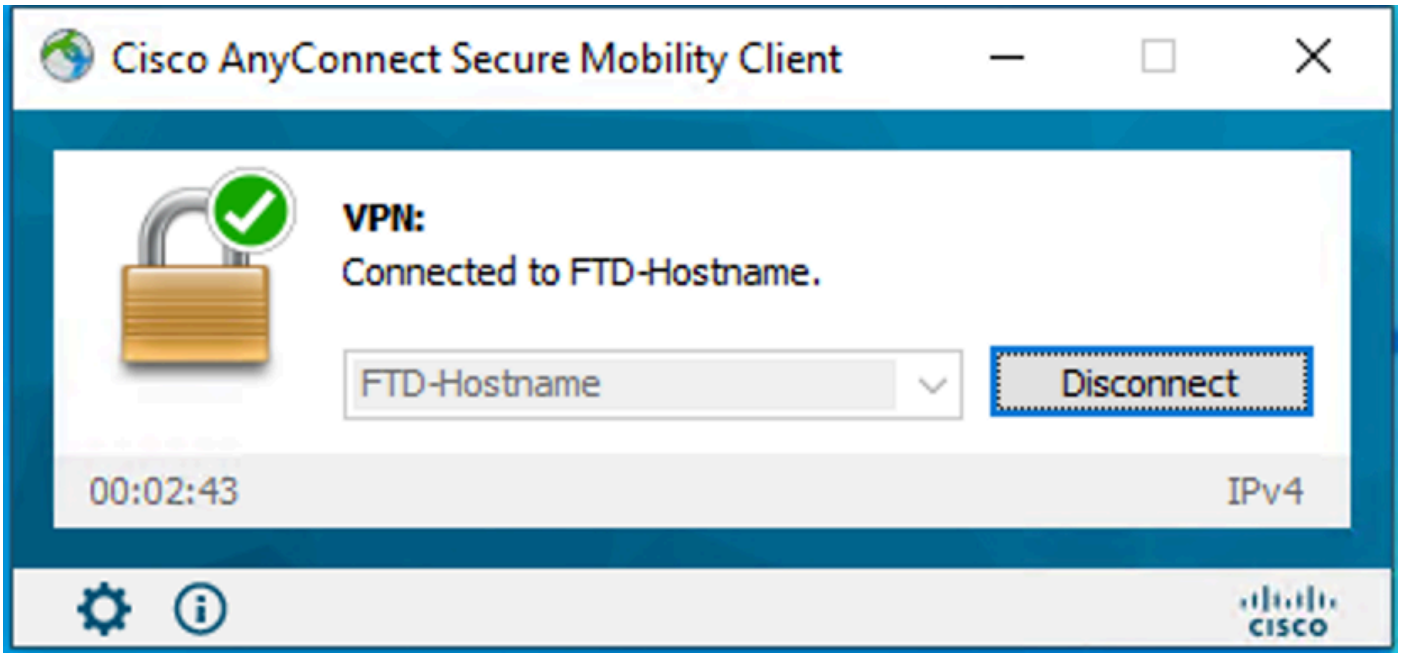
Verbinding maken met AnyConnect en wachtwoordbeheer voor de gebruikersverbinding controleren

1. Start een verbinding met het betreffende verbindingsprofiel. Zodra bij de eerste aanmelding is bepaald dat het wachtwoord moet worden gewijzigd omdat het eerdere wachtwoord door de Microsoft Server is geweigerd omdat het is verlopen, wordt de gebruiker gevraagd het wachtwoord te wijzigen.





2. Zodra de gebruiker het nieuwe wachtwoord voor aanmelding invoert, is de verbinding tot stand gebracht.



3. Controleer de gebruikersverbinding op de FTD CLI:

<#root>

```
FTD_2# sh vpn-sessiondb anyconnect


Session Type: AnyConnect


Username     : admin
               Index        : 7
<------- Username, IP address assigned information of the client


Assigned IP  : 10.1.x.x
             Public IP    : 10.106.xx.xx
Protocol     :
AnyConnect-Parent SSL-Tunnel DTLS-Tunnel


License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx     : 16316                 Bytes Rx     : 2109

Group Policy : AnyConnect-Group      Tunnel Group : AnyConnect-AD

Login Time   : 13:22:24 UTC Mon Apr 25 2022

Duration     : 0h:00m:51s

Inactivity   : 0h:00m:00s

VLAN Mapping : N/A                   VLAN         : none

Audt Sess ID : 0ac5e0fa000070006266a090

Security Grp : none                  Tunnel Zone  : 0
```

Problemen oplossen

Debugs

Dit debug kan worden uitgevoerd in diagnostische CLI om problemen op te lossen met wachtwoordbeheer: debug ladp 255.

Debugs voor werkwachtwoordbeheer

<#root>

```
[24] Session Start

[24] New request Session, context 0x0000148f3c271830, reqType = Authentication

[24] Fiber started

[24] Creating LDAP context with uri=ldaps://10.106.71.234:636

[24] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful

[24] supportedLDAPVersion: value = 3

[24] supportedLDAPVersion: value = 2

[24] Binding as *****@razor.local

[24] Performing Simple authentication for *****@razor.local to 10.106.71.234

[24] LDAP Search:
```

Base DN = [DC=razor,DC=local]

Filter = [sAMAccountName=admin]

Scope   = [SUBTREE]

[24] User DN = [CN=admin,CN=Users,DC=razor,DC=local]

[24] Talking to Active Directory server 10.106.71.234

[24] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[24] Read bad password count 3

[24] Binding as admin

[24] Performing Simple authentication for admin to 10.106.71.234

[24] Simple authentication for admin returned code (49) Invalid credentials

[24] Message (admin): 80090308: LdapErr: DSID-0C0903C5, comment: AcceptSecurityContext error, data 773,

[24] Checking password policy

[24] New password is required for admin

[24] Fiber exit Tx=622 bytes Rx=2771 bytes, status=-1

[24] Session End

[25] Session Start

[25] New request Session, context 0x0000148f3c271830, reqType = Modify Password

[25] Fiber started

[25] Creating LDAP context with uri=ldaps://10.106.71.234:636

[25] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful

[25] supportedLDAPVersion: value = 3

[25] supportedLDAPVersion: value = 2

[25] Binding as *****@razor.local

[25] Performing Simple authentication for *****@razor.local to 10.106.71.234

[25] LDAP Search:

Base DN = [DC=razor,DC=local]

Filter = [sAMAccountName=admin]

Scope = [SUBTREE]

[25] User DN = [CN=admin,CN=Users,DC=razor,DC=local]

[25] Talking to Active Directory server 10.106.71.234

[25] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[25] Read bad password count 3

[25] Change Password for admin successfully converted old password to unicode

[25] Change Password for admin successfully converted new password to unicode

[25] Password for admin successfully changed

[25] Retrieved User Attributes:

[25] objectClass: value = top

[25] objectClass: value = person

[25] objectClass: value = organizationalPerson

[25] objectClass: value = user

[25] cn: value = admin

[25] givenName: value = admin

[25] distinguishedName: value = CN=admin,CN=Users,DC=razor,DC=local

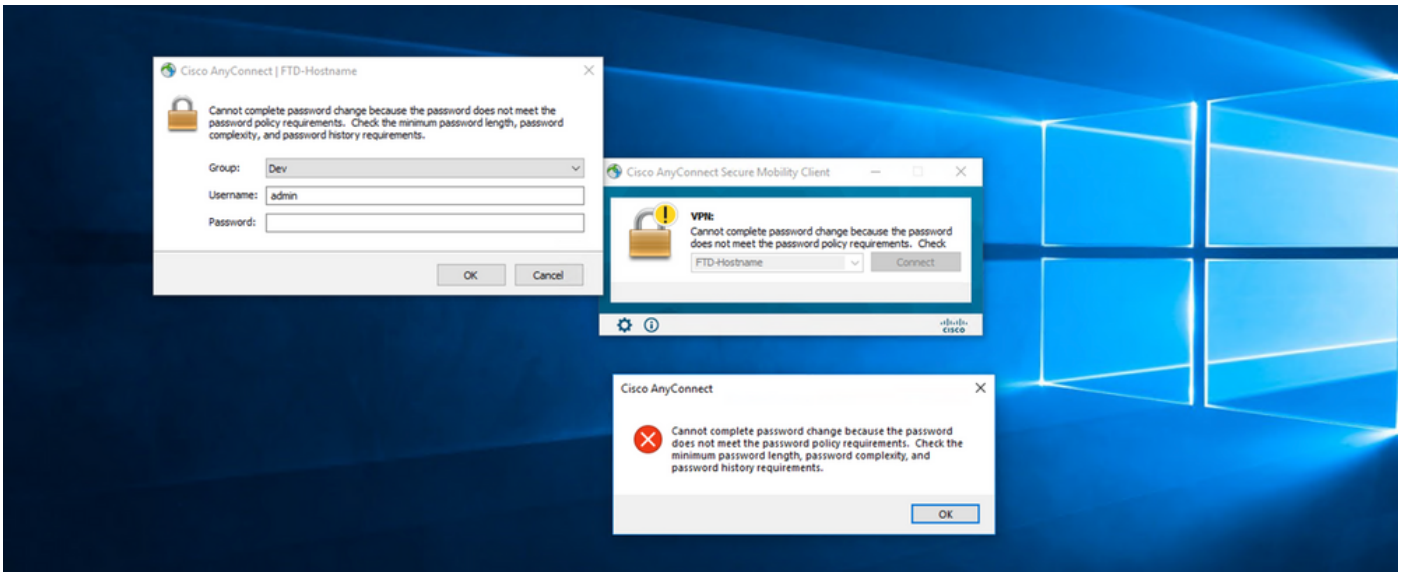
[25] instanceType: value = 4

[25] whenCreated: value = 20201029053516.0Z

```
[25]   whenChanged: value = 20220426032127.0Z
[25]   displayName: value = admin
[25]   uSNCreated: value = 16710
[25]   uSNChanged: value = 98431
[25]   name: value = admin
[25]   objectGUID: value = ..0.].LH.....9.4
[25]   userAccountControl: value = 512
[25]   badPwdCount: value = 3
[25]   codePage: value = 0
[25]   countryCode: value = 0
[25]   badPasswordTime: value = 132610388348662803
[25]   lastLogoff: value = 0
[25]   lastLogon: value = 132484577284881837
[25]   pwdLastSet: value = 0
[25]   primaryGroupID: value = 513
[25]   objectSid: value = ................7Z|....RQ...
[25]   accountExpires: value = 9223372036854775807
[25]   logonCount: value = 0
[25]   sAMAccountName: value = admin
[25]   sAMAccountType: value = 805306368
[25]   userPrincipalName: value = ******@razor.local
[25]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=razor,DC=local
[25]   dSCorePropagationData: value = 20220425125800.0Z
[25]   dSCorePropagationData: value = 20201029053516.0Z
[25]   dSCorePropagationData: value = 16010101000000.0Z
[25]   lastLogonTimestamp: value = 132953506361126701
[25]   msDS-SupportedEncryptionTypes: value = 0
[25]   uid: value = ******@razor.local
[25] Fiber exit Tx=714 bytes Rx=2683 bytes, status=1
[25] Session End
```

Veelvoorkomende fouten die tijdens het wachtwoordbeheer worden aangetroffen

Als het wachtwoordbeleid dat door de Microsoft Server is ingesteld niet wordt nageleefd wanneer de gebruiker het nieuwe wachtwoord invoert, wordt de verbinding verbroken met de fout "Wachtwoord voldoet niet aan de Wachtwoordbeleidsvereisten". Zorg er dus voor dat het nieuwe wachtwoord voldoet aan het beleid dat door de Microsoft Server voor LDAP's is ingesteld.



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.