Kennwortverwaltung mit LDAPs für RA VPN auf FTD konfiguriert, von FMC verwaltet

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der Kennwortverwaltung mithilfe von LDAPs für AnyConnect-Clients beschrieben, die eine Verbindung mit Cisco FirePOWER Threat Defense (FTD) herstellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- Grundkenntnisse der RA VPN-Konfiguration (Remote Access Virtual Private Network) auf FMC
- Grundkenntnisse der LDAP-Serverkonfiguration auf FMC
- Grundkenntnisse von Active Directory

Verwendete Komponenten

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

- Microsoft 2012 R2-Server
- FMCv mit 7.3.0
- FTDv mit 7.3.0

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

Konfiguration

Netzwerkdiagramm und -szenario

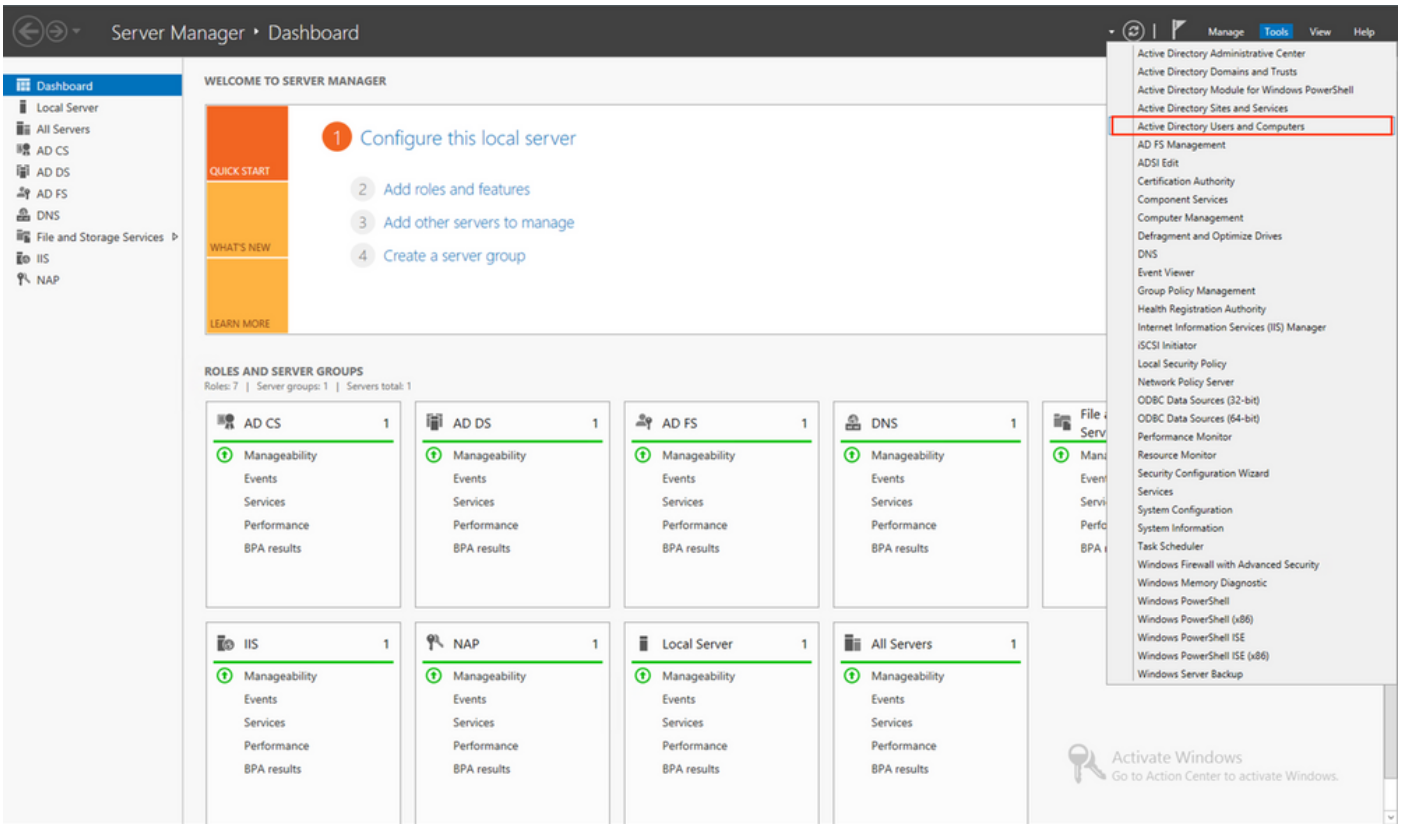
Der Windows-Server ist mit ADDS und ADCS vorkonfiguriert, um die Verwaltung des Benutzerkennworts zu testen. In dieser Konfigurationsanleitung werden diese Benutzerkonten erstellt.

Benutzerkonten:

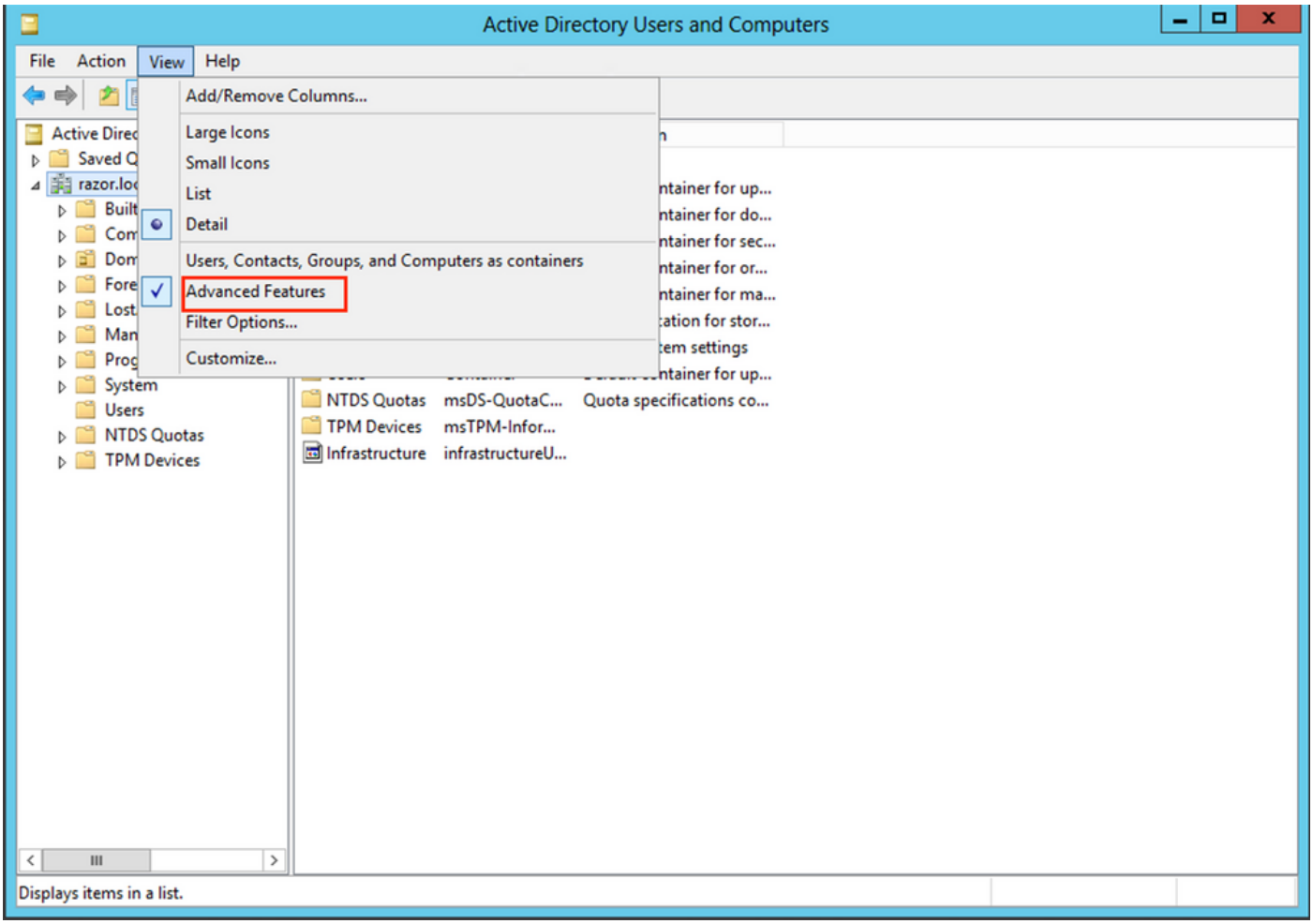
- Administrator: Dieser Parameter wird als Verzeichniskonto verwendet, damit die FTD eine Bindung zum Active Directory-Server herstellen kann.
- admin: Ein Test-Administratorkonto, mit dem die Benutzeridentität veranschaulicht wird.

Ermitteln der LDAP-Basis-DN und Gruppen-DN

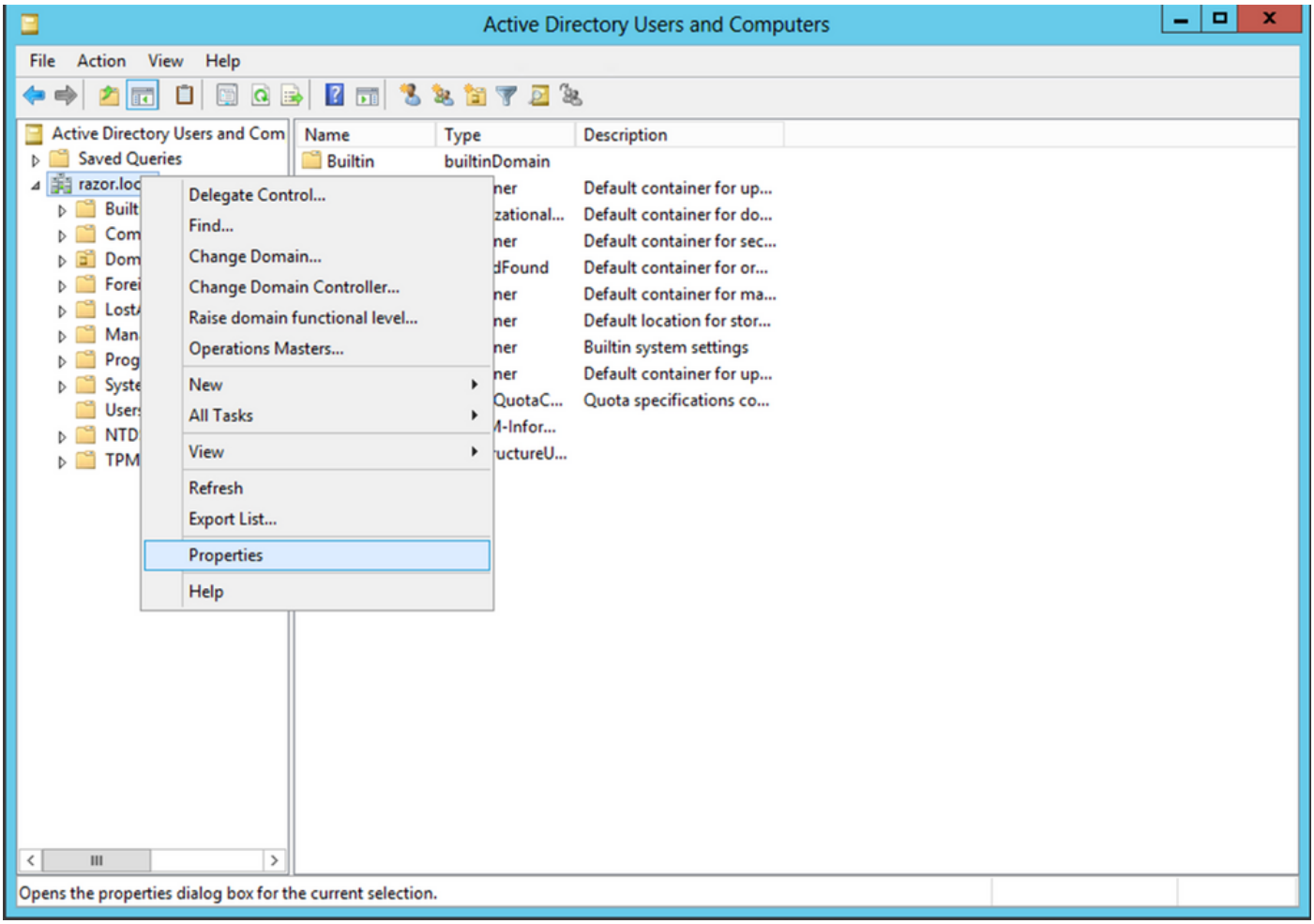
1. Offen Active Directory Users and Computers über das Server Manager-Dashboard.



2. Öffnen Sie View Option oben an, und aktivieren Sie die Advanced Features, wie in der Abbildung dargestellt:



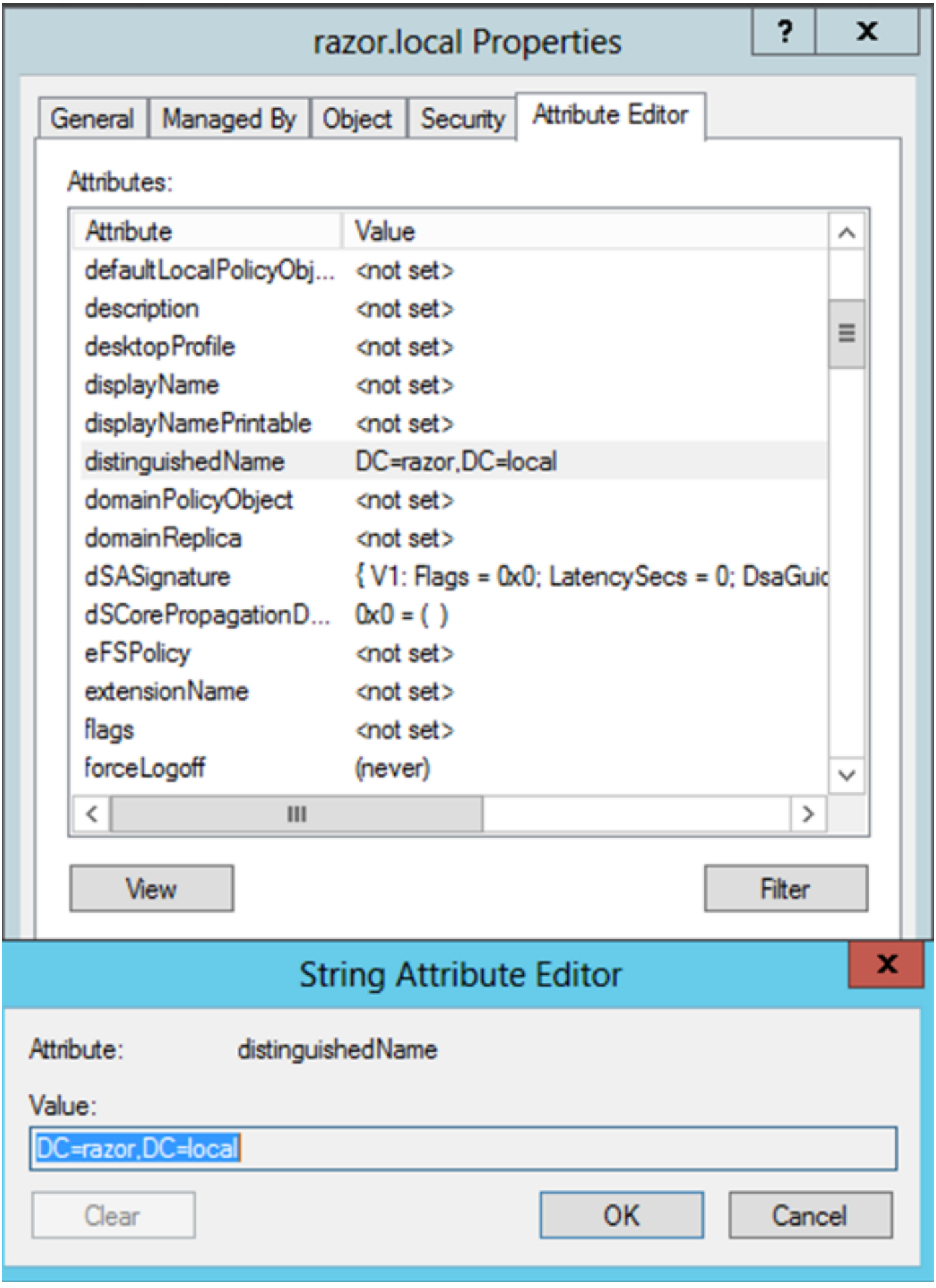
3. Dies ermöglicht die Anzeige zusätzlicher Eigenschaften unter den AD-Objekten. Um z. B. den DN für den Root zu finden, razor.local, Rechtsklick razor.local, und wählen Sie Properties, wie in diesem Bild gezeigt:



4. Unter Properties, wählen Sie Attribute Editor aus. Suchen distinguishedName klicken Sie unter den Attributen auf View, wie im Bild dargestellt.

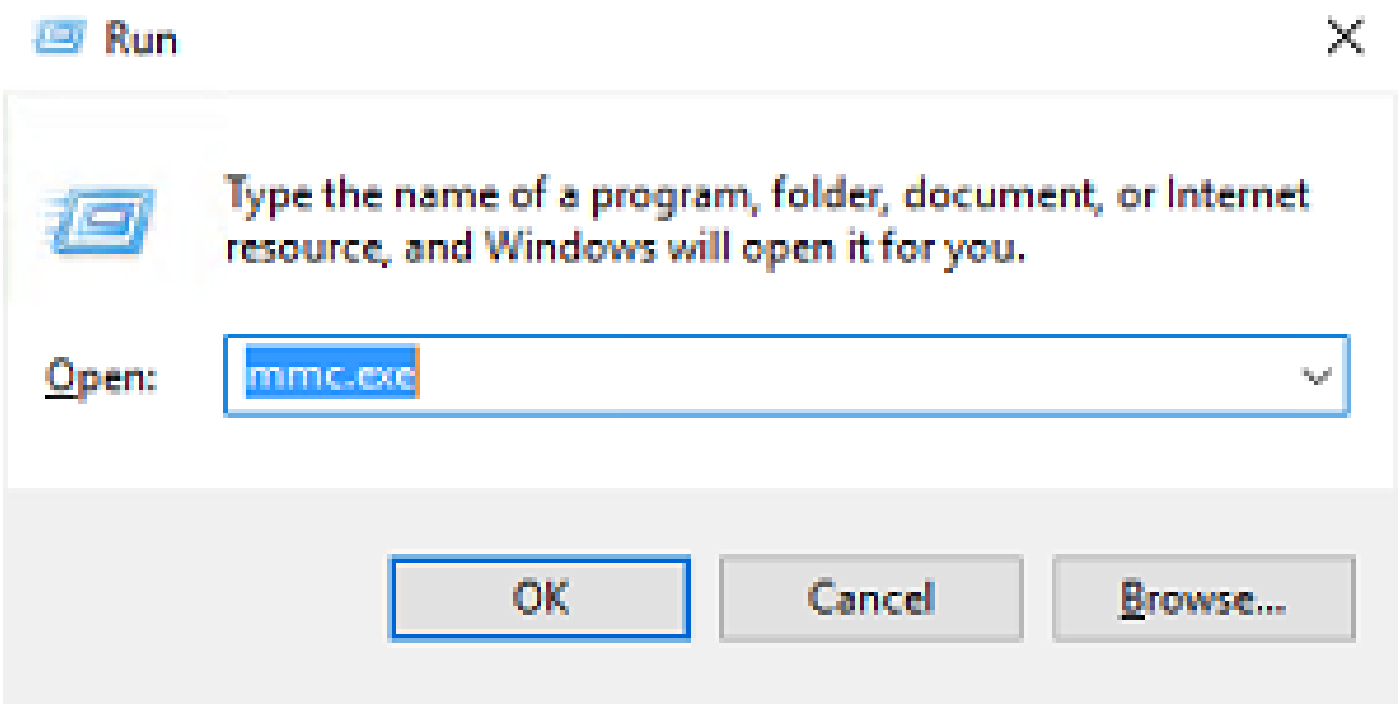
Daraufhin wird ein neues Fenster geöffnet, in das die DN kopiert und später in FMC eingefügt werden kann.

In diesem Beispiel ist der Stamm-DN DC=razor, DC=local. Kopieren Sie den Wert, und speichern Sie ihn für einen späteren Zeitpunkt. Klicken Sie auf OK um das Fenster String Attribute Editor zu verlassen und auf OK um die Eigenschaften zu beenden.

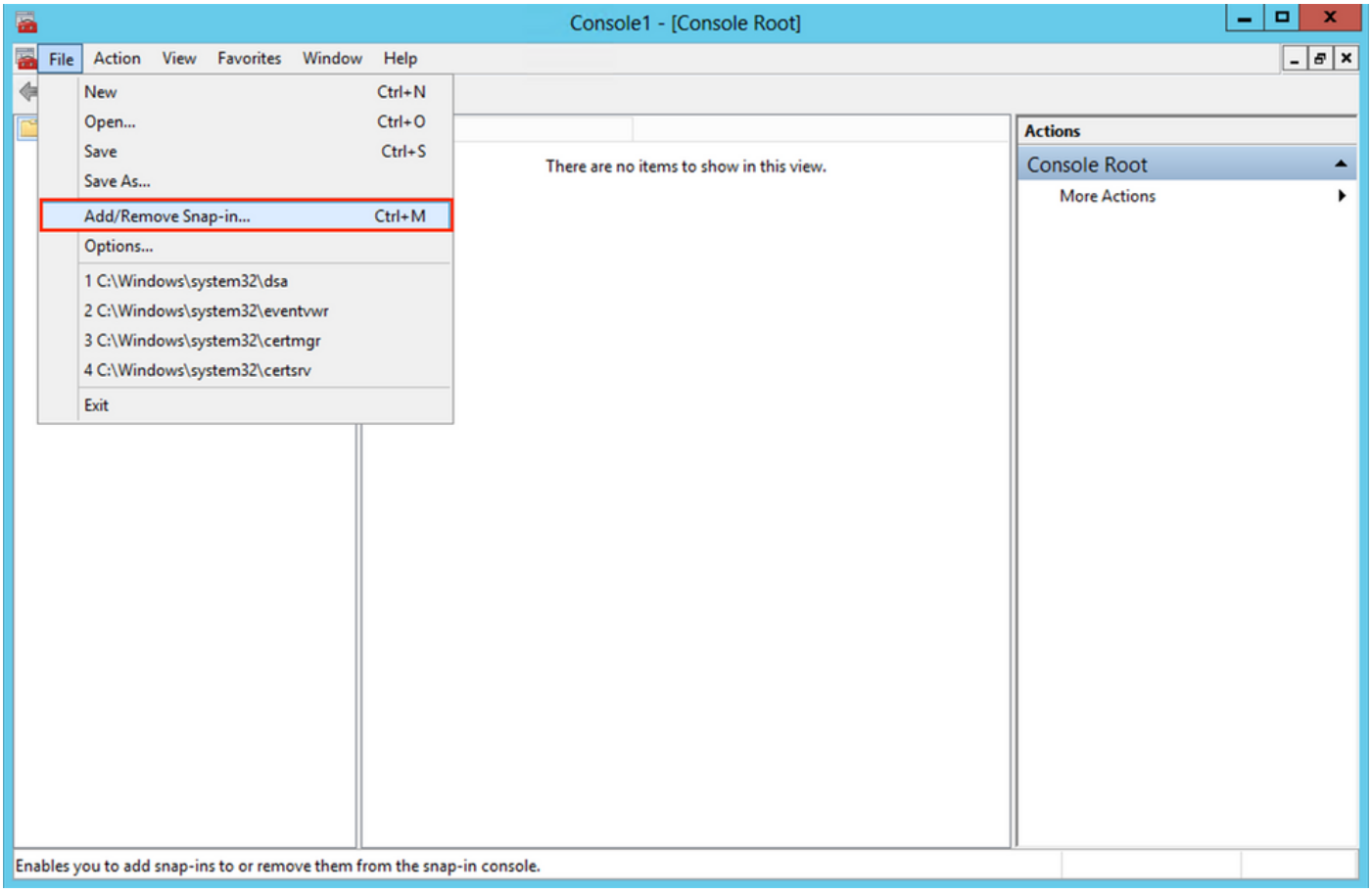

razor.local Properties
General
Managed By
Object
Security
Attribute Editor
Attributes:
Attribute
Value
defaultLocalPolicyObj...
<not set>
description
<not set>
desktopProfile
<not set>
displayName
<not set>
displayNamePrintable
<not set>
distinguishedName
DC=razor,DC=local
domainPolicyObject
<not set>
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

LDAP SSL-Zertifikatstamm kopieren

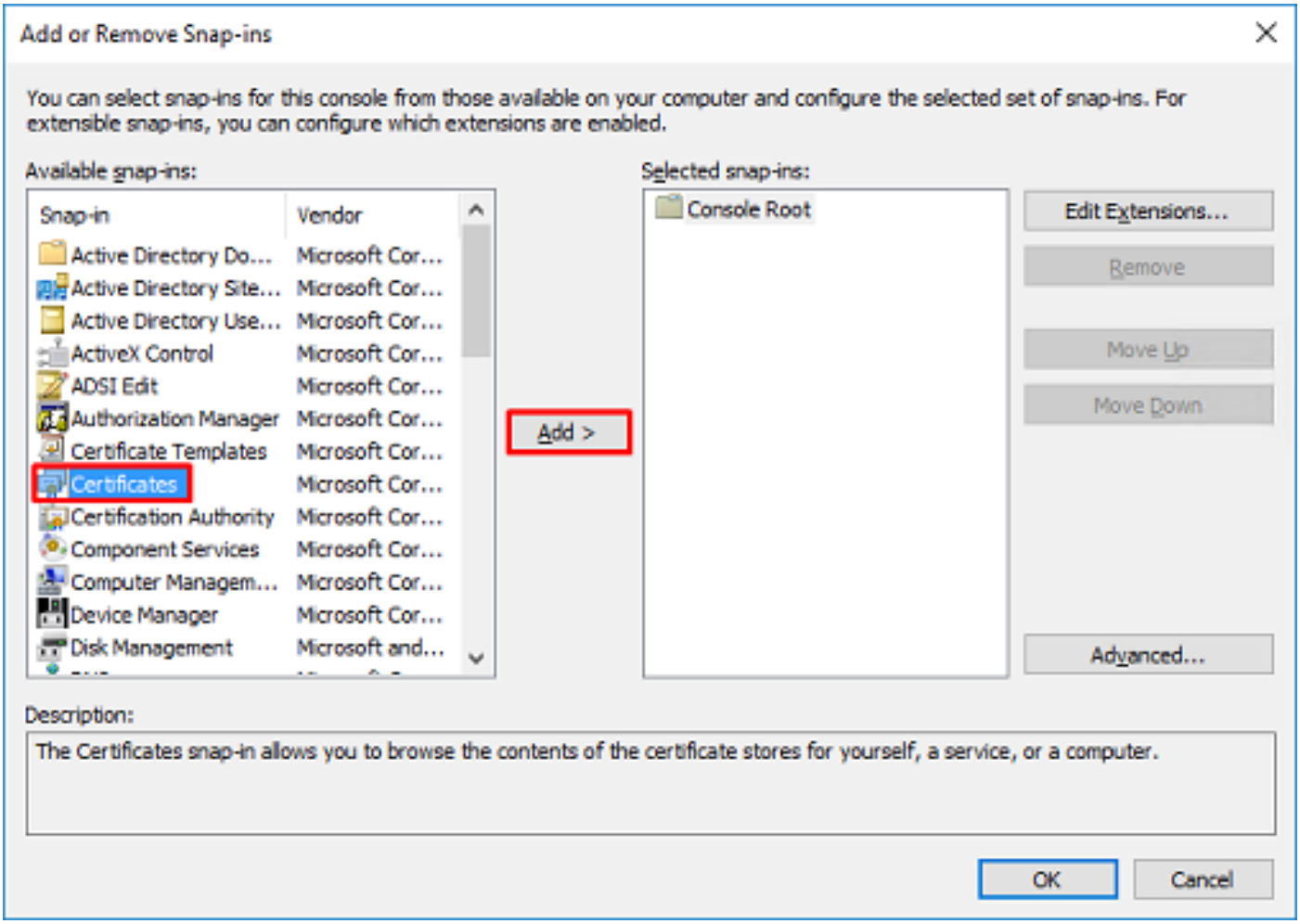
1. Presse Win+R und geben mmc.exe, und klicken Sie dann auf OK, wie in diesem Bild dargestellt.



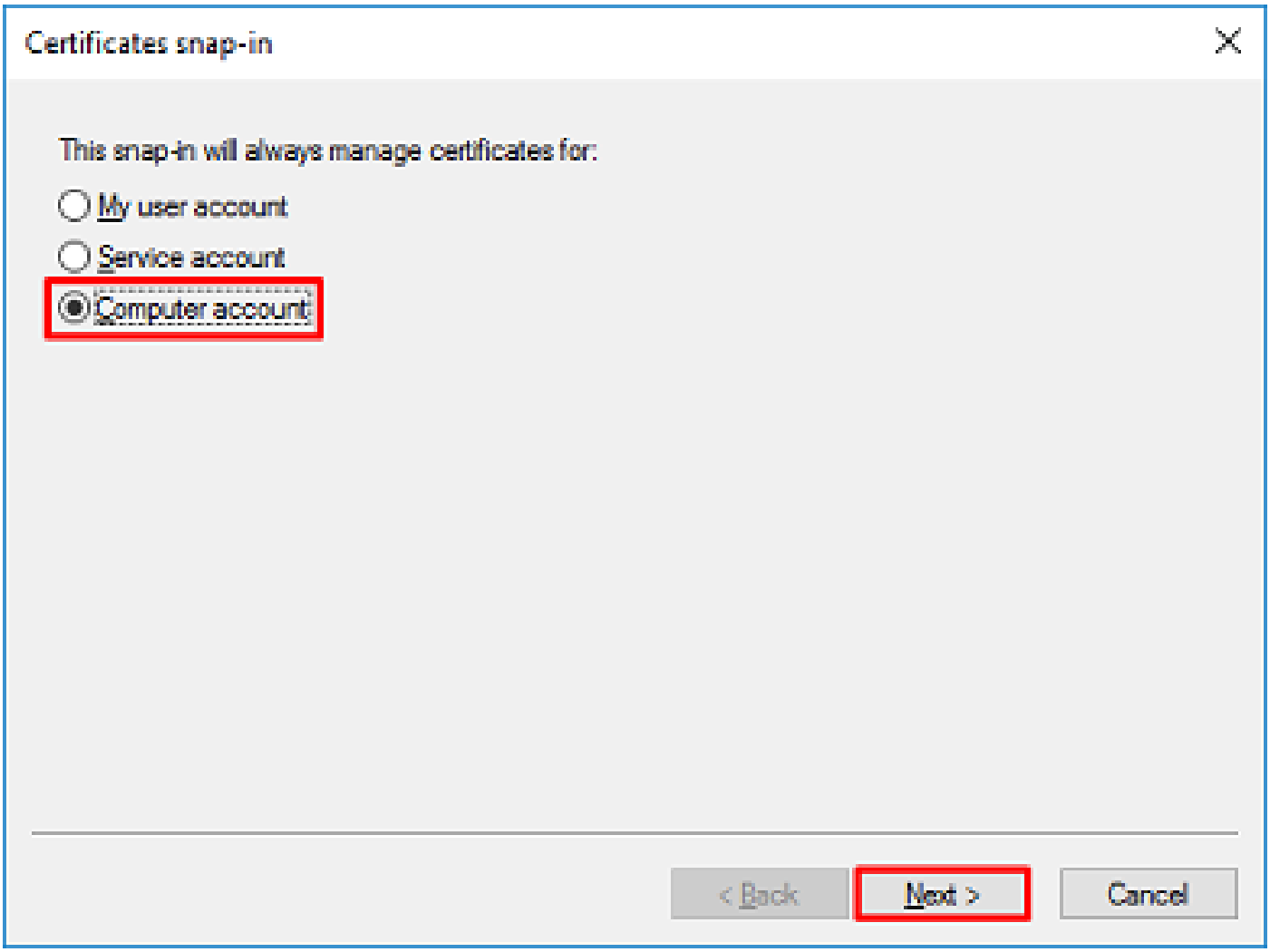
2. Navigieren Sie zu File > Add/Remove Snap-in..., wie in diesem Bild gezeigt:



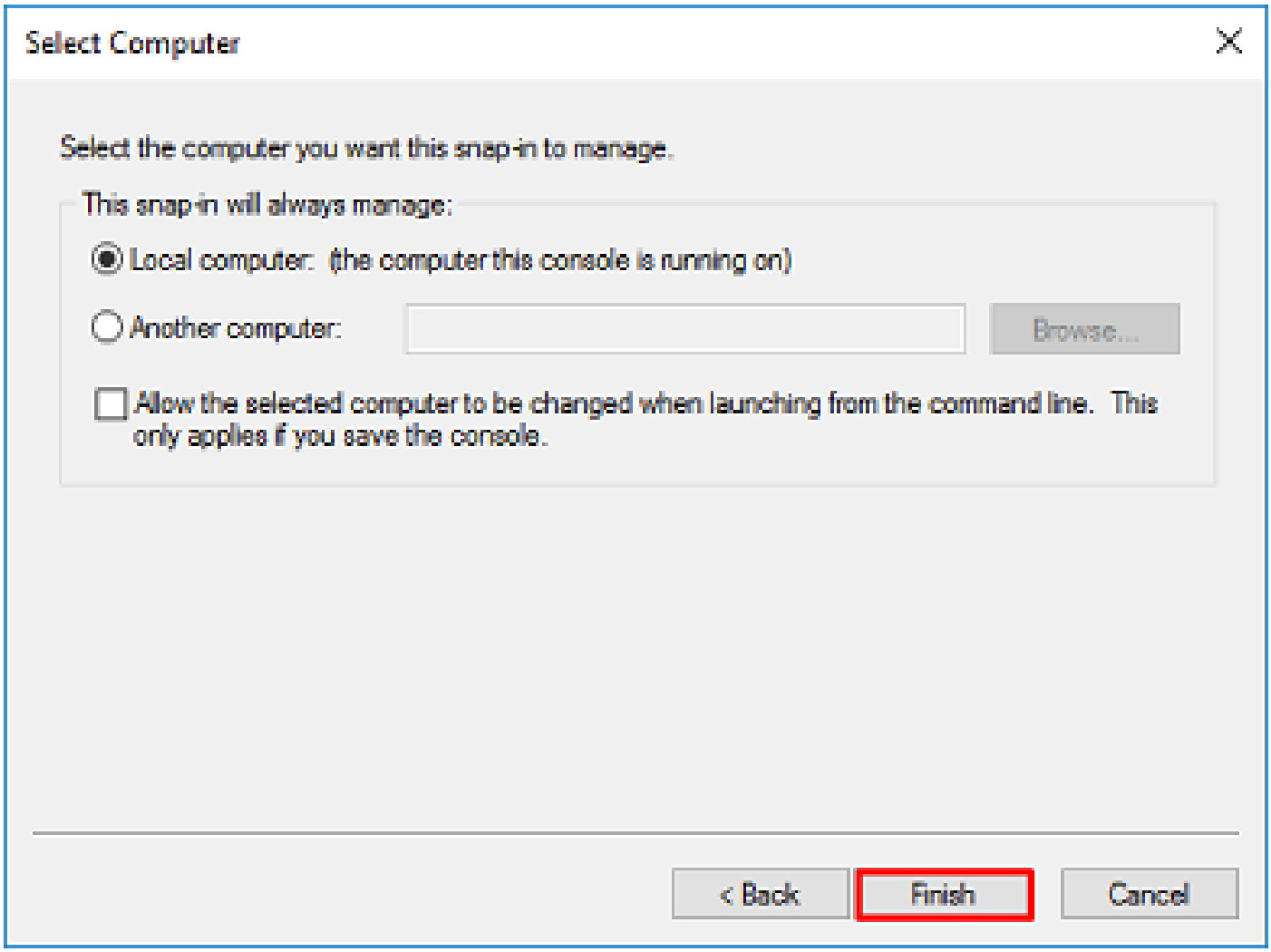
3. Wählen Sie unter Verfügbare Snap-Ins die Option Certificates und dann auf Add, wie in diesem Bild gezeigt:



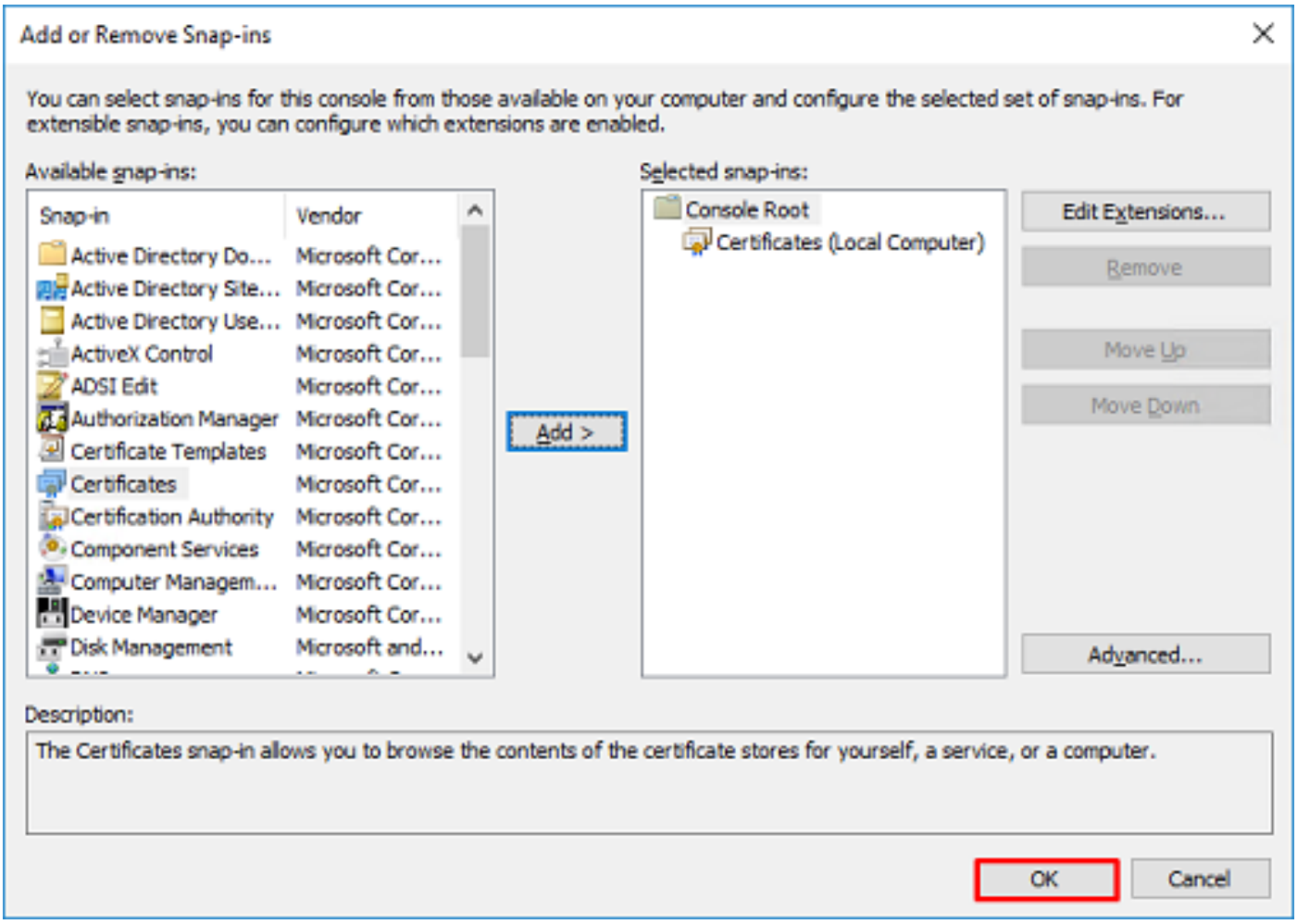
4. Auswählen Computer account und dann auf Next, wie in diesem Bild gezeigt:



Klicken Sie wie hier gezeigt auf Finish.



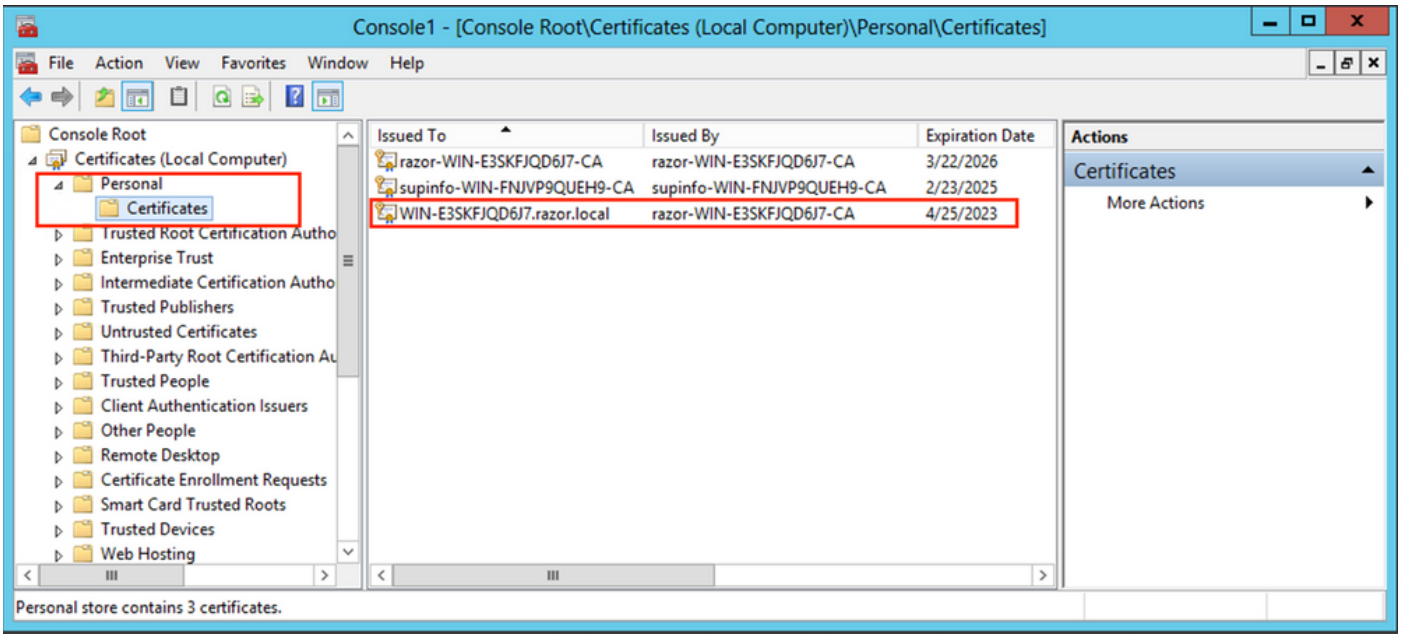
5. Klicken Sie jetzt auf OK, wie in diesem Bild dargestellt.



6. Erweitern Sie die Personal Ordner, und klicken Sie auf Certificates. Das von LDAPs verwendete Zertifikat muss für den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Windows-Servers ausgestellt werden. Auf diesem Server sind drei Zertifikate aufgelistet:

- Ein Zertifizierungsstellenzertifikat wurde ausgestellt von und an razor-WIN-E3SKFJQD6J7-CA.
- Ein Zertifizierungsstellenzertifikat, das an und von supinfo-WIN-FNJVP9QUEH9-CA.
- Ein Identitätszertifikat wurde ausgestellt für WIN-E3SKFJQD6J7.razor.local von razor-WIN-E3SKFJQD6J7-CA.

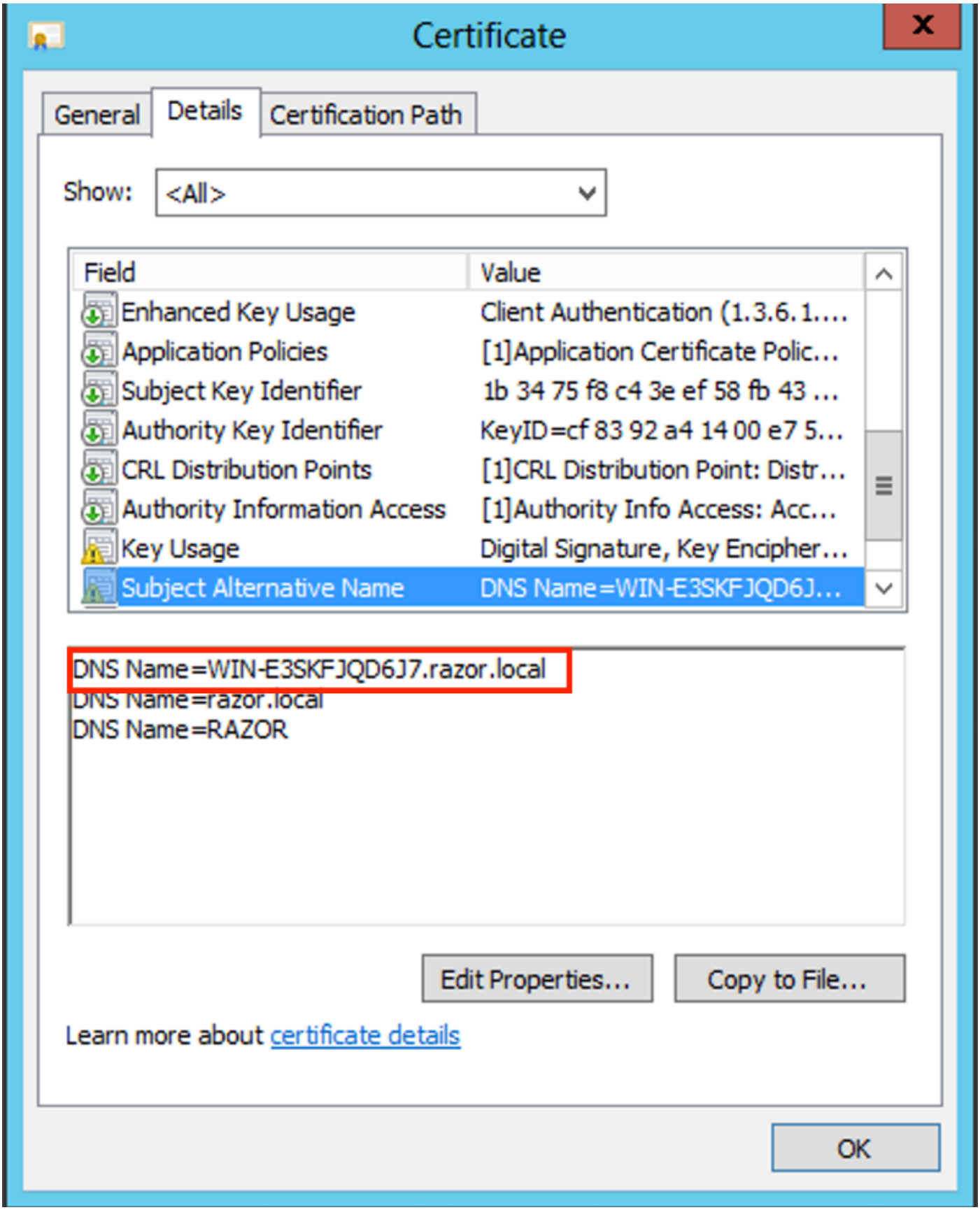
In diesem Konfigurationsleitfaden wird der FQDN WIN-E3SKFJQD6J7.razor.local Daher sind die ersten beiden Zertifikate nicht als LDAP SSL-Zertifikat gültig. Das Identitätszertifikat, das ausgestellt wurde an WIN-E3SKFJQD6J7.razor.local ist ein Zertifikat, das automatisch vom Windows Server-Zertifizierungsstellendienst ausgestellt wurde. Doppelklicken Sie auf das Zertifikat, um die Details zu überprüfen.



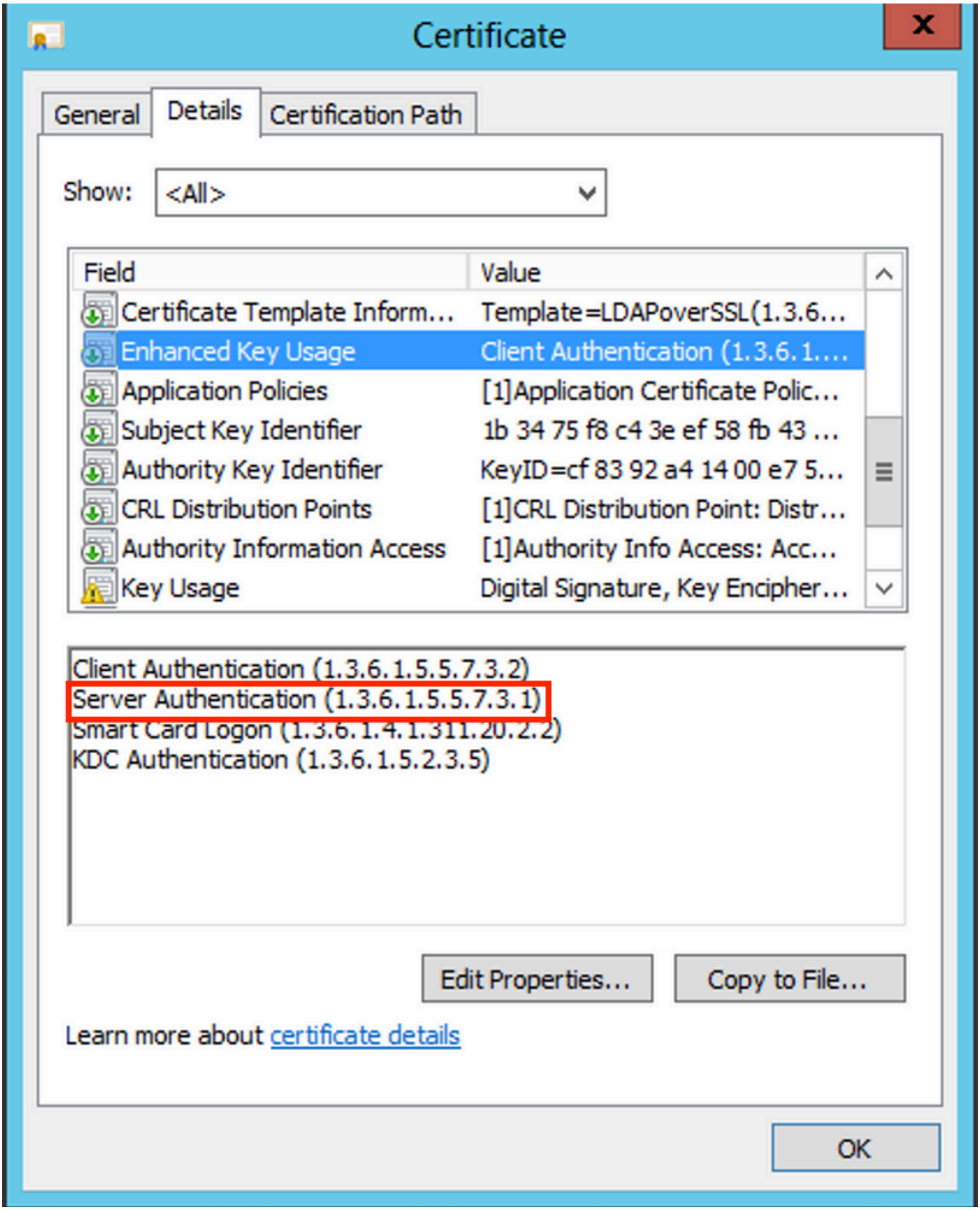
7. Um als LDAP SSL-Zertifikat verwendet werden zu können, muss das Zertifikat folgende Anforderungen erfüllen:

- Der allgemeine Name oder alternative DNS-Betreffname stimmt mit dem FQDN des Windows Servers überein.
- Das Zertifikat weist im Feld "Enhanced Key Usage" (Erweiterte Schlüsselverwendung) eine Serverauthentifizierung auf.

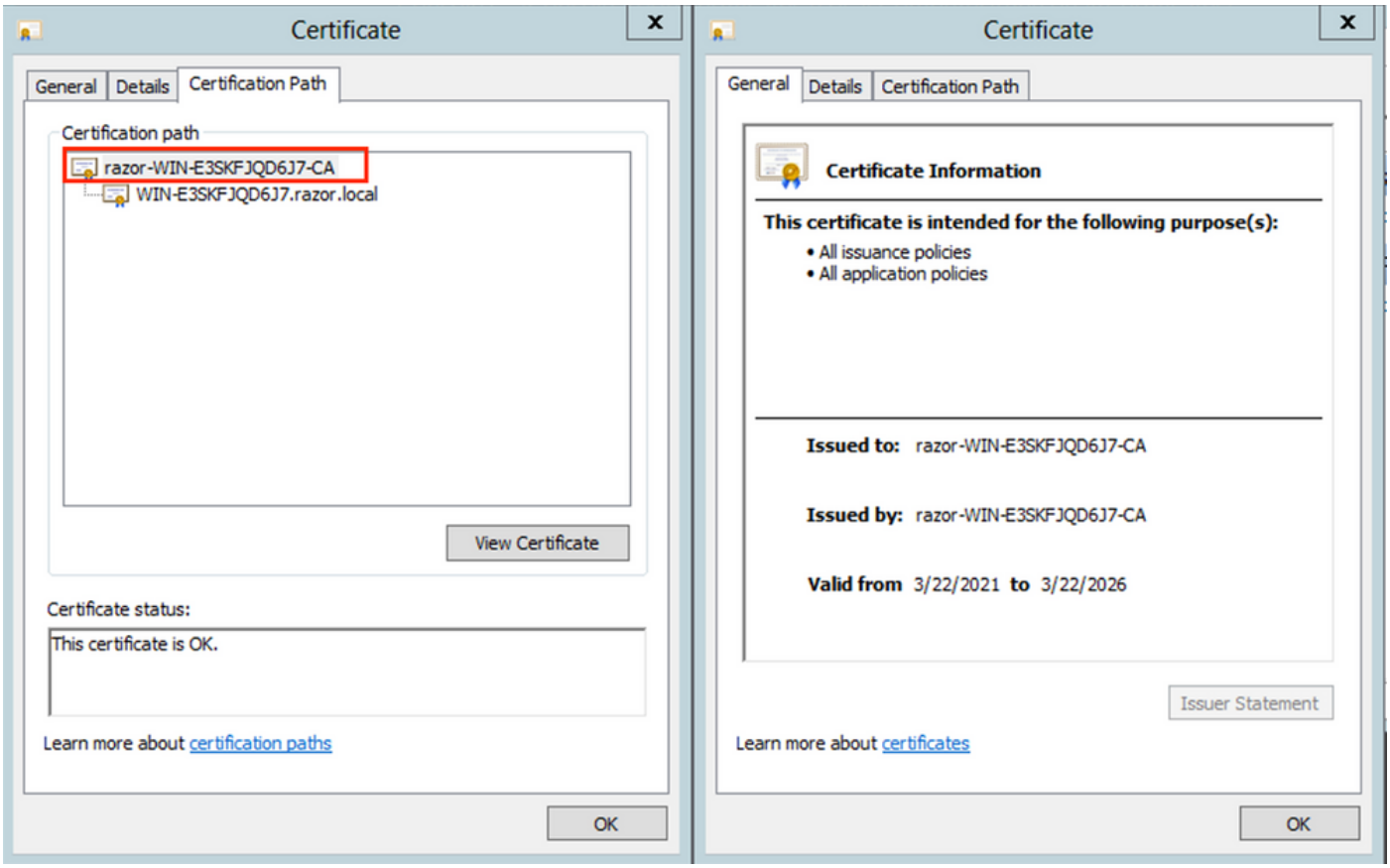
Im Details Registerkarte für das Zertifikat, wählen Sie Subject Alternative Name, wobei der FQDN WIN-E3SKFJQD6J7.razor.local vorhanden ist.



Unter Enhanced Key Usage, Server Authentication vorhanden ist.

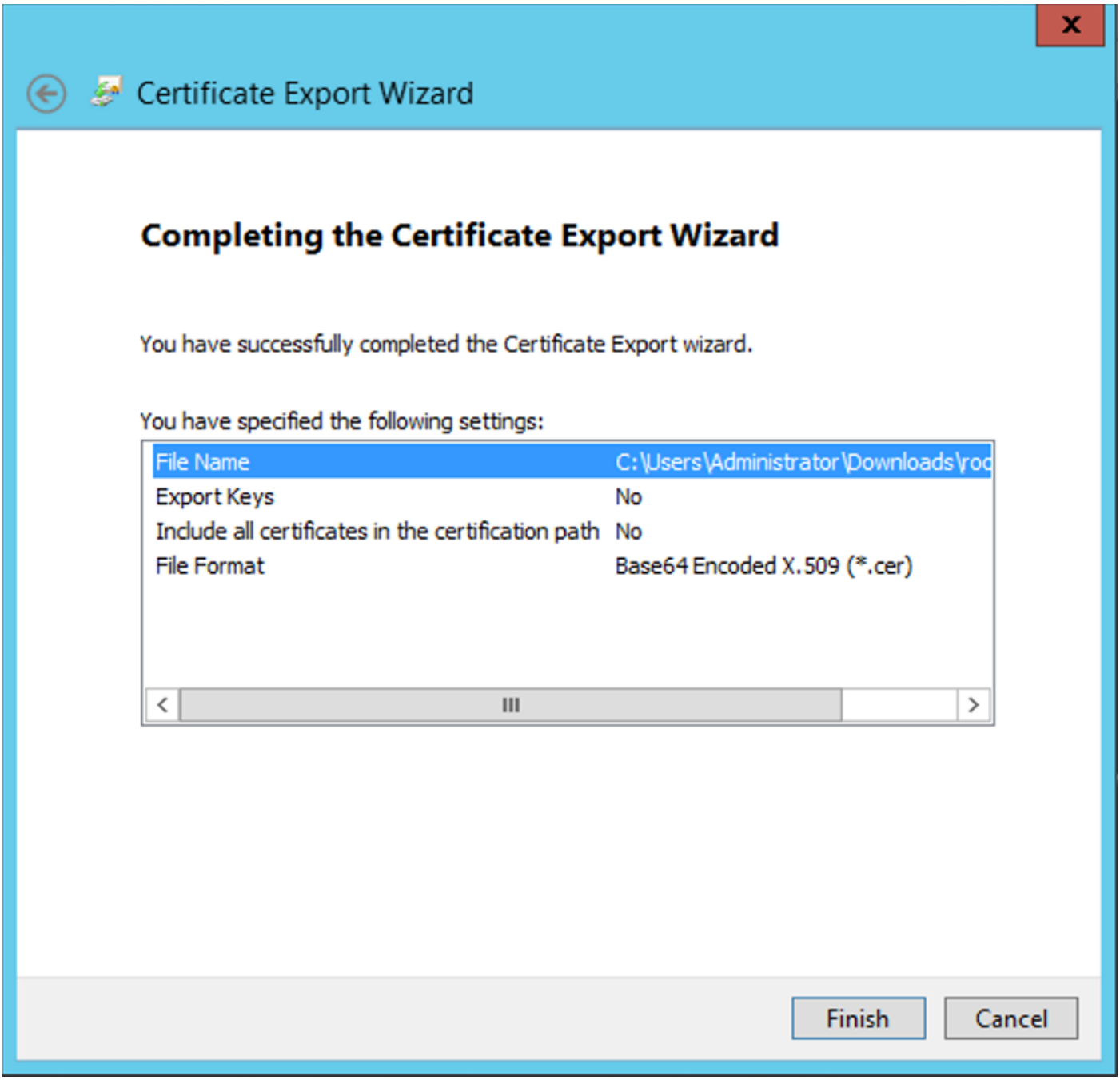


8. Sobald dies bestätigt ist, wird im Rahmen des Certification Path auf, wählen Sie das Zertifikat der obersten Ebene aus, das das Root-Zertifizierungsstellenzertifikat darstellt, und klicken Sie dann auf View Certificate. Dadurch werden die Zertifikatdetails für das Stammzertifikat der Zertifizierungsstelle geöffnet, wie im Bild gezeigt:



9. Im Details Registerkarte des Stammzertifikats der Zertifizierungsstelle klicken Sie auf Copy to File und navigieren Sie durch dieCertificate Export Wizard der die Stammzertifizierungsstelle im PEM-Format exportiert.

Auswählen Base-64 encoded X.509 als Dateiformat.



10. Öffnen Sie das Zertifikat der Stammzertifizierungsstelle, das am ausgewählten Speicherort auf dem Computer gespeichert ist, mit einem Notizblock oder einem anderen Texteditor.

Zeigt das Zertifikat im PEM-Format an. Speichern Sie das für später.

```
-----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-----
```

Wenn mehrere Zertifikate im lokalen Computerspeicher auf dem LDAP-Server installiert sind (optional)

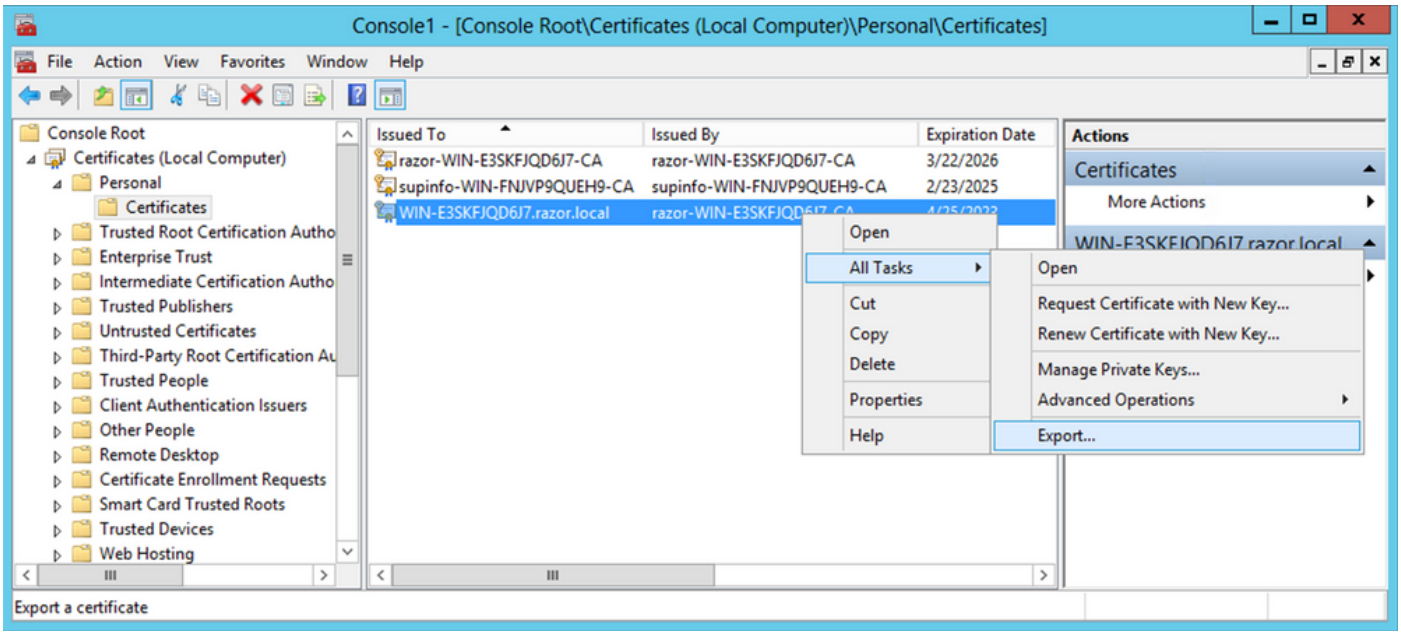
1. Bei mehreren Identitätszertifikaten, die von LDAPS verwendet werden können und bei Unsicherheit darüber, welche verwendet werden, oder wenn kein Zugriff auf den LDAPS-Server besteht, ist es weiterhin möglich, die Stammzertifizierungsstelle aus einer Paketerfassung auf dem FTD zu extrahieren.

2. Wenn Sie im lokalen Computer-Zertifikatspeicher des LDAP-Servers (z. B. AD DS-Domänencontroller) mehrere Zertifikate haben, die für die Serverauthentifizierung gültig sind, kann festgestellt werden, dass für die LDAPS-Kommunikation ein anderes Zertifikat verwendet wird. Die beste Lösung für ein solches Problem besteht darin, alle nicht benötigten Zertifikate aus dem Zertifikatspeicher des lokalen Computers zu entfernen und nur ein Zertifikat zu haben, das für die Serverauthentifizierung gültig ist.

Wenn jedoch ein legitimer Grund vorliegt, dass Sie zwei oder mehr Zertifikate benötigen und mindestens über einen Windows Server 2008 LDAP-Server verfügen, kann der Active Directory Domain Services (NTDS\Personal)-Zertifikatspeicher für die LDAP-Kommunikation verwendet werden.

Diese Schritte zeigen, wie ein LDAPS-aktiviertes Zertifikat aus einem Zertifikatspeicher des lokalen Domänencontrollers in den Zertifikatspeicher des Active Directory-Domänendiensts (NTDS\Personal) exportiert wird.

- Navigieren Sie zur MMC-Konsole auf dem Active Directory-Server, wählen Sie Datei aus, und klicken Sie dann auf Add/Remove Snap-in.
- Klicken Sie auf Certificates und dann auf Add.
- Im Certificates snap-in, wählen Computer account und dann auf Next.
- In Select Computer, wählen Local Computer,Klicken Sie auf OK, und klicken Sie dann auf Finish. In Add or Remove Snap-ins,Klicken Sie auf OK.
- Klicken Sie in der Zertifikatskonsole eines Computers, der ein für die Serverauthentifizierung verwendetes Zertifikat enthält, mit der rechten Maustaste auf den certificate,Klicken Sie auf All Tasks, und klicken Sie dann auf Export.

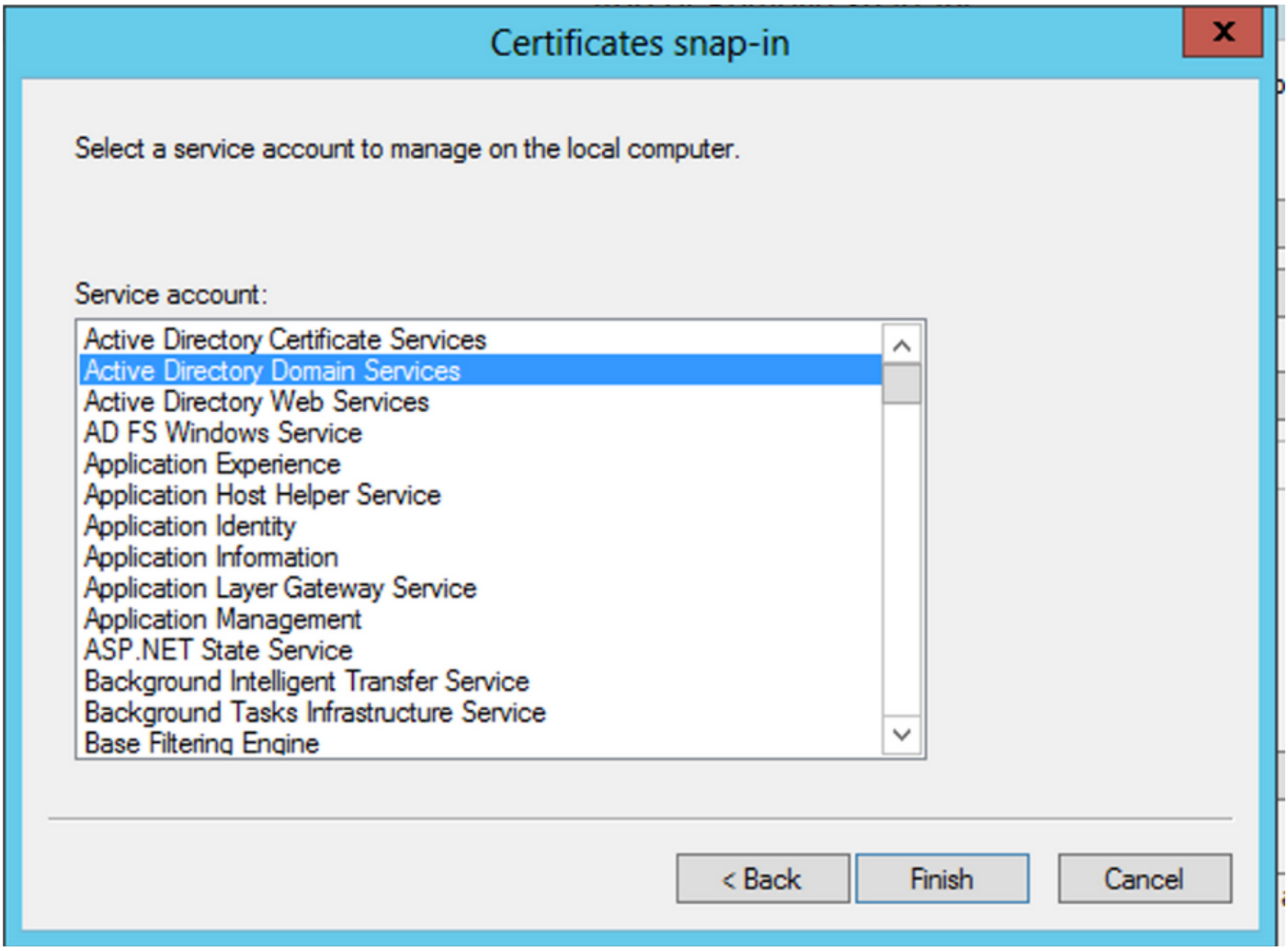


- Exportieren Sie das Zertifikat im pfx in den nachfolgenden Abschnitten formatieren. Verweisen Sie in diesem Artikel darauf, wie ein Zertifikat im pfx Format aus MMC:

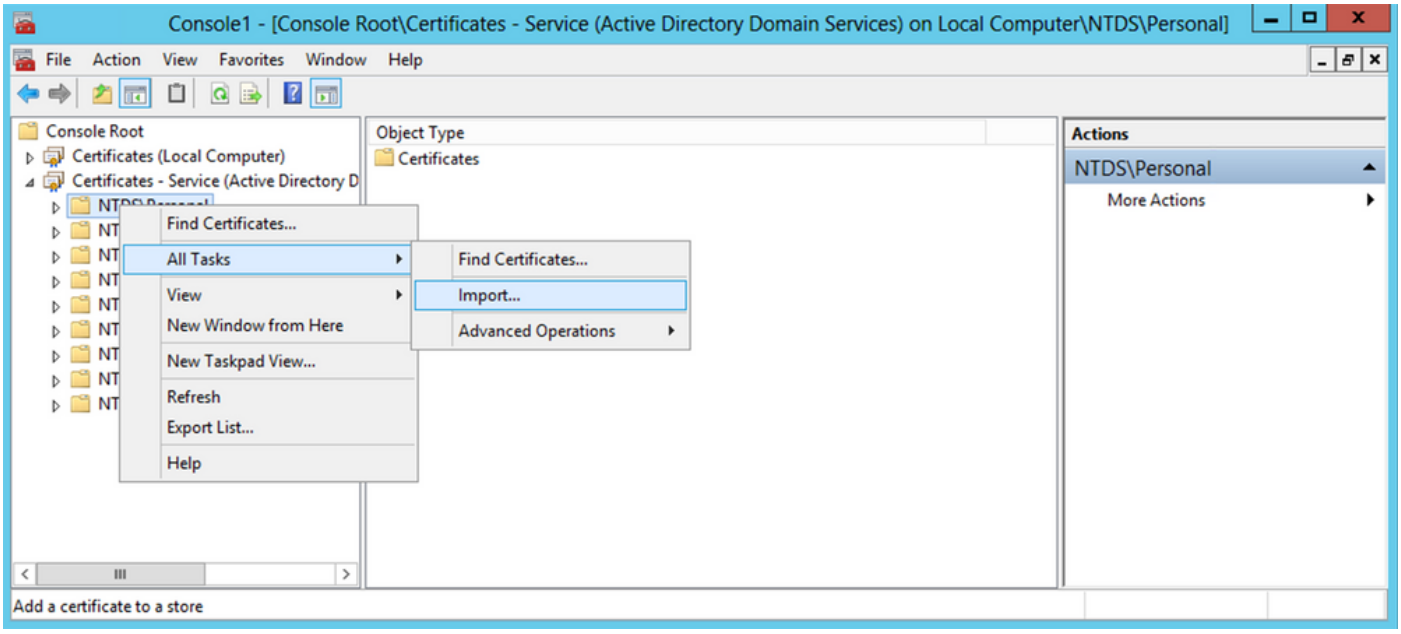
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html

- Sobald der Export des Zertifikats abgeschlossen ist, navigieren Sie zu Add/Remove Snap-in on MMC console. Klicken Sie auf Certificates und dann auf Add.
- Auswählen Service account und dann auf Next.

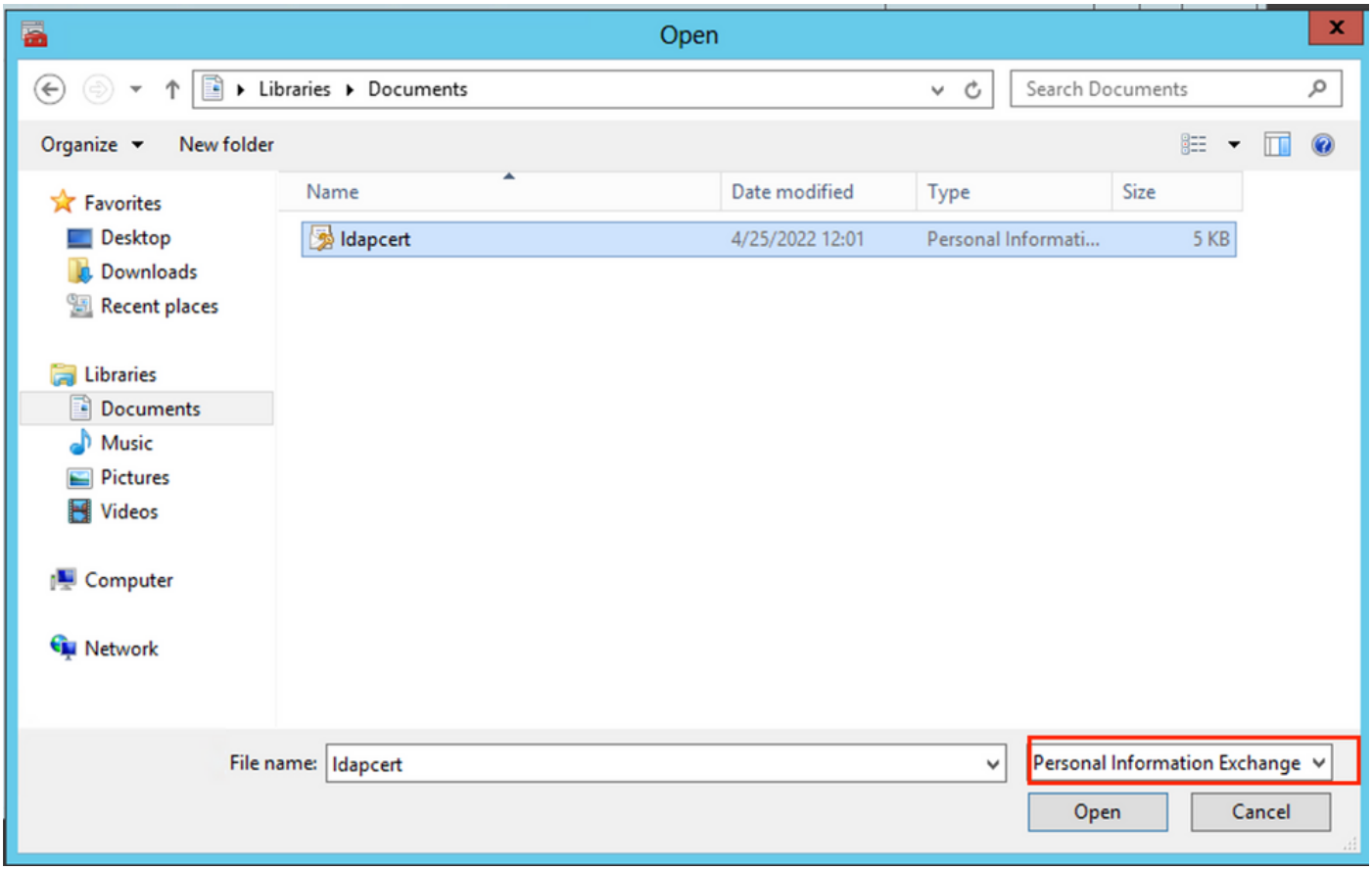
- Im Select Computer Dialogfeld auswählen, Local Computer und klicke auf Next.
- Auswählen Active Directory Domain Services und dann auf Finish.



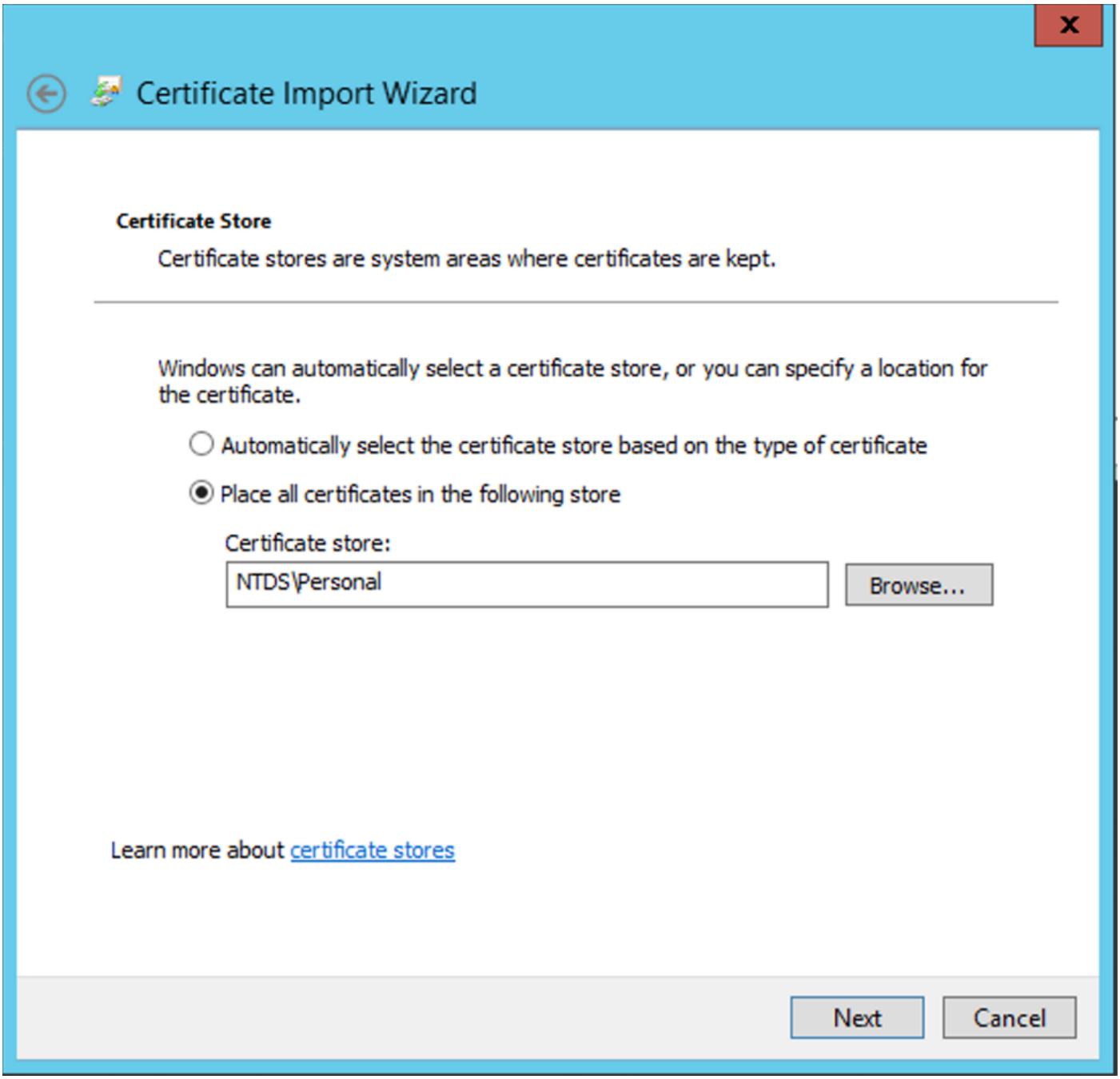
- Auf dem Add/Remove Snap-ins auf OK.
- Erweitern Certificates - Services (Active Directory Domain Services) und dann auf NTDS\Personal.
- Rechtsklick NTDS\Personal,Klicken Sie auf All Tasks, und klicken Sie dann auf Import.



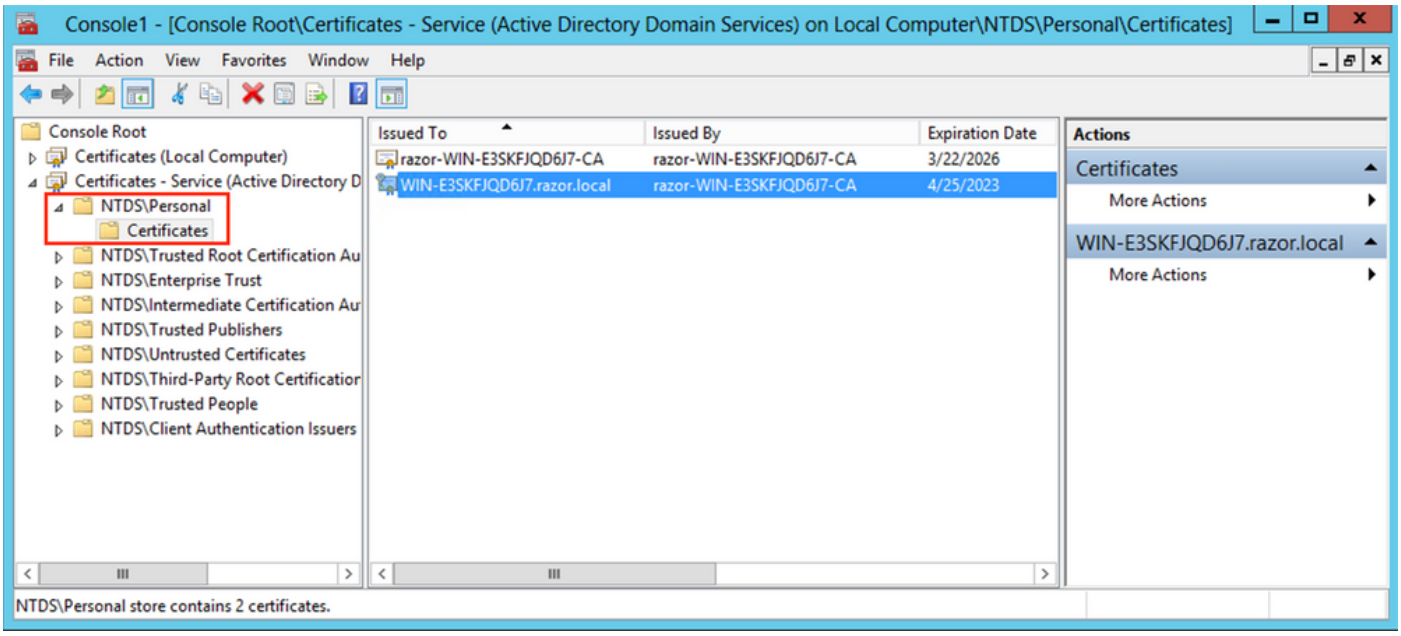
- Auf dem Certificate Import Wizard Willkommensbildschirm, auf Next.
- Klicken Sie im Bildschirm Zu importierende Datei auf Browse, und suchen Sie die Zertifikatsdatei, die Sie zuvor exportiert haben.
- Stellen Sie auf dem Bildschirm Öffnen sicher, dass Persönliche Informationen ausgetauscht werden (*pfx,*.p12) als Dateityp ausgewählt ist, und navigieren Sie dann im Dateisystem, um das zuvor exportierte Zertifikat zu suchen. Klicken Sie dann auf das Zertifikat.



- Klicken Sie auf Open und dann auf Next.
- Geben Sie im Bildschirm Password (Kennwort) das Kennwort ein, das Sie für die Datei festgelegt haben, und klicken Sie dann auf Next.
- Stellen Sie auf der Seite Zertifikatspeicher sicher, dass Alle Zertifikate platzieren ausgewählt ist, und lesen Sie den Zertifikatspeicher: NTDS\Personal und dann auf Next.



- Auf dem Certificate Import Wizard Vervollständigungsbildschirm, klicken Sie auf Finish. Daraufhin wird die Meldung angezeigt, dass der Import erfolgreich war. Klicken Sie auf OK. Es wird angezeigt, dass das Zertifikat unter dem Zertifikatspeicher importiert wurde: NTDS\Personal.



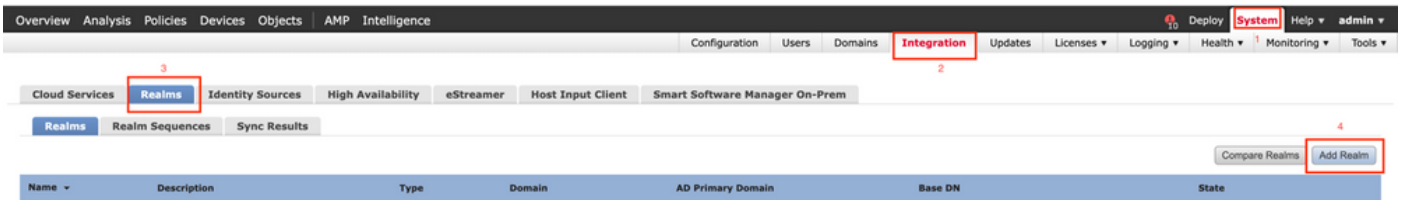
FMC-Konfigurationen

Lizenzierung überprüfen

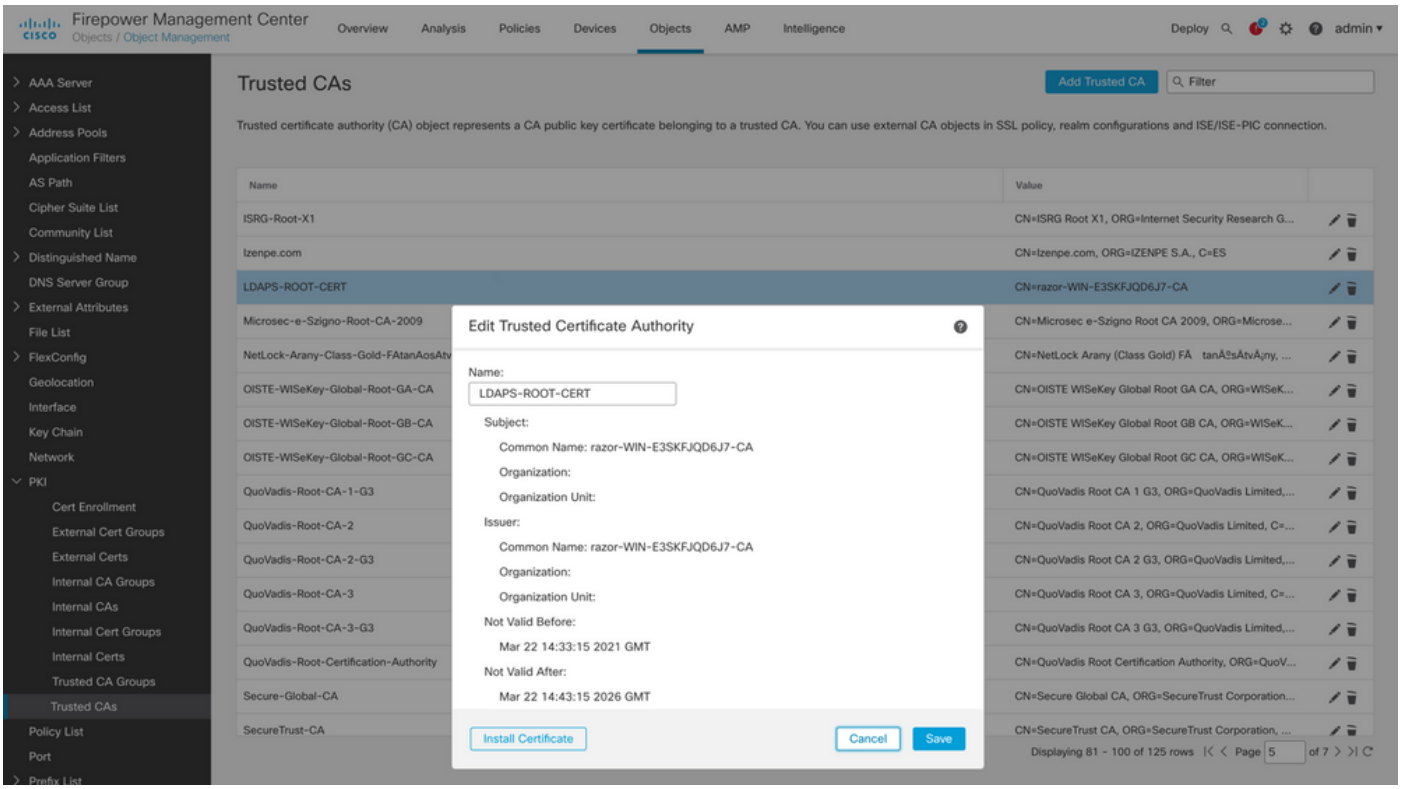
Um die AnyConnect-Konfiguration bereitzustellen, muss der FTD beim Smart Licensing-Server registriert sein und eine gültige Plus-, Apex- oder VPN Only-Lizenz auf das Gerät angewendet werden.

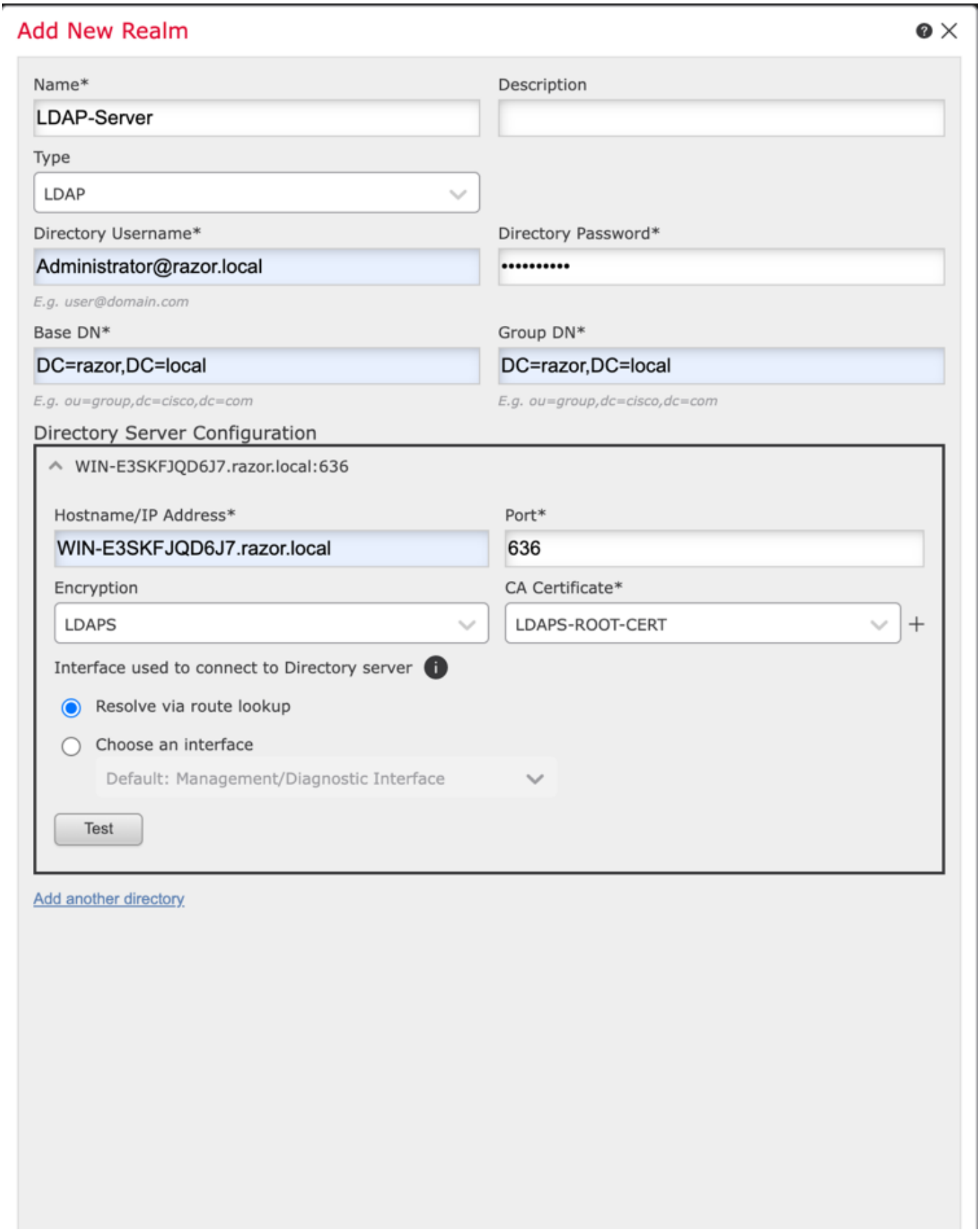
Setup-Bereich

1. Navigieren Sie zu System > Integration. Navigieren Sie zu Realms, und klicken Sie dann auf Add Realm, wie in diesem Bild gezeigt:



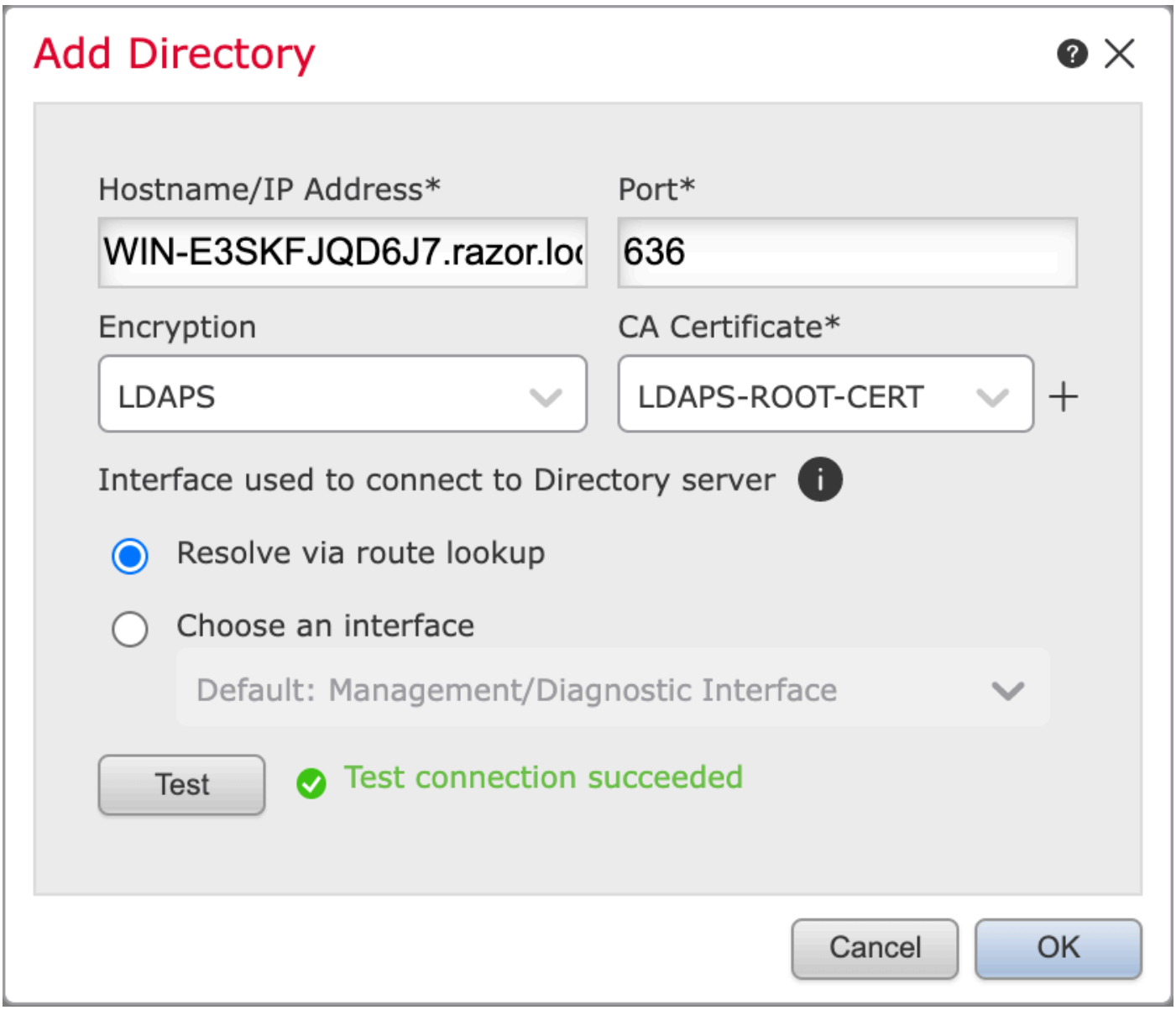
2. Füllen Sie die angezeigten Felder basierend auf den Informationen aus, die vom Microsoft-Server für LDAPs erfasst wurden. Importieren Sie zuvor das Zertifikat der Stammzertifizierungsstelle, das das LDAP-Dienstzertifikat auf dem Windows Server signiert hat unter Objects > PKI > Trusted CAs > Add Trusted CA, wie dies imDirectory Server Configuration des Bereichs. Klicken Sie abschließend auf 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

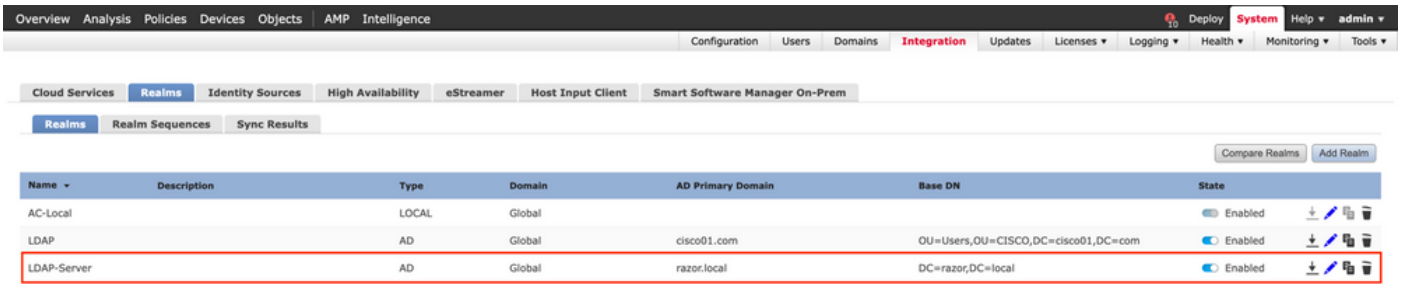


3. Klicken Sie auf Test um sicherzustellen, dass FMC eine erfolgreiche Bindung mit dem im vorherigen Schritt angegebenen Benutzernamen und Kennwort für das Verzeichnis herstellen kann. Da diese Tests vom FMC und nicht über eine der im FTD konfigurierten routingfähigen Schnittstellen (z. B. intern, extern, dmz) initiiert werden, garantiert eine

erfolgreiche (oder fehlgeschlagene) Verbindung nicht dasselbe Ergebnis für die AnyConnect-Authentifizierung, da AnyConnect LDAP-Authentifizierungsanforderungen von einer der FTD-routingfähigen Schnittstellen initiiert werden.



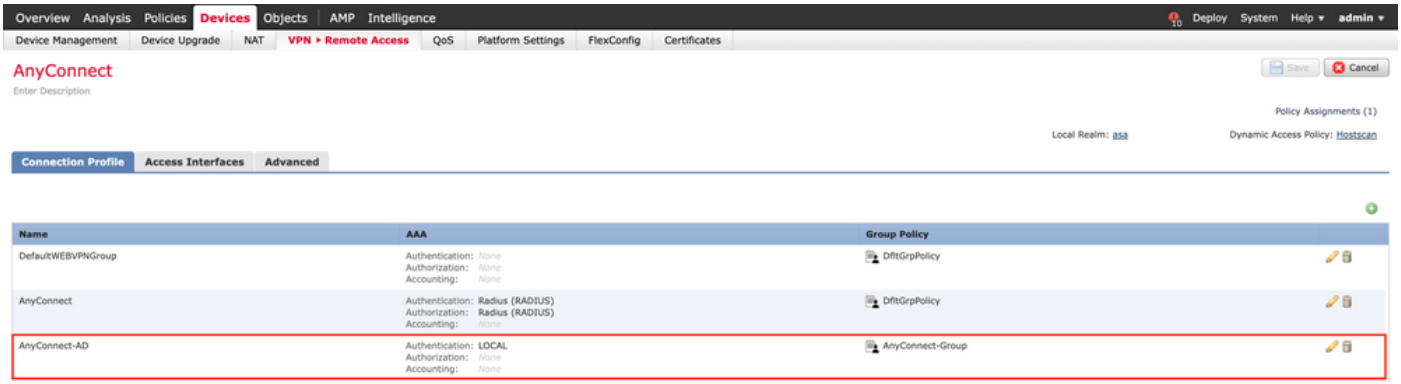
4. Aktivieren des neuen Bereichs.



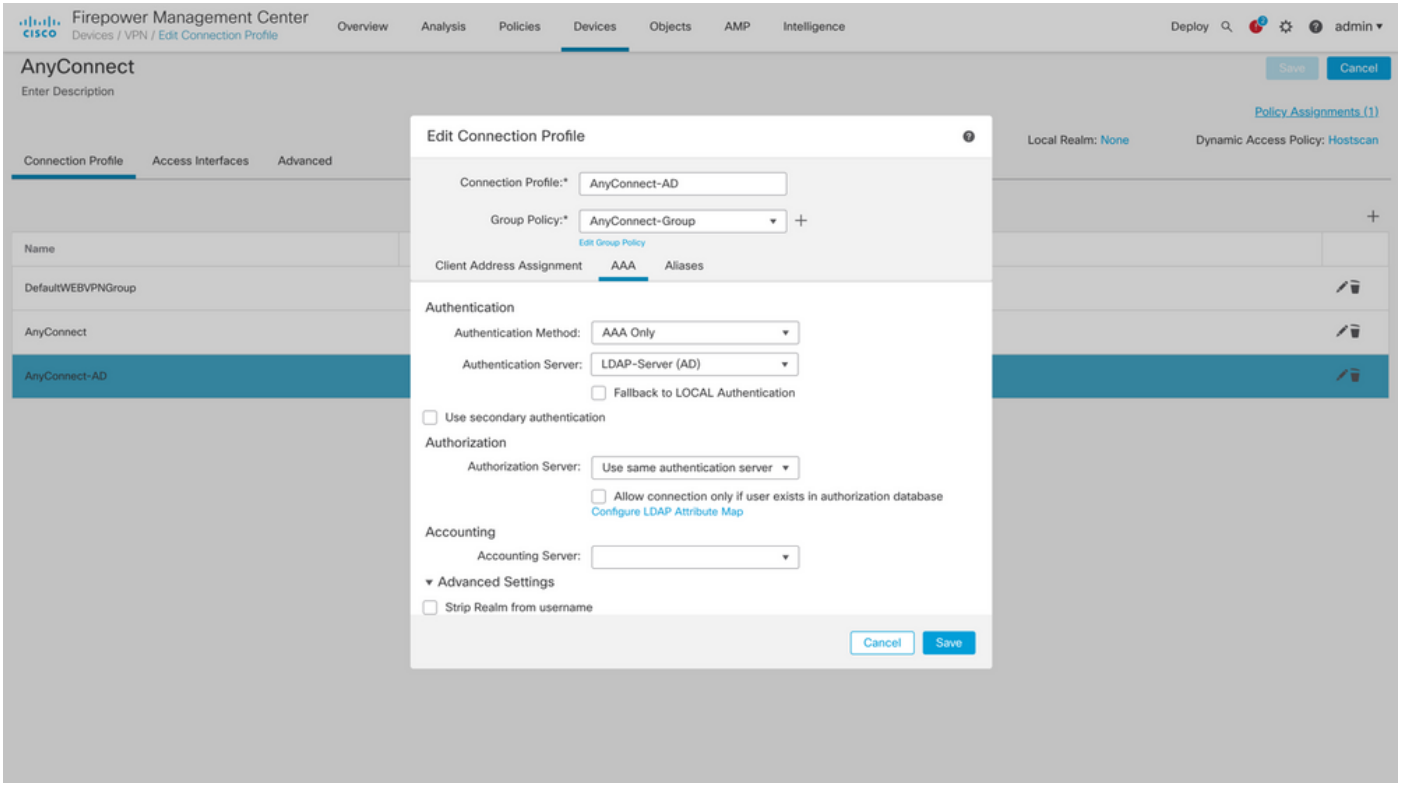
AnyConnect für die Passwortverwaltung konfigurieren

1. Wählen Sie das vorhandene Verbindungsprofil aus, oder erstellen Sie ein neues, wenn es sich um eine Ersteinrichtung von AnyConnect handelt. Hier wird ein vorhandenes

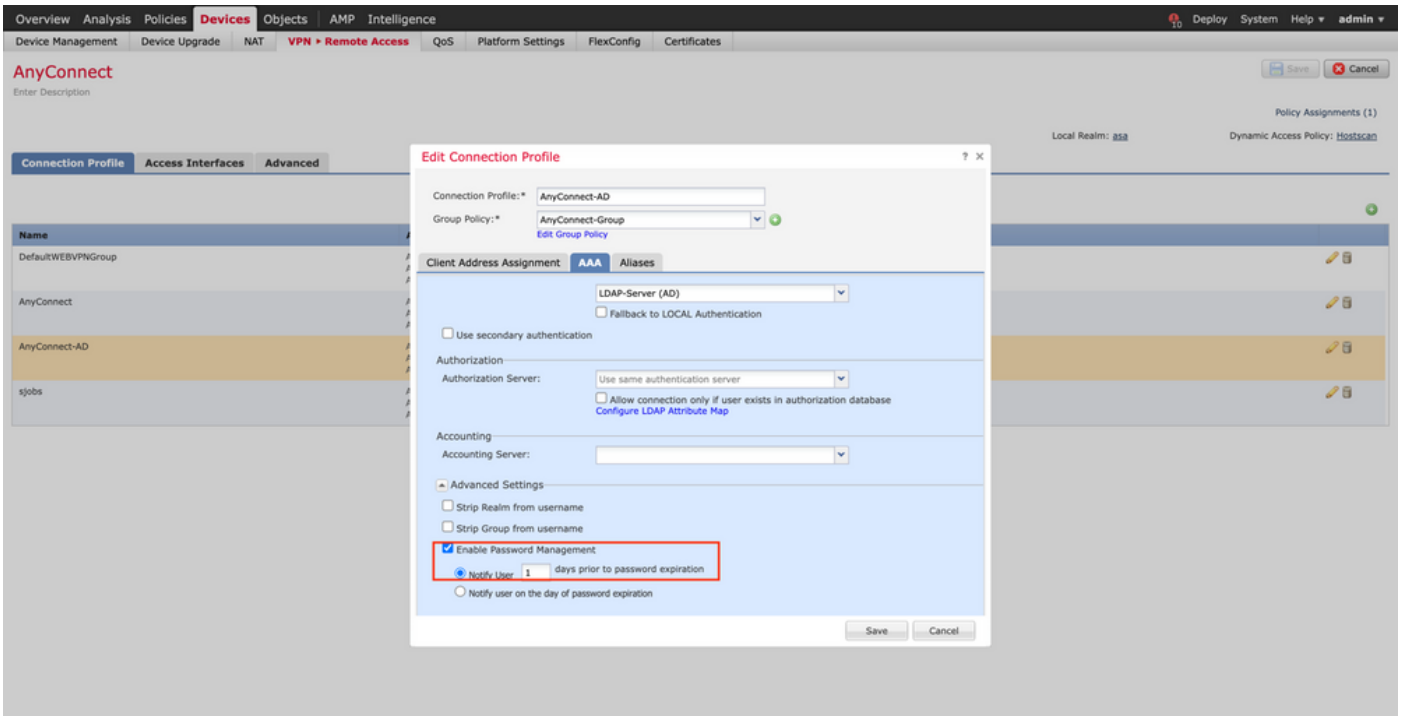
Verbindungsprofil mit dem Namen "AnyConnect-AD" verwendet, das der lokalen Authentifizierung zugeordnet ist.



2. Bearbeiten Sie das Verbindungsprofil, und ordnen Sie den neuen LDAP-Server zu, der in den vorherigen Schritten unter den AAA-Einstellungen des Verbindungsprofils konfiguriert wurde. Klicken Sie abschließend auf Save in der rechten oberen Ecke.



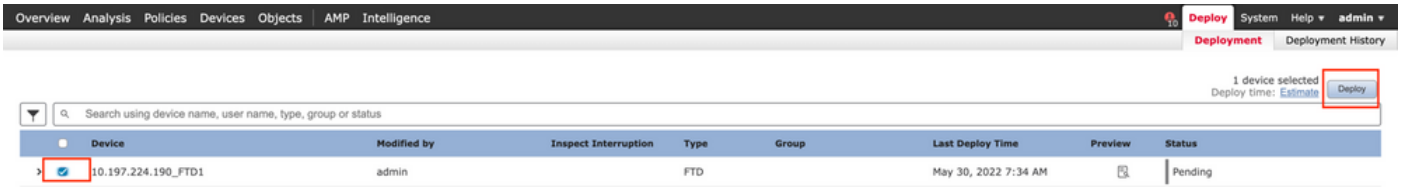
3. Passwortverwaltung unter dem AAA > Advanced Settings und speichert die Konfiguration.



Bereitstellung

1. Klicken Sie nach Abschluss der Konfiguration auf Deploy -Taste oben rechts.

2. Klicken Sie auf das Kontrollkästchen neben der FTD-Konfiguration, die darauf angewendet wurde, und klicken Sie dann auf Deploy, wie in diesem Bild gezeigt:



Abschließende Konfiguration

Dies ist die Konfiguration, die Sie nach der erfolgreichen Bereitstellung in der FTD-CLI sehen.

AAA-Konfiguration

<#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
```

AnyConnect-Konfiguration

<#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
```

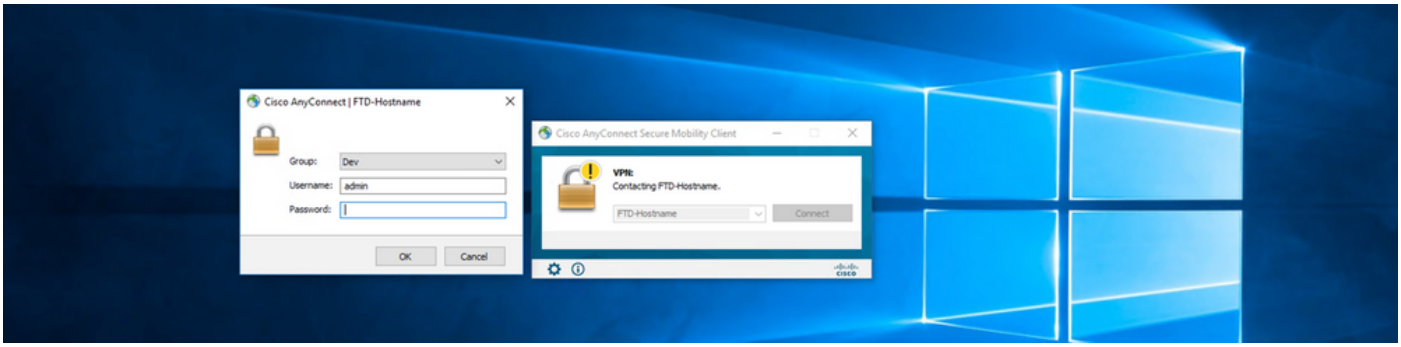
```
 default-domain none
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private 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
```

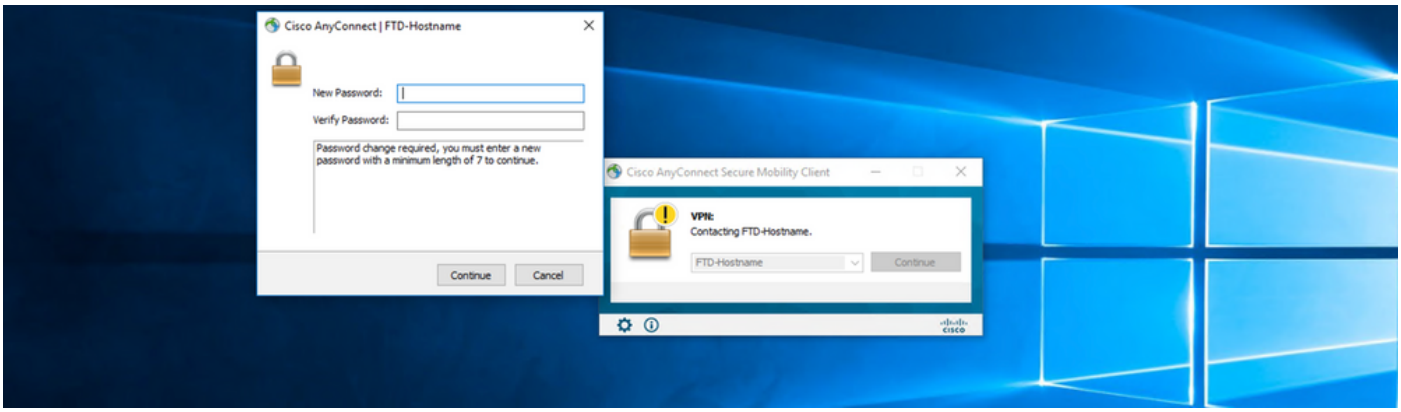
```
> show running-config ssl

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

Verifizierung

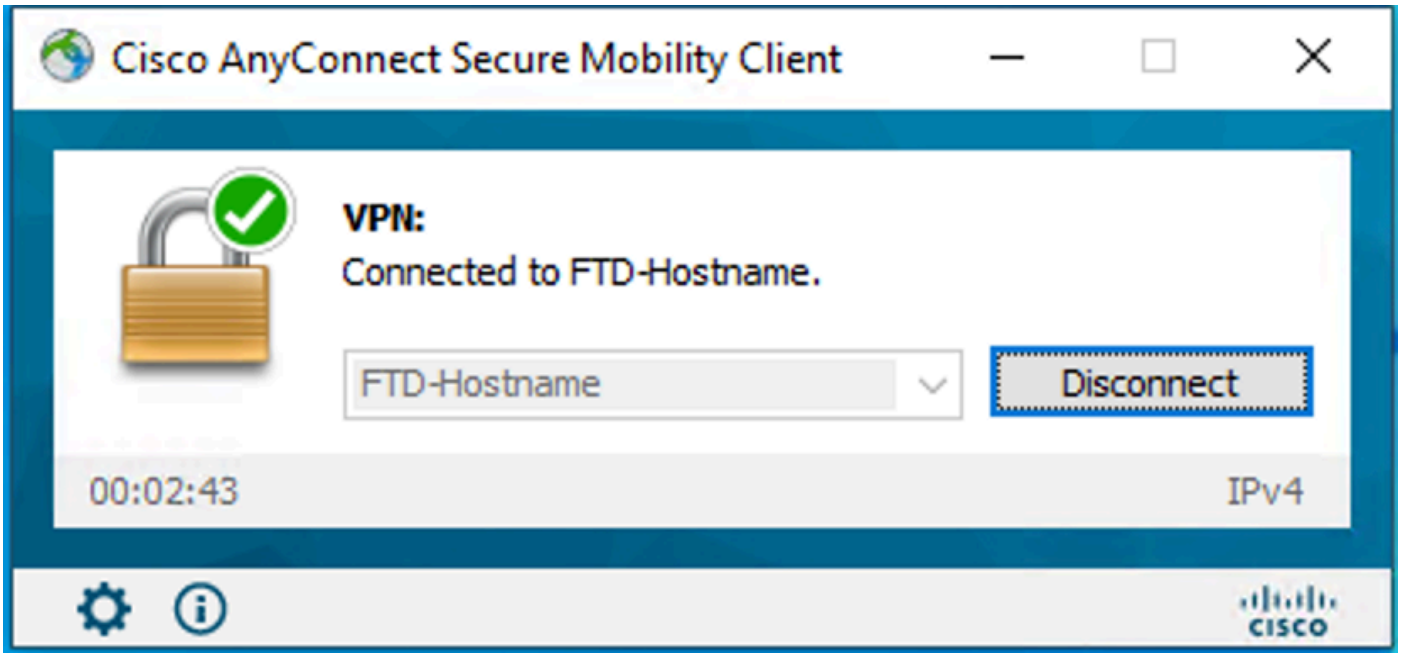
Stellen Sie eine Verbindung mit AnyConnect her, und überprüfen Sie den Kennwortverwaltungsprozess für die Benutzerverbindung.

1. Stellen Sie eine Verbindung mit dem betreffenden Verbindungsprofil her. Sobald bei der erstmaligen Anmeldung festgestellt wird, dass das Kennwort geändert werden muss, da das frühere Kennwort vom Microsoft Server nach Ablauf zurückgewiesen wurde, wird der Benutzer aufgefordert, das Kennwort zu ändern.





2. Sobald der Benutzer das neue Kennwort für die Anmeldung eingegeben hat, wird die Verbindung erfolgreich hergestellt.



3. Überprüfen Sie die Benutzerverbindung der 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
```

Fehlerbehebung

Fehlerbehebung

Dieses Debugging kann in der Diagnose-CLI ausgeführt werden, um Probleme im Zusammenhang mit der Kennwortverwaltung zu beheben: debug ldap 255.

Arbeiten mit Kennwortverwaltungsdebugs

<#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

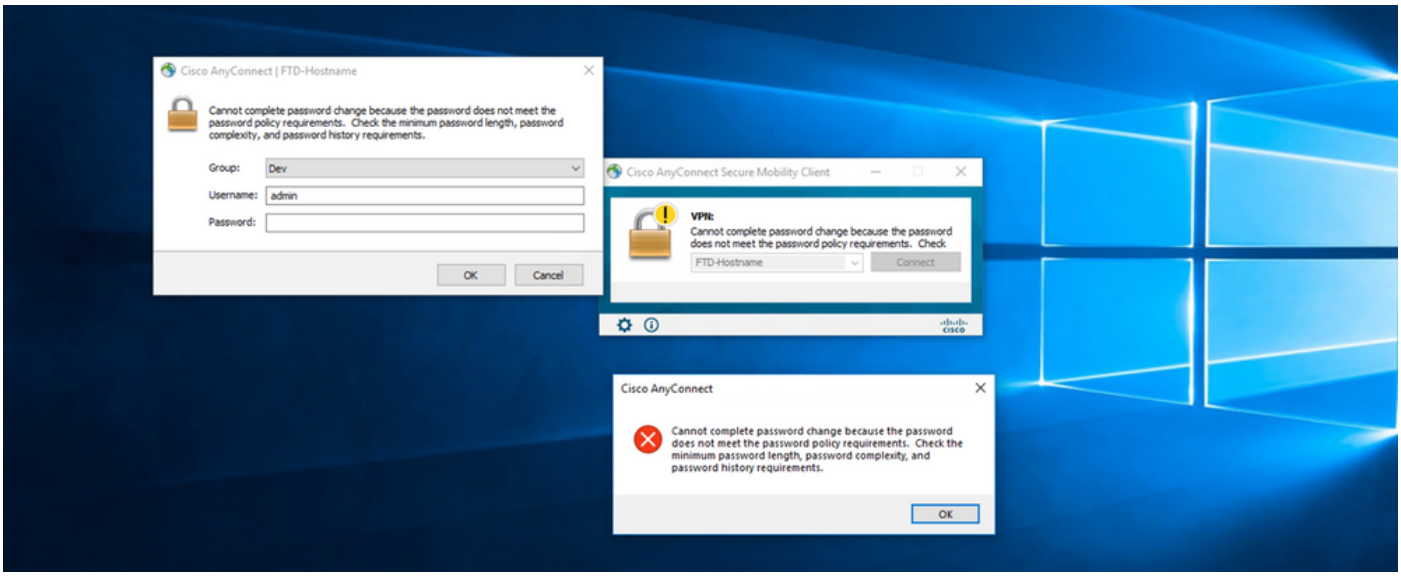
[25] instanceType: value = 4

[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
```

Häufige Fehler bei der Kennwortverwaltung

Wenn die vom Microsoft Server festgelegte Kennwortrichtlinie während der Bereitstellung des neuen Kennworts durch den Benutzer nicht erfüllt wird, wird die Verbindung in der Regel mit der Fehlermeldung "Kennwort erfüllt nicht die Anforderungen der Kennwortrichtlinie" beendet. Stellen Sie daher sicher, dass das neue Kennwort der vom Microsoft Server für LDAPs festgelegten Richtlinie entspricht.



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.