Configure Password Management Using LDAPs for RA VPN on FTD Managed by FMC

Contents

Introduction

This document describes configuring Password Management using LDAPs for AnyConnect Clients connecting to Cisco Firepower Threat Défense (FTD).

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- Basic knowledge of RA VPN (Remote Access Virtual Private Network) configuration on FMC
- Basic knowledge of LDAP server configuration on FMC
- Basic knowledge of Active Directory

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configuration

Network Diagram and Scenario

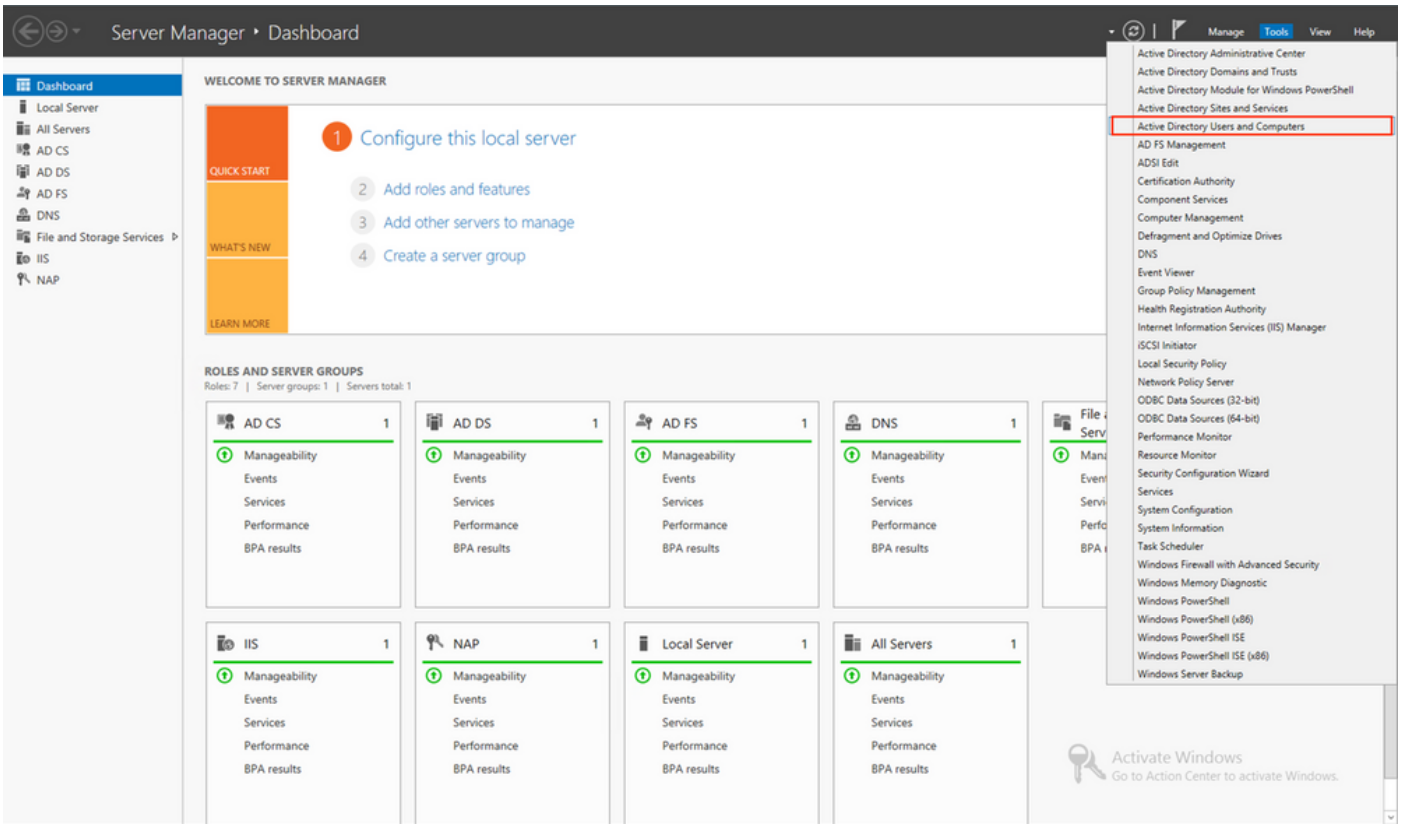
Windows server is pre-configured with ADDS and ADCS in order to test the user password-management process. In this configuration guide, these user accounts are created.

User Accounts:

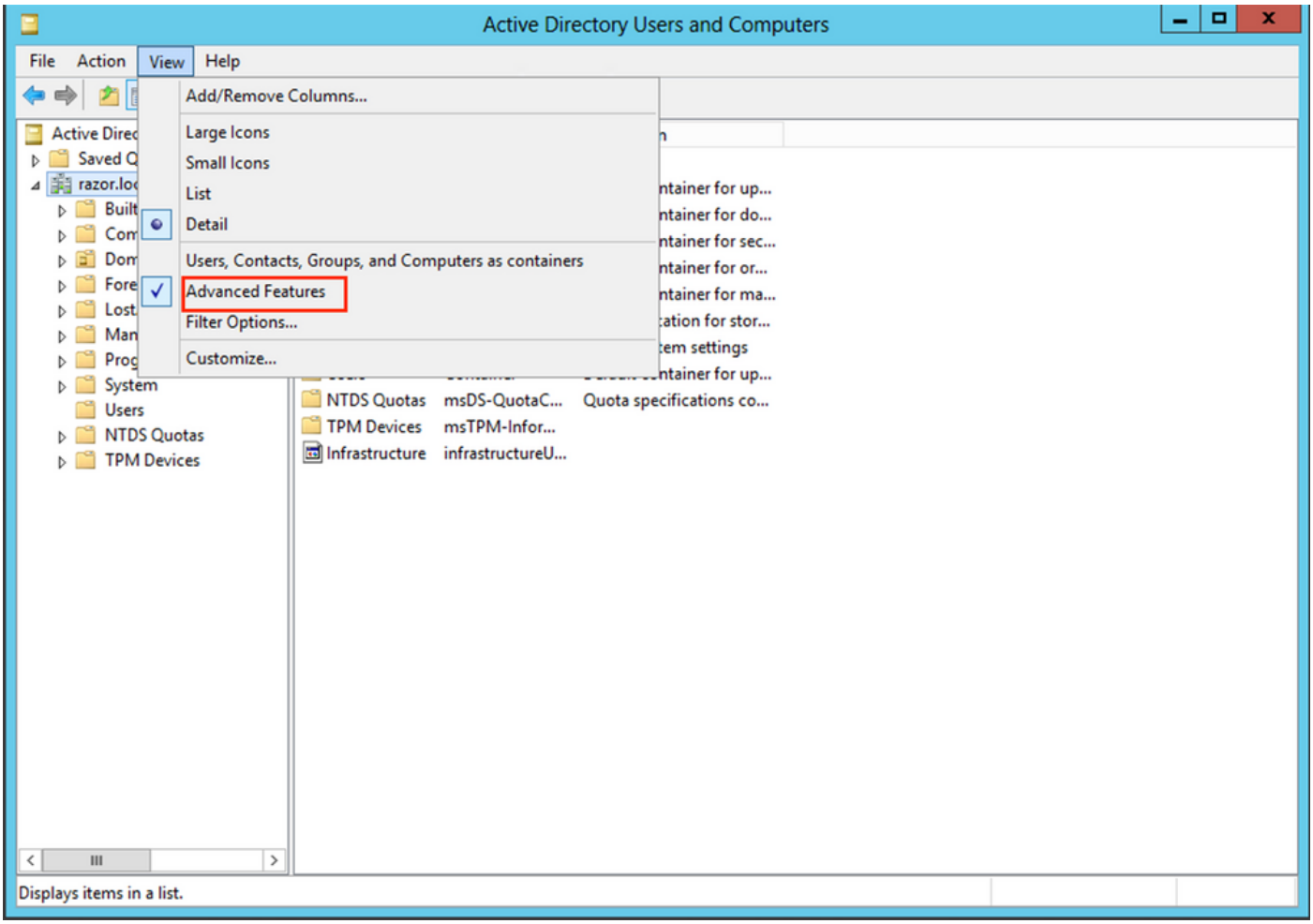
- Administrator: This is used as the directory account in order to allow the FTD to bind to the Active Directory server.
- admin: A test administrator account used to demonstrate user identity.

Determine LDAP Base DN and Group DN

1. Open Active Directory Users and Computers through the Server Manager Dashboard.

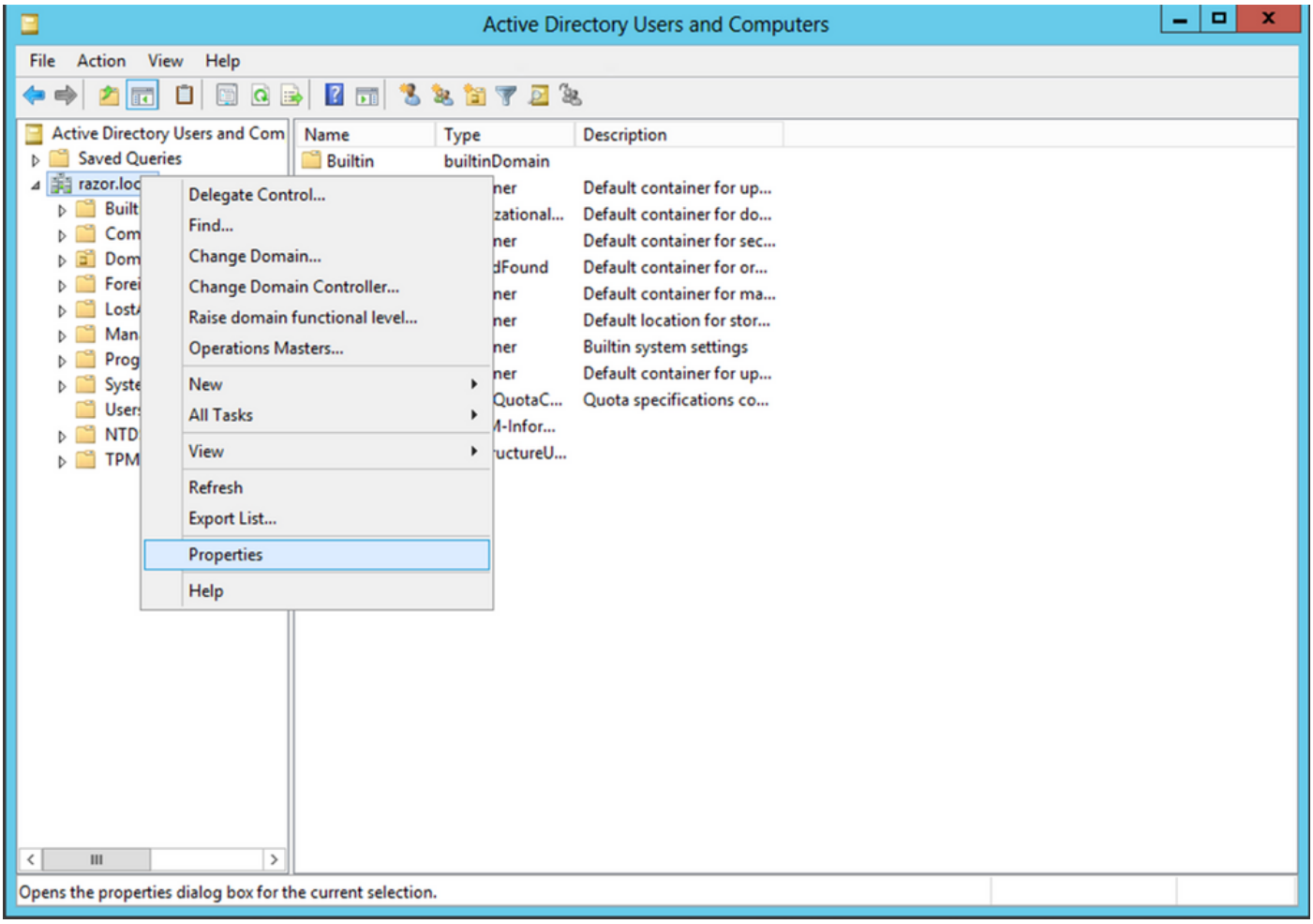


2. Open the View Option on the top panel, and enable the Advanced Features, as shown in the image:



3. This allows the view of additional properties under the AD objects.

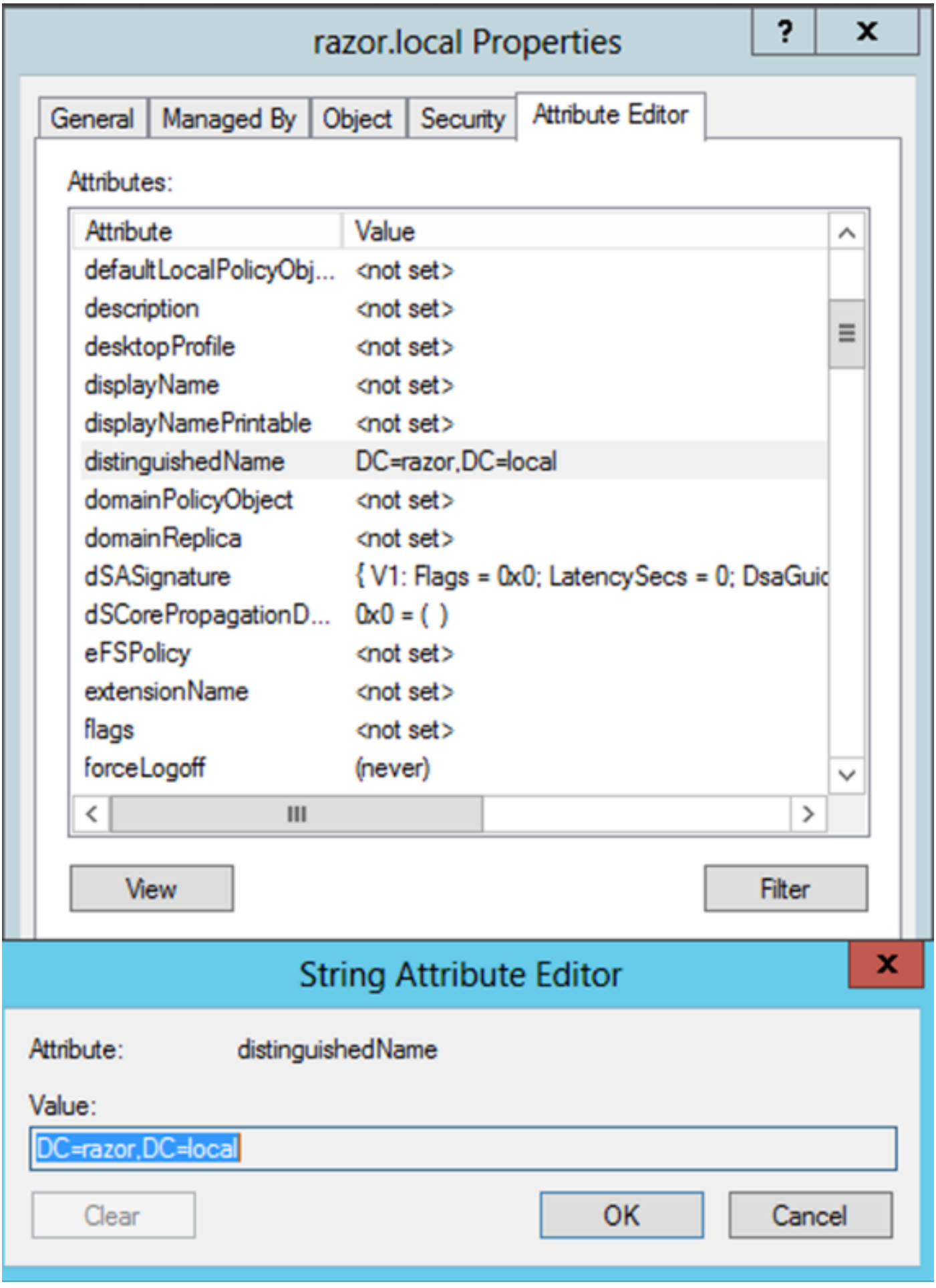
For example, in order to find the DN for the root razor.local, right-click razor.local, and then choose Properties, as shown in this image:



4. Under Properties, choose the Attribute Editor tab. Find distinguishedName under the Attributes, then click View, as shown in the image.

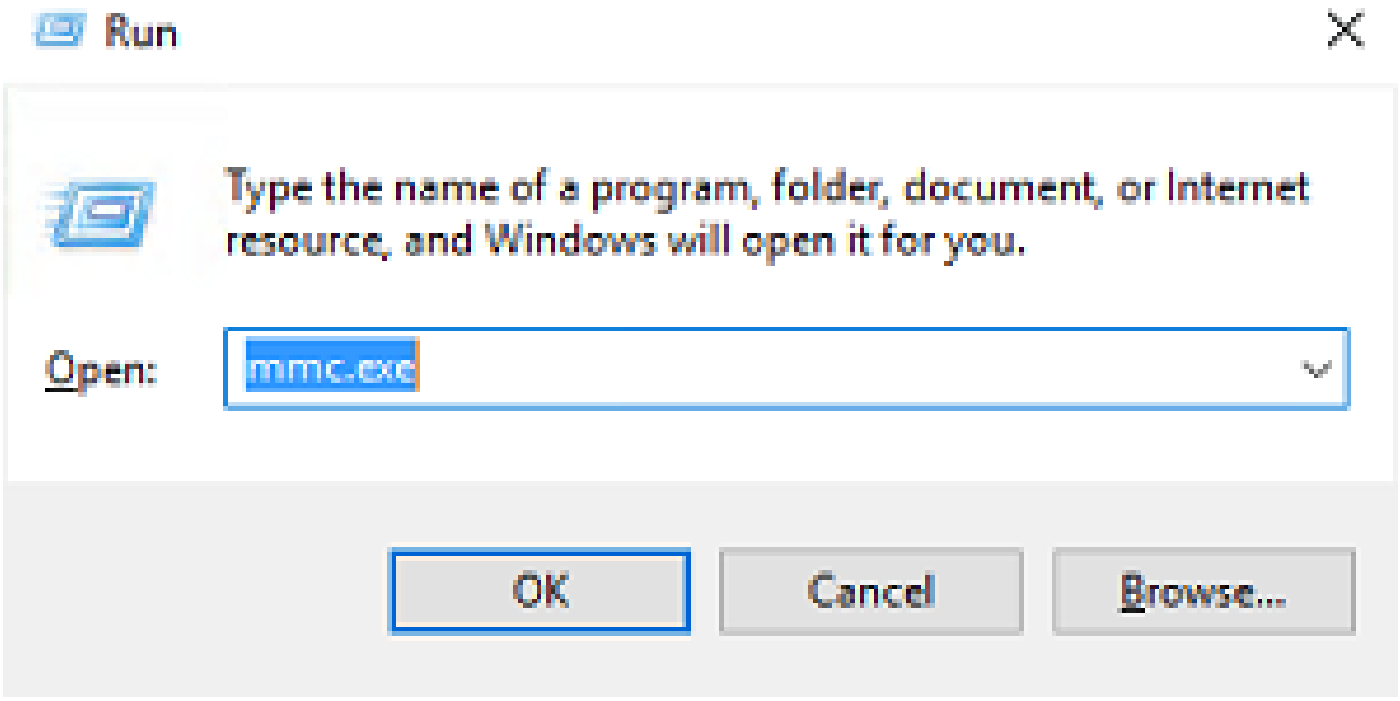
This opens a new window where the DN can be copied and pasted into FMC later.

In this example, the root DN is DC=razor, DC=local. Copy the value and save it for later. Click OK in order to exit the String Attribute Editor window and click OK again in order to exit the Properties.

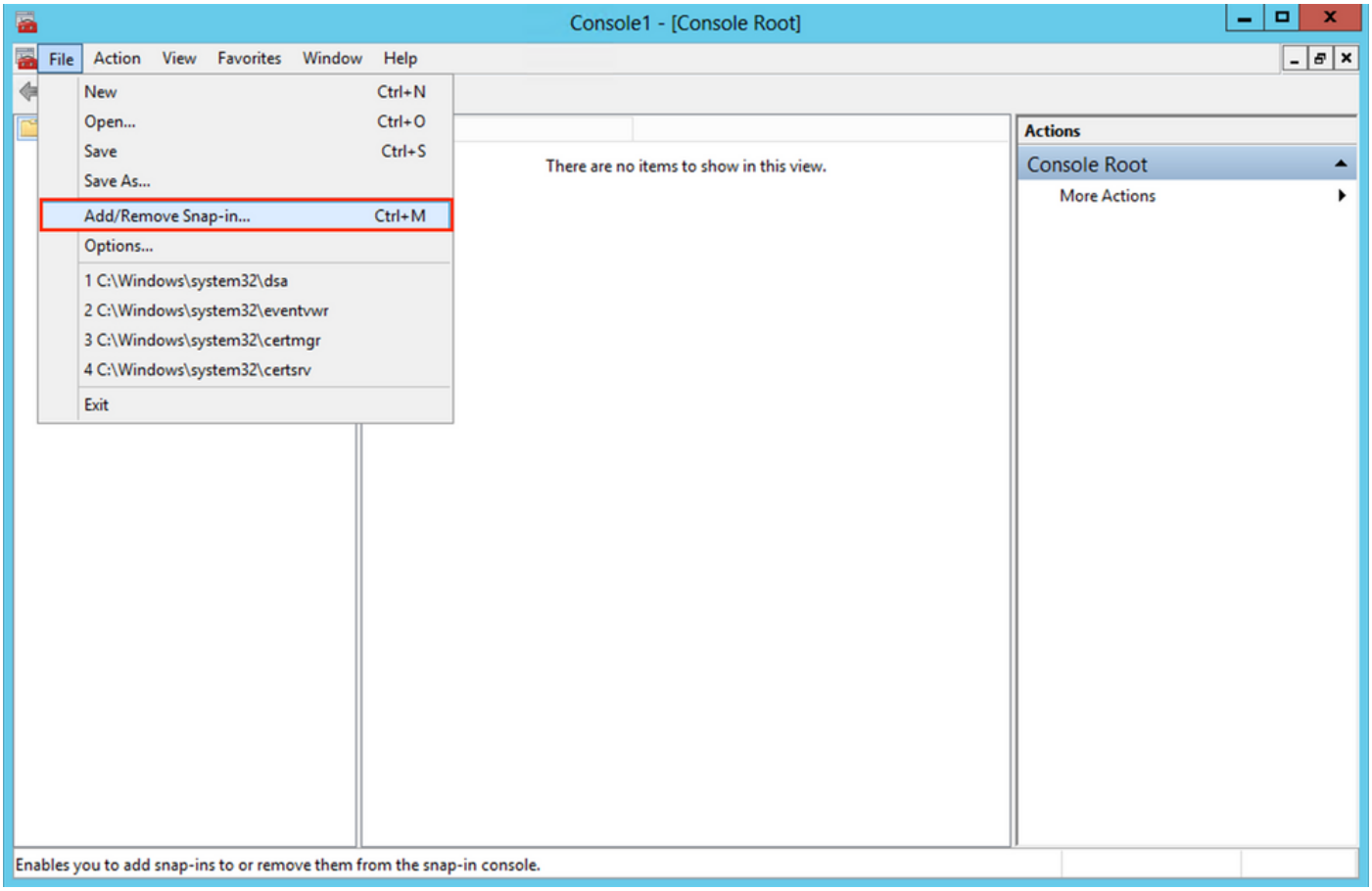

razor.local Properties
General
Managed By
Object
Security
Attribute Editor
Attributes:
Attribute
Value
defaultLocalPolicyObj...
<not set>
description
<not set>
desktopProfile
<not set>
displayName
<not set>
displayNamePrintable
<not set>
distinguishedName
DC=razor,DC=local
domainPolicyObject
<not set>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

Copy the LDAPS SSL Certificate Root

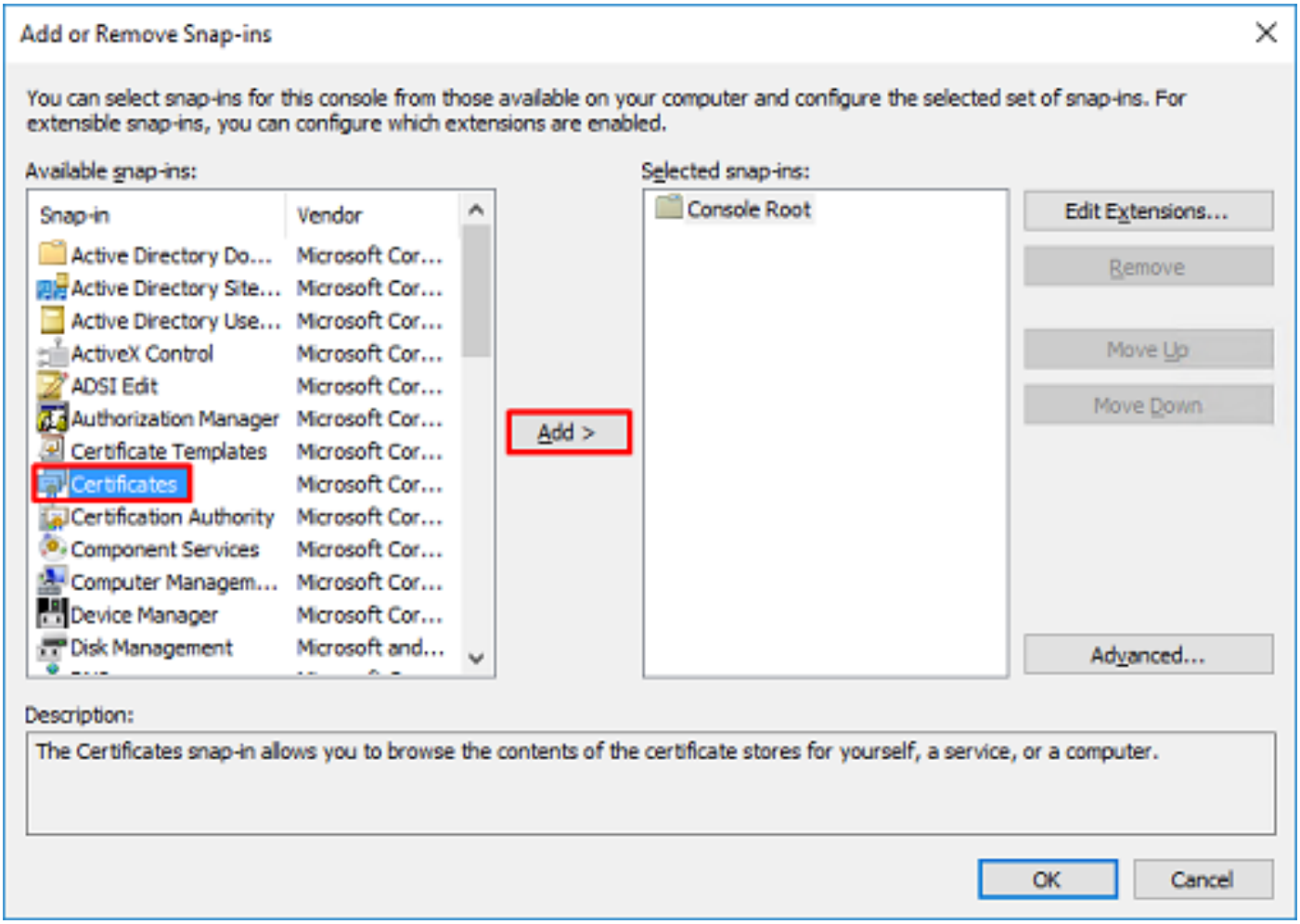
1. Press Win+R and enter mmc.exe, then click OK, as shown in this image.



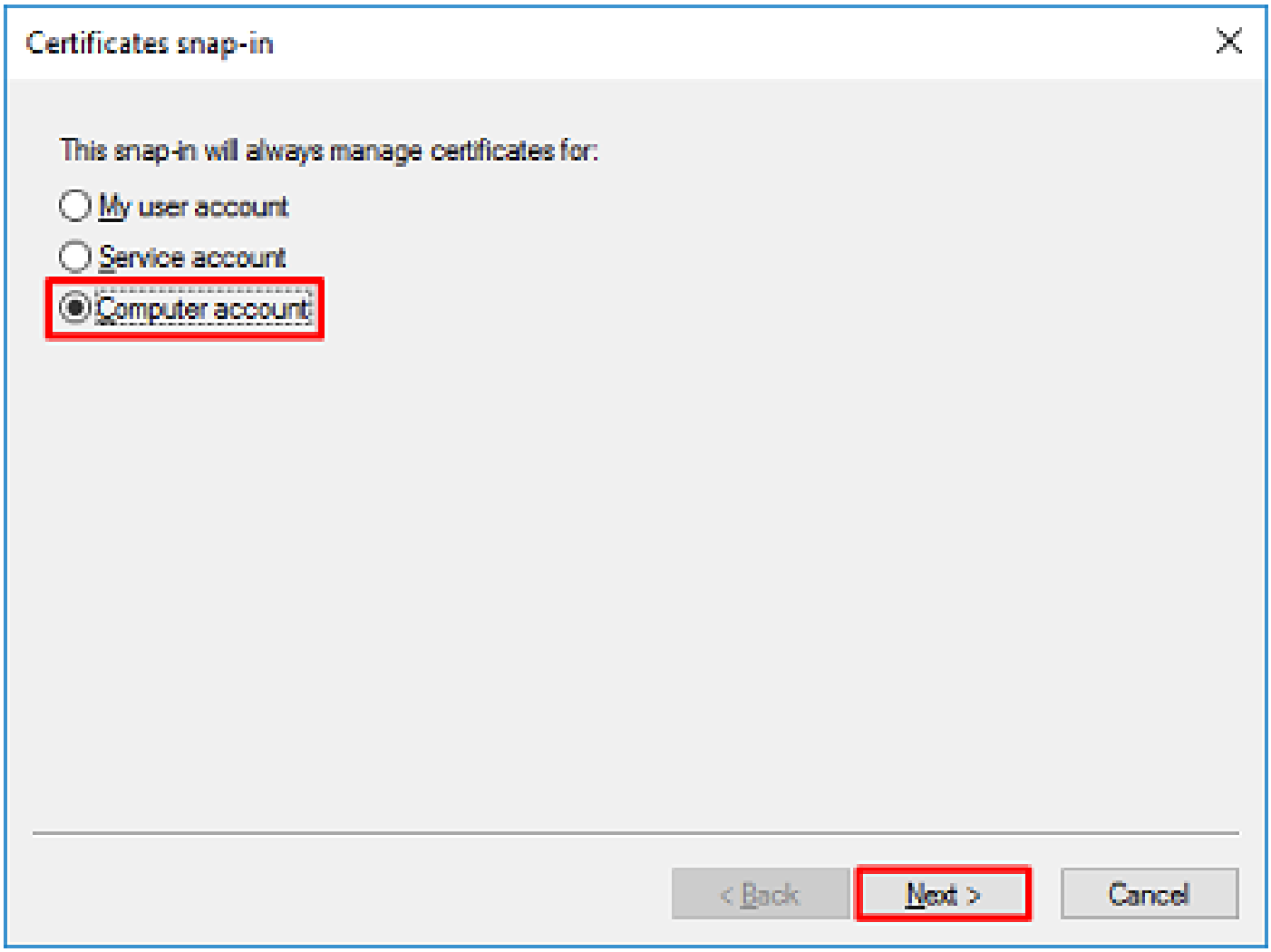
2. Navigate to File > Add/Remove Snap-in..., ss shown in this image:



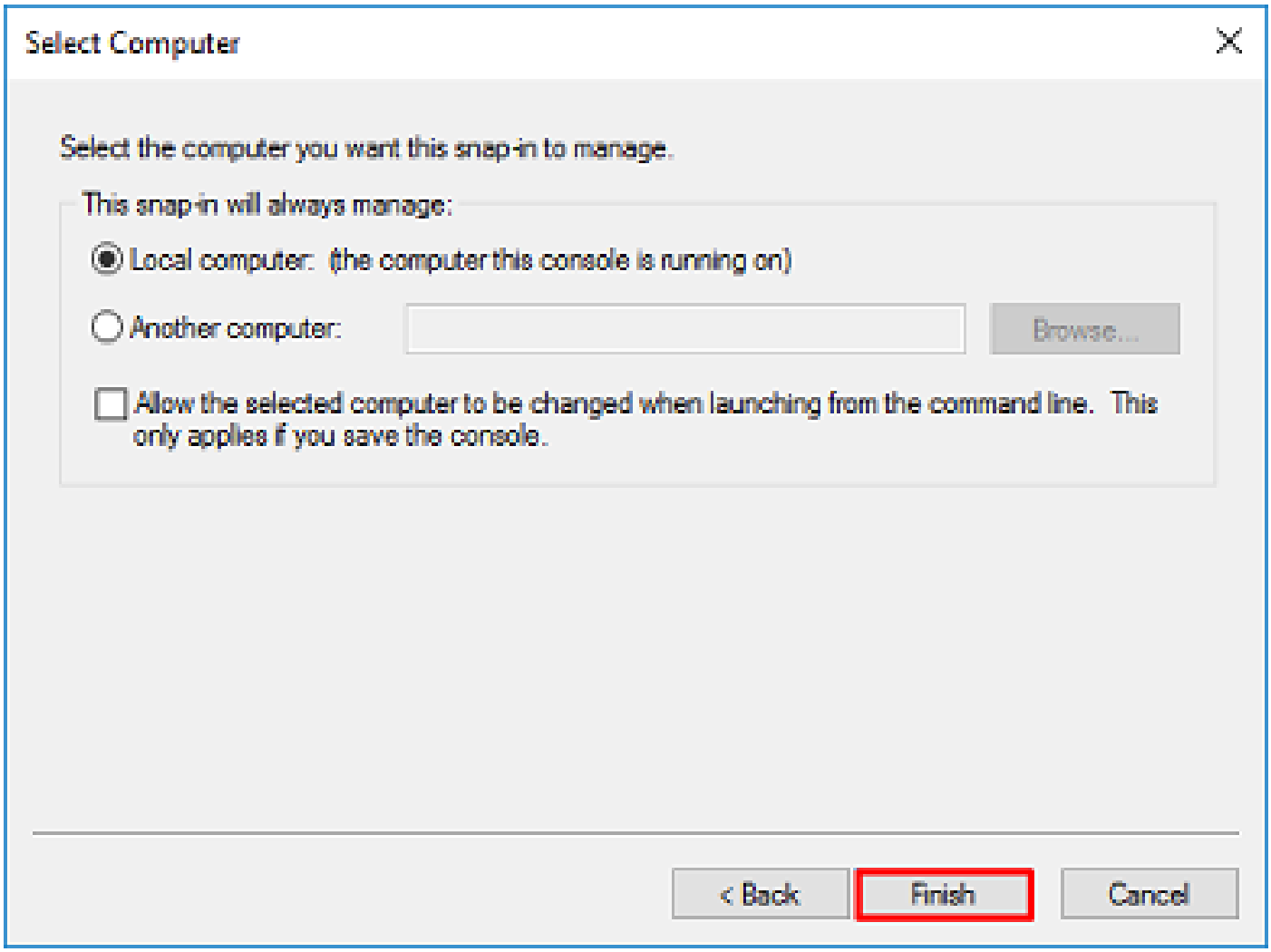
3. Under available snap-ins, choose Certificates and then click Add, as shown in this image:



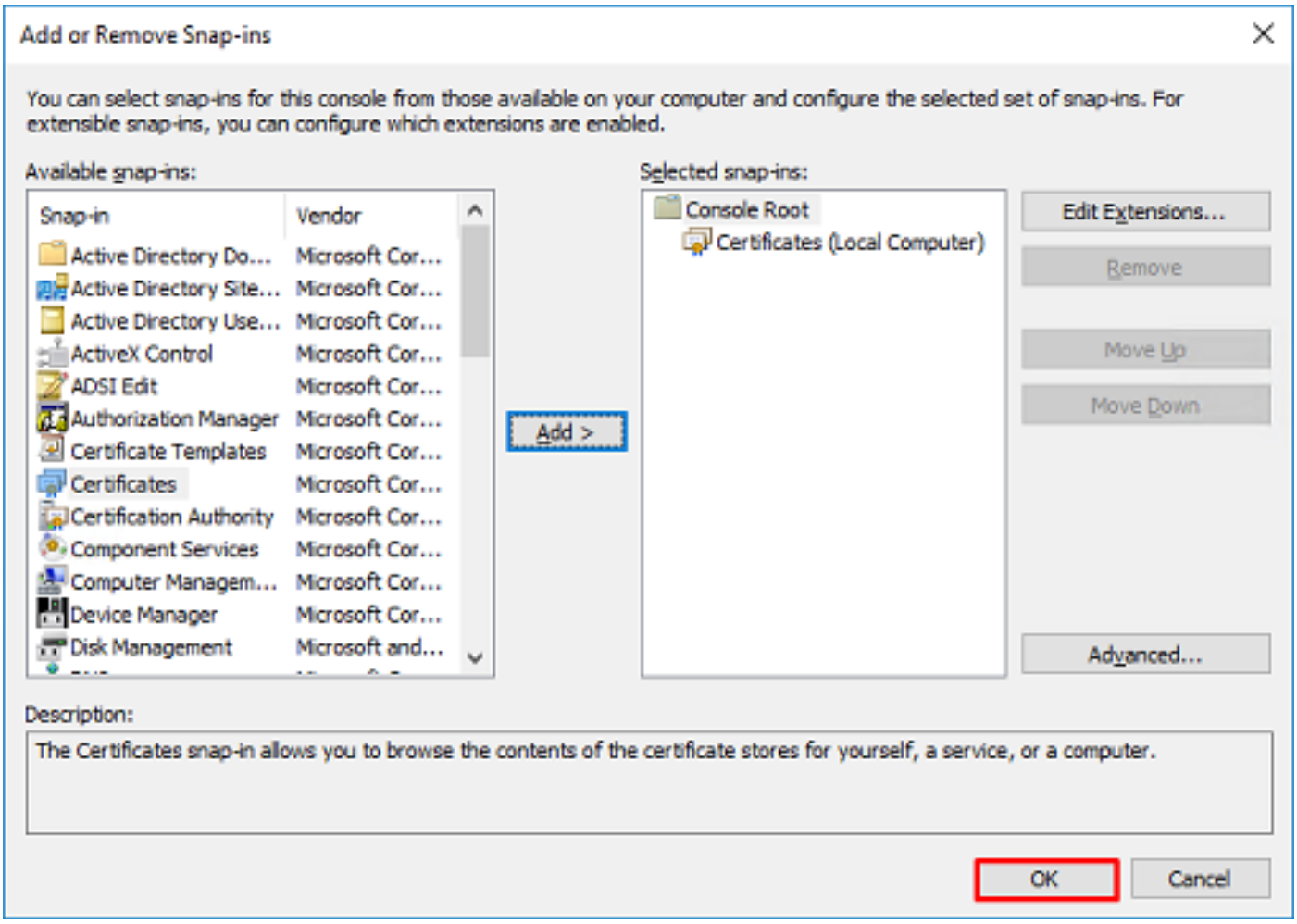
4. Choose Computer account and then click Next, as shown in this image:



As shown here, click Finish.



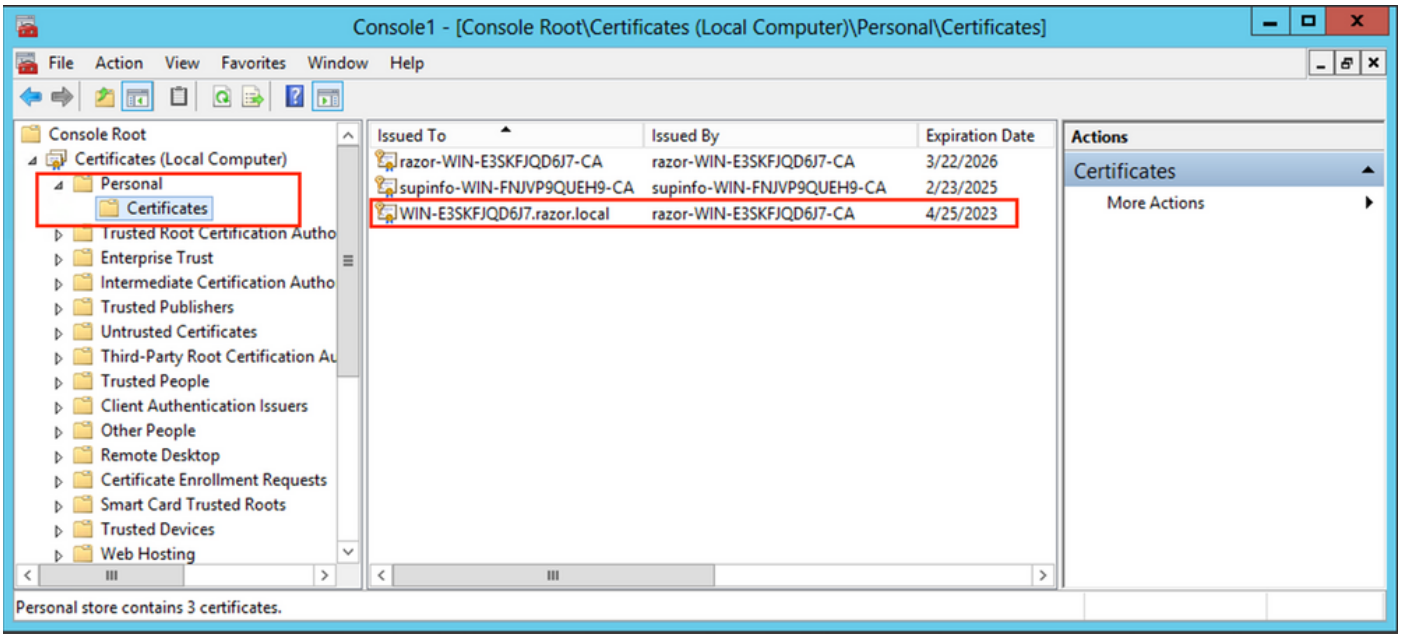
5. Now, click OK, as shown in this image.



6. Expand the Personal folder, then click Certificates. The certificate used by LDAPs must be issued to the Fully Qualified Domain Name (FQDN) of the Windows server. On this server, there are three certificates listed:

- A CA Certificate was issued to and by razor-WIN-E3SKFJQD6J7-CA.
- A CA Certificate issued to and by supinfo-WIN-FNJVP9QUEH9-CA.
- An identity certificate was issued to WIN-E3SKFJQD6J7.razor.local by razor-WIN-E3SKFJQD6J7-CA.

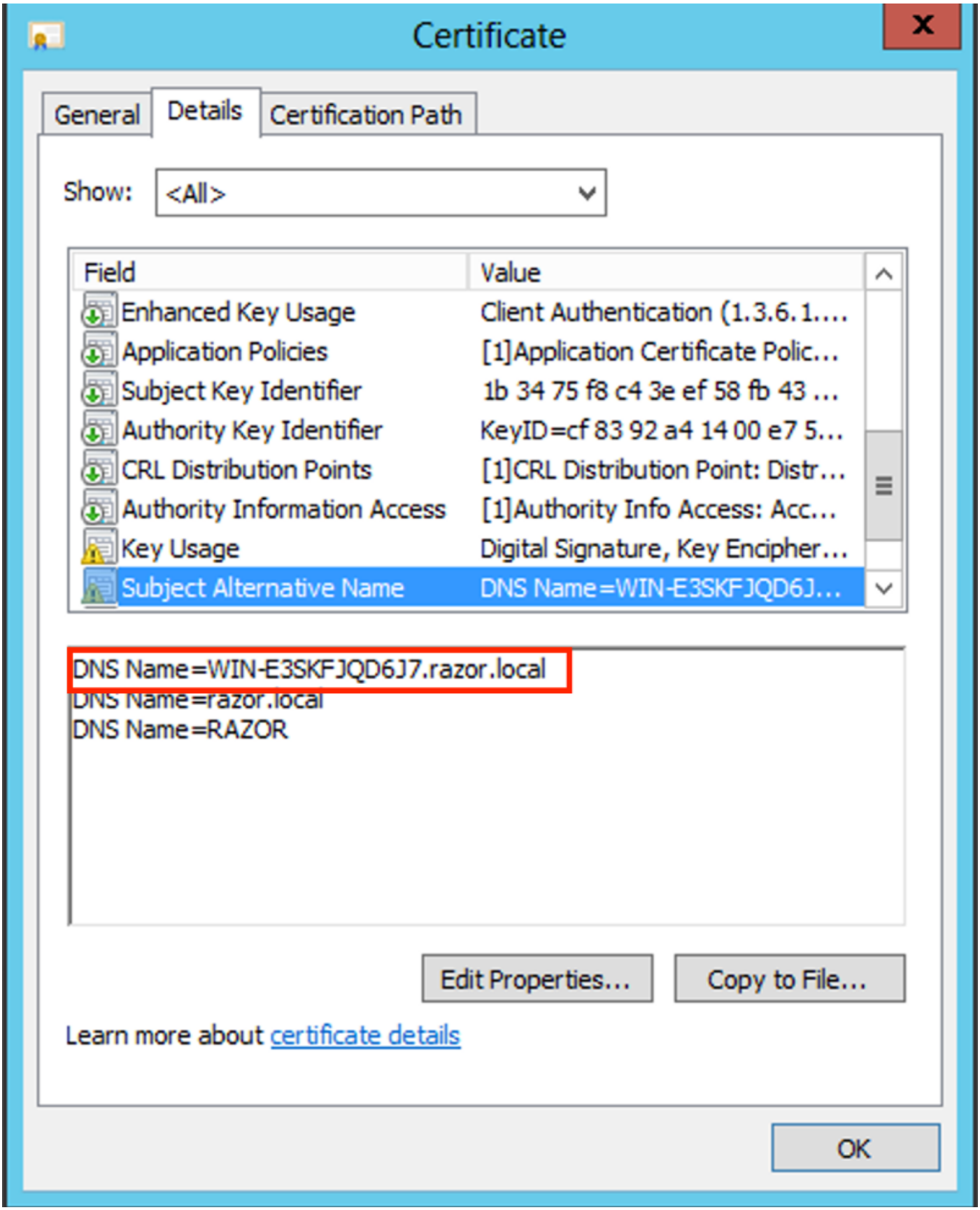
In this configuration guide, the FQDN is WIN-E3SKFJQD6J7.razor.local and so the first two certificates are not valid for use as the LDAPs SSL certificate. The identity certificate issued to WIN-E3SKFJQD6J7.razor.local is a certificate that was automatically issued by the Windows Server CA service. Double-click the certificate in order to check the details.



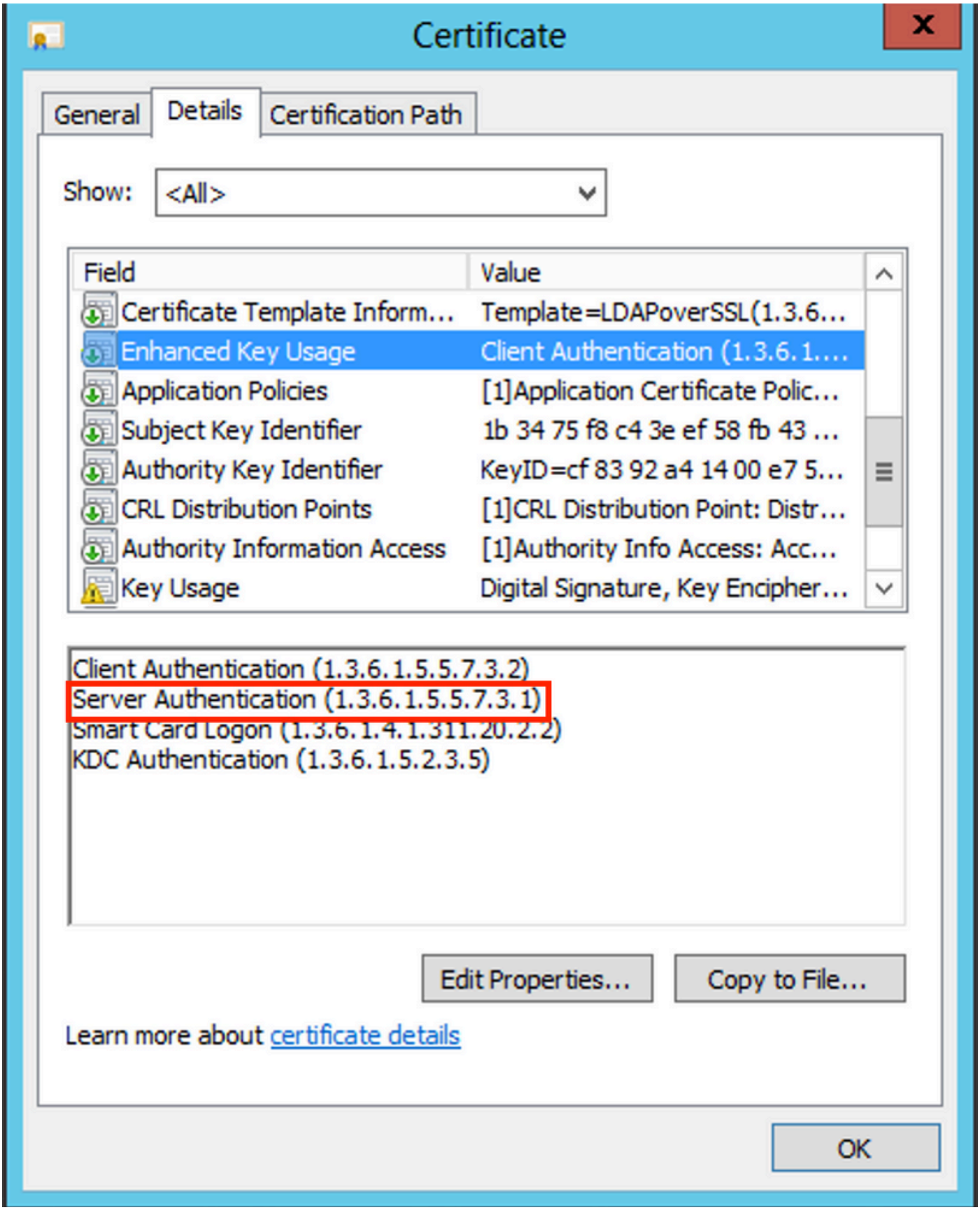
7. In order to be used as the LDAPs SSL Certificate, the certificate must meet these requirements:

- The common name or DNS Subject Alternate Name matches the FQDN of the Windows Server.
- The Certificate has Server Authentication under the Enhanced Key Usage field.

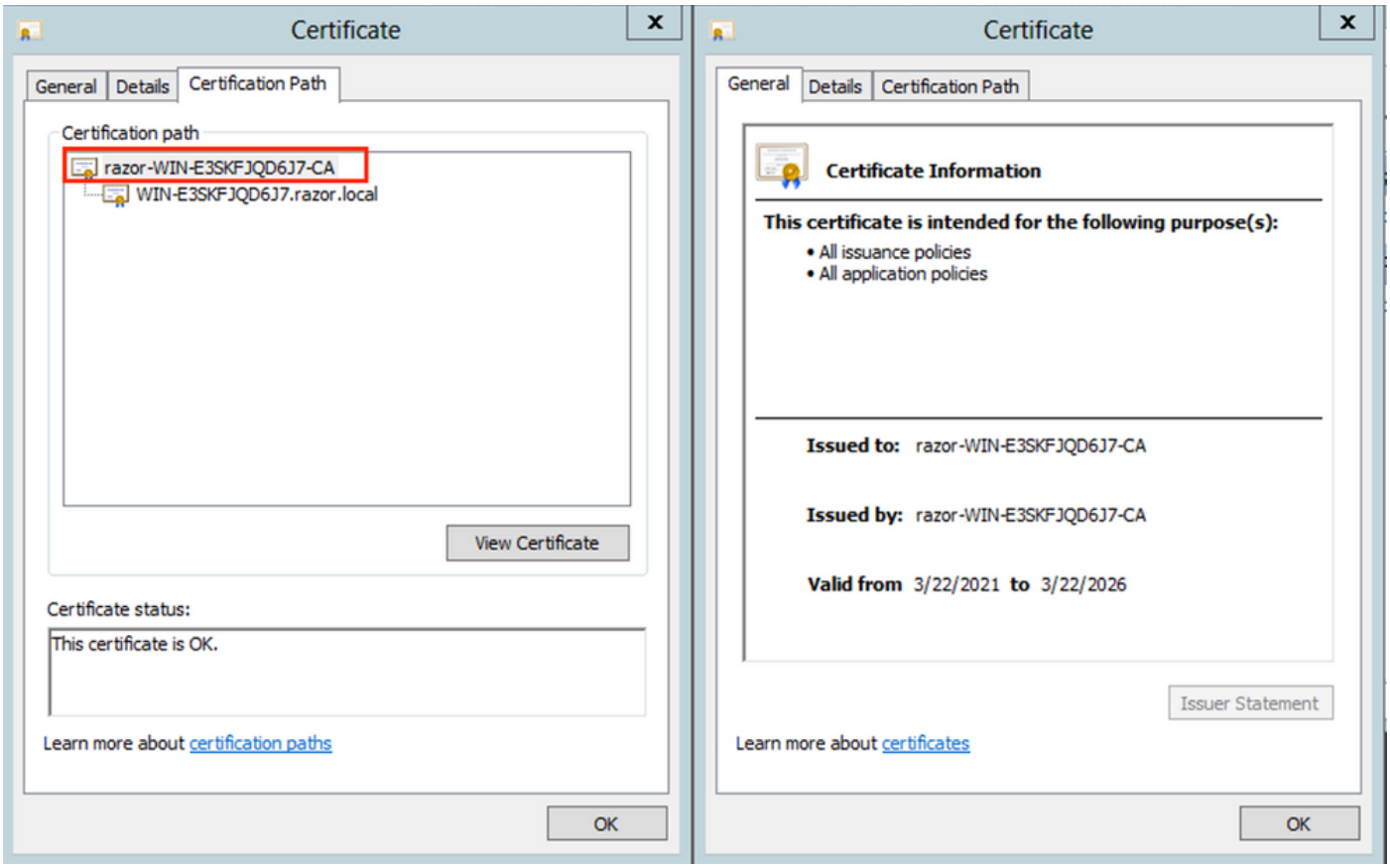
Under the Details tab for the certificate, choose Subject Alternative Name, where the FQDN WIN-E3SKFJQD6J7.razor.local is present.



Under Enhanced Key Usage, Server Authentication is present.

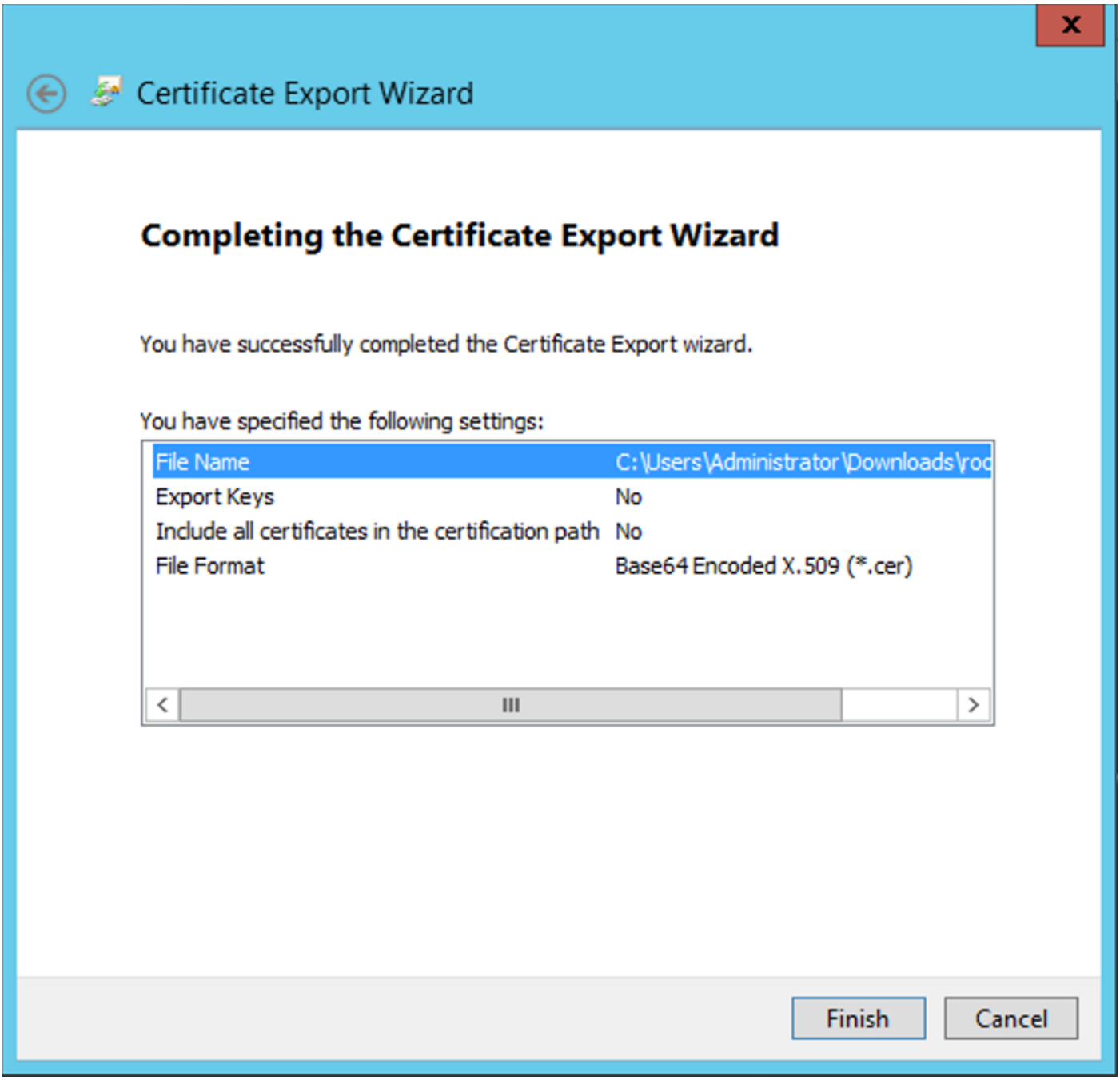


8. Once that is confirmed, under the Certification Path tab, choose the top-level certificate which is the root CA certificate, and then click View Certificate. This opens the certificate details for the root CA certificate as shown in the image:



9. Under the Details tab of the root CA certificate, click Copy to File and navigate through theCertificate Export Wizard which exports the root CA in PEM format.

Choose Base-64 encoded X.509 as the file format**.**



10. Open the Root CA certificate stored in the selected location on the machine with a notepad or some other text editor.

This shows the PEM format certificate. Save this for later.

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgo
vcjEhMB8GA1UEAxMYcmF6b3ItV0lOLUUzU0tGSlFENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCg
BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvc
CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnblxwtXOB2G4UxZ3LRrWznjXaSO2Rc3qVw4lnOAziGs4ZMNM1X8UWeKuwi8
9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU3OaiiI/tp422ydy3Kgl7Iqt1s4XqpZmTezykWra7dUyXfkuESk6lEOAV
CSkTQTRXYryy8dJrWjAF/n6A3VnS/l7Uhujlx4CD2OBkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwE
DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFM+DkqQUAOdY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSI
AA4IBAQCiSm5U7U6Y7zXdx+dleJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7BnO6f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q
4sMZffbVrGlRz7twWY36J5G5vhNUhzZ1N2OLw6wtHg2SO8XlvpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nrylb
GuDsepY7/u2uWfy/vpTJigeok2DH6HFfOET3sE+7rsIAY+of0kWW5gNwQ4hOwv4Goqj+YQRAXXi2OZyltHR1dfUUbwVENSFQtDnFA7X
-----END CERTIFICATE-----
```

In Case of Multiple Certificates Installed in the Local Machine Store on the LDAPs Server (Optional)

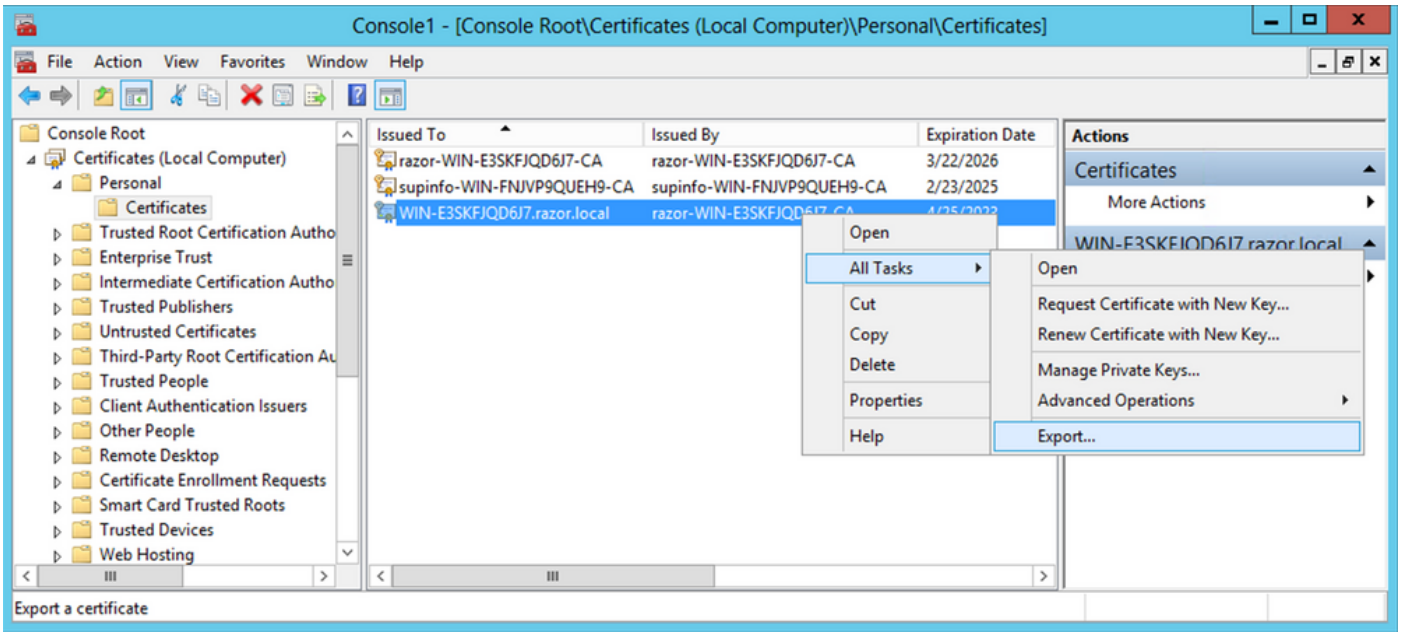
1. In a situation of multiple identity certificates that can be used by LDAPS and when there is uncertainty as to which is used, or there is no access to the LDAPS server, it is still possible to extract the root CA from a packet capture done on the FTD.

2. In the case where you have multiple certificates valid for Server Authentication in the LDAP server (such as AD DS domain controller) local computer certificate store, it can be noticed that a different certificate is used for LDAPS communications. The best resolution for such an issue is to remove all unnecessary certificates from the local computer certificate store and have only one certificate that is valid for server authentication.

However, if there is a legitimate reason that you require two or more certificates and have at least a Windows Server 2008 LDAP server, the Active Directory Domain Services (NTDS\Personal) certificate store can be used for LDAPs communications.

These steps demonstrate how to export an LDAPS-enabled certificate from a domain controller local computer certificate store to the Active Directory Domain Services service certificate store (NTDS\Personal).

- Navigate to the MMC console on the Active Directory Server, choose File, and then click Add/Remove Snap-in.
- Click Certificates and then click Add.
- In the Certificates snap-in, choose Computer account and then click Next.
- In Select Computer, choose Local Computer, click OK, and then click Finish. In Add or Remove Snap-ins, click OK.
- In the certificates console of a computer that contains a certificate used for Server Authentication, right-click the certificate, click All Tasks, and then click Export.

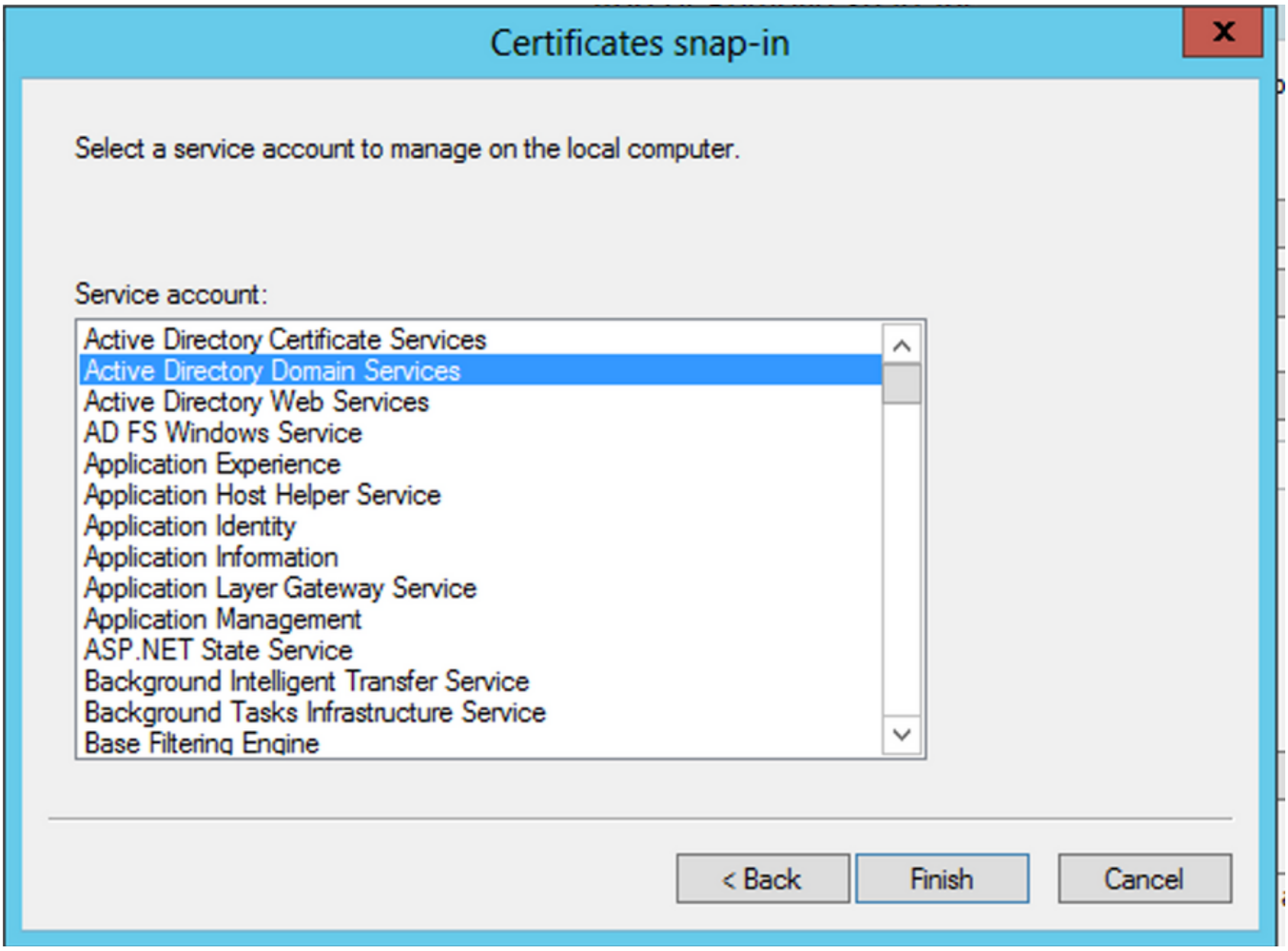


- Export the certificate in the pfx format in the subsequent sections. Reference this article on how to export a certificate in the pfx format from MMC:

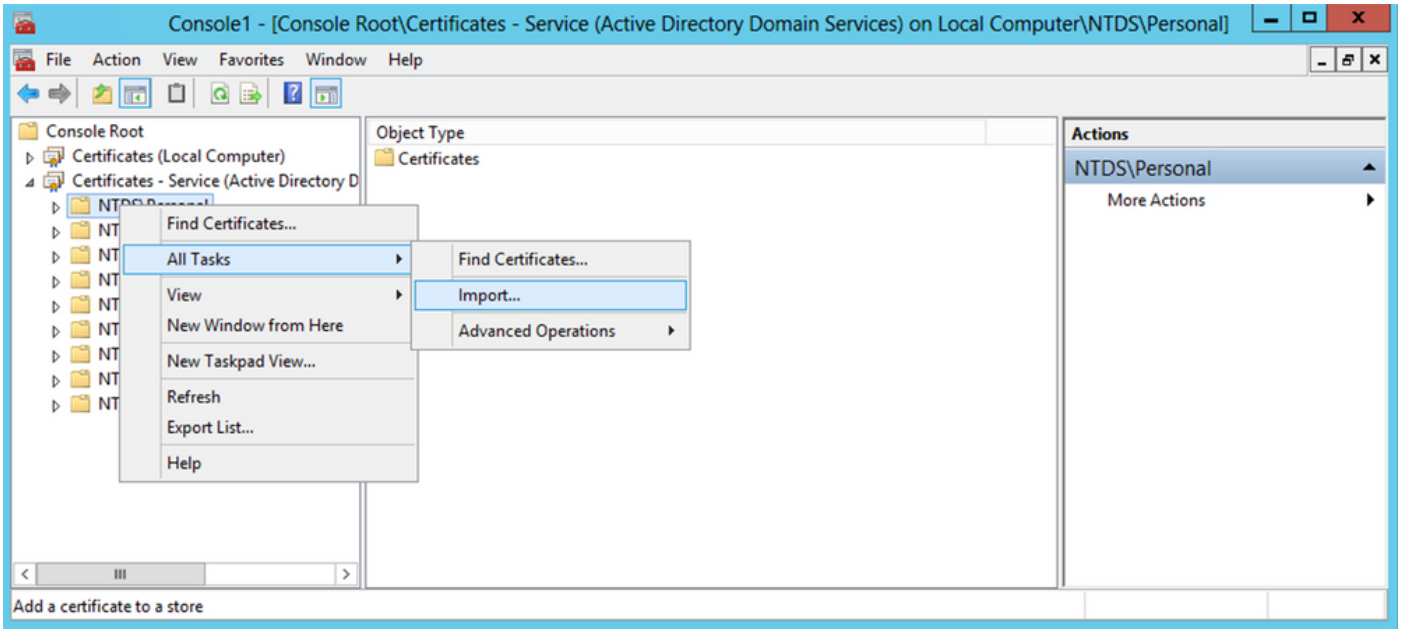
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html.

- Once the export of the certificate is done, navigate to Add/Remove Snap-in on MMC console. Click Certificates and then click Add.
- Choose Service account and then click Next.

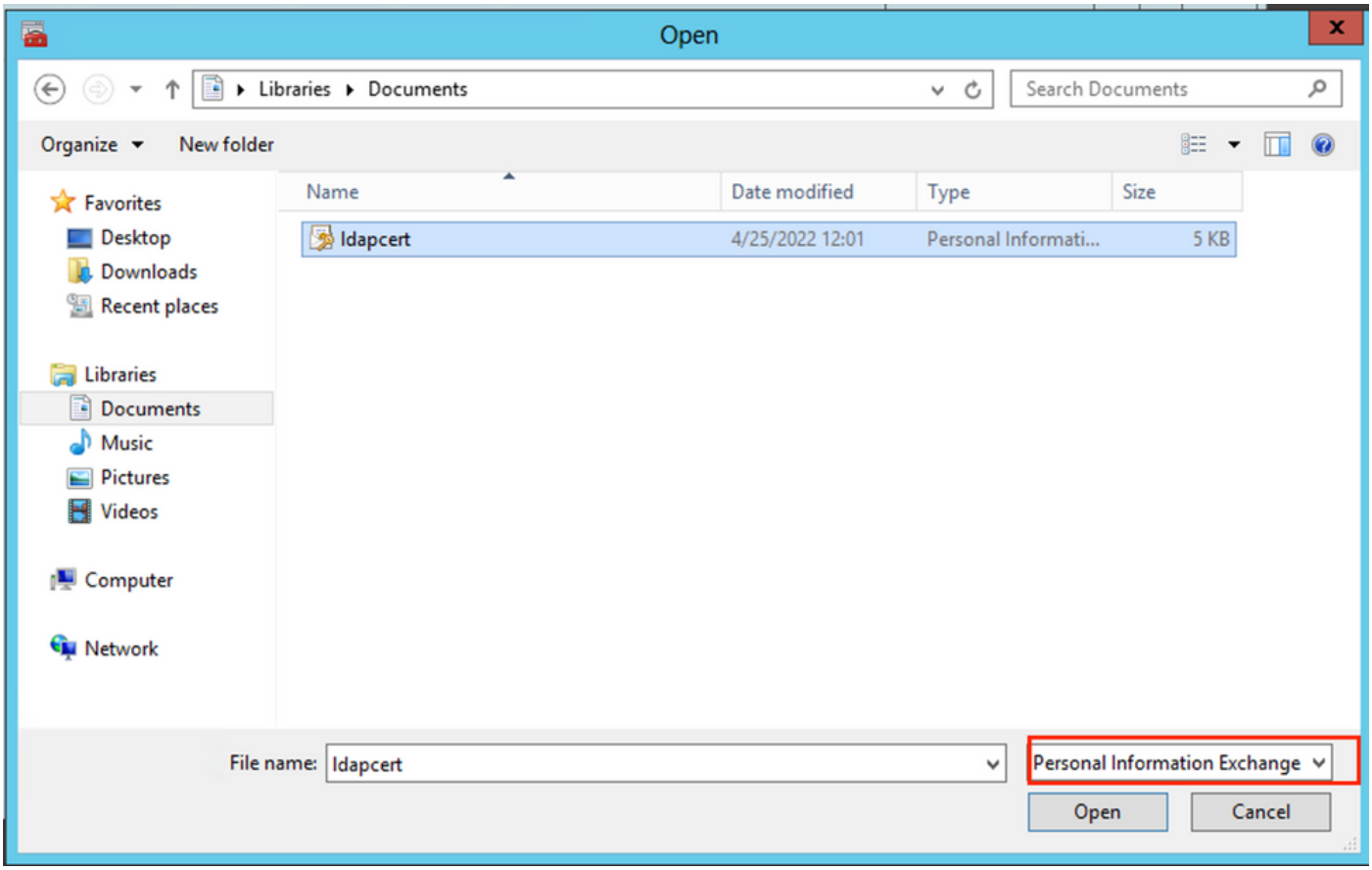
- In the Select Computer dialog box, choose Local Computer and click Next.
- Choose Active Directory Domain Services and then click Finish.



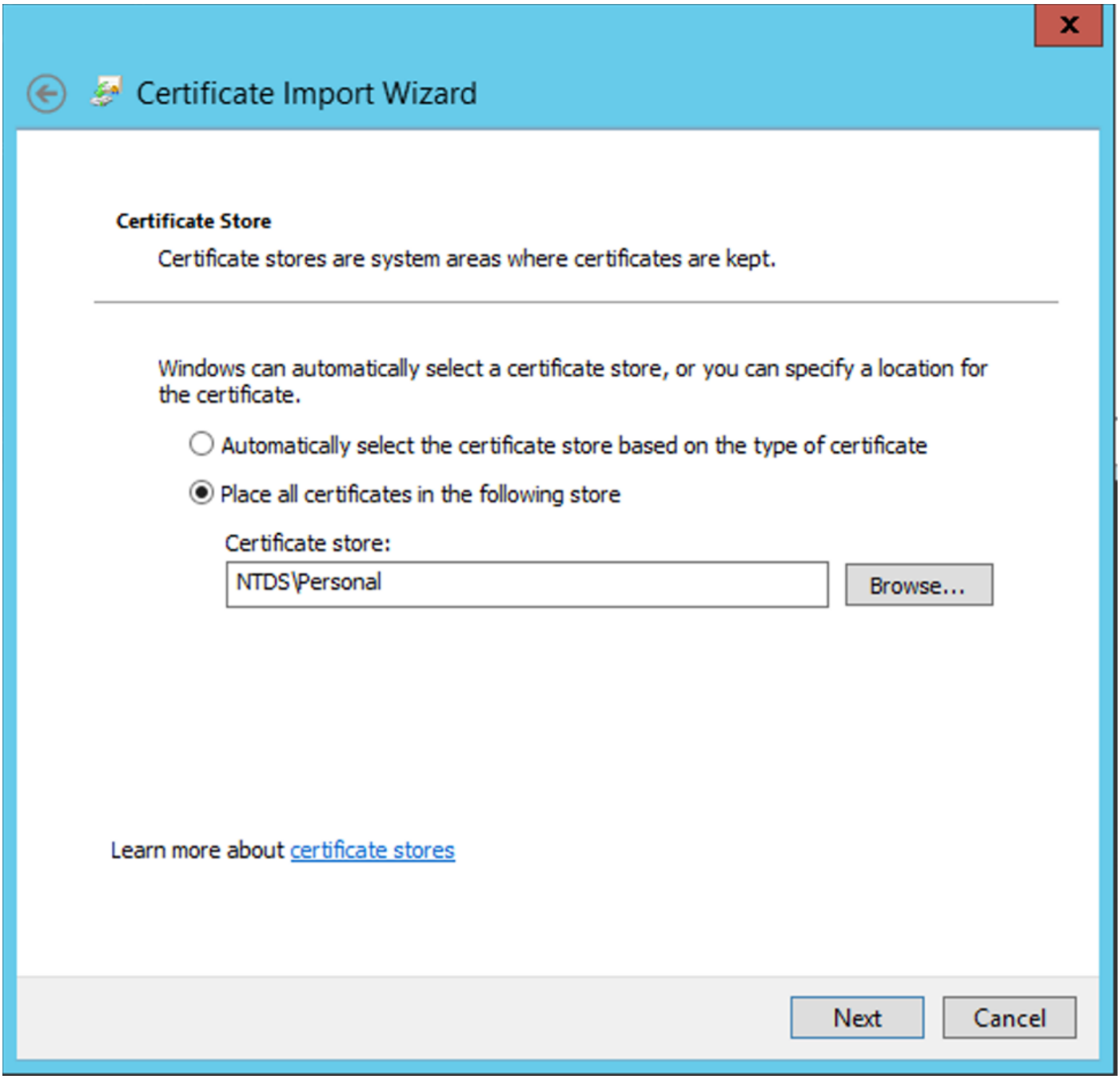
- On the Add/Remove Snap-ins dialog box, click OK.
- Expand Certificates - Services (Active Directory Domain Services) and then click NTDS\Personal.
- Right-click NTDS\Personal, click All Tasks, and then click Import.



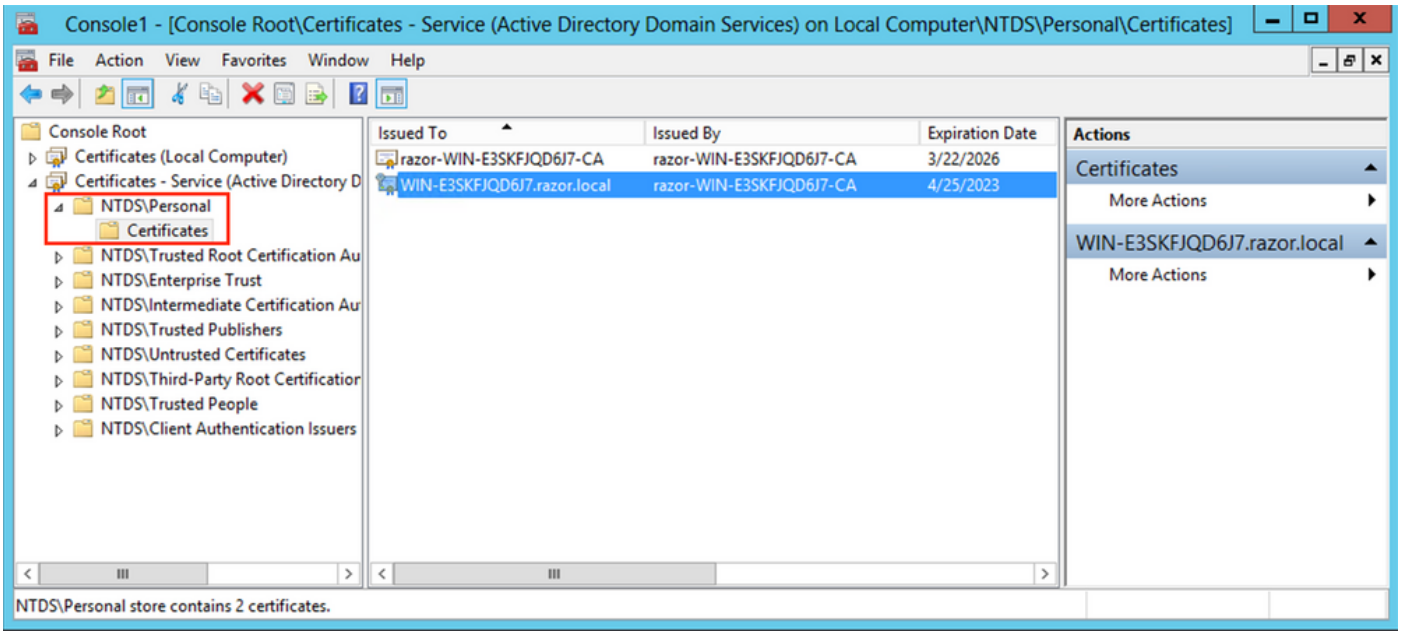
- On the Certificate Import Wizard welcome screen, click Next.
- On the File to Import screen, click Browse, and locate the certificate file that you exported previously.
- On the Open screen, ensure that Personal Information Exchange (*pfx,*.p12) is selected as the file type and then navigate the file system to locate the certificate you exported previously. Then, click that certificate.



- Click Open and then click Next.
- On the Password screen, enter the password you set for the file, and then click Next.
- On the Certificate Store page, ensure that Place all certificates are selected and read Certificate Store: NTDS\Personal and then click Next.



- On the Certificate Import Wizard completion screen, click Finish. You then see a message that the import was successful. Click OK. It is seen that the certificate has been imported under the Certificate store: NTDS\Personal.



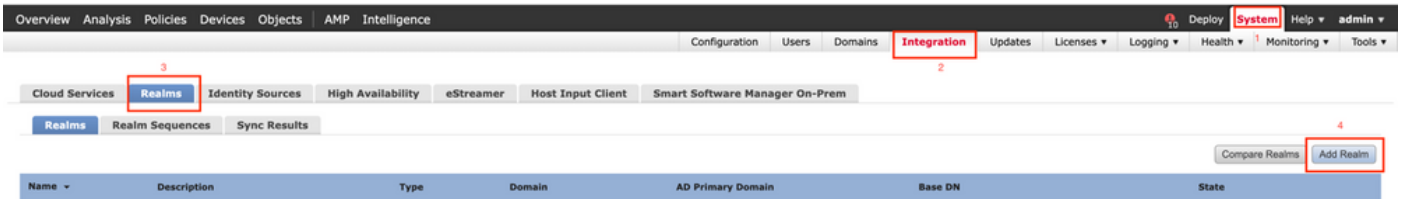
FMC Configurations

Verify Licensing

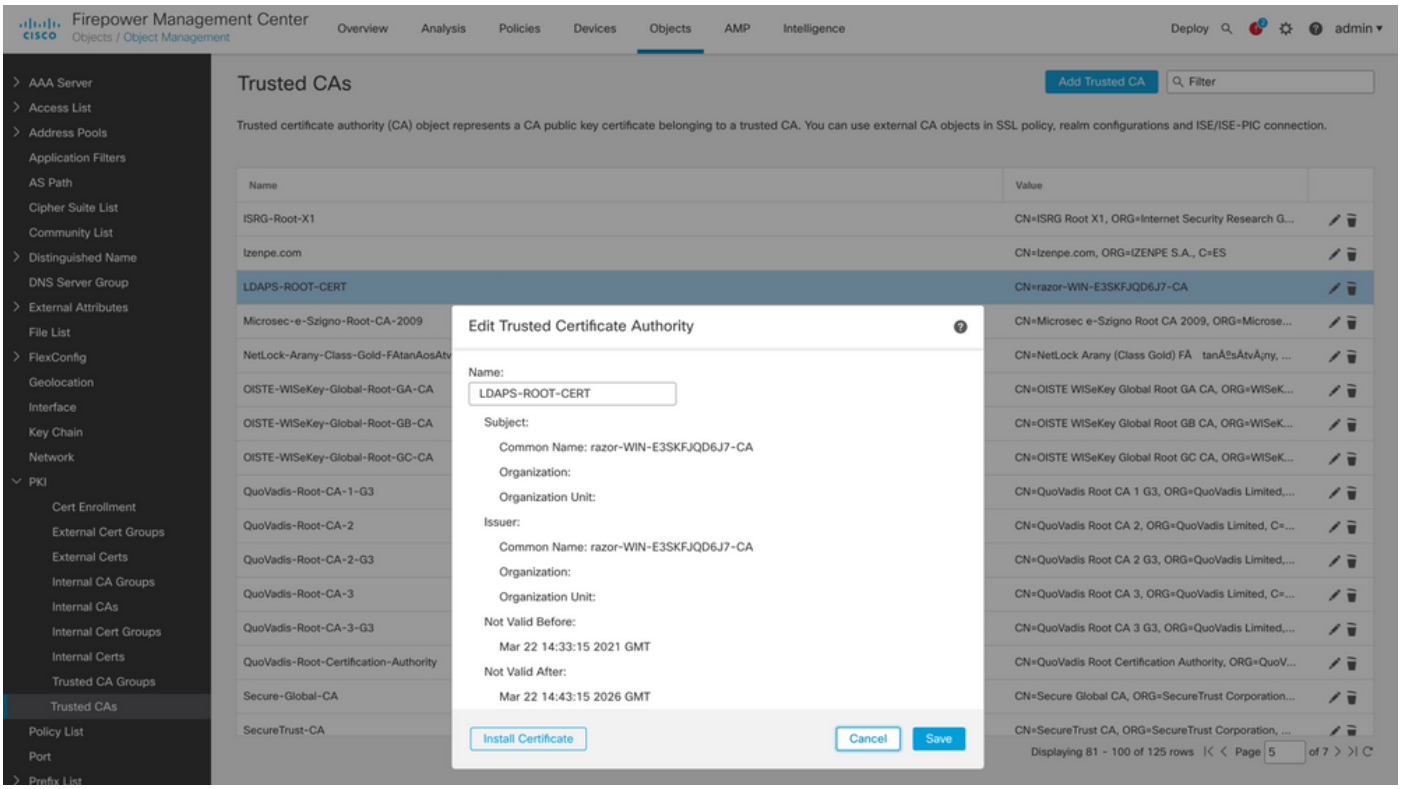
In order to deploy the AnyConnect configuration, the FTD must be registered with the smart licensing server, and a valid Plus, Apex, or VPN Only license must be applied to the device.

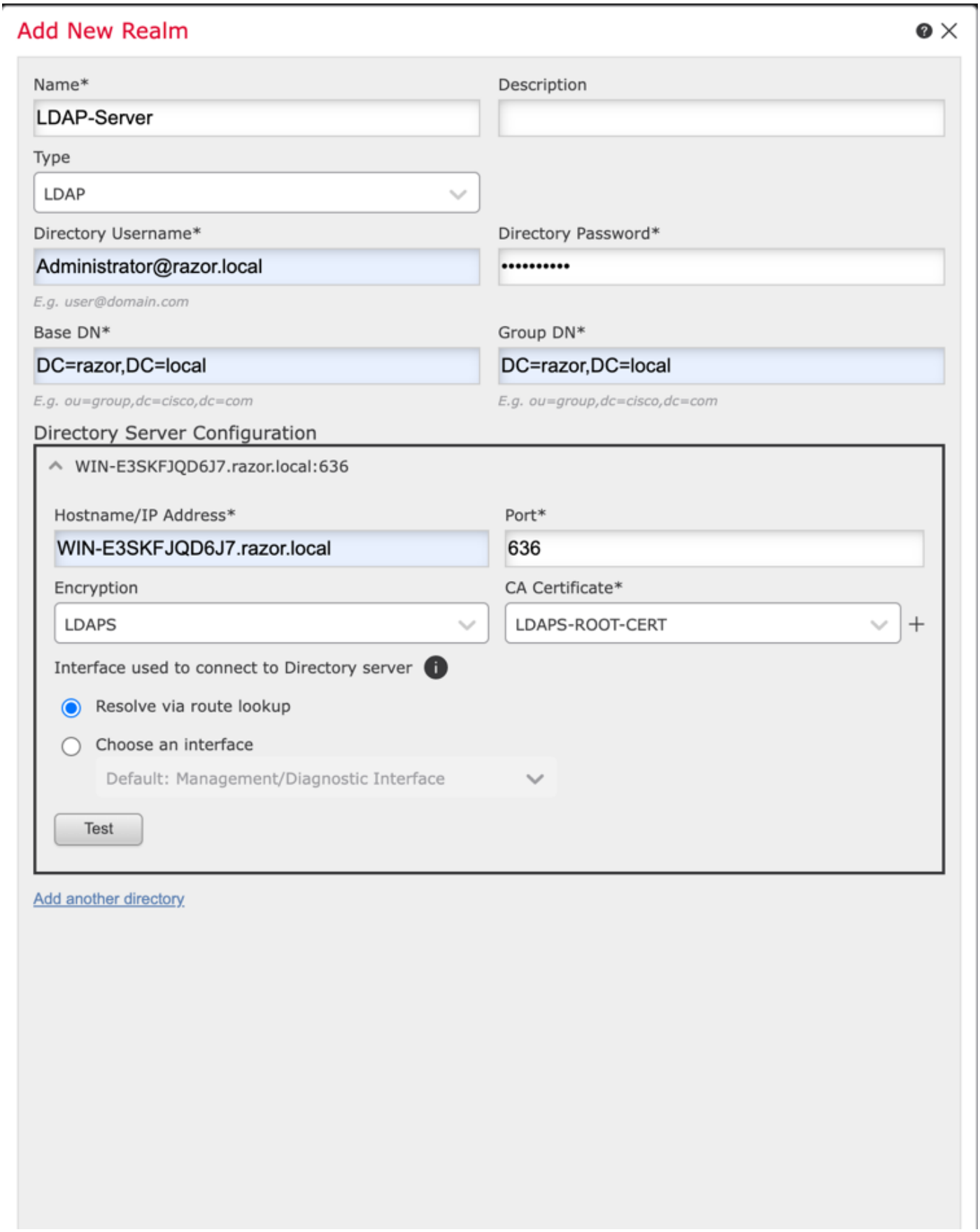
Setup Realm

1. Navigate to System > Integration. Navigate to Realms, then click Add Realm, as shown in this image:

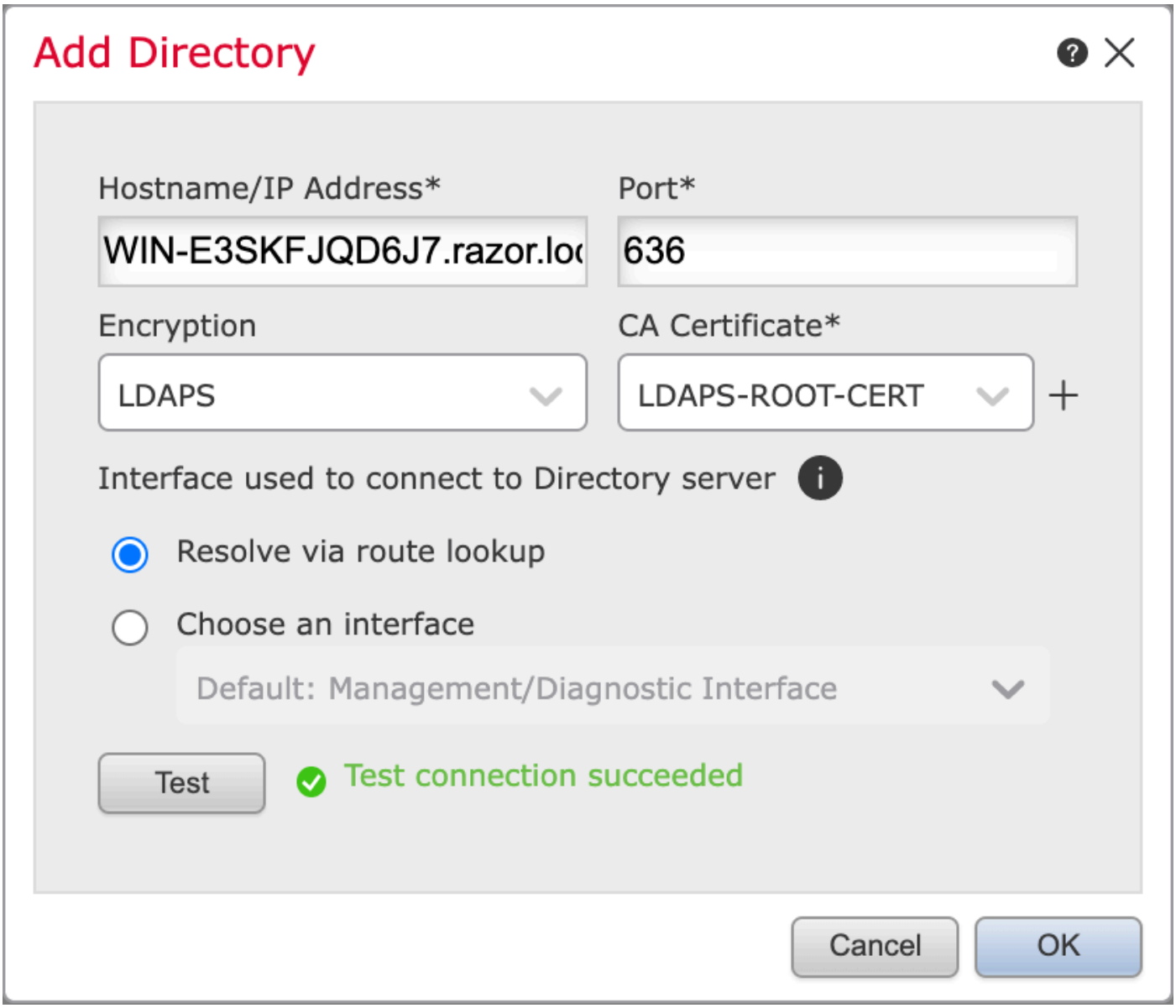


2. Fill out the displayed fields based on the information collected from the Microsoft server for LDAPs. Prior to this, import the Root CA Certificate that has signed the LDAPs service Certificate on the Windows Server under Objects > PKI > Trusted CAs > Add Trusted CA, as this is referenced under theDirectory Server Configuration of the Realm. Once done, click OK.

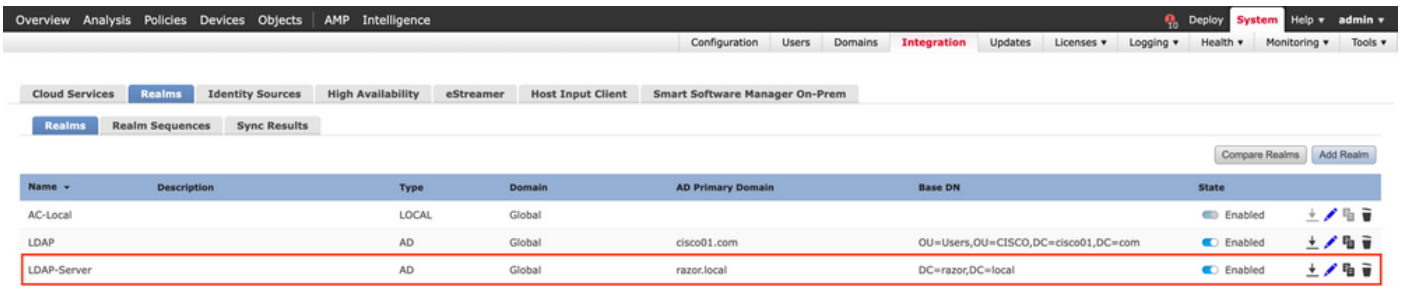

Firepower Management Center
Objects / Object Management
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Deploy
admin
AAA Server
Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
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. Click Test in order to ensure FMC can successfully bind with the Directory Username and password provided in the earlier step. Since these tests are initiated from the FMC and not through one of the routable interfaces configured on the FTD (such as inside, outside, dmz), a successful (or failed) connection does not guarantee the same result for AnyConnect authentication since AnyConnect LDAP authentication requests are initiated from one of the FTD routable interfaces.

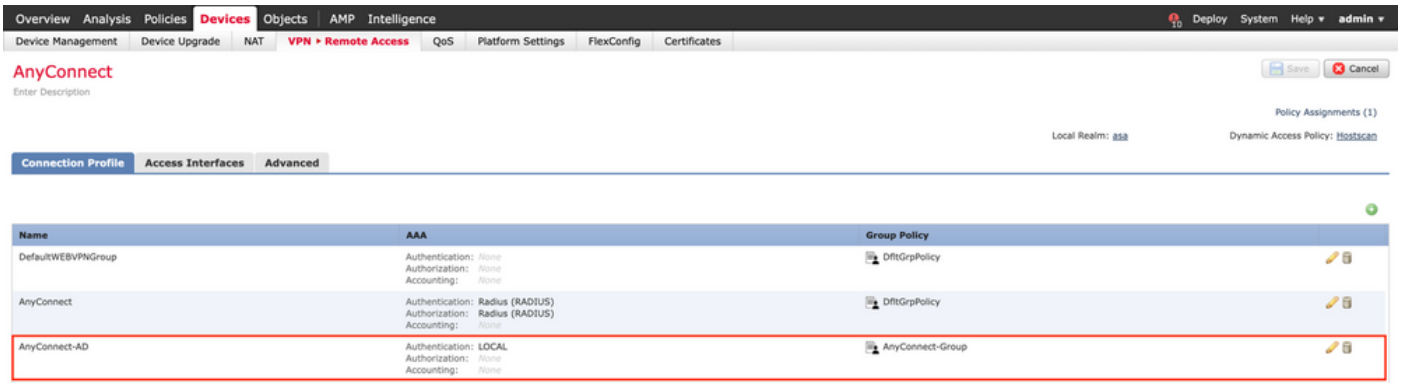


4. Enable the new realm.

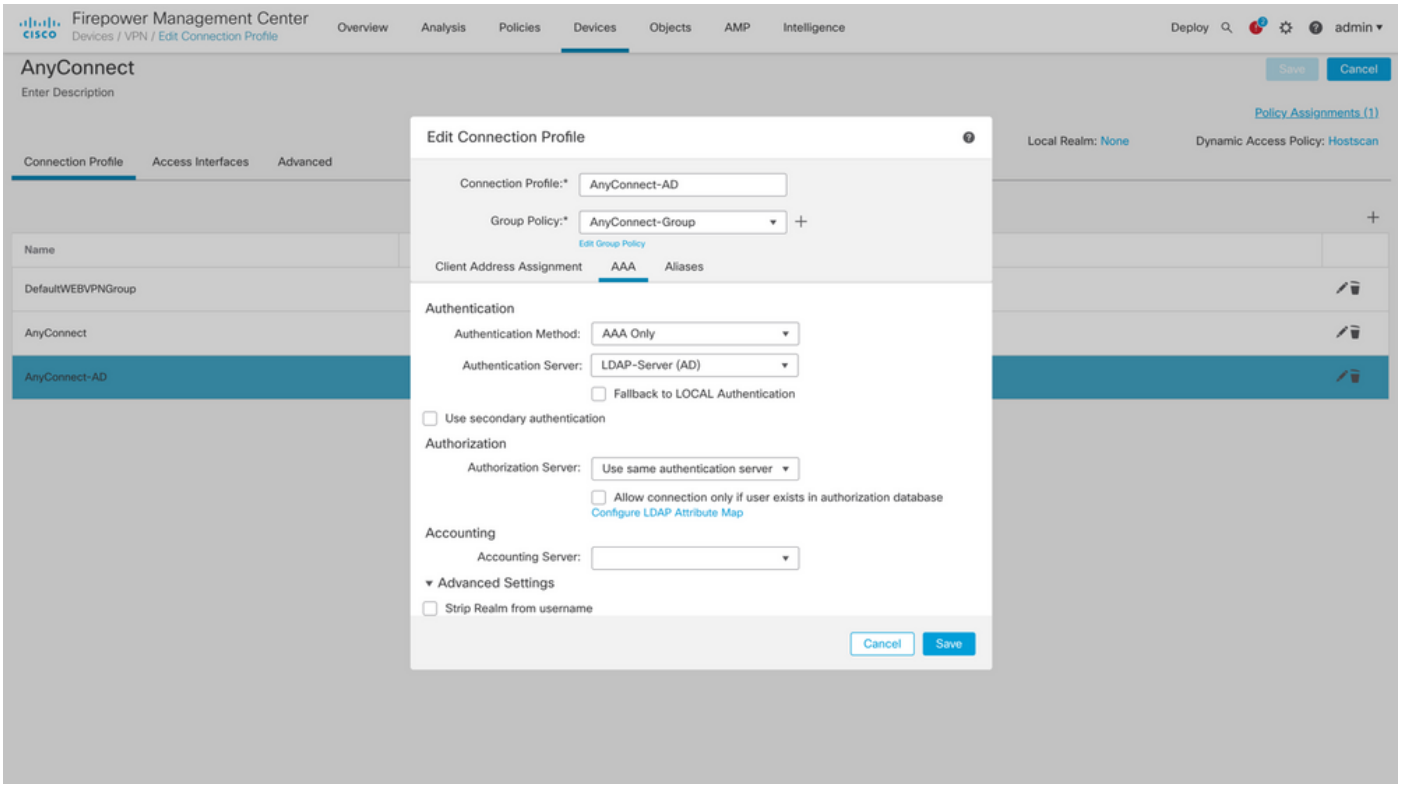


Configure AnyConnect for Password-Management

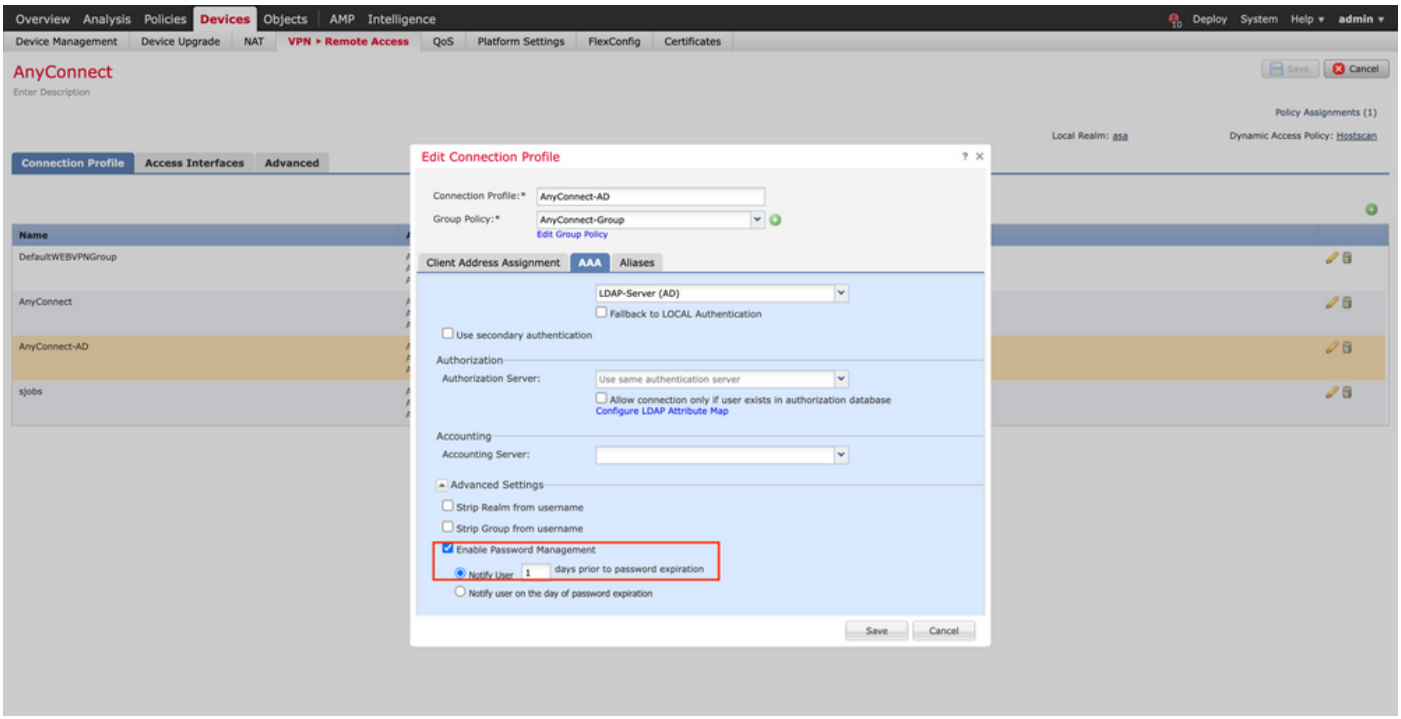
1. Choose the existing Connection Profile or create a new one, if it is an initial setup of AnyConnect. Here, an existing Connection Profile named 'AnyConnect-AD' mapped with Local Authentication is used.



2. Edit the Connection profile and map the new LDAPs server configured in the earlier steps, under the AAA settings of the Connection Profile. Once done, click Save on the top right corner.



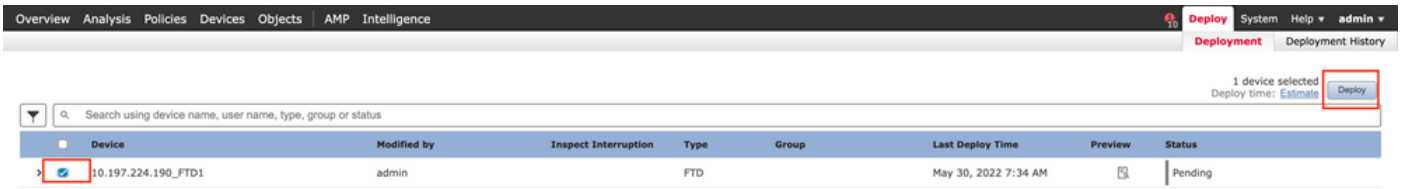
3. Enable password management under the AAA > Advanced Settings and save the configuration.



Deploy

1. Once done with all the configuration, click theDeploy button on the top right.

2. Click the checkbox next to the FTD configuration applied to it and then click Deploy, as shown in this image:



Final Configuration

This is the configuration seen in the FTD CLI after the successful deployment.

AAA Configuration

<#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 Configuration

<#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
```

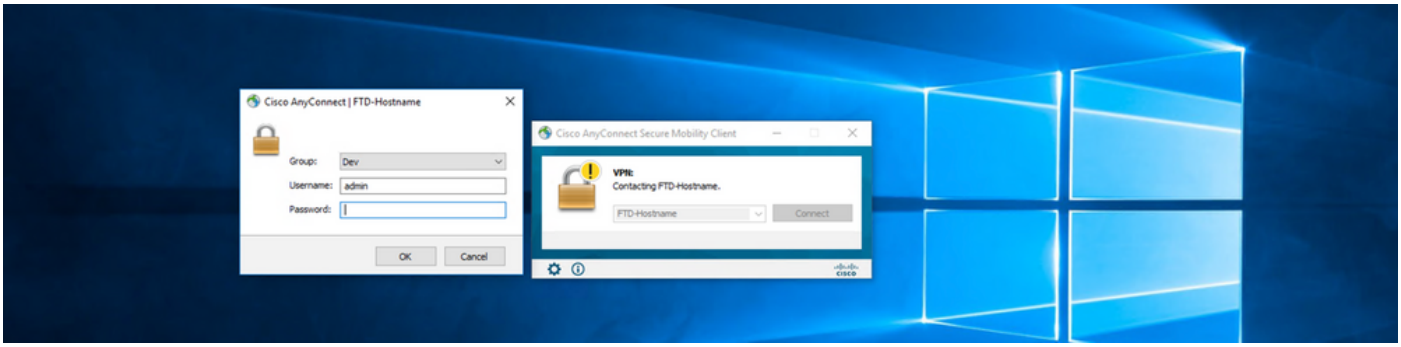
```
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private none
  anyconnect ssl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

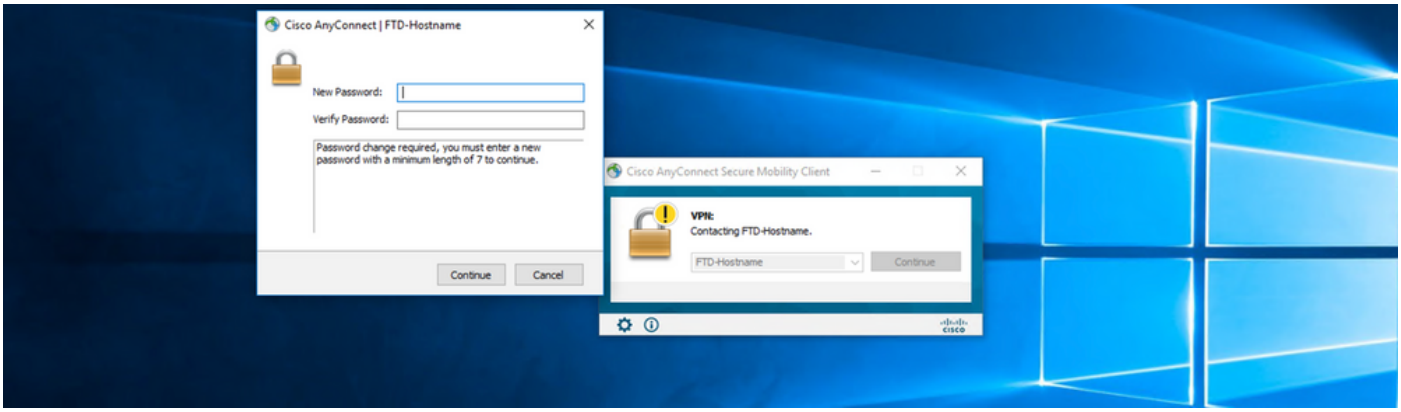
```
> show running-config ssl

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

Verification

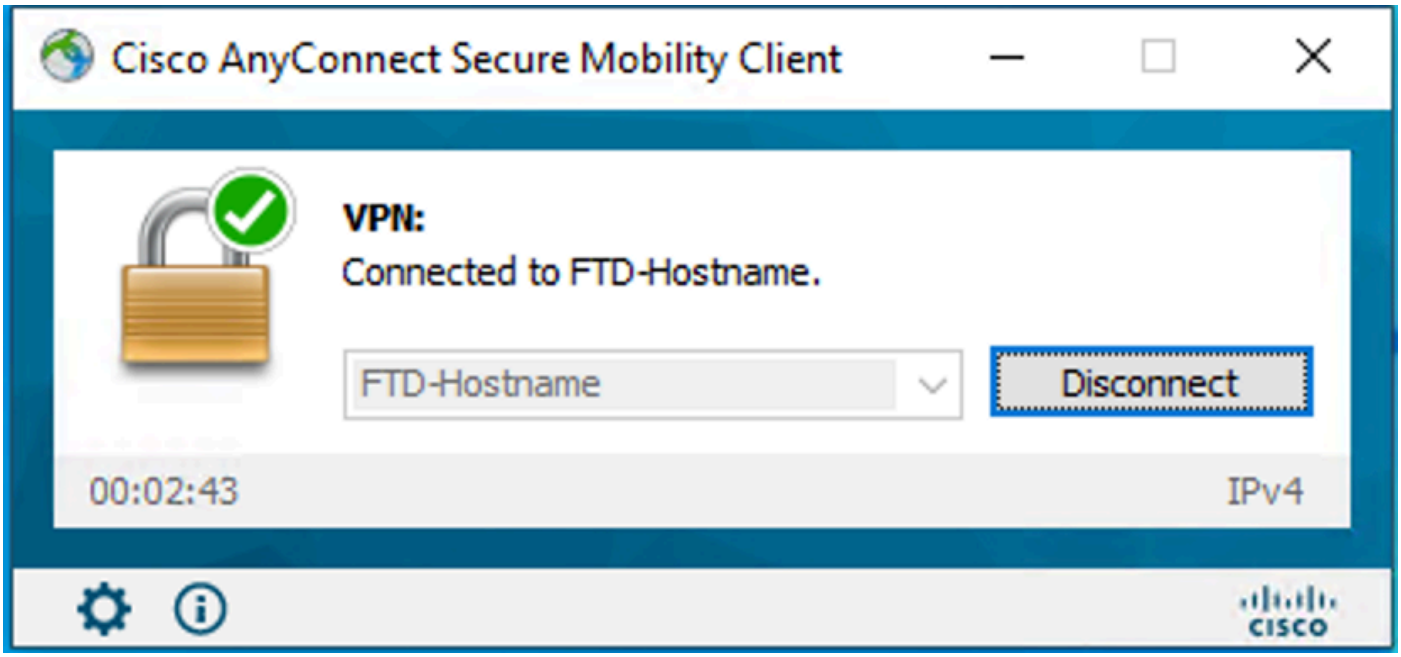
Connect with AnyConnect and Verify the Password-Management Process for the User Connection

1. Initiate a Connection to the concerned connection profile. Once it is determined at the initial login that the password must be changed since the earlier password was rejected by the Microsoft Server as it is expired, the user is prompted with the change of password.





2. Once the user enters the new password for login, the connection is established successfully.



3. Verify the user connection on the 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
```

Troubleshoot

Debugs

This debug can be run in diagnostic CLI in order to troubleshoot password management-related issues: **debug ldap 255**.

Working Password-Management Debugs

<#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
```

Common Errors Encountered During the Password-Management

Usually, if the password policy that is set by the Microsoft Server is not met during the time the user provides the new password, the connection gets terminated with the error “Password does not meet the Password Policy Requirements”. Hence, ensure that the new password meets the policy set by the Microsoft Server for LDAPs.