FMC에서 관리하는 FTD의 RA VPN에 대해 LDAP를 사용하여 비밀번호 관리 구성

목차

소개

이 문서에서는 Cisco FTD(Firepower Threat Defense)에 연결하는 AnyConnect 클라이언트에 대해 LDAP를 사용하여 비밀번호 관리를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- FMC의 RA VPN(Remote Access Virtual Private Network) 구성에 대한 기본 지식
- FMC의 LDAP 서버 컨피그레이션에 대한 기본 지식

- Active Directory에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft 2012 R2 서버
- 7.3.0을 실행하는 FMCv
- 7.3.0을 실행하는 FTDv

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

설정

네트워크 다이어그램 및 시나리오

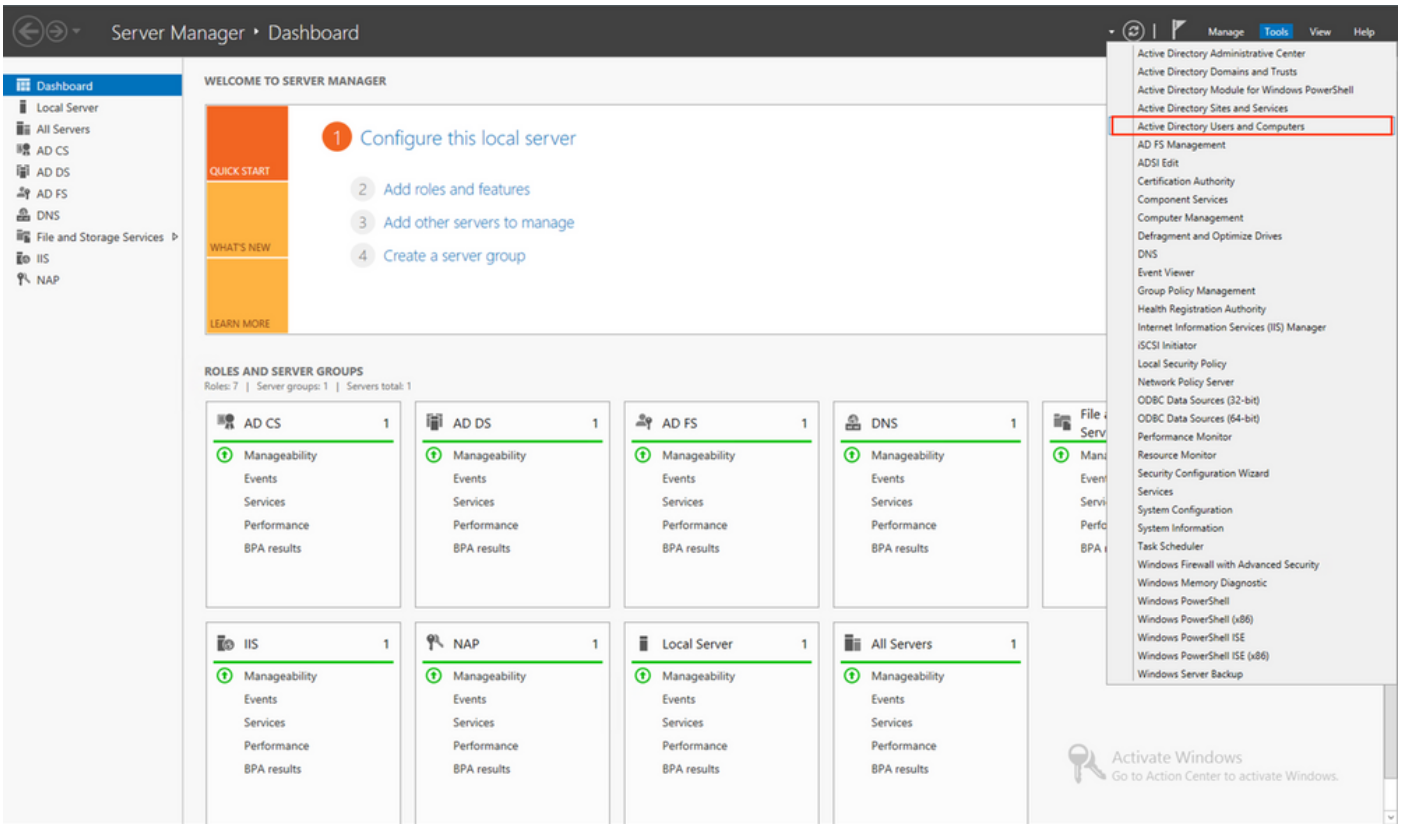
Windows 서버는 사용자 암호 관리 프로세스를 테스트하기 위해 ADDS 및 ADCS로 미리 구성되어 있습니다. 이 컨피그레이션 가이드에서는 이러한 사용자 계정을 생성합니다.

사용자 계정:

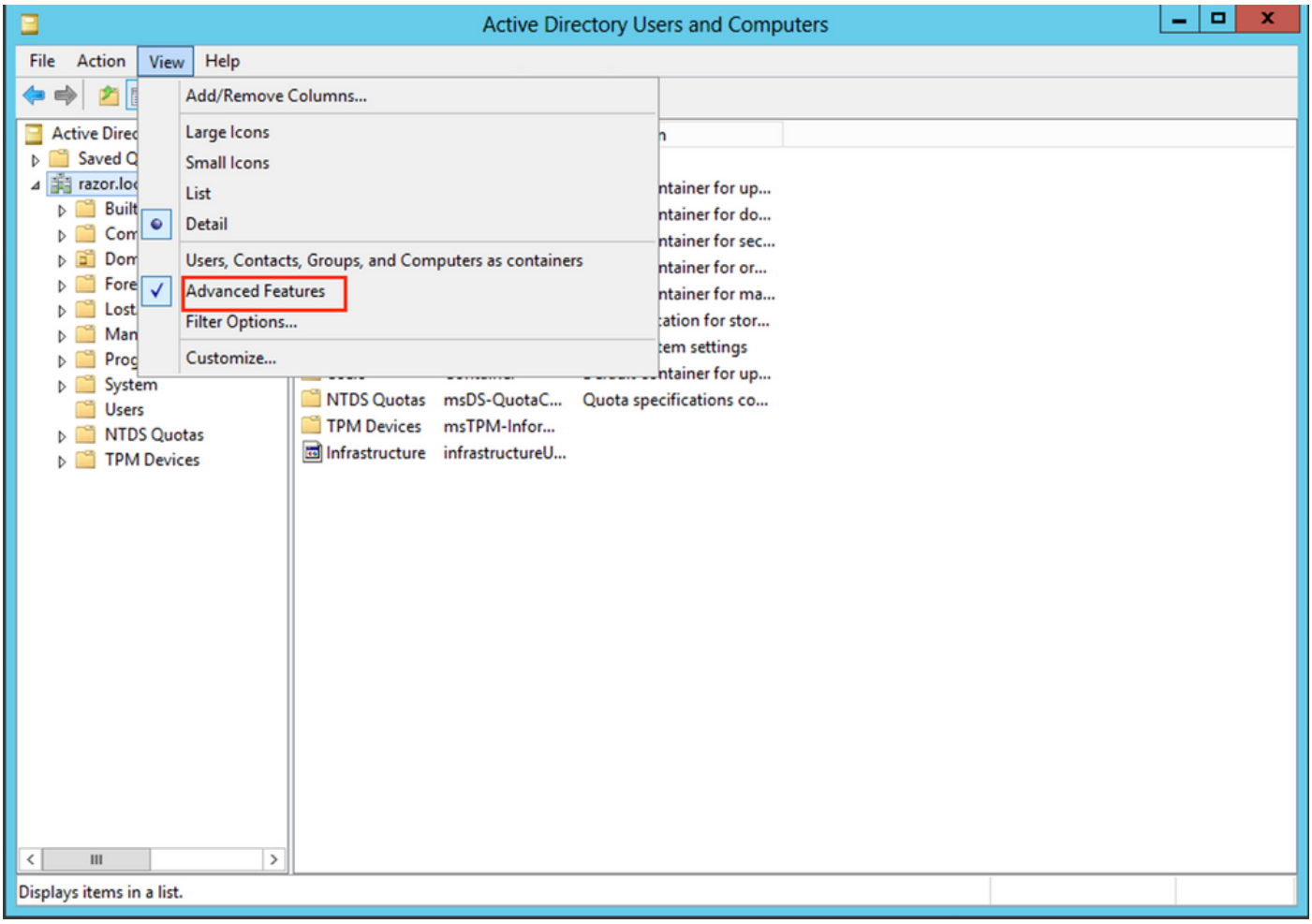
- 관리자: FTD가 Active Directory 서버에 바인딩될 수 있도록 디렉토리 계정으로 사용됩니다.
- admin: 사용자 ID를 시연하는 데 사용되는 테스트 관리자 계정입니다.

LDAP 기본 DN 및 그룹 DN 결정

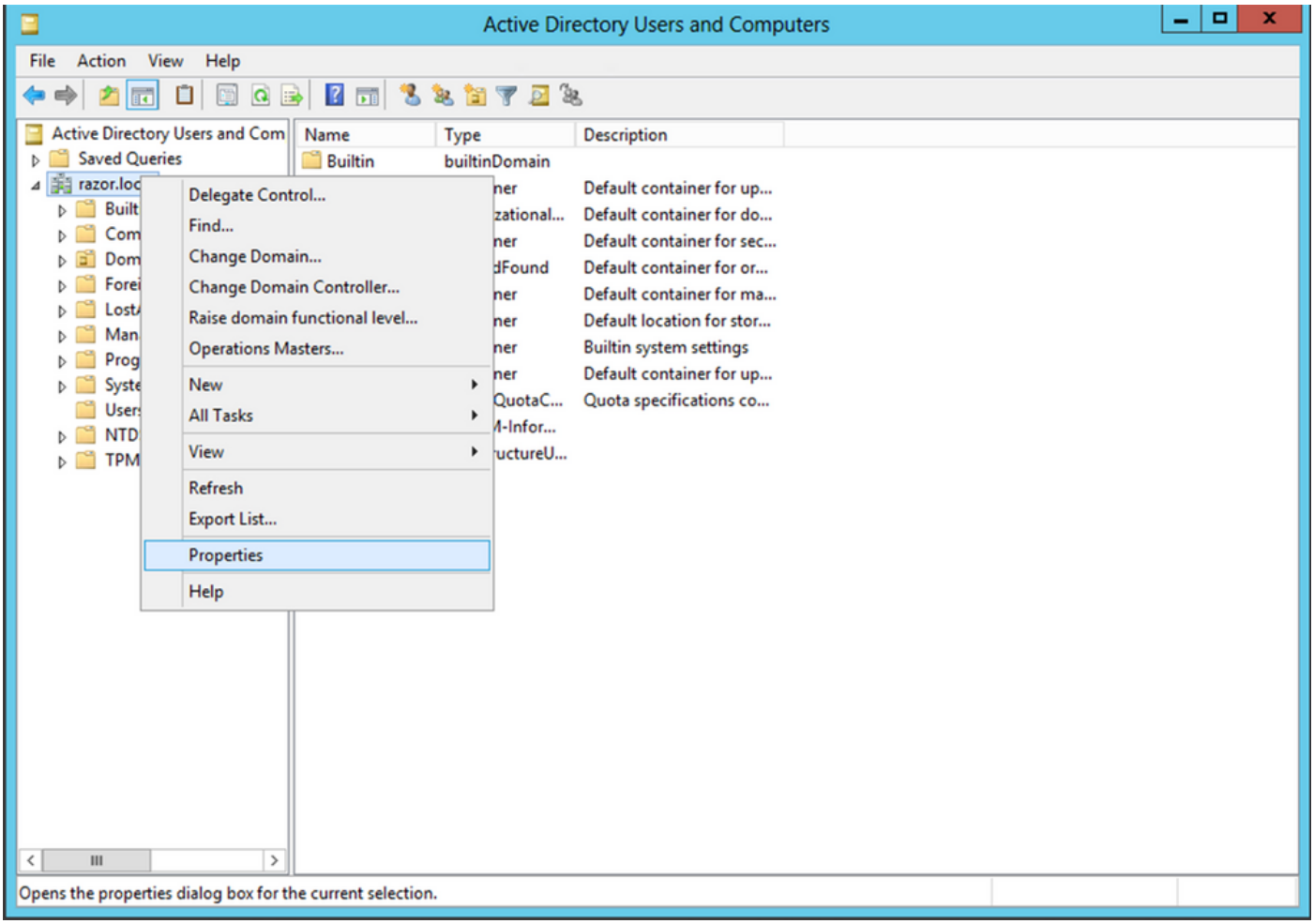
1. 열기 Active Directory Users and Computers Server Manager Dashboard(서버 관리자 대시보드)를 클릭합니다.



2. 열기 View Option 을 활성화하여 Advanced Features, 이미지에 표시된 대로



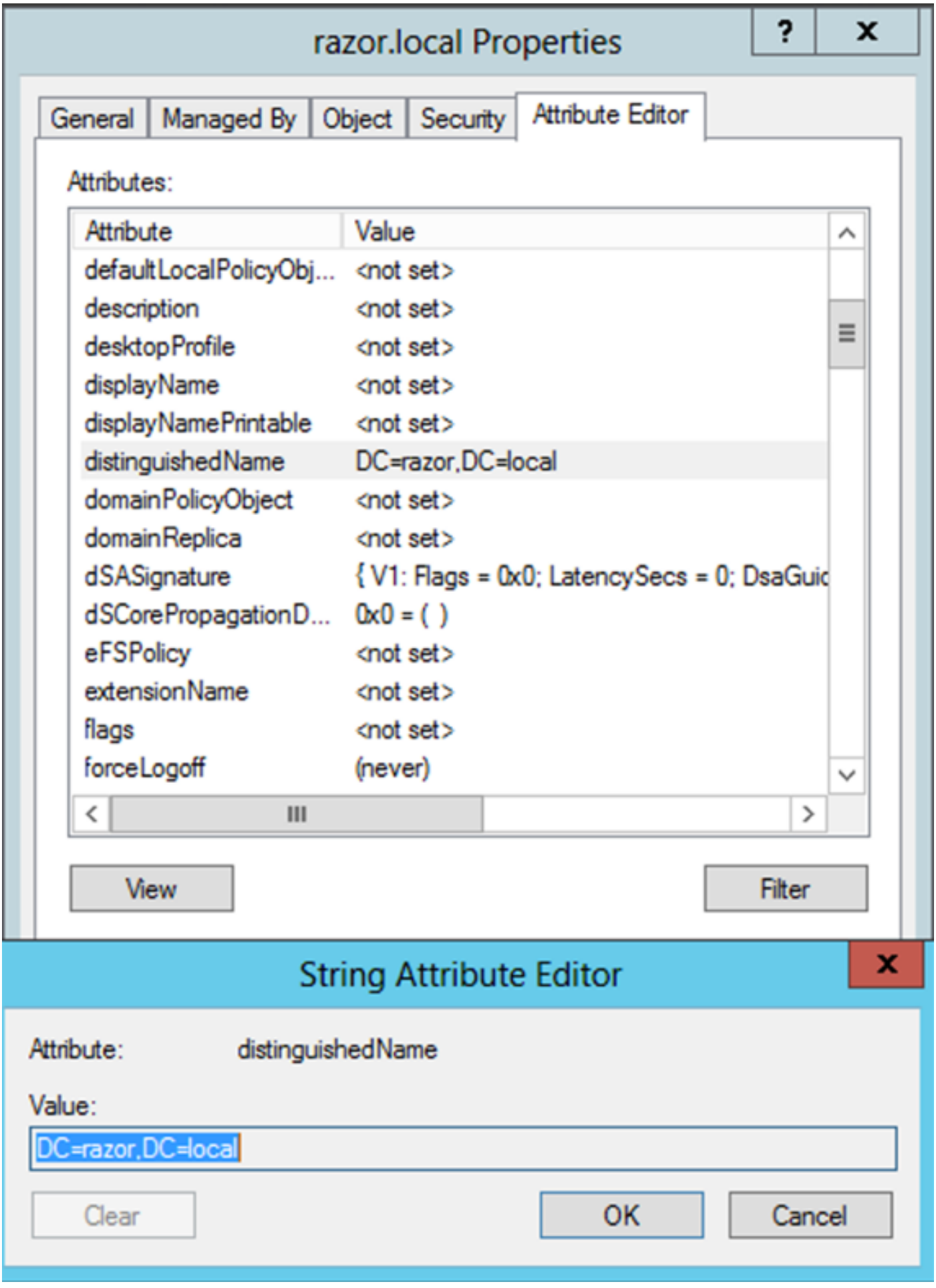
3. 이렇게 하면 AD 개체 아래의 추가 속성을 볼 수 있습니다.
   예를 들어, 루트에 대한 DN을 찾으려면 razor.local마우스 오른쪽 버튼으로 클릭 razor.local을 선택한 다음 Properties, 이 이미지에 표시된 대로



4. 아래 Properties을 선택합니다. Attribute Editor 탭을 클릭합니다. 찾기 distinguishedName 속성 아래에서 View에 나와 있는 것처럼.

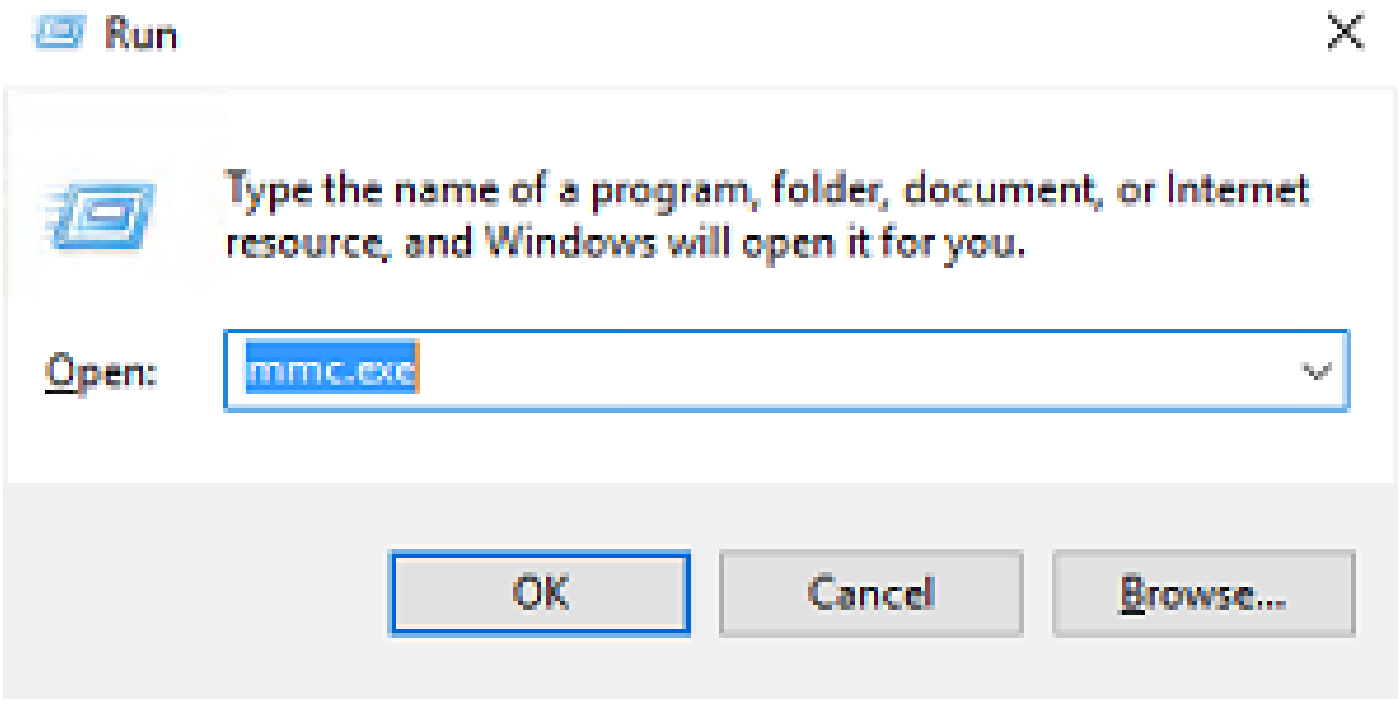
이렇게 하면 나중에 DN을 복사하여 FMC에 붙여넣을 수 있는 새 창이 열립니다.

이 예에서 루트 DN은 DC=razor, DC=local. 값을 복사하여 나중에 저장할 수 있습니다. 클릭 OK string Attribute Editor 창을 종료하고 OK 등록 정보를 종료하려면 다시 시도하십시오.

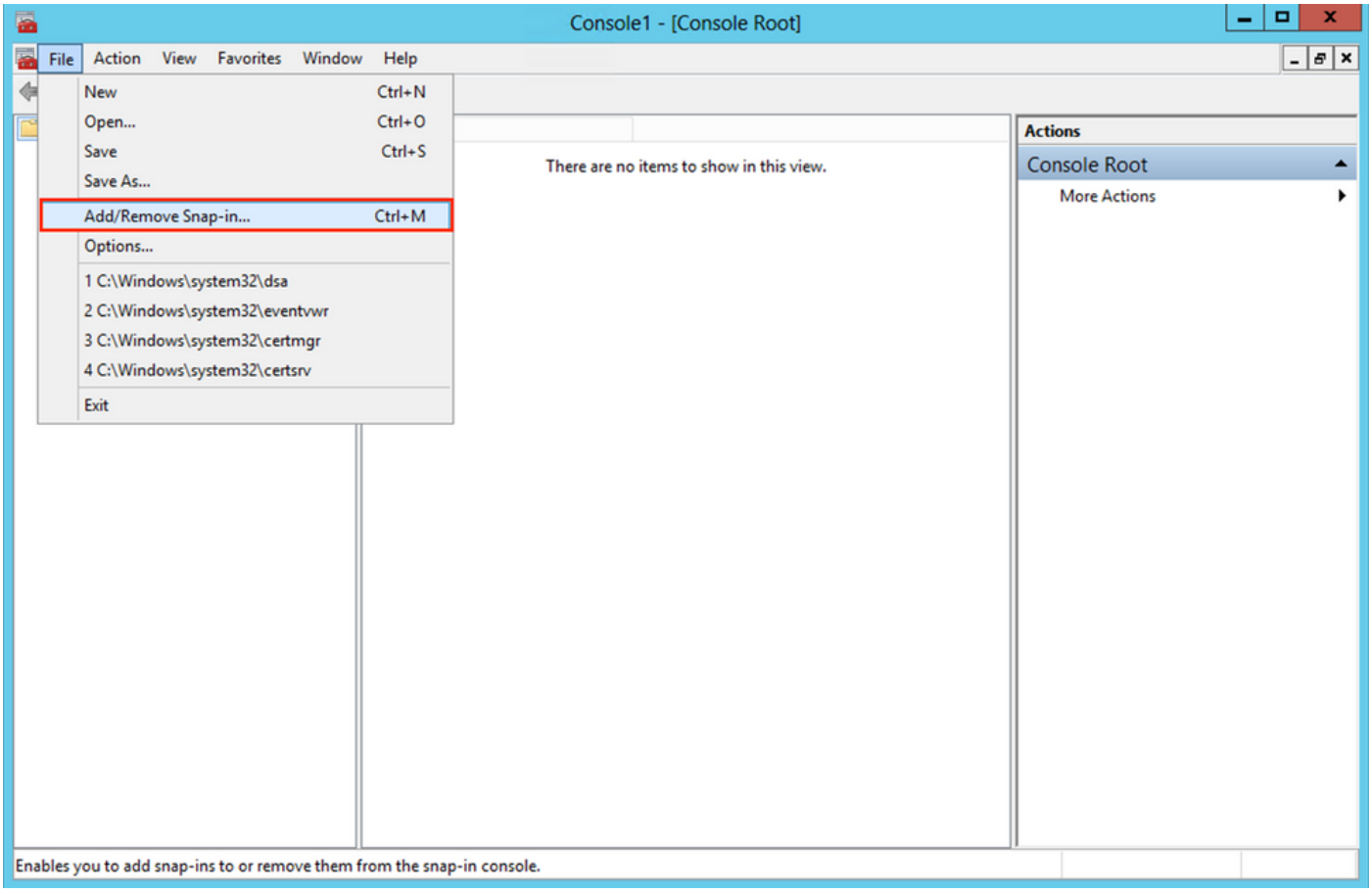

razor.local Properties
General
Managed By
Object
Security
Attribute Editor
Attributes:
Attribute
Value
defaultLocalPolicyObj...
<not set>
description
<not set>
desktopProfile
<not set>
displayName
<not set>
displayNamePrintable
<not set>
distinguishedName
DC=razor,DC=local
domainPolicyObject
<not set>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

LDAPS SSL 인증서 루트 복사

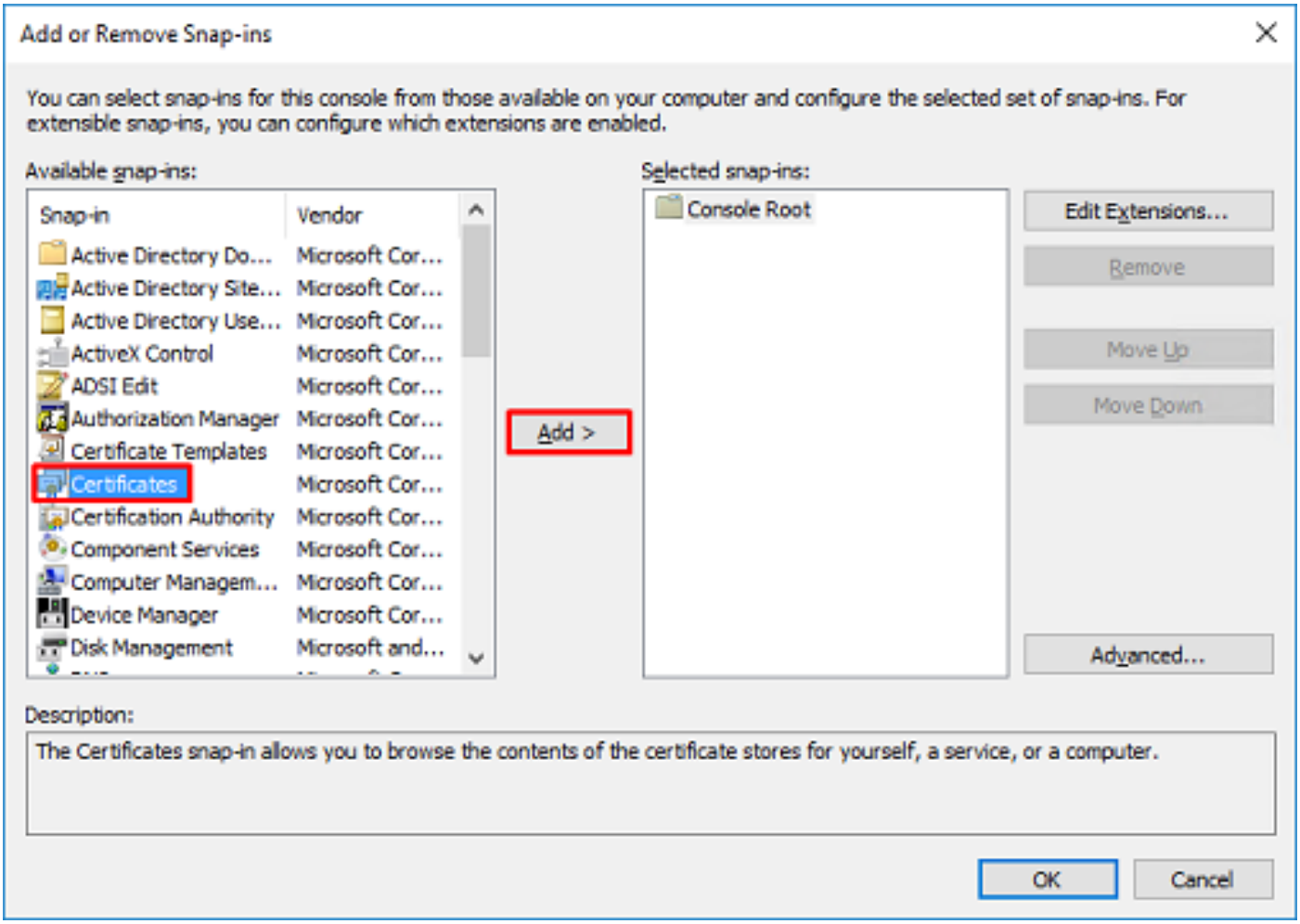
1. 누르기 Win+R 및 입력 mmc.exe를 클릭한 다음 OK이 그림에 나와 있는 것처럼.



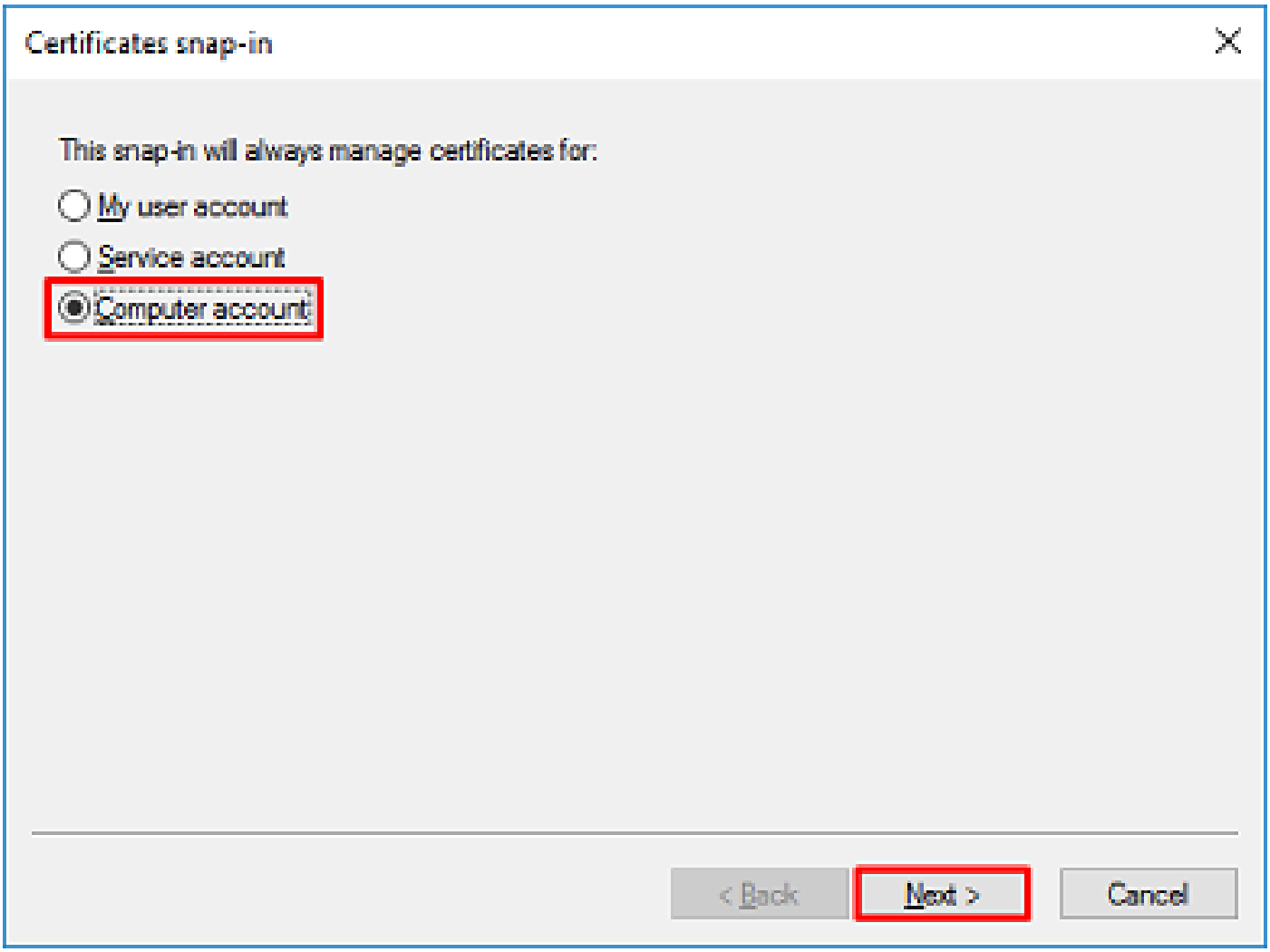
2. 탐색 File > Add/Remove Snap-in..., 이 이미지에 표시된 ss:



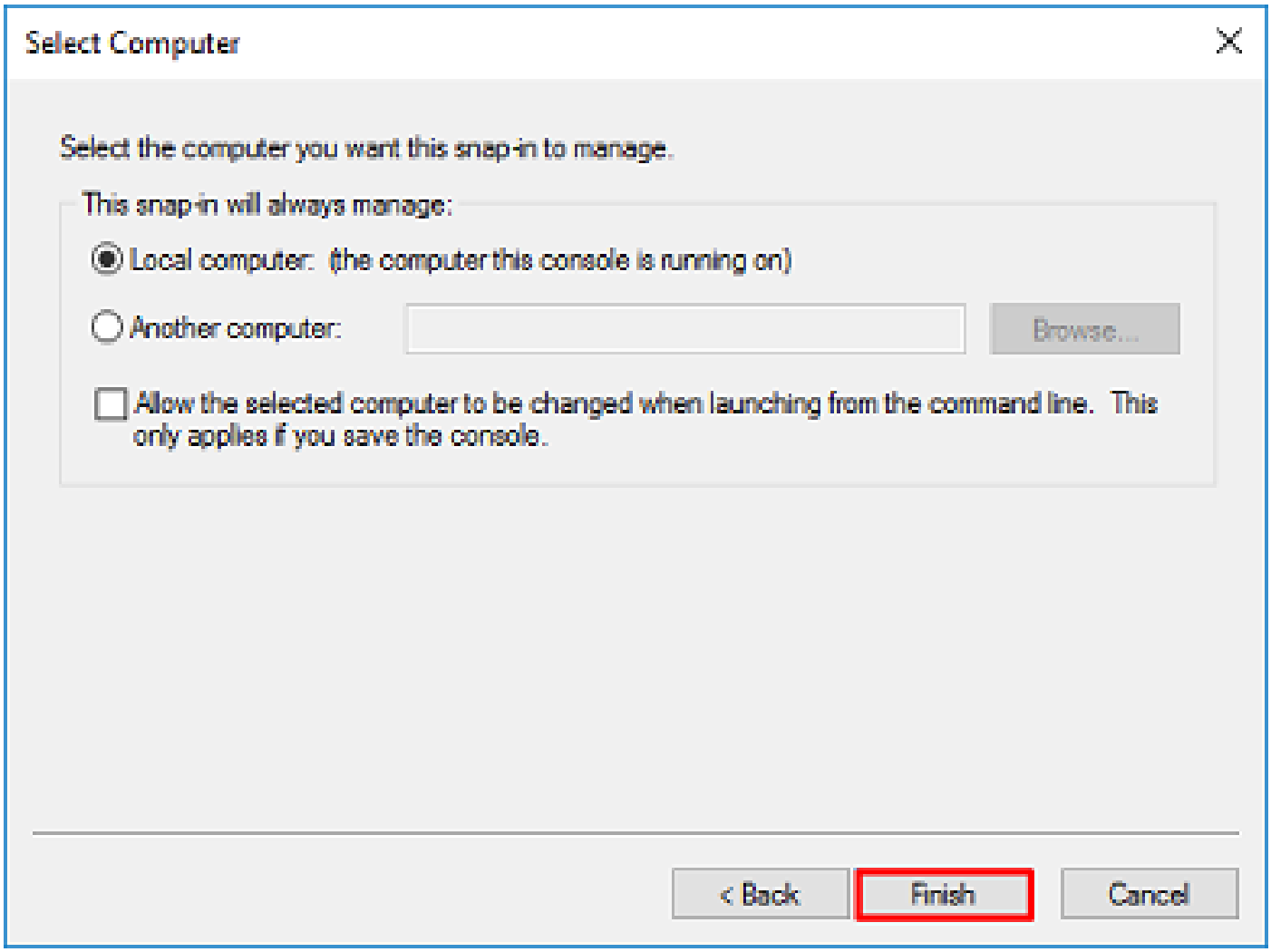
3. 사용 가능한 스냅인에서 Certificates 다음을 클릭합니다. Add, 이 이미지에 표시된 대로



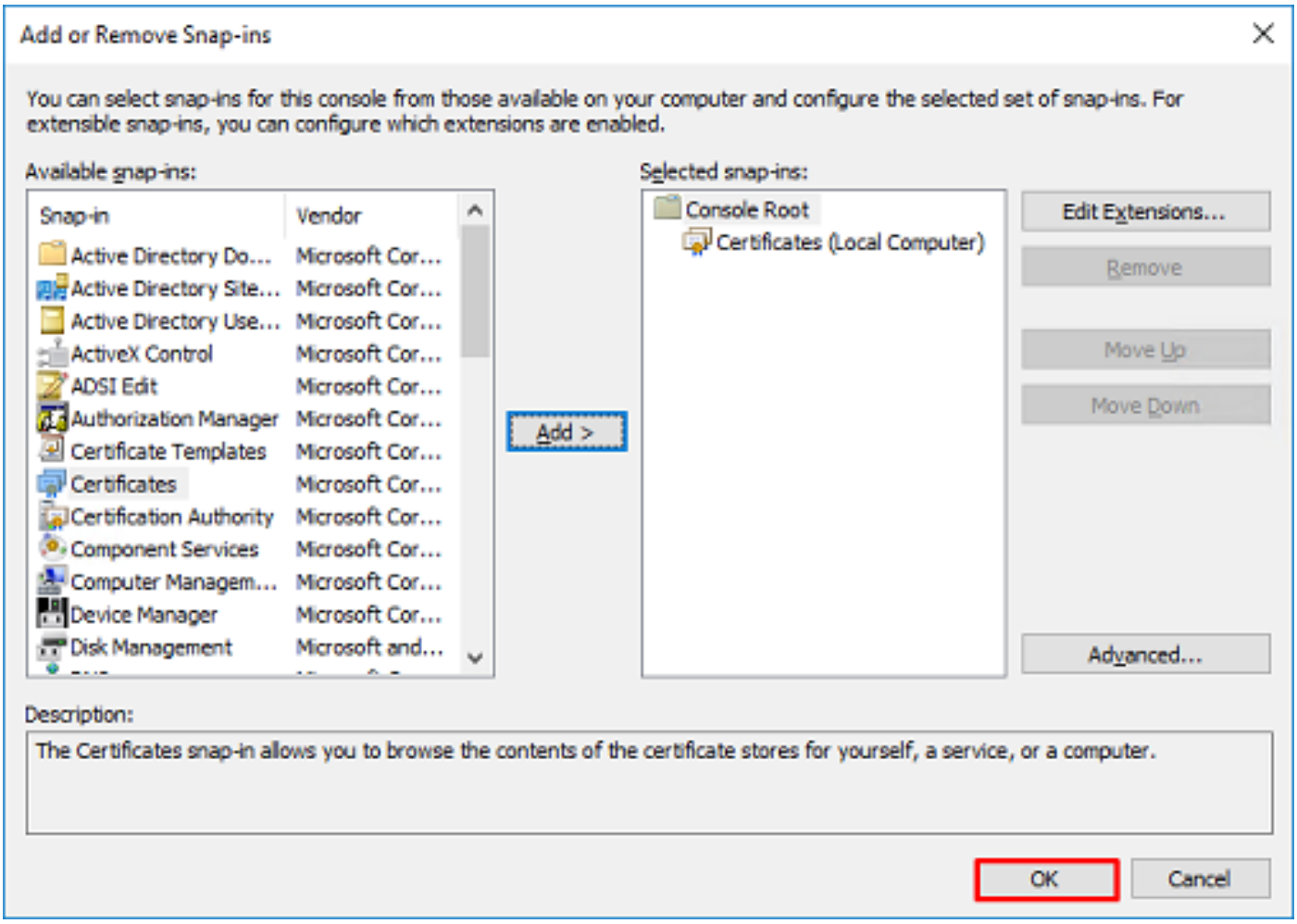
4. 선택 Computer account 다음을 클릭합니다. Next, 이 이미지에 표시된 대로



여기에 표시된 대로 Finish.



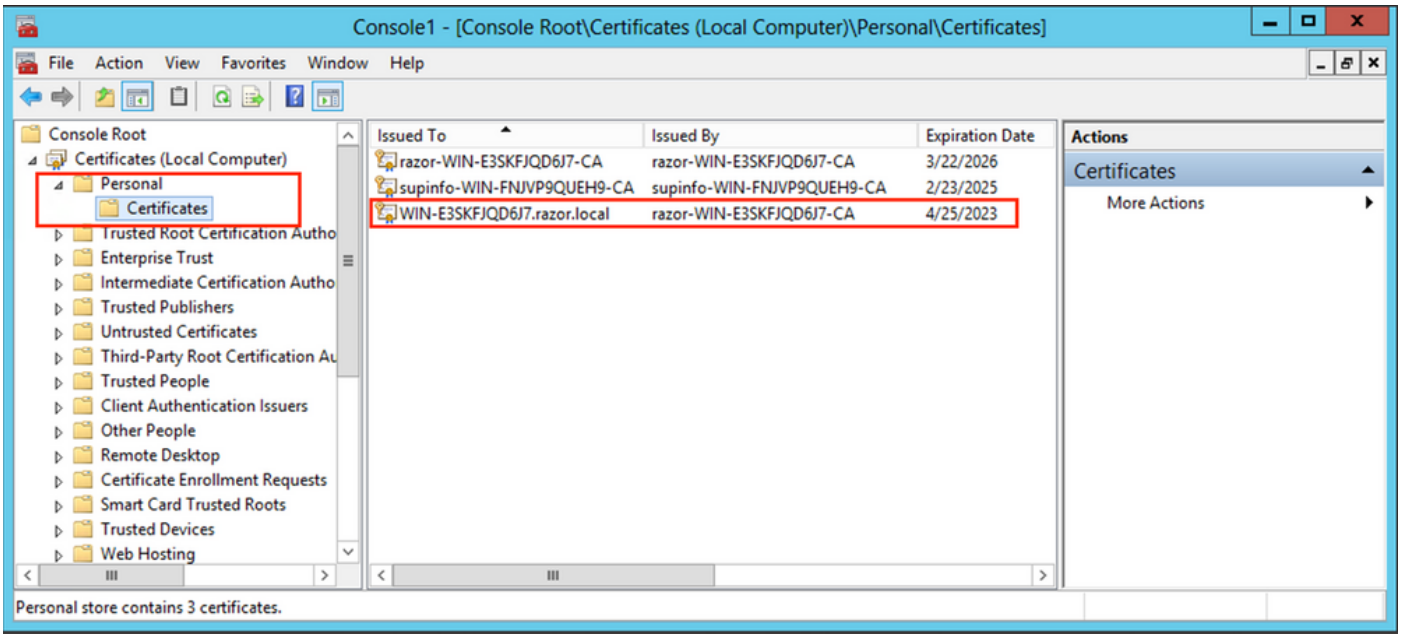
5. 이제 OK이 그림에 나와 있는 것처럼.



6. 를 펼칩니다. Personal 폴더를 클릭한 다음 Certificates. LDAP에서 사용하는 인증서는 Windows 서버의 FQDN(Fully Qualified Domain Name)에 발급해야 합니다. 이 서버에는 세 가지 인증서가 나열됩니다.

- CA 인증서는 razor-WIN-E3SKFJQD6J7-CA.
- 에 의해 발급된 CA 인증서 supinfo-WIN-FNJVP9QUEH9-CA.
- ID 인증서가 WIN-E3SKFJQD6J7.razor.local 에 의해 razor-WIN-E3SKFJQD6J7-CA.

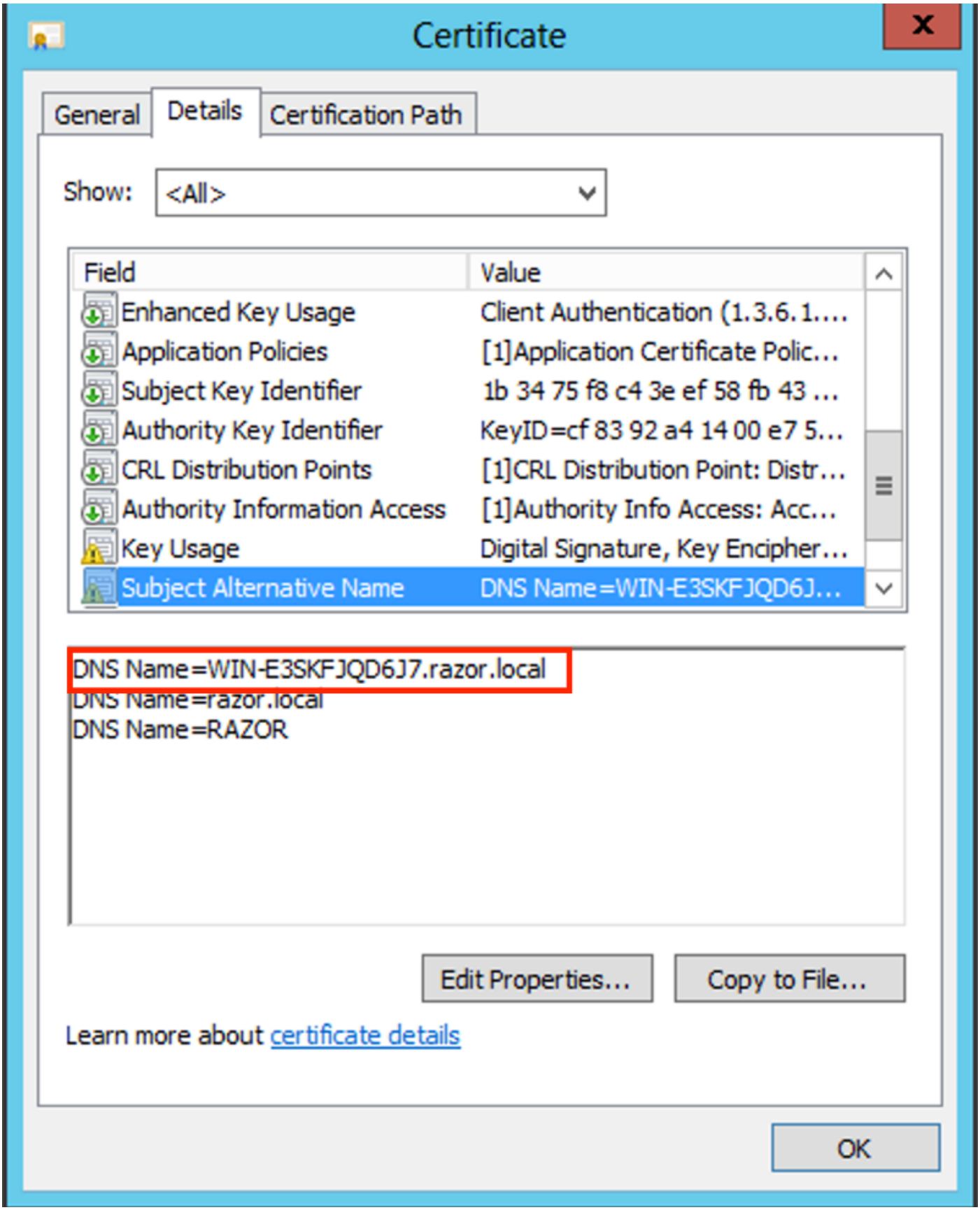
이 컨피그레이션 가이드에서 FQDN은 WIN-E3SKFJQD6J7.razor.local 따라서 처음 두 인증서는 LDAPs SSL 인증서로 사용할 수 없습니다. 발급된 ID 인증서 WIN-E3SKFJQD6J7.razor.local 은(는) Windows Server CA 서비스에서 자동으로 발급한 인증서입니다. 세부 정보를 확인하려면 인증서를 두 번 클릭합니다.



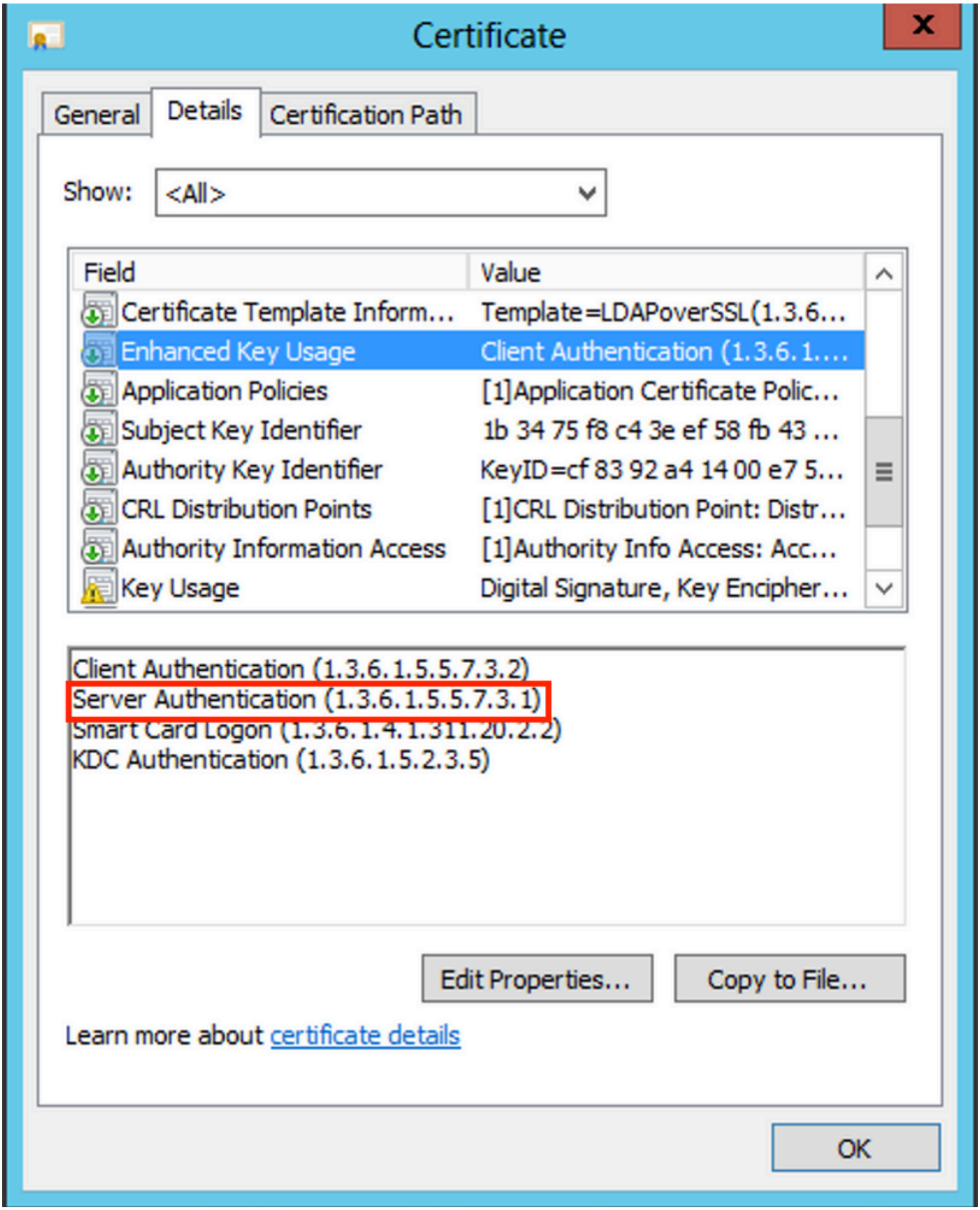
7. LDAPs SSL 인증서로 사용하려면 인증서가 다음 요구 사항을 충족해야 합니다.

- 공용 이름 또는 DNS 주체 대체 이름이 Windows Server의 FQDN과 일치합니다.
- 인증서에는 Enhanced Key Usage(고급 키 사용) 필드 아래에 서버 인증이 있습니다.

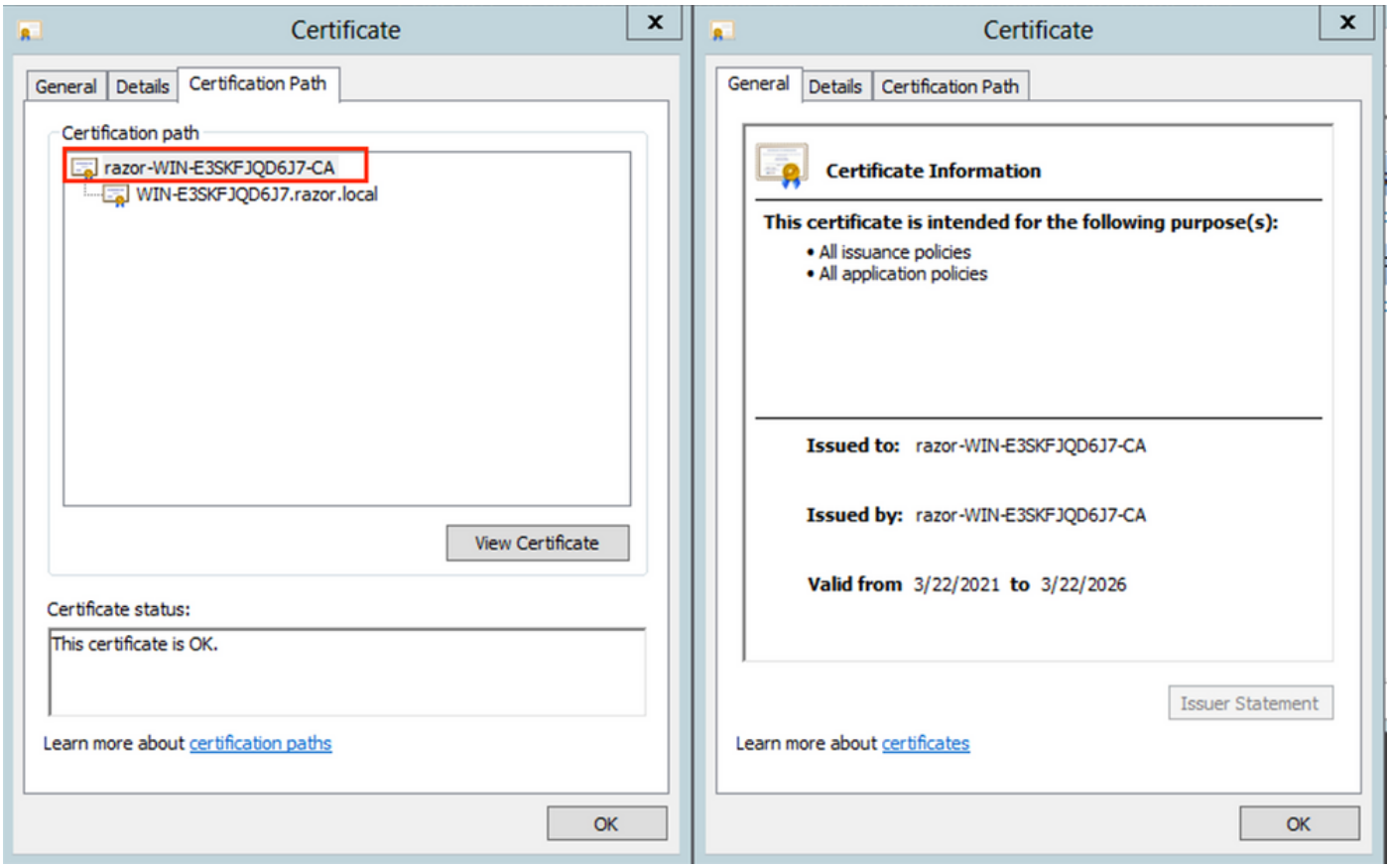
아래 Details 인증서의 탭에서 Subject Alternative Name여기서 FQDN은 WIN-E3SKFJQD6J7.razor.local 이(가) 있습니다.



아래 Enhanced Key Usage, Server Authentication 이(가) 있습니다.

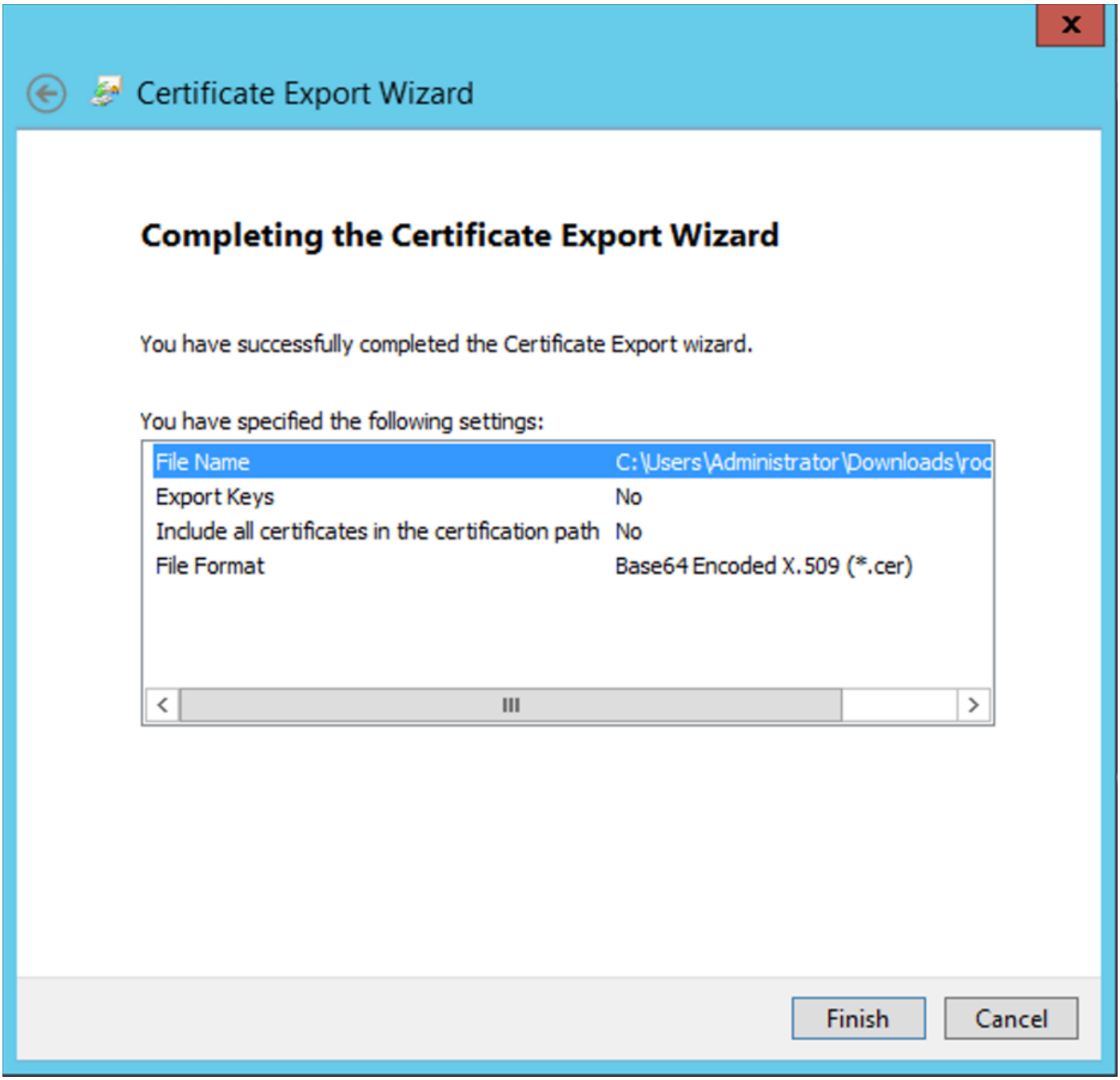


8. 확인되시면, Certification Path 탭에서 루트 CA 인증서인 최상위 인증서를 선택한 다음 View Certificate. 그러면 이미지에 표시된 것처럼 루트 CA 인증서에 대한 인증서 세부사항이 열립니다.



9. 아래 Details 루트 CA 인증서의 탭에서 Copy to File Cisco의Certificate Export Wizard PEM 형식으로 루트 CA를 내보냅니다.

선택 Base-64 encoded X.509 파일 형식으로



10. 메모장이나 다른 텍스트 편집기를 사용하여 시스템의 선택한 위치에 저장된 루트 CA 인증서를 엽니다.

PEM 형식 인증서가 표시됩니다. 나중에 사용할 수 있도록 저장하십시오.

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

LDAP 서버의 로컬 컴퓨터 저장소에 여러 인증서가 설치된 경우(선택 사항)

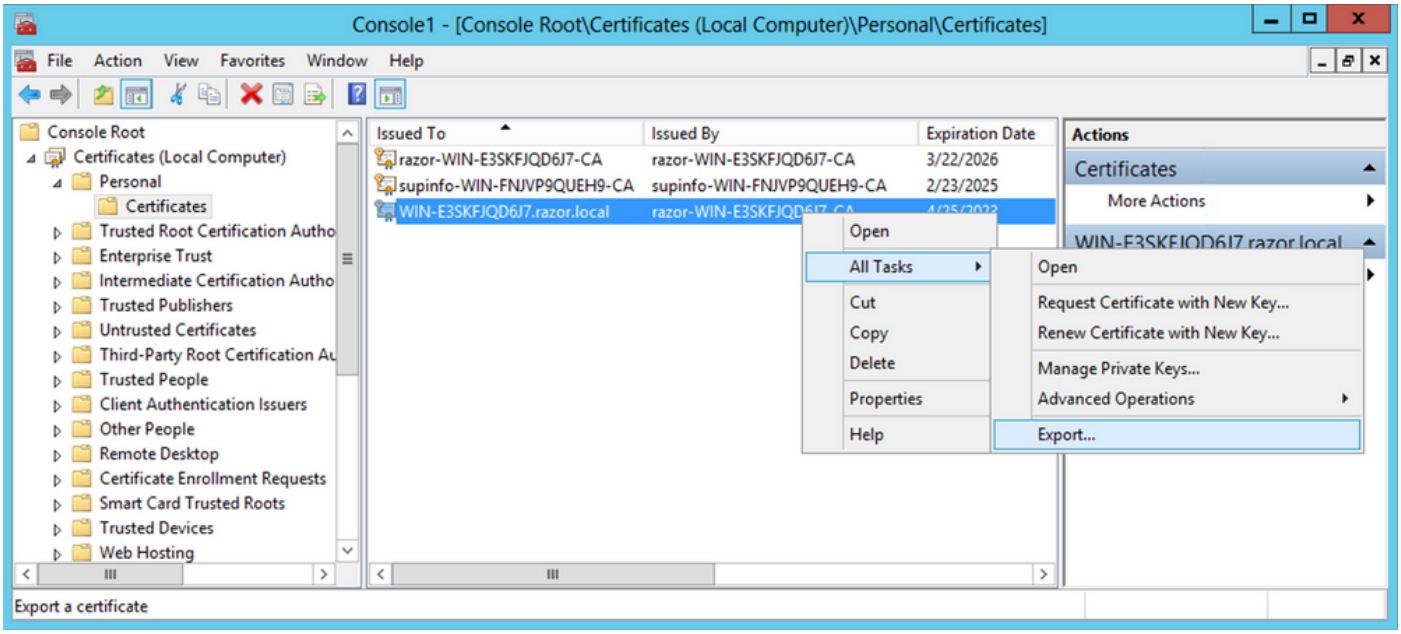
1. LDAPS에서 사용 할 수 있는 여러 ID 인증서의 경우 및 사용 할 수 있는 불확실성이 있거나 LDAPS 서버에 액세스 할 수 없는 경우, FTD에서 수행 한 패킷 캡처에서 루트 CA를 추출 할 수 있습니다.

2. LDAP 서버(예: AD DS 도메인 컨트롤러) 로컬 컴퓨터 인증서 저장소에 서버 인증에 유효한 인증서가 여러 개 있는 경우 LDAPS 통신에 다른 인증서가 사용된다는 것을 알 수 있습니다. 이러한 문제의 가장 좋은 해결책은 로컬 컴퓨터 인증서 저장소에서 불필요한 인증서를 모두 제거하고 서버 인증에 유효한 인증서를 하나만 갖는 것입니다.

그러나 둘 이상의 인증서가 필요하고 Windows Server 2008 LDAP 서버가 하나 이상 있는 합당한 이유가 있는 경우 LDAP 통신에 Active Directory 도메인 서비스(NTDS\개인) 인증서 저장소를 사용할 수 있습니다.

이 단계에서는 도메인 컨트롤러 로컬 컴퓨터 인증서 저장소에서 Active Directory 도메인 서비스 서비스 인증서 저장소(NTDS\Personal)로 LDAPS 지원 인증서를 내보내는 방법을 보여 줍니다.

- Active Directory 서버에서 MMC 콘솔로 이동하여 파일을 선택한 다음 Add/Remove Snap-in.
- 클릭 Certificates 다음을 클릭합니다. Add.
- 의 Certificates snap-in, 선택 Computer account 다음을 클릭합니다. Next.
- 수신 Select Computer, 선택 Local Computer, 클릭 OK을 클릭한 다음 Finish. 수신 Add or Remove Snap-ins, 클릭 OK.
- 서버 인증에 사용되는 인증서가 들어 있는 컴퓨터의 인증서 콘솔에서 certificate, 클릭 All Tasks을 클릭한 다음 Export.

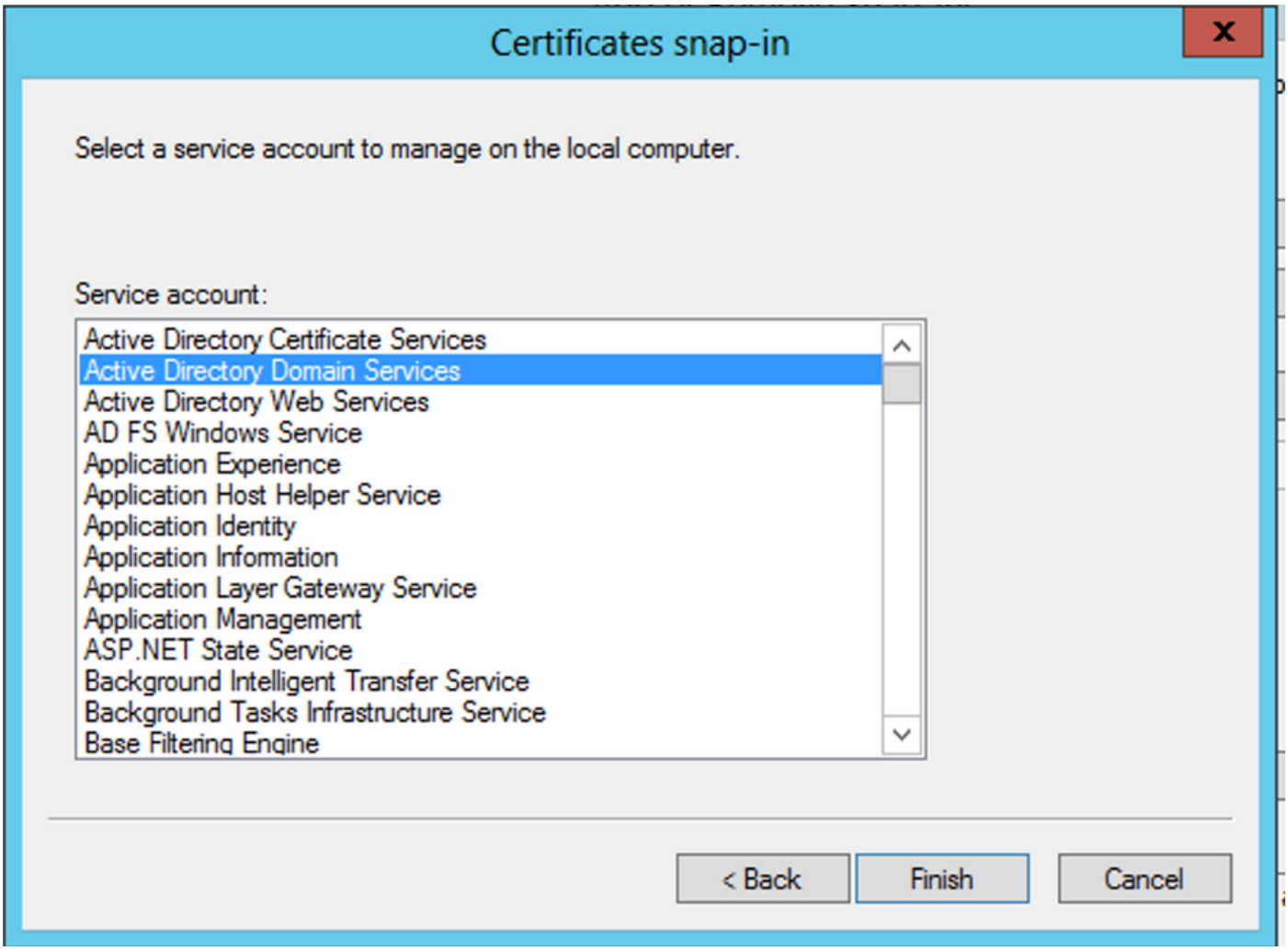


- 에서 인증서 내보내기 pfx 다음 섹션에서 형식을 지정합니다. 에서 인증서를 내보내는 방법에 대한 이 문서를 참조하십시오. pfx MMC에서 형식:

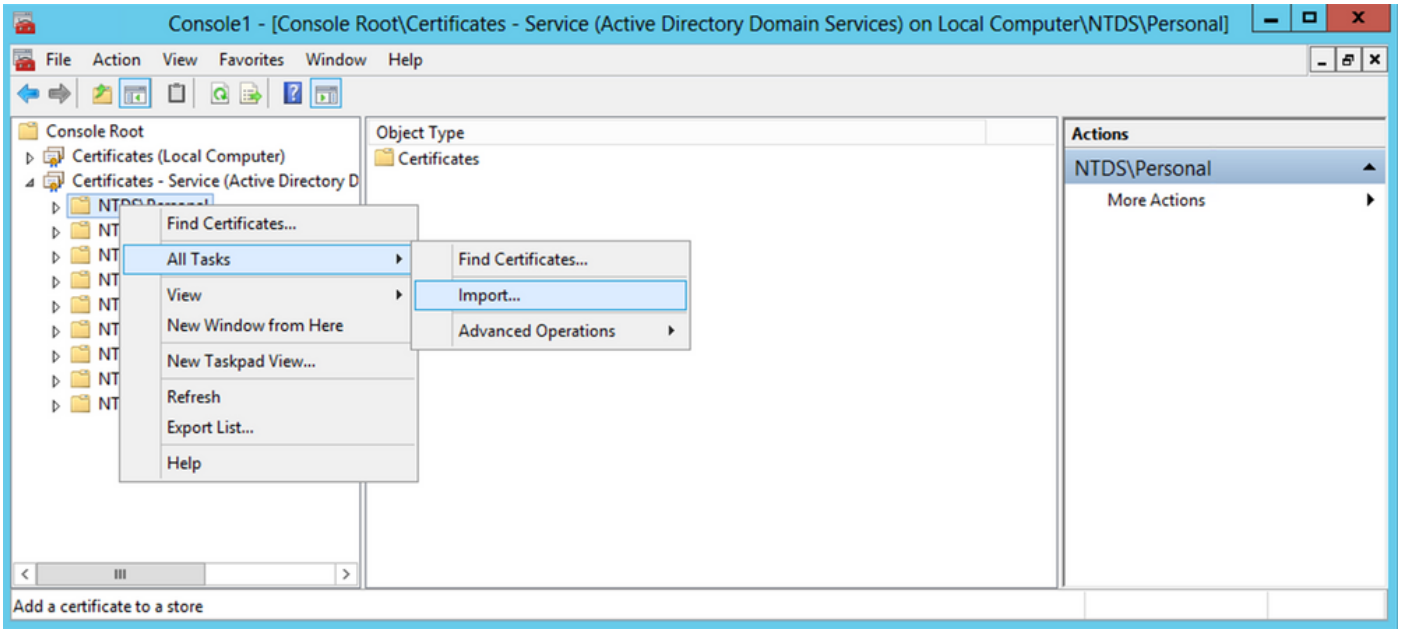
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html

- 인증서 내보내기가 완료되면 Add/Remove Snap-in on MMC console. 클릭 Certificates 다음을 클릭합니다. Add.
- 선택 Service account 다음을 클릭합니다. Next.

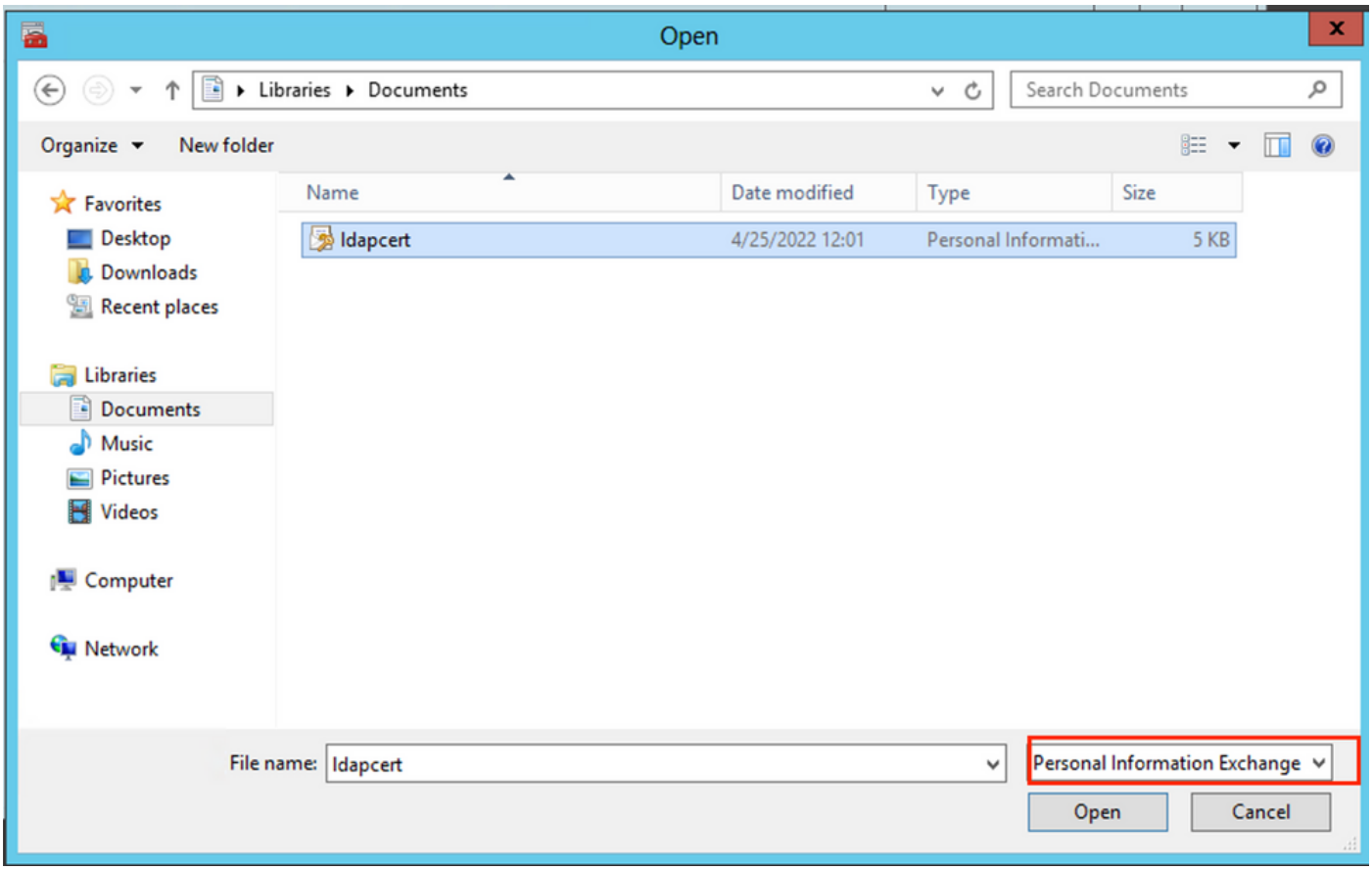
- 의 Select Computer 대화 상자에서 Local Computer 을 클릭하고 Next.
- 선택 Active Directory Domain Services 다음을 클릭합니다. Finish.



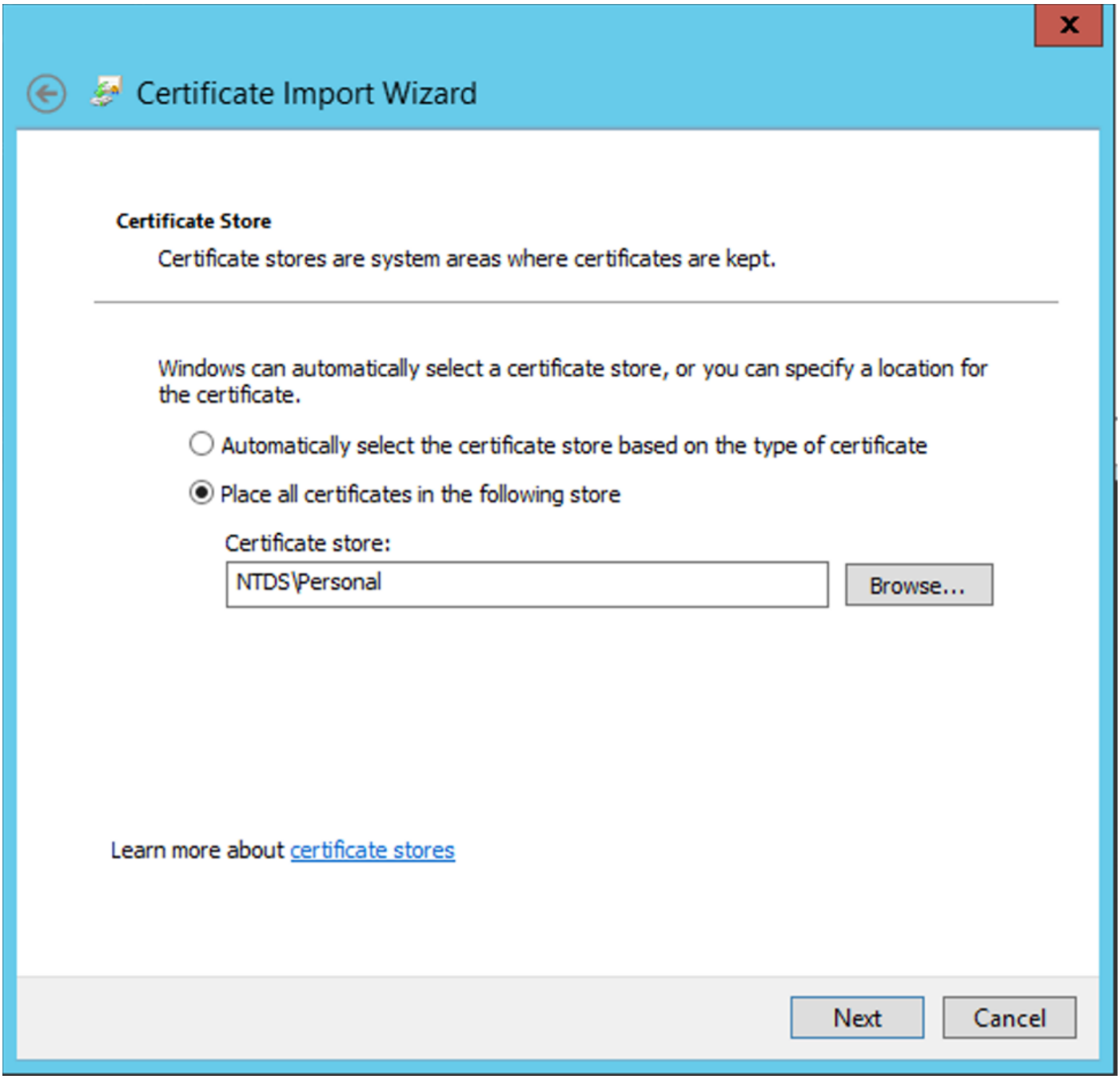
- 에 Add/Remove Snap-ins 대화 상자에서 OK.
- Expand Certificates - Services (Active Directory Domain Services) 다음을 클릭합니다. NTDS\Personal.
- 마우스 오른쪽 단추 클릭 NTDS\Personal, 클릭 All Tasks을 클릭한 다음 Import.



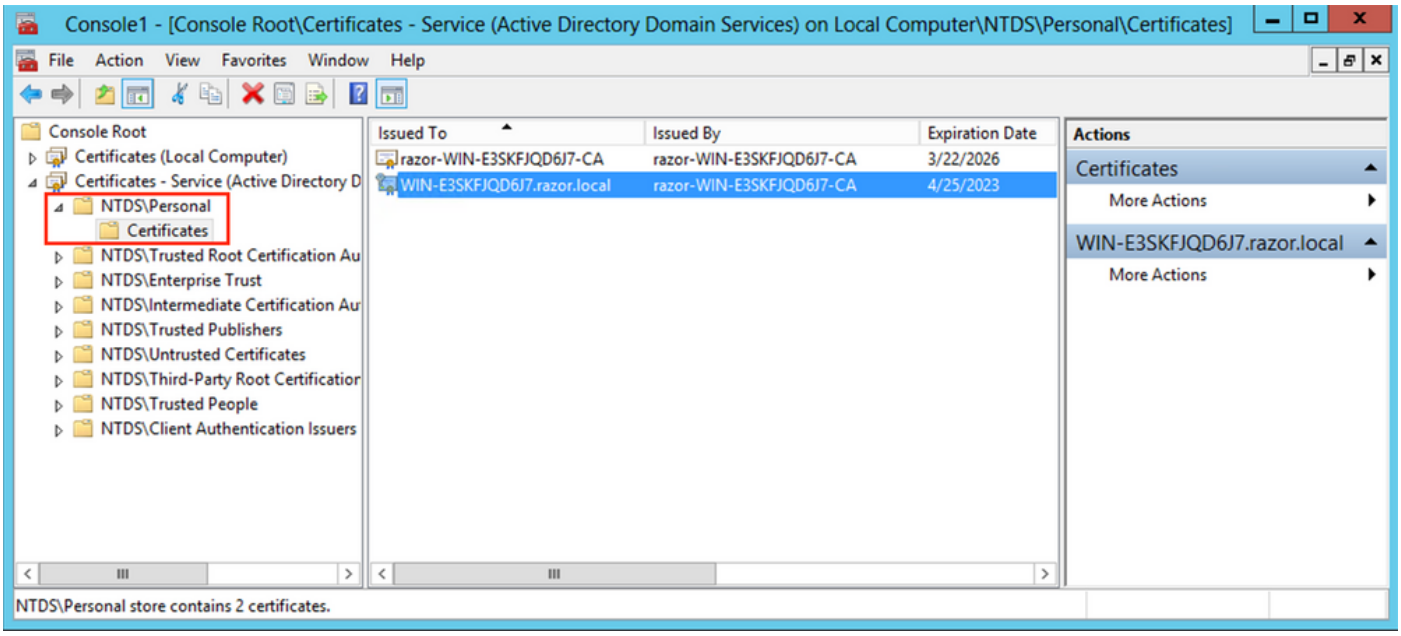
- 에 Certificate Import Wizard 시작 화면에서 Next.
- 가져올 파일 화면에서 Browse을 누르고 이전에 내보낸 인증서 파일을 찾습니다.
- Open(열기) 화면에서 개인 정보 교환(*pfx,*.p12)가 파일 유형으로 선택된 다음 파일 시스템을 탐색하여 이전에 내보낸 인증서를 찾습니다. 그런 다음 해당 인증서를 클릭합니다.



- 클릭 Open 다음을 클릭합니다. Next.
- 암호 화면에서 파일에 대해 설정한 암호를 입력한 다음 Next.
- Certificate Store(인증서 저장소) 페이지에서 Place all certificates(모든 인증서 가져오기)가 선택되어 있는지 확인하고 Certificate Store(인증서 저장소)를 읽습니다. NTDS\Personal 다음을 클릭합니다. Next.



- 에 Certificate Import Wizard 완료 화면에서 Finish. 그러면 가져오기가 성공했다는 메시지가 표시됩니다. 클릭 OK. 다음과 같이 인증서 저장소 아래에서 인증서를 가져왔습니다. NTDS\Personal.



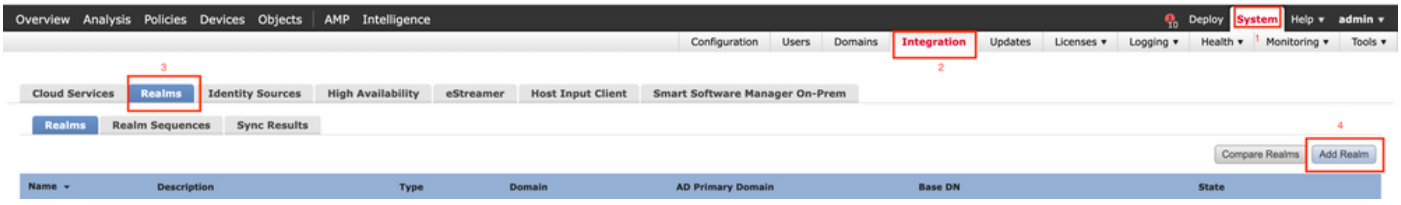
FMC 컨피그레이션

라이센싱 확인

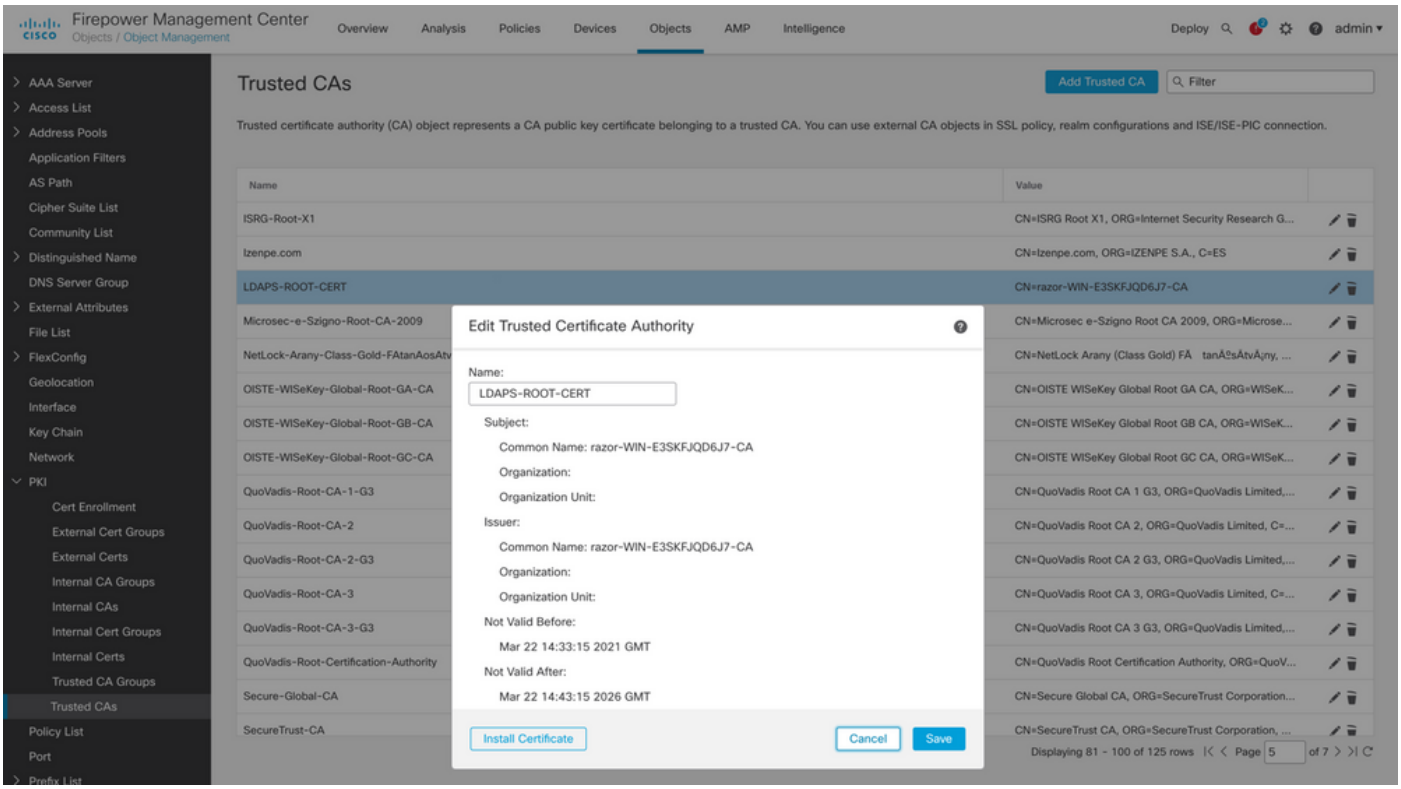
AnyConnect 컨피그레이션을 구축하려면 FTD를 Smart Licensing Server에 등록하고 유효한 Plus, Apex 또는 VPN Only 라이센스를 디바이스에 적용해야 합니다.

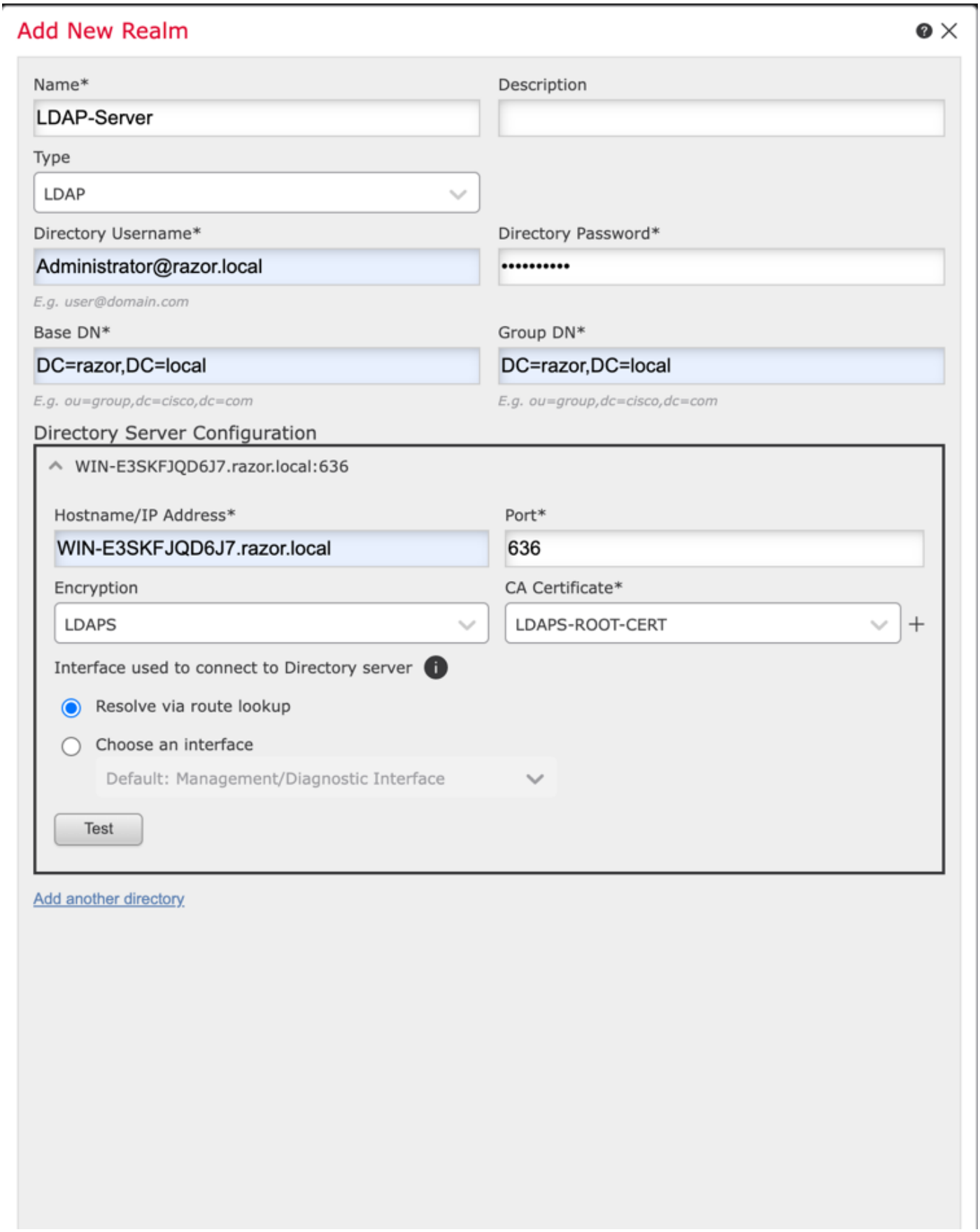
영역 설정

1. 탐색 System > Integration. 탐색 Realms를 클릭한 다음 Add Realm, 이 이미지에 표시된 대로



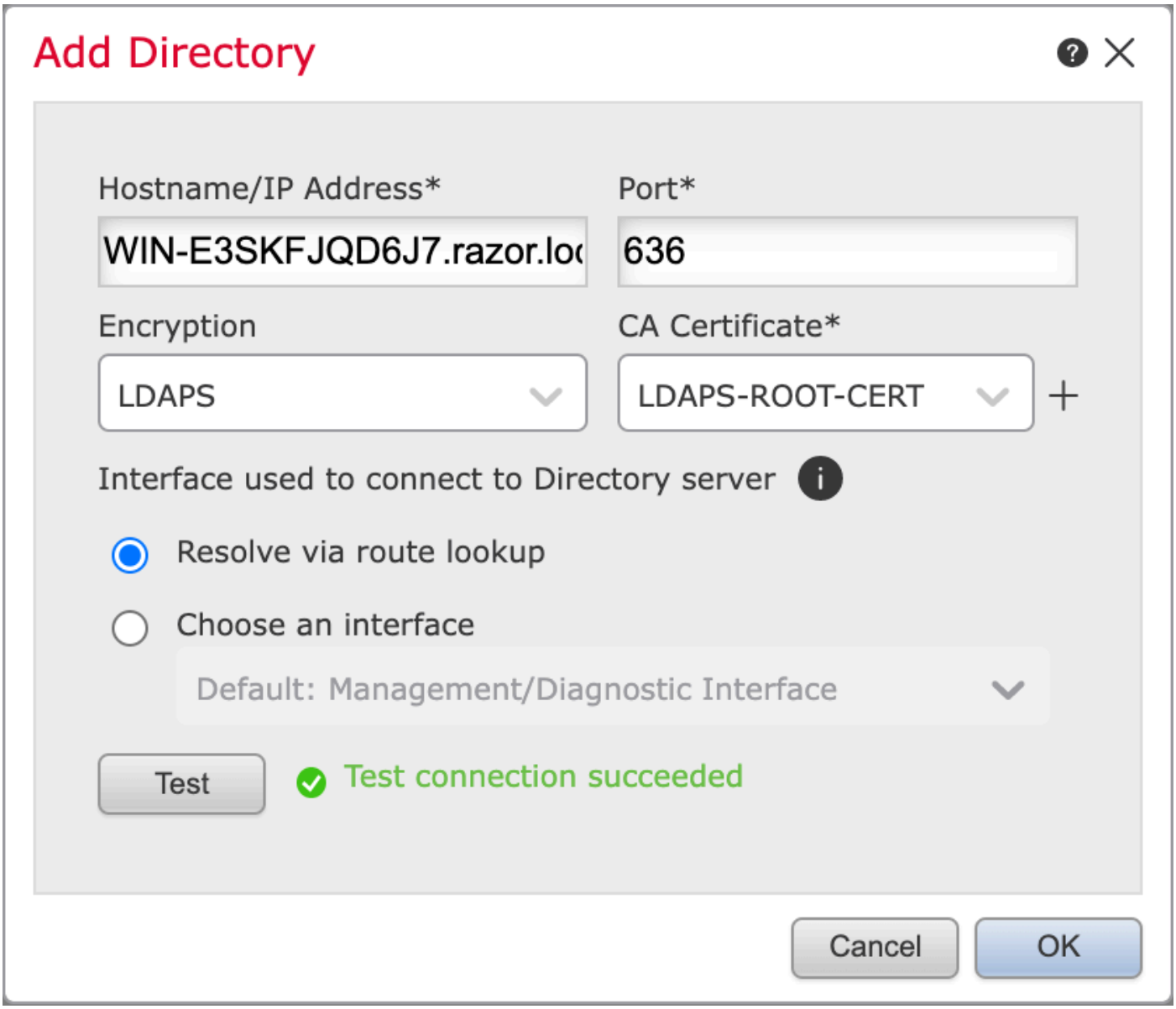
2. LDAP용 Microsoft 서버에서 수집된 정보를 기반으로 표시된 필드를 입력합니다. 이 전에 Windows Server의 LDAP 서비스 인증서에 서명한 루트 CA 인증서를 Objects > PKI > Trusted CAs > Add Trusted CA에서 참조되는 대로Directory Server Configuration Realm의 약어입니다 작업을 마치면 OK.


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

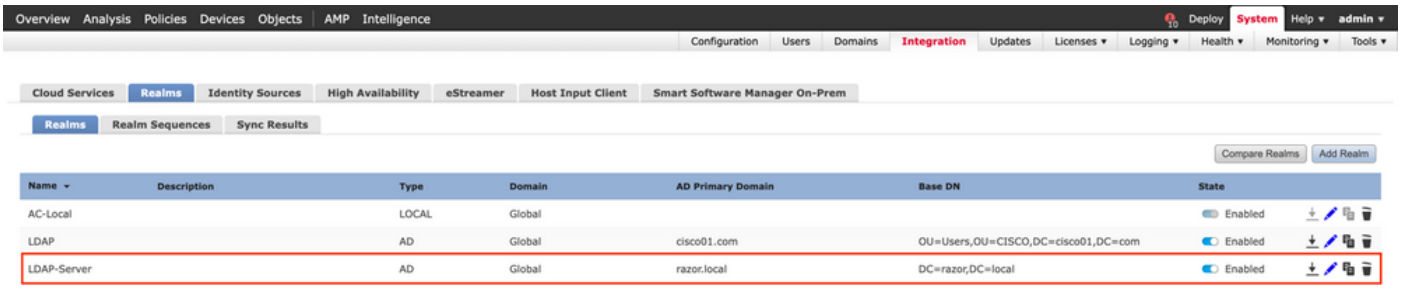


3. 클릭 Test FMC가 이전 단계에서 제공한 디렉토리 사용자 이름 및 비밀번호로 성공적으로 바인딩할 수 있도록 하려면 다음을 수행합니다. 이러한 테스트는 FTD에 구성된 라우팅 가능한 인터페이스(예: 내부, 외부, dmz)를 통하지 않고 FMC에서 시작되므로, AnyConnect LDAP 인증 요청이 FTD 라우팅 가능한 인터페이스 중 하나에서 시작되므로 연결에 성공하거나 실패하더

라도 AnyConnect 인증에 대한 동일한 결과가 보장되지 않습니다.

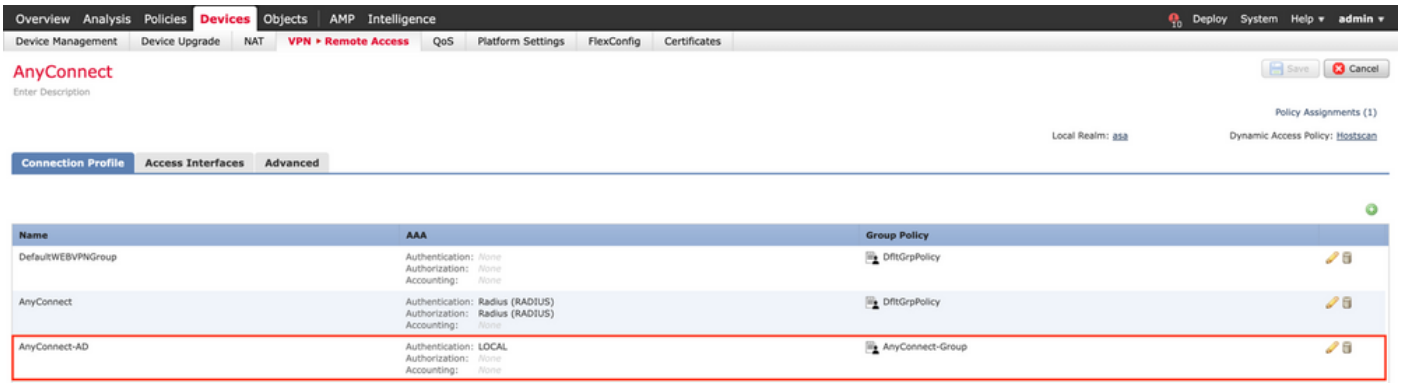


4. 새 영역을 활성화합니다.

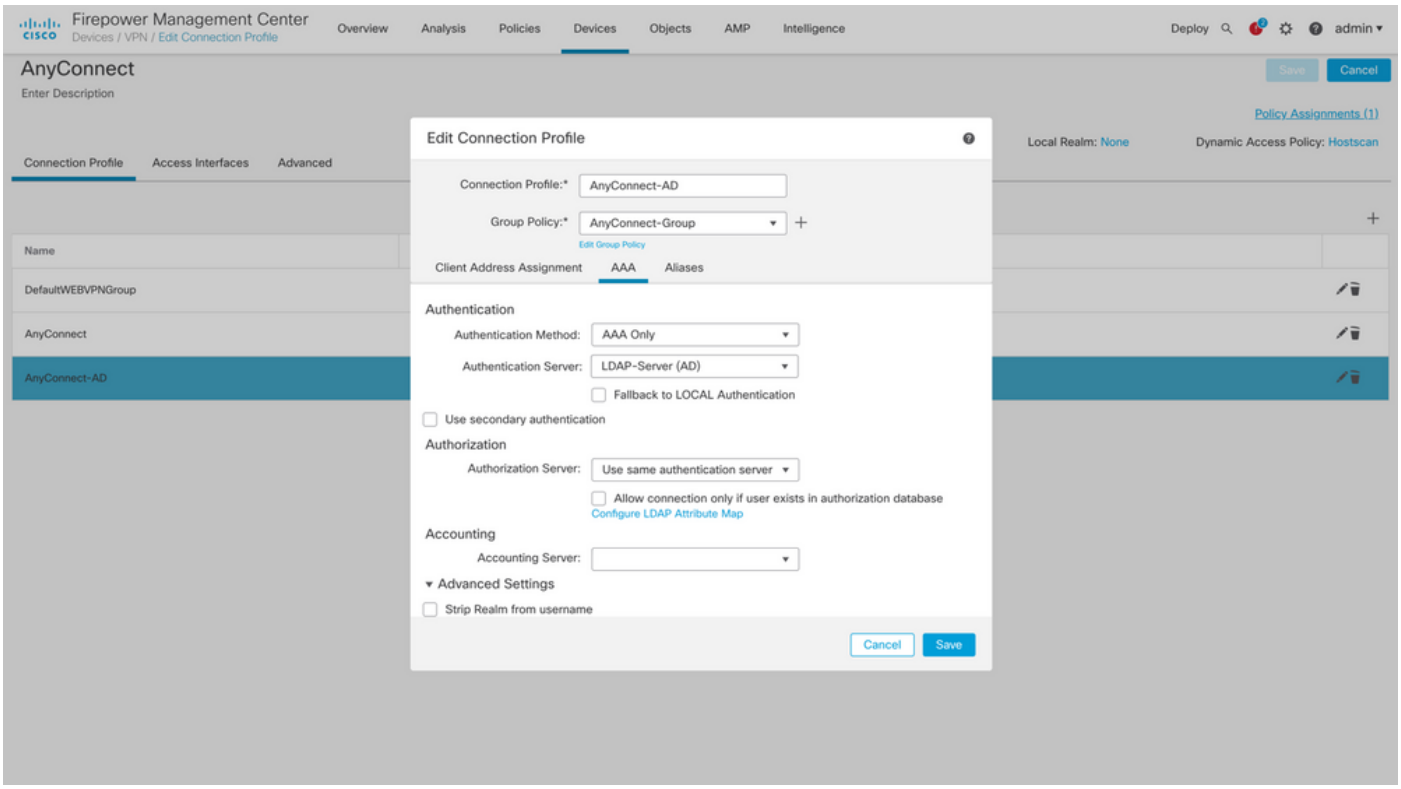


비밀번호 관리를 위한 AnyConnect 구성

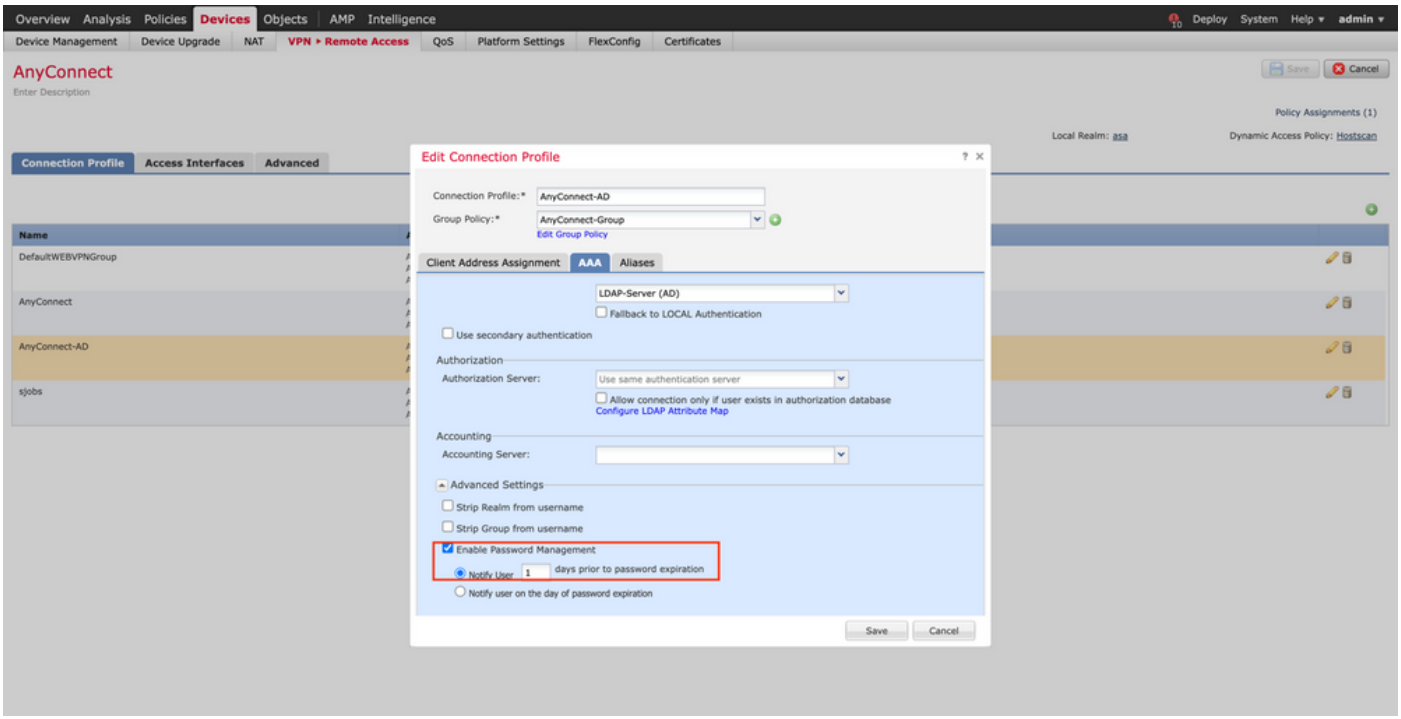
1. AnyConnect의 초기 설정인 경우 기존 연결 프로파일을 선택하거나 새 프로파일을 생성합니다. 여기서는 로컬 인증과 매핑된 'AnyConnect-AD'라는 기존 연결 프로파일을 사용합니다.



2. 연결 프로파일을 편집하고 이전 단계에서 구성한 새 LDAP 서버를 연결 프로파일의 AAA 설정에서 매핑합니다. 작업을 마치면 Save 오른쪽 상단 구석에 있습니다



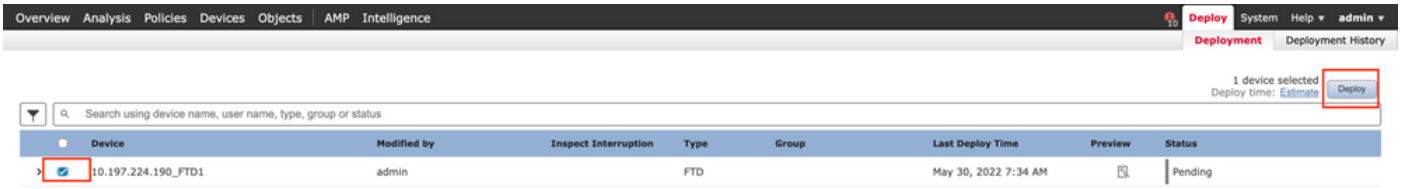
3. 비밀번호 관리 활성화 AAA > Advanced Settings 구성을 저장합니다.



구축

1. 모든 컨피그레이션이 완료되면Deploy 버튼을 누르시면 됩니다.

2. 적용된 FTD 컨피그레이션 옆의 확인란을 클릭한 다음 Deploy, 이 이미지에 표시된 대로



최종 컨피그레이션

성공적인 구축 후 FTD CLI에 표시되는 컨피그레이션입니다.

AAA 컨피그레이션

<#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 컨피그레이션

<#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
```

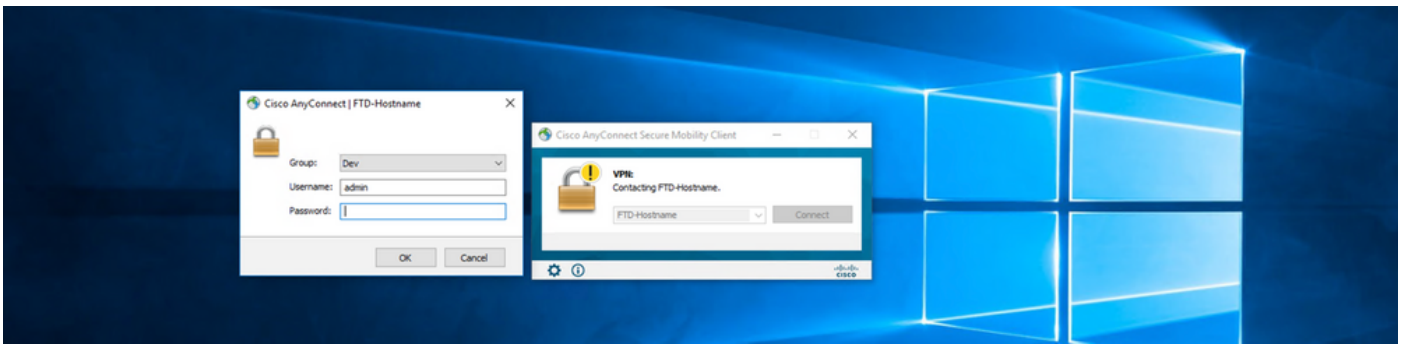
```
tunnel-group AnyConnect-AD type remote-access
tunnel-group AnyConnect-AD general-attributes
 address-pool Pool-1
authentication-server-group LDAP-Server                                    <-------- LDAPs Serve

 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
```

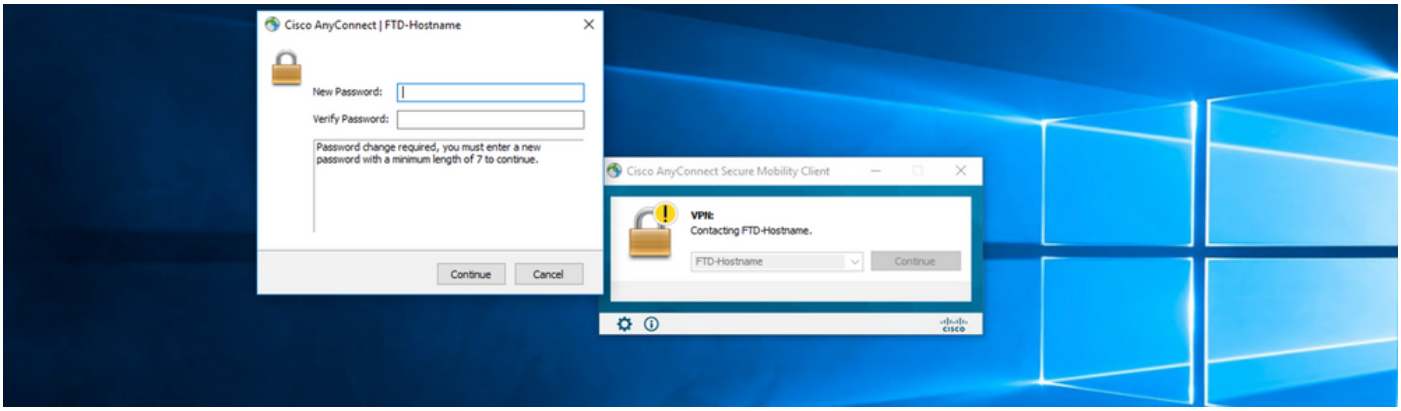
```
 default-domain none
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private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

확인

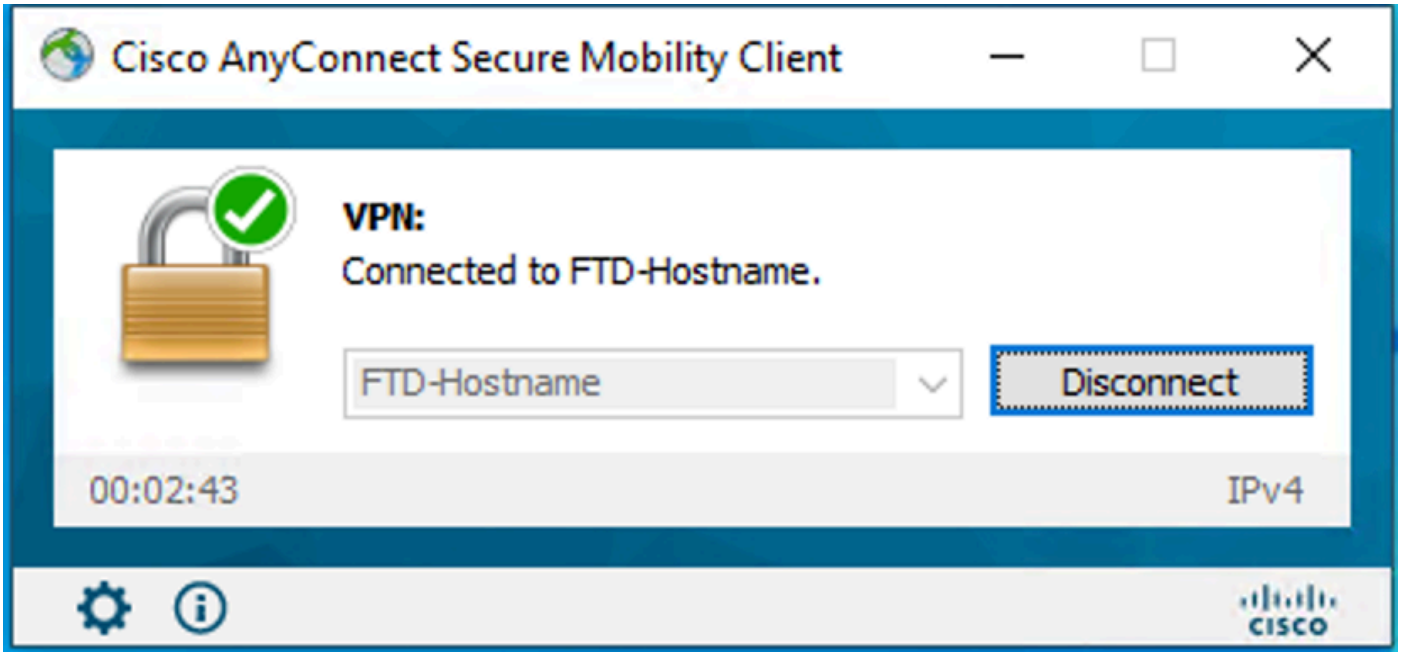
AnyConnect에 연결하고 사용자 연결에 대한 비밀번호 관리 프로세스 확인

1. 관련 연결 프로파일에 대한 연결을 시작합니다. 최초 로그인 시 이전 비밀번호가 만료되어 Microsoft Server에서 거부되었으므로 비밀번호를 변경해야 한다고 판단되면 사용자에게 비밀번호 변경 프롬프트가 표시됩니다.





2. 사용자가 로그인을 위해 새 비밀번호를 입력하면 연결이 성공적으로 설정됩니다.



3. FTD CLI에서 사용자 연결을 확인합니다.

<#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

문제 해결

디버그

이 디버그는 진단 CLI에서 실행하여 비밀번호 관리 관련 문제를 해결할 수 있습니다. debug ldap 255.

작동 중인 비밀번호 관리 디버그

<#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

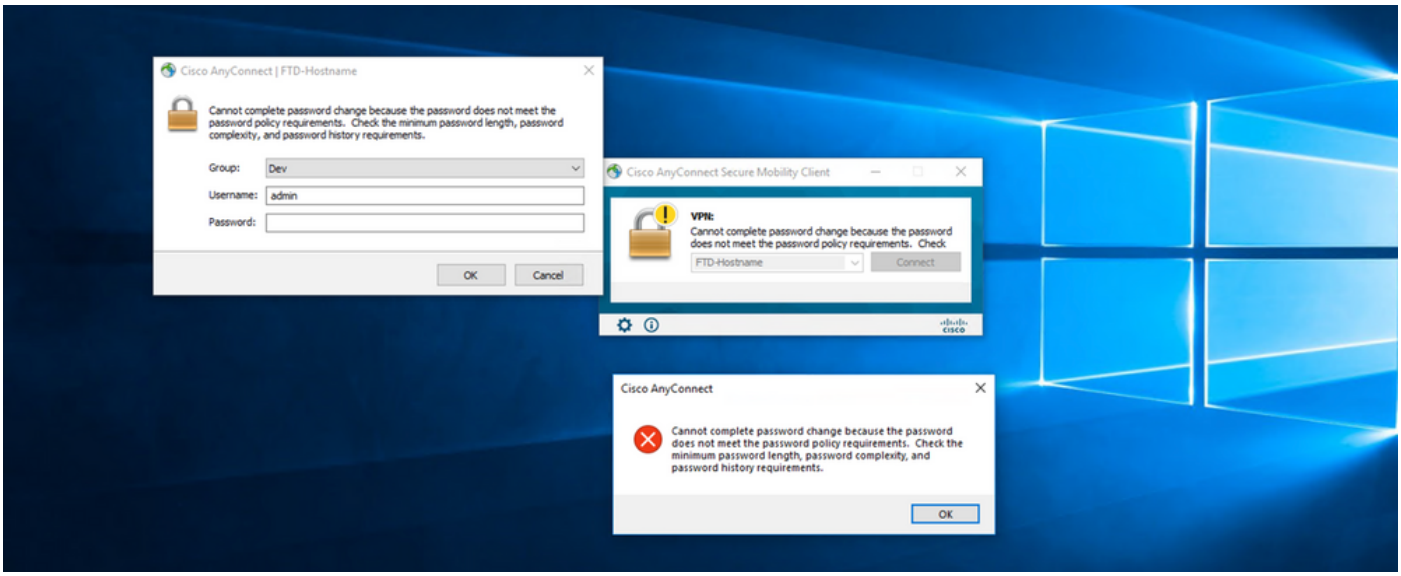
[25] badPasswordTime: value = 132610388348662803

[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
```

비밀번호 관리 중에 발생하는 일반적인 오류

일반적으로 사용자가 새 암호를 제공하는 동안 Microsoft Server에서 설정한 암호 정책이 충족되지 않으면 "암호가 암호 정책 요구 사항을 충족하지 않습니다."라는 오류 메시지와 함께 연결이 종료됩니다. 따라서 새 비밀번호가 LDAP에 대해 Microsoft Server에서 설정한 정책에 부합하는지 확인합니다.


Cisco AnyConnect | FTD-Hostname
Cannot complete password change because the password does not meet the password policy requirements. Check the minimum password length, password complexity, and password history requirements.
Group:
Dev
Username:
admin
Password:
OK
Cancel
Cisco AnyConnect Secure Mobility Client
VPN:
Cannot complete password change because the password does not meet the password policy requirements. Check
FTD-Hostname
Connect
Cisco AnyConnect
Cannot complete password change because the password does not meet the password policy requirements. Check the minimum password length, password complexity, and password history requirements.
OK

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.