在FMC管理的FTD上使用RA VPN的LDAP配置密码管理

目录

简介

本文档介绍如何使用LDAP为连接到思科Firepower威胁防御(FTD)的AnyConnect客户端配置密码管理。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 基本了解FMC上的RA VPN（远程访问虚拟专用网络）配置
- 基本了解FMC上的LDAP服务器配置

- Active Directory基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft 2012 R2服务器
- 运行7.3.0的FMCv
- 运行7.3.0的FTDv

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图和场景

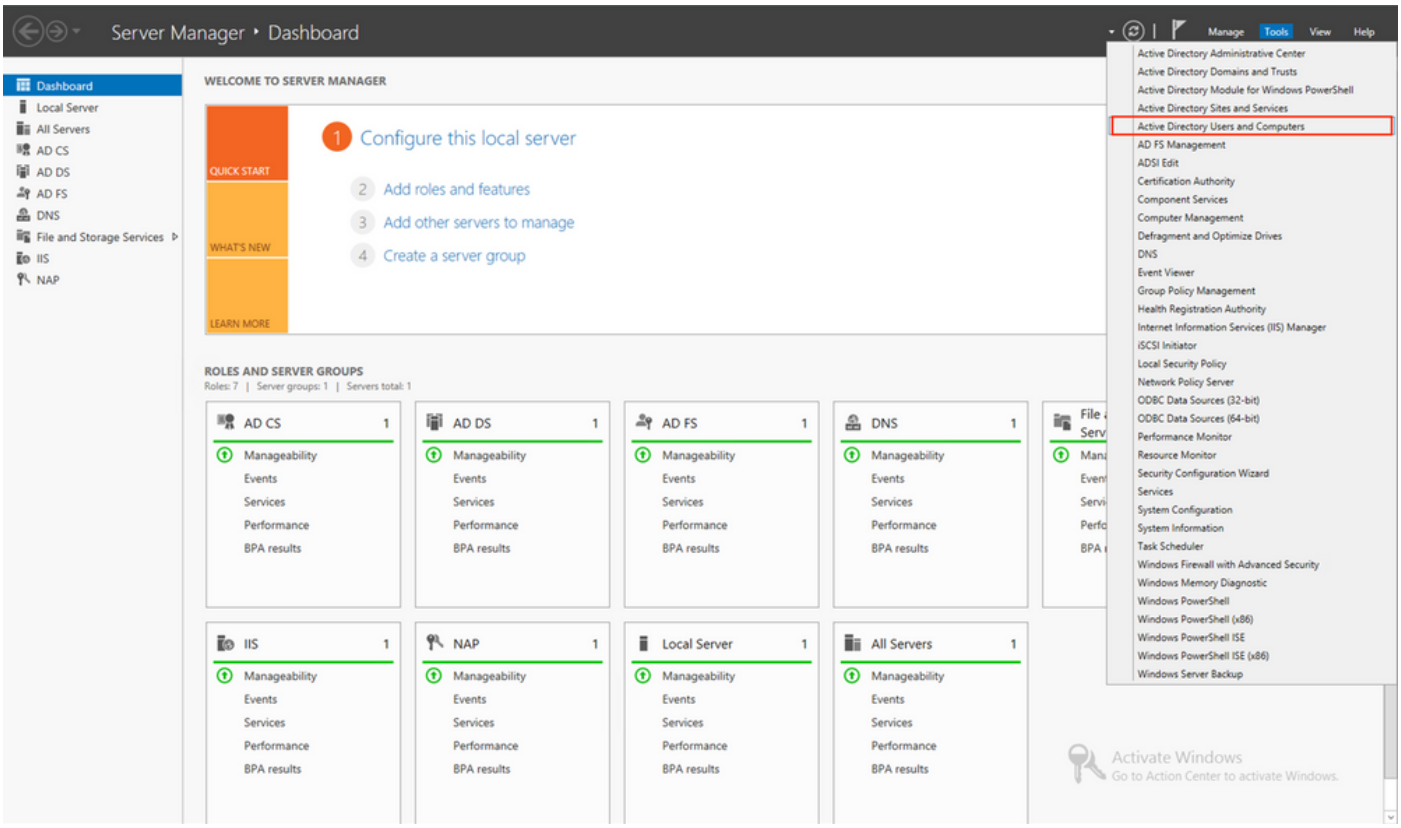
Windows服务器预配置了ADDS和ADCS以测试用户密码管理过程。在本配置指南中，将创建这些用户帐户。

用户帐户：

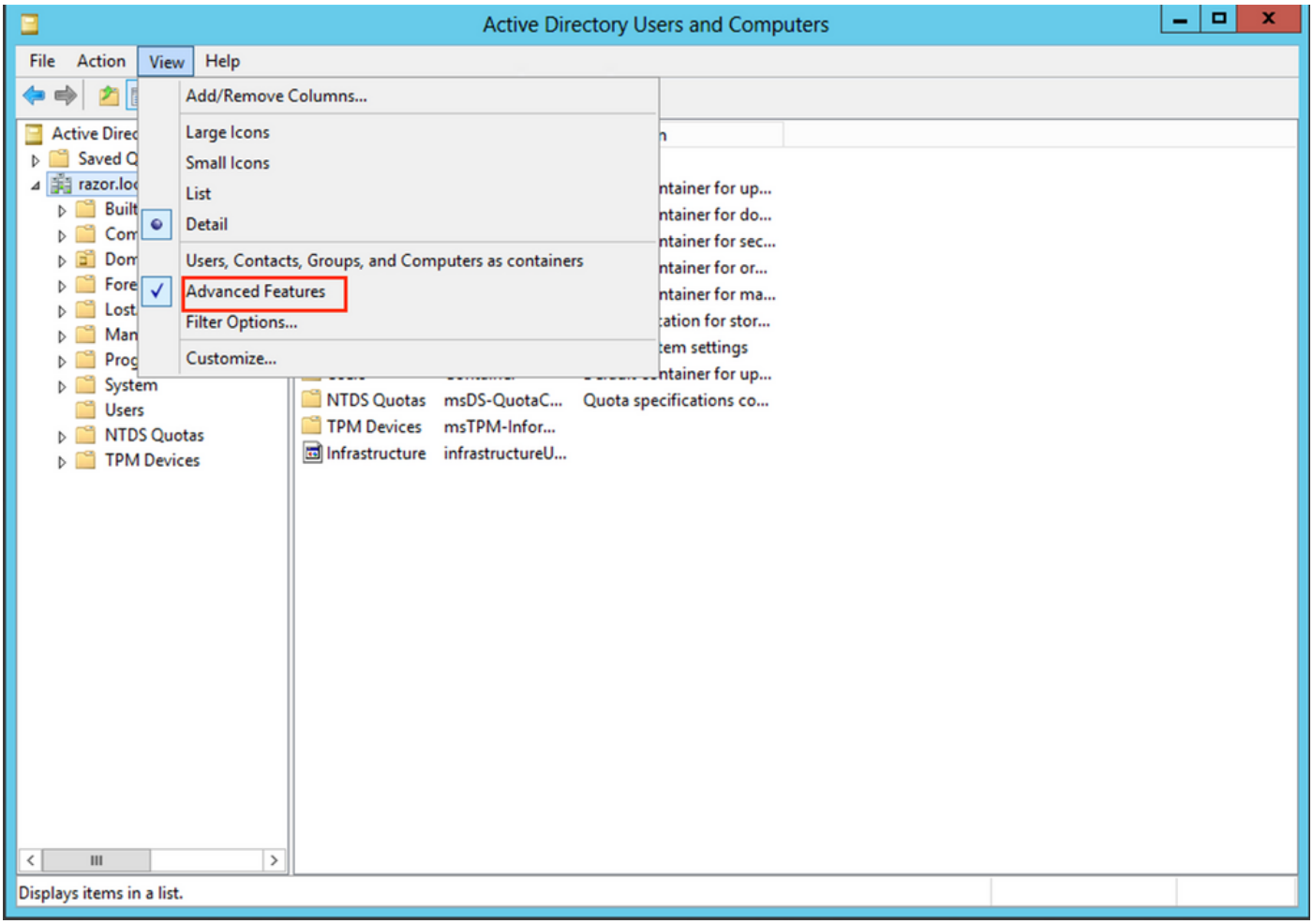
- 管理员：此帐户用作目录帐户，以允许FTD绑定到Active Directory服务器。
- admin：用于演示用户身份的测试管理员帐户。

确定LDAP基本DN和组DN

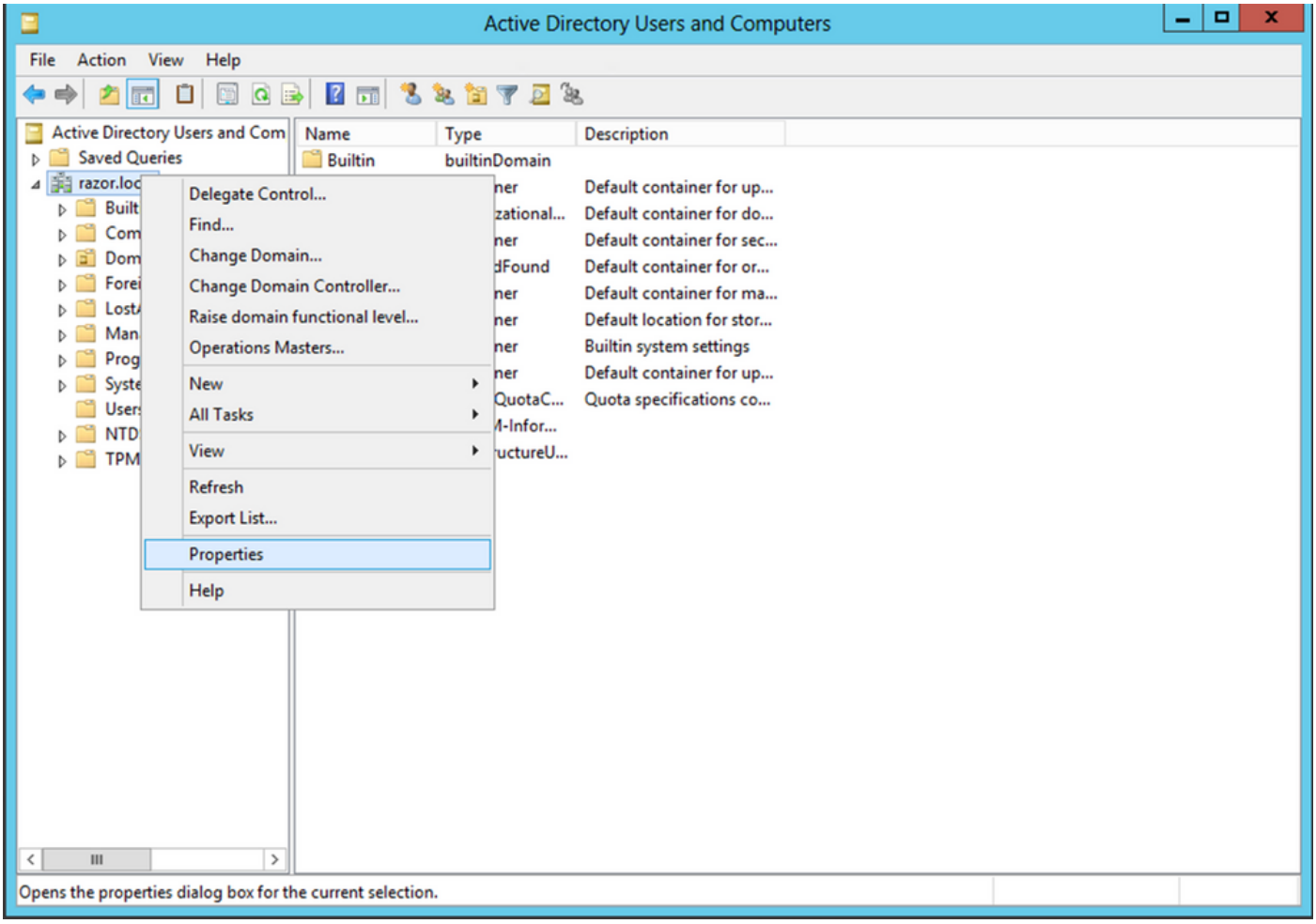
1. Open（未解决） Active Directory Users and Computers 通过服务器管理器控制面板。



2. 打开 View Option 并启用 Advanced Features,如图所示:



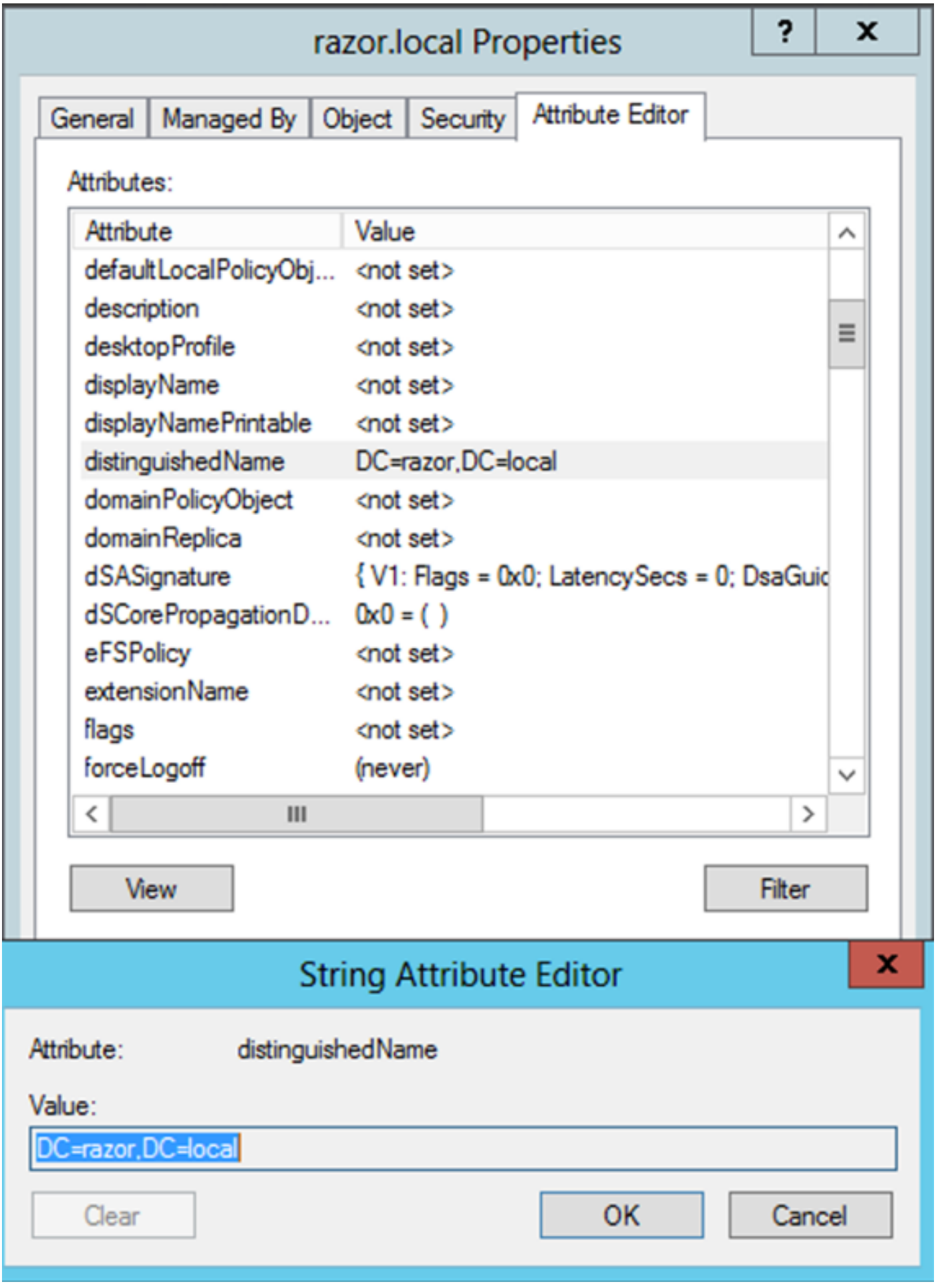
3. 这允许查看AD对象下的其他属性。
   例如，要查找根的DN， razor.local右键点击 razor.local，然后选择 Properties，如下图所示：



4. 低于 Properties，选择 Attribute Editor 选项卡。查找 distinguishedName 在Attributes下，单击 View,如图所示.

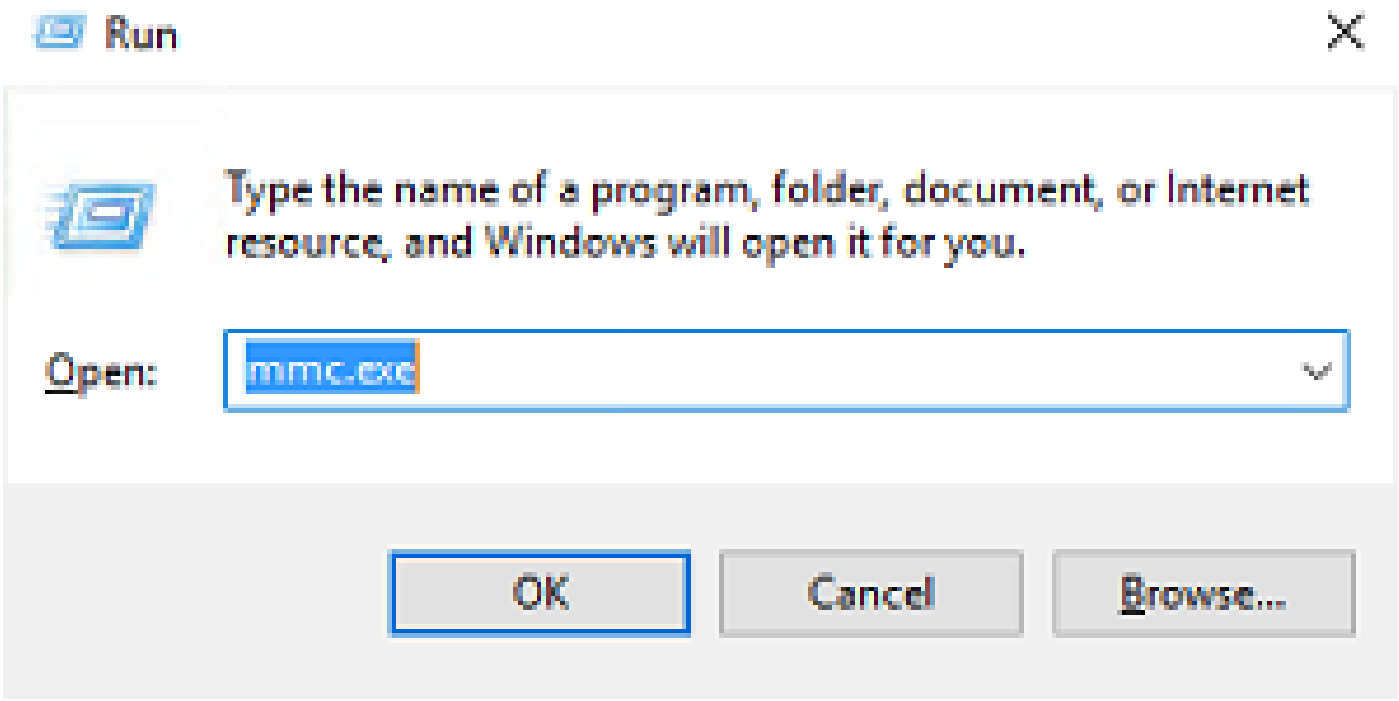
这将打开一个新窗口，可在其中复制DN并在以后粘贴到FMC。

在本示例中，根DN是 DC=razor, DC=local.复制该值并保存以备后用。点击 OK 要退出“字符串属性编辑器”窗口，请单击 OK 以退出属性。

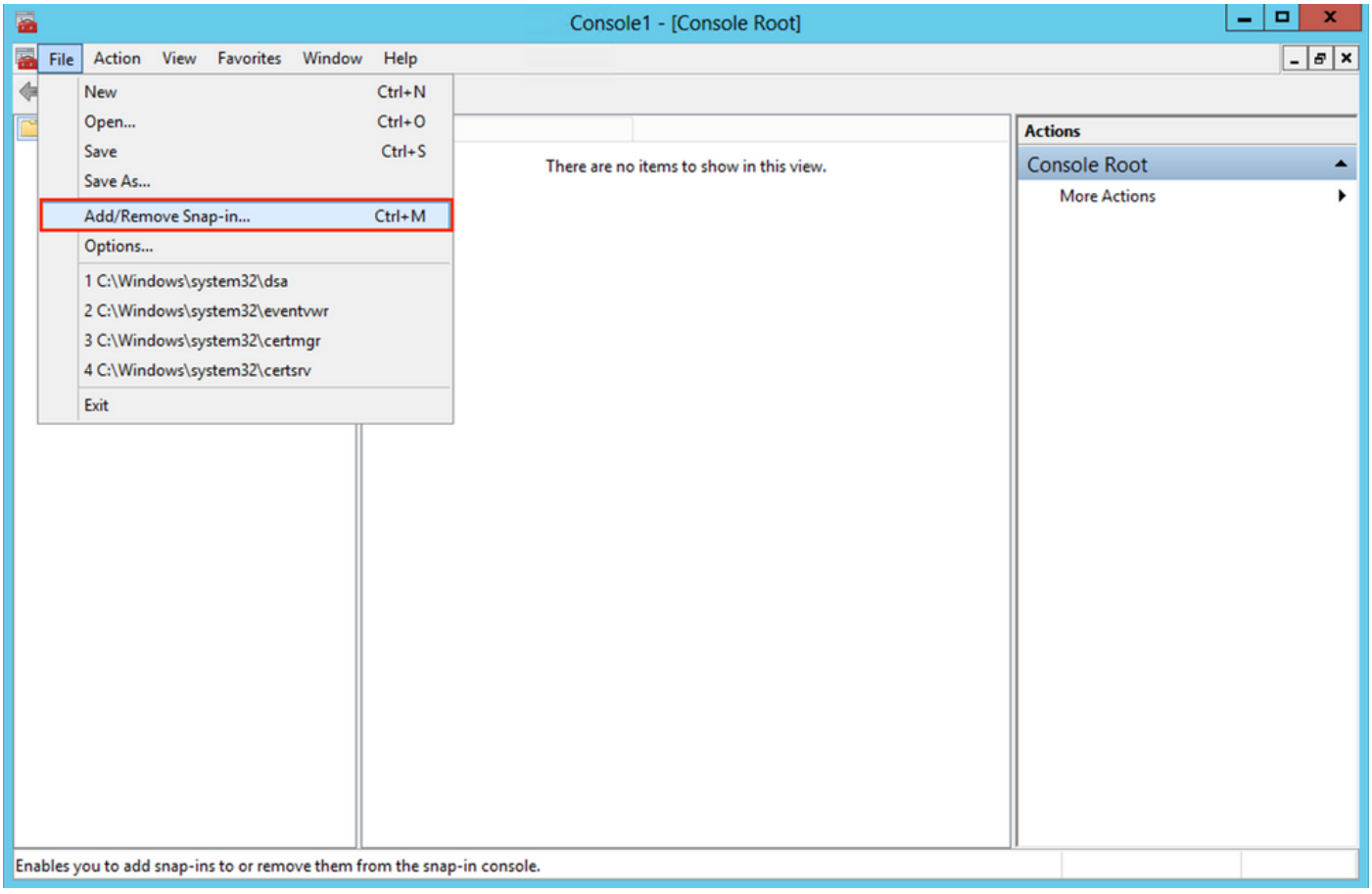

razor.local Properties
General
Managed By
Object
Security
Attribute Editor
Attributes:
Attribute
Value
defaultLocalPolicyObj...
<not set>
description
<not set>
desktopProfile
<not set>
displayName
<not set>
displayNamePrintable
<not set>
distinguishedName
DC=razor,DC=local
domainPolicyObject
<not set>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

复制LDAPS SSL证书根

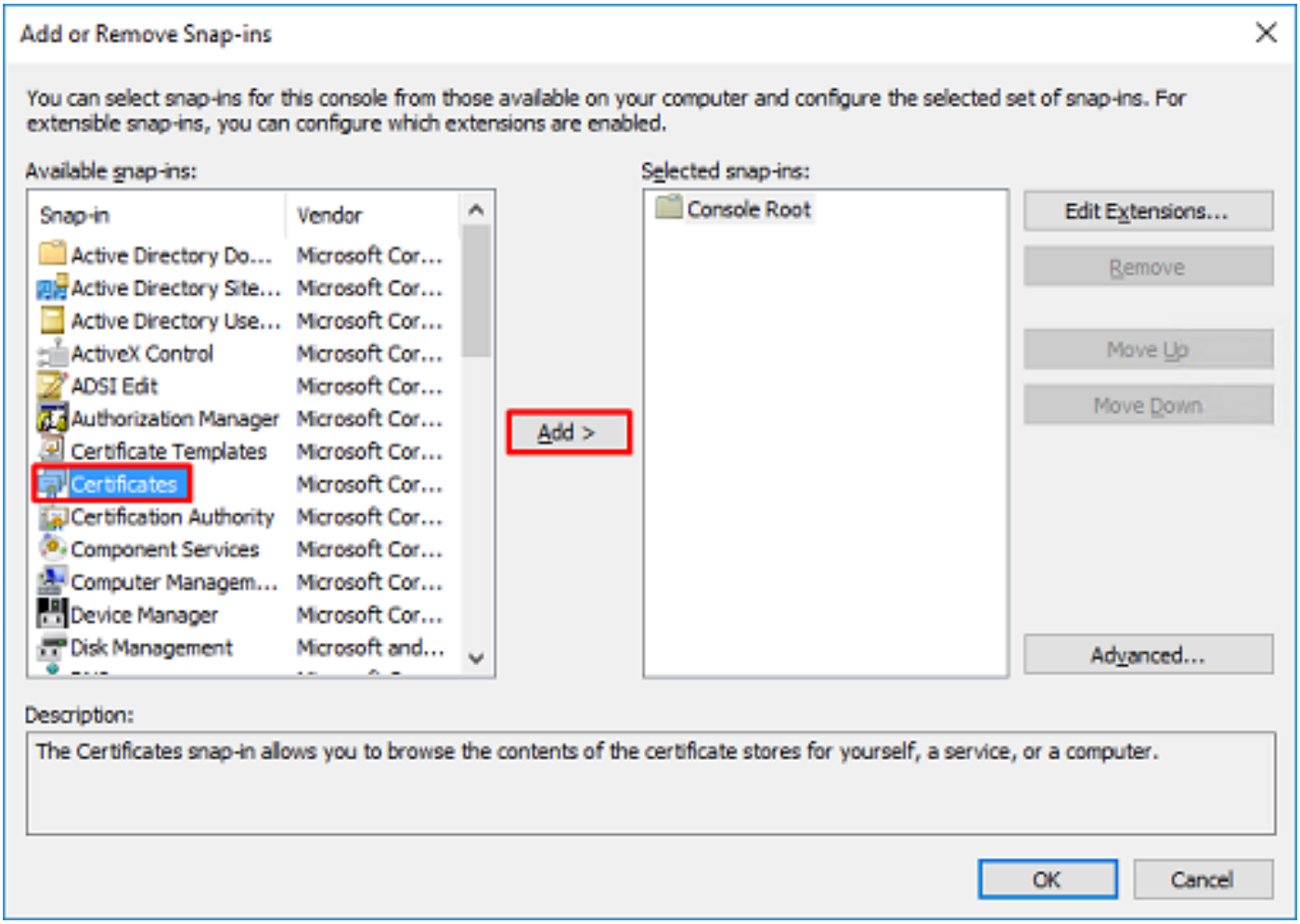
1. 按 Win+R 并输入 mmc.exe，然后单击 OK，如图所示。



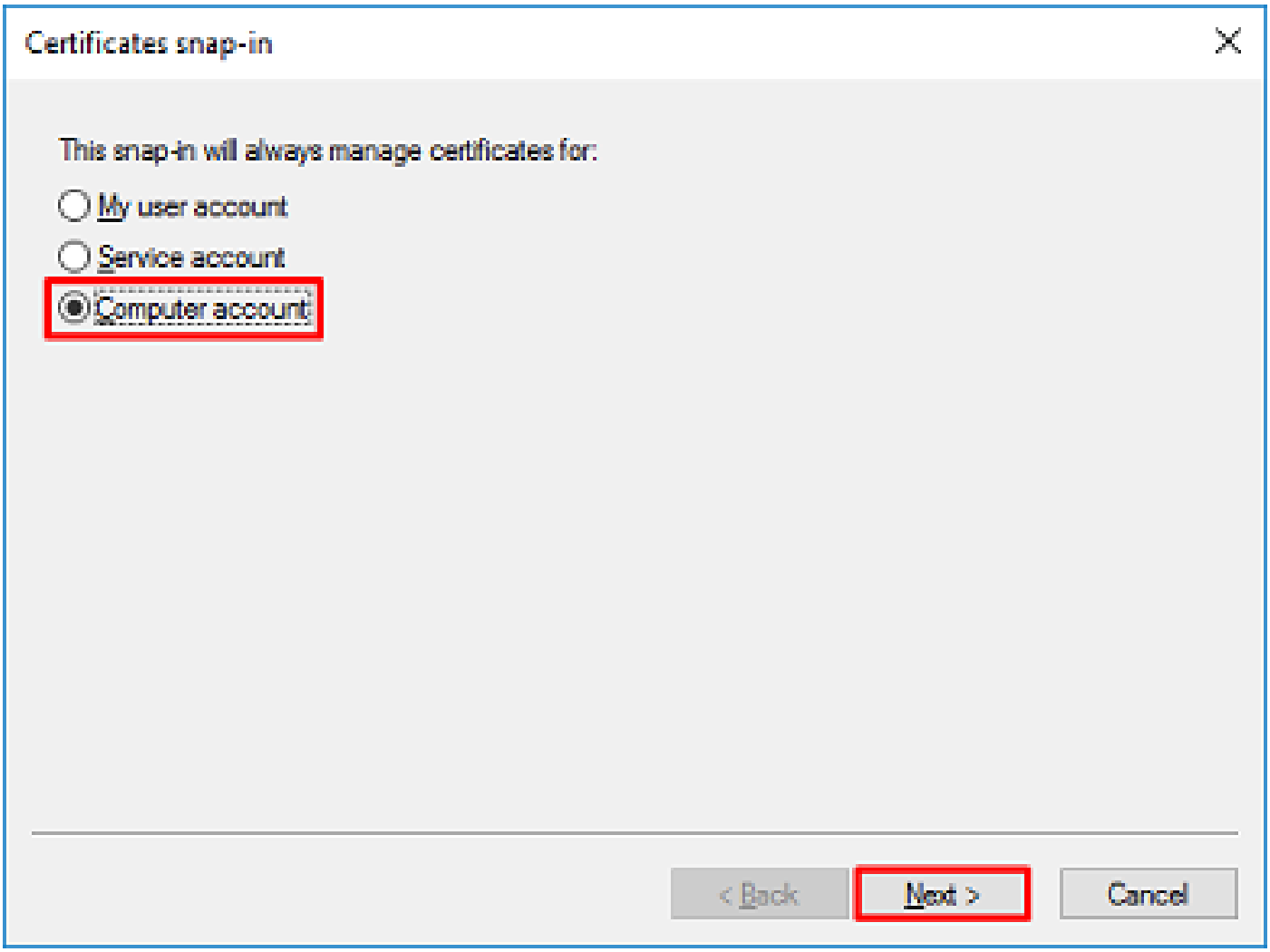
2. 导航至 File > Add/Remove Snap-in...，如图所示：



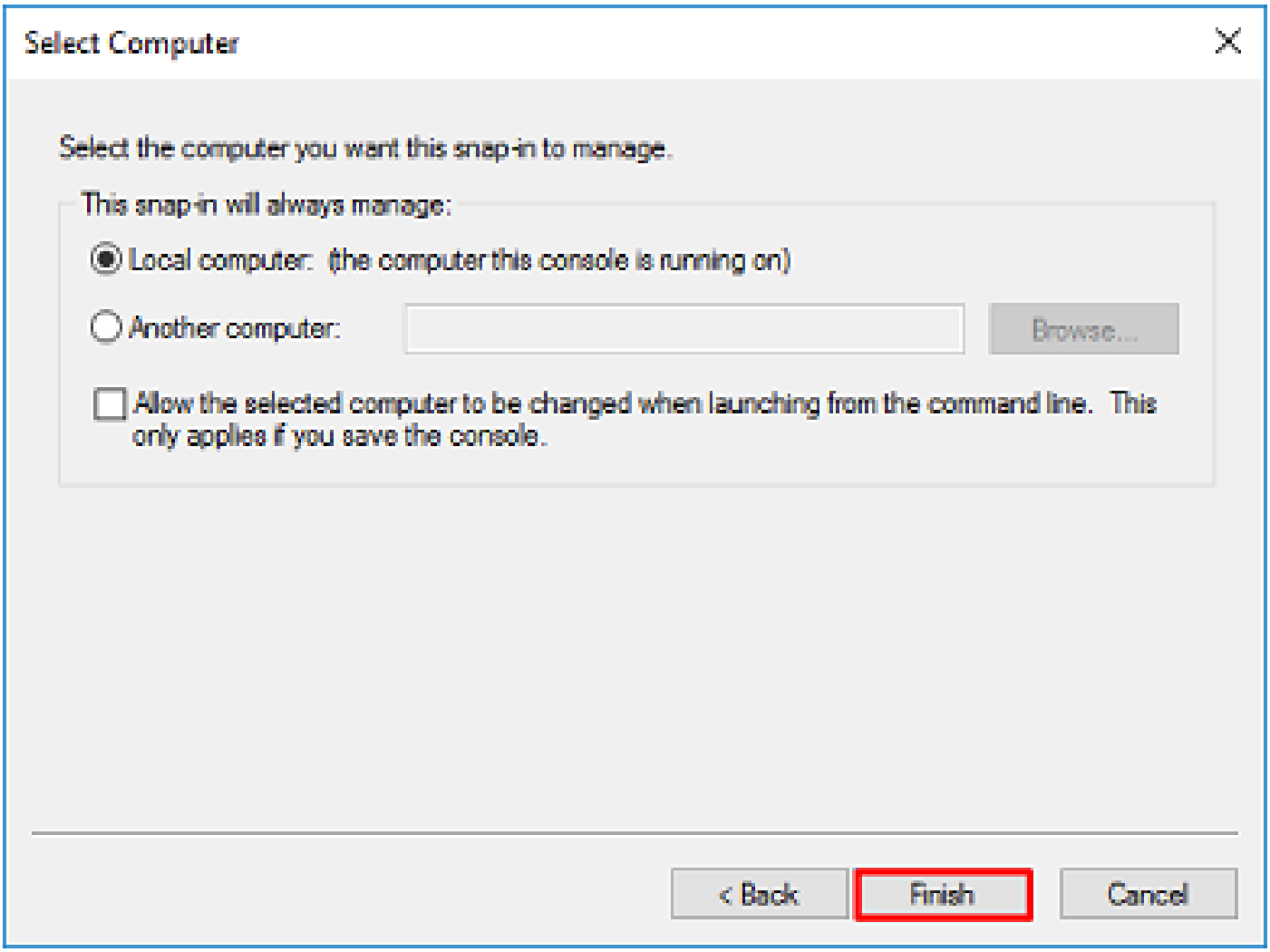
3. 在可用管理单元下，选择 Certificates 然后单击 Add，如下图所示：



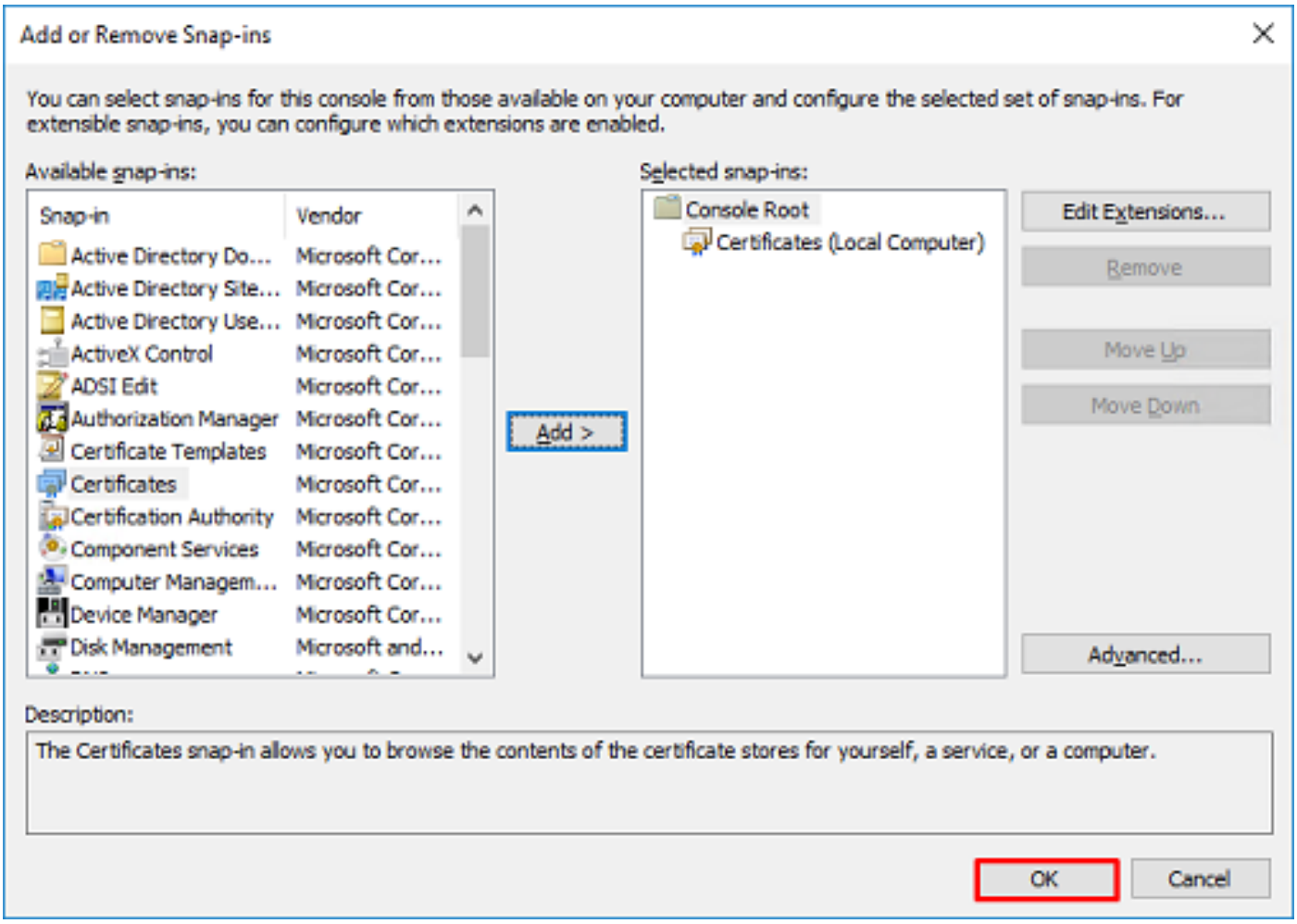
4. 选择 Computer account 然后单击 Next，如下图所示：



如图所示，单击 Finish.



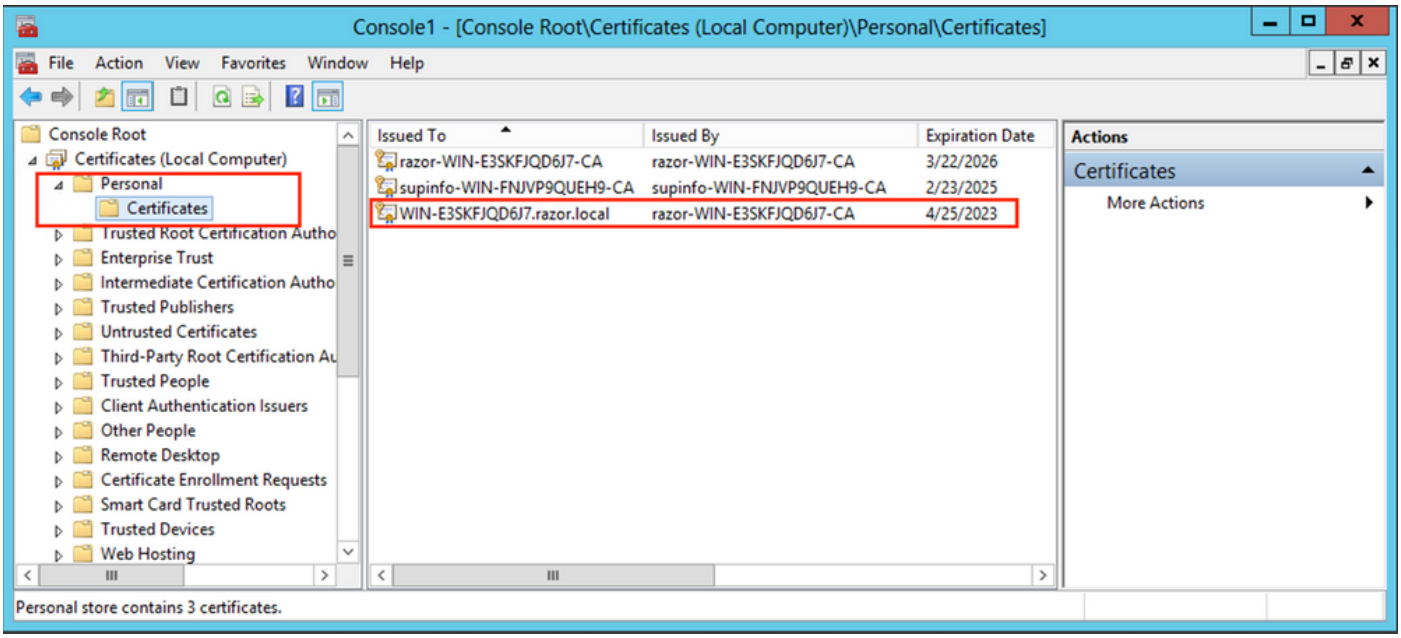
5. 现在，单击 OK，如图所示。



6. 展开 Personal 文件夹，然后单击 Certificates.LDAP使用的证书必须颁发给Windows服务器的完全限定域名(FQDN)。在此服务器上列出三个证书：

- CA证书颁发给和颁发者 razor-WIN-E3SKFJQD6J7-CA.
- 颁发给和颁发者的CA证书 supinfo-WIN-FNJVP9QUEH9-CA.
- 身份证书颁发给 WIN-E3SKFJQD6J7.razor.local 通过 razor-WIN-E3SKFJQD6J7-CA.

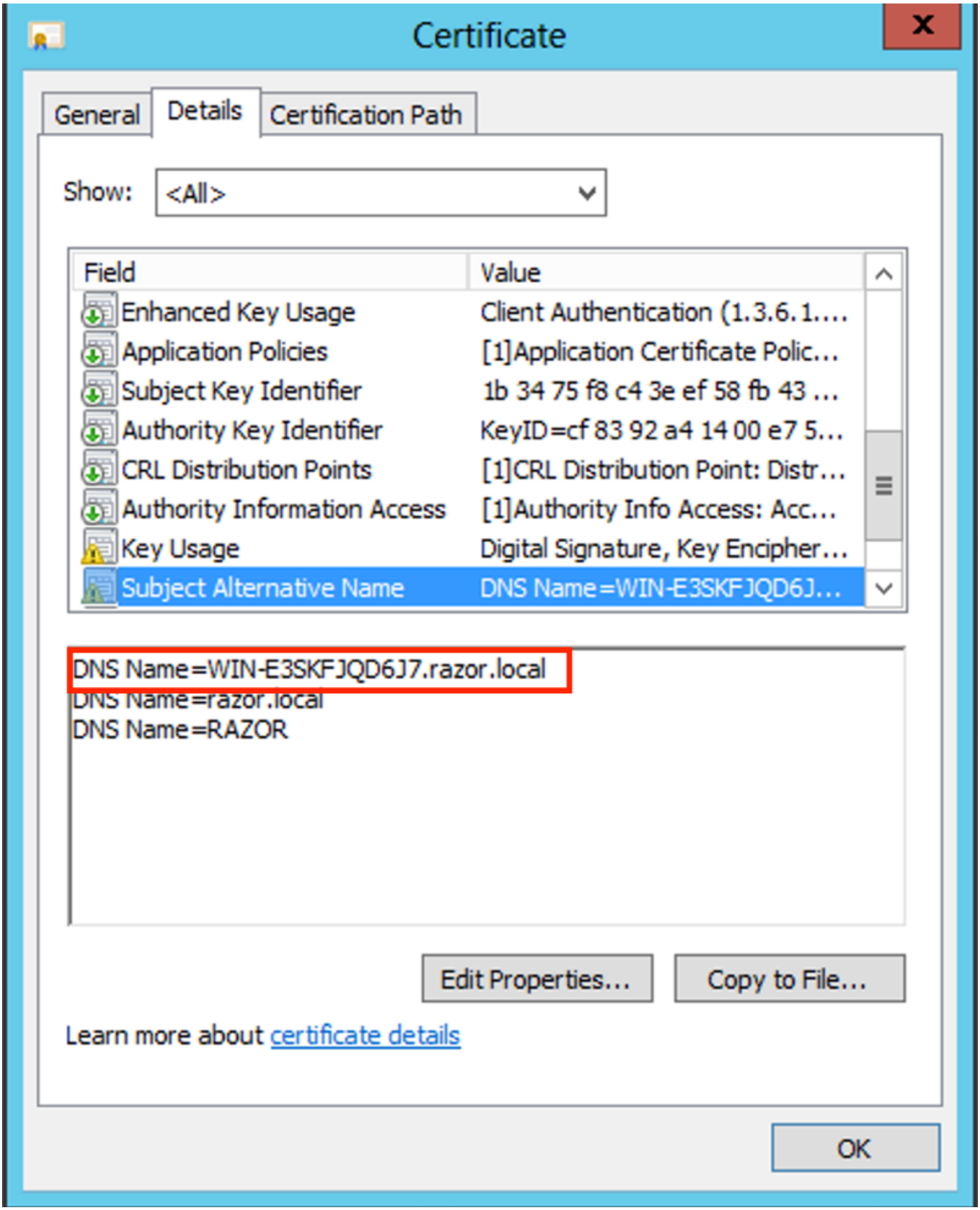
在本配置指南中，FQDN是 WIN-E3SKFJQD6J7.razor.local 因此，前两个证书不能用作LDAP的SSL证书。颁发给的标识证书 WIN-E3SKFJQD6J7.razor.local 是由Windows Server CA服务自动颁发的证书。双击证书以检查详细信息。



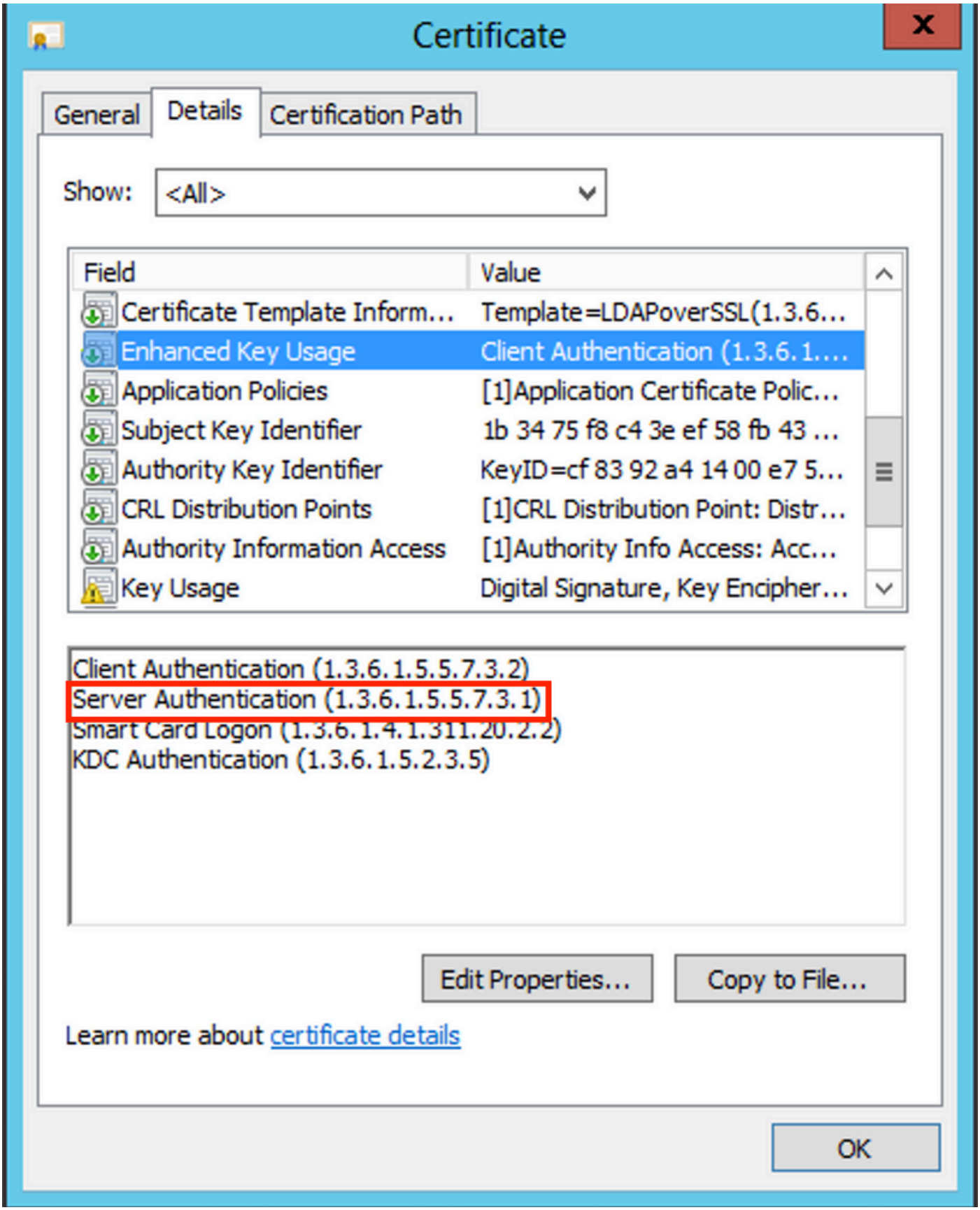
7. 要用作LDAP的SSL证书，证书必须满足以下要求：

- 公用名或DNS主题备用名与Windows Server的FQDN匹配。
- 证书在Enhanced Key Usage字段下有Server Authentication。

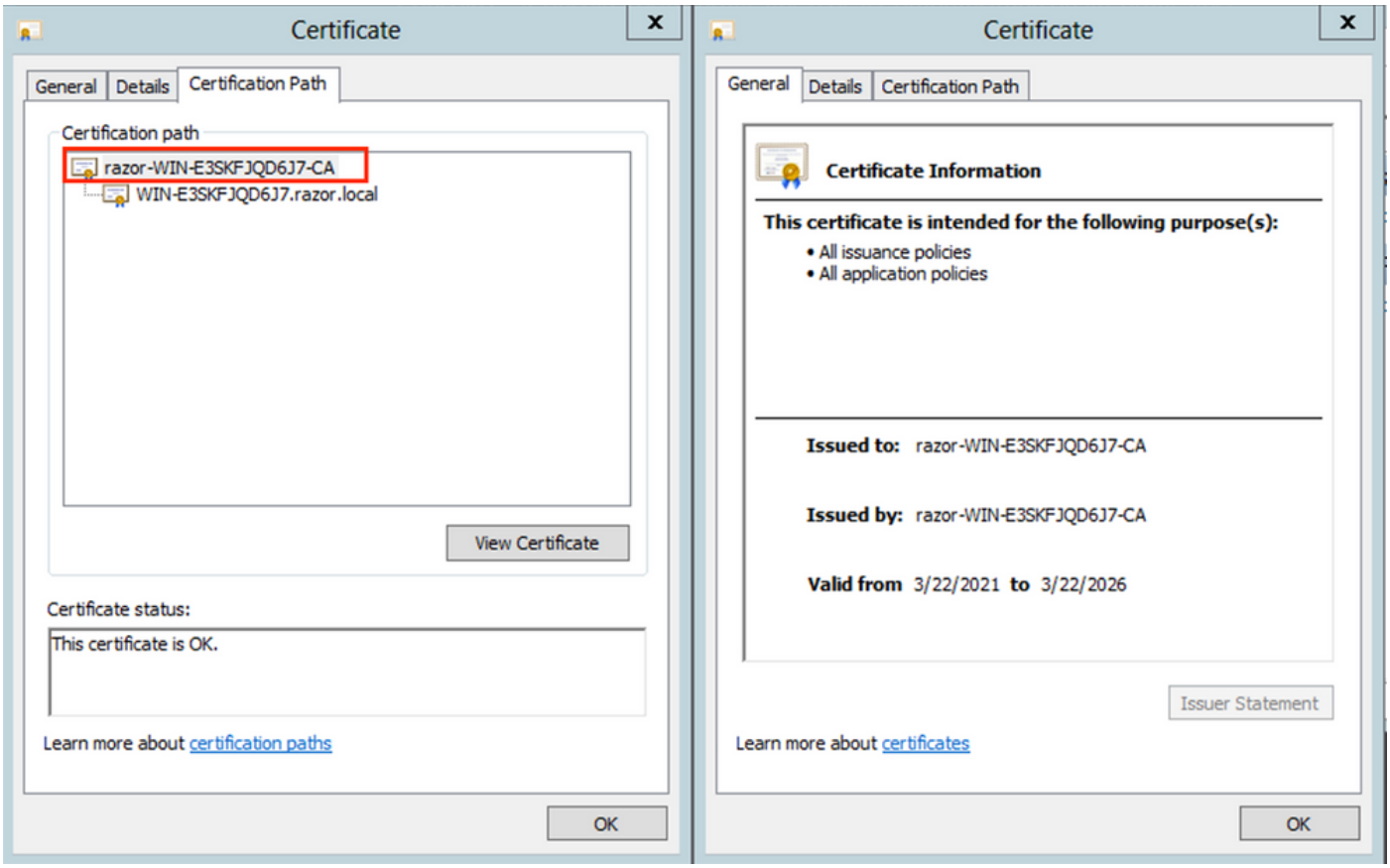
在 Details 选项卡中，选择 Subject Alternative Name，其中FQDN WIN-E3SKFJQD6J7.razor.local 存在。



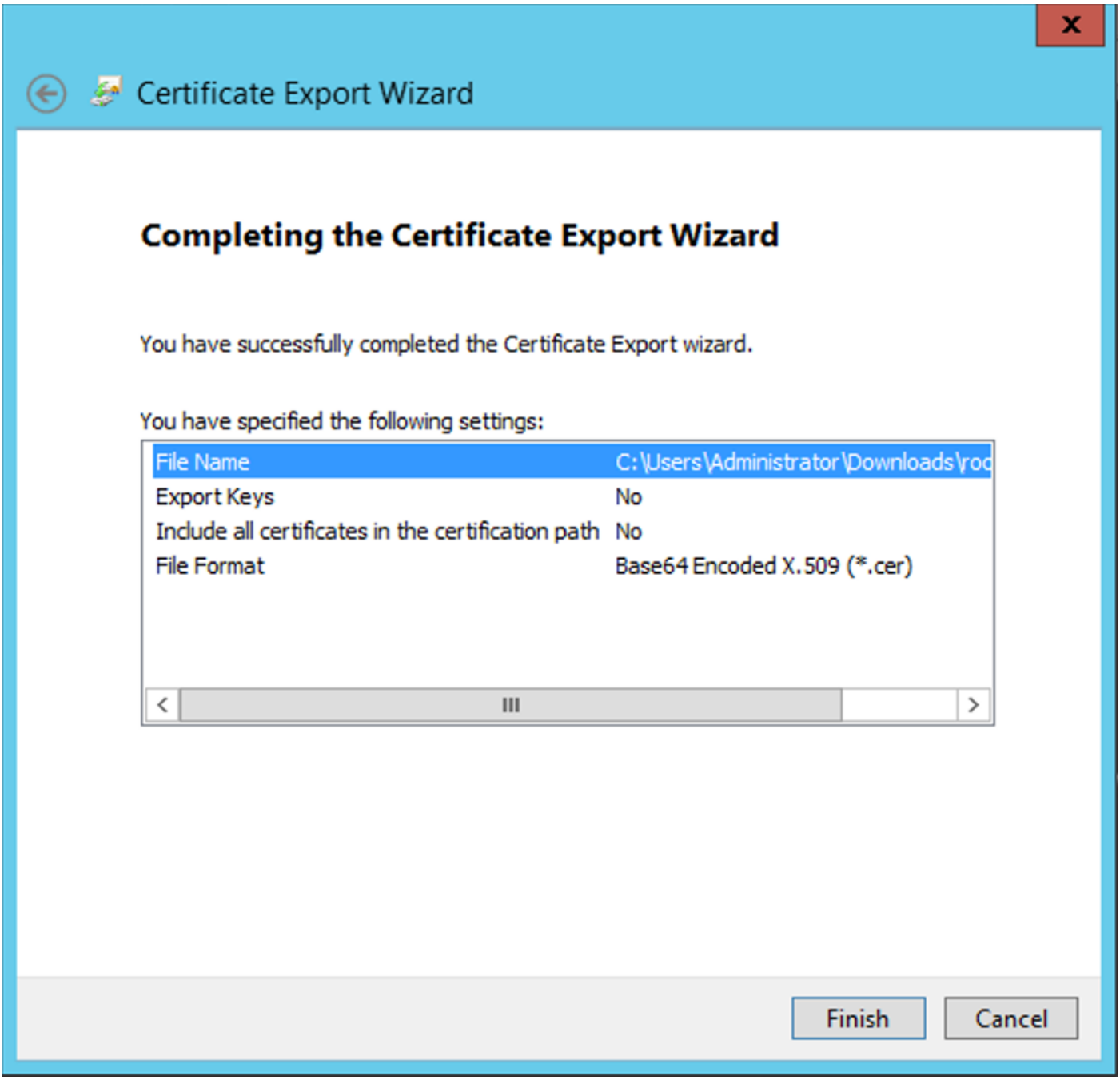
低于 Enhanced Key Usage，Server Authentication 存在。



8. 一旦确认，在 Certification Path 选项卡，选择作为根CA证书的顶级证书，然后单击 View Certificate.这将打开根CA证书的证书详细信息，如图所示：



9. 在 Details 根CA证书，点击 Copy to File 并浏览Certificate Export Wizard 该命令以PEM格式导出根CA。选择 Base-64 encoded X.509 作为文件格式。



10. 使用记事本或其他文本编辑器打开计算机上选定位置中存储的根CA证书。

这显示PEM格式证书。请保存以备后用。

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

在LDAP服务器上的本地计算机存储中安装多个证书的情况下（可选）

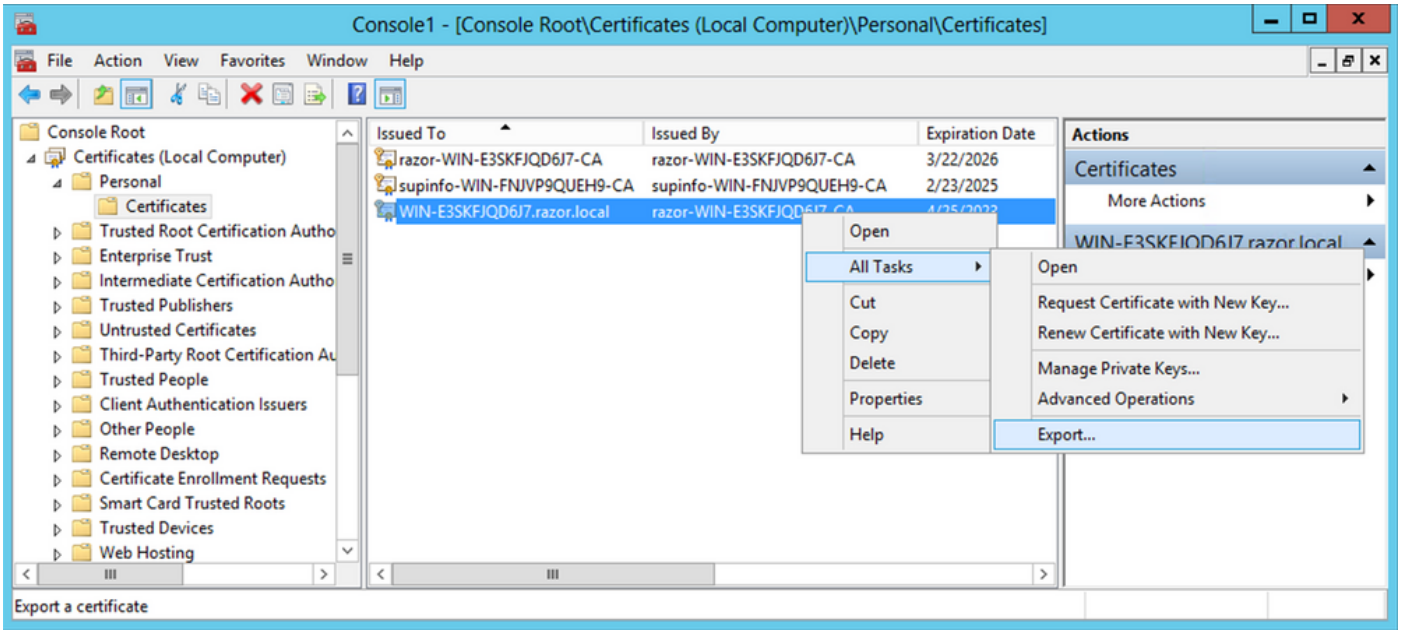
1.在LDAPS可以使用多个身份证书的情况下，当使用哪个身份证书存在不确定性，或者无法访问LDAPS服务器时，仍然可以从在FTD上完成的数据包捕获中提取根CA。

2.如果您在LDAP服务器（如AD DS域控制器）本地计算机证书存储中有多个有效进行服务器身份验证的证书，则可以注意到不同的证书用于LDAPS通信。解决此类问题的最佳方法是从本地计算机证书存储中删除所有不必要的证书，并且仅有一个对服务器身份验证有效的证书。

但是，如果有正当理由需要两个或更多证书并且至少具有一个Windows Server 2008 LDAP服务器，则Active Directory域服务(NTDS\Personal)证书存储区可用于LDAP通信。

以下步骤演示如何将启用LDAPS的证书从域控制器本地计算机证书存储导出到Active Directory域服务证书存储(NTDS\Personal)。

- 导航到Active Directory服务器上的MMC控制台，选择文件，然后单击 Add/Remove Snap-in.
- 点击 Certificates 然后单击 Add.
- 如果 Certificates snap-in，选择 Computer account 然后单击 Next.
- 在 Select Computer，选择 Local Computer，单击 OK，然后单击 Finish.在 Add or Remove Snap-ins，单击 OK.
- 在包含用于服务器身份验证的证书的计算机的证书控制台中，右击 certificate，单击 All Tasks，然后单击 Export.

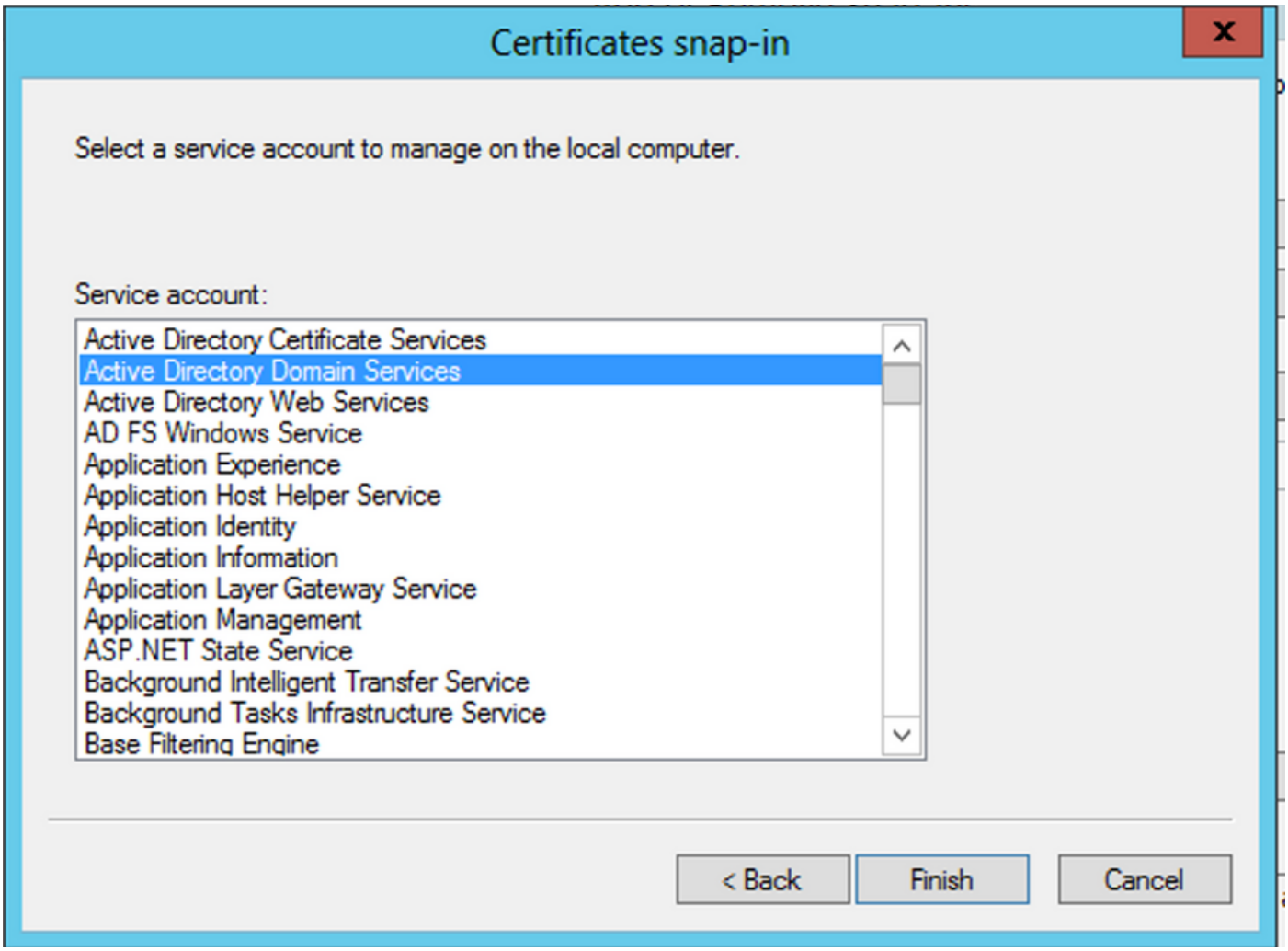


- 在中导出证书 pfx 在后续章节中设置。有关如何在中导出证书的文章，请参阅 pfx 来自MMC的格式：

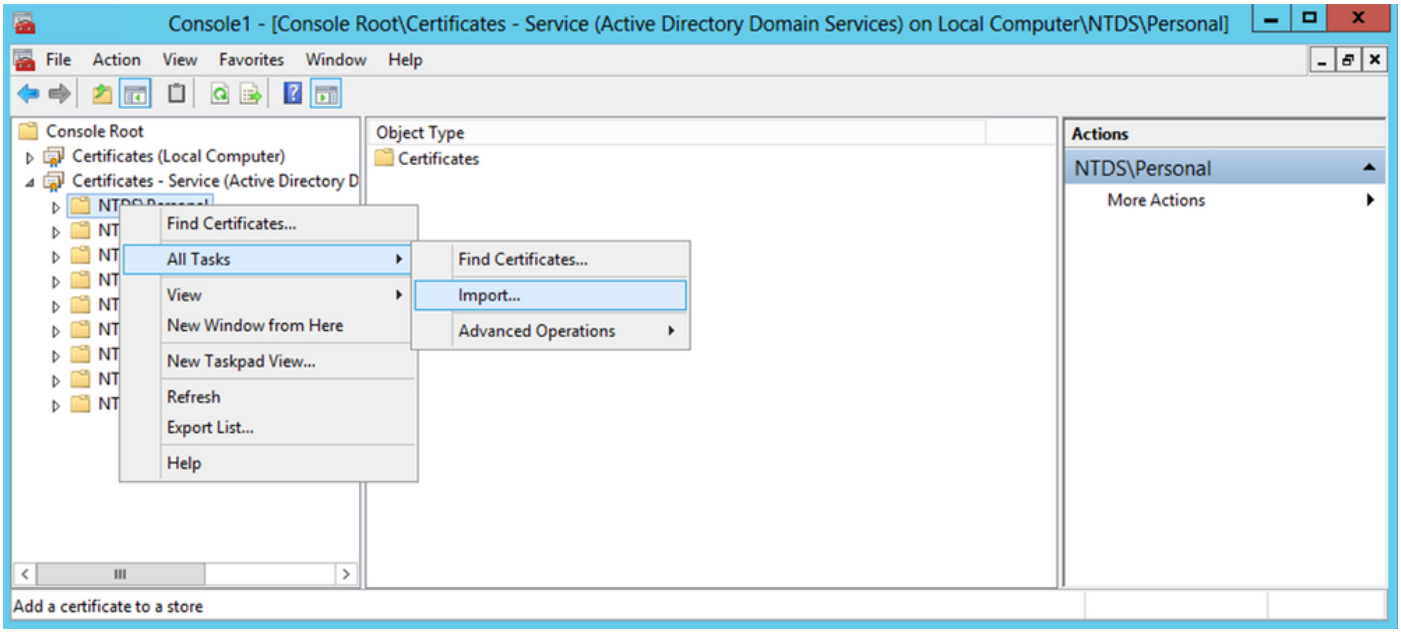
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html。

- 导出证书后，导航至 Add/Remove Snap-in 在 MMC console.点击 Certificates 然后单击 Add.
- 选择 Service account 然后单击 Next.

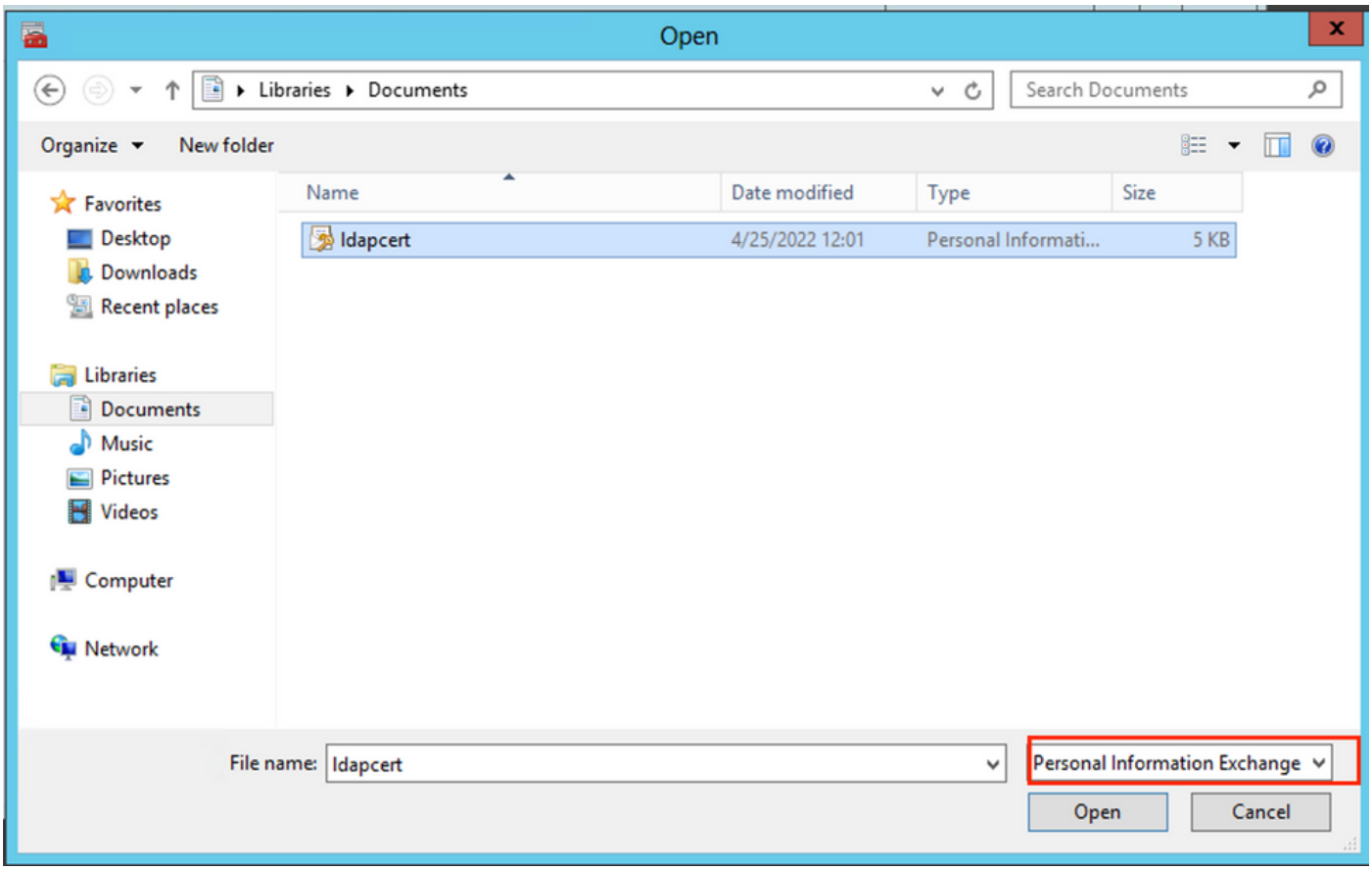
- 如果 Select Computer 对话框，选择 Local Computer 并点击 Next.
- 选择 Active Directory Domain Services 然后单击 Finish.



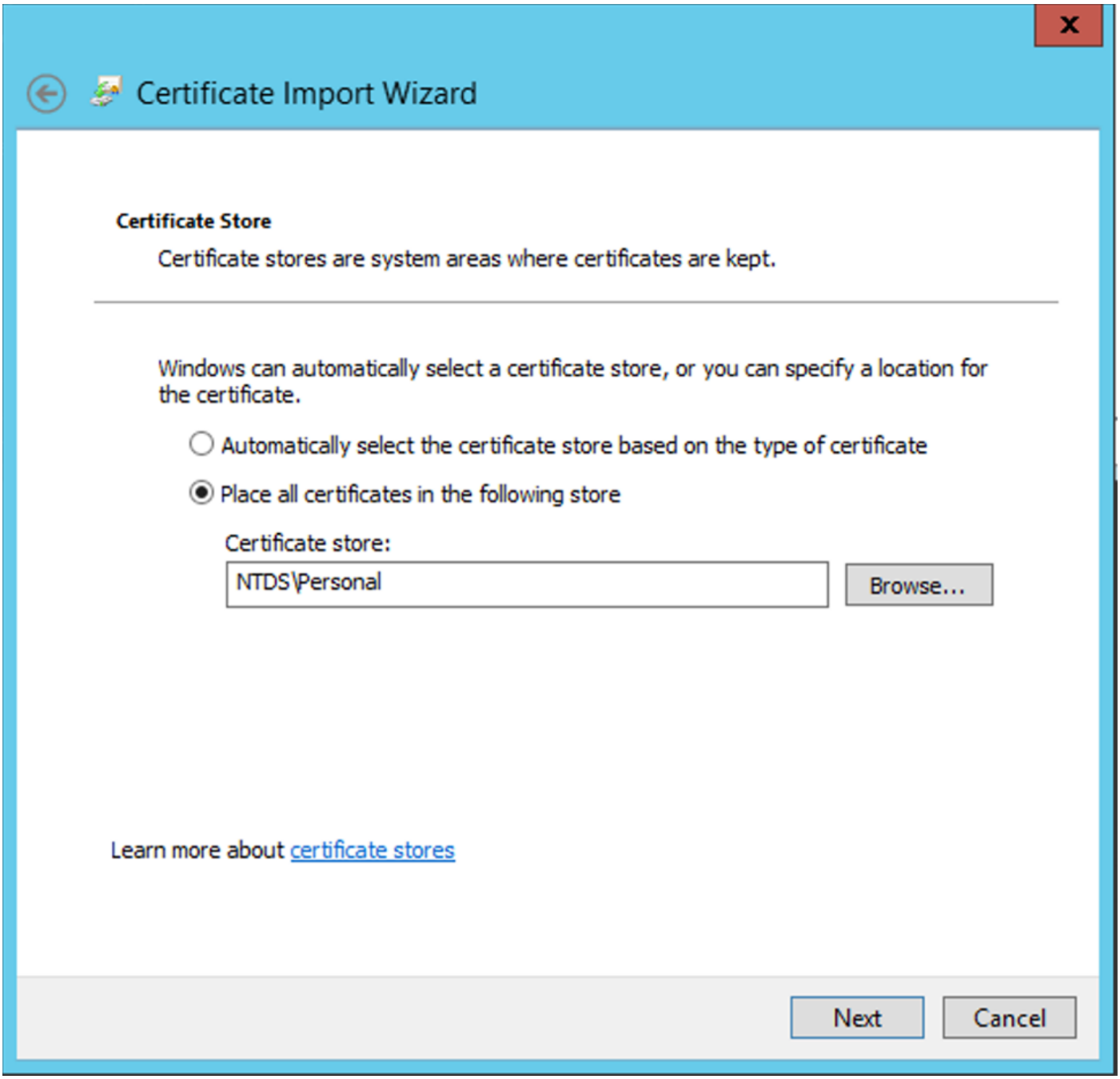
- 在 Add/Remove Snap-ins 对话框，单击 OK.
- 扩大采购 Certificates - Services (Active Directory Domain Services) 然后单击 NTDS\Personal.
- 右键单击 NTDS\Personal，单击 All Tasks，然后单击 Import.



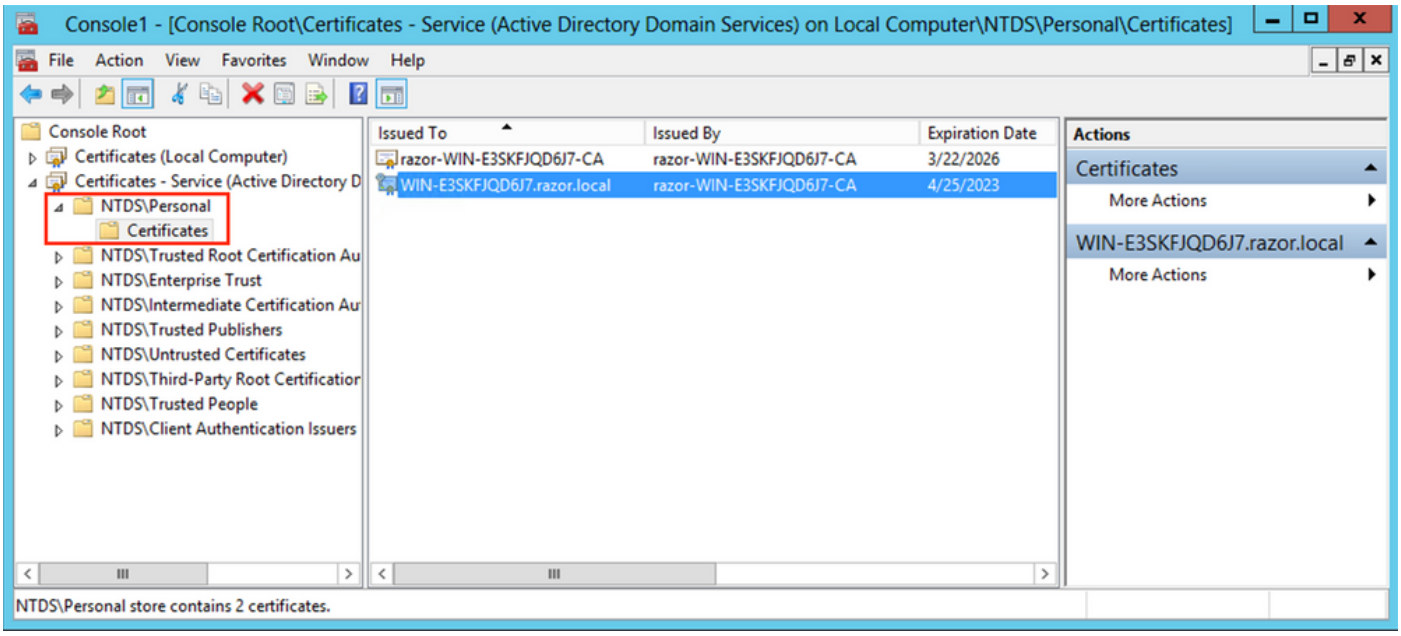
- 在 Certificate Import Wizard 欢迎屏幕，单击 Next.
- 在“要导入的文件”屏幕上，单击 Browse，并找到先前导出的证书文件。
- 在“打开”屏幕上，确保个人信息交换(*pfx,*.p12)被选为文件类型，然后导航文件系统以查找先前导出的证书。然后，点击该证书。



- 点击 Open 然后单击 Next.
- 在“密码”屏幕上，输入为文件设置的密码，然后单击 Next.
- 在Certificate Store页面上，确保选中Place all certificates并阅读Certificate Store: NTDS\Personal 然后单击 Next.



- 在 Certificate Import Wizard 完成屏幕，单击 Finish.然后您会看到一条消息，表明导入成功。点击 OK.可以看到证书已导入到证书存储区下： NTDS\Personal.



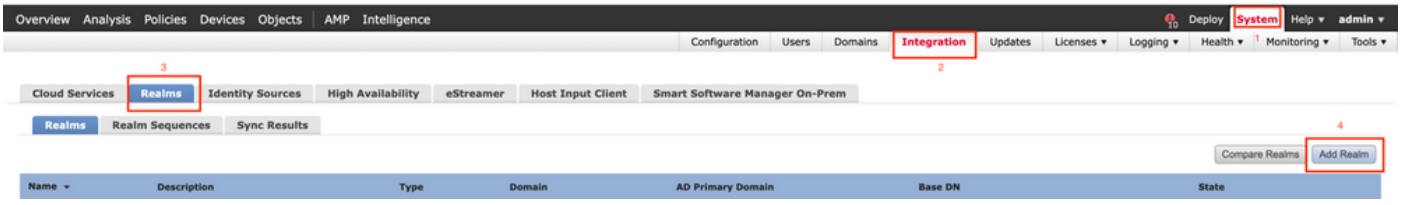
FMC配置

验证许可

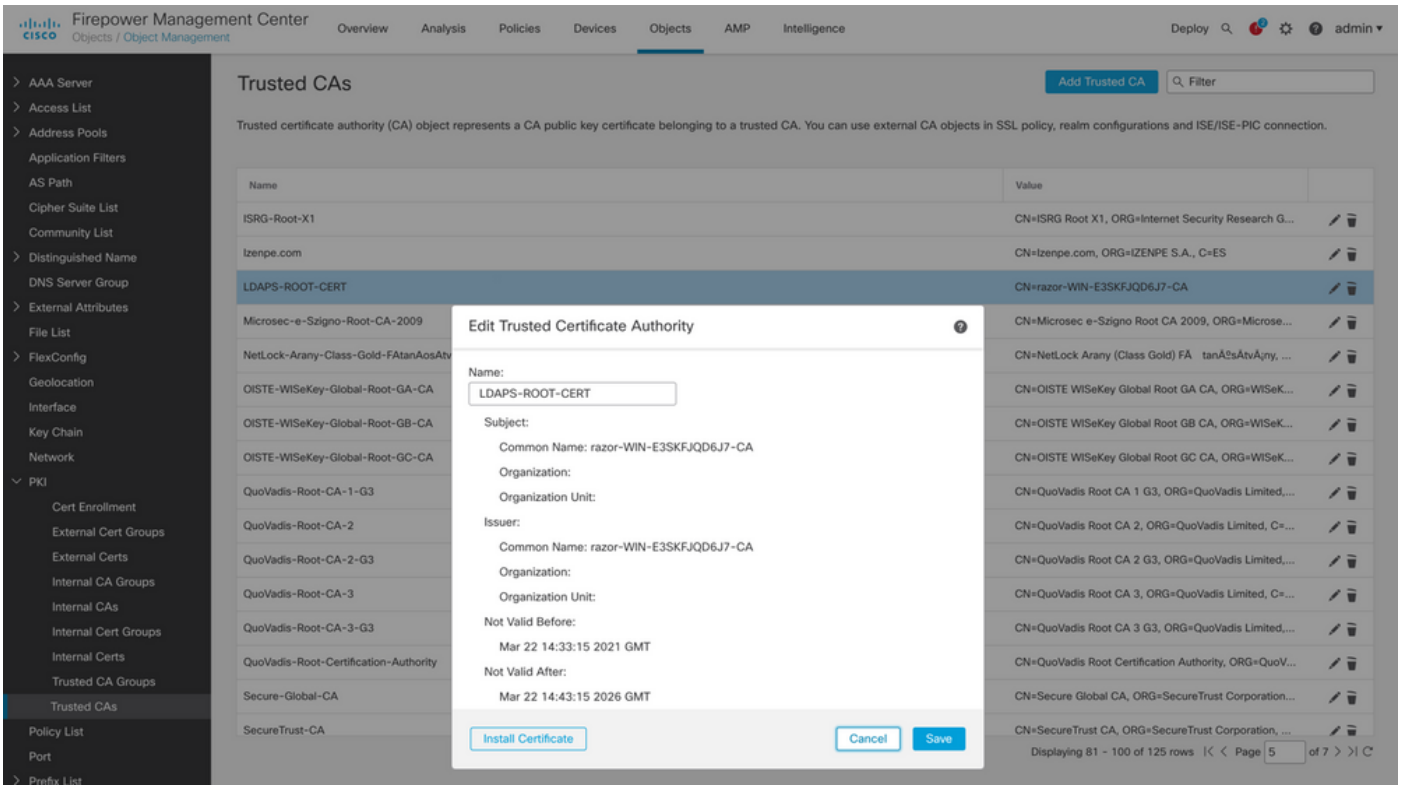
要部署AnyConnect配置，FTD必须注册到智能许可服务器，并且必须将有效的Plus、Apex或仅VPN许可证应用到设备。

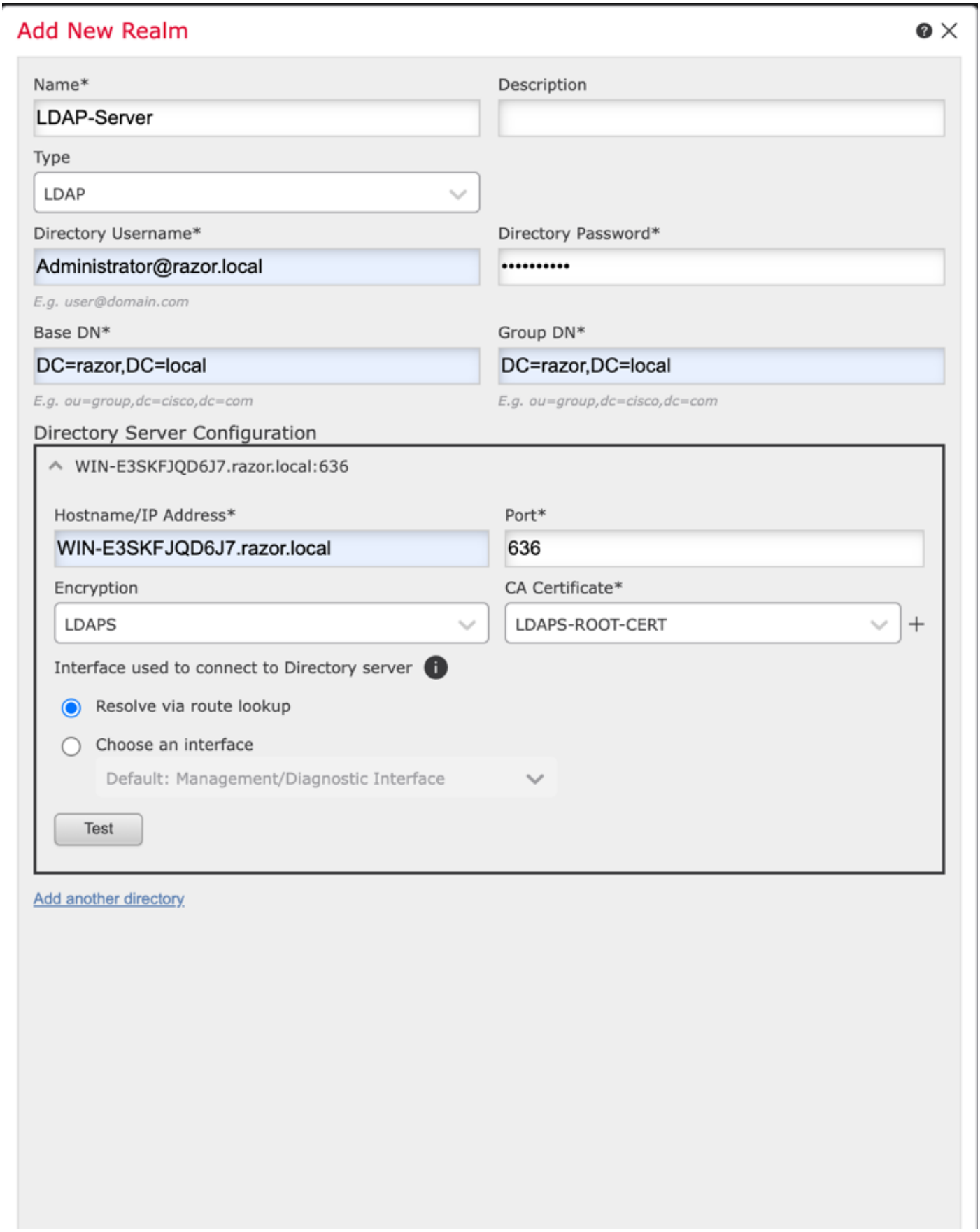
设置领域

1. 导航至 System > Integration.导航至 Realms ，然后单击 Add Realm ，如下图所示：

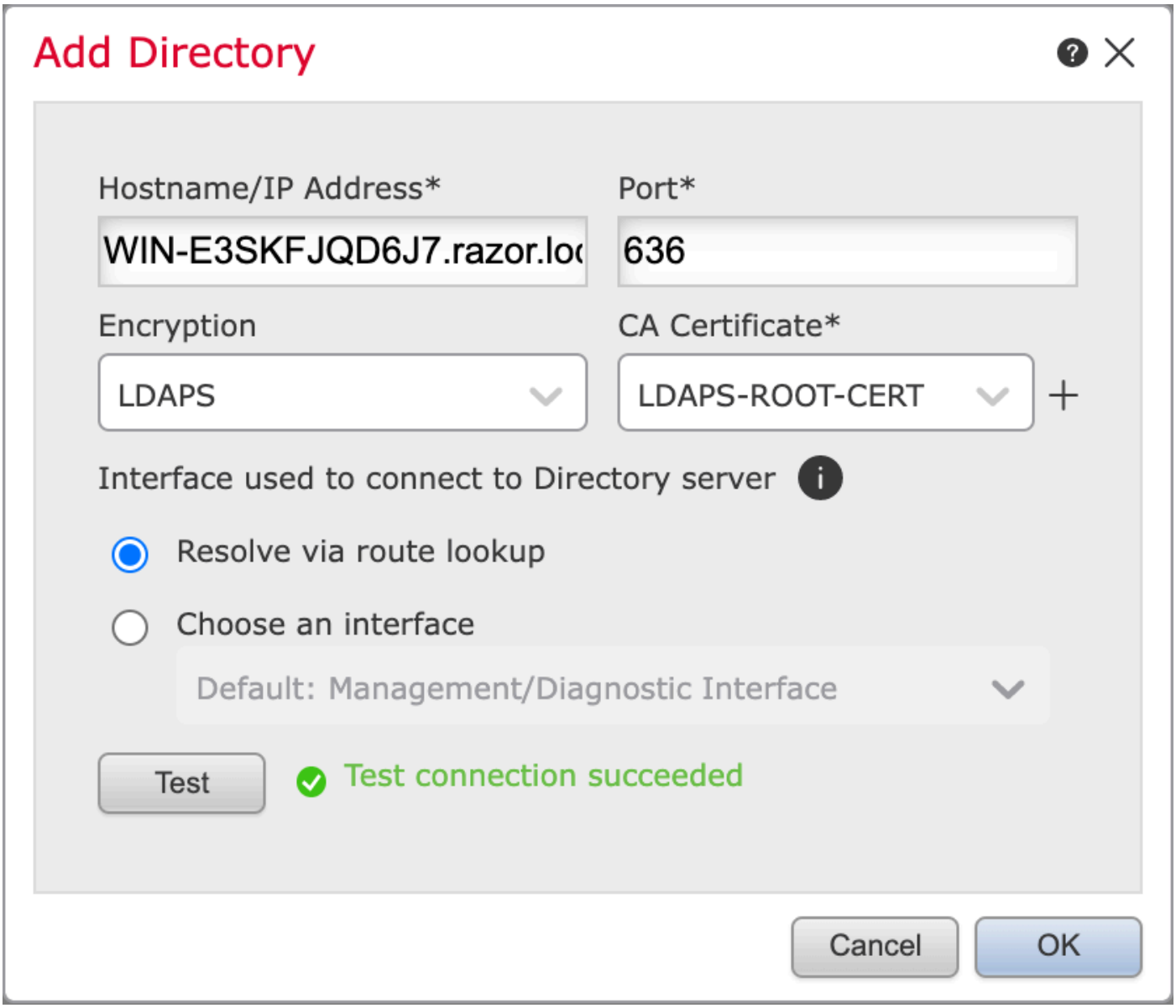


2. 根据从Microsoft LDAP服务器收集的信息填写显示的字段。在此之前，请导入在Windows Server上签署LDAP服务证书的根CA证书 Objects > PKI > Trusted CAs > Add Trusted CA ，因为在Directory Server Configuration 领域。完成后，单击 OK.

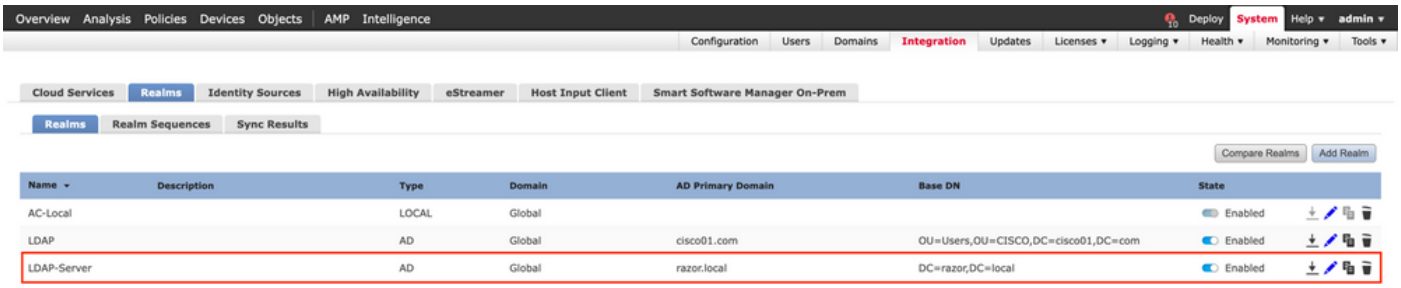

Firepower Management Center
Objects / Object Management
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Deploy
admin
AAA Server
Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
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. 点击 Test 为了确保FMC能够成功绑定到前面步骤中提供的目录用户名和密码。由于这些测试是从FMC启动的，而不是通过FTD上配置的可路由接口（例如内部、外部和dmz）之一启动，因此成功（或失败）的连接不能保证AnyConnect身份验证的相同结果，因为AnyConnect LDAP身份验证请求是从一个FTD可路由接口启动的。

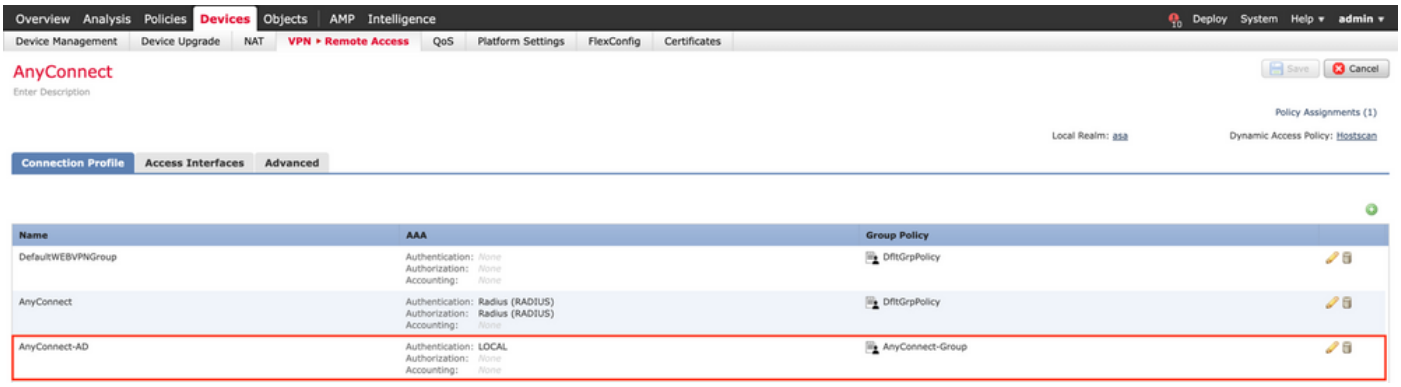


4. 启用新领域。

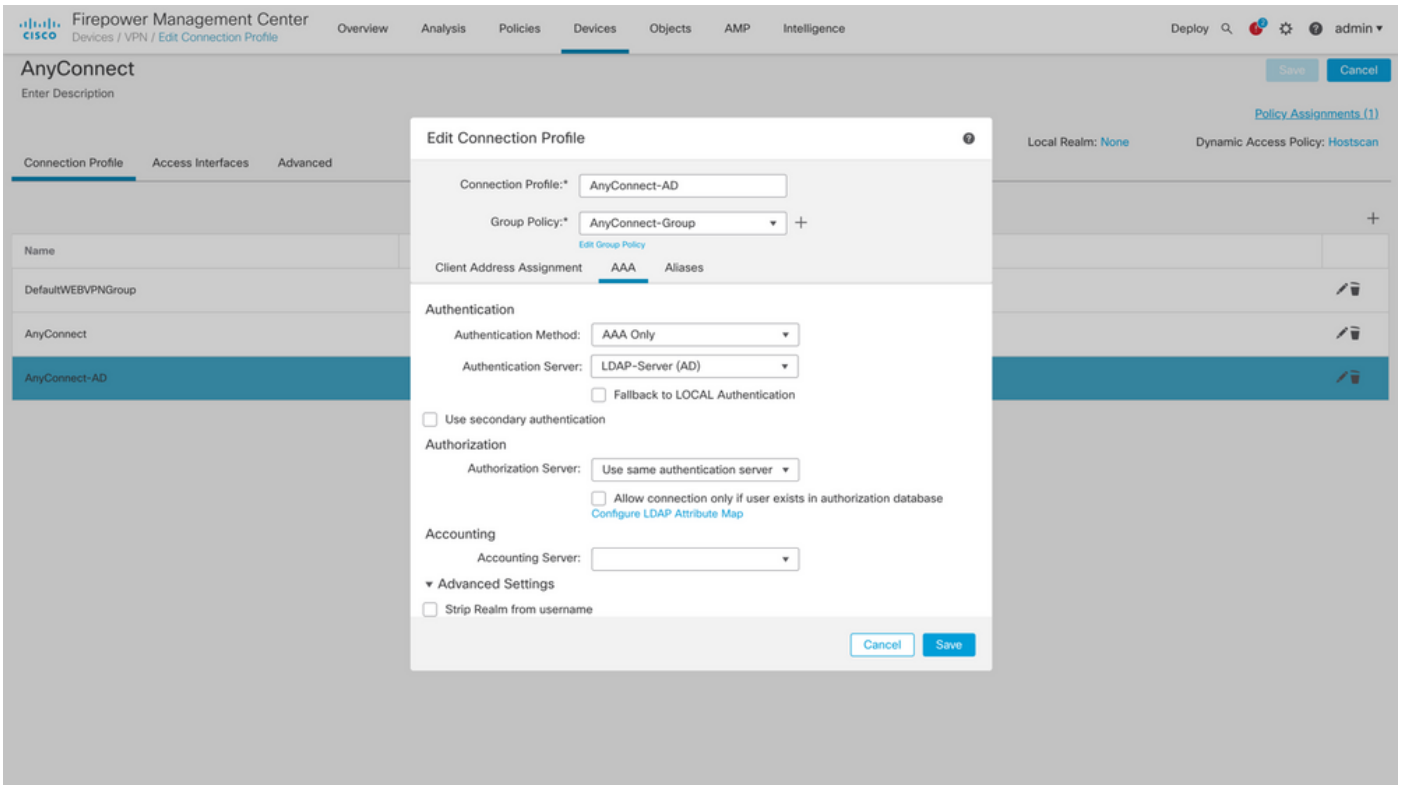


配置AnyConnect进行密码管理

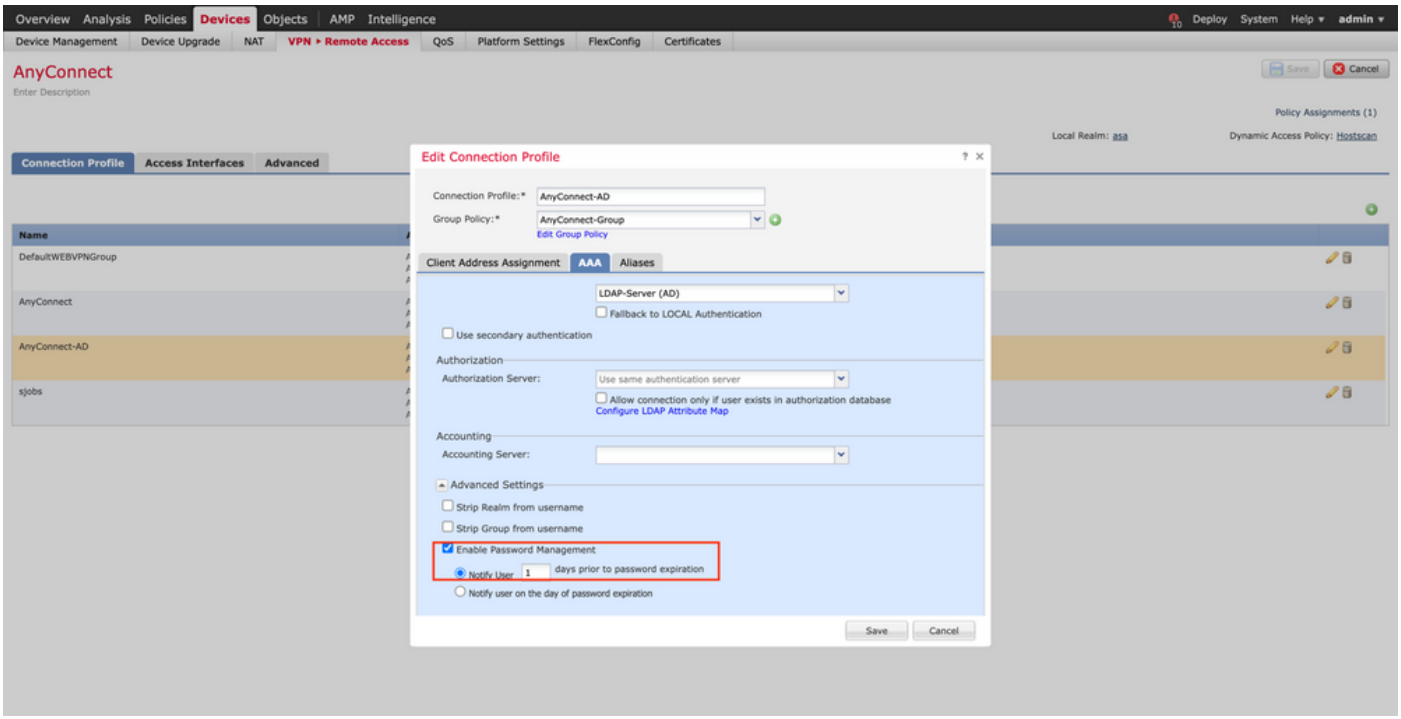
1. 选择现有连接配置文件，或创建新连接配置文件（如果是AnyConnect的初始设置）。此处使用名为“AnyConnect-AD”且映射了本地身份验证的现有连接配置文件。



2. 在连接配置文件的AAA设置下，编辑连接配置文件并映射在之前步骤中配置的新LDAP服务器。完成后，单击 Save 在右上角。



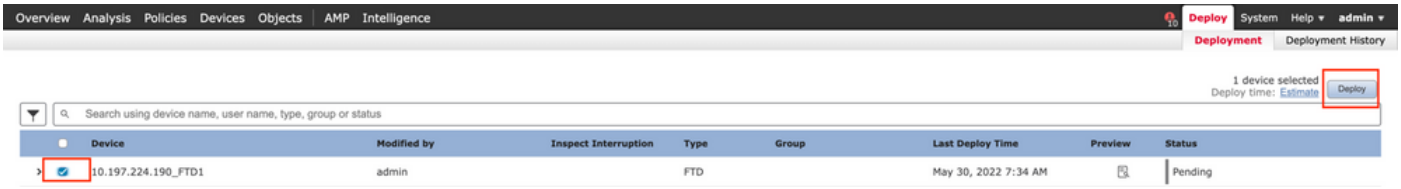
3. 在 AAA > Advanced Settings 并保存配置。



部署

1. 完成所有配置后，点击Deploy 按钮右上角。

2. 点击应用到它的FTD配置旁边的复选框，然后点击 Deploy，如下图所示：



最终配置

这是成功部署后在FTD CLI中看到的配置。

AAA配置

<#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配置

<#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
```

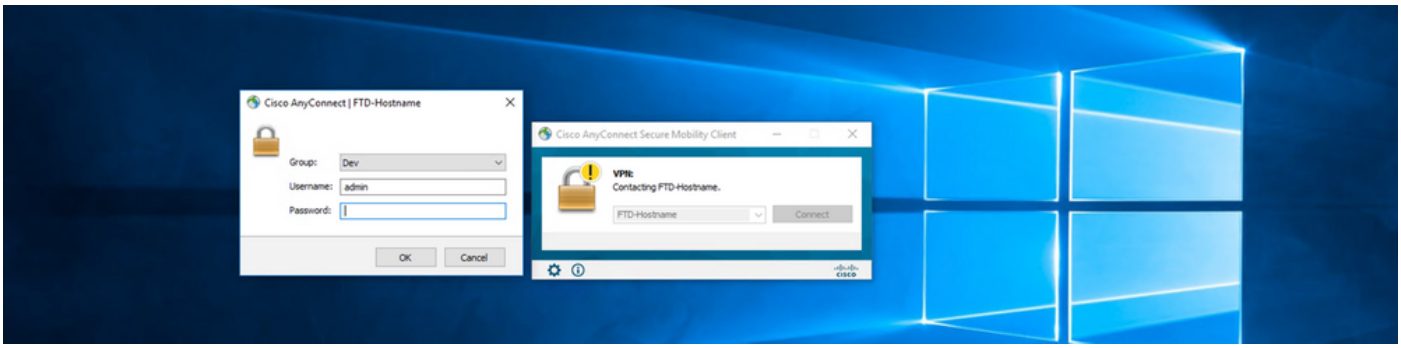
```
tunnel-group AnyConnect-AD type remote-access
tunnel-group AnyConnect-AD general-attributes
 address-pool Pool-1
authentication-server-group LDAP-Server                                    <-------- LDAPs Serve

 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
```

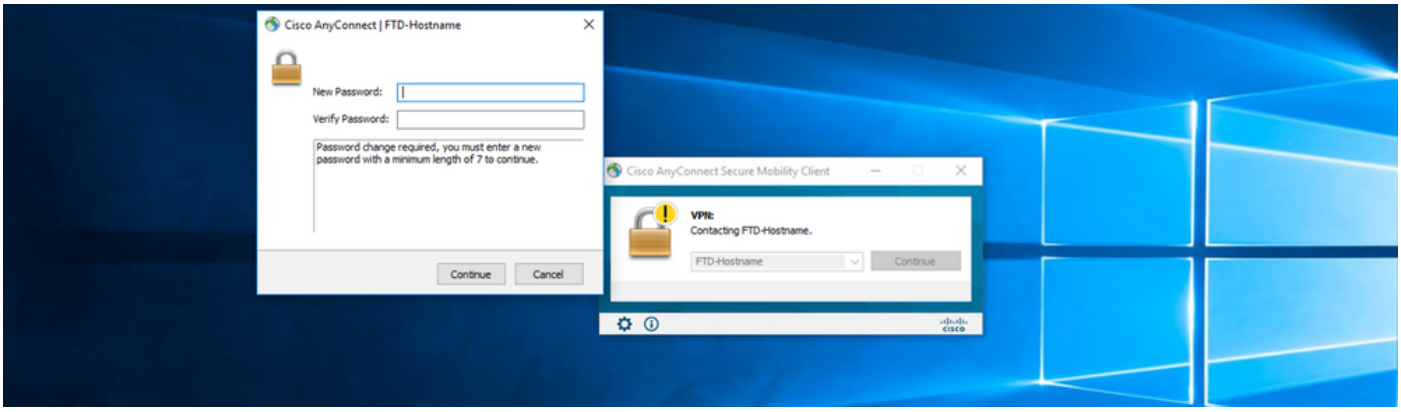
```
 default-domain none
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private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

确认

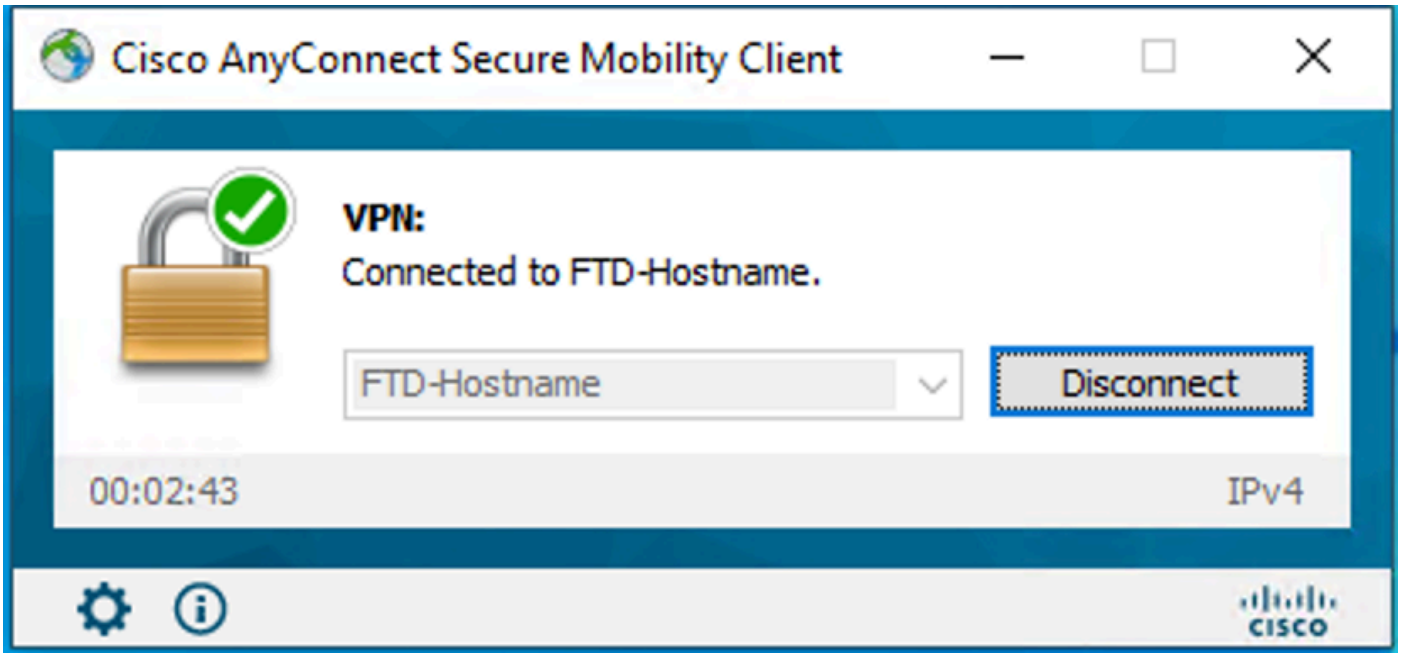
使用AnyConnect连接并验证用户连接的密码管理过程

1.发起到相关连接配置文件的连接。一旦在初始登录时确定必须更改密码，因为较早的密码已过期，被Microsoft Server拒绝，系统将提示用户更改密码。





2. 用户输入登录新密码后，连接成功建立。



3. 验证FTD CLI上的用户连接：

<#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

故障排除

调试

此调试可以在诊断CLI中运行，以便排除与密码管理相关的问题：debug ldap 255。

工作密码管理调试

<#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

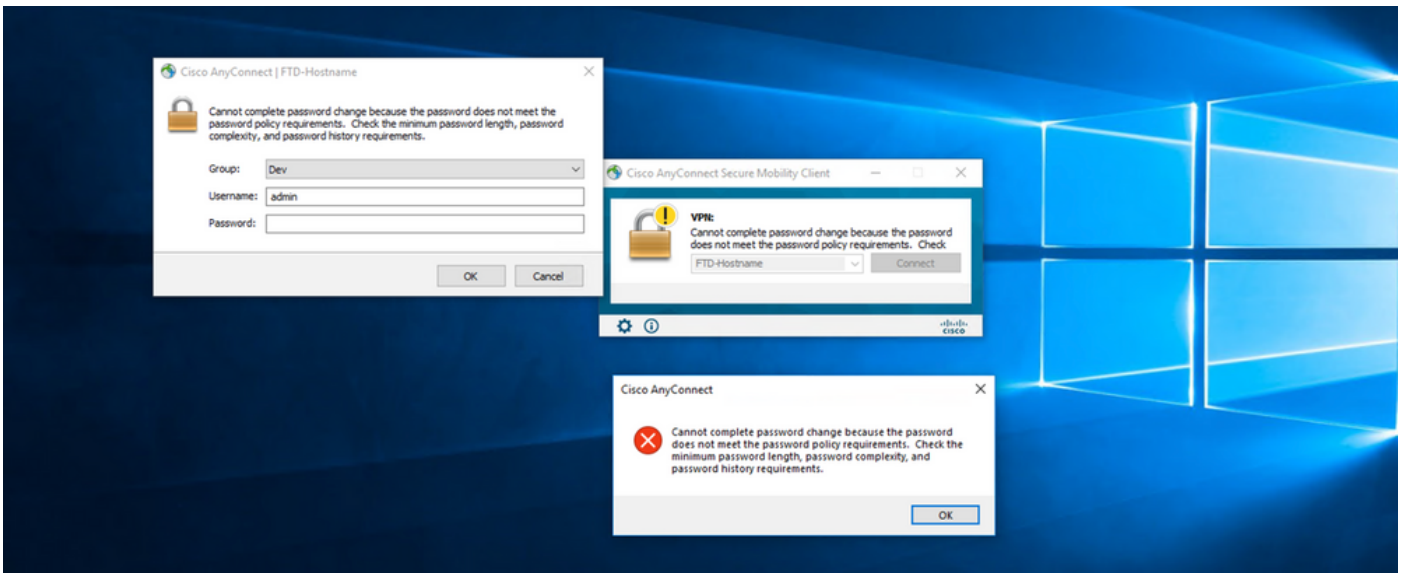
[25]   lastLogon: value = 132484577284881837

[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
```

密码管理过程中遇到的常见错误

通常，如果在用户提供新密码期间未满足Microsoft Server设置的密码策略，连接将终止，并显示错误“Password does the Password Policy Requirements”。因此，请确保新密码符合Microsoft Server为LDAP设置的策略。



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。