FMCによって管理されるFTD上のRA VPNに対するLDAPを使用したパスワード管理の設定

内容

概要

このドキュメントでは、Cisco Password Threat Défense(FTD)に接続するAnyConnectクライアントのLDAPを使用したFirepower管理(PMS)の設定について説明します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- FMCでのRA VPN（リモートアクセス仮想プライベートネットワーク）設定に関する基本的

な知識
- FMCでのLDAPサーバ設定に関する基本的な知識
- Active Directoryの基礎知識

使用するコンポーネント

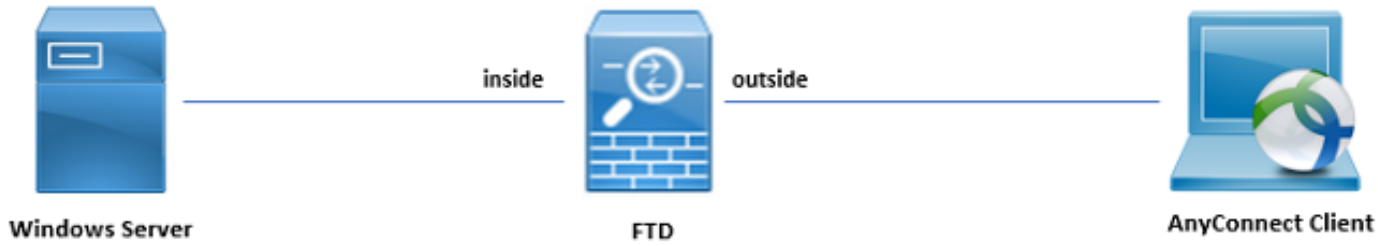
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft 2012 R2サーバ
- 7.3.0を実行するFMCv
- 7.3.0が稼働するFTDv

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

コンフィギュレーション

ネットワークダイアグラムとシナリオ



Windowsサーバは、ユーザパスワード管理プロセスをテストするために、ADDSおよびADCSで事前設定されています。この設定ガイドでは、これらのユーザアカウントが作成されます。

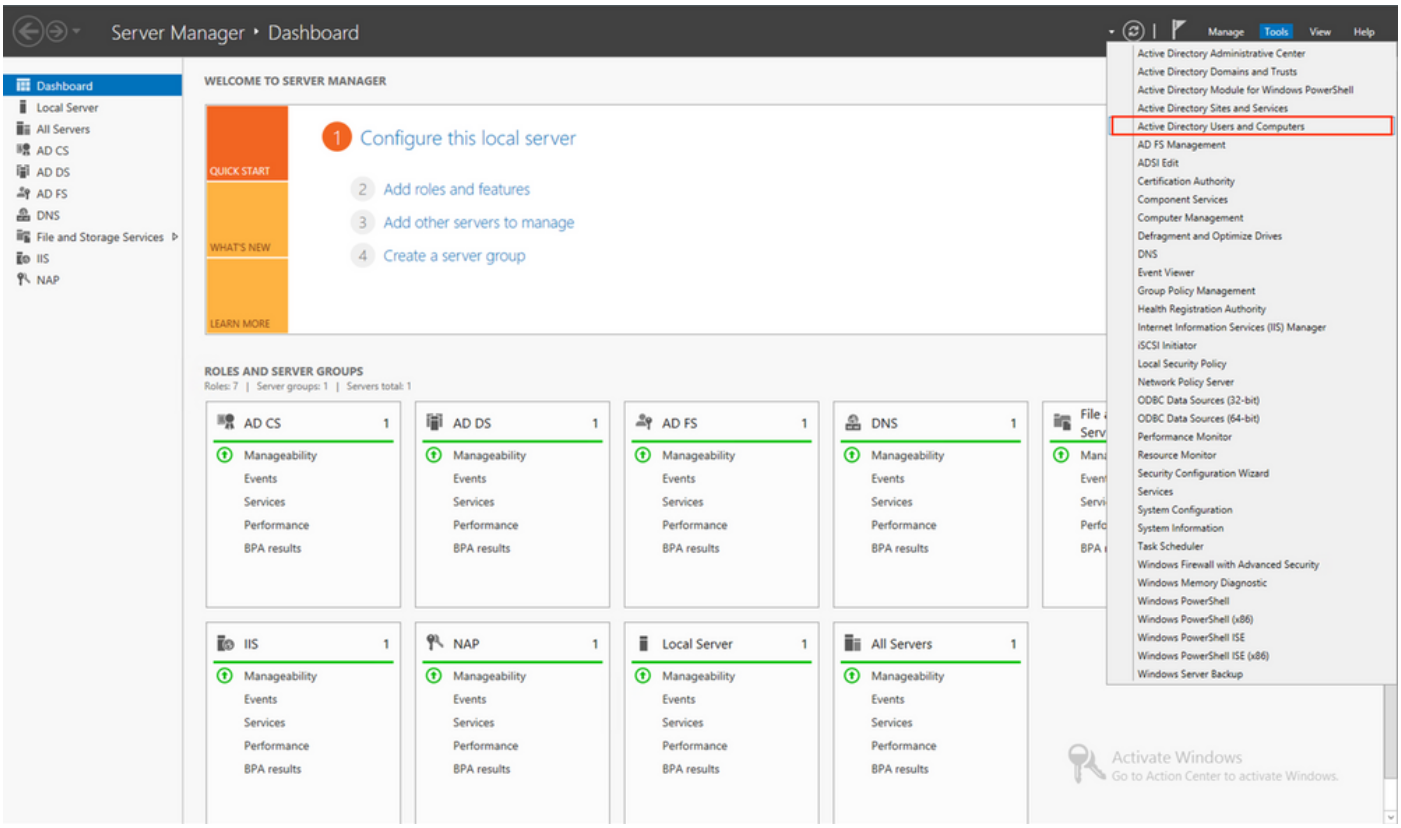
ユーザアカウント:

- 管理者：これは、FTDがActive Directoryサーバにバインドできるようにするためのディレクトリアカウントとして使用されます。

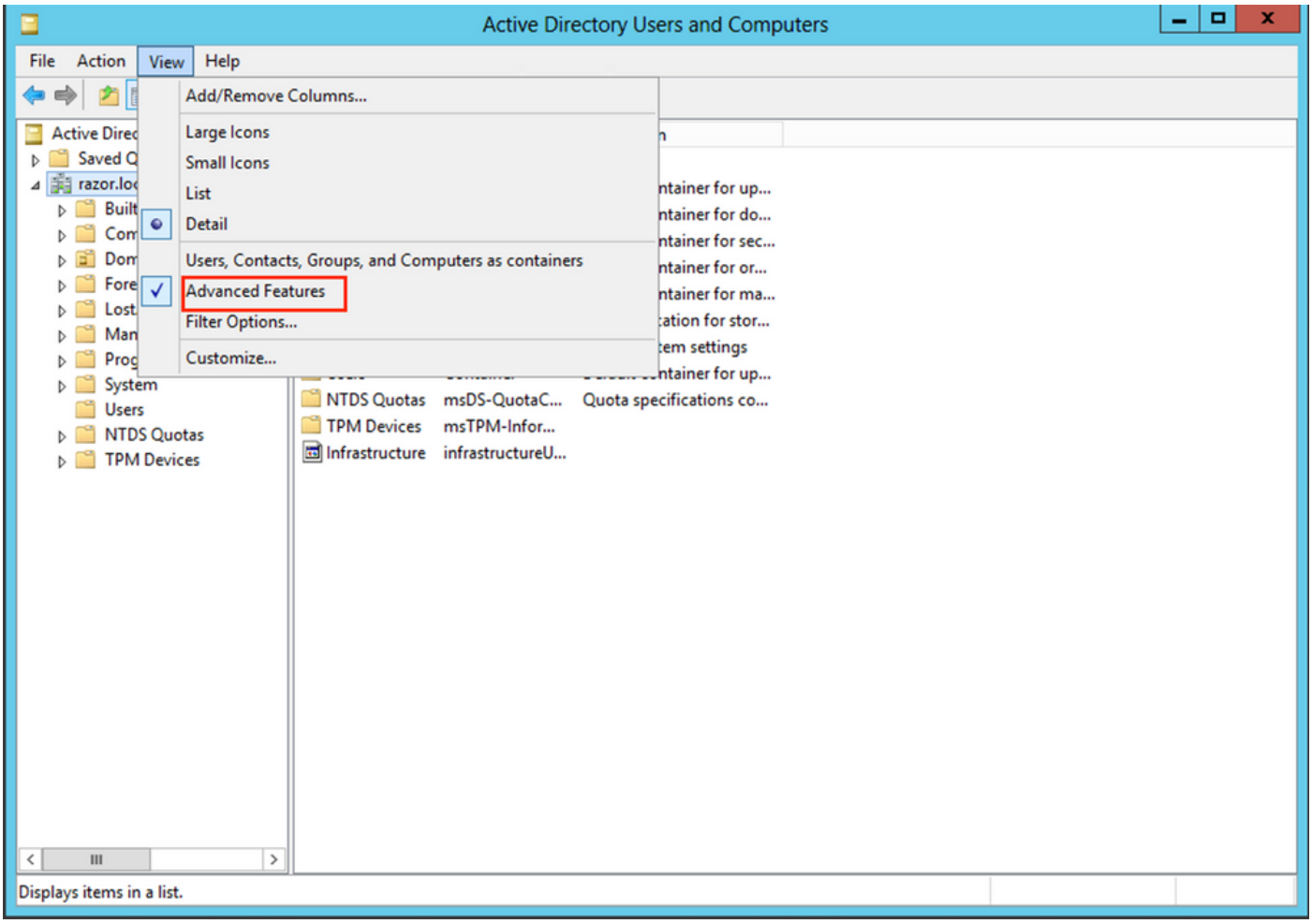
- admin：ユーザーIDを示すために使用されるテスト管理者アカウント。

LDAPベースDNとグループDNの決定

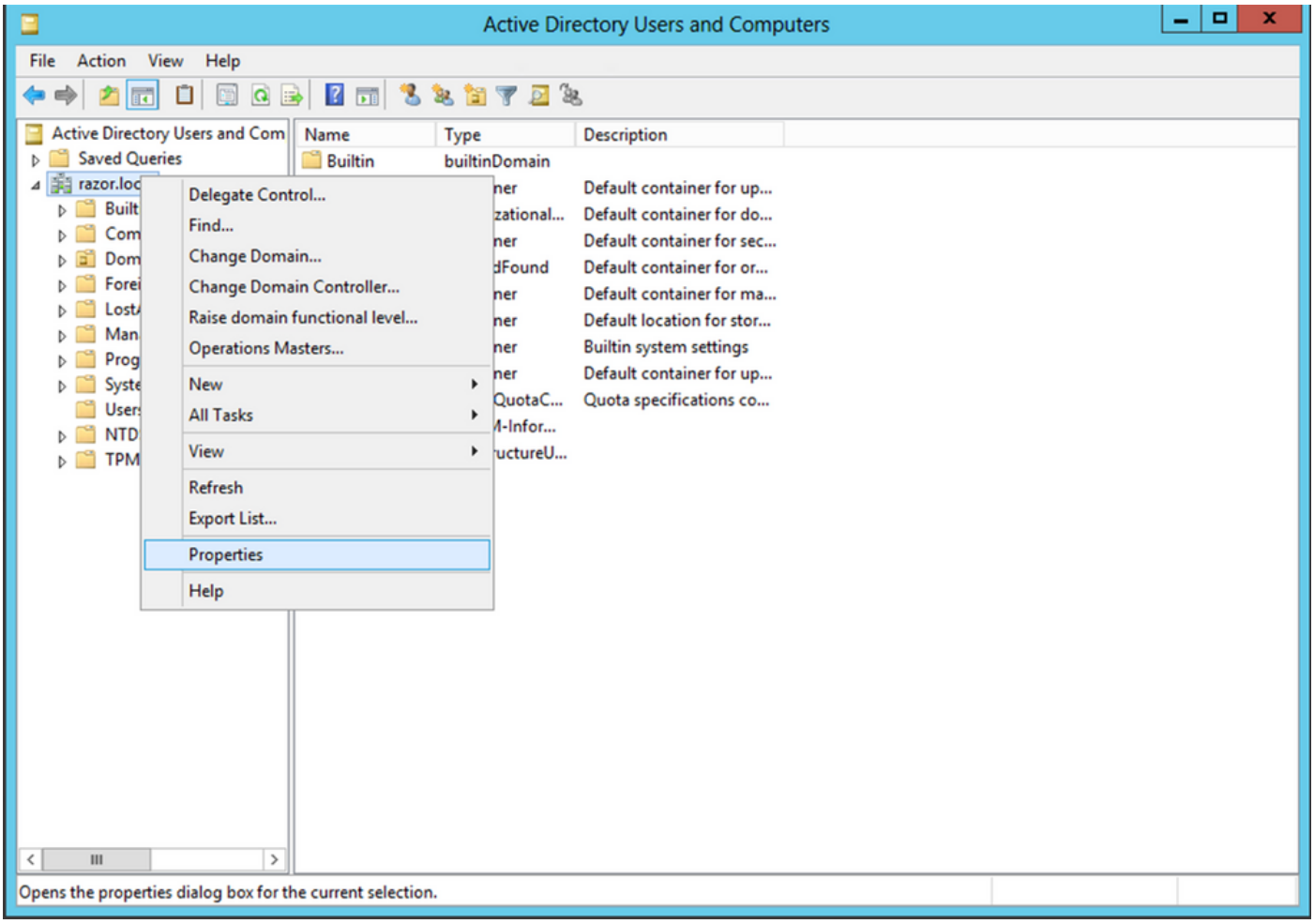
1. 開く Active Directory Users and Computers Server Manager Dashboardを使用します。



2. を開きます。 View Option をオンにし、 Advanced Featuresをクリックします（図を参照）。



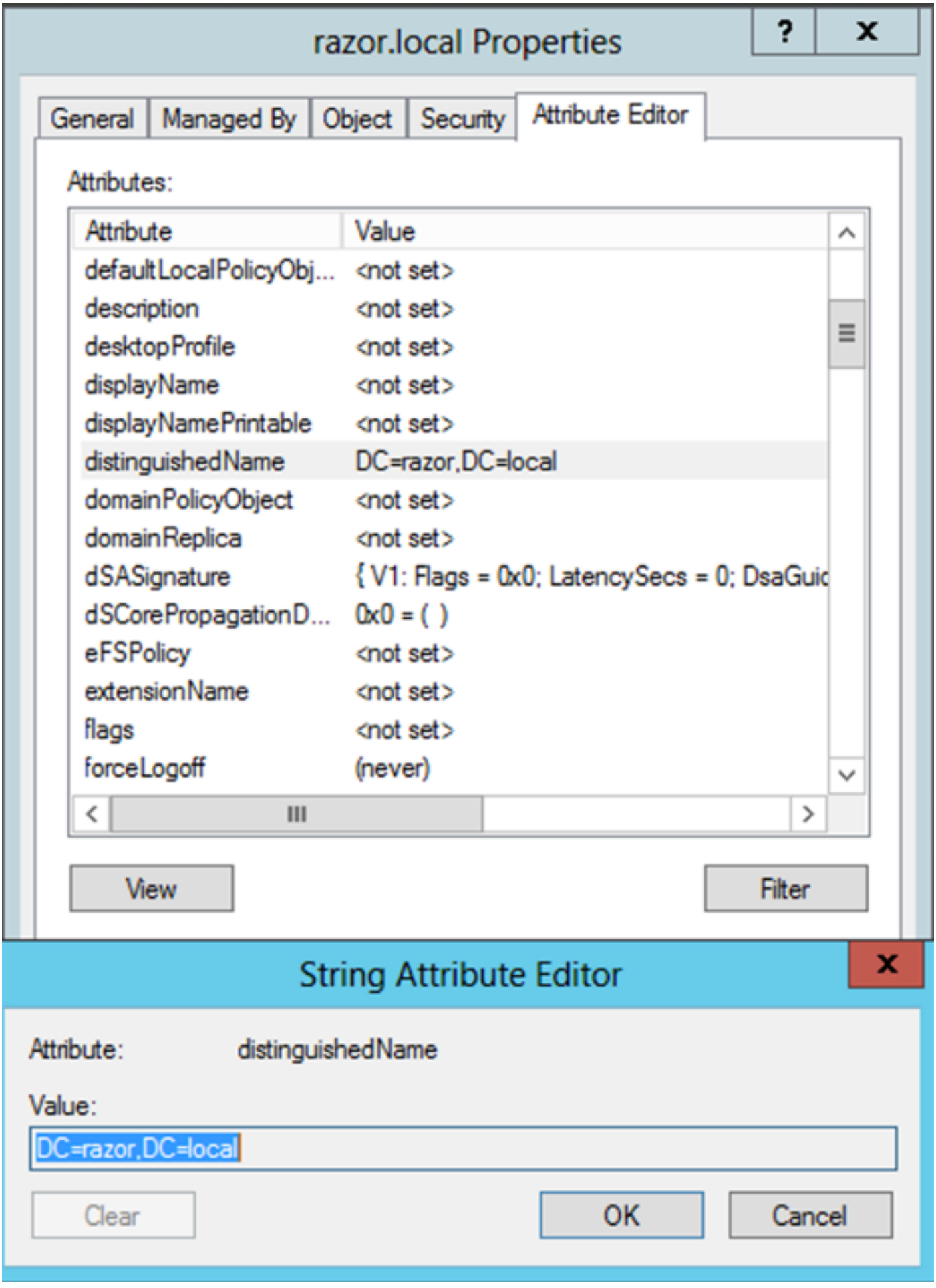
3. これにより、ADオブジェクトの下に追加のプロパティを表示できます。
   たとえば、ルートのDNを見つけるには、 razor.local、右クリック razor.localを選択し、 Properties次の図に示すように、



4. 通常の Propertiesを選択し、 Attribute Editor tab.検索 distinguishedName 「属性」の下のをクリックし、 Viewをクリックします。

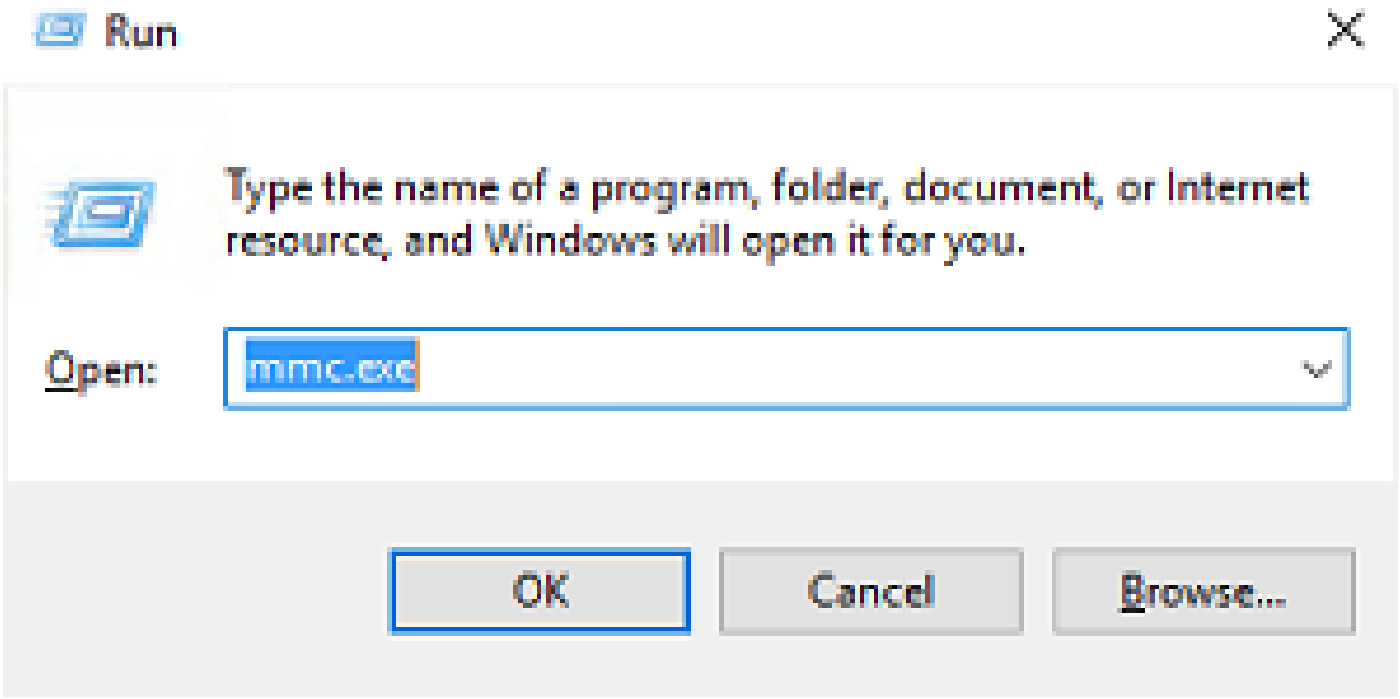
新しいウィンドウが開き、DNをコピーして後でFMCに貼り付けることができます。

この例では、ルートDNは DC=razor、 DC=localを参照。値をコピーして、後で使用できるように保存します。クリック OK String Attribute Editorウィンドウを終了し、 OK プロパティを終了します。

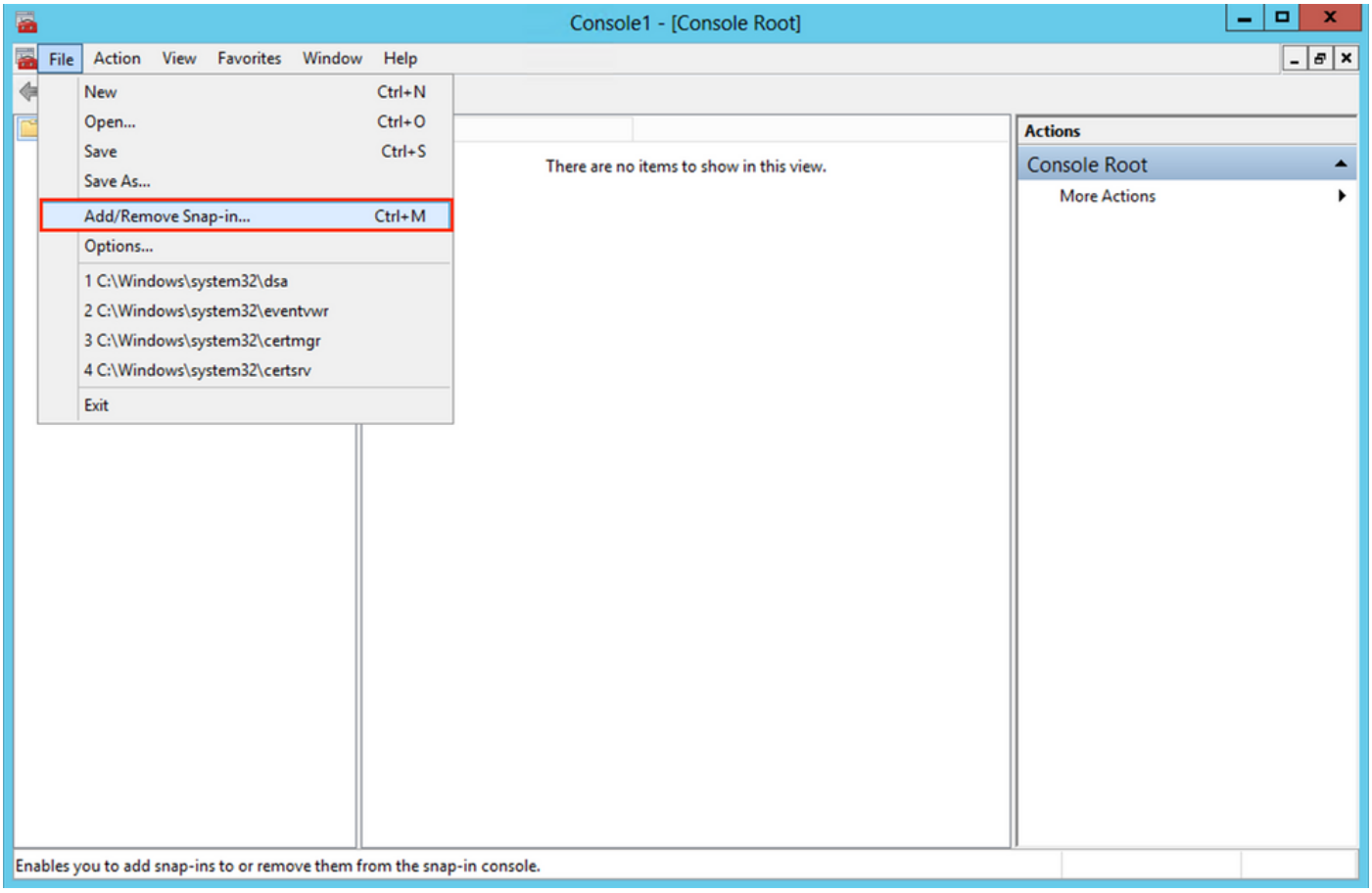

razor.local Properties
General
Managed By
Object
Security
Attribute Editor
Attributes:
Attribute
Value
defaultLocalPolicyObj...
<not set>
description
<not set>
desktopProfile
<not set>
displayName
<not set>
displayNamePrintable
<not set>
distinguishedName
DC=razor,DC=local
domainPolicyObject
<not set>
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証明書ルートのコピー

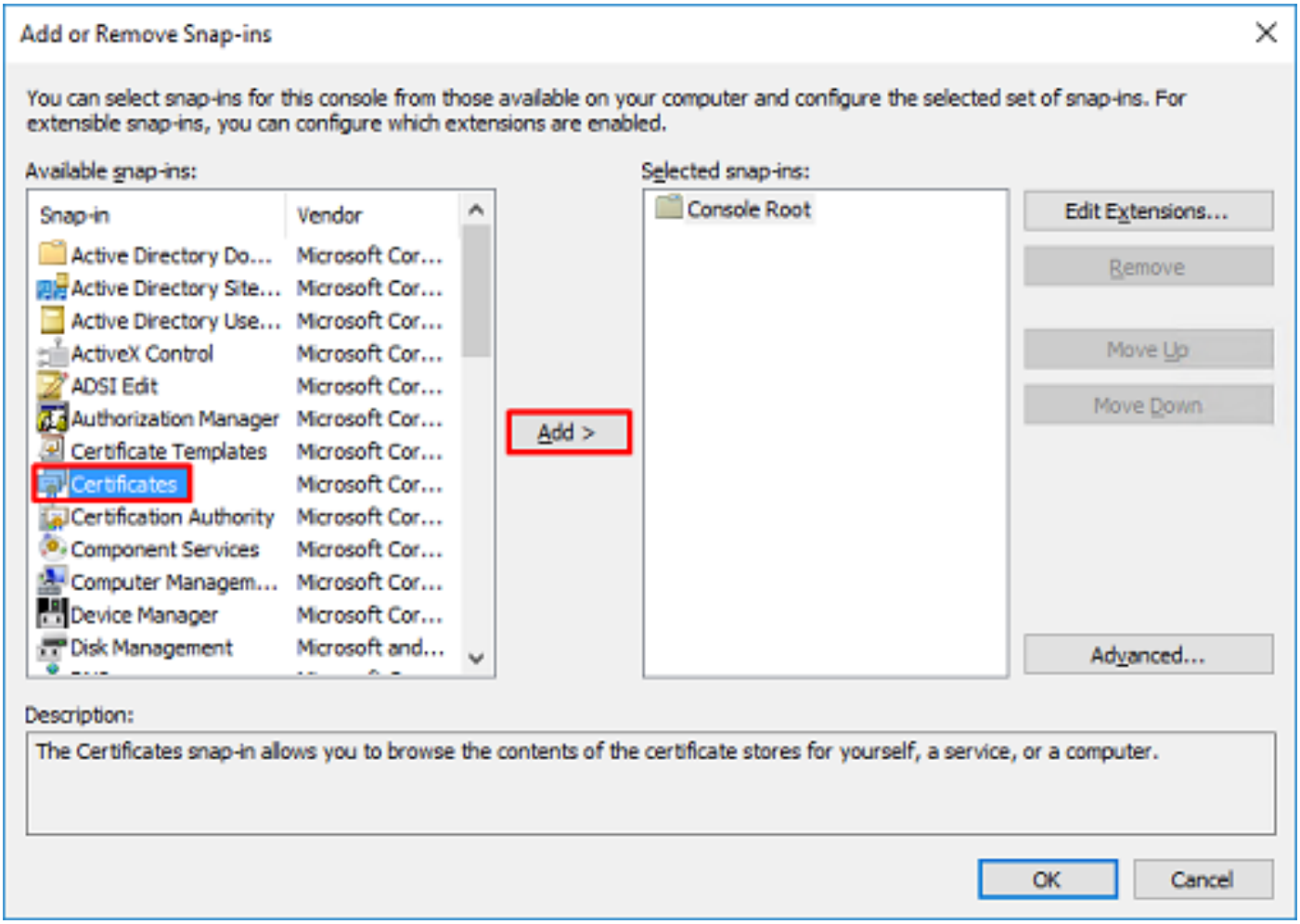
1. プレス Win+R 次のように入力します。 mmc.exeをクリックし、 OK,以下の図に、出力例を示します。



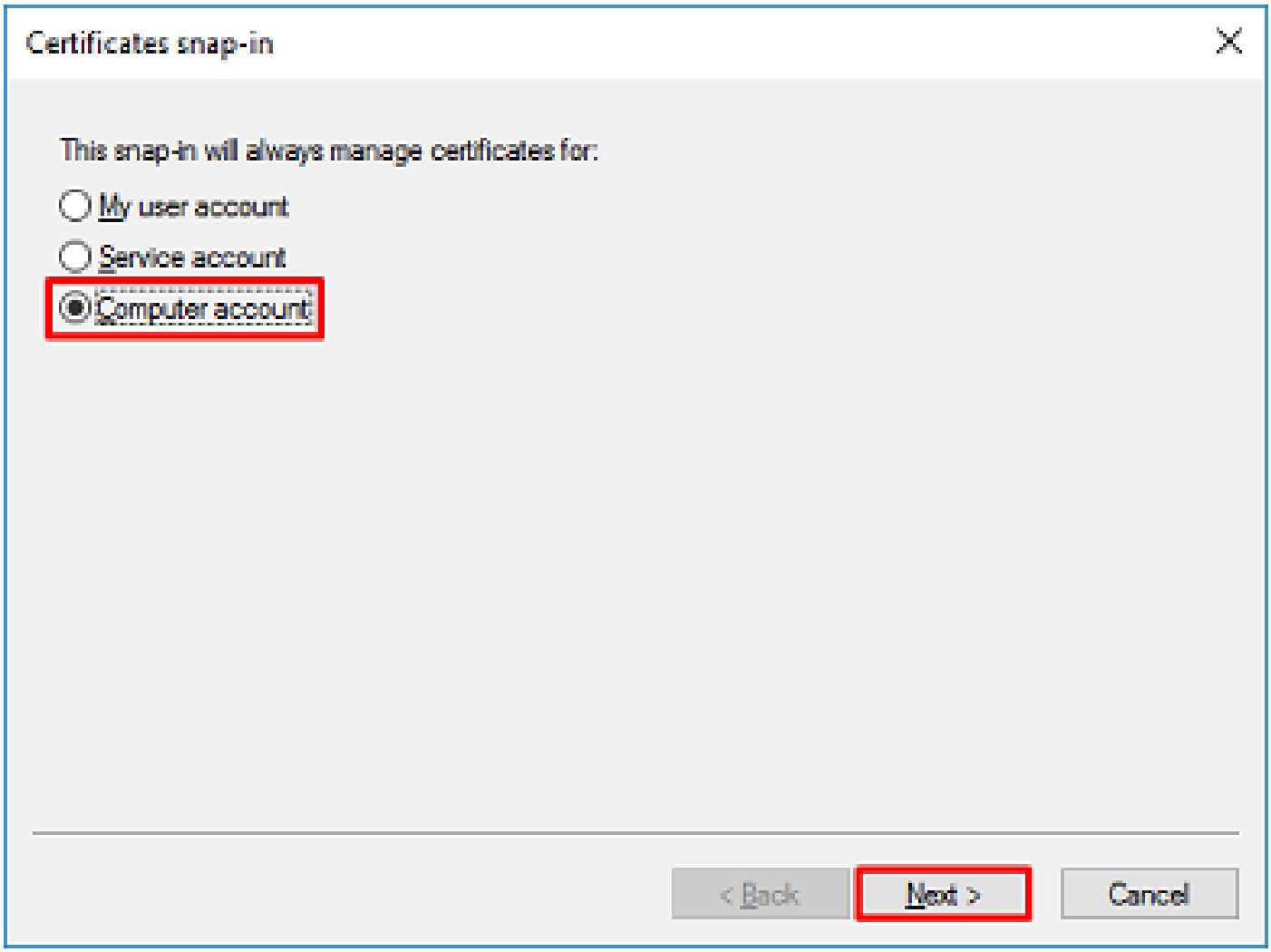
2. 移動先 File > Add/Remove Snap-in...、次の図に示すss:



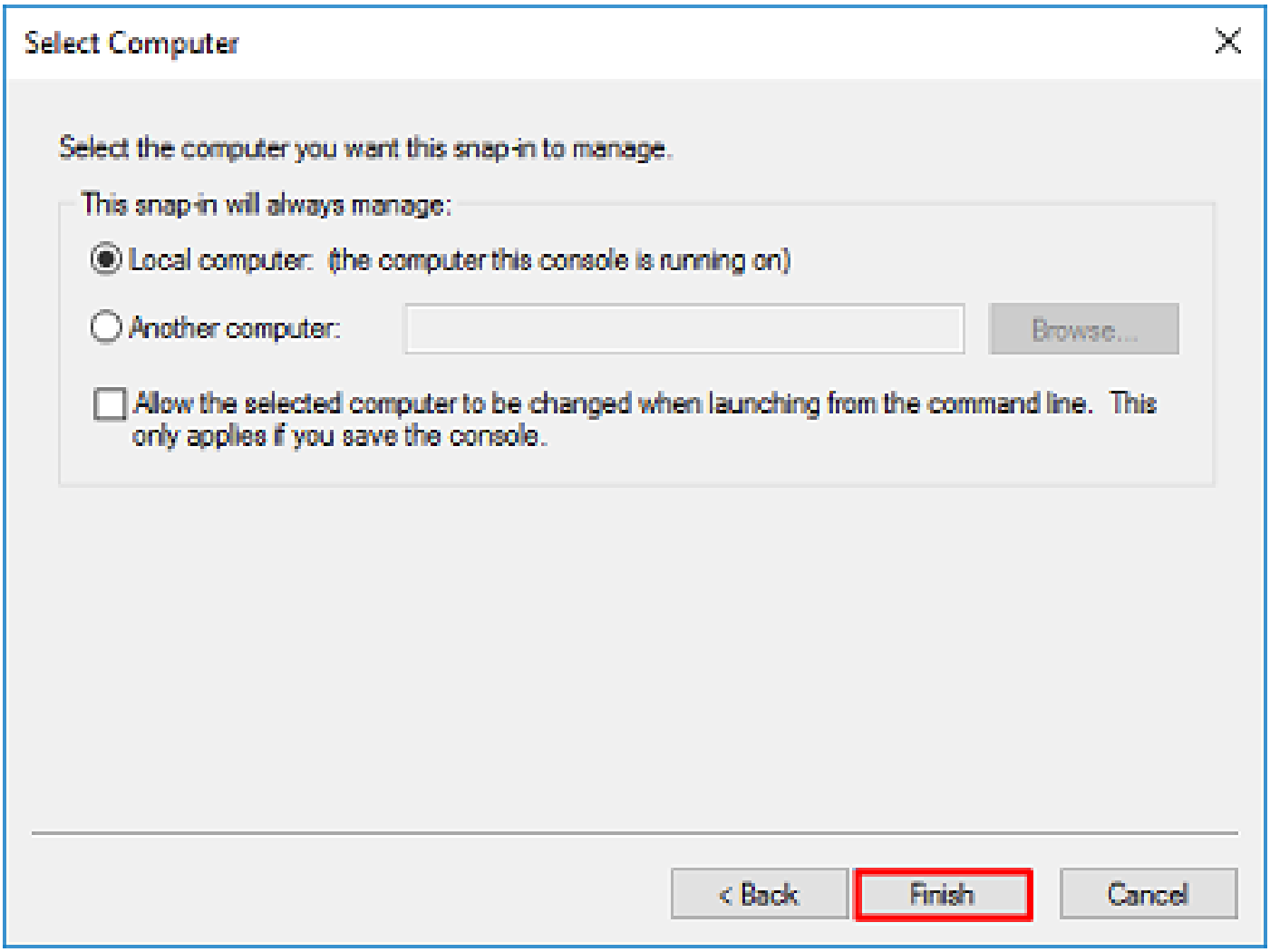
3. [使用可能なスナップイン]で、 Certificates 次に、 Add次の図に示すように、



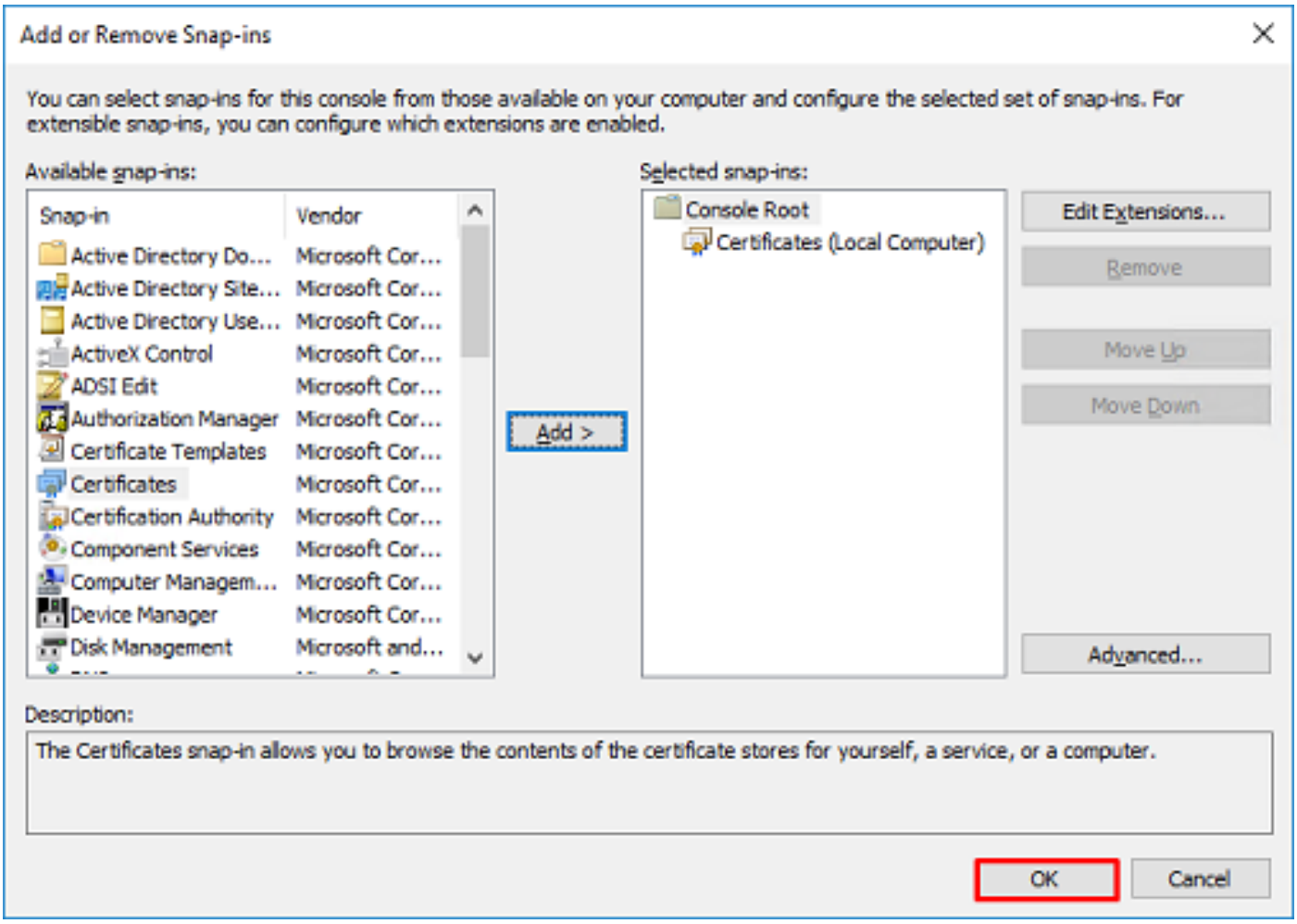
4. 選択 Computer account 次に、 Next次の図に示すように、



次に示すように、 Finishを参照。



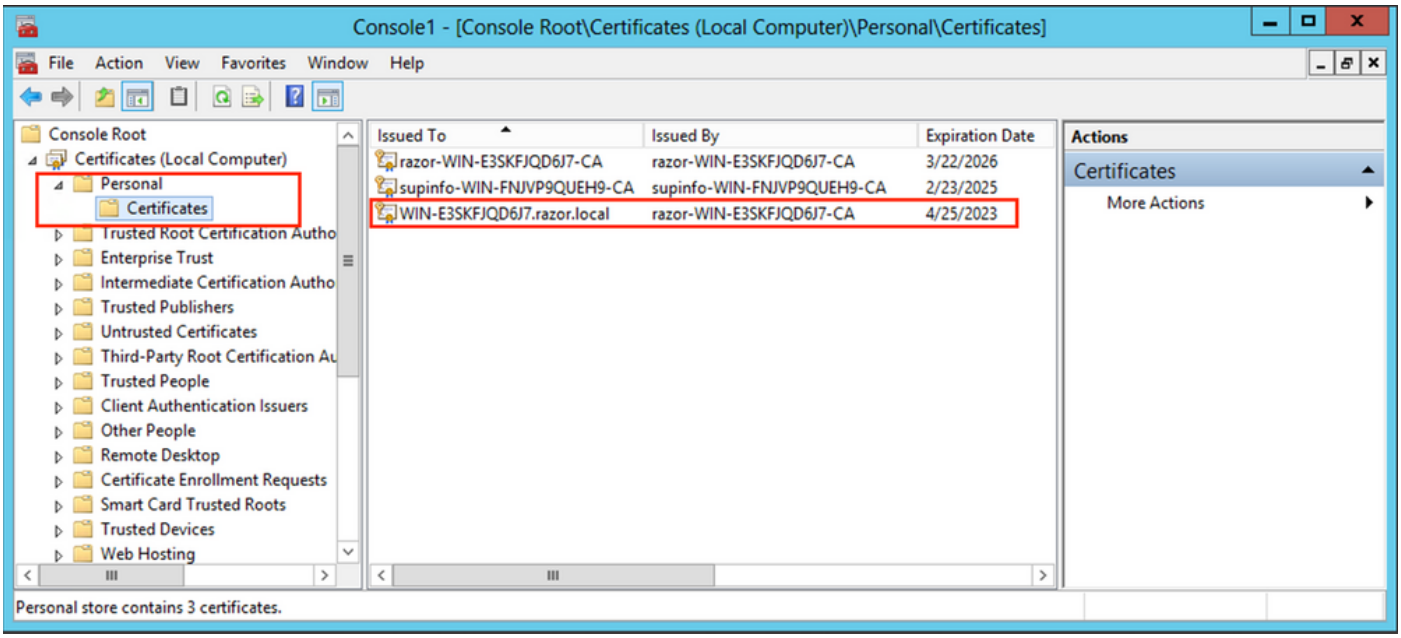
5. ここで、 OK,以下の図に、出力例を示します。



6. を展開します Personal フォルダを選択し、 Certificatesを参照。LDAPで使用される証明書は、Windowsサーバの完全修飾ドメイン名(FQDN)に対して発行する必要があります。このサーバには、次の3つの証明書がリストされています。

- CA証明書の発行先および発行元 razor-WIN-E3SKFJQD6J7-CAを参照。
- およびによって発行されたCA証明書 supinfo-WIN-FNJVP9QUEH9-CAを参照。
- ID証明書が発行されました WIN-E3SKFJQD6J7.razor.local by razor-WIN-E3SKFJQD6J7-CAを参照。

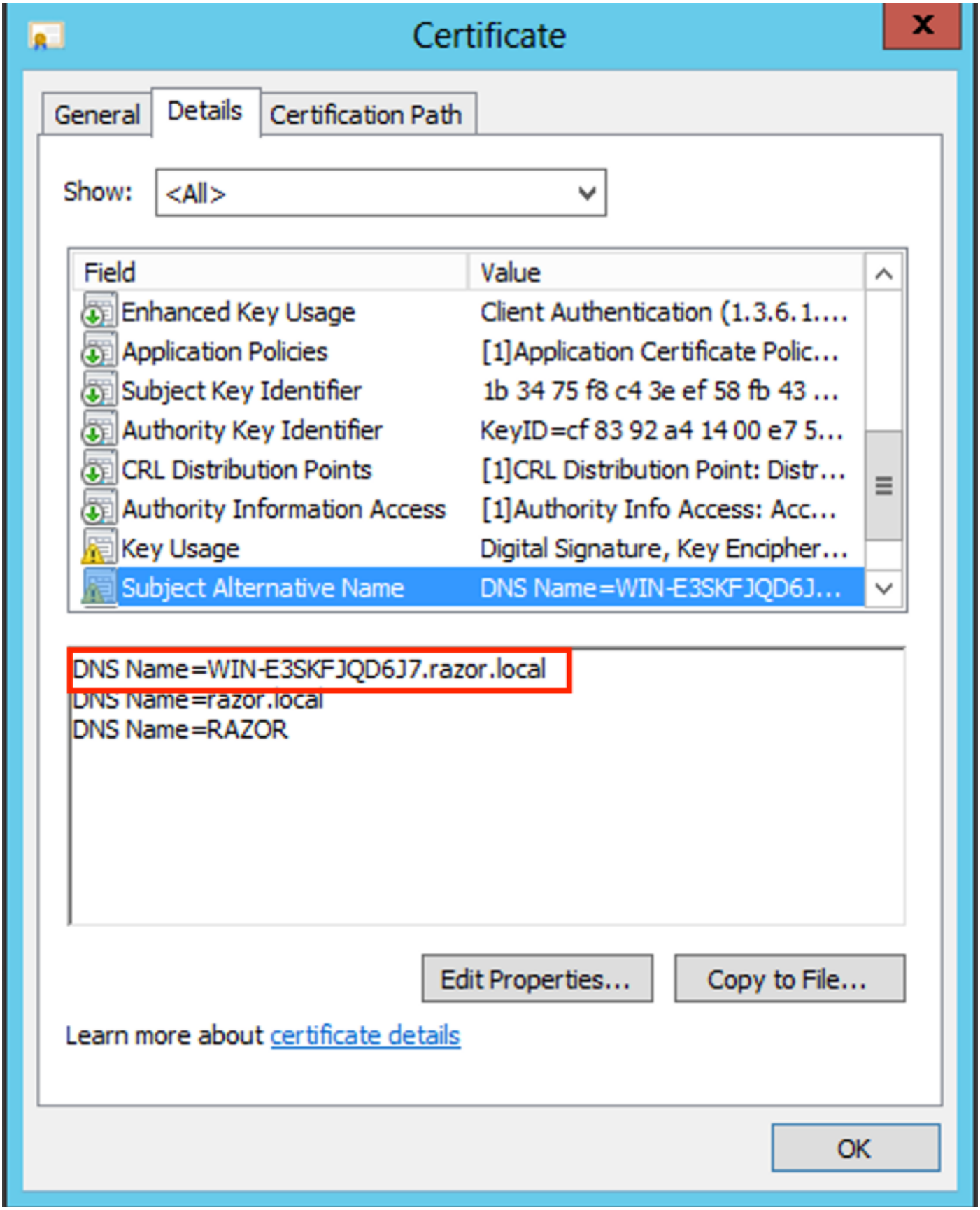
この設定ガイドでは、FQDNは WIN-E3SKFJQD6J7.razor.local したがって、最初の2つの証明書はLDAP SSL証明書として使用することはできません。ID証明書の発行先 WIN-E3SKFJQD6J7.razor.local は、Windows Server CAサービスによって自動的に発行された証明書です。詳細を確認するには、証明書をダブルクリックします。



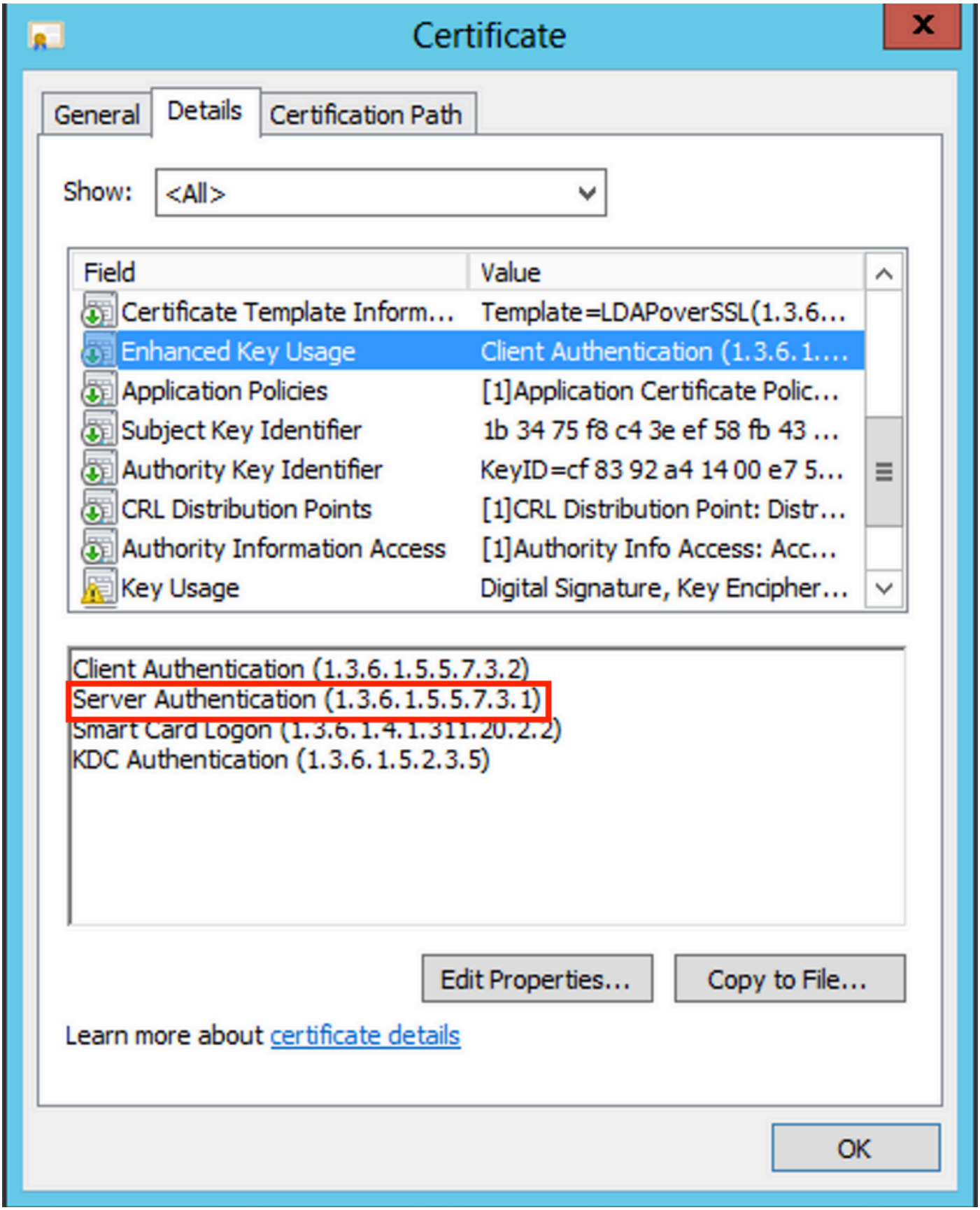
7. LDAP SSL証明書として使用するには、証明書が次の要件を満たしている必要があります。

- 共通名またはDNSサブジェクトの別名がWindows ServerのFQDNと一致します。
- 証明書のEnhanced Key Usageフィールドにサーバ認証が設定されている。

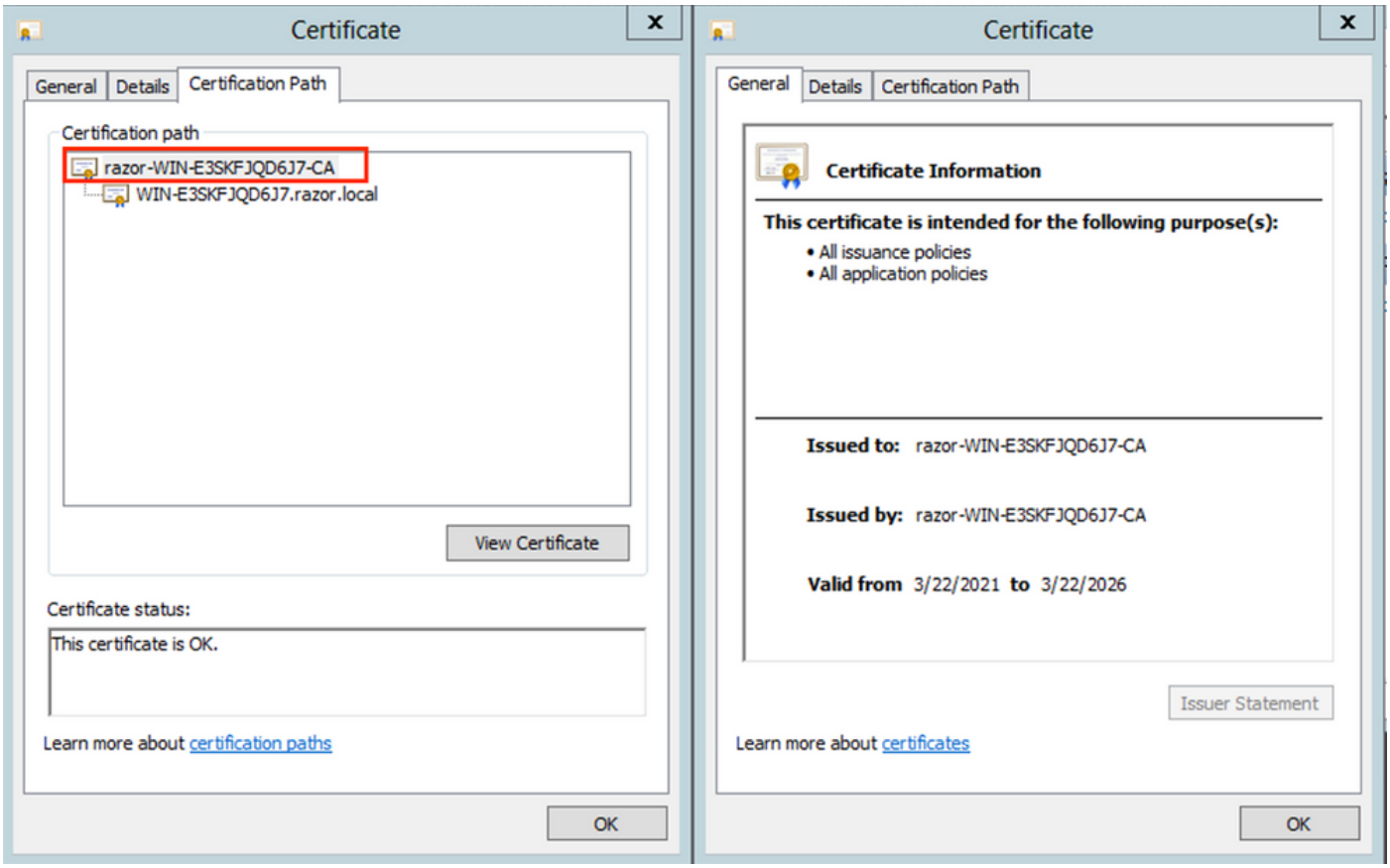
の下 Details タブをクリックし、 Subject Alternative NameFQDNが WIN-E3SKFJQD6J7.razor.local が存在します。



通常の Enhanced Key Usage、 Server Authentication が存在します。

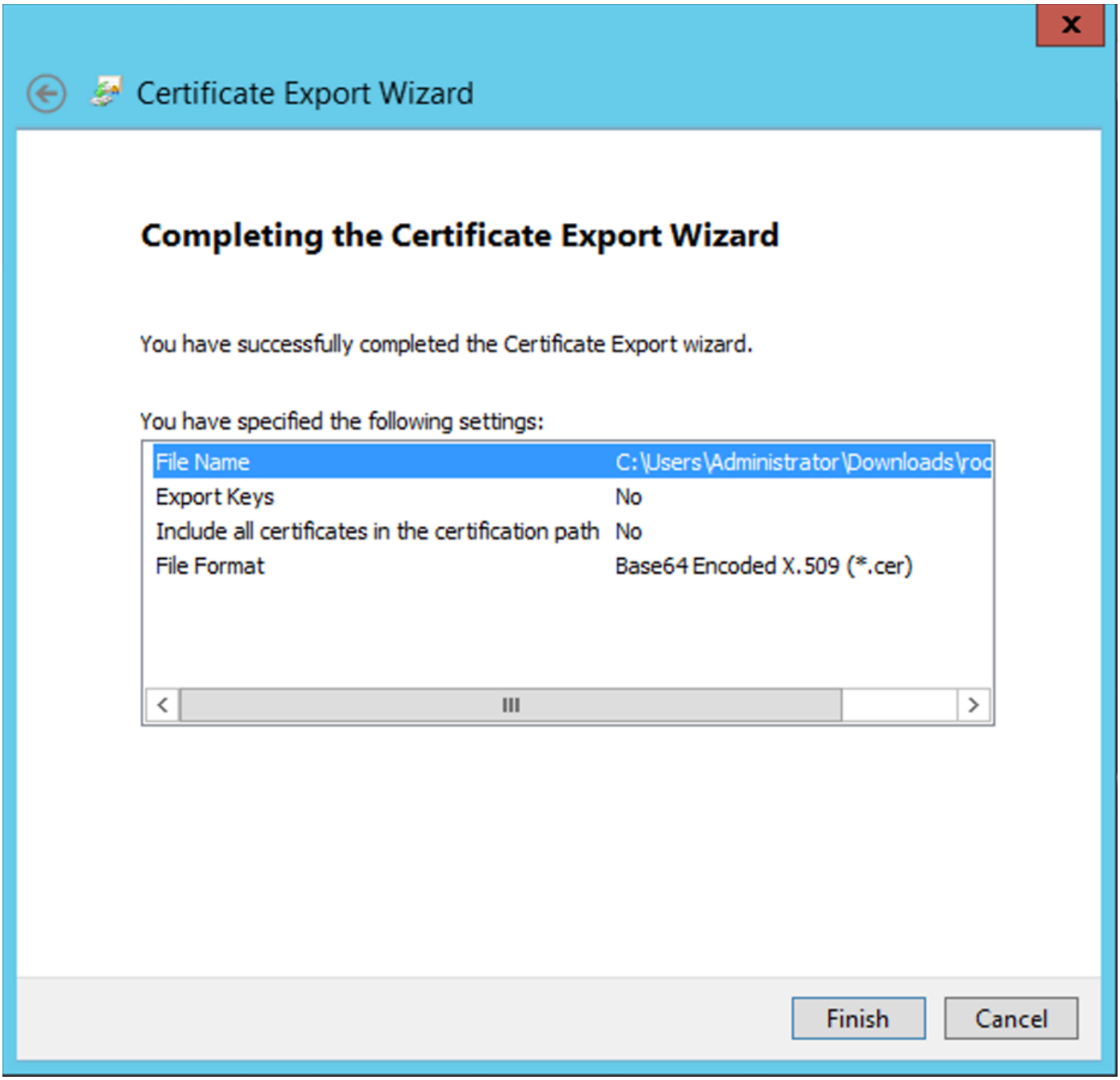


8. これが確認されたら、 Certification Path タブで、ルートCA証明書である最上位の証明書を選択し、 View Certificateを参照。次の図に示すように、ルートCA証明書の詳細な証明書が開きます。



9. の下 Details タブをクリックし、 Copy to File ネットワーク内のCertificate Export Wizard ルートCAをPEM形式でエクスポートします。

選択 Base-64 encoded X.509 をファイル形式として使用します。



10. メモ帳またはその他のテキストエディタを使用して、マシン上の選択した場所に格納されているルートCA証明書を開きます。

PEM形式の証明書を示します。後で使用するために保存します。

```
-----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サーバのローカルマシンストアに複数の証明書がインストールされている場合（オプション）

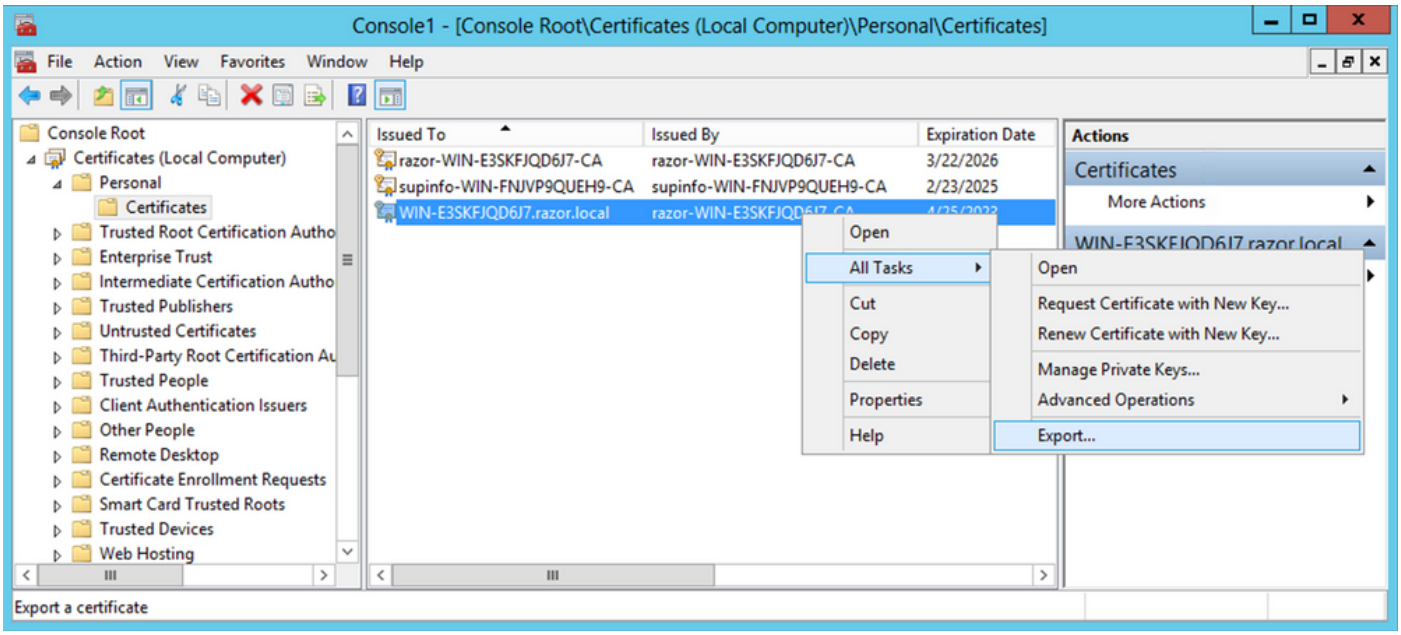
1. LDAPSで使用できるID証明書が複数ある状況で、使用されるIDが不明な場合、またはLDAPSサーバへのアクセスがない場合でも、FTDで実行されたパケットキャプチャからルートCAを抽出することは可能です。

2. LDAPサーバー（AD DSドメインコントローラーなど）のローカルコンピューターの証明書ストアに、サーバー認証に有効な証明書が複数ある場合は、LDAPS通信に別の証明書が使用されている可能性があります。このような問題の最善の解決策は、ローカルコンピュータの証明書ストアから不要な証明書をすべて削除し、サーバ認証に有効な証明書を1つだけ保持することです。

ただし、複数の証明書が必要で、少なくとも1台のWindows Server 2008 LDAPサーバを所有しているという正当な理由がある場合は、LDAP通信にActive Directoryドメインサービス(NTDS\Personal)証明書ストアを使用できます。

次の手順では、LDAPS対応の証明書をドメインコントローラーのローカルコンピューターの証明書ストアからActive Directoryドメインサービスのサービスの証明書ストア(NTDS\Personal)にエクスポートする方法を示します。

- Active DirectoryサーバのMMCコンソールに移動し、Fileを選択して、 Add/Remove Snap-inを参照。
- クリック Certificates 次に、 Addを参照。
- 内 Certificates snap-in,選択 Computer account 次に、 Nextを参照。
- イン Select Computer,選択 Local Computerをクリックし、 OKをクリックし、 Finishを参照。イン Add or Remove Snap-insをクリックし、 OKを参照。
- サーバ認証に使用する証明書が格納されているコンピュータの証明書コンソールで、certificateをクリックし、 All Tasksをクリックし、 Exportを参照。

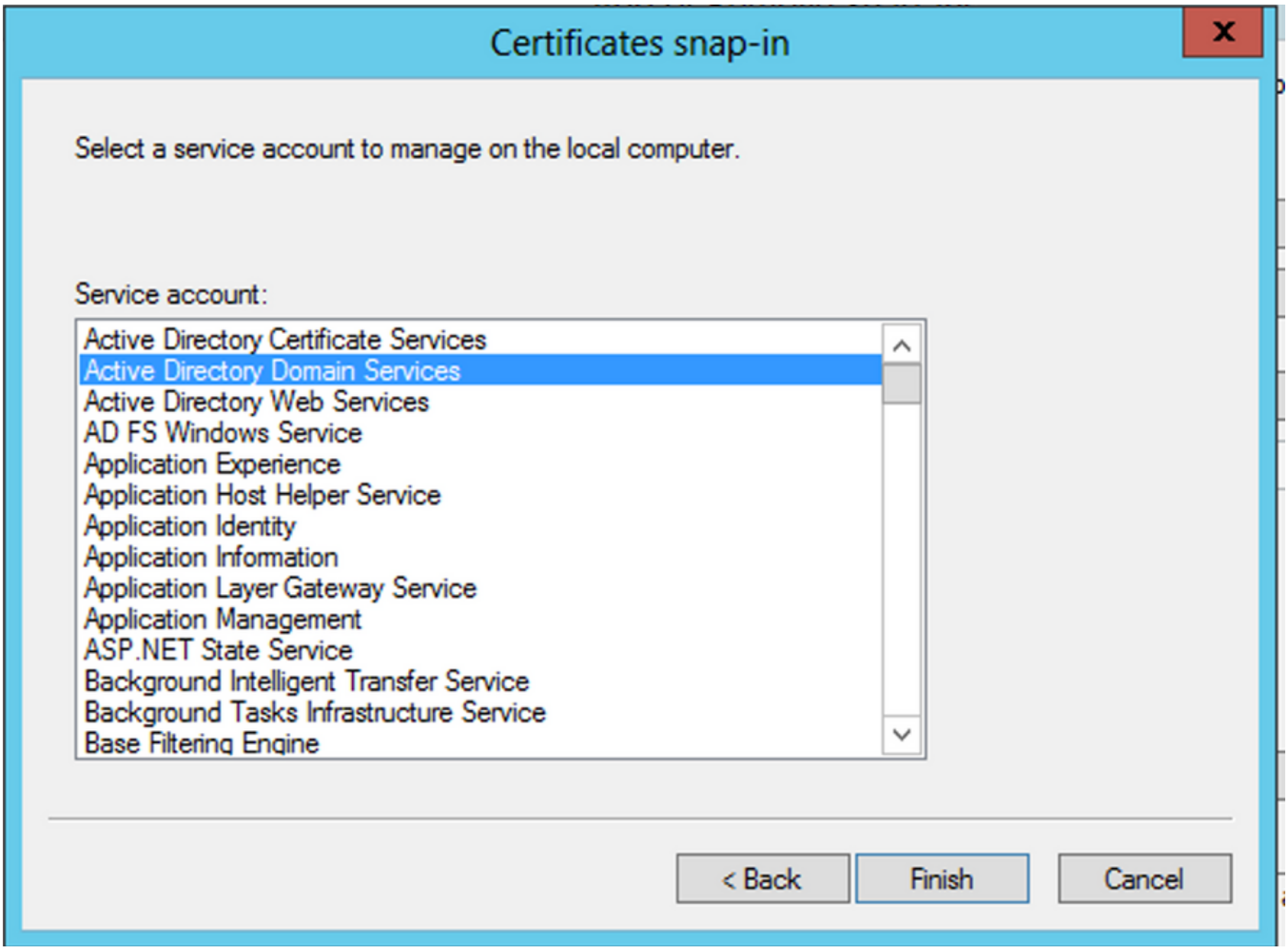


- 証明書を pfx フォーマットについては、以降のセクションを参照してください。で証明書をエクスポートする方法については、この記事を参照してください。 pfx mmcからのフォーマット：

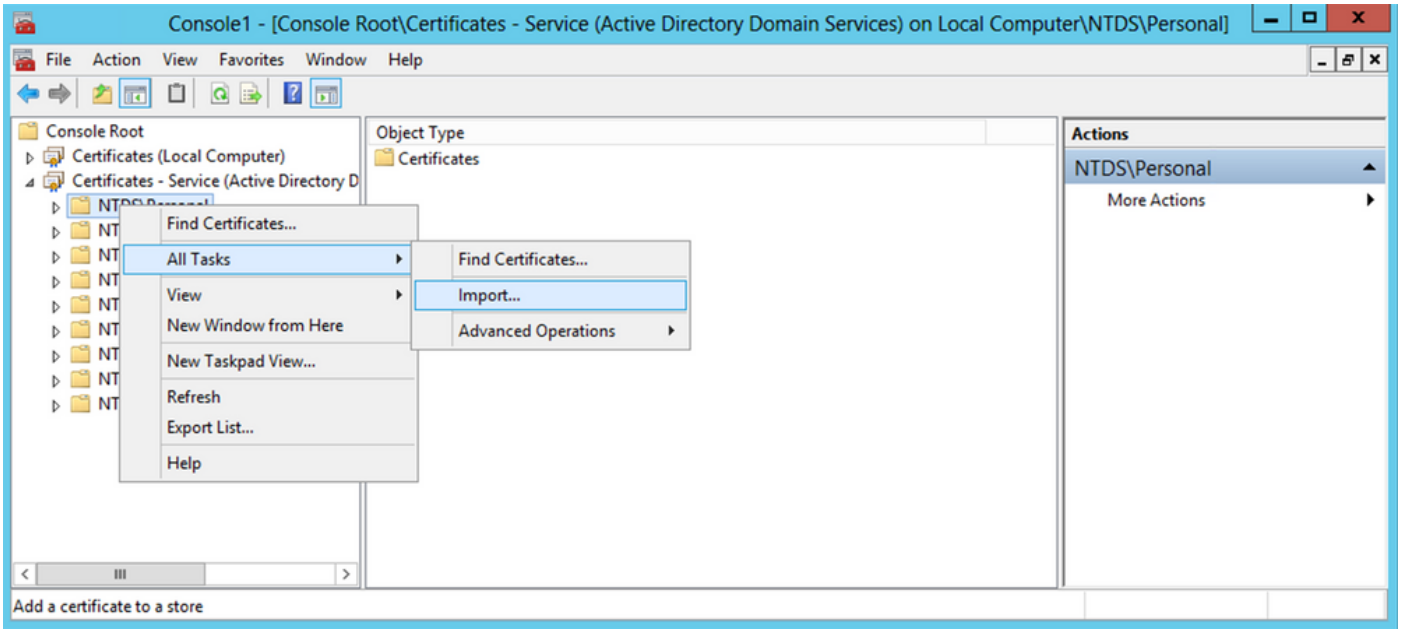
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html にアクセスしてください。

- 証明書のエクスポートが完了したら、 Add/Remove Snap-in 日付： MMC consoleを参照。クリック Certificates 次に、 Addを参照。
- 選択 Service account 次に、 Nextを参照。

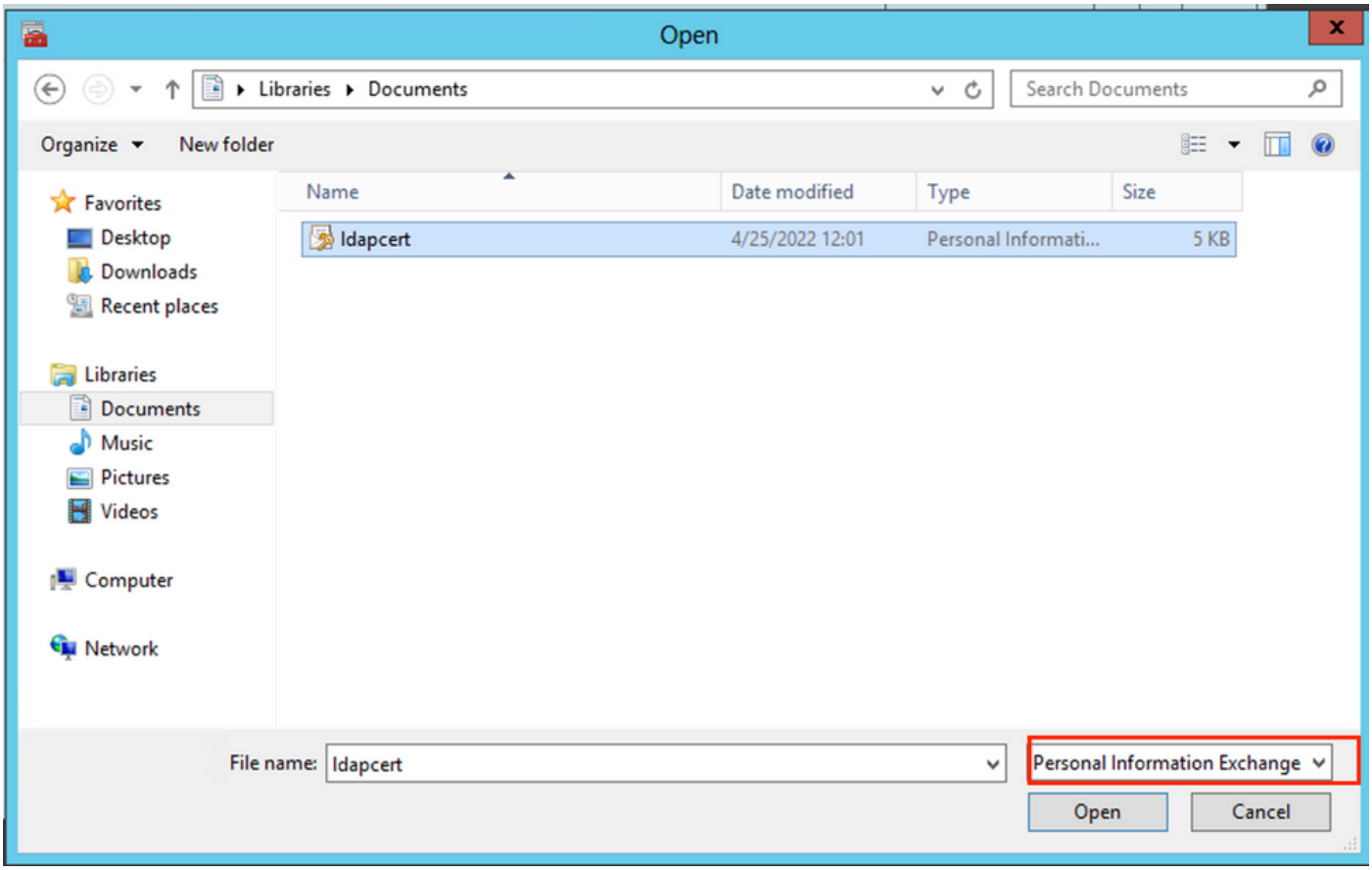
- 内 Select Computer ダイアログボックス、選択 Local Computer をクリックして Nextを参照。
- 選択 Active Directory Domain Services 次に、 Finishを参照。



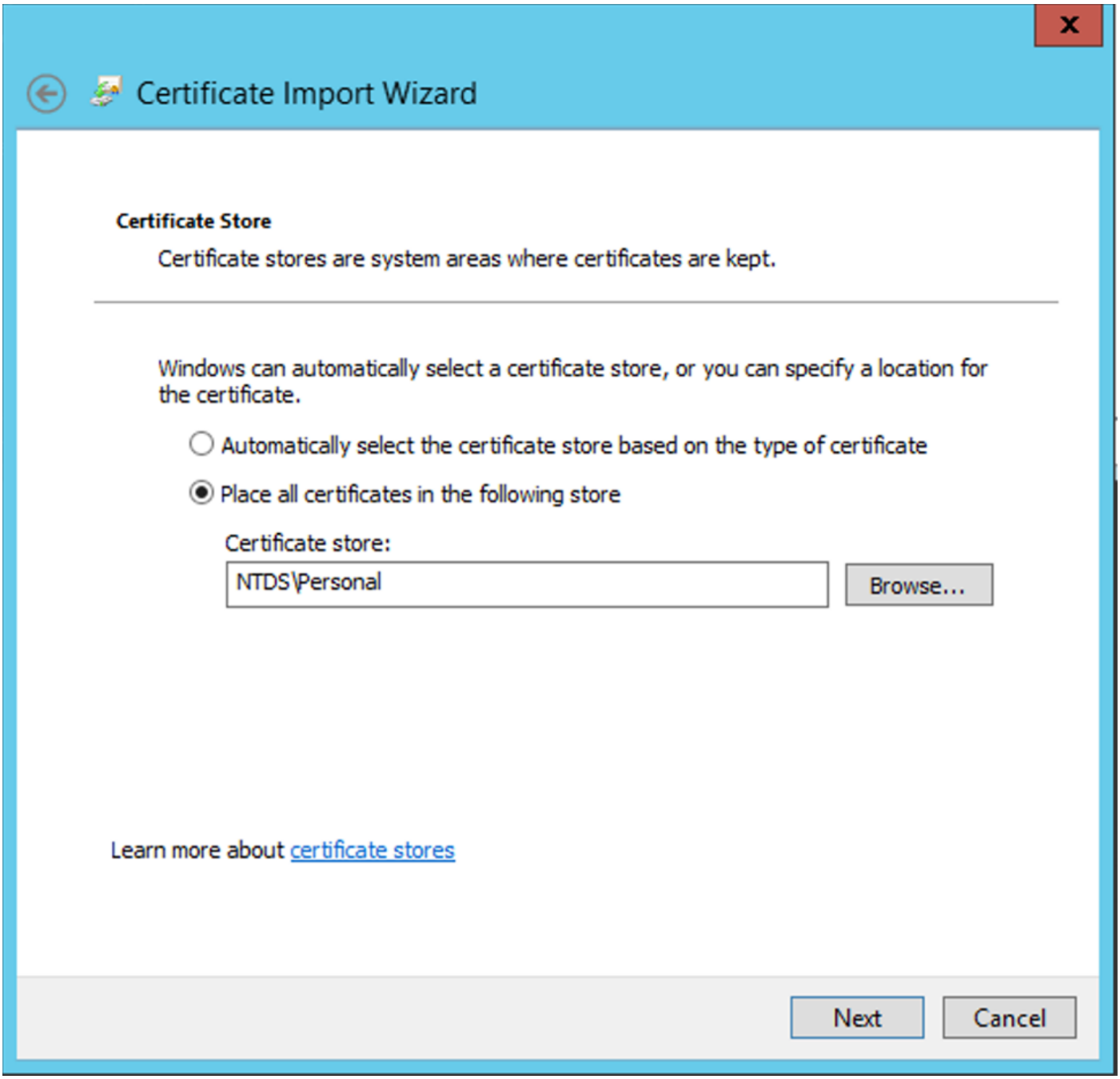
- 次の Add/Remove Snap-ins ダイアログボックスを開き、 OKを参照。
- 拡張 Certificates - Services (Active Directory Domain Services) 次に、 NTDS\Personalを参照。
- 右クリック NTDS\Personalをクリックし、 All Tasksをクリックし、 Importを参照。



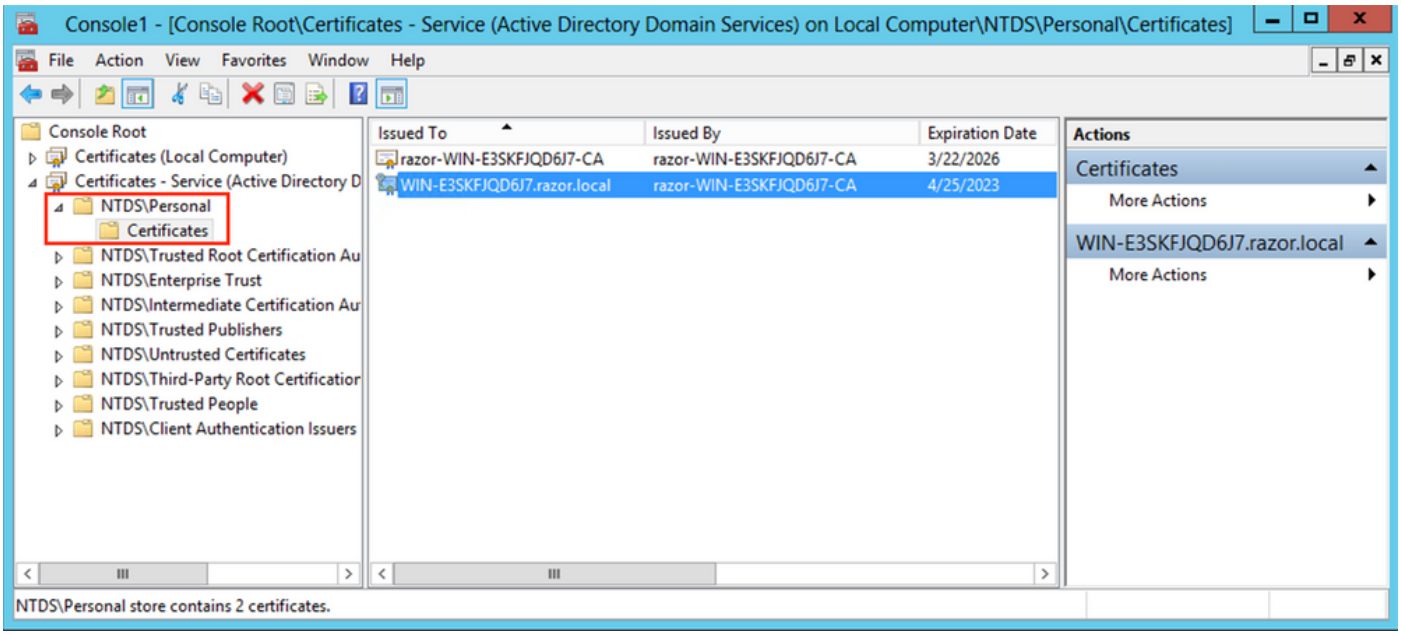
- 次の Certificate Import Wizard ようこそ画面で、 Nextを参照。
- [インポートするファイル]画面で、 Browseをクリックし、以前にエクスポートした証明書ファイルを探します。
- Open画面で、Personal Information Exchange(*pfx、*.p12)をファイルタイプとして選択し、ファイルシステムをナビゲートして、以前にエクスポートした証明書を見つけます。次に、その証明書をクリックします。



- クリック Open 次に、 Nextを参照。
- [パスワード]画面で、ファイルに設定したパスワードを入力し、 Nextを参照。
- Certificate Storeページで、Place all certificatesが選択されていることを確認し、Certificate Storeを読み取ります。 NTDS\Personal 次に、 Nextを参照。



- 次の Certificate Import Wizard 完了の画面で、 Finishを参照。インポートが成功したことを示すメッセージが表示されます。クリック OKを参照。証明書が証明書ストアにインポートされたことを確認できます。 NTDS\Personalを参照。



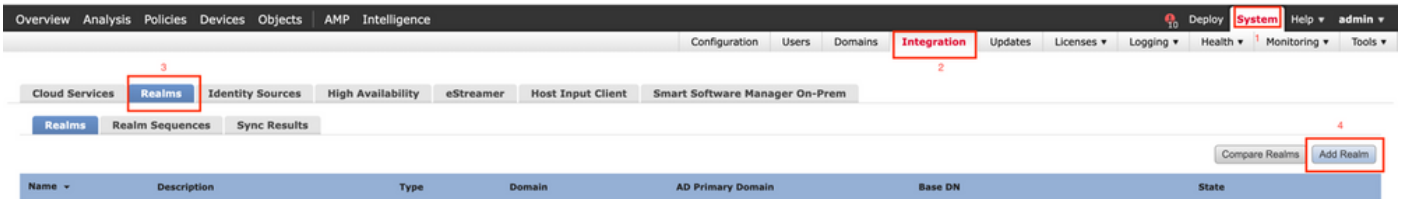
FMCの設定

ライセンスの確認

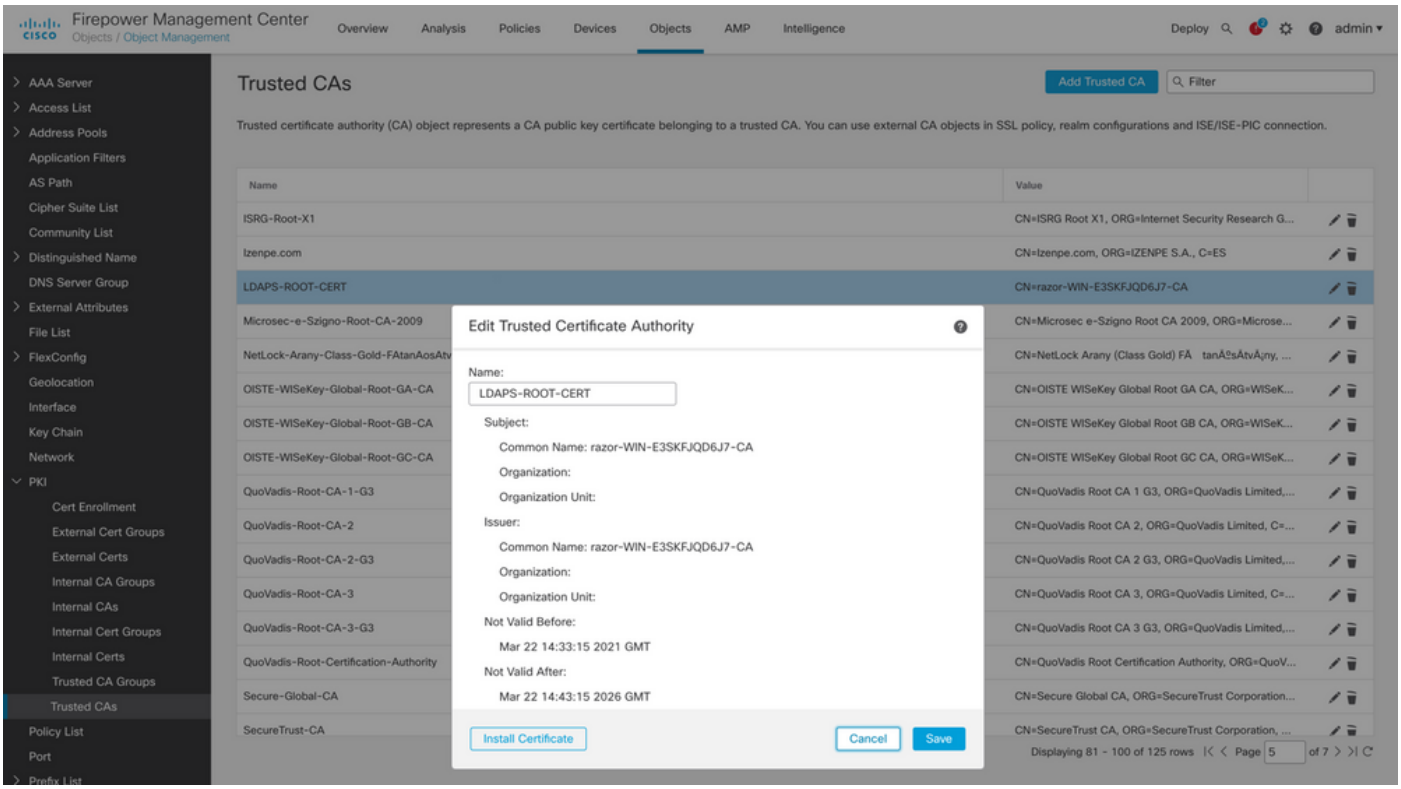
AnyConnect設定を導入するには、FTDがスマートライセンスサーバに登録され、有効なPlus、Apex、またはVPN Onlyライセンスがデバイスに適用されている必要があります。

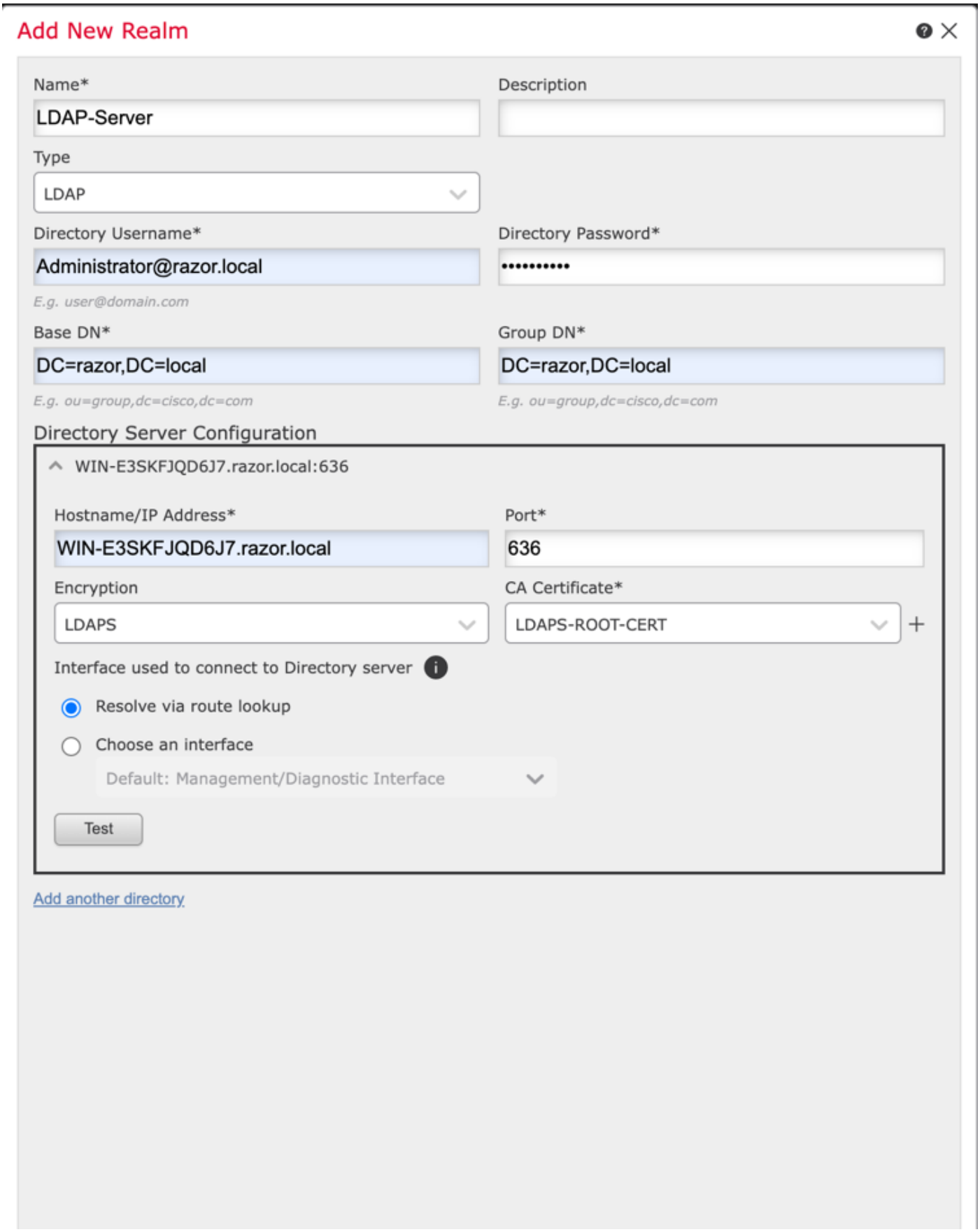
レルムの設定

1. 移動先 System > Integrationを参照。移動先 Realmsをクリックし、 Add Realm次の図に示すように、



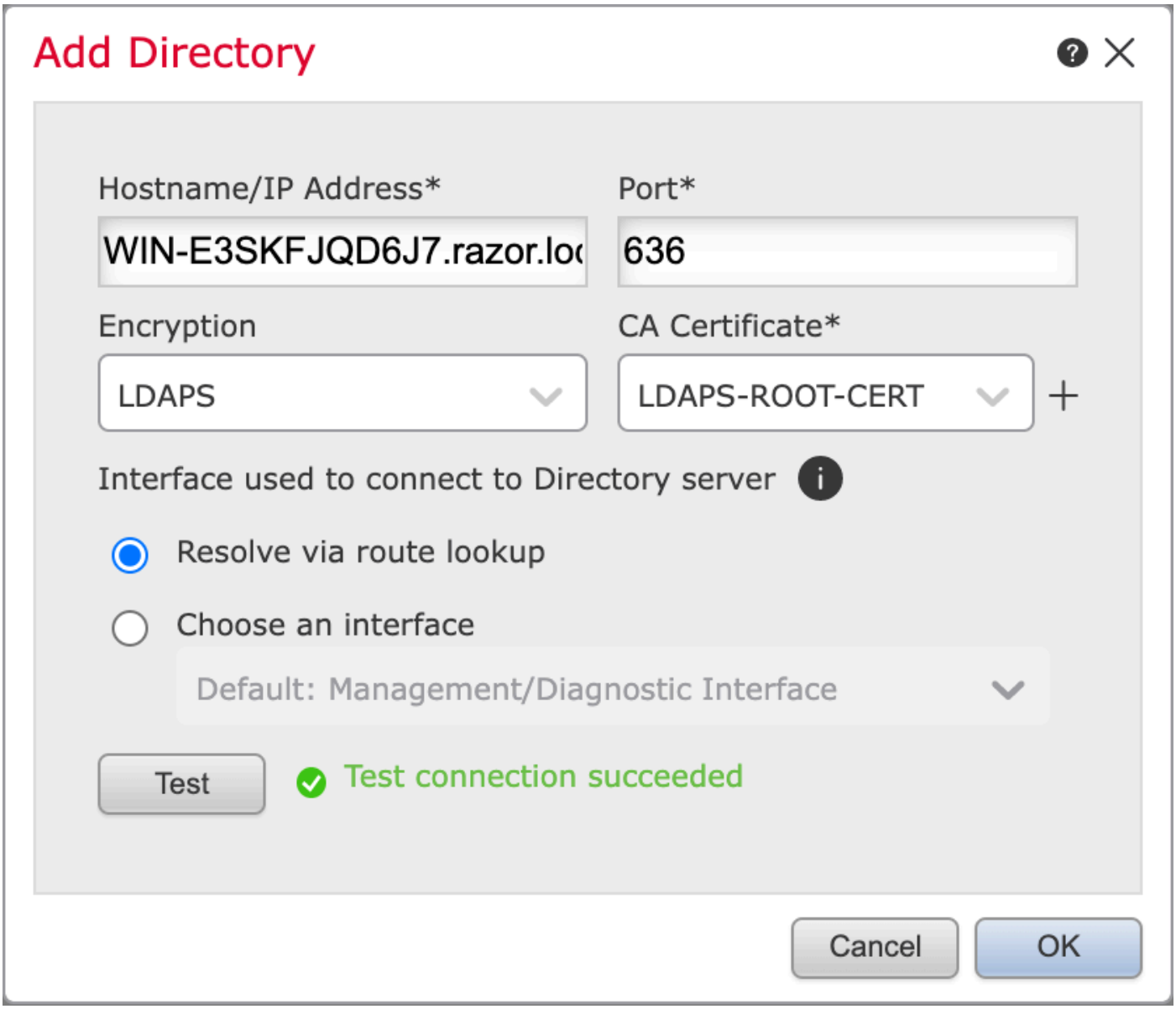
2. LDAPに関してMicrosoftサーバから収集した情報に基づいて、表示されているフィールドに入力します。その前に、LDAPsサービス証明書に署名したルートCA証明書をWindows Serverの Objects > PKI > Trusted CAs > Add Trusted CAを参照してください。これはDirectory Server Configuration を指定します。完了したら、 OKを参照。


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

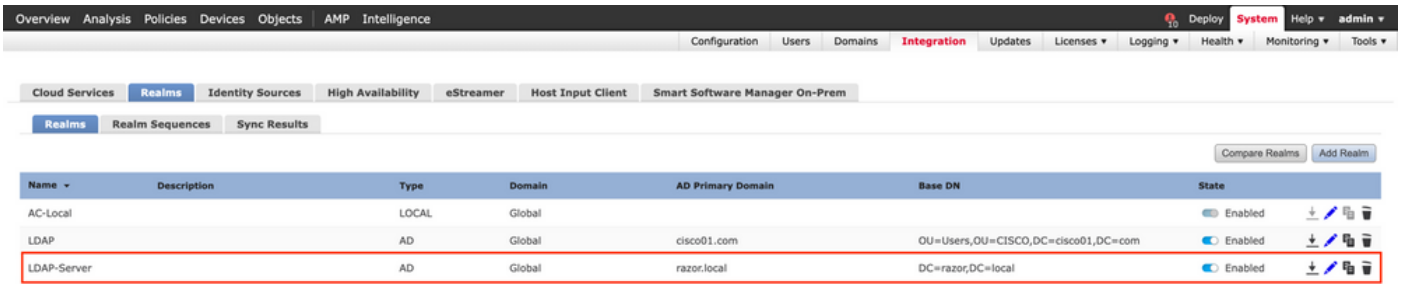


3. クリック Test FMCが、前の手順で指定したディレクトリのユーザ名とパスワードで正常にバインドできることを確認します。これらのテストは、FTDに設定されたルーティング可能なインターフェイス（inside、outside、dmzなど）の1つではなく、FMCから開始されるため、接続が成功（または失敗）しても、AnyConnect LDAP認証要求がFTDのルーティング可

能なインターフェイスの1つから開始されるため、AnyConnect認証で同じ結果が得られることは保証されません。

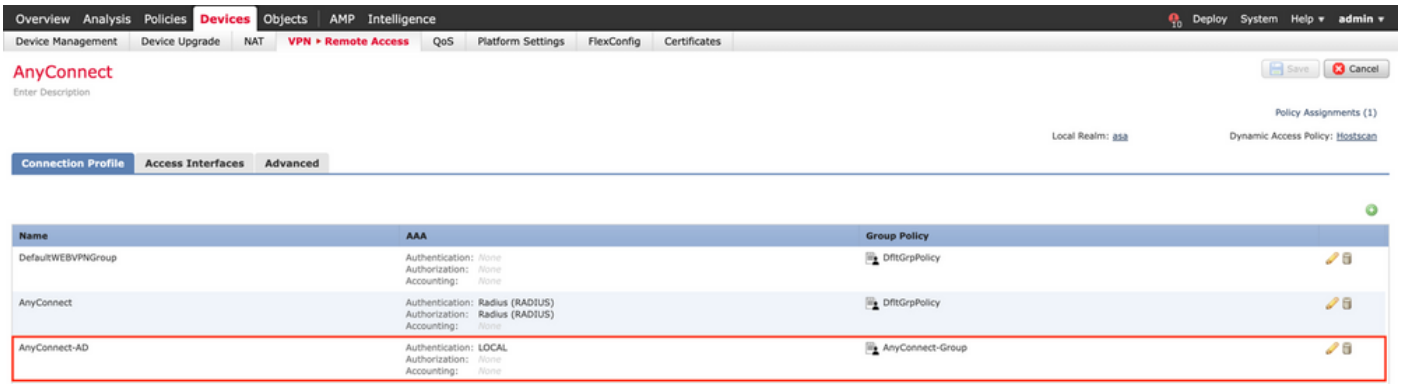


4. 新しいレルムを有効にします。

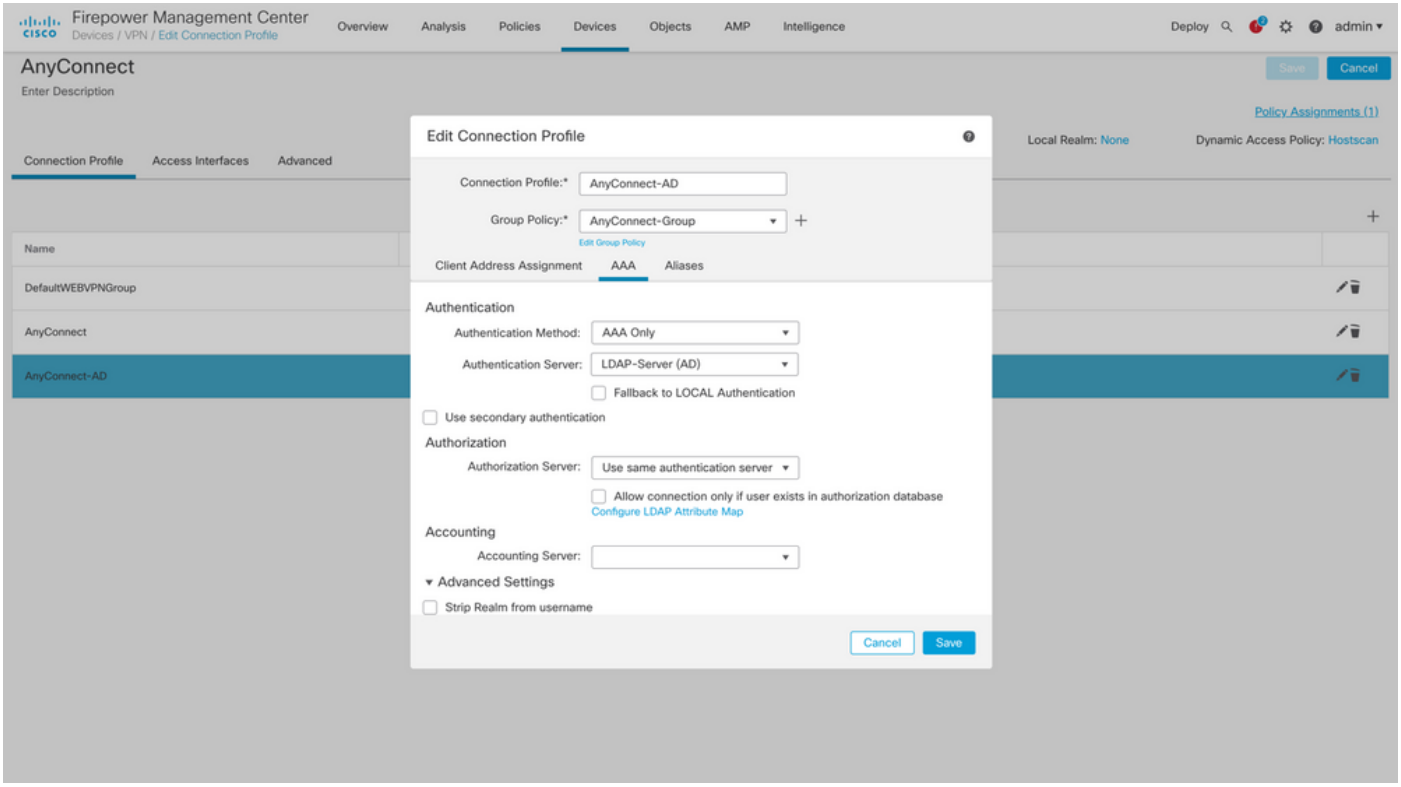


パスワード管理用のAnyConnectの設定

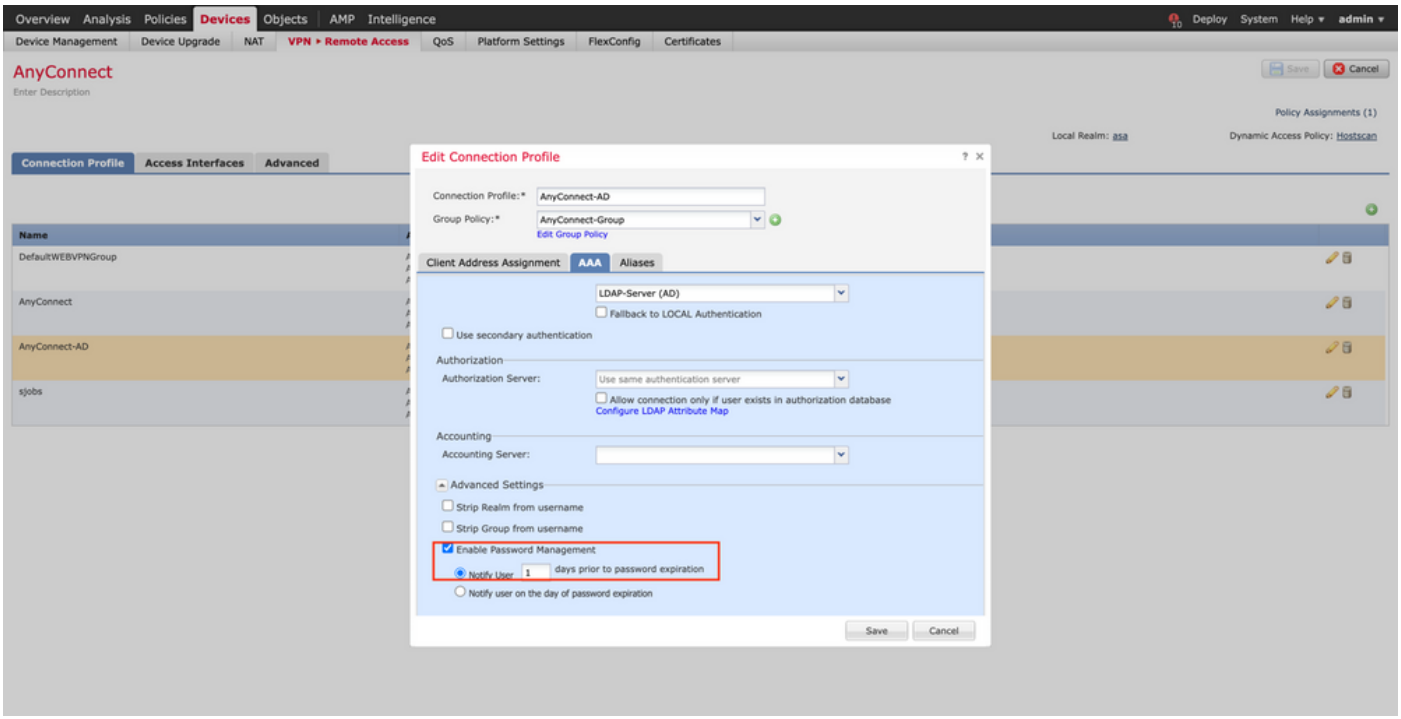
1. AnyConnectの初期設定の場合は、既存の接続プロファイルを選択するか、新しい接続プロファイルを作成します。ここでは、ローカル認証にマッピングされた「AnyConnect-AD」という名前の既存の接続プロファイルが使用されます。



2. 接続プロファイルを編集し、前の手順で設定した新しいLDAPサーバを接続プロファイルのAAA設定の下にマッピングします。完了したら、 Save をクリックします。



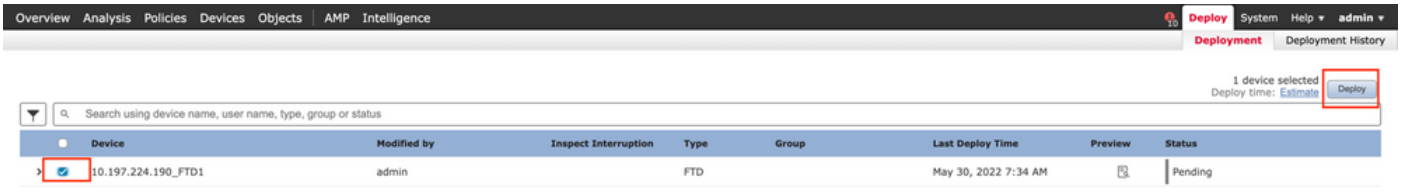
3. パスワード管理を有効にする AAA > Advanced Settings 設定を保存します。



展開

1. すべての設定が完了したら、Deploy ボタンをクリックします。

2. 適用されているFTD設定の横にあるチェックボックスをクリックし、 Deploy次の図に示すように、



Final Configuration

これは、導入が成功した後にFTD CLIに表示される設定です。

AAA 設定

<#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の設定

<#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
```

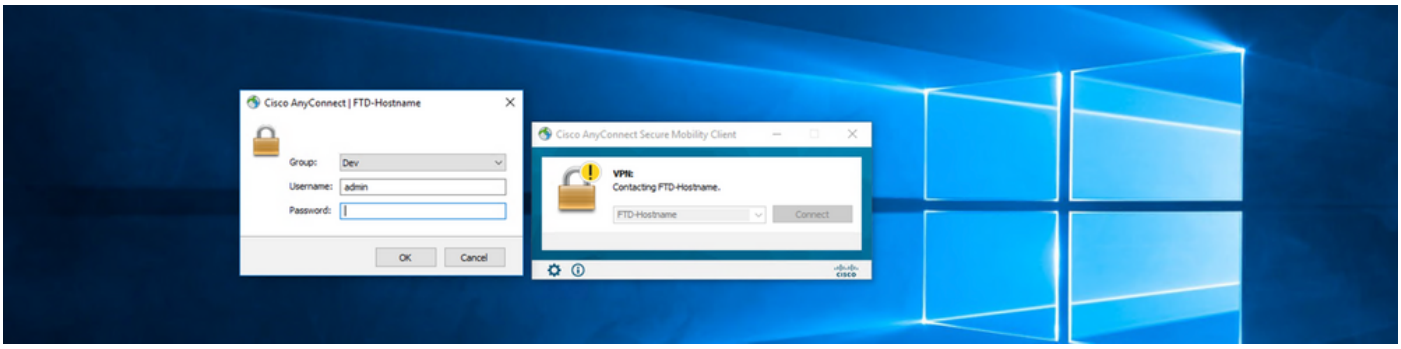
```
 default-domain none
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private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

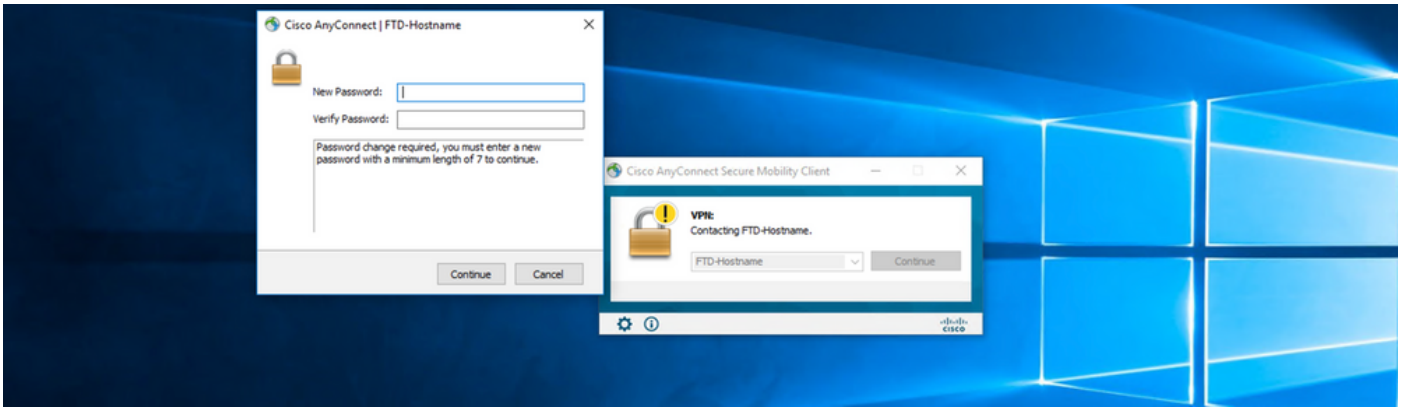
```
> show running-config ssl

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

検証

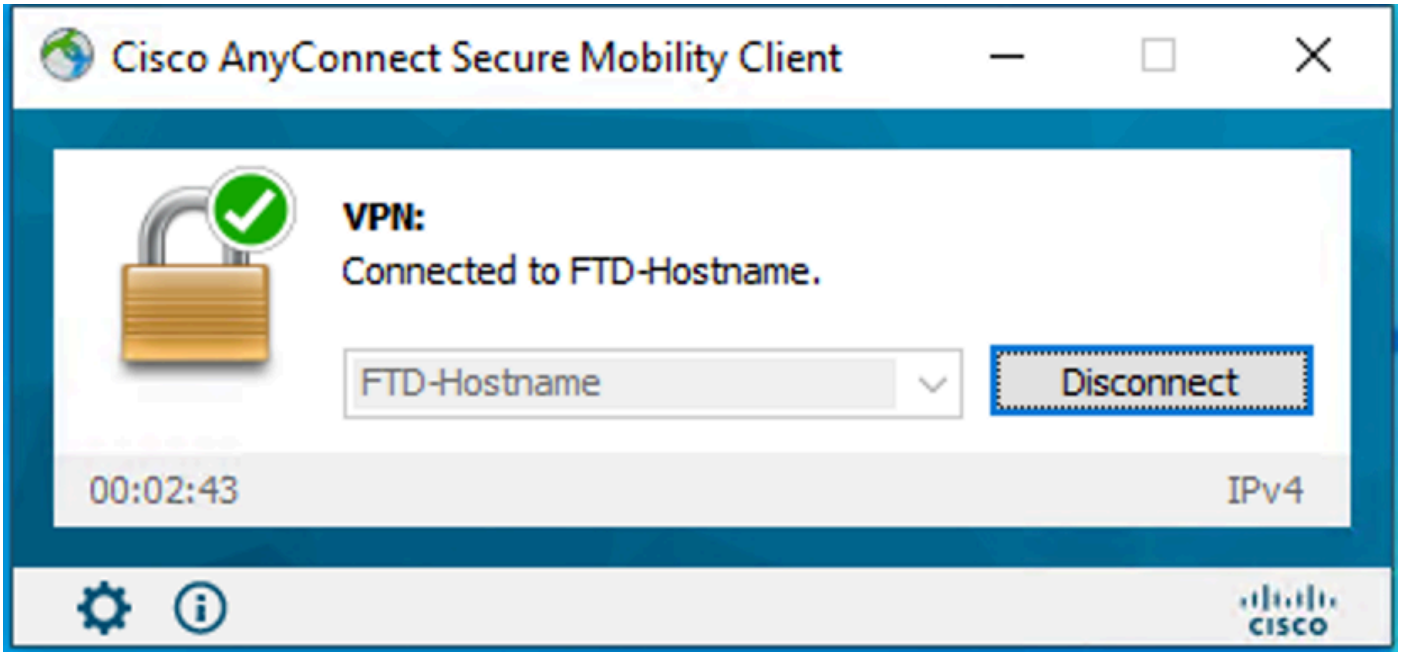
AnyConnectに接続し、ユーザ接続のパスワード管理プロセスを確認する

1.関連する接続プロファイルへの接続を開始します。初期ログイン時に、パスワードの有効期限が切れていたため以前のパスワードがMicrosoft Serverによって拒否されたため、パスワードを変更する必要があると判断されると、パスワードの変更を求めるメッセージがユーザーに表示されます。





2. ユーザがログイン用の新しいパスワードを入力すると、接続が正常に確立されます。



3. FTD CLIでユーザ接続を確認します。

<#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

トラブルシュート

デバッグ

このデバッグは、パスワード管理に関連する問題をトラブルシューティングするために、診断CLI(debug ldap 255)で実行できます。

パスワード管理のデバッグの実行

<#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

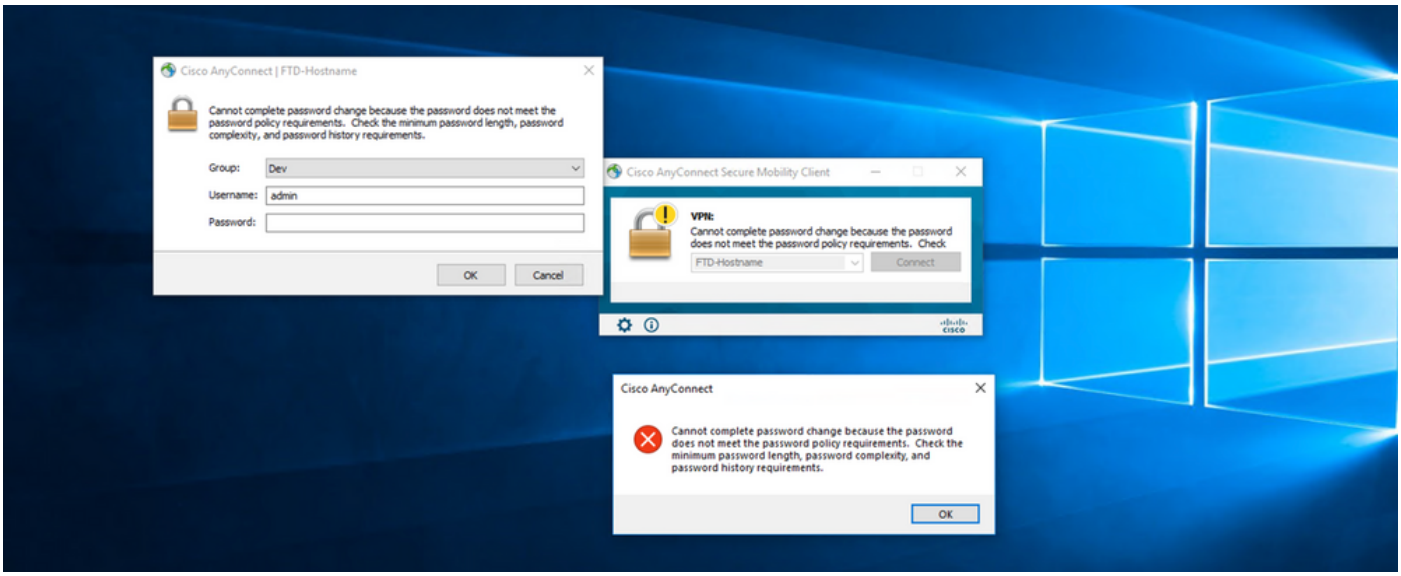
[25] badPasswordTime: value = 132610388348662803

[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
```

パスワード管理中に発生する一般的なエラー

通常、ユーザーが新しいパスワードを入力する間にMicrosoft Serverによって設定されたパスワードポリシーが満たされない場合、接続は終了し、「パスワードがパスワードポリシーの要件を満たしていません」というエラーが表示されます。したがって、新しいパスワードがMicrosoft Serverで設定されているLDAPのポリシーを満たしていることを確認します。


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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。