Configurare la gestione delle password utilizzando LDAP per RA VPN su FTD Gestito da FMC

Sommario

Introduzione

In questo documento viene descritto come configurare la gestione delle password con gli elenchi LDAP per i client AnyConnect che si connettono a Cisco Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Conoscenze base della configurazione di RMA VPN (Remote Access Virtual Private Network) su FMC
- Conoscenze base della configurazione del server LDAP in FMC
- Conoscenze base di Active Directory

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Server Microsoft 2012 R2
- FMCv con versione 7.3.0
- FTDv in esecuzione 7.3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete e scenario

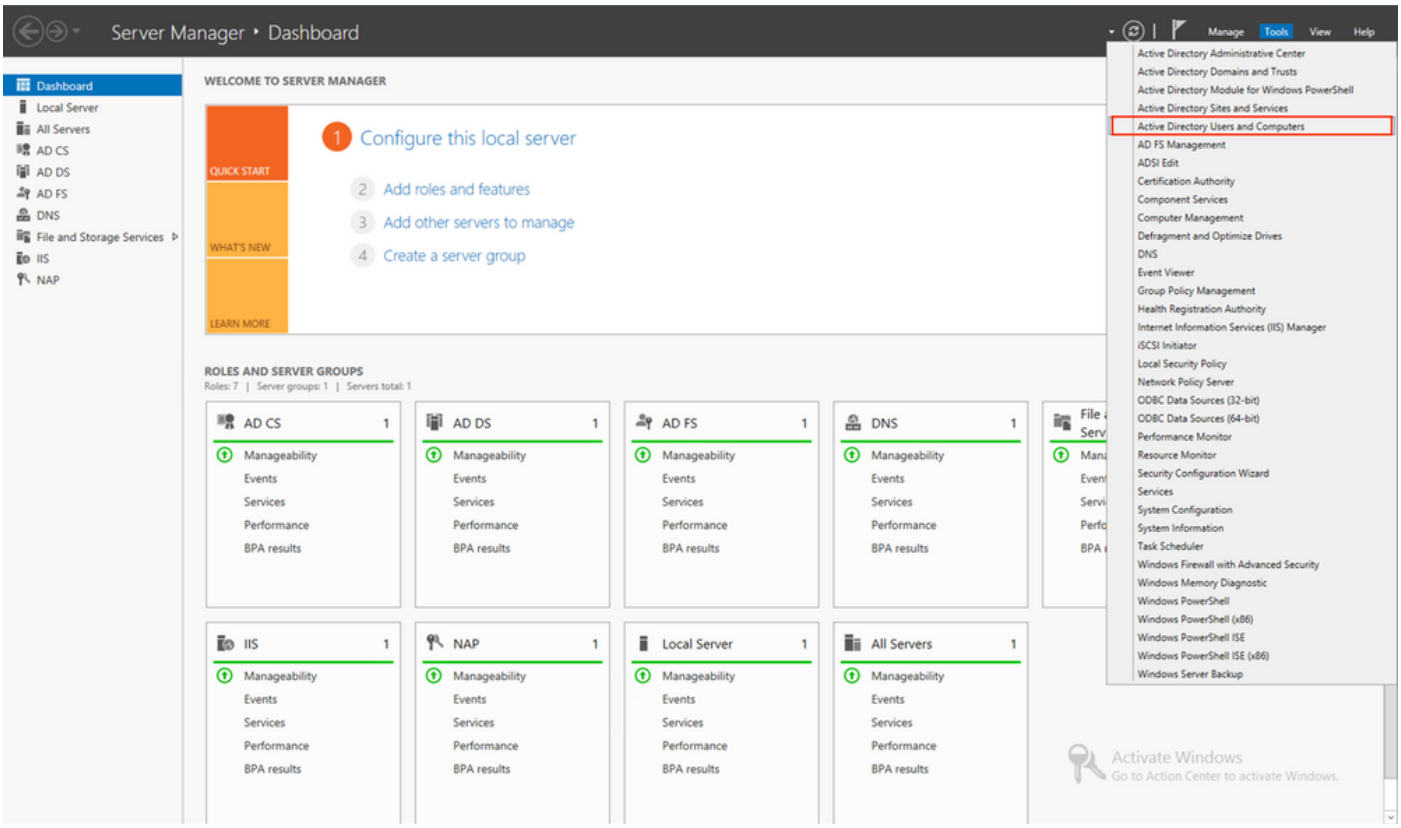
Il server Windows è preconfigurato con ADDS e ADCS per verificare il processo di gestione delle password degli utenti. In questa guida alla configurazione, vengono creati questi account utente.

Account utente:

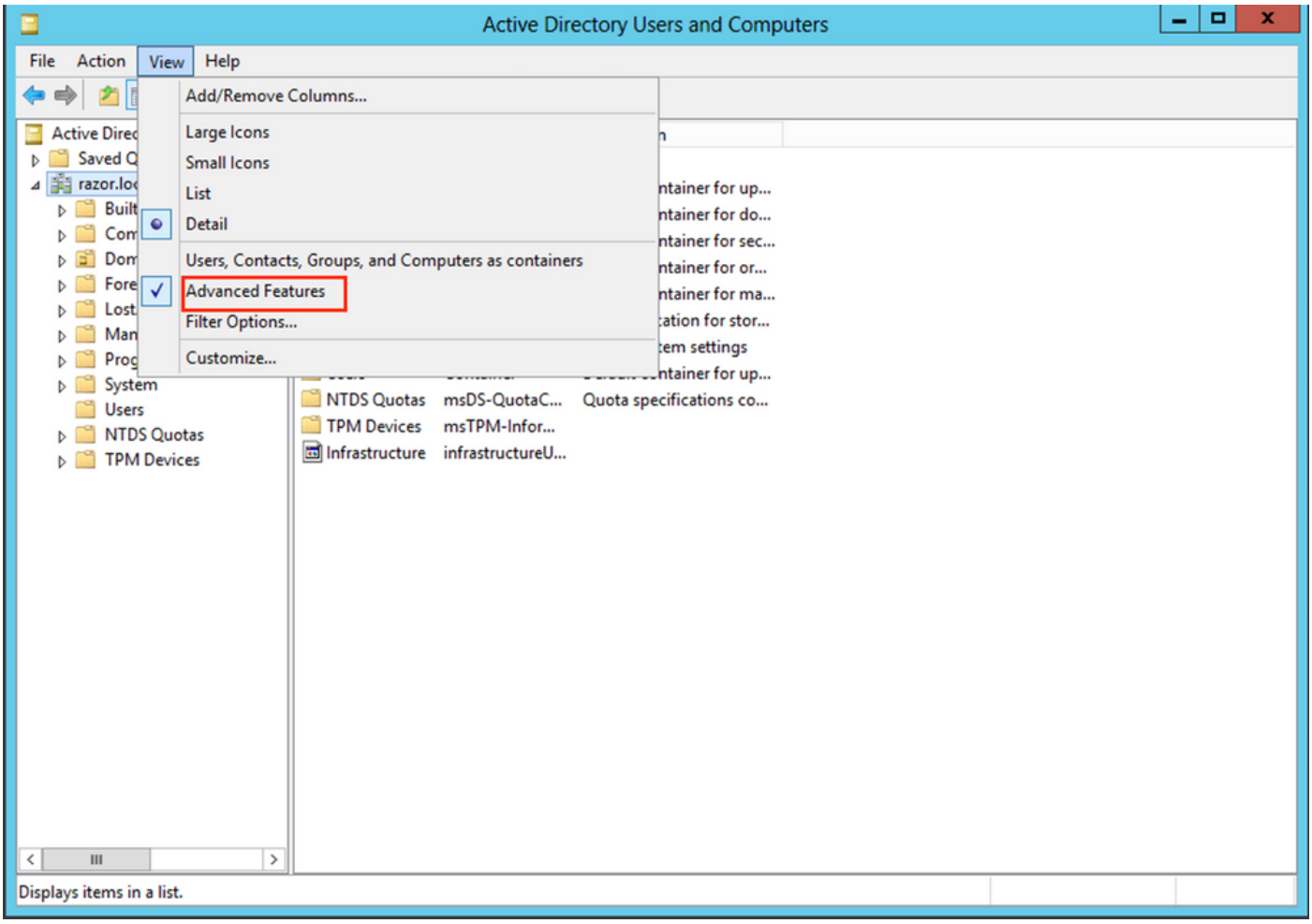
- Amministratore: viene utilizzato come account di directory per consentire l'associazione di FTD al server Active Directory.
- admin: account di amministratore di test utilizzato per dimostrare l'identità dell'utente.

Determinare il DN di base e il DN gruppo LDAP

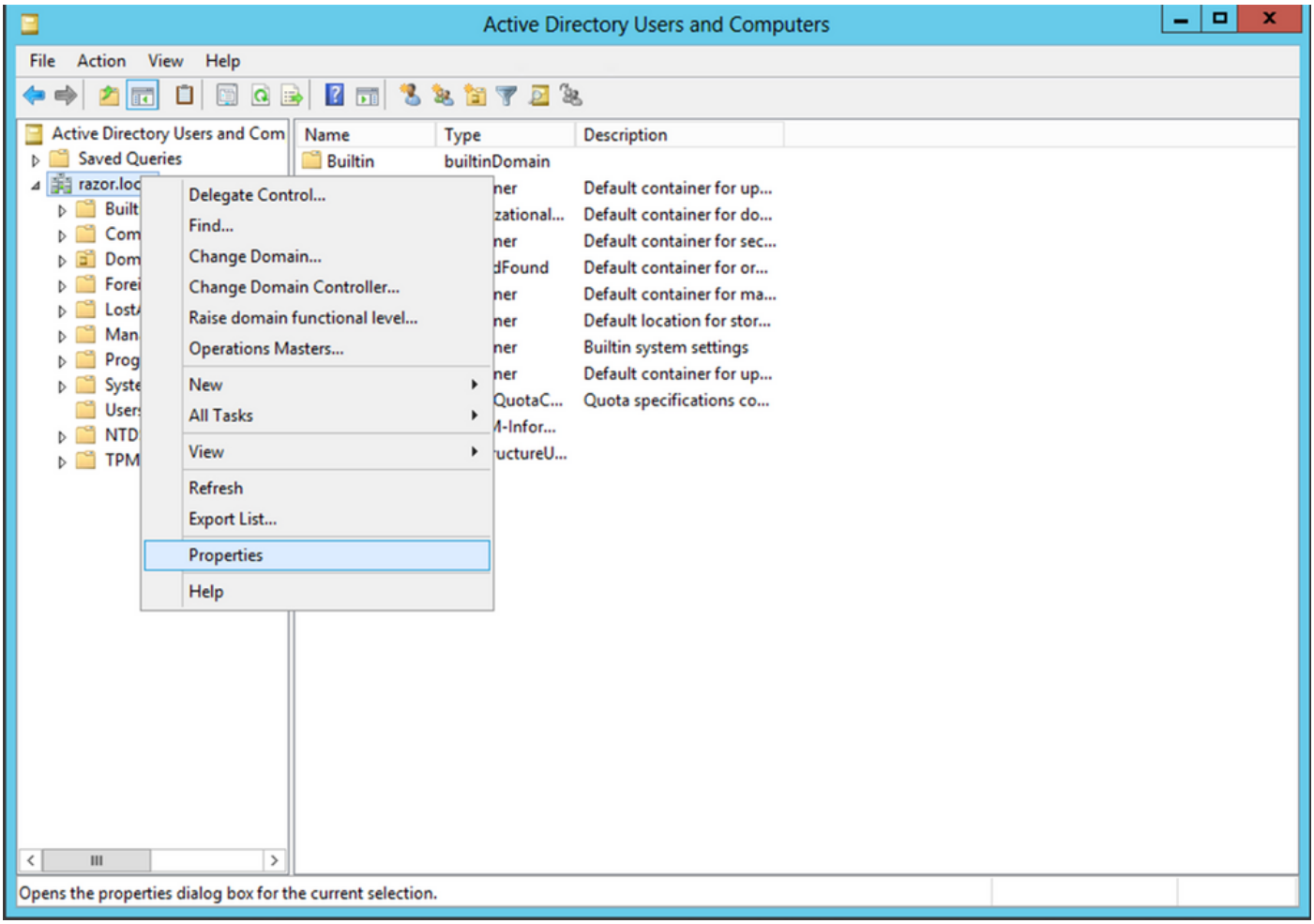
1. Open (Aperto) Active Directory Users and Computers tramite il dashboard di Server Manager.



2. Aprire il View Option nel pannello superiore e attivare Advanced Features, come mostrato nell'immagine:



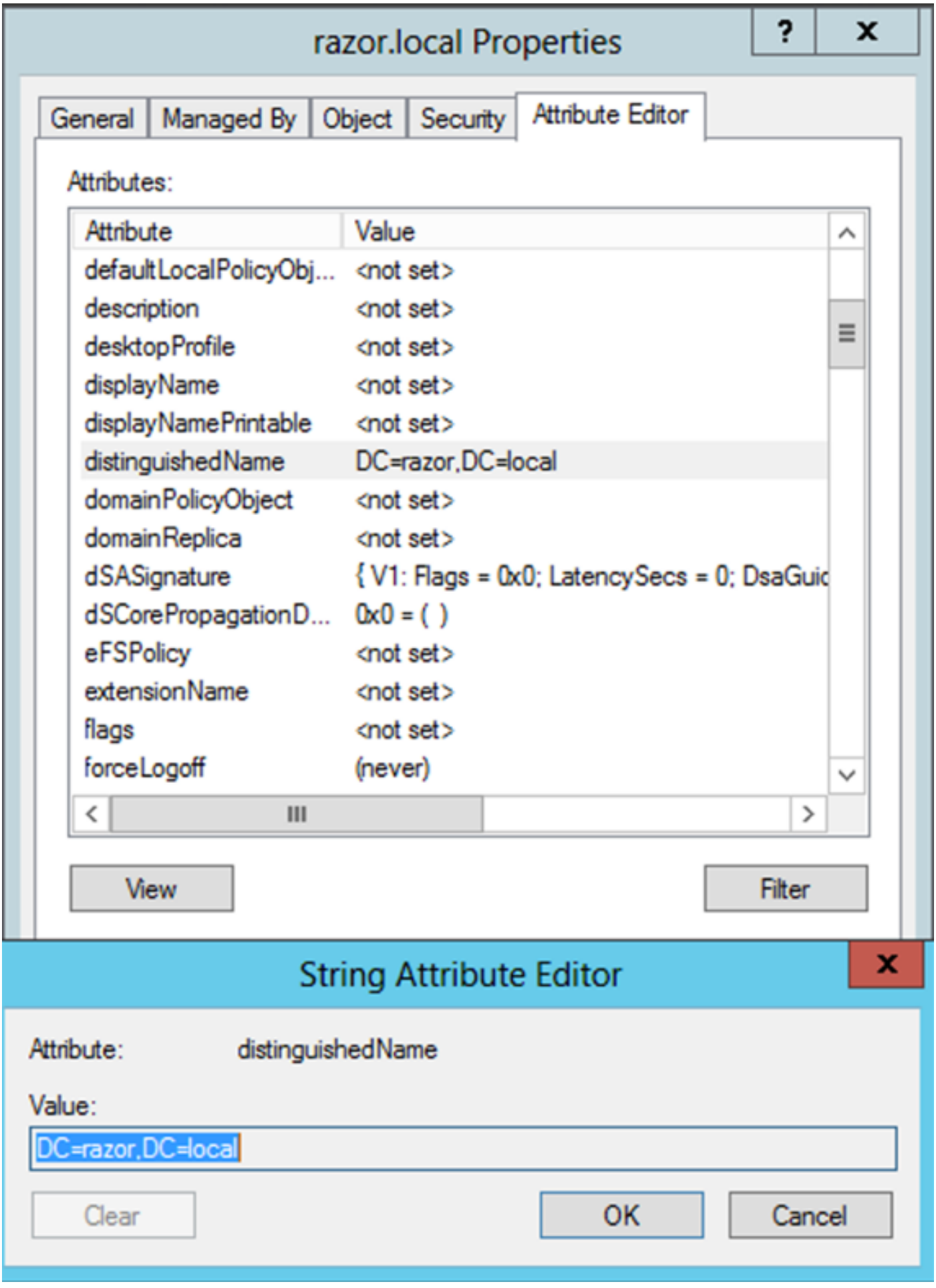
3. In questo modo è possibile visualizzare proprietà aggiuntive negli oggetti AD.
   Ad esempio, per trovare il DN per la radice razor.local, fare clic con il pulsante destro del mouse razor.localе quindi scegliere Properties, come mostrato nell'immagine:



4. Inferiore Properties, scegliere il Attribute Editor scheda. Cerca distinguishedName in Attributi (Attributes), fate clic su View, come illustrato nell'immagine.

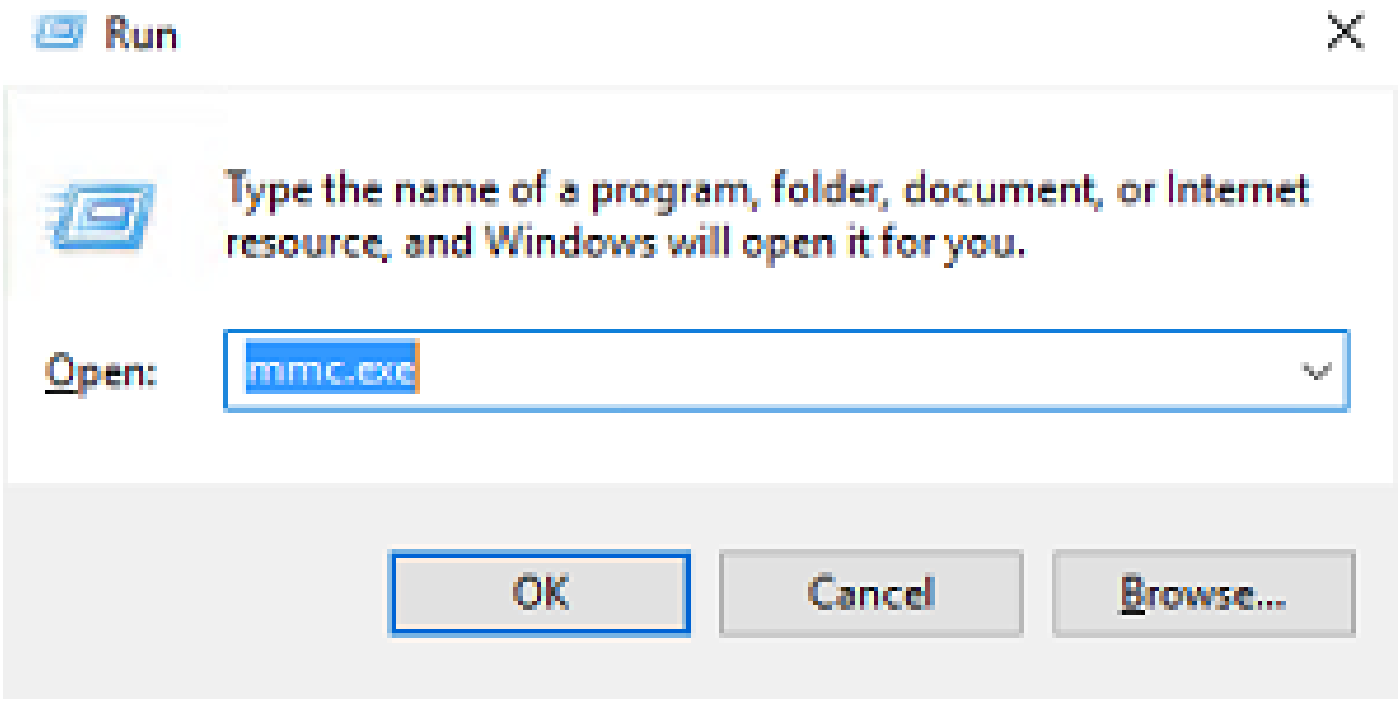
Verrà visualizzata una nuova finestra in cui il DN può essere copiato e incollato in FMC in un secondo momento.

In questo esempio, il DN radice è DC=razor, DC=local. Copiare il valore e salvarlo per utilizzarlo in seguito. Fare clic su OK per uscire dalla finestra Editor attributi stringa e fare clic su OK per uscire dalla finestra di dialogo Proprietà.

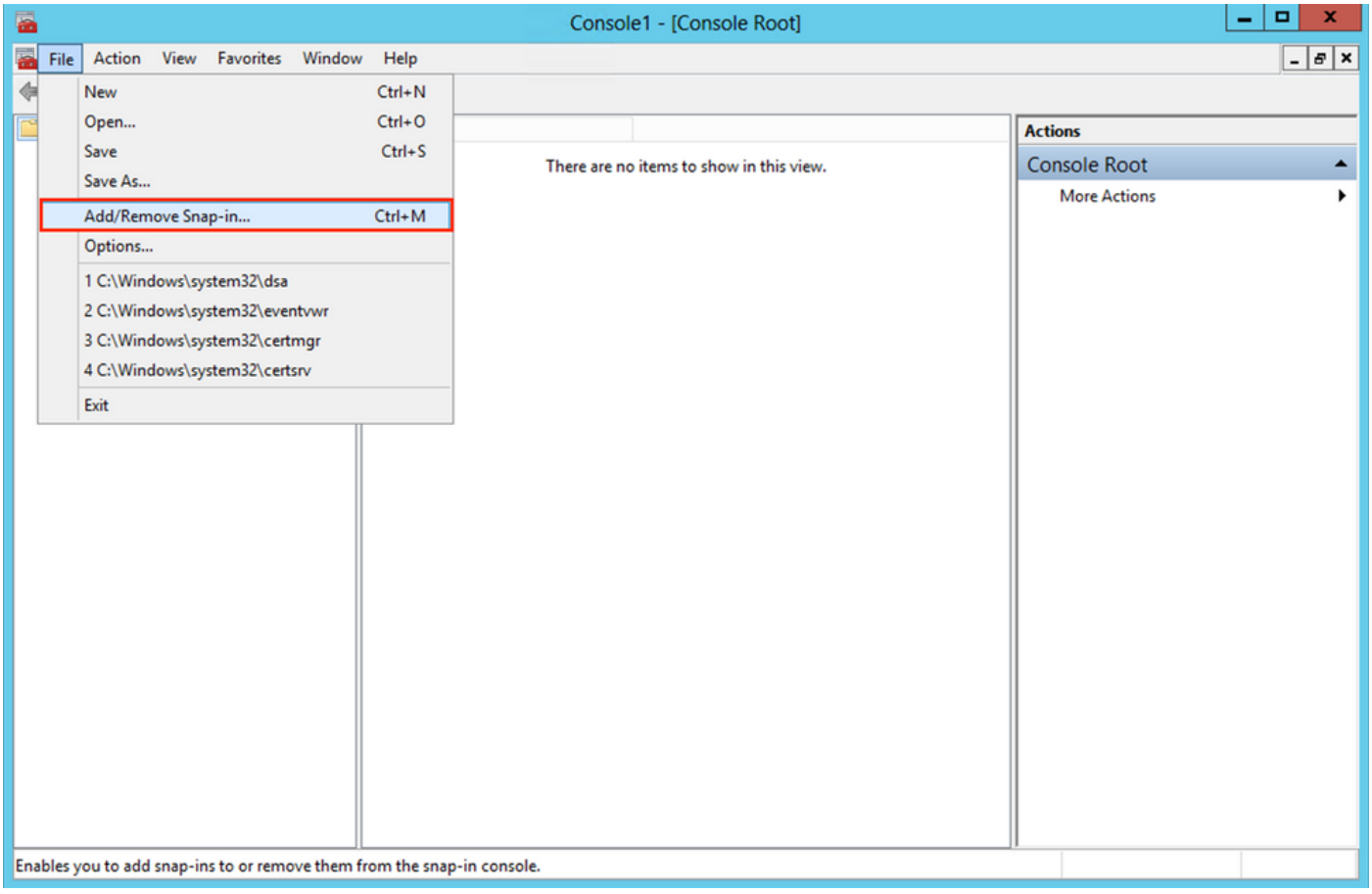

razor.local Properties
General
Managed By
Object
Security
Attribute Editor
Attributes:
Attribute
Value
defaultLocalPolicyObj...
<not set>
description
<not set>
desktopProfile
<not set>
displayName
<not set>
displayNamePrintable
<not set>
distinguishedName
DC=razor,DC=local
domainPolicyObject
<not set>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

Copia radice certificato SSL LDAPS

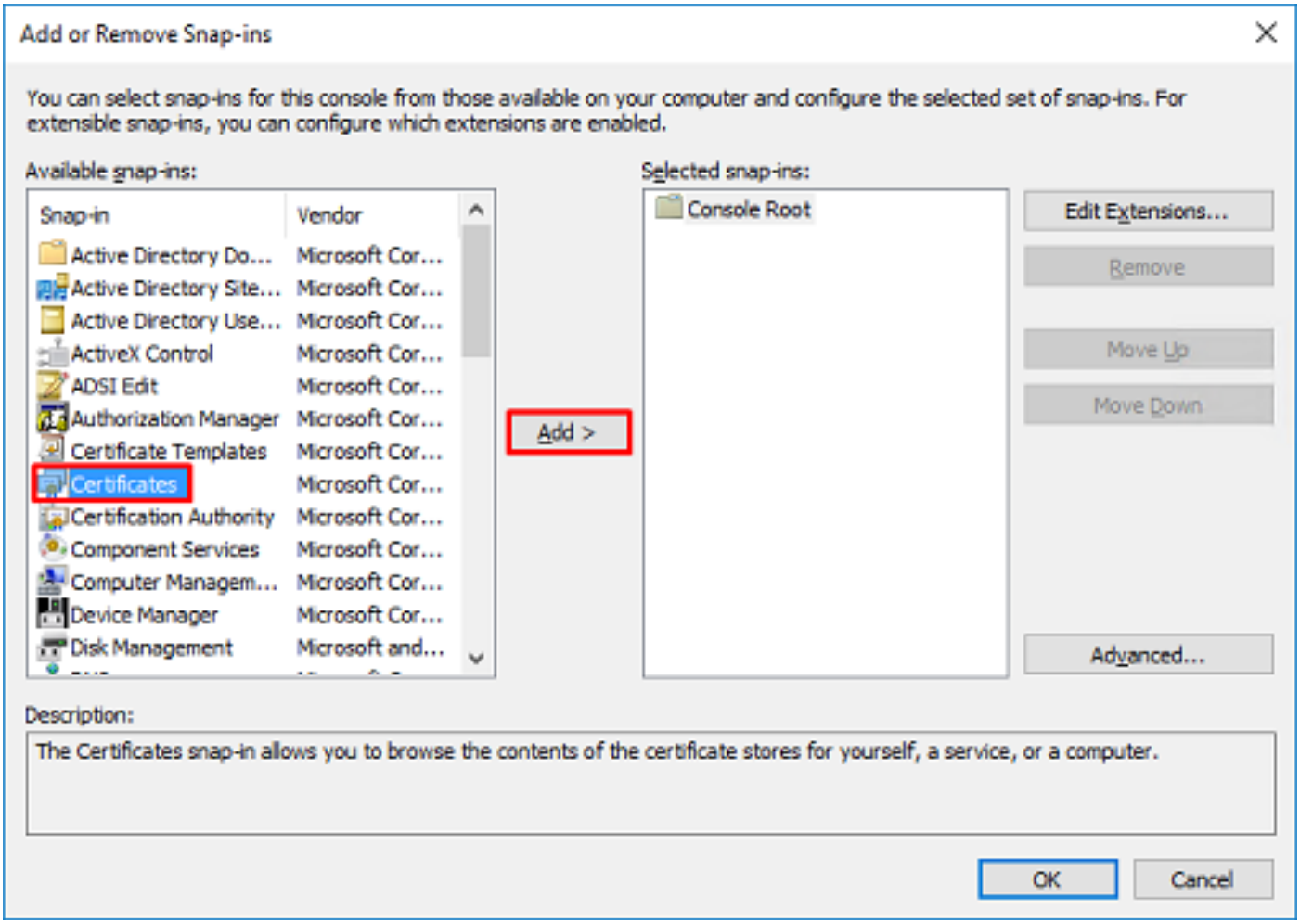
1. Premere Win+R e immettere mmc.exe, quindi scegliere OK, come mostrato nell'immagine.



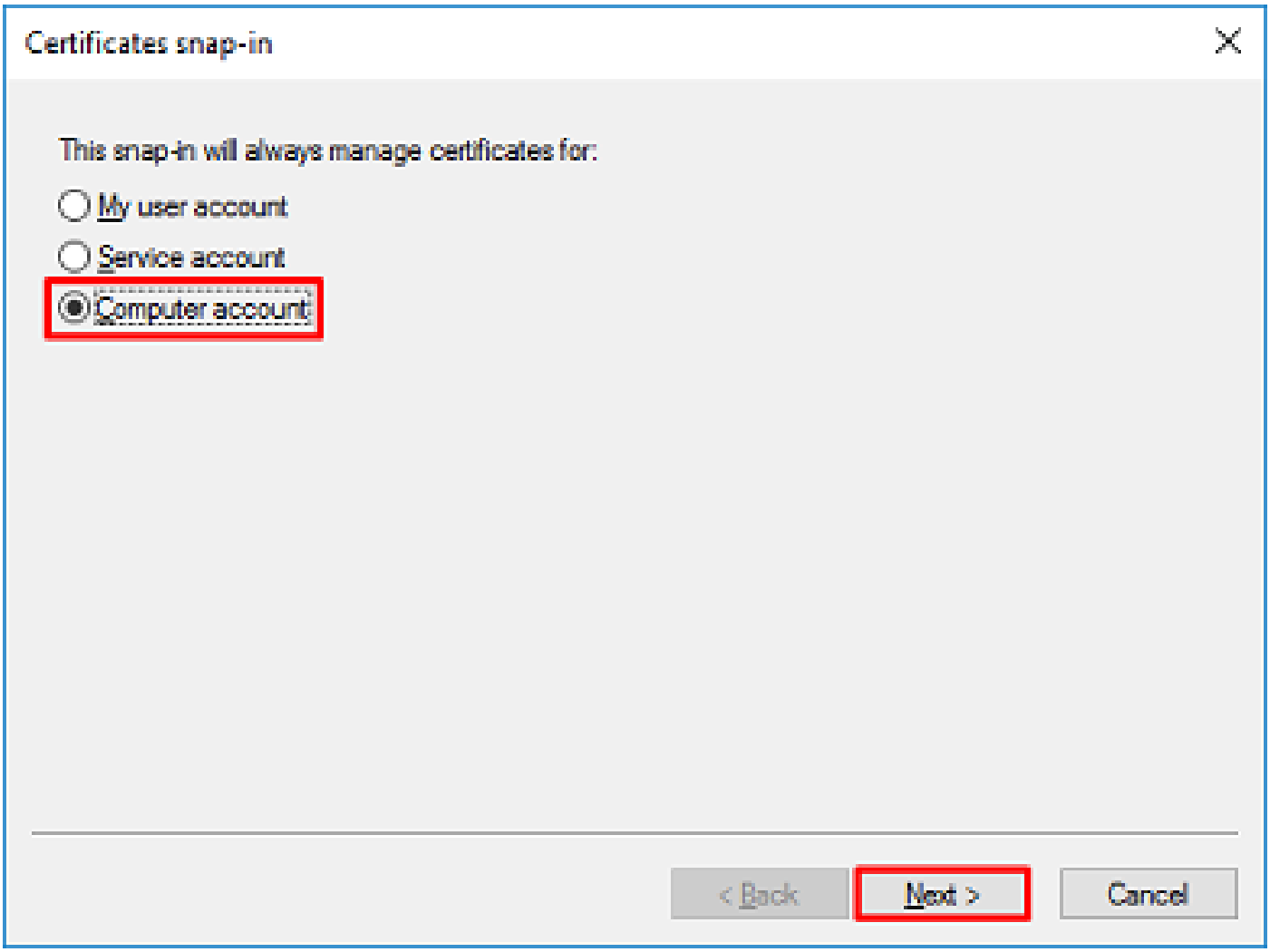
2. Passa a File > Add/Remove Snap-in..., come mostrato nell'immagine:



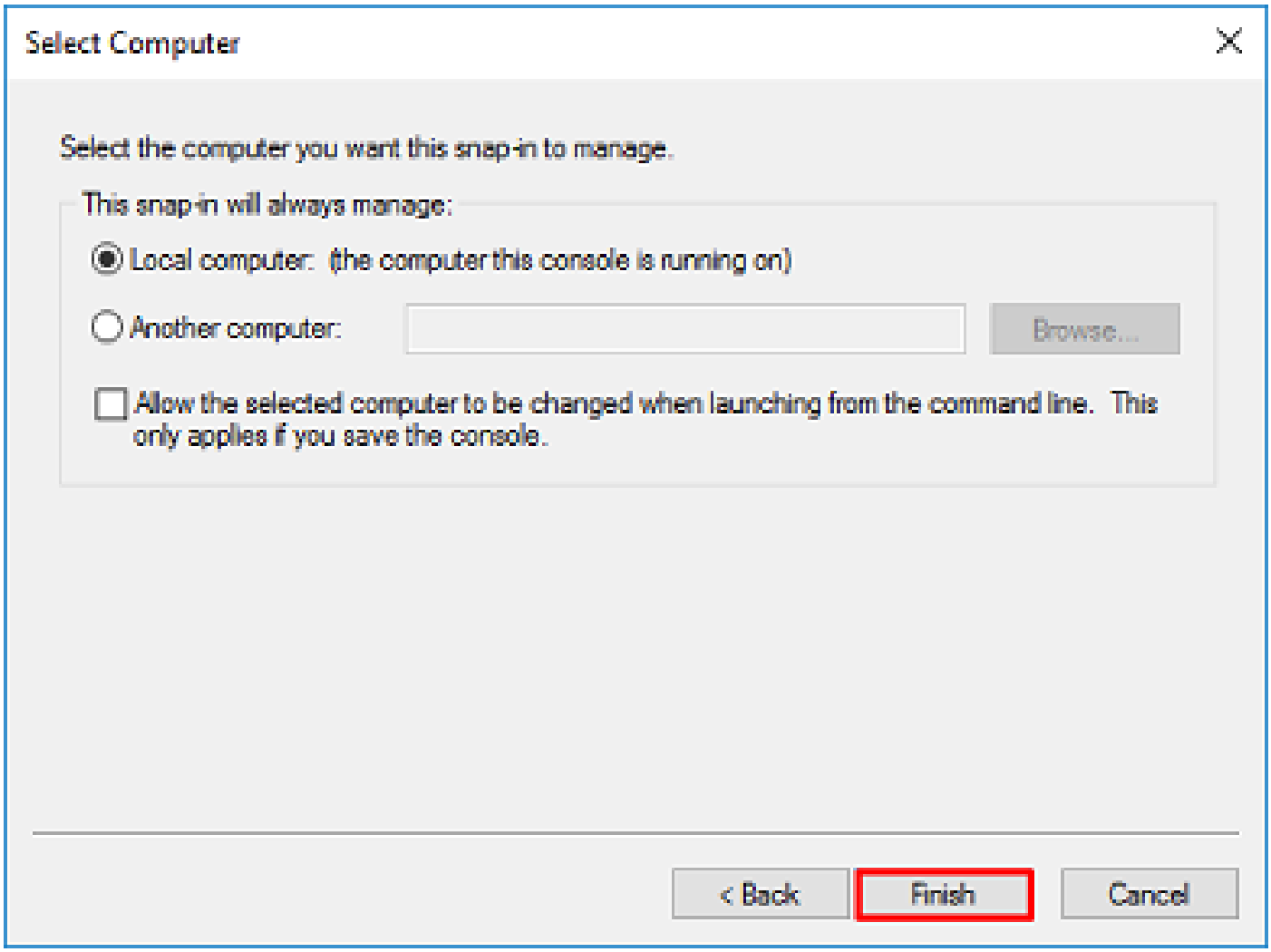
3. In snap-in disponibili scegliere Certificates e quindi fare clic su Add, come mostrato nell'immagine:



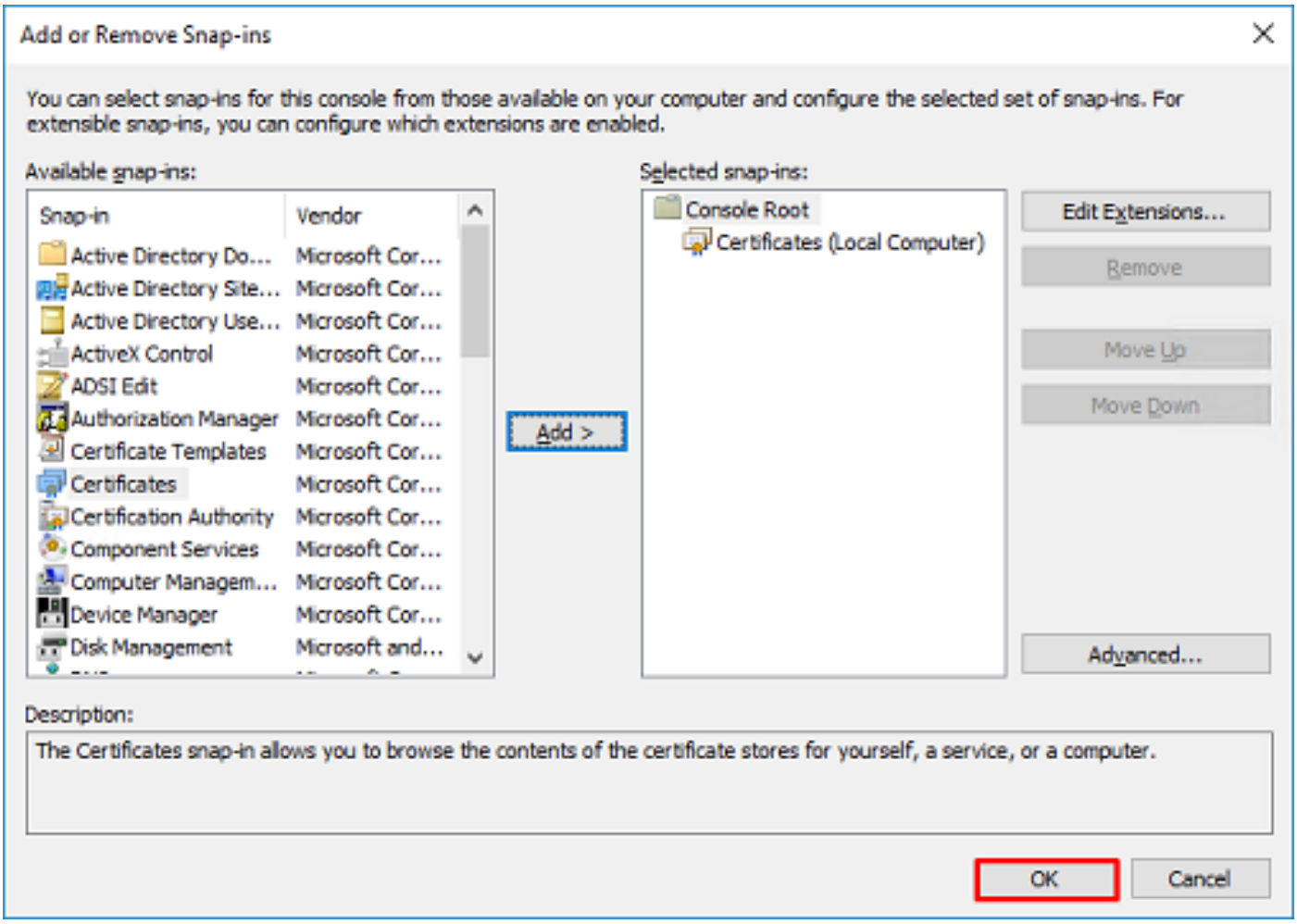
4. Scegli Computer account e quindi fare clic su Next, come mostrato nell'immagine:



Come mostrato di seguito, fare clic su Finish.



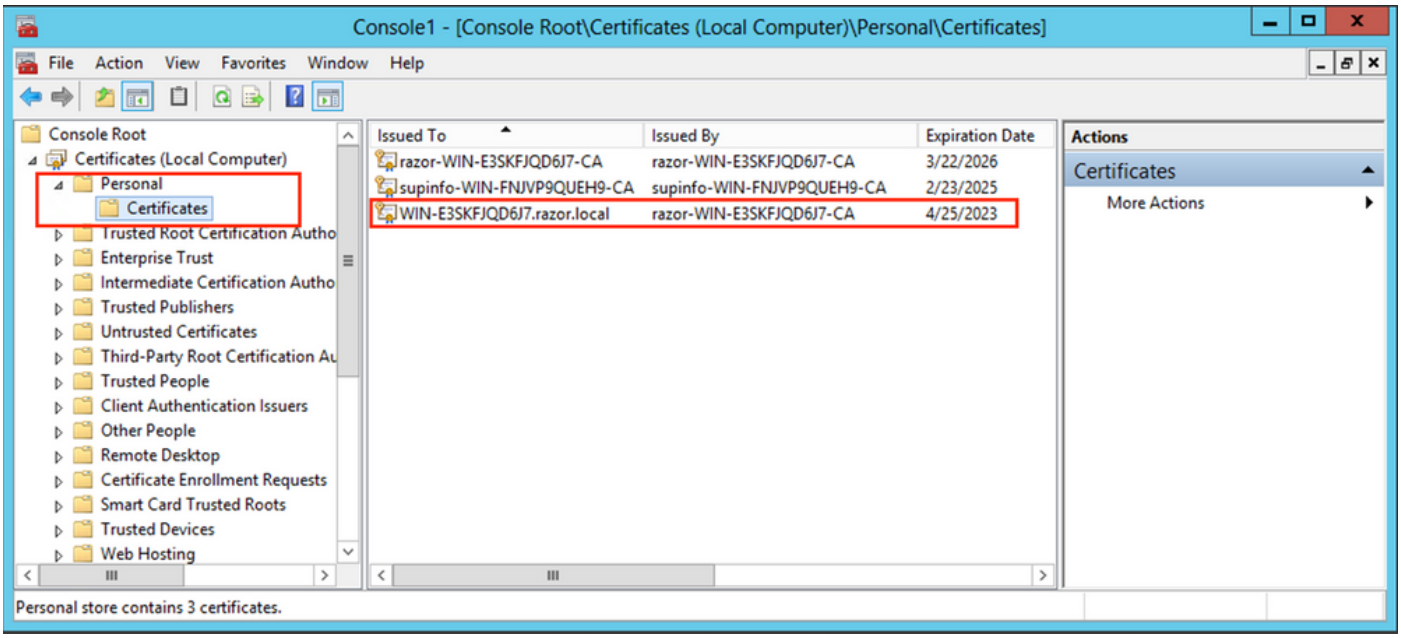
5. Fare clic su OK, come mostrato nell'immagine.



6. Espandere la Personal , quindi fare clic su Certificates. Il certificato utilizzato da LDAP deve essere rilasciato al nome di dominio completo (FQDN) del server Windows. In questo server sono elencati tre certificati:

- Certificato CA rilasciato a e da razor-WIN-E3SKFJQD6J7-CA.
- Certificato CA rilasciato a e da supinfo-WIN-FNJVP9QUEH9-CA.
- Un certificato di identità è stato rilasciato a WIN-E3SKFJQD6J7.razor.local da razor-WIN-E3SKFJQD6J7-CA.

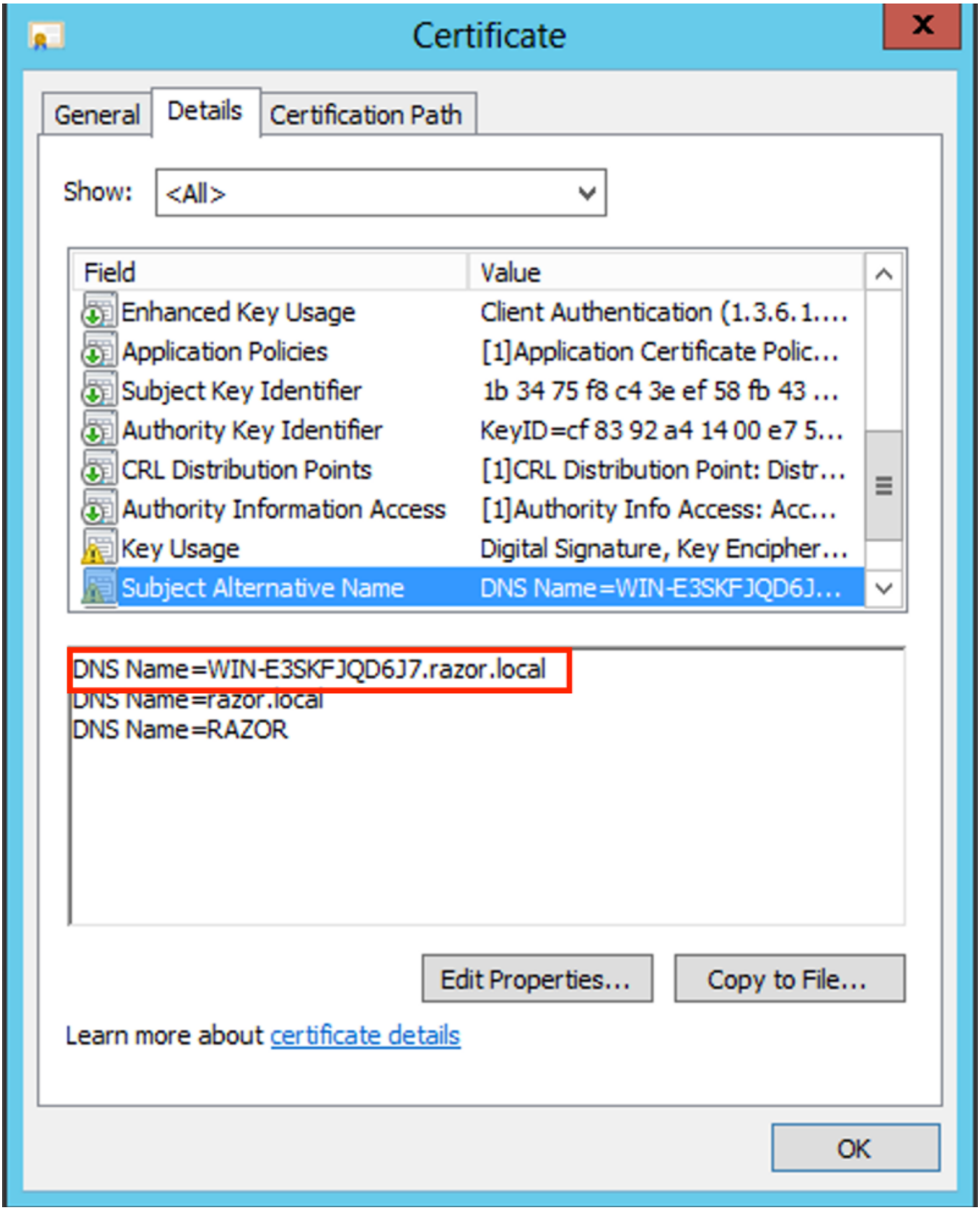
In questa guida alla configurazione, il nome di dominio completo è WIN-E3SKFJQD6J7.razor.local i primi due certificati non sono pertanto validi per l'utilizzo come certificato SSL LDAP. Il certificato di identità rilasciato a WIN-E3SKFJQD6J7.razor.local è un certificato rilasciato automaticamente dal servizio CA di Windows Server. Fare doppio clic sul certificato per controllare i dettagli.



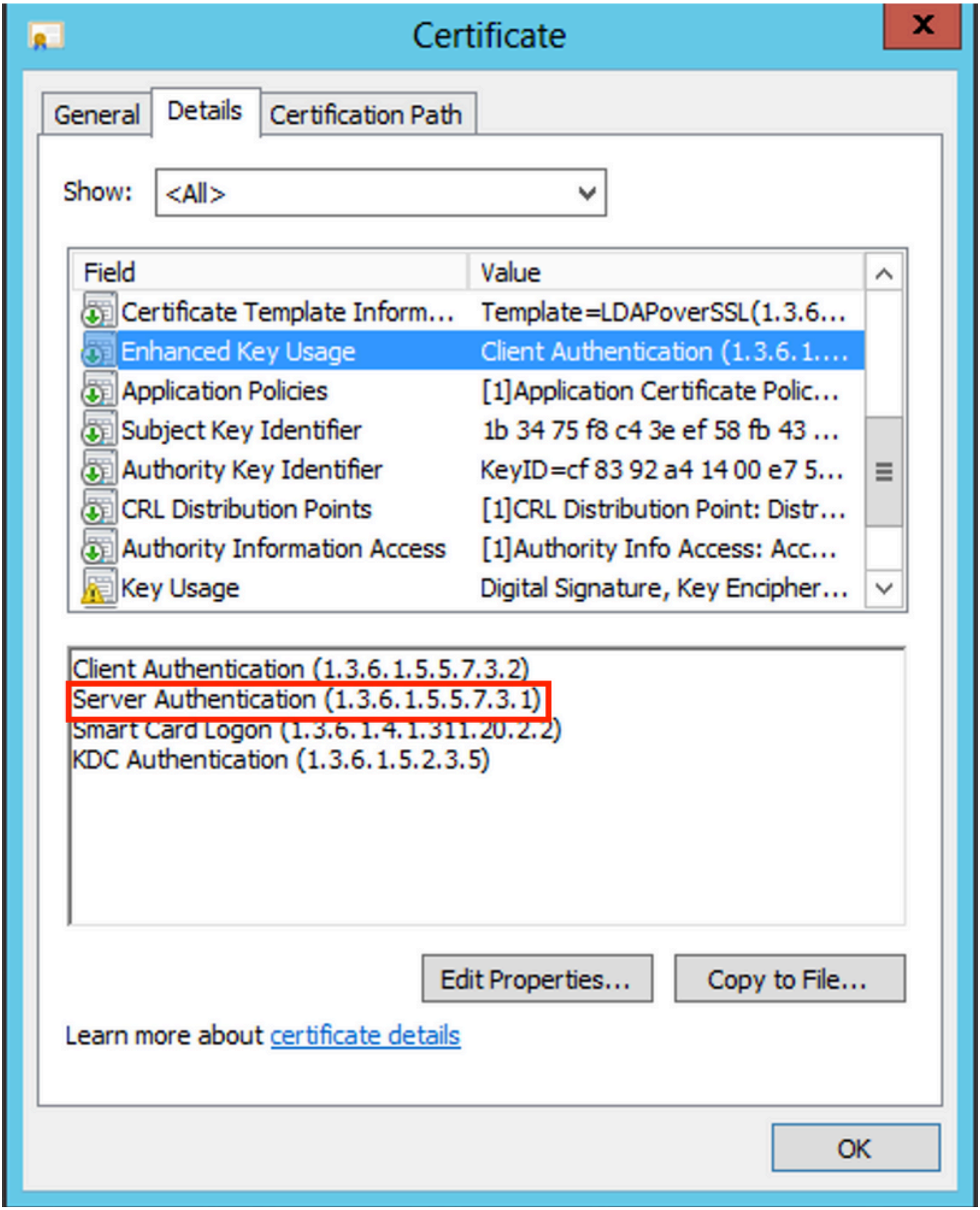
7. Per essere utilizzato come certificato SSL LDAP, il certificato deve soddisfare i seguenti requisiti:

- Il nome comune o il nome alternativo del soggetto DNS corrisponde al nome di dominio completo (FQDN) di Windows Server.
- Nel campo Utilizzo chiavi avanzato del certificato è impostata l'autenticazione server.

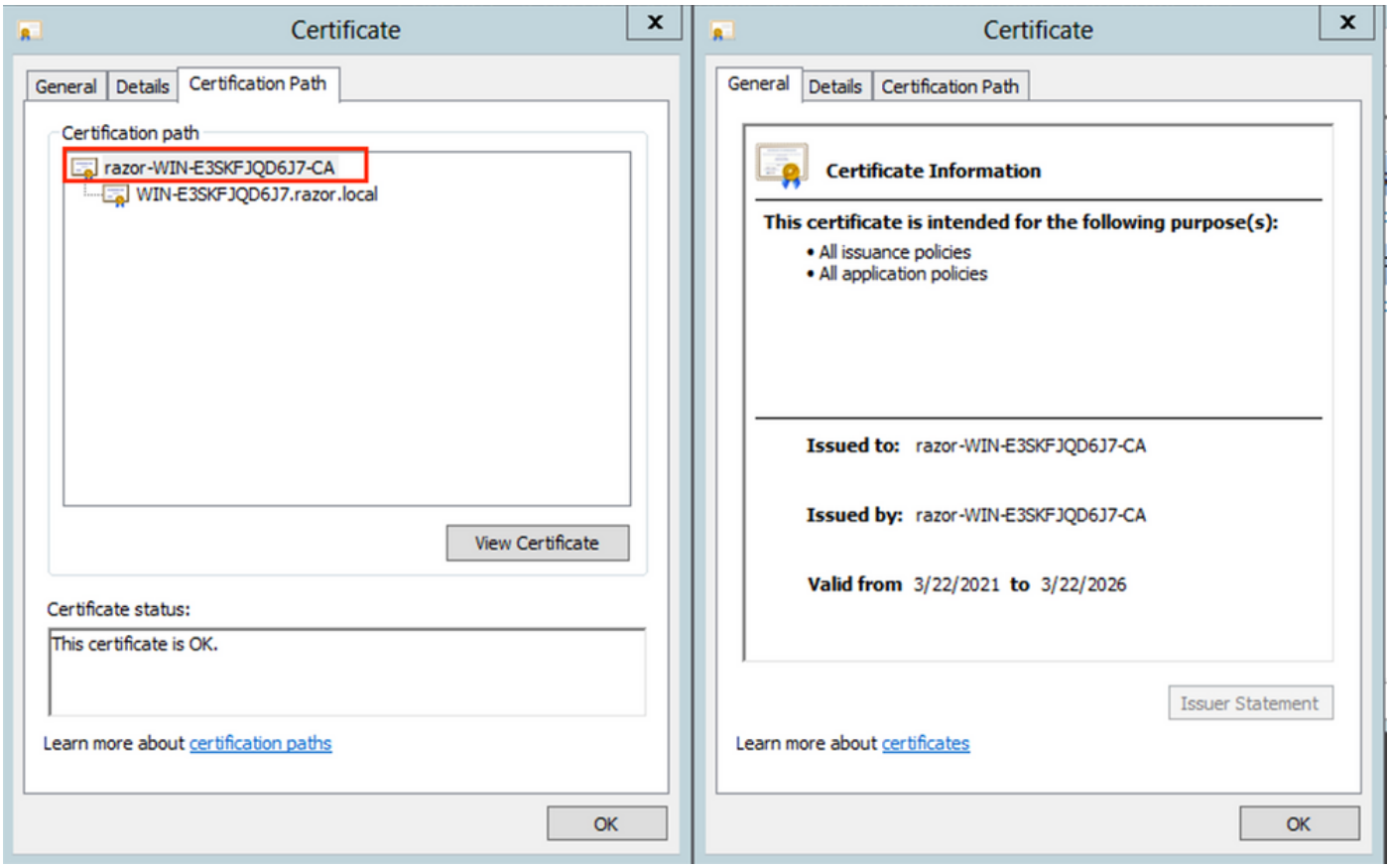
Nell'ambito Details per il certificato, scegliere Subject Alternative Name, dove FQDN WIN-E3SKFJQD6J7.razor.local presente.



Inferiore Enhanced Key Usage, Server Authentication presente.

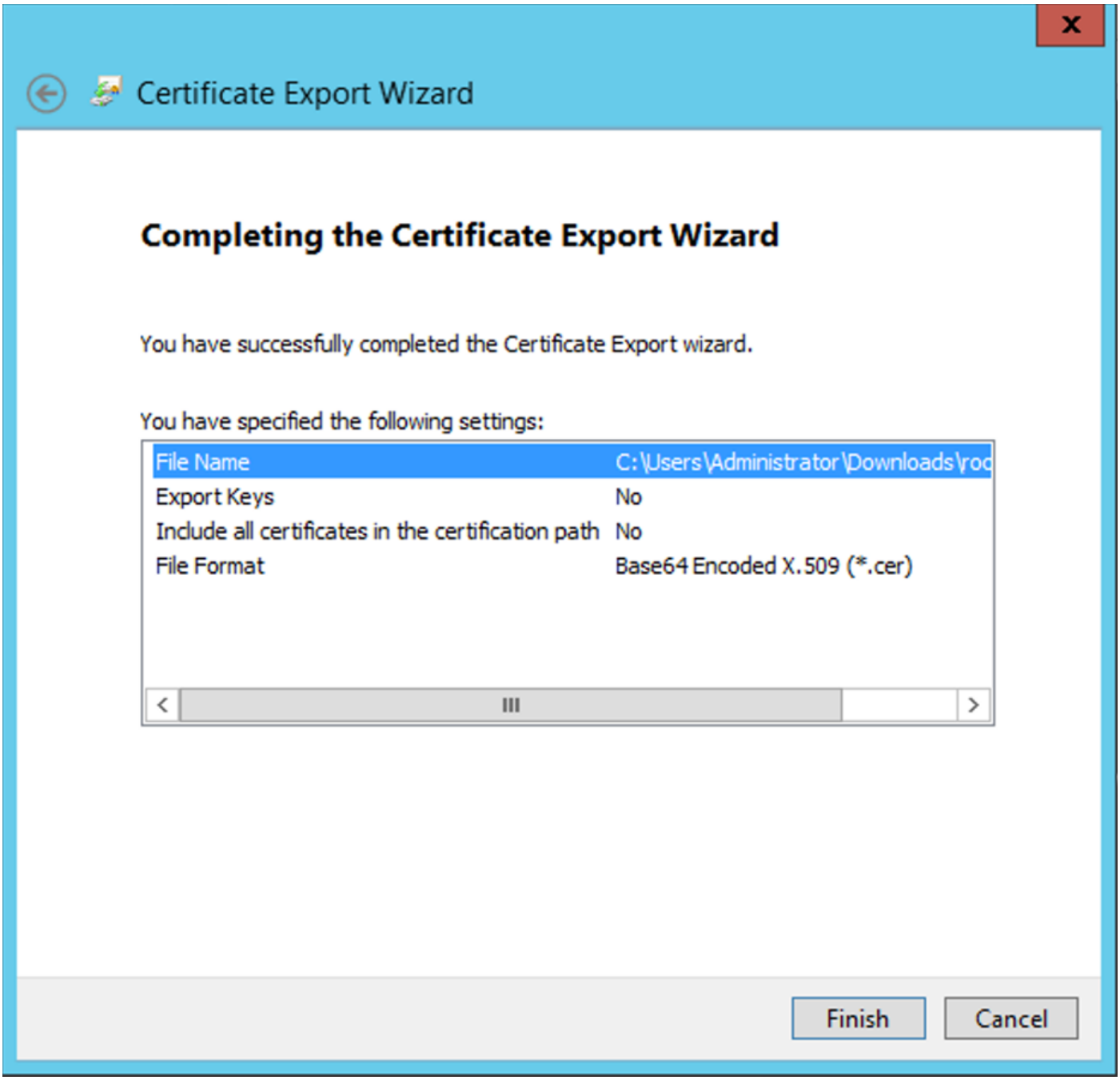


8. Una volta confermata, ai sensi dell'articolo Certification Path , scegliere il certificato di primo livello che corrisponde al certificato CA radice e quindi fare clic su View Certificate. Verranno aperti i dettagli del certificato della CA radice, come illustrato nell'immagine:



9. Nell'ambito Details del certificato CA radice, fare clic su Copy to File e navigare attraversoCertificate Export Wizard che esporta la CA radice in formato PEM.

Scegli Base-64 encoded X.509 come formato di file.



10. Aprire il certificato CA radice archiviato nel percorso selezionato nel computer con un blocco note o un altro editor di testo.

Mostra il certificato del formato PEM. Salva per uso futuro.

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

In caso di più certificati installati nell'archivio del computer locale sul server LDAP (facoltativo)

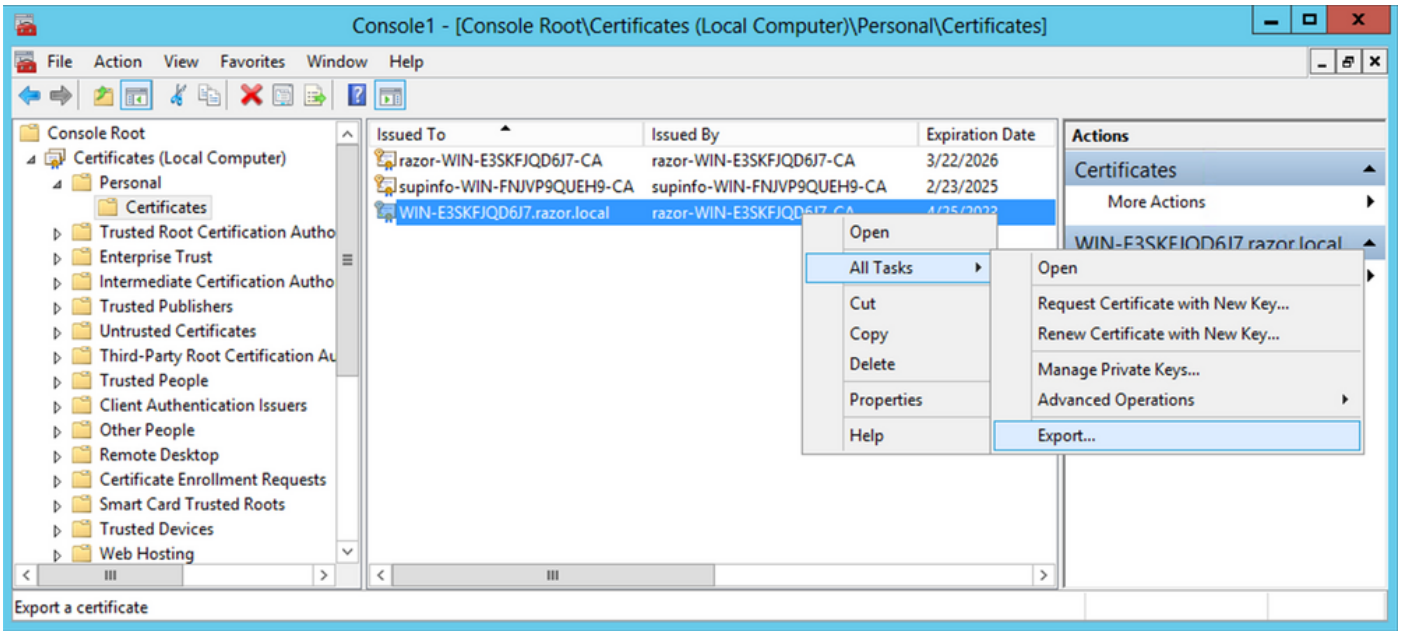
1. In una situazione di più certificati di identità utilizzabili da LDAPS e in caso di incertezza sul tipo di certificato utilizzato o in assenza di accesso al server LDAPS, è ancora possibile estrarre la CA radice da un'acquisizione di pacchetti effettuata sul FTD.

2. Se si dispone di più certificati validi per l'autenticazione server nell'archivio certificati del computer locale del server LDAP (ad esempio il controller di dominio di Servizi di dominio Active Directory), si noterà che per le comunicazioni LDAPS viene utilizzato un certificato diverso. La soluzione migliore per questo problema è rimuovere tutti i certificati non necessari dall'archivio certificati del computer locale e disporre di un solo certificato valido per l'autenticazione del server.

Se tuttavia esiste un motivo legittimo per cui sono necessari due o più certificati e si dispone almeno di un server LDAP di Windows Server 2008, è possibile utilizzare l'archivio certificati di Servizi di dominio Active Directory (NTDS\Personale) per le comunicazioni LDAP.

In questa procedura viene illustrato come esportare un certificato abilitato per LDAPS dall'archivio certificati di un computer locale del controller di dominio all'archivio certificati del servizio Servizi di dominio Active Directory (NTDS\Personale).

- Passare alla console MMC nel server Active Directory, scegliere File e quindi fare clic su Add/Remove Snap-in.
- Fare clic su Certificates e quindi fare clic su Add.
- Nella scheda Certificates snap-in, scegliere Computer account e quindi fare clic su Next.
- Dentro Select Computer, scegliere Local Computer,fare clic su OKe quindi fare clic su Finish. Dentro Add or Remove Snap-ins,fare clic su OK.
- Nella console dei certificati di un computer che contiene un certificato utilizzato per l'autenticazione del server, fare clic con il pulsante destro del mouse sulla scheda certificate,fare clic su All Taskse quindi fare clic su Export.



- Esporta il certificato in pfx nelle sezioni successive. Fare riferimento a questo articolo per informazioni su come esportare un certificato in pfx formato da MMC:

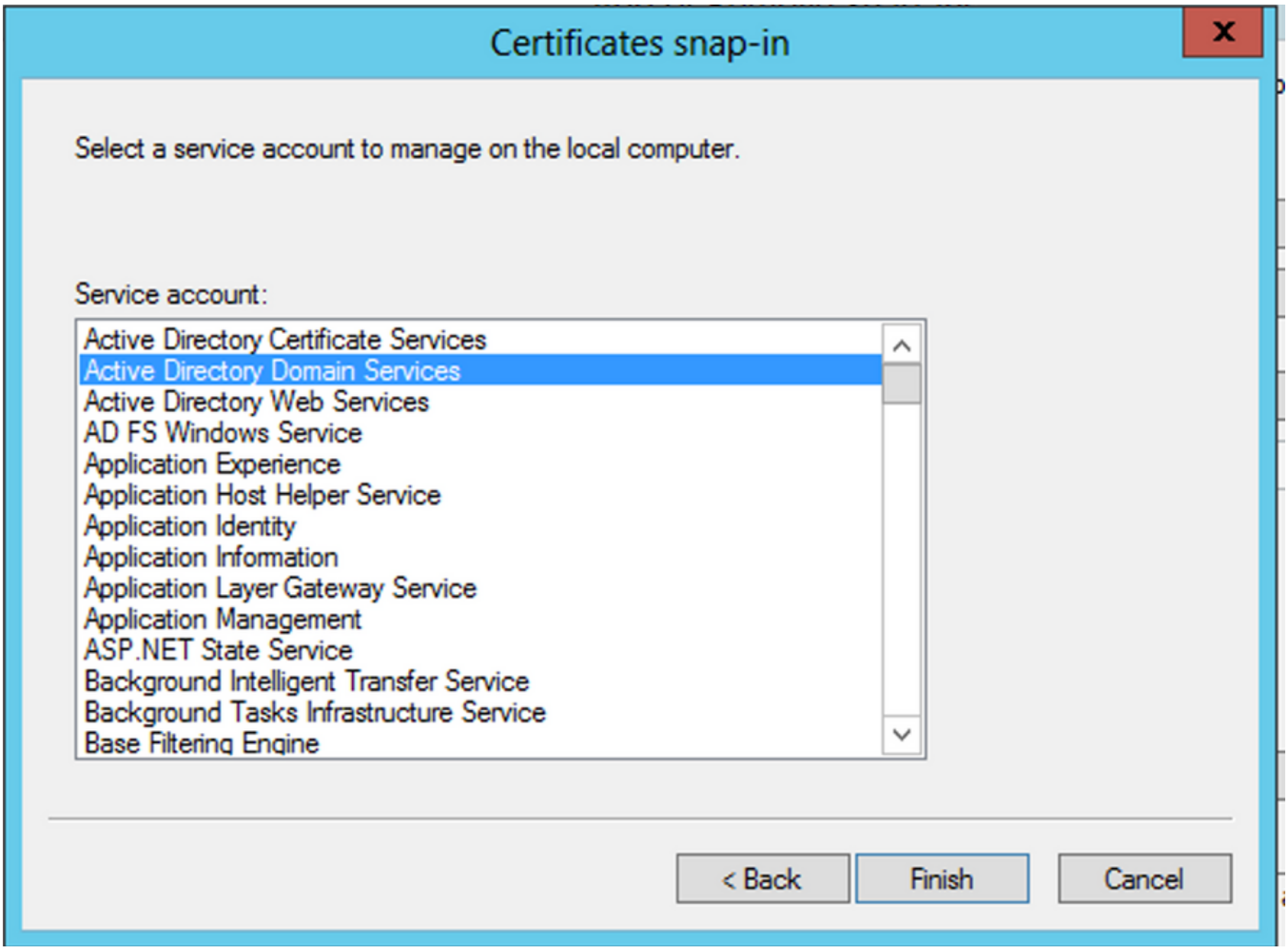
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html.

- Al termine dell'esportazione del certificato, passare a Add/Remove Snap-in on MMC console. Fare clic su Certificates e quindi fare clic su Add.

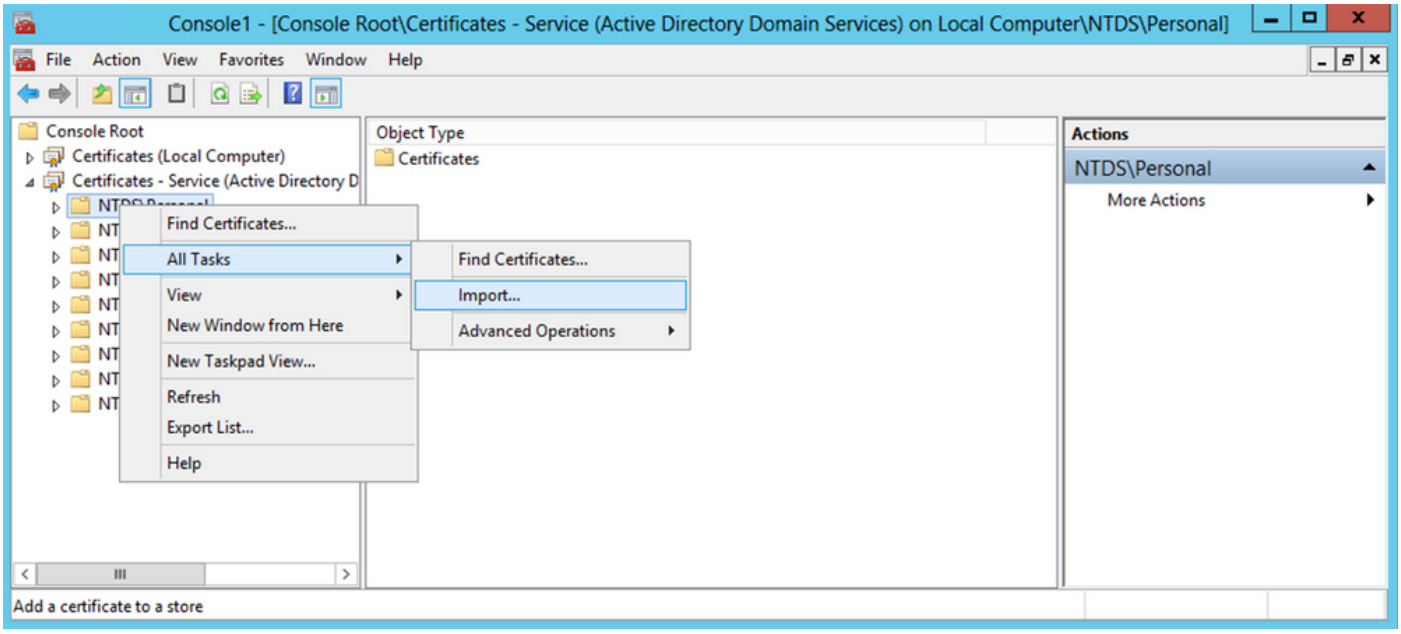
- Scegli Service account e quindi fare clic su Next.

- Nella scheda Select Computer , scegliere Local Computer e fare clic su Next.

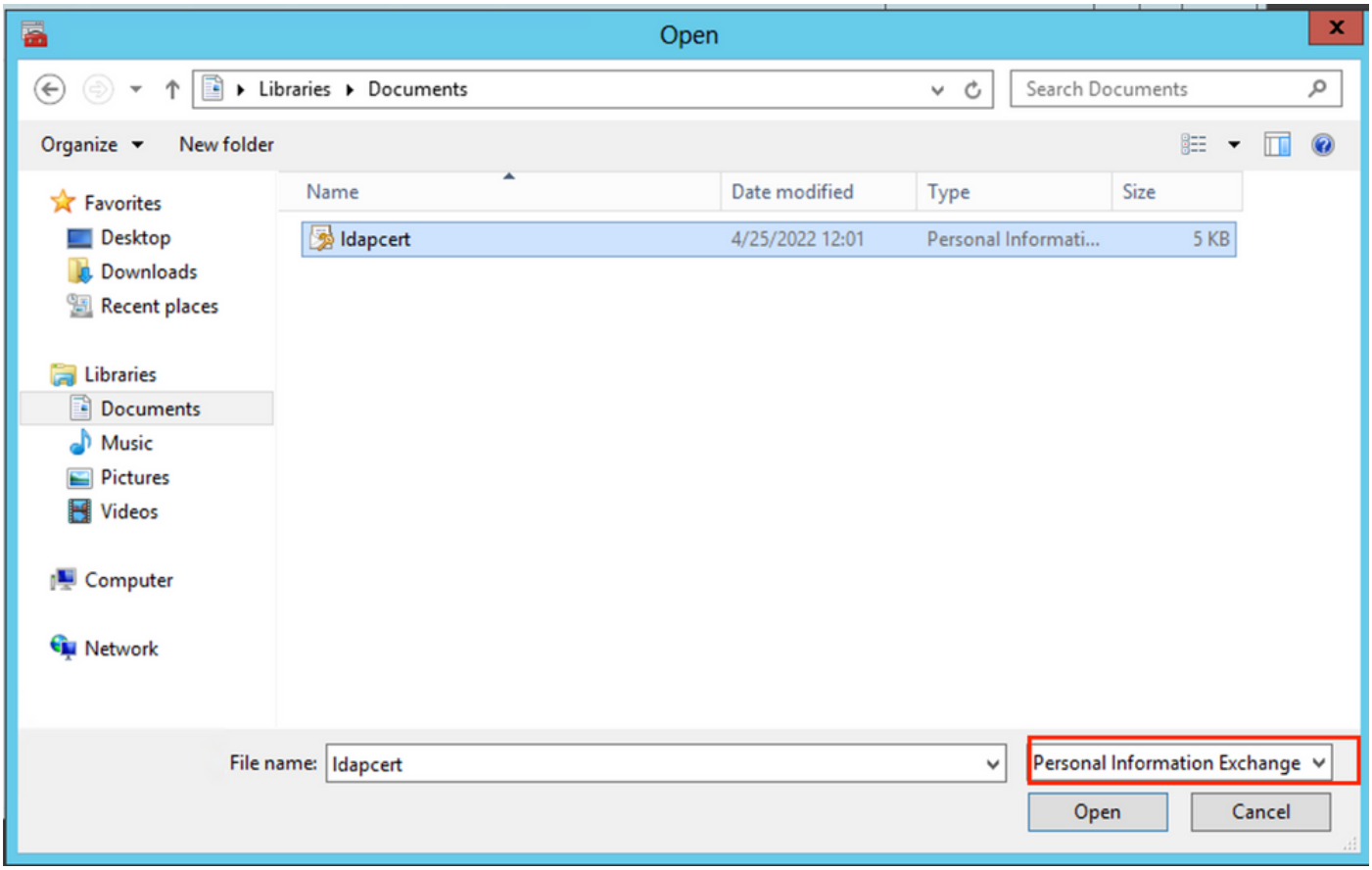
- Scegli Active Directory Domain Services e quindi fare clic su Finish.



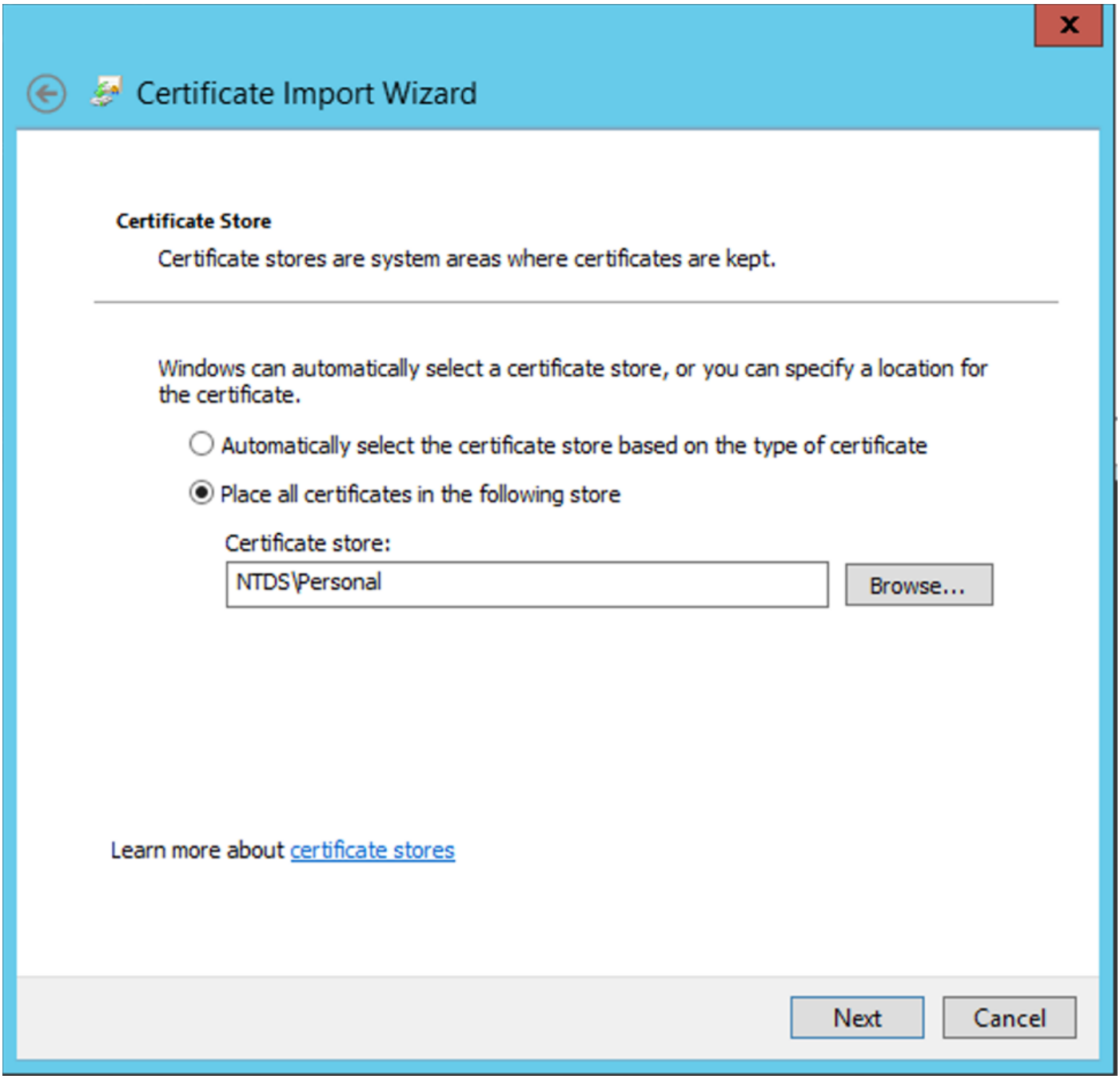
- Nella scheda Add/Remove Snap-ins fare clic su OK.
- Espansione Certificates - Services (Active Directory Domain Services) e quindi fare clic su NTDS\Personal.
- Clic con il pulsante destro del mouse NTDS\Personal,fare clic su All Taskse quindi fare clic su Import.



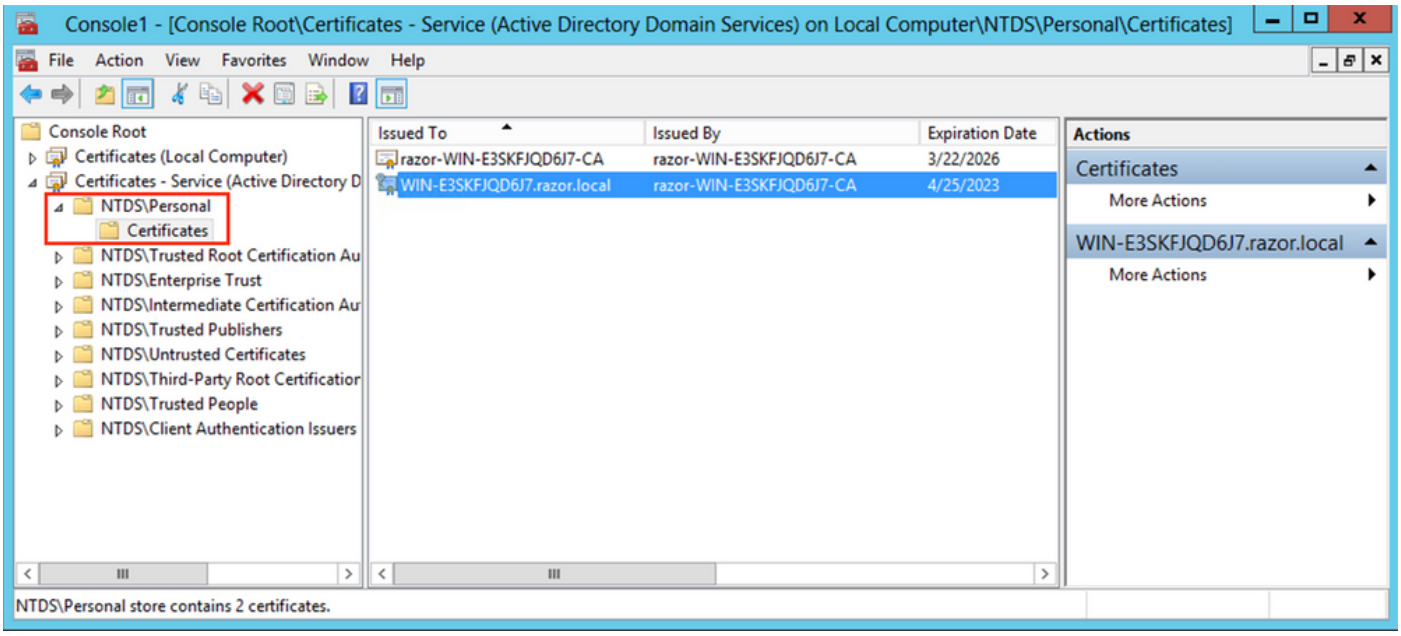
- Nella scheda Certificate Import Wizard schermata iniziale, fare clic su Next.
- Nella schermata File da importare fare clic su Browsee individuare il file del certificato esportato in precedenza.
- Nella schermata Apri, verificare che Scambio di informazioni personali (*pfx,*.p12) è selezionato come tipo di file, quindi spostarsi nel file system per individuare il certificato esportato in precedenza. Fare quindi clic sul certificato.



- Fare clic su Open e quindi fare clic su Next.
- Nella schermata Password, immettere la password impostata per il file, quindi fare clic su Next.
- Nella pagina Archivio certificati verificare che l'opzione Inserisci tutti i certificati sia selezionata e leggere Archivio certificati: NTDS\Personal e quindi fare clic su Next.



- Nella scheda Certificate Import Wizard completamento, fare clic su Finish. Viene quindi visualizzato un messaggio che indica che l'importazione è stata completata. Fare clic su OK. Il certificato è stato importato nell'archivio certificati: NTDS\Personal.



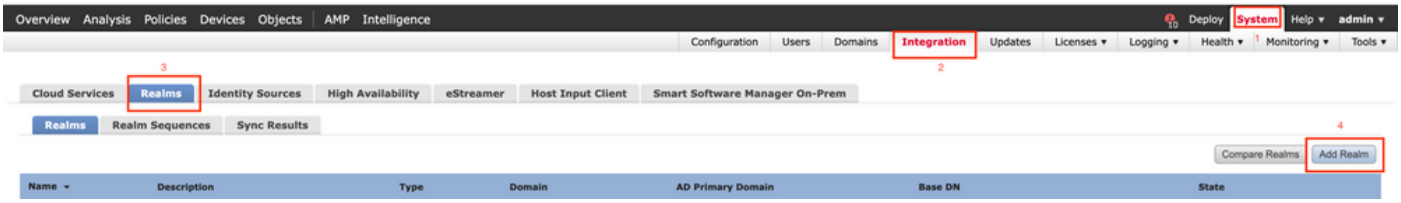
Configurazioni FMC

Verifica delle licenze

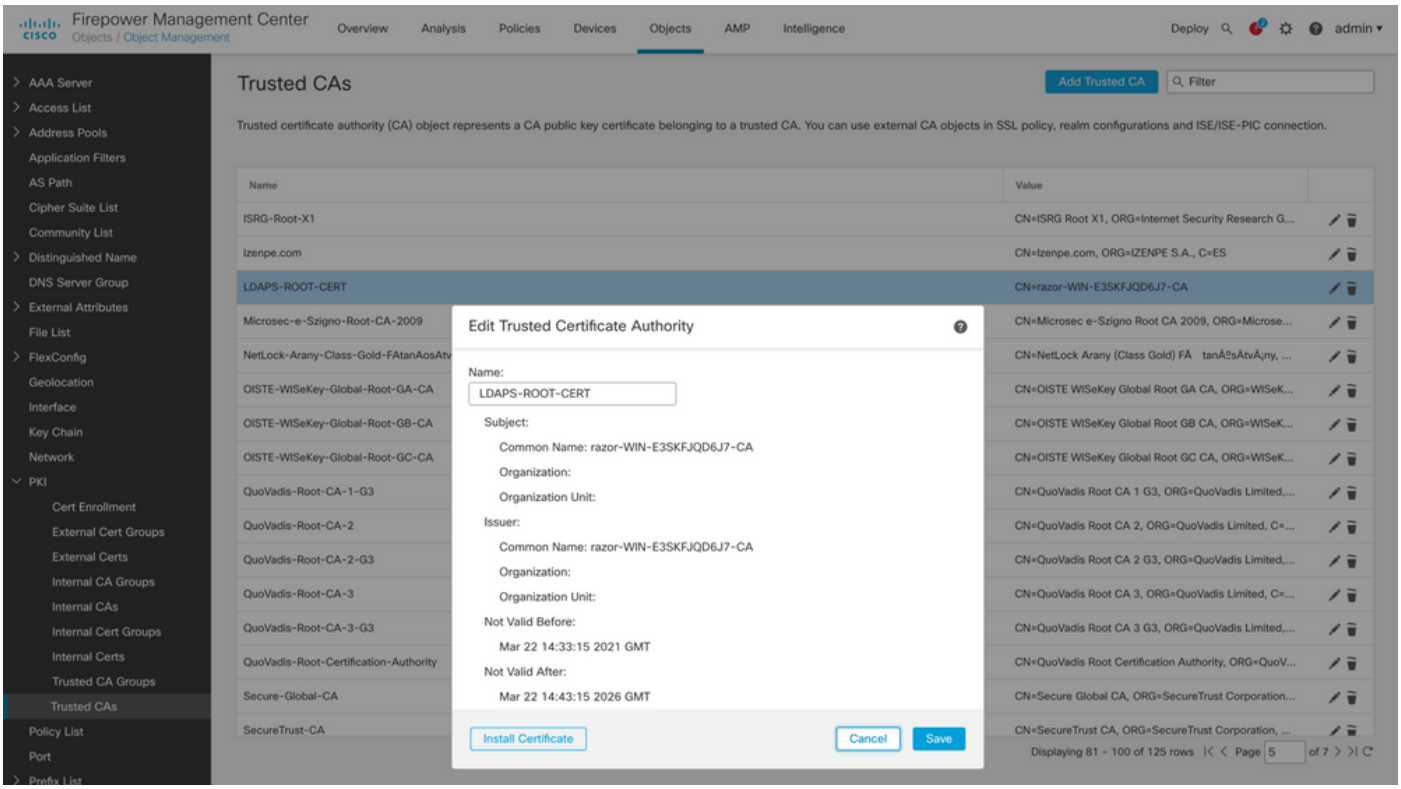
Per implementare la configurazione AnyConnect, l'FTD deve essere registrato con il server delle licenze Smart, e al dispositivo deve essere applicata una licenza Plus, Apex o VPN Only valida.

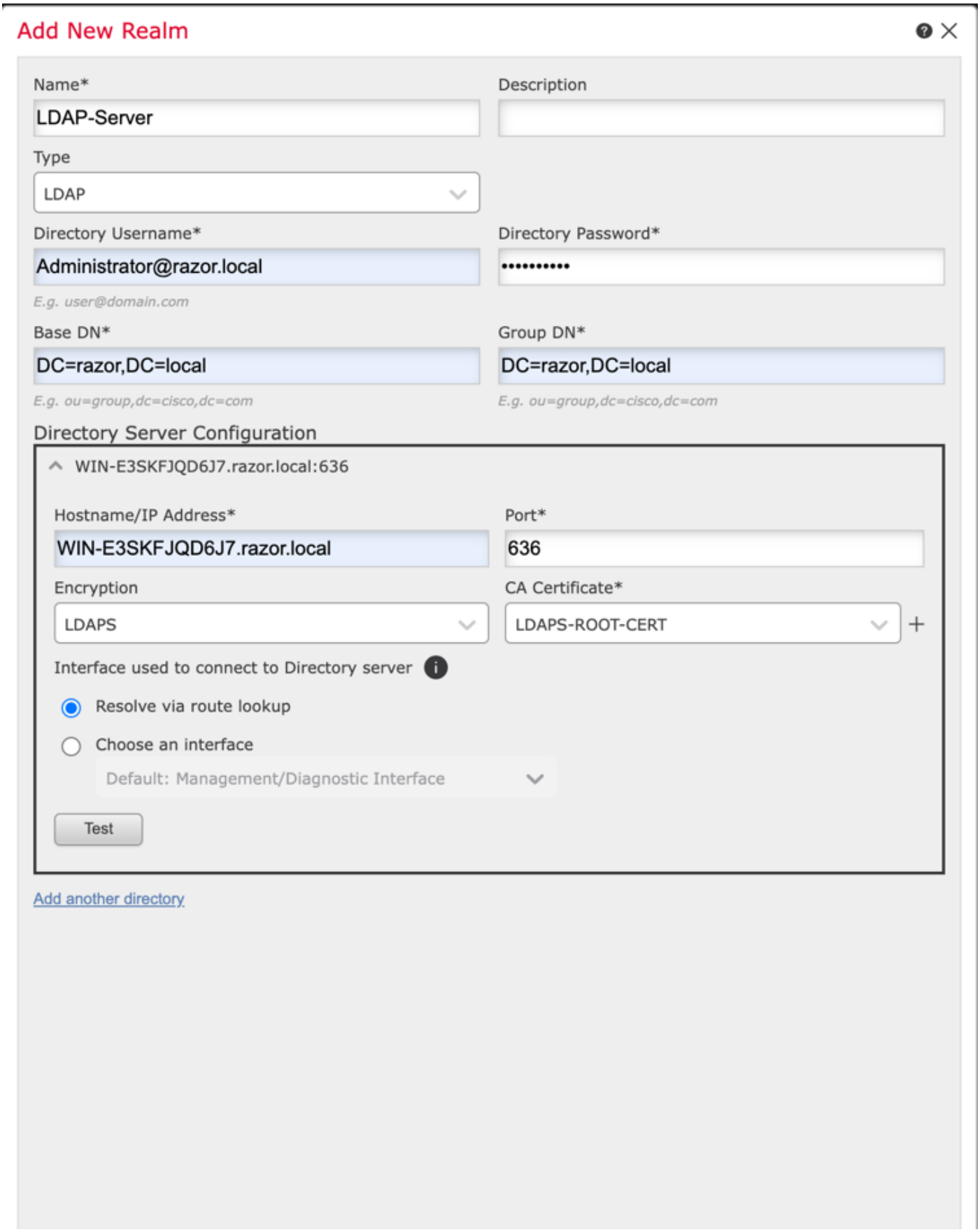
Imposta realm

1. Passa a System > Integration. Passa a Realms, quindi scegliere Add Realm, come mostrato nell'immagine:



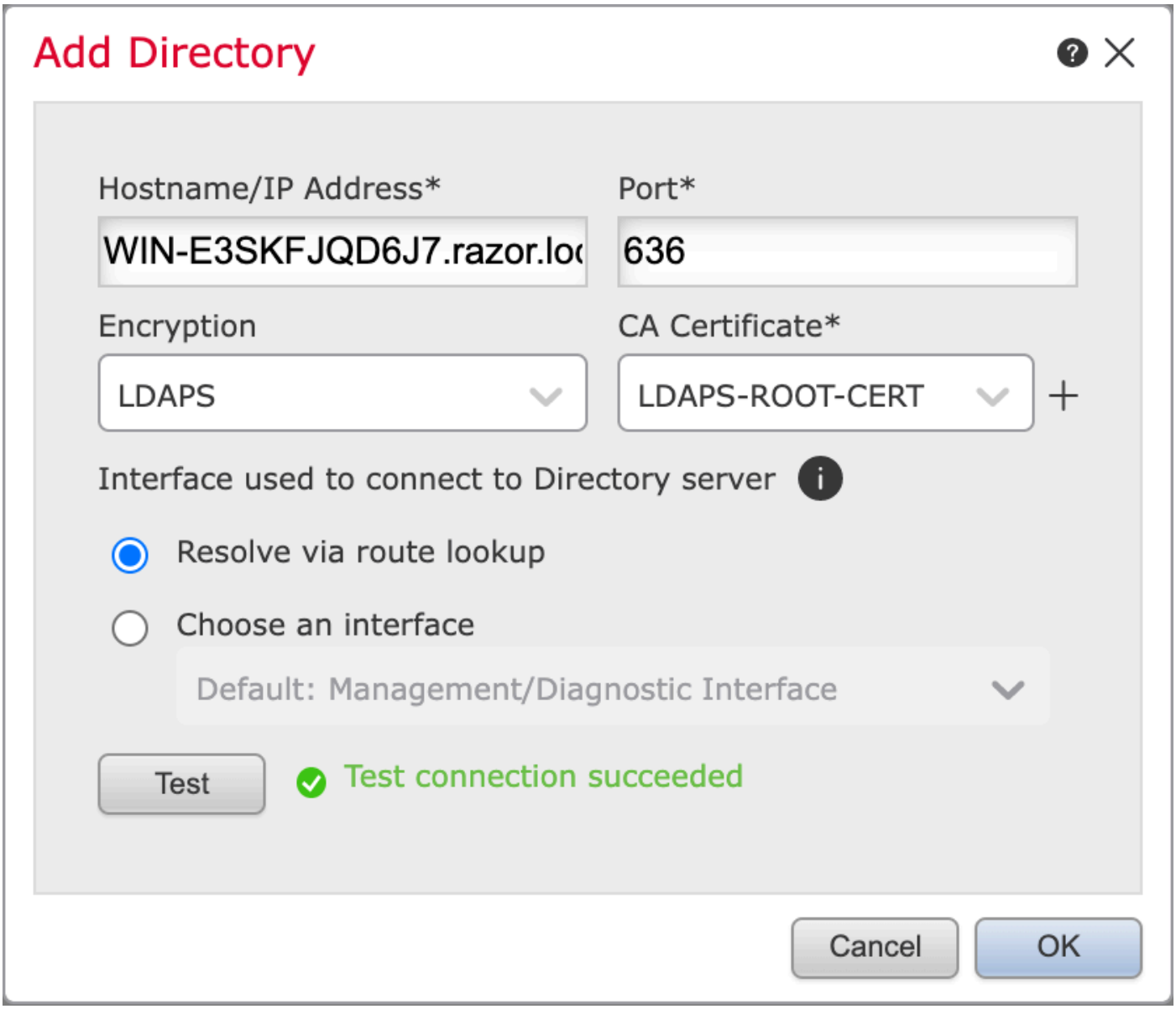
2. Compilare i campi visualizzati in base alle informazioni raccolte dal server Microsoft per LDAP. In precedenza, importare il certificato CA radice che ha firmato il certificato del servizio LDAP sul server Windows in Objects > PKI > Trusted CAs > Add Trusted CA, in quanto è indicato nell'Directory Server Configuration del Realm. Al termine, fare clic su 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

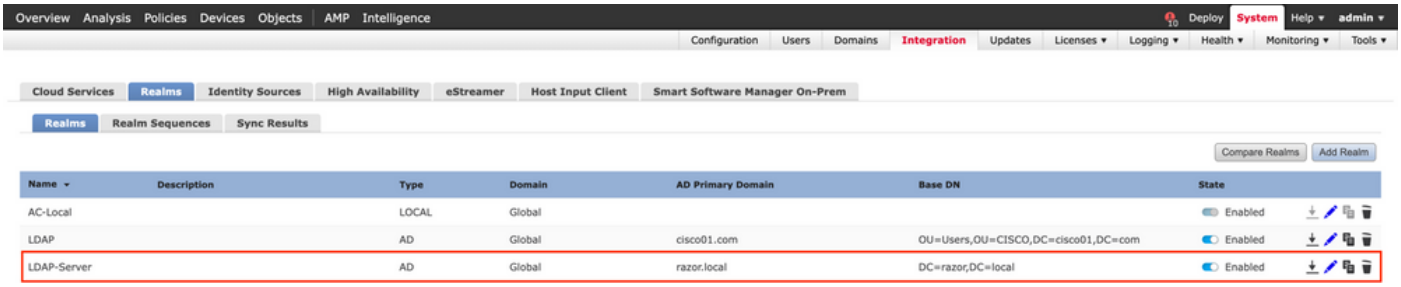


3. Fare clic su Test per garantire che FMC sia in grado di eseguire correttamente il binding con il nome utente e la password della directory forniti nel passaggio precedente. Poiché questi test vengono avviati dal FMC e non tramite una delle interfacce instradabili configurate sull'FTD (come interna, esterna, dmz), una connessione riuscita (o non riuscita) non

garantisce lo stesso risultato per l'autenticazione AnyConnect poiché le richieste di autenticazione LDAP AnyConnect vengono avviate da una delle interfacce instradabili FTD.

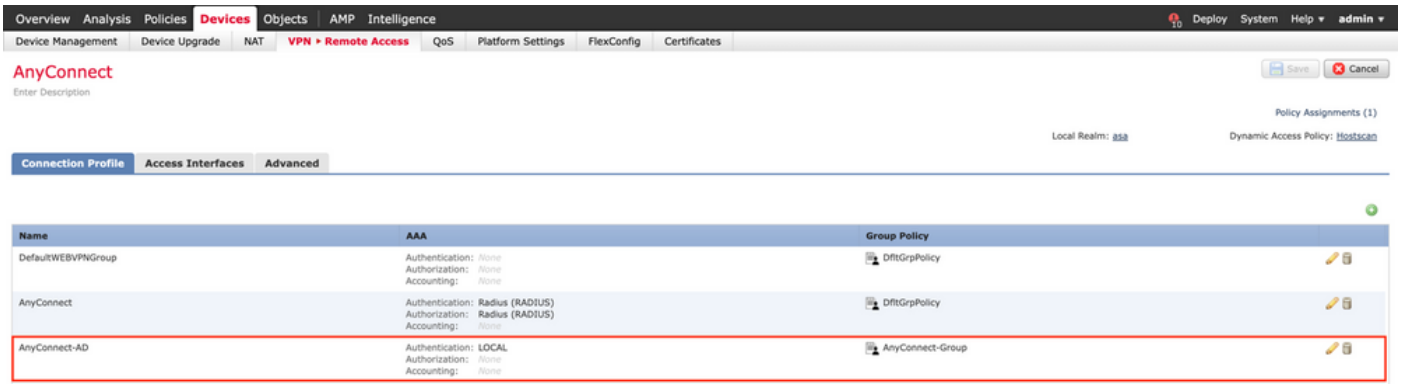


4. Abilitare il nuovo realm.

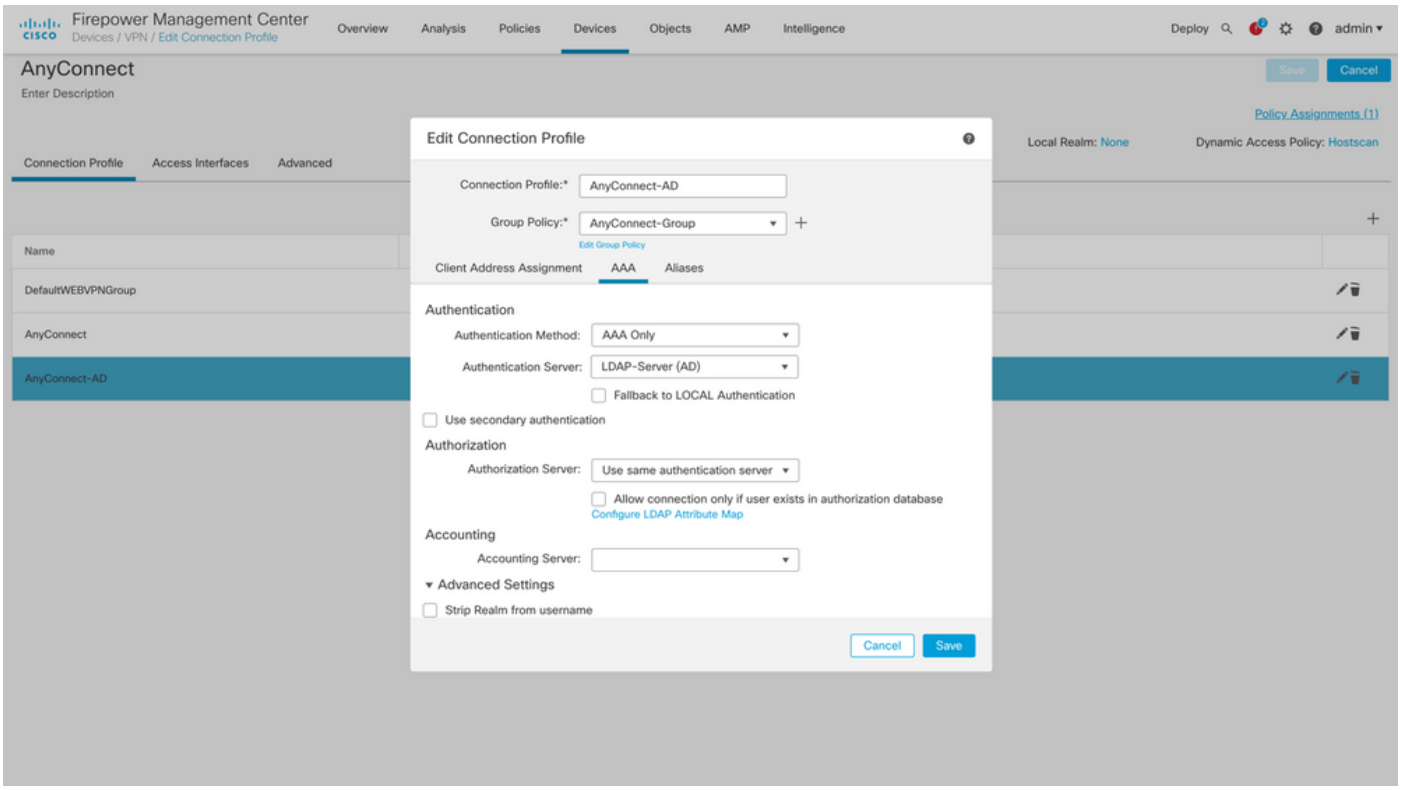


Configurazione di AnyConnect per la gestione delle password

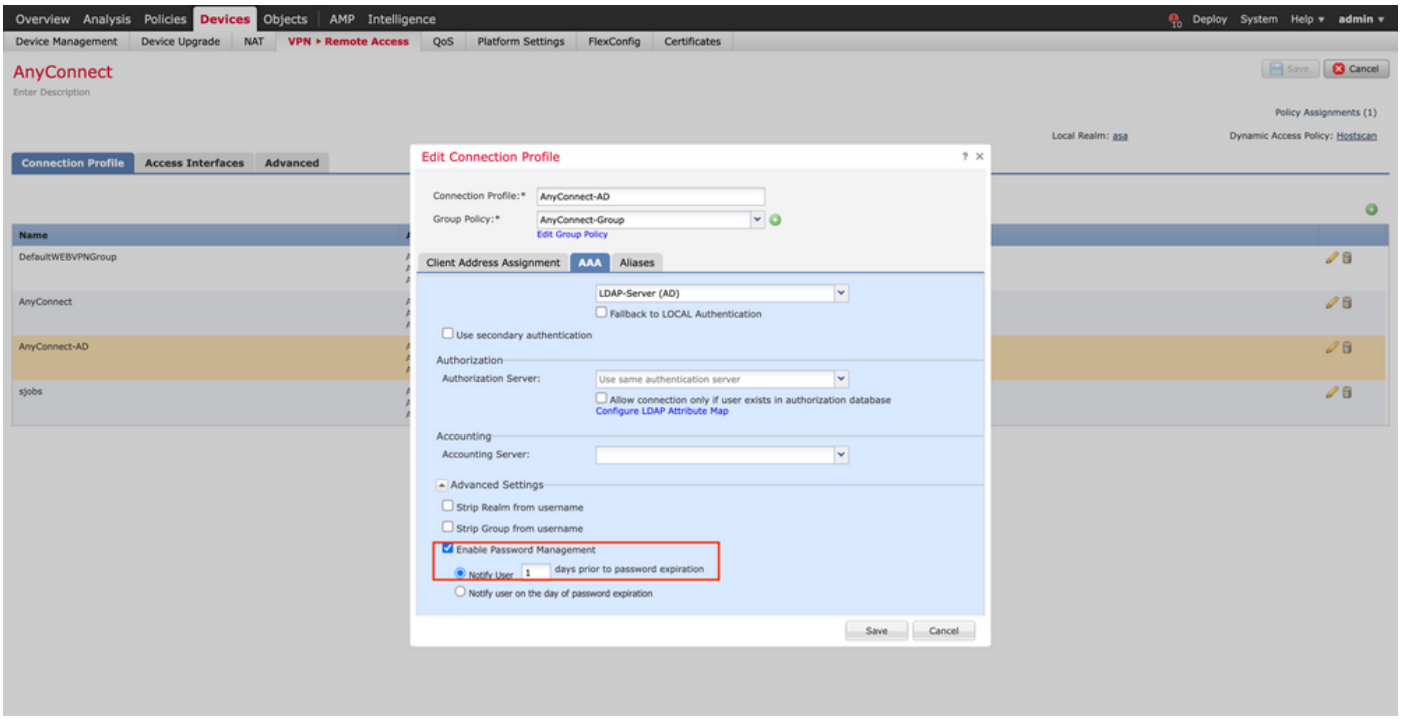
1. Selezionare il profilo di connessione esistente o crearne uno nuovo, se si tratta dell'impostazione iniziale di AnyConnect. In questo caso, viene utilizzato un profilo di connessione esistente denominato 'AnyConnect-AD' mappato con l'autenticazione locale.



2. Modificare il profilo di connessione ed eseguire il mapping del nuovo server LDAP configurato nei passaggi precedenti, nelle impostazioni AAA del profilo di connessione. Al termine, fare clic su Save nell'angolo superiore destro.



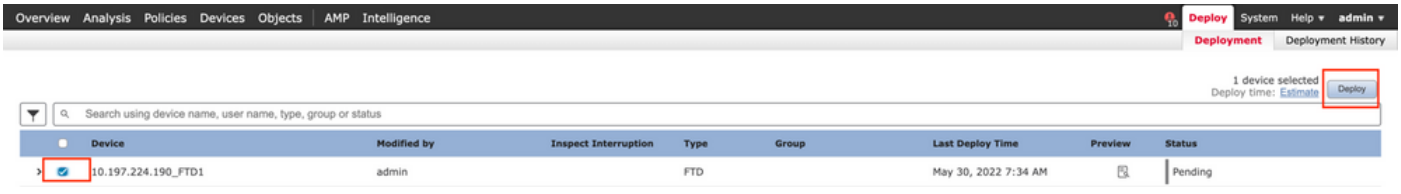
3. Abilitare la gestione delle password in AAA > Advanced Settings e salvare la configurazione.



Implementazione

1. Una volta completata la configurazione, fare clic sul pulsante Deploy in alto a destra.

2. Fare clic sulla casella di controllo accanto alla configurazione FTD applicata e quindi fare clic su Deploy, come mostrato nell'immagine:



Configurazione finale

Questa è la configurazione rilevata nella CLI FTD dopo la corretta distribuzione.

Configurazione AAA

<#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
```

Configurazione AnyConnect

<#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
```

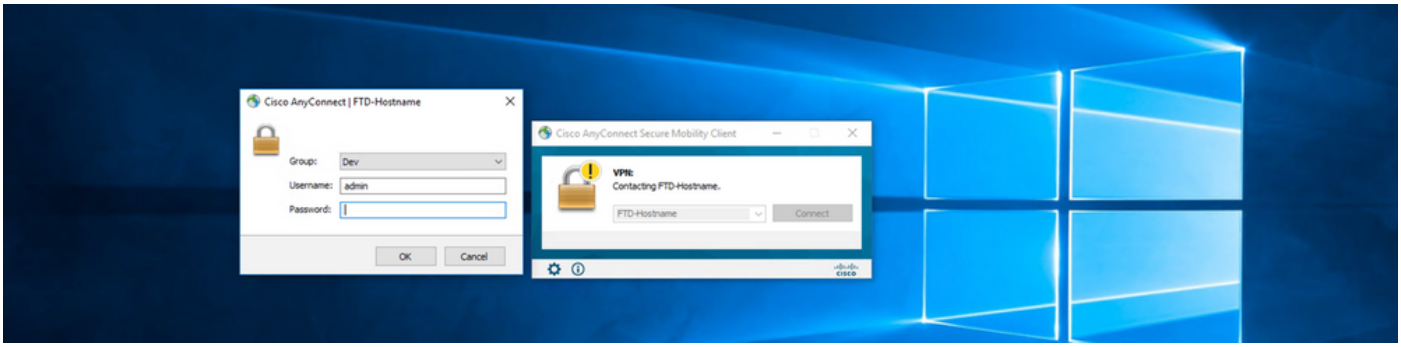
```
 default-domain none
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private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

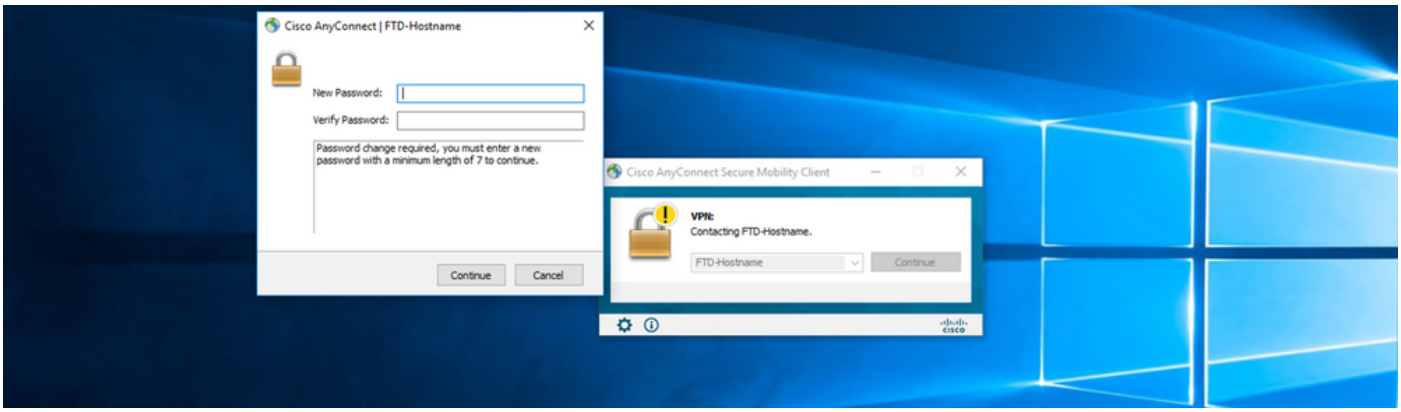
```
> show running-config ssl

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

Verifica

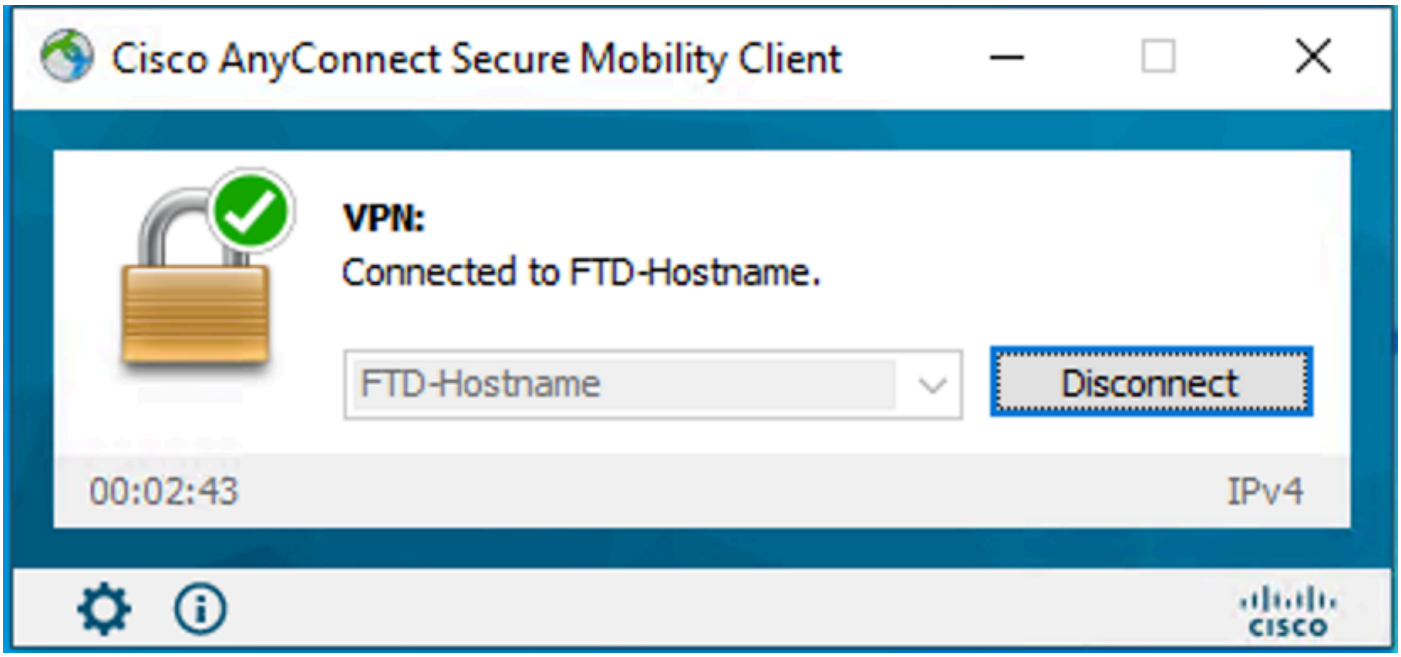
Connettersi con AnyConnect e verificare il processo di gestione delle password per la connessione utente

1. Avviare una connessione al profilo di connessione interessato. Una volta stabilito al primo accesso che la password deve essere cambiata poiché la password precedente è stata rifiutata da Microsoft Server poiché è scaduta, all'utente viene richiesto di cambiare la password.





2. Una volta che l'utente ha immesso la nuova password per l'accesso, la connessione viene stabilita correttamente.



3. Verificare la connessione utente nella CLI FTD:

<#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
```

Risoluzione dei problemi

Debug

Questo debug può essere eseguito nella CLI diagnostica per risolvere i problemi relativi alla gestione delle password: debug ldap 255.

Debug relativi alla gestione delle password durante il lavoro

<#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

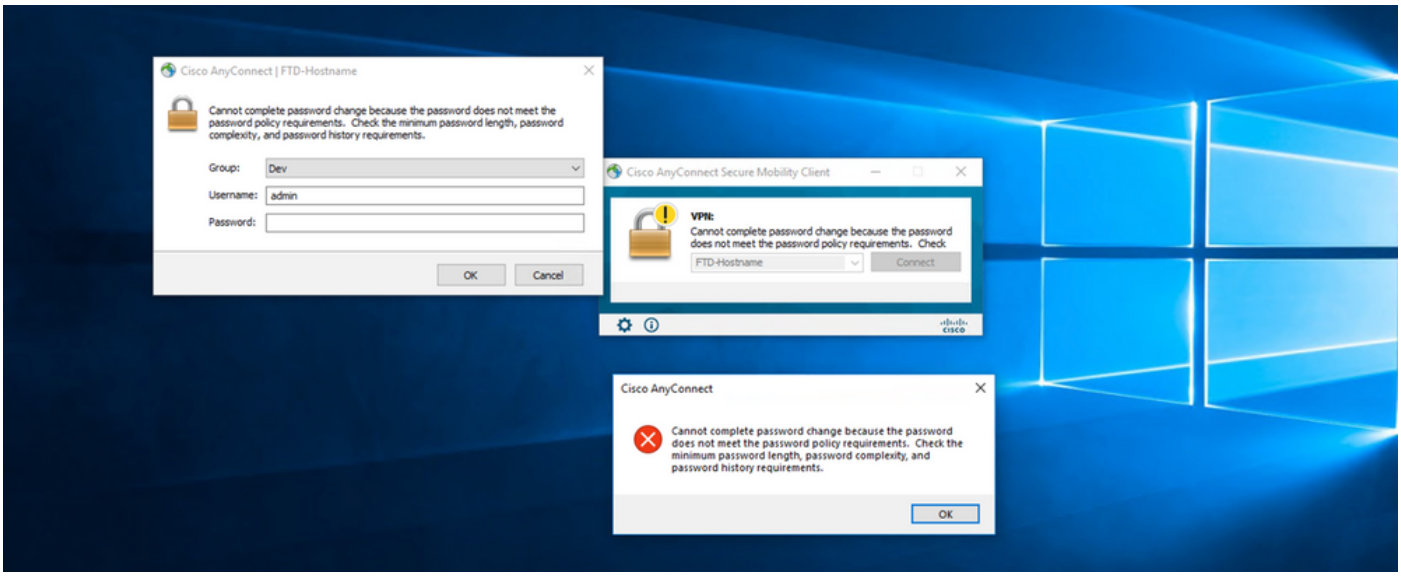
[25] instanceType: value = 4

[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
```

Errori comuni rilevati durante la gestione delle password

In genere, se i criteri password impostati da Microsoft Server non vengono soddisfatti durante il periodo di tempo in cui l'utente immette la nuova password, la connessione viene terminata con l'errore "La password non soddisfa i requisiti dei criteri password". Verificare quindi che la nuova password soddisfi i criteri impostati da Microsoft Server per LDAP.



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).