

在FMC管理的FTD上，使用RA VPN的LDAP配置密碼管理

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[組態](#)

[網路圖表和案例](#)

[確定LDAP基本DN和組DN](#)

[複製LDAPS SSL證書根](#)

[在LDAP伺服器上的本地電腦儲存中安裝多個證書的情況下 \(可選 \)](#)

[FMC配置](#)

[驗證許可](#)

[設定領域](#)

[配置AnyConnect進行密碼管理](#)

[部署](#)

[最終配置](#)

[AAA組態](#)

[AnyConnect配置](#)

[驗證](#)

[使用AnyConnect連線並驗證使用者連線的密碼管理過程](#)

[疑難排解](#)

[調試](#)

[正在處理的密碼管理調試](#)

[密碼管理過程中遇到的常見錯誤](#)

簡介

本文檔介紹使用LDAP為連線到Cisco Firepower Threat Defense(FTD)的AnyConnect客戶端配置密碼管理。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 基本瞭解FMC上的RA VPN (遠端訪問虛擬專用網路) 配置
- FMC上的LDAP伺服器配置基礎知識

- Active Directory基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft 2012 R2伺服器
- 運行7.3.0的FMCv
- 執行7.3.0的FTDv

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

網路圖表和案例



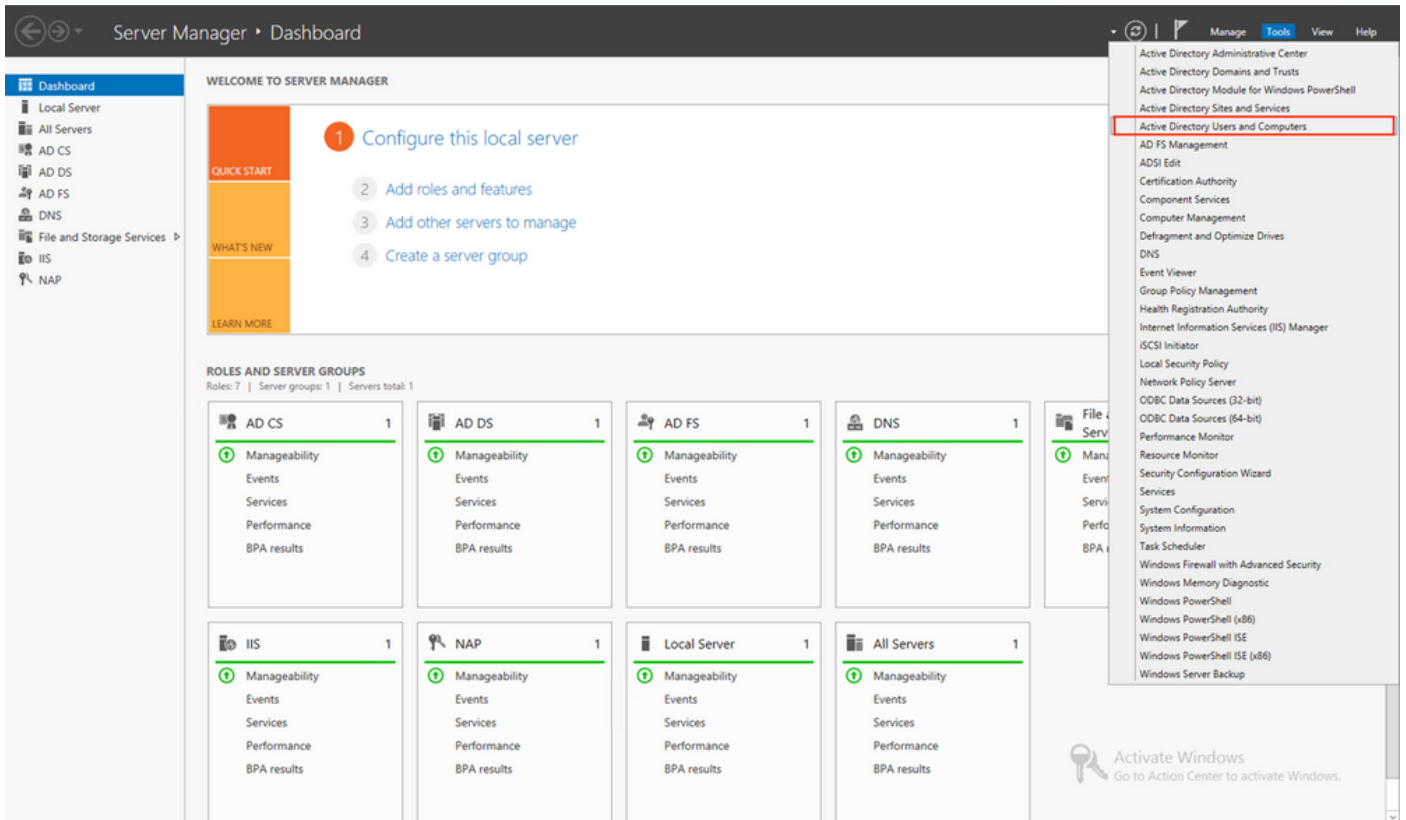
Windows伺服器預配置了ADDS和ADCS以測試使用者密碼管理過程。在此配置指南中，將建立這些使用者帳戶。

使用者帳戶：

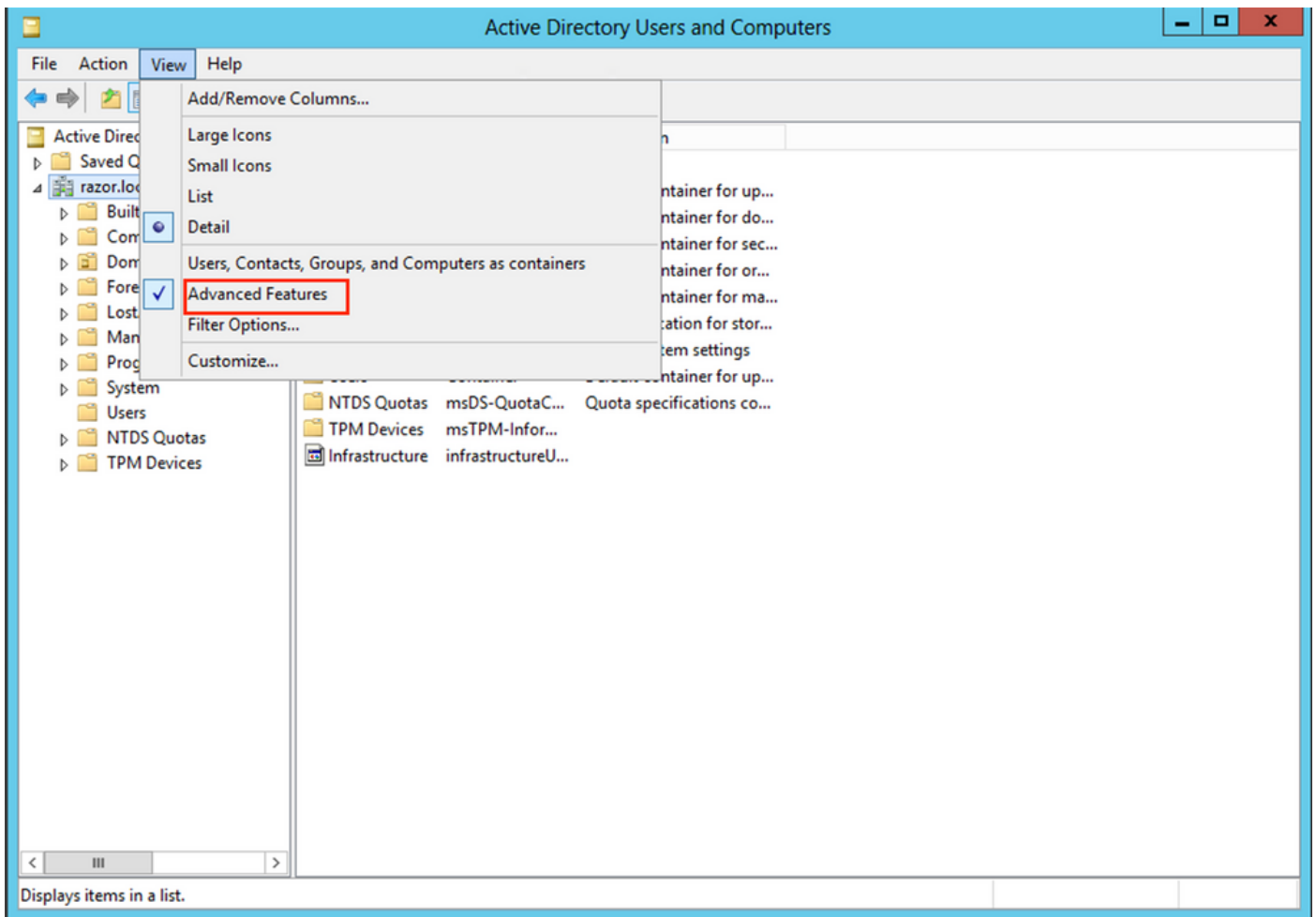
- 管理員：此帳戶用作目錄帳戶，以允許FTD繫結到Active Directory伺服器。
- admin：用於演示使用者身份的測試管理員帳戶。

確定LDAP基本DN和組DN

1. 通過Active Directory Users and Computers「Server Manager Dashboard」（伺服器管理器控制面板）開啟。

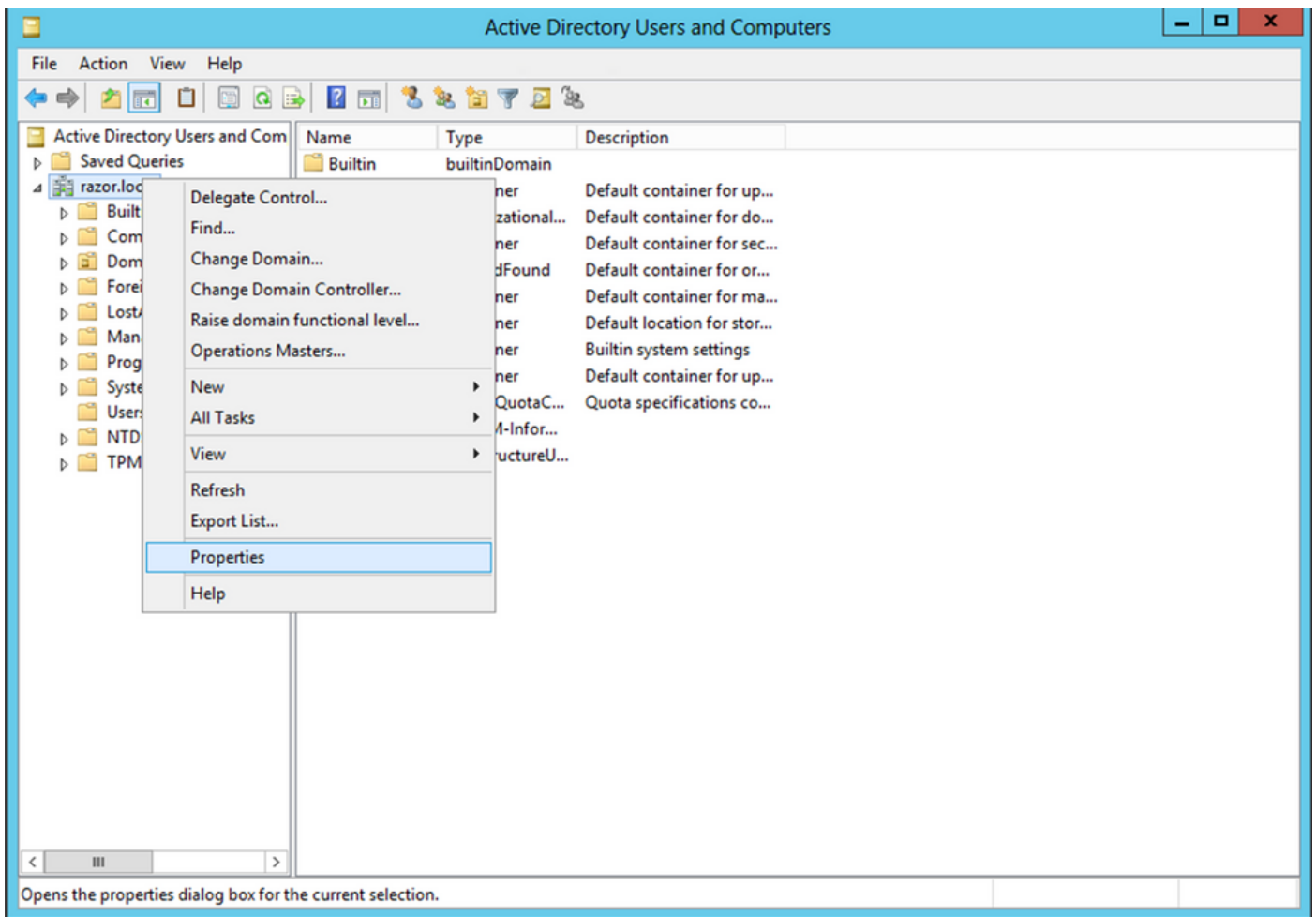


開啟View Option 「頂部」 面板上的，然後啟用Advanced Features，如下圖所示：



•
這允許檢視AD對象下的其他屬性。

例如，若要尋找根的DNrazor.local，請按一下右鍵razor.local，然後選擇Properties，如下圖所示：



在Properties下，選擇Attribute Editor頁籤。在「distinguishedNameAttributes」下查詢，然後按一下View，如下圖所示。

這將開啟一個新視窗，可以在其中複製並稍後將DN貼上到FMC中。

在本例中，根DN是DC=razor, DC=local。複製該值並儲存以備以後使用。按一下OK「字串屬性編輯器」視窗退出，然後按一下OK「再次按一下」以退出「屬性」。

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; DsaGuid
dSCorePropagationD...	0x0 = ()
eFSPolicy	<not set>
extensionName	<not set>
flags	<not set>
forceLogoff	(never)

View Filter

String Attribute Editor

Attribute: distinguishedName

Value:

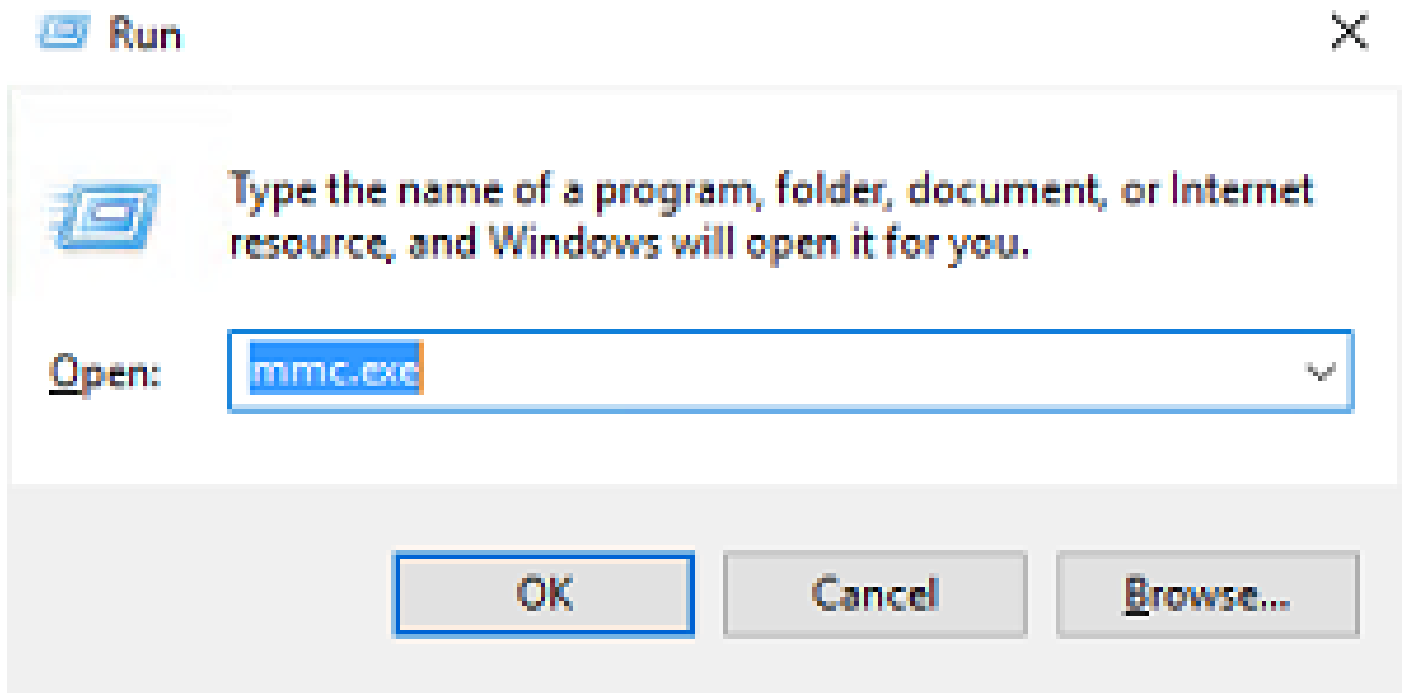
DC=razor,DC=local

Clear OK Cancel

複製LDAPS SSL證書根

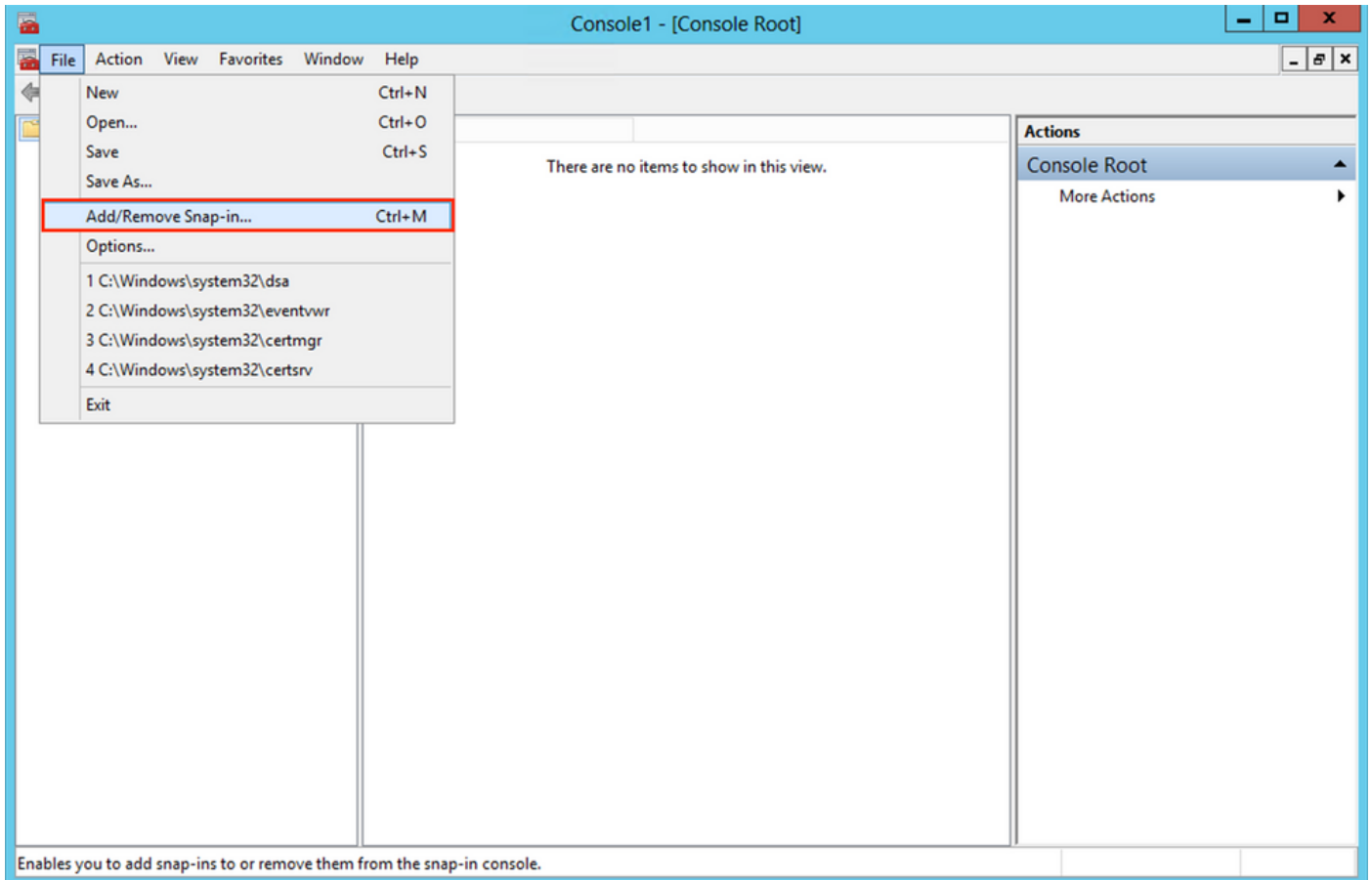
•

按Win+REnter鍵mmc.exe，然後按一下OK，如下圖所示。

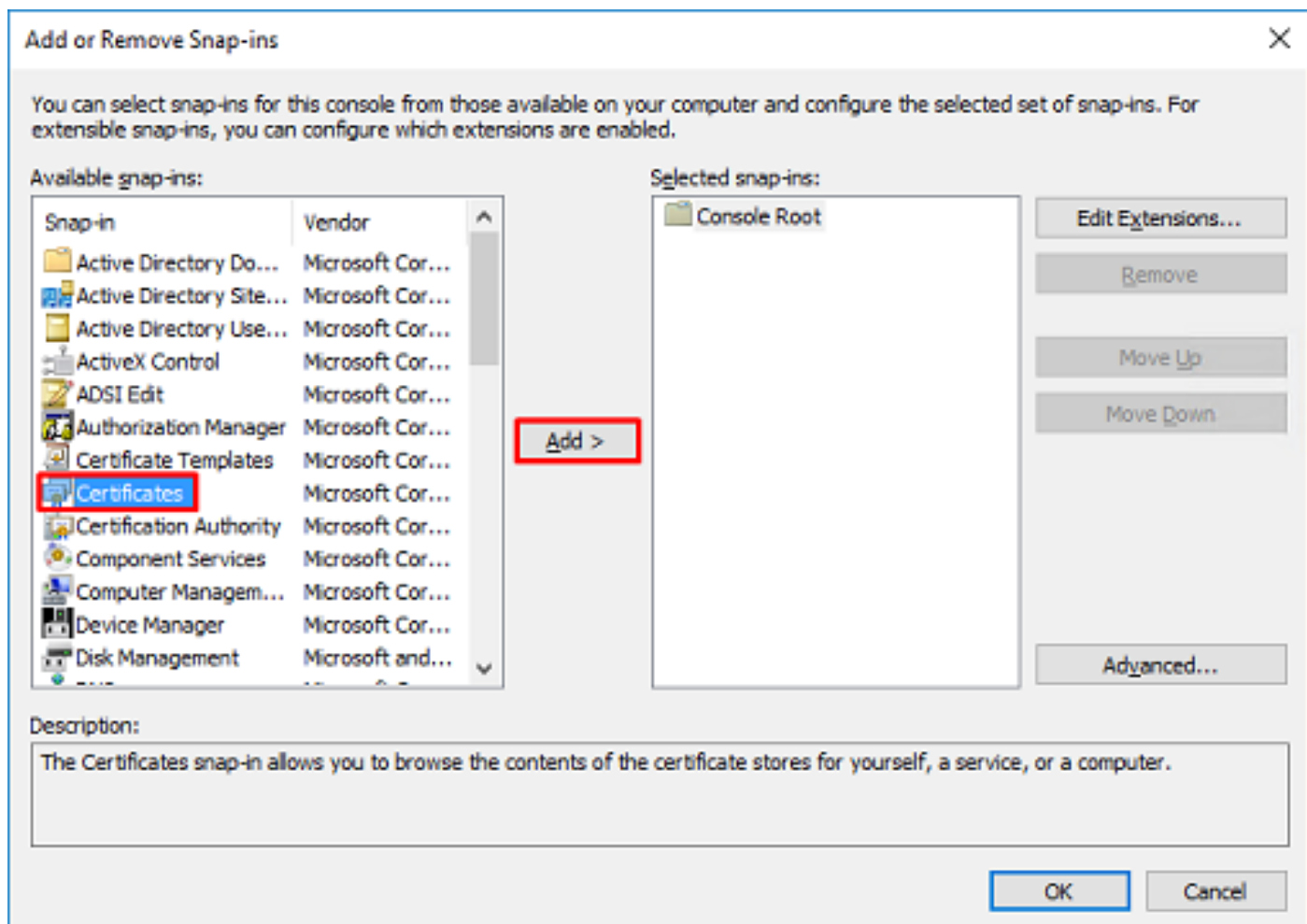


•

導覽至File > Add/Remove Snap-in..., ss，如下圖所示：

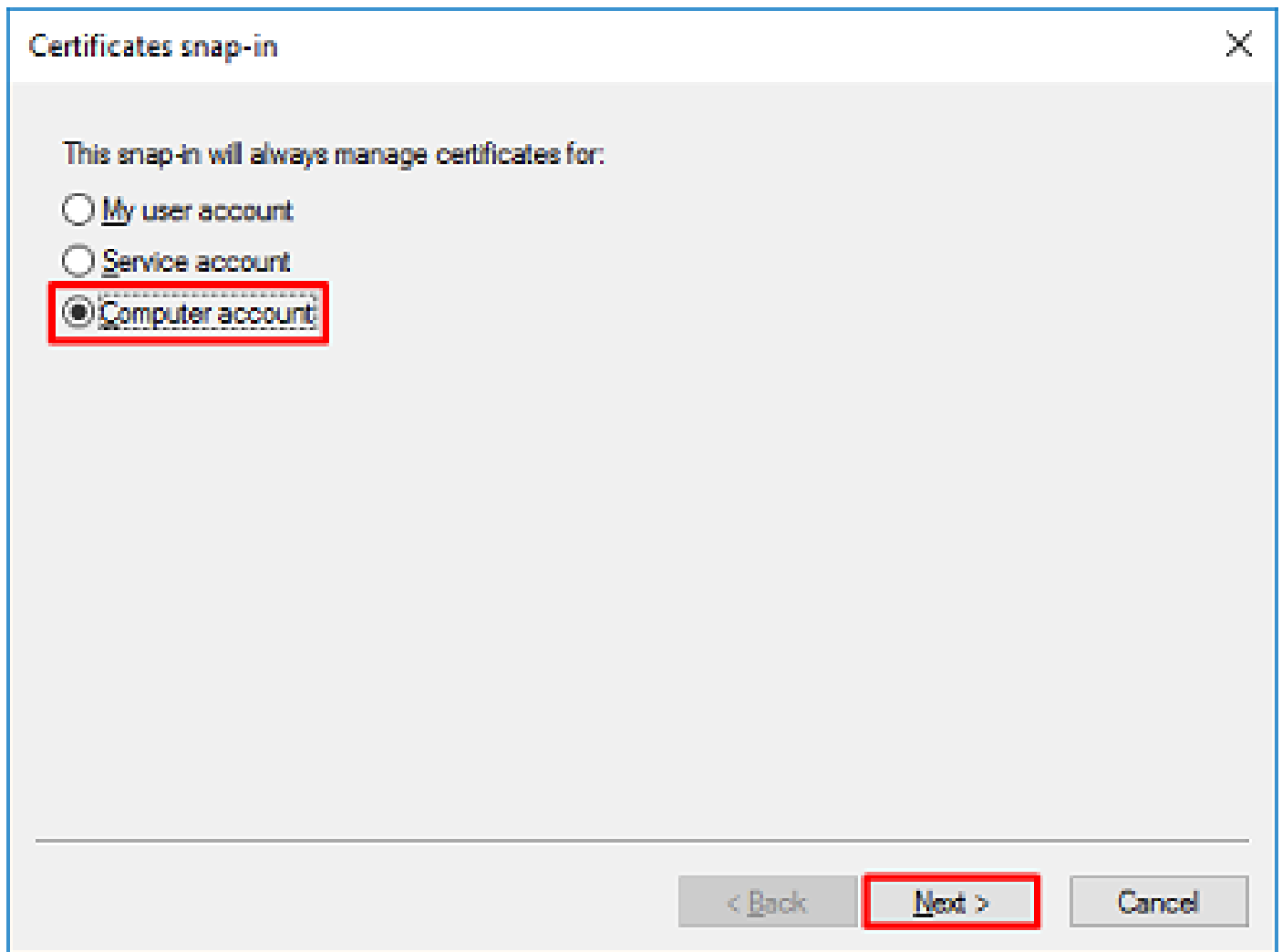


- 在「可用管理單元」下，選擇Certificates 然後按一下Add，如下圖所示：

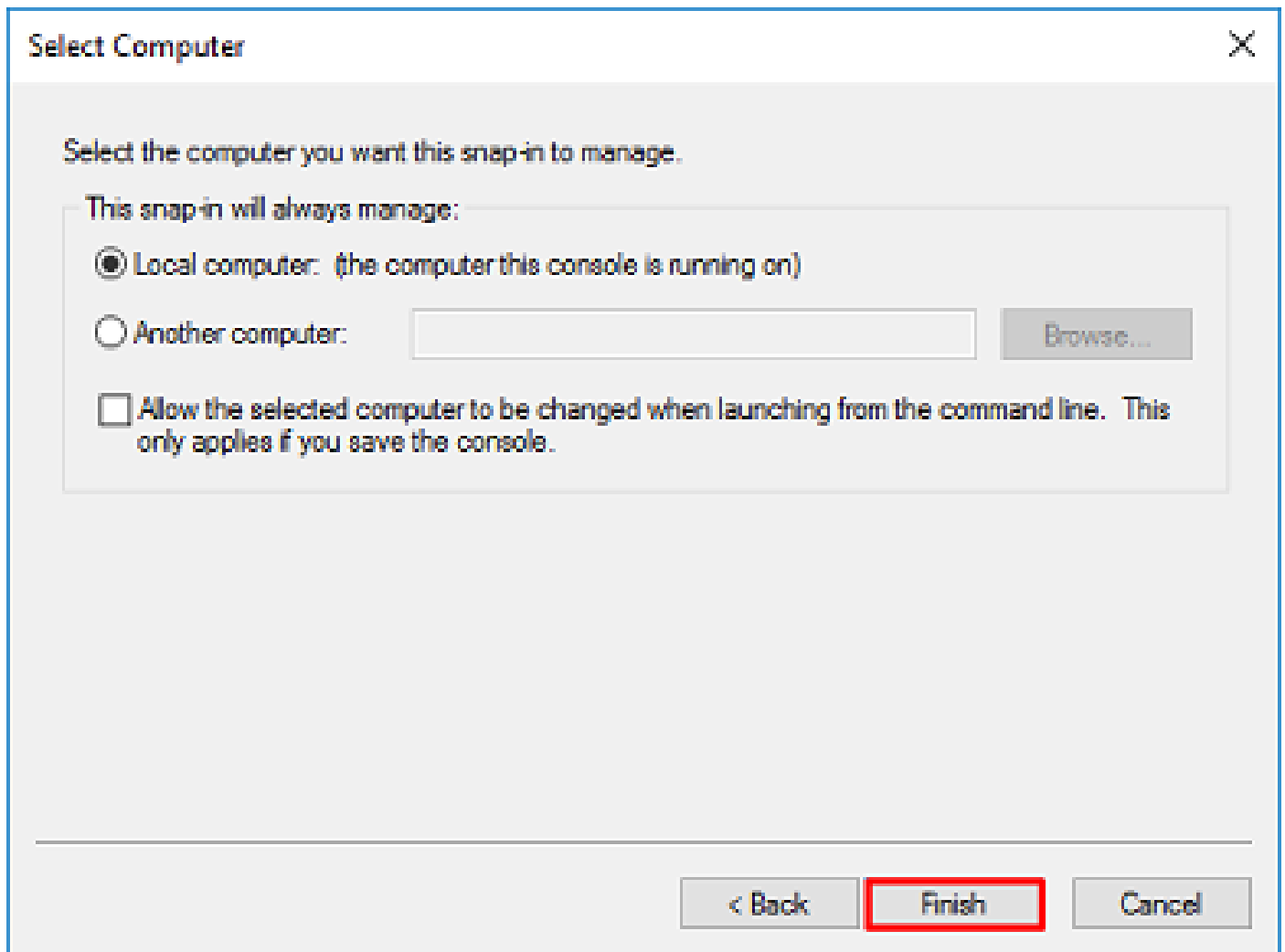


•

選擇「Computer account」，然後按一下Next「」，如下圖所示：

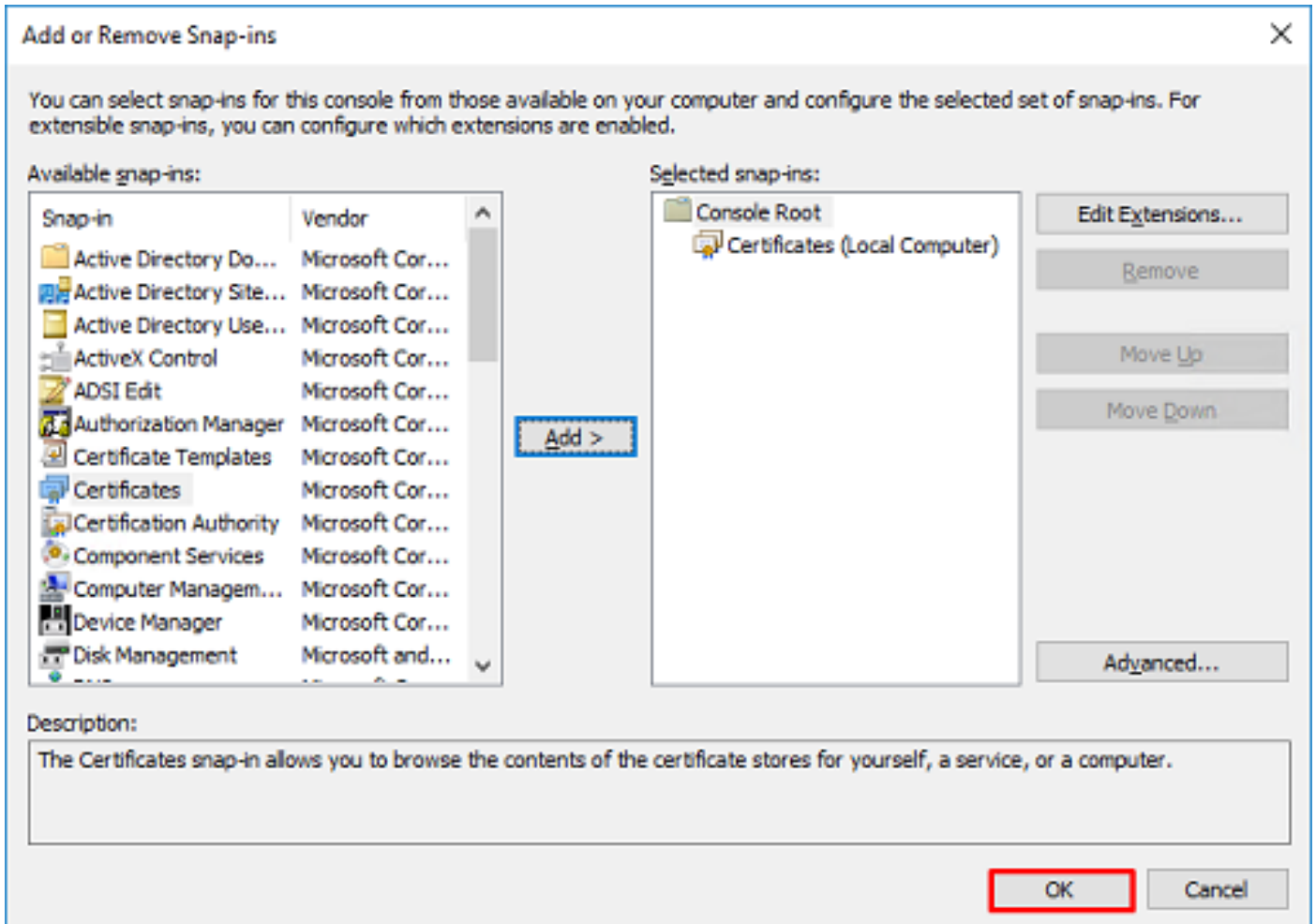


如圖所示，按一下Finish。



.

現在，按一下OK，如下圖所示。



•

展開檔案夾Personal，然後按一下Certificates。LDAP使用的證書必須頒發給Windows伺服器的完全限定域名(FQDN)。在此伺服器上列出三個憑證：

•

CA證書頒發給和頒發者razor-WIN-E3SKFJQD6J7-CA。

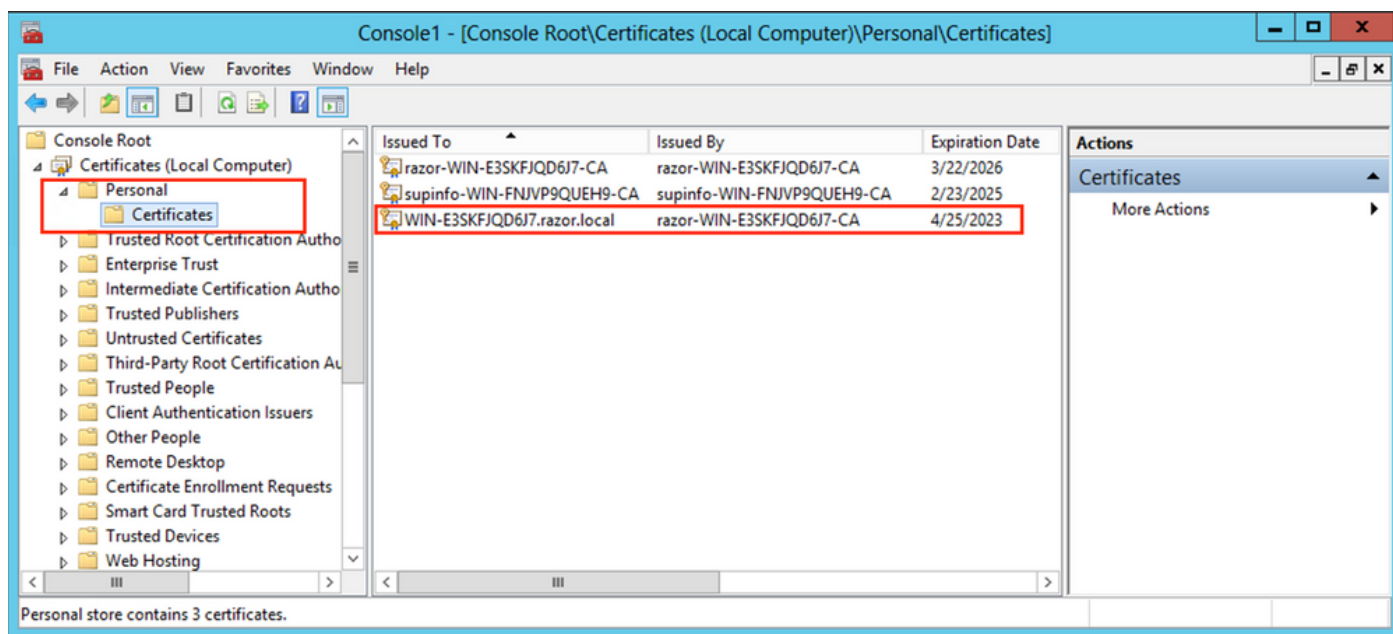
•

頒發給和頒發者的CA證書supinfo-WIN-FNJVP9QUEH9-CA。

•

已將身份證書頒發給WIN-E3SKFJQD6J7.razor.local。razor-WIN-E3SKFJQD6J7-CA。

在此配置指南中，FQDN為WIN-E3SKFJQD6J7.razor.local，因此前兩個證書不能用作LDAP的SSL證書。頒發給的身份證書WIN-E3SKFJQD6J7.razor.local，是由Windows Server CA服務自動頒發的證書。按兩下憑證以檢查詳細資訊。



-

要用作LDAP的SSL證書，證書必須滿足以下要求：

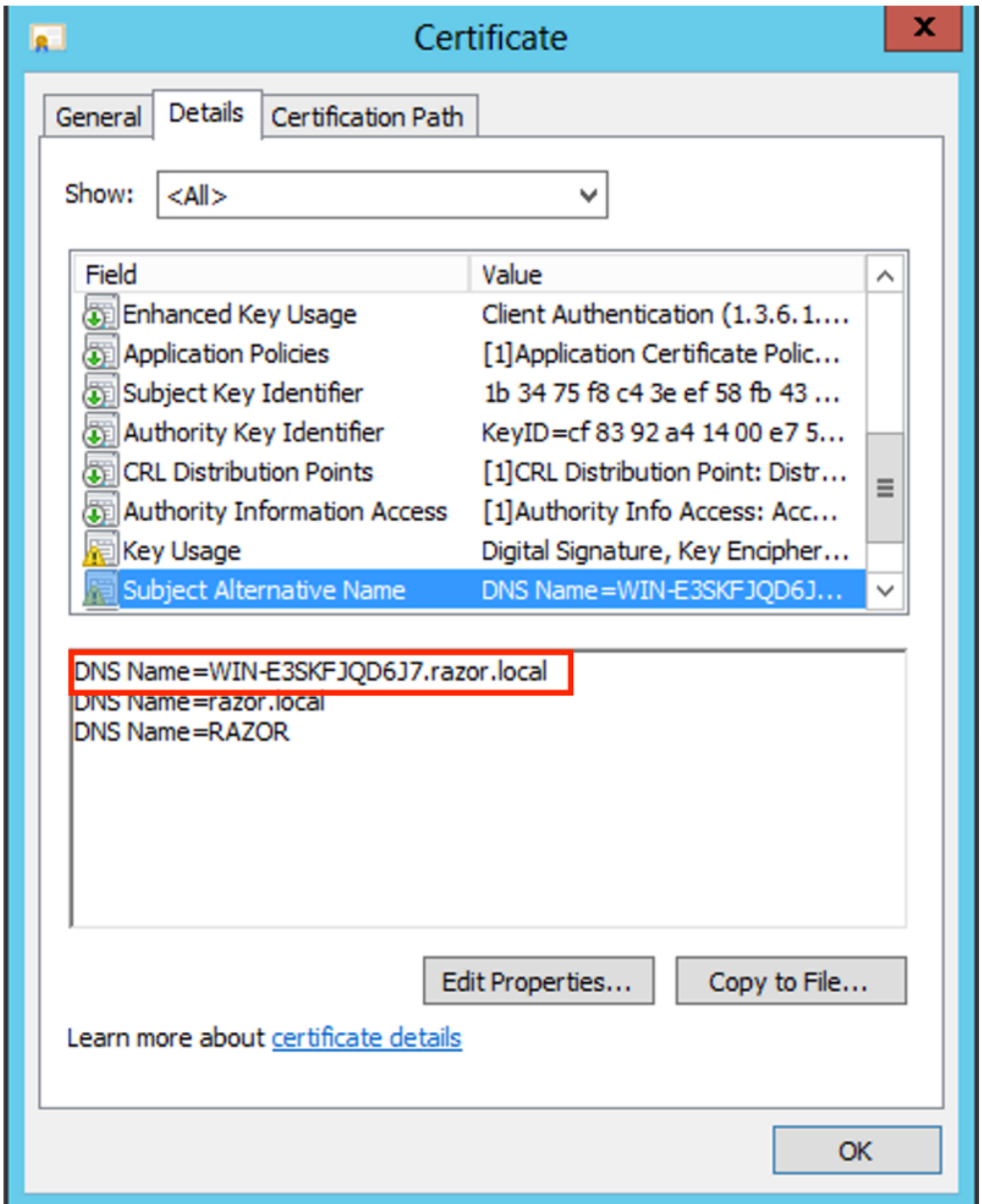
-

公用名稱或DNS使用者替代名稱與Windows Server的FQDN匹配。

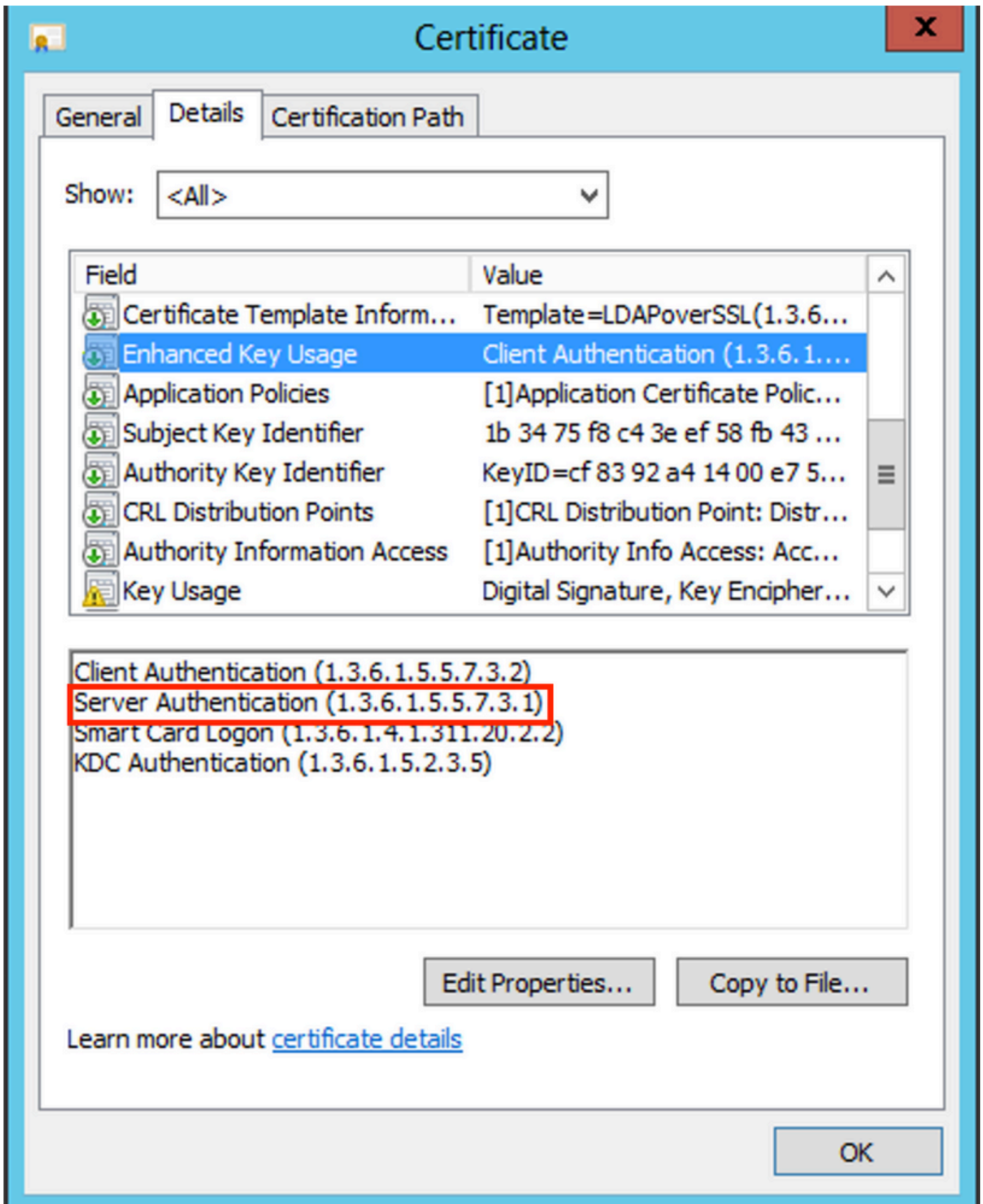
-

證書在Enhanced Key Usage欄位下有Server Authentication。

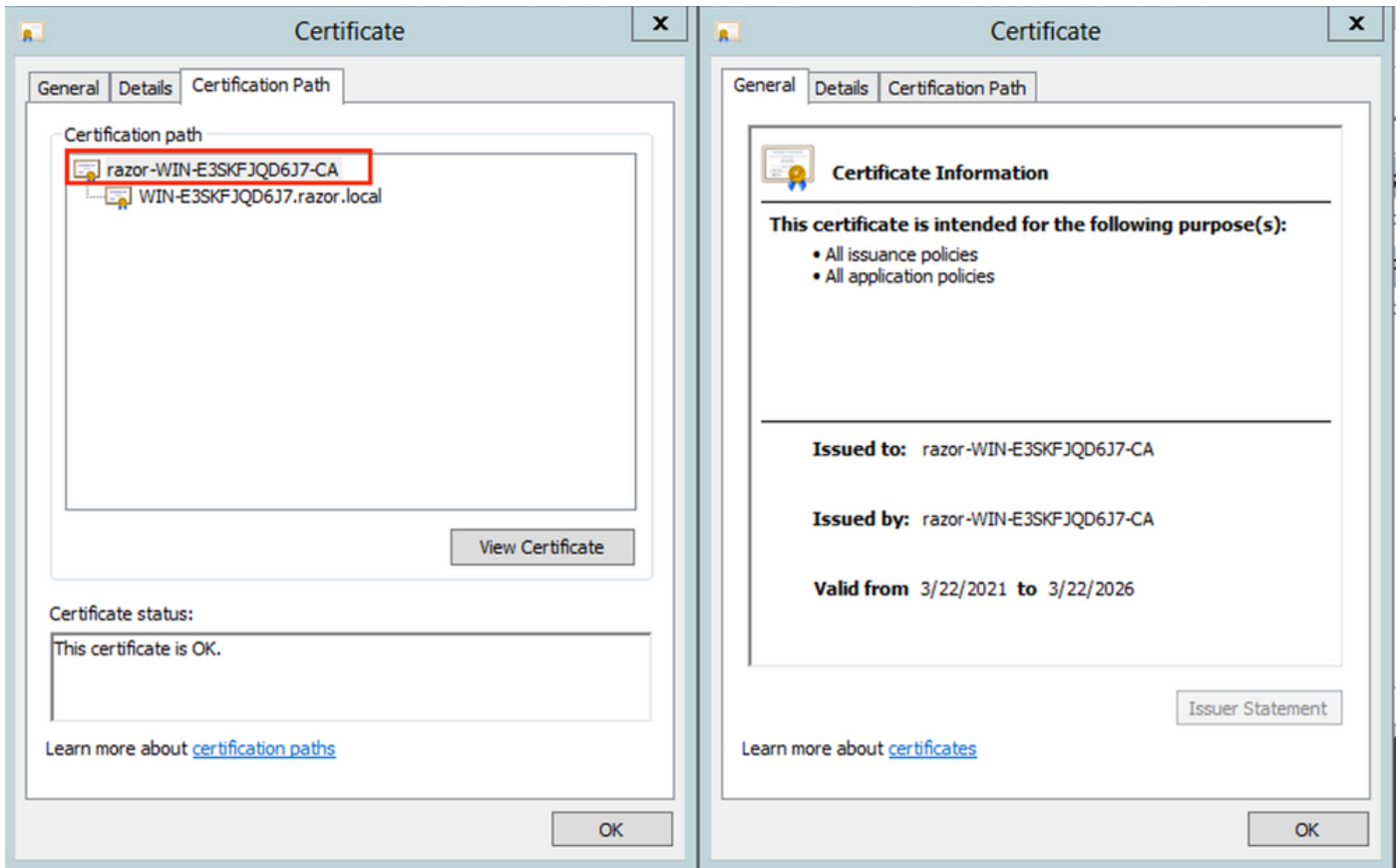
在證書的頁籤下Details，選擇Subject Alternative NameFQDN所在的WIN-E3SKFJQD6J7.razor.local位置。



在Enhanced Key Usage下Server Authentication，存在。



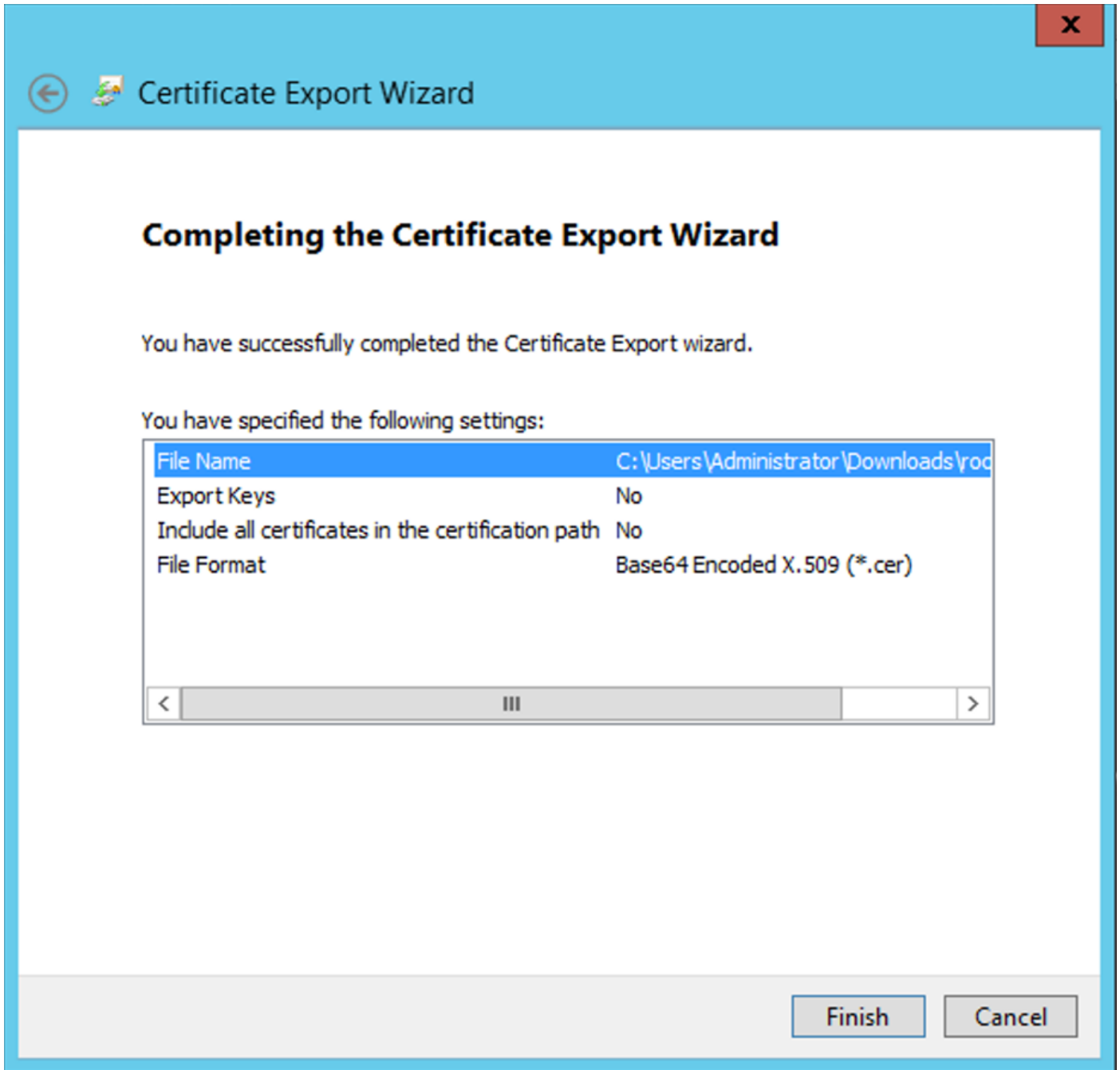
確認後，在Certification Path頁籤下，選擇作為根CA證書的頂級證書，然後按一下View Certificate。這將開啟根CA證書的證書詳細資訊，如下圖所示：



•

在根CADetails證書的頁籤下，按一下Copy to File 並導航到以PEM格式匯出根CA的Certificate Export Wizard。

選擇Base-64 encoded X.509 作為檔案格式。



•
使用記事本或其他文本編輯器開啟儲存在電腦上選定位置的根CA證書。

這顯示PEM格式證書。儲存以備以後使用。

-----BEGIN CERTIFICATE-----

MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBMRUwEwYKcZImiZPyLQGBGRYFbG9jYWwxFTATBgo.
vcjEhMB8GA1UEAxMYcmF6b3ItV0lOLUzU0tGSIFENko3LUNBMB4XDTIxMDMyMjE0NDMxNVowUTEVMBM0
BWxvY2FsMRUwEwYKcZImiZPyLQGBGRYFcmF6b3IxITAfBgNVBAMTGHEm9yLVdJTl1FM1NLRkpRRDZKNy1DQTCCASlwDQYJKoZIhvc.
CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnblxwtXOB2G4UxZ3LRrWznjXaS02Rc3qVw4lnOaziGs4ZMNM1X8UWeKuwi8QZQlJ.
9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU3OaiiI/tp422ydy3KgI7Iqt1s4XqpZmTezykWra7dUyXfkuESk6lEOAV+zNxfBj3Q9NzP

```
CSkTQTRXYryy8dJrWjAF/n6A3VnS/17UhuJlx4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPf0Ijehh+tZk3bxpoxTDXECaWEEAAaNRME8w
DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFM+DkqQUAOdY379NnViaMIJAVTZ1MBAGCSsGAQQBgicVAQQDAgEAMAOC
AA4IBAQCISm5U7U6Y7zXdx+dleJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7BnO6f/VnF6VGYpXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6qZu
4sMZffbVrGIRz7twWY36J5G5vhNUhzZ1N2OLw6wtHg2SO8XlvpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nrylbBfn0NEX7I
GuDsepY7/u2uWfy/vpTJigeok2DH6HFfOET3sE+7rsIAY+of0kWW5gNwQ4hOwv4Goqj+YQRAXXi2OZyltHR1dfUUbwVENSFQtDnFA7X
-----END CERTIFICATE-----
```

在LDAP伺服器上的本地電腦儲存中安裝多個證書的情況下（可選）

1. 在LDAPS可以使用多個身份證書的情況下，當使用哪個身份證書存在不確定性，或者無法訪問LDAPS伺服器時，仍然可以從在FTD上完成的資料包捕獲中提取根CA。

2. 如果在LDAP伺服器（如AD DS域控制器）本地電腦證書儲存中有多個對伺服器身份驗證有效的證書，則可以注意到，不同的證書用於LDAPS通訊。解決此類問題的最佳方法是從本地電腦證書儲存中刪除所有不必要的證書，並且僅具有一個對伺服器身份驗證有效的證書。

但是，如果有正當理由需要兩個或更多證書並且至少具有一個Windows Server 2008 LDAP伺服器，則Active Directory域服務(NTDS\Personal)證書儲存區可用於LDAP通訊。

以下步驟演示如何從域控制器本地電腦證書儲存匯出啟用LDAPS的證書到Active Directory域服務證書儲存(NTDS\Personal)。

•

導航到Active Directory伺服器上的MMC控制檯，選擇檔案，然後按一下Add/Remove Snap-in。

•

按一下Certificates，然後按一下Add。

•

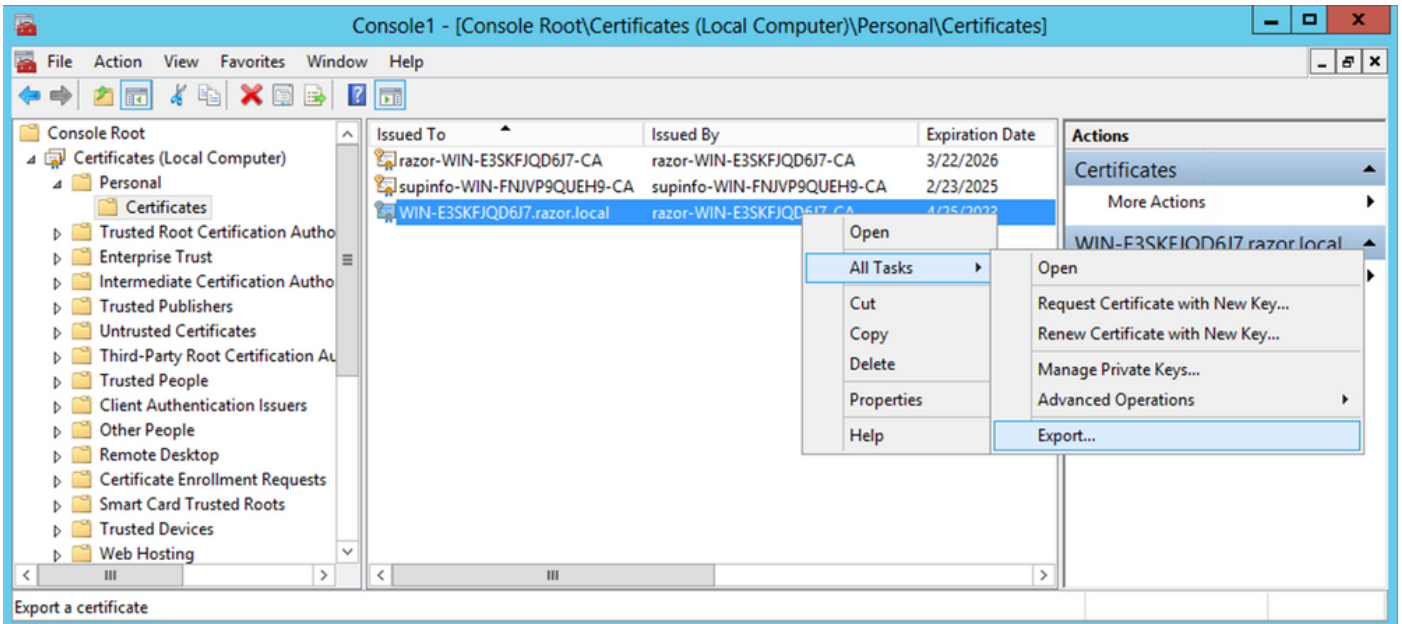
在中Certificates snap-in，選擇Computer account，然後按一下Next。

•

在Select Computer，選擇Local Computer，按一下OK，然後按一下Finish。在Add or Remove Snap-ins中，按一下OK。

•

在包含用於伺服器身份驗證的證書的電腦證書控制檯中，按一下右鍵certificate，按一下All Tasks，然後按一下Export。

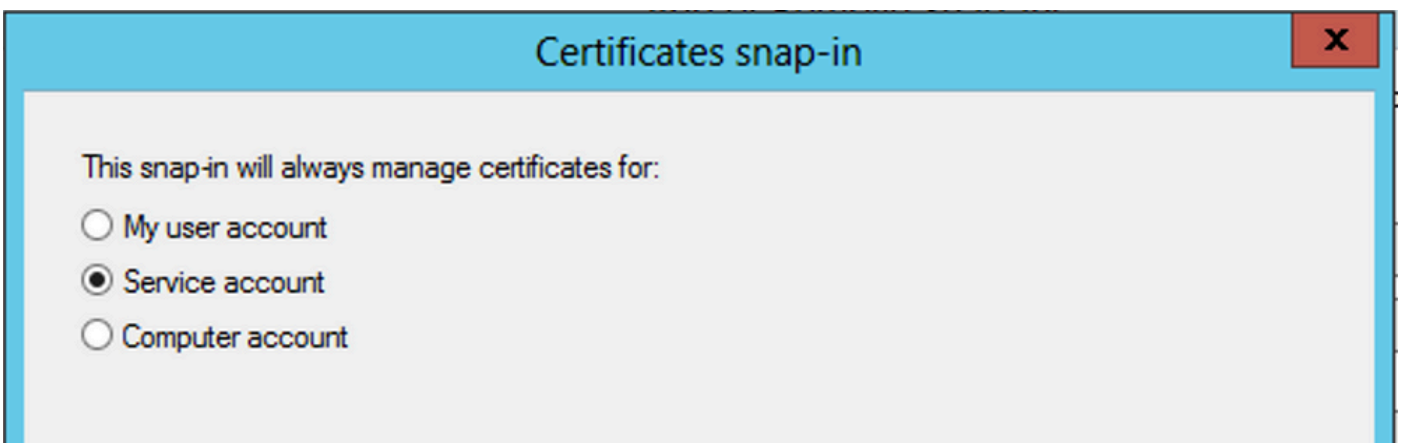


- 在後續部分中pfx,以格式匯出證書。有關如何從MMC匯出格式證書的文章pfx，請參閱以下文章:

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

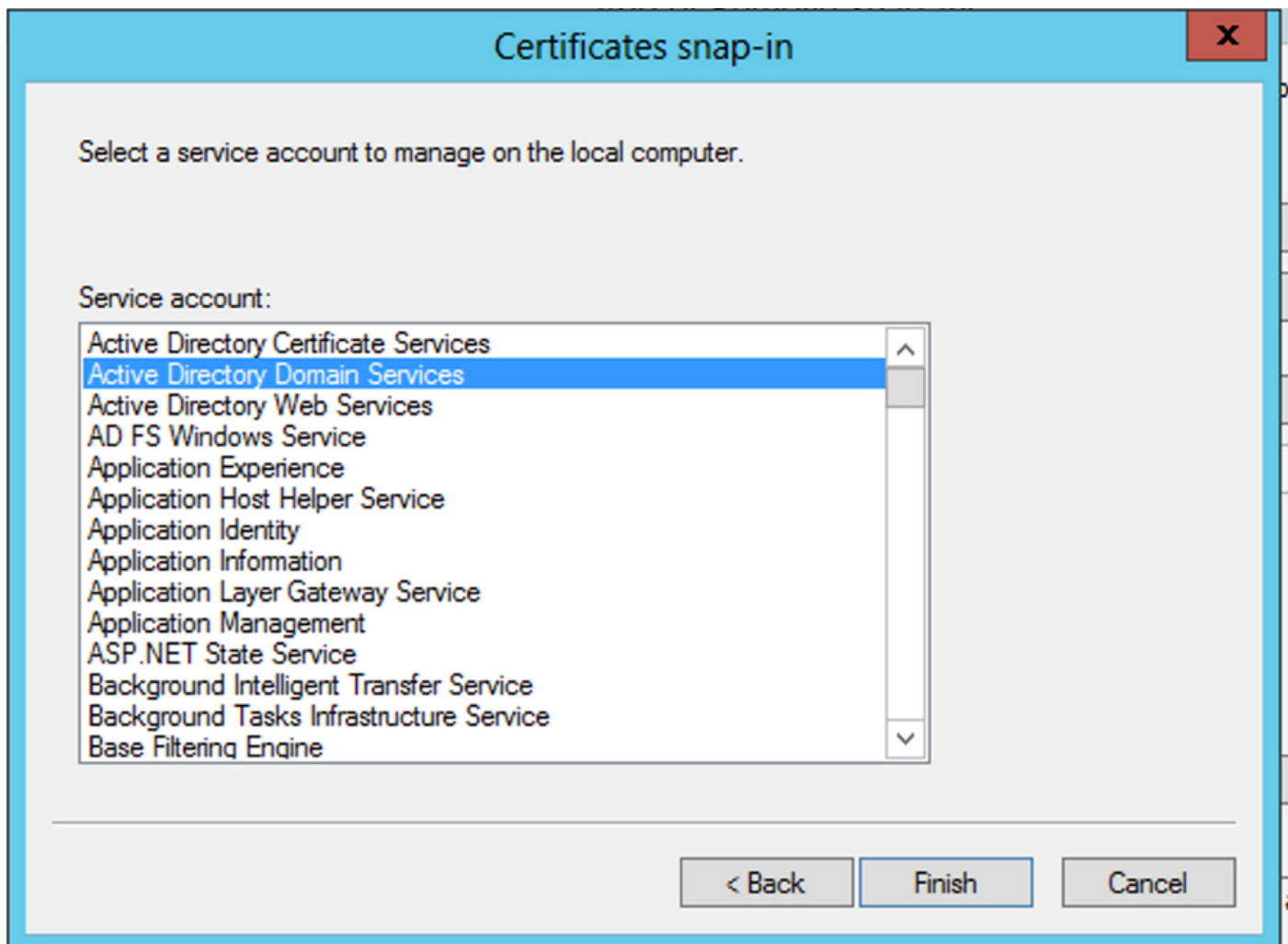
- 匯出憑證後，導覽至Add/Remove Snap-in onMMC console。按一下Certificates，然後按一下Add。

- 選擇Service account，然後按一下Next。



•
在對話Select Computer框中，選擇Local Computer，然後按一下Next。

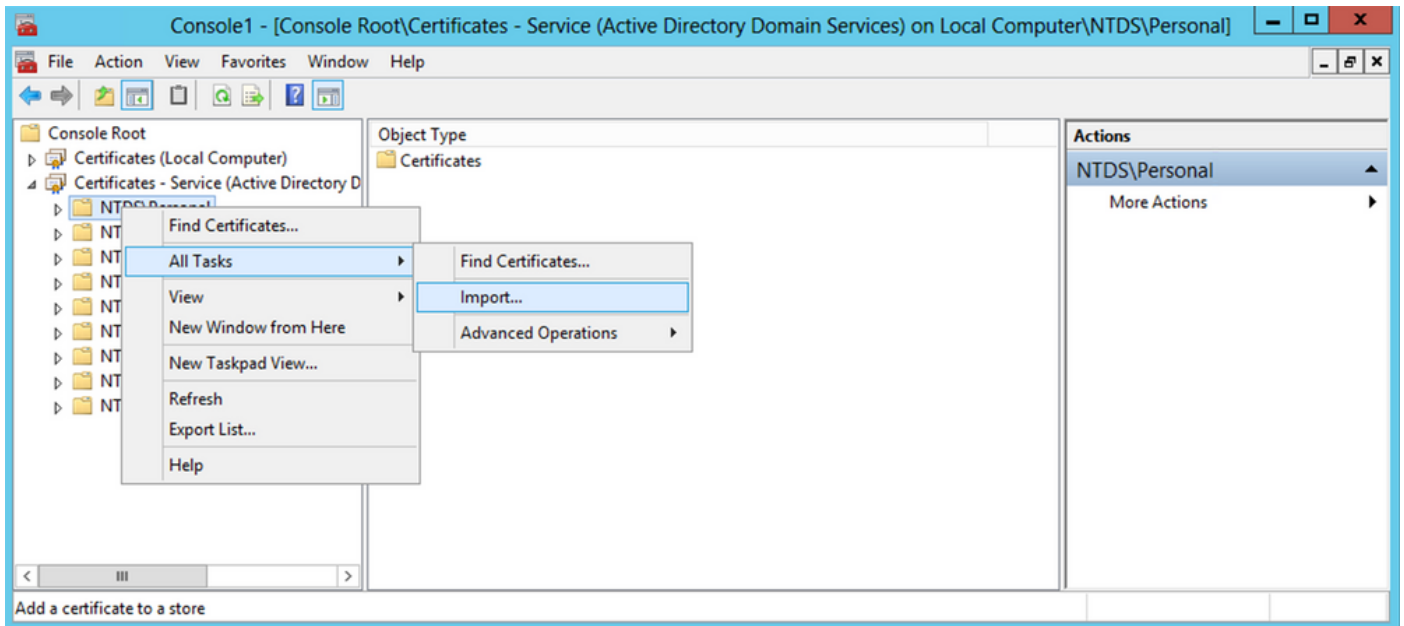
•
選擇Active Directory Domain Services，然後按一下Finish。



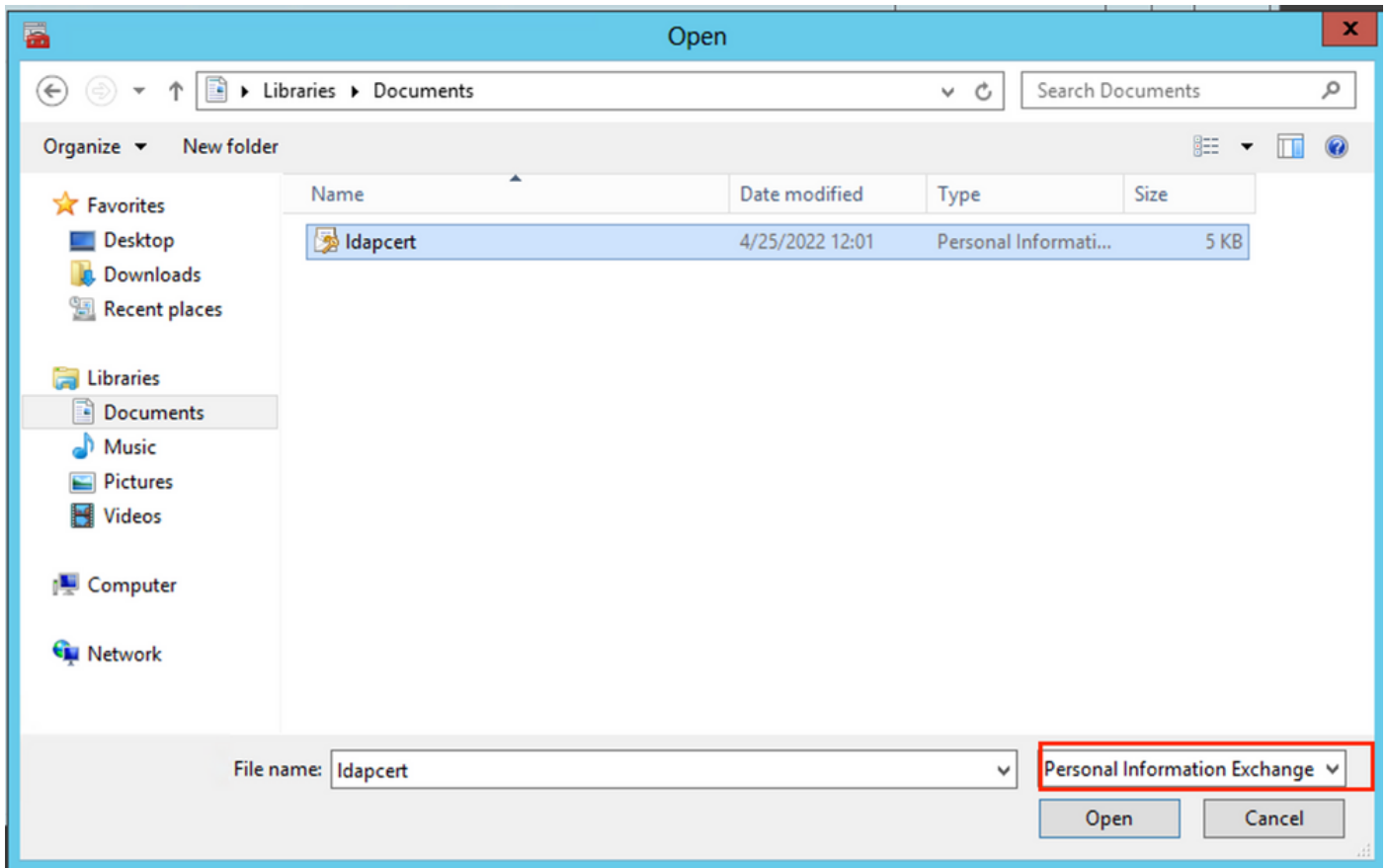
•
在對話Add/Remove Snap-ins框中，按一下OK。

•
展開Certificates - Services (Active Directory Domain Services)，然後按一下NTDS\Personal。

按一下右鍵NTDS\Personal，按一下All Tasks，然後按一下Import。



- 在歡迎螢幕Certificate Import Wizard，按一下Next。
- 在「File to Import (要匯入的檔案)」螢幕上，按一下Browse，然後找到您之前匯出的證書檔案。
- 在「開啟」螢幕上，確保選擇「個人資訊交換」(*pfx,*p12)作為檔案型別，然後導航到檔案系統以找到先前匯出的證書。然後，按一下該證書。



-

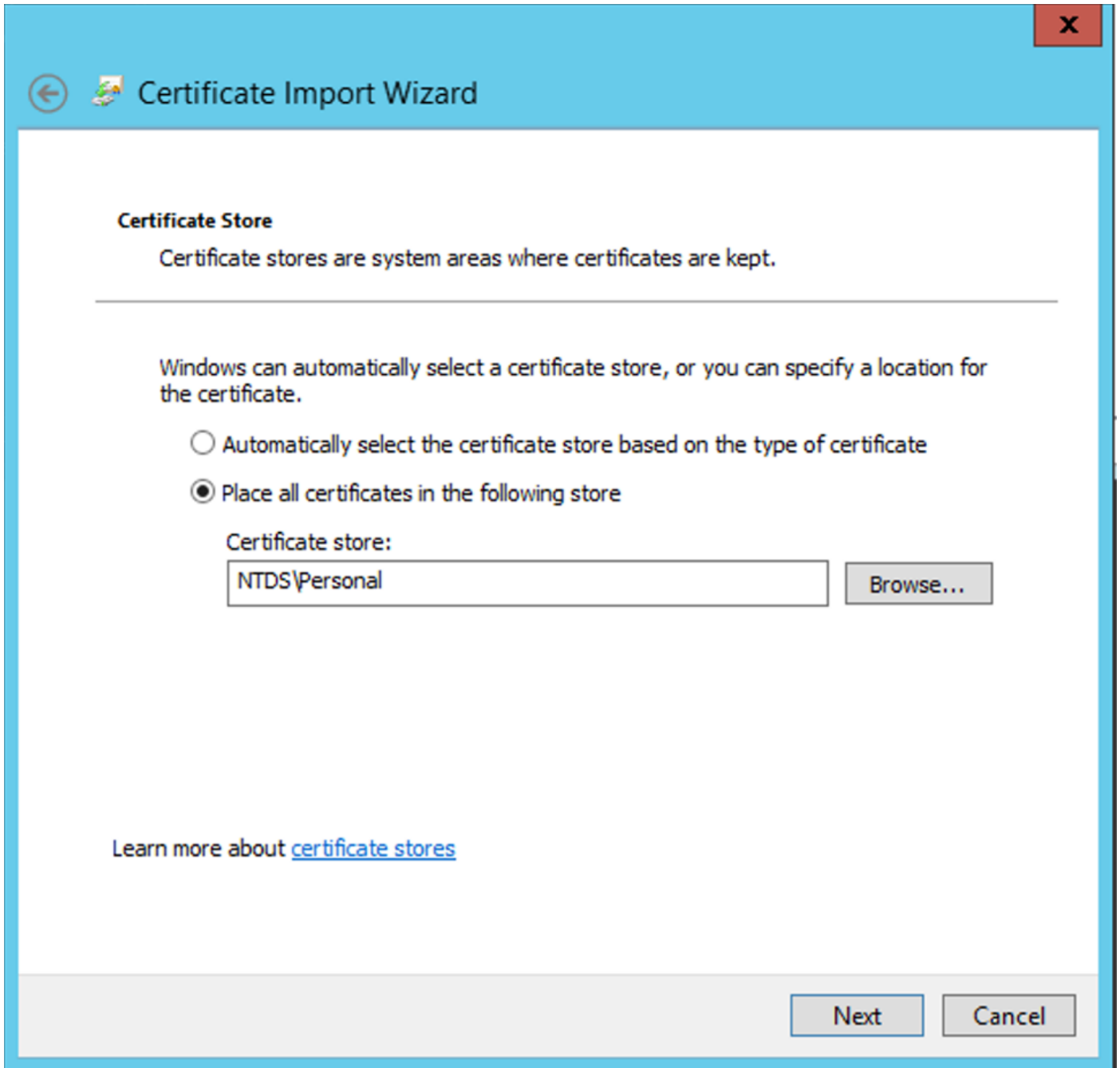
按一下Open，然後按一下Next。

-

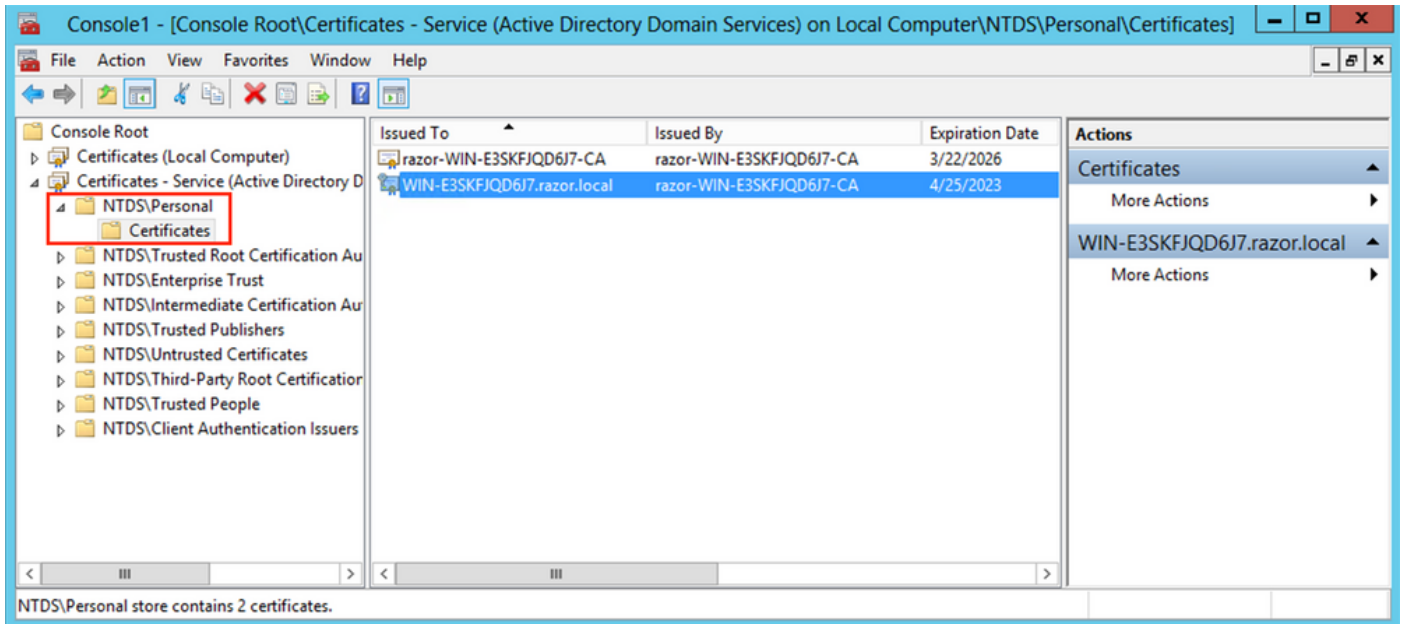
在「密碼」螢幕上，輸入為檔案設定的密碼，然後按一下Next。

-

在「證書儲存」頁面上，確保選中「放置所有證書」，然後閱讀「證書儲存：NTDS\Personal」，然後按一下Next。



•
在完成螢幕上Certificate Import Wizard，按一下Finish。然後您會看到一條消息，說明匯入成功。按一下OK。您會看到證書已匯入到證書儲存區：NTDS\Personal。



FMC配置

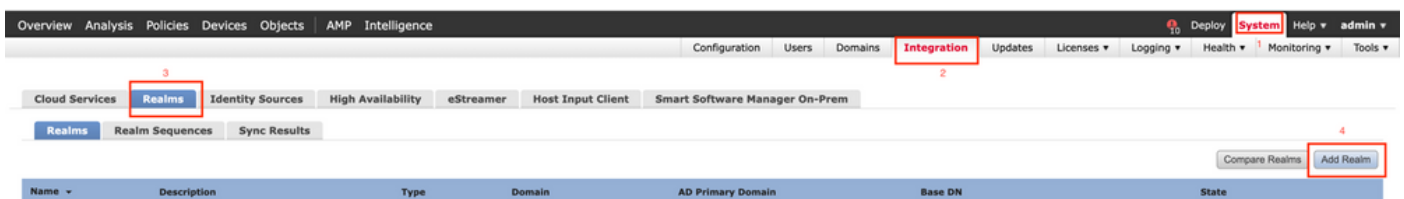
驗證許可

為了部署AnyConnect配置，必須在智慧許可伺服器上註冊FTD，並且必須向裝置應用有效的Plus、Apex或VPN許可證。

設定領域

-

導航至System > Integration。導覽至Realms，然後按一下Add Realm，如下圖所示：



-

根據從Microsoft Server for LDAP收集的資訊填寫顯示的欄位。在此之前，請匯入根CA證書，該證書已在下面的Windows伺服器上的LDAP服務證書上簽名Objects > PKI > Trusted CAs > Add Trusted CA，因為在「領域」下Directory Server Configuration 會引用該證書。完成後，按一下OK。

- > 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
 - Prefix List

Trusted CAs

Add Trusted CA

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) FA tanA2sAtvAry, ...	
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, ...	

Edit Trusted Certificate Authority

Name:

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

Add New Realm



Name*

LDAP-Server

Description

Type

LDAP

Directory Username*

Administrator@razor.local

E.g. user@domain.com

Directory Password*

.....

Base DN*

DC=razor,DC=local

E.g. ou=group,dc=cisco,dc=com

Group DN*

DC=razor,DC=local

E.g. ou=group,dc=cisco,dc=com

Directory Server Configuration

^ WIN-E3SKFJQD6J7.razor.local:636

Hostname/IP Address*

WIN-E3SKFJQD6J7.razor.local

Port*

636

Encryption

LDAPS

CA Certificate*

LDAPS-ROOT-CERT

Interface used to connect to Directory server ⓘ

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface

Test

[Add another directory.](#)

.

按一下Test，確保FMC能夠使用先前步驟中提供的目錄使用者名稱和密碼成功繫結。由於這些測試是從FMC啟動的，而不是通過FTD上配置的某個可路由介面（如內部、外部、dmz），因此成功（或失敗）的連線不能保證AnyConnect身份驗證的相同

結果，因為AnyConnect LDAP身份驗證請求是從FTD可路由介面之一啟動的。

Add Directory ? X

Hostname/IP Address*	Port*
<input type="text" value="WIN-E3SKFJQD6J7.razor.local"/>	<input type="text" value="636"/>
Encryption	CA Certificate*
<input type="text" value="LDAPS"/>	<input type="text" value="LDAPS-ROOT-CERT"/> +

Interface used to connect to Directory server i

Resolve via route lookup

Choose an interface

✔ Test connection succeeded

啟用新領域。

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains **Integration** Updates Licenses Logging Health Monitoring Tools

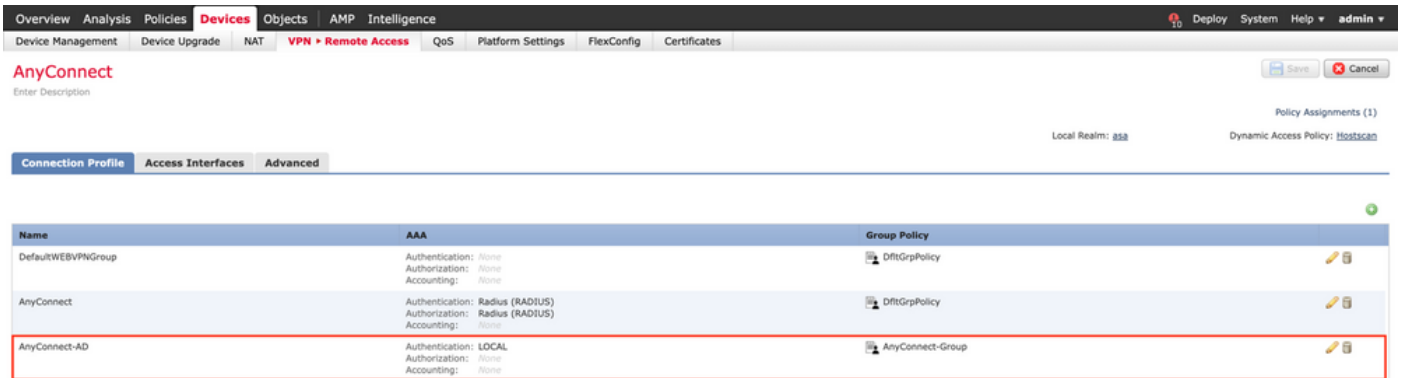
Cloud Services **Realms** Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Realms Realm Sequences Sync Results Compare Realms Add Realm

Name	Description	Type	Domain	AD Primary Domain	Base DN	State
AC-Local		LOCAL	Global			Enabled
LDAP		AD	Global	cisco01.com	OU=Users,OU=CISCO,DC=cisco01,DC=com	Enabled
LDAP-Server		AD	Global	razor.local	DC=razor,DC=local	Enabled

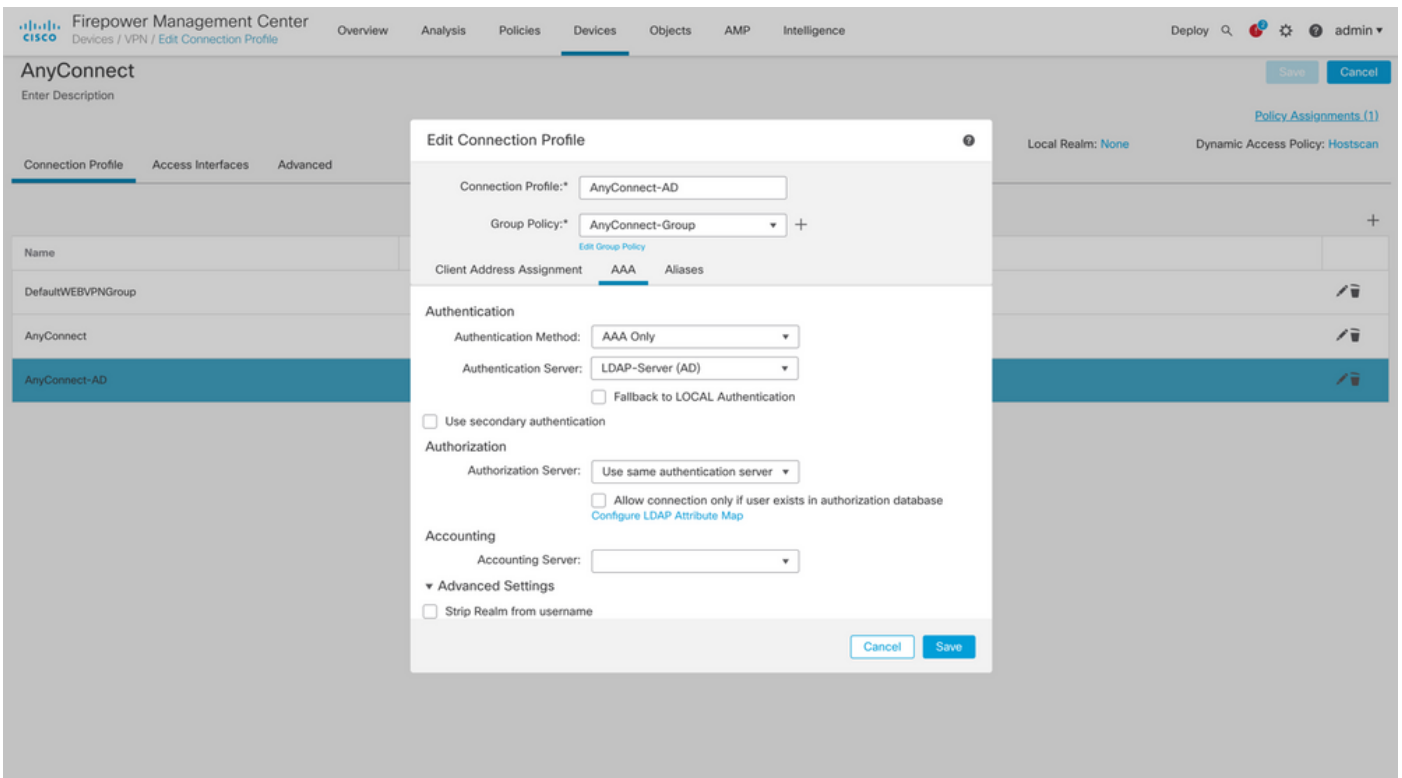
配置AnyConnect進行密碼管理

選擇現有的連線配置檔案，或建立一個新的連線配置檔案（如果是AnyConnect的初始設定）。此處使用與本地身份驗證對映的名為「AnyConnect-AD」的現有連線配置檔案。



Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
AnyConnect	Authentication: Radius (RADIUS) Authorization: Radius (RADIUS) Accounting: None	DfltGrpPolicy
AnyConnect-AD	Authentication: LOCAL Authorization: None Accounting: None	AnyConnect-Group

在連線配置檔案的AAA設定下，編輯連線配置檔案並對映在前面步驟中配置的新LDAP伺服器。完成後Save，按一下右上角。



Firepower Management Center
Devices / VPN / Edit Connection Profile

AnyConnect
Enter Description

Connection Profile: AnyConnect-AD
Group Policy: AnyConnect-Group

Client Address Assignment: AAA

Authentication
Authentication Method: AAA Only
Authentication Server: LDAP-Server (AD)
 Fallback to LOCAL Authentication
 Use secondary authentication

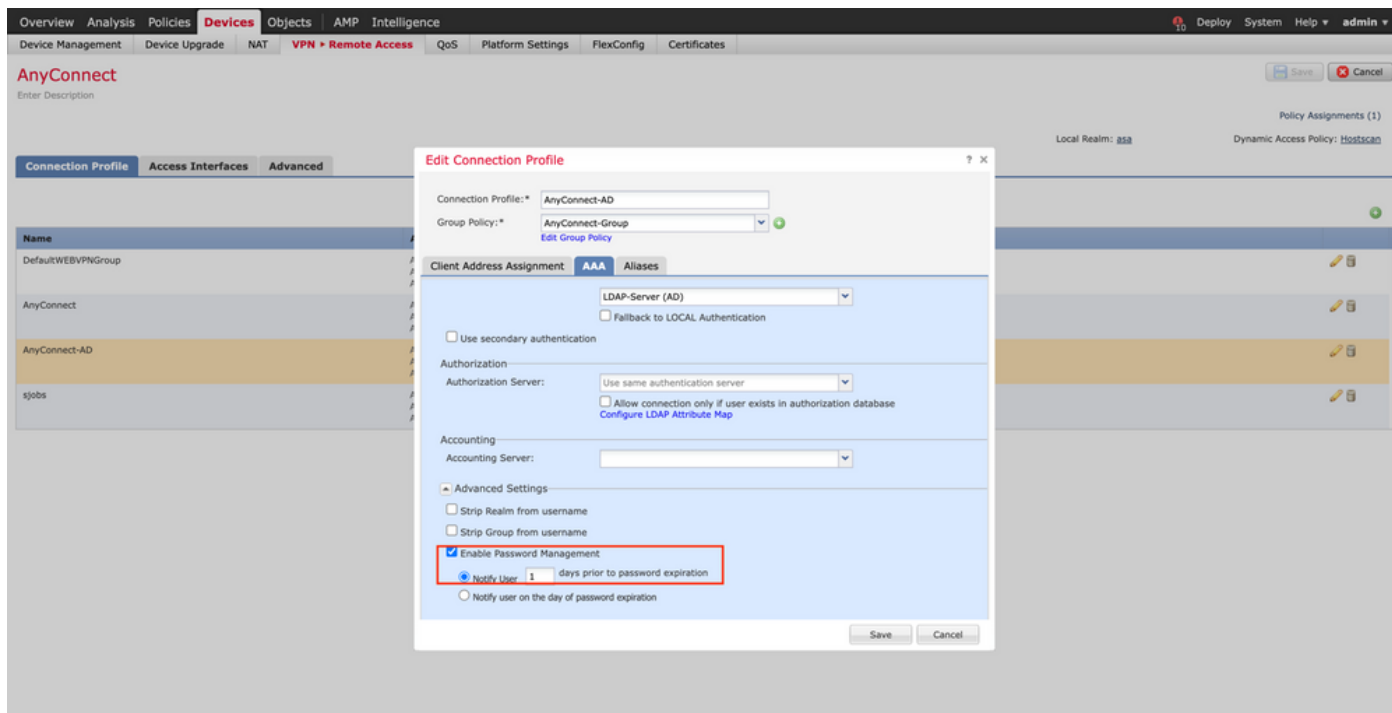
Authorization
Authorization Server: Use same authentication server
 Allow connection only if user exists in authorization database
[Configure LDAP Attribute Map](#)

Accounting
Accounting Server:

Advanced Settings
 Strip Realm from username

Buttons: Cancel, Save

在下啟用密碼管理AAA > Advanced Settings，並儲存配置。

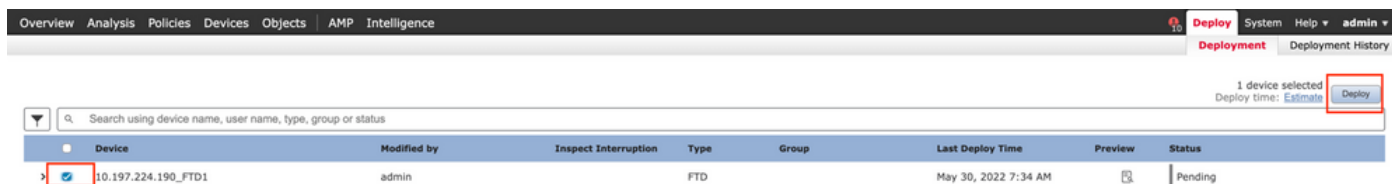


部署

完成所有配置後Deploy，按一下右上角的按鈕。



按一下應用於它的FTD設定旁邊的擷取方塊，然後按一下Deploy，如下圖所示：



最終配置

這是成功部署後FTD CLI中看到的組態。

AAA組態

```
<#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 Server

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
```

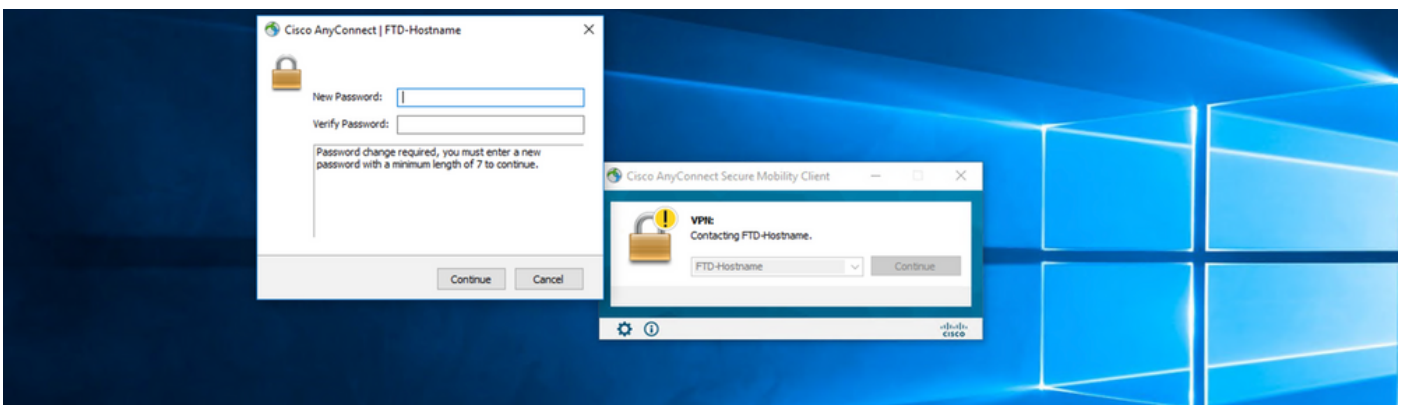
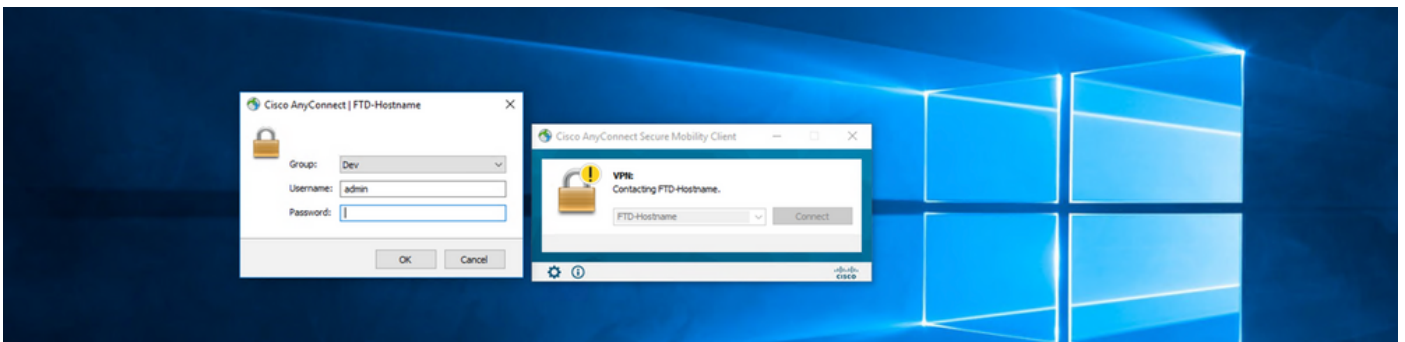
```
ssl trust-point ID-New-Cert Outside
```

```
<----- FTD ID-cert trustpoint name mapped to the outside interface on which AnyConnect Connections
```

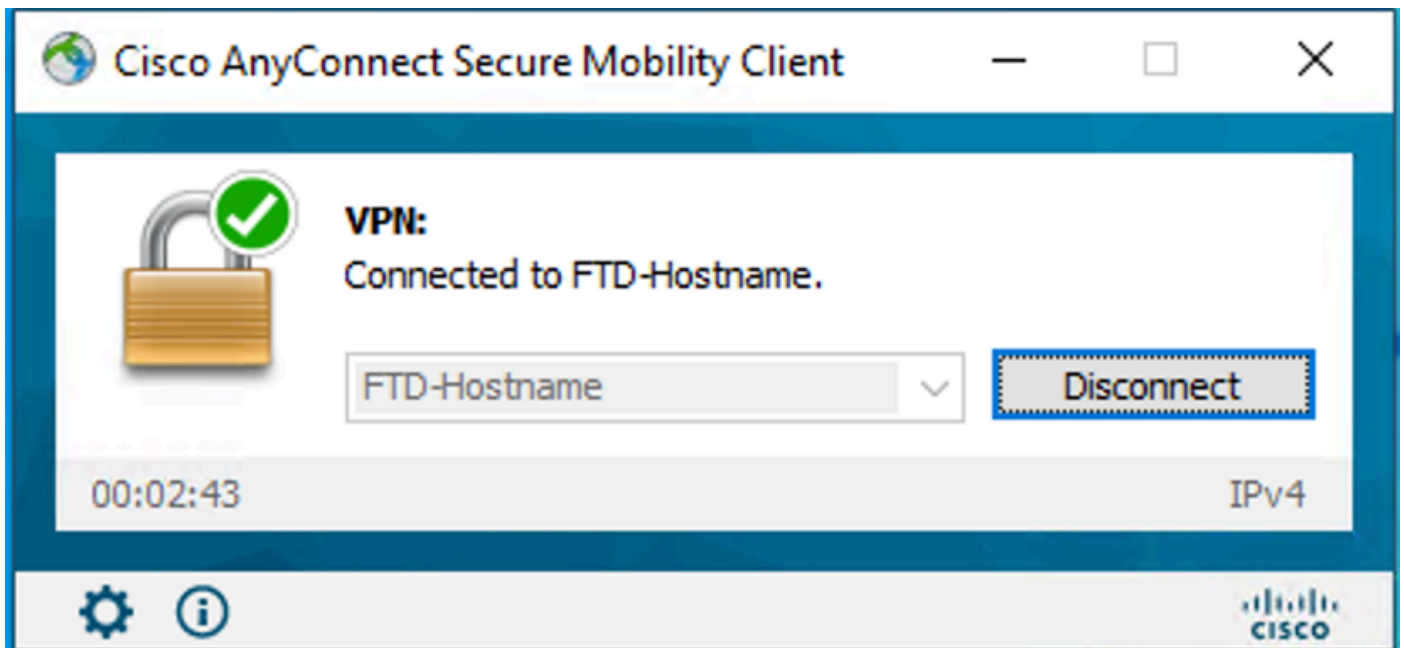
驗證

使用AnyConnect連線並驗證使用者連線的密碼管理過程

1. 啟動到相關連線配置檔案的連線。初次登入時確定必須更改密碼後，Microsoft Server在密碼到期時拒絕了該較早的密碼，系統將提示使用者更改密碼。



使用者輸入登入新密碼後，連線成功建立。



•
在FTD CLI上驗證使用者連線：

```
<#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

疑難排解

調試

此調試可以在診斷CLI中運行，以便解決與密碼管理相關的問題：`debug ldap 255`。

正在處理的密碼管理調試

<#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:

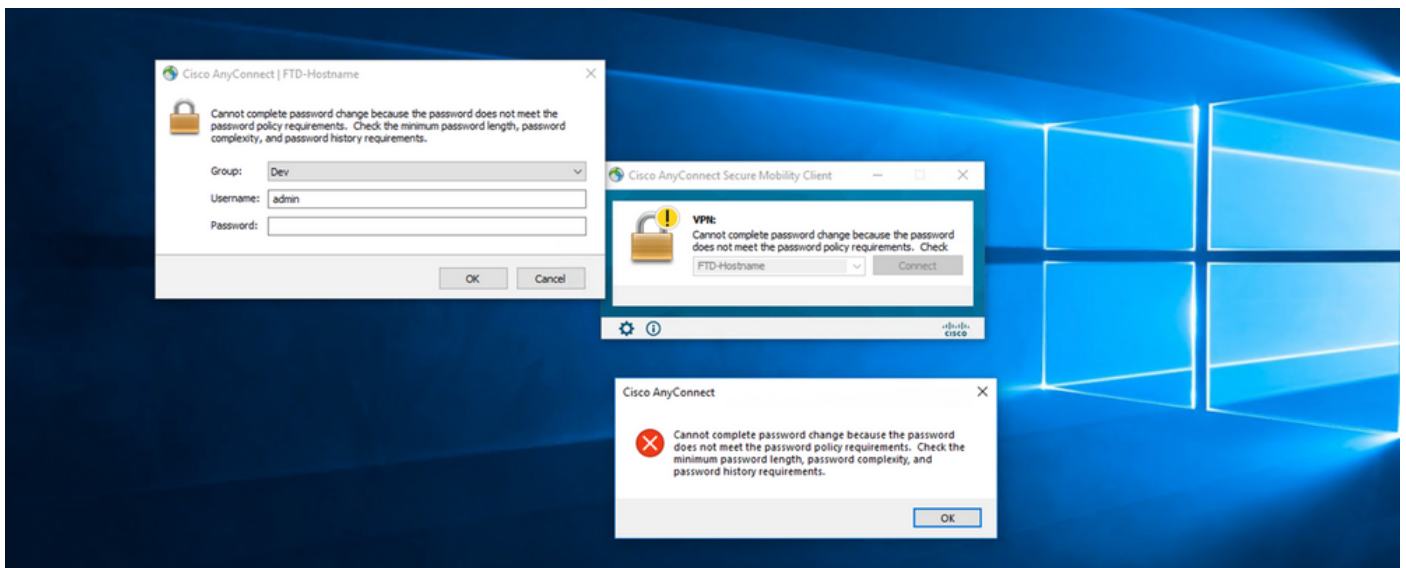
- [25] objectClass: value = top
- [25] objectClass: value = person
- [25] objectClass: value = organizationalPerson

[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

密碼管理過程中遇到的常見錯誤

通常，如果在使用者提供新密碼期間未滿足Microsoft Server設定的密碼策略，連線將終止，並出現錯誤「Password does the Password Policy Requirements」。因此，請確保新密碼符合Microsoft Server為LDAP設定的策略。



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。