شكلت كلمة إدارة يستعمل LDAPs ل RA VPN على FTD يدار ب FMC

المحتويات

المقدمة

يصف هذا المستند تكوين إدارة كلمة المرور باستخدام LDAPs لعملاء AnyConnect الذين يتصلون ب Cisco Firepower Threat Defense (FTD).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- معرفة أساسية بتكوين شبكة RA VPN (شبكة الوصول عن بعد الخاصة الظاهرية) على FMC

- معرفة أساسية بتكوين خادم LDAP على FMC
- معرفة أساسية ب Active Directory

المكونات المستخدمة

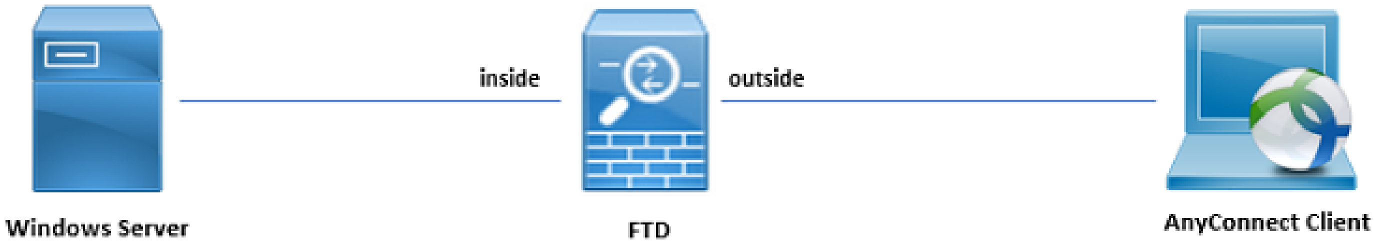
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- خادم Microsoft 2012 R2
- تشغيل FMCv 7.3.0
- تشغيل FTDv 7.3.0

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة والسيناريو



تم تكوين خادم Windows مسبقا باستخدام ADD و ADCS لاختبار عملية إدارة كلمة مرور المستخدم. في دليل التكوين هذا، يتم إنشاء حسابات المستخدمين هذه.

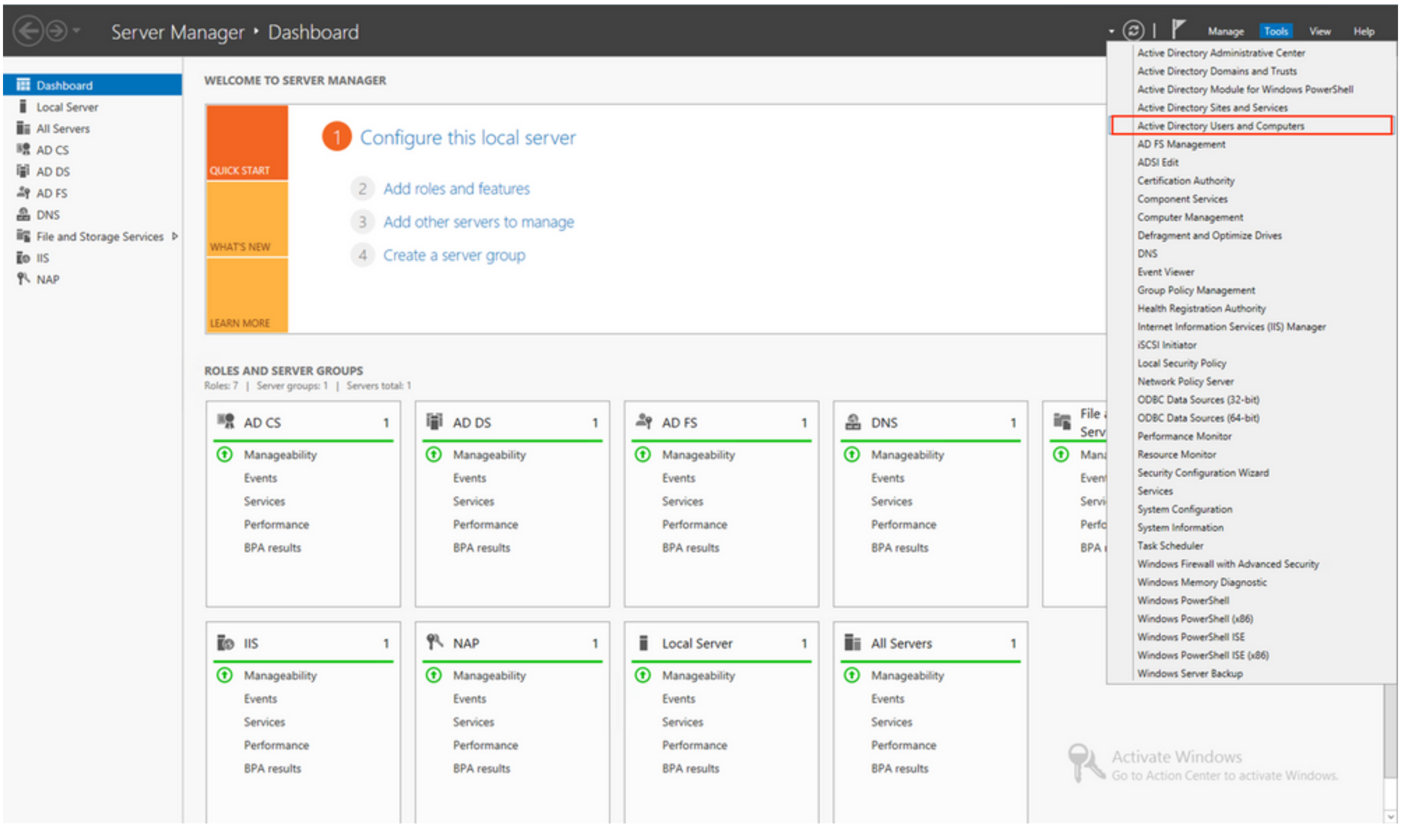
حسابات المستخدمين:

- المسؤول: يتم إستخدام هذا الحساب كحساب دليل للسماح ل FTD بالارتباط بخادم Active Directory.

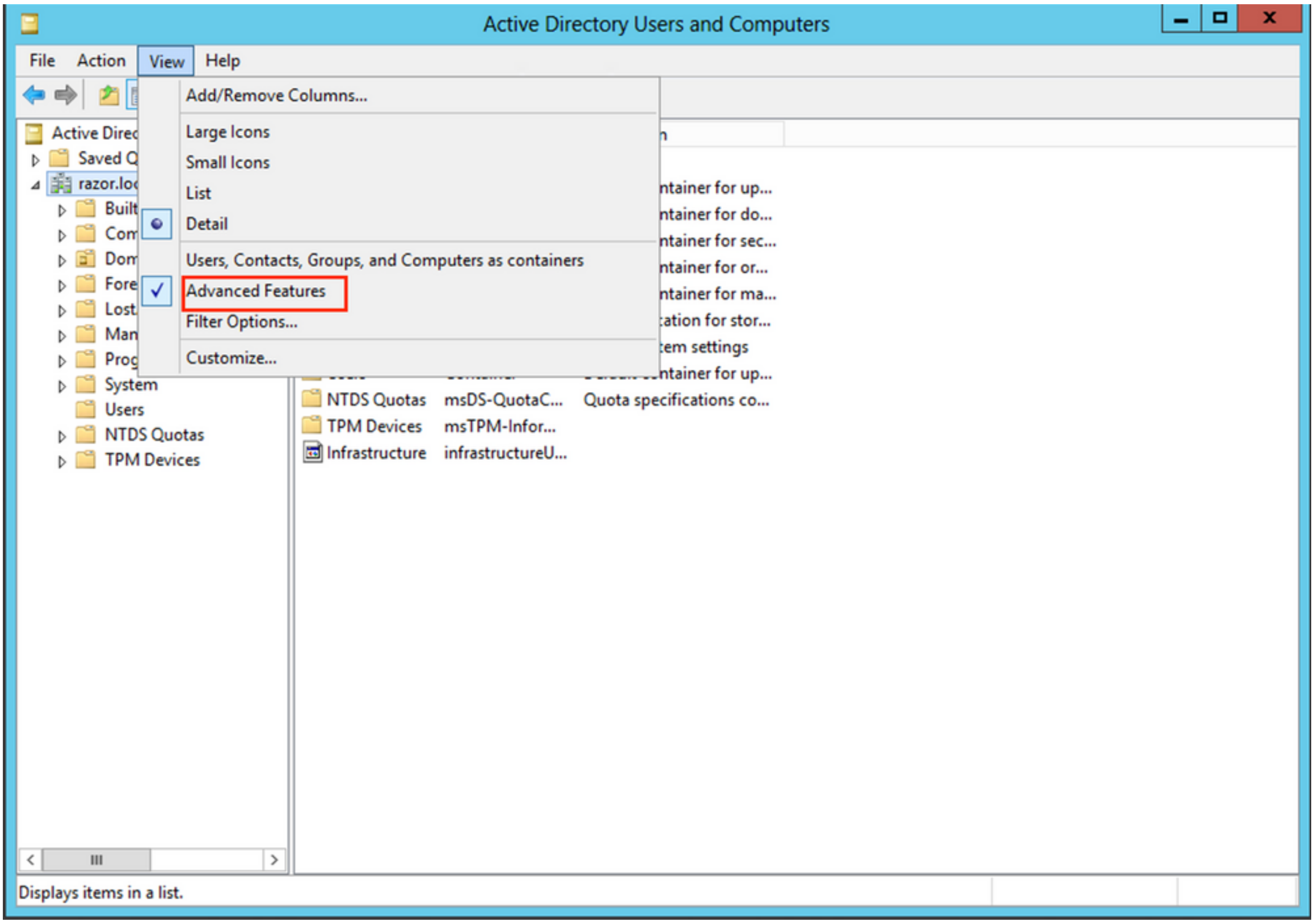
- admin: حساب مسؤول إختبار يستخدم لإظهار هوية المستخدم.

تحديد LDAP DN الأساسي و DN للمجموعة

1. فتح Active Directory Users and Computers من خلال لوحة معلومات إدارة الخادم.

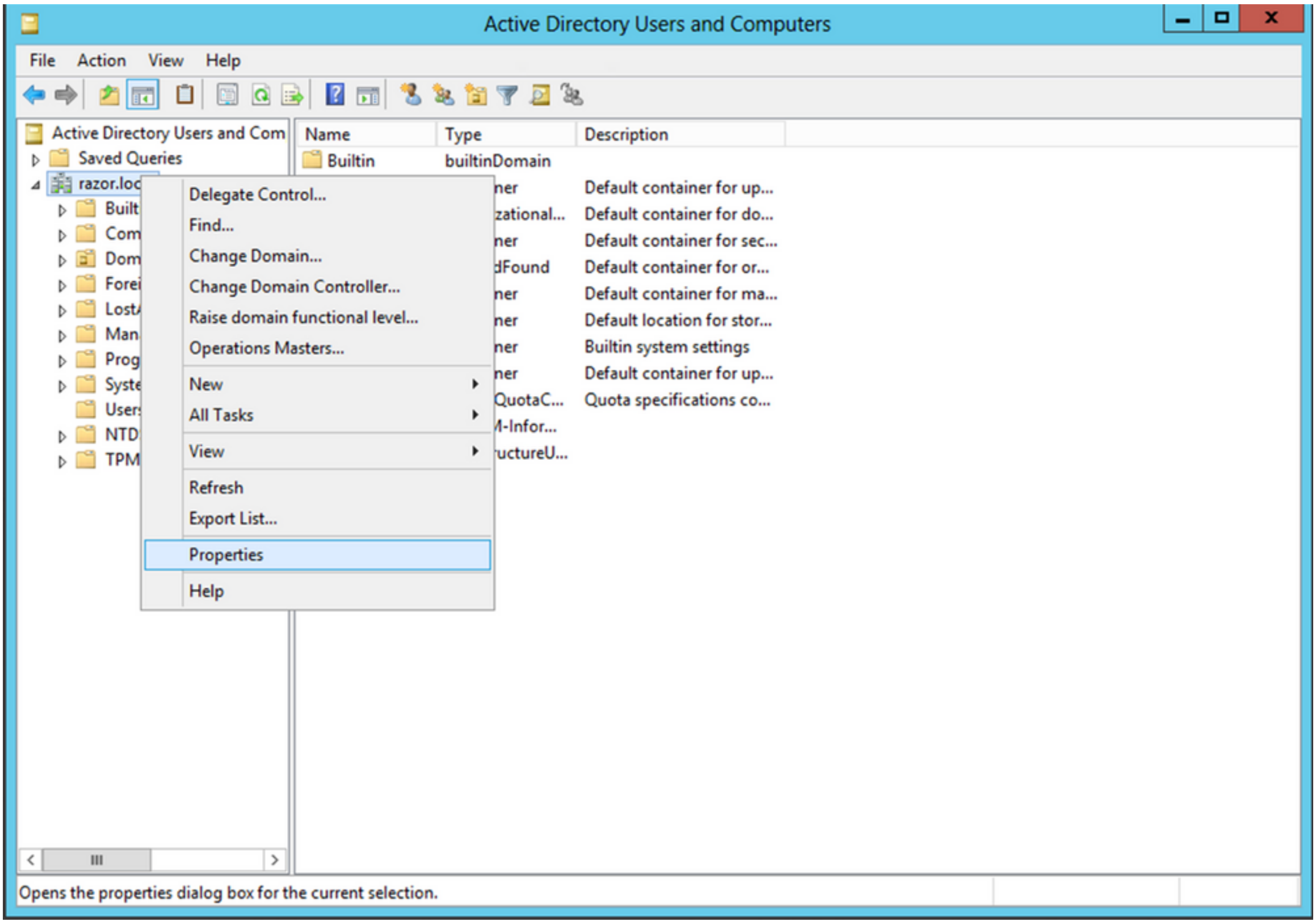

Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD CS
AD DS
AD FS
DNS
File and Storage Services
IIS
NAP
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
ROLES AND SERVER GROUPS
Roles: 7 | Server groups: 1 | Servers total: 1
AD CS 1
AD DS 1
AD FS 1
DNS 1
IIS 1
NAP 1
Local Server 1
All Servers 1
Manageability
Events
Services
Performance
BPA results
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
Health Registration Authority
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Network Policy Server
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
Activate Windows
Go to Action Center to activate Windows.

افتح View Option اللوحة في الأعلى، وقم بإتاحة Advanced Features، كما هو موضح في الصورة:



-

يتيح ذلك عرض الخصائص الإضافية تحت كائنات AD.
على سبيل المثال، للعثور على شبكة DN الخاصة بالجذر razor.local، انقر بزر الماوس الأيمن فوق razor.local، ثم أختر Properties، كما هو موضح في هذه الصورة:


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
razor.loc
Built
Com
Dom
Forei
Lost
Man
Prog
Syste
Users
NTD
TPM
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
View
Refresh
Export List...
Properties
Help
Name
Type
Description
Builtin
builtinDomain
ner
zational...
ner
dFound
ner
ner
ner
ner
QuotaC...
M-Infor...
uctureU...
Default container for up...
Default container for do...
Default container for sec...
Default container for or...
Default container for ma...
Default location for stor...
Builtin system settings
Default container for up...
Quota specifications co...

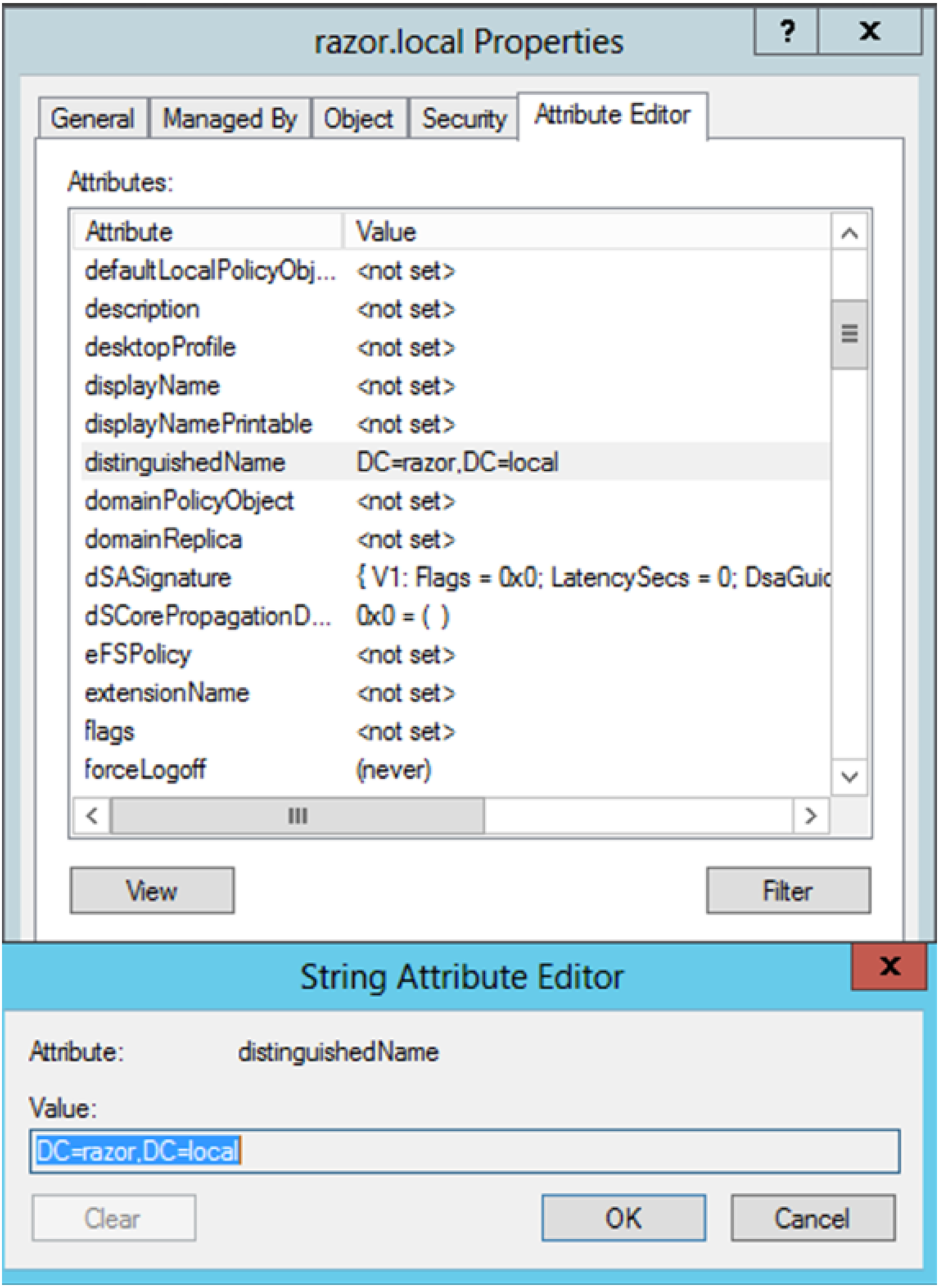
Opens the properties dialog box for the current selection.

-

تحت Properties، أختر Attribute Editor علامة التبويب. ابحث distinguishedName تحت الخصائص، ثم انقر View، كما هو موضح في الصورة.

وهذا يفتح نافذة جديدة حيث يمكن نسخ DN ولصقه في FMC لاحقا.

في هذا المثال، يكون DN الجذر DC=razor، DC=local. انسخ القيمة واحفظها لوقت لاحق. طقطقت OK in order to خرجت الخيط سمة محرر نافذة وطقطقت OK ثانية in order to خرجت الخصائص.



Attributes:

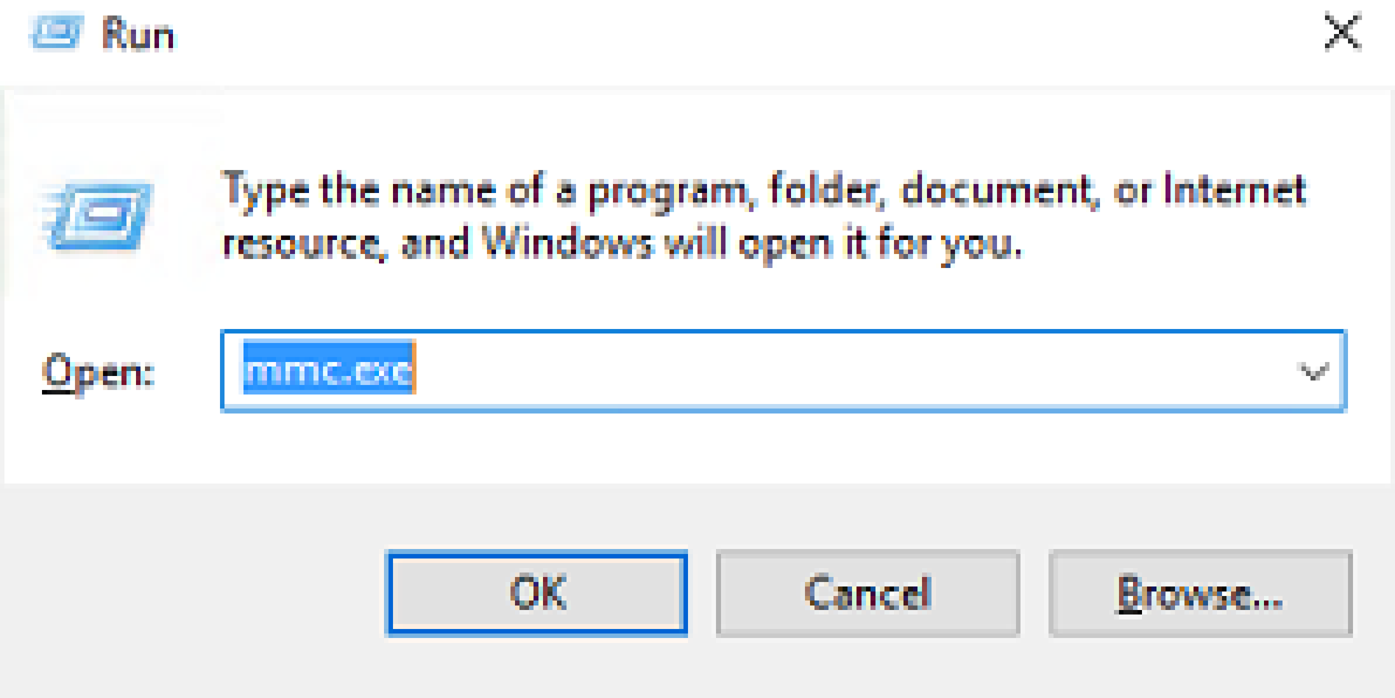
Attribute	Value
defaultLocalPolicyObj...	<not set>
description	<not set>
desktopProfile	<not set>
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	DC=razor,DC=local
domainPolicyObject	<not set>
domainReplica	<not set>
dSASignature	{ V1: Flags = 0x0; LatencySecs = 0; DsaGuic
dSCorePropagationD...	0x0 = ( )
eFSPolicy	<not set>
extensionName	<not set>
flags	<not set>
forceLogoff	(never)

Attribute: distinguishedName

Value: DC=razor,DC=local

نسخ جذر شهادة SSL ل LDAP

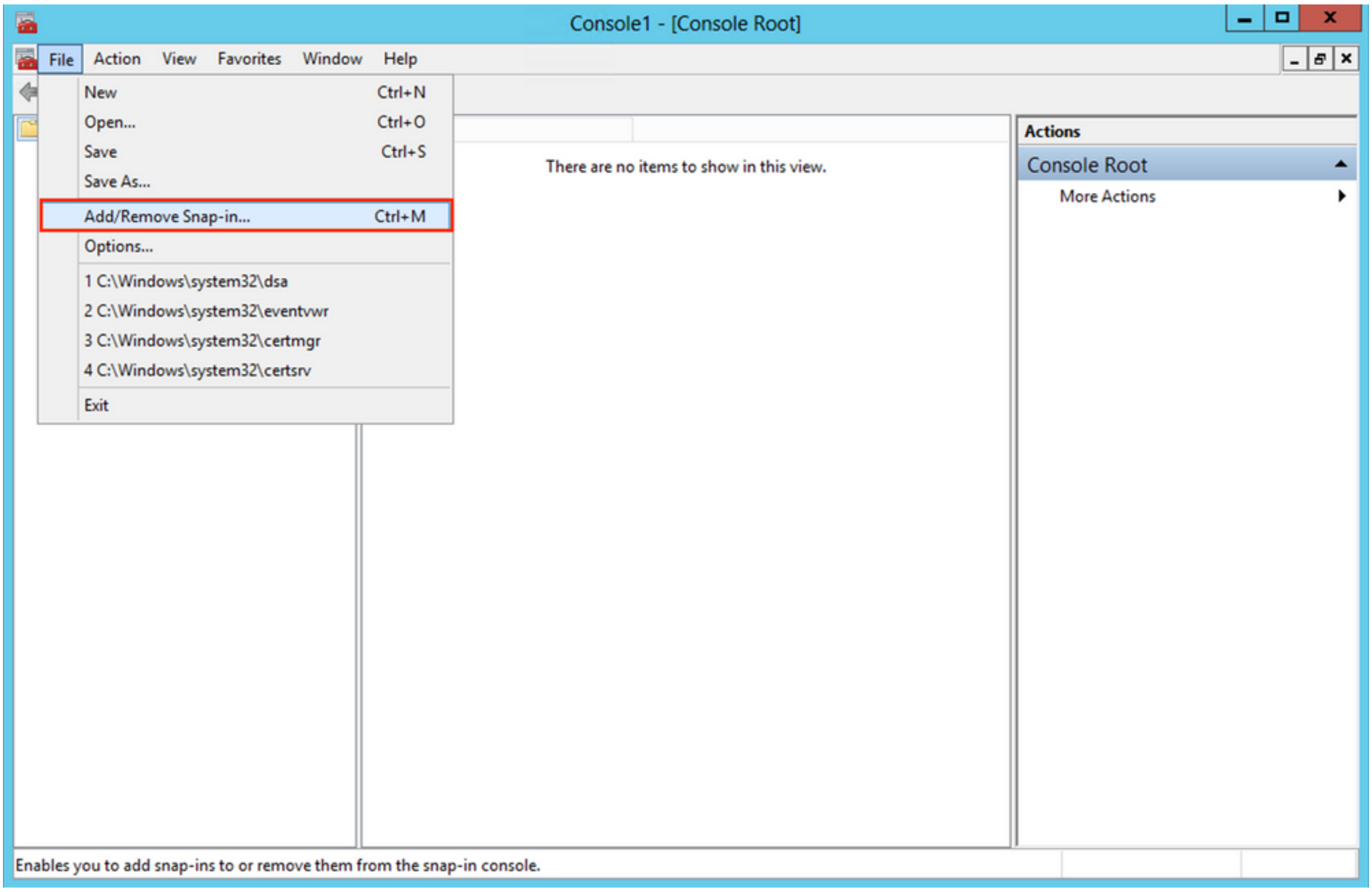
- اضغط Win+R وأدخل mmc.exe، ثم انقر OK، كما هو موضح في هذه الصورة.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc.exe

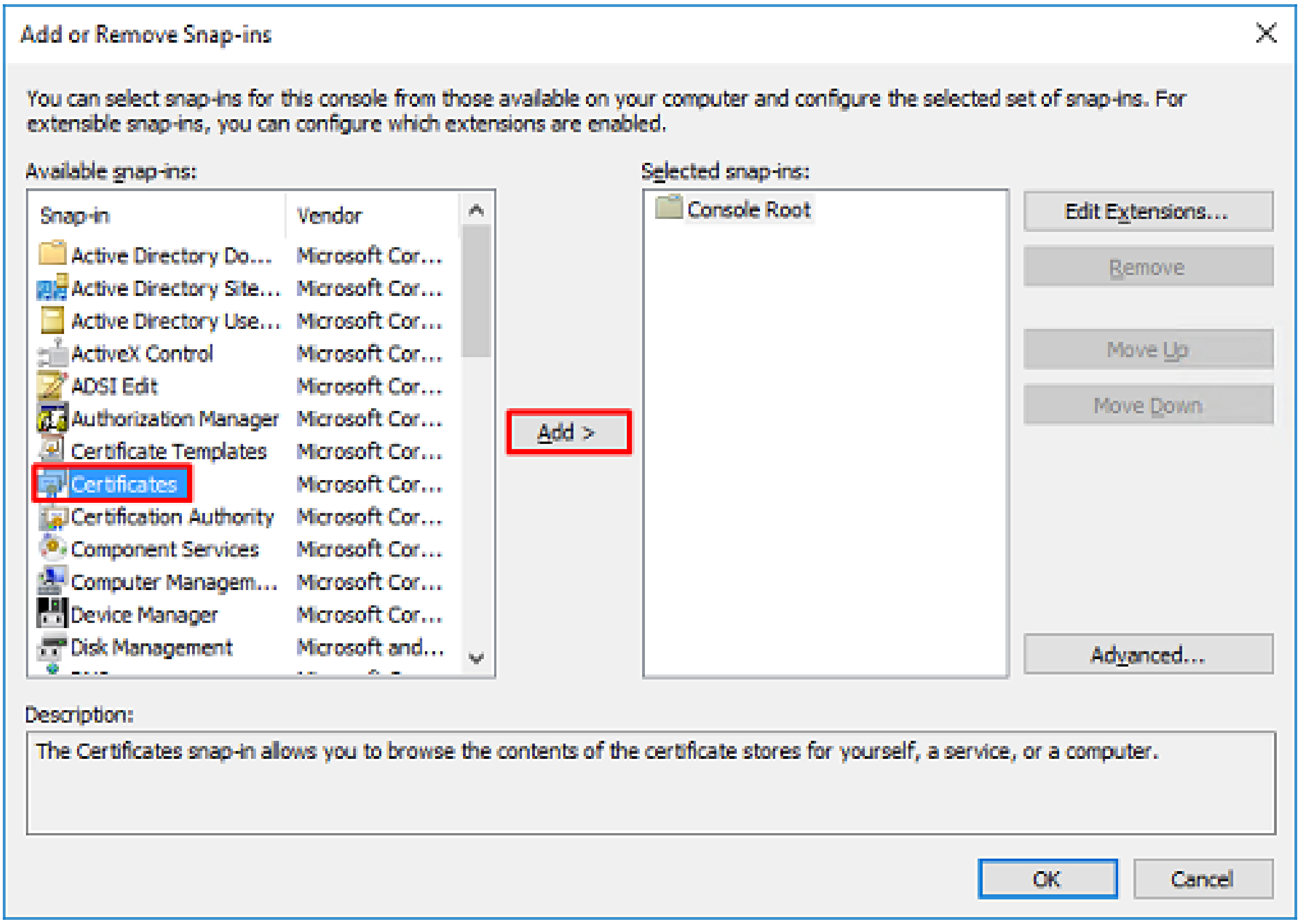
- انتقل إلى File > Add/Remove Snap-in...، كما هو موضح في هذه الصورة:


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\dsa
2 C:\Windows\system32\eventvwr
3 C:\Windows\system32\certmgr
4 C:\Windows\system32\certsrv
Exit
Actions
Console Root
More Actions

There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

- تحت الأدوات الإضافية المتاحة، أختر Certificates ثم انقر Add، كما هو موضح في هذه الصورة:



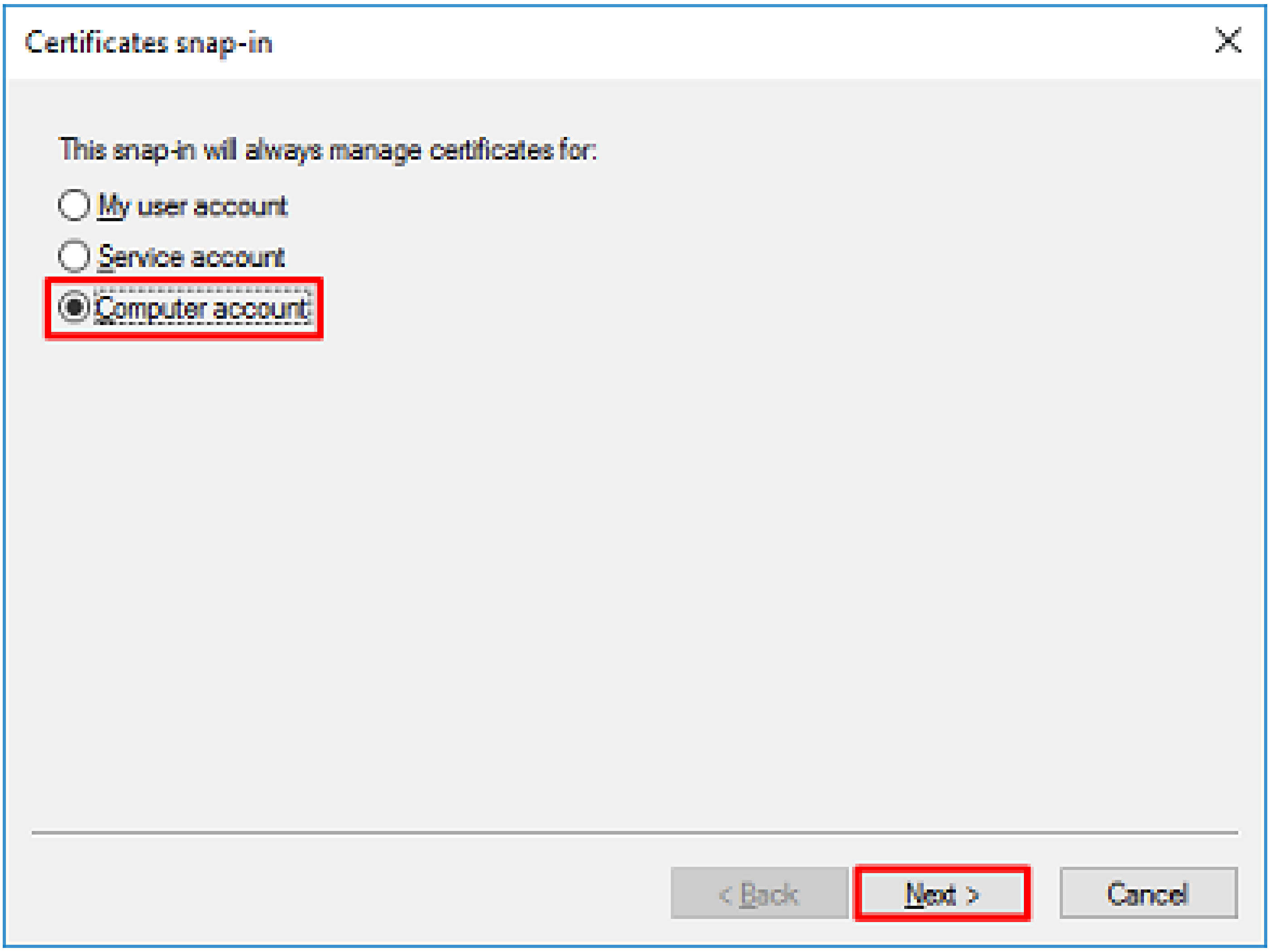
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

-

أختر Computer account ثم انقر Next، كما هو موضح في هذه الصورة:



Certificates snap-in

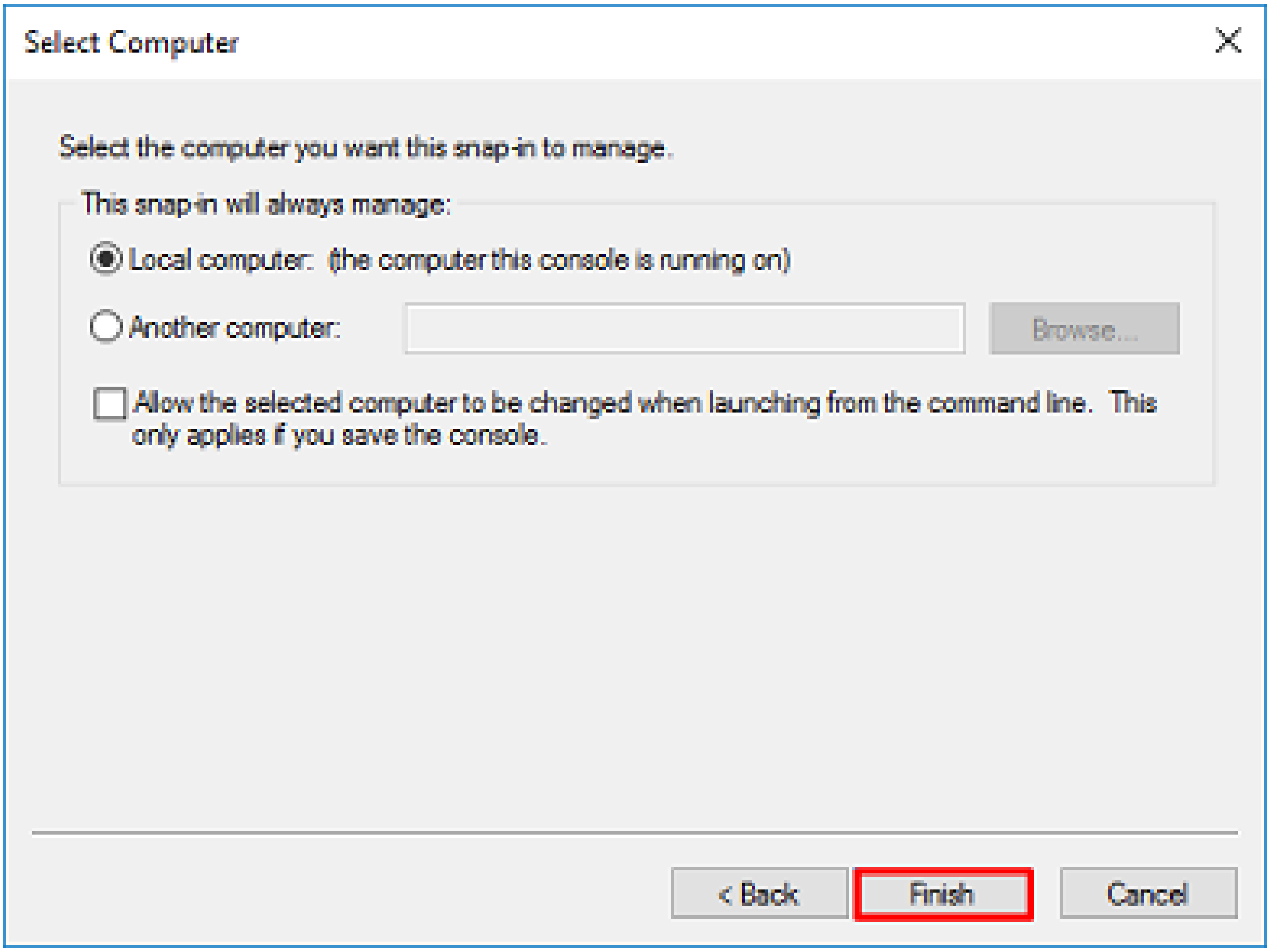
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

كما هو موضح هنا، انقر Finish.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

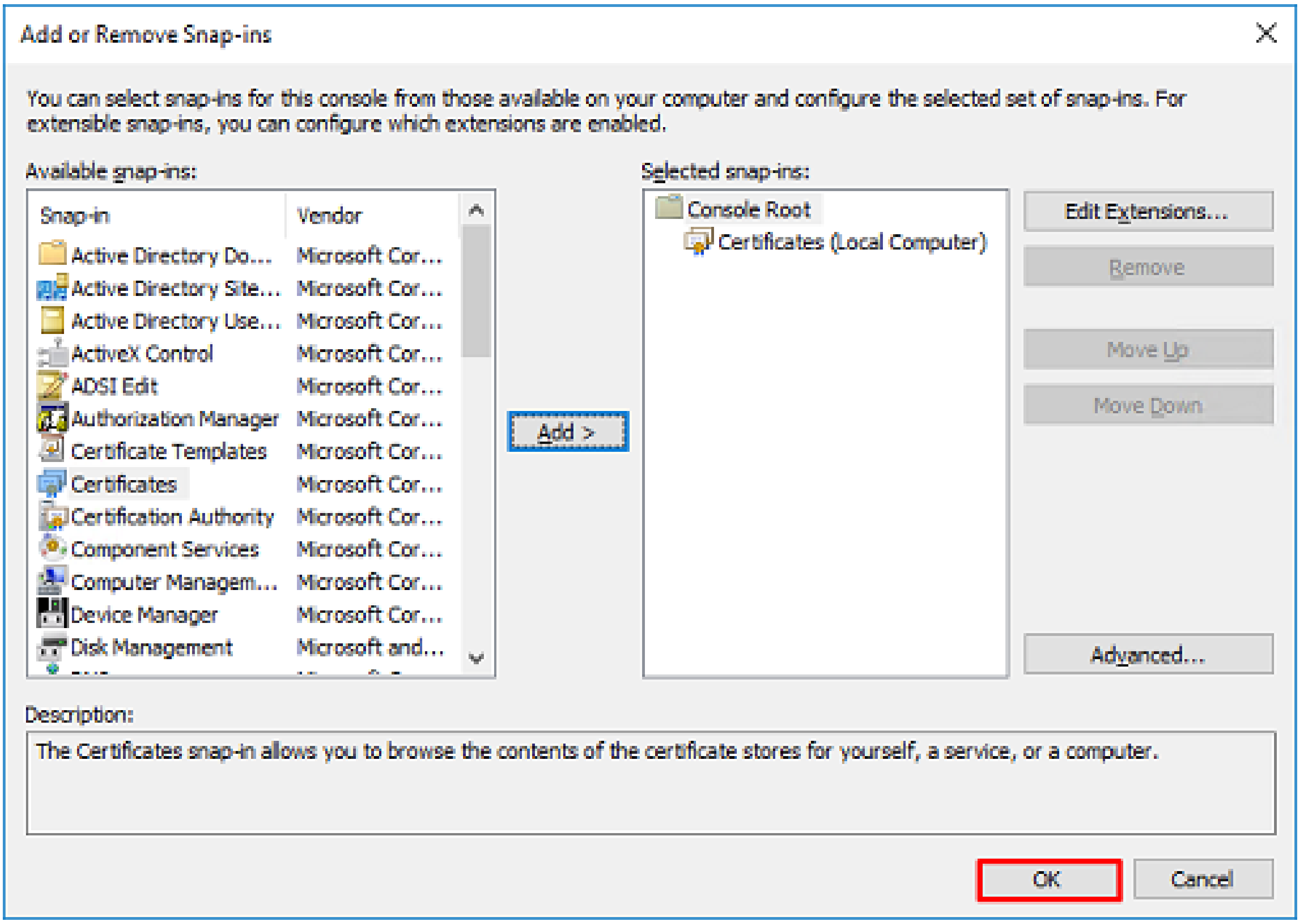
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

-

الآن، انقر OK، كما هو موضح في هذه الصورة.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

Selected snap-ins:

Console Root
Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

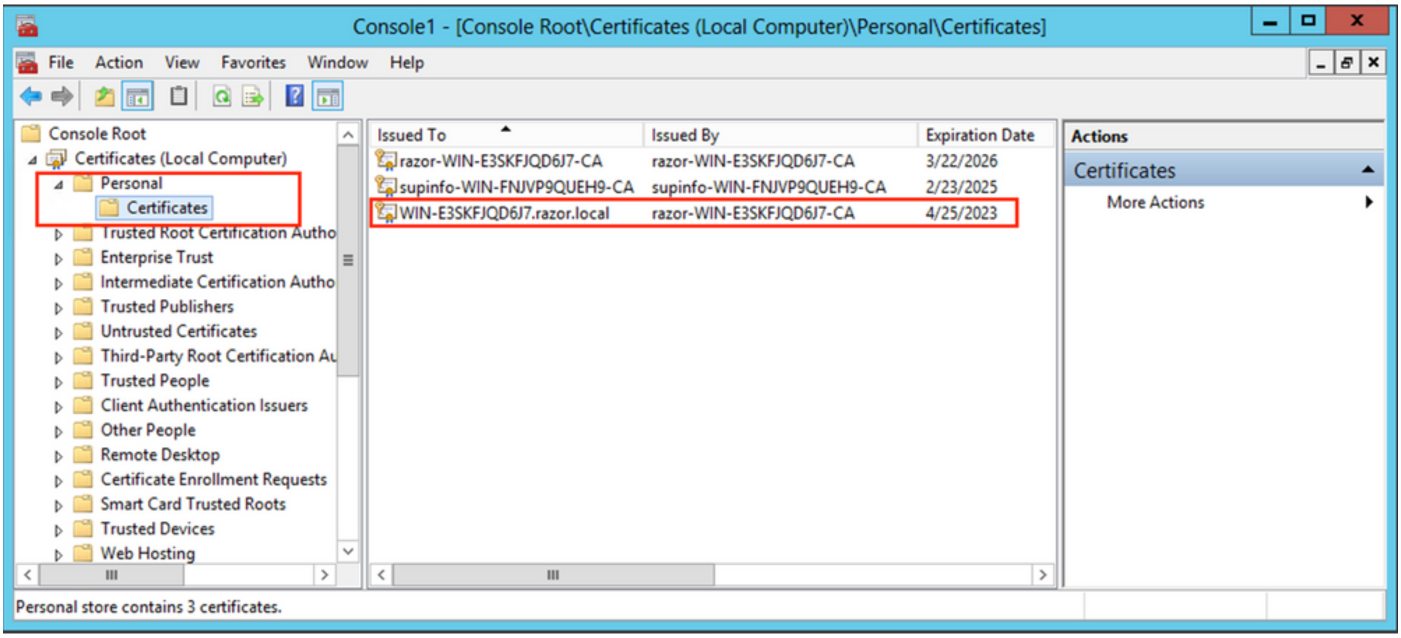
- قم بتوسيع Personal المجلد، ثم انقر Certificates. يجب إصدار الشهادة المستخدمة من قبل LDAPs إلى اسم المجال المؤهل بالكامل (FQDN) الخاص بخادم Windows. يوجد على هذا الخادم ثلاث شهادات مدرجة:

- تم إصدار شهادة مرجع مصدق إلى razor-WIN-E3SKFJQD6J7-CA وبواسطة.

- شهادة مرجع مصدق صادرة من وإلى supinfo-WIN-FNJVP9QUEH9-CA.

- تم إصدار شهادة هوية إلى WIN-E3SKFJQD6J7.razor.local razor-WIN-E3SKFJQD6J7-CA.

في دليل التكوين هذا، يكون FQDN هو WIN-E3SKFJQD6J7.razor.local، وبالتالي فإن الشهادتين الأوليين غير صالحتين للاستخدام كشهادة LDAPs SSL. شهادة الهوية التي تم إصدارها WIN-E3SKFJQD6J7.razor.local هي شهادة تم إصدارها تلقائيا بواسطة خدمة المرجع المصدق ل Windows Server. انقر نقرا مزدوجا على الشهادة للتحقق من التفاصيل.



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

Issued To	Issued By	Expiration Date
razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026
supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	2/23/2025
WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023

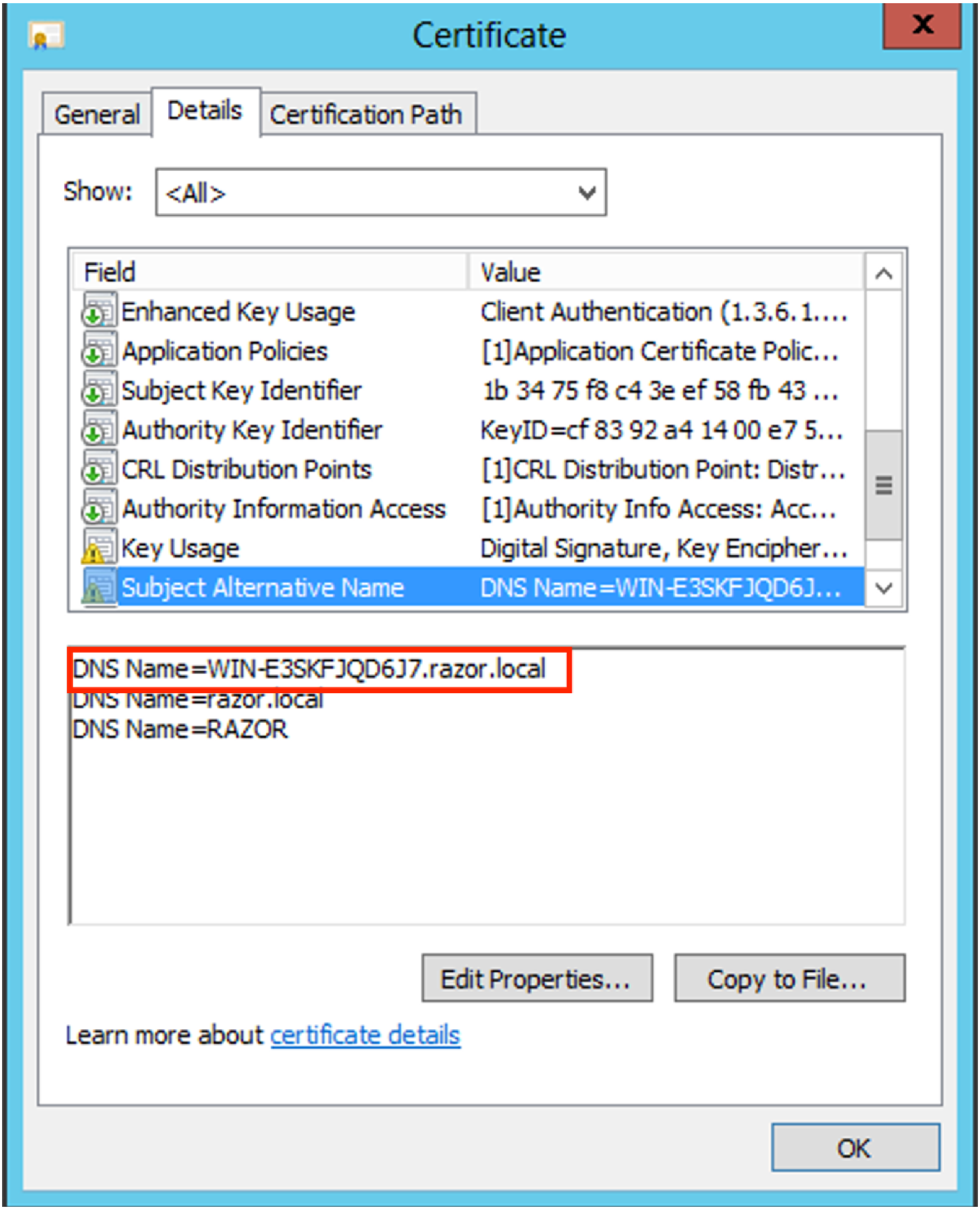
Personal store contains 3 certificates.

- من أجل إستخدامها كشهادة LDAPs SSL، يجب أن تستوفي الشهادة المتطلبات التالية:

- يتطابق الاسم الشائع أو الاسم البديل لموضوع DNS مع FQDN الخاص بخادم Windows.

- تحتوي الشهادة على مصادقة الخادم ضمن حقل إستخدام المفتاح المحسن.

تحت Details علامة التبويب الخاصة بالشهادة، أختر Subject Alternative Name، حيث WIN-E3SKFJQD6J7.razor.localيكون FQDN موجودا.



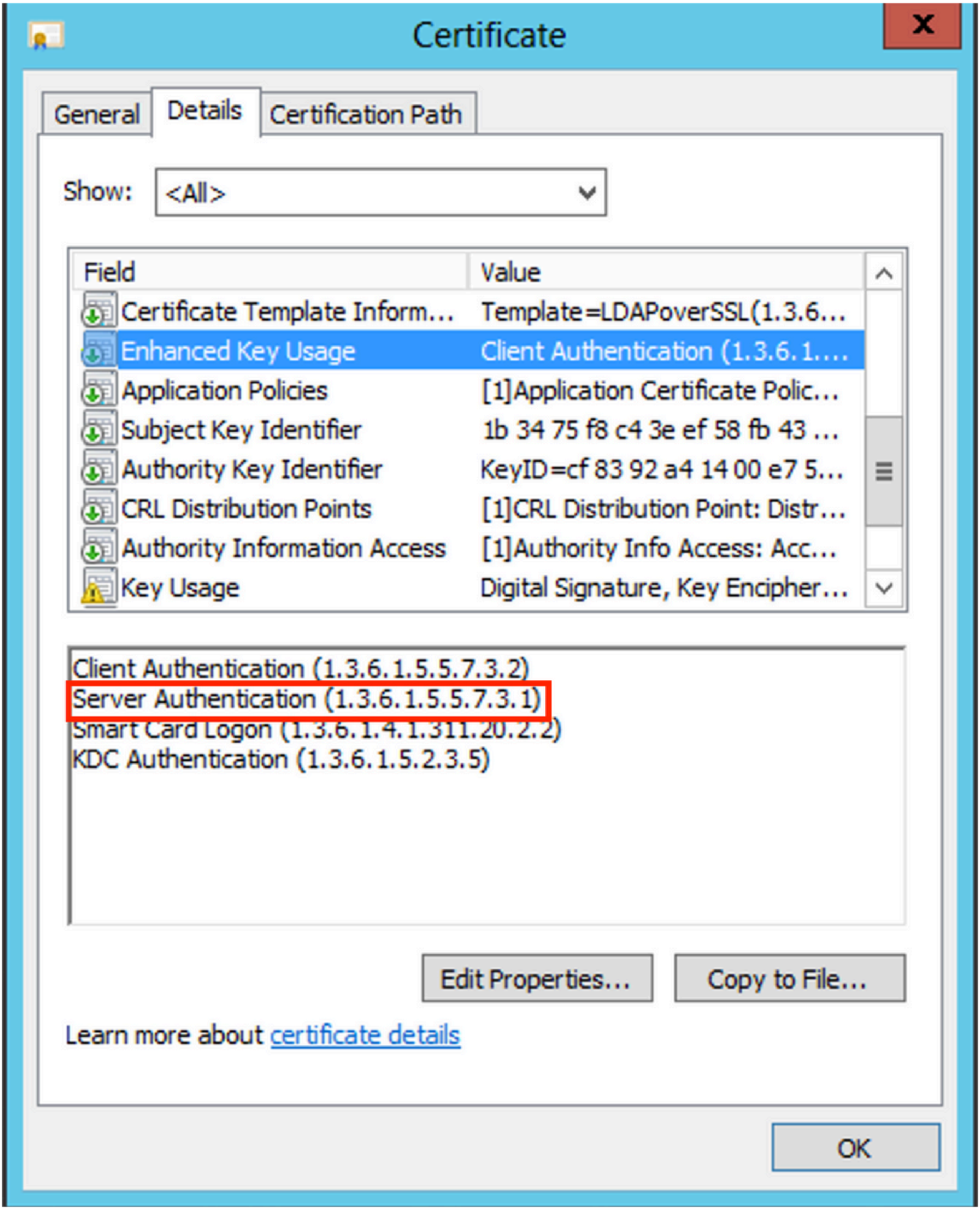
Certificate

Show: <All>

Field	Value
Enhanced Key Usage	Client Authentication (1.3.6.1....
Application Policies	[1]Application Certificate Polic...
Subject Key Identifier	1b 34 75 f8 c4 3e ef 58 fb 43 ...
Authority Key Identifier	KeyID=cf 83 92 a4 14 00 e7 5...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Key Encipher...
Subject Alternative Name	DNS Name=WIN-E3SKFJQD6J...

```
DNS Name=WIN-E3SKFJQD6J7.razor.local
DNS Name=razor.local
DNS Name=RAZOR
```

تحت Enhanced Key Usage، Server Authentication حاضر.



Show: <All>

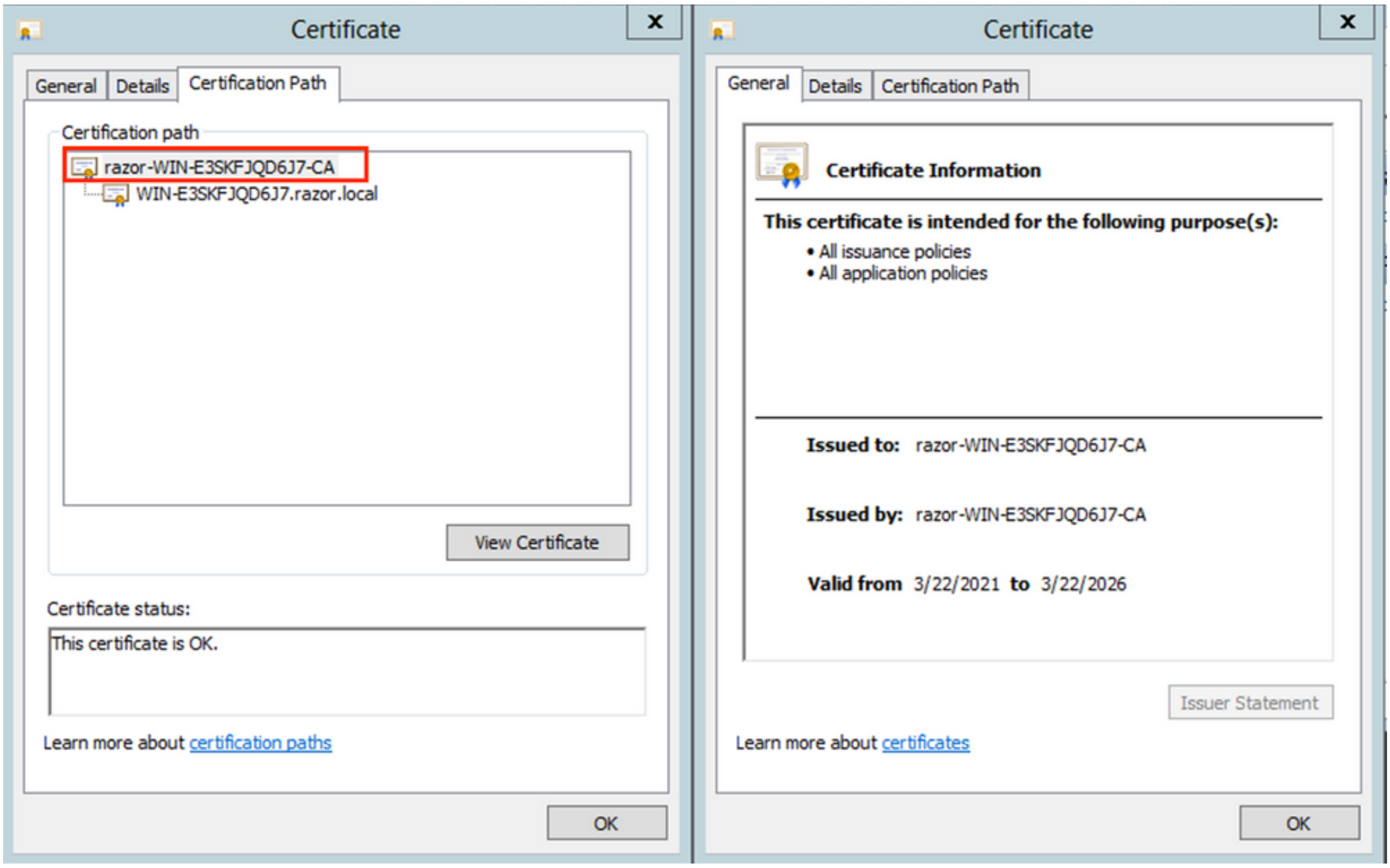
Field	Value
Certificate Template Inform...	Template=LDAPoverSSL(1.3.6...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Application Policies	[1]Application Certificate Polic...
Subject Key Identifier	1b 34 75 f8 c4 3e ef 58 fb 43 ...
Authority Key Identifier	KeyID=cf 83 92 a4 14 00 e7 5...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Key Encipher...

Client Authentication (1.3.6.1.5.5.7.3.2)
Server Authentication (1.3.6.1.5.5.7.3.1)
Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
KDC Authentication (1.3.6.1.5.2.3.5)

Learn more about certificate details

-

عندما يتم تأكيد ذلك، تحت Certification Path علامة التبويب، أختر شهادة المستوى الأعلى والتي هي شهادة المرجع المصدق الجذر، ثم انقر View Certificate. يؤدي هذا إلى فتح تفاصيل الشهادة لشهادة المرجع المصدق الجذر كما هو موضح في الصورة:



Certification path

razor-WIN-E3SKFJQD6J7-CA

WIN-E3SKFJQD6J7.razor.local

Certificate status:

This certificate is OK.

Learn more about certification paths

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: razor-WIN-E3SKFJQD6J7-CA

Issued by: razor-WIN-E3SKFJQD6J7-CA

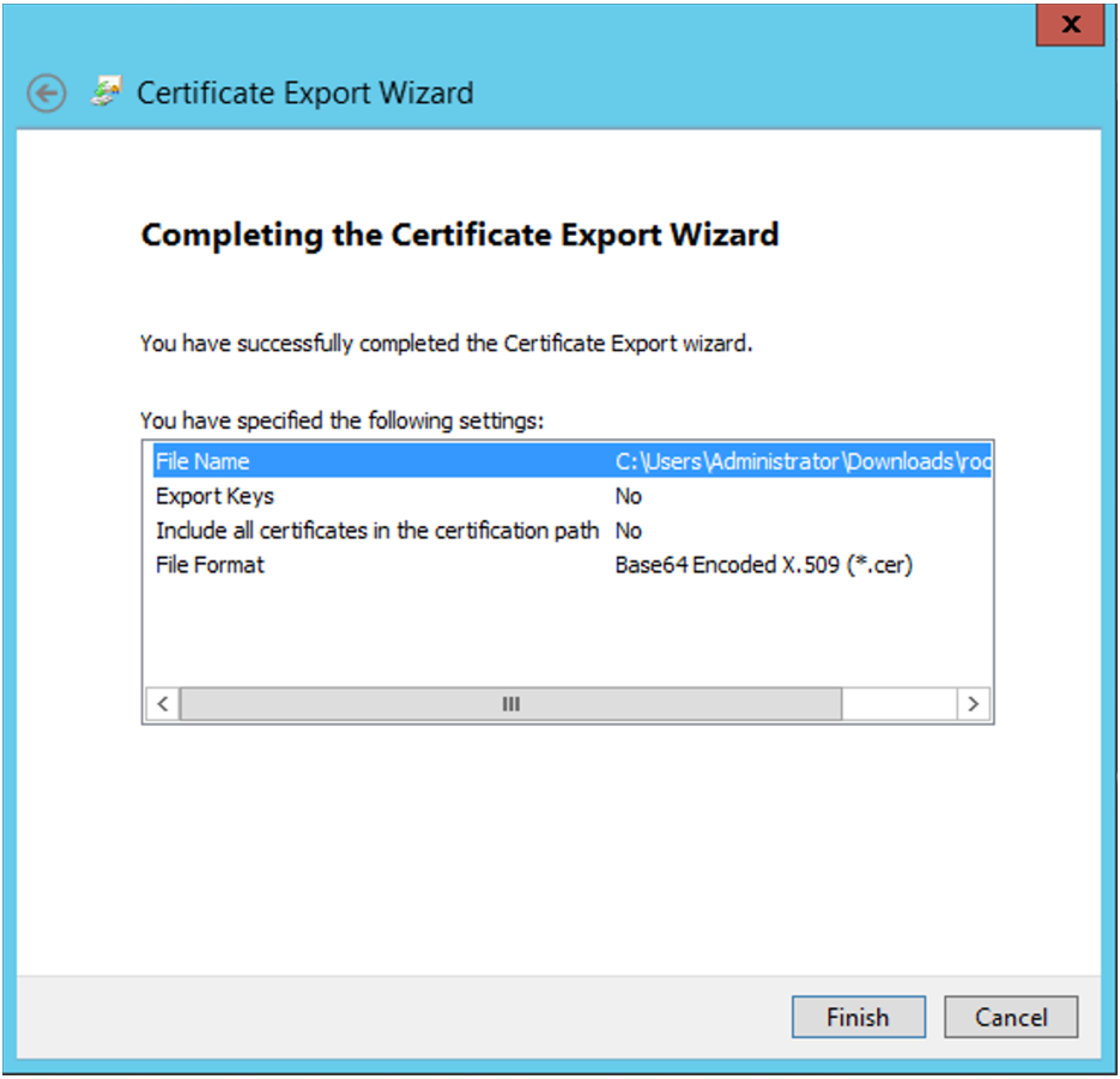
Valid from 3/22/2021 to 3/22/2026

Learn more about certificates

-

تحت Details علامة التبويب الخاصة بشهادة المرجع المصدق الجذر، انقر Copy to File وتصفح الCertificate Export Wizard الذي يصدر المرجع المصدق الجذر بتنسيق PEM.

أختر Base-64 encoded X.509 كتنسيق ملف.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\Administrator\Downloads\roo
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

- افتح شهادة المرجع المصدق الجذر المخزنة في الموقع المحدد على الجهاز باستخدام مفكرة أو أي محرر نصوص آخر.

يعرض هذا شهادة تنسيق PEM. احفظ هذا لوقت لاحق.

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgoJ
vcjEhMB8GA1UEAxMYcmF6b3ItV0lOLUUzU0tGSlFENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBM
BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvc
CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnblxwtXOB2G4UxZ3LRrWznjXaS02Rc3qVw4lnOAziGs4ZMNM1X8UWeKuwi8QZQljJ
9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU3OaiiI/tp422ydy3Kgl7Iqt1s4XqpZmTezykWra7dUyXfkuESk6lEOAV+zNxfBJh3Q9Nzp
```

```
CSkTQTRXYryy8dJrWjAF/n6A3VnS/l7Uhujlx4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwEAAaNRME8w
DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFM+DkqQUAOdY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0G
AA4IBAQCiSm5U7U6Y7zXdx+dleJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7BnO6f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6qZu
4sMZffbVrGlRz7twWY36J5G5vhNUhzZ1N2OLw6wtHg2SO8XlvpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nrylbBfn0NEX7l
GuDsepY7/u2uWfy/vpTJigeok2DH6HFfOET3sE+7rsIAY+of0kWW5gNwQ4hOwv4Goqj+YQRAXXi2OZyltHR1dfUUbwVENSFQtDnFA7X
-----END CERTIFICATE-----
```

في حالة وجود شهادات متعددة مثبتة في "مخزن الجهاز المحلي" على خادم LDAPs (إختياري)

1. في حالة وجود العديد من شهادات الهوية التي يمكن إستخدامها من قبل LDAPs وعندما يكون هناك عدم يقين فيما يتعلق بالمستخدم، أو لا يوجد وصول إلى خادم LDAP، يظل من الممكن إستخراج المرجع المصدق الجذر من التقاط حزمة تم على FTD.

2. في حالة وجود عدة شهادات صالحة لمصادقة الخادم في مخزن شهادات الكمبيوتر المحلي لخادم LDAP (مثل وحدة التحكم بالمجال AD DS)، يمكن ملاحظة إستخدام شهادة مختلفة لاتصالات LDAP. أفضل حل لمثل هذه المشكلة هو إزالة كل الشهادات غير الضرورية من مخزن شهادات الكمبيوتر المحلي وفيها شهادة واحدة فقط صالحة لمصادقة الخادم.

ومع ذلك، إذا كان هناك سبب منطقي يتطلب وجود شهادتين أو أكثر وأن يكون لديك خادم Windows Server 2008 LDAP على الأقل، يمكن إستخدام مخزن الشهادات لخدمات مجال خدمة Active Directory (NTDS\Personal) لاتصالات LDAP.

توضح هذه الخطوات كيفية تصدير شهادة تم تمكين LDAP عليها من مخزن شهادات الكمبيوتر المحلي لوحدة التحكم بالمجال إلى مخزن شهادات خدمة مجال خدمة Active Directory (NTDS\Personal).

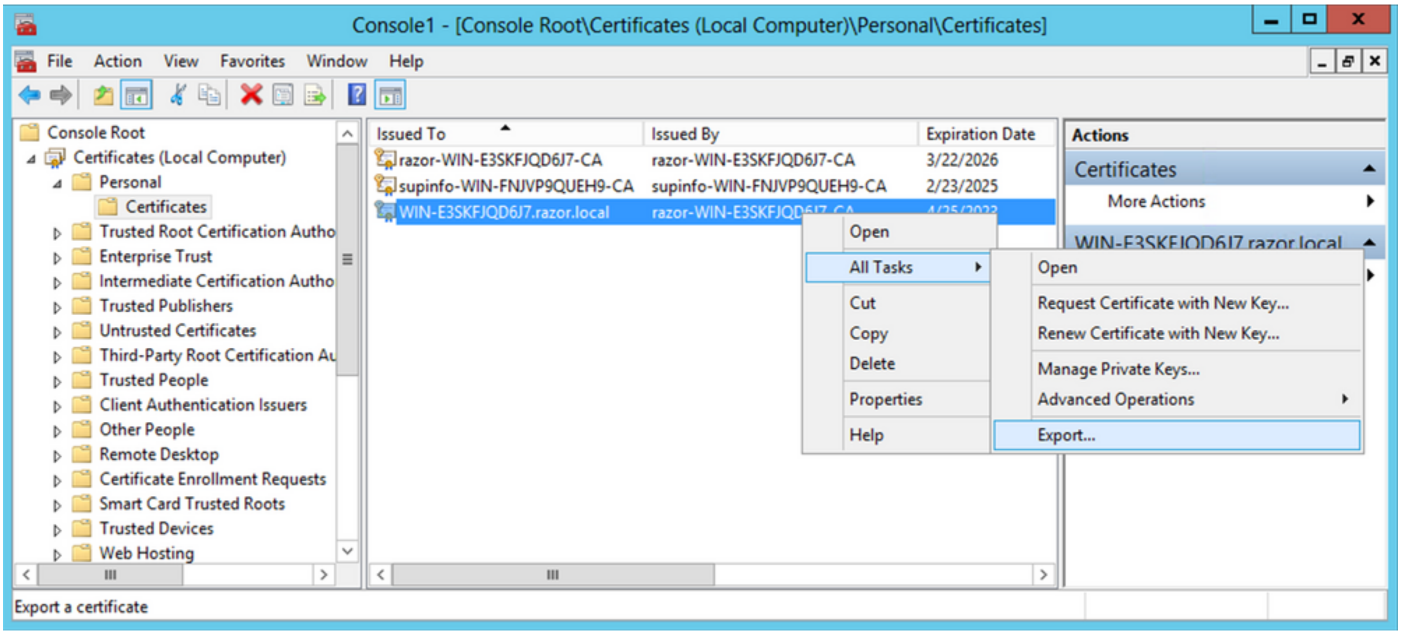
- انتقل إلى وحدة تحكم MMC على خادم Active Directory، واختر File، ثم انقر Add/Remove Snap-in.

- انقر Certificates ثم انقر Add.

- في Certificates snap-in، أختر Computer account ثم انقر Next.

- في Select Computer، أختر Local Computer، انقر OK، ثم انقر Finish. في Add or Remove Snap-ins، انقر OK.

- في وحدة تحكم الشهادات الخاصة بالكمبيوتر الذي يحتوي على شهادة تستخدم لمصادقة الخادم، انقر بزر الماوس الأيمن فوق certificate All Tasks، ثم انقر Export.



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

Issued To	Issued By	Expiration Date
razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026
supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	2/23/2025
WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023

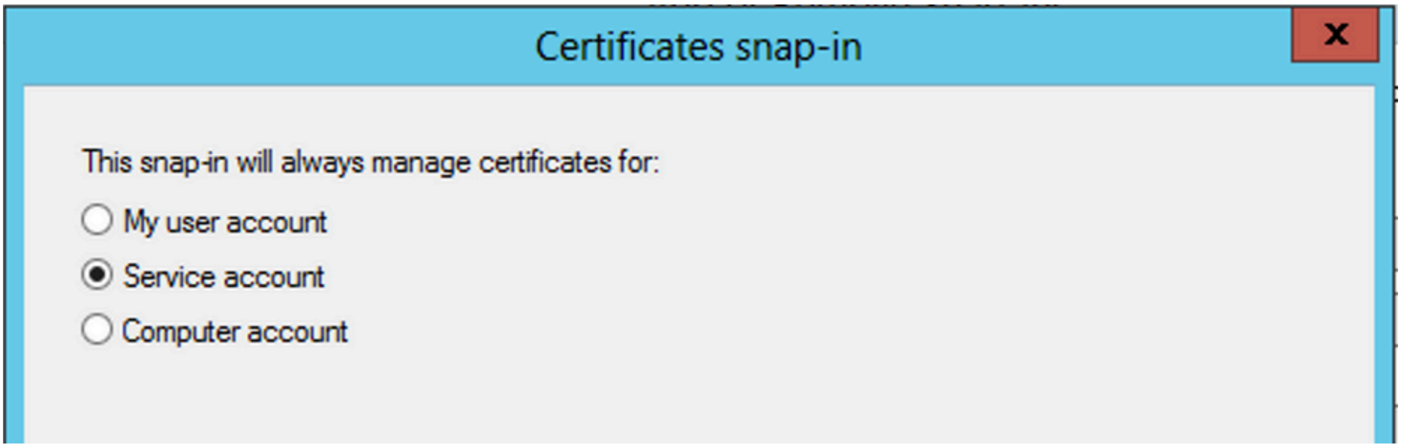
Export a certificate

- تصدير الشهادة بالتنسيق pfx في الأقسام التالية. الإشارة إلى هذه المقالة حول كيفية تصدير شهادة بالتنسيق pfx من MMC:

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

- بمجرد إتمام تصدير الشهادة، انتقل إلى Add/Remove Snap-in تشغيل MMC console. انقر Certificates ثم انقر Add.

- أختر Service account ثم انقر Next.



Certificates snap-in

This snap-in will always manage certificates for:

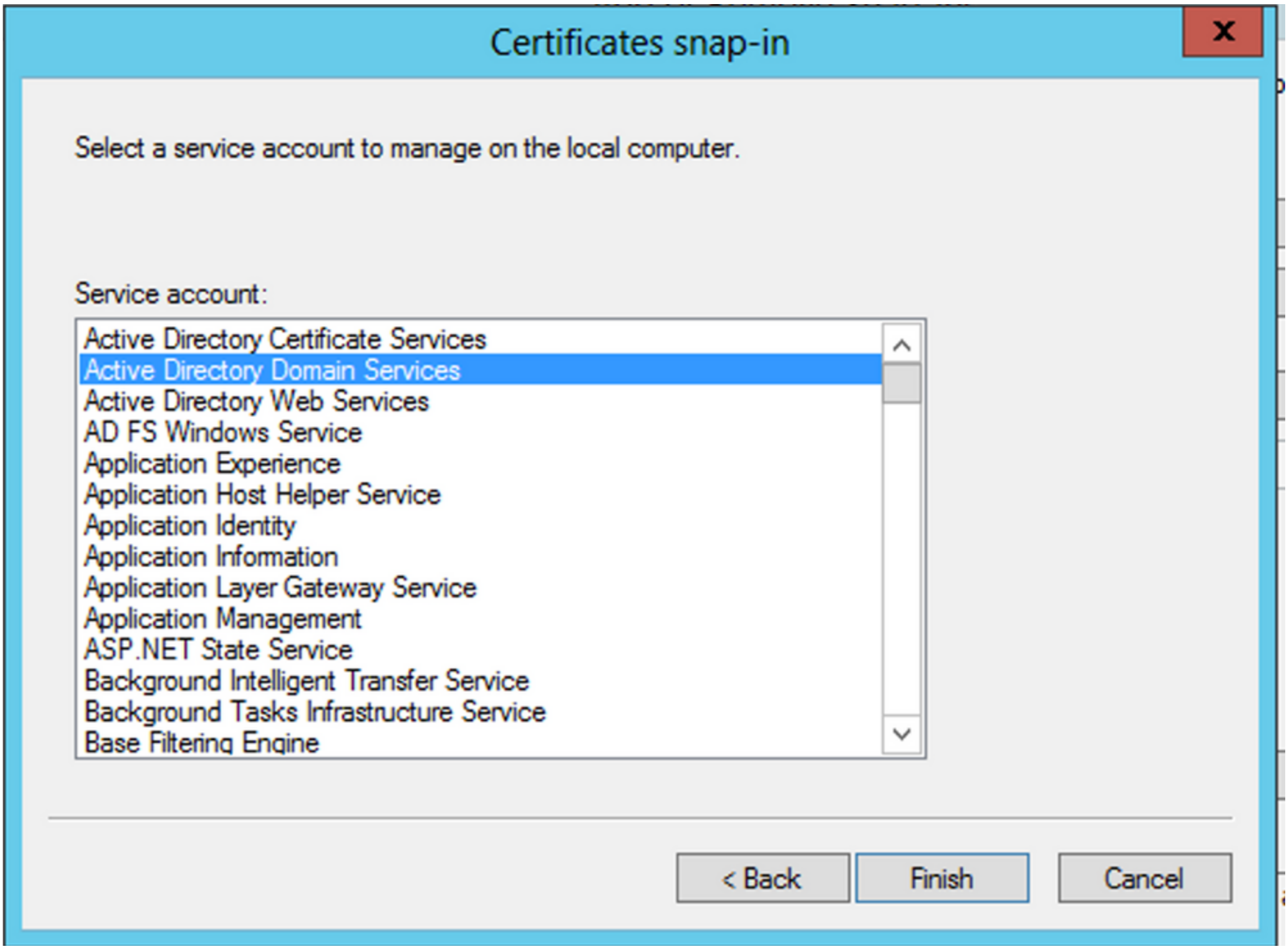
○ My user account

● Service account

○ Computer account

- في Select Computer الشاشة، أختر Local Computer وانقر Next.

- أختر Active Directory Domain Services ثم انقر Finish.



Certificates snap-in

Select a service account to manage on the local computer.

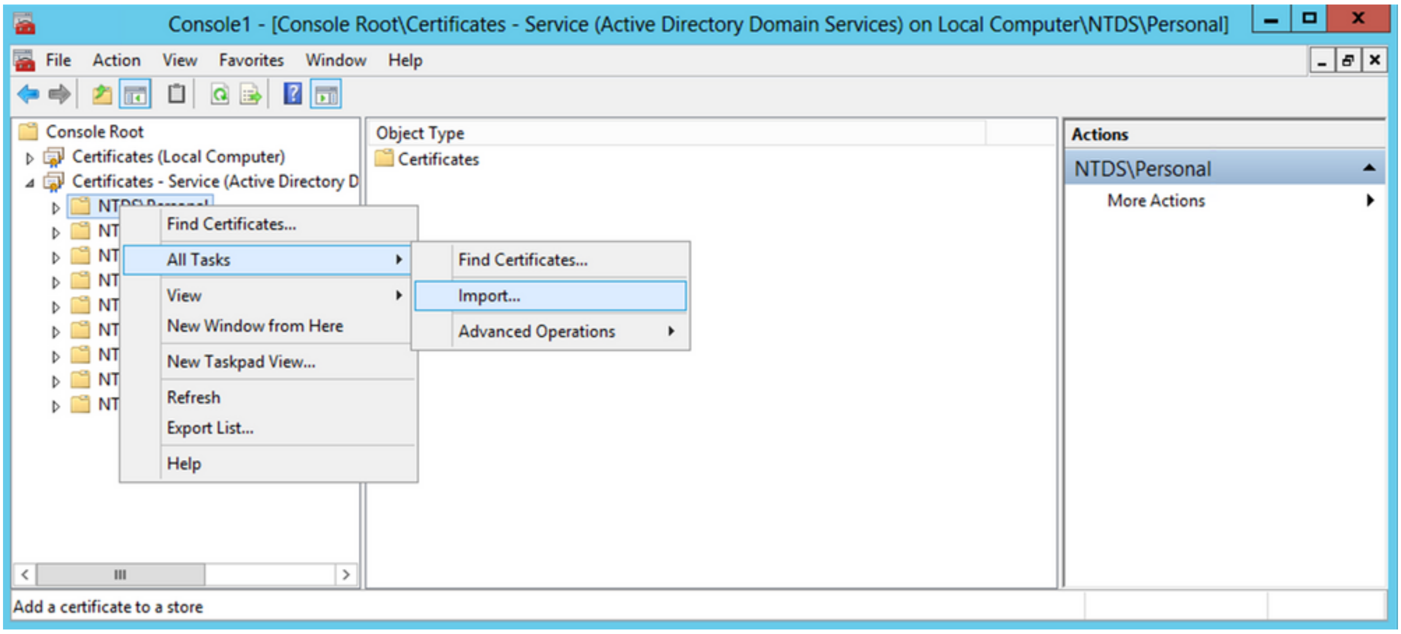
Service account: Active Directory Domain Services

Active Directory Certificate Services
Active Directory Domain Services
Active Directory Web Services
AD FS Windows Service
Application Experience
Application Host Helper Service
Application Identity
Application Information
Application Layer Gateway Service
Application Management
ASP.NET State Service
Background Intelligent Transfer Service
Background Tasks Infrastructure Service
Base Filtering Engine
< Back
Finish
Cancel

- في Add/Remove Snap-ins الشاشة، انقر OK.

- تمدد Certificates - Services (Active Directory Domain Services) ثم انقر NTDS\Personal.

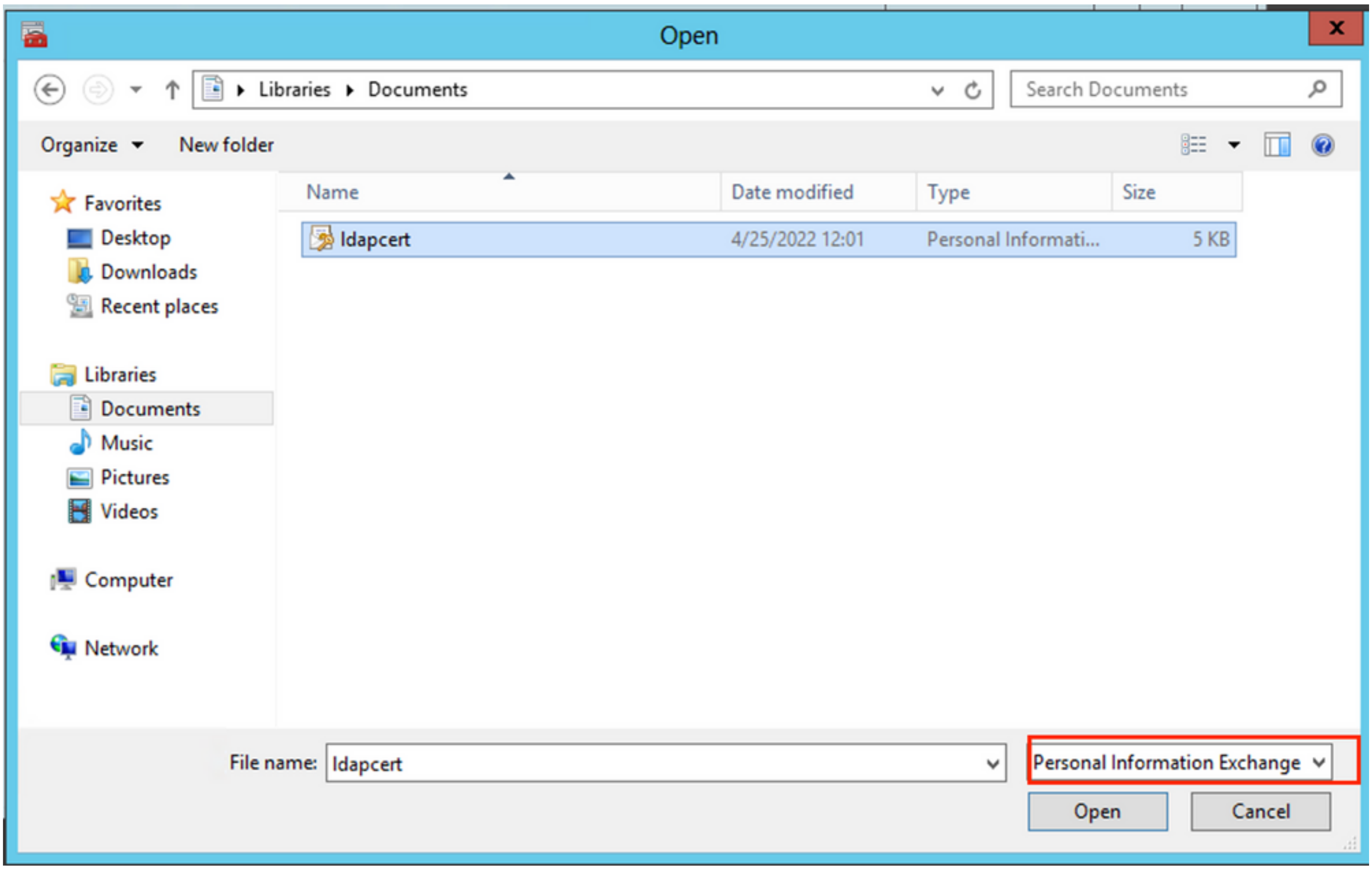
- انقر بزر الماوس الأيمن NTDS\Personal، وانقر All Tasks، ثم انقر Import.



- في Certificate Import Wizard شاشة الترحيب، انقر Next.

- في شاشة ملف للاستيراد، انقر Browse، وحدد مكان ملف الترخيص الذي قمت بتصديره مسبقا.

- على الشاشة المفتوحة، تأكد من تحديد تبادل المعلومات الشخصية (*pfx،*.p12) كنوع الملف ثم قم بالتنقل في نظام الملفات لتحديد مكان الشهادة التي قمت بتصديرها مسبقا. ثم انقر على تلك الشهادة.



Name	Date modified	Type	Size
ldapcert	4/25/2022 12:01	Personal Informati...	5 KB

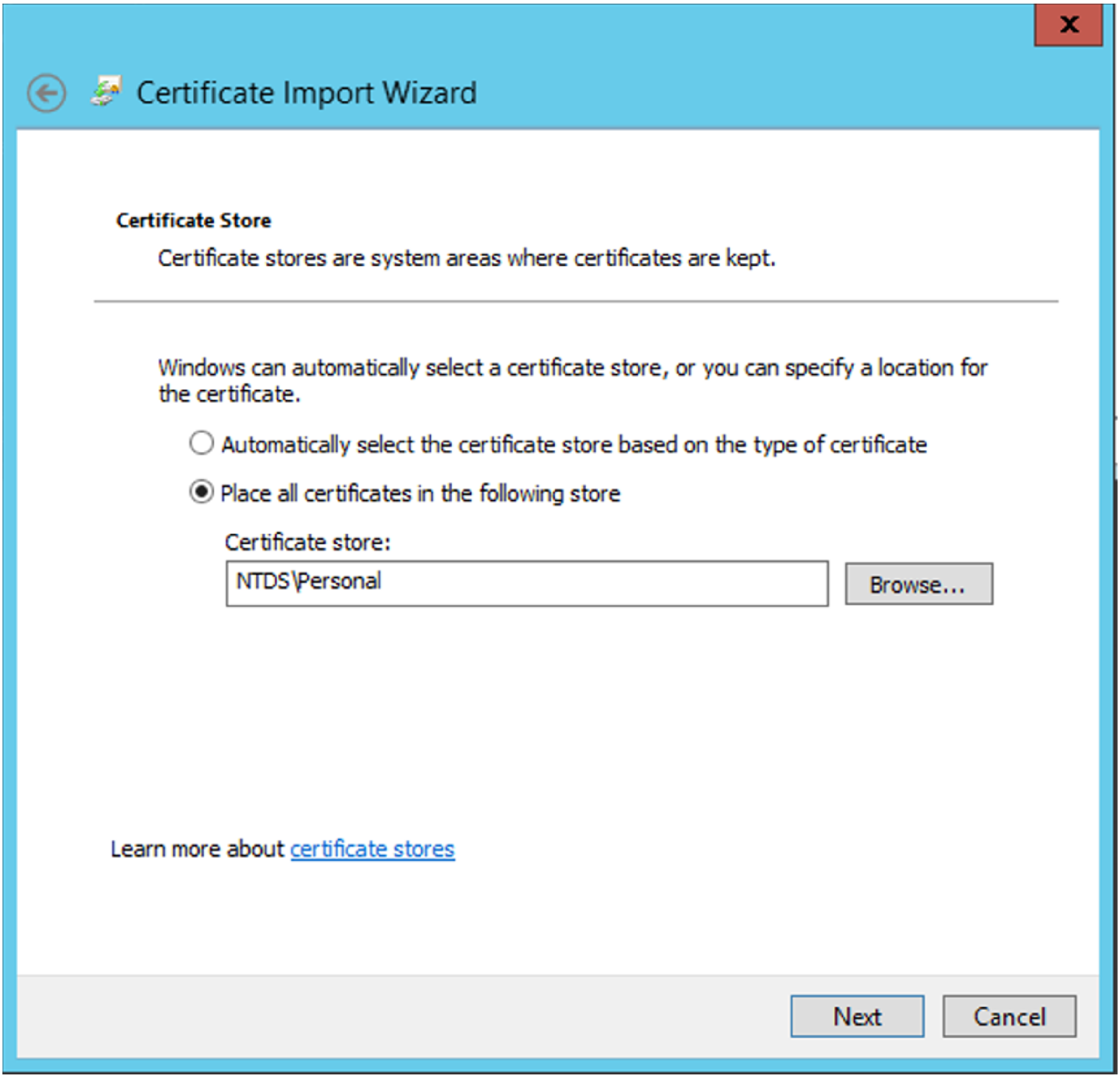
File name: ldapcert

Personal Information Exchange

- انقر Open ثم انقر Next.

- أدخل كلمة المرور على الشاشة، ثم انقر Next فوق كلمة المرور التي قمت بضبطها للملف.

- في صفحة مخزن الشهادات، تأكد من تحديد وضع كل الشهادات واقرأ مخزن الشهادات: NTDS\Personal ثم انقر Next.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

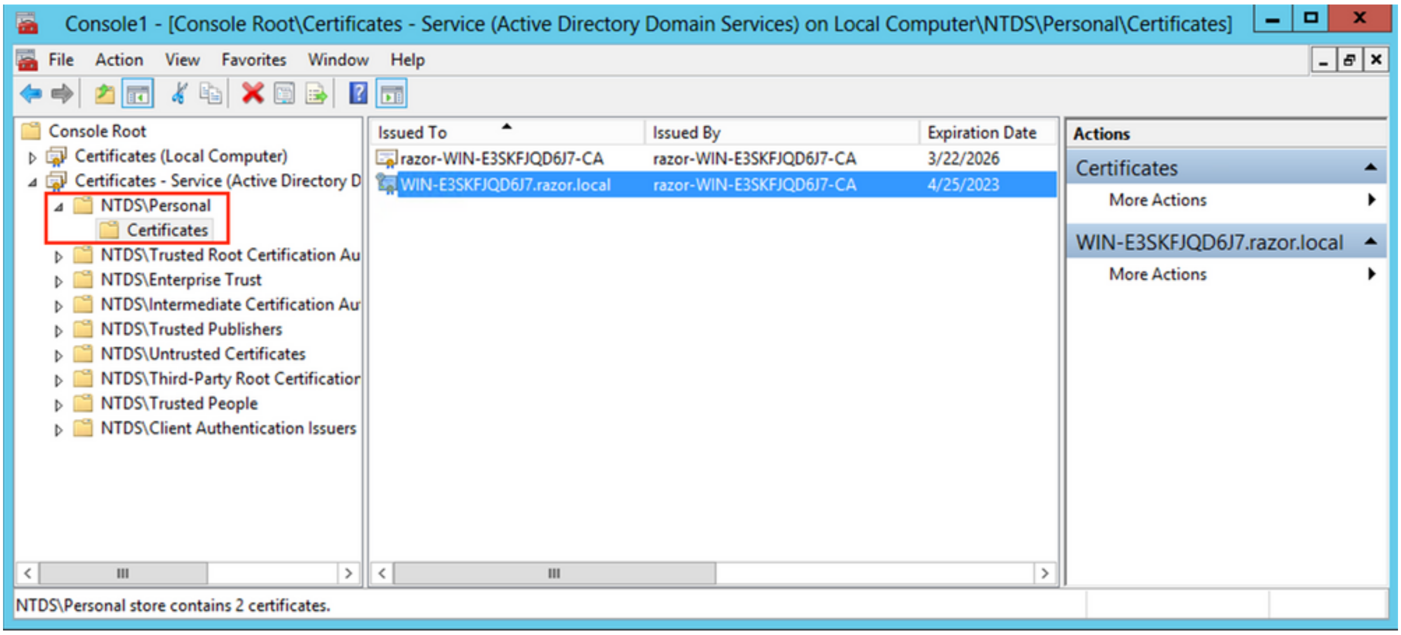
● Place all certificates in the following store

Certificate store: NTDS\Personal

Learn more about certificate stores

-

في Certificate Import Wizard شاشة الإكمال، انقر Finish. ثم ترى رسالة تفيد بأن عملية الاستيراد تمت بنجاح. انقر.OK يظهر أن الشهادة تم إستيرادها تحت مخزن الشهادات: NTDS\Personal.



Console1 - [Console Root\Certificates - Service (Active Directory Domain Services) on Local Computer\NTDS\Personal\Certificates]

Issued To	Issued By	Expiration Date
razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026
WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023

NTDS\Personal store contains 2 certificates.

File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Certificates - Service (Active Directory D
NTDS\Personal
Certificates
NTDS\Trusted Root Certification Au
NTDS\Enterprise Trust
NTDS\Intermediate Certification Au
NTDS\Trusted Publishers
NTDS\Untrusted Certificates
NTDS\Third-Party Root Certificatior
NTDS\Trusted People
NTDS\Client Authentication Issuers
Actions
Certificates
More Actions
WIN-E3SKFJQD6J7.razor.local
More Actions

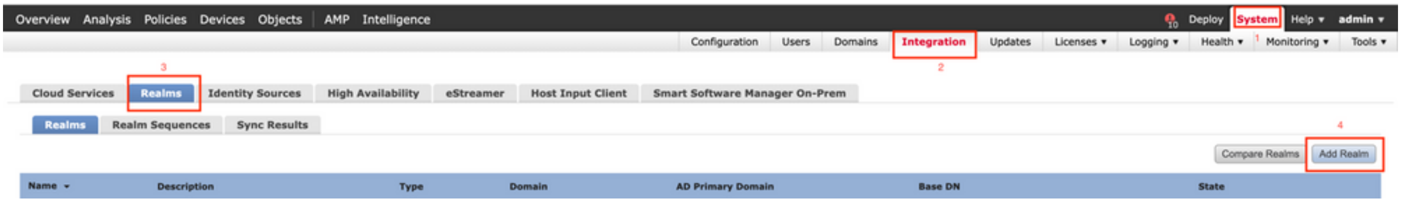
تكوينات FMC

التحقق من الترخيص

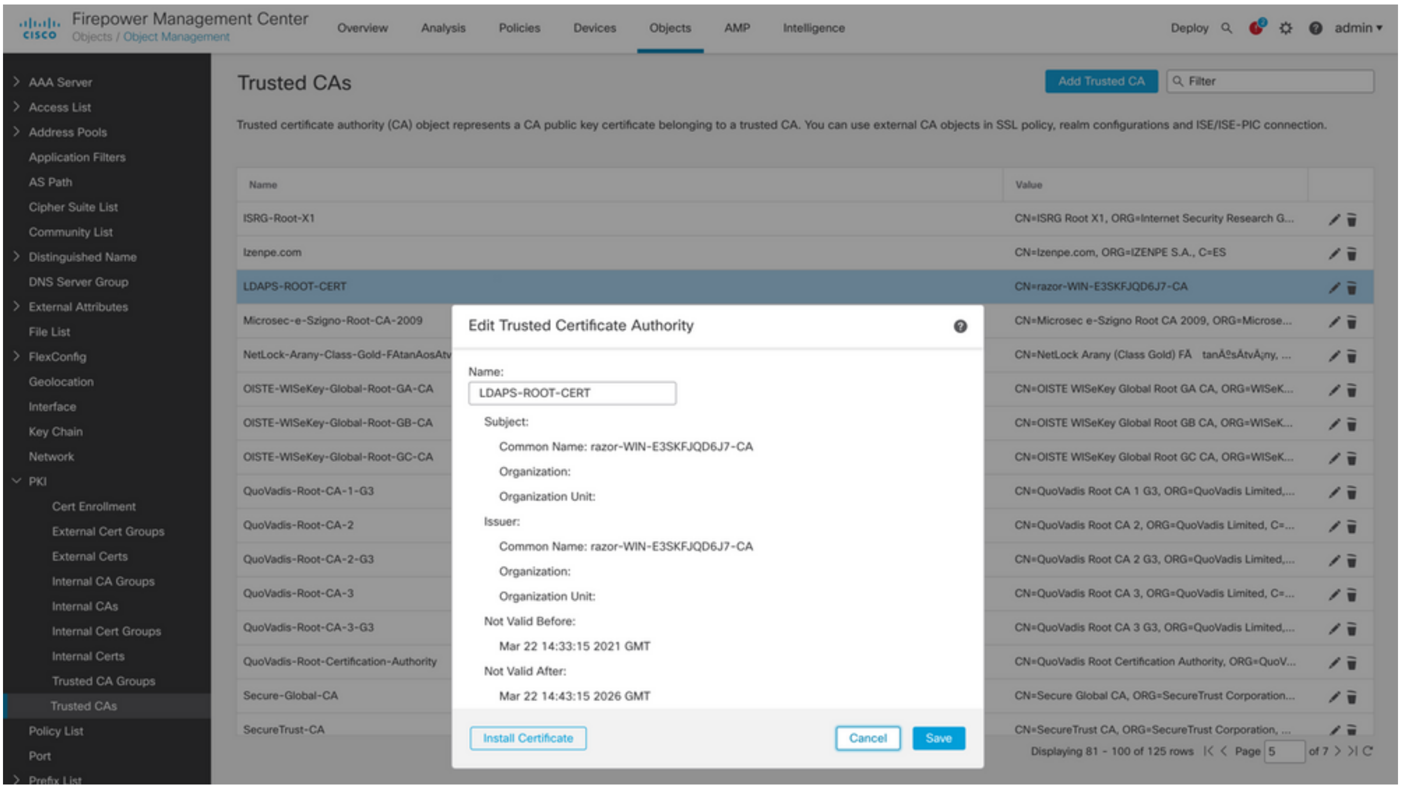
لنشر تكوين AnyConnect، يجب تسجيل FTD مع خادم الترخيص الذكي، ويجب تطبيق ترخيص Plus أو Apex أو VPN صالح على الجهاز فقط.

عالم الإعداد

- انتقل إلى System > Integration. انتقل إلى Realms، ثم انقر فوق Add Realm، كما هو موضح في هذه الصورة:



- املأ الحقول المعروضة بناء على المعلومات التي تم تجميعها من خادم Microsoft ل LDAPs. قبل ذلك، قم باستيراد شهادة المرجع المصدق الجذر التي وقعت على شهادة خدمة LDAP على خادم Windows Objects > PKI > Trusted CAs > Add Trusted CA أسفل، حيث يشار إلى ذلك أسفل Directory Server Configuration النطاق. عند الانتهاء، انقر OK.



Trusted CAs

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) FÅ tanÃºsÃtvÃ¡ny, ...
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:

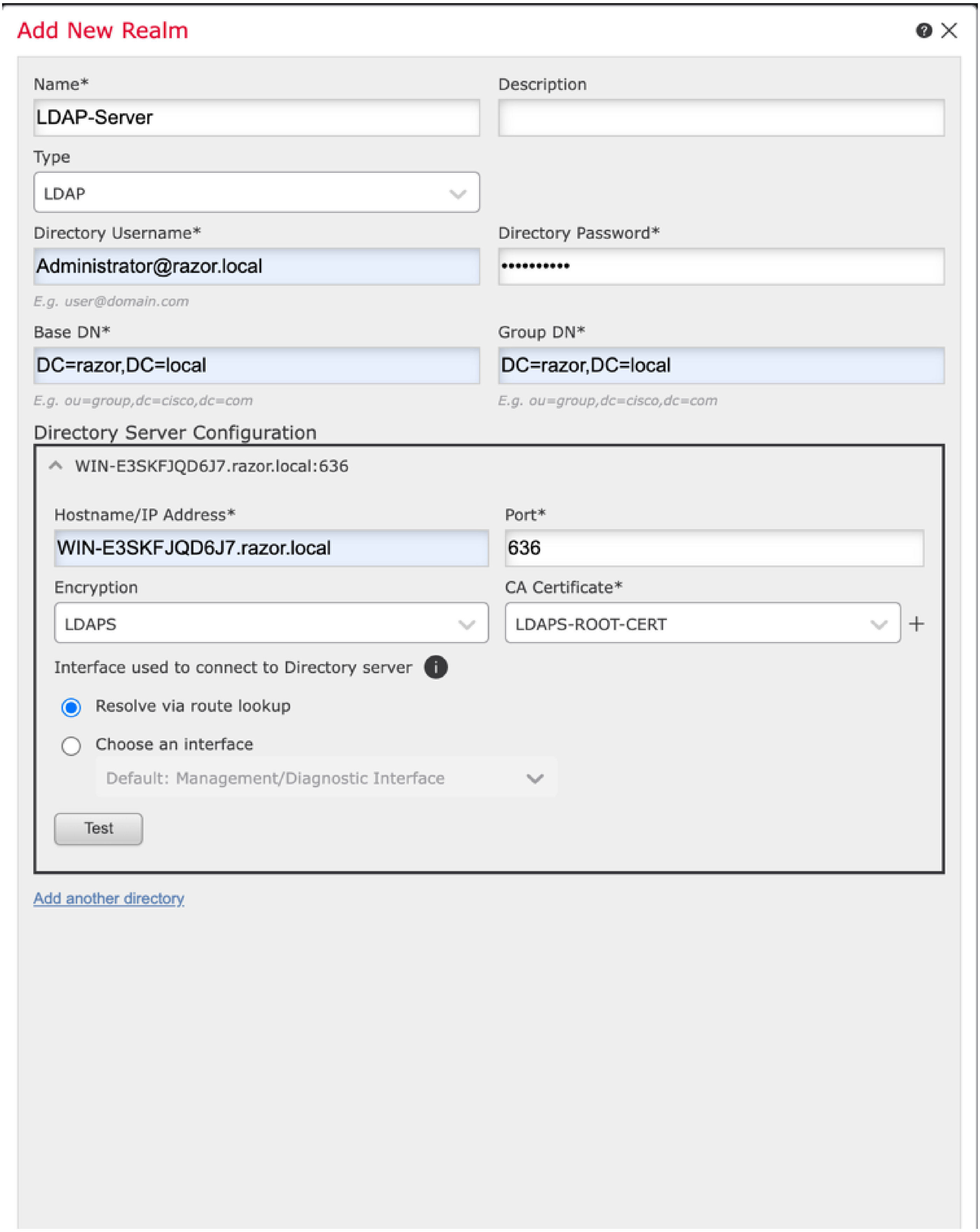
Organization Unit:

Not Valid Before:

Mar 22 14:33:15 2021 GMT

Not Valid After:

Mar 22 14:43:15 2026 GMT



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

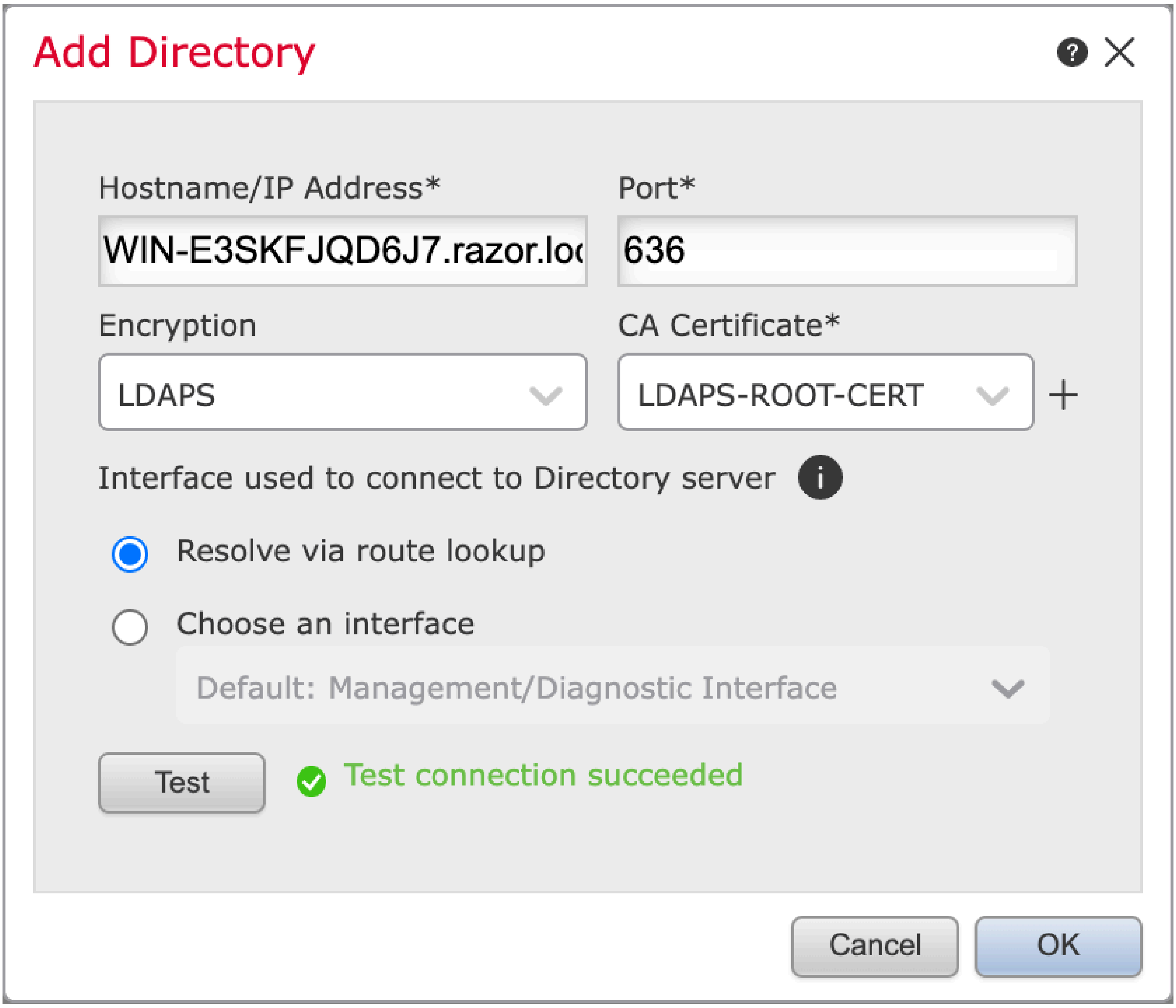
● Resolve via route lookup

○ Choose an interface

Default: Management/Diagnostic Interface

- انقر فوق Test in order to ضمنت أن FMC يستطيع بنجاح ربط مع الدليل username وكلمة يزود في الخطوة مبكر. ونظرا لأن هذه الاختبارات يتم بدؤها من وحدة التحكم في إدارة اللوحة الأساسية (FMC) وليس من خلال إحدى الواجهات

القابلة للتوجيه التي تم تكوينها على FTD (كما هو الحال في الداخل أو الخارج أو dmz)، فإن الاتصال الناجح (أو الفاشل) لا يضمن نفس النتيجة لمصادقة AnyConnect نظرا لأن طلبات مصادقة AnyConnect LDAP يتم أداؤها من إحدى واجهات FTD القابلة للتوجيه.



Add Directory

Hostname/IP Address*: WIN-E3SKFJQD6J7.razor.loc

Port*: 636

Encryption: LDAPS

CA Certificate*: LDAPS-ROOT-CERT

Interface used to connect to Directory server

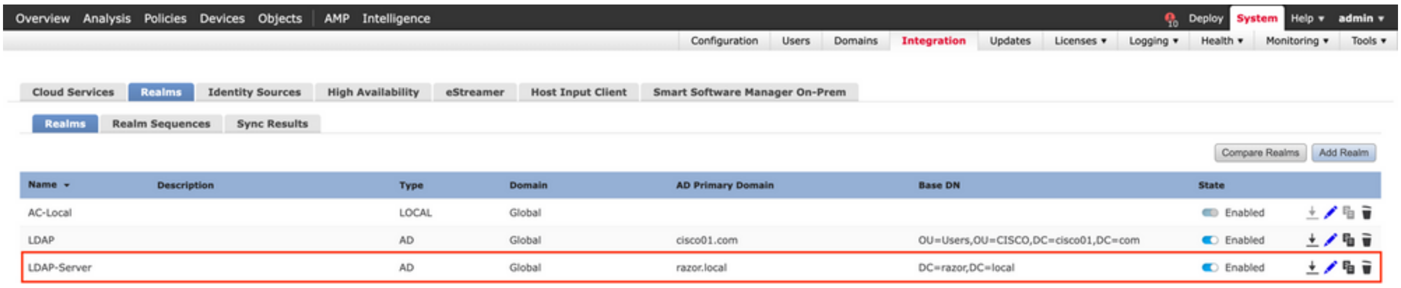
● Resolve via route lookup

○ Choose an interface

Default: Management/Diagnostic Interface

Test ✓ Test connection succeeded

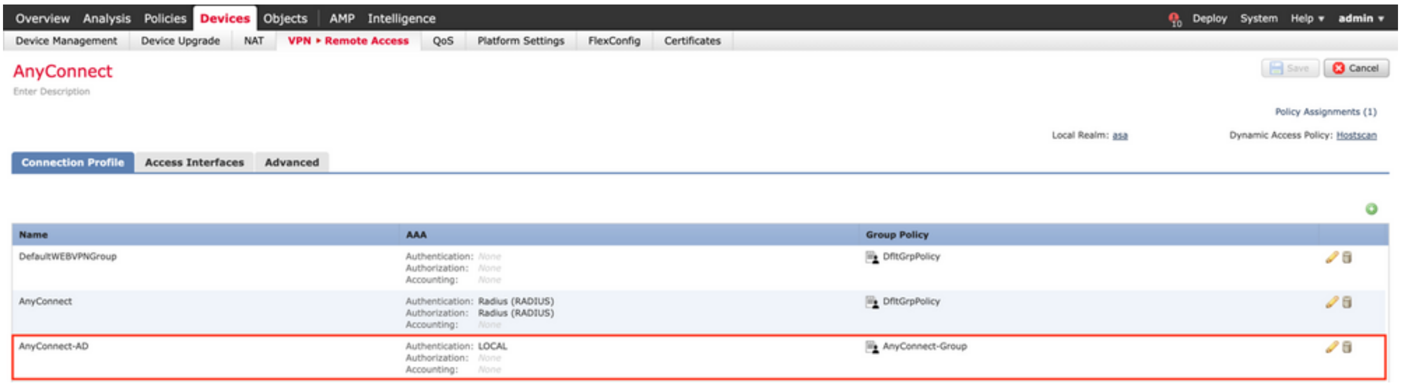
- قم بتمكين النطاق الجديد.


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

تكوين AnyConnect لإدارة كلمة المرور

- أختر ملف تعريف الاتصال الموجود أو قم بإنشاء ملف تعريف جديد، إذا كان إعدادا أوليا ل AnyConnect. هنا، يستخدم توصيف توصيل موجود اسمه 'AnyConnect-AD' معين بمصادقة محلية.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management Device Upgrade NAT VPN ▸ Remote Access QoS Platform Settings FlexConfig Certificates
Save
Cancel
Connection Profile Access Interfaces Advanced

AnyConnect
Enter Description

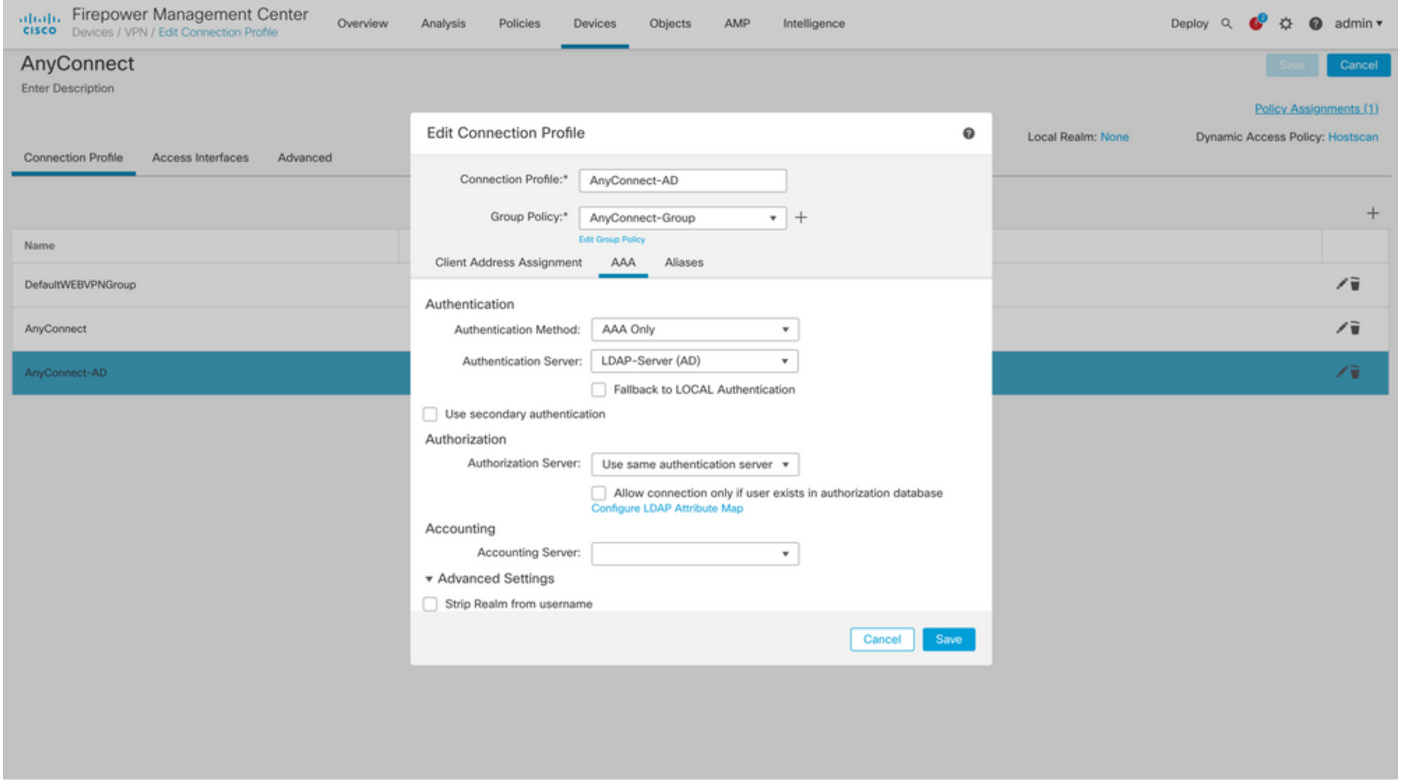
Policy Assignments (1)

Local Realm: asa

Dynamic Access Policy: Hostscan

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

- قم بتحرير ملف تعريف الاتصال وتعيين خادم LDAP الجديد الذي تم تكوينه في الخطوات السابقة، أسفل إعدادات AAA الخاصة بملف تعريف الاتصال. بمجرد الانتهاء، انقر Save فوق الزاوية العليا اليمنى.



AnyConnect

Enter Description

Local Realm: None

Dynamic Access Policy: Hostscan

DefaultWEBVPNGroup

AnyConnect

AnyConnect-AD

Edit Connection Profile

Connection Profile:* AnyConnect-AD

Group Policy:* AnyConnect-Group

Edit Group Policy

Client Address Assignment | AAA | Aliases

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:

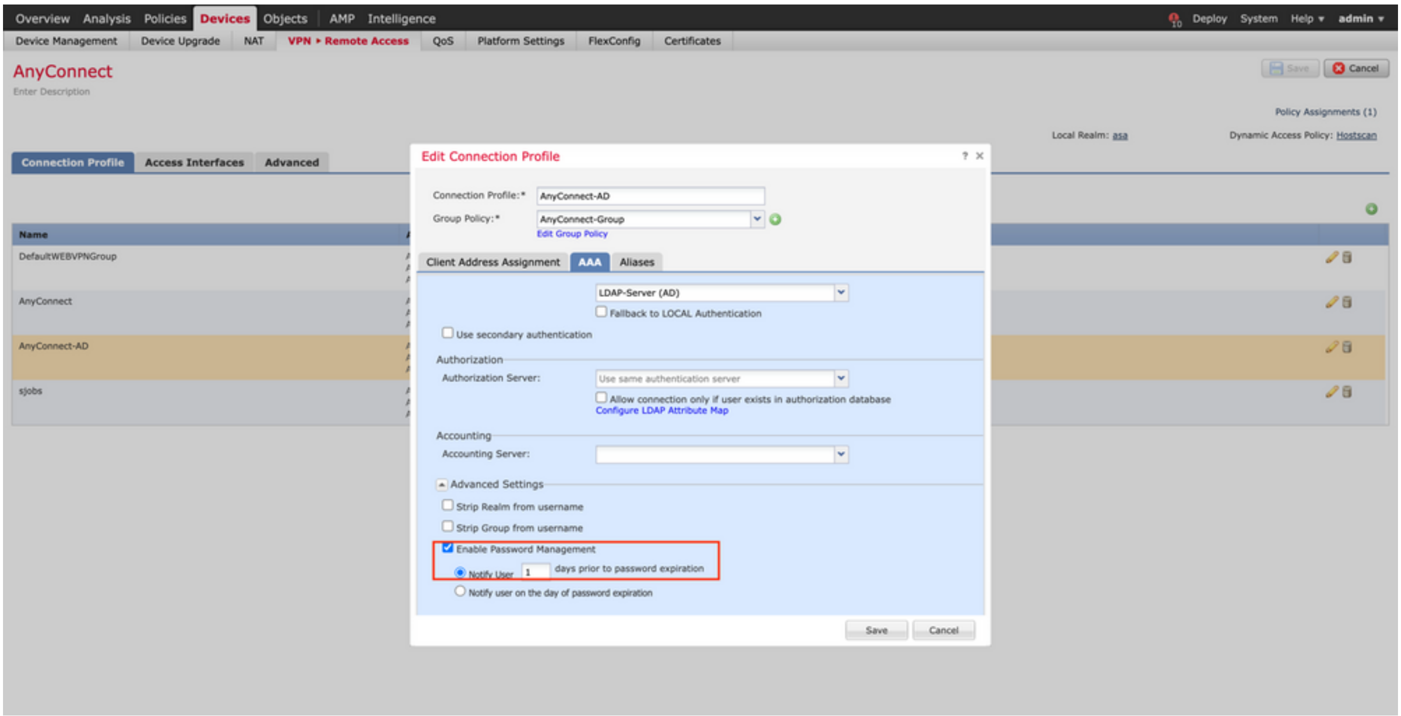
▾ Advanced Settings

□ Strip Realm from username

Cancel | Save

-

مكنت كلمة إدارة تحت ال AAA > Advanced Settingsوحفظ التشكيل.



AnyConnect

Enter Description

Local Realm: asa

Dynamic Access Policy: Hostscan

DefaultWEBVPNGroup

AnyConnect

AnyConnect-AD

sjobs

Edit Connection Profile

Connection Profile:* AnyConnect-AD

Group Policy:* AnyConnect-Group

Edit Group Policy

Client Address Assignment | AAA | Aliases

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

□ Strip Group from username

☑ Enable Password Management

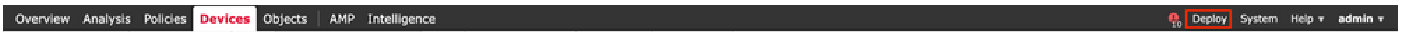
● Notify User 1 days prior to password expiration

○ Notify user on the day of password expiration

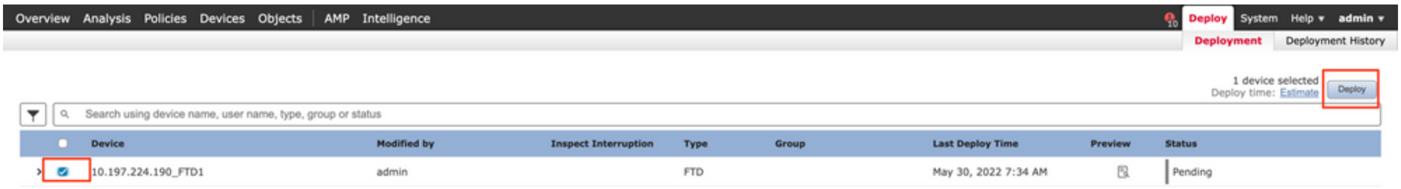
Save | Cancel

النشر

- ما إن يتم مع كل التشكيل، طقطقتDeploy الزر على الأعلى يمين.



- انقر فوق خانة الاختيار المجاورة لتكوين FTD المطبق عليها ثم انقر فوق Deploy، كما هو موضح في هذه الصورة:



☐	Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
☑	10.197.224.190_FTD1	admin		FTD		May 30, 2022 7:34 AM		Pending

الترتيب النهائي

هذا هو التكوين الذي يظهر في واجهة سطر الأوامر (CLI) الخاصة ب FTD بعد النشر الناجح.

تكوين 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
```

تكوين AnyConnect

<#root>

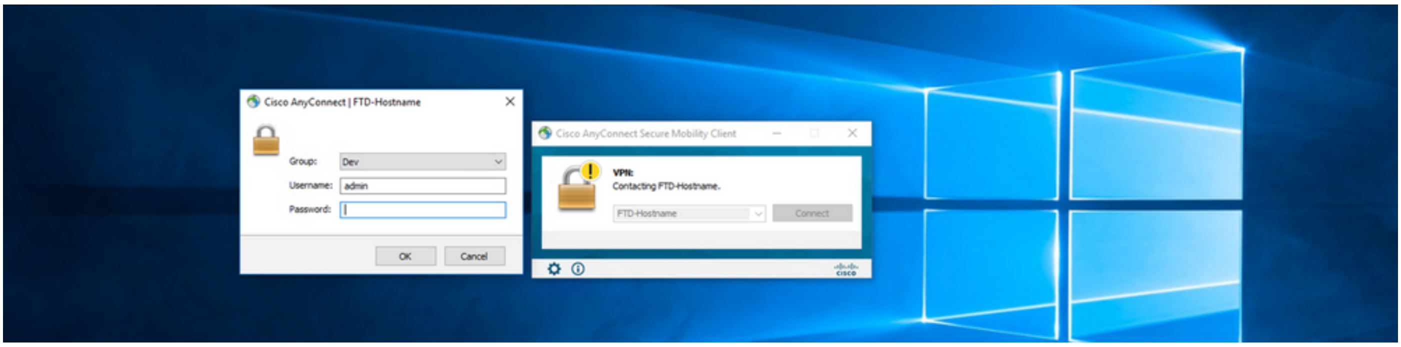
```
> show running-config webvpn


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
```

التحقق

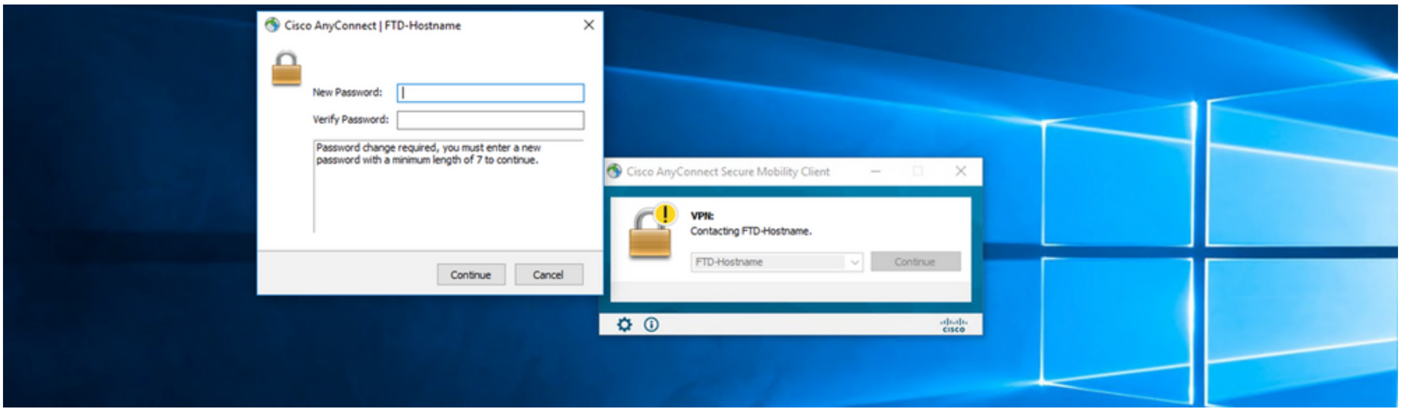
الاتصال ب AnyConnect والتحقق من عملية إدارة كلمة المرور لاتصال المستخدم

1. بدء اتصال بملف تعريف الاتصال المعني. بمجرد تحديد تغيير كلمة المرور عند تسجيل الدخول الأولي نظرا لأن كلمة المرور السابقة تم رفضها بواسطة Microsoft Server عند انتهاء صلاحيتها، تتم مطالبة المستخدم بتغيير كلمة المرور.


Cisco AnyConnect | FTD-Hostname
OK
Cancel
Cisco AnyConnect Secure Mobility Client
Connect

Group: Dev
Username: admin
Password:

VPN:
Contacting FTD-Hostname.
FTD-Hostname

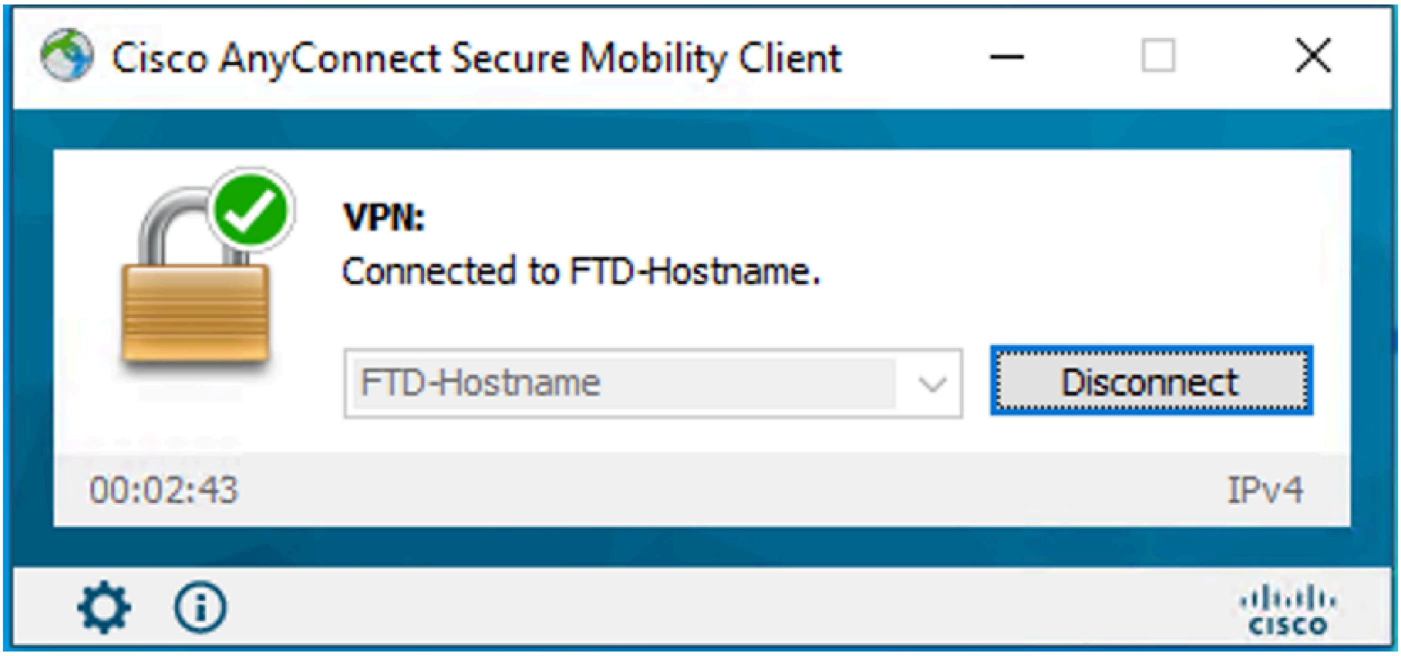

Cisco AnyConnect | FTD-Hostname
Continue
Cancel
Cisco AnyConnect Secure Mobility Client
Continue

New Password:
Verify Password:

Password change required, you must enter a new password with a minimum length of 7 to continue.

VPN:
Contacting FTD-Hostname.
FTD-Hostname

- بمجرد إدخال المستخدم لكلمة المرور الجديدة لتسجيل الدخول، يتم إنشاء الاتصال بنجاح.



VPN:
Connected to FTD-Hostname.
FTD-Hostname
00:02:43
IPv4

- التحقق من اتصال المستخدم على واجهة سطر الأوامر (CLI) ل 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
```

استكشاف الأخطاء وإصلاحها

تصحيح الأخطاء

يمكن تشغيل تصحيح الأخطاء هذا في CLI تشخيصي لاستكشاف أخطاء إدارة كلمة المرور وإصلاحها: **debug ldap 255**.

عمليات تصحيح أخطاء إدارة كلمة المرور العاملة

```
<#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
```

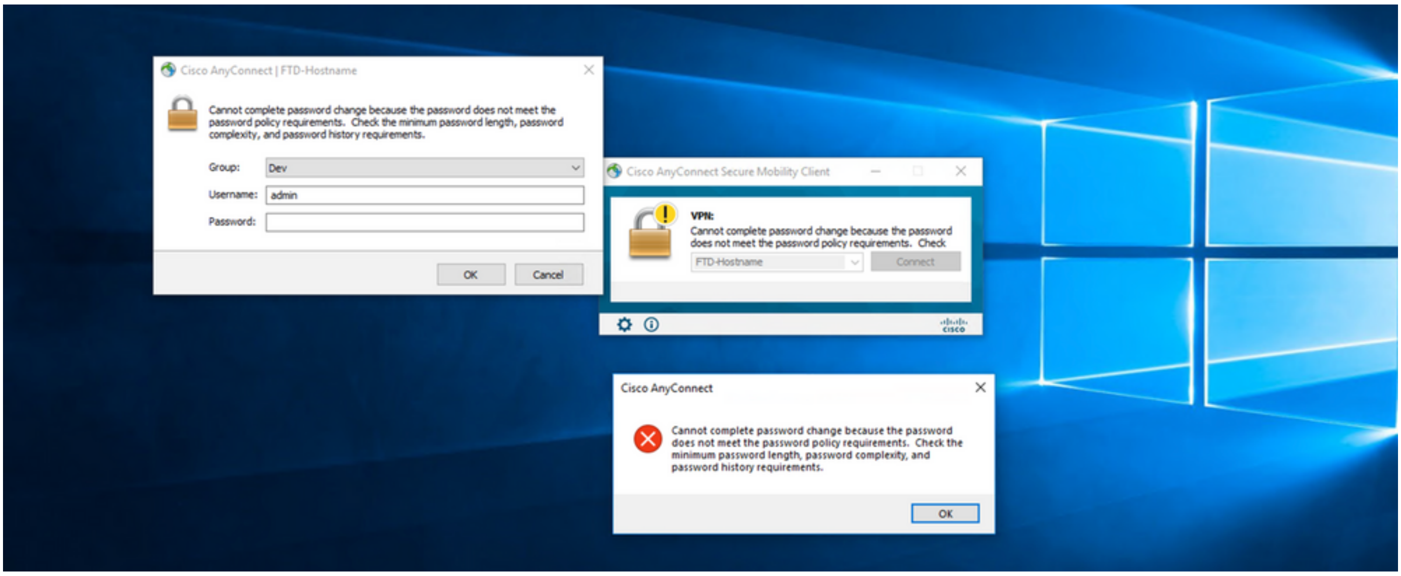
```
[24] Performing Simple authentication for admin to 10.106.71.234

[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
```

الأخطاء الشائعة التي تمت مصادفتها أثناء إدارة كلمة المرور

عادة، إذا لم يتم الوفاء بنهج كلمة المرور الذي تم تعيينه بواسطة Microsoft Server خلال الوقت الذي يقوم فيه المستخدم بتوفير كلمة المرور الجديدة، يتم إنهاء الاتصال بالخطأ "لا تفي كلمة المرور بمتطلبات نهج كلمة المرور". وبالتالي، تأكد من تطابق كلمة المرور الجديدة مع النهج الذي تم تعيينه بواسطة Microsoft Server ل LDAPs.



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
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.

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).