Configuración de la administración de contraseñas mediante LDAPs para VPN de RA en FTD administrado por FMC

Contenido

Introducción

Este documento describe la configuración de la administración de contraseñas mediante LDAP para los clientes de AnyConnect que se conectan a Cisco Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- Conocimiento básico de la configuración de VPN (red privada virtual de acceso remoto) de RA en FMC
- Conocimiento básico de la configuración del servidor LDAP en FMC
- Conocimientos básicos de Active Directory

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor Microsoft 2012 R2
- FMCv con 7.3.0
- FTDv con 7.3.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración

Diagrama y escenario de la red

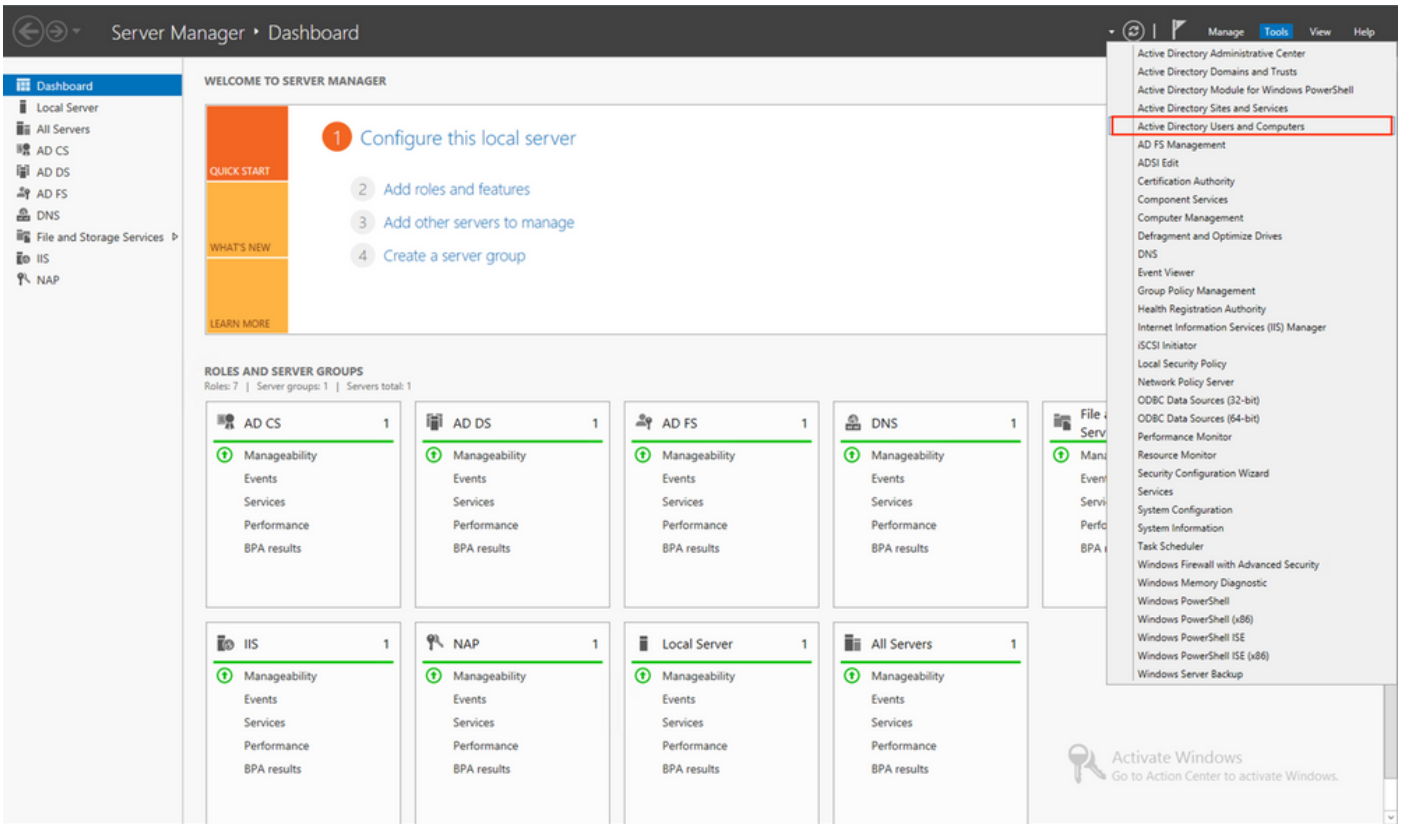
Windows Server está preconfigurado con ADDS y ADCS para probar el proceso de administración de contraseñas de usuario. En esta guía de configuración, se crean estas cuentas de usuario.

Cuentas de usuario:

- Administrador: se utiliza como cuenta de directorio para permitir que el FTD se enlace al servidor de Active Directory.
- admin: cuenta de administrador de prueba utilizada para demostrar la identidad del usuario.

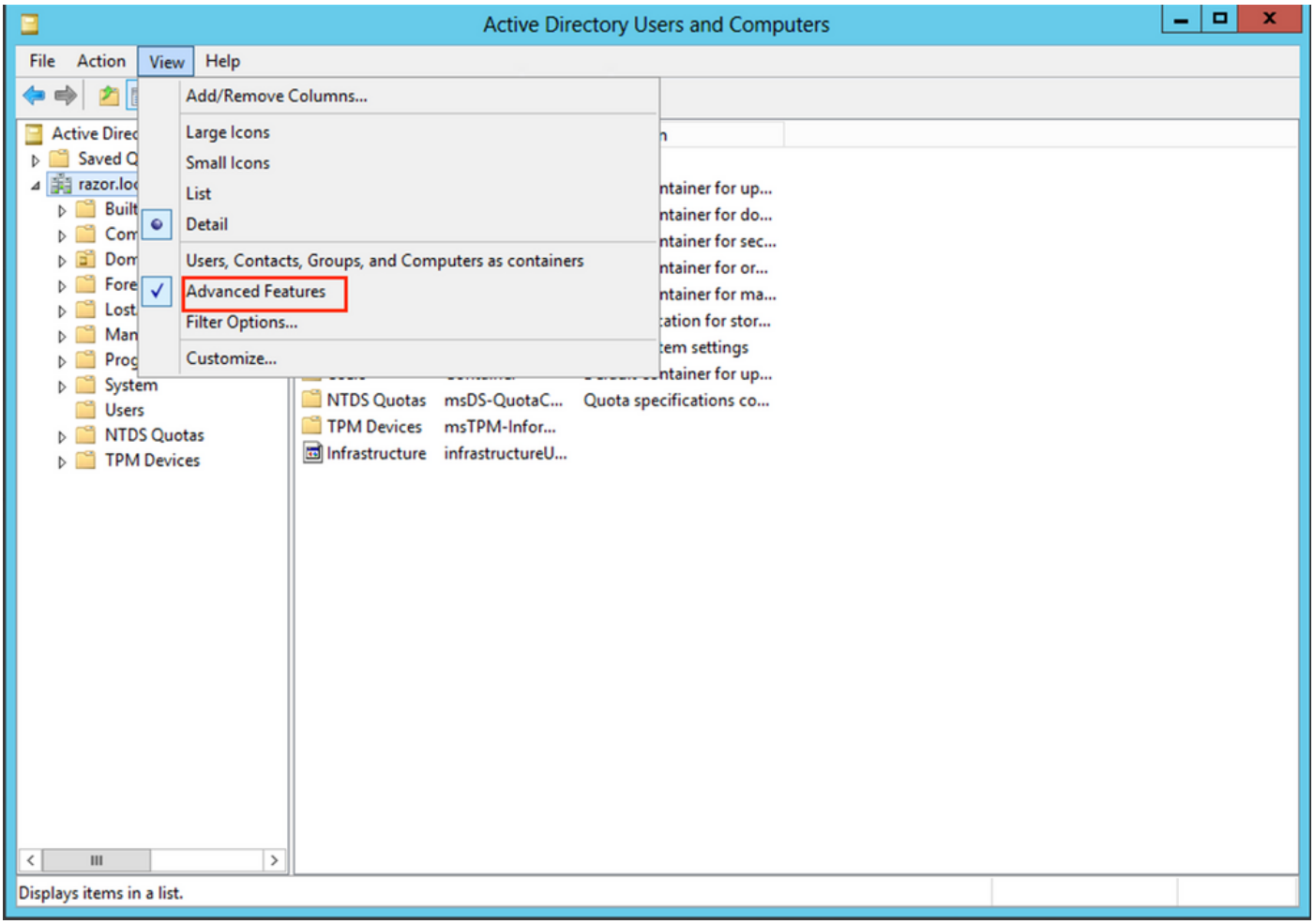
Determinar DN Base LDAP y DN de Grupo

1. Abra Active Directory Users and Computers a través del panel del Administrador del servidor.



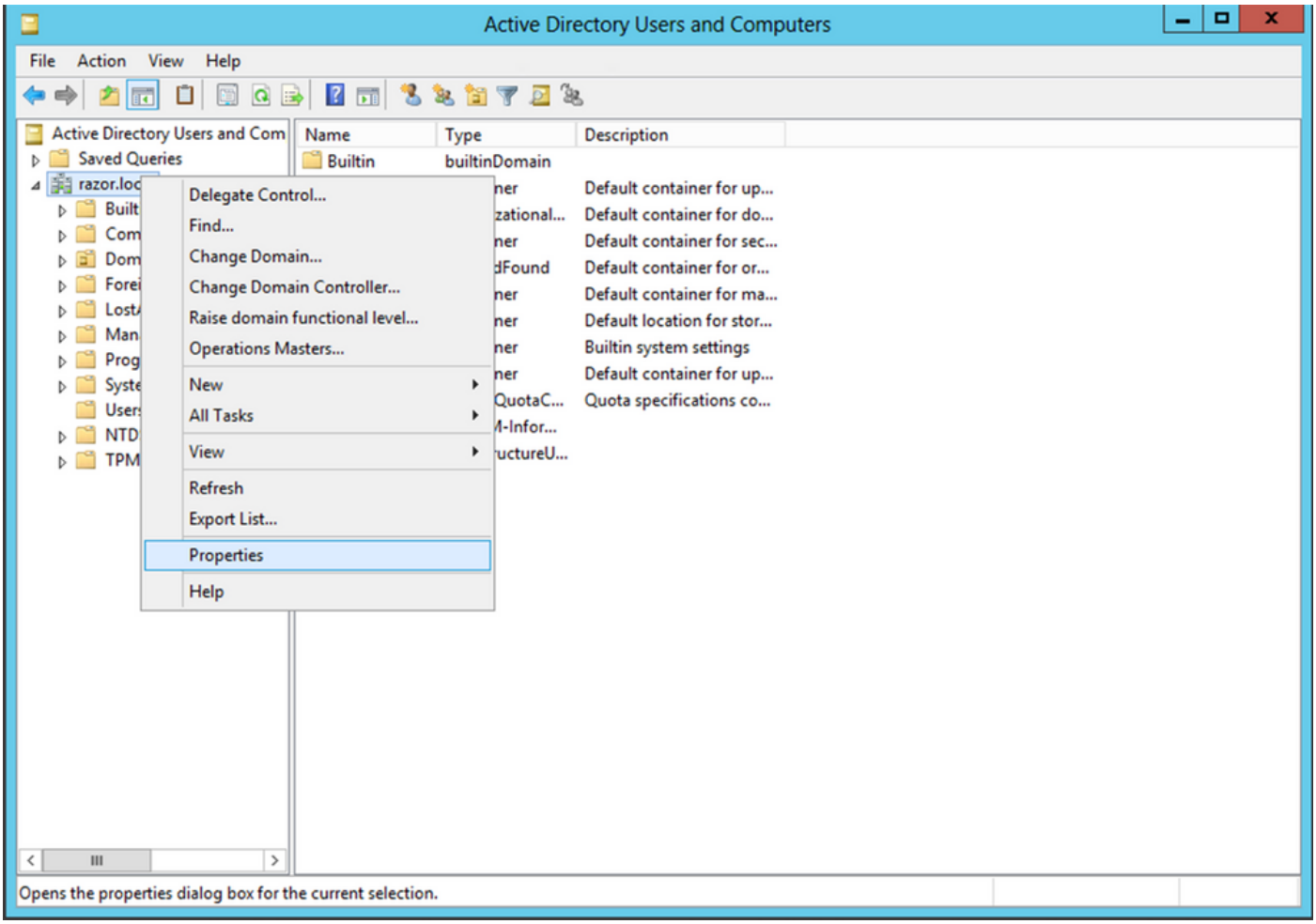
-

Abra el View Option en el panel superior y habilite el Advanced Features, como se muestra en la imagen:



-

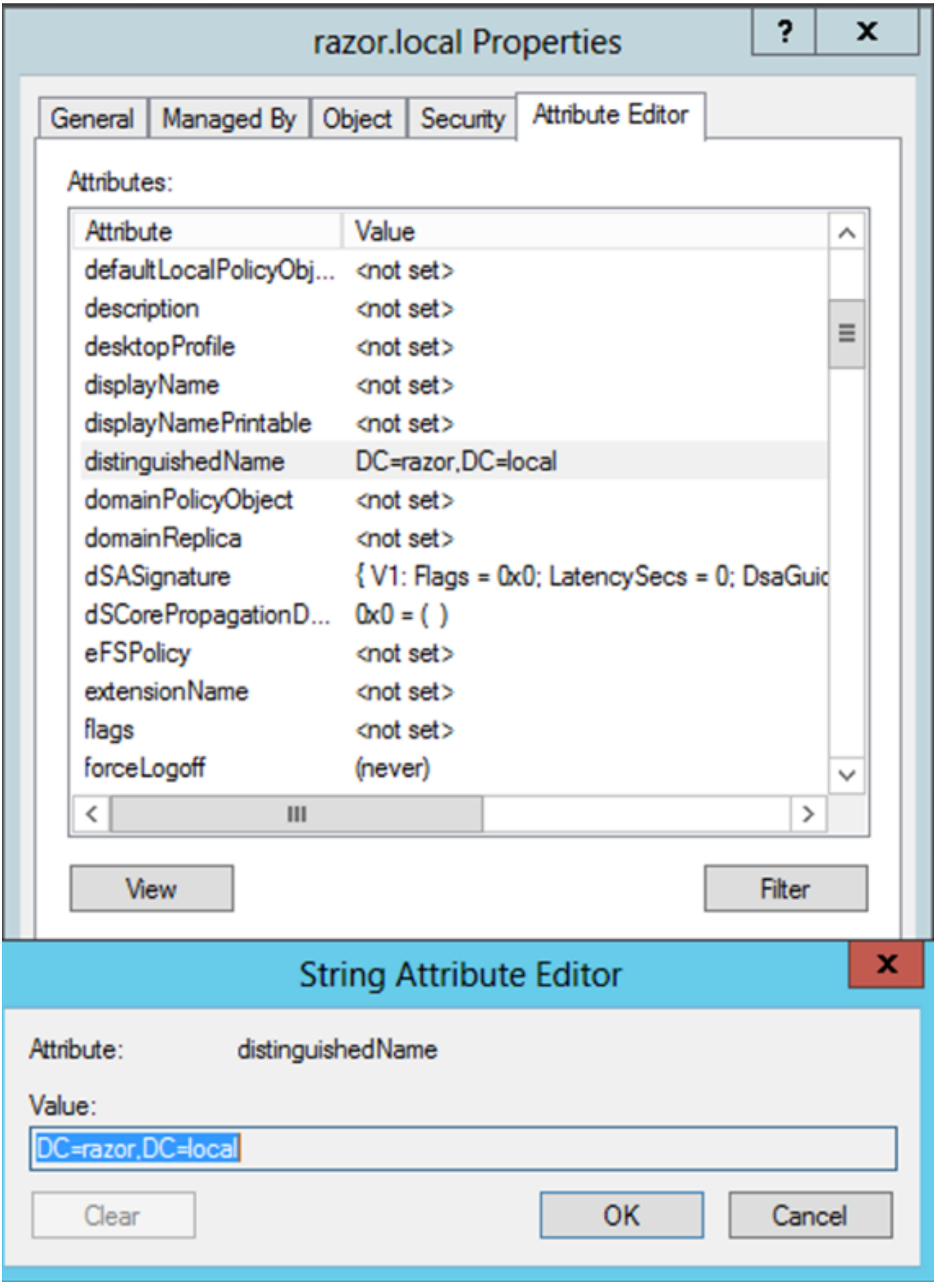
Esto permite ver propiedades adicionales debajo de los objetos de AD.
Por ejemplo, para buscar el DN para la raízrazor.local, haga clic con el botón derecho razor.local y luego elija Properties, como se muestra en esta imagen:



- En Properties, elija la Attribute Editor ficha. Busque distinguishedName en Atributos y, a continuación, haga clic en View, como se muestra en la imagen.

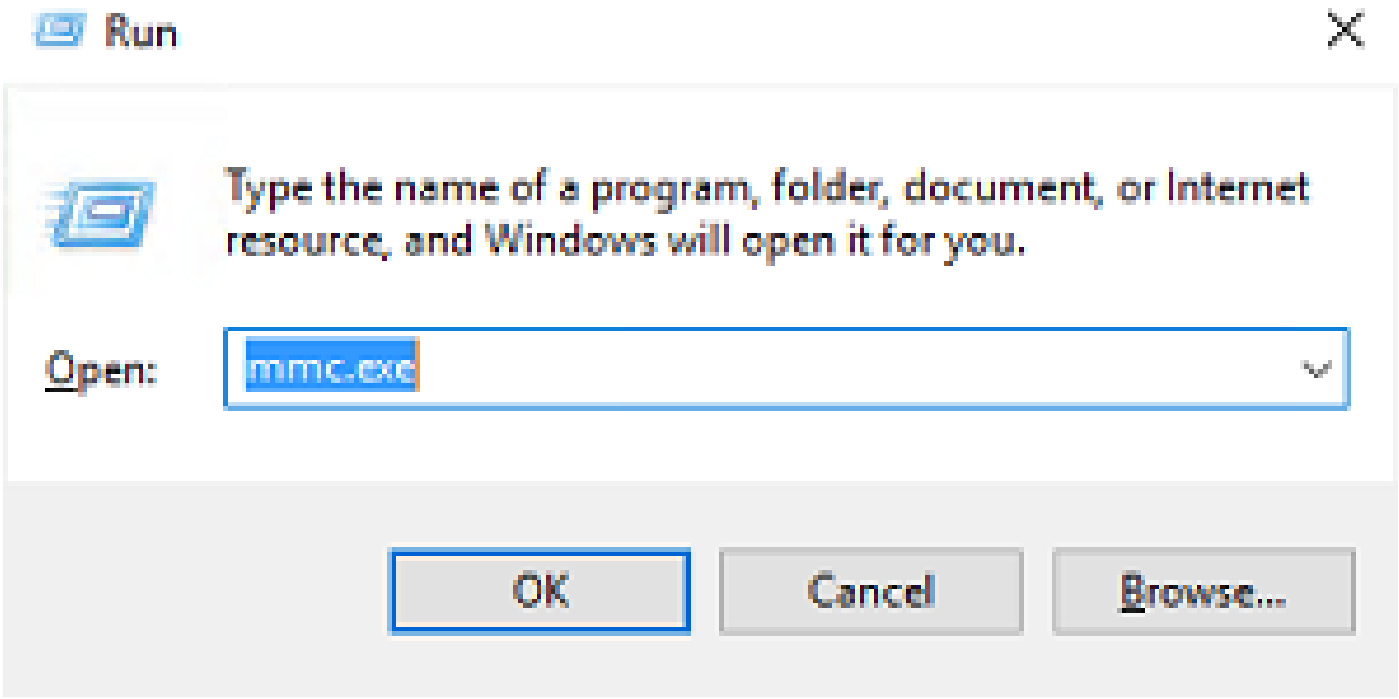
Esto abre una nueva ventana donde el DN se puede copiar y pegar en FMC más adelante.

En este ejemplo, el DN raíz es DC=razor, DC=local. Copie el valor y guárdelo para más tarde. Haga clic OK para salir de la ventana Editor de atributos de cadena y haga clic OK nuevamente para salir de Propiedades.

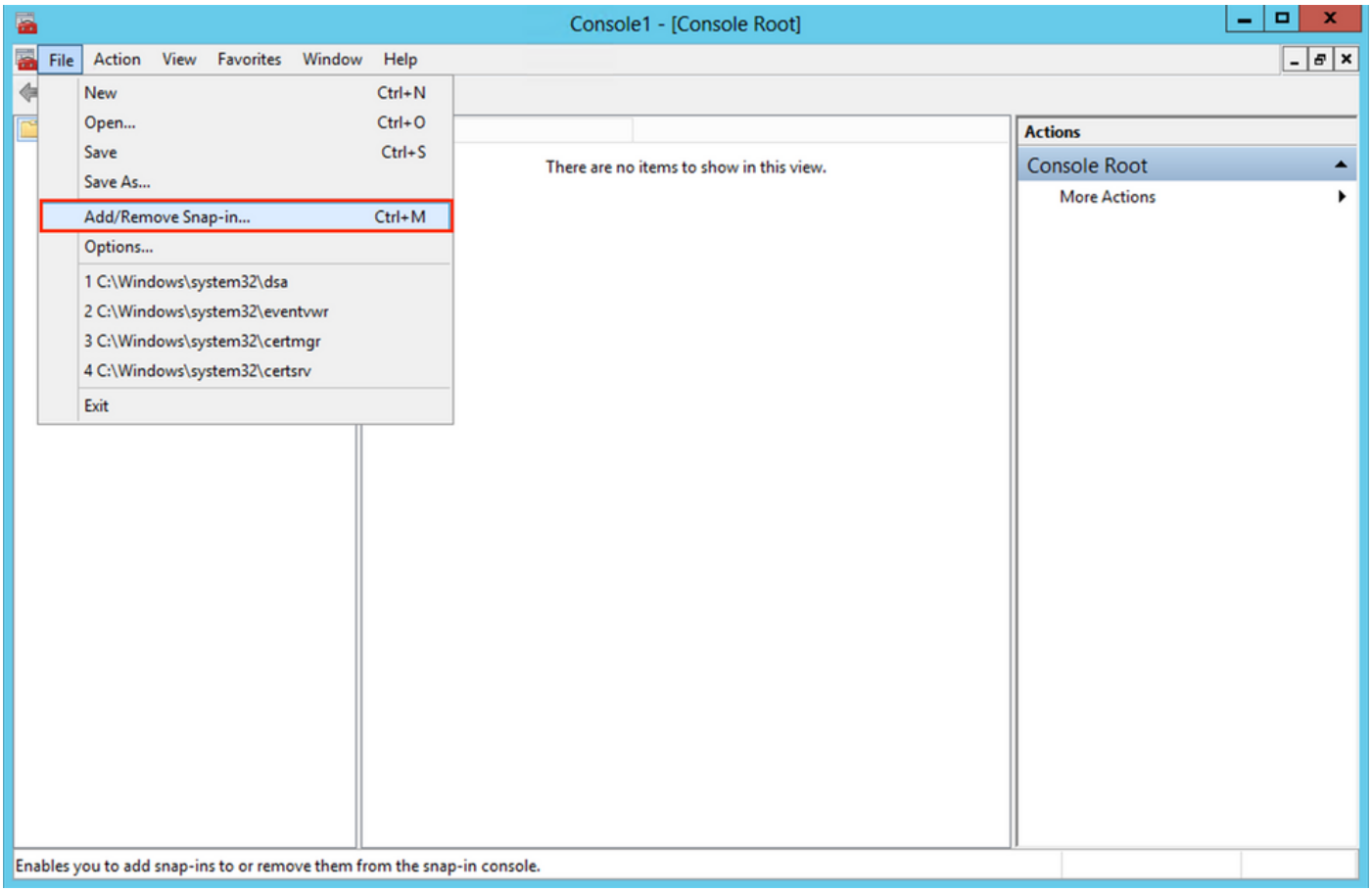

razor.local Properties
General
Managed By
Object
Security
Attribute Editor
Attributes:
Attribute
Value
defaultLocalPolicyObj...
<not set>
description
<not set>
desktopProfile
<not set>
displayName
<not set>
displayNamePrintable
<not set>
distinguishedName
DC=razor,DC=local
domainPolicyObject
<not set>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

Copiar la raíz del certificado SSL LDAPS

- Presione Win+R e ingrese mmc.exe, luego haga clic en OK, como se muestra en esta imagen.

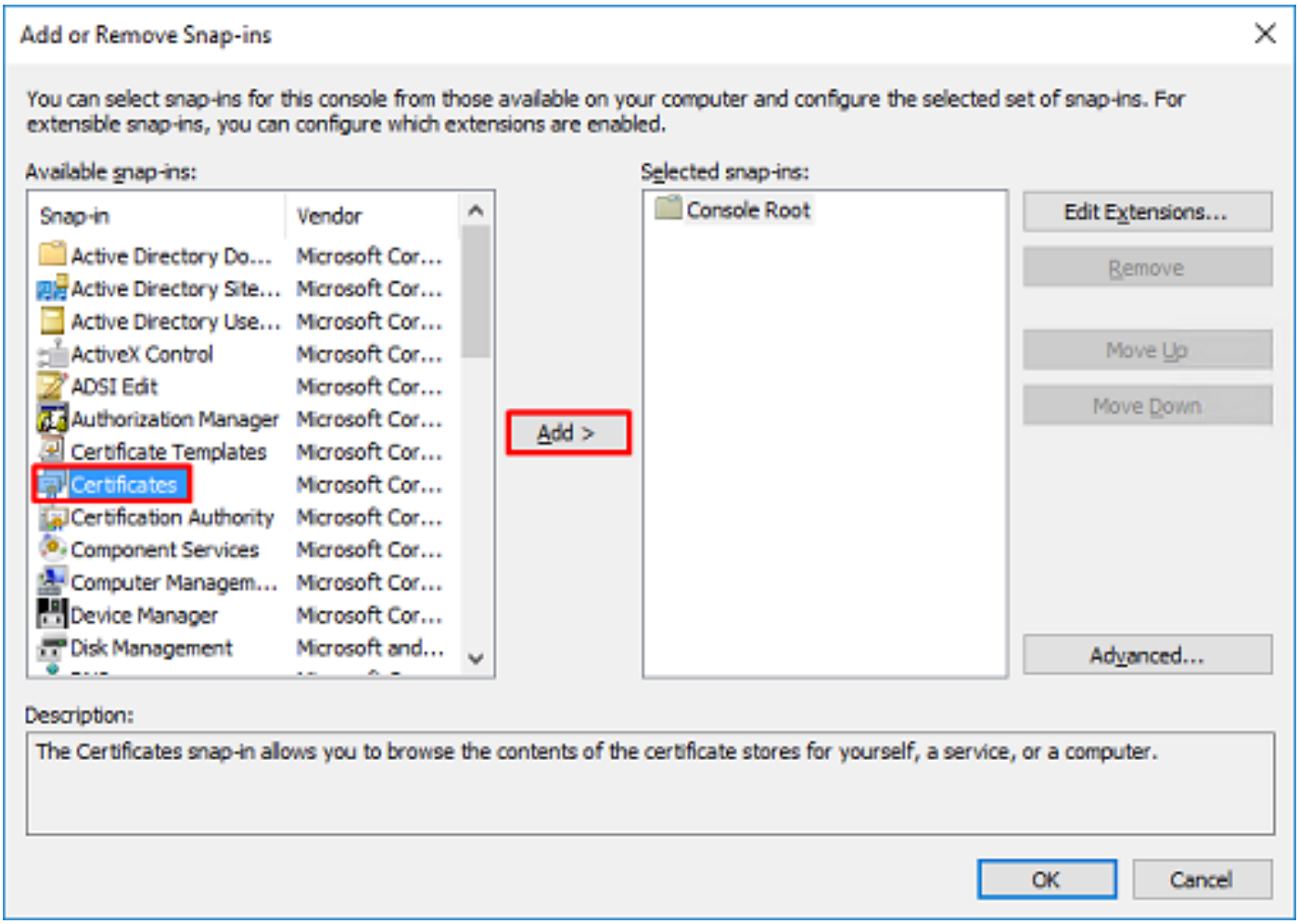


- Navegue hasta File > Add/Remove Snap-in..., como se muestra en esta imagen:



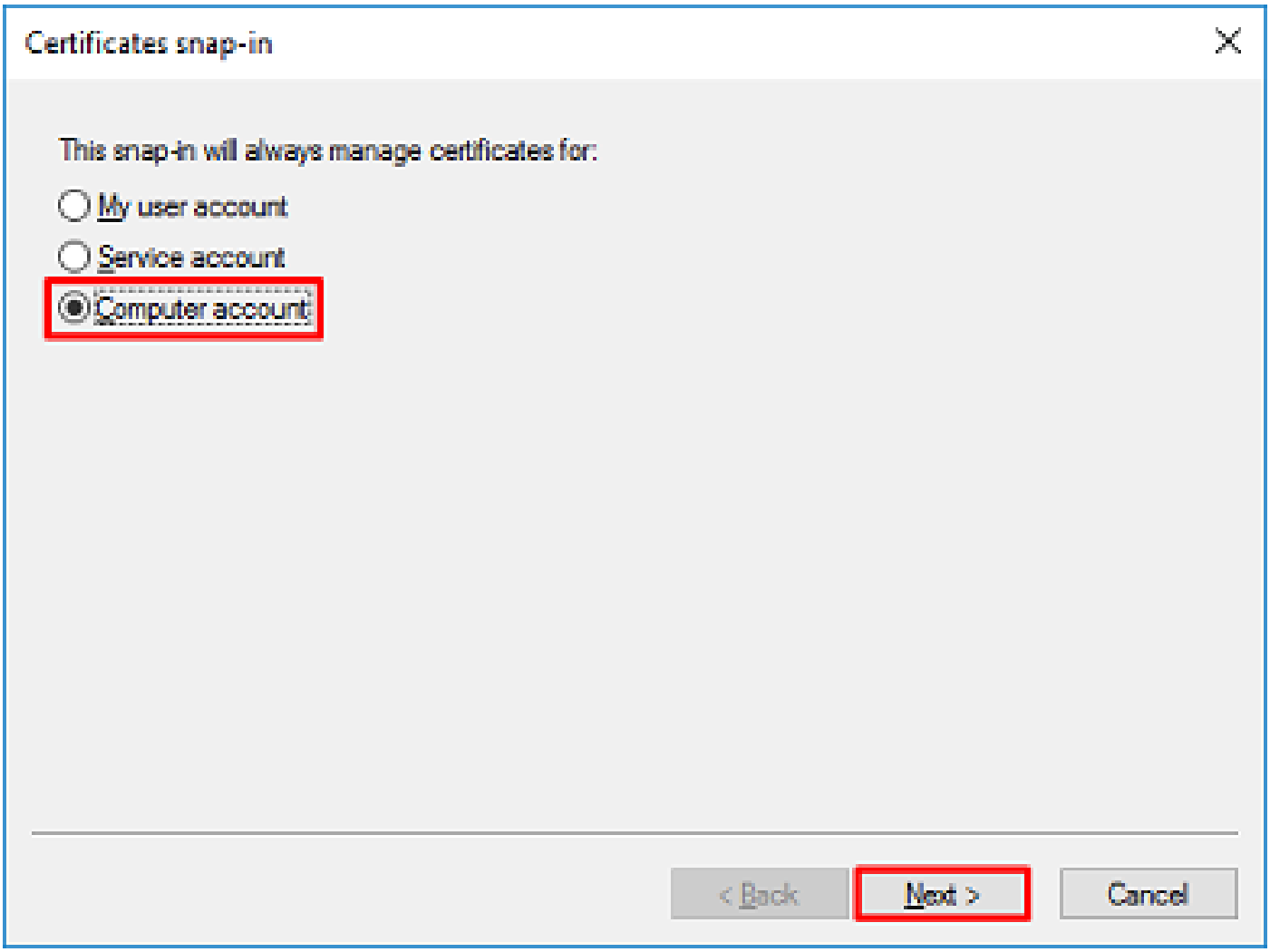
-

En complementos disponibles, elija Certificates y haga clic en Add, como se muestra en esta imagen:

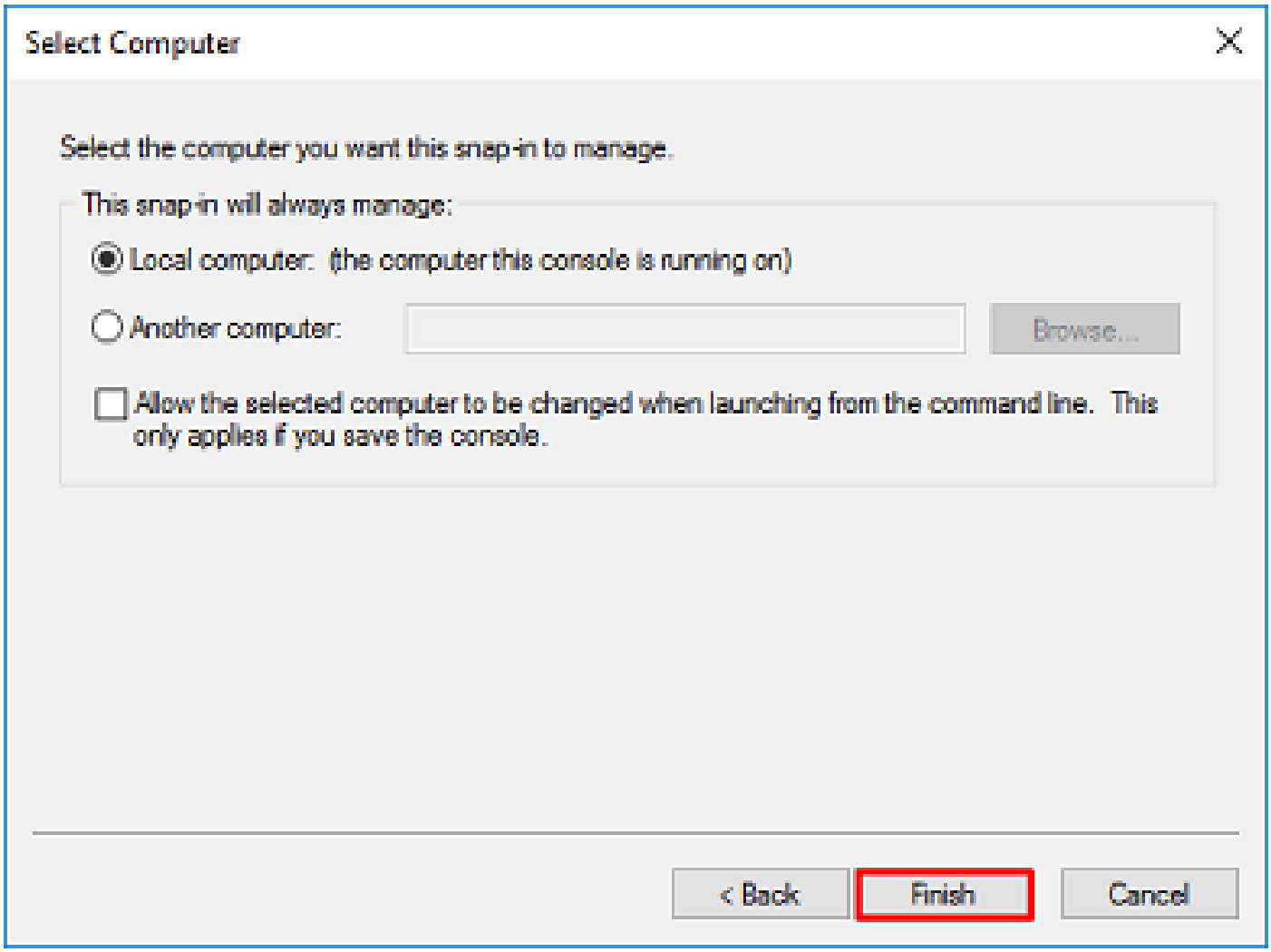


-

Elija Computer account y luego haga clic Next, como se muestra en esta imagen:

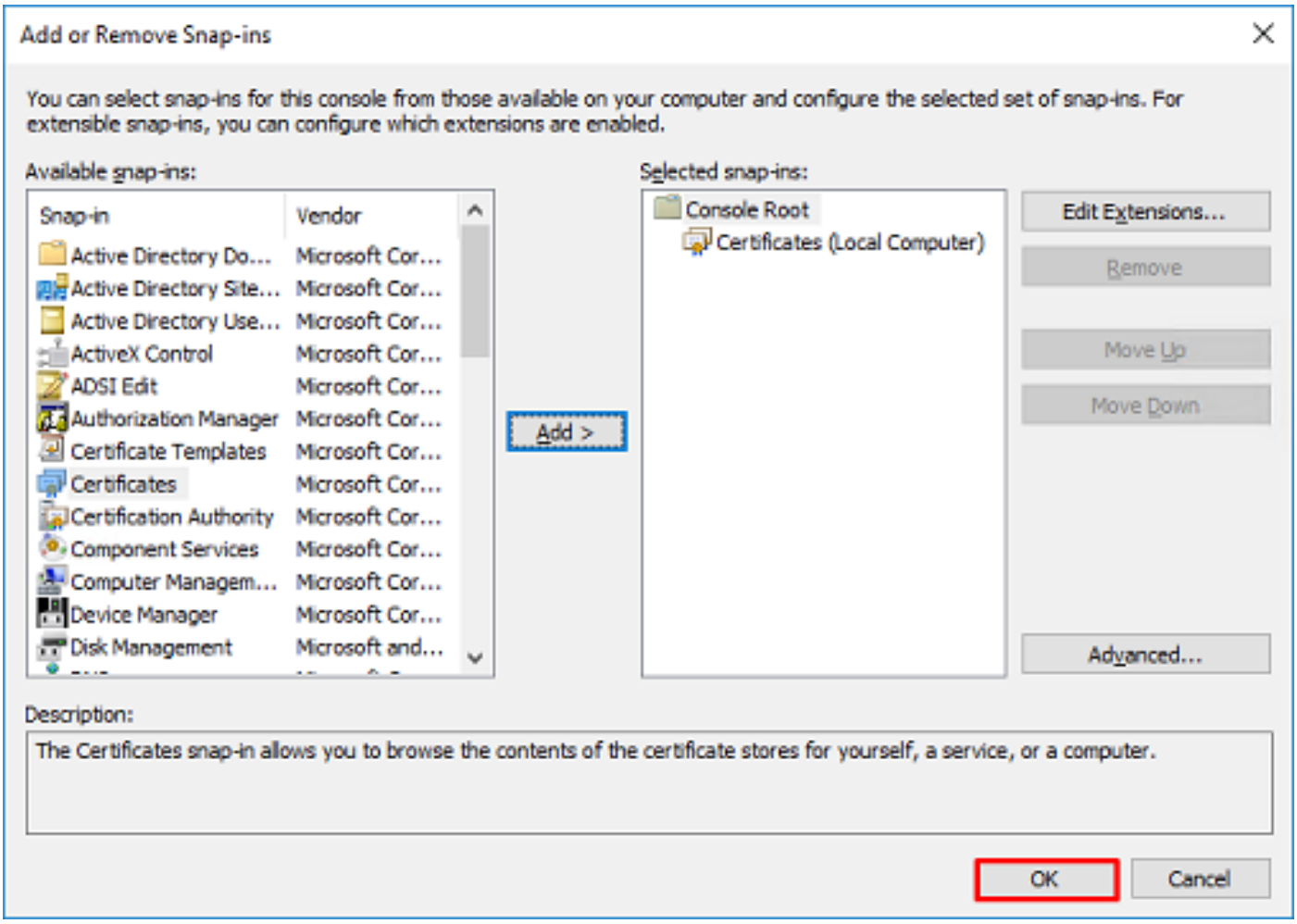


Como se muestra aquí, haga clic en Finish.



-

Ahora, haga clic OK, como se muestra en esta imagen.



- Expanda la Personal carpeta y haga clic en Certificates. El certificado utilizado por LDAP debe emitirse con el nombre de dominio completo (FQDN) del servidor de Windows. En este servidor, hay tres certificados enumerados:

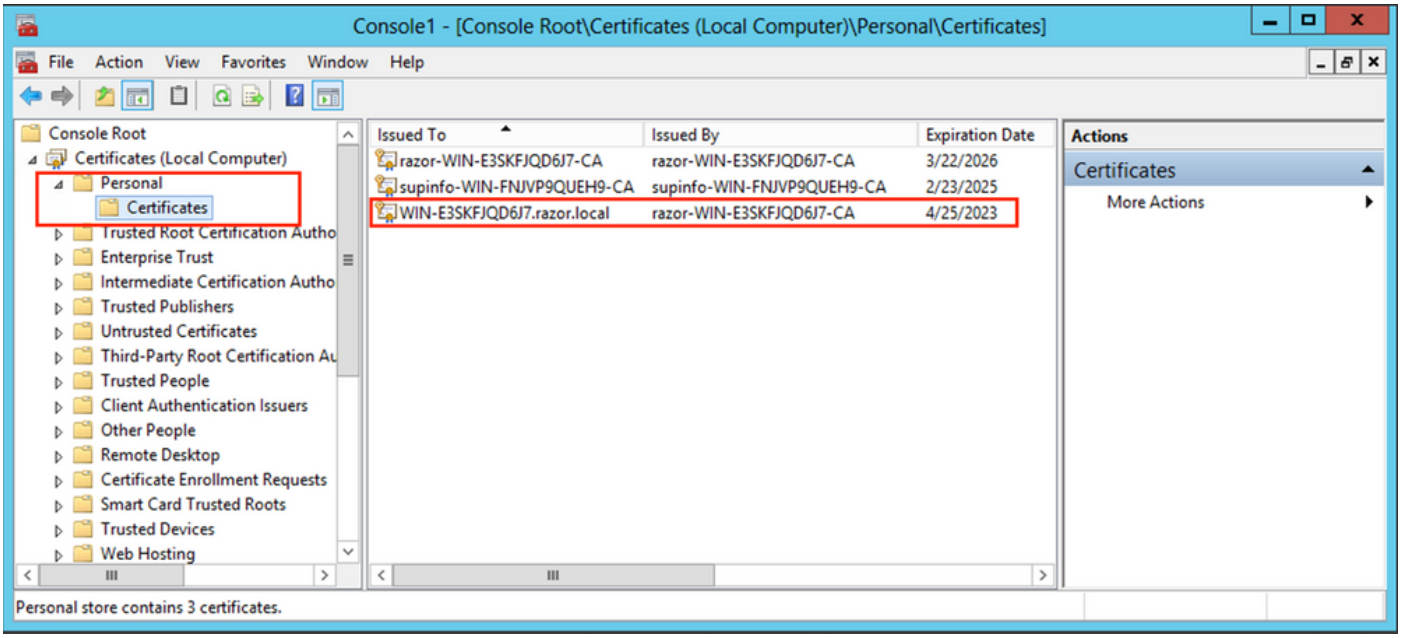
- Se ha emitido un certificado de CA a y por razor-WIN-E3SKFJQD6J7-CA.

- Certificado de CA emitido a y por supinfo-WIN-FNJVP9QUEH9-CA.

- Ha emitido un certificado de identidad WIN-E3SKFJQD6J7.razor.local para razor-WIN-E3SKFJQD6J7-CA.

En esta guía de configuración, el FQDN es WIN-E3SKFJQD6J7.razor.local y, por lo tanto, los dos primeros certificados no son válidos para su

uso como certificado SSL de LDAPs. El certificado de identidad emitido para WIN-E3SKFJQD6J7.razor.local es un certificado emitido automáticamente por el servicio de CA de Windows Server. Haga doble clic en el certificado para verificar los detalles.

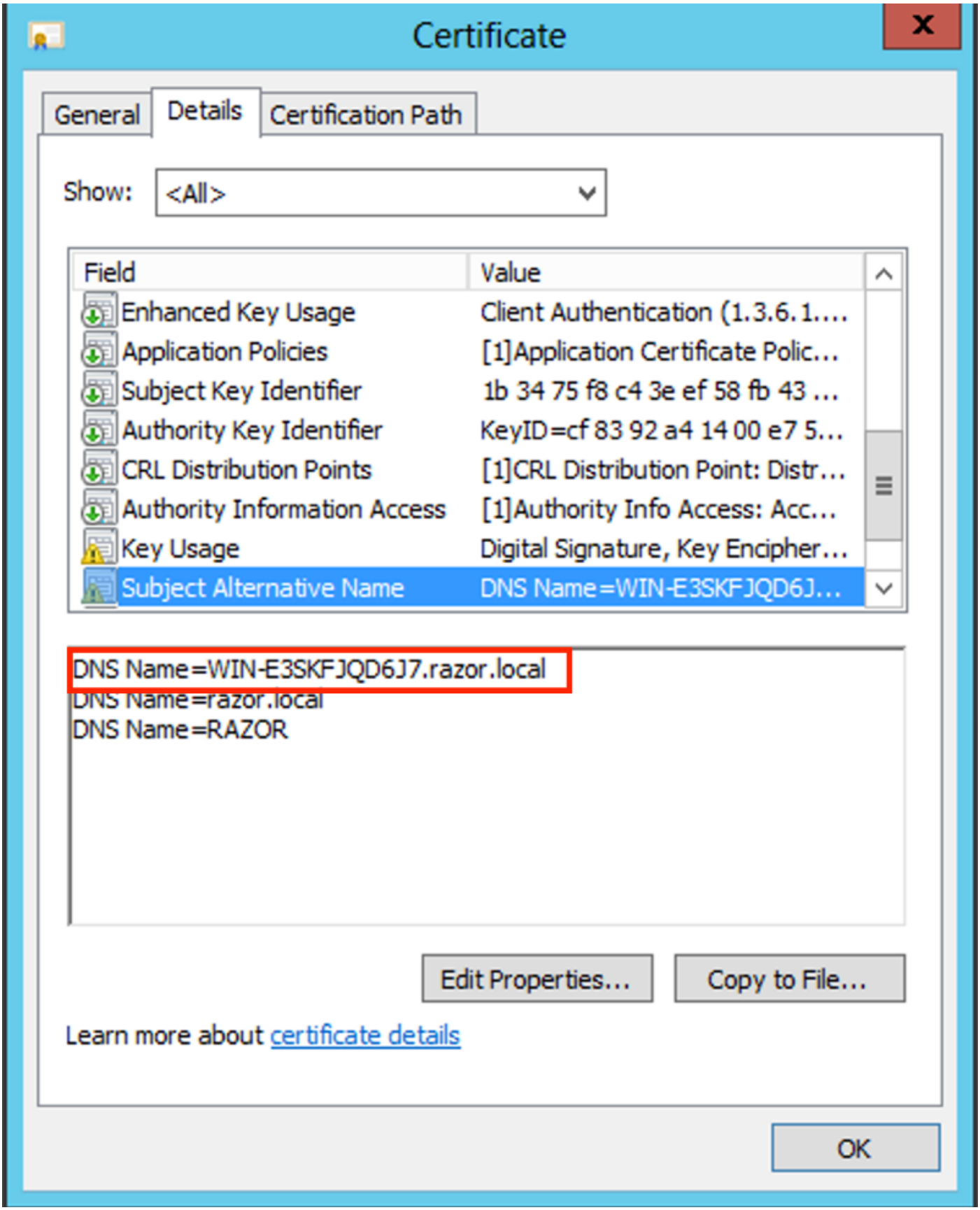


- Para ser utilizado como certificado SSL de LDAPs, el certificado debe cumplir con estos requisitos:

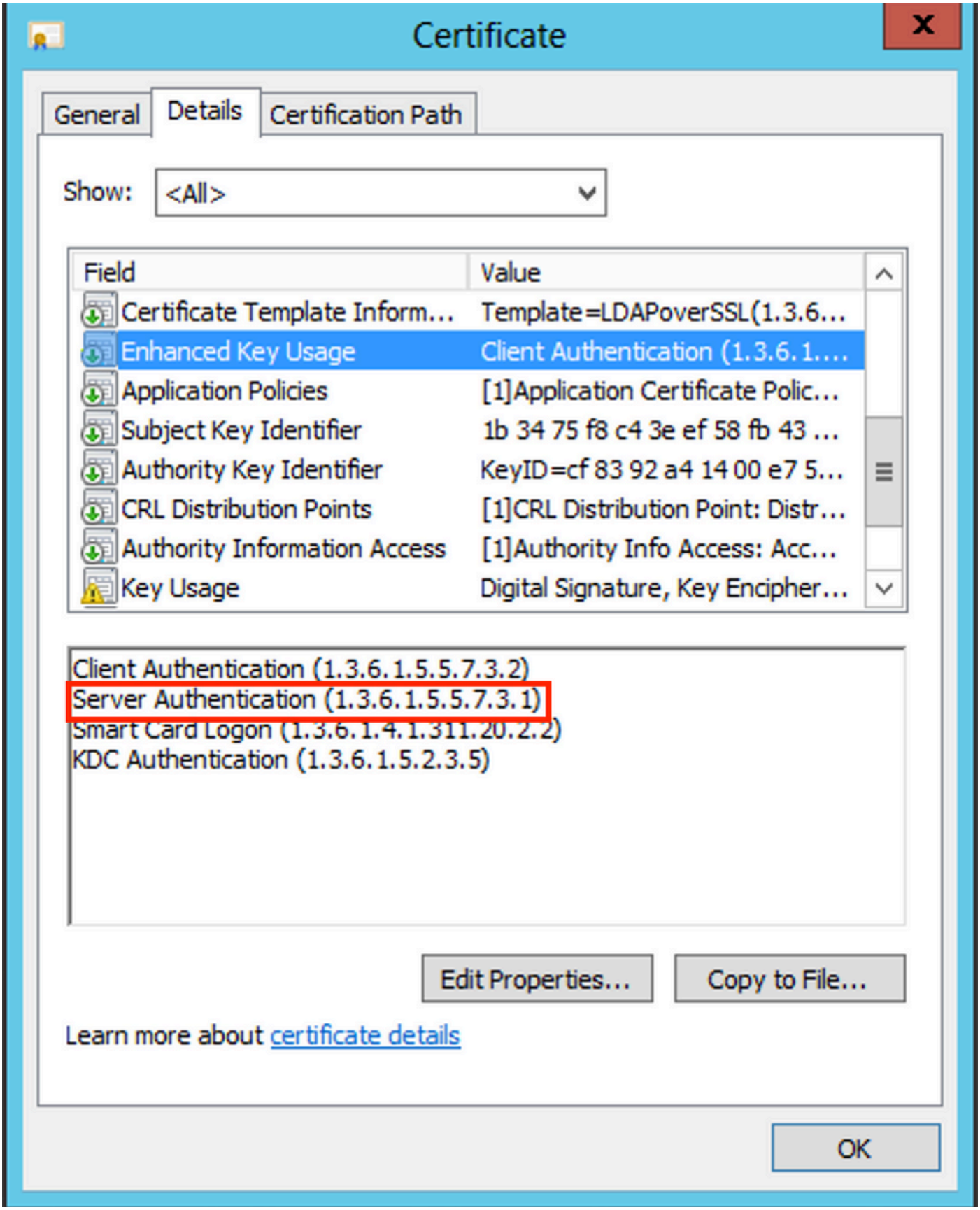
- El nombre común o el nombre alternativo de asunto DNS coincide con el FQDN del servidor de Windows.

- El certificado tiene autenticación de servidor en el campo Enhanced Key Usage (Uso mejorado de clave).

En la Details ficha del certificado, elija Subject Alternative Name, donde WIN-E3SKFJQD6J7.razor.local aparece el FQDN.

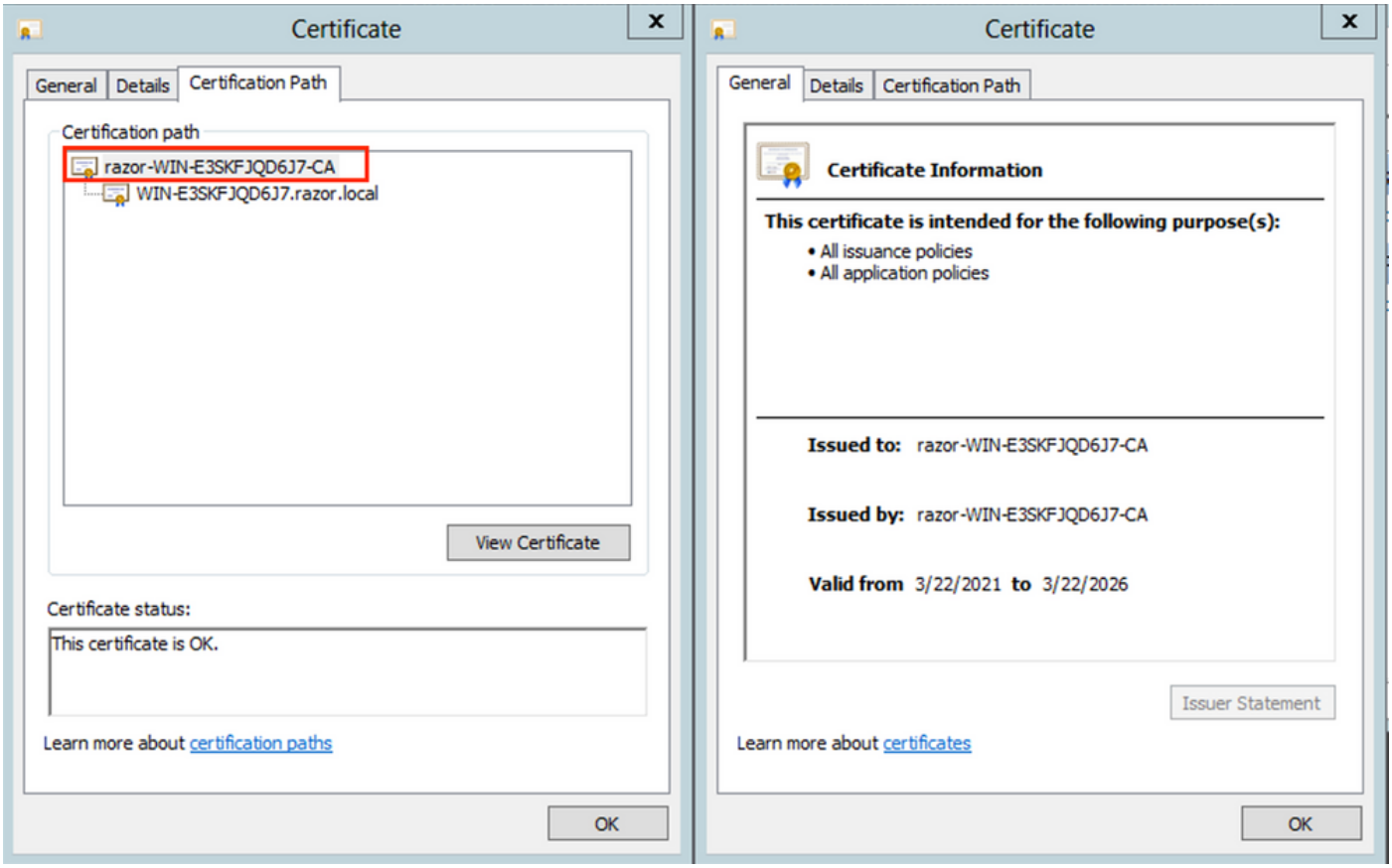


Debajo Enhanced Key Usage, Server Authentication está presente.



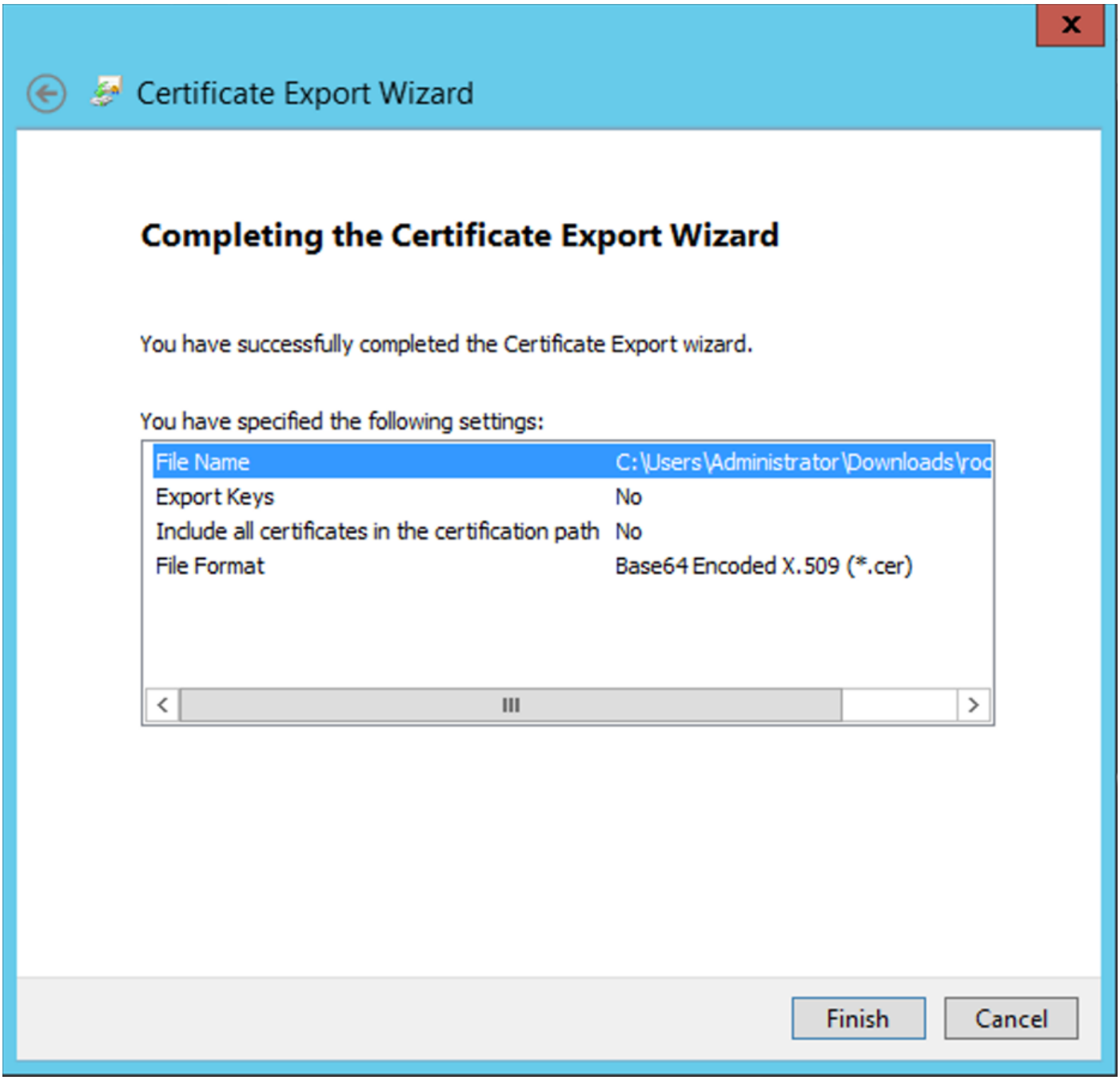
•

Una vez confirmado, en la Certification Path ficha, elija el certificado de nivel superior que es el certificado de CA raíz y, a continuación, haga clic en View Certificate. Esto abre los detalles del certificado para el certificado de CA raíz como se muestra en la imagen:



- En la Details ficha del certificado de la CA raíz, haga clic en Copy to File y navegue por lasCertificate Export Wizard que exporta la CA raíz en formato PEM.

Elija Base-64 encoded X.509 como formato de archivo.



- Abra el certificado de CA raíz almacenado en la ubicación seleccionada en el equipo con un bloc de notas u otro editor de texto.

Muestra el certificado de formato PEM. Guarde esto para más tarde.

-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgoJ
vcjEhMB8GA1UEAxMYcmF6b3ItV0lOLUUzU0tGSlFENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMG
BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvcN
CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnblxwtXOB2G4UxZ3LRrWznjXaS02Rc3qVw4lnOAziGs4ZMNM1X8UWeKuwi8QZQljJt
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-----

En caso de tener varios certificados instalados en el almacén del equipo local en el servidor LDAPs (opcional)

1. En una situación de múltiples certificados de identidad que pueden ser utilizados por LDAPS y cuando hay incertidumbre sobre cuál se utiliza, o no hay acceso al servidor LDAPS, todavía es posible extraer la CA raíz de una captura de paquetes realizada en el FTD.

2. En el caso de que tenga varios certificados válidos para Autenticación de servidor en el almacén de certificados del equipo local del servidor LDAP (como el controlador de dominio AD DS), se puede observar que se utiliza un certificado diferente para las comunicaciones LDAP. La mejor solución para este problema es quitar todos los certificados innecesarios del almacén de certificados del equipo local y tener sólo un certificado válido para la autenticación del servidor.

Sin embargo, si hay un motivo legítimo para que necesite dos o más certificados y tenga al menos un servidor LDAP de Windows Server 2008, se puede utilizar el almacén de certificados de Servicios de dominio de Active Directory (NTDS\Personal) para las comunicaciones LDAP.

Estos pasos muestran cómo exportar un certificado habilitado para LDAPS desde un almacén de certificados de equipo local del controlador de dominio al almacén de certificados del servicio de Servicios de dominio de Active Directory (NTDS\Personal).

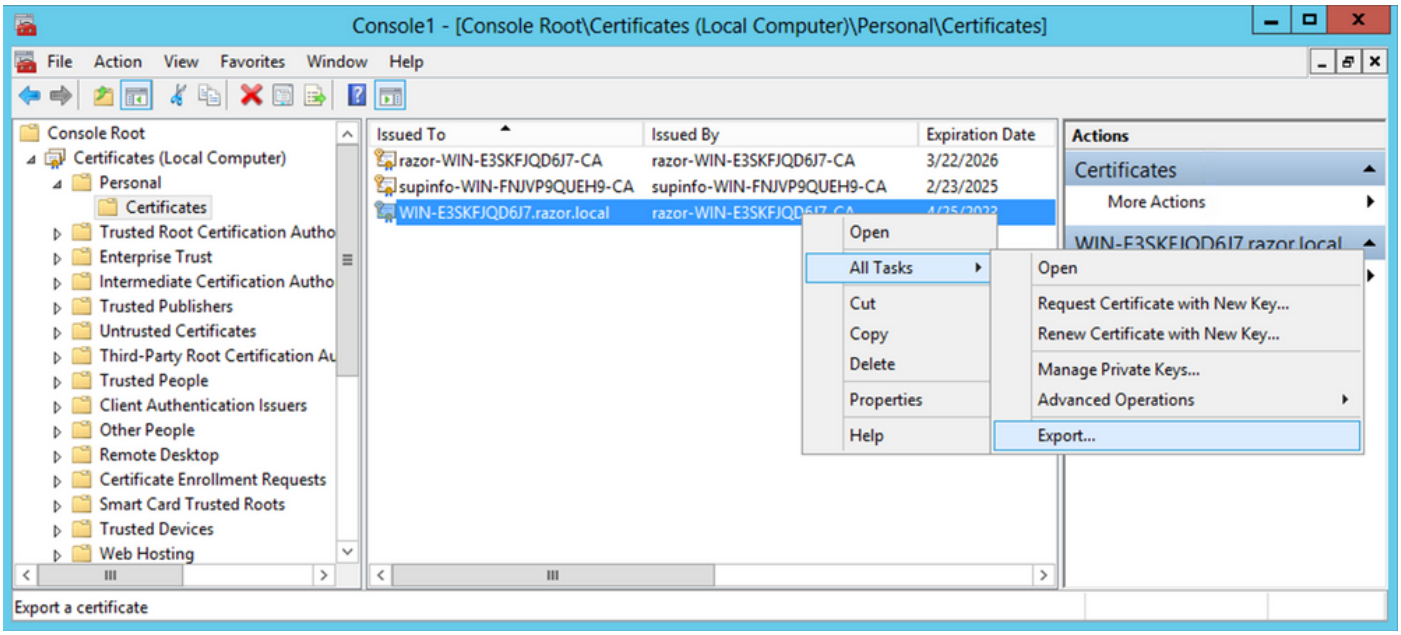
- Vaya a la consola de MMC en el servidor de Active Directory, elija Archivo y, a continuación, haga clic en Add/Remove Snap-in.

- Haga clic Certificates y, a continuación, haga clic en Add.

- En la Certificates snap-in, elija Computer account y, a continuación, haga clic en Next.

- En Select Computer, elija Local Computer, haga clic en OK y, a continuación, haga clic en Finish. En Add or Remove Snap-ins, haga clic en OK.

- En la consola de certificados de un equipo que contiene un certificado utilizado para la Autenticación de servidor, haga clic con el botón secundario del mouse en el certificate, haga clic en All Tasks y, a continuación, haga clic en Export.



- Exporte el certificado en el pfx formato de las secciones siguientes. Consulte este artículo sobre cómo exportar un certificado en el pfx formato de MMC:

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

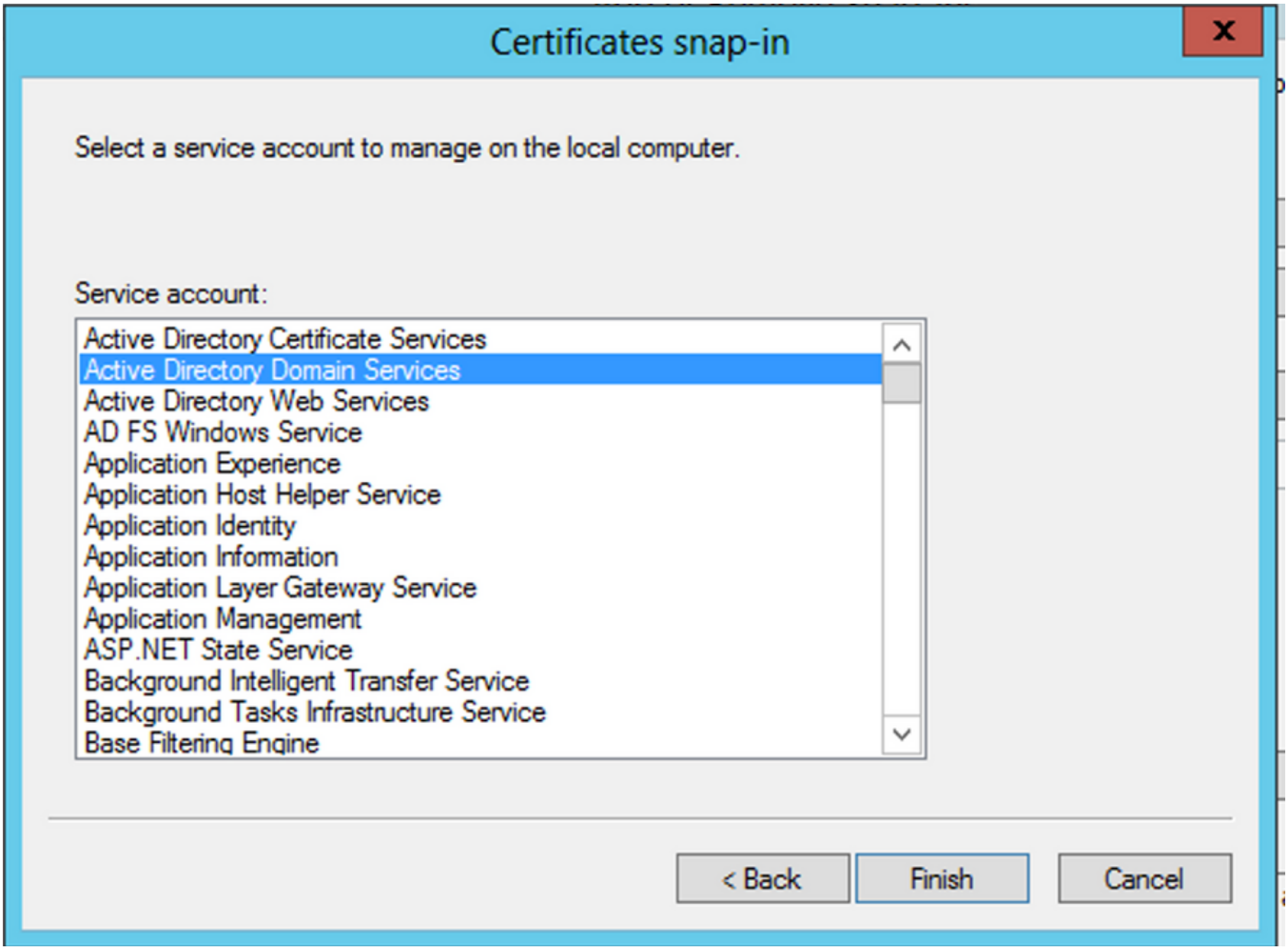
-

Una vez que haya finalizado la exportación del certificado, navegue hasta Add/Remove Snap-in en MMC console. Haga clic Certificates y, a continuación, haga clic en Add.

-

Elija Service account y haga clic en Next.

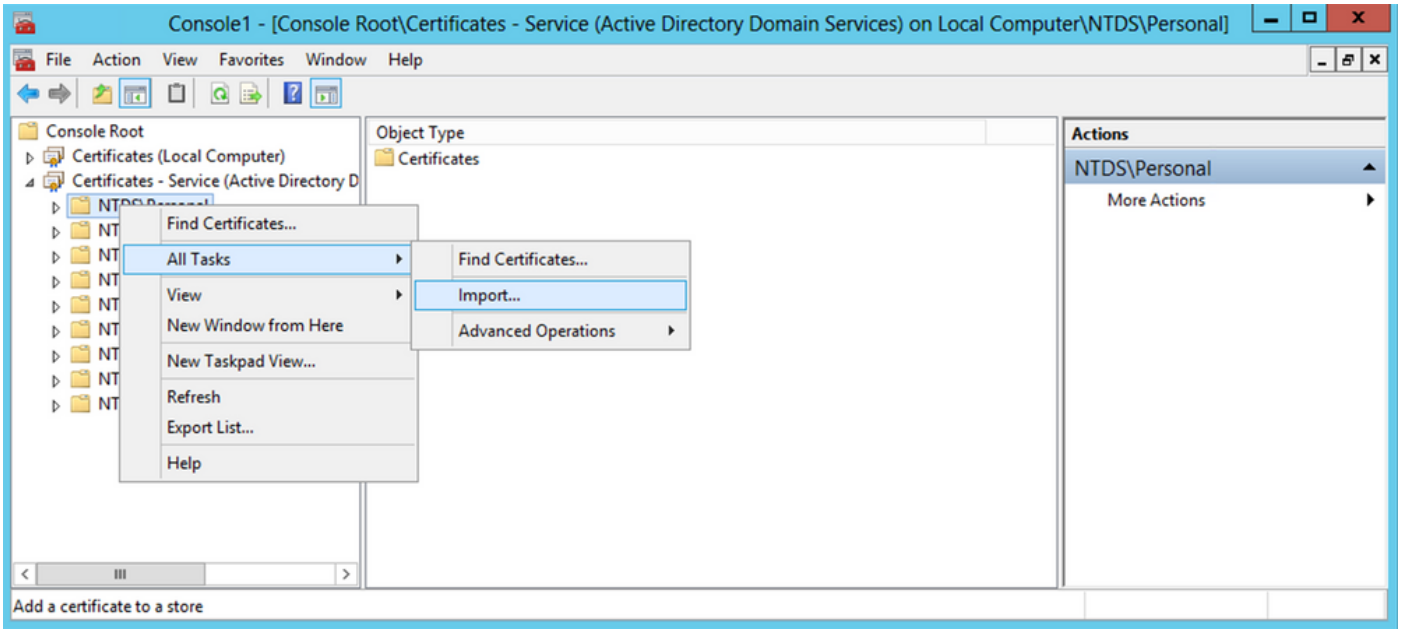
- En el Select Computer cuadro de diálogo, elija Local Computer y haga clic en Next.
- Elija Active Directory Domain Services y haga clic en Finish.



- En el Add/Remove Snap-ins cuadro de diálogo, haga clic en OK.
- Expanda Certificates - Services (Active Directory Domain Services) y, a continuación, haga clic en NTDS\Personal.

-

Haga clic con el botón secundario NTDS\Personal, haga clic en All Tasks y, a continuación, haga clic en Import.



-

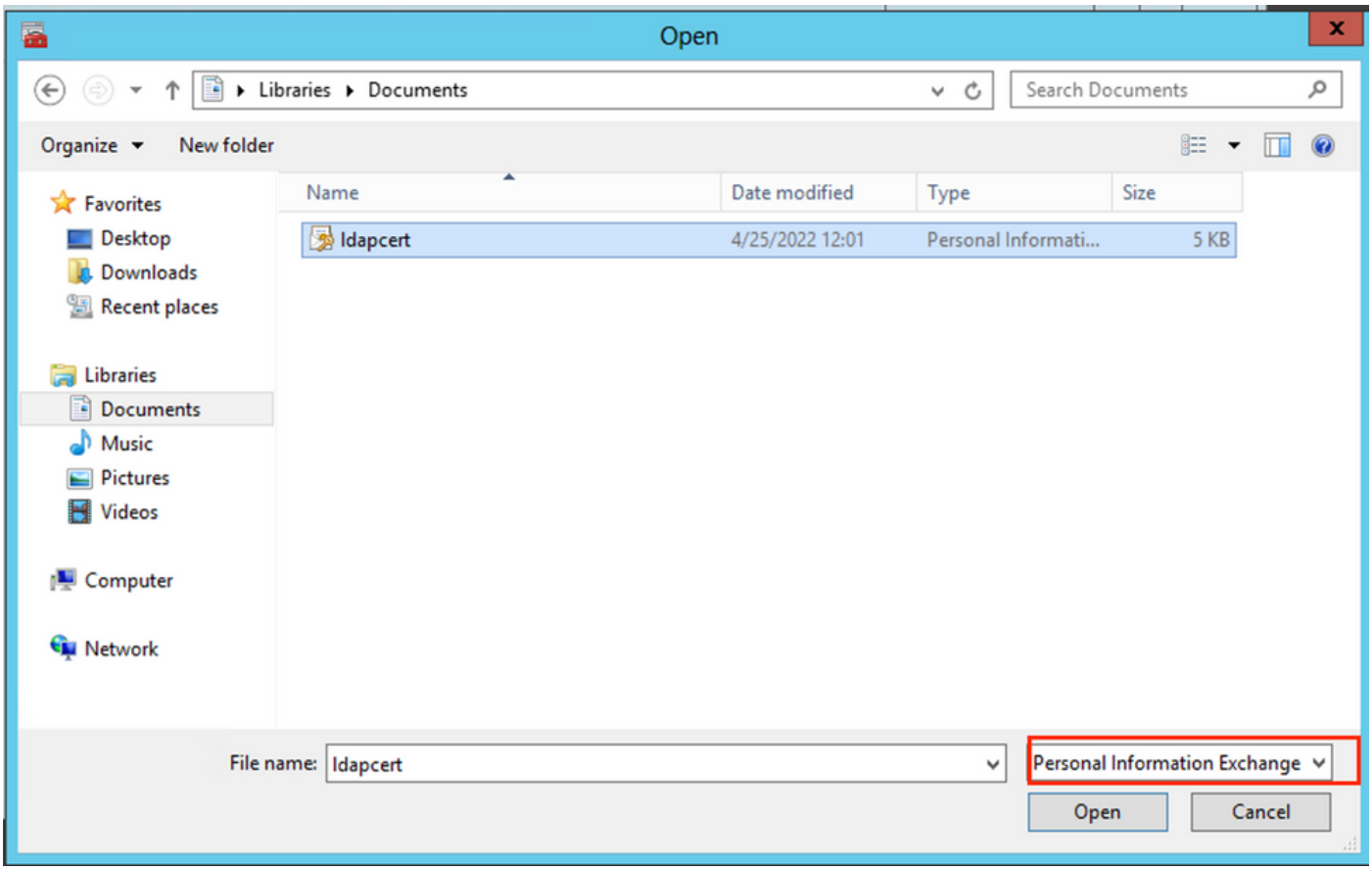
En la Certificate Import Wizard pantalla de bienvenida, haga clic en Next.

-

En la pantalla Archivo para importar, haga clic en Browse y localice el archivo de certificado que exportó anteriormente.

-

En la pantalla Abrir, asegúrese de que está seleccionado Intercambio de información personal (*pfx,*.p12) como tipo de archivo y, a continuación, desplácese por el sistema de archivos para localizar el certificado exportado anteriormente. A continuación, haga clic en ese certificado.



-

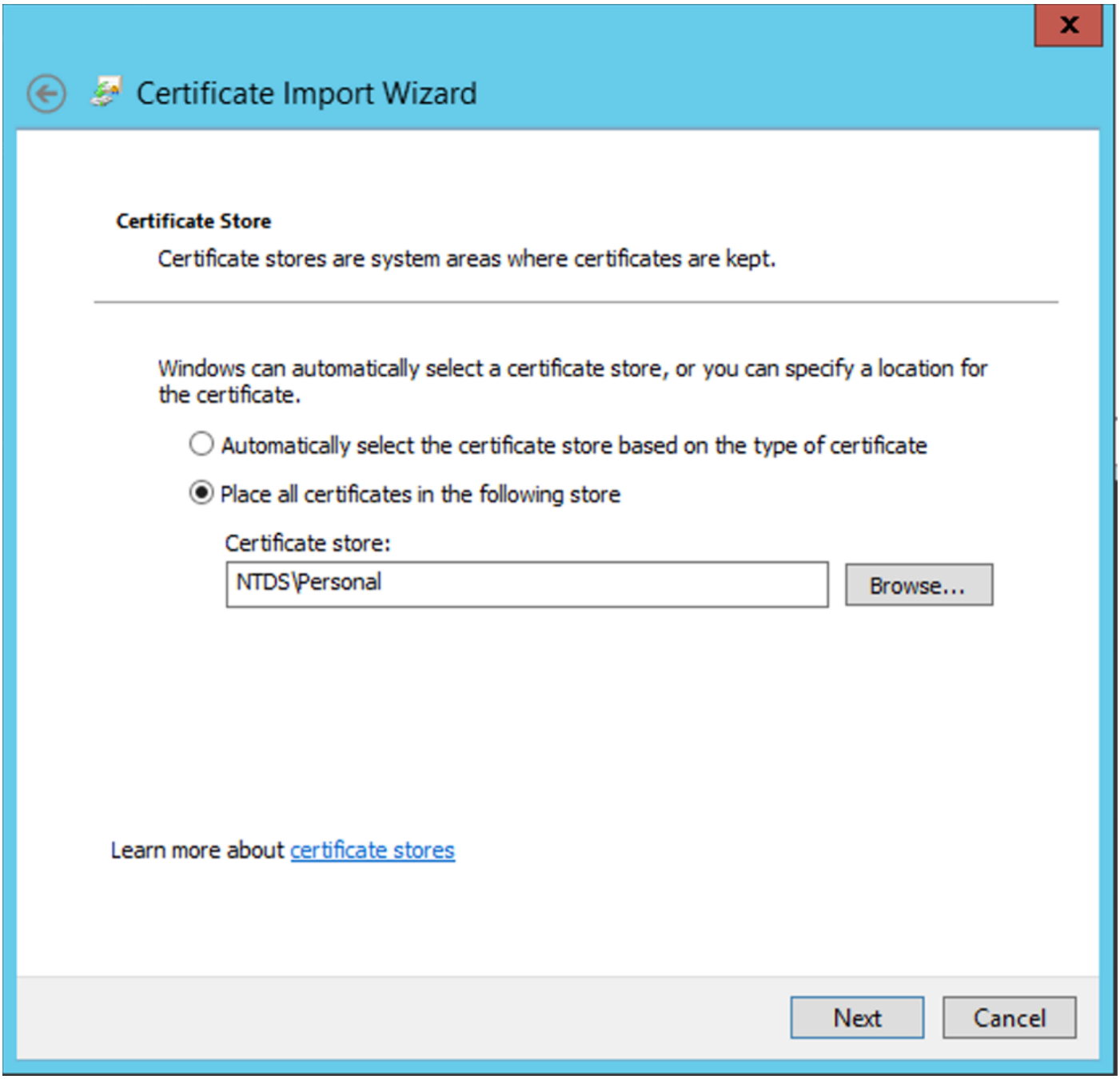
Haga clic Open y, a continuación, haga clic en Next.

-

En la pantalla Password (Contraseña), introduzca la contraseña establecida para el archivo y, a continuación, haga clic en Next.

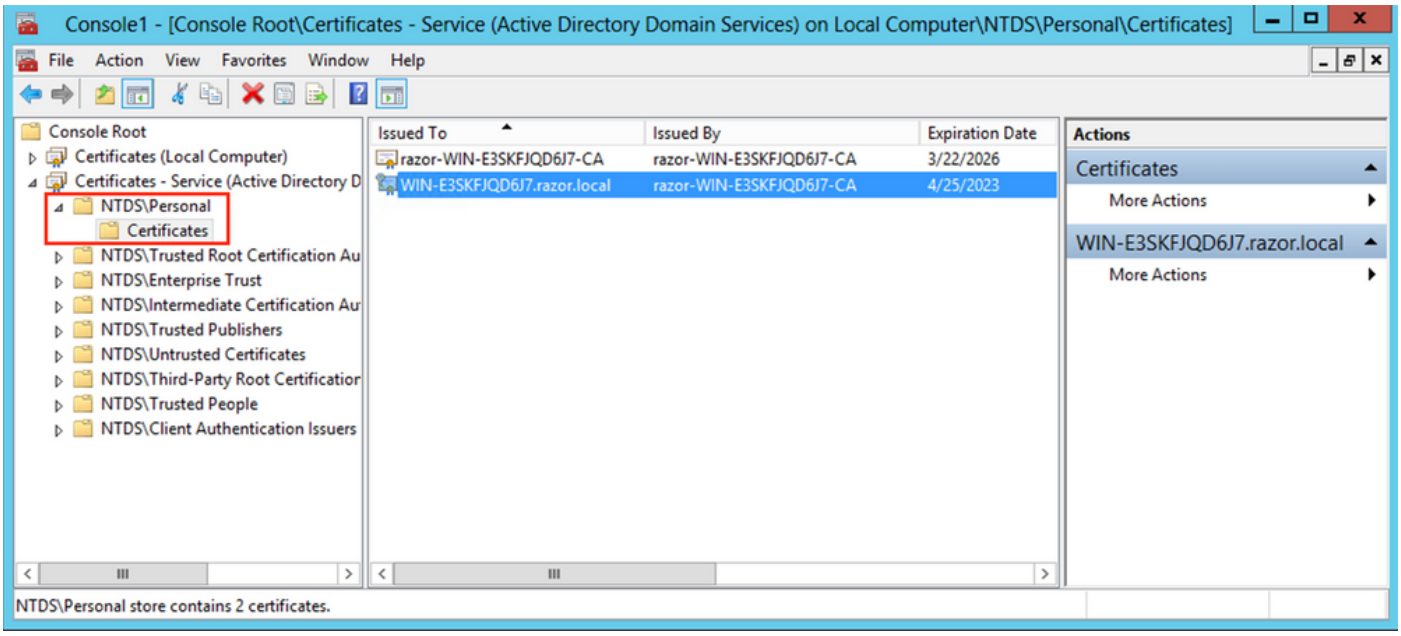
-

En la página Almacén de certificados, asegúrese de que la opción Colocar todos los certificados está seleccionada y lea Almacén de certificados: NTDS\Personal y, a continuación, haga clic en Next.



-

En la pantallaCertificate Import Wizard de finalización, haga clic en Finish. A continuación, verá un mensaje que indica que la importación se ha realizado correctamente. Haga clic en OK. Se observa que el certificado se ha importado en el almacén de certificados: NTDS\Personal.



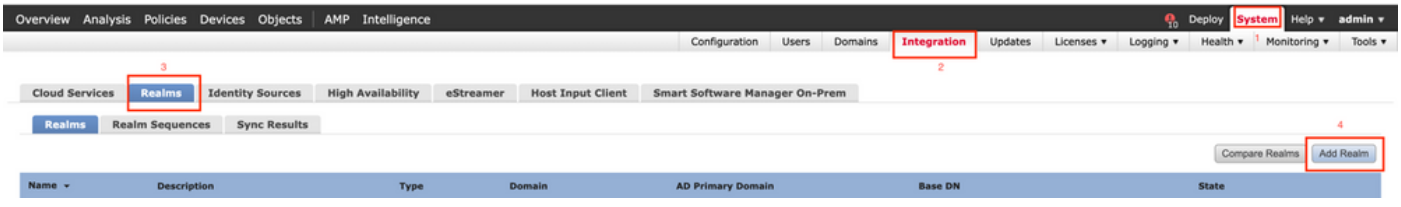
Configuraciones de FMC

Verificar licencia

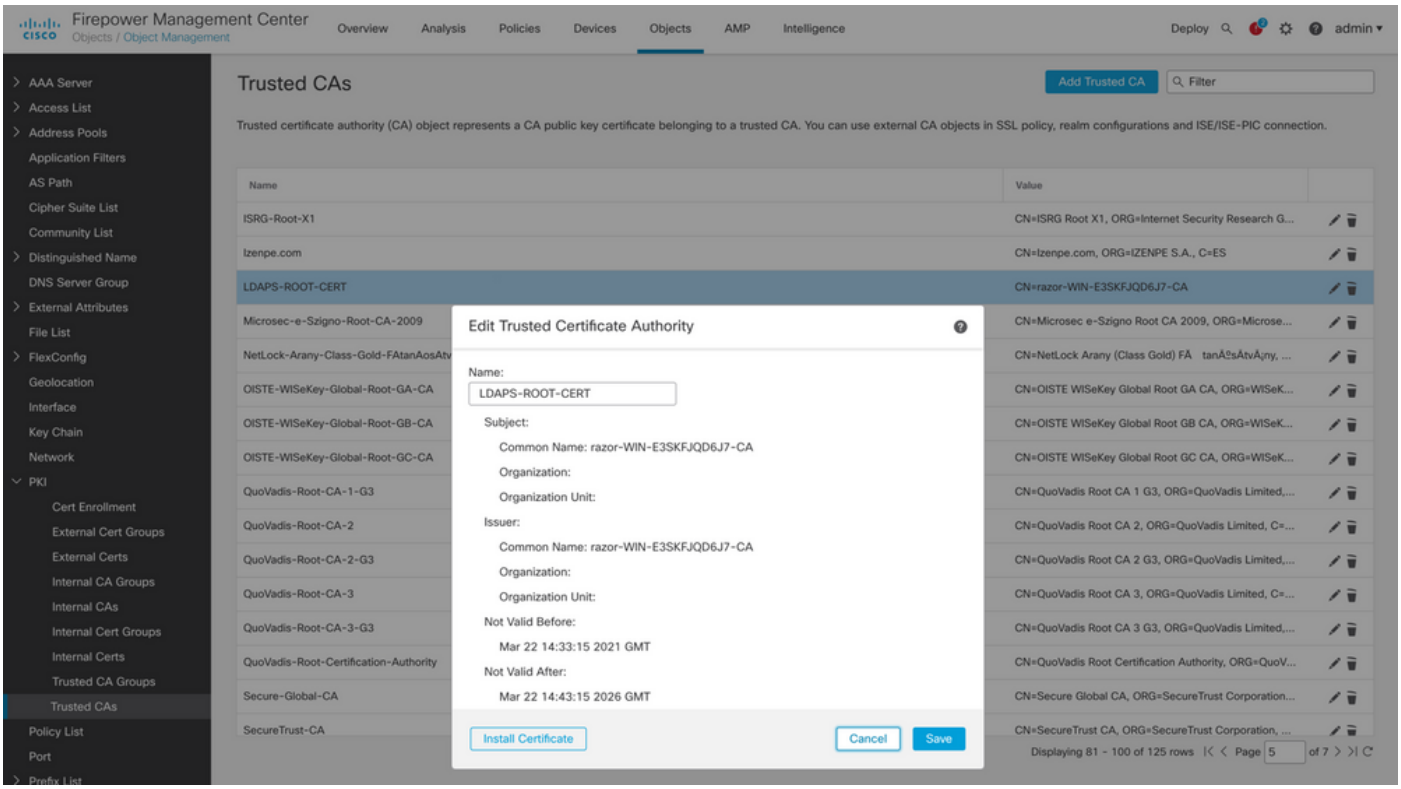
Para implementar la configuración de AnyConnect, el FTD debe estar registrado con el servidor de licencias inteligentes y se debe aplicar al dispositivo una licencia válida Plus, Apex o VPN Only.

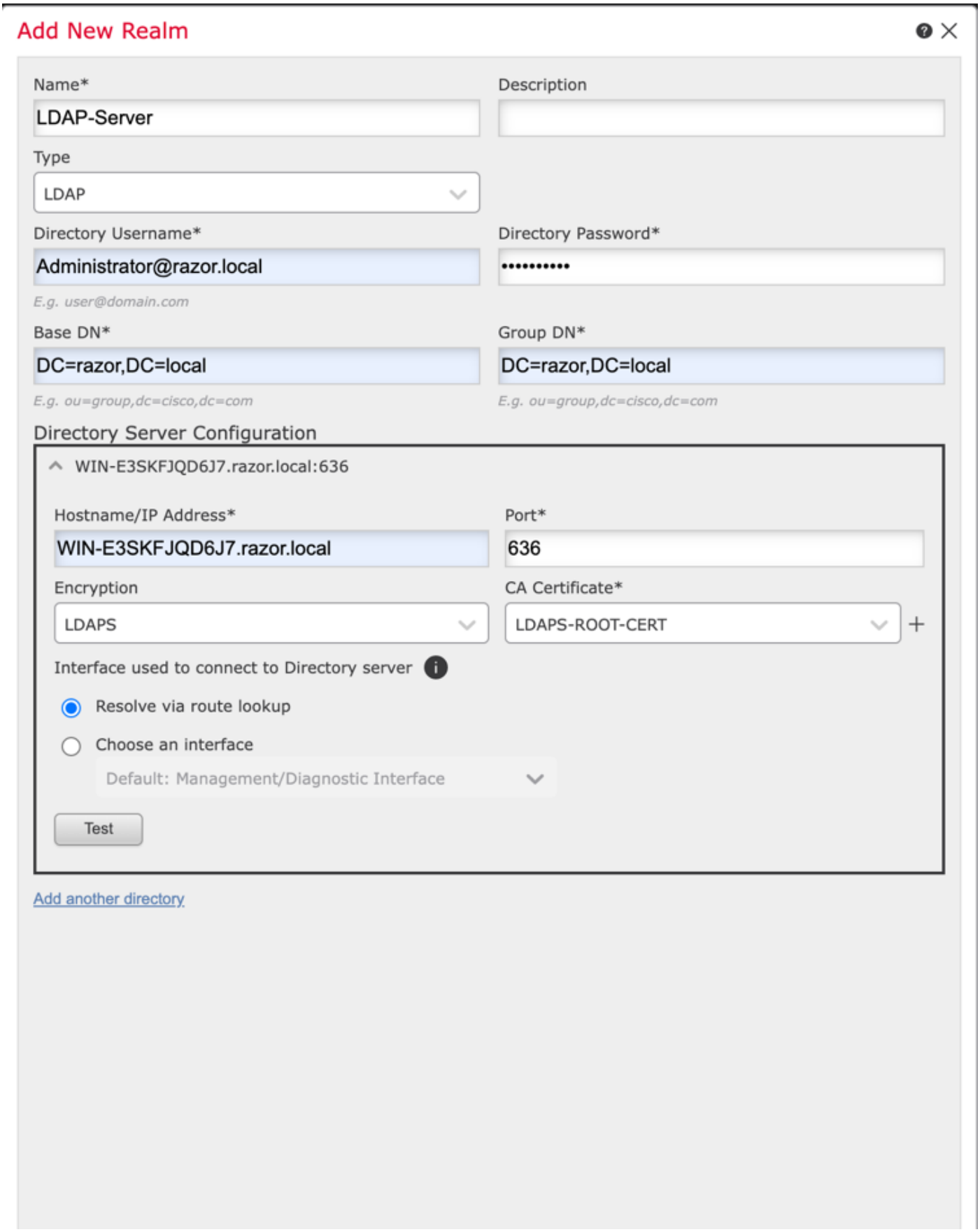
Rango de configuración

- Desplácese hasta System > Integration. Navegue hasta Realms y haga clic en Add Realm, como se muestra en esta imagen:



- Rellene los campos mostrados en función de la información recopilada del servidor de Microsoft para LDAP. Antes de esto, importe el certificado de CA raíz que ha firmado el certificado de servicio LDAPs en el servidor de Windows bajo Objects > PKI > Trusted CAs > Add Trusted CA, ya que se hace referencia a este en Directory Server Configuration el rango del rango. Una vez hecho esto, haga clic en OK.

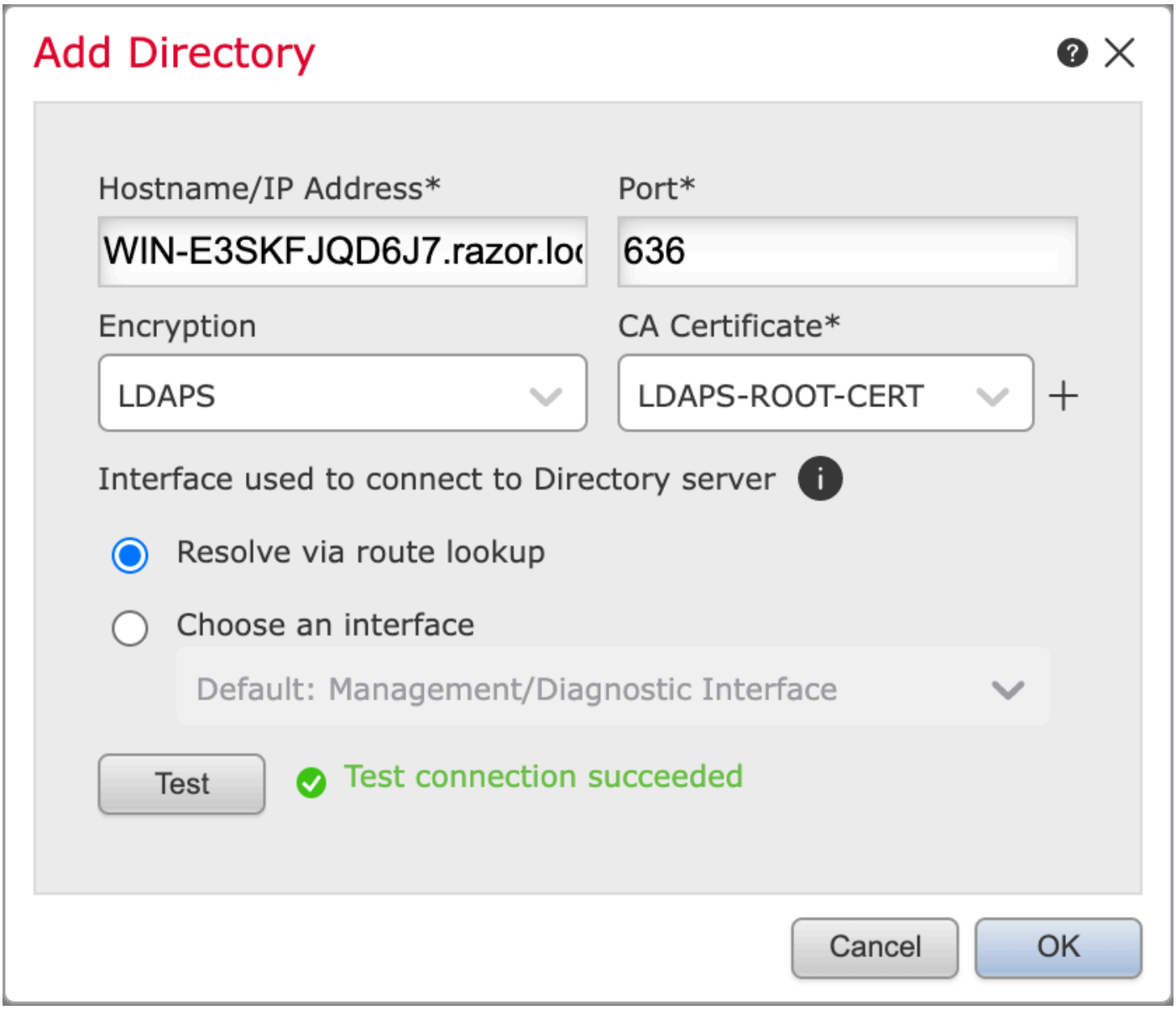

Firepower Management Center
Objects / Object Management
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Deploy
admin
AAA Server
Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
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



-

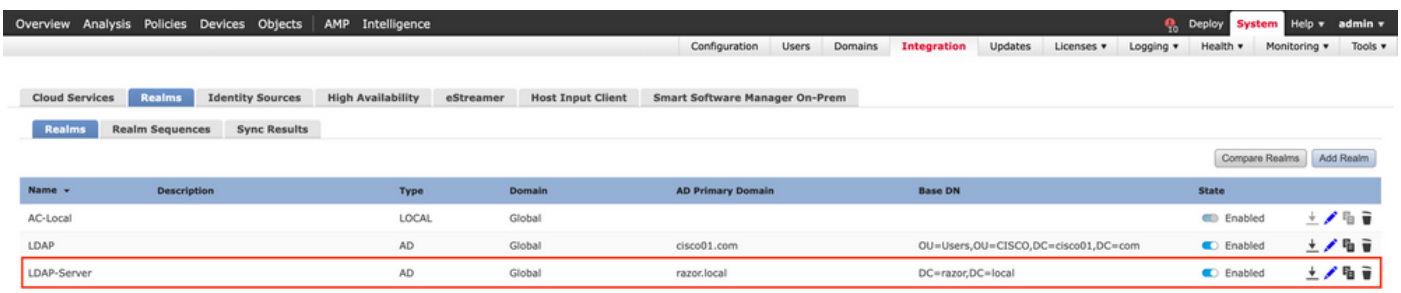
Haga clic Test para asegurarse de que FMC pueda enlazarse correctamente con el nombre de usuario y la contraseña del directorio proporcionados en el paso anterior. Dado que estas pruebas se inician desde el FMC y no a través de una de las interfaces enrutables configuradas en el FTD (como interna, externa o dmz), una conexión exitosa (o fallida) no garantiza el mismo resultado para la

autenticación de AnyConnect, ya que las solicitudes de autenticación LDAP de AnyConnect se inician desde una de las interfaces enrutables del FTD.



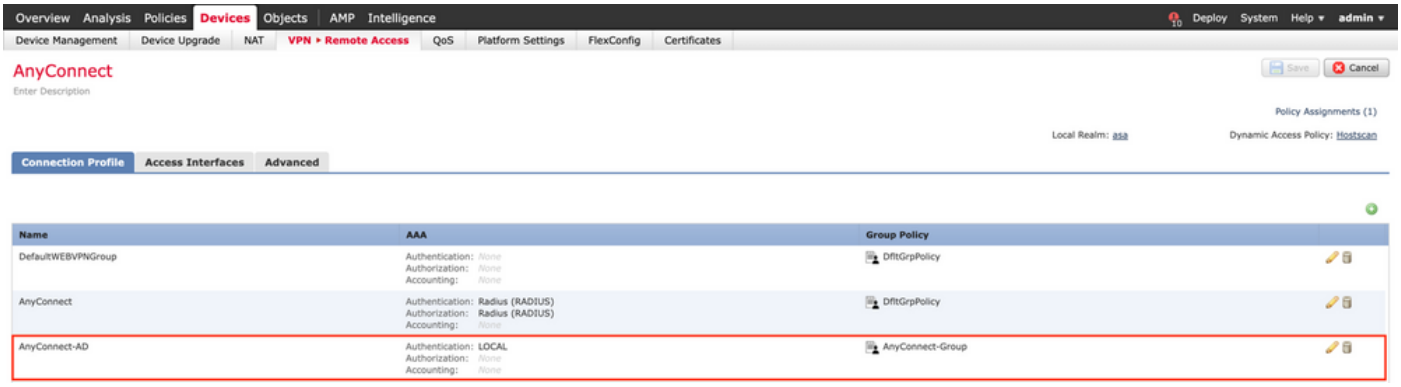
-

Habilite el nuevo rango.

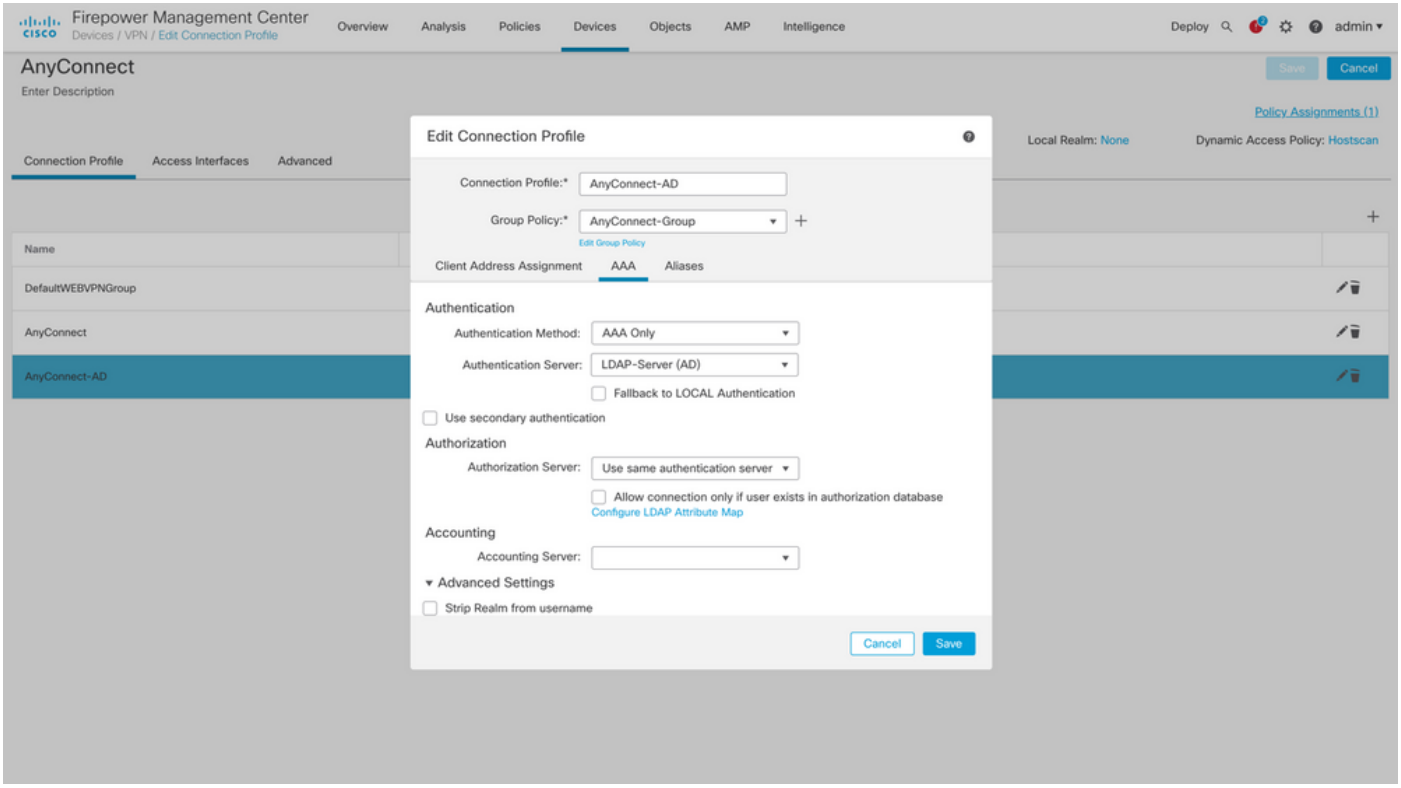


Configuración de AnyConnect para la gestión de contraseñas

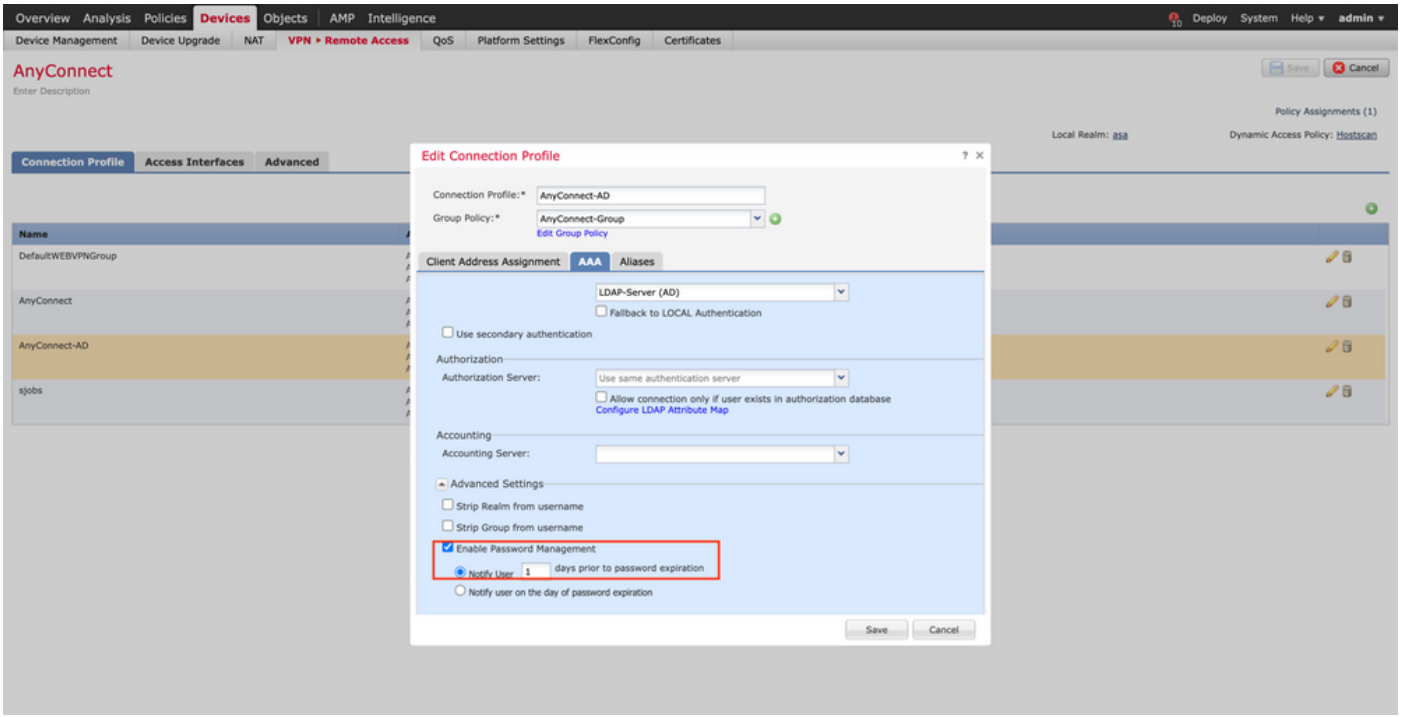
- Elija el perfil de conexión existente o cree uno nuevo, si es una configuración inicial de AnyConnect. Aquí, se utiliza un perfil de conexión existente denominado 'AnyConnect-AD' asignado con la autenticación local.



- Edite el perfil de conexión y asigne el nuevo servidor LDAPs configurado en los pasos anteriores, en la configuración AAA del perfil de conexión. Una vez hecho esto, haga clic Save en la esquina superior derecha.



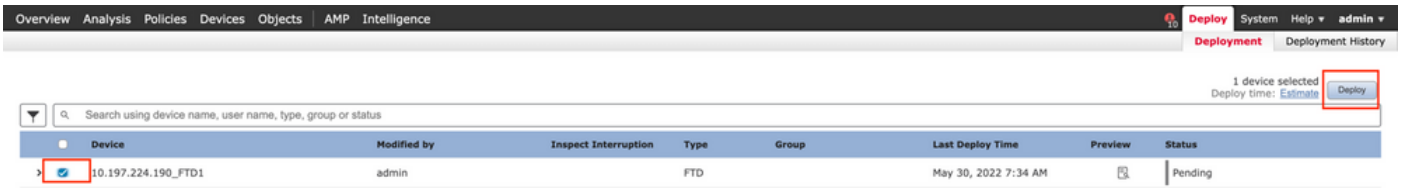
- Active la gestión de contraseñas en la AAA > Advanced Settings y guarde la configuración.



Implementación

- Una vez finalizada la configuración, haga clic en elDeploy botón de la parte superior derecha.

- Haga clic en la casilla de verificación junto a la configuración de FTD que se le ha aplicado y, a continuación, haga clic en Deploy, como se muestra en esta imagen:



Configuración final

Esta es la configuración que se observa en la CLI de FTD después de la implementación correcta.

Configuración 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
```

Configuración de 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
```

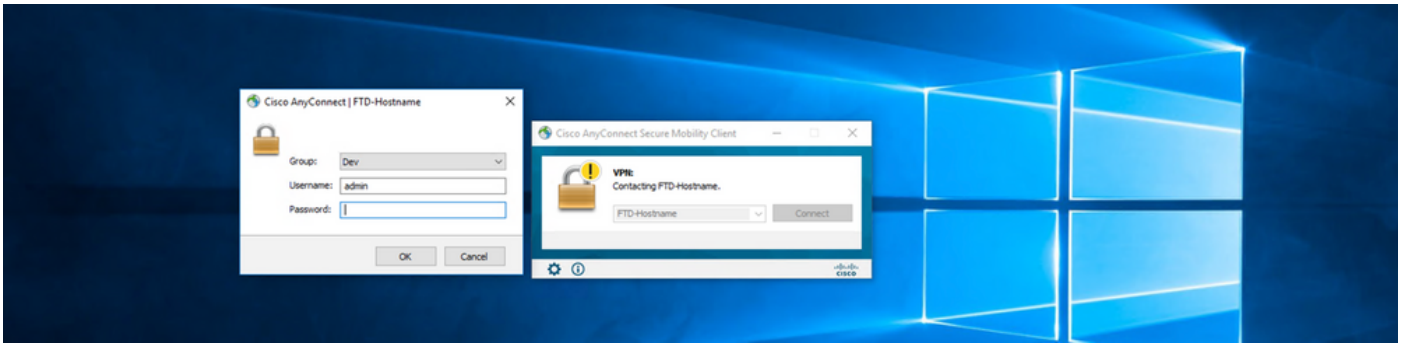
```
  anyconnect dtls compression none
  anyconnect modules value none
  anyconnect profiles value FTD-Client-Prof type user
  anyconnect ask none default anyconnect
  anyconnect ssl df-bit-ignore disable
```

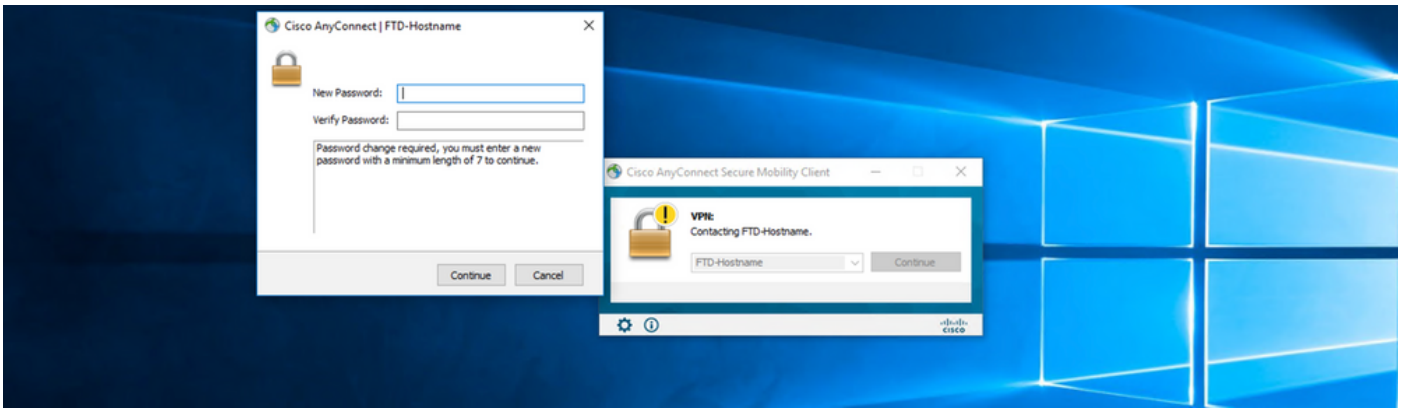
```
> show running-config ssl

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

Verificación

Conectar con AnyConnect y verificar el proceso de administración de contraseñas para la conexión de usuario

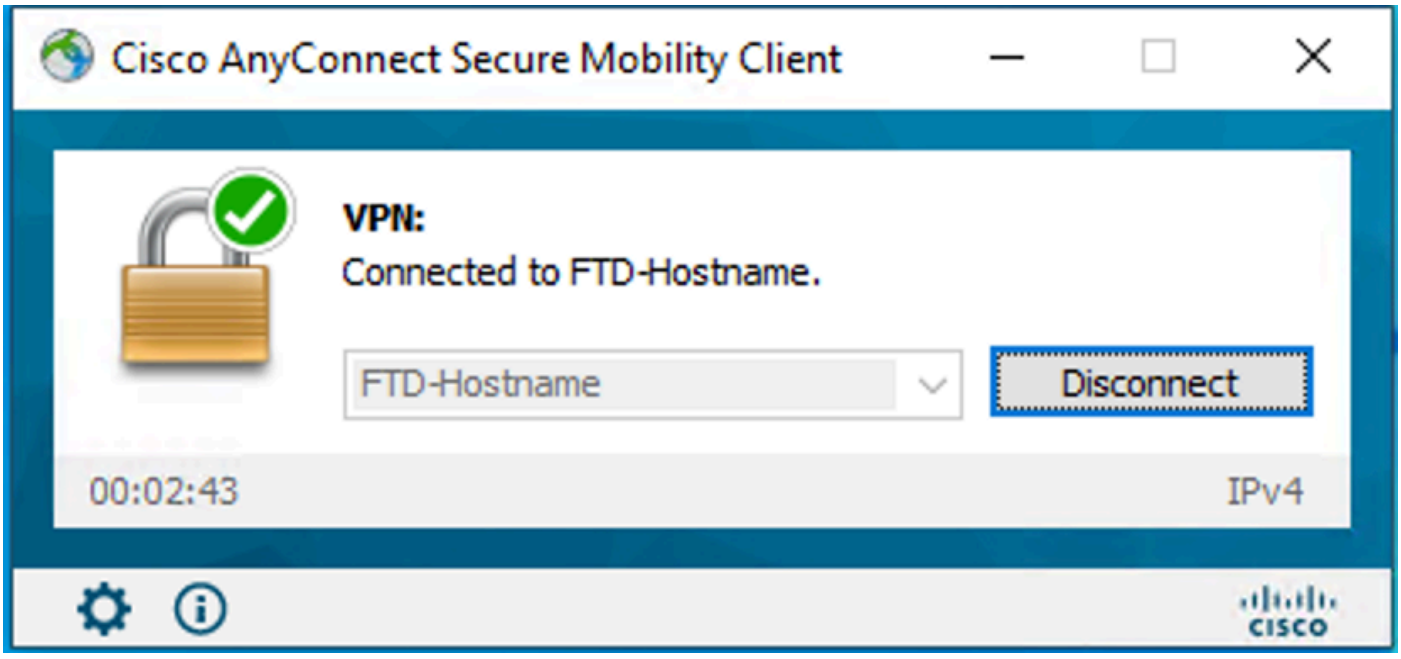
1. Inicie una conexión con el perfil de conexión correspondiente. Una vez que se determina en el inicio de sesión inicial que la contraseña debe cambiarse, ya que el servidor de Microsoft rechazó la contraseña anterior al expirar, se le pide al usuario que cambie la contraseña.





-

Una vez que el usuario introduzca la nueva contraseña para el inicio de sesión, la conexión se establecerá correctamente.



-

Verifique la conexión del usuario en la CLI de 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
```

Troubleshoot

Depuraciones

Esta depuración se puede ejecutar en la CLI de diagnóstico para resolver problemas relacionados con la administración de contraseñas: **debug ldap 255**.

Depuraciones de administración de contraseñas en funcionamiento

<#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

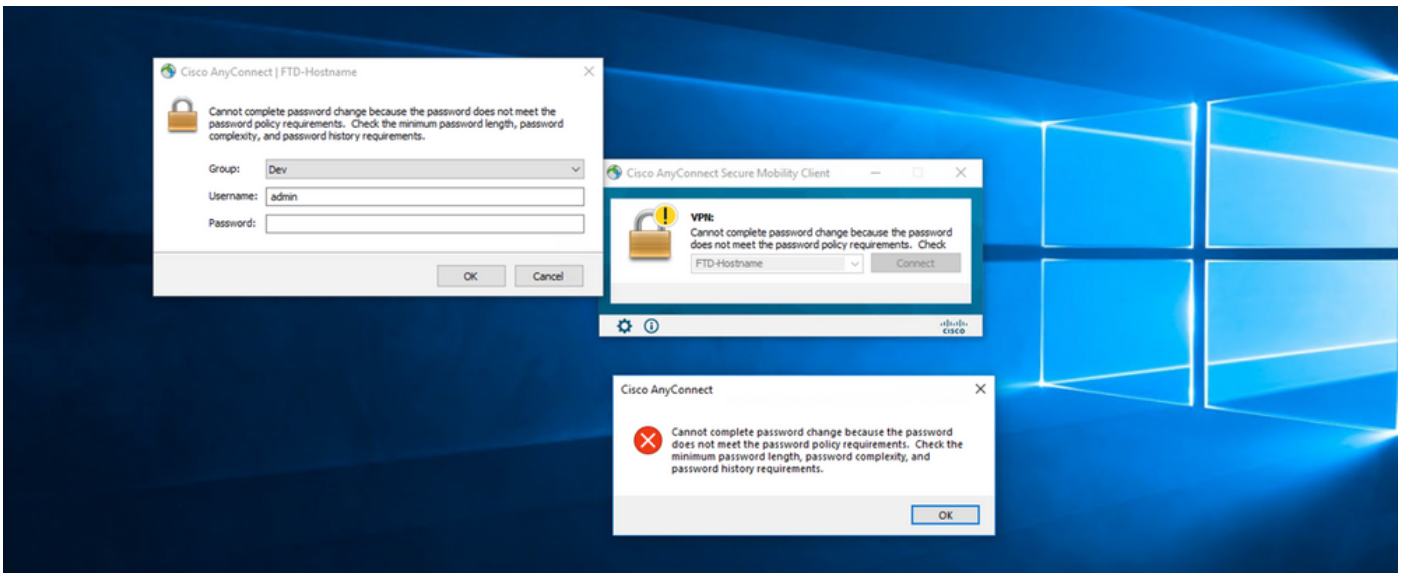
[25] primaryGroupID: value = 513

[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
```

Errores comunes encontrados durante la administración de contraseñas

Normalmente, si la directiva de contraseñas establecida por el servidor de Microsoft no se cumple durante el tiempo que el usuario proporciona la nueva contraseña, la conexión finaliza con el error "La contraseña no cumple los requisitos de la directiva de contraseñas". Por lo tanto, asegúrese de que la nueva contraseña cumpla con la política establecida por el servidor de Microsoft para LDAP.



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).