Configuración de la autenticación de AD (LDAP) y la identidad de usuario en FTD gestionadas por FDM para clientes de AnyConnect

Contenido

Introducción

El propósito de este documento es detallar cómo configurar la autenticación de Active Directory (AD) para los clientes de AnyConnect que se conectan a un Cisco Firepower Threat Defense (FTD) administrado por Firepower Device Management (FDM). La identidad del usuario se utilizará en las políticas de acceso para restringir a los usuarios de AnyConnect a direcciones IP y puertos específicos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración de VPN de RA en FDM
- Conocimiento básico de la configuración del servidor LDAP en FDM
- Conocimiento básico de AD

Componentes Utilizados

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

- Microsoft 2016 Server
- FTDv ejecutando 6.5.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama y escenario de red

El servidor de Windows está preconfigurado con Servicios de Internet Information Server (IIS) y Protocolo de Escritorio remoto (RDP) para probar la identidad del usuario. En esta guía de configuración, se crearán tres cuentas de usuario y dos grupos.

Cuentas de usuario:

- FTD Admin: Esto se utilizará como la cuenta de directorio para permitir que FTD se enlace al servidor AD.
- Administrador de TI: Cuenta de administrador de pruebas utilizada para demostrar la identidad del usuario.
- Usuario de prueba: Cuenta de usuario de prueba utilizada para demostrar la identidad del usuario.

Grupos:

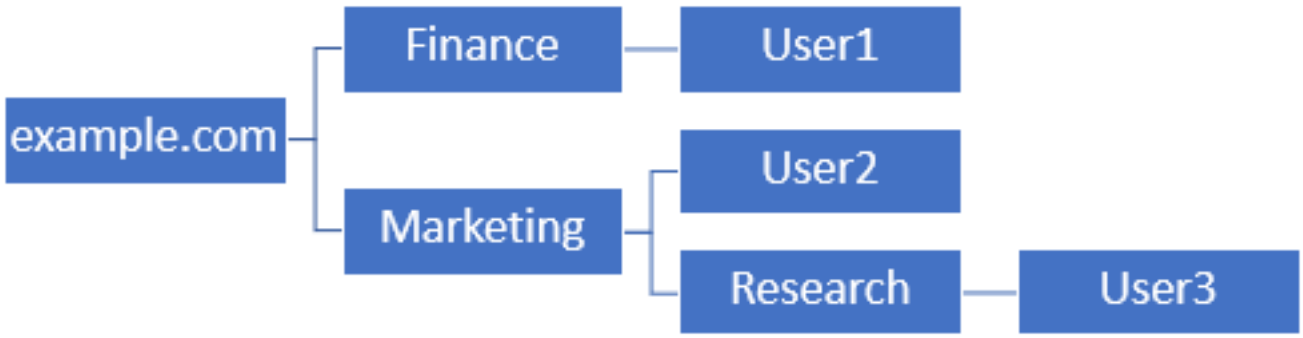
- Administradores de AnyConnect: Un grupo de prueba al que se agregará el administrador de TI para demostrar la identidad del usuario. Este grupo solo tendrá acceso RDP a Windows

Server
- Usuarios de AnyConnect: Grupo de prueba al que se agregará el usuario de prueba para demostrar la identidad del usuario. Este grupo solo tendrá acceso HTTP al servidor de Windows

Configuraciones de AD

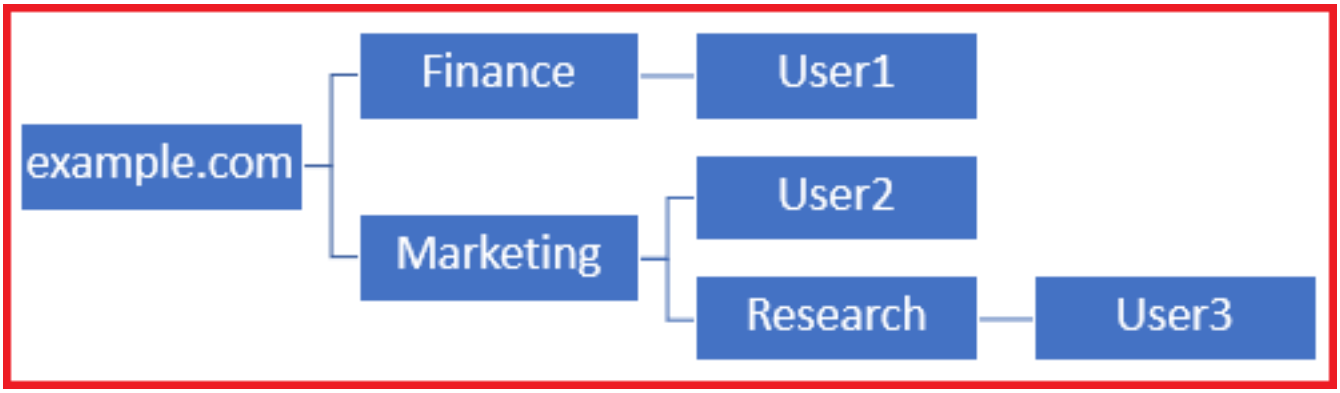
Para configurar adecuadamente la autenticación AD y la identidad del usuario en FTD, se necesitarán algunos valores. Todos estos detalles se deben crear o recopilar en Microsoft Server antes de que se pueda realizar la configuración en FDM. Los valores principales son:

- Nombre de dominio: Este es el nombre de dominio del servidor. En esta guía de configuración, example.com es el nombre de dominio.
- Dirección IP/FQDN del servidor: La dirección IP o FQDN utilizados para alcanzar el servidor de Microsoft. Si se utiliza un FQDN, se debe configurar un servidor DNS dentro de FDM y FTD para resolver el FQDN. En esta guía de configuración, estos valores son **win2016.example.com** que se resuelve en 192.168.1.1.
- Puerto del servidor: El puerto utilizado por el servicio LDAP. De forma predeterminada, LDAP y STARTTLS utilizarán el puerto TCP 389 para LDAP y LDAP sobre SSL (LDAPS) utilizará el puerto TCP 636.
- CA raíz: Si se utiliza LDAPS o STARTTLS, se requiere la CA raíz utilizada para firmar el certificado SSL utilizado por LDAPS.
- Nombre de usuario y contraseña del directorio: Esta es la cuenta utilizada por FDM y FTD para enlazar al servidor LDAP y autenticar usuarios y buscar usuarios y grupos. Se creará una cuenta denominada FTD Admin para este fin.
- Nombre distintivo básico (DN): El DN base es el FDM de punto de partida y el FTD indicará a Active Directory que comience en cuando busque usuarios. En esta guía de configuración, el dominio raíz example.com se utilizará como DN base; sin embargo, para un entorno de producción, el uso de un DN base más dentro de la jerarquía LDAP podría ser mejor. Por ejemplo, tome esta jerarquía LDAP:



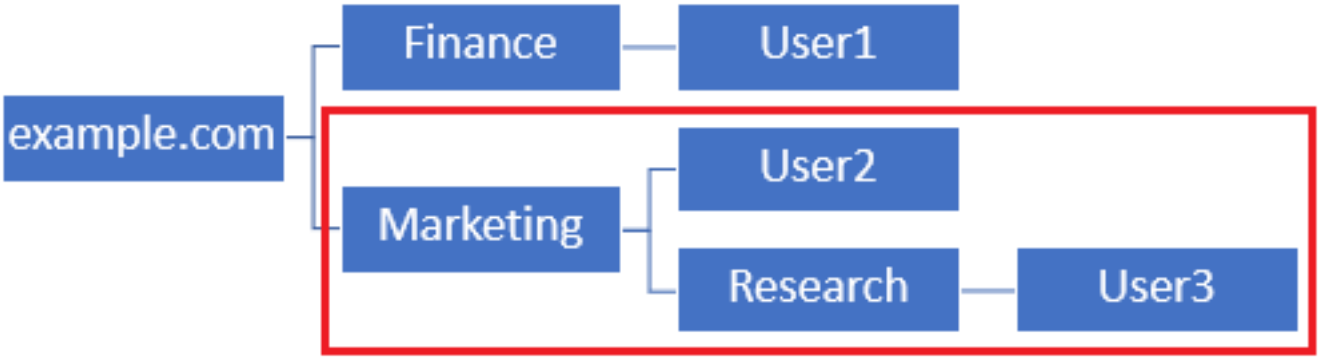
Si un administrador desea que los usuarios de la unidad organizativa de marketing puedan autenticar el DN base se puedan establecer en la raíz (ejemplo.com), esto también permitirá que el usuario1 de la unidad organizativa de finanzas también inicie sesión, ya que la búsqueda de usuario comenzará en la raíz y bajará a Finanzas, Marketing e Investigación.

DN base establecido en example.com.



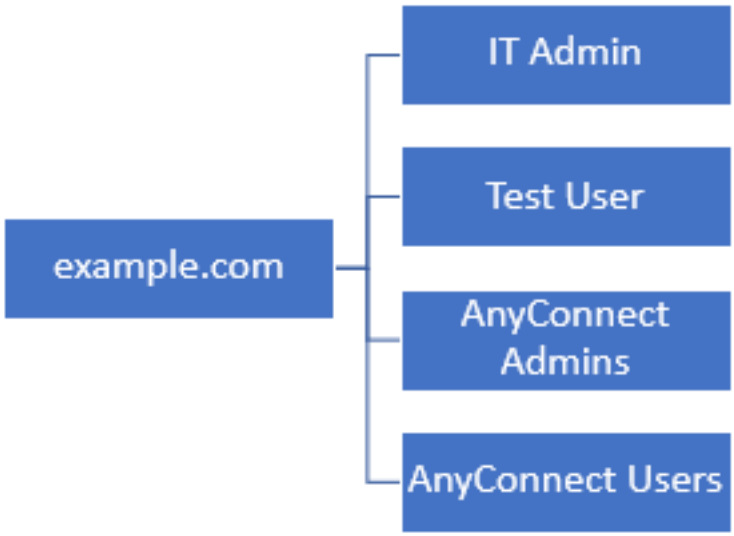
Para restringir los inicios de sesión sólo a los usuarios de la unidad organizativa de marketing y a los usuarios inferiores, el administrador puede establecer el DN base en Marketing. Ahora solo los usuarios 2 y 3 podrán autenticarse porque la búsqueda comenzará en Marketing.

DN base establecido en Marketing:



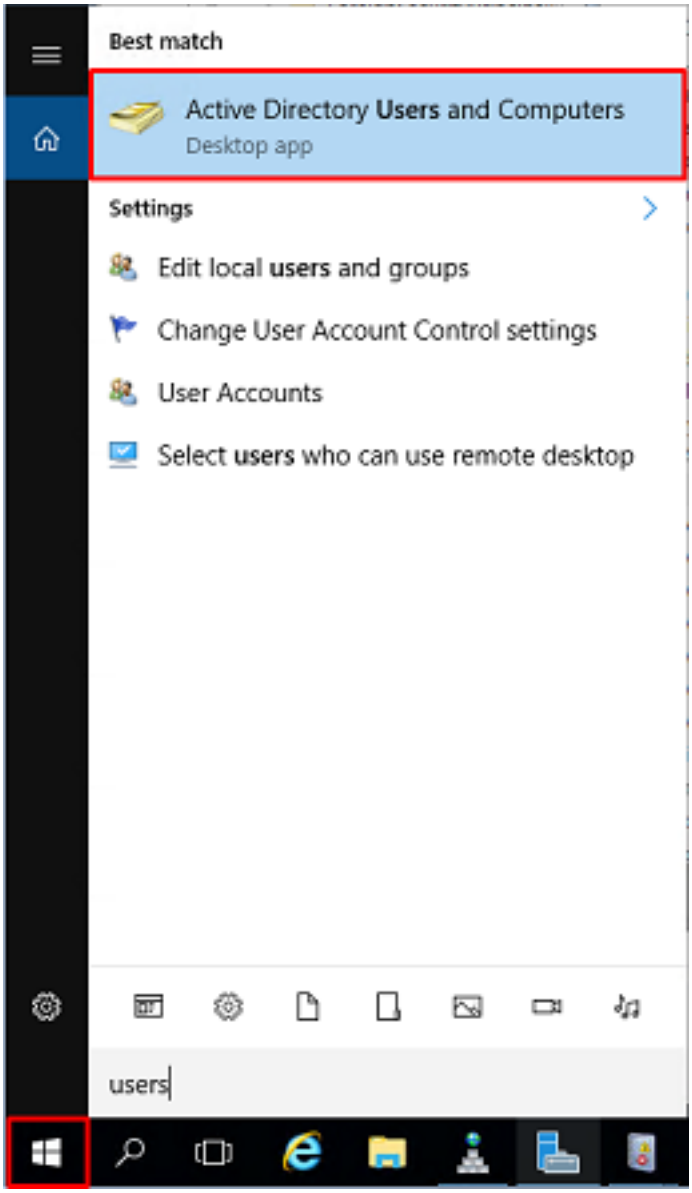
Tenga en cuenta que para un control más granular dentro del FTD para el cual se permitirá a los usuarios conectar o asignar diferentes autorizaciones según sus atributos de AD, será necesario configurar un mapa de autorización LDAP.

Esta jerarquía LDAP simplificada se utiliza en esta guía de configuración y el DN para el ejemplo raíz.com se utilizará para el DN base.

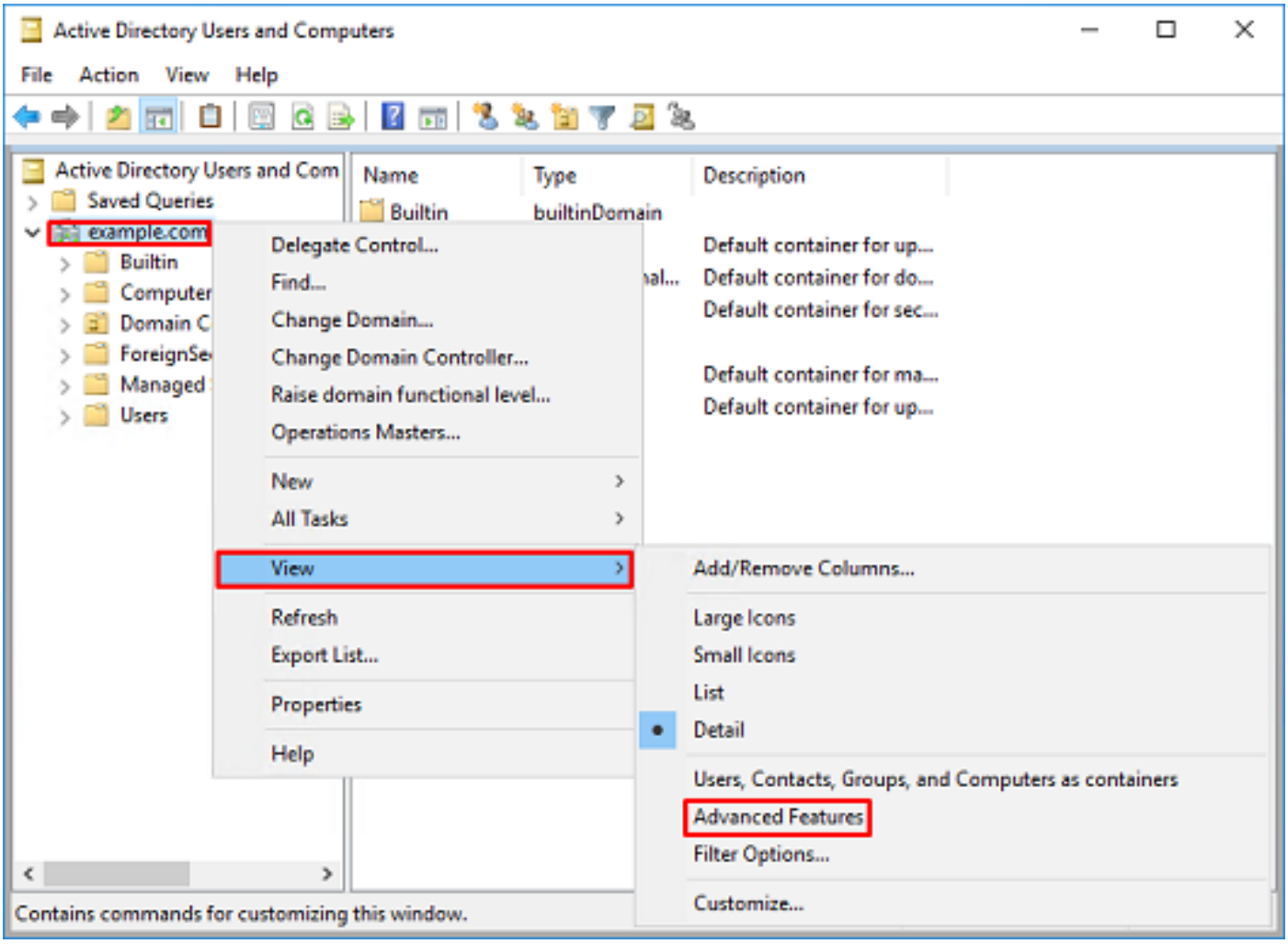


Determinación de LDAP Base DN

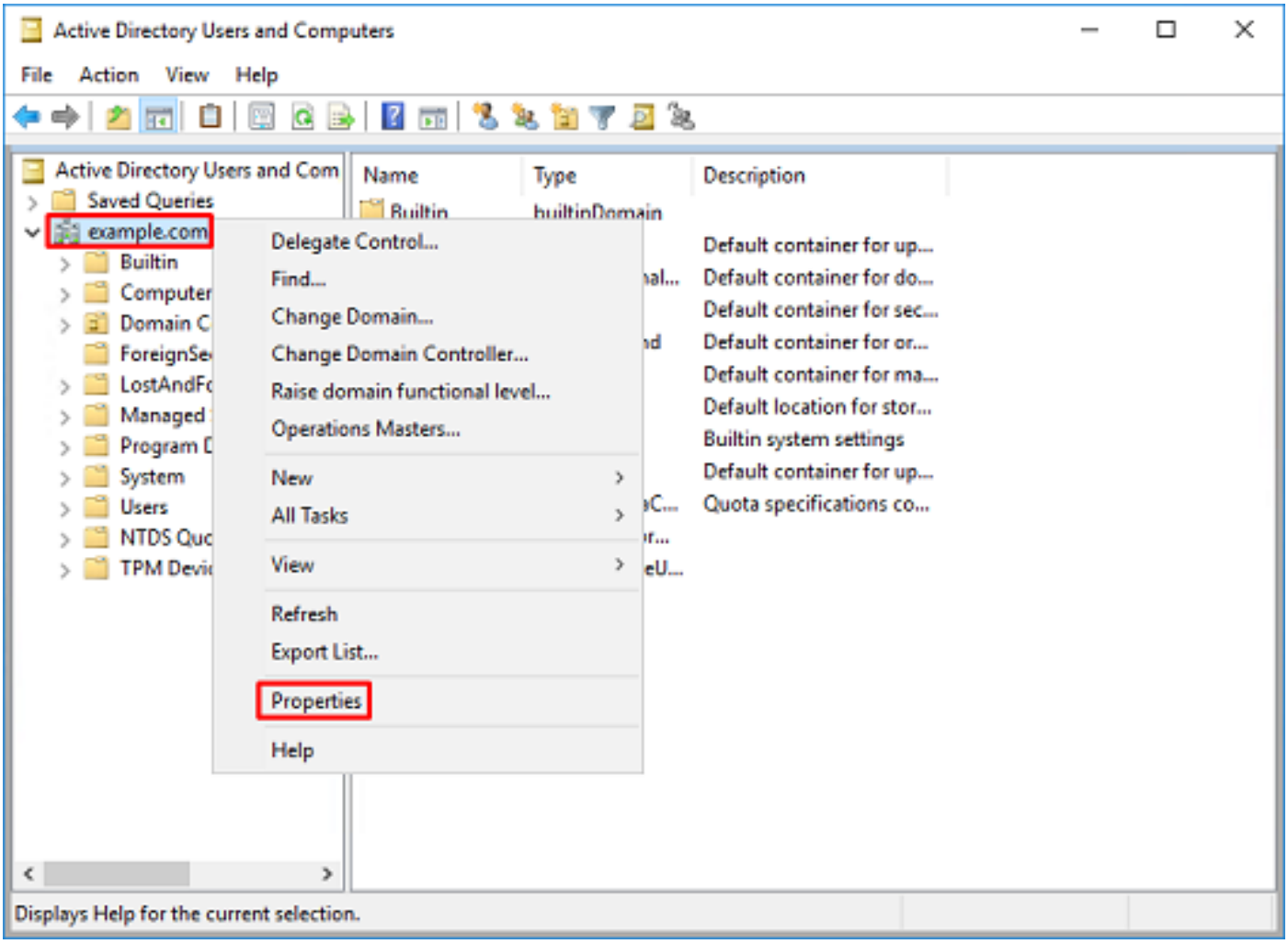
1. Abra Usuarios y ordenadores AD.



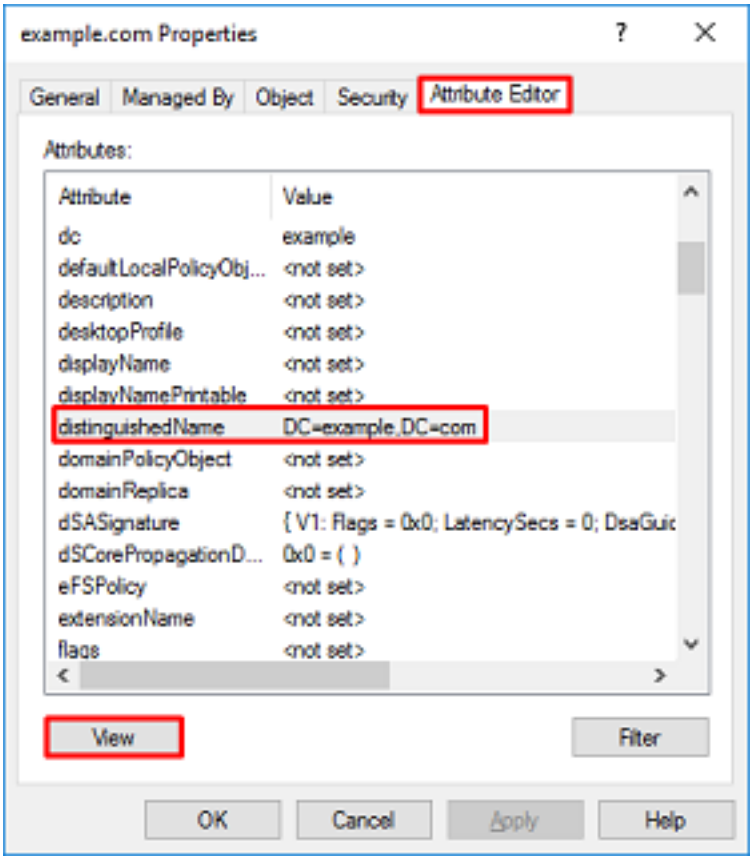
2. Haga clic con el botón izquierdo en el dominio raíz (para abrir el contenedor), haga clic con el botón derecho en el dominio raíz, luego navegue hasta **Ver** y haga clic en **Funciones avanzadas**.



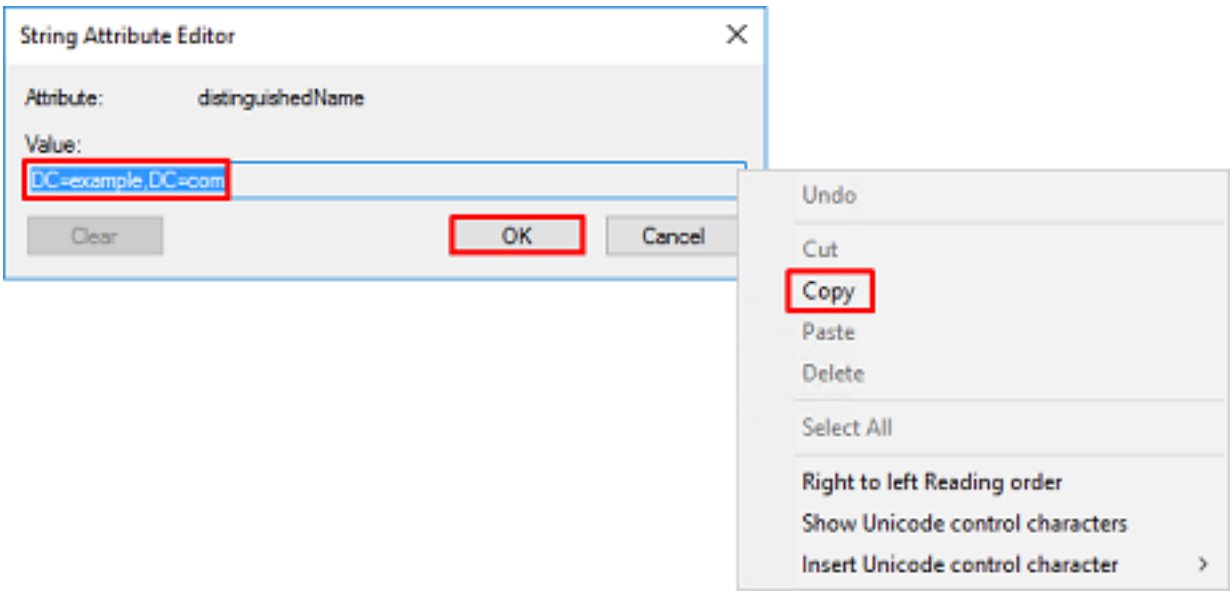
3. Esto habilitará la vista de propiedades adicionales bajo los objetos AD. Por ejemplo, para buscar el DN para la raíz example.com, haga clic con el botón derecho en **example.com** y luego navegue hasta **Propiedades**.

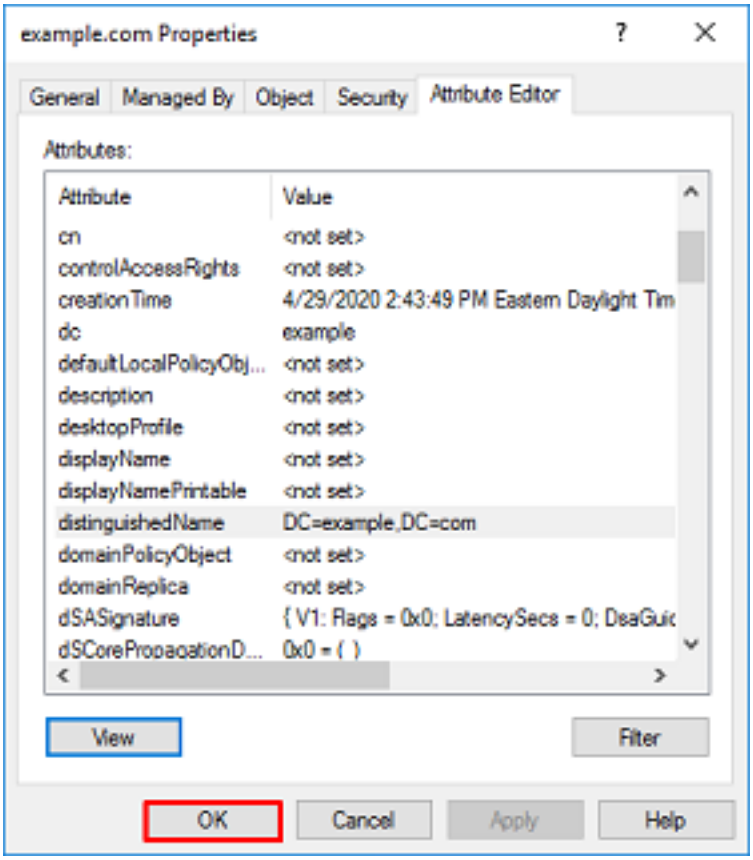


4. En **Propiedades**, haga clic en la ficha **Editor de atributos**. Busque **nombre distinguido** en los atributos y, a continuación, haga clic en **Ver**.

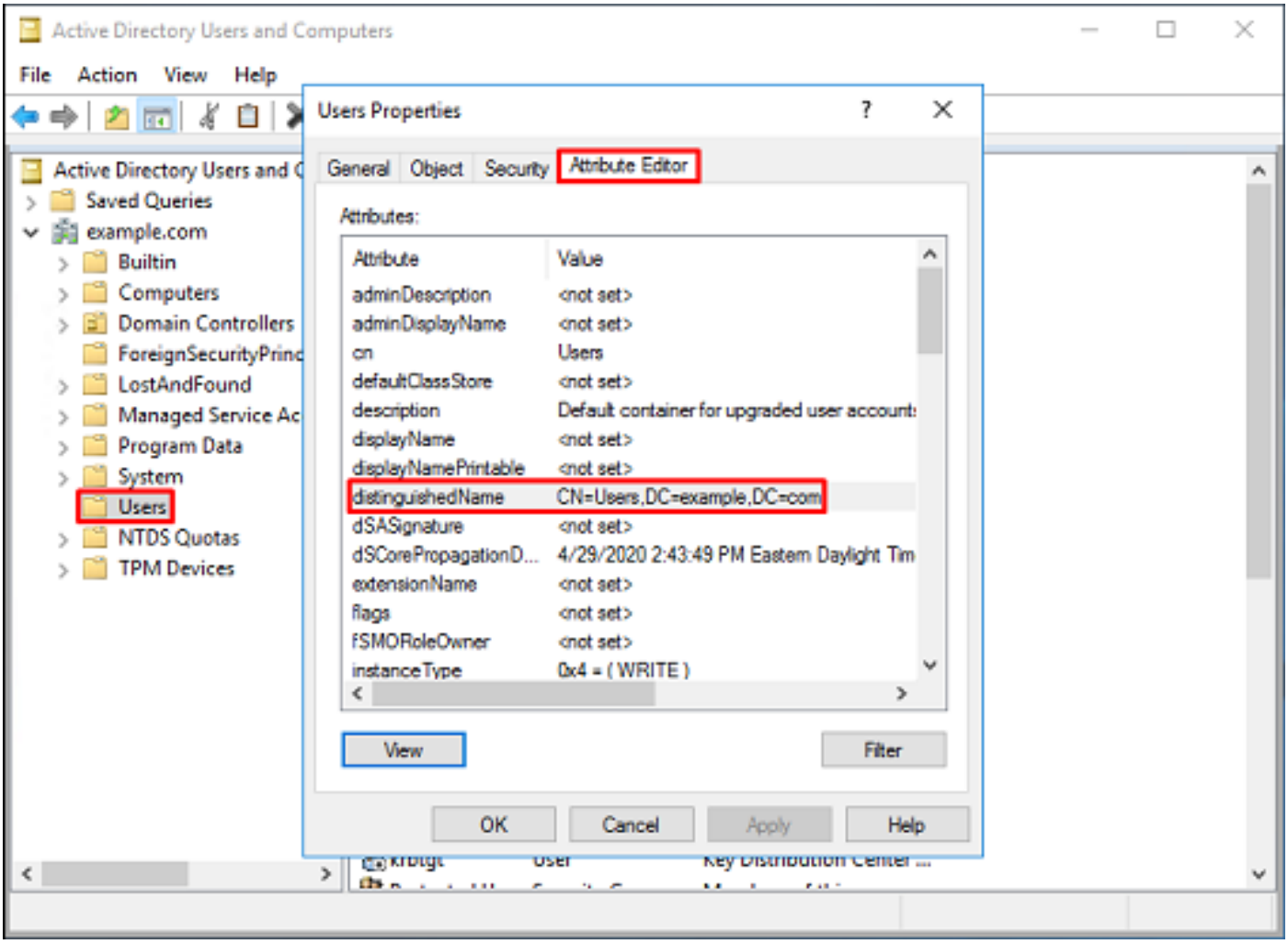


5. Esto abrirá una nueva ventana donde el DN se puede copiar y pegar en FDM más adelante. En este ejemplo, el DN raíz es DC=ejemplo, DC=com. Copie el valor. Haga clic en **Aceptar** para salir de la ventana del Editor de atributos de cadena y haga clic **Aceptar** nuevamente para salir de las propiedades.

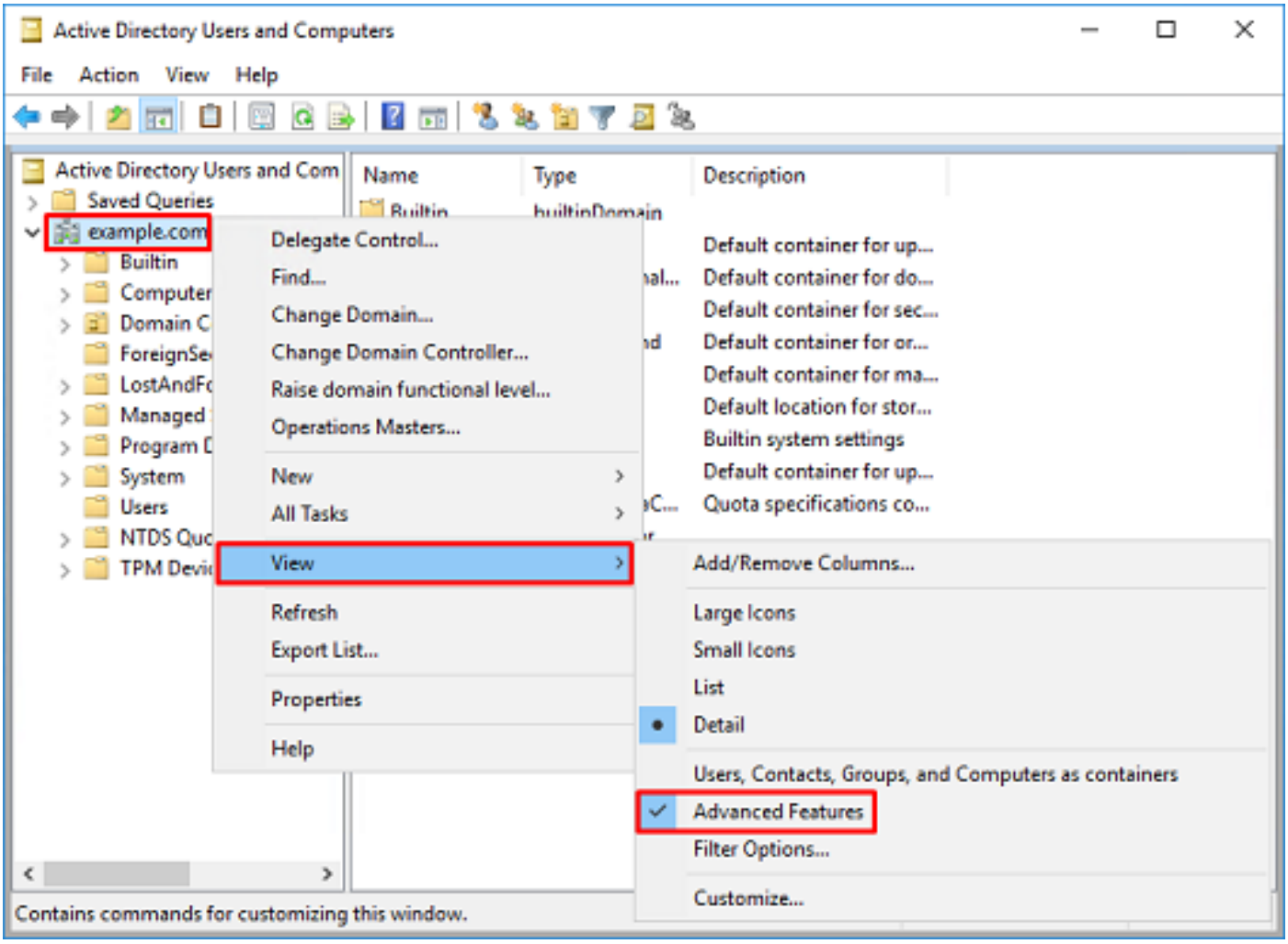




Esto se puede hacer para varios objetos dentro de AD. Por ejemplo, estos pasos se utilizan para buscar el DN del contenedor de usuario:



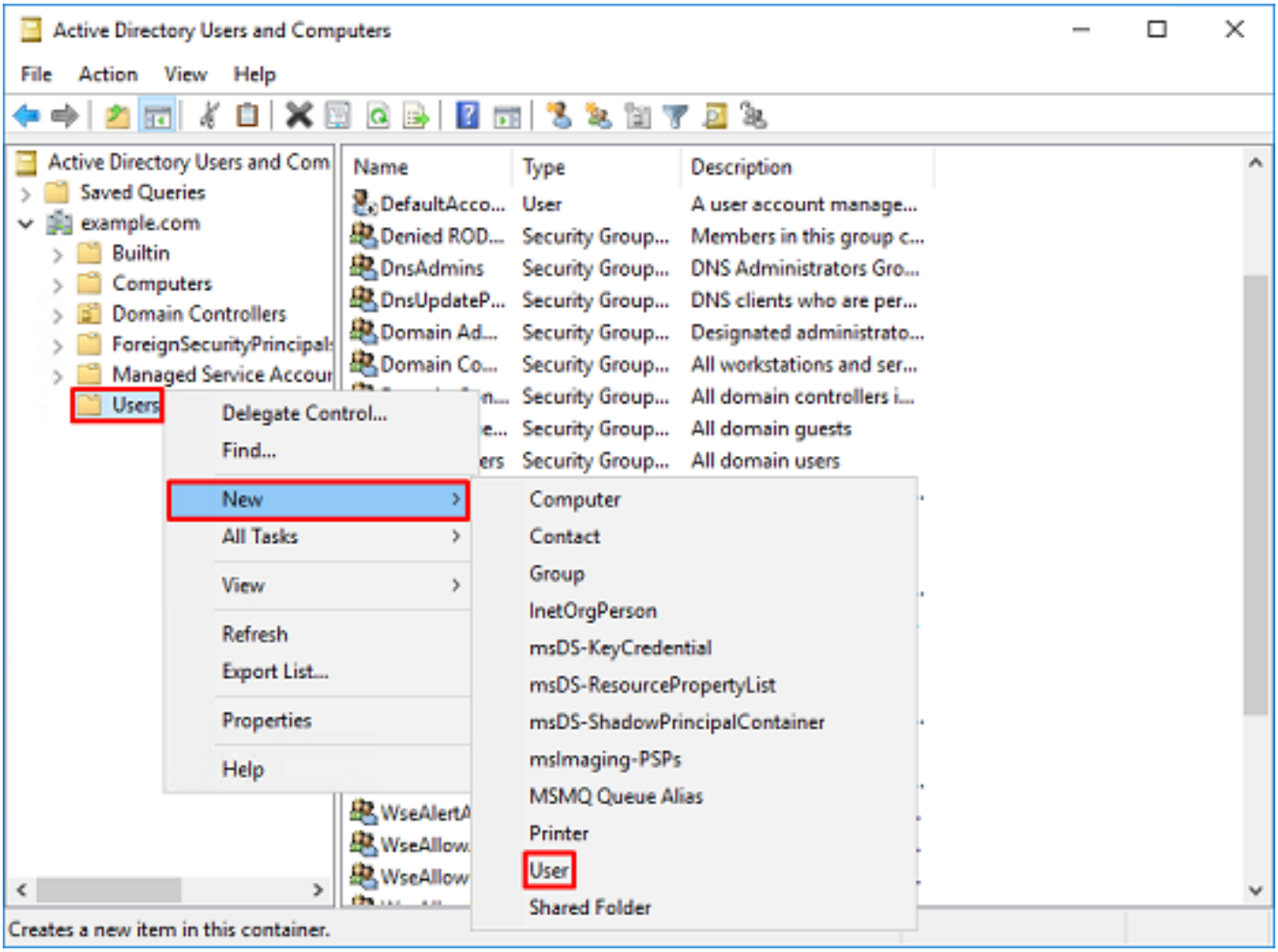
6. Se puede quitar la vista Funciones avanzadas. Haga clic con el botón derecho del ratón en el DN raíz, navegue hasta **Ver** y haga clic **Funciones avanzadas** una vez más.



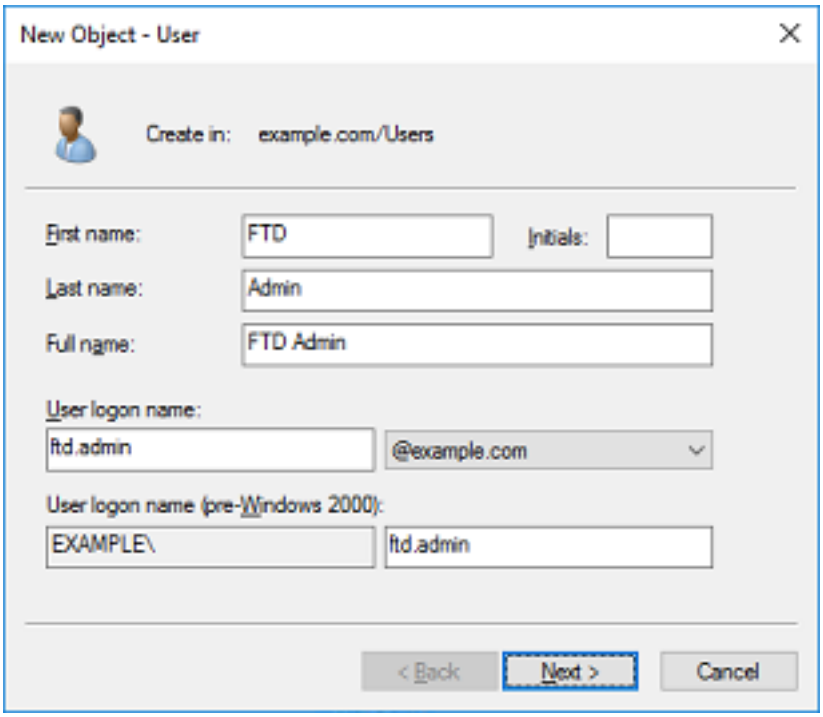
Crear una cuenta FTD

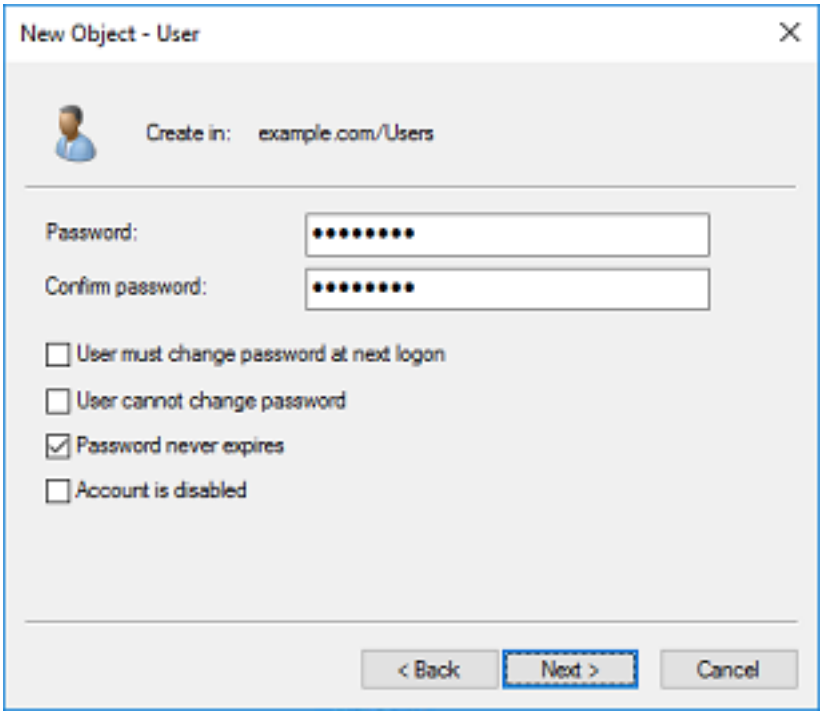
Esta cuenta de usuario permitirá que FDM y FTD se enlacen con AD para buscar usuarios y grupos y autenticarlos. El propósito de crear una cuenta FTD independiente es evitar el acceso no autorizado a otras partes de la red si las credenciales utilizadas para el enlace se ven comprometidas. Esta cuenta no necesita estar dentro del alcance del DN base.

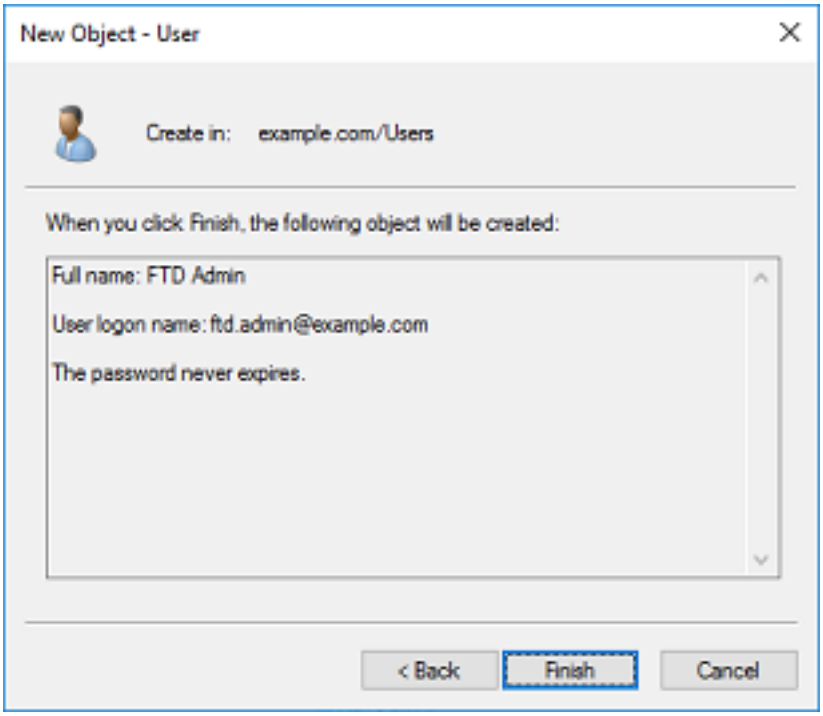
1. En **Active Directory Users and Computers**, haga clic con el botón derecho del ratón en el contenedor/organización al que se agregará la cuenta FTD. En esta configuración, la cuenta FTD se agregará bajo el contenedor Users bajo el nombre de usuario **ftd.admin@example.com**. Haga clic con el botón derecho del ratón en **Usuarios** y, a continuación, haga clic en **Nuevo > Usuario**.



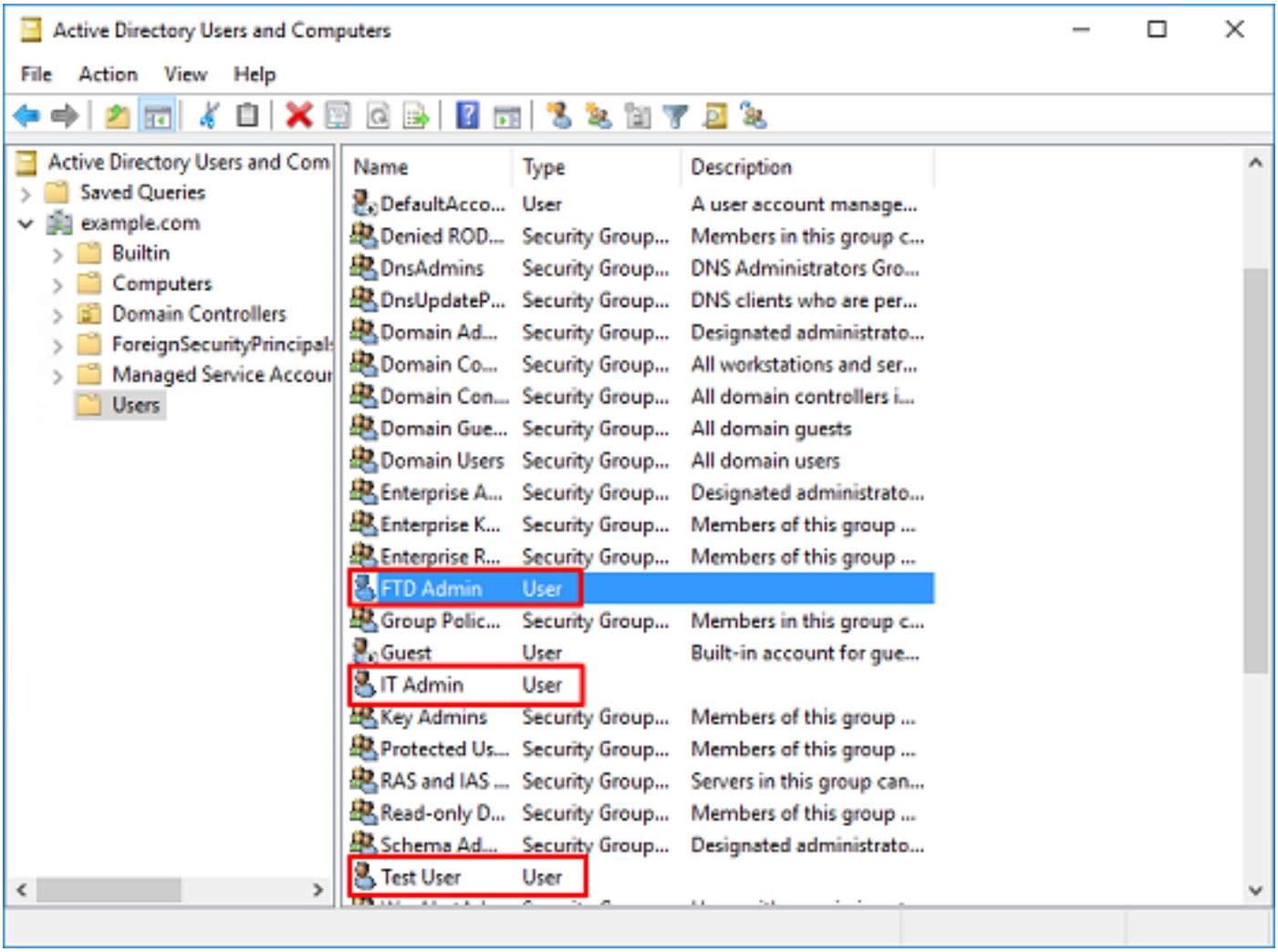
2. Desplácese por el Asistente **Nuevo objeto - Usuario**.







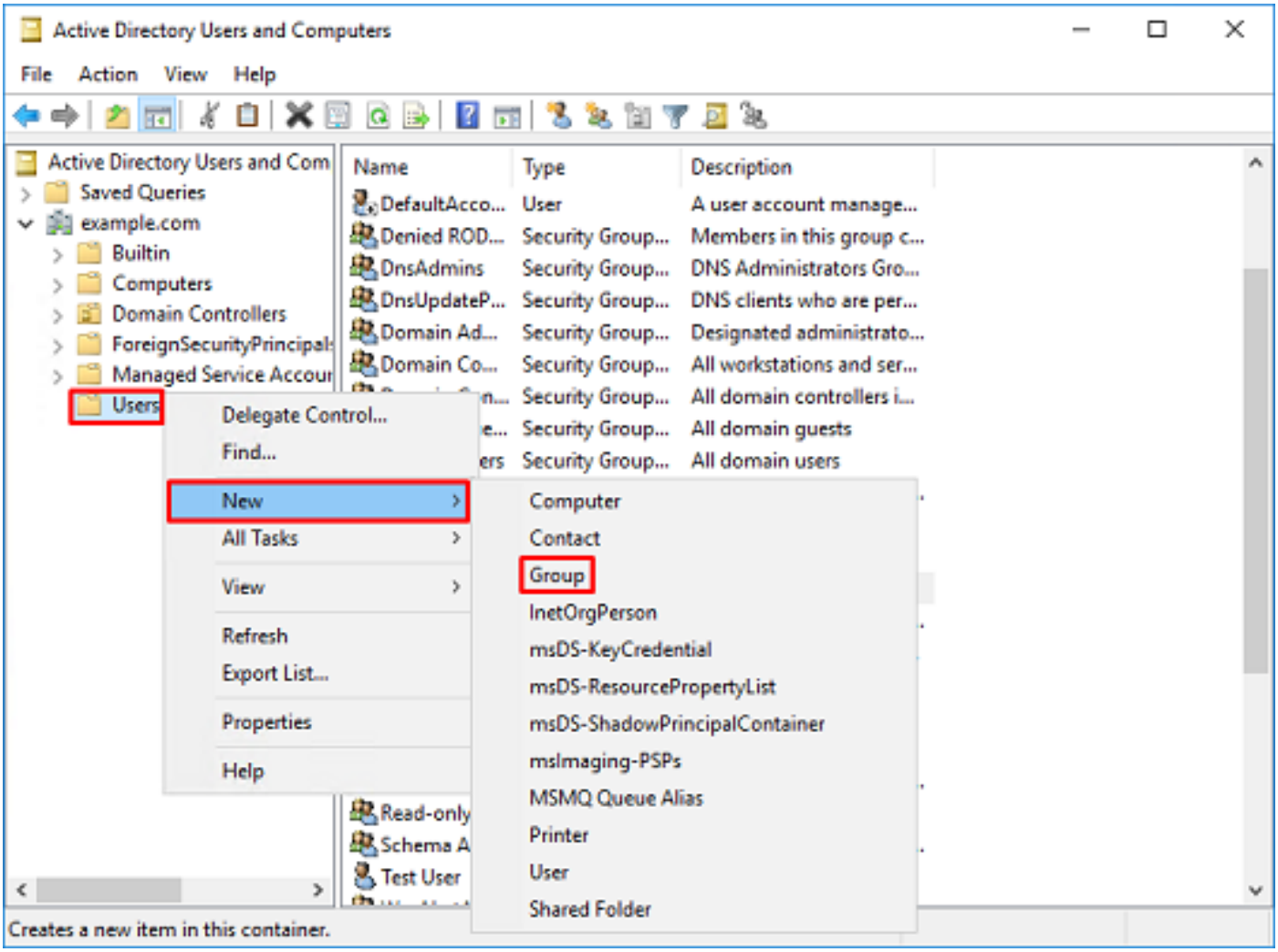
3. Verifique que se haya creado la cuenta FTD. Además, se han creado dos cuentas adicionales, **Administración de TI** y **Usuario de prueba**.



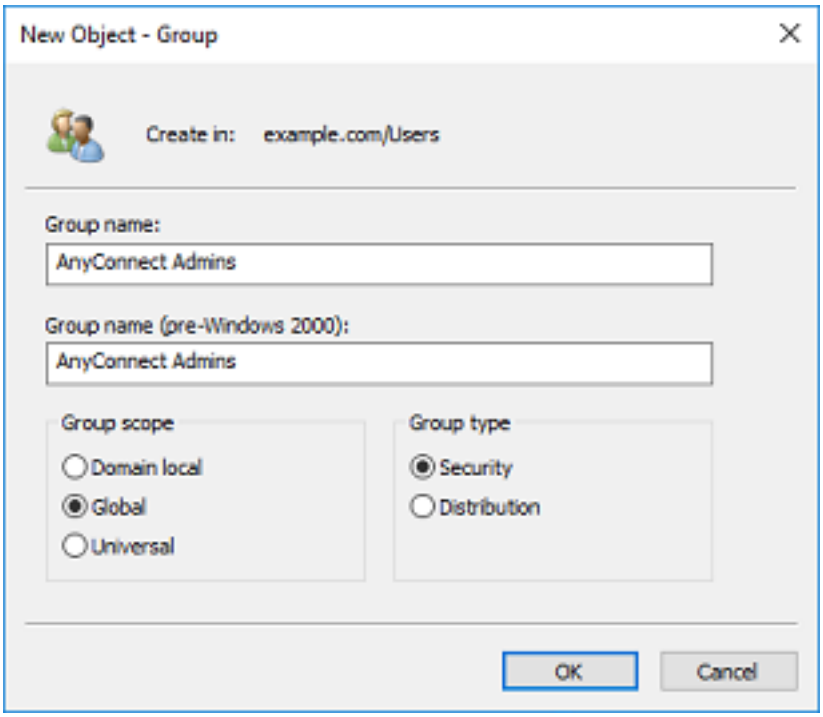
Crear grupos AD y agregar usuarios a grupos AD (opcional)

Aunque no se requiere para la autenticación, los grupos se pueden utilizar para facilitar la aplicación de políticas de acceso a varios usuarios, así como la autorización LDAP. En esta guía de configuración, los grupos se utilizarán más adelante para aplicar la configuración de la política de control de acceso a través de la identidad del usuario dentro de FDM.

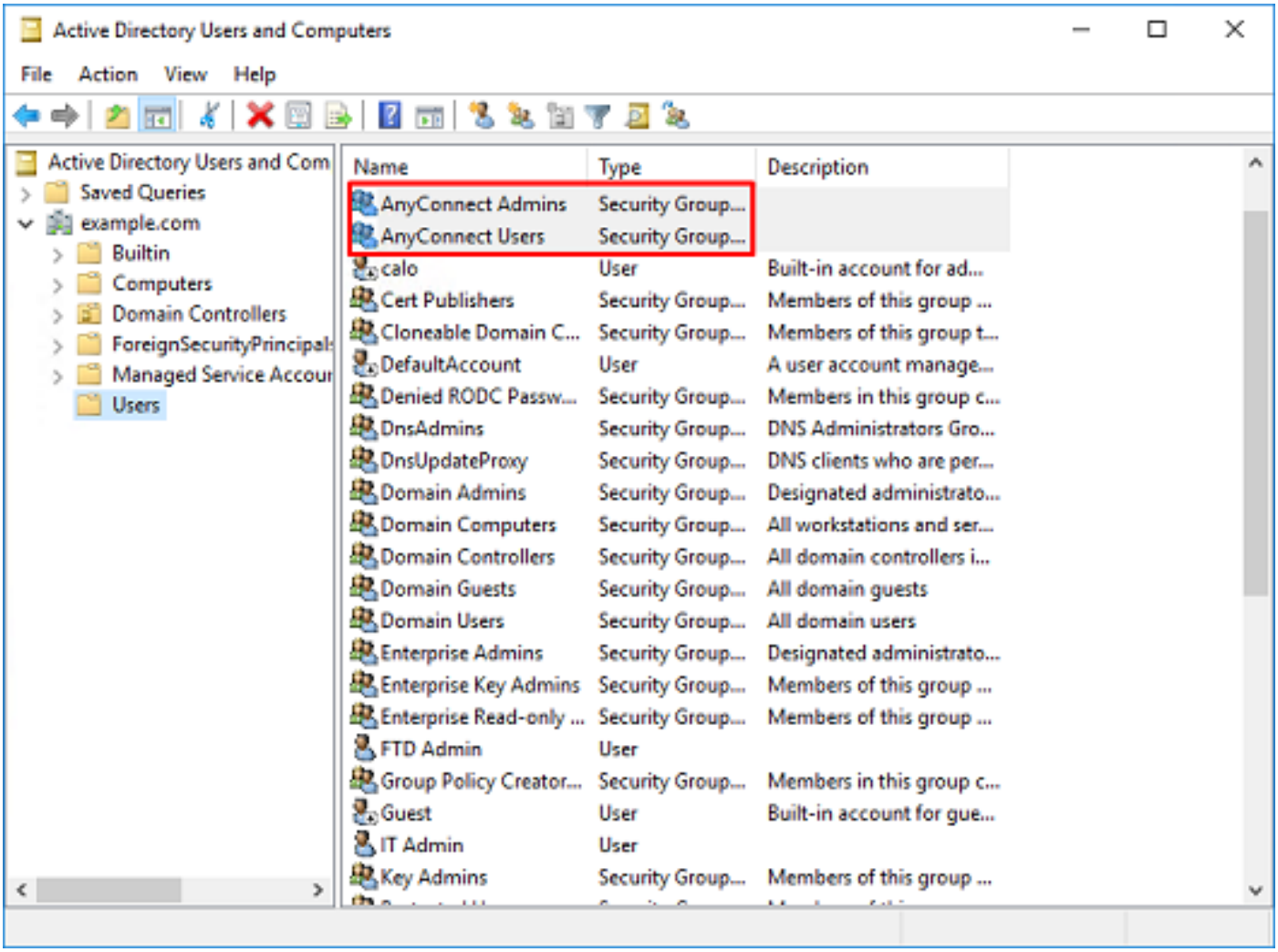
1. En **Active Directory Users and Computers**, haga clic con el botón derecho en el contenedor/organización al que se agregará el nuevo grupo. En este ejemplo, el grupo **Administradores de AnyConnect** se agregará debajo del contenedor Usuarios. Haga clic con el botón derecho del ratón en **Usuarios** y, a continuación, haga clic en **Nuevo > Grupo**.



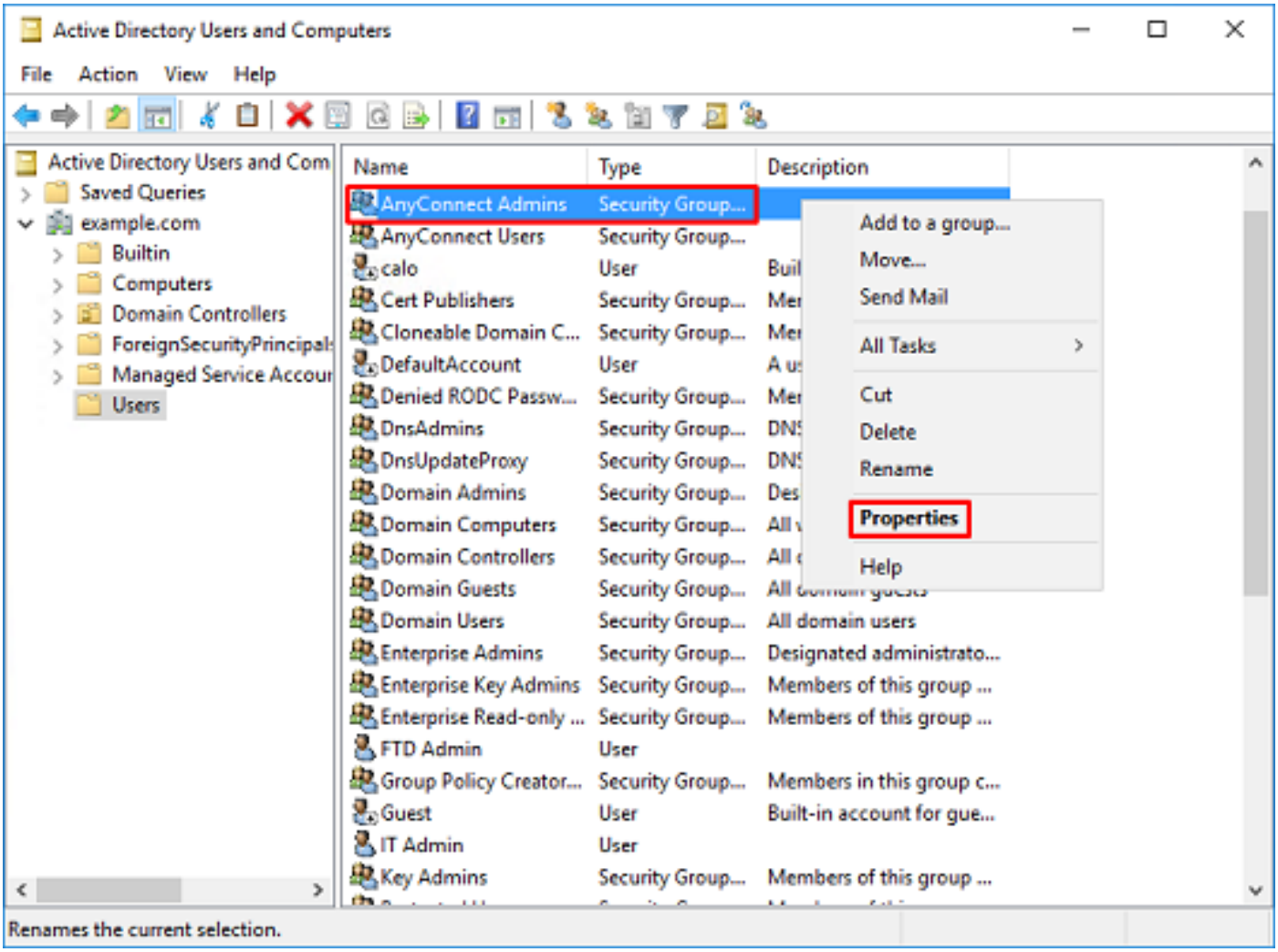
2. Desplácese por el Asistente **Nuevo objeto - grupo** como se muestra en la imagen.



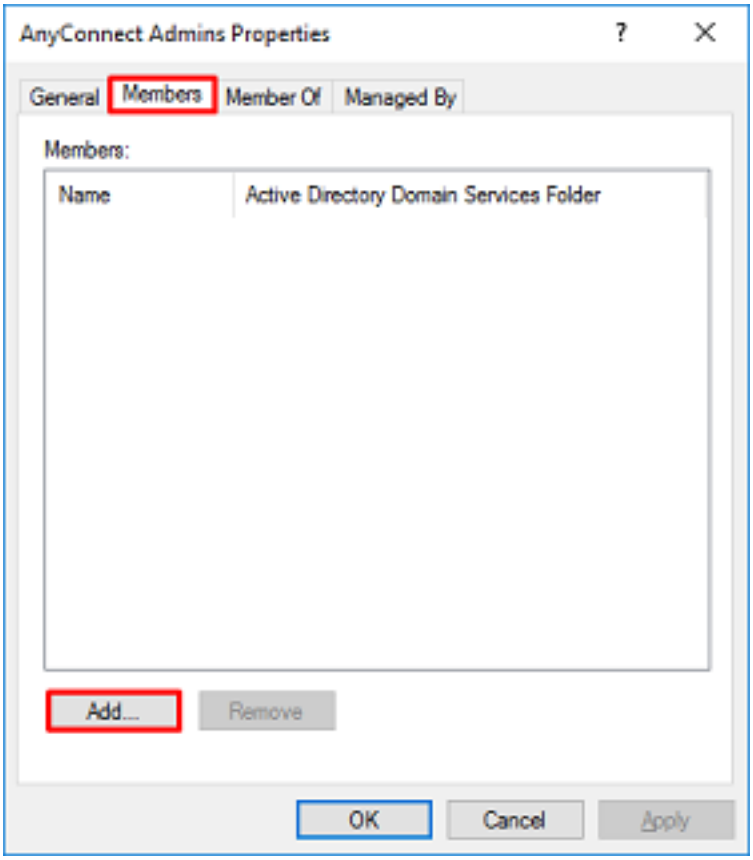
3. Verifique que se haya creado el grupo. También se ha creado el grupo **Usuarios de AnyConnect**.



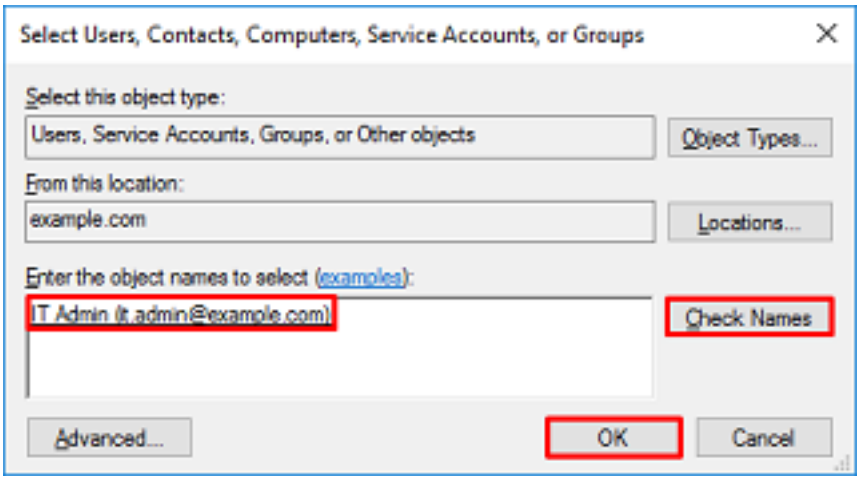
4. Haga clic con el botón derecho del ratón en el grupo al que se agregarán los usuarios y, a continuación, seleccione **Propiedades**. En esta configuración, el usuario **IT Admin** se agregará al grupo **AnyConnect Admins** y el usuario **Test User** se agregará al grupo **AnyConnect Users**.



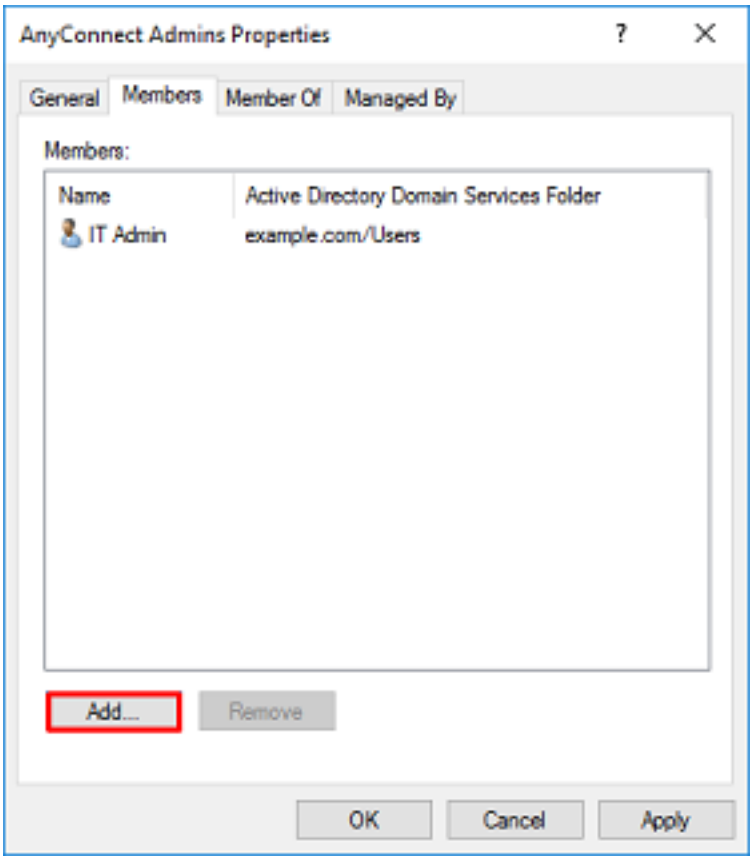
5. Haga clic en la ficha **Miembros** y luego haga clic en **Agregar** como se muestra en la imagen.



Ingrese el usuario en el campo y haga clic en el botón **Verificar nombres** para verificar que se encuentra el usuario. Una vez verificado, haga clic en **Aceptar**.

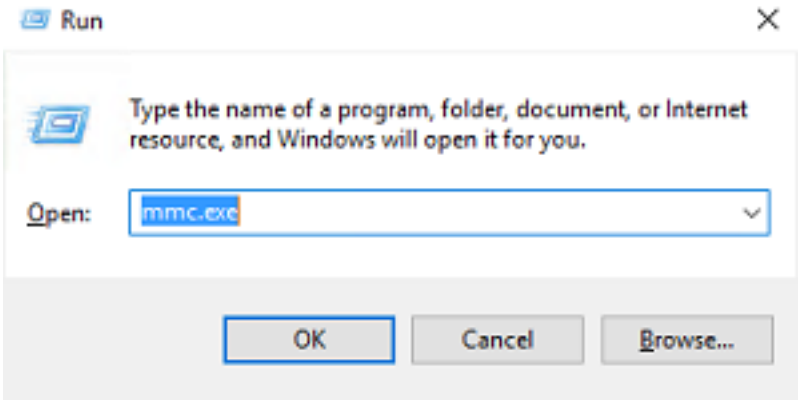


Compruebe que se ha agregado el usuario correcto y, a continuación, haga clic en el botón **Aceptar**. El usuario Test User también se agrega para agrupar usuarios de AnyConnect con el uso de los mismos pasos.

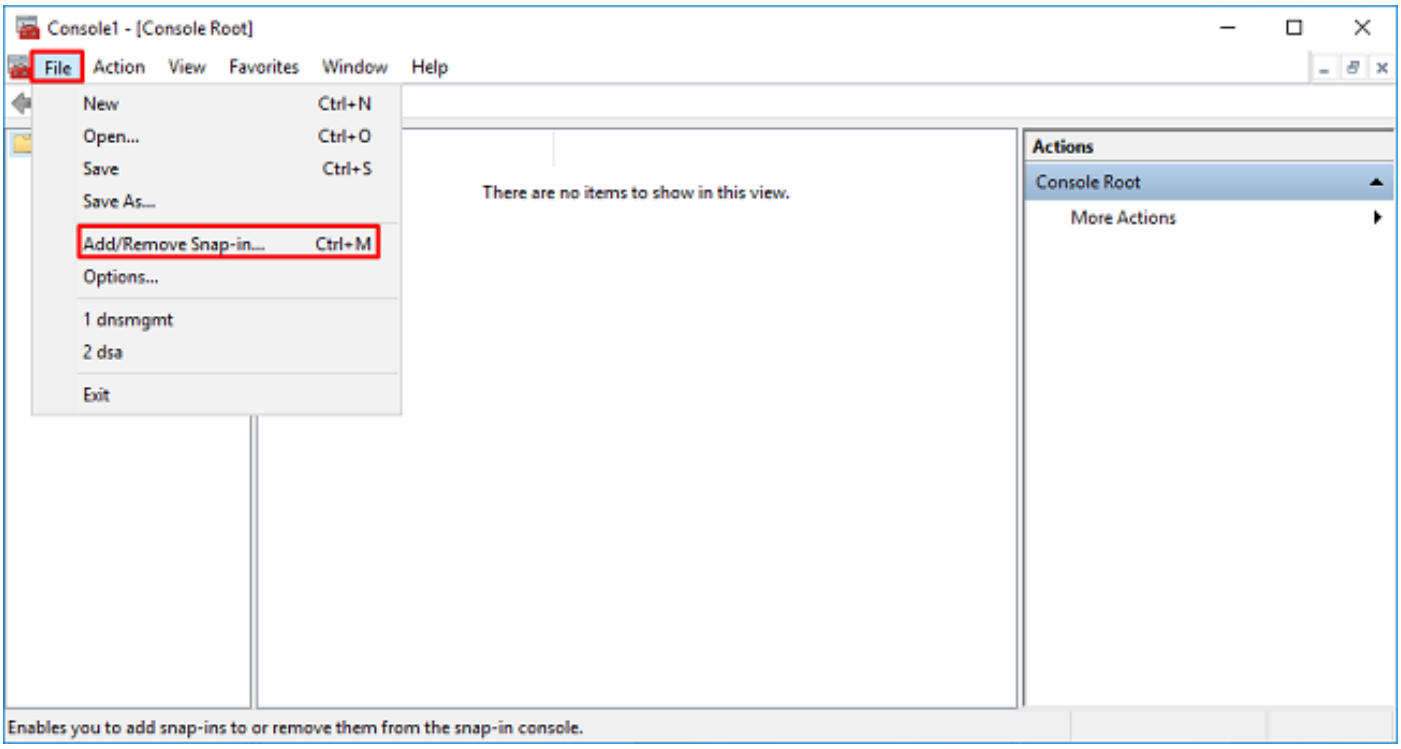


Copie la raíz del certificado SSL de LDAPS (sólo se requiere para LDAPS o STARTTLS)

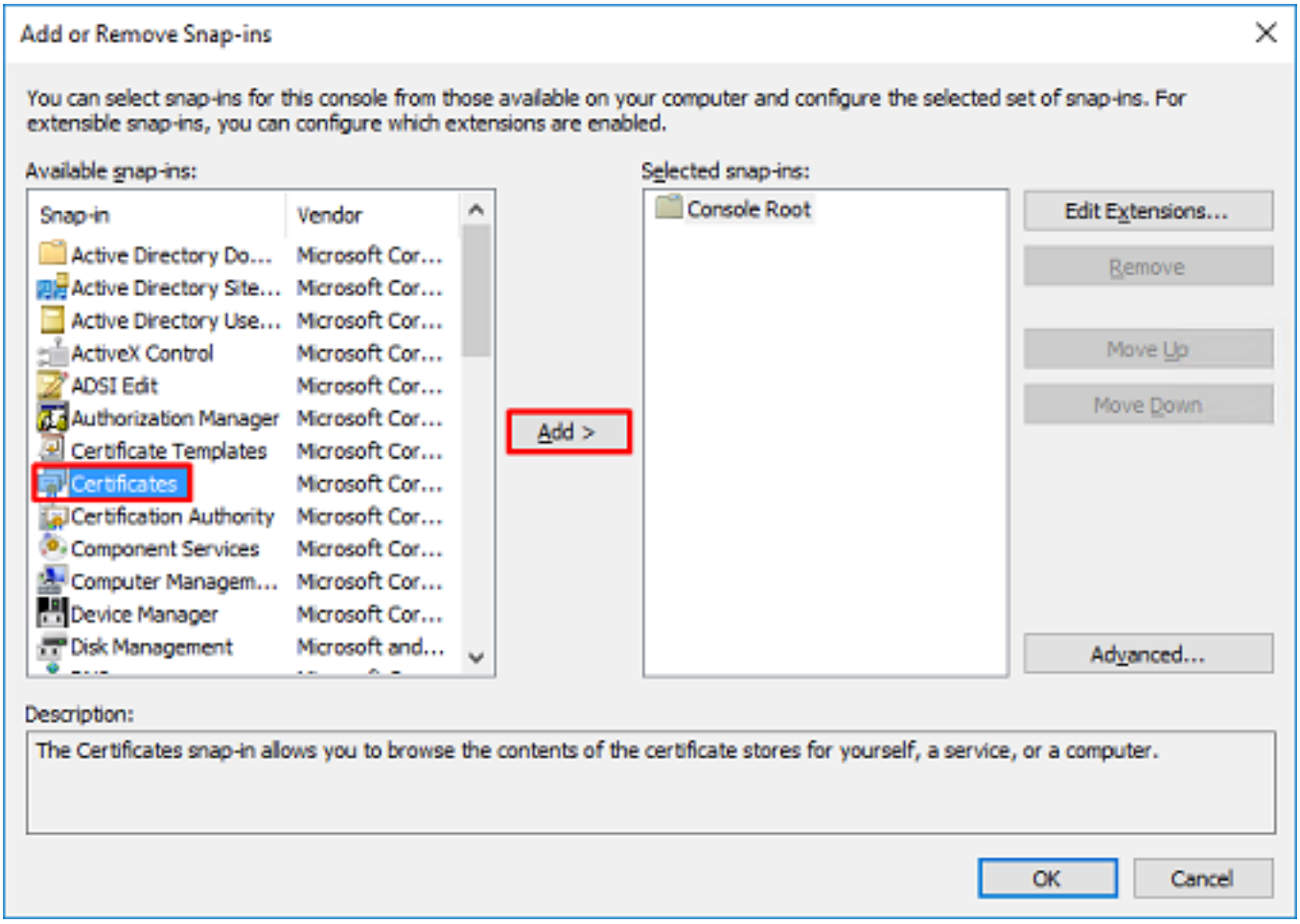
1. Presione **Win+R** y escriba **mmc.exe**. Click OK.



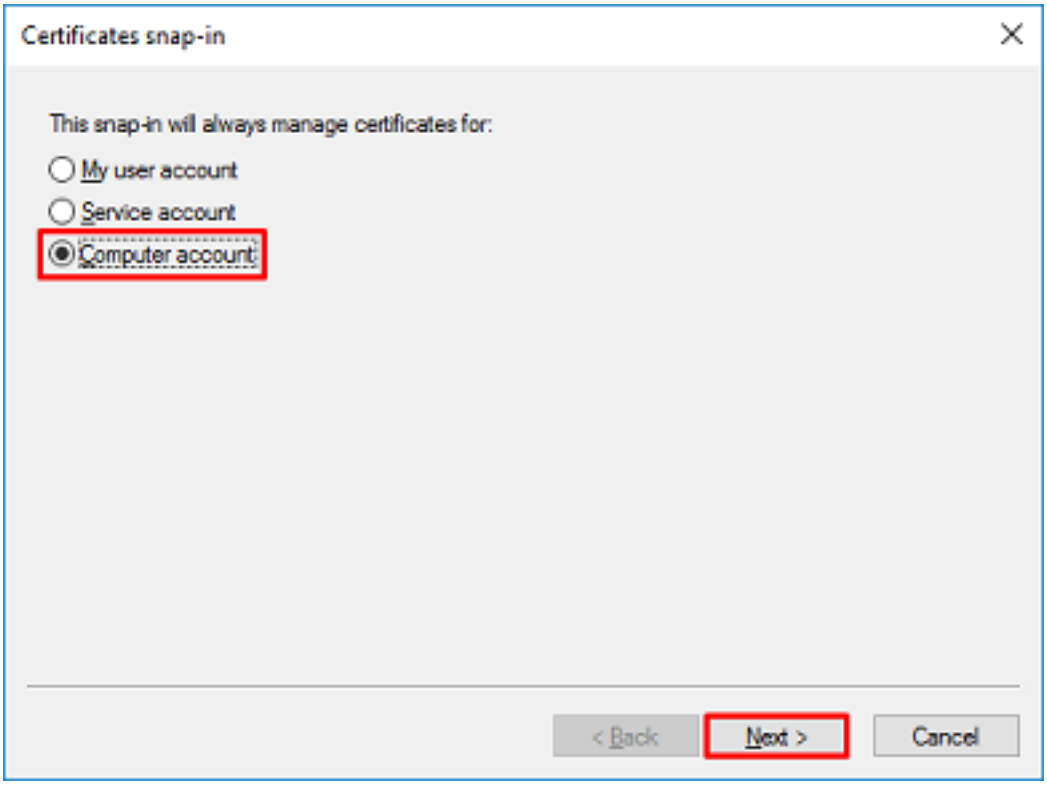
2. Vaya a **Archivo > Agregar/quitar complemento...** como se muestra en la imagen.



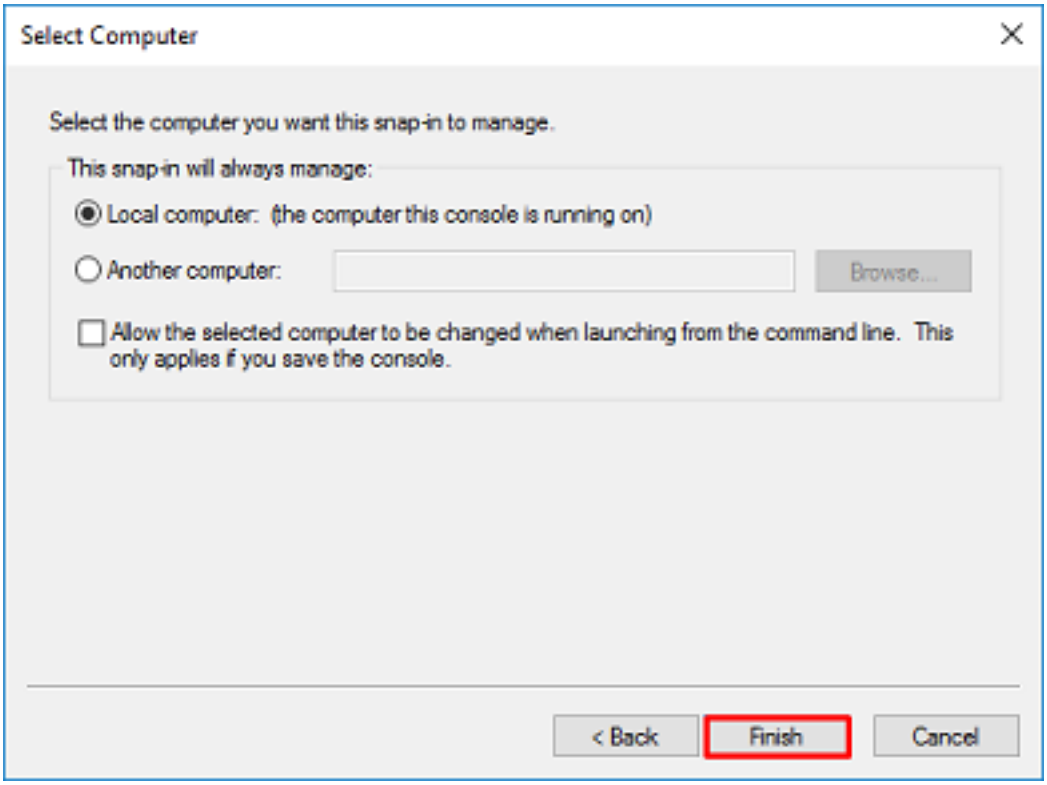
3. En los complementos disponibles, haga clic en **Certificados** y, a continuación, haga clic en **Agregar**.



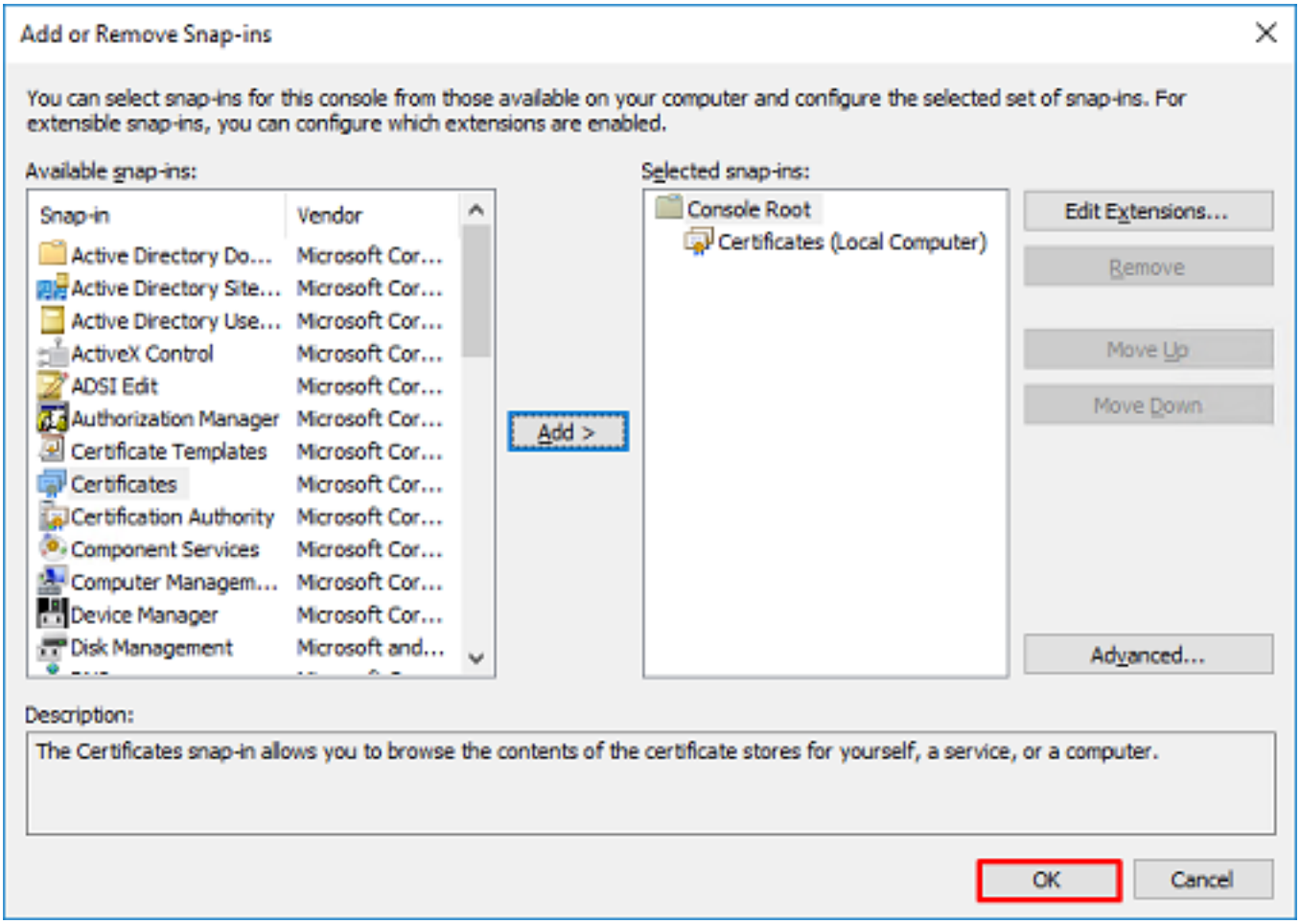
4. Seleccione **Computer account** y luego haga clic en **Next** como se muestra en la imagen.



Haga clic en Finish (Finalizar).



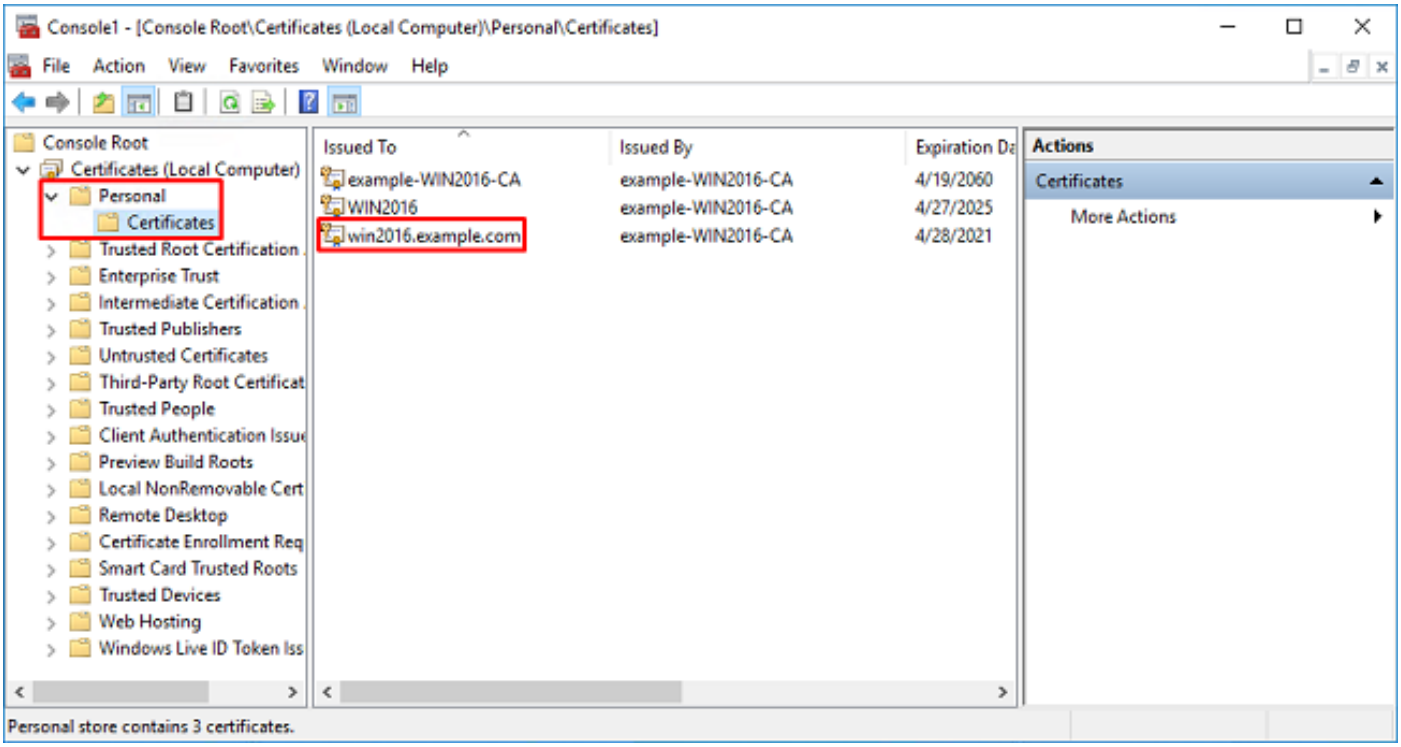
5. Click OK.



6. Expanda la carpeta **Personal** y, a continuación, haga clic en **Certificados**. El certificado utilizado por LDAPS se debe emitir al nombre de dominio completo (FQDN) del servidor de Windows. En este servidor, hay 3 certificados en la lista.

- Un certificado CA emitido a y por ejemplo-WIN2016-CA.
- Un certificado de identidad emitido a WIN2016 por ejemplo-WIN2016-CA.
- Un certificado de identidad emitido para win2016.example.com por ejemplo-WIN2016-CA.

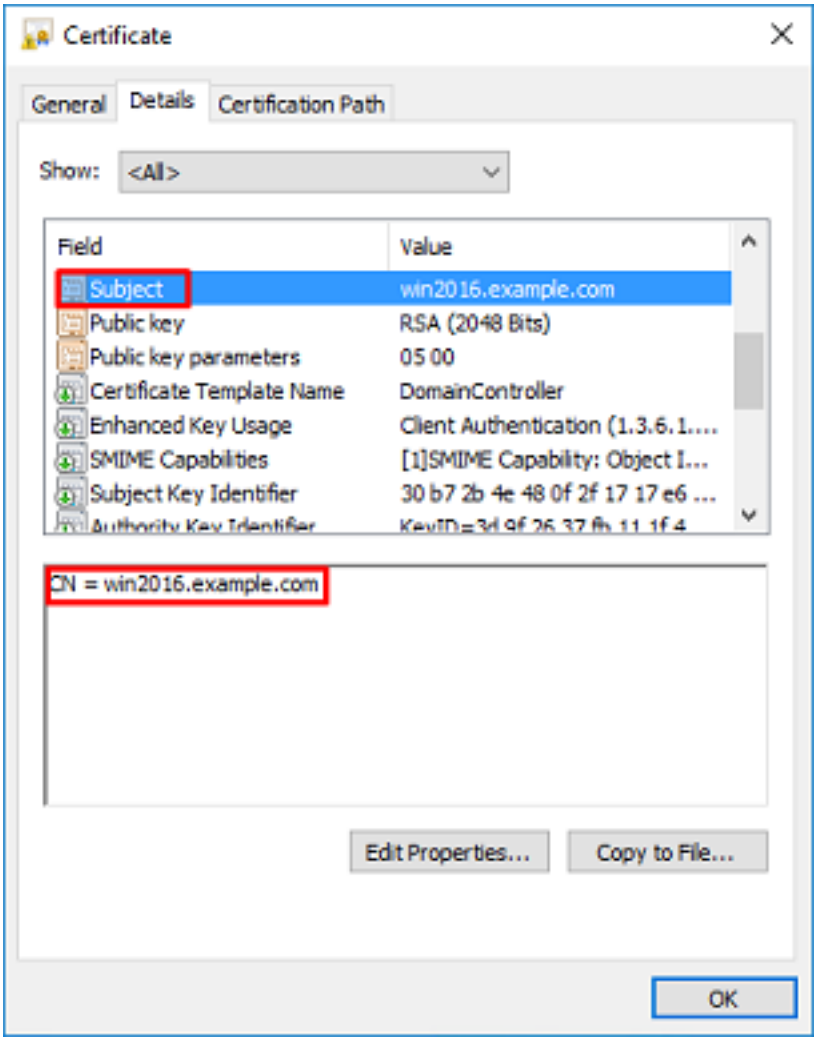
En esta guía de configuración, el FQDN es win2016.example.com, por lo que los primeros 2 certificados no son válidos para utilizarse como certificado SSL de LDAPS. El certificado de identidad emitido para win2016.example.com es un certificado que fue emitido automáticamente por el servicio CA de Windows Server. Haga doble clic en el certificado para comprobar los detalles.

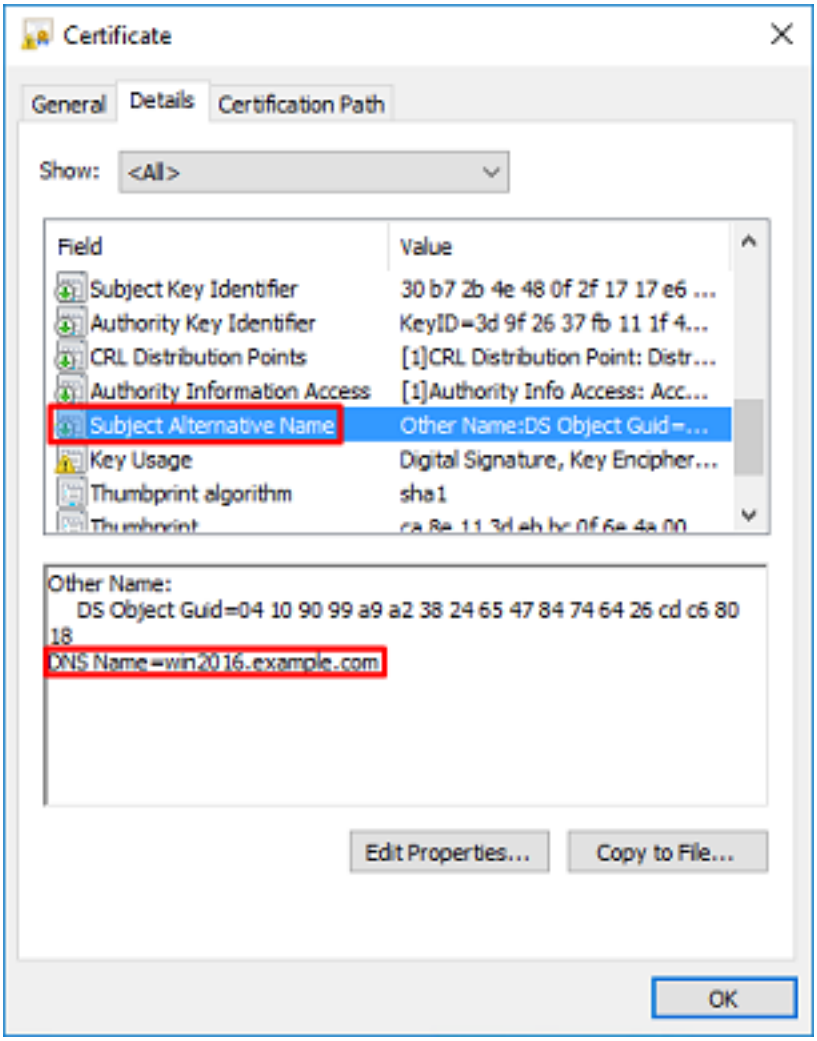


7. Para ser utilizado como certificado SSL LDAPS, el certificado debe cumplir estos requisitos:

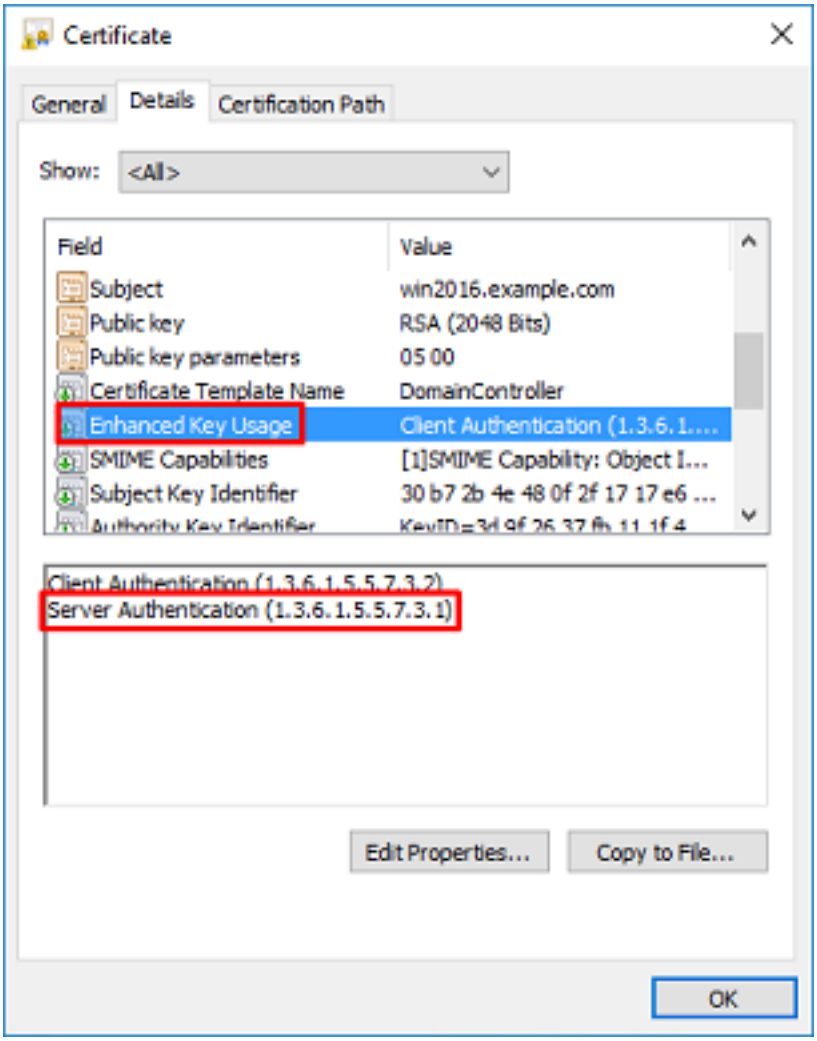
- El nombre común o el nombre alternativo del asunto DNS coincide con el FQDN del servidor de Windows.
- El certificado tiene autenticación de servidor en el campo Uso mejorado de clave.

En la pestaña Detalles del certificado, bajo **Asunto** y **Nombre alternativo del sujeto**, está presente el FQDN **win2016.example.com**.

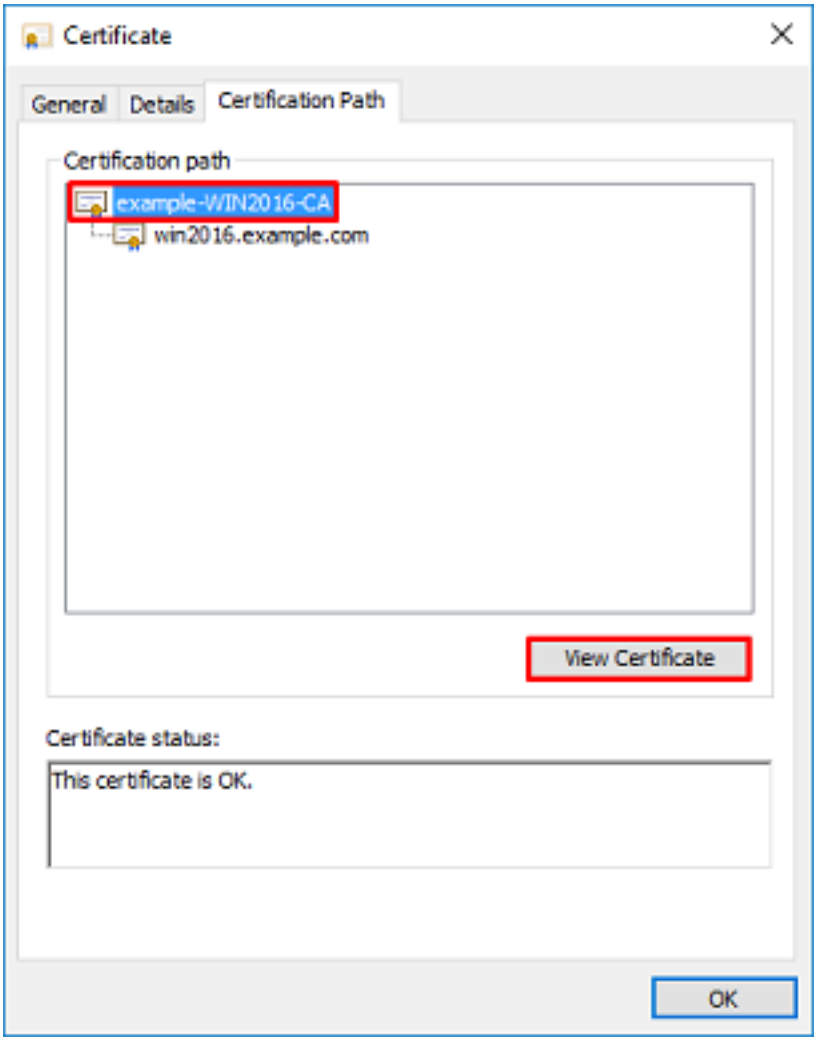

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
win2016.example.com
Public key
RSA (2048 Bits)
Public key parameters
05 00
Certificate Template Name
DomainController
Enhanced Key Usage
Client Authentication (1.3.6.1....
SMIME Capabilities
[1]SMIME Capability: Object I...
Subject Key Identifier
30 b7 2b 4e 48 0f 2f 17 17 e6 ...
CN = win2016.example.com
Edit Properties...
Copy to File...
OK



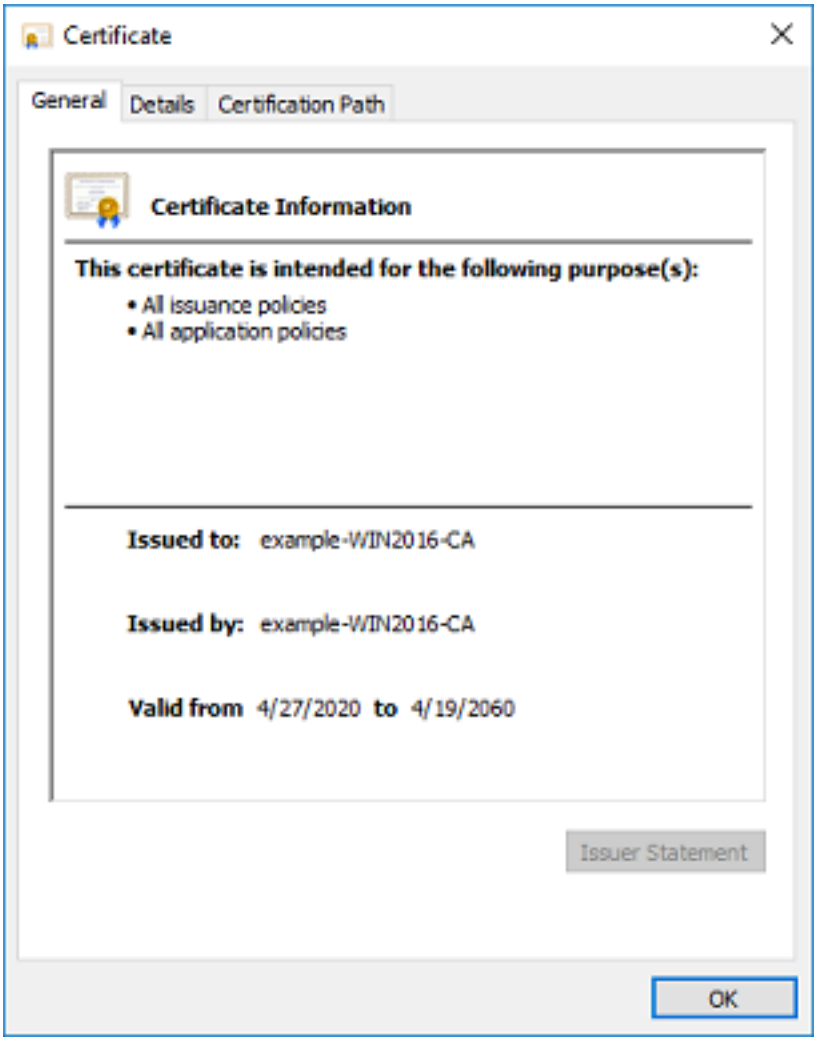
En **Uso mejorado de claves**, **Server Authentication** está presente.



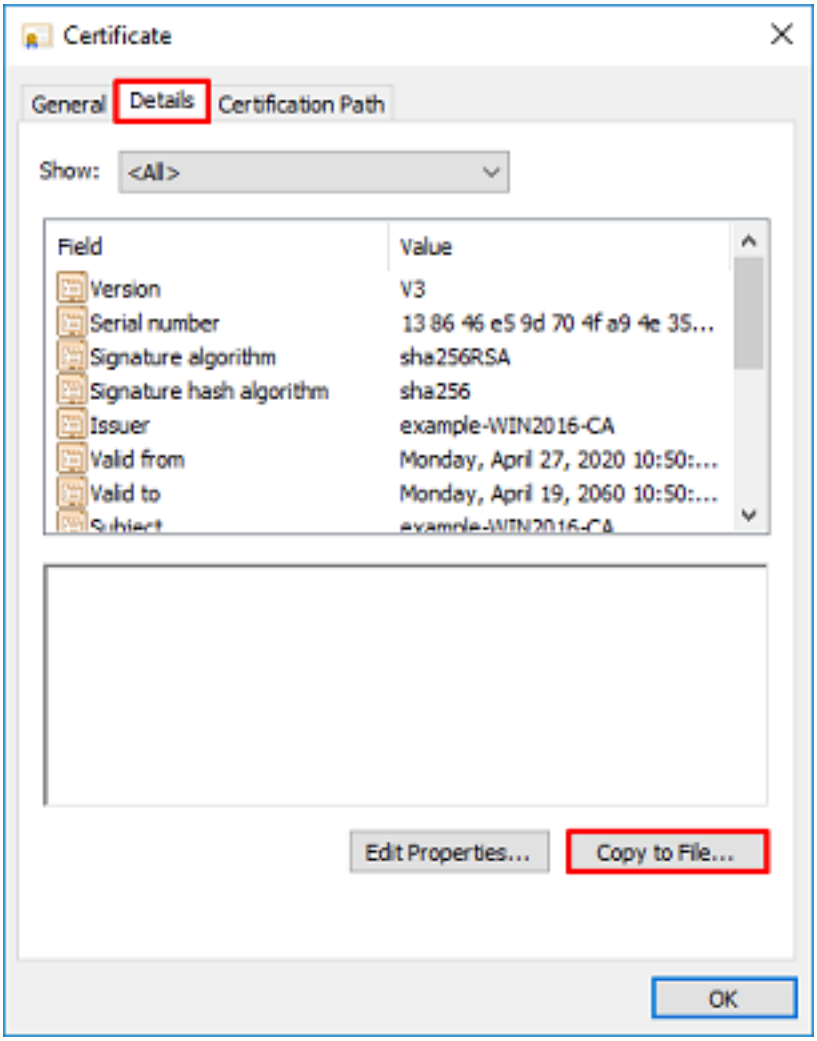
8. Una vez que se confirme, vaya a la pestaña **Ruta de certificación**. Haga clic en el certificado superior que debe ser el certificado de CA raíz y luego haga clic en el botón **Ver certificado**.



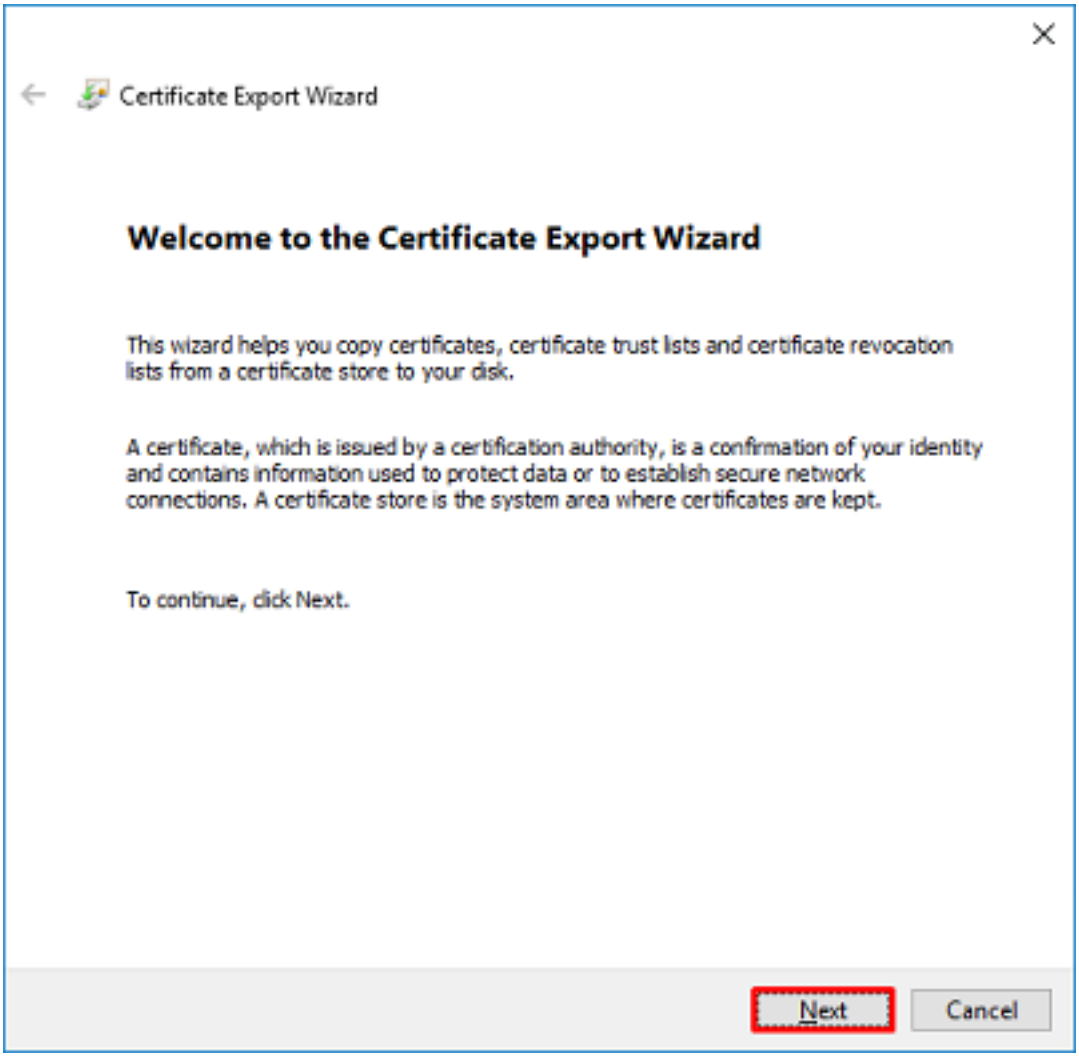
9. Esto abrirá los detalles del certificado para el certificado de CA raíz.



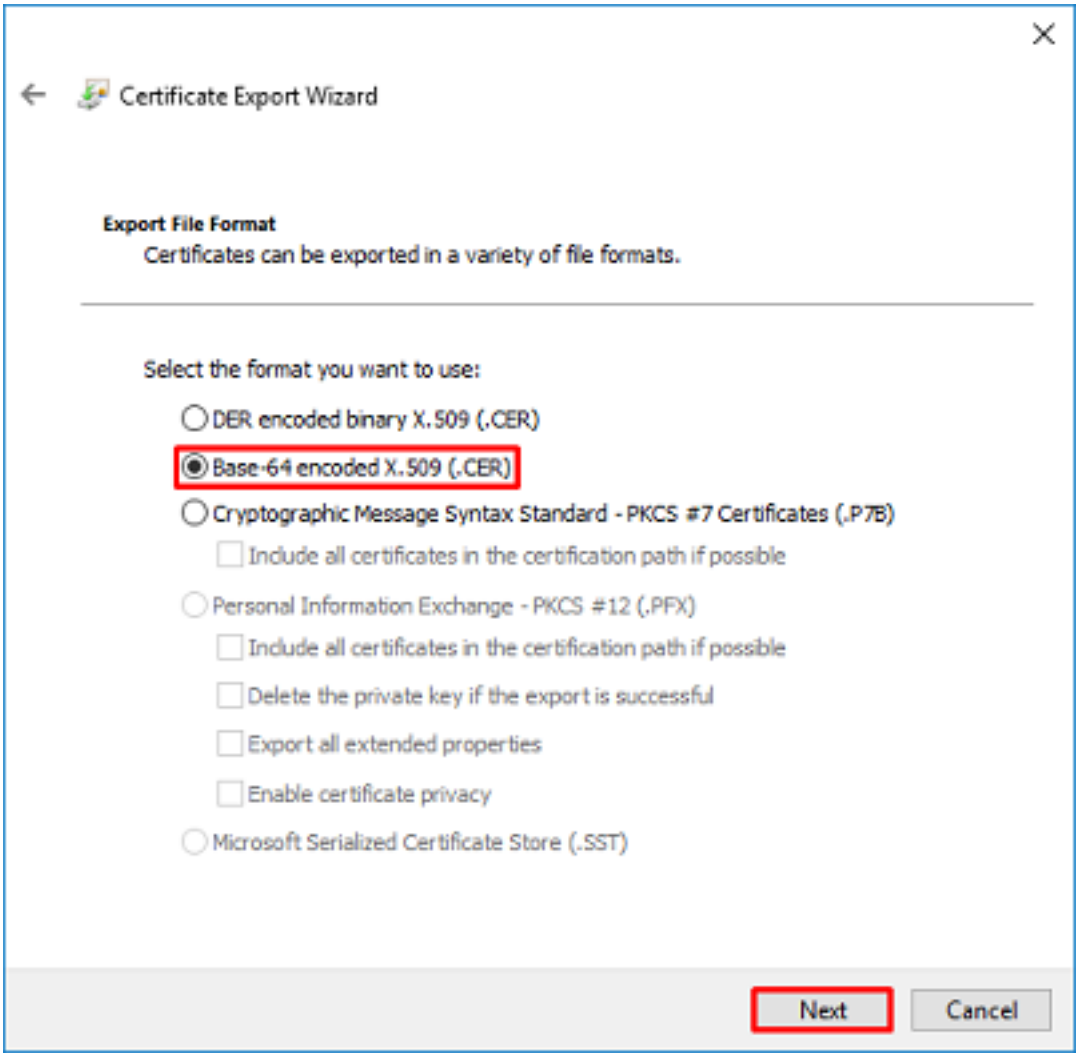
10. Abra la pestaña **Detalles** y haga clic en **Copiar a archivo...** como se muestra en la imagen.



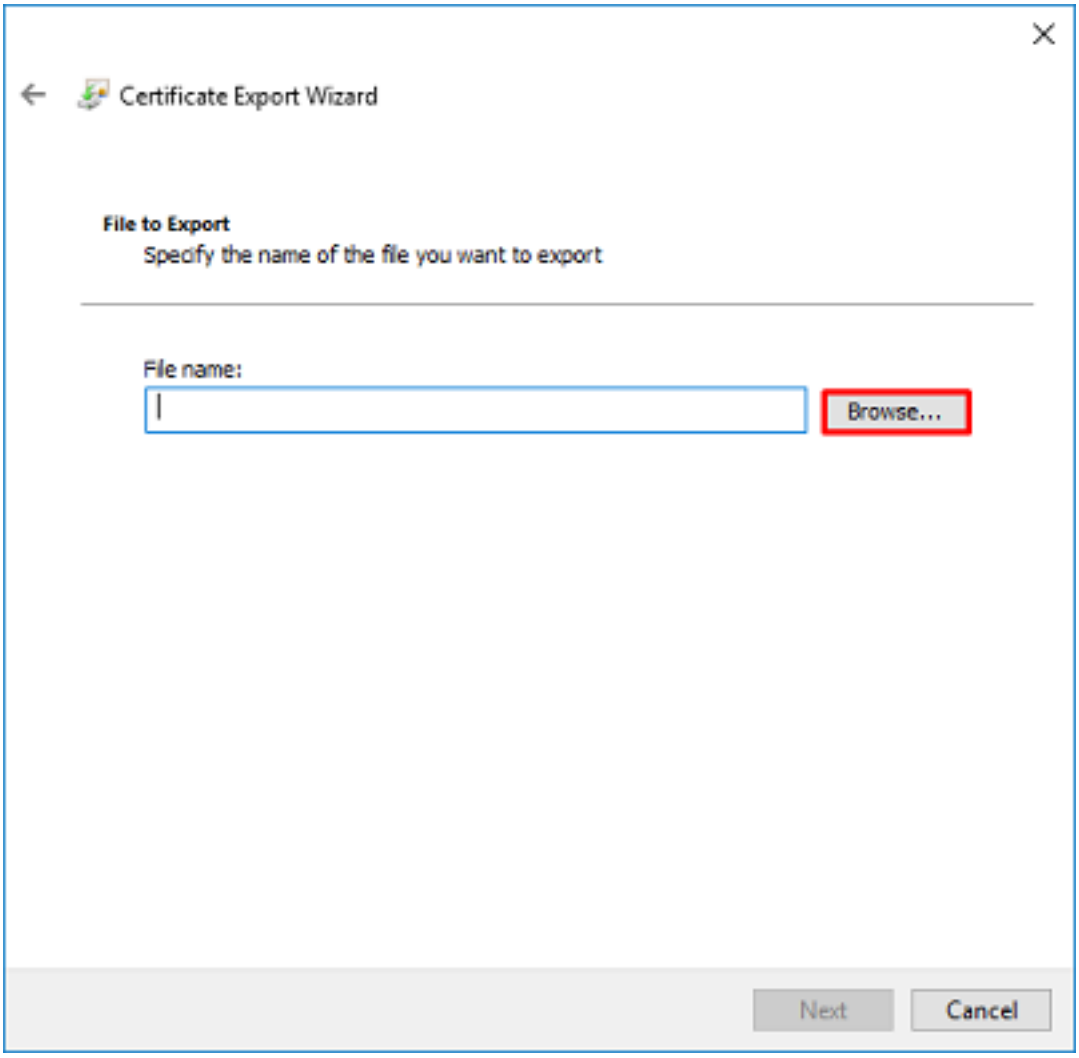
11. Desplácese por el Asistente para exportación de certificados que exportará la CA raíz en formato PEM.

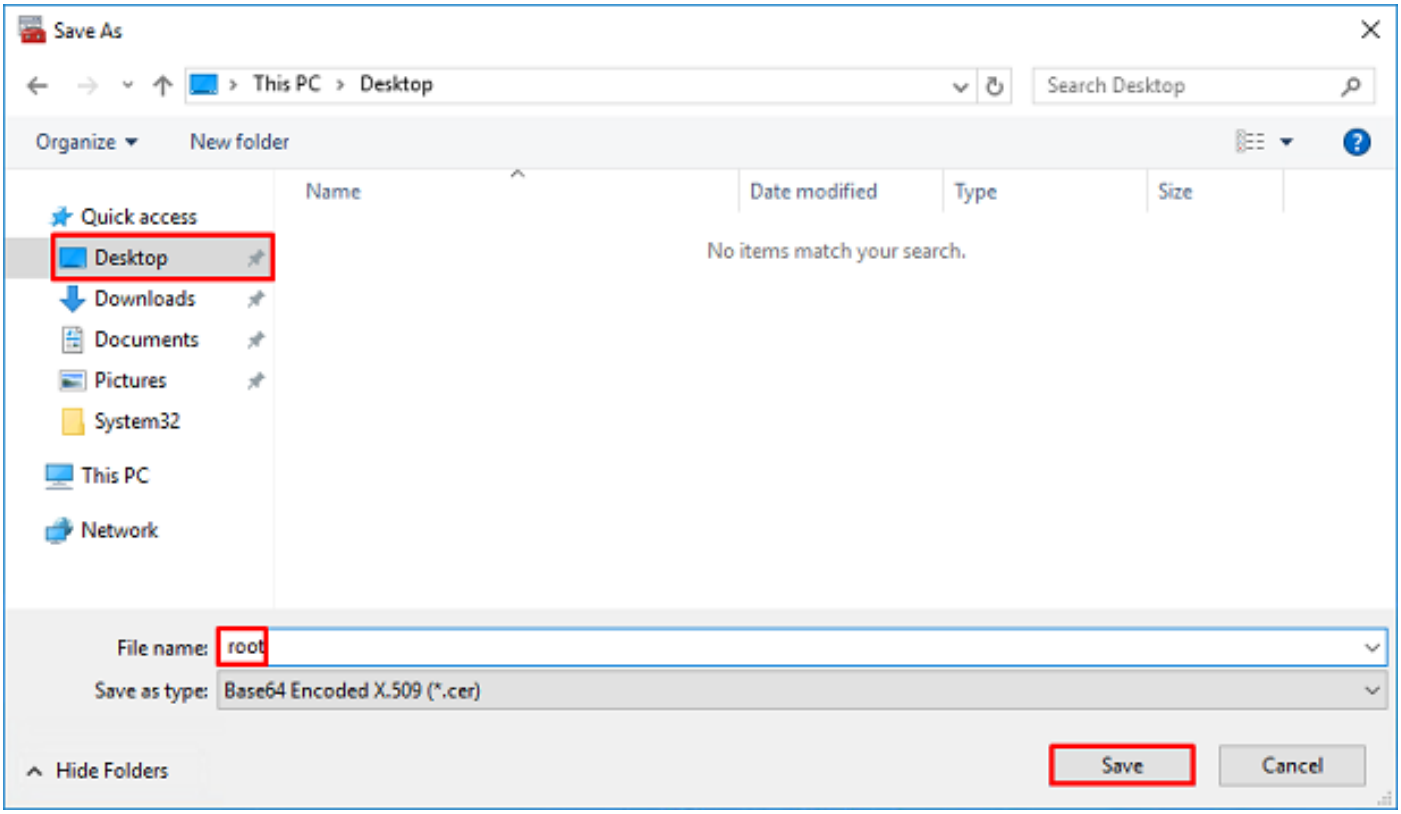


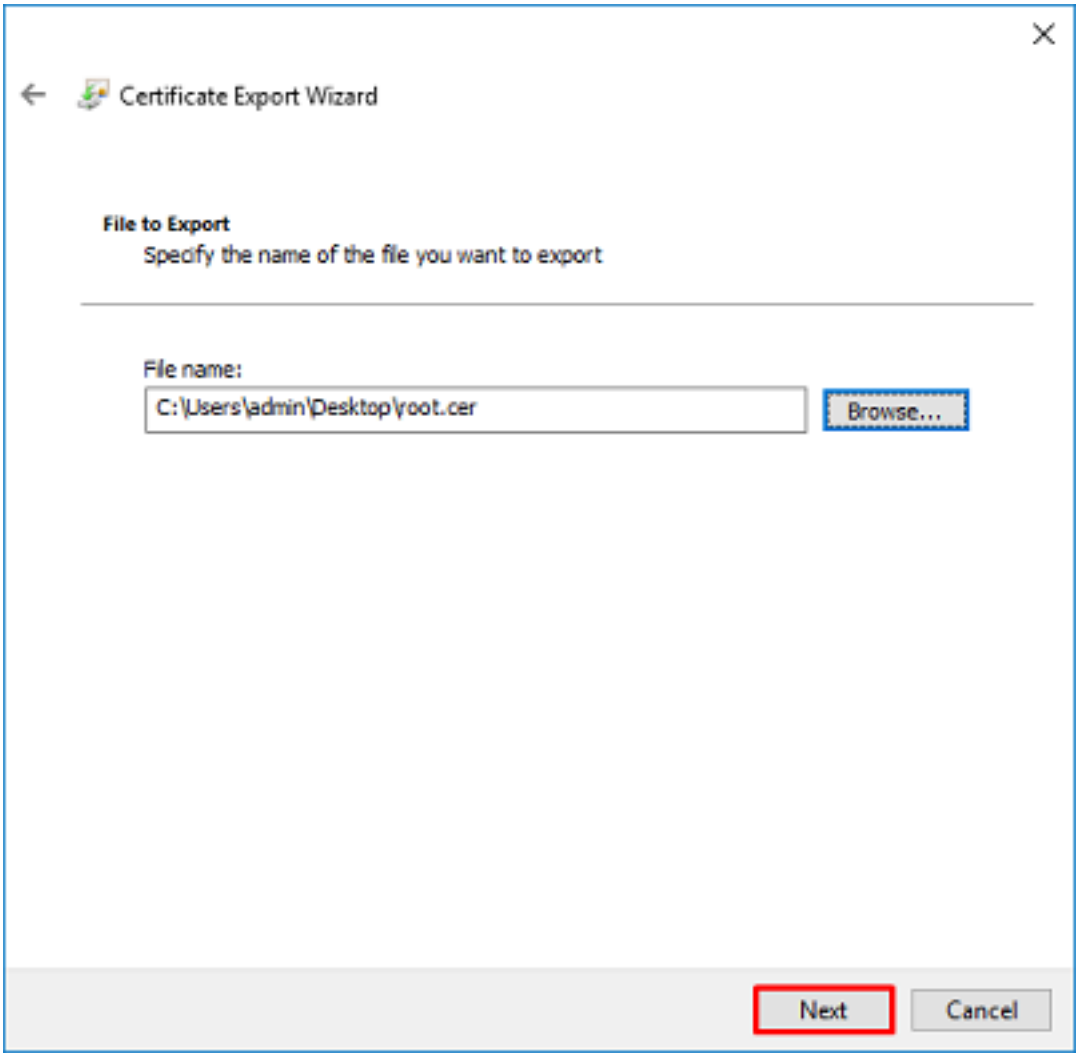
12. Seleccione **Base-64 codificada X.509**.



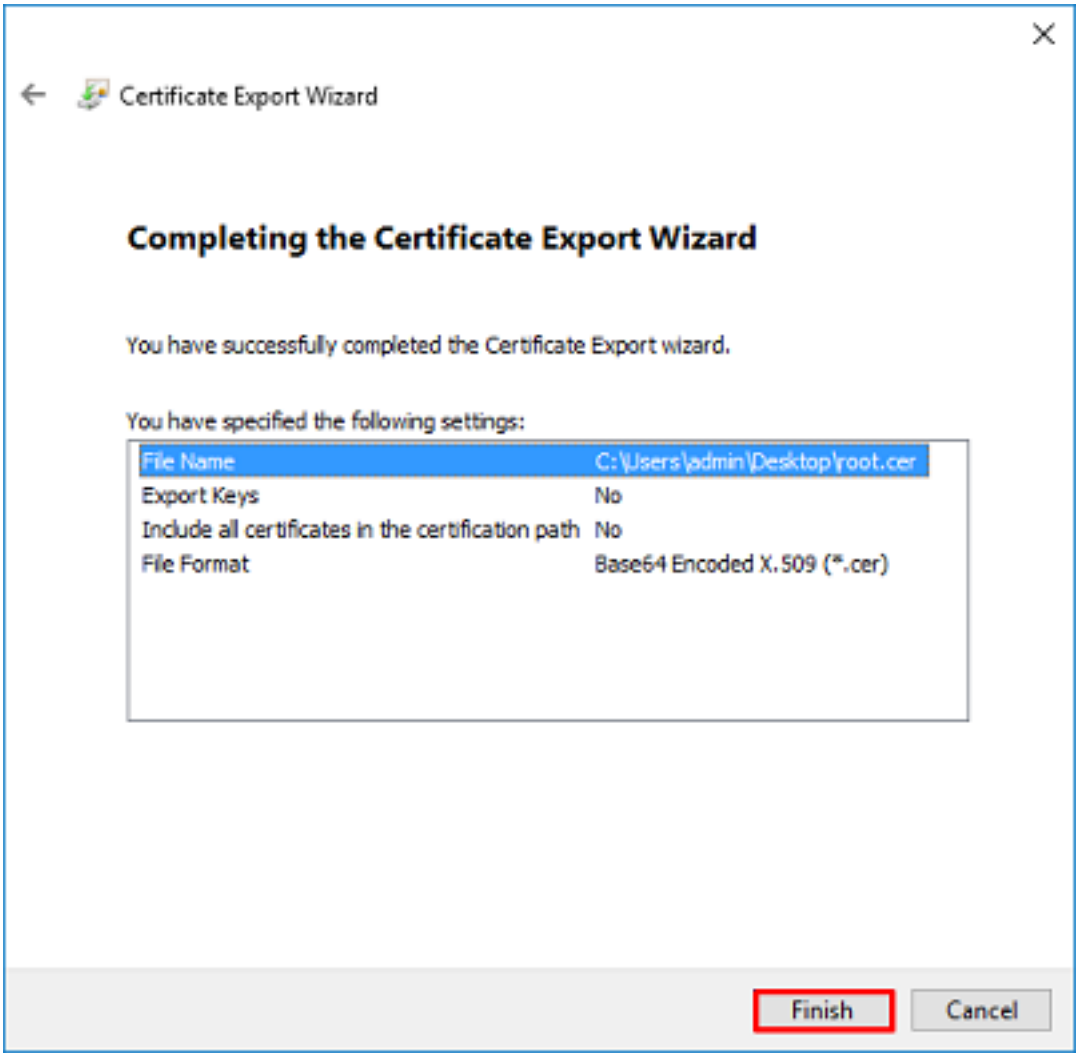
13. Seleccione el nombre del archivo y el lugar al que se exportará.


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Browse...
Next
Cancel


Save As
This PC
Desktop
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
No items match your search.
File name:
root
Save as type:
Base64 Encoded X.509 (*.cer)
Hide Folders
Save
Cancel



14. Haga clic en Finish (Finalizar).



15. Ahora, desplácese a la ubicación y abra el certificado con un bloc de notas o con algún otro editor de texto. Esto mostrará el certificado de formato PEM. Guarde esto para más adelante.

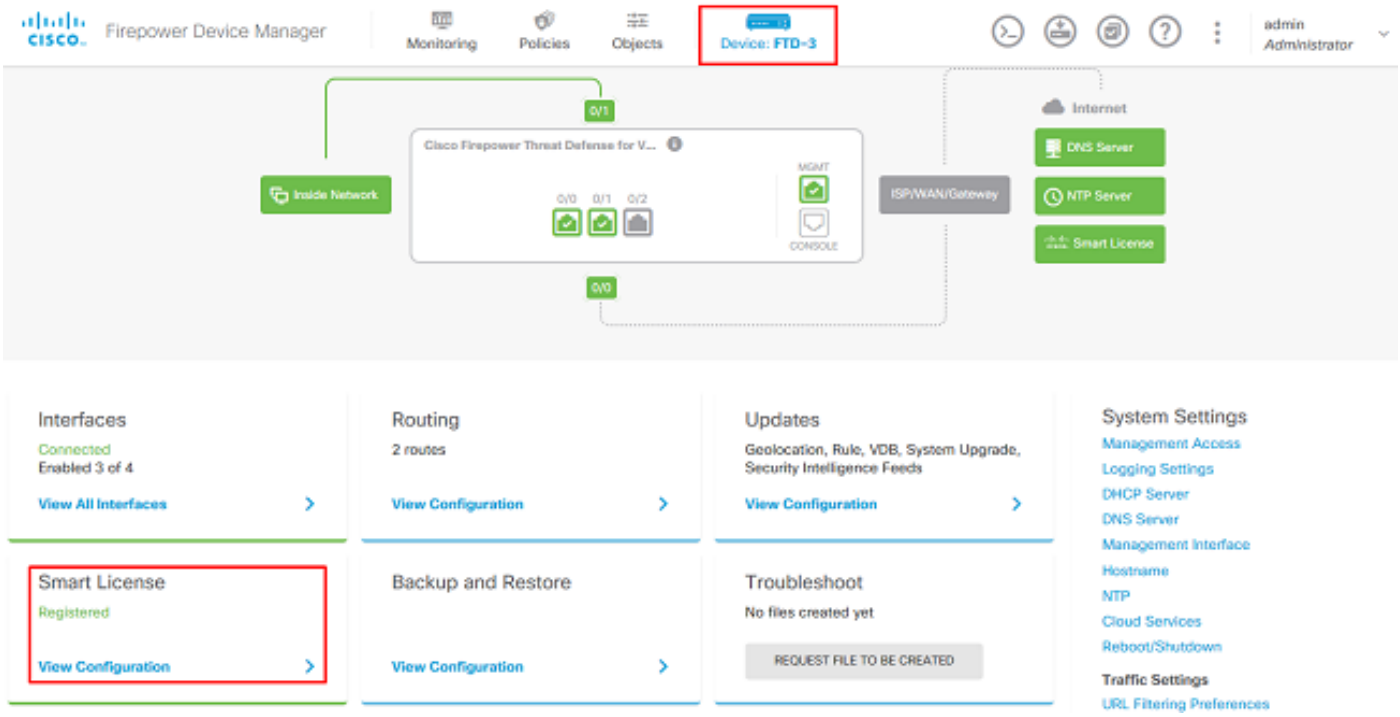
```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

Configuraciones de FDM

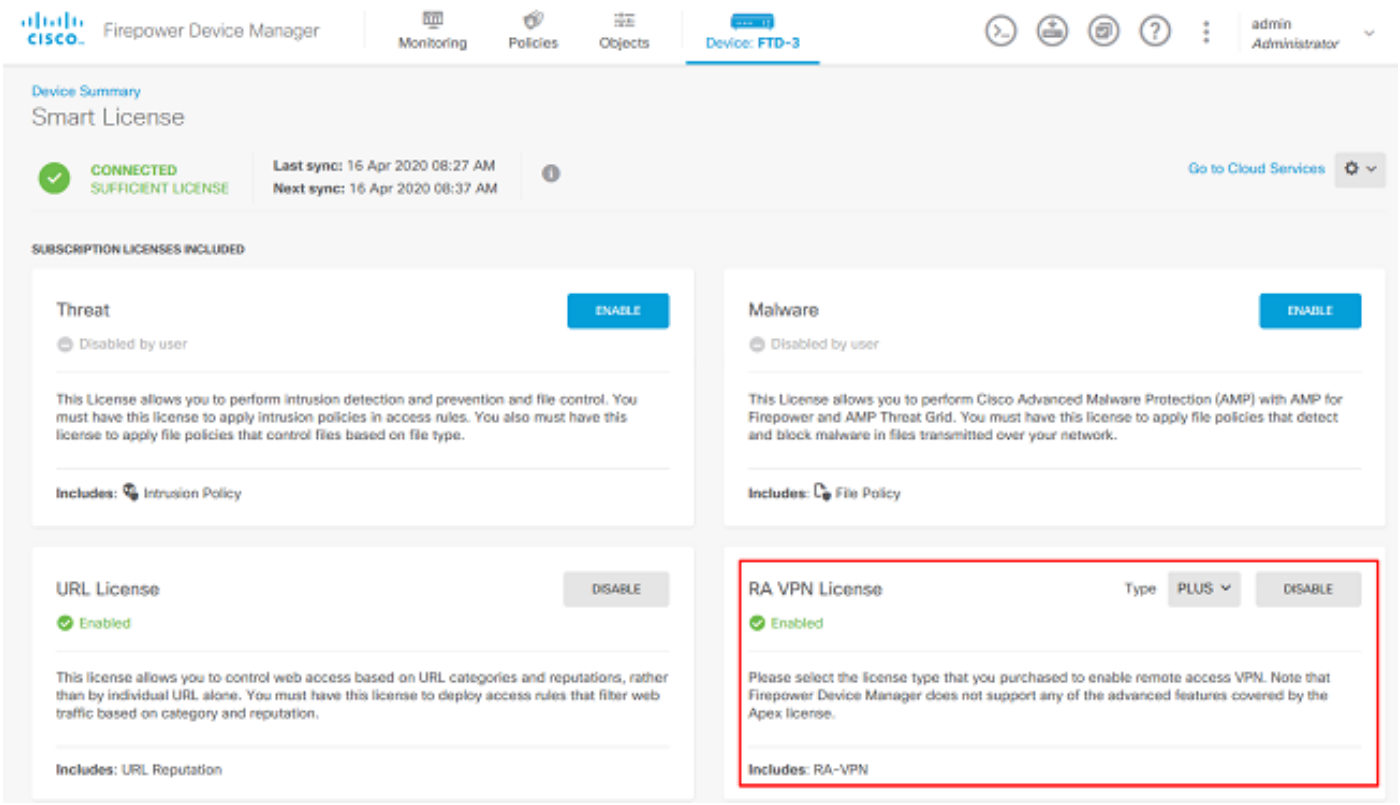
Verificación de licencias

Para configurar AnyConnect en FDM, el FTD deberá estar registrado con el servidor de licencias inteligente y se debe aplicar una licencia válida Plus, Apex o VPN Only al dispositivo.

1. Vaya a **Device > Smart License** como se muestra en la imagen.



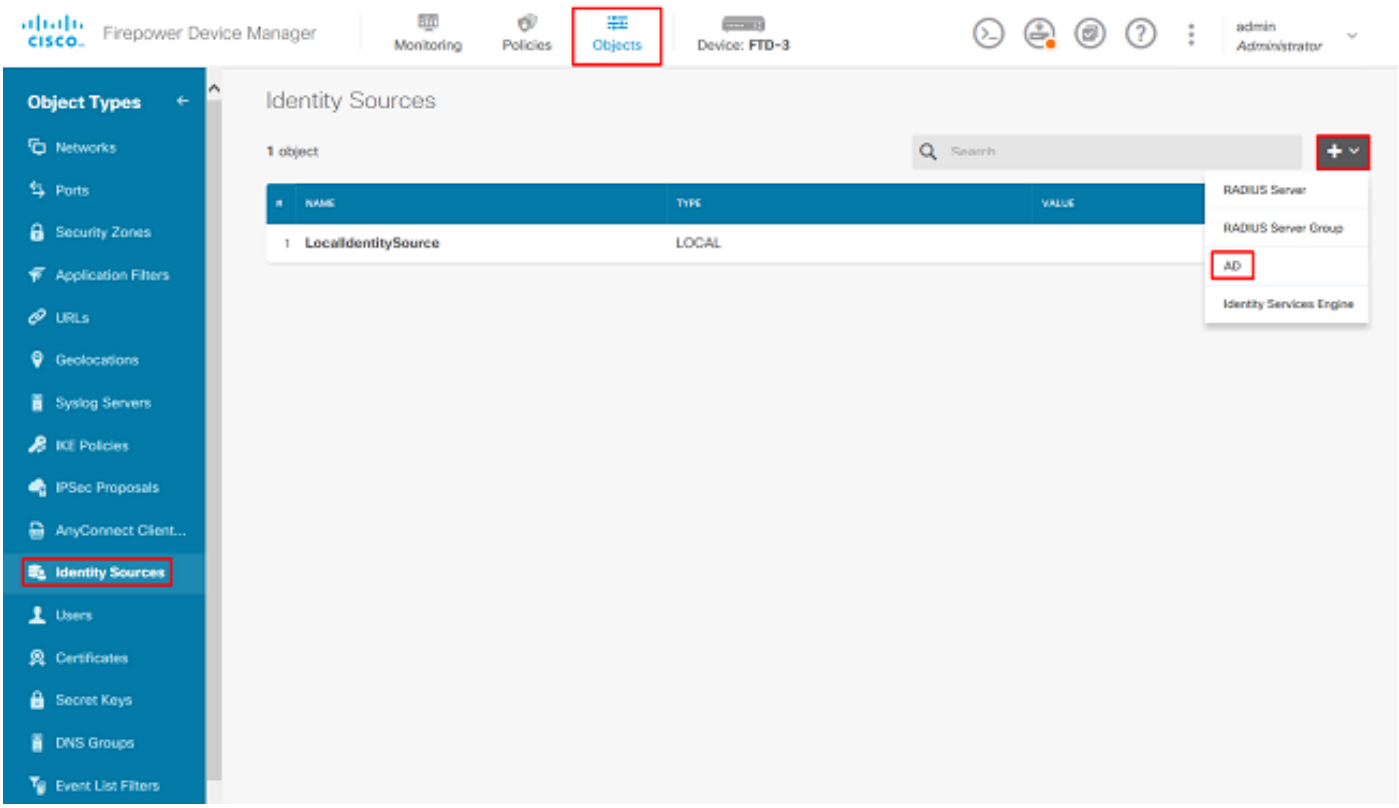
2. Verifique que el FTD esté registrado en el servidor de licencias inteligente y que la licencia AnyConnect Plux, Apex o VPN Only esté habilitada.



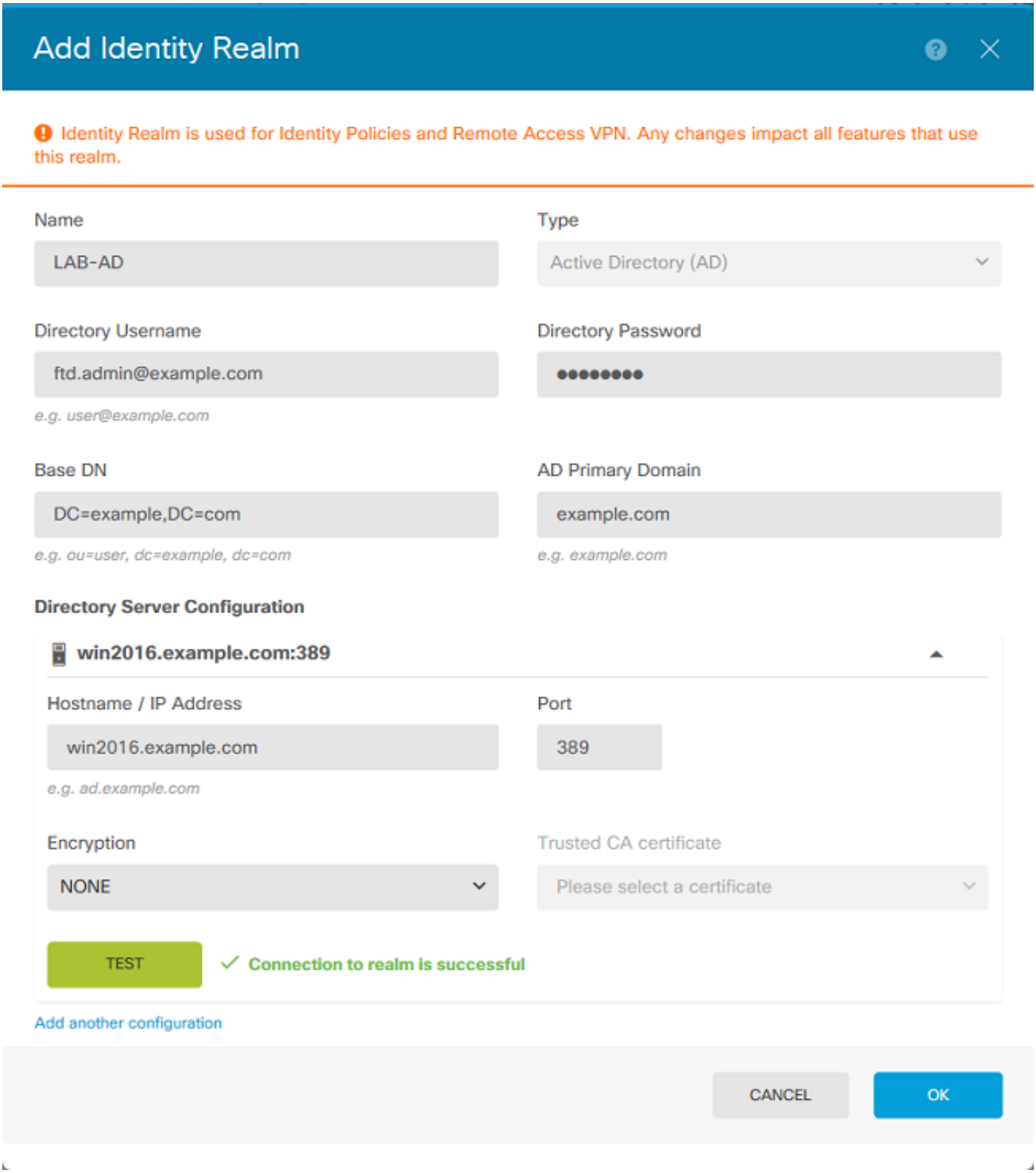
Configurar origen de identidad AD

1. Navegue hasta **Objetos > Orígenes de identidad**, luego haga clic en el **+** símbolo y seleccione

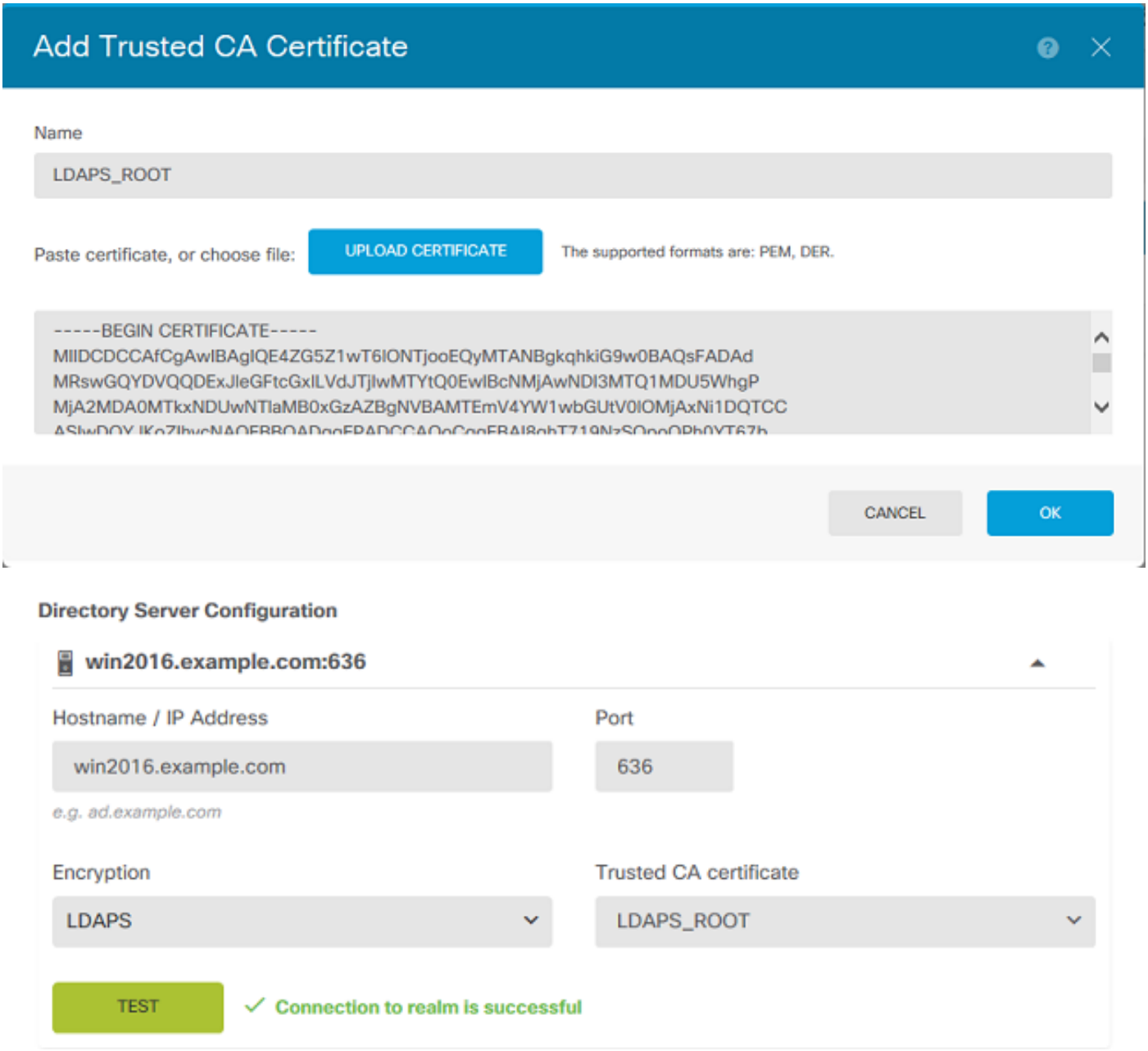
AD como se muestra en la imagen.



2. Complete los parámetros adecuados para el servidor de Active Directory con la información recolectada anteriormente. Si se utiliza un nombre de host (FQDN) para el servidor de Microsoft en lugar de una dirección IP, asegúrese de crear un grupo DNS adecuado en **Objetos > Grupo DNS**. A continuación, aplique ese grupo DNS al FTD navegando a **Device > System Settings > DNS Server**, aplicando el grupo DNS en **Management Interface** y **Data Interface**, y luego especifique la interfaz de salida adecuada para las consultas DNS. Haga clic en el botón **Prueba** para verificar una configuración y alcance exitosos desde la interfaz de administración de FTD. Dado que estas pruebas se inician desde la interfaz de administración del FTD y no a través de una de las interfaces enrutables configuradas en el FTD (como interna, externa, 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 iniciarán desde una de las interfaces enrutables del FTD. Para obtener más información sobre la prueba de conexiones LDAP desde el FTD, revise las secciones Test AAA y Packet Capture en el área Troubleshooting.



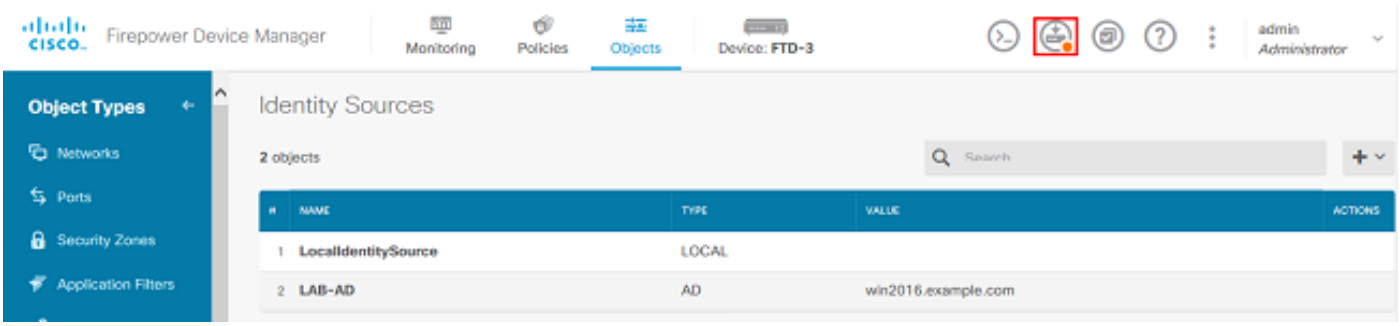
Si se utiliza LDAPS o STARTTLS, seleccione el cifrado adecuado y, a continuación, seleccione el certificado de CA de confianza. Si la CA raíz no se ha agregado aún, haga clic en **Crear nuevo certificado de CA de confianza**. Proporcione un nombre para el certificado de CA raíz y luego pegue el certificado de CA raíz del formato PEM recolectado anteriormente.



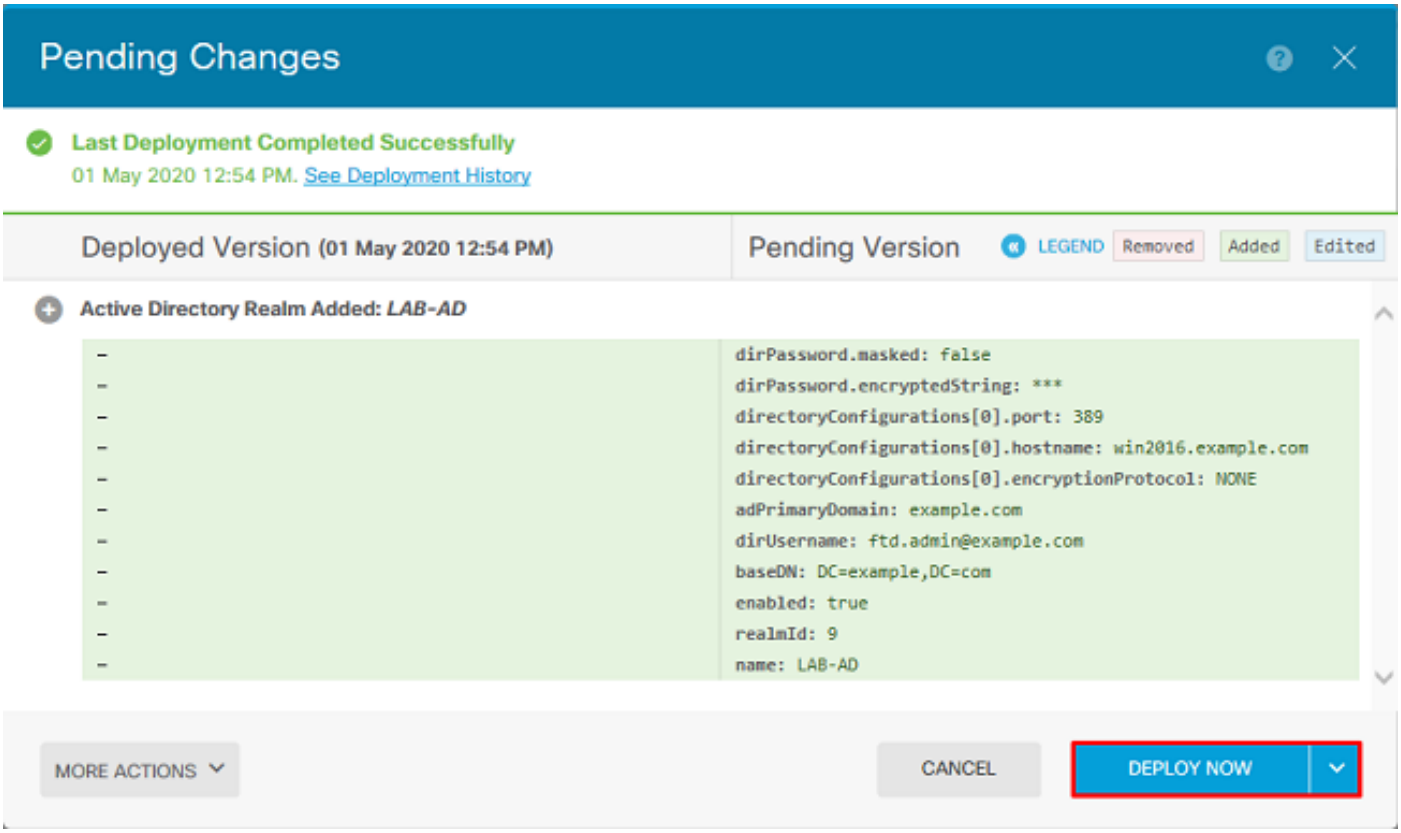
En esta configuración, se utilizaron estos valores:

- Nombre: LAB-AD
- Nombre de usuario del directorio: ftd.admin@example.com
- DN base: DC=ejemplo,DC=com
- Dominio primario de AD: example.com
- Nombre de host/Dirección IP: win2016.example.com
- Puerto: 389

3. Haga clic en el botón **Cambios pendientes** en la parte superior derecha, como se muestra en la imagen.



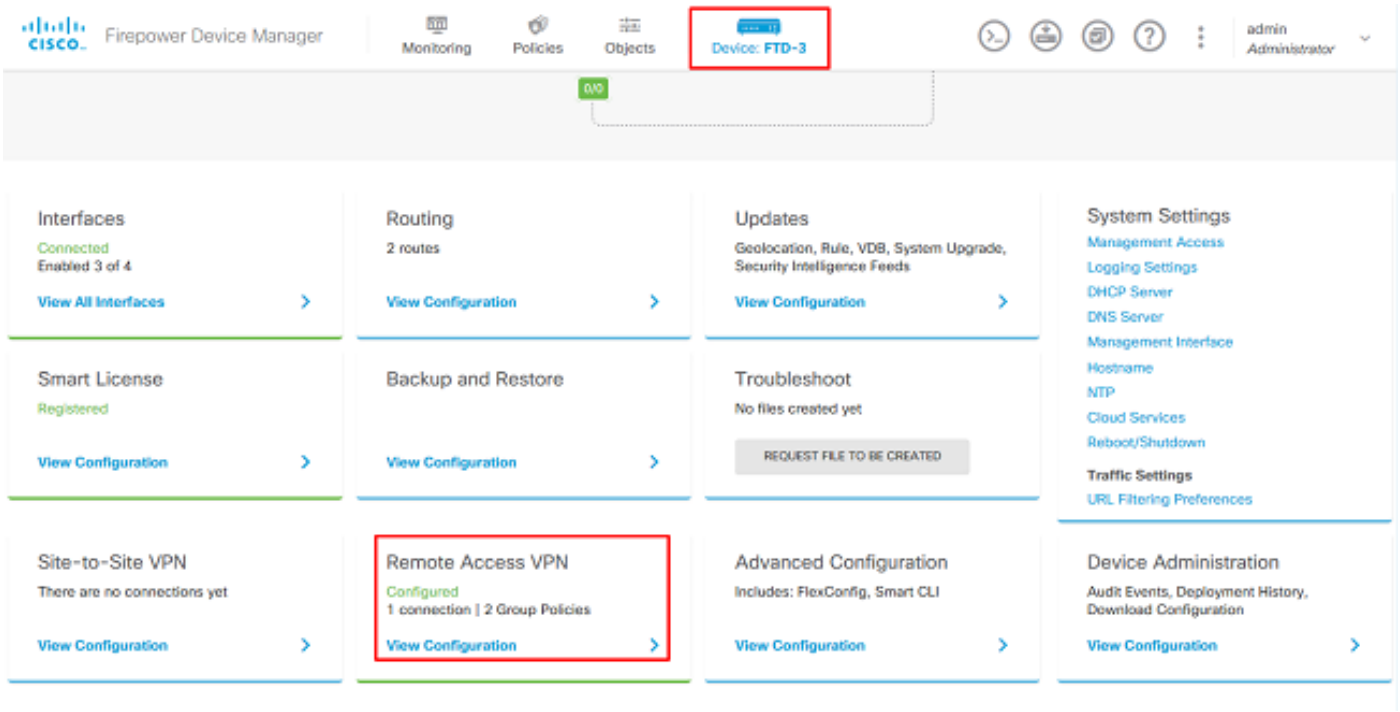
4. Haga clic en el botón **Implementar ahora**.



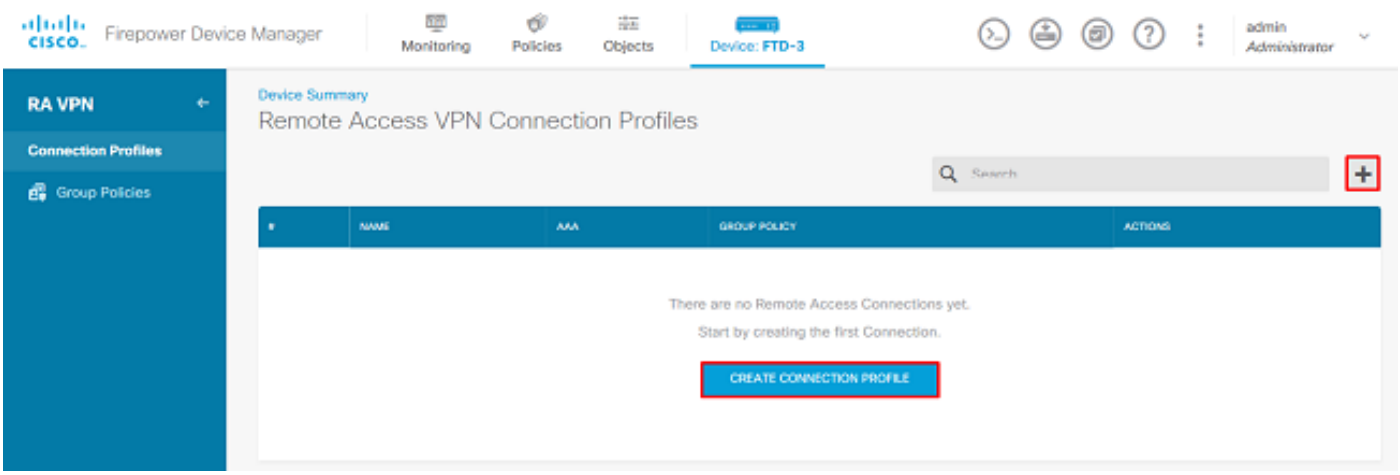
Configurar AnyConnect para la autenticación AD

Para utilizar el origen de identidad AD configurado, deberá aplicarse a la configuración de AnyConnect.

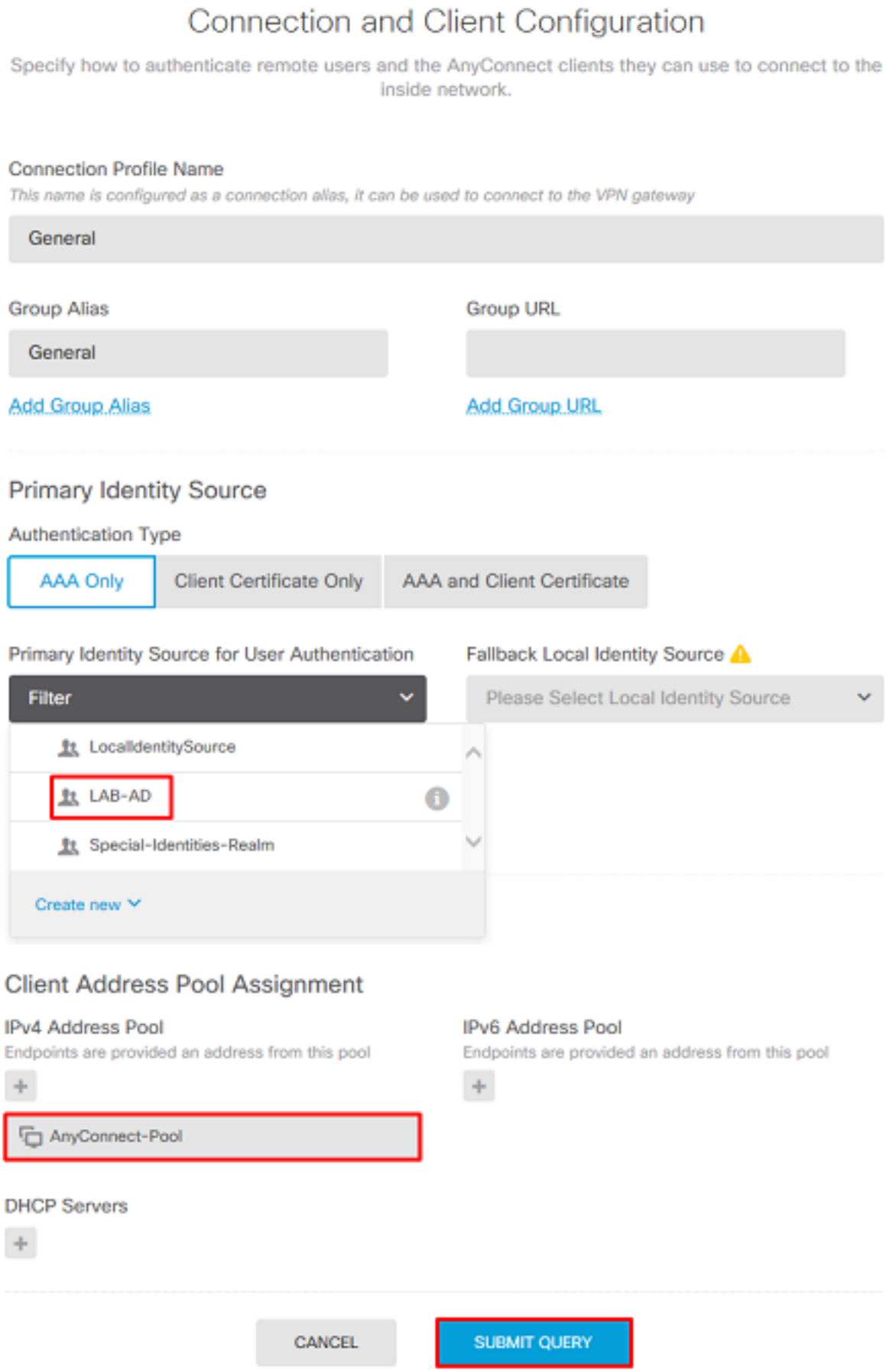
1. Vaya a **Device > Remote Access VPN** como se muestra en la imagen.



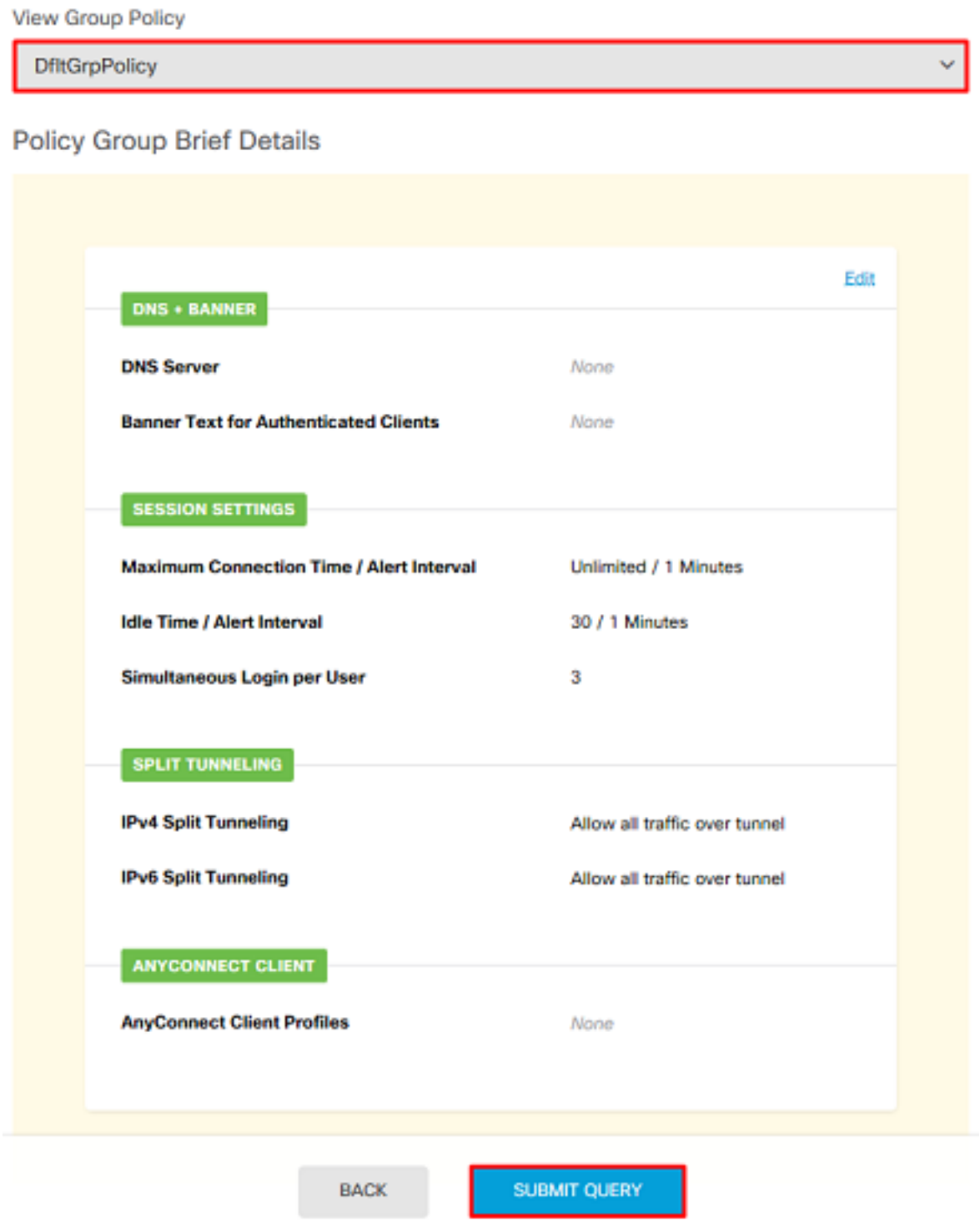
2. Haga clic en el símbolo **+** o en el botón **Crear perfil de conexión** como se muestra en la imagen.



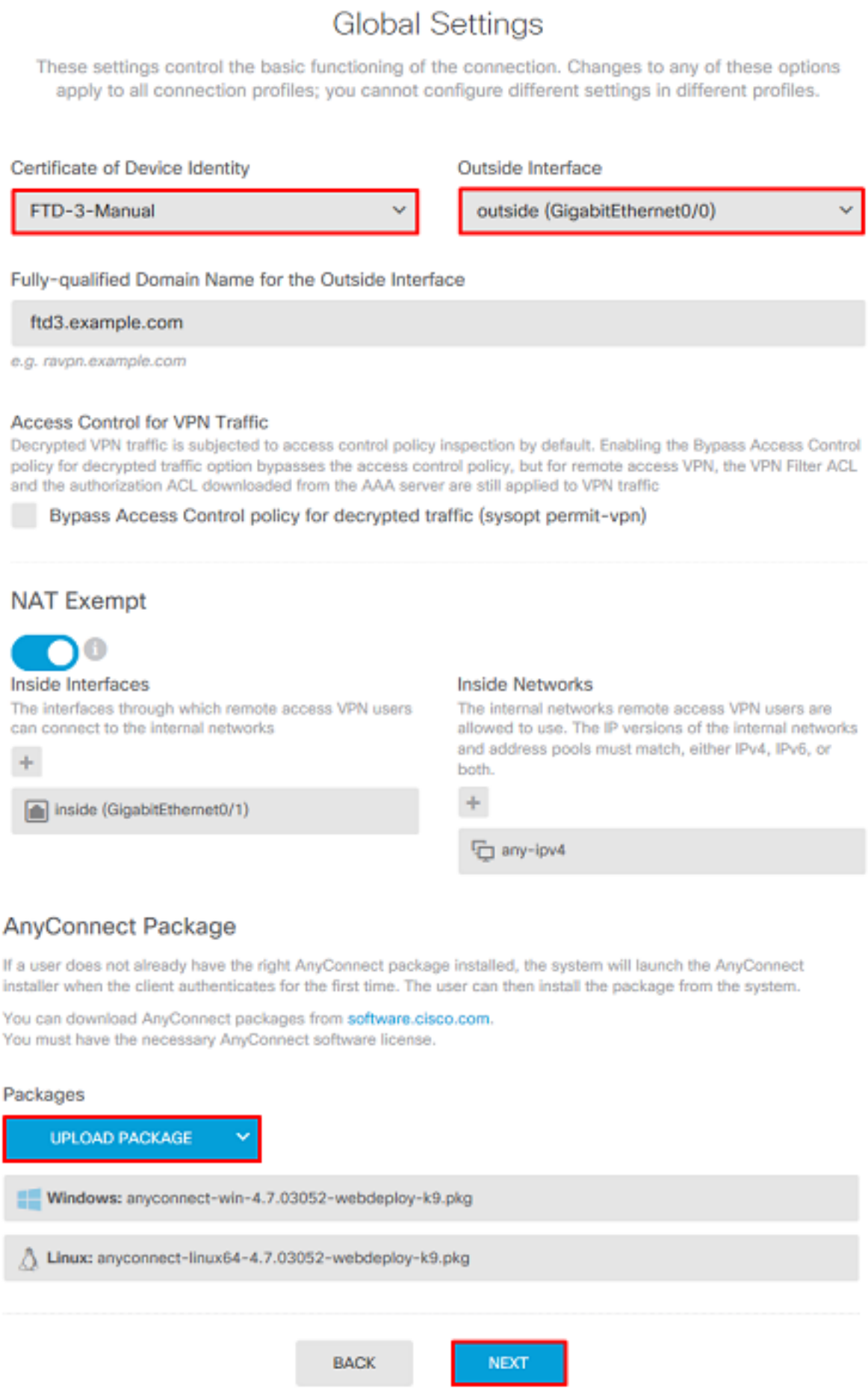
3. En la sección Connection and Client Configuration , seleccione el origen de identidad AD creado anteriormente. Configure los valores adecuados para las demás secciones, incluidos el nombre del perfil de conexión y la asignación del grupo de direcciones del cliente. Haga clic en **Enviar consulta** cuando haya terminado.



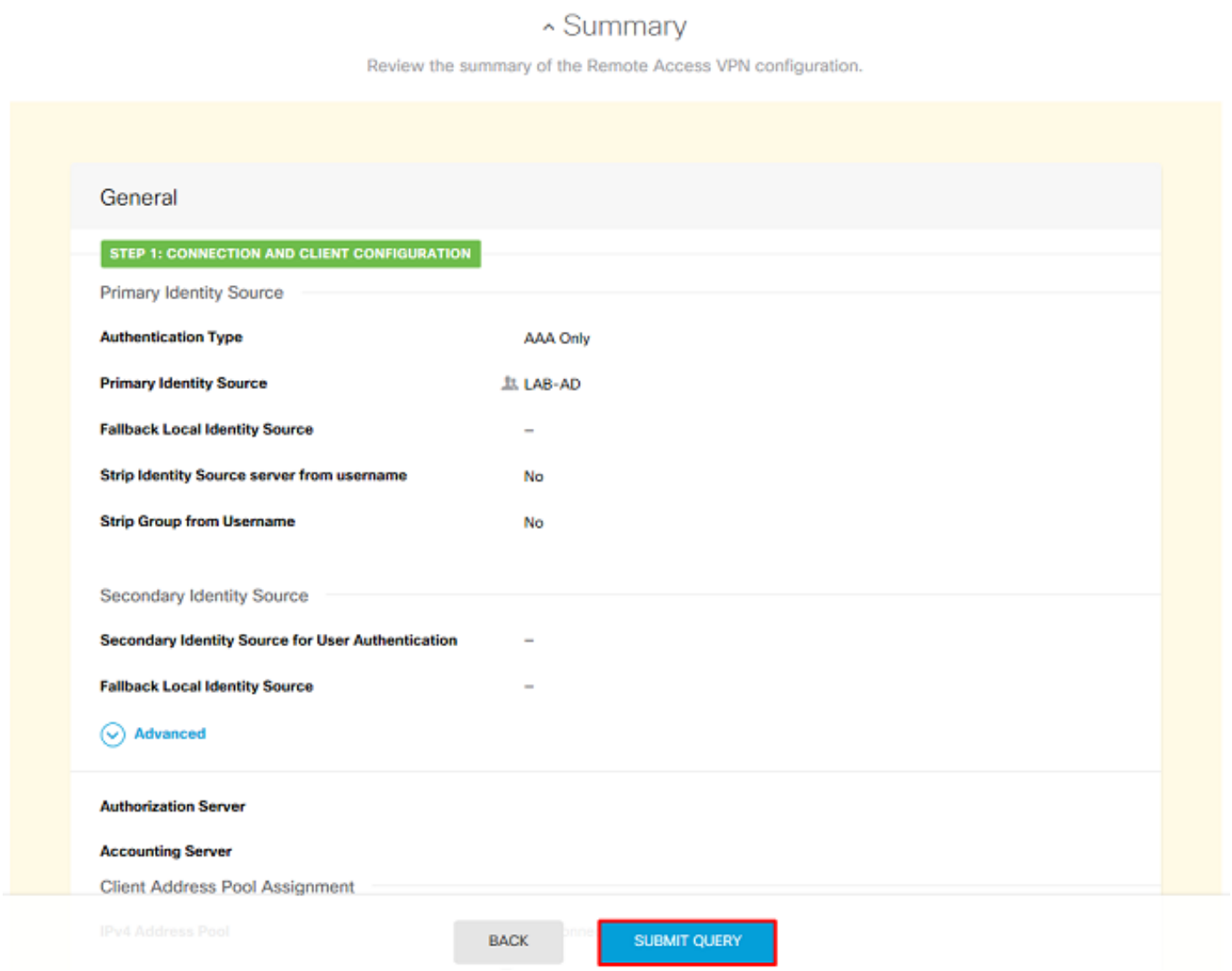
4. En la sección Experiencia de usuario remoto, seleccione la política de grupo adecuada. De forma predeterminada, se utilizará **DfltGrpPolicy**; sin embargo, se puede crear uno diferente.



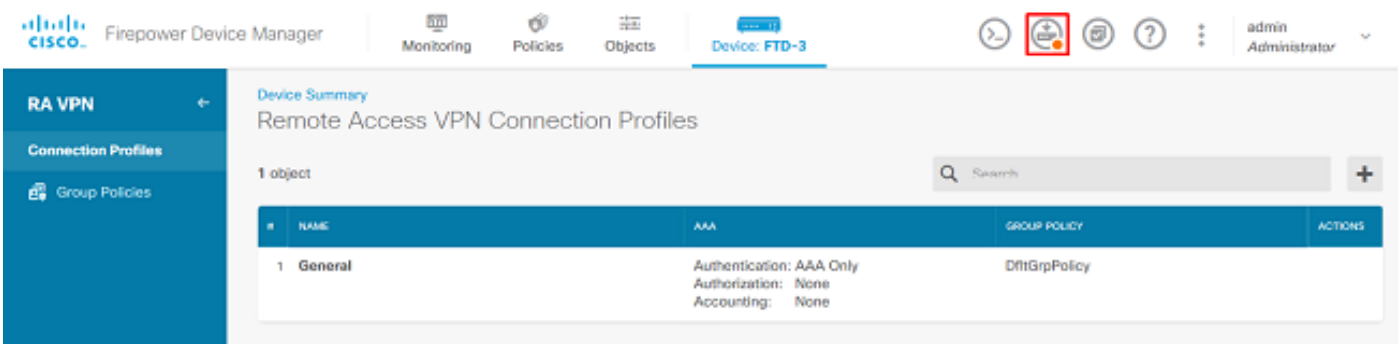
5. En la sección Configuración global, como mínimo, especifique los paquetes SSL Certificate, Outside Interface y AnyConnect. Si no se ha creado un certificado previamente, se puede seleccionar un certificado autofirmado predeterminado (DefaultInternalCertificate) sin embargo se verá un mensaje de certificado de servidor no confiable. La política de control de acceso de omisión para el tráfico descifrado (sysopt permit-vpn) debe desmarcarse para que las reglas de la política de acceso de identidad de usuario entren en vigor más adelante. La exención de NAT también se puede configurar aquí. En esta configuración, todo el tráfico ipv4 desde la interfaz interna que va a las direcciones IP del cliente AnyConnect es excepto desde NAT. Para configuraciones más complejas como el hairpinning externo a externo, se deberán crear reglas NAT adicionales bajo la política NAT. Los paquetes de AnyConnect se pueden encontrar en el sitio de soporte de Cisco: https://software.cisco.com/download/home. Se requiere una licencia Plus o Apex válida para descargar el paquete AnyConnect.



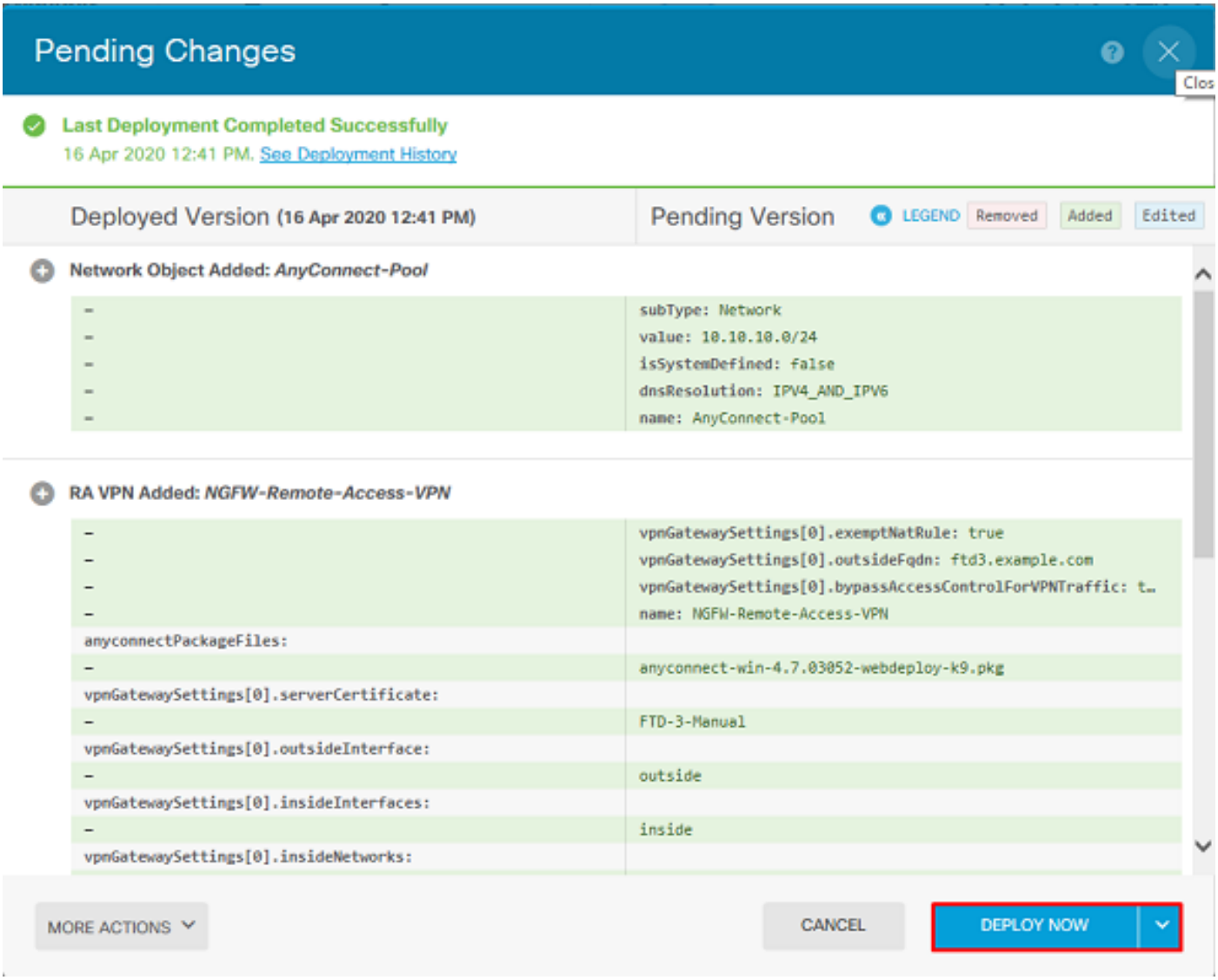
6. En la sección Resumen, verifique que AnyConnect esté configurado correctamente y, a continuación, haga clic en **Enviar consulta**.



7. Haga clic en el botón **Cambios pendientes** en la parte superior derecha, como se muestra en la imagen.



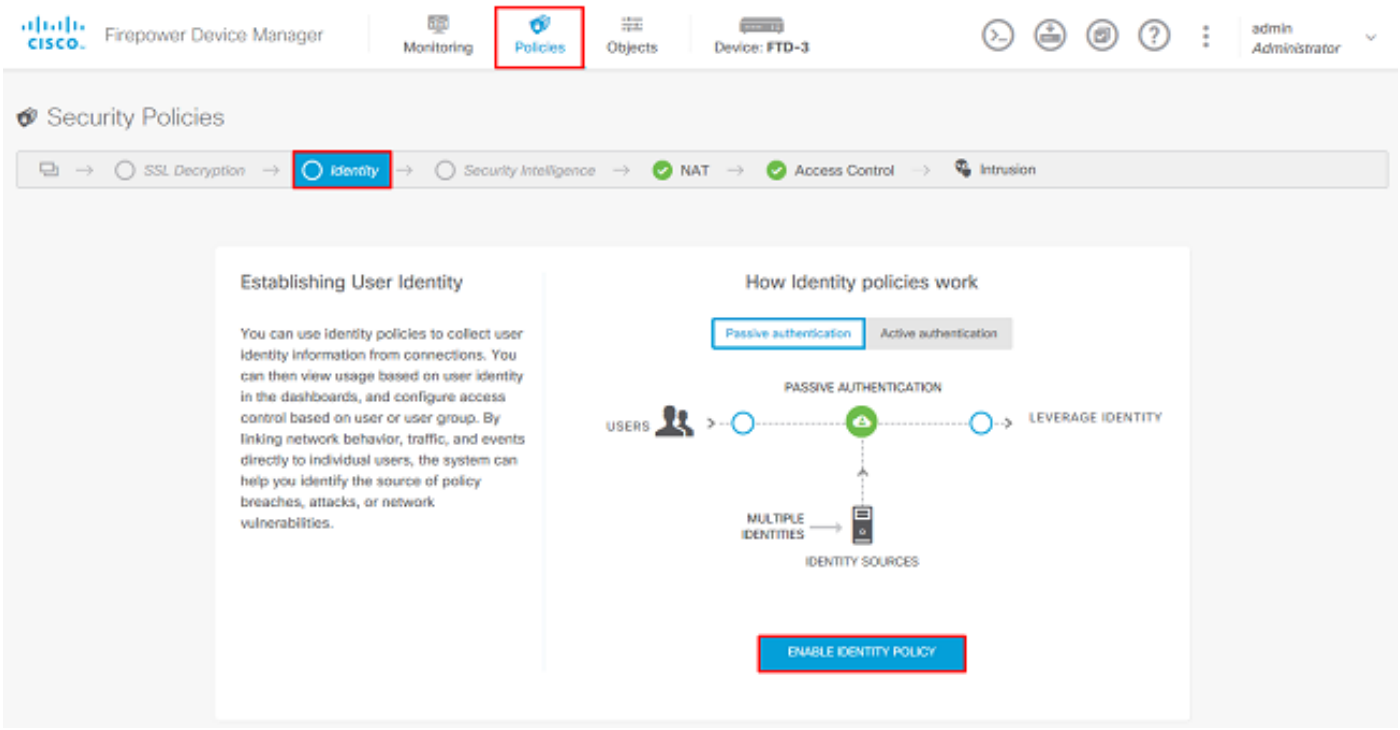
8. Haga clic en **Implementar ahora**.



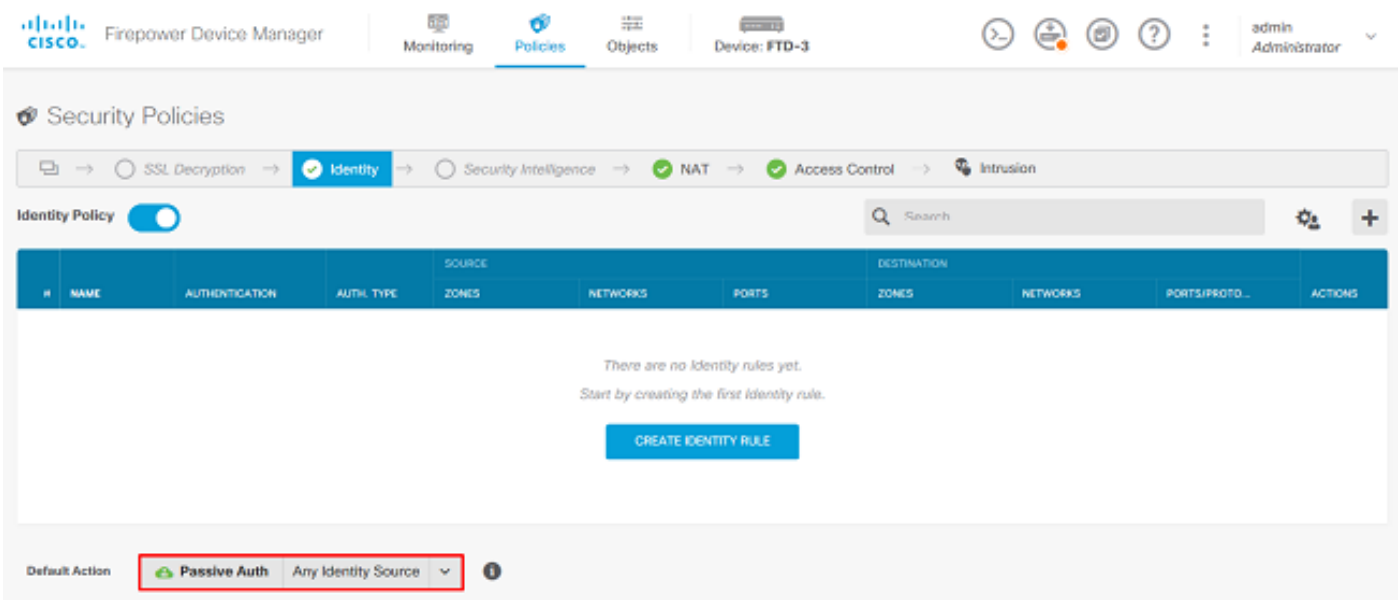
Habilitar la política de identidad y configurar las políticas de seguridad para la identidad de usuario

En este momento, los usuarios de AnyConnect deben poder conectarse correctamente, pero es posible que no puedan acceder a recursos específicos. Este paso habilitará la identidad del usuario de modo que sólo los usuarios de AnyConnect Admins puedan conectarse a los recursos internos con el uso de RDP y sólo los usuarios del grupo AnyConnect usuarios pueden conectarse a los recursos internos con el uso de HTTP.

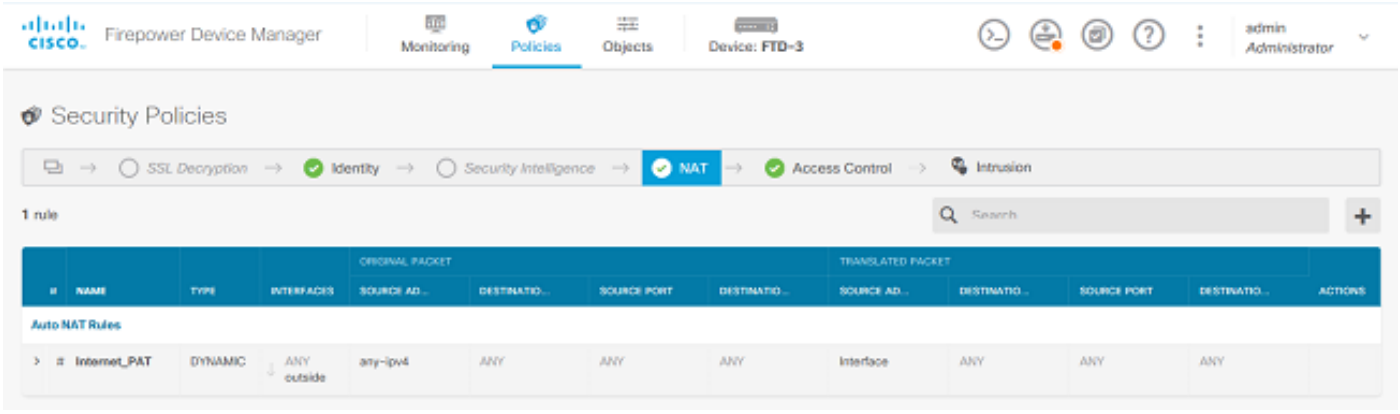
1. Navegue hasta **Políticas > Identidad** y haga clic en **Habilitar política de identidad**.



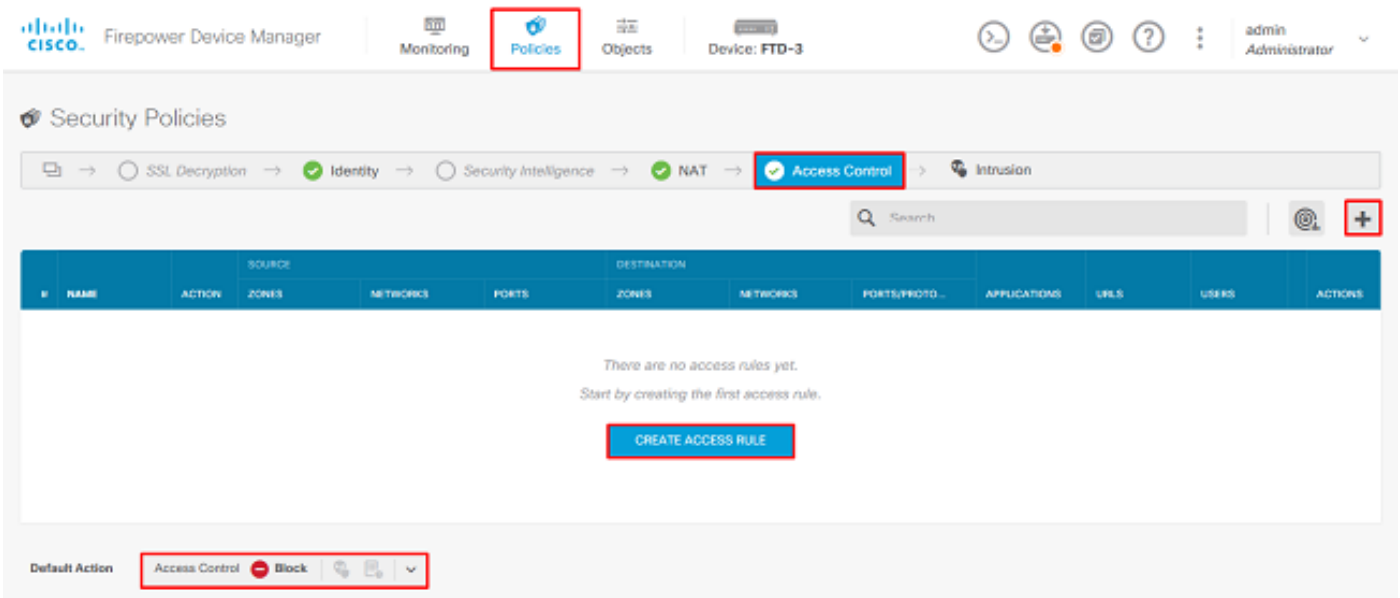
Para esta configuración, no se necesita ninguna configuración adicional y la Acción predeterminada es suficiente.



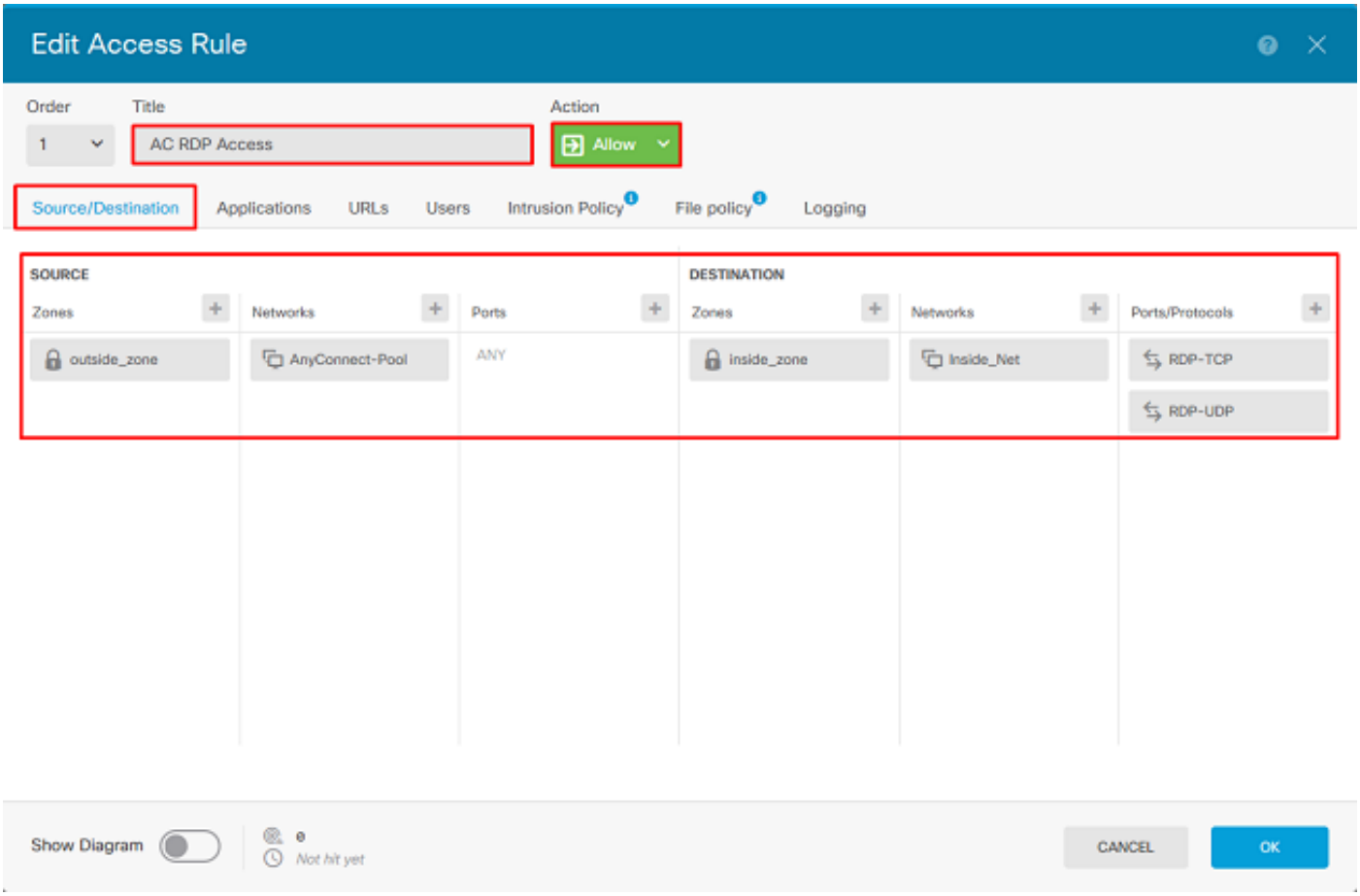
2. Navegue hasta **Políticas > NAT** y asegúrese de que NAT esté configurada apropiadamente. Si la excepción NAT configurada en los parámetros de AnyConnect es suficiente, no se necesitará ninguna configuración adicional aquí.



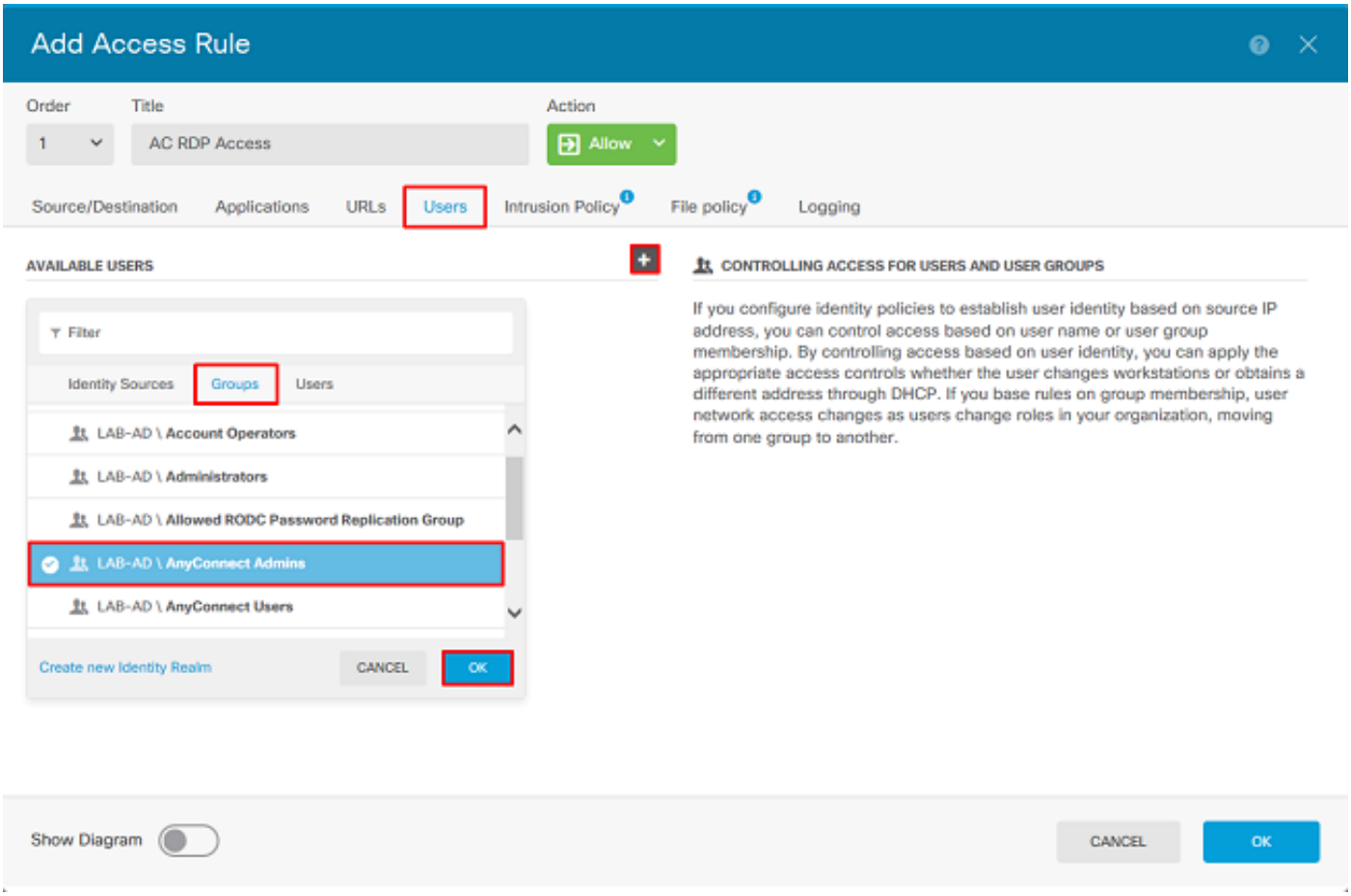
3. Vaya a **Políticas > Control de acceso**. En esta sección, la acción predeterminada se establece en Block (Bloquear) y no se han creado reglas de acceso, por lo que una vez que un usuario de AnyConnect se conecte, no podrá acceder a nada. Haga clic en el símbolo **+** o en Crear regla de acceso para agregar una nueva regla.



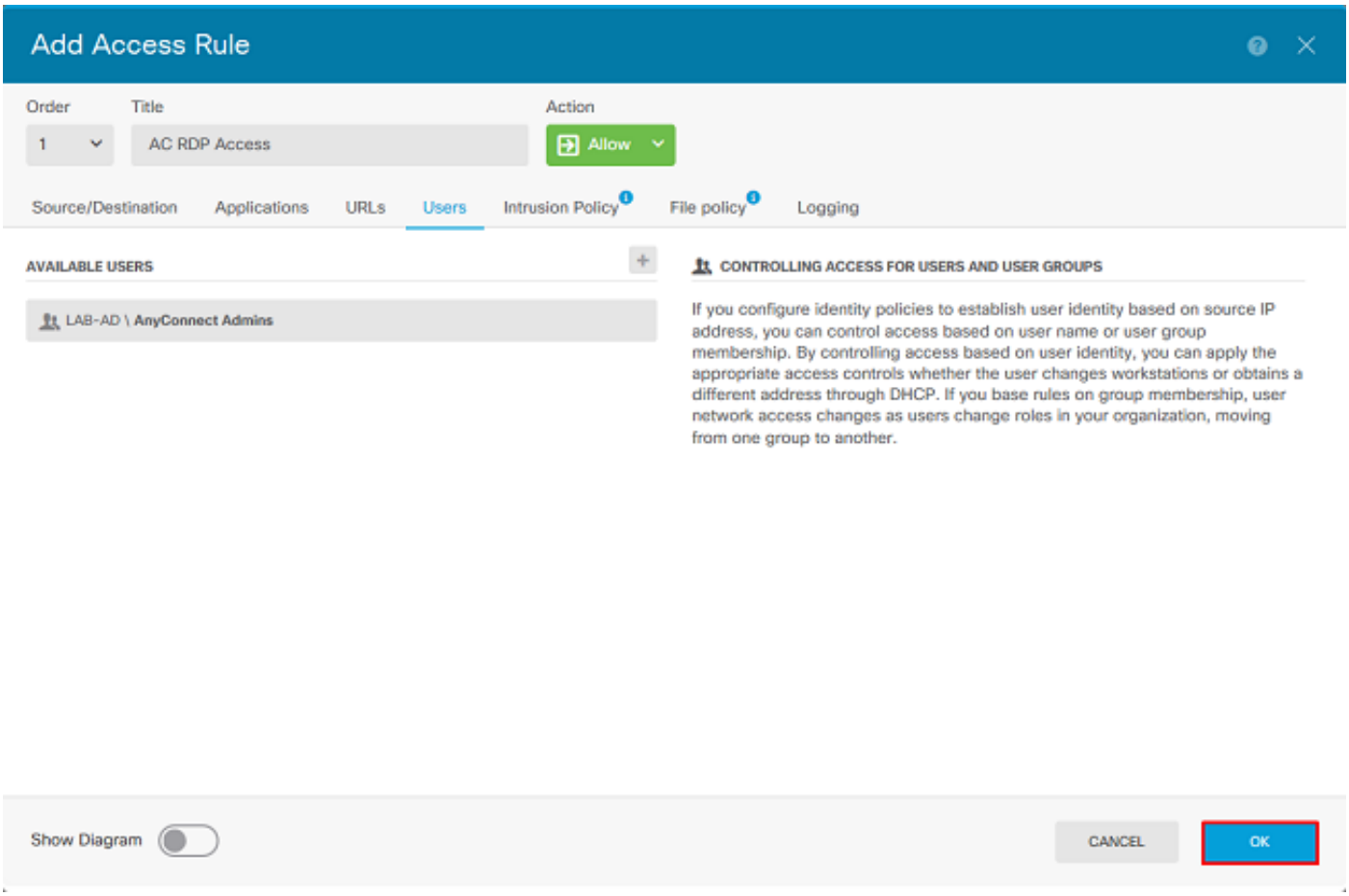
4. Rellene los campos con los valores adecuados. En esta configuración, los usuarios del grupo Administradores de AnyConnect deben tener acceso RDP a Windows Server en la red interna. Para el origen, la zona se configura como outside_zone, que es la interfaz exterior a la que se conectarán los usuarios de AnyConnect y la red se configura como el objeto AnyConnect-Pool que se configuró anteriormente para asignar direcciones IP a los clientes de AnyConnect. Para la identidad de usuario en FDM, el origen debe ser la zona y la red desde la que el usuario iniciará la conexión. Para el destino, la zona se configura como inside_zone, que es la interfaz interna en la que se encuentra Windows Server, la red se configura como el objeto Inside_Net, que es un objeto que define la subred en la que se encuentra Windows Server, y los puertos/protocolos se establecen en dos objetos de puerto personalizados para permitir el acceso RDP a través de TCP 3389 y UDP 3389.



En la sección Users (Usuarios), se agregará el grupo AnyConnect Admins para que se permita el acceso RDP a Windows Server a los usuarios que no formen parte de este grupo. Haga clic en el símbolo **+**, haga clic en la ficha Grupos, haga clic en el grupo correspondiente y, a continuación, haga clic en **Aceptar**. Tenga en cuenta que también se pueden seleccionar usuarios individuales y el origen de identidad.

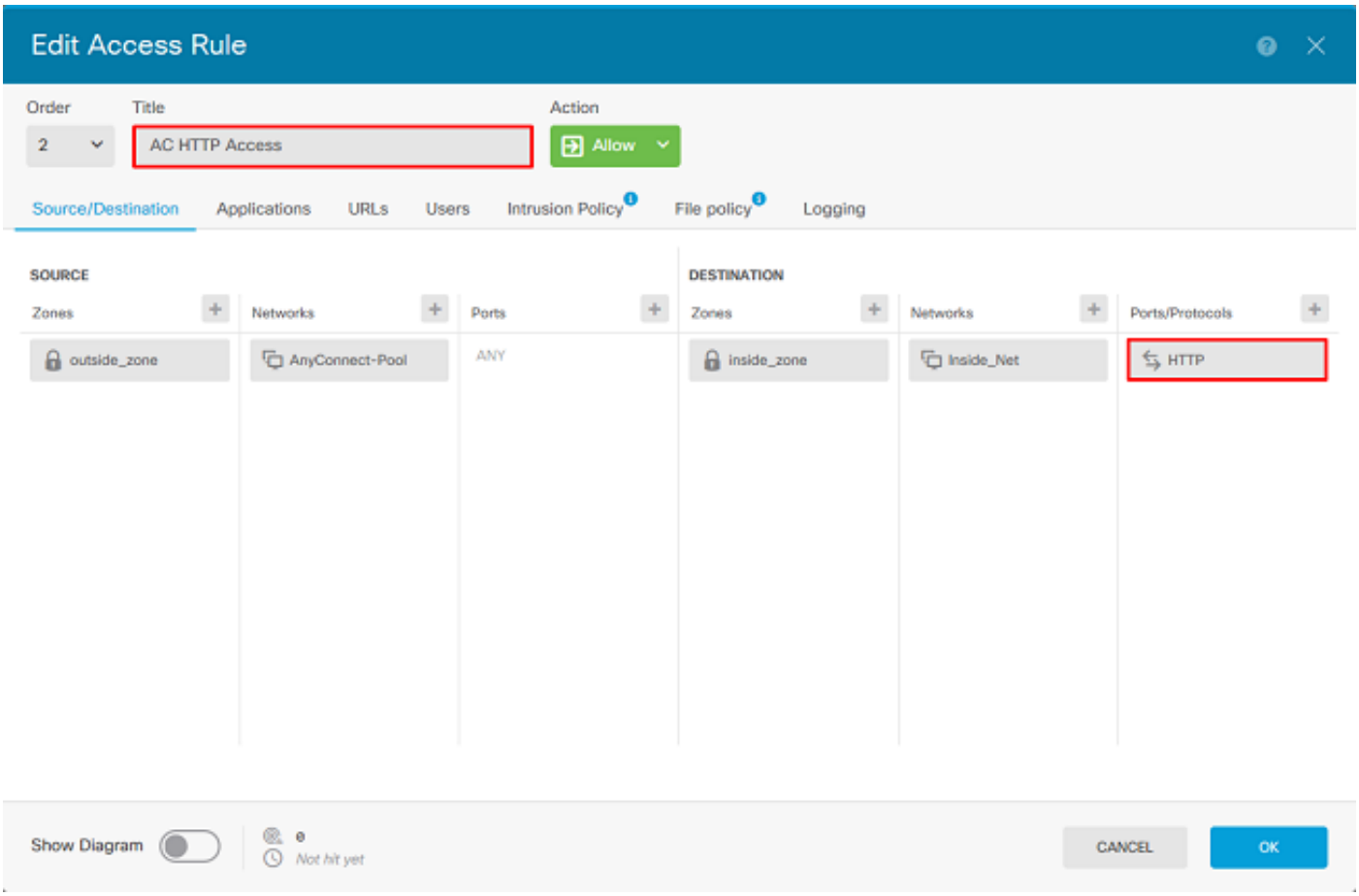


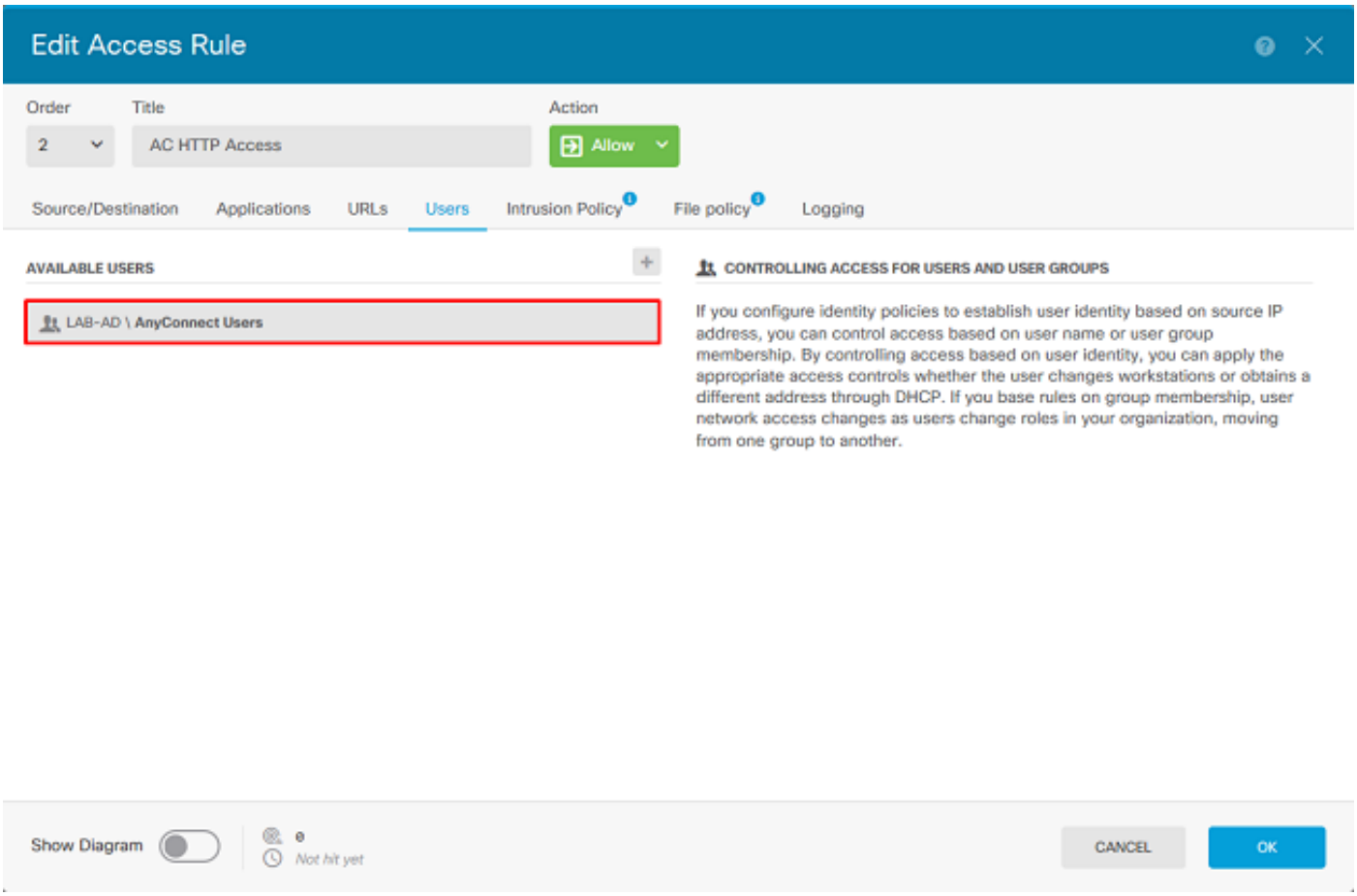
Una vez seleccionadas las opciones correspondientes, haga clic en **Aceptar**.



5. Cree más reglas de acceso si es necesario. En esta configuración, se crea otra regla de acceso

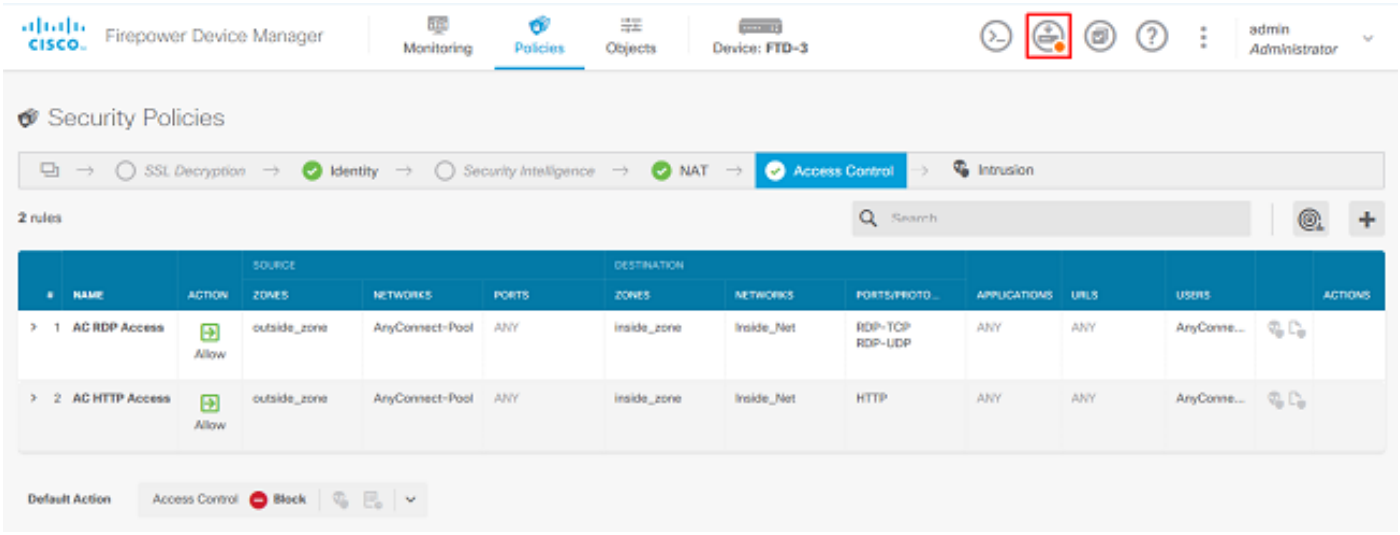
para permitir que los usuarios del grupo Usuarios de AnyConnect accedan a HTTP al servidor de Windows.



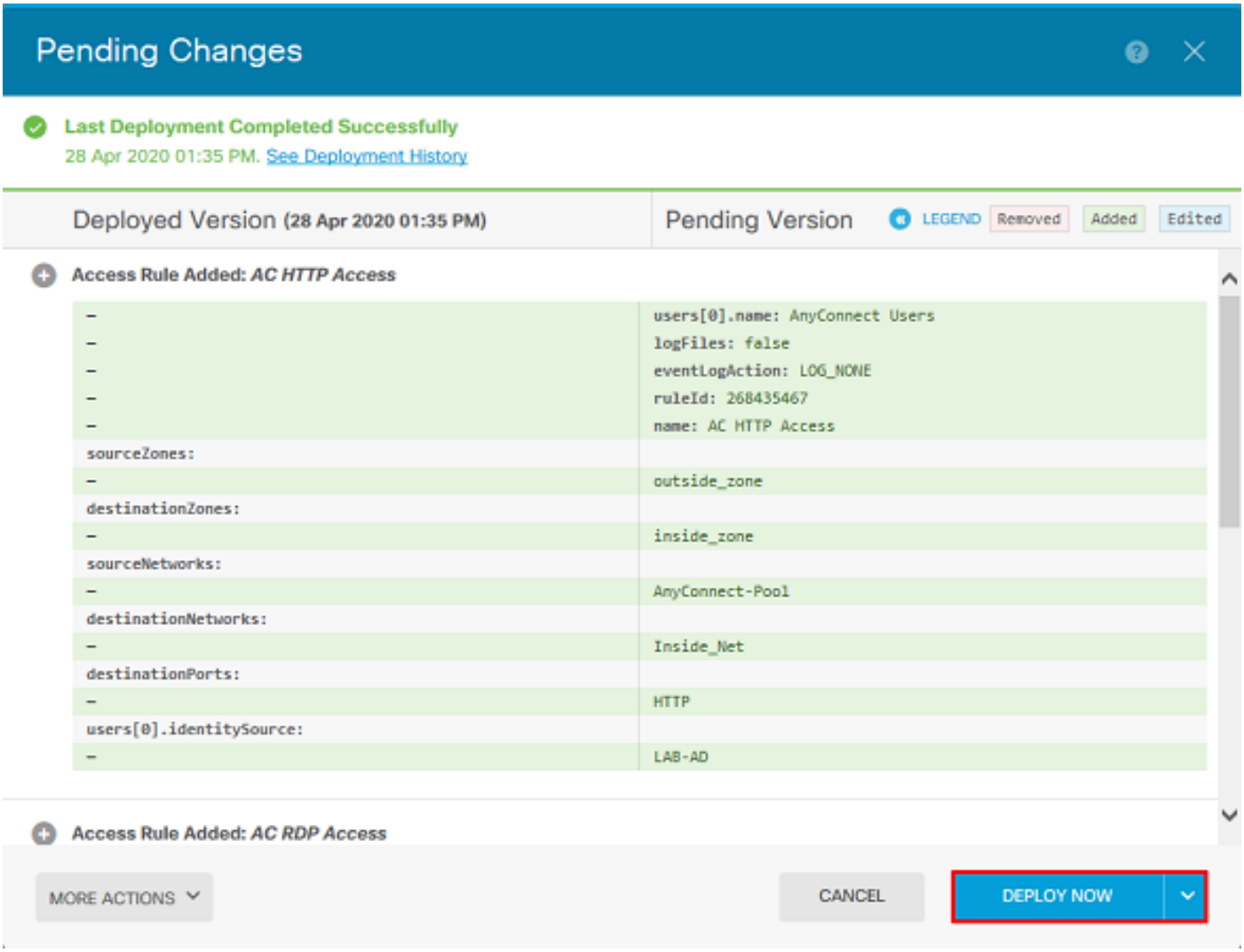


6. Verifique la configuración de la regla de acceso y luego haga clic en el botón **Cambios**

pendientes en la parte superior derecha como se muestra en la imagen.



7. Verifique los cambios y luego haga clic en **Implementar ahora**.



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Configuración final

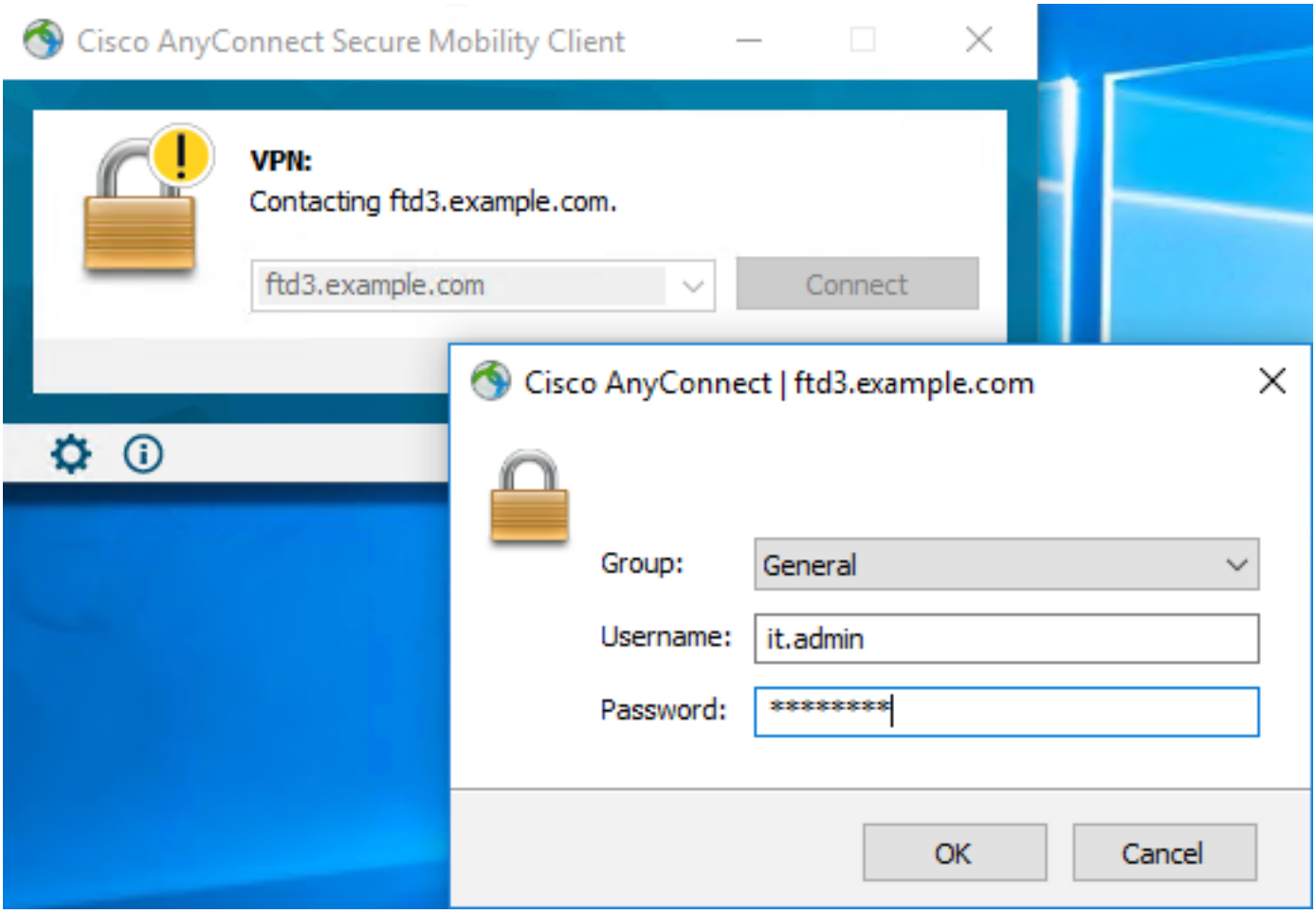
Configuración AAA

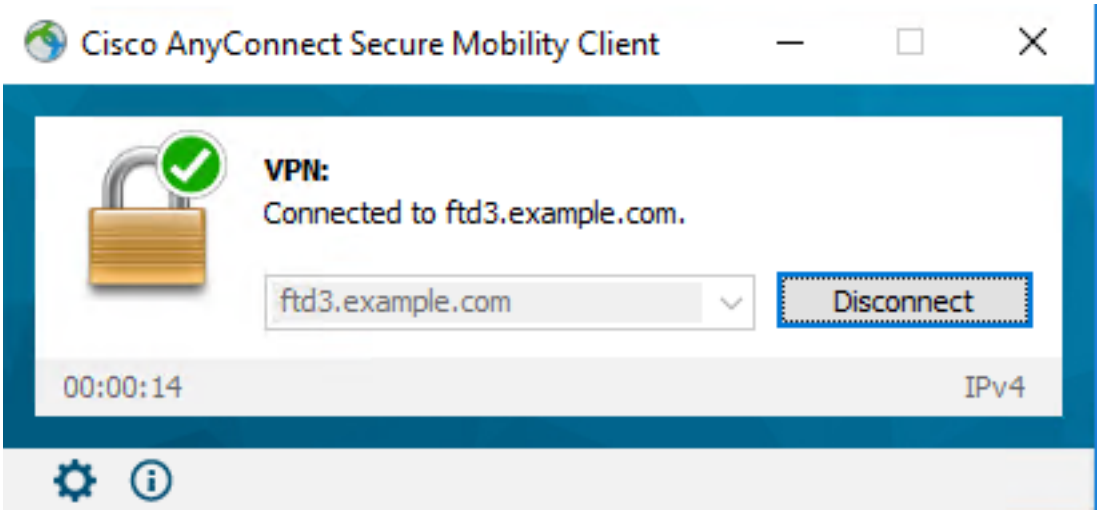
```
show running-configuration aaa-server
aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com server-
port 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-login-
dn ftd.admin@example.com server-type auto-detect
```

Configurar AnyConnect

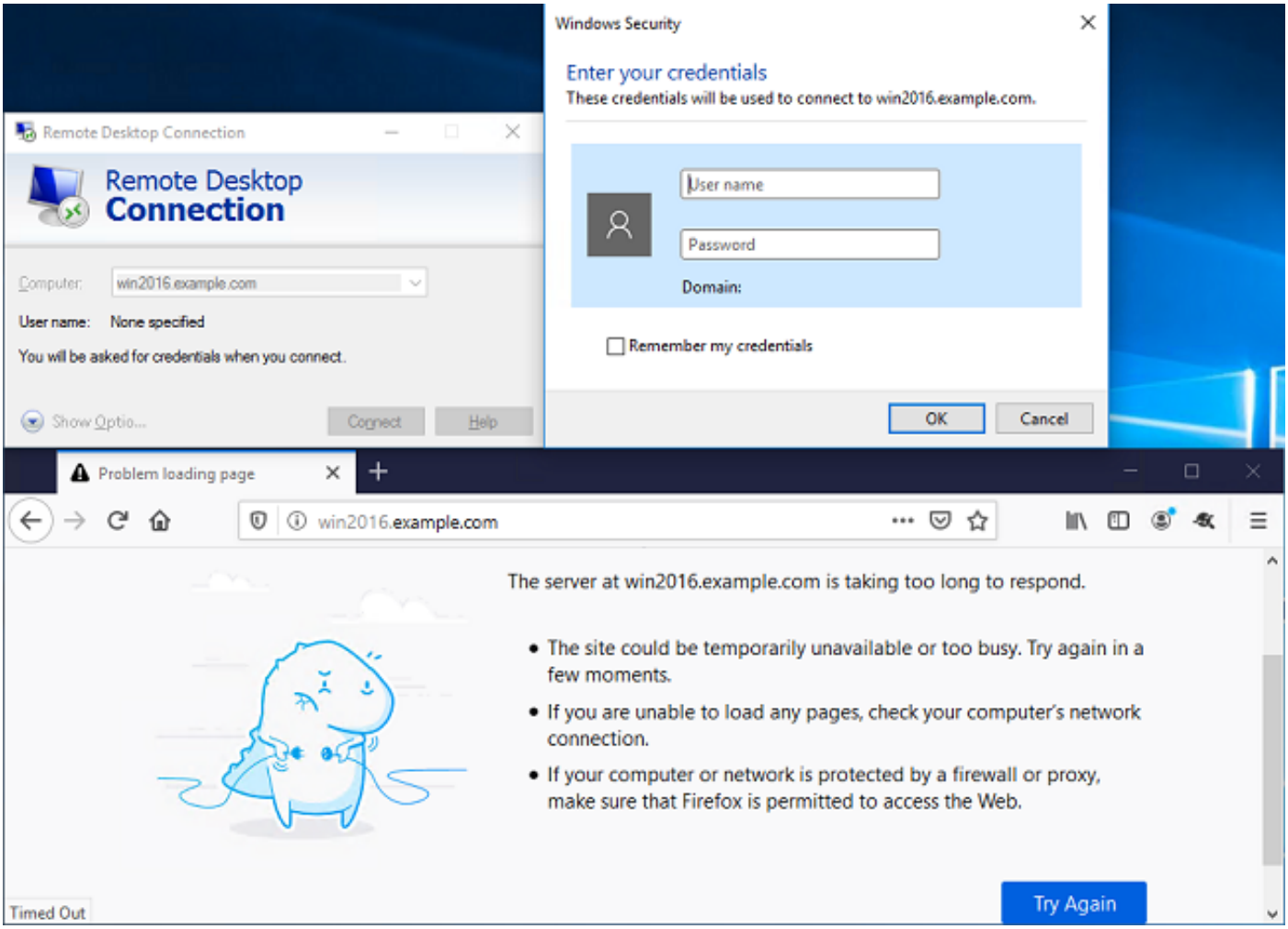
```
> show running-config webvpn
webvpn
 enable outside
 http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
 anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable

> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
 address-pool AnyConnect-Pool
 authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
 group-alias General enable

> show running-config group-policy
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value DfltGrpPolicy|splitAcl
 webvpn
  anyconnect ssl dtls none

> show running-config ssl
ssl trust-point FTD-3-Manual outside
```

Conéctese con AnyConnect y verifique las normas de política de control de acceso

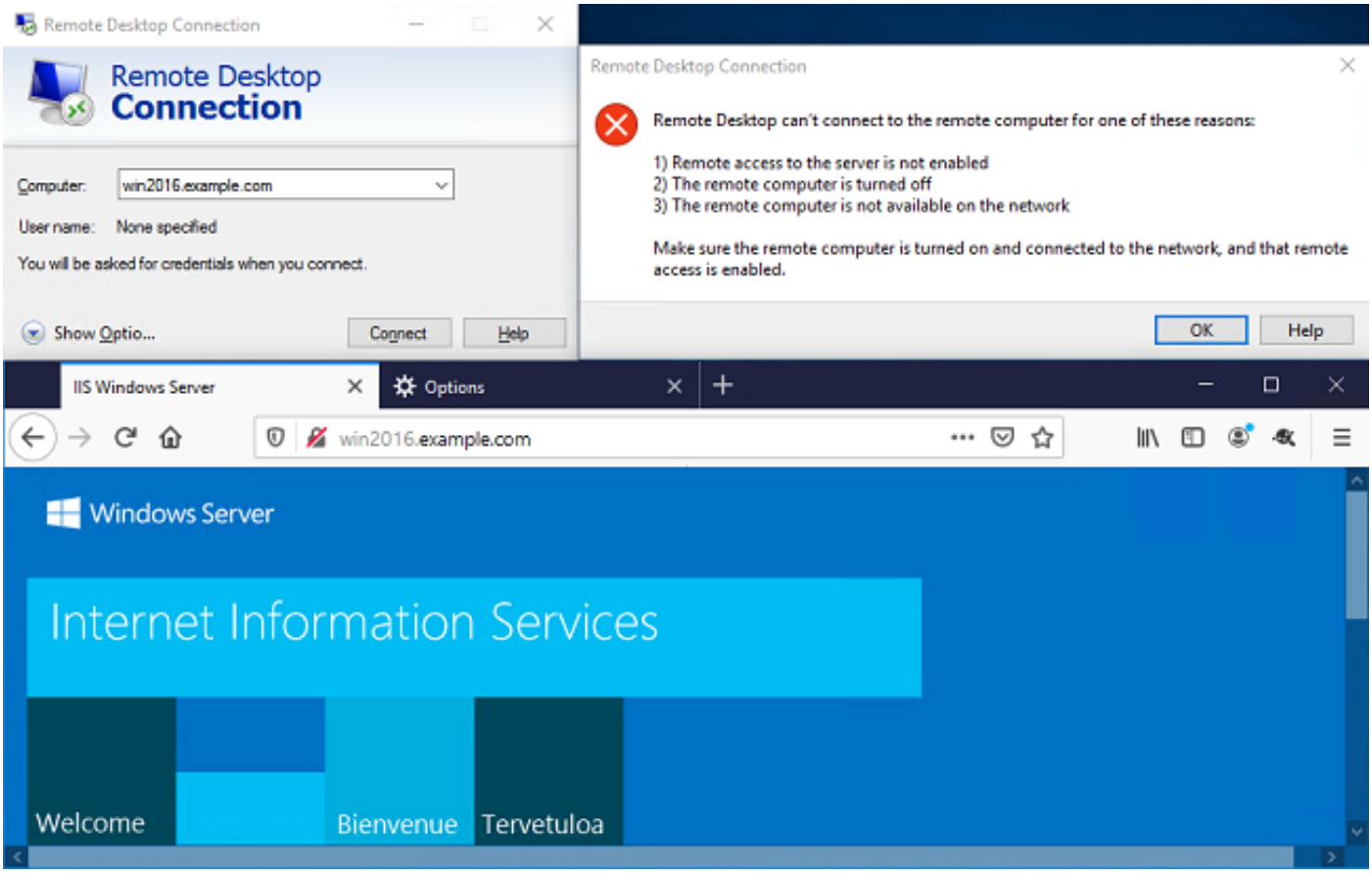




User IT Admin se encuentra en el grupo AnyConnect Admins que tiene acceso RDP a Windows Server; sin embargo, no tiene acceso a HTTP. Al abrir una sesión RDP y Firefox en este servidor, se comprueba que este usuario sólo puede acceder al servidor a través de RDP.



Si ha iniciado sesión con un usuario de prueba que se encuentra en el grupo Usuarios de AnyConnect que tienen acceso HTTP pero no RDP, puede verificar que las reglas de la política de control de acceso están surtiendo efecto.



Troubleshoot

Utilize esta sección para confirmar que su configuración funcione correctamente.

Depuraciones

Este debug se puede ejecutar en la CLI de diagnóstico para resolver problemas relacionados con la autenticación LDAP: **debug ldap 255**.

Para resolver problemas de la política de control de acceso de identidad del usuario, el **sistema soporta firewall-engine-debug** se puede ejecutar en clish para determinar por qué el tráfico se permite o se bloquea inesperadamente.

Depuraciones LDAP en funcionamiento

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
        Base DN = [DC=example,DC=com]
        Filter  = [sAMAccountName=it.admin]
```

```
        Scope   = [SUBTREE]
[53] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53]    objectClass: value = top
[53]    objectClass: value = person
[53]    objectClass: value = organizationalPerson
[53]    objectClass: value = user
[53]    cn: value = IT Admin
[53]    sn: value = Admin
[53]    givenName: value = IT
[53]    distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]    instanceType: value = 4
[53]    whenCreated: value = 20200421025811.0Z
[53]    whenChanged: value = 20200421204622.0Z
[53]    displayName: value = IT Admin
[53]    uSNCreated: value = 25896
[53]    memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]    uSNChanged: value = 26119
[53]    name: value = IT Admin
[53]    objectGUID: value = &...J..O..2w...c
[53]    userAccountControl: value = 512
[53]    badPwdCount: value = 6
[53]    codePage: value = 0
[53]    countryCode: value = 0
[53]    badPasswordTime: value = 132320354378176394
[53]    lastLogoff: value = 0
[53]    lastLogon: value = 0
[53]    pwdLastSet: value = 132319114917186142
[53]    primaryGroupID: value = 513
[53]    objectSid: value = .............{I...;.....j...
[53]    accountExpires: value = 9223372036854775807
[53]    logonCount: value = 0
[53]    sAMAccountName: value = it.admin
[53]    sAMAccountType: value = 805306368
[53]    userPrincipalName: value = it.admin@example.com
[53]    objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
[53]    dSCorePropagationData: value = 16010101000000.0Z
[53]    lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

No se puede establecer la conexión con el servidor LDAP

```
[-2147483611] Session Start
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611] Connect to LDAP server: ldap://172.16.1.1:389, status = Failed
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

Soluciones potenciales:

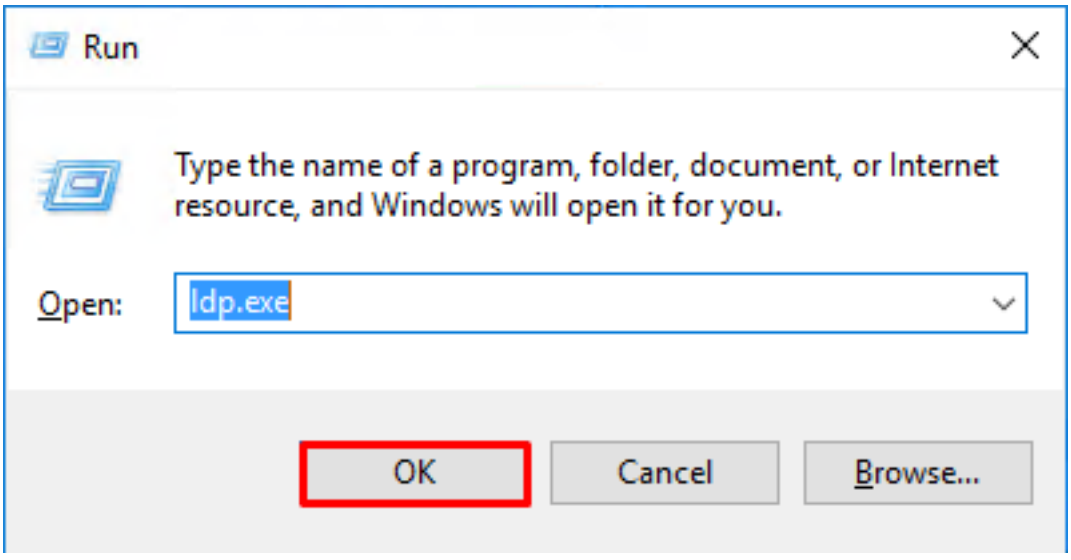
- Verifique el ruteo y asegúrese de que el FTD reciba una respuesta del servidor LDAP.
- Si se utiliza LDAPS o STARTTLS, asegúrese de que se confía en el certificado de CA raíz correcto para que el intercambio de señales SSL pueda completarse correctamente.
- Verifique que se utilicen la dirección IP y el puerto correctos. Si se utiliza un nombre de host, verifique que DNS pueda resolverlo a la dirección IP correcta

Enlace de DN de inicio de sesión o contraseña incorrecta

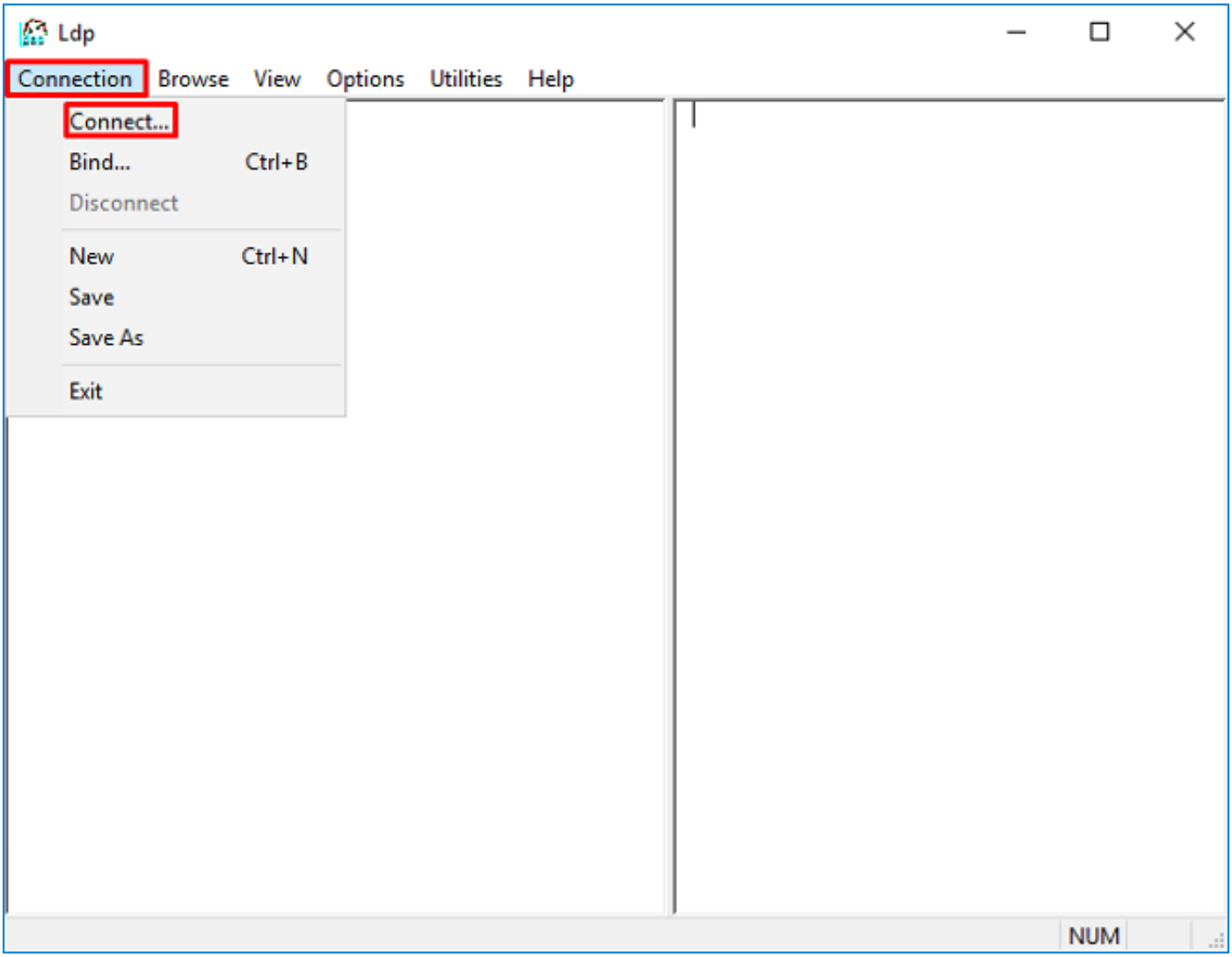
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid
credentials
[-2147483615] Failed to bind as administrator returned code (-1) Can't contact LDAP server
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

Solución potencial: Verifique que el DN de inicio de sesión y la contraseña de inicio de sesión estén configurados correctamente. Esto se puede verificar en el servidor AD con **ldp.exe**. Para verificar que una cuenta puede enlazarse correctamente con el uso de ldp, navegue a través de estos pasos:

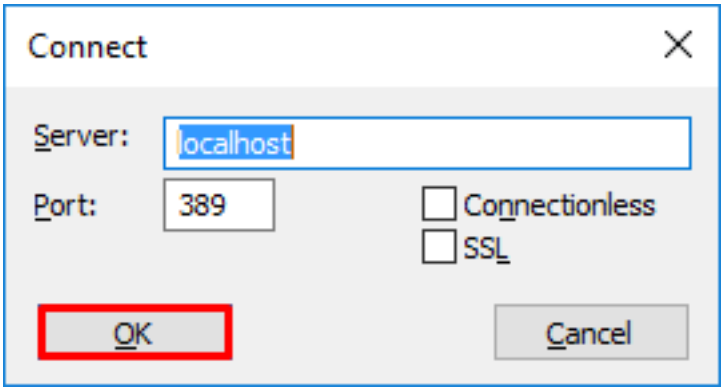
1. En el servidor AD, presione **Win+R** y busque **ldp.exe**.



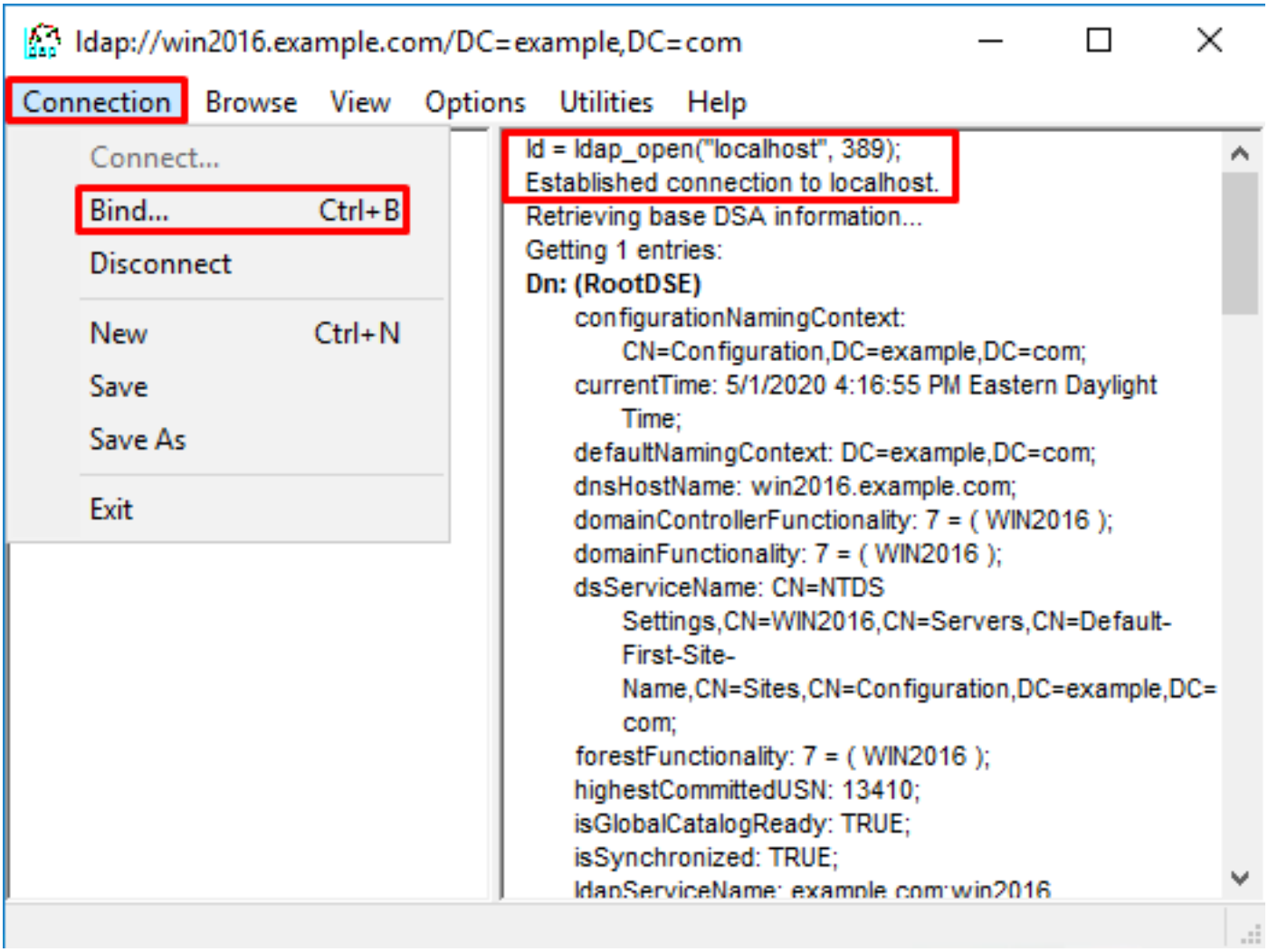
2. Haga clic en **Connection > Connect...** como se muestra en la imagen.



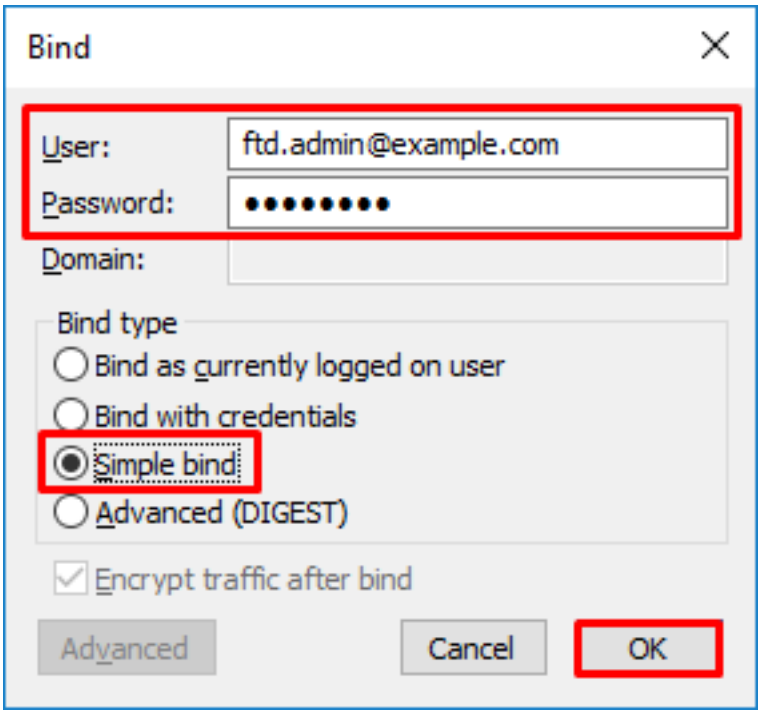
3. Especifique localhost para el servidor y el puerto apropiado, luego haga clic en **Aceptar**.



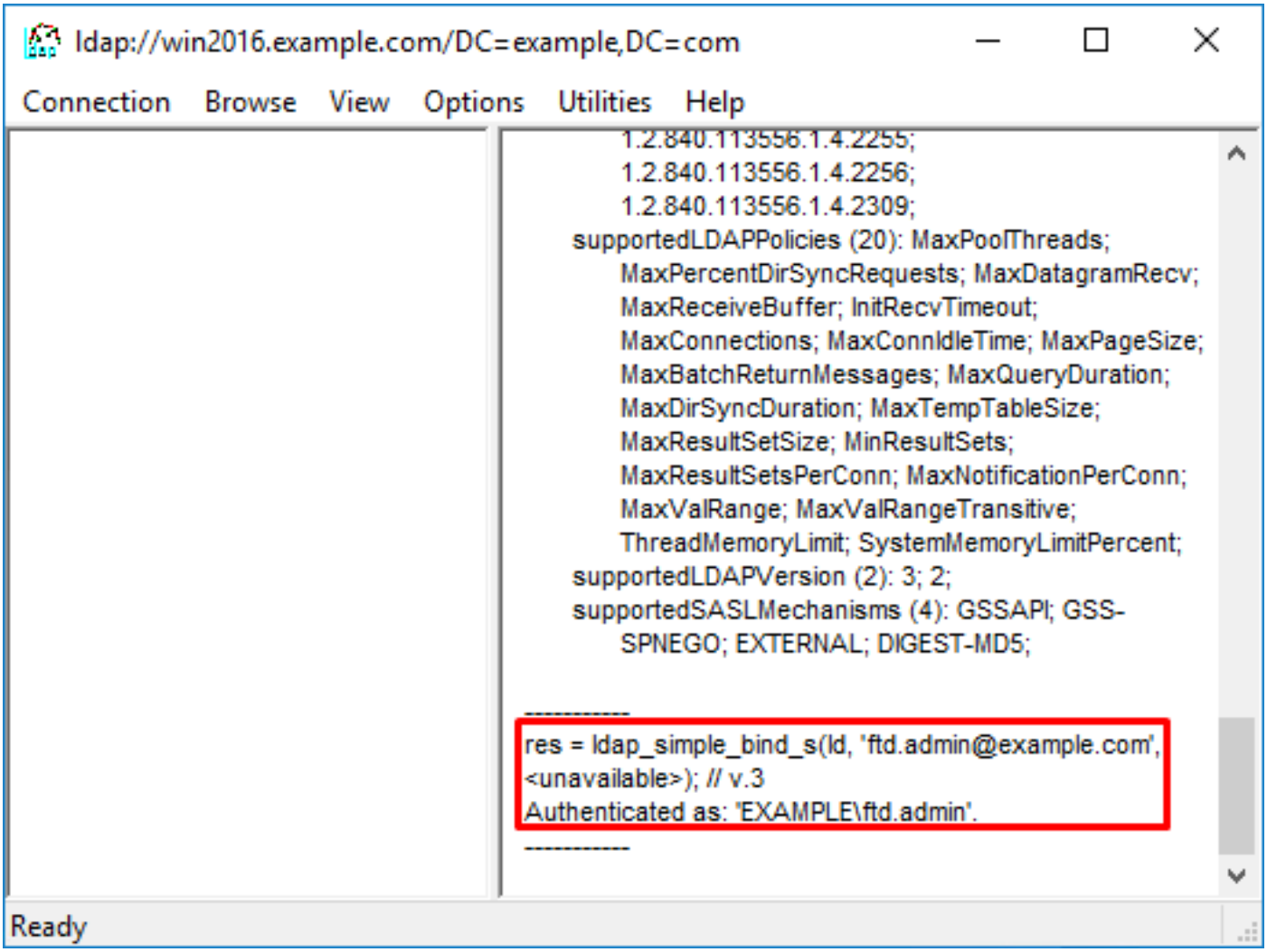
4. La columna Derecha muestra el texto que indica una conexión correcta. Haga clic en **Conexión > Enlazar...** como se muestra en la imagen.



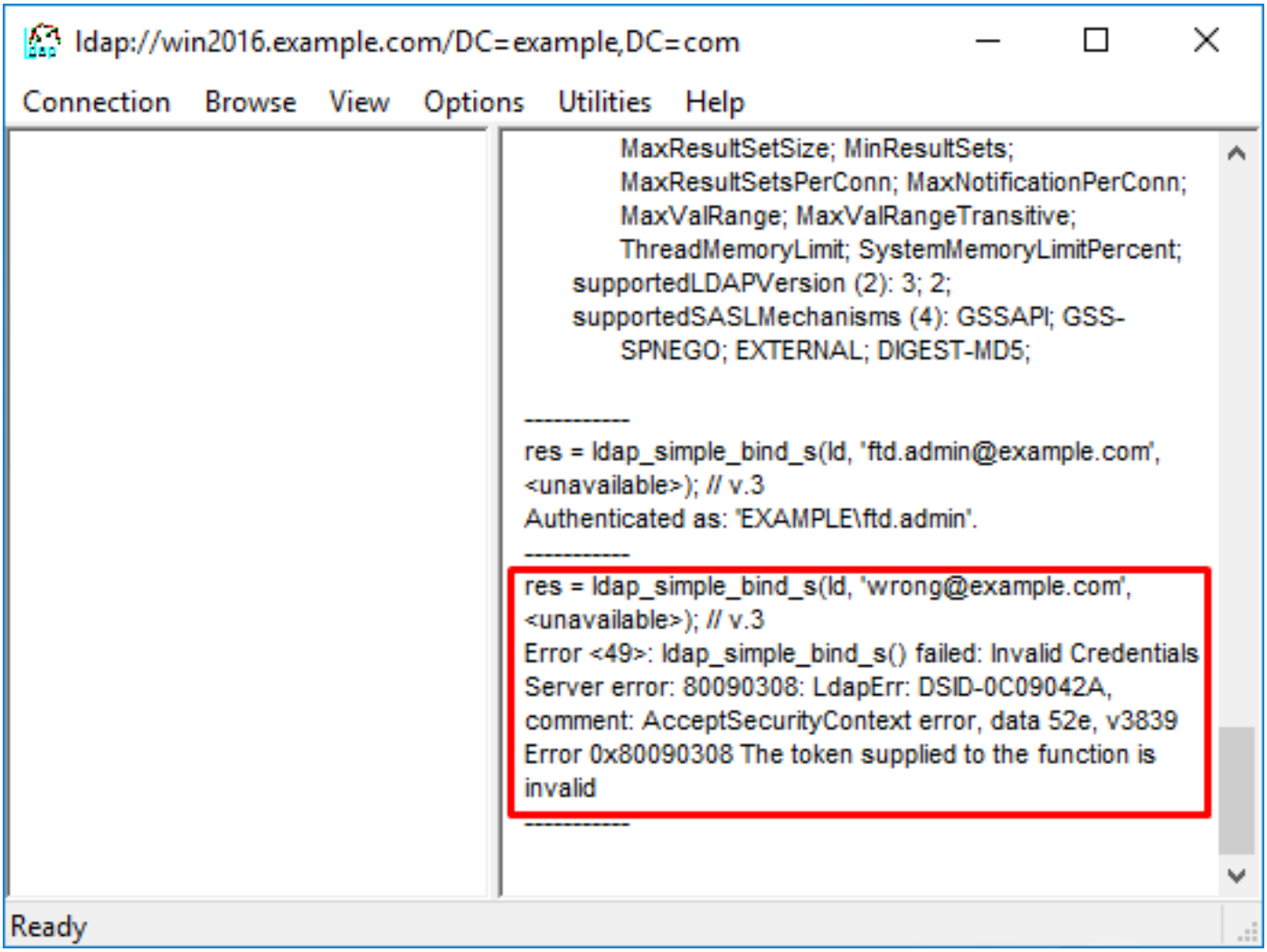
5. Seleccione **Simple Bind** y especifique el nombre de usuario y la contraseña de la cuenta de directorio. Click OK.



Con un enlace exitoso, ldp mostrará Authenticated como **DOMAIN\username**.



Si intenta un enlace con un nombre de usuario o una contraseña no válidos, se producirá un error como este.

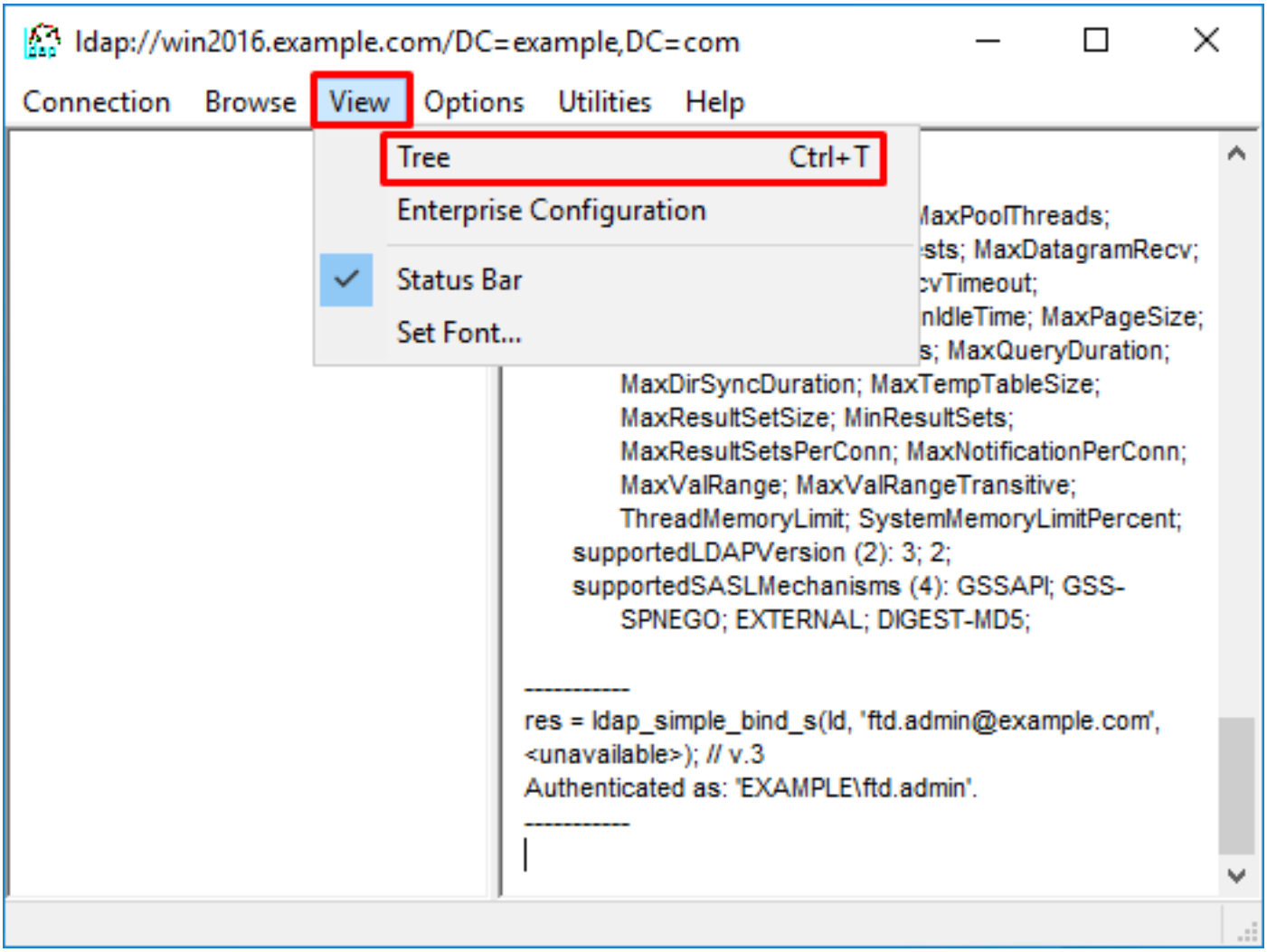


El servidor LDAP no puede encontrar el nombre de usuario

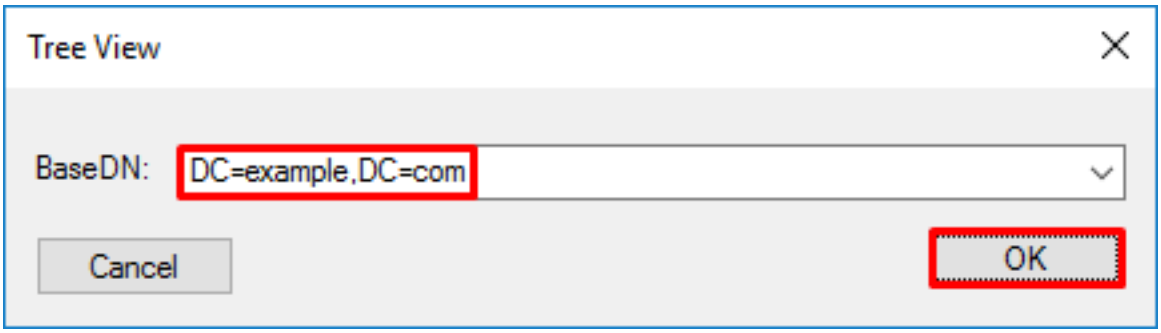
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter  = [samaccountname=it.admi]
        Scope   = [SUBTREE]
[-2147483612] Search result parsing returned failure status
[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End
```

Solución potencial: Verifique que AD pueda encontrar al usuario con la búsqueda realizada por el FTD. Esto también se puede hacer con ldp.exe.

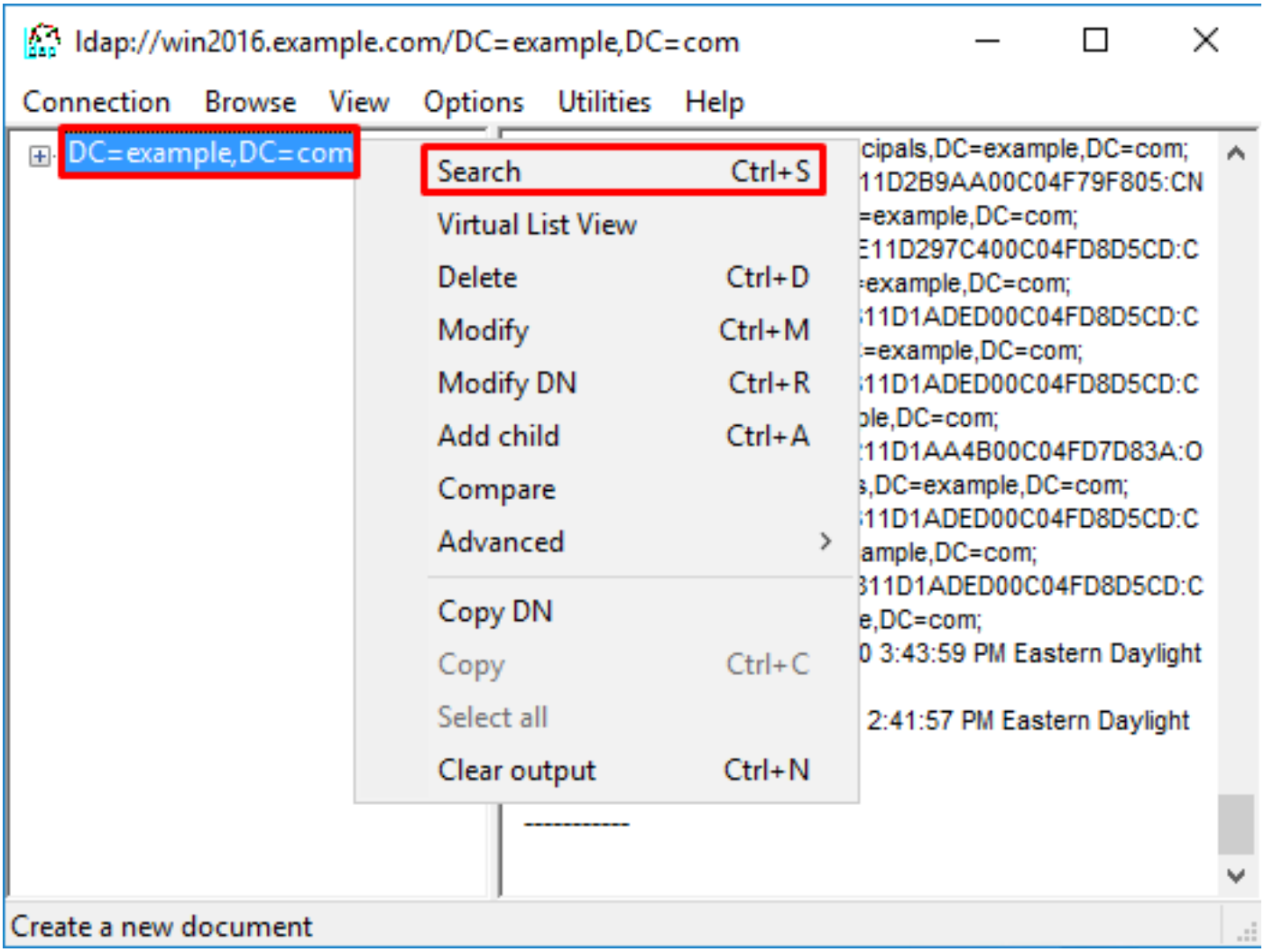
1. Después de enlazar correctamente, navegue hasta **Ver > Árbol** como se muestra en la imagen.



2. Especifique el DN base configurado en el FTD y haga clic en **Aceptar**.

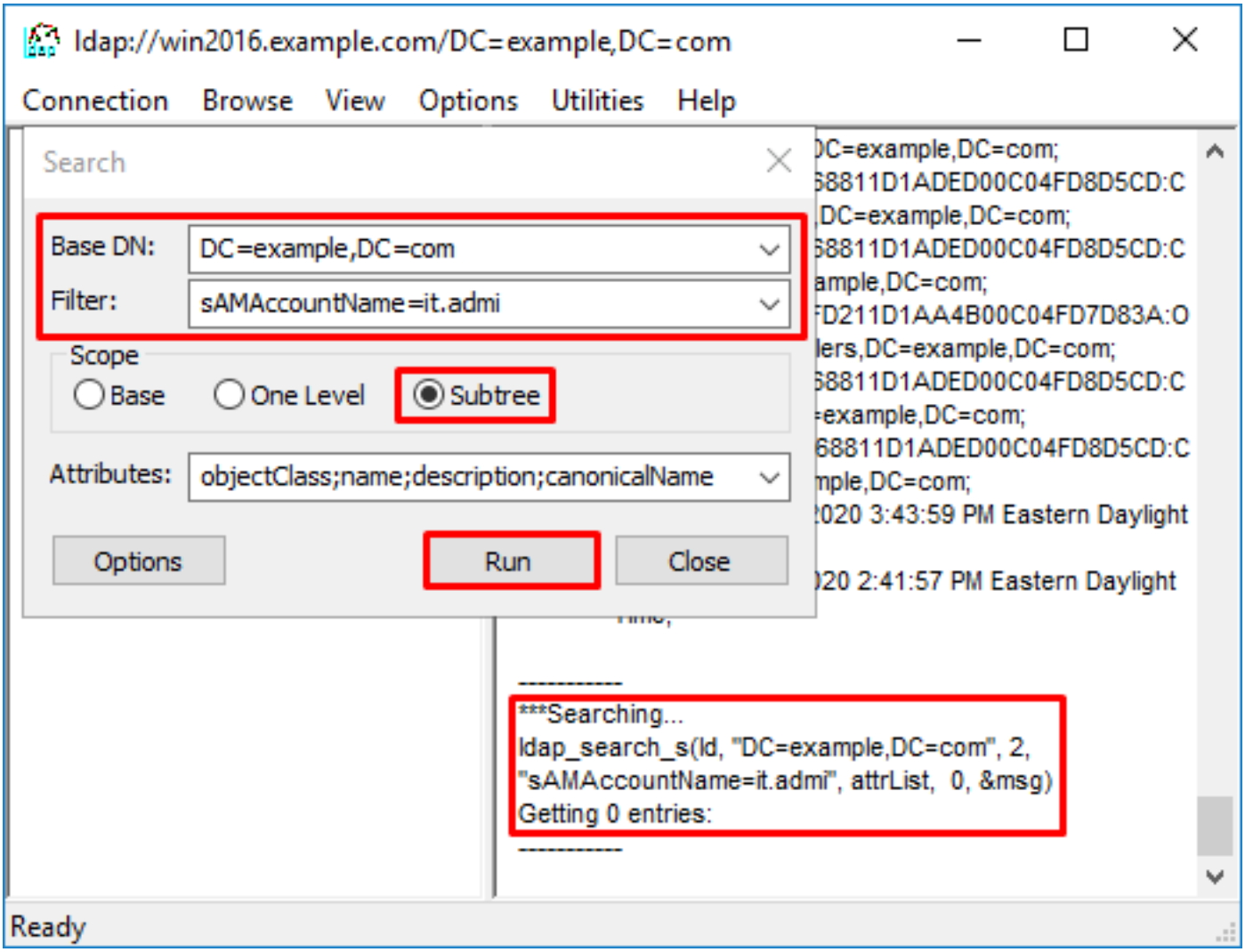


3. Haga clic con el botón derecho del ratón en el DN base y, a continuación, haga clic en Buscar como se muestra en la imagen.



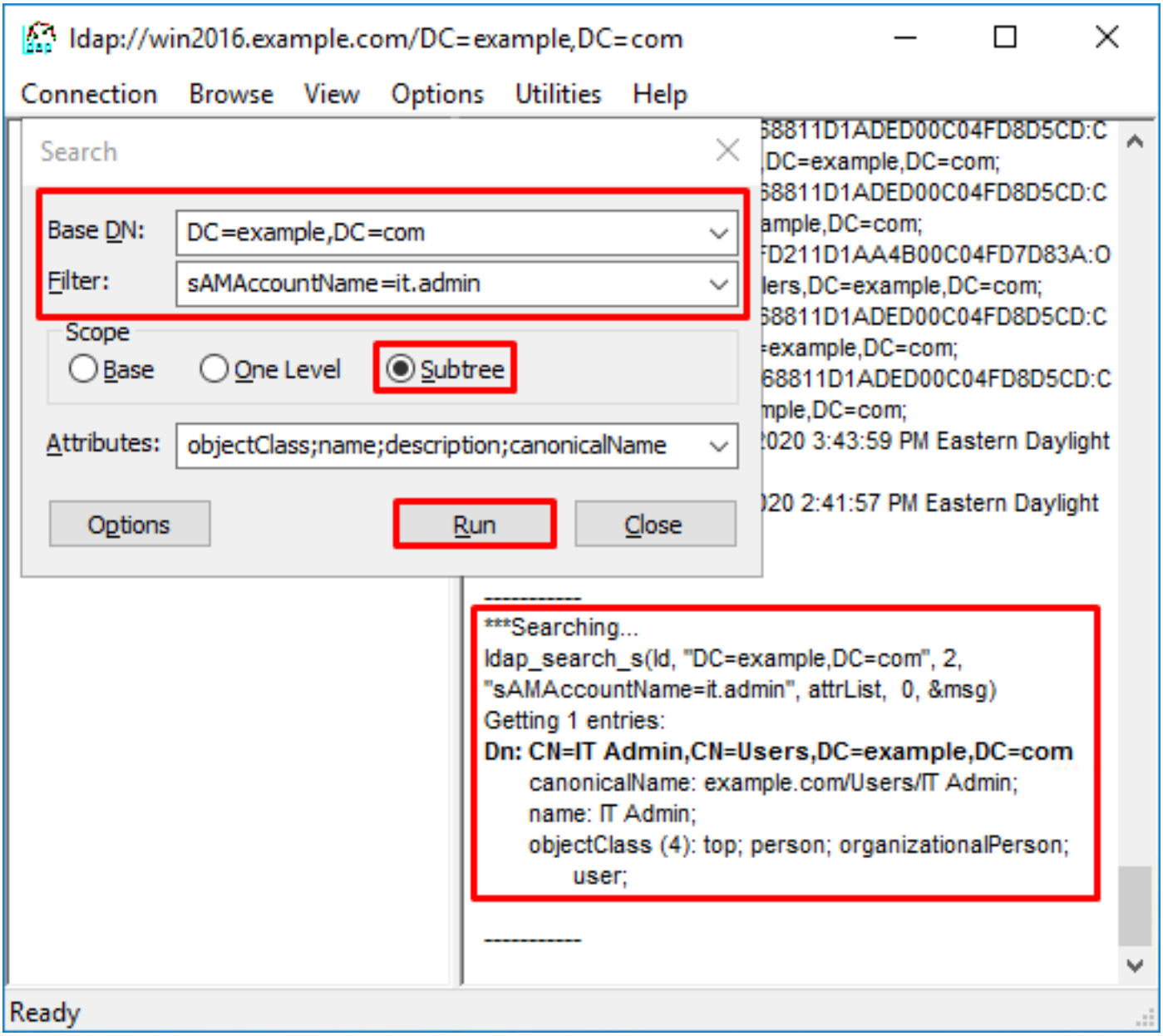
4. Especifique los mismos valores Base DB, Filter y Scope que se ven en las depuraciones. En este ejemplo, estos son:

- DN base: dc=ejemplo,dc=com
- Filtro: samaccounting tname=it.admi
- Ámbito:SUBTREE



ldp encuentra 0 entradas debido a que no hay una cuenta de usuario con el **samaccounting tname=it.admi** bajo el DN base dc=example,dc=com.

Intentar de nuevo con el **samaccountname=it.admin** correcto muestra un resultado diferente. ldp encuentra 1 entrada bajo el DN base dc=example,dc=com e imprime el DN del usuario.



Contraseña incorrecta para el nombre de usuario

```
[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter  = [samaccountname=it.admin]
        Scope   = [SUBTREE]
[-2147483613] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
```

```
[-2147483613] Simple authentication for it.admin returned code (49) Invalid credentials
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment:
AcceptSecurityContext error, data 52e, v3839
[-2147483613] Invalid password for it.admin
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

Solución potencial: Verifique que la contraseña del usuario esté configurada correctamente y que no haya caducado. Al igual que el DN de inicio de sesión, el FTD realizará un enlace contra AD con las credenciales del usuario. Este enlace también se puede hacer en ldp para verificar que AD pueda reconocer las mismas credenciales de nombre de usuario y contraseña. Los pasos en ldp se muestran en la sección **Enlace de DN de Inicio de Sesión y/o Contraseña Incorrecta**. Además, los registros del Visor de eventos del servidor de Microsoft se pueden revisar por un posible motivo.

Prueba AAA

El comando test aaa-server se puede utilizar para simular un intento de autenticación del FTD con un nombre de usuario y una contraseña específicos. Esto se puede utilizar para probar las fallas de conexión o autenticación. El comando es **test aaa-server authentication [AAA-server] host [AD IP/hostname]**.

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
 realm-id 7
aaa-server LAB-AD host win2016.example.com
 server-port 389
 ldap-base-dn DC=example,DC=com
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn ftd.admin@example.com
 server-type auto-detect

> test aaa-server authentication LAB-AD host win2016.example.com
Username: it.admin
Password: ********
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

Capturas de paquetes

Las capturas de paquetes se pueden utilizar para verificar el alcance del servidor AD. Si los paquetes LDAP dejan el FTD, pero no hay respuesta, esto podría indicar un problema de ruteo.

Esta es una captura hecha que muestra el tráfico LDAP bidireccional:

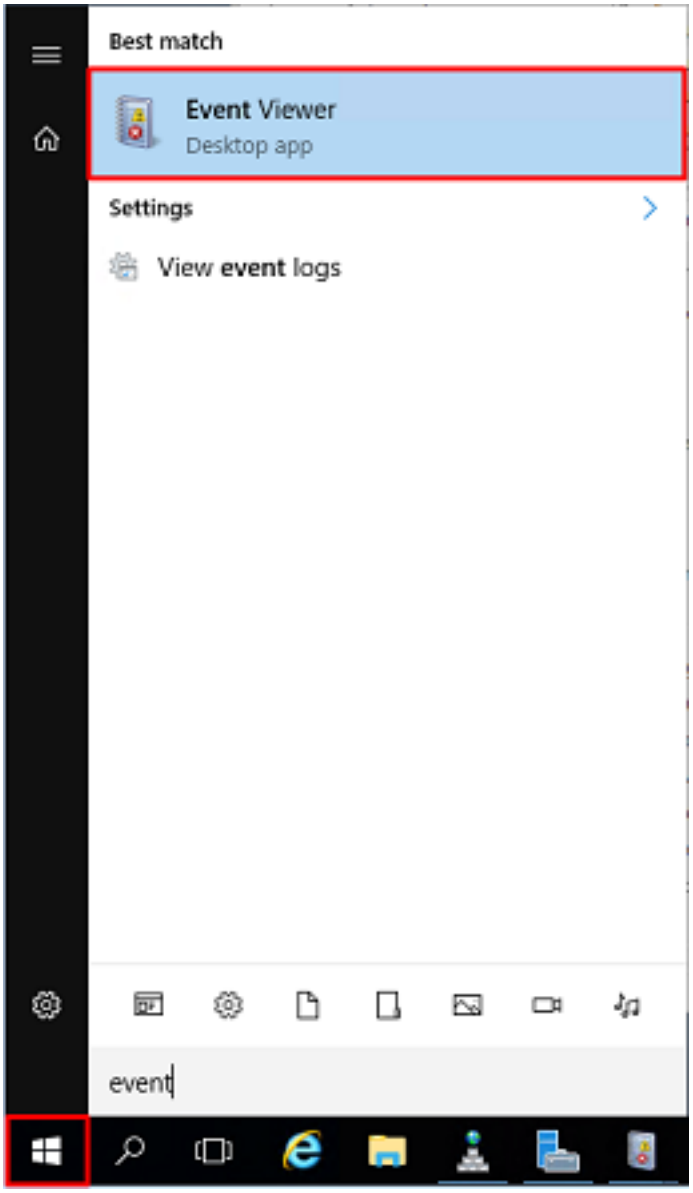
```
> show route 192.168.1.1

Routing entry for 192.168.1.0 255.255.255.0
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via inside
      Route metric is 0, traffic share count is 1

> capture AD interface inside match tcp any host 192.168.1.1 eq 389
```

```
> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
  match tcp any host 192.168.1.1 eq ldap

> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password
******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful

> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
  match tcp any host 192.168.1.1 eq ldap

> show capture AD

54 packets captured

   1: 23:02:16.770712       192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
   2: 23:02:16.772009       192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
   3: 23:02:16.772039       192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768
<nop,nop,timestamp 1061373058 762393884>
   4: 23:02:16.772482       192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145)
ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0>
   5: 23:02:16.772924       192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
   6: 23:02:16.772955       192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
<nop,nop,timestamp 1061373059 762393885>
   7: 23:02:16.773428       192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
   8: 23:02:16.775030       192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
   9: 23:02:16.775075       192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop,nop,timestamp 1061373061 762393887>
[...]
54 packets shown
```

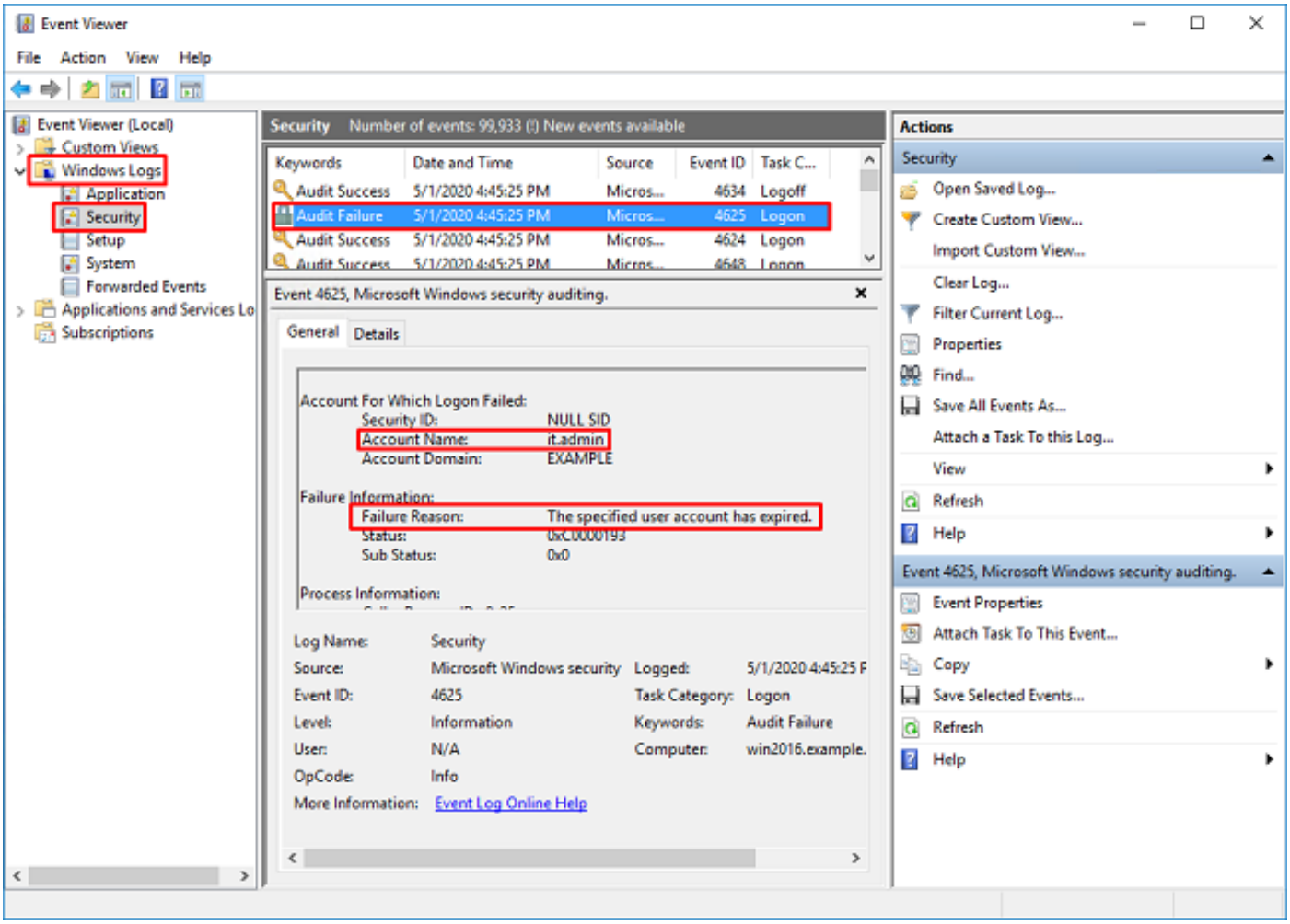
Registros del Visor de eventos de Windows Server

Los registros del Visor de eventos en la furgoneta del servidor AD proporcionan información más detallada sobre el motivo del error.

1. Busque y abra **Event Viewer**.



2. Expanda **Registros de Windows** y haga clic en **Seguridad**. Busque **Falla de Auditoría** con el Nombre de Cuenta del usuario y revise la Información de Fallas como se muestra en la imagen.



An account failed to log on.

Subject:
Security ID:SYSTEM
Account Name:WIN2016$
Account Domain:EXAMPLE
Logon ID:0x3E7

Logon Type:3

Account For Which Logon Failed:
Security ID:NULL SID
Account Name:it.admin
Account Domain:EXAMPLE

Failure Information:
Failure Reason:The specified user account has expired.
Status:0xC0000193
Sub Status:0x0

Process Information:
Caller Process ID:0x25c
Caller Process Name:C:\Windows\System32\lsass.exe

Network Information:
Workstation Name:WIN2016
Source Network Address:192.168.1.17
Source Port:56321