Configurar a autenticação do AD (LDAP) e a identidade do usuário no FTD gerenciado pelo FDM para clientes AnyConnect

Contents

Introduction

O objetivo deste documento é detalhar como configurar a autenticação do Ative Diretory (AD) para clientes AnyConnect que se conectam a um Cisco Firepower Threat Defense (FTD) gerenciado pelo Firepower Device Management (FDM). A identidade do usuário será usada nas políticas de acesso para restringir os usuários do AnyConnect a endereços IP e portas específicos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração da VPN RA no FDM
- Conhecimento básico da configuração do servidor LDAP no FDM
- Conhecimento básico do AD

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft 2016 Server
- FTDv executando 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama e cenário de rede

O servidor Windows é pré-configurado com o Internet Information Services (IIS) e o Remote Desktop Protocol (RDP) para testar a identidade do usuário. Neste guia de configuração, três contas de usuário e dois grupos serão criados.

Contas do usuário:

- Administrador do FTD: Isso será usado como a conta de diretório para permitir que o FTD se vincule ao servidor do AD.
- Administrador de TI: Uma conta de administrador de teste usada para demonstrar a identidade do usuário.
- Testar usuário: Uma conta de usuário de teste usada para demonstrar a identidade do usuário.

Grupos:

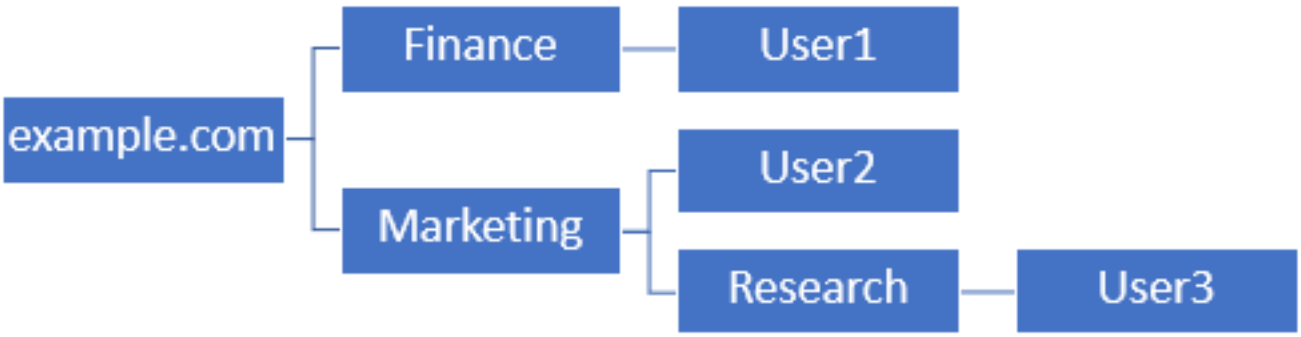
- Administradores do AnyConnect: Um grupo de teste ao qual o administrador de TI será adicionado para demonstrar a identidade do usuário. Este grupo terá apenas acesso RDP ao

Windows Server
- Usuários do AnyConnect: Um grupo de teste ao qual o usuário do teste será adicionado para demonstrar a identidade do usuário. Este grupo terá apenas acesso HTTP ao Windows Server

Configurações do AD

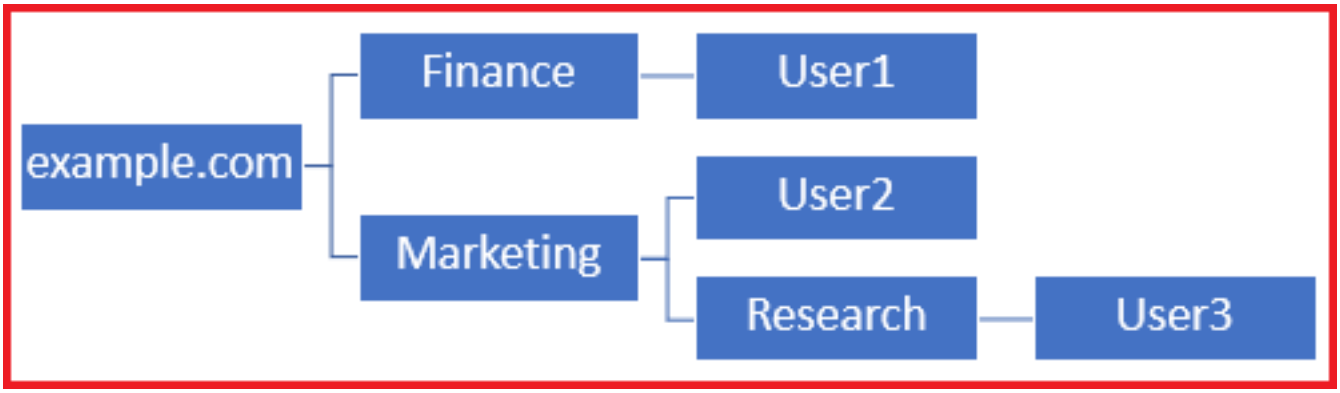
Para configurar apropriadamente a autenticação do AD e a identidade do usuário no FTD, alguns valores serão necessários. Todos esses detalhes devem ser criados ou coletados no Microsoft Server para que a configuração possa ser feita no FDM. Os principais valores são:

- Nome de domínio: Este é o nome de domínio do servidor. Neste guia de configuração, example.com é o nome de domínio.
- Endereço IP/FQDN do servidor: O endereço IP ou FQDN usado para acessar o servidor Microsoft. Se um FQDN for usado, um servidor DNS deverá ser configurado no FDM e no FTD para resolver o FQDN. Neste guia de configuração, esses valores são **win2016.example.com**, que é resolvido para 192.168.1.1.
- Porta do servidor: A porta usada pelo serviço LDAP. Por padrão, LDAP e STARTTLS usarão a porta TCP 389 para LDAP e LDAP sobre SSL (LDAPS) usarão a porta TCP 636.
- CA raiz: Se LDAPS ou STARTTLS for usado, a CA raiz usada para assinar o certificado SSL usado pelo LDAPS será necessária.
- Nome de usuário e senha do diretório: Esta é a conta usada pelo FDM e FTD para se vincular ao servidor LDAP e autenticar usuários e procurar usuários e grupos. Uma conta chamada Administrador do FTD será criada para essa finalidade.
- Nome distinto básico (DN): O DN base é o FDM do ponto de partida e o FTD instruirá o Ative Diretory a começar a procurar usuários. Neste guia de configuração, o domínio raiz example.com será usado como o DN base; no entanto, para um ambiente de produção, o uso de um DN base além da hierarquia LDAP pode ser melhor. Por exemplo, tome esta hierarquia LDAP:



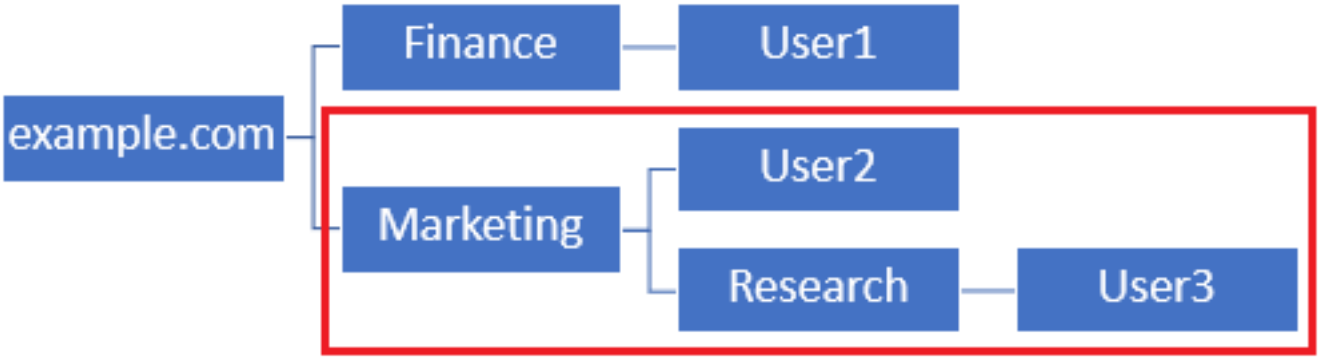
Se um administrador deseja que os usuários na unidade organizacional de Marketing possam autenticar o DN base para a raiz (example.com), no entanto, isso também permitirá que o Usuário1 na unidade organizacional de Finanças também faça login, já que a pesquisa do usuário começará na raiz e descerá para Finanças, Marketing e Pesquisa.

DN base definido como example.com.



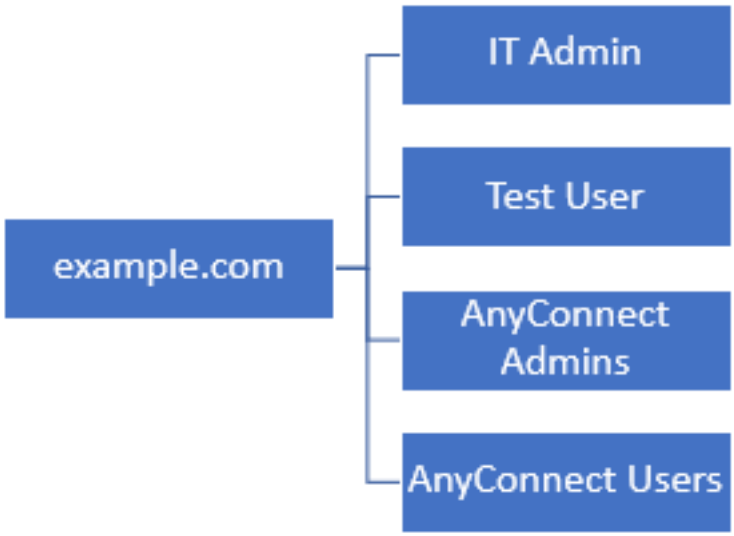
Para restringir os logins somente aos usuários na unidade organizacional de Marketing e abaixo, o administrador pode definir o DN base como Marketing. Agora, somente Usuário2 e Usuário3 poderão autenticar porque a pesquisa começará no Marketing.

DN base definido para Marketing:



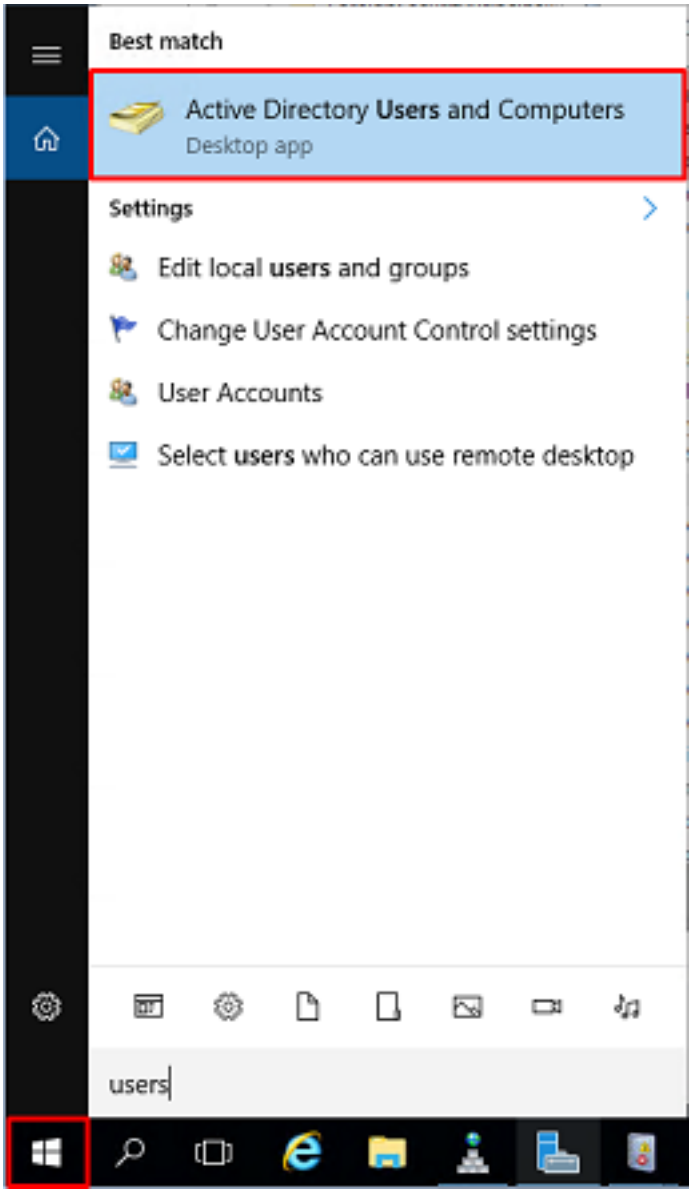
Observe que para um controle mais granular dentro do FTD para o qual os usuários poderão se conectar ou atribuir a usuários autorizações diferentes com base em seus atributos do AD, um mapa de autorização LDAP precisará ser configurado.

Essa hierarquia LDAP simplificada é usada neste guia de configuração e o DN para o exemplo raiz.com será usado para o DN base.

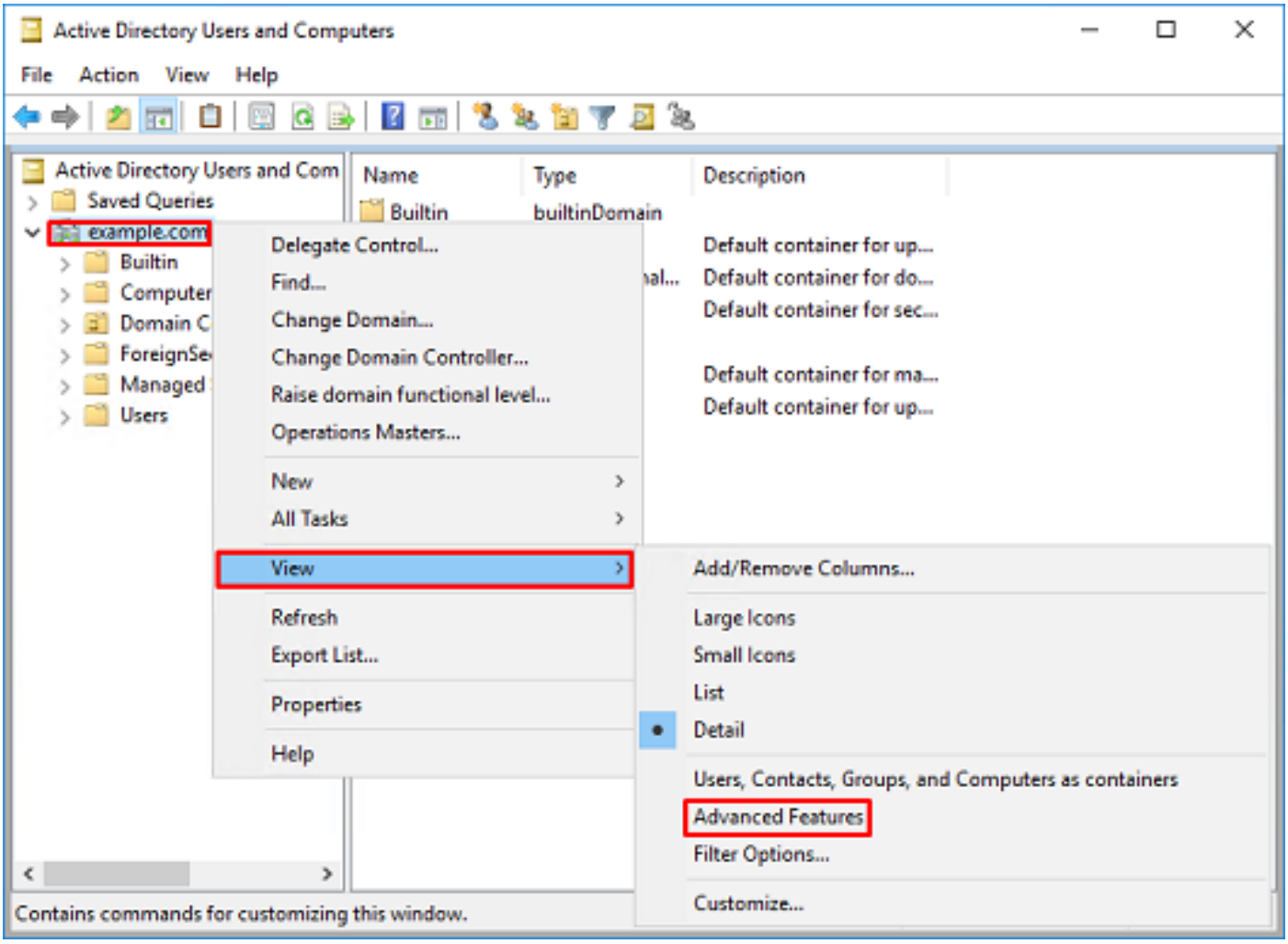


Determinar DN base LDAP

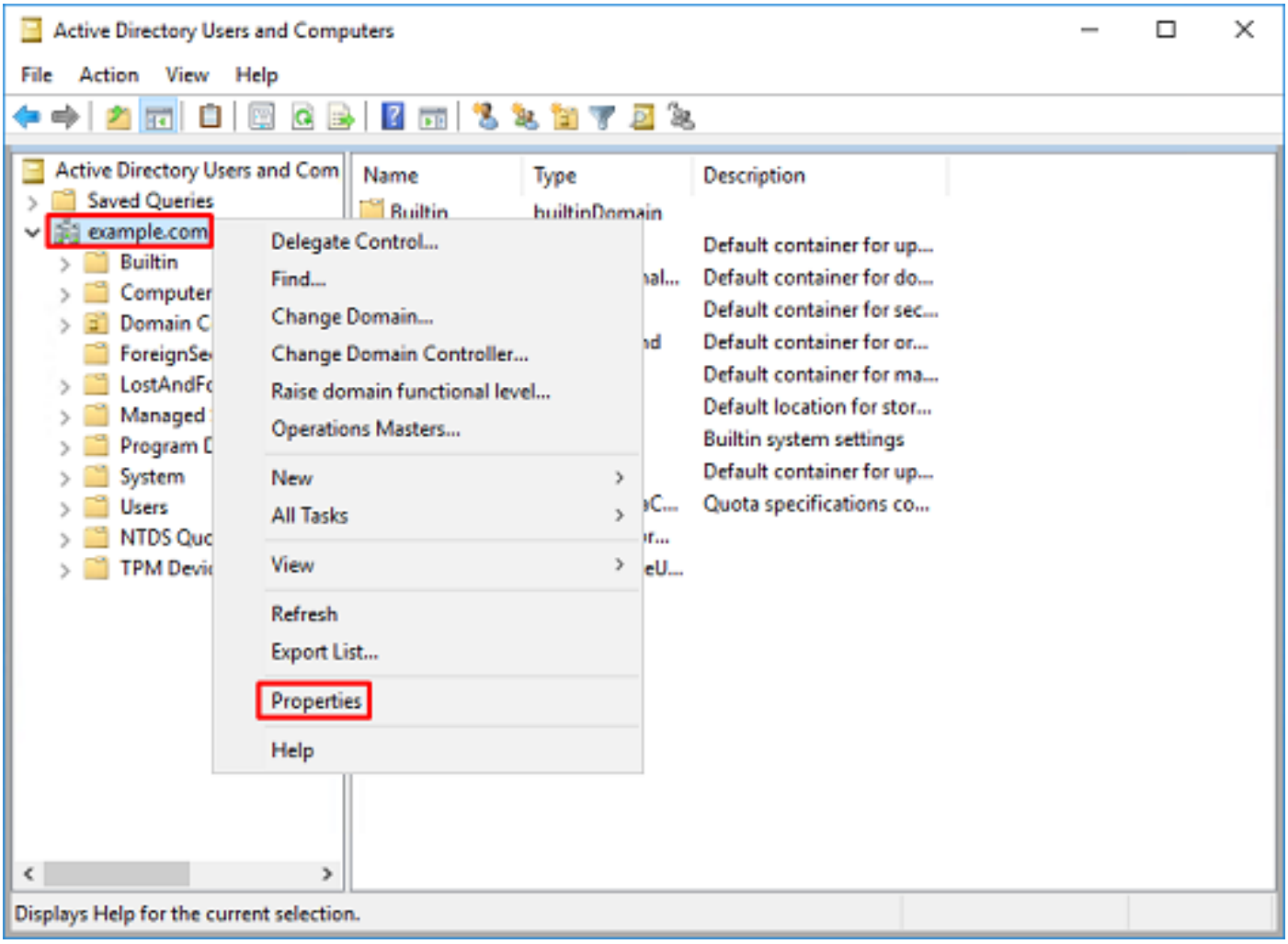
1. Abra usuários e computadores do AD.



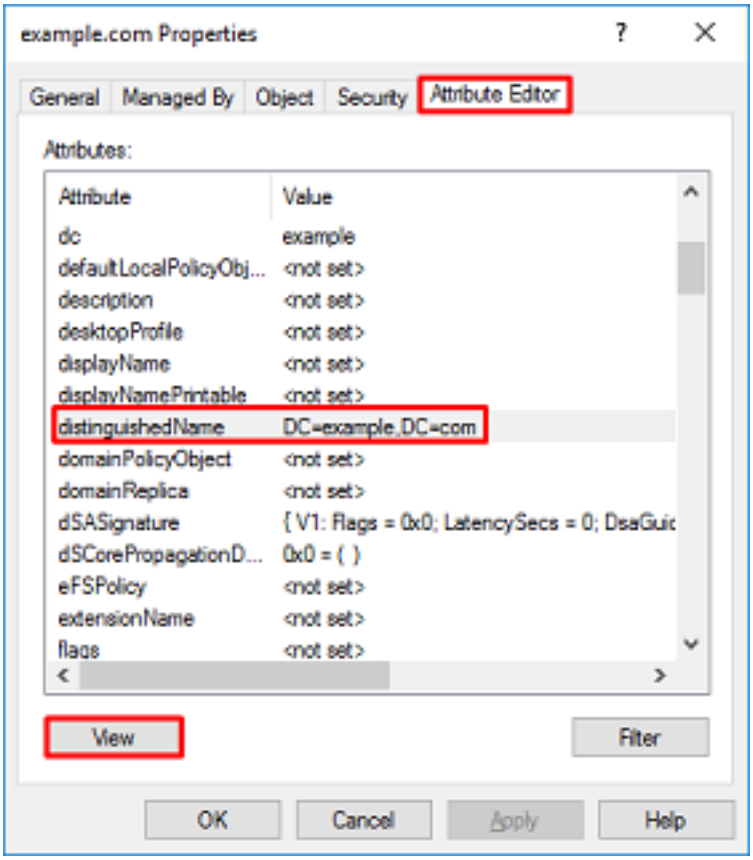
2. Clique com o botão esquerdo do mouse no domínio raiz (para abrir o contêiner), clique com o botão direito do mouse no domínio raiz e, em seguida, navegue para **Exibir** e clique em **Recursos avançados**.



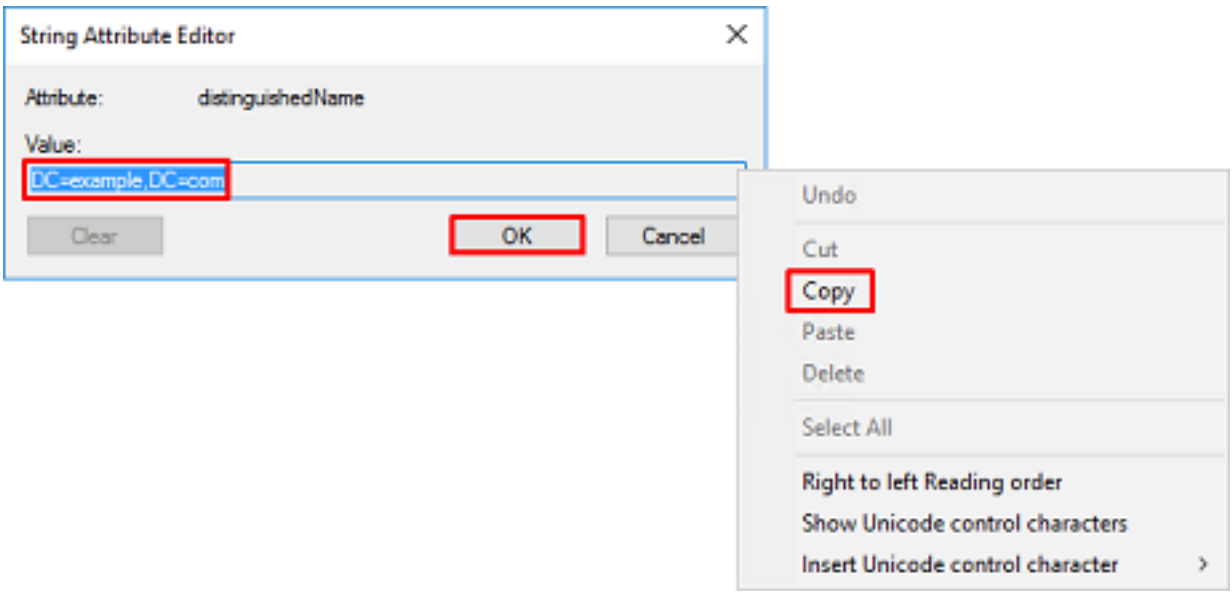
3. Isso ativará a exibição de propriedades adicionais nos objetos do AD. Por exemplo, para localizar o DN para o exemplo raiz.com, clique com o botão direito do mouse em **example.com** e navegue até **Properties**.

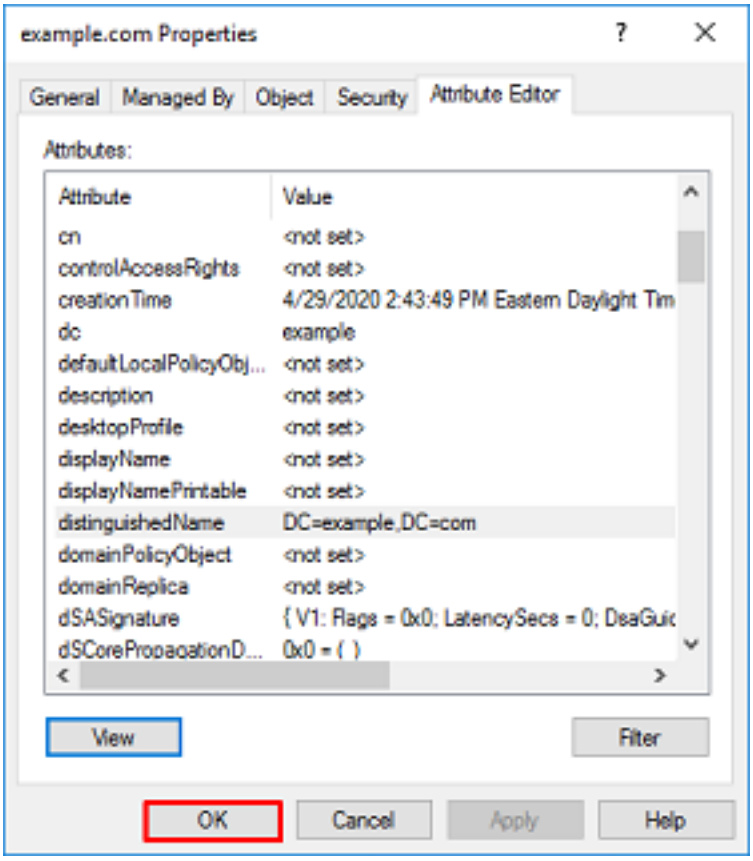


4. Em **Propriedades**, clique na guia **Editor de atributos**. Localizar **DistinguishedName** em Attributes e, em seguida, clique em **View**.

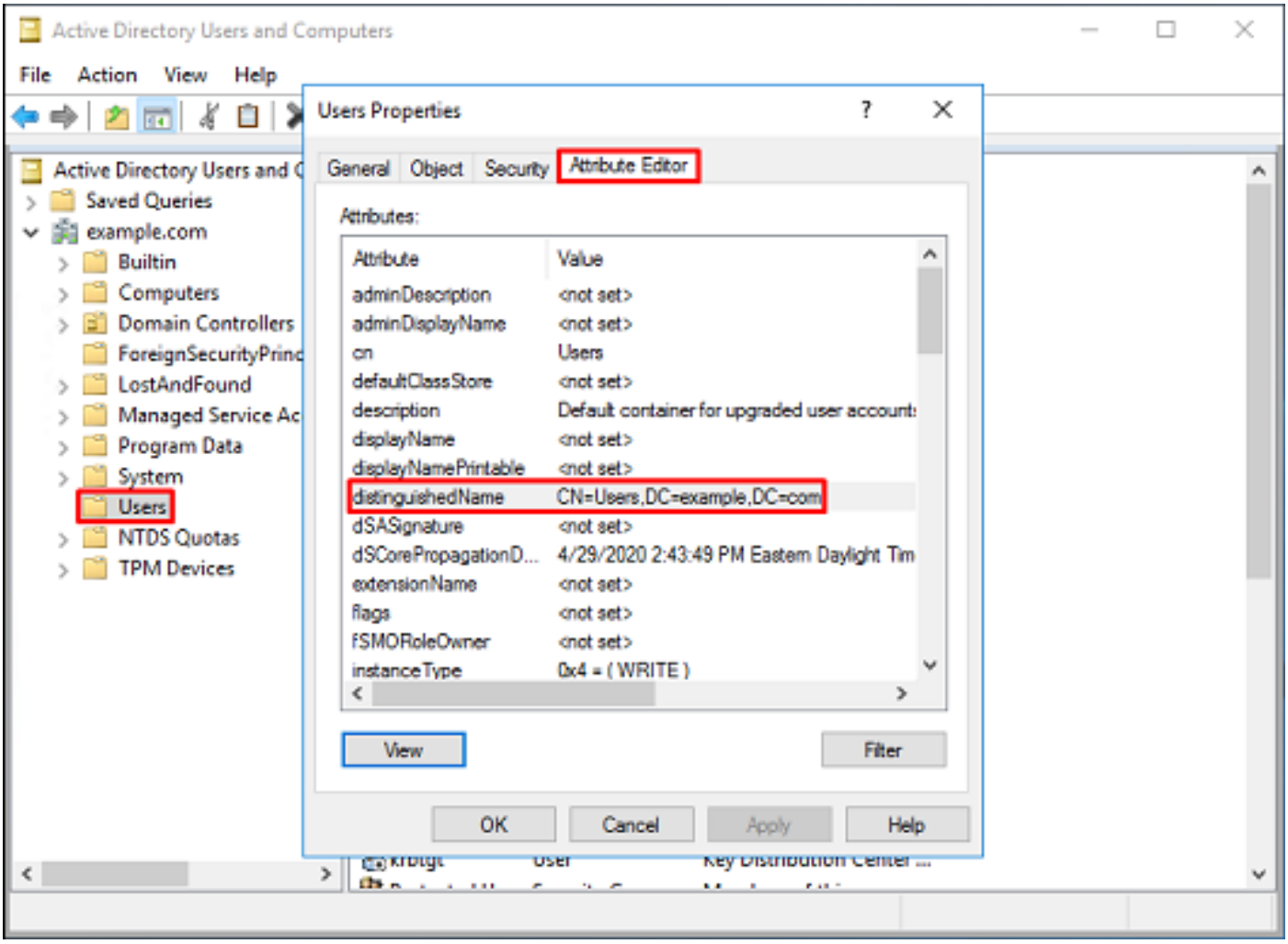


5. Isso abrirá uma nova janela na qual o DN poderá ser copiado e colado no FDM posteriormente. Neste exemplo, o DN raiz é DC=example, DC=com. Copie o valor. Clique em **OK** para sair da janela Editor de atributos de cadeia de caracteres e clique em **OK** novamente para sair das Propriedades.

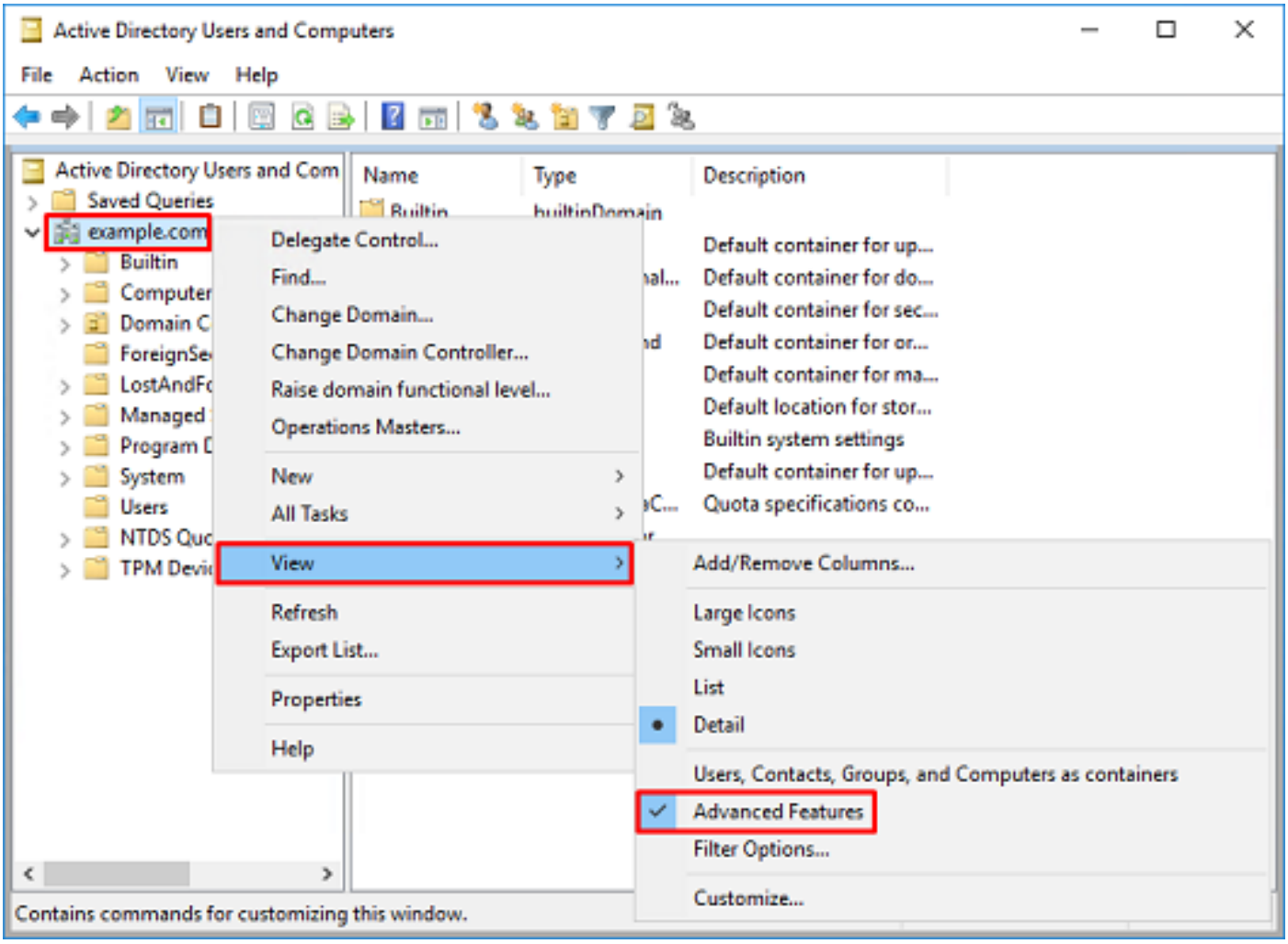




Isso pode ser feito para vários objetos no AD. Por exemplo, estas etapas são usadas para localizar o DN do contêiner do usuário:



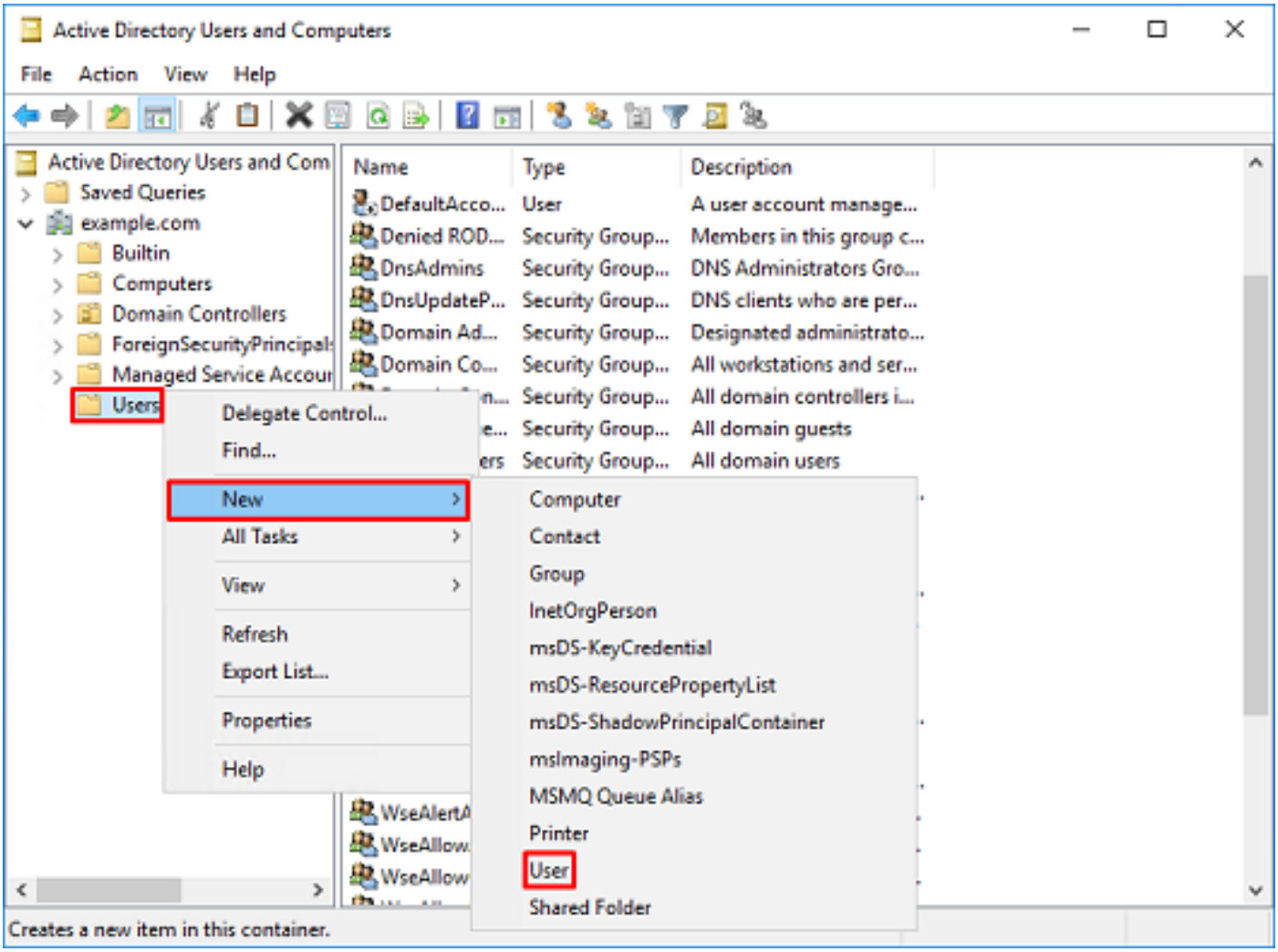
6. A exibição Recursos avançados pode ser removida. Clique com o botão direito do mouse no DN raiz, navegue para **View** e clique em **Advanced Features** mais uma vez.



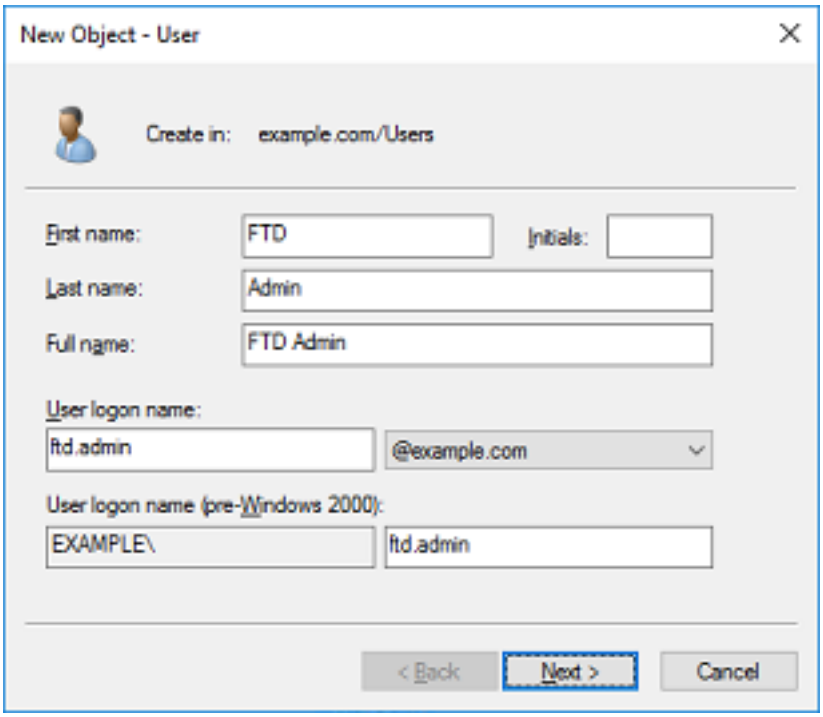
Criar uma conta FTD

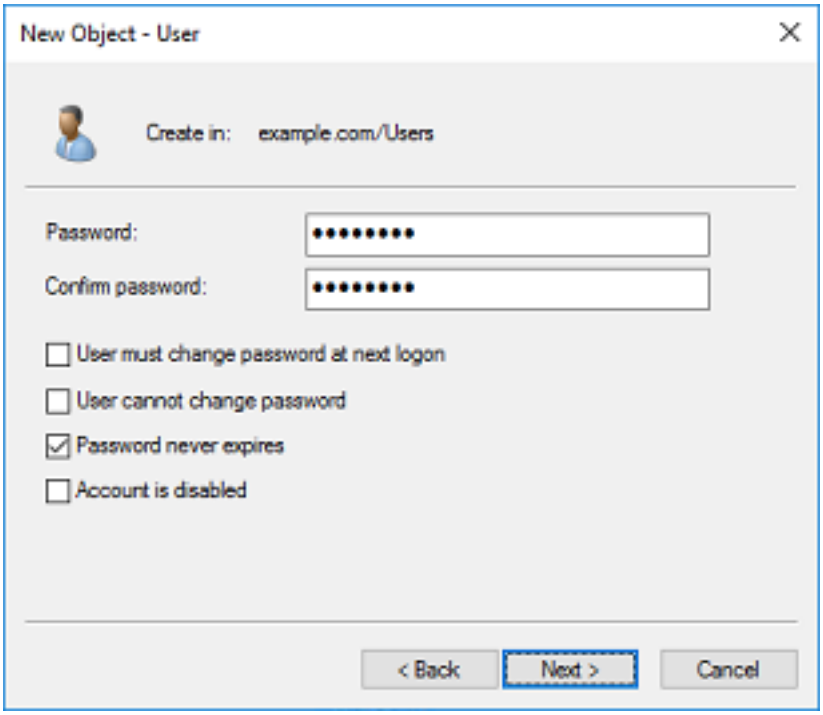
Essa conta de usuário permitirá que o FDM e o FTD se vinculem ao AD para pesquisar usuários e grupos e autenticá-los. A finalidade da criação de uma conta FTD separada é impedir o acesso não autorizado em outro lugar da rede se as credenciais usadas para a vinculação forem comprometidas. Essa conta não precisa estar dentro do escopo do DN base.

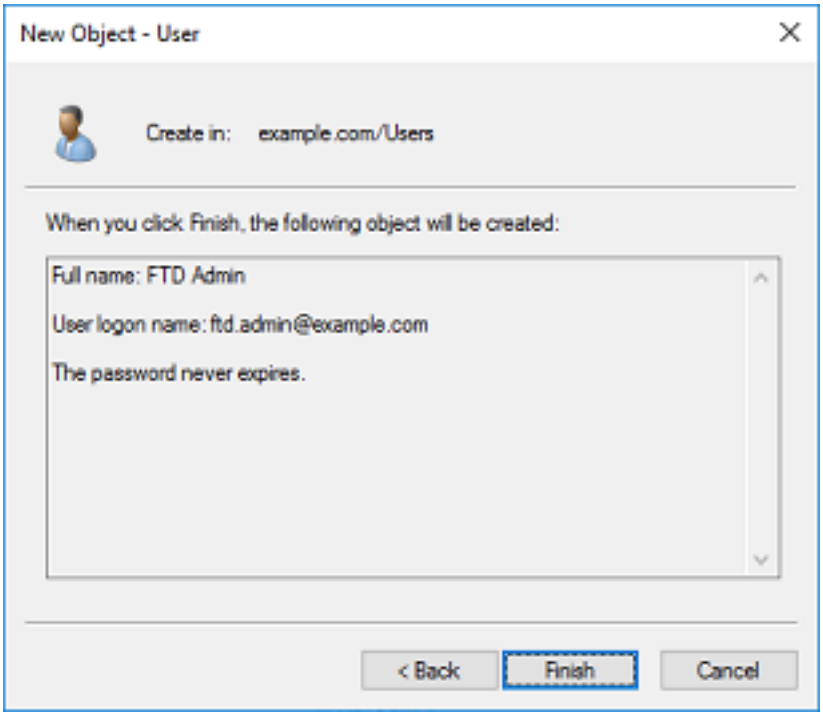
1. Em **Usuários e Computadores do Ative Diretory**, clique com o botão direito do mouse no contêiner/organizacional ao qual a conta FTD será adicionada. Nesta configuração, a conta FTD será adicionada no contêiner Usuários no nome de usuário **ftd.admin@example.com**. Clique com o botão direito do mouse em **Usuários** e clique em **Novo > Usuário**.



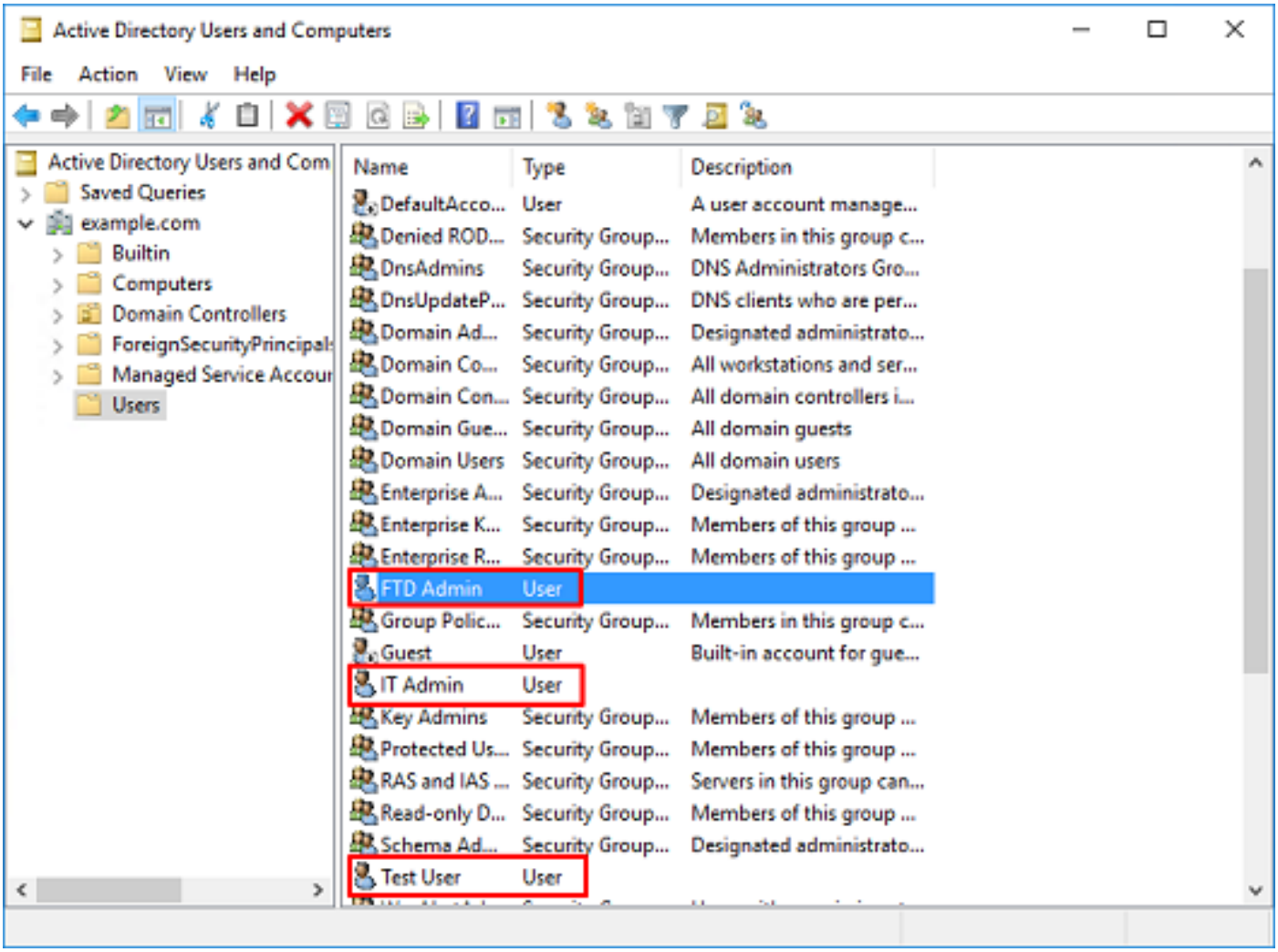
2. Navegue pelo Assistente **Novo Objeto - Usuário**.







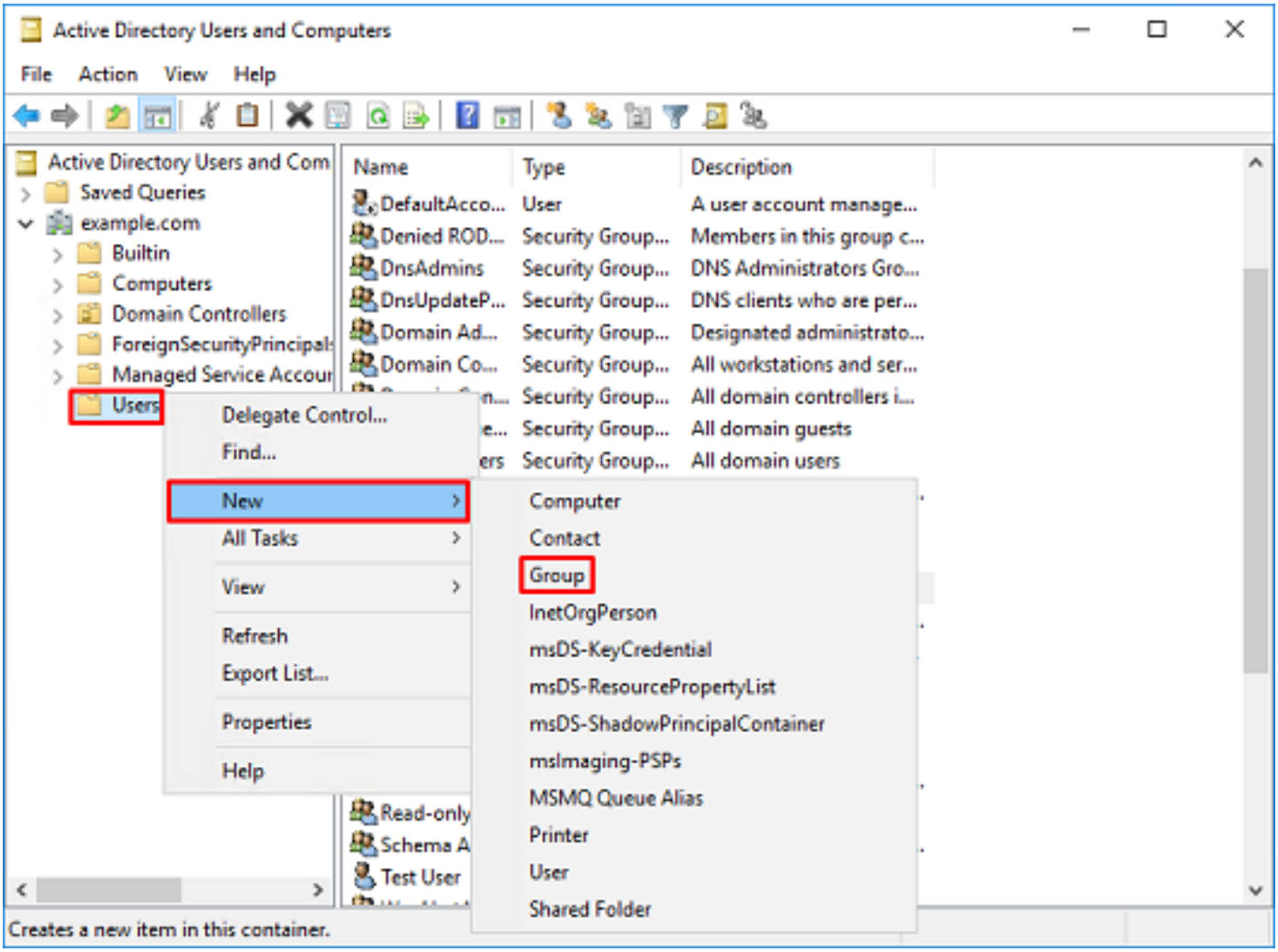
3. Verifique se a conta FTD foi criada. Além disso, duas contas adicionais foram criadas, **administrador de TI** e **usuário de teste**.



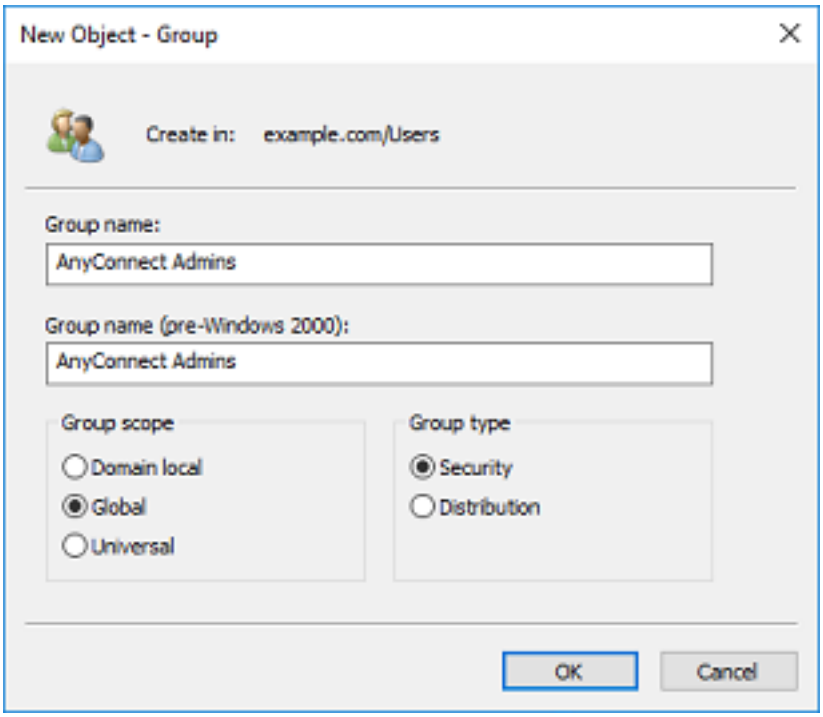
Criar grupos AD e Adicionar usuários a grupos AD (opcional)

Embora não seja necessário para autenticação, os grupos podem ser usados para facilitar a aplicação de políticas de acesso a vários usuários, bem como a autorização LDAP. Neste guia de configuração, os grupos serão usados para aplicar as configurações de política de controle de acesso posteriormente por meio da identidade do usuário no FDM.

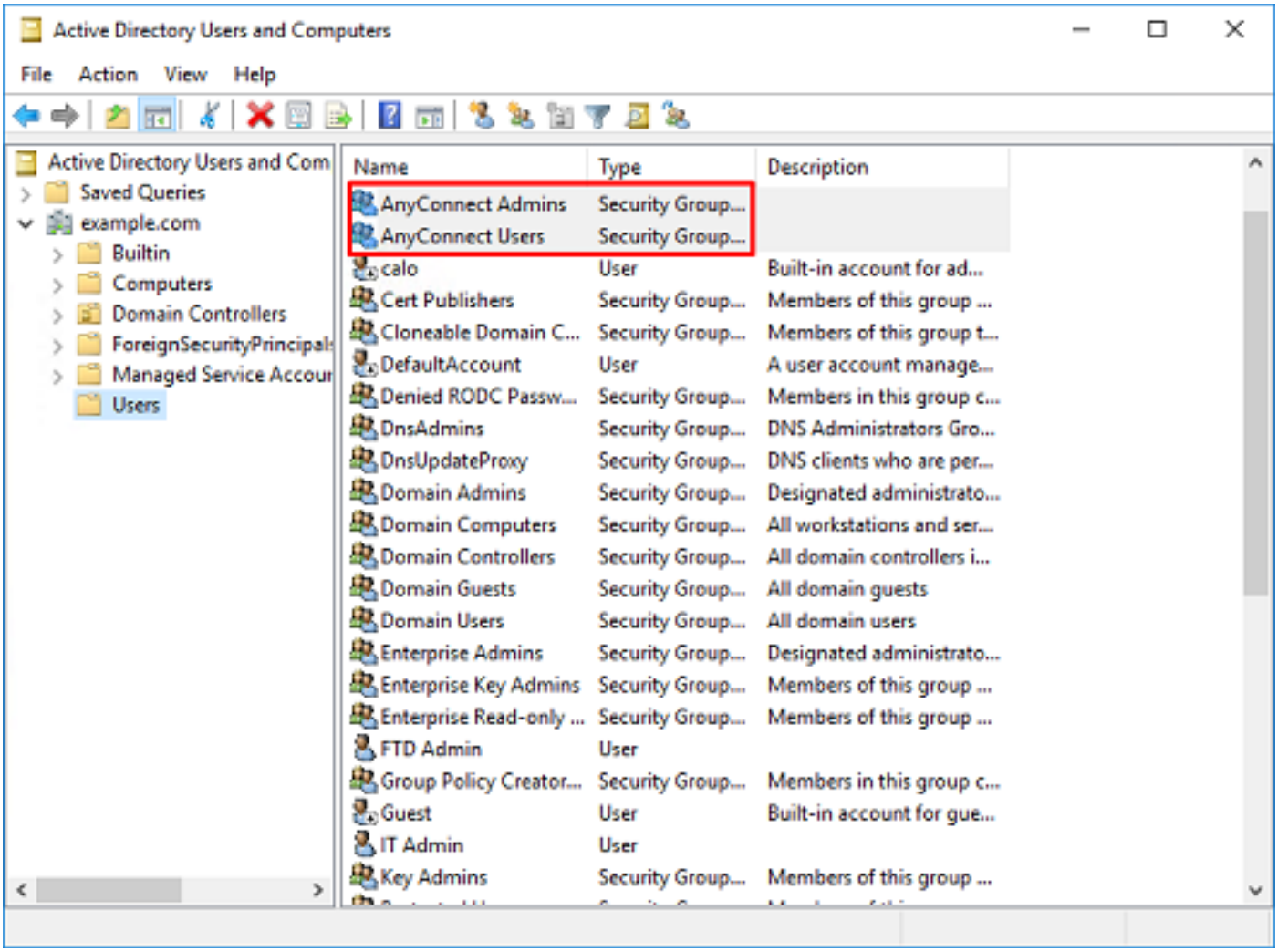
1. Em **Usuários e Computadores do Ative Diretory**, clique com o botão direito do mouse no contêiner/organizacional ao qual o novo grupo será adicionado. Neste exemplo, o grupo **AnyConnect Admins** será adicionado no contêiner Users. Clique com o botão direito do mouse em **Usuários** e clique em **Novo > Grupo**.



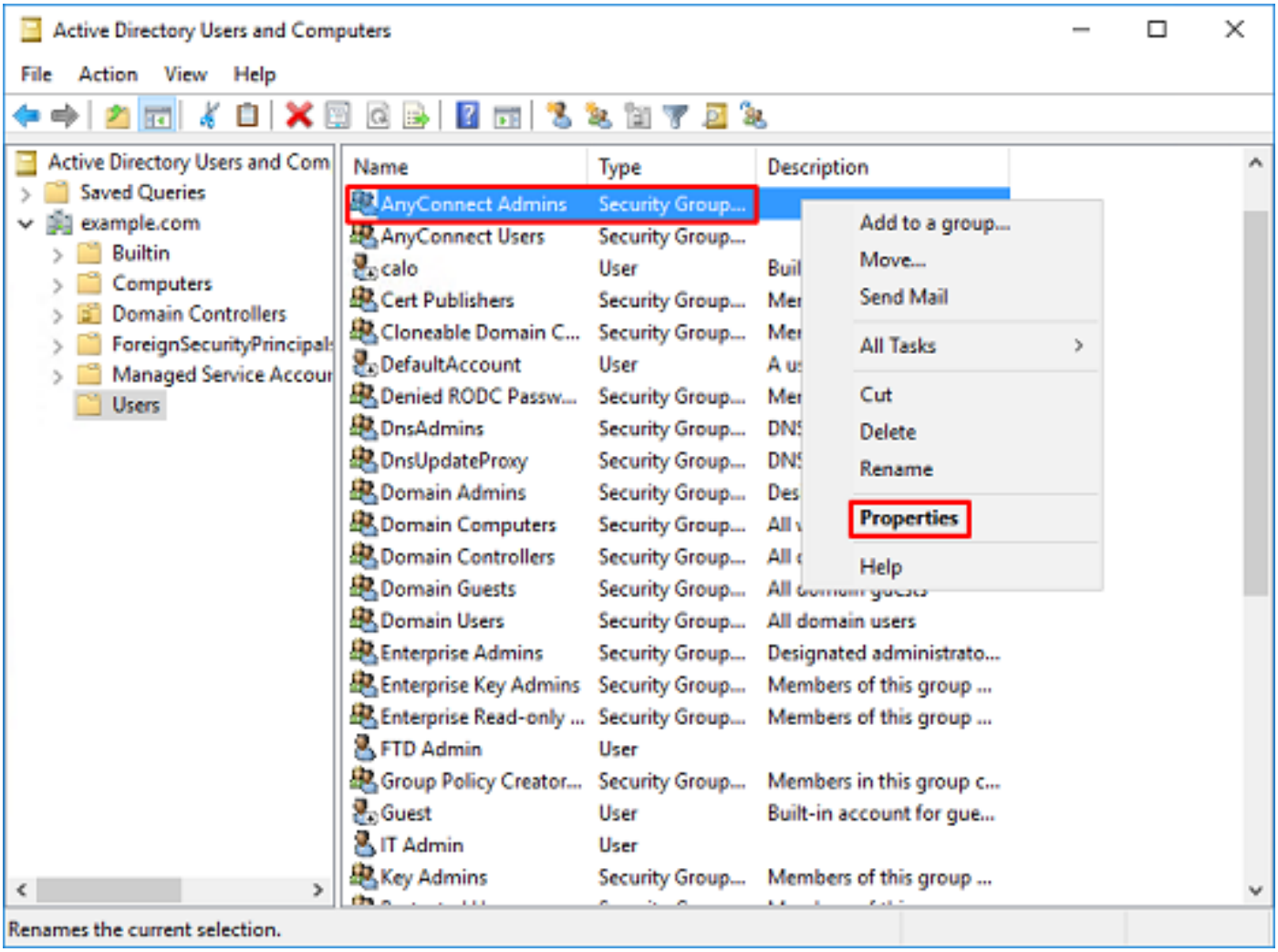
2. Navegue pelo Assistente **Novo Objeto - Grupo**, conforme mostrado na imagem.



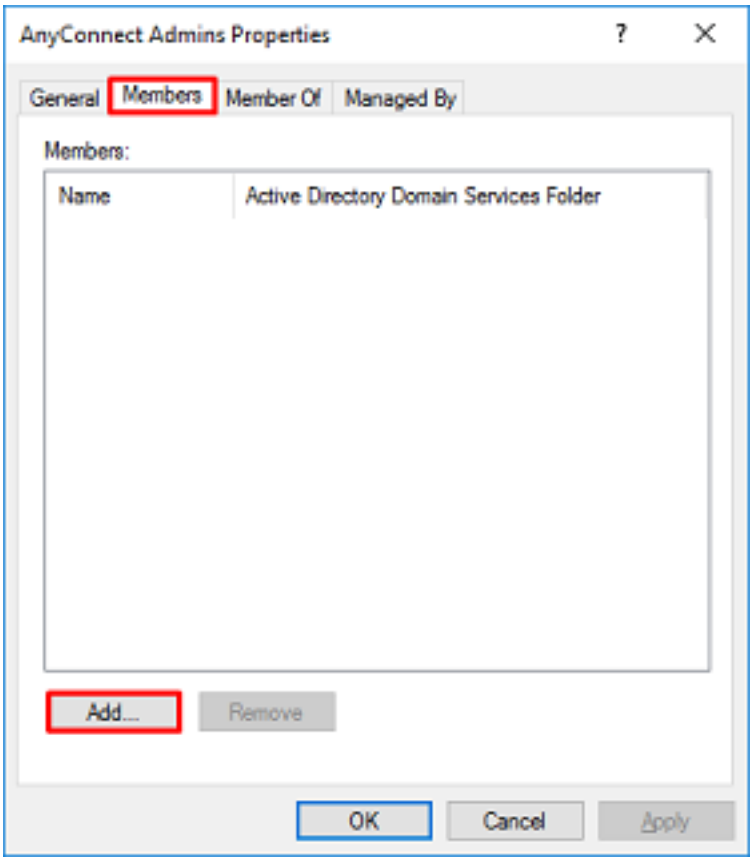
3. Verifique se o grupo foi criado. O grupo **Usuários do AnyConnect** também foi criado.



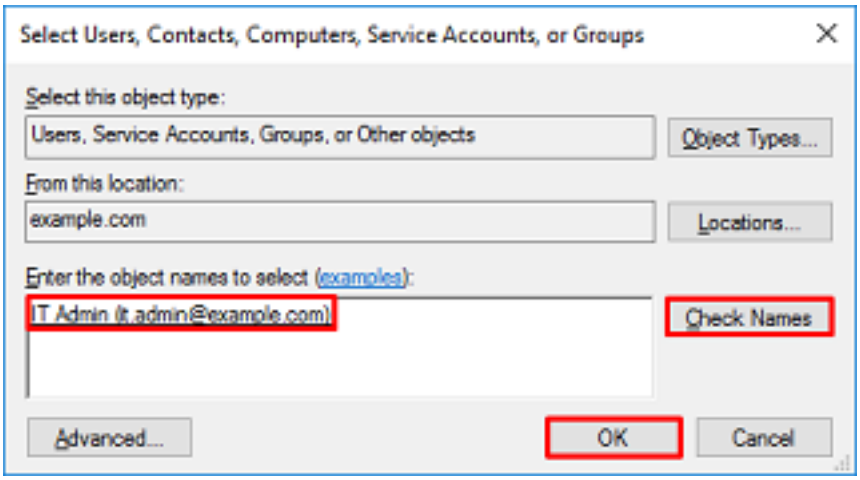
4. Clique com o botão direito do mouse no grupo ao qual os usuários serão adicionados e selecione **Propriedades**. Nesta configuração, o usuário **IT Admin** será adicionado ao grupo **AnyConnect Admins** e o usuário **Test User** será adicionado ao grupo **AnyConnect Users**.



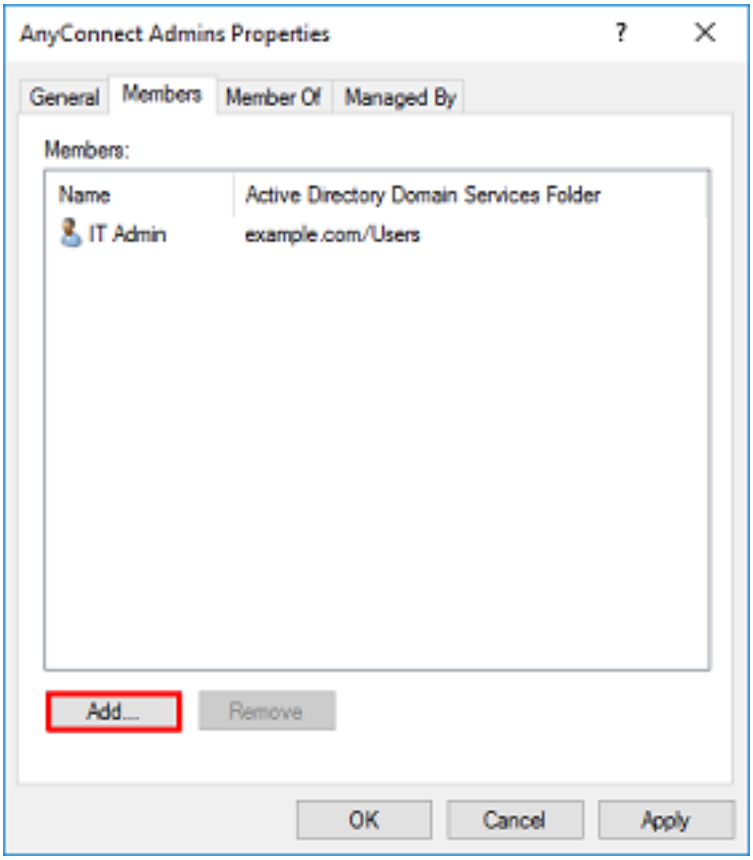
5. Clique na guia **Membros** e clique em **Adicionar** conforme mostrado na imagem.



Insira o usuário no campo e clique no botão **Verificar nomes** para verificar se o usuário foi encontrado. Depois de verificado, clique em **OK**.

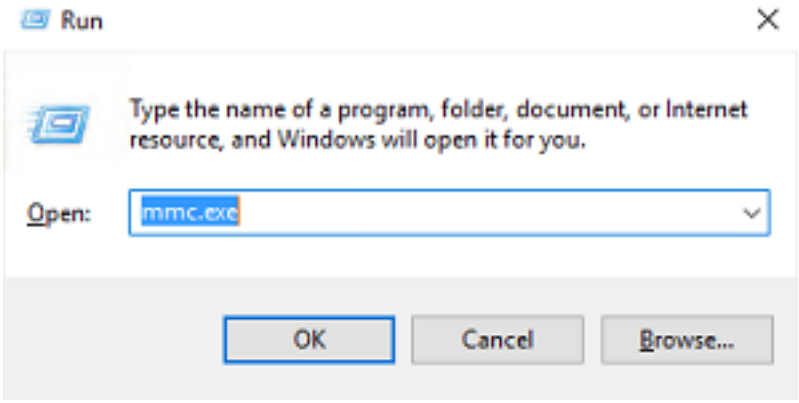


Verifique se o usuário correto foi adicionado e clique no botão **OK**. O usuário Testar usuário também é adicionado ao grupo Usuários do AnyConnect com o uso das mesmas etapas.

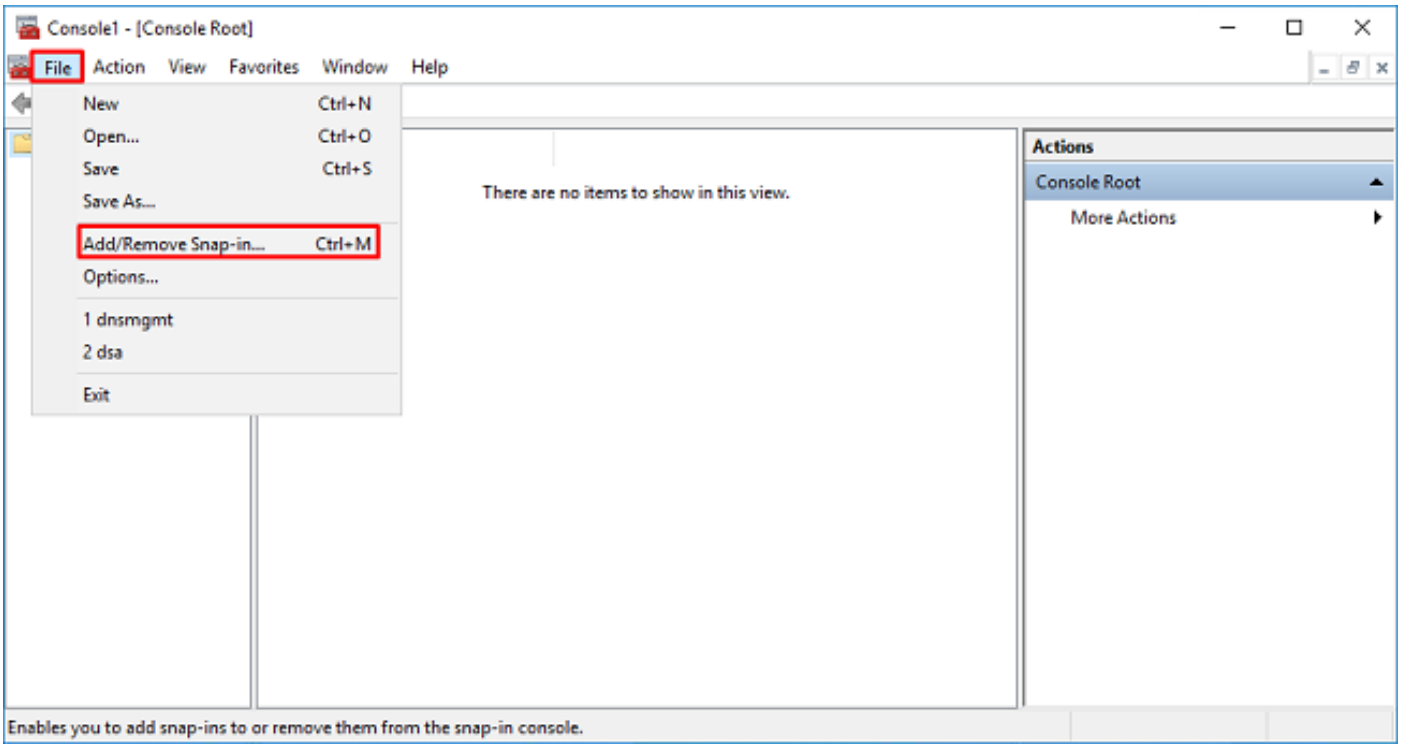


Copiar a raiz do certificado SSL LDAPS (obrigatório apenas para LDAPS ou STARTTLS)

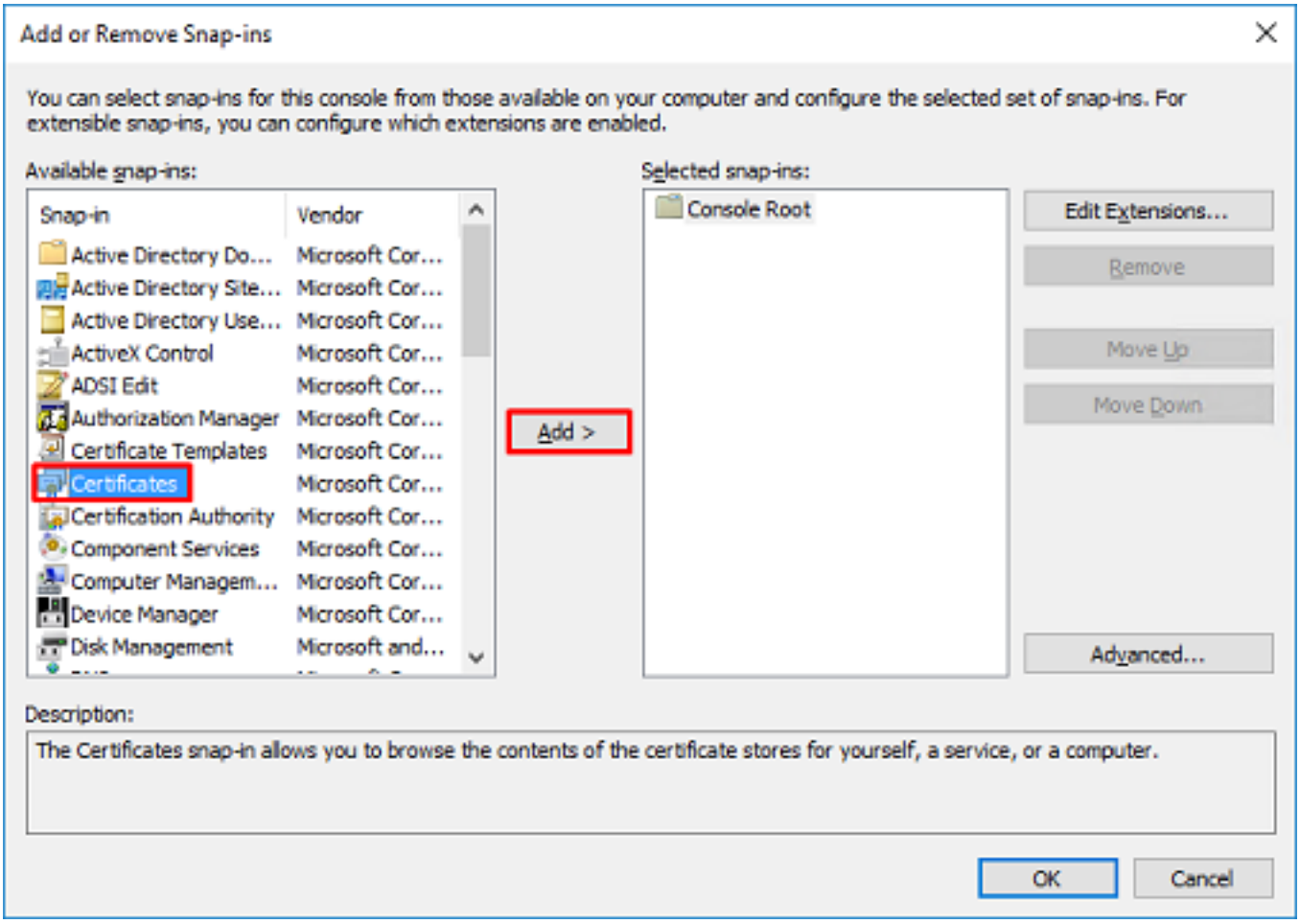
1. Pressione **Win+R** e digite **mc.exe**. Click **OK**.



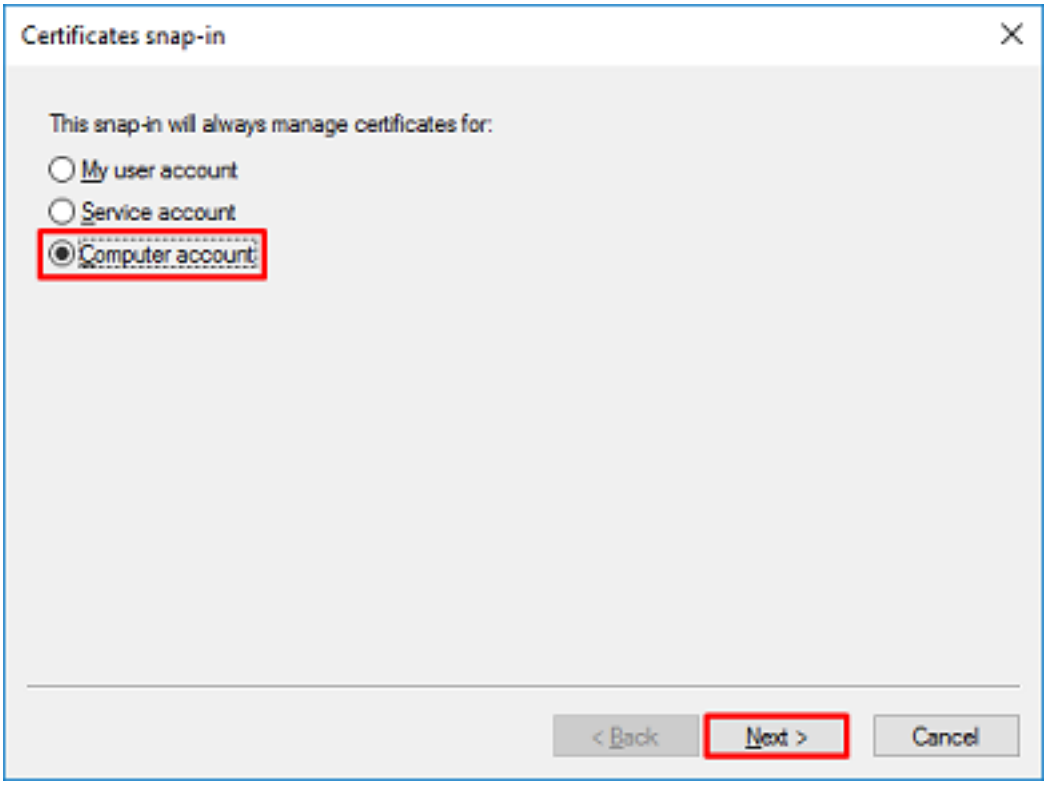
2. Navegue até **Arquivo > Adicionar/remover snap-in...** conforme mostrado na imagem.



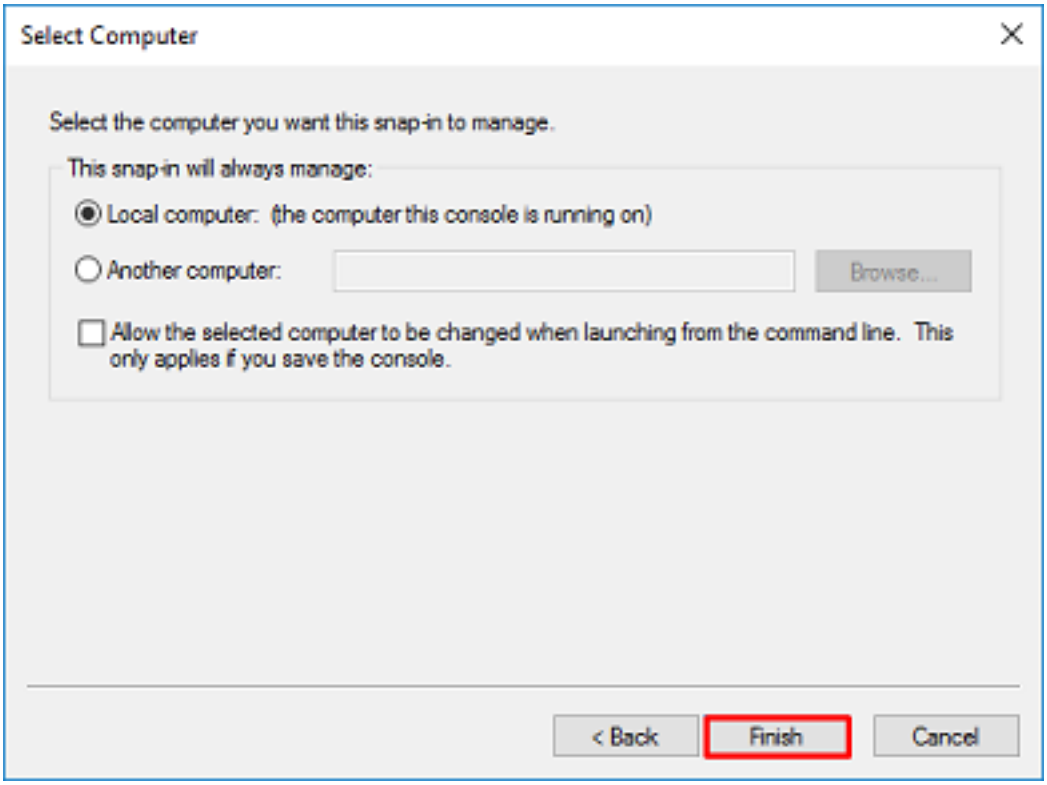
3. Em snap-ins disponíveis, clique em **Certificados** e, em seguida, clique em **Adicionar**.



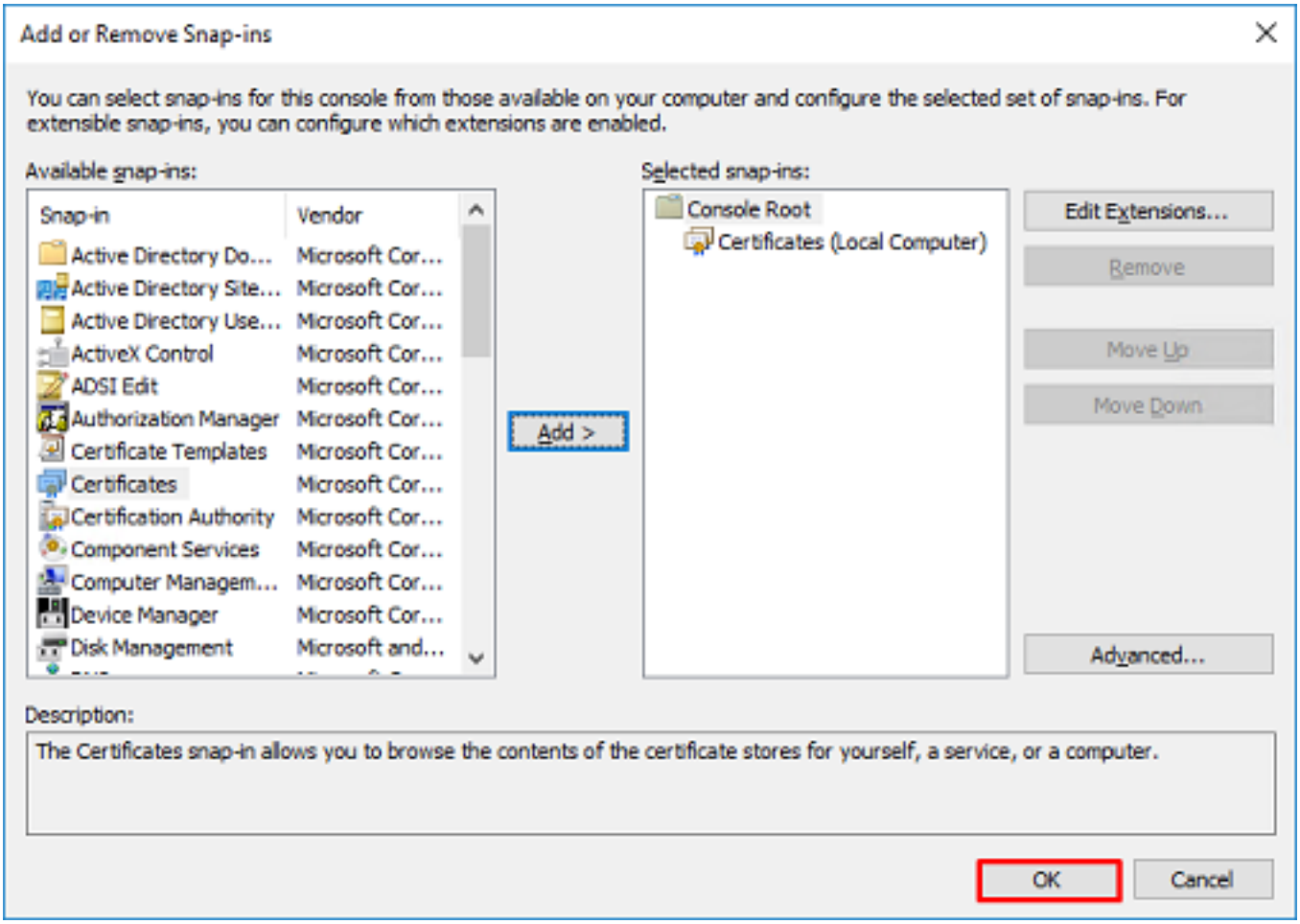
4. Selecione **Conta do computador** e clique em **Avançar** conforme mostrado na imagem.



Clique em Finish.



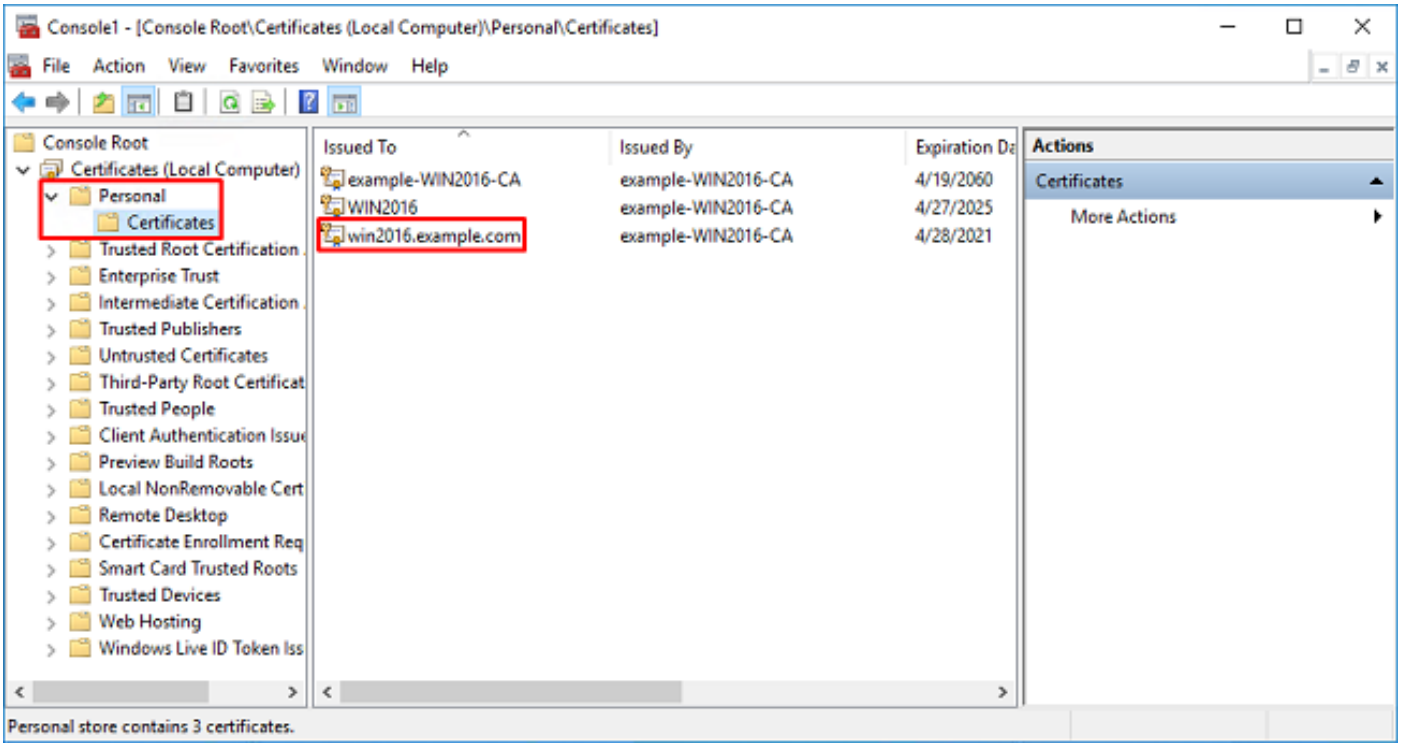
5. Click **OK**.



6. Expanda a pasta **Pessoal** e clique em **Certificados**. O certificado usado pelo LDAPS deve ser emitido para o Nome de domínio totalmente qualificado (FQDN) do servidor Windows. Neste servidor, há 3 certificados listados.

- Um certificado CA emitido para e por exemplo - WIN2016-CA.
- Um certificado de identidade emitido para WIN2016 por exemplo-WIN2016-CA.
- Um certificado de identidade emitido para win2016.example.com por example-WIN2016-CA.

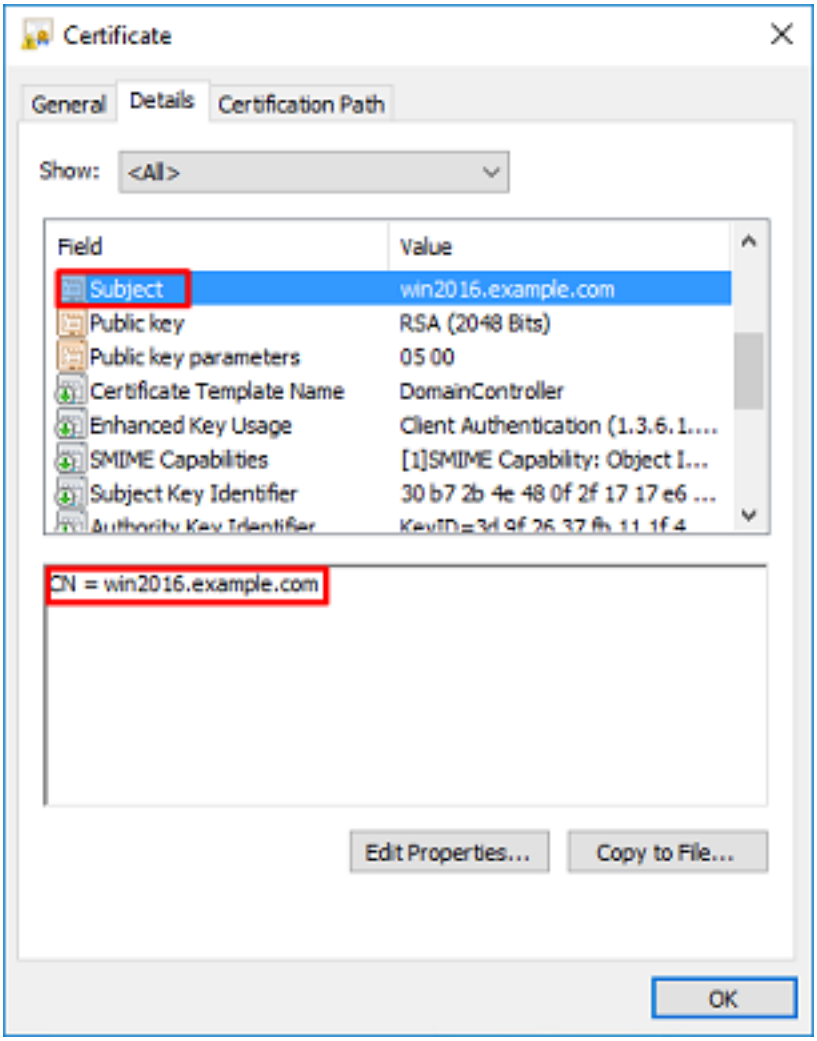
Neste guia de configuração, o FQDN é win2016.example.com e, portanto, os dois primeiros certificados não são válidos para uso como o certificado SSL LDAPS. O certificado de identidade emitido para win2016.example.com é um certificado emitido automaticamente pelo serviço de AC do Windows Server. Clique duas vezes no certificado para verificar os detalhes.

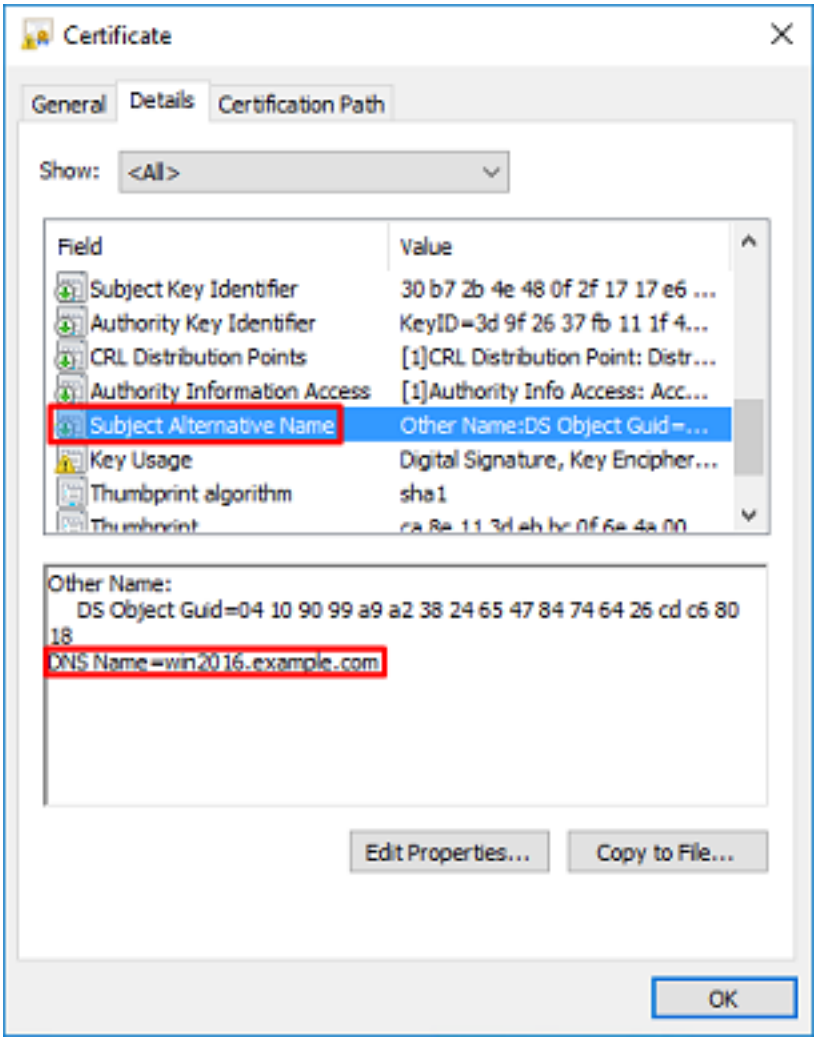


7. Para ser usado como o certificado SSL LDAPS, o certificado deve atender aos seguintes requisitos:

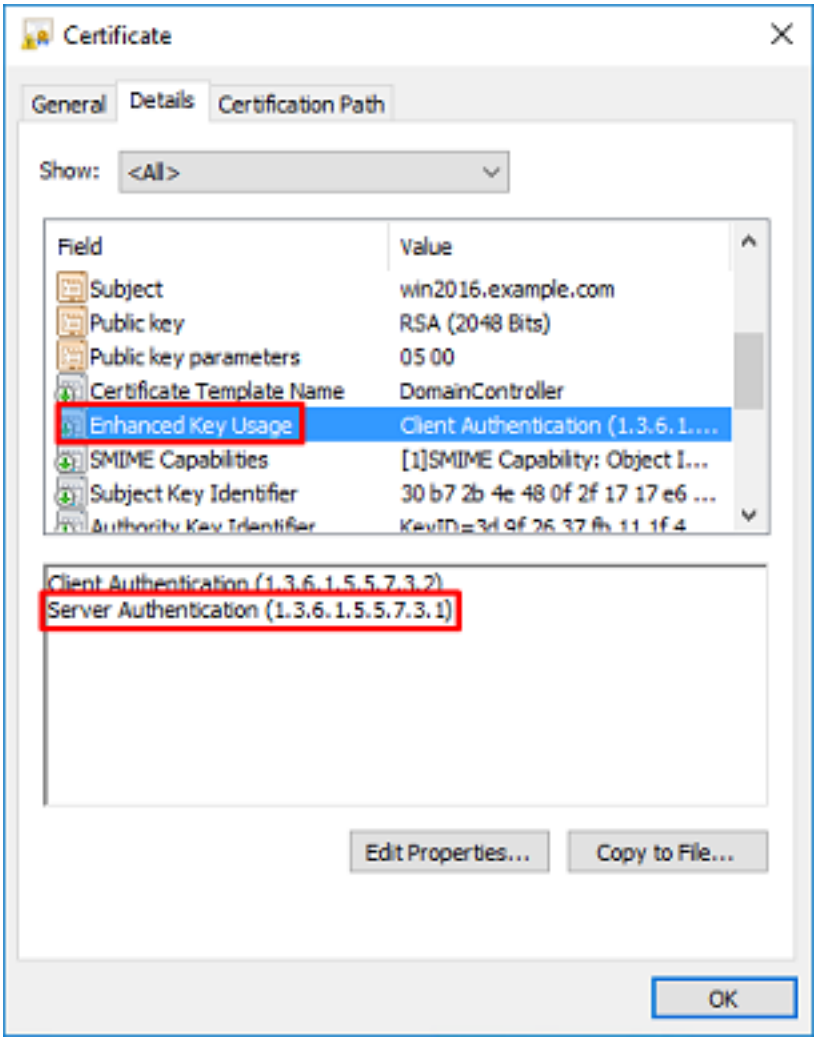
- O nome comum ou o nome alternativo do assunto DNS corresponde ao FQDN do Windows Server.
- O certificado tem a autenticação do servidor no campo Enhanced Key Usage.

Na guia Detalhes do certificado, em **Subject** and **Subject Alternative Name**, o FQDN **win2016.example.com** está presente.

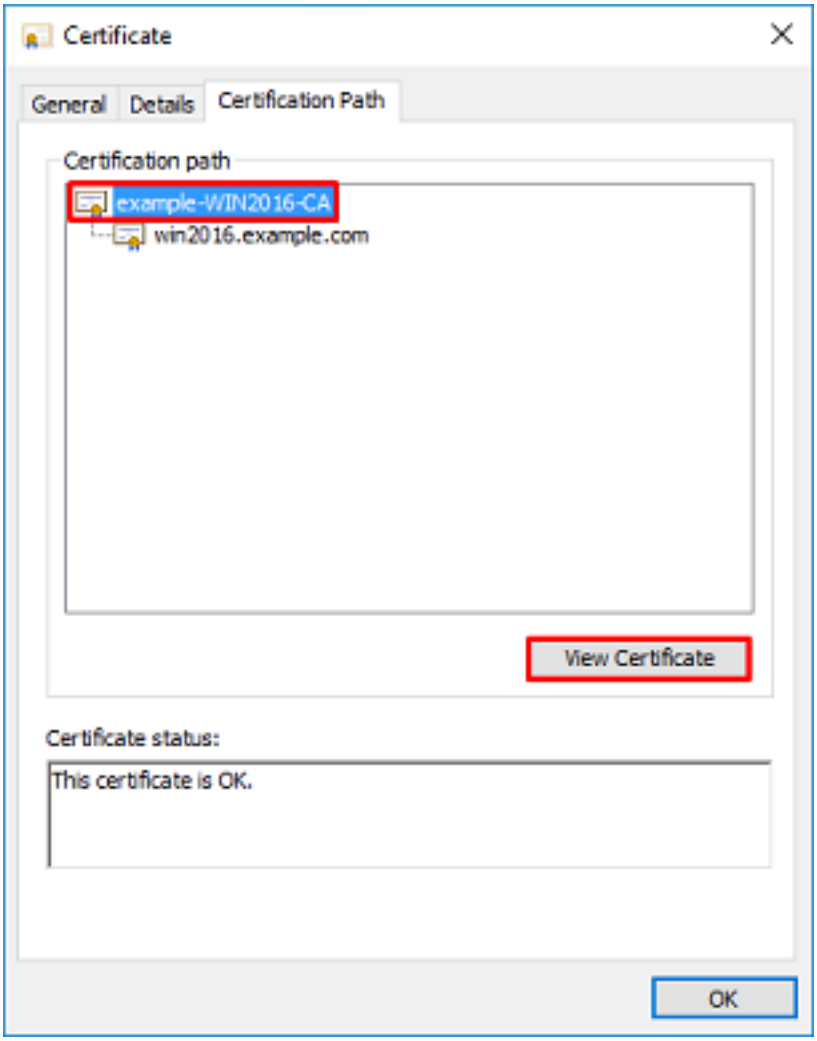

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
win2016.example.com
Public key
RSA (2048 Bits)
Public key parameters
05 00
Certificate Template Name
DomainController
Enhanced Key Usage
Client Authentication (1.3.6.1....
SMIME Capabilities
[1]SMIME Capability: Object I...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



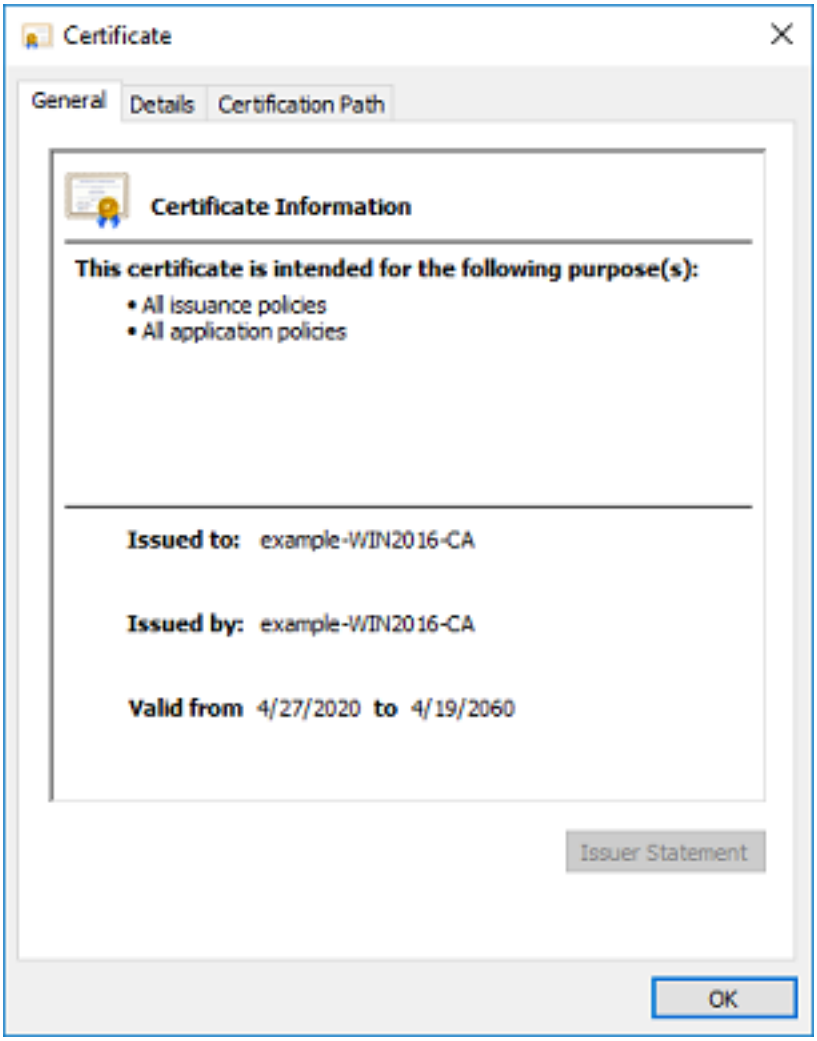
Em **Enhanced Key Usage**, **Server Authentication** está presente.



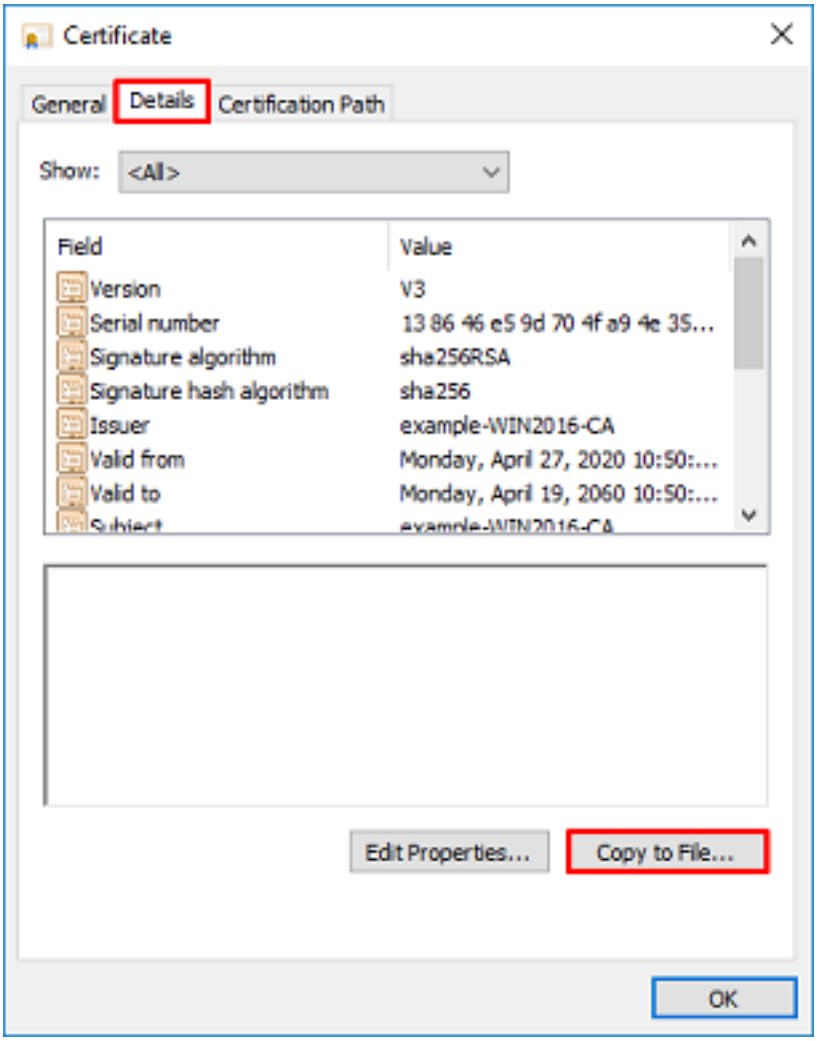
8. Depois que isso for confirmado, navegue até a guia **Certification Path**. Clique no certificado superior que deve ser o certificado CA raiz e clique no botão **Exibir certificado**.



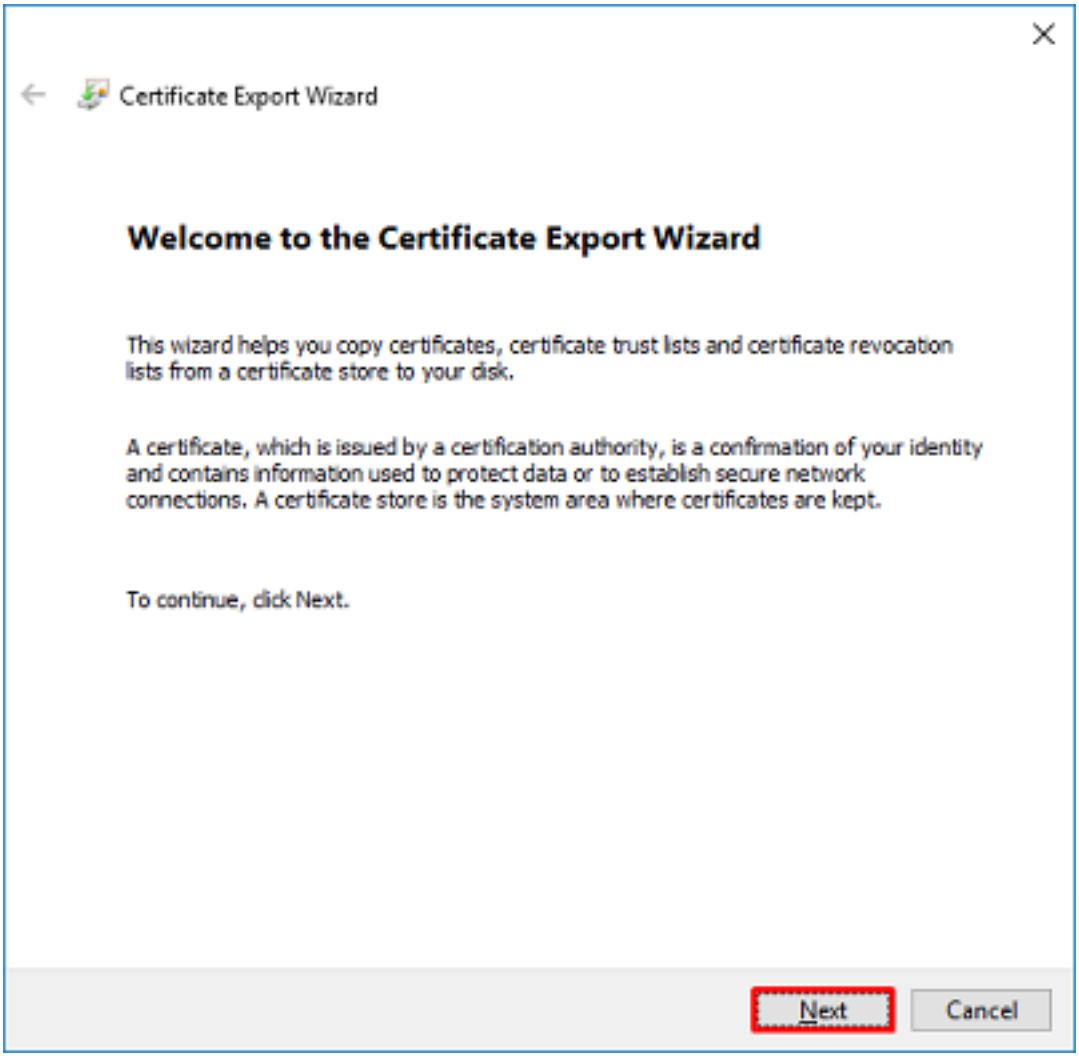
9. Isso abrirá os detalhes do certificado para o certificado CA raiz.



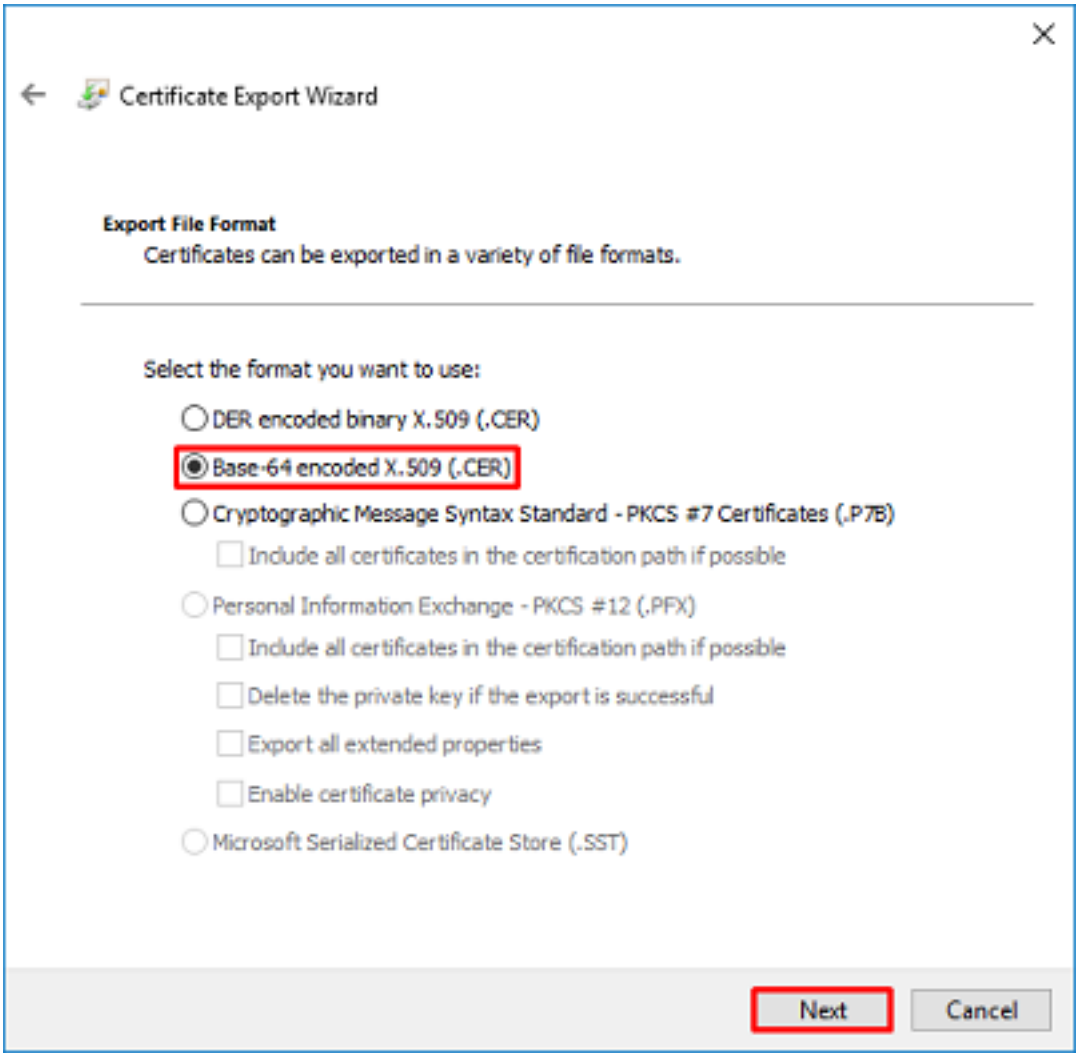
10. Abra a guia **Detalhes** e clique em **Copiar para arquivo...** conforme mostrado na imagem.



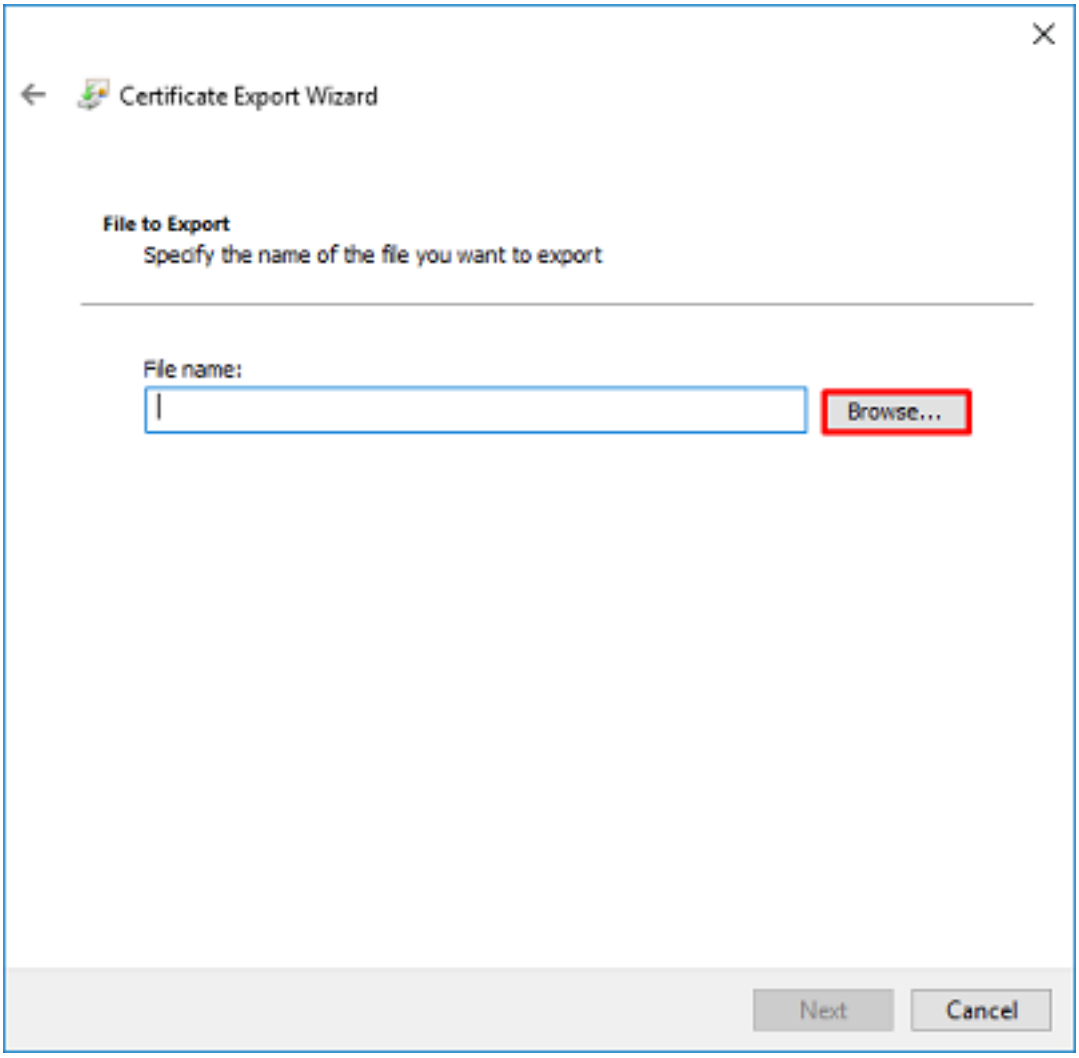
11. Navegue pelo Assistente de exportação de certificado que exportará a CA raiz no formato PEM.

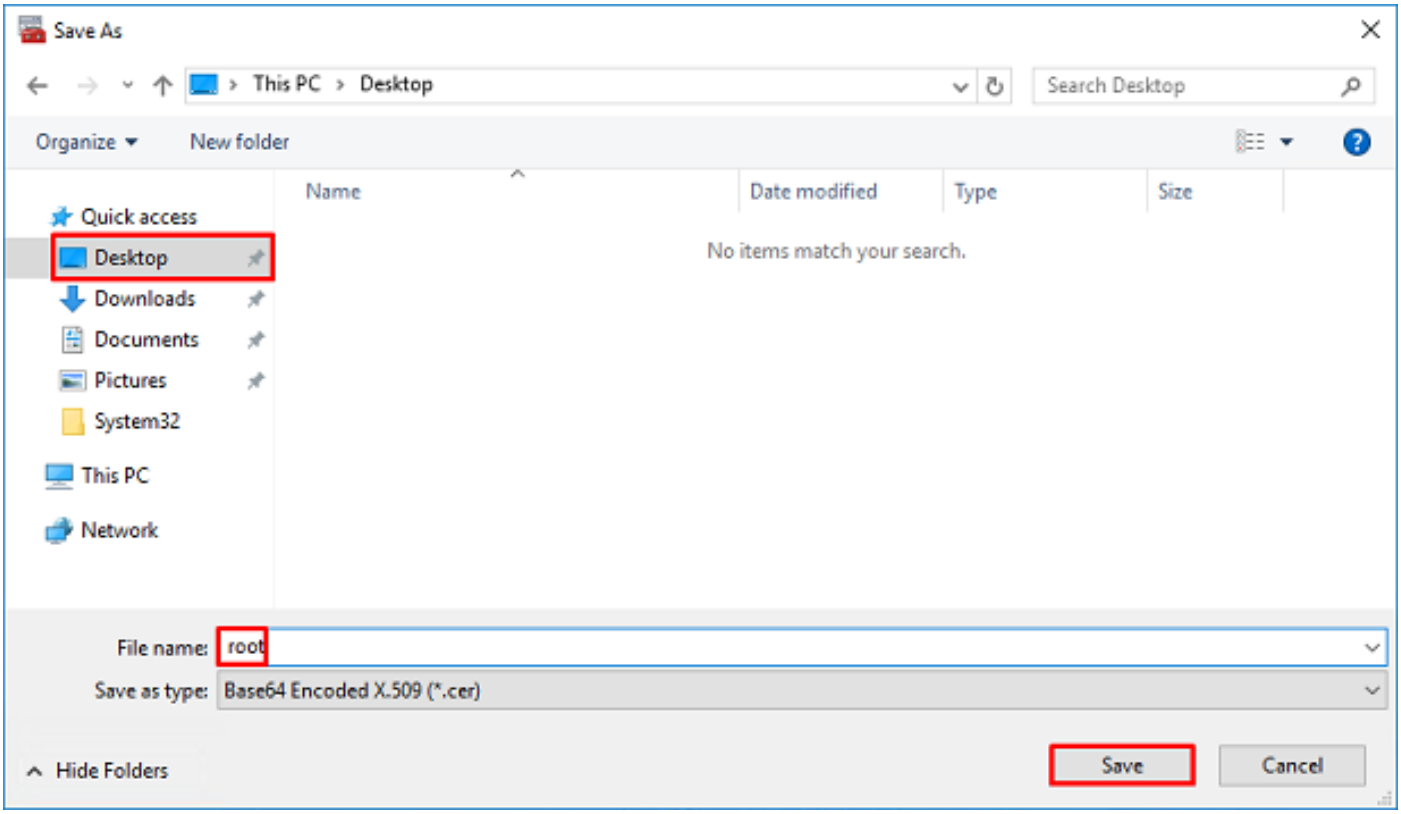


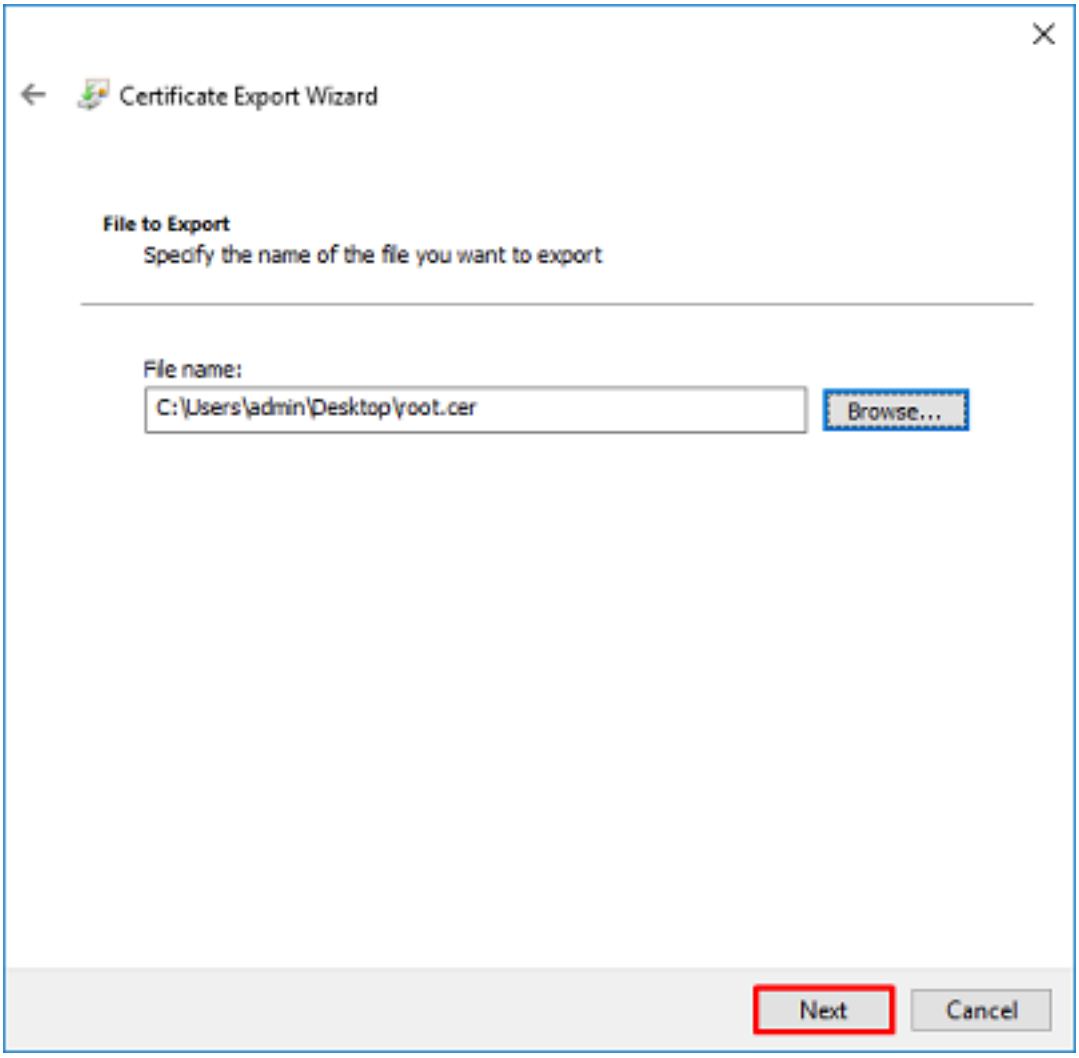
12. Selecione **X.509 codificado em Base 64**.



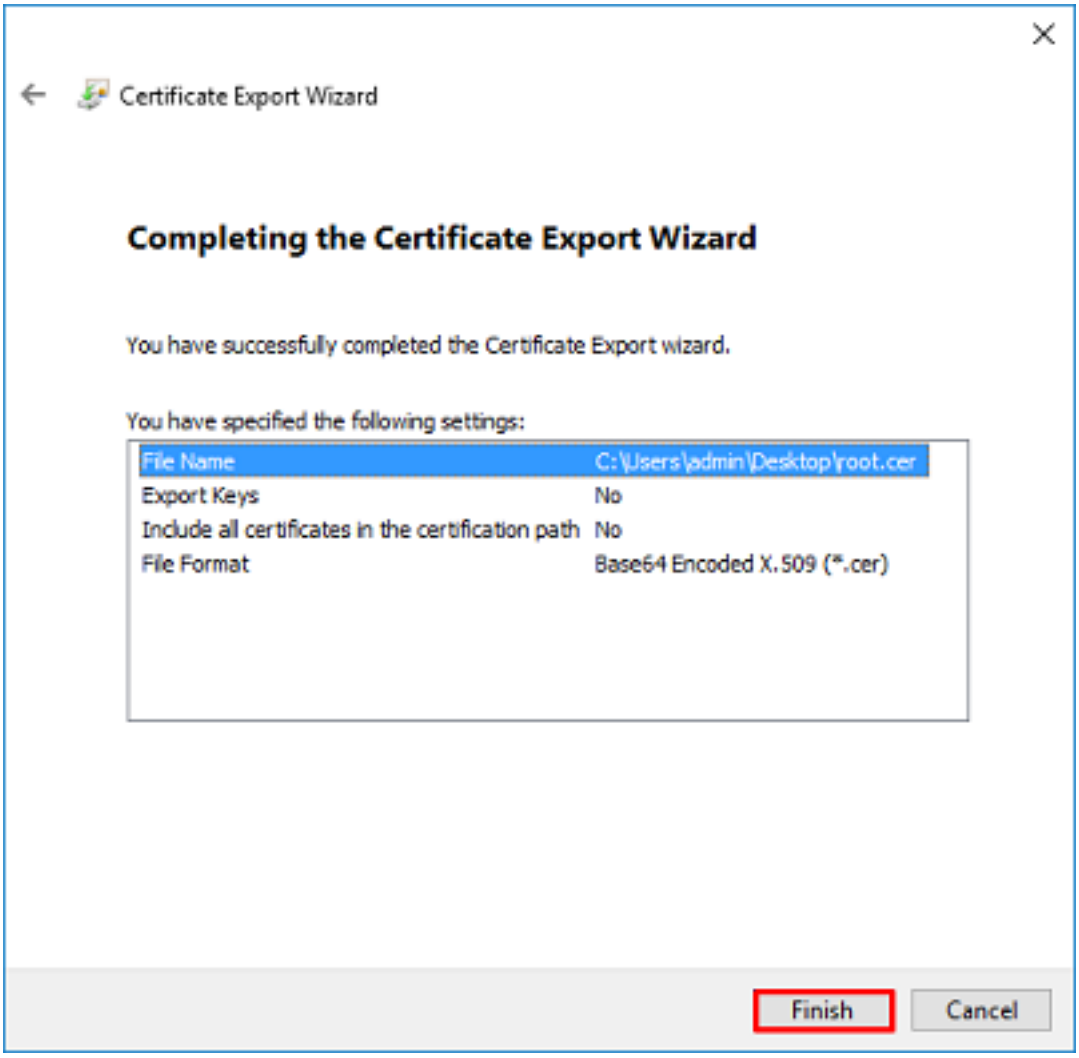
13. Selecione o nome do arquivo e para onde ele será exportado.


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. Clique em Finish.



15. Agora, navegue até o local e abra o certificado com um bloco de notas ou algum outro editor de texto. Isso exibirá o certificado de formato PEM. Guarde isto para mais tarde.

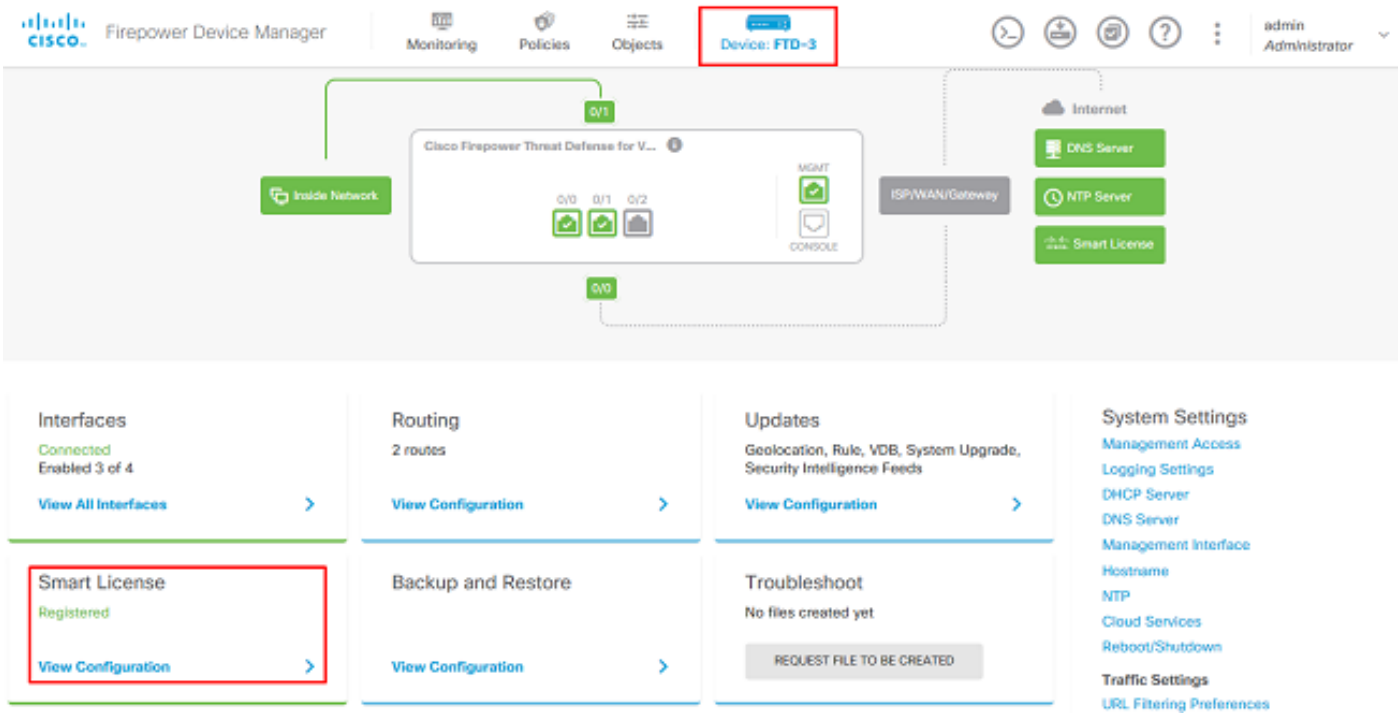
```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
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-----
```

Configurações de FDM

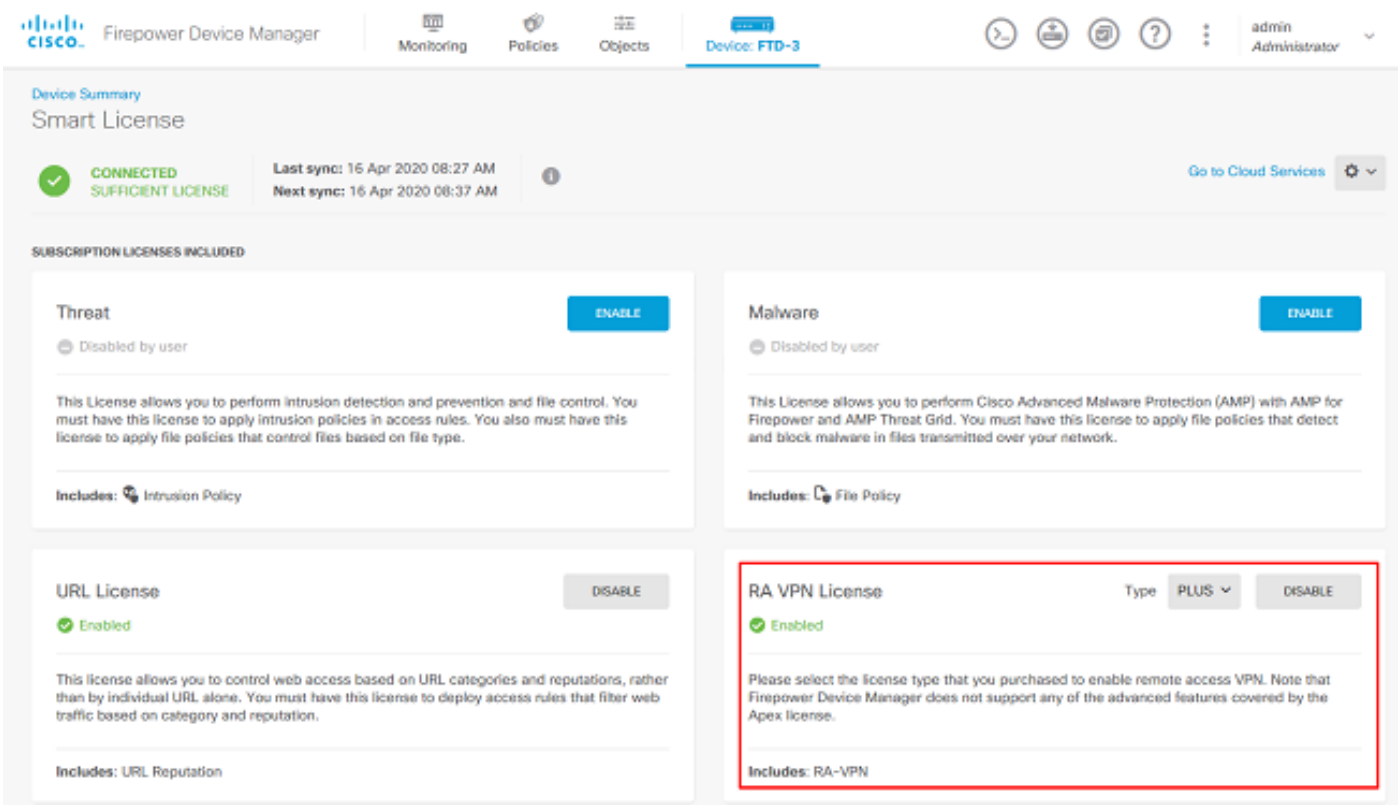
Verificar o licenciamento

Para configurar o AnyConnect no FDM, o FTD precisará ser registrado no servidor de licenciamento inteligente e uma licença Plus, Apex ou VPN Only válida deverá ser aplicada ao dispositivo.

1. Navegue até **Device > Smart License** conforme mostrado na imagem.

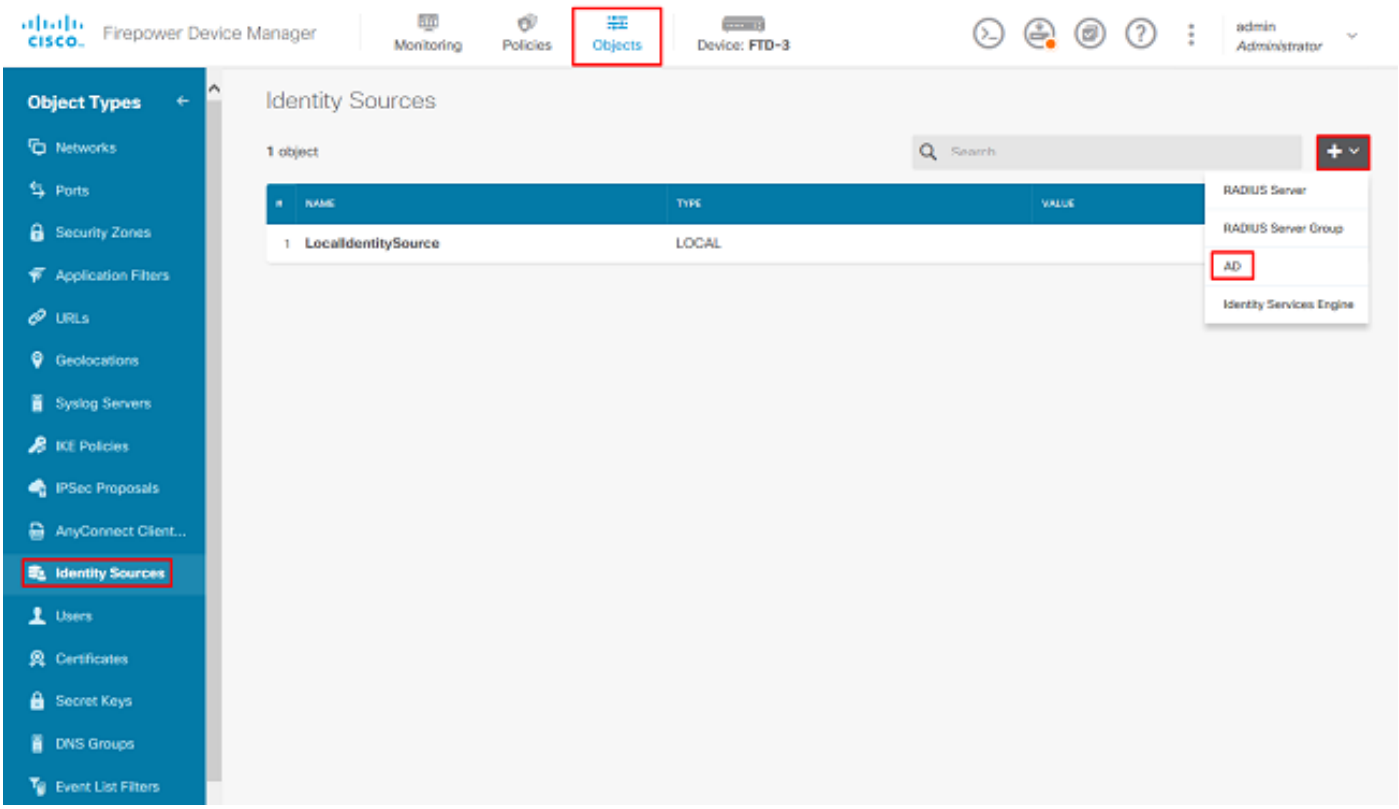


2. Verifique se o FTD está registrado no servidor de licenciamento inteligente e se a licença AnyConnect Plux, Apex ou VPN Only está habilitada.

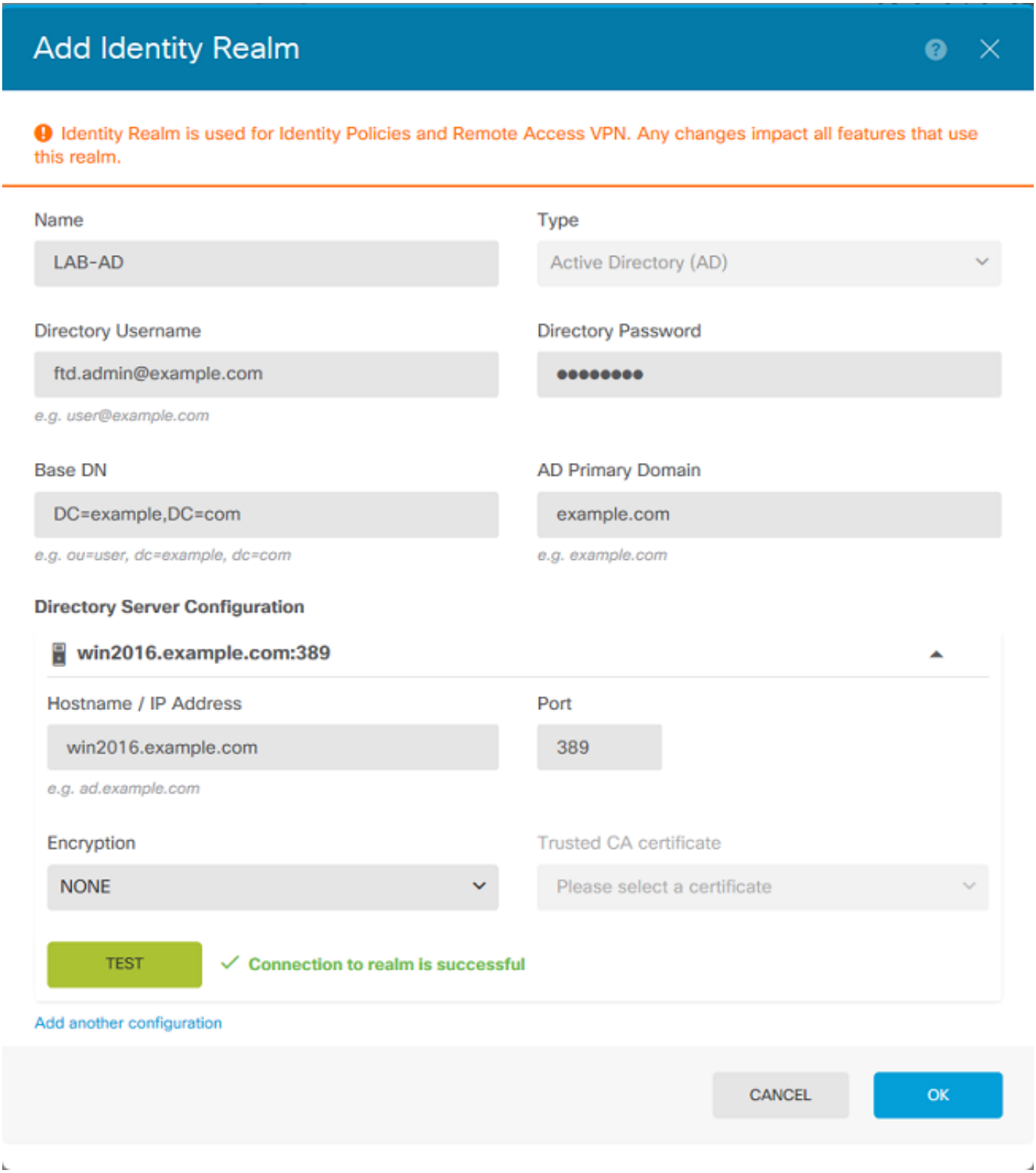


Configurar fonte de identidade do AD

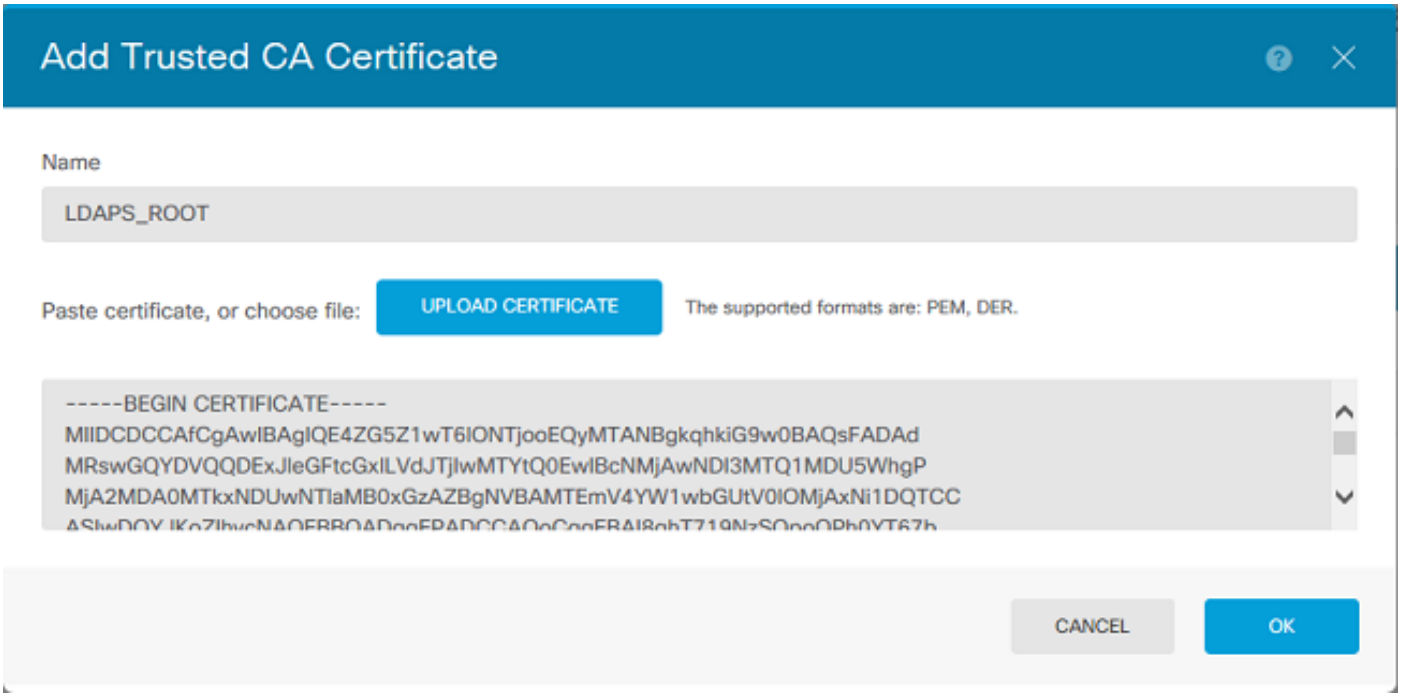
1. Navegue até **Objetos > Fontes de identidade**, clique no **+** símbolo e selecione **AD** como mostrado na imagem.

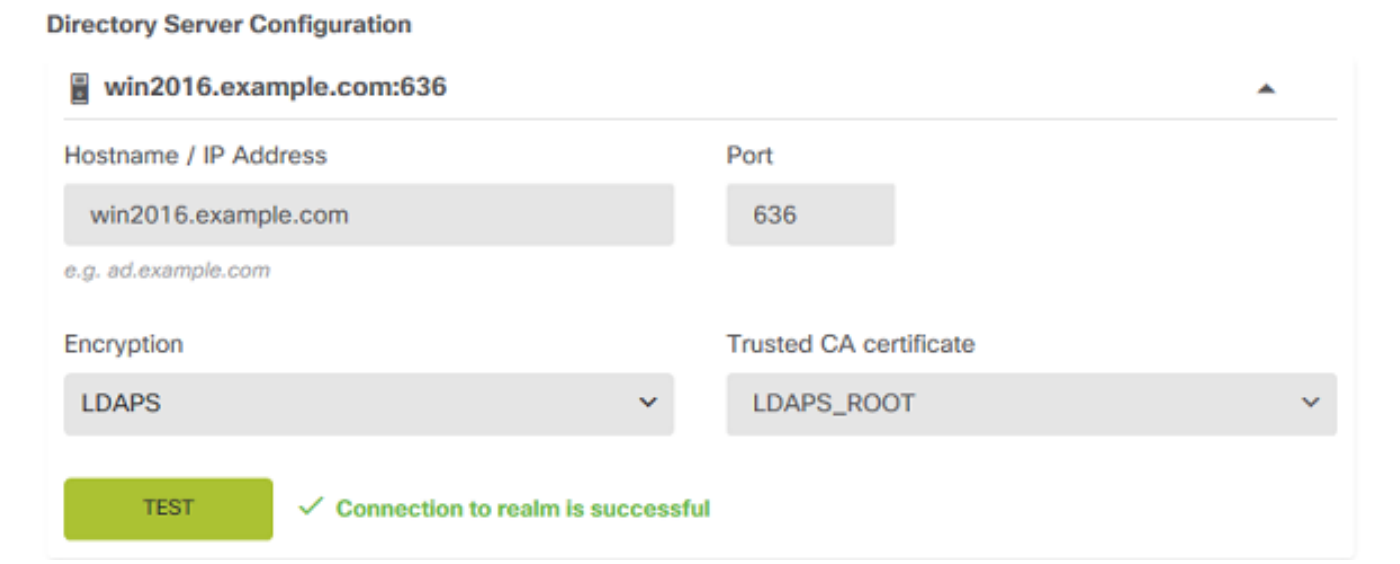


2. Preencha as configurações apropriadas para o servidor do Ative Diretory com as informações coletadas anteriormente. Se um nome de host (FQDN) for usado para o servidor Microsoft em vez de um endereço IP, certifique-se de criar um grupo DNS apropriado em **Objetos > Grupo DNS**. Em seguida, aplique esse grupo DNS ao FTD navegando para **Device > System Settings > DNS Server**, aplicando o grupo DNS na **Management Interface** e **Data Interface**, e então especifique a interface de saída apropriada para consultas DNS. Clique no botão **Test** para verificar uma configuração bem-sucedida e a acessibilidade na interface de gerenciamento do FTD. Como esses testes são iniciados a partir da interface de gerenciamento do FTD e não através de uma das interfaces roteáveis configuradas no FTD (como interno, externo, dmz), uma conexão bem-sucedida (ou com falha) não garante o mesmo resultado para a autenticação do AnyConnect, pois as solicitações de autenticação LDAP do AnyConnect serão iniciadas a partir de uma das interfaces roteáveis do FTD. Para obter mais informações sobre como testar conexões LDAP do FTD, consulte as seções Testar AAA e Captura de Pacotes na área Solução de Problemas.



Se LDAPS ou STARTTLS for usado, selecione a Criptografia apropriada e selecione o certificado de CA confiável. Se a AC raiz ainda não tiver sido adicionada, clique em **Criar novo certificado CA confiável**. Forneça um nome para o certificado CA raiz e cole o certificado ca raiz do formato PEM coletado anteriormente.

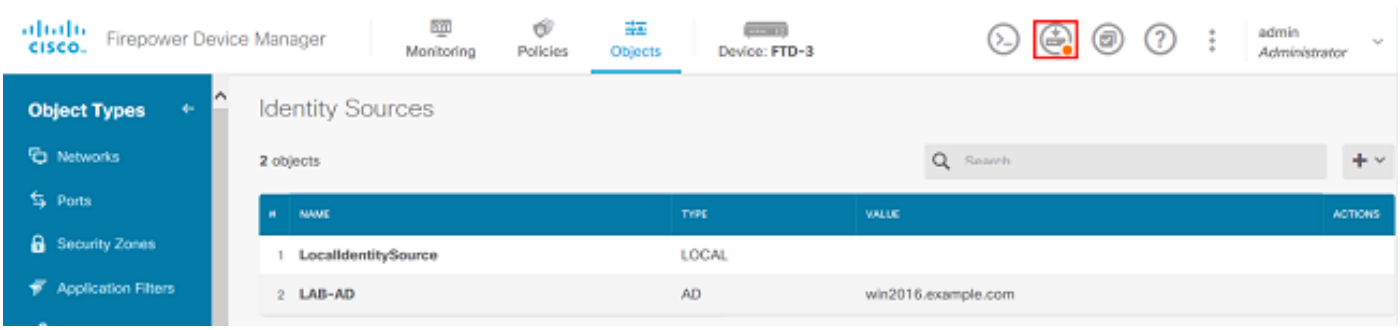




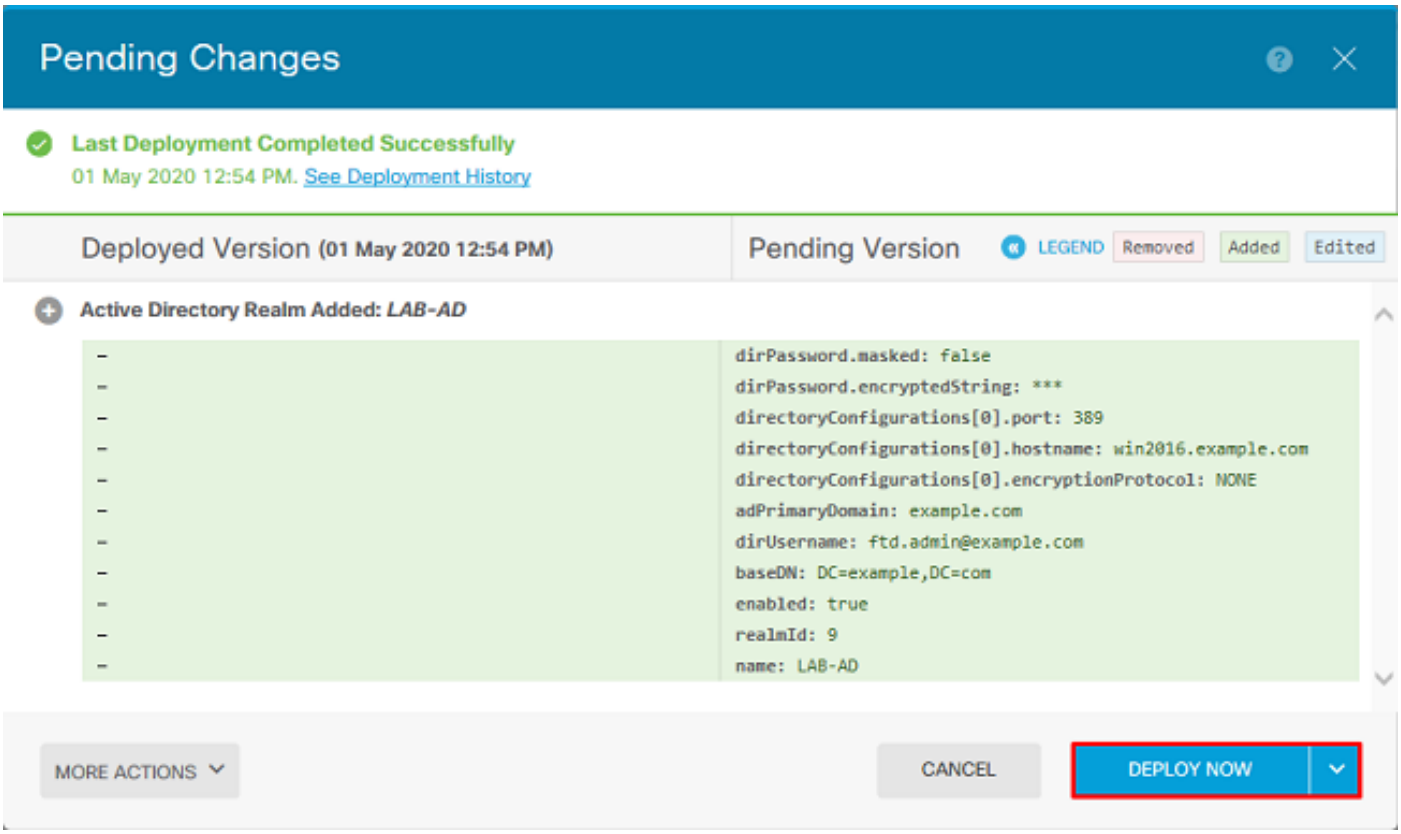
Nesta configuração, esses valores foram usados:

- Nome: LAB-AD
- Nome de usuário do diretório: ftd.admin@example.com
- DN base: DC=exemplo,DC=com
- Domínio principal do AD: example.com
- Nome do host/Endereço IP: win2016.example.com
- Porta: 389

3. Clique no botão **Alterações pendentes** na parte superior direita, como mostrado na imagem.



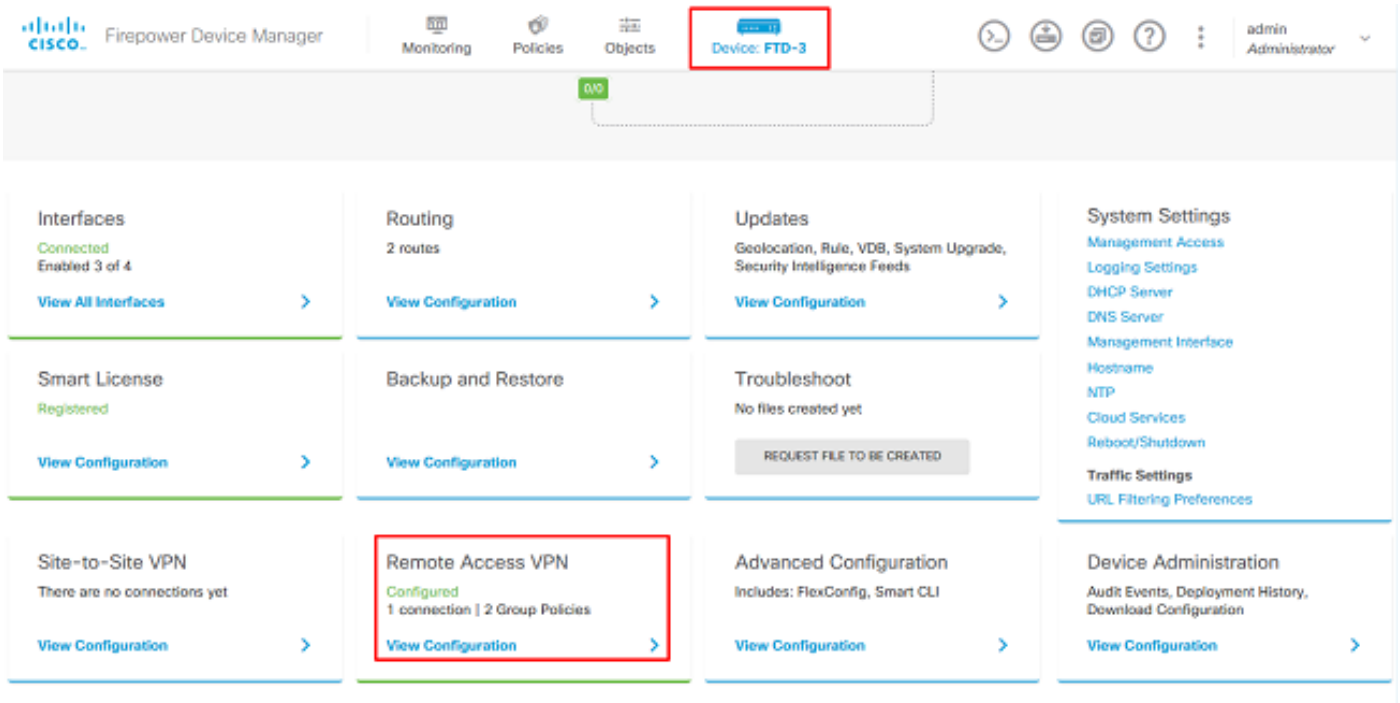
4. Clique no botão **Implantar agora**.



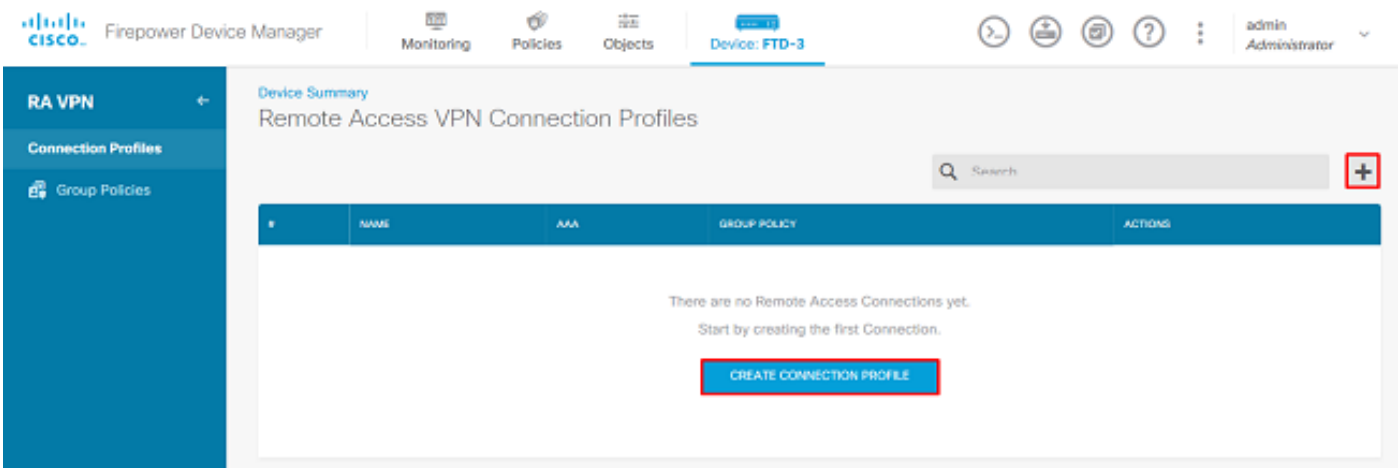
Configurar o AnyConnect para autenticação do AD

Para usar a fonte de identidade do AD configurada, ela precisará ser aplicada à configuração do AnyConnect.

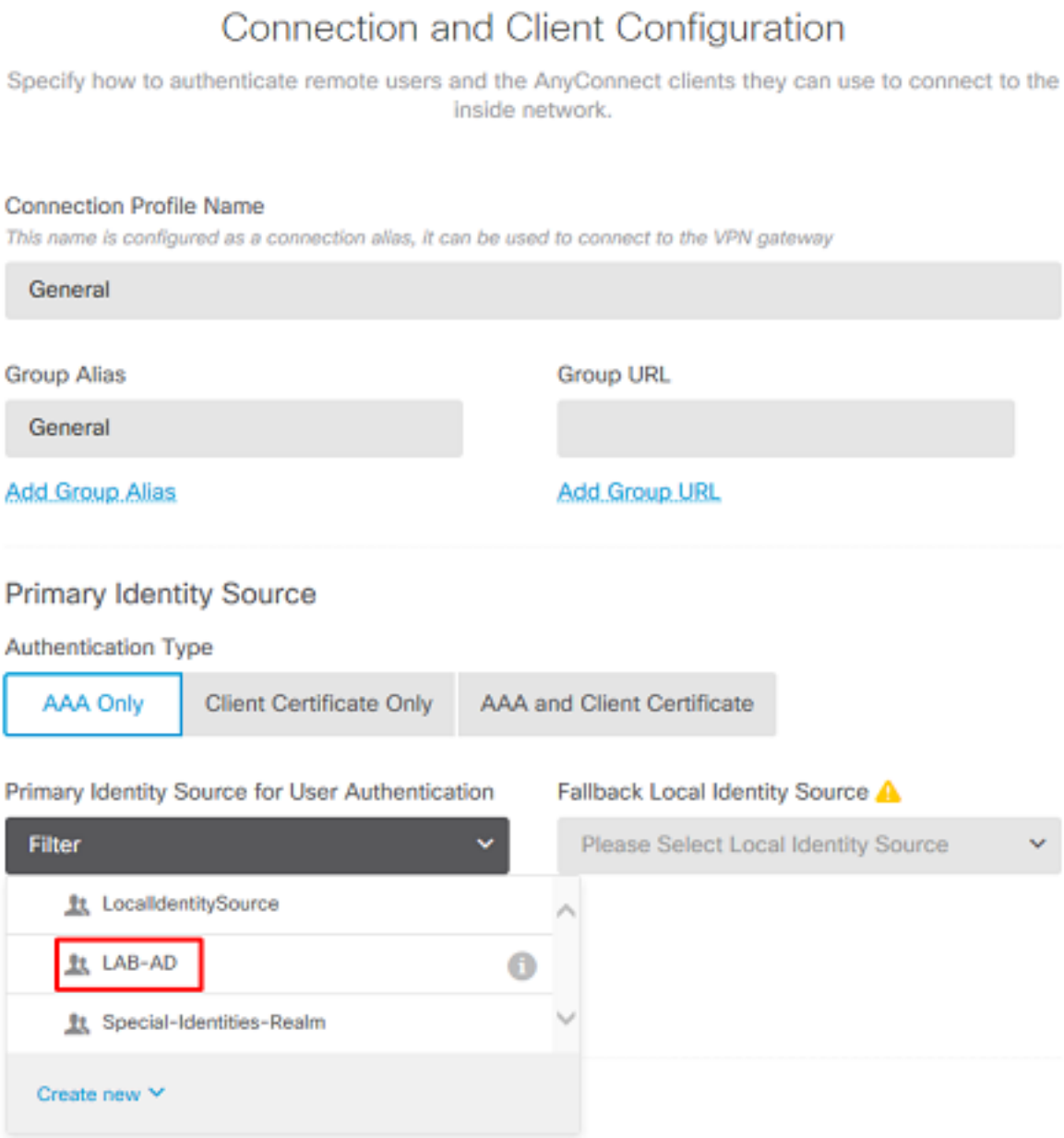
1. Navegue até **Device > Remote Access VPN (Dispositivo > VPN de acesso remoto)** conforme mostrado na imagem.

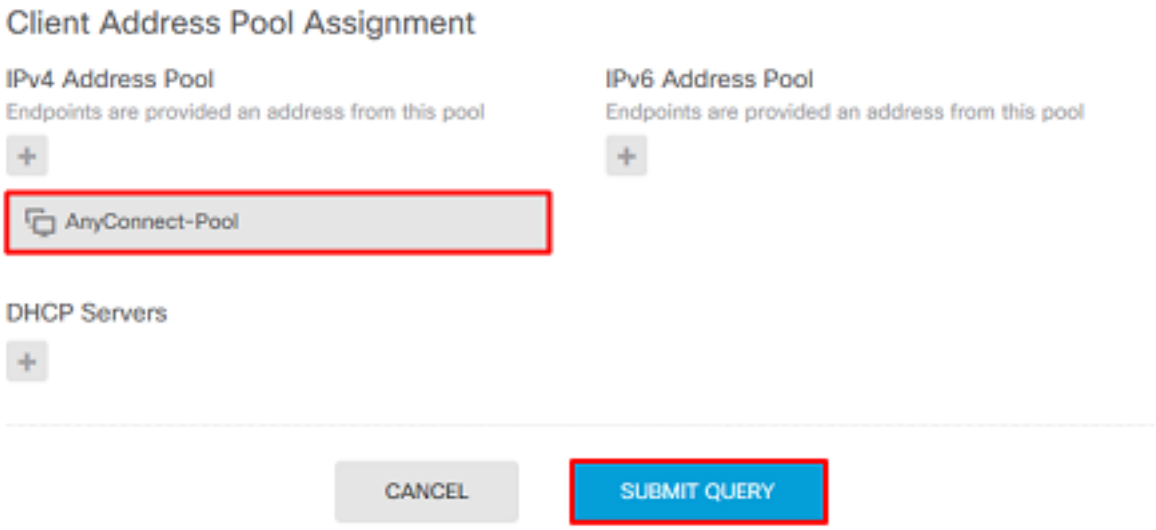


2. Clique no **+** símbolo ou no botão **Criar perfil de conexão**, como mostrado na imagem.

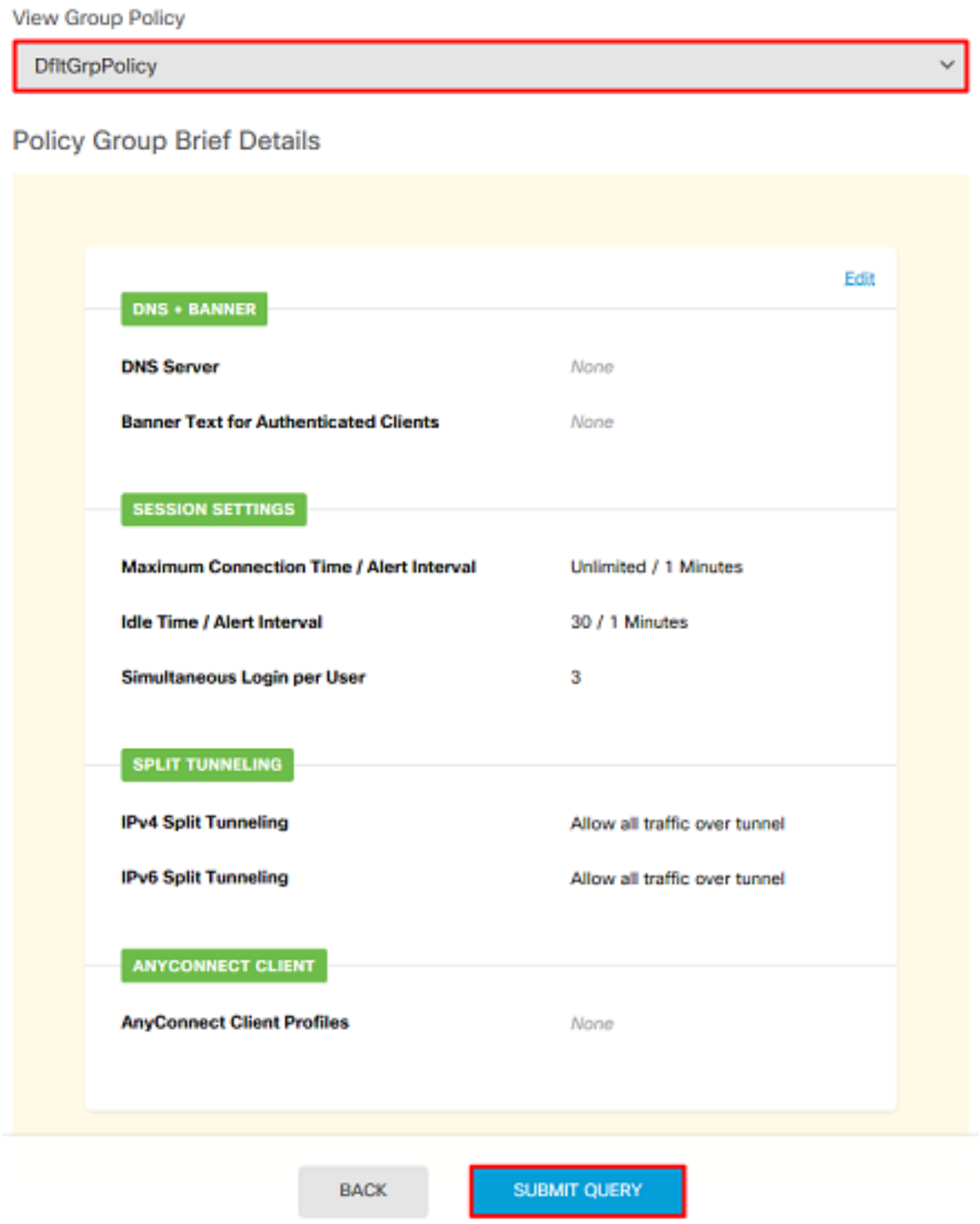


3. Na seção Conexão e configuração do cliente, selecione a fonte de identidade do AD criada anteriormente. Configure os valores apropriados para as outras seções, incluindo o Nome do perfil de conexão e a Atribuição do pool de endereços do cliente. Clique em **Enviar consulta** quando terminar.

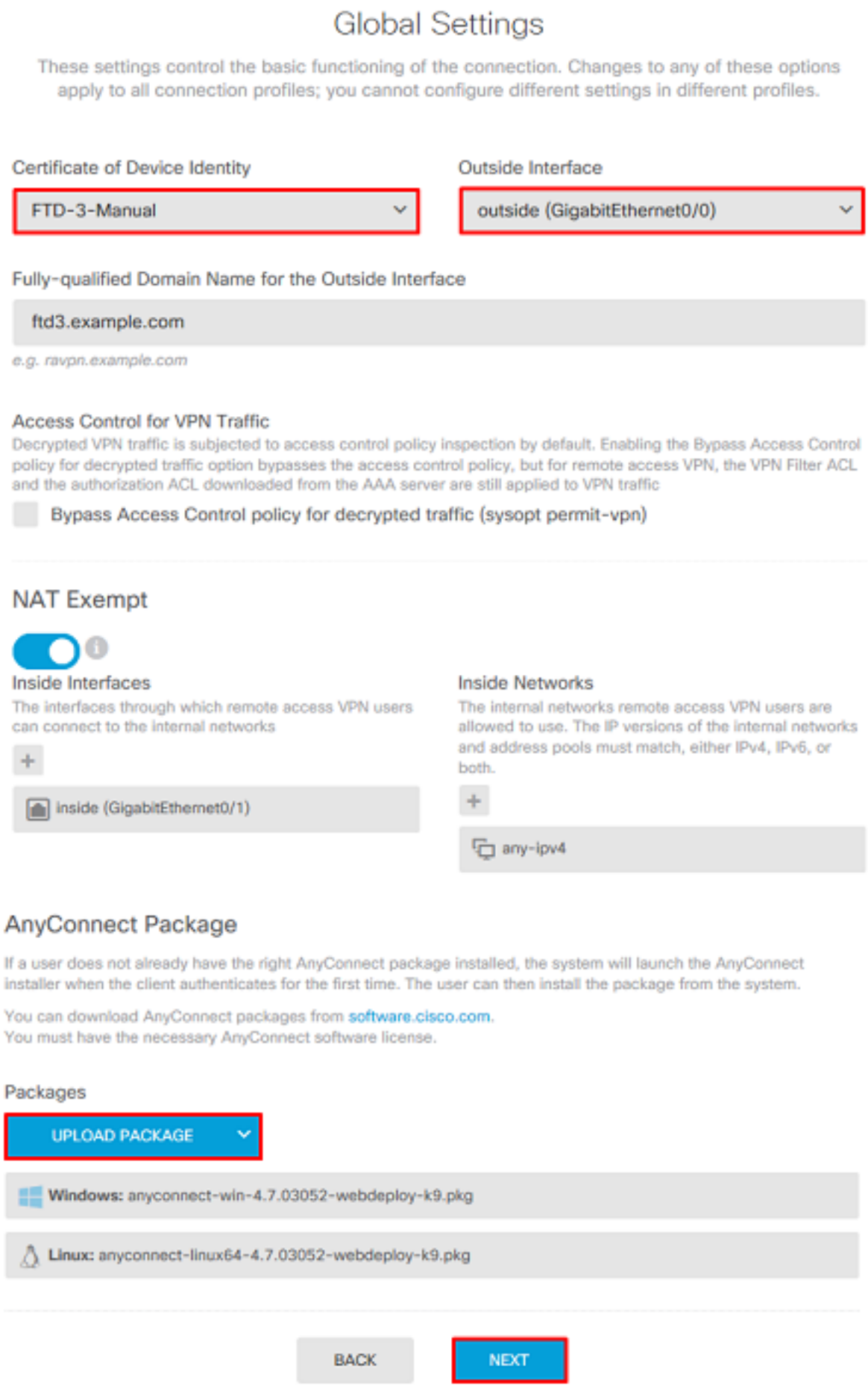




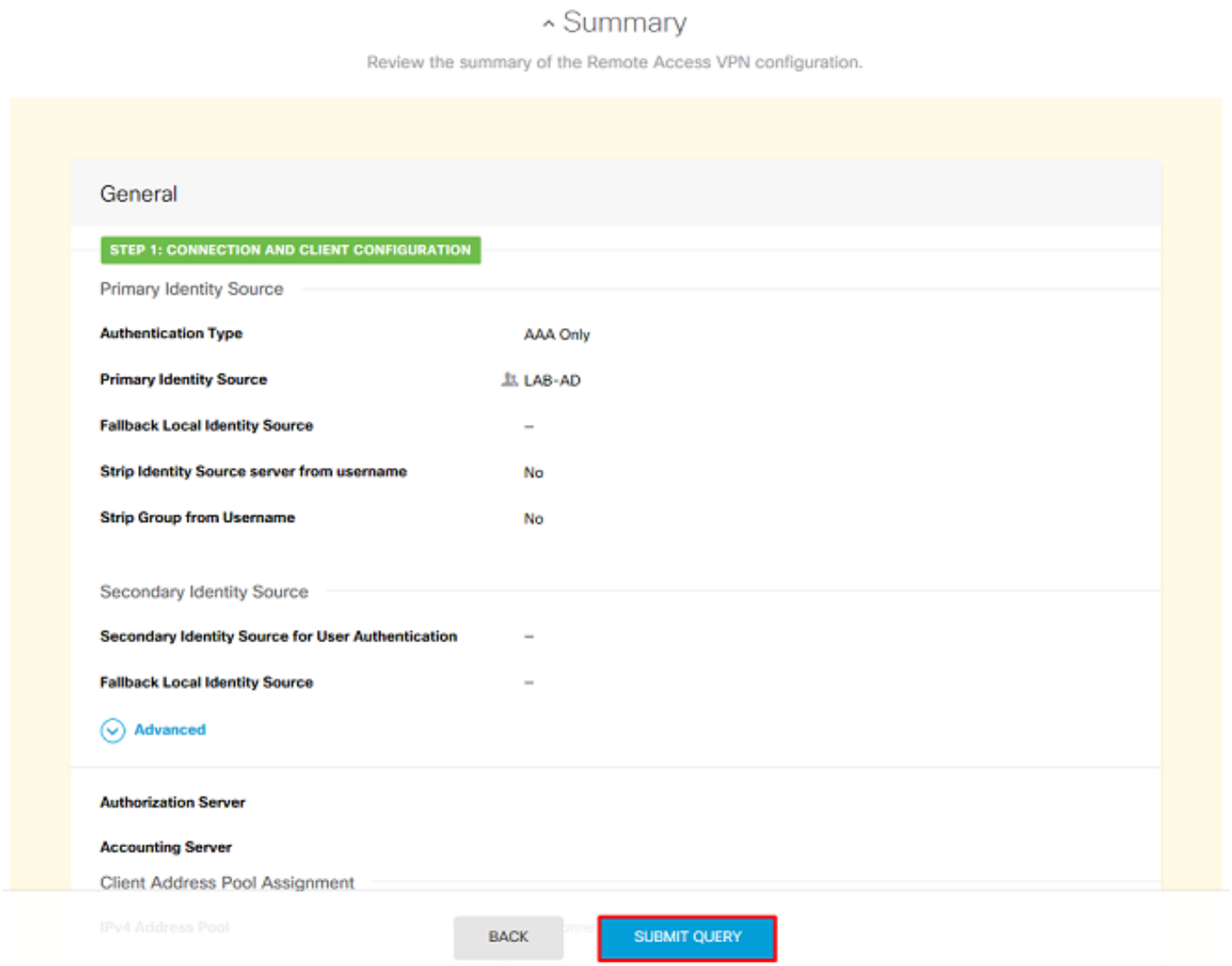
4. Na seção Experiência do usuário remoto, selecione a política de grupo apropriada. Por padrão, a **DfltGrpPolicy** será usada; no entanto, é possível criar um outro.



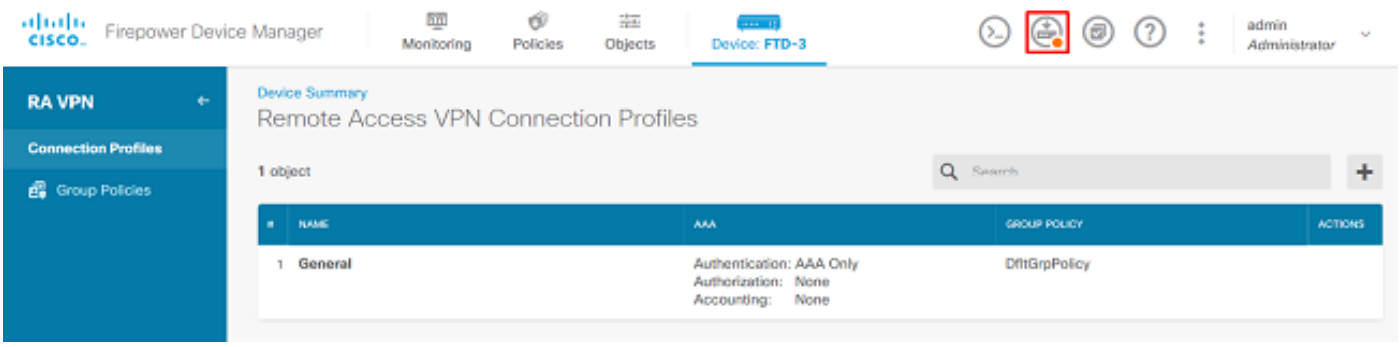
5. Na seção Configurações globais, no mínimo, especifique os pacotes Certificado SSL, Interface externa e AnyConnect. Se um certificado não tiver sido criado anteriormente, um certificado autoassinado padrão (DefaultInternalCertificate) pode ser selecionado, mas uma mensagem de certificado de servidor não confiável será exibida. Ignorar política de controle de acesso para tráfego descriptografado (sysopt permit-vpn) deve ser desmarcada para que as regras da política de acesso à identidade do usuário entrem em vigor posteriormente. O NAT isento também pode ser configurado aqui. Nesta configuração, todo o tráfego ipv4 da interface interna indo para os endereços IP do cliente AnyConnect é exceto do NAT. Para configurações mais complexas, como hairpinning externa para externa, serão necessárias regras de NAT adicionais sob a política de NAT. Os pacotes do AnyConnect podem ser encontrados no site de suporte da Cisco: https://software.cisco.com/download/home. É necessária uma licença Plus ou Apex válida para baixar o pacote do AnyConnect.



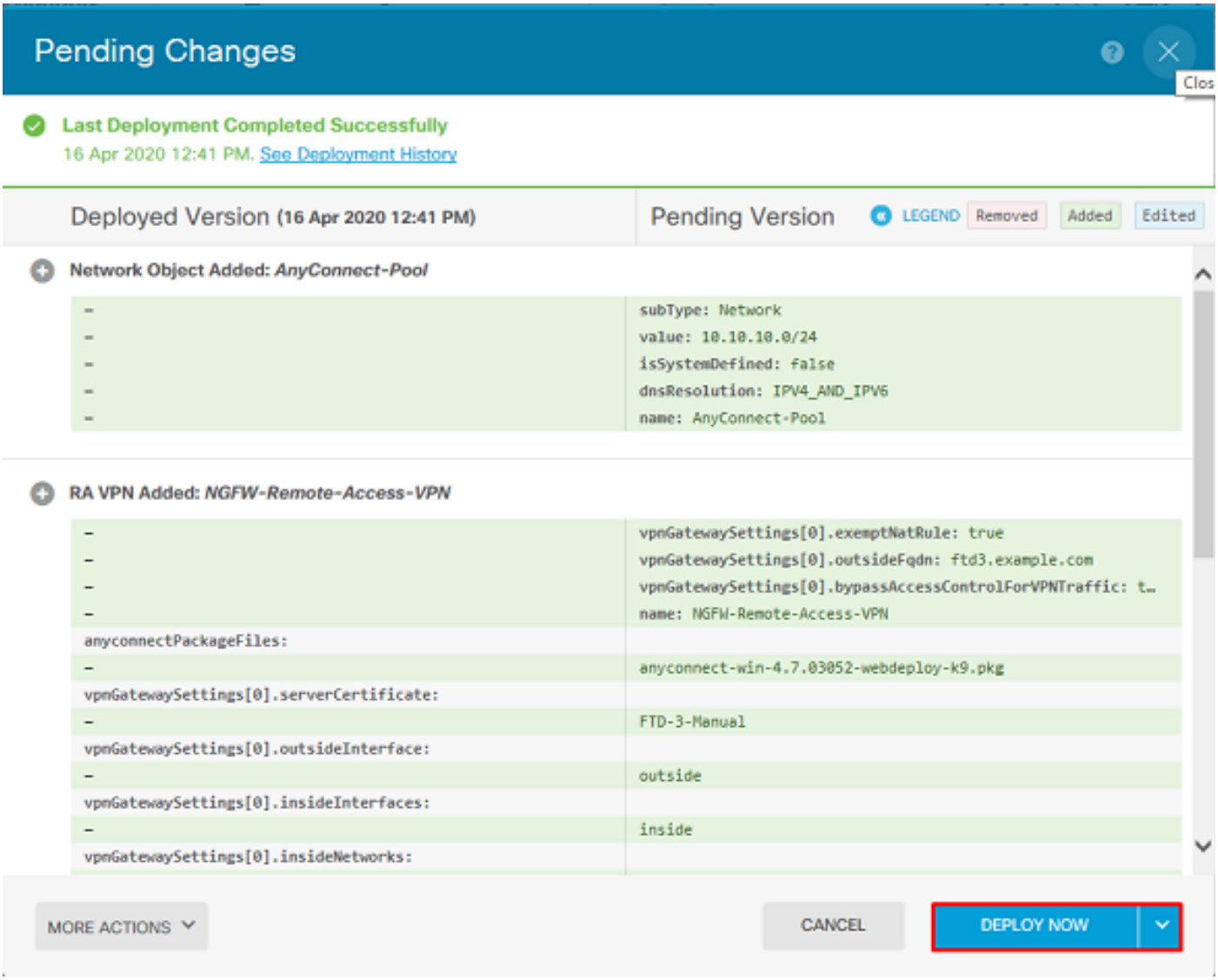
6. Na seção Resumo, verifique se o AnyConnect está configurado corretamente e clique em **Enviar consulta**.



7. Clique no botão **Alterações pendentes** na parte superior direita, como mostrado na imagem.



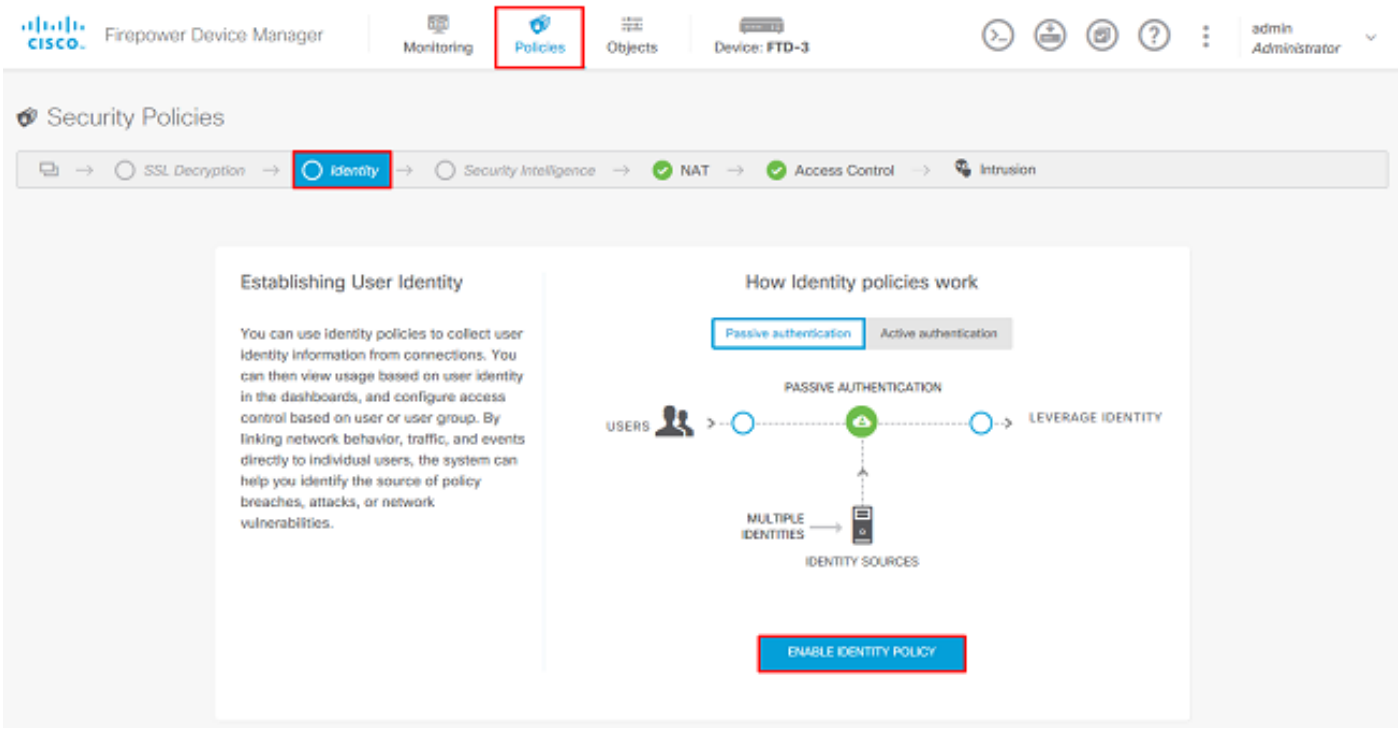
8. Clique em **Implantar agora**.



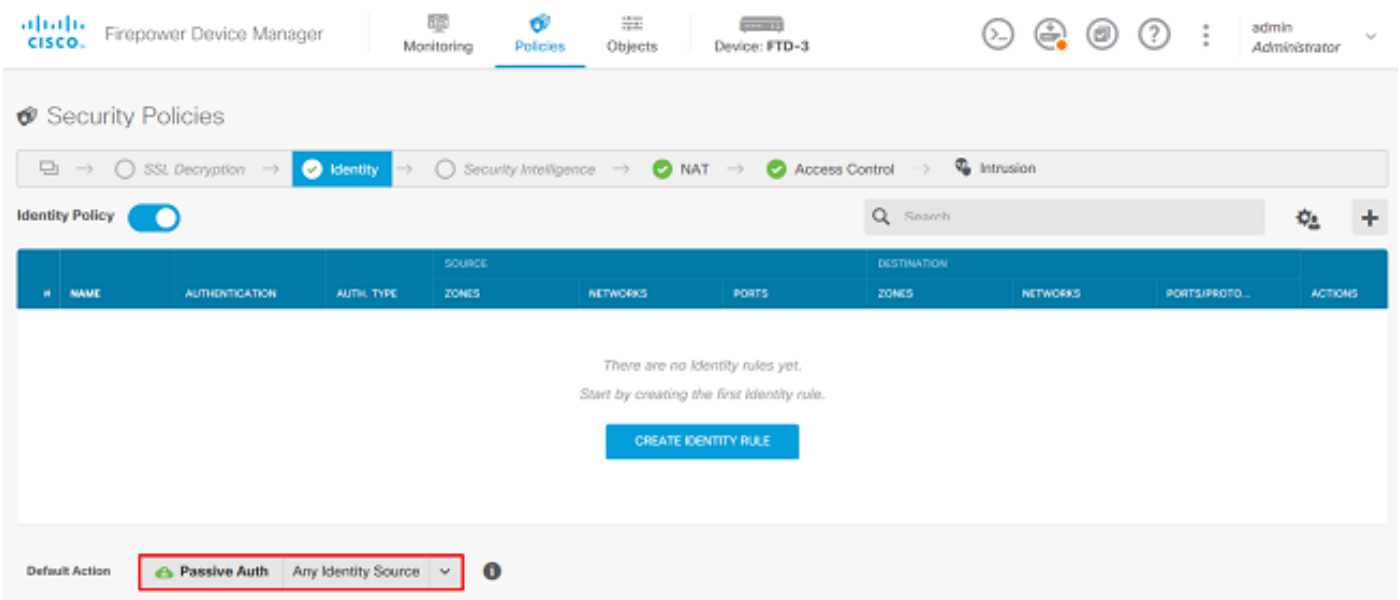
Habilitar política de identidade e configurar políticas de segurança para identidade do usuário

Neste ponto, os usuários do AnyConnect devem ser capazes de se conectar com êxito, mas talvez não possam acessar recursos específicos. Esta etapa ativará a identidade do usuário para que somente os usuários nos administradores do AnyConnect possam se conectar aos recursos internos com o uso do RDP e somente os usuários no grupo Usuários do AnyConnect possam se conectar aos recursos internos com o uso do HTTP.

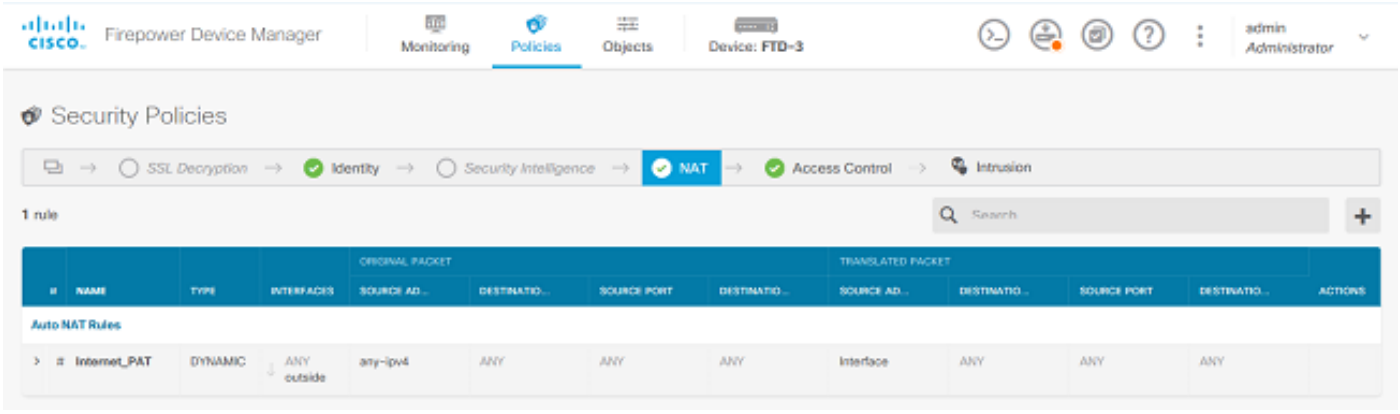
1. Navegue para **Políticas > Identidade** e clique em **Ativar política de identidade**.



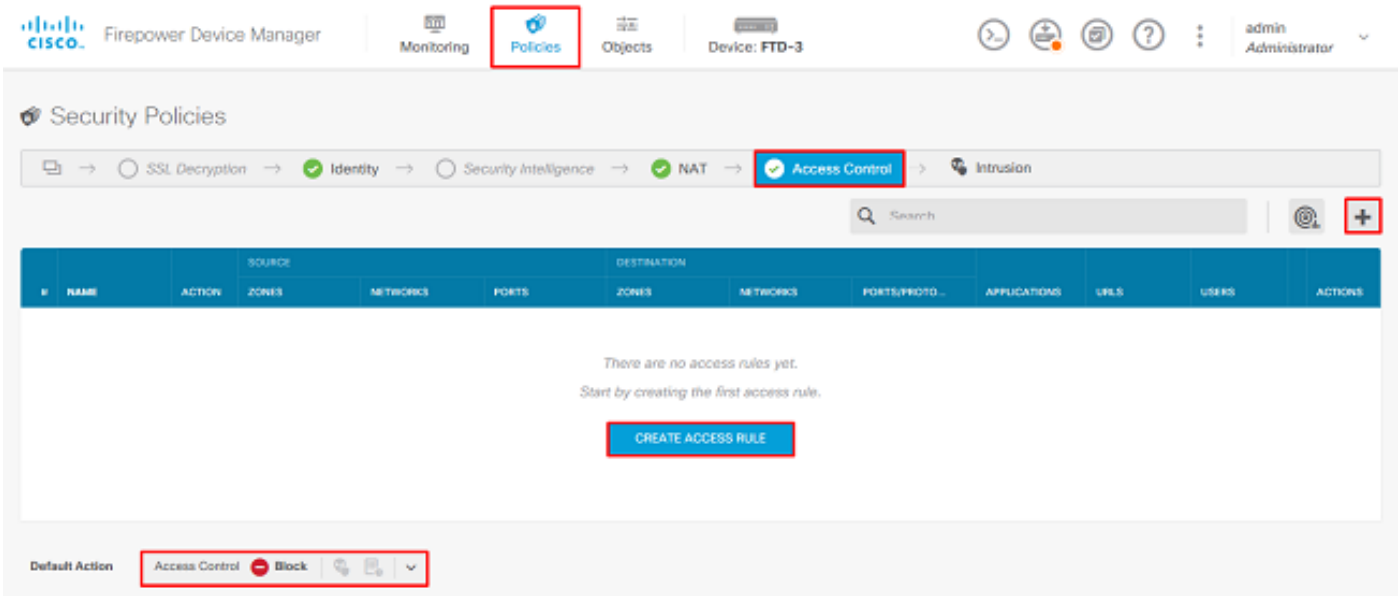
Para essa configuração, nenhuma configuração adicional é necessária e a ação padrão é suficiente.



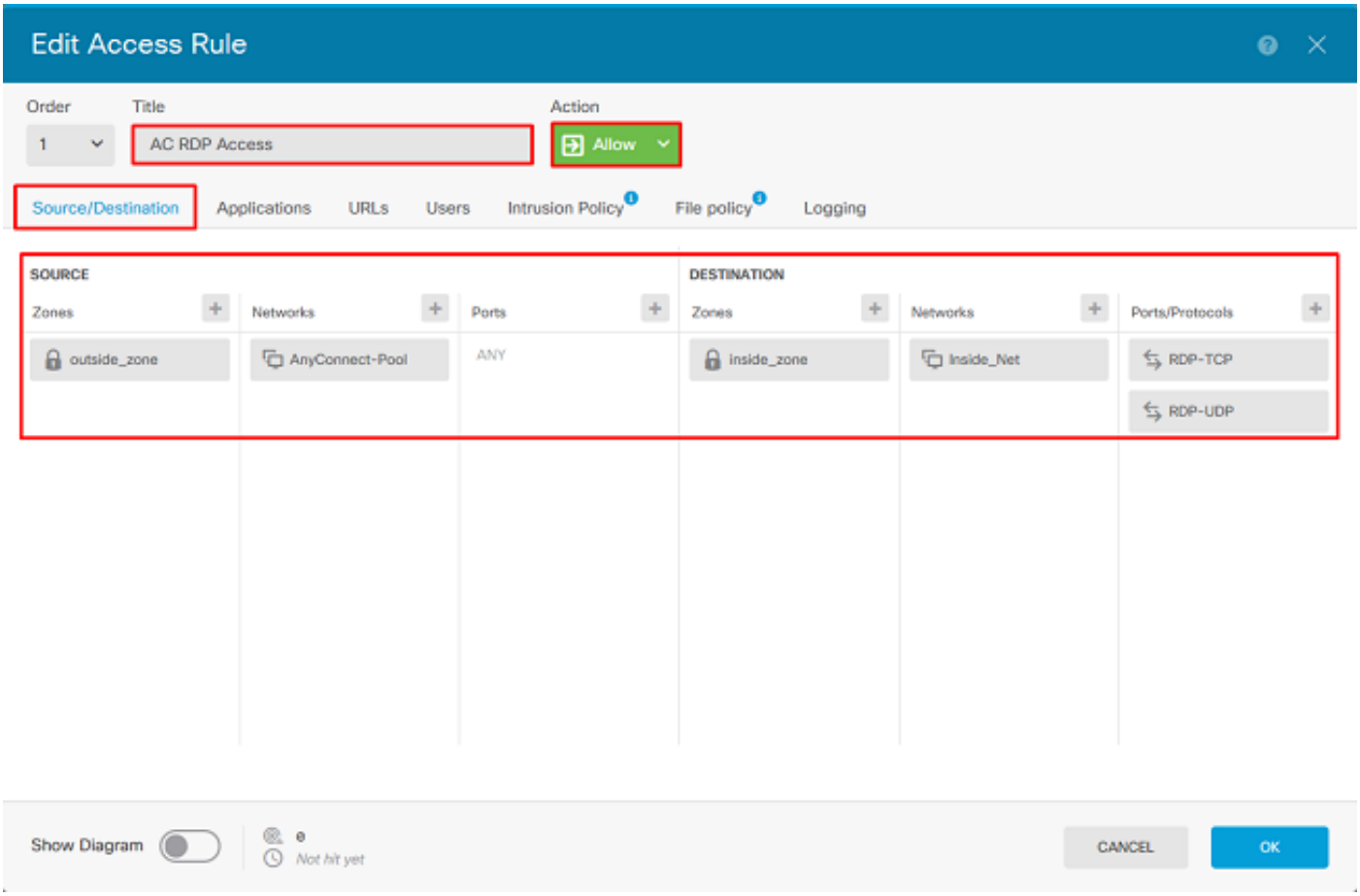
2. Navegue até **Policies > NAT** e certifique-se de que o NAT esteja configurado corretamente. Se a exceção de NAT configurada nas configurações do AnyConnect for suficiente, nenhuma configuração adicional será necessária aqui.



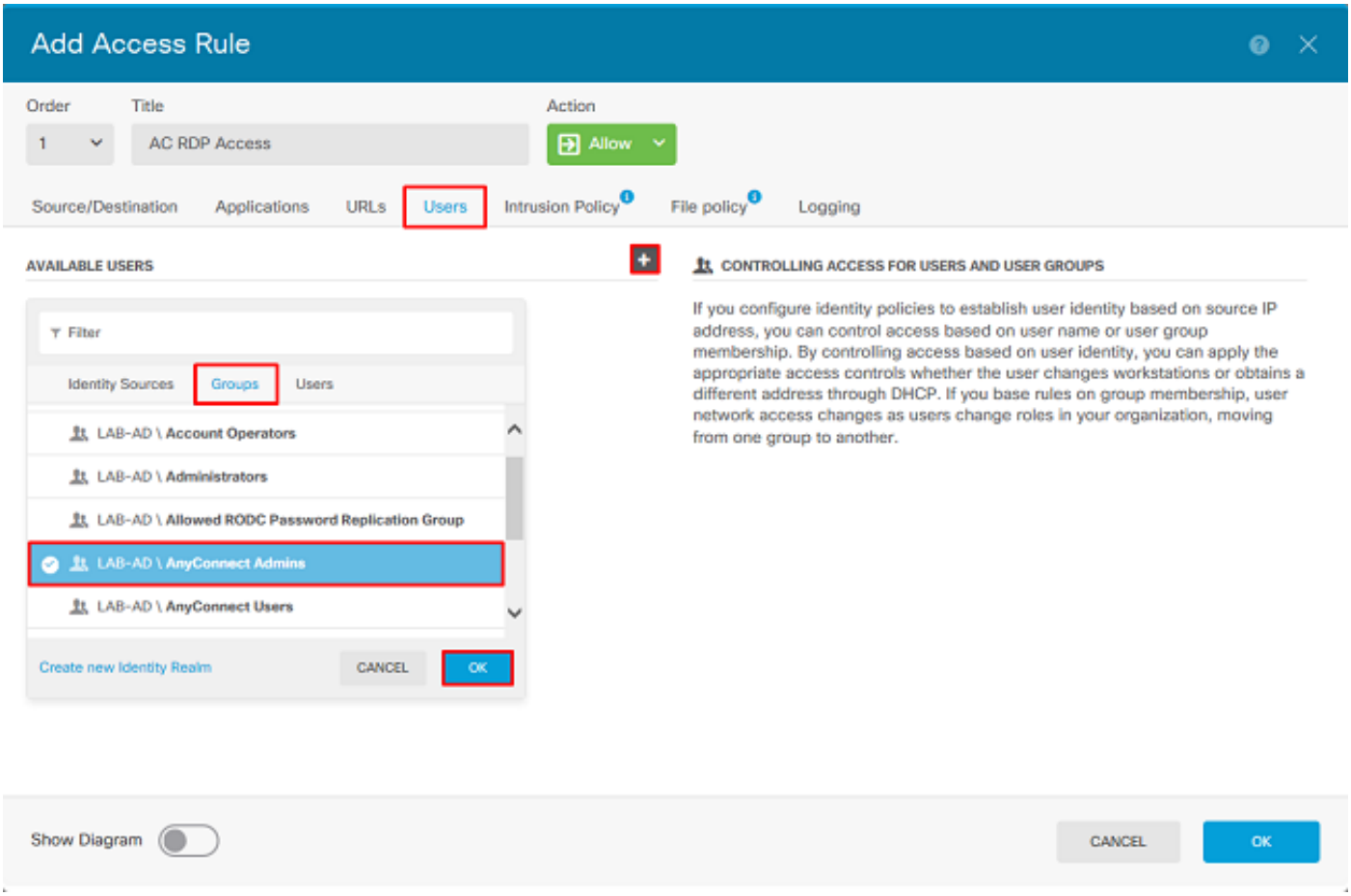
3. Navegue até **Políticas > Controle de acesso**. Nesta seção, a ação padrão é definida como Bloquear e nenhuma regra de acesso foi criada, de modo que, assim que um usuário do AnyConnect se conectar, ele não poderá acessar nada. Clique no **+** símbolo ou em Criar regra de acesso para adicionar uma nova regra.



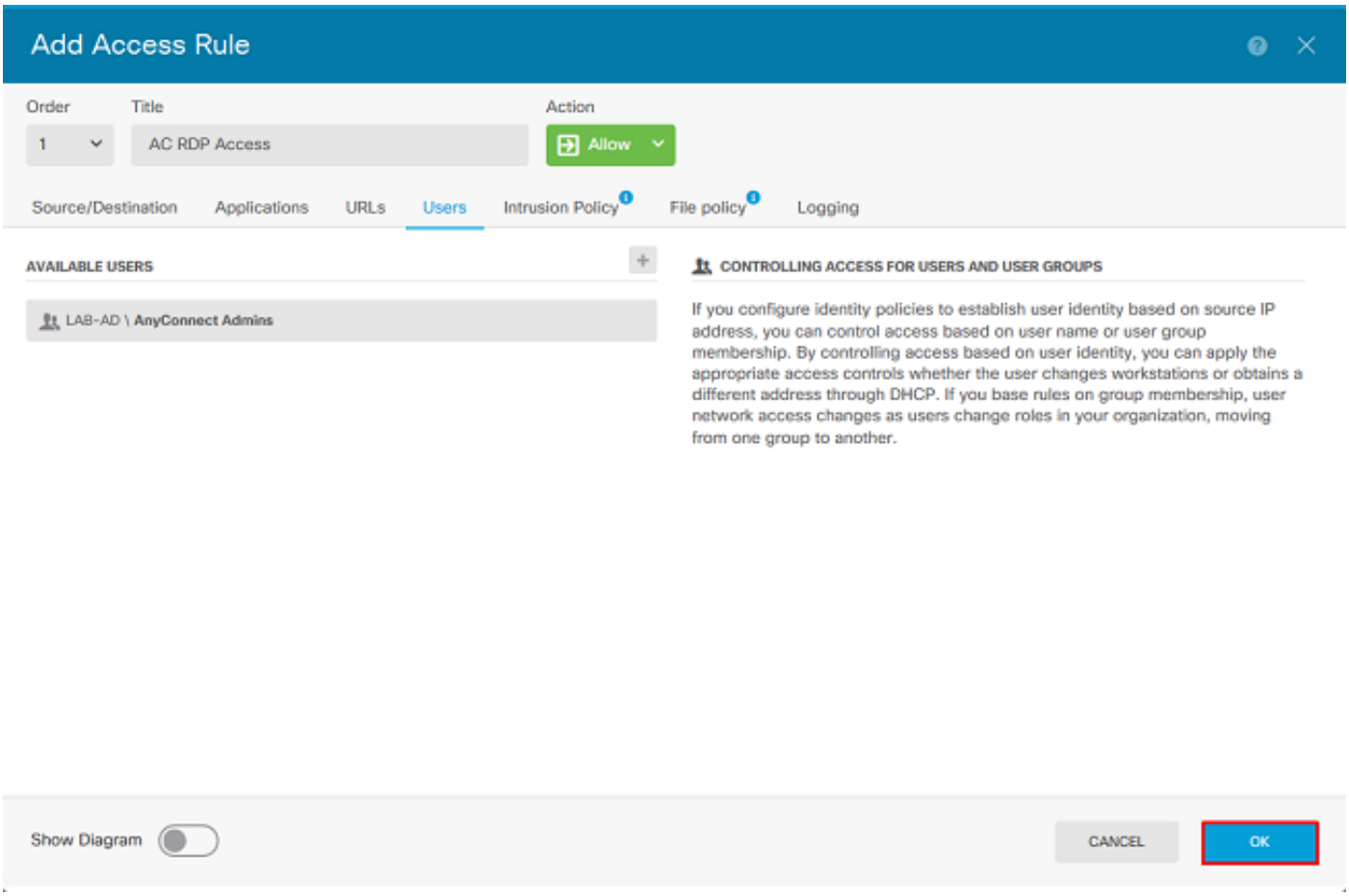
4. Preencha os campos com os valores apropriados. Nesta configuração, os usuários no grupo de administradores do AnyConnect devem ter acesso RDP ao Windows Server na rede interna. Para a origem, a zona é configurada como outside_zone, que é a interface externa à qual os usuários do AnyConnect se conectarão e a rede é configurada como o objeto do AnyConnect-Pool configurado anteriormente para atribuir endereços IP a clientes do AnyConnect. Para a identidade do usuário no FDM, a origem deve ser a zona e a rede de onde o usuário iniciará a conexão. Para o destino, a zona é configurada como inside_zone, que é a interface interna em que o Windows Server está localizado, a rede é configurada como o objeto Inside_Net, que é um objeto que define a sub-rede em que o Windows Server está, e Portas/Protocolos são definidos como dois objetos de porta personalizados para permitir acesso RDP sobre TCP 3389 e UDP 3389.



Na seção Users (Usuários), o grupo AnyConnect Admins (Administradores do AnyConnect) será adicionado, de modo que os usuários separados desse grupo terão acesso RDP ao Windows Server. Clique no **+** símbolo, clique na guia Grupos, clique no grupo apropriado e clique em **OK**. Observe que usuários individuais e a fonte de identidade também podem ser selecionados.

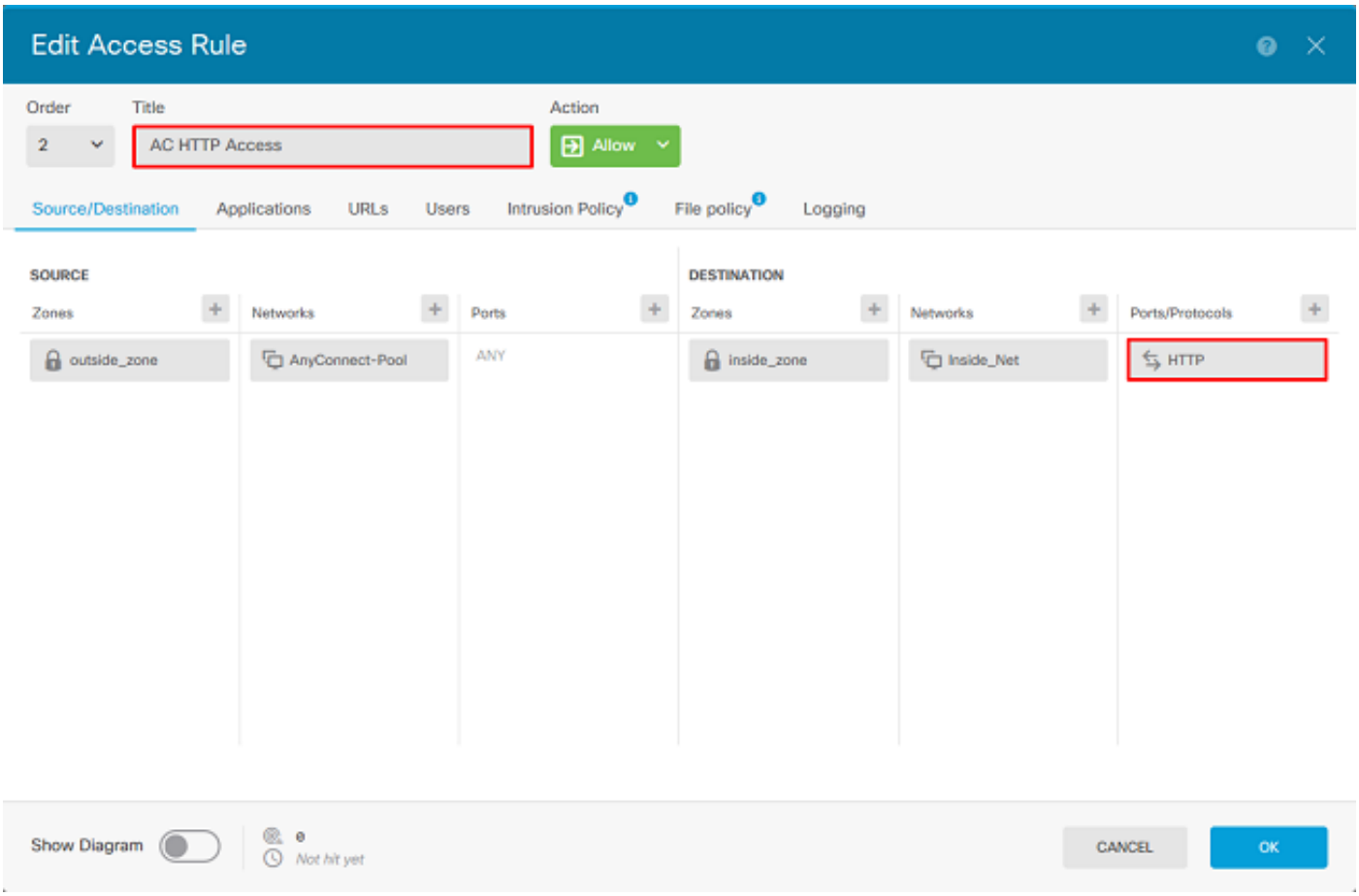


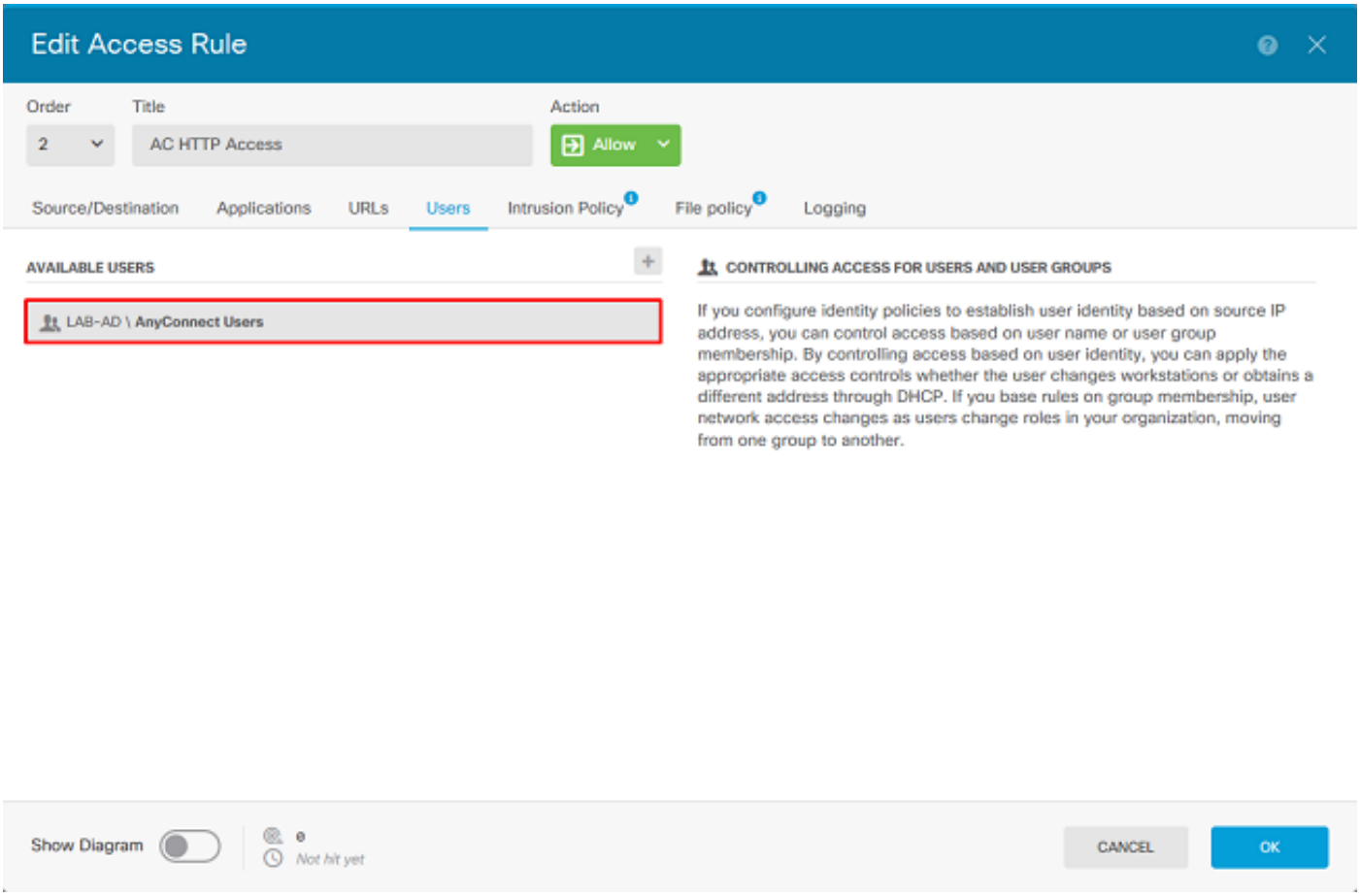
Depois de selecionar as opções apropriadas, clique em **OK**.



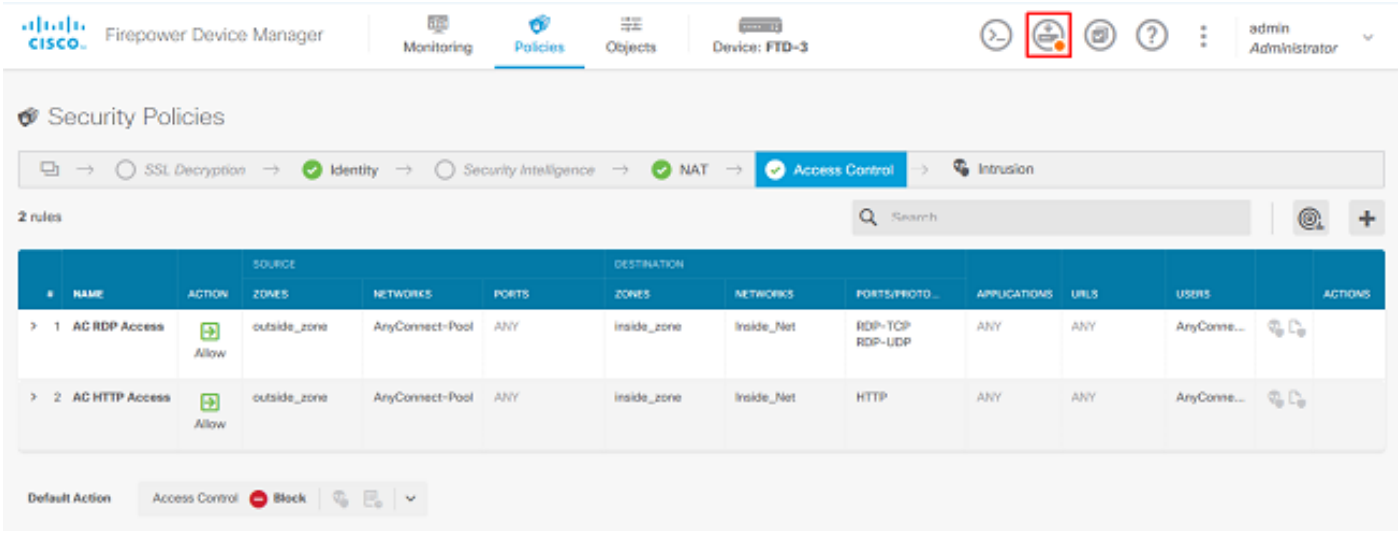
5. Crie mais regras de acesso, se necessário. Nesta configuração, outra regra de acesso é criada

para permitir aos usuários do grupo Usuários do AnyConnect acesso HTTP ao Windows Server.

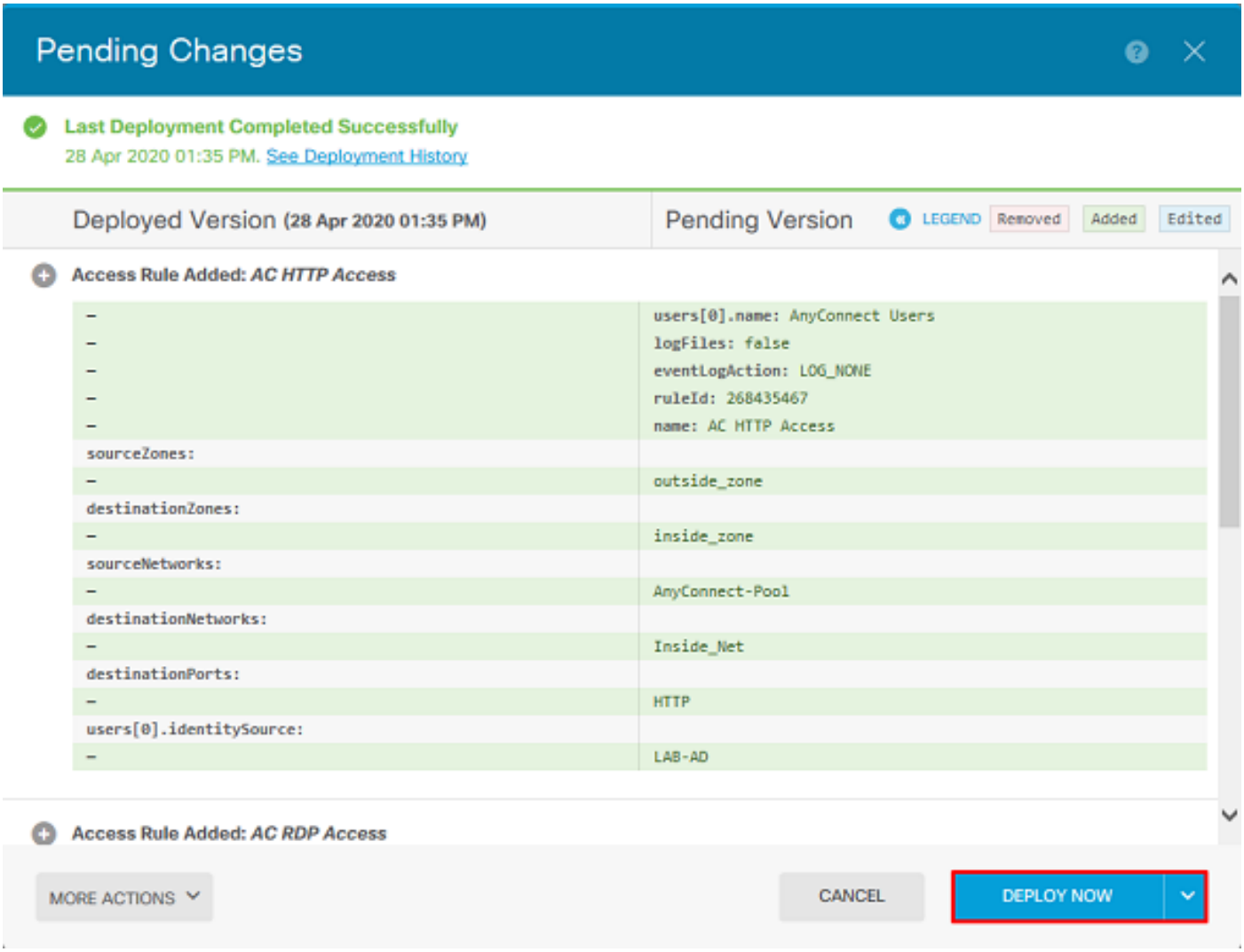




6. Verifique a configuração da regra de acesso e clique no botão **Pending Changes** na parte superior direita, como mostrado na imagem.



7. Verifique as alterações e clique em **Implantar agora**.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Configuração final

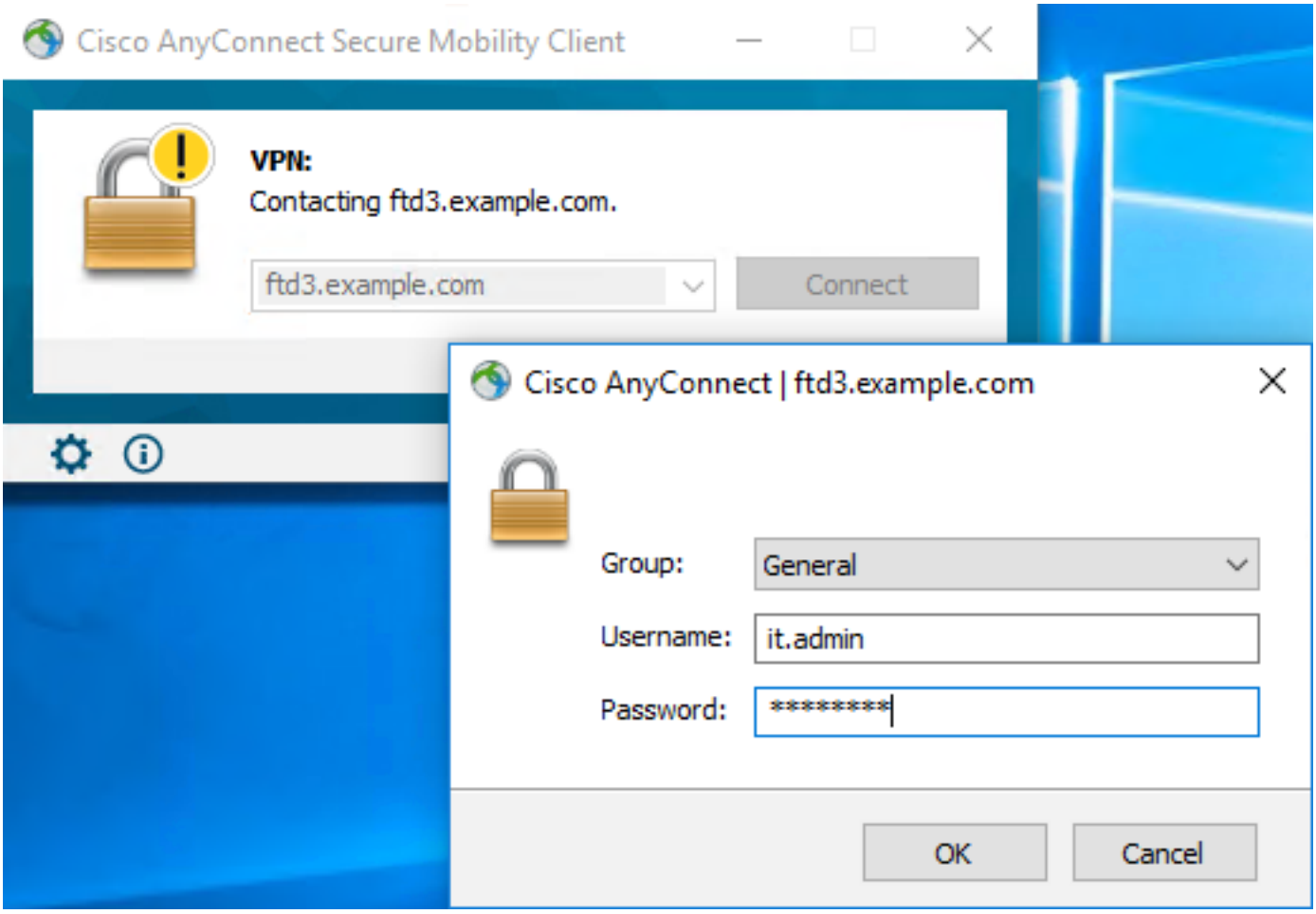
Configuração AAA

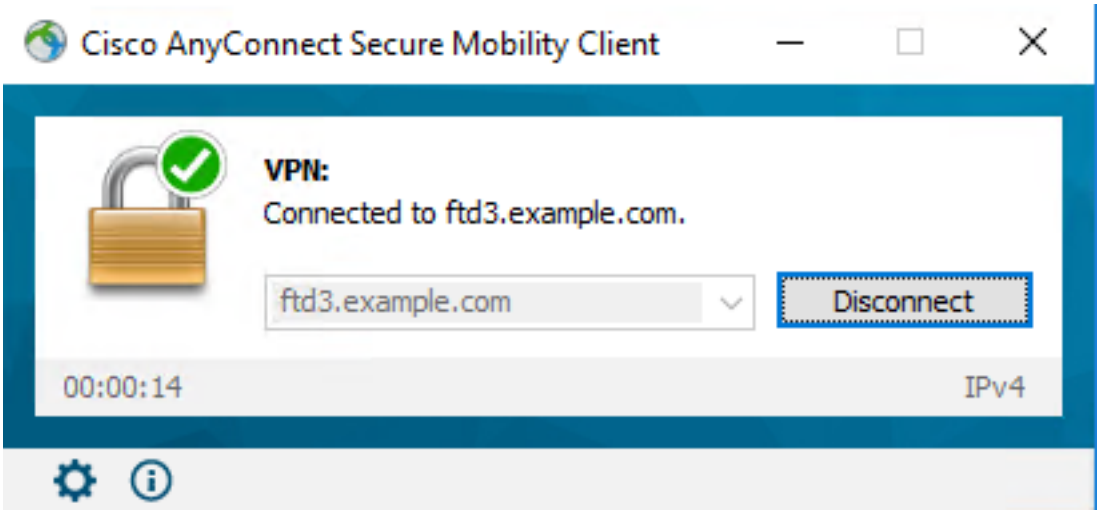
```
show running-configuration aaa-server
aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com server-
port 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-login-
dn ftd.admin@example.com server-type auto-detect
```

Configurar o AnyConnect

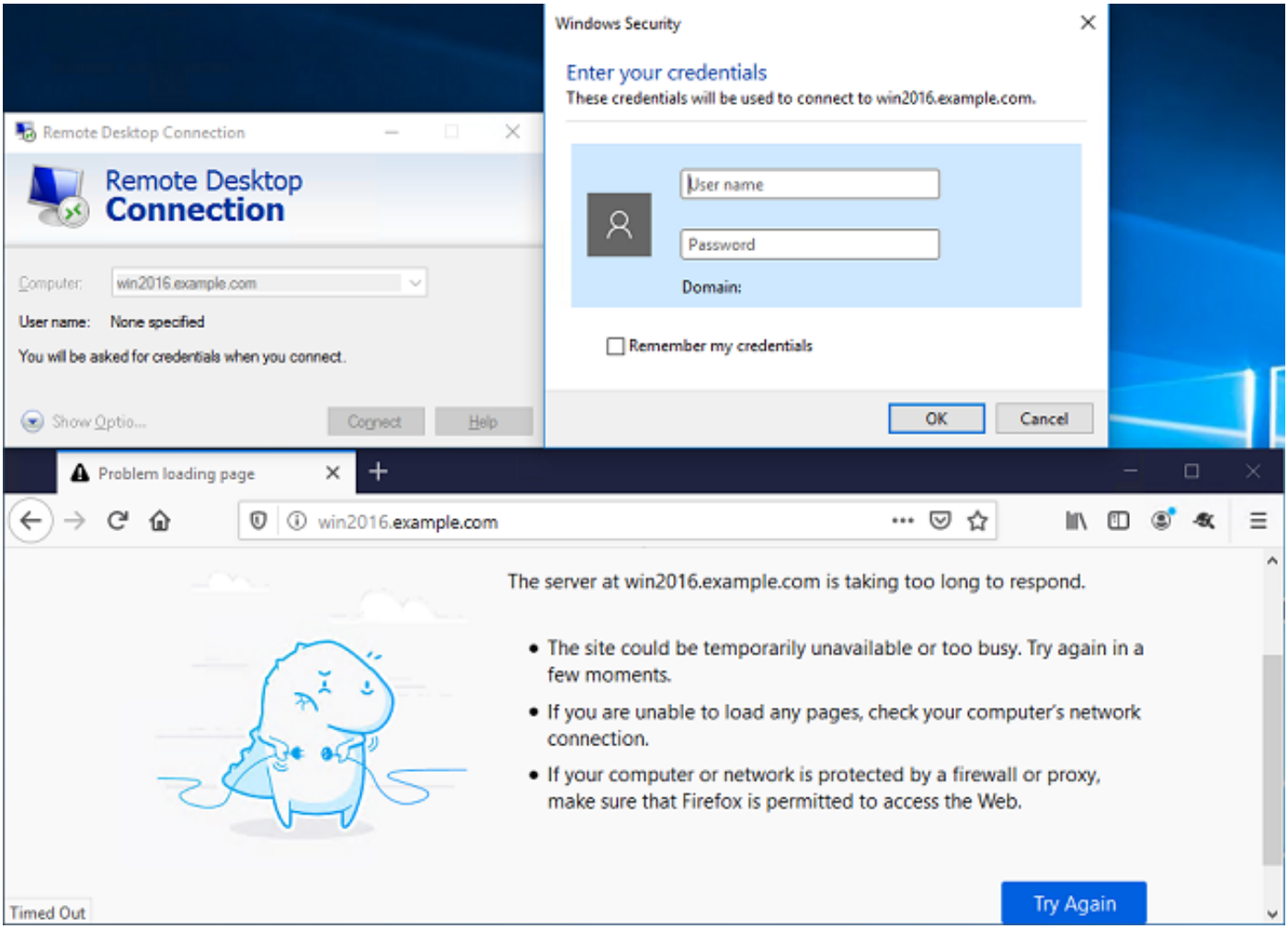
```
> show running-config webvpn
webvpn
 enable outside
 http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
 anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg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

Conecte-se com o AnyConnect e verifique as regras da política de controle de acesso

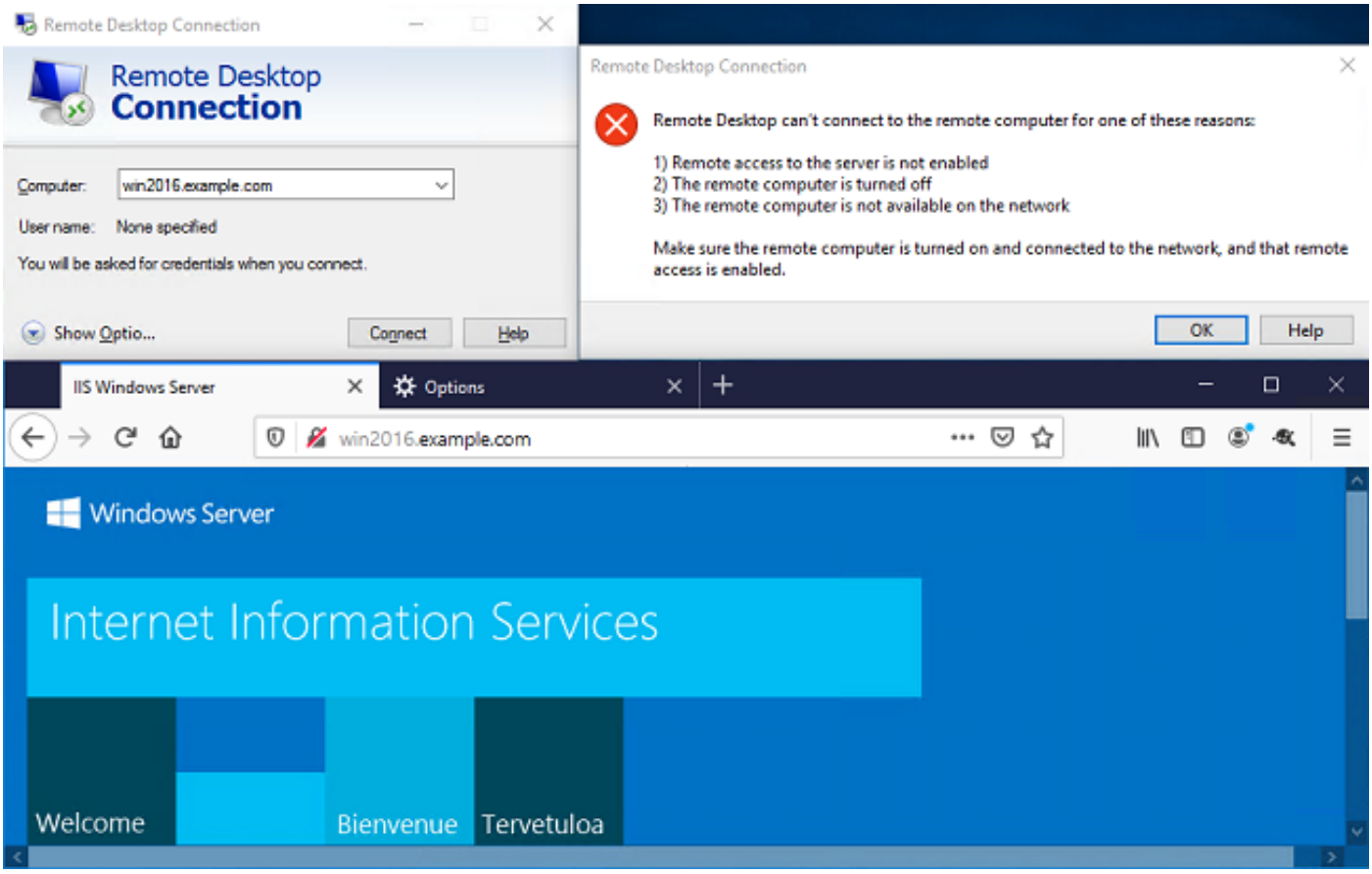




O User IT Admin está no grupo AnyConnect Admins que tem acesso RDP ao Windows Server, mas não tem acesso ao HTTP. A abertura de uma sessão RDP e Firefox para este servidor verifica se este usuário só pode acessar o servidor através do RDP.



Se estiver conectado a um usuário de teste que está no grupo Usuários do AnyConnect que têm acesso HTTP, mas não acesso RDP, você poderá verificar se as regras de política de controle de acesso estão sendo aplicadas.



Troubleshoot

Use esta seção para confirmar se a sua configuração funciona corretamente.

Debugs

Essa depuração pode ser executada na CLI de diagnóstico para solucionar problemas relacionados à autenticação LDAP: **debug ldap 255**.

Para solucionar problemas de Política de Controle de Acesso de identidade do usuário, o **sistema oferece suporte a firewall-engine-debug** pode ser executado em ordem para determinar por que o tráfego é permitido ou bloqueado inesperadamente.

Trabalhando com depurações LDAP

```
[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
```

Não é possível estabelecer conexão com o 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
```

Soluções em potencial:

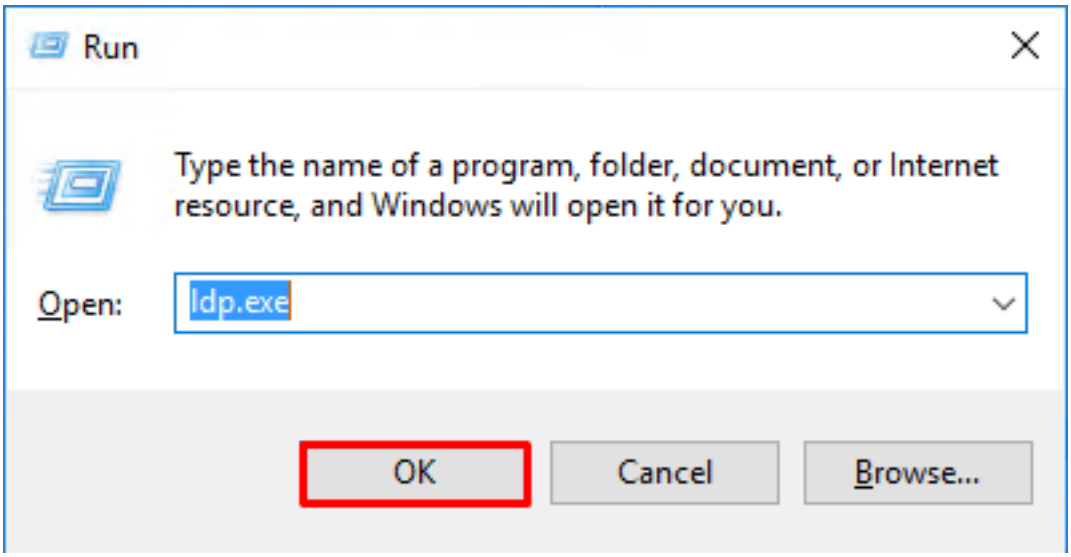
- Verifique o roteamento e certifique-se de que o FTD receba uma resposta do servidor LDAP.
- Se LDAPS ou STARTTLS for usado, verifique se o certificado de CA raiz correto é confiável para que o handshake SSL possa ser concluído com êxito.
- Verifique se o endereço IP e a porta corretos estão sendo usados. Se um nome de host for usado, verifique se o DNS é capaz de resolvê-lo para o endereço IP correto

DN de login de vinculação e/ou senha incorreta

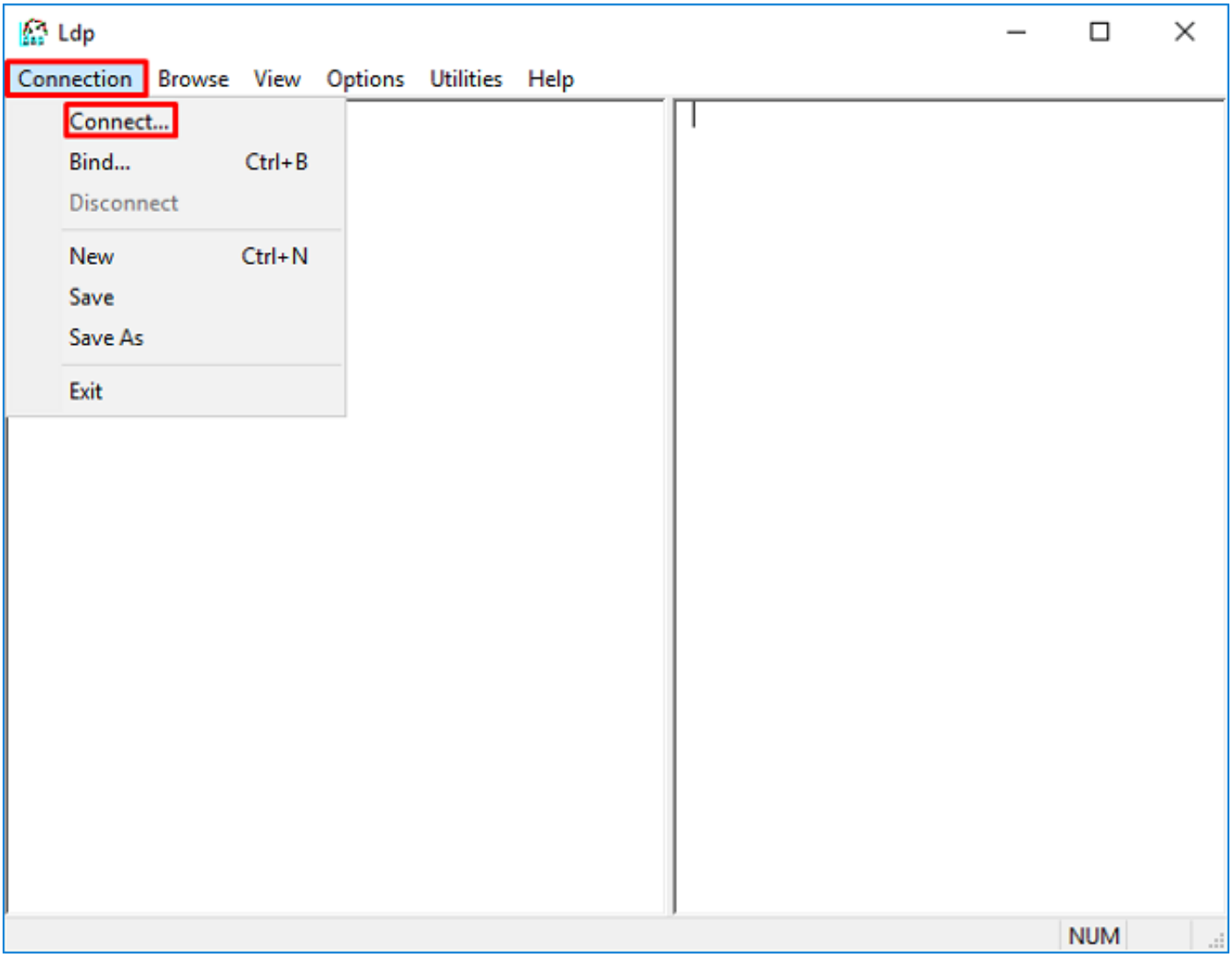
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] 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
```

Solução em potencial: Verifique se o DN de login e a senha de login estão configurados corretamente. Isso pode ser verificado no servidor do AD com **ldp.exe**. Para verificar se uma conta pode se vincular com êxito ao uso de ldp, navegue através destas etapas:

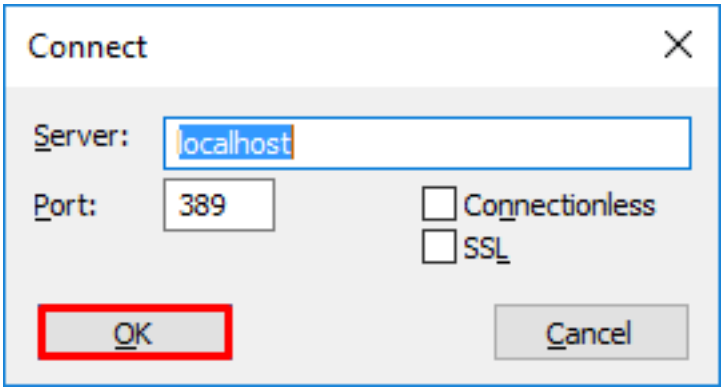
1. No servidor AD, pressione **Win+R** e procure **ldp.exe**.



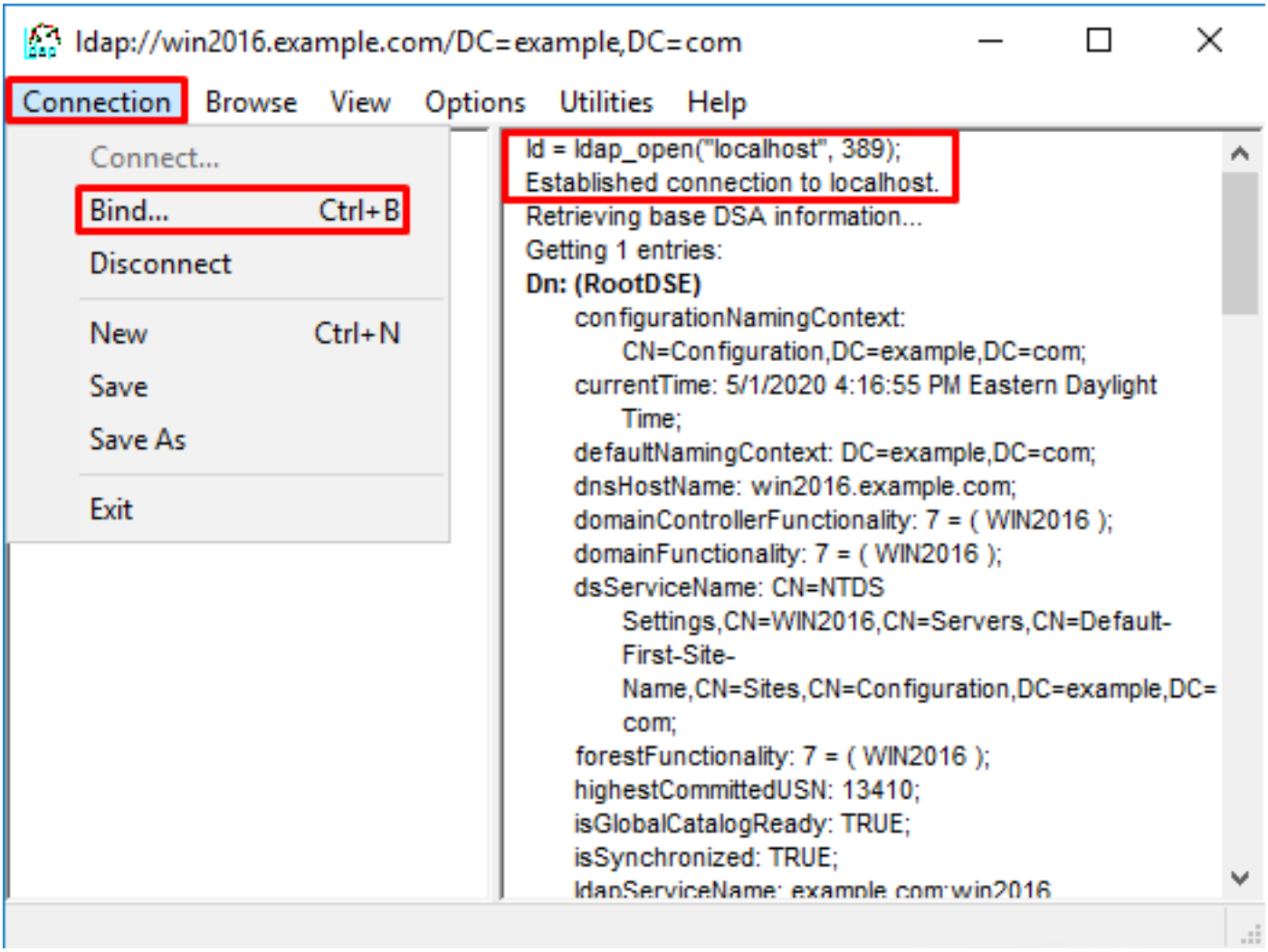
2. Clique em **Conexão > Conectar...** conforme mostrado na imagem.



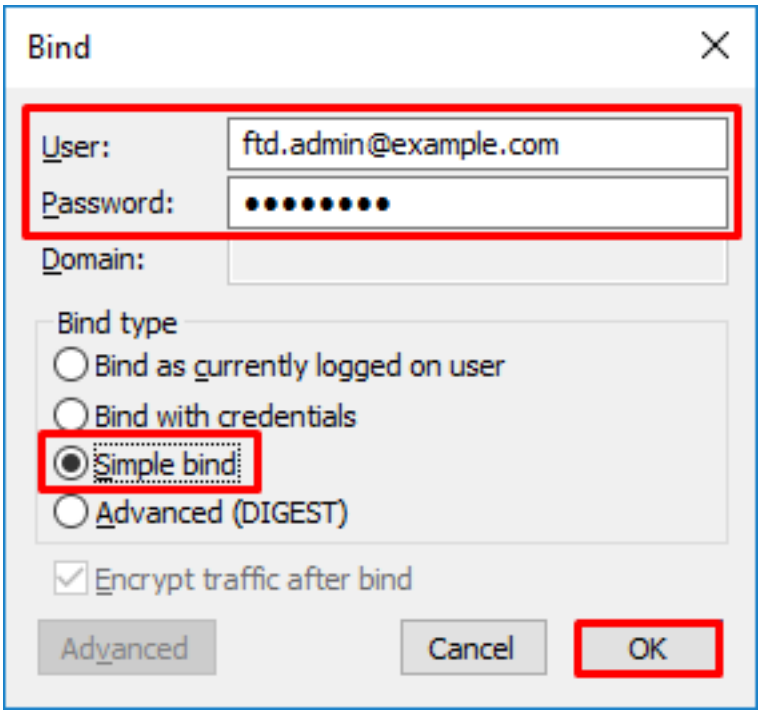
3. Especifique localhost para o servidor e a porta apropriada e clique em **OK**.



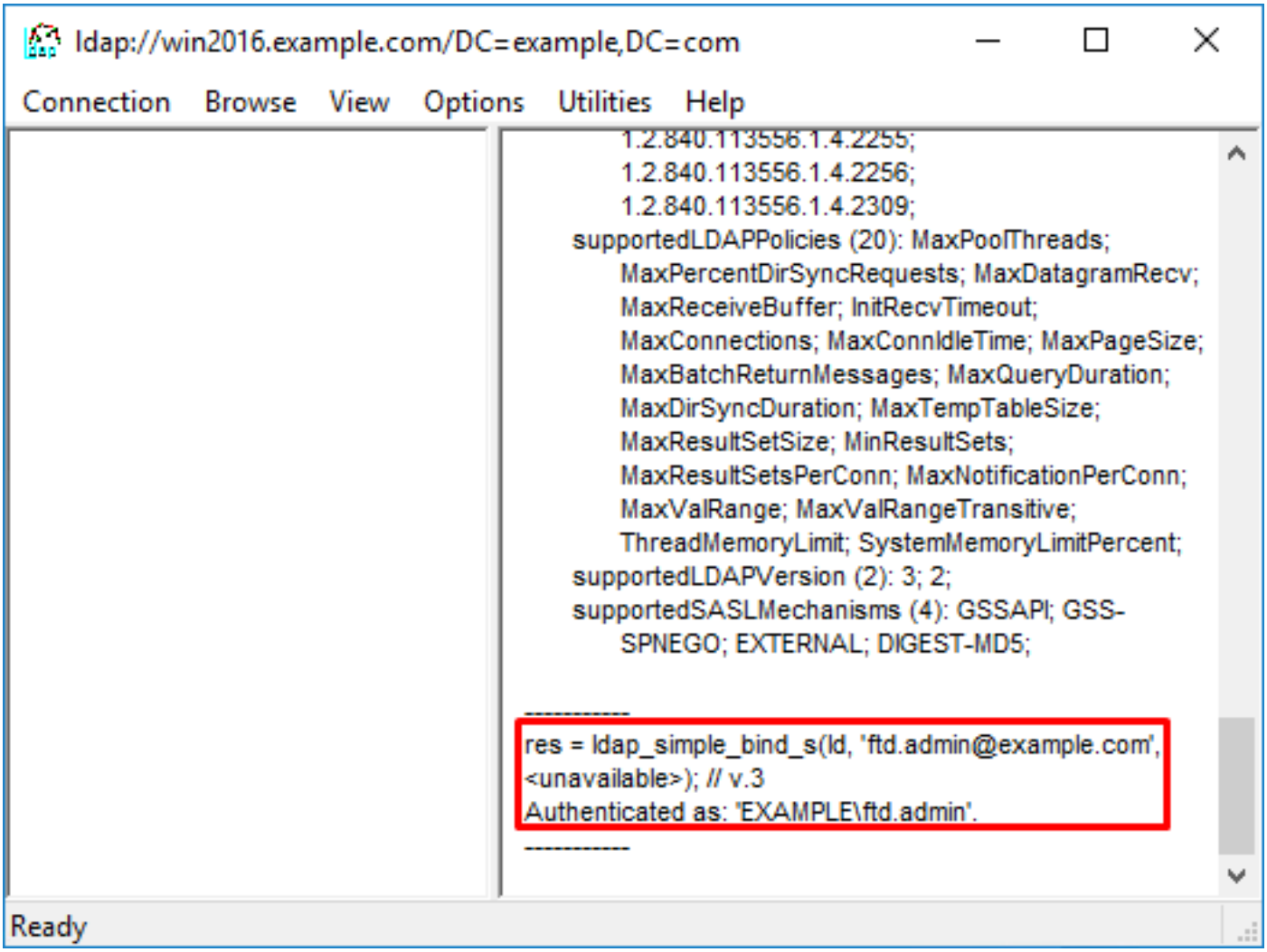
4. A coluna Direito mostra o texto que indica uma conexão bem-sucedida. Clique em **Conexão > Vincular...** conforme mostrado na imagem.



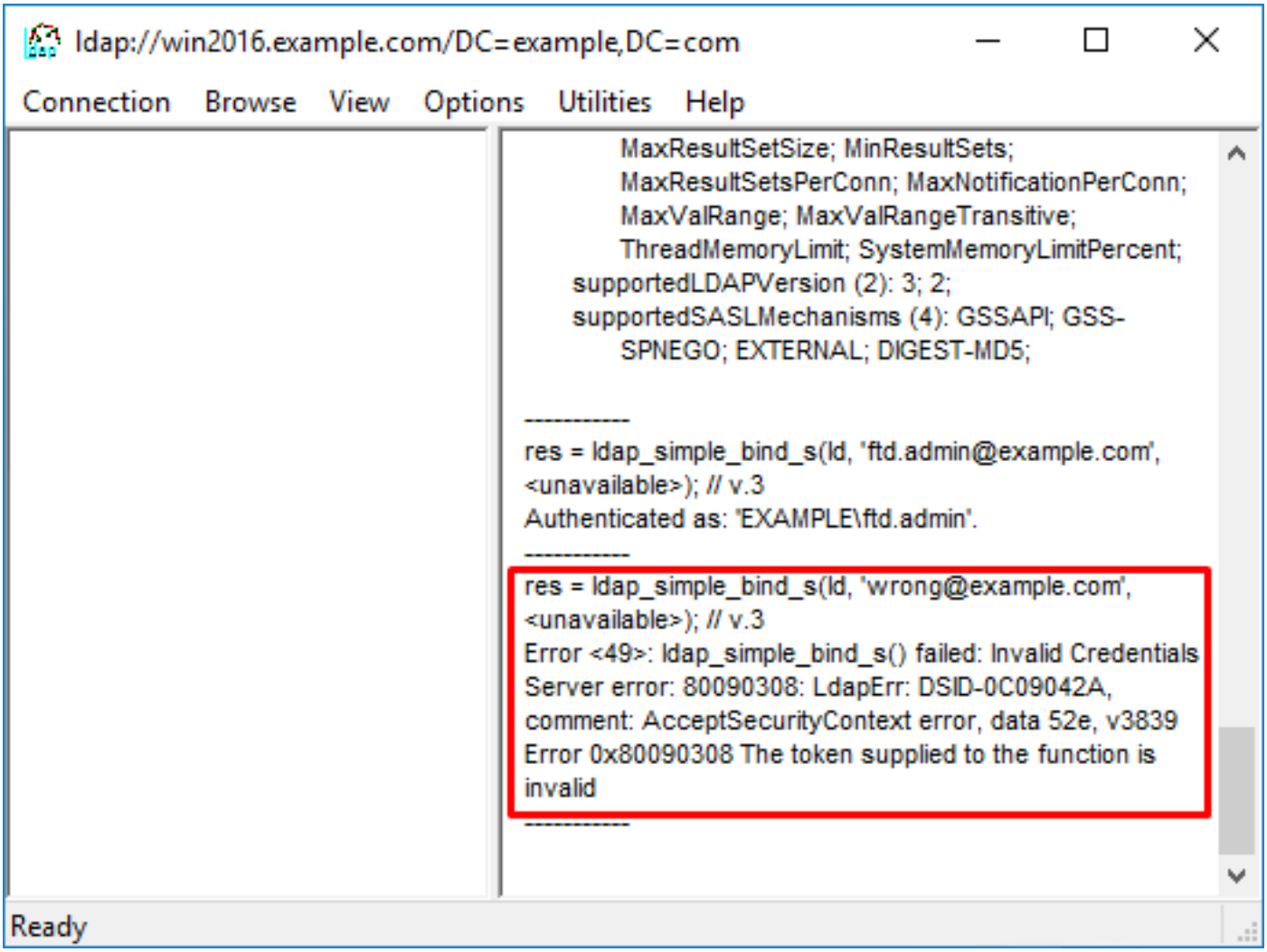
5. Selecione **Simple Bind** e especifique o nome de usuário e a senha da conta de diretório. Click **OK**.



Com uma associação bem-sucedida, ldp mostrará Authenticated como **DOMAIN\username**.



Se você tentar uma associação com um nome de usuário ou senha inválidos, isso resultará em uma falha como esta.

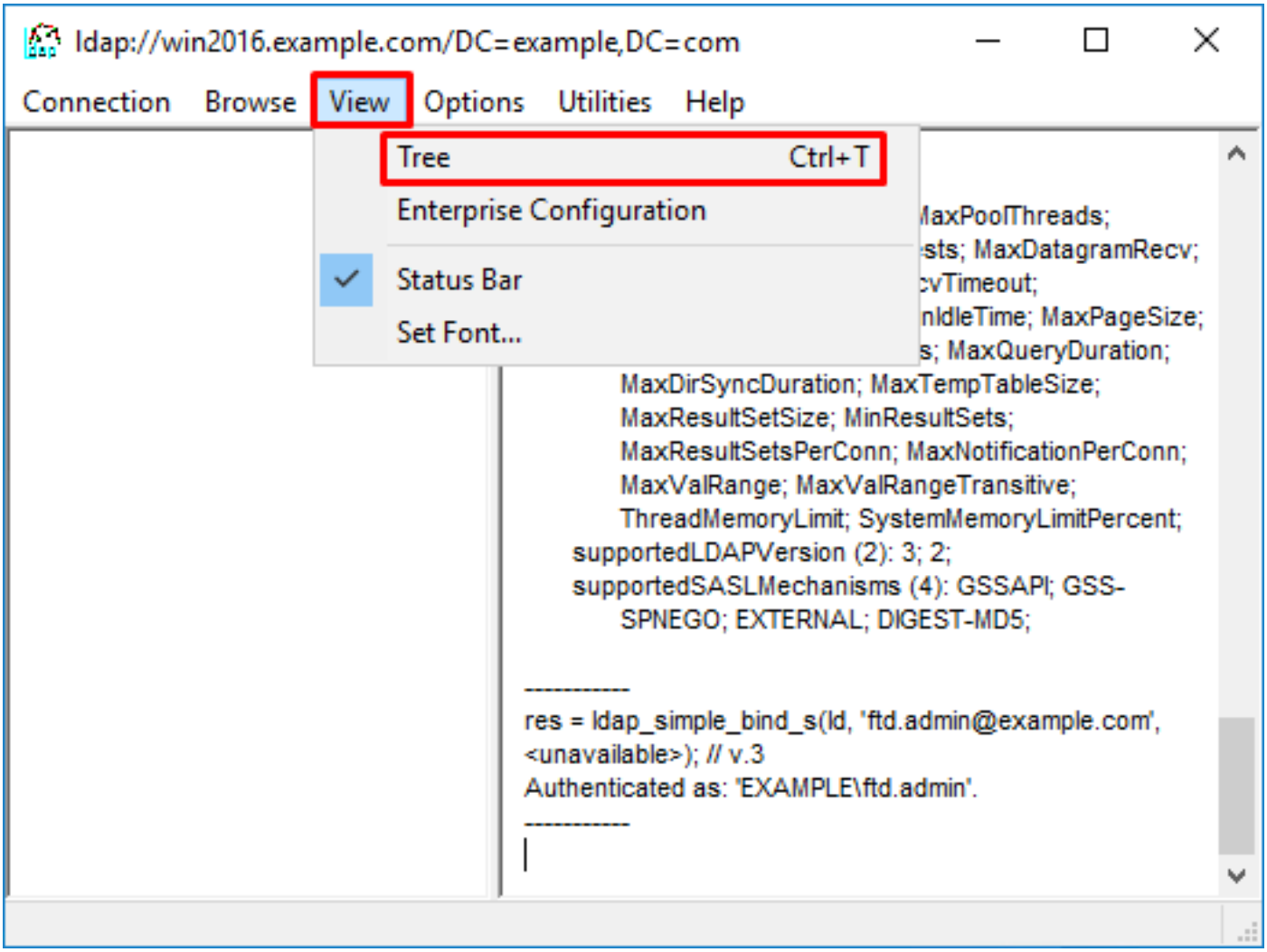


Servidor LDAP não pode localizar nome de usuário

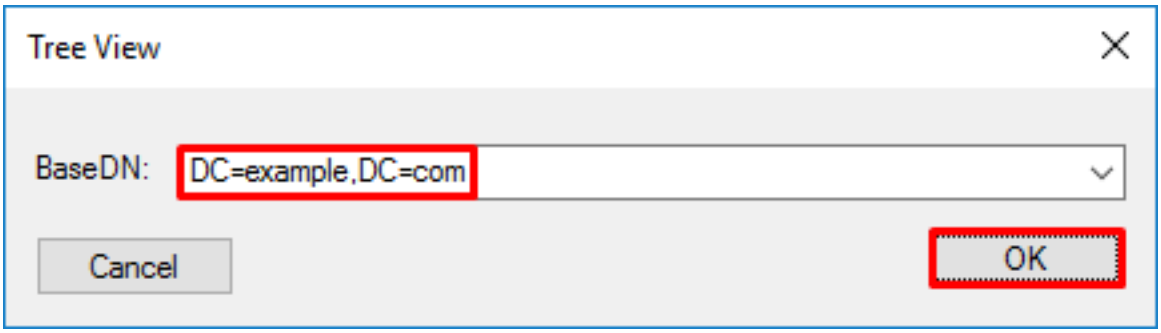
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] 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
```

Solução em potencial: Verifique se o AD pode localizar o usuário com a pesquisa feita pelo FTD. Isso também pode ser feito com ldp.exe.

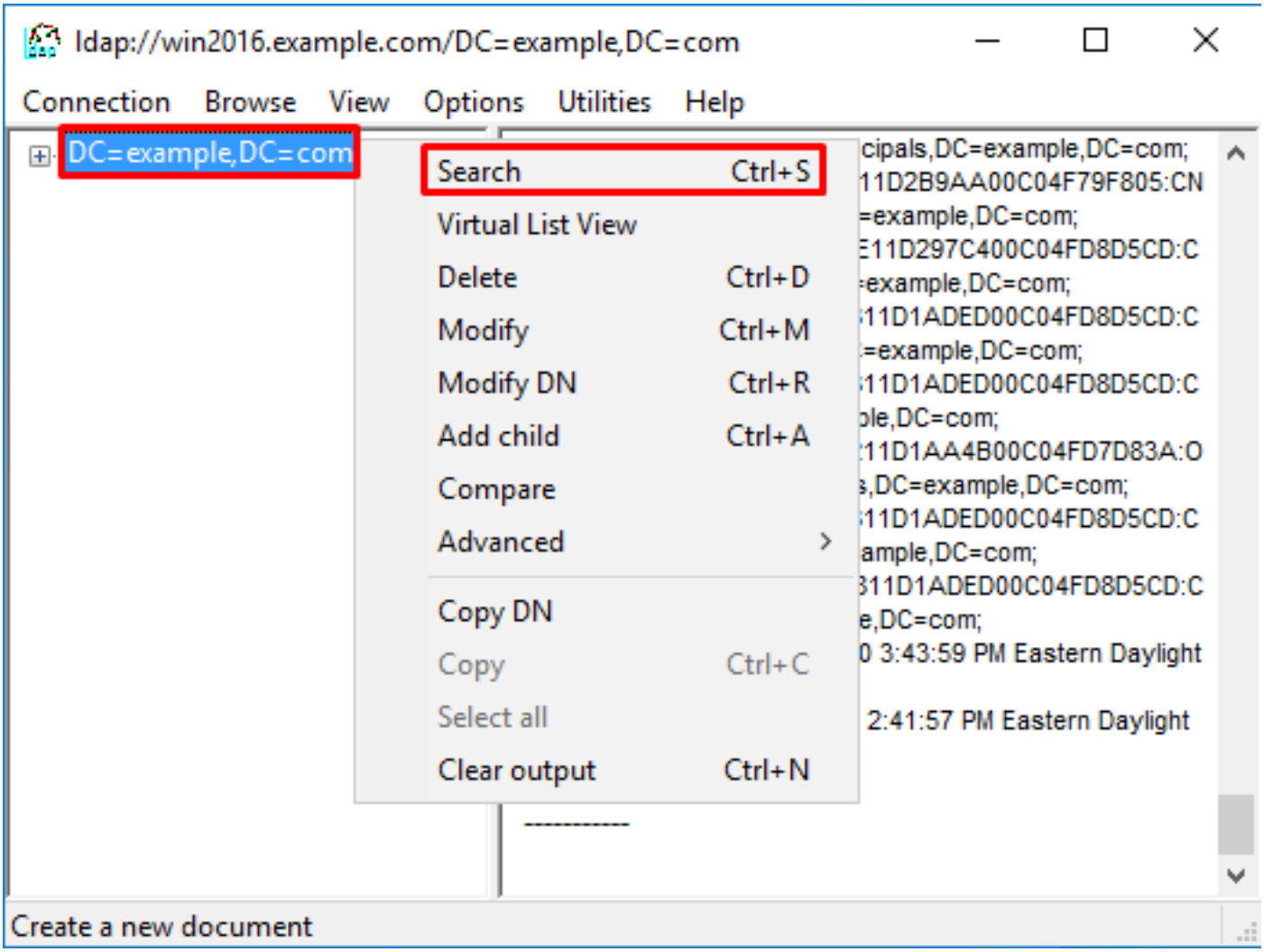
1. Após a associação com êxito, navegue para **Exibir > Árvore** como mostrado na imagem.



2. Especifique o DN base configurado no FTD e clique em **OK**.

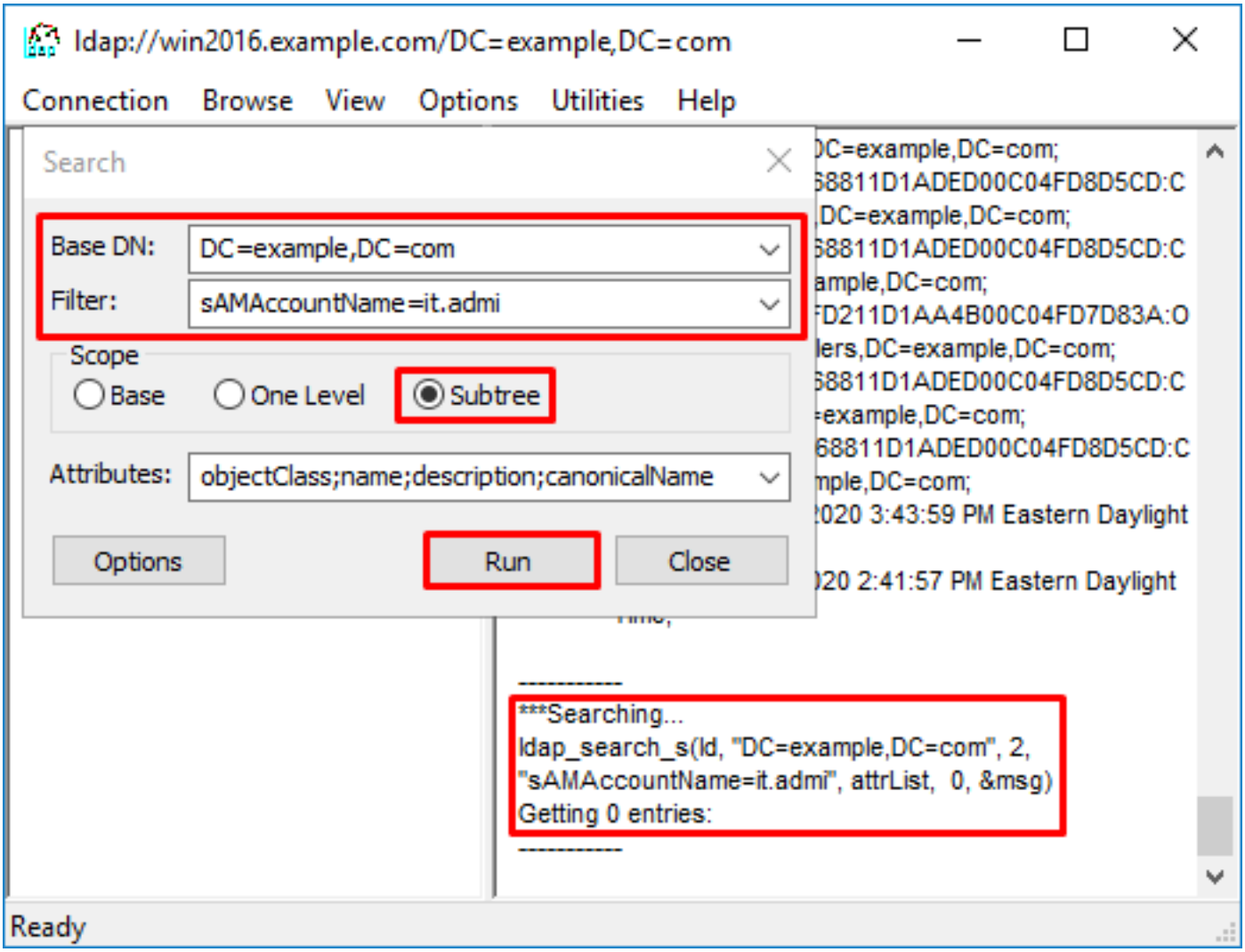


3. Clique com o botão direito do mouse no DN base e clique em Pesquisar como mostrado na imagem.



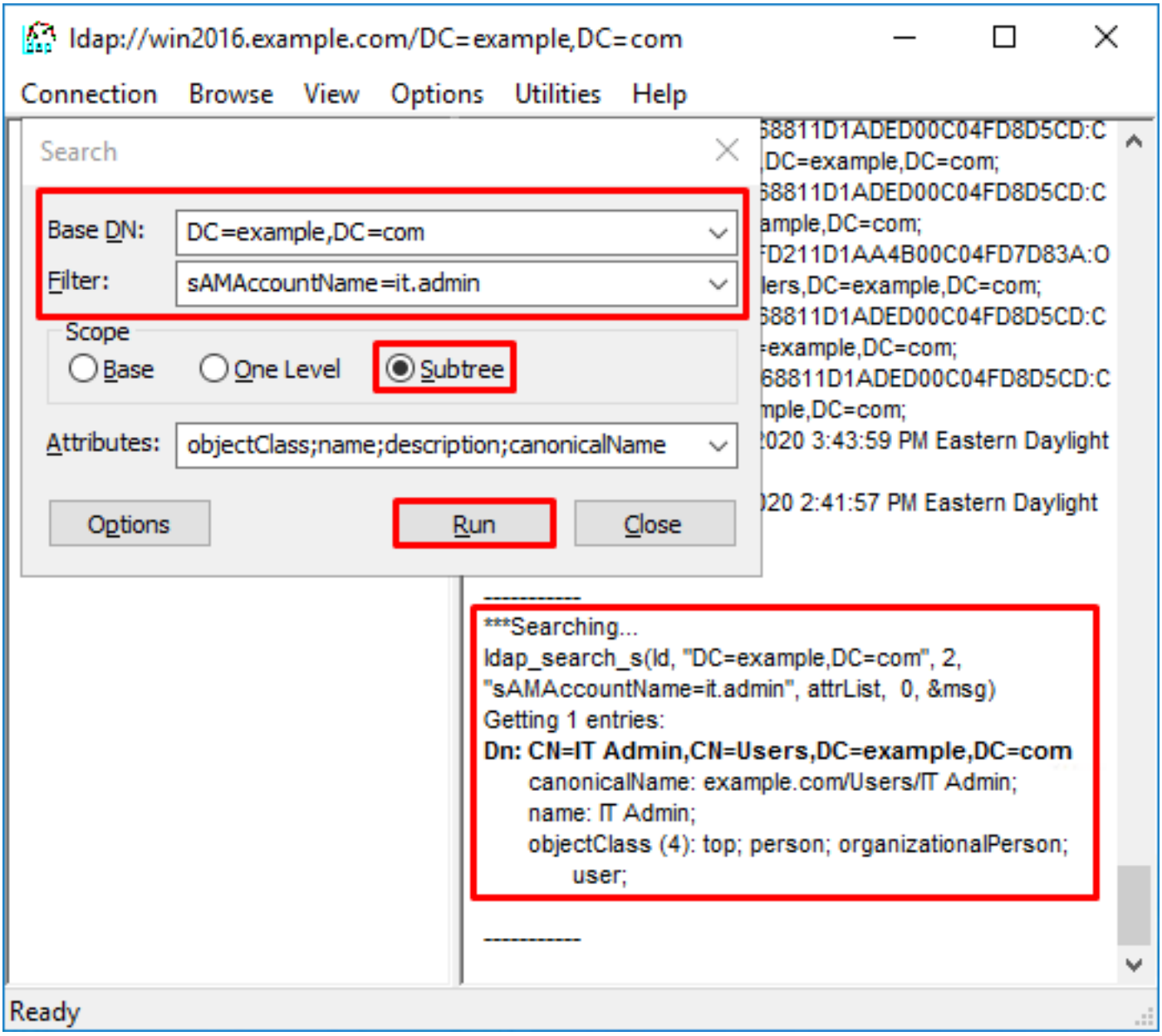
4. Especifique os mesmos valores de Base DB, Filtro e Escopo conforme vistos nas depurações. Neste exemplo, eles são:

- DN base: dc=exemplo,dc=com
- Filtro: samaccountingname=it.admi
- Escopo:SUBTREE



ldp encontra 0 entradas devido a não haver uma conta de usuário com o **samaccountingname=it.admi** sob o DN base dc=example,dc=com.

Tentar novamente com o **samaccountingname=it.admin** mostra um resultado diferente. ldp encontra 1 entrada sob o DN base dc=example,dc=com e imprime o DN do usuário.



Senha incorreta para o nome de usuário

```
[-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
```

Solução em potencial: Verifique se a senha do usuário está configurada corretamente e se ela não expirou. Semelhante ao DN de login, o FTD fará uma associação ao AD com as credenciais do usuário. Essa associação também pode ser feita em ldp para verificar se o AD é capaz de reconhecer as mesmas credenciais de nome de usuário e senha. As etapas em ldp são mostradas na seção **Vinculando DN de login e/ou Senha incorreta**. Além disso, os registros do Visualizador de Eventos do servidor Microsoft podem ser analisados por um motivo potencial.

Test AAA

O comando test aaa-server pode ser usado para simular uma tentativa de autenticação do FTD com um nome de usuário e senha específicos. Isso pode ser usado para testar se há falhas de conexão ou autenticação. O comando é **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 pacotes

Capturas de pacotes podem ser usadas para verificar a acessibilidade ao servidor AD. Se os pacotes LDAP saírem do FTD, mas não houver resposta, isso pode indicar um problema de roteamento.

Aqui está uma captura que mostra o tráfego LDAP bidirecional:

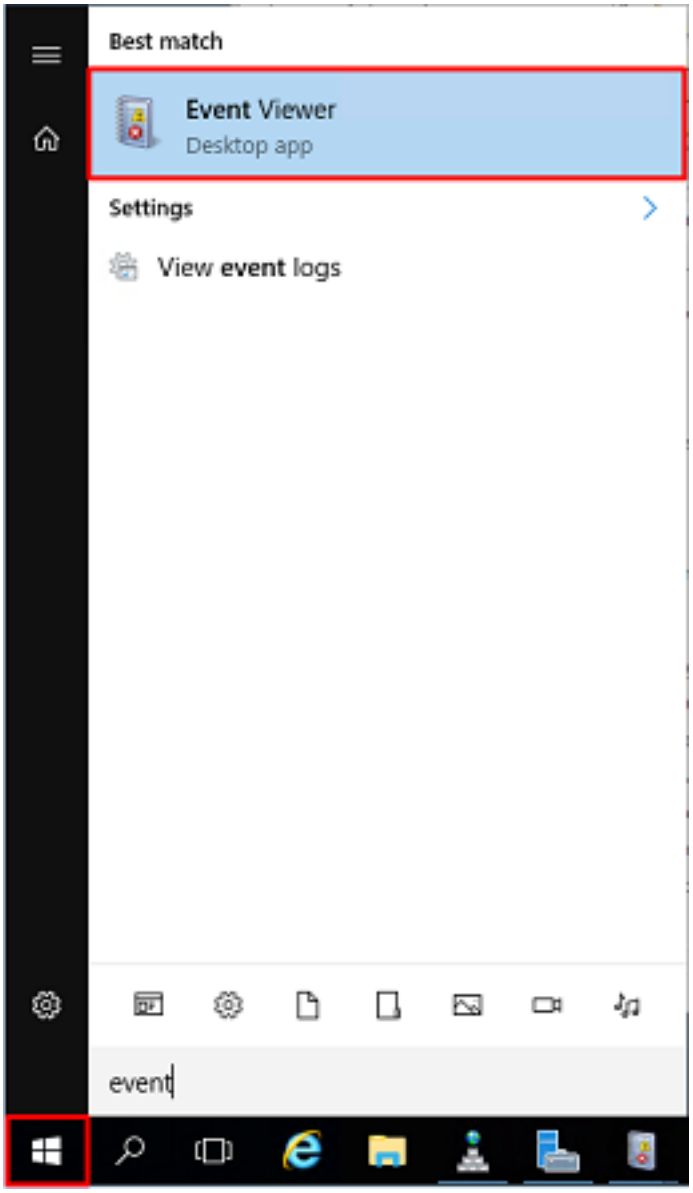
```
> show route 192.168.1.1

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
```

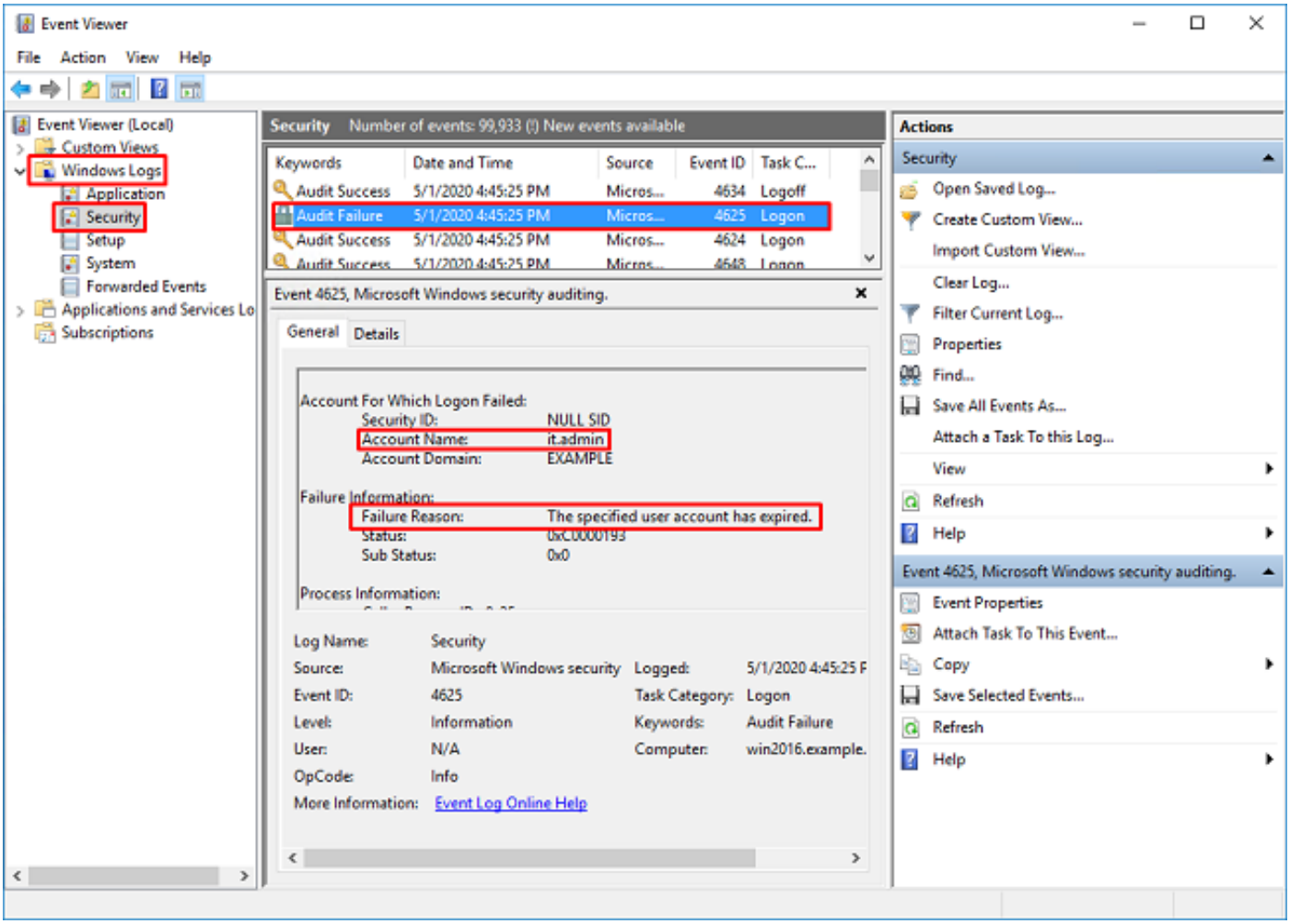
Logs do Visualizador de Eventos do Windows Server

Os registros do Visualizador de Eventos no carrinho do servidor AD fornecem informações mais detalhadas sobre por que ocorreu uma falha.

1. Procure e abra o **Visualizador de Eventos**.



2. Expanda **Logs do Windows** e clique em **Segurança**. Procure **Falha de auditoria** com o Nome da conta do usuário e revise as Informações de falha como mostrado na imagem.



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