Configurar o gerenciamento de senhas usando LDAPs para VPN RA no FTD gerenciado pelo FMC

Contents

Introdução

Este documento descreve a configuração do Gerenciamento de senhas usando LDAPs para clientes AnyConnect que se conectam ao Cisco Firepower Threat Defense (FTD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- Conhecimento básico da configuração da VPN (Remote Access Virtual Private Network) do RA no FMC
- Conhecimento básico da configuração do servidor LDAP no FMC
- Conhecimento básico do Active Directory

Componentes Utilizados

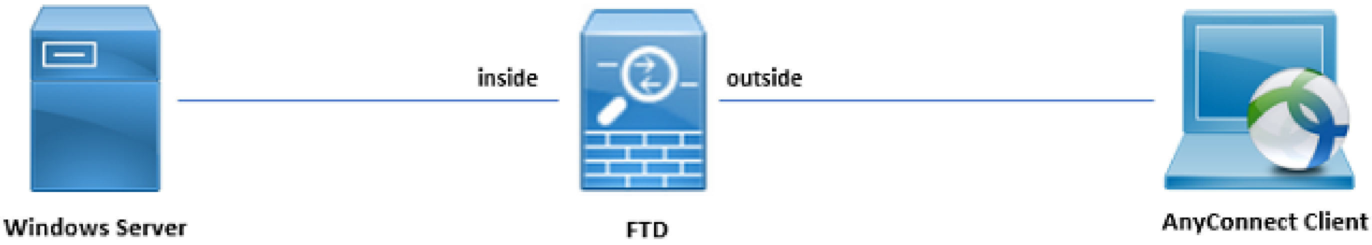
As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuração

Diagrama e cenário de rede



O servidor Windows é pré-configurado com ADDS e ADCS para testar o processo de gerenciamento de senha do usuário. Neste guia de configuração, essas contas de usuário são criadas.

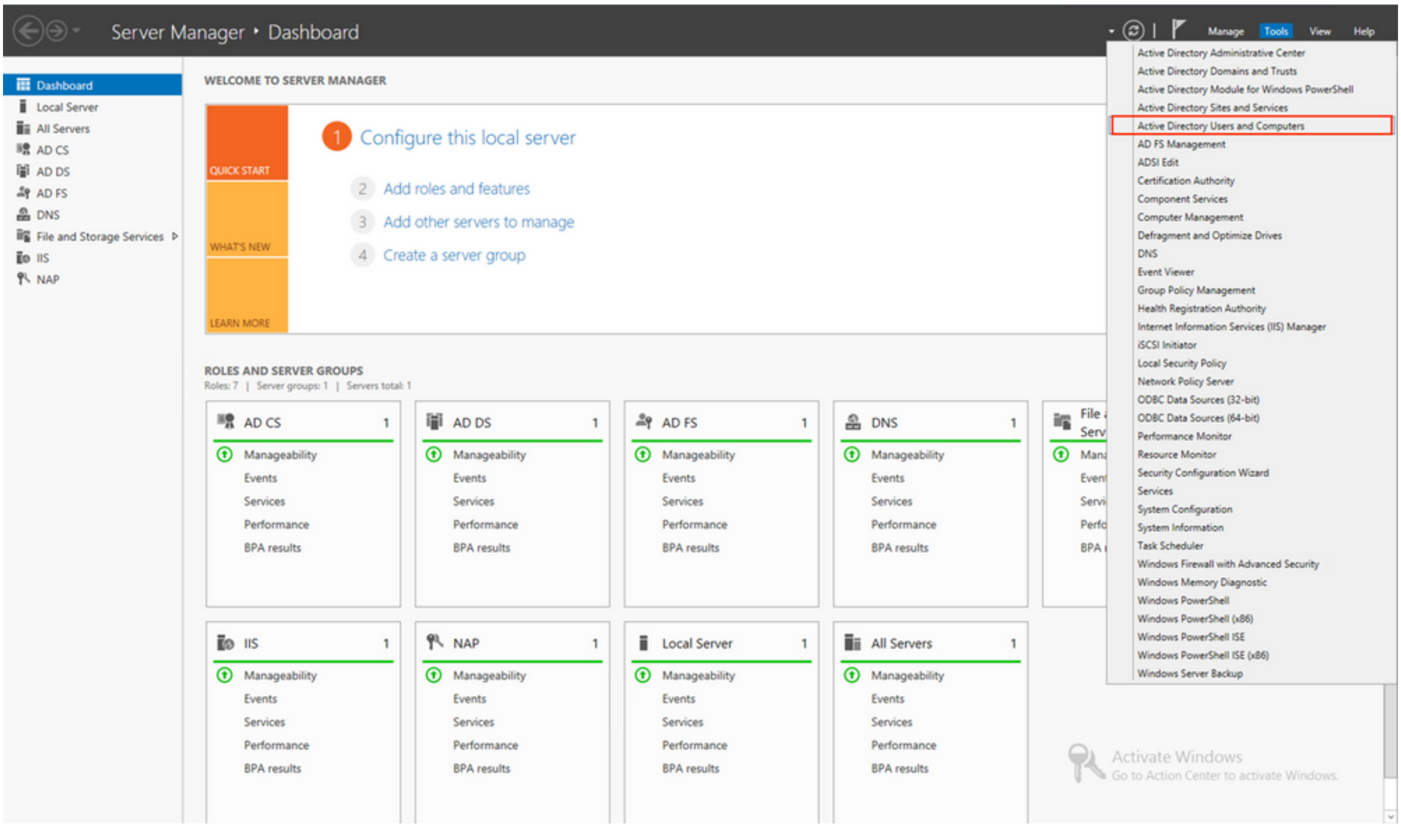
Contas do usuário:

- Administrador: usado como a conta do diretório para permitir que o FTD se vincule ao servidor do Ative Diretory.

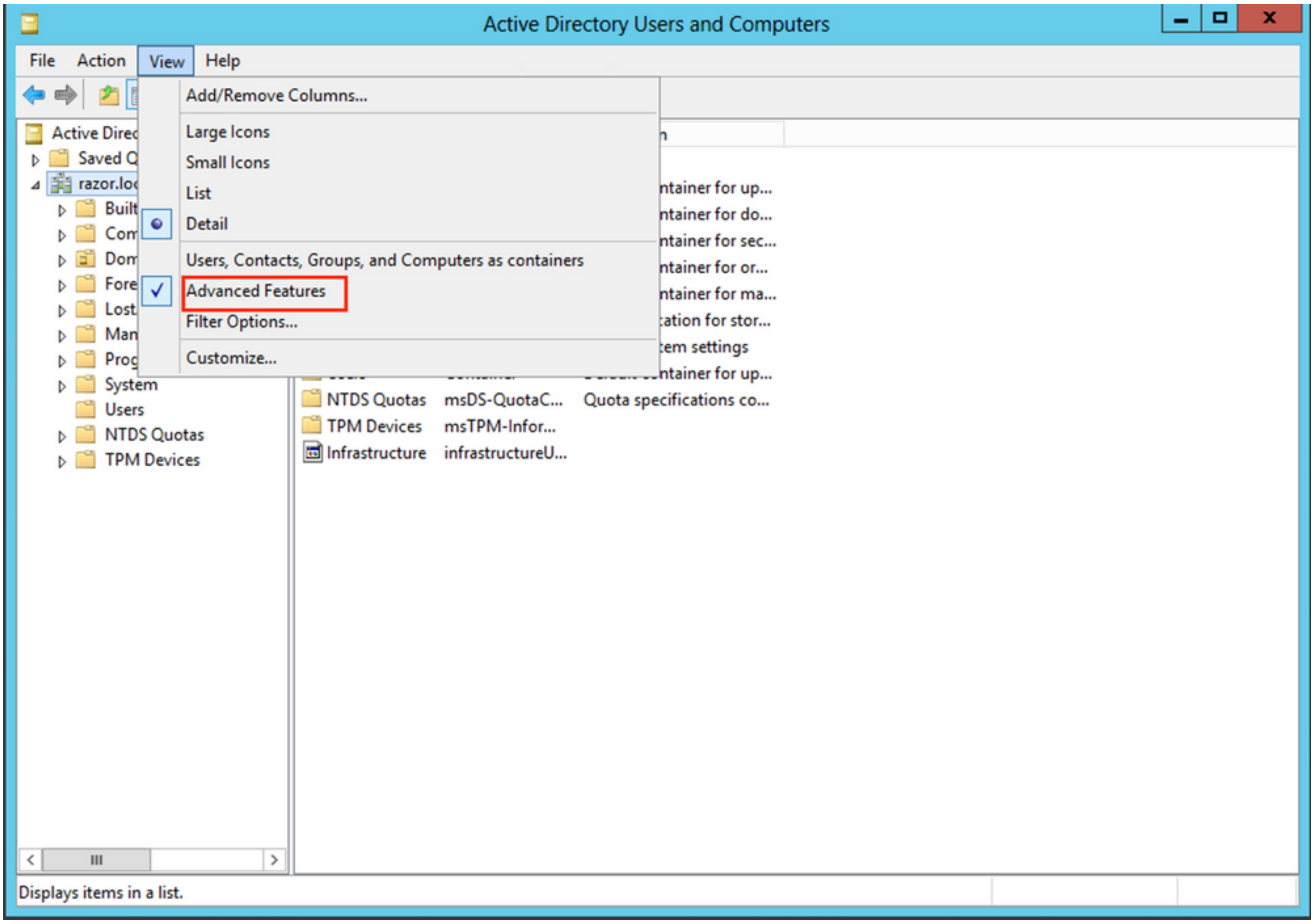
- admin: uma conta de administrador de teste usada para demonstrar a identidade do usuário.

Determinar o DN de base e o DN do grupo do LDAP

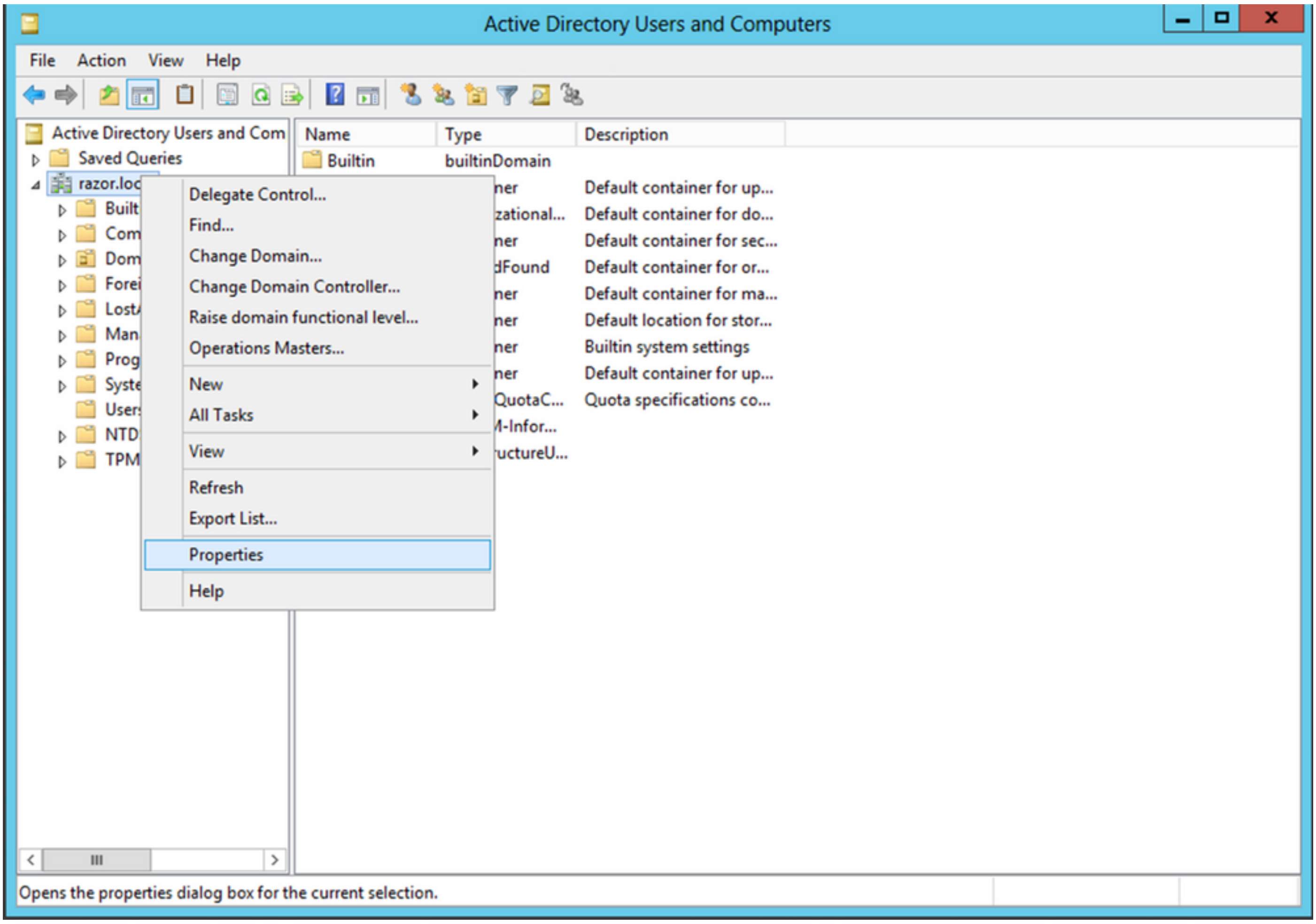
1. Abrir Active Directory Users and Computers através do Painel do Gerenciador do Servidor.


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

2. Abra o View Option no painel superior e ative a opção Advanced Features,conforme mostrado na imagem:



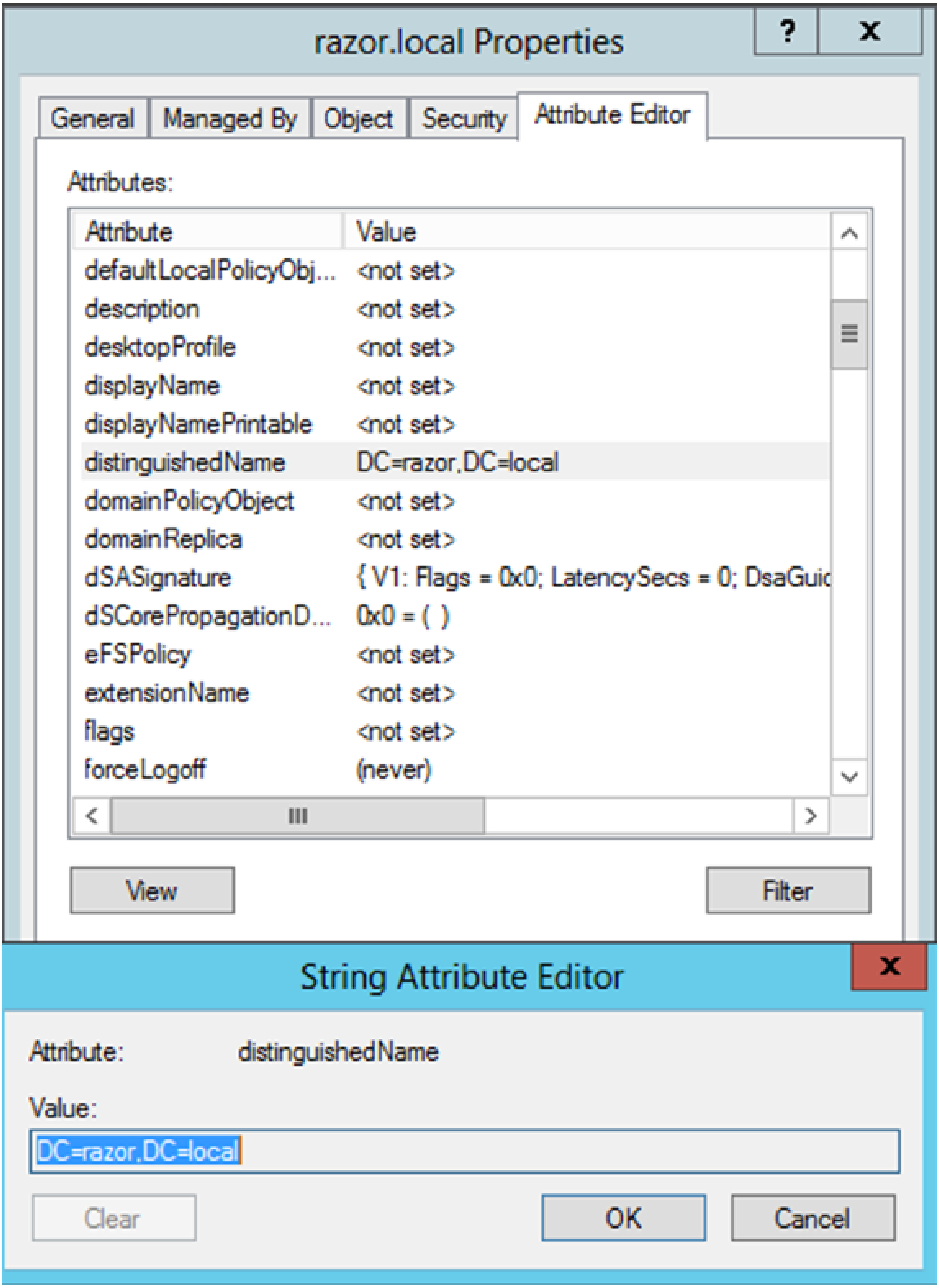
3. Isso permite a exibição de propriedades adicionais sob os objetos do AD.
   Por exemplo, para encontrar o DN da raiz razor.local, clique com o botão direito do mouse razor.locale escolha Properties, como mostrado nesta imagem:


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

4. Sob Properties, escolha o Attribute Editor guia. Localizar distinguishedName em Atributos, clique em View,conforme mostrado na imagem.

Essa ação abre uma nova janela em que o DN pode ser copiado e colado no FMC posteriormente.

Neste exemplo, o DN raiz é DC=razor, DC=local. Copie o valor e salve-o para depois. Clique em OK para sair da janela Editor de atributos de string e clique em OK novamente para sair das Propriedades.



Attributes:

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

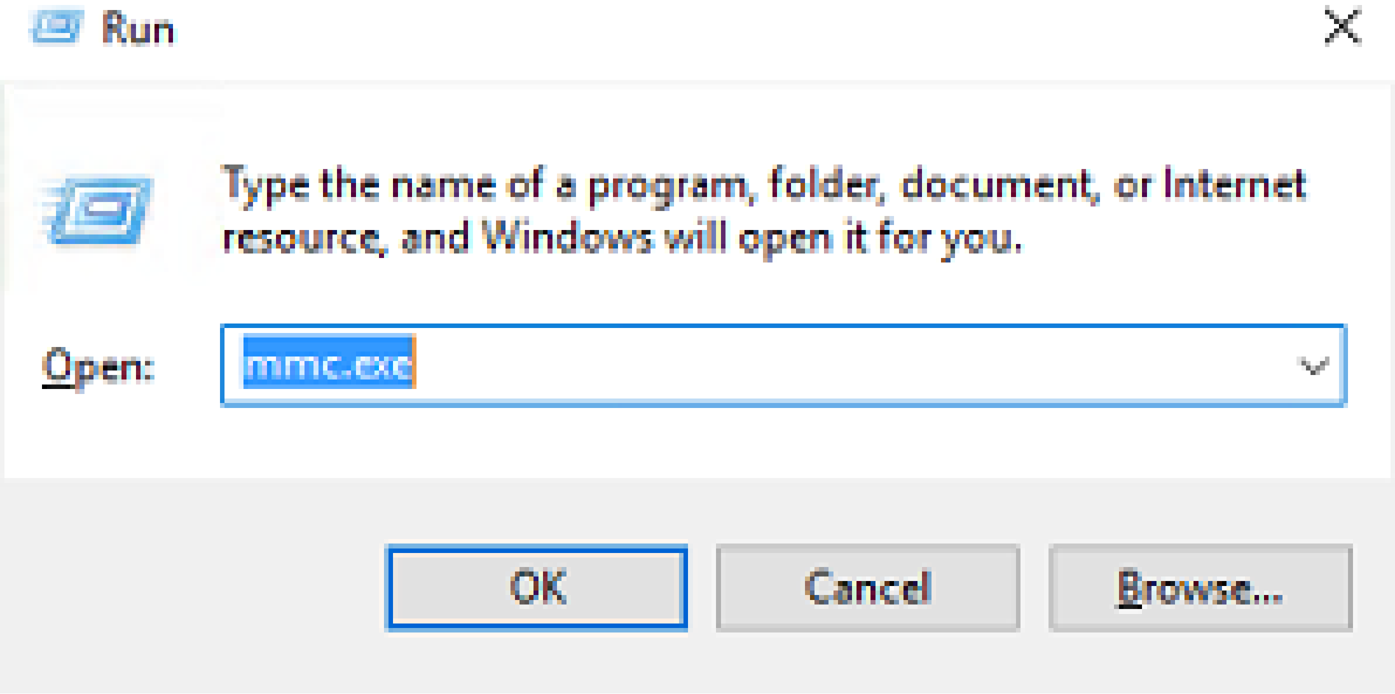
Attribute: distinguishedName

Value:

DC=razor,DC=local

Copiar a Raiz do Certificado SSL LDAPS

1. Pressione Win+R e insira mmc.exee clique em OK, como mostrado nesta imagem.

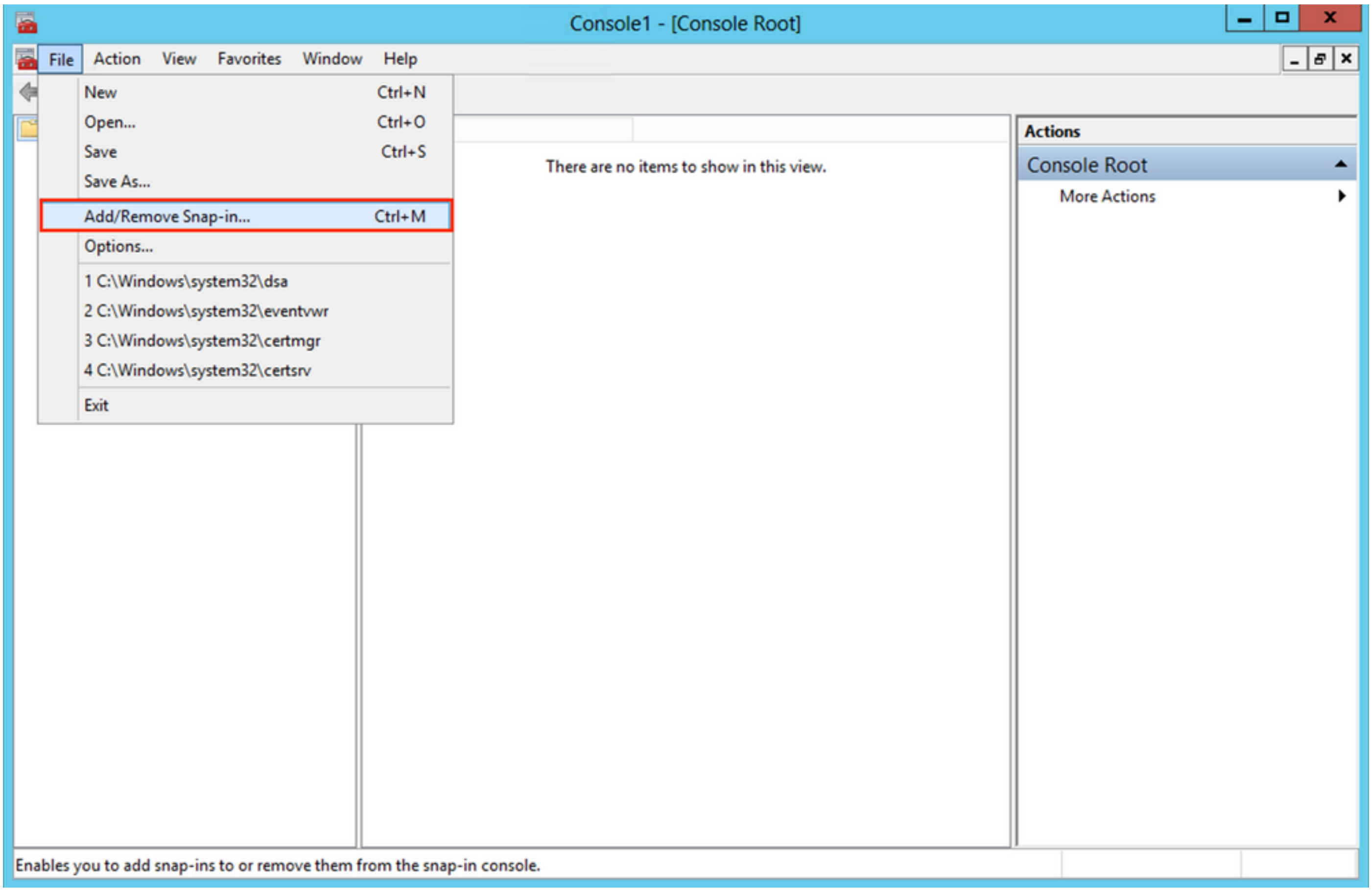


Run

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

Open: mmc.exe

2. Navegue até File > Add/Remove Snap-in..., conforme mostrado nesta imagem:



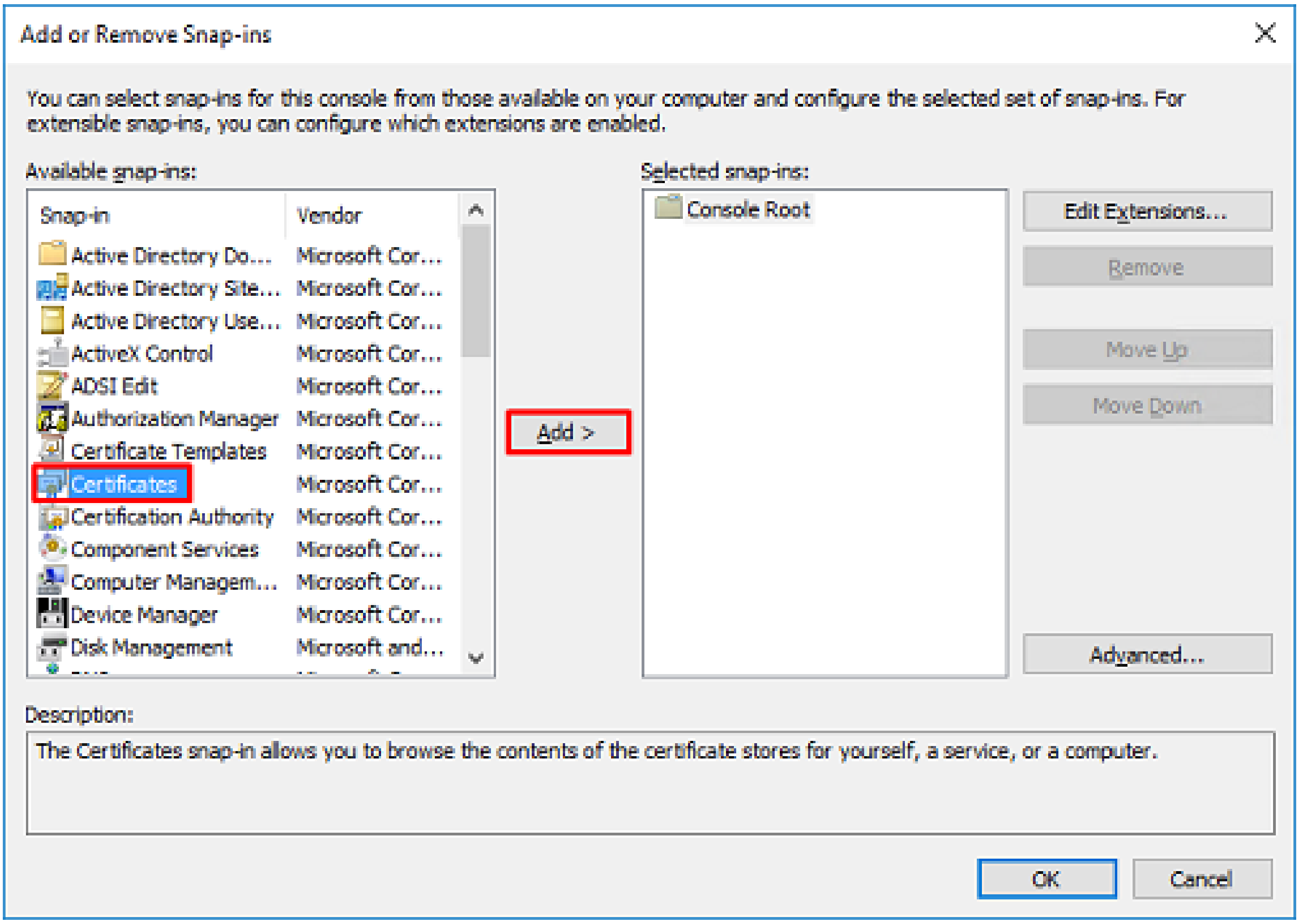
Console1 - [Console Root]

There are no items to show in this view.

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

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

3. Em snap-ins disponíveis, escolha Certificates e clique em Add, como mostrado nesta imagem:



Add or Remove Snap-ins

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

Available snap-ins:

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

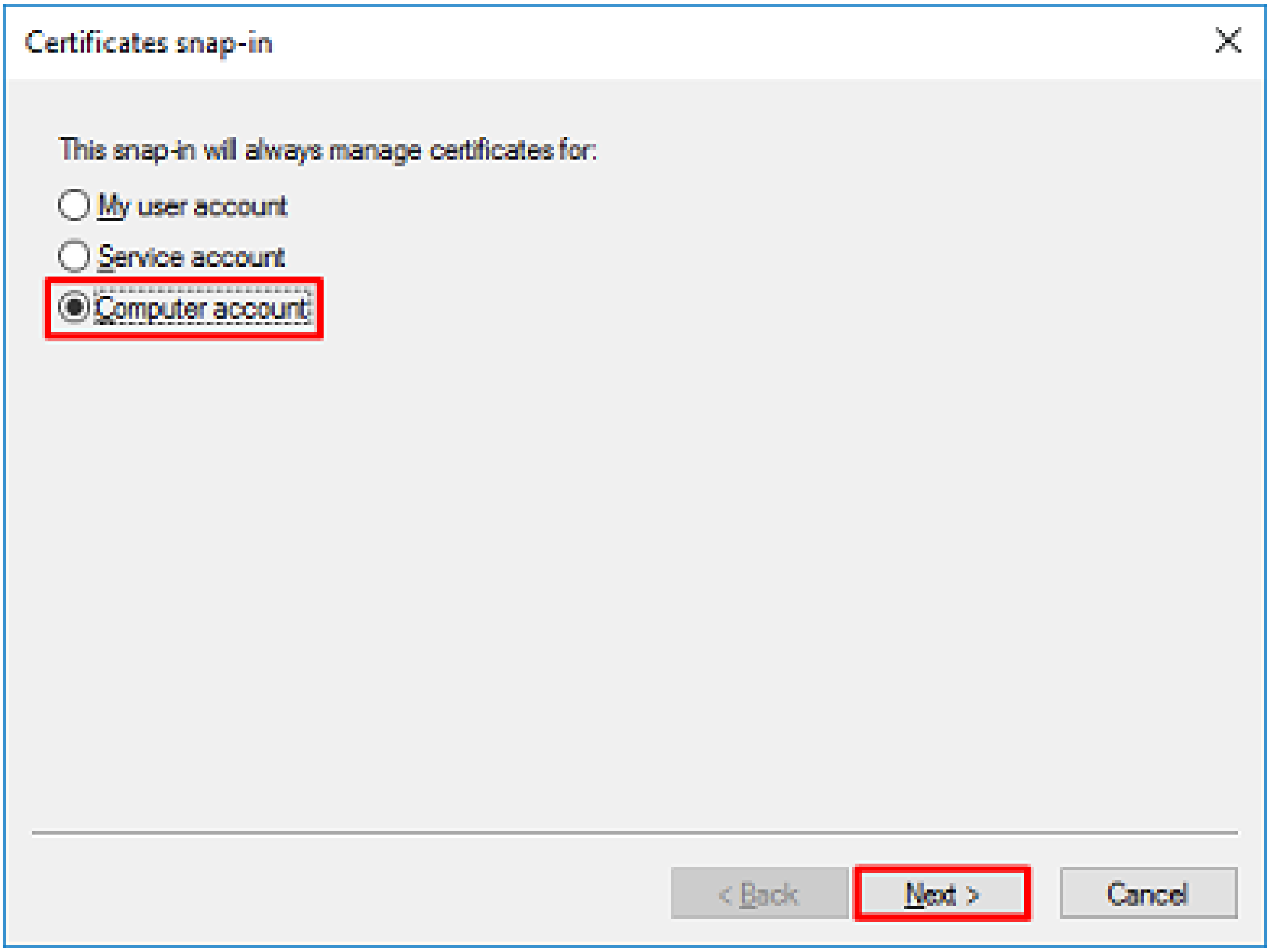
Selected snap-ins:

Console Root

Description:

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

4. Escolher Computer account e clique em Next, como mostrado nesta imagem:



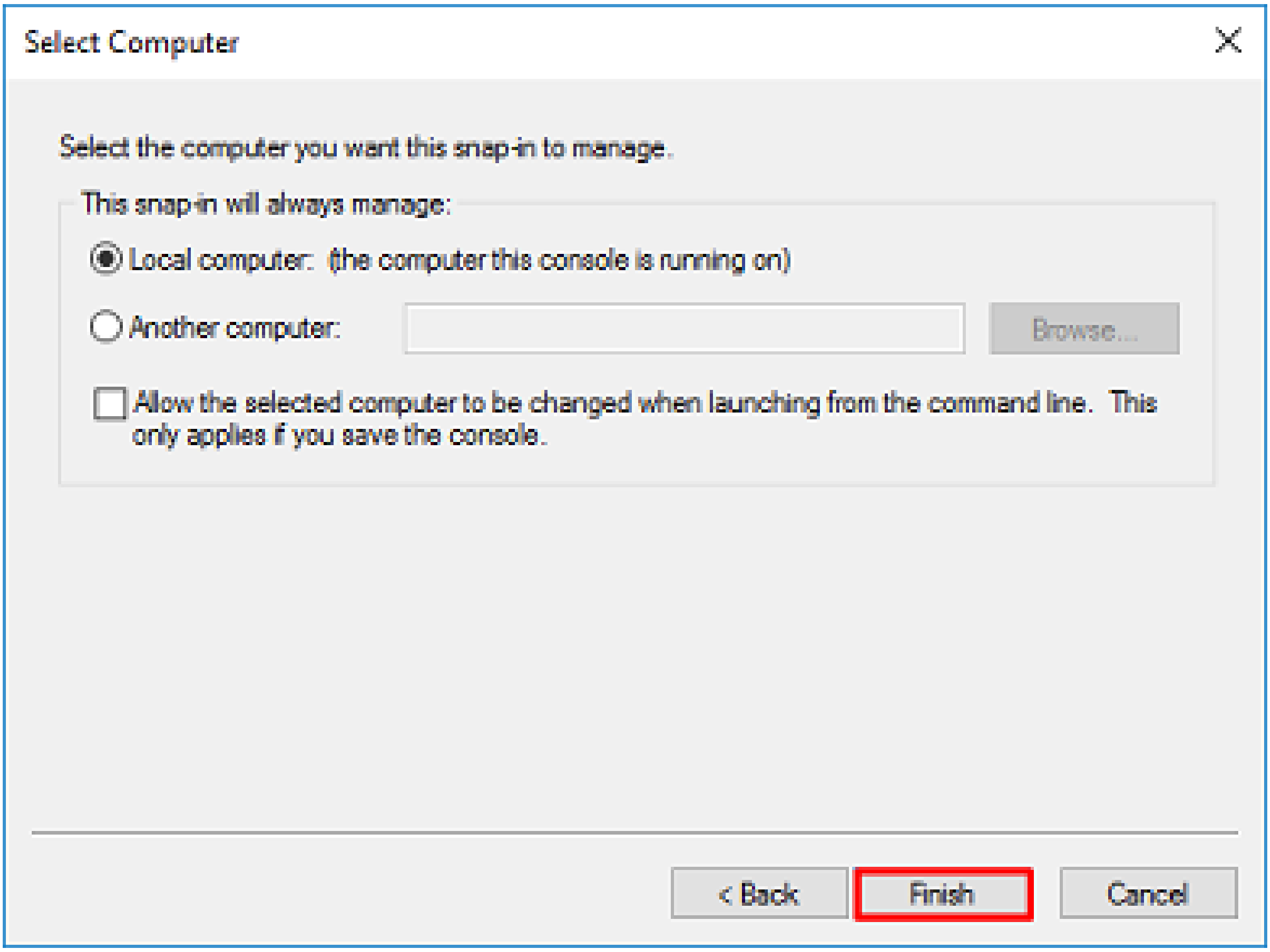
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

Como mostrado aqui, clique em Finish.



Select Computer

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

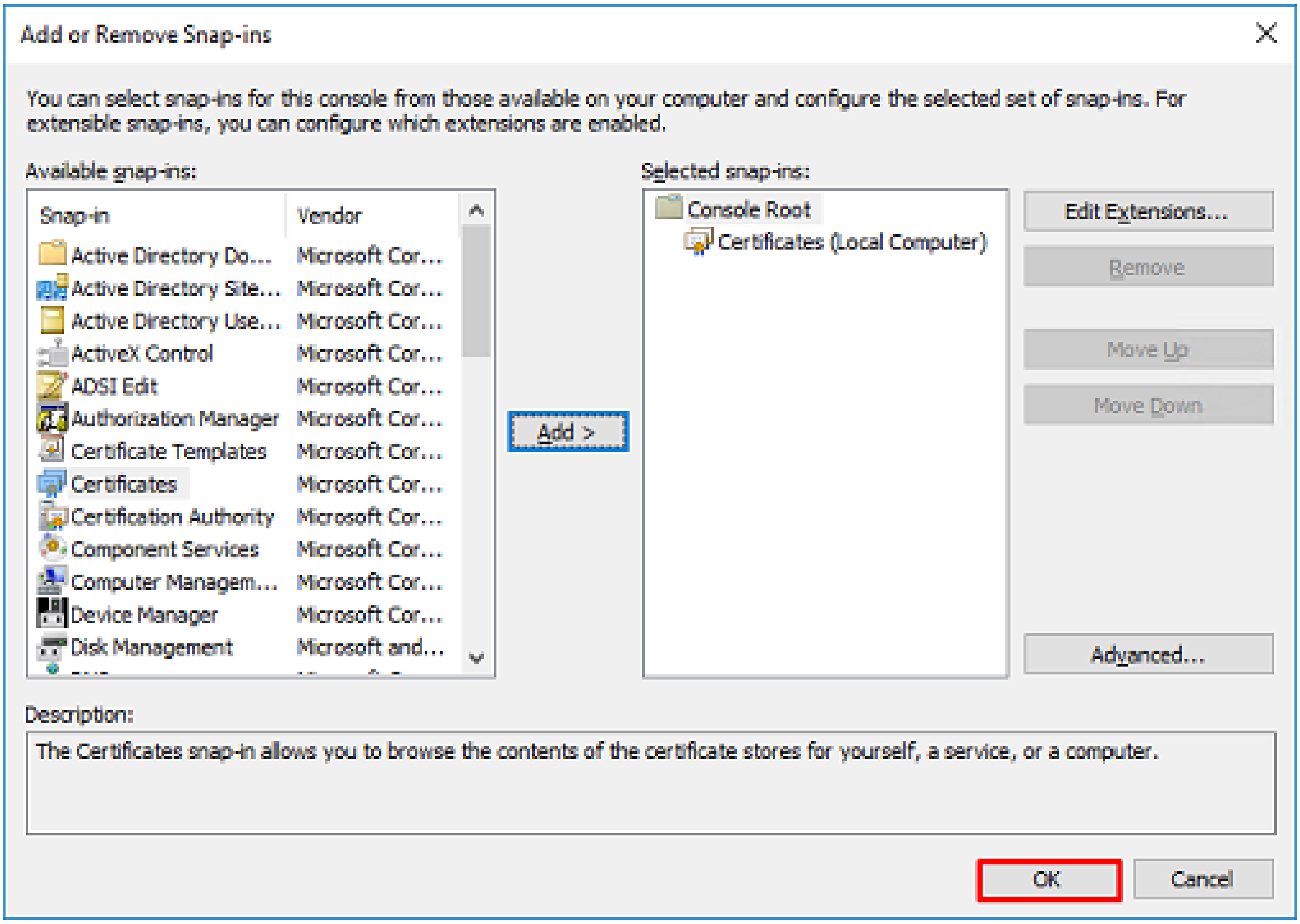
This snap-in will always manage:

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

○ Another computer:

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

5. Agora, clique em OK, como mostrado nesta imagem.



Add or Remove Snap-ins

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

Available snap-ins:

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

Selected snap-ins:

- Console Root
  - Certificates (Local Computer)

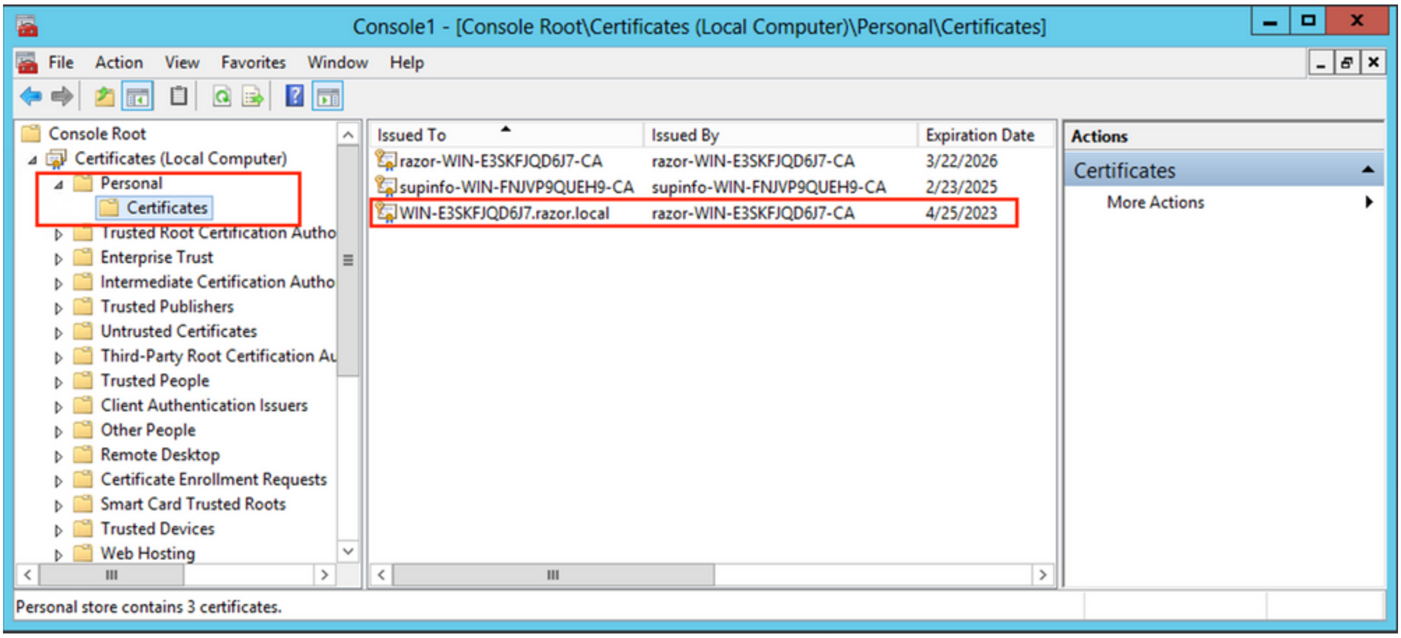
Description:

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

6. Expanda a Personal e clique em Certificates. O certificado usado por LDAPs deve ser emitido para o FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) do servidor Windows. Neste servidor, há três certificados listados:

- Um Certificado CA foi emitido para e por razor-WIN-E3SKFJQD6J7-CA.
- Um certificado CA emitido para e por supinfo-WIN-FNJVP9QUEH9-CA.
- Um certificado de identidade foi emitido para WIN-E3SKFJQD6J7.razor.local por razor-WIN-E3SKFJQD6J7-CA.

Neste guia de configuração, o FQDN é WIN-E3SKFJQD6J7.razor.local e, portanto, os dois primeiros certificados não são válidos para uso como o certificado SSL LDAPs. O certificado de identidade emitido para WIN-E3SKFJQD6J7.razor.local é um certificado que foi emitido automaticamente pelo serviço de CA do Windows Server. Clique duas vezes no certificado para verificar os detalhes.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Client Authentication Issuers
Other People
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Actions
Certificates
More Actions

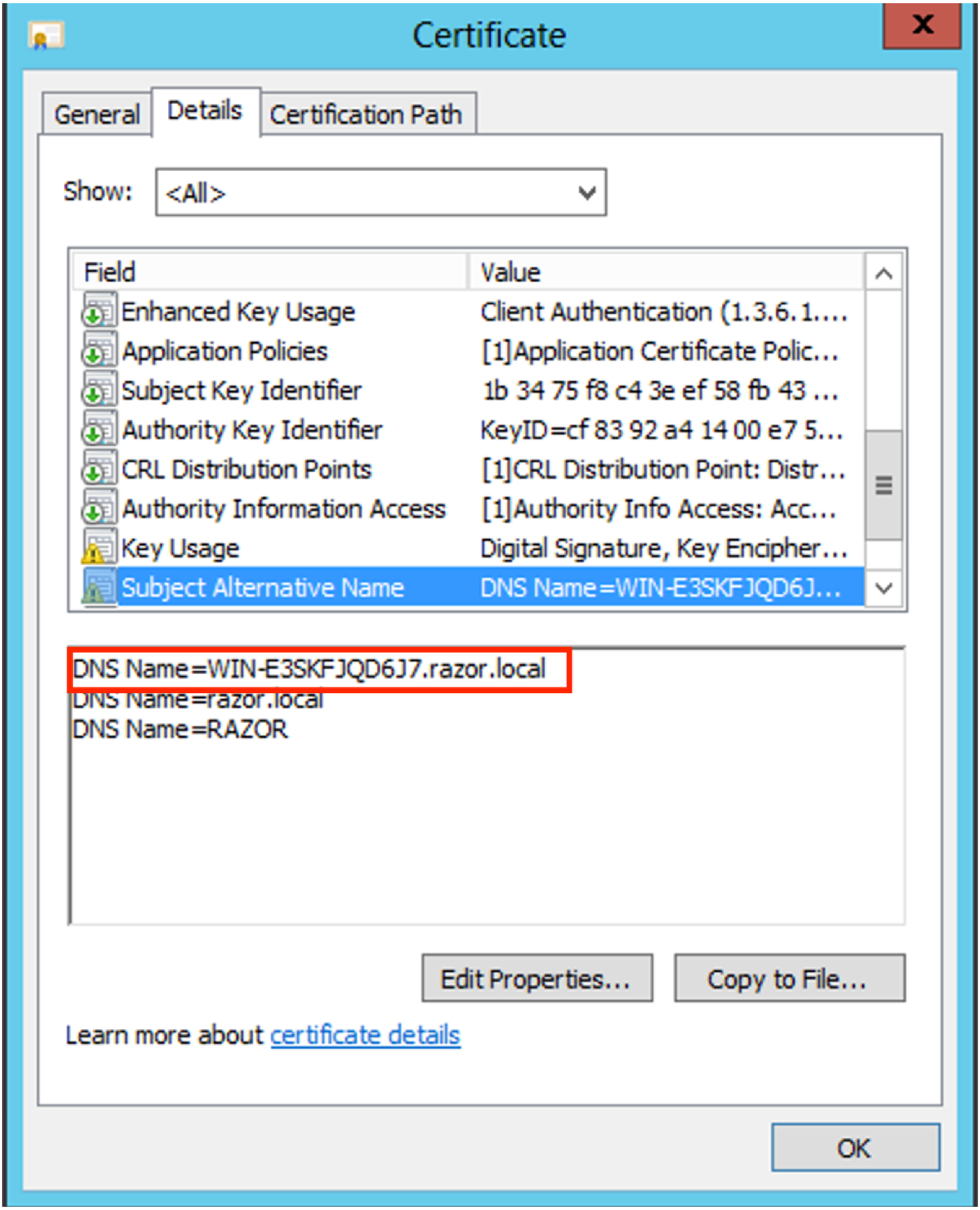
Issued To	Issued By	Expiration Date
razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026
supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	2/23/2025
WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023

Personal store contains 3 certificates.

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

- O nome comum ou nome alternativo do assunto DNS corresponde ao FQDN do Windows Server.
- O certificado tem autenticação de servidor no campo Uso avançado de chave.

Sob o comando Details para o certificado, escolha Subject Alternative Name, onde o FQDN WIN-E3SKFJQD6J7.razor.local está presente.



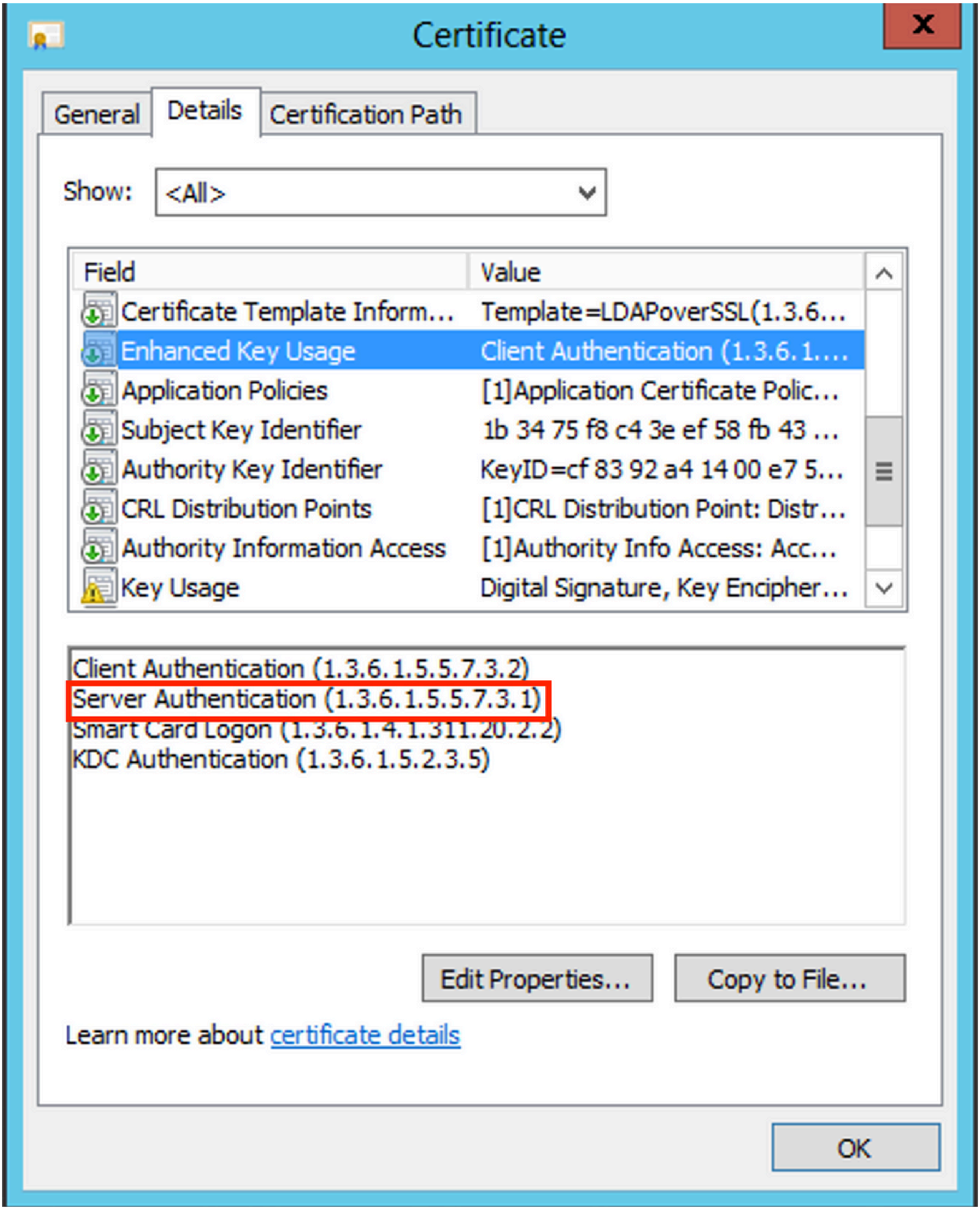
Show: <All>

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

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

Learn more about certificate details

Sob Enhanced Key Usage, Server Authentication está presente.

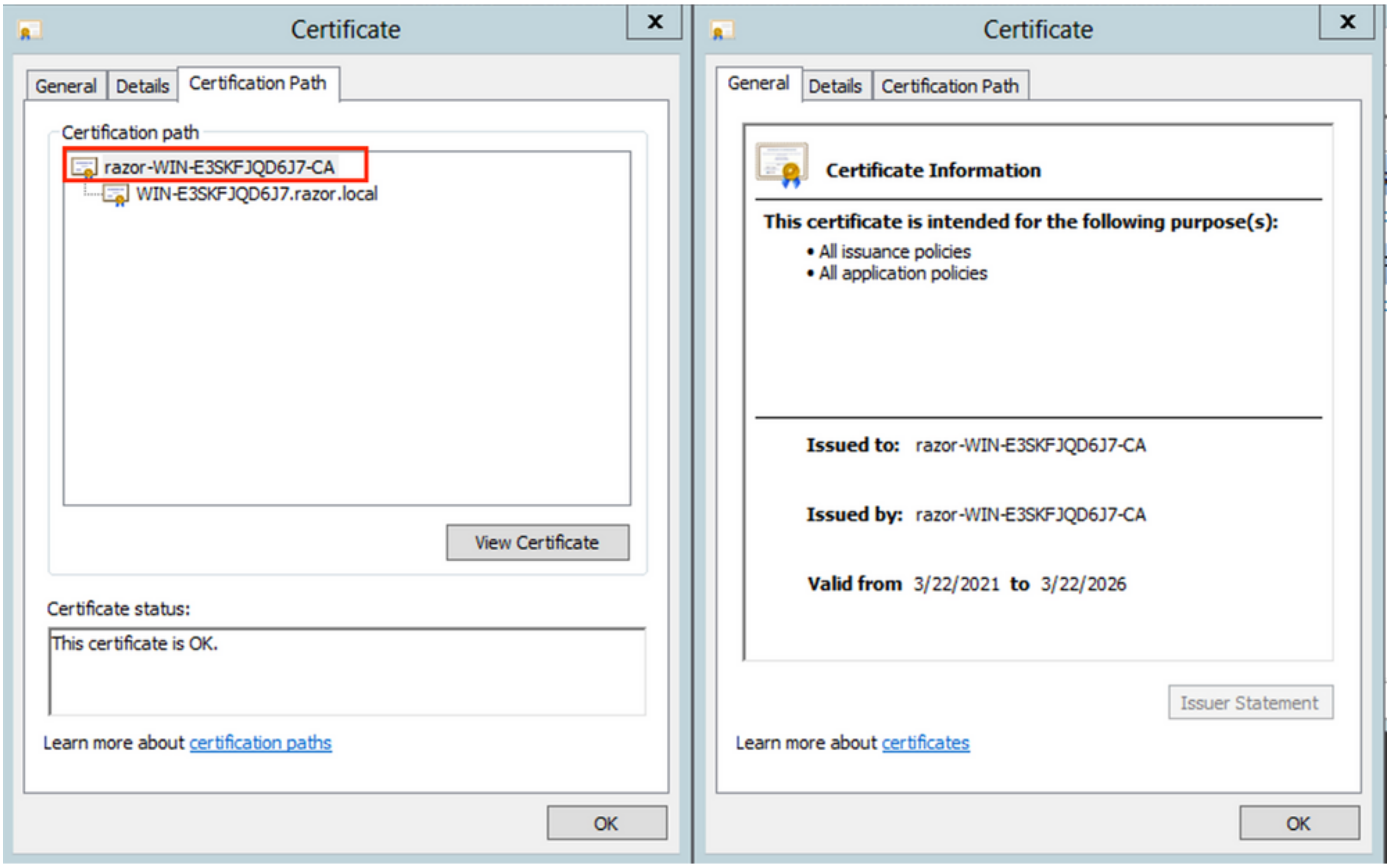


Show: <All>

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

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

8. Uma vez confirmado, sob o comando Certification Path selecione o certificado de nível superior, que é o certificado raiz da CA, e clique em View Certificate. Isso abre os detalhes do certificado para o certificado CA raiz conforme mostrado na imagem:



Certification path

razor-WIN-E3SKFJQD6J7-CA

WIN-E3SKFJQD6J7.razor.local

View Certificate

Certificate status:

This certificate is OK.

Learn more about certification paths

Certificate Information

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

- All issuance policies
- All application policies

Issued to: razor-WIN-E3SKFJQD6J7-CA

Issued by: razor-WIN-E3SKFJQD6J7-CA

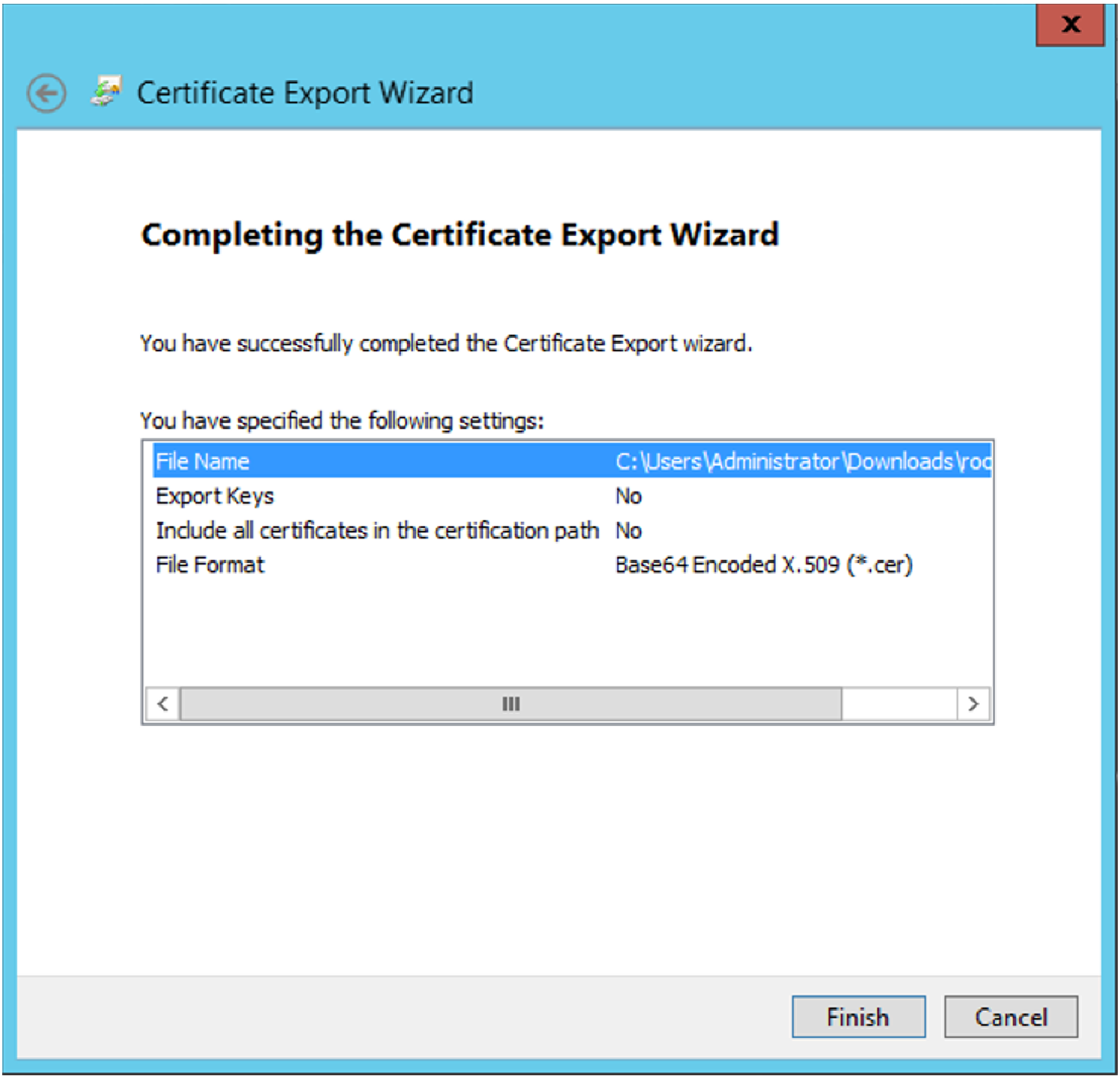
Valid from 3/22/2021 **to** 3/22/2026

Issuer Statement

Learn more about certificates

9. Sob o comando Details do certificado CA raiz, clique em Copy to File e navegue peloCertificate Export Wizard que exporta a CA raiz no formato PEM.

Escolher Base-64 encoded X.509 como o formato do arquivo.



Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

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

10. Abra o certificado de CA raiz armazenado no local selecionado na máquina com um bloco de notas ou algum outro editor de texto.

Essa ação mostra o certificado em formato PEM. Salve-o para usar mais tarde.

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgo
vcjEhMB8GA1UEAxMYcmF6b3ItV0lOLUUzU0tGSlFENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCg
BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvc
CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnblxwtXOB2G4UxZ3LRrWznjXaS02Rc3qVw4lnOAziGs4ZMNM1X8UWeKuwi8
9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU3OaiiI/tp422ydy3Kgl7Iqt1s4XqpZmTezykWra7dUyXfkuESk6lEOAV
CSkTQTRXYryy8dJrWjAF/n6A3VnS/l7Uhujlx4CD2OBkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwE
DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFM+DkqQUA0dY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSI
AA4IBAQCiSm5U7U6Y7zXdx+dleJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7BnO6f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q
4sMZffbVrGlRz7twWY36J5G5vhNUhzZ1N2OLw6wtHg2SO8XlvpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nrylb
GuDsepY7/u2uWfy/vpTJigeok2DH6HFfOET3sE+7rsIAY+of0kWW5gNwQ4hOwv4Goqj+YQRAXXi2OZyltHR1dfUUbwVENSFQtDnFA7X
```

```
-----END CERTIFICATE-----
```

No caso de vários certificados instalados no armazenamento do computador local no servidor LDAPs (opcional)

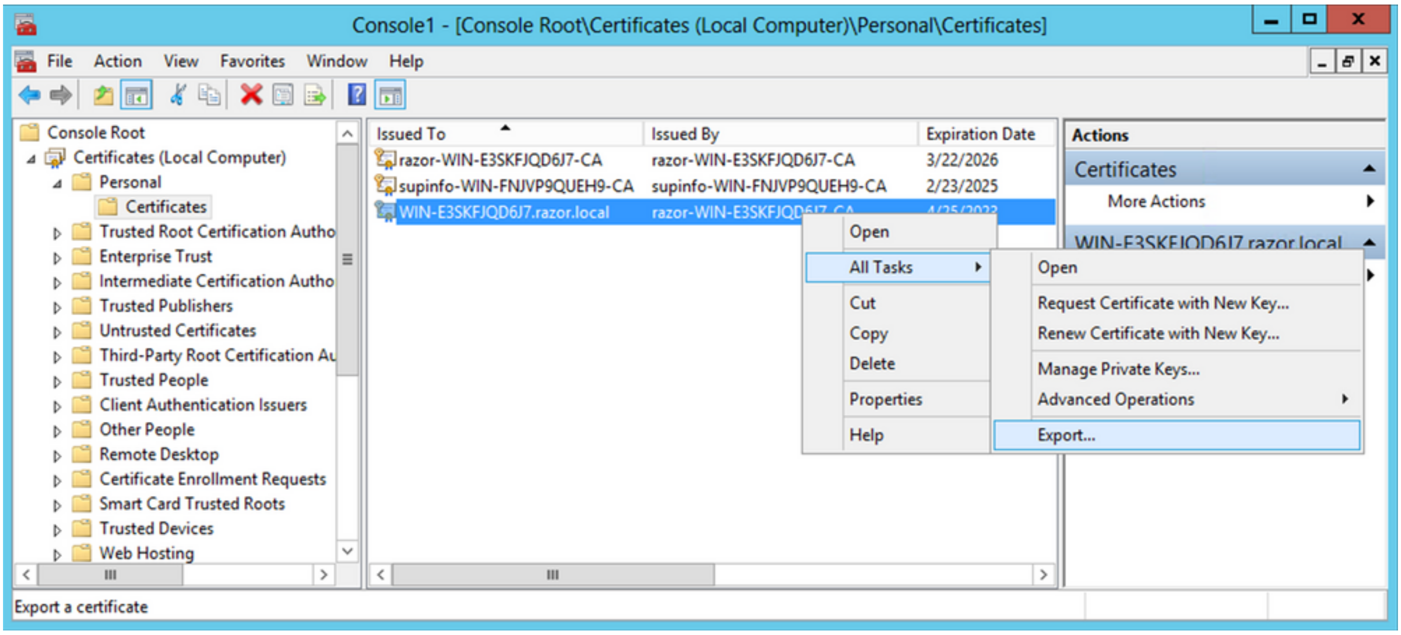
1. Numa situação de múltiplos certificados de identificação que podem ser utilizados pelo LDAPS e quando há incerteza quanto ao que é utilizado, ou quando não há acesso ao servidor LDAPS, ainda é possível extrair a AC raiz de uma captura de pacotes efetuada no FTD.

2. Caso você tenha vários certificados válidos para Autenticação de Servidor no servidor LDAP (como o controlador de domínio do AD DS) armazenamento de certificados de computador local, observe que um certificado diferente é usado para comunicações LDAPS. A melhor solução para esse problema é remover todos os certificados desnecessários do repositório de certificados do computador local e ter apenas um certificado válido para a autenticação do servidor.

No entanto, se houver um motivo legítimo para você exigir dois ou mais certificados e ter pelo menos um servidor LDAP do Windows Server 2008, o armazenamento de certificados dos Serviços de Domínio Ative Diretory (NTDS\Personal) poderá ser usado para comunicações LDAPs.

Estas etapas demonstram como exportar um certificado habilitado para LDAPS de um repositório de certificados do computador local do controlador de domínio para o repositório de certificados do serviço dos Serviços de Domínio Ative Diretory (NTDS\Personal).

- Navegue até o console MMC no servidor do Ative Diretory, escolha Arquivo e clique em Add/Remove Snap-in.
- Clique em Certificates e clique em Add.
- No Certificates snap-in, escolha Computer account e clique em Next.
- IN Select Computer, escolha Local Computer, clique em OKe clique em Finish. IN Add or Remove Snap-ins, clique em OK.
- No console de certificados de um computador que contém um certificado usado para Autenticação de Servidor, clique com o botão direito do mouse no certificate, clique em All Taskse clique em Export.



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

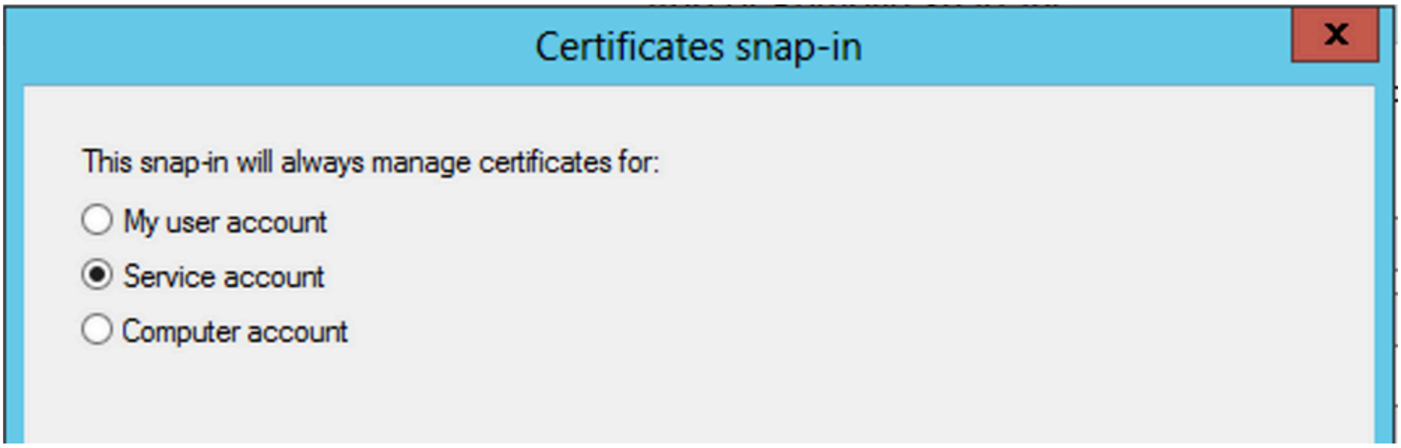
Issued To	Issued By	Expiration Date
razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026
supinfo-WIN-FNJVP9QUEH9-CA	supinfo-WIN-FNJVP9QUEH9-CA	2/23/2025
WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023

Export a certificate

- Exportar o certificado no pfx nas seções subsequentes. Consulte este artigo sobre como exportar um certificado no pfx formato do MMC:

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

- Quando a exportação do certificado for concluída, navegue até Add/Remove Snap-in ligado MMC console. Clique em Certificates e clique em Add.
- Escolher Service account e clique em Next.



Certificates snap-in

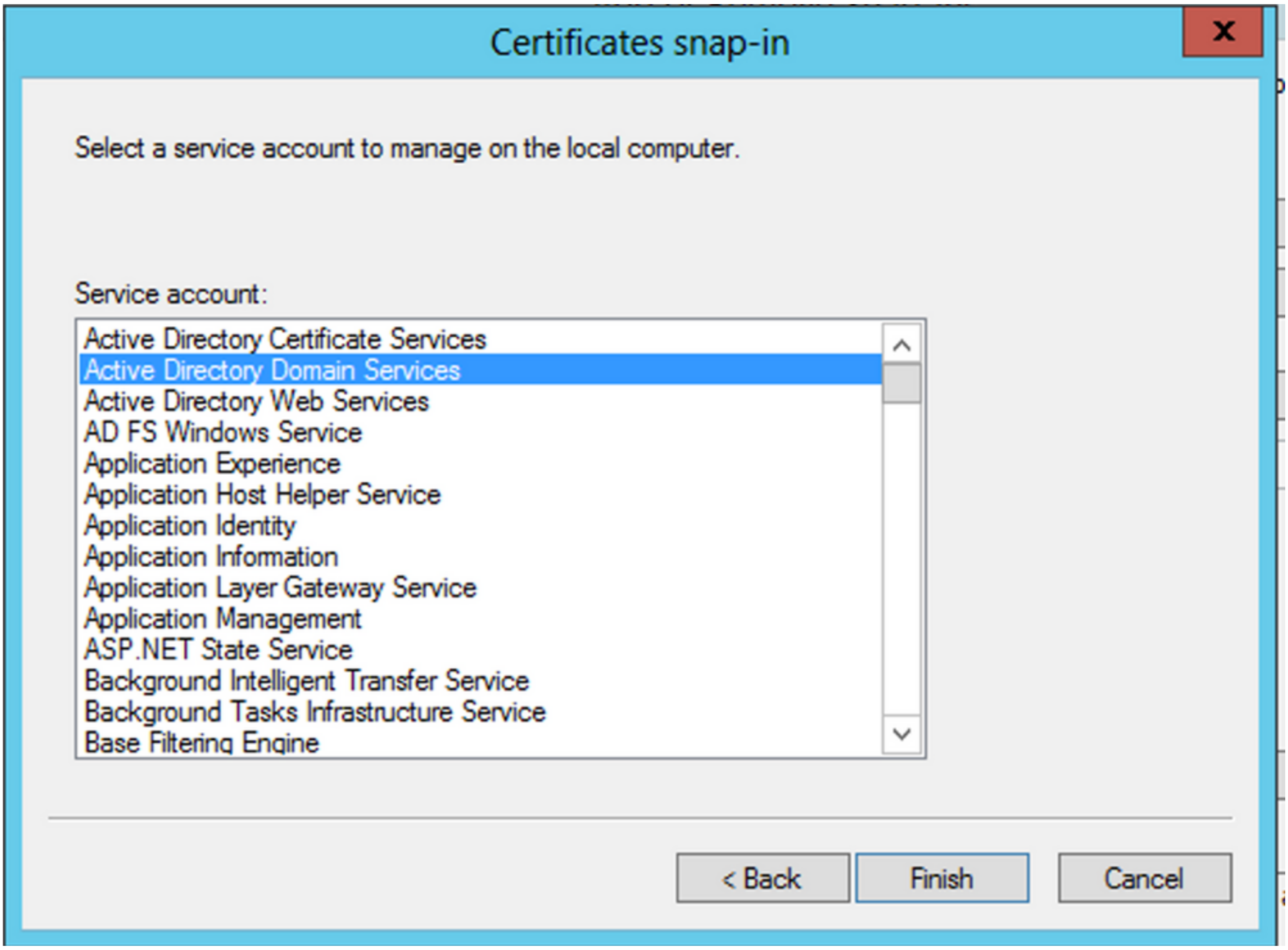
This snap-in will always manage certificates for:

○ My user account

● Service account

○ Computer account

- No Select Computer , escolha Local Computer e clique em Next.
- Escolher Active Directory Domain Services e clique em Finish.



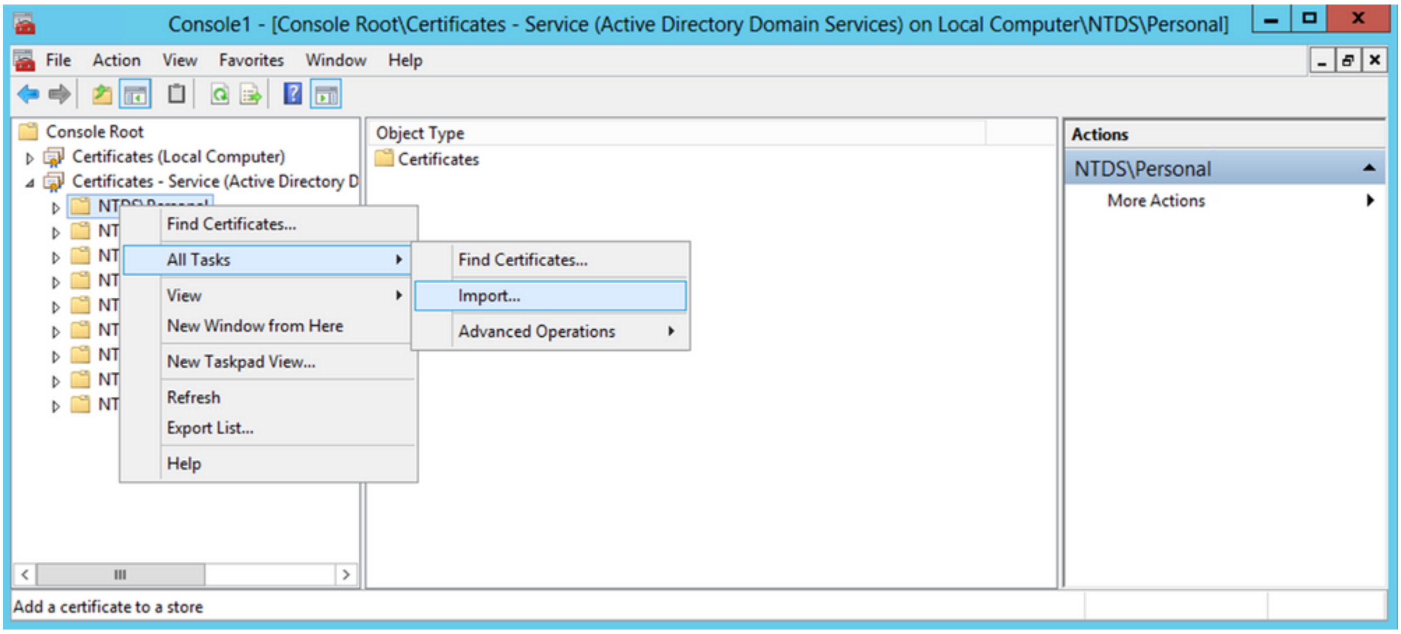
Certificates snap-in

Select a service account to manage on the local computer.

Service account:

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

- Na guia Add/Remove Snap-ins , clique em OK.
- Expandir Certificates - Services (Active Directory Domain Services) e clique em NTDS\Personal.
- Clique com o botão direito do mouse NTDS\Personal, clique em All Taskse clique em Import.



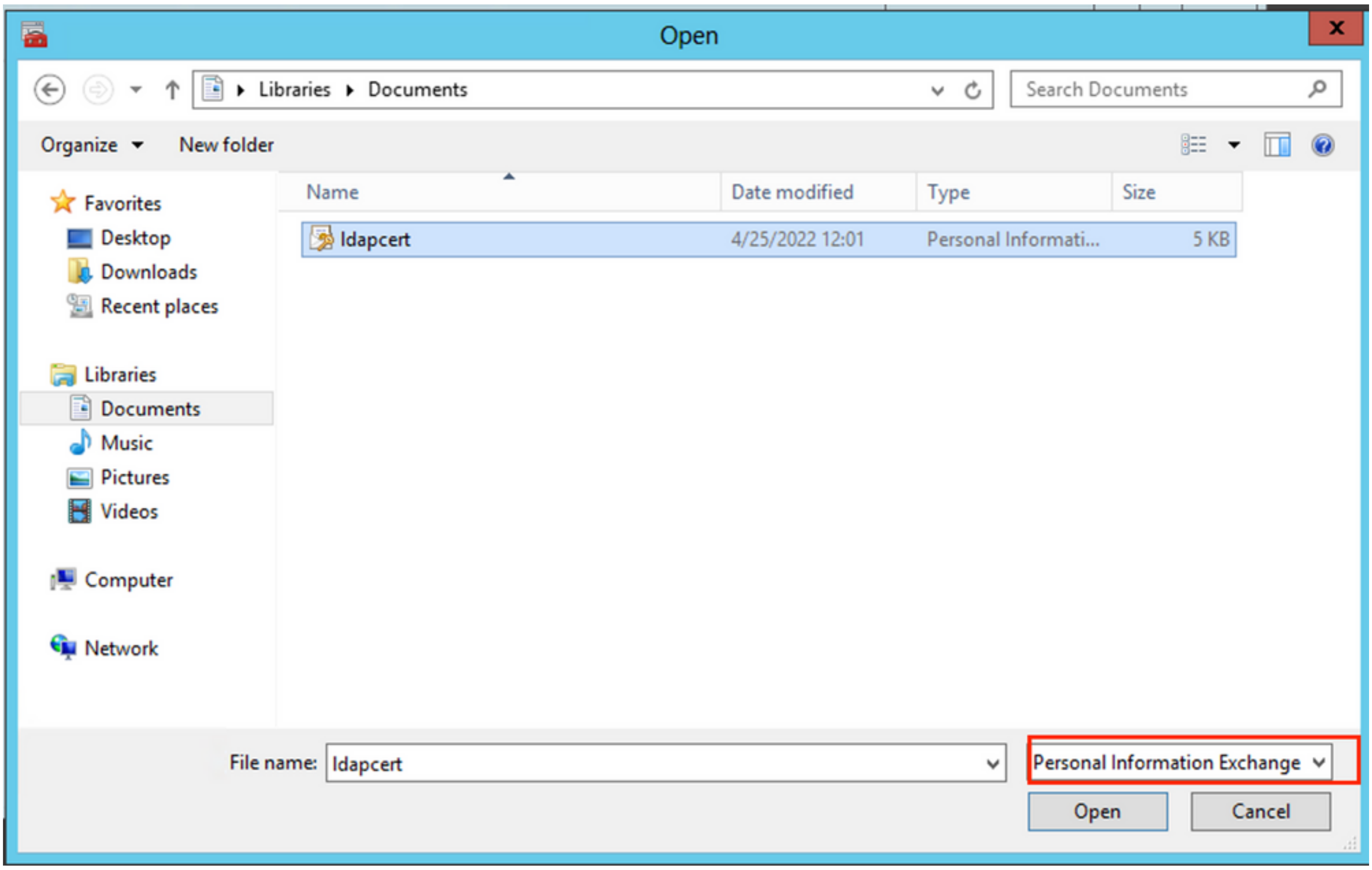
Console1 - [Console Root\Certificates - Service (Active Directory Domain Services) on Local Computer\NTDS\Personal]

Add a certificate to a store

- Na guia Certificate Import Wizard bem-vindo, clique em Next.

- Na tela Arquivo a ser importado, clique em Browsee localize o arquivo de certificado que você exportou anteriormente.

- Na tela Aberta, verifique se a opção Troca de informações pessoais (*pfx,*.p12) é selecionado como o tipo de arquivo e, em seguida, navegue pelo sistema de arquivos para localizar o certificado exportado anteriormente. Em seguida, clique nesse certificado.



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

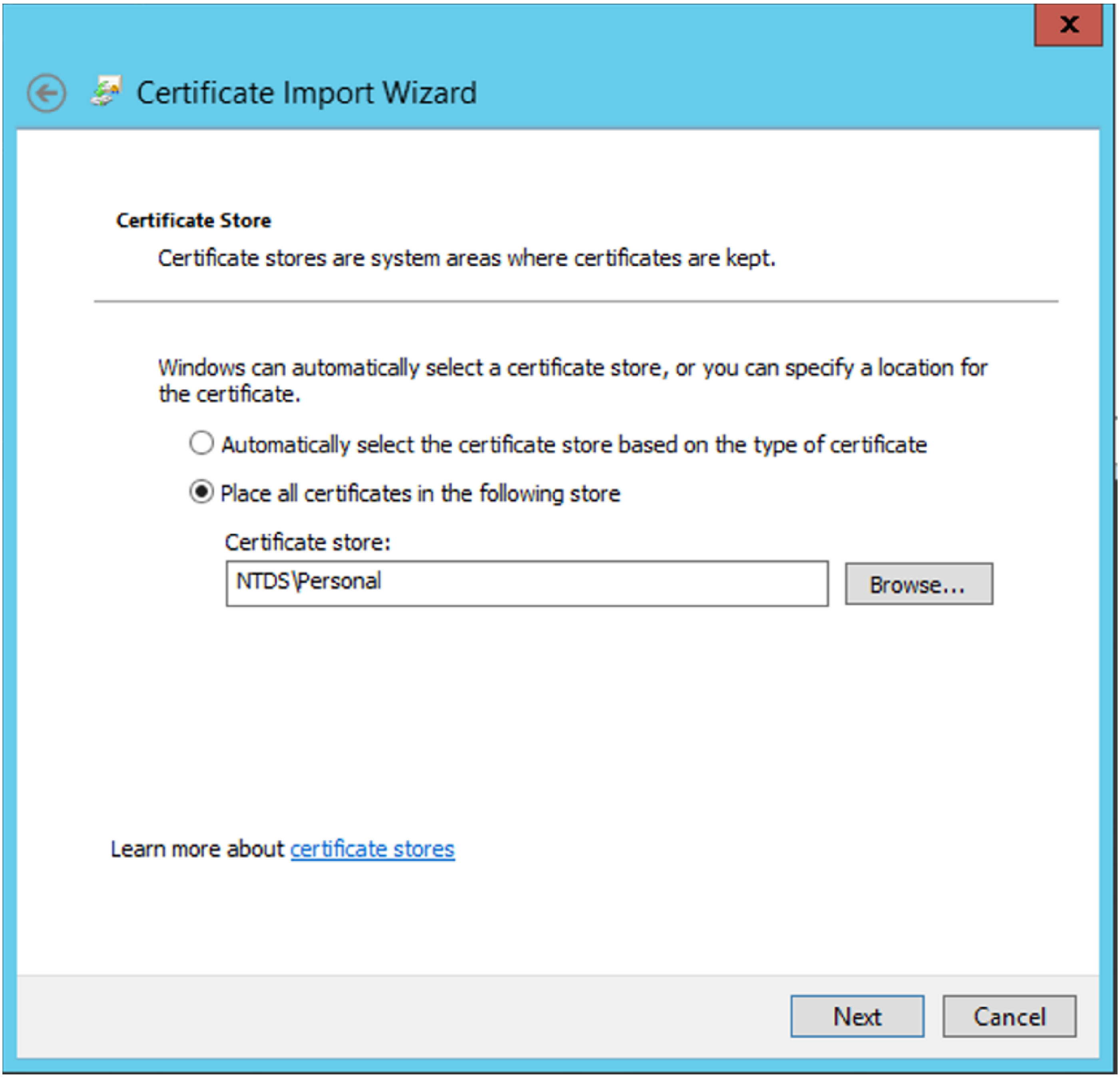
File name: ldapcert

Personal Information Exchange

- Clique em Open e clique em Next.

- Na tela Senha, digite a senha definida para o arquivo e clique em Next.

- Na página Repositório de Certificados, certifique-se de que a opção Colocar todos os certificados esteja selecionada e leia Repositório de Certificados: NTDS\Personal e clique em Next.



Certificate Store

Certificate stores are system areas where certificates are kept.

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

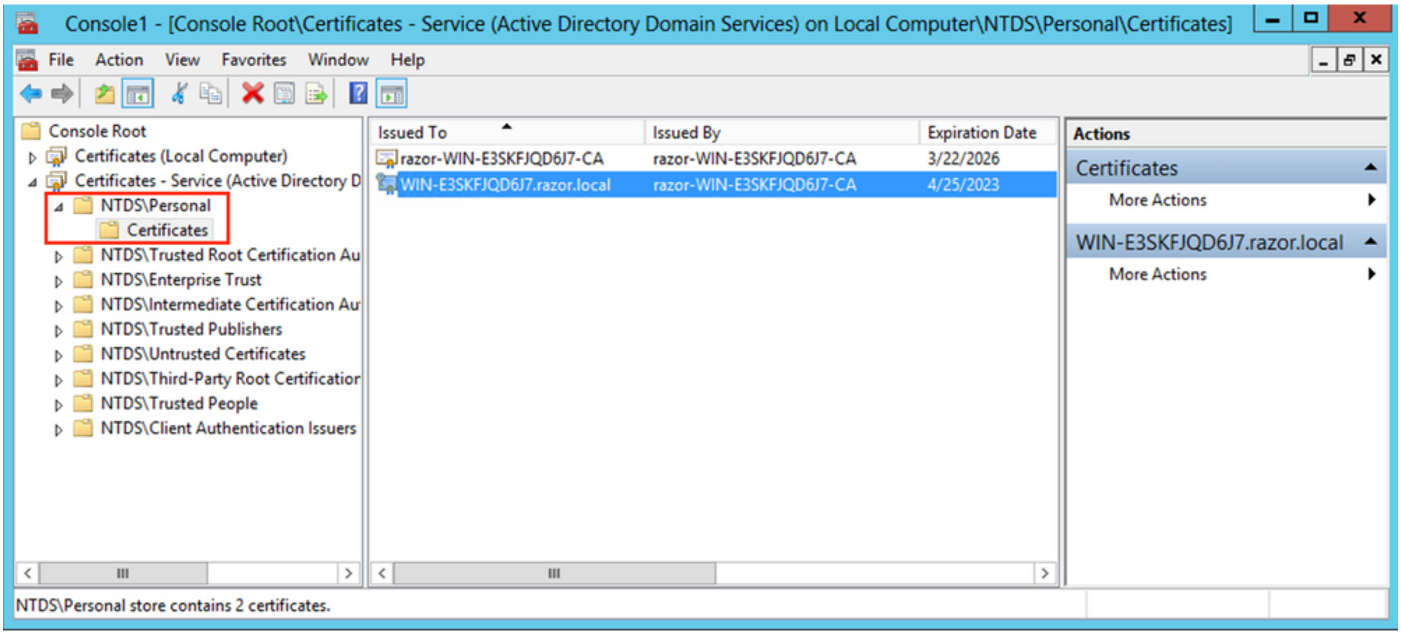
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: NTDS\Personal

Learn more about certificate stores

- Na guia Certificate Import Wizard de conclusão, clique em Finish. Em seguida, você verá uma mensagem de que a importação foi bem-sucedida. Clique em OK. Verifica-se que o certificado foi importado no armazenamento de certificados: NTDS\Personal.



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

- Console Root
  - Certificates (Local Computer)
  - Certificates - Service (Active Directory D
    - NTDS\Personal
      - Certificates
    - NTDS\Trusted Root Certification Au
    - NTDS\Enterprise Trust
    - NTDS\Intermediate Certification Au
    - NTDS\Trusted Publishers
    - NTDS\Untrusted Certificates
    - NTDS\Third-Party Root Certificatior
    - NTDS\Trusted People
    - NTDS\Client Authentication Issuers

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

NTDS\Personal store contains 2 certificates.

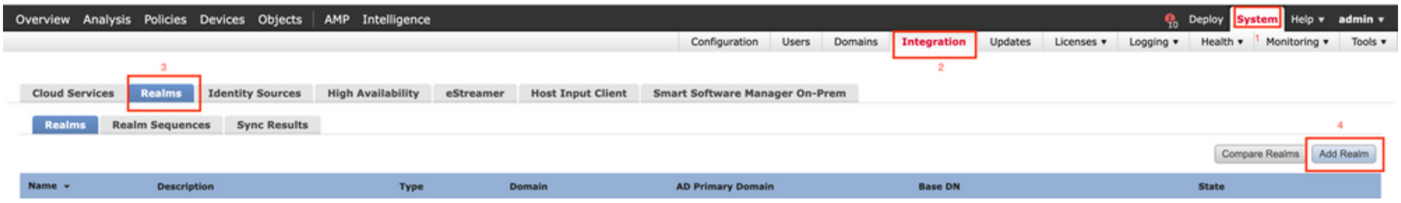
Configurações do FMC

Verificar licenciamento

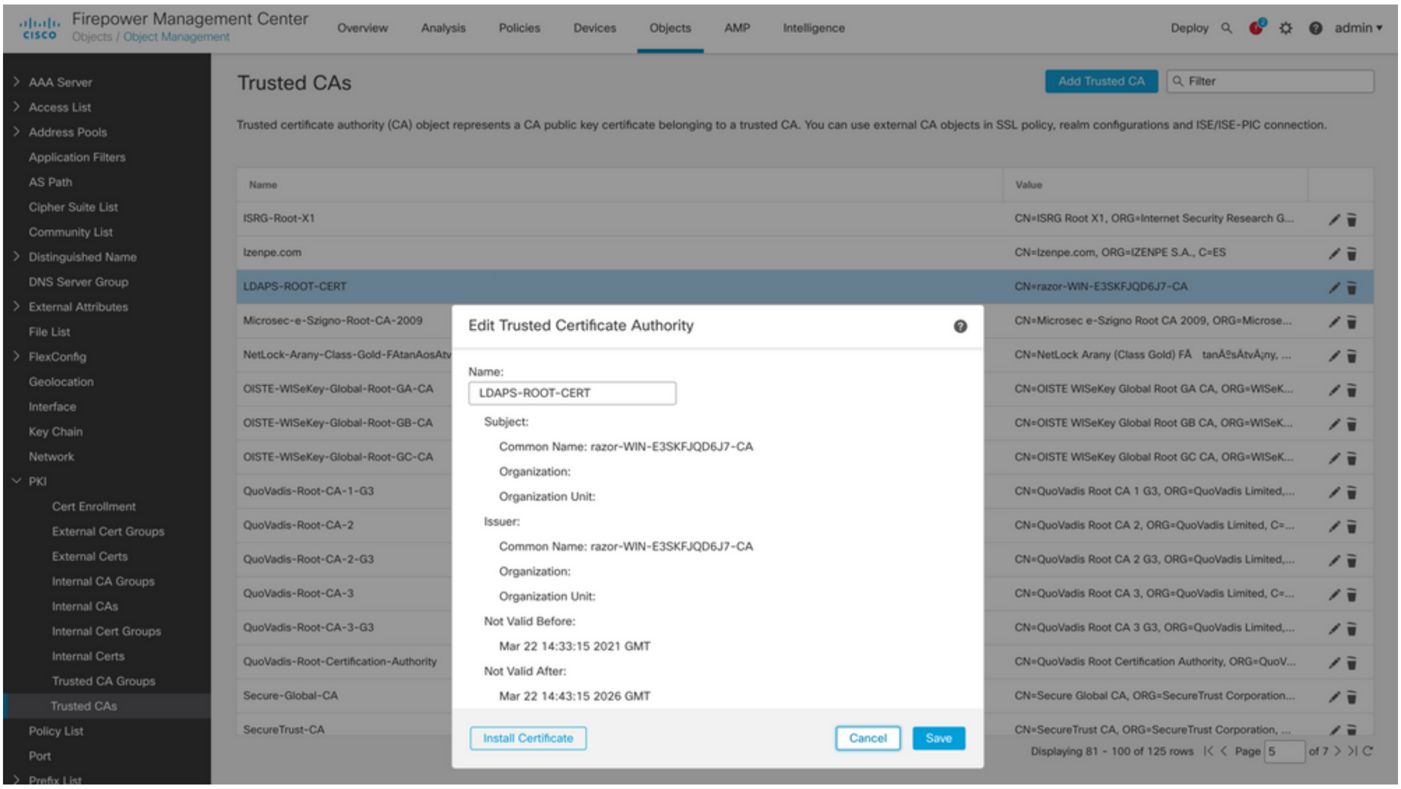
Para implantar a configuração do AnyConnect, o FTD deve ser registrado com o servidor de licenciamento inteligente e uma licença Plus, Apex ou VPN Only válida deve ser aplicada ao dispositivo.

Configurar realm

1. Navegue até System > Integration. Navegue até Realmse clique em Add Realm, como mostrado nesta imagem:



2. Preencha os campos exibidos com base nas informações coletadas do servidor Microsoft para LDAPs. Antes disso, importe o Certificado de CA raiz que assinou o certificado do serviço LDAP no Windows Server em Objects > PKI > Trusted CAs > Add Trusted CA, como é referenciado noDirectory Server Configuration do território. Depois de concluído, clique em OK.



Trusted CAs

Trusted certificate authority (CA) object represents a CA public key certificate belonging to a trusted CA. You can use external CA objects in SSL policy, realm configurations and ISE/ISE-PIC connection.

Name	Value
ISRG-Root-X1	CN=ISRG Root X1, ORG=Internet Security Research G...
Izenpe.com	CN=Izenpe.com, ORG=IZENPE S.A., C=ES
LDAPS-ROOT-CERT	CN=razor-WIN-E3SKFJQD6J7-CA
Microsec-e-Szigno-Root-CA-2009	CN=Microsec e-Szigno Root CA 2009, ORG=Microse...
NetLock-Arany-Class-Gold-FAtanAosAtv	CN=NetLock Arany (Class Gold) FÅ tanÅºsÃtvÃ¡ny, ...
OISTE-WISeKey-Global-Root-GA-CA	CN=OISTE WISeKey Global Root GA CA, ORG=WISeK...
OISTE-WISeKey-Global-Root-GB-CA	CN=OISTE WISeKey Global Root GB CA, ORG=WISeK...
OISTE-WISeKey-Global-Root-GC-CA	CN=OISTE WISeKey Global Root GC CA, ORG=WISeK...
QuoVadis-Root-CA-1-G3	CN=QuoVadis Root CA 1 G3, ORG=QuoVadis Limited,...
QuoVadis-Root-CA-2	CN=QuoVadis Root CA 2, ORG=QuoVadis Limited, C=...
QuoVadis-Root-CA-2-G3	CN=QuoVadis Root CA 2 G3, ORG=QuoVadis Limited,...
QuoVadis-Root-CA-3	CN=QuoVadis Root CA 3, ORG=QuoVadis Limited, C=...
QuoVadis-Root-CA-3-G3	CN=QuoVadis Root CA 3 G3, ORG=QuoVadis Limited,...
QuoVadis-Root-Certification-Authority	CN=QuoVadis Root Certification Authority, ORG=QuoV...
Secure-Global-CA	CN=Secure Global CA, ORG=SecureTrust Corporation...
SecureTrust-CA	CN=SecureTrust CA, ORG=SecureTrust Corporation, ...

Displaying 81 - 100 of 125 rows Page 5 of 7

Edit Trusted Certificate Authority

Name: LDAPS-ROOT-CERT

Subject:

Common Name: razor-WIN-E3SKFJQD6J7-CA

Organization:

Organization Unit:

Issuer:

Common Name: razor-WIN-E3SKFJQD6J7-CA

Organization:

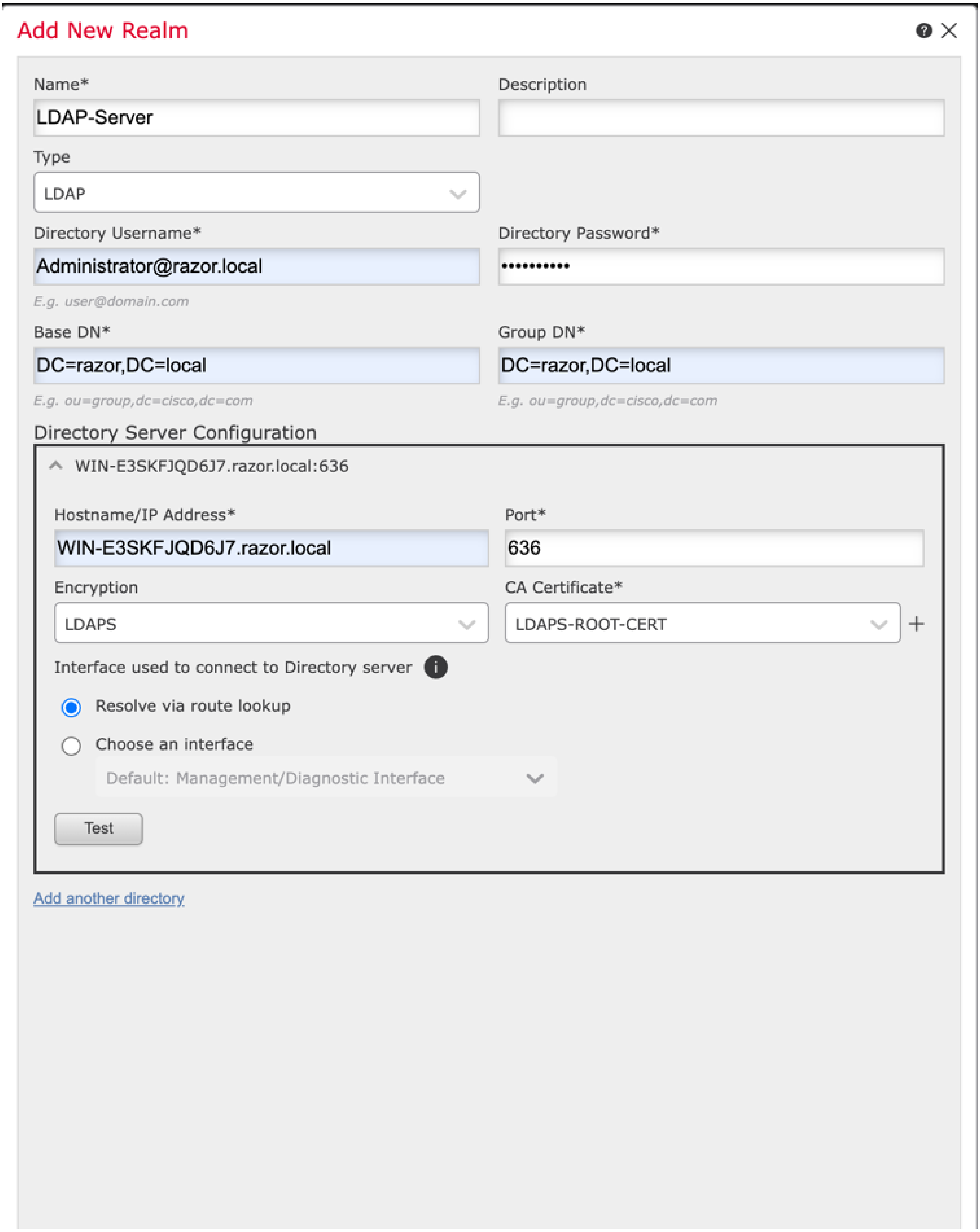
Organization Unit:

Not Valid Before:

Mar 22 14:33:15 2021 GMT

Not Valid After:

Mar 22 14:43:15 2026 GMT



Add New Realm

Name*: LDAP-Server

Description:

Type: LDAP

Directory Username*: Administrator@razor.local

E.g. user@domain.com

Directory Password*: •••••••••••

Base DN*: DC=razor,DC=local

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

Group DN*: DC=razor,DC=local

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

Directory Server Configuration

WIN-E3SKFJQD6J7.razor.local:636

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

Port*: 636

Encryption: LDAPS

CA Certificate*: LDAPS-ROOT-CERT

Interface used to connect to Directory server

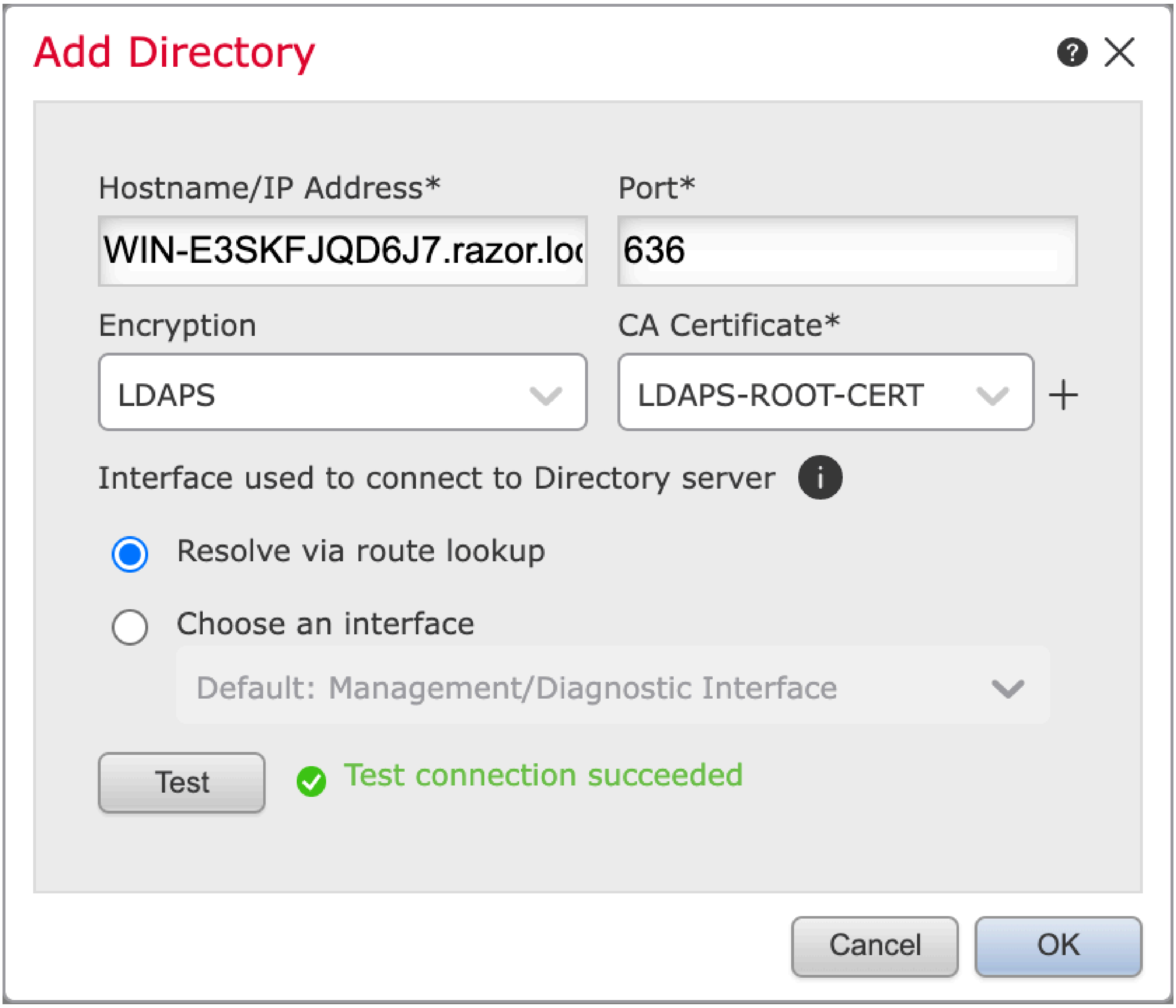
● Resolve via route lookup

○ Choose an interface

Default: Management/Diagnostic Interface

3. Clique em Test para garantir que o FMC possa ligar-se com êxito ao nome de usuário e à senha do diretório fornecidos na etapa anterior. Como esses testes são iniciados a partir do FMC e não por meio 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, já que as solicitações de autenticação LDAP do AnyConnect são iniciadas a partir de uma das interfaces roteáveis do FTD.



Add Directory

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

Port*: 636

Encryption: LDAPS

CA Certificate*: LDAPS-ROOT-CERT

Interface used to connect to Directory server

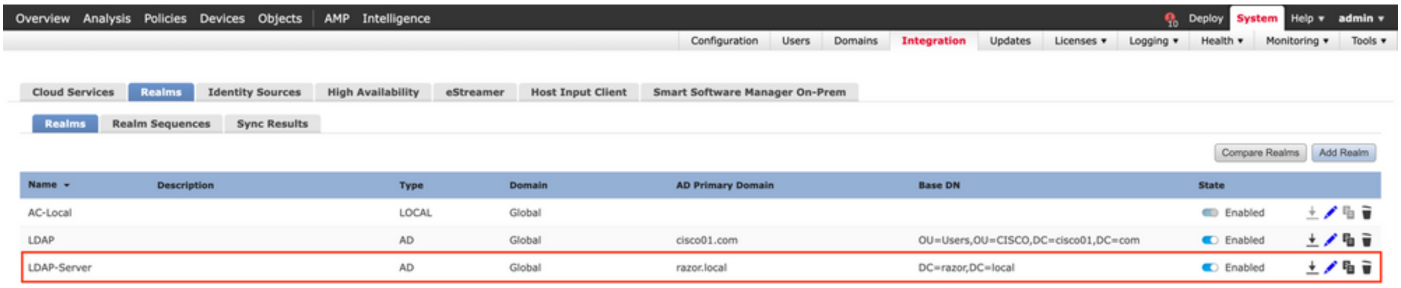
● Resolve via route lookup

○ Choose an interface

Default: Management/Diagnostic Interface

Test ✓ Test connection succeeded

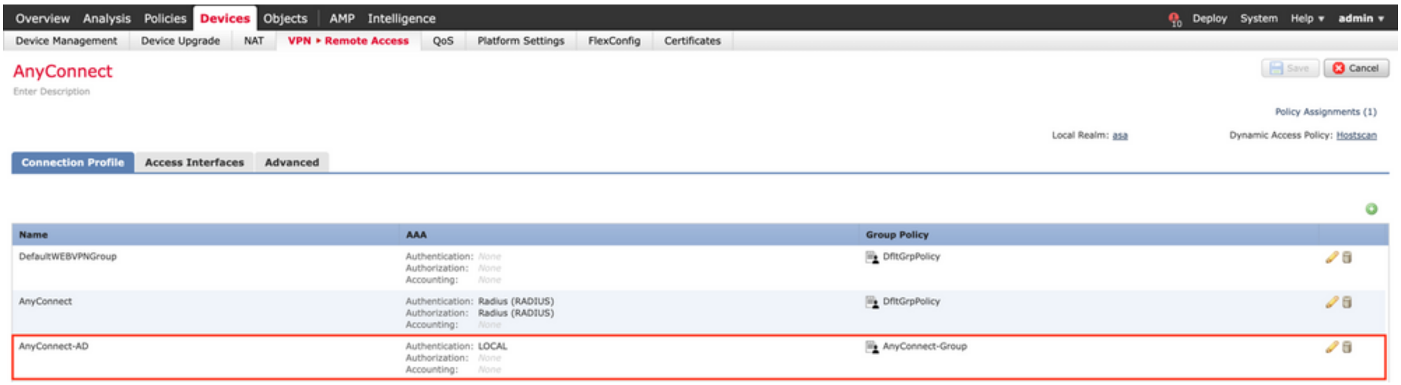
4. Ative o novo realm.



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

Configurar o AnyConnect para gerenciamento de senha

1. Escolha o perfil de conexão existente ou crie um novo, se for uma configuração inicial do AnyConnect. Aqui, é usado um perfil de conexão existente chamado 'AnyConnect-AD' mapeado com autenticação local.


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

AnyConnect

Enter Description

Policy Assignments (1)

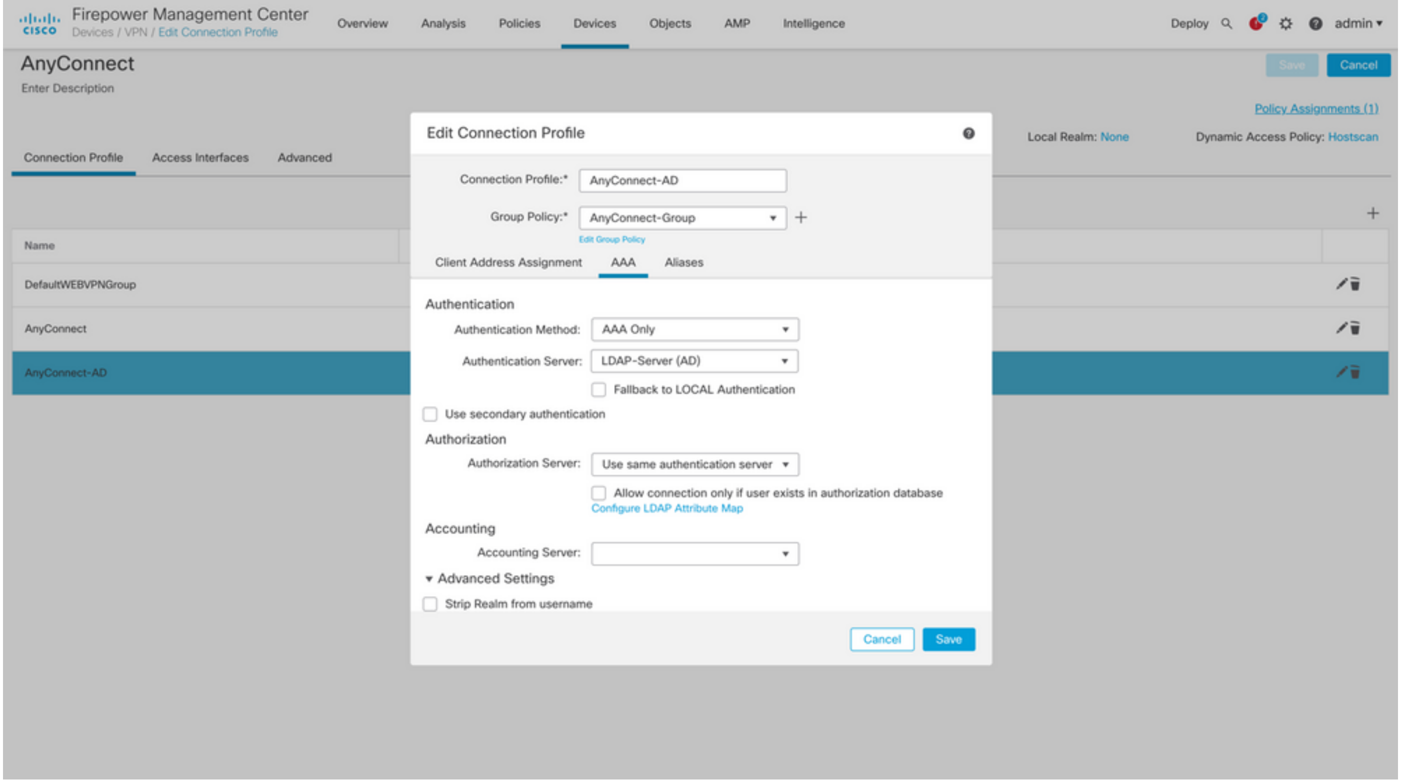
Local Realm: asa

Dynamic Access Policy: Hostscan

Connection Profile | Access Interfaces | Advanced

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

2. Edite o perfil do Connection e mapeie o novo servidor LDAP configurado nas etapas anteriores, sob as configurações AAA do Perfil de conexão. Depois de concluído, clique em Save no canto superior direito.


Firepower Management Center
Devices / VPN / Edit Connection Profile
Overview Analysis Policies Devices Objects AMP Intelligence
Deploy admin ▾
Save
Cancel
Connection Profile Access Interfaces Advanced
Name
DefaultWEBVPNGroup
AnyConnect
AnyConnect-AD

AnyConnect

Enter Description

Policy Assignments (1)

Local Realm: None

Dynamic Access Policy: Hostscan

Edit Connection Profile

Connection Profile:* AnyConnect-AD

Group Policy:* AnyConnect-Group ▾ +

Edit Group Policy

Client Address Assignment | AAA | Aliases

Authentication

Authentication Method: AAA Only ▾

Authentication Server: LDAP-Server (AD) ▾

□ Fallback to LOCAL Authentication

□ Use secondary authentication

Authorization

Authorization Server: Use same authentication server ▾

□ Allow connection only if user exists in authorization database

Configure LDAP Attribute Map

Accounting

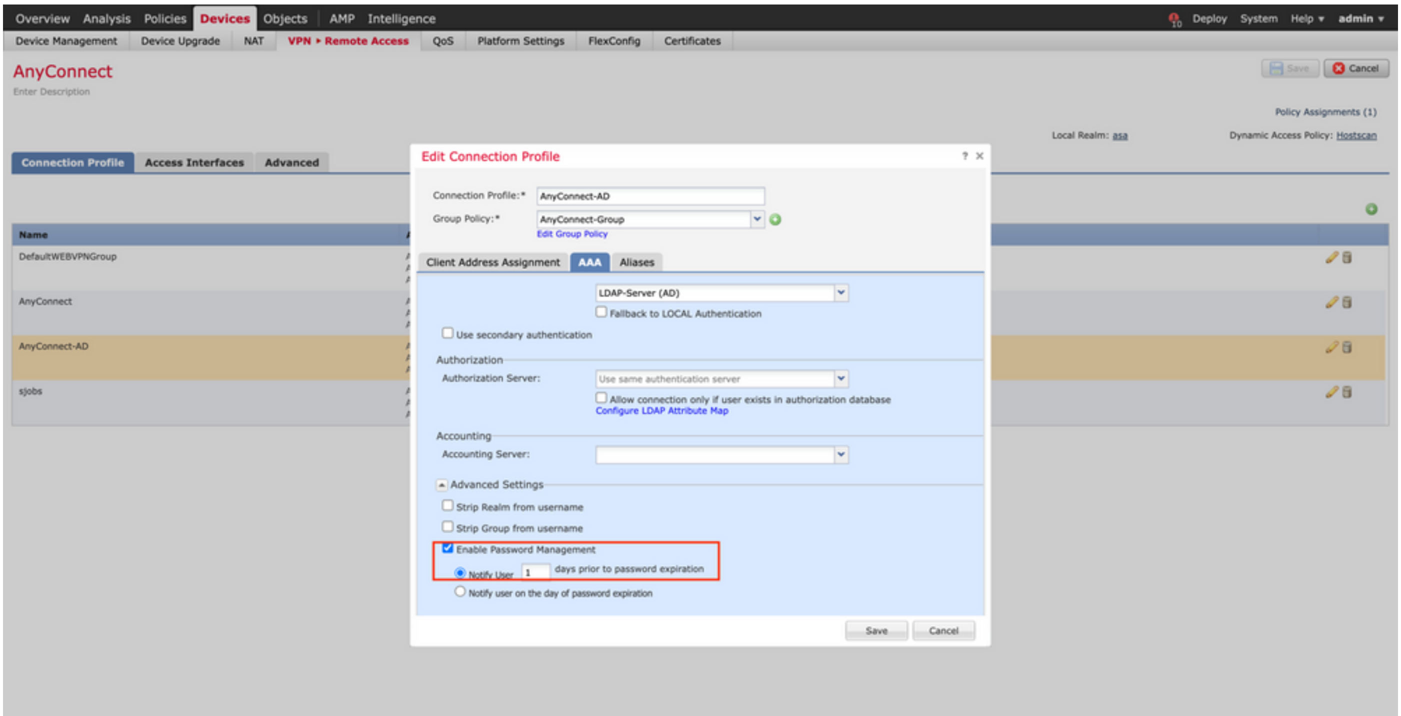
Accounting Server: ▾

▾ Advanced Settings

□ Strip Realm from username

Cancel Save

3. Habilite o gerenciamento de senhas no AAA > Advanced Settings e salve a configuração.



Edit Connection Profile

Connection Profile:* AnyConnect-AD

Group Policy:* AnyConnect-Group

Edit Group Policy

Client Address Assignment | AAA | Aliases

LDAP-Server (AD)

□ Fallback to LOCAL Authentication

□ Use secondary authentication

Authorization

Authorization Server: Use same authentication server

□ Allow connection only if user exists in authorization database

Configure LDAP Attribute Map

Accounting

Accounting Server:

Advanced Settings

□ Strip Realm from username

□ Strip Group from username

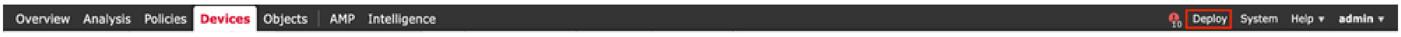
☑ Enable Password Management

● Notify User 1 days prior to password expiration

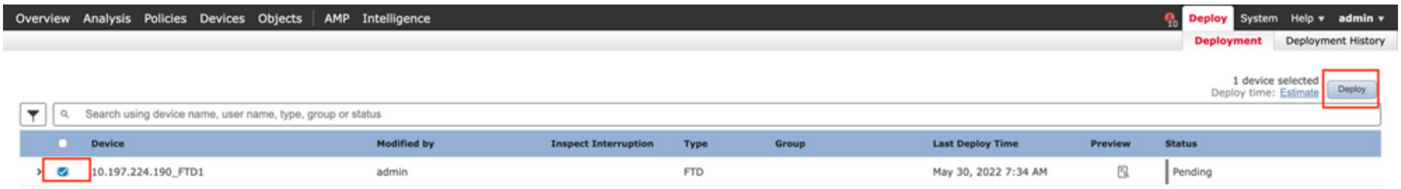
○ Notify user on the day of password expiration

Implantar

1. Depois de concluir todas as configurações, clique no botãoDeploy na parte superior direita.



2. Clique na caixa de seleção ao lado da configuração do FTD aplicada a ele e clique em Deploy, como mostrado nesta imagem:



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

Configuração final

Esta é a configuração vista na CLI do FTD após a implantação bem-sucedida.

Configuração do AAA

```
<#root>
> show running-config aaa-server


aaa-server LDAP-Server protocol ldap
                                                     <------ aaa-server group configured for LDAPs
```

```
 max-failed-attempts 4
 realm-id 8
aaa-server LDAP-Server host WIN-E3SKFJQD6J7.razor.local
                          <-------- LDAPs Server to which the queries are sent

 server-port 636
 ldap-base-dn DC=razor,DC=local
 ldap-group-base-dn DC=razor,DC=local
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn *****@razor.local
 ldap-over-ssl enable
 server-type microsoft
```

Configuração do AnyConnect

<#root>

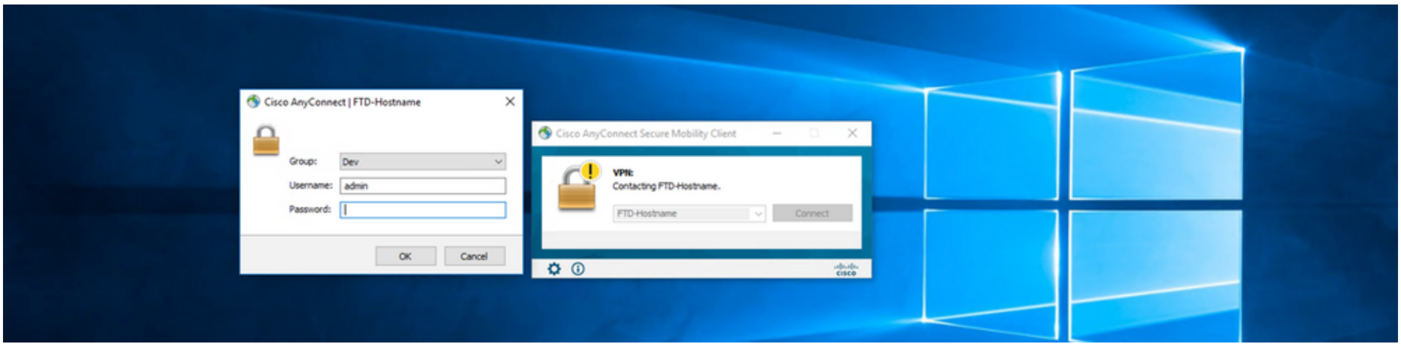
```
> show running-config webvpn

webvpn
 enable Outside
 anyconnect image disk0:/csm/anyconnect-win-4.10.01075-webdeploy-k9.pkg 1 regex "Windows"
 anyconnect profiles FTD-Client-Prof disk0:/csm/ftd.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  no disable
error-recovery disable
```

```
> show running-config tunnel-group

tunnel-group AnyConnect-AD type remote-access
tunnel-group AnyConnect-AD general-attributes
 address-pool Pool-1
authentication-server-group LDAP-Server                                     <-------- LDAPs Serve

 default-group-policy AnyConnect-Group

 password-management password-expire-in-days 1                        <-------- Password-management

tunnel-group AnyConnect-AD webvpn-attributes
 group-alias Dev enable



> show running-config group-policy AnyConnect-Group

group-policy
AnyConnect-Group
 internal
<--------- Group-Policy configuration that is mapped once the user is authenticated

group-policy AnyConnect-Group attributes
 vpn-simultaneous-logins 3
 vpn-idle-timeout 35791394
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
vpn-tunnel-protocol ikev2 ssl-client                                          <-------- Protocol

 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Remote-Access-Allow
 default-domain none
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private none
  anyconnect ssl keepalive 20
  anyconnect ssl rekey time none
  anyconnect ssl rekey method none
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression none
  anyconnect modules value none
  anyconnect profiles value FTD-Client-Prof type user
  anyconnect ask none default anyconnect
  anyconnect ssl df-bit-ignore disable


> show running-config ssl

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

Verificação

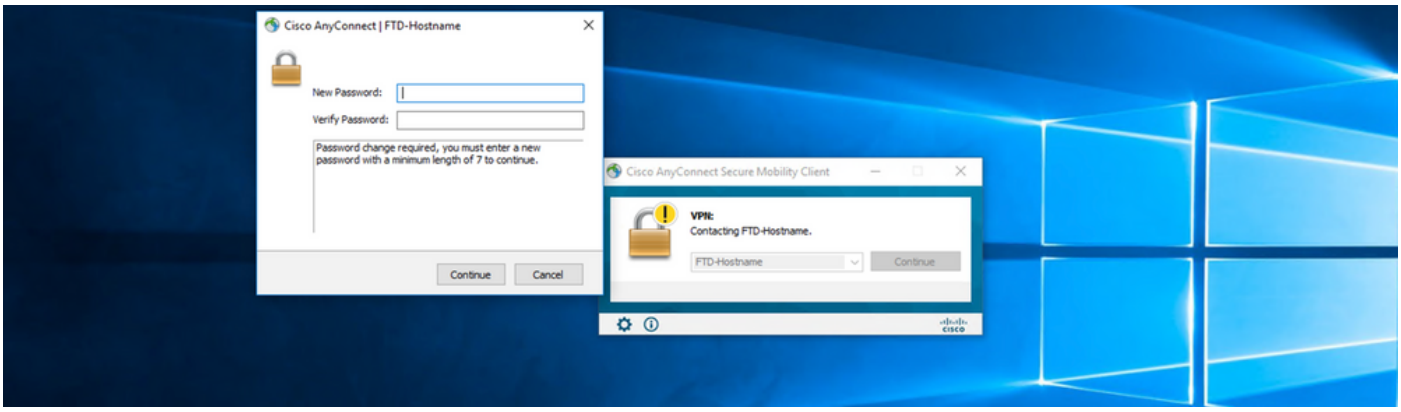
Conectar-se ao AnyConnect e verificar o processo de gerenciamento de senhas para a conexão do usuário

1. Inicie uma Conexão com o perfil de conexão em questão. Depois que for determinado no login inicial que a senha deve ser alterada, uma vez que a senha anterior foi rejeitada pelo Microsoft Server quando expirou, o usuário é solicitado a alterar a senha.


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

Group: Dev
Username: admin
Password:

VPN:
Contacting FTD-Hostname.
FTD-Hostname

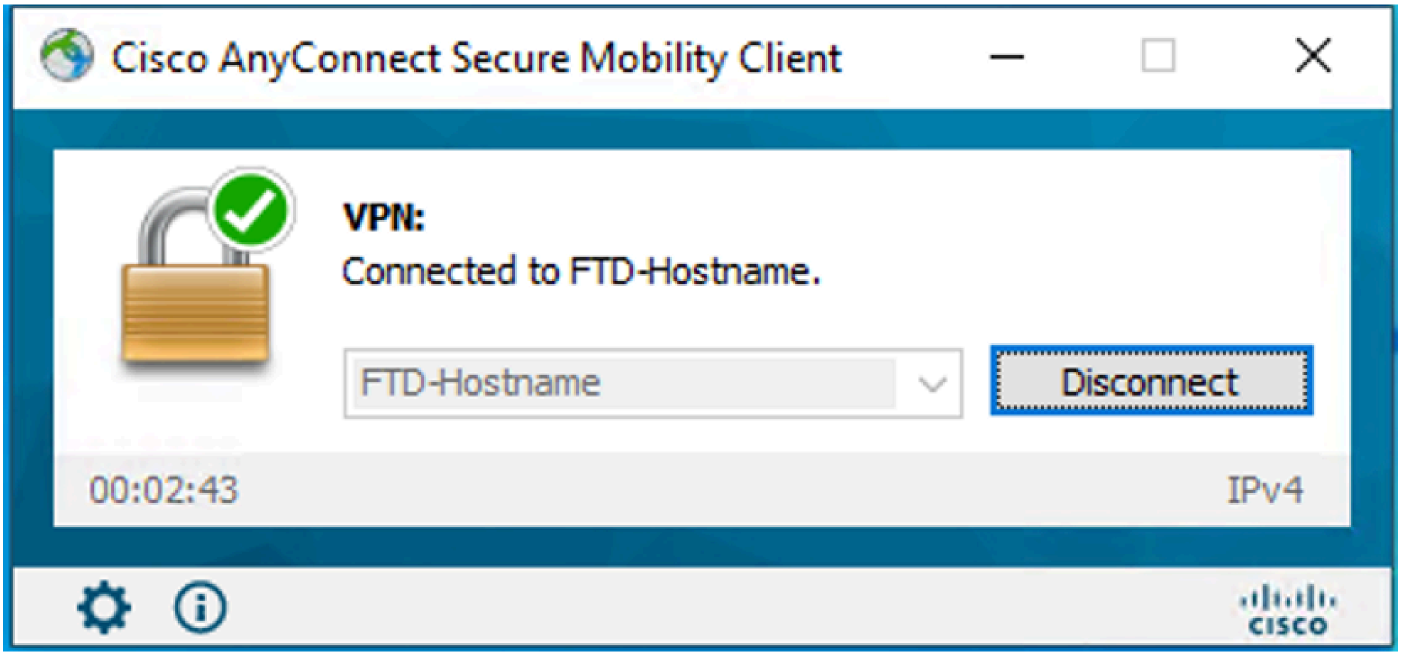

Cisco AnyConnect | FTD-Hostname
Continue
Cancel
Cisco AnyConnect Secure Mobility Client
Continue

New Password:
Verify Password:

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

VPN:
Contacting FTD-Hostname.
FTD-Hostname

2. Depois que o usuário digitar a nova senha para login, a conexão será estabelecida com êxito.



Cisco AnyConnect Secure Mobility Client

VPN:
Connected to FTD-Hostname.

3. Verifique a conexão do usuário na CLI do FTD:

```
<#root>
FTD_2# sh vpn-sessiondb anyconnect




Session Type: AnyConnect




Username     : admin
                 Index        : 7
<------- Username, IP address assigned information of the client



Assigned IP  : 10.1.x.x
               Public IP    : 10.106.xx.xx
Protocol     :
AnyConnect-Parent SSL-Tunnel DTLS-Tunnel


License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx     : 16316                 Bytes Rx     : 2109

Group Policy : AnyConnect-Group       Tunnel Group : AnyConnect-AD


Login Time   : 13:22:24 UTC Mon Apr 25 2022

Duration     : 0h:00m:51s

Inactivity   : 0h:00m:00s

VLAN Mapping : N/A                   VLAN         : none

Audt Sess ID : 0ac5e0fa000070006266a090

Security Grp : none                  Tunnel Zone  : 0
```

Troubleshooting

Debugs

Essa depuração pode ser executada na CLI de diagnóstico para solucionar problemas relacionados ao gerenciamento de senhas: debug ldap 255.

Trabalhando com depurações de gerenciamento de senhas

<#root>

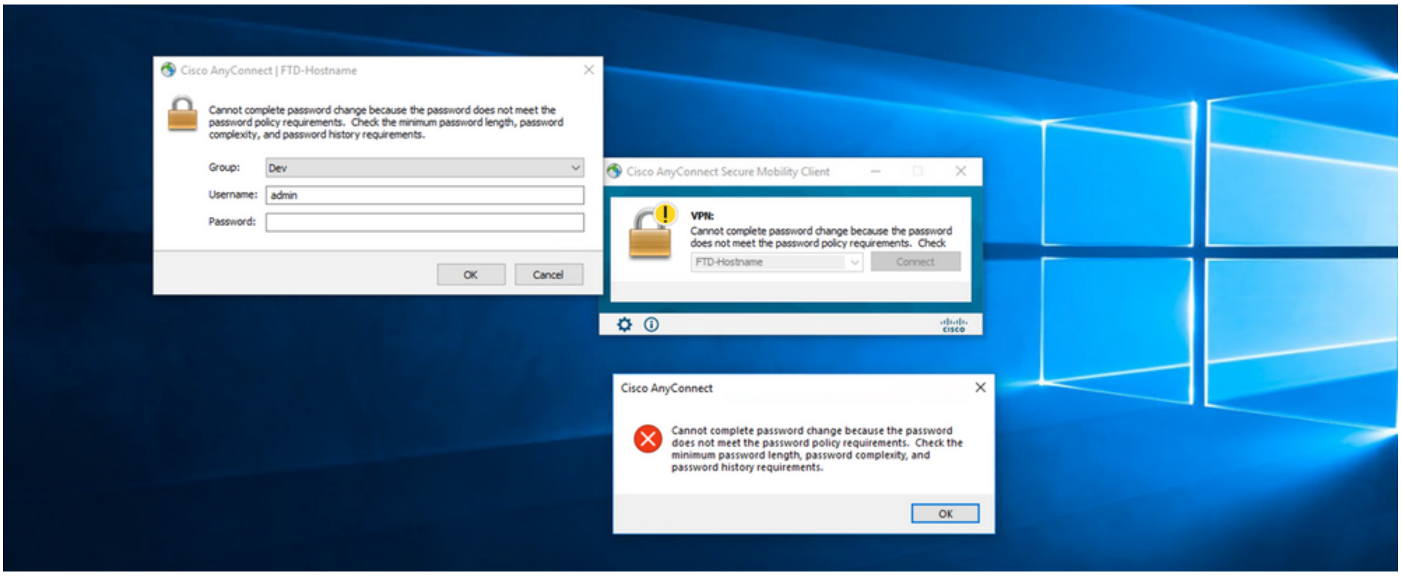
```
[24] Session Start

[24] New request Session, context 0x0000148f3c271830, reqType = Authentication

[24] Fiber started

[24] Creating LDAP context with uri=ldaps://10.106.71.234:636

[24] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful


[24] supportedLDAPVersion: value = 3

[24] supportedLDAPVersion: value = 2

[24] Binding as *****@razor.local

[24] Performing Simple authentication for *****@razor.local to 10.106.71.234

[24] LDAP Search:
        Base DN = [DC=razor,DC=local]

        Filter  = [sAMAccountName=admin]

        Scope   = [SUBTREE]

[24] User DN = [CN=admin,CN=Users,DC=razor,DC=local]

[24] Talking to Active Directory server 10.106.71.234

[24] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[24] Read bad password count 3

[24] Binding as admin

[24] Performing Simple authentication for admin to 10.106.71.234

[24] Simple authentication for admin returned code (49) Invalid credentials

[24] Message (admin): 80090308: LdapErr: DSID-0C0903C5, comment: AcceptSecurityContext error, data 773,

[24] Checking password policy

[24] New password is required for admin

[24] Fiber exit Tx=622 bytes Rx=2771 bytes, status=-1

[24] Session End



[25] Session Start

[25] New request Session, context 0x0000148f3c271830, reqType = Modify Password

[25] Fiber started

[25] Creating LDAP context with uri=ldaps://10.106.71.234:636

[25] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful
```

```
[25] supportedLDAPVersion: value = 3
[25] supportedLDAPVersion: value = 2
[25] Binding as *****@razor.local
[25] Performing Simple authentication for *****@razor.local to 10.106.71.234
[25] LDAP Search:
        Base DN = [DC=razor,DC=local]
        Filter  = [sAMAccountName=admin]
        Scope   = [SUBTREE]
[25] User DN = [CN=admin,CN=Users,DC=razor,DC=local]
[25] Talking to Active Directory server 10.106.71.234
[25] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local


[25] Read bad password count 3


[25] Change Password for admin successfully converted old password to unicode


[25] Change Password for admin successfully converted new password to unicode


[25] Password for admin successfully changed


[25] Retrieved User Attributes:
[25]   objectClass: value = top
[25]   objectClass: value = person
[25]   objectClass: value = organizationalPerson
[25]   objectClass: value = user
[25]   cn: value = admin
[25]   givenName: value = admin
[25]   distinguishedName: value = CN=admin,CN=Users,DC=razor,DC=local
[25]   instanceType: value = 4
[25]   whenCreated: value = 20201029053516.0Z
```

```
[25]   whenChanged: value = 20220426032127.0Z
[25]   displayName: value = admin
[25]   uSNCreated: value = 16710
[25]   uSNChanged: value = 98431
[25]   name: value = admin
[25]   objectGUID: value = ..0.].LH.....9.4
[25]   userAccountControl: value = 512
[25]   badPwdCount: value = 3
[25]   codePage: value = 0
[25]   countryCode: value = 0
[25]   badPasswordTime: value = 132610388348662803
[25]   lastLogoff: value = 0
[25]   lastLogon: value = 132484577284881837
[25]   pwdLastSet: value = 0
[25]   primaryGroupID: value = 513
[25]   objectSid: value = ................7Z|....RQ...
[25]   accountExpires: value = 9223372036854775807
[25]   logonCount: value = 0
[25]   sAMAccountName: value = admin
[25]   sAMAccountType: value = 805306368
[25]   userPrincipalName: value = ******@razor.local
[25]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=razor,DC=local
[25]   dSCorePropagationData: value = 20220425125800.0Z
[25]   dSCorePropagationData: value = 20201029053516.0Z
[25]   dSCorePropagationData: value = 16010101000000.0Z
[25]   lastLogonTimestamp: value = 132953506361126701
[25]   msDS-SupportedEncryptionTypes: value = 0
[25]   uid: value = ******@razor.local
[25] Fiber exit Tx=714 bytes Rx=2683 bytes, status=1
[25] Session End
```

Erros comuns encontrados durante o gerenciamento de senhas

Geralmente, se a política de senha definida pelo Microsoft Server não for atendida durante o tempo em que o usuário fornecer a nova senha, a conexão será encerrada com o erro "A senha não atende aos requisitos da política de senha". Portanto, certifique-se de que a nova senha atenda à política definida pelo Microsoft Server para LDAPs.



Cisco AnyConnect | FTD-Hostname

Cannot complete password change because the password does not meet the password policy requirements. Check the minimum password length, password complexity, and password history requirements.

Group: Dev

Username: admin

Password:

Cisco AnyConnect Secure Mobility Client

VPN:
Cannot complete password change because the password does not meet the password policy requirements. Check

Cisco AnyConnect

Cannot complete password change because the password does not meet the password policy requirements. Check the minimum password length, password complexity, and password history requirements.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.