

# Konfigurieren der AD-Authentifizierung (LDAP) und Benutzeridentität auf dem vom FDM verwalteten FTD für AnyConnect-Clients

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[Netzwerkdiagramm und Szenario](#)

[AD-Konfigurationen](#)

[LDAP-Basis-DN ermitteln](#)

[FTD-Konto erstellen](#)

[AD-Gruppen erstellen und AD-Gruppen Benutzer hinzufügen \(optional\)](#)

[Kopieren Sie die LDAS SSL-Zertifikatsroot \(nur für LDAPS oder STARTTLS erforderlich\).](#)

[FDM-Konfigurationen](#)

[Lizenzierung überprüfen](#)

[AD-Identitätsquelle einrichten](#)

[Konfigurieren von AnyConnect für die AD-Authentifizierung](#)

[Identitätsrichtlinie aktivieren und Sicherheitsrichtlinien für Benutzeridentität konfigurieren](#)

[Überprüfung](#)

[Endgültige Konfiguration](#)

[Herstellen einer Verbindung mit AnyConnect und Überprüfen der Zugriffskontrollrichtlinien](#)

[Fehlerbehebung](#)

[Debugger](#)

[Arbeiten mit LDAP-Debuggern](#)

[Verbindung mit LDAP-Server kann nicht hergestellt werden](#)

[Binden der Anmelde-DN und/oder des Kennworts falsch](#)

[LDAP-Server kann Benutzernamen nicht finden](#)

[Falsches Kennwort für Benutzername](#)

[AAA testen](#)

[Paketerfassung](#)

[Windows Server Event Viewer-Protokolle](#)

## Einführung

In diesem Dokument wird erläutert, wie die Active Directory-Authentifizierung (AD) für AnyConnect-Clients konfiguriert wird, die mit einer Cisco FirePOWER Threat Defense (FTD) verbunden sind, die von FirePOWER Device Management (FDM) verwaltet wird. Die Benutzeridentität wird in den Zugriffsrichtlinien verwendet, um AnyConnect-Benutzer auf bestimmte IP-Adressen und Ports zu beschränken.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der RA VPN-Konfiguration für FDM
- Grundkenntnisse der LDAP-Serverkonfiguration auf FDM
- Grundkenntnisse von AD

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Microsoft 2016-Server
- FTDv läuft 6.5.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfiguration

### Netzwerkdiagramm und Szenario



Windows-Server ist mit Internetinformationsdienste (IIS) und Remote Desktop Protocol (RDP) vorkonfiguriert, um die Benutzeridentität zu testen. In diesem Konfigurationsleitfaden werden drei Benutzerkonten und zwei Gruppen erstellt.

Benutzerkonten:

- FTD-Administrator: Diese wird als Verzeichniskonto verwendet, damit die FTD an den AD-Server gebunden werden kann.
- IT-Administrator: Ein Testadministrator-Konto, das zum Demonstrieren der Benutzeridentität verwendet wird.
- Testbenutzer: Ein Testbenutzerkonto, das zum Demonstrieren der Benutzeridentität verwendet wird.

Gruppen:

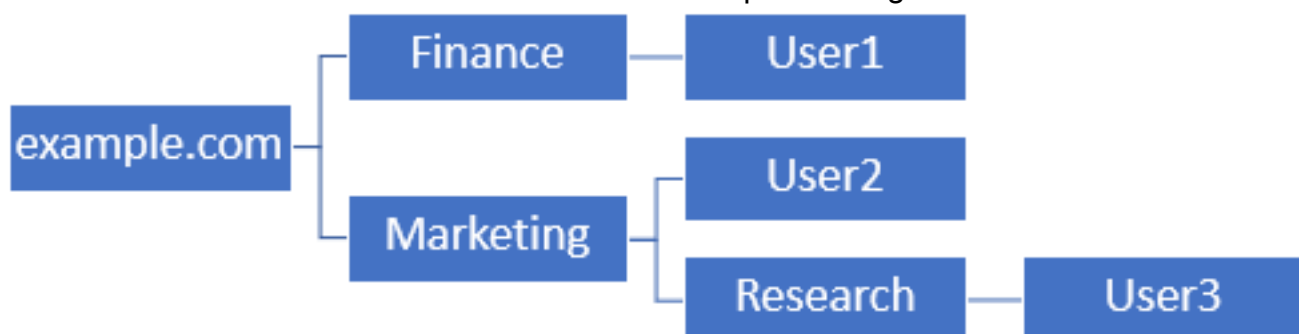
- AnyConnect-Administratoren: Eine Testgruppe, der IT-Administrator hinzugefügt wird, um die

- Benutzeridentität nachzuweisen. Diese Gruppe hat nur RDP-Zugriff auf Windows Server.
- AnyConnect-Benutzer: Eine Testgruppe, der Testbenutzer hinzugefügt wird, um die Benutzeridentität zu demonstrieren. Diese Gruppe hat nur HTTP-Zugriff auf Windows Server.

## AD-Konfigurationen

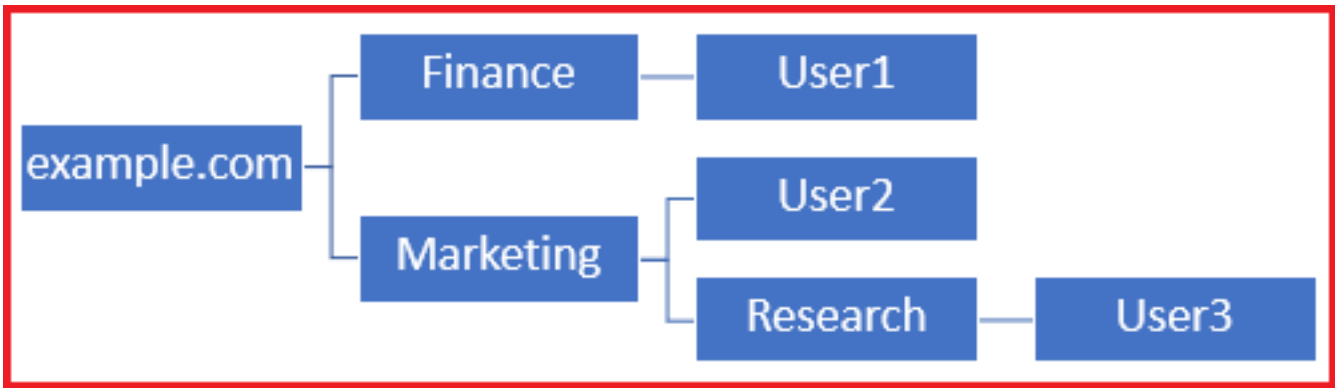
Um die AD-Authentifizierung und die Benutzeridentität auf FTD korrekt konfigurieren zu können, sind einige Werte erforderlich. Alle diese Details müssen auf dem Microsoft Server erstellt oder gesammelt werden, bevor die Konfiguration auf dem FDM erfolgen kann. Die wichtigsten Werte sind:

- Domänenname: Dies ist der Domänenname des Servers. In diesem Konfigurationsleitfaden ist `example.com` der Domänenname.
- Server-IP/FQDN-Adresse: Die IP-Adresse oder der FQDN, die zum Erreichen des Microsoft-Servers verwendet wird. Wenn ein FQDN verwendet wird, muss ein DNS-Server innerhalb von FDM und FTD konfiguriert werden, um den FQDN aufzulösen. In diesem Konfigurationsleitfaden sind diese Werte `win2016.example.com`, die zu `192.168.1.1` aufgelöst wird.
- Server-Port: Der vom LDAP-Dienst verwendete Port. Standardmäßig verwenden LDAP und STARTTLS den TCP-Port 389 für LDAP und LDAP über SSL (LDAPS) den TCP-Port 636.
- Stammzertifizierungsstelle: Wenn LDAPS oder STARTTLS verwendet wird, ist die Root-CA zum Signieren des SSL-Zertifikats erforderlich, das von LDAPS verwendet wird.
- Benutzername und Kennwort des Verzeichnisses: Dies ist das Konto, das von FDM und FTD verwendet wird, um eine Verbindung zum LDAP-Server herzustellen, Benutzer zu authentifizieren und nach Benutzern und Gruppen zu suchen. Zu diesem Zweck wird ein Konto mit dem Namen FTD Admin erstellt.
- DN (Base Distinguished Name): Die Basis-DN ist der Ausgangspunkt für FDM, und die FTD weist Active Directory an, bei der Suche nach Benutzern anzufangen. In diesem Konfigurationsleitfaden wird die Stammdomäne `example.com` als Basis-DN verwendet. In einer Produktionsumgebung kann es jedoch besser sein, einen Basis-DN weiter in der LDAP-Hierarchie zu verwenden. Nehmen wir zum Beispiel die folgende LDAP-Hierarchie:



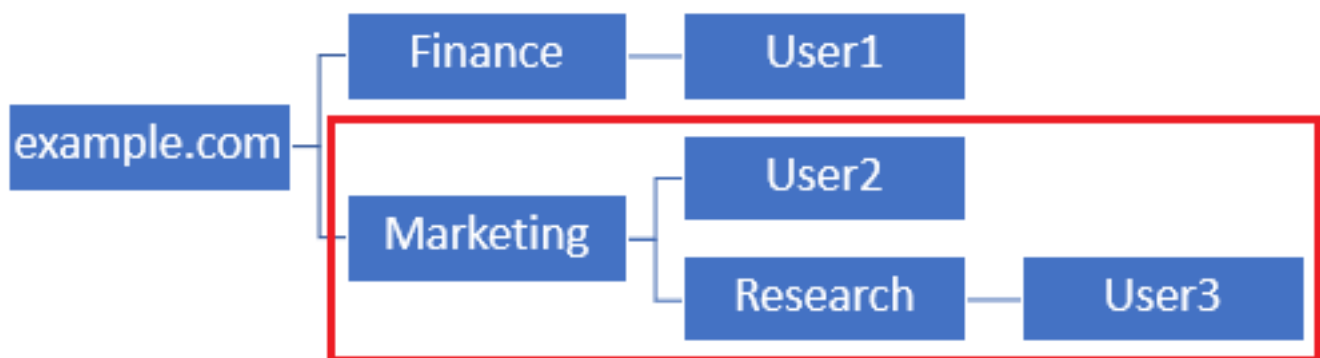
Wenn ein Administrator möchte, dass Benutzer innerhalb der Marketing-Organisationseinheit die Basis-DN auf den Root (`example.com`) authentifizieren können, kann sich `User1` unter der Abteilung `Finance` organisational ebenfalls anmelden, da die Benutzersuche am Root beginnt und zu Finanzen, Marketing und Forschung führt.

Basis-DN auf `beispiel.com` festgelegt.



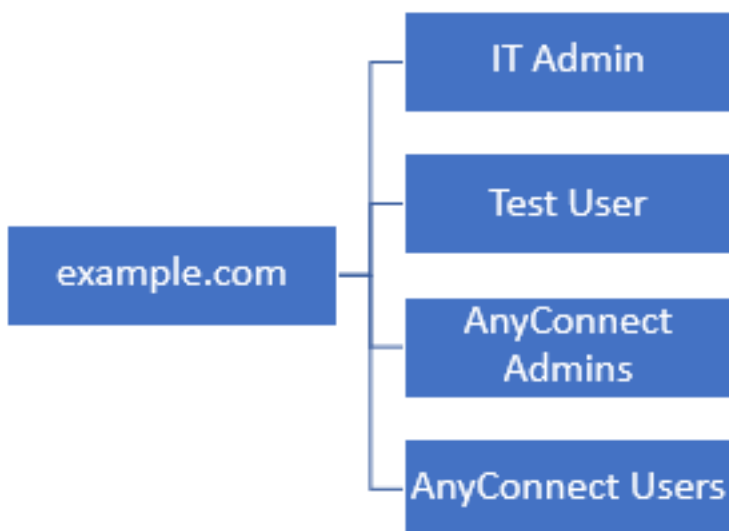
Um Anmeldungen auf Benutzer in der Organisationseinheit Marketing und darunter zu beschränken, kann der Administrator stattdessen die Basis-DN auf Marketing festlegen. Jetzt können sich nur Benutzer2 und User3 authentifizieren, da die Suche bei Marketing beginnt.

Basis-DN auf Marketing eingestellt:



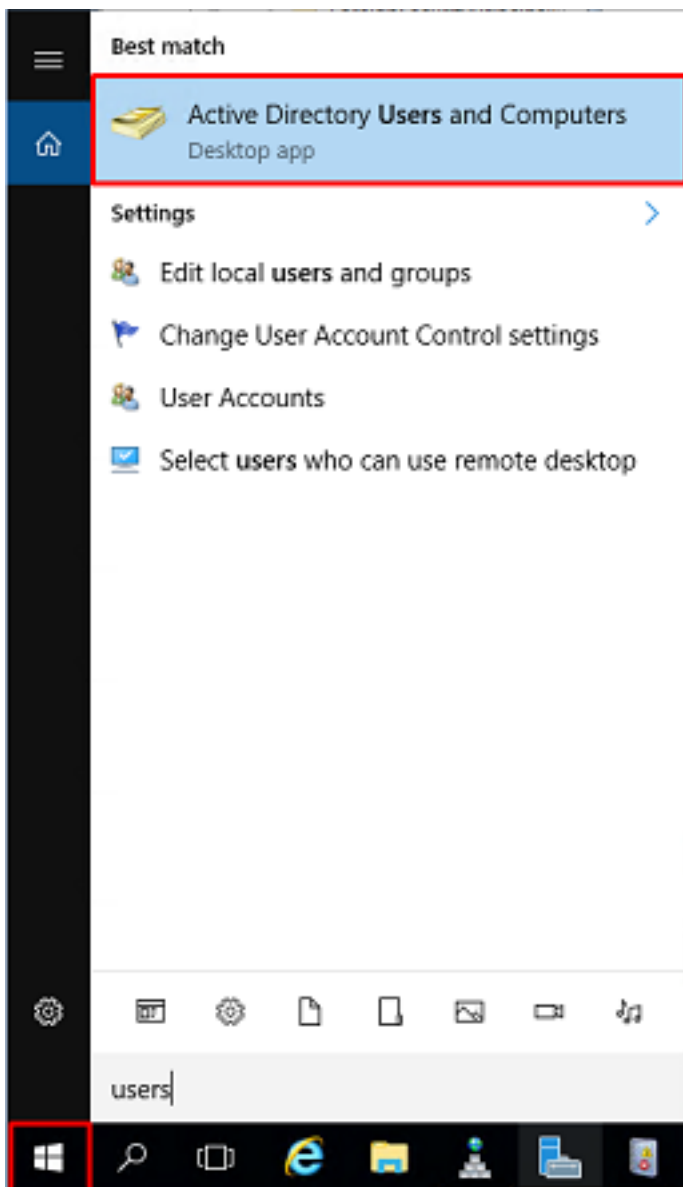
Beachten Sie, dass für eine detailliertere Steuerung innerhalb der FTD, für die Benutzer Verbindungen herstellen oder Benutzern unterschiedliche Autorisierungen basierend auf ihren AD-Attributen zuweisen dürfen, eine LDAP-Autorisierungszuordnung konfiguriert werden muss.

Diese vereinfachte LDAP-Hierarchie wird in diesem Konfigurationsleitfaden verwendet, und der DN für die root example.com wird für die Basis-DN verwendet.

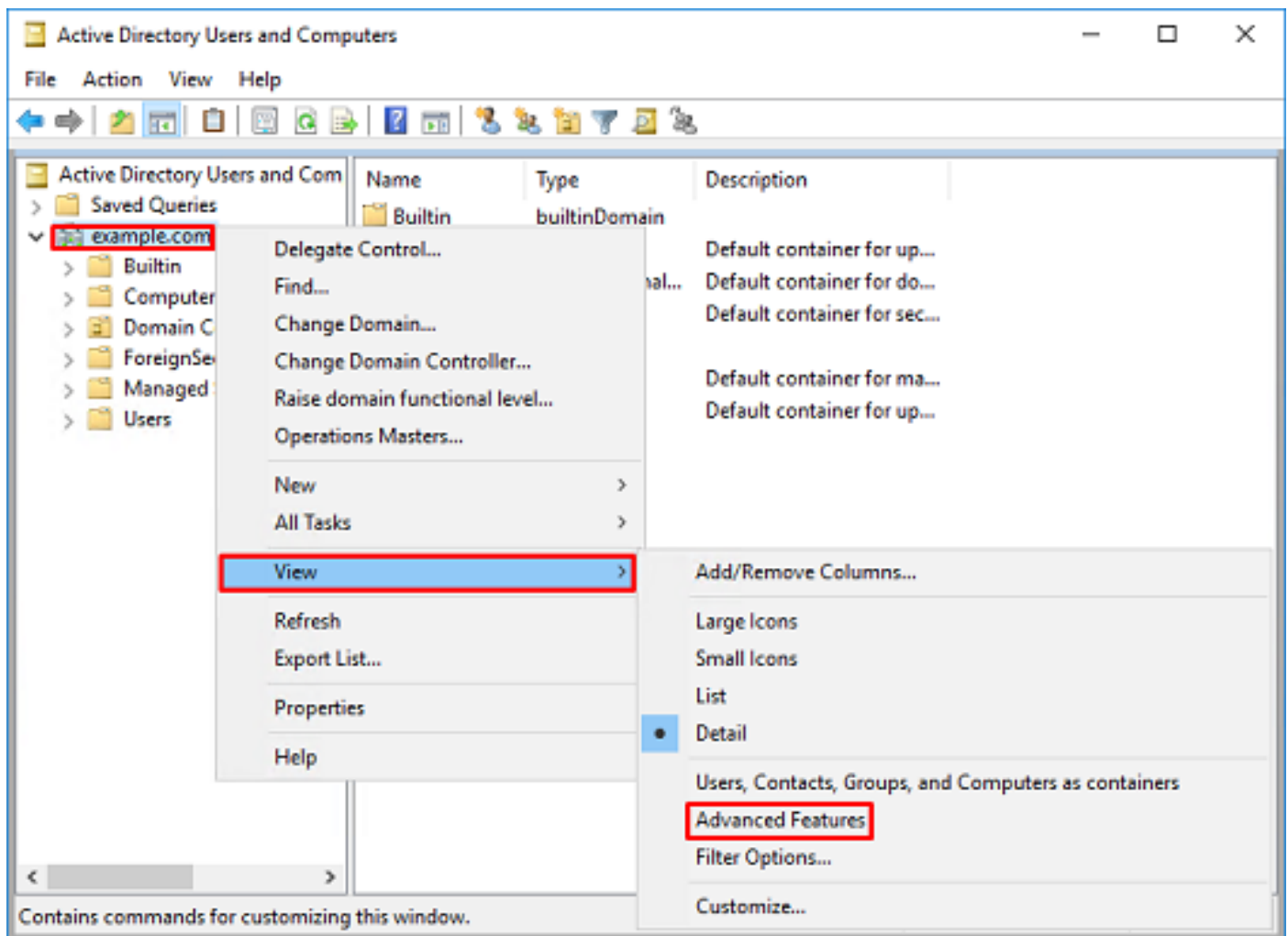


### LDAP-Basis-DN ermitteln

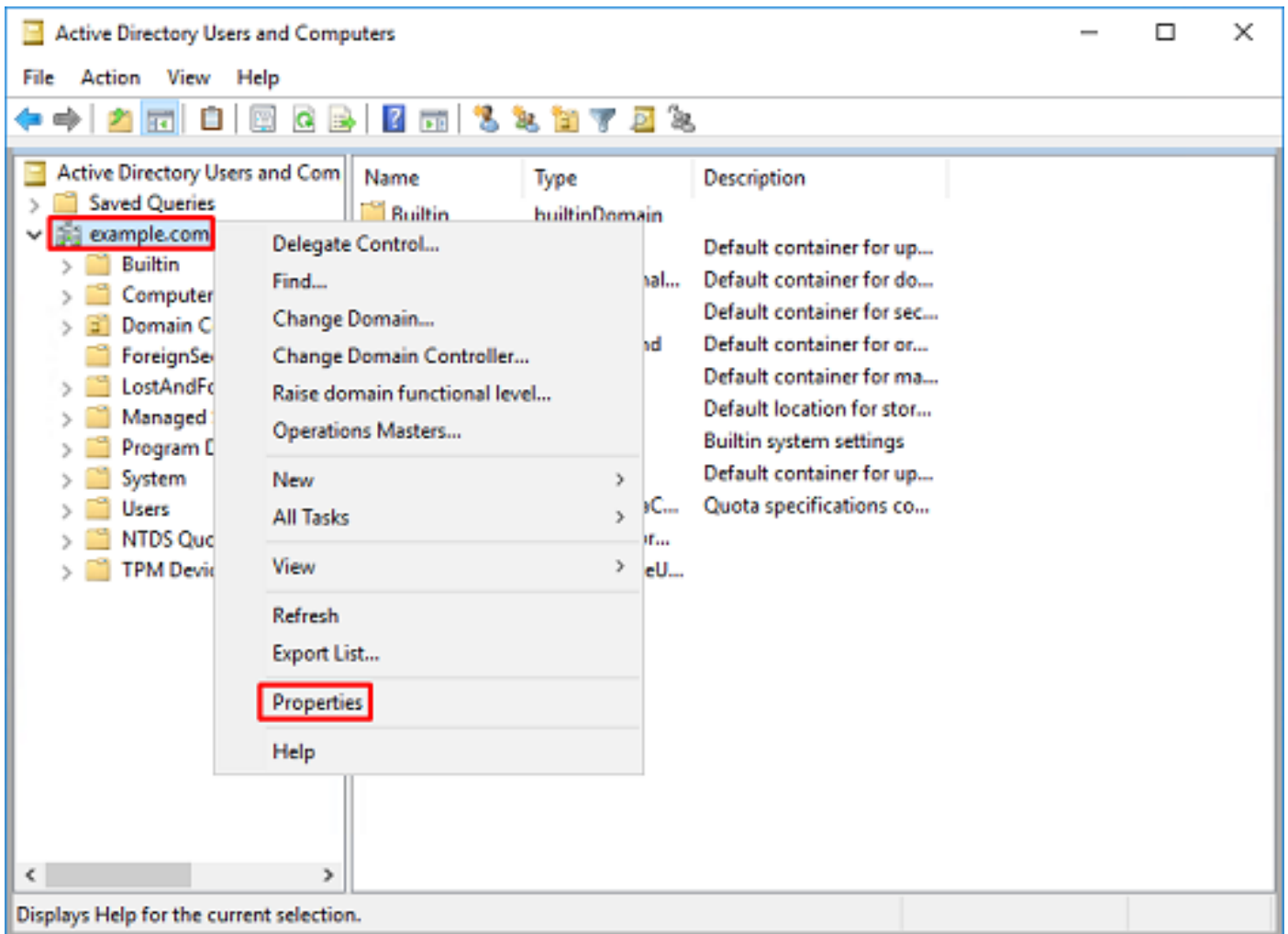
1. Öffnen Sie AD-Benutzer und -Computer.



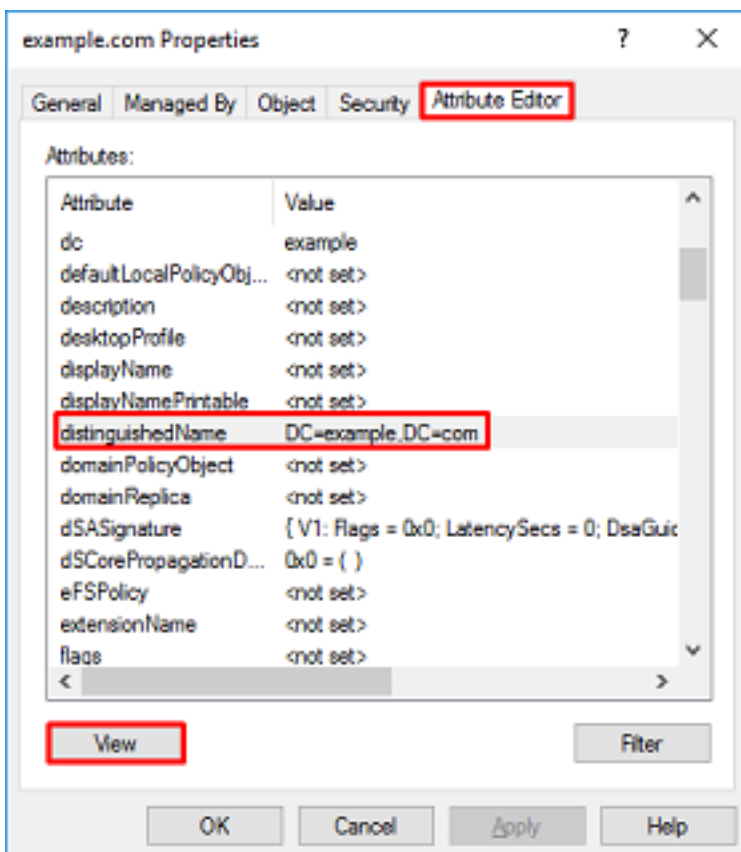
2. Klicken Sie mit der linken Maustaste auf die Stammdomäne (um den Container zu öffnen), klicken Sie mit der rechten Maustaste auf die Stammdomäne, navigieren Sie dann zu **Ansicht**, und klicken Sie auf **Erweiterte Funktionen**.



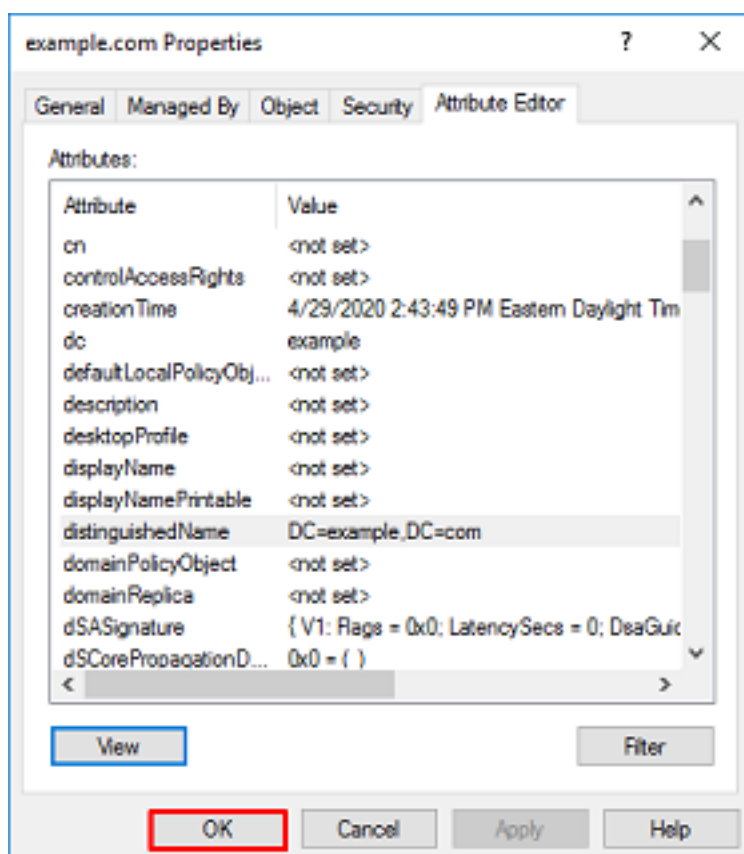
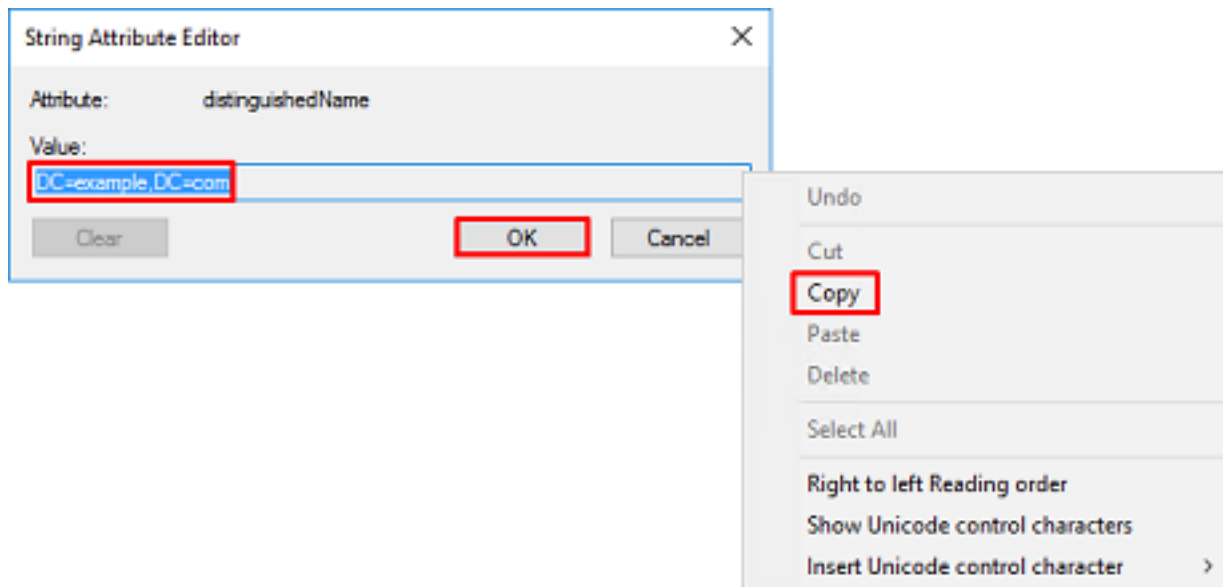
3. Dadurch wird die Ansicht zusätzlicher Eigenschaften unter den AD-Objekten aktiviert. Um z. B. den DN für die root example.com zu suchen, klicken Sie mit der rechten Maustaste auf **example.com** und navigieren Sie dann zu **Properties**.



4. Klicken Sie unter **Eigenschaften** auf die Registerkarte **Attributeditor**. Suchen Sie **DistinguishedName** unter Attributes, und klicken Sie dann auf **Anzeigen**.

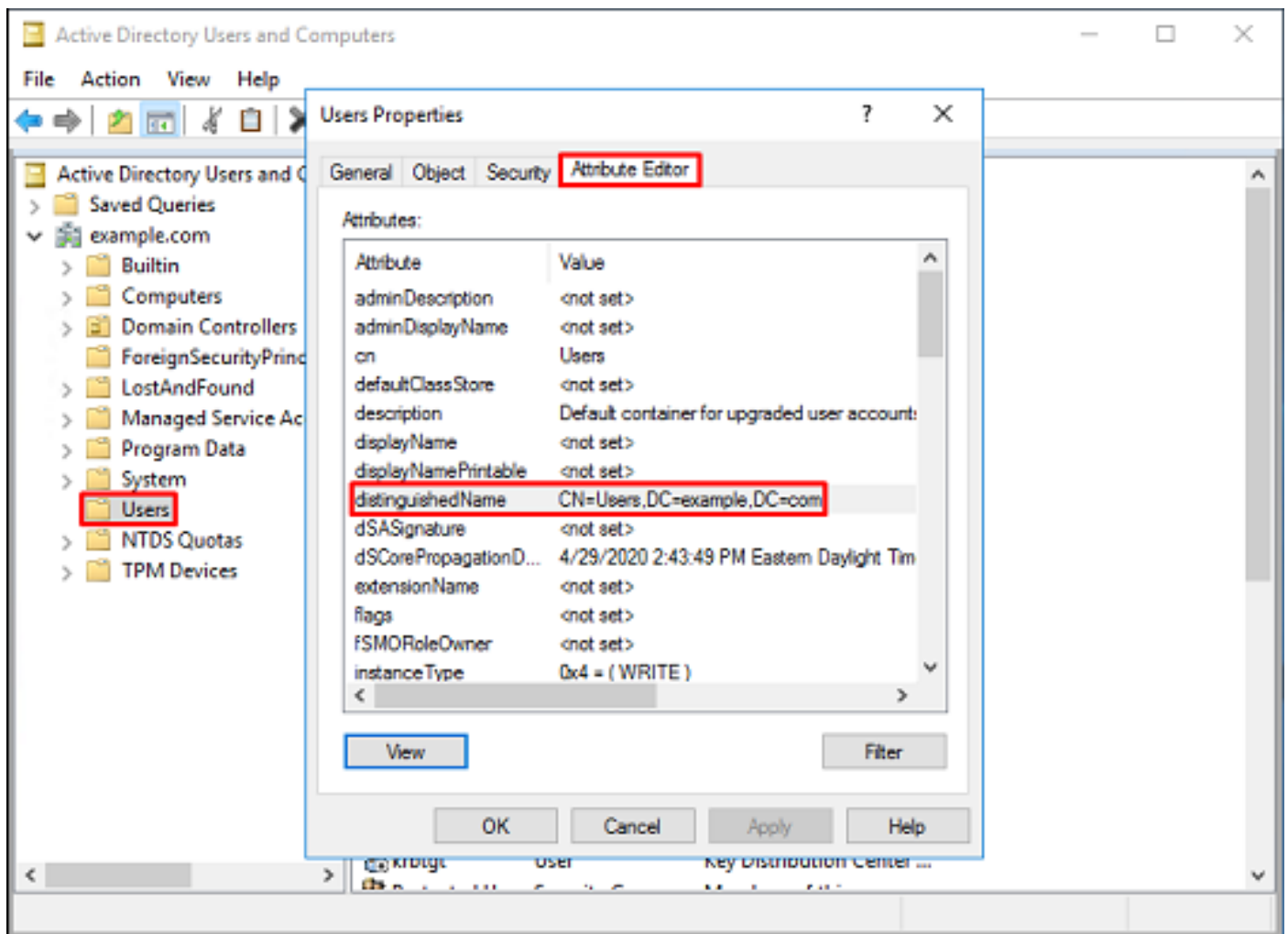


5. Dadurch wird ein neues Fenster geöffnet, in das die DN kopiert und später in FDM eingefügt werden kann. In diesem Beispiel lautet die Root-DN DC=example, DC=com. Kopieren Sie den Wert. Klicken Sie auf **OK**, um das Fenster Zeichenfolgen-Editor zu verlassen, und klicken Sie erneut auf **OK**, um die Eigenschaften zu verlassen.

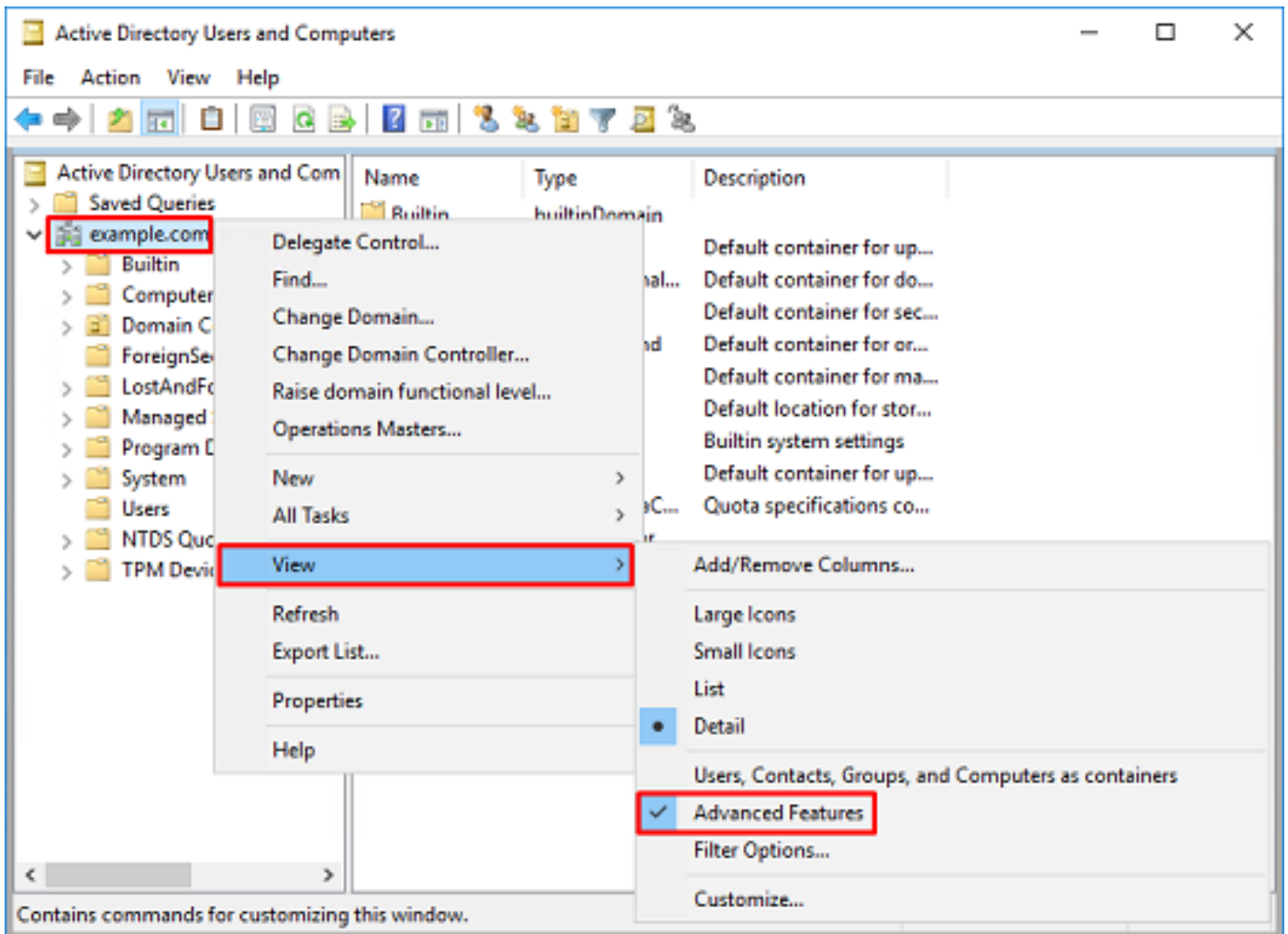


Dies kann für mehrere Objekte in AD erfolgen. Diese Schritte werden beispielsweise verwendet, um die DN des Benutzercontainers zu finden:





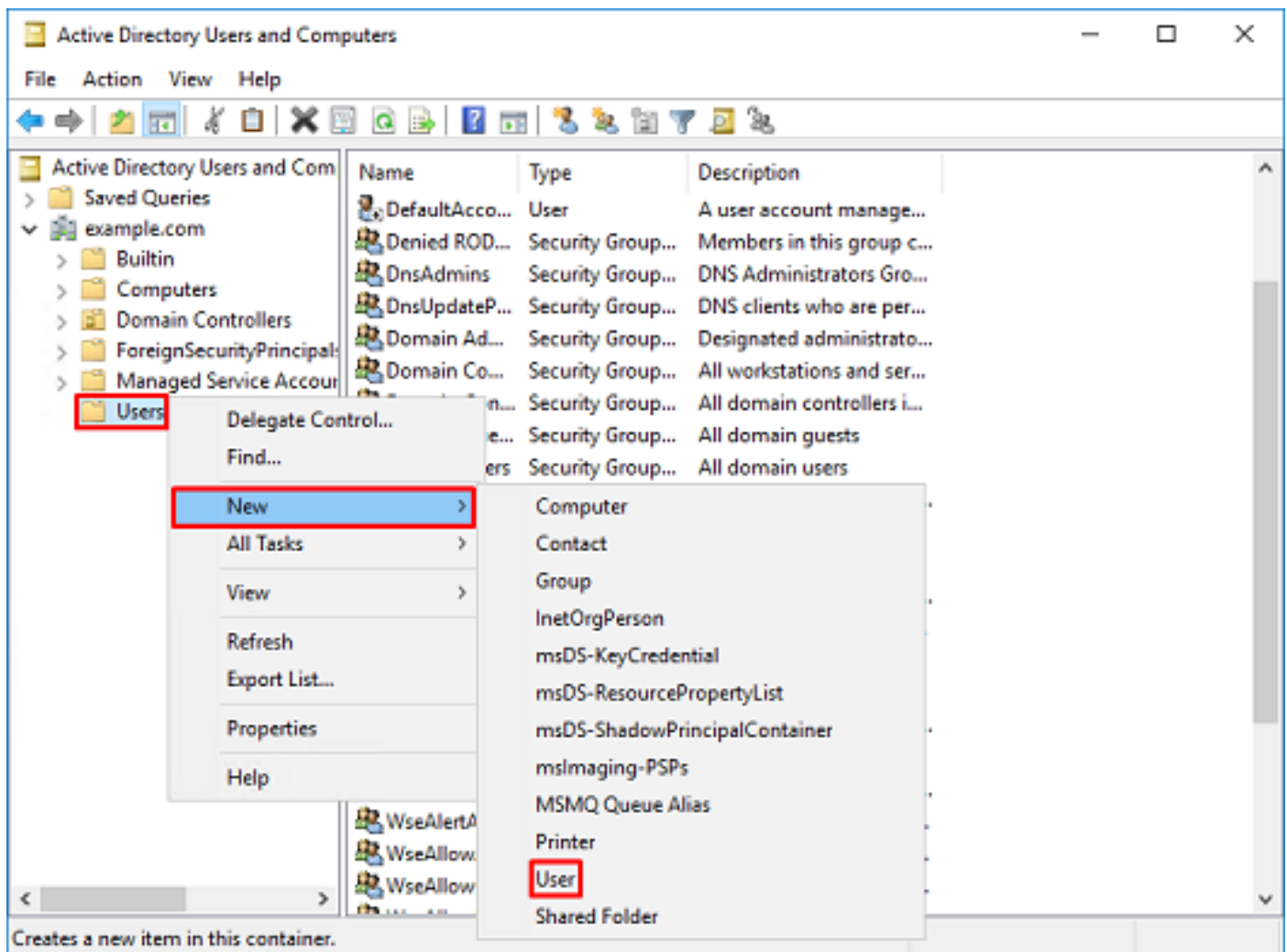
6. Die Ansicht Erweiterte Funktionen kann entfernt werden. Klicken Sie mit der rechten Maustaste auf die Root-DN, navigieren Sie zur **Ansicht**, und klicken Sie erneut auf **Erweiterte Funktionen**.



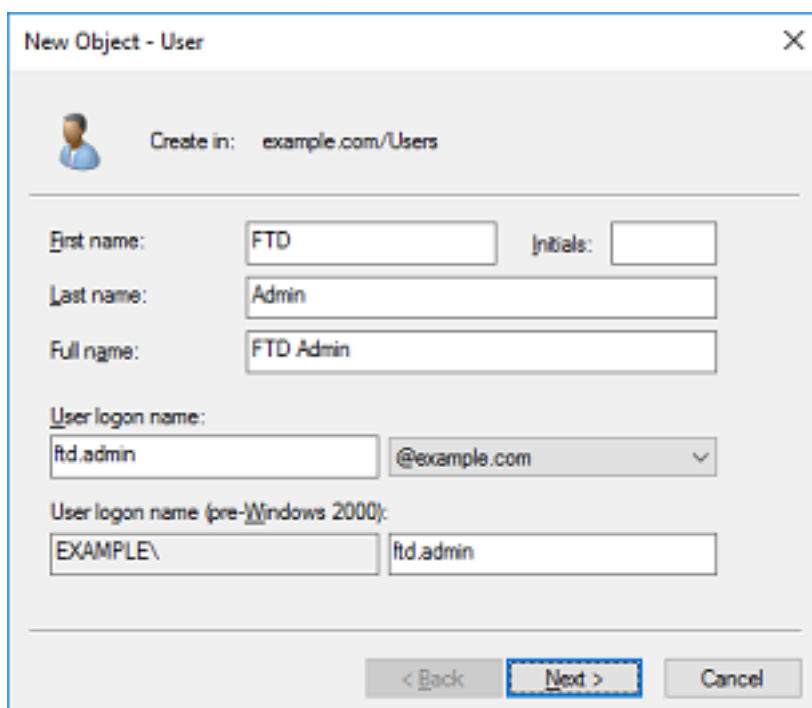
## FTD-Konto erstellen

Dieses Benutzerkonto ermöglicht es dem FDM und der FTD, sich mit dem AD zu verbinden, um Benutzer und Gruppen zu suchen und zu authentifizieren. Der Zweck der Erstellung eines separaten FTD-Kontos besteht darin, den unbefugten Zugriff an anderen Stellen im Netzwerk zu verhindern, wenn die für die Bindung verwendeten Anmeldeinformationen beeinträchtigt werden. Dieses Konto muss nicht im Rahmen der Basis-DN liegen.

1. Klicken Sie in **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf den Container/die Organisation, dem das FTD-Konto hinzugefügt wird. In dieser Konfiguration wird das FTD-Konto unter dem Benutzercontainer unter dem Benutzernamen **ftd.admin@example.com** hinzugefügt. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und klicken Sie dann auf **Neu > Benutzer**.



2. Navigieren Sie durch den Assistenten **New Object - User**.



New Object - User

Create in: example.com/Users

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

New Object - User

Create in: example.com/Users

When you click Finish, the following object will be created:

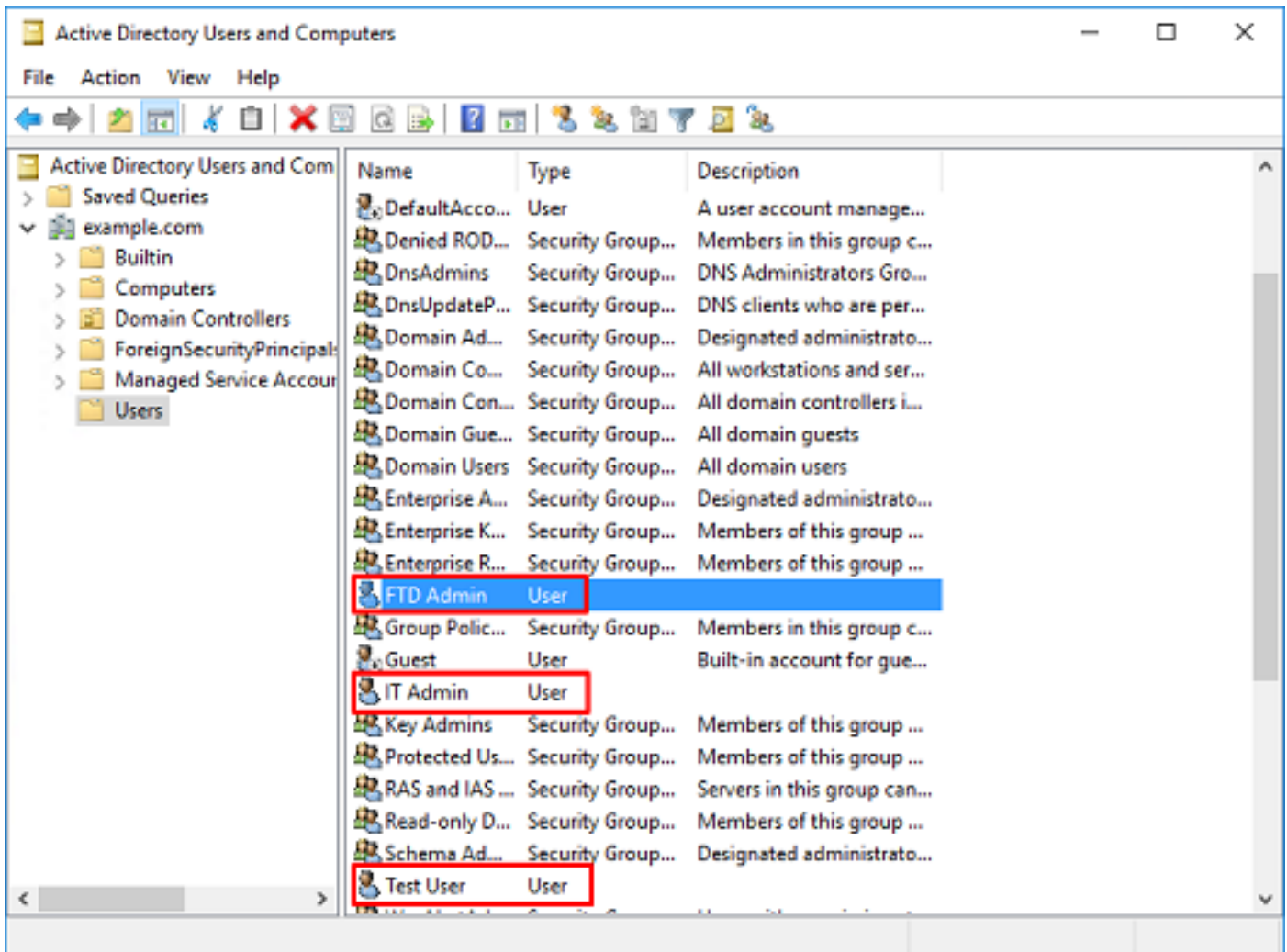
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

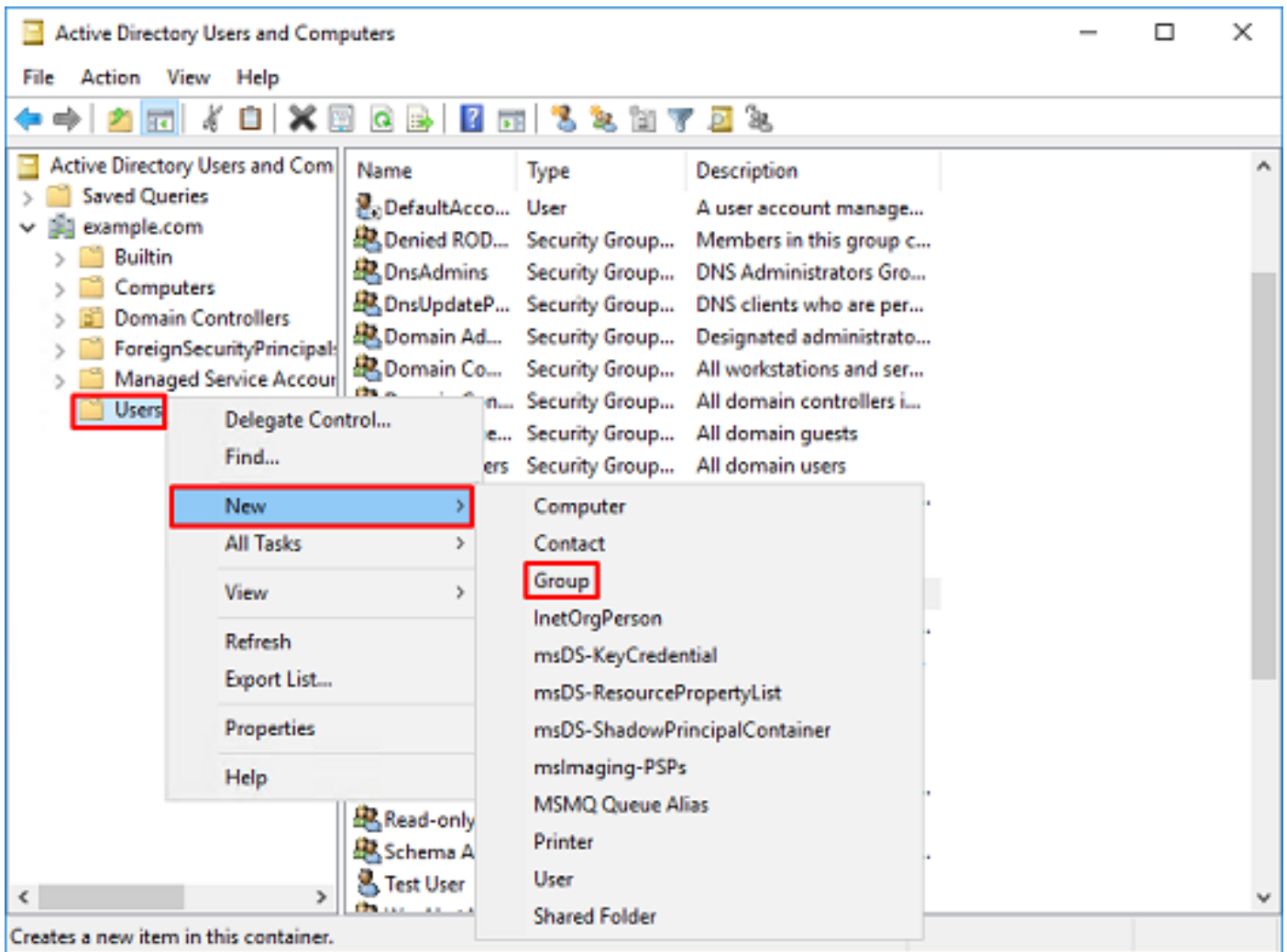
3. Überprüfen Sie, ob das FTD-Konto erstellt wurde. Darüber hinaus wurden zwei zusätzliche Konten erstellt: **IT-Administrator** und **Testbenutzer**.



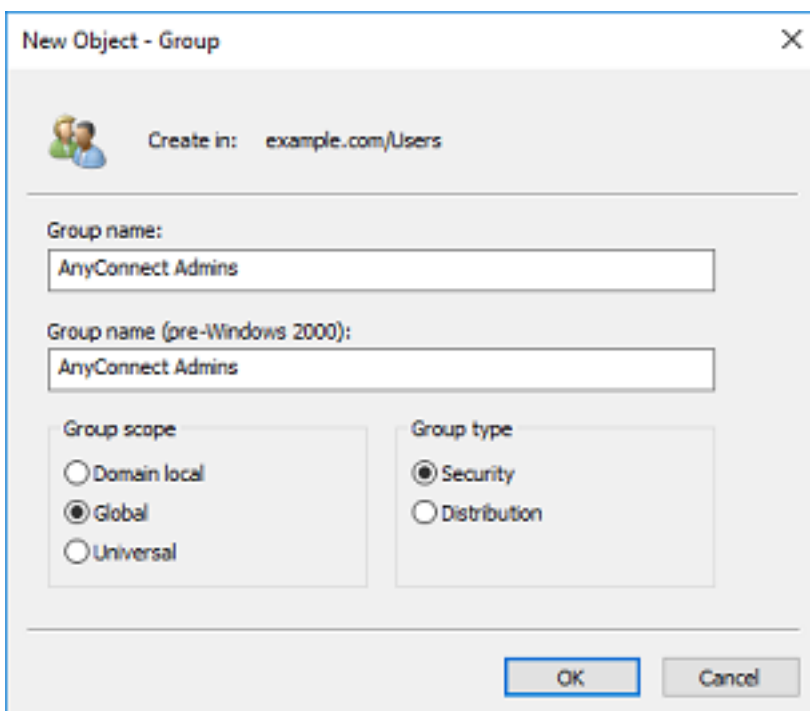
## AD-Gruppen erstellen und AD-Gruppen Benutzer hinzufügen (optional)

Obwohl die Authentifizierung nicht erforderlich ist, können Gruppen verwendet werden, um die Anwendung von Zugriffsrichtlinien auf mehrere Benutzer sowie die LDAP-Autorisierung zu vereinfachen. In diesem Konfigurationsleitfaden werden Gruppen verwendet, um die Richtlinieneinstellungen für die Zugriffskontrolle später über die Benutzeridentität innerhalb des FDM anzuwenden.

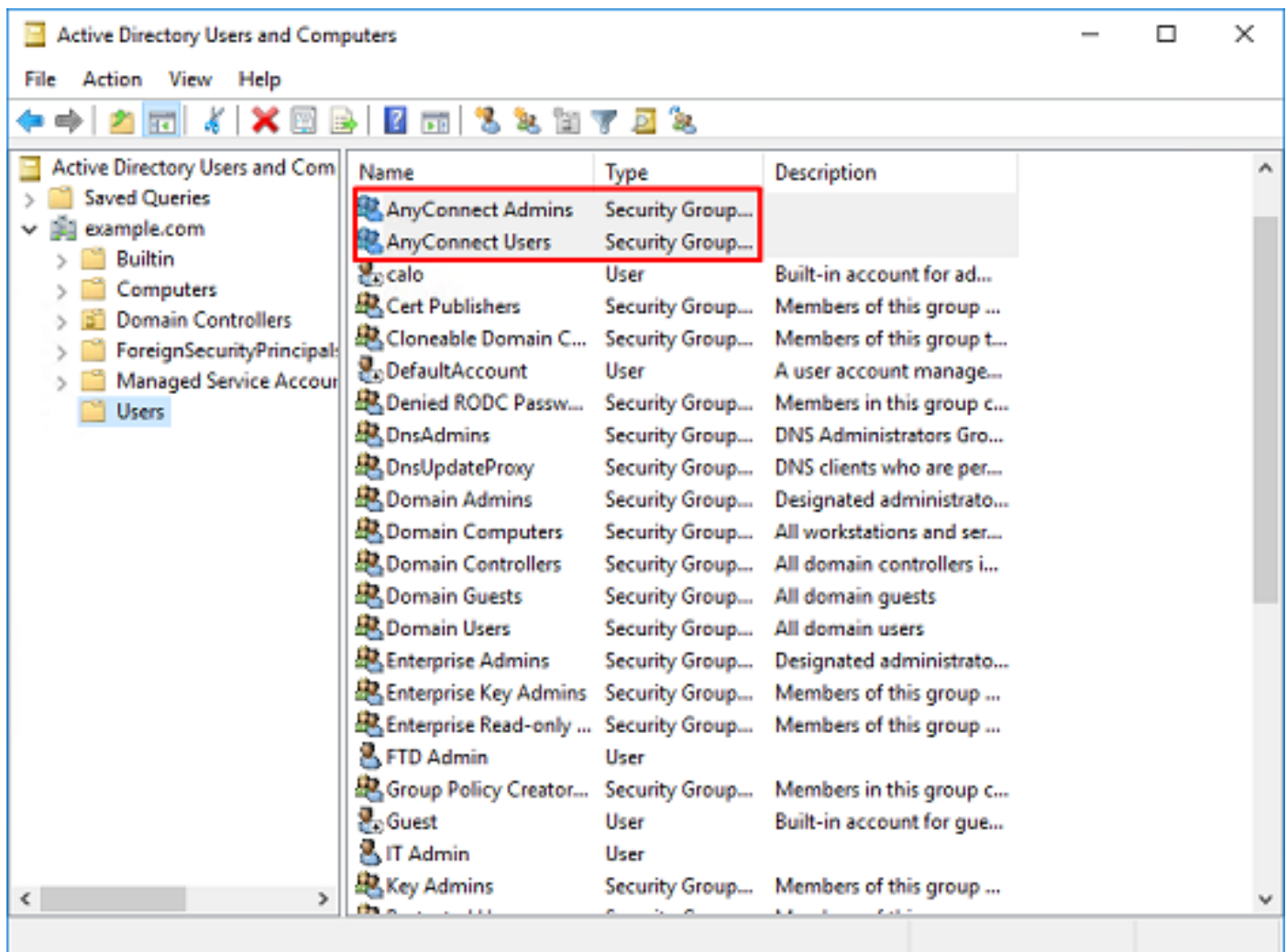
1. Klicken Sie in **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf den Container bzw. die Organisation, der bzw. der die neue Gruppe hinzugefügt wird. In diesem Beispiel wird die Gruppe **AnyConnect-Administratoren** unter dem Benutzercontainer hinzugefügt. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und klicken Sie dann auf **Neu > Gruppe**.



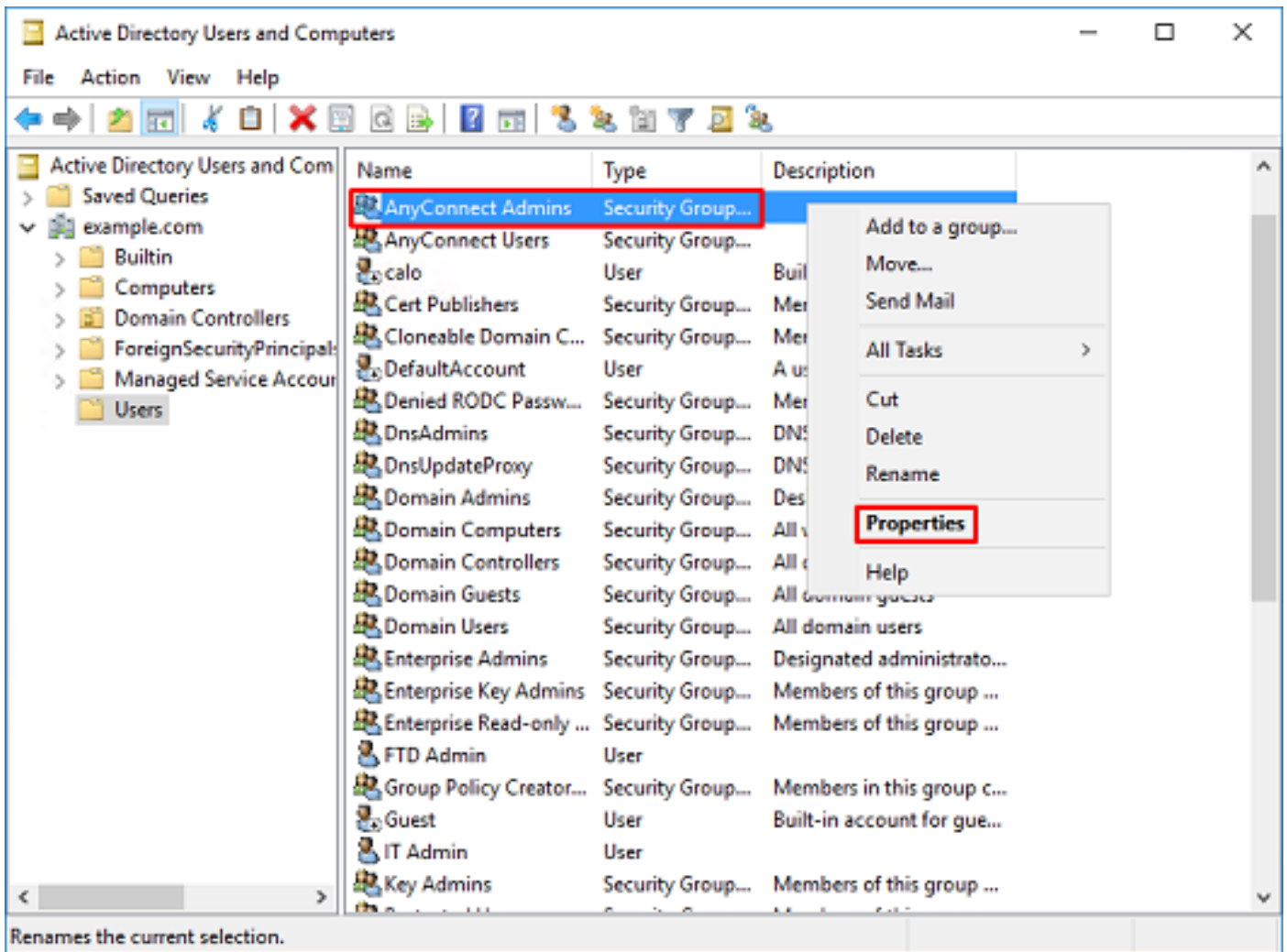
2. Navigieren Sie durch den Assistenten **New Object - Group** (Neues Objekt - Gruppe), wie im Bild gezeigt.



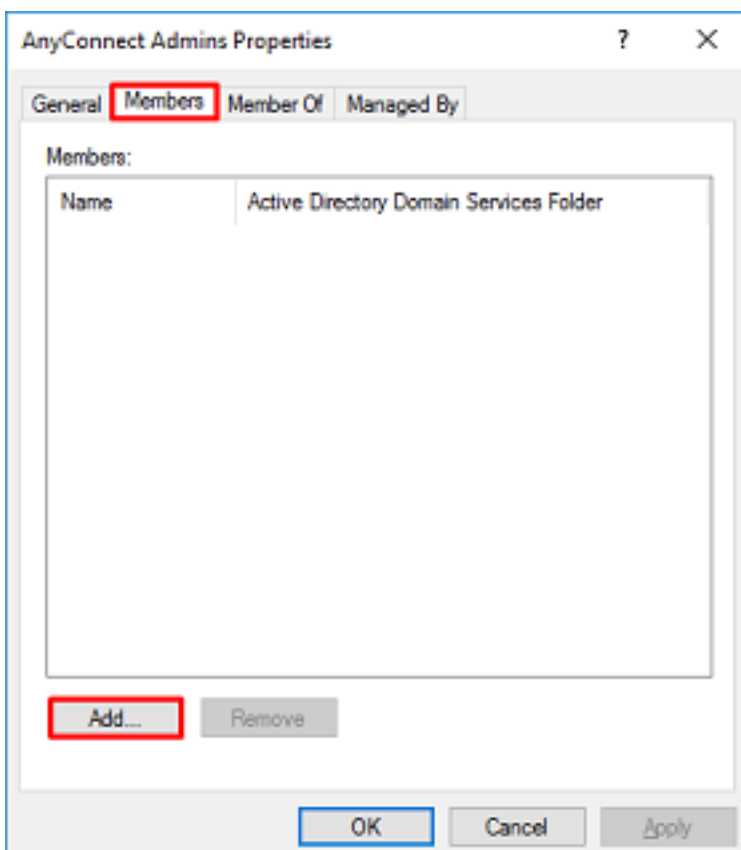
3. Überprüfen Sie, ob die Gruppe erstellt wurde. Die Gruppe **AnyConnect-Benutzer** wurde ebenfalls erstellt.



4. Klicken Sie mit der rechten Maustaste auf die Gruppe, der der Benutzer hinzugefügt wird, und wählen Sie dann **Eigenschaften aus**. In dieser Konfiguration wird der Benutzer **IT-Administrator** der Gruppe **AnyConnect-Administratoren** hinzugefügt, und der Benutzer **Test-Benutzer** wird der Gruppe **AnyConnect-Benutzer** hinzugefügt.

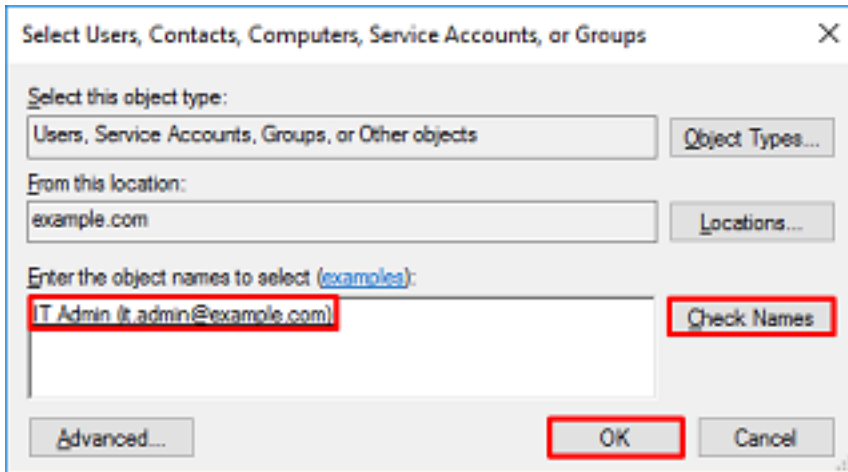


5. Klicken Sie auf die Registerkarte **Members** und anschließend auf **Add** (Hinzufügen), wie im Bild gezeigt.

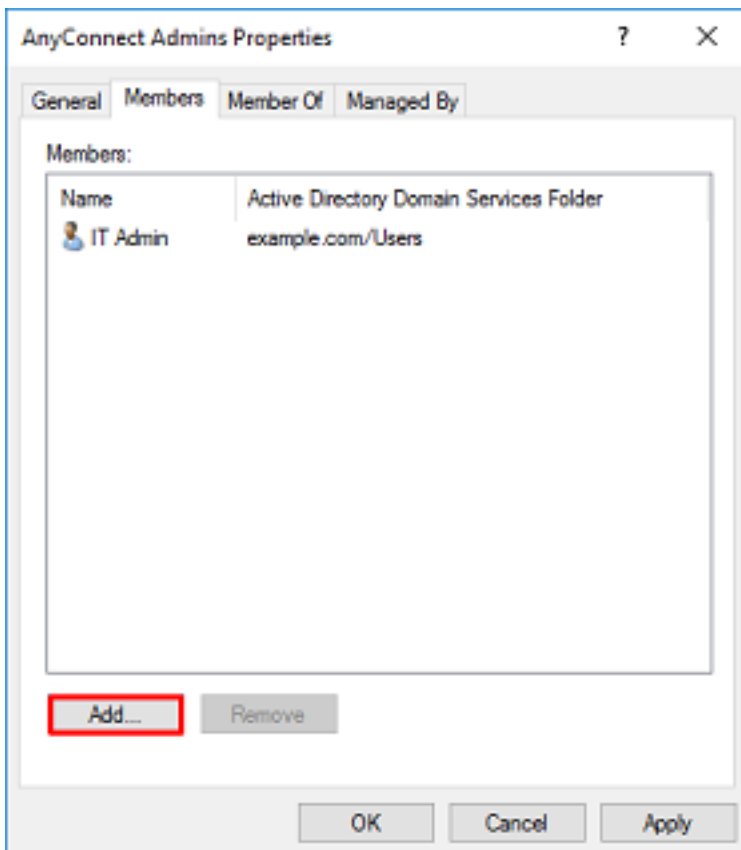




Geben Sie den Benutzer in das Feld ein, und klicken Sie auf die Schaltfläche **Namen überprüfen**, um zu überprüfen, ob der Benutzer gefunden wurde. Klicken Sie nach der Überprüfung auf **OK**.

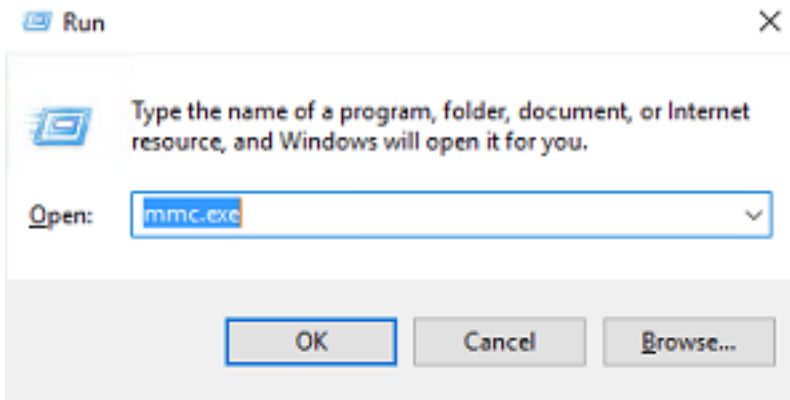


Überprüfen Sie, ob der richtige Benutzer hinzugefügt wurde, und klicken Sie dann auf die Schaltfläche **OK**. Der Benutzer Testbenutzer wird auch zur Gruppe AnyConnect-Benutzer hinzugefügt, wobei dieselben Schritte verwendet werden.

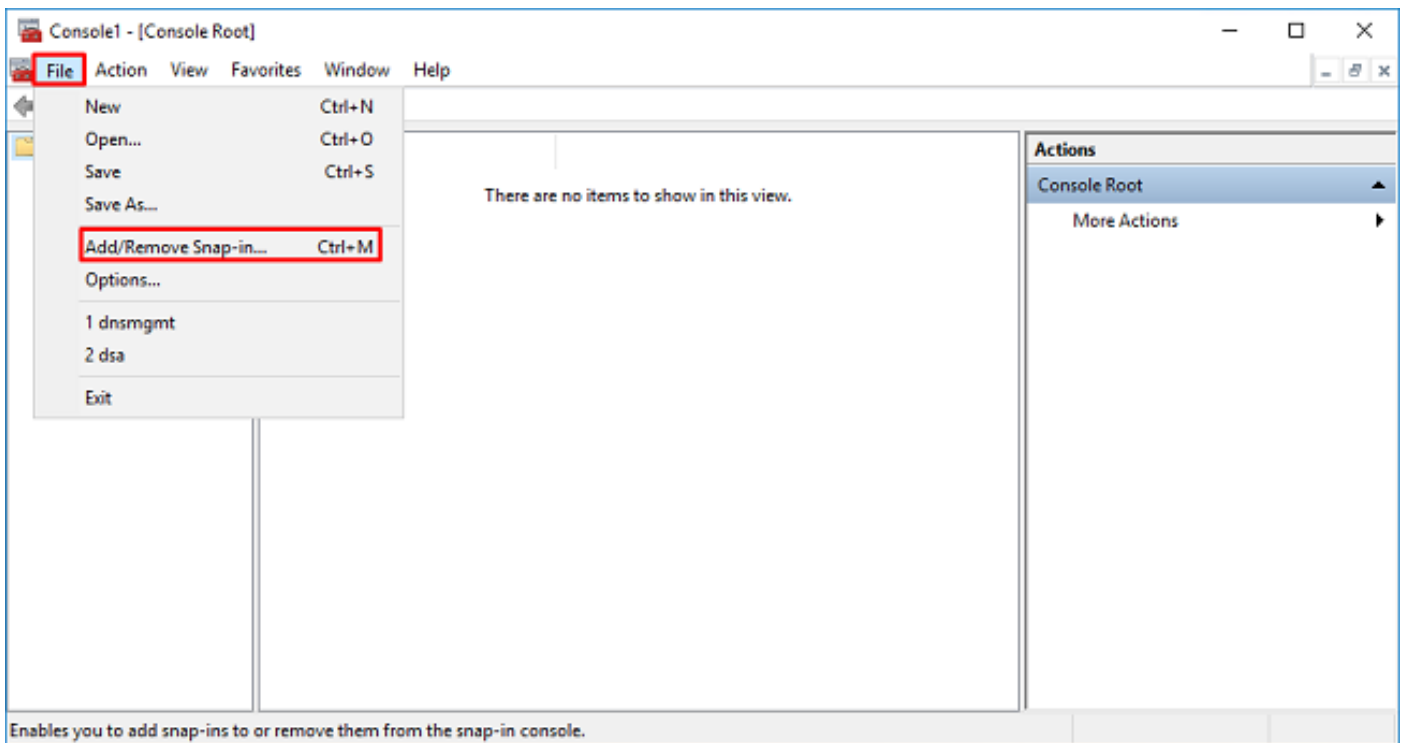


Kopieren Sie die LDAS SSL-Zertifikatsroot (nur für LDAPS oder STARTTLS erforderlich).

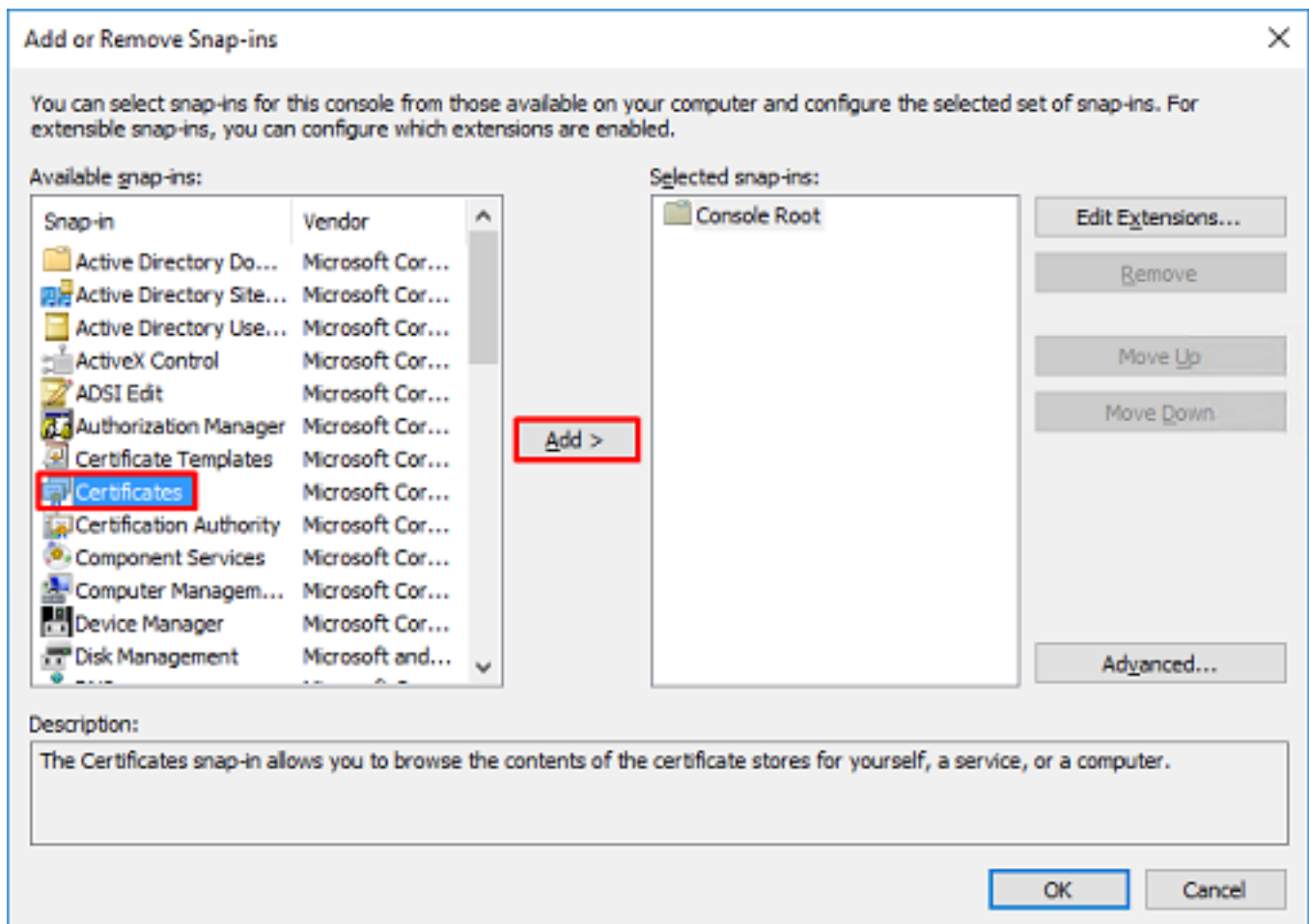
1. Drücken Sie **Win+R**, und geben Sie **mmc.exe** ein. Klicken Sie auf **OK**.



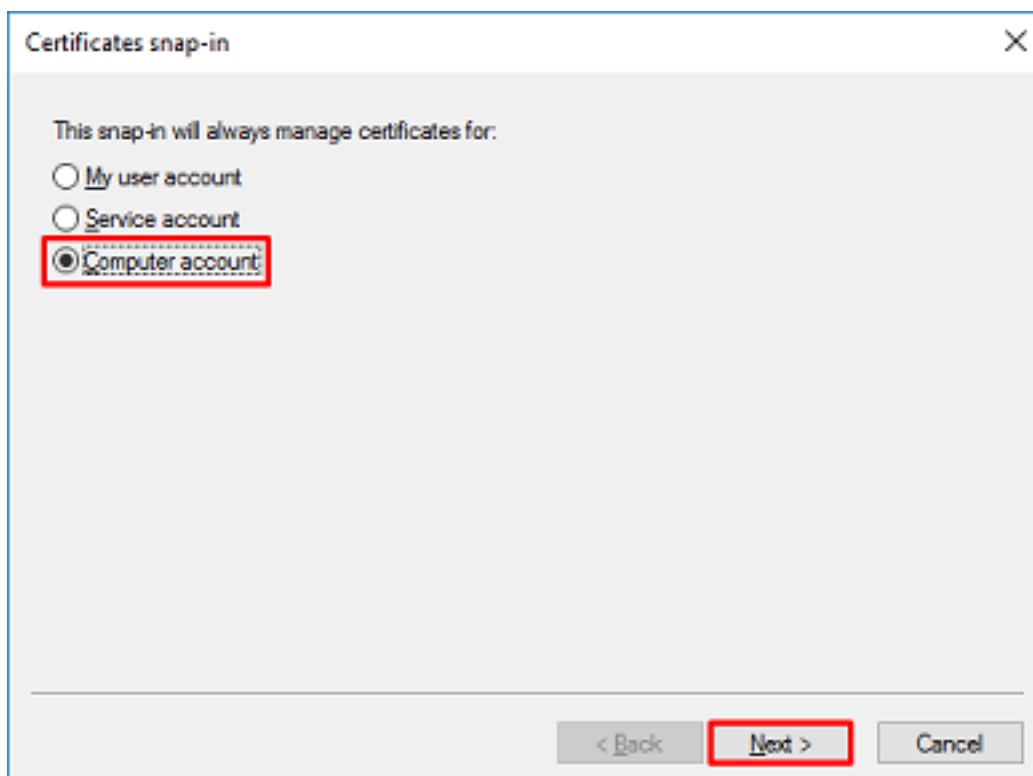
2. Navigieren Sie zu **Datei > Snap-In hinzufügen/entfernen...** wie im Bild gezeigt.



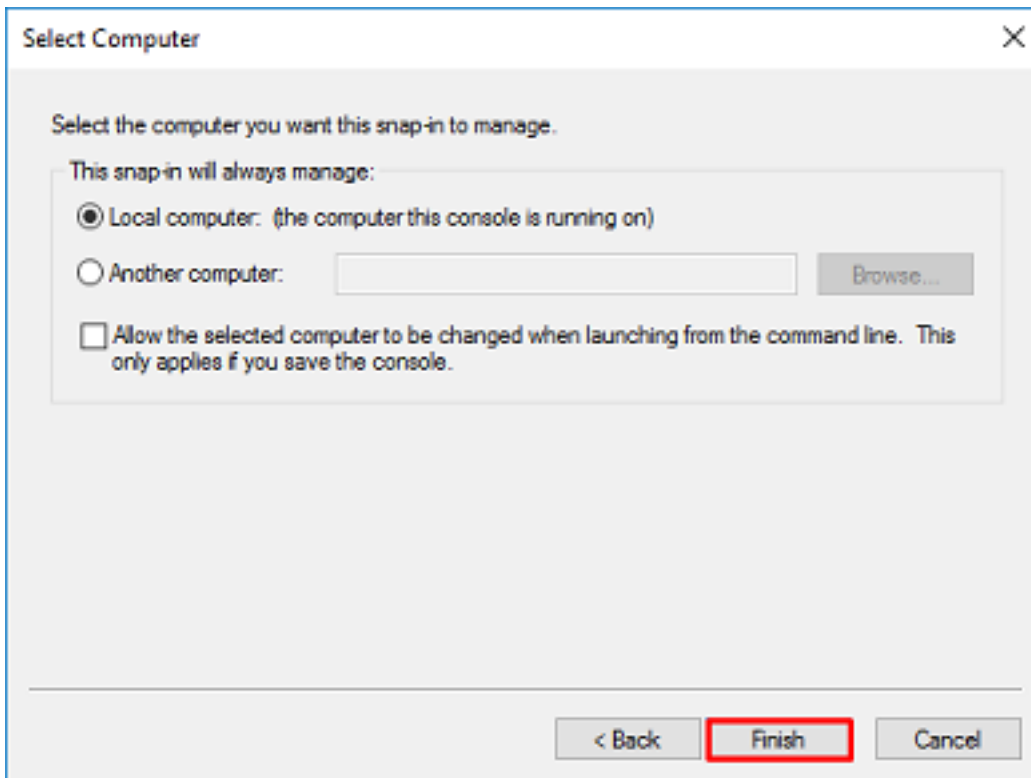
3. Klicken Sie unter **Verfügbare Snap-Ins** auf **Zertifikate** und dann auf **Hinzufügen**.



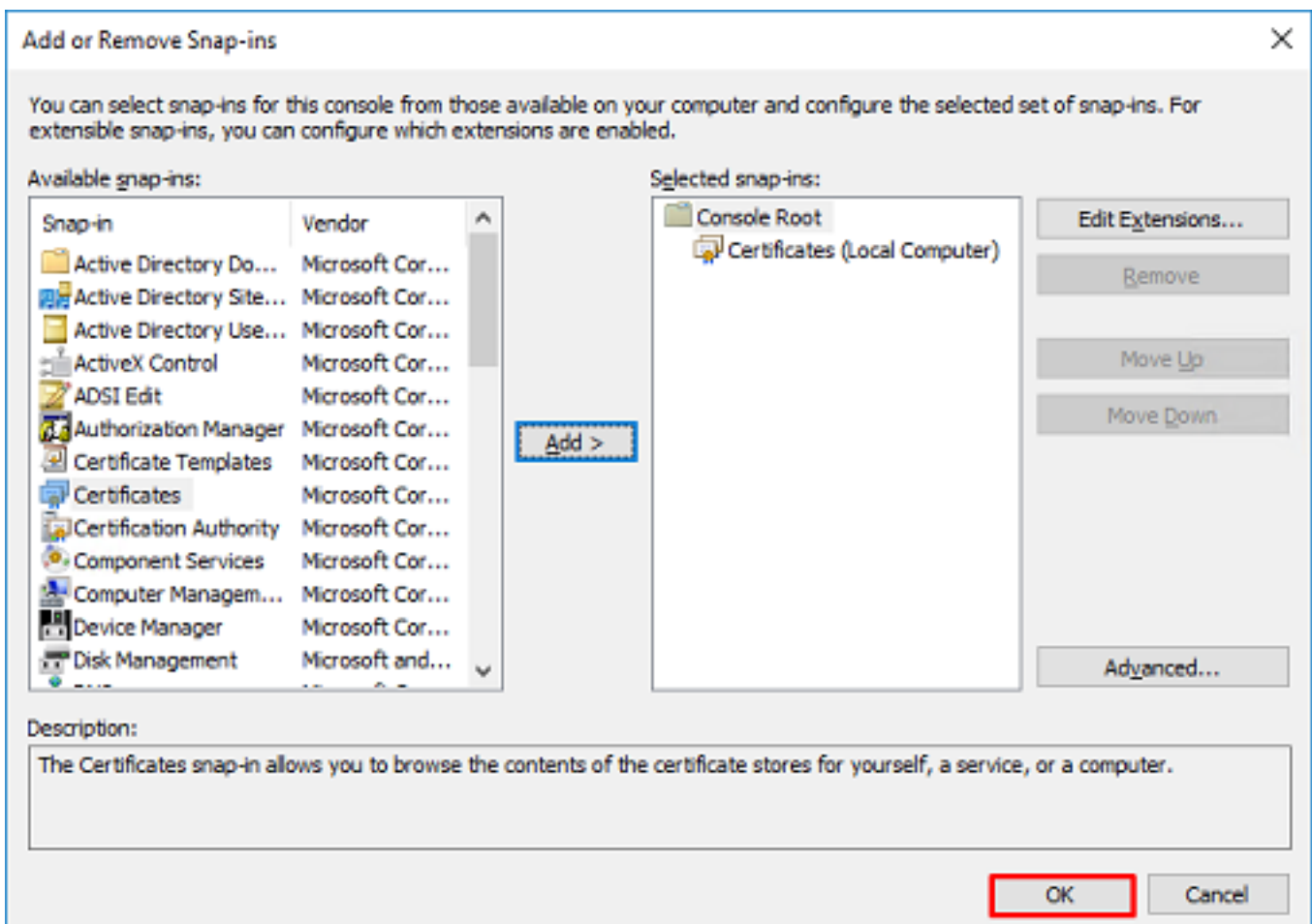
4. Wählen Sie **Computerkonto** aus, und klicken Sie dann wie im Bild gezeigt auf **Weiter**.



Klicken Sie auf **Fertig stellen**.



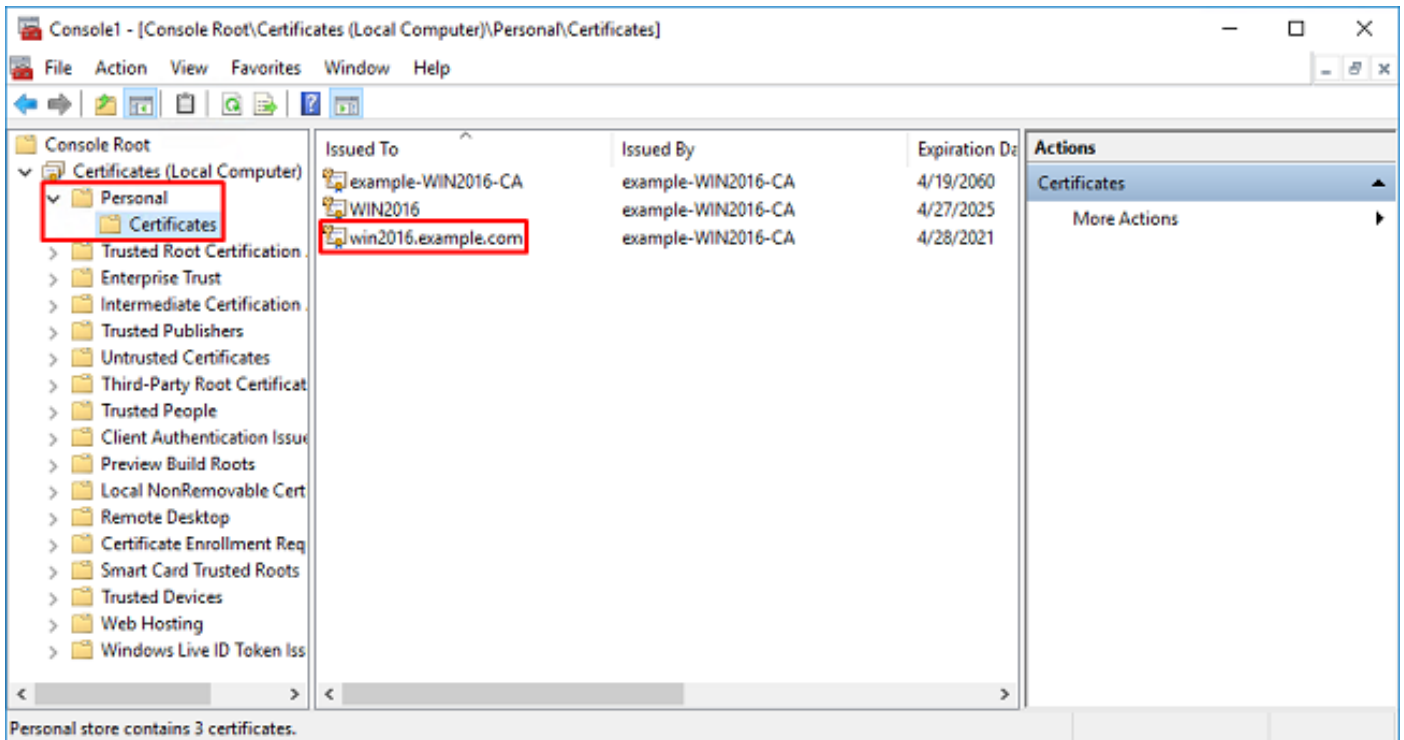
5. Klicken Sie auf OK.



6. Erweitern Sie den **persönlichen** Ordner, und klicken Sie dann auf **Zertifikate**. Das von LDAPS verwendete Zertifikat muss an den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) des Windows-Servers ausgestellt werden. Auf diesem Server sind drei Zertifikate aufgelistet.

- Ein Zertifizierungsstellenzertifikat, das an und von Beispiel-WIN2016-CA ausgestellt wird.
- Ein Identitätszertifikat, das WIN2016 vom Beispiel-WIN2016-CA ausgestellt wurde.
- Ein Identitätszertifikat, das von example-WIN2016-CA für win2016.example.com ausgestellt wurde.

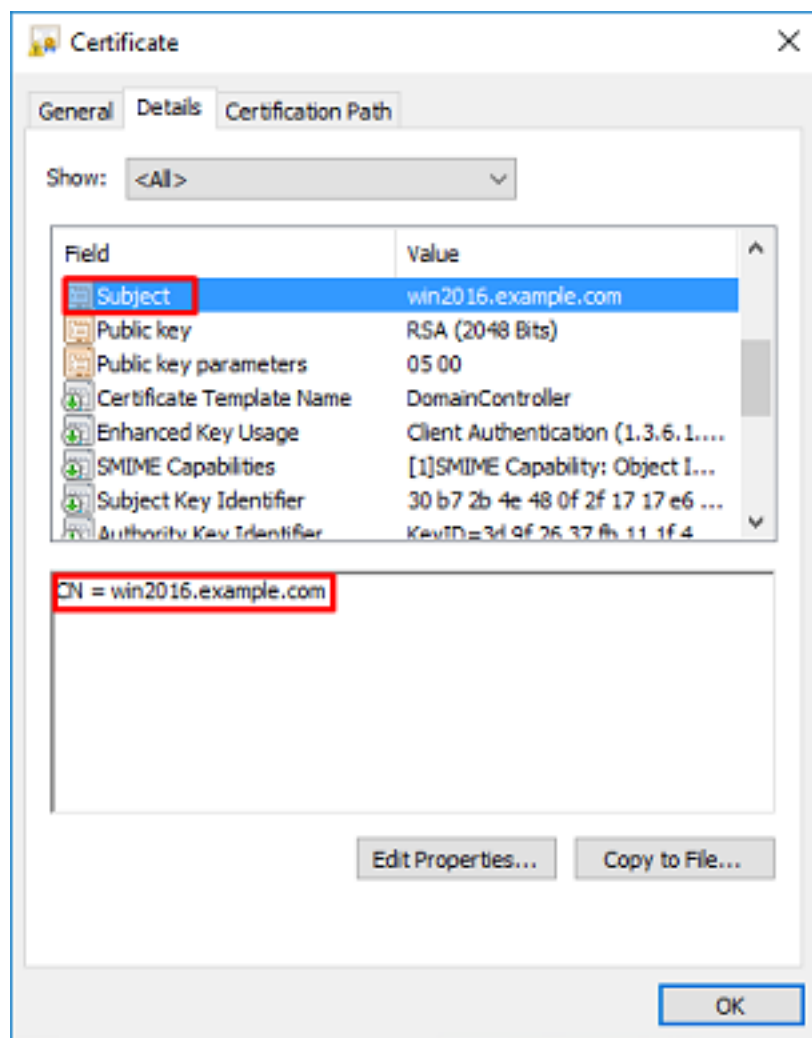
In diesem Konfigurationsleitfaden lautet der FQDN "win2016.example.com", daher sind die ersten beiden Zertifikate nicht für die Verwendung als LDAPS SSL-Zertifikat gültig. Das für win2016.example.com ausgestellte Identitätszertifikat ist ein Zertifikat, das automatisch vom Zertifizierungsstellendienst für Windows Server ausgestellt wurde. Doppelklicken Sie auf das Zertifikat, um die Details zu überprüfen.

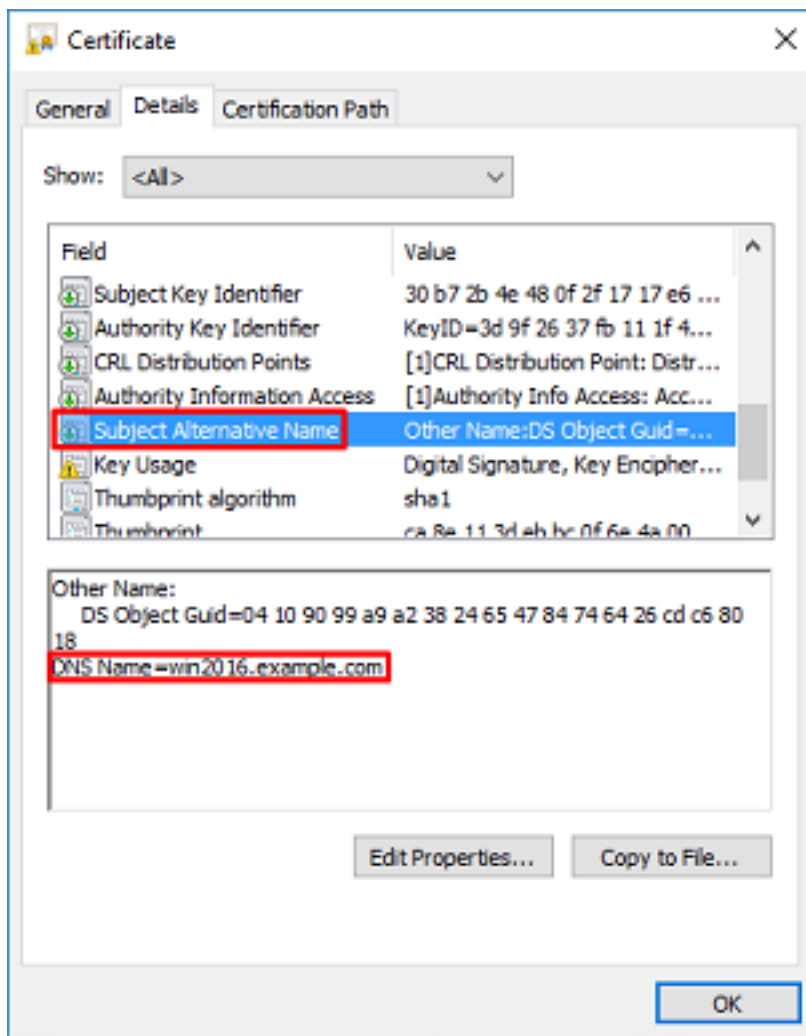


7. Um als LDAPS SSL-Zertifikat verwendet zu werden, muss das Zertifikat die folgenden Anforderungen erfüllen:

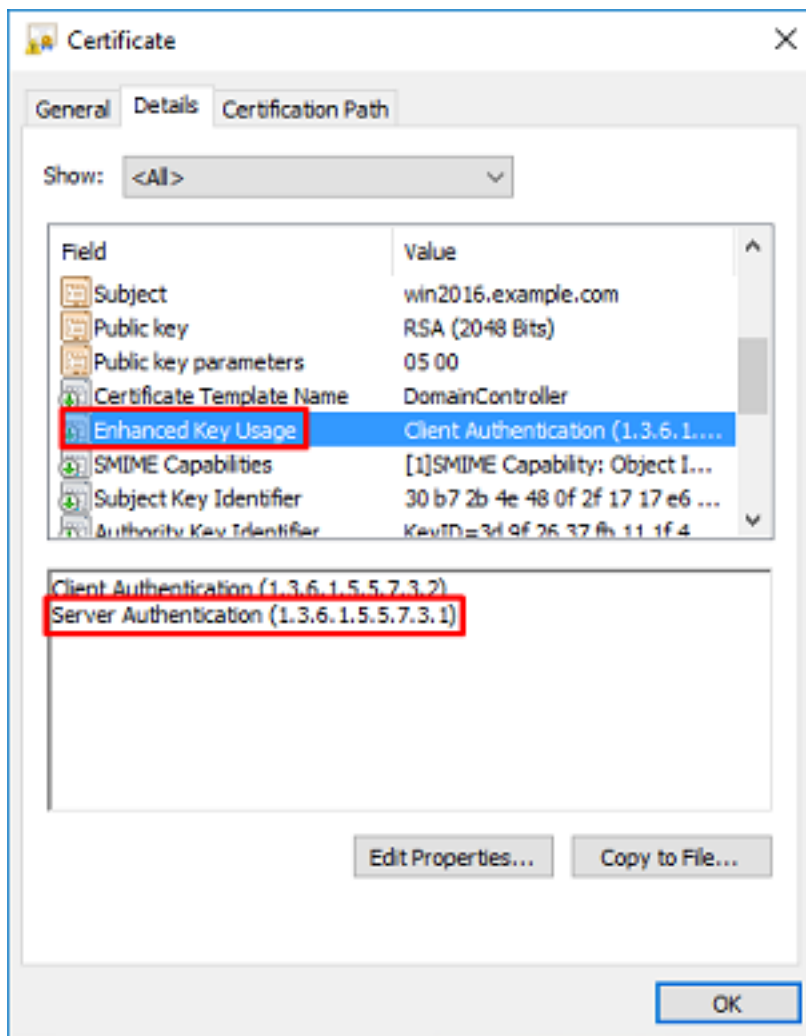
- Der allgemeine Name oder der alternative DNS-Betreff-Name entspricht dem FQDN des Windows-Servers.
- Das Zertifikat verfügt über eine Serverauthentifizierung im Feld Verwendung des erweiterten Schlüssels.

Auf der Registerkarte Details des Zertifikats unter dem **Betreff** und dem **Betreff Alternative Name** ist FQDN **win2016.example.com** vorhanden.



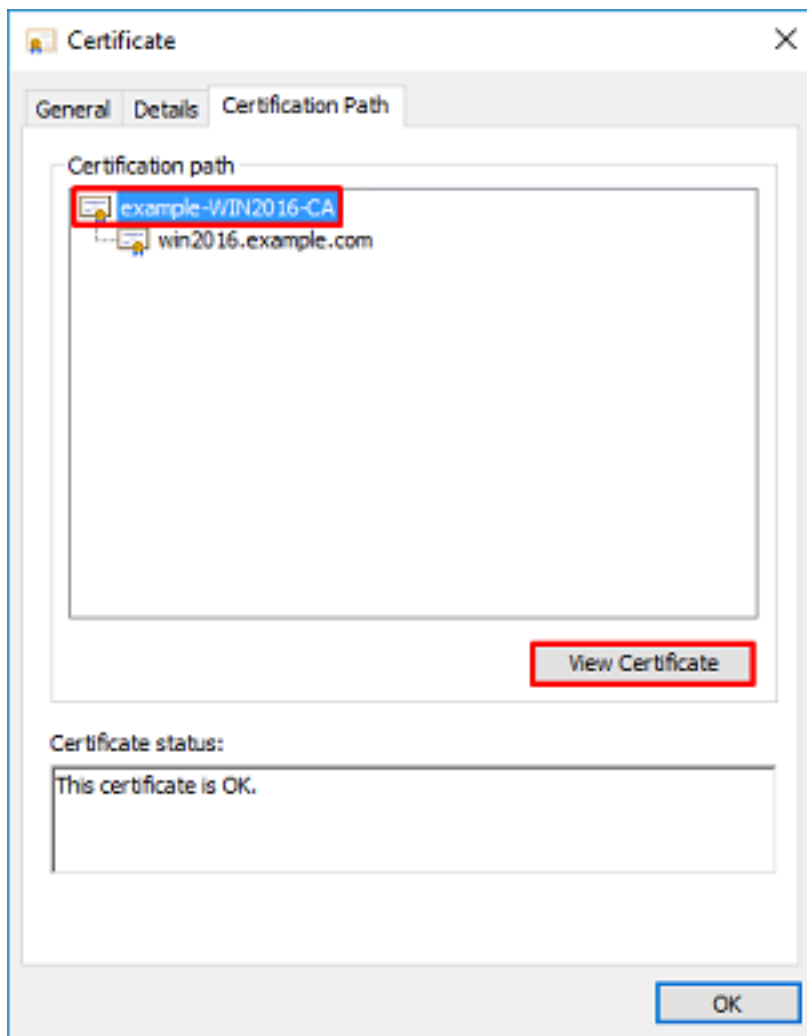


Unter **Erweiterte Schlüsselerwendung** ist **Serverauthentifizierung** vorhanden.

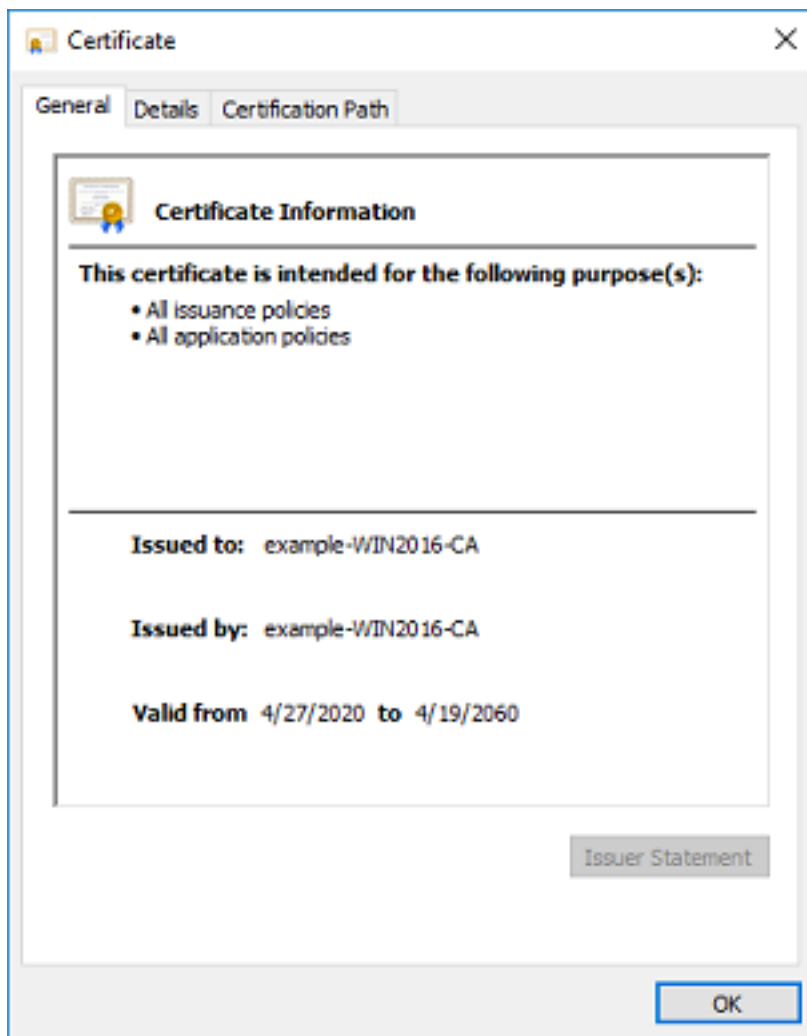


8. Navigieren Sie nach der Bestätigung zur Registerkarte **Zertifizierungspfad**. Klicken Sie auf das oberste Zertifikat, das das Stammzertifikat der Zertifizierungsstelle sein soll, und klicken Sie dann auf die Schaltfläche **Zertifikat anzeigen**.

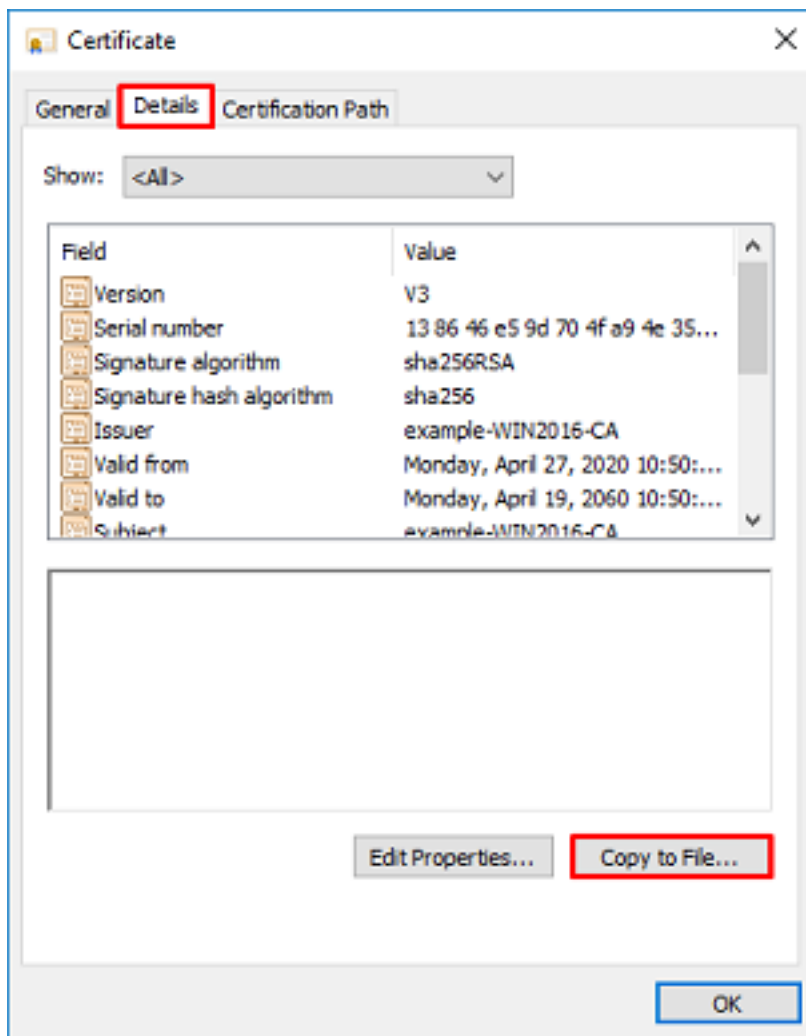




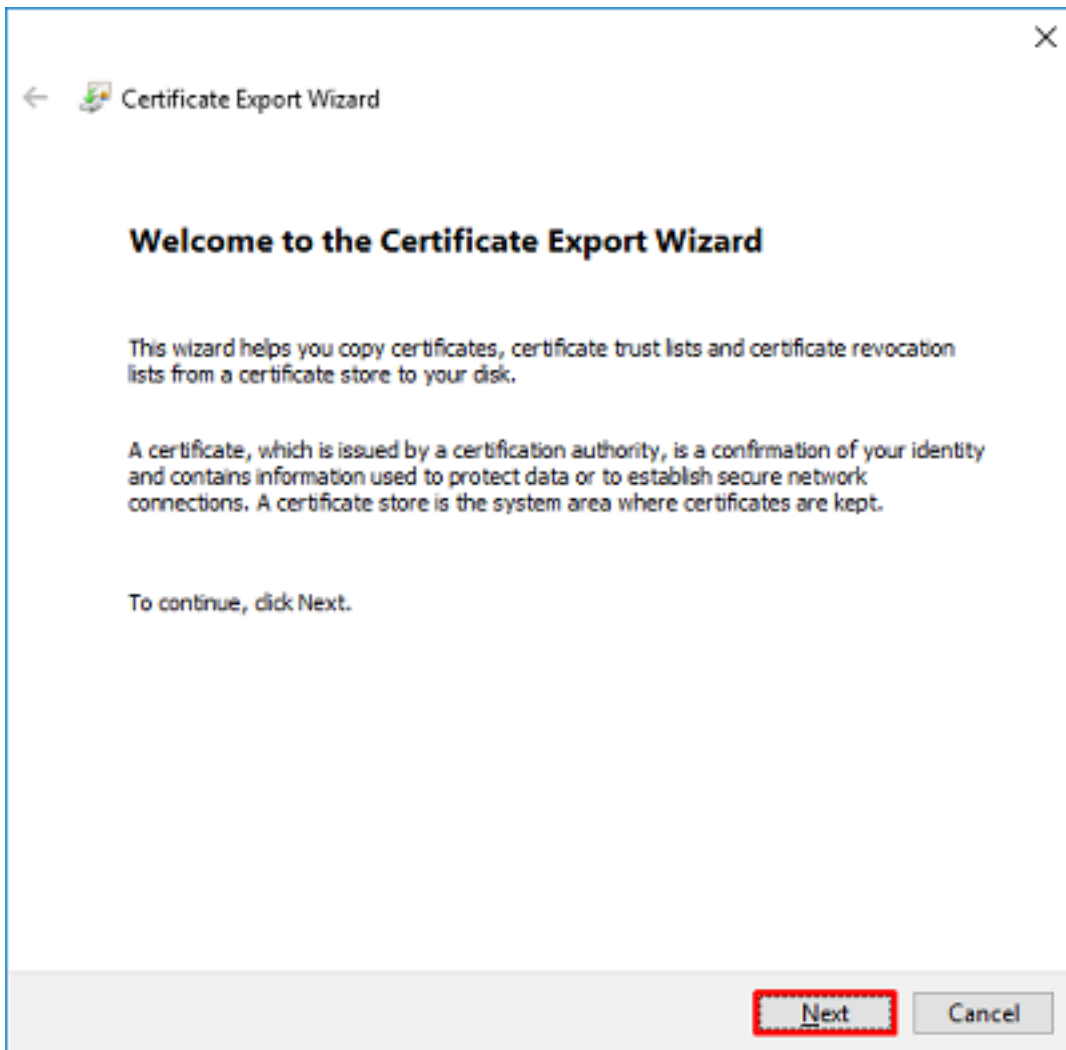
9. Dadurch werden die Zertifikatdetails für das Stammzertifikat der CA geöffnet.



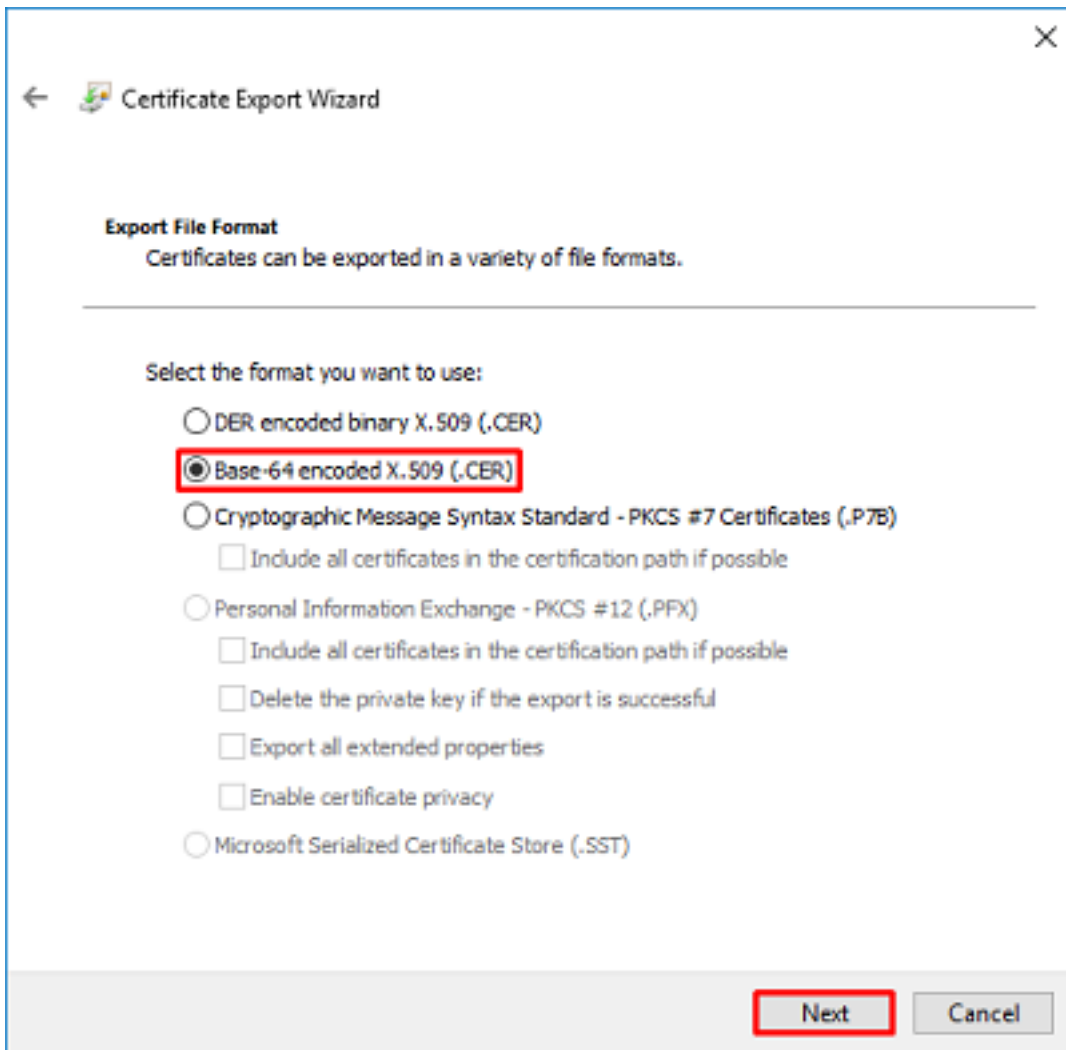
10. Öffnen Sie die Registerkarte **Details**, und klicken Sie dann auf **In Datei kopieren...** wie im Bild gezeigt.



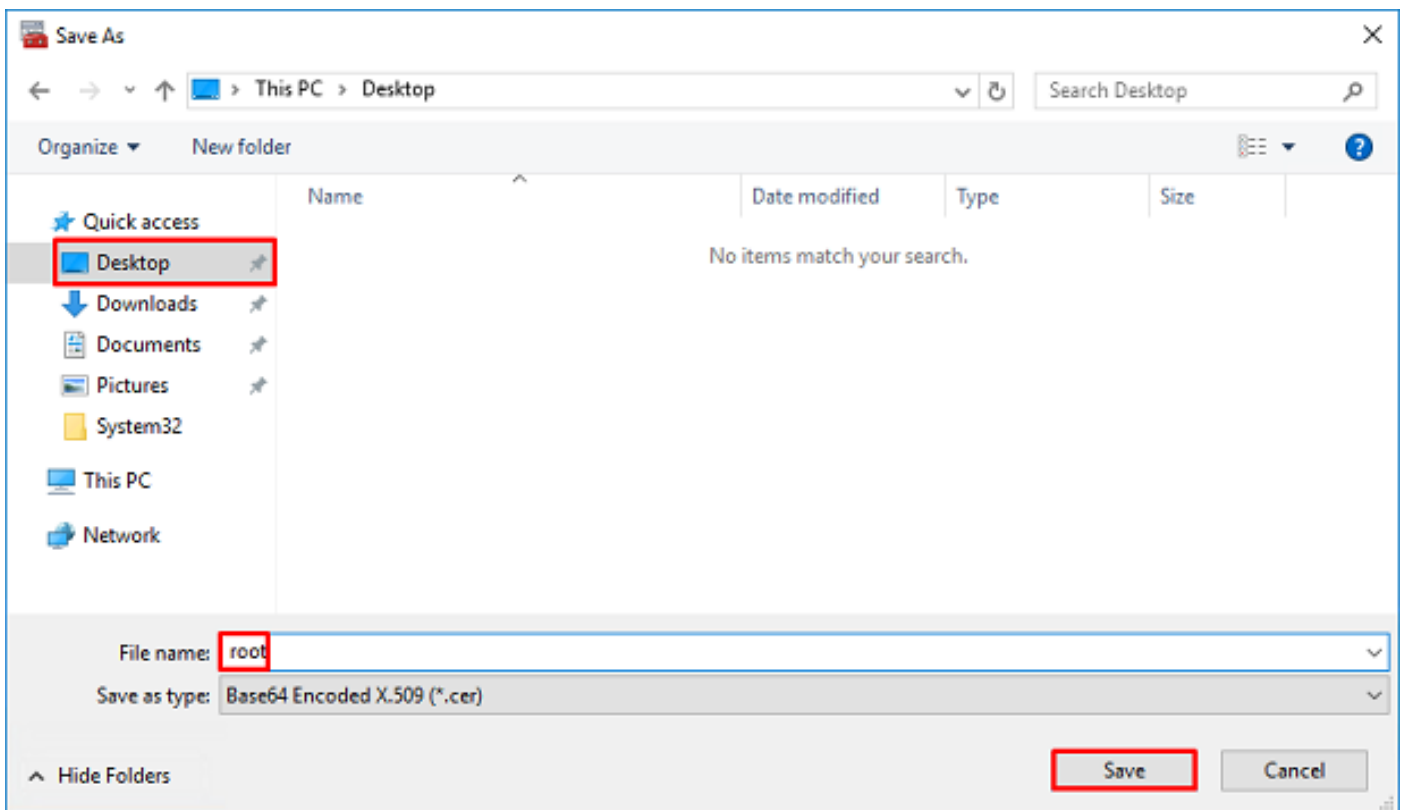
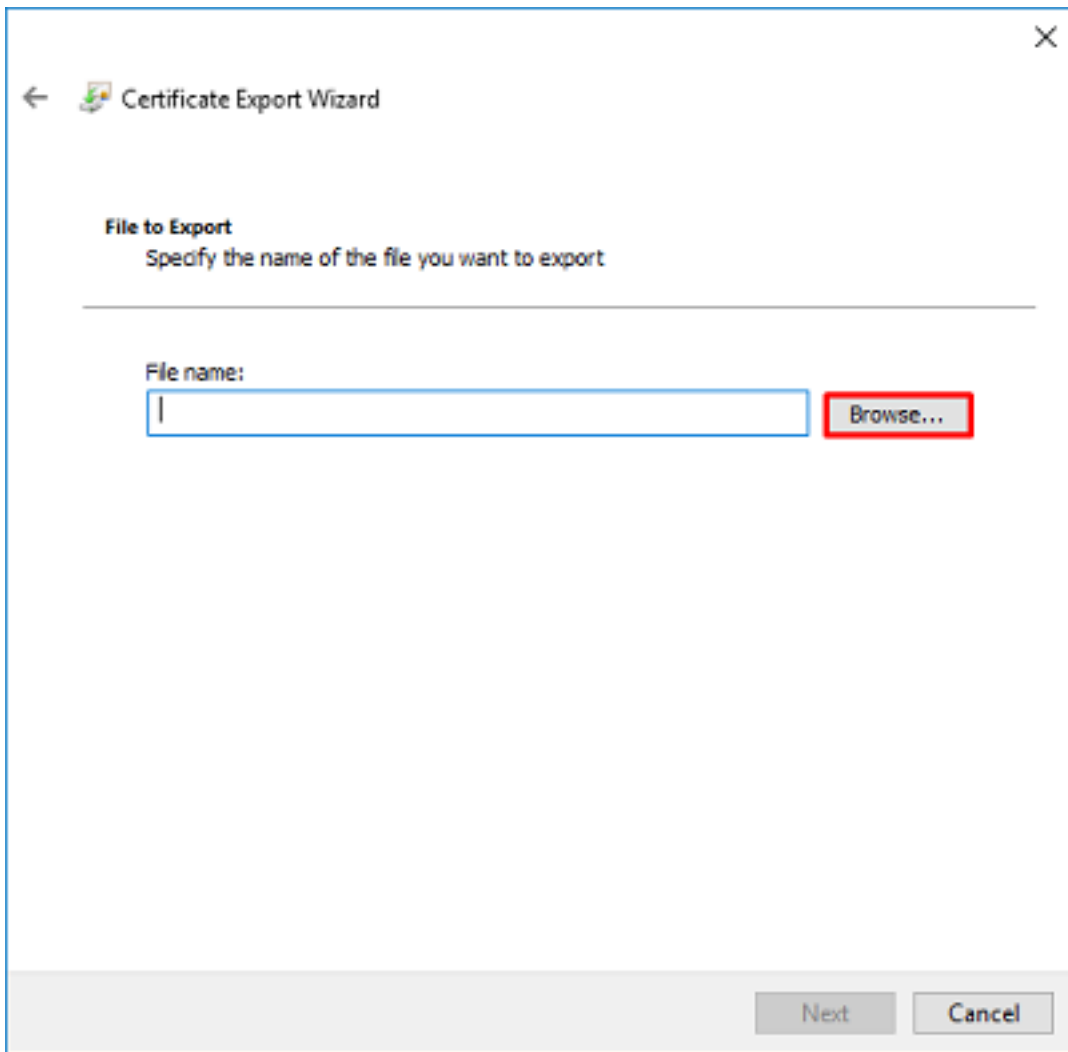
11. Navigieren Sie durch den Assistenten für den Zertifikatsexport, der die Stammzertifizierungsstelle im PEM-Format exportiert.

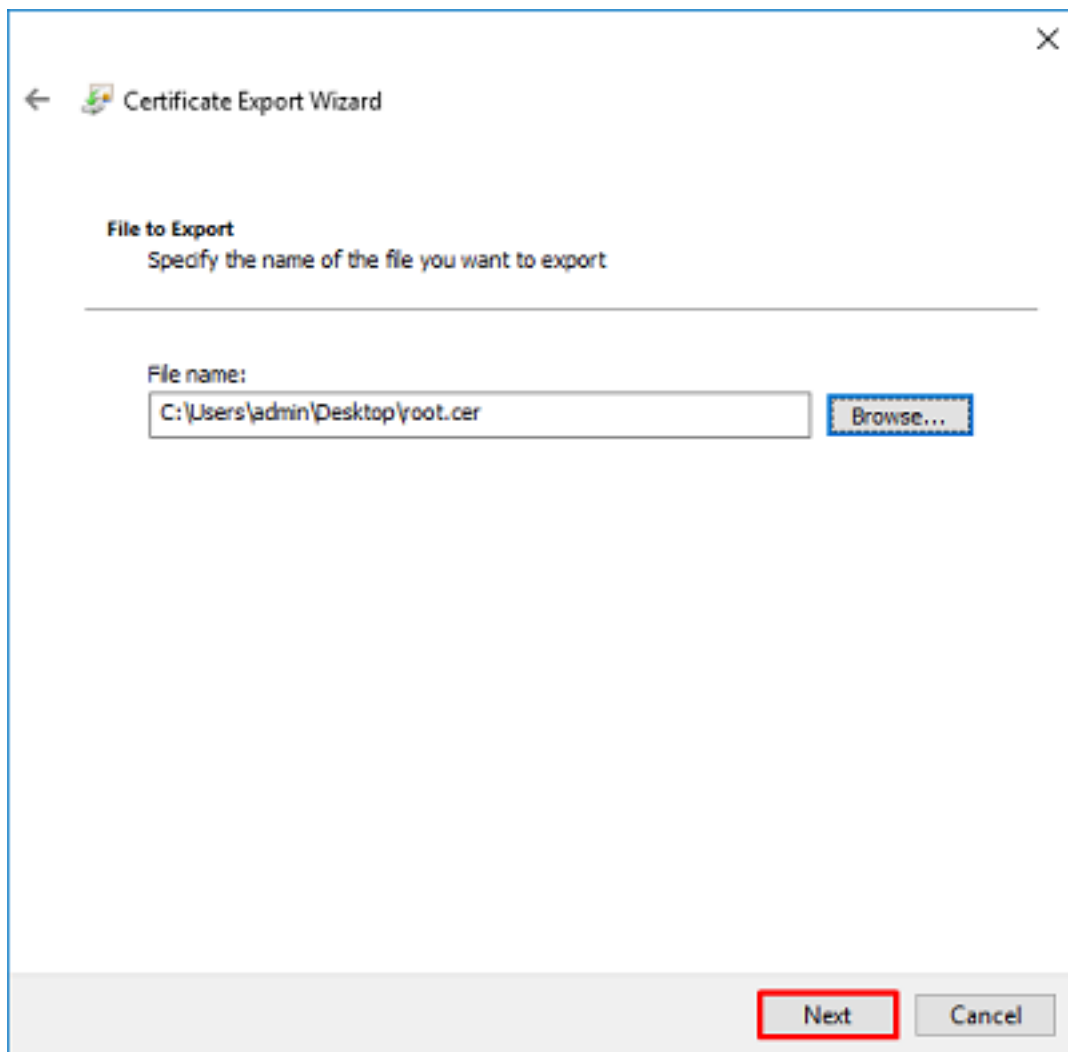


12. Wählen Sie **Base-64-verschlüsseltes X.509** aus.

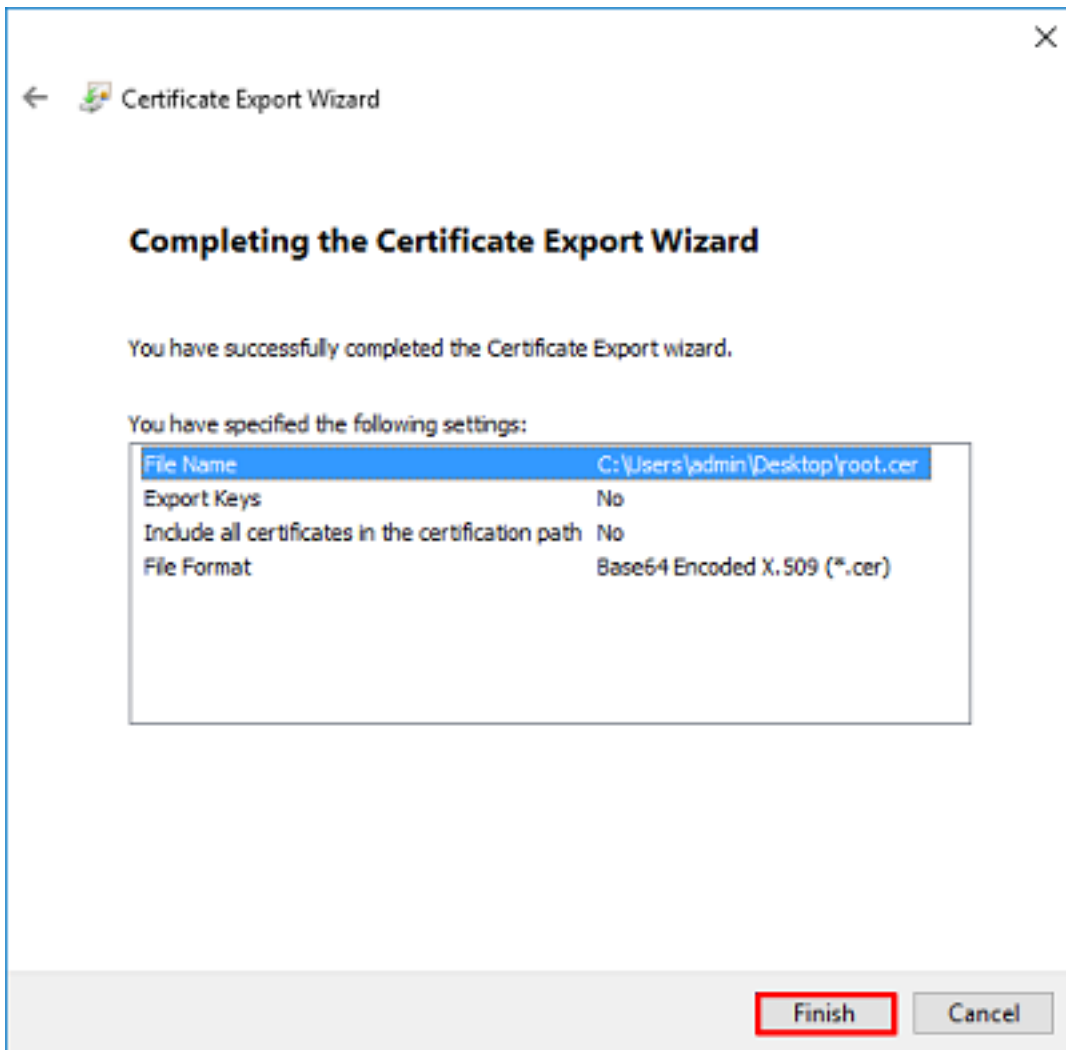


13. Wählen Sie den Namen der Datei und den Speicherort aus, in den die Datei exportiert werden soll.





14. Klicken Sie auf **Fertig stellen**.



15. Navigieren Sie jetzt zum Speicherort, und öffnen Sie das Zertifikat mit einem Notizblock oder einem anderen Texteditor. Es wird das PEM-Formatzertifikat angezeigt. Speichern Sie diese Datei später.

```
-----BEGIN CERTIFICATE-----
MIIDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExJleGftcGx1LVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlamb0xGzAZBgNVBAMTEV4YW1wbGUtV01OMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GAlUdEwEB/wQFMAMBAf8wHQYDVDR0
BBYEFD2fJjf7ER9EM/HCxVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq620FpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAet7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgrEtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxstscubR1+d
dLEFKQqmMeYvkVf+a7a64mqPzSG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixwPdrbADO6zMhbEYehkh00jBrUEBBI6Cy83iTZ9ejsk
KgWBJXEu33PplW6E
-----END CERTIFICATE-----
```

## FDM-Konfigurationen



## Lizenzierung überprüfen

Um AnyConnect auf FDM zu konfigurieren, muss die FTD beim Smart Licensing-Server registriert und eine gültige Plus-, Apex- oder VPN Only-Lizenz auf das Gerät angewendet werden.

1. Navigieren Sie zu **Gerät > Smart License** wie im Bild gezeigt.

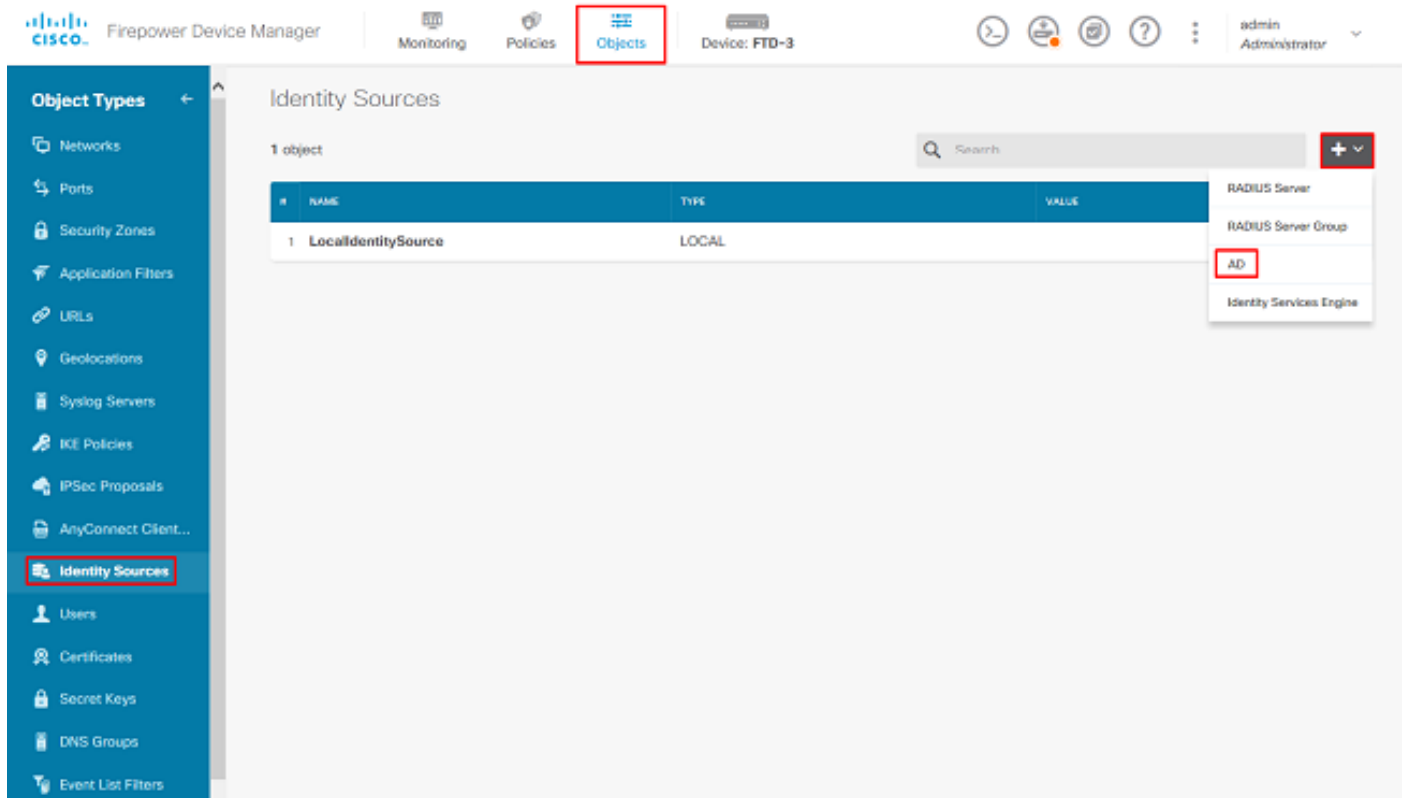
The screenshot shows the Cisco Firepower Device Manager (FDM) interface. At the top, the navigation menu includes Monitoring, Policies, Objects, and a highlighted **Device: FTD-3**. Below the navigation is a network diagram showing the device connected to an Inside Network and an Internet cloud. The Internet cloud contains services like DNS Server, NTP Server, and Smart License. Below the diagram are several configuration panels: Interfaces (Connected, Enabled 3 of 4), Routing (2 routes), Updates (Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds), System Settings (Management Access, Logging Settings, DHCP Server, DNS Server, Management interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences), Backup and Restore, and Troubleshoot (No files created yet). The **Smart License** panel is highlighted with a red box, showing it is **Registered** and has a **View Configuration** link.

2. Überprüfen Sie, ob die FTD beim Smart Licensing Server registriert ist und die AnyConnect Plus-, Apex- oder VPN Only-Lizenz aktiviert ist.

The screenshot shows the Cisco Firepower Device Manager (FDM) interface for the Smart License configuration page of device FTD-3. The page title is **Smart License**. It shows the device is **CONNECTED** with a **SUFFICIENT LICENSE**. The last sync was on 16 Apr 2020 08:27 AM and the next sync is on 16 Apr 2020 08:37 AM. Below this, there are four license configuration cards: Threat (Disabled by user, ENABLE button), Malware (Disabled by user, ENABLE button), URL License (Enabled, DISABLE button), and RA VPN License (Enabled, Type PLUS, DISABLE button). The RA VPN License card is highlighted with a red box. The RA VPN License card includes a description: "Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license." and includes "RA-VPN".

## AD-Identitätsquelle einrichten

1. Navigieren Sie zu **Objekte > Identitätsquellen**, klicken Sie dann auf das **+**-Symbol, und wählen Sie **AD** wie im Bild dargestellt aus.



2. Füllen Sie die entsprechenden Einstellungen für den Active Directory-Server mit den zuvor gesammelten Informationen aus. Wenn für den Microsoft-Server anstelle einer IP-Adresse ein Hostname (FQDN) verwendet wird, stellen Sie sicher, dass unter **Objects > DNS Group (Objekte > DNS-Gruppe)** eine entsprechende DNS-Gruppe erstellt wird. Wenden Sie dann diese DNS-Gruppe auf die FTD an, indem Sie zu **Device > System Settings > DNS Server** navigieren, die DNS-Gruppe unter der **Management Interface (Verwaltungsschnittstelle)** und **Data Interface (Datenschnittstelle)** anwenden und dann die entsprechende Ausgangsschnittstelle für DNS-Abfragen angeben. Klicken Sie auf die **Test**-Schaltfläche, um die erfolgreiche Konfiguration und Erreichbarkeit über die Verwaltungsoberfläche der FTD zu überprüfen. Da diese Tests von der Verwaltungsschnittstelle der FTD und nicht über eine der im FTD konfigurierten routingfähigen Schnittstellen (z. B. innen, außen, dmz) initiiert werden, gewährleistet eine erfolgreiche (oder fehlgeschlagene) Verbindung nicht das gleiche Ergebnis für die AnyConnect-Authentifizierung, da AnyConnect LDAP-Authentifizierungsanforderungen von einer der routingfähigen Schnittstellen der FTD initiiert werden. Weitere Informationen zum Testen von LDAP-Verbindungen vom FTD finden Sie in den Abschnitten **Test AAA** und **Packet Capture** im Bereich **Troubleshooting (Fehlerbehebung)**.

# Add Identity Realm



! Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name

LAB-AD

Type

Active Directory (AD)

Directory Username

ftd.admin@example.com

e.g. user@example.com

Directory Password

••••••••

Base DN

DC=example,DC=com

e.g. ou=user, dc=example, dc=com

AD Primary Domain

example.com

e.g. example.com

## Directory Server Configuration

win2016.example.com:389

Hostname / IP Address

win2016.example.com

e.g. ad.example.com

Port

389

Encryption

NONE

Trusted CA certificate

Please select a certificate

TEST

✓ Connection to realm is successful

[Add another configuration](#)

CANCEL

OK

Wenn LDAPS oder STARTTLS verwendet wird, wählen Sie die entsprechende Verschlüsselung aus, und wählen Sie dann das Zertifikat der vertrauenswürdigen Zertifizierungsstelle aus. Wenn die Stammzertifizierungsstelle nicht bereits hinzugefügt wurde, klicken Sie auf **Neues Zertifikat für vertrauenswürdige CA erstellen**. Geben Sie einen Namen für das Stammzertifikat der Zertifizierungsstelle ein, und fügen Sie dann das zuvor erfasste Root-Zertifizierungsstellenzertifikat im PEM-Format ein.

## Add Trusted CA Certificate ? ✕

Name

LDAPS\_ROOT

Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExJleGFtcGxlLVdJTlJwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC
ASwDQYIKoZIhvcNAQEFBQADQgEPADCCAQCgCnFRAl8chT719NzSQncOPh0YT67h
```

CANCEL OK

### Directory Server Configuration

**win2016.example.com:636**

<p>Hostname / IP Address</p> <p>win2016.example.com</p> <p><i>e.g. ad.example.com</i></p>	<p>Port</p> <p>636</p>
<p>Encryption</p> <p>LDAPS</p>	<p>Trusted CA certificate</p> <p>LDAPS_ROOT</p>

TEST ✓ Connection to realm is successful

In dieser Konfiguration wurden folgende Werte verwendet:

- Name: LAB-AD
- Verzeichnisbenutzername: ftd.admin@example.com
- Basis-DN: DC=Beispiel, DC=com
- Primäre AD-Domäne: example.com
- Hostname/IP-Adresse: win2016.example.com
- Anschluss: 389

3. Klicken Sie oben rechts auf die Schaltfläche **Ausstehende Änderungen**, wie im Bild gezeigt.

The screenshot shows the Cisco Firepower Device Manager interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: FTD-3'. The 'Objects' tab is active. On the left, a sidebar shows 'Object Types' with categories like Networks, Ports, Security Zones, and Application Filters. The main content area is titled 'Identity Sources' and shows a table with 2 objects:

#	NAME	TYPE	VALUE	ACTIONS
1	LocalIdentitySource	LOCAL		
2	LAB-AD	AD	win2016.example.com	

At the top right of the main content area, there is a search bar and a red box highlights a button with a red exclamation mark icon, representing 'Outstanding Changes'.

4. Klicken Sie auf die Schaltfläche **Jetzt bereitstellen**.

**Pending Changes**

✓ **Last Deployment Completed Successfully**  
01 May 2020 12:54 PM. [See Deployment History](#)

Deployed Version (01 May 2020 12:54 PM) | Pending Version **LEGEND** Removed Added Edited

+ **Active Directory Realm Added: LAB-AD**

```
dirPassword.masked: false
dirPassword.encryptedString: ***
directoryConfigurations[0].port: 389
directoryConfigurations[0].hostname: win2016.example.com
directoryConfigurations[0].encryptionProtocol: NONE
adPrimaryDomain: example.com
dirUsername: ftd.admin@example.com
baseDN: DC=example,DC=com
enabled: true
realmId: 9
name: LAB-AD
```

MORE ACTIONS ▼ | CANCEL | **DEPLOY NOW** ▼

## Konfigurieren von AnyConnect für die AD-Authentifizierung

Um die konfigurierte AD-Identitätsquelle zu verwenden, muss sie auf die AnyConnect-Konfiguration angewendet werden.

1. Navigieren Sie zu **Device > Remote Access VPN** wie im Bild gezeigt.

CISCO Firepower Device Manager | Monitoring Policies Objects **Device: FTD-3** admin Administrator

Interfaces: Connected Enabled 3 of 4 | View All Interfaces >

Smart License: Registered | View Configuration >

Site-to-Site VPN: There are no connections yet | View Configuration >

**Remote Access VPN: Configured 1 connection | 2 Group Policies** | View Configuration >

Routing: 2 routes | View Configuration >

Backup and Restore: | View Configuration >

Updates: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds | View Configuration >

Troubleshoot: No files created yet | REQUEST FILE TO BE CREATED

Advanced Configuration: Includes: FlexConfig, Smart CLI | View Configuration >

System Settings: Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences

Device Administration: Audit Events, Deployment History, Download Configuration | View Configuration >

2. Klicken Sie auf das + Symbol oder die Schaltfläche **Verbindungsprofil erstellen**, wie im Bild gezeigt.

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

Search

	NAME	AAA	GROUP POLICY	ACTIONS
<p>There are no Remote Access Connections yet. Start by creating the first Connection.</p> <p><a href="#">CREATE CONNECTION PROFILE</a></p>				

3. Wählen Sie im Abschnitt "Connection and Client Configuration" (Verbindung und Client-Konfiguration) die zuvor erstellte AD-Identitätsquelle aus. Richten Sie die entsprechenden Werte für die anderen Abschnitte ein, einschließlich Verbindungsprofilname und Client-Adresspoolzuweisung. Klicken Sie abschließend auf **Abfrage senden**.

## Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

### Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

General

### Group Alias

General

[Add Group Alias](#)

### Group URL

[Add Group URL](#)

## Primary Identity Source

### Authentication Type

AAA Only

Client Certificate Only

AAA and Client Certificate

### Primary Identity Source for User Authentication

Filter

LocalIdentitySource

LAB-AD

Special-Identities-Realm

[Create new](#)

### Fallback Local Identity Source ⚠


Please Select Local Identity Source

## Client Address Pool Assignment

### IPv4 Address Pool

Endpoints are provided an address from this pool



 AnyConnect-Pool

### IPv6 Address Pool

Endpoints are provided an address from this pool



### DHCP Servers



CANCEL

SUBMIT QUERY

4. Wählen Sie im Abschnitt Remote User Experience (Remote-Benutzererfahrung) die entsprechende Gruppenrichtlinie aus. Standardmäßig wird **DfltGrpPolicy** verwendet. Es kann jedoch ein anderer erstellt werden.

DfltGrpPolicy

## Policy Group Brief Details

DNS + BANNER		Edit
DNS Server	None	
Banner Text for Authenticated Clients	None	
SESSION SETTINGS		
Maximum Connection Time / Alert Interval	Unlimited / 1 Minutes	
Idle Time / Alert Interval	30 / 1 Minutes	
Simultaneous Login per User	3	
SPLIT TUNNELING		
IPv4 Split Tunneling	Allow all traffic over tunnel	
IPv6 Split Tunneling	Allow all traffic over tunnel	
ANYCONNECT CLIENT		
AnyConnect Client Profiles	None	

BACK

SUBMIT QUERY

5. Geben Sie im Abschnitt Global Settings (Globale Einstellungen) mindestens das SSL-Zertifikat, die externe Schnittstelle und die AnyConnect-Pakete an. Wenn zuvor kein Zertifikat erstellt wurde, kann ein selbstsigniertes Standardzertifikat ([DefaultInternalCertificate](#)) ausgewählt werden, jedoch wird eine nicht vertrauenswürdige Serverzertifikatmeldung angezeigt. Zugriffskontrollrichtlinien für entschlüsselten Datenverkehr umgehen (sysopt permit-vpn) sollte deaktiviert werden, damit die Benutzeridentitätszugriffsrichtlinien zu einem späteren Zeitpunkt wirksam werden. NAT-Freistellung kann auch hier konfiguriert werden. In dieser Konfiguration ist der gesamte IPv4-Datenverkehr von der internen Schnittstelle, der zu den AnyConnect-Client-IP-Adressen führt, außer von NAT. Für komplexere Konfigurationen, wie z. B. externe Hairpinning, müssen im Rahmen der NAT-Richtlinie zusätzliche NAT-Regeln erstellt werden. AnyConnect-Pakete finden Sie auf der Cisco Support-Website unter <https://software.cisco.com/download/home>. Zum Herunterladen des AnyConnect-Pakets ist eine gültige Plus- oder Apex-Lizenz erforderlich.



# Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

## Certificate of Device Identity

FTD-3-Manual

## Outside Interface

outside (GigabitEthernet0/0)

## Fully-qualified Domain Name for the Outside Interface

ftd3.example.com

e.g. ravpn.example.com

## Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

## NAT Exempt



### Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

### Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



any-ipv4

## AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from [software.cisco.com](https://software.cisco.com).

You must have the necessary AnyConnect software license.

## Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.03052-webdeploy-k9.pkg

Linux: anyconnect-linux64-4.7.03052-webdeploy-k9.pkg

BACK

NEXT

6. Überprüfen Sie im Abschnitt Zusammenfassung, ob AnyConnect korrekt eingerichtet ist, und klicken Sie dann auf **Abfrage senden**.

## ^ Summary

Review the summary of the Remote Access VPN configuration.

### General

**STEP 1: CONNECTION AND CLIENT CONFIGURATION**

Primary Identity Source

**Authentication Type** AAA Only

**Primary Identity Source** LAB-AD

**Fallback Local Identity Source** -

**Strip Identity Source server from username** No

**Strip Group from Username** No

Secondary Identity Source

**Secondary Identity Source for User Authentication** -

**Fallback Local Identity Source** -

Advanced

**Authorization Server**

**Accounting Server**

Client Address Pool Assignment

IPv4 Address Pool

BACK SUBMIT QUERY

7. Klicken Sie oben rechts auf die Schaltfläche **Ausstehende Änderungen**, wie im Bild gezeigt.

Firepower Device Manager | Monitoring | Policies | Objects | Device: FTD-3 | admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

1 object

#	NAME	AAA	GROUP POLICY	ACTIONS
1	General	Authentication: AAA Only Authorization: None Accounting: None	DfltGrpPolicy	

8. Klicken Sie auf **Jetzt bereitstellen**.

## Pending Changes ? X

✔ Last Deployment Completed Successfully  
16 Apr 2020 12:41 PM, [See Deployment History](#)

Deployed Version (16 Apr 2020 12:41 PM)	Pending Version <span style="float: right;">LEGEND <span style="border: 1px solid red; padding: 2px;">Removed</span> <span style="border: 1px solid green; padding: 2px;">Added</span> <span style="border: 1px solid blue; padding: 2px;">Edited</span></span>
<b>+ Network Object Added: AnyConnect-Pool</b>	
-	subType: Network
-	value: 10.10.10.0/24
-	isSystemDefined: false
-	dnsResolution: IPV4_AND_IPV6
-	name: AnyConnect-Pool
<b>+ RA VPN Added: NGFW-Remote-Access-VPN</b>	
-	vpnGatewaySettings[0].exemptNatRule: true
-	vpnGatewaySettings[0].outsideFqdn: ftd3.example.com
-	vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t...
-	name: NGFW-Remote-Access-VPN
anyconnectPackageFiles:	
-	anyconnect-win-4.7.03052-webdeploy-k9.pkg
vpnGatewaySettings[0].serverCertificate:	
-	FTD-3-Manual
vpnGatewaySettings[0].outsideInterface:	
-	outside
vpnGatewaySettings[0].insideInterfaces:	
-	inside
vpnGatewaySettings[0].insideNetworks:	

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

### Identitätsrichtlinie aktivieren und Sicherheitsrichtlinien für Benutzeridentität konfigurieren

An diesem Punkt sollten AnyConnect-Benutzer erfolgreich eine Verbindung herstellen können, aber möglicherweise nicht auf bestimmte Ressourcen zugreifen können. In diesem Schritt wird die Benutzeridentität aktiviert, sodass nur Benutzer innerhalb von AnyConnect Admins mit RDP eine Verbindung zu internen Ressourcen herstellen können und nur Benutzer innerhalb der Gruppe AnyConnect-Benutzer mit HTTP eine Verbindung zu internen Ressourcen herstellen können.

1. Navigieren Sie zu **Richtlinien > Identität**, und klicken Sie auf **Identitätsrichtlinie aktivieren**.

Firepower Device Manager

Monitoring **Policies** Objects Device: FTD-3

Security Policies

SSL Decryption → **Identity** → Security Intelligence → NAT → Access Control → Intrusion

### Establishing User Identity

You can use identity policies to collect user identity information from connections. You can then view usage based on user identity in the dashboards, and configure access control based on user or user group. By linking network behavior, traffic, and events directly to individual users, the system can help you identify the source of policy breaches, attacks, or network vulnerabilities.

### How Identity policies work

Passive authentication Active authentication

ENABLE IDENTITY POLICY

Für diese Konfiguration ist keine weitere Konfiguration erforderlich, und die Standardaktion ist ausreichend.

Firepower Device Manager

Monitoring **Policies** Objects Device: FTD-3

Security Policies

SSL Decryption → **Identity** → Security Intelligence → NAT → Access Control → Intrusion

Identity Policy

Search

#	NAME	AUTHENTICATION	AUTH. TYPE	SOURCE			DESTINATION			ACTIONS
				ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO...	
<p>There are no Identity rules yet. Start by creating the first identity rule.</p> <p><a href="#">CREATE IDENTITY RULE</a></p>										

Default Action **Passive Auth** Any Identity Source

2. Navigieren Sie zu **Richtlinien > NAT**, und stellen Sie sicher, dass NAT korrekt konfiguriert ist. Wenn die in den AnyConnect-Einstellungen konfigurierte NAT-Ausnahme ausreicht, ist hier keine zusätzliche Konfiguration erforderlich.

1 rule

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
>	Internet_PAT	DYNAMIC	ANY outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

3. Navigieren Sie zu **Richtlinien > Zugriffskontrolle**. In diesem Abschnitt ist die Standardaktion auf "Blockieren" gesetzt. Es wurden keine Zugriffsregeln erstellt, sodass ein AnyConnect-Benutzer nach der Verbindung auf nichts zugreifen kann. Klicken Sie auf das + Symbol oder auf Zugriffsregel erstellen, um eine neue Regel hinzuzufügen.

There are no access rules yet.  
Start by creating the first access rule.

CREATE ACCESS RULE

Default Action: Access Control - Block

4. Füllen Sie die Felder mit den entsprechenden Werten aus. Bei dieser Konfiguration sollten Benutzer innerhalb der AnyConnect-Administratorgruppe über RDP-Zugriff auf den Windows-Server im internen Netzwerk verfügen. Für die Quelle wird die Zone als `outside_zone` konfiguriert. Dies ist die externe Schnittstelle, mit der die AnyConnect-Benutzer eine Verbindung herstellen, und das Netzwerk wird als AnyConnect-Pool-Objekt konfiguriert, das zuvor konfiguriert wurde, um AnyConnect-Clients IP-Adressen zuzuweisen. Für die Benutzeridentität im FDM muss die Quelle die Zone sein, von der der Benutzer die Verbindung initiiert. Für das Ziel wird die Zone als `inside_zone` konfiguriert, d. h. als interne Schnittstelle, die sich der Windows Server befindet, das Netzwerk wird als `Inside_Net`-Objekt konfiguriert. Dies ist ein Objekt, das das Subnetz definiert, in dem sich der Windows Server befindet, und Ports/Protokolle werden auf zwei benutzerdefinierte Port-Objekte festgelegt, um den RDP-Zugriff über TCP 3389 und UDP 3389 zu ermöglichen.

## Edit Access Rule

Order: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP

Show Diagram  | Not hit yet | CANCEL | OK

Im Abschnitt "Benutzer" wird die Gruppe "AnyConnect-Administratoren" hinzugefügt, sodass Benutzer außerhalb dieser Gruppe RDP-Zugriff auf den Windows-Server erhalten. Klicken Sie auf das + Symbol, klicken Sie auf die Registerkarte Gruppen, klicken Sie auf die entsprechende Gruppe und dann auf **OK**. Beachten Sie, dass auch einzelne Benutzer und die Identitätsquelle ausgewählt werden können.

**Add Access Rule**

Order: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

**AVAILABLE USERS**

Filter: [ ]

Identity Sources: **Groups** | Users

- LAB-AD \ Account Operators
- LAB-AD \ Administrators
- LAB-AD \ Allowed RODC Password Replication Group
- LAB-AD \ AnyConnect Admins**
- LAB-AD \ AnyConnect Users

Create new Identity Realm | CANCEL | **OK**

**CONTROLLING ACCESS FOR USERS AND USER GROUPS**

If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.

Show Diagram:  | CANCEL | **OK**

Klicken Sie nach Auswahl der entsprechenden Optionen auf **OK**.

**Add Access Rule**

Order: 1 | Title: AC RDP Access | Action: Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

**AVAILABLE USERS**

- LAB-AD \ AnyConnect Admins**

**CONTROLLING ACCESS FOR USERS AND USER GROUPS**

If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.

Show Diagram:  | CANCEL | **OK**

5. Erstellen Sie bei Bedarf weitere Zugriffsregeln. In dieser Konfiguration wird eine weitere

Zugriffsregel erstellt, um Benutzern innerhalb der AnyConnect-Benutzergruppe HTTP-Zugriff auf den Windows-Server zu ermöglichen.

**Edit Access Rule**

Order	Title	Action
2	AC HTTP Access	Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

**SOURCE**

Zones	Networks	Ports
outside_zone	AnyConnect-Pool	ANY

**DESTINATION**

Zones	Networks	Ports/Protocols
inside_zone	Inside_Net	HTTP

Show Diagram  Not hit yet CANCEL OK

**Edit Access Rule**

Order	Title	Action
2	AC HTTP Access	Allow

Source/Destination | Applications | URLs | **Users** | Intrusion Policy | File policy | Logging

**AVAILABLE USERS**

LAB-AD \ AnyConnect Users
---------------------------

**CONTROLLING ACCESS FOR USERS AND USER GROUPS**

If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.

Show Diagram  Not hit yet CANCEL OK

6. Überprüfen Sie die Konfiguration der Zugriffsregel, und klicken Sie dann oben rechts auf die



Schaltfläche **Ausstehende Änderungen**, wie im Bild gezeigt.

Firepower Device Manager | Monitoring | Policies | Objects | Device: FTD-3 | admin Administrator

Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion

2 rules

#	NAME	ACTION	SOURCE			DESTINATION					ACTIONS	
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO...	APPLICATIONS	URLS		USERS
1	AC RDP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP	ANY	ANY	AnyConne...	
2	AC HTTP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne...	

Default Action: Access Control - Block

7. Überprüfen Sie die Änderungen, und klicken Sie dann auf **Jetzt bereitstellen**.

Pending Changes

✓ Last Deployment Completed Successfully  
28 Apr 2020 01:35 PM. [See Deployment History](#)

Deployed Version (28 Apr 2020 01:35 PM) | Pending Version | LEGEND | Removed | Added | Edited

+ Access Rule Added: AC HTTP Access

- users[0].name: AnyConnect Users
- logFiles: false
- eventLogAction: LOG\_NONE
- ruleId: 268435467
- name: AC HTTP Access

sourceZones: outside\_zone

destinationZones: inside\_zone

sourceNetworks: AnyConnect-Pool

destinationNetworks: Inside\_Net

destinationPorts: HTTP

users[0].identitySource: LAB-AD

+ Access Rule Added: AC RDP Access

MORE ACTIONS ▼ | CANCEL | DEPLOY NOW ▼

## Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

## Endgültige Konfiguration

## AAA-Konfiguration

```
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
```

## Konfigurieren von AnyConnect

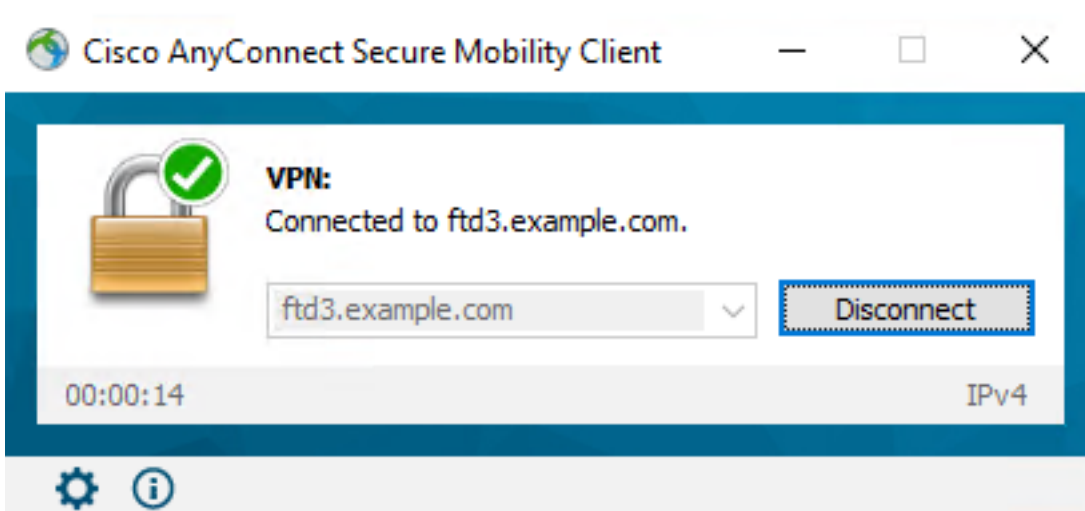
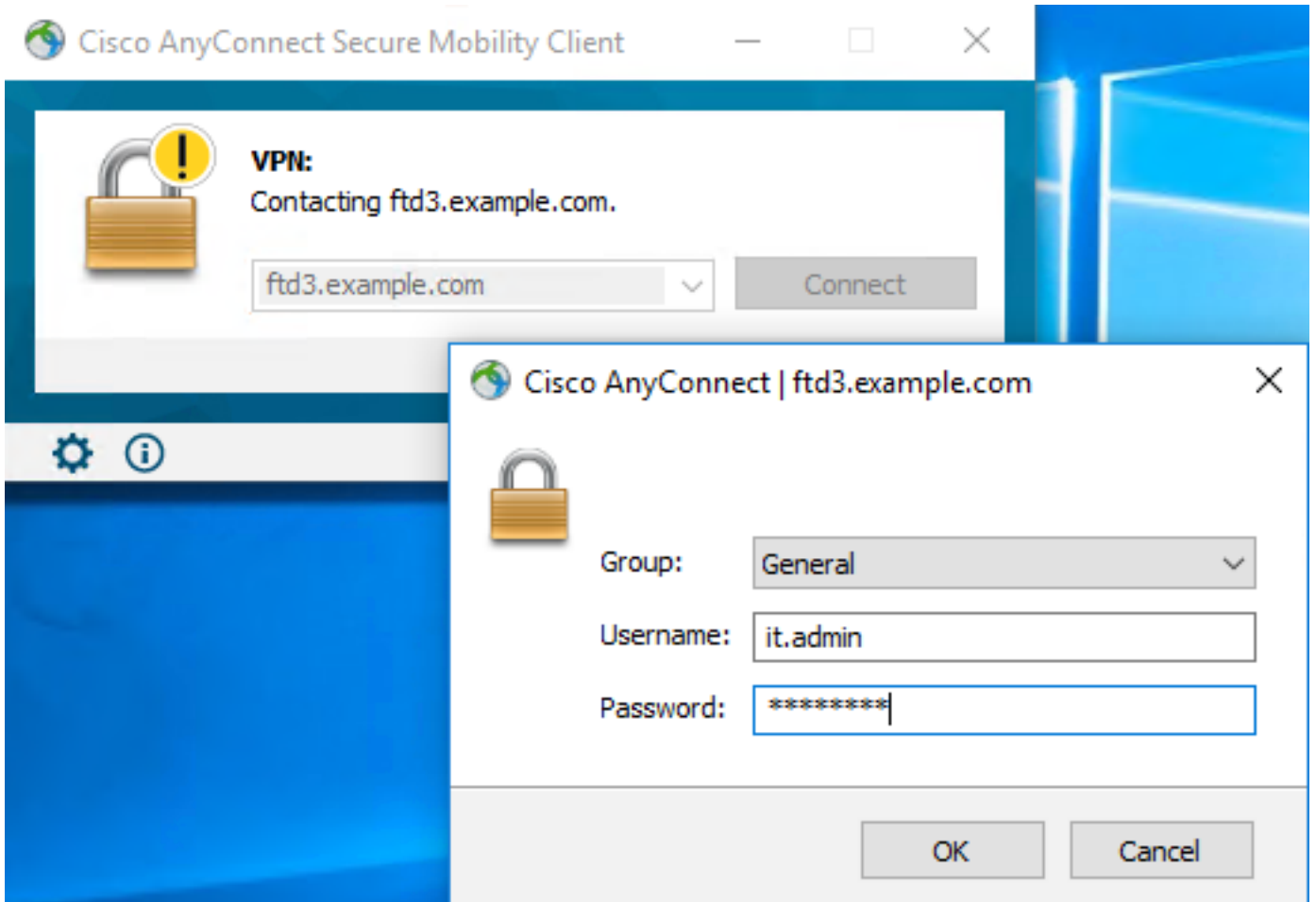
```
> show running-config webvpn
webvpn
  enable outside
  http-headers
    hsts-server
      enable
      max-age 31536000
      include-sub-domains
      no preload
    hsts-client
      enable
  x-content-type-options
  x-xss-protection
  content-security-policy
anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg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

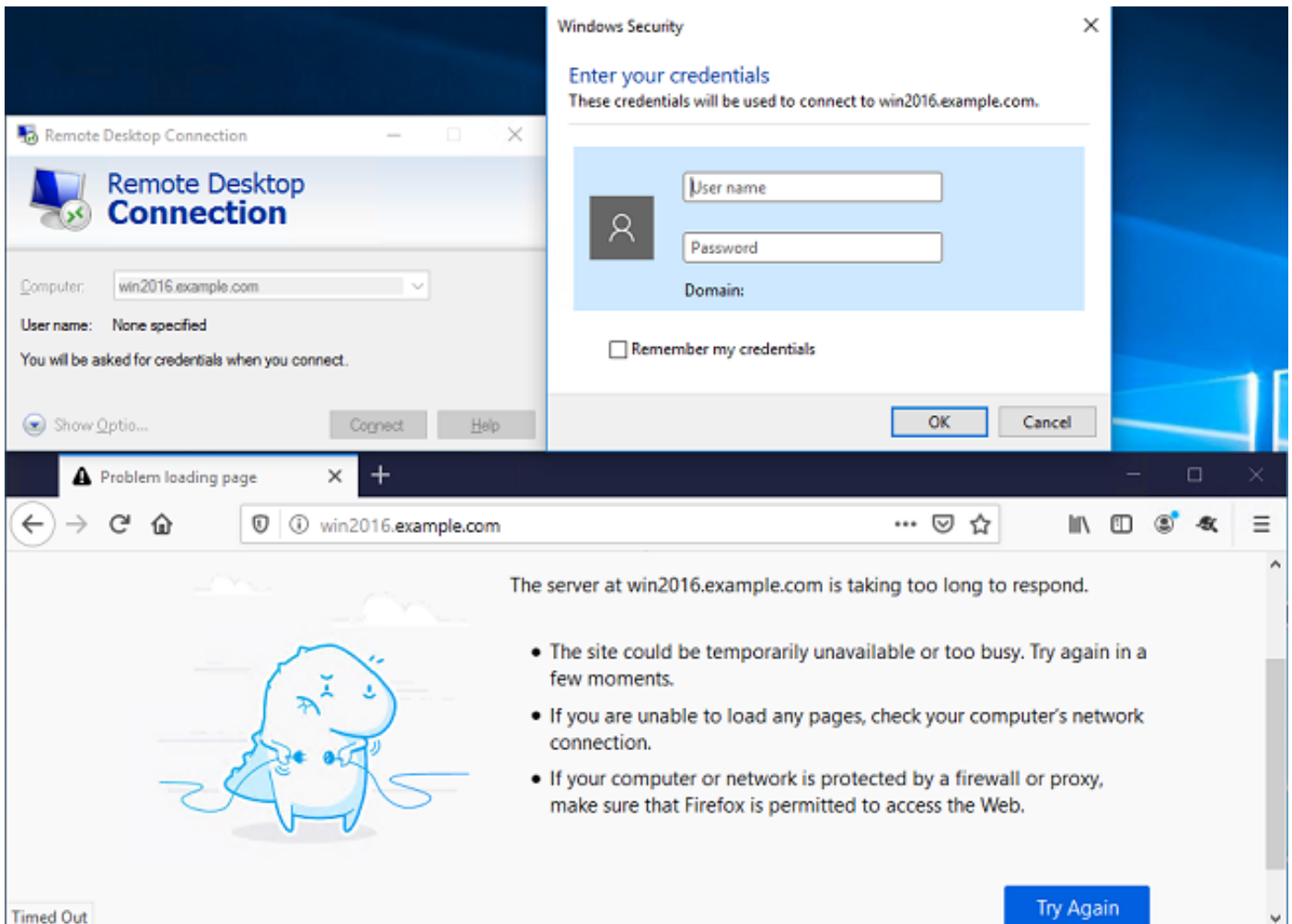
```
> show running-config group-policy
group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
  anyconnect ssl dtls none
```

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

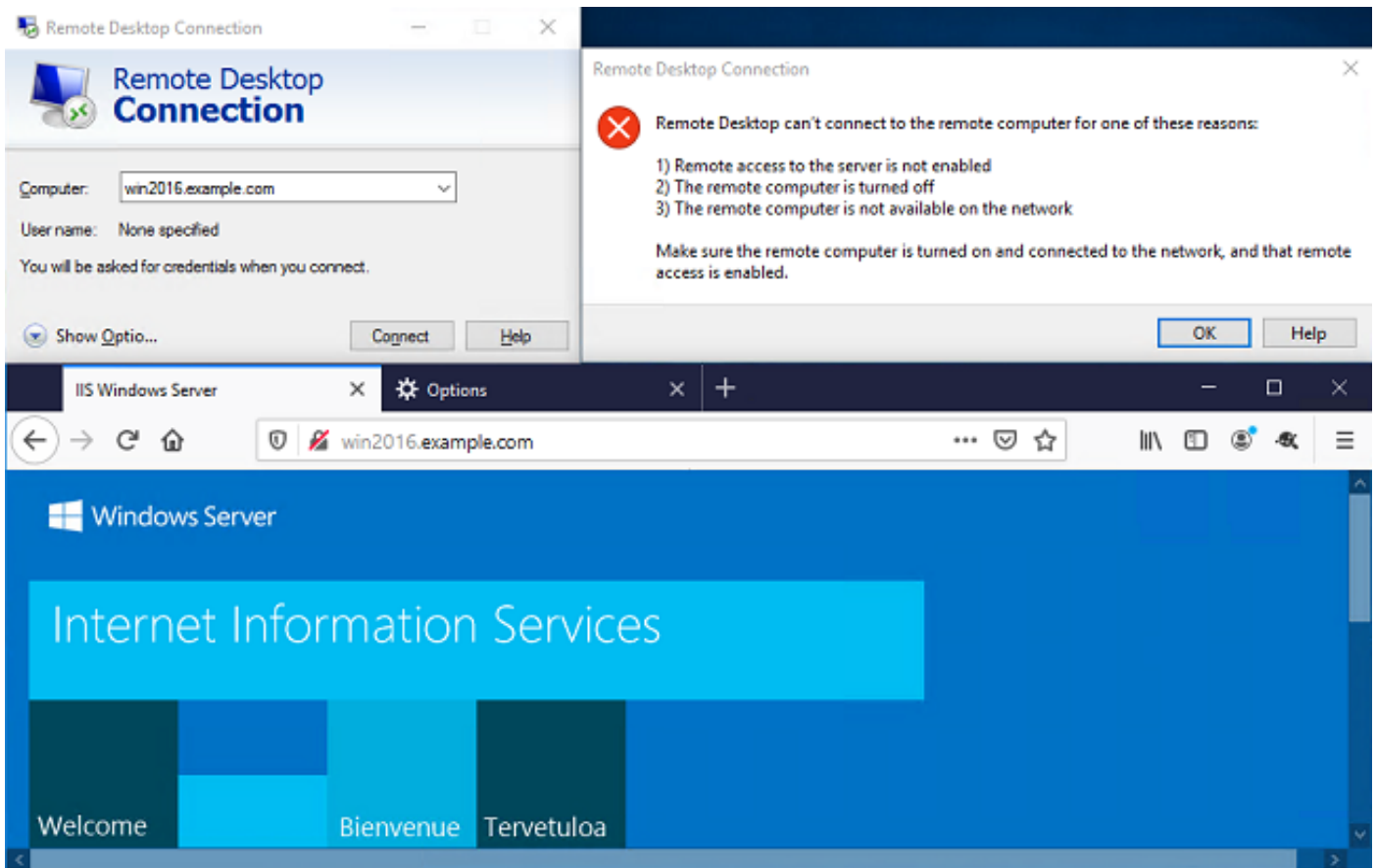
## Herstellen einer Verbindung mit AnyConnect und Überprüfen der Zugriffskontrollrichtlinien



Benutzer-IT-Admin ist in der Gruppe AnyConnect-Administratoren, die über RDP-Zugriff auf den Windows-Server verfügt, jedoch keinen Zugriff auf HTTP hat. Durch das Öffnen einer RDP- und Firefox-Sitzung mit diesem Server wird überprüft, ob dieser Benutzer nur über RDP auf den Server zugreifen kann.



Wenn Sie bei einem Testbenutzer angemeldet sind, der zur Gruppe AnyConnect-Benutzer gehört, die über HTTP-Zugriff, aber keinen RDP-Zugriff verfügen, können Sie überprüfen, ob die Zugriffskontrollrichtlinien wirksam werden.



## Fehlerbehebung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

## Debugger

Dieser Debugger kann in der CLI der Diagnose ausgeführt werden, um Probleme mit der LDAP-Authentifizierung zu beheben: **debug ldap 255**.

Um Probleme mit der Zugriffskontrollrichtlinie für die Benutzeridentität zu beheben, kann die **Firewall-Engine-Debugging-Funktion des Systems** in clish ausgeführt werden, um zu ermitteln, warum Datenverkehr unerwartet zugelassen oder blockiert wird.

## Arbeiten mit LDAP-Debuggern

```
[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...;.....}...
[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

```

## Verbindung mit LDAP-Server kann nicht hergestellt werden

```

[-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

```

## Potenzielle Lösungen:

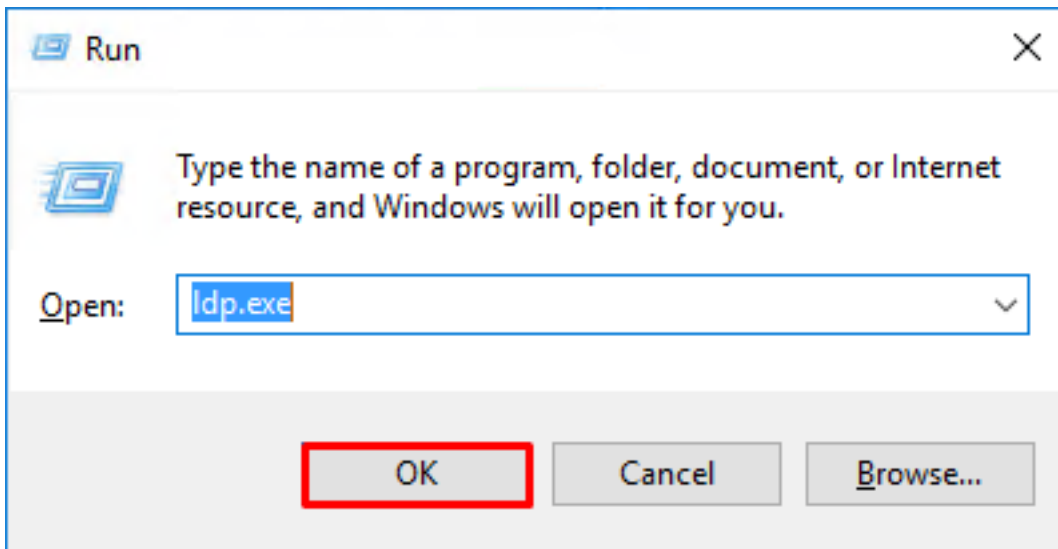
- Überprüfen Sie das Routing, und stellen Sie sicher, dass die FTD eine Antwort vom LDAP-Server erhält.
- Wenn LDAPS oder STARTTLS verwendet wird, stellen Sie sicher, dass das richtige Root-Zertifizierungsstellenzertifikat vertrauenswürdig ist, damit der SSL-Handshake erfolgreich abgeschlossen werden kann.
- Überprüfen Sie, ob die richtige IP-Adresse und der richtige Port verwendet werden. Wenn ein Hostname verwendet wird, überprüfen Sie, ob der DNS in der Lage ist, diesen auf die richtige IP-Adresse aufzulösen.

## Binden der Anmelde-DN und/oder des Kennworts falsch

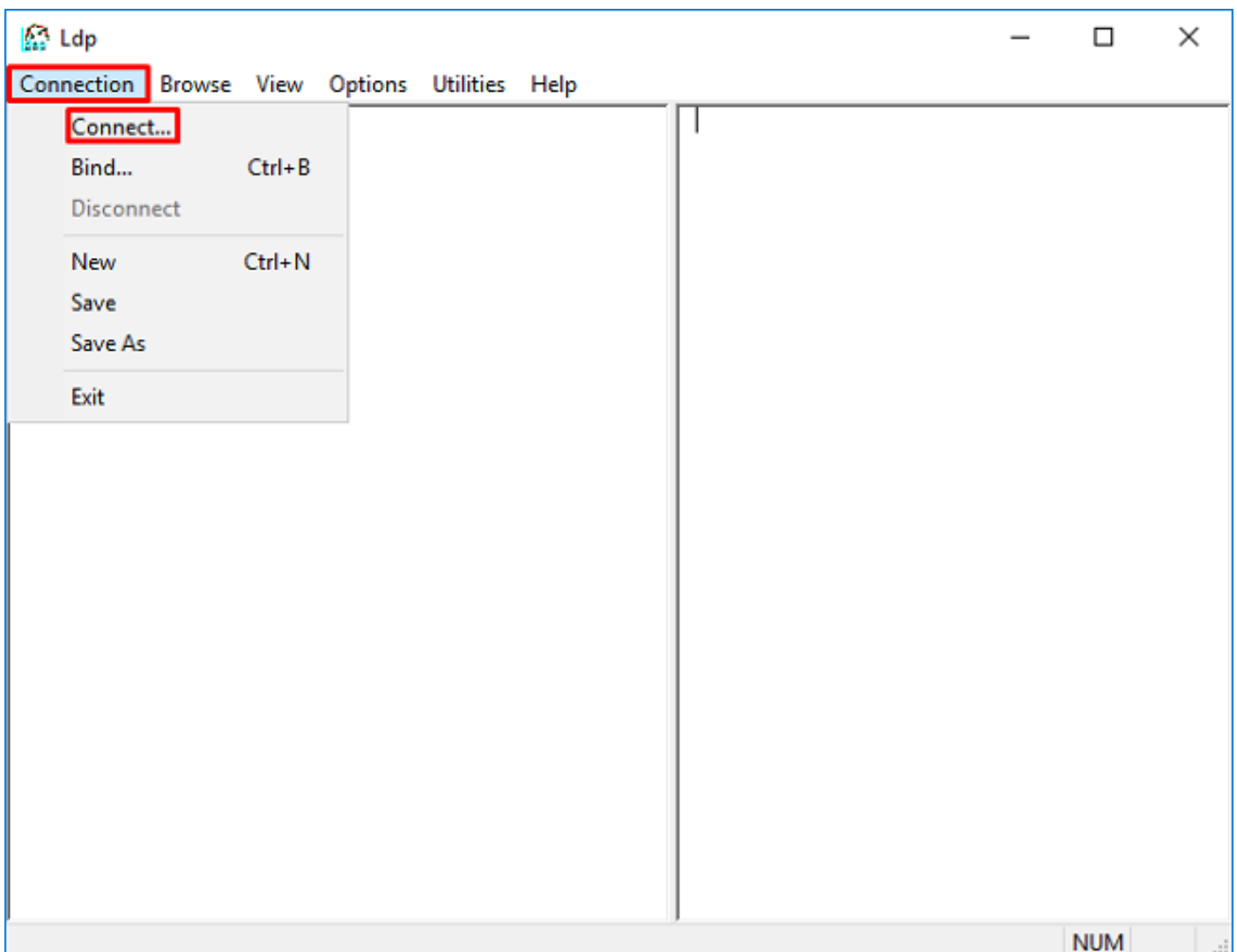
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615]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

Mögliche Lösung: Überprüfen Sie, ob die Anmelde-DN und das Anmeldekennwort entsprechend konfiguriert sind. Dies kann auf dem AD-Server mit **ldp.exe** überprüft werden. Um zu überprüfen, ob ein Konto erfolgreich mit der Verwendung von **ldp** verknüpft werden kann, gehen Sie durch die folgenden Schritte:

1. Drücken Sie auf dem AD-Server **Win+R** und suchen Sie nach **ldp.exe**.

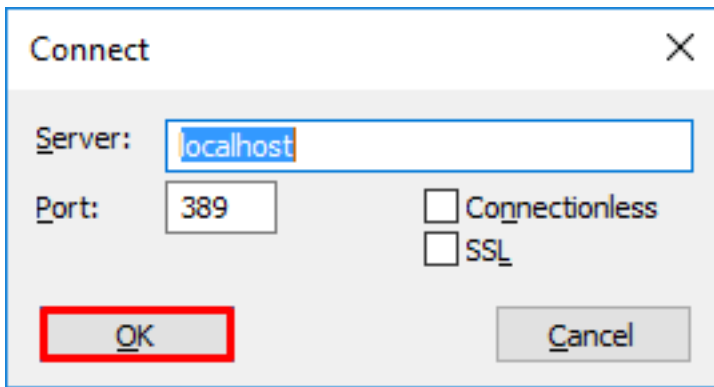


2. Klicken Sie auf **Verbindung > Verbindung herstellen...** wie im Bild gezeigt.

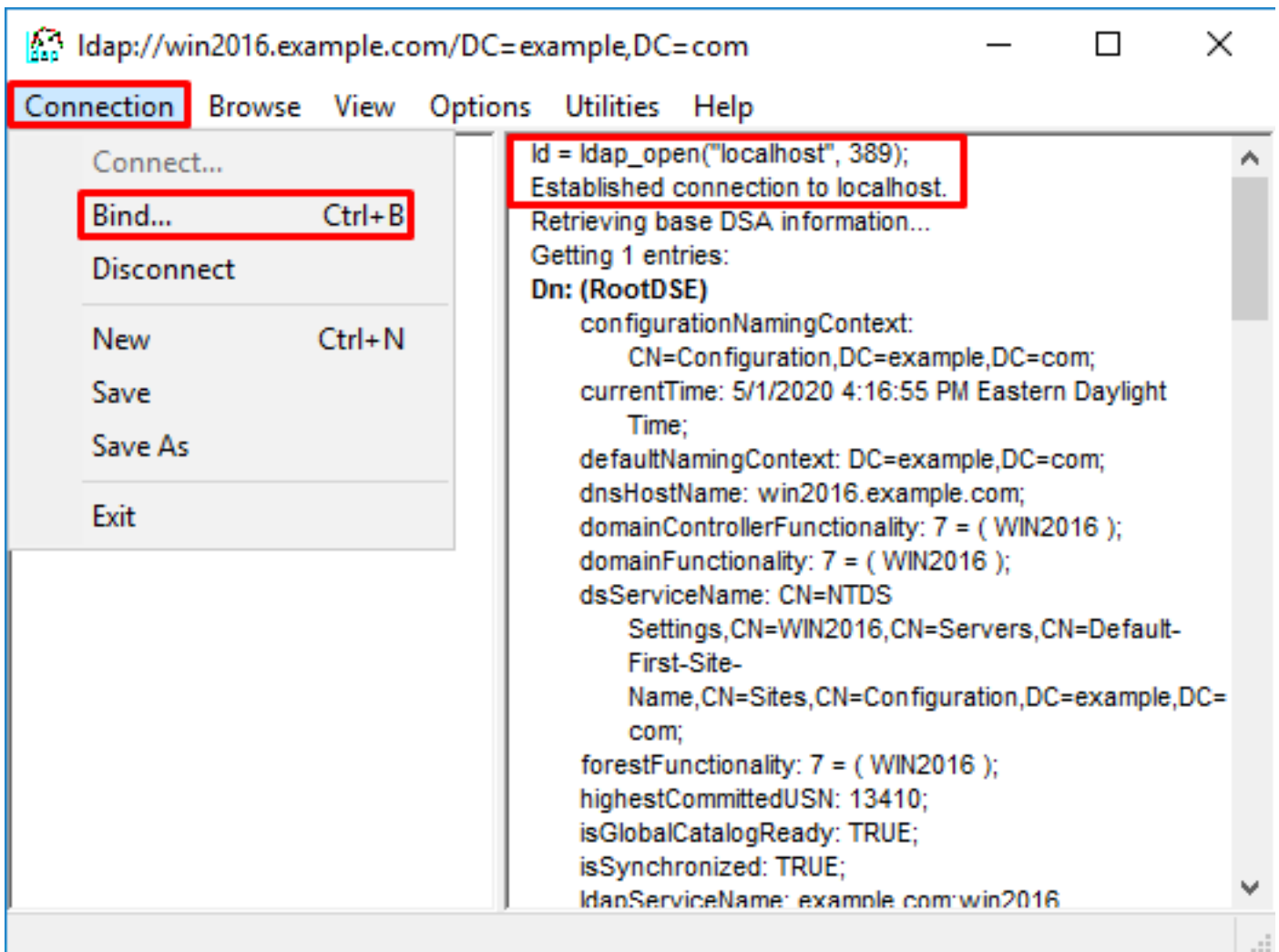


3. Geben Sie localhost für den Server und den entsprechenden Port an, und klicken Sie dann auf **OK**.





4. Die rechte Spalte zeigt den Text an, der auf eine erfolgreiche Verbindung hinweist. Klicken Sie auf **Verbindung > Bind..** wie im Bild gezeigt.



5. Wählen Sie **Einfache Bindung**, und geben Sie dann Benutzername und Kennwort des Verzeichniskontos an. Klicken Sie auf **OK**.

Bind

User: ftd.admin@example.com

Password: ●●●●●●●●

Domain:

Bind type

Bind as currently logged on user

Bind with credentials

Simple bind

Advanced (DIGEST)

Encrypt traffic after bind

Advanced Cancel OK

Bei erfolgreicher Bindung wird ldap als **DOMÄNEBenutzername** authentifiziert angezeigt.

Idap://win2016.example.com/DC=example,DC=com

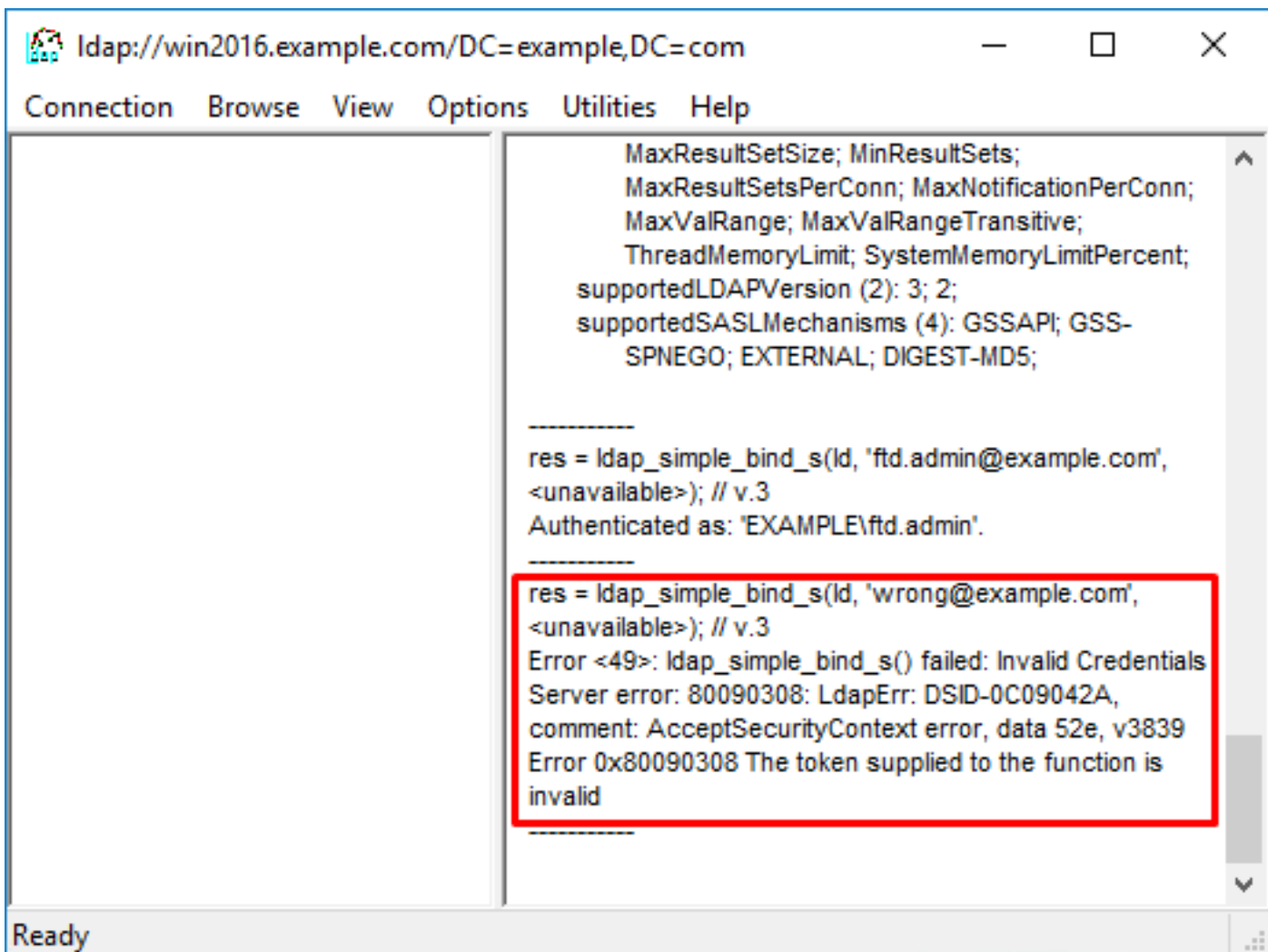
Connection Browse View Options Utilities Help

1.2.840.113556.1.4.2255;  
1.2.840.113556.1.4.2256;  
1.2.840.113556.1.4.2309;  
supportedLDAPPolicies (20): MaxPoolThreads;  
MaxPercentDirSyncRequests; MaxDatagramRecv;  
MaxReceiveBuffer; InitRecvTimeout;  
MaxConnections; MaxConnIdleTime; MaxPageSize;  
MaxBatchReturnMessages; MaxQueryDuration;  
MaxDirSyncDuration; MaxTempTableSize;  
MaxResultSetSize; MinResultSets;  
MaxResultSetsPerConn; MaxNotificationPerConn;  
MaxValRange; MaxValRangeTransitive;  
ThreadMemoryLimit; SystemMemoryLimitPercent;  
supportedLDAPVersion (2): 3; 2;  
supportedSASLMechanisms (4): GSSAPI; GSS-  
SPNEGO; EXTERNAL; DIGEST-MD5;

-----  
res = ldap\_simple\_bind\_s(ld, 'ftd.admin@example.com',  
<unavailable>); // v.3  
Authenticated as: 'EXAMPLE\ftd.admin'.  
-----

Ready

Wenn Sie versuchen, eine Bindung mit einem ungültigen Benutzernamen oder Kennwort zu erstellen, führt dies zu einem solchen Fehler.

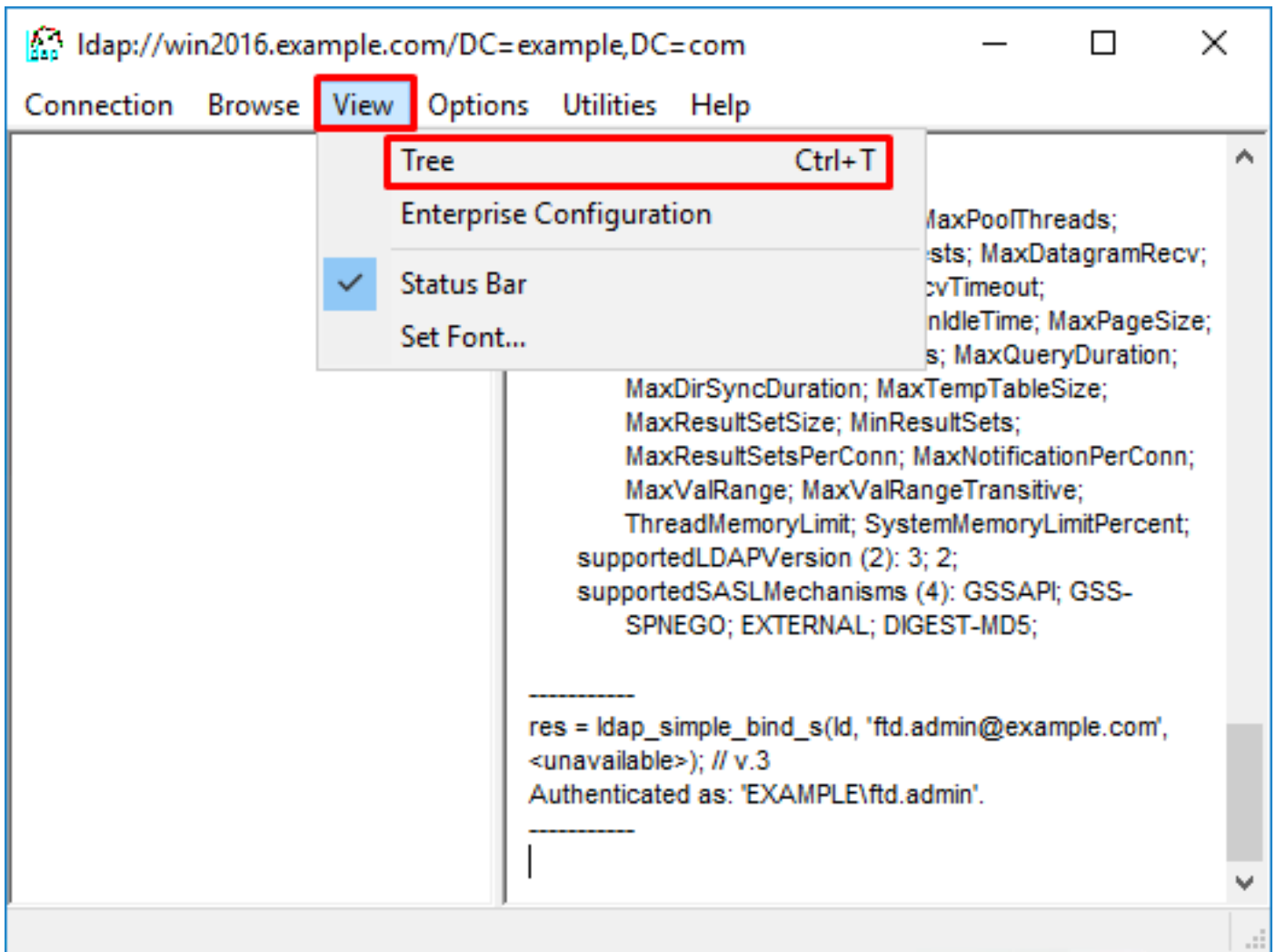


## LDAP-Server kann Benutzernamen nicht finden

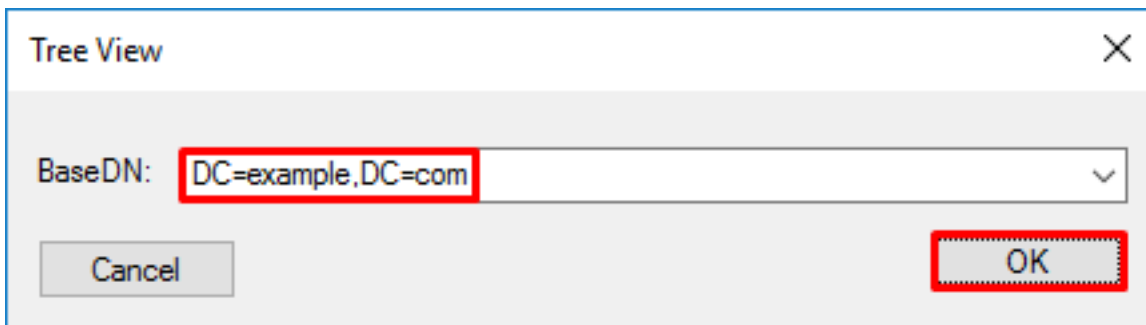
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612]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

Mögliche Lösung: Vergewissern Sie sich, dass AD den Benutzer mit der Suche durch die FTD finden kann. Dies kann auch mit ldp.exe durchgeführt werden.

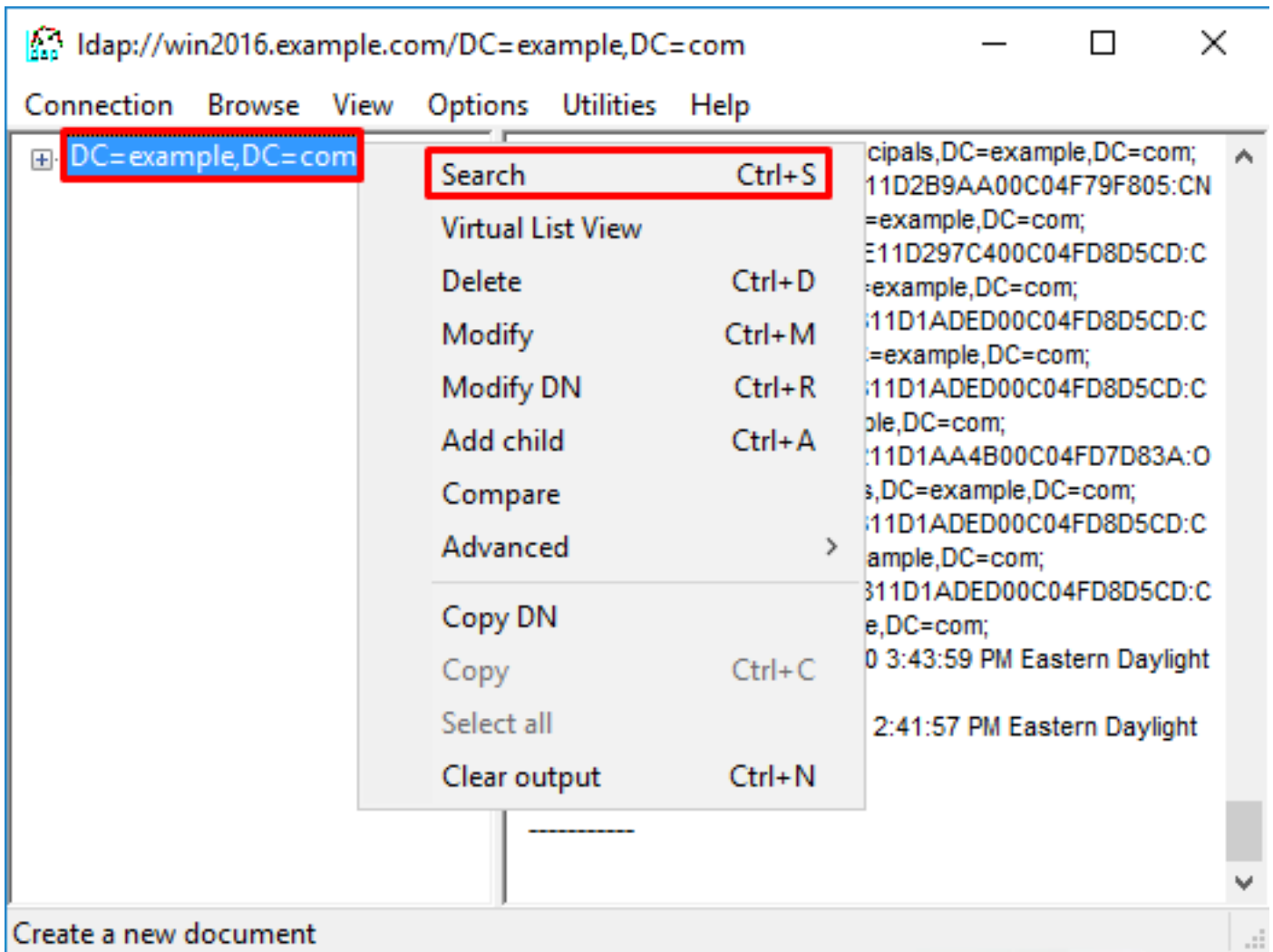
1. Navigieren Sie nach der erfolgreichen Bindung zu **Ansicht > Struktur** wie im Bild gezeigt.



2. Geben Sie die für FTD konfigurierte Basis-DN an, und klicken Sie dann auf **OK**.

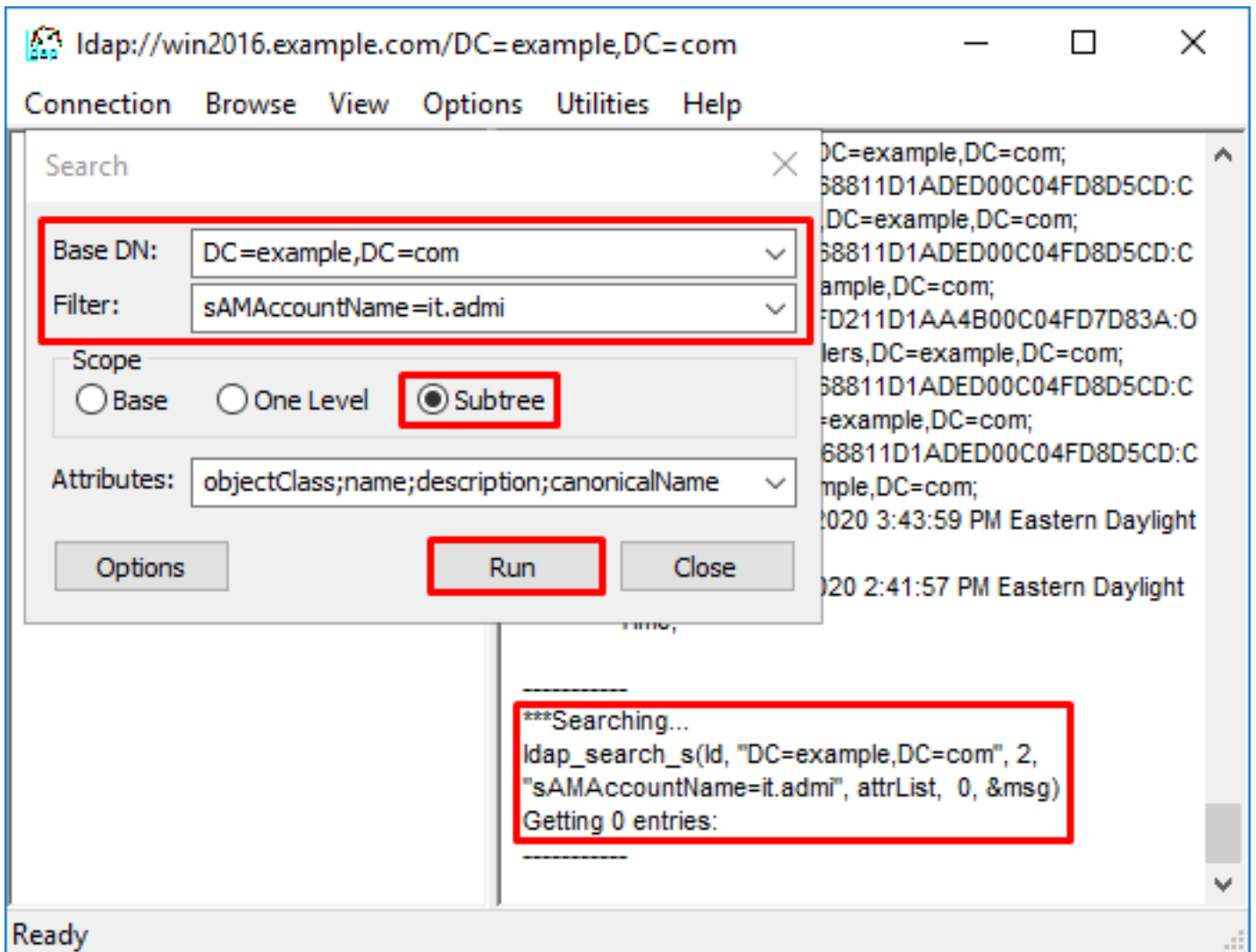


3. Klicken Sie mit der rechten Maustaste auf die Basis-DN, und klicken Sie dann auf Suchen, wie im Bild gezeigt.



4. Geben Sie die Werte für Basisdatenbank, Filter und Bereich an, die im Debuggen angezeigt werden. In diesem Beispiel sind folgende Beispiele:

- Basis-DN: `dc=beispiel,dc=com`
- Filtern: `samaccountName=it.admi`
- Geltungsbereich: `SUBTREE`



Idp findet 0 Einträge, da kein Benutzerkonto mit dem **gleichenAccountName=it.admi** unter Basis-DN dc=beispiel,dc=com vorhanden ist.

Bei einem erneuten Versuch mit dem richtigen **samaccountName=it.admin** wird ein anderes Ergebnis angezeigt. Idp sucht 1 Eintrag unter der Basis-DN dc=beispiel,dc=com und gibt die DN des Benutzers aus.

Search

Base DN: DC=example,DC=com

Filter: sAMAccountName=it.admin

Scope

Base  One Level  Subtree

Attributes: objectClass;name;description;canonicalName

Options Run Close

68811D1AED00C04FD8D5CD:C  
DC=example,DC=com;  
68811D1AED00C04FD8D5CD:C  
example,DC=com;  
FD211D1AA4B00C04FD7D83A:O  
lers,DC=example,DC=com;  
68811D1AED00C04FD8D5CD:C  
=example,DC=com;  
68811D1AED00C04FD8D5CD:C  
mple,DC=com;  
020 3:43:59 PM Eastern Daylight  
020 2:41:57 PM Eastern Daylight

-----  
\*\*\*Searching...  
ldap\_search\_s(ld, "DC=example,DC=com", 2,  
"sAMAccountName=it.admin", attrList, 0, &msg)  
Getting 1 entries:  
**Dn: CN=IT Admin,CN=Users,DC=example,DC=com**  
canonicalName: example.com/Users/IT Admin;  
name: IT Admin;  
objectClass (4): top; person; organizationalPerson;  
user;  
-----

Ready

## Falsches Kennwort für Benutzername

```
[ -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
```

Mögliche Lösung: Überprüfen Sie, ob das Kennwort des Benutzers korrekt konfiguriert wurde und nicht abgelaufen ist. Ähnlich wie bei der Anmelde-DN ist auch die FTD an AD mit den Anmeldeinformationen des Benutzers gebunden. Diese Bindung kann auch in ldp erfolgen, um zu überprüfen, ob das AD denselben Benutzernamen und dieselben Anmeldeinformationen für das Kennwort erkennen kann. Die Schritte in ldp sind im Abschnitt **Anmelde-DN und/oder Kennwort falsch** anzeigen. Darüber hinaus können die Microsoft Server Event Viewer-Protokolle aus einem potenziellen Grund überprüft werden.

## AAA testen

Der Befehl `test aaa-server` kann verwendet werden, um einen Authentifizierungsversuch der FTD mit einem bestimmten Benutzernamen und Kennwort zu simulieren. Dies kann zum Testen auf Verbindungs- oder Authentifizierungsfehler verwendet werden. Der Befehl lautet **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
```

## Paketerfassung

Paketerfassungen können verwendet werden, um die Erreichbarkeit zum AD-Server zu überprüfen. Wenn LDAP-Pakete die FTD verlassen, aber keine Antwort gibt, könnte dies auf ein Routing-Problem hinweisen.

Im Folgenden wird ein bidirektionaler LDAP-Datenverkehr aufgezeichnet:

```
> 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

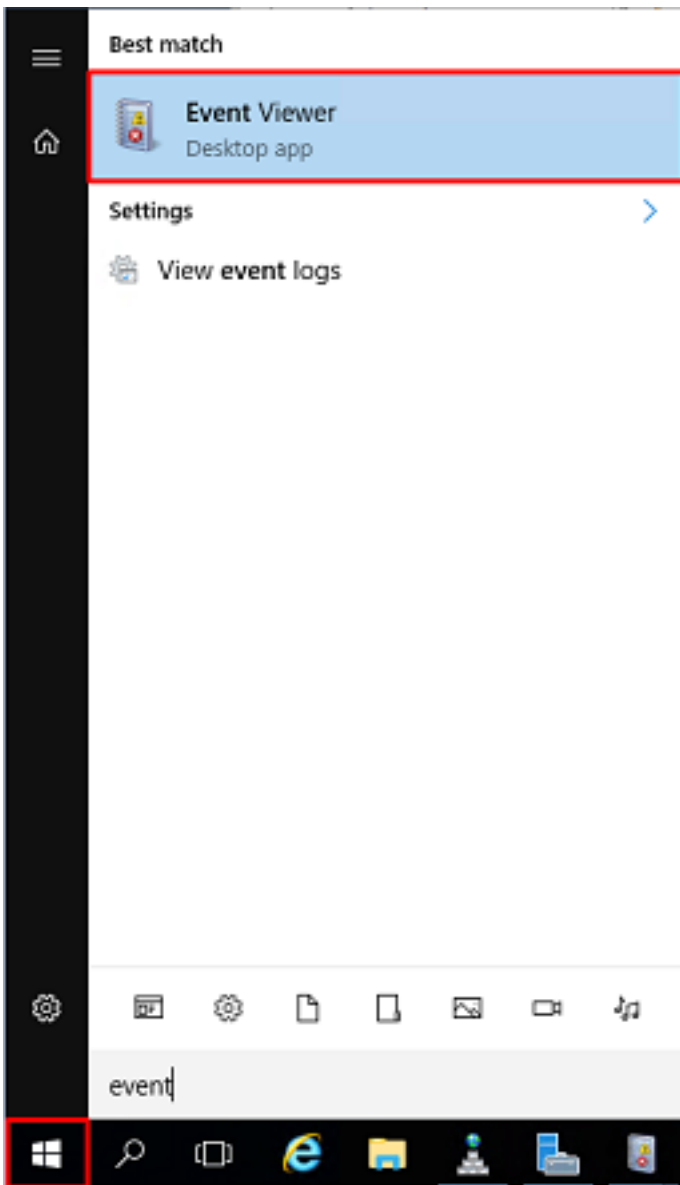
54 packets captured

  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
```

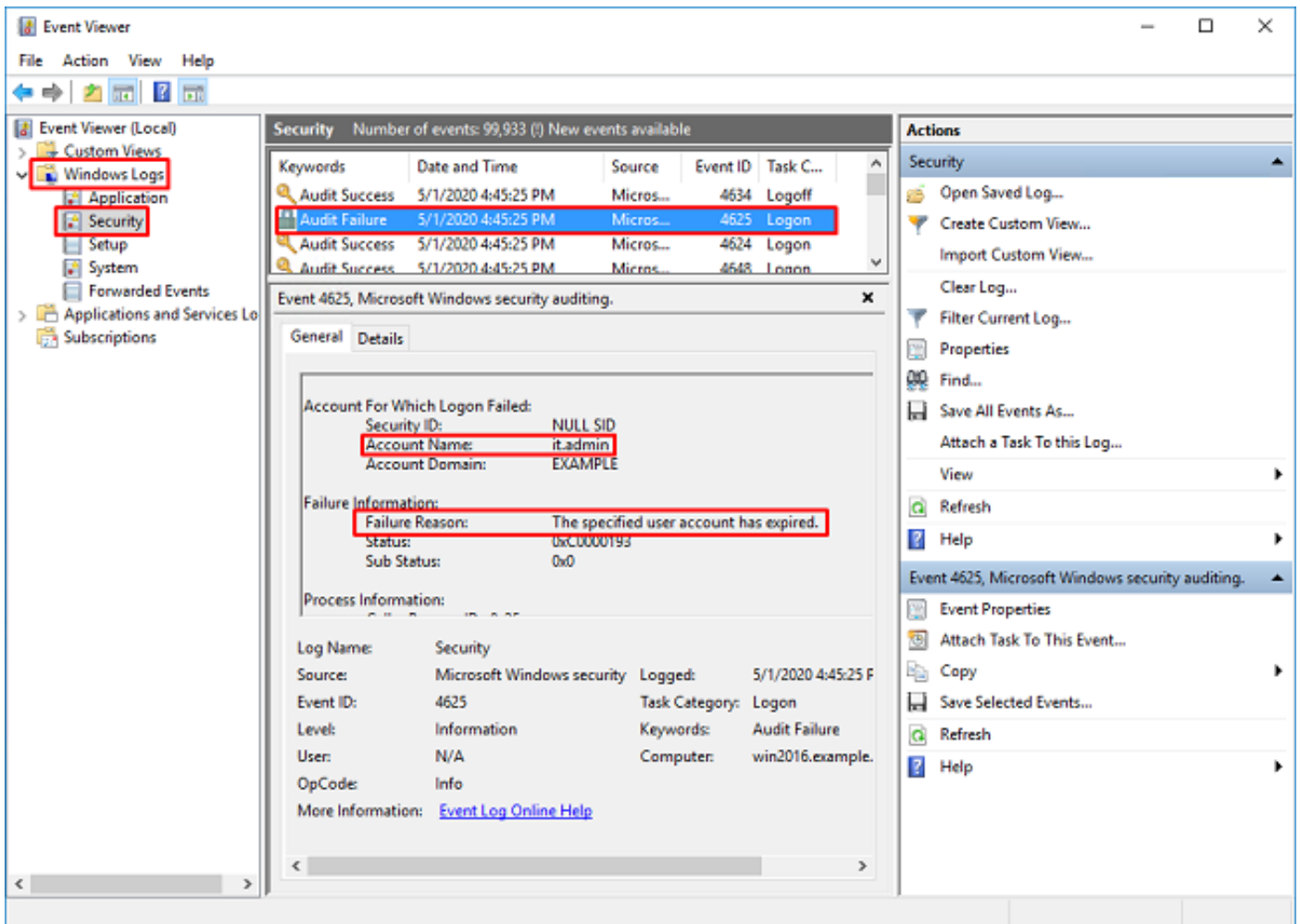
## Windows Server Event Viewer-Protokolle

Die Ereignisanzeige meldet sich im AD-Servervan an und liefert detailliertere Informationen, warum ein Fehler aufgetreten ist.

1. **Ereignisanzeige** suchen und öffnen.



2. Erweitern Sie **Windows-Protokolle**, und klicken Sie auf **Sicherheit**. Suchen Sie mit dem Kontonamen des Benutzers nach **Audit Failure (Audit-Fehler)**, und überprüfen Sie die Fehlerinformationen, wie im Bild gezeigt.



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