

Konfigurieren der AD-Authentifizierung (LDAP) und Benutzeridentität auf von FMC verwalteten FTD für AnyConnect-Clients

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm und -szenario](#)

[Active Directory-Konfigurationen](#)

[Ermitteln der LDAP-Basis-DN und Gruppen-DN](#)

[FTD-Konto erstellen](#)

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

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

[FMC-Konfigurationen](#)

[Lizenzierung überprüfen](#)

[Setup-Bereich](#)

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

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

[NAT-Ausnahme konfigurieren](#)

[Bereitstellen](#)

[Überprüfung](#)

[Abschließende Konfiguration](#)

[AAA-Konfiguration](#)

[AnyConnect-Konfiguration](#)

[AnyConnect verwenden und Richtlinien für die Zugriffskontrolle überprüfen](#)

[Mit FMC-Verbindungsereignissen überprüfen](#)

[Fehlerbehebung](#)

[Fehlerbehebung](#)

[LDAP-Debugger](#)

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

[Ungültiger Bindungs-Anmelde-DN und/oder falsches Kennwort](#)

[LDAP-Server konnte den Benutzernamen nicht finden](#)

[Falsches Kennwort für den Benutzernamen](#)

[AAA testen](#)

[Paketerfassung](#)

[Windows Server-Ereignisanzeige - Protokolle](#)

Einleitung

In diesem Dokument wird beschrieben, wie die AD-Authentifizierung für AnyConnect-Clients konfiguriert wird, die eine Verbindung mit Cisco Firepower Threat Defense (FTD) herstellen.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse der RA VPN-Konfiguration auf FMC
- Grundkenntnisse der LDAP-Serverkonfiguration auf FMC
- Grundkenntnisse von **Active Directory (AD)**

Verwendete Komponenten

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

- Microsoft Server 2016
- FMCv mit 6.5.0
- FTDv mit 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 möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

In diesem Dokument wird beschrieben, wie Sie die **Active Directory (AD)**-Authentifizierung für **AnyConnect-Clients** konfigurieren, die eine Verbindung zu **Cisco FirePOWER Threat Defense (FTD)** herstellen, das vom FirePOWER Management Center (**FMC**) verwaltet wird.

Die Benutzeridentität wird in den Zugriffsrichtlinien verwendet, um AnyConnect-Benutzer auf bestimmte IP-Adressen und Ports zu beschränken.

Konfigurieren

Netzwerkdiagramm und -szenario



Der Windows-Server ist mit IIS und RDP vorkonfiguriert, um die Benutzeridentität zu testen. In diesem Konfigurationsleitfaden werden drei Benutzerkonten und zwei Gruppen erstellt.

Benutzerkonten:

- **FTD-Administrator:** Dieser Parameter wird als Verzeichniskonto verwendet, damit die FTD an den Active Directory-Server gebunden werden kann.
- **IT-Administrator:** Ein Test-Administratorkonto, mit dem die Benutzeridentität veranschaulicht wird.
- **Test User (Testbenutzer):** Ein Testbenutzerkonto, mit dem die Benutzeridentität demonstriert wird.

Gruppen:

- **AnyConnect Admins:** Eine hinzugefügte Testgruppe für IT-Administratoren, die die Benutzeridentität veranschaulicht. Diese Gruppe hat nur RDP-Zugriff auf den Windows Server.
- **AnyConnect-Benutzer:** Eine Testgruppe, die Test User (Testbenutzer) hinzugefügt wird, um die Benutzeridentität zu veranschaulichen. Diese Gruppe hat nur HTTP-Zugriff auf den Windows Server.

Active Directory-Konfigurationen

Um die AD-Authentifizierung und die Benutzeridentität auf FTD ordnungsgemäß zu konfigurieren, sind einige Werte erforderlich.

Alle diese Details müssen auf dem Microsoft-Server erstellt oder erfasst werden, bevor die Konfiguration auf dem FMC durchgeführt werden 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 für die Verbindung zum Microsoft-Server. Wenn ein FQDN verwendet wird, muss ein DNS-Server innerhalb von FMC und FTD konfiguriert werden, um den FQDN aufzulösen.

In diesem Konfigurationsleitfaden lautet der Wert win2016.example.com (wird zu 192.168.1.1 aufgelöst).

- **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 Stammzertifizierungsstelle zum Signieren des von LDAPS verwendeten SSL-Zertifikats erforderlich.

- **Verzeichnisbenutzername und -kennwort:**

Dieses Konto wird von FMC und FTD verwendet, um eine Bindung 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.

- **Distinguished Name (DN) für Basis und Gruppe:**

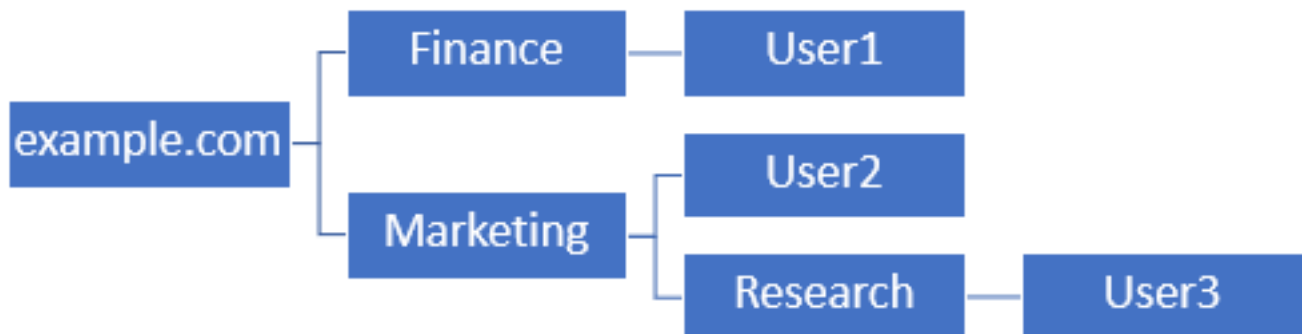
Die Basis-DN ist der Startpunkt für FMC, und die FTD weist das Active Directory an, mit der Suche und Authentifizierung von Benutzern zu beginnen.

Ebenso ist die Gruppen-DN der Ausgangspunkt, an dem FMC dem Active Directory mitteilt, wo nach Gruppen nach Benutzeridentitäten gesucht werden soll.

In diesem Konfigurationsleitfaden wird die Root-Domäne example.com als Basis-DN und Gruppen-DN verwendet.

Für eine Produktionsumgebung ist es jedoch besser, weiter innerhalb der LDAP-Hierarchie einen **Basis-DN** und einen **Gruppen-DN** zu verwenden.

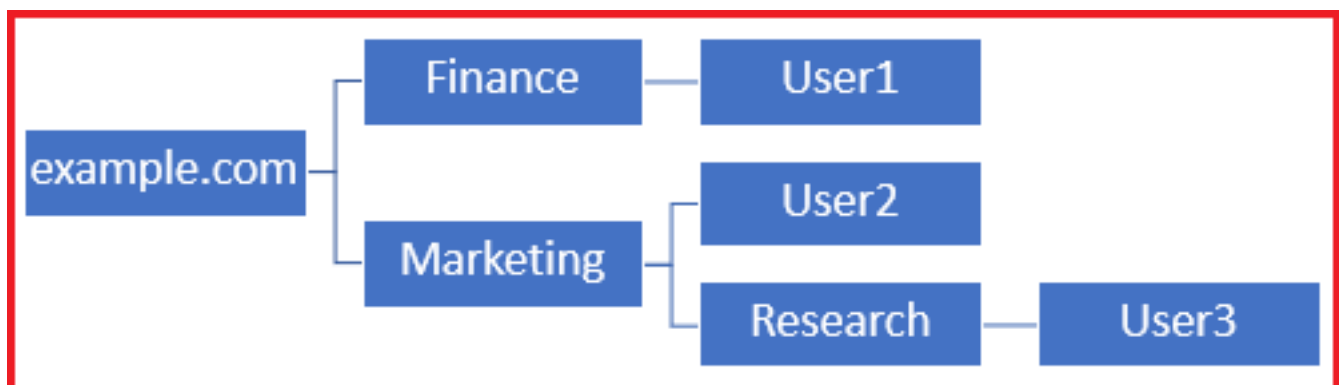
Beispiel für diese LDAP-Hierarchie:



Wenn ein Administrator möchte, dass Benutzer innerhalb der **Marketing**-Organisationseinheit die Basis-DN authentifizieren können, kann dies auf den Root (example.com) festgelegt werden.

Dies ermöglicht es User1 unter der Organisationseinheit **Finanzen** jedoch auch, sich anzumelden, da die Benutzersuche am Stamm beginnt und zu **Finanzen, Marketing** und **Forschung** führt.

Basis-DN eingestellt auf example.com

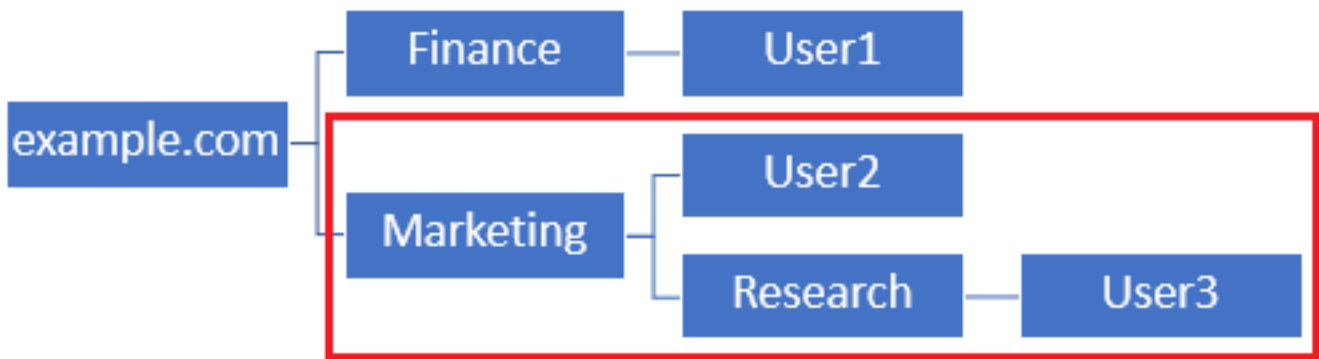


Um Anmeldungen auf den einzigen Benutzer in der Organisationseinheit **Marketing** und darunter zu beschränken, kann der Administrator stattdessen die Basis-DN auf **Marketing** festlegen.

Jetzt können nur noch User2 und User3 authentifiziert werden, da die Suche bei **Marketing**

beginnt.

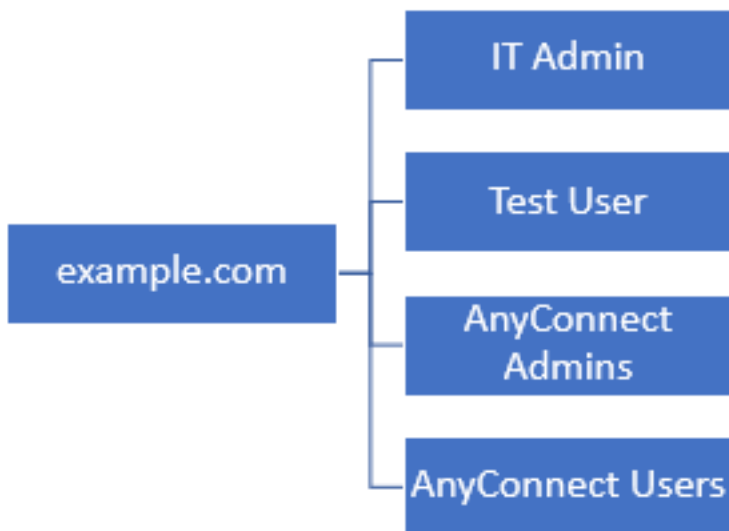
Basis-DN auf "Marketing" gesetzt



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

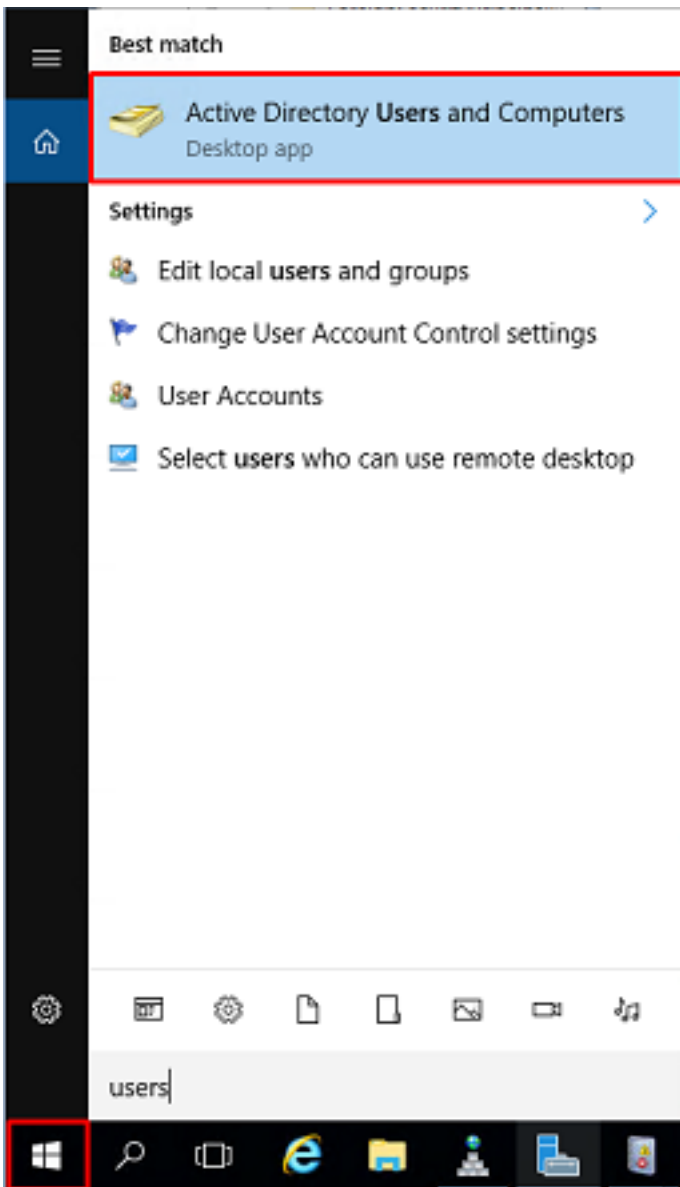
Weitere Informationen hierzu finden Sie hier: [Konfigurieren Sie AnyConnect LDAP-Zuordnung auf Firepower Threat Defense \(FTD\)](#).

Diese vereinfachte LDAP-Hierarchie wird in diesem Konfigurationsleitfaden verwendet, und der DN für den Stamm example.com wird sowohl für den Basis-DN als auch für den Gruppen-DN verwendet.

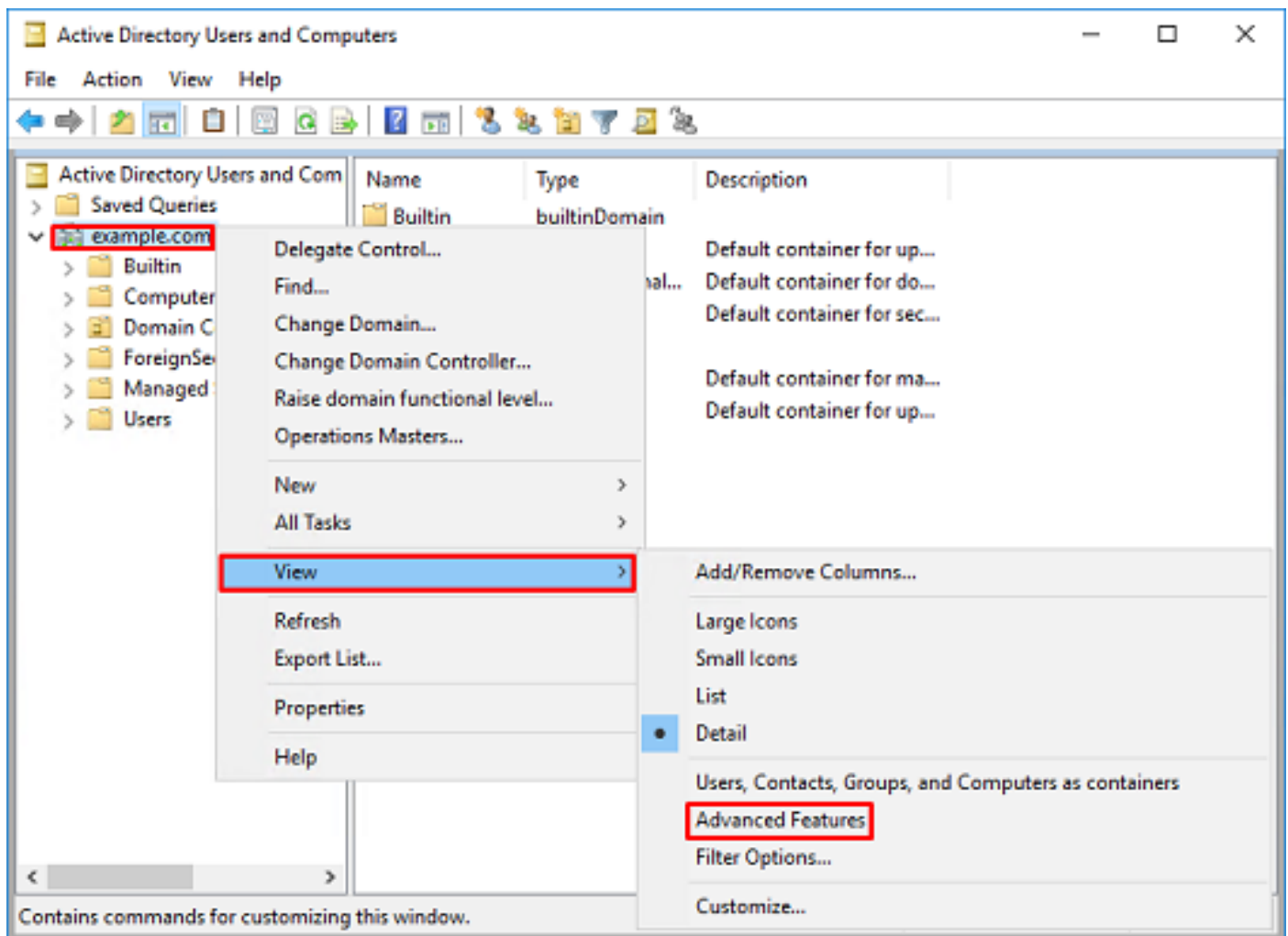


Ermitteln der LDAP-Basis-DN und Gruppen-DN

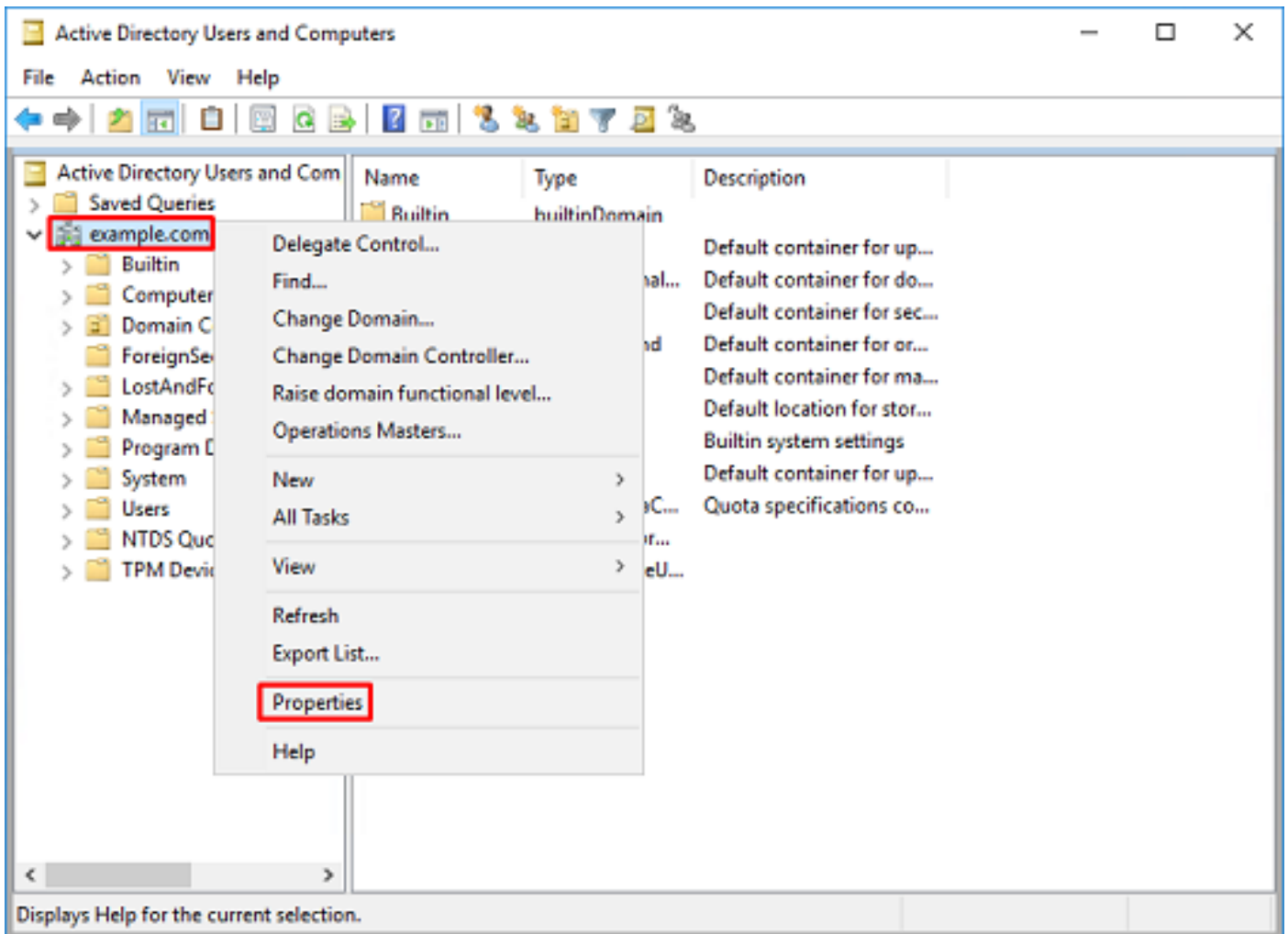
1. Öffnen Sie Active Directory-Benutzer und -Computer.



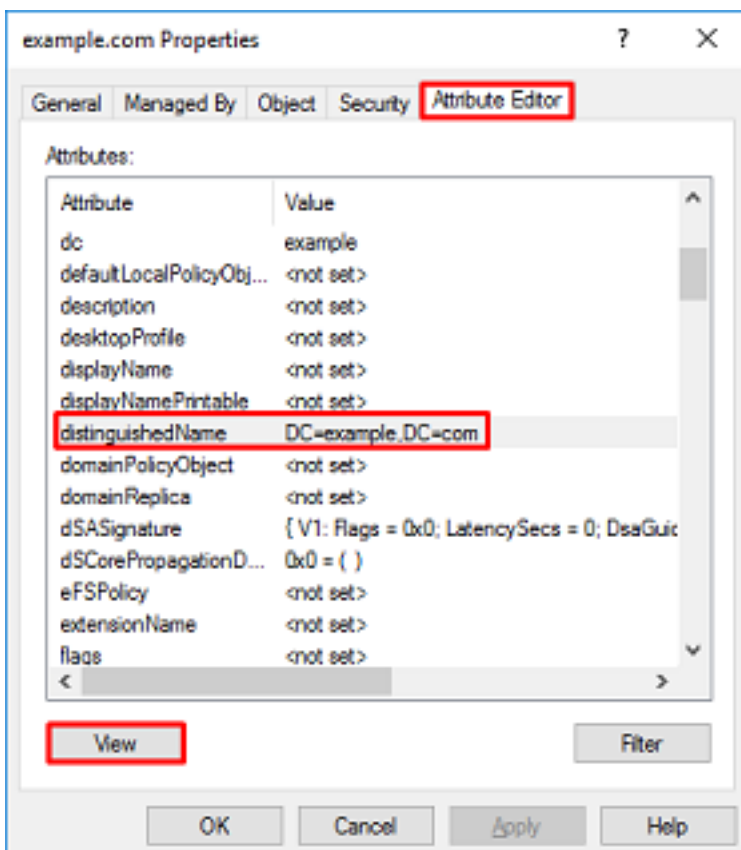
2. Klicken Sie mit der linken Maustaste auf die **Stammdomäne** (um den Container zu öffnen), klicken Sie mit der rechten Maustaste auf die **Stammdomäne**, und klicken Sie dann unter **Ansicht** auf **Erweiterte Funktionen**.



3. Dies ermöglicht die Anzeige zusätzlicher Eigenschaften unter den AD-Objekten. Um beispielsweise den DN für den Stamm example.com zu finden, klicken Sie mit der rechten Maustaste auf example.com, und wählen Sie dann **Eigenschaften** aus.

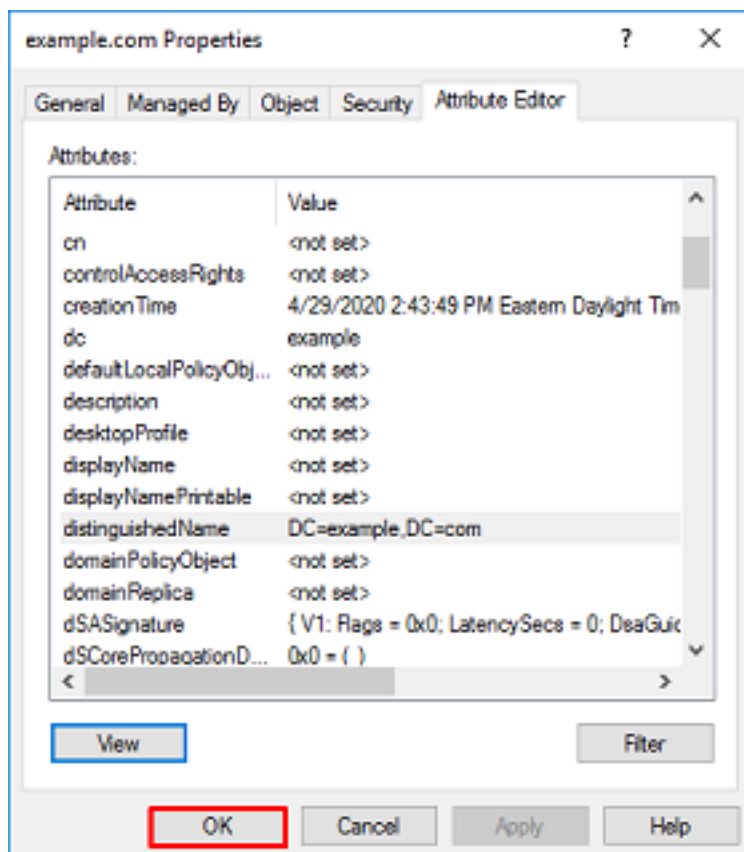
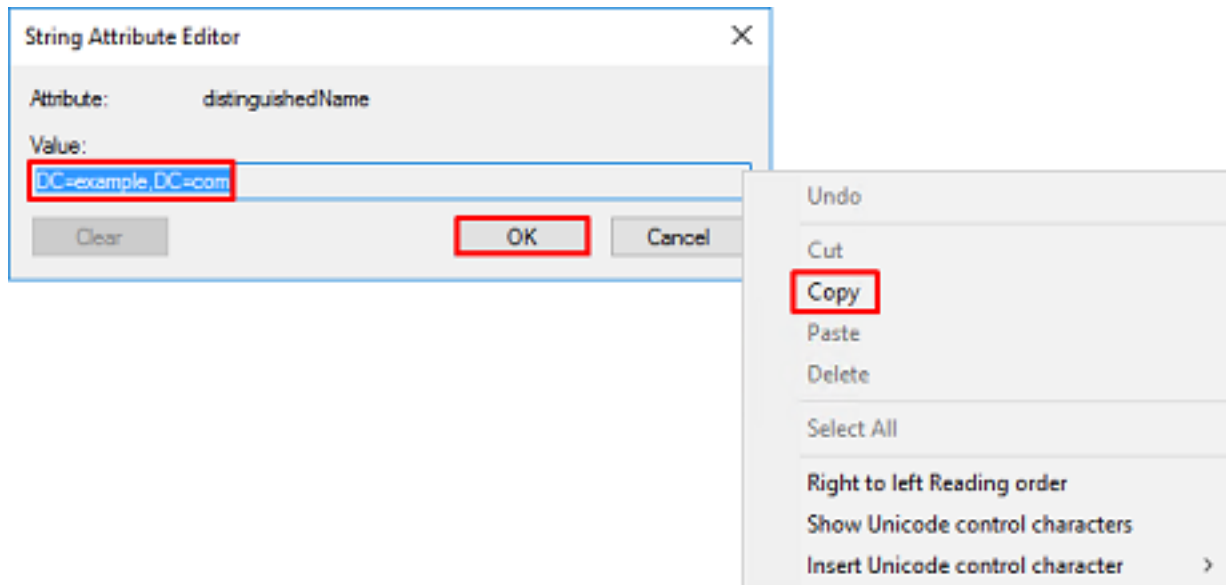


4. Wählen Sie unter **Eigenschaften** die Registerkarte **Attributeditor**. Suchen Sie unter den **Attributen** den **DistinguishedName**, und klicken Sie dann auf **Anzeigen**.

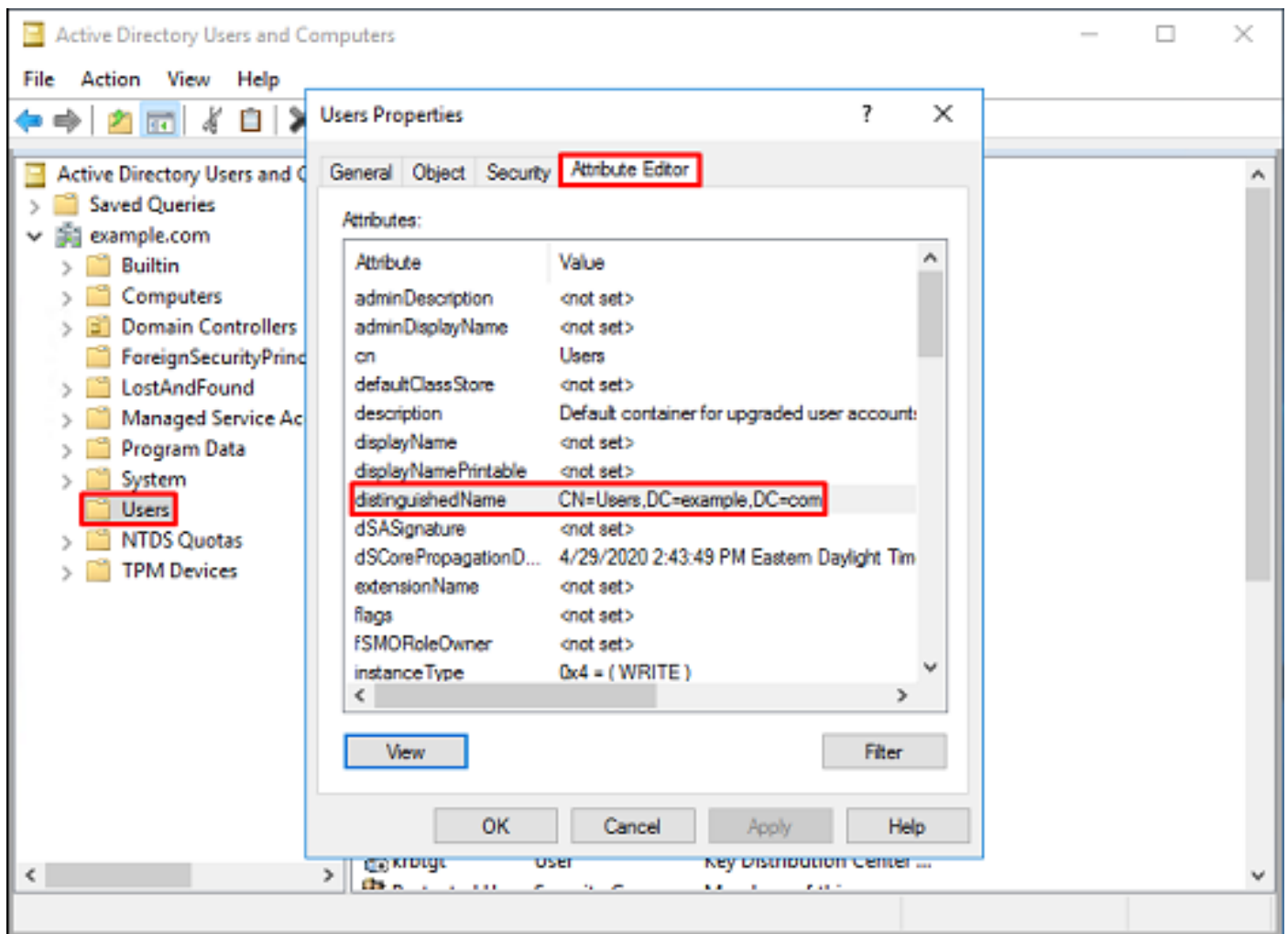


5. Dadurch wird ein neues Fenster geöffnet, in das die DN kopiert und später in FMC eingefügt werden kann. In diesem Beispiel ist die Stamm-DN DC=example,DC=com.

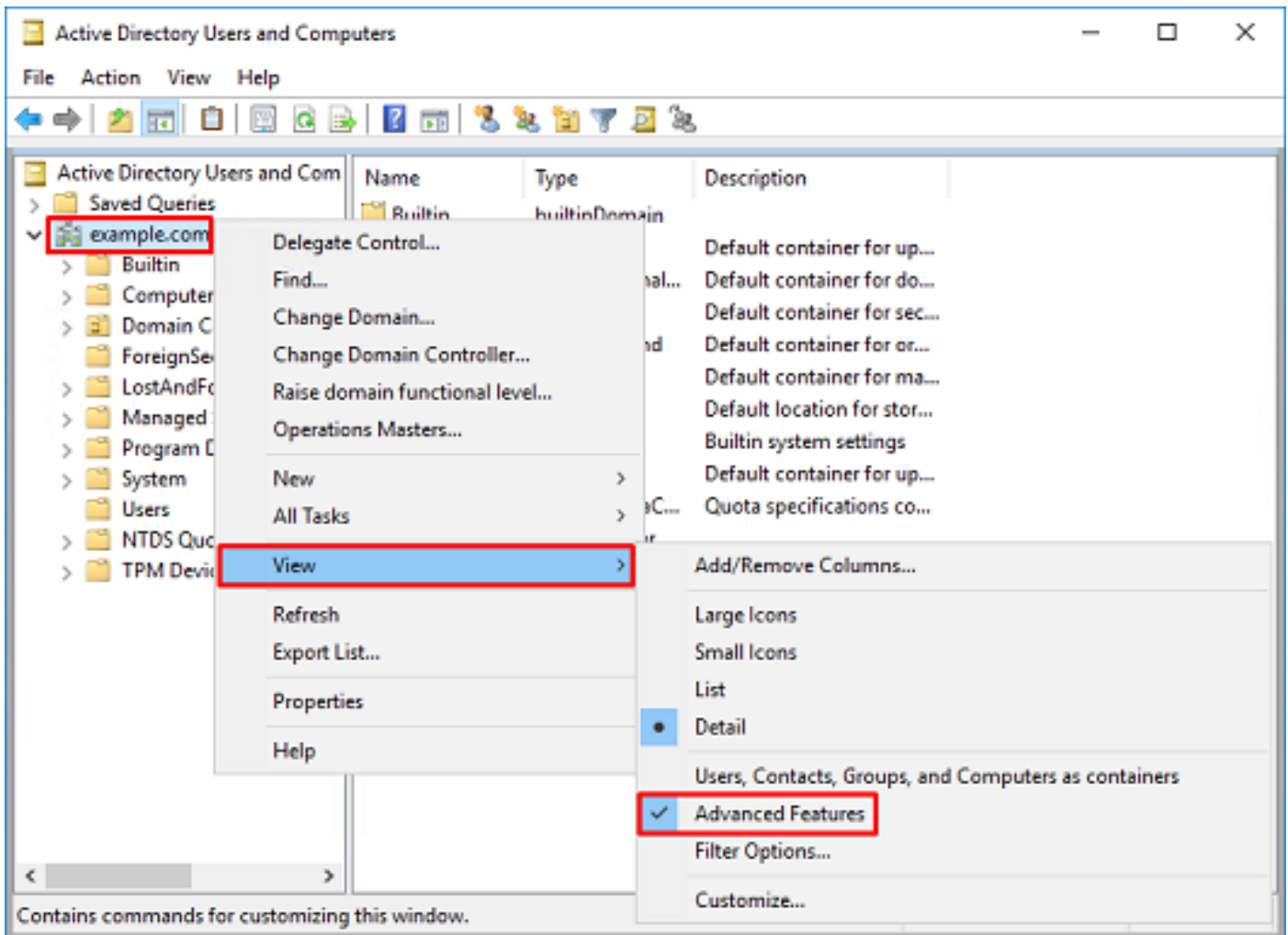
Kopieren Sie den Wert, und speichern Sie ihn für später. Klicken Sie auf **OK**, um das Fenster **Zeichenfolgenattribut-Editor** zu schließen, und klicken Sie erneut auf OK, um die **Eigenschaften** zu beenden.



Dies kann für mehrere Objekte in **Active Directory** erfolgen. Beispielsweise werden die folgenden Schritte verwendet, um den DN des **User-Containers** zu ermitteln:



6. Die Ansicht **Erweiterte Funktionen** kann entfernt werden, indem Sie erneut mit der rechten Maustaste auf die Stamm-DN klicken. Klicken Sie dann unter **Ansicht** erneut auf **Erweiterte Funktionen**.



FTD-Konto erstellen

Dieses Benutzerkonto ermöglicht FMC und FTD, eine Bindung mit dem Active Directory herzustellen, um nach Benutzern und Gruppen zu suchen und Benutzer zu authentifizieren.

Durch die Einrichtung eines separaten FTD-Kontos soll verhindert werden, dass Unbefugte an anderen Stellen im Netzwerk auf die für die Bindung verwendeten Anmeldeinformationen zugreifen können.

Dieses Konto muss sich nicht im Bereich des Basis-DN oder Gruppen-DNs befinden.

1. Klicken Sie in **Active Directory User and Computers** mit der rechten Maustaste auf den Container/die Organisation, der/der das FTD-Konto hinzugefügt wird.

In dieser Konfiguration wird das FTD-Konto unter dem Benutzernamen `ftd.admin@example.com` unter dem Container **Users** hinzugefügt.

Klicken Sie mit der rechten Maustaste auf **Benutzer**, und navigieren Sie dann zu **Neu > Benutzer**.

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:

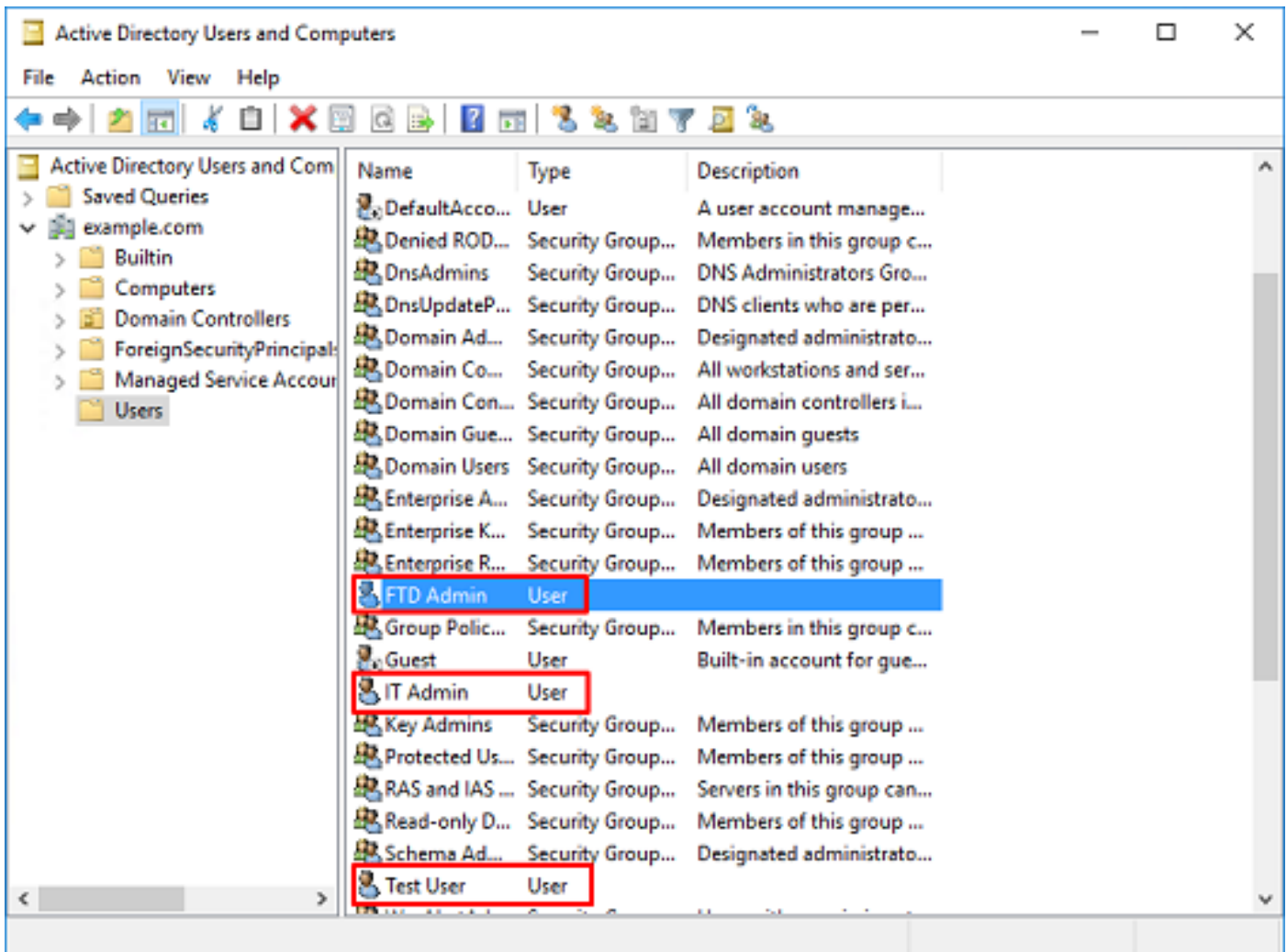
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

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



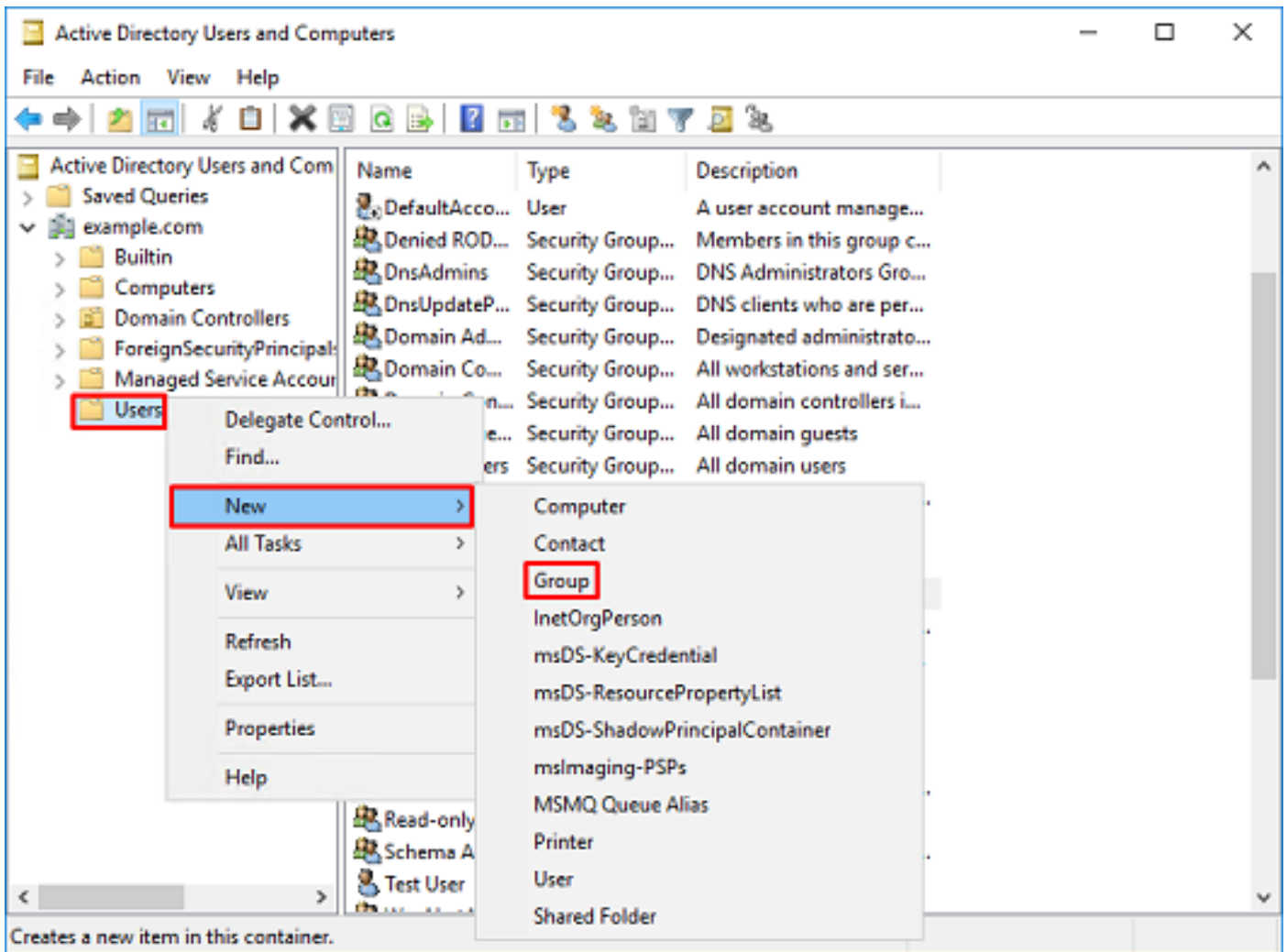
AD-Gruppen erstellen und AD-Gruppen Benutzer hinzufügen (optional)

Obwohl sie für die Authentifizierung nicht erforderlich sind, können Gruppen verwendet werden, um die Anwendung von Zugriffsrichtlinien auf mehrere Benutzer sowie die LDAP-Autorisierung zu vereinfachen.

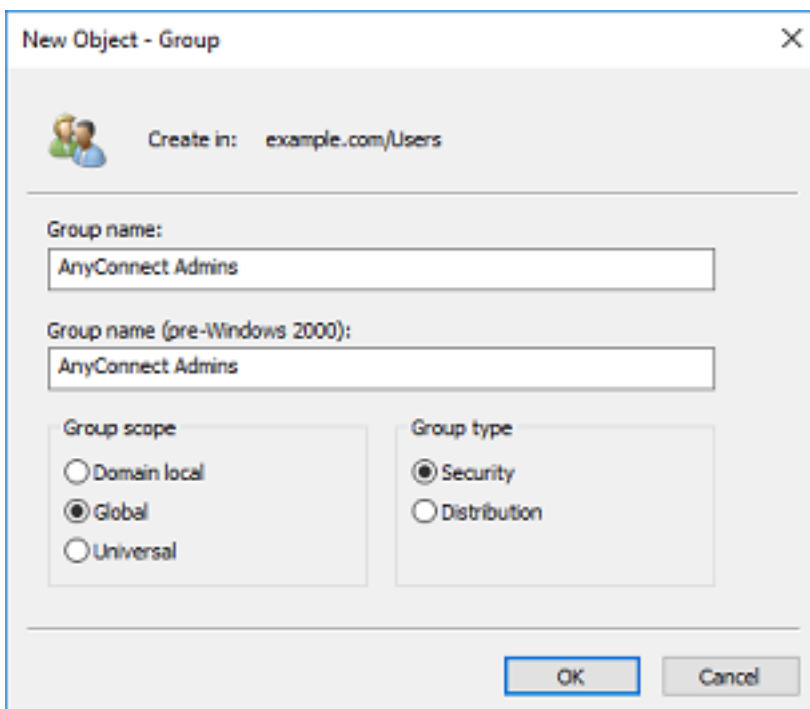
In diesem Konfigurationsleitfaden werden Gruppen verwendet, um die Richtlinieneinstellungen für die Zugriffskontrolle später über die Benutzeridentität in FMC anzuwenden.

1. Klicken Sie in **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf den Container oder die Organisationseinheit, zu dem bzw. der die neue Gruppe hinzugefügt wird.

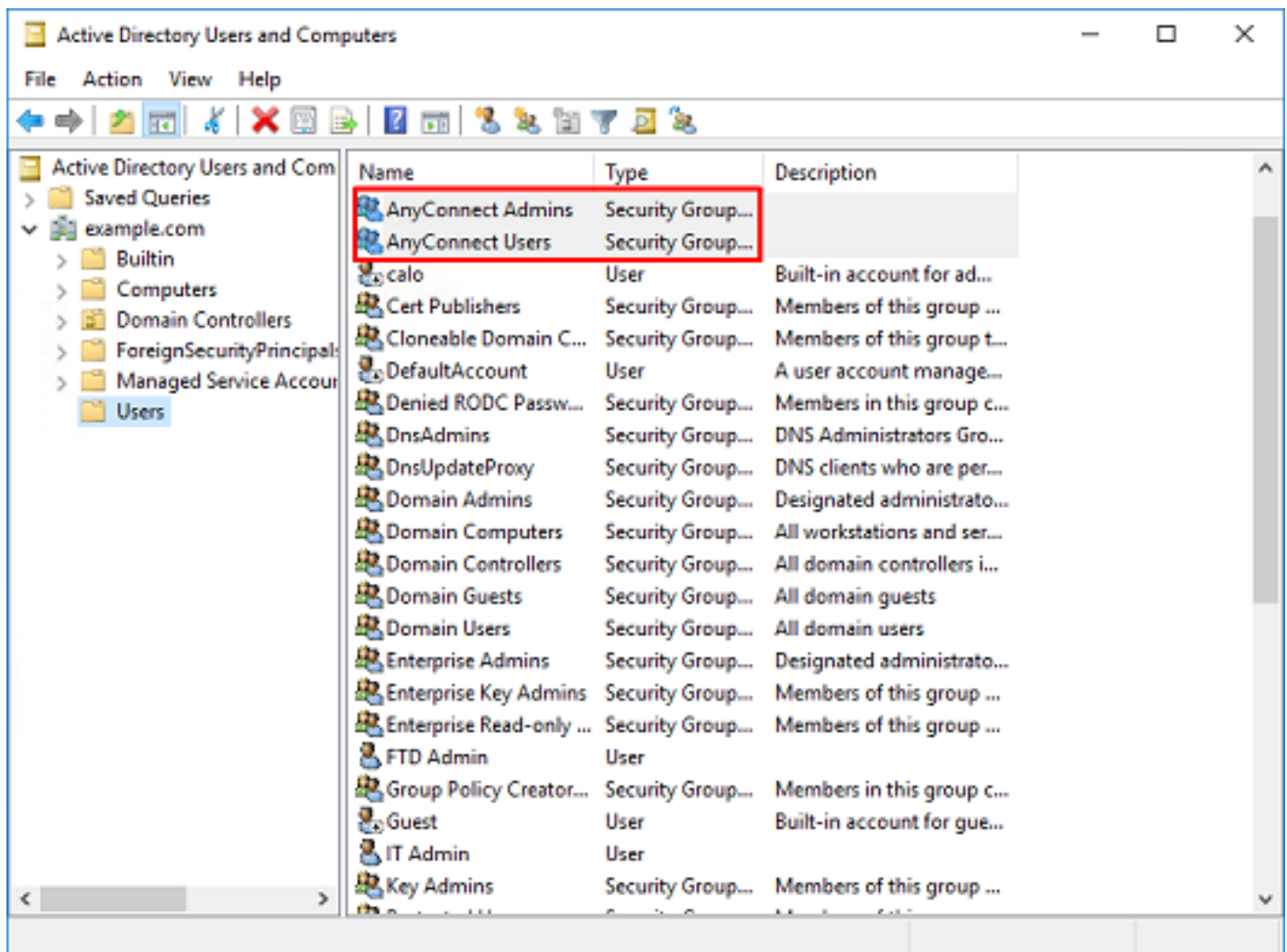
In diesem Beispiel wird die Gruppe AnyConnect-Administratoren unter dem Container **Benutzer** hinzugefügt. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und navigieren Sie dann zu **Neu > Gruppe**.



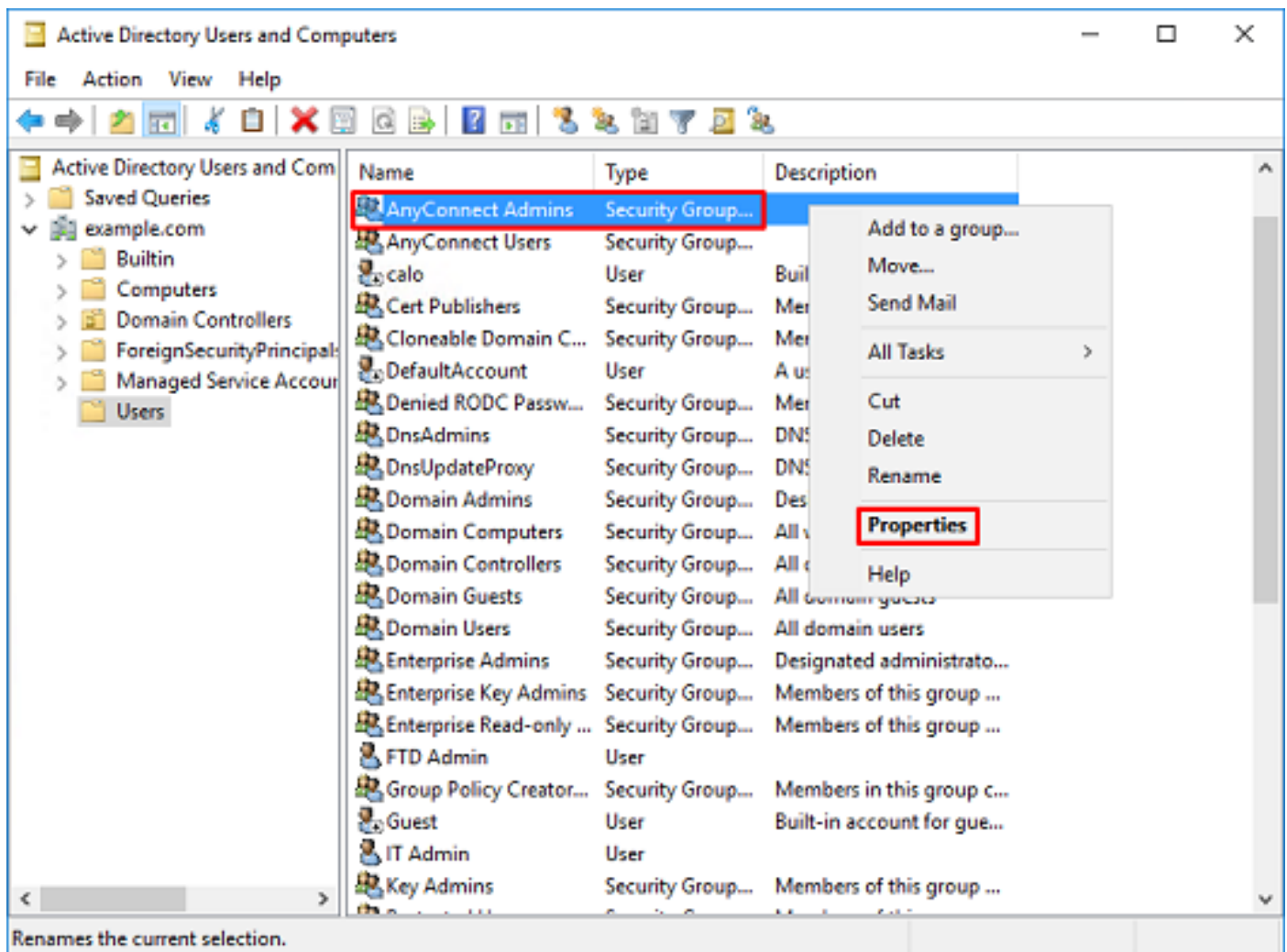
2. Gehen Sie durch den **New Object - Group Wizard**.



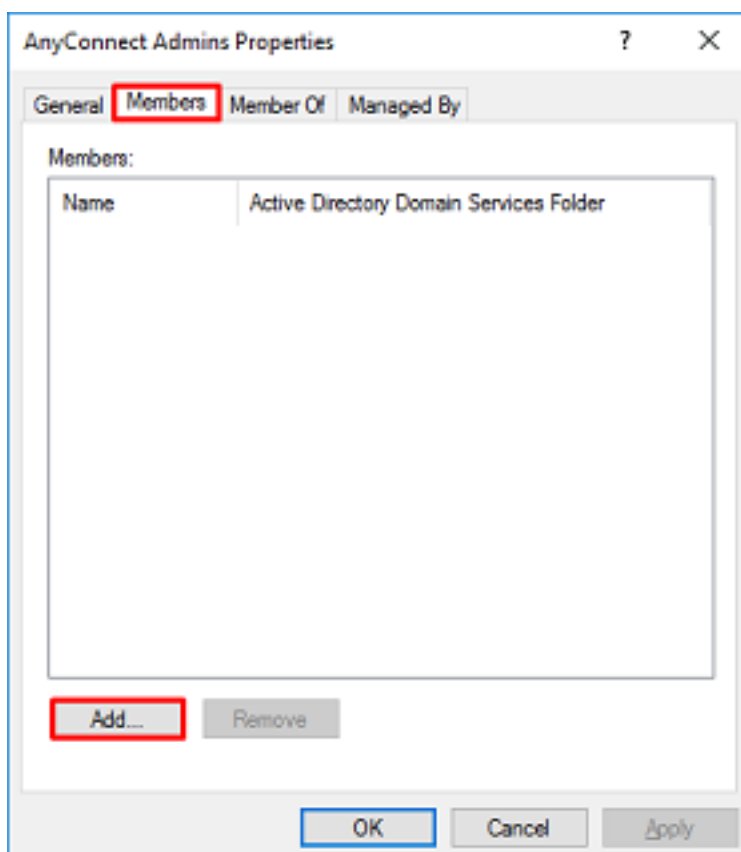
3. Überprüfen Sie, ob die Gruppe erstellt wurde. Die Gruppe **AnyConnect-Benutzer** wird ebenfalls erstellt.



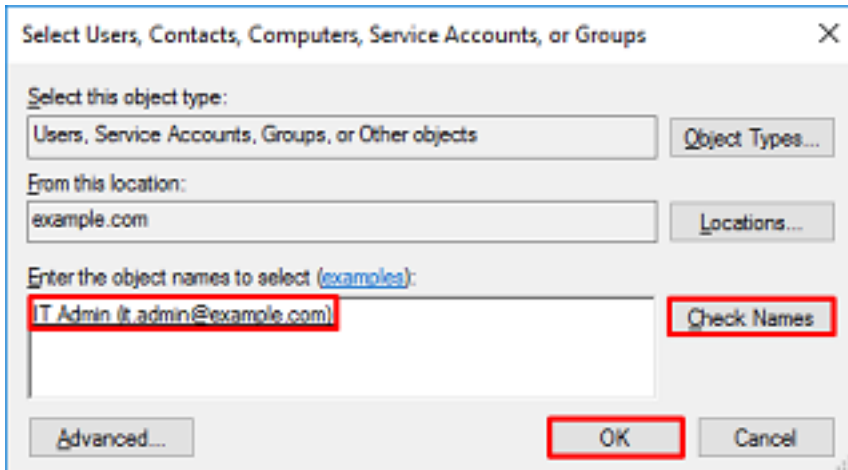
4. Klicken Sie mit der rechten Maustaste auf die Gruppe der Benutzer, und wählen Sie dann **Eigenschaften**. In dieser Konfiguration wird der Benutzer IT-Administrator der Gruppe AnyConnect-Administratoren hinzugefügt, und der Benutzer **Test-Benutzer** wird der Gruppe AnyConnect-Benutzer hinzugefügt.



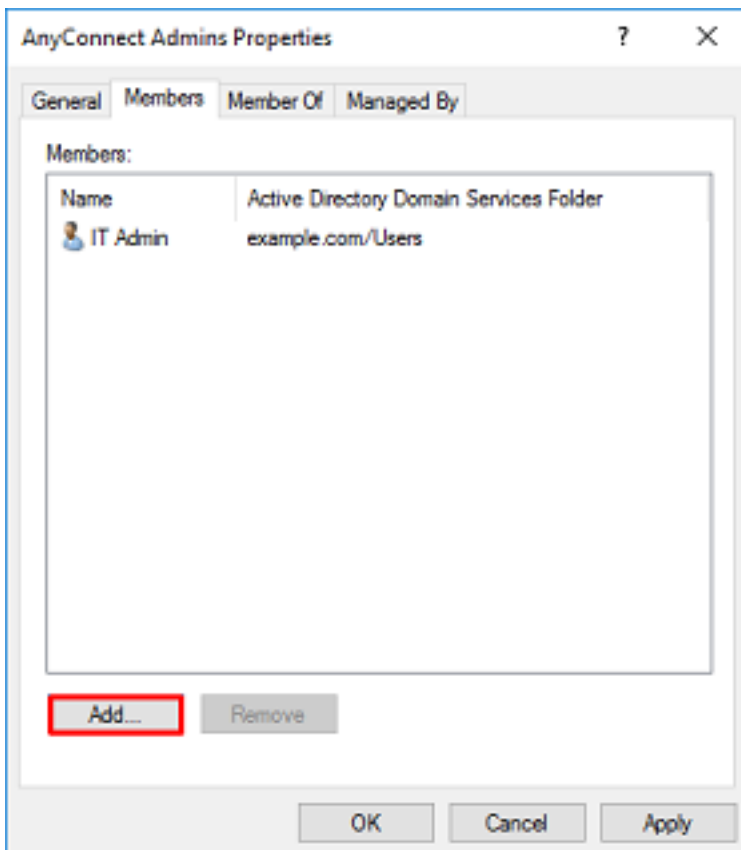
5. Klicken Sie unter Mitglieder auf Hinzufügen.



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

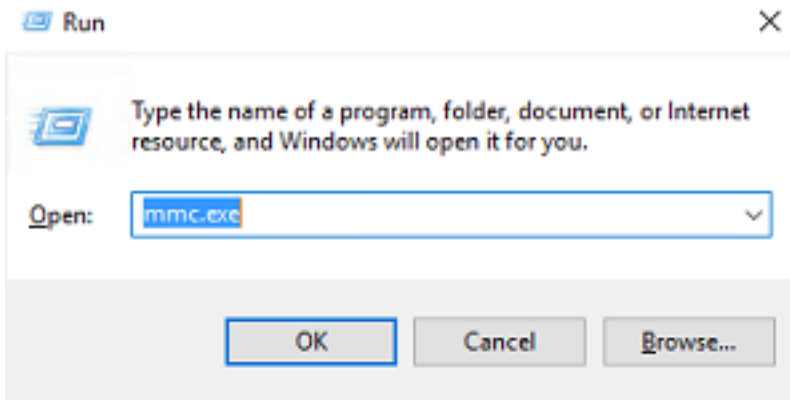


Vergewissern Sie sich, dass der richtige Benutzer hinzugefügt wurde, und klicken Sie dann auf die Schaltfläche **OK**. Der Benutzer **Testbenutzer** wird mit denselben Schritten zur Gruppe **AnyConnect-Benutzer** hinzugefügt.

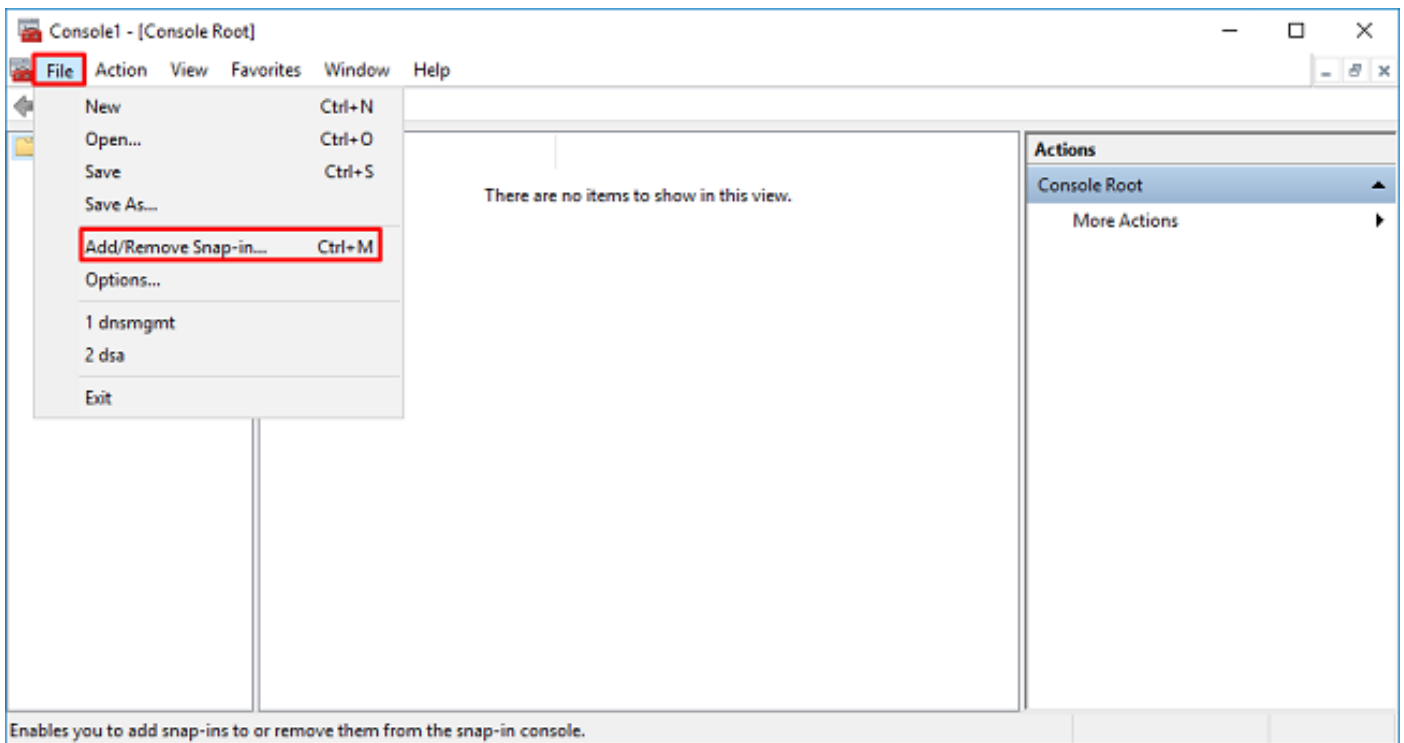


Kopieren Sie die LDAPS SSL-Zertifikatwurzel (nur für LDAPS oder STARTTLS erforderlich).

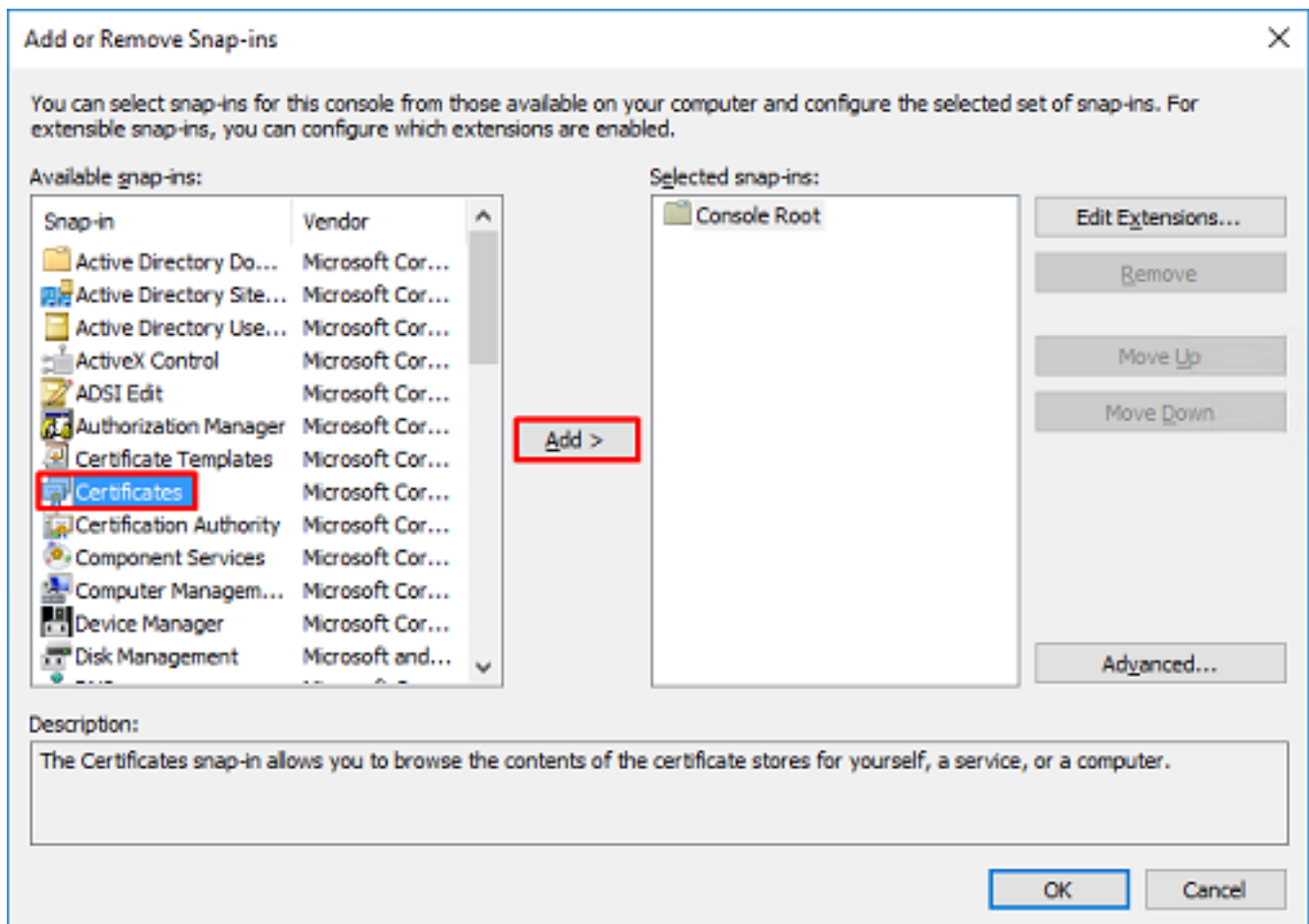
1. Drücken Sie **Win+R**, und geben Sie **mmc.exe** ein. Klicken Sie dann auf **OK**.



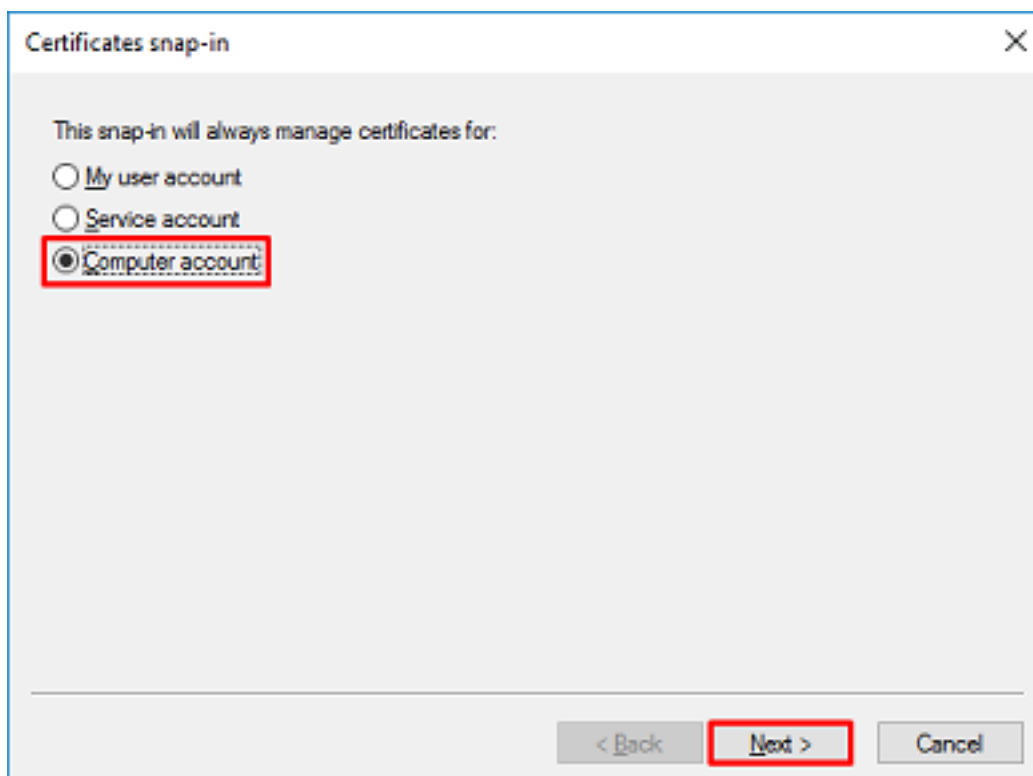
2. Navigieren Sie zu **Datei > Snap-In hinzufügen/entfernen...**



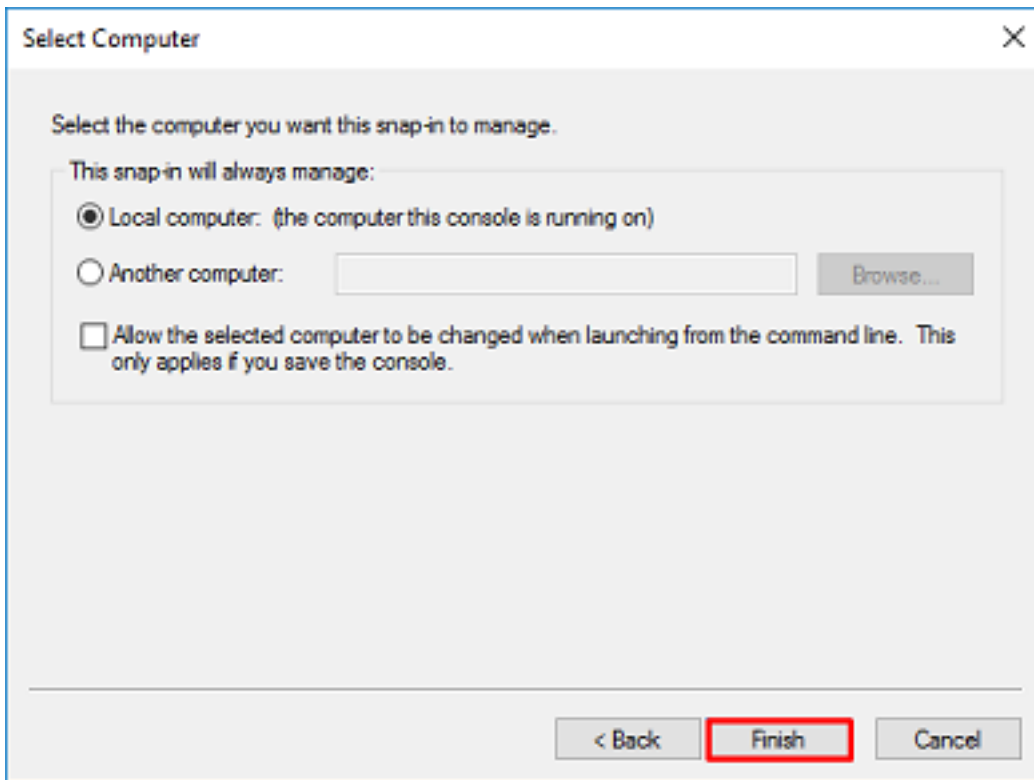
3. Wählen Sie unter **Verfügbare Snap-Ins** die Option **Zertifikate aus**, und klicken Sie dann auf **Hinzufügen**.



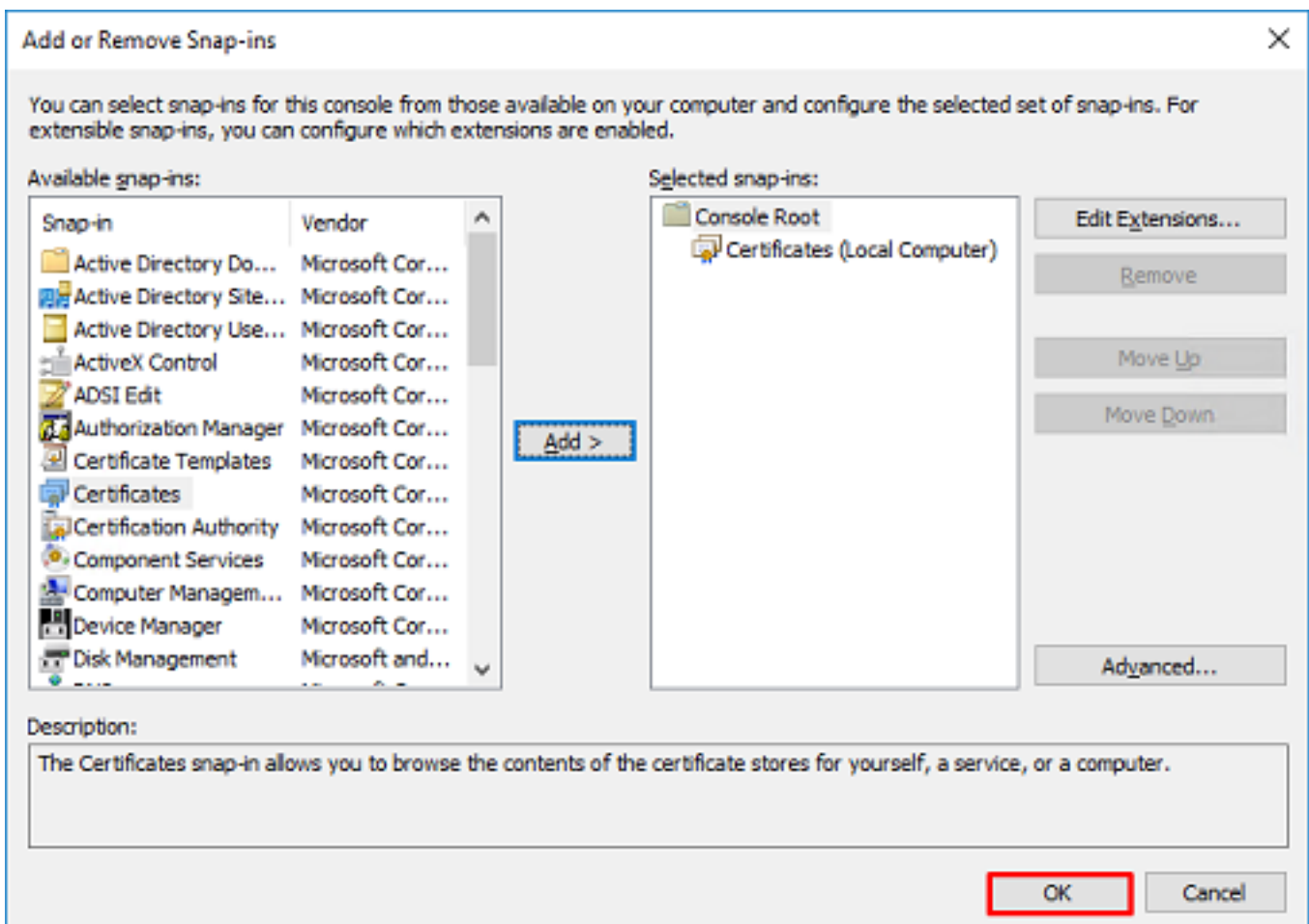
4. Wählen Sie **Computerkonto** aus, und klicken Sie dann auf **Weiter**.



Klicken Sie auf **Beenden**.



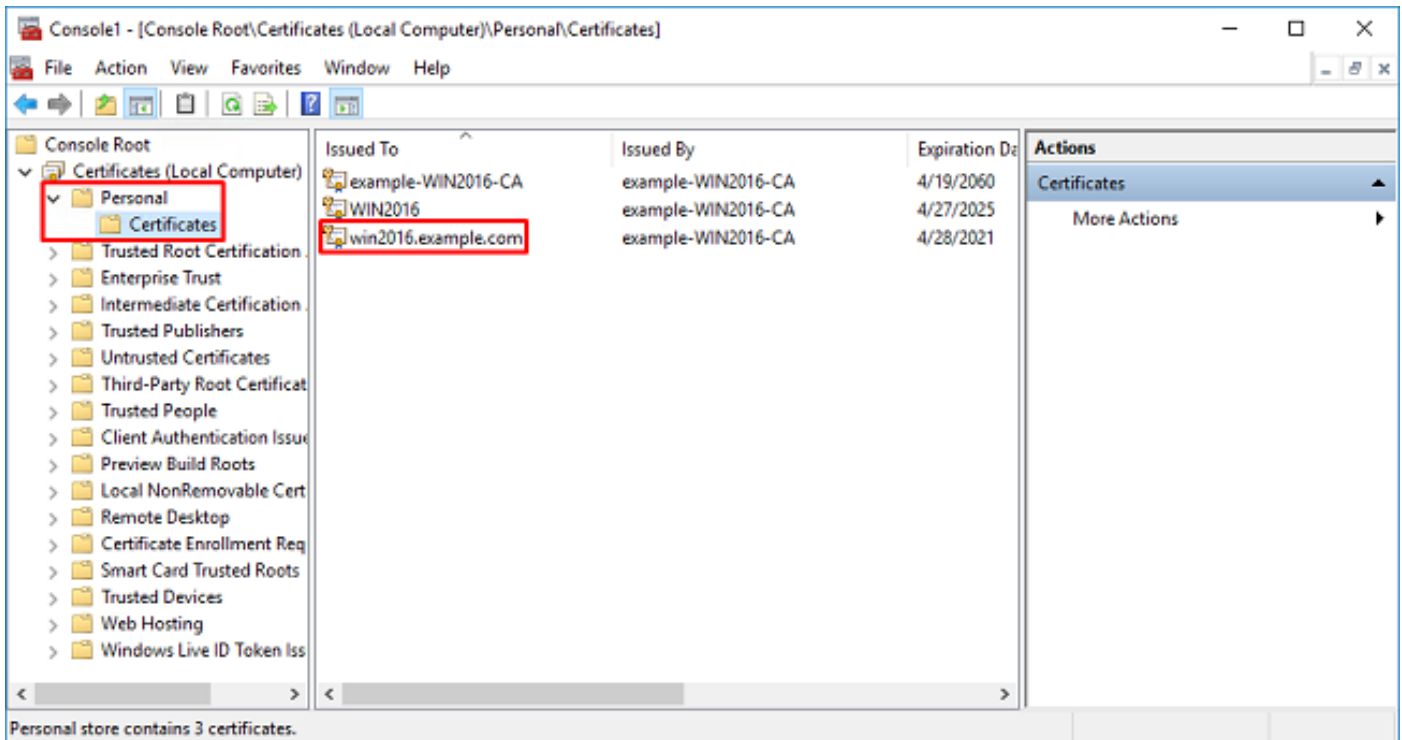
5. Klicken Sie nun auf **OK**.



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

- Ein Zertifizierungsstellenzertifikat, das von example-WIN2016-CA ausgegeben wird.
- Ein Identitätszertifikat, das von example-WIN2016-CA für WIN2016 ausgestellt wurde.
- Ein von example-WIN2016-CA an win2016.example.com ausgestelltes Identitätszertifikat.

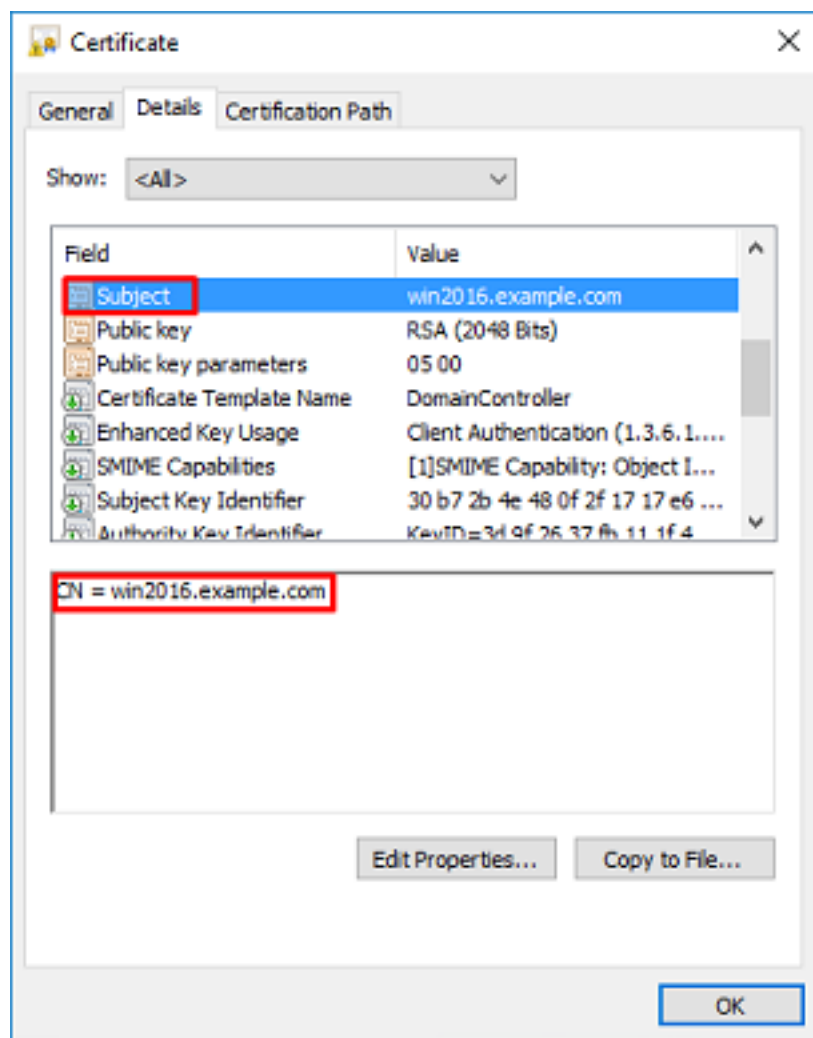
In diesem Konfigurationsleitfaden lautet der FQDN win2016.example.com. Daher sind die ersten beiden Zertifikate nicht als LDAPS SSL-Zertifikat gültig. Das an win2016.example.com ausgestellte Identitätszertifikat ist ein Zertifikat, das automatisch vom Windows Server-Zertifizierungsstellendienst ausgestellt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

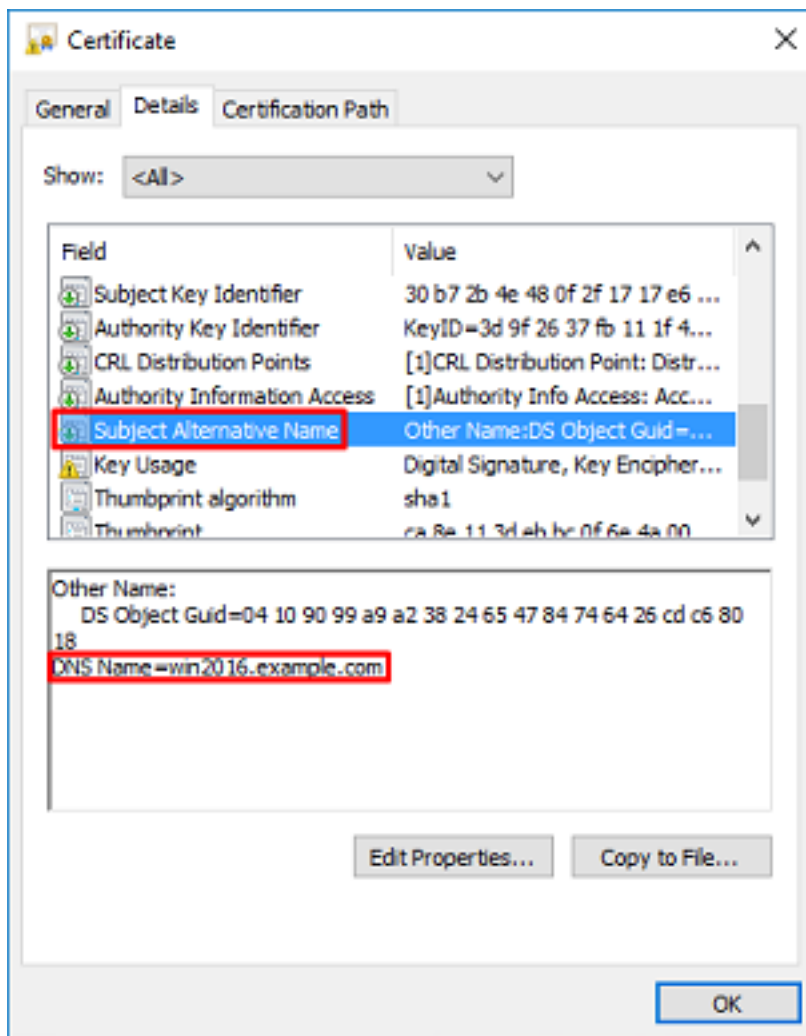


7. Um als LDAPS SSL Zertifikat verwendet werden zu können, muss das Zertifikat folgende Anforderungen erfüllen:

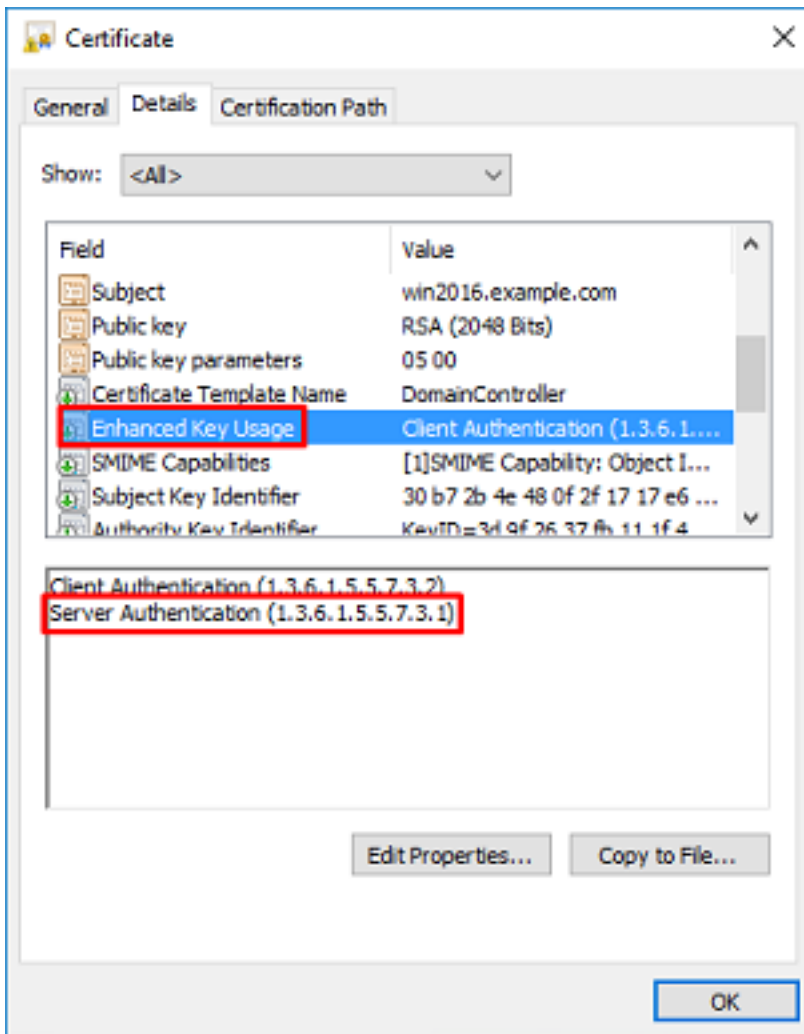
- Der allgemeine Name oder der **alternative Name für den DNS-Betreff** stimmt mit dem FQDN von Windows Server überein.
- Das Zertifikat verfügt im Feld **Erweiterte Schlüsselverwendung über Serverauthentifizierung**.

Wählen Sie auf der Registerkarte **Details** für das Zertifikat **Subject (Betreff)** und **Subject Alternative Name (Alternativer Name des Betreffs)** aus, um den FQDN win2016.example.com aufzurufen.

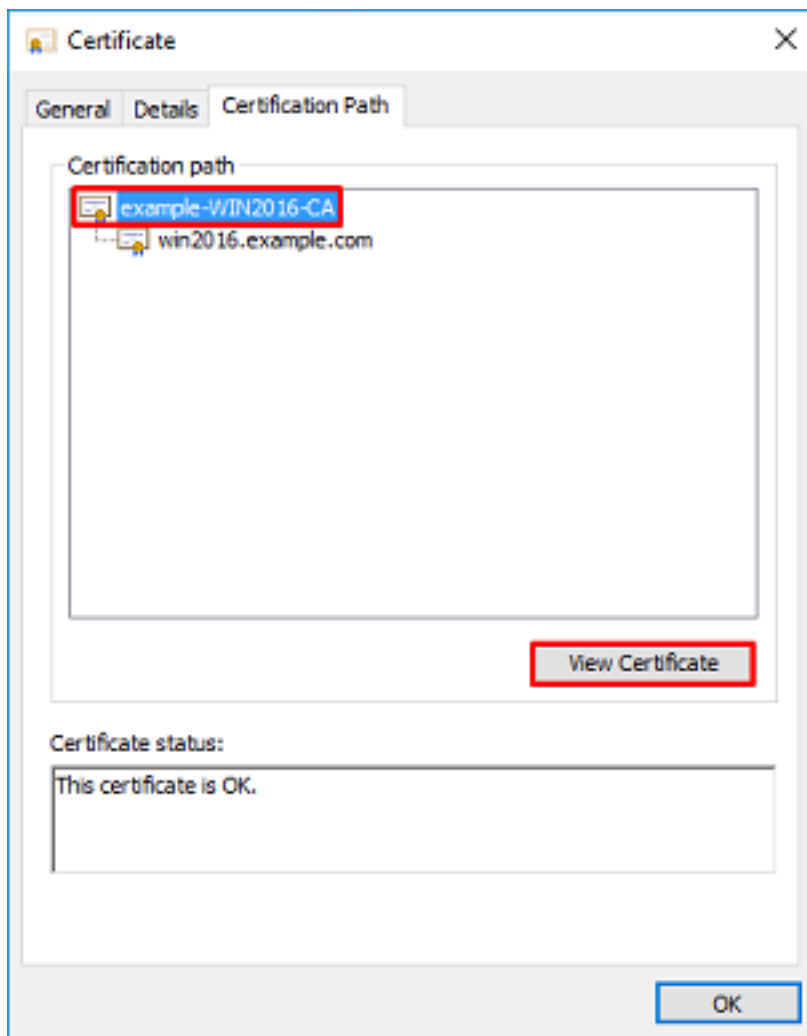




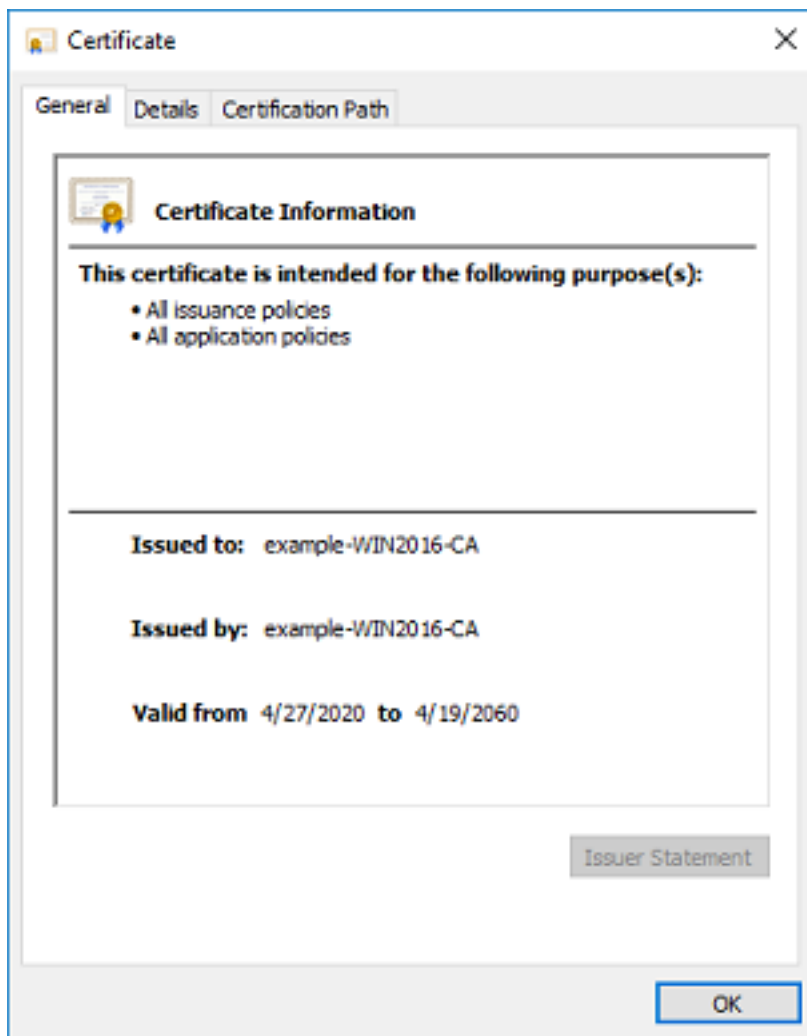
Unter **Erweiterte Schlüsselverwendung** ist die **Serverauthentifizierung** vorhanden.



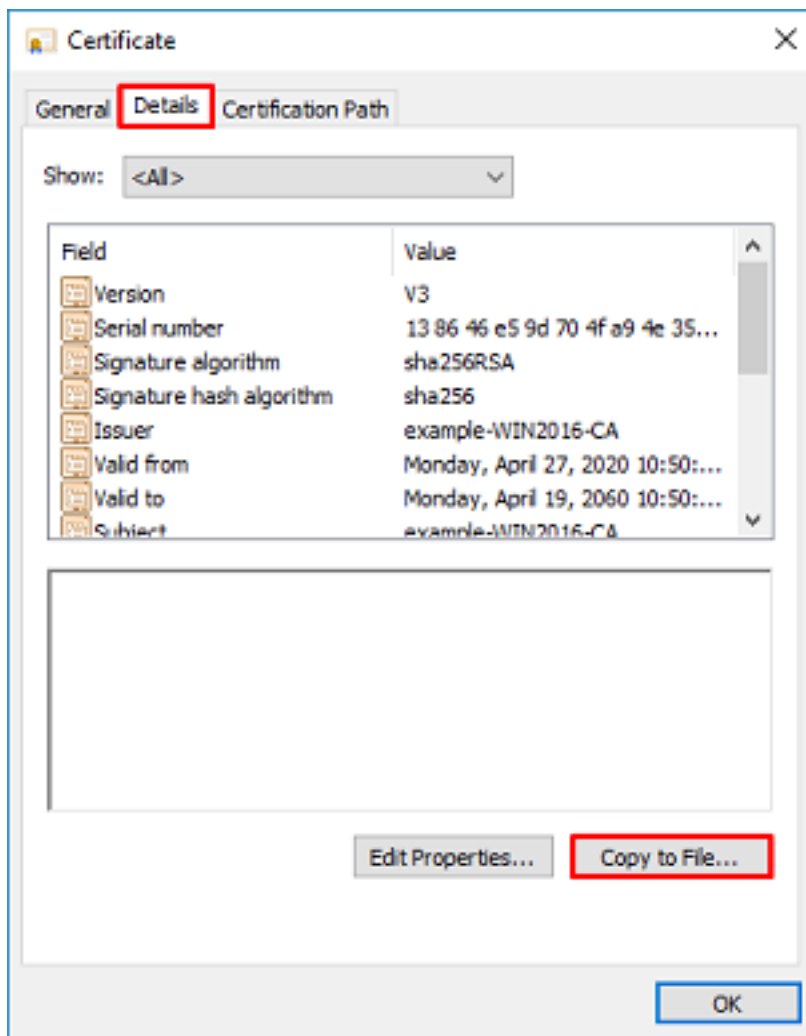
8. Nachdem dies bestätigt wurde, wählen Sie auf der Registerkarte **Zertifizierungspfad** das oberste Zertifikat aus, das das Stammzertifikat der Zertifizierungsstelle ist, und klicken Sie dann auf **Zertifikat anzeigen**.



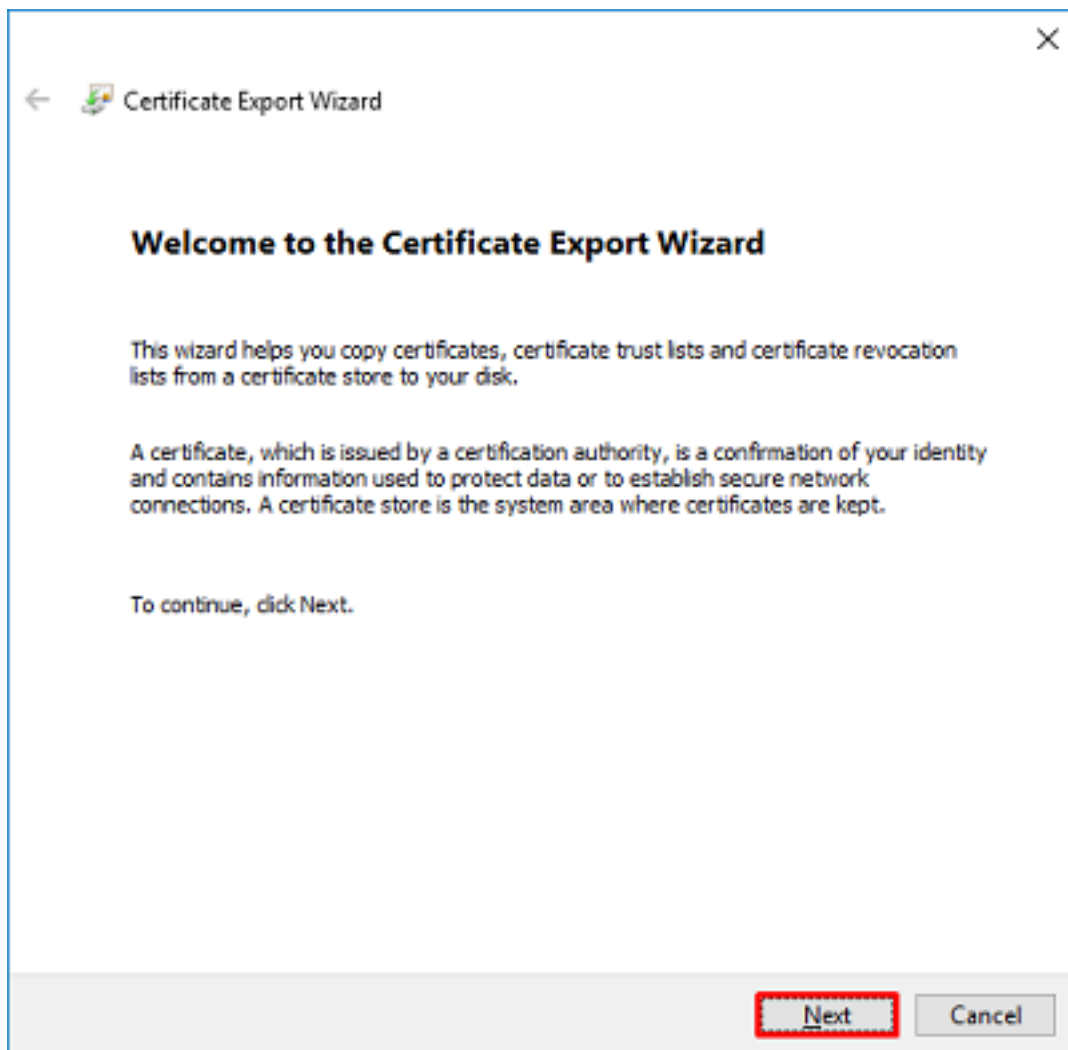
9. Dadurch werden die Zertifikatdetails für das Stammzertifikat der Zertifizierungsstelle geöffnet.



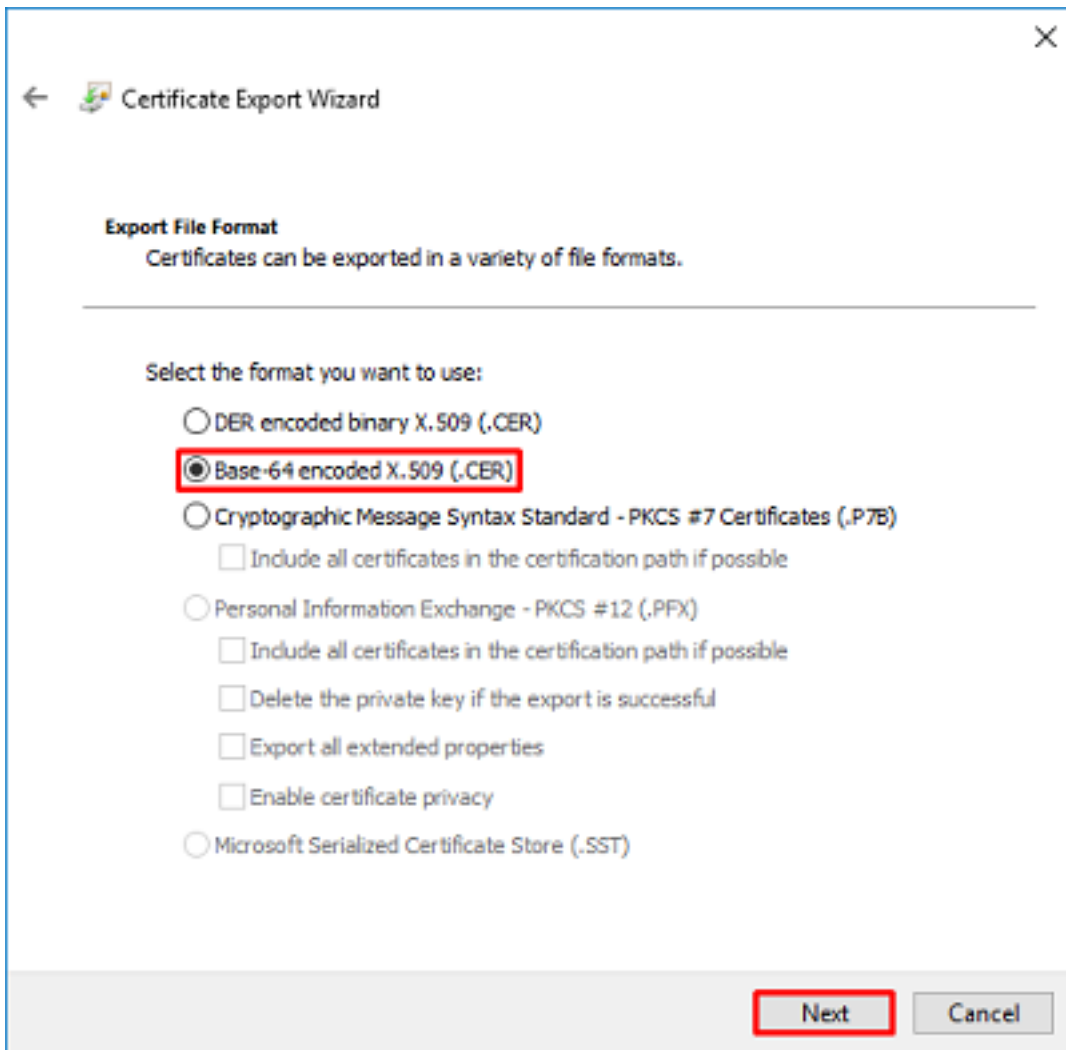
Klicken Sie auf der Registerkarte **Details** auf **In Datei kopieren...**



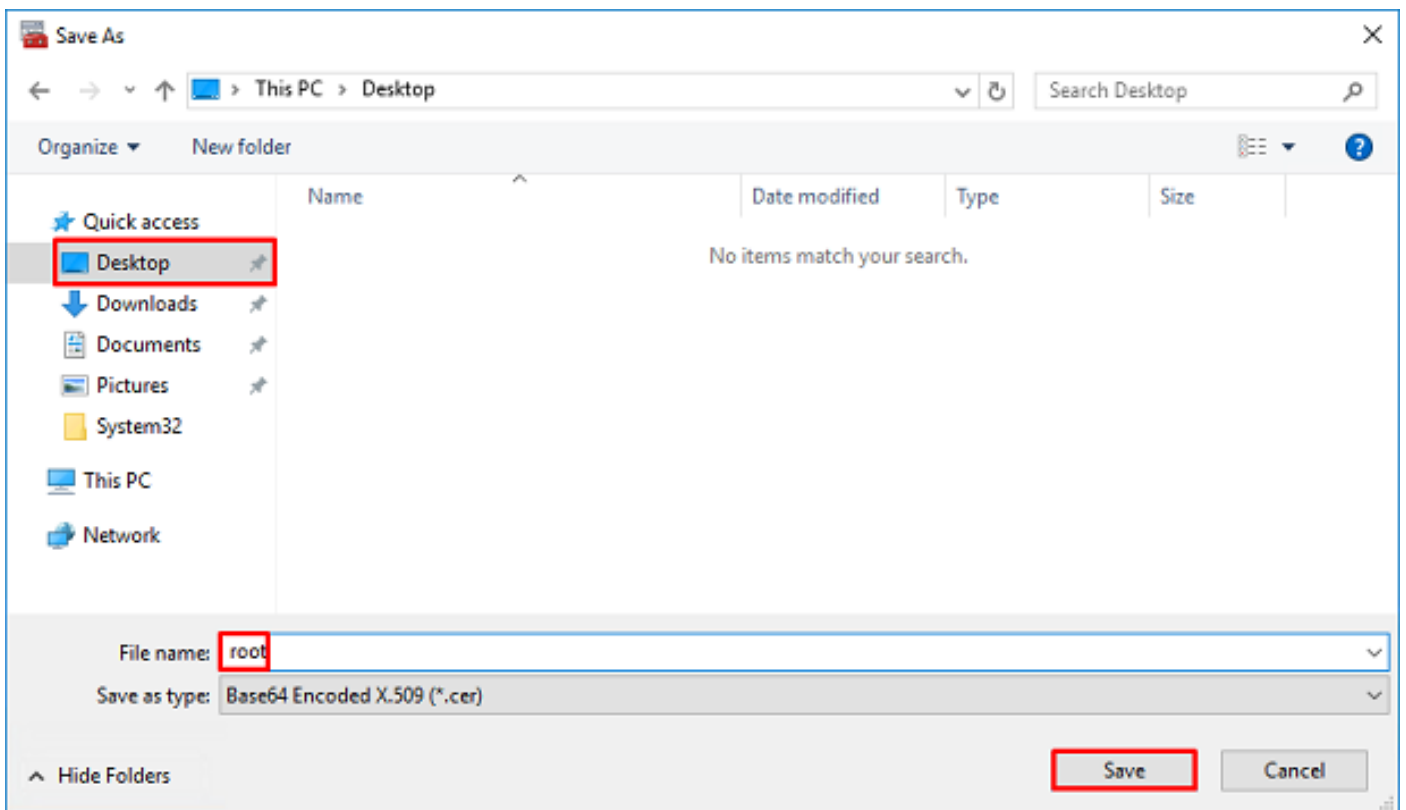
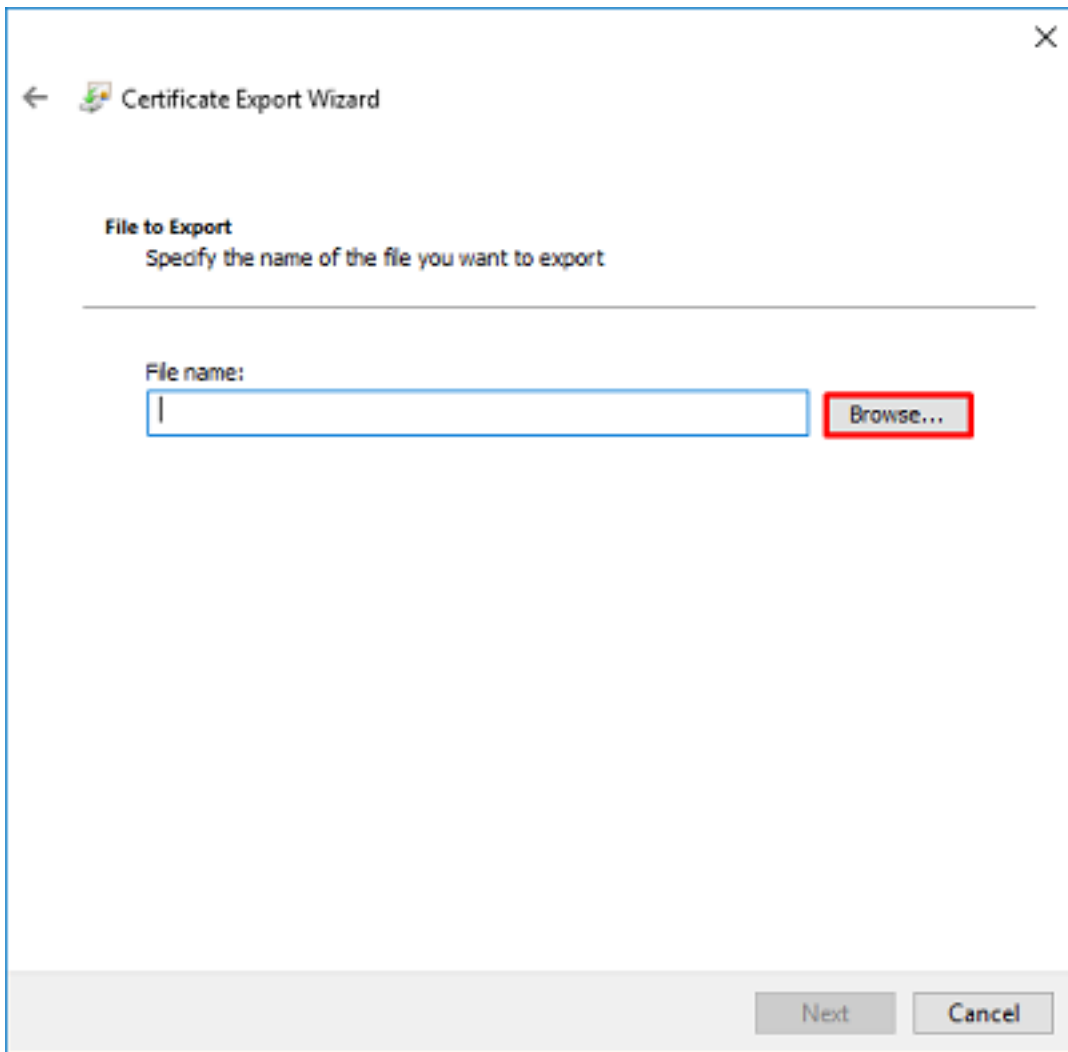
10. Gehen Sie durch den **Zertifikatexport-Assistenten**, der die Stammzertifizierungsstelle im PEM-Format exportiert.

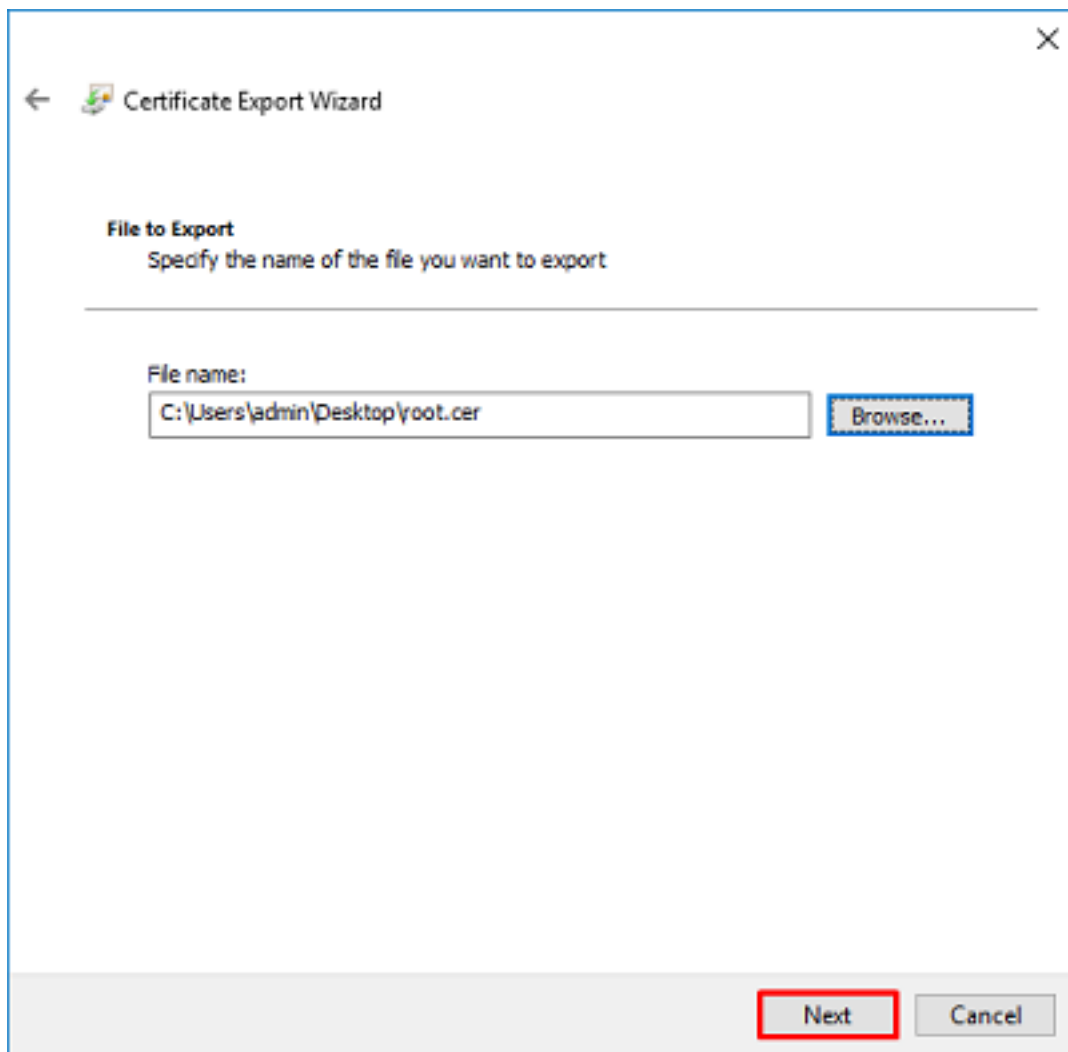


Wählen Sie **Base-64-codiertes X.509** aus

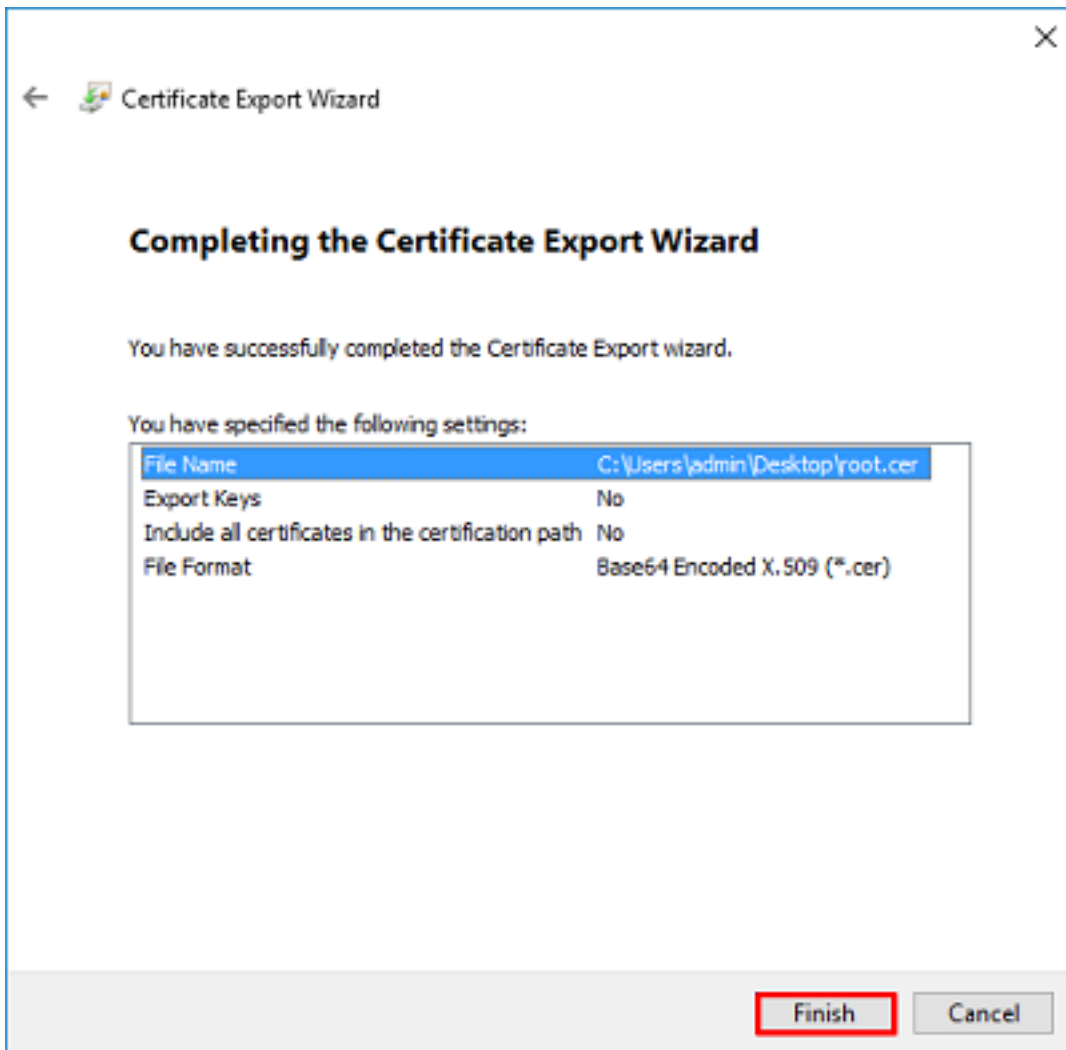


Wählen Sie den Namen der Datei und den Speicherort aus, in den sie exportiert wird.





Klicken Sie nun auf **Fertig stellen**.



11. Gehen Sie nun zum Ort und öffnen Sie das Zertifikat mit einem Notizblock oder einem anderen Texteditor. Zeigt das Zertifikat im PEM-Format an. Speichern Sie das für später.

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlAMB0xGzAZBgNVBAMTEmV4YW1wbGUtV01OMjAxNi1lDQTC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAEt7r
pHFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEm0c9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgrEtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubRl+d
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixwPdrbAD06zMHbEYEHkh00jBrUEBBI6Cy83iTZ9ejsk
KgWBJXEu33PplW6E
-----END CERTIFICATE-----
```

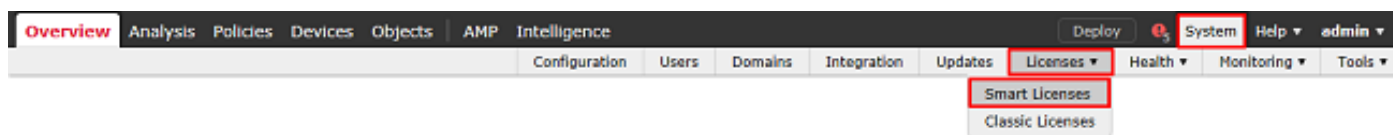
12. (Optional) Falls es mehrere Identitätszertifikate gibt, die von LDAPS verwendet werden können und Unsicherheit darüber besteht, welche davon verwendet wird, oder wenn kein Zugriff auf den LDAPS-Server besteht, ist es möglich, die Root-CA aus einer Paketerfassung zu extrahieren, die auf dem Windows-Server oder FTD danach durchgeführt wird.

FMC-Konfigurationen

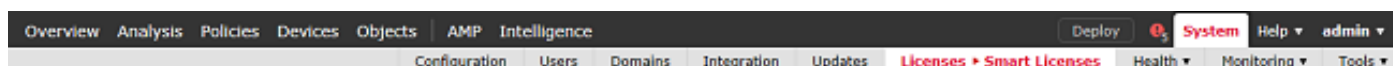
Lizenzierung überprüfen

Um eine AnyConnect-Konfiguration bereitzustellen, muss der FTD beim Smart Licensing-Server registriert werden, und es muss eine gültige Plus-, Apex- oder VPN Only-Lizenz auf das Gerät angewendet werden.

1. Navigieren Sie zu **System > Licenses > Smart Licensing (System > Lizenzen > Smart Licensing)**.



2. Stellen Sie sicher, dass die Geräte die Compliance-Anforderungen erfüllen und erfolgreich registriert wurden. Stellen Sie sicher, dass das Gerät mit einer **AnyConnect Apex-, Plus- oder VPN Only-Lizenz** registriert ist.



Smart License Status

Cisco Smart Software Manager

Usage Authorization:	✓	Authorized (Last Synchronized On May 03 2020)
Product Registration:	✓	Registered (Last Renewed On Mar 03 2020)
Assigned Virtual Account:		SEC TAC
Export-Controlled Features:		Enabled
Cisco Success Network:		Disabled ⓘ
Cisco Support Diagnostics:		Disabled ⓘ

Smart Licenses

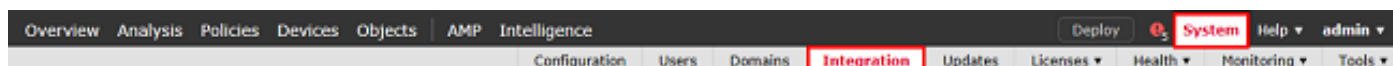
Filter Devices... Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	✓			
Base (2)	✓			
Malware (1)	✓			
Threat (2)	✓			
URL Filtering (2)	✓			
AnyConnect Apex (1)	✓			
FTD-2 192.168.1.17 - Cisco Firepower Threat Defense for VMWare - v6.3.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

Note: Container Instances of same blade share feature licenses

Setup-Bereich

1. Navigieren Sie zu **System > Integration**.



2. Klicken Sie unter **Bereiche** auf **Neuer Bereich**.



3. Füllen Sie die entsprechenden Felder basierend auf den Informationen vom Microsoft-Server gesammelt. Klicken Sie abschließend auf **OK**.

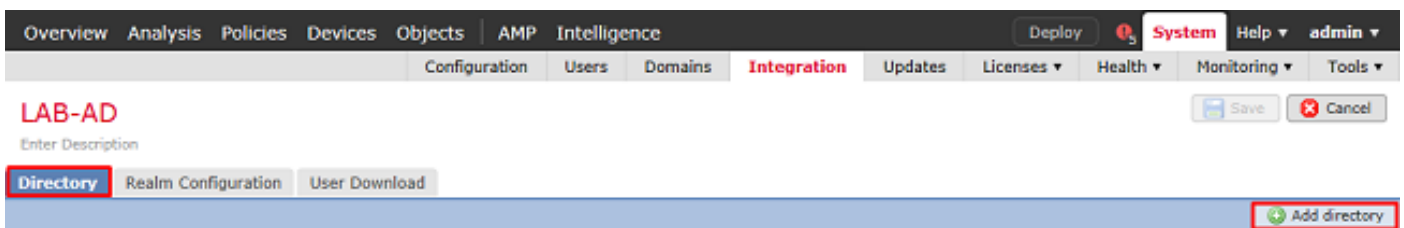
The 'Add New Realm' dialog box contains the following fields and values:

- Name: LAB-AD
- Description: (empty)
- Type: AD
- AD Primary Domain: example.com (example: domain.com)
- AD Join Username: (empty) (example: user@domain)
- AD Join Password: (empty) (Test AD Join button)
- Directory Username: ftd.admin@example.com (example: user@domain)
- Directory Password: (masked with dots)
- Base DN: DC=example,DC=com (example: ou=user,dc=cisco,dc=com)
- Group DN: DC=example,DC=com (example: ou=group,dc=cisco,dc=com)
- Group Attribute: Member

* Required Field

Buttons: OK, Cancel

4. Wählen Sie im neuen Fenster **Verzeichnis** aus, falls noch nicht ausgewählt, und klicken Sie auf **Verzeichnis hinzufügen**.



Geben Sie die Details für den AD-Server an. Beachten Sie, dass bei Verwendung des FQDN FMC und FTD nur dann eine erfolgreiche Bindung herstellen können, wenn DNS für die Auflösung des FQDN konfiguriert ist.

Um DNS für FMC einzurichten, navigieren Sie zu **System > Configuration**, und wählen Sie **Management Interfaces (Verwaltungsschnittstellen)**.

Um DNS für die FTD einzurichten, navigieren Sie zu **Devices > Platform Settings**, erstellen Sie eine neue Richtlinie, oder bearbeiten Sie eine aktuelle Richtlinie, und wechseln Sie dann zu DNS.


Add directory



Hostname / IP Address:

Port:

Encryption: STARTTLS LDAPS None

SSL Certificate: 

Wenn LDAPS oder STARTTLS verwendet wird, klicken Sie auf das Symbol Grün +, geben Sie dem Zertifikat einen Namen, und kopieren Sie das Zertifikat der Stammzertifizierungsstelle im PEM-Format. Klicken Sie abschließend auf **Speichern**.

Import Trusted Certificate Authority



Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YVw1wGUTV0lOMjAxNi1DQTCC
ASIWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVKEKSGoY+v940S2316lzdwrEMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkFA1LPuM
aob4XE/OzxYQpPa18djsNnskfCfQD/HOTFQN4+SrOhHWIRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBTcIeyC062a8BKqOL7N86HFPfKMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fj7ER9EM/HcXCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhchw8MDIoxW2dTsjenAET7r
phFIHZoCoSfjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgrEtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjBCxsTscubRI+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFQV3DgZg+R96
9WLCR30big6xyo9Zu+lixWpdrbADO6zMhbEYEHkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

Encrypted, and the password is:

Wählen Sie die neu hinzugefügte Stammzertifizierungsstelle aus dem Dropdown-Menü neben SSL-Zertifikat aus, und klicken Sie auf STARTTLS oder LDAPS.

Edit directory

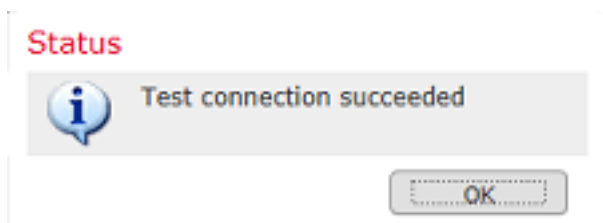


Hostname / IP Address	<input type="text" value="win2016.example.com"/>
Port	<input type="text" value="636"/>
Encryption	<input type="radio"/> STARTTLS <input checked="" type="radio"/> LDAPS <input type="radio"/> None
SSL Certificate	<input type="text" value="LDAPS_ROOT"/>

Klicken Sie auf Test, um sicherzustellen, dass FMC eine erfolgreiche Bindung mit dem im vorherigen Schritt angegebenen Benutzernamen und Kennwort für das Verzeichnis herstellen kann.

Da diese Tests vom FMC und nicht über eine der im FTD konfigurierten routingfähigen Schnittstellen (z. B. intern, extern, dmz) initiiert werden, garantiert eine erfolgreiche (oder fehlgeschlagene) Verbindung nicht dasselbe Ergebnis für die AnyConnect-Authentifizierung, da AnyConnect LDAP-Authentifizierungsanforderungen von einer der FTD-routingfähigen Schnittstellen initiiert werden.

Weitere Informationen zum Testen von LDAP-Verbindungen aus dem FTD finden Sie in den Abschnitten Test AAA und Packet Capture im Bereich Troubleshooting (Fehlerbehebung).



5. Laden Sie unter **Benutzer-Download** die Gruppen herunter, die in späteren Schritten für die Benutzeridentität verwendet werden.

Aktivieren Sie das Kontrollkästchen **Benutzer und Gruppen herunterladen**, und die Spalte für **Verfügbare Gruppen** wird mit den in Active Directory konfigurierten Gruppen ausgefüllt.

Gruppen können ein- oder ausgeschlossen werden, standardmäßig sind jedoch alle Gruppen enthalten, die unter der Gruppen-DN zu finden sind.

Bestimmte Benutzer können ebenfalls ein- oder ausgeschlossen werden. Alle enthaltenen Gruppen und Benutzer können zu einem späteren Zeitpunkt als Benutzeridentitäten ausgewählt werden.

Klicken Sie abschließend auf **Speichern**.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains **Integration** Updates Licenses Health Monitoring Tools

LAB-AD You have unsaved changes Save Cancel

Directory Realm Configuration **User Download**

Download users and groups

Begin automatic download at 8 AM America/New York Repeat Every 24 Hours

Download Now

Available Groups

Search by name

- AnyConnect Admins
- DnsUpdateProxy
- WseRemoteAccessUsers
- WseInvisibleToDashboard
- Allowed RODC Password Replication Group
- Enterprise Key Admins
- Domain Admins
- WseAlertAdministrators
- Event Log Readers
- Replicator
- Domain Guests
- Windows Authorization Access Group
- Account Operators
- Hyper-V Administrators
- System Managed Accounts Group

Groups to Include (2)

- AnyConnect Admins
- AnyConnect Users

Groups to Exclude (0)

None

Enter User Inclusion Add Enter User Exclusion Add

6. Aktivieren Sie den neuen Bereich.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains **Integration** Updates Licenses Health Monitoring Tools

Cloud Services **Realms** Identity Sources eStreamer Host Input Client Smart Software Satellite Compare realms New realm

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
LAB-AD		Global	AD	DC=example,DC=com	DC=example,DC=com	member	<input checked="" type="checkbox"/>

7. Wenn LDAPS oder STARTTLS verwendet wird, muss die Stammzertifizierungsstelle auch von der FTD als vertrauenswürdig eingestuft werden. Navigieren Sie dazu zunächst zu **Geräte > Zertifikate**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Klicken Sie oben rechts auf Hinzufügen.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin


Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates** Add

Wählen Sie das FTD aus. Die LDAP-Konfiguration wird hinzugefügt, und klicken Sie dann auf das grüne + Symbol.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*: 

Geben Sie dem Vertrauenspunkt einen **Namen**, und wählen Sie dann im Dropdown-Menü **Anmeldetyp** die Option **Manuelle** Anmeldung aus. Fügen Sie hier das PEM-Stammzertifikat ein, und klicken Sie dann auf **Speichern**.

Add Cert Enrollment

Name*

Description

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type:

CA Certificate:*

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki
G9w0BAQsFADAd
MRswGQYDVQQDEExJeGFtcGxlVdJTjIwMTYtQ0EwEwIBcNMjAwNDI
3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGU
tV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N
zSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBf
d++M+bLn3AiZnHV
OO+k6dVVY/E5qVKEKSGoY+v940S2316lzdwrReMOFhgbc2qMertIo
ficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN
O7KEMkfa1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBU
aLdQaabhipD/
sVs5PneYJX8YKma821uYI6i90YuytmsHBTcIeyC062a8BKqOL7N86
-----
```

Allow Overrides

Vergewissern Sie sich, dass der erstellte Vertrauenspunkt ausgewählt ist, und klicken Sie dann auf **Hinzufügen**.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: LDAPS_ROOT
 Enrollment Type: Manual
 SCEP URL: NA

Der neue Vertrauenspunkt erscheint unter der FTD. Obwohl erwähnt wird, dass ein Import von Identitätszertifikaten erforderlich ist, ist es für die FTD nicht erforderlich, das vom LDAPS-Server gesendete SSL-Zertifikat zu authentifizieren, sodass diese Nachricht ignoriert werden kann.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

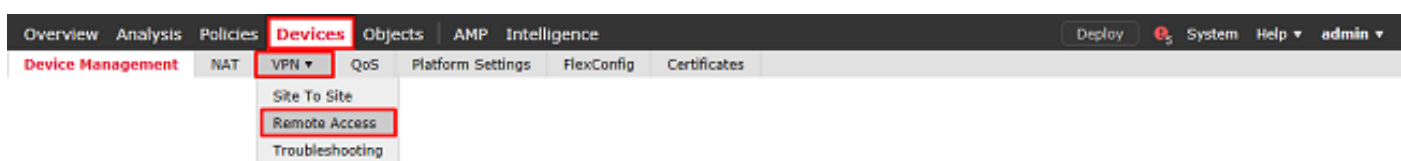
Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates** Add

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID
FTD-2			
FTD-2-PKCS12	Global	PKCS12 file	CA ID
FTD-2-Selfsigned	Global	Self-Signed	CA ID
LDAPS_ROOT	Global	Manual	CA ID Identity certificate import required

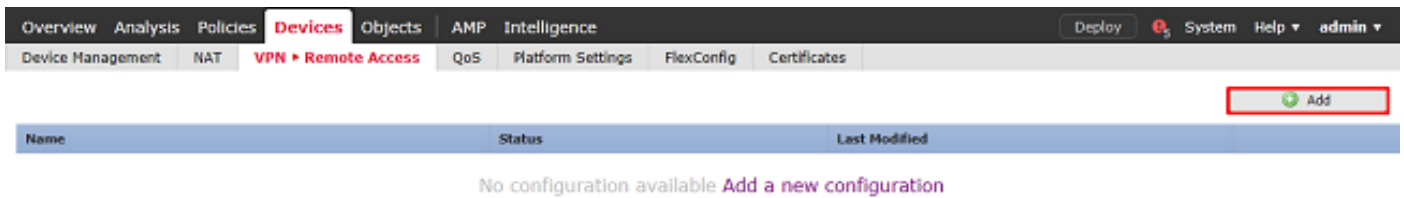
Konfigurieren von AnyConnect für die AD-Authentifizierung

1. Bei diesen Schritten wird davon ausgegangen, dass noch keine VPN-Richtlinie für den Remote-Zugriff erstellt wurde. Wenn eine solche erstellt wurde, klicken Sie auf die Schaltfläche zum Bearbeiten für diese Richtlinie, und fahren Sie mit Schritt 3 fort.

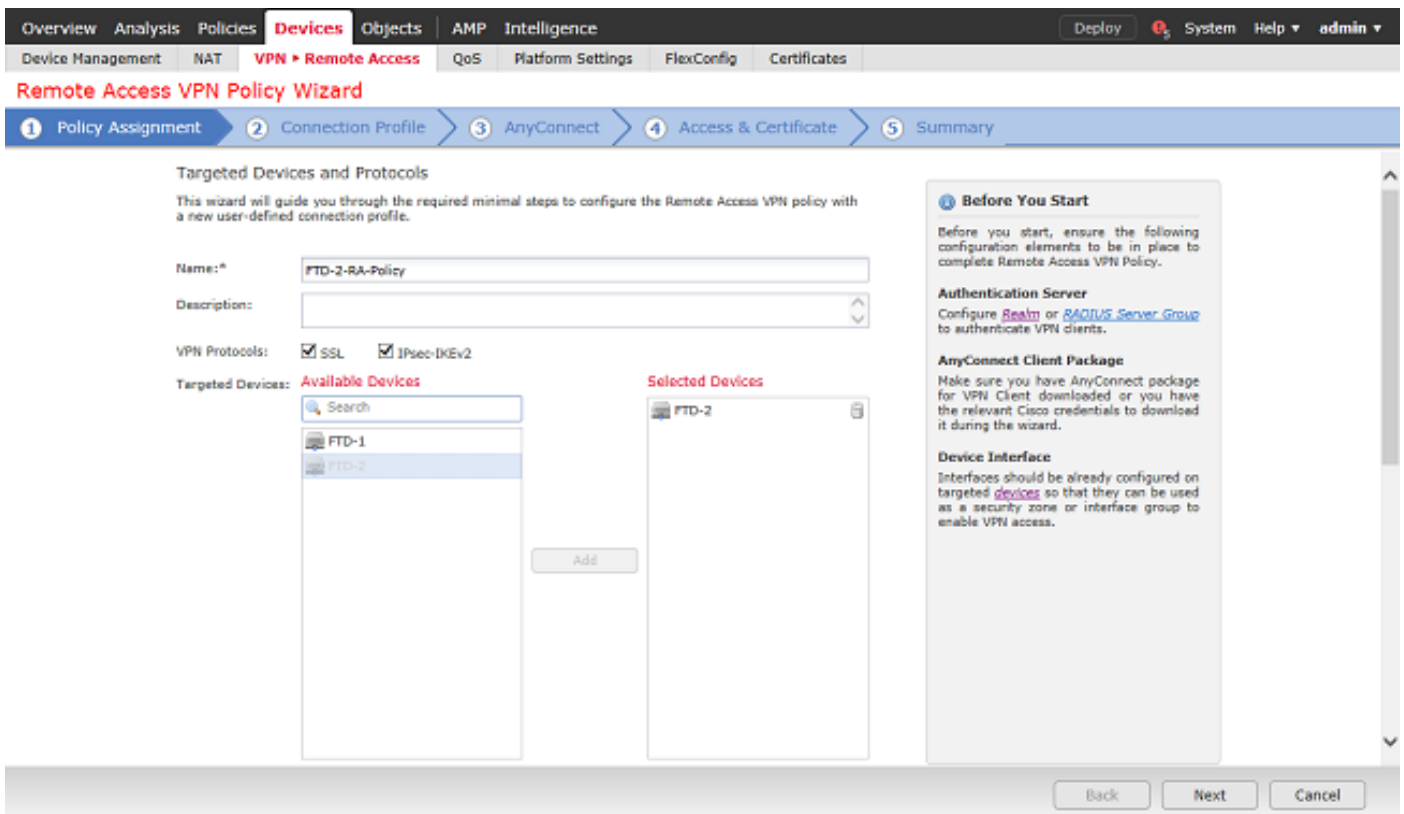
Navigieren Sie zu **Geräte > VPN > Remotezugriff**.



Klicken Sie auf **Hinzufügen**, um eine neue VPN-Richtlinie für den Remote-Zugriff zu erstellen.



2. Schließen Sie den **Assistenten für VPN-Richtlinien für den Remotezugriff ab**. Geben Sie unter **Richtlinienzuweisung** einen Namen für die Richtlinie und die Geräte an, auf die die Richtlinie angewendet wird.



Geben Sie unter **Verbindungsprofil** den Namen des **Verbindungsprofils** an, das auch als Gruppenalias verwendet wird, den AnyConnect-Benutzer sehen, wenn sie eine Verbindung herstellen.

Geben Sie den Bereich an, der zuvor unter **Authentifizierungsserver** erstellt wurde.

Methode angeben AnyConnect-Clients werden IP-Adressen zugewiesen.

Geben Sie die Standardgruppenrichtlinie an, die für dieses Verbindungsprofil verwendet wird.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 **Connection Profile** 3 AnyConnect 4 Access & Certificate 5 Summary

Connection Profile:
 Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name: *
This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):
 Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:
 Authentication Server: * (Realm or RADIUS)
 Authorization Server: (RADIUS)
 Accounting Server: (RADIUS)

Client Address Assignment:
 Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only) ⓘ
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools:
 IPv6 Address Pools:

Group Policy:
 A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy: * [Edit Group Policy](#)

Back Next Cancel

Laden Sie unter AnyConnect die verwendeten AnyConnect-Pakete hoch, und geben Sie sie an.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

AnyConnect Client Image
 The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from Cisco Software Download Center.

Show Re-order buttons

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	anyconnect-linux64-4.7.03052-we...	anyconnect-linux64-4.7.03052-webdeploy-k9...	Linux
<input checked="" type="checkbox"/>	anyconnect-win-4.7.001136-webde...	anyconnect-win-4.7.001136-webdeploy-k9.pkg	Windows

Back Next Cancel

Geben Sie unter **Access & Certificate** (Zugriff und Zertifikat) die Schnittstelle an, auf die AnyConnect-Benutzer für AnyConnect zugreifen.

Erstellen und/oder spezifizieren Sie das Zertifikat, das vom FTD während des SSL-Handshakes verwendet wird.

Stellen Sie sicher, dass das Kontrollkästchen für die **Richtlinie zur Umgehung der Zugriffskontrolle** für entschlüsselten Datenverkehr (sysopt permit-vpn) nicht aktiviert ist, sodass die später erstellte Benutzeridentität für RAVPN-Verbindungen übernommen wird.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Network Interface for Incoming VPN Access
 Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:

Enable DTLS on member interfaces

Device Certificates
 Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:

Enroll the selected certificate object on the target devices

Access Control for VPN Traffic
 All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Back Next Cancel

Überprüfen Sie unter **Übersicht** die Konfiguration, und klicken Sie auf **Fertig stellen**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: FTD-2-RA-Policy

Device Targets: FTD-2

Connection Profile: General

Connection Alias: General

AAA:

- Authentication Method: AAA Only
- Authentication Server: LAB-AD
- Authorization Server: -
- Accounting Server: -

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): AnyConnect-Pool
- Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images:

- anyconnect-linux64-4.7.03052-webdeploy-k9.pkg
- anyconnect-win-4.7.00136-webdeploy-k9.pkg

Interface Objects: outside-zone

Device Certificates: FTD-2-Selfsigned

Device Identity Certificate Enrollment

Certificate enrollment object 'FTD-2-Selfsigned' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.

Network Interface Configuration
 Make sure to add interface from targeted devices to SecurityZone object 'outside-zone'

Back Finish Cancel

3. Klicken Sie unter der VPN-Richtlinie für den Remotezugriff auf **Bearbeiten**, um das entsprechende **Verbindungsprofil** anzuzeigen.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

FTD-2-RA-Policy Save Cancel

Enter Description Policy Assignments (1)

Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy
DefaultWEB/VPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
General	Authentication: LAB-AD (AD) Authorization: None Accounting: None	DfltGrpPolicy

Stellen Sie sicher, dass der Authentifizierungsserver auf den zuvor erstellten Bereich festgelegt ist.

Unter **Erweiterte Einstellungen** kann **Kennwortverwaltung aktivieren** aktiviert werden, damit Benutzer ihr Kennwort ändern können, wenn oder bevor das Kennwort abläuft.

Diese Einstellung erfordert jedoch, dass der Bereich LDAPS verwendet. Wenn Änderungen vorgenommen wurden, klicken Sie auf **Speichern**.

Edit Connection Profile ? X

Connection Profile:* General

Group Policy:* DfltGrpPolicy [Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: LAB-AD (AD)

Use secondary authentication

Authorization

Authorization Server:

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

Advanced Settings

Strip Realm from username

Strip Group from username

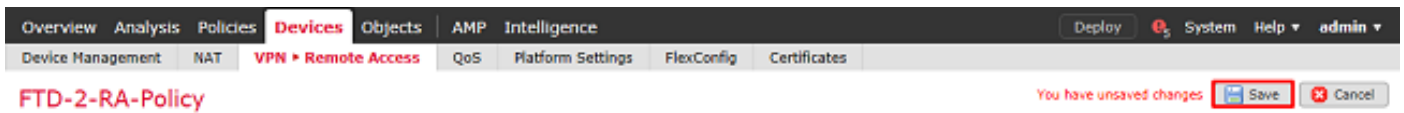
Enable Password Management

Notify User 14 days prior to password expiration

Notify user on the day of password expiration

Save Cancel

Klicken Sie abschließend oben rechts auf **Speichern**.



Identitätsrichtlinie aktivieren und Sicherheitsrichtlinien für Benutzeridentität konfigurieren

1. Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Identität**.

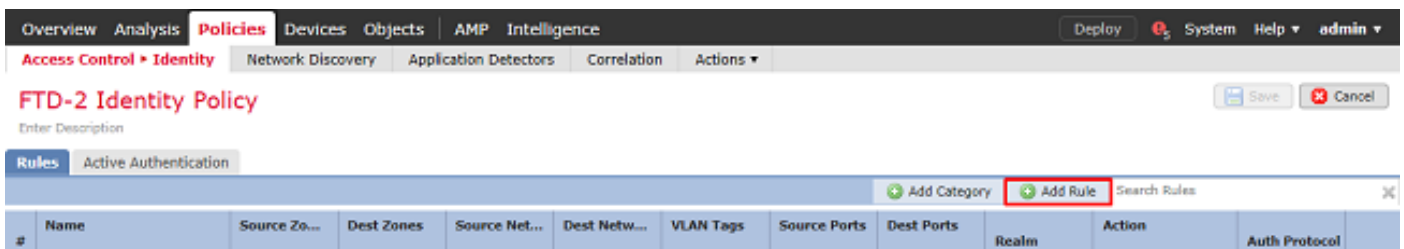


Erstellen einer neuen Identitätsrichtlinie



Geben Sie einen **Namen** für die neue **Identitätsrichtlinie** an.

2. Klicken Sie auf **Regel hinzufügen**.



3. Geben Sie einen **Namen** für die neue Regel an. Stellen Sie sicher, dass sie aktiviert ist und dass Aktion auf **Passive Authentifizierung** festgelegt ist.

Klicken Sie auf die Registerkarte **Bereich und Einstellungen**, und wählen Sie den zuvor erstellten Bereich aus. Klicken Sie abschließend auf **Hinzufügen**.

Add Rule

Name: Enabled

Insert: into Category

Action: Realm: LAB-AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Remote access VPN sessions are actively authenticated by VPN. Other sessions use the rule Action.

Zones Networks VLAN Tags Ports **Realm & Settings**

Realm *

Use active authentication if passive or VPN identity cannot be established

* Required Field

4. Klicken Sie auf Speichern.

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control > Identity Network Discovery Application Detectors Correlation Actions

FTD-2 Identity Policy You have unsaved changes

Rules Active Authentication

#	Name	Source Zo...	Dest Zones	Source Net...	Dest Netw...	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules This category is empty											
Standard Rules											
1	RAVPN	any	any	any	any	any	any	any	LAB-AD	Passive Authentication	none
Root Rules This category is empty											

Displaying 1 - 1 of 1 rules Page 1 of 1

5. navigieren Sie zu Richtlinien > Zugriffskontrolle > Zugriffskontrolle.

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control > Identity Network Discovery Application Detectors Correlation Actions

Access Control

- Intrusion
- Malware & File
- DNS
- Identity**
- SSL
- Prefilter

6. Bearbeiten Sie die Zugriffskontrollrichtlinie, unter der das FTD konfiguriert ist.

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control > Access Control Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Import/Export

Access Control Policy	Status	Last Modified
Default-Policy	Targeting 1 devices Up-to-date on all targeted devices	2020-05-04 09:15:56 Modified by "admin"

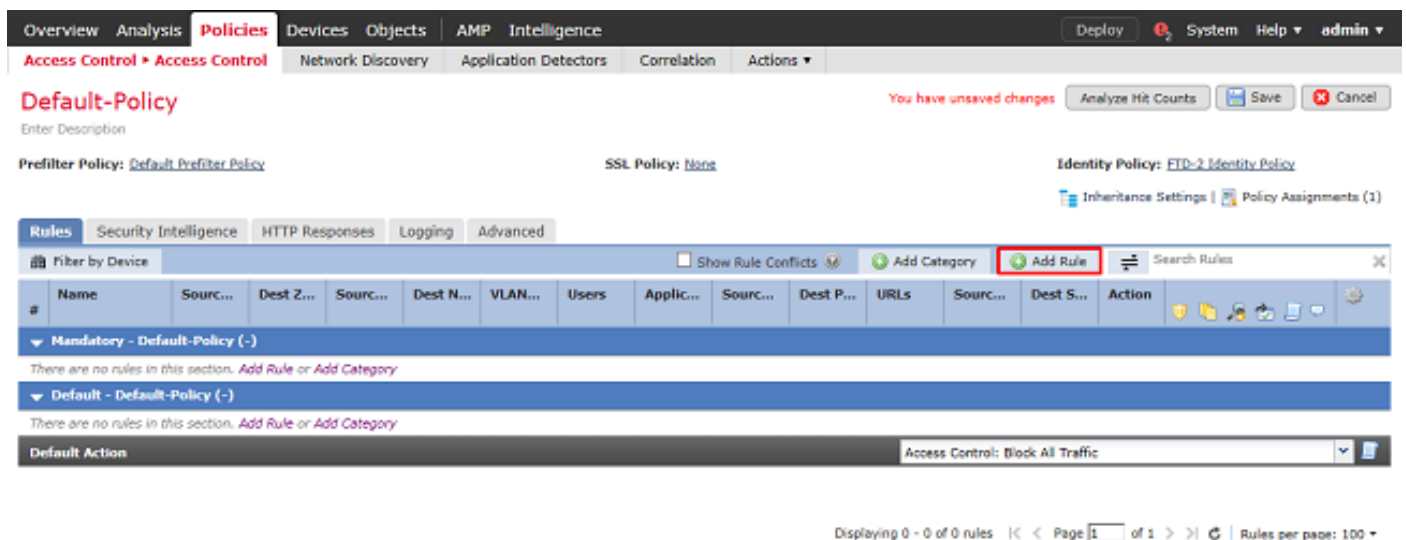
7. Klicken Sie auf den Wert neben **Identitätsrichtlinie**.



Wählen Sie die zuvor erstellte **Identitätsrichtlinie aus**, und klicken Sie dann auf **OK**.



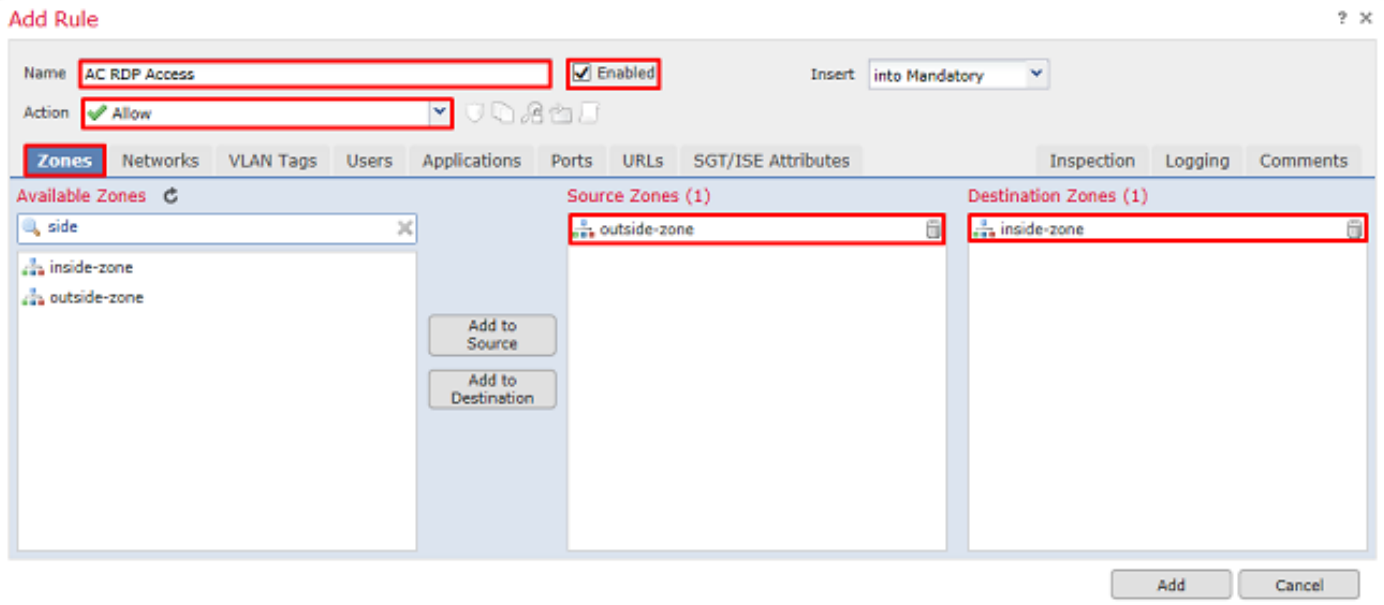
8. Klicken Sie auf **Regel hinzufügen**, um eine neue AKP-Regel zu erstellen. Mit diesen Schritten wird eine Regel erstellt, die es Benutzern in der Gruppe der AnyConnect-Administratoren ermöglicht, mithilfe von RDP eine Verbindung zu Geräten im Netzwerk herzustellen.



Geben Sie einen Namen für die Regel an. Stellen Sie sicher, dass die Regel aktiviert ist und über die entsprechende Aktion verfügt.

Geben Sie auf der Registerkarte **Zonen** die entsprechenden Zonen für den interessanten Datenverkehr an.

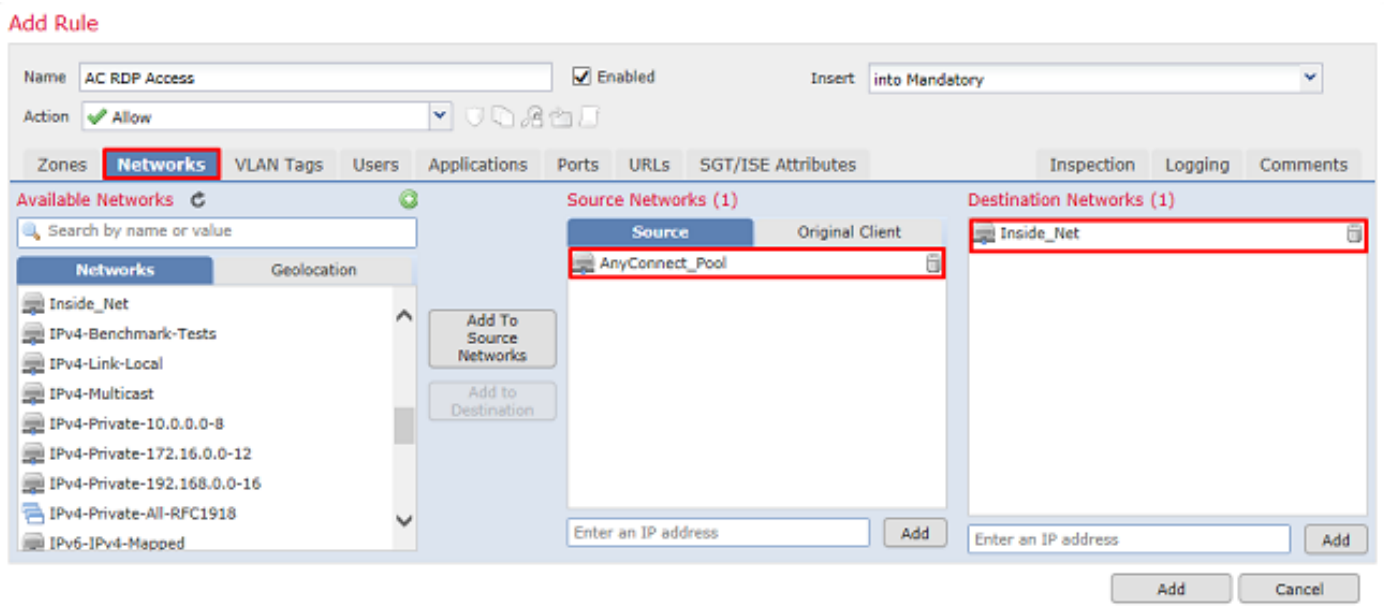
Von Benutzern initiiertes RDP-Datenverkehr gelangt über die Schnittstelle der Außenzone in den FTD und gelangt in die Innenzone.



Definieren Sie unter **Netzwerke** die Quell- und Zielnetzwerke.

Das Objekt AnyConnect_Pool enthält die IP-Adressen, die AnyConnect-Clients zugewiesen sind.

Objekt Inside_Net enthält das interne Netzwerk-Subnetz.



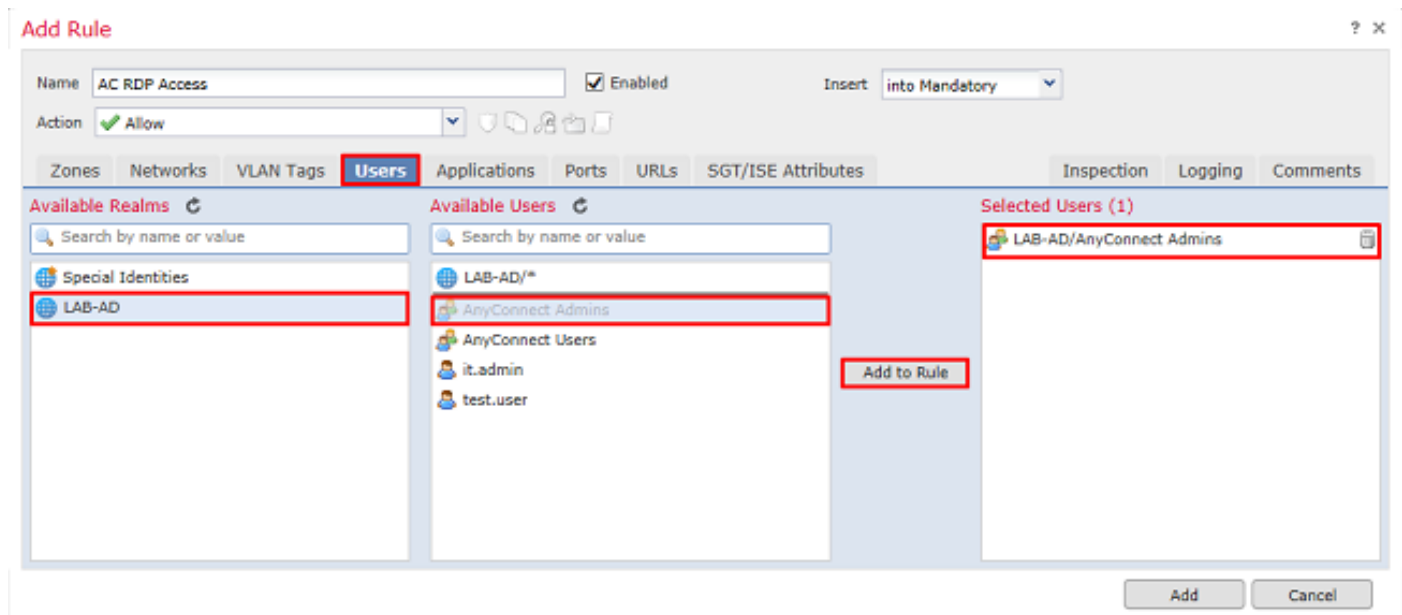
Klicken Sie unter **Benutzer** auf den Bereich, der zuvor unter **Verfügbare Bereiche** erstellt wurde, klicken Sie unter **Verfügbare Benutzer** auf die entsprechende Gruppe bzw. den entsprechenden Benutzer, und klicken Sie dann auf **Zur Regel hinzufügen**.

Wenn keine Benutzer oder Gruppen im Abschnitt **Verfügbare Benutzer** verfügbar sind, stellen Sie sicher, dass FMC die **Benutzer** und **Gruppen** im Abschnitt Bereich heruntergeladen konnte und dass die entsprechenden **Gruppen/Benutzer** enthalten sind.

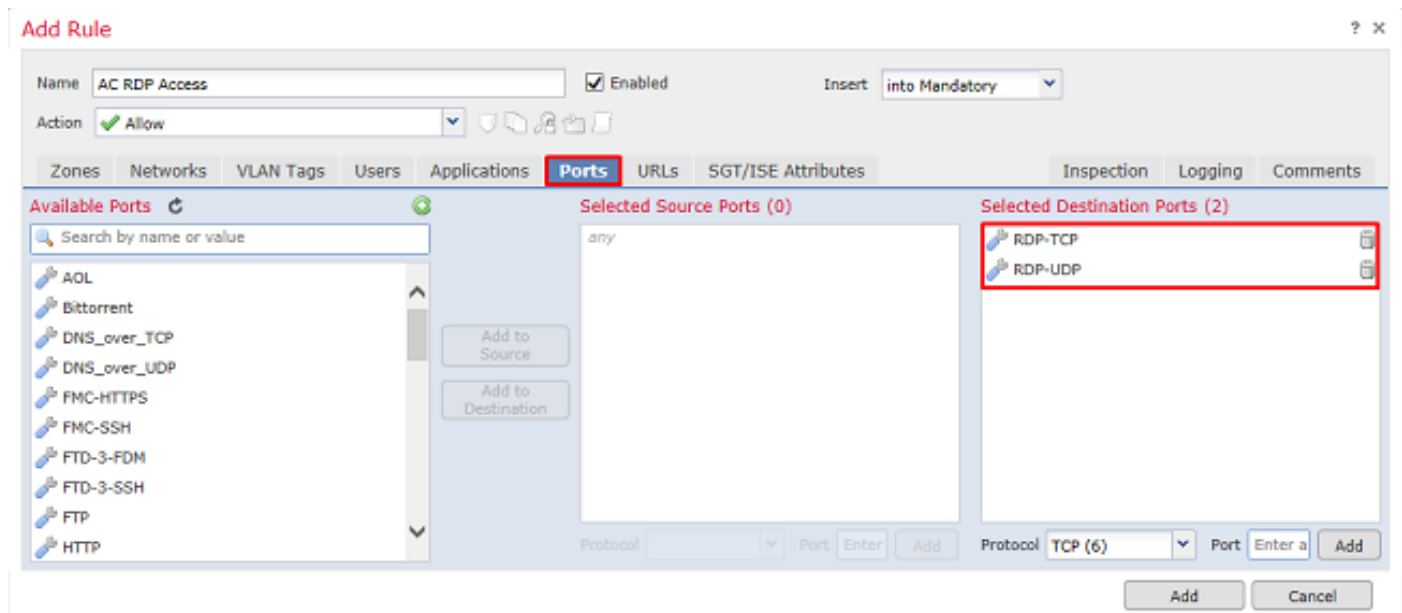
Die hier angegebenen **Benutzer/Gruppen** werden aus der Quellperspektive überprüft.

So bewertet die FTD anhand der bisher in dieser Regel definierten Kriterien, dass der Datenverkehr von der Außenzone zur Innenzone, vom Netzwerk im AnyConnect_Pools-Objekt und vom Netzwerk im Inside_Net-Objekt stammt und von einem Benutzer in der Gruppe

AnyConnect-Administratoren stammt.



Unter "Ports" wurden benutzerdefinierte RDP-Objekte erstellt und hinzugefügt, um den TCP- und UDP-Port 3389 zuzulassen. Beachten Sie, dass RDP im Abschnitt "**Anwendungen**" hätte hinzugefügt werden können, aber aus Gründen der Einfachheit werden nur die Ports überprüft.



Schließlich wird unter **Protokollierung** das **Protokoll am Ende der Verbindung** zu einem späteren Zeitpunkt auf zusätzliche Verifizierung hin überprüft. Klicken Sie abschließend auf **Hinzufügen**.

Add Rule ? x

Name: Enabled Insert:

Action:

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection **Logging** Comments

Log at Beginning of Connection
 Log at End of Connection

File Events:
 Log Files

Send Connection Events to:
 Event Viewer
 Syslog Server (Using default syslog configuration in Access Control Logging) [Show Overrides](#)
 SNMP Trap

9. Es wird eine zusätzliche Regel für den HTTP-Zugriff erstellt, um Benutzern innerhalb der Gruppe **AnyConnect-Benutzer** den Zugriff auf die **Windows Server IIS-Website** zu ermöglichen. Klicken Sie auf **Speichern**.

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control **Access Control** Network Discovery Application Detectors Correlation Actions

Default-Policy You have unsaved changes

Enter Description

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [FTD-2 Identity Policy](#)

Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Show Rule Conflicts

#	Name	Source Zo...	Dest Zones	Source Networks	Dest Netwo...	V...	Users	A...	S...	Dest Ports	U...	S...	D...	Action
Mandatory - Default-Policy (1-2)														
1	AC RDP Access	outside-zone	inside-zone	AnyConnect_Pool	Inside_Net	Any	LAB-AD/AnyConnect Admins	Any	Any	RDP-TCP RDP-UDP	Any	Any	Any	Allow
2	AC HTTP Access	outside-zone	inside-zone	AnyConnect_Pool	Inside_Net	Any	LAB-AD/AnyConnect Users	Any	Any	HTTP	Any	Any	Any	Allow
Default - Default-Policy (-)														
There are no rules in this section. Add Rule or Add Category														

Default Action:

Displaying 1 - 2 of 2 rules | Page 1 of 1 | Rules per page: 100

NAT-Ausnahme konfigurieren

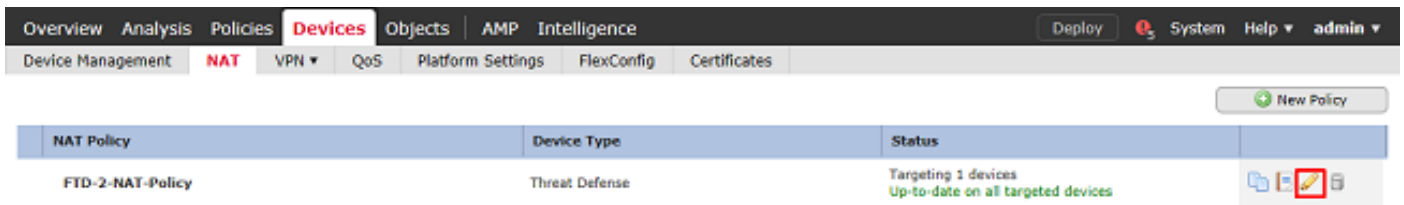
Wenn es NAT-Regeln gibt, die sich auf den AnyConnect-Datenverkehr auswirken, z. B. Internet-PAT-Regeln, ist es wichtig, NAT-Freistellungsregeln zu konfigurieren, damit der AnyConnect-Datenverkehr nicht durch die NAT beeinträchtigt wird.

1. Navigieren Sie zu **Geräte > NAT**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

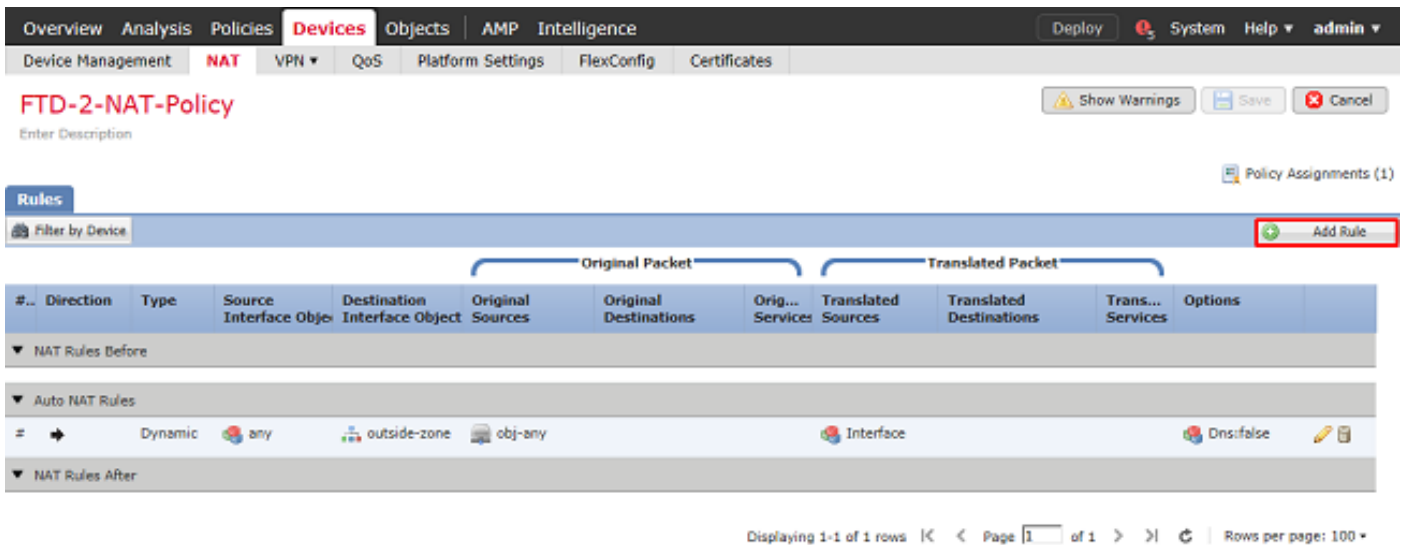
Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

Wählen Sie die auf den FTD angewendete NAT-Richtlinie aus.



2. In dieser NAT-Richtlinie gibt es eine dynamische PAT am Ende, die den gesamten Datenverkehr (einschließlich AnyConnect-Datenverkehr) betrifft, der von der externen Schnittstelle zur externen Schnittstelle abgeht.

Um zu verhindern, dass AnyConnect-Datenverkehr von NAT beeinflusst wird, klicken Sie oben rechts auf **Add Rule (Regel hinzufügen)**.



3. Konfigurieren Sie eine NAT-Ausnahmeregel. Stellen Sie sicher, dass es sich bei der Regel um eine manuelle NAT-Regel mit dem Typ "Statisch" handelt. Dies ist eine bidirektionale NAT-Regel, die auf AnyConnect-Datenverkehr angewendet wird.

Wenn die FTD anhand dieser Einstellungen Datenverkehr erkennt, der von Inside_Net stammt und an eine AnyConnect-IP-Adresse gerichtet ist (definiert durch AnyConnect_Pool), wird die Quelle in denselben Wert (Inside_Net) und das Ziel in denselben Wert (AnyConnect_Pool) umgewandelt, wenn der Datenverkehr in die Inside_Zone eintritt und aus der Outside_Zone austritt. Dadurch wird NAT im Wesentlichen umgangen, wenn diese Bedingungen erfüllt sind.

Add NAT Rule ? x

NAT Rule: **Manual NAT Rule** Insert: In Category NAT Rules Before

Type: **Static** Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

Source Interface Objects (1) **inside-zone**

Destination Interface Objects (1) **outside-zone**

OK Cancel

Add NAT Rule ? x

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* **Inside_Net**

Original Destination: Address

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address **Inside_Net**

Translated Destination: **AnyConnect_Pool**

Translated Source Port:

Translated Destination Port:

OK Cancel

Darüber hinaus ist die FTD so konfiguriert, dass sie eine Routensuche für diesen Datenverkehr und nicht für Proxy-ARP durchführt. Klicken Sie abschließend auf **OK**.

Add NAT Rule ? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

4. Klicken Sie auf **Speichern**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

FTD-2-NAT-Policy You have unsaved changes Show Warnings

Enter Description Policy Assignments (1)

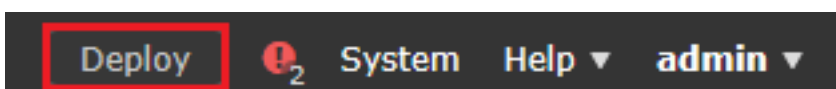
Rules Filter by Device Add Rule

#	Direction	Type	Original Packet		Translated Packet		Orig... Services	Translated Sources	Translated Destinations	Trans... Services	Options
			Source Interface Object	Destination Interface Object	Original Sources	Original Destinations					
▼ NAT Rules Before											
1	↔	Static	inside-zone	outside-zone	Inside_Net	AnyConnect_Pool		Inside_Net	AnyConnect_Pool		Dns:false route-lookup no-proxy-arp
▼ Auto NAT Rules											
=	→	Dynamic	any	outside-zone	obj-any			Interface			Dns:false
▼ NAT Rules After											

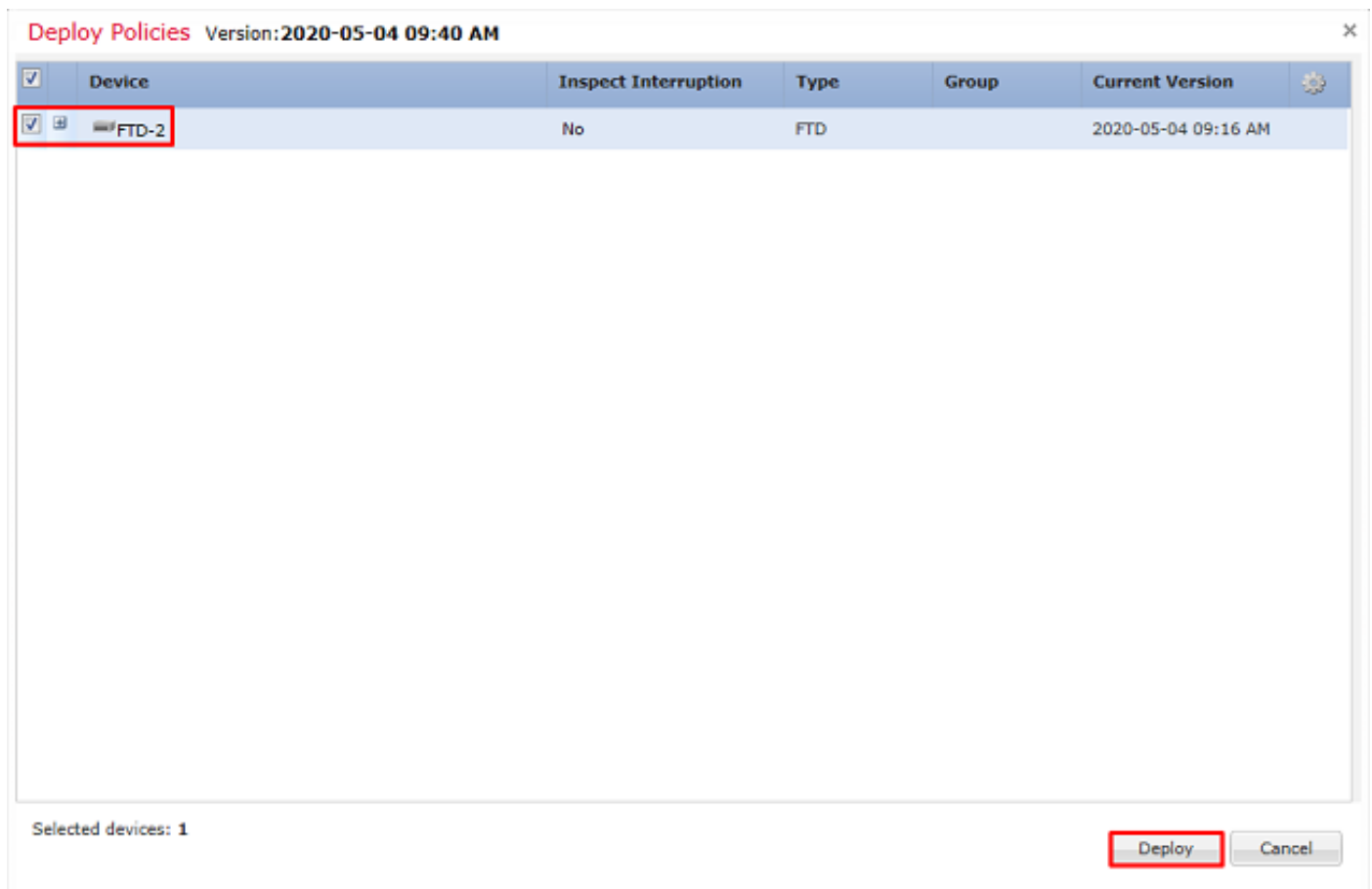
Displaying 1-2 of 2 rows Page 1 of 1 Rows per page: 100

Bereitstellen

1. Wenn die Konfiguration abgeschlossen ist, klicken Sie oben rechts auf die Schaltfläche **Bereitstellen**.



2. Aktivieren Sie das Kontrollkästchen neben dem FTD, auf das die Konfiguration angewendet wird, und klicken Sie dann auf **Bereitstellen**.



Überprüfung

Abschließende Konfiguration

AAA-Konfiguration

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
  max-failed-attempts 4
  realm-id 5
aaa-server LAB-AD host win2016.example.com
  server-port 389
  ldap-base-dn DC=example,DC=com
  ldap-group-base-dn DC=example,DC=com
  ldap-scope subtree
  ldap-naming-attribute samaccountname
  ldap-login-password *****
  ldap-login-dn ftd.admin@example.com
  server-type microsoft
```

AnyConnect-Konfiguration

```
> show running-config webvpn
webvpn
  enable Outside
  anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
  anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
  anyconnect profiles Lab disk0:/csm/lab.xml
```

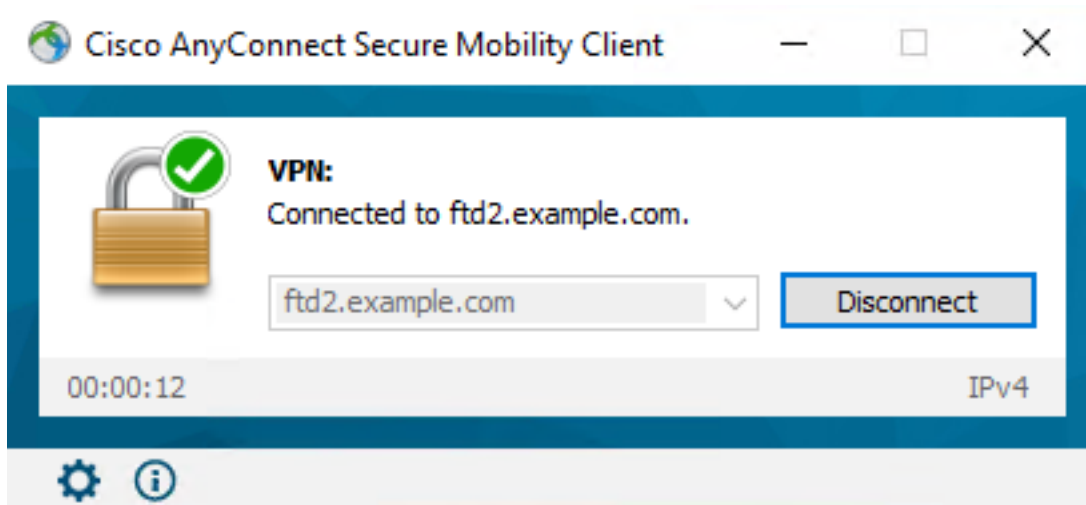
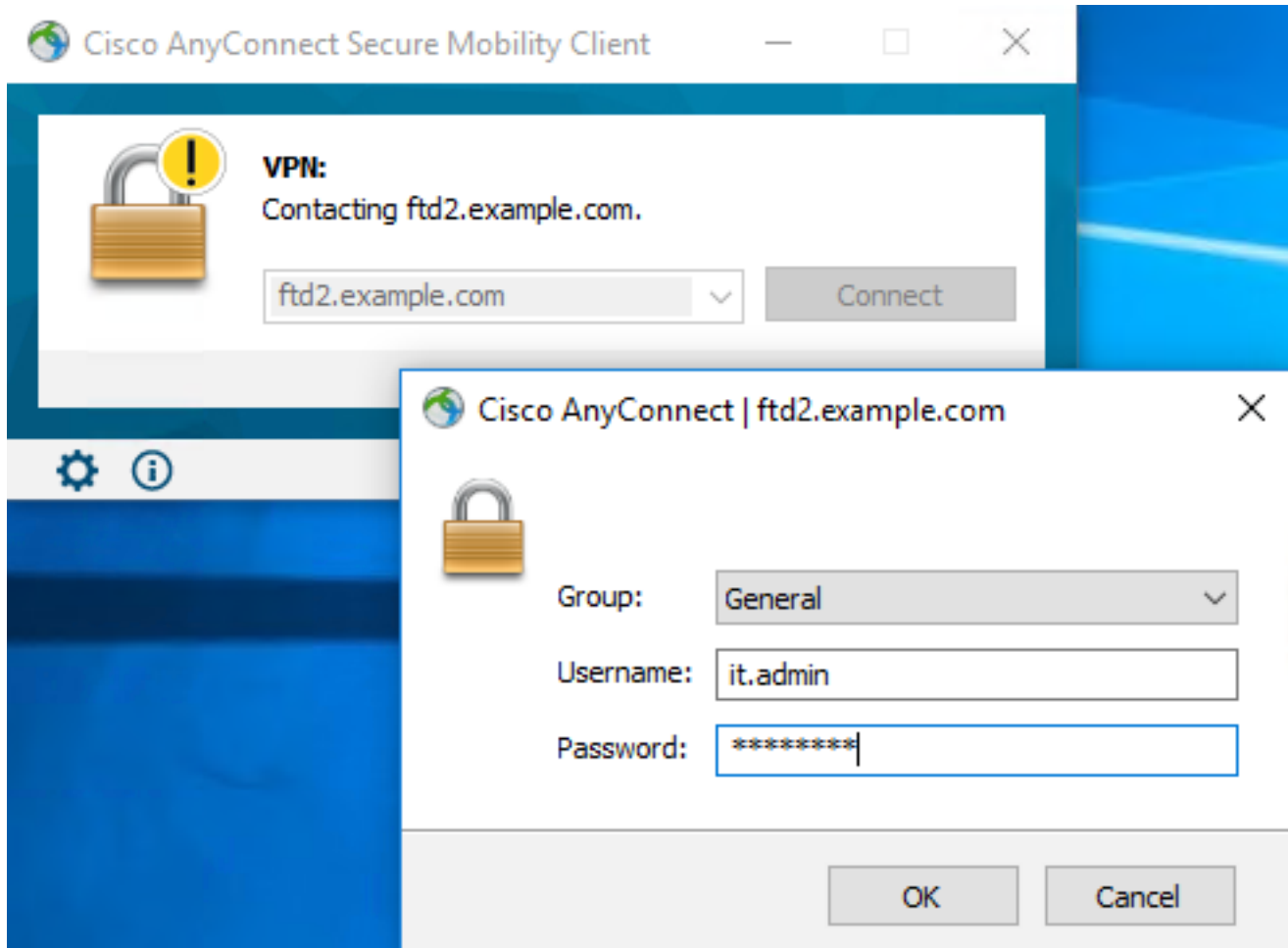
```
anyconnect enable
tunnel-group-list enable
cache
  no disable
error-recovery disable

> 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-simultaneous-logins 10
  vpn-tunnel-protocol ikev2 ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value Lab
  user-authentication-idle-timeout none
webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
  deny-message none
  anyconnect ssl df-bit-ignore enable

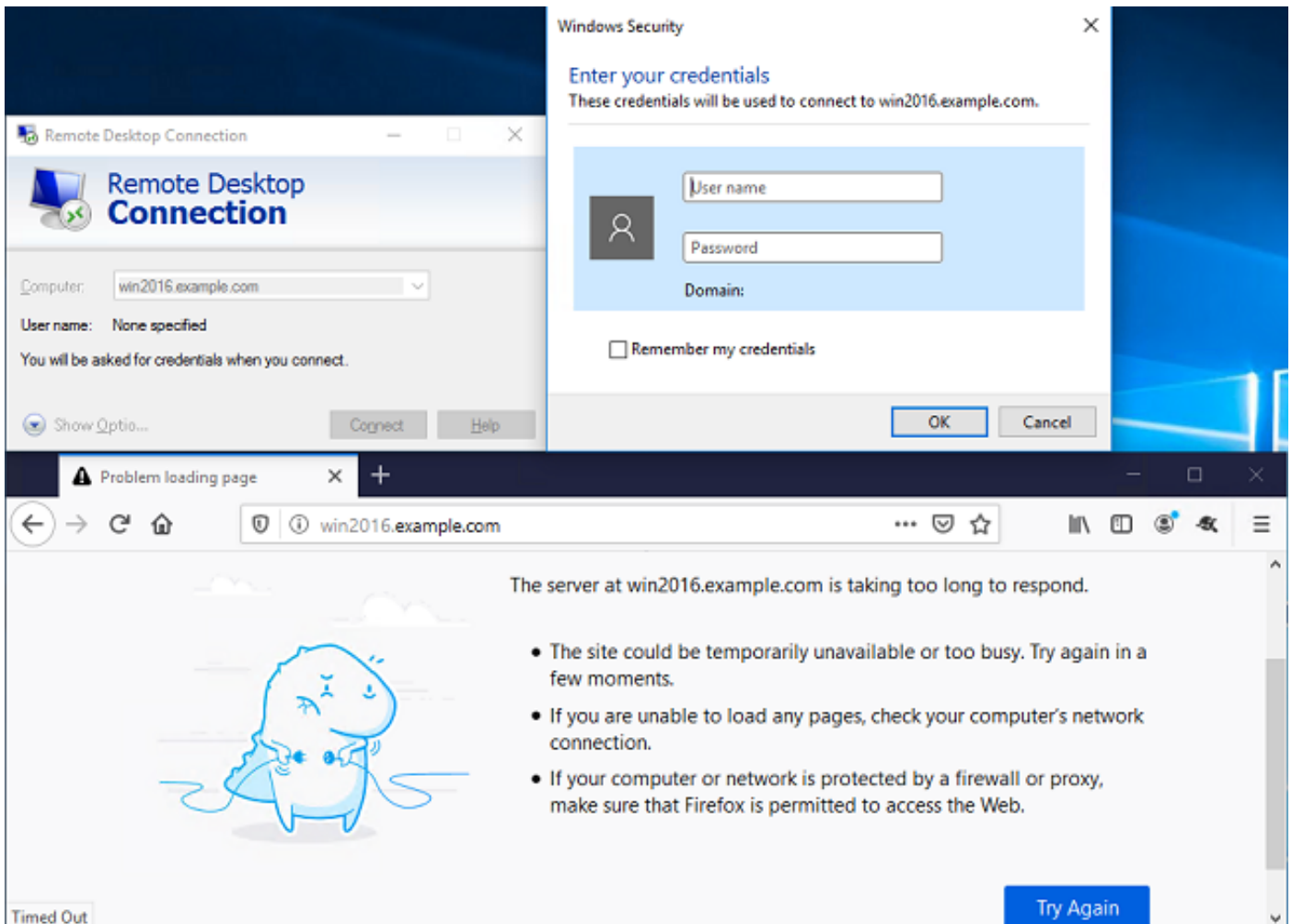
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

AnyConnect verwenden und Richtlinien für die Zugriffskontrolle überprüfen

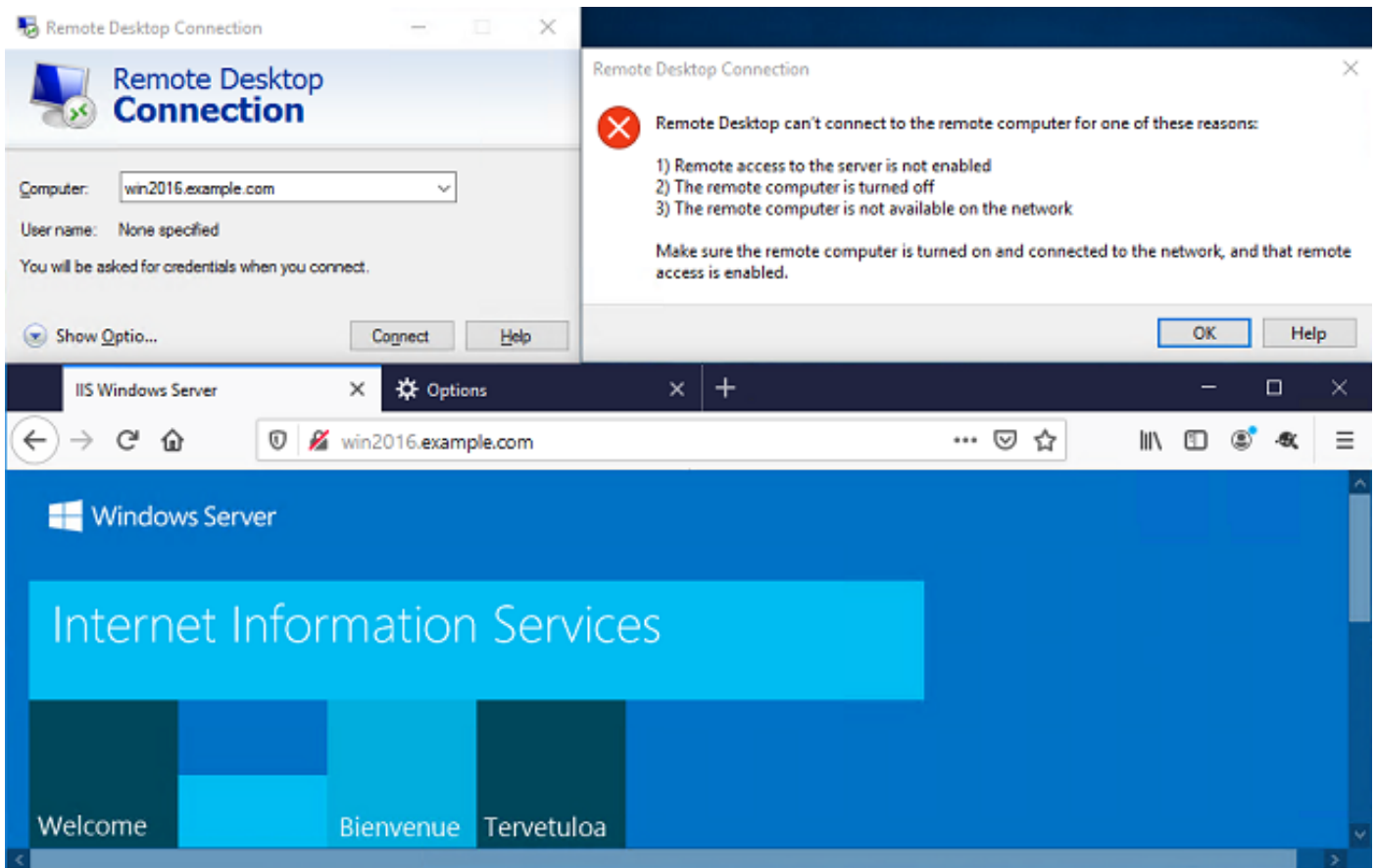


Der Benutzer IT-Administrator gehört zur Gruppe AnyConnect-Administratoren, die über RDP-Zugriff auf den Windows-Server verfügen, jedoch nicht auf HTTP zugreifen können.

Durch das Öffnen einer RDP- und Firefox-Sitzung mit diesem Server wird sichergestellt, dass dieser Benutzer nur über RDP auf den Server zugreifen kann.



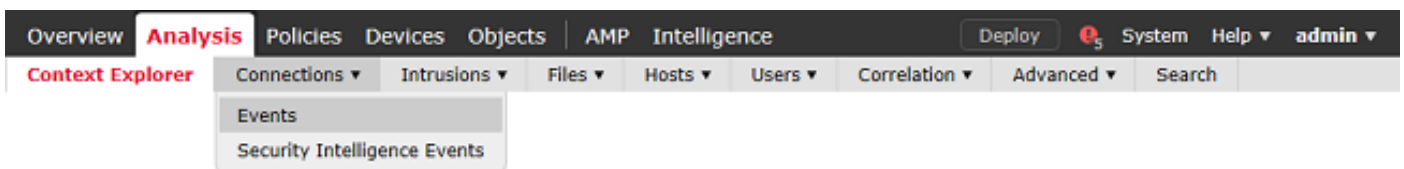
Wenn der Benutzer Testbenutzer in der Gruppe AnyConnect-Benutzer angemeldet ist, die zwar HTTP-, aber keinen RDP-Zugriff haben, können wir überprüfen, ob die Regeln für die Zugriffskontrollrichtlinie wirksam werden.



Mit FMC-Verbindungsereignissen überprüfen

Da die Protokollierung in den Regeln der Zugriffskontrollrichtlinie aktiviert wurde, können die Verbindungsereignisse auf jeden Datenverkehr überprüft werden, der diesen Regeln entspricht

Navigieren Sie zu **Analyse > Verbindungen > Ereignisse**.



In der **Tabellenansicht der Verbindungsereignisse** werden die Protokolle so gefiltert, dass nur Verbindungsereignisse für den IT-Administrator angezeigt werden.

Hier können Sie überprüfen, ob RDP-Datenverkehr zum Server (TCP und UDP 3389) zulässig ist, der Datenverkehr an Port 80 jedoch blockiert wird.

Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
Allow	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62473 / tcp	3389 / tcp
Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62474 / tcp	80 (http) / tcp
Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62475 / tcp	80 (http) / tcp
Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62476 / tcp	80 (http) / tcp

Für den Benutzer **Test User** können Sie überprüfen, ob der RDP-Datenverkehr zum Server blockiert und der Datenverkehr an Port 80 zulässig ist.

Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
Block	10.10.10.1	test_user (LAB-AD\test.user, LDAP)	192.168.1.1	outside-zone	inside-zone	62493 / tcp	3389 / tcp
Allow	10.10.10.1	test_user (LAB-AD\test.user, LDAP)	192.168.1.1	outside-zone	inside-zone	62494 / tcp	80 (http) / tcp

Fehlerbehebung

Fehlerbehebung

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

Um Probleme mit den Richtlinien für die Benutzeridentitätssteuerung zu beheben, kann der **Systemsupport "firewall-engine-debug"** in clish ausgeführt werden, um zu bestimmen, warum der Datenverkehr unerwartet zugelassen oder blockiert wird.

LDAP-Debugger

```
[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...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 zum 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:

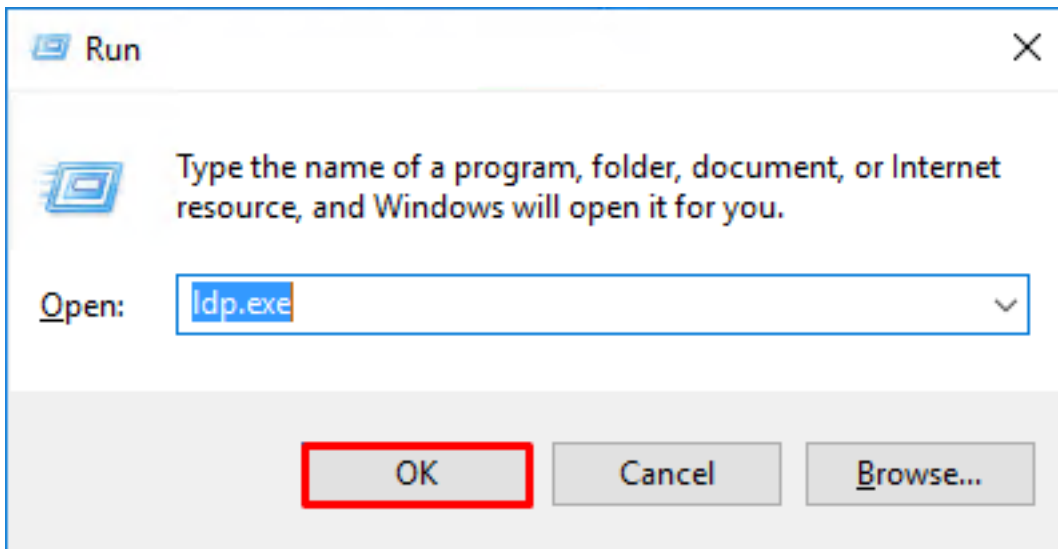
- Überprüfen Sie die Weiterleitung, und stellen Sie sicher, dass die FTD eine Antwort vom LDAP-Server erhält.
- Wenn LDAPS oder STARTTLS verwendet wird, stellen Sie sicher, dass das richtige Stammzertifikat der Zertifizierungsstelle vertrauenswürdig ist, damit der SSL-Handshake erfolgreich abgeschlossen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

Ungültiger Bindungs-Anmelde-DN und/oder falsches Kennwort

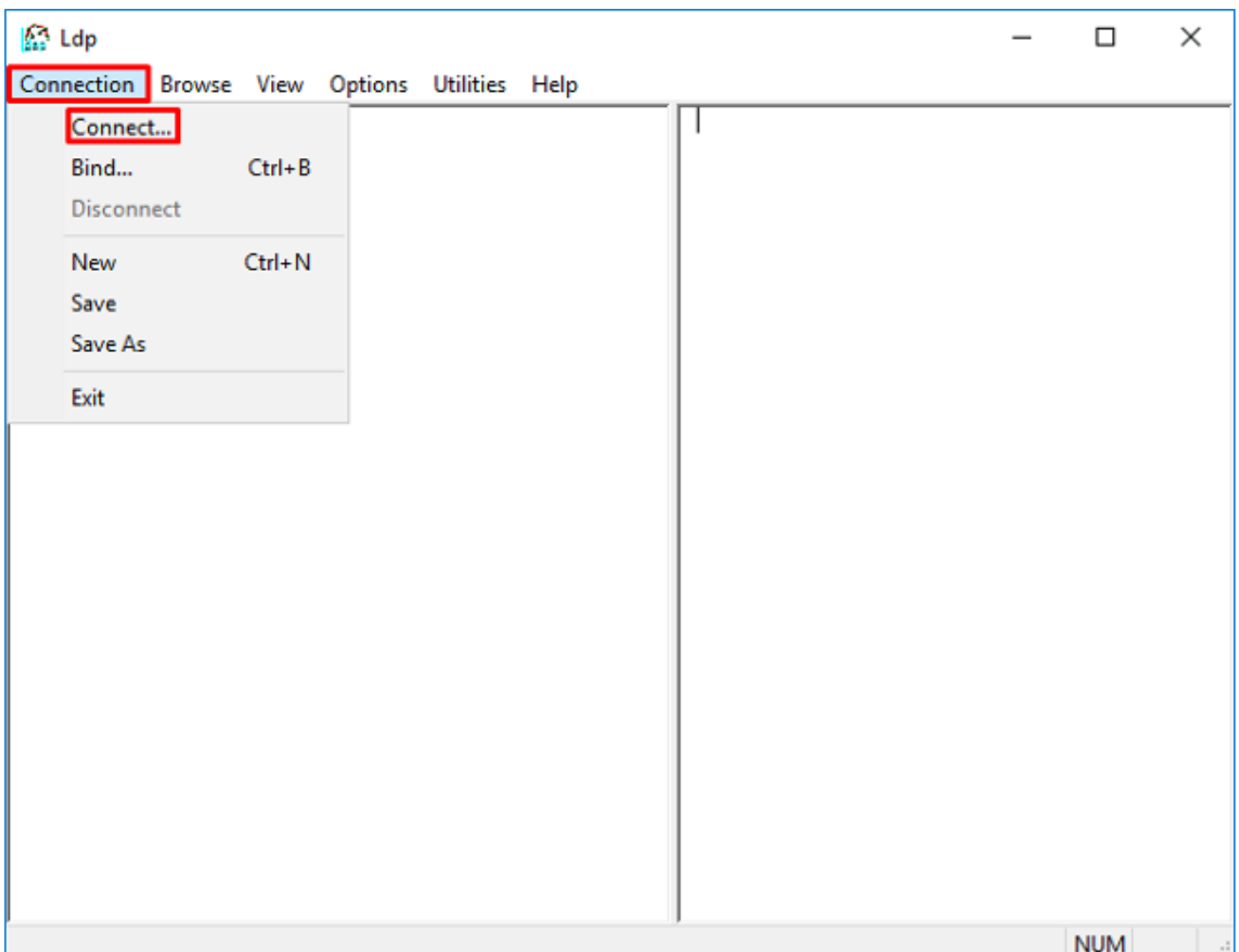
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] 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 Anmelde-Kennwort richtig konfiguriert sind. Dies kann auf dem AD-Server mit **ldp.exe** überprüft werden. Gehen Sie folgendermaßen vor, um sicherzustellen, dass ein Konto erfolgreich über ldp gebunden werden kann:

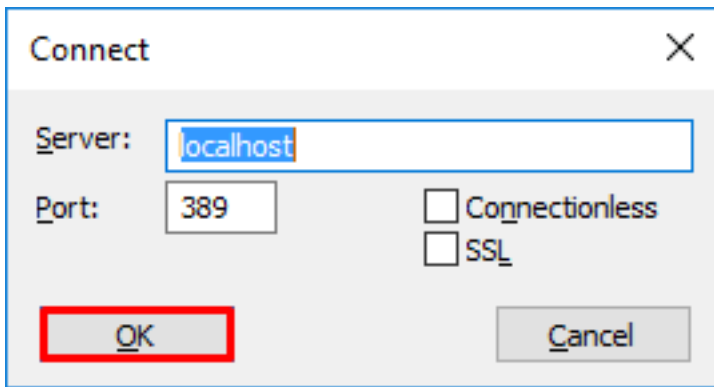
1. Drücken Sie auf dem AD-Server **Win+R**, und suchen Sie nach **ldp.exe**.



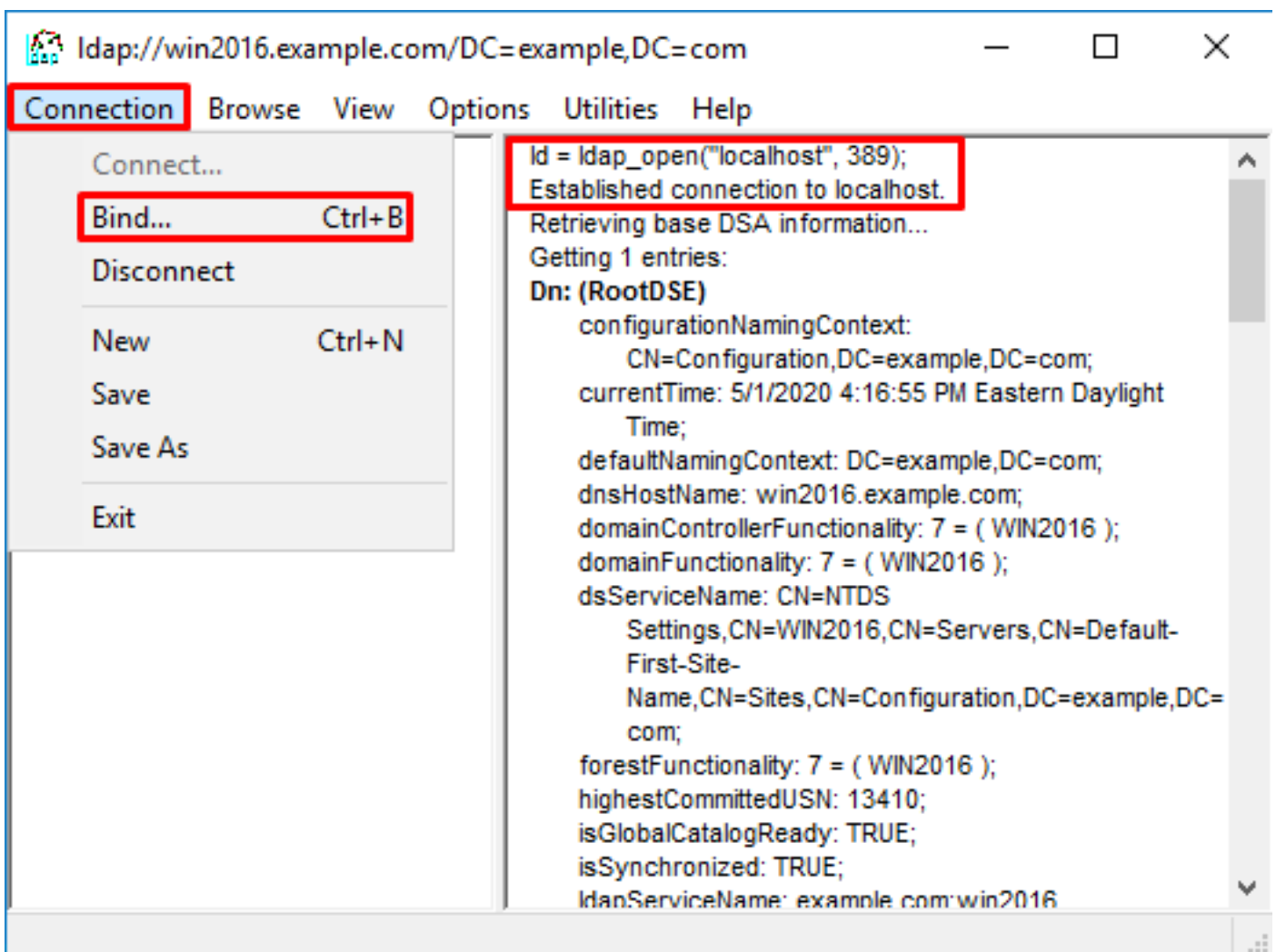
2. Wählen Sie unter **Verbindung** die Option **Verbinden...**



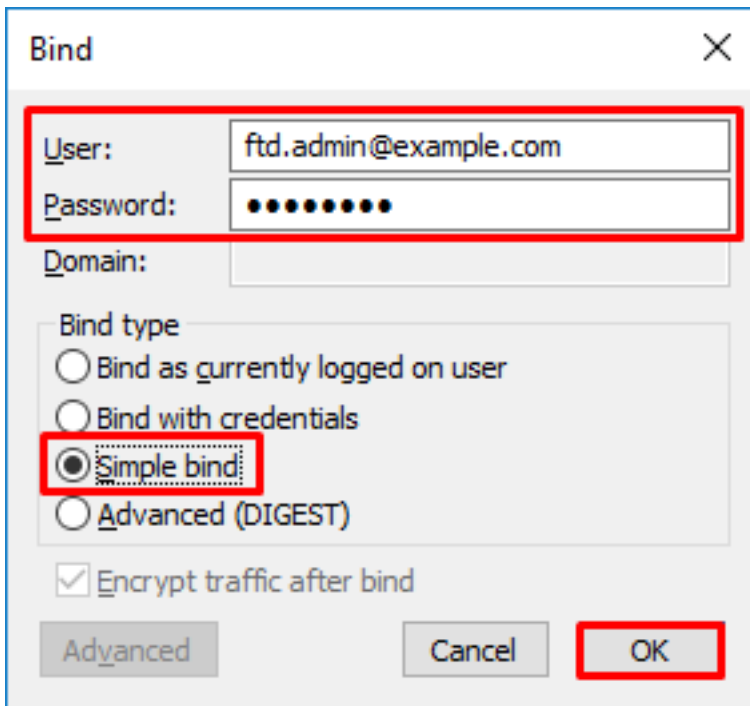
3. Geben Sie localhost für den Server und den entsprechenden Port an, und klicken Sie dann auf **OK**.



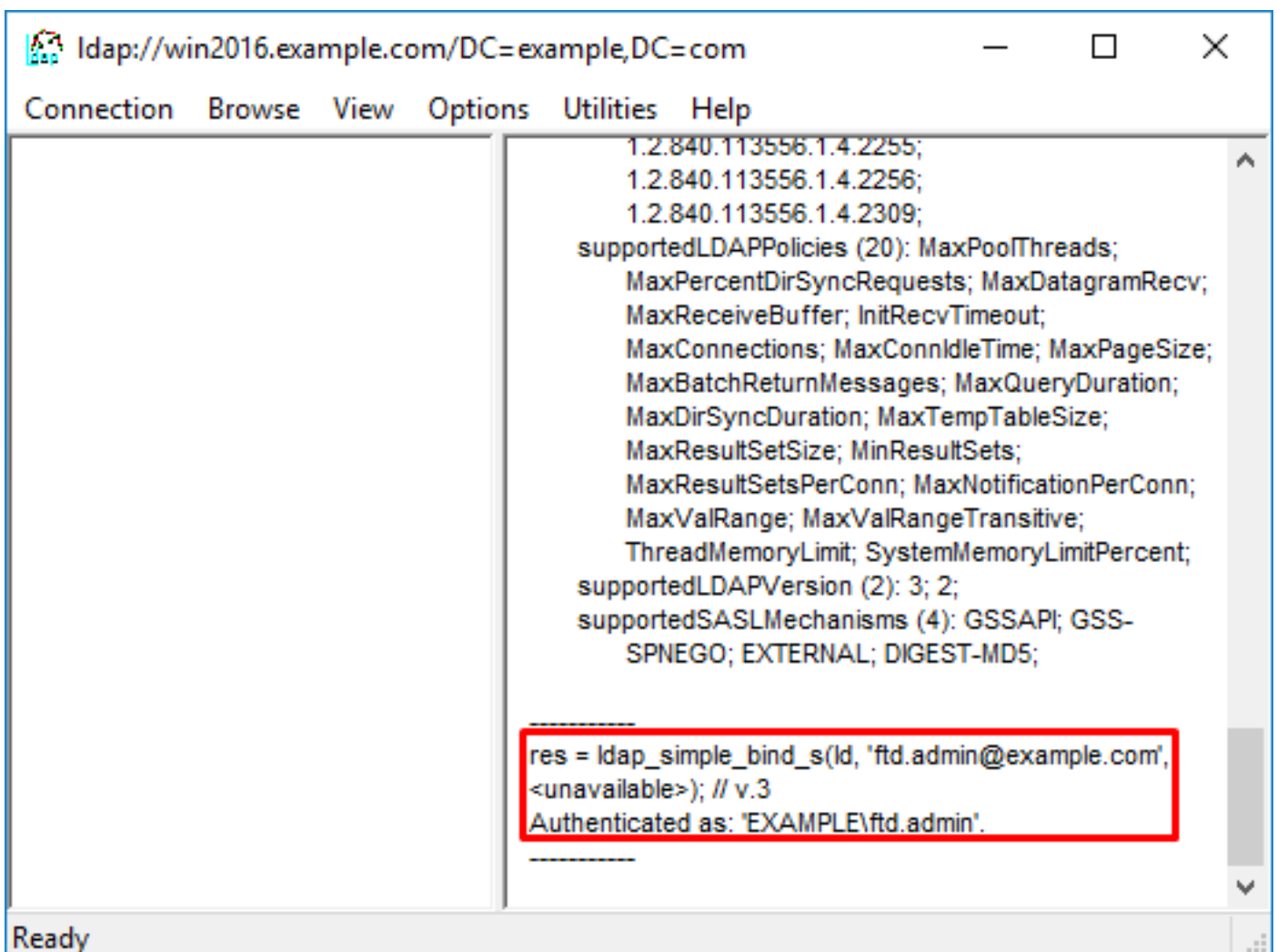
4. Die rechte Spalte zeigt Text an, der auf eine erfolgreiche Verbindung hinweist. Navigieren Sie zu **Verbindung > Binden...**



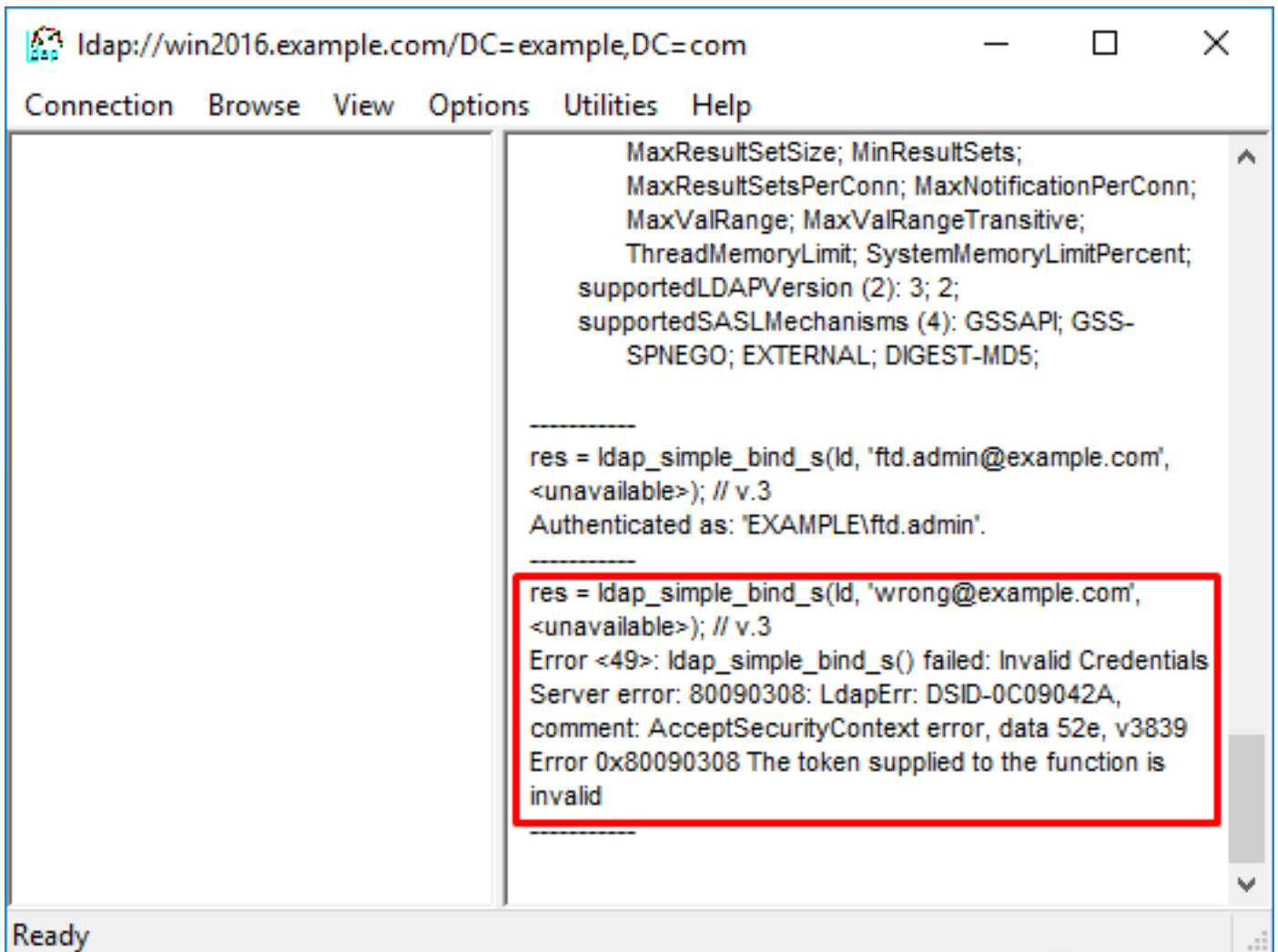
5. Wählen Sie **Simple Bind** und geben Sie dann den **Benutzernamen** und das **Passwort** des **Verzeichniskontos** an. Klicken Sie auf **OK**.



Bei erfolgreicher Bindung wird ldap Authentifiziert als: **DOMÄNE\Benutzername**



Ein Versuch, eine Bindung mit einem ungültigen Benutzernamen oder Kennwort herzustellen, führt zu einem Fehler wie den beiden hier gezeigten.

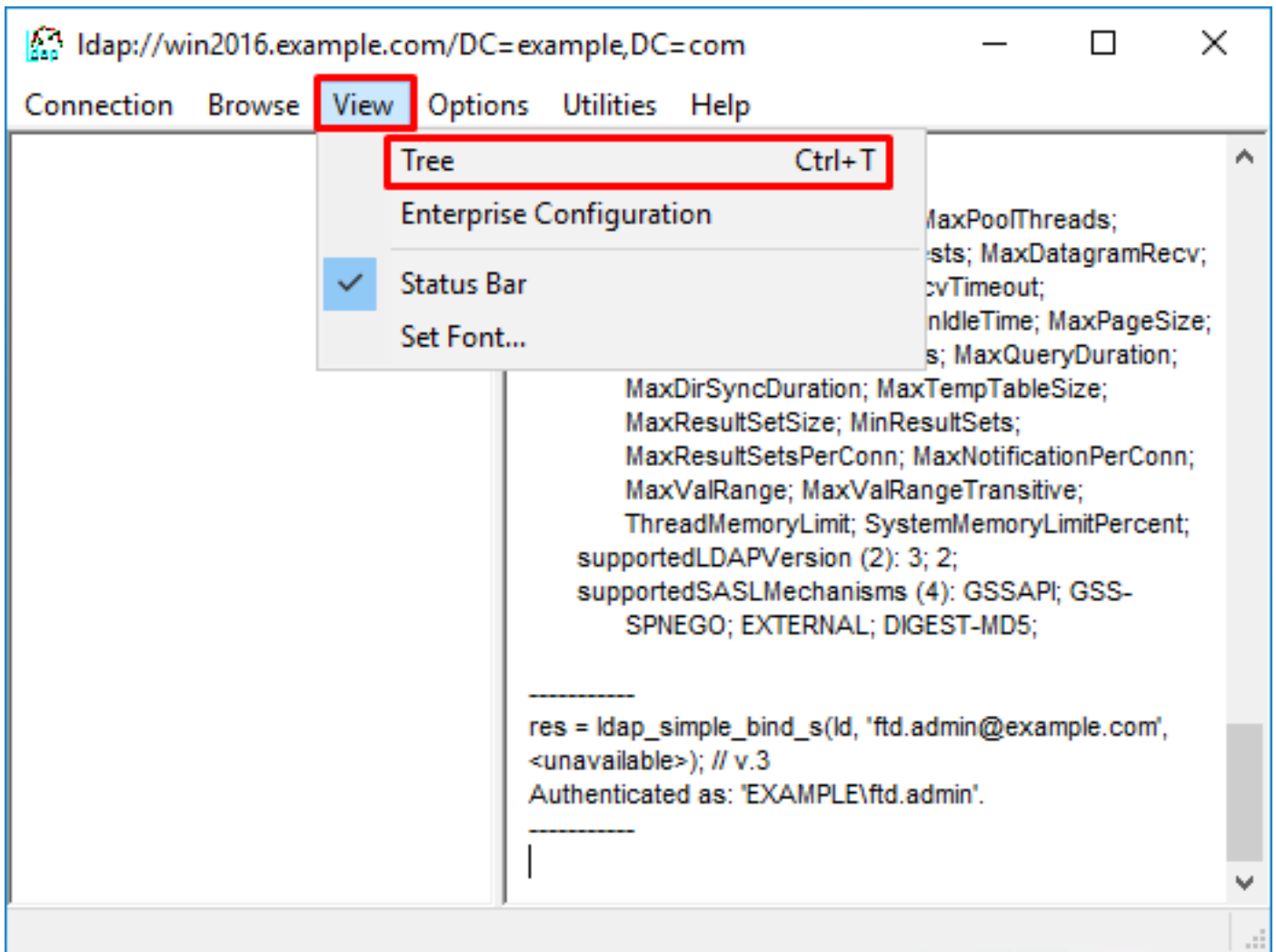


LDAP-Server konnte den Benutzernamen nicht finden

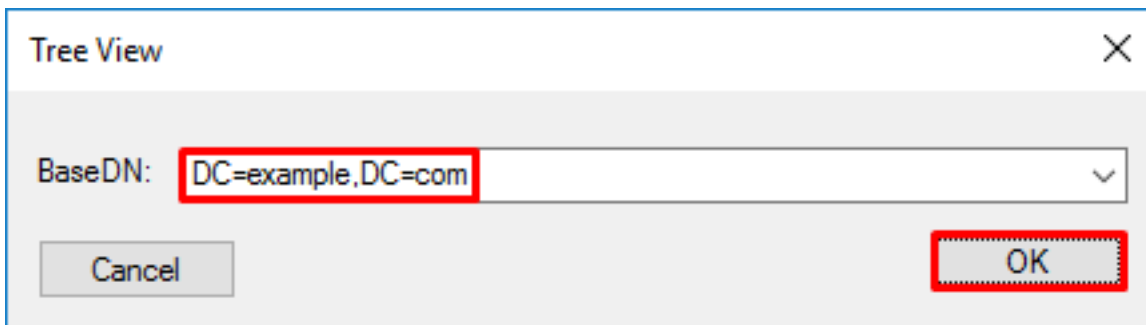
```
[ -2147483612] Session Start
[ -2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[ -2147483612] Fiber started
[ -2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[ -2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[ -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 vom FTD durchgeführten Suche finden kann. Dies kann auch mit **ldp.exe** durchgeführt werden.

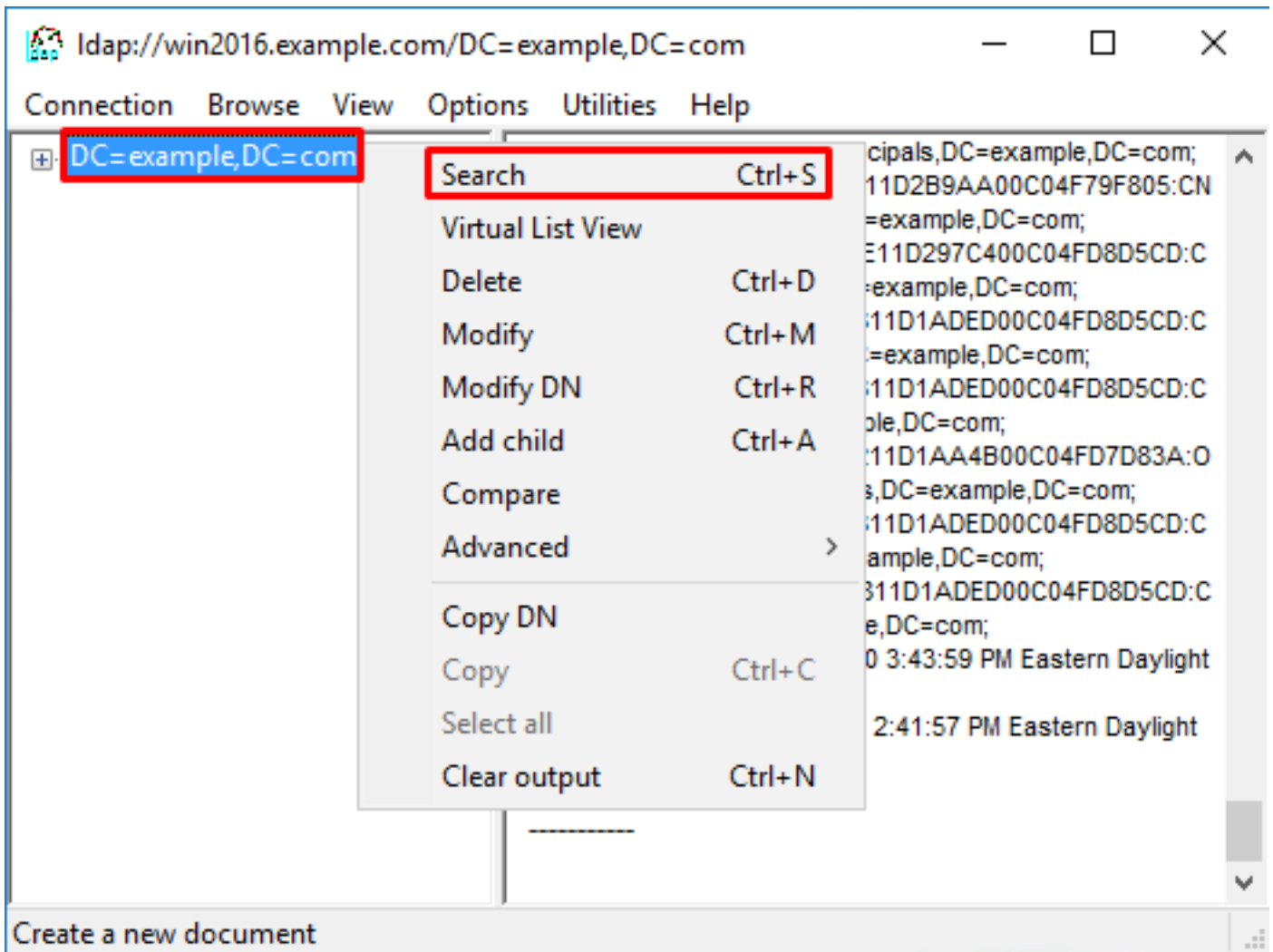
1. Navigieren Sie nach dem erfolgreichen Binden (siehe oben) zu **Ansicht > Baum**.



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



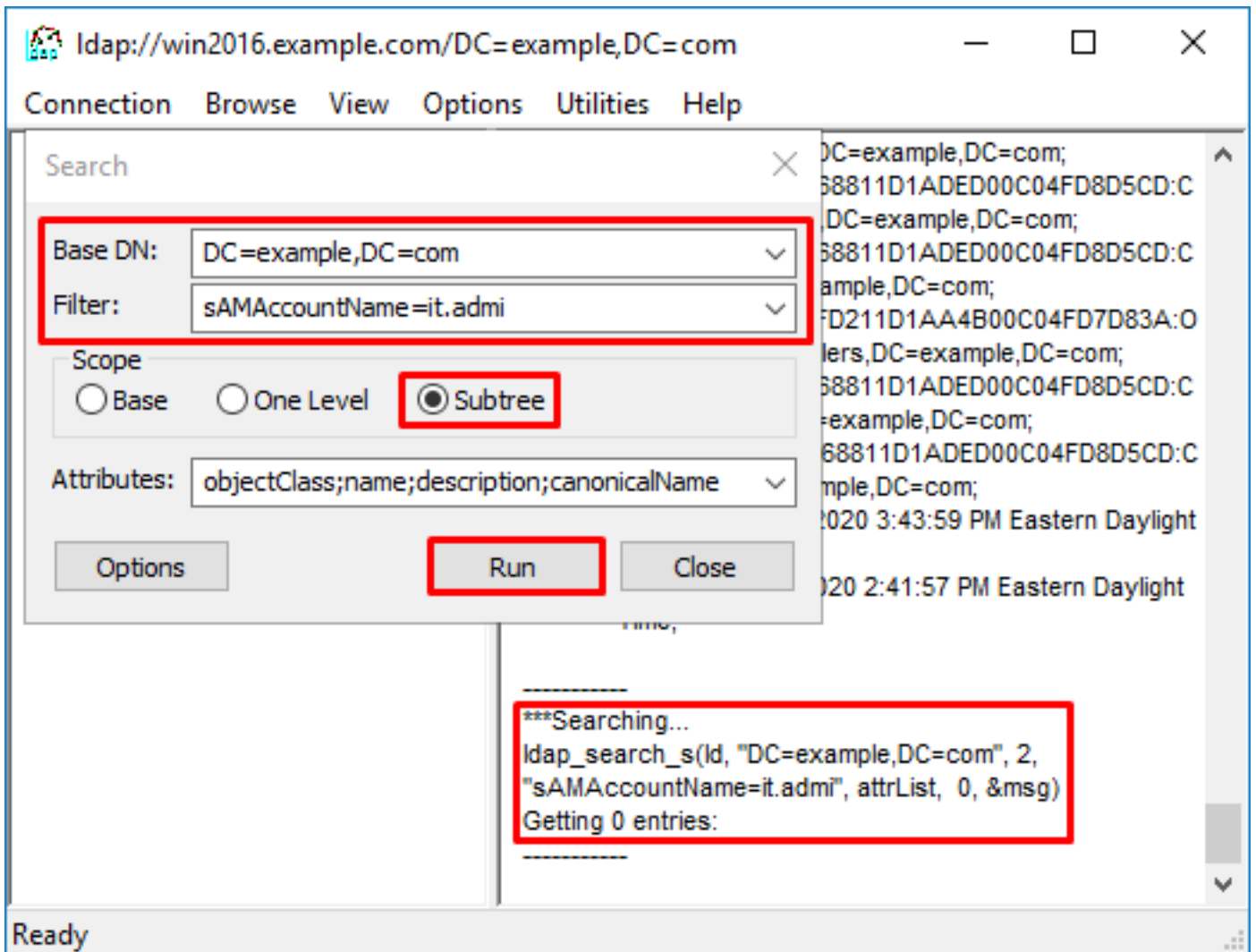
3. Klicken Sie mit der rechten Maustaste auf die Basis-DN, und klicken Sie dann auf **Suchen**.



4. Geben Sie die gleichen Werte für **Basisdatenbank**, **Filter** und **Bereich** an, wie sie in den Debugs angezeigt werden.

In diesem Beispiel sind dies:

- Basis-DN: dc=beispiel,dc=com
- Filter: samaccountname=it.admi
- Umfang:SUBTREE



Idp findet 0 Einträge, da es kein Benutzerkonto mit dem samaccountnamen **it.admi** unter der Basis-DN dc=beispiel,dc=com gibt

Ein weiterer Versuch mit dem richtigen samaccountname **it.admin** zeigt ein anderes Ergebnis an. Idp findet 1 Eintrag unter der Basis-DN dc=example,dc=com und druckt diese Benutzer-DN aus.

LDAP Search Tool Interface

Connection: ldap://win2016.example.com/DC=example,DC=com

Search Dialog:

- Base DN: DC=example,DC=com
- Filter: sAMAccountName=it.admin
- Scope: Subtree
- Attributes: objectClass;name;description;canonicalName
- Buttons: Options, Run, Close

Main Window Output:

```

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

```

Highlighted Entry:

```

***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;

```

Status: Ready

Falsches Kennwort für den Benutzernamen

```

[-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
```

Potenzielle Lösung: Vergewissern Sie sich, dass das Benutzerkennwort richtig konfiguriert ist und nicht abgelaufen ist. Ähnlich wie bei der Anmelde-DN führt die FTD eine Bindung mit AD mit den Benutzeranmeldeinformationen durch.

Diese Bindung kann auch in ldp durchgeführt werden, um zu überprüfen, ob das AD denselben Benutzernamen und dasselbe Kennwort erkennen kann. Die Schritte in ldp werden im Abschnitt **Ungültiger Binding Login DN und/oder falsches Kennwort** angezeigt.

Darüber hinaus können die Protokolle der Microsoft Server-**Ereignisanzeige** auf einen möglichen Grund hin überprüft werden.

AAA testen

Der Befehl `test aaa-server` kann verwendet werden, um einen Authentifizierungsversuch durch die FTD mit einem bestimmten Benutzernamen und Kennwort zu simulieren. Dies kann zum Testen von Verbindungs- oder Authentifizierungsfehlern 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 den FTD verlassen, aber keine Antwort erhalten, kann dies auf ein Routing-Problem hinweisen.

Capture zeigt den bidirektionalen LDAP-Datenverkehr an.

```
> 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

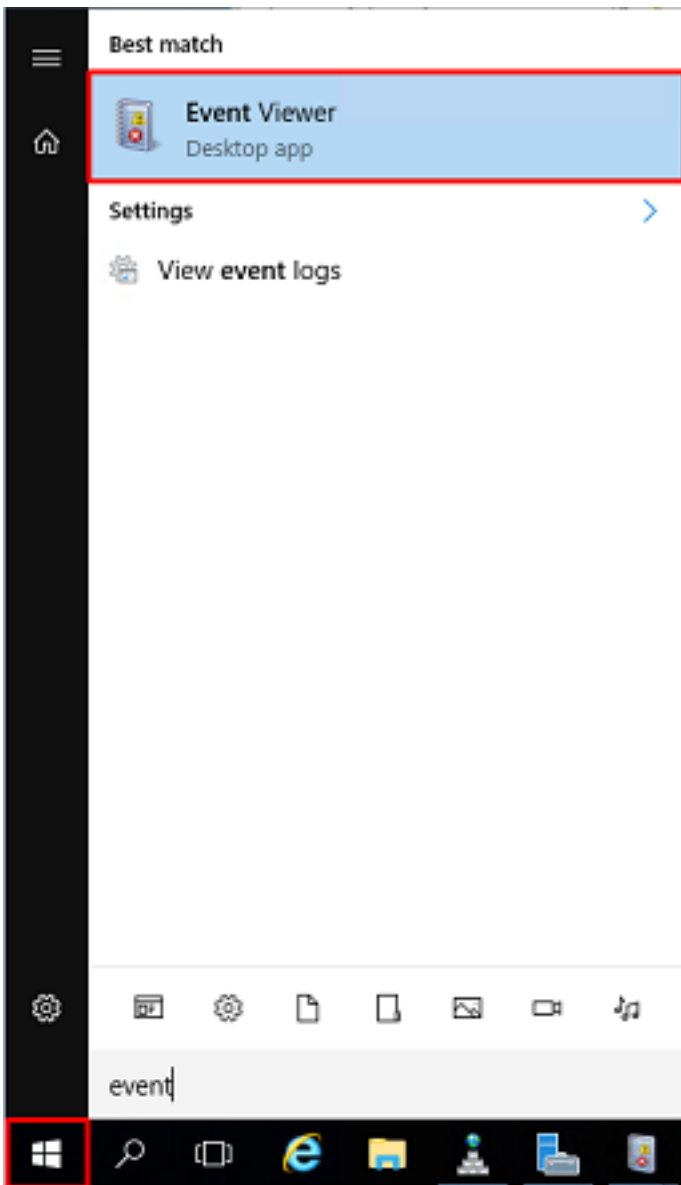
  1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
  2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
  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

```

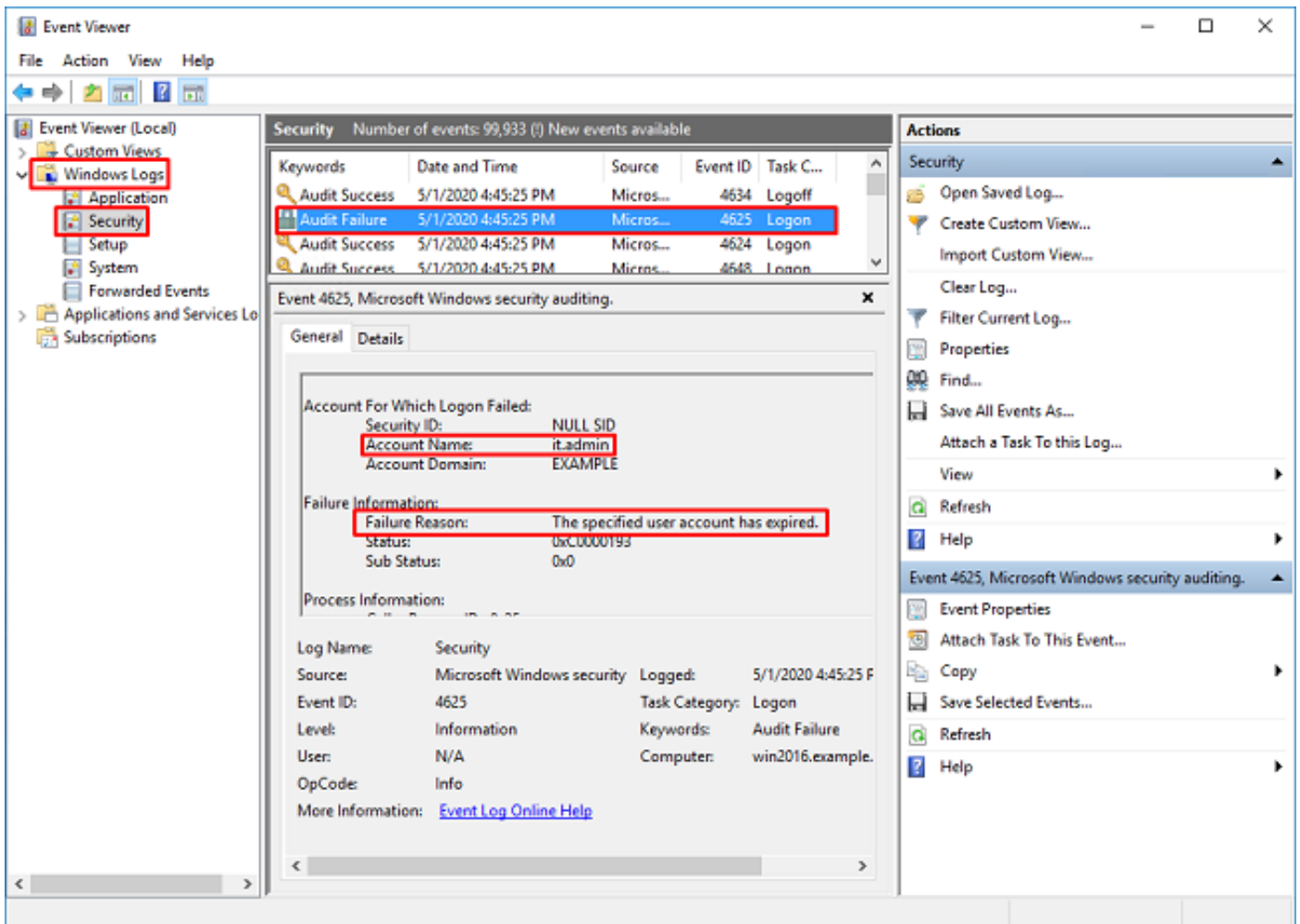
Windows Server-Ereignisanzeige - Protokolle

Die Protokolle der **Ereignisanzeige** auf dem AD-Server können detailliertere Informationen darüber bereitstellen, warum ein Fehler aufgetreten ist.

1. Suchen Sie nach der **Ereignisanzeige**, und öffnen Sie sie.



2. Erweitern Sie **Windows-Protokolle**, und klicken Sie auf **Sicherheit**. Suchen Sie mit dem Benutzernamen nach **Audit Failures (Überwachungsfehler)**, und überprüfen Sie die Fehlerinformationen.



An account failed to log on.

Subject:

Security ID:SYSTEM
Account Name:WIN2016\$\br/>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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.