AnyConnectクライアント用にFDMによって管理されるFTDでのAD(LDAP)認証およびユーザIDの設定

内容

概要

このドキュメントの目的は、Firepower Device Management(FDM)によって管理されるCisco Firepower Threat Defense(FTD)に接続するAnyConnectクライアントのActive Directory(AD)認証を設定する方法を詳しく説明します。 AnyConnectユーザを特定のIPアドレスおよびポートに制限するために、アクセスポリシーでユーザIDが使用されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FDMでのRA VPN設定に関する基礎知識
- FDMでのLDAPサーバ設定に関する基礎知識
- ADに関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft 2016サーバ
- 6.5.0を実行するFTDv

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワークダイアグラムとシナリオ

Windowsサーバには、ユーザーIDをテストするため、インターネットインフォメーションサービス(IIS)およびリモートデスクトッププロトコル(RDP)があらかじめ設定されています。この設定ガイドでは、3つのユーザアカウントと2つのグループが作成されます。

ユーザアカウント:

- FTD管理者：これは、FTDがADサーバにバインドできるように、ディレクトリアカウントとして使用されます。
- IT管理者：ユーザIDを実証するために使用されるテスト管理者アカウント。
- テストユーザー：ユーザIDを実証するために使用されるテストユーザアカウント。

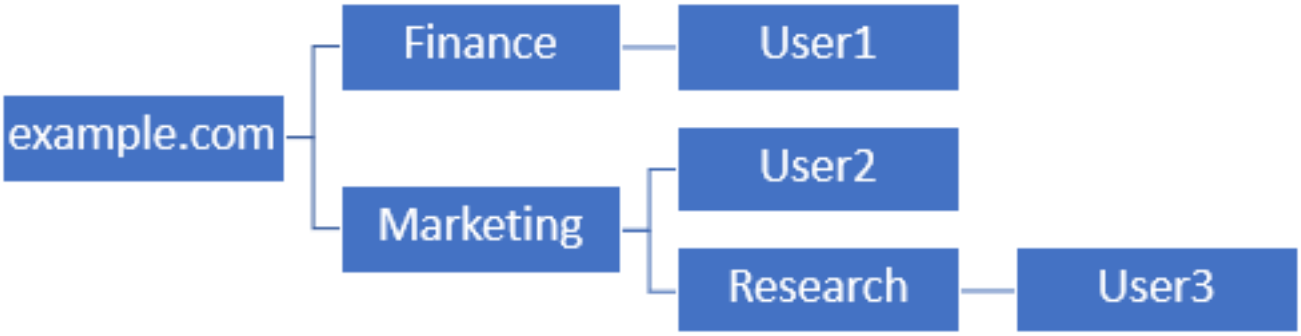
グループ:

- AnyConnect Admins:ユーザIDを実証するためにIT管理者が追加されるテストグループ。このグループには、Windows ServerへのRDPアクセスのみが許可されます
- AnyConnect ユーザ:ユーザIDを実証するためにテストユーザが追加されるテストグループ。このグループには、Windows ServerへのHTTPアクセスのみが許可されます

ADの設定

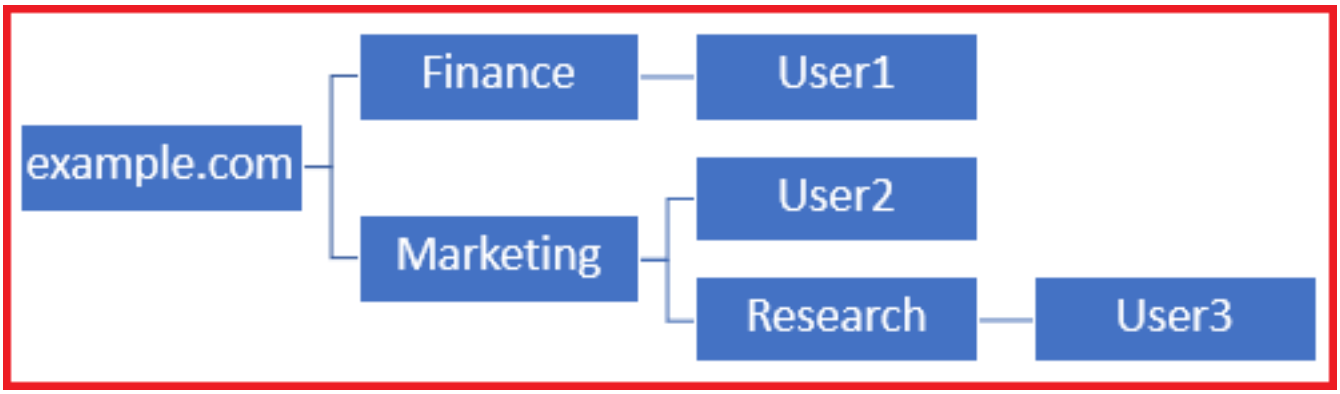
FTDでAD認証とユーザIDを適切に設定するには、いくつかの値が必要です。FDMで構成を行う前に、これらの詳細をすべてMicrosoft Serverで作成または収集する必要があります。主な値は次のとおりです。

- [Domain Name]：これは、サーバのドメイン名です。この設定ガイドでは、example.comがドメイン名です。
- サーバIP/FQDNアドレス：Microsoftサーバに到達するために使用されるIPアドレスまたはFQDN。FQDNを使用する場合、FQDNを解決するには、FDMおよびFTD内でDNSサーバを設定する必要があります。この設定ガイドでは、これらの値はwin2016.example.comで、192.168.1.1に解決されます。
- サーバポート：LDAPサービスで使用されるポート。デフォルトでは、LDAPとSTARTTLSはLDAPにTCPポート389を使用し、LDAP over SSL(LDAPS)はTCPポート636を使用します。
- ルートCA:LDAPSまたはSTARTTLSを使用する場合、LDAPSで使用されるSSL証明書の署名に使用されるルートCAが必要です。
- ディレクトリのユーザ名とパスワード：これは、FDMとFTDがLDAPサーバにバインドし、ユーザを認証し、ユーザとグループを検索するために使用するアカウントです。この目的で、FTD Adminという名前のアカウントが作成されます。
- 基本識別名(DN):ベースDNはFDMの開始点であり、FTDはActive Directoryに対してユーザの検索時に開始するように指示します。この設定ガイドでは、ルートドメインexample.comがベースDNとして使用されます。ただし、実稼働環境では、LDAP階層内でベースDNをさらに使用する方が適している場合があります。たとえば、次のLDAP階層を使用します。



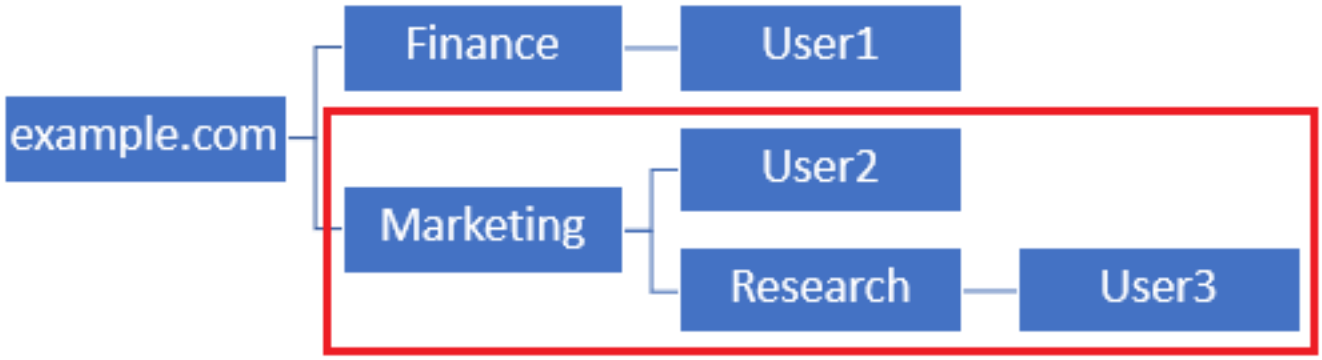
管理者がマーケティング組織ユニット内のユーザにベースDNを認証できるようにしたい場合は、ルート(example.com)に設定できます。ただし、これは、Finance組織ユニットのUser1もログインできます。これは、ユーザ検索がルートで始まり、Finance、Marketing、Researchに移動するためです。

ベースDNをexample.comに設定します。



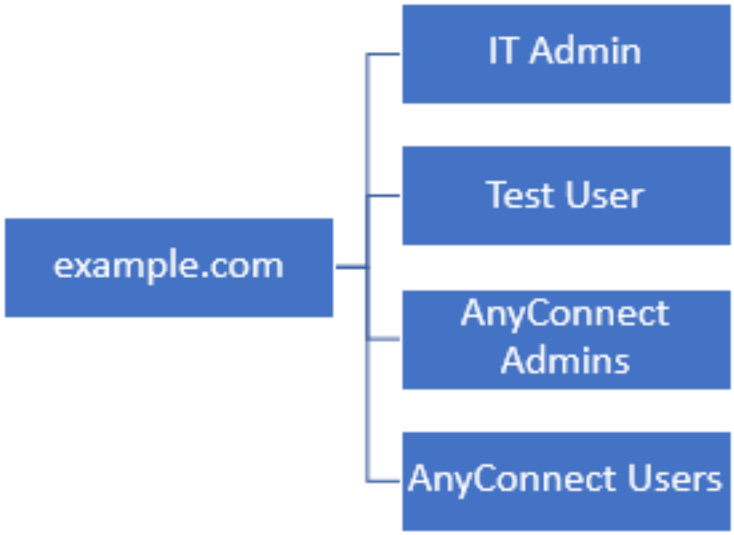
ログインをマーケティング組織単位以下のユーザだけに制限するには、管理者がBase DNをMarketingに設定します。これで、User2とUser3のみが認証を実行できます。これは、検索がマーケティングで開始されるためです。

[Base DN set to Marketing]:



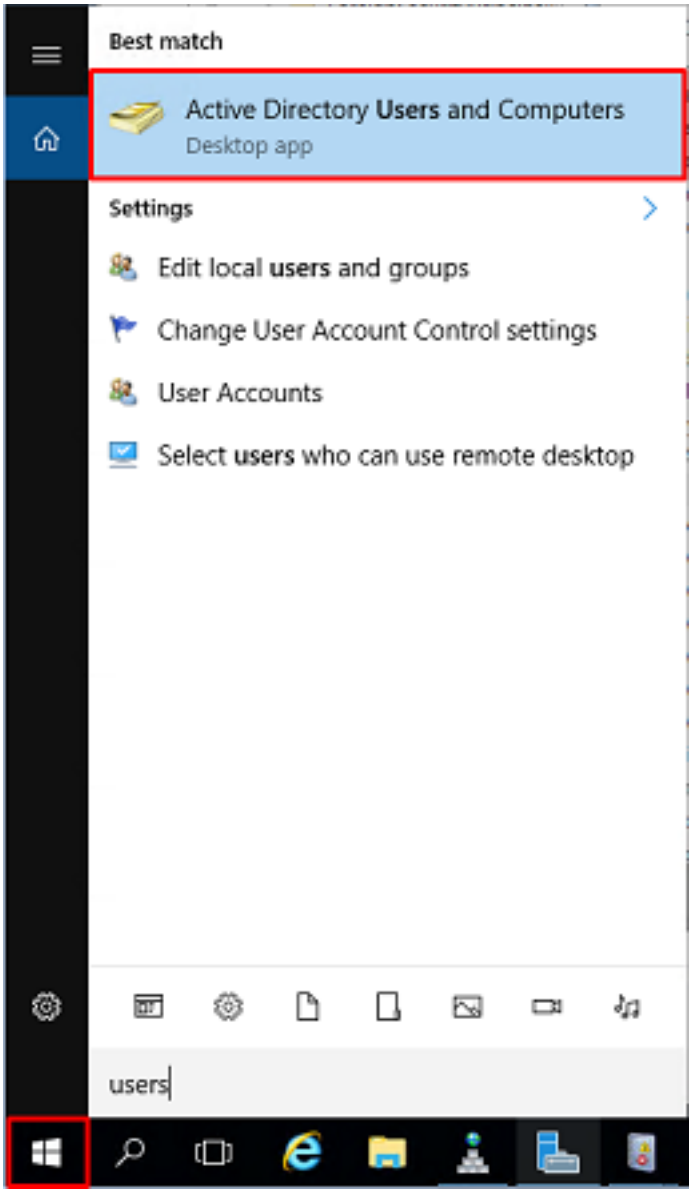
FTD内でより詳細な制御を行うために、ユーザが接続したり、AD属性に基づいて異なる許可をユーザに割り当てたりできるように、LDAP許可マップを設定する必要があることに注意してください。

この簡素化されたLDAP階層は、この設定ガイドで使用され、ルートexample.comのDNがベースDNに使用されます。

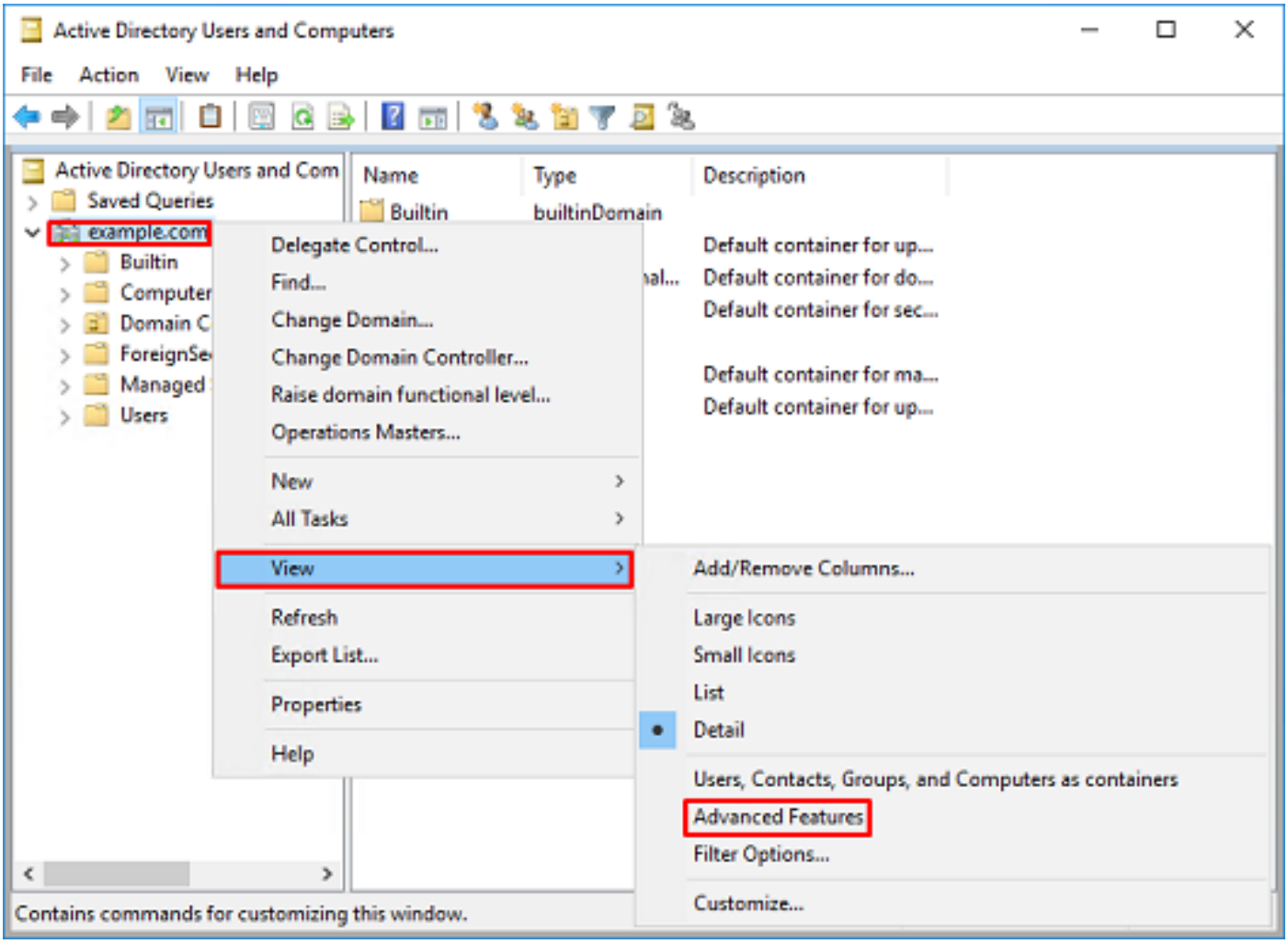


LDAPベースDNの決定

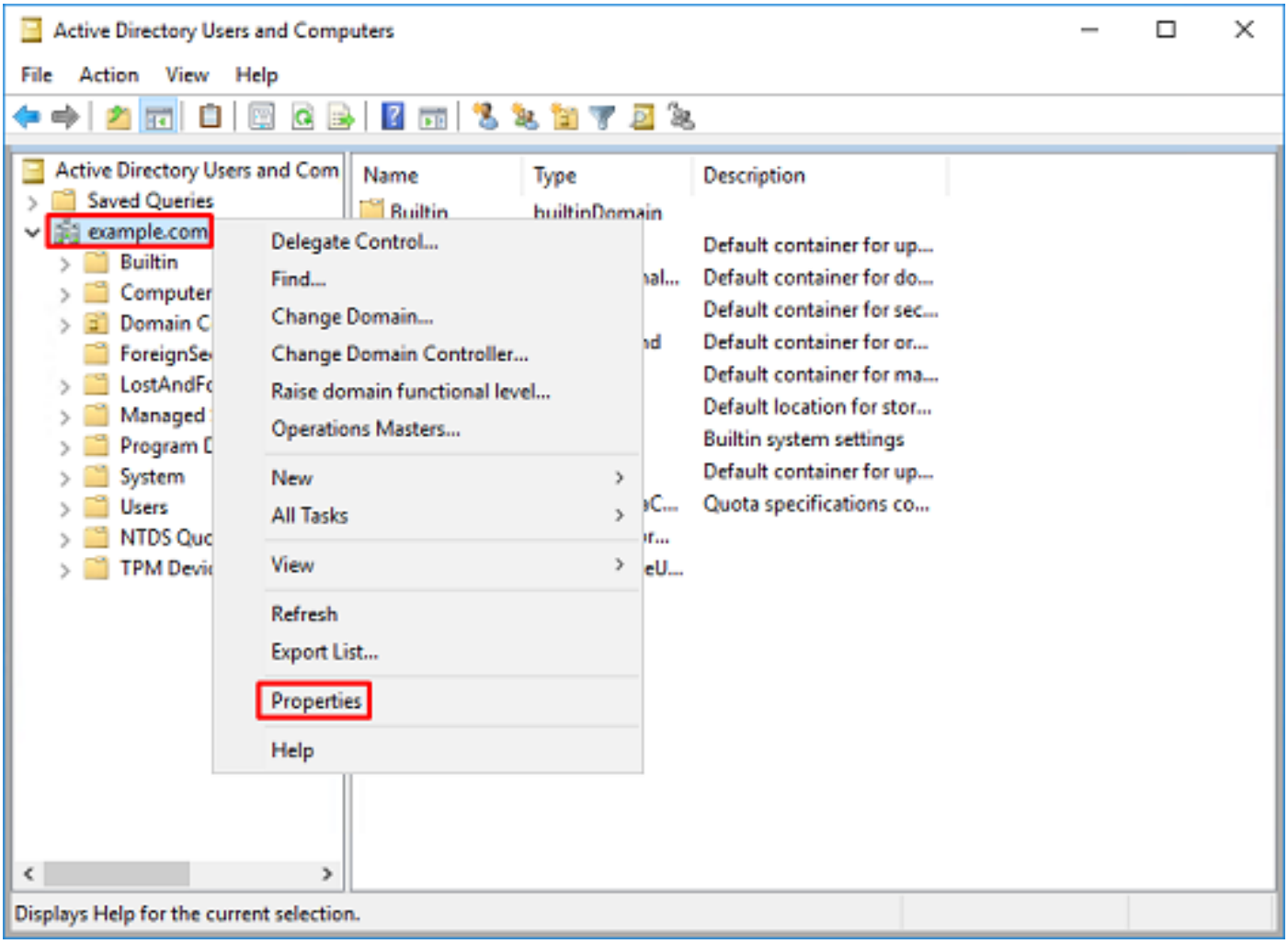
1. ADユーザーとコンピューターを開きます。



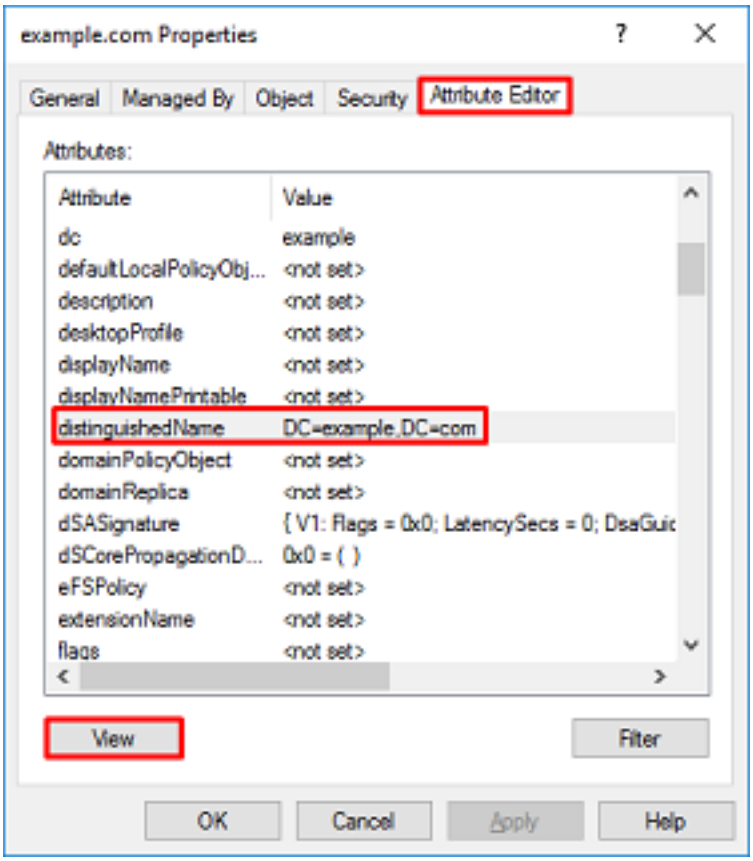
2.ルートドメイン（コンテナを開くには）を左クリックし、ルートドメインを右クリックして、[View]に移動し、**[Advanced Features]をクリックします。**



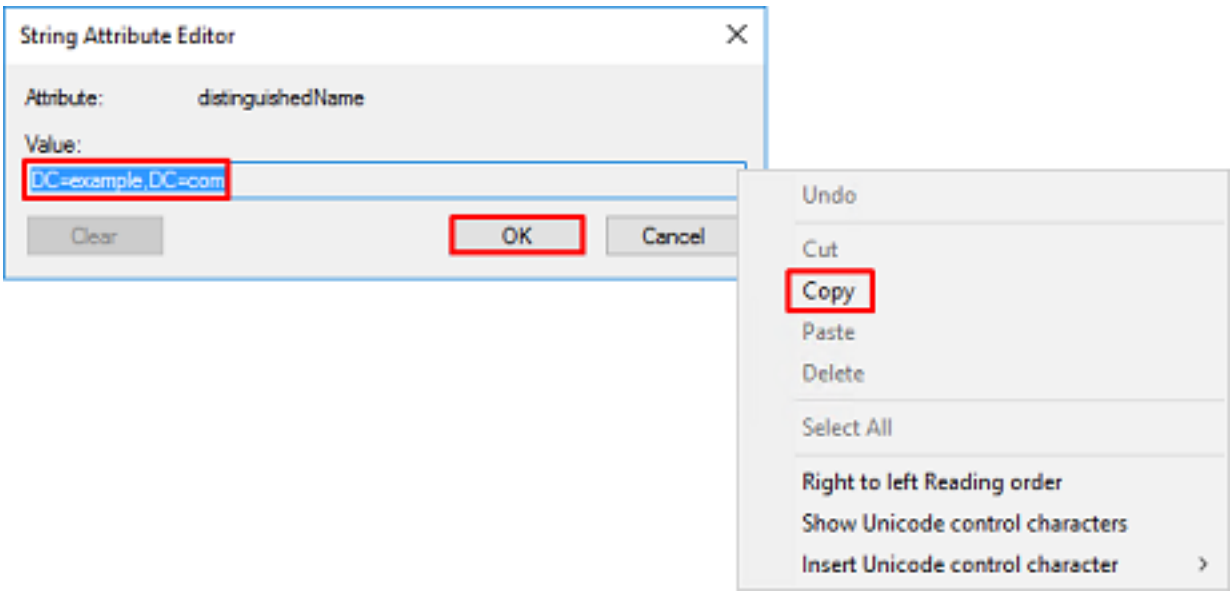
3.これにより、ADオブジェクトの下に追加のプロパティが表示されます。たとえば、ルートexample.comのDNを検索するには、**example.com**を右クリックして、**Properties**に移動します。

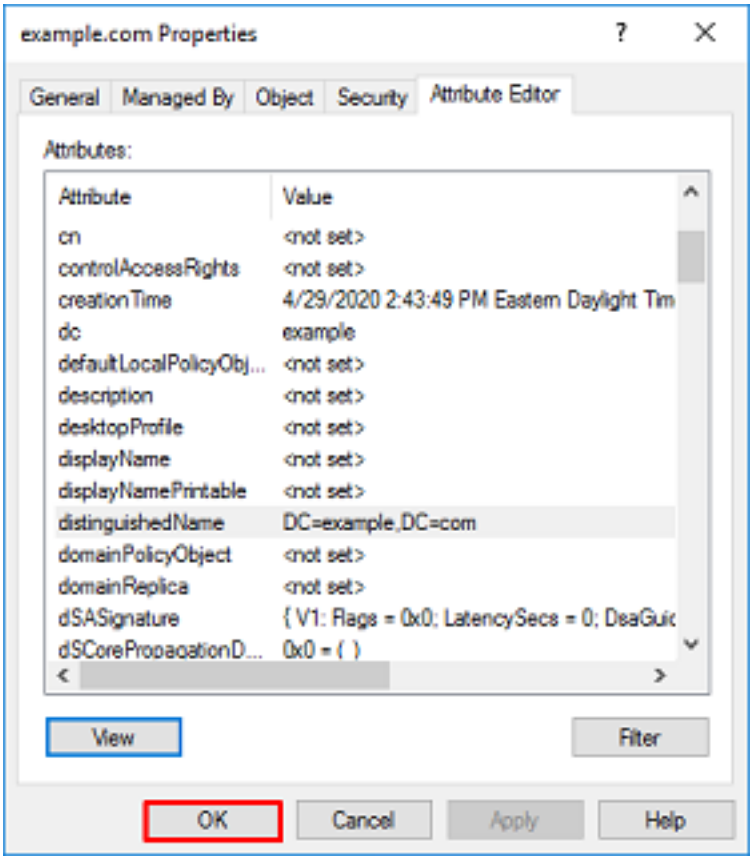


4. [プロパティ]の下の[属性エディタ]タブをクリックします。属性の下でdistinguishedNameを検索し、[表示]をクリックします。

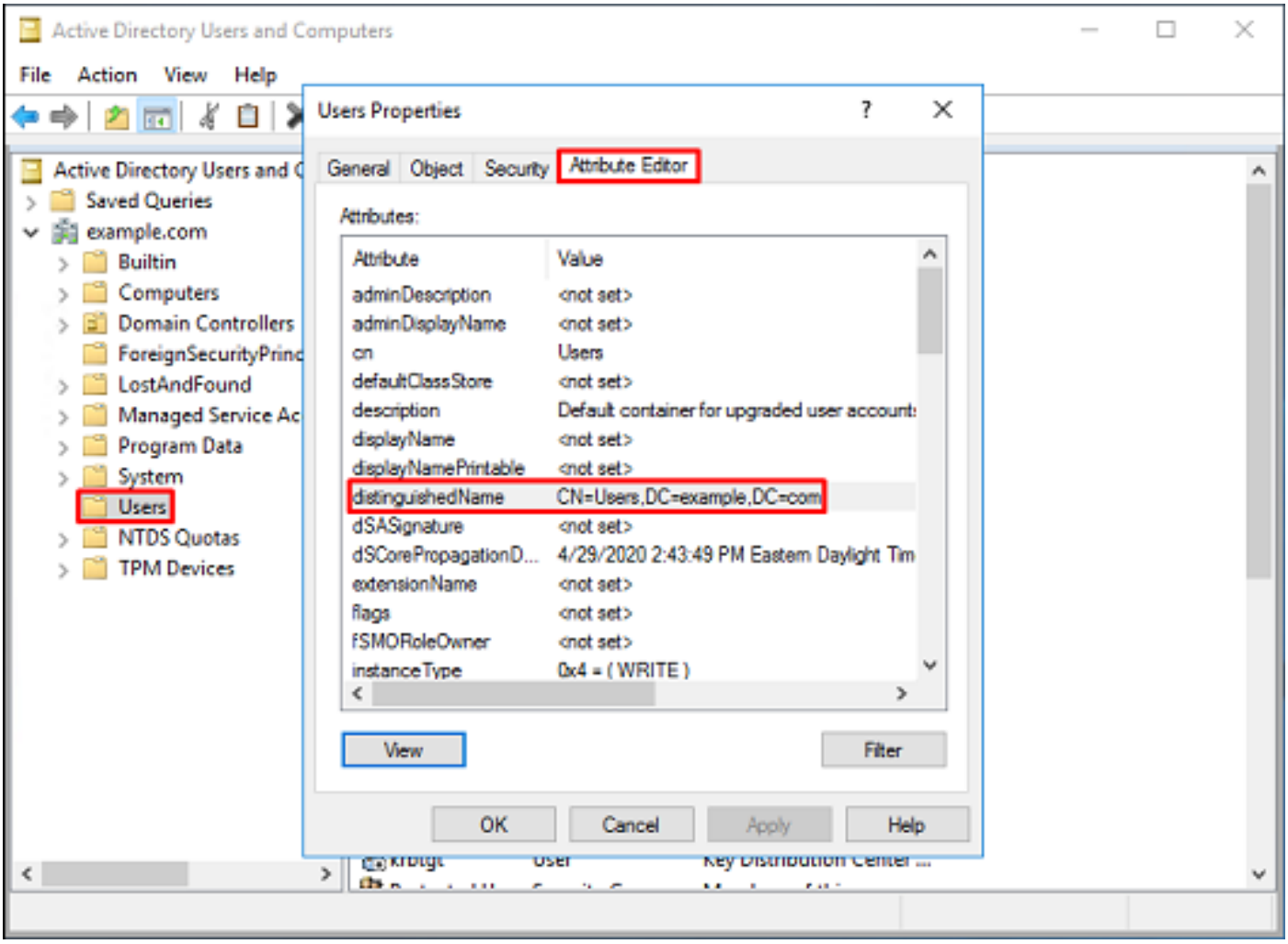


5.これにより、新しいウィンドウが開き、DNを後でコピーしてFDMに貼り付けることができます。この例では、ルートDNはDC=example、DC=comです。値をコピーします。[OK]をクリックして[String Attribute Editor]ウィンドウを終了し、もう一度[OK]をクリックして[Properties]を終了します。

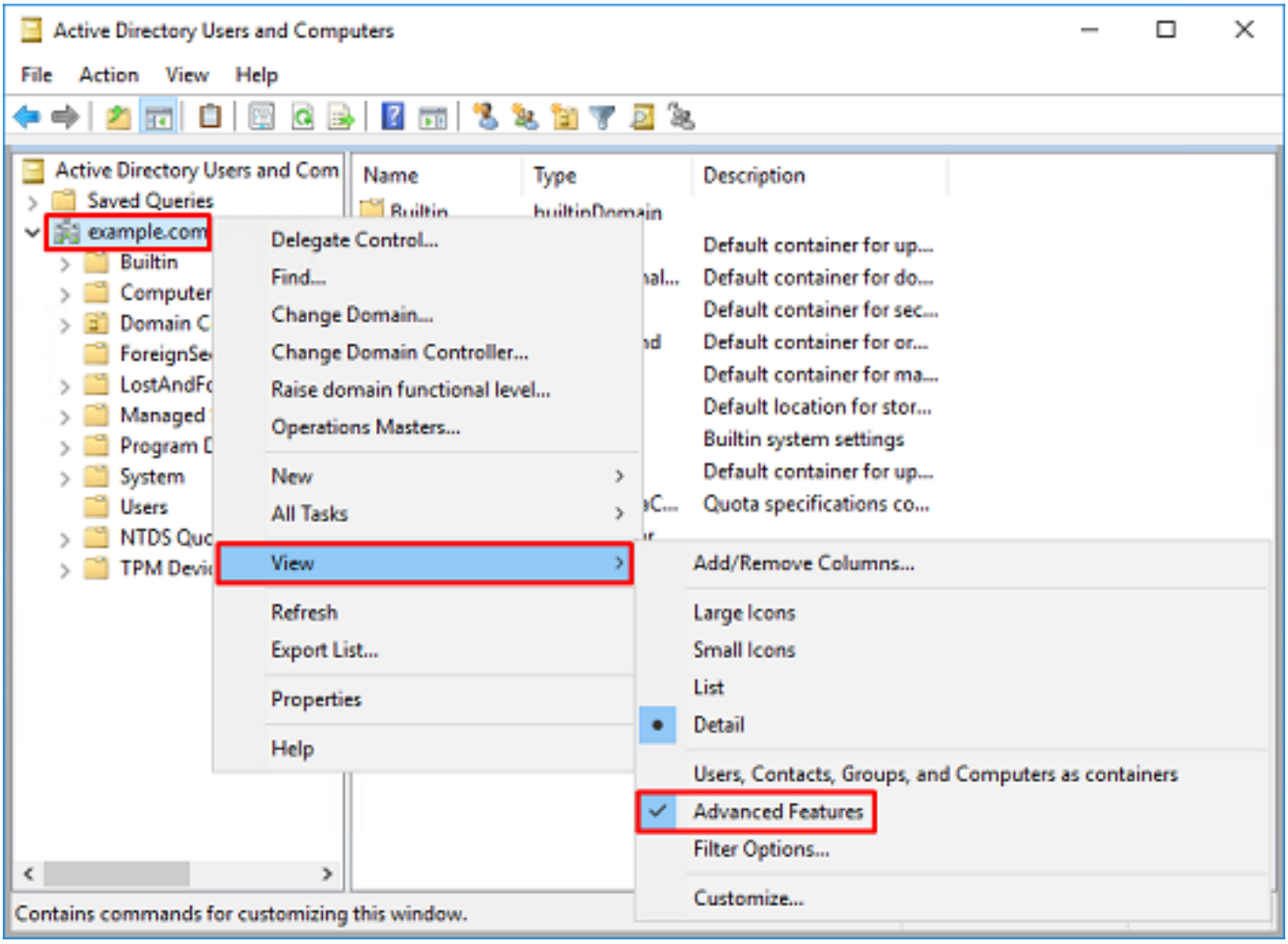




これは、AD内の複数のオブジェクトに対して実行できます。たとえば、ユーザコンテナのDNを検索するには、次の手順を使用します。



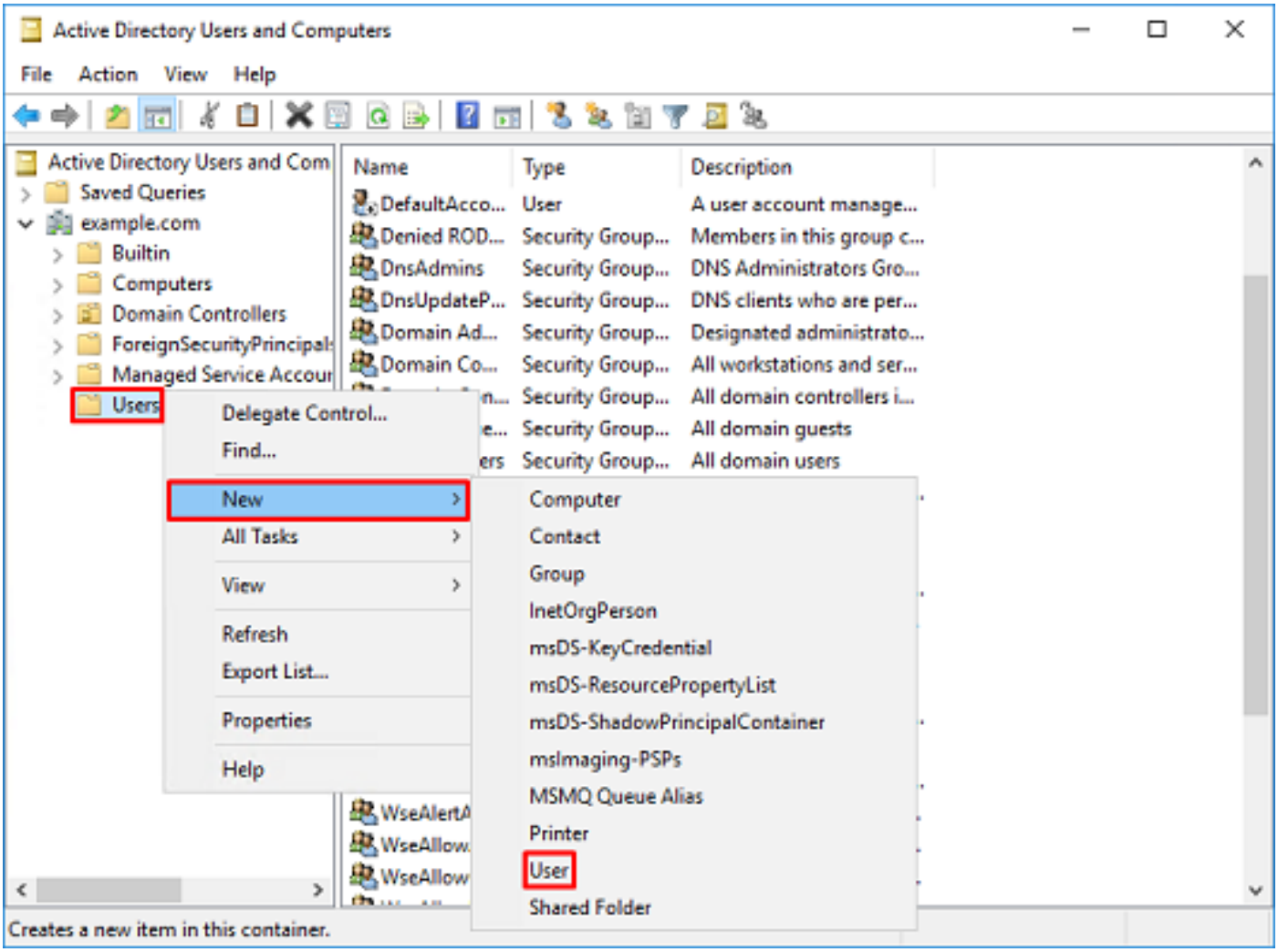
6. [拡張機能]ビューは削除できます。ルートDNを右クリックし、[View]に移動し、[Advanced Features]をもう一度クリックします。



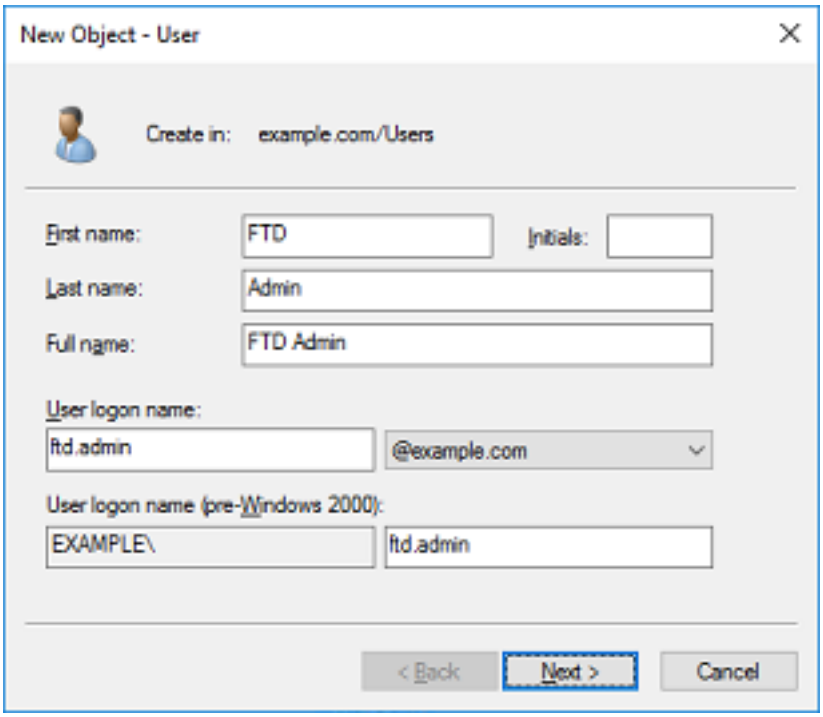
FTDアカウントの作成

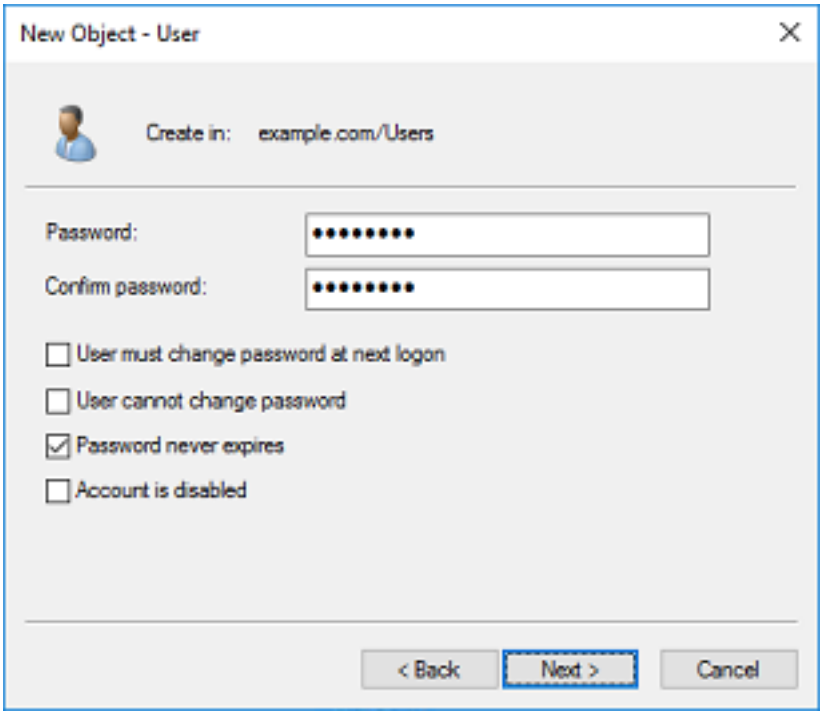
このユーザアカウントを使用すると、FDMとFTDをADにバインドし、ユーザとグループを検索して認証できます。別のFTDアカウントを作成する目的は、バインディングに使用されるクレデンシャルが侵害された場合に、ネットワーク内の他の場所で不正アクセスを防止することです。このアカウントは、ベースDNの範囲内である必要はありません。

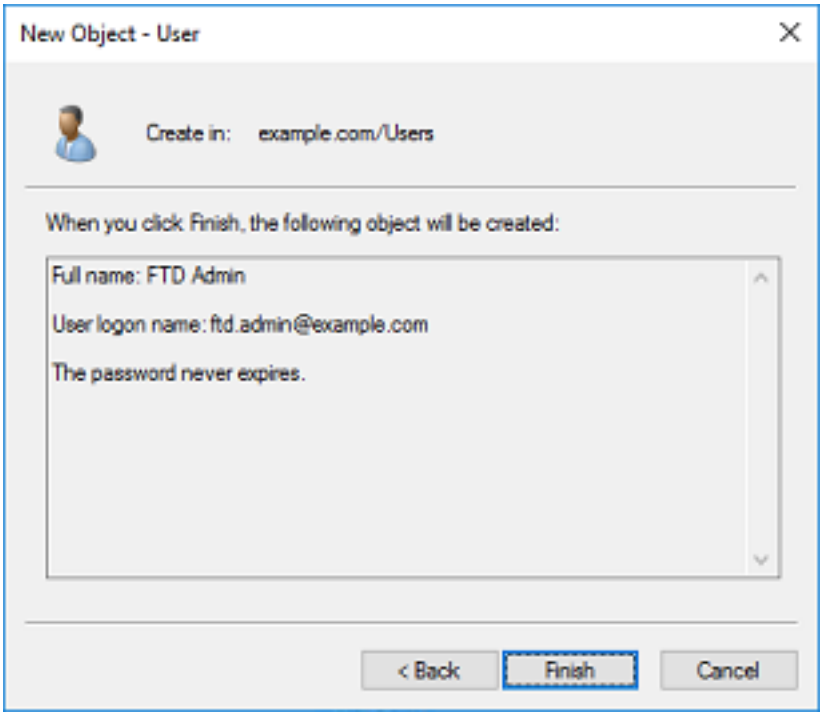
1. [Active Directory Users and Computers]で、FTDアカウントを追加するコンテナまたは組織を右クリックします。この構成では、FTDアカウントがユーザ名ftd.admin@example.comの下のUsersコンテナに追加されます。[Users]を右クリックし、[New] > [User]をクリックします。



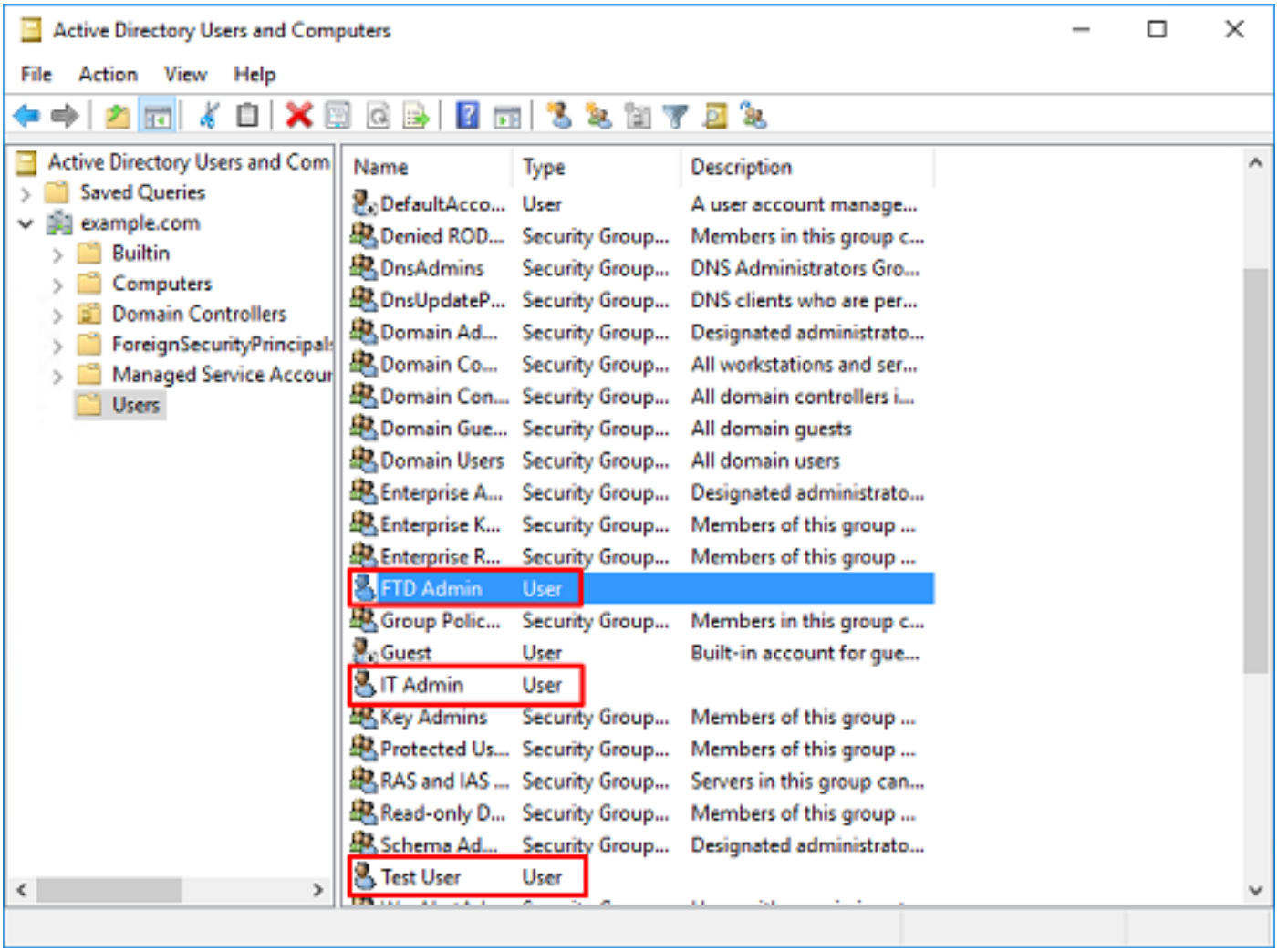
2. 「新規オブジェクト – ユーザー」**ウィザードをナビゲート**します。







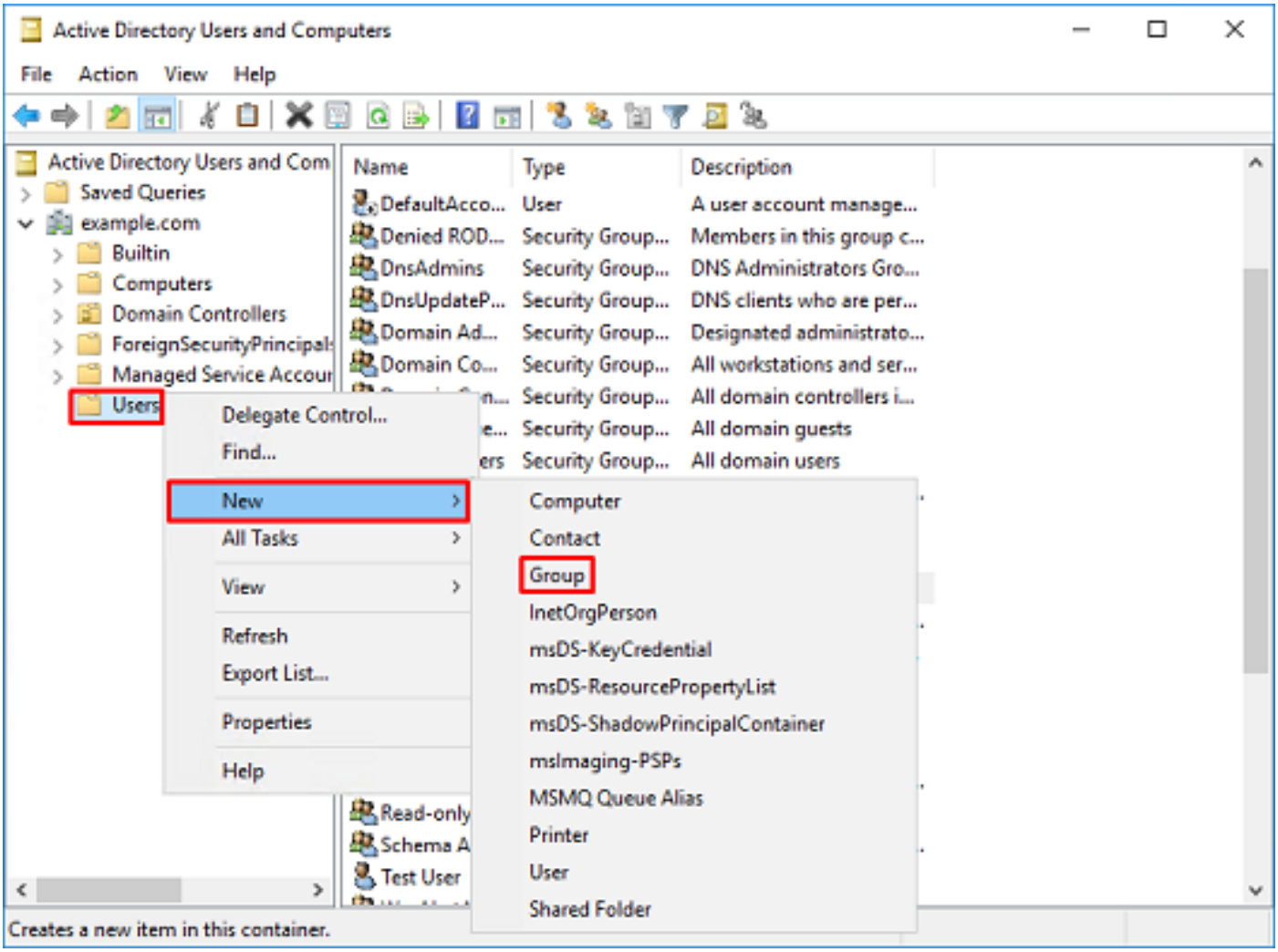
3. FTDアカウントが作成されたことを確認します。さらに、**IT** Adminと**Test User**という2つの追加アカウント**が作成されました。**



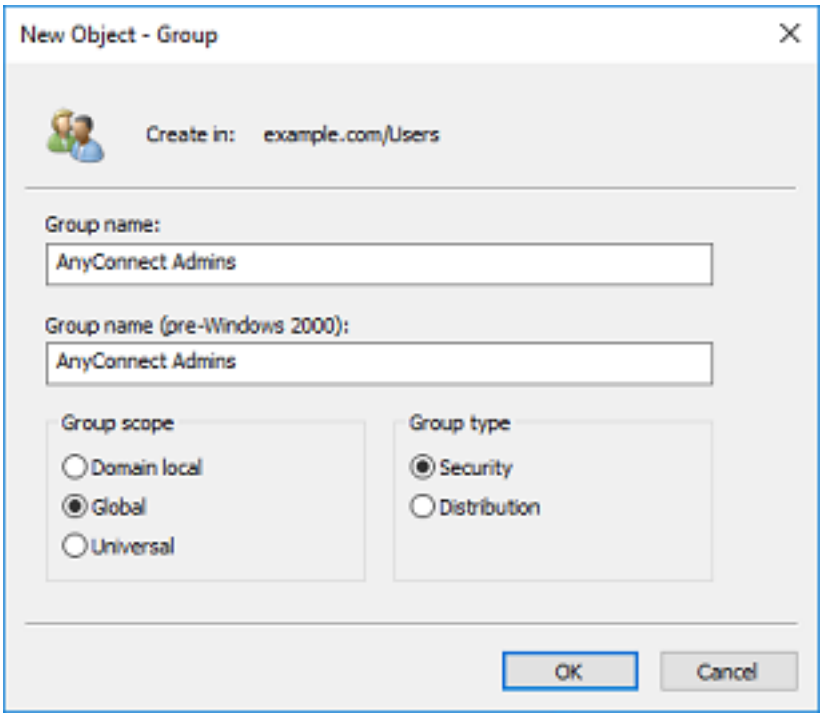
ADグループの作成とADグループへのユーザの追加（オプション）

認証に不要なグループを使用すると、アクセスポリシーを複数のユーザに簡単に適用したり、LDAP認可を適用したりできます。この構成ガイドでは、グループを使用して、後でFDM内のユーザーIDを介してアクセス制御ポリシー設定を適用します。

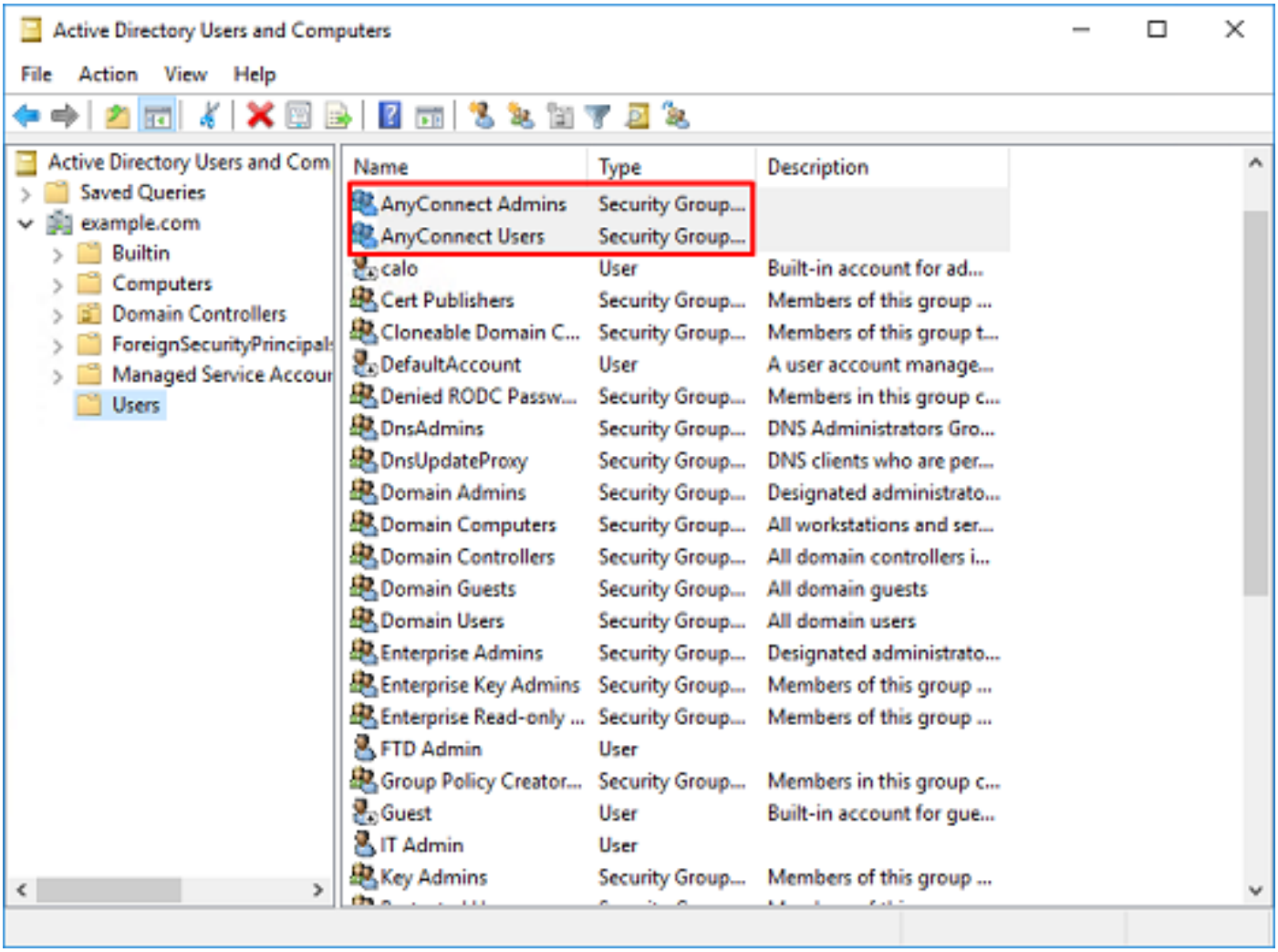
1. [Active Directory Users and Computers]で、**新しいグループが追加されるコンテナ**/組織を右クリックします。この例では、グループ**AnyConnect Admins**が**Users**コンテナの下に追加されます。[ユーザー]を右クリックし、[新規作成] > [グループ]をクリックします。



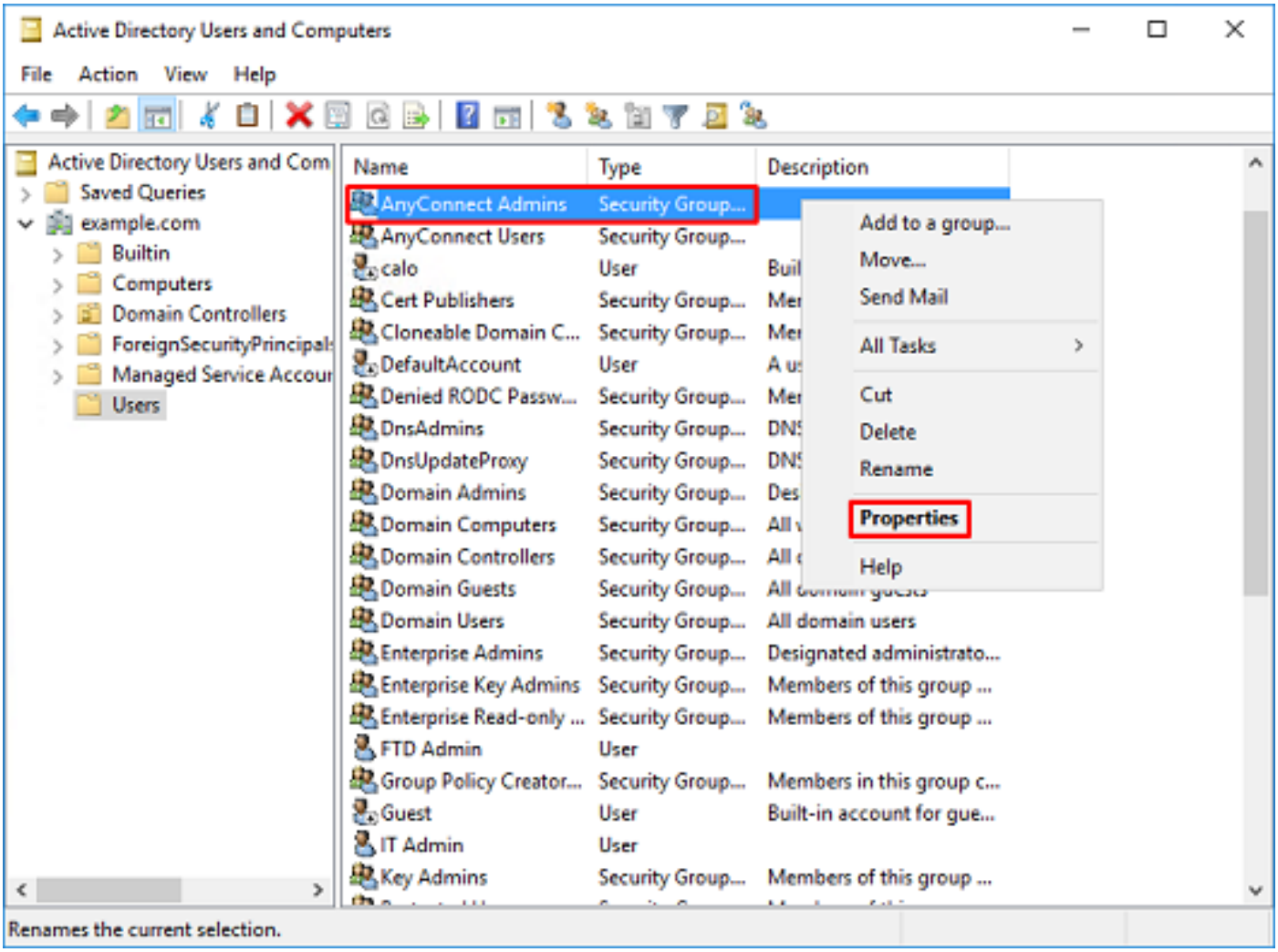
2.図に示すように、**New Object - Group** Wizardをナビゲートします。



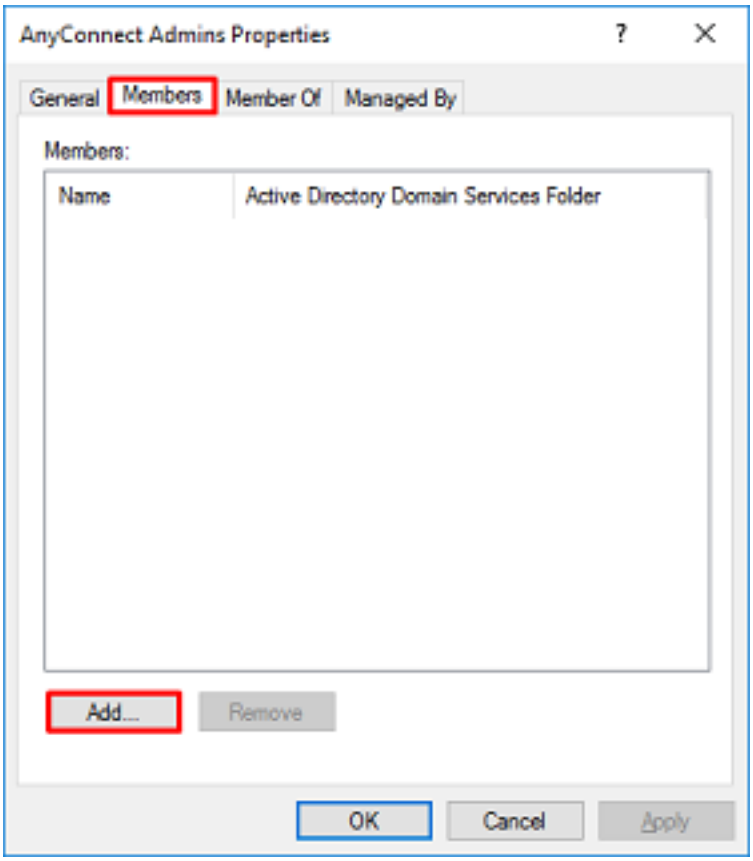
3.グループが作成されたことを確認します。AnyConnect Users**グループ**も作成されています。



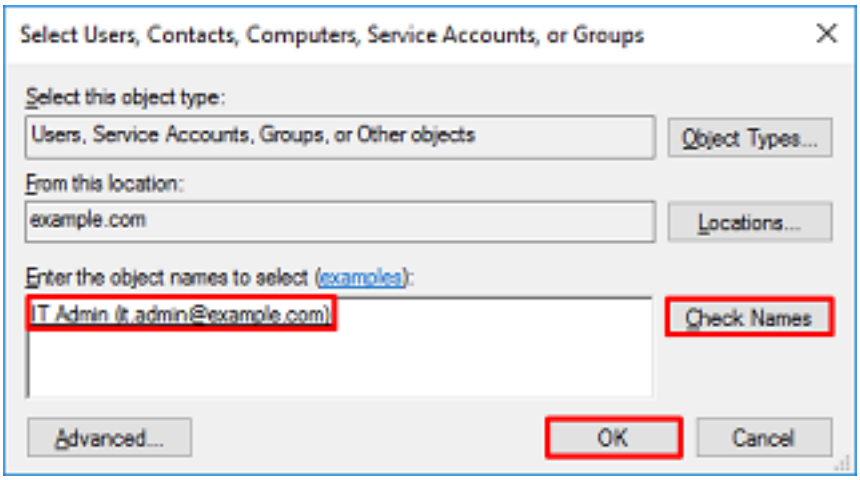
4.ユーザーを追加するグループを右クリックし、「プロパティ」を選択します。この構成では、ユーザーIT Adminがグループ**AnyConnect Admins**に追加され、ユーザーTest Userがグループ**AnyConnect Users**に追加されます。



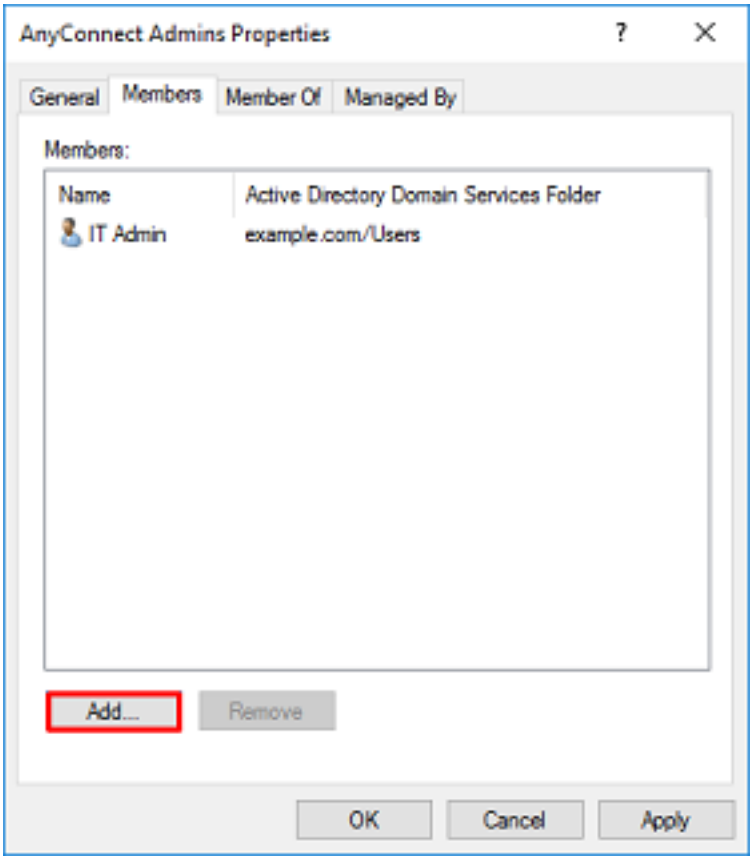
5.図に示すように、[メンバ]タブをクリックし、[追加]をクリックします。



フィールドにユーザを入力し、[Check Names]ボタンをクリックして、ユーザが見つかったことを確認します。確認したら、[OK]をクリックします。

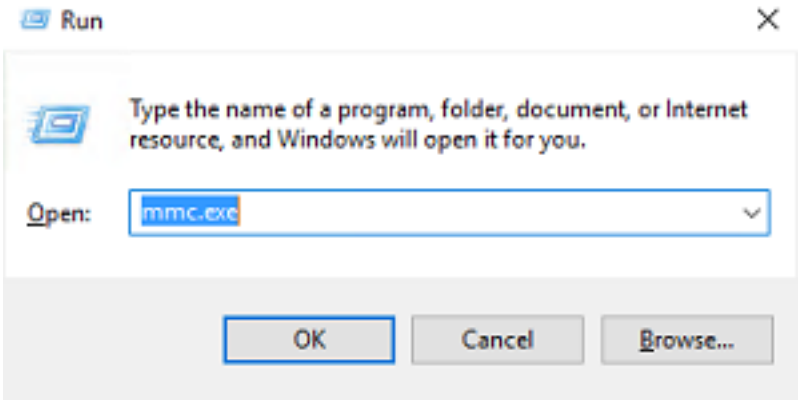


正しいユーザーが追加されていることを確認し、[OK]ボタンをクリックします。同じ手順を使用して、ユーザTest UserをグループAnyConnect Usersに追加します。

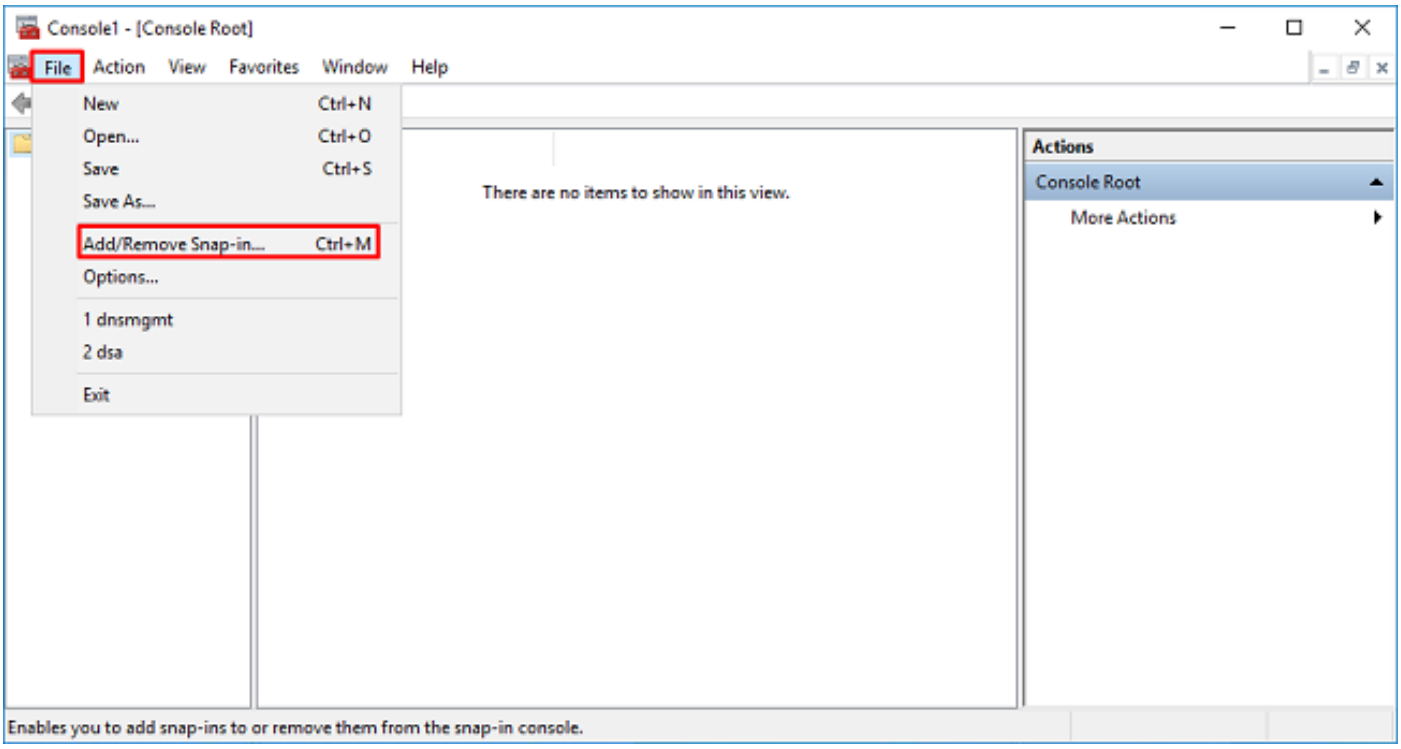


LDAPS SSL証明書ルートのコピー（LDAPSまたはSTARTTLSでのみ必要）

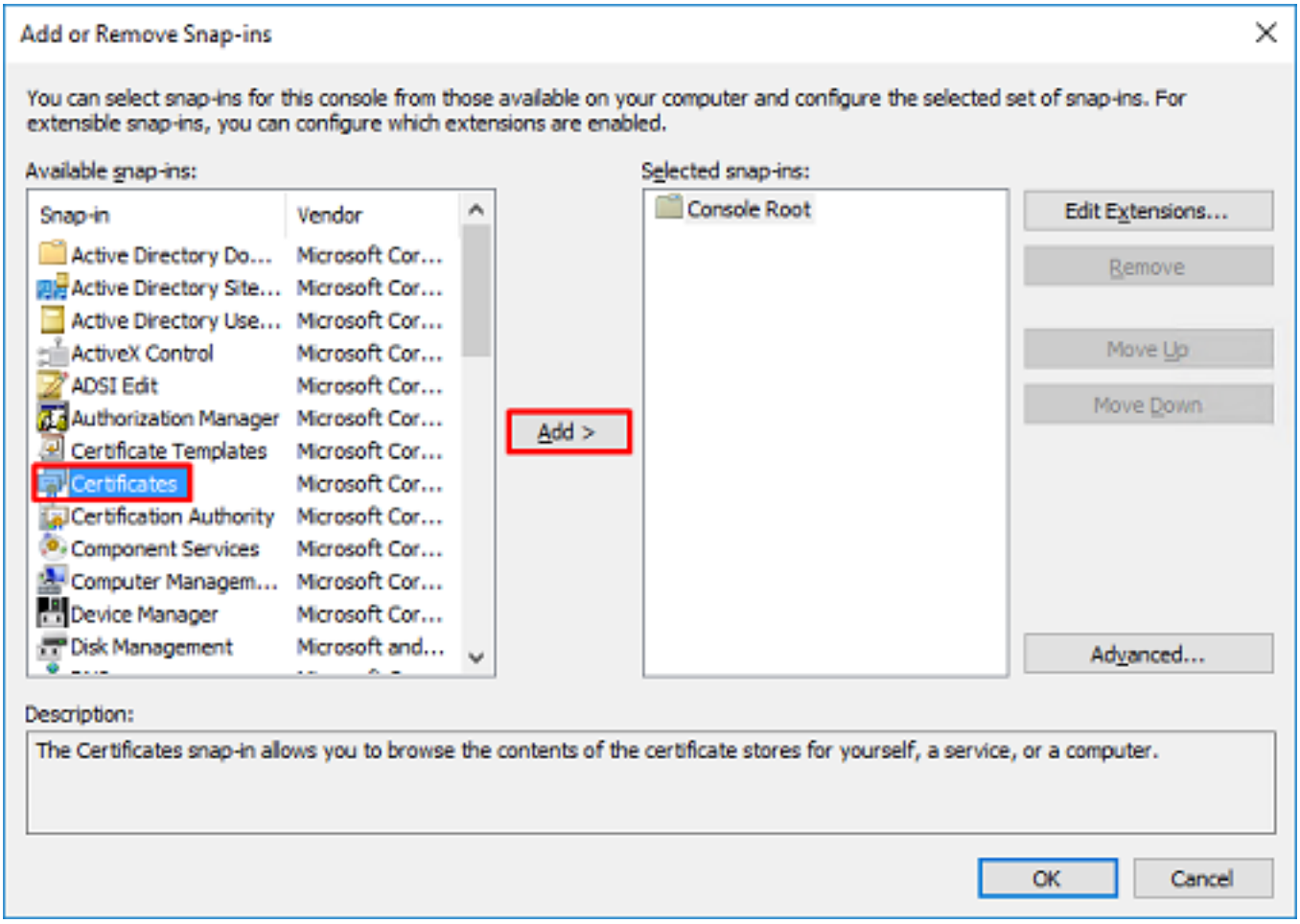
1. Win+Rを押し、mmc.exeと入力します。[OK] をクリックします。



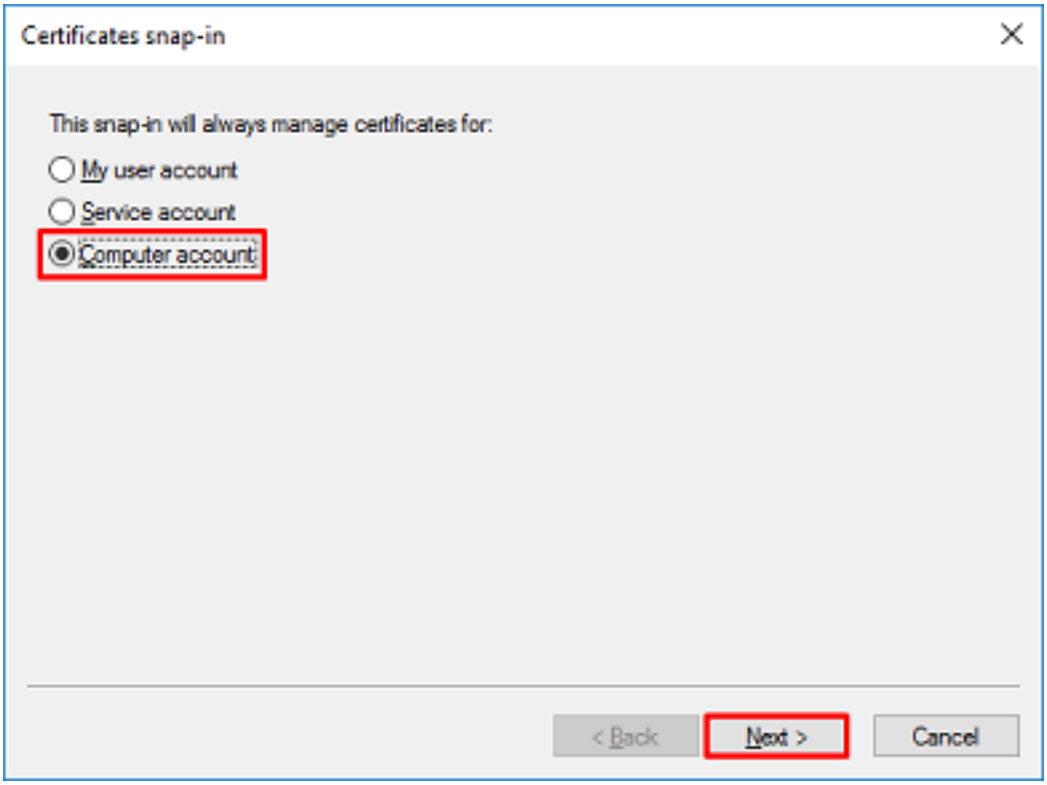
2. [ファイル] > **[スナップインの追加と削除...]に移動します。** 図に示すように



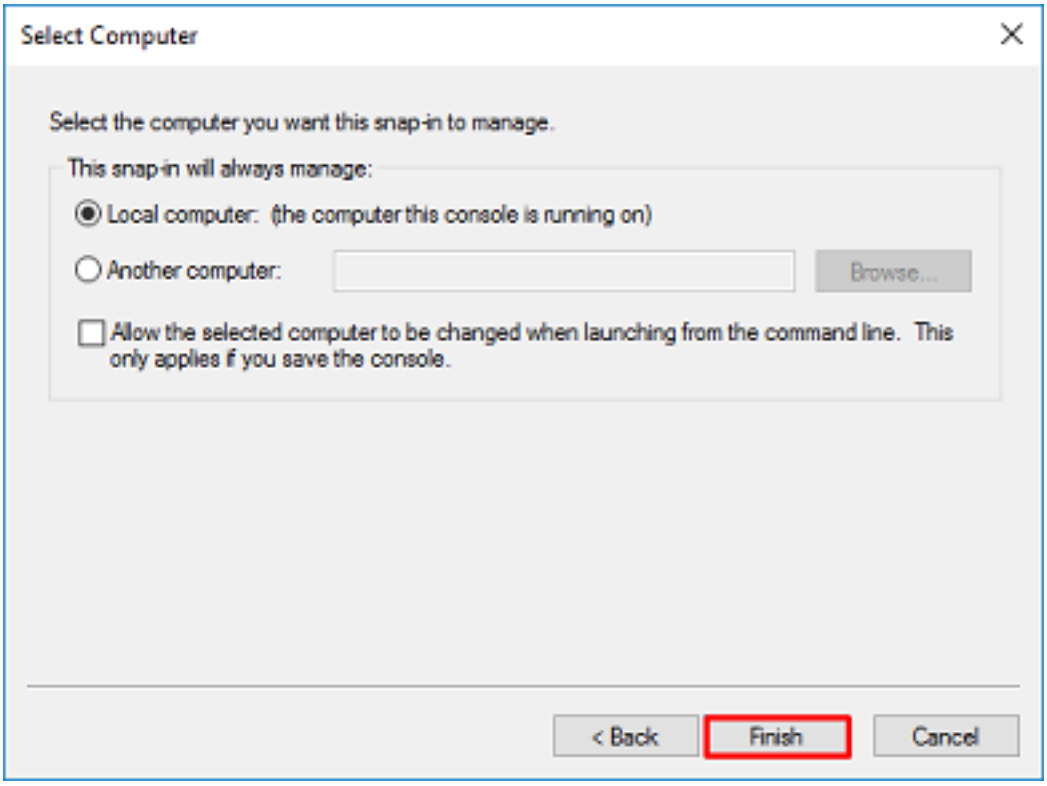
3.使用可能なスナップインの下で、[証明書]をクリックし、**[追加]をクリックします。**



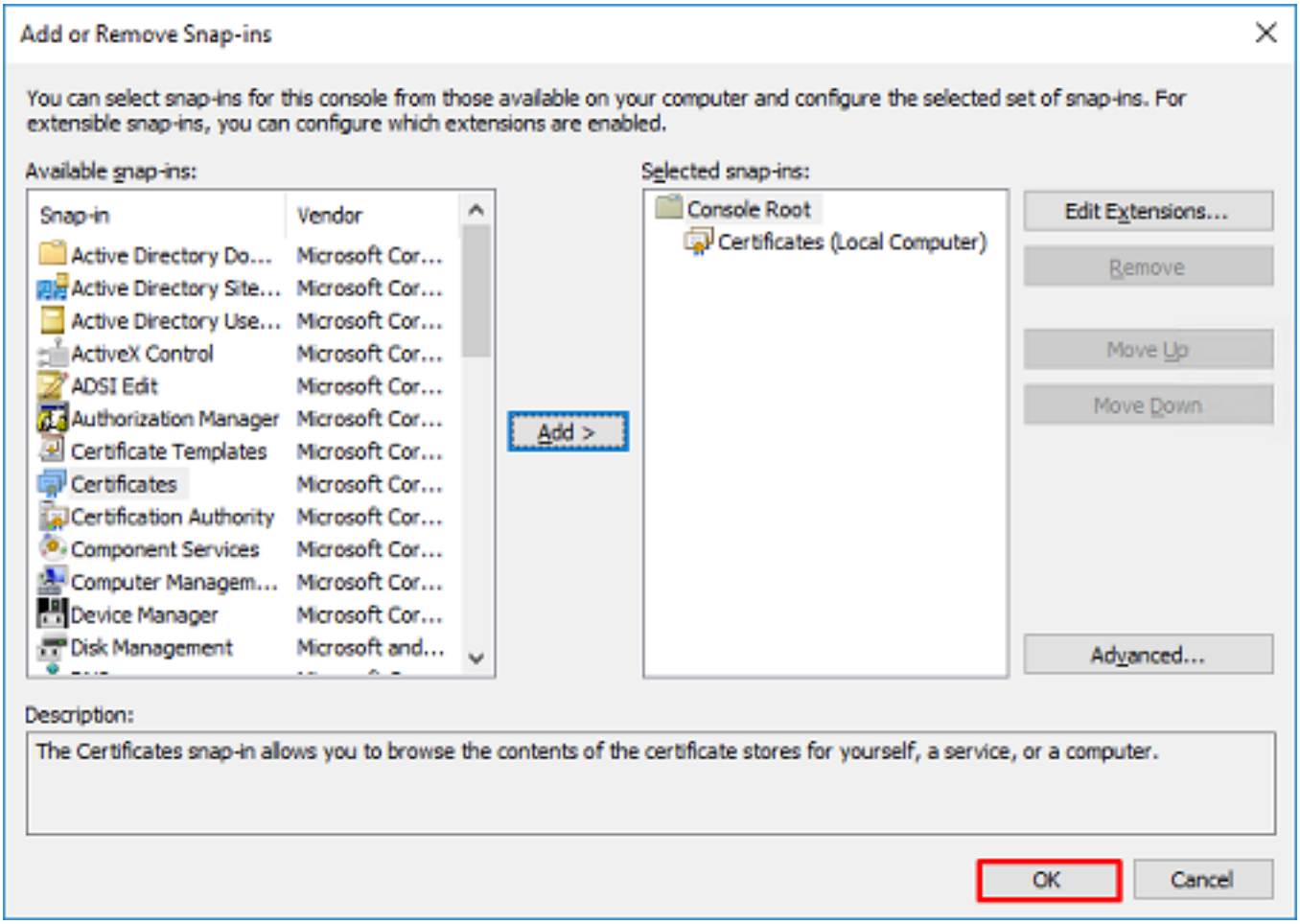
4.図に示すように、[コンピュータアカウント]を選択し、[次へ]をクリックします。



[Finish] をクリックします。



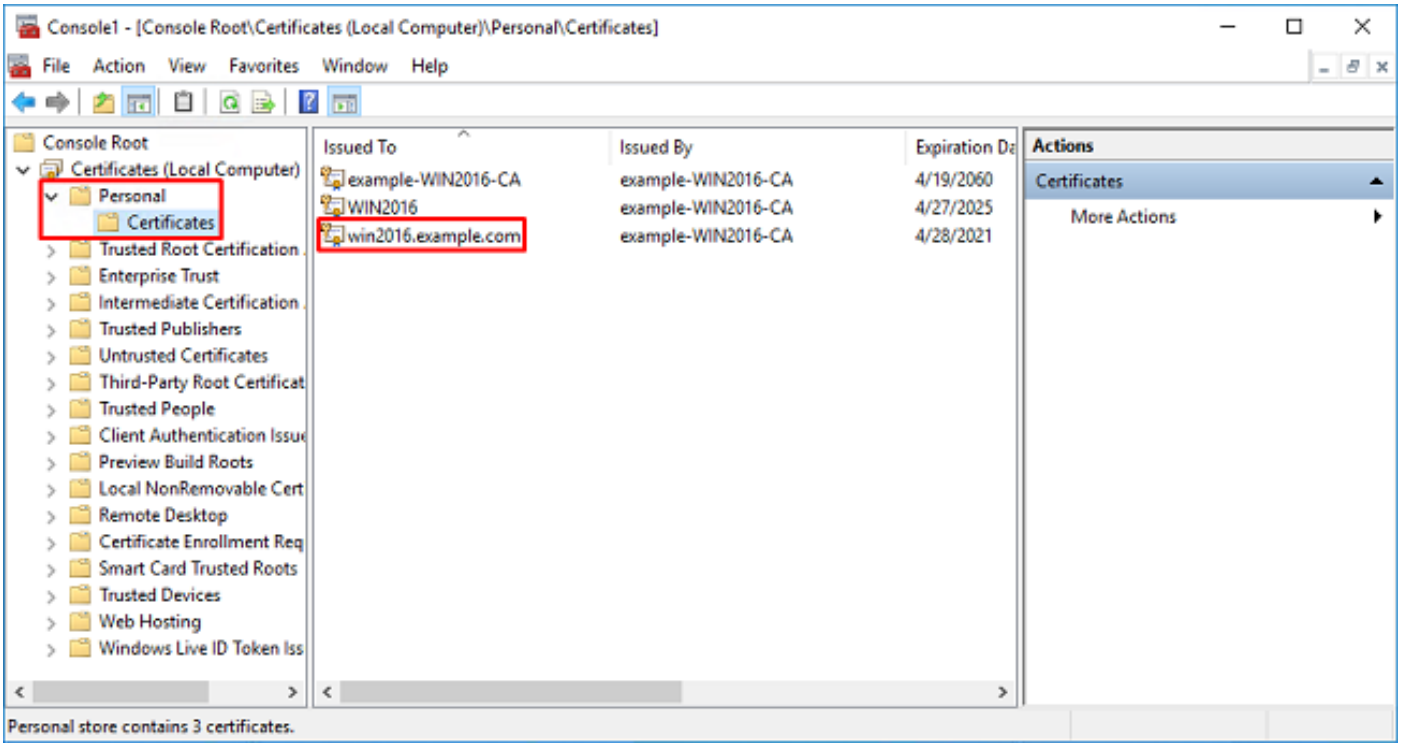
5. 「**OK**」をクリックします。



6. [Personal]フォルダを展開し、[**Certificates**]をクリックします。LDAPSで使用される証明書は、Windowsサーバの完全修飾ドメイン名(FQDN)に発行する必要があります。このサーバには3つの証明書がリストされています。

- example-WIN2016-CAとの間で発行されるCA証明書。
- example-WIN2016-CAによってWIN2016に発行されたID証明書。
- example-WIN2016-CAによってwin2016.example.comに発行されたID証明書。

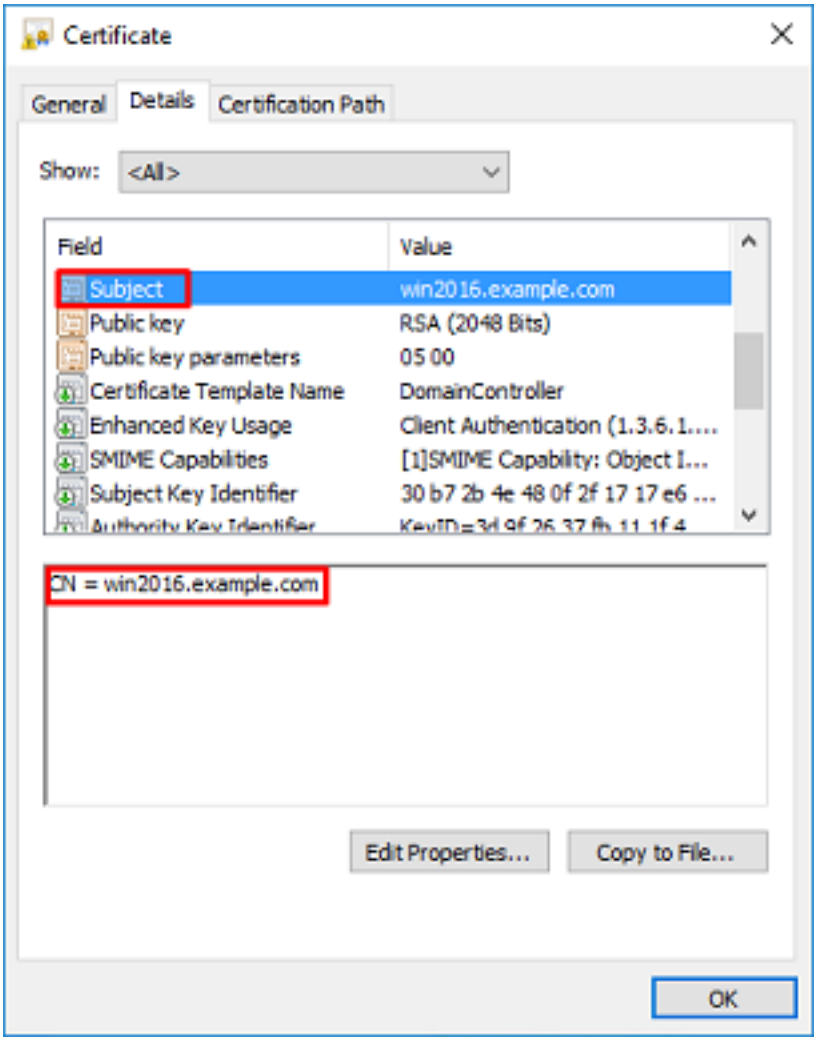
この設定ガイドでは、FQDNはwin2016.example.comであるため、最初の2つの証明書はLDAPS SSL証明書として使用するには有効ではありません。win2016.example.comに発行されるID証明書は、Windows Server CAサービスによって自動的に発行された証明書です。証明書をダブルクリックして詳細を確認します。

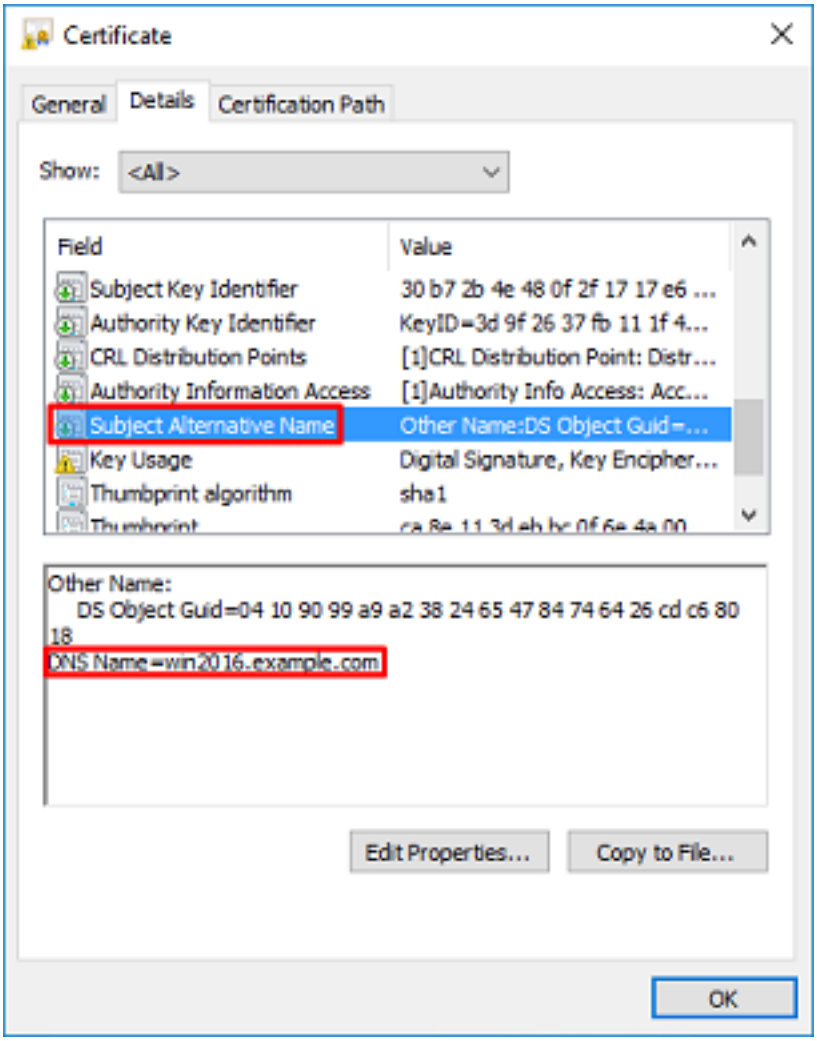


7. LDAPS SSL証明書として使用するには、証明書が次の要件を満たしている必要があります。

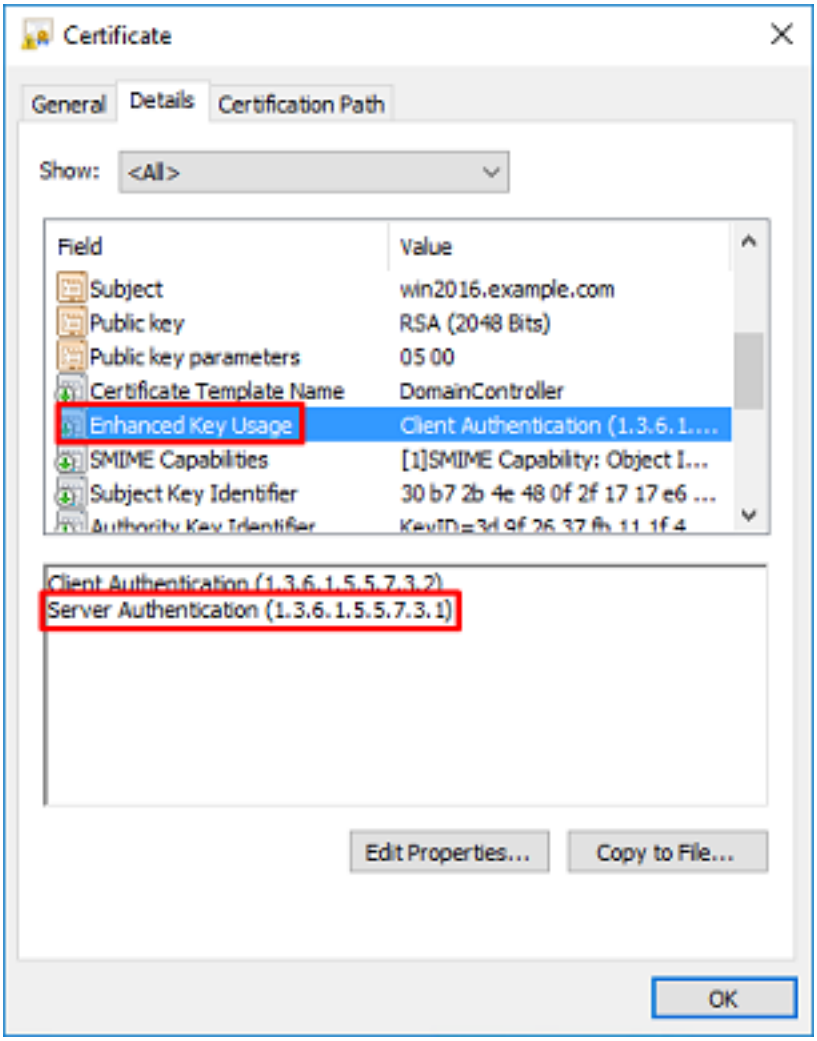
- 共通名またはDNSサブジェクト代替名は、Windows ServerのFQDNと一致します。
- 証明書の[Enhanced Key Usage]フィールドに[Server Authentication]が表示されます。

証明書の[Details]タブの[Subject] と[Subject Alternative Name] に、FQDN **win2016.example.comが表示されます。**

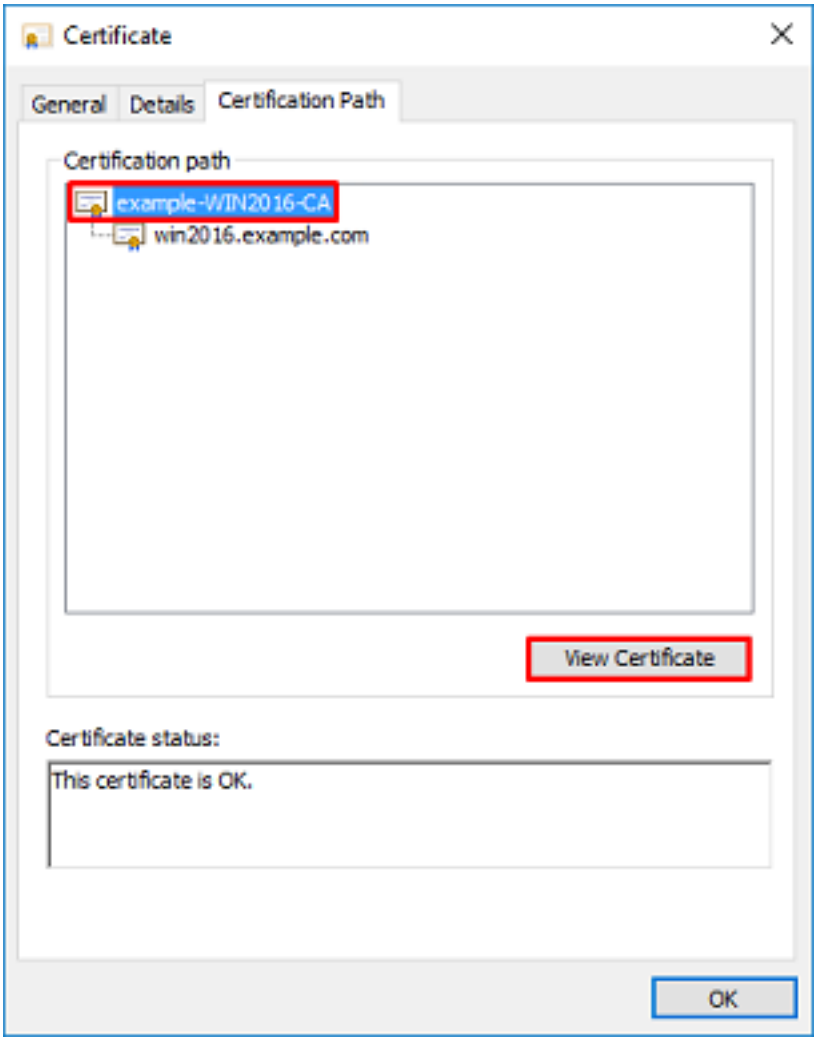

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
win2016.example.com
Public key
RSA (2048 Bits)
Public key parameters
05 00
Certificate Template Name
DomainController
Enhanced Key Usage
Client Authentication (1.3.6.1....
SMIME Capabilities
[1]SMIME Capability: Object I...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



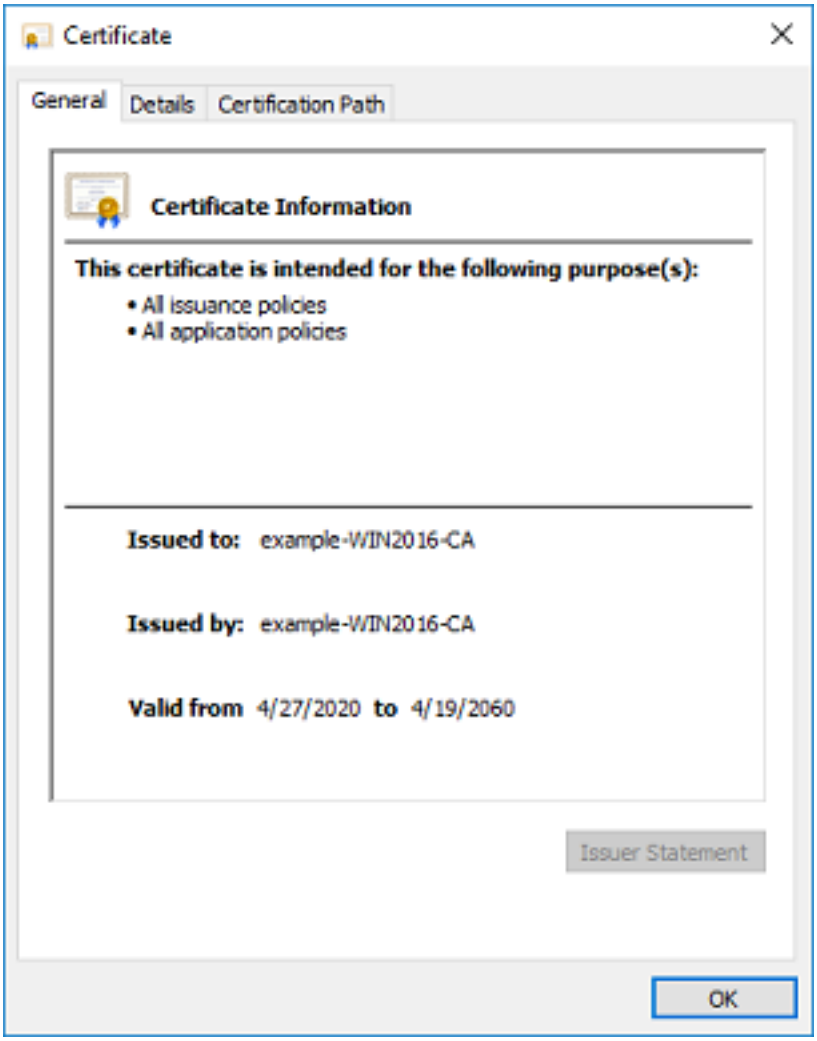
[Enhanced Key Usage] の下に**[Server Authentication]が表示されています。**



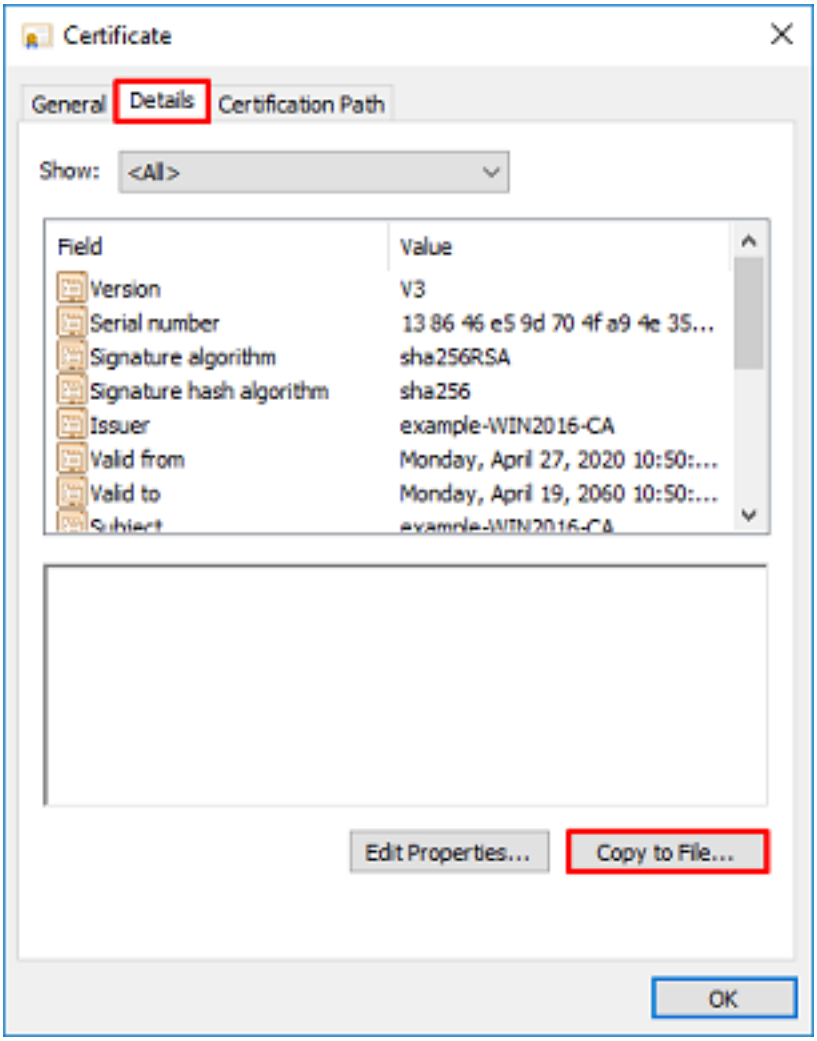
8.確認したら、[Certification Path]タブに**移動します**。ルートCA証明書にする証明書の一番上をクリックし、[**View Certificate**]ボタンをクリックします。



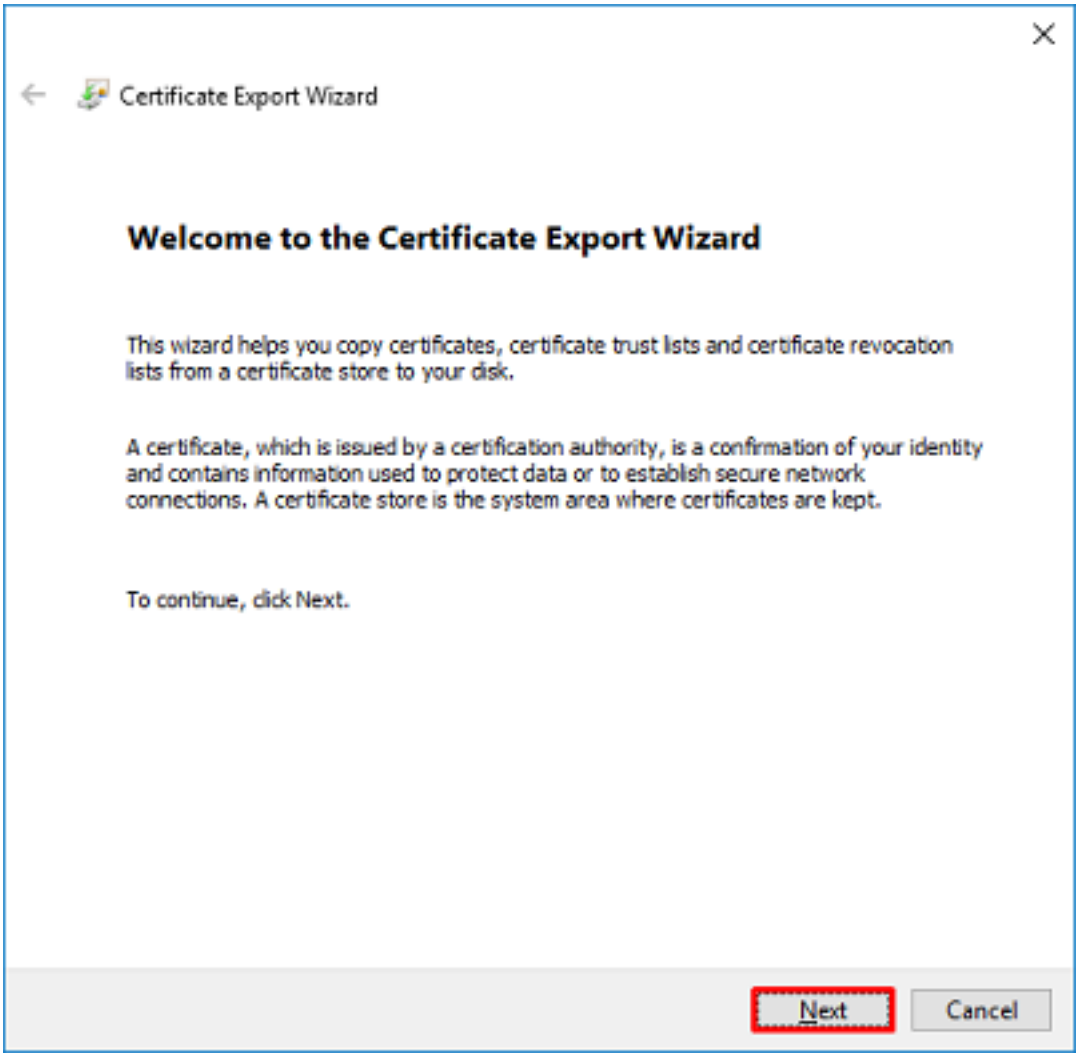
9.これにより、ルートCA証明書の証明書の詳細が開きます。



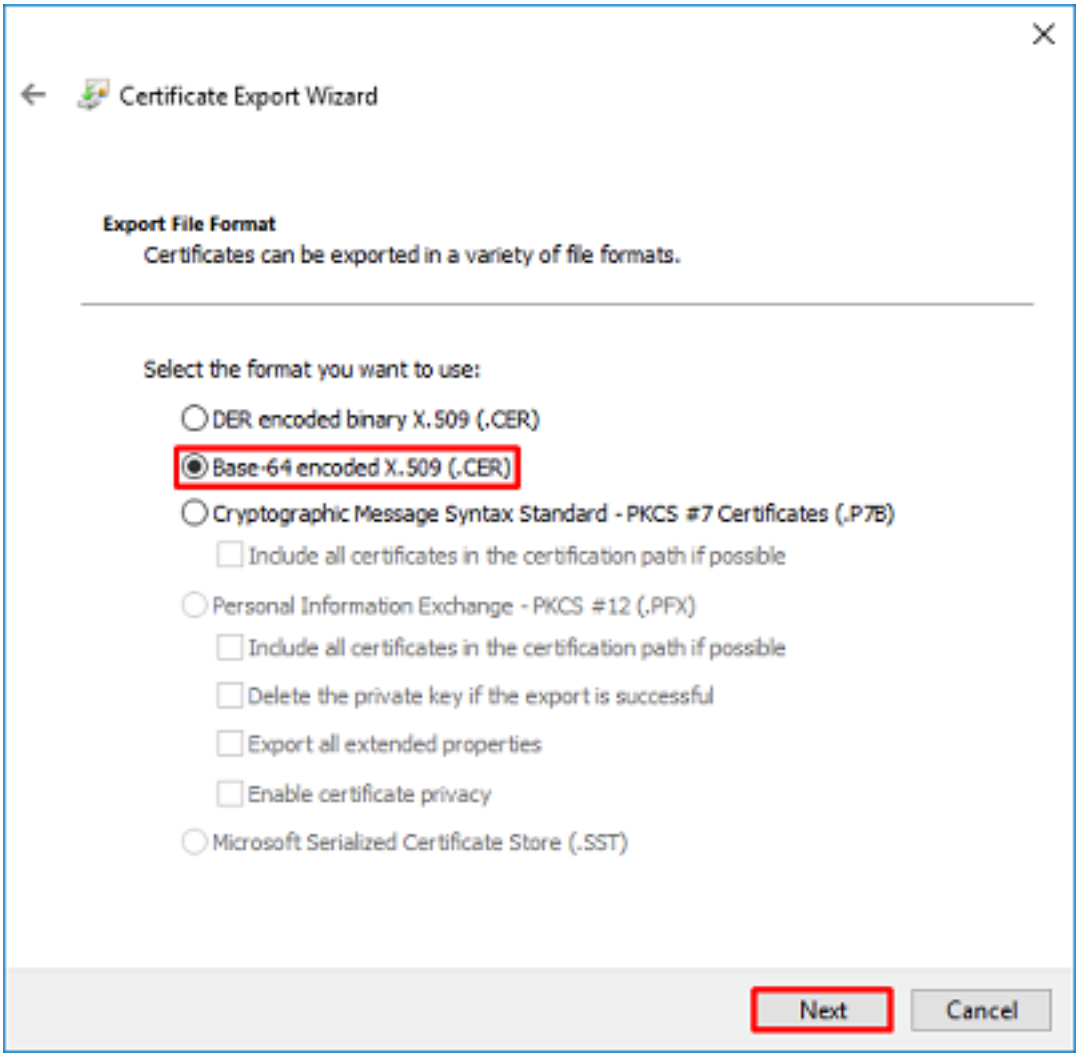
10. [詳細]タブを**開き**、[ファイル**にコピー...]をクリックします。** 図に示すように



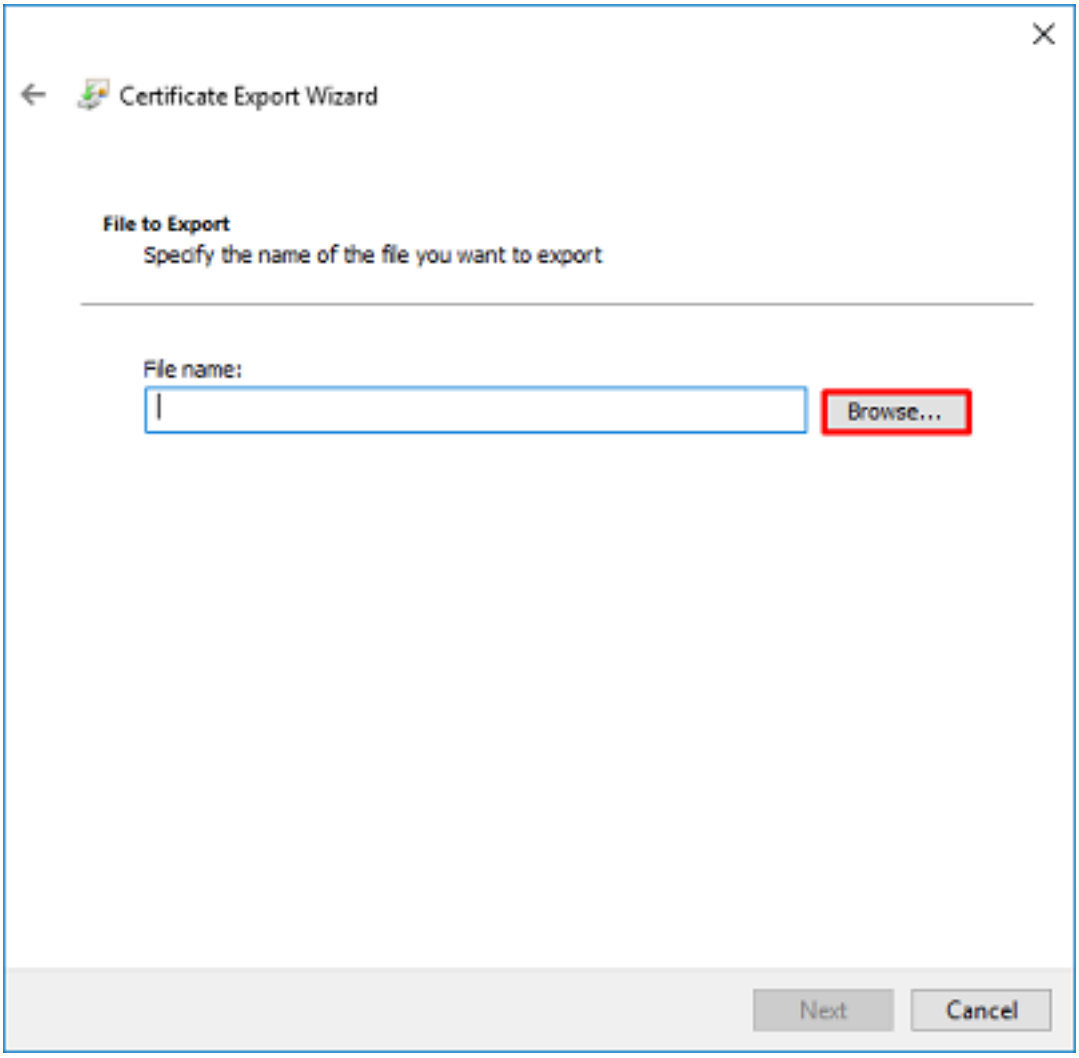
11.ルートCAをPEM形式でエクスポートする証明書エクスポートウィザードをナビゲートします。

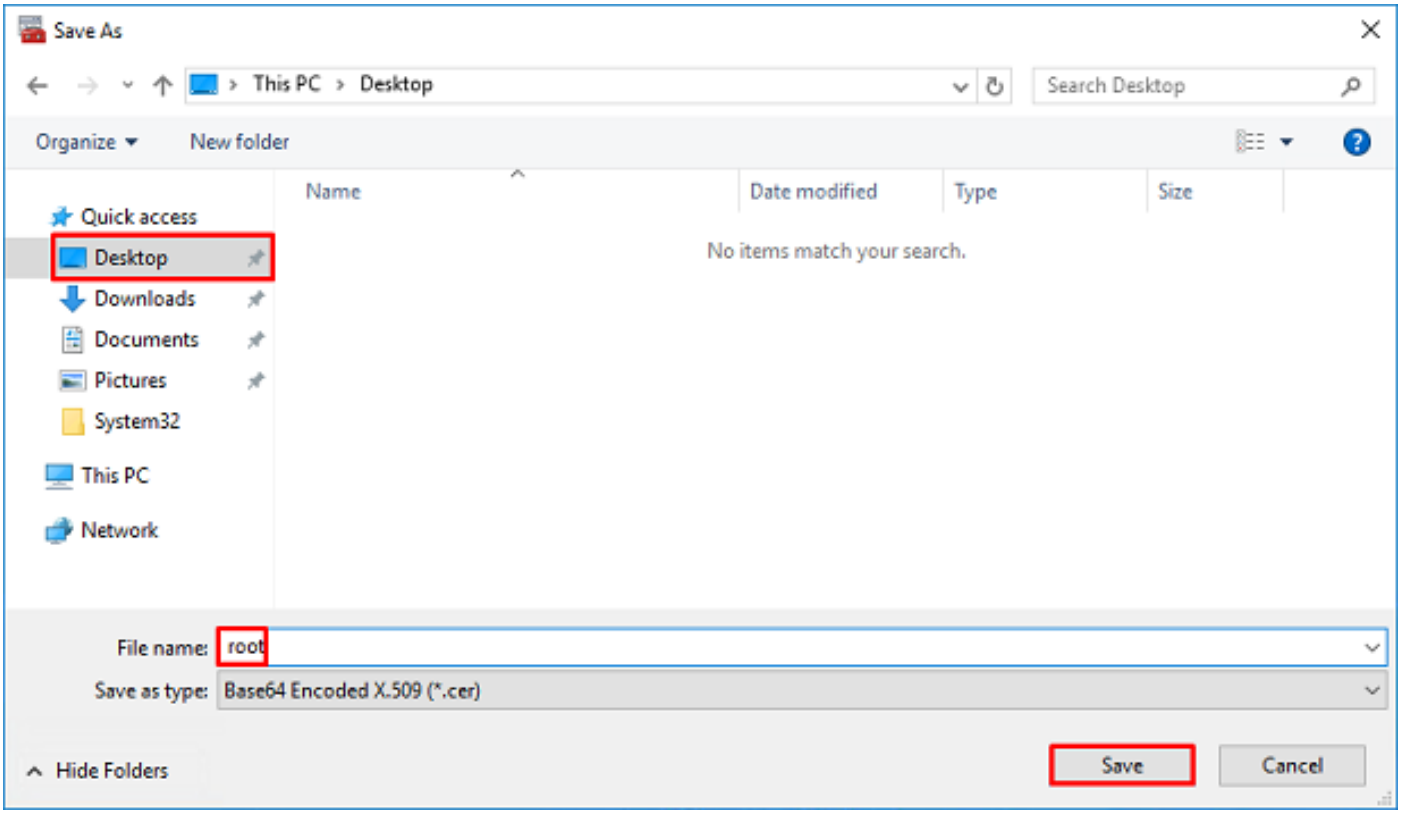


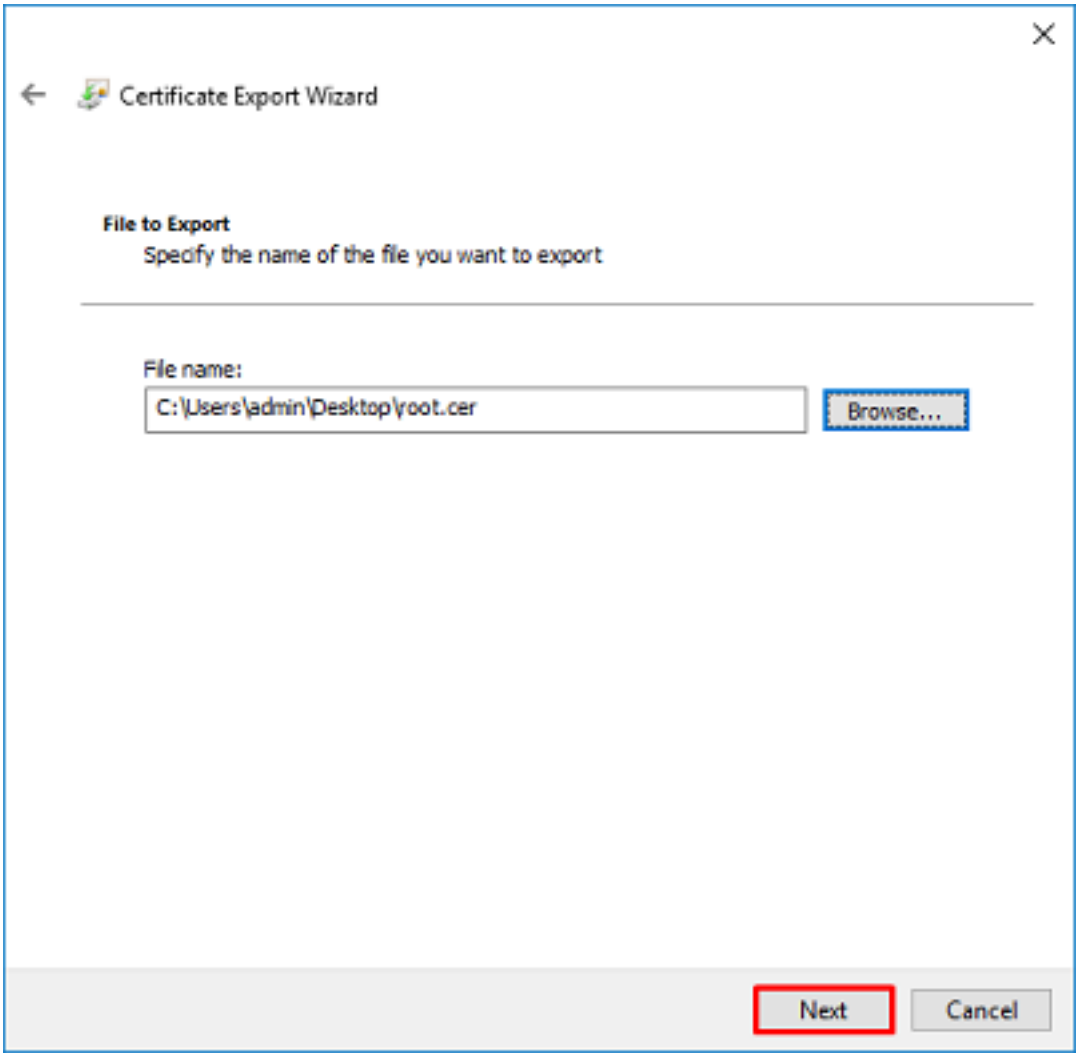
12. **Base-64 encoded X.509を選択します。**



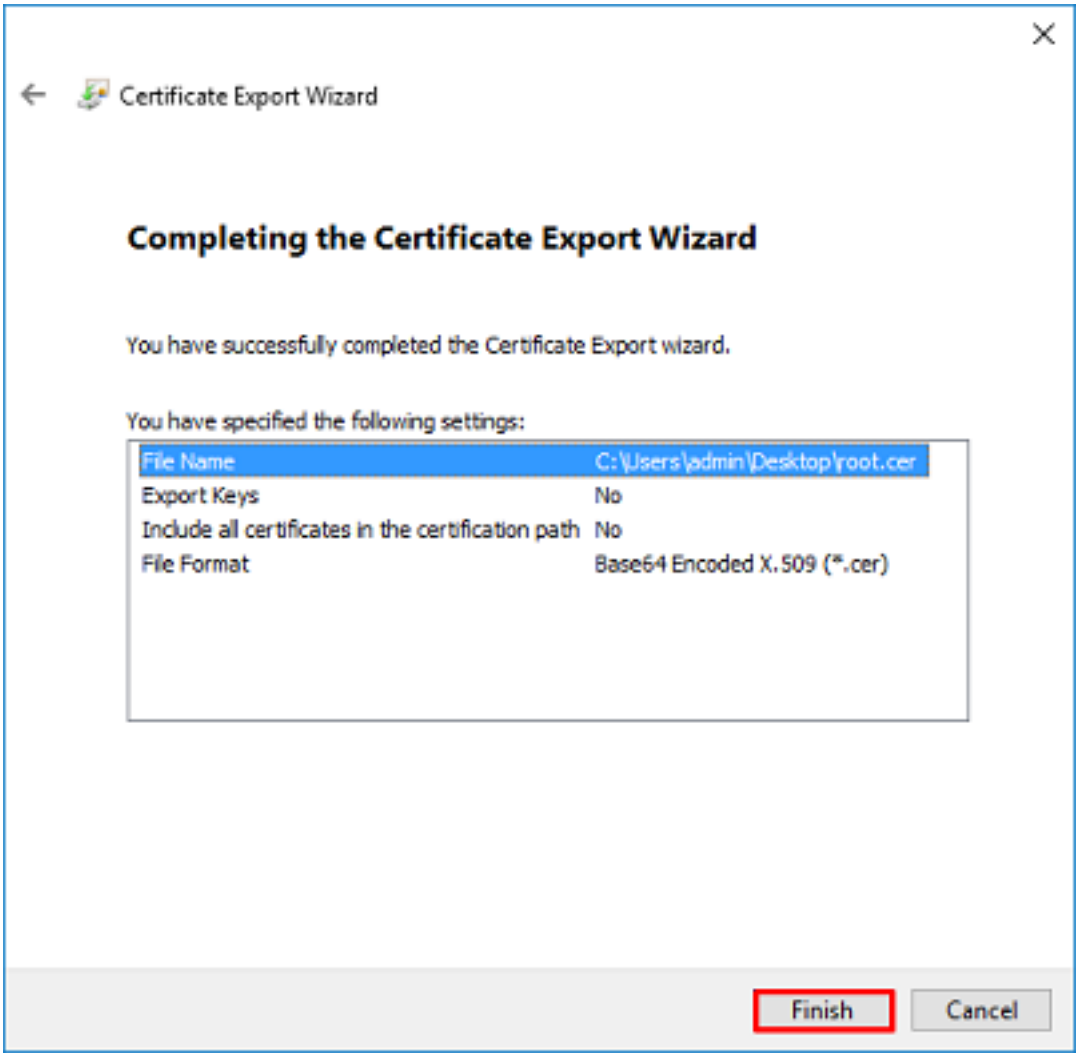
13.ファイルの名前とエクスポート先を選択します。


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


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



14. 「完了」をクリックします。



15.ここで、場所に移動し、メモ帳などのテキストエディタで証明書を開きます。PEM形式の証明書が表示されます。後で保存します。

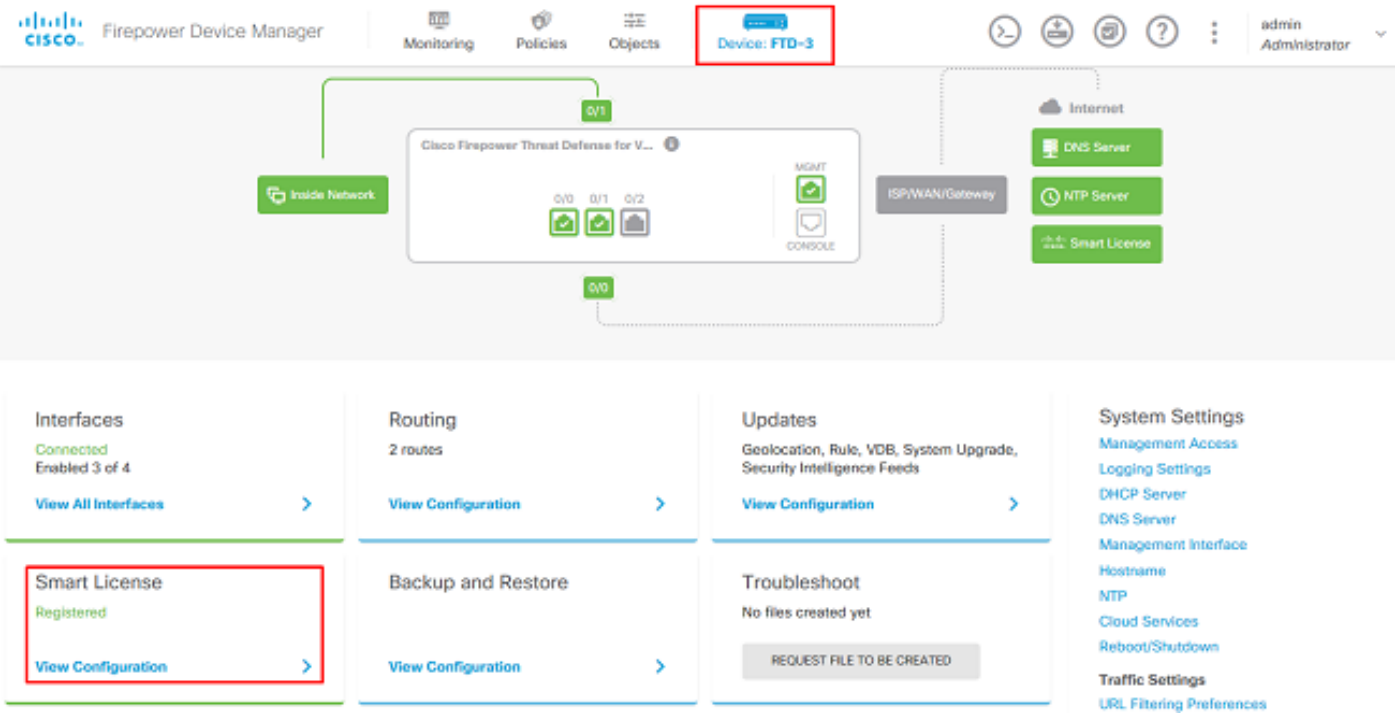
```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV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

FDMの構成

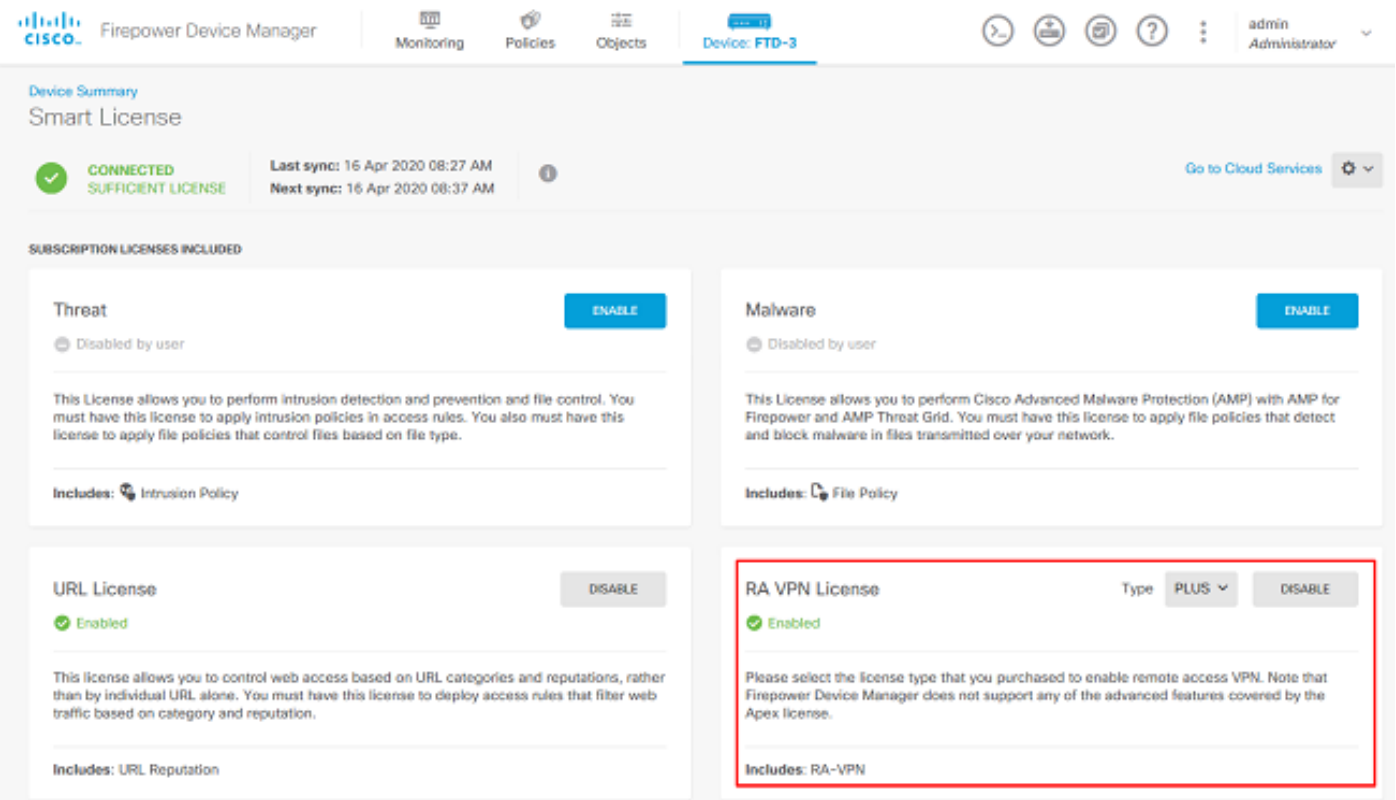
ライセンスの確認

FDMでAnyConnectを設定するには、FTDをスマートライセンスサーバに登録し、有効なPlus、Apex、またはVPN Onlyライセンスをデバイスに適用する必要があります。

1.図に示すように、[Device] > [Smart License]に移動します。



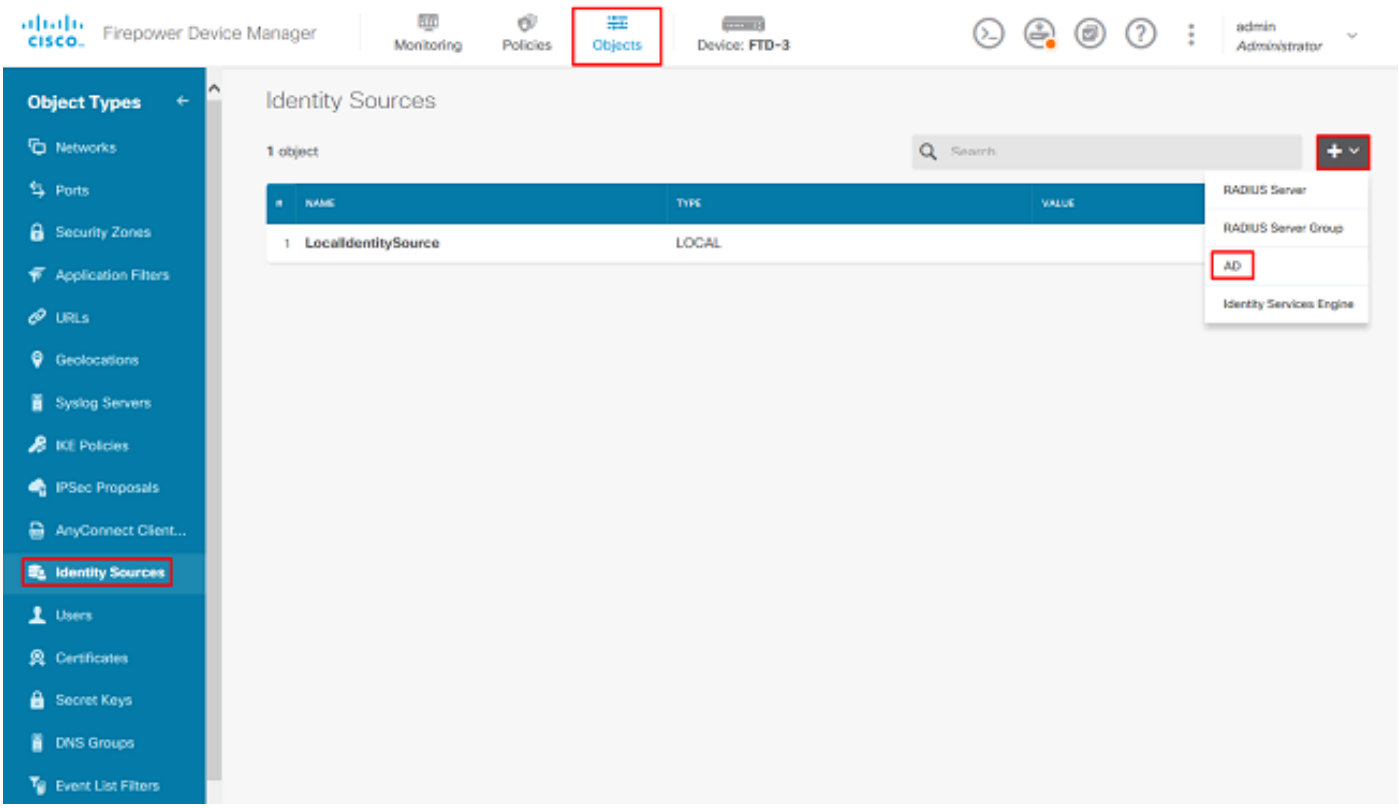
2. FTDがスマートライセンスサーバに登録され、AnyConnect Plux、Apex、またはVPN Onlyライセンスが有効になっていることを確認します。



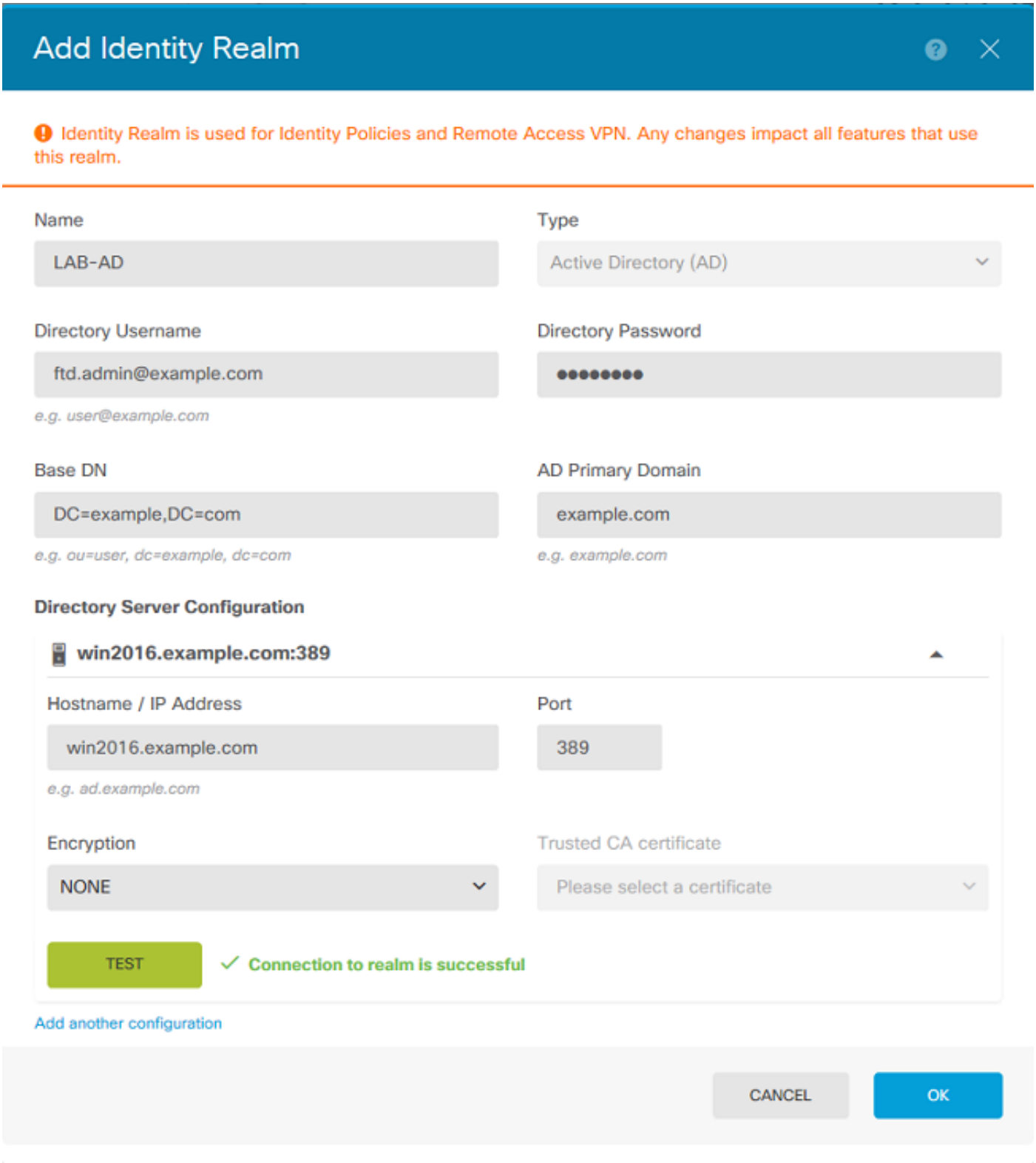
AD IDソースの設定

1. [Objects] > [Identity Sources]に移動し、+記号をクリックし、図に示すように[AD]を選択します

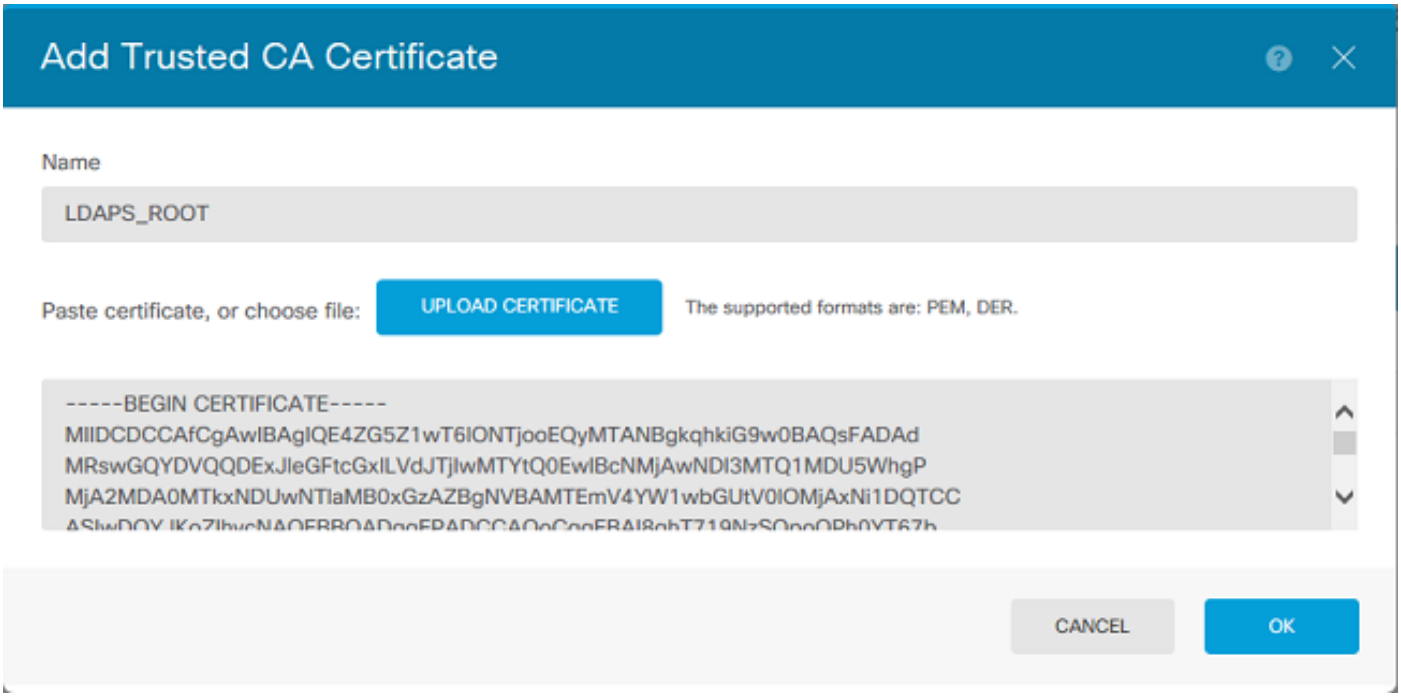
。

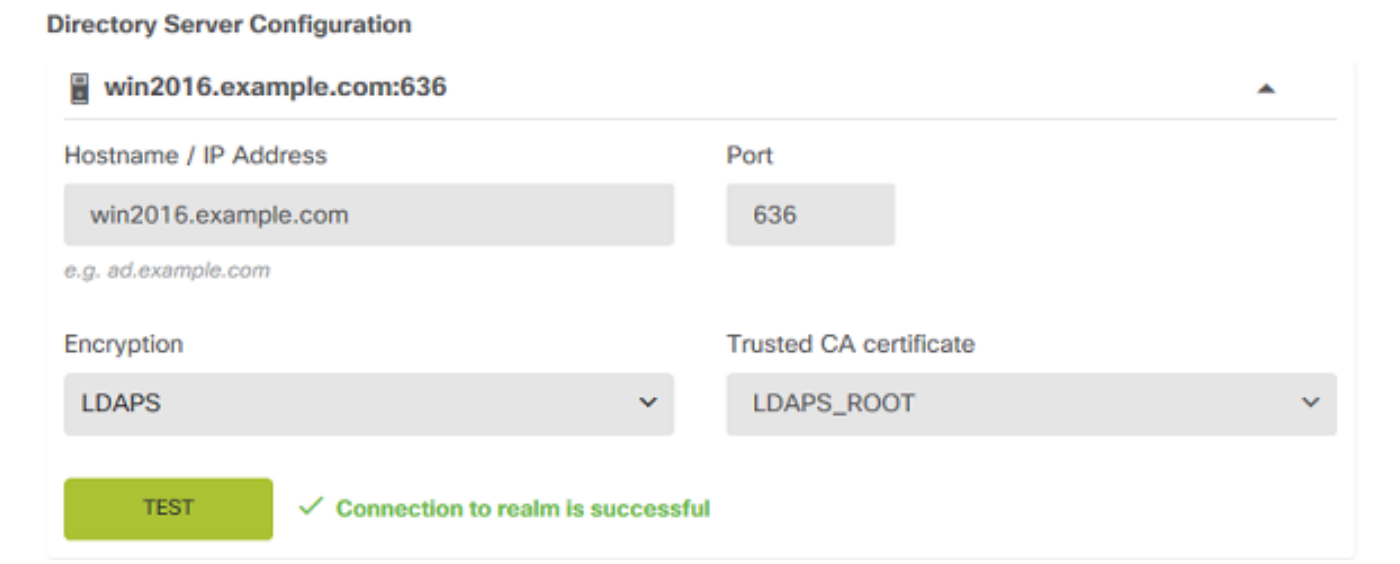


2. Active Directoryサーバの適切な設定に、以前に収集した情報を入力します。IPアドレスの代わりにMicrosoftサーバにホスト名(FQDN)を使用する場合は、**[Objects] > [DNS Group]**で適切なDNSグループを必ず作成してください。次に、**[Device] > [System Settings] > [DNS Server]に移動し、[Management Interface]**および**[Data Interface]**でDNSグループを適用し、DNSクエリに適切な出力インターフェイスを指定して、そのDNSグループをFTDにに適用します。**Test**ボタンをクリックして、FTDの管理インターフェイスから正常な設定と到達可能性を確認します。これらのテストはFTDの管理インターフェイスから開始され、FTDに設定されているルーティング可能インターフェイス（内部、外部、dmzなど）からは開始されないため、正常な（または失敗した）接続ではAnyConnect認証の結果は保証されません。FTDからのLDAP接続のテストの詳細については、「トラブルシューティング」領域の「AAAのテスト」および「パケットキャプチャ」の項を参照してください。



LDAPSまたはSTARTTLSを使用する場合は、適切な暗号化を選択し、信頼できるCA証明書を選択します。ルートCAがまだ追加されていない場合は、**[Create New Trusted CA Certificate]をクリックします**。ルートCA証明書の[Name]を指定し、先ほど収集したPEM形式のルートCA証明書を貼り付けます。

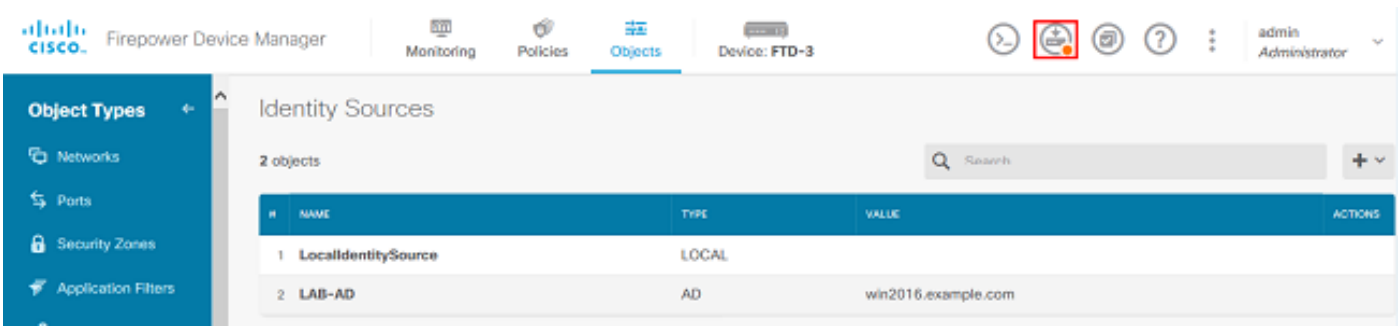




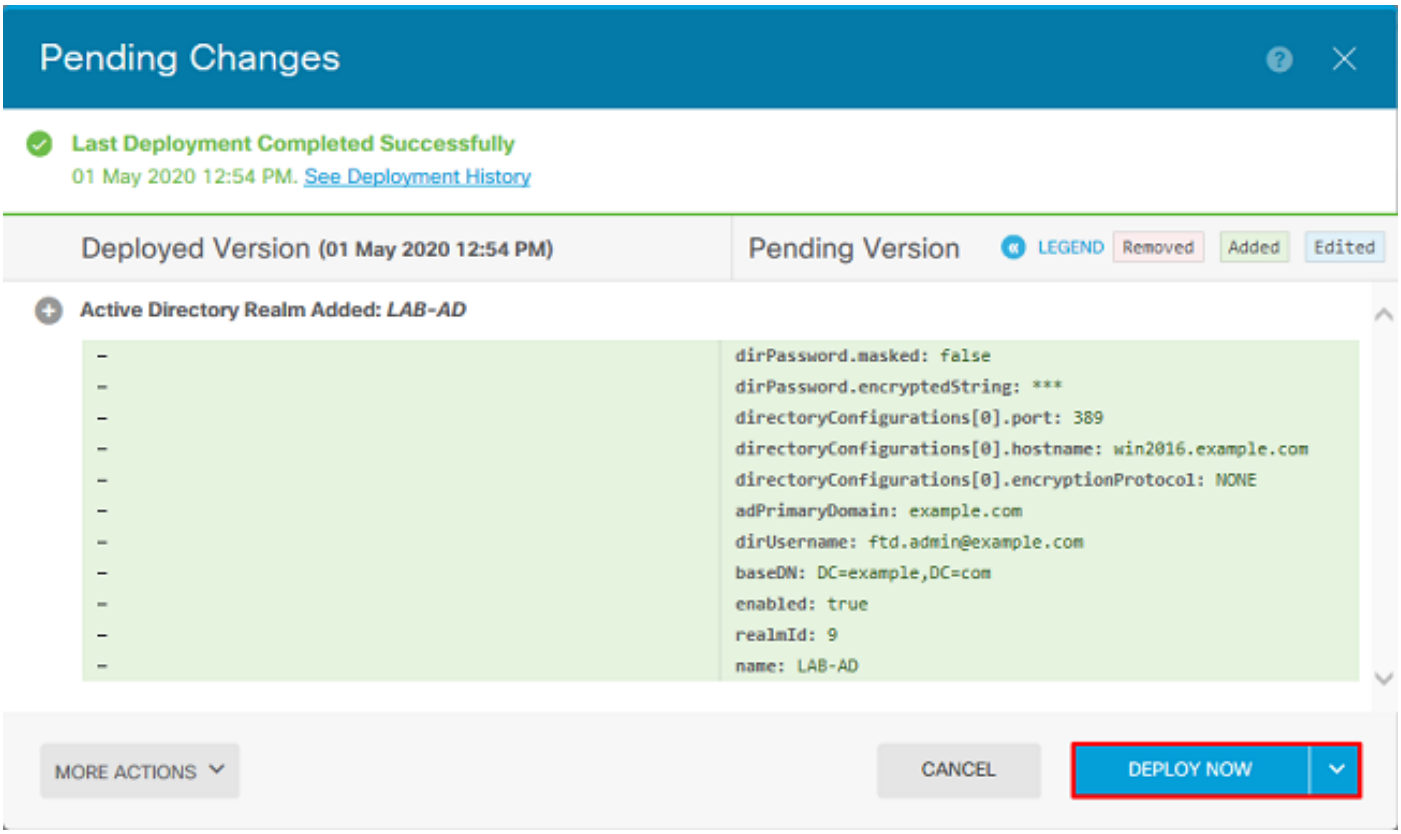
この設定では、次の値が使用されています。

- [Name]：ラボ広告
- [Directory Username]：ftd.admin@example.com
- [Base DN]：dc=example,dc=com
- [AD Primary Domain]：example.com
- [Hostname/IP Address]：win2016.example.com
- [Port]：389

3.図に示すように、右上の**[Pending Changes]**ボタンをクリックします。



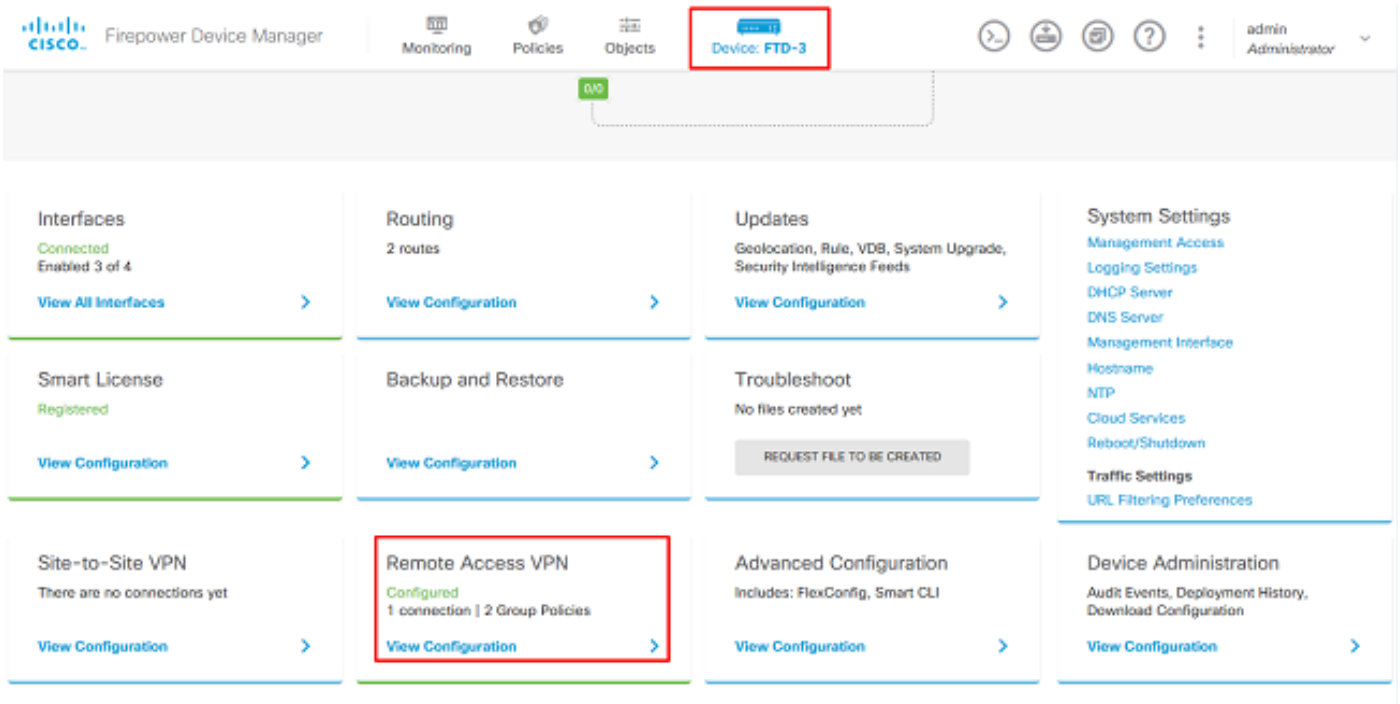
4. [今すぐ展開]ボタンをクリックします。



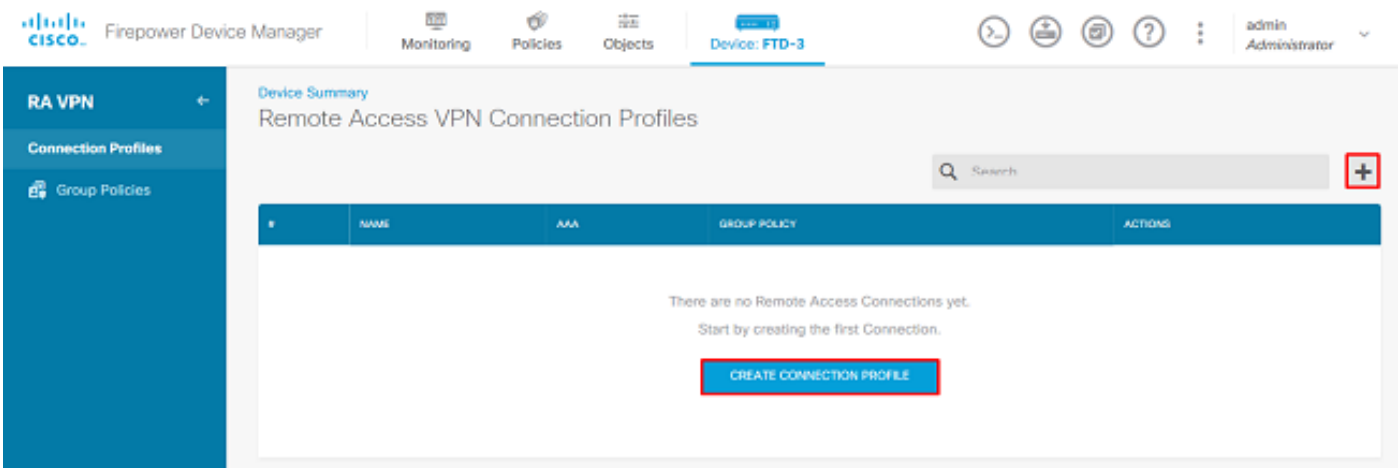
AD認証用のAnyConnectの設定

設定されたAD IDソースを使用するには、AnyConnect設定に適用する必要があります。

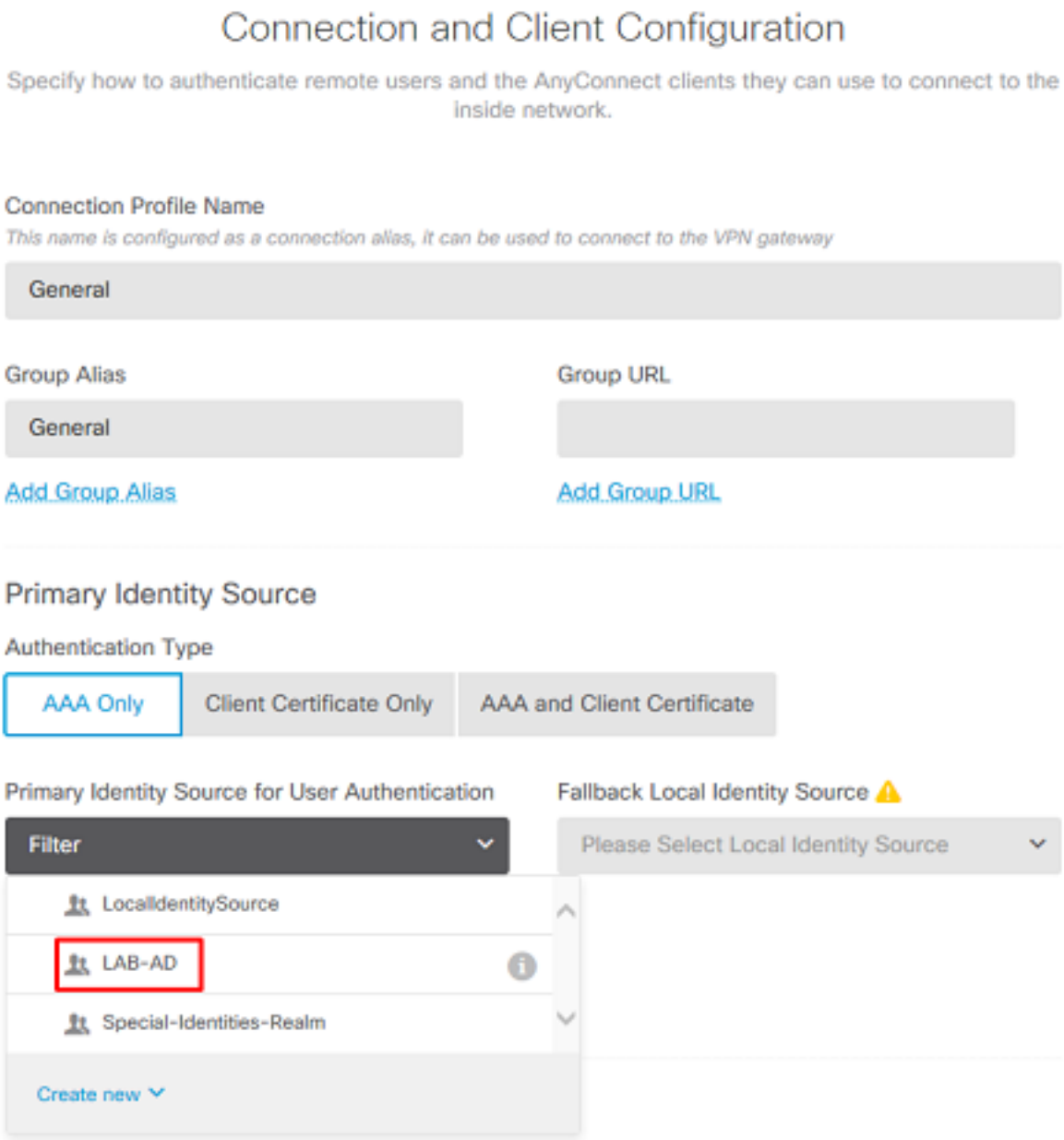
1.図に示すように、[Device] > [Remote Access VPN]に移動します。

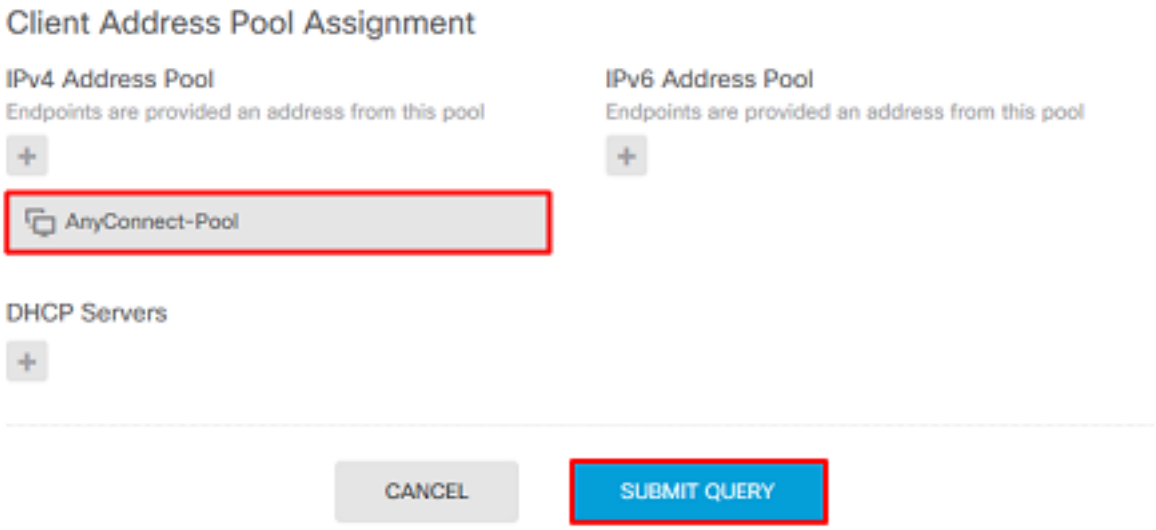


2.図に示すように、+記号または[接続プロファイルの作成]ボタンをクリックします。

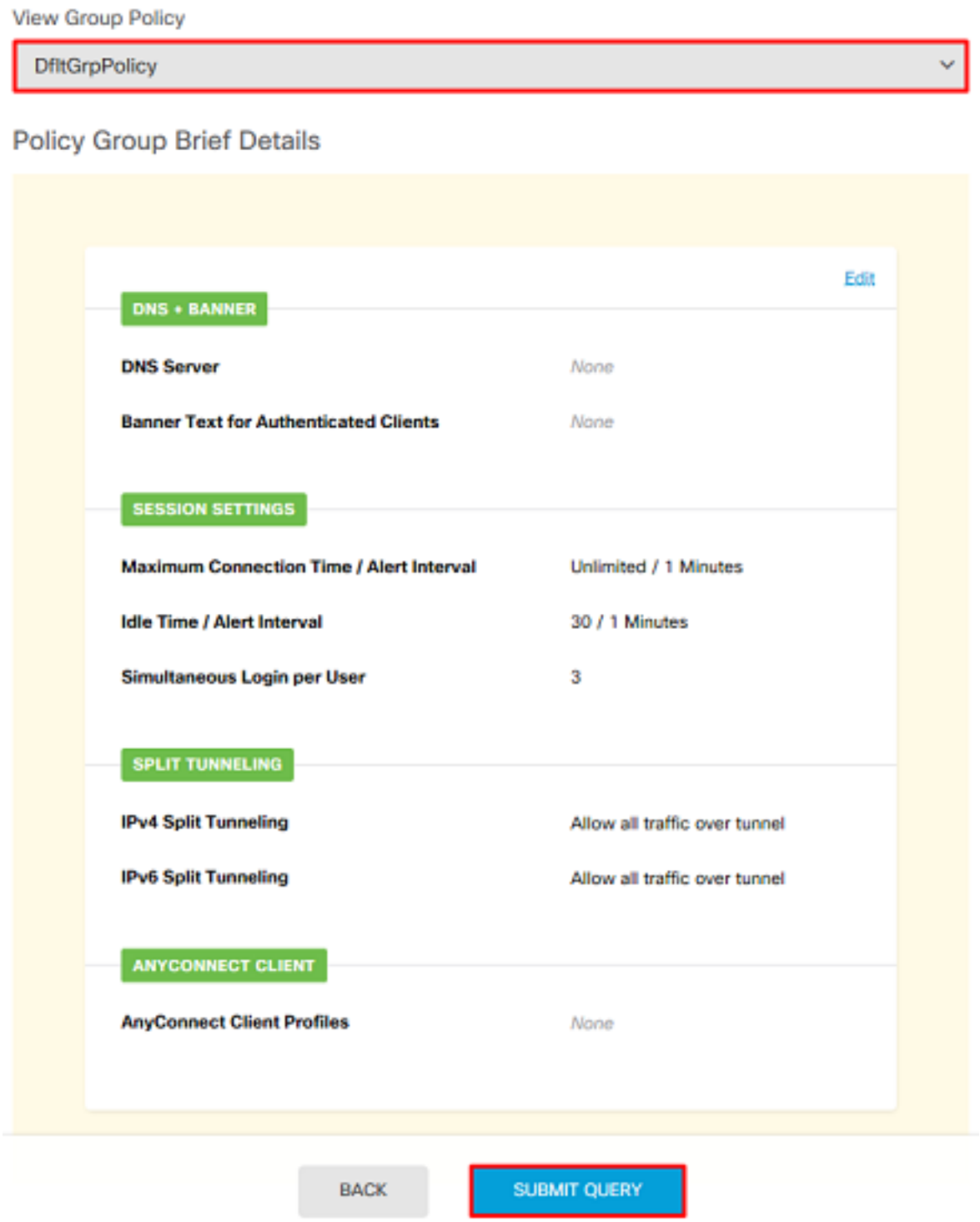


3. [Connection and Client Configuration]セクションで、以前に作成したAD IDソースを選択します。[接続プロファイル名(Connection Profile Name)]や[クライアントアドレスプールの割り当て(Client Address Pool Assignment)]など、他のセクションに適切な値を設定します。完了したら**[Submit Query]**をクリックします。

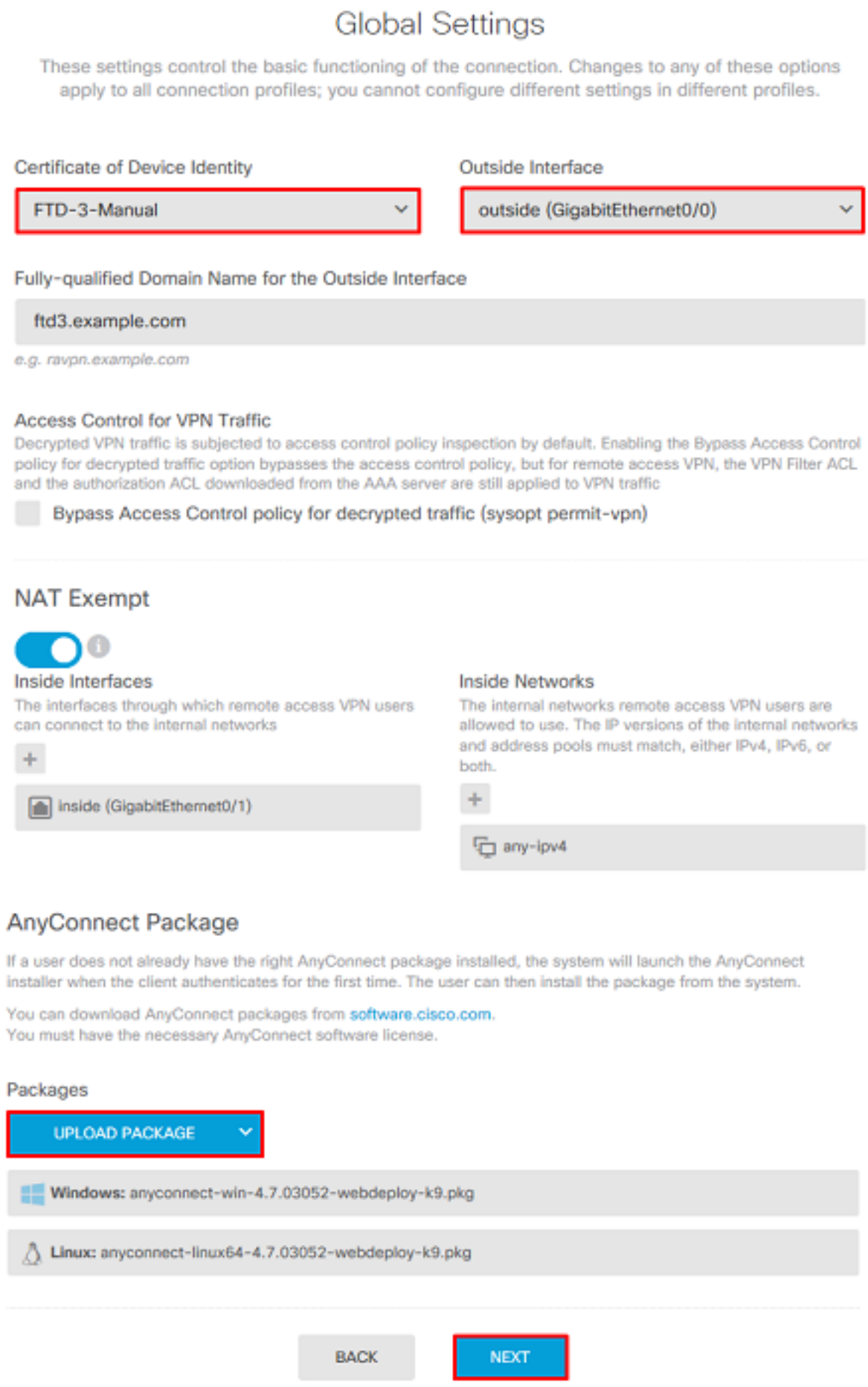




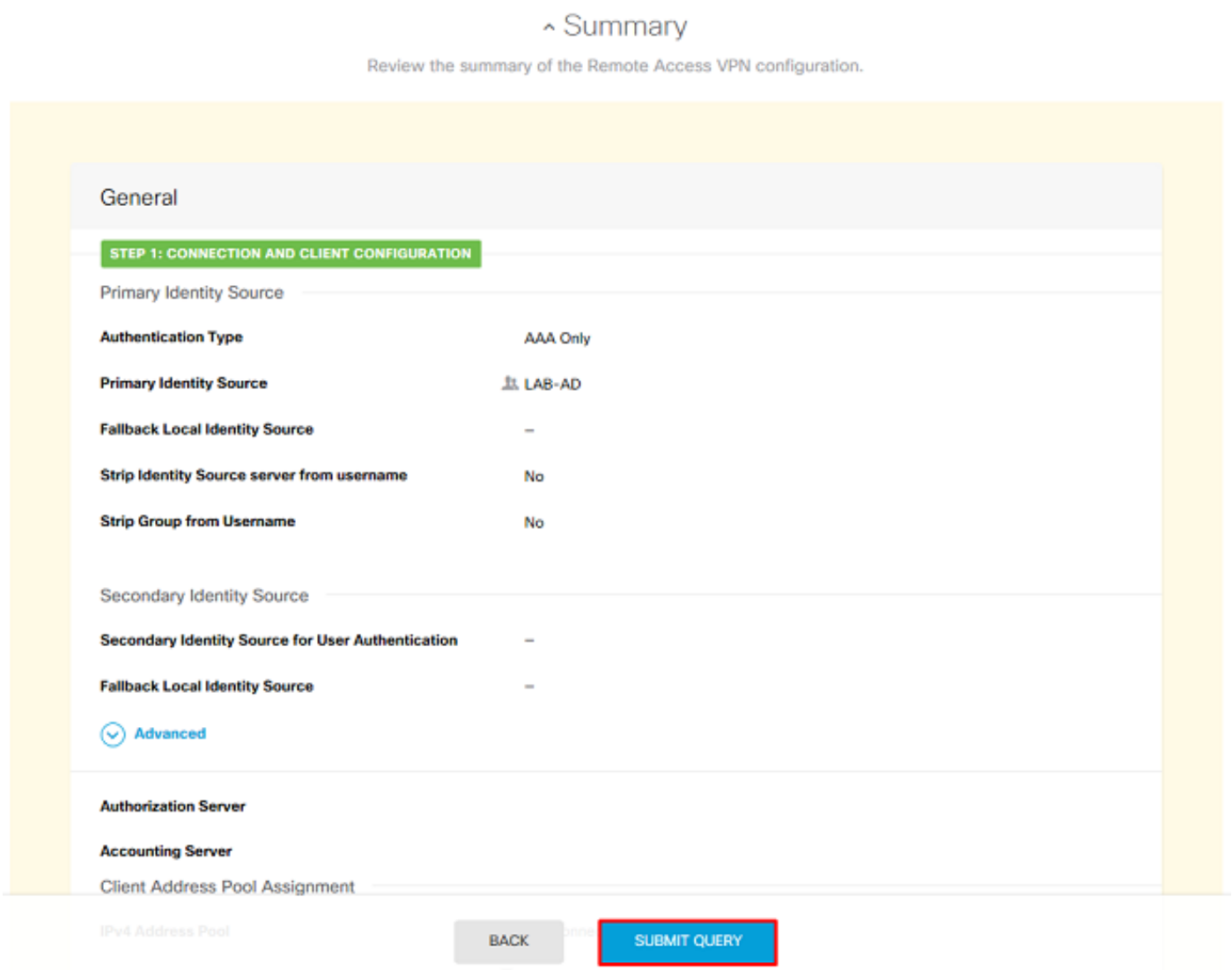
4. [Remote User Experience]セクションで、適切なグループポリシーを選択します。デフォルトでは、DfltGrpPolicy**が使用**されます。ただし、別のものを作成できます。



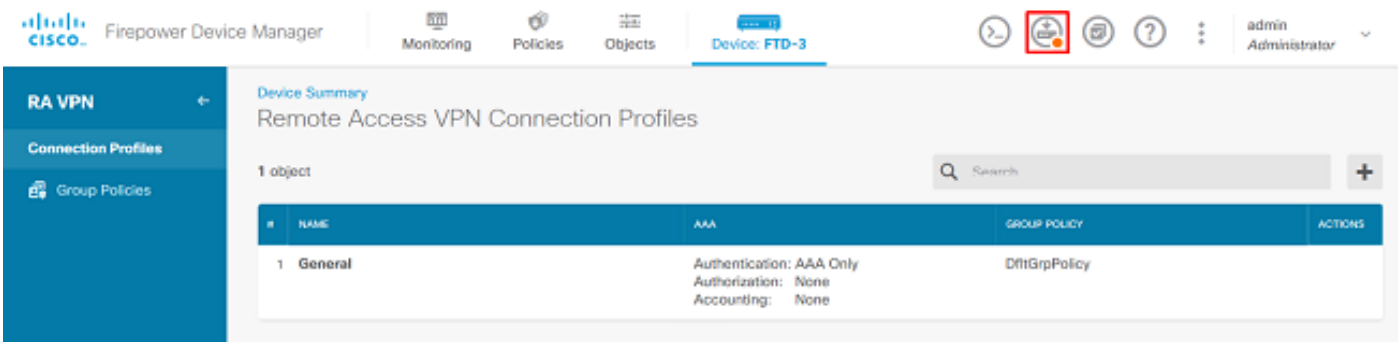
5. [Global Settings]セクションで、少なくとも[SSL Certificate]、[Outside Interface]、および[AnyConnect]パッケージを指定します。証明書が以前に作成されていない場合は、デフォルトの自己署名証明書(DefaultInternalCertificate)を選択できますが、信頼できないサーバ証明書メッセージが表示されます。ユーザIDアクセスポリシーのルールが後で有効になるように、復号化されたトラフィック(sysopt permit-vpn)のBypass Access Control policyをオフにする必要があります。NAT免除は、ここでも設定できます。この設定では、AnyConnectクライアントのIPアドレスに向かう内部インターフェイスからのipv4トラフィックはすべて、NAT以外のものです。外部から外部へのヘアピニングなどのより複雑な設定では、NATポリシーの下に追加のNATルールを作成する必要があります。AnyConnectパッケージは、シスコのサポートサイトにあります。https://software.cisco.com/download/homeAnyConnectパッケージをダウンロードするには、有効なPlusライセンスまたはApexライセンスが必要です。



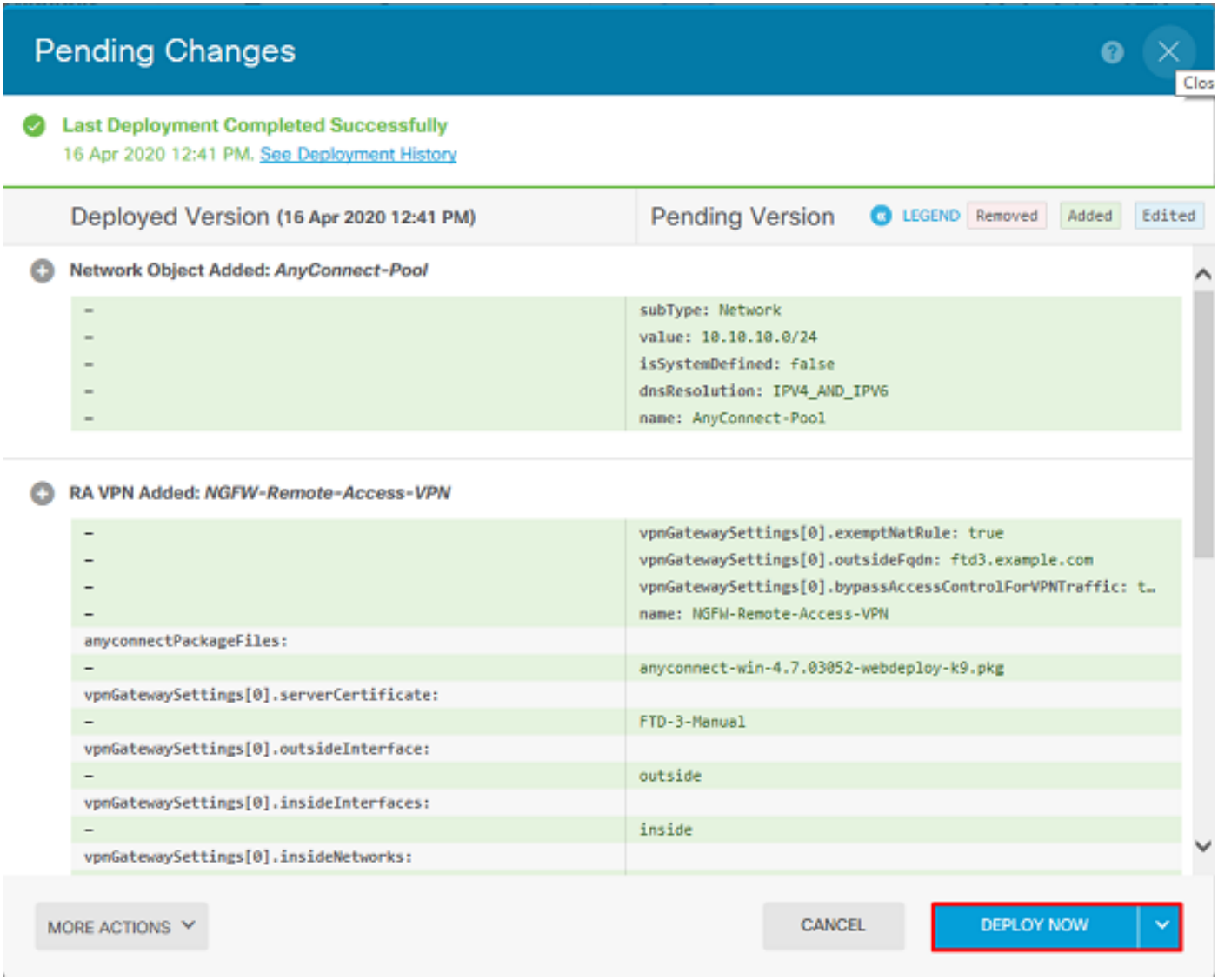
6. [Summary]セクションで、AnyConnectが適切に設定されていることを確認し、**[Submit Query]をクリックします。**



7.図に示すように、右上の**[Pending Changes]**ボタンをクリックします。



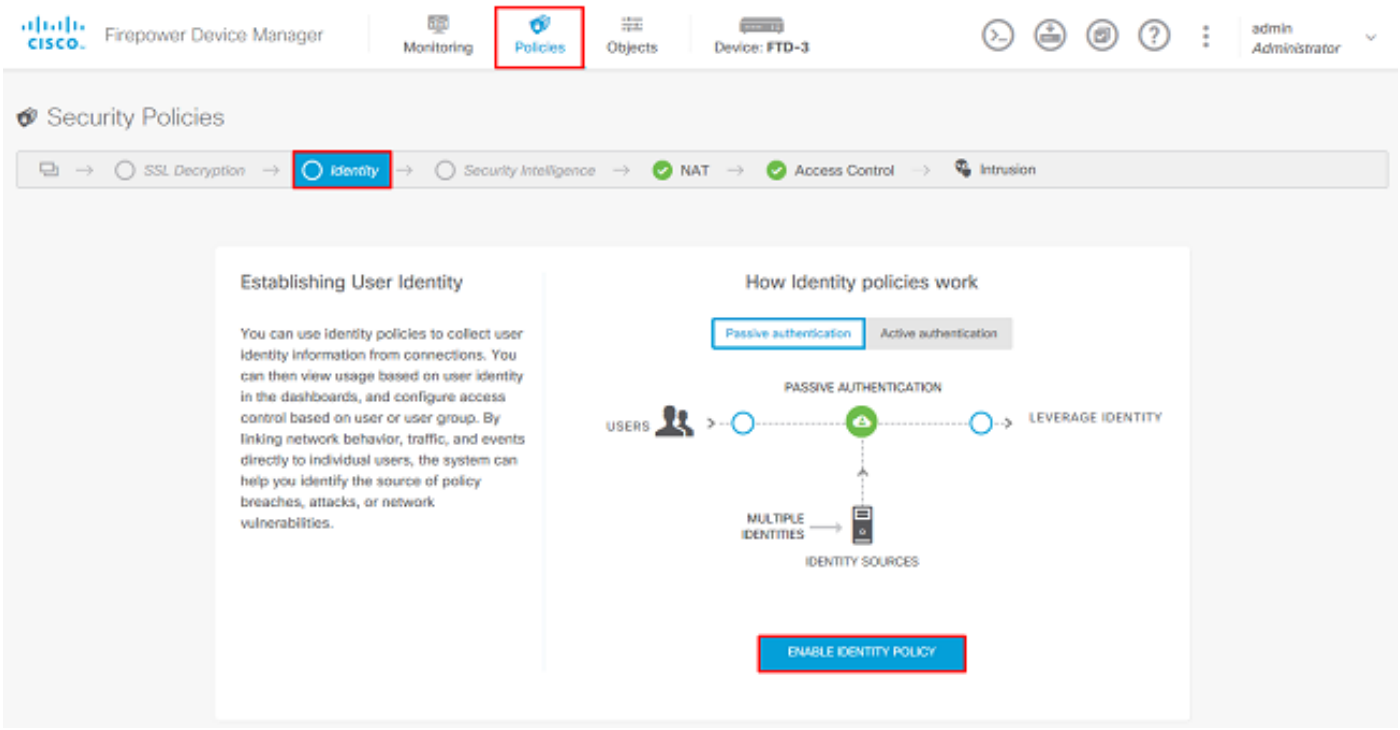
8. [今すぐ展開]をクリックします。



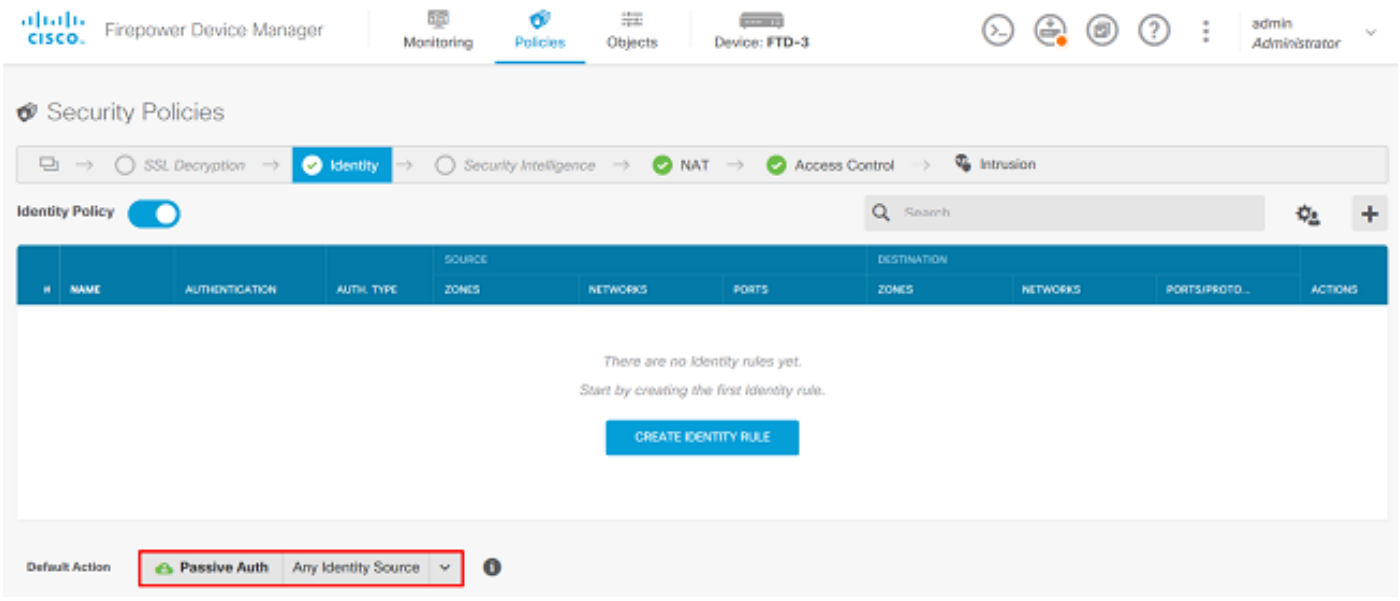
アイデンティティポリシーの有効化とユーザIDのセキュリティポリシーの設定

この時点で、AnyConnectユーザは正常に接続できますが、特定のリソースにアクセスできない可能性があります。この手順では、ユーザIDを有効にして、AnyConnect Admins内のユーザだけがRDPを使用して内部リソースに接続でき、AnyConnect Usersグループ内のユーザだけがHTTPを使用して内部リソースに接続できるようにします。

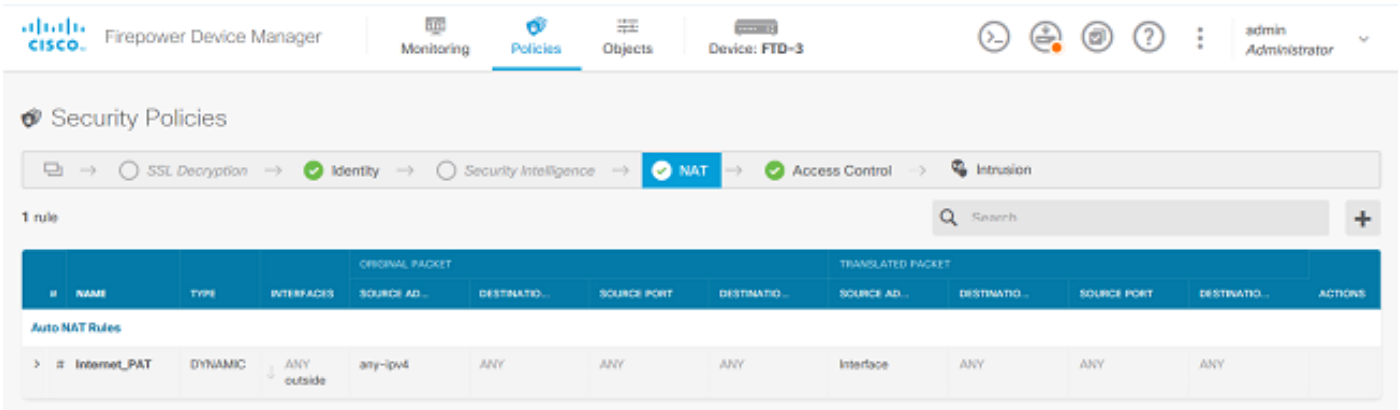
1. [Policies] > [Identity]に移動し、**[Enable Identity Policy]**をクリックします。



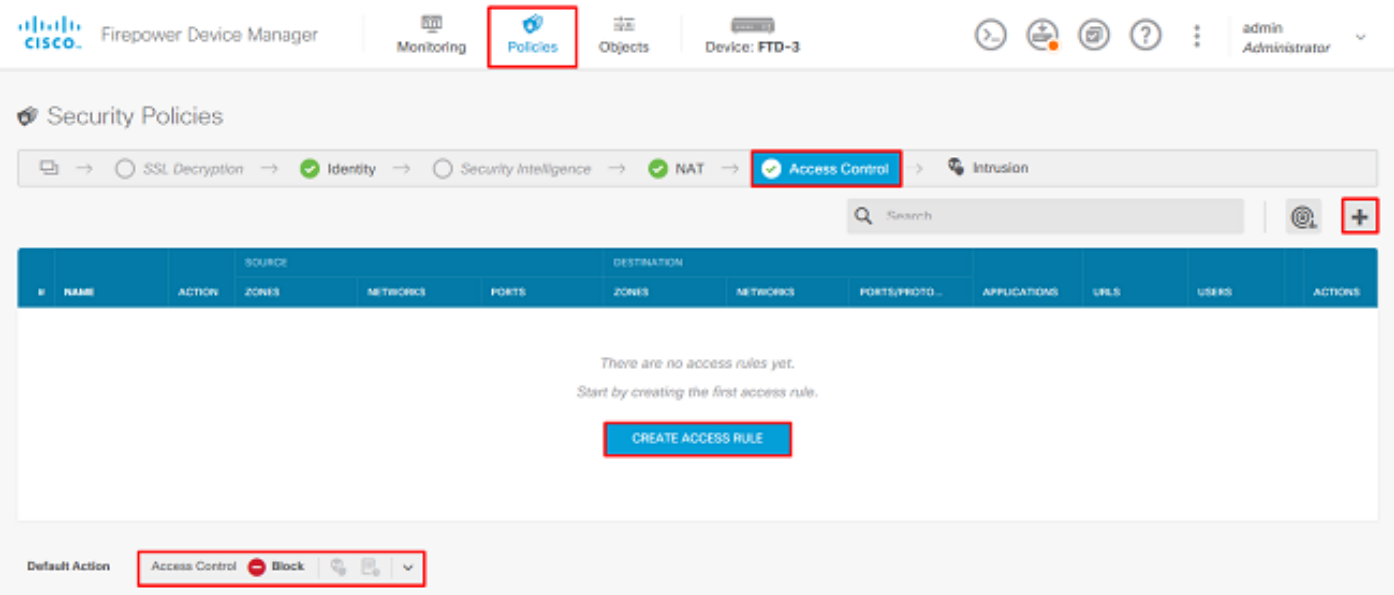
この設定では、これ以上の設定は必要なく、デフォルトアクションで十分です。



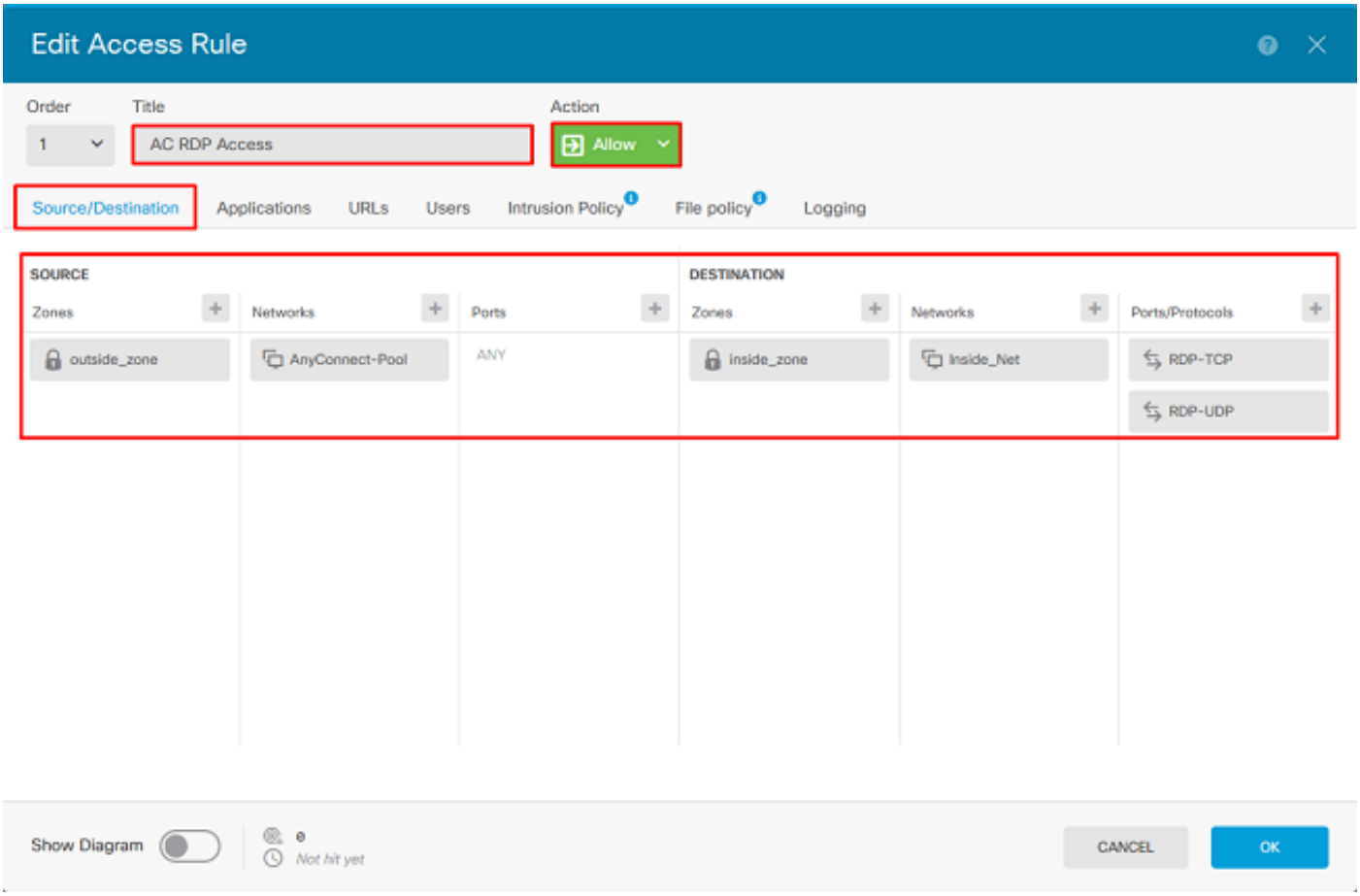
2. [Policies] > [NAT] に移動し、NATが適切に設定されていることを確認します。AnyConnect設定で設定されたNAT例外で十分な場合、ここでは追加の設定は必要ありません。



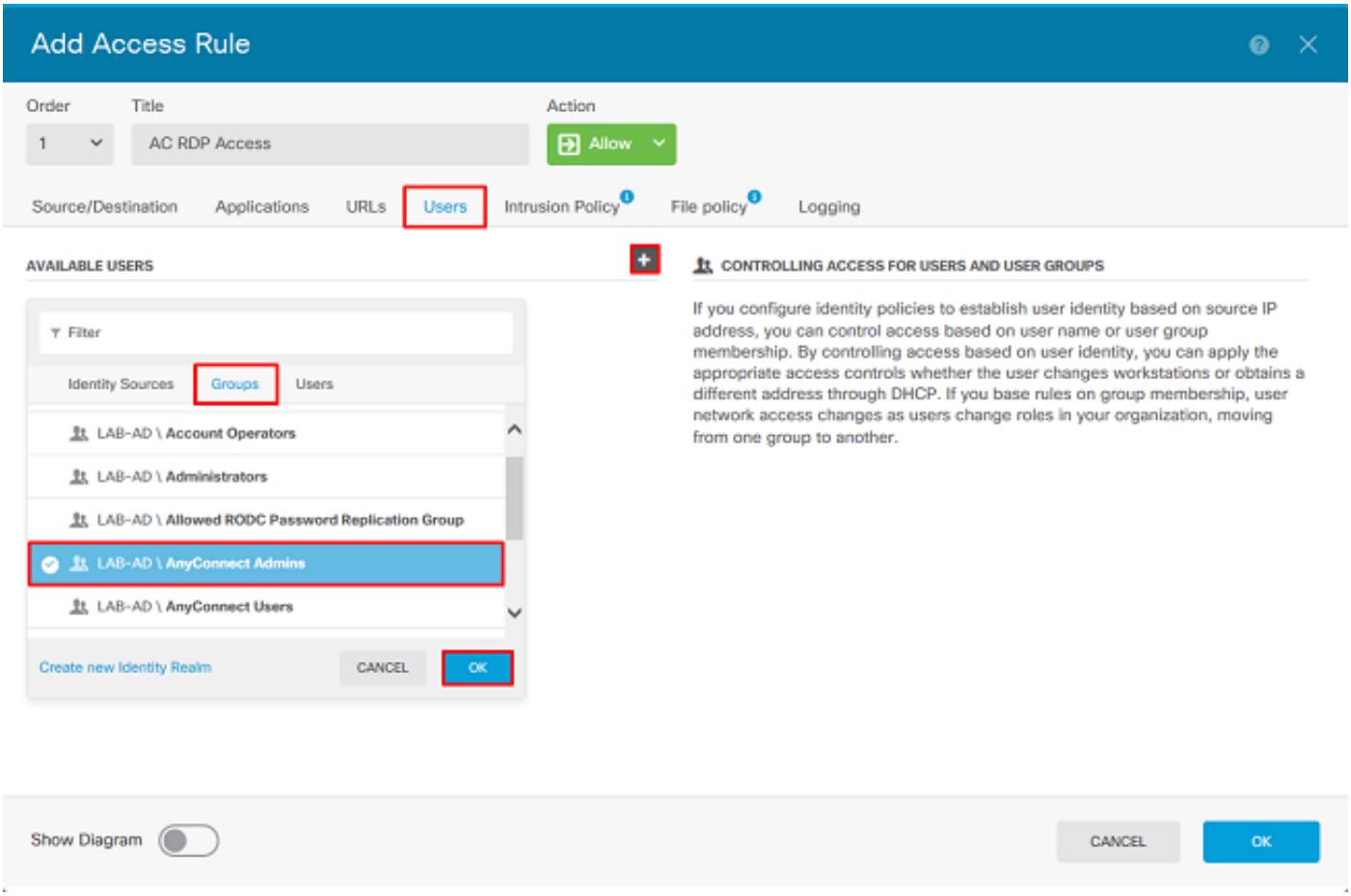
3.[Policies] > [Access Control] に移動します。このセクションでは、[Default Action]が[Block]に設定されており、アクセスルールは作成されていないため、AnyConnectユーザが接続すると、何にもアクセスできなくなります。+記号または[アクセス規則の作成]をクリックして、新しい規則を追加します。



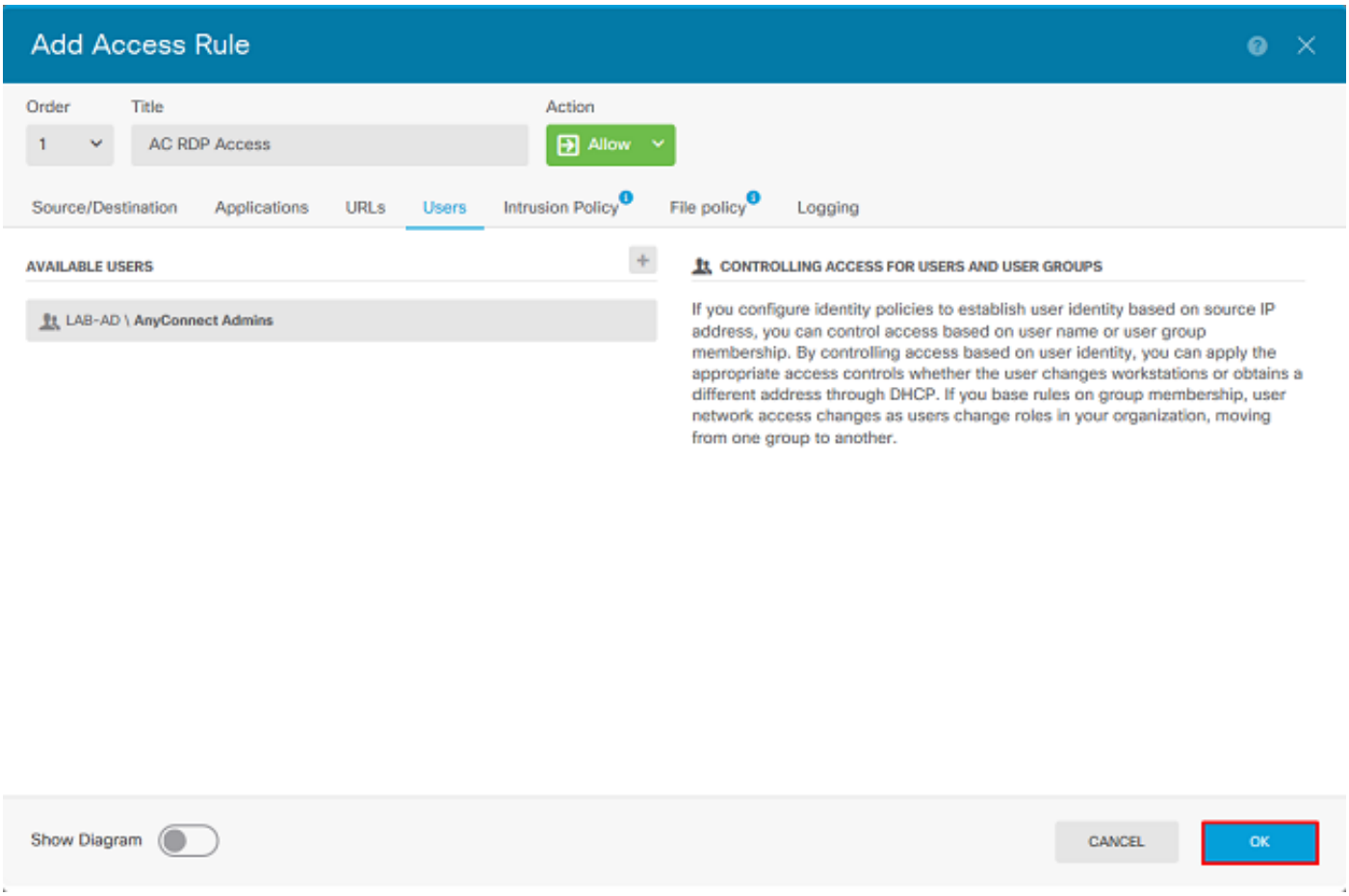
4.フィールドに適切な値を入力します。この設定では、AnyConnect Adminsグループ内のユーザは、内部ネットワーク内のWindows ServerにRDPアクセスできる必要があります。送信元の場合、ゾーンはoutside_zoneとして設定されます。これはAnyConnectユーザが接続する外部インターフェイスであり、ネットワークはAnyConnectクライアントにIPアドレスを割り当てるために以前に設定されたAnyConnect-Poolオブジェクトです。FDMのユーザーIDの場合、ソースはユーザーが接続を開始するゾーンとネットワークである必要があります。宛先に対して、ゾーンはWindows Serverの内部インターフェイスであるinside_zone、ネットワークはWindows Serverのサブネットを定義するオブジェクトであるInside_Netオブジェクト、ポート/プロトコルは2つのカスタムポートオブジェクトに設定され、TCP 3389とUDP 3389で9への8への8RDP8アクセス8を8を8を8可能8可能8に89



[Users]セクションで、グループAnyConnect Adminsが追加され、このグループ以外のユーザはWindows ServerへのRDPアクセスが許可されます。+記号をクリックし、[グループ]タブをクリックし、該当するグループをクリックして、[OK]をクリックします。個々のユーザとアイデンティティソースも選択できます。

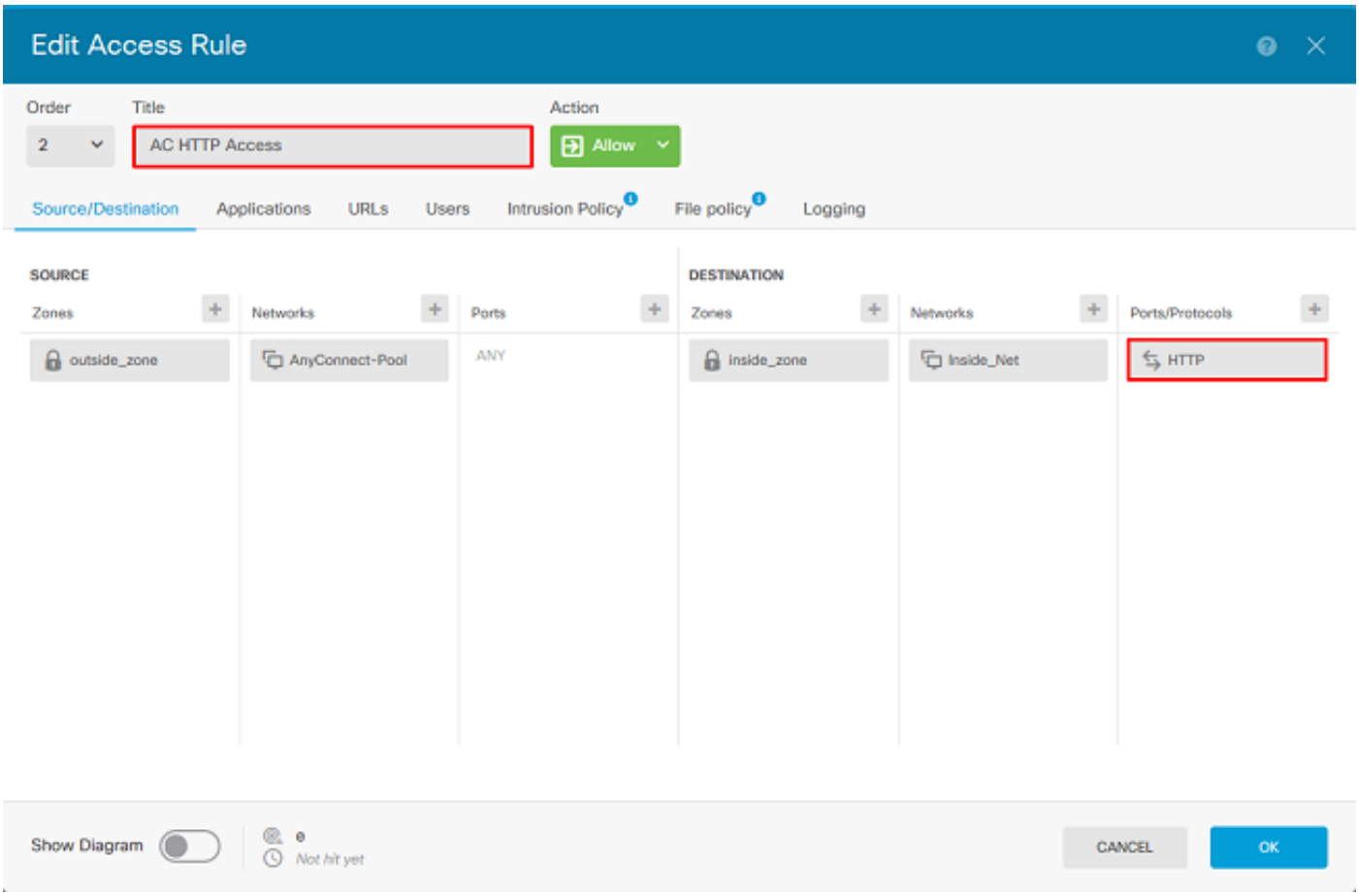


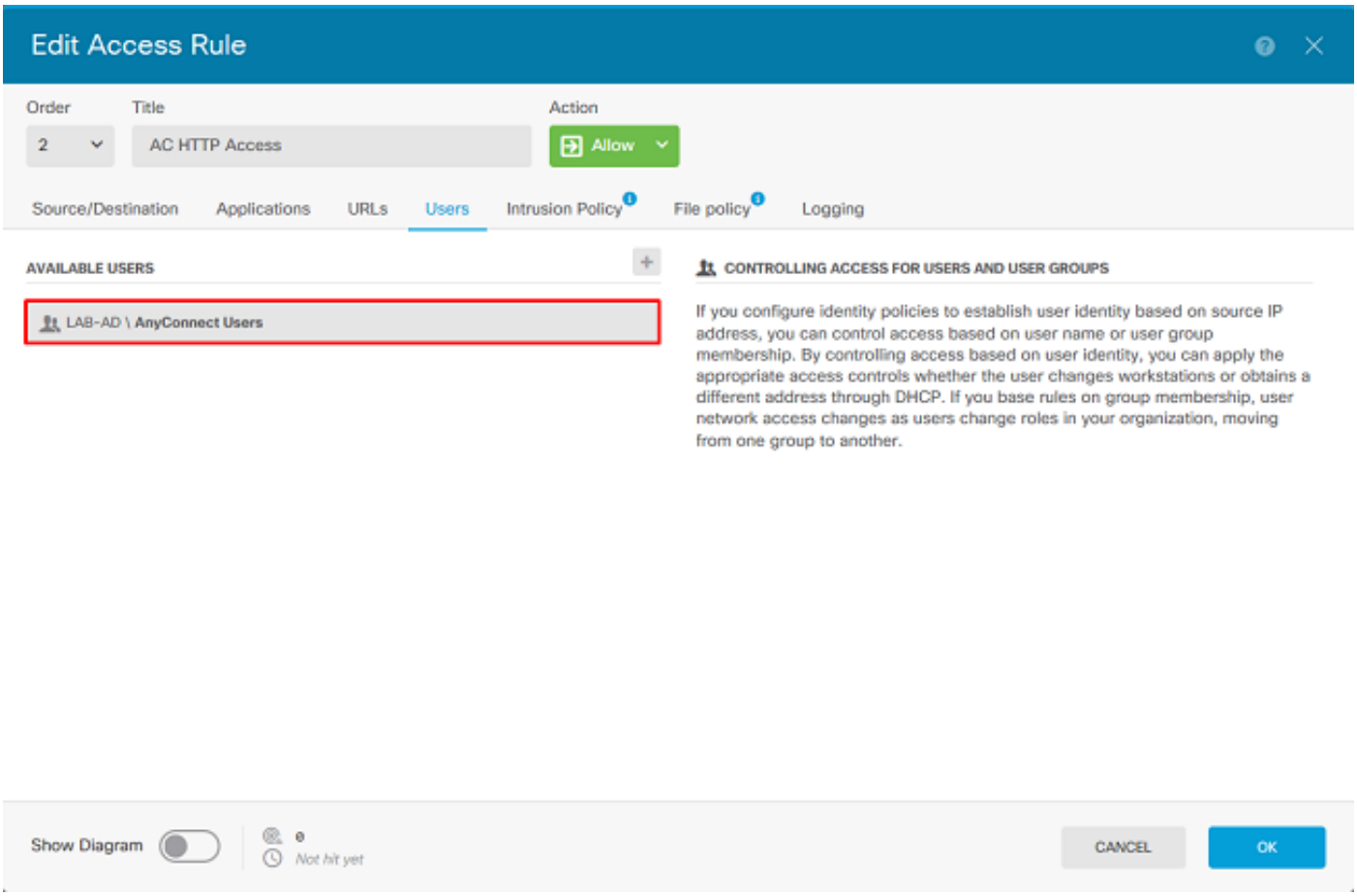
適切なオプションを選択したら、[OK]をクリックします。



5.必要に応じて、さらにアクセスルールを作成します。この設定では、AnyConnect Usersグルー

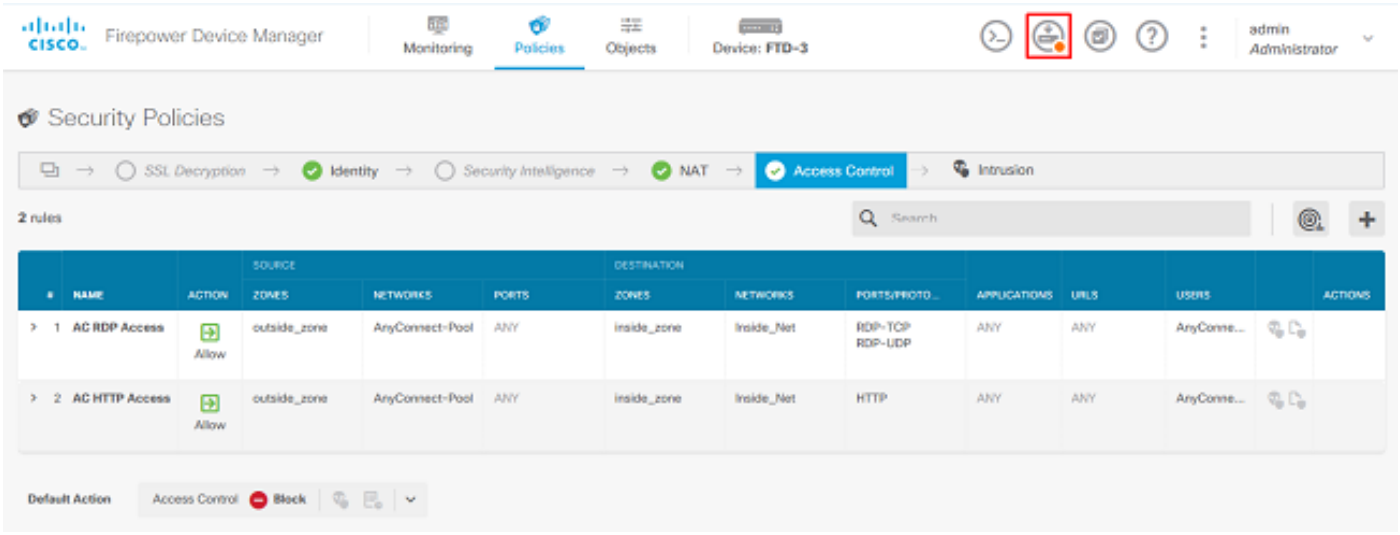
プ内のユーザがWindows ServerにHTTPアクセスできるように、別のアクセスルールが作成されます。



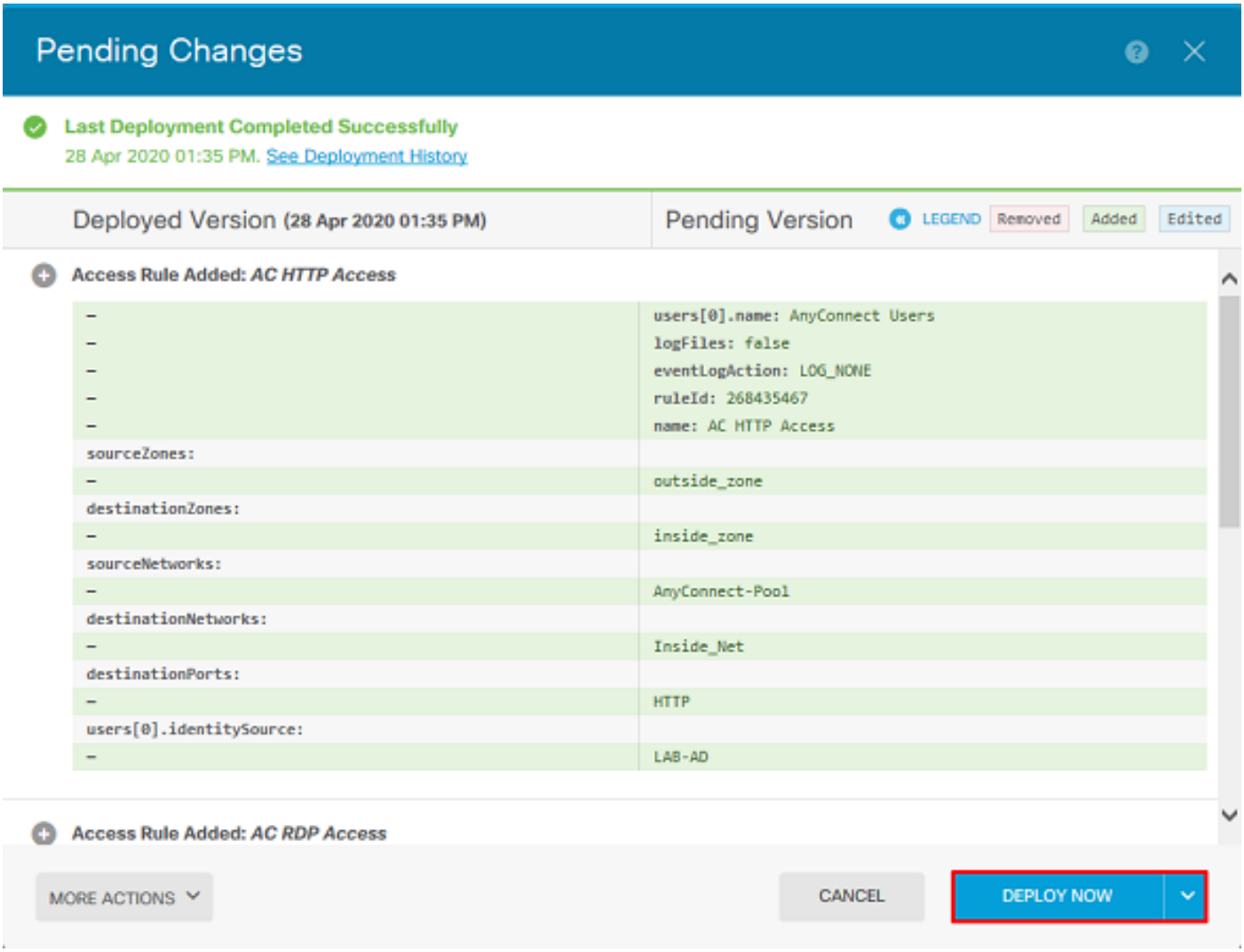


6.アクセスルールの設定を確認し、図に示すように、右上の**[Pending Changes]**ボタンをクリック

します。



7.変更を確認し、[今すぐ展開]をクリックします。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

Final Configuration

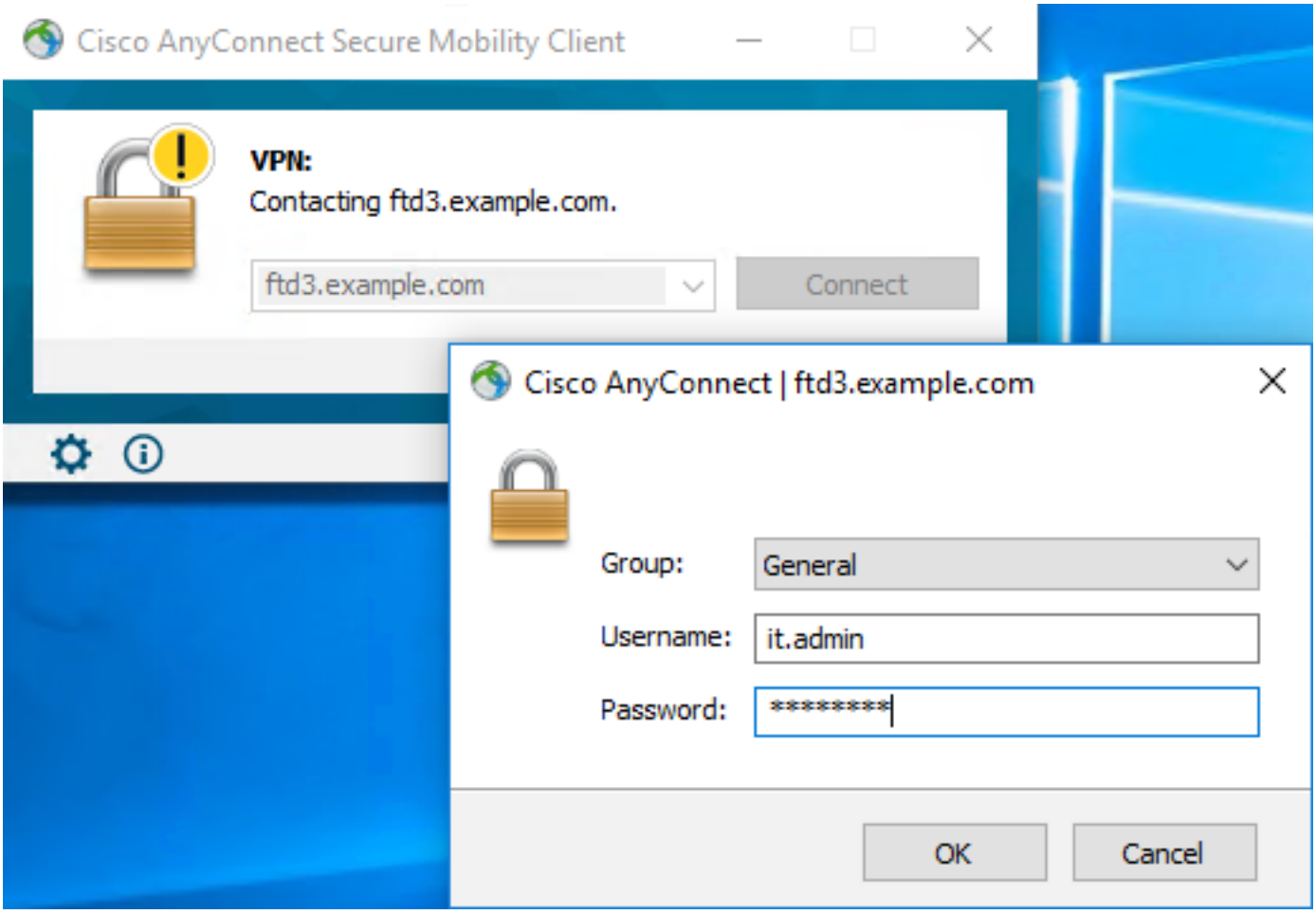
AAA 設定

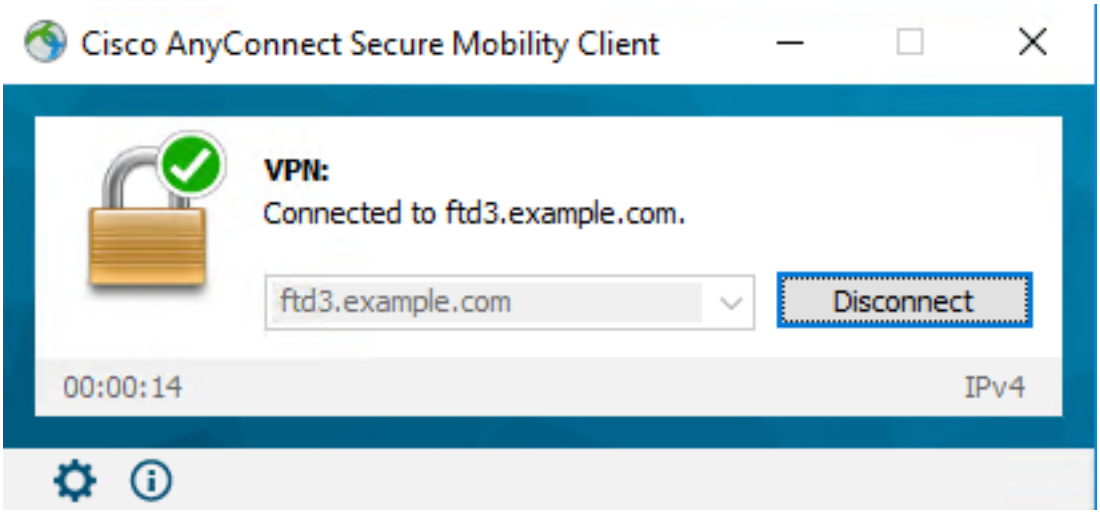
```
show running-configuration aaa-server
aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com server-
port 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-login-
dn ftd.admin@example.com server-type auto-detect
```

AnyConnectの設定

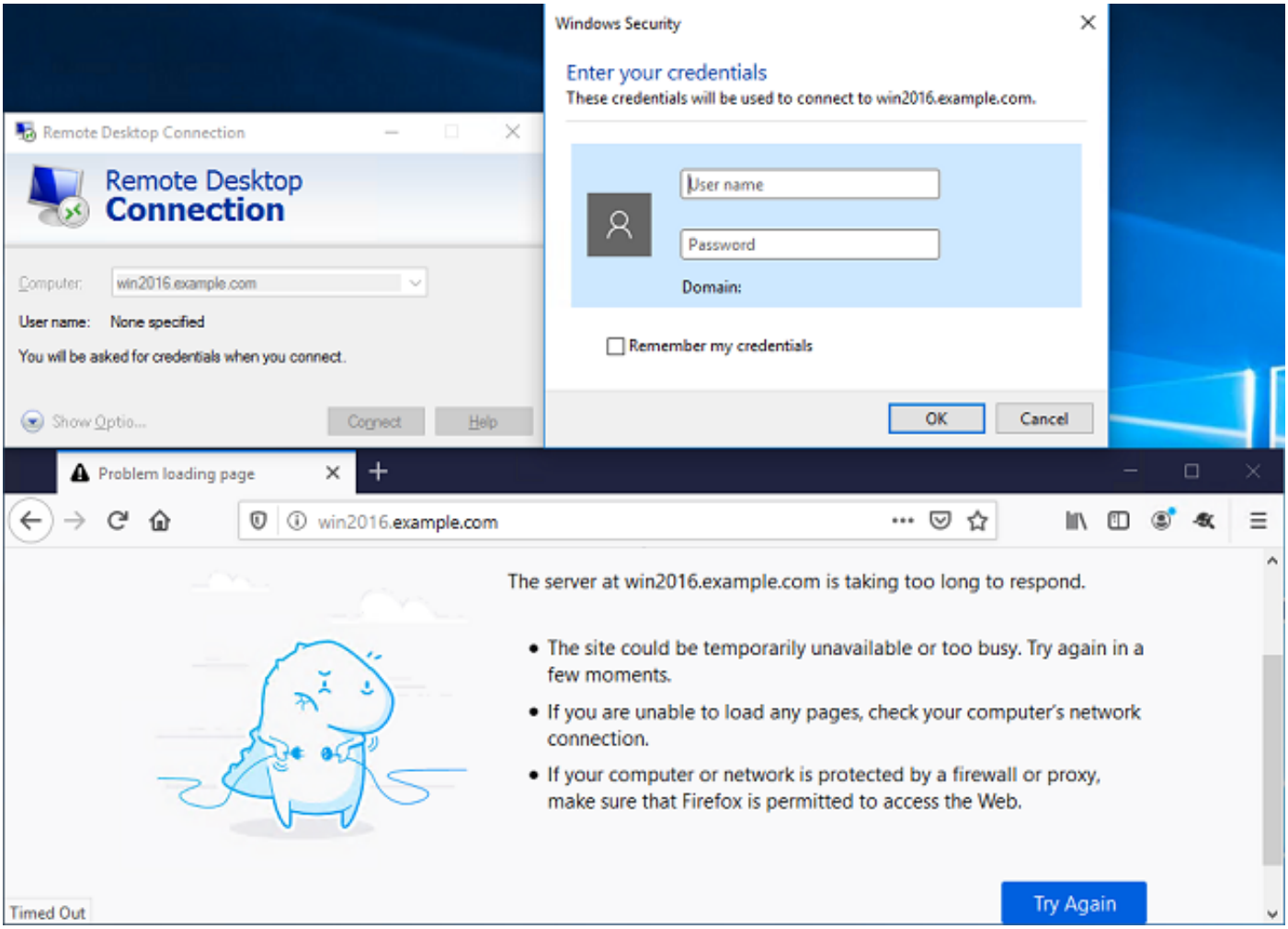
```
> show running-config webvpn
webvpn
 enable outside
 http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
 anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg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

AnyConnectによる接続とアクセスコントロールポリシールールの確認

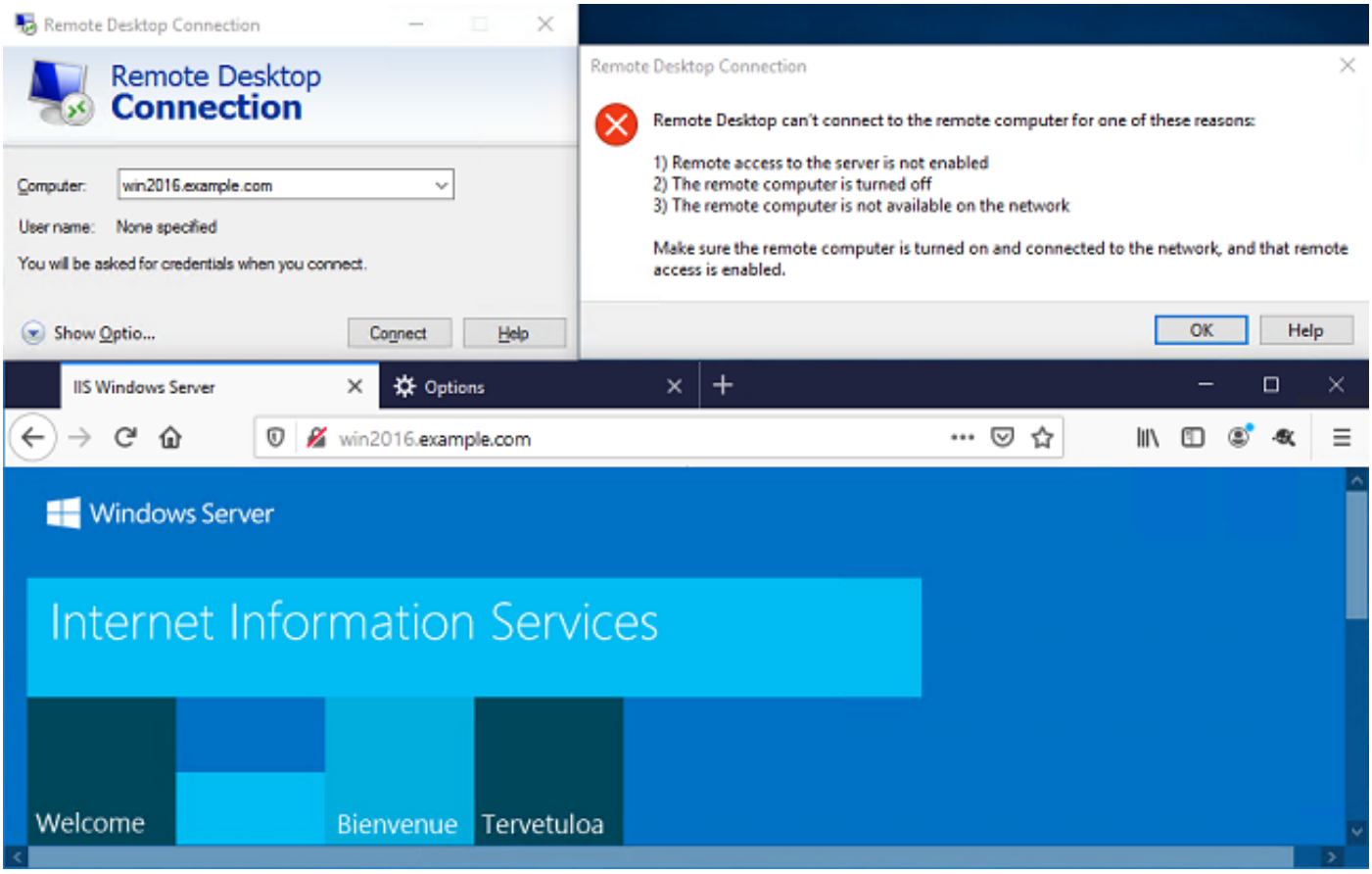




ユーザIT Adminは、Windows ServerにRDPアクセスできるグループAnyConnect Adminsに属していますが、HTTPにアクセスできません。このサーバーに対してRDPおよびFirefoxセッションを開くと、このユーザーはRDP経由でのみサーバーにアクセスできます。



HTTPアクセスを持ち、RDPアクセスを持たないグループAnyConnect Usersに属するテストユーザでログインした場合、アクセスコントロールポリシールールが有効であることを確認できます。



トラブルシュート

ここでは、設定が正常に機能しているかどうかを確認します。

デバッグ

このデバッグは、LDAP認証に関連する問題をトラブルシューティングするために、診断CLIで実行できます。**debug ldap 255**を使用します。

ユーザIDのアクセスコントロールポリシーの問題をトラブルシューティングするために、**system support firewall-engine-debugをclishで実行**し、トラフィックが予期せず許可またはブロックされる理由を判別できます。

LDAPデバッグの動作

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

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

LDAPサーバとの接続を確立できない

```
[-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
```

潜在的なソリューション：

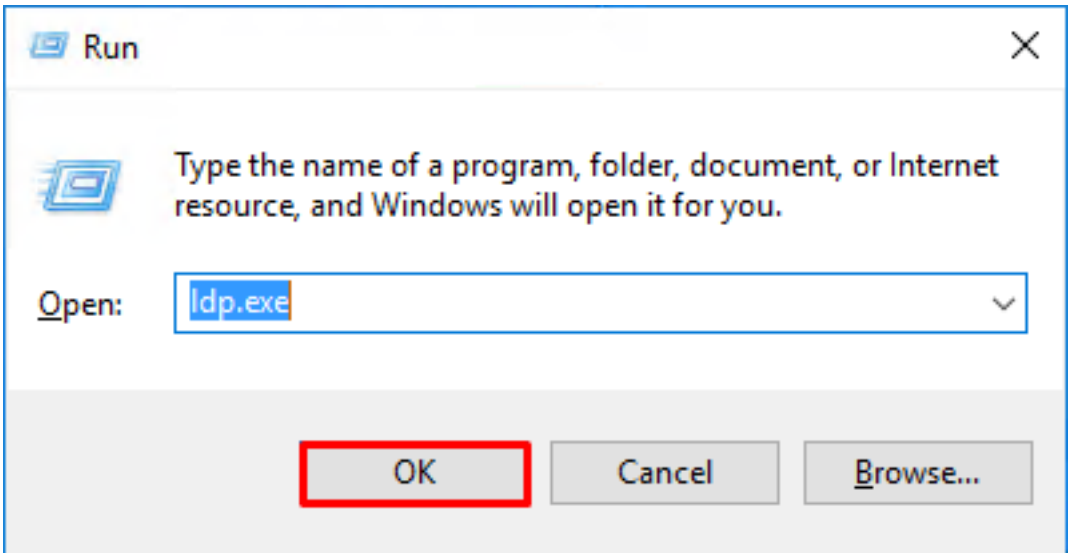
- ルーティングを確認し、FTDがLDAPサーバから応答を受信することを確認します。
- LDAPSまたはSTARTTLSを使用する場合は、SSLハンドシェイクが正常に完了できるように、正しいルートCA証明書が信頼されていることを確認します。
- 正しいIPアドレスとポートが使用されていることを確認します。ホスト名を使用する場合は、DNSが正しいIPアドレスに解決できることを確認します

Binding Login DN and/or Password Incorrect

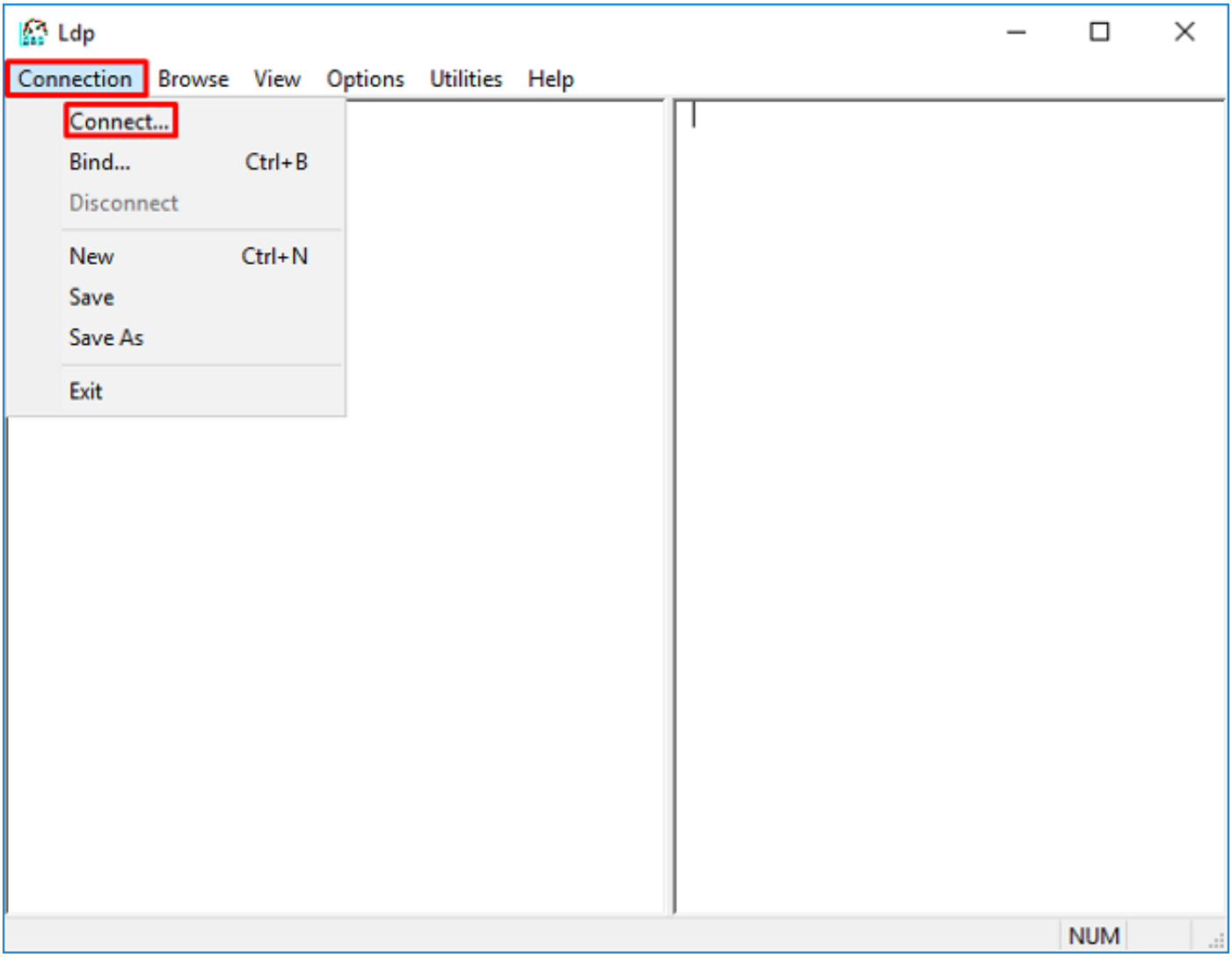
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615]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

考えられる解決策:ログインDNとログインパスワードが適切に設定されていることを確認します。これは、ADサーバでldp.exeを使用して確認**できます**。アカウントがldpを使用して正常にバインドできることを確認するには、次の手順を実行します。

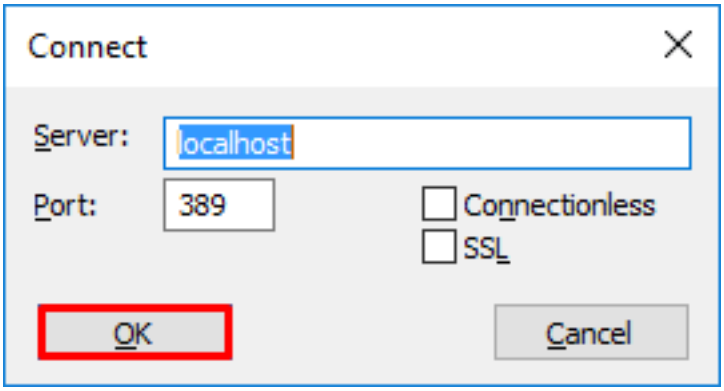
1. ADサーバーで**Win**+Rを押し、**ldp.exe**を検索**します**。



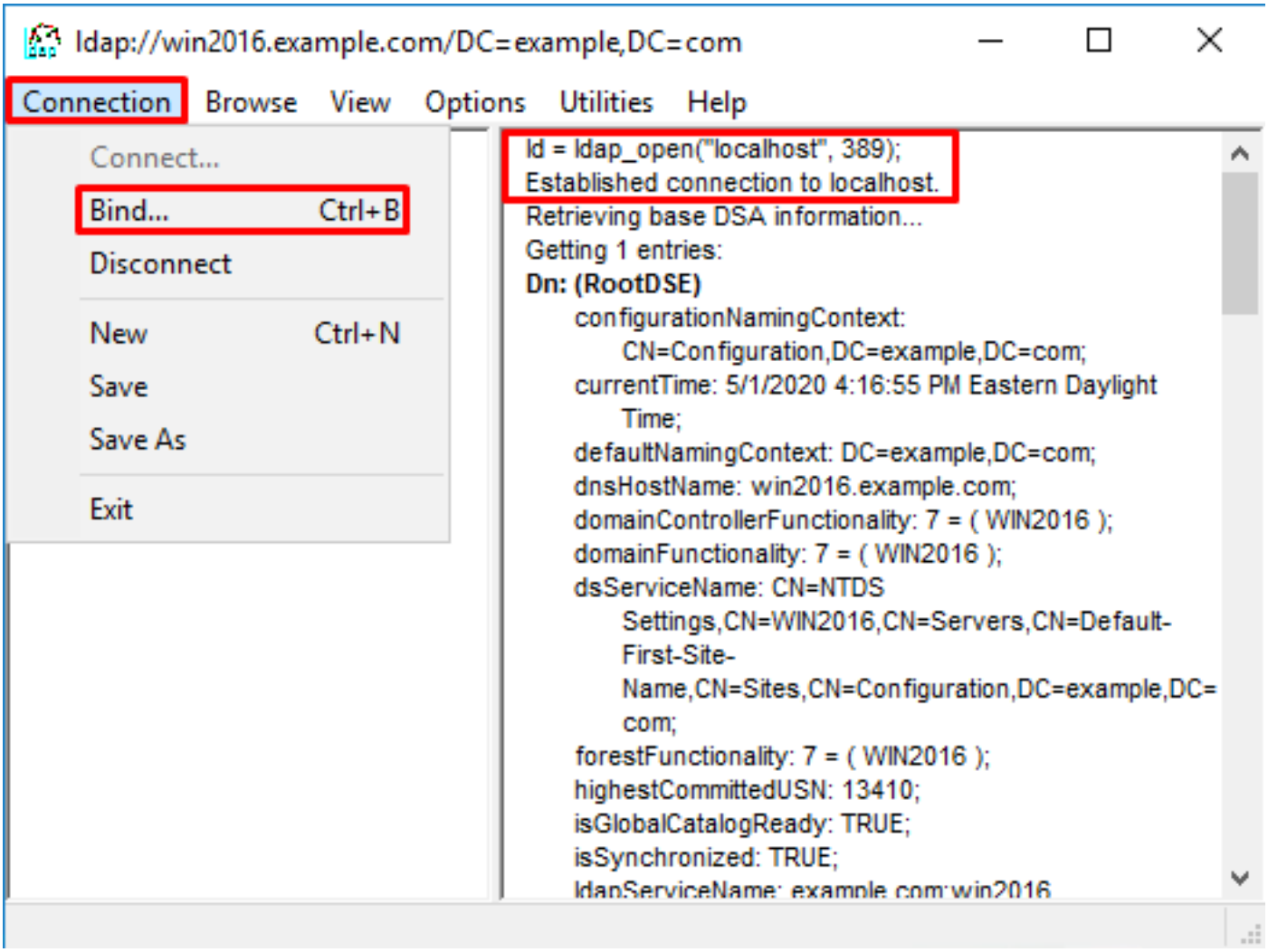
2. [接続] > [接**続]をクリックします。** 図に示すように



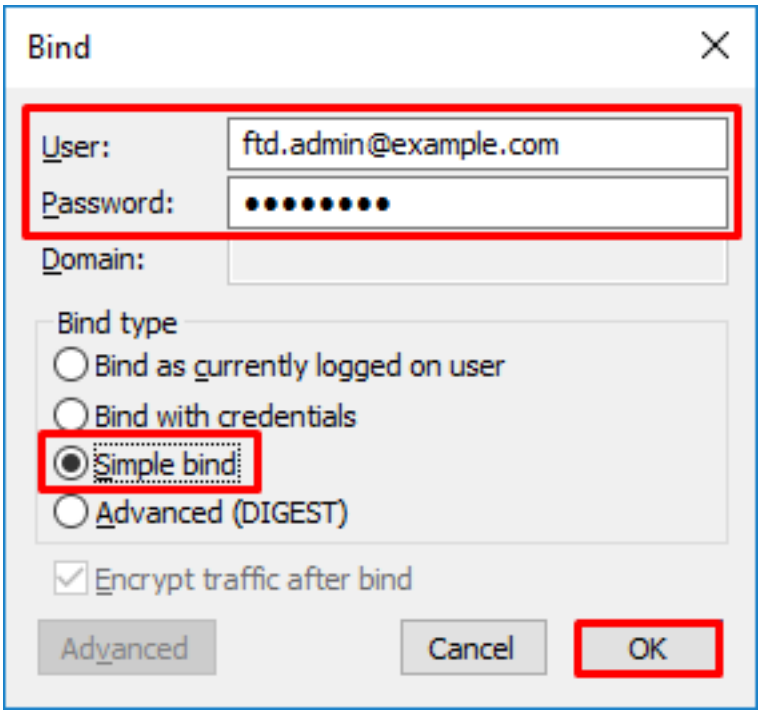
3.サーバーにlocalhostと適切なポートを指定し、「OK」をクリックします。



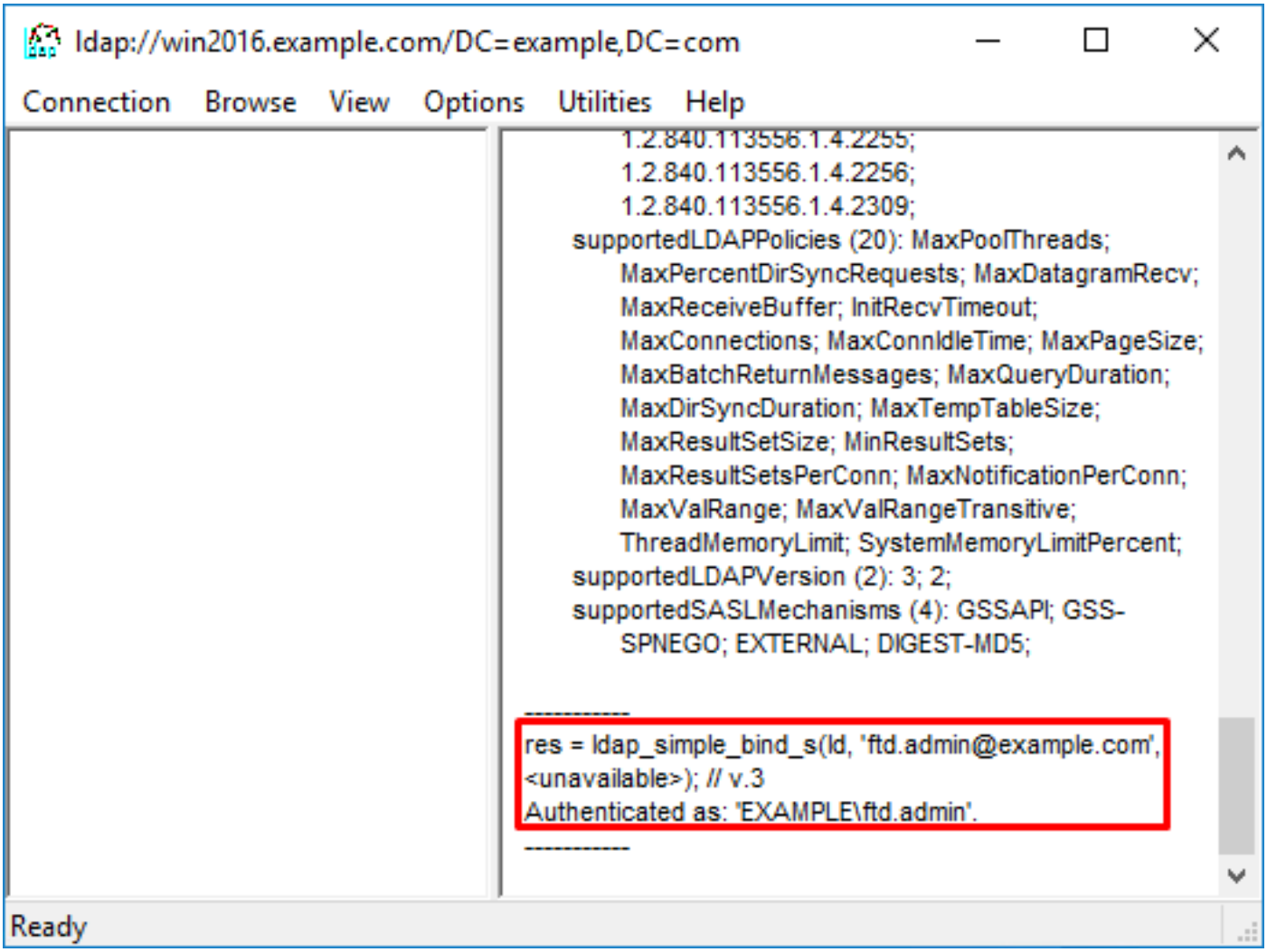
4. [Right]列には、接続が成功したことを示すテキストが表示されます。「接続」>「バインド」をクリックします。 図に示すように



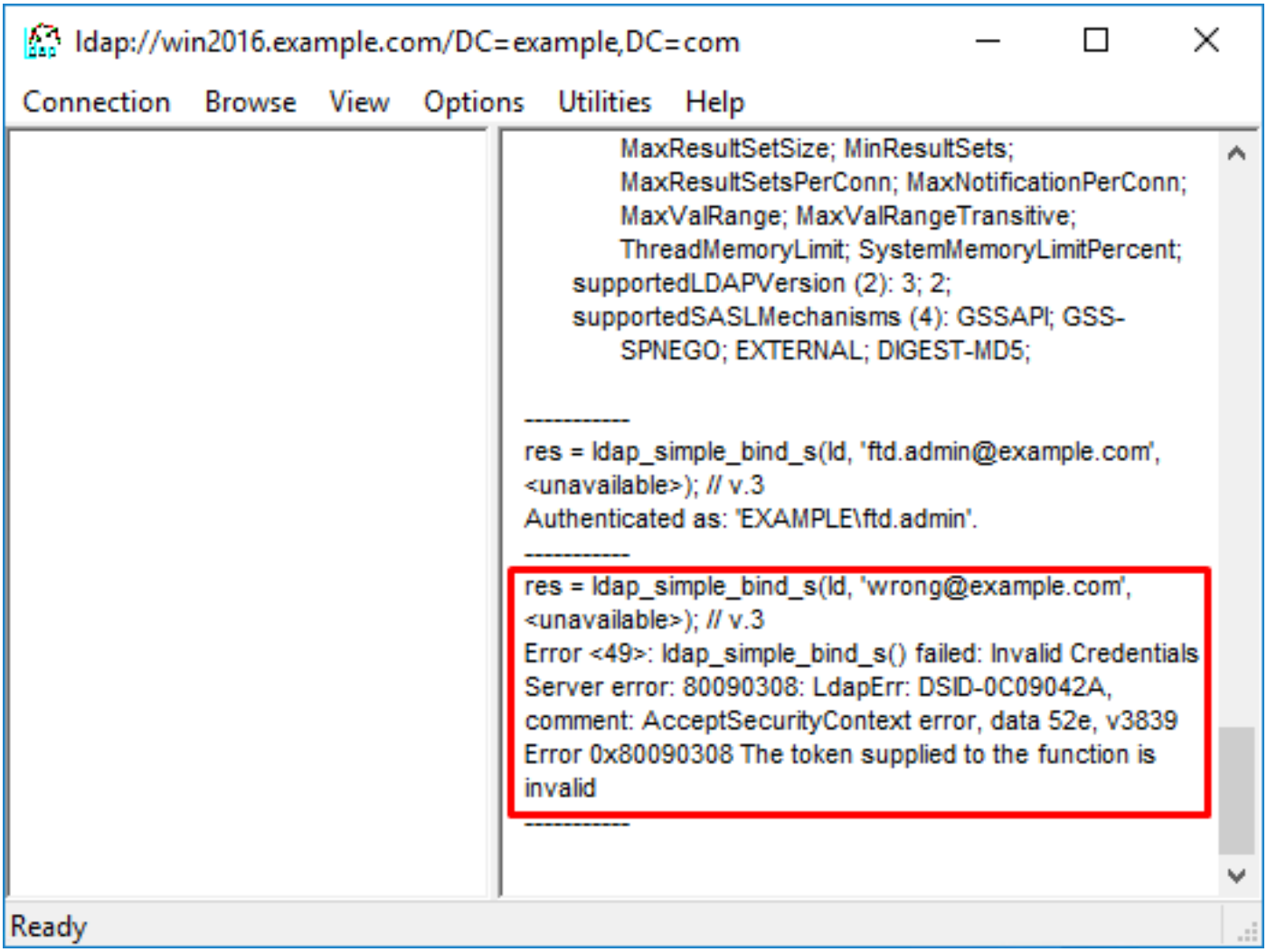
5. 「簡易バインド」**を選択**し、ディレクトリ・アカウントのユーザー名とパスワードを指定します。[OK] をクリックします。



バインドが成功すると、ldpは**DOMAIN\username**としてAuthenticatedと表示**されます**。



無効なユーザ名またはパスワードを使用してバインドしようとすると、次のようなエラーが発生します。

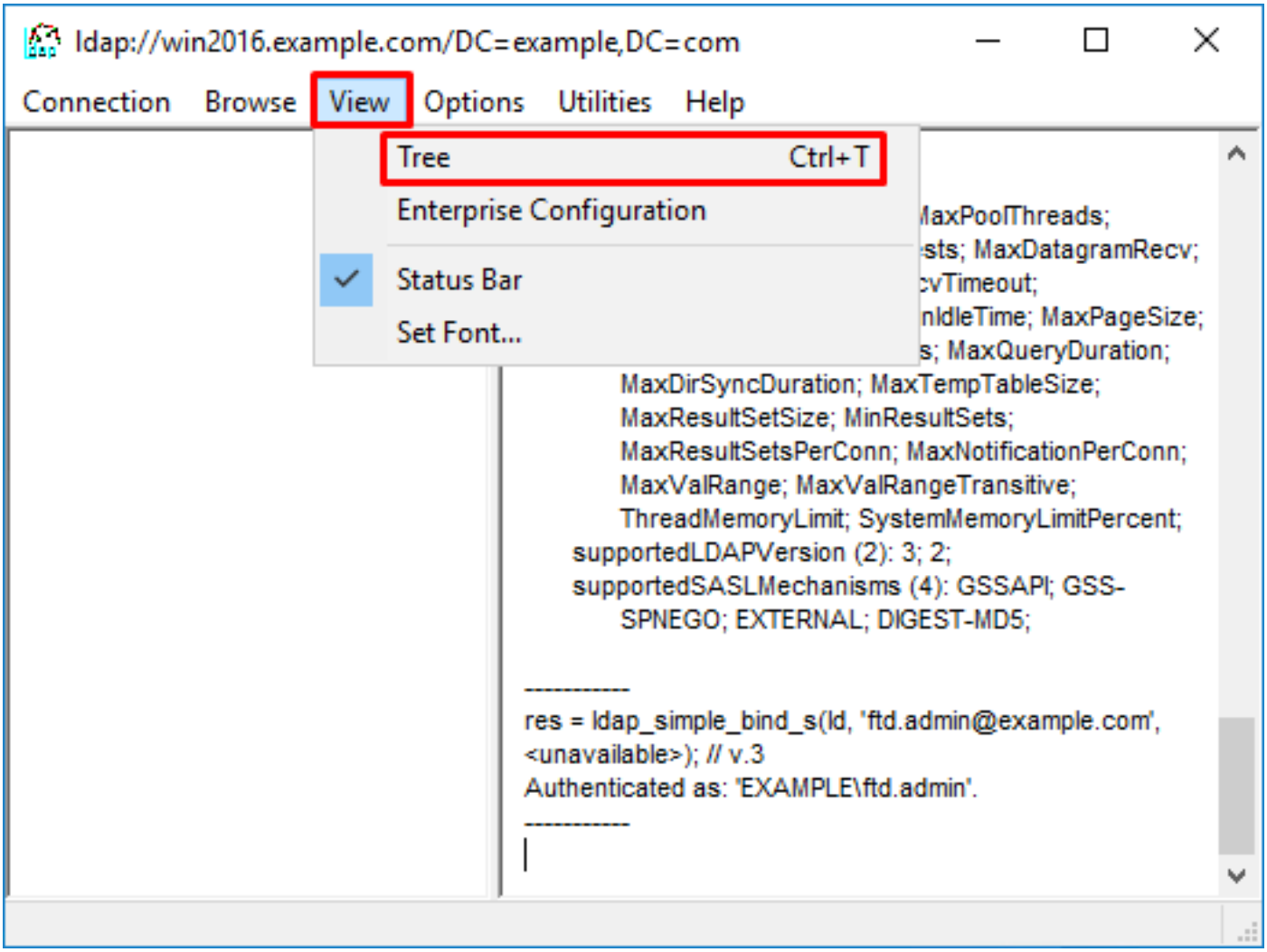


LDAPサーバがユーザ名を見つけることができない

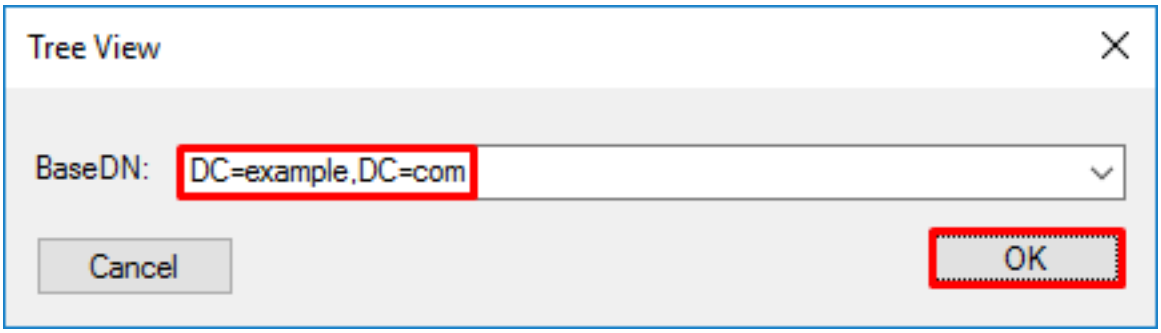
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612]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

考えられる解決策:ADがFTDによる検索でユーザを検索できることを確認します。これは、ldp.exeでも実行できます。

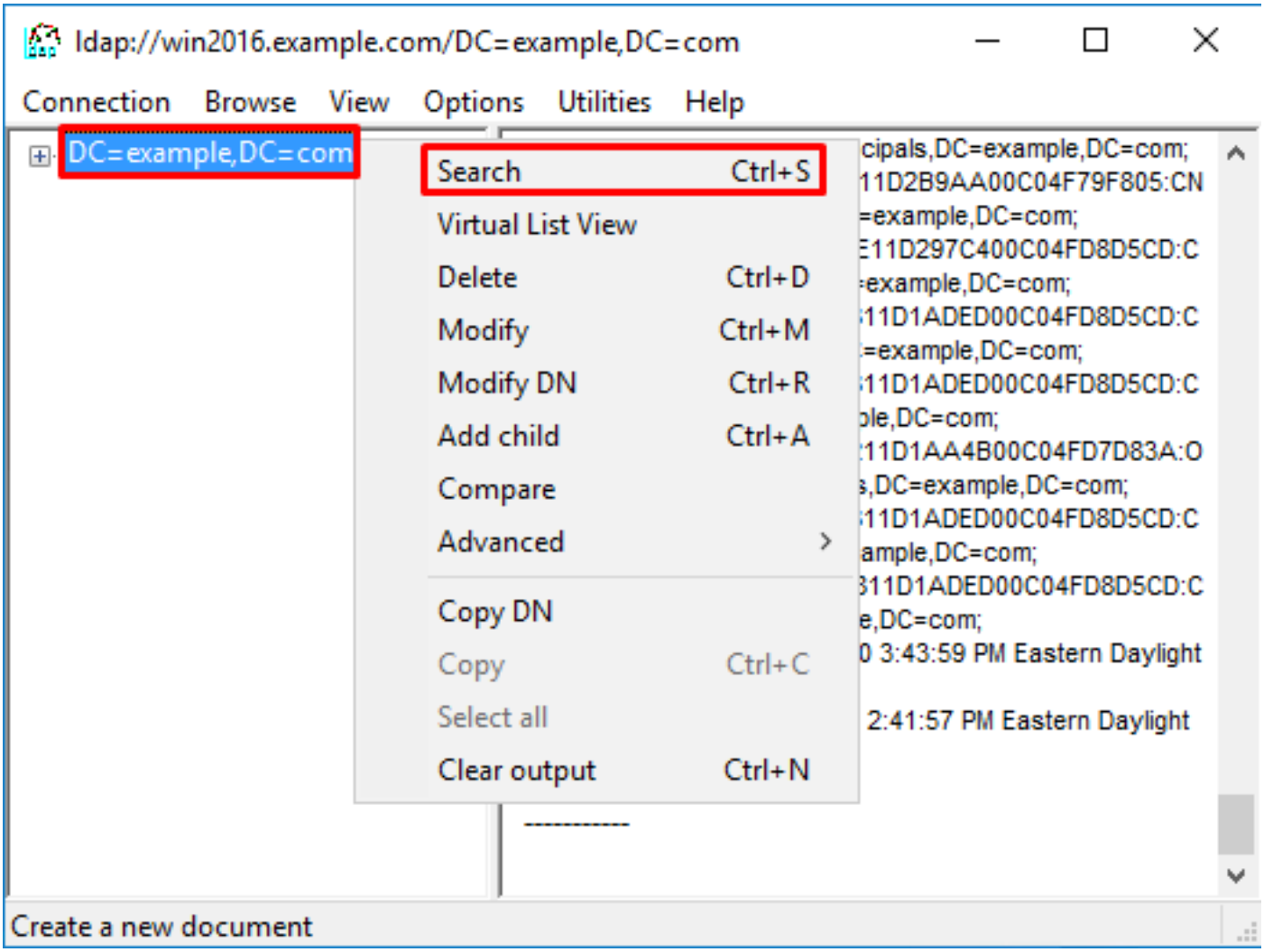
1.バインドが正常に完了したら、図に示すように**[View] > [Tree]**に移動します。



2. FTDに設定されているベースDNを指定し、[OK]をクリックします。

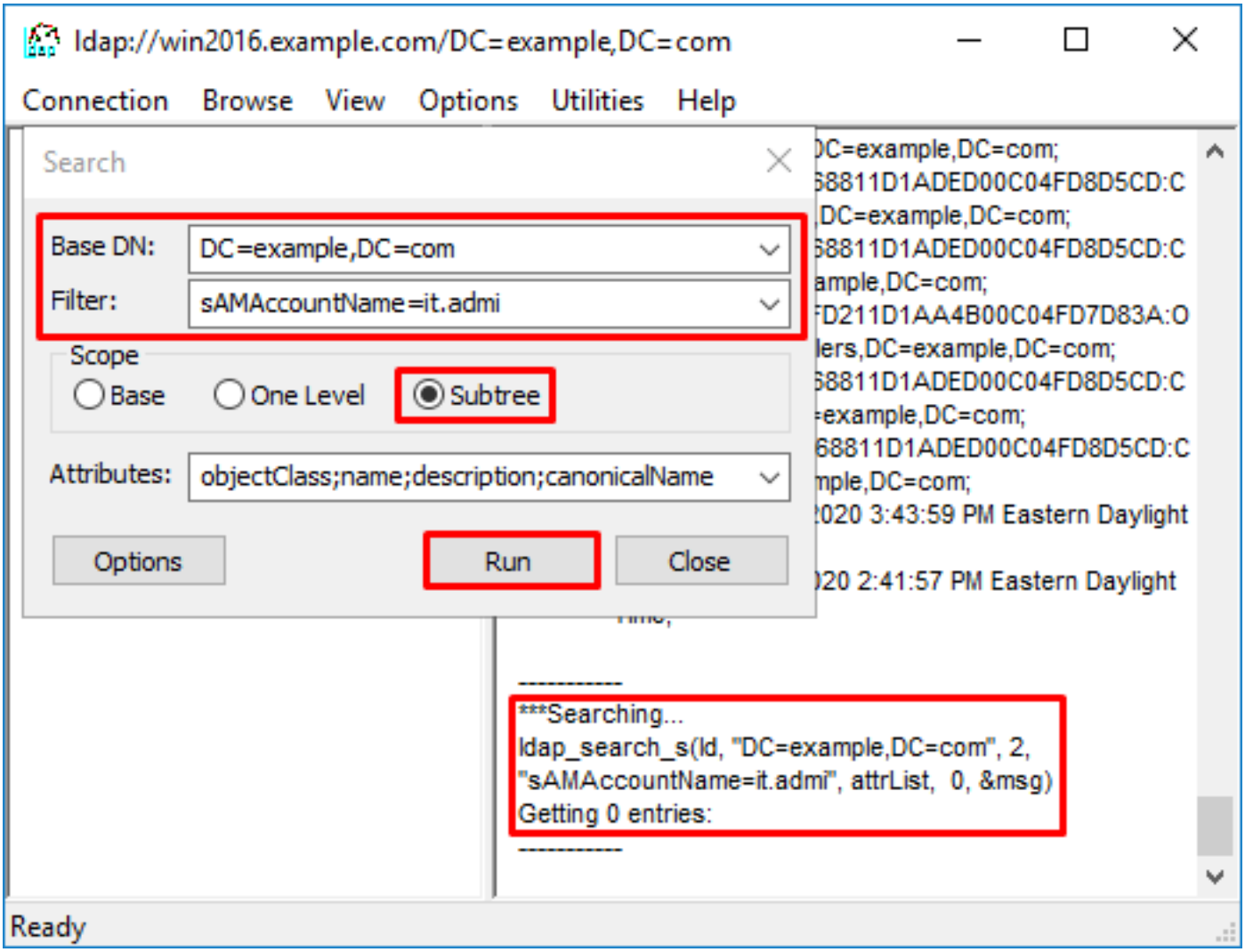


3. [Base DN]を右クリックし、図に示すように[Search]をクリックします。



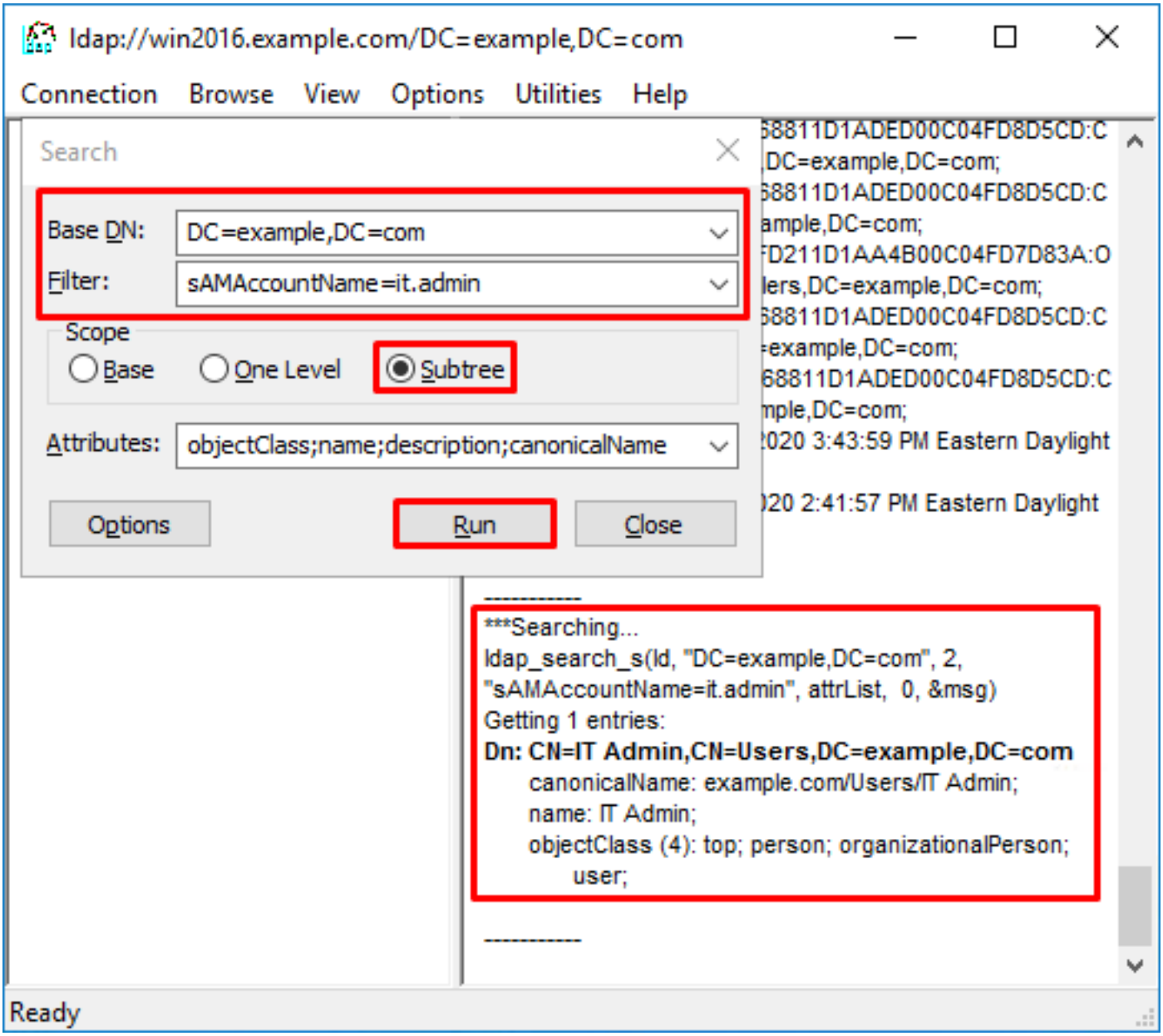
4.デバッグに示されているのと同じベースDB、フィルタ、スコープの値を指定します。この例では、次の項目を示します。

- [Base DN]：dc=example,dc=com
- [Filter]：samaccountname=it.admi
- スコープ：サブツリー



ldpは、**samaccountname=it.admi**のユーザアカウントがベースDN dc=example,dc=comに存在しないため、0エントリを見つけます。

正しい**samaccountname=it.admin**を使用して再**試行すると**、結果が異なります。ldpは、ベースDN dc=example,dc=comの下に1つのエントリを見つけ、そのユーザのDNを出力します。



ユーザ名のパスワードが正しくない

```
[-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
```

考えられる解決策:ユーザのパスワードが適切に設定され、期限が切れていないことを確認します。Login DNと同様に、FTDはユーザのクレデンシャルを使用してADに対してバインドを実行します。このバインドは、ADが同じユーザ名とパスワードのクレデンシャルを認識できることを確認するために、ldpでも実行できます。ldpの手順は、「ログインDNのバインド」セクションと「パスワードが正しくない」セクションのいずれかまたは両方で示されています。さらに、Microsoftサーバのイベントビューアのログを確認して、潜在的な理由を調べることができます。

AAAのテスト

test aaa-serverコマンドを使用すると、FTDから特定のユーザ名とパスワードを使用した認証の試みをシミュレートできます。これは、接続または認証の失敗をテストするために使用できます。コマンドはtest aaa-server authentication [AAA-server] host [AD IP/hostname]です。

```
> 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
```

パケット キャプチャ

パケットキャプチャは、ADサーバへの到達可能性を確認するために使用できます。LDAPパケットがFTDから送信されても応答がない場合は、ルーティングの問題を示している可能性があります。

双方向LDAPトラフィックを示すキャプチャを次に示します。

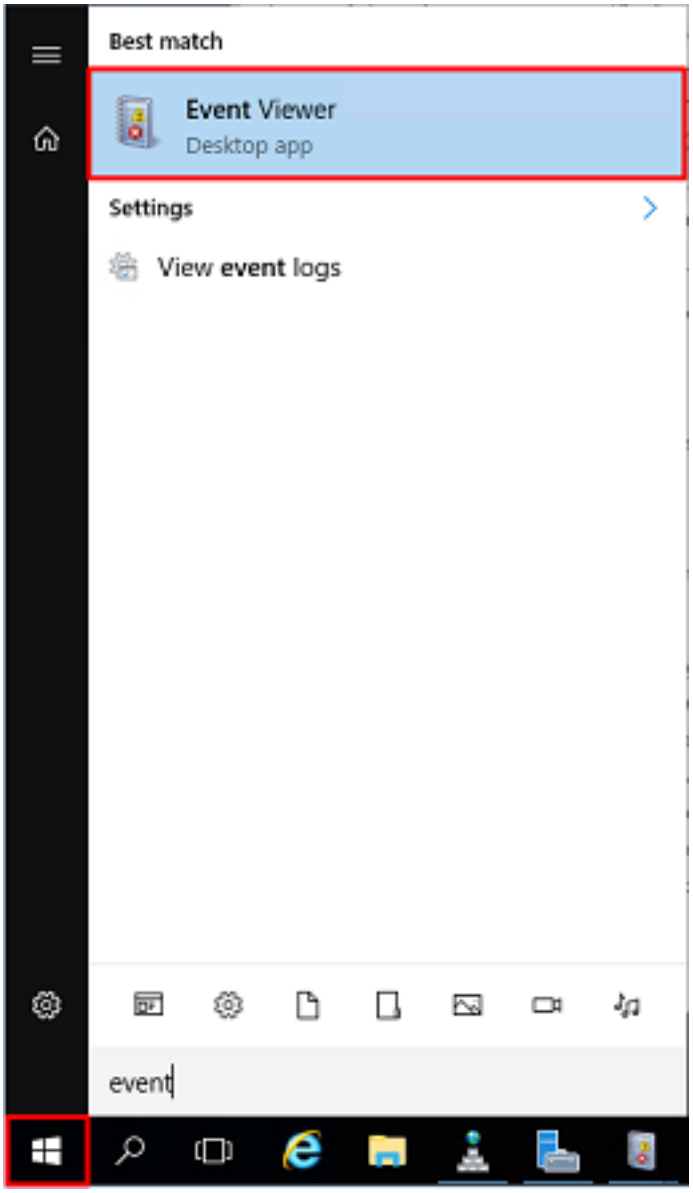
```
> show route 192.168.1.1

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
```

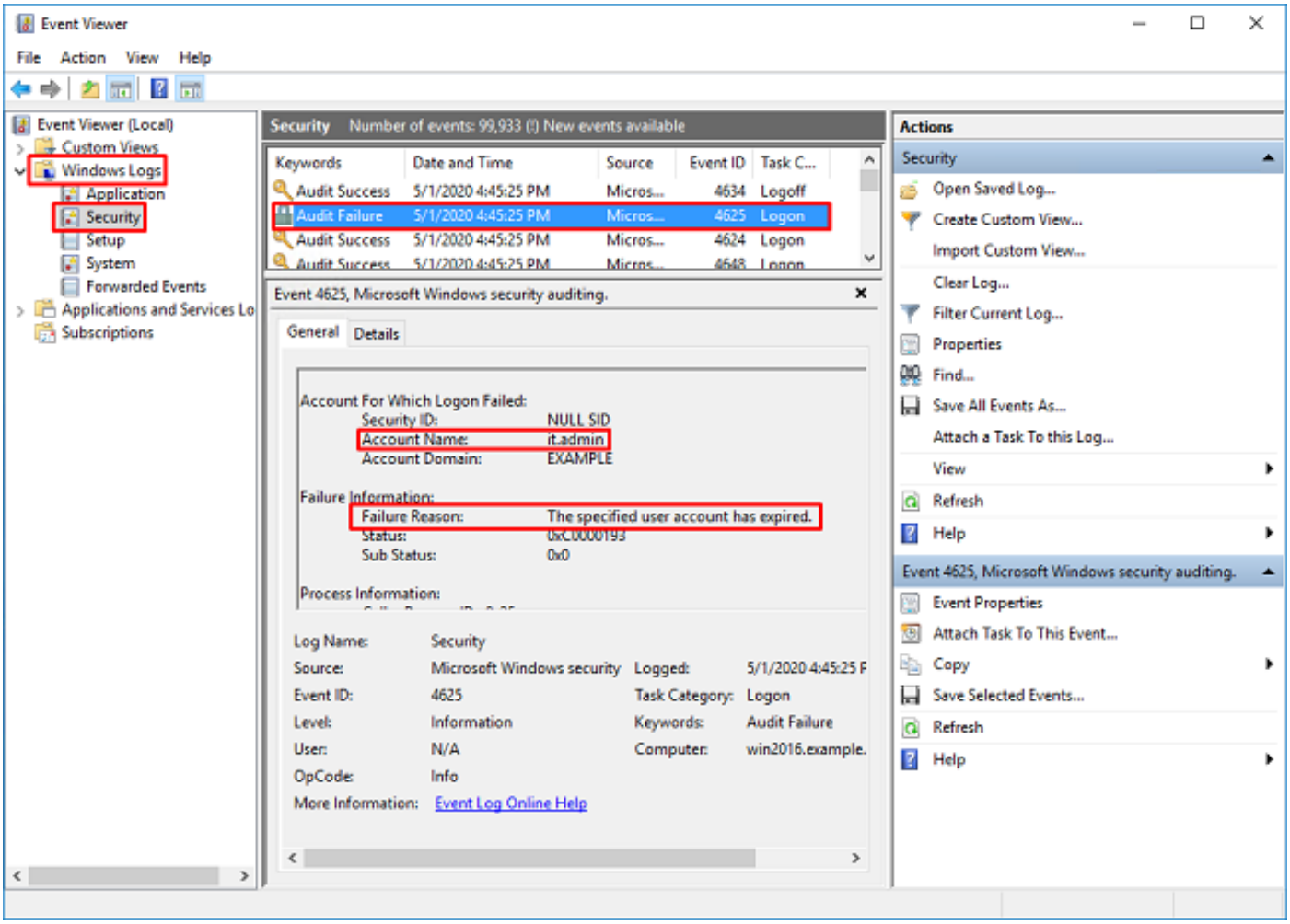
Windows Serverイベントビューアのログ

ADサーバのバンに関するイベントビューアの口グには、障害が発生した理由に関する詳細情報が記載されています。

1.イベントビューアを検索して**開きます。**



2. [**Windows** Logs]を展開し、[**Security**]をクリック**します**。図に示すように、**ユーザーのアカ**ウント名で[Audit Failure]を検索し、[Failure Information]を確認します。



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