تكوين مصادقة AD (LDAP) وهوية المستخدم على FTD المدارة بواسطة FDM لعملاء AnyConnect

المحتويات

المقدمة

الغرض من هذا المستند هو توضيح كيفية تكوين مصادقة Active Directory (AD) لعملاء AnyConnect الذين يتصلون بدفاع عن تهديد FirePOWER (FTD) من Cisco المدارة بواسطة إدارة جهاز FirePOWER (FDM). سيتم استخدام هوية المستخدم في سياسات الوصول لتقييد مستخدمي AnyConnect بعناوين IP ومنافذ معينة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بتكوين RA VPN على FDM
- معرفة أساسية بتكوين خادم LDAP على FDM
- معرفة أساسية بالإعلان

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- خادم Microsoft 2016
- تشغيل FTDv 6.5.0

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة والسيناريو

تم تكوين خادم Windows مسبقا باستخدام خدمات معلومات الإنترنت (IIS) وبروتوكول سطح المكتب البعيد (RDP) لاختبار هوية المستخدم. في دليل التكوين هذا، سيتم إنشاء ثلاثة حسابات مستخدمين ومجموعتين.

حسابات المستخدمين:

- مسؤول FTD: سيتم استخدام هذا كحساب دليل للسماح لـ FTD بالارتباط بخادم AD.
- مسؤول تقنية المعلومات: يستخدم حساب مسؤول الاختبار لإظهار هوية المستخدم.
- مستخدم الاختبار: حساب مستخدم اختبار يستخدم لإظهار هوية المستخدم.

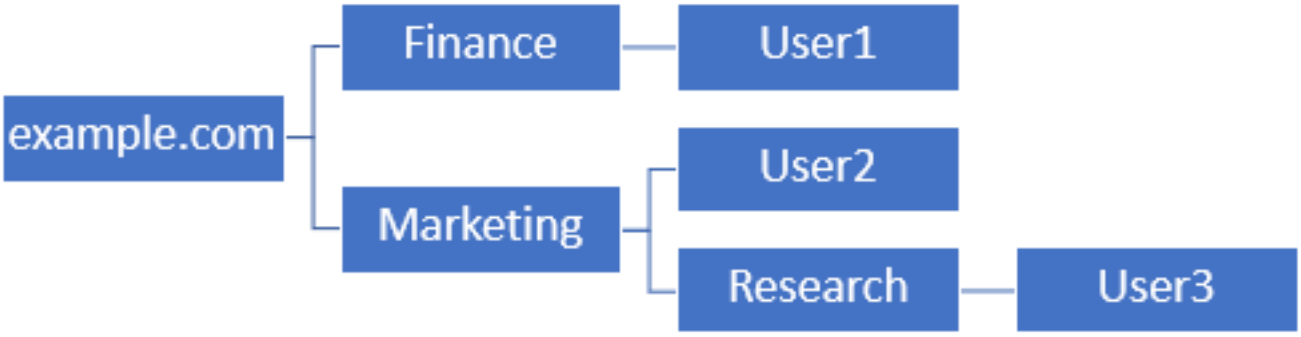
المجموعات:

- AnyConnect Admins: سيتم إضافة مجموعة اختبار إلى مسؤول تقنية المعلومات لإظهار هوية المستخدم. سيكون لهذه المجموعة وصول RDP إلى خادم Windows فقط
- مستخدمو AnyConnect: ستتم إضافة مجموعة اختبار إلى المستخدم لإظهار هوية المستخدم. سيكون لهذه المجموعة حق وصول HTTP إلى Windows Server فقط

تكوينات AD

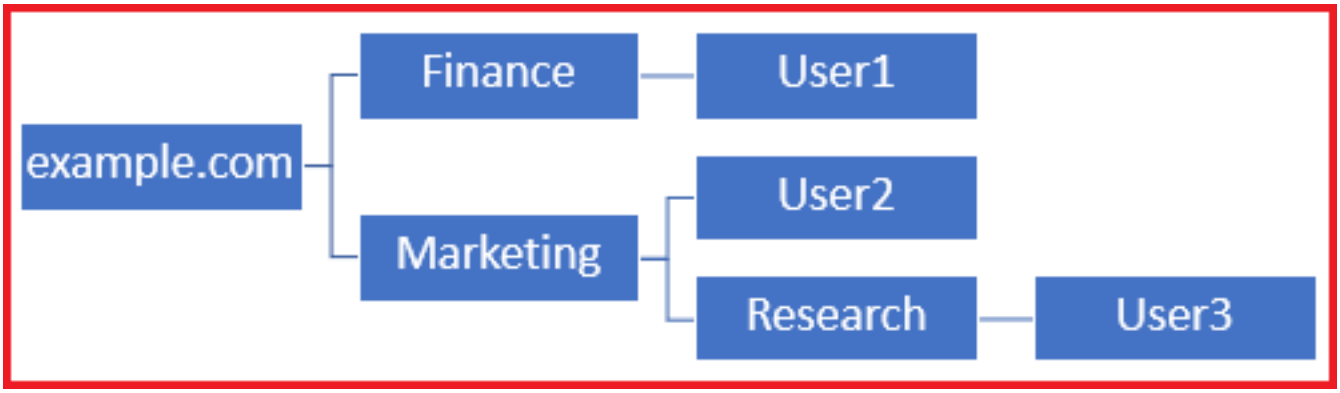
لتكوين مصادقة AD وهوية المستخدم بشكل مناسب على FTD، يلزم توفر عدد قليل من القيم. يجب إنشاء جميع هذه التفاصيل أو تجميعها على خادم Microsoft قبل إجراء التكوين على إدارة قاعدة بيانات المحول (FDM). القيم الرئيسية هي:

- اسم المجال: هذا هو اسم المجال للخادم. في دليل التكوين هذا، example.com هو اسم المجال.
- عنوان IP/FQDN للخادم: عنوان IP أو FQDN المستخدم للوصول إلى خادم Microsoft. إذا تم استخدام FQDN، فيجب تكوين خادم DNS داخل FDM و FTD لحل FQDN. في دليل التكوين هذا، تكون هذه القيم هي **win2016.example.com** الذي يتم الحل إلى 192.168.1.1.
- منفذ الخادم: المنفذ المستخدم بواسطة خدمة LDAP. بشكل افتراضي، سيستخدم LDAP و STARTTLS منفذ TCP 389 لـ LDAP و LDAP عبر SSL (LDAPs) منفذ TCP 636.
- المرجع المصدق الجذر: في حالة إستخدام LDAP أو STARTTLS، يلزم إستخدام المرجع المصدق الجذر لتوقيع شهادة SSL المستخدمة بواسطة LDAPs.
- اسم مستخدم الدليل وكلمة المرور: هذا هو الحساب المستخدم من قبل FDM و FTD للربط بخادم LDAP ومصادقة المستخدمين والبحث عن مستخدمين ومجموعات. سيتم إنشاء حساب باسم "مسؤول FTD" لهذا الغرض.
- الاسم المميز الأساسي (DN): يمثل DN الأساسي نقطة البدء FDM وسيطلب FTD من Active Directory البدء عند البحث عن مستخدمين. في دليل التكوين هذا، سيتم إستخدام المجال الجذر example.com على أنه DN الأساسي، ومع ذلك، لبيئة الإنتاج، قد يكون إستخدام DN الأساسي بشكل إضافي داخل التدرج الهرمي لـ LDAP أفضل. على سبيل المثال، أستخدم التدرج الهرمي LDAP هذا:



إذا كان المسؤول يريد أن يكون المستخدمون داخل وحدة التسويق التنظيمية قادرين على المصادقة على DN الأساسي الذي يمكن تعيينه على الجذر (example.com)، فإن ذلك سيسمح أيضا لـ User1 الموجود ضمن الوحدة التنظيمية المالية بتسجيل الدخول أيضا نظرا لأن بحث المستخدم سيبدأ من الجذر ويتجه إلى المالية والتسويق والبحث.

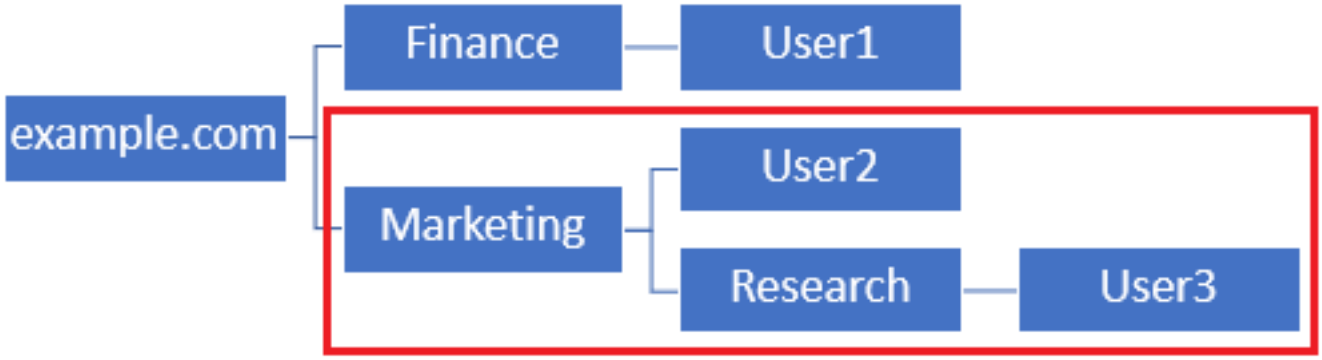
تم تعيين DN الأساسي على example.com.



من أجل تقييد عمليات تسجيل الدخول للمستخدمين فقط في وحدة مؤسسة التسويق أو أدناه، يمكن للمسؤول بدلا من ذلك تعيين DN الأساسي على "التسويق". يمكن الآن ل

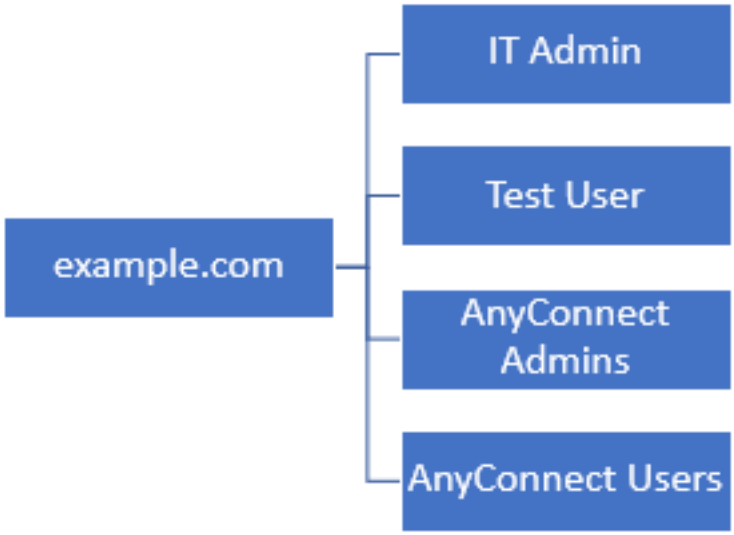
User2 و User3 فقط المصادقة لأن البحث سيبدأ في "التسويق".

تعيين DN الأساسي على التسويق:



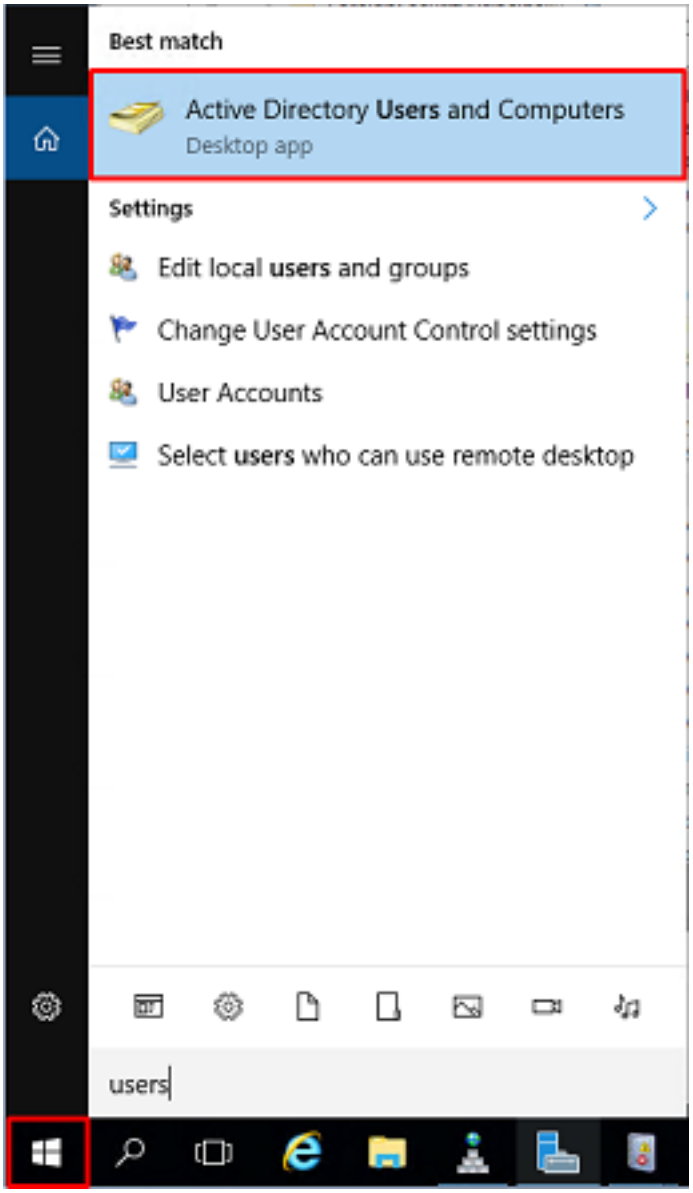
لاحظ أنه لمزيد من التحكم متعدد المستويات داخل FTD والذي سيتم السماح للمستخدمين بتوصيل أو تعيين تفويض مختلف للمستخدمين استنادا إلى سمات AD الخاصة بهم، سيتعين تكوين خريطة تفويض LDAP.

يتم إستخدام هذا التدرج الهرمي ل LDAP المبسط في دليل التكوين هذا وسيتم إستخدام DN للجذر example.com ل DN الأساسي.

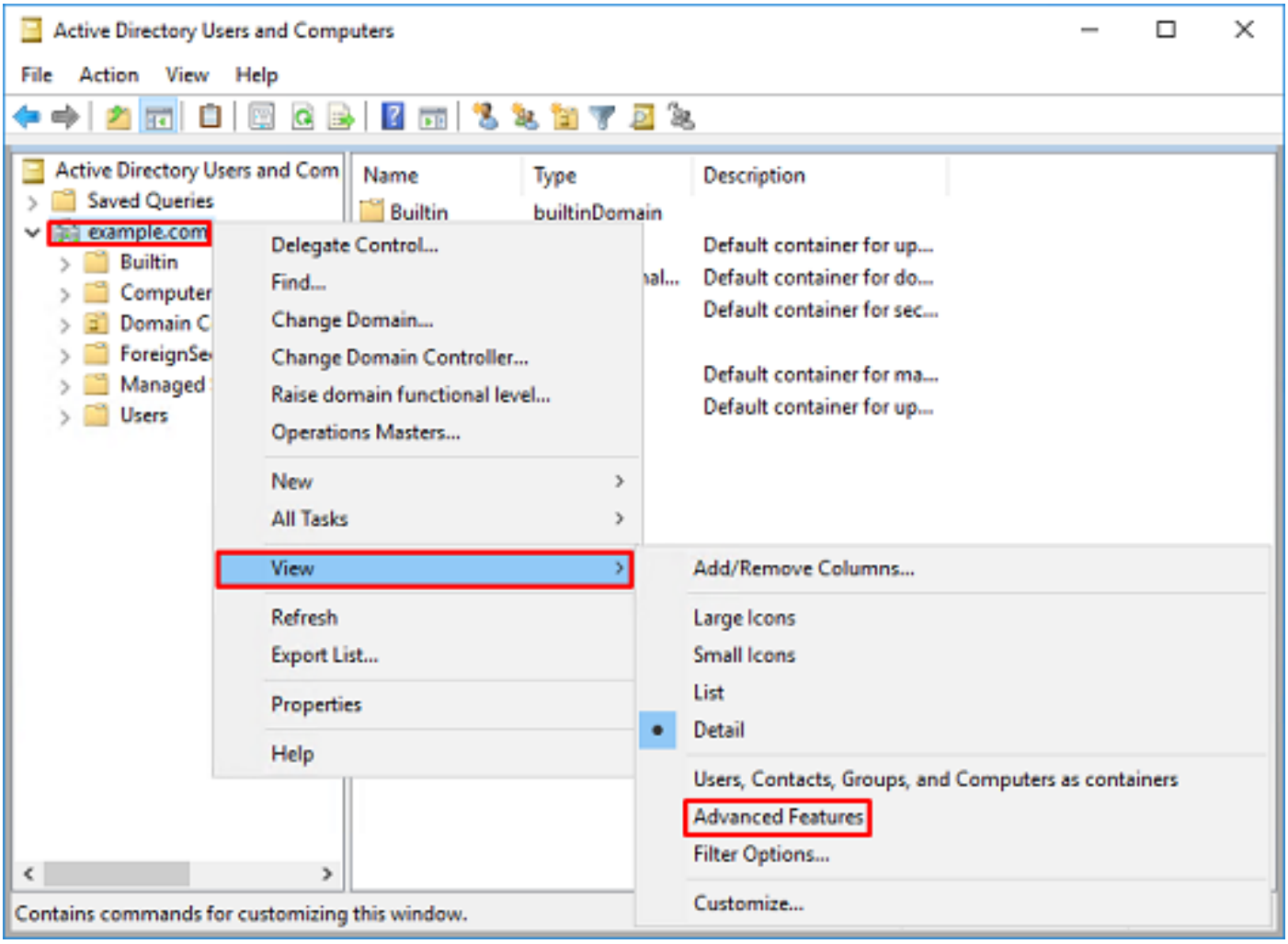


تحديد LDAP الأساسي DN

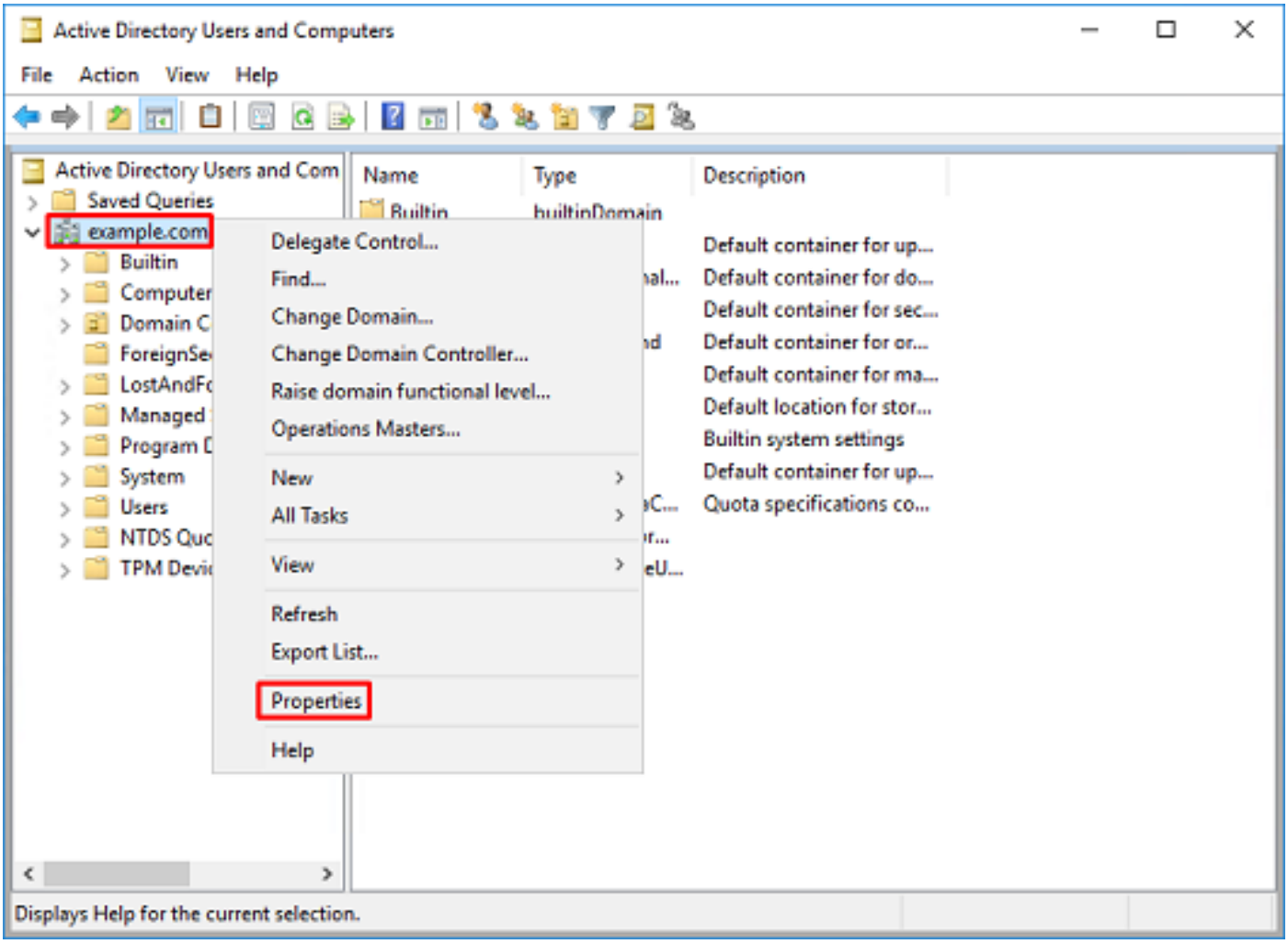
1. مستخدمو الإعلان المفتوح وأجهزة الكمبيوتر.



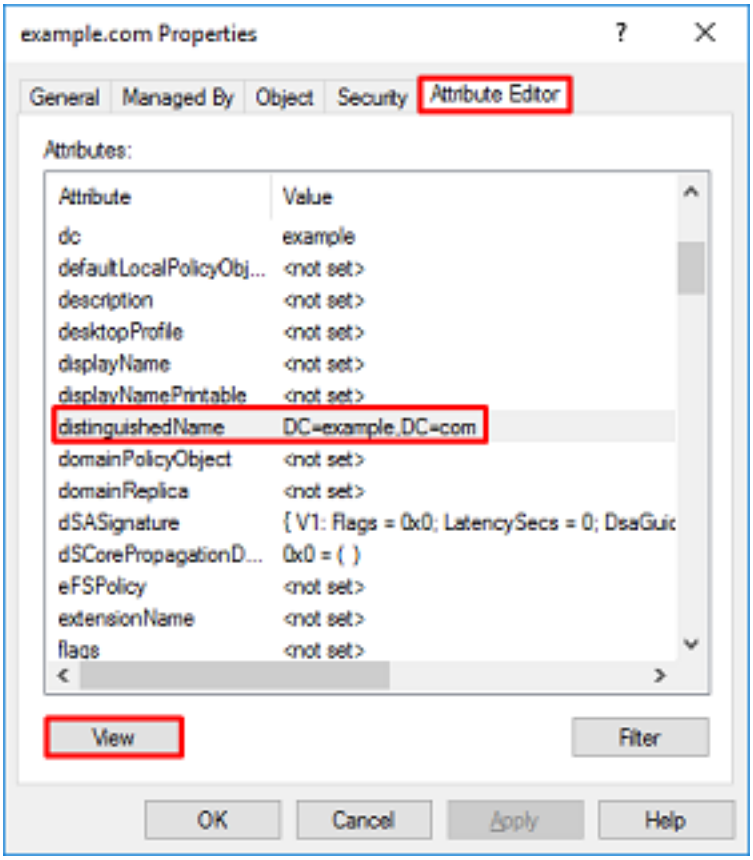
2. انقر بزر الماوس الأيمن فوق المجال الجذر (لفتح الحاوية)، ثم انقر بزر الماوس الأيمن فوق المجال الجذر، ثم انتقل إلى **عرض** وانقر فوق **ميزات متقدمة**.



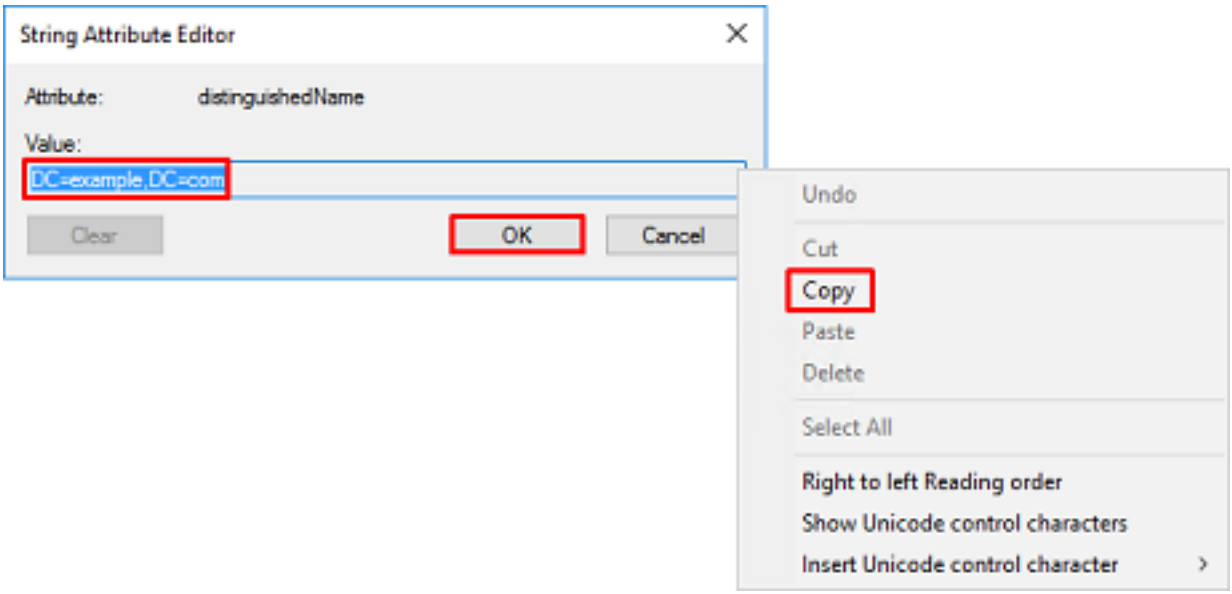
3. سيتيح ذلك عرض الخصائص الإضافية تحت كائنات AD. على سبيل المثال، للعثور على شبكة DN الخاصة بالجذر الرئيسي example.com، انقر بزر الماوس الأيمن فوق **example.com** ثم انتقل إلى **الخصائص**.

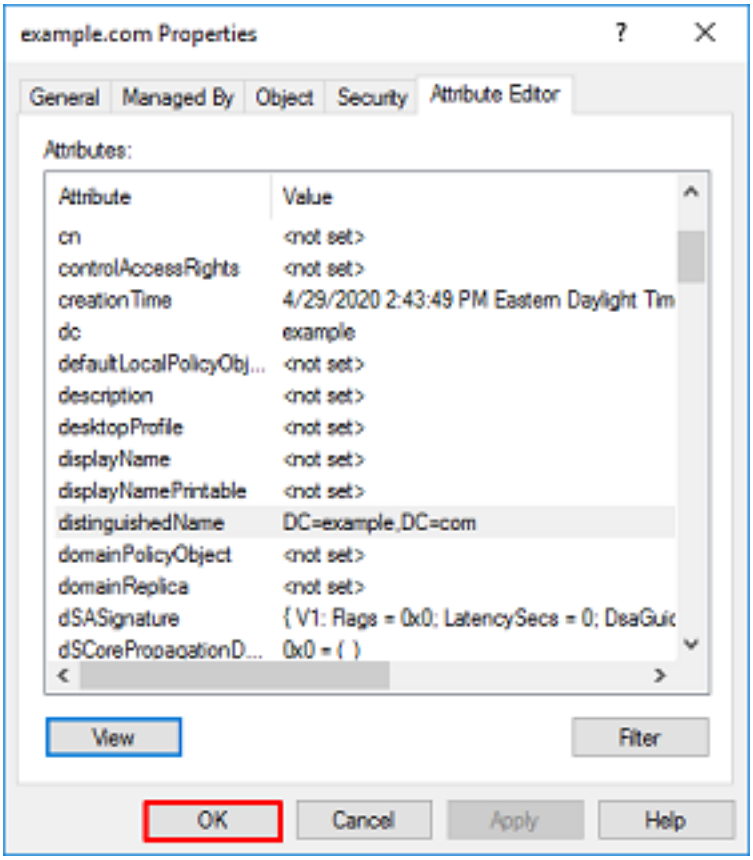


4. تحت **خصائص**، انقر فوق علامة التبويب **محرر السمات**. ابحث عن **اسم مميز** تحت السمات، ثم انقر فوق **عرض**.

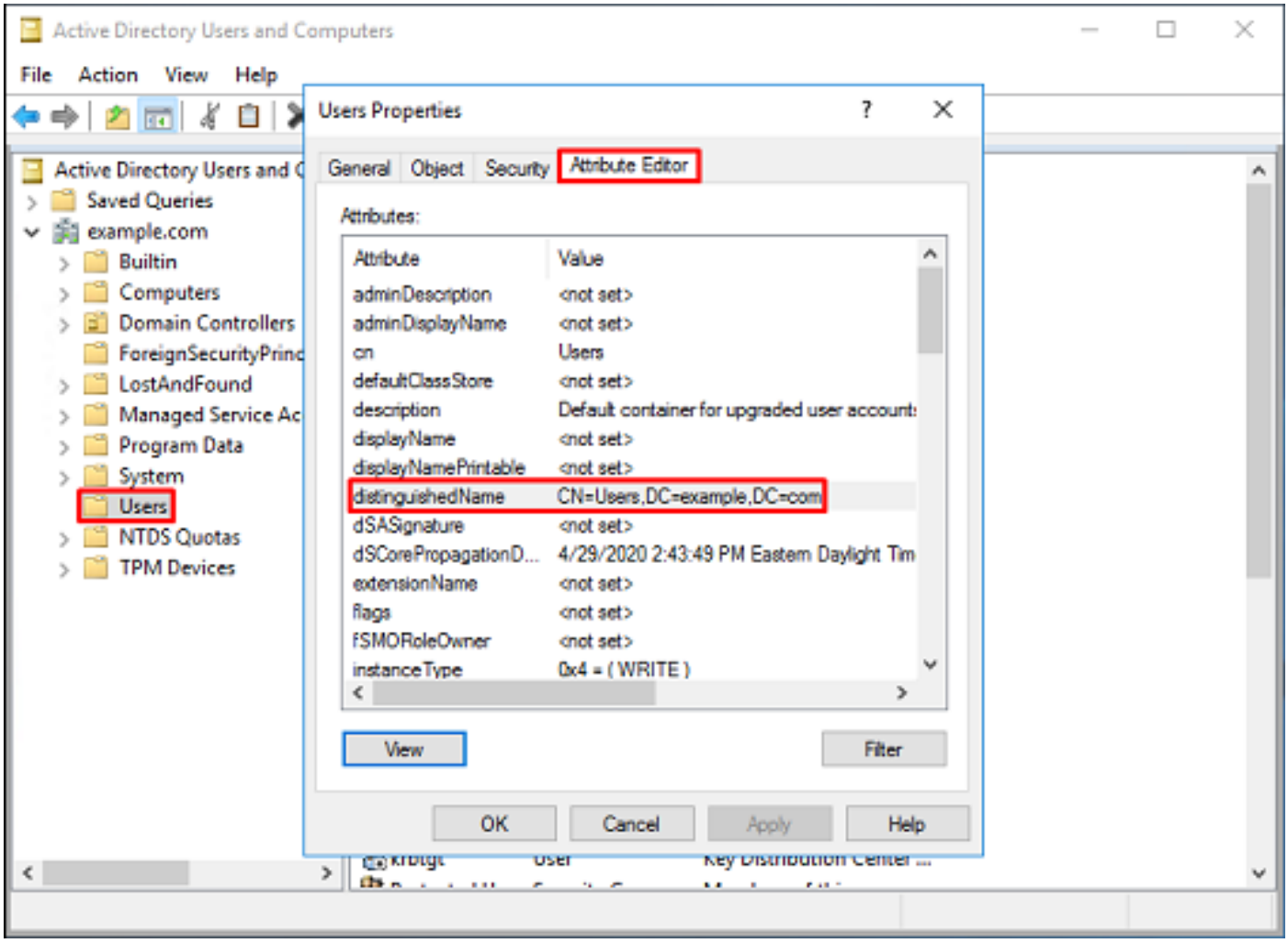


5. سيؤدي ذلك إلى فتح نافذة جديدة حيث يمكن نسخ DN ولصقه في FDM لاحقا. في هذا المثال، يكون DN الجذر هو DC=example، dc=com. انسخ القيمة. انقر فوق **موافق** للخروج من نافذة محرر سمات السلسلة، وانقر فوق **موافق** مرة أخرى للخروج من الخصائص.

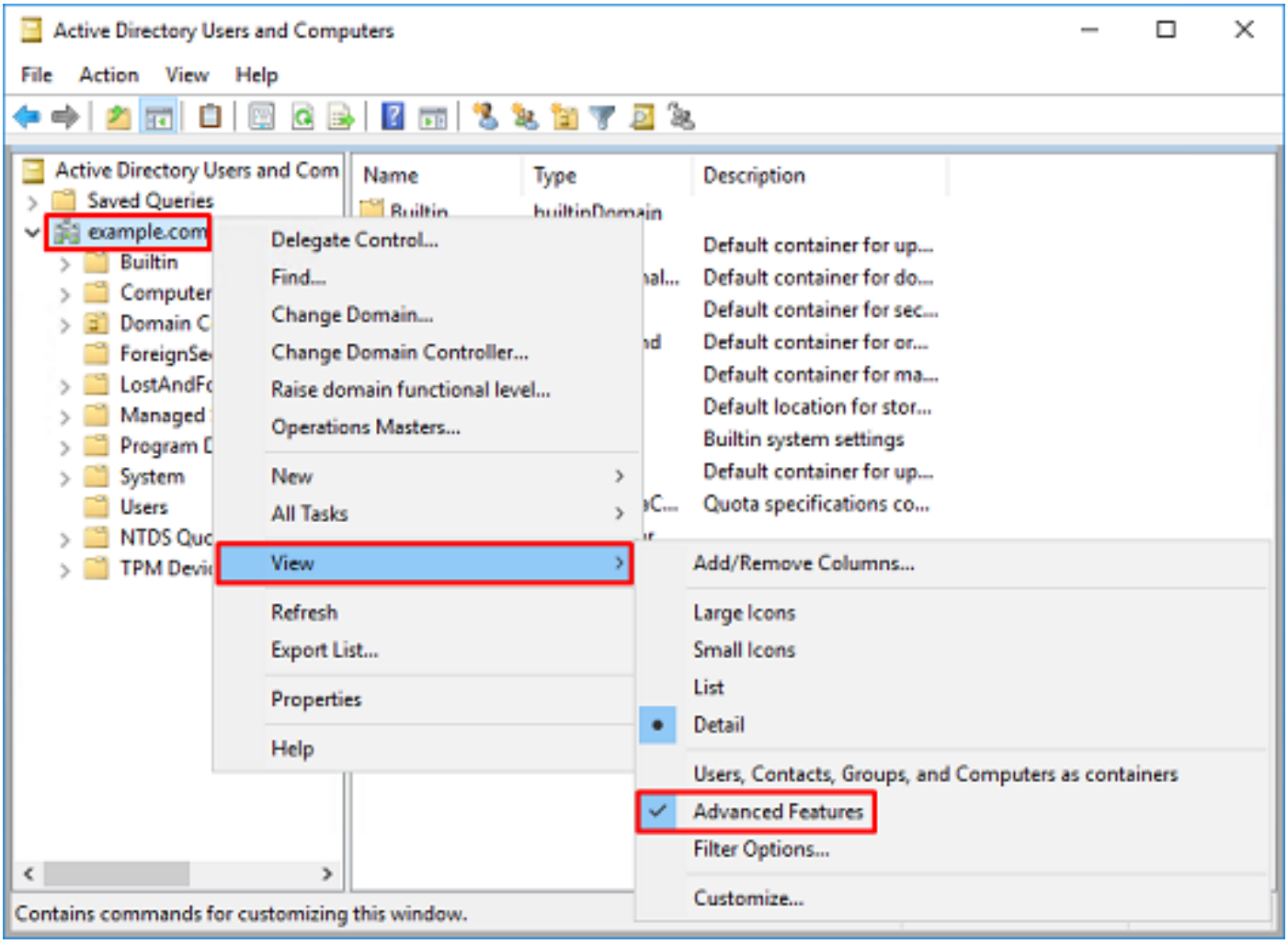




يمكن القيام بذلك بالنسبة لكائنات متعددة داخل AD. على سبيل المثال، يتم إستخدام هذه الخطوات للعثور على DN الخاص بحاوية المستخدم:



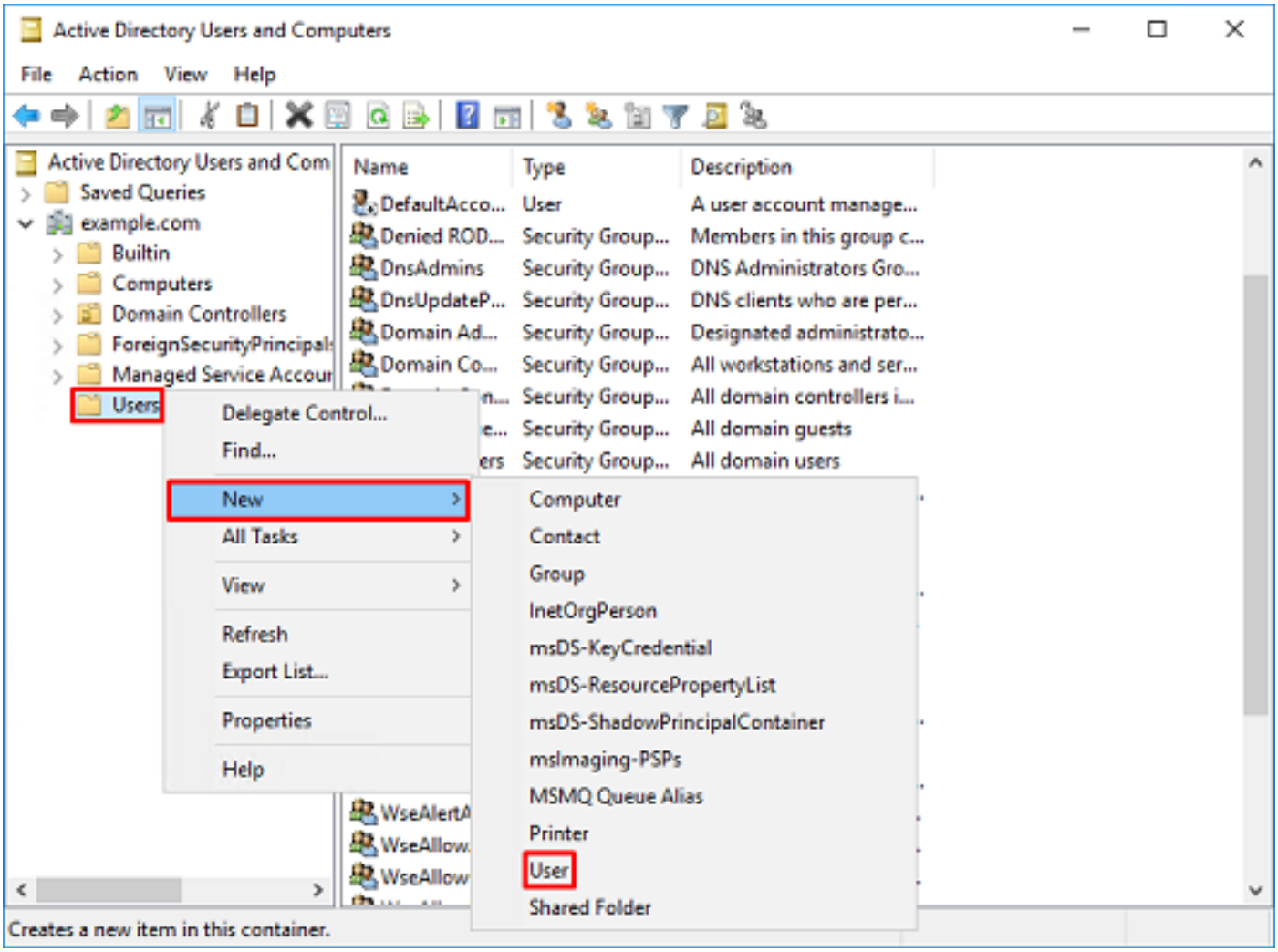
6. يمكن إزالة طريقة عرض المميزات المتقدمة. انقر بزر الماوس الأيمن على شبكة DN الجذر، وتصفح **للعرض**، وانقر فوق **المميزات المتقدمة** مرة أخرى.



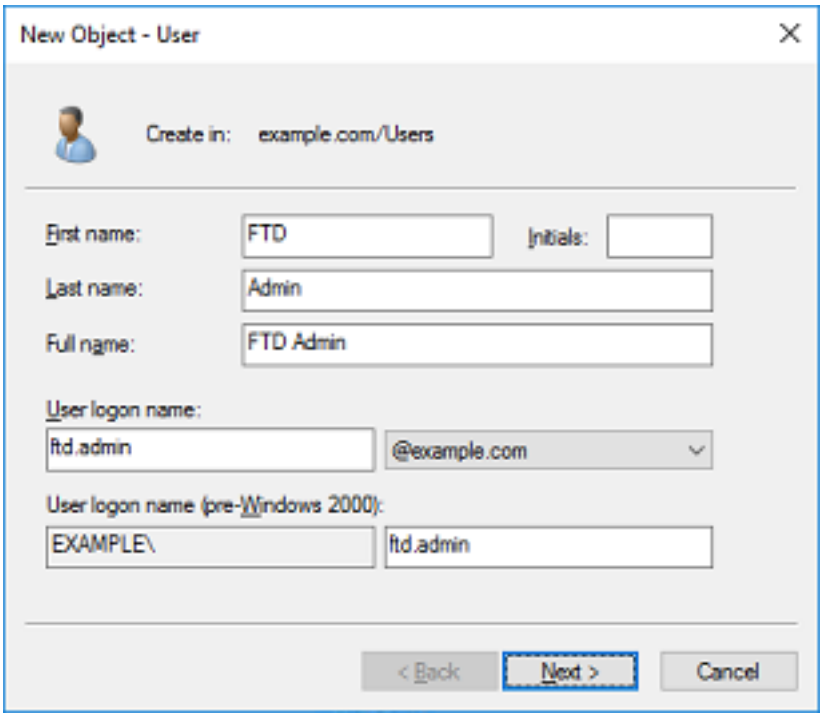
إنشاء حساب FTD

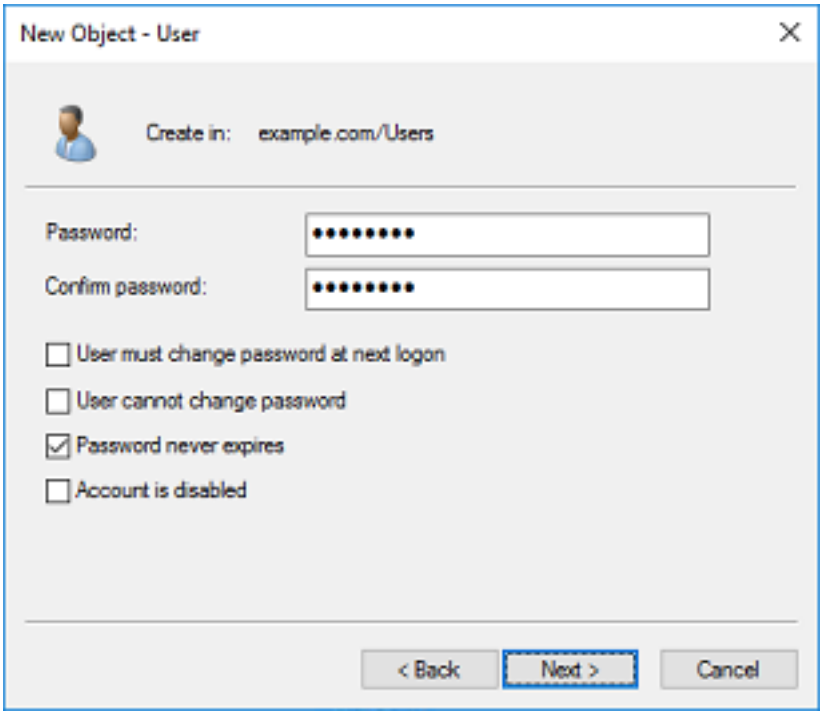
سيسمح حساب المستخدم هذا لـ FDM و FTD بالارتباط مع AD للبحث عن المستخدمين والمجموعات ومصادقتهم. الغرض من إنشاء حساب FTD منفصل هو منع الوصول غير المصرح به إلى مكان آخر داخل الشبكة إذا تم اختراق بيانات الاعتماد المستخدمة للربط. لا يلزم أن يكون هذا الحساب ضمن نطاق DN الأساسي.

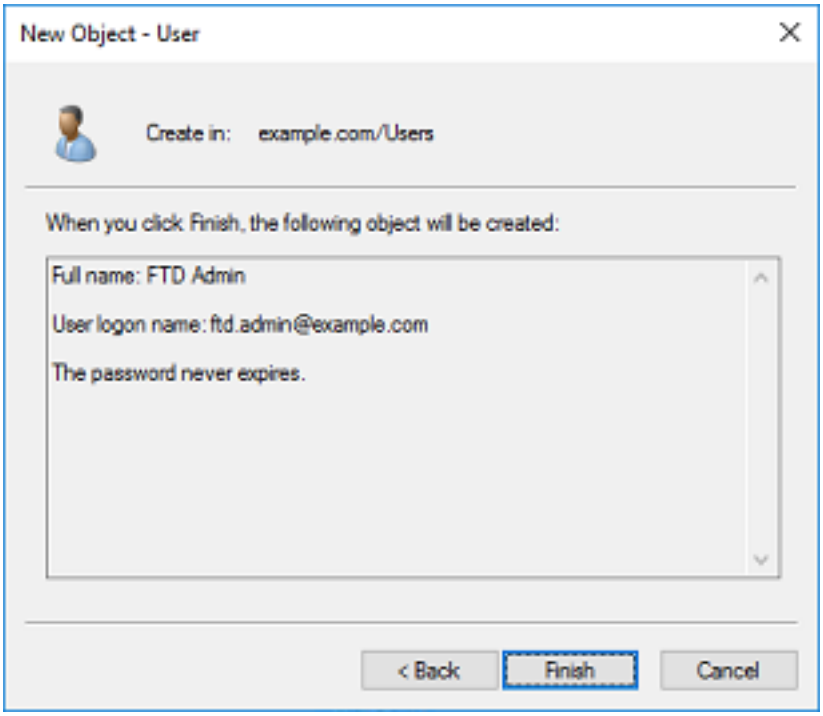
1. في **Active Directory Users and Computers**، انقر بزر الماوس الأيمن فوق الحاوية/المنظمة التي سيتم إضافة حساب FTD إليها. في هذا التكوين، ستتم إضافة حساب FTD ضمن حاوية "المستخدمون" ضمن اسم المستخدم **ftd.admin@example.com**. انقر بزر الماوس الأيمن فوق **مستخدمين**، ثم انقر فوق **جديد > مستخدم**.



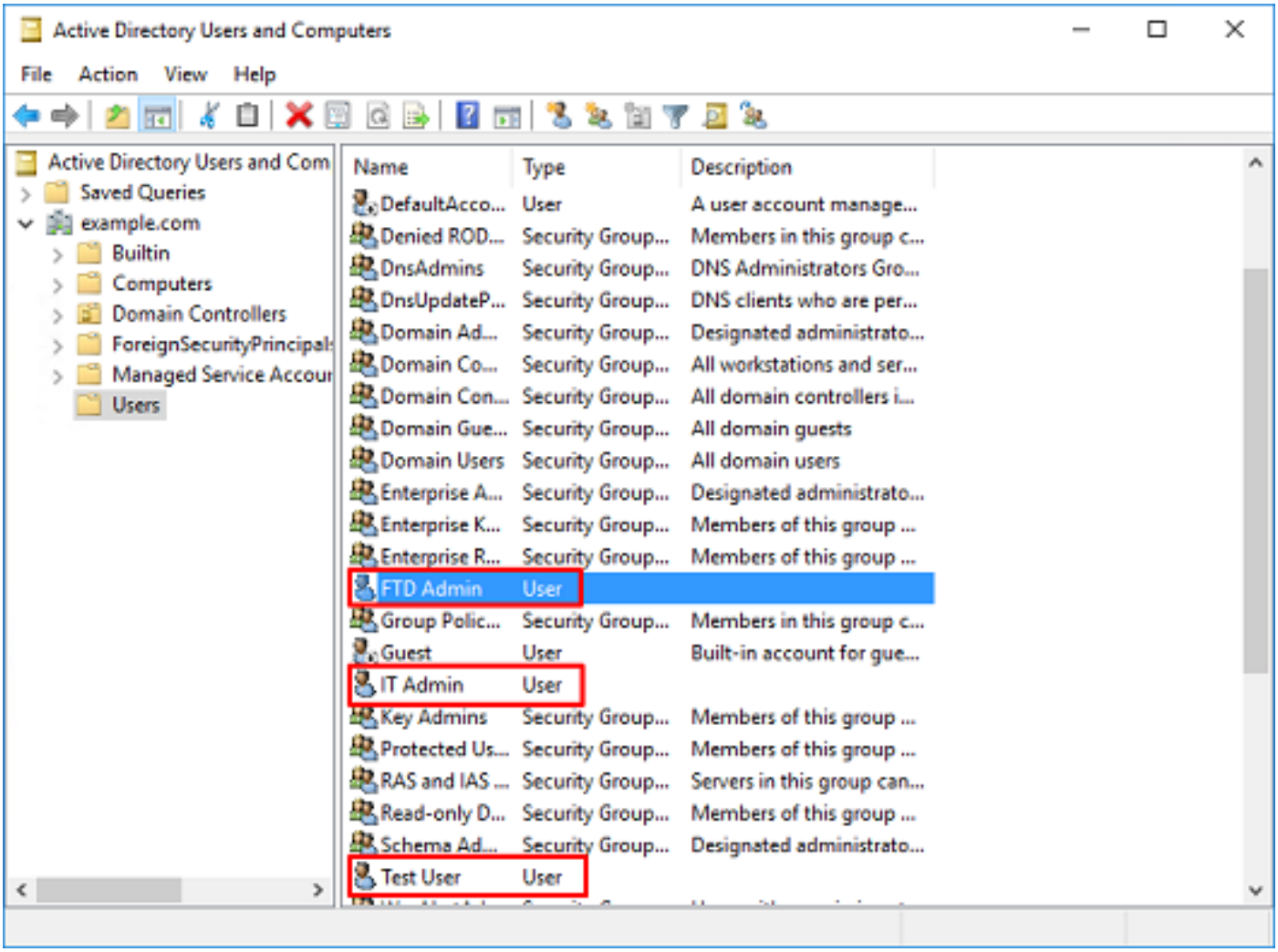
2. التنقل عبر معالج **كائن جديد - مستخدم**.







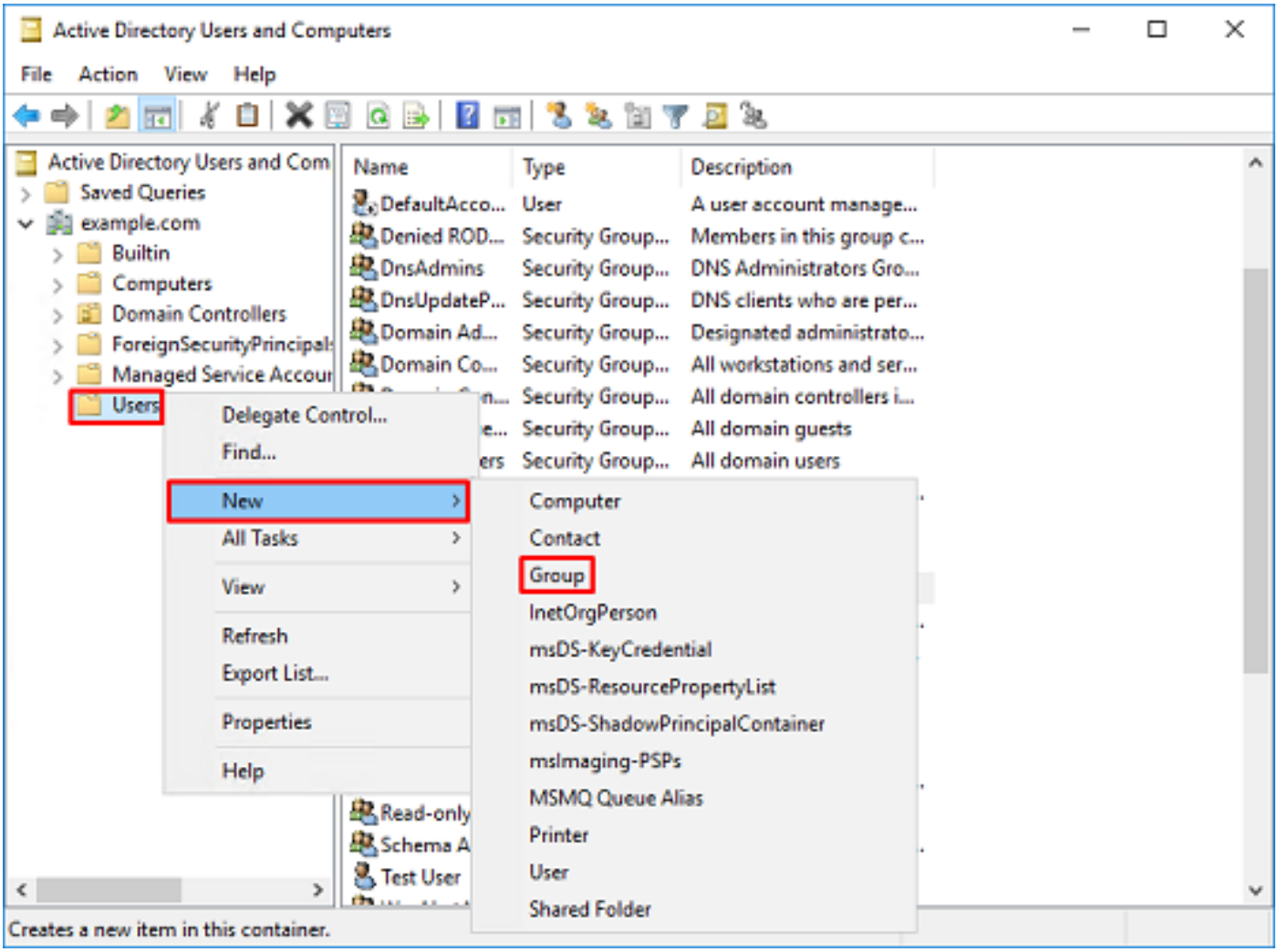
3. تحقق من إنشاء حساب FTD. وبالإضافة إلى ذلك، تم إنشاء حسابين إضافيين، وهما **مسؤول تقنية المعلومات ومستخدم الاختبار**.



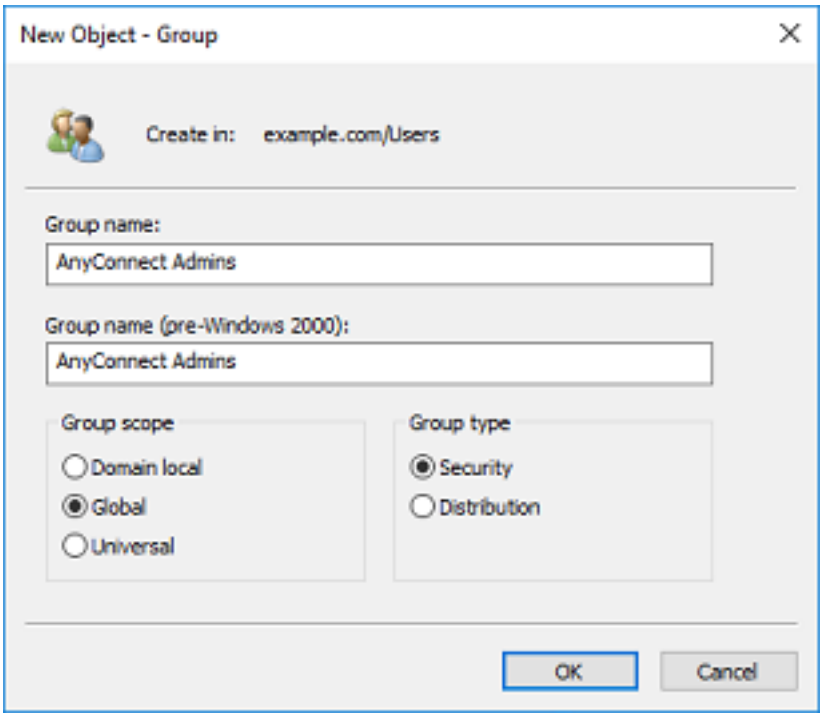
إنشاء مجموعات العلامات وإضافة مستخدمين إلى مجموعات العلامات (إختياري)

وعلى الرغم من عدم الحاجة إلى المصادقة، يمكن إستخدام المجموعات لتسهيل تطبيق سياسات الوصول على عدة مستخدمين بالإضافة إلى تفويض LDAP. في دليل التكوين هذا، سيتم إستخدام المجموعات لتطبيق إعدادات نهج التحكم بالوصول لاحقا من خلال هوية المستخدم داخل FDM.

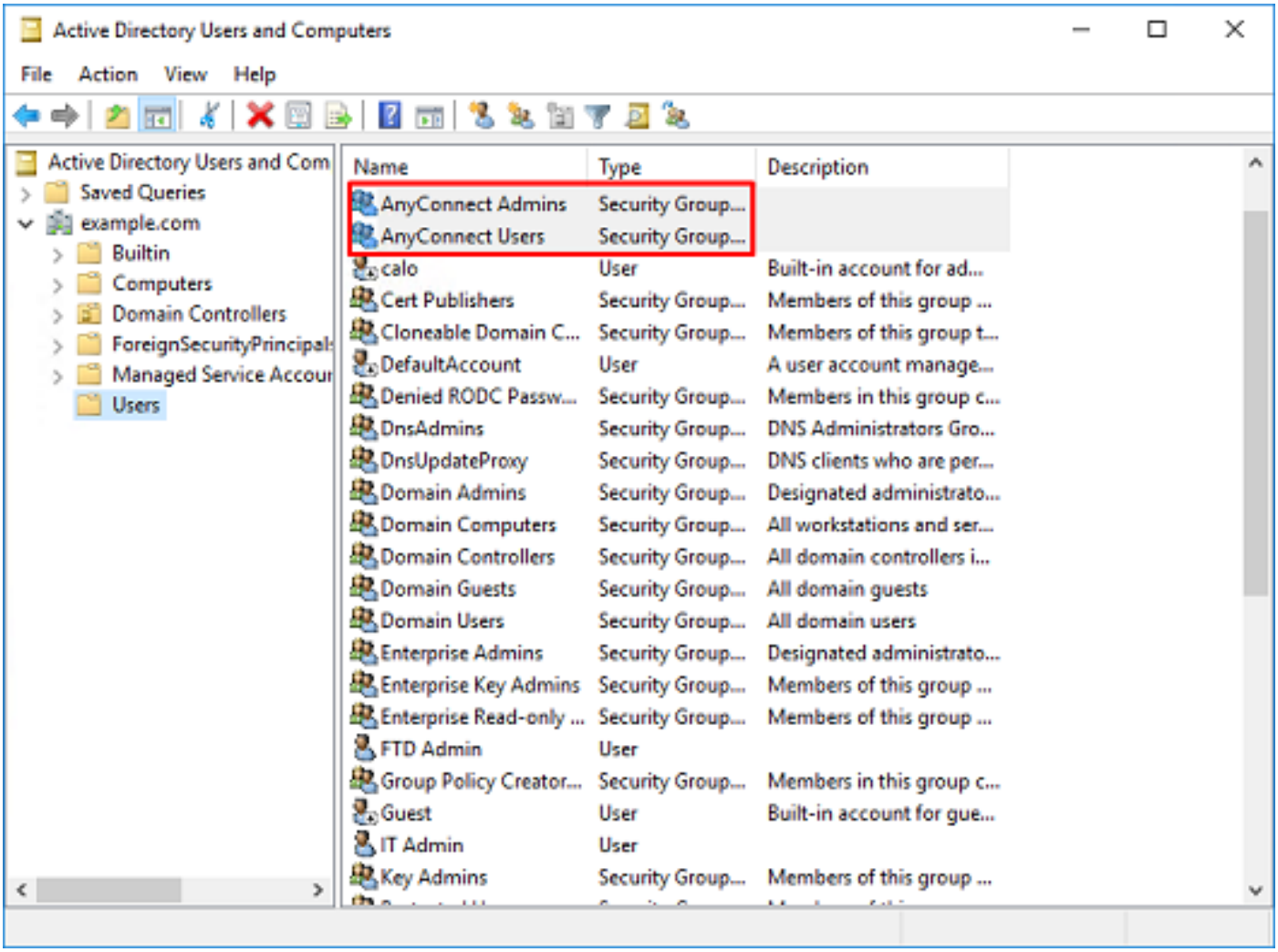
1. في **Active Directory Users and Computers**، انقر بزر الماوس الأيمن فوق الحاوية/المؤسسة التي ستتم إضافة المجموعة الجديدة إليها. في هذا المثال، ستتم إضافة **مسؤولي AnyConnect** في المجموعة ضمن الحاوية مستخدمين. انقر بزر الماوس الأيمن فوق **المستخدمين**، ثم انقر فوق **جديد > مجموعة**.



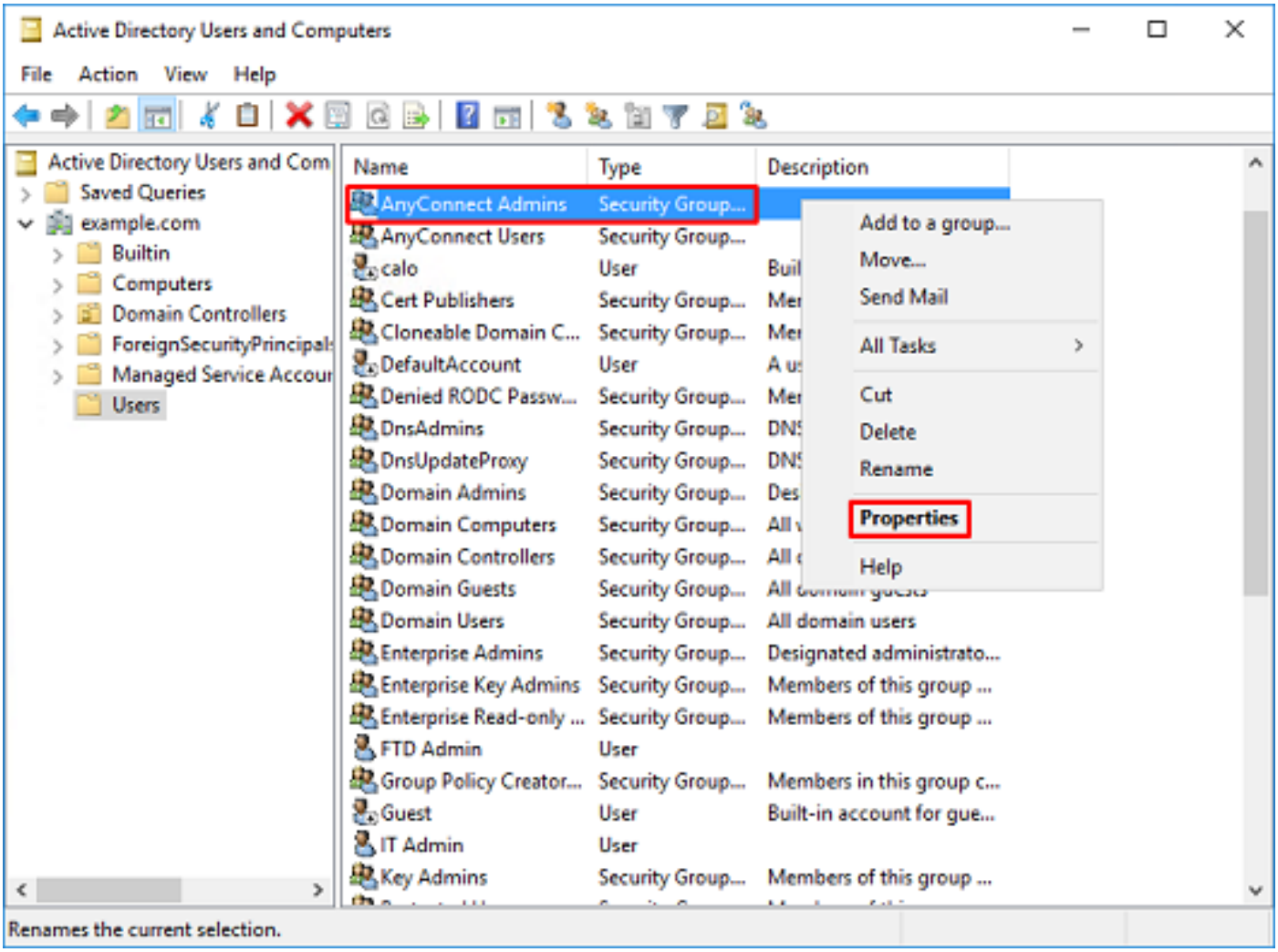
2. تصفح خلال معالج **الكائن الجديد - المجموعة** كما هو موضح في الصورة.



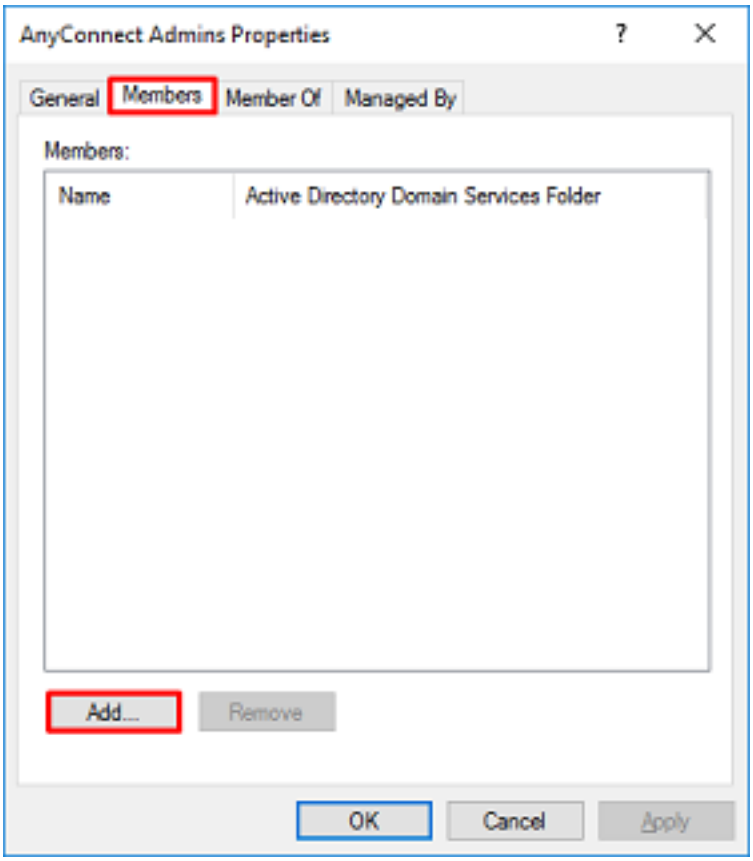
3. تأكد من إنشاء المجموعة. تم أيضا إنشاء مجموعة **مستخدمي AnyConnect**.



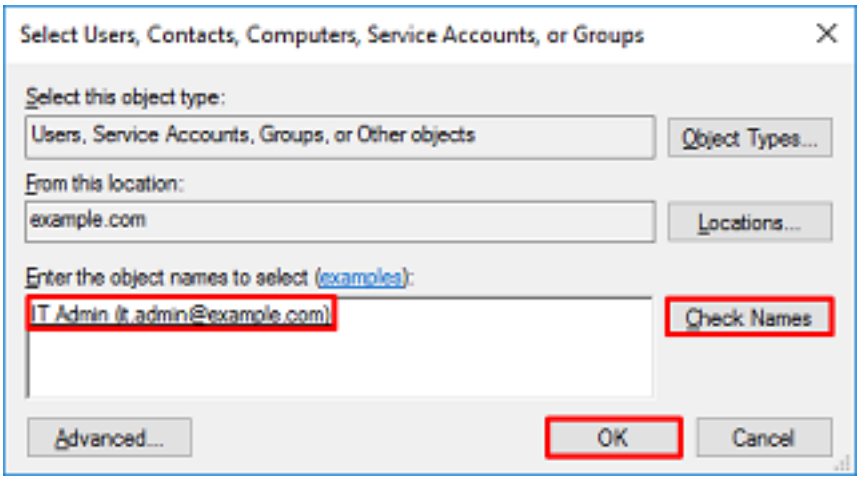
4. انقر بزر الماوس الأيمن فوق المجموعة التي سيتم إضافة المستخدم (المستخدمين) إليها، ثم حدد **خصائص**. في هذا التكوين، ستتم إضافة **مسؤول تقنية المعلومات** للمستخدم إلى المجموعة AnyConnect Admins وسيتم إضافة **مستخدم اختبار المستخدم** إلى المجموعة **مستخدمي** AnyConnect.



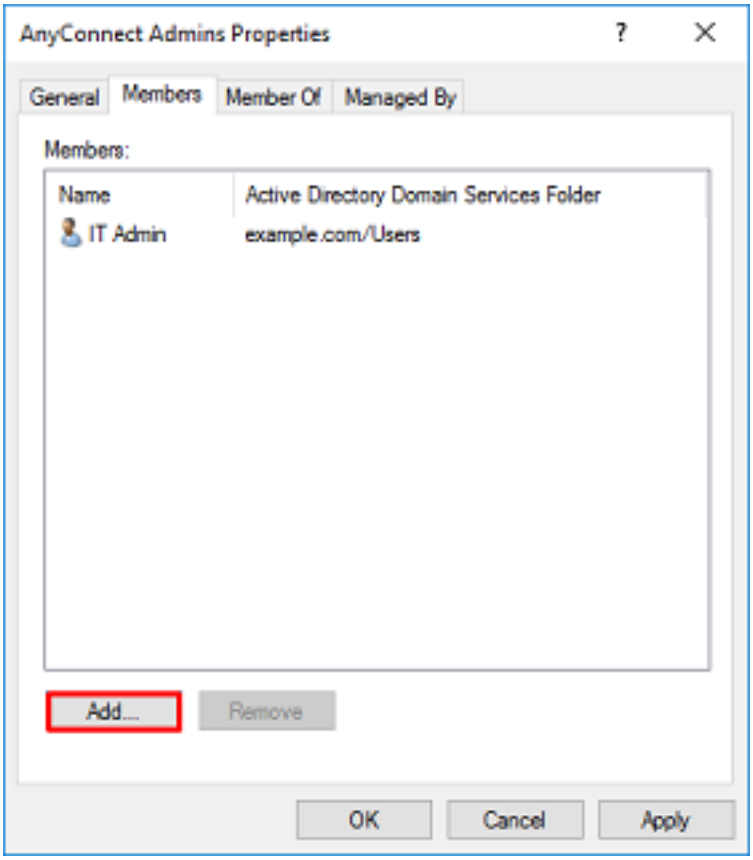
5. انقر فوق علامة التبويب **أعضاء** ثم انقر فوق **إضافة** كما هو موضح في الصورة.



أدخل المستخدم في الحقل وانقر فوق الزر **التحقق من الأسماء** للتحقق من العثور على المستخدم. ما إن تم التحقق، طقطقت **ok**.

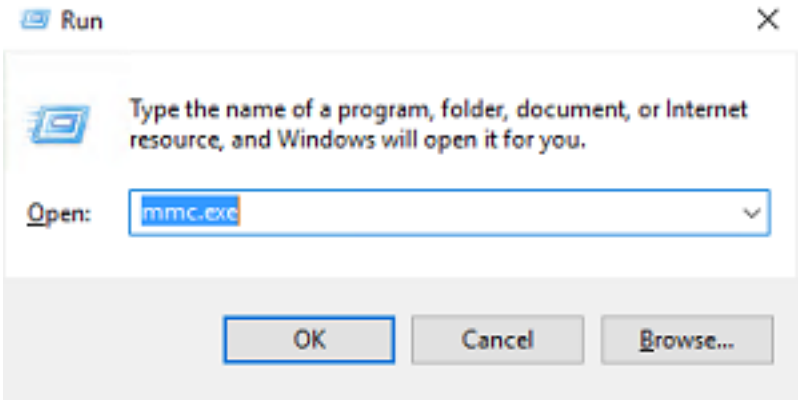


تحقق من إضافة المستخدم الصحيح، ثم انقر فوق الزر **موافق**. كما تتم إضافة "مستخدم إختبار المستخدم" إلى مجموعة مستخدمي AnyConnect باستخدام الخطوات نفسها.

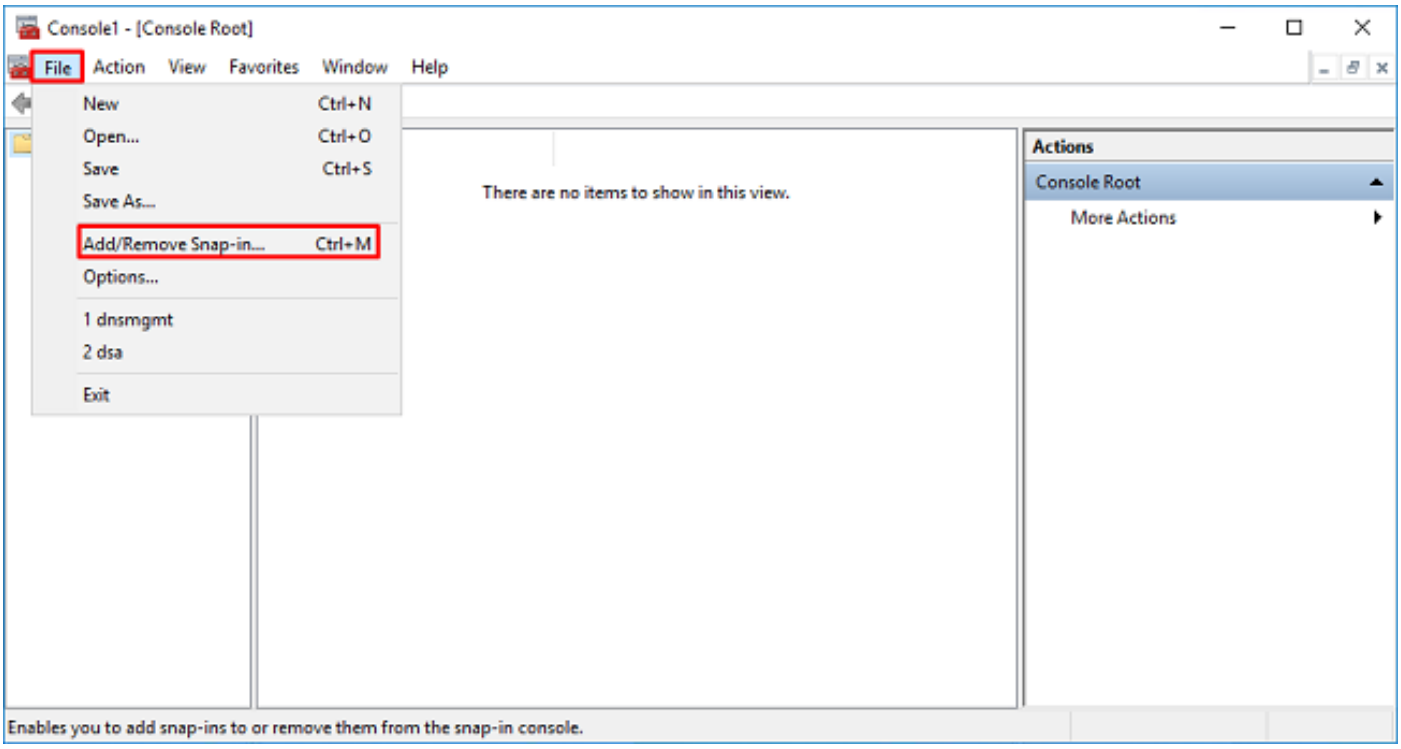


نسخ جذر شهادة SSL الخاص ب LDAP (مطلوب فقط ل LDAPs أو STARTTLS)

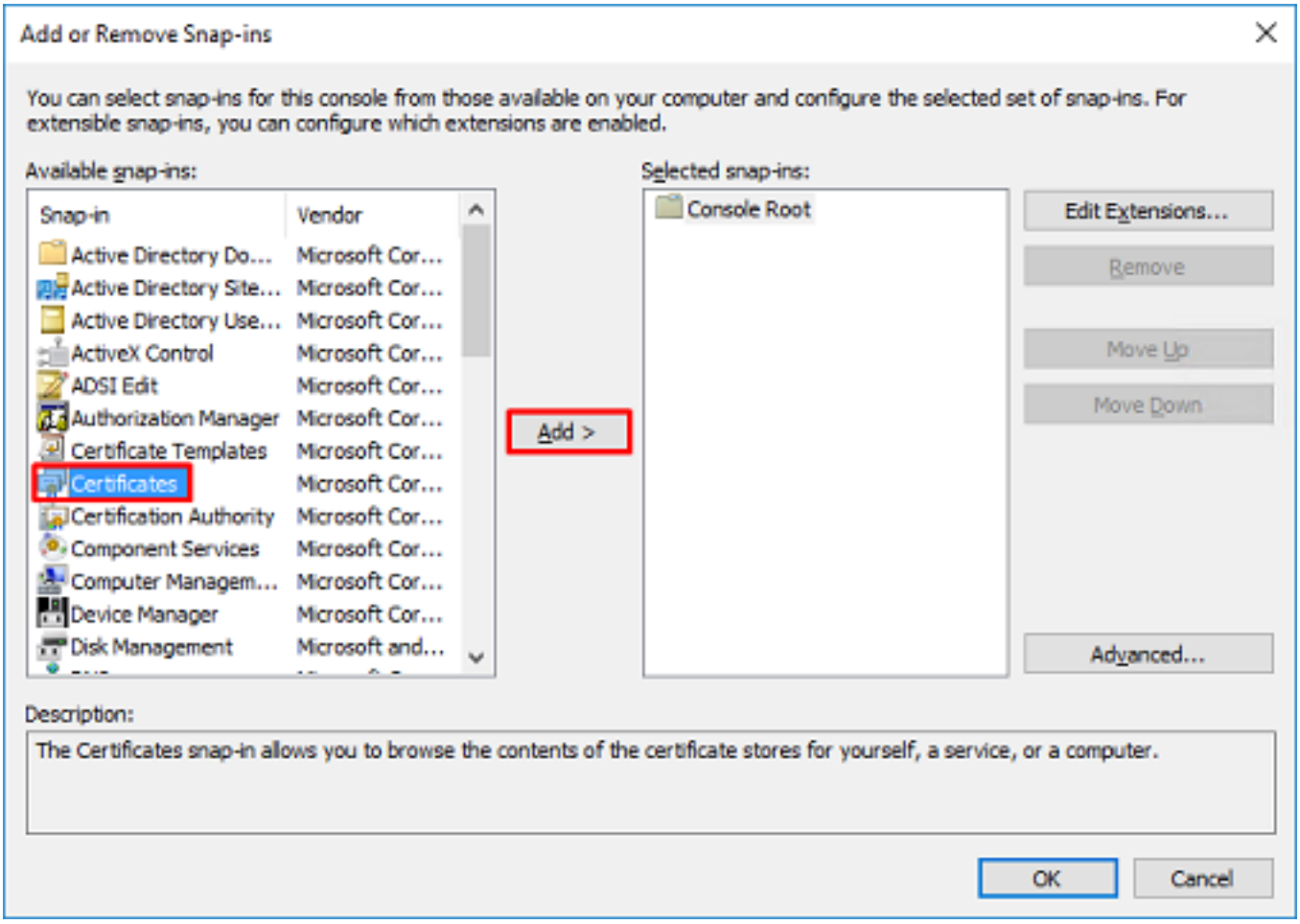
1. اضغط على **Win+R** واكتب **mmc.exe**. وانقر فوق **OK**.



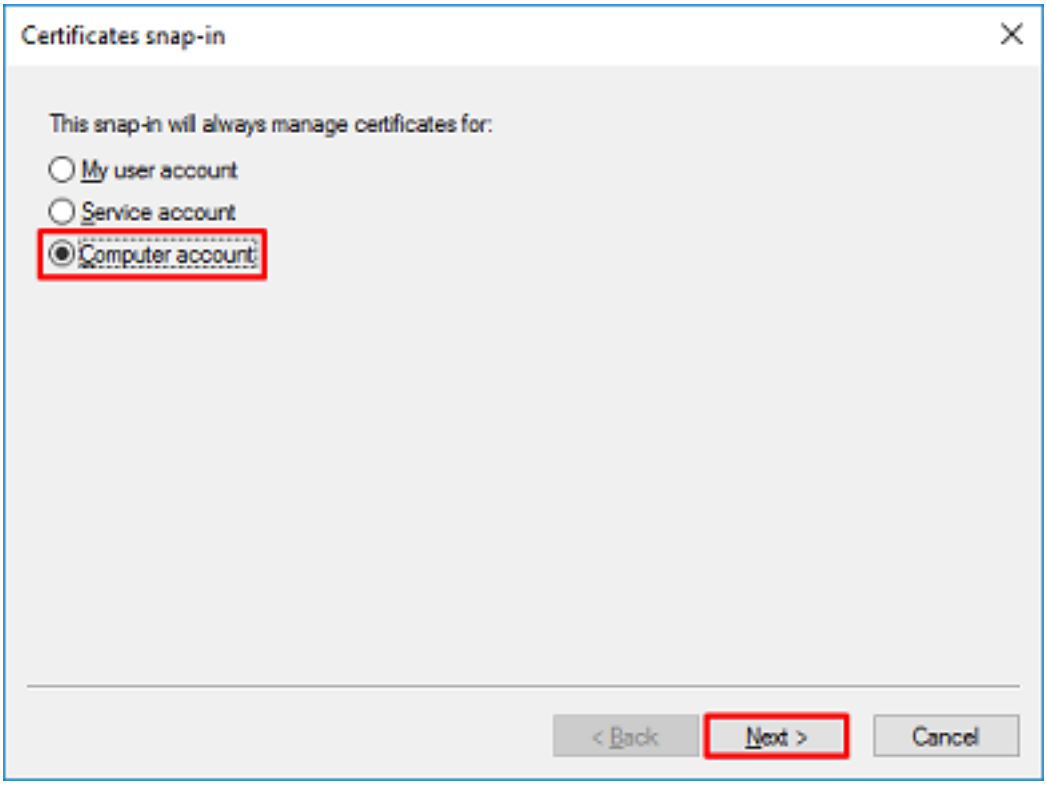
2. انتقل إلى **ملف > إضافة/إزالة الأداة الإضافية...** كما هو موضح في الصورة.



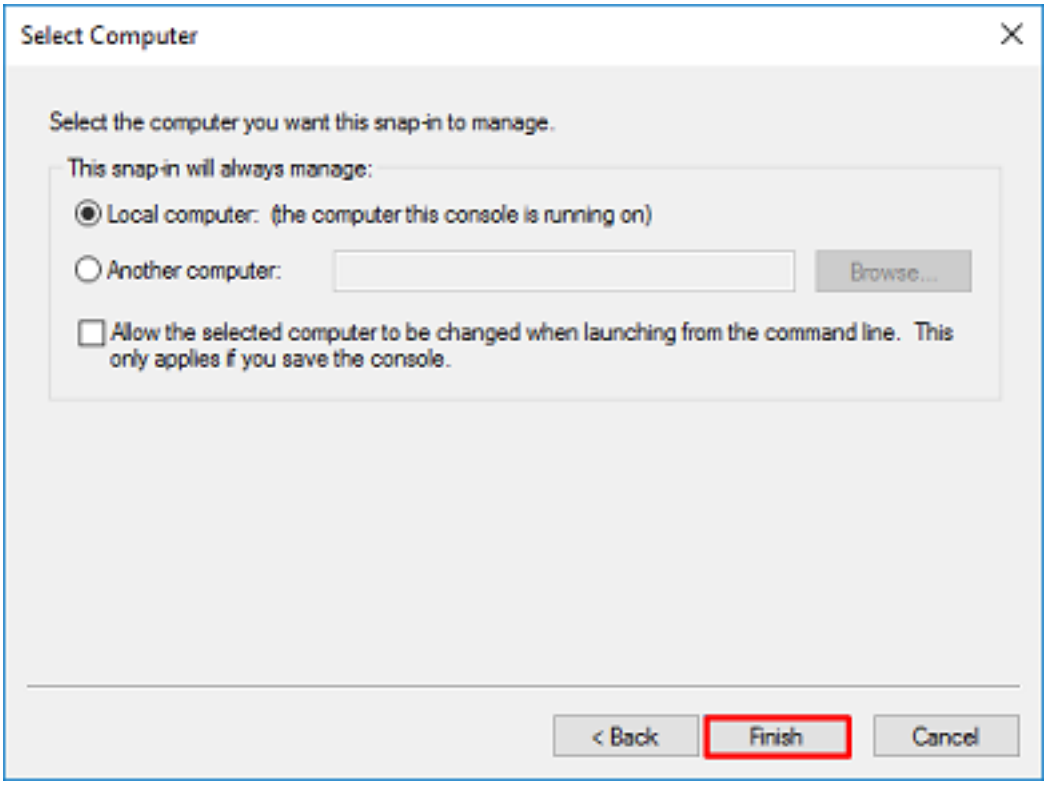
3. تحت الأدوات الإضافية المتاحة، انقر فوق **الشهادات**، ثم انقر فوق **إضافة**.



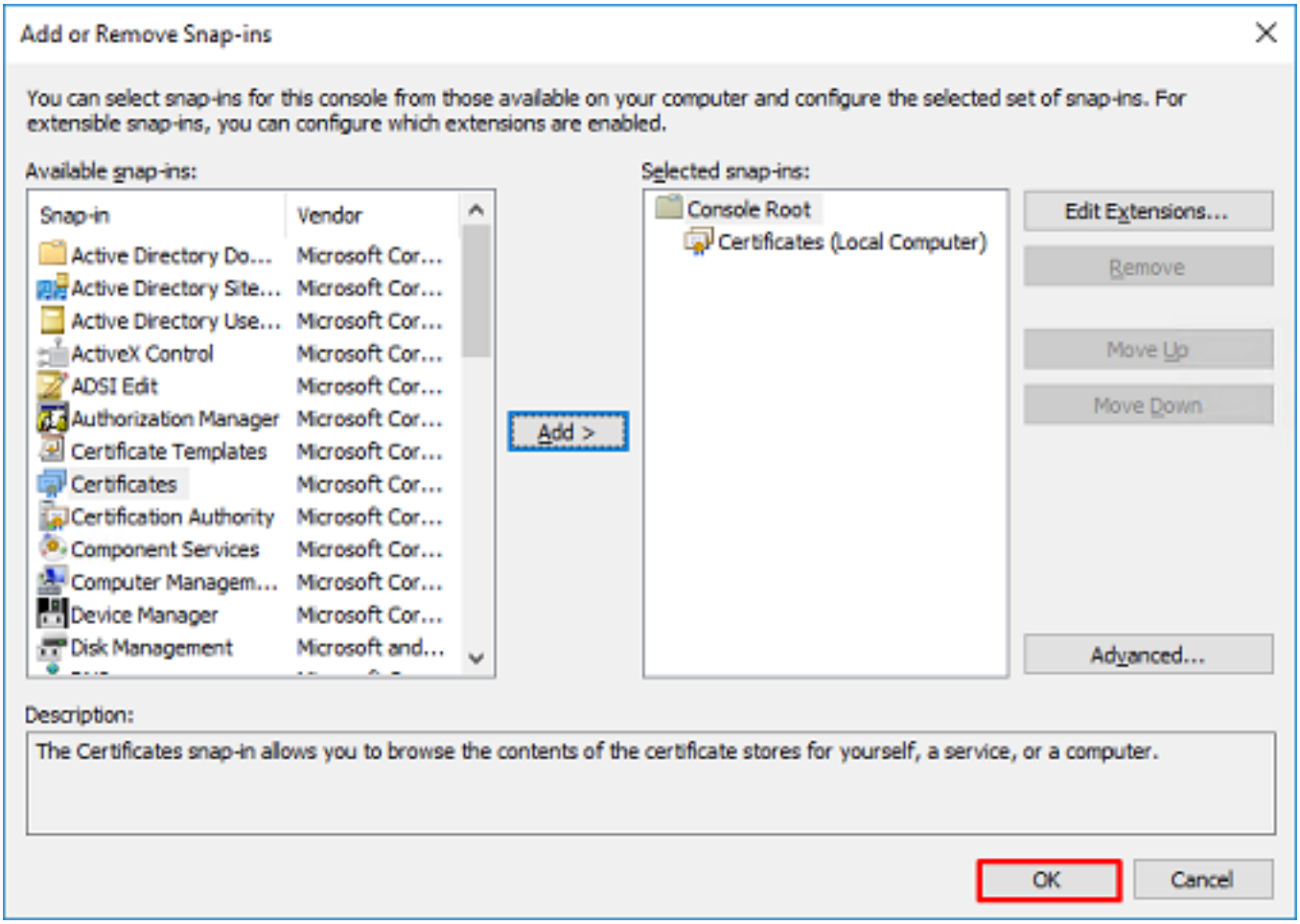
4. حدد **حساب الكمبيوتر**، ثم انقر فوق **التالي** كما هو موضح في الصورة.



انقر فوق **إنهاء**.



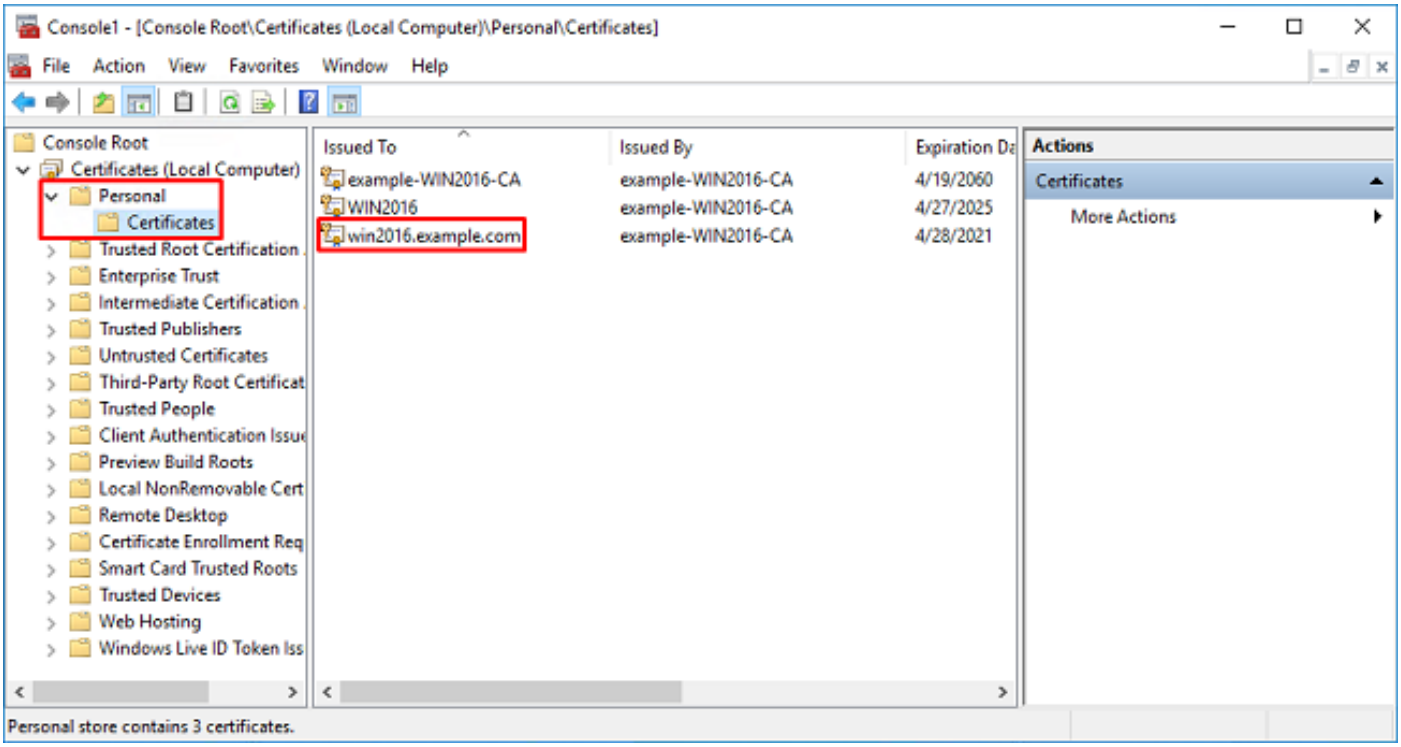
5. انقر فوق **OK**.



6. قم بتوسيع المجلد **الشخصي**، ثم انقر فوق **الشهادات**. يجب إصدار الشهادة المستخدمة من قبل LDAPs إلى اسم المجال المؤهل بالكامل (FQDN) الخاص بخادم Windows. يوجد 3 شهادات مدرجة على هذا الخادم.

- شهادة مرجع مصدق صادرة إلى والمثال WIN2016-CA.
- شهادة هوية صادرة لنظام التشغيل Win2016 بواسطة example-WIN2016-CA.
- شهادة هوية صادرة إلى win2016.example.com بواسطة example-win2016-ca.

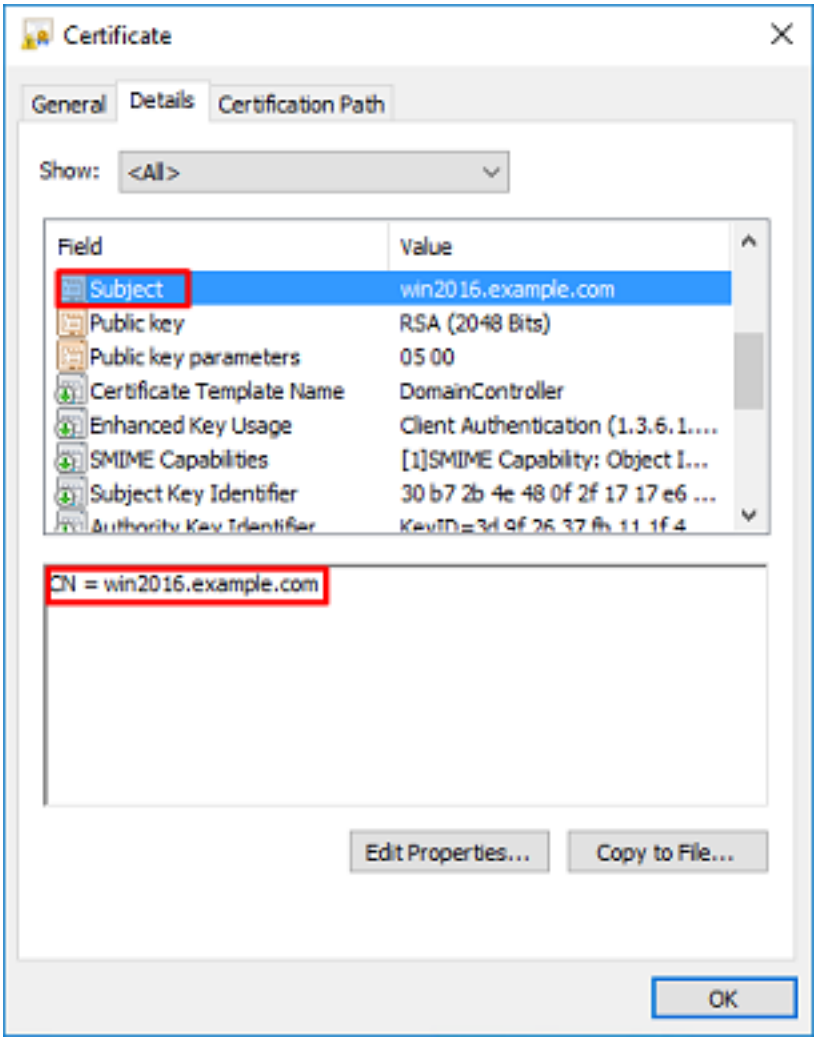
في دليل التكوين هذا، يكون FQDN هو win2016.example.com، وبالتالي فإن الشهادات الأولى والثانية غير صالحة للاستخدام كشهادة LDAP SSL. شهادة الهوية التي تم إصدارها إلى win2016.example.com هي شهادة تم إصدارها تلقائيا بواسطة خدمة المرجع المصدق لـ Windows Server. انقر نقرا مزدوجا على الشهادة للتحقق من التفاصيل.

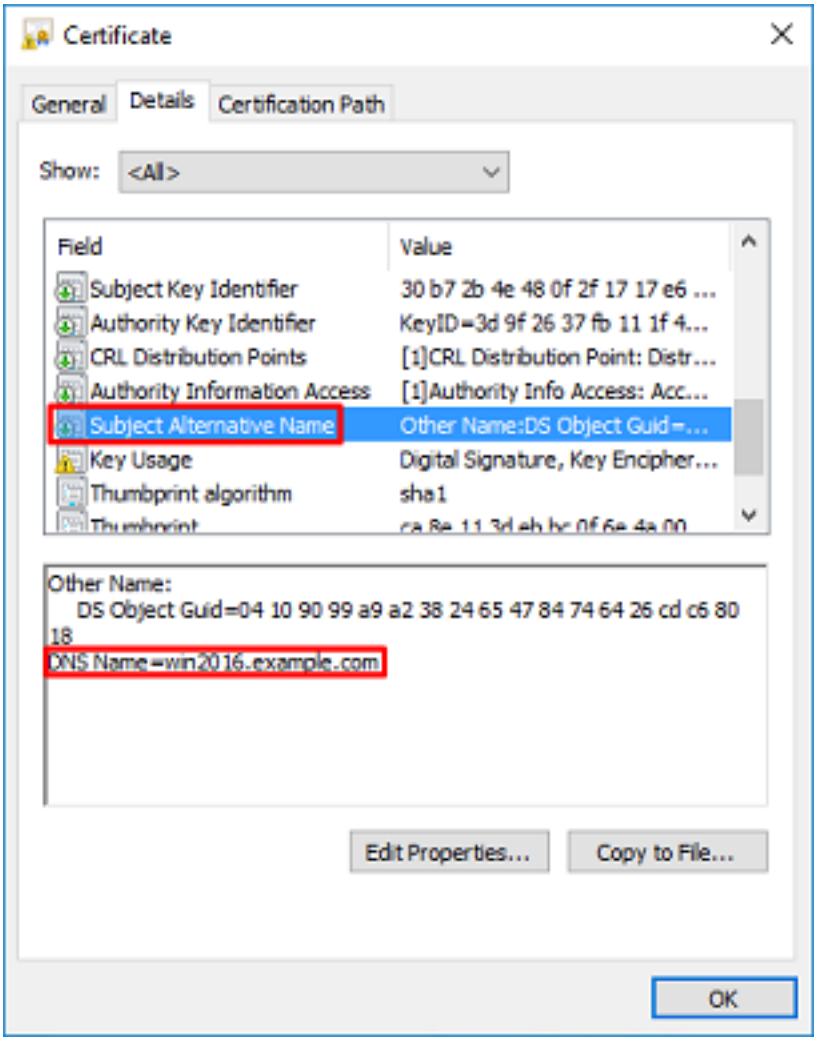


7. من أجل إستخدامها كشهادة SSL لـ LDAPS، يجب أن تستوفي الشهادة هذه المتطلبات:

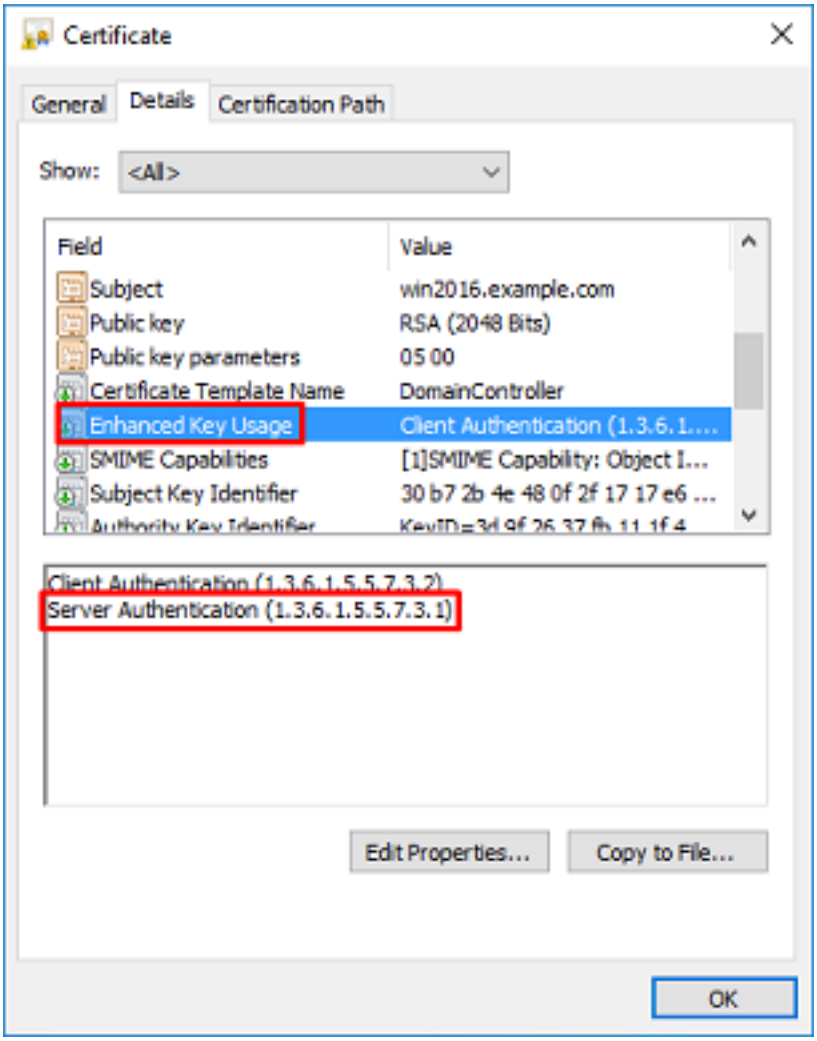
- يتطابق الاسم الشائع أو الاسم البديل لموضوع DNS مع FQDN الخاص بخادم Windows.
- تحتوي الشهادة على مصادقة الخادم ضمن حقل إستخدام المفتاح المحسن.

تحت علامة التبويب تفاصيل للشهادة، تحت اسم **الموضوع** و**الموضوع البديل**، يكون FQDN **win2016.example.com** موجودا.

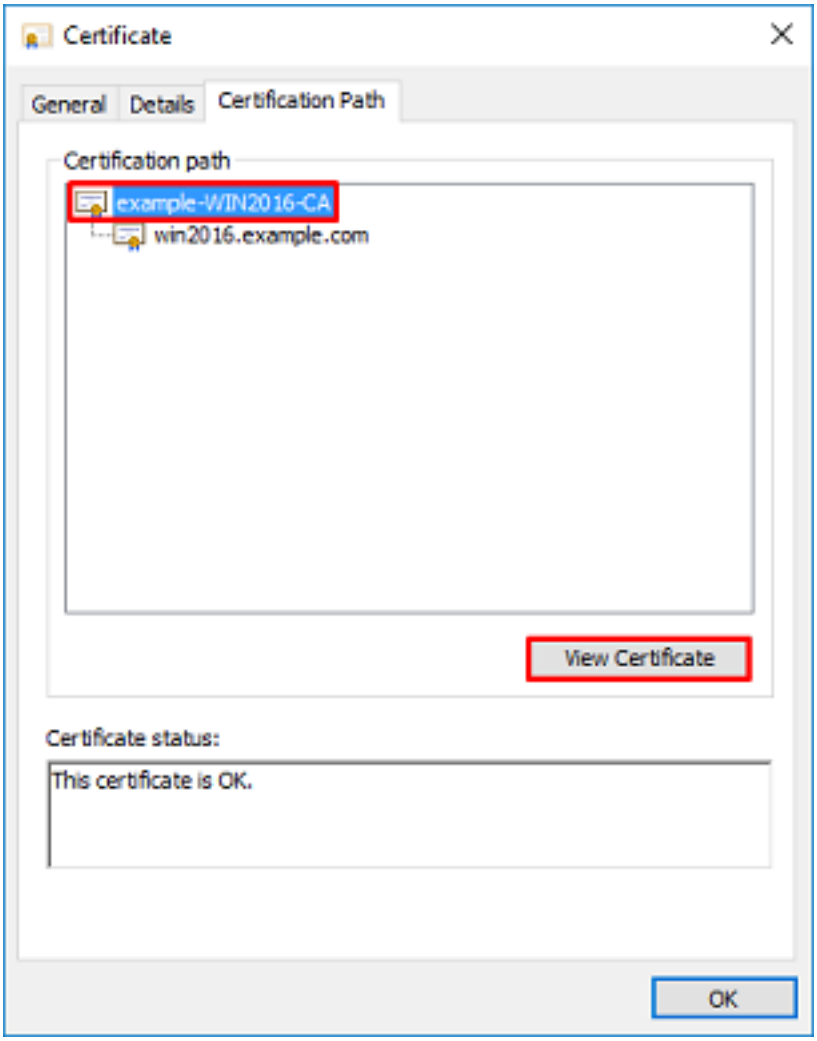

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
win2016.example.com
Public key
RSA (2048 Bits)
Public key parameters
05 00
Certificate Template Name
DomainController
Enhanced Key Usage
Client Authentication (1.3.6.1....
SMIME Capabilities
[1]SMIME Capability: Object I...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



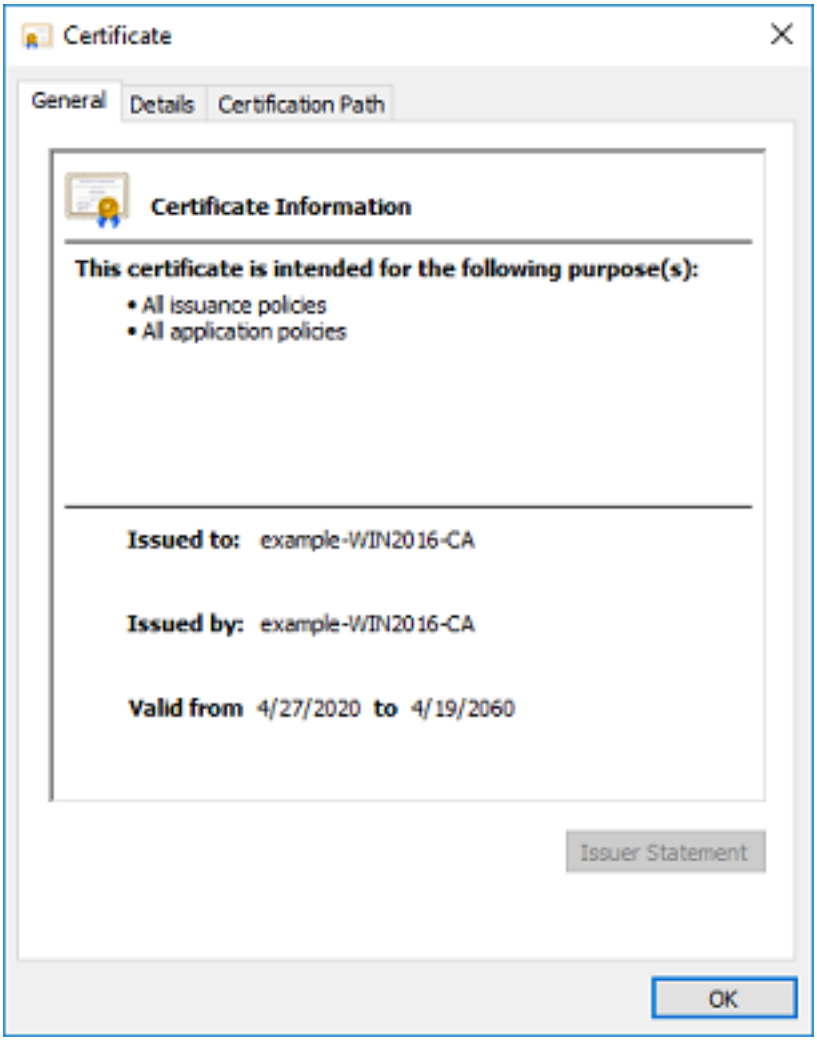
تحت الاستخدام المحسن للمفاتيح، توجد مصادقة الخادم.



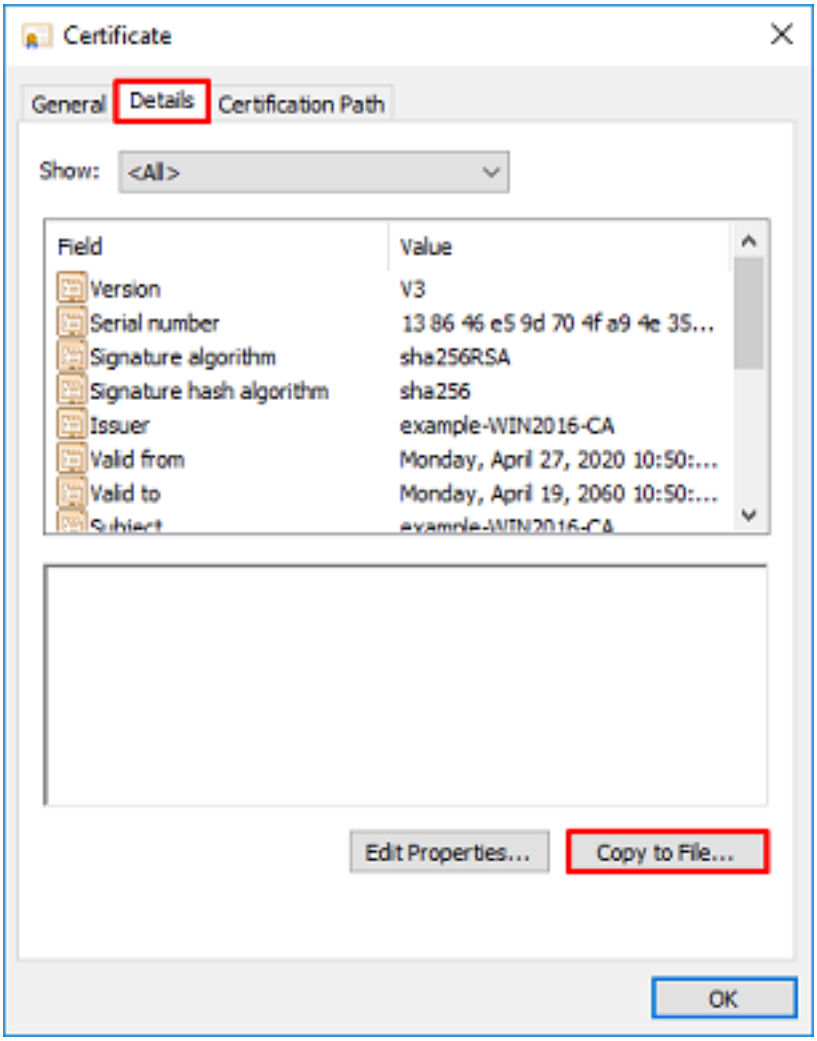
8. بمجرد التأكد من ذلك، انتقل إلى علامة التبويب **مسار الاعتماد**. انقر فوق الشهادة العليا التي يجب أن تكون شهادة المرجع المصدق الجذر، ثم انقر على زر **عرض الشهادة**.



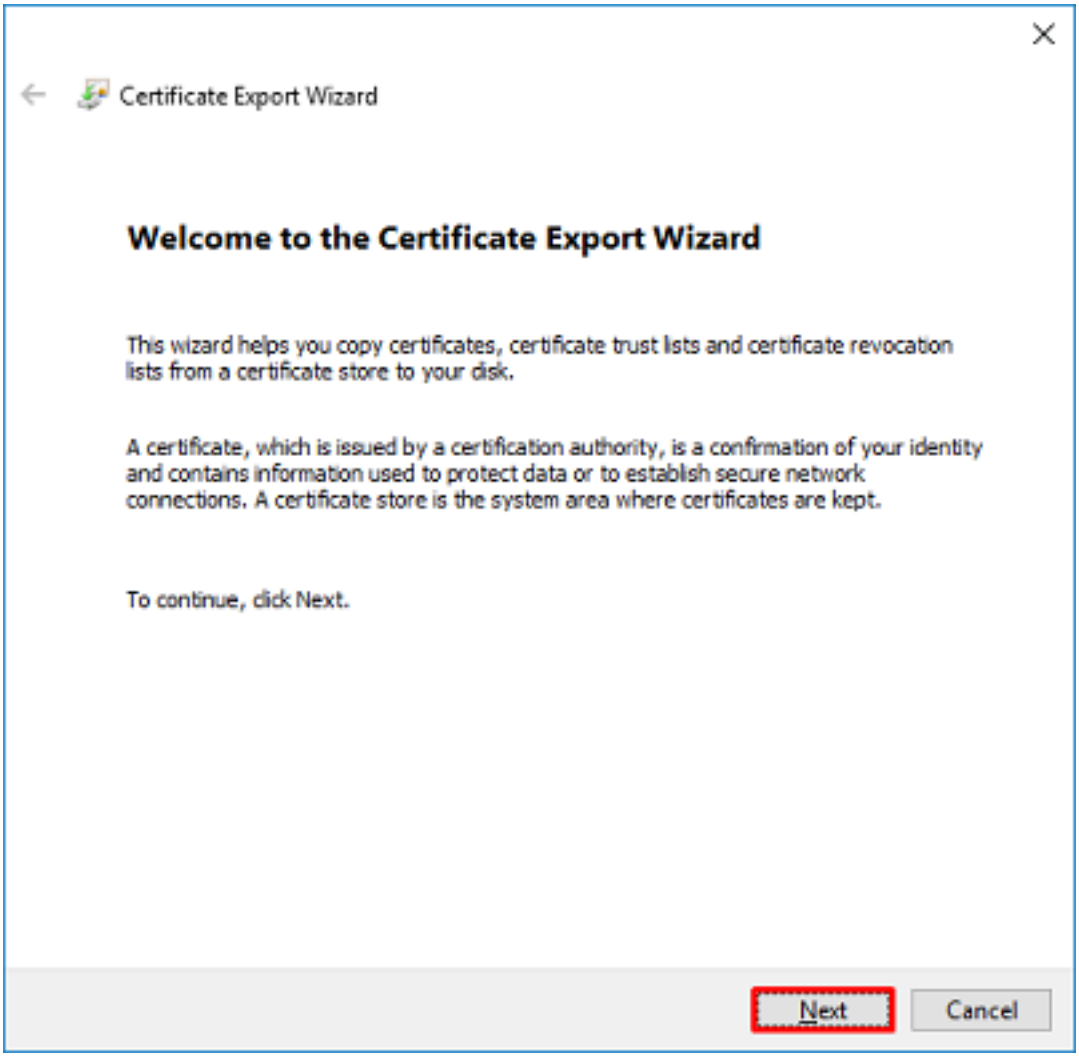
9. سيؤدي ذلك إلى فتح تفاصيل الشهادة لشهادة المرجع المصدق الجذر.



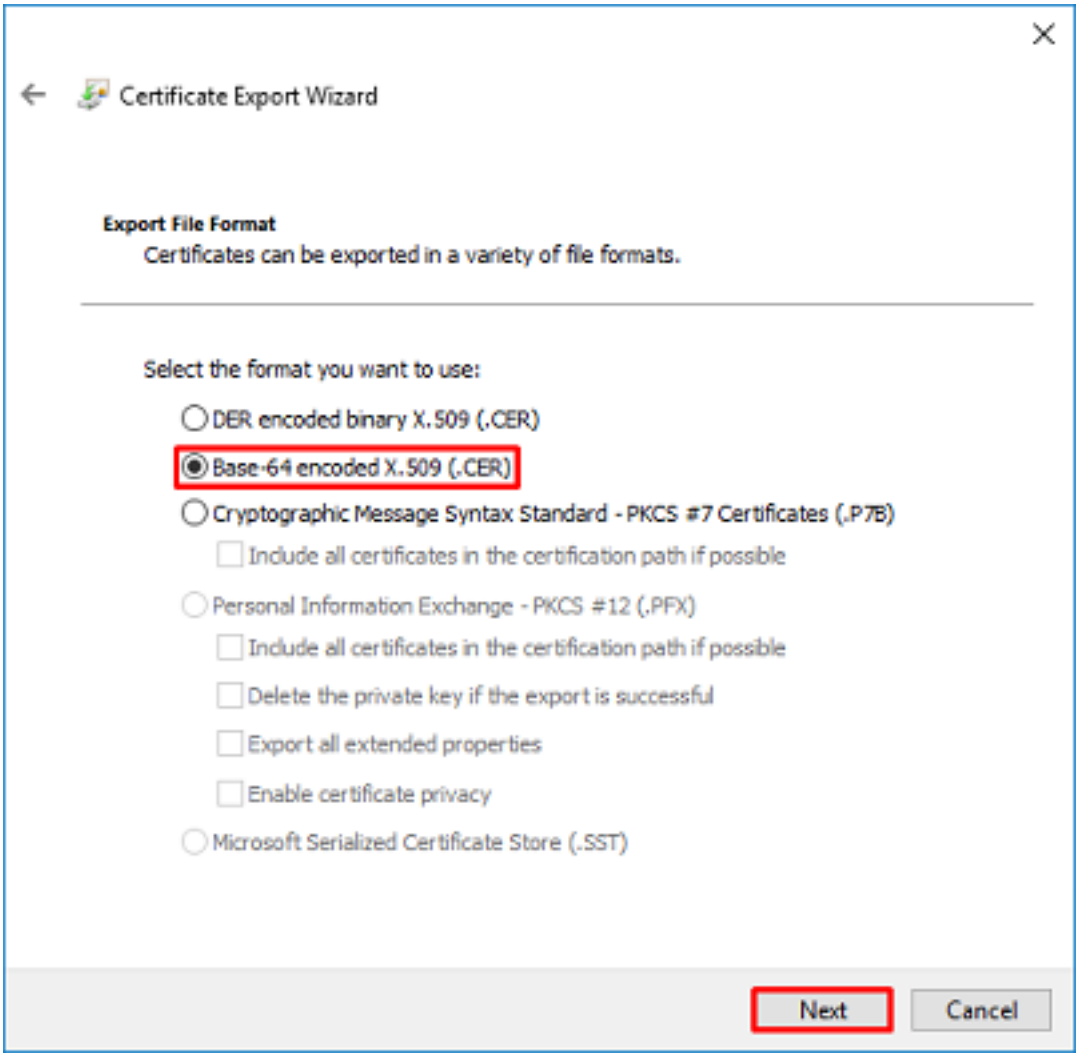
10. افتح علامة التبويب **تفاصيل** ثم انقر فوق **نسخ إلى ملف...** كما هو موضح في الصورة.



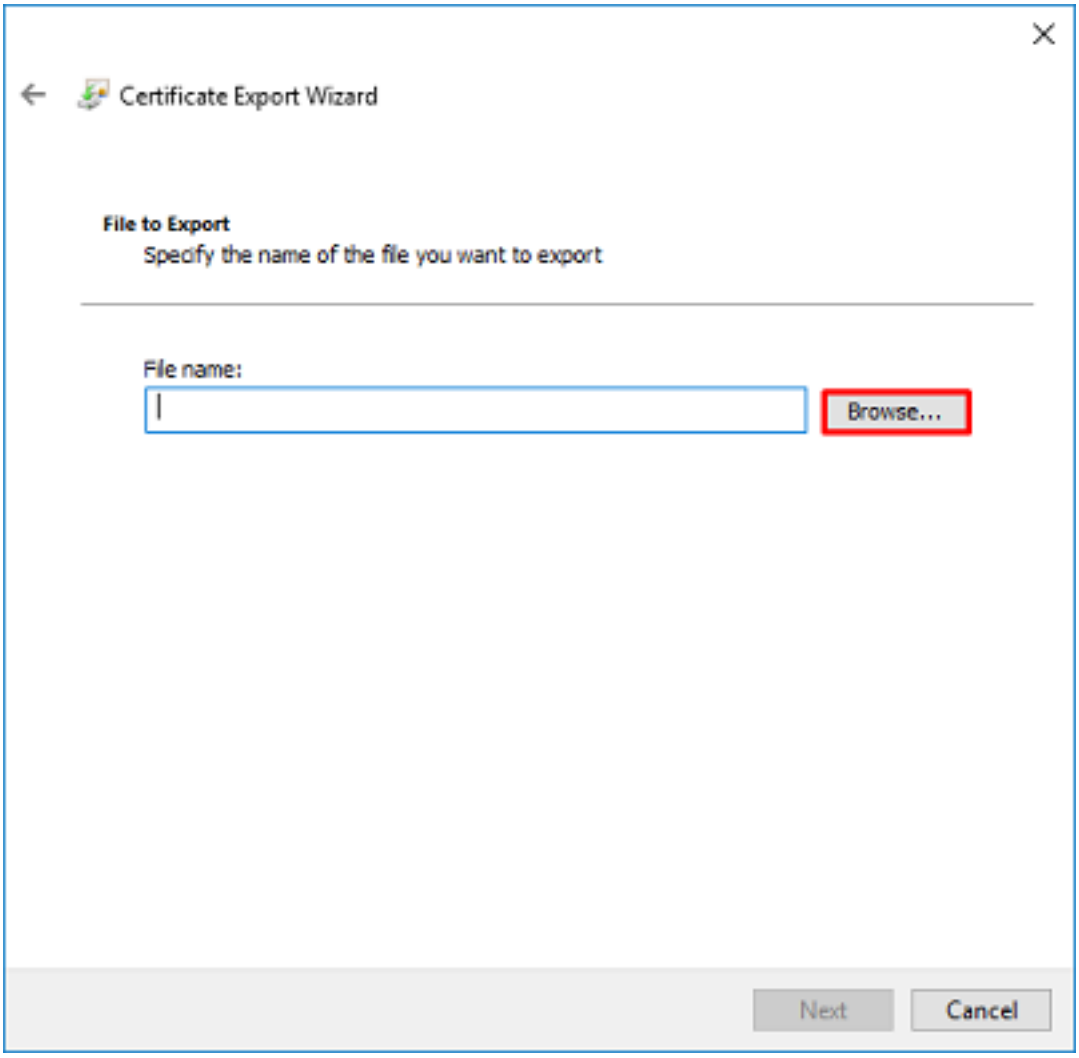
11. انتقل عبر معالج تصدير الشهادات الذي سيصدر المرجع المصدق الجذر بتنسيق PEM.

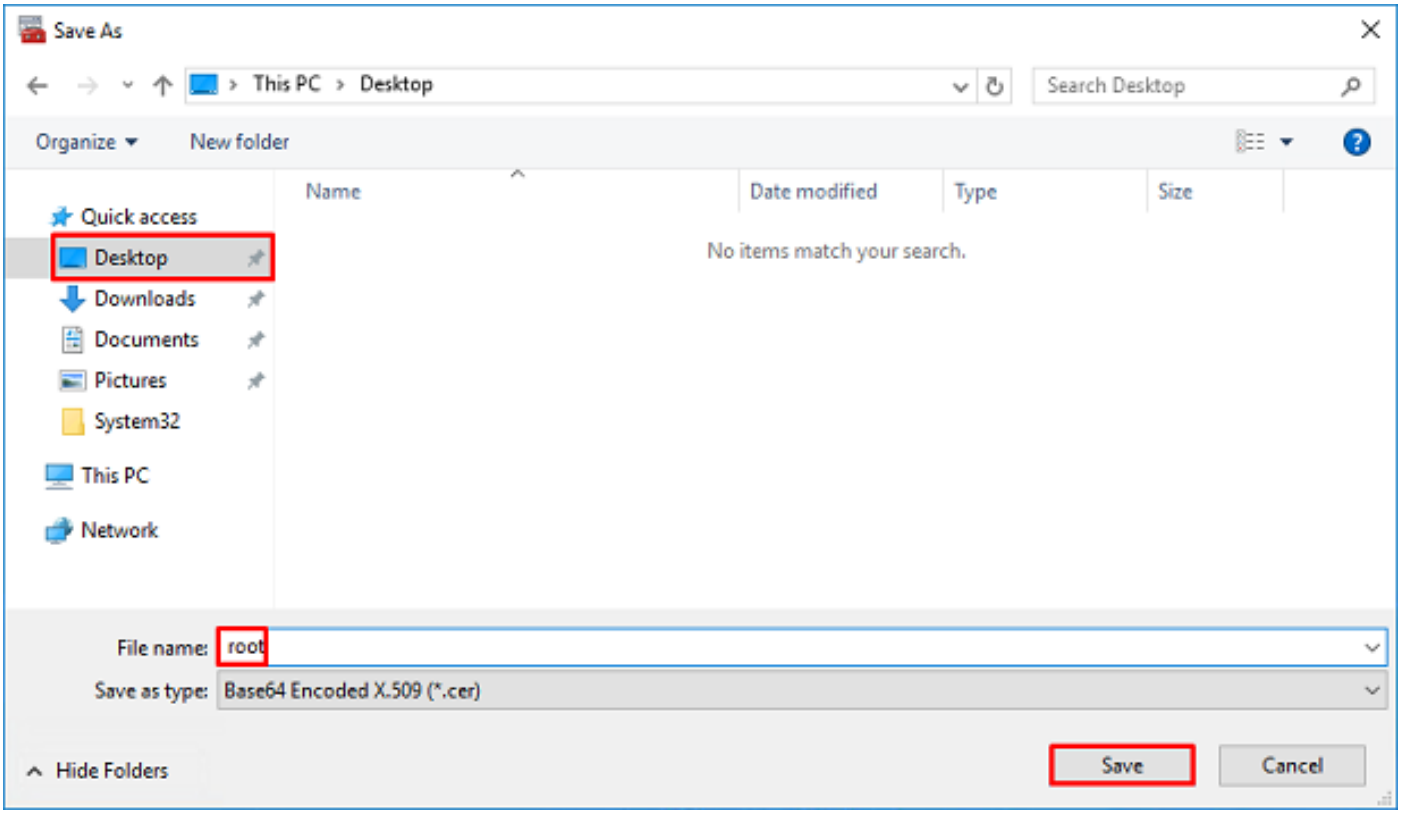


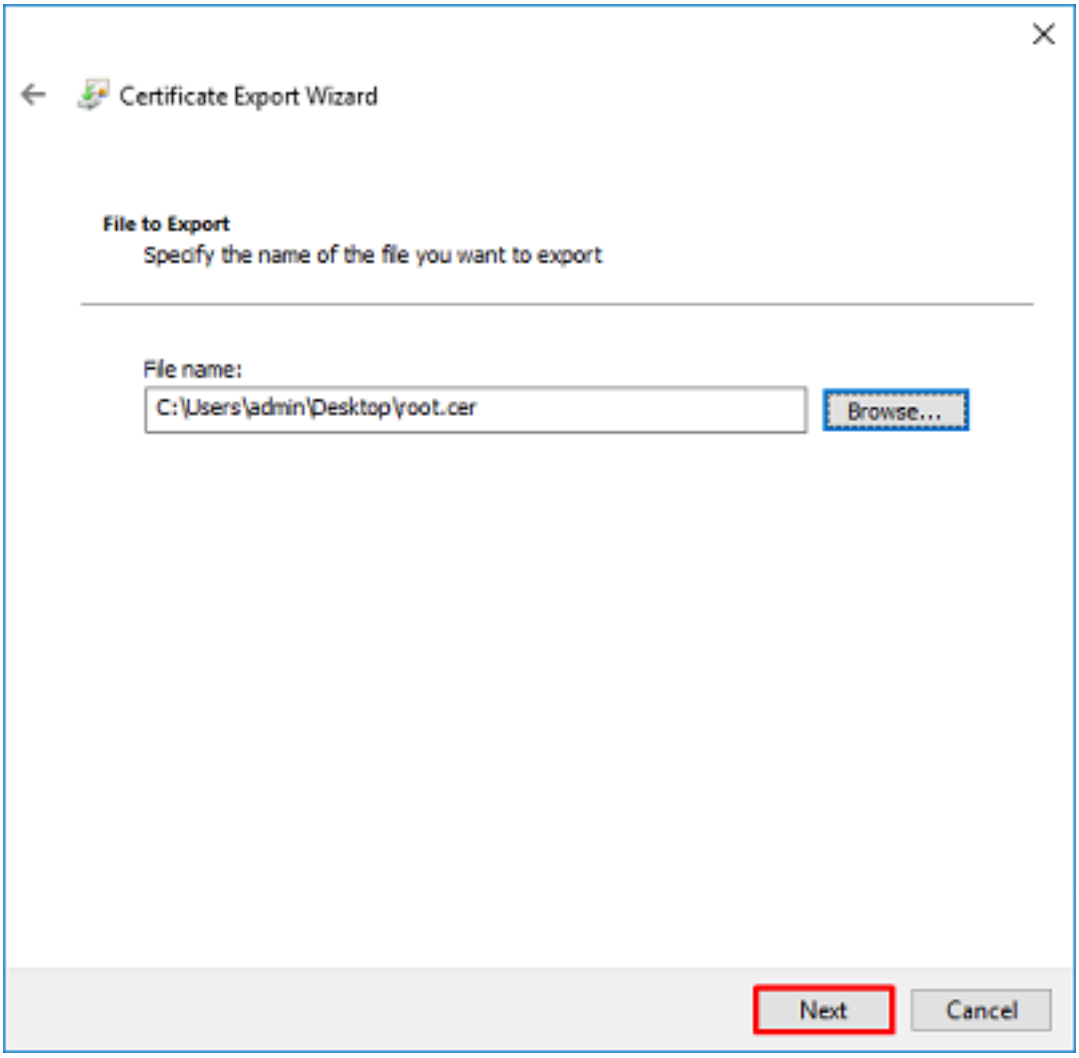
12. ددح **Base-64 المرمز X.509**.



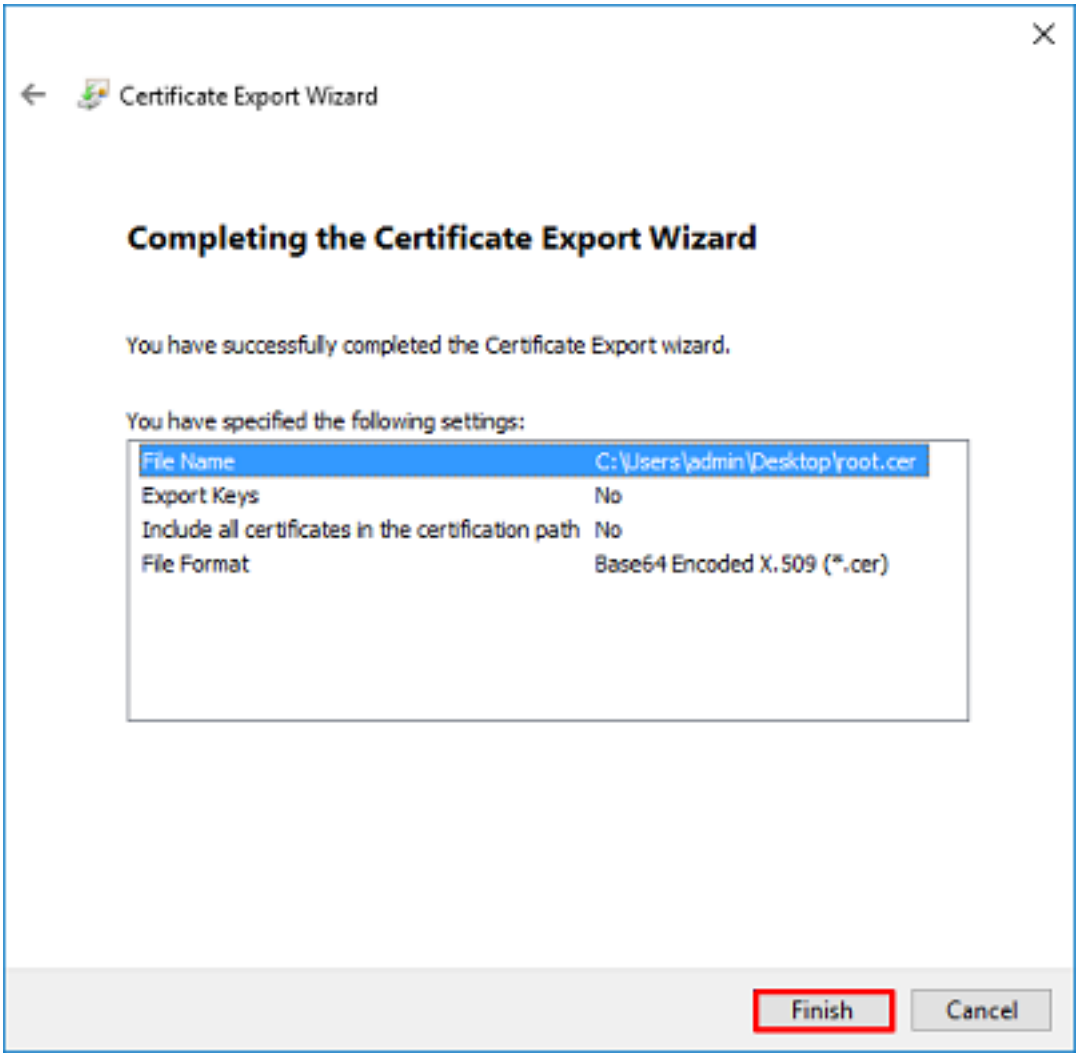
13. حدد اسم الملف وأين سيتم تصديره إليه.


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. انقر فوق **إنهاء**.



15. والآن، انتقل إلى الموقع وافتح الشهادة باستخدام مفكرة أو أي محرر نصوص آخر. سيظهر هذا شهادة بتنسيق PEM. احفظ هذا لوقت لاحق.

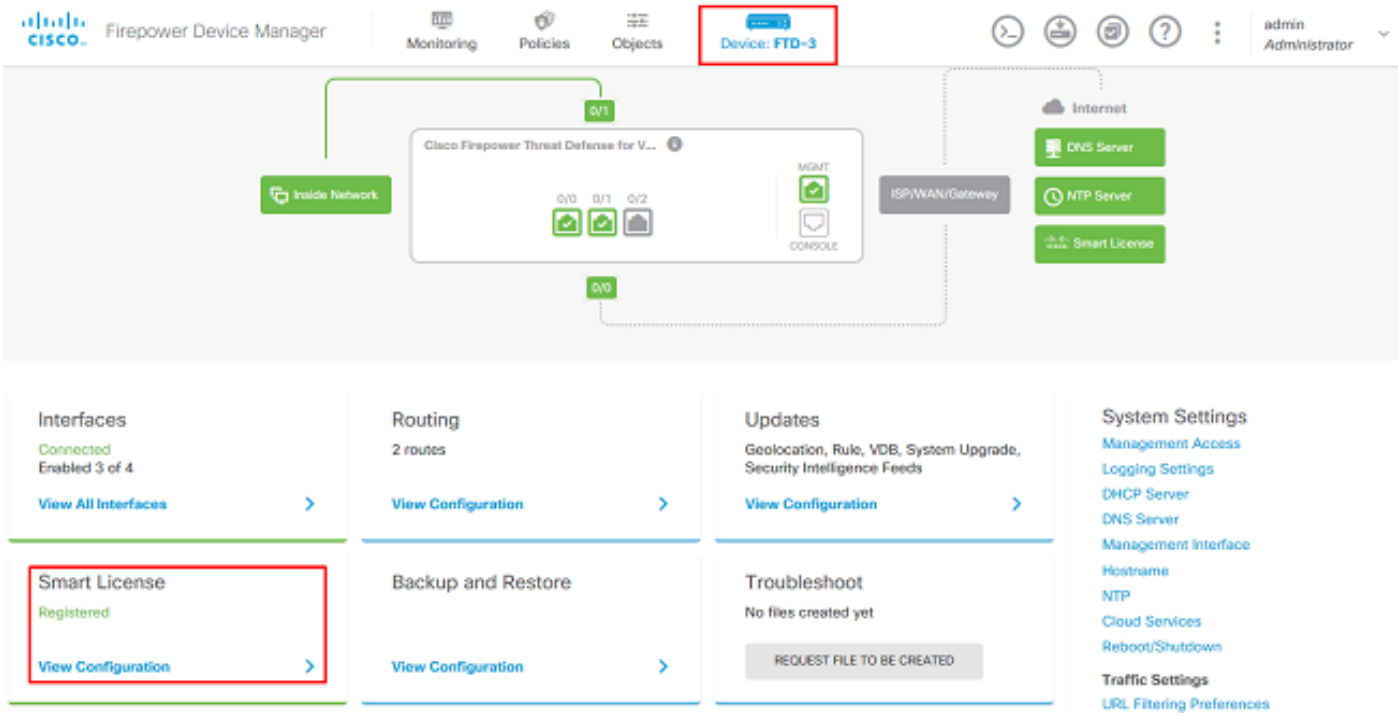
```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV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

تكوينات FDM

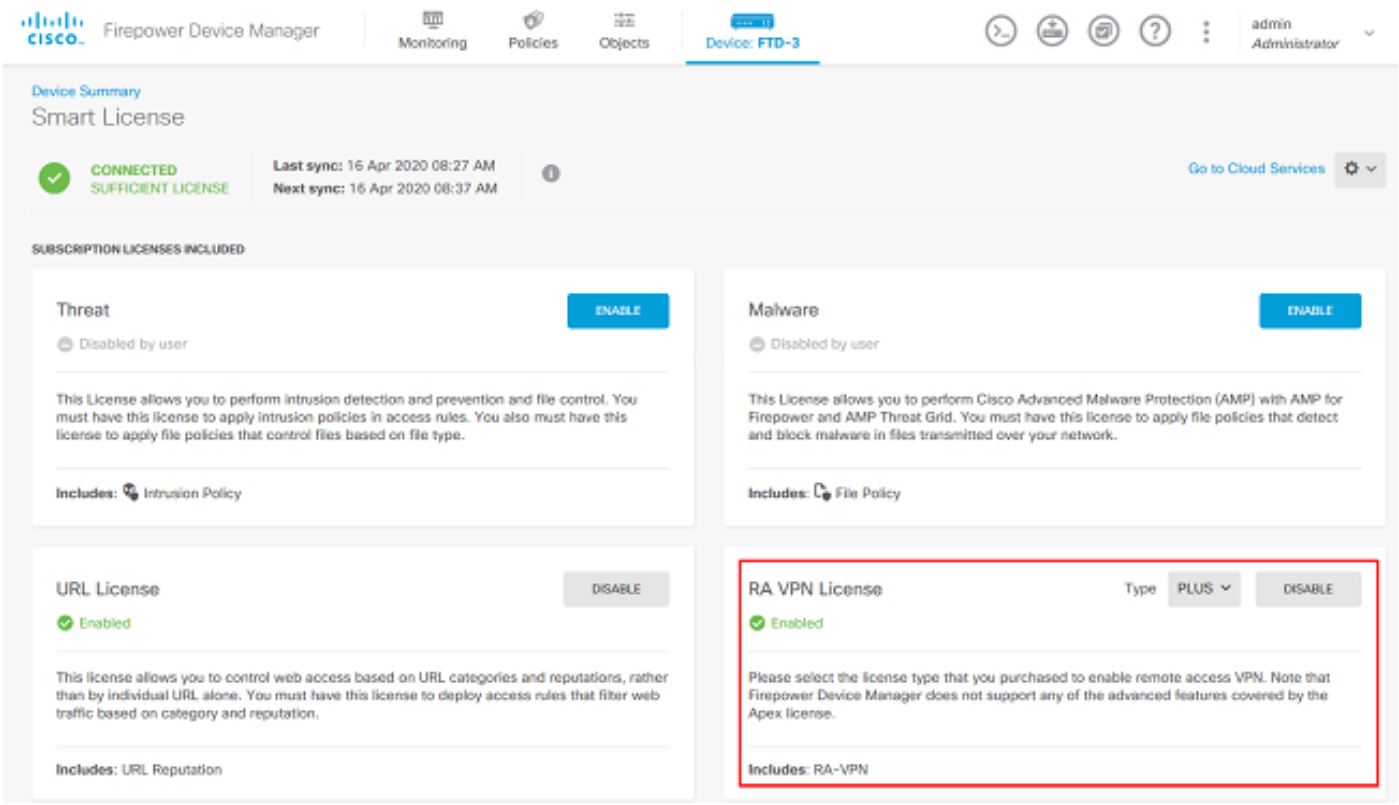
التحقق من الترخيص

لتكوين AnyConnect على FDM، سيحتاج FTD إلى التسجيل مع خادم الترخيص الذكي ويجب تطبيق ترخيص Plus أو Apex أو VPN صالح فقط على الجهاز.

1. انتقل إلى **الجهاز > الترخيص الذكي** كما هو موضح في الصورة.



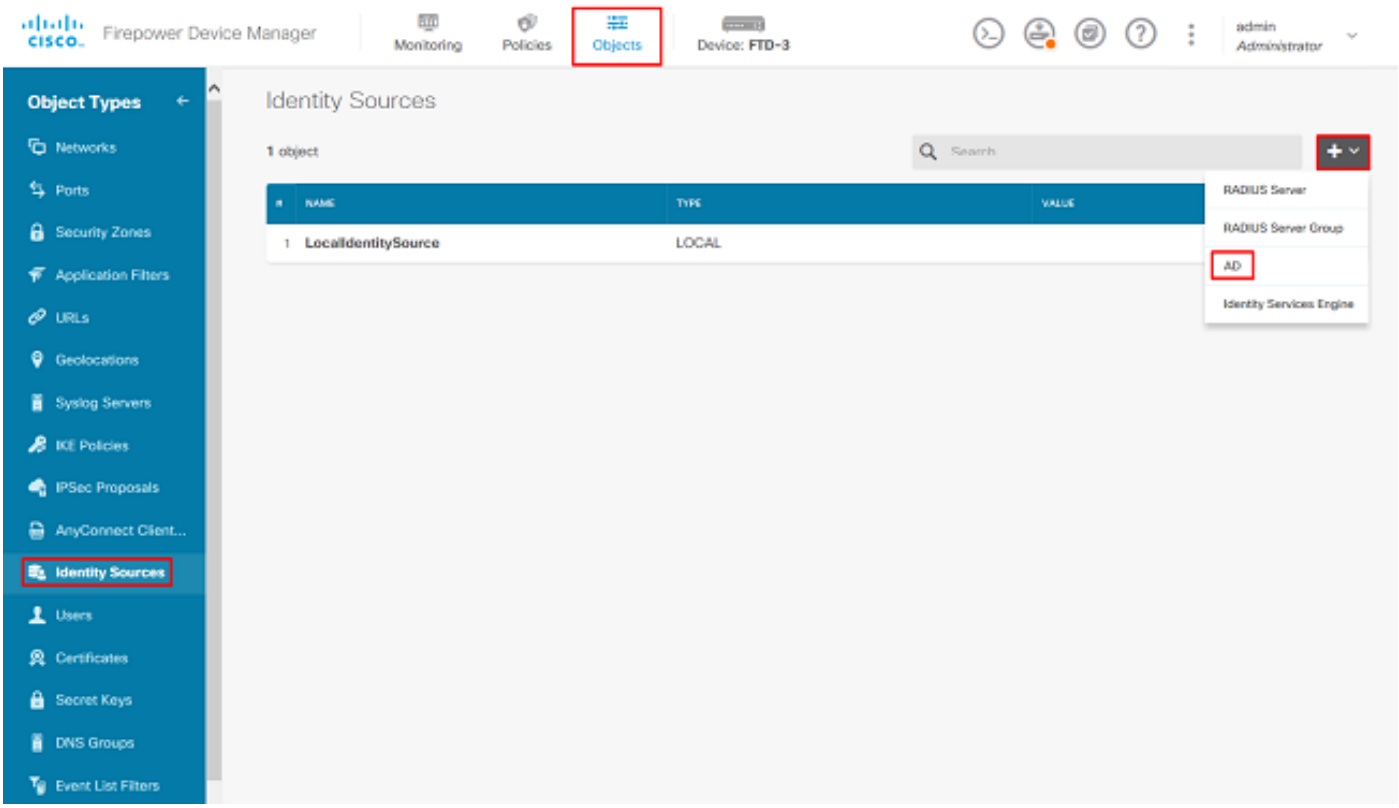
2. تحقق من تسجيل FTD لدى خادم الترخيص الذكي ومن تمكين ترخيص AnyConnect Plux أو Apex أو VPN فقط.



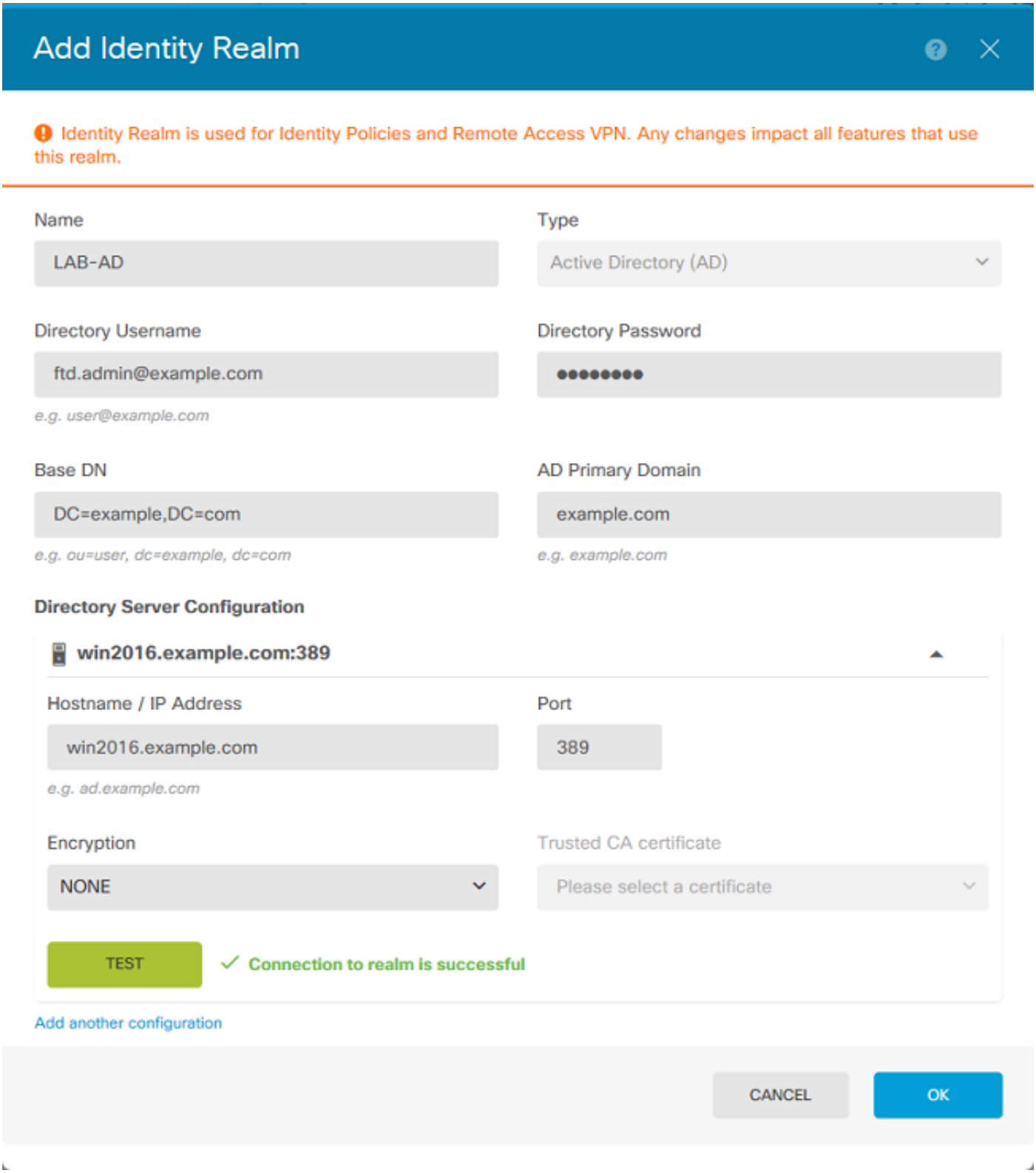
إعداد مصدر هوية الإعلانات

1. انتقل إلى **كائنات > مصادر الهوية**، ثم انقر فوق + الرمز وحدد AD كما هو موضح في

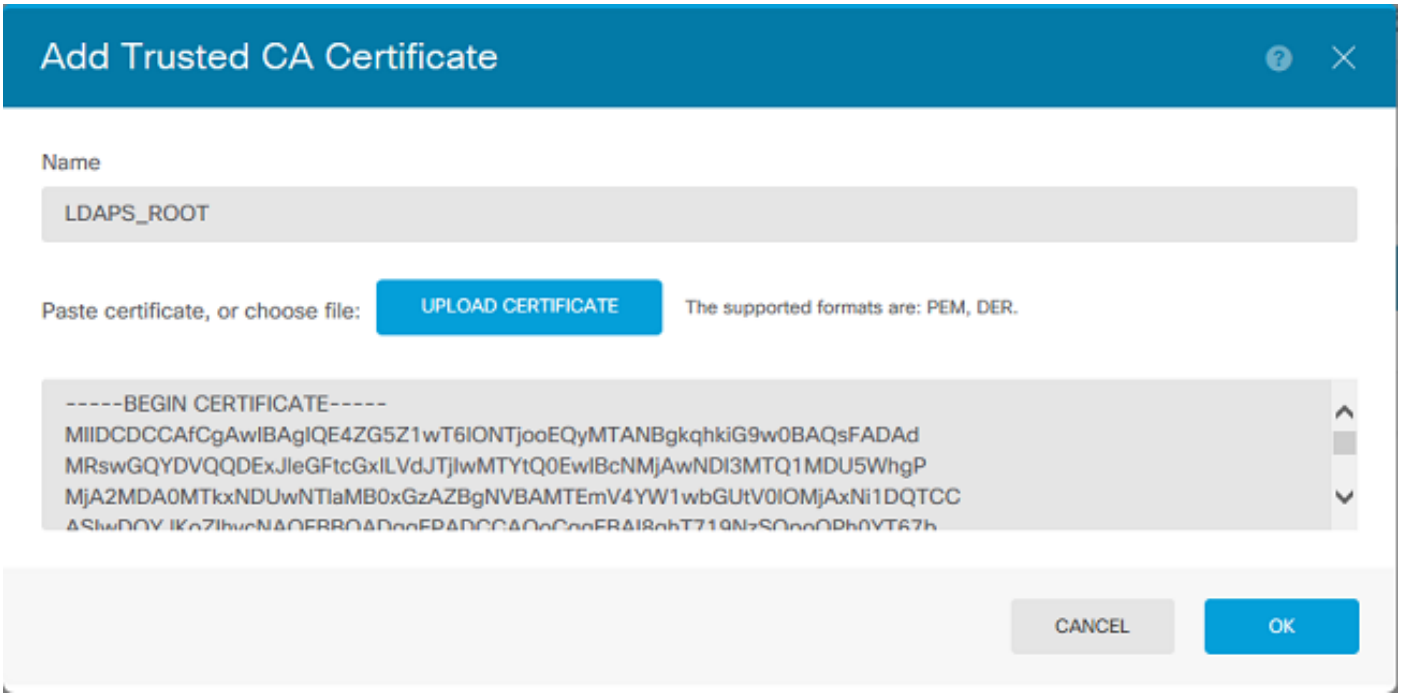
الصورة.

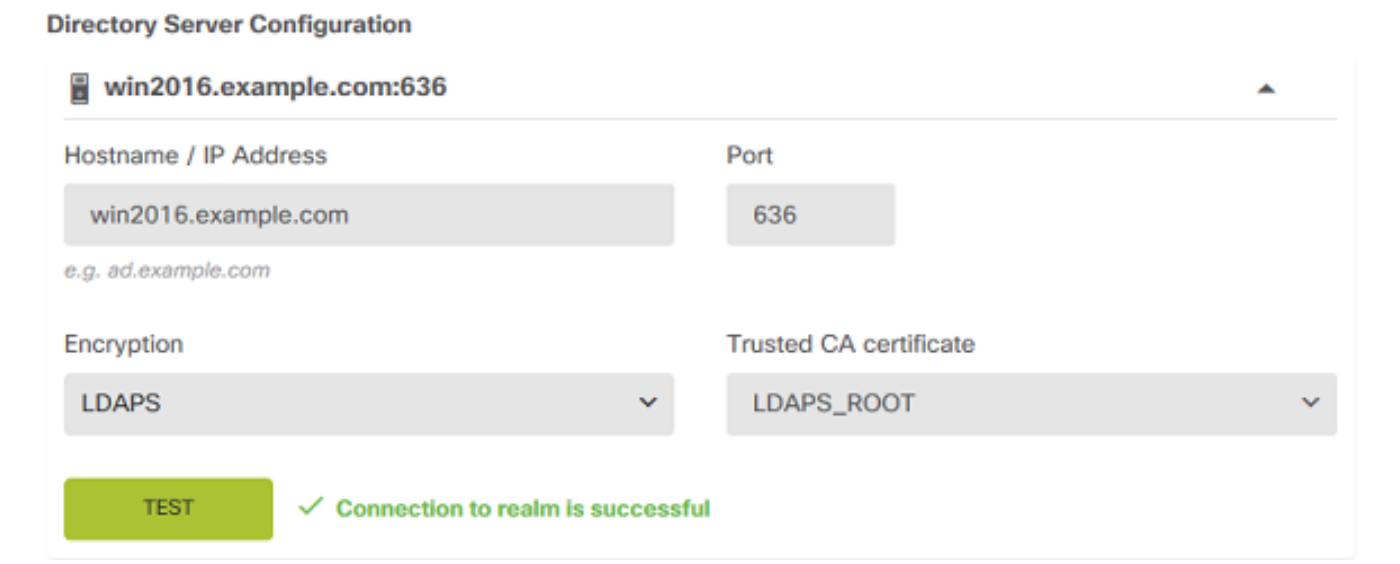


2. المألإ الإعدادات المناسبة لخادم Active Directory بالمعلومات التي تم تجميعها في وقت سابق. إذا تم إستخدام اسم المضيف (FQDN) لخادم Microsoft بدلا من عنوان IP، فتأكد من إنشاء مجموعة DNS مناسبة تحت **الكائنات > مجموعة DNS**. ثم قم بتطبيق مجموعة DNS هذه على FTD بالانتقال إلى **الجهاز > إعدادات النظام > خادم DNS**، تطبيق مجموعة DNS تحت **واجهة الإدارة وواجهة البيانات**، ثم حدد واجهة الخروج المناسبة لاستعلامات DNS. انقر فوق زر **الاختبار** للتحقق من نجاح التكوين وإمكانية الوصول من واجهة إدارة FTD. بما أن هذه الاختبارات يتم بدؤها من واجهة إدارة FTD وليس من خلال إحدى الواجهات القابلة للتوجيه التي تم تكوينها على FTD (مثل الداخل، الخارج، DMZ)، فإن الاتصال الناجح (أو الفاشل) الذي يتضمن نفس النتيجة لمصادقة AnyConnect نظرا لأنه سيتم بدء طلبات مصادقة AnyConnect LDAP من إحدى واجهات FTD القابلة للتوجيه. لمزيد من المعلومات حول إختبار إتصالات LDAP من FTD، راجع قسم Test AAA و Packet Capture في منطقة أستكشاف الأخطاء وإصلاحها.



في حالة إستخدام LDAP أو STARTTLS، حدد التشفير المناسب ثم حدد شهادة CA الموثوق بها. إذا لم تتم إضافة المرجع المصدق الجذر بالفعل، انقر على **إنشاء شهادة مرجع مصدق ثقة جديدة**. قم بتوفير اسم لشهادة المرجع المصدق الجذر ثم الصق شهادة المرجع المصدق الجذر بتنسيق PEM التي تم تجميعها سابقا.

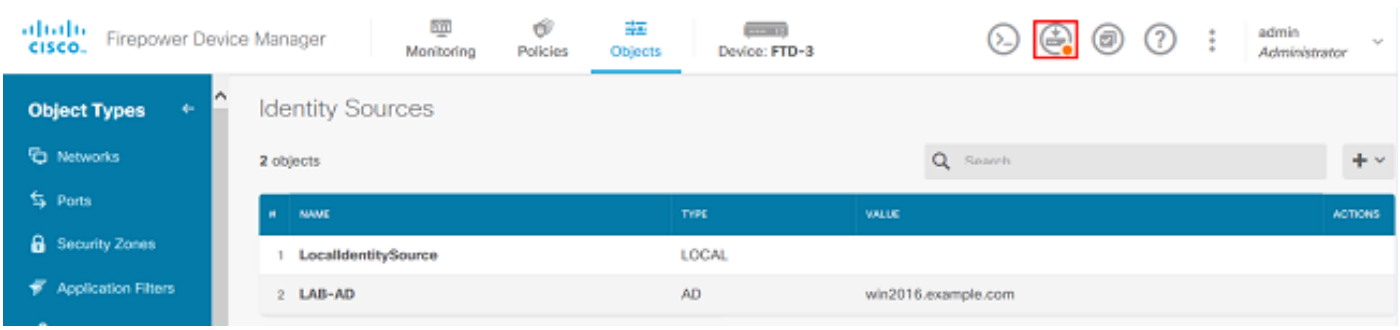




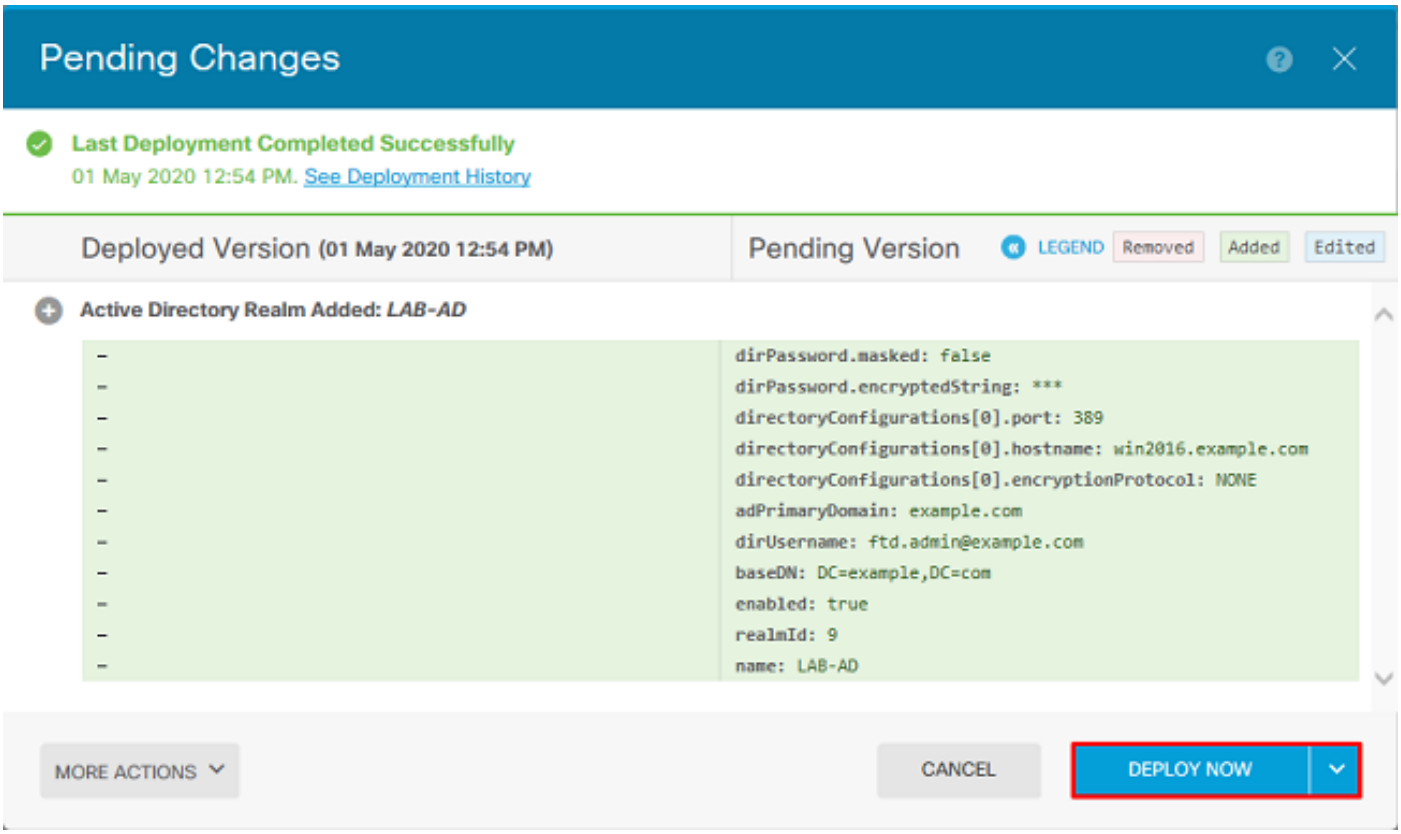
في هذا التكوين، تم إستخدام هذه القيم:

- الاسم: Lab-ad
- اسم مستخدم الدليل: ftd.admin@example.com
- شبكة DN الأساسية: DC=example،DC=com
- المجال الأساسي الخاص بالإعلان: example.com
- اسم المضيف/عنوان IP: win2016.example.com
- المنفذ: 389

3. انقر زر **التغييرات المعلقة** في أعلى اليمين كما هو موضح في الصورة.



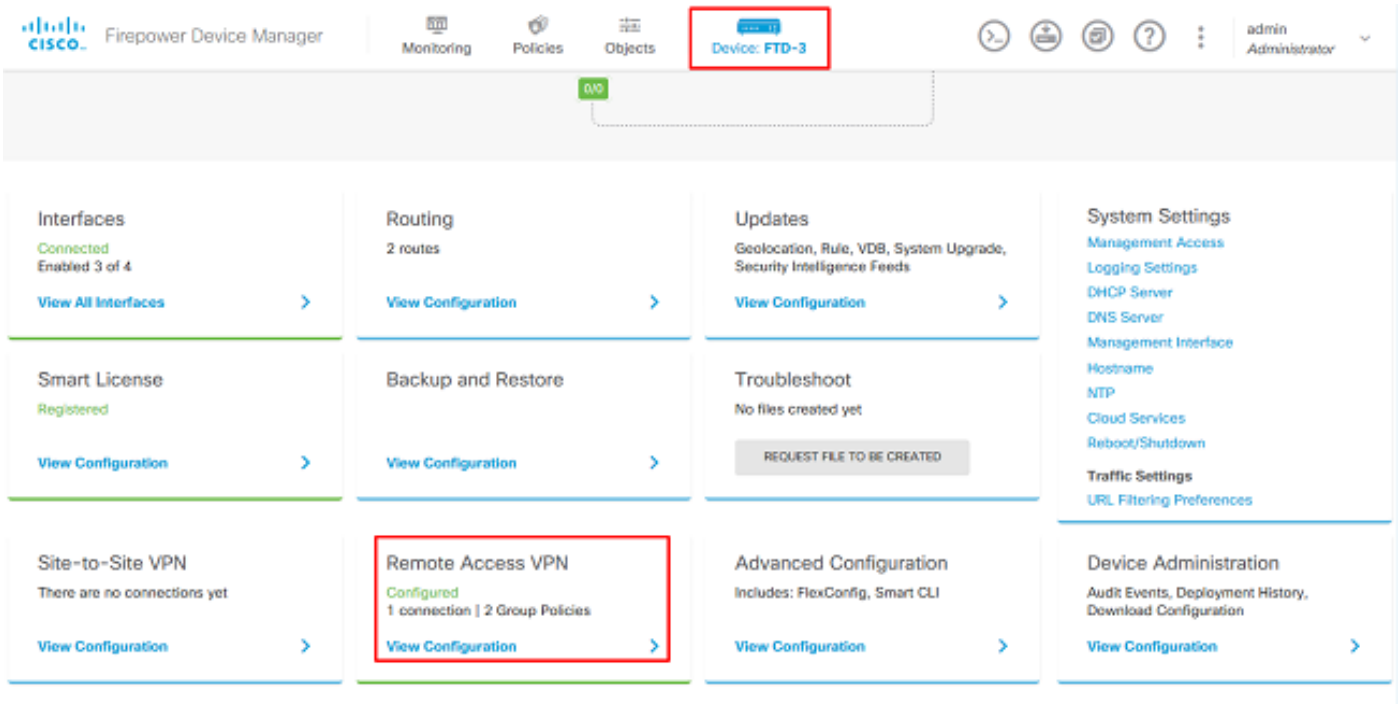
4. انقر فوق الزر **نشر الآن**.



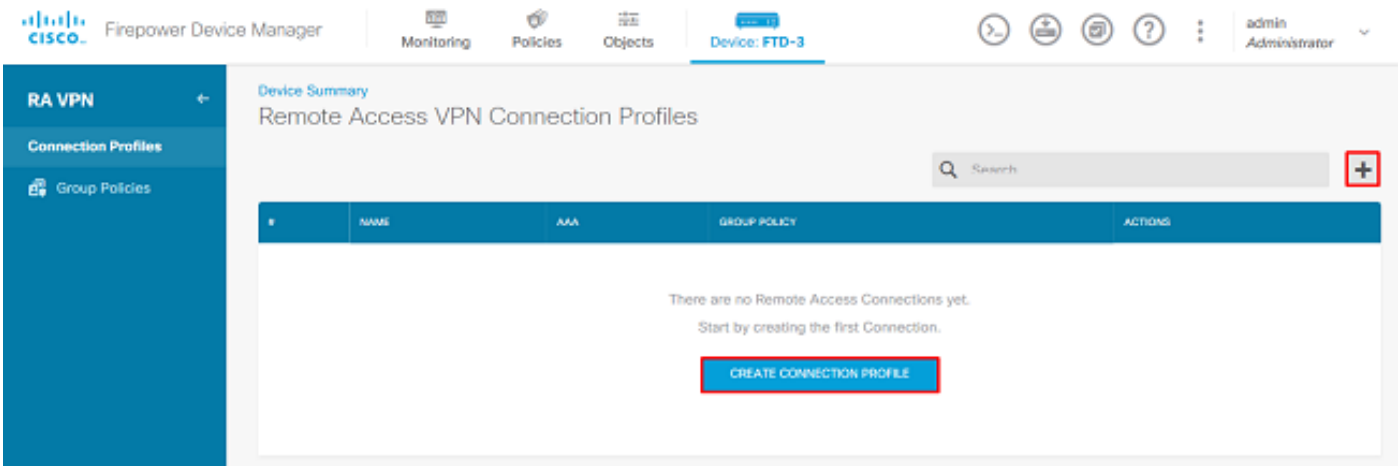
تكوين AnyConnect لمصادقة AD

لاستخدام مصدر هوية AD الذي تم تكوينه، يجب تطبيقه على تكوين AnyConnect.

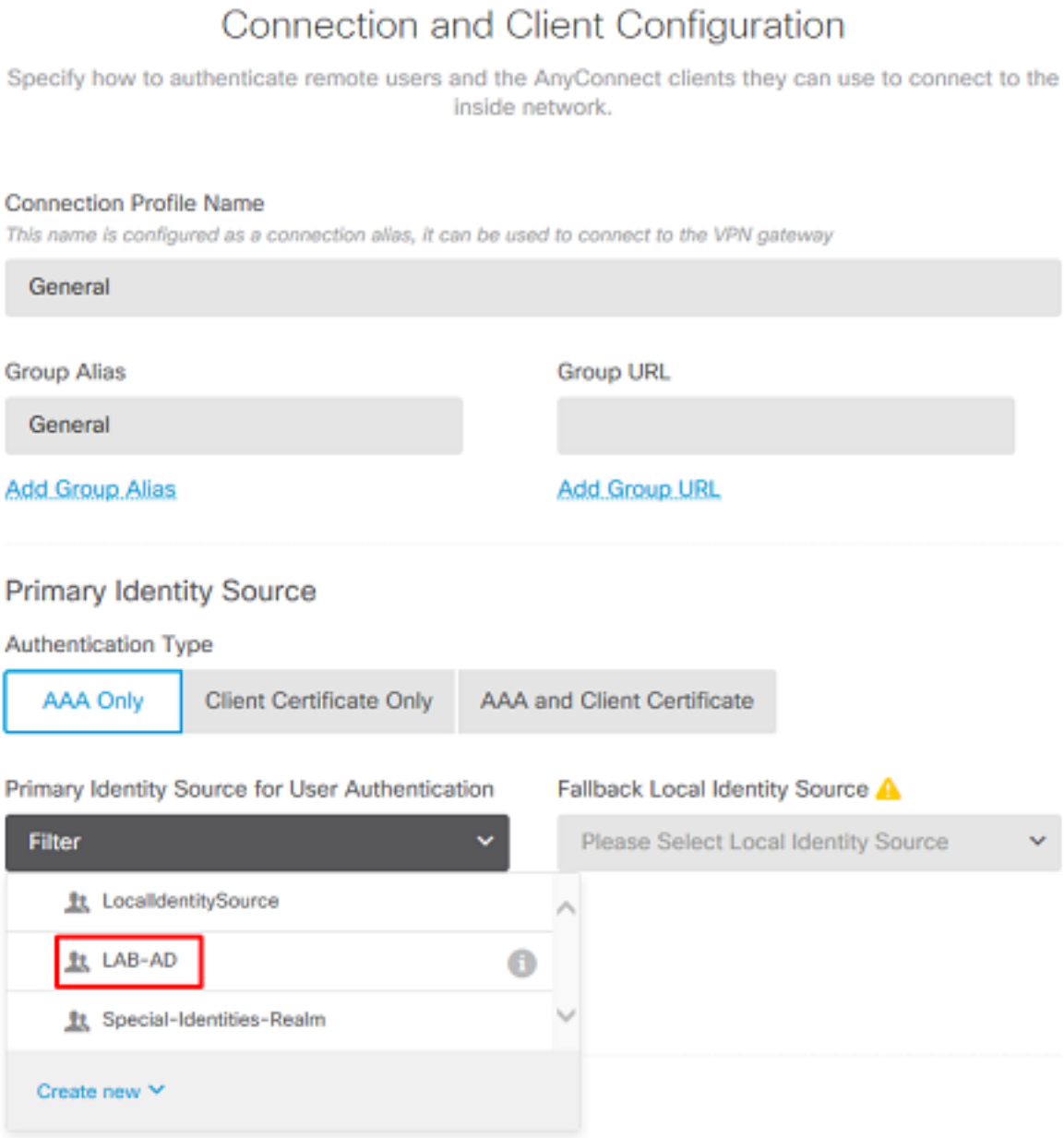
1. انتقل إلى **جهاز > Remote Access VPN** كما هو موضح في الصورة.

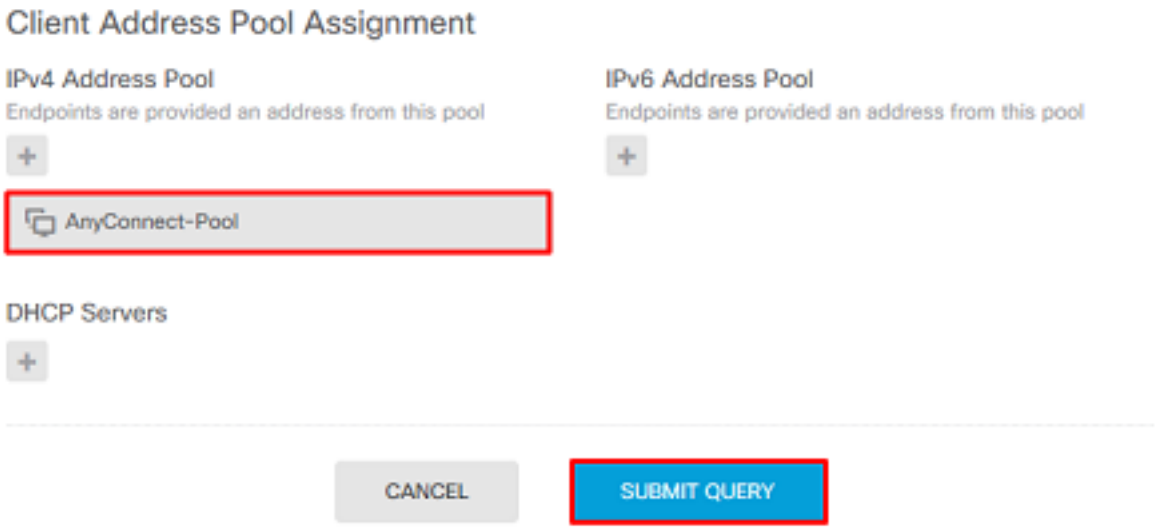


2. انقر زر + أو **إنشاء ملف تعريف اتصال** كما هو موضح في الصورة.

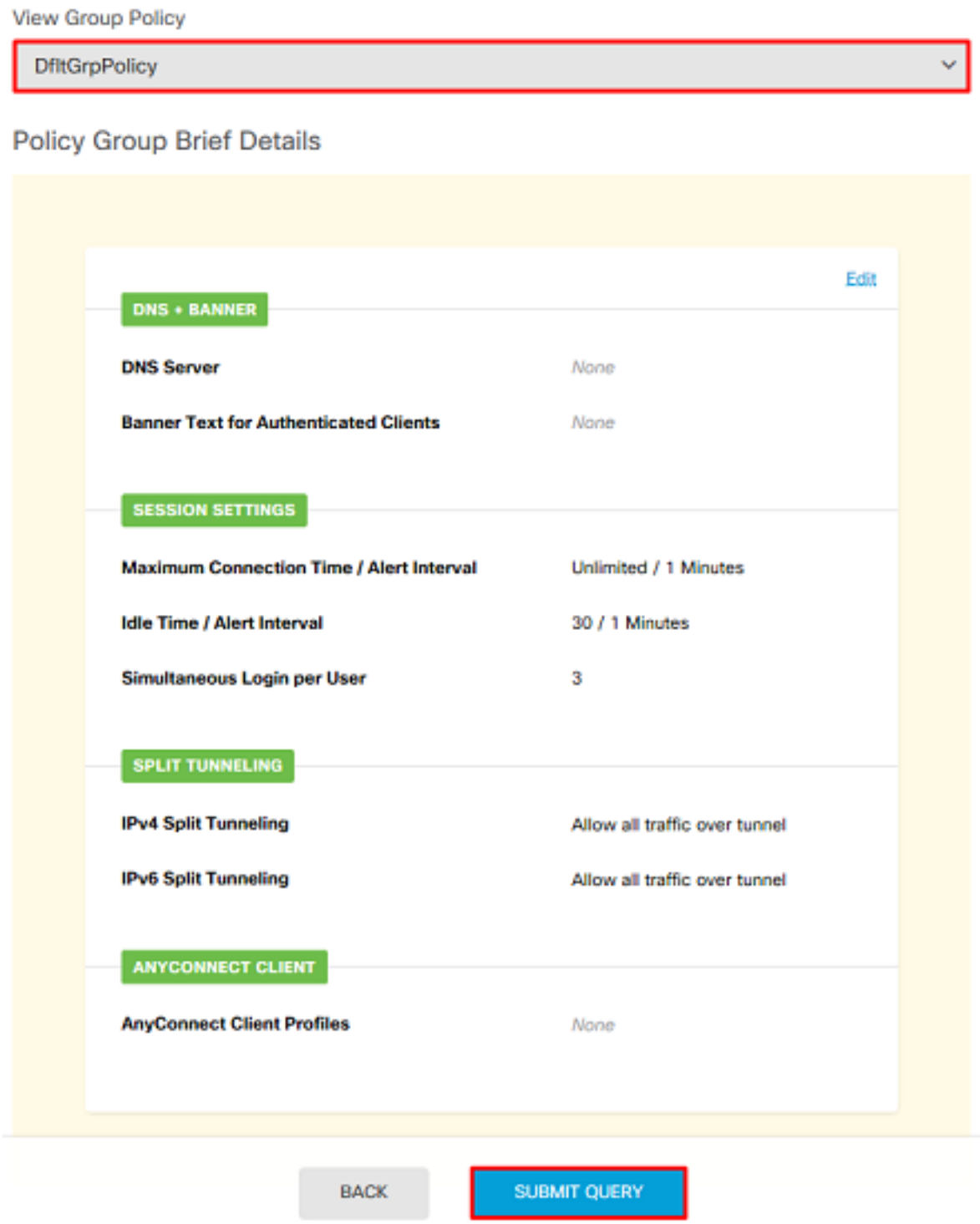


3. تحت قسم "الاتصال وتكوين العميل"، حدد مصدر هوية AD الذي تم إنشاؤه مسبقا. قم بإعداد القيم المناسبة للأقسام الأخرى بما في ذلك اسم ملف تعريف الاتصال وتعيين تجمع عناوين العملاء. انقر فوق **إرسال الاستعلام** عند الانتهاء.

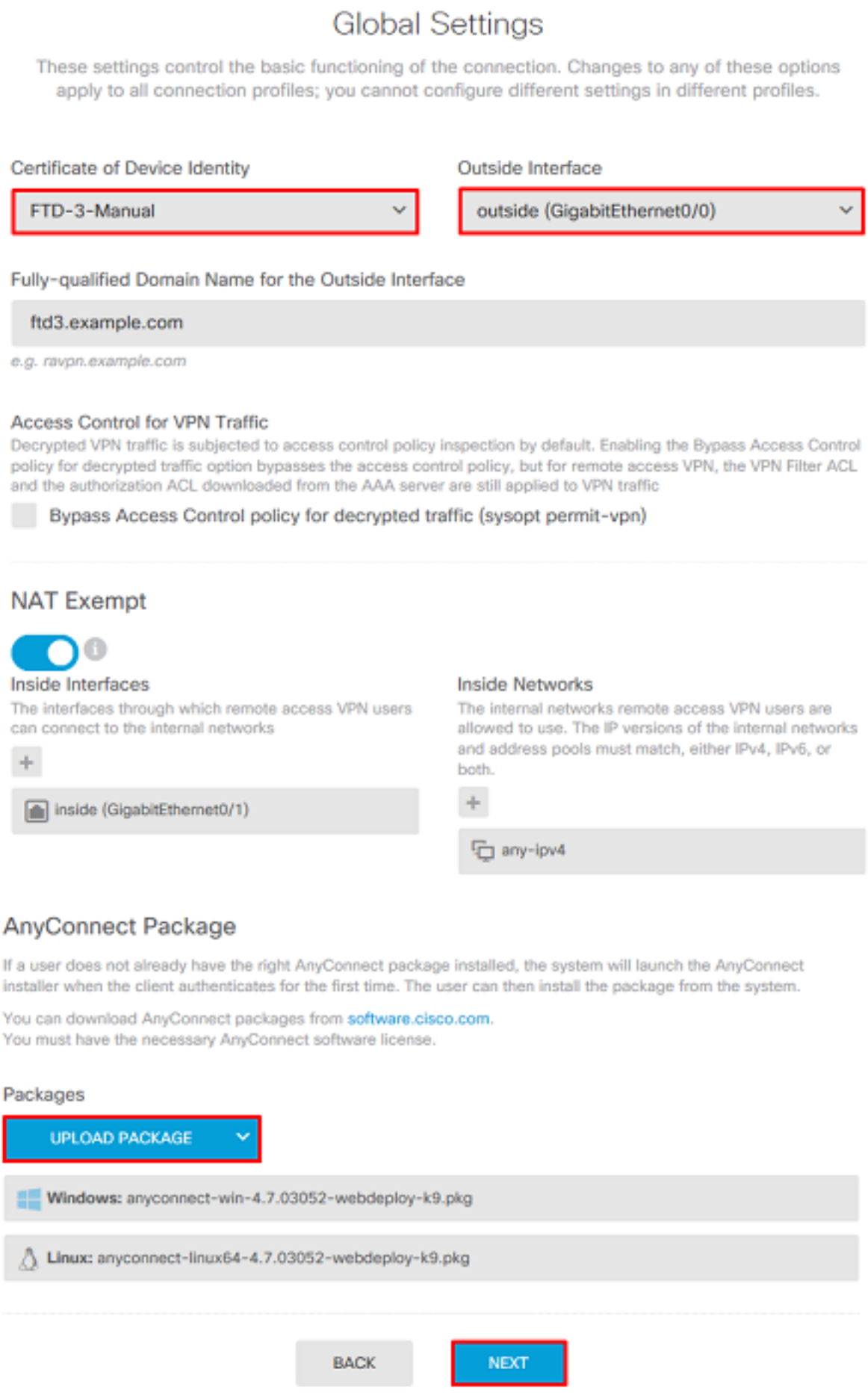




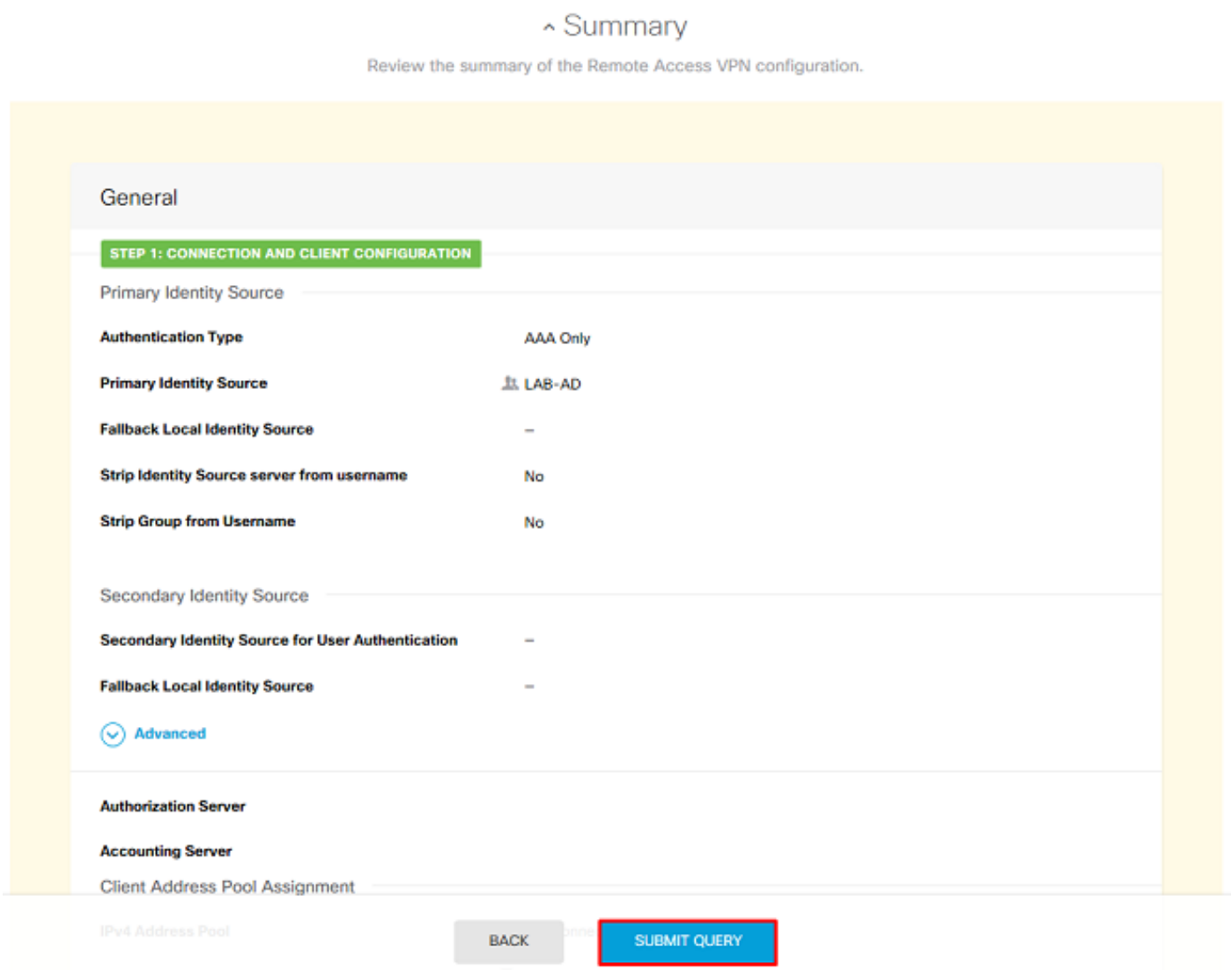
4. تحت قسم تجربة المستخدم عن بعد، حدد نهج المجموعة المناسب. بشكل افتراضي، سيتم إستخدام **DfltGrpPolicy**، ومع ذلك، يمكن إنشاء سياسة مختلفة.



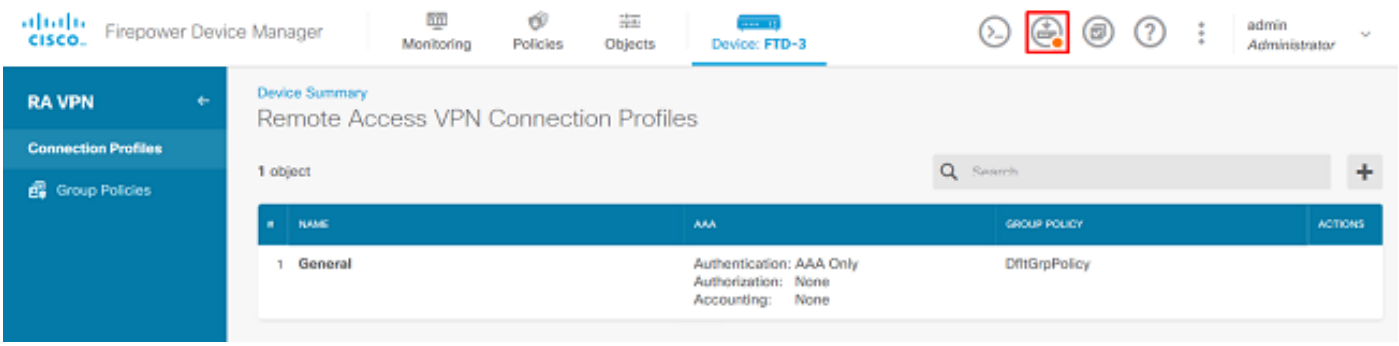
5. ضمن قسم الإعدادات العامة، على الأقل، حدد شهادة SSL، والواجهة الخارجية، وحزم AnyConnect. إذا لم يتم إنشاء شهادة سابقا، يمكن تحديد شهادة موقعة ذاتيا افتراضية (DefaultInternalCertificate) على أي حال ستظهر رسالة شهادة خادم غير موثوق بها. يجب إلغاء تحديد سياسة التحكم بالوصول الالتفافي لحركة المرور التي تم فك تشفيرها (sysopt allowed-vpn) بحيث تخضع لقواعد نهج الوصول إلى هوية المستخدم حيز التنفيذ الحالي. يمكن تكوين إستثناء NAT هنا أيضا. في هذا التكوين، تكون جميع حركة مرور IPv4 من الواجهة الداخلية التي تنتقل إلى عناوين IP لعميل AnyConnect باستثناء من NAT. بالنسبة للتعيينات الأكثر تعقيدا مثل تقييم الأطراف من الخارج إلى الخارج، ستحتاج قواعد NAT إضافية في إطار سياسة NAT. يمكن العثور على حزم AnyConnect على موقع دعم Cisco: https://software.cisco.com/download/home. يلزم توفر ترخيص Plus أو Apex صالح لتنزيل حزمة AnyConnect.



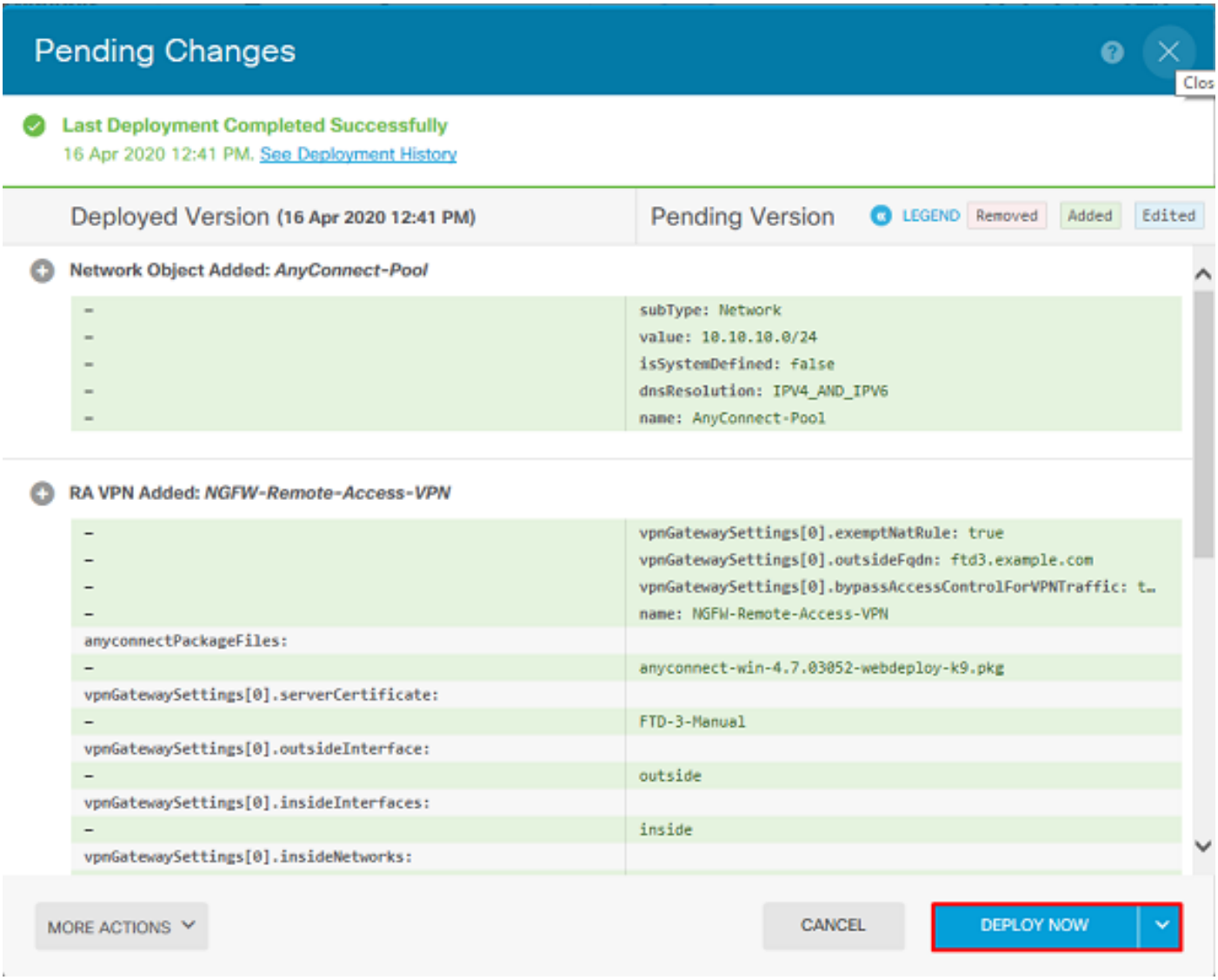
6. ضمن قسم الملخص، تحقق من إعداد AnyConnect بشكل مناسب، ثم انقر فوق **إرسال الاستعلام**.



7. انقر زر **التغييرات المعلقة** في أعلى اليمين كما هو موضح في الصورة.



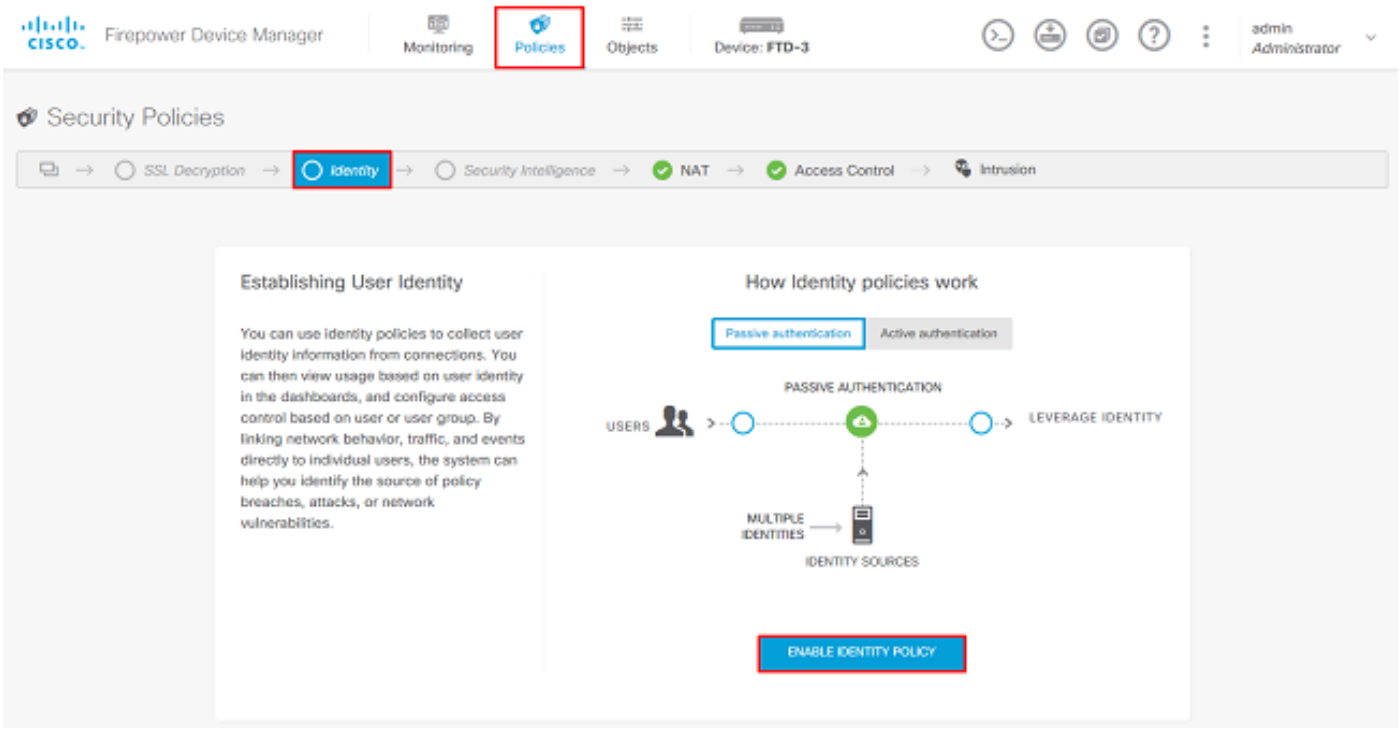
8. انقر فوق **نشر الآن**.



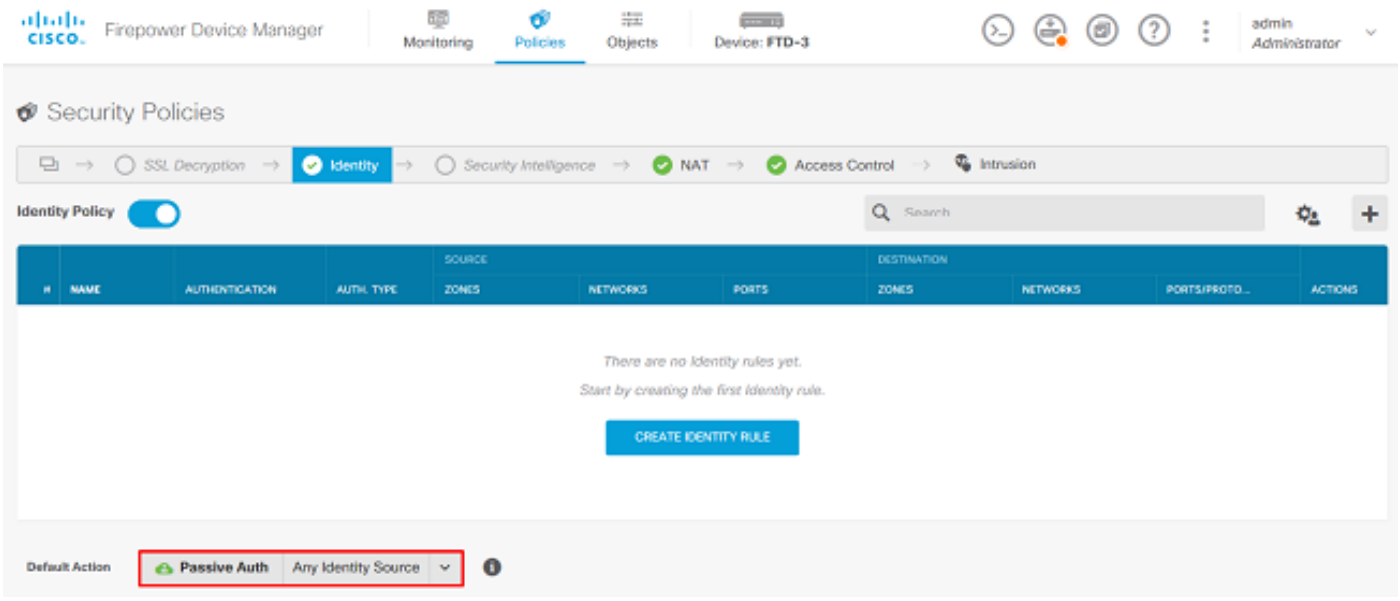
تمكين نهج الهوية وتكوين سياسات الأمان لهوية المستخدم

عند هذه النقطة، يجب أن يكون مستخدم AnyConnect قادرين على الاتصال بنجاح، ولكن قد لا يكونوا قادرين على الوصول إلى موارد معينة. ستؤدي هذه الخطوة إلى تمكين هوية المستخدم بحيث يمكن فقط للمستخدمين ضمن مسؤولي AnyConnect الاتصال بالموارد الداخلية باستخدام RDP ويمكن فقط لمستخدمي AnyConnect ضمن المجموعة الاتصال بالموارد الداخلية باستخدام HTTP.

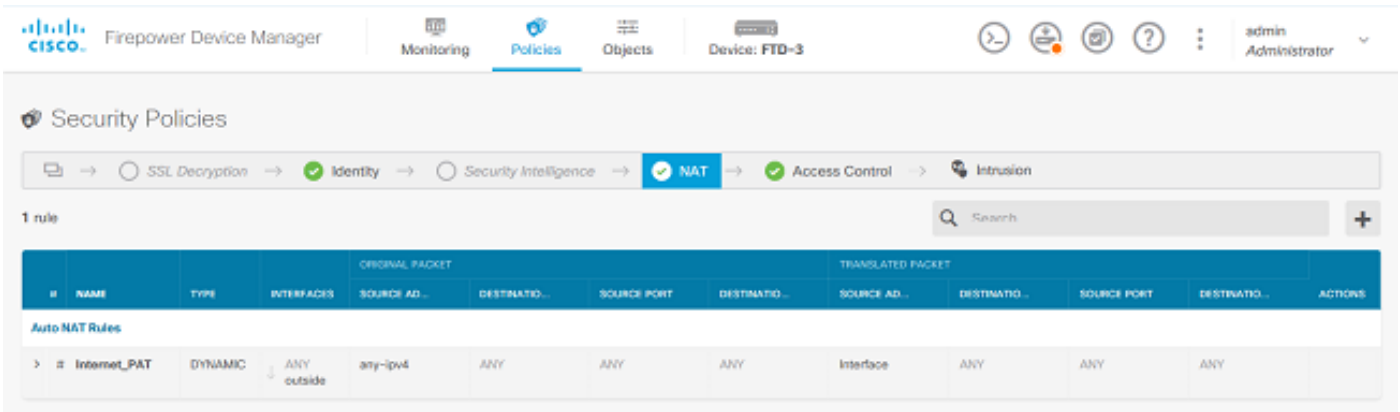
1. انتقل إلى **السياسات > الهوية** وانقر فوق **تمكين نهج الهوية**.



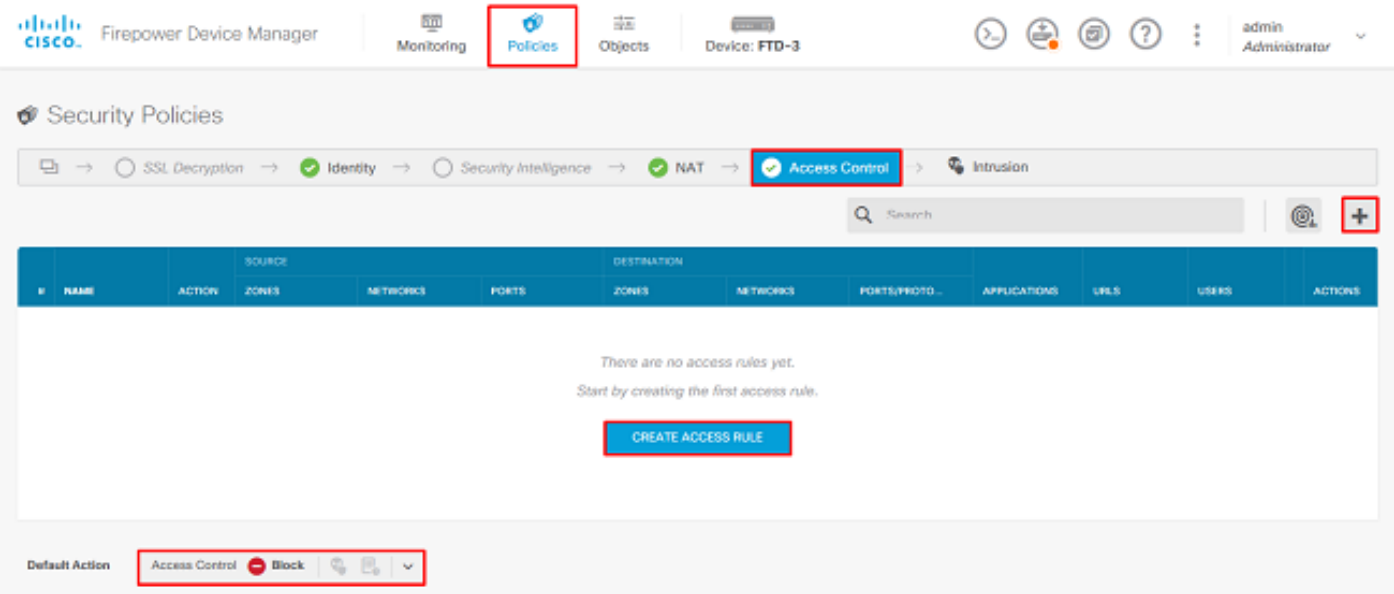
ل هذا تشكيل، ام من تشكيل إضافي مطلوب والإجراء تقصير كافي.



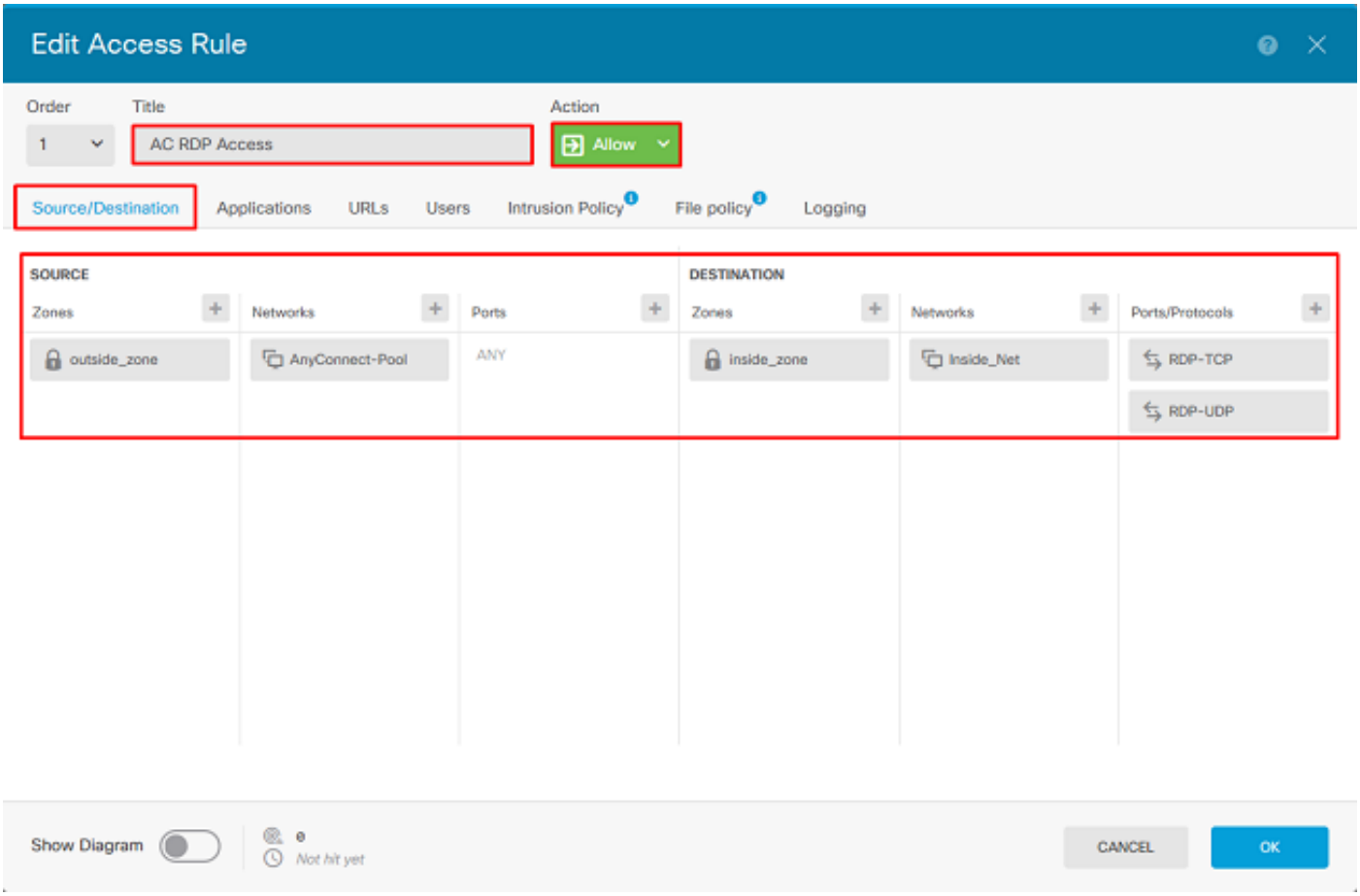
2. انتقل إلى **السياسات > NAT** وتأكد أن NAT شكلت بشكل مناسب. إذا كان إستثناء NAT الذي تم تكوينه في إعدادات AnyConnect كافيا، فلن تكون هناك حاجة إلى تكوين إضافي هنا.



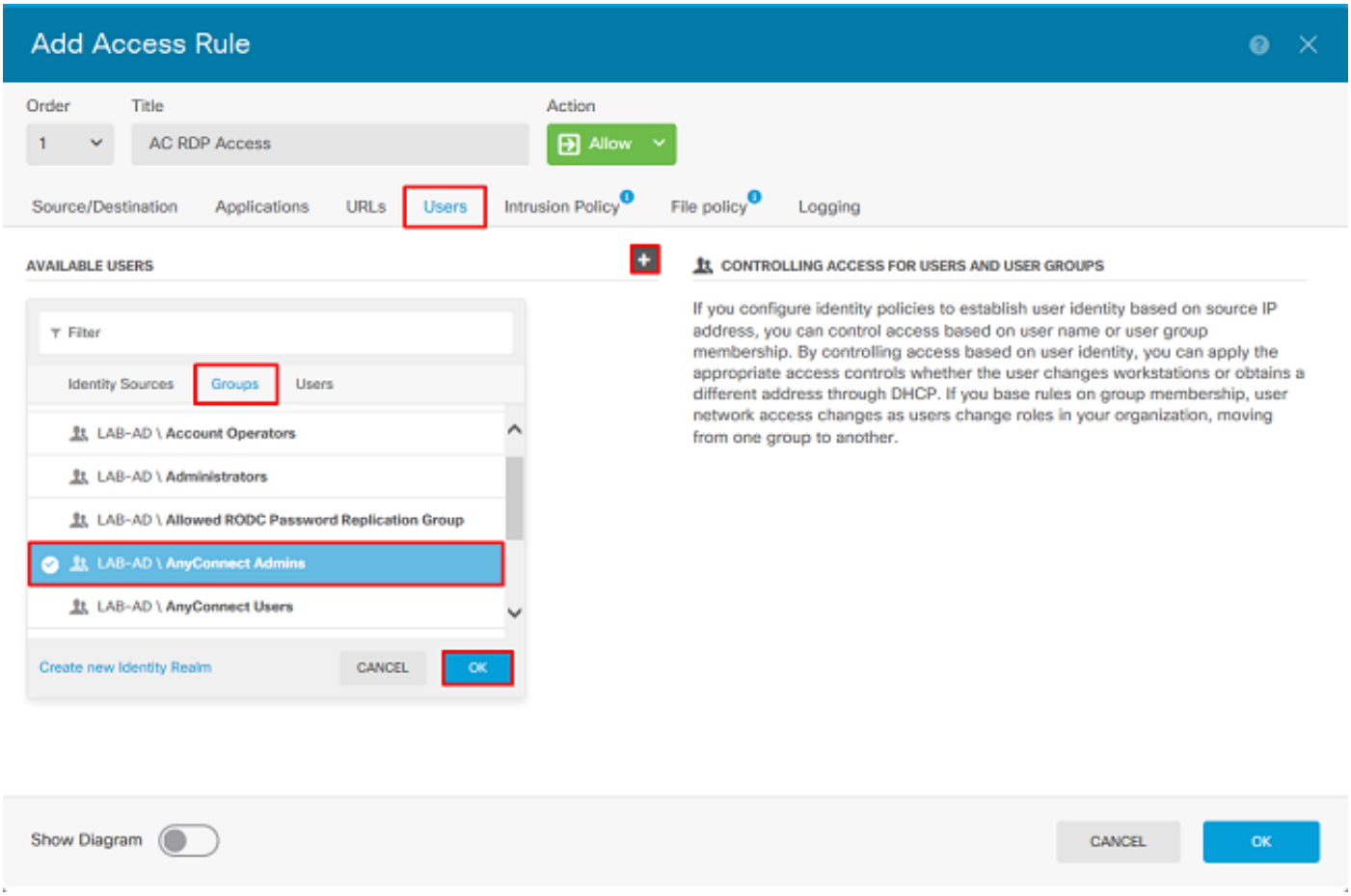
3. انتقل إلى **السياسات > التحكم في الوصول**. في هذا القسم، يتم تعيين "الإجراء الافتراضي" على "الحظر" ولم يتم إنشاء قواعد وصول لذلك بمجرد اتصال مستخدم AnyConnect، لن يكون قادرا على الوصول إلى أي شيء. انقر فوق + الرمز أو قم بإنشاء قاعدة وصول إضافة قاعدة جديدة.



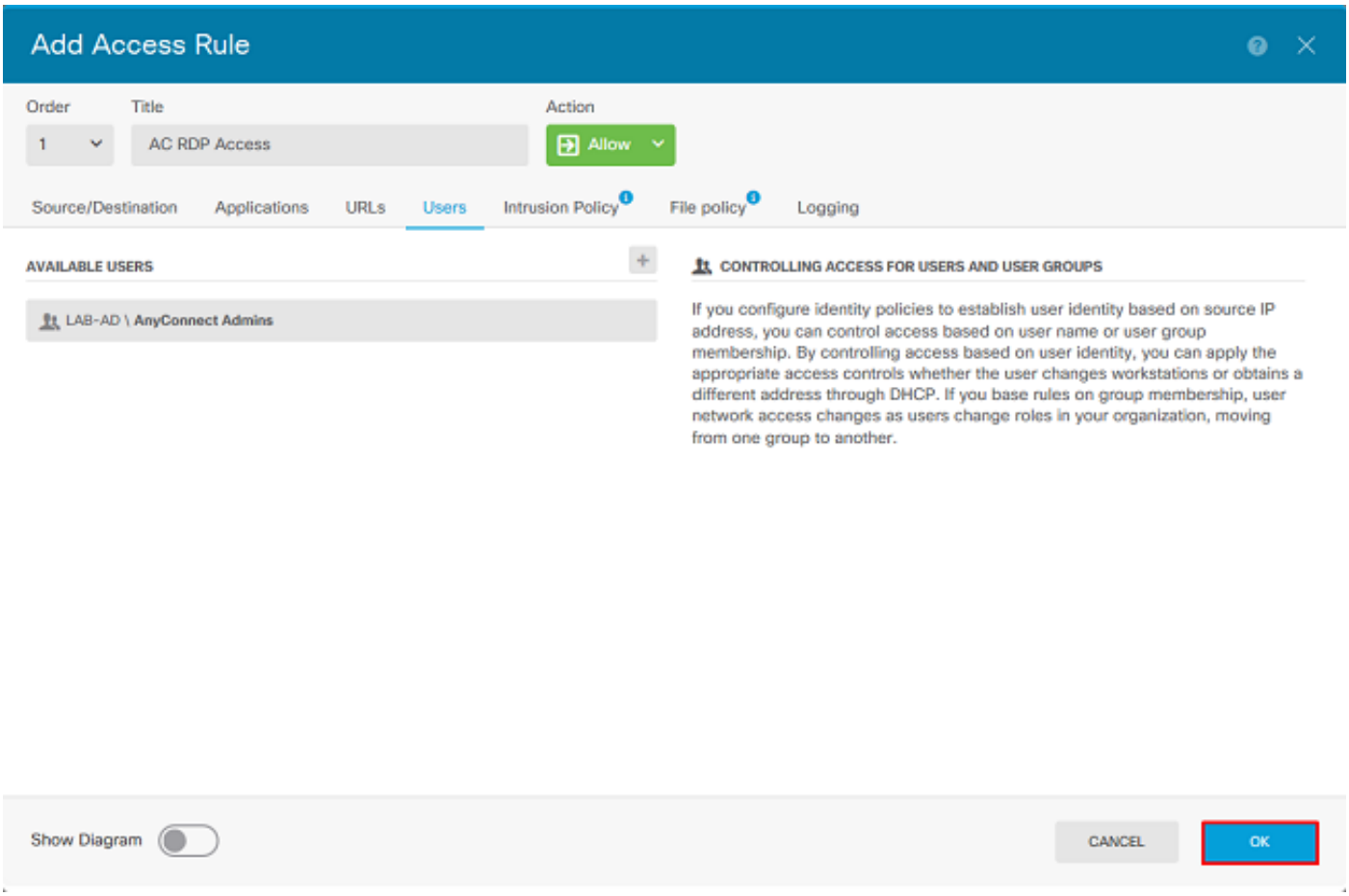
4. المأل الحقول بالقيم المناسبة. في هذا التكوين، يجب أن يتمتع المستخدمون داخل مجموعة مسؤولي AnyConnect بحق وصول RDP إلى خادم Windows في الشبكة الداخلية. بالنسبة للمصدر، تم تكوين المنطقة كمنطقة خارجية هي الواجهة الخارجية التي ستتم تصال مستخدمي AnyConnect بها وتم تكوين الشبكة كائن AnyConnect-Pool الذي تم تكوينه مسبقا لتعيين عناوين IP لعملاء AnyConnect. بالنسبة لوجهة المستخدم في FDM، يجب أن يكون المصدر هو المنطقة والشبكة التي سيقوم المستخدم ببدء الاتصال منها. بالنسبة للوجهة، تم تكوين المنطقة كما هو داخل_zone وهو الواجهة الداخلية التي يقع عليها خادم Windows، وتم تكوين الشبكة كائن Inside_Net الذي هو كائن يعرف الشبكة الفرعية التي يوجد فيها خادم Windows، وتم تعيين المنافذ/البروتوكولات على كائنين من المنافذ المخصصة للسماح بوصول RDP عبر بروتوكول TCP 3389 و UDP 3389.



تحت قسم "المستخدمون"، ستتم إضافة مسؤولي AnyConnect للمجموعة بحيث يتم السماح للمستخدمين الذين يفصلون عن هذه المجموعة بوصول RDP إلى خادم Windows. انقر فوق + الرمز، وانقر فوق عالمة التبويب مجموعات، وانقر فوق المجموعة المناسبة، ثم انقر فوق **موافق**. الحظ أنه يمكن تحديد مستخدمين فرديين ومصدر الهوية كذلك.

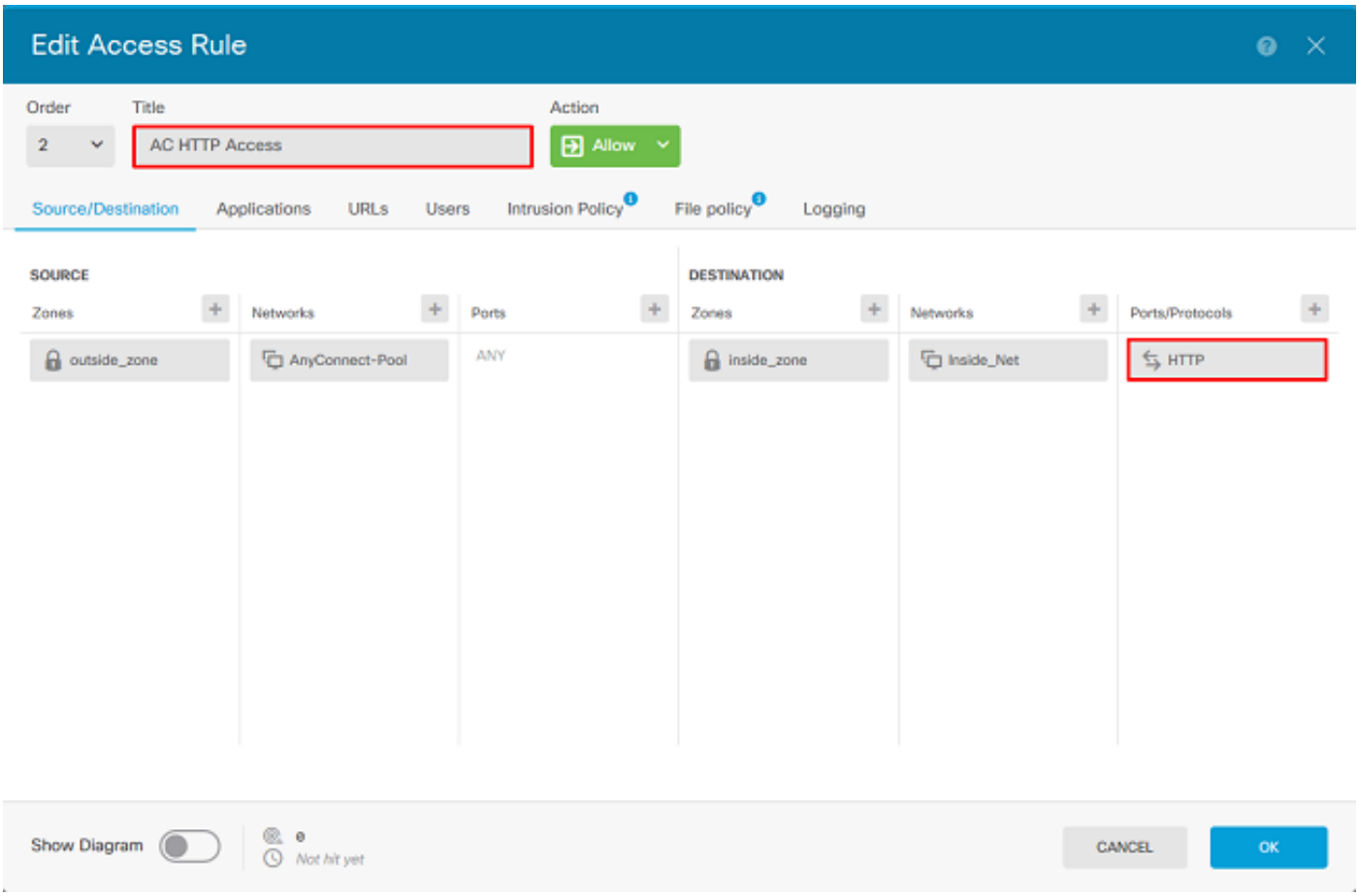


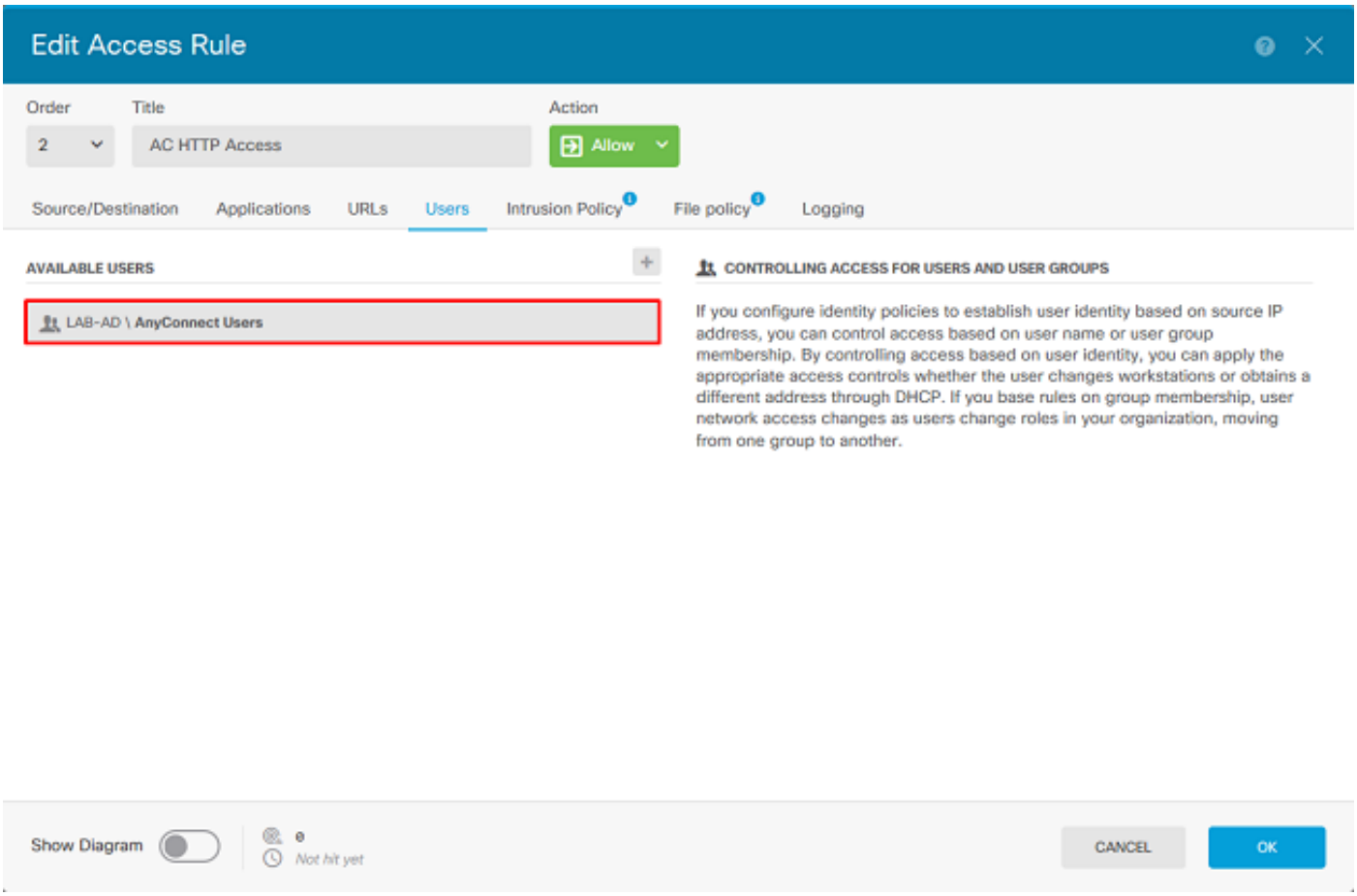
بمجرد تحديد الخيارات المناسبة، انقر فوق **موافق**.



5. قم بإنشاء المزيد من قواعد الوصول إذا لزم الأمر. في هذا التكوين، يتم إنشاء قاعدة

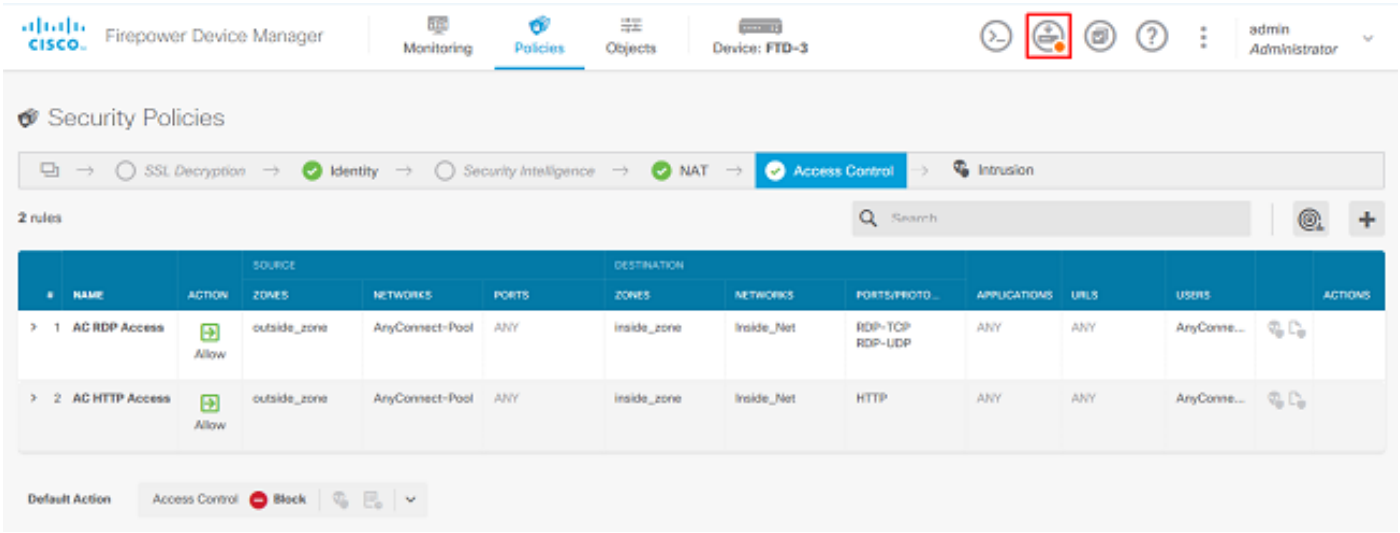
وصول أخرى للسماح للمستخدمين ضمن مجموعة مستخدمي AnyConnect بالوصول إلى HTTP من خادم Windows.



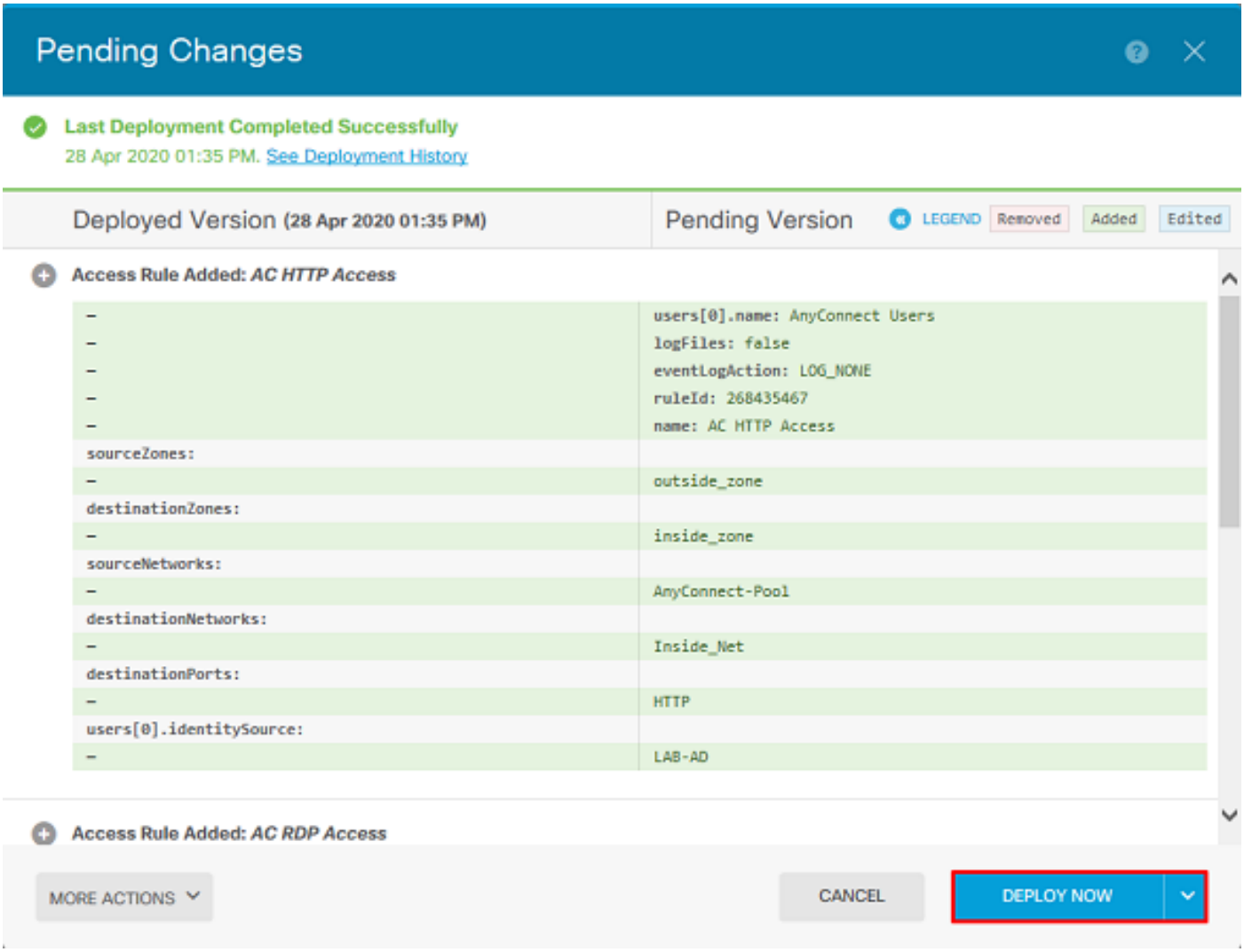


6. تحقق من تكوين قاعدة الوصول ثم انقر فوق زر **التغييرات المعلقة** في أعلى اليمين

كما هو موضح في الصورة.



7. تحقق من التغييرات، ثم انقر فوق **نشر الآن**.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

الترتيب النهائي

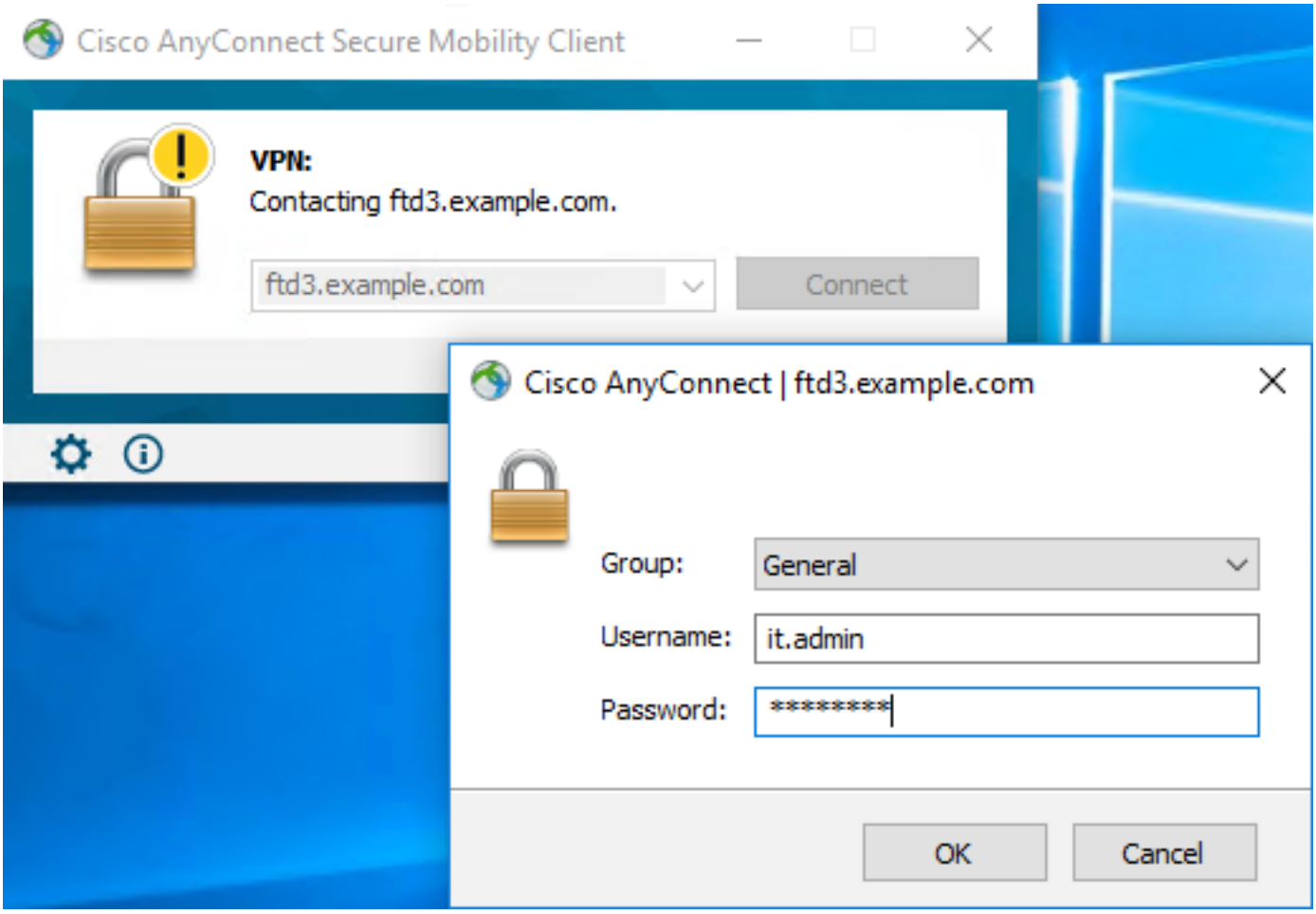
تكوين AAA

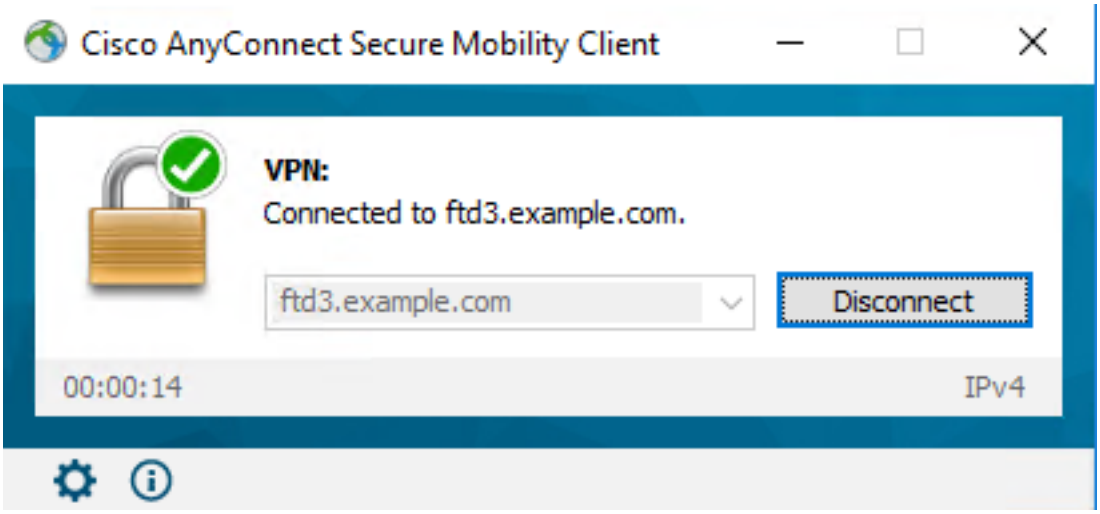
```
show running-configuration aaa-server
aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com server-
port 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-login-
dn ftd.admin@example.com server-type auto-detect
```

تكوين AnyConnect

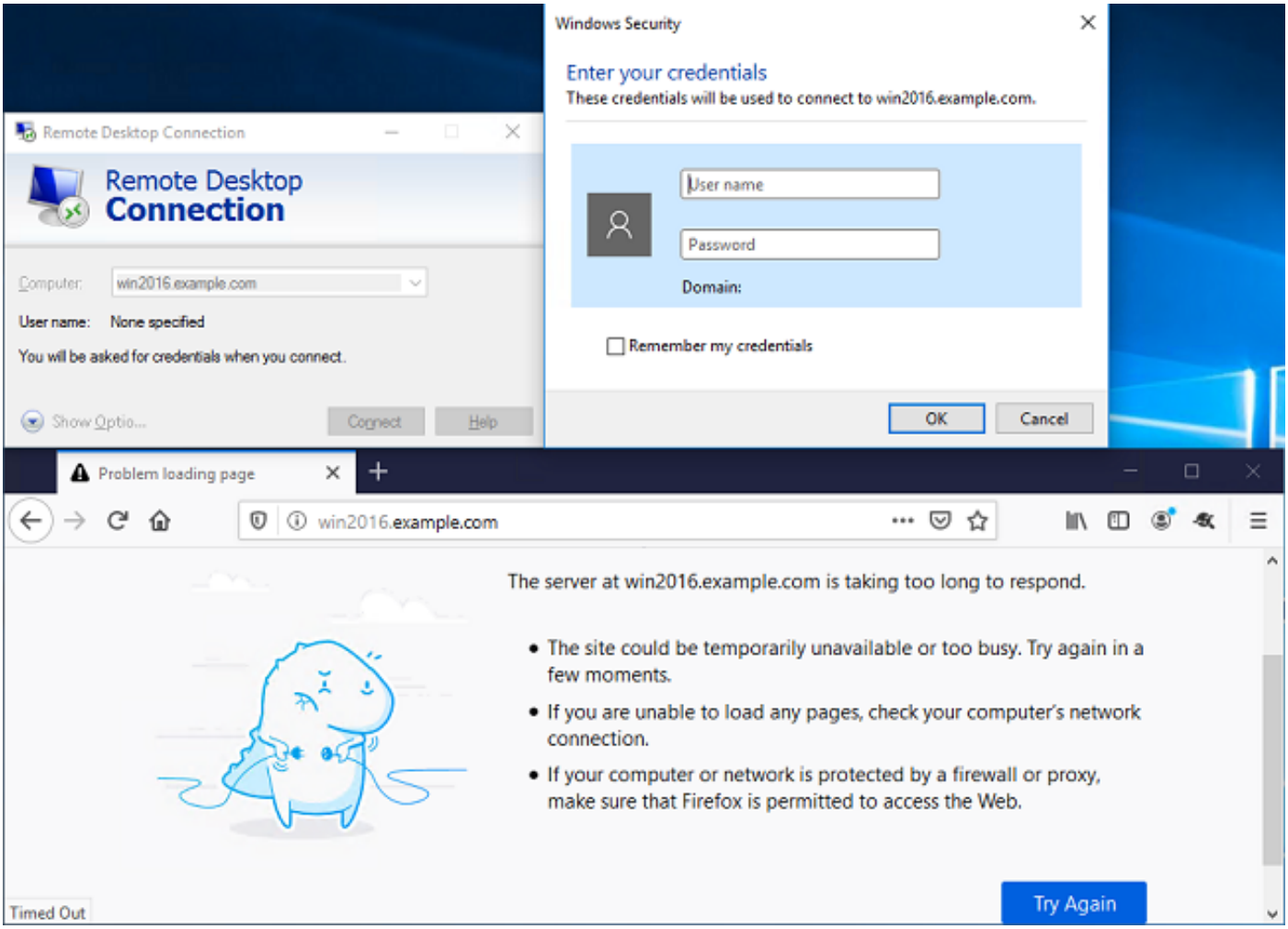
```
> show running-config webvpn
webvpn
 enable outside
 http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
 anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable

> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
 address-pool AnyConnect-Pool
 authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
 group-alias General enable

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

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

الاتصال بقواعد سياسة التحكم في الوصول من AnyConnect والتحقق منها

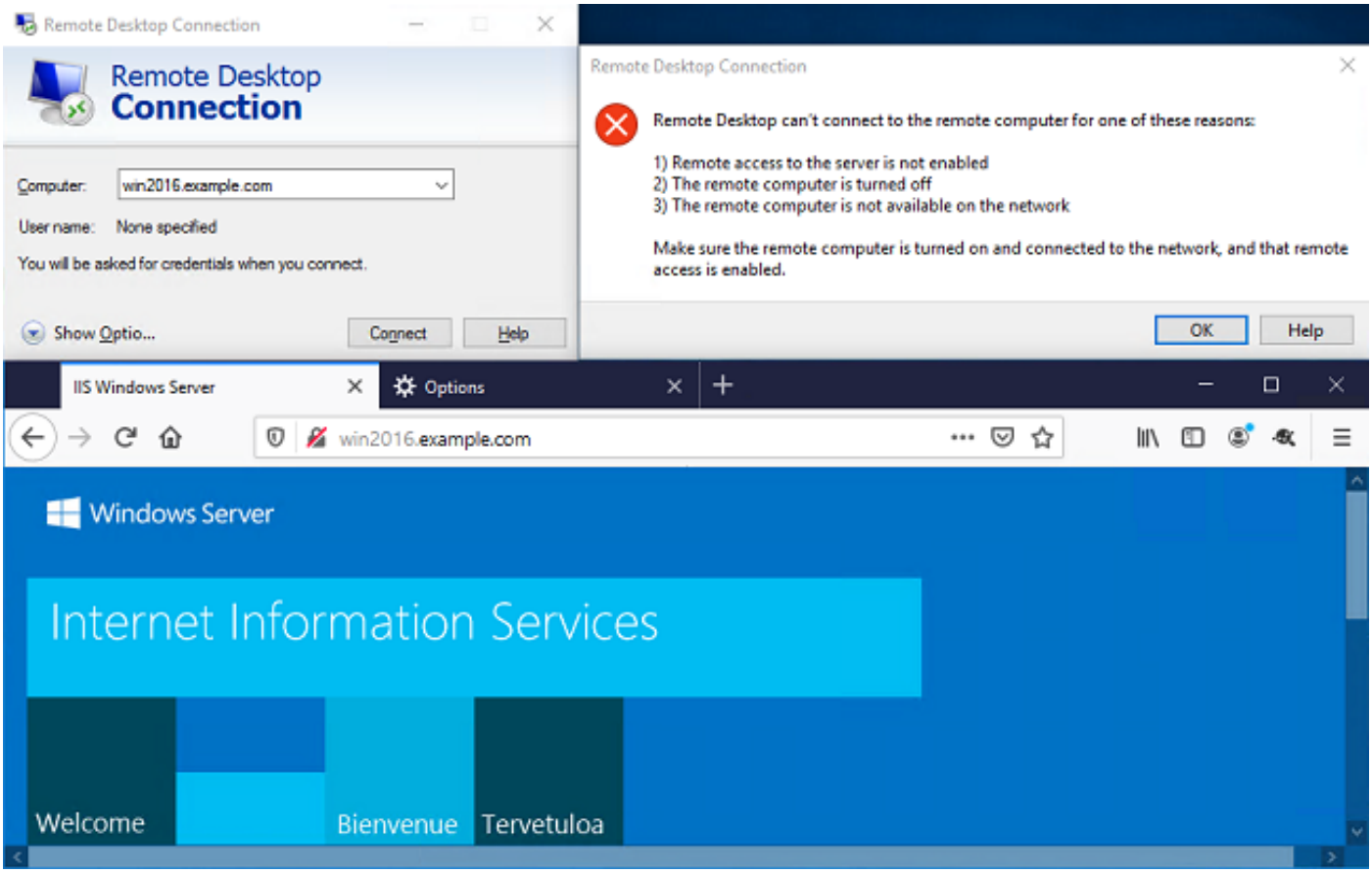




User IT Admin موجود في المجموعة AnyConnect Admins التي لديها وصول RDP إلى Windows Server، ومع ذلك ليس لديها وصول إلى HTTP. إن فتح جلسة عمل RDP و Firefox لهذا الخادم يتحقق من أن هذا المستخدم يمكنه الوصول إلى الخادم عبر RDP فقط.



إذا قمت بتسجيل الدخول باستخدام مستخدم إختبار موجود في مجموعة مستخدمي AnyConnect الذين لديهم وصول HTTP وليس وصول RDP، فيمكنك التحقق من أن قواعد سياسة التحكم في الوصول أصبحت سارية المفعول.



استكشاف الأخطاء وإصلاحها

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تصحيح الأخطاء

يمكن تشغيل تصحيح الأخطاء هذا في CLI تشخيصي لاستكشاف أخطاء مصادقة LDAP وإصلاحها: **debug ldap 255**.

لاستكشاف أخطاء سياسة التحكم في الوصول لهوية المستخدم وإصلاحها، يمكن تشغيل **جدار حماية محرك تصحيح الأخطاء** الخاص **بدعم النظام** في قائمة التحكم لتحديد سبب السماح بحركة المرور أو منعها بشكل غير متوقع.

تصحيح أخطاء LDAP العاملة

```
[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
```

تعذر إنشاء اتصال بخادم LDAP

```
[-2147483611] Session Start
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611] Connect to LDAP server: ldap://172.16.1.1:389, status = Failed
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

الحلول المحتملة:

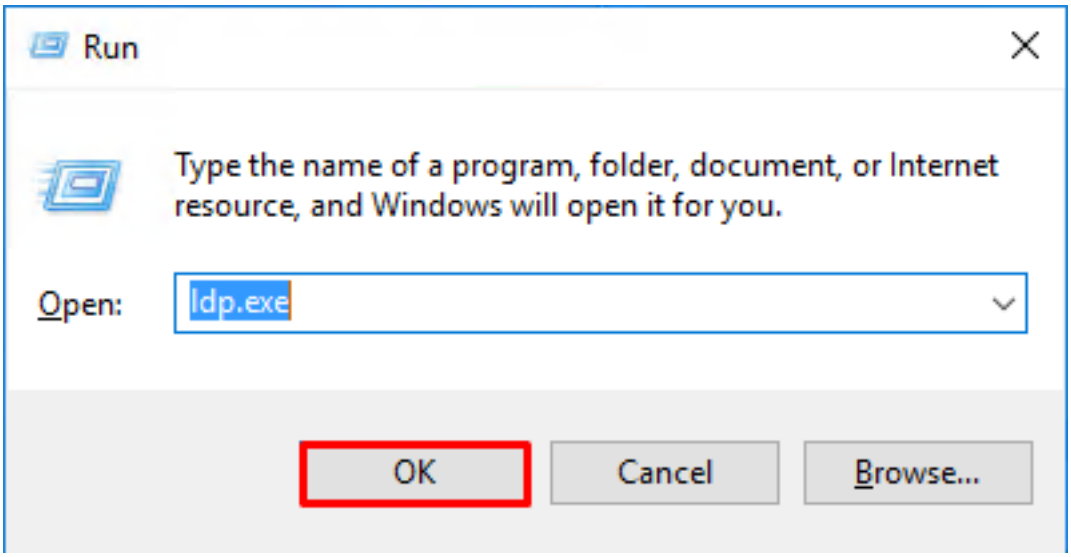
- تحقق من التوجيه وتأكد من أن FTD يتلقى إستجابة من خادم LDAP.
- في حالة إستخدام LDAP أو STARTTLS، تأكد من أن شهادة CA الجذر الصحيحة موثوق بها بحيث يمكن إكمال مصافحة SSL بنجاح.
- دقق أن يستعمل العنوان ومينا صحيح. إذا تم إستخدام اسم المضيف، فتحقق من قدرة DNS على حله إلى عنوان IP الصحيح

DN و/أو كلمة المرور للربط غير صحيحة

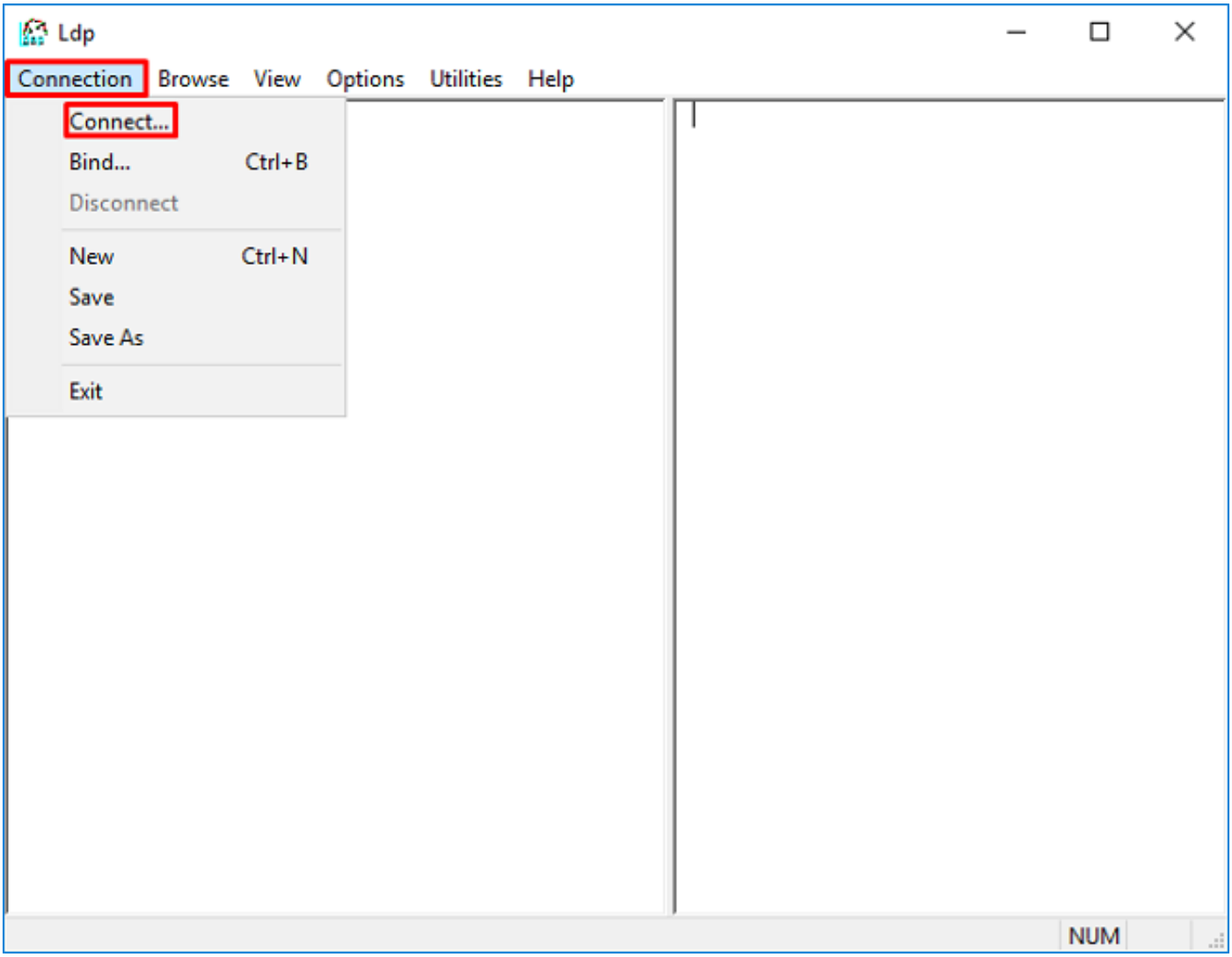
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615]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

الحل المحتمل: تحقق من تكوين شبكة DN الخاصة بتسجيل الدخول وكلمة مرور تسجيل الدخول بشكل صحيح. يمكن التحقق من هذا الإجراء على خادم AD باستخدام **ldp.exe**. للتحقق من إمكانية ربط حساب بنجاح باستخدام LDP، انتقل عبر الخطوات التالية:

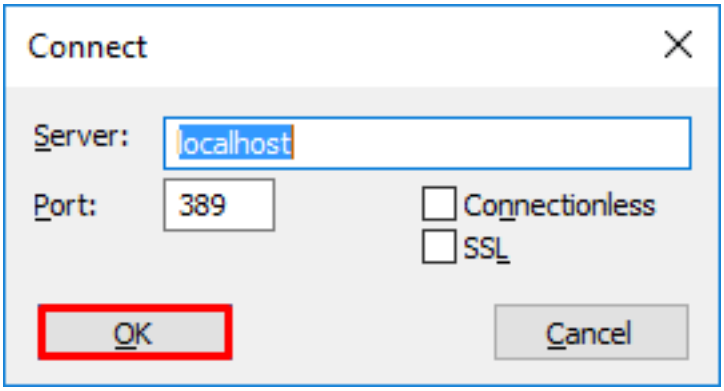
1. على خادم AD، اضغط على **Win+R** وابحث عن **ldp.exe**.



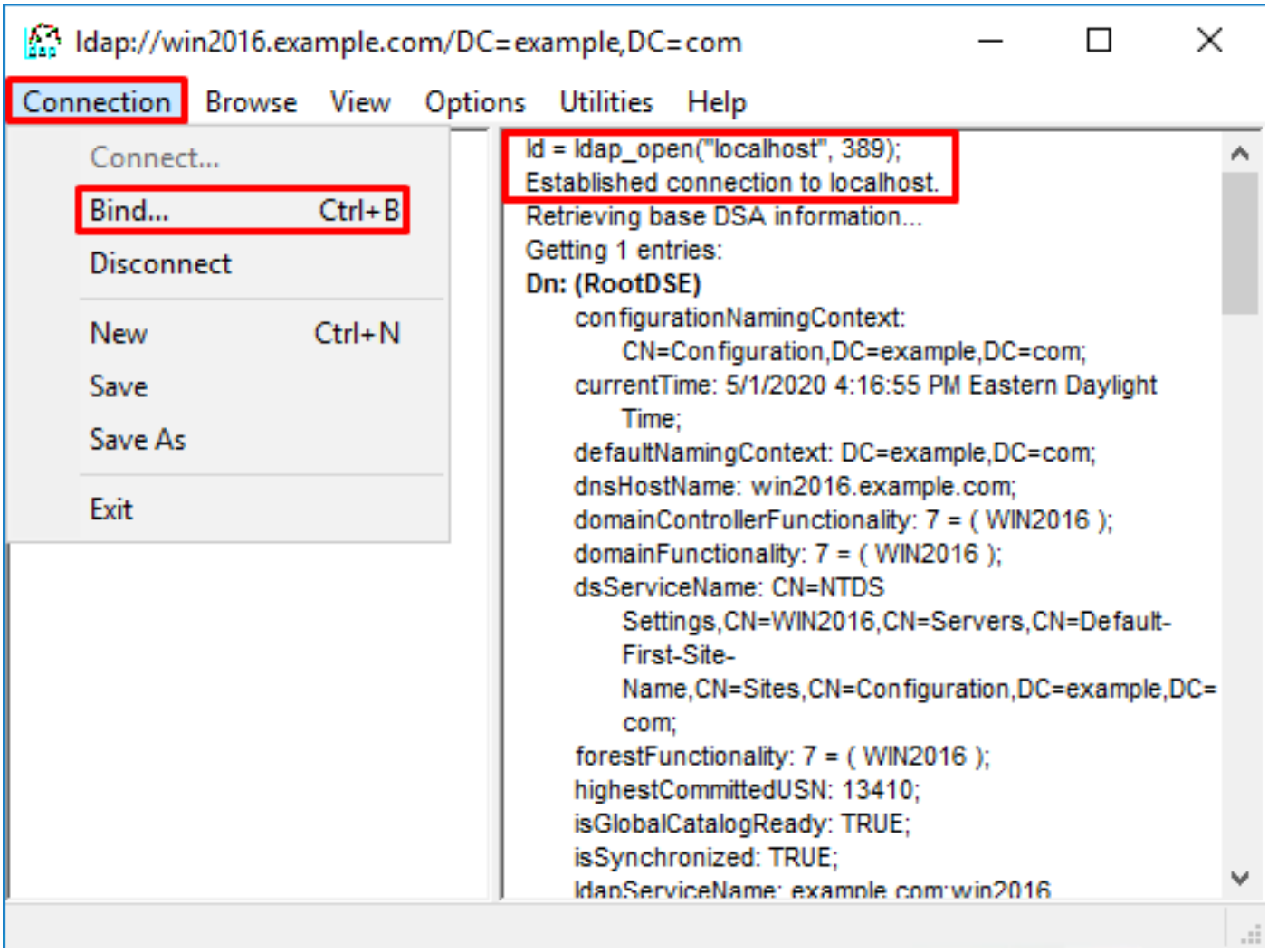
2. انقر فوق **اتصال > اتصال...** كما هو موضح في الصورة.



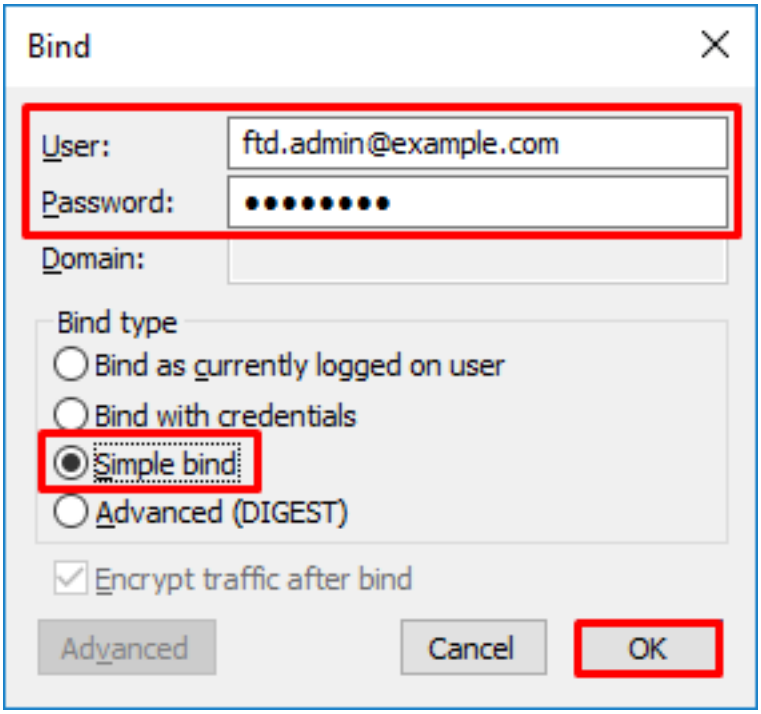
3. حدد مضيف محلي للخادم والمنفذ المناسب، ثم انقر فوق **موافق**.



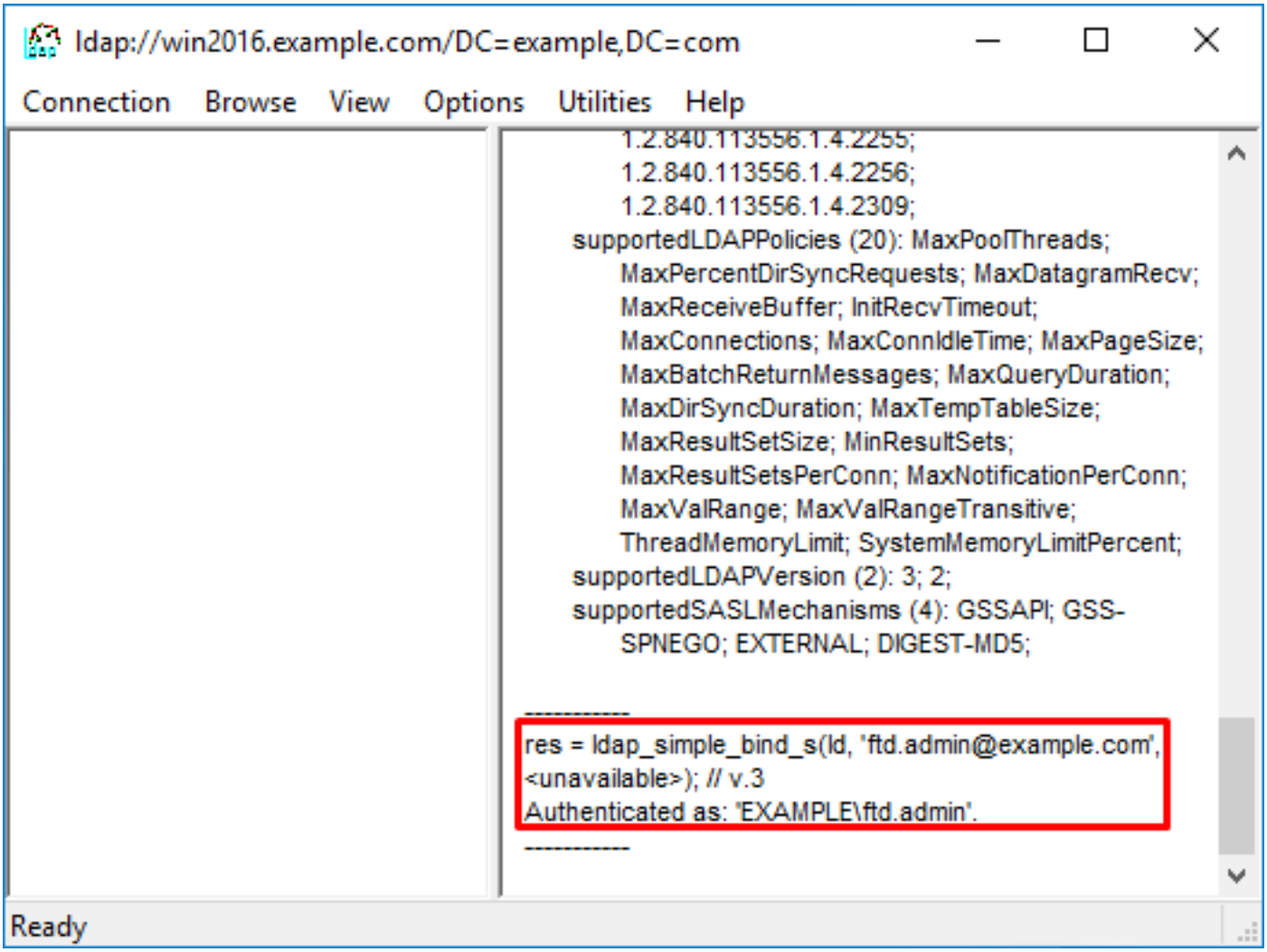
4. يظهر العمود الأيمن النص الذي يشير إلى اتصال ناجح. انقر على **اتصال > ربط...** كما هو موضح في الصورة.



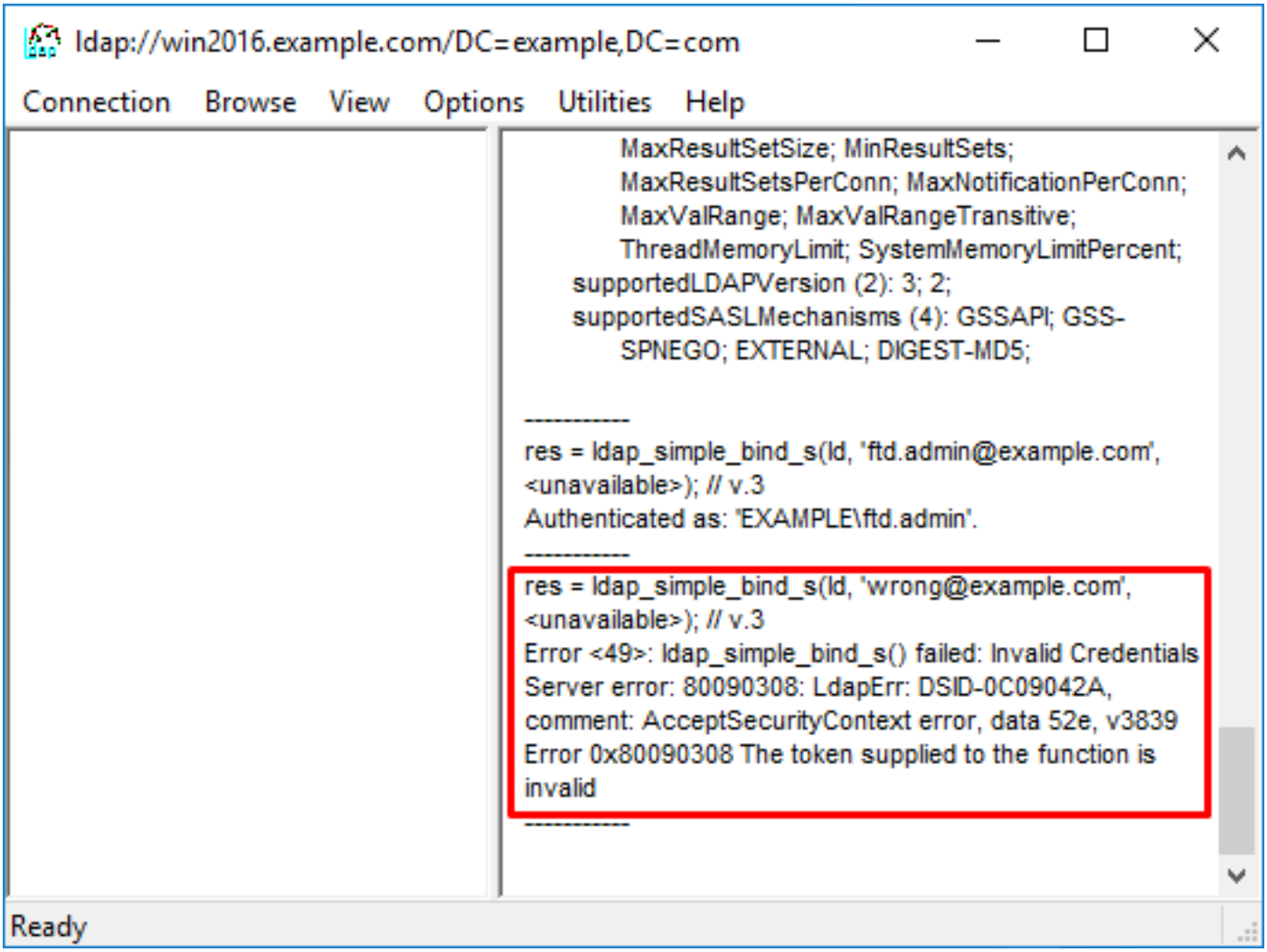
5. حدد **ربط بسيط**، ثم حدد اسم مستخدم حساب الدليل وكلمة المرور. وانقر فوق **OK**.



باستخدام ربط ناجح، سيظهر LDP مصدق عليه كـ **DOMAIN\username**.



إذا حاولت ربط اسم مستخدم أو كلمة مرور غير صحيحة، فسيؤدي ذلك إلى فشل مثل هذا.

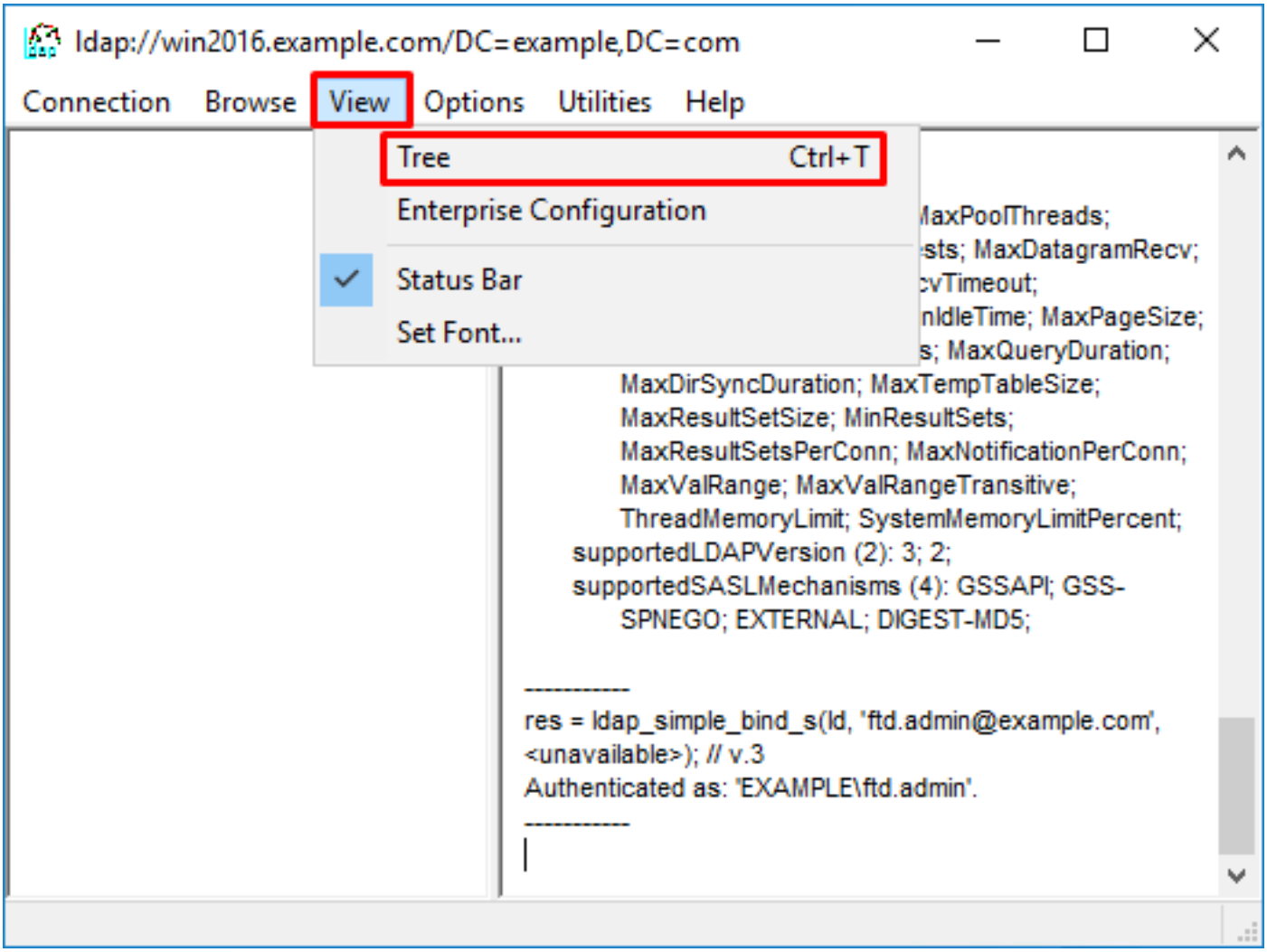


تعذر على خادم LDAP العثور على اسم المستخدم

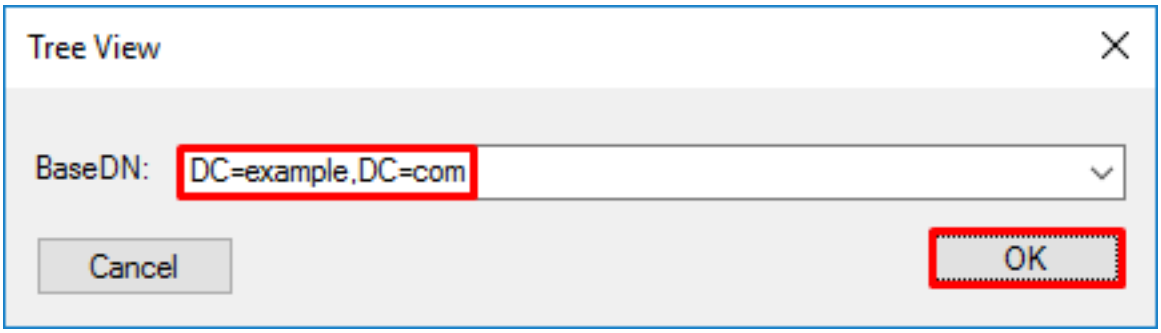
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612]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

الحل المحتمل: تحقق من أن AD يمكنه العثور على المستخدم مع البحث الذي تم بواسطة FTD. ويمكن القيام بذلك أيضا مع LDP.exe.

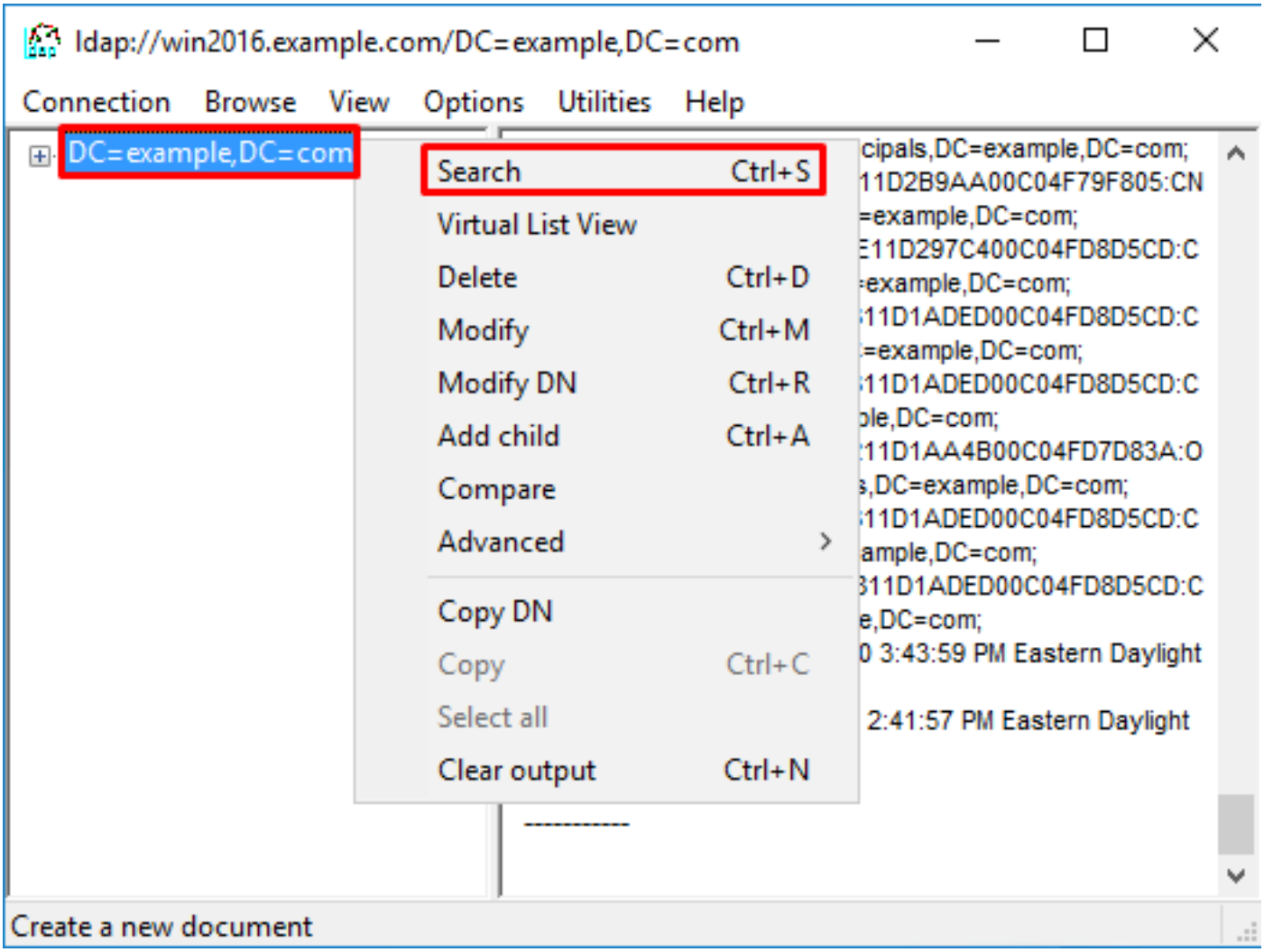
1. بعد الربط بنجاح، انتقل إلى **عرض > شجرة** كما هو موضح في الصورة.



2. حدد DN الأساسي الذي تم تكوينه على FTD ثم انقر فوق **موافق**.

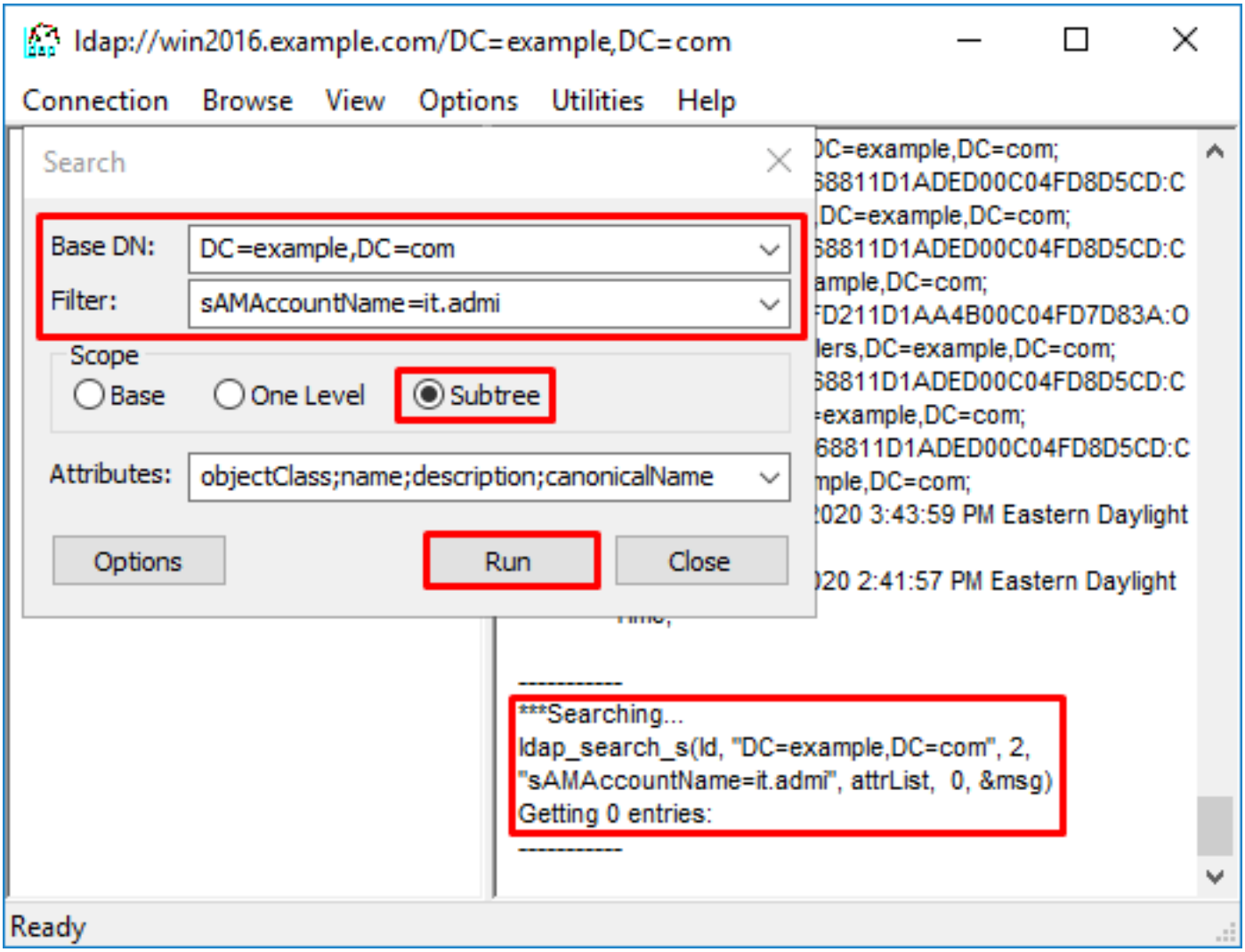


3. انقر بزر الماوس الأيمن فوق DN الأساسي ثم انقر فوق بحث كما هو موضح في الصورة.



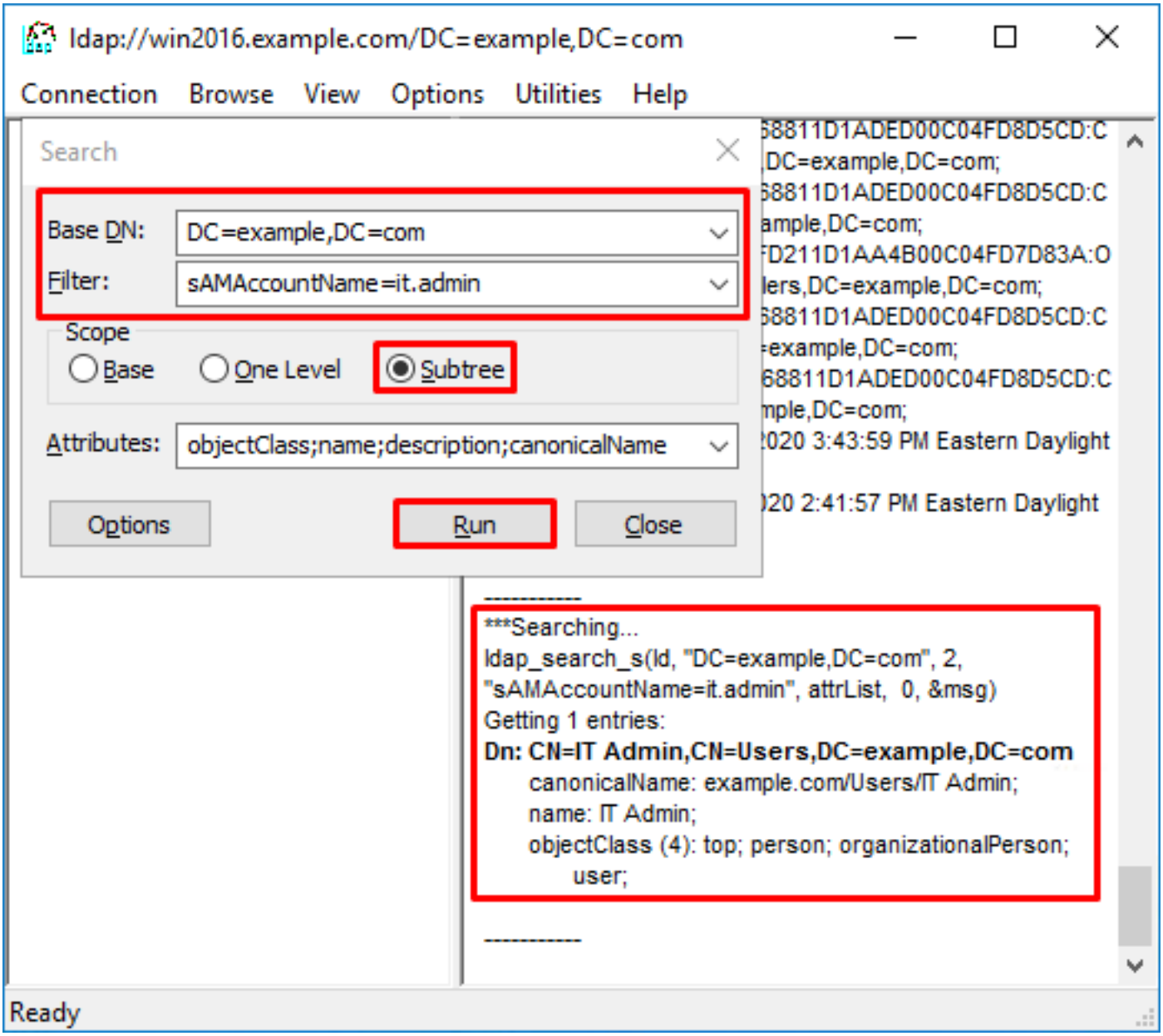
4. حدد نفس قيم قاعدة البيانات (DB) وعامل التصفية والنطاق الأساسية كما ظهر في تصحيح الأخطاء. في هذا المثال، هذه:

- شبكة DN الأساسية: dc=example،dc=com
- عامل التصفية: samaccountName=it.admi
- النطاق:الشجرة الفرعية



يبحث LDP عن 0 إدخالات نظرا لعدم وجود حساب مستخدم باسم **samaccountName=it.admi** أسفل DN الأساسي=example،dc=com.

تظهر المحاولة مرة أخرى باستخدام **samaccountName=it.admin** الصحيح نتيجة مختلفة.
يبحث LDP عن إدخال واحد تحت DN الأساسي=example،dc=com ويطبع DN الخاص بالمستخدم.



كلمة المرور غير صحيحة لاسم المستخدم

```
[-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
```

الحل المحتمل: تحقق من تكوين كلمة مرور المستخدم بشكل صحيح ومن عدم انتهاء صلاحيته. وهو الحال مع DN التسجيل الدخول، سيوقف FTD بإجراء ربط ضد AD باستخدام بيانات اعتماد المستخدم. كما يمكن تنفيذ هذه الربط في ldp للتحقق من قدرة AD على التعرف على نفس بيانات اعتماد اسم المستخدم وكلمة المرور. تظهر الخطوات في LDP في هذه المقالة. بالإضافة إلى ذلك، يمكن مراجعة سجلات "عارض أحداث خادم Microsoft" لسبب محتمل.

اختبار AAA

يمكن استخدام الأمر test aaa-server من FTD باستخدام اسم مستخدم وهمي وكلمة مرور محددين. يمكن استخدام هذا الاختبار لحالات فشل المصادقة أو الاتصال. الأمر هو **اختبار مصادقة خادم aaa [AAA-server] المضيف [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
```

التقاط الحزم

يمكن استخدام مجموعات الحزم للتحقق من إمكانية الوصول إلى خادم AD. إذا تداخلت حزم LDAP، ولكن لا توجد استجابة، فقد يشير ذلك إلى مشكلة في التوجيه.

هنا التقاط تم أن يبدي ثنائي اتجاه حركة مرور LDAP:

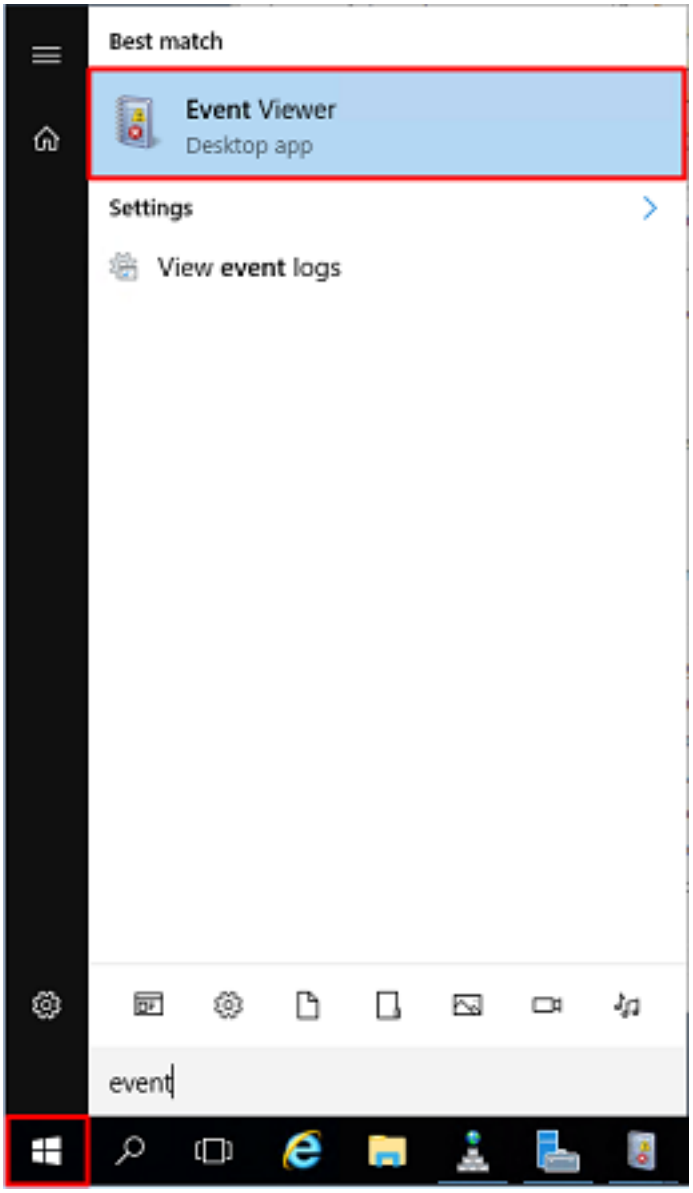
```
> show route 192.168.1.1

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
```

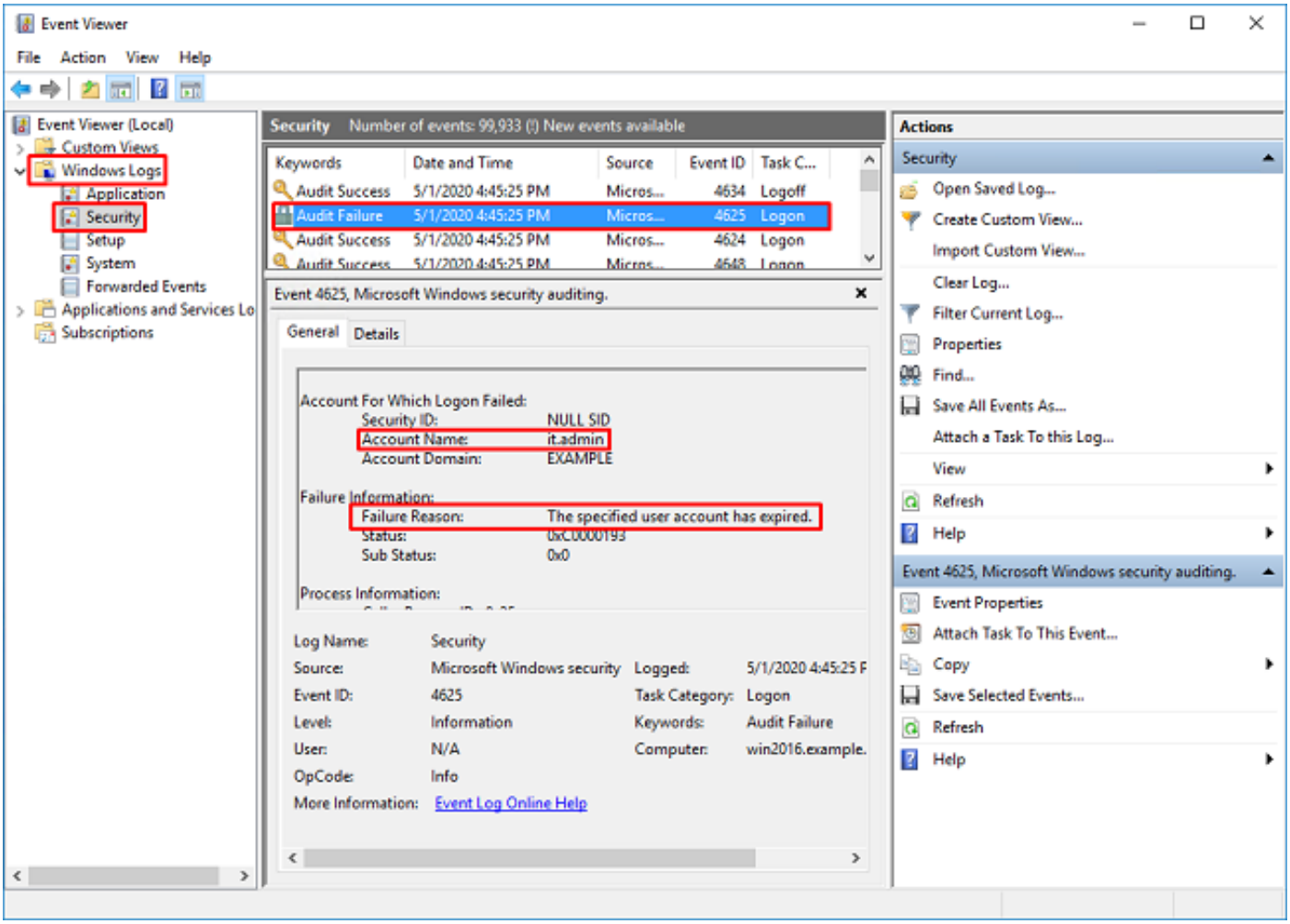
سجلات عارض أحداث Windows Server

تقوم سجلات "عارض الأحداث" الموجودة على عربة "خادم AD" بتوفير معلومات أكثر تفصيلا حول سبب حدوث عطل.

1. البحث عن **عارض الأحداث** وافتتاحه.



2. قم بتوسيع **سجلات Windows** وانقر فوق **الأمان**. ابحث عن **فشل التدقيق** باستخدام اسم حساب المستخدم وراجع معلومات الفشل كما هو موضح في الصورة.



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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).