تكوين المصادقة المستندة إلى شهادة AnyConnect للوصول أثناء التنقل

المحتويات

المقدمة

يوضح هذا المستند مثال لتنفيذ المصادقة المستندة إلى الشهادة على الأجهزة المحمولة.

المتطلبات الأساسية

الأدوات والأجهزة المستخدمة في الدليل هي:

- الدفاع ضد تهديد FirePOWER (FTD) من Cisco
- مركز إدارة Firepower (FMC)
- جهاز Apple iOS (iPhone، iPad)
- جهة منح الشهادة (CA)
- برنامج AnyConnect Client من Cisco

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة VPN أساسية
- SSL/TLS
- البنية الأساسية للمفتاح العام
- تجربة مع FMC
- OpenSSL

- Cisco AnyConnect

المكونات المستخدمة

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

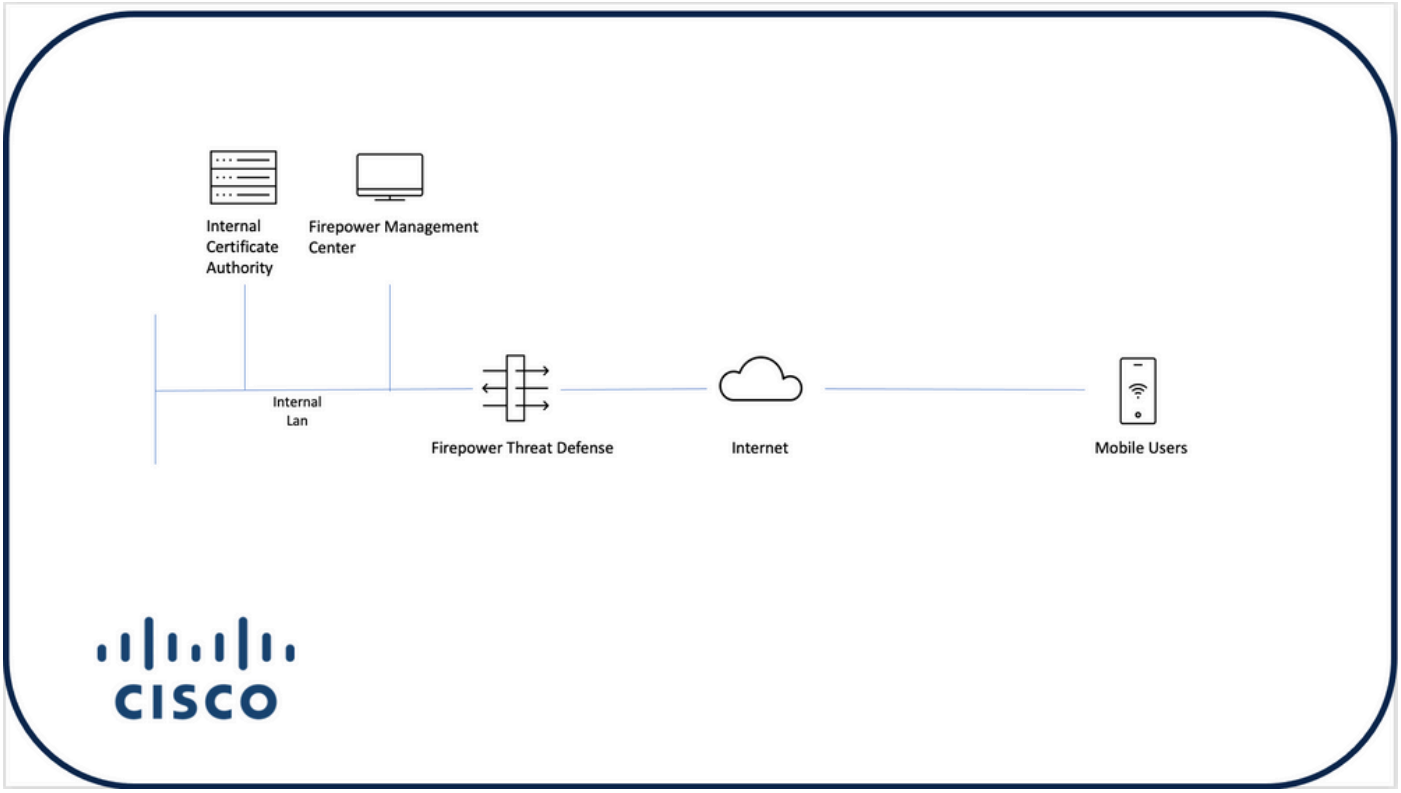
- Cisco FTD
- Cisco FMC
- خادم Microsoft CA
- XCA
- Cisco AnyConnect
- آبل آي باد

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.

تكوين Cisco AnyConnect على FTD

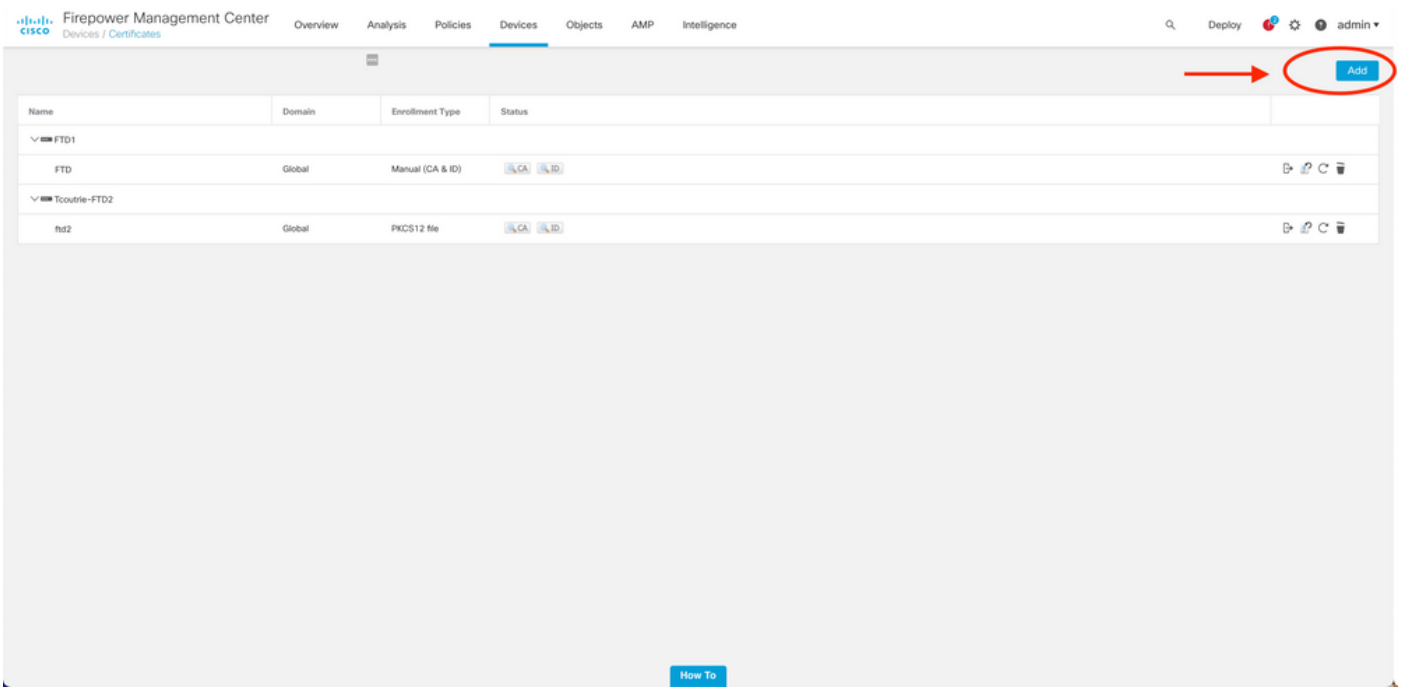
يصف هذا القسم خطوات تكوين AnyConnect عبر FMC. قبل البدء، تأكد من نشر جميع التكوينات.

الرسم التخطيطي للشبكة

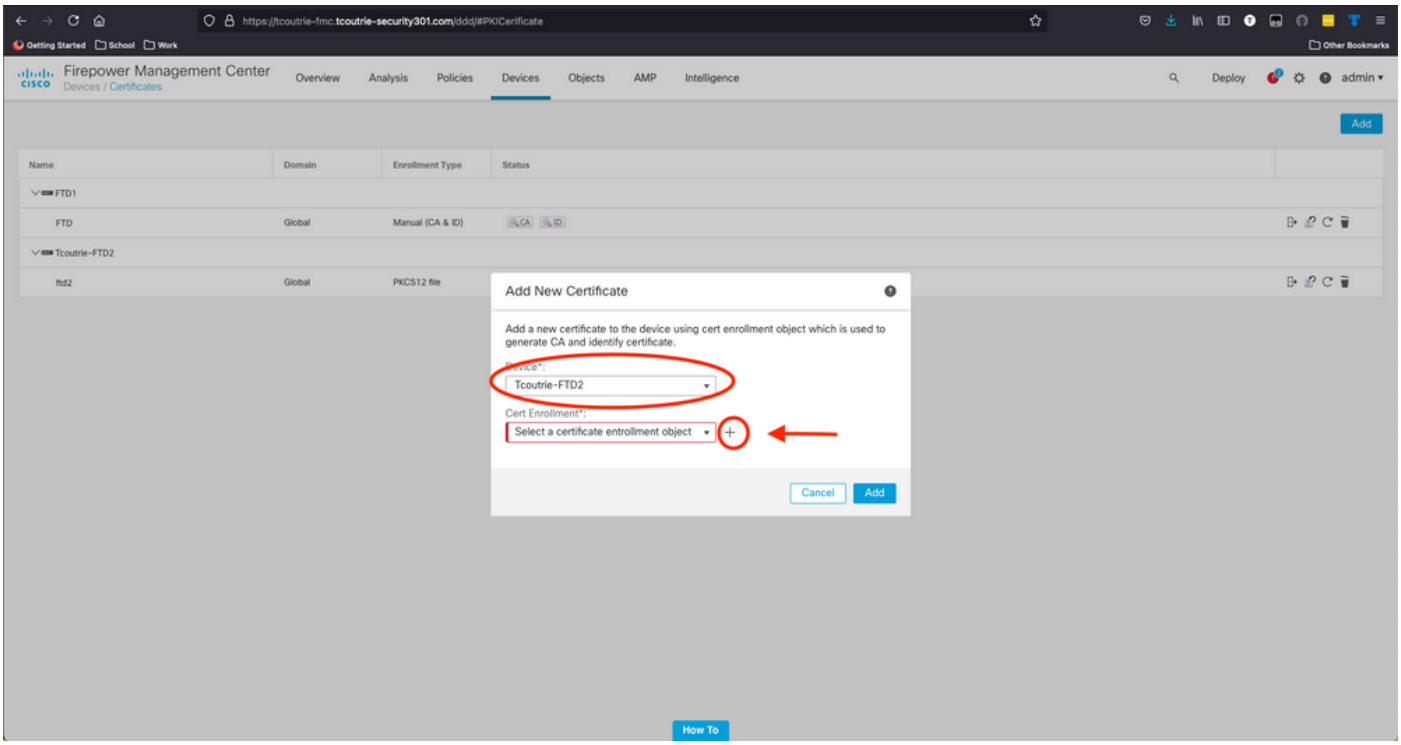


إضافة شهادة إلى FTD

الخطوة 1. قم بإنشاء شهادة ل FTD على جهاز FMC. انتقل إلى الأجهزة > الترخيص واختر إضافة، كما هو موضح في هذه الصورة:



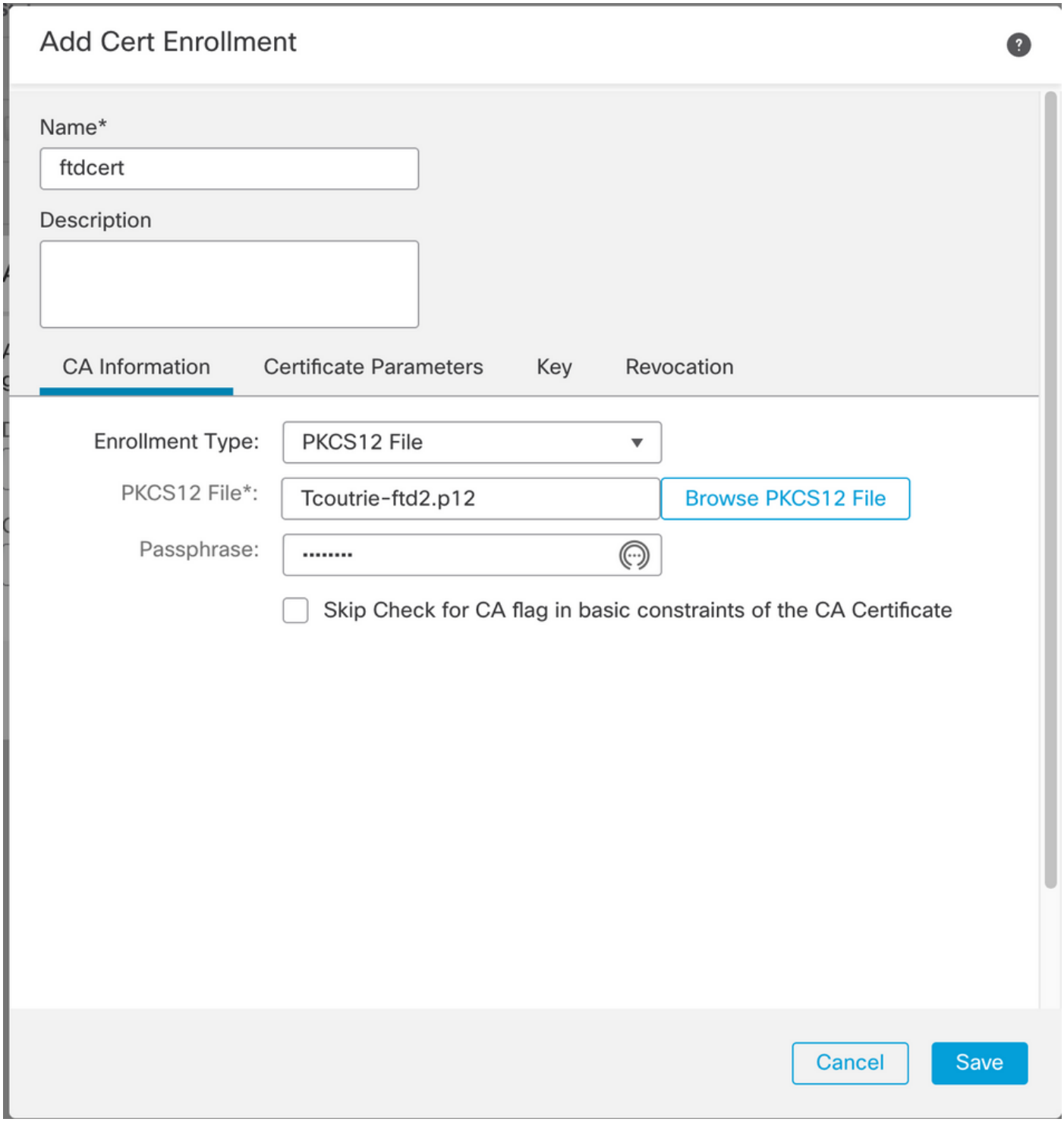
الخطوة 2. أختر FTD ب رغب ل ال VPN توصيل. أختر جهاز FTD من القائمة المنسدلة للأجهزة. انقر على أيقونة + لإضافة أسلوب تسجيل شهادة جديد، كما هو موضح في هذه الصورة:



الخطوة 3. قم بإضافة الشهادات إلى الجهاز. أختر الخيار الذي هو الطريقة المفضلة للحصول على الشهادات في البيئة.

تلميح: الخيارات المتاحة هي: شهادة موقعة ذاتيا - إنشاء شهادة جديدة محليا، SCEP - إستخدام بروتوكول تسجيل الشهادة البسيط للحصول على شهادة من CA، تثبيت يدوي- لشهادة الجذر والهوية، PKCS12 - تحميل حزمة الشهادة المشفرة بالجذر والهوية والمفتاح الخاص.

الخطوة 4. تحميل الشهادة إلى جهاز FTD. أدخل رمز المرور (PKCS12 فقط) وانقر حفظ، كما هو موضح في هذه الصورة:



ملاحظة: بمجرد حفظ الملف، يتم نشر الشهادات على الفور. لمشاهدة تفاصيل

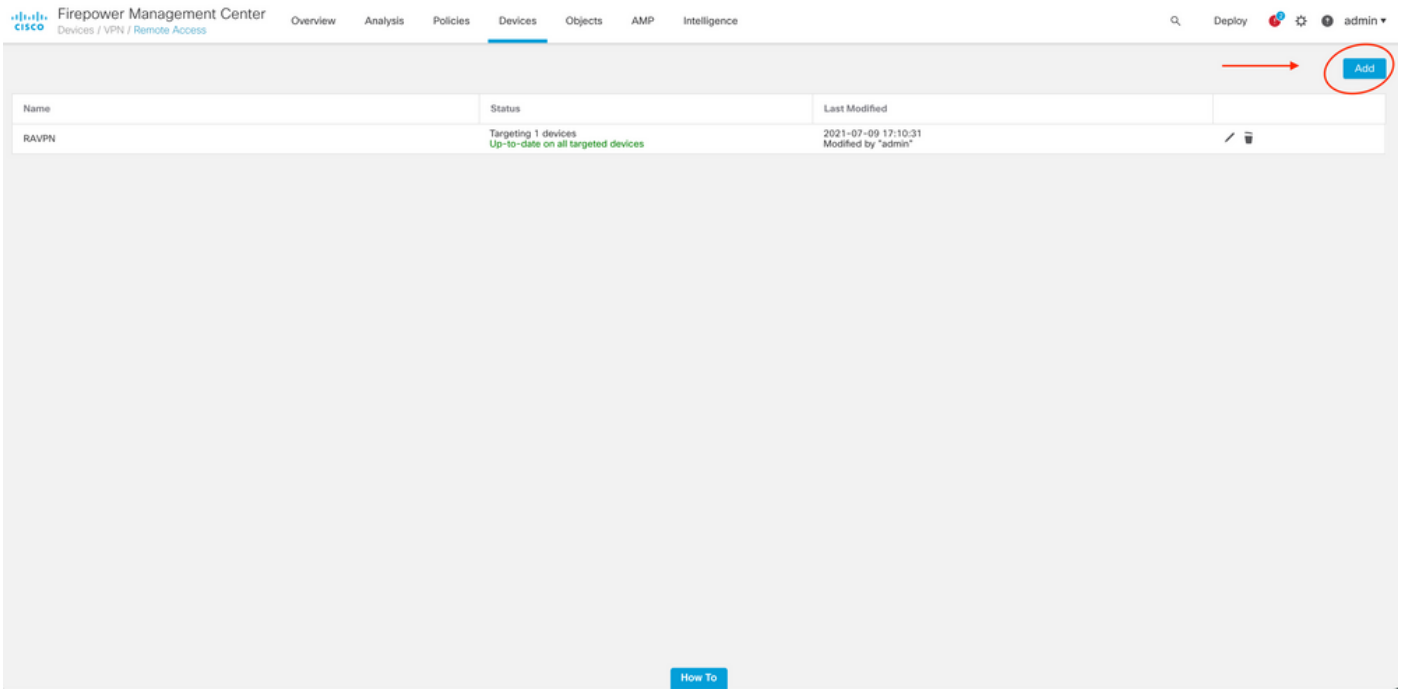
الشهادة، أختر المعرف.

تكوين Cisco AnyConnect

قم بتكوين AnyConnect عبر FMC باستخدام معالج الوصول عن بعد.

الخطوة 1. بدء تشغيل معالج نهج Remote Access VPN لتكوين AnyConnect.

انتقل إلى الأجهزة > Remote Access (الوصول عن بعد) واختر Add.

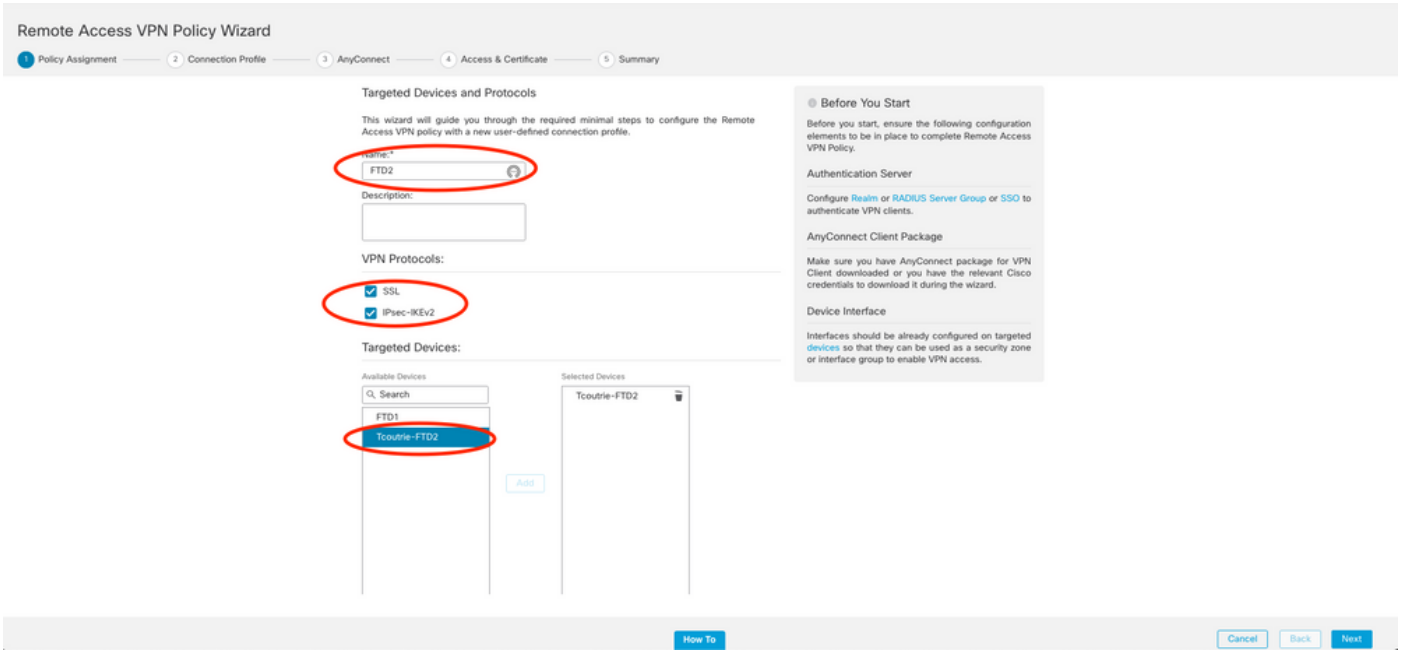


الخطوة 2. تعيين النهج.

إكمال تعيين النهج:
أ. قم بتسمية السياسة.

ب. أختر بروتوكولات VPN المطلوبة.

c. أختر الجهاز المستهدف لتطبيق التكوين.

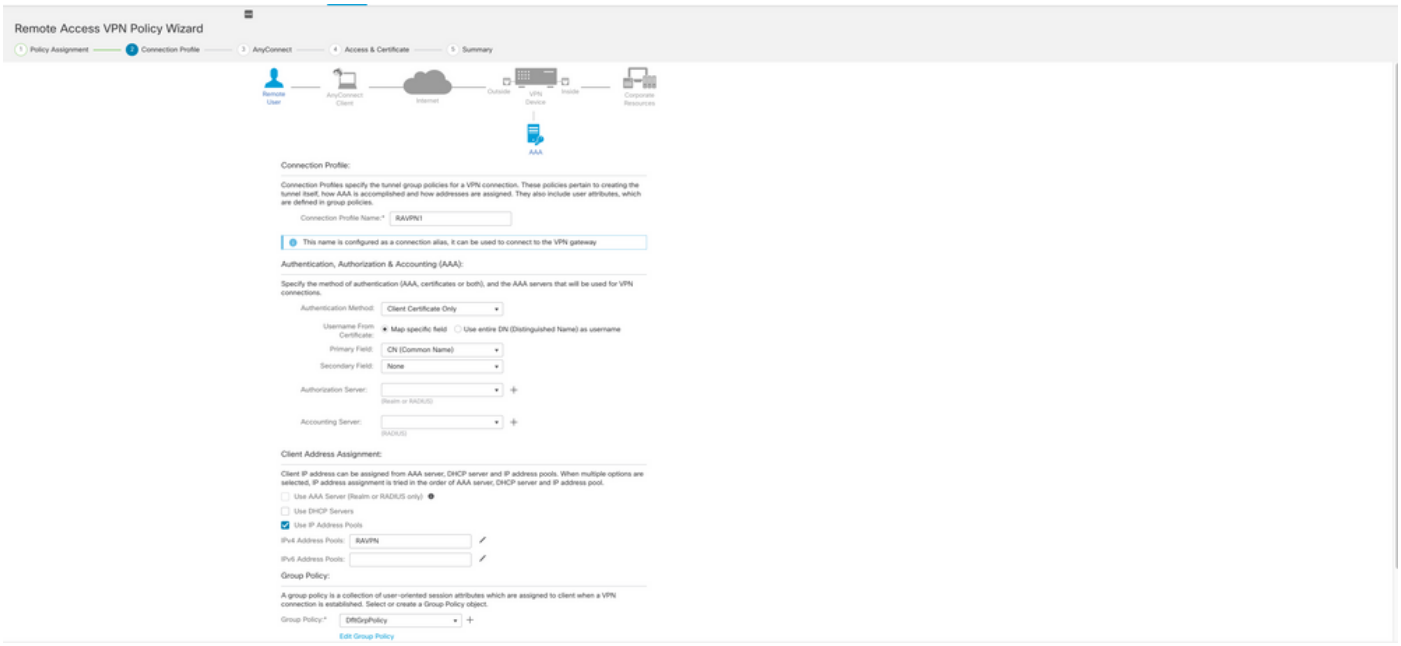


الخطوة 3. ملف تعريف الاتصال.

أ. اسم ملف تعريف الاتصال.
ب. تعيين أسلوب المصادقة على شهادة العميل فقط.

ج. قم بتعيين تجمع عناوين IP، وإذا لزم الأمر، قم بإنشاء نهج مجموعة جديد.

د. طقطقت بعد ذلك.



ملاحظة: أختر الحقل الأساسي المراد إستخدامه لإدخال اسم المستخدم لجلسات المصادقة. يستخدم CN للشهادة في هذا الدليل.

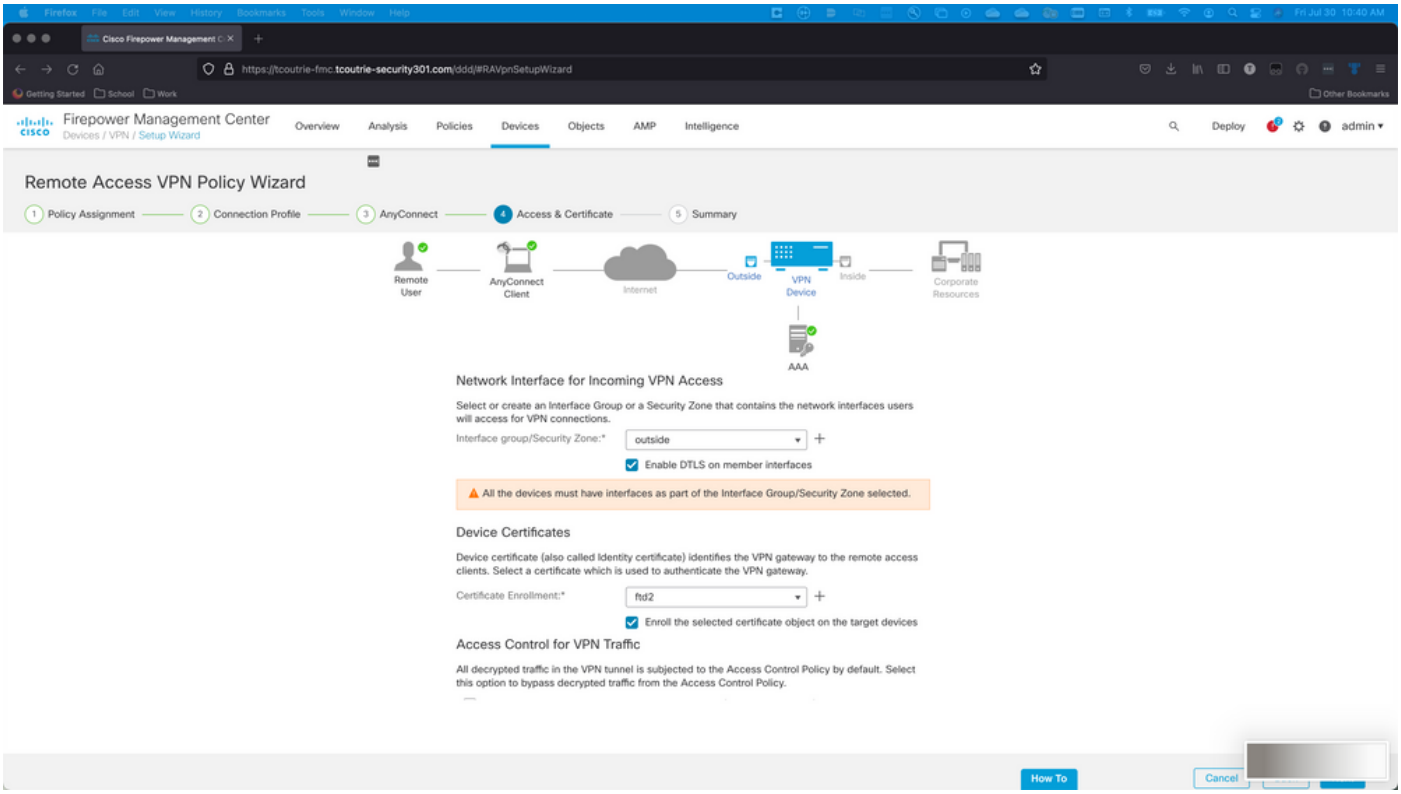
الخطوة 4. AnyConnect.

إضافة حزمة AnyConnect إلى الجهاز. قم بتحميل الإصدار المفضل من AnyConnect وانقر فوق التالي.

ملاحظة: يمكن تنزيل حزم Cisco AnyConnect من Software.cisco.com.

الخطوة 5. الوصول والشهادة.

قم بتطبيق الشهادة على واجهة وتمكين AnyConnect على مستوى الواجهة، كما هو موضح في هذه الصورة، وانقر فوق التالي.



الخطوة 6. ملخص.

راجع التكوينات. إذا تم سحب كافة عمليات السحب، انقر فوق إنهاء ثم النشر.

إنشاء شهادة لمستخدمي الأجهزة المحمولة

إنشاء شهادة إضافتها إلى الجهاز المحمول المستخدم في التوصيل.

الخطوة 1. XCA.

أ - فتح XCA

ب. بدء تشغيل قاعدة بيانات جديدة

الخطوة 2. إنشاء CSR.

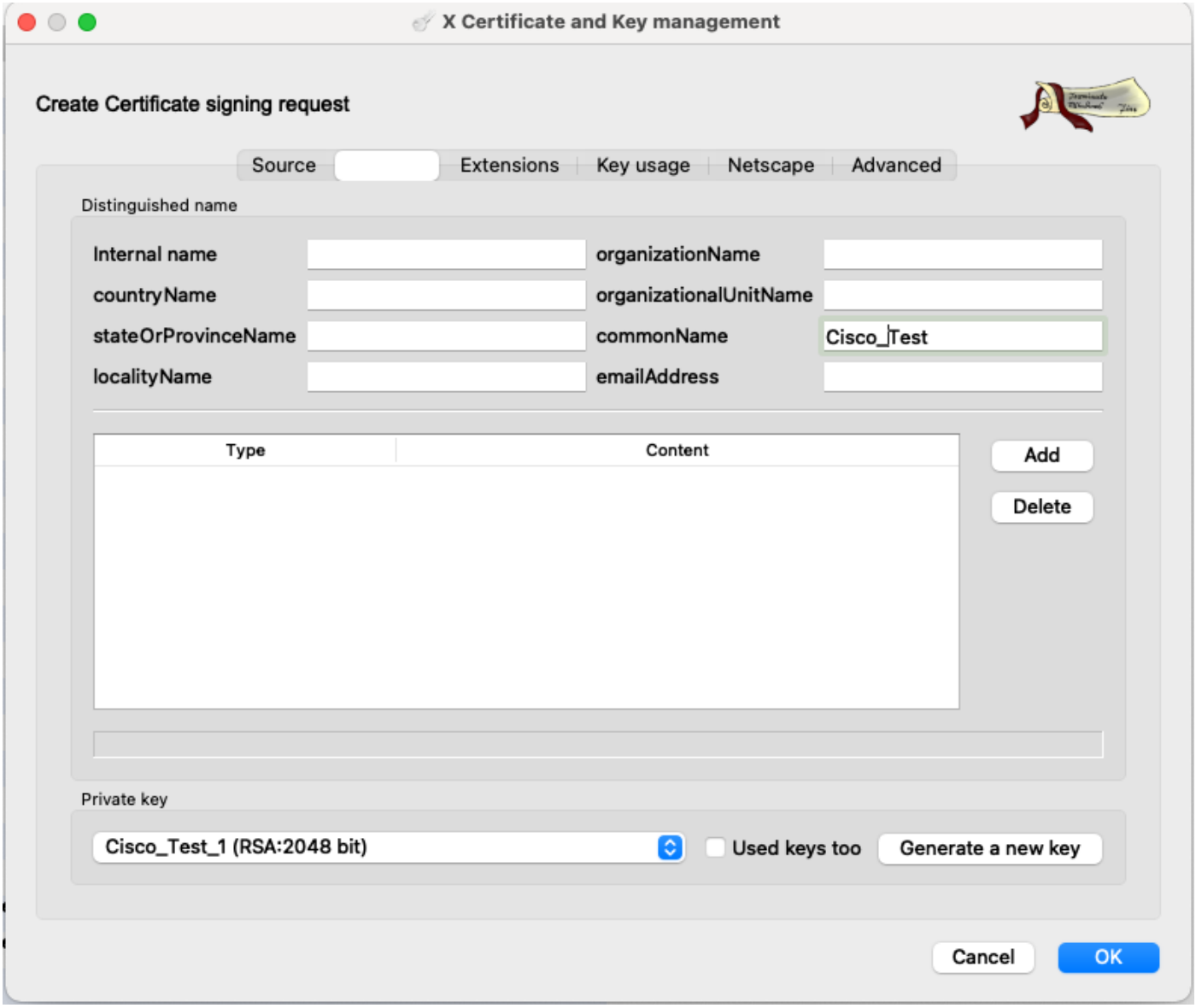
أ. أختر طلب توقيع الشهادة (CSR)

ب. إختيار طلب جديد

ج. أدخل القيمة مع كل المعلومات اللازمة للشهادة

د. إنشاء مفتاح جديد

ه. عند الانتهاء، انقر فوق موافق

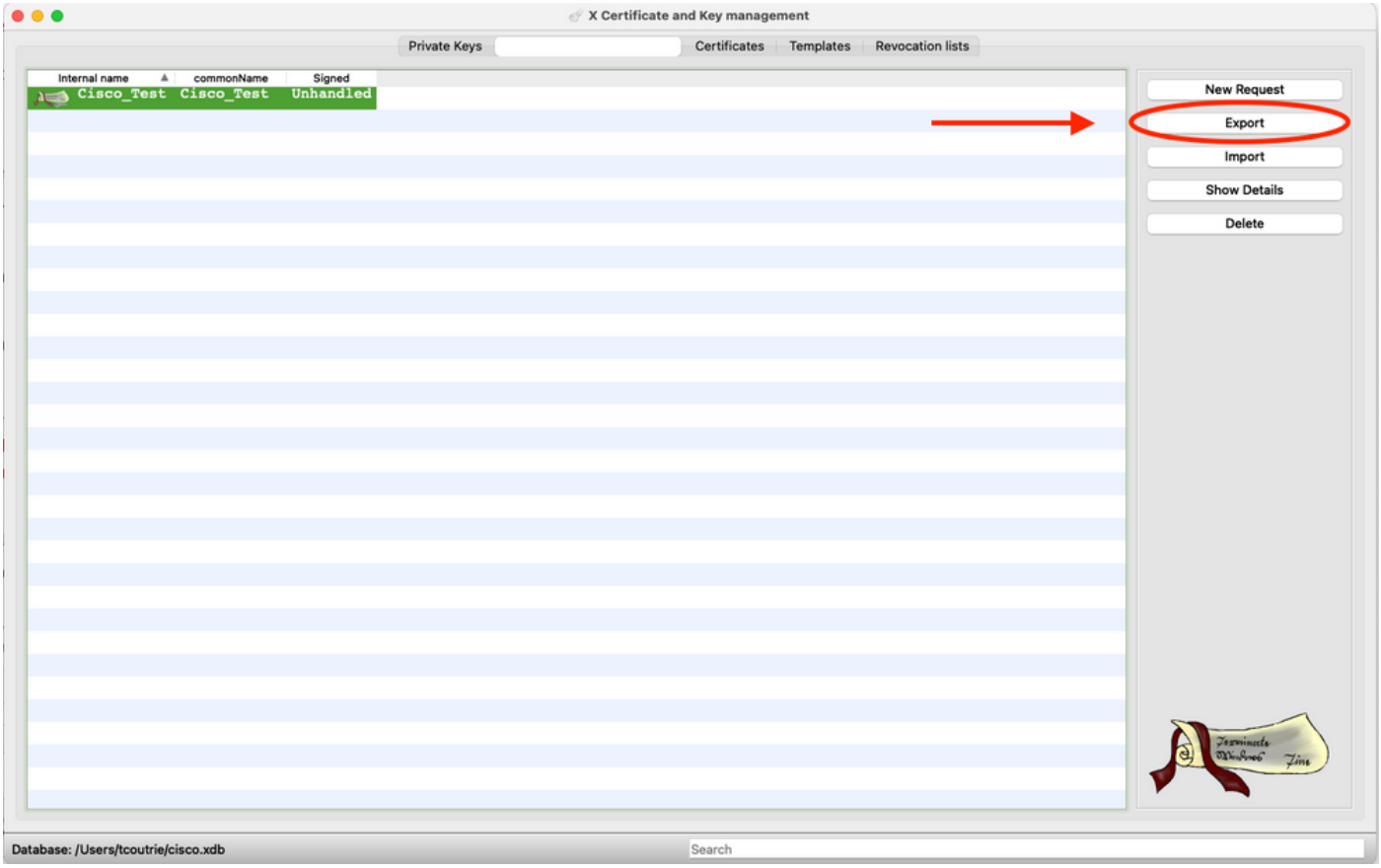


ملاحظة: يستخدم هذا المستند CN الخاص بالشهادة.

الخطوة 3. إرسال CSR.

أ - تصدير المسؤولية الاجتماعية للشركات

ب. تقديم CSR إلى CA للحصول على شهادة جديدة

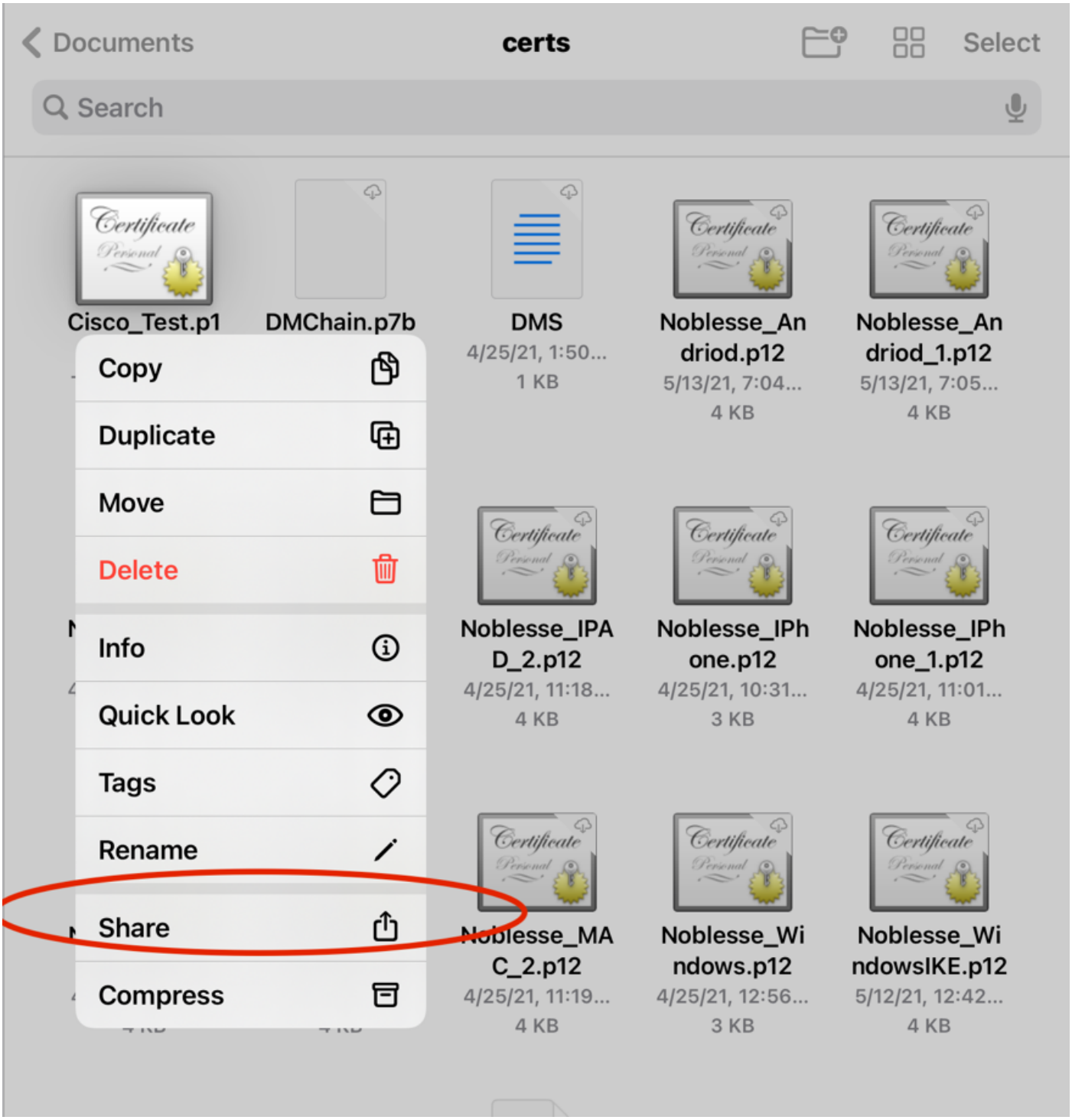


ملاحظة: أستخدم تنسيق PEM الخاص ب CSR.

التثبيت على الجهاز المحمول

الخطوة 1. إضافة شهادة الجهاز إلى الجهاز المحمول.
الخطوة 2. شارك الشهادة مع تطبيق AnyConnect لإضافة تطبيق الشهادة الجديد.

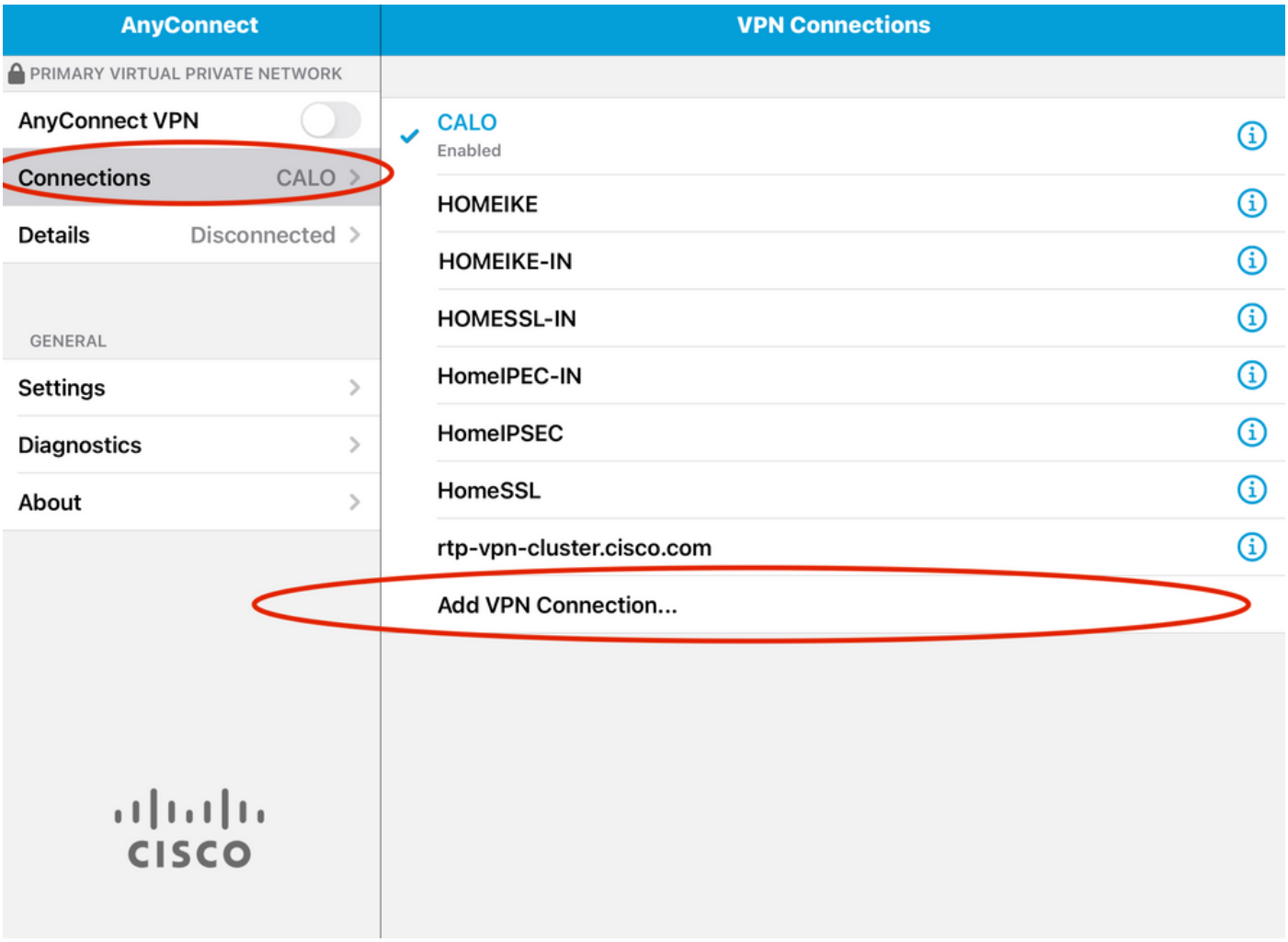
تحذير: يتطلب التثبيت اليدوي من المستخدم مشاركة الشهادة مع التطبيق. لا ينطبق هذا على الشهادات التي يتم دفعها عبر MDMs.



الخطوة 3. أدخل كلمة مرور الشهادة لملف PKCS12.

الخطوة 4. إنشاء اتصال جديد على AnyConnect.

الخطوة 5. انتقل إلى إتصالات جديدة؛ إتصالات > إضافة اتصال VPN.



الخطوة 6. أدخل معلومات الاتصال الجديد.

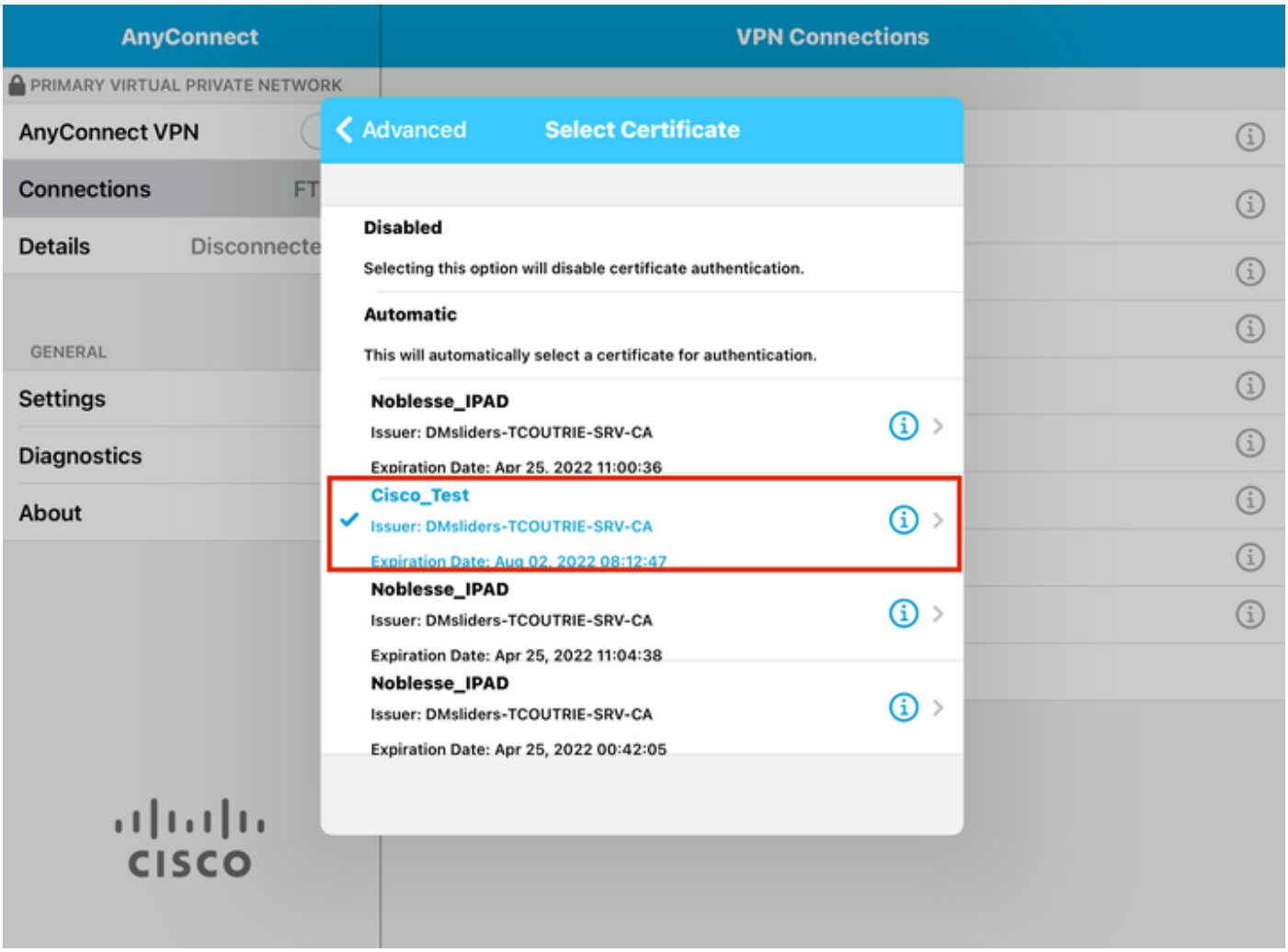
الوصف: تسمية الاتصال

عنوان الخادم: عنوان IP أو FQDN الخاص ب FTD

متقدم: تكوينات إضافية

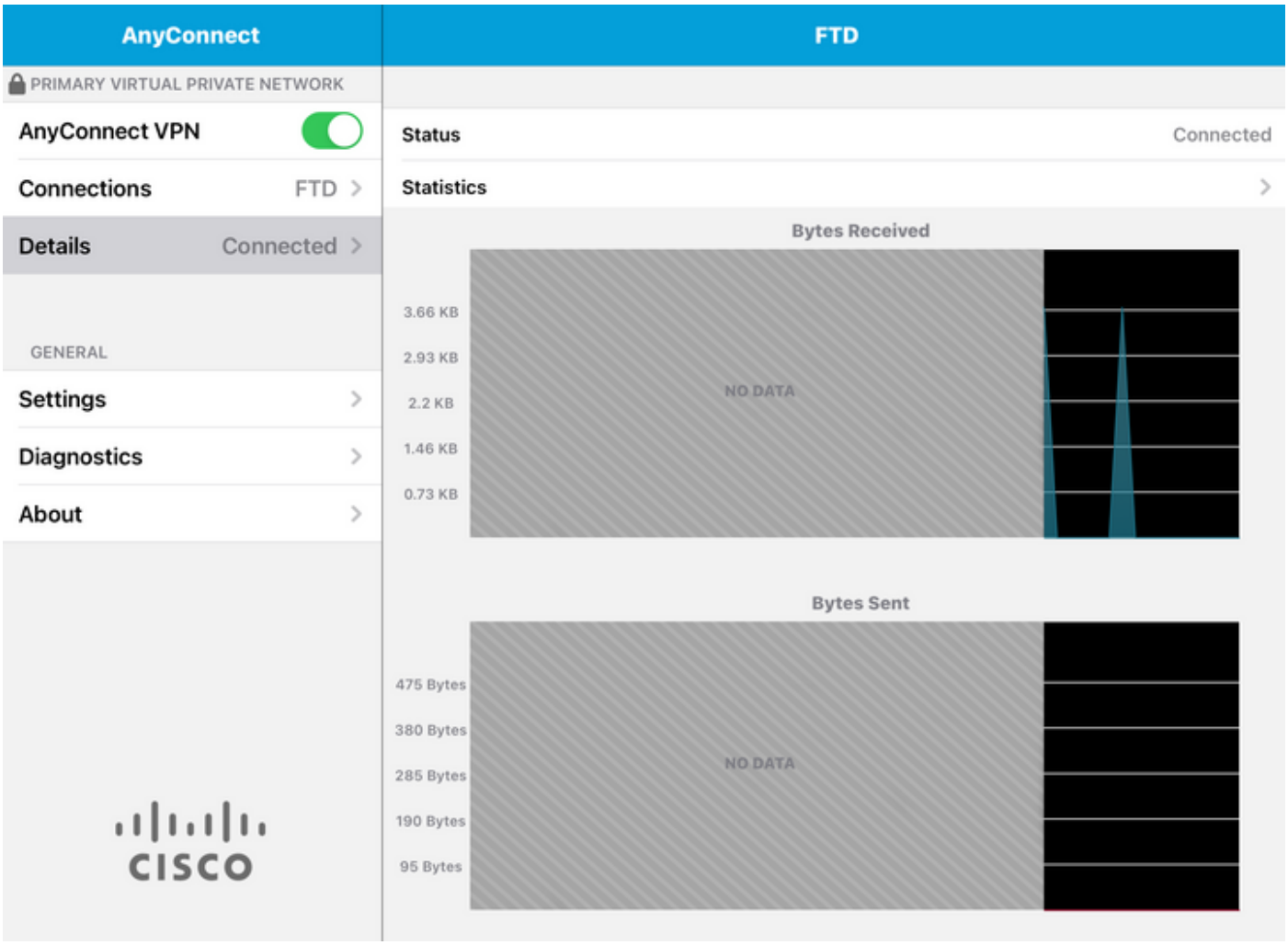
الخطوة 7. أختر متقدم.

الخطوة 8. أختر ترخيص واختر شهادتك التي تمت إضافتها حديثا.



الخطوة 9. قم بالانتقال مرة أخرى إلى الاتصالات والاختبار.

بمجرد نجاح التبديل، يبقى التبديل قيد التشغيل وتظهر التفاصيل متصلا في الحالة.



التحقق من الصحة

يعرض الأمر show vpn-sessionDB detail AnyConnect جميع المعلومات حول المضيف المتصل.

تلميح: الخيار لتصفية هذا الأمر أكثر هو كلمات البحث 'filter' أو 'sort' التي تمت إضافتها إلى الأمر.

على سبيل المثال:

```
Tcoutrie-FTD3# show vpn-sessiondb detail Anyconnect


Username : Cisco_Test Index : 23
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Protocol : Anyconnect-Parent SSL-Tunnel DTLS-Tunnel
License : Anyconnect Premium, Anyconnect for Mobile
Encryption : Anyconnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hash : Anyconnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 8627 Bytes Rx : 220
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : SSL Tunnel Group : SSL
Login Time : 13:03:28 UTC Mon Aug 2 2021
```

```
Duration : 0h:01m:49s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a7aa95d000170006107ed20
Security Grp : none Tunnel Zone : 0

Anyconnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Anyconnect-Parent:
Tunnel ID : 23.1
Public IP : 10.118.18.168
Encryption : none Hashing : none
TCP Src Port : 64983 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : apple-ios
Client OS Ver: 14.6
Client Type : Anyconnect
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 6299 Bytes Rx : 220
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 23.2
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 64985
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Apple iOS
Client Type : SSL VPN Client
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 2328 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 23.3
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 51003
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Apple iOS
Client Type : DTLS VPN Client
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

استكشاف الأخطاء وإصلاحها

تصحيح الأخطاء

التصحيح المطلوب لاستكشاف أخطاء هذه المشكلة وإصلاحها هو:

```
Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255
```

إذا كان الاتصال هو IPsec وليس SSL:

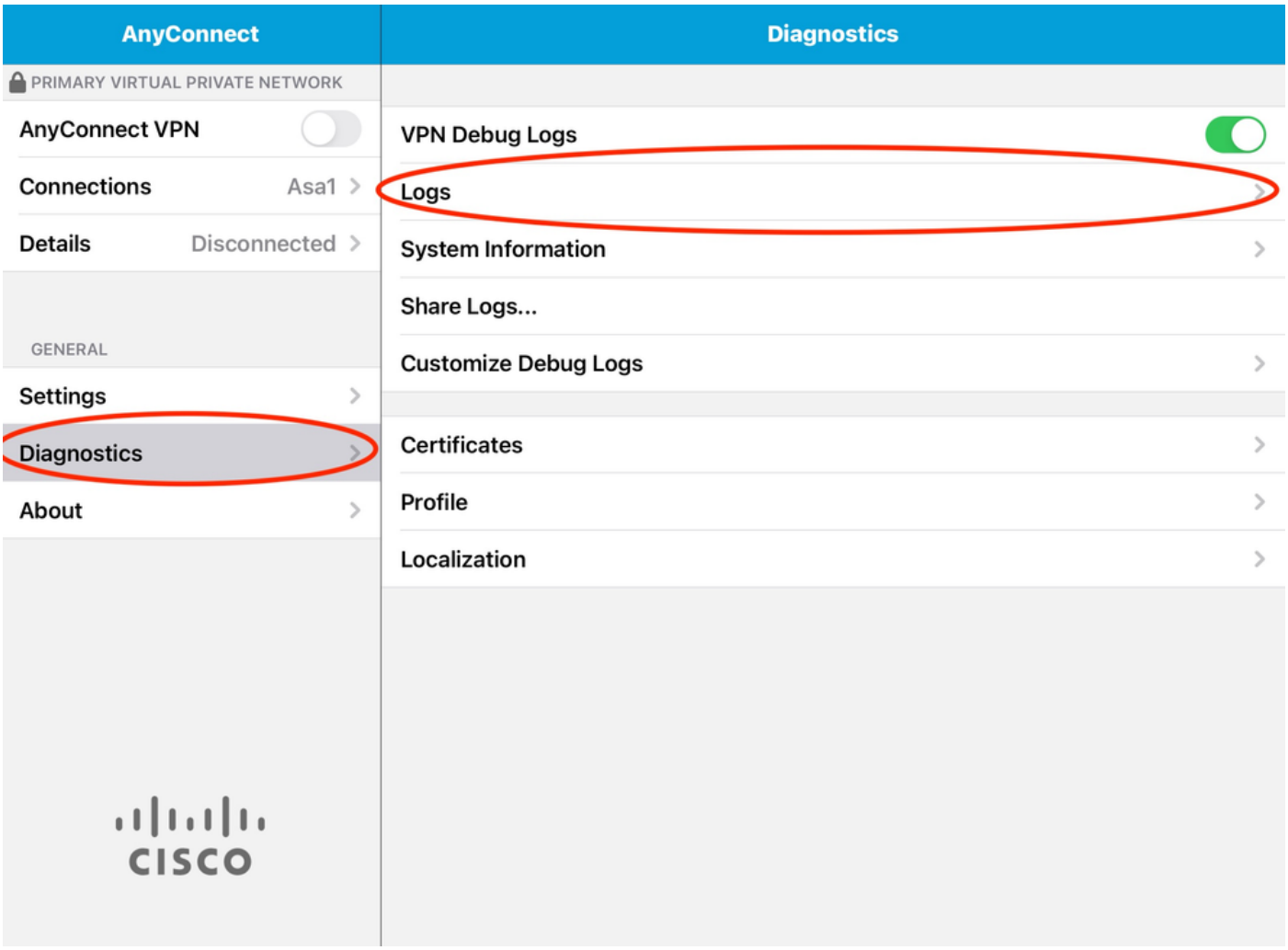
```
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14
```

السجلات من تطبيق AnyConnect للأجهزة المحمولة:

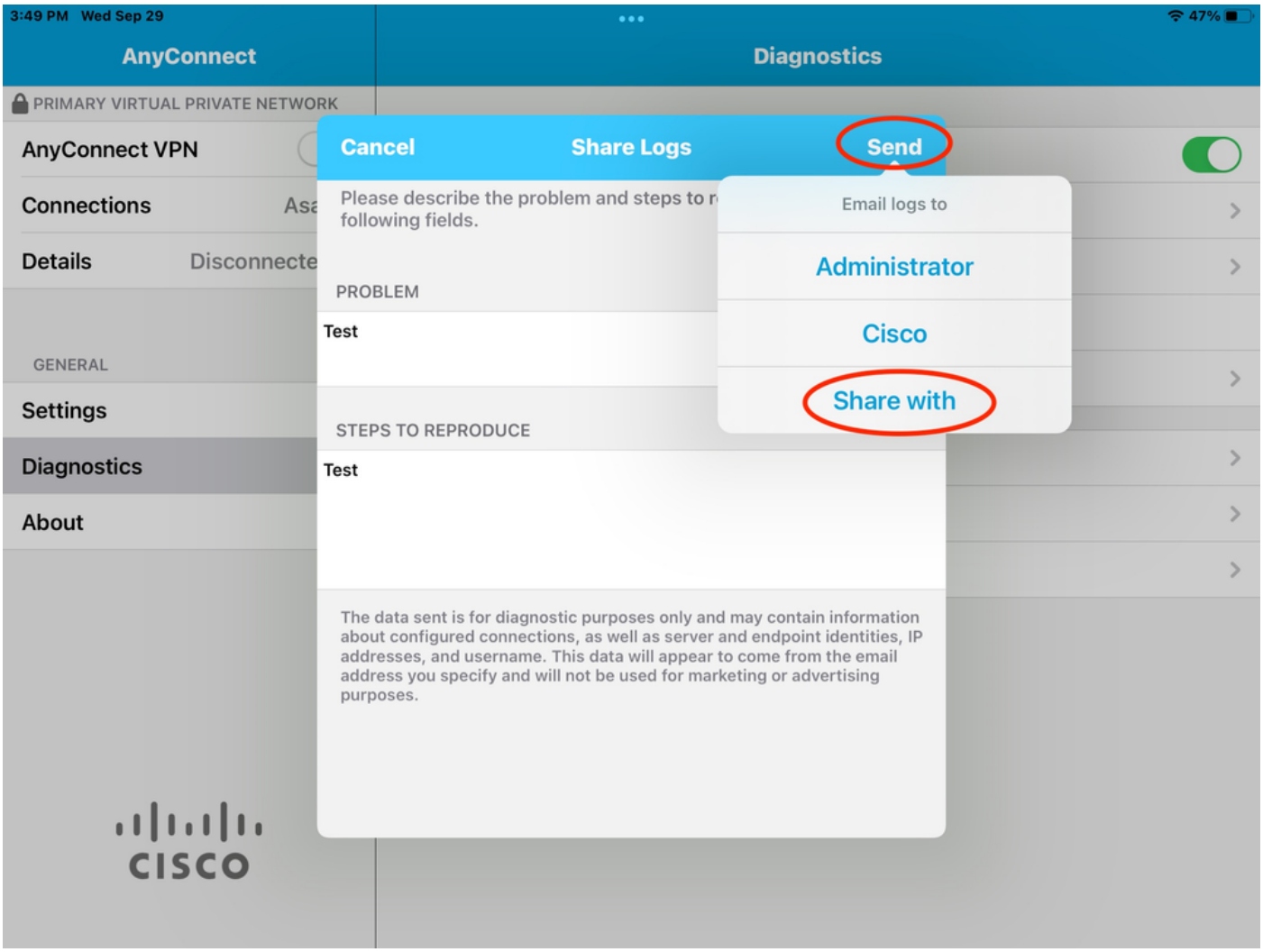
انتقل إلى التشخيص > سجلات تصحيح أخطاء VPN > مشاركة السجلات.



أدخل المعلومات:

- المشكلة
- خطوات للتكاثر

ثم انتقل إلى إرسال > مشاركة مع.



وهذا يقدم خيار إستخدام عميل بريد إلكتروني لإرسال السجلات.

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).