

ةداهش ىلع لوصحلل VPN 3.x ليمع نيوكت ةيمقر

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [تكوين عميل VPN](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

[المقدمة](#)

يوضح هذا المستند كيفية تكوين عميل Cisco VPN 3.x للحصول على شهادة رقمية.

[المتطلبات الأساسية](#)

[المتطلبات](#)

لا توجد متطلبات خاصة لهذا المستند.

[المكونات المستخدمة](#)

تستند المعلومات الواردة في هذا المستند إلى كمبيوتر شخصي يشغل عميل Cisco VPN 3.x.

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

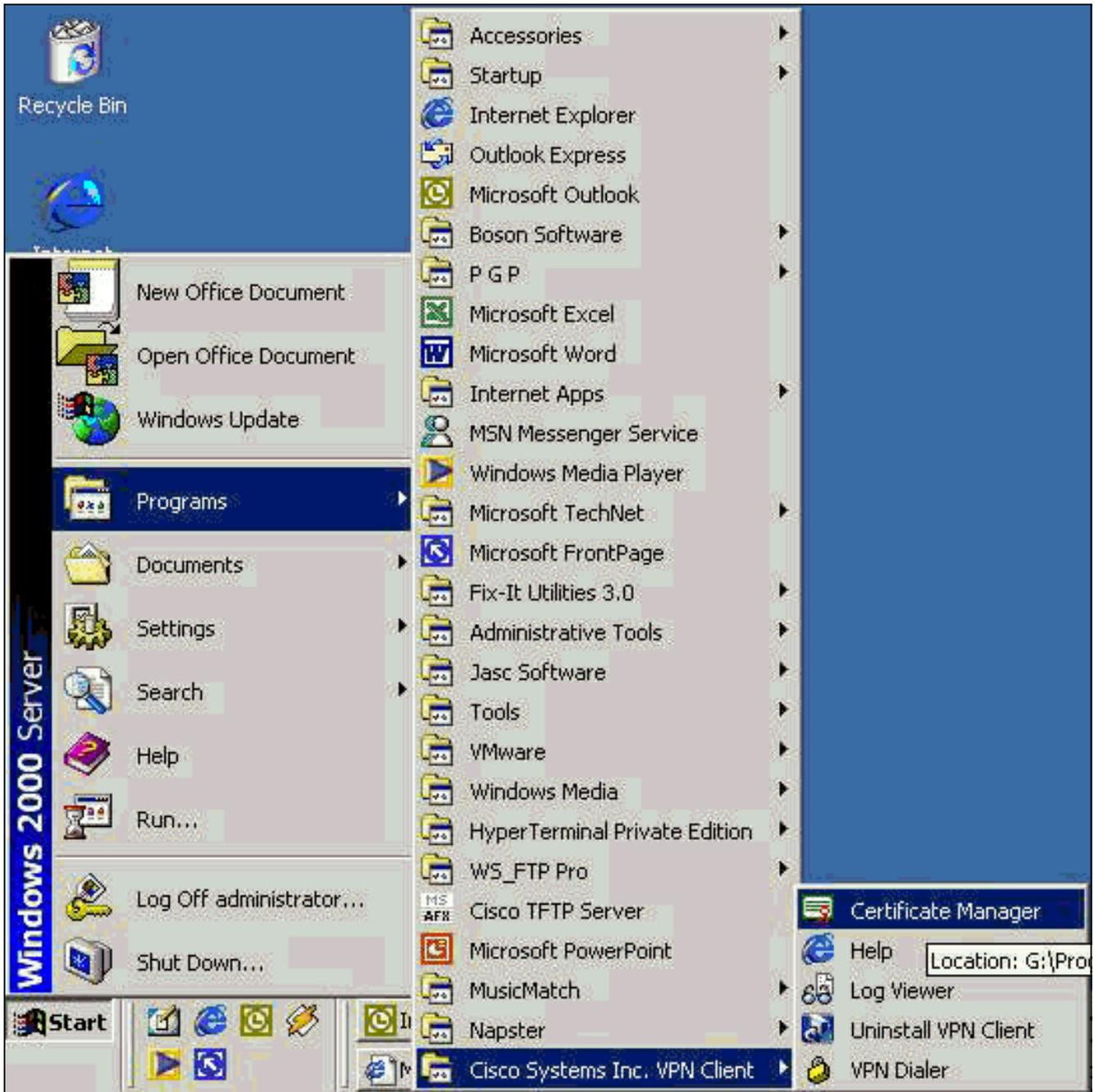
[الاصطلاحات](#)

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

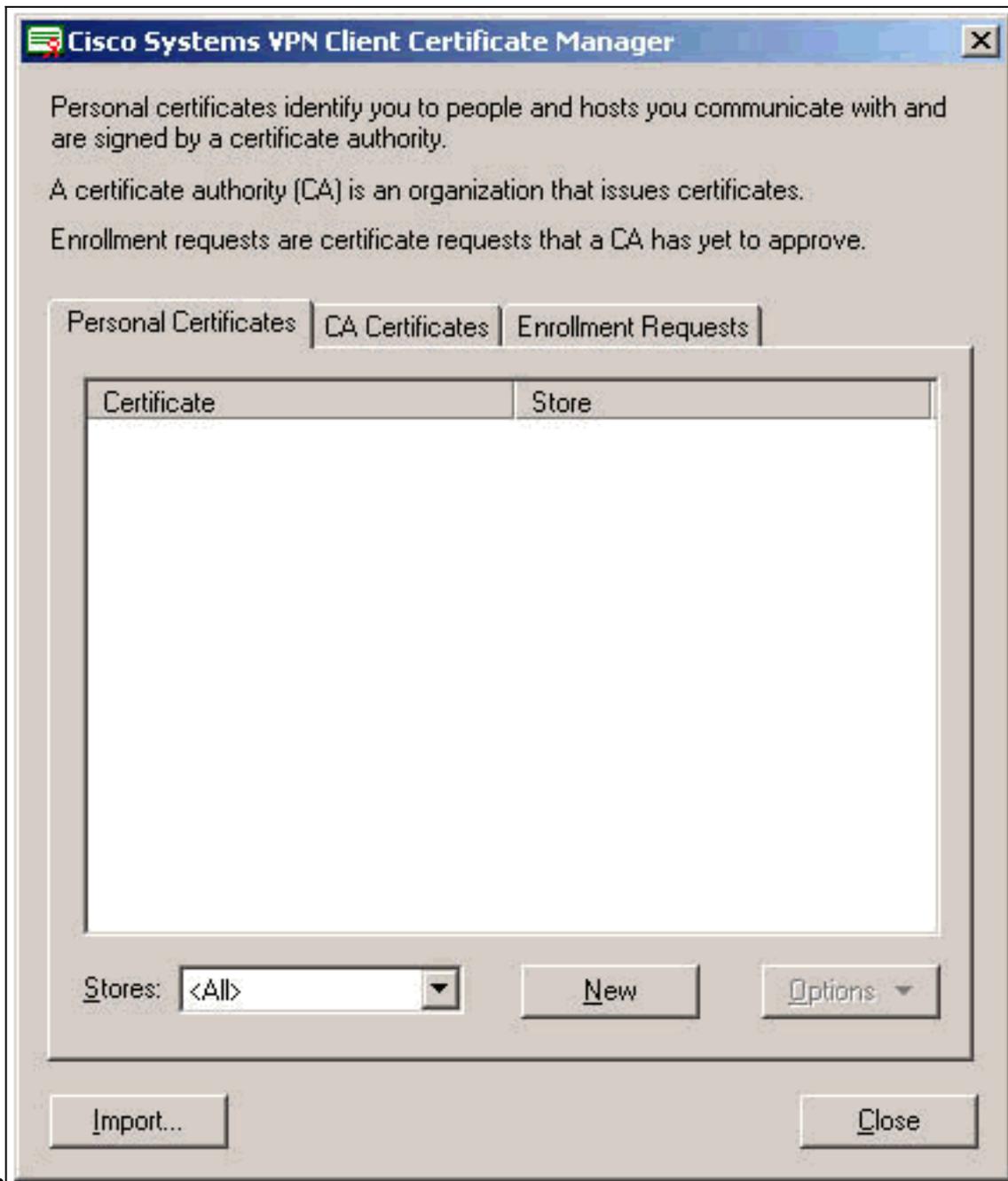
[تكوين عميل VPN](#)

أكمل هذه الخطوات لتكوين عميل شبكة VPN.

1. حدد بداية <برامج> Cisco Systems Inc. VPN Client <مدير الشهادات لتشغيل مدير شهادات عميل شبكة .VPN>



2. حدد علامة التبويب شهادات شخصية وانقر فوق



ملاحظة:

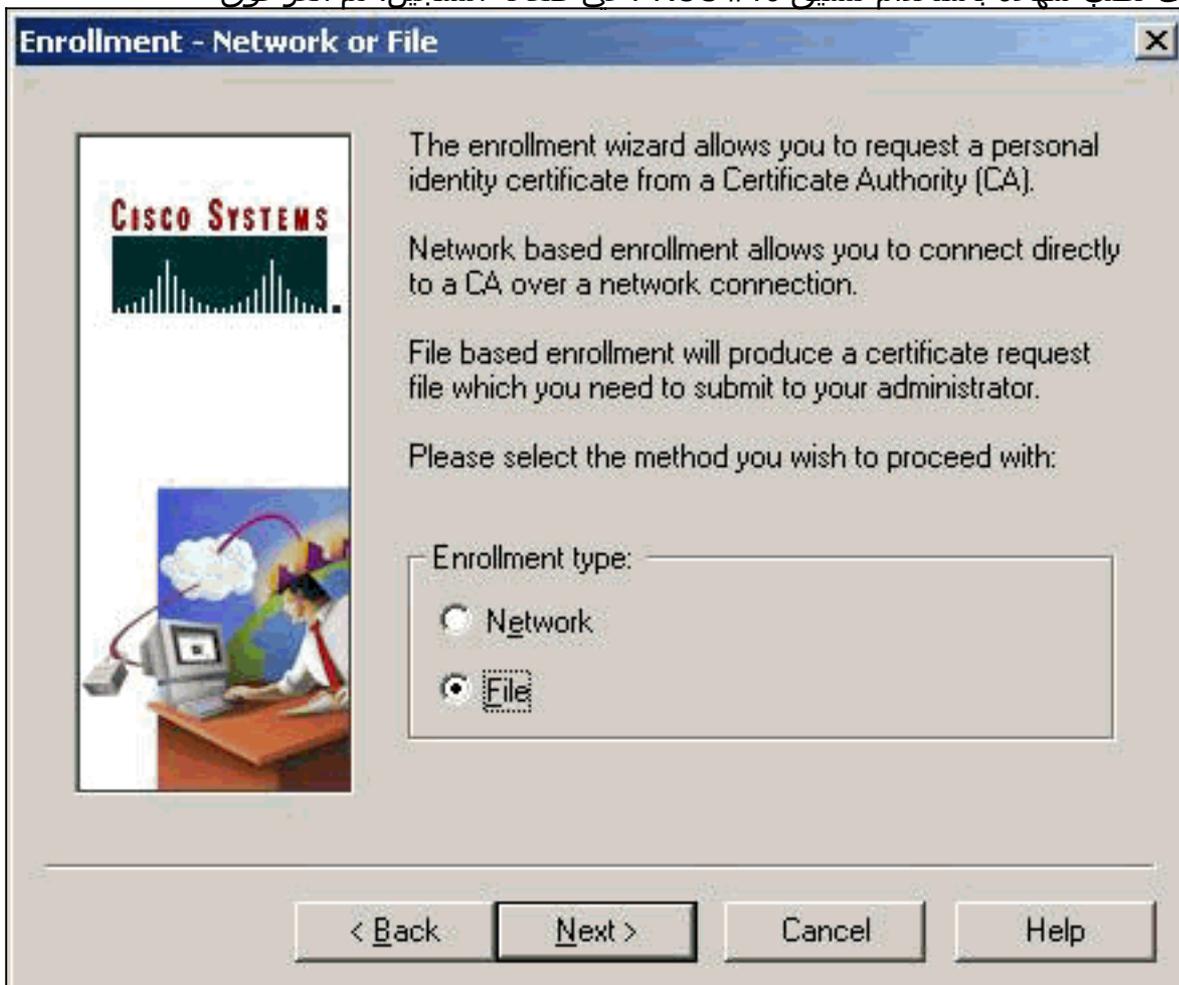
جديد.

لا يمكن إجراء شهادات الجهاز لمصادقة المستخدمين لاتصالات VPN باستخدام IPsec. 3. عندما يطلب منك عميل VPN كلمة مرور، حدد كلمة مرور لحماية الشهادة. تتطلب أي عملية تتطلب الوصول إلى المفتاح الخاص للشهادة إستمرار كلمة المرور



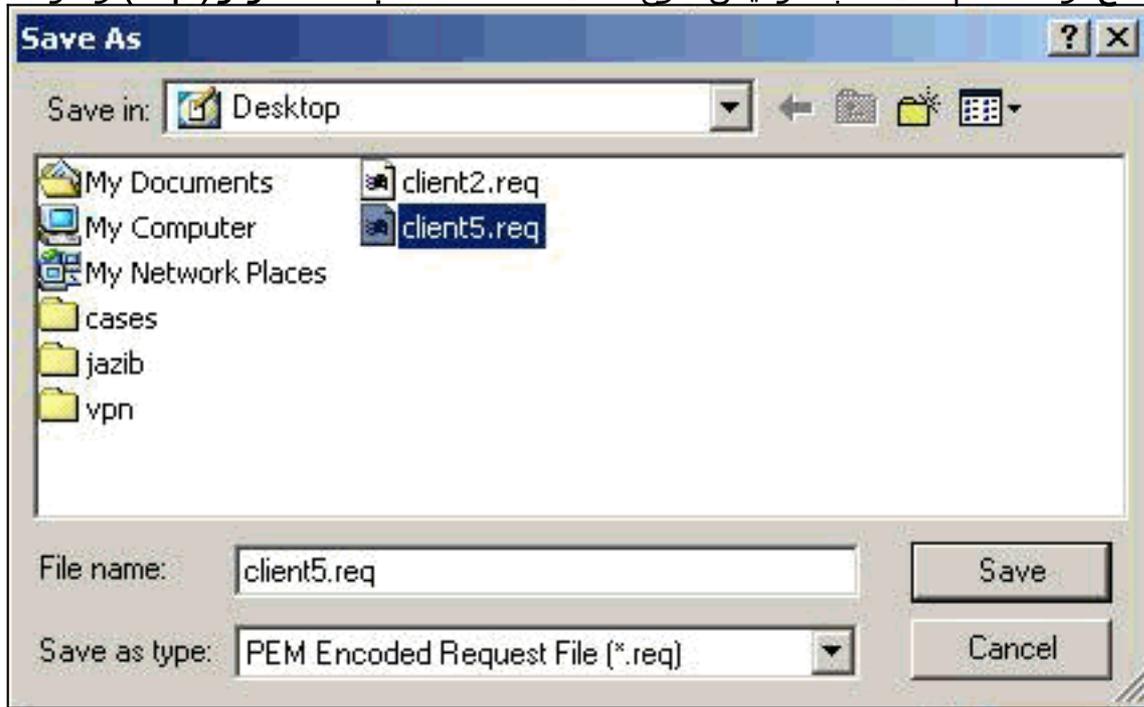
المحددة.

4. حدد ملف لطلب شهادة باستخدام تنسيق PKCS #10 في صفحة التسجيل. ثم انقر فوق



التالي.

5. انقر تصفح، وحدد اسم ملف طلب الترخيص. لنوع الملف، حدد ملف طلب PEM مرمرز (req.*) وانقر



حفظ

6. انقر فوق التالي في صفحة تسجيل عميل شبكة



VPN

7. املأ الحقول الموجودة في نموذج التسجيل. يوضح هذا المثال الحقول: الاسم الشائع = user1 الإدارة = IPSECERT (يجب أن يتطابق هذا مع الوحدة التنظيمية (OU) واسم المجموعة على مركز VPN الشركة = Cisco Systems الولاية = كارولينا الشمالية البلد = الولايات المتحدة البريد الإلكتروني = 3000@user1.com عنوان IP = (إختياري، يستخدم لتحديد عنوان IP في طلب الشهادة) المجال = cisco.com طقطقت بعد ذلك عندما أنت

Enrollment - Form

Enter your certificate enrollment information in the fields provided below.




Common Name (cn):* User1
DePARTMENT (ou): IPSECCERT
Company (o): Cisco Systems
State (st): NorthCarolina
Country (c): US
Email (e): User1@email.com
IP Address:
Domain: cisco.com

* Required Field

< Back Next > Cancel Help

إنتهيت.
8. انقر فوق إنهاء لمتابعة

Enrollment - Summary

This is a summary of the information you have provided for this certificate enrollment request.

Select Finish to proceed with the enrollment or Back to make modifications.

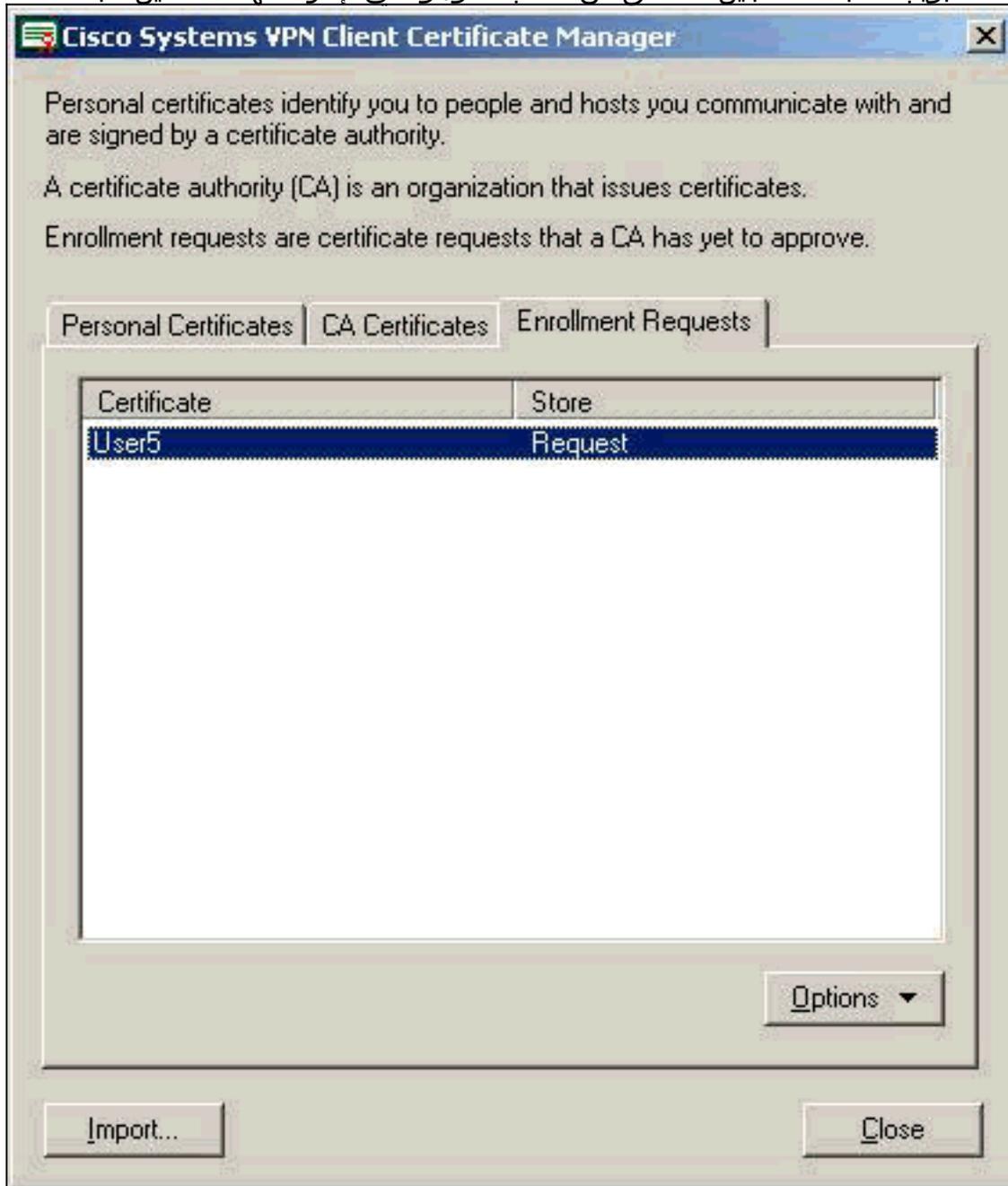



Enrollment: File - client5.req
Certificate Store: Cisco
Common Name: User1
Department: IPSECCERT
Company: Cisco Systems
State: NorthCarolina
Country: US
Email: User1@email.com
IP Address:
Domain: cisco.com

< Back Finish Cancel Help

التسجيل

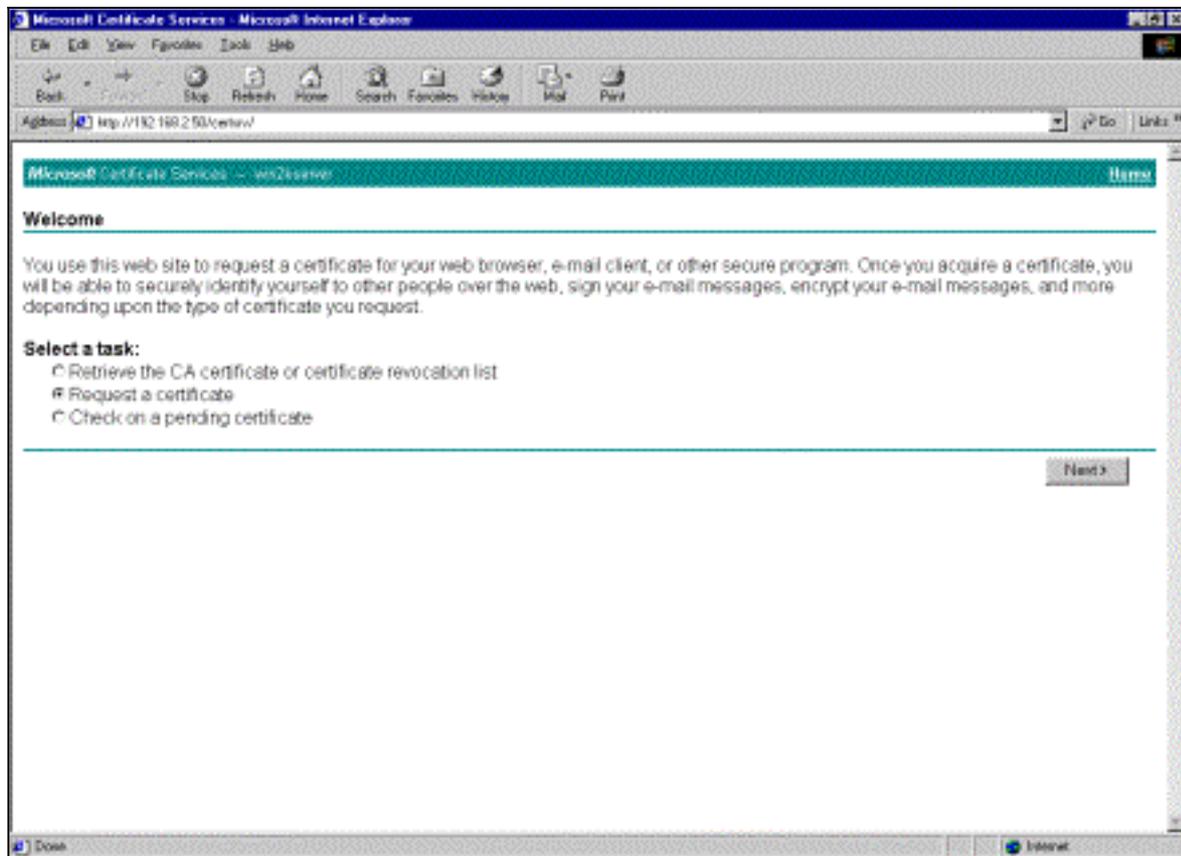
9. حدد علامة التبويب "طلبات التسجيل" للتحقق من الطلب الموجود في "إدارة شهادات عميل شبكة



"VPN

10. قم بإحضار خادم المرجع المصدق (CA) وواجهات عميل شبكة VPN في آن واحد لإرسال الطلب.

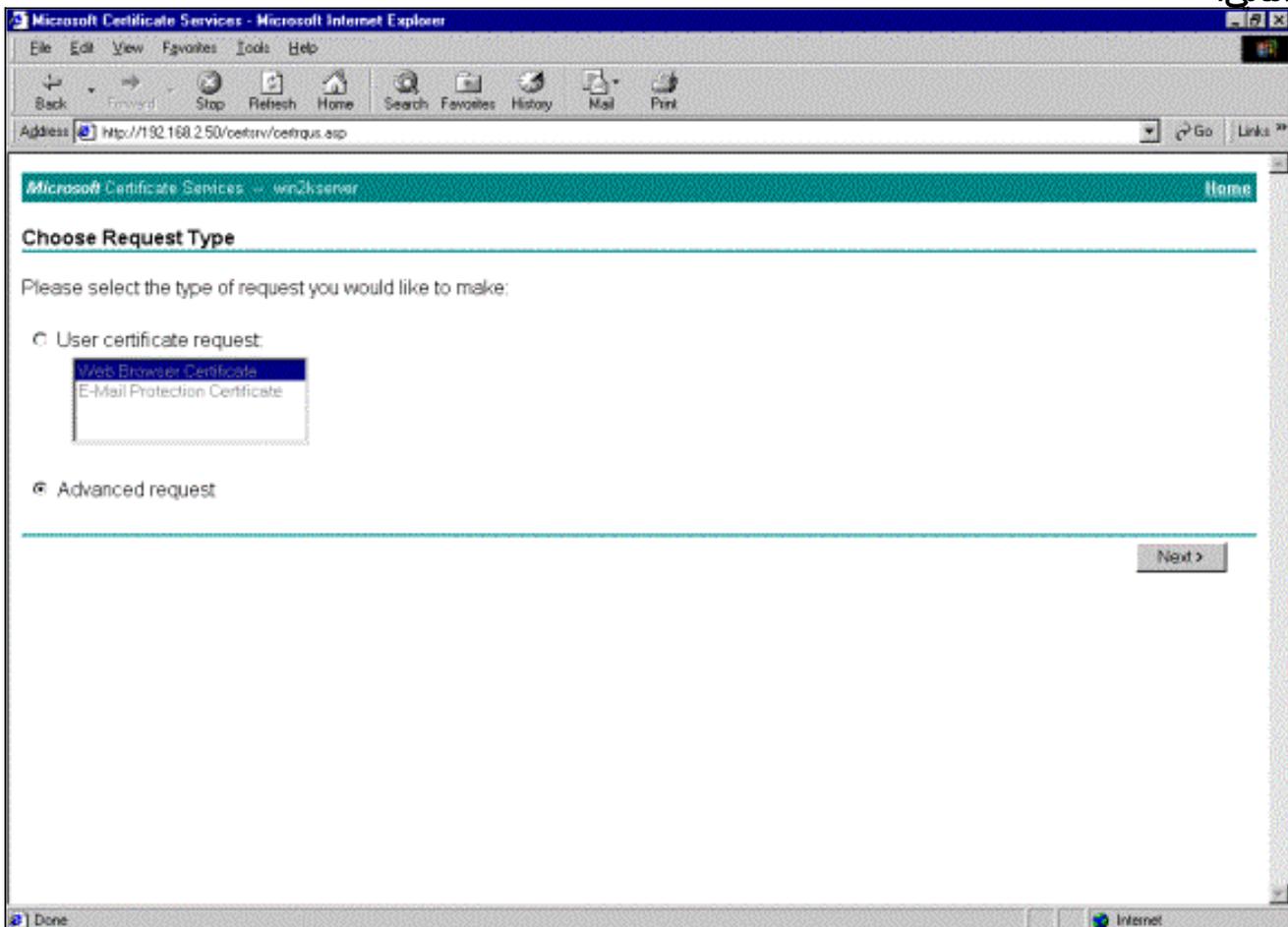
11. حدد طلب شهادة وانقر التالي على خادم



CA

12. حدد طلب متقدم لنوع الطلب وانقر

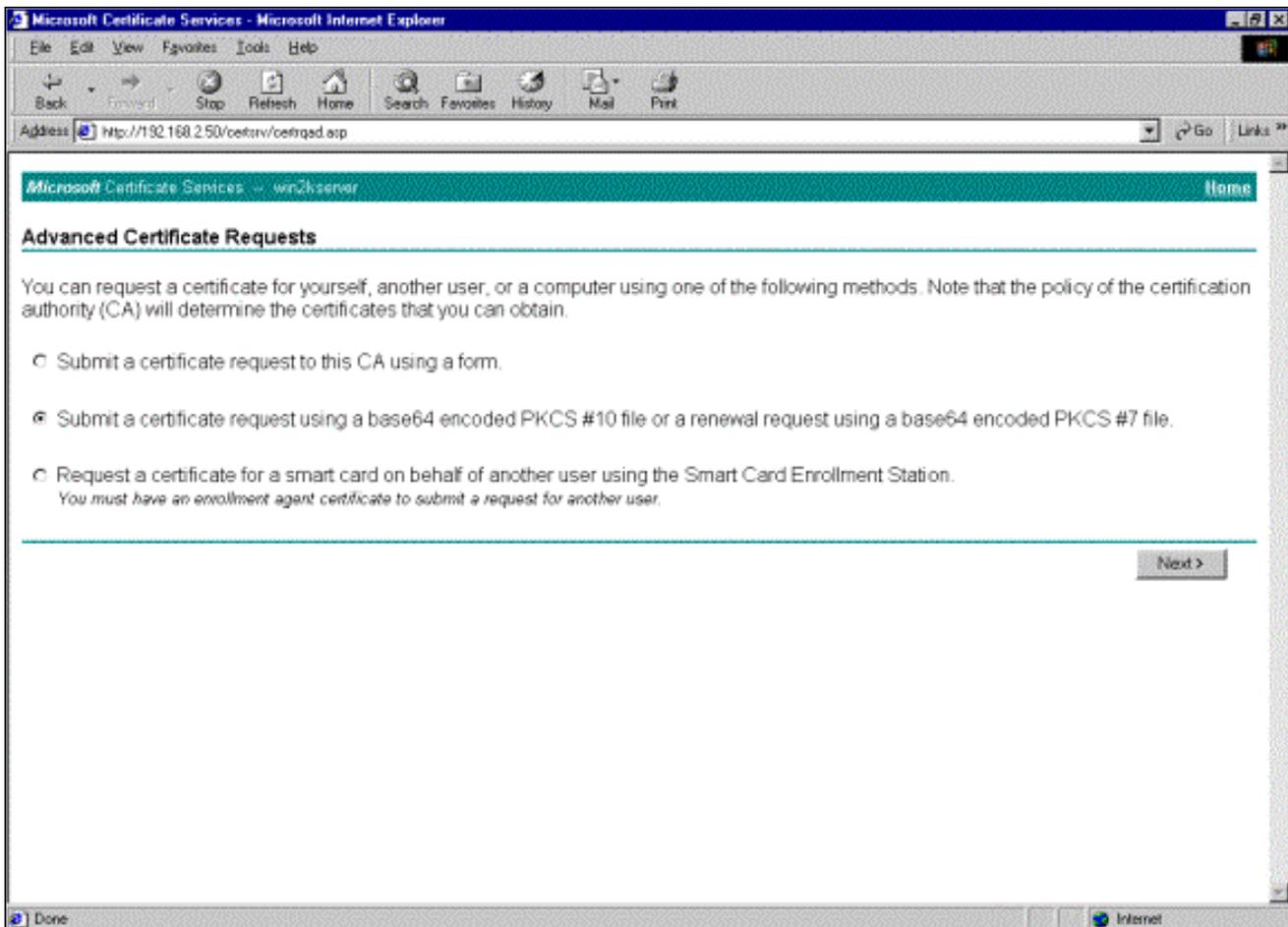
التالي.



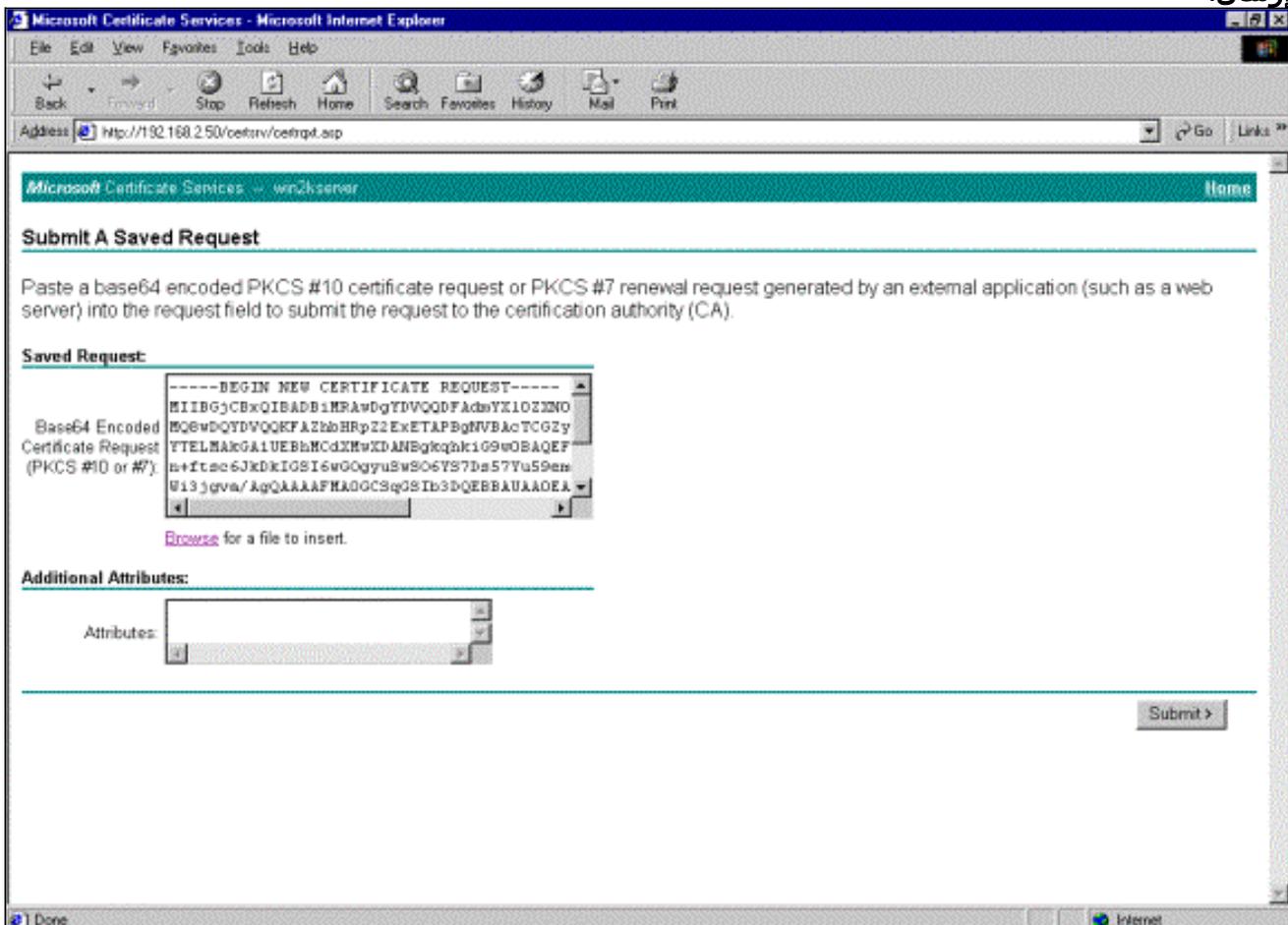
13. حدد إرسال طلب شهادة باستخدام ملف #10 PKCS رمز للأساس 64 أو طلب تجديد باستخدام ملف PKCS

#7 رمز للأساس 64 تحت طلبات شهادات متقدمة، ثم انقر

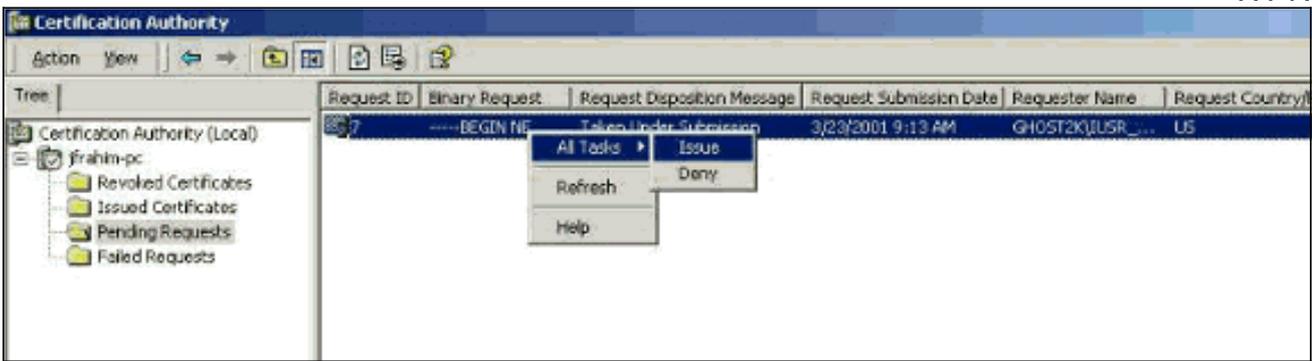
التالي.



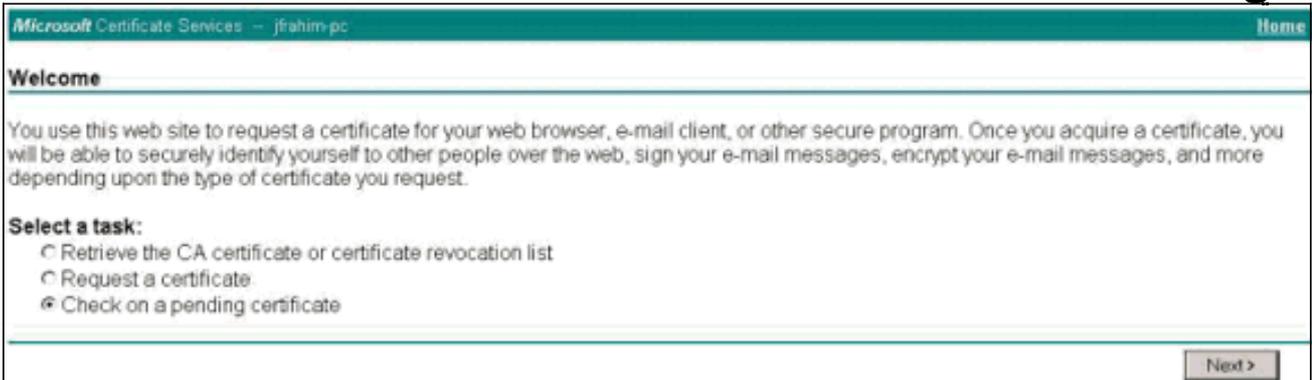
14. قم بتمييز ملف طلب عميل شبكة VPN، ولصقه في خادم CA ضمن "الطلب المحفوظ". ثم انقر فوق إرسال.



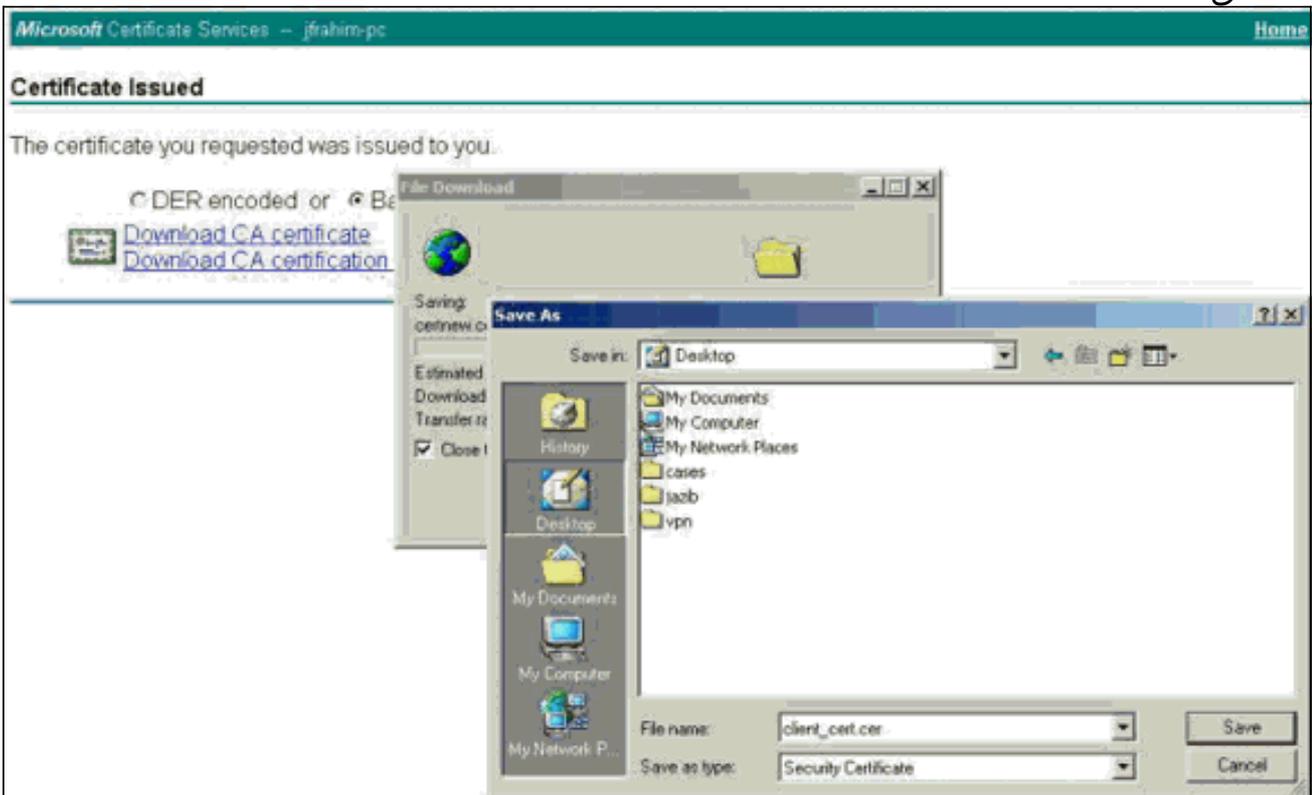
15. على خادم CA، قم بإصدار شهادة الهوية الخاصة بطلب عميل



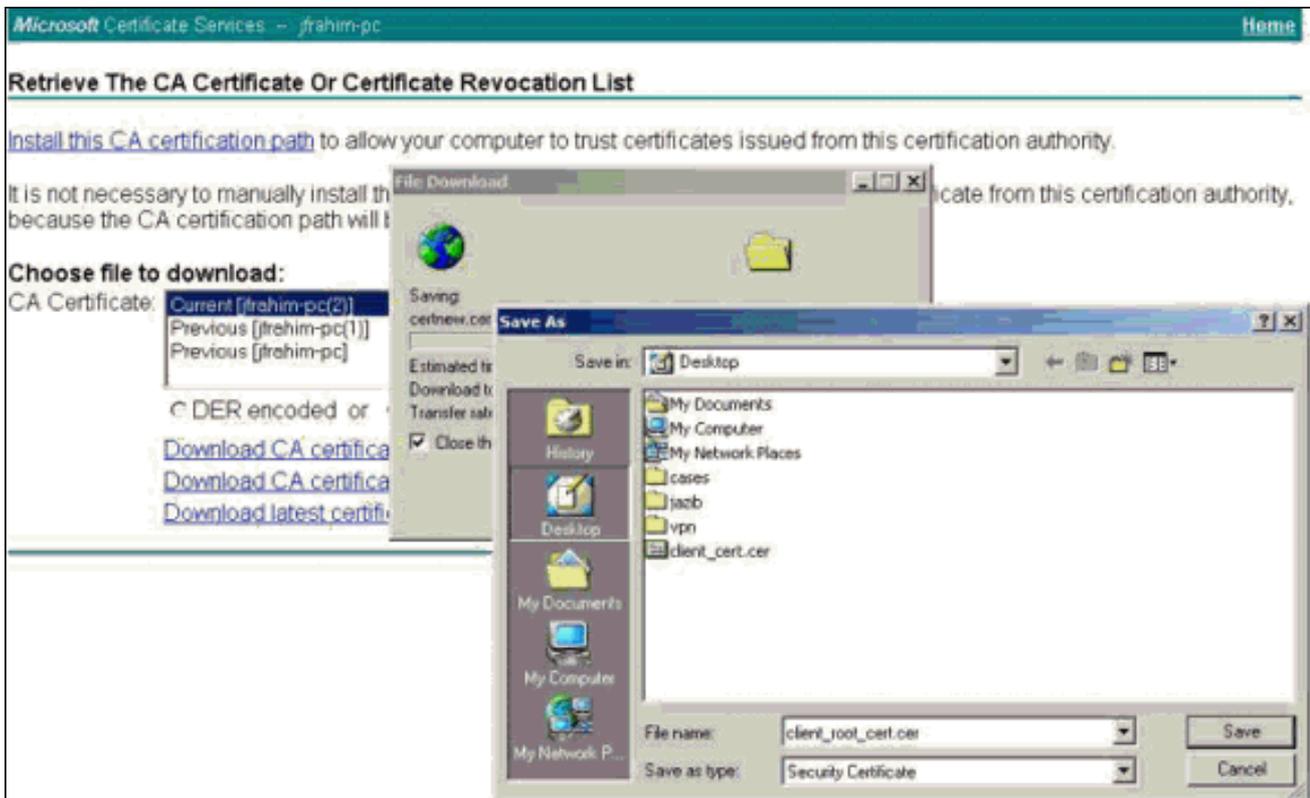
16. قم بتنزيل شهادات الجذر والهوية إلى عميل VPN. على خادم CA، حدد التحقق من شهادة معلقة، ثم انقر التالي.



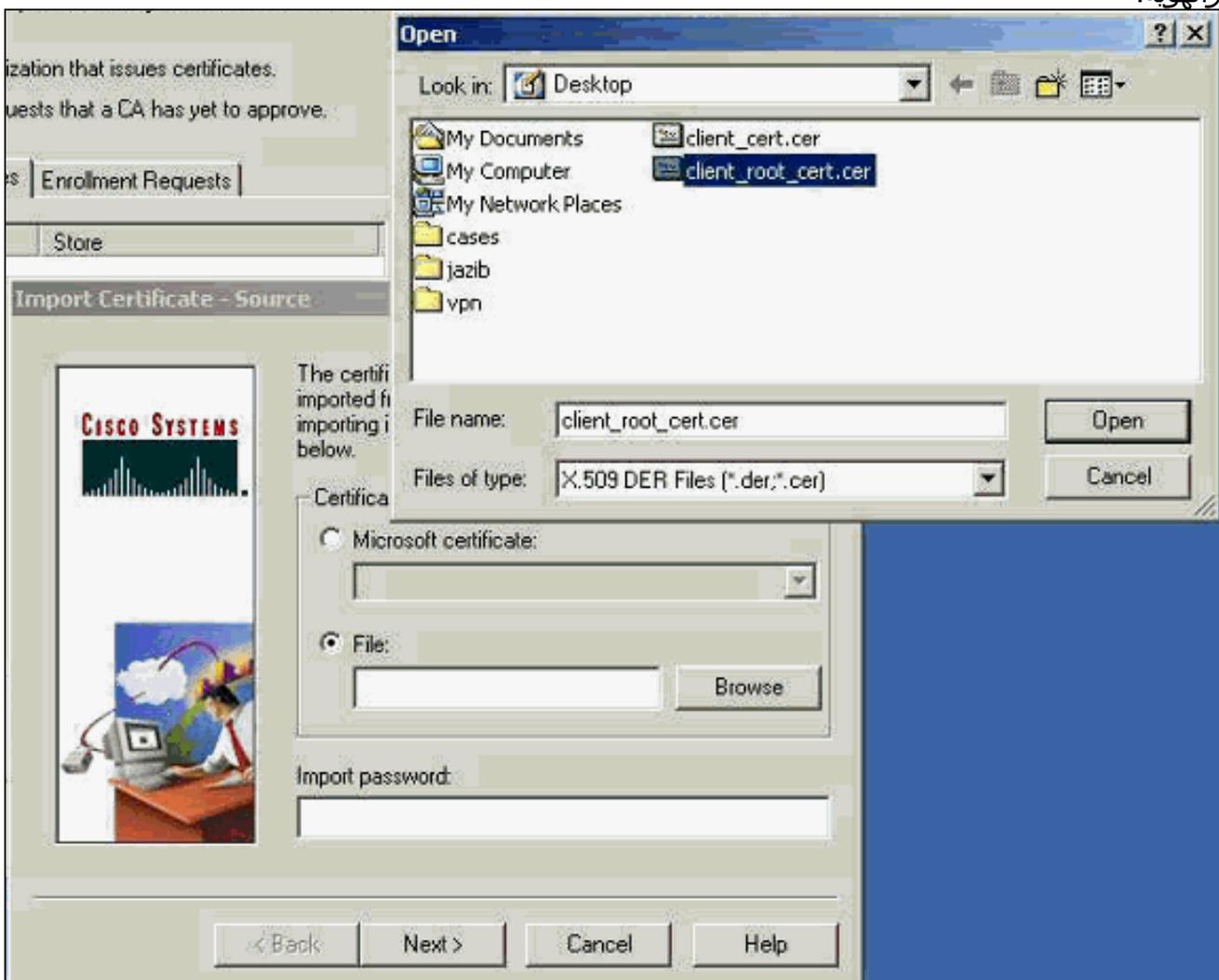
17. حدد Base 64 المشفر. ثم انقر على تنزيل شهادة المرجع المصدق على خادم المرجع المصدق.



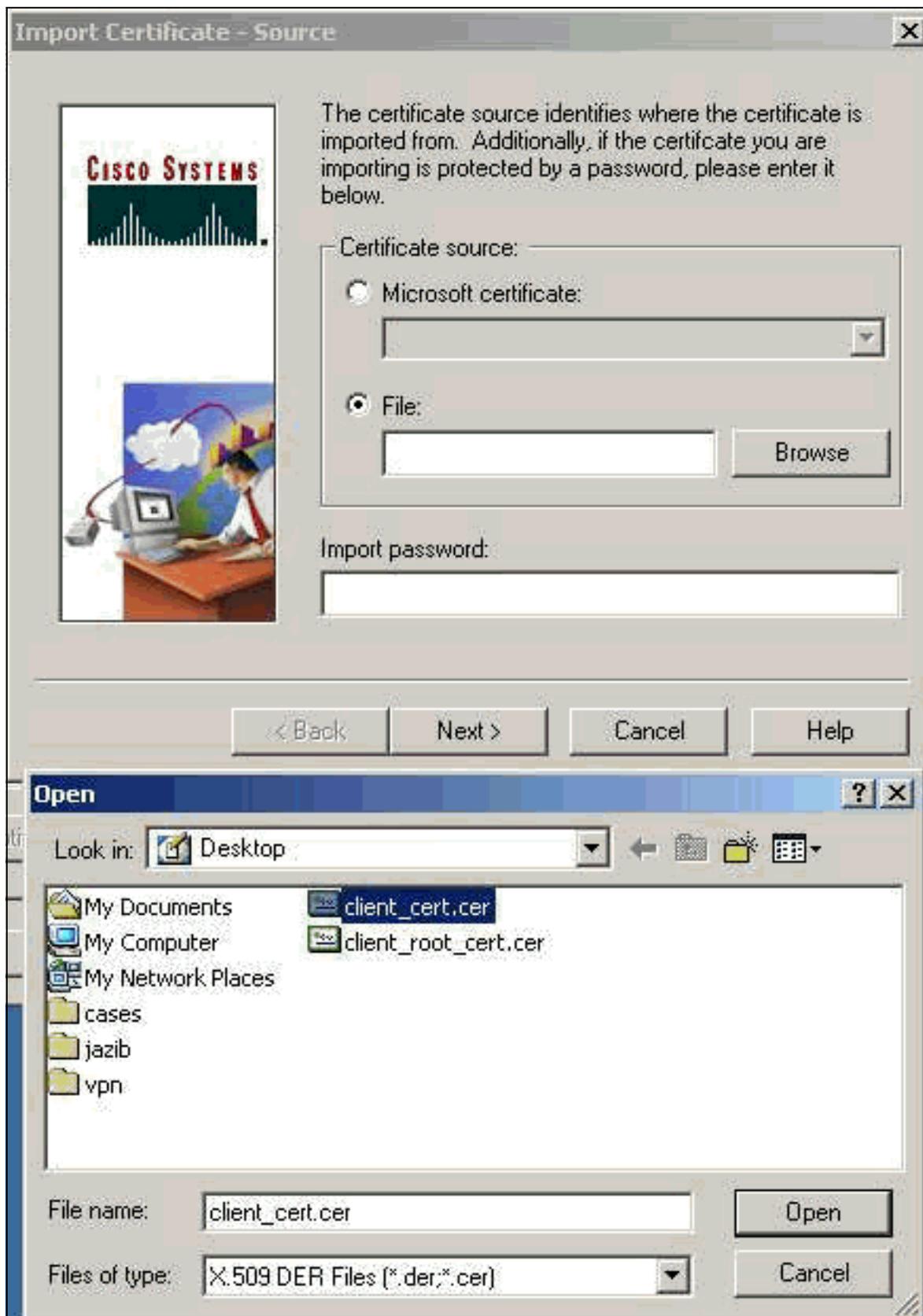
18. حدد ملفًا لتنزيله من صفحة إسترجاع شهادة المرجع المصدق أو قائمة إبطال الشهادة للحصول على الشهادة الجذر على خادم المرجع المصدق. ثم انقر فوق التالي.



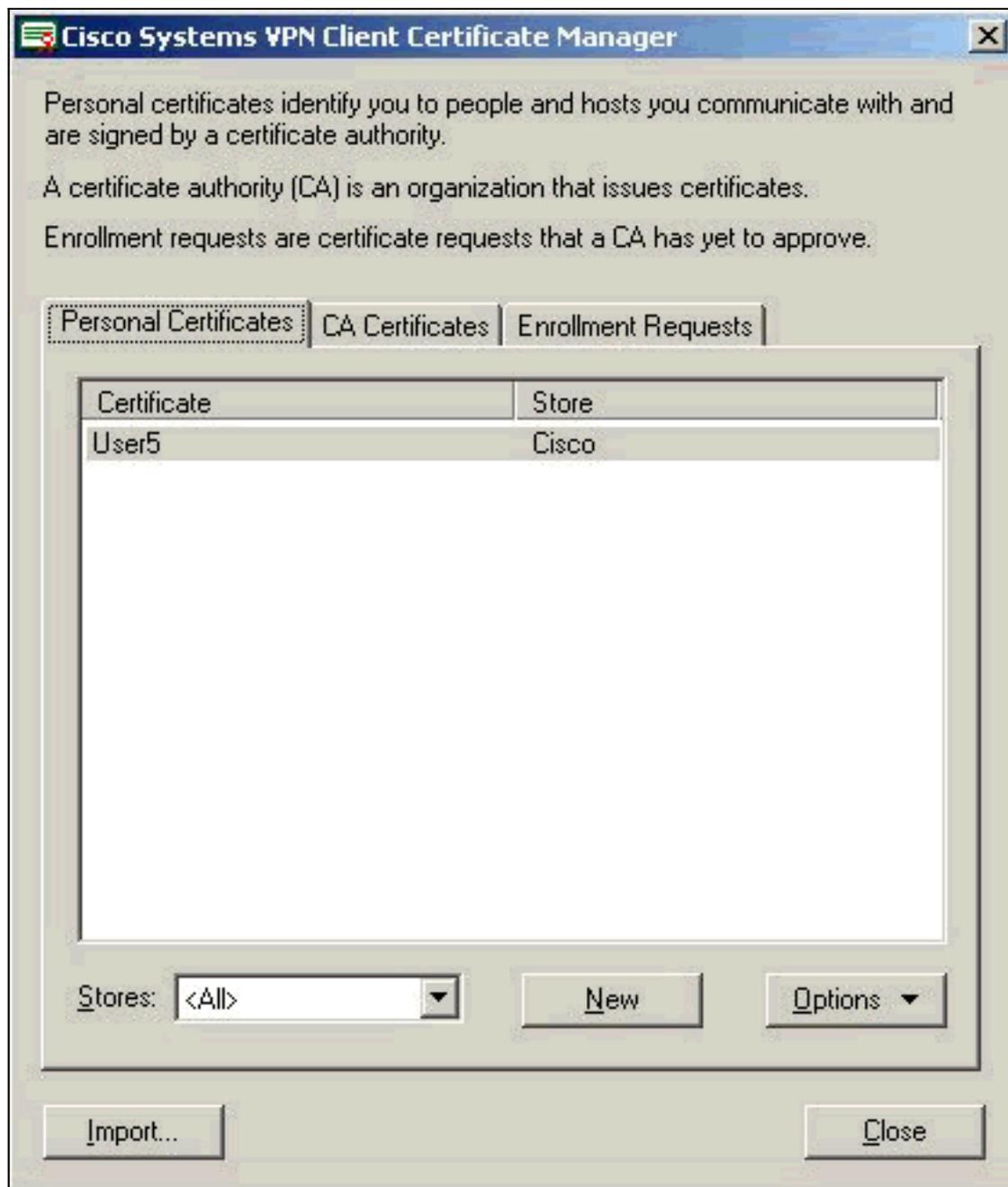
19. حدد مدير الشهادة < شهادة CA > إستيراد على عميل VPN ، ثم حدد ملف CA الجذر لتثبيت شهادات الجذر والهوية.



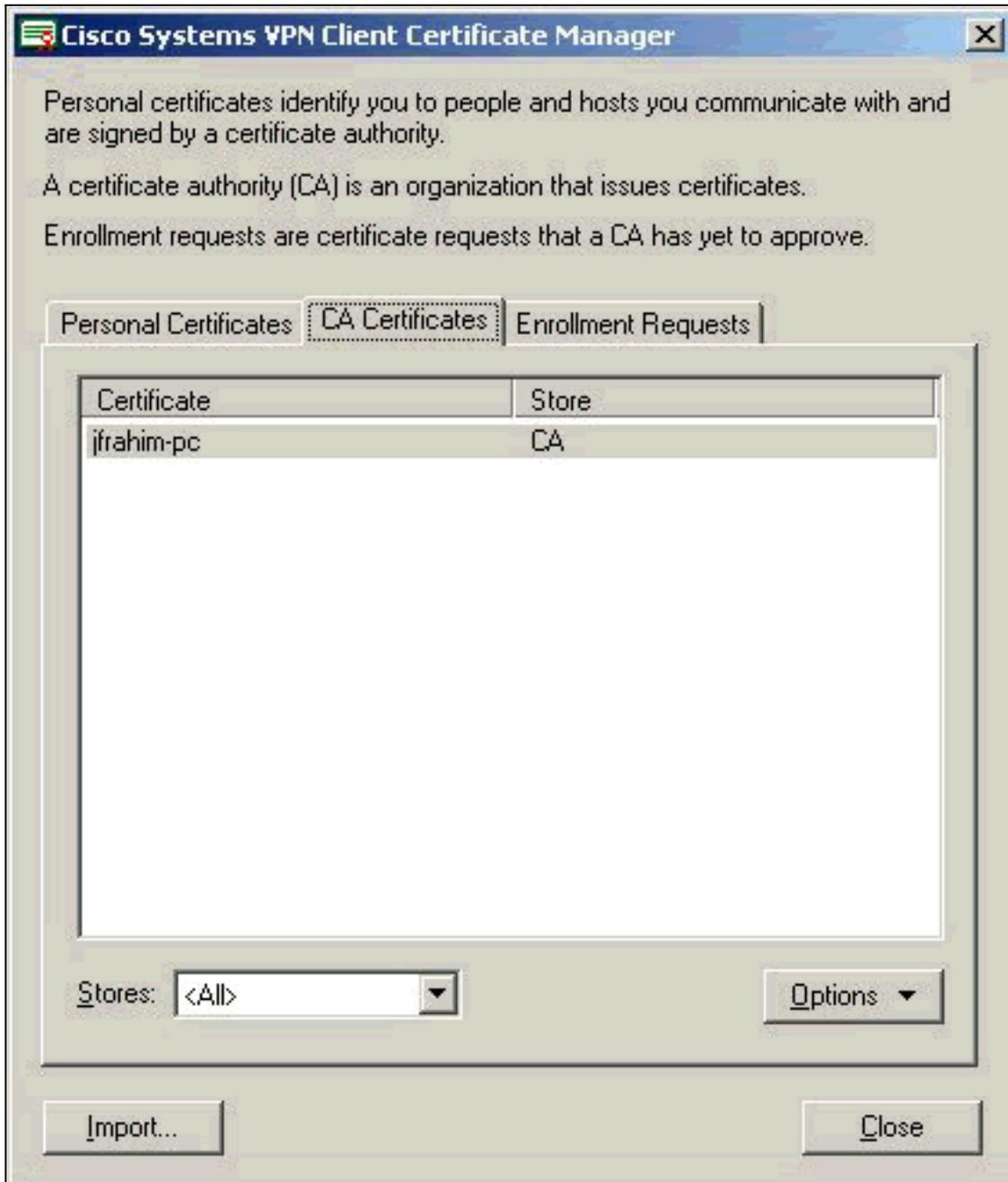
20. حدد مدير الترخيص < شهادات شخصية > إستيراد، واختر ملف شهادة



الهوية.
21. تأكد من أن شهادة الهوية تظهر تحت علامة التبويب شهادات



شخصية. 22. تأكد من ظهور الشهادة الجذر ضمن علامة التبويب شهادات



.CA

[التحقق من الصحة](#)

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

[استكشاف الأخطاء وإصلاحها](#)

عند محاولة التسجيل في Microsoft CA Server، يمكن إنشاء رسالة الخطأ هذه.

Initiating online request
Generating key pair
Generating self-signed Certificate
Initiating online request
Received a response from the CA
Your certificate request was denied

إذا ظهرت رسالة الخطأ هذه، ارجع إلى سجلات Microsoft CA للحصول على تفاصيل أو ارجع إلى هذه الموارد

للحصول على مزيد من المعلومات.

- [بتعذر على Windows العثور على مرجع شهادات يقوم بمعالجة الطلب](#)
- [XCCC: تحدث رسالة الخطأ "تم رفض طلب الشهادة الخاص بك" عند طلب شهادة لمؤتمرات آمنة](#)

معلومات ذات صلة

- [مفاوضة IPsec/بروتوكولات IKE](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا