PEAP تحت شبكات لاسلكية موحدة مع خدمة مصادقة الإنترنت من Microsoft (IAS)

المحتويات

المقدمة

يقدم هذا المستند مثالا لتكوين إعداد بروتوكول المصادقة المتوسع المحمي (PEAP) مع مصادقة الإصدار 2 لبروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي (MS-CHAP) من Microsoft في شبكة لاسلكية موحدة من Cisco مع خدمة مصادقة الإنترنت من Microsoft (IAS) كخادم RADIUS.

المتطلبات الأساسية

المتطلبات

هناك افتراض بأن القارئ لديه معرفة بتثبيت Windows 2003 الأساسي وتثبيت وحدة التحكم من Cisco نظرا لأن هذا المستند يغطي فقط التكوينات المحددة لتسهيل الاختبارات.

ملاحظة: الغرض من هذا المستند هو إعطاء القراء مثالا على التكوين المطلوب على خادم MS من أجل مصادقة PEAP - MS CHAP. تم إختبار تكوين خادم Microsoft المعروض في هذا القسم في المختبر وتبين أنه يعمل كما هو متوقع. إذا واجهت مشكلة في تكوين خادم Microsoft، فاتصل ب Microsoft للحصول على تعليمات. لا يدعم Cisco TAC تكوين Microsoft Windows Server.

للحصول على معلومات التثبيت الأولي ومعلومات التكوين لوحدات التحكم من السلسلة Cisco 4400 Series، ارجع إلى دليل البدء السريع: وحدات التحكم في الشبكة المحلية اللاسلكية من السلسلة Cisco 4400 Series.

يمكن العثور على أدلة التكوين والتثبيت الخاصة بنظام التشغيل Microsoft Windows 2003 في تثبيت نظام التشغيل Windows Server 2003 R2 .

قبل البدء، قم بتثبيت Microsoft Windows Server 2003 باستخدام نظام التشغيل SP1 على كل خادم في مختبر الاختبار وقم بتحديث جميع حزم الخدمات. قم بتثبيت وحدات التحكم ونقاط الوصول في الوضع Lightweight (نقاط الوصول في الوضع Lightweight (LAPs) وتأكد من تكوين آخر تحديثات البرامج.

المكونات المستخدمة

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

- وحدة التحكم من السلسلة Cisco 4400 Series التي تشغل البرنامج الثابت، الإصدار 4.0
- نقطة الوصول Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise Server (SP1) مع تثبيت خدمات خدمة مصادقة الإنترنت (IAS) ومرجع الشهادات (CA) و DHCP ونظام اسم المجال (DNS)
- Windows XP Professional مع SP 2 (وحزم الخدمة المحدثة) وبطاقة واجهة الشبكة اللاسلكية Cisco (Aironet 802.11a/b/g (NIC
- Aironet Desktop Utility، الإصدار 4.0
- المحول Cisco 3560 Switch

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.

نظرة عامة على PEAP

يستخدم PEAP تأمين مستوى النقل (TLS) لإنشاء قناة مشفرة بين عميل PEAP مصدق، مثل كمبيوتر محمول لاسلكي، ومصادقة PEAP، مثل خدمة مصادقة الإنترنت من Microsoft (IAS) أو أي خادم RADIUS. لا يحدد PEAP طريقة مصادقة، ولكنه يوفر أمانا إضافيا لبروتوكولات مصادقة EAP الأخرى، مثل EAP-MSCHAPv2، التي يمكن أن تعمل من خلال القناة المشفرة TLS التي يوفرها PEAP. تتألف عملية مصادقة PEAP من مرحلتين رئيسيتين:

المرحلة الأولى من PEAP: قناة TLS المشفرة

يرتبط العميل اللاسلكي بنقطة الوصول. يوفر الاقتران القائم على IEEE 802.11 مصادقة نظام مفتوح أو مصادقة مفتاح مشترك قبل إنشاء اقتران آمن بين العميل ونقطة الوصول (LAP). بعد إنشاء الاقتران القائم على IEEE 802.11 بنجاح بين العميل ونقطة الوصول، يتم التفاوض على جلسة TLS مع نقطة الوصول. بعد اكتمال المصادقة

بين العميل اللاسلكي وخادم IAS بنجاح، يتم التفاوض على جلسة عمل TLS فيما بينهما. يتم إستخدام المفتاح المستمد من هذا التفاوض لتشفير كل الاتصالات اللاحقة.

المرحلة الثانية من PEAP: الاتصال الذي تم التصديق عليه بواسطة EAP

يحدث اتصال EAP، الذي يتضمن تفاوض EAP، داخل قناة TLS التي أنشأها PEAP ضمن المرحلة الأولى من عملية مصادقة PEAP. يصادق خادم IAS العميل اللاسلكي مع EAP-MS-CHAP v2. تقوم نقاط الوصول في الوضع Lightweight ووحدة التحكم فقط بإعادة توجيه الرسائل بين العميل اللاسلكي وخادم RADIUS. يتعذر على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وعنصر التحكم في الوصول (LAP) فك تشفير هذه الرسائل لأنها ليست نقطة نهاية TLS.

بعد حدوث المرحلة الأولى من PEAP، وإنشاء قناة TLS بين خادم IAS والعميل اللاسلكي 802. 1X، من أجل محاولة مصادقة ناجحة حيث قدم المستخدم بيانات اعتماد صالحة مستندة إلى كلمة المرور مع PEAP-MS-CHAP v2، فإن تسلسل رسالة RADIUS هو:

1. يرسل خادم IAS رسالة طلب هوية إلى العميل: EAP-Request/Identity.
2. يرد العميل برسالة إستجابة الهوية: EAP-Response/Identity.
3. يرسل خادم IAS رسالة تحدي MS-CHAP v2: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (التحدي).
4. يستجيب العميل بتحدي MS-CHAP v2 واستجابته: EAP-response/EAP-type=EAP-MS-CHAP-V2 (الاستجابة).
5. يرسل خادم IAS حزمة نجاح MS-CHAP v2 عندما يقوم الخادم بمصادقة العميل: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (نجاح) بنجاح.
6. يستجيب العميل بواسطة حزمة نجاح MS-CHAP v2 عندما يقوم العميل بمصادقة الخادم بنجاح: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (نجاح).
7. يرسل خادم IAS EAP-TLV الذي يشير إلى المصادقة الناجحة.
8. يستجيب العميل برسالة نجاح حالة EAP-TLV.
9. يكمل الخادم المصادقة ويرسل رسالة نجاح EAP باستخدام النص العادي. إذا تم نشر شبكات VLAN لعزل العميل، فسيتم تضمين سمات شبكة VLAN في هذه الرسالة.

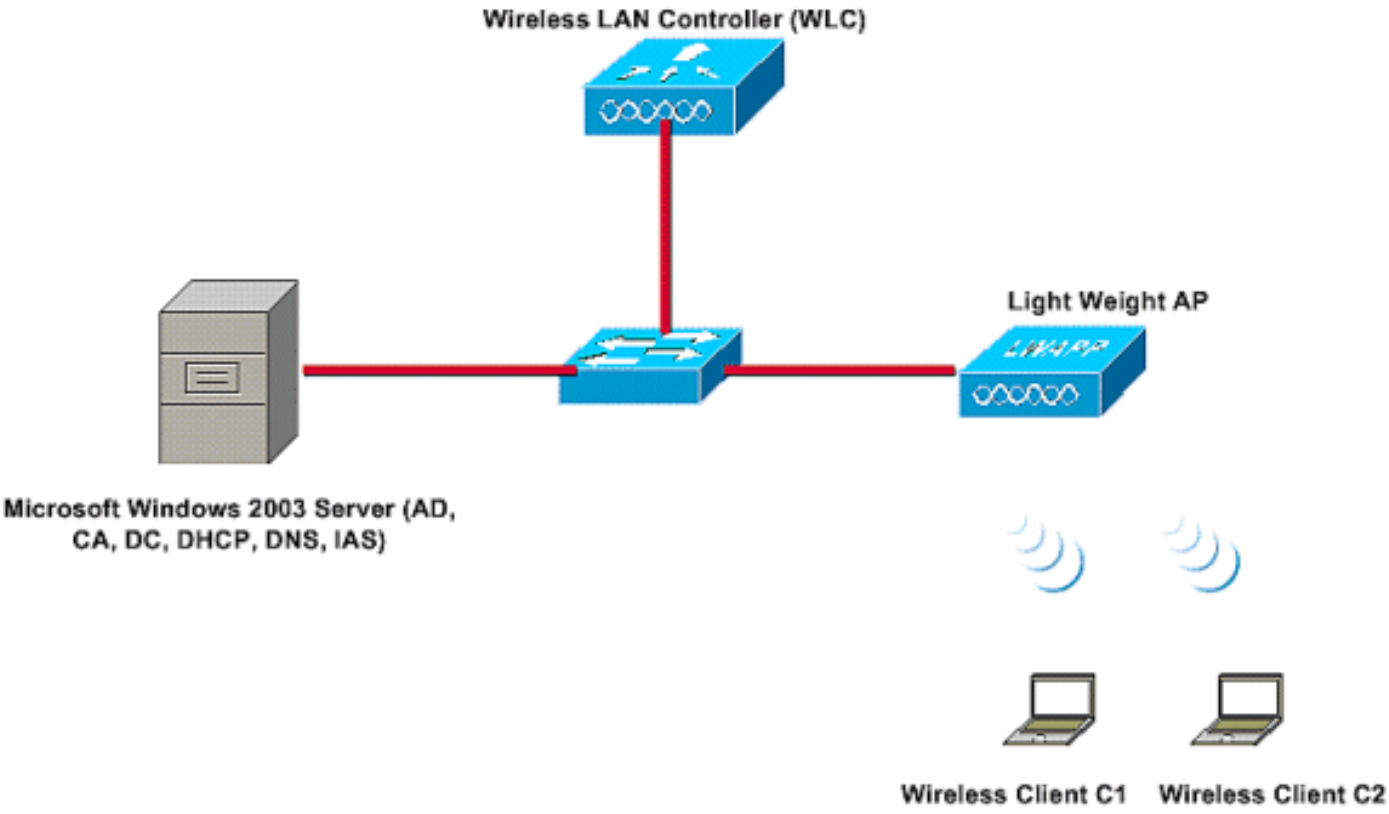
التكوين

يقدم هذا المستند مثالا لتكوين PEAP MS-CHAP v2.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



في هذا الإعداد، يقوم خادم Microsoft Windows 2003 بتنفيذ الأدوار التالية:

- وحدة التحكم بالمجال للمجال **Wireless.com**
- خادم DHCP/DNS
- خادم جهة منح الشهادة (CA)
- خدمة Active Directory - للحفاظ على قاعدة بيانات المستخدم
- خدمة مصادقة الإنترنت (IAS) - لمصادقة المستخدمين اللاسلكيين

يتصل هذا الخادم بالشبكة السلكية من خلال محول من الطبقة 2 كما هو موضح.

كما تتصل وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية (WLC) ونقطة الوصول في الوضع Lightweight (LAP)) المسجلة بالشبكة من خلال محول الطبقة 2.

سيستخدم العملان اللاسلكيان C1 و C2 (WPA2 Wi-Fi Protected Access 2) - مصادقة PEAP MSCHAP v2 للاتصال بالشبكة اللاسلكية.

الهدف هو تكوين خادم Microsoft 2003 ووحدة تحكم في الشبكة المحلية (LAN) اللاسلكية ونقطة وصول (AP) خفيفة الوزن لمصادقة الأجهزة العميلة اللاسلكية باستخدام مصادقة PEAP MSCHAP v2.

يشرح القسم التالي كيفية تكوين الأجهزة لهذا الإعداد.

التكوينات

ينظر هذا القسم في التكوين المطلوب لإعداد مصادقة PEAP MS-CHAP v2 في شبكة WLAN هذه:

- تكوين خادم Microsoft Windows 2003
- تكوين وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) ونقاط الوصول في الوزن الخفيف
- تكوين عملاء اللاسلكي

ابدأ بتكوين خادم Microsoft Windows 2003.

تكوين خادم Microsoft Windows 2003

تكوين خادم Microsoft Windows 2003

كما هو مذكور في قسم إعداد الشبكة، أستخدم خادم Microsoft Windows 2003 في الشبكة لتنفيذ هذه الوظائف.

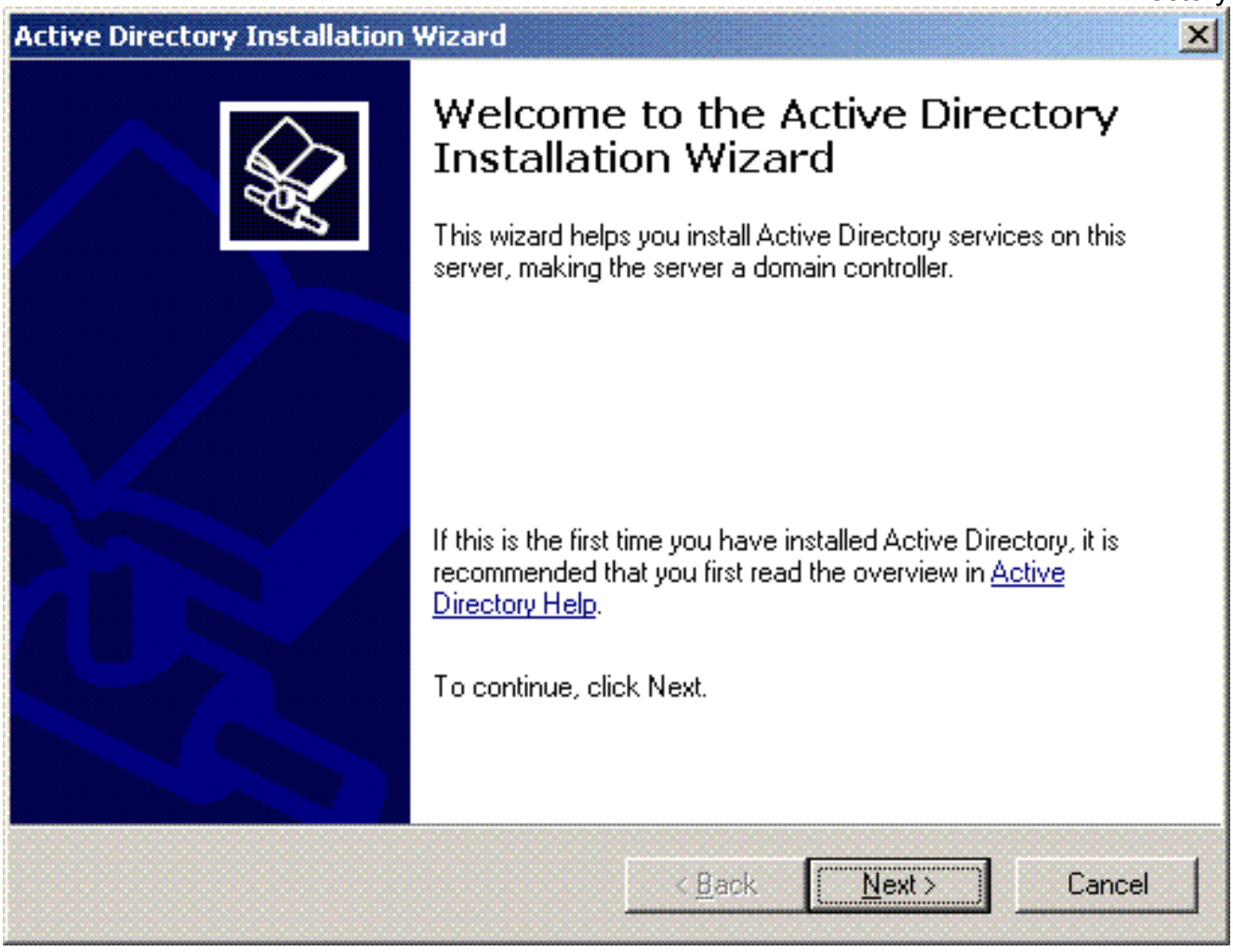
- **وحدة التحكم بالمجال** - للمجال **اللاسلكي**
- خادم **DHCP/DNS**
- **خادم جهة منح الشهادة (CA)**
- **خدمة مصادقة الإنترنت (IAS)** - لمصادقة المستخدمين اللاسلكيين
- **خدمة Active Directory** - للحفاظ على قاعدة بيانات المستخدم

قم بتكوين خادم Microsoft Windows 2003 لهذه الخدمات. ابدأ بتكوين خادم Microsoft Windows 2003 كوحدة تحكم بالمجال.

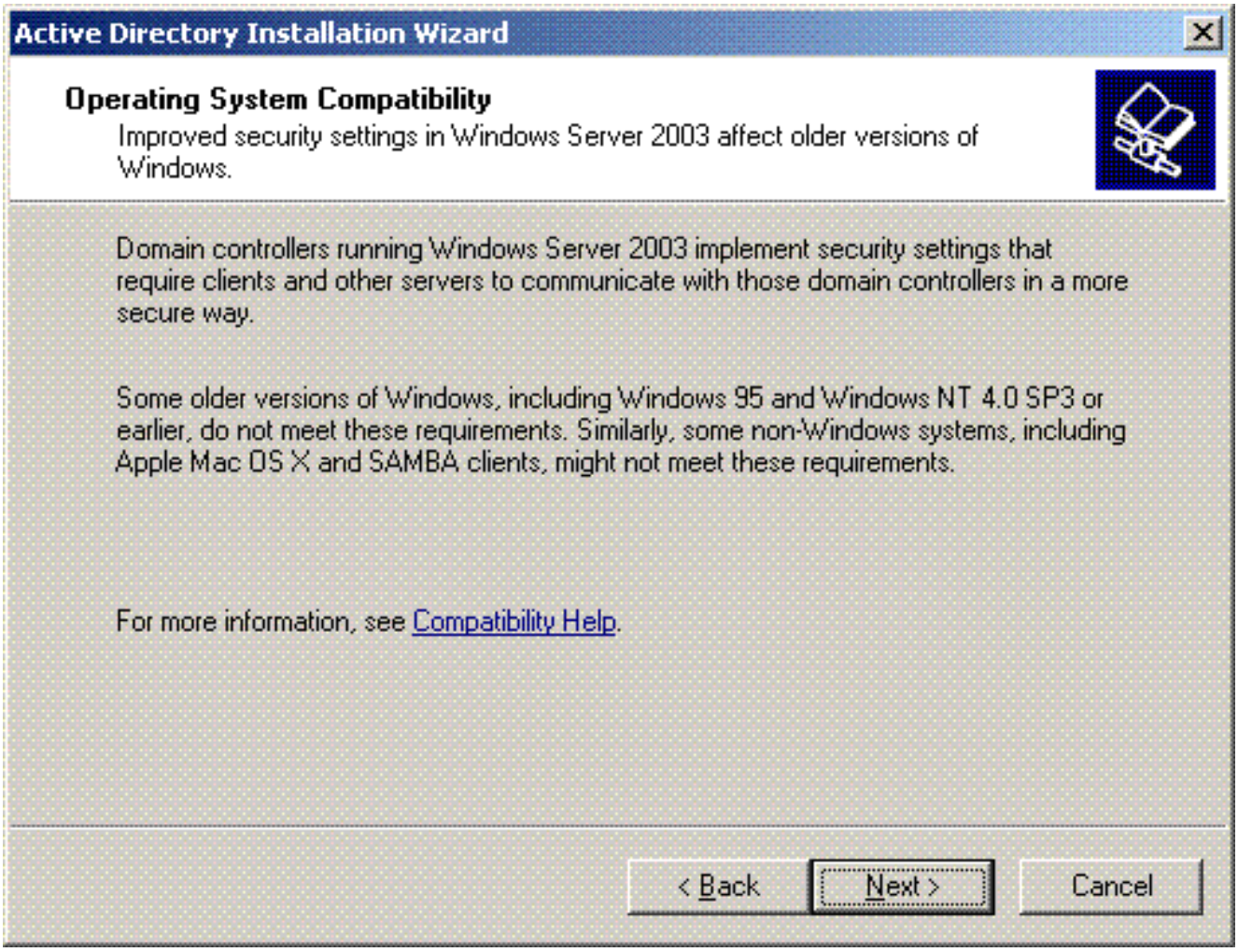
تكوين خادم Microsoft Windows 2003 كوحدة تحكم بالمجال

لتكوين خادم Microsoft Windows 2003 كوحدة تحكم بالمجال، أكمل الخطوات التالية:

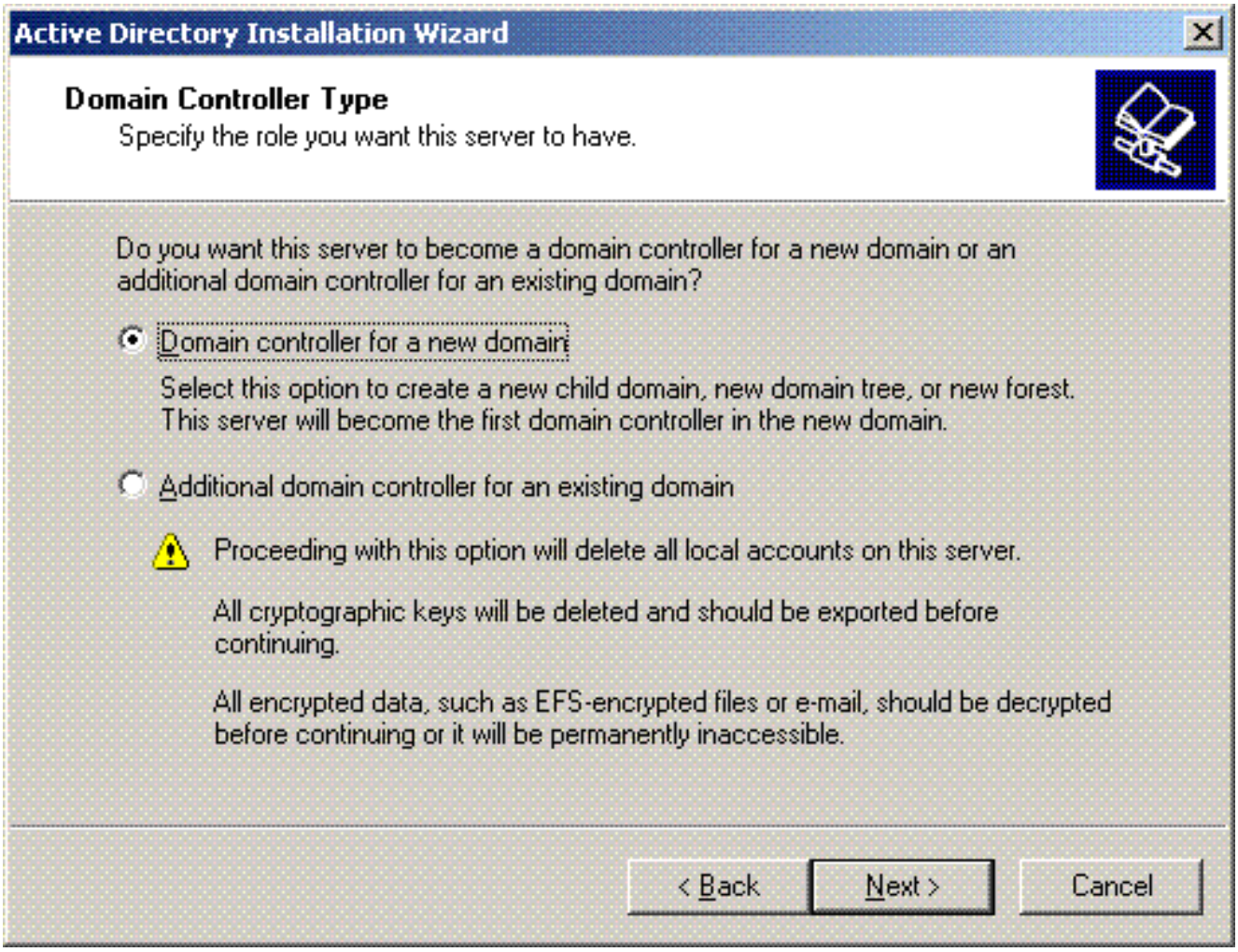
1. انقر فوق **بدء**، وانقر فوق **تشغيل**، واكتب **dcpromo.exe**، ثم انقر فوق **موافق** لبدء معالج تثبيت Active Directory.



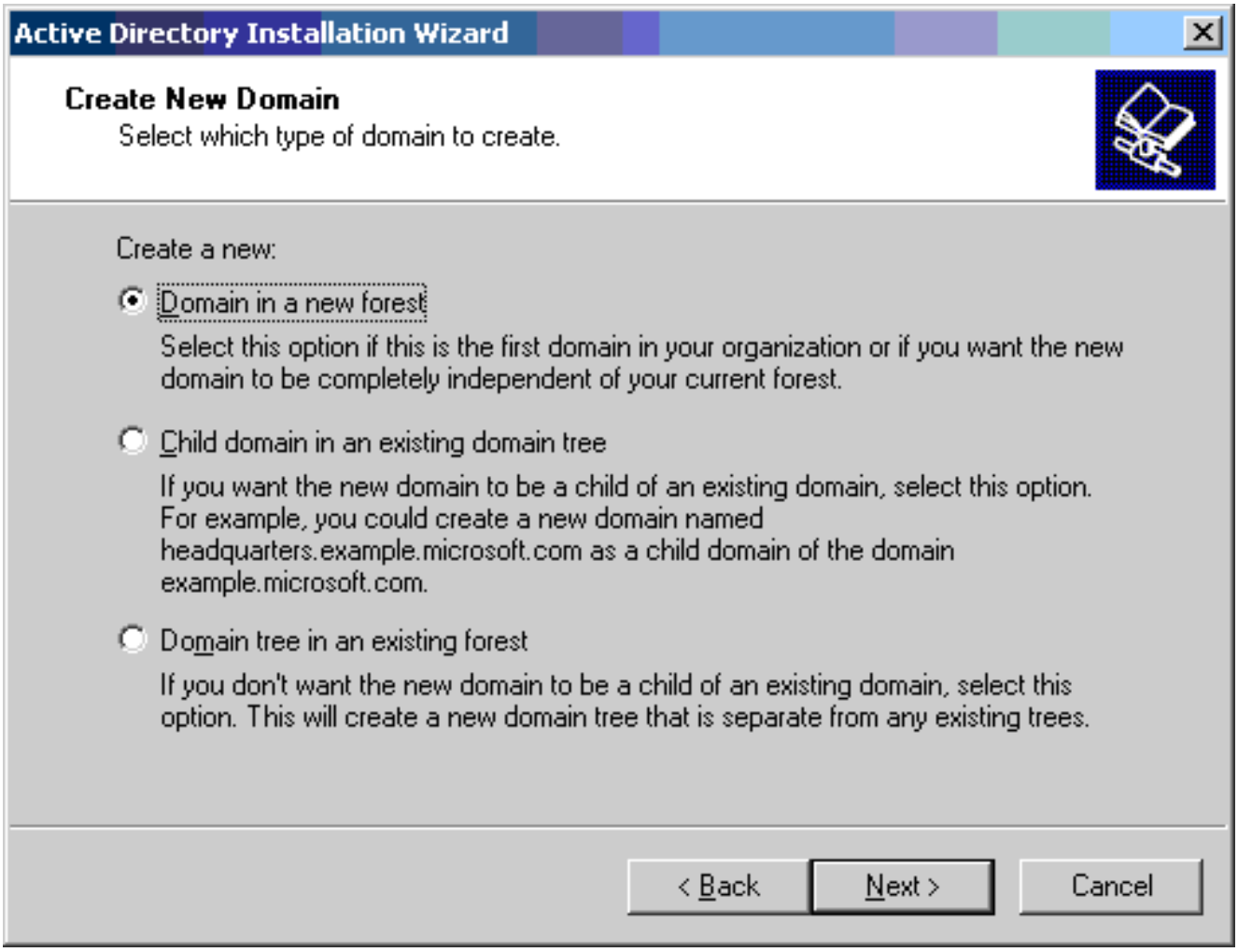
2. انقر فوق **التالي** لتشغيل معالج تثبيت Active Directory.



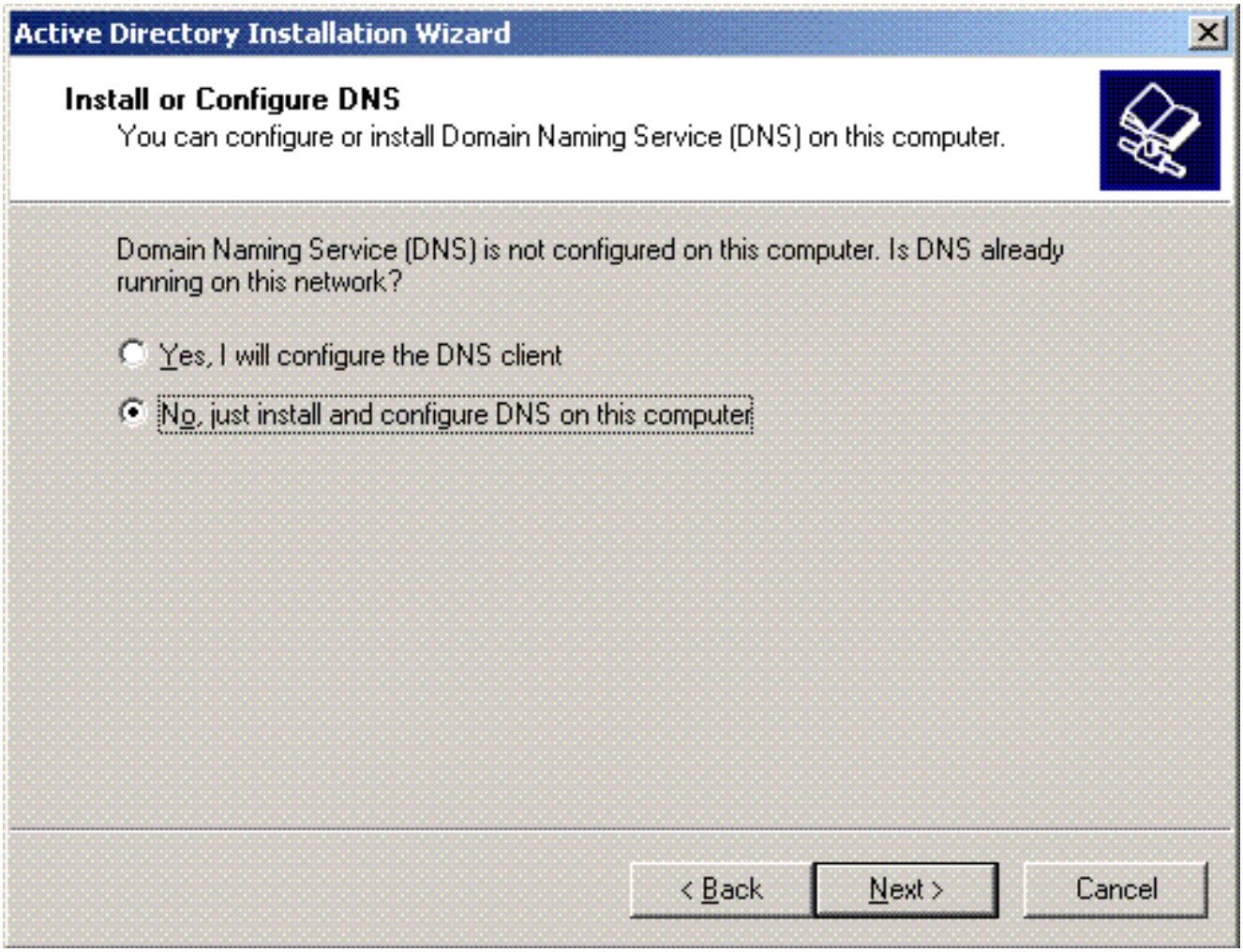
3. لإنشاء مجال جديد، أختر خيار **وحدة التحكم بالمجال** لمجال جديد.



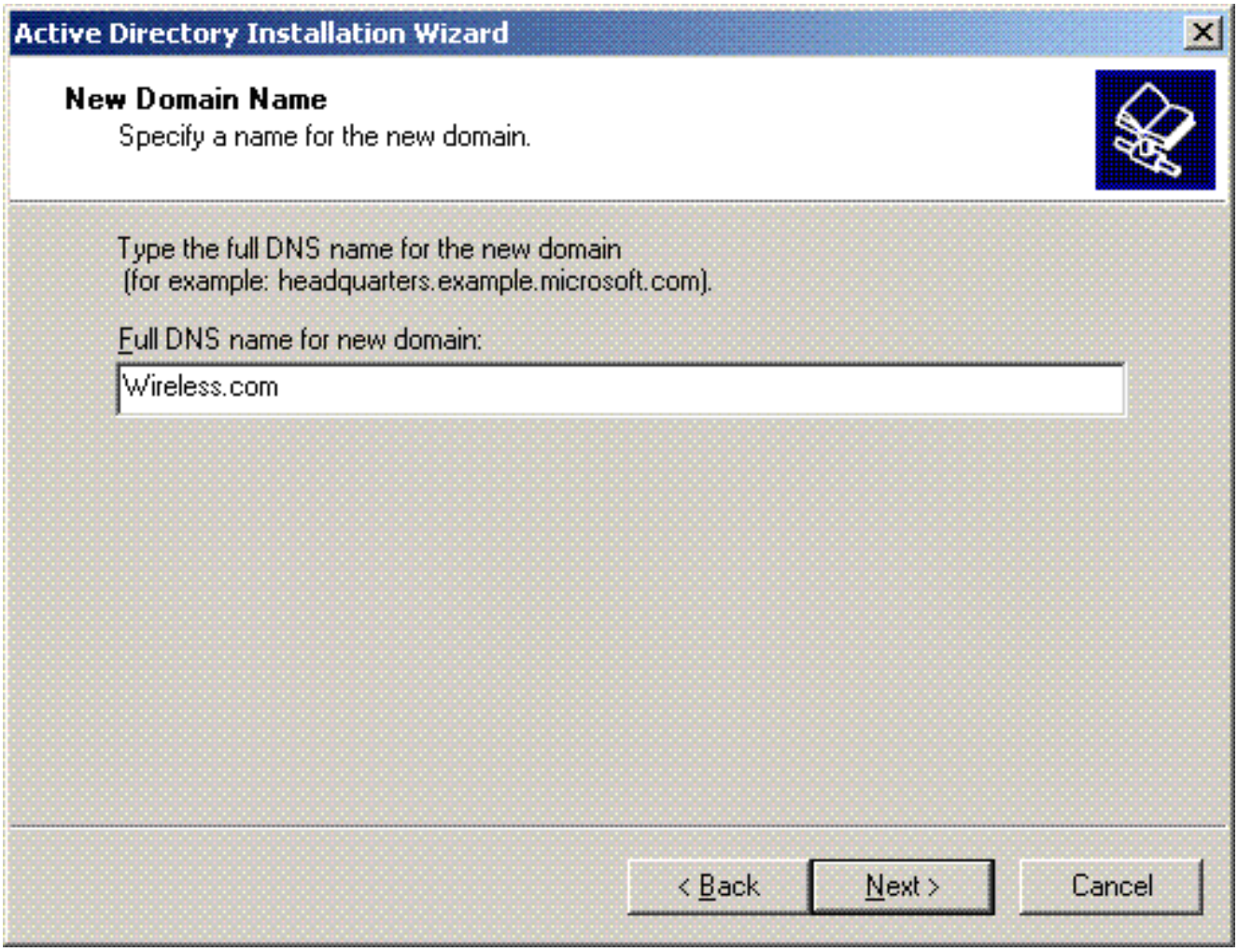
4. انقر فوق **التالي** لإنشاء غابة جديدة من أشجار المجال.



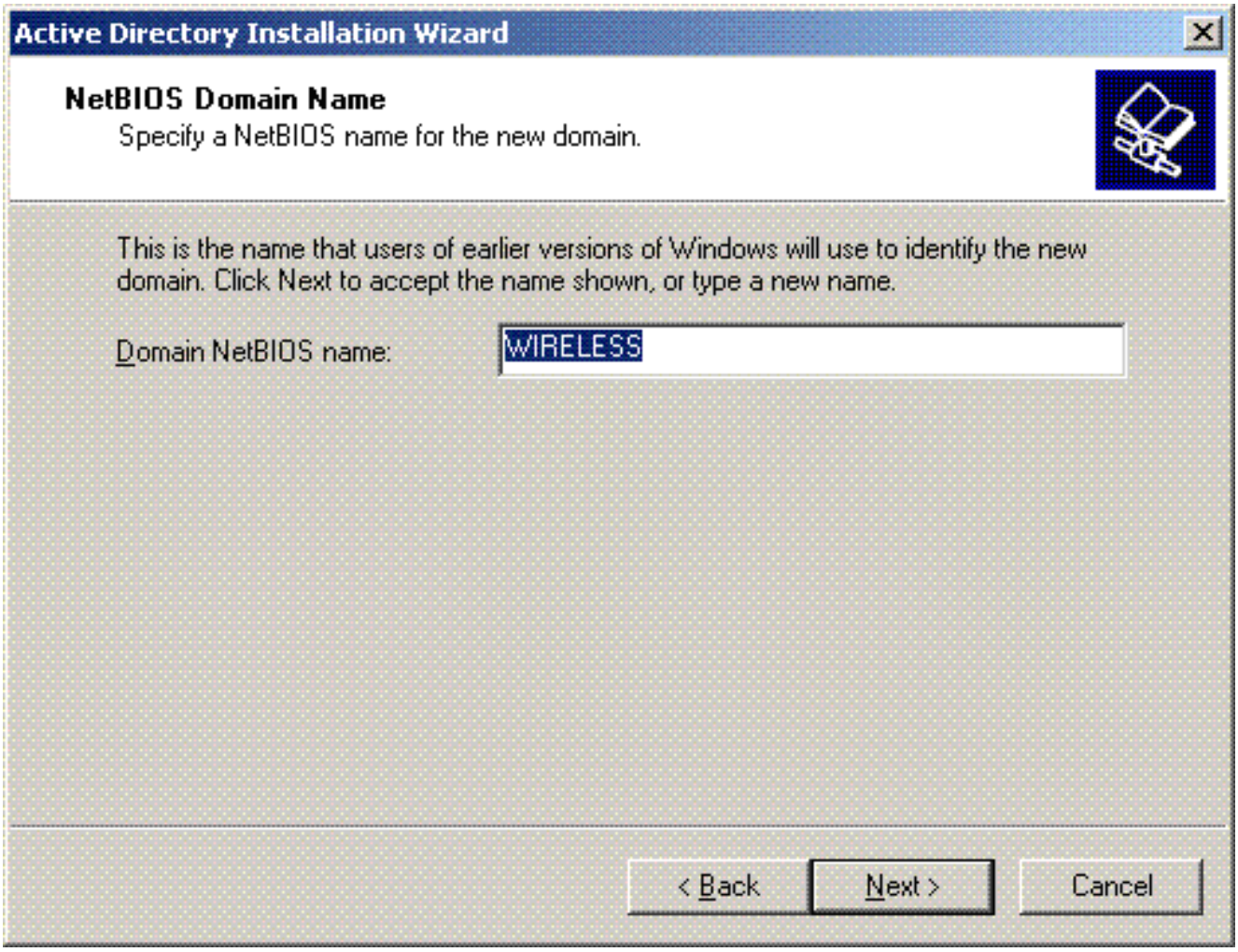
5. في حالة عدم تثبيت DNS على النظام، يوفر لك المعالج خيارات تكوين DNS بها. أختر **لا، قم فقط بتثبيت DNS وتكوينه** على هذا الكمبيوتر. انقر فوق **Next (التالي)**.



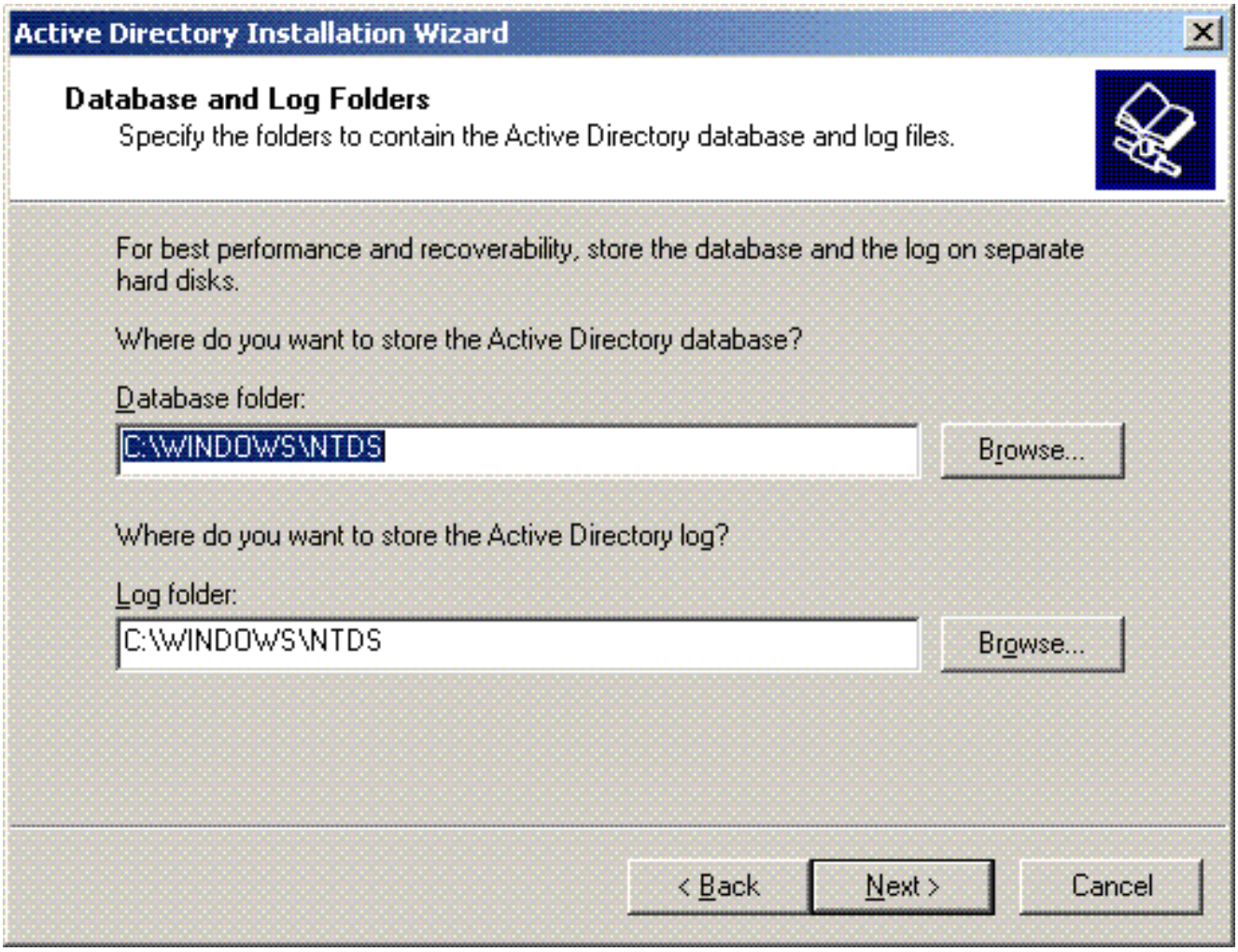
6. اكتب اسم DNS الكامل للمجال الجديد. في هذا المثال، يتم إستخدام **Wireless.com** وانقر على **التالي**.



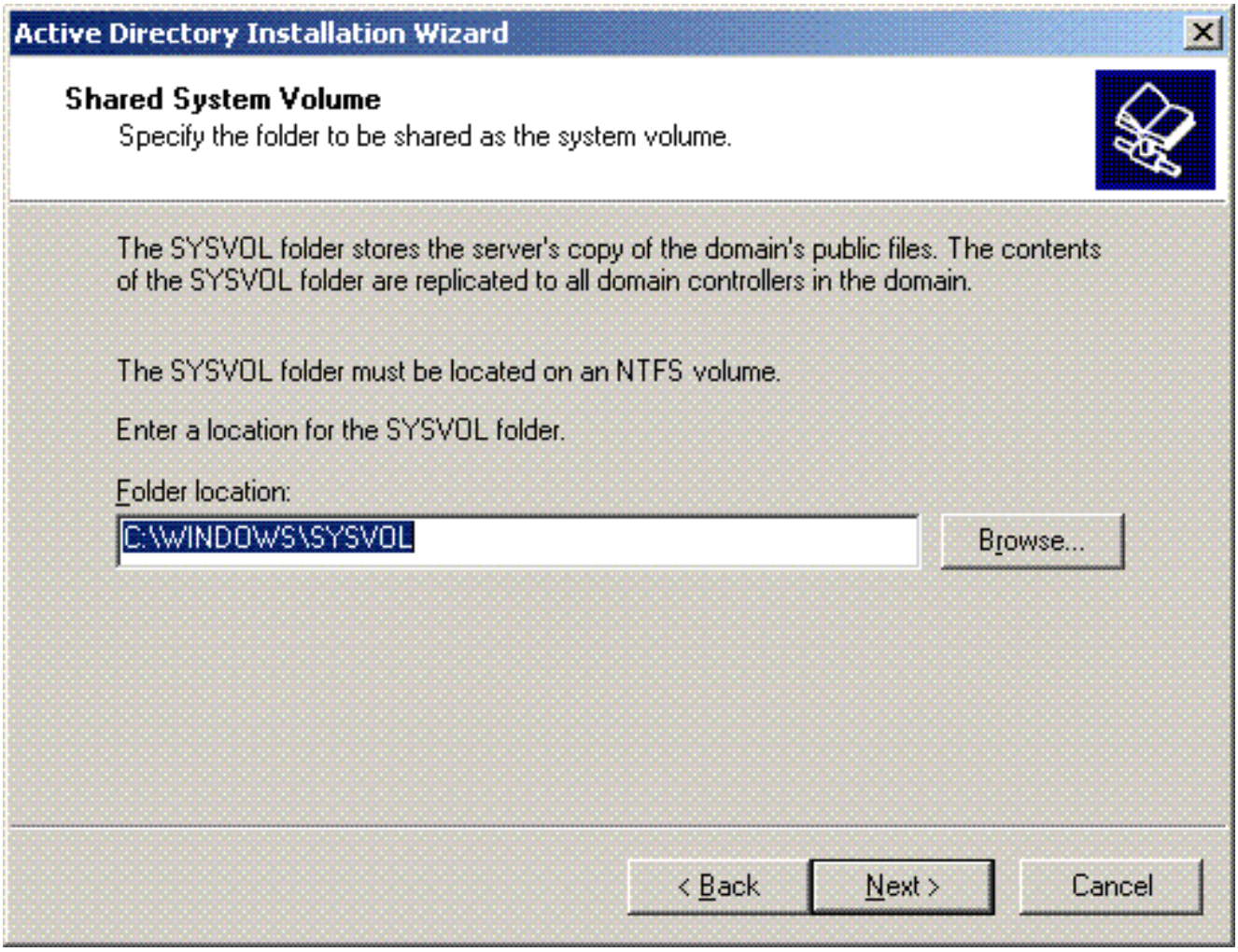
7. أدخل اسم NetBIOS للمجال وانقر على **التالي**. يستخدم هذا المثال **الاتصال اللاسلكي**.



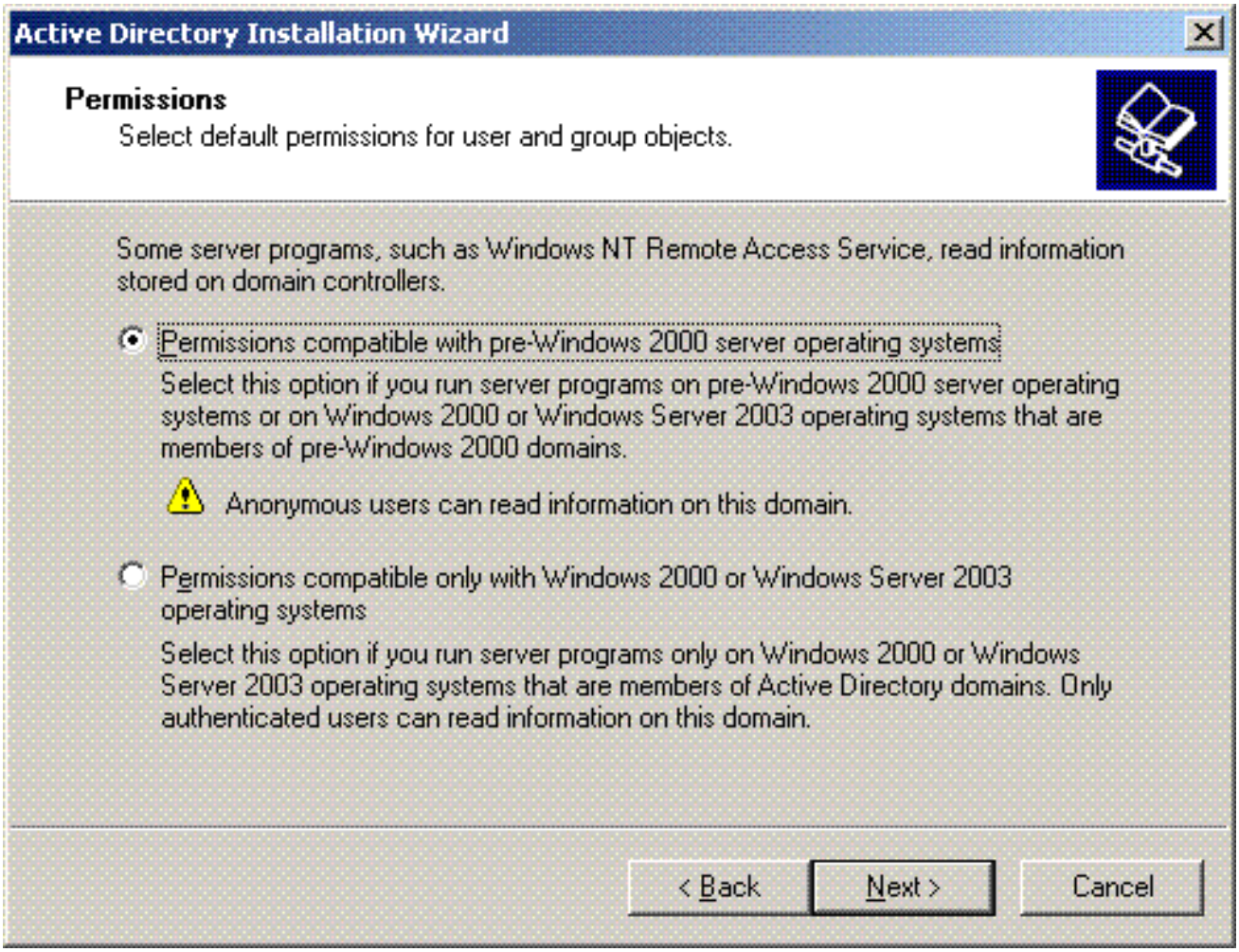
8. أختر قاعدة البيانات ومواقع السجلات للمجال. انقر فوق **Next (التالي)**.



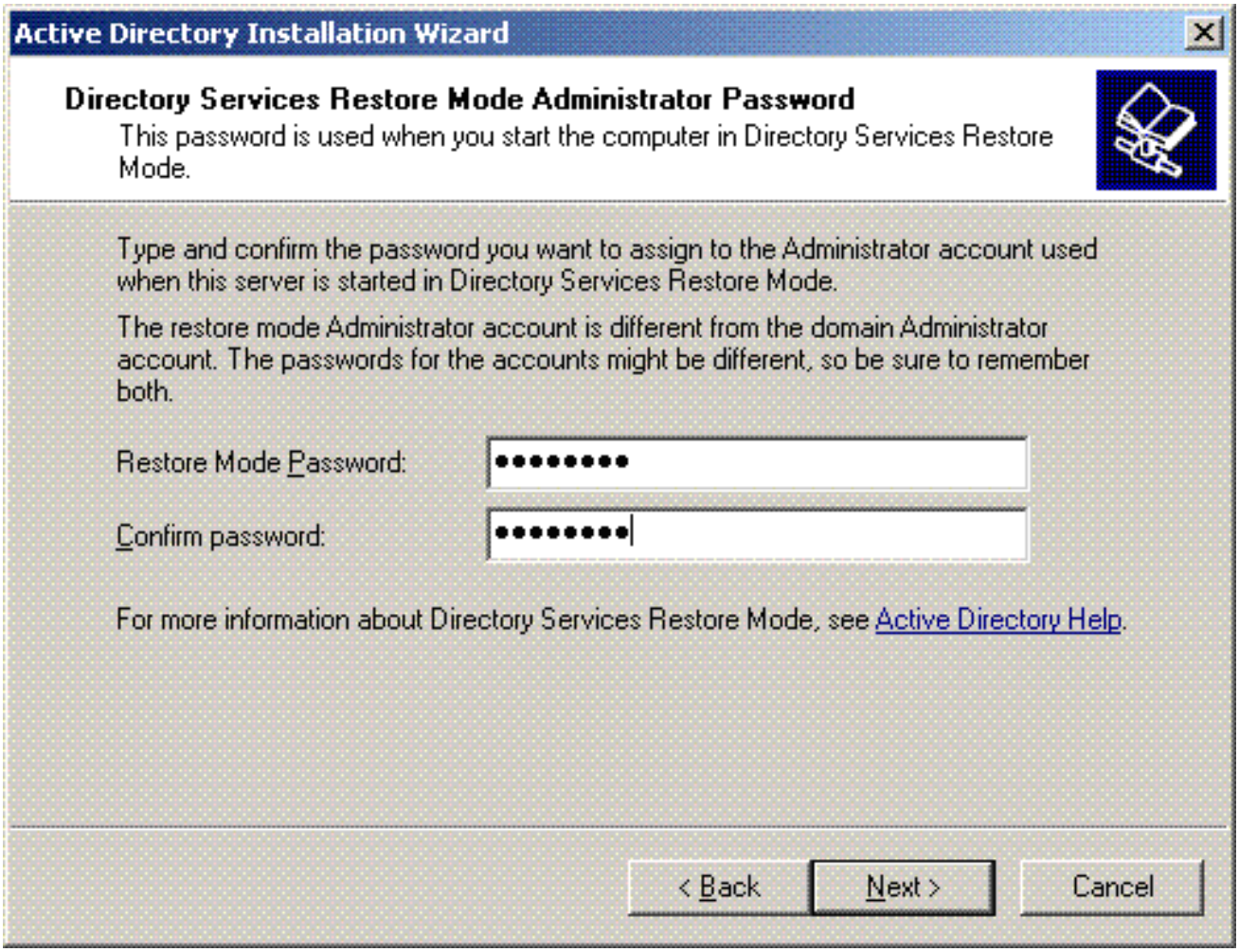
9. أختر موقع لمجلد Sysvol. انقر فوق **Next (التالي)**.



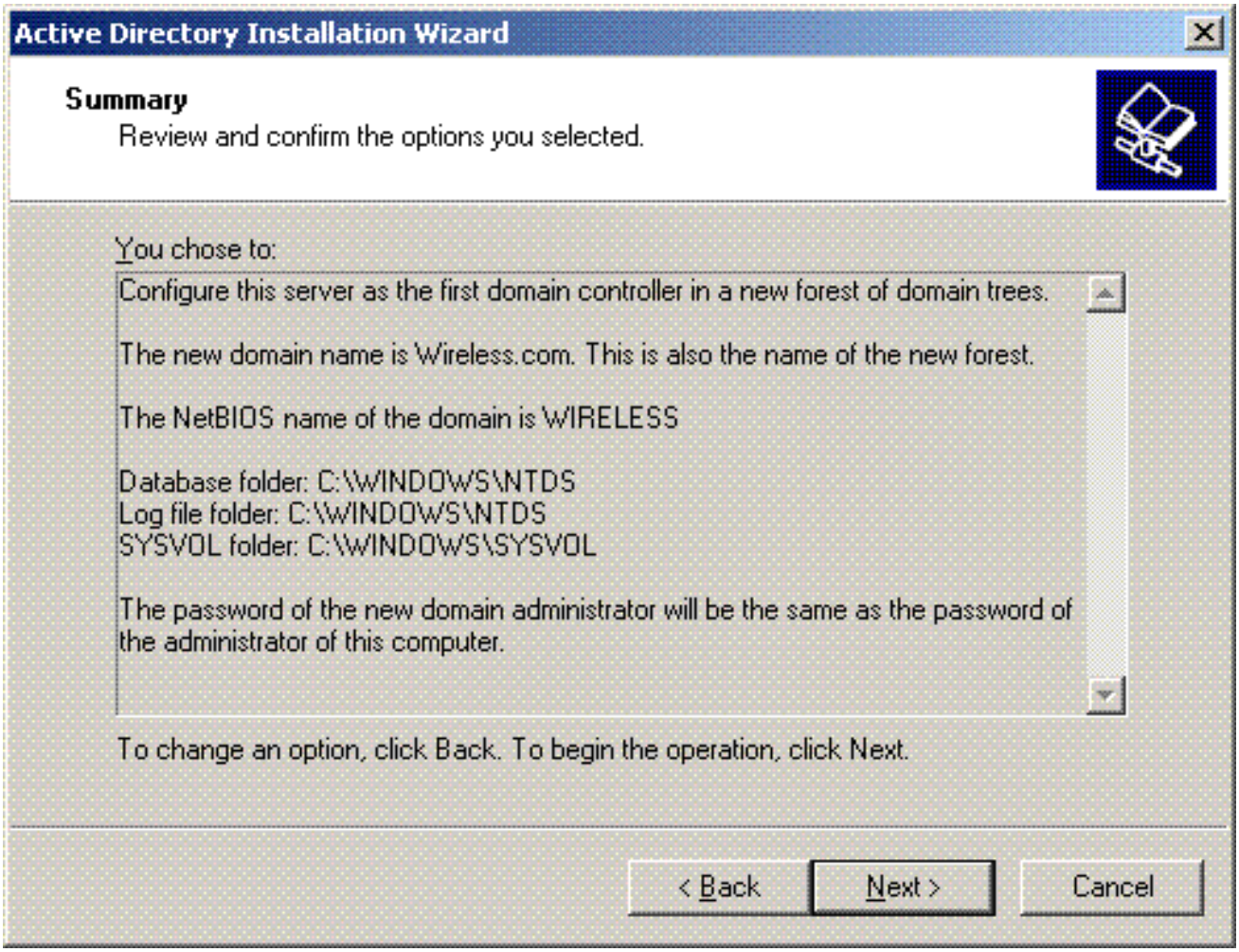
10. أختر الأذونات الافتراضية للمستخدمين والمجموعات. انقر فوق **Next (التالي)**.



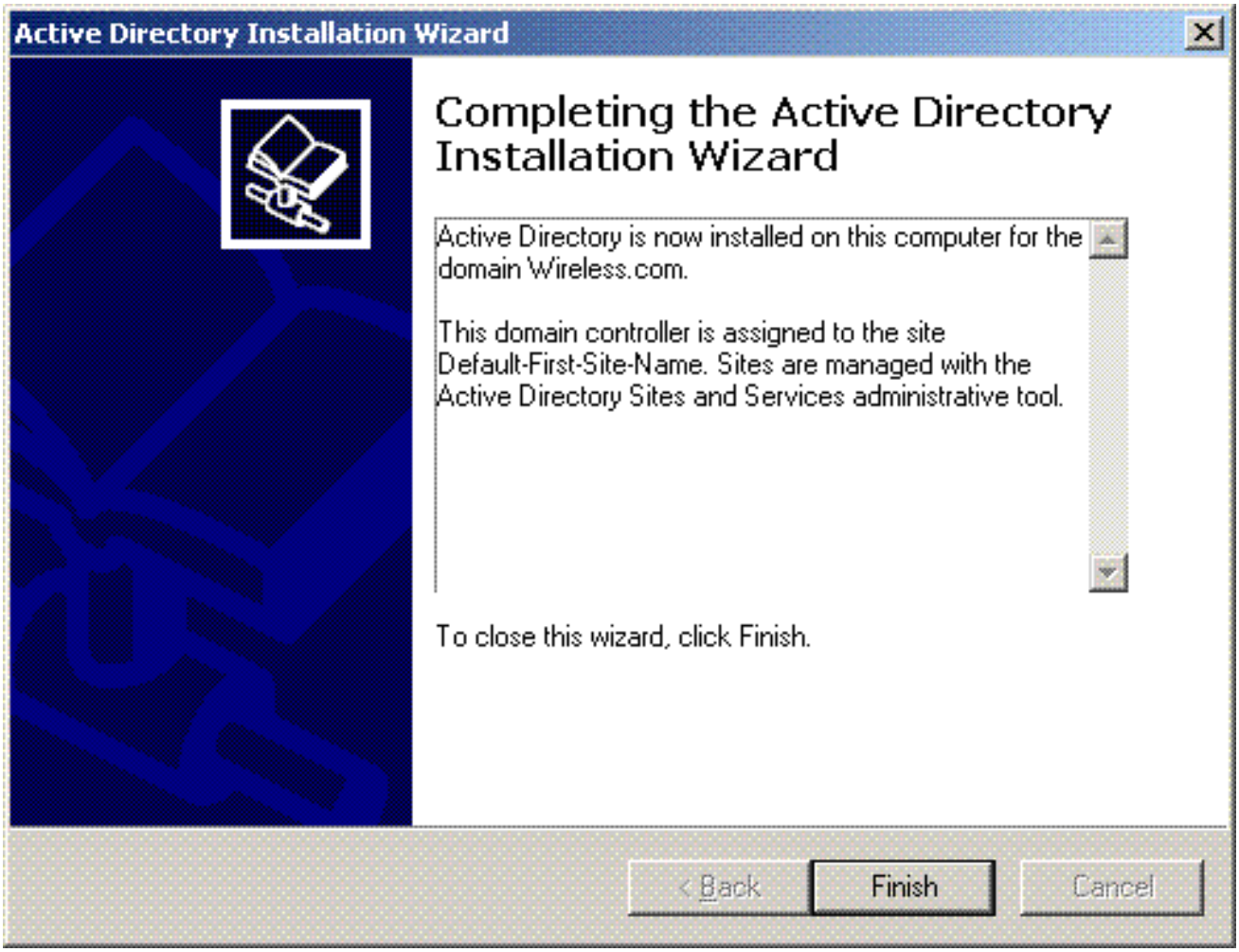
11. ثبت الإدارة كلمة مرور وطقطقة **بعد ذلك**.



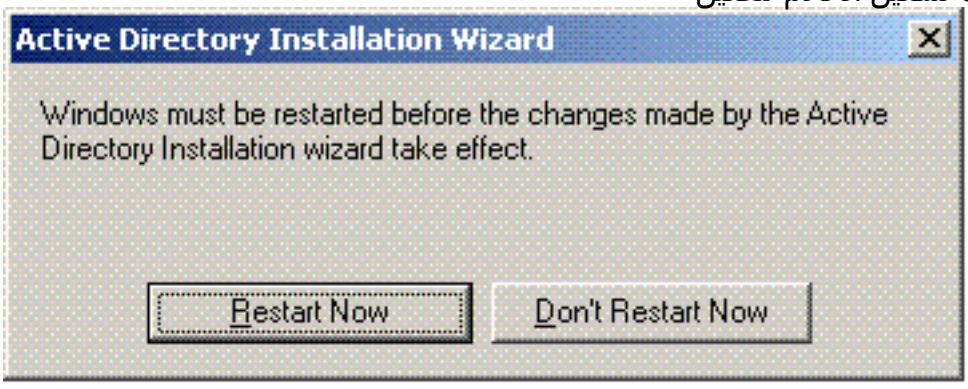
12. انقر فوق **التالي** لقبول مجموعة خيارات المجال مسبقا.



13. انقر فوق **إنهاء**" لإغلاق معالج تثبيت Active Directory.



14. قم بإعادة تشغيل الخادم لتفعيل



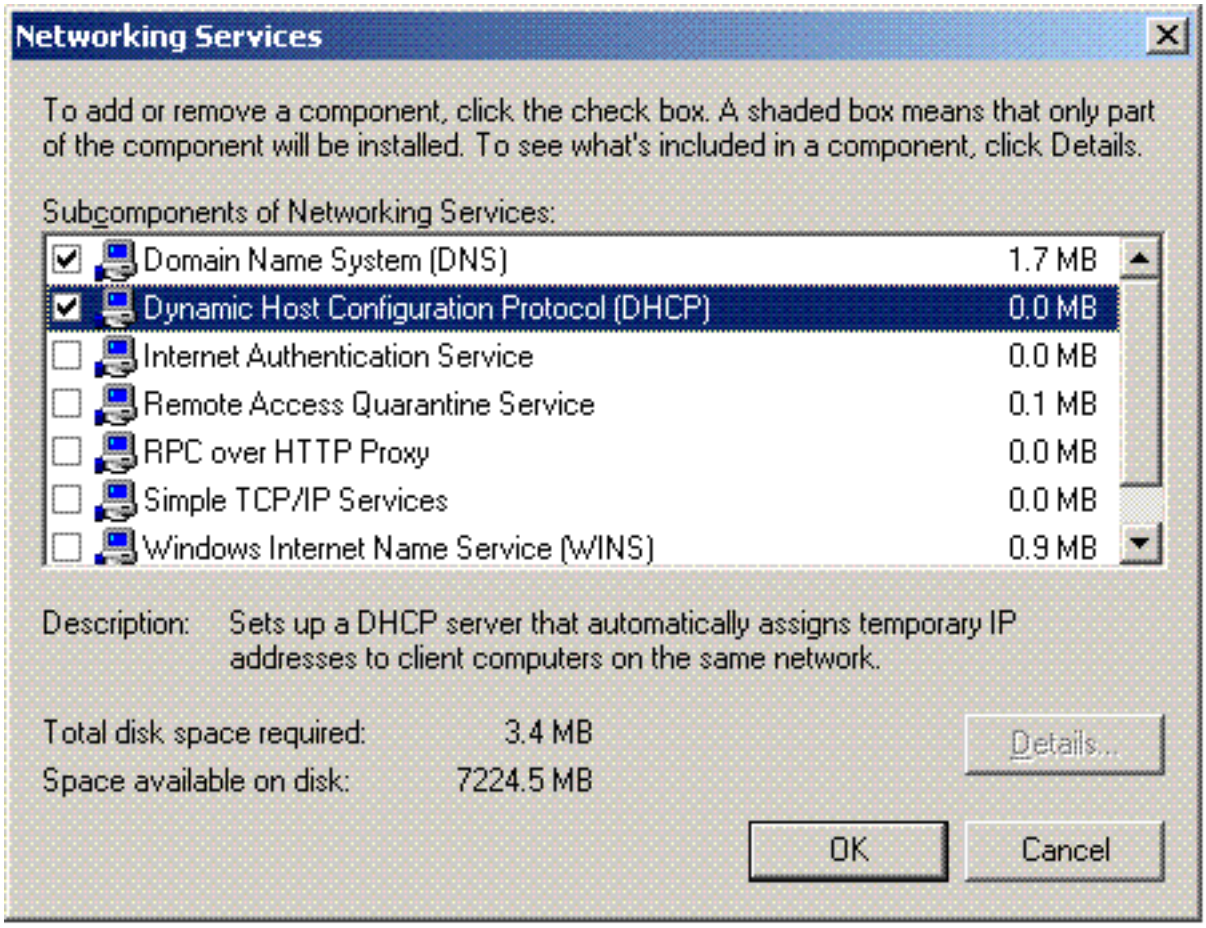
التغييرات.

بهذه الخطوة، قمت بتكوين خادم Microsoft Windows 2003 كوحدة تحكم بالمجال وإنشاء مجال جديد **Wireless.com**. بعد ذلك قم بتكوين خدمات DHCP على الخادم.

قم بتثبيت خدمات DHCP وتكوينها على خادم Microsoft Windows 2003

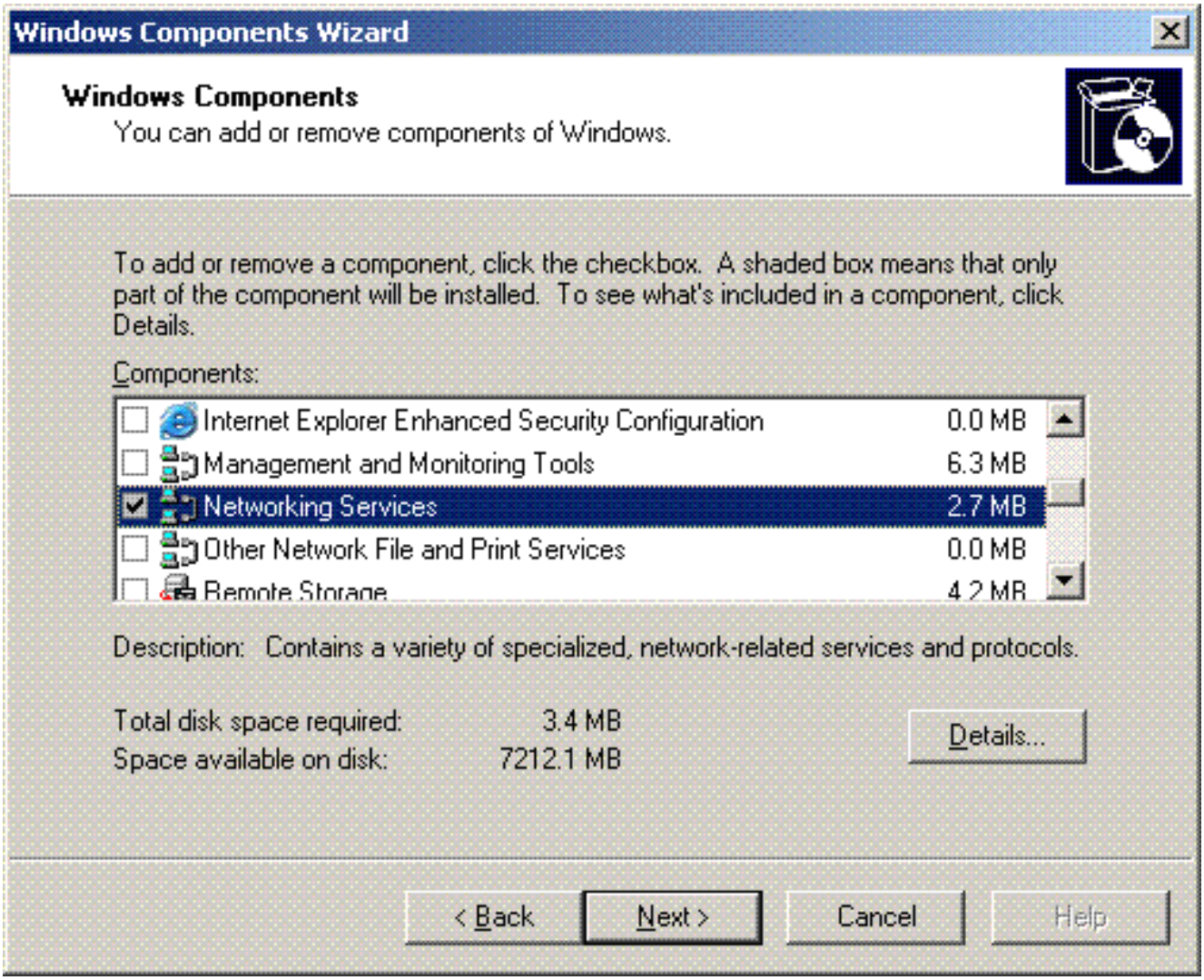
يتم إستخدام خدمة DHCP على خادم Microsoft 2003 لتوفير عناوين IP للعملاء اللاسلكيين. أتمت in order to ركبت وشكلت DHCP خدمة على هذا نادل، هذا steps:

1. انقر فوق **إضافة أو إزالة برامج** في لوحة التحكم.
2. انقر فوق **إضافة/إزالة مكونات Windows**.
3. أختر **خدمات الشبكة** وانقر فوق **تفاصيل**.
4. أخترت **حركي مضيف تشكيل بروتوكول (DHCP)** وطقطقة

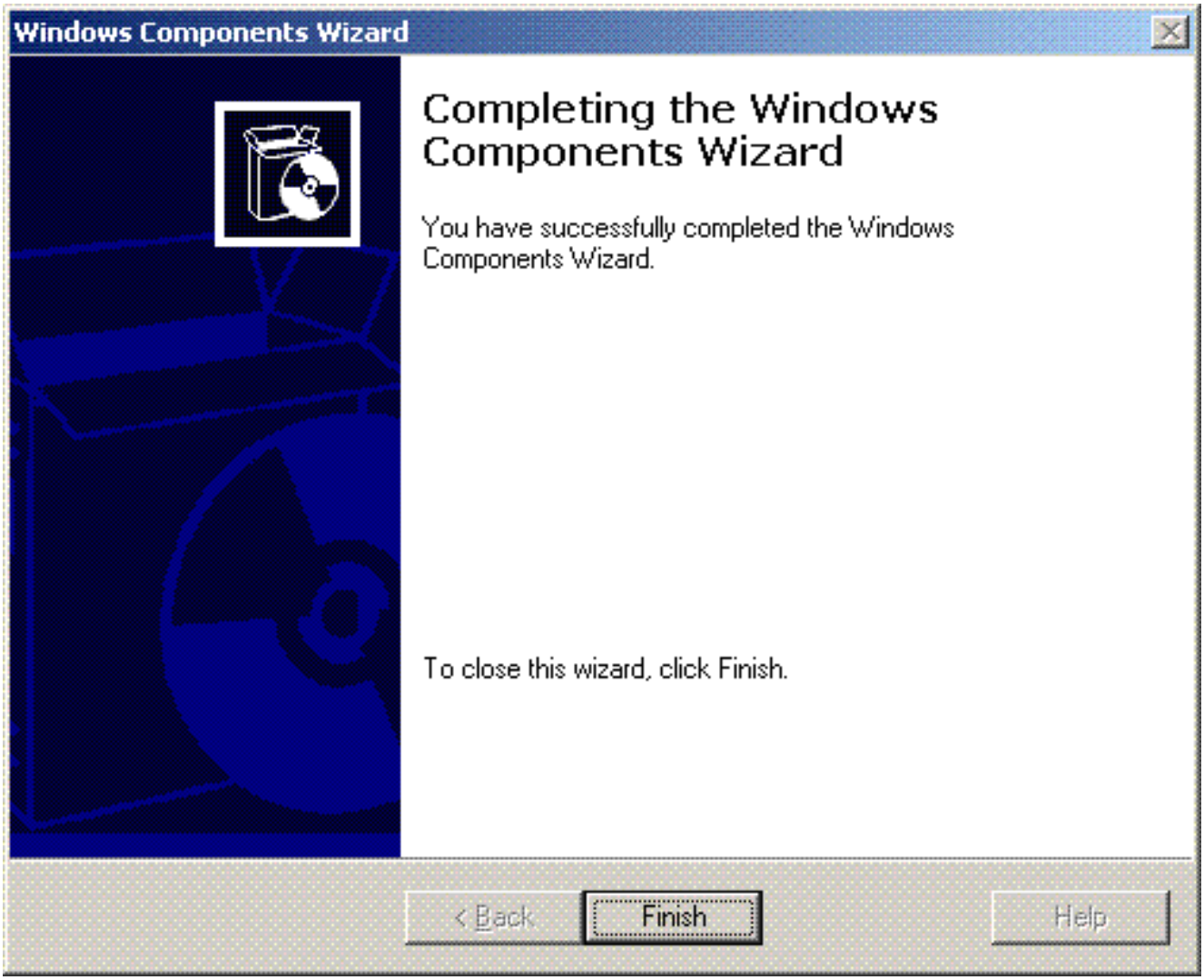


ok.

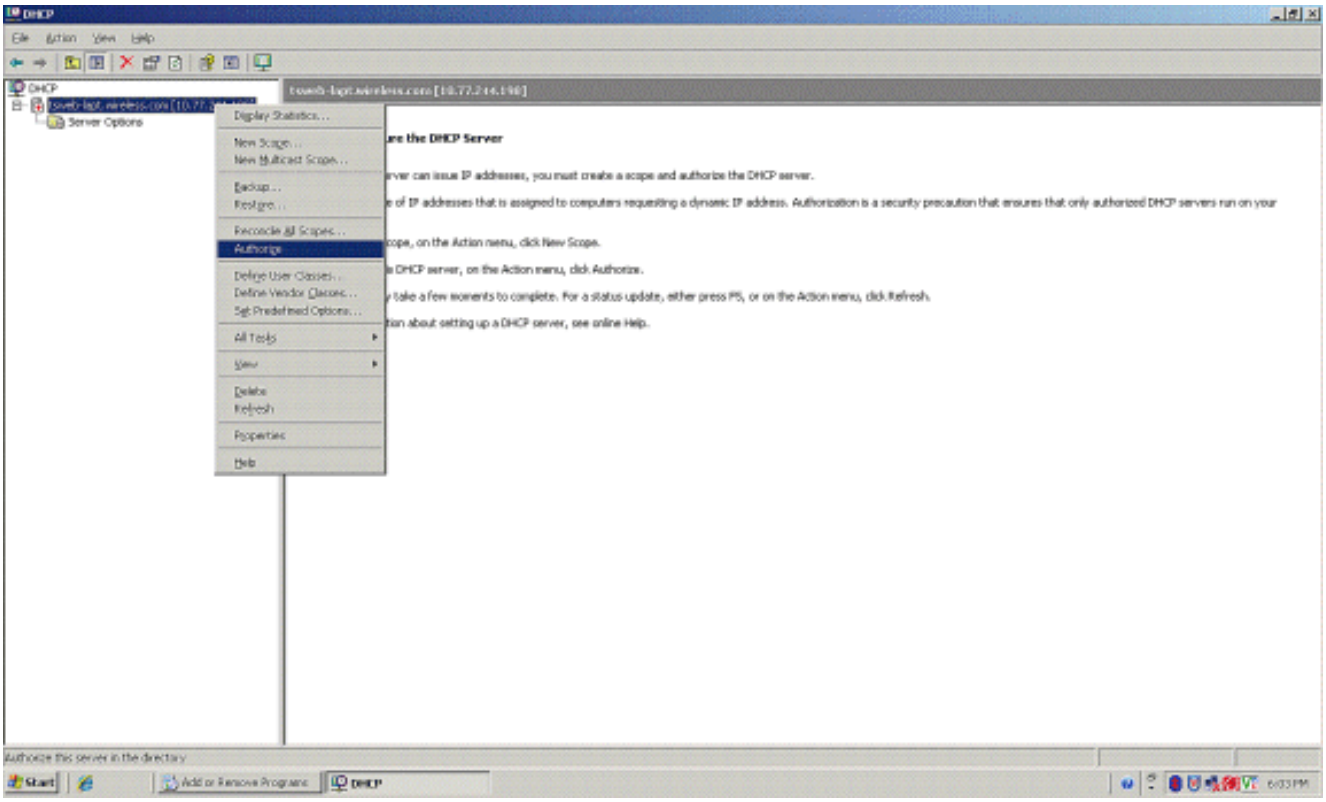
5. طقطقت **بعد ذلك** أن يركب ال DHCP خدمة.



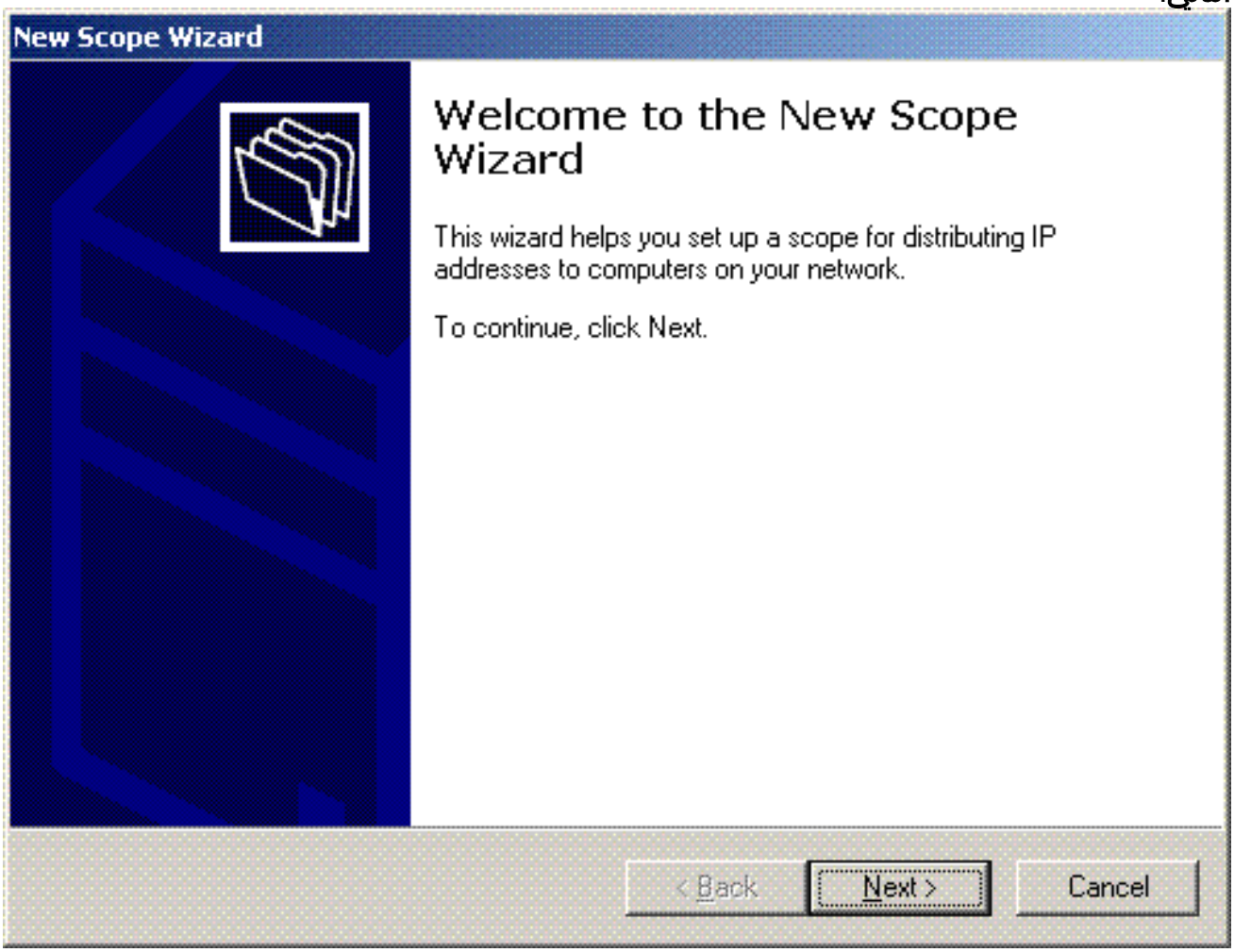
6. انقر فوق **إنهاء"** لإكمال التثبيت.



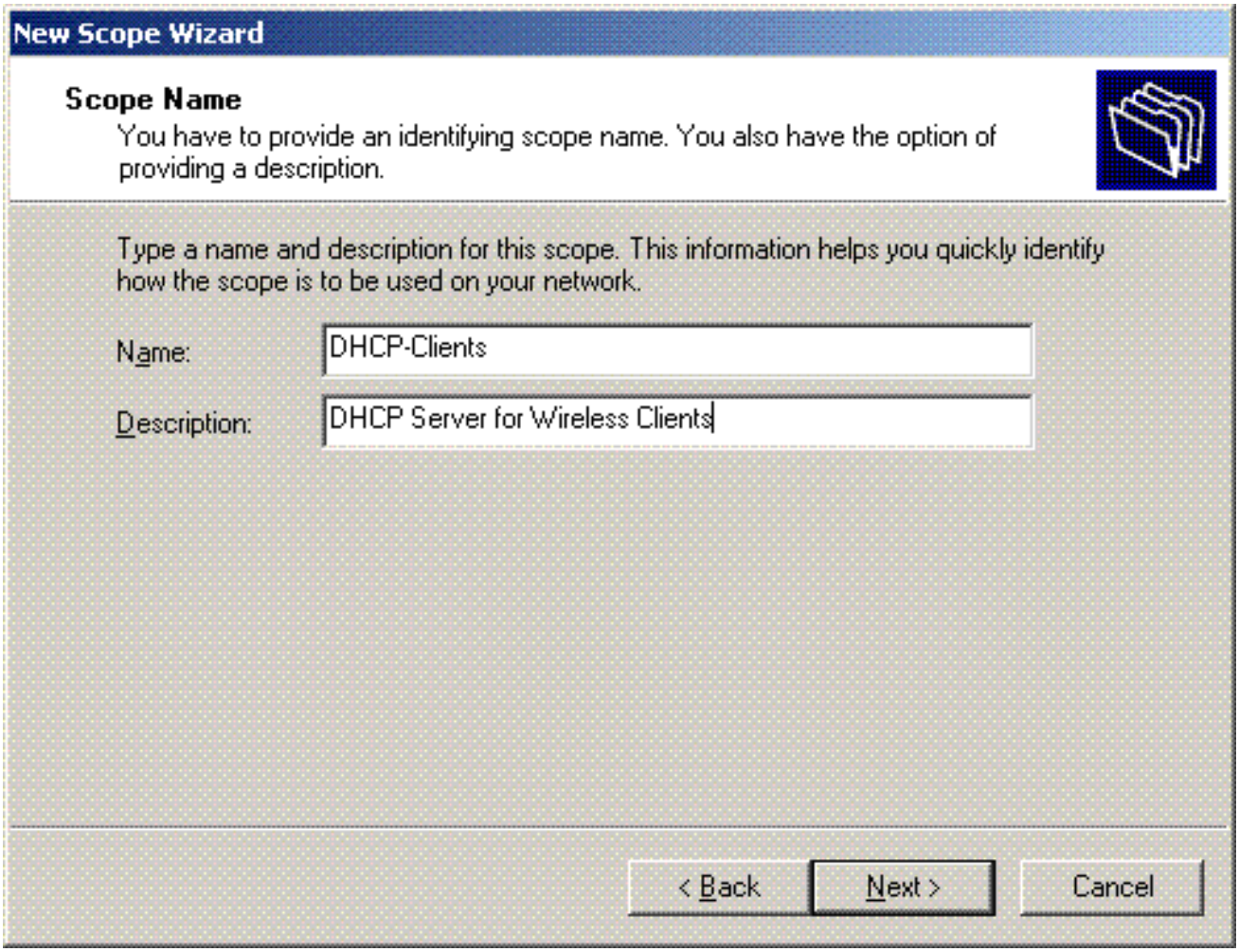
7. طقطقت in order to شكلت DHCP خدمة، **بداية>برنامج>أداة إداري** وطقطقت **ال DHCP** إضافي.
8. أخترت ال DHCP نادل - **tsweb-lapt.wireless.com** (في هذا مثال).
9. طقطقت **إجراء** وبعد ذلك طقطقت **يخول** أن يخول DHCP خدمة.



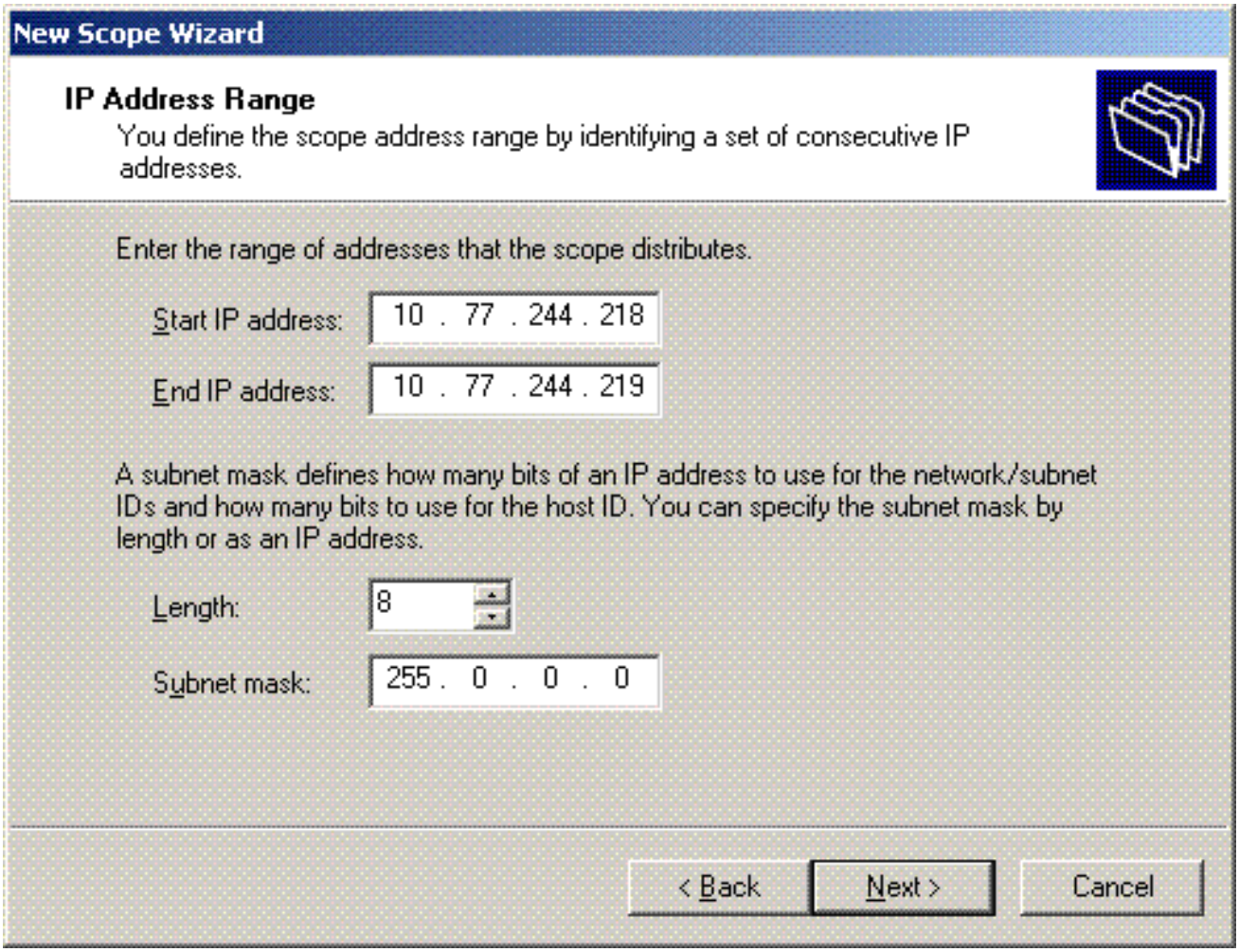
10. في شجرة وحدة التحكم، انقر بزر الماوس الأيمن فوق **tsweb-lapt.wireless.com** ثم انقر فوق **نطاق جديد** لتحديد نطاق عنوان IP للعملاء اللاسلكيين.
11. في صفحة "معالج نطاق جديد" لمعالج "نطاق جديد"، انقر فوق **التالي**.



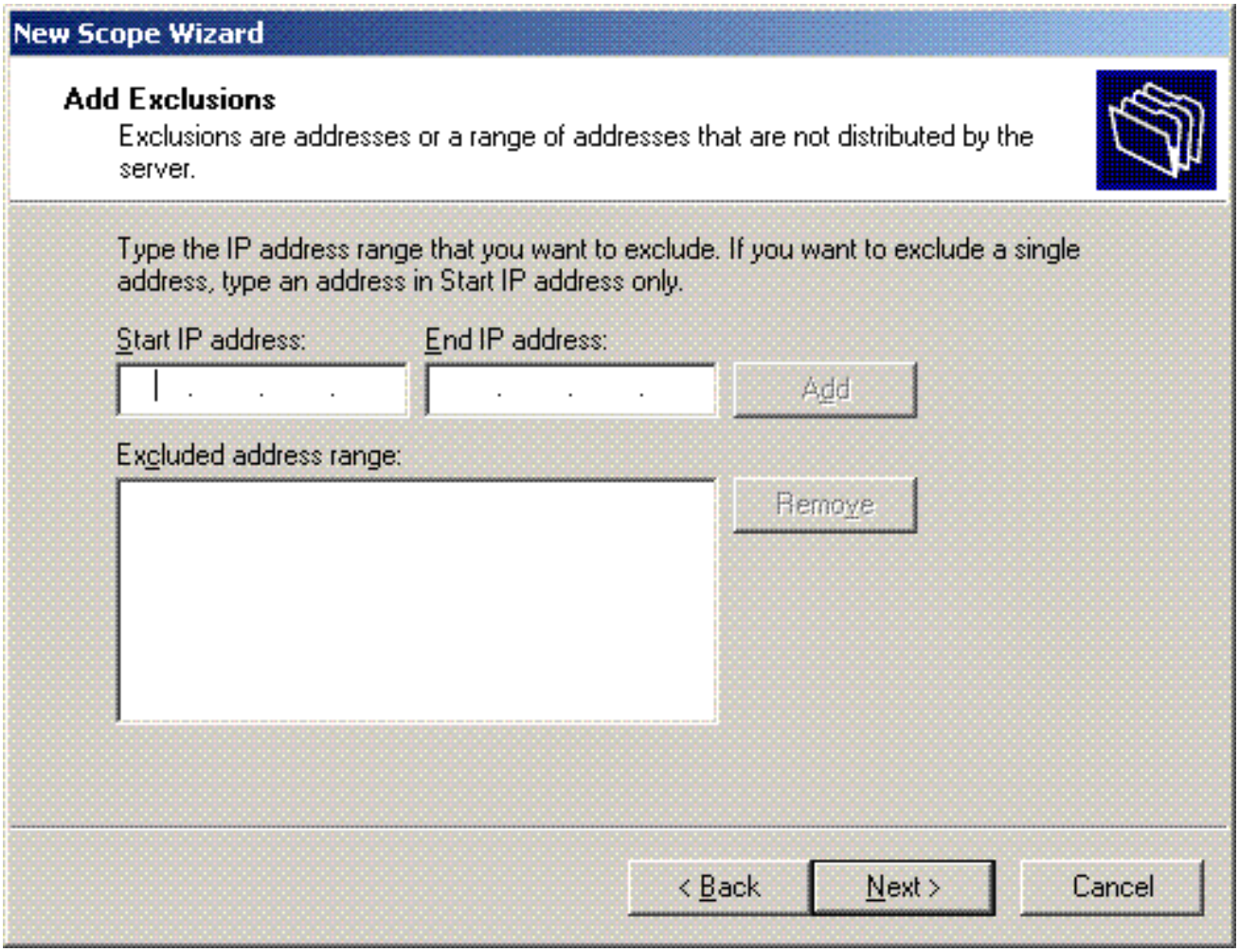
12. في صفحة اسم النطاق، اكتب اسم نطاق DHCP. في هذا المثال، أستخدم **عملاء DHCP** كاسم النطاق. انقر فوق **Next (التالي)**.



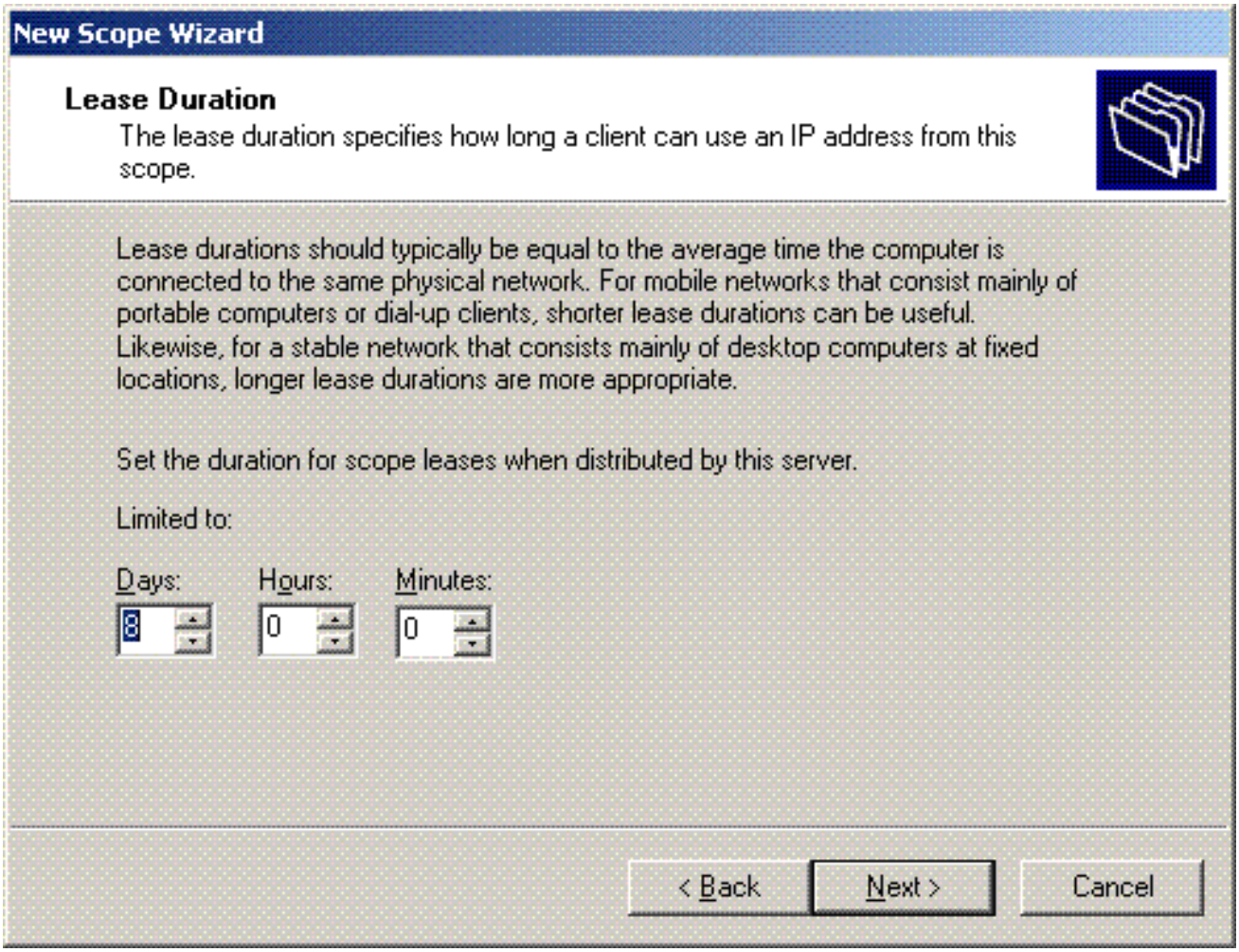
13. في صفحة نطاق عنوان IP، أدخل عناوين IP البداية والنهاية للنطاق، وانقر **التالي**.



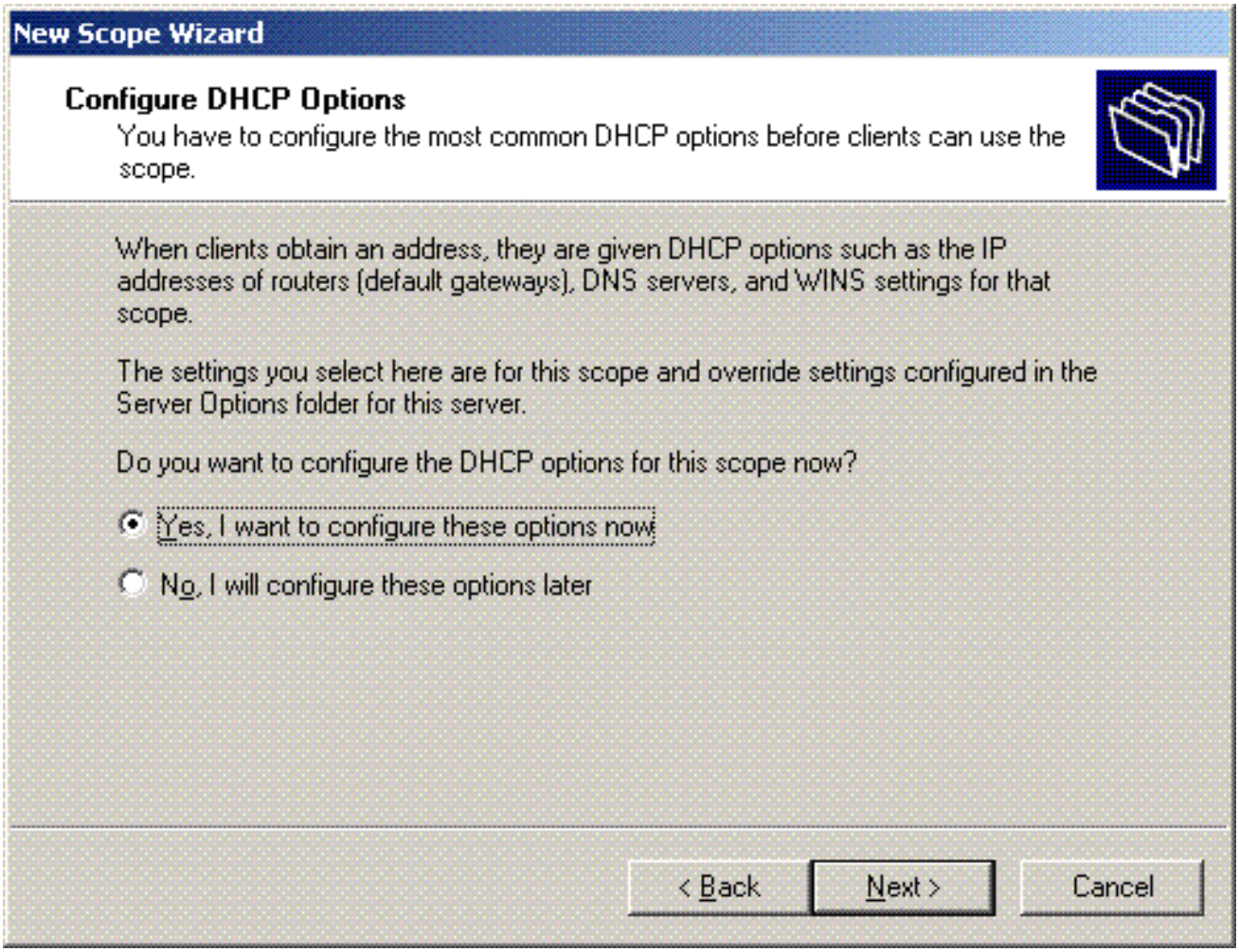
14. في صفحة إضافة الاستبعاد، أذكر عنوان IP الذي تريد حجزه/إستبعاده من نطاق DHCP. انقر فوق **Next (التالي)**.



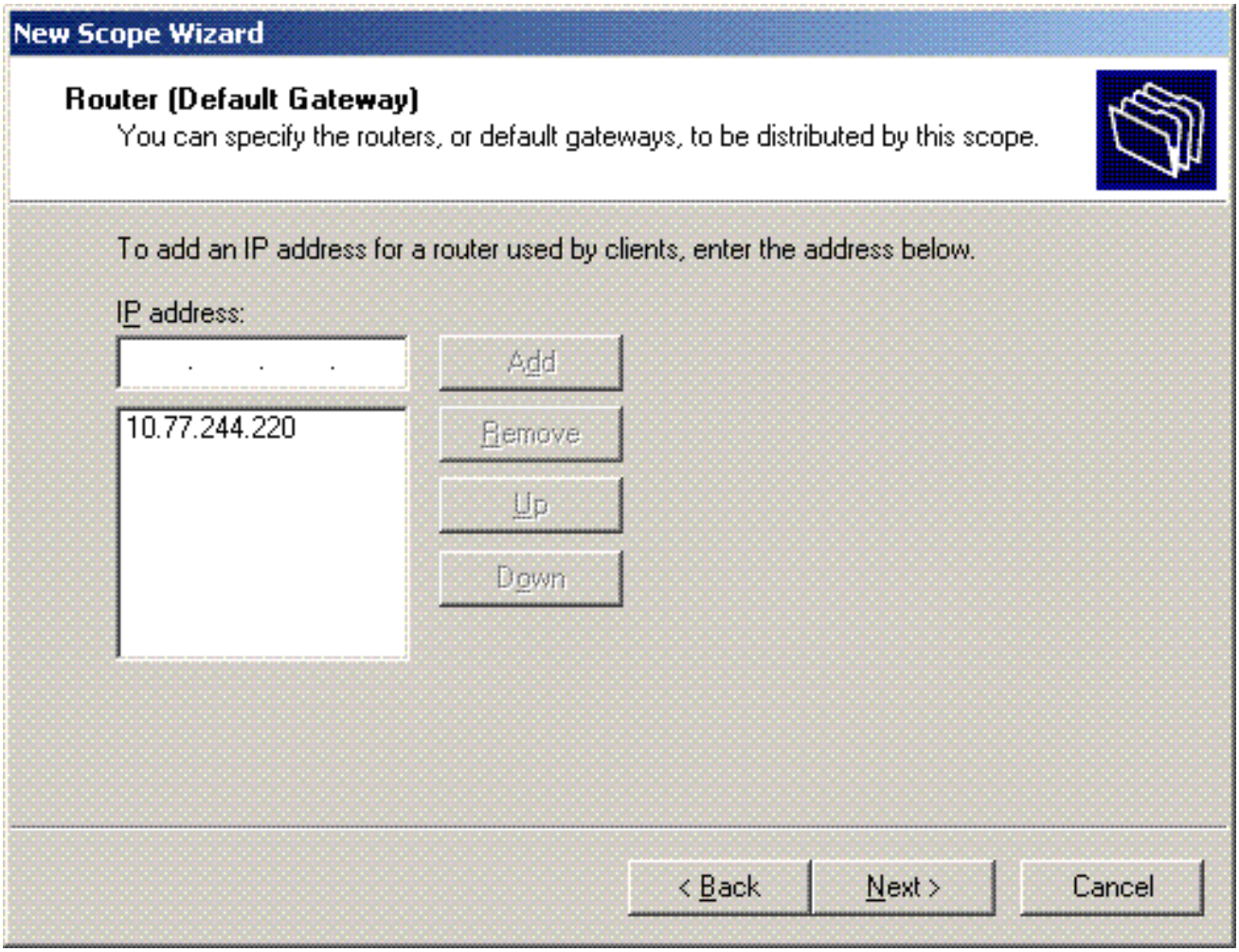
15. أذكر مدة التأجير في صفحة مدة التأجير، وانقر فوق **التالي**.



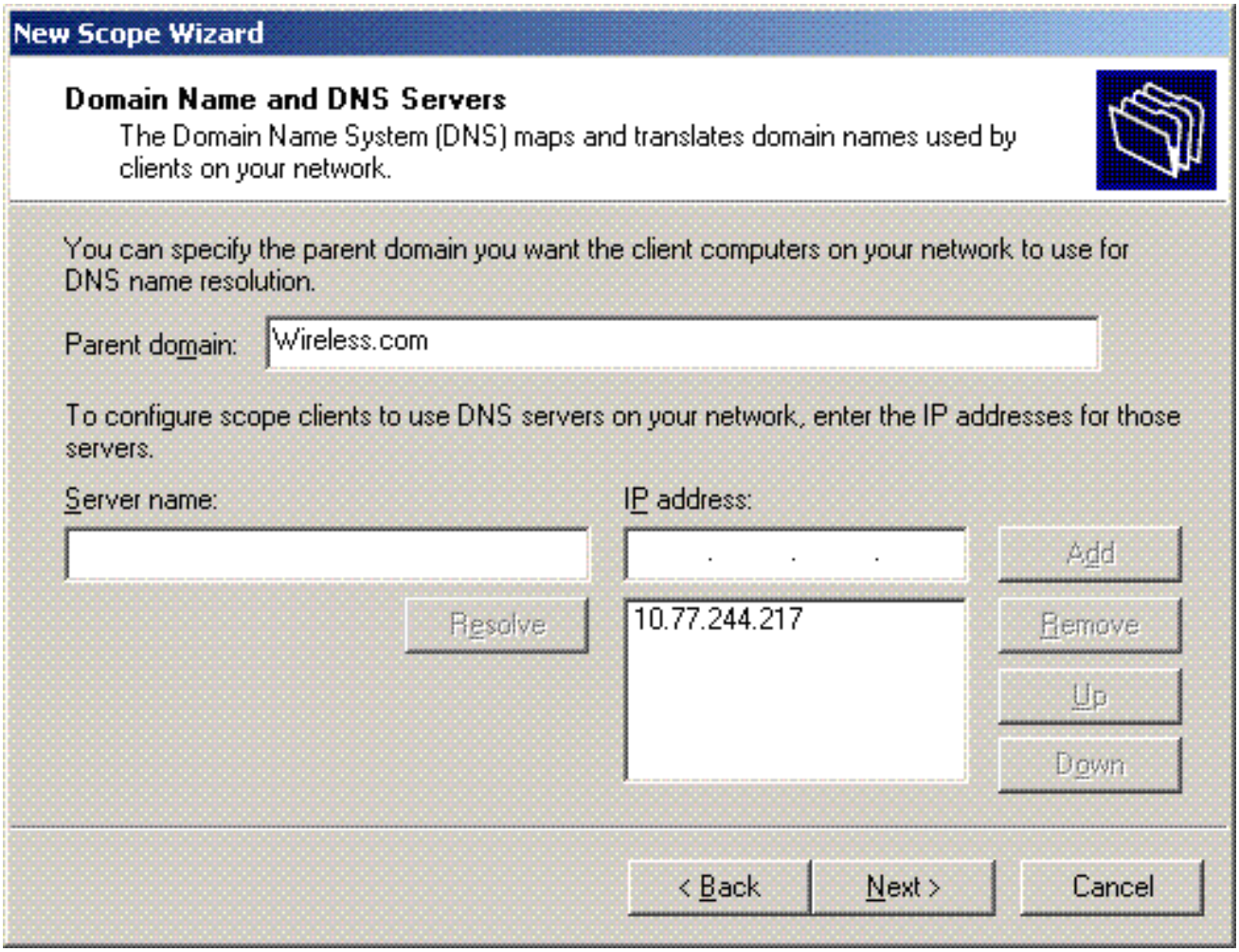
16. أخترت على ال configure DHCP خيار، **نعم، أنا أريد أن يشكل DHCP خيار الآن**، وطقطقة **بعد ذلك**.



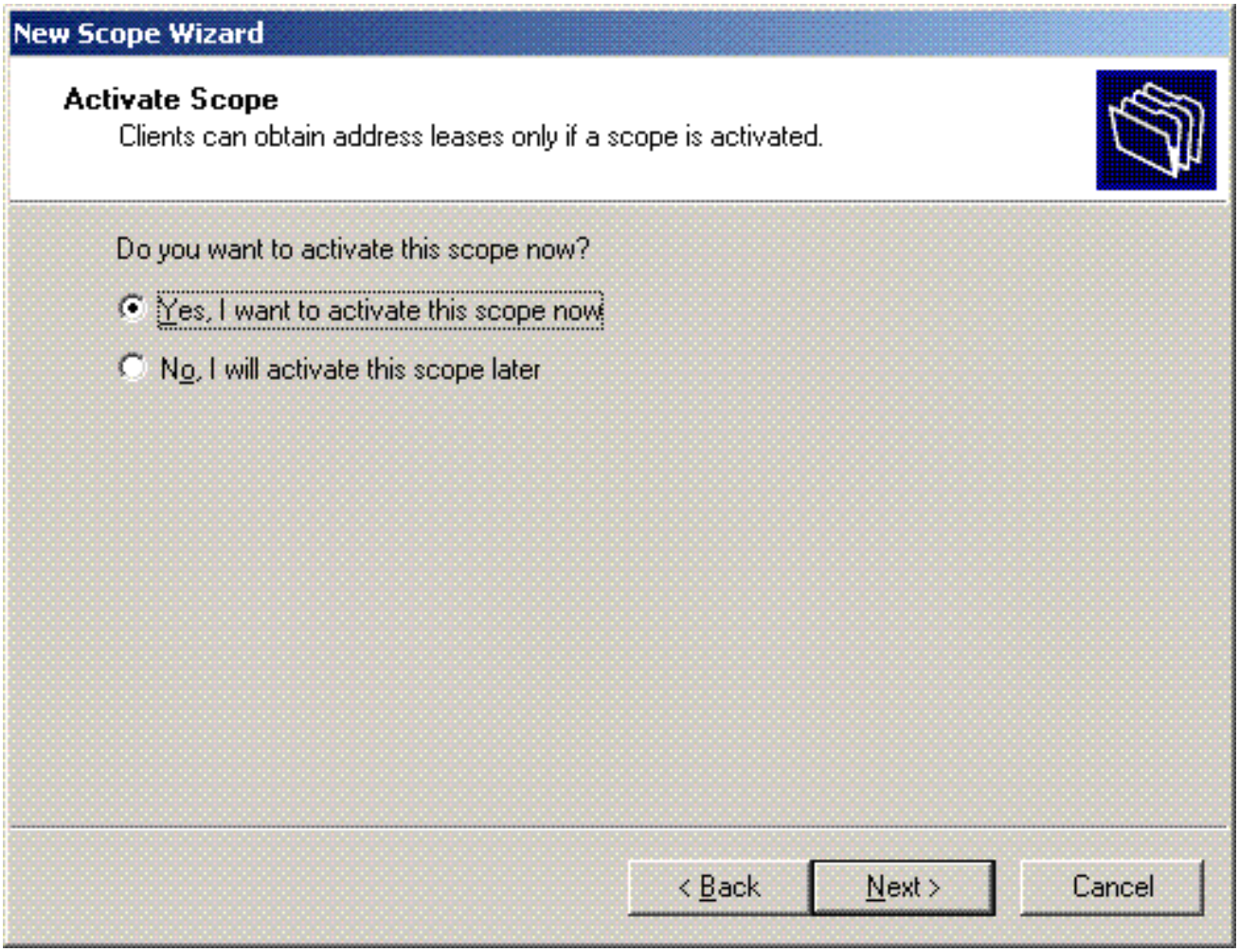
17. إذا كان هناك موجه عبارة افتراضي، فعليك الإشارة إلى عنوان IP الخاص بموجه العبارة في صفحة الموجه (البوابة الافتراضية)، وانقر فوق **التالي**.



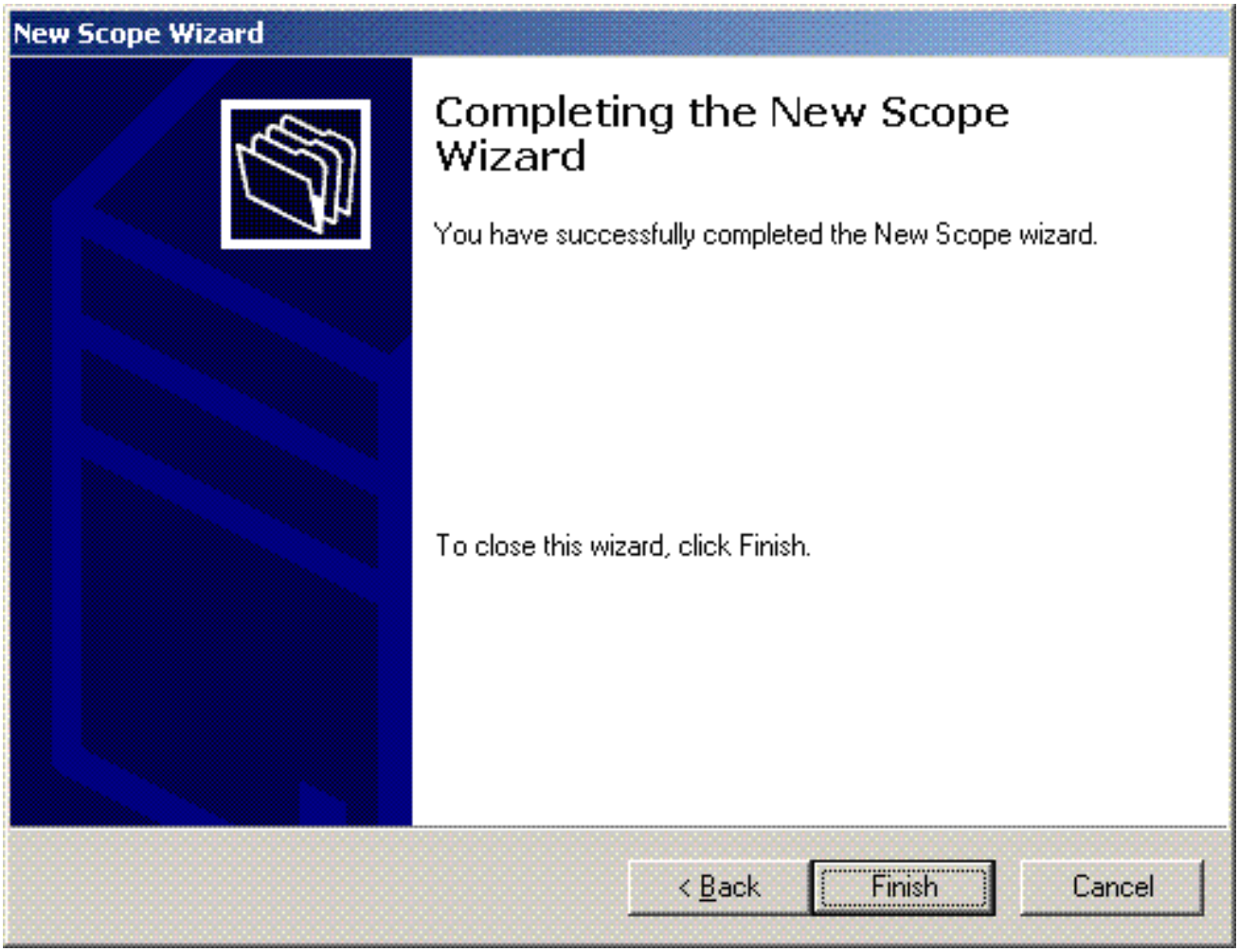
18. في الصفحة اسم المجال وخوادم DNS، اكتب اسم المجال الذي تم تكوينه مسبقا. في المثال، أستخدم **Wireless.com**. أدخل عنوان IP الخاص بالخادم. انقر فوق **إضافة (Add)**.



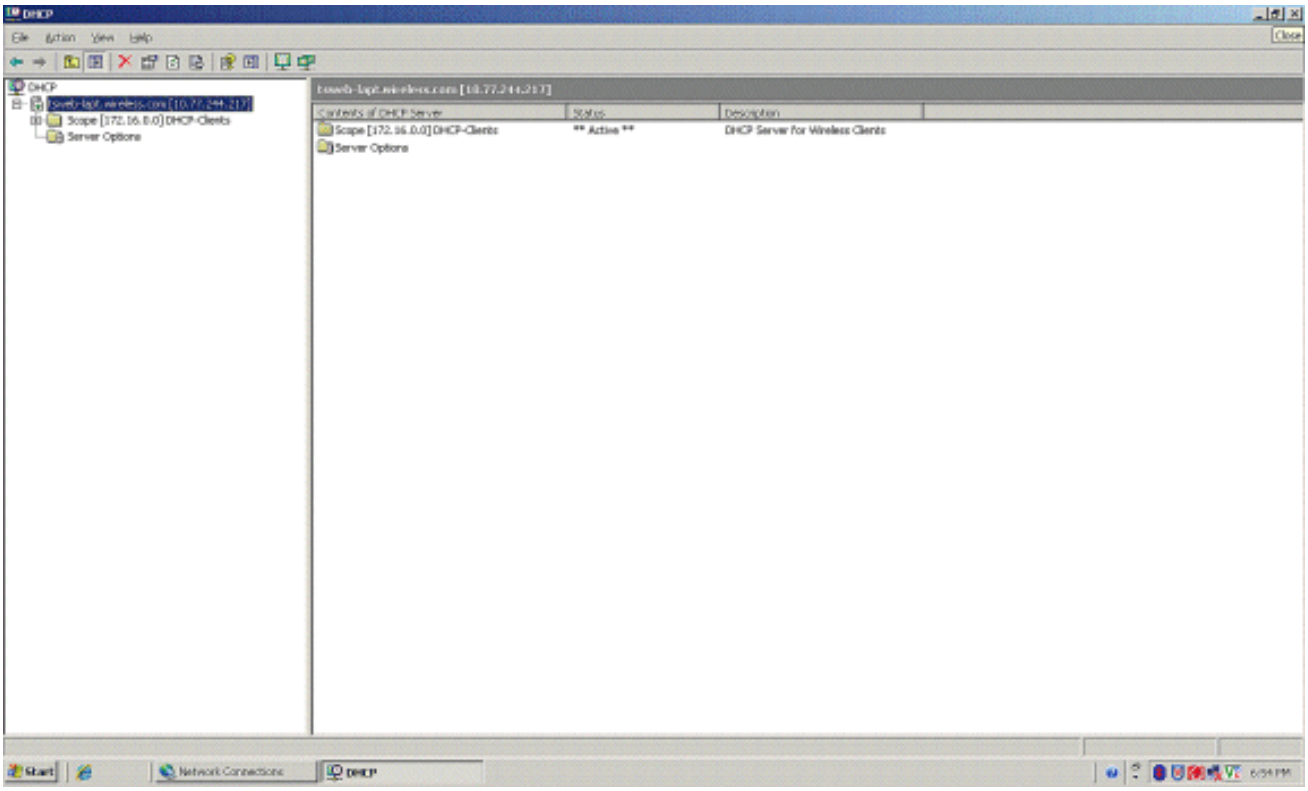
19. انقر فوق **Next (التالي)**.
20. في صفحة خادم WINS، انقر فوق **التالي**.
21. في صفحة "تنشيط النطاق"، أختر **نعم، أريد تنشيط النطاق الآن**، وانقر فوق **التالي**.



22. عند إكمال معالج نطاق جديد، انقر فوق **إنهاء**.



23. في نافذة نافذة DHCP الإضافية، تحقق من أن نطاق DHCP الذي تم إنشاؤه نشط.



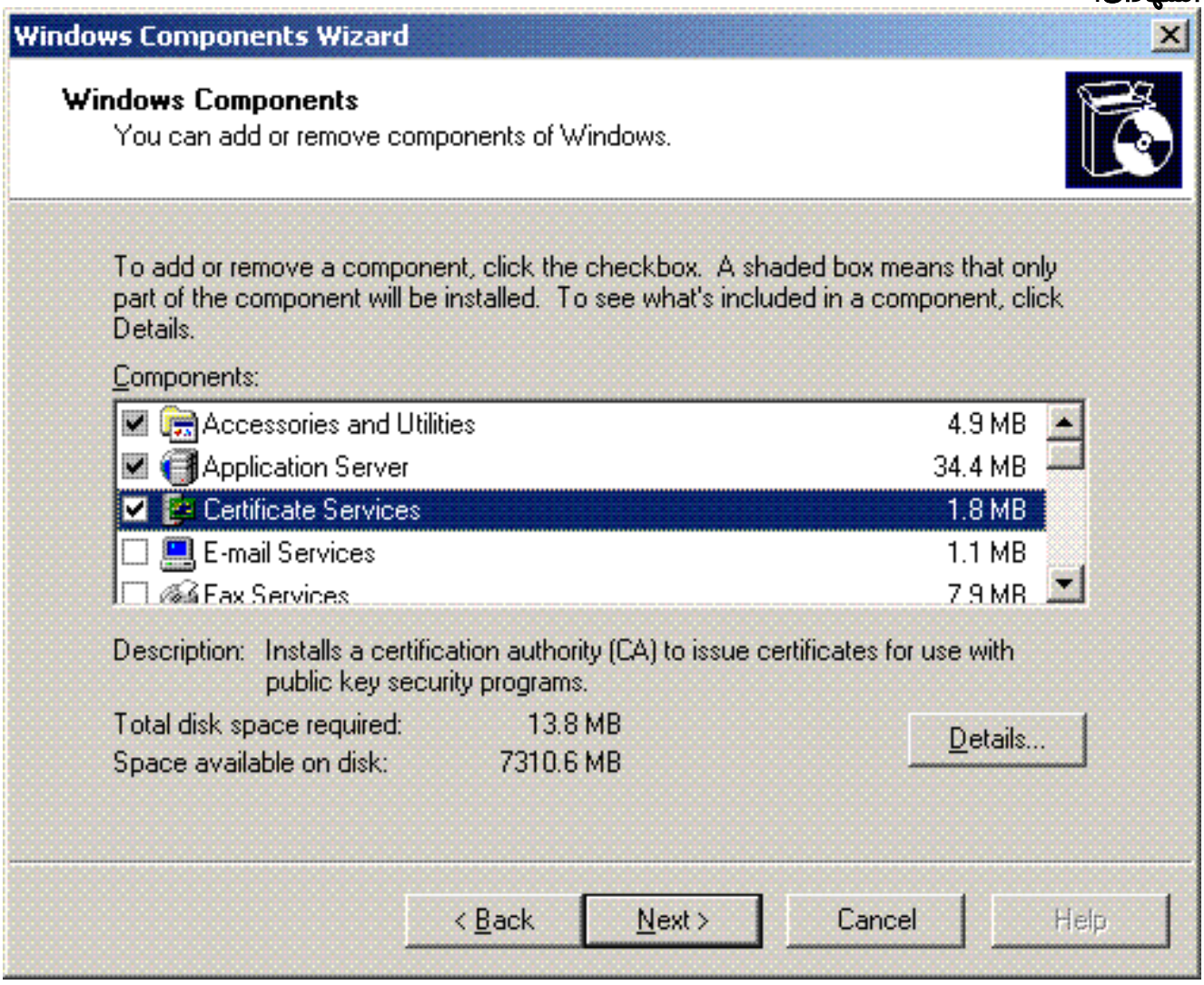
الآن بعد تمكين DHCP/ DNS على الخادم، قم بتكوين الخادم كخادم مرجع مصدق للمؤسسة (CA).

تثبيت خادم Microsoft Windows 2003 وتكوينه كخادم مرجع شهادات (CA)

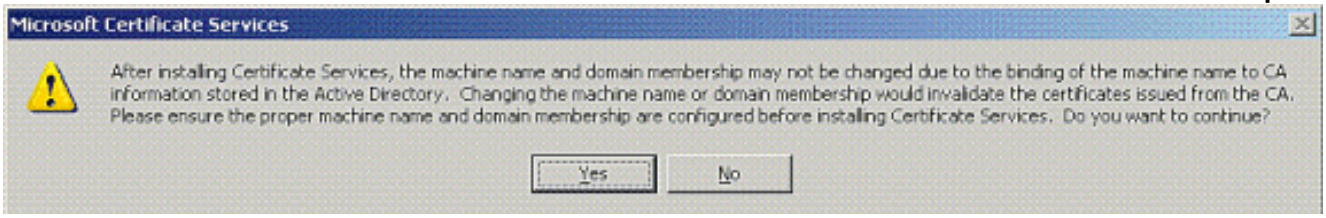
يقوم PEAP مع EAP-MS-CHAPv2 بالتحقق من خادم RADIUS بناء على الشهادة الموجودة على الخادم. بالإضافة إلى ذلك، يجب إصدار شهادة الخادم من قبل مرجع مصدق عام (CA) موثوق به من قبل كمبيوتر العميل (أي أن شهادة المرجع المصدق العام موجودة بالفعل في مجلد مرجع التصديق الجذر الموثوق به الموجود في مخزن شهادات الكمبيوتر العميل). في هذا المثال، قم بتكوين خادم Microsoft Windows 2003 كمرجع مصدق (CA) يصدر الشهادة إلى خدمة مصادقة الإنترنت (IAS).

لتثبيت خدمات الشهادات وتكوينها على الخادم، أكمل الخطوات التالية:

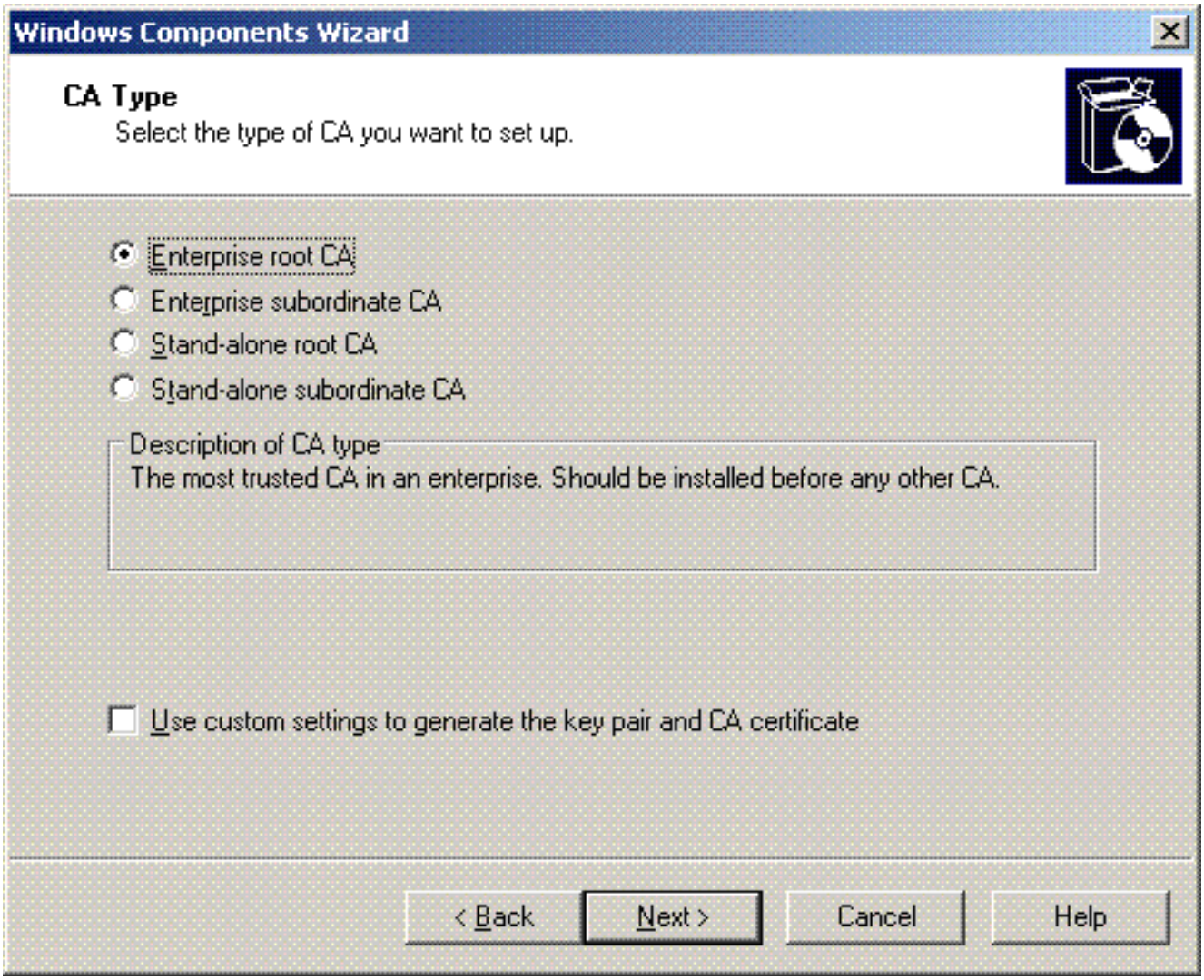
1. انقر فوق **إضافة أو إزالة برامج في لوحة التحكم**.
2. انقر فوق **إضافة/إزالة مكونات Windows**.
3. انقر على **خدمات الشهادات**.



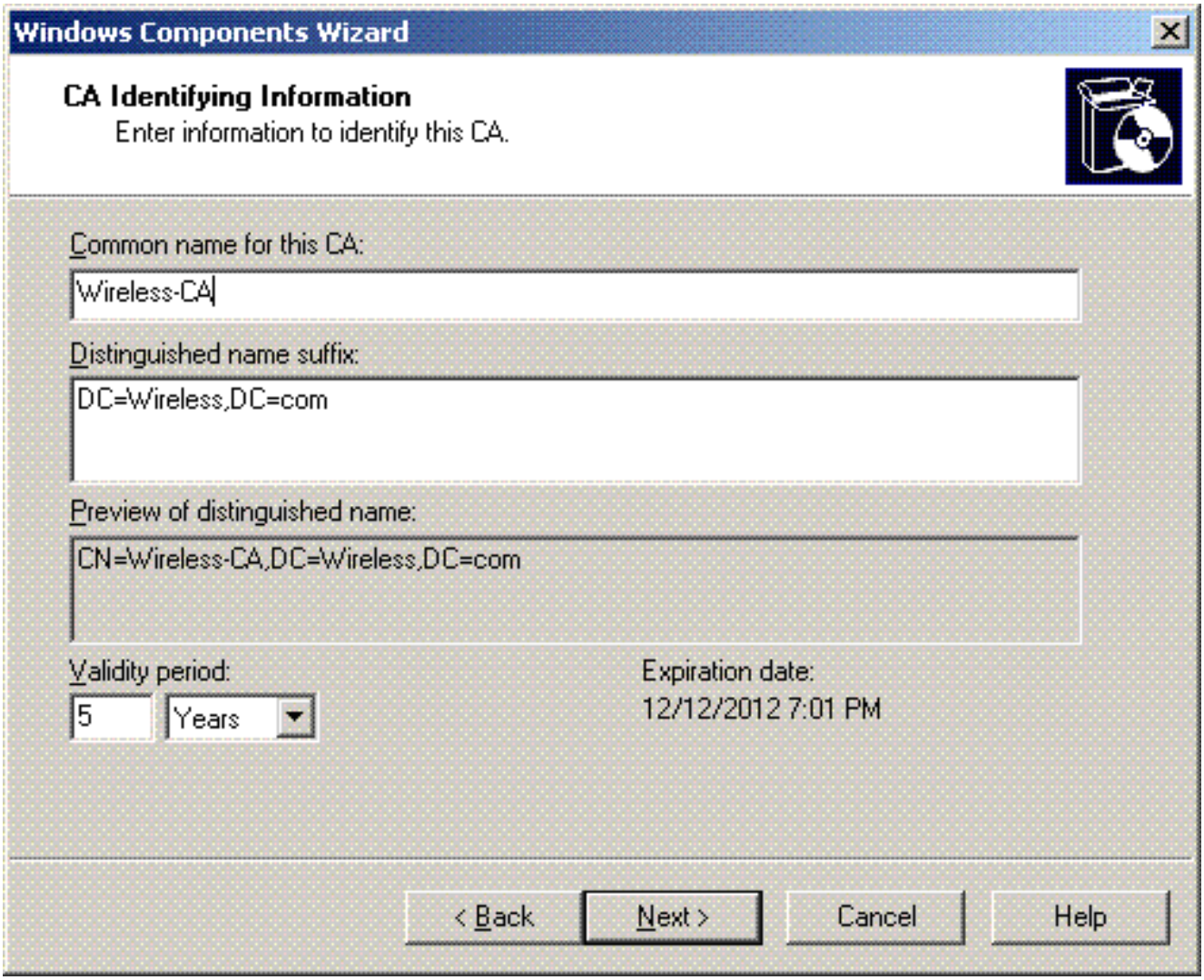
4. انقر فوق **نعم** إلى رسالة التحذير، **بعد تثبيت "خدمات الشهادات"، لا يمكن إعادة تسمية الكمبيوتر ويتعذر على الكمبيوتر الانضمام إلى مجال أو إزالته منه. هل تريد المتابعة؟**



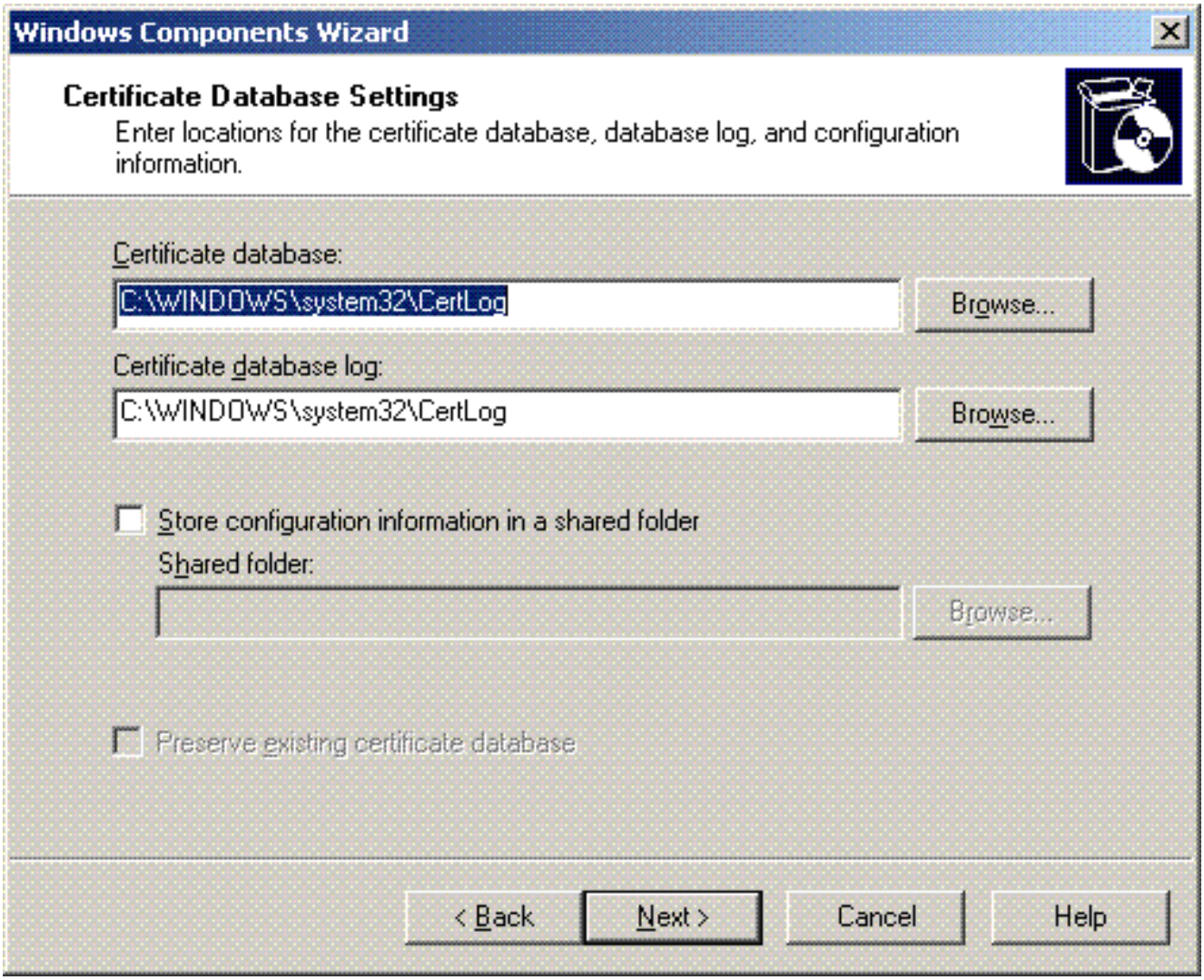
5. تحت نوع المرجع المصدق، أختر **المرجع المصدق الجذر للمؤسسة**، وانقر **بعد ذلك**.



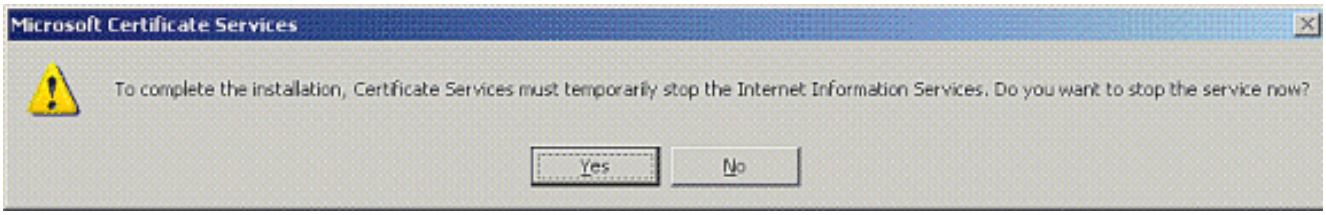
6. أدخل اسما لتعريف المرجع المصدق. يستخدم هذا المثال **Wireless-CA**. انقر فوق **Next (التالي)**.



7. يتم إنشاء دليل "سجل الشهادات" لتخزين قاعدة بيانات الشهادات. انقر فوق **Next (التالي)**.



8. إذا تم تمكين IIS، يجب إيقافه قبل المتابعة. انقر فوق **موافق"** إلى رسالة التحذير التي تشير إلى وجوب إيقاف IIS. تتم إعادة تشغيله تلقائيا بعد تثبيت CA.



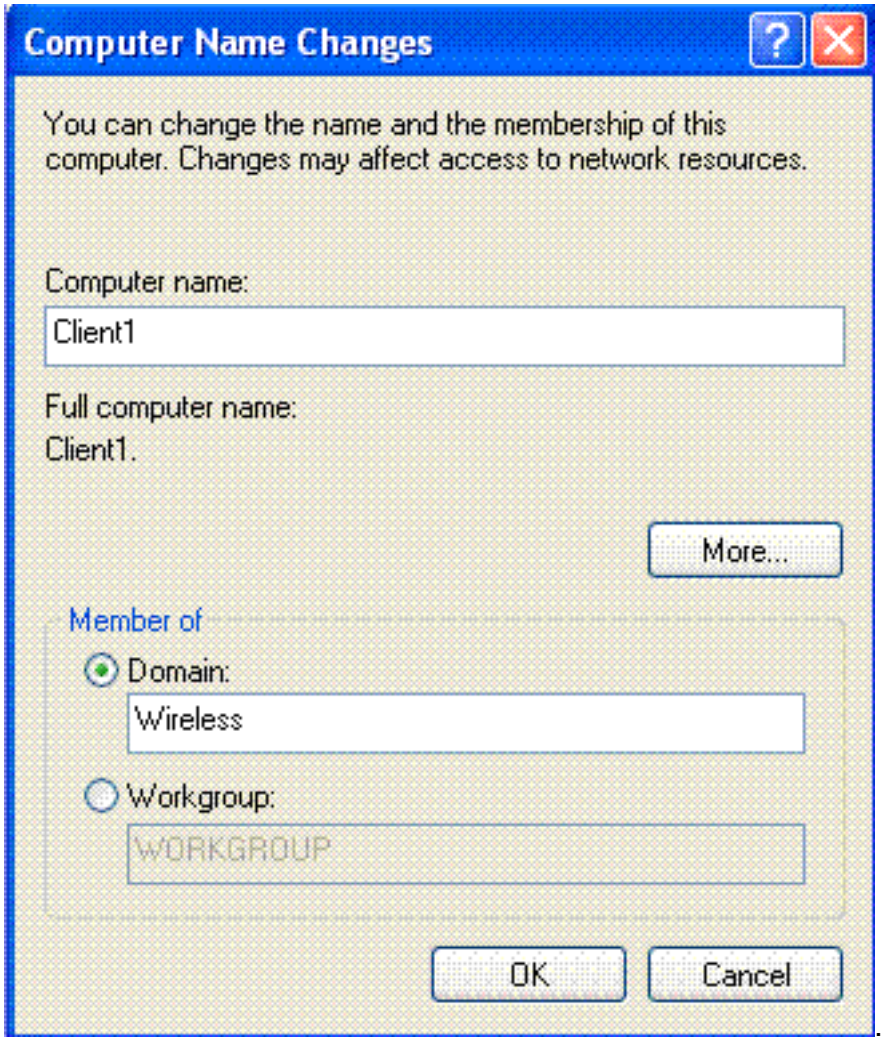
9. انقر على **إنهاء** لإكمال تثبيت خدمات المرجع المصدق (CA).

تتمثل الخطوة التالية في تثبيت خدمة مصادقة الإنترنت وتكوينها على خادم Microsoft Windows 2003.

توصيل العملاء بالمجال

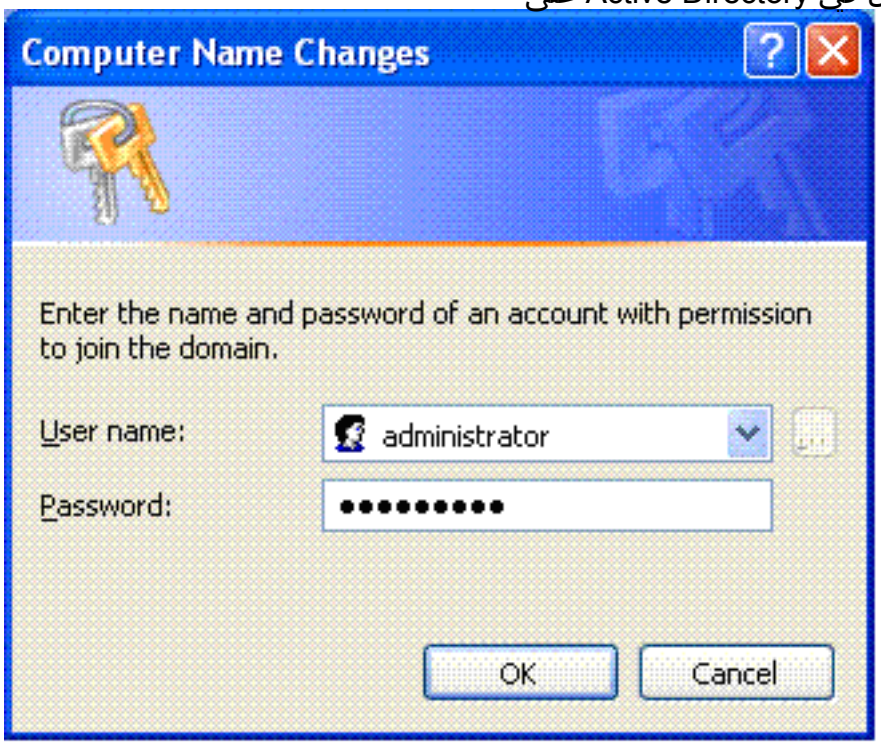
تتمثل الخطوة التالية في توصيل العملاء بالشبكة السلكية وتنزيل المعلومات الخاصة بالمجال من المجال الجديد. بمعنى آخر، قم بتوصيل العملاء بالمجال. للقيام بذلك، أكمل الخطوات التالية:

1. قم بتوصيل العملاء بالشبكة السلكية باستخدام كبل توصيل متناظر عبر شبكة إيثرنت.
2. قم بتحميل العميل وتسجيل الدخول باستخدام اسم المستخدم/كلمة المرور الخاصة بالعميل.
3. انقر فوق **بدء**؛ وانقر فوق **تشغيل**؛ واكتب **cmd**؛ وانقر فوق **موافق**.
4. في موجه الأمر، اكتب **ipconfig**، وانقر فوق **enter** للتحقق من عمل DHCP بشكل صحيح واستلم العميل عنوان IP من خادم DHCP.
5. لربط العميل بالمجال، انقر بزر الماوس الأيمن فوق **الكمبيوتر**، واختر **خصائص**.
6. انقر على علامة التبويب **اسم الكمبيوتر**.
7. طقطقة **تغير**.
8. انقر فوق **مجال**؛ واكتب **wireless.com**؛ وانقر فوق



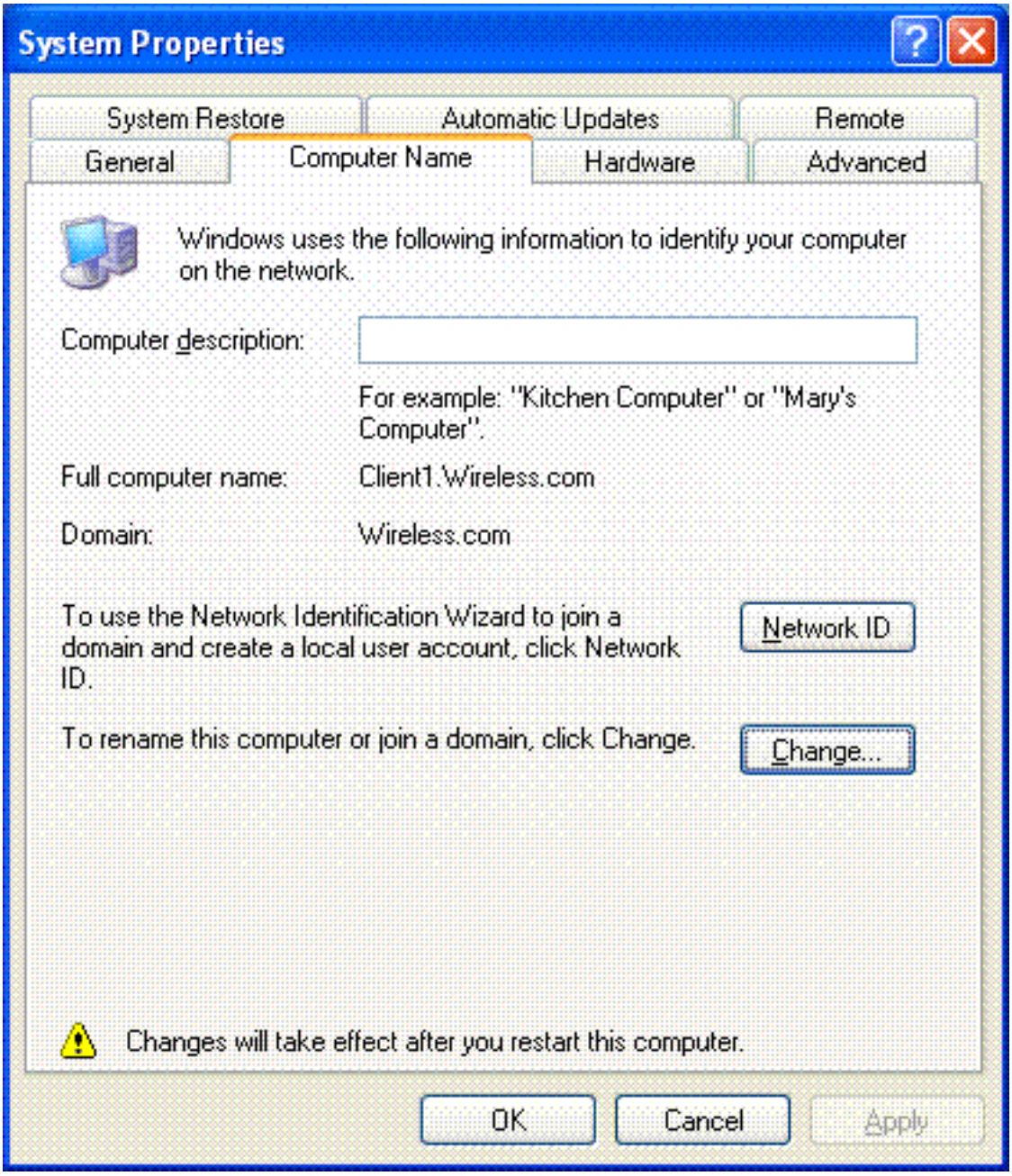
موافق.

9. اكتب **username administrator** وكلمة المرور الخاصة بالمجال الذي ينضم إليه العميل. (هذا هو حساب المسؤول في Active Directory على

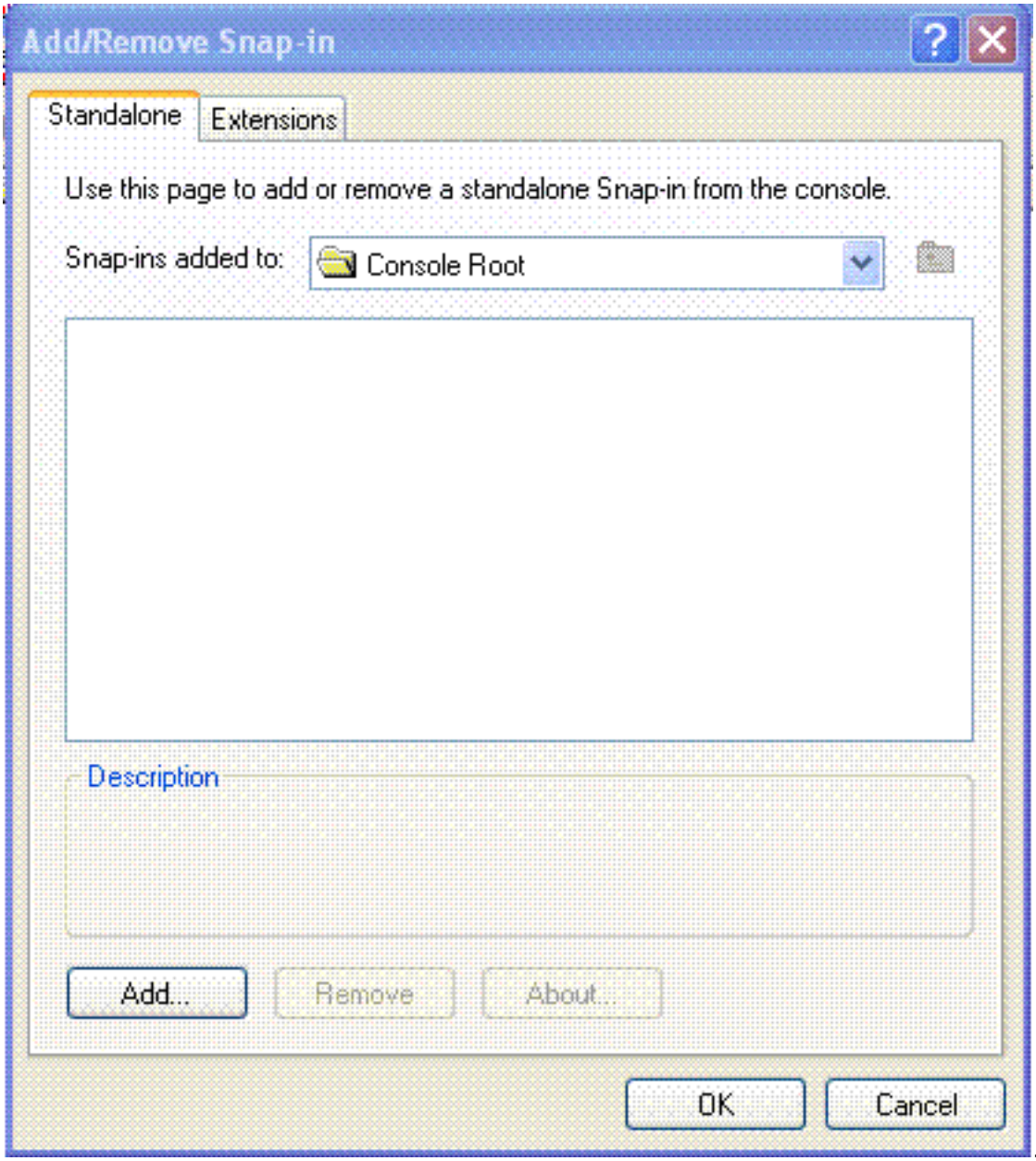


الخادم.)

10. وانقر فوق **OK**.
11. انقر فوق **نعم** لإعادة تشغيل الكمبيوتر.
12. بمجرد إعادة تشغيل الكمبيوتر، قم بتسجيل الدخول باستخدام هذه المعلومات: اسم المستخدم = **المسؤول**؛ كلمة المرور = **<كلمة مرور المجال>**؛ المجال = **لاسلكي**.
13. انقر بزر الماوس الأيمن فوق **الكمبيوتر**، ثم انقر فوق **خصائص**.
14. انقر فوق علامة التبويب **اسم الكمبيوتر** للتحقق من أنك في المجال Wireless.com.

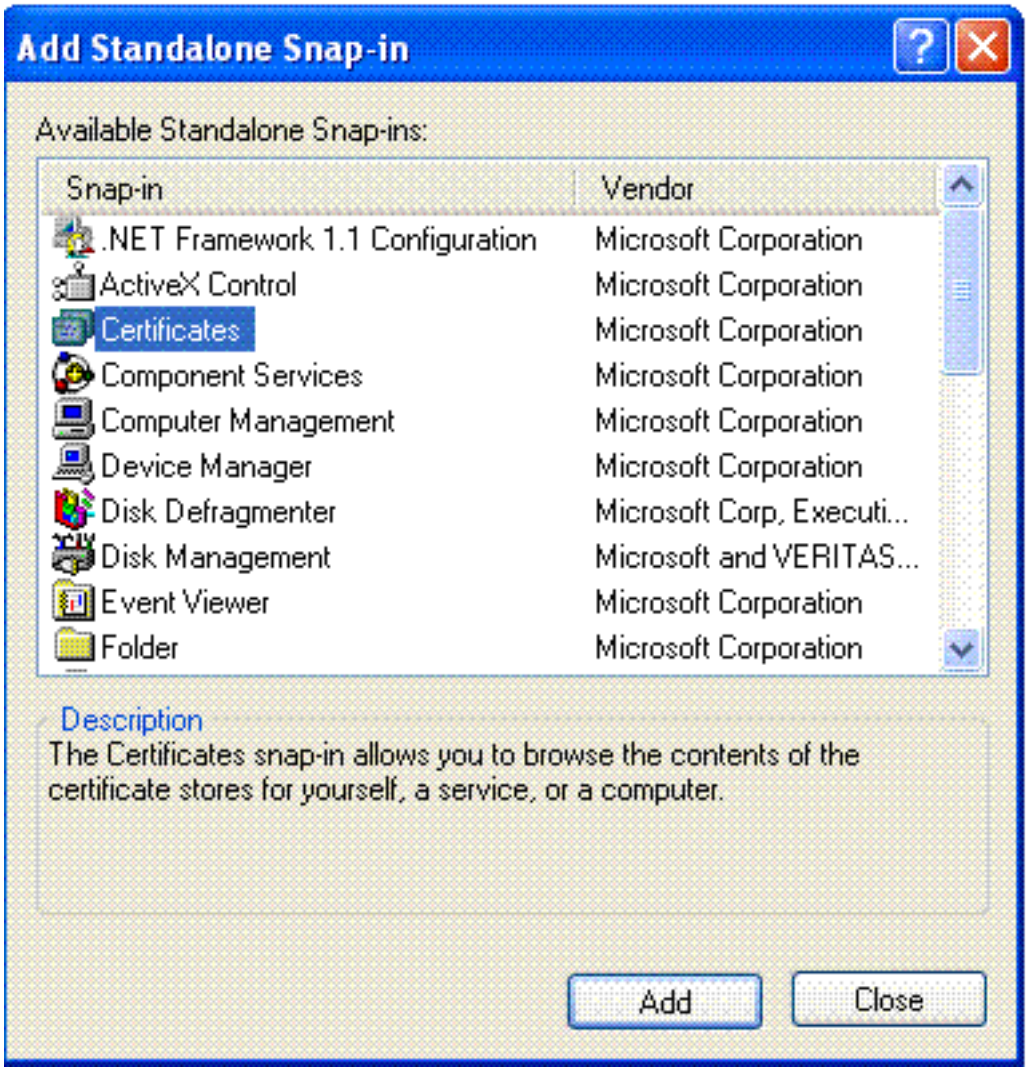


15. تتمثل الخطوة التالية في التحقق من تلقي العميل لشهادة CA (الثقة) من الخادم.
16. انقر فوق **بدء**؛ وانقر فوق **تشغيل**؛ واكتب **mmc**، وانقر فوق **موافق**.
17. انقر **ملف**، وانقر **إضافة/إزالة** الأداة



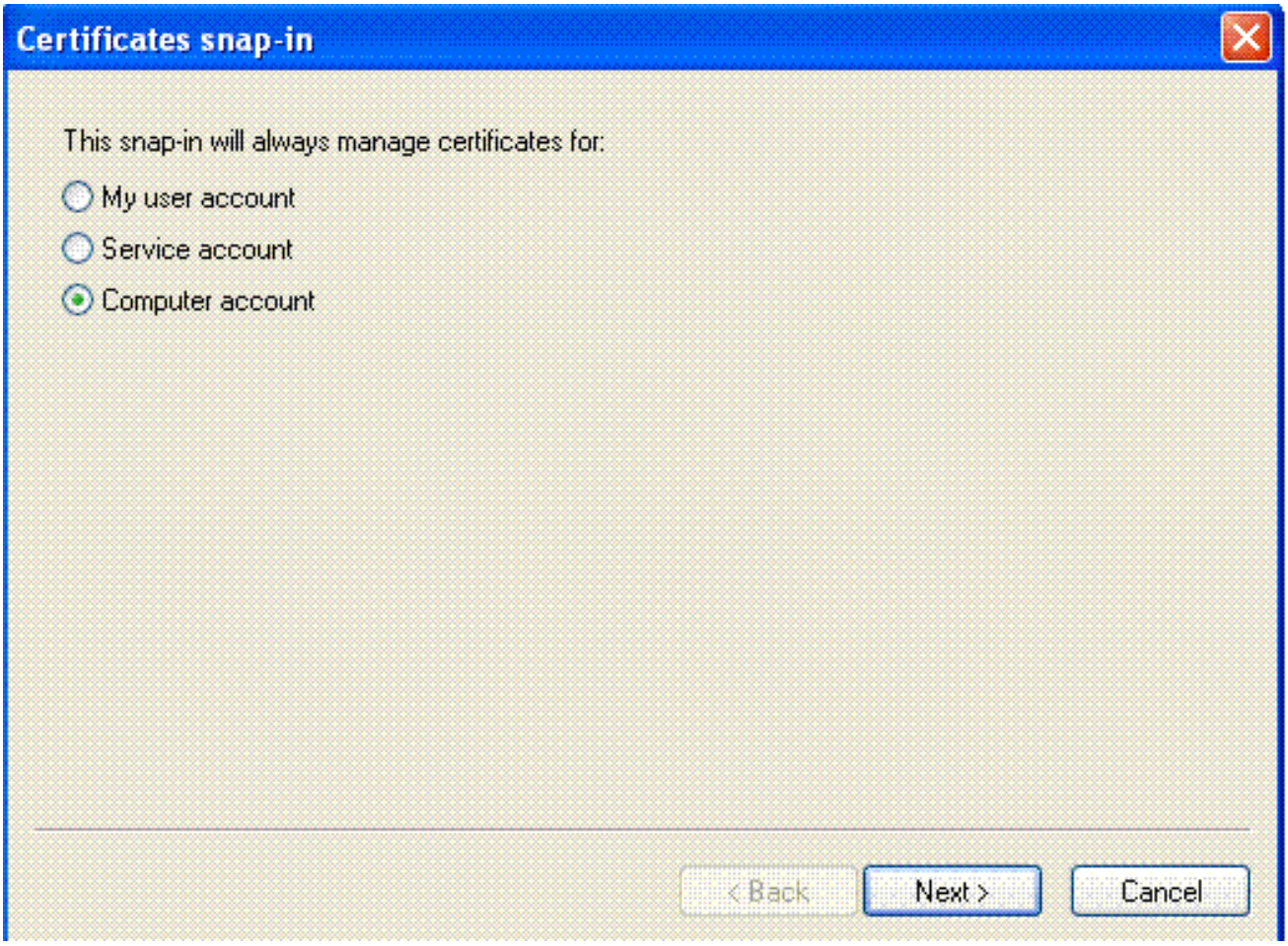
الإضافية.

18. انقر فوق **إضافة (Add)**.
19. أختر **ترخيص**، وانقر

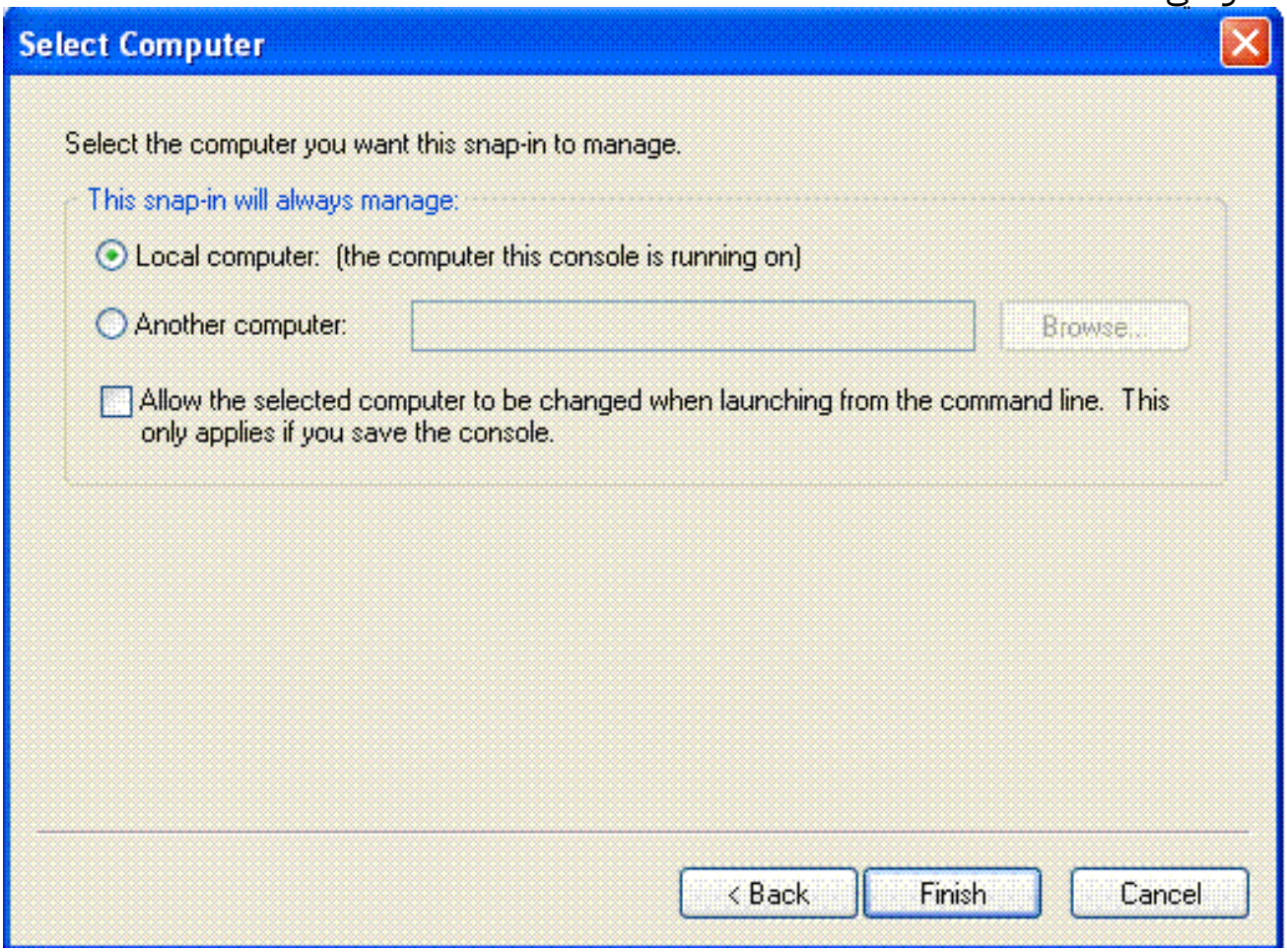


إضافة.

20. أختر **حساب الكمبيوتر**، وانقر فوق **التالي**.

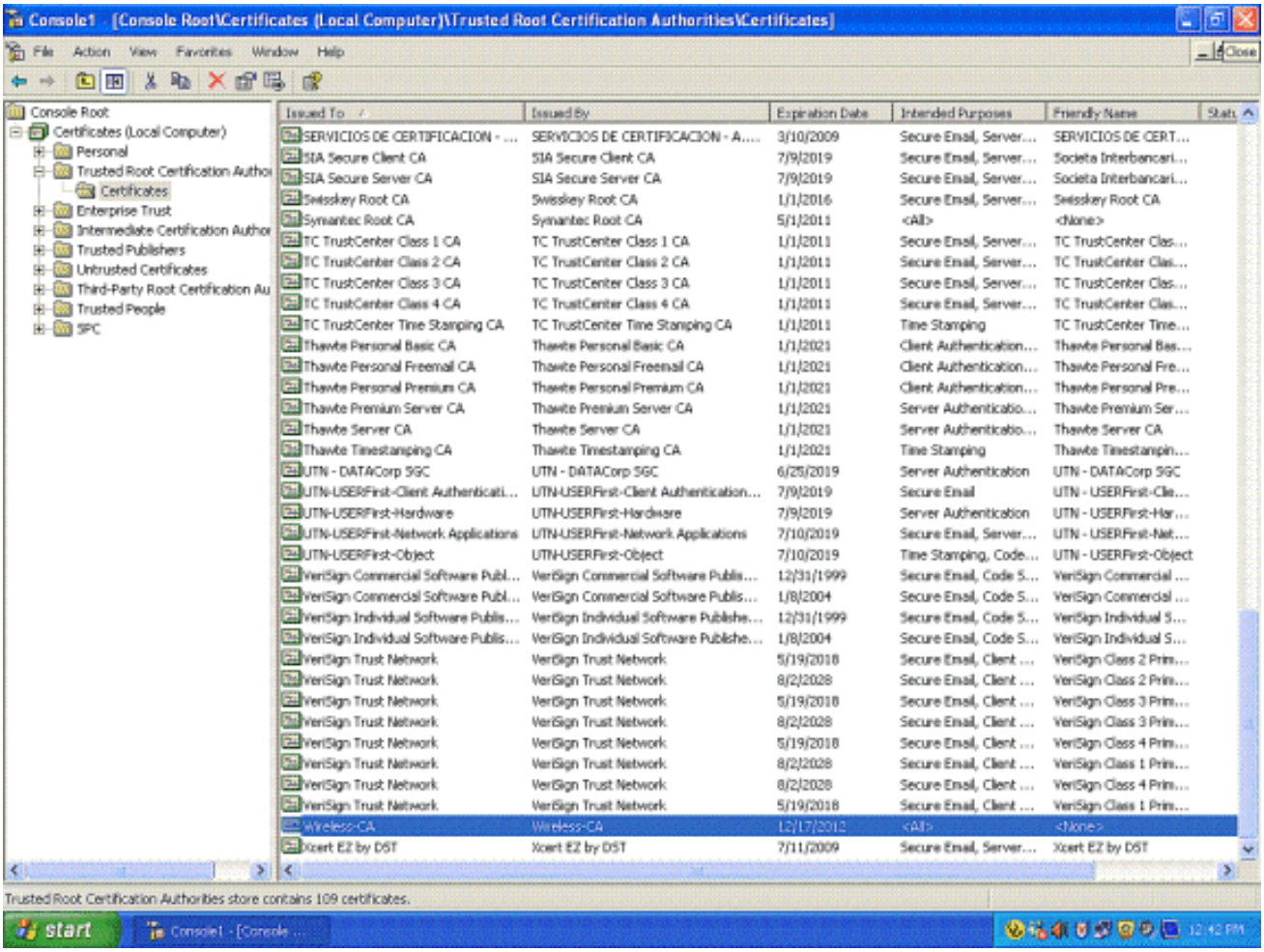


21. انقر فوق **إنهاء** لقبول الكمبيوتر المحلي الافتراضي.



22. طقطقة **ختام**، وطقطقة **ok**.

23. قم بتوسيع **التراخيص (الكمبيوتر المحلي)**، **قم** بتوسيع **مراجع التصديق الجذر الموثوقة**، وانقر على **الشهادات**. البحث عن **لاسلكي** في القائمة.



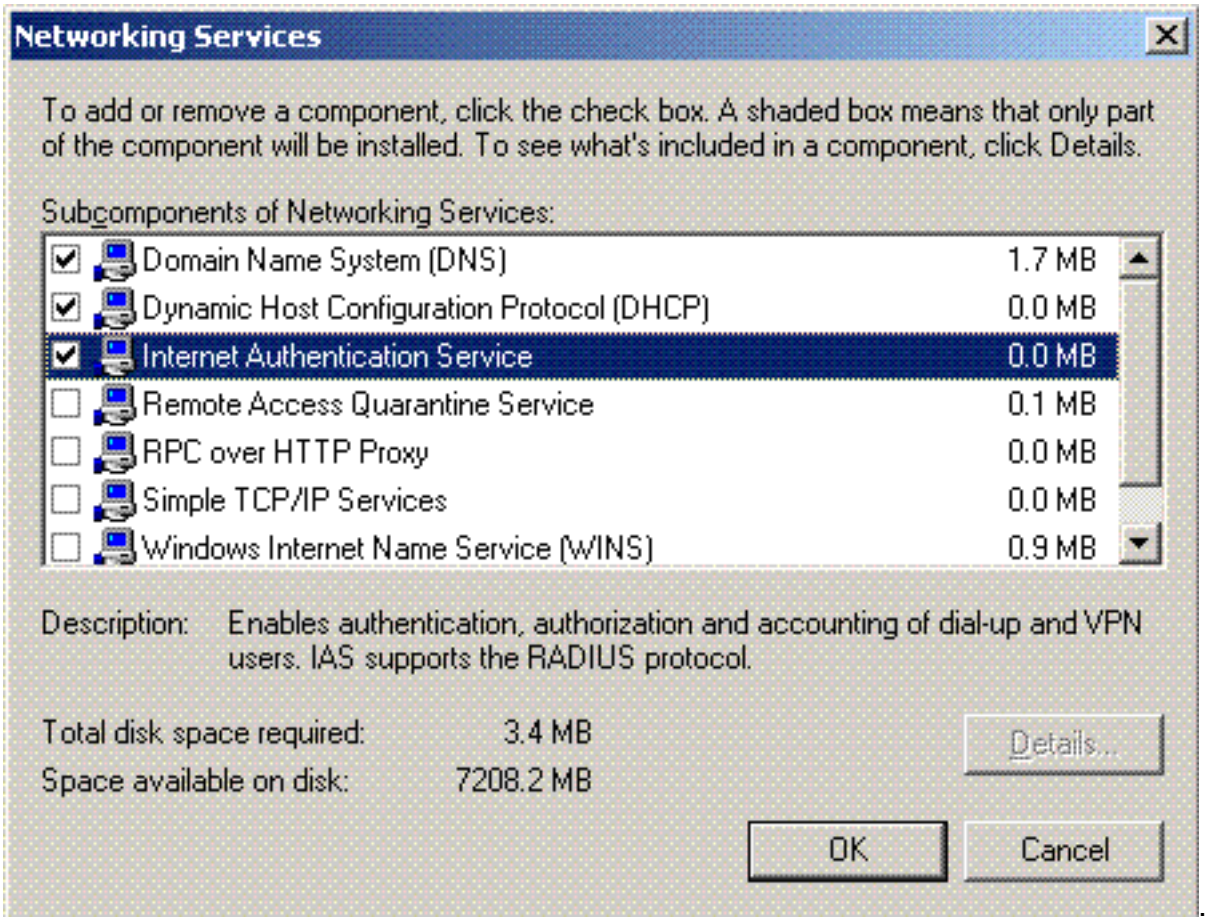
24. كرر هذا الإجراء لإضافة المزيد من العملاء إلى المجال.

تثبيت خدمة مصادقة الإنترنت على خادم Microsoft Windows 2003 وطلب شهادة

في هذا الإعداد، تستخدم خدمة مصادقة الإنترنت (IAS) كخادم RADIUS لمصادقة عملاء اللاسلكي بمصادقة PEAP.

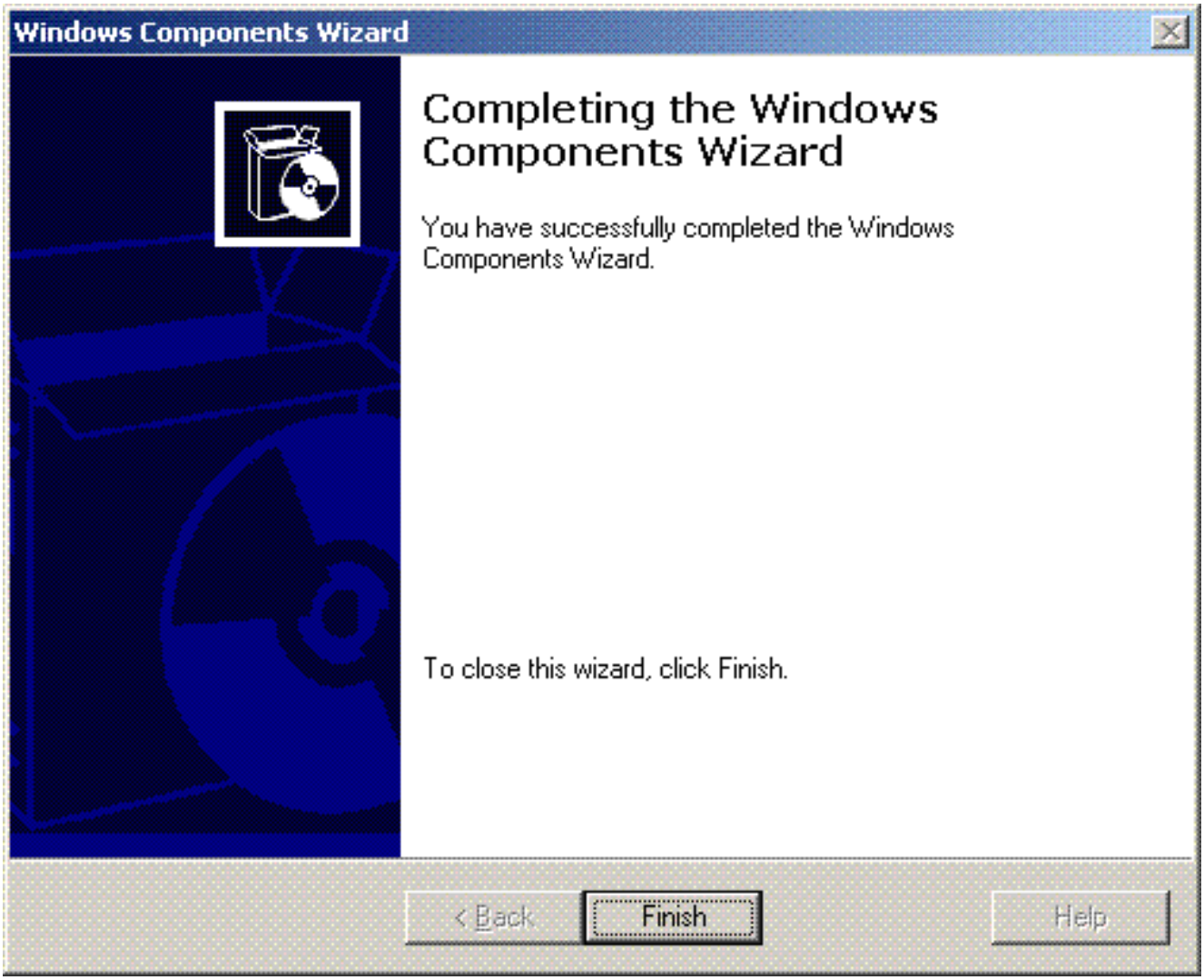
أكمل الخطوات التالية لتثبيت IAS وتكوينه على الخادم.

1. انقر فوق **إضافة أو إزالة برامج** في لوحة التحكم.
2. انقر فوق **إضافة/إزالة مكونات Windows**.
3. أختر **خدمات الشبكة**، وانقر فوق **تفاصيل**.
4. أختر **خدمة مصادقة الإنترنت**، وانقر **موافق**، وانقر

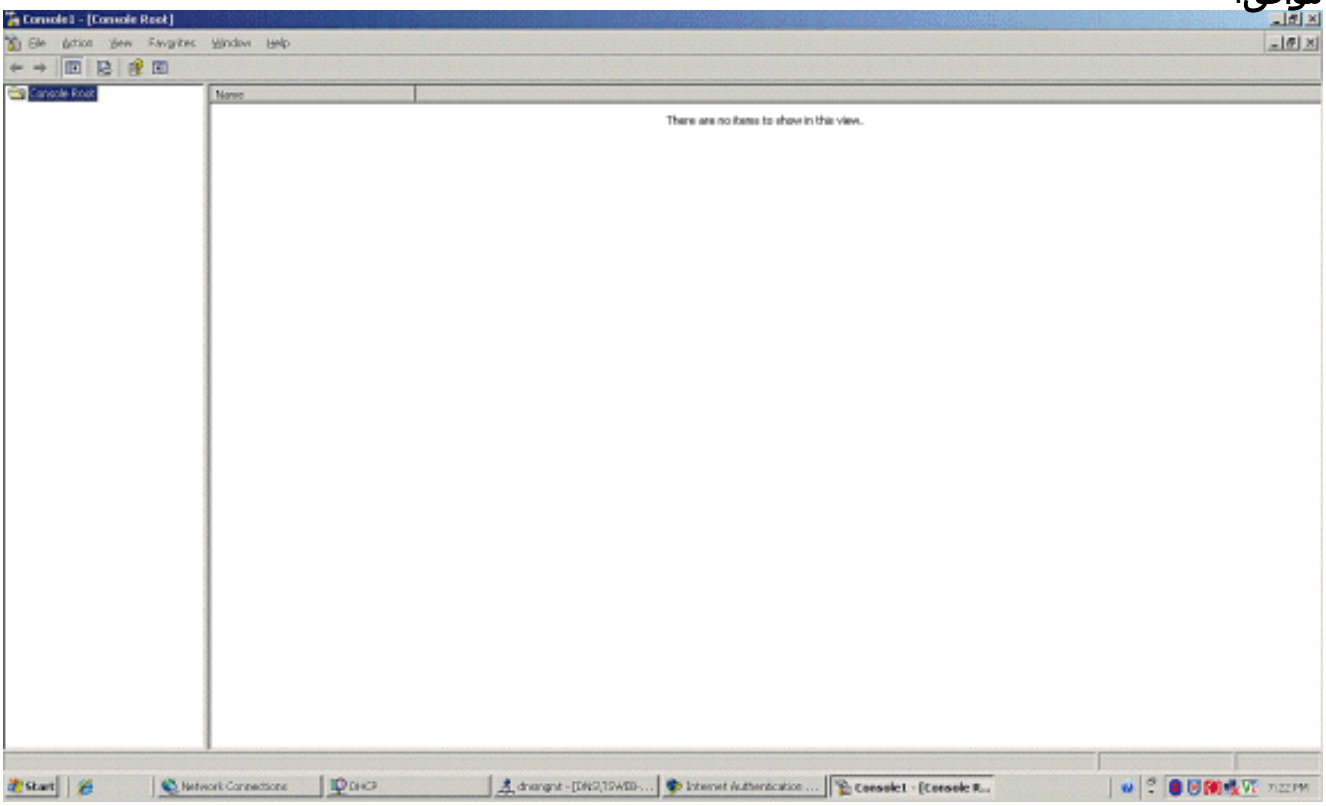


التالي.

5. انقر فوق **إنهاء**" لإكمال تثبيت IAS.

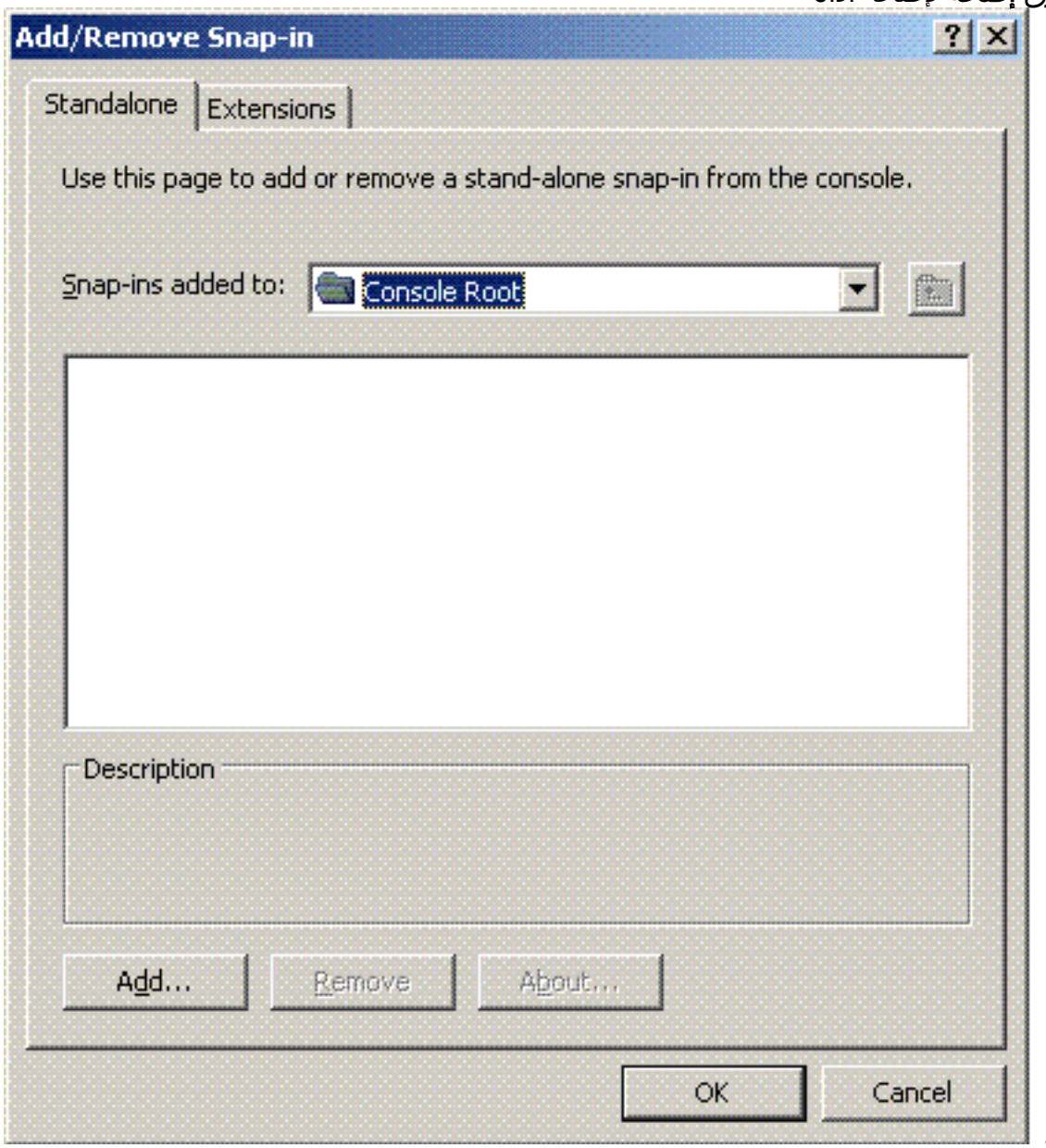


6. تتمثل الخطوة التالية في تثبيت شهادة الكمبيوتر لخدمة مصادقة الإنترنت (IAS).
7. انقر فوق **بدء**؛ وانقر فوق **تشغيل**؛ واكتب **mmc**؛ وانقر فوق **موافق**.



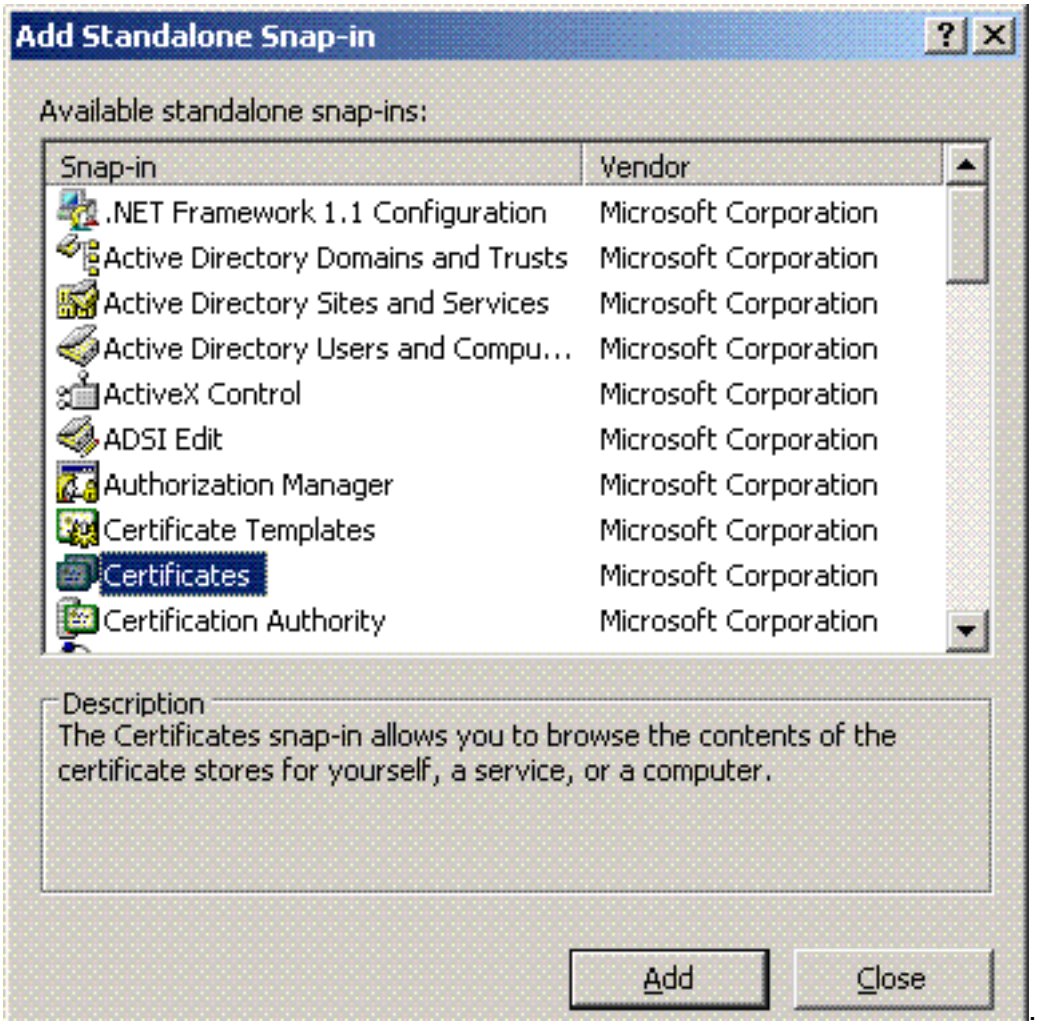
8. انقر فوق **وحدة التحكم** في قائمة الملف، ثم أختر **إضافة/إزالة** الأداة الإضافية.

9. انقر فوق **إضافة** لإضافة أداة



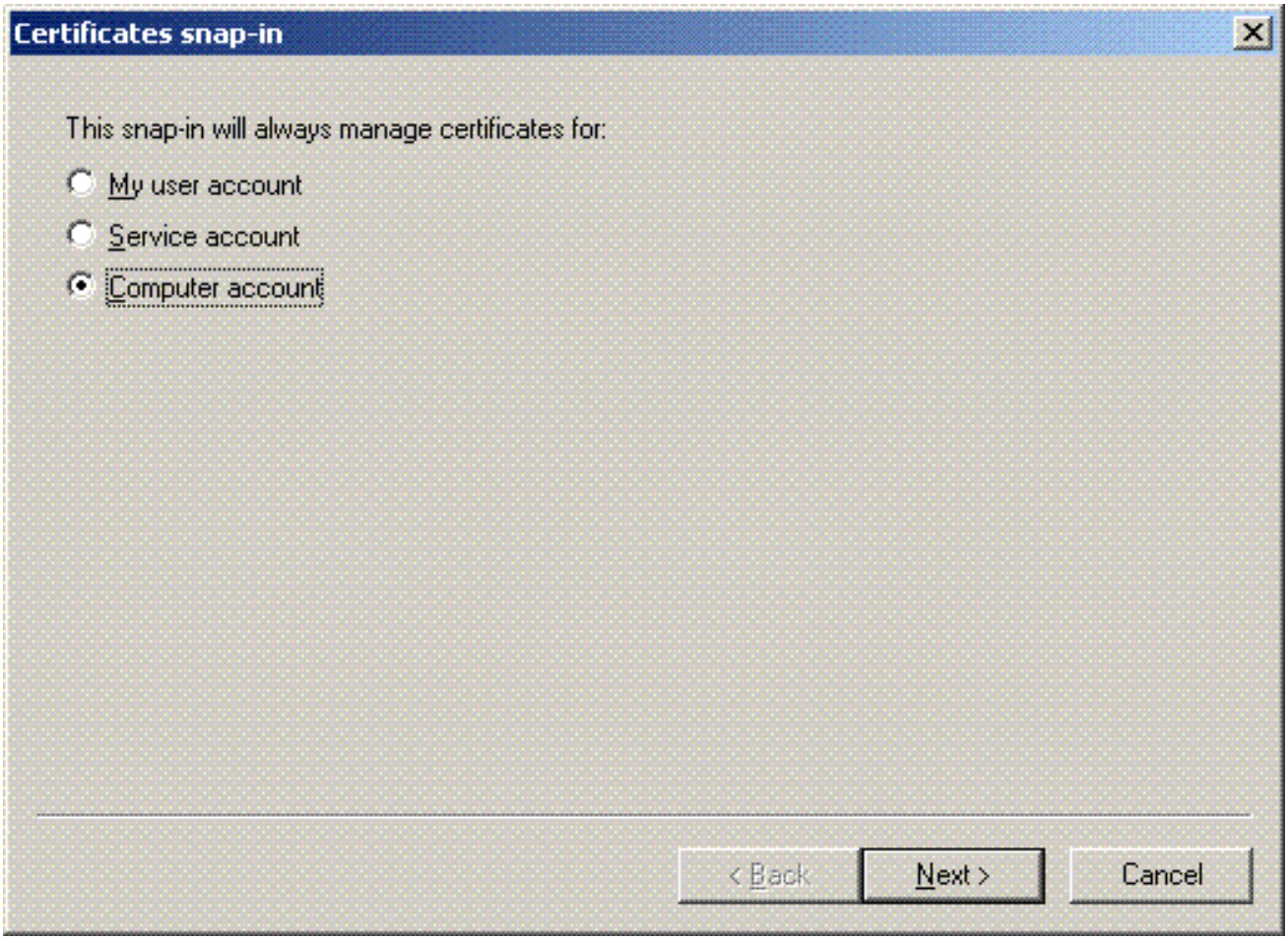
إضافية.

10. أختر **شهادات** من قائمة الأدوات الإضافية، وانقر

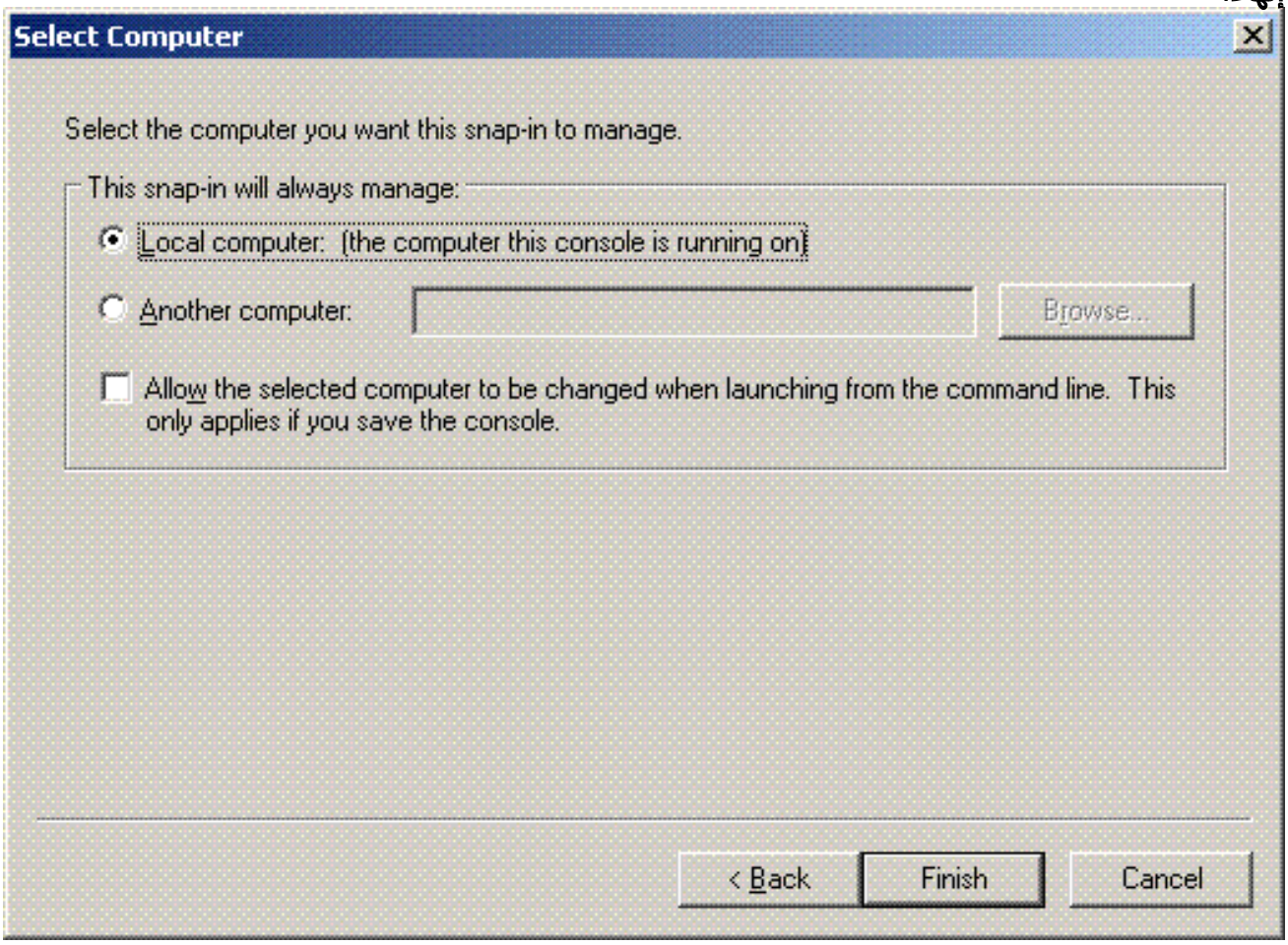


إضافة.

11. أخترت **حاسوب حساب**، وطقطقة **بعد ذلك**.

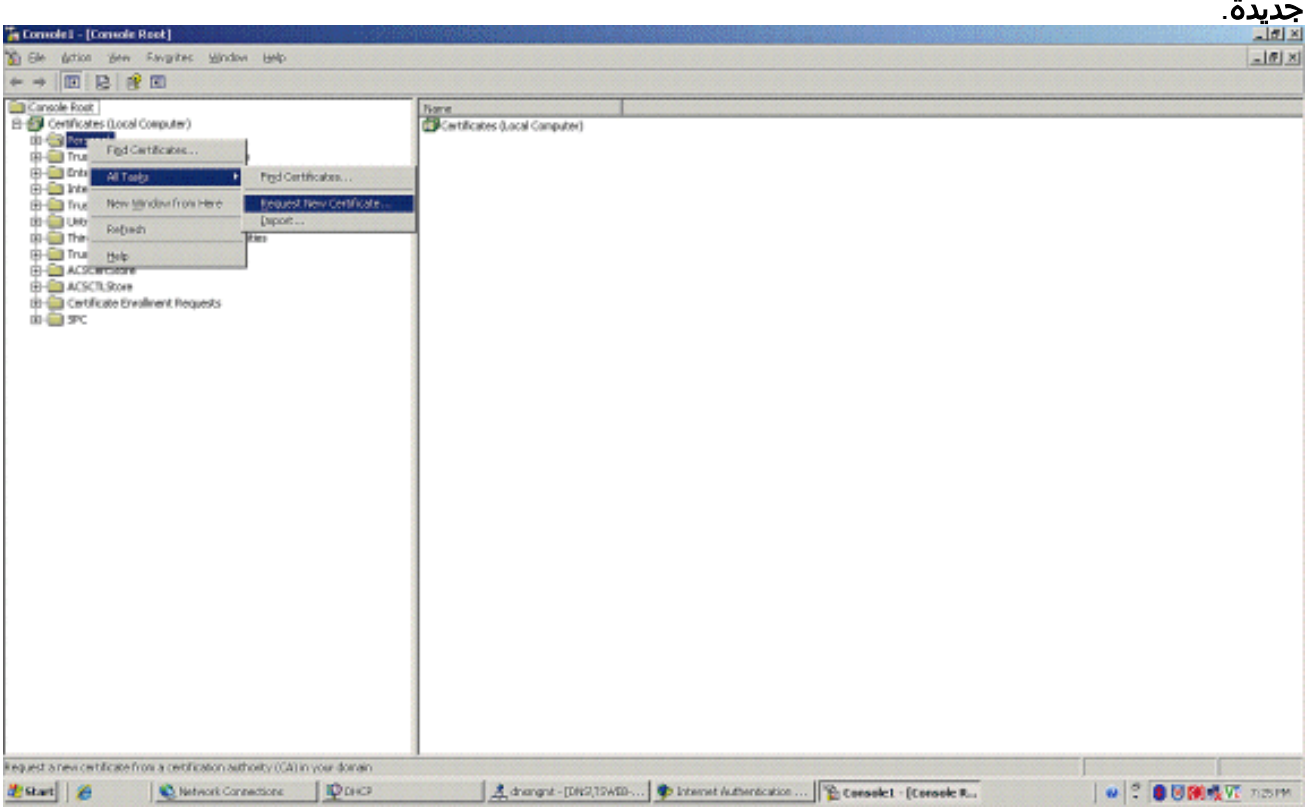


12. أختر **كمبيوتر محلي**، وانقر **إنهاء**.



13. طقطقة **ختام**، وطقطقة **ok**.

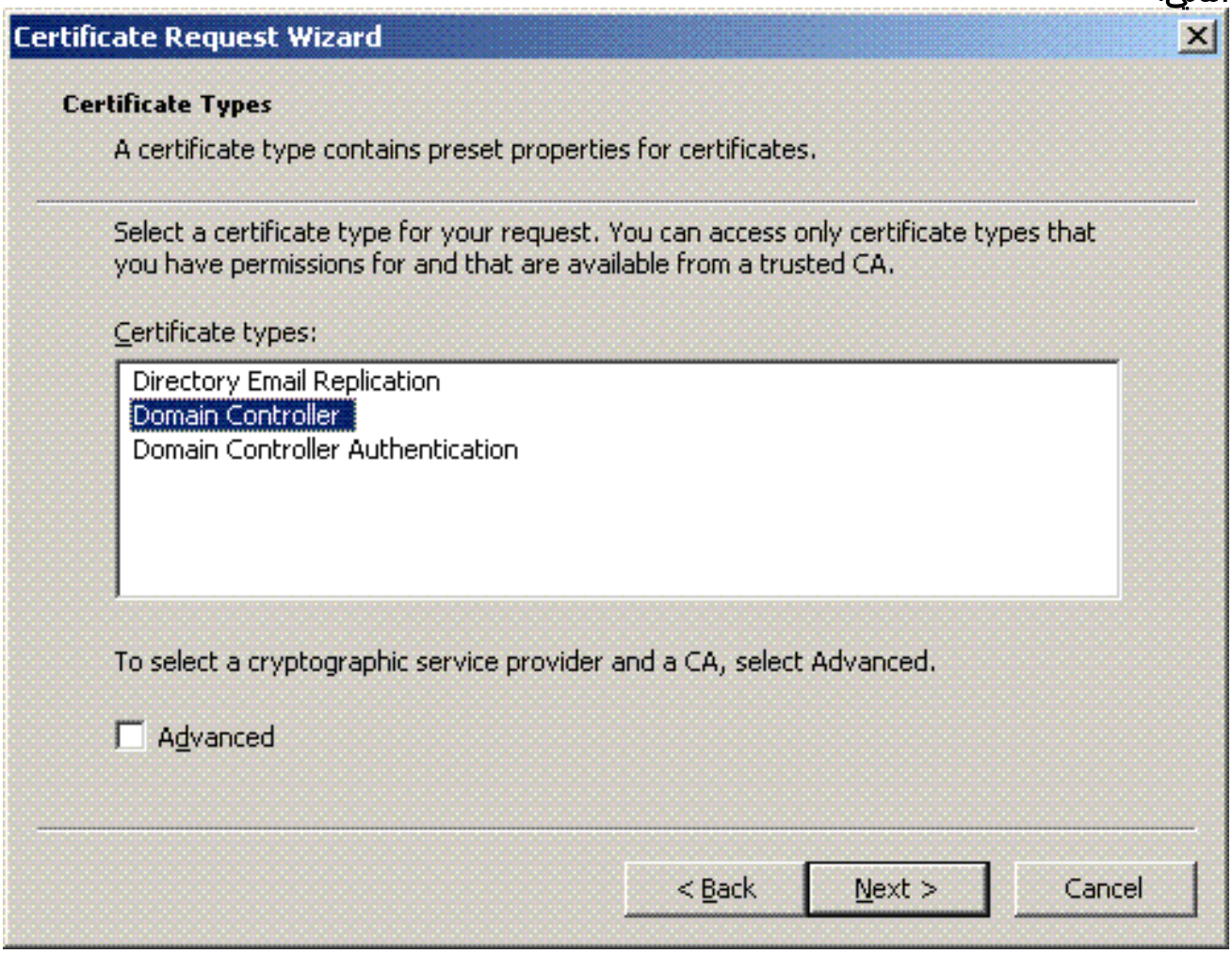
14. قم بتوسيع **الشهادات (الكمبيوتر المحلي)**، انقر بزر الماوس الأيمن على **مجلد شخصي**، واختر **جميع المهام**، ثم **اطلب شهادة جديدة**.



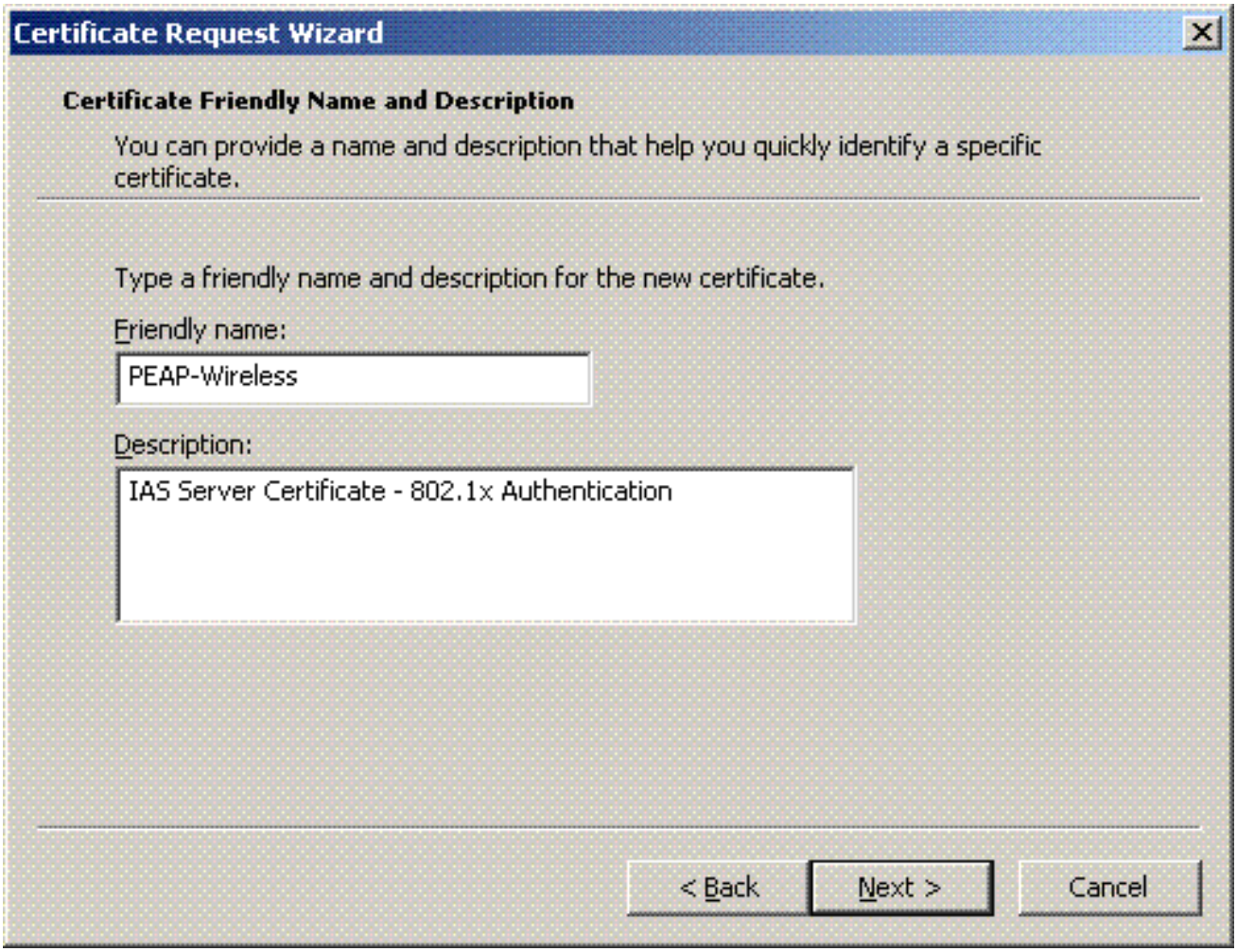
15. انقر فوق **التالي** في *معالج طلب الشهادة Welcome to the Certificate Request Processor*.

16. أختر قالب شهادة **وحدة التحكم بالمجال** (إذا طلبت شهادة كمبيوتر على خادم غير وحدة التحكم بالمجال، أختر

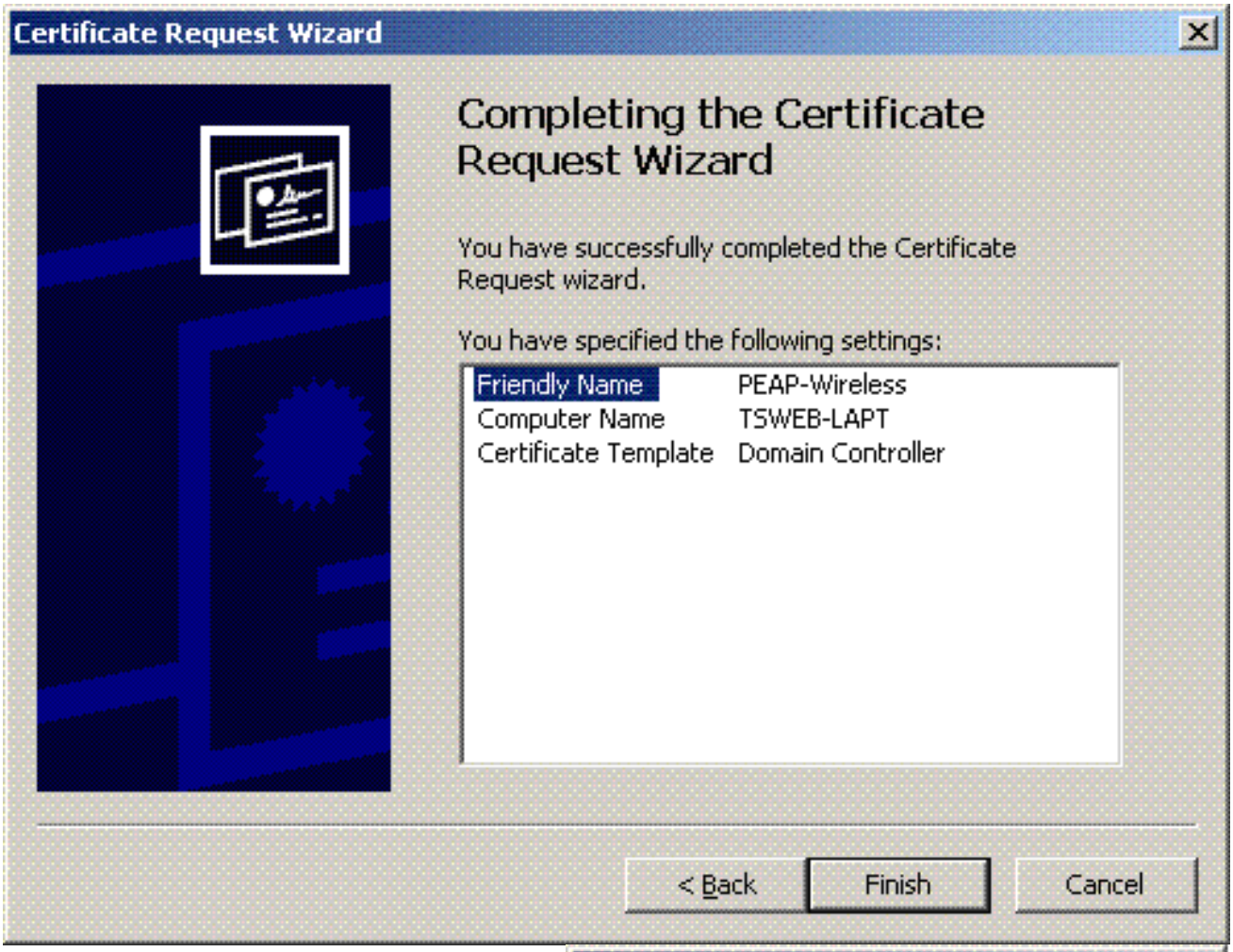
قالب شهادة **كمبيوتر**)، وانقر فوق **التالي**.

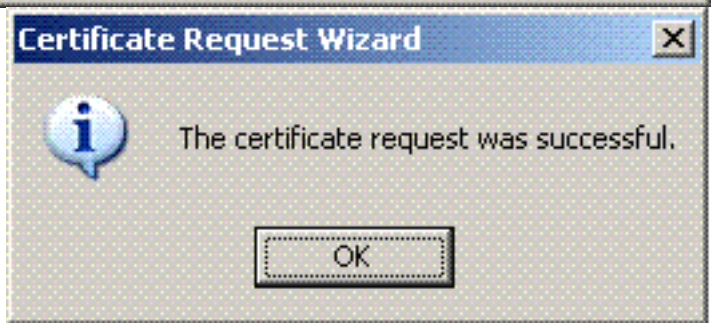


17. اكتب اسما ووصف للشهادة.



18. انقر فوق **إنهاء**" لإكمال معالج طلب الاعتماد.



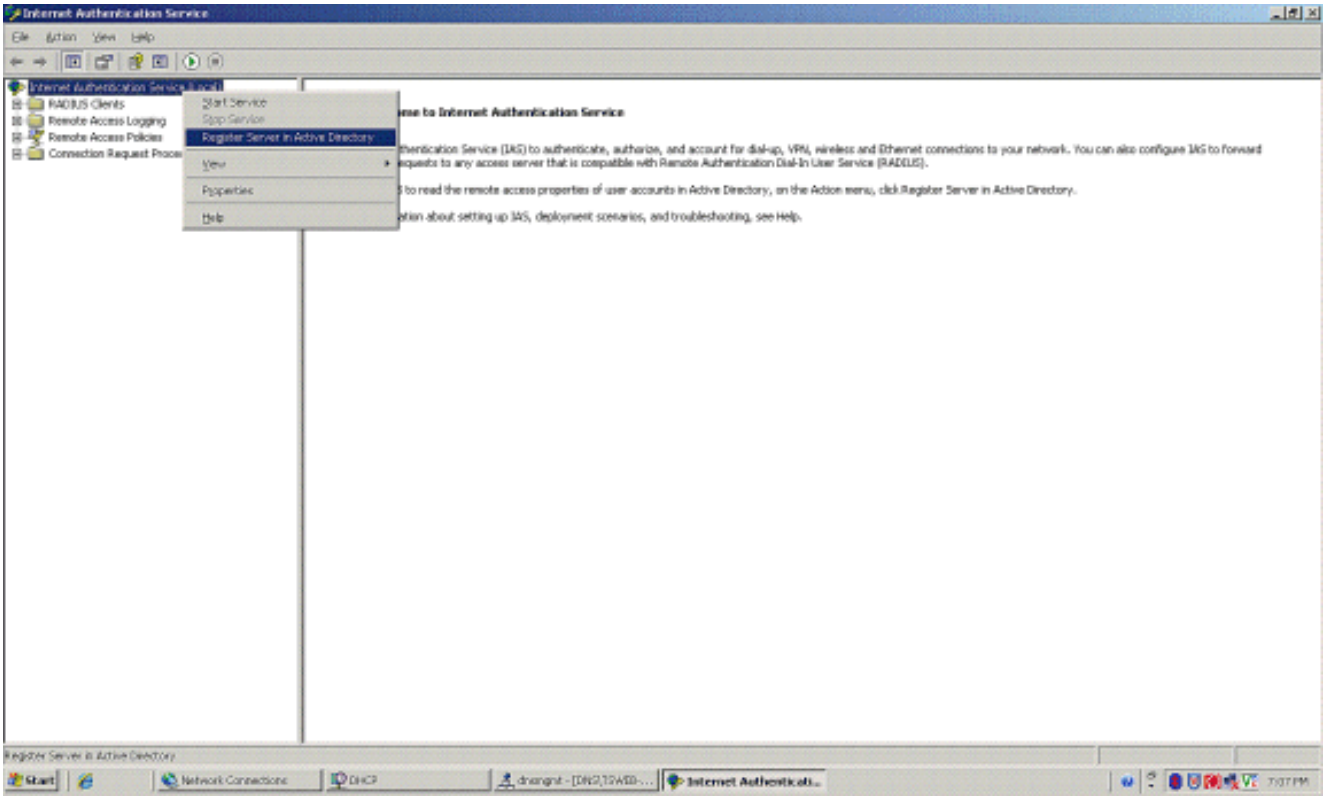


تكوين خدمة مصادقة الإنترنت لمصادقة PEAP-MS-CHAP v2

الآن بعد أن قمت بتثبيت طلب شهادة ل IAS، قم بتكوين IAS للمصادقة.

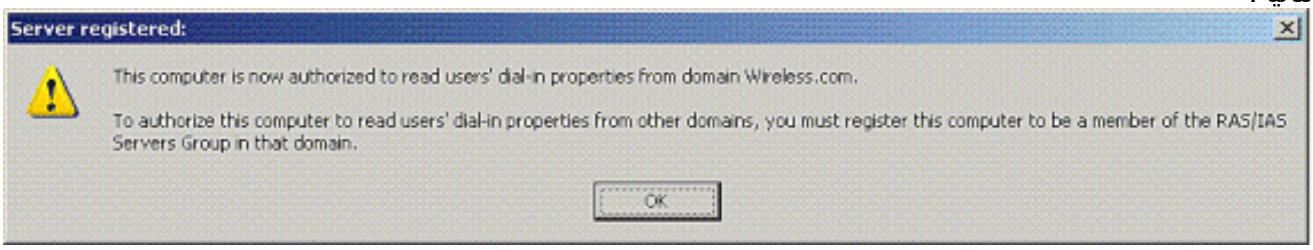
أكمل الخطوات التالية:

1. انقر على **ابدأ > برامج > أدوات إدارية**، وانقر فوق الأداة الإضافية **لخدمة مصادقة الإنترنت**.
2. انقر بزر الماوس الأيمن فوق **خدمة مصادقة الإنترنت (IAS)**، ثم انقر فوق **تسجيل الخدمة في Active Directory**.

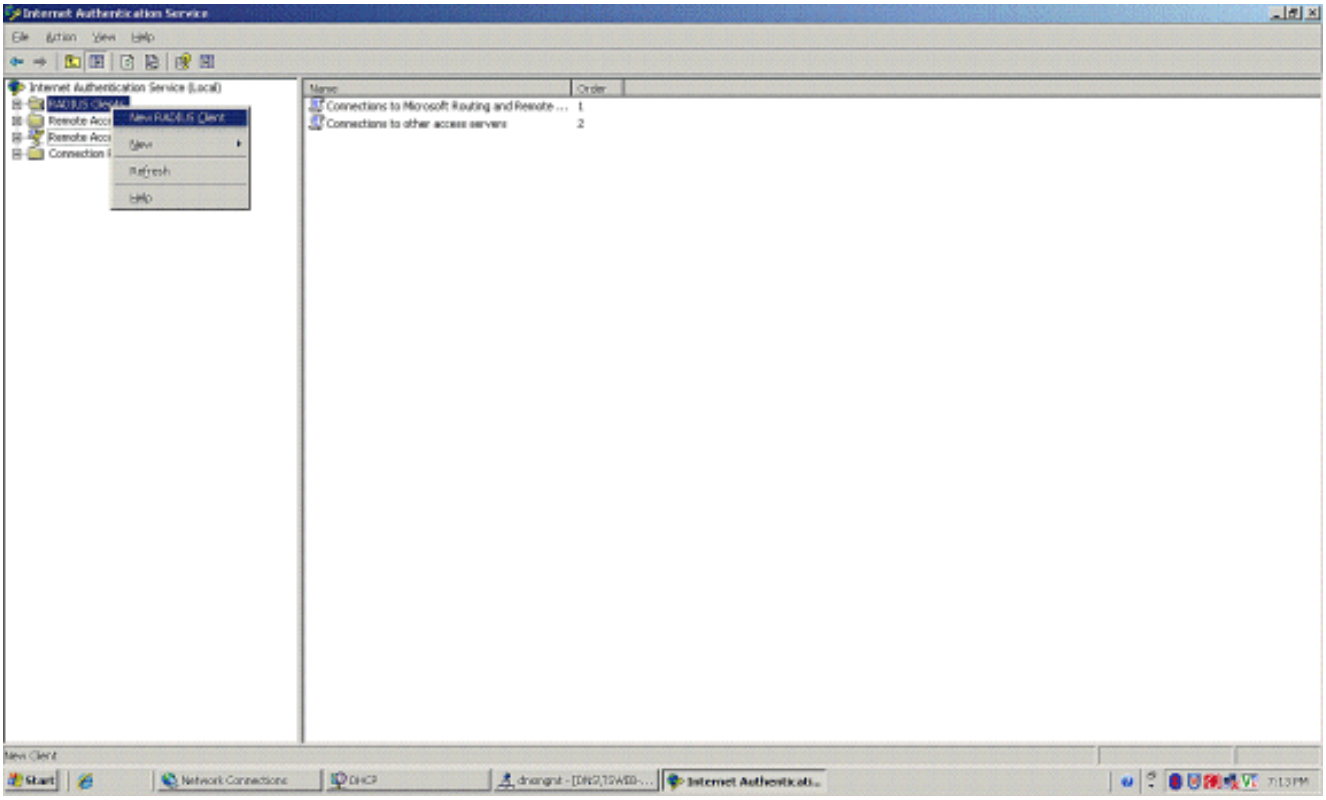


3. يظهر مربع الحوار **تسجيل خدمة مصادقة الإنترنت في Active Directory**، انقر **موافق**. هذا يمكن IAS من مصادقة المستخدمين في Active Directory.

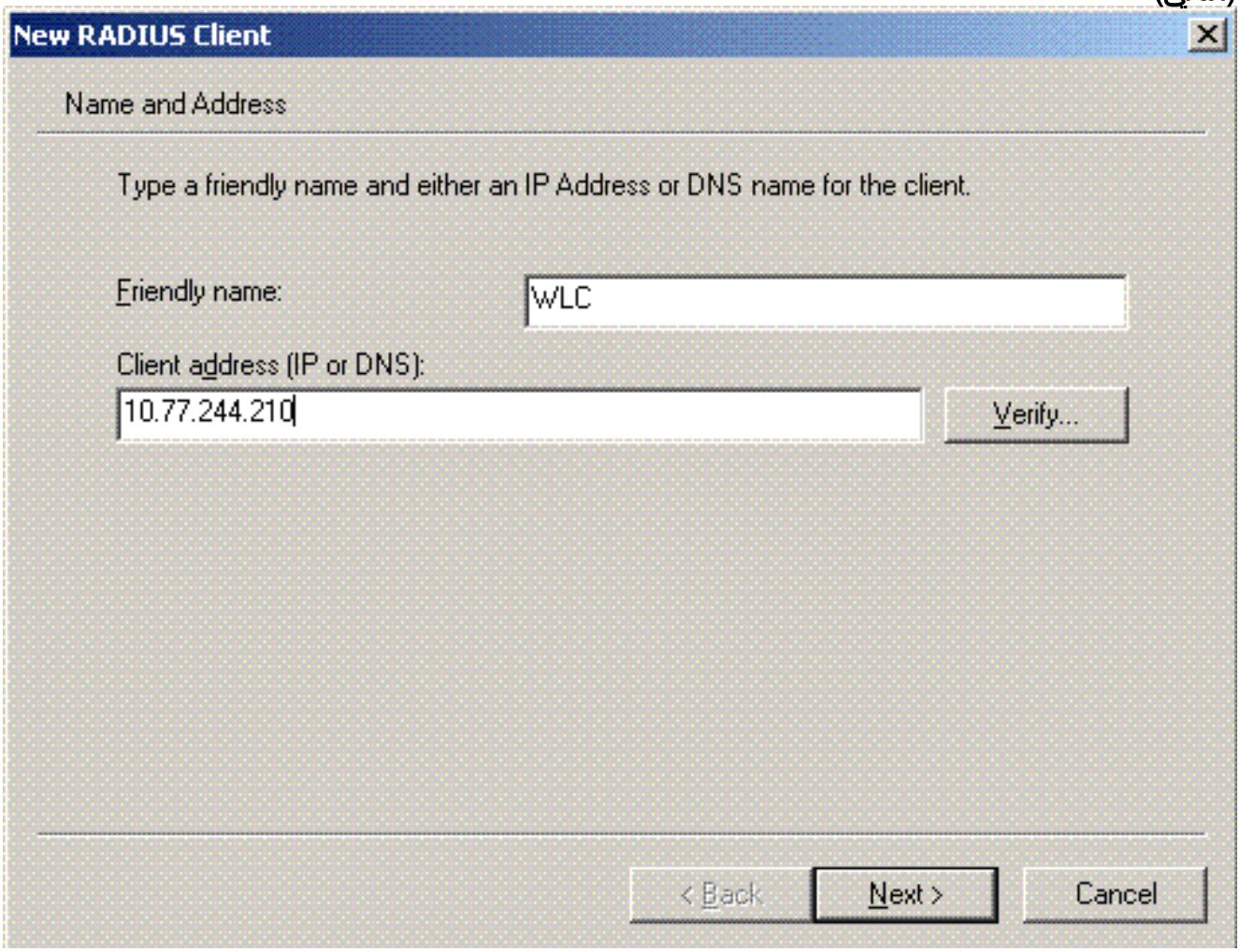
4. طقطقة **ok** في الشاشة التالية.



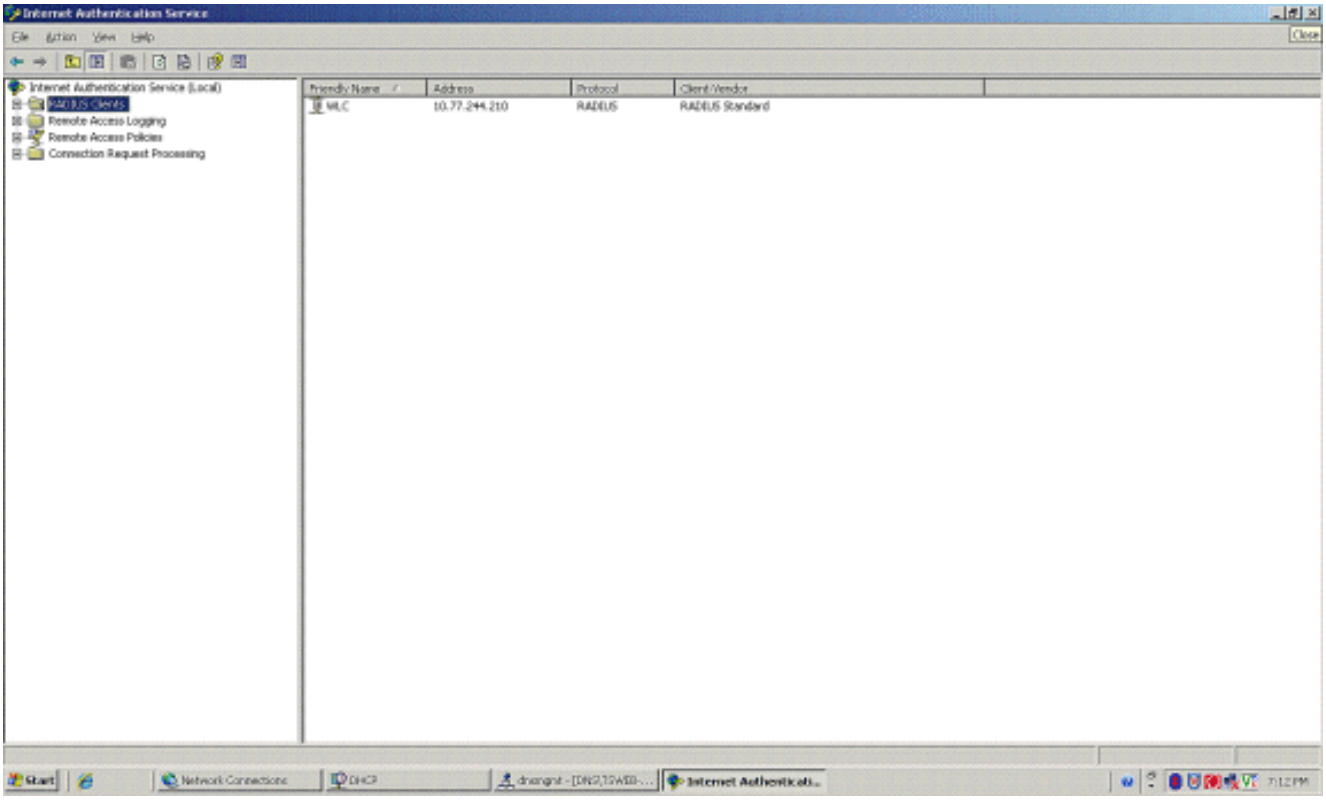
5. إضافة وحدة التحكم في شبكة LAN اللاسلكية كعميل AAA على خادم MS IAS.
6. انقر بزر الماوس الأيمن فوق **عملاء RADIUS**، واختر **عميل RADIUS الجديد**.



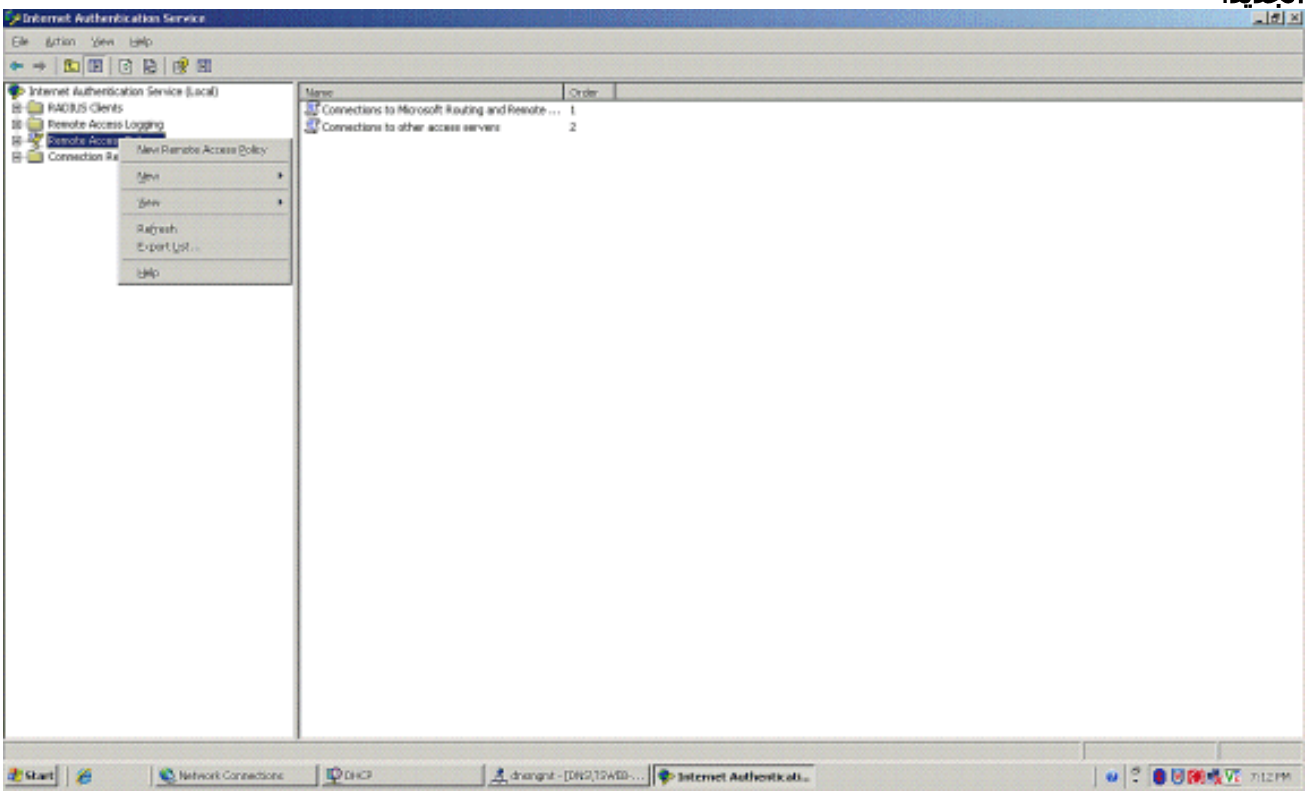
7. اكتب اسم العميل (WLC في هذه الحالة)، وأدخل عنوان IP الخاص ب WLC. انقر فوق **Next (التالي)**.



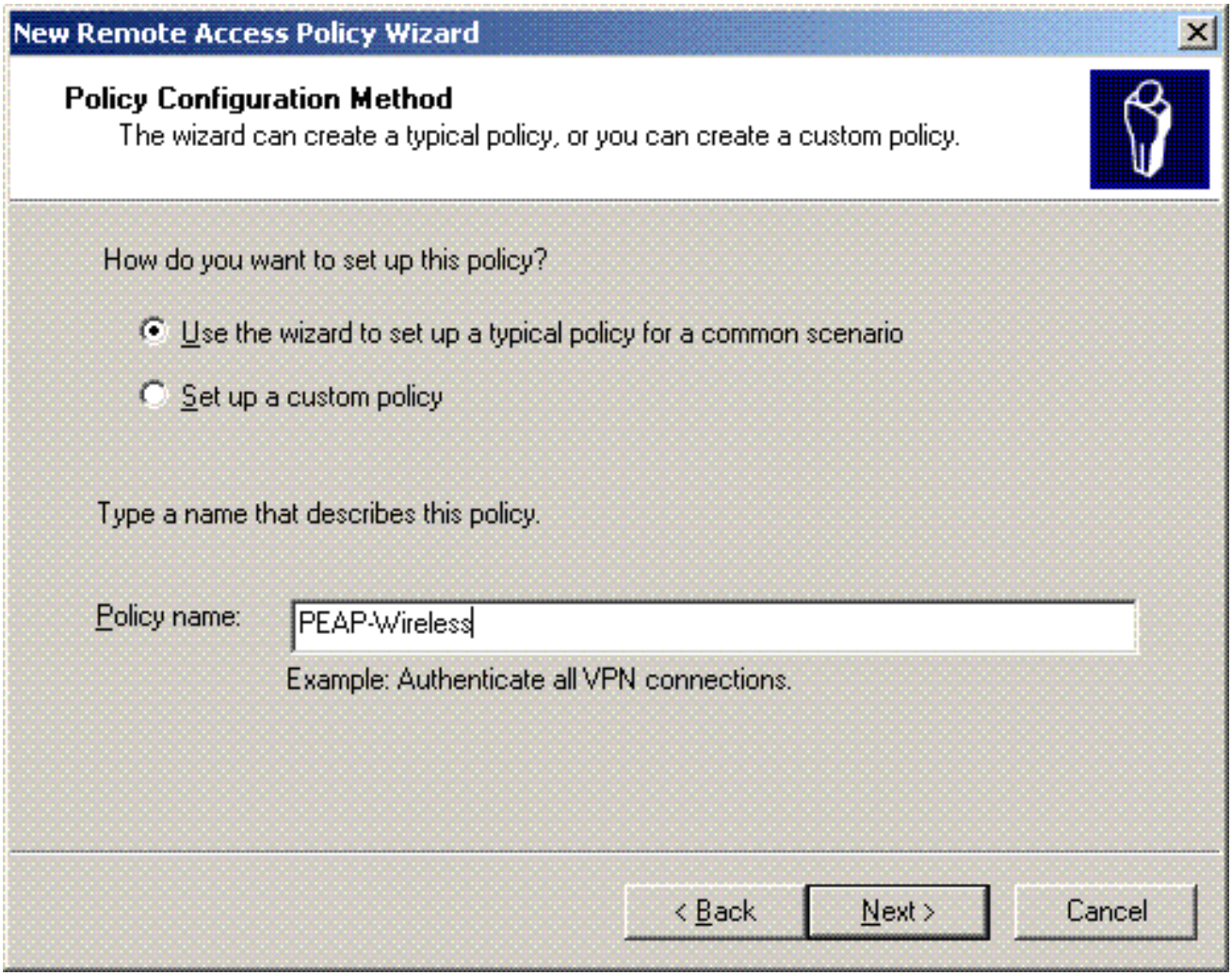
8. أخترت في الصفحة التالية، تحت زبون-بائع، **RADIUS معياري**؛ دخلت ال يشارك سر؛ وطقطقة **إنجاز**.
9. لاحظ إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA على IAS.



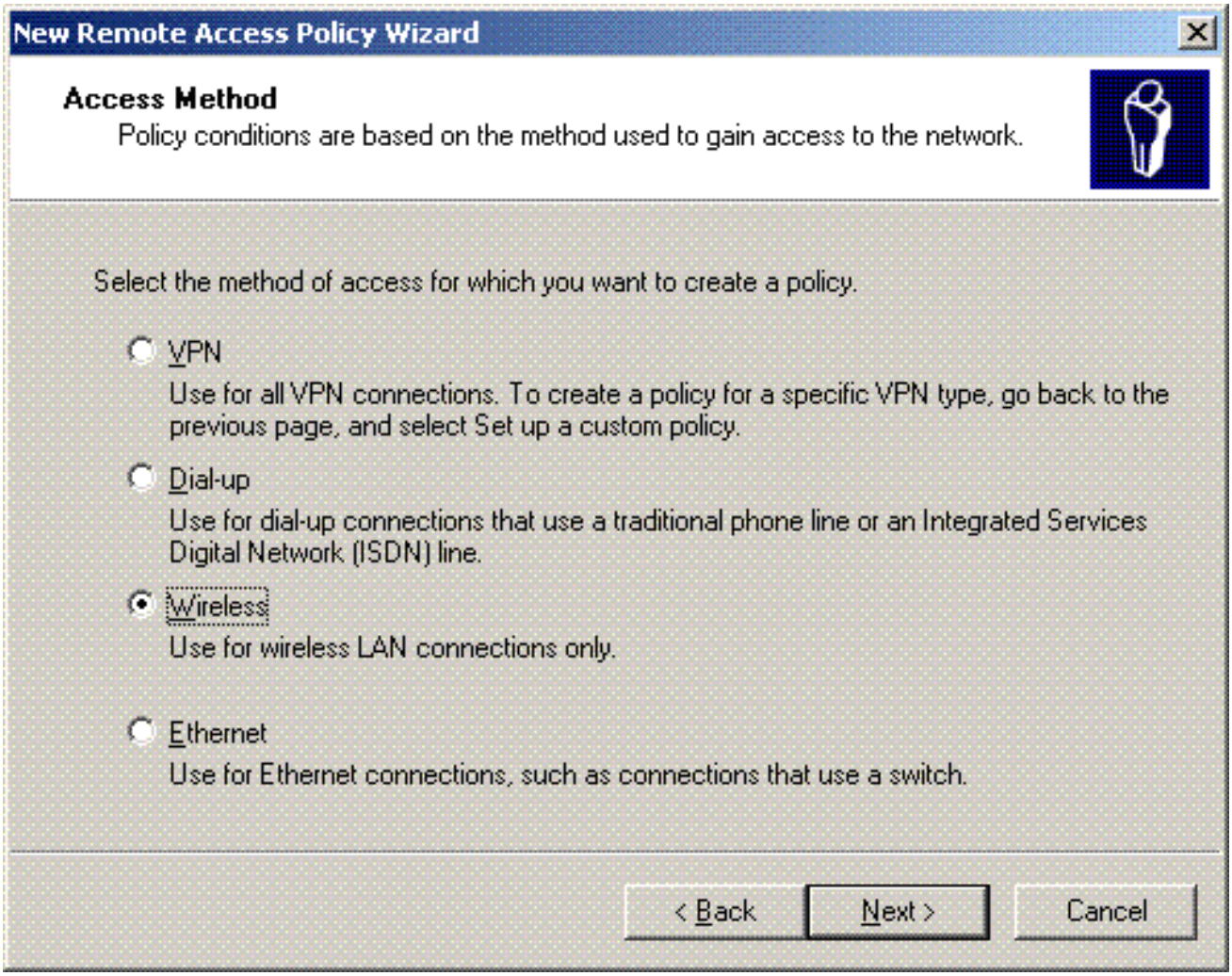
10. إنشاء نهج وصول عن بعد للعملاء.
11. للقيام بذلك، انقر بزر الماوس الأيمن فوق **سياسات الوصول عن بعد**، واختر **نهج الوصول عن بعد الجديد**.



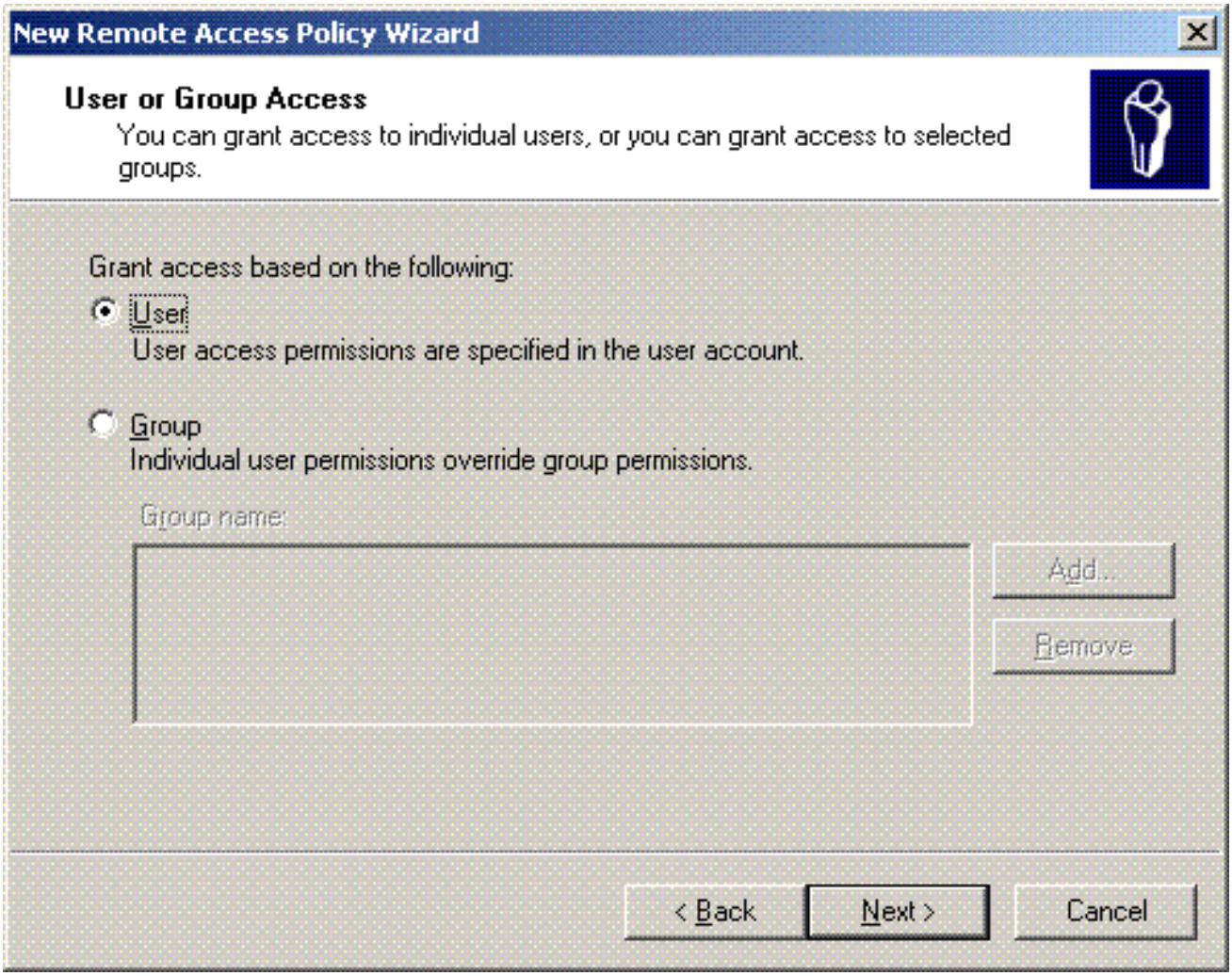
12. اكتب اسما لنهج الوصول عن بعد. في هذا المثال، أستخدم اسم **PEAP**. ثم انقر فوق **التالي**.



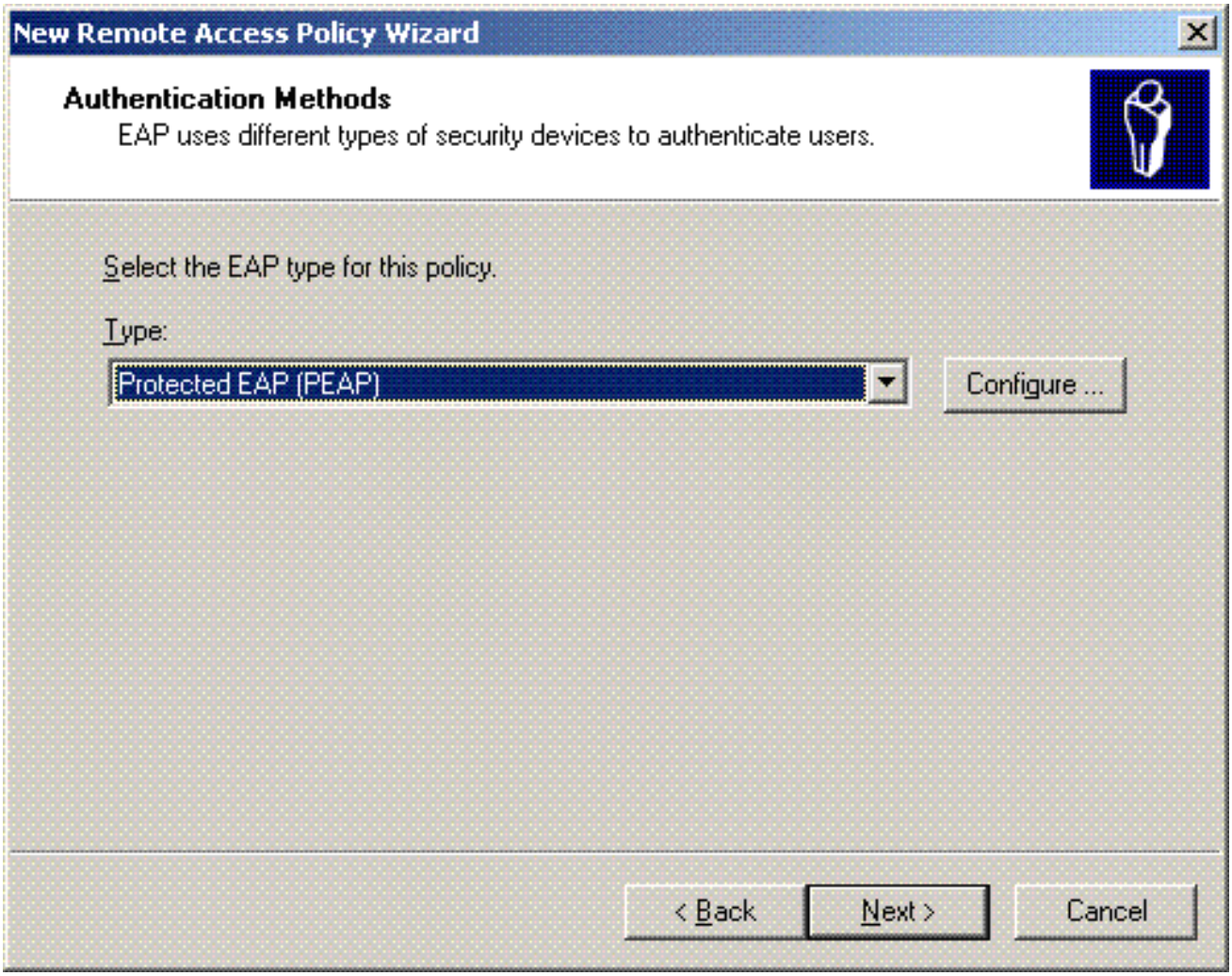
13. أختر سمات النهج استنادا إلى متطلباتك. في هذا المثال، أختر **لاسلكي**.



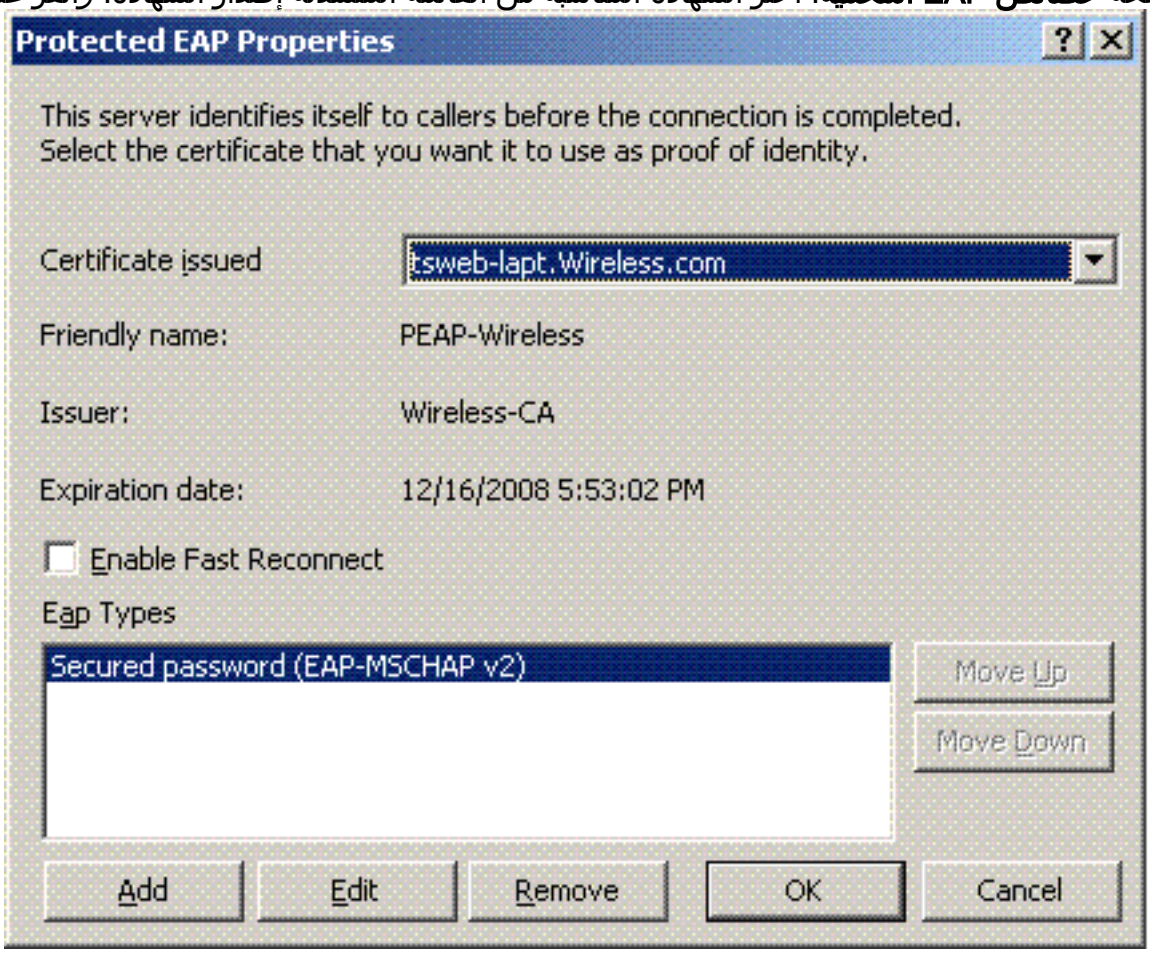
14. في الصفحة التالية، أختر **User** لتطبيق نهج الوصول عن بعد هذا على قائمة المستخدمين.



15. أخترت تحت أسلوب صحة هوية، **محمي** EAP (PEAP)، وطقطقة **يشكل**.

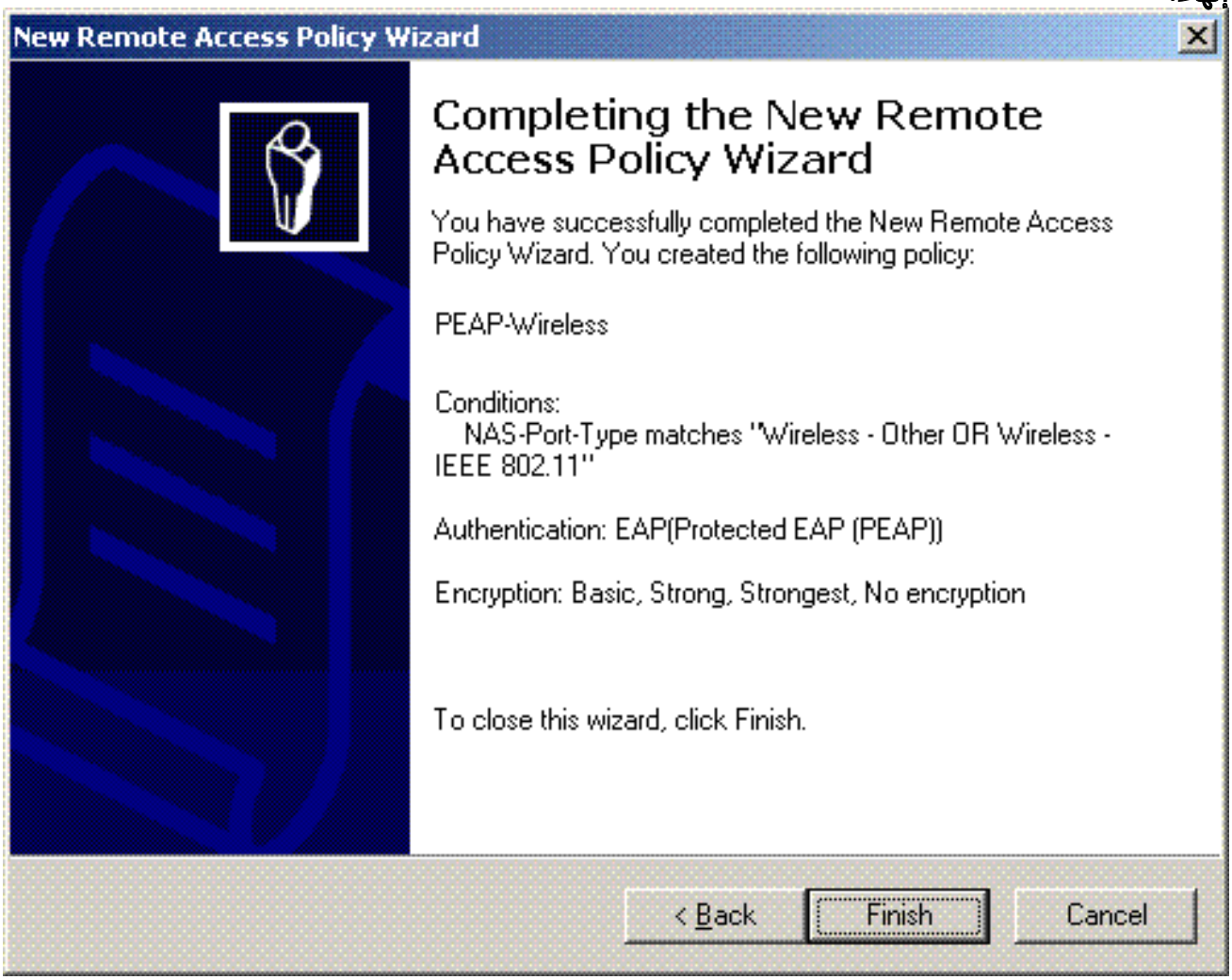


16. في صفحة **خصائص EAP المحمية**، أختر الشهادة المناسبة من القائمة المنسدلة إصدار الشهادة، وانقر على

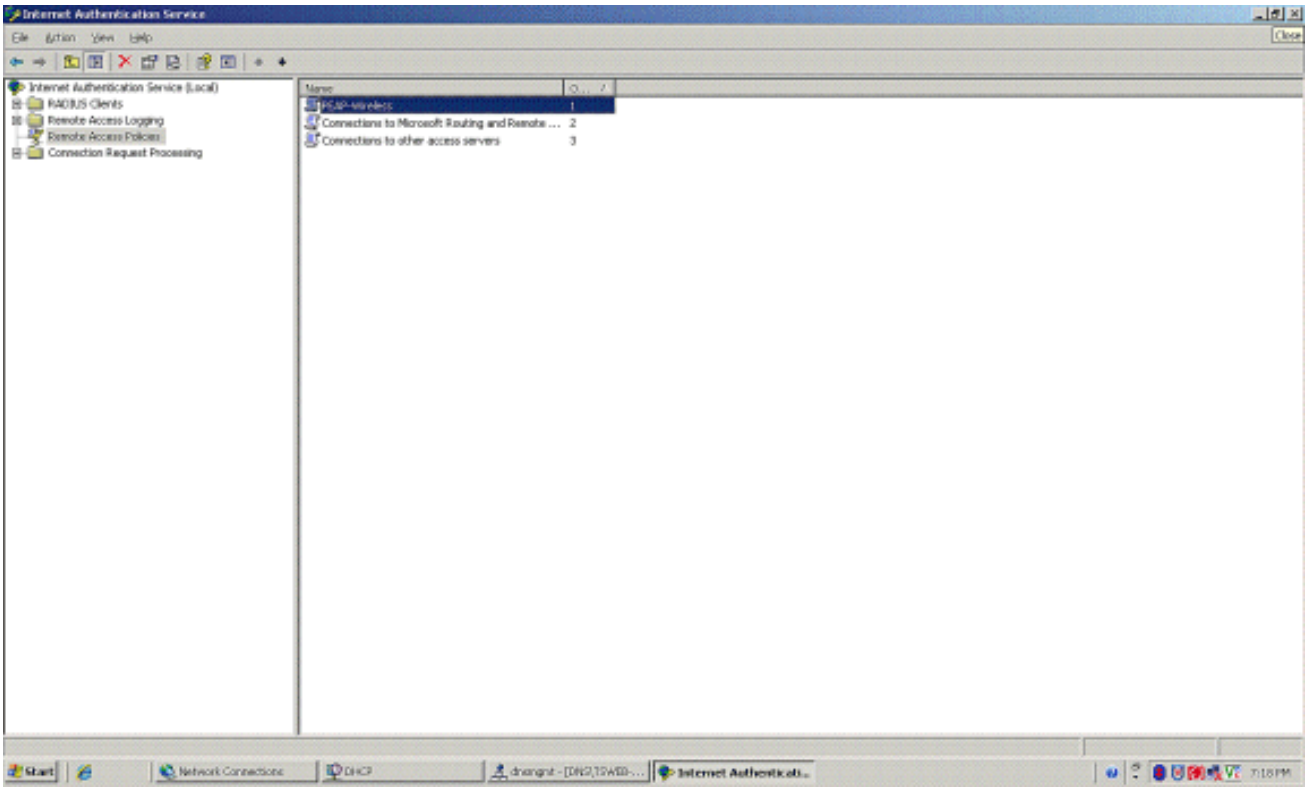


موافق.

17. تحقق من تفاصيل نهج الوصول عن بعد، ثم انقر فوق **إنهاء**.

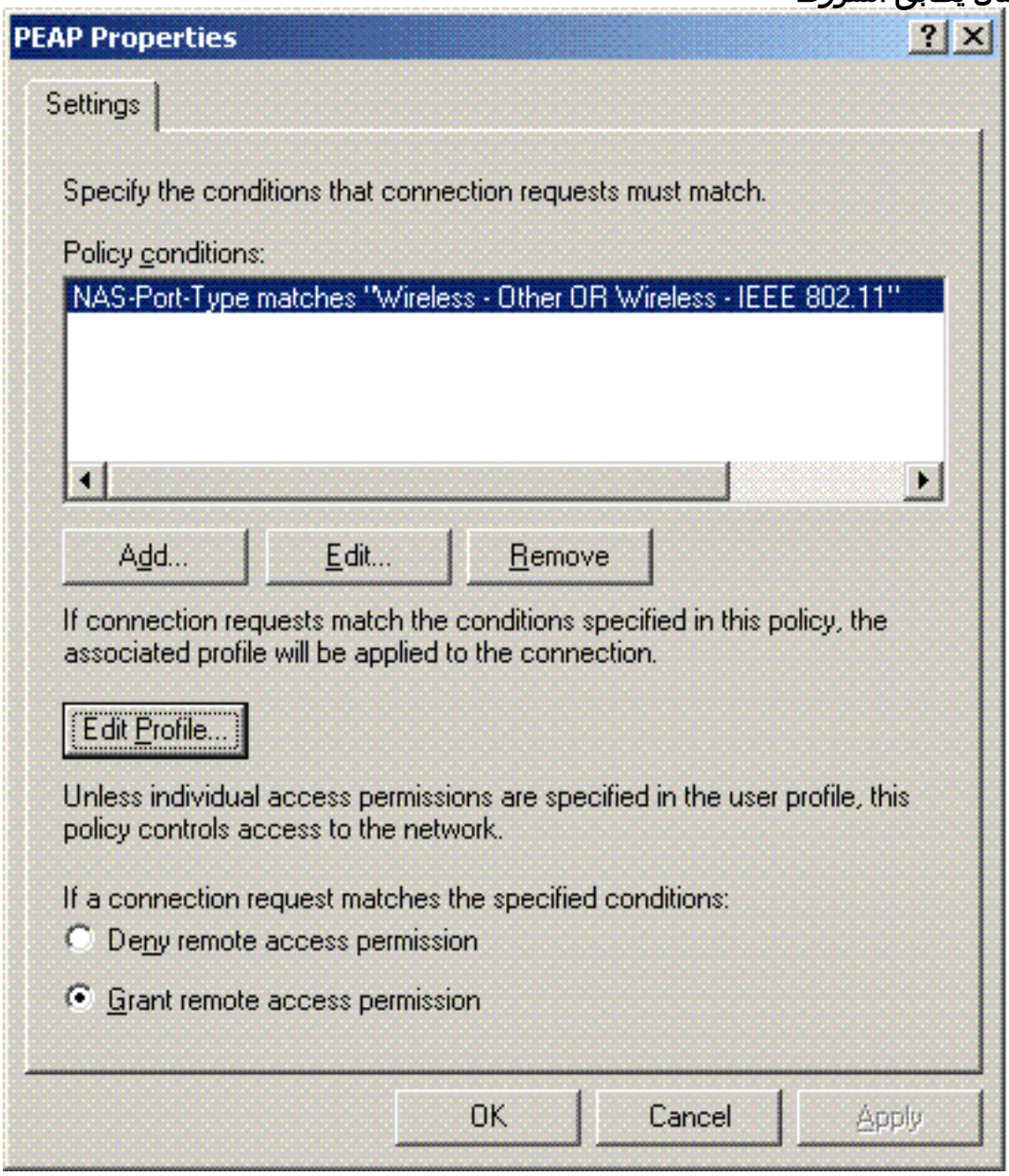


18. تمت إضافة نهج الوصول عن بعد إلى القائمة.



19. انقر بزر الماوس الأيمن فوق النهج، ثم انقر فوق **خصائص**. أختر **منح إذن الوصول عن بعد** تحت **"إذا كان**

طلب الاتصال يطابق الشروط



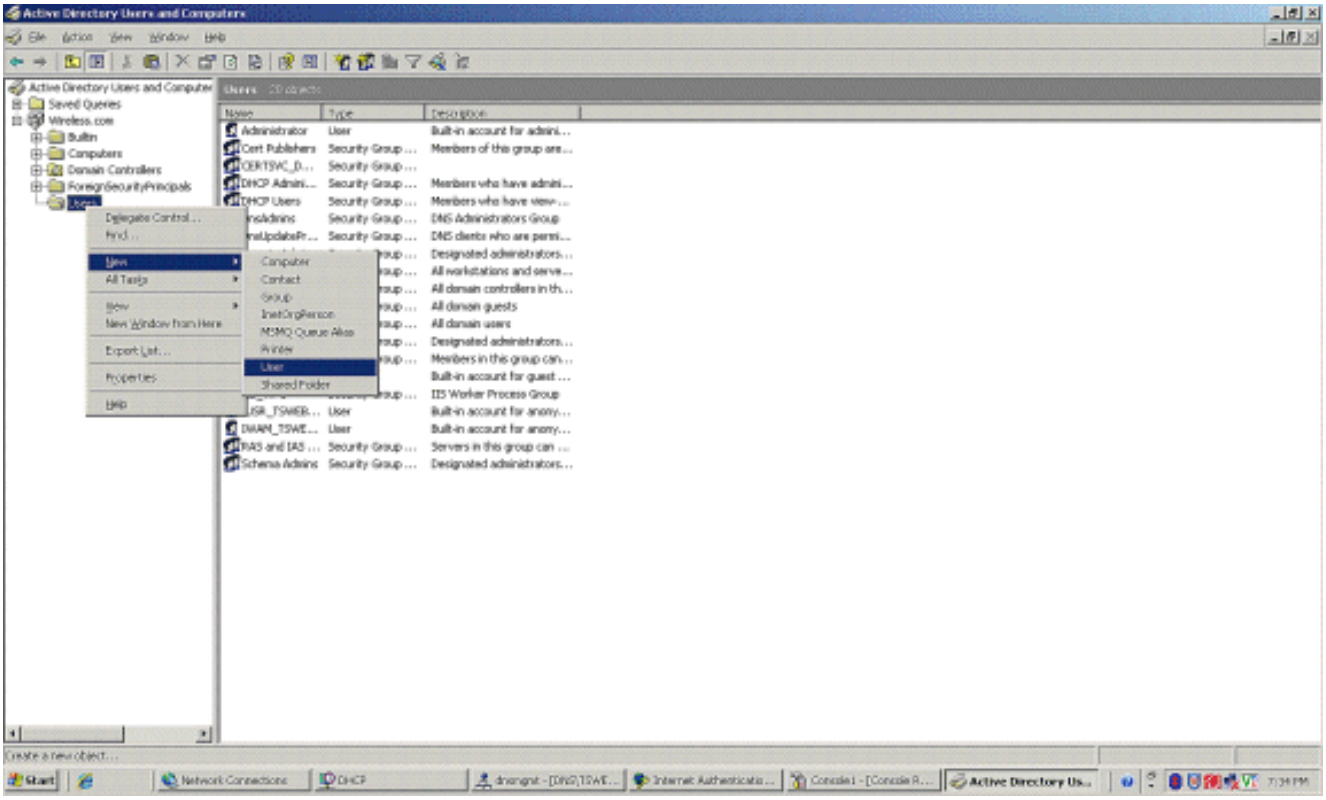
المحددة".

إضافة مستخدمين إلى Active Directory

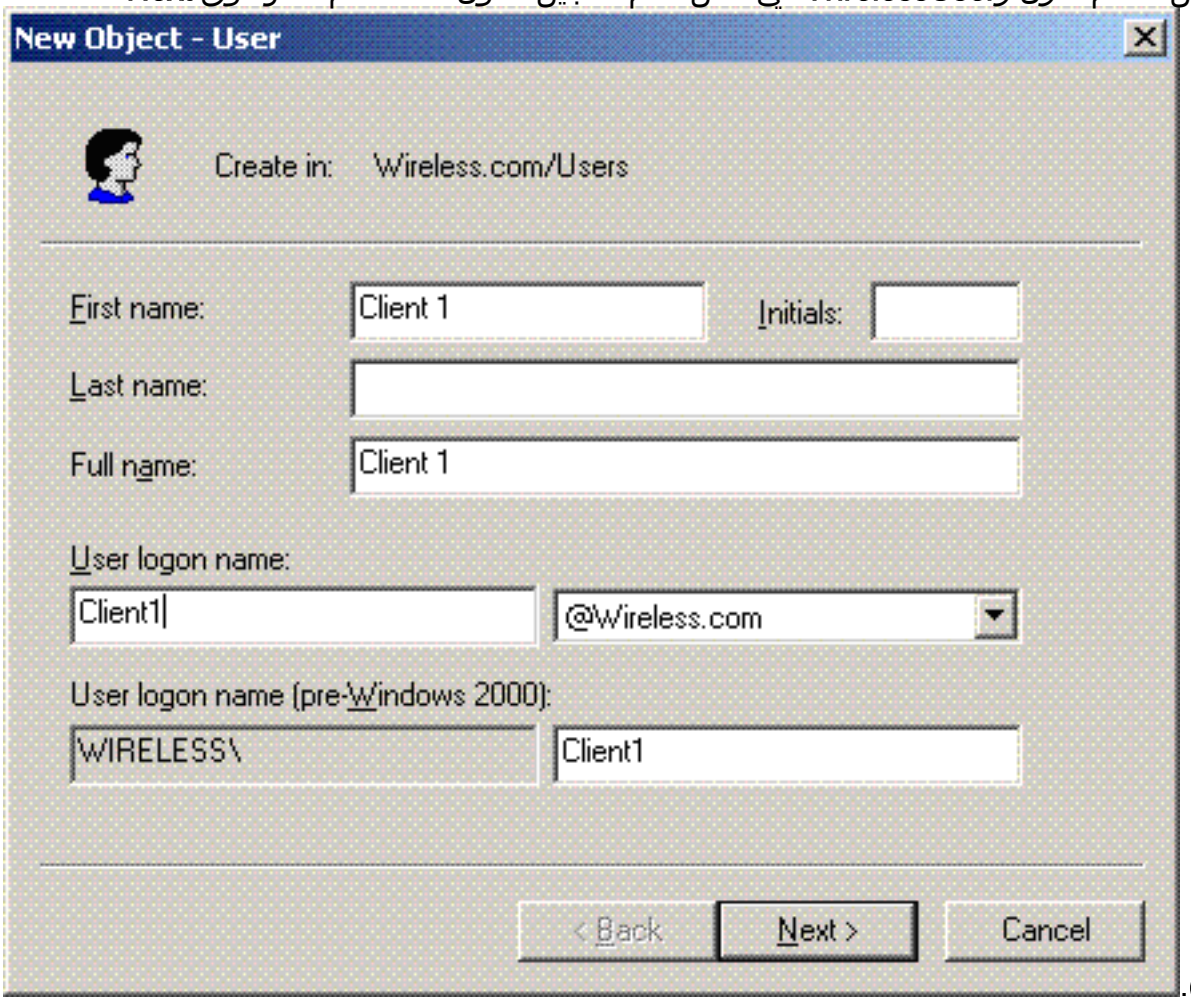
في هذا الإعداد، يتم الاحتفاظ بقاعدة بيانات المستخدم على Active Directory.

لإضافة مستخدمين إلى قاعدة بيانات Active Directory، أكمل الخطوات التالية:

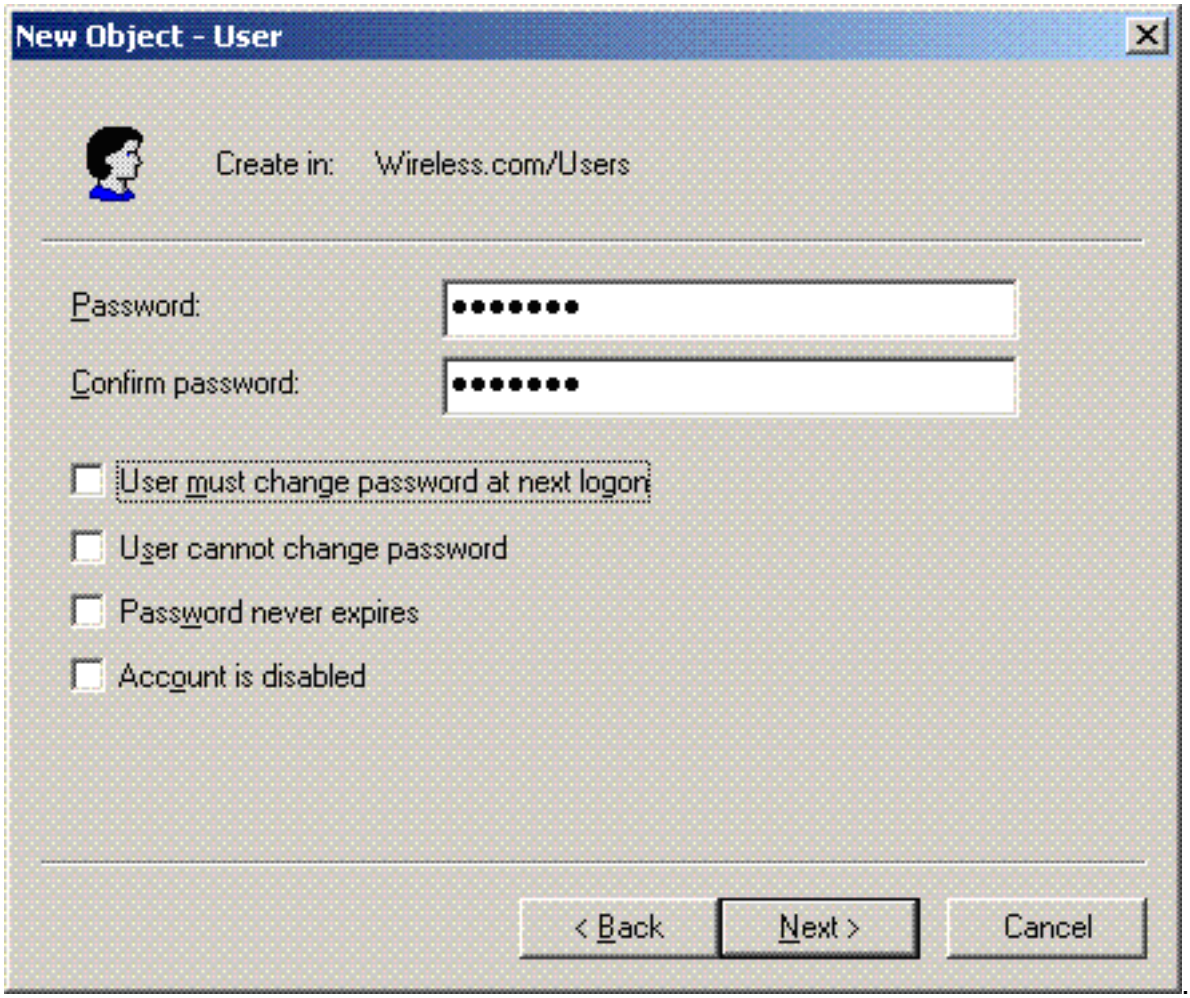
1. في شجرة وحدة تحكم مستخدمي Active Directory وأجهزة الكمبيوتر، انقر بزر الماوس الأيمن فوق **المستخدمين**، ثم انقر فوق **جديد**، ثم انقر فوق **مستخدم**.



2. في شاشة كائن جديد - مستخدم، اكتب اسم المستخدم اللاسلكي. يستخدم هذا المثال اسم **WirelessUser** في حقل الاسم الأول و**WirelessUser** في حقل اسم تسجيل دخول المستخدم. انقر فوق **Next** (التالي).

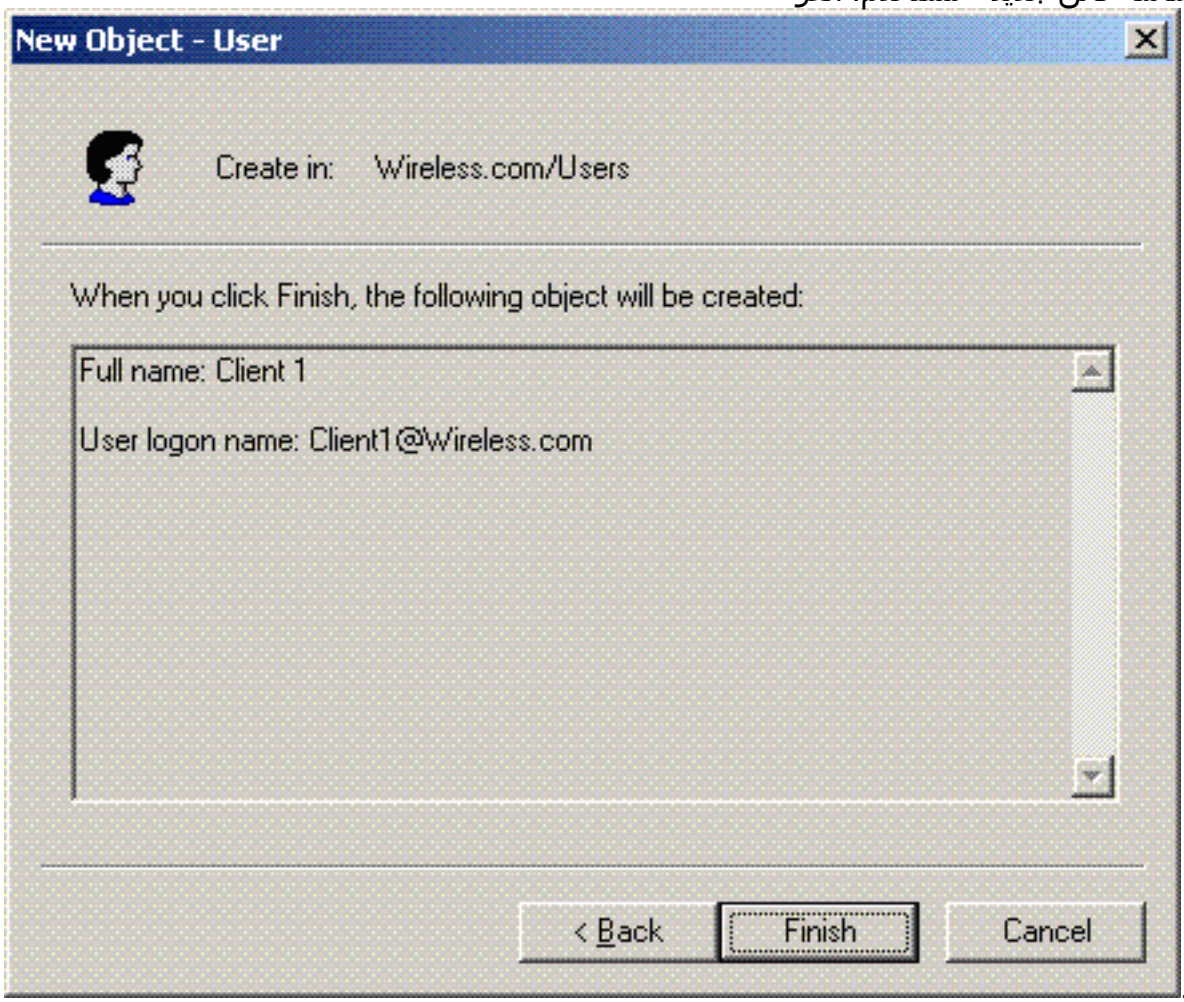


3. في شاشة كائن جديد - مستخدم، اكتب كلمة مرور من إختيارك في حقول كلمة المرور و قم بتأكيد كلمة المرور. امسح **المستخدم يجب أن يغير كلمة المرور في** خانة الاختيار **تسجيل الدخول التالي**، ثم انقر فوق



التالي.

4. في شاشة كائن جديد - مستخدم، انقر



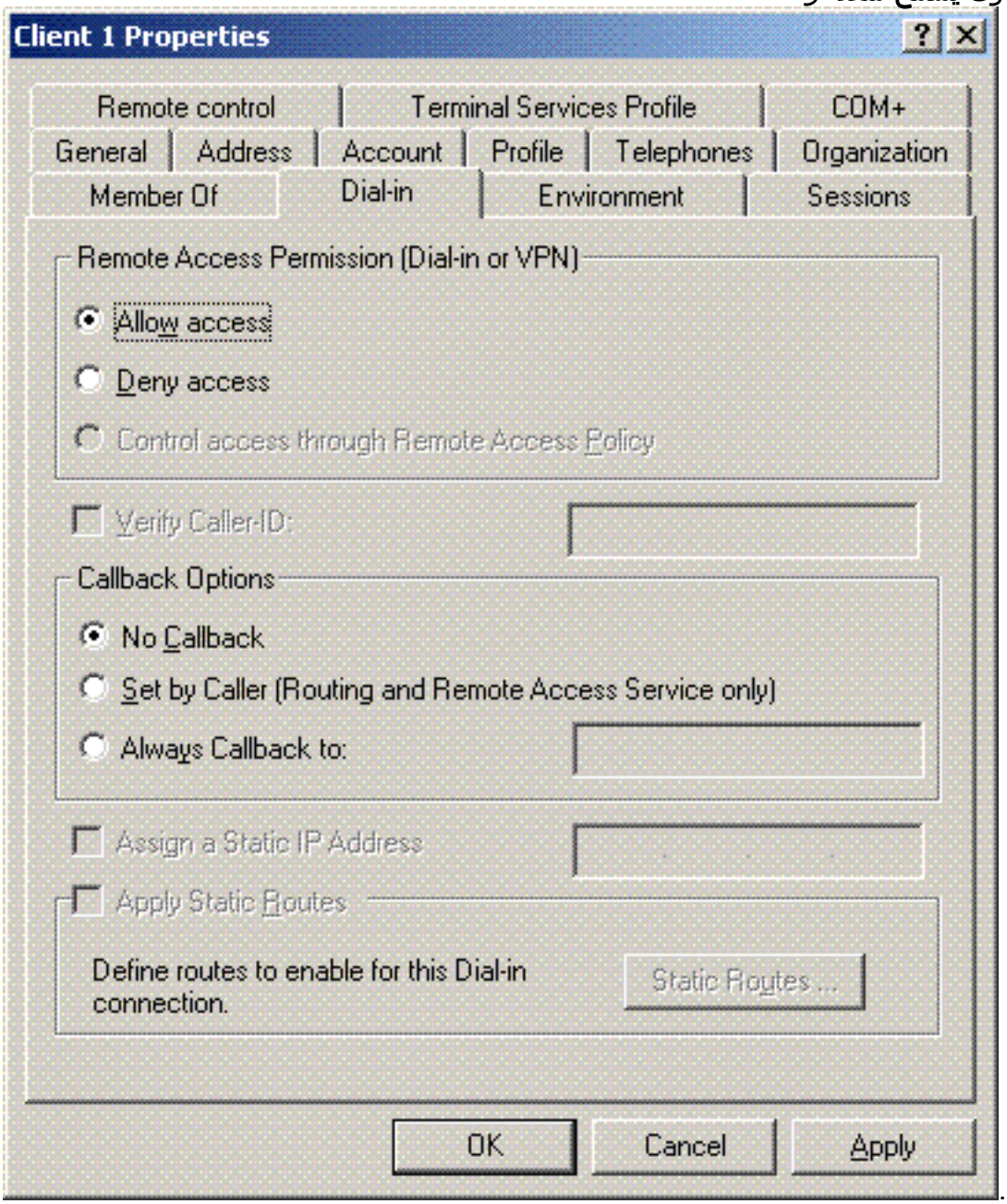
إنهاء.

5. كرر الخطوات من 2 إلى 4 لإنشاء حسابات مستخدمين إضافية.

السماح بالوصول اللاسلكي للمستخدمين

أكمل الخطوات التالية:

1. في شجرة وحدة تحكم مستخدمي Active Directory وأجهزة الكمبيوتر، انقر فوق المجلد **Users**؛ وانقر بزر الماوس الأيمن فوق **WirelessUser**؛ وانقر فوق **Properties**؛ ثم انتقل إلى علامة التبويب **طلب** الدخول.
2. أخترت **يسمح منفذ**، وطقطقة



.ok

تكوين وحدة التحكم في الشبكة المحلية اللاسلكية ونقاط الوصول في الوضع Lightweight

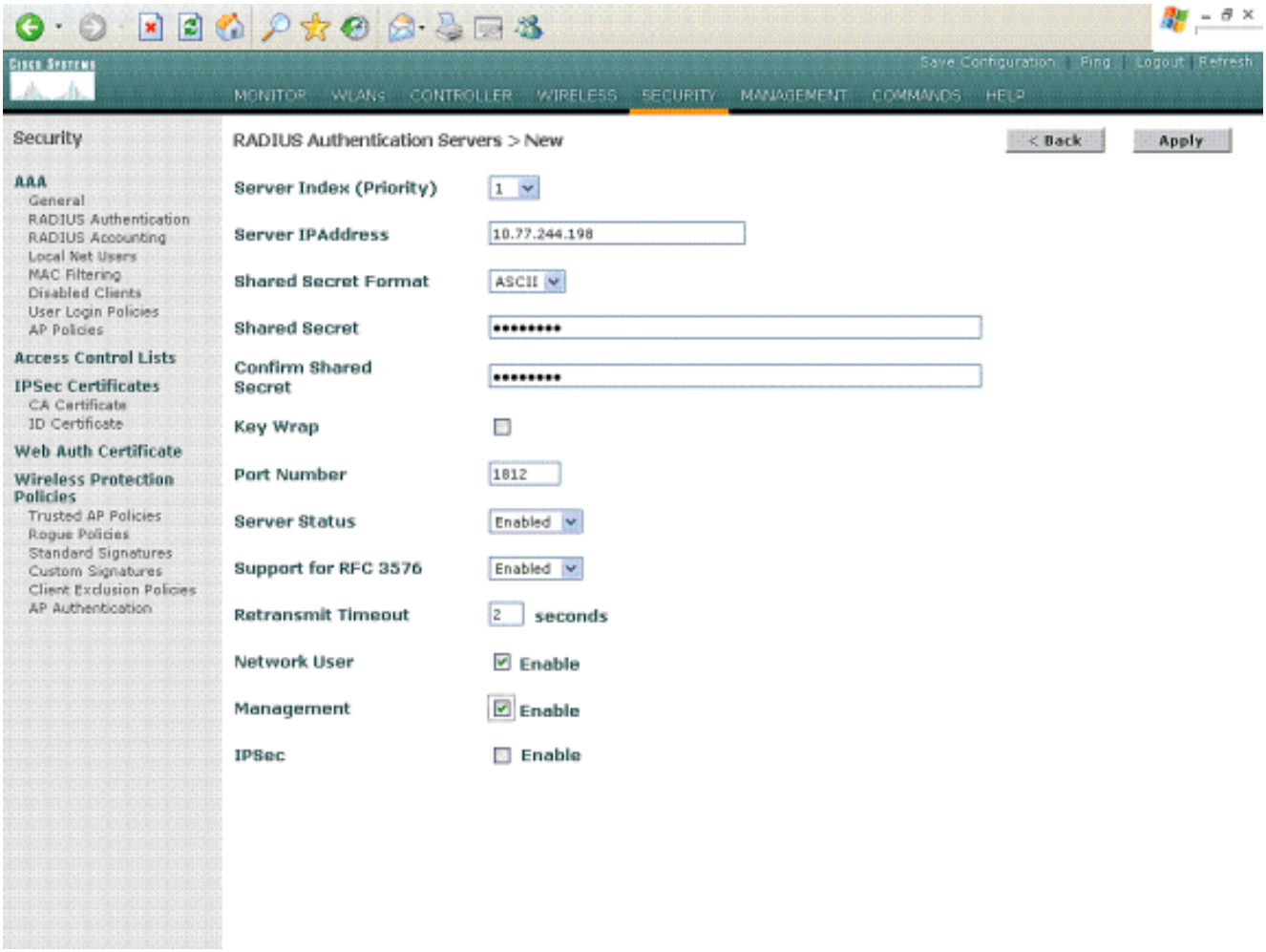
قم الآن بتكوين الأجهزة اللاسلكية لهذا الإعداد. وهذا يتضمن تكوين وحدات التحكم في الشبكة المحلية اللاسلكية ونقاط الوصول في الوضع Lightweight والعملاء اللاسلكيين.

تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة RADIUS من خلال خادم MS IAS RADIUS

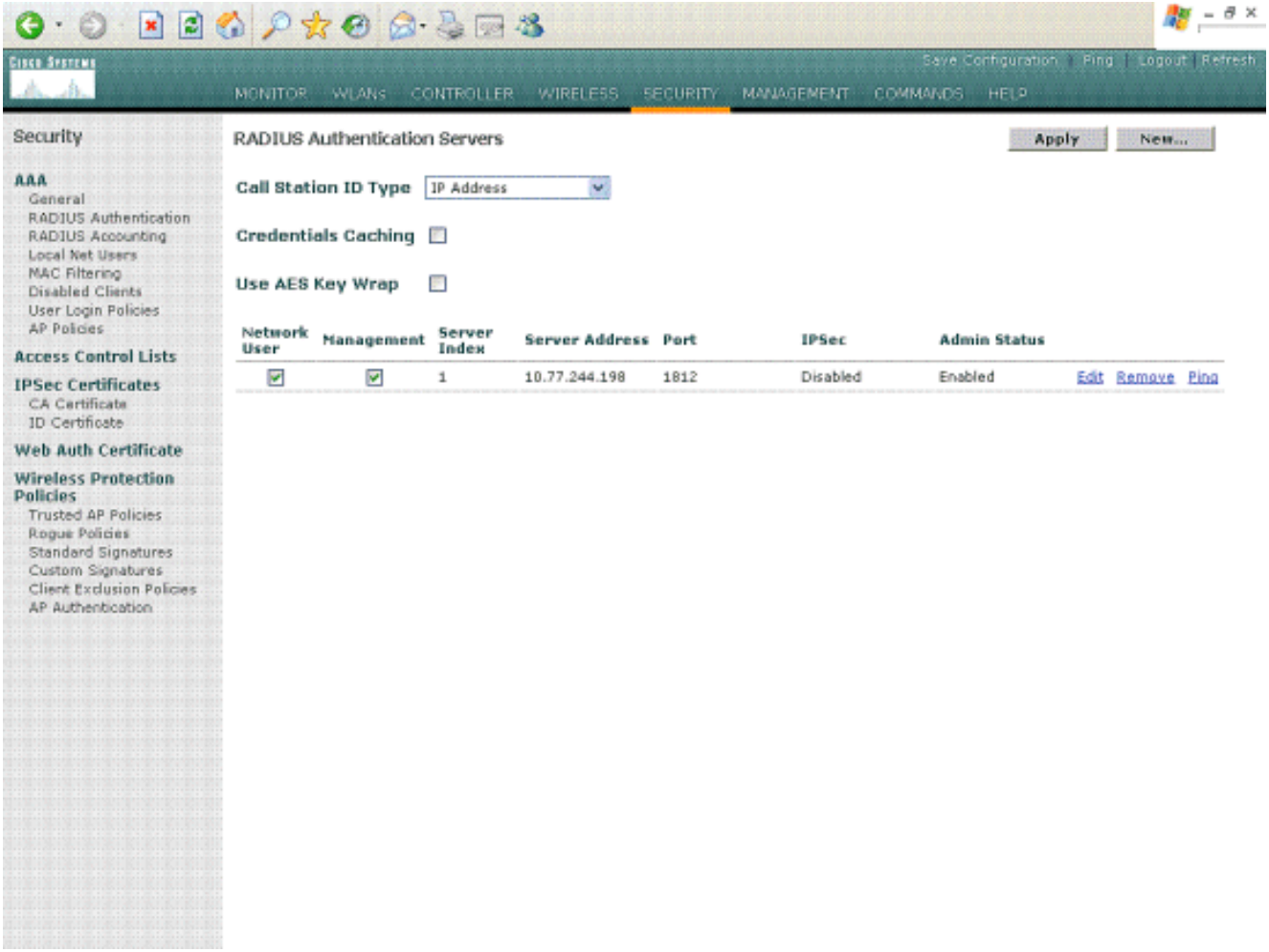
قم أولا بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لاستخدام MS IAS كخادم مصادقة. يلزم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإعادة توجيه بيانات اعتماد المستخدم إلى خادم RADIUS خارجي. ثم يتحقق خادم RADIUS الخارجي من مسوغات المستخدم ويوفر الوصول إلى عملاء اللاسلكي. للقيام بذلك، أضف خادم MS IAS كخادم RADIUS في صفحة **التأمين > مصادقة RADIUS**.

أكمل الخطوات التالية:

1. أخترت **أمن** و**RADIUS صحة هوية** من الجهاز تحكم gui أن يعرض ال RADIUS صحة هوية نادل صفحة. ثم انقر فوق **جديد** لتحديد خادم RADIUS.



2. قم بتعريف معلمات خادم RADIUS في **خوادم مصادقة RADIUS >** صفحة **جديدة**. وتتضمن هذه المعلمات عنوان IP لخادم RADIUS والسر المشترك ورقم المنفذ وحالة الخادم. تحدد خانات الاختيار الخاصة بمستخدم الشبكة وإدارتها ما إذا كانت المصادقة المستندة إلى RADIUS تنطبق على الإدارة ومستخدمي الشبكة. يستخدم هذا المثال MS IAS كخادم RADIUS بعنوان IP 10.77.244.198.



3. طقطقة **يطبق**.
4. تمت إضافة خادم MS IAS إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كخادم Radius ويمكن إستخدامه لمصادقة العملاء اللاسلكيين.

تكوين شبكة WLAN للعملاء

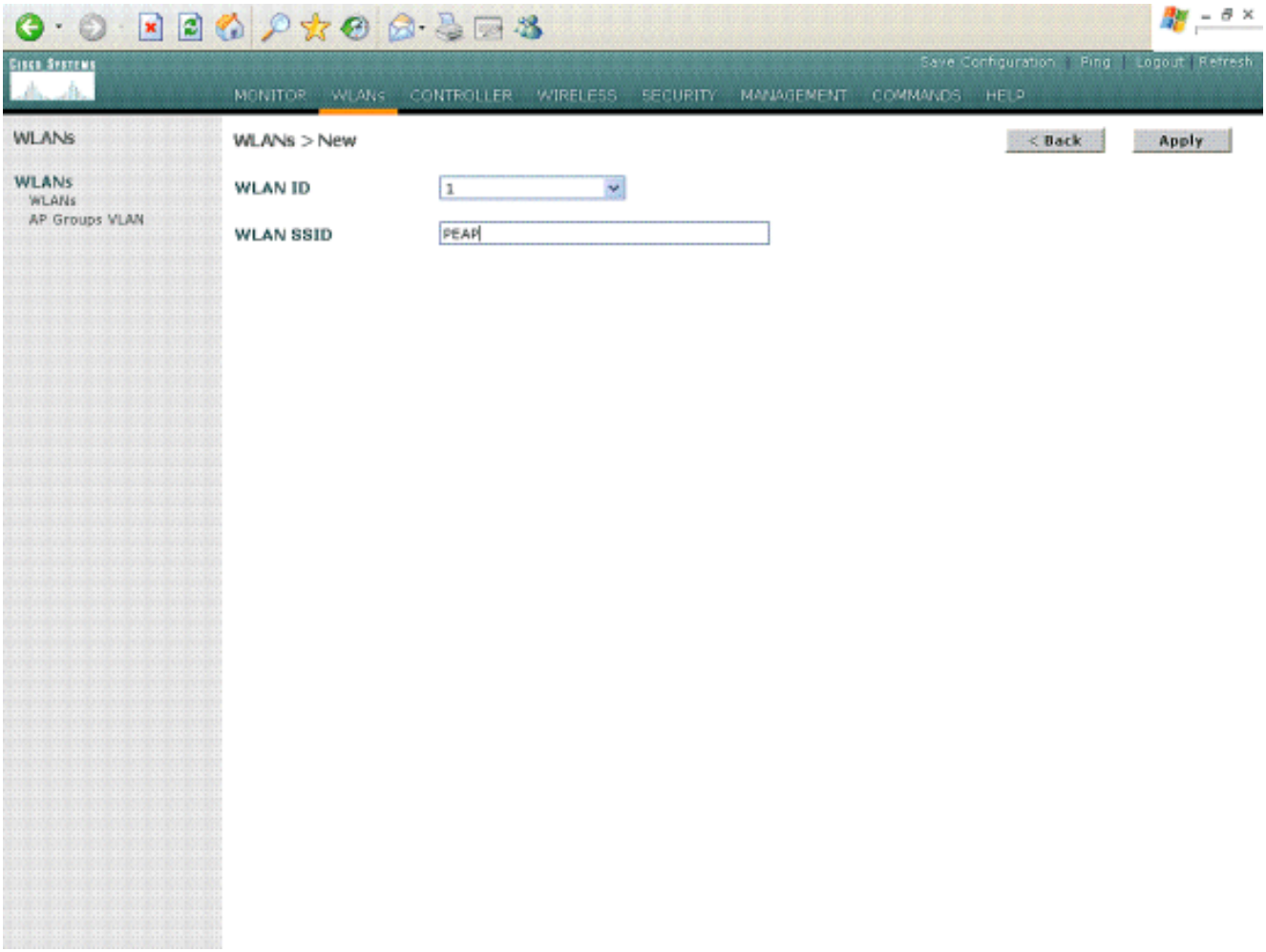
تكوين WLAN SSID) الذي يتصل به العملاء اللاسلكيين. في هذا المثال، قم بإنشاء SSID، وقم بتسميته **PEAP**.

قم بتعريف مصادقة الطبقة 2 على أنها WPA2 حتى يقوم العملاء بإجراء مصادقة تستند إلى EAP (PEAP-MSCHAPv2 في هذه الحالة) واستخدم AES كآلية تشفير. أترك كل القيم الأخرى عند وضعها الافتراضي.

ملاحظة: يربط هذا المستند شبكة WLAN بواجهات الإدارة. عندما يكون لديك شبكات VLAN متعددة في شبكتك، يمكنك إنشاء شبكة VLAN منفصلة وربطها بمعرف SSID. أحلت لمعلومة على كيف أن يشكل VLANs على WLCs، VLANs على لاسلكي lan جهاز تحكم تشكيل مثال.

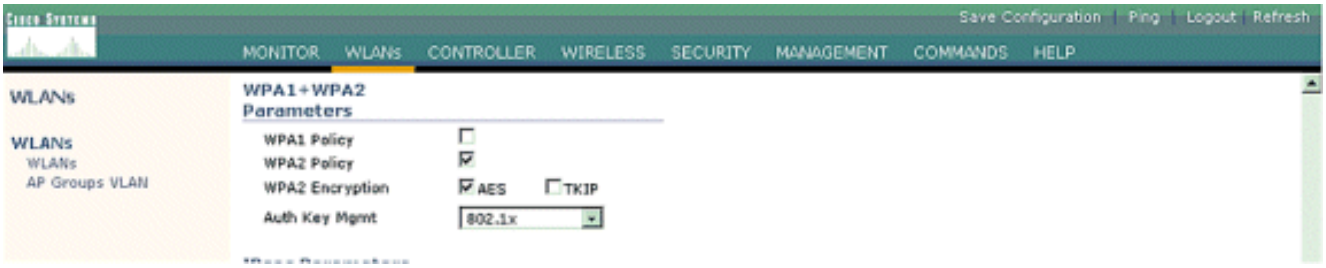
أتمت in order to شكلت WLAN على ال WLC هذا steps:

1. طقطقت **WLANs** من ال gui من الجهاز تحكم in order to عرضت WLANs صفحة. تسرد هذه الصفحة شبكات WLAN الموجودة على وحدة التحكم.
2. أخترت **جديد** in order to خلقت WLAN جديد. أدخل معرف WLAN و WLAN SSID للشبكة المحلية اللاسلكية (WLAN)، وانقر فوق **تطبيق**.

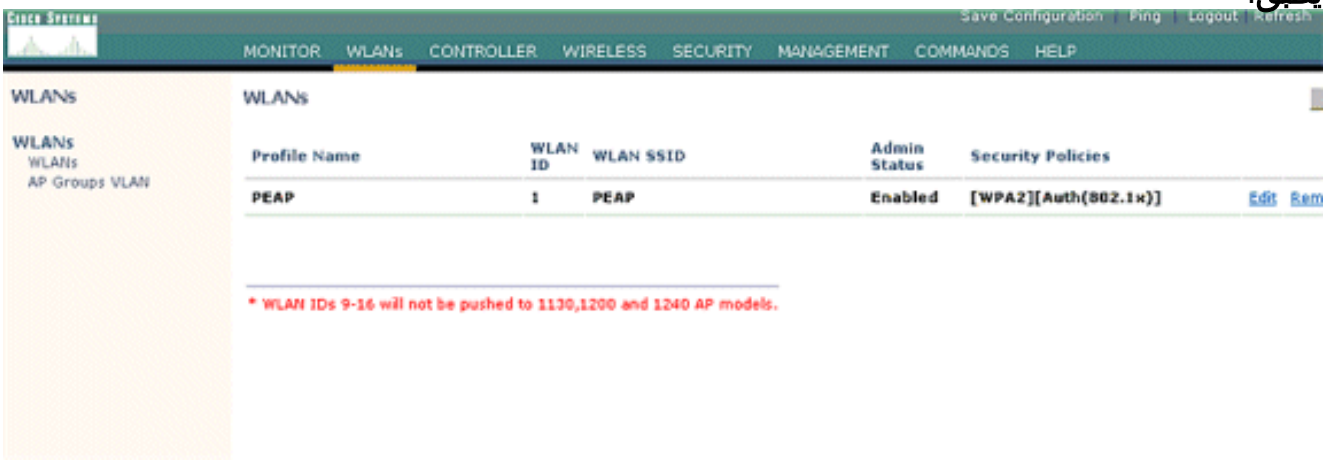


3. ما إن يخلق أنت WLAN جديد، ال **WLAN > تحرير** صفحة ل WLAN جديد يظهر. في هذه الصفحة، يمكنك تحديد معلمات مختلفة خاصة بشبكة WLAN هذه تتضمن السياسات العامة، وخوادم RADIUS، وسياسات الأمان، ومعاملات 802.1x.

4. تحقق من **حالة المسؤول** ضمن السياسات العامة لتمكين شبكة WLAN. إذا أردت لنقطة الوصول أن تبث SSID في إطارات منارتها، فتحقق من **بث SSID**.
5. تحت تأمين الطبقة 2، أختر **WPA1+WPA2**. هذا يمكن WPA على ال WLAN. انزلق إلى أسفل الصفحة واختر سياسة WPA. يستخدم هذا المثال تشفير WPA2 و AES. أختر خادم RADIUS المناسب من القائمة المنسدلة تحت خوادم RADIUS. في هذا المثال، أستخدم **10.77.244.198** (عنوان IP الخاص بخادم MS IAS). يمكن تعديل المعلمات الأخرى استنادا إلى متطلبات شبكة WLAN.



6. طقطقة **يطبق**.



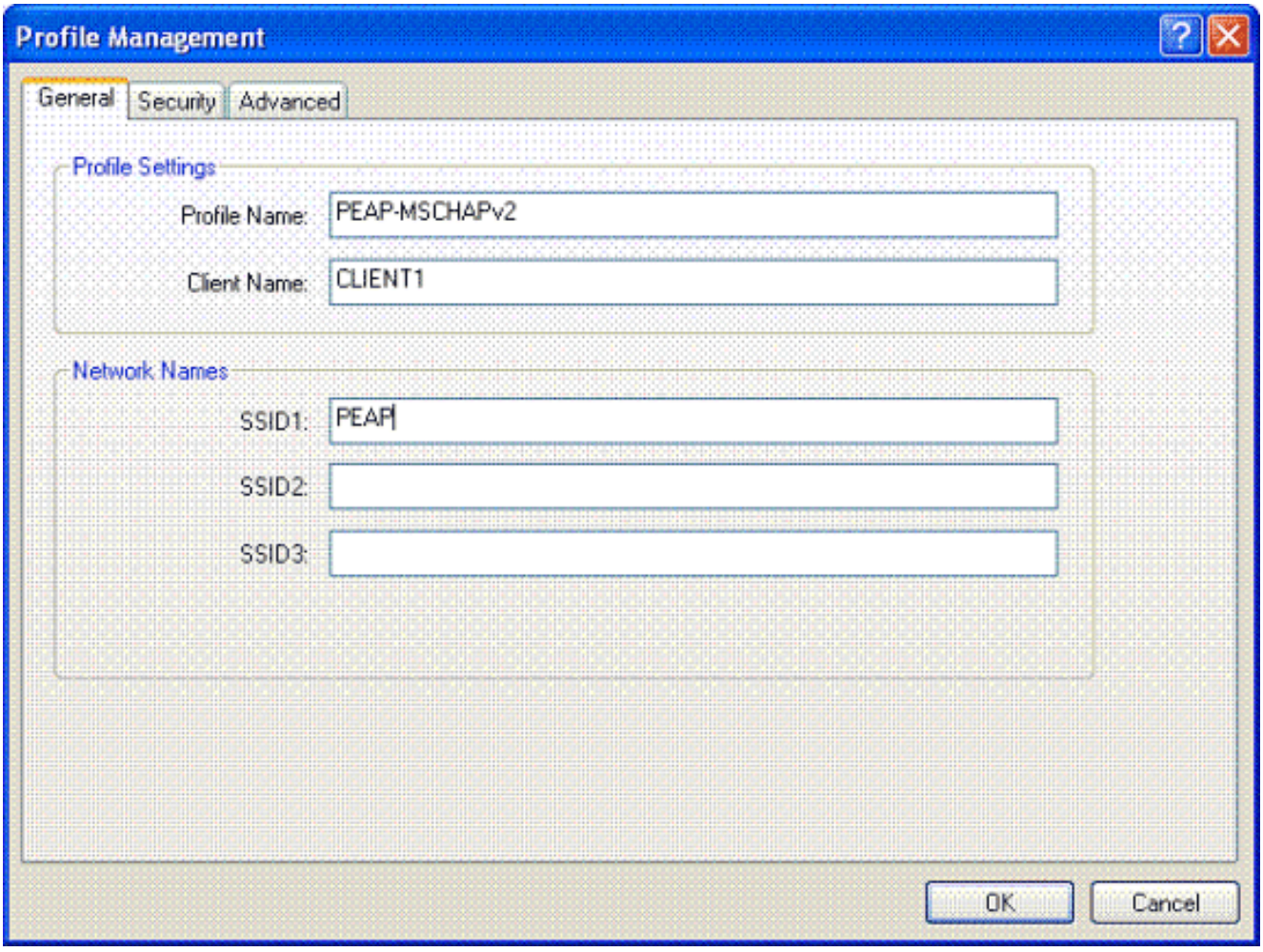
تكوين عملاء اللاسلكي

تكوين عملاء اللاسلكي لمصادقة PEAP-MS CHAPv2

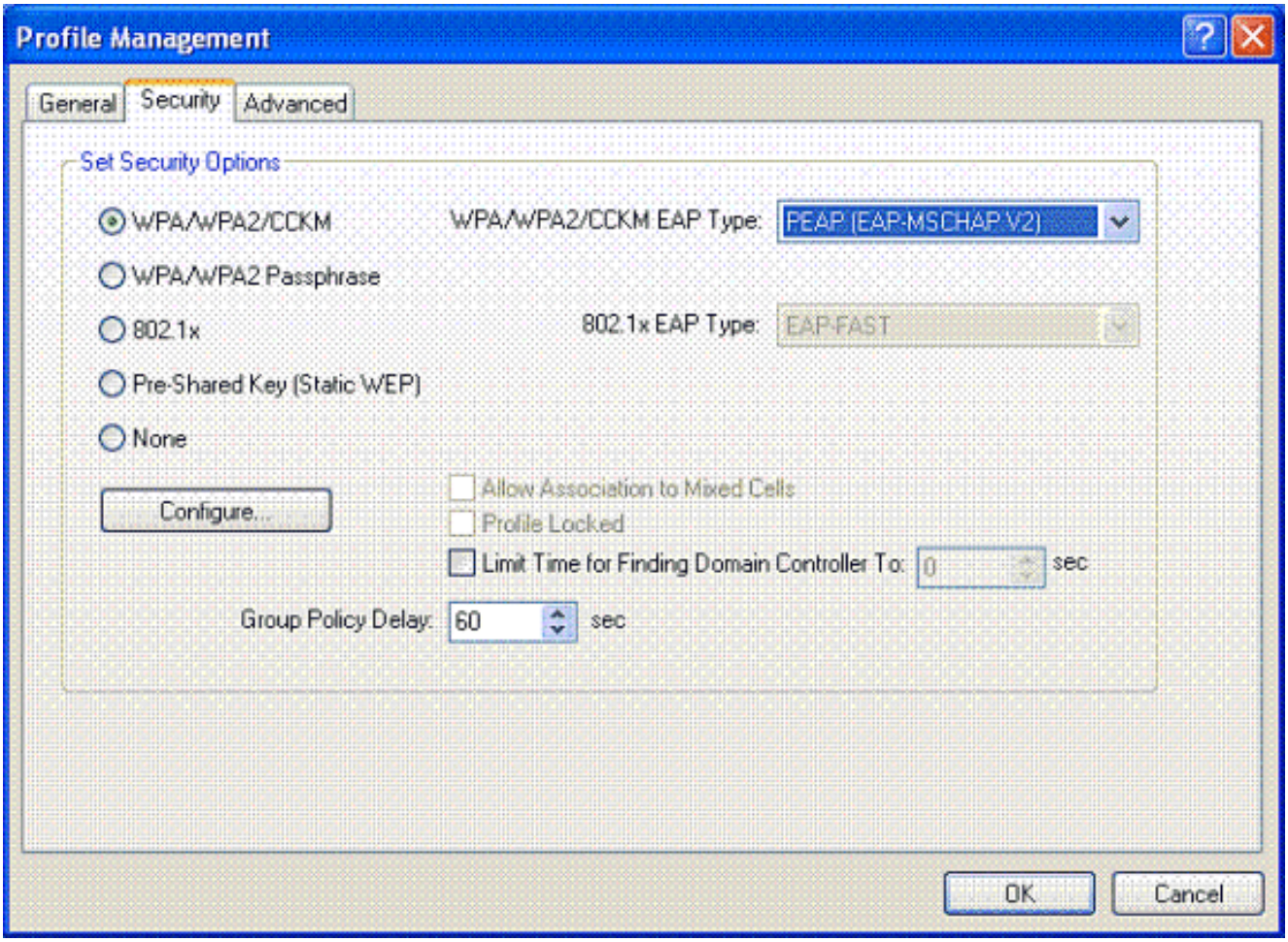
يقدم هذا المثال معلومات حول كيفية تكوين العميل اللاسلكي باستخدام أداة Cisco Aironet Desktop المساعدة. قبل تكوين مهايئ العميل، تأكد من إستخدام أحدث إصدار من البرامج الثابتة والأداة المساعدة. ابحث عن أحدث إصدار من البرامج الثابتة والأدوات المساعدة في صفحة تنزيلات الشبكات اللاسلكية على موقع الويب Cisco.com.

لتكوين مهايئ العميل اللاسلكي Cisco Aironet 802.11 a/b/g مع ADU، أكمل الخطوات التالية:

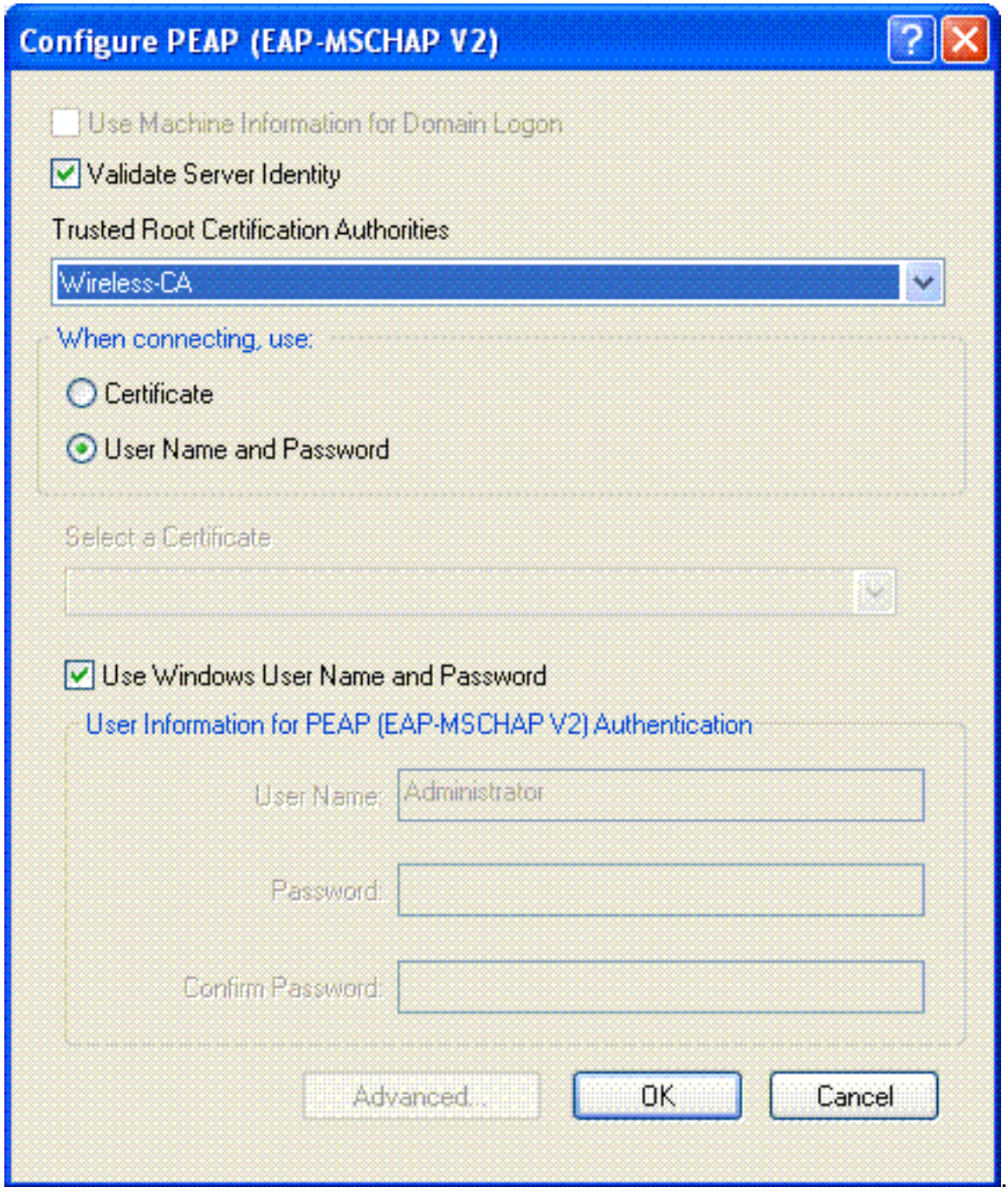
1. افتح أداة Aironet Desktop Utility.
2. انقر على **إدارة التوصيف**، وانقر **جديد** لتعريف توصيف.
3. تحت علامة التبويب عام أدخل اسم التوصيف و SSID. في هذا المثال، أستخدم معرف SSID الذي قمت بتكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية ((WLC PEAP)).



4. أختر علامة التبويب تأمين، أختر **WPA/WPA2/CCKM**، تحت WPA/WPA2/CCKM EAP، اكتب **PEAP [[EAP-MSCHAPv2]**، وانقر فوق **تكوين**.



5. أختر **التحقق من شهادة الخادم**، واختر **Wireless-CA** ضمن القائمة المنسدلة مراجع التصديق الجذر الموثوق

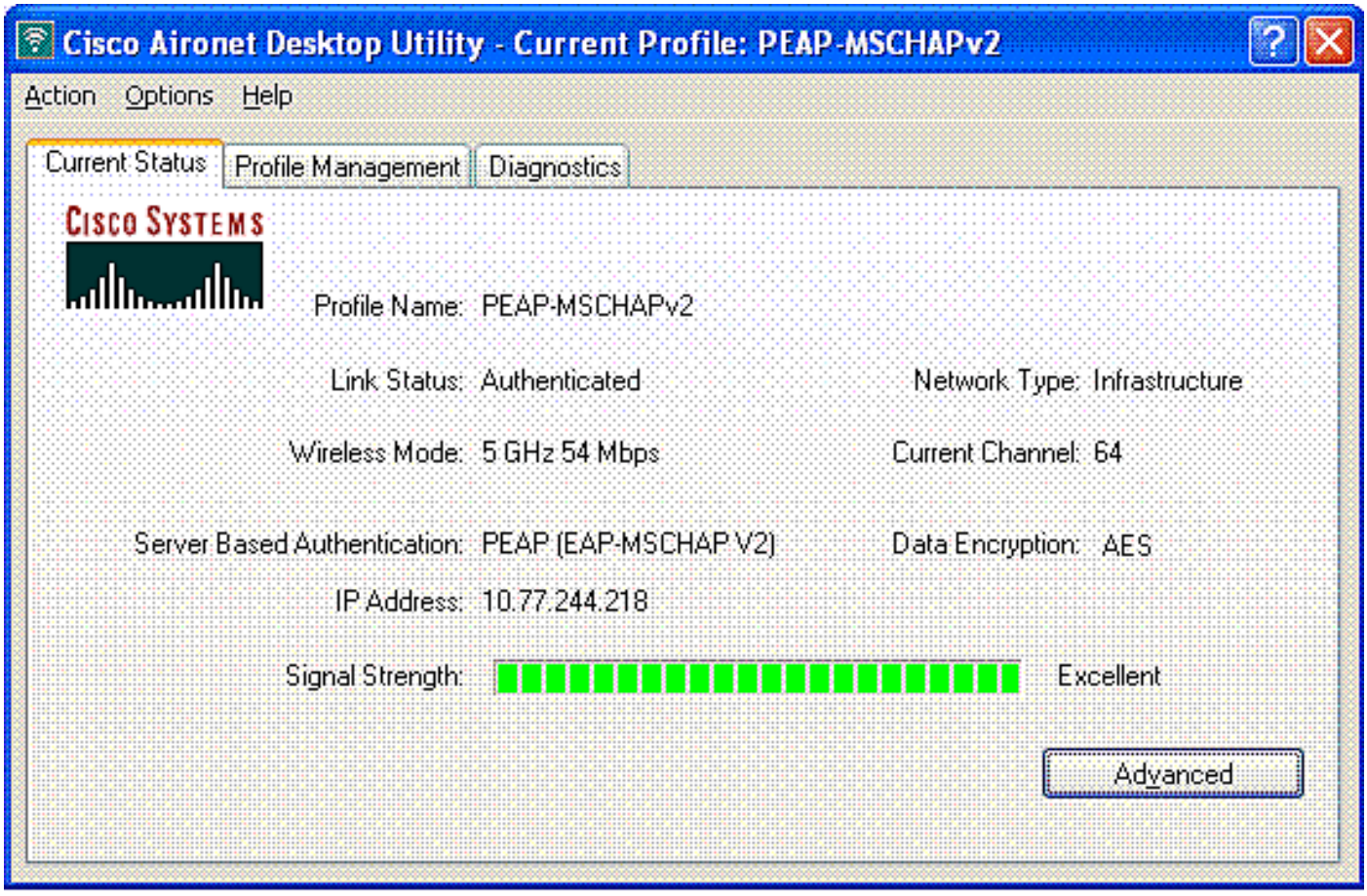


فيها.

6. انقر على **موافق**، وقم بتنشيط ملف التخصيص.**ملاحظة:** عند إستخدام بروتوكول المصادقة لتأكيد اتصال EAP-Microsoft مع التحدي المحمي الإصدار 2 (PEAP-MSCHAPv2) مع Microsoft XP SP2، تتم إدارة البطاقة اللاسلكية بواسطة Microsoft Wireless Zero Configuration (WZC)، يجب تطبيق Microsoft Hotfix KB885453. وهذا يؤدي إلى منع حدوث العديد من المشاكل في المصادقة المتعلقة بالاستئناف السريع ل PEAP.

التحقق من الصحة واستكشاف الأخطاء وإصلاحها

للتحقق من عمل التكوين كما هو متوقع، قم بتنشيط التوصيف PEAP-MSCHAPv2 على العميل اللاسلكي 1.



بمجرد تنشيط التوصيف PEAP-MSCHAPv2 على وحدة التحكم بالوصول (ADU)، يجري العميل مصادقة 802.11 مفتوحة ثم يجري مصادقة PEAP-MSCHAPv2. فيما يلي مثال على مصادقة PEAP-MSCHAPv2 الناجحة.

أستخدم أوامر تصحيح الأخطاء لفهم تسلسل الأحداث التي تحدث.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

تعد أوامر تصحيح الأخطاء هذه على وحدة التحكم في الشبكة المحلية اللاسلكية مفيدة.

- **debug dot1x events enable** — in order to شكلت ال debug لأحداث 802.1x
- **debug aaa events enable** — لتكوين تصحيح أحداث AAA
- **debug mac addr <mac address>** — in order to شكلت debug mac MAC debudebug command
- **debug dhcp رسالة** **enable** — in order to شكلت يضبط من DHCP خطأ رسالة

هذا هو المثال الذي ينتج من الأمر **debug dot1x events enable** و**debug client <mac address>** .

debug dot1x حادث يمكن:

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
                                                mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
                                                (mobile 00:40:96:ac:e6:57 (EAP Id 2
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
                                                mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
                                                mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
```

(mobile 00:40:96:ac:e6:57 (EAP Id 3
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Received EAP Response from**
(mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
(mobile 00:40:96:ac:e6:57 (EAP Id 4
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
(mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
(mobile 00:40:96:ac:e6:57 (EAP Id 5
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
(mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
(mobile 00:40:96:ac:e6:57 (EAP Id 6
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
(mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
(mobile 00:40:96:ac:e6:57 (EAP Id 7
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
(mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
(mobile 00:40:96:ac:e6:57 (EAP Id 8
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
(mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
(mobile 00:40:96:ac:e6:57 (EAP Id 9
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
(mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
(mobile 00:40:96:ac:e6:57 (EAP Id 10
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from
(mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
(mobile 00:40:96:ac:e6:57 (EAP Id 11
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from
(mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
(mobile 00:40:96:ac:e6:57 (EAP Id 12
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from
(mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Processing Access-Accept for**
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Creating a new PMK Cache**
(Entry for station 00:40:96:ac:e6:57 (RSN 0
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending EAP-Success to**
(mobile 00:40:96:ac:e6:57 (EAP Id 13
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to**

mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57**
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57**

:<debug mac addr <MAC address

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0**
- Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0
(Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20 (Change state to START (0**
(Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0 Initializing policy**
(Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0 (Change state to AUTHCHECK (2**
(Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2 (Change state to 8021X_REQD (3**
(Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3**
Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of (Mobile Station: 00:40:96:ac:e6:57 (callerId: 48
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to (station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
.Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Connecting state
-Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP (Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from mobile 00:40:96:ac:e6:57**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from Connecting to Authenticating for mobile 00:40:96:ac:e6:57**
- Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x moving mobile 00:40:96:ac:e6:57 into Authenticating state**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **(Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **(Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 (Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 (Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57

```
                Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
                        Processing Access-Challenge for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
             Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
            (Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5
                                    Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
    (Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25
                                    Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
                Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
                        Processing Access-Challenge for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
             Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
            (Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
    (Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
                Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
                        Processing Access-Challenge for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
           Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
           (Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   (Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
                Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
                        Processing Access-Challenge for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
           Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
           (Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   (Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
                Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
                          Processing Access-Accept for mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
           (Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
                    (Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
                            Sending default RC4 key to mobile 00:40:96:ac:e6:57
                                    Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
                       Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57
                     Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
                          (8021X_REQD (3) Change state to L2AUTHCOMPLETE (4
                     Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
                     Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
                                (L2AUTHCOMPLETE (4) Change state to RUN (20
                   Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
                                 Reached PLUMBFASTPATH: from line 4041 (20)
                   Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
                                       Replacing Fast Path rule (20)
                                          type = Airespace AP Client
                                    on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
   ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
```

```
(Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20
                      ,Card = 0 (slot 0), InHandle = 0x00000000
                  OutHandle = 0x00000000, npuCryptoFlag = 0x0000
      Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
             (Successfully plumbed mobile rule (ACL ID 255 (20)
      Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
                          Reached RETURN: from line 4041 (20)
       Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
         Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
      while in Authenticating state for mobile 00:40:96:ac:e6:57
               - Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x
    moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

ملاحظة: إذا كنت تستخدم ممول Microsoft للمصادقة مع مصدر ACS آمن من Cisco لمصادقة PEAP، فمن المحتمل ألا يقوم العميل بالمصادقة بنجاح. في بعض الأحيان، يمكن أن يصادق التوصيل الأولي بنجاح، لكن محاولات مصادقة التوصيل السريع التالية لا تتصل بنجاح. وهذه مسألة معروفة. تتوفر تفاصيل هذا الإصدار والإصلاحات الخاصة به هنا.

معلومات ذات صلة

- PEAP تحت شبكات لاسلكية موحدة مع ACS 4.0 و Windows 2003
- مصادقة EAP باستخدام مثال تكوين وحدات التحكم في الشبكة المحلية اللاسلكية (WLC)
- ترقية برنامج وحدة التحكم في شبكة LAN اللاسلكية (WLC) إلى الإصدارات 3.2 و 4.0 و 4.1
- أدلة تكوين وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية سلسلة Cisco 4400
- الدعم التقني والمستندات - Cisco Systems

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).