

# مَدْخَمُ عَمْدِ حُومِ عَيْكِلْسَالِ تَاكْبَشِ تَحْتِ PEAP مِنْ مِيسَرْتِنِإِلِإِ قَدَا صَمِ (IAS) مِيسَرْتِنِإِلِإِ

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[نظرة عامة على PEAP](#)

[التكوين](#)

[الرسم التخطيطي للشبكة](#)

[التكوينات](#)

[تكوين خادم Microsoft Windows 2003](#)

[تكوين خادم Microsoft Windows 2003](#)

[قم بتثبيت خدمات DHCP وتكوينها على خادم Microsoft Windows 2003](#)

[تثبيت خادم Microsoft Windows 2003 وتكوينه كخادم مرجع شهادات \(CA\)](#)

[توصيل العملاء بالمجال](#)

[تثبيت خدمة مصادقة الإنترنت على خادم Microsoft Windows 2003 وطلب شهادة](#)

[تكوين خدمة مصادقة الإنترنت لمصادقة PEAP-MS-CHAP v2](#)

[إضافة مستخدمين إلى Active Directory](#)

[السماح بالوصول اللاسلكي للمستخدمين](#)

[تكوين وحدة التحكم في الشبكة المحلية اللاسلكية ونقاط الوصول في الوضع Lightweight](#)

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

[تكوين شبكة WLAN للعملاء](#)

[تكوين عملاء اللاسلكي](#)

[تكوين عملاء اللاسلكي لمصادقة PEAP-MS CHAPv2](#)

[التحقق من الصحة واستكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

## 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 مثلا على التكوين المطلوب على خادم MS من أجل مصادقة PEAP - MS CHAP. تم اختبار تكوين خادم Microsoft المعروف 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 الأولى ومعلومات التكوين لوحدة 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 استخدام 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 وإستجابته: EAP-response/EAP-type=EAP-MS-CHAP-V2 (الإستجابة).
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.

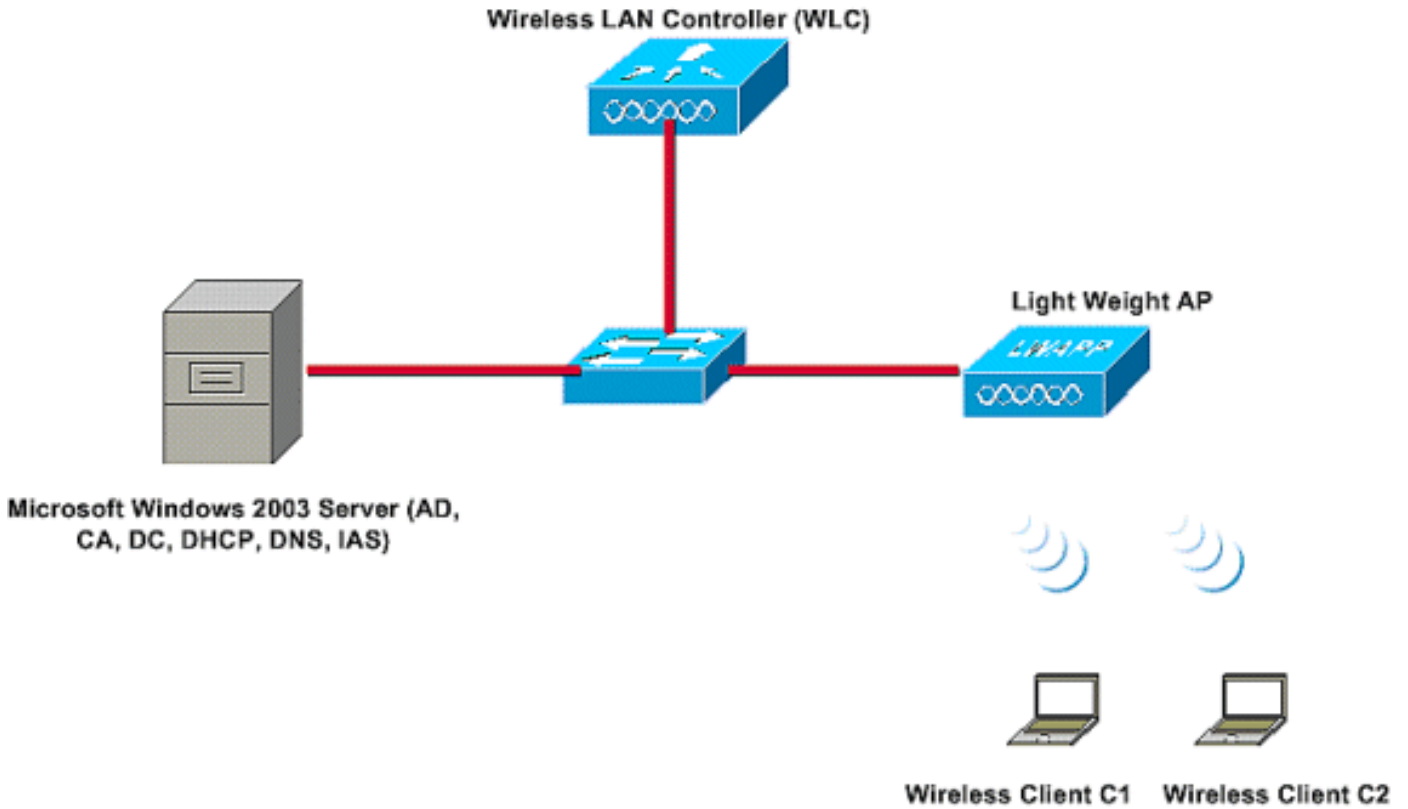
## التكوين

يقدم هذا المستند مثالاً لتكوين PEAP MS-CHAP v2.

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [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 العاملان اللاسلكيان C1 و C2 (WPA2 و 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 العملية 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.

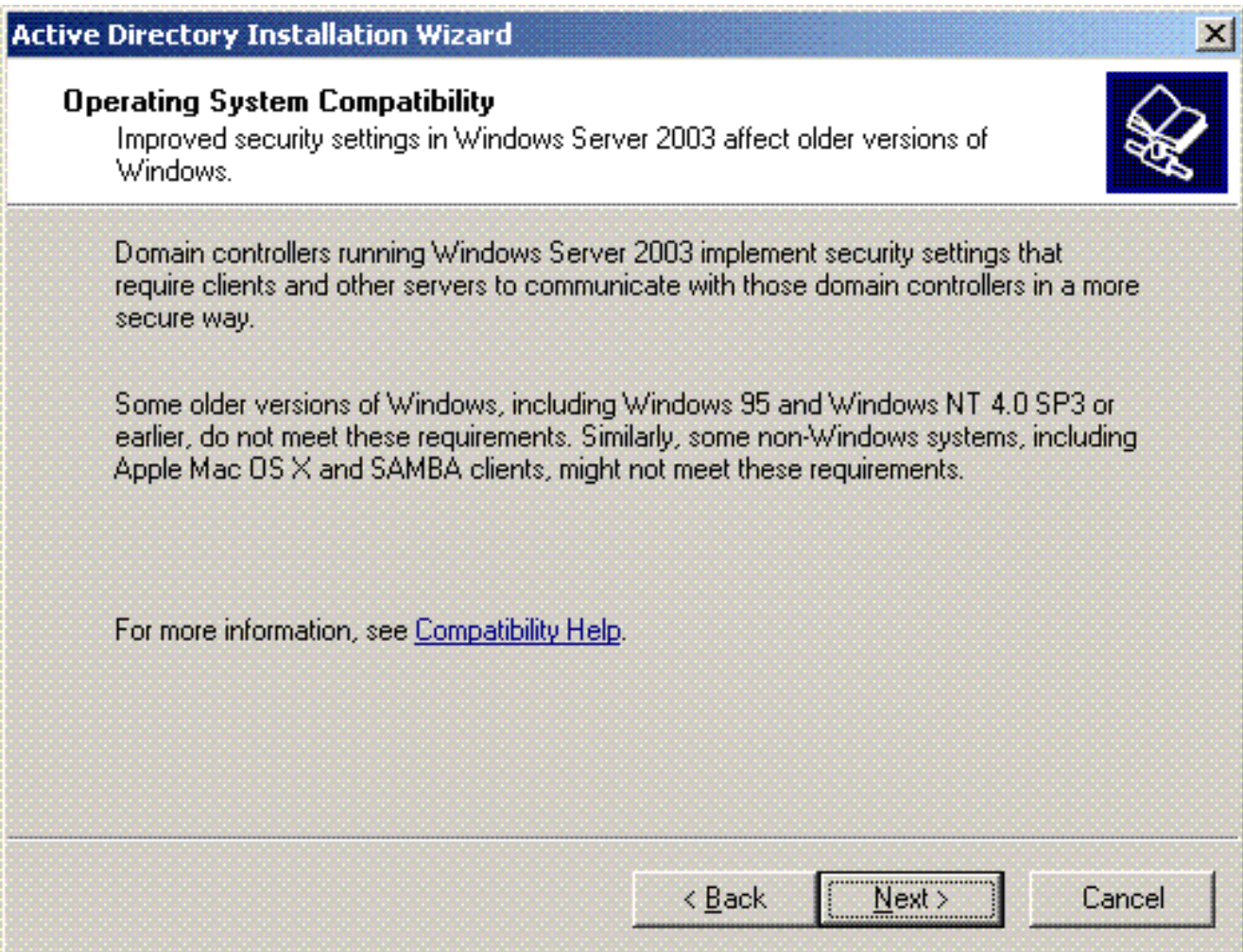
### تكوين خادم Microsoft Windows 2003 كوحدة تحكم بالمجال

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

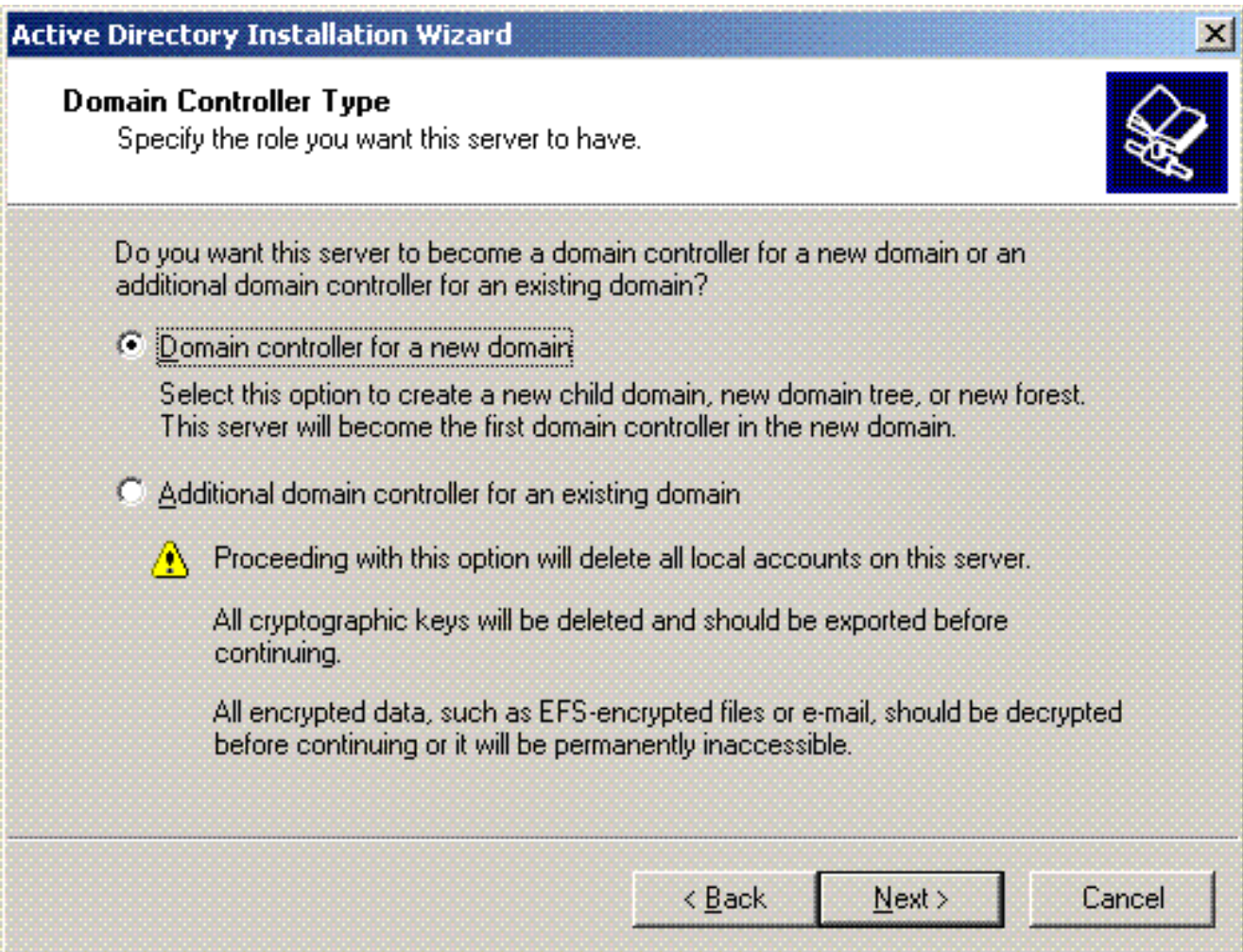
1. انقر فوق بدء، وانقر فوق تشغيل، واكتب `dcpromo.exe`، ثم انقر فوق موافق لبدء معالج تثبيت Active Directory.



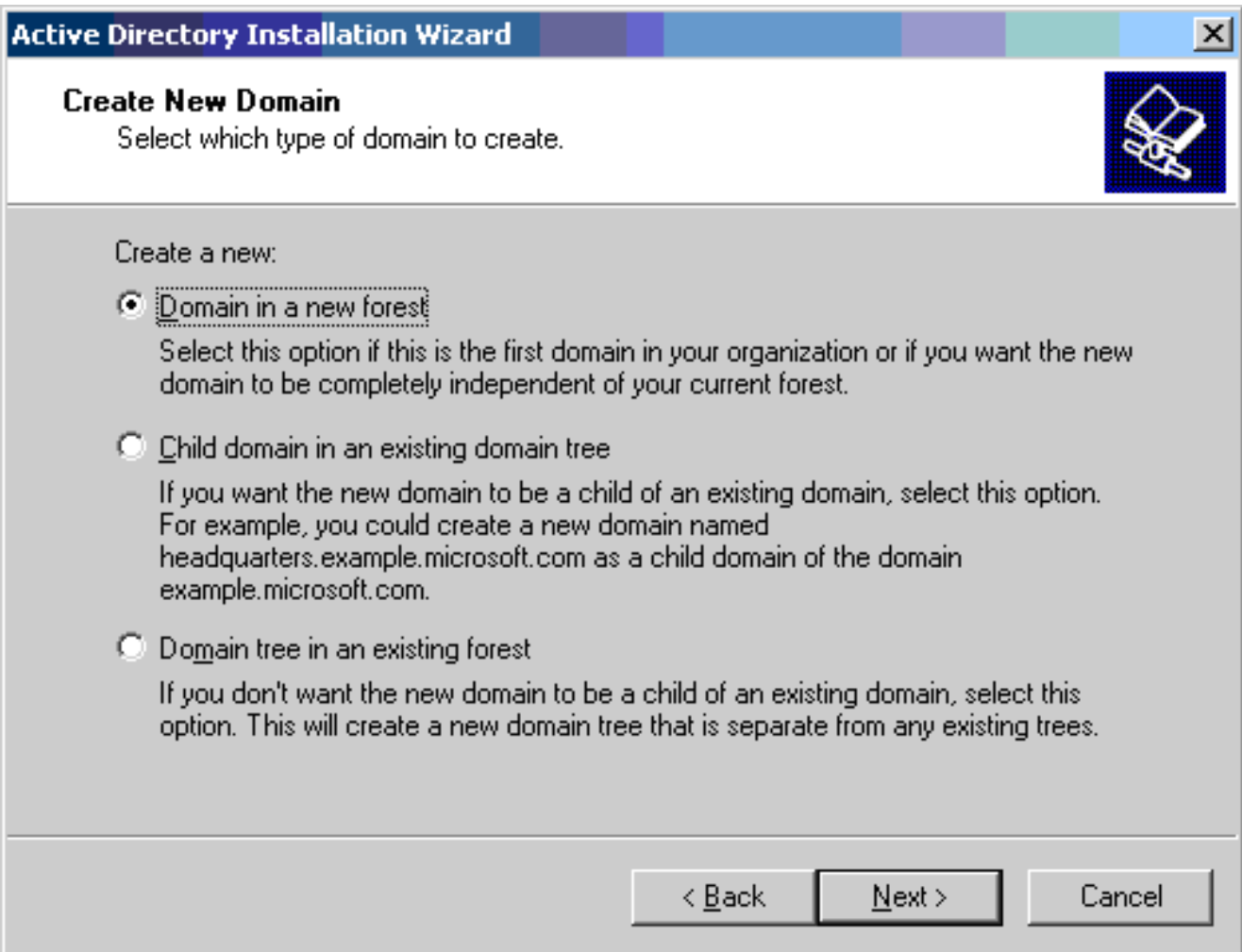
2. انقر فوق التالي لتشغيل معالج تثبيت Active Directory.



3. لإنشاء مجال جديد، اختر خيار وحدة التحكم بالمجال لمجال جديد.

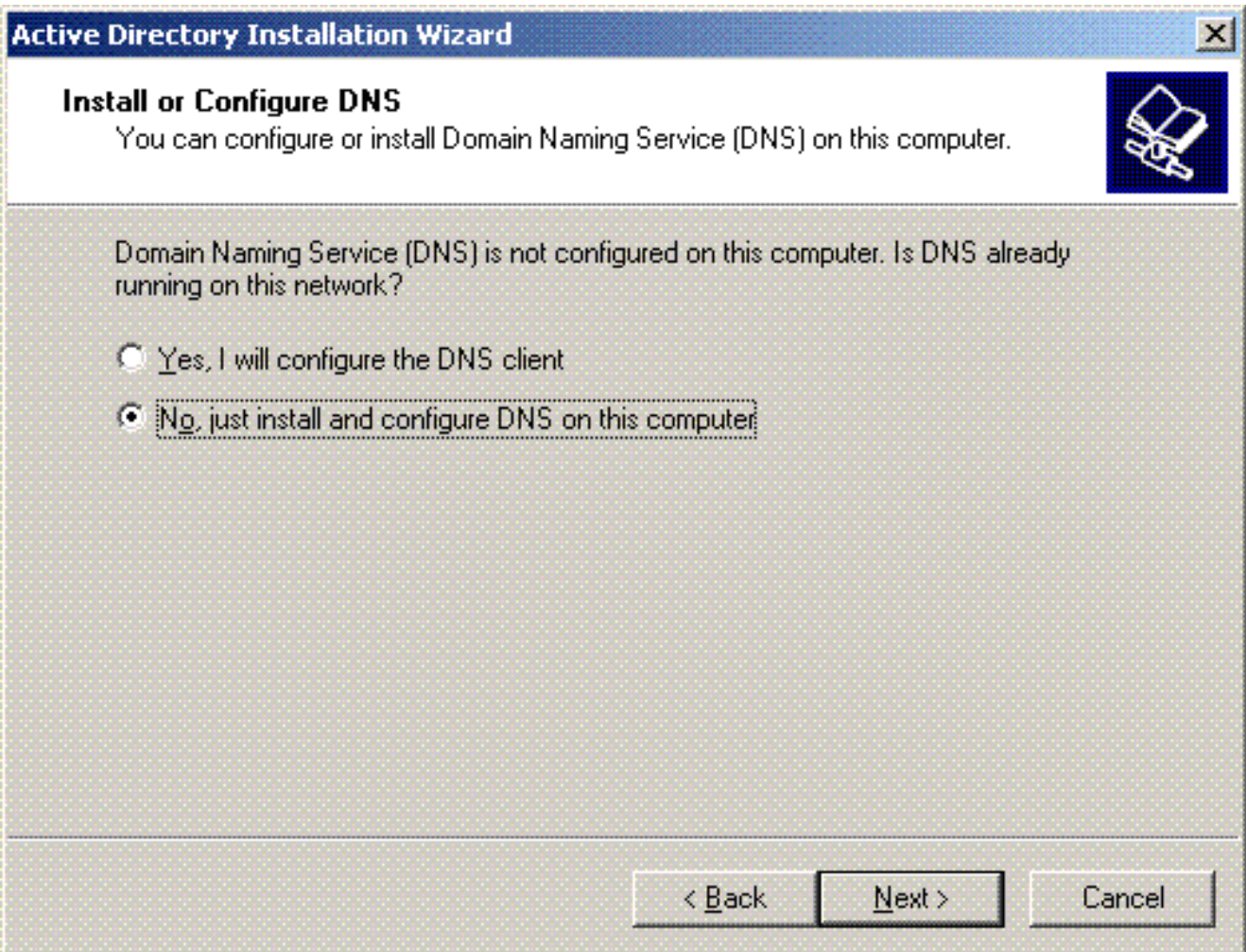


4. انقر فوق التالي لإنشاء غابة جديدة من أشجار المجال.

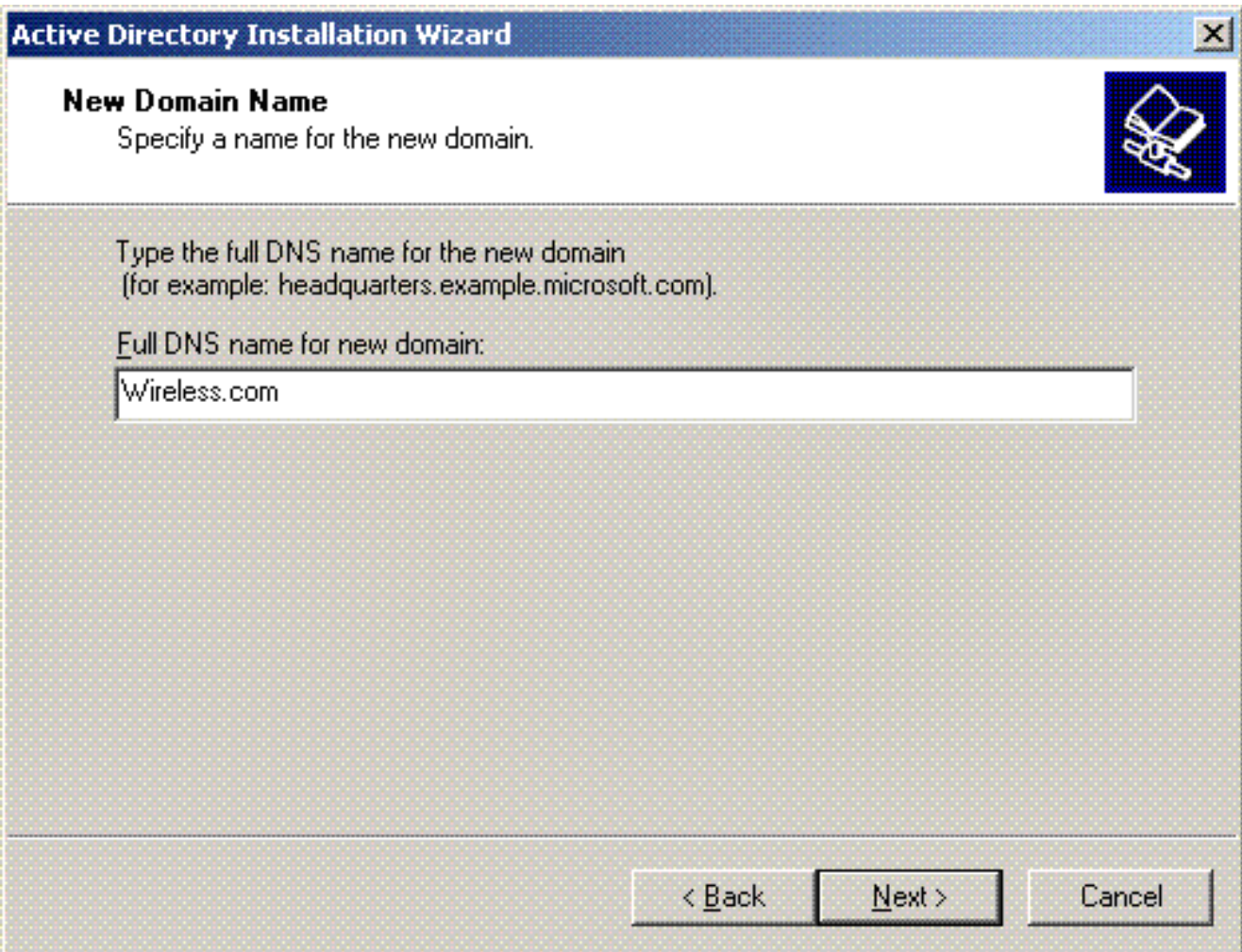


5. في حالة عدم تثبيت DNS على النظام، يوفر لك المعالج خيارات تكوين DNS بها. اختر لا، قم فقط بتثبيت DNS وتكوينه على هذا الكمبيوتر. انقر فوق **Next** (التالي).

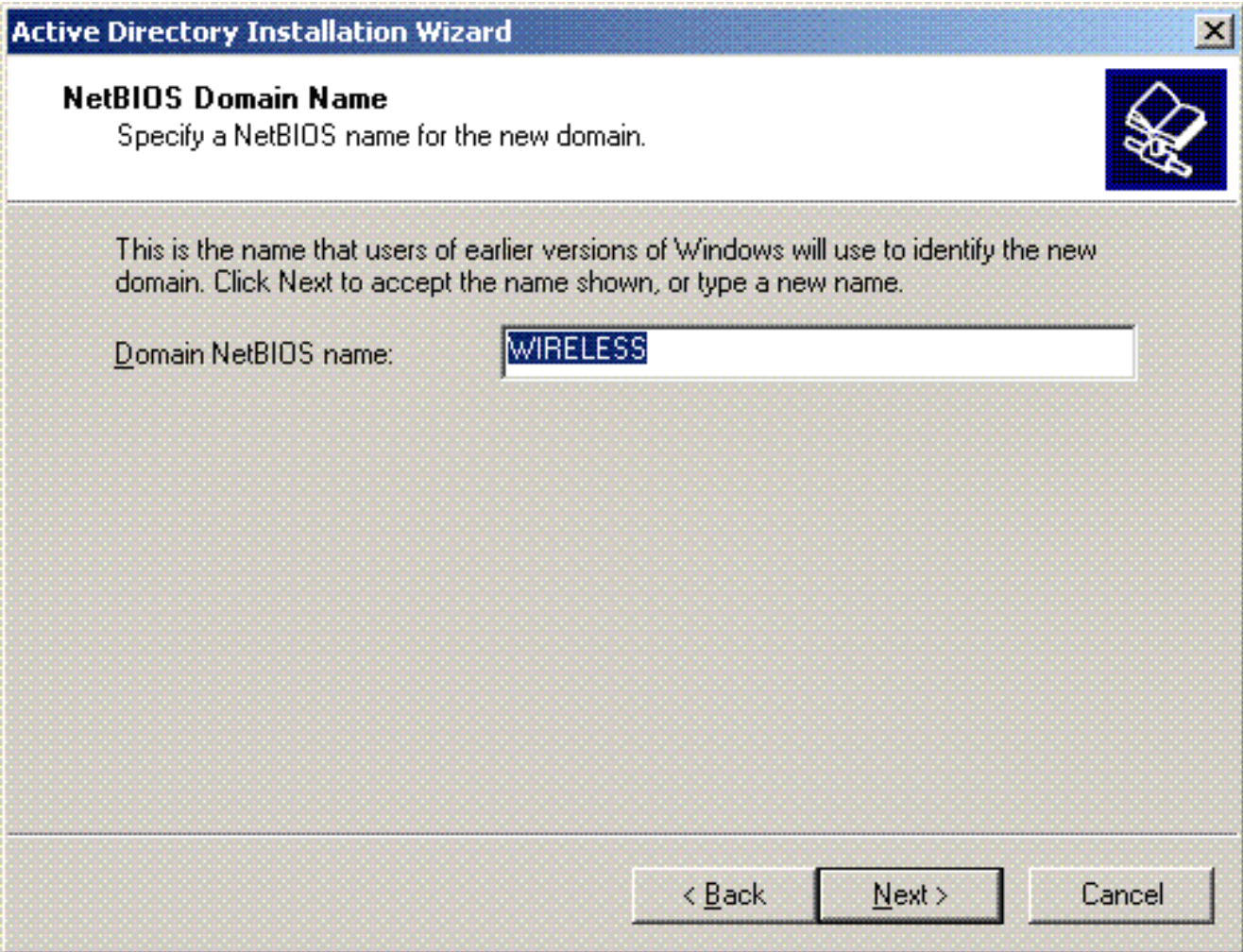




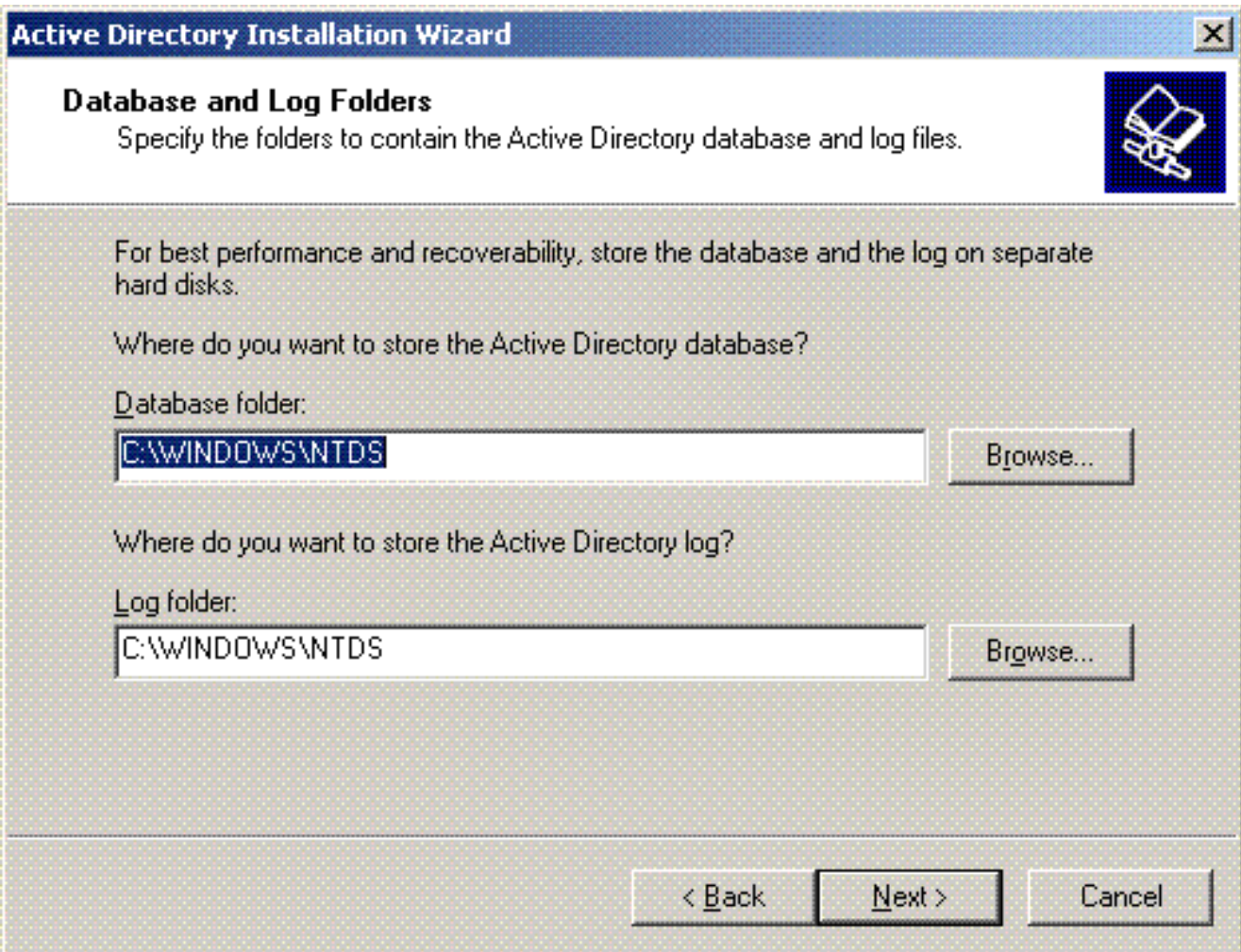
6. اكتب اسم DNS الكامل للمجال الجديد. في هذا المثال، يتم استخدام **Wireless.com** وانقر على التالي.



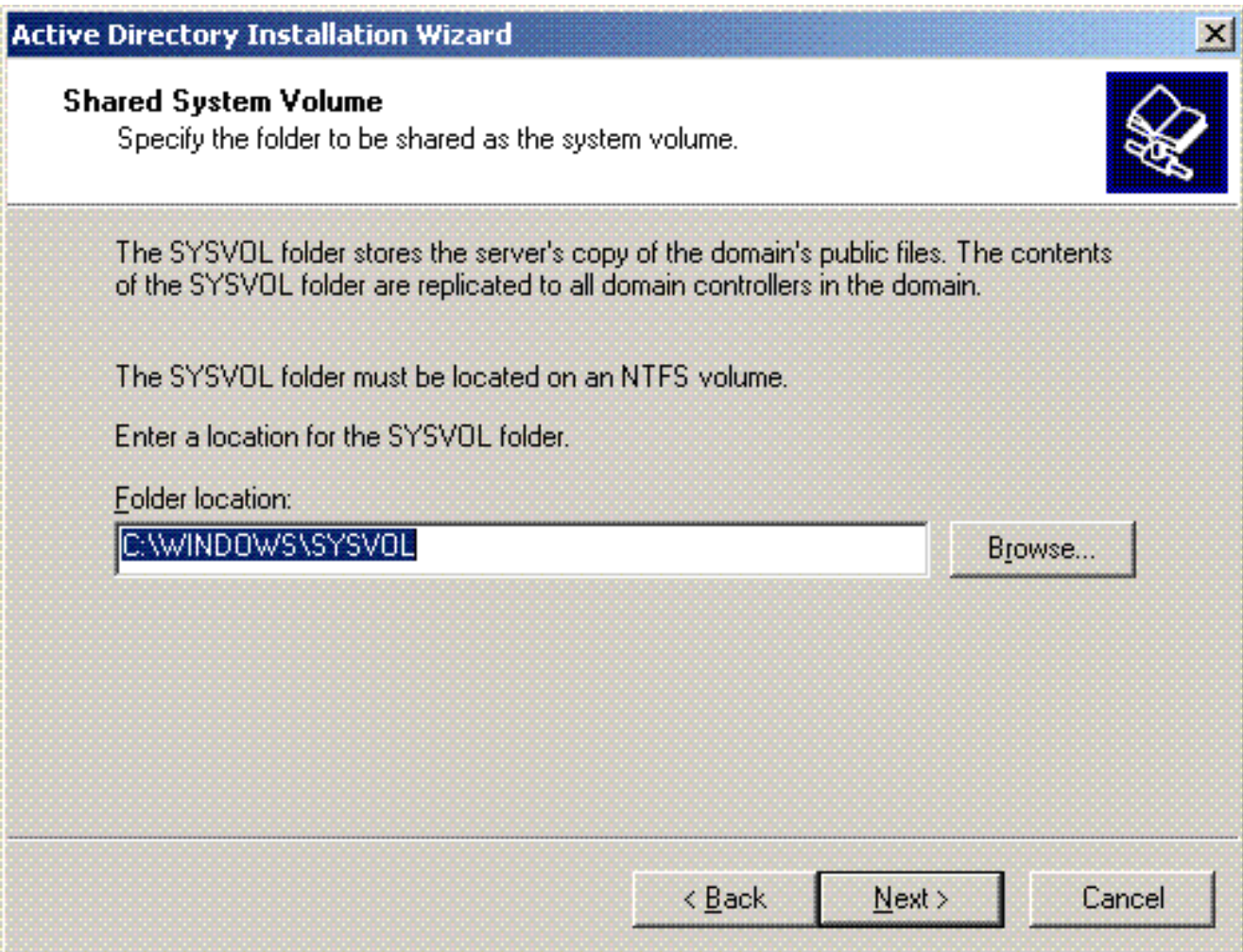
7. أدخل اسم NetBIOS للمجال وانقر على التالي. يستخدم هذا المثال الاتصال اللاسلكي.



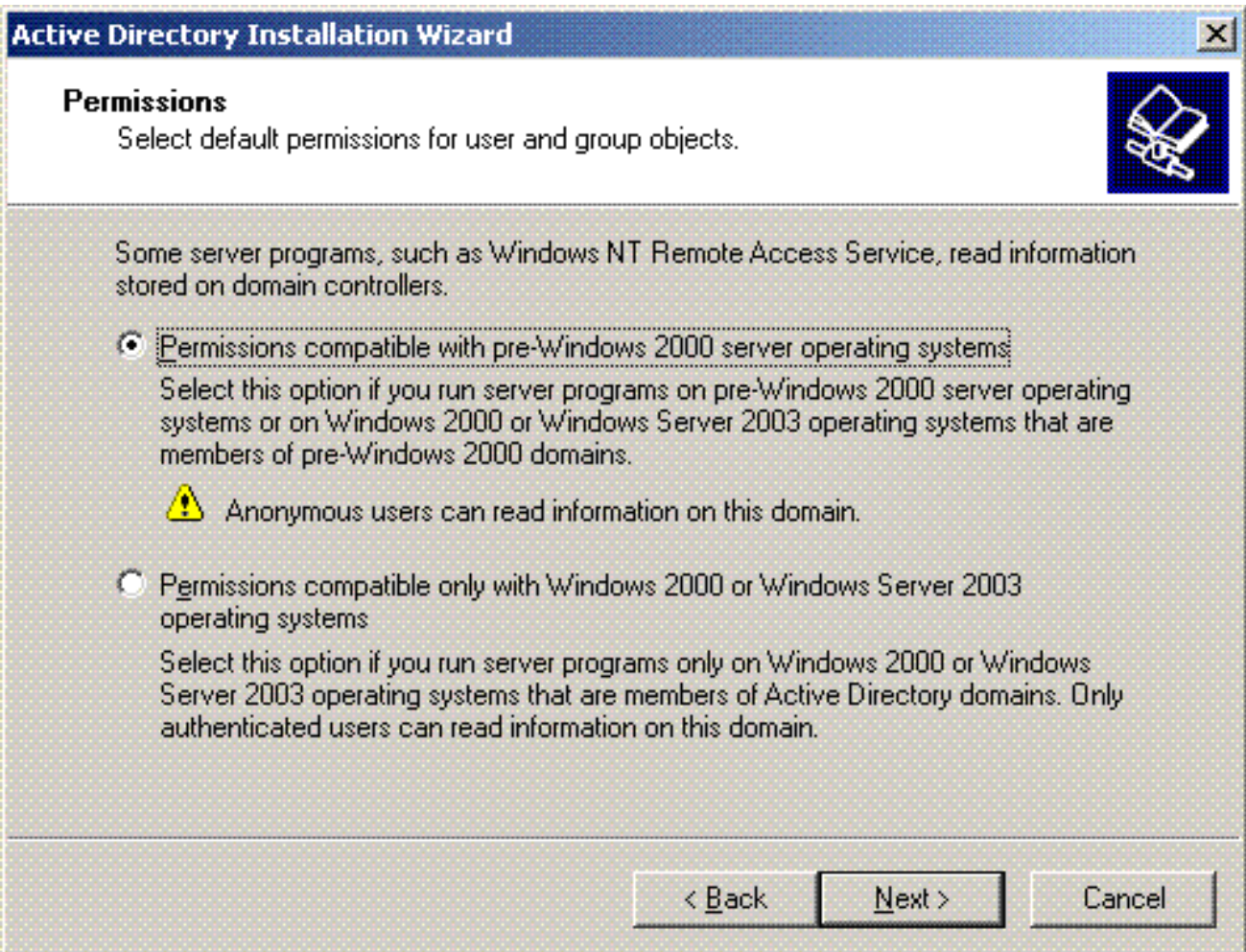
8. أختَر قاعدة البيانات ومواقع السجلات للمجال. انقر فوق **Next** (التالي).



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



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




11. ثبتت الإدارة كلمة مرور وطققة بعد ذلك.

**Active Directory Installation Wizard** [X]

### Directory Services Restore Mode Administrator Password

This password is used when you start the computer in Directory Services Restore Mode.



Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.

The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

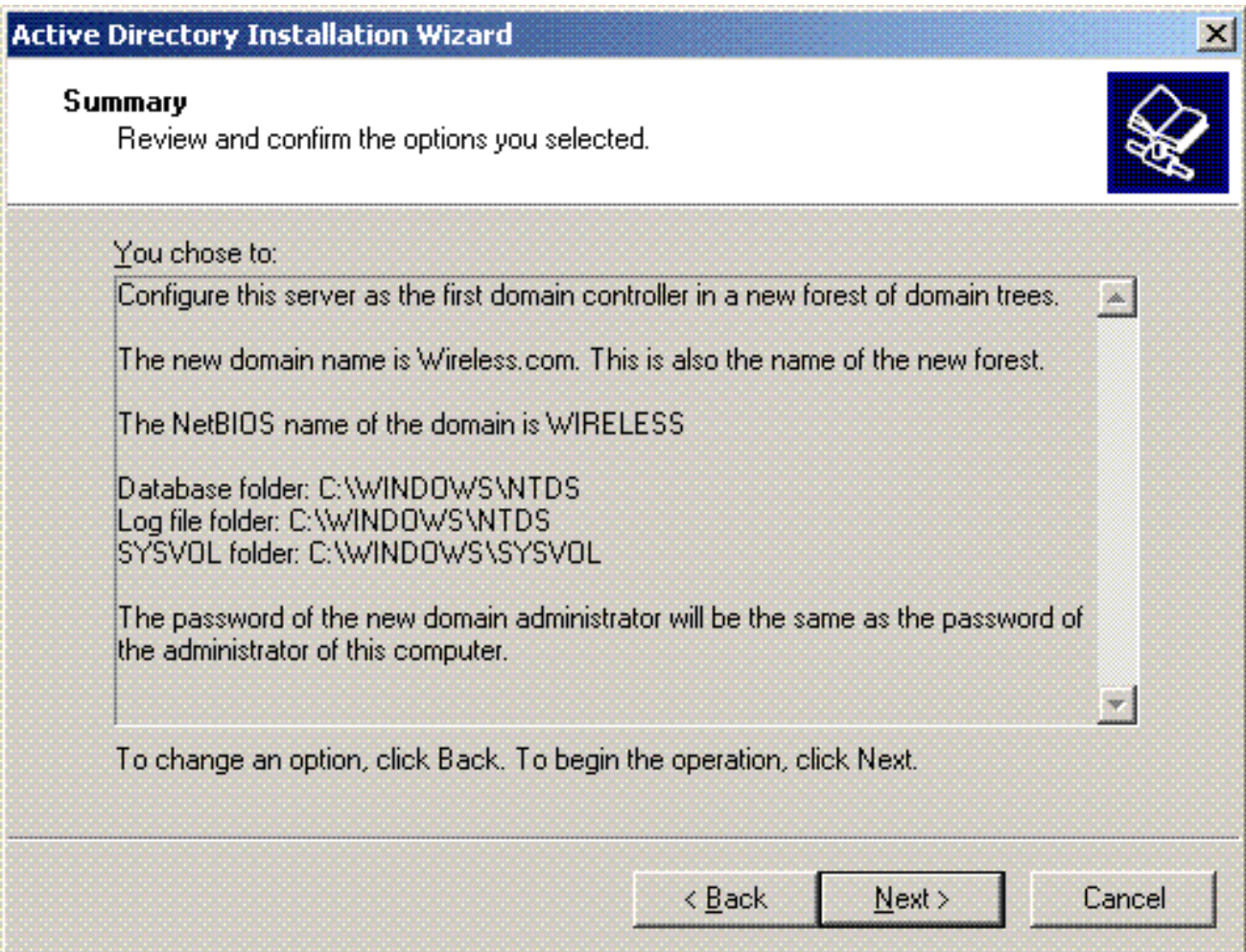
Restore Mode Password:

Confirm password:

For more information about Directory Services Restore Mode, see [Active Directory Help](#).

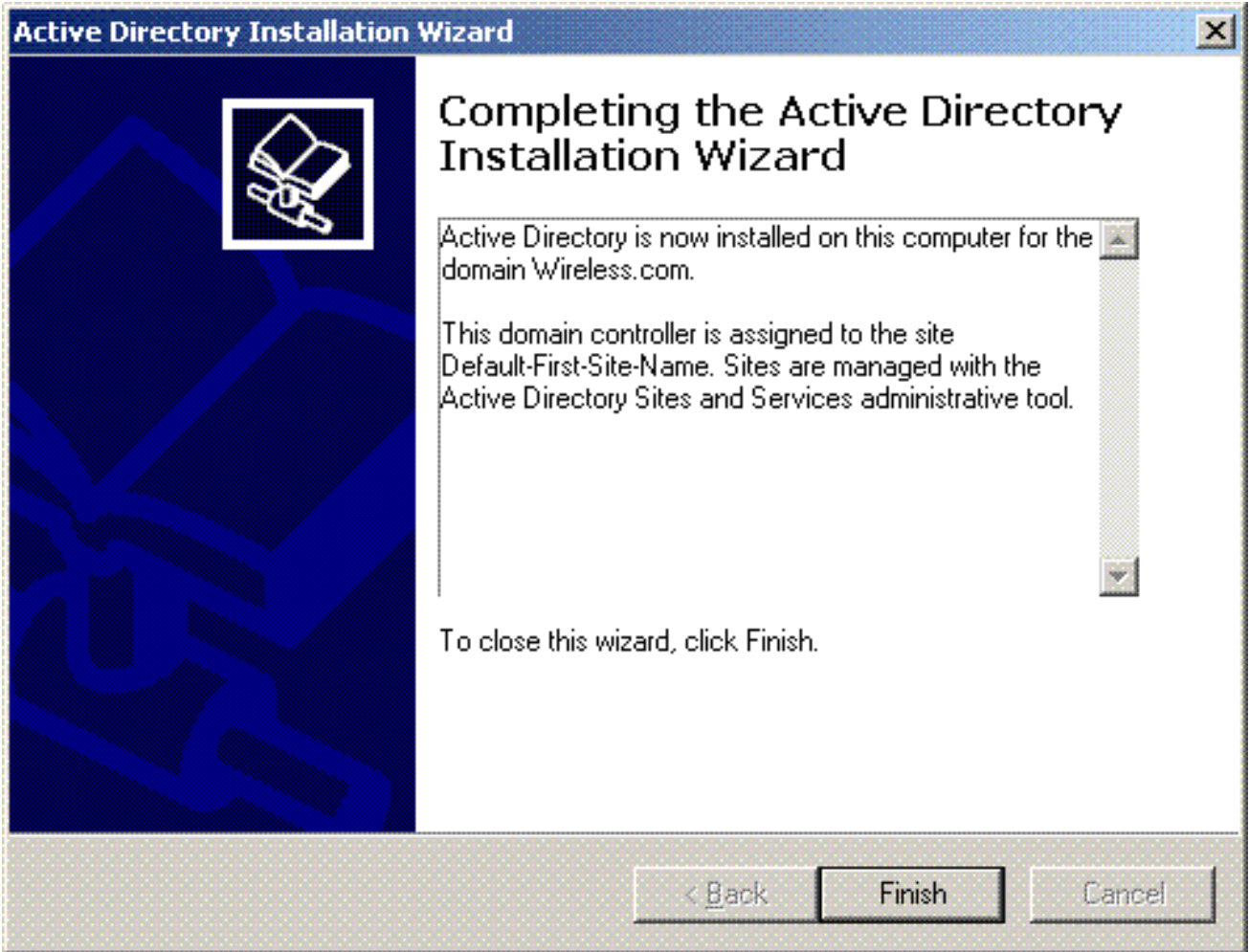
< Back   Next >   Cancel

12. انقر فوق التالي لقبول مجموعة خيارات المجال مسبقاً.

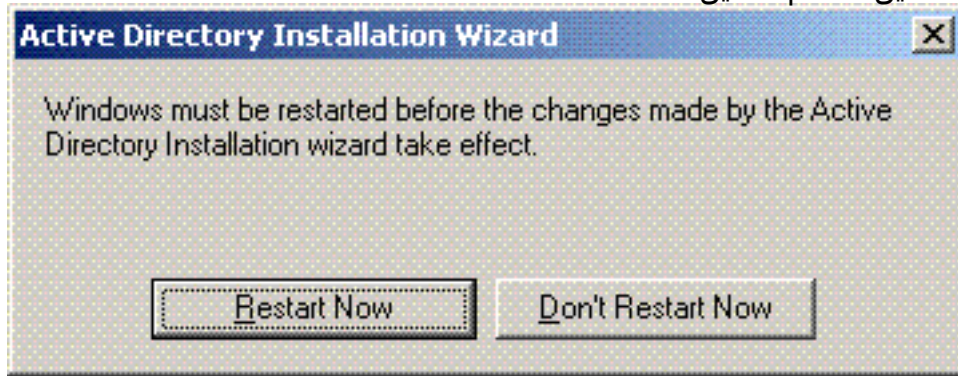


13. انقر فوق إنهاء" لإغلاق معالج تثبيت Active Directory.





14. قم بإعادة تشغيل الخادم لتفعيل



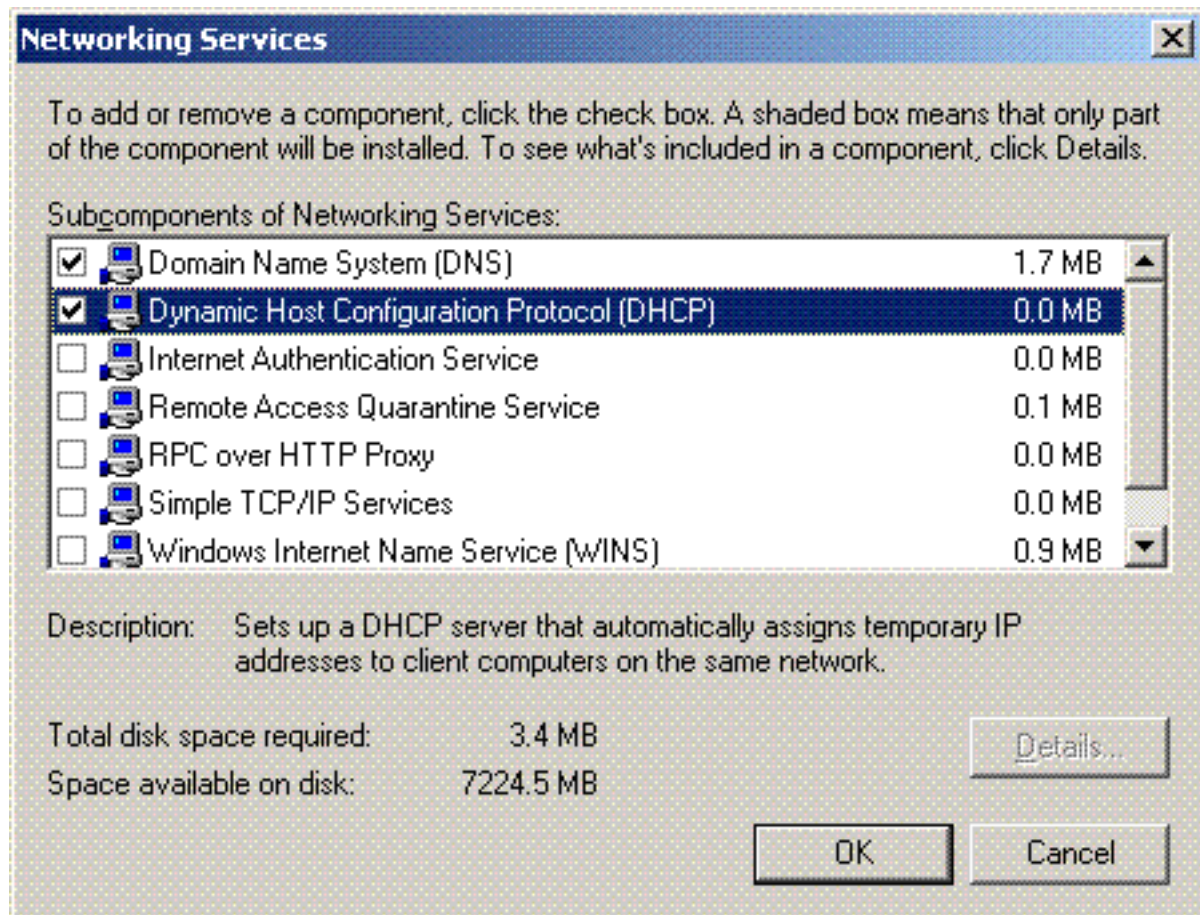
التغييرات.

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

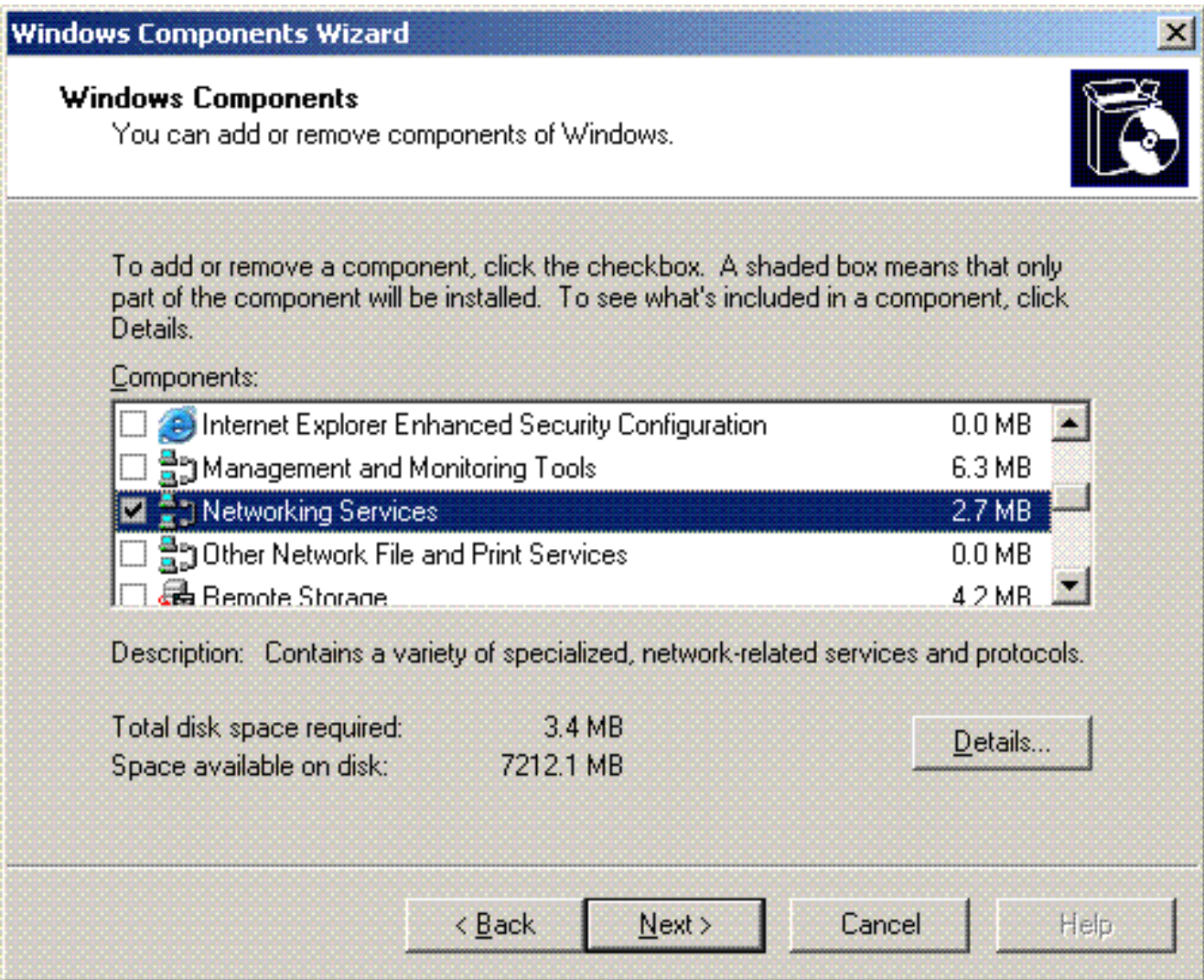
يتم استخدام خدمة DHCP على خادم Microsoft 2003 لتوفير عناوين IP للعملاء اللاسلكيين. أتمت in order to ركب وشكلت DHCP خدمة على هذا نادل، هذا steps:

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

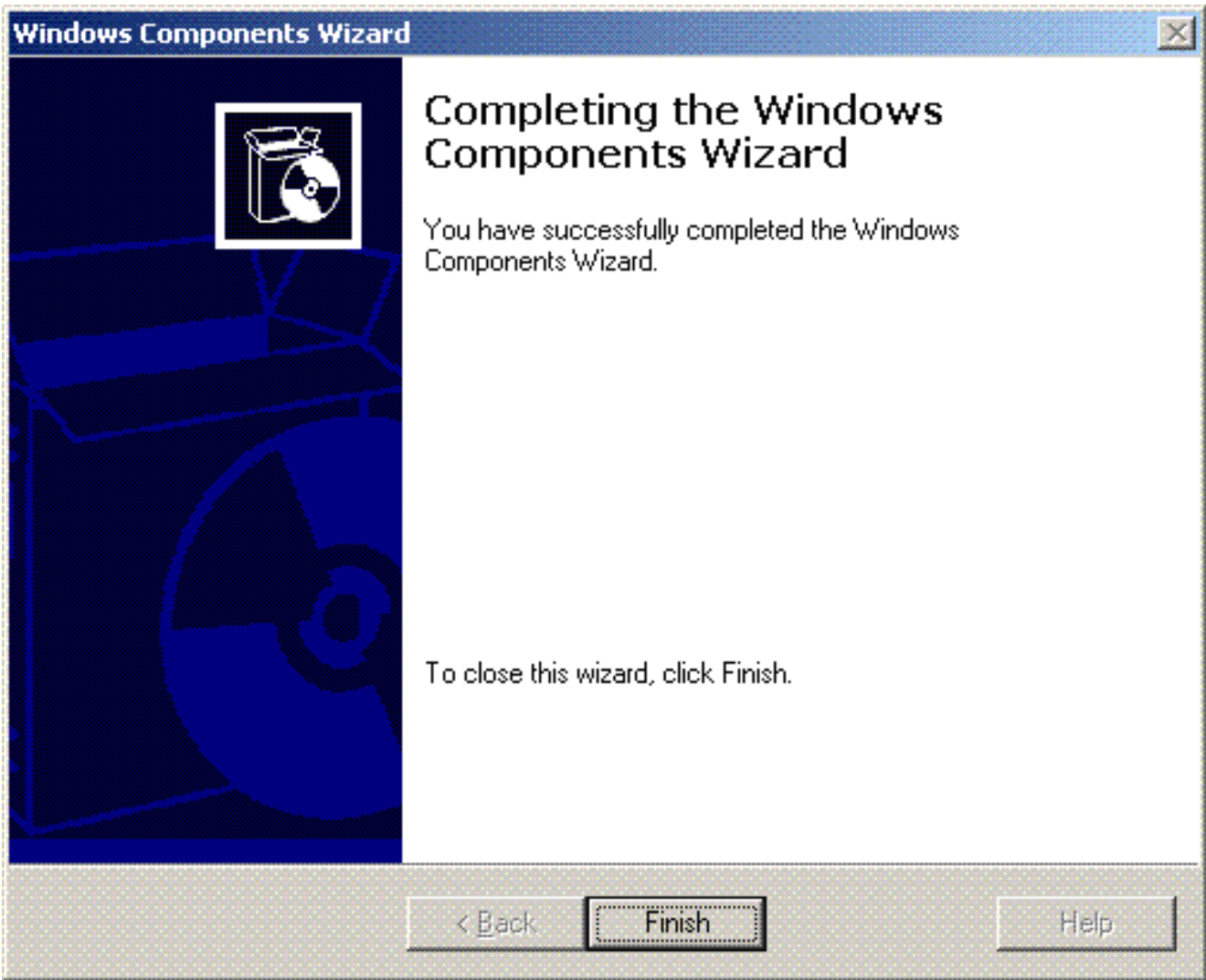


.ok

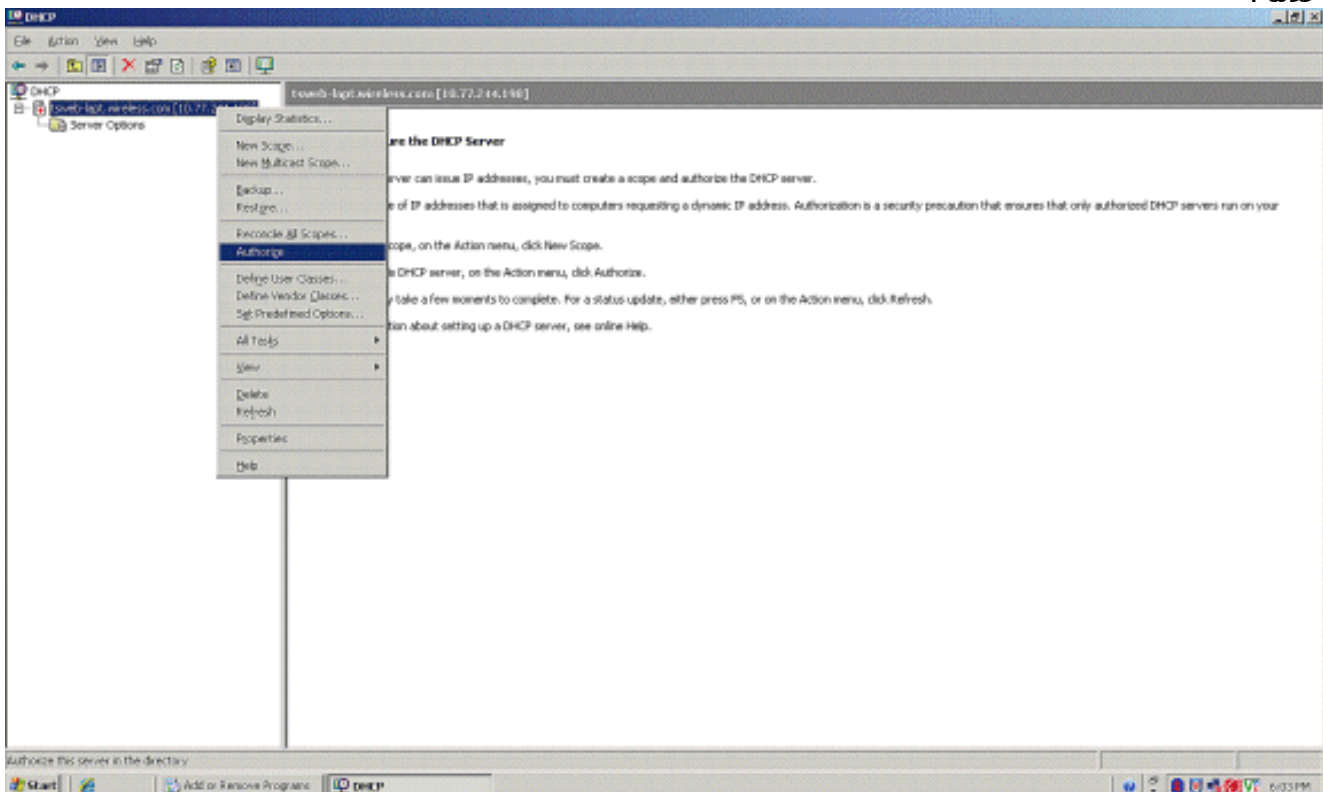
5. طقطقت بعد ذلك أن يركب ال DHCP خدمة.



6. انقر فوق إنهاء " لإكمال التثبيت.



7. طقطقت in order to شملت DHCP خدمة، بداية<برنامج>أداة إداري وطقطقت ال DHCP إضافي.
8. أخترت ال DHCP نادل - [tsweb-lapt.wireless.com](http://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).

## New Scope Wizard

### Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

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

## New Scope Wizard

### IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Enter the range of addresses that the scope distributes.

Start IP address: 10 . 77 . 244 . 218

End IP address: 10 . 77 . 244 . 219

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 8

Subnet mask: 255 . 0 . 0 . 0

< Back

Next >

Cancel

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

## New Scope Wizard

### Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Remove

< Back

Next >

Cancel

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



## New Scope Wizard

### Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:	Hours:	Minutes:
<input type="text" value="8"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

< Back

Next >

Cancel

16. أخترت على ال DHCP configure خيار، نعم، أنا أريد أن يشكّل DHCP خيار الآن، وطققة بعد ذلك.

## New Scope Wizard

### Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

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

## New Scope Wizard

### Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

Add

10.77.244.220

Remove

Up

Down

< Back

Next >

Cancel

18. في الصفحة اسم المجال وخواص DNS، اكتب اسم المجال الذي تم تكوينه مسبقاً. في المثال، استخدم Wireless.com. أدخل عنوان IP الخاص بالخادم. انقر فوق إضافة (Add).

## New Scope Wizard

### Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

Add

Resolve

10.77.244.217

Remove

Up

Down

< Back

Next >

Cancel

19. انقر فوق **Next** (التالي).

20. في صفحة خادم WINS، انقر فوق التالي.

21. في صفحة "تنشيط النطاق"، اختر نعم، أريد تنشيط النطاق الآن، وانقر فوق التالي.

## New Scope Wizard

### Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

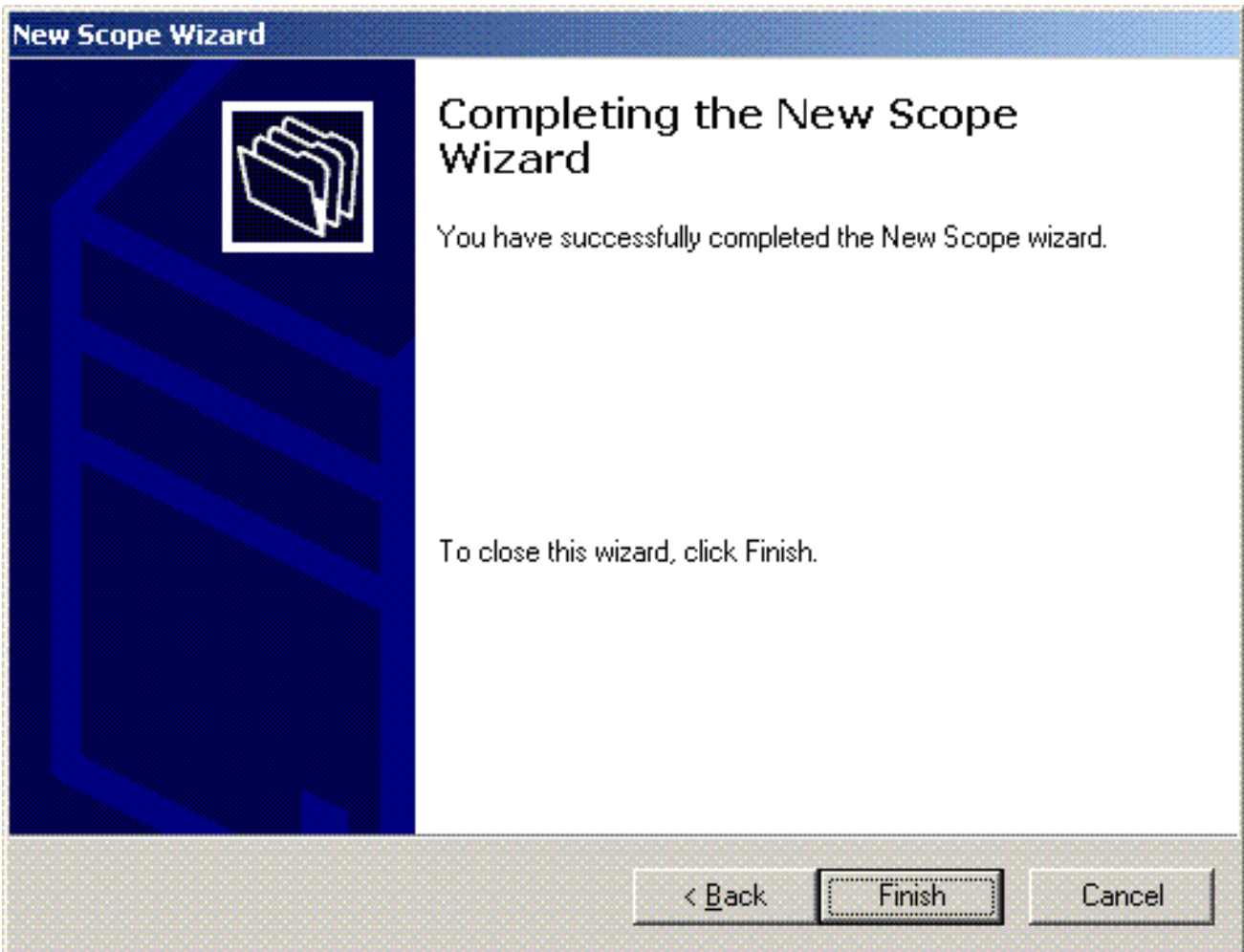
- Yes, I want to activate this scope now
- No, I will activate this scope later

< Back

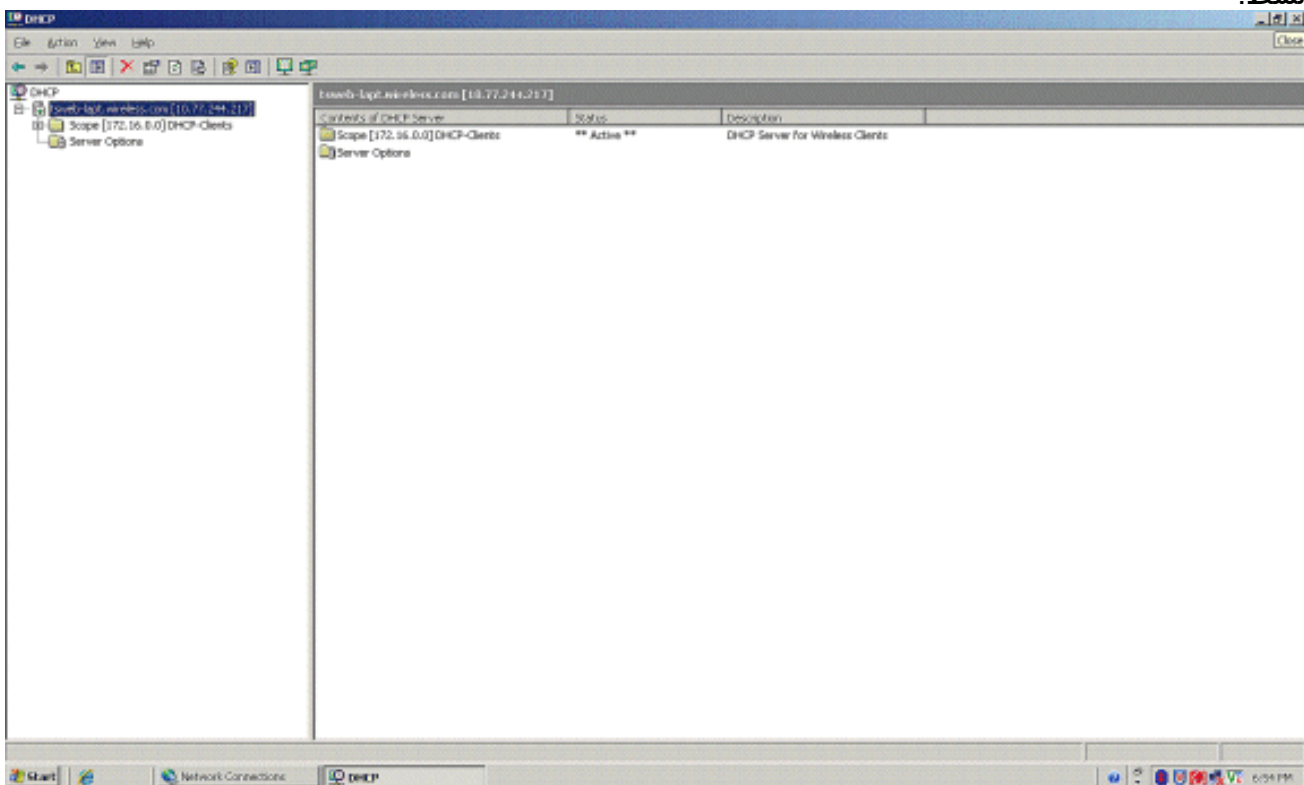
Next >

Cancel

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



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



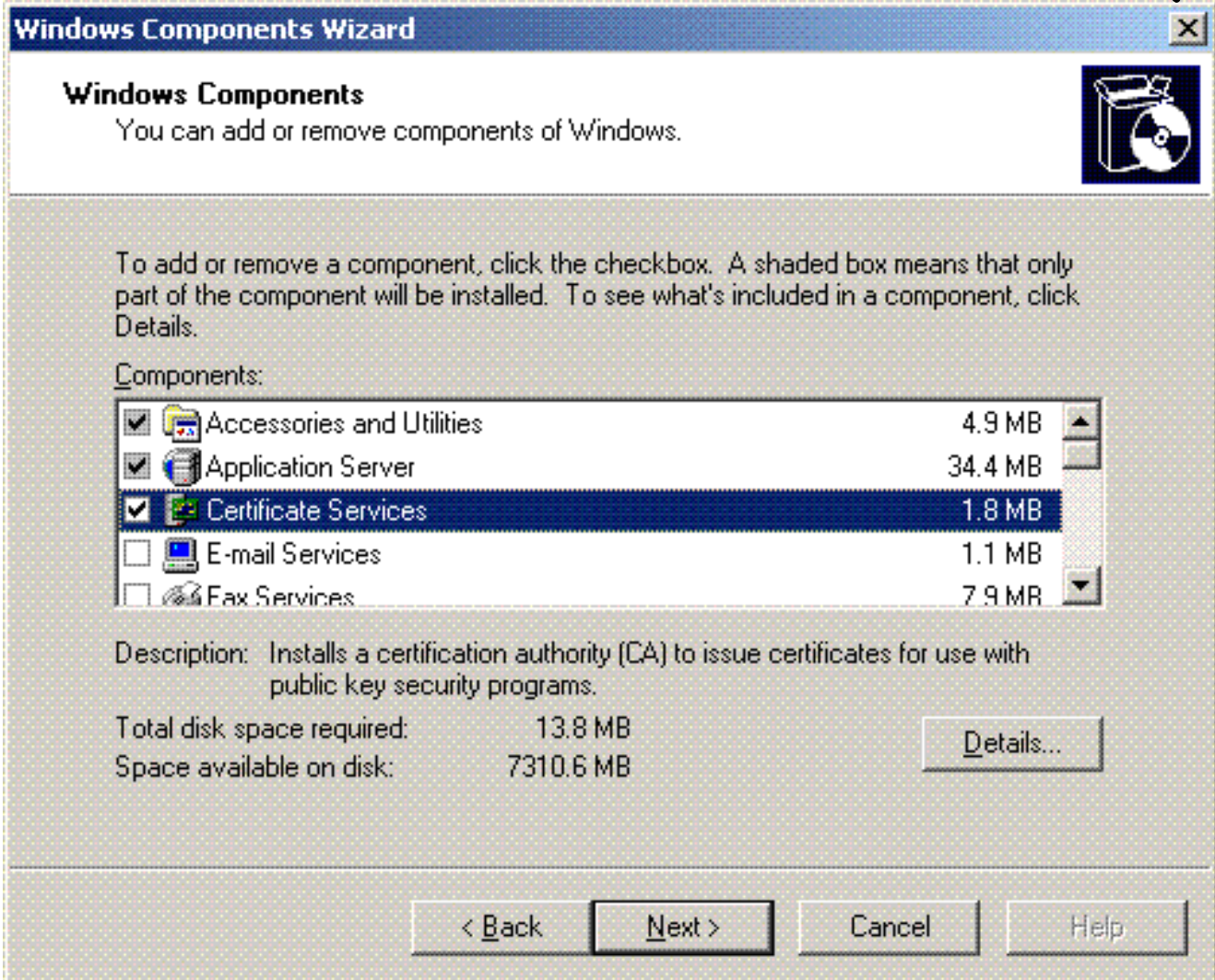
الآن بعد تمكين DHCP/ DNS على الخادم، قم بتكوين الخادم كخادم مرجع مصدق للمؤسسة (CA).

[تثبيت خادم Microsoft Windows 2003 وتكوينه كخادم مرجع شهادات \(CA\)](#)

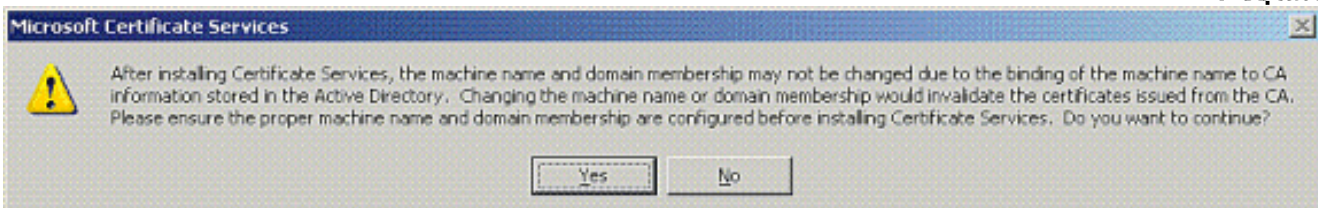
يقوم PEAP مع EAP-MS-CHAPv2 بالتحقق من خادم RADIUS بناء على الشهادة الموجودة على الخادم. بالإضافة إلى ذلك، يجب إصدار شهادة الخادم من قبل مرجع مصدق عام (CA) موثوق به من قبل كمبيوتر العميل (أي أن شهادة المرجع المصدق العام موجودة بالفعل في مجلد مرجع التصديق الجذر الموثوق به الموجود في مخزن شهادات الكمبيوتر 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:

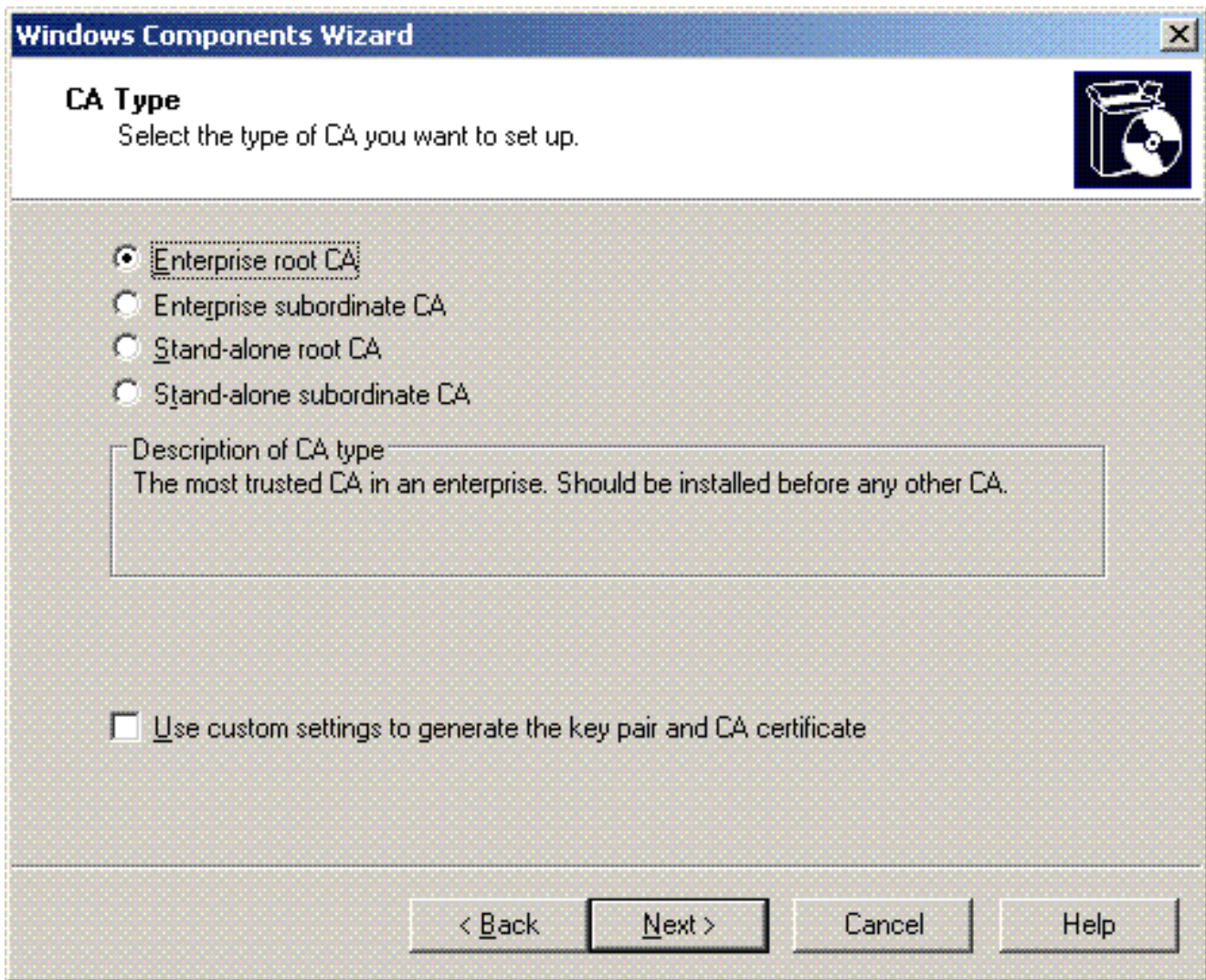
1. انقر فوق إضافة أو إزالة برامج في لوحة التحكم.
2. انقر فوق إضافة/إزالة مكونات Windows.
3. انقر على خدمات الشهادات.



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، أختار المرجع المصدق الجذر للمؤسسة، وانقر بعد ذلك.




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



**Windows Components Wizard** [X]

### CA Identifying Information

Enter information to identify this CA.



Common name for this CA:  
Wireless-CA

Distinguished name suffix:  
DC=Wireless,DC=com

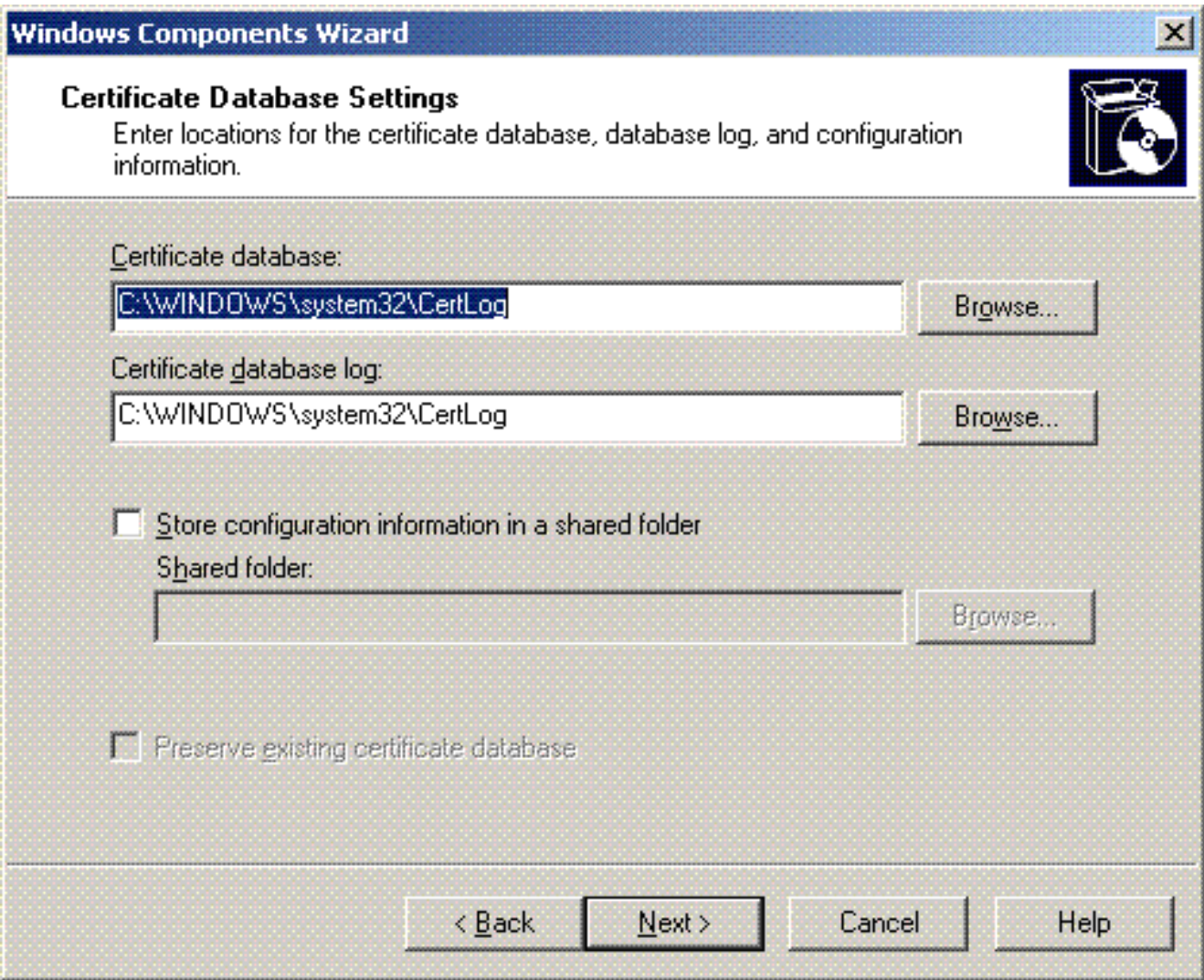
Preview of distinguished name:  
CN=Wireless-CA,DC=Wireless,DC=com

Validity period: 5 Years

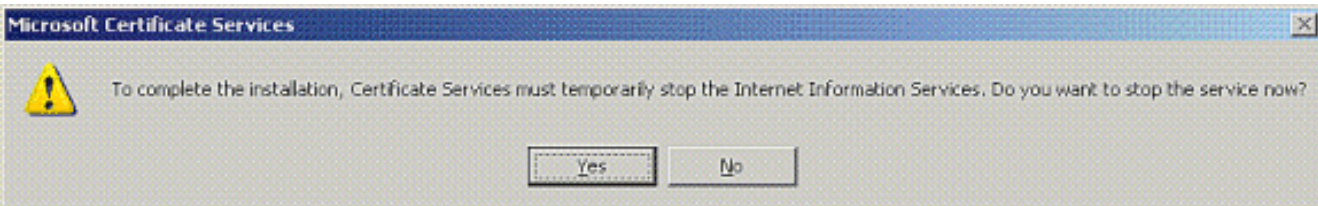
Expiration date: 12/12/2012 7:01 PM

< Back   Next >   Cancel   Help

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 تلقائياً بعد تثبيت .CA.



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

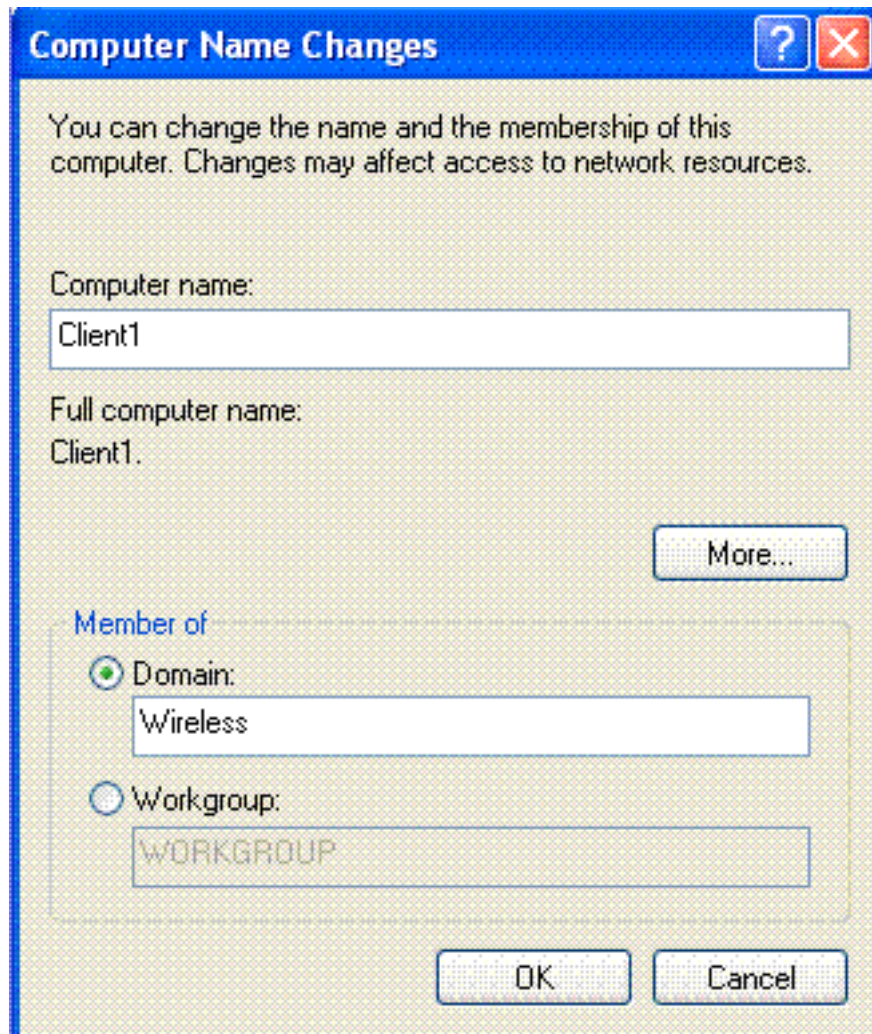


تمثل الخطوة التالية في تثبيت خدمة مصادقة الإنترنت وتكوينها على خادم Microsoft Windows 2003.

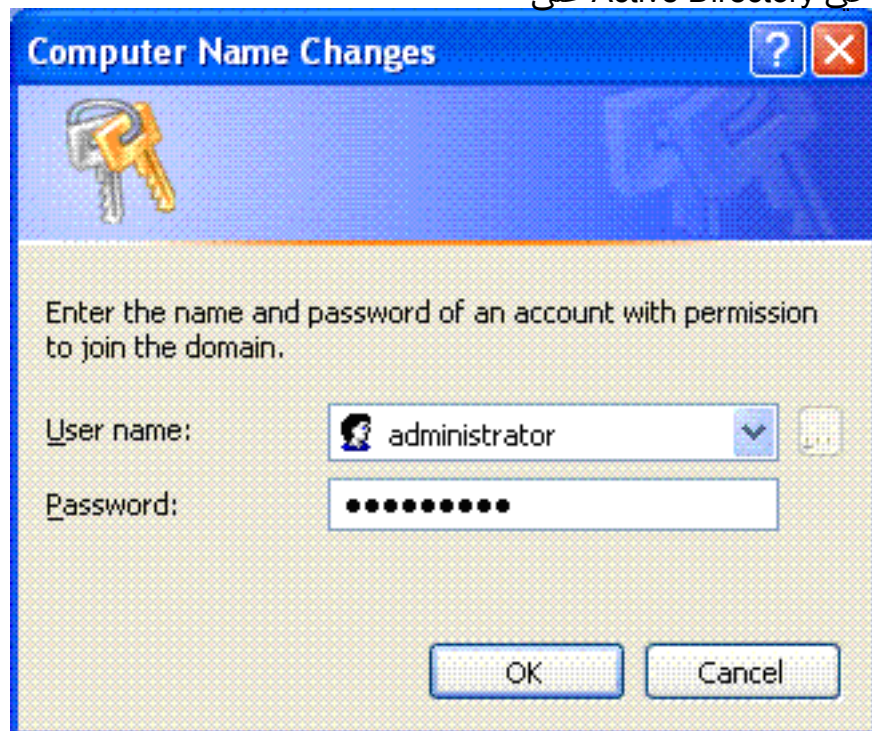
### توصيل العملاء بالمجال

تمثل 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. طغطة تغيير.
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.)



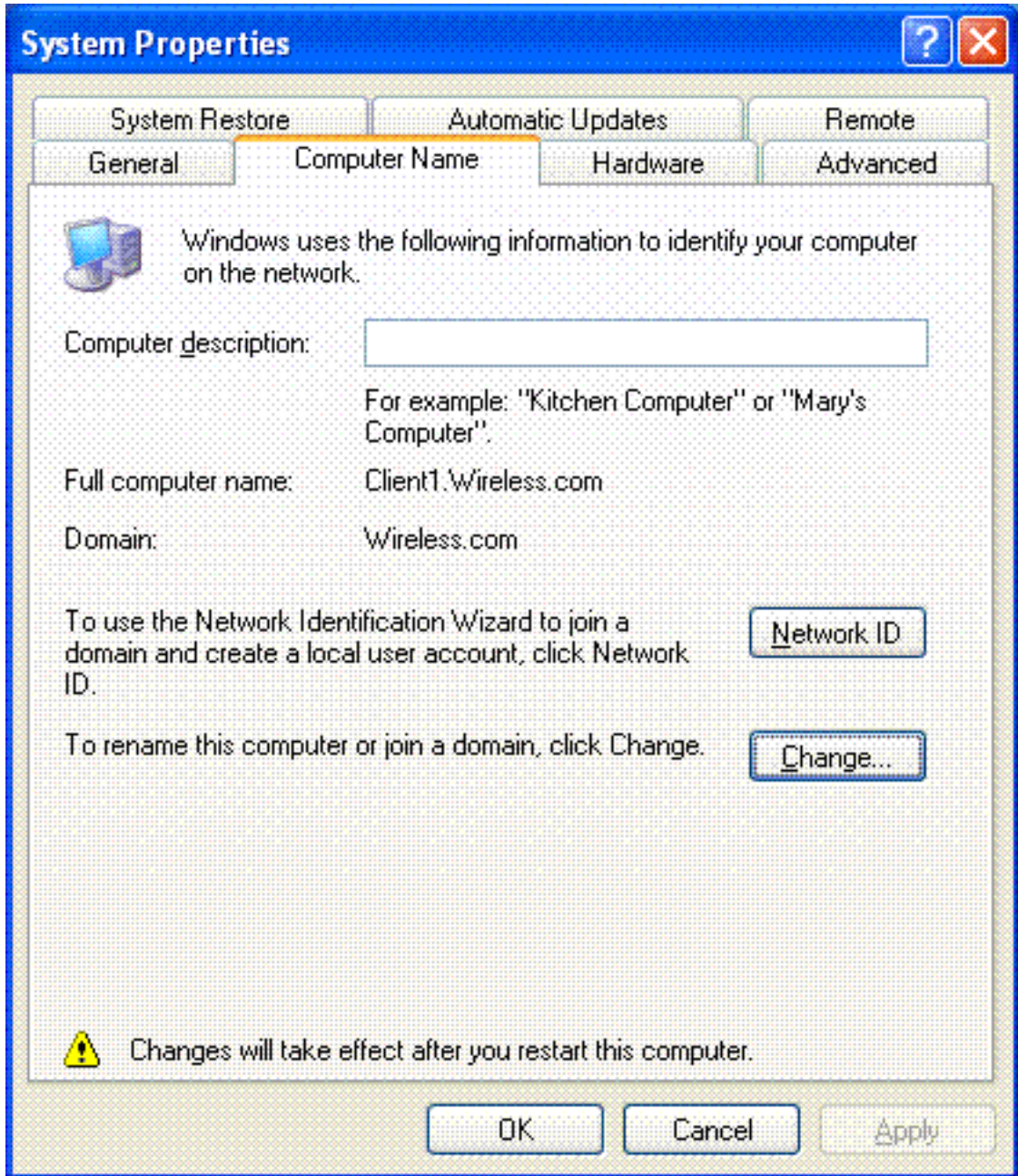
10. انقر فوق OK.

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.

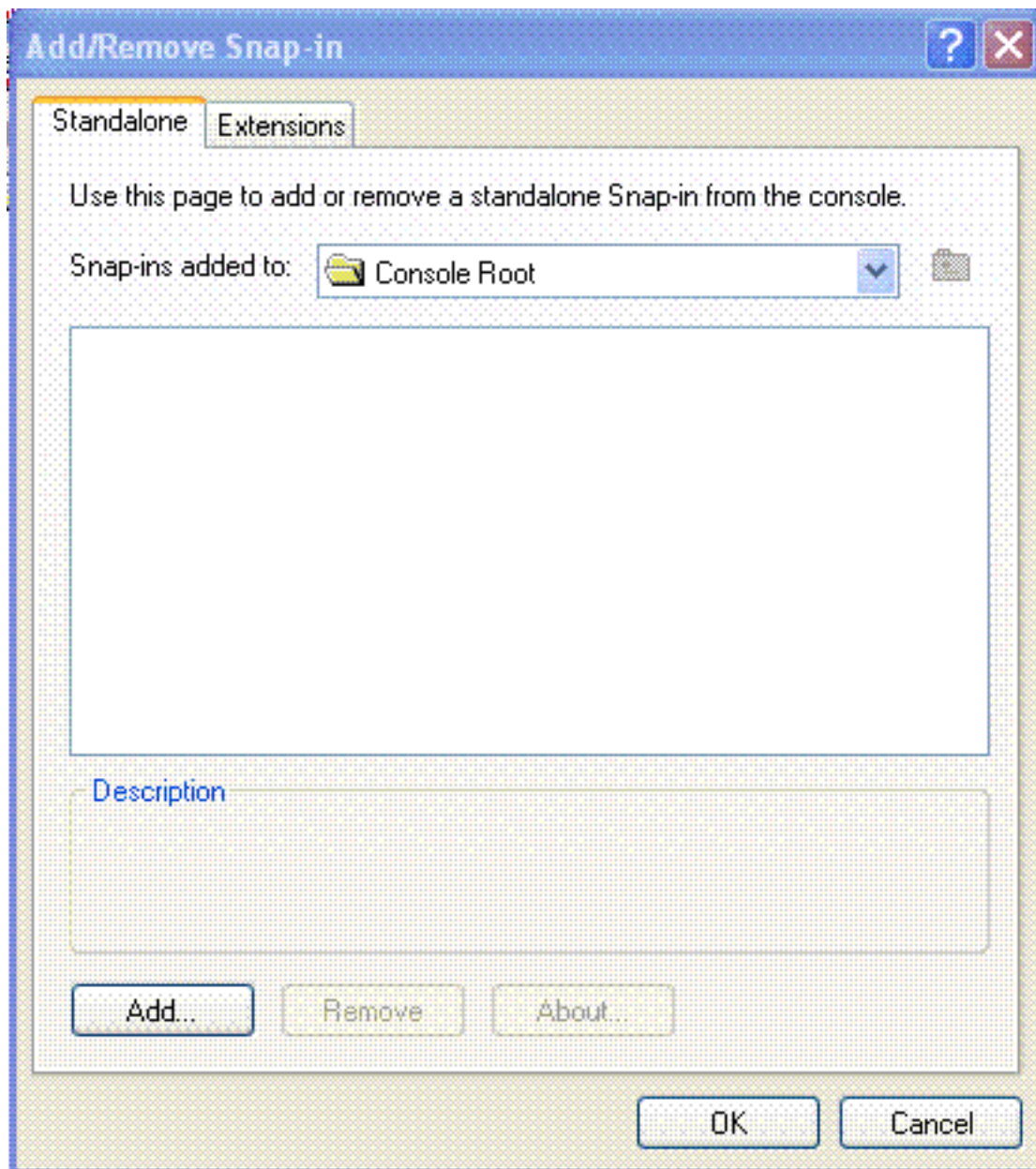
14. انقر فوق علامة التبويب اسم الكمبيوتر للتحقق من أنك في المجال Wireless.com.



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.

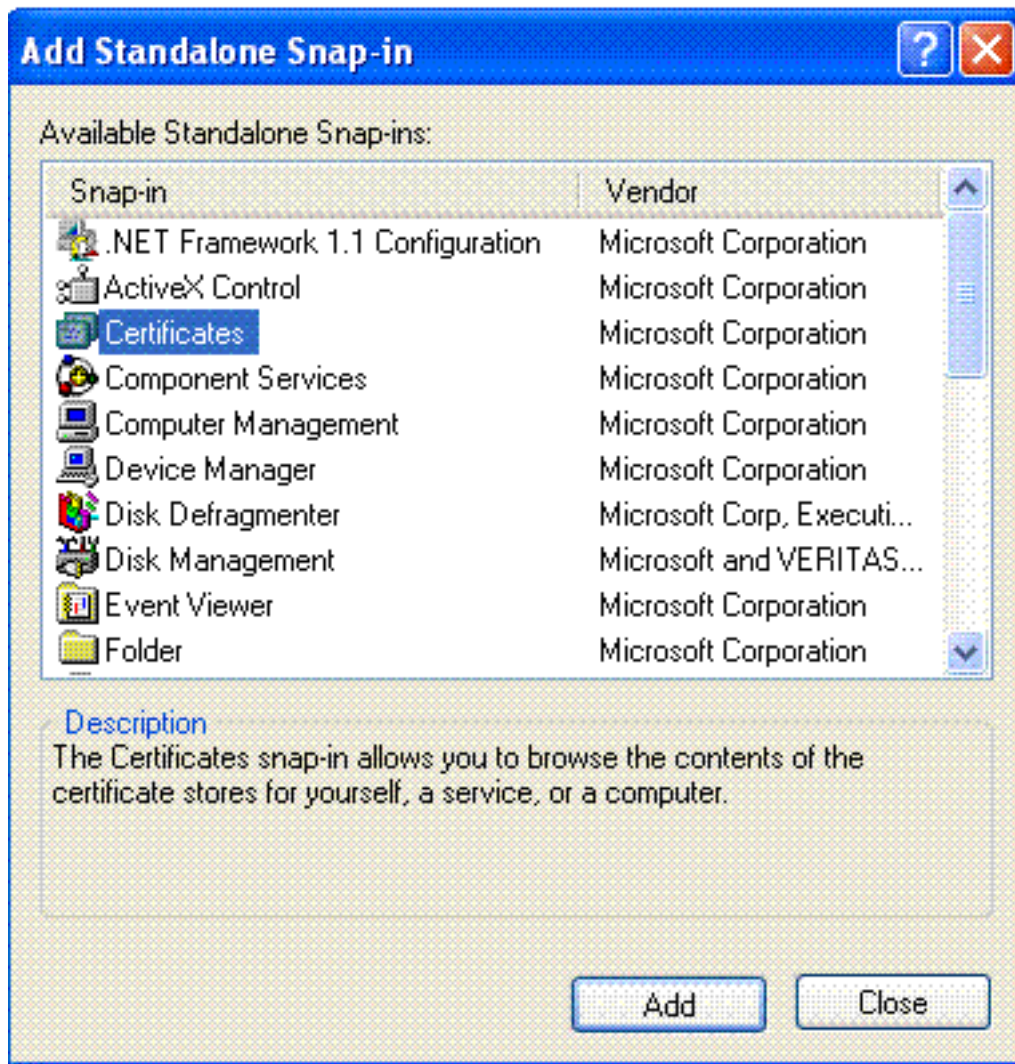
17. انقر ملف، وانقر إضافة/إزالة الأداة



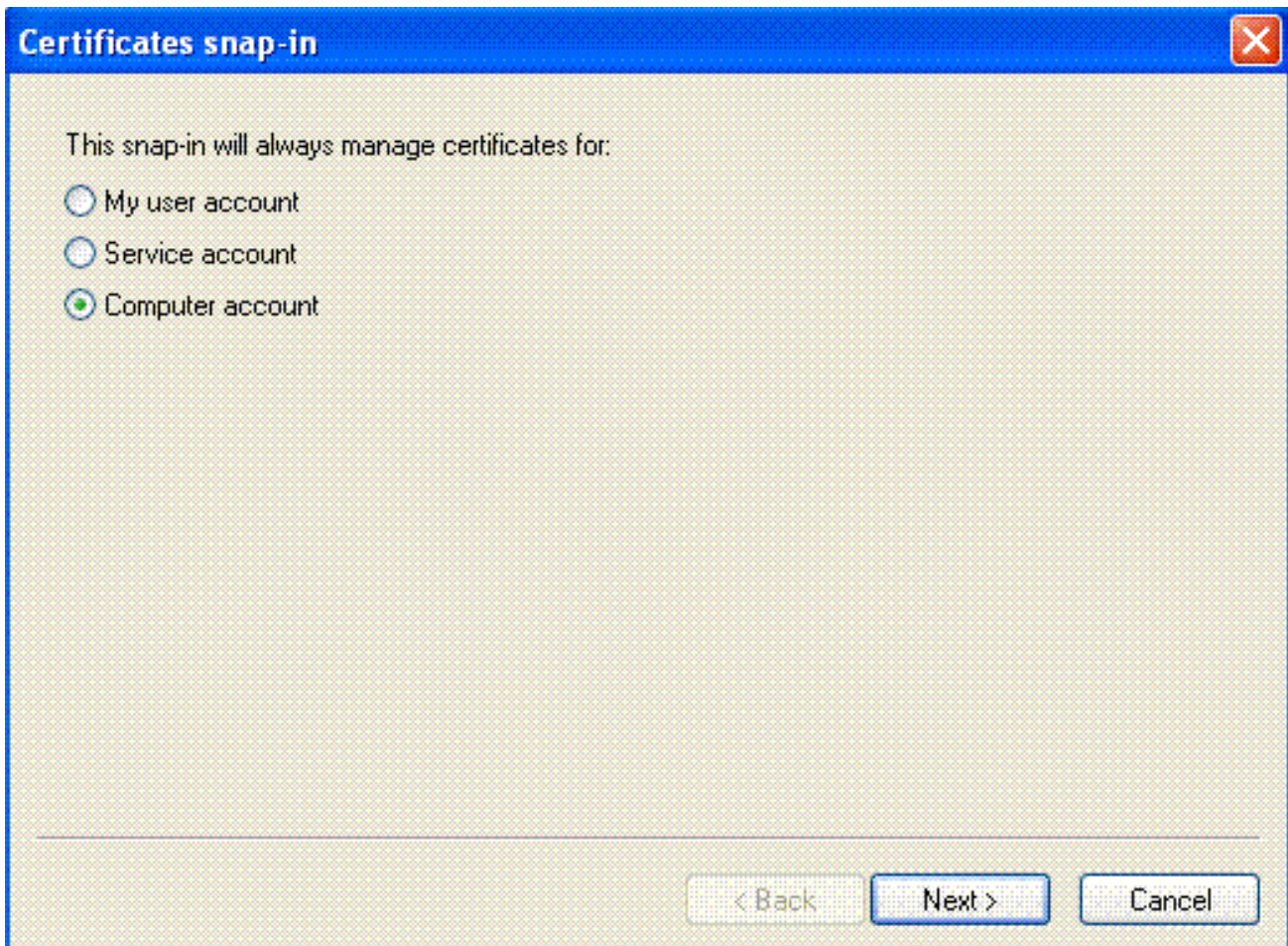
الإضافة.

18. انقر فوق إضافة (Add).

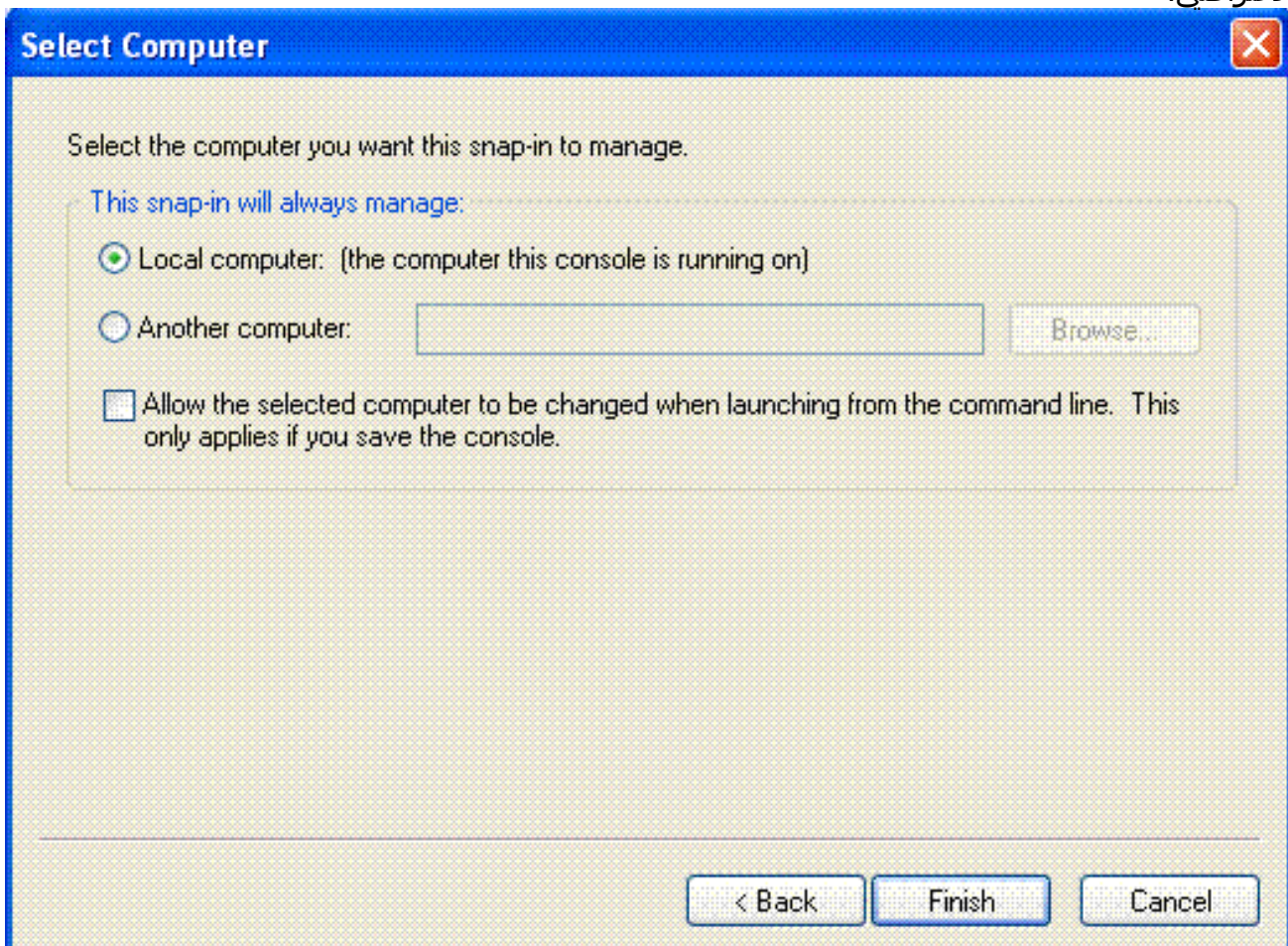
19. أختار ترخيص، وانقر



إضافة.  
20. أختار حساب الكمبيوتر، وانقر فوق  
التالي.



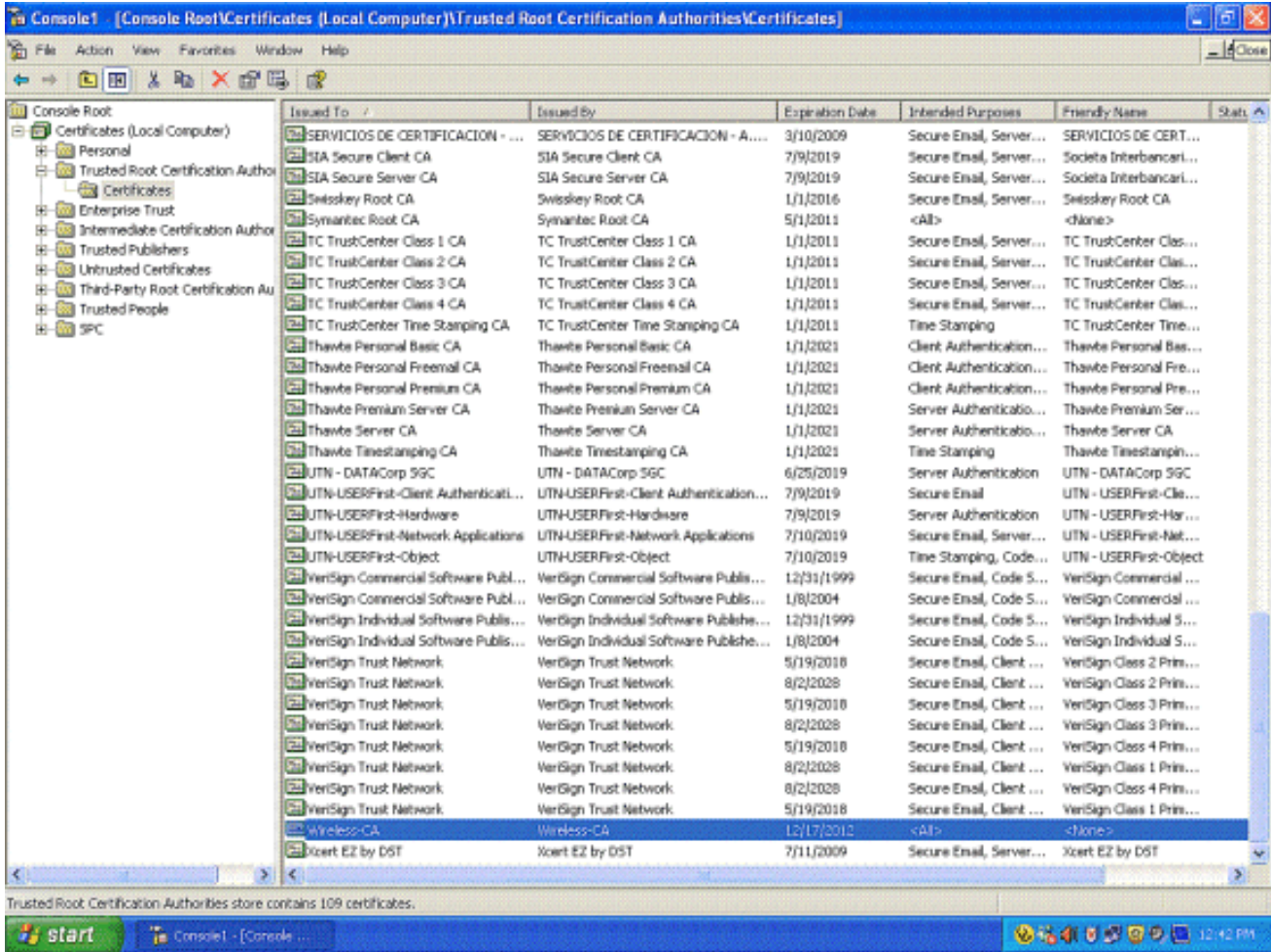
21. انقر فوق إنهاء لقبول الكمبيوتر المحلي الافتراضي.



22. طغطة ختام، وطغطة ok.



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



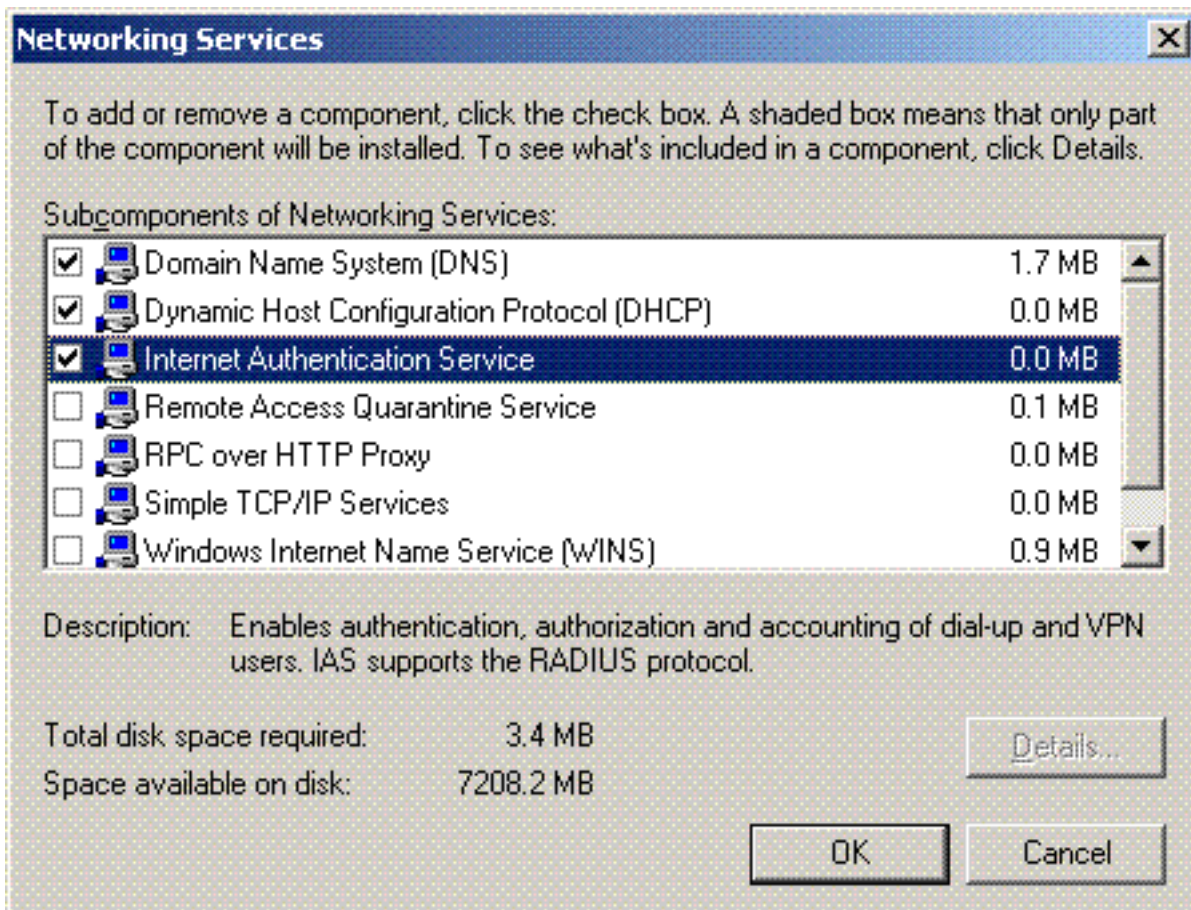
24. كرر هذا الإجراء لإضافة المزيد من العملاء إلى المجال.

## 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. اختر خدمات الشبكة، وانقر فوق تفاصيل.
4. اختر خدمة مصادقة الإنترنت، وانقر موافق، وانقر

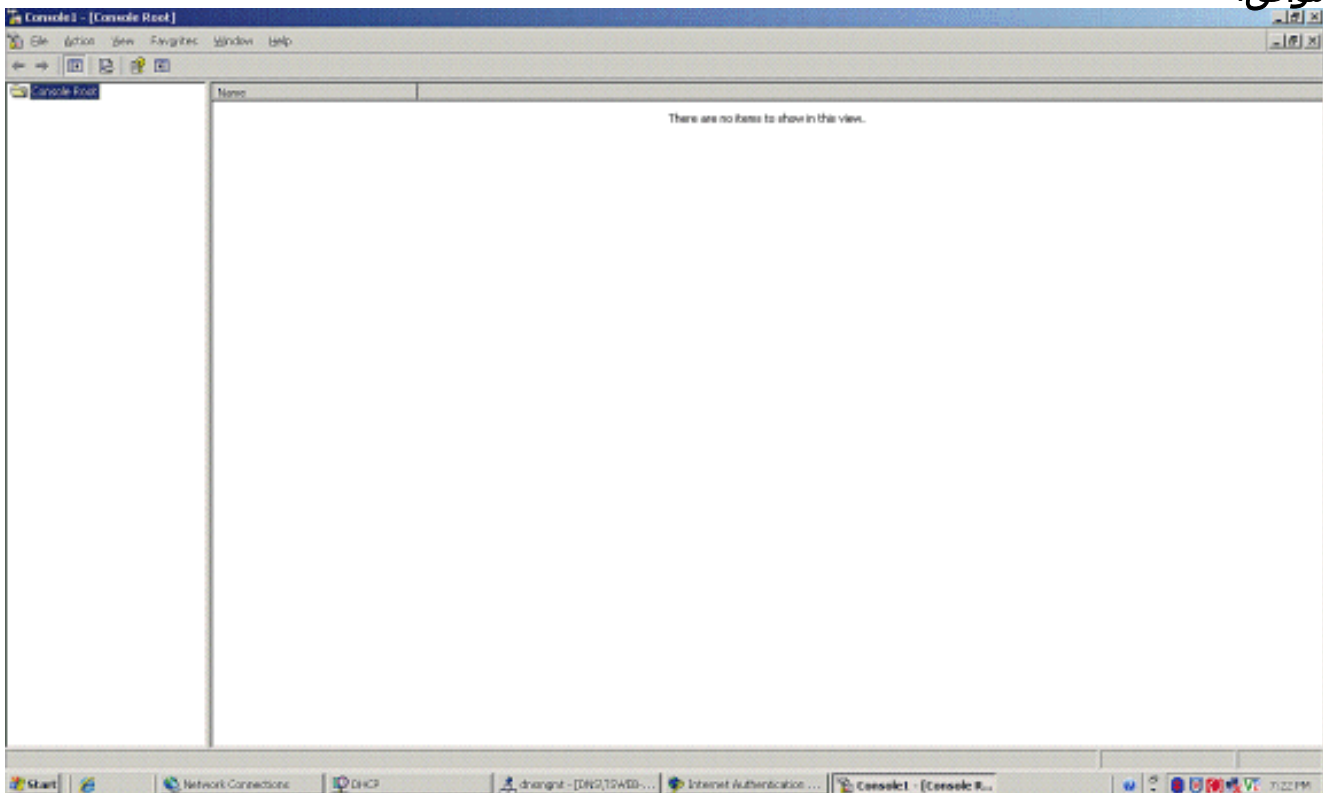


التالي.  
5. انقر فوق إنهاء" لإكمال تثبيت  
.IAS



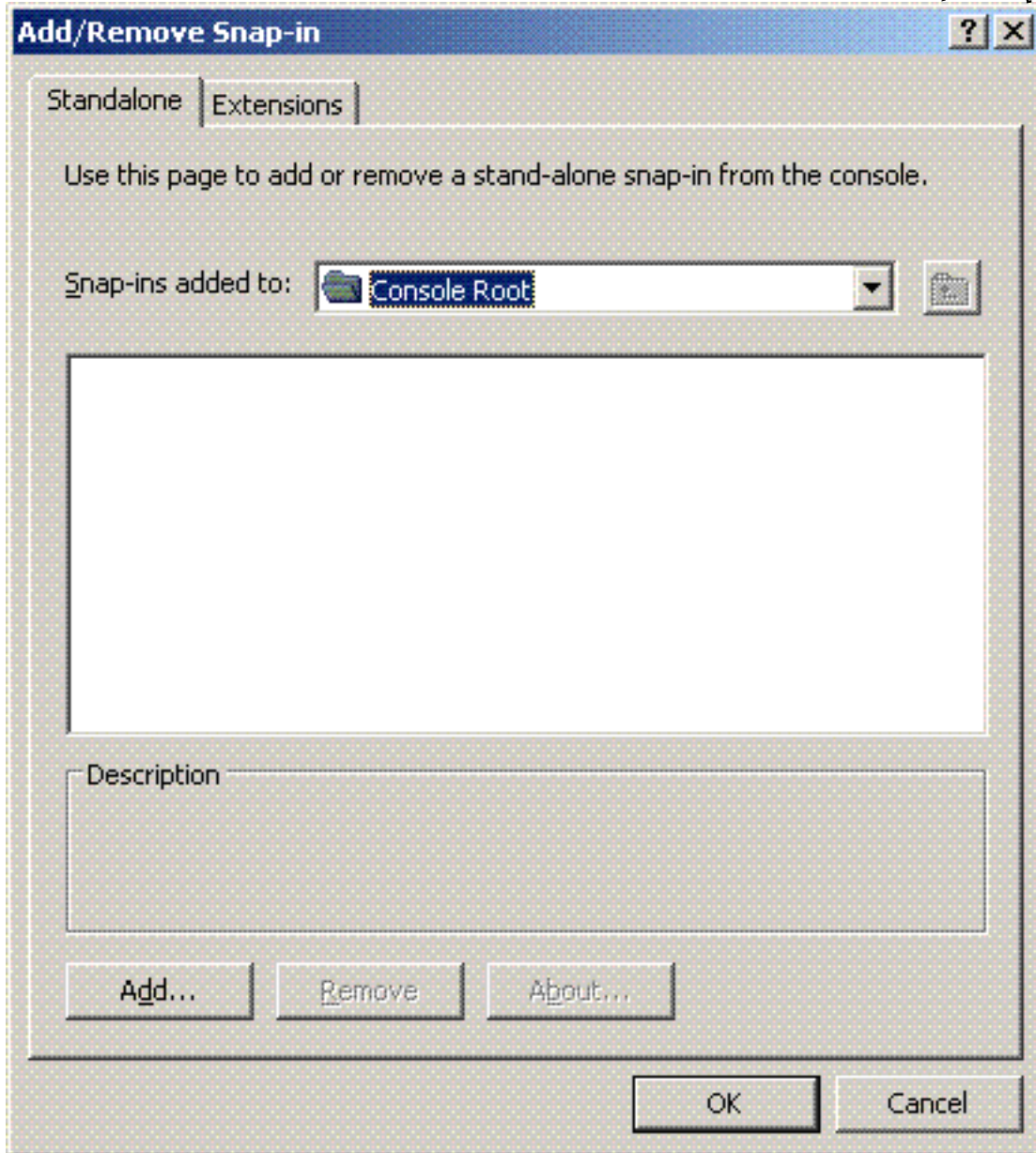
6. تمثل الخطوة التالية في تثبيت شهادة الكمبيوتر لخدمة مصادقة الإنترنت (IAS).  
7. انقر فوق بدء؛ وانقر فوق تشغيل؛ واكتب mmc؛ وانقر فوق

موافق.



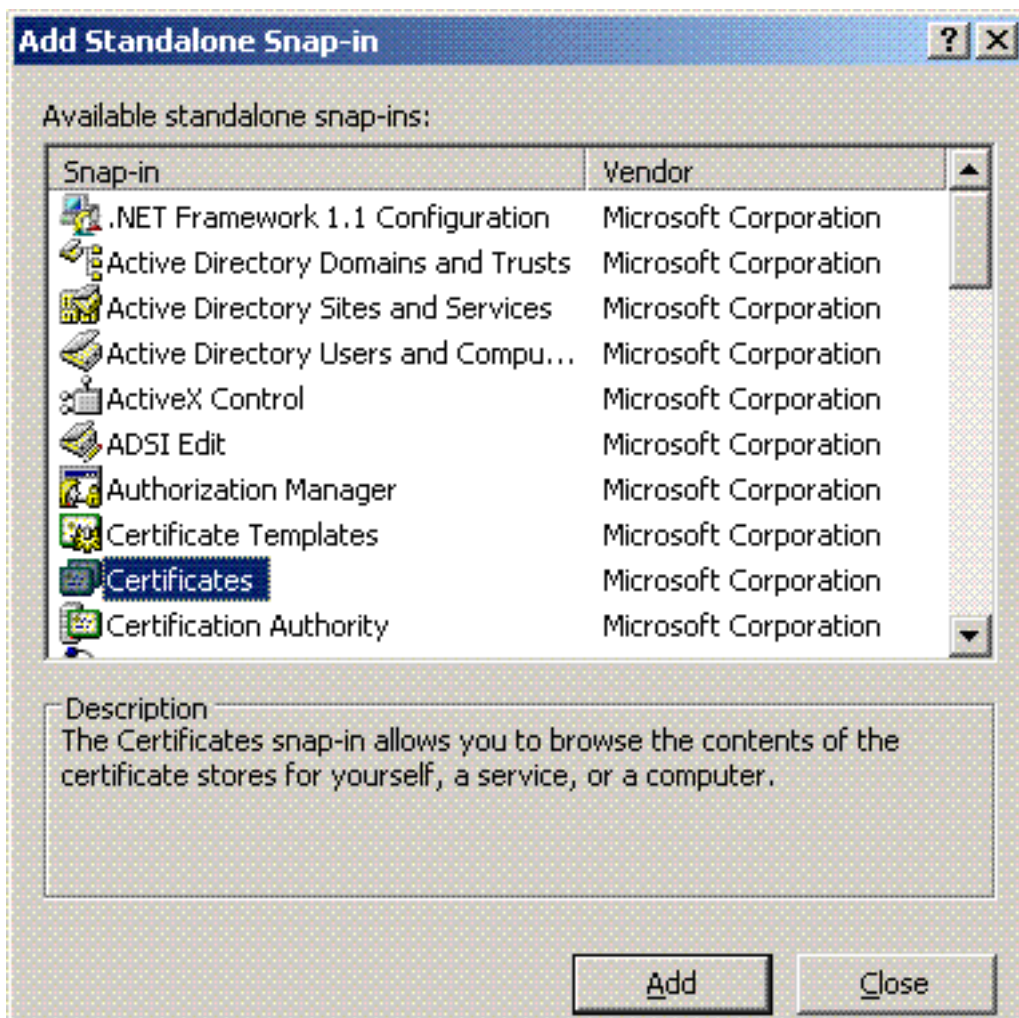
8. انقر فوق وحدة التحكم في قائمة الملف، ثم أختار إضافة/إزالة الأداة الإضافية.

9. انقر فوق إضافة لإضافة أداة

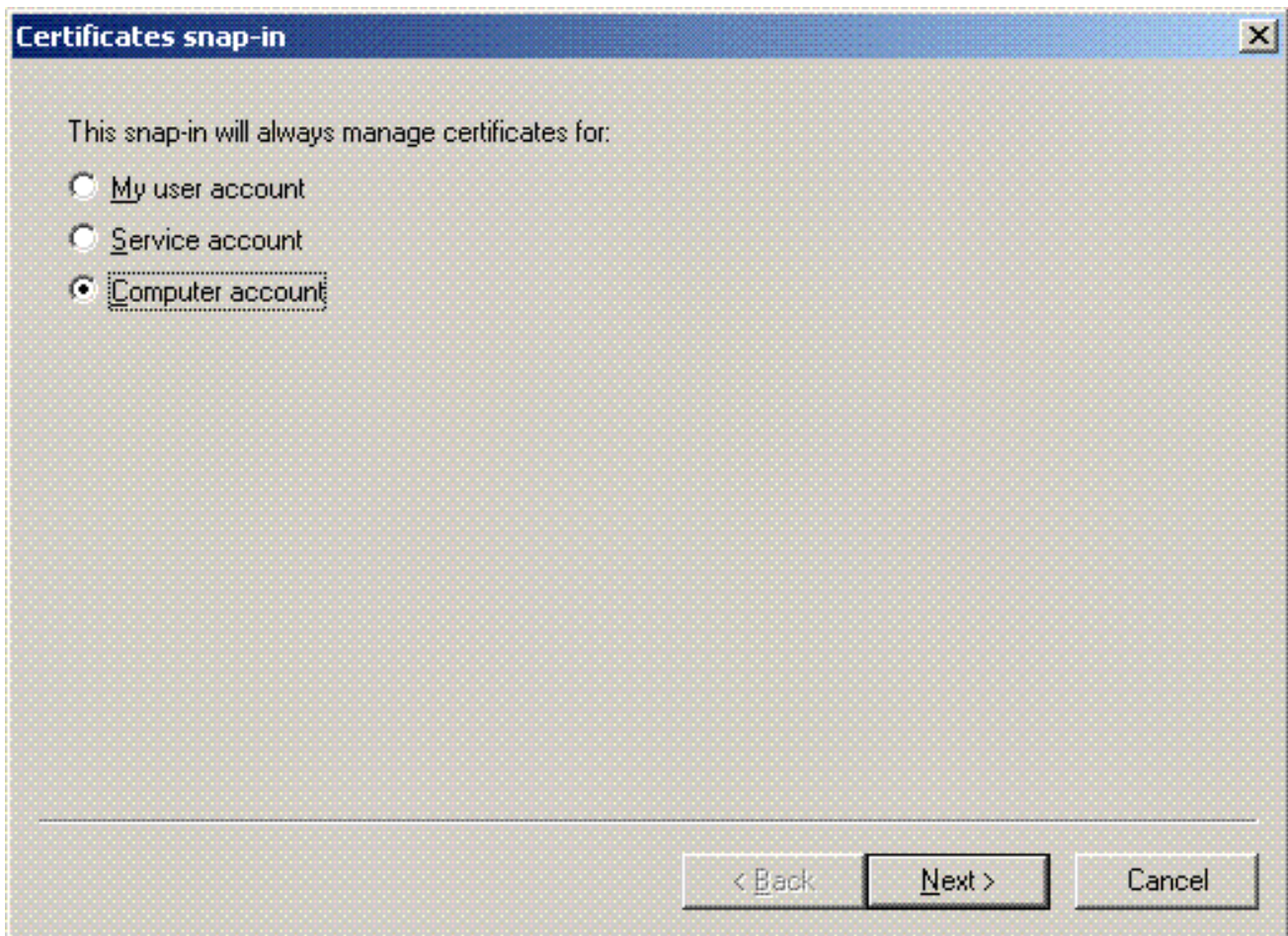


إضافة.

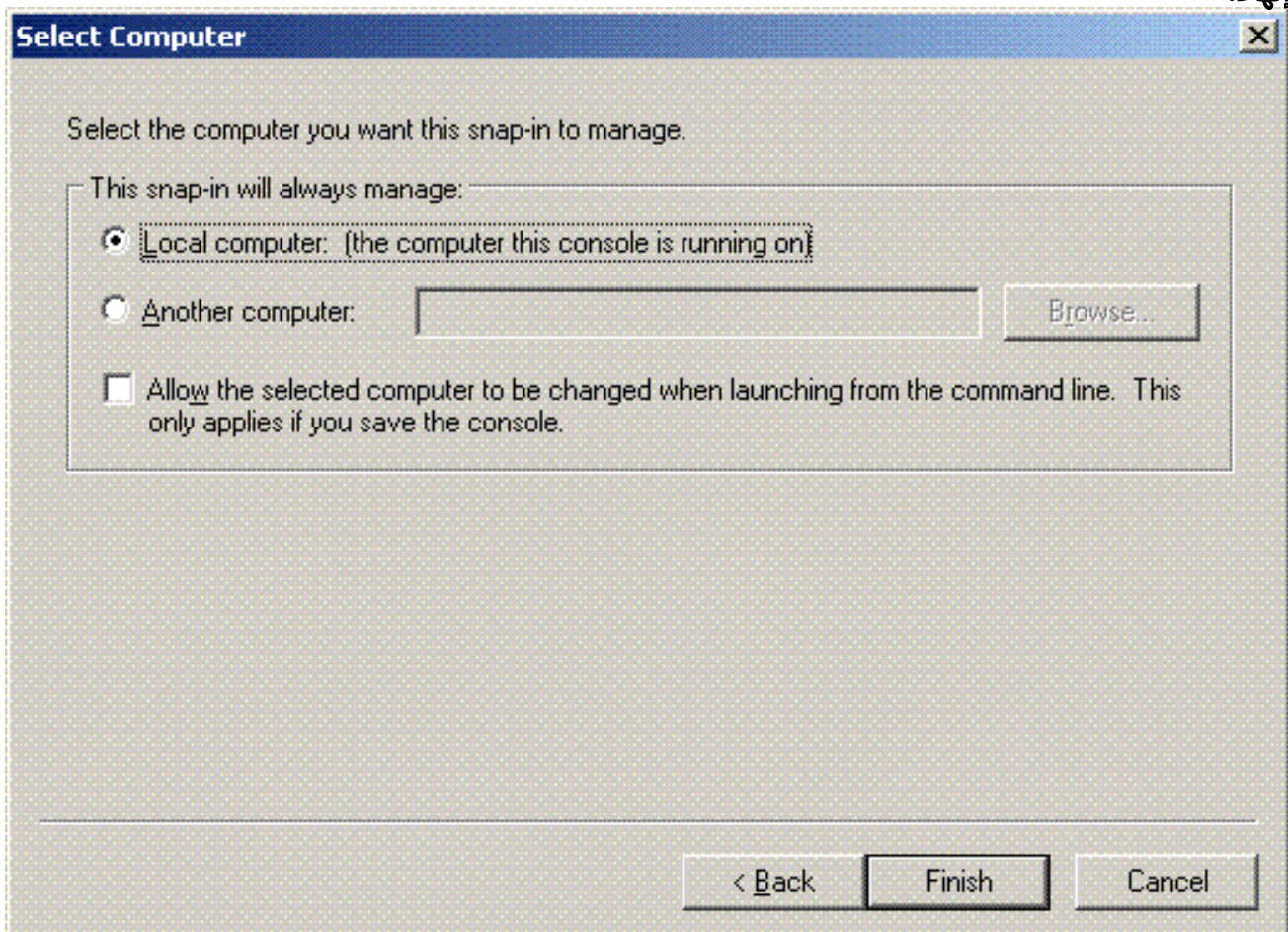
10. أختَر شهادات من قائمة الأدوات الإضافية، وانقر



إضافة.  
11. أخترت حاسوب حساب، وطققة بعد ذلك.

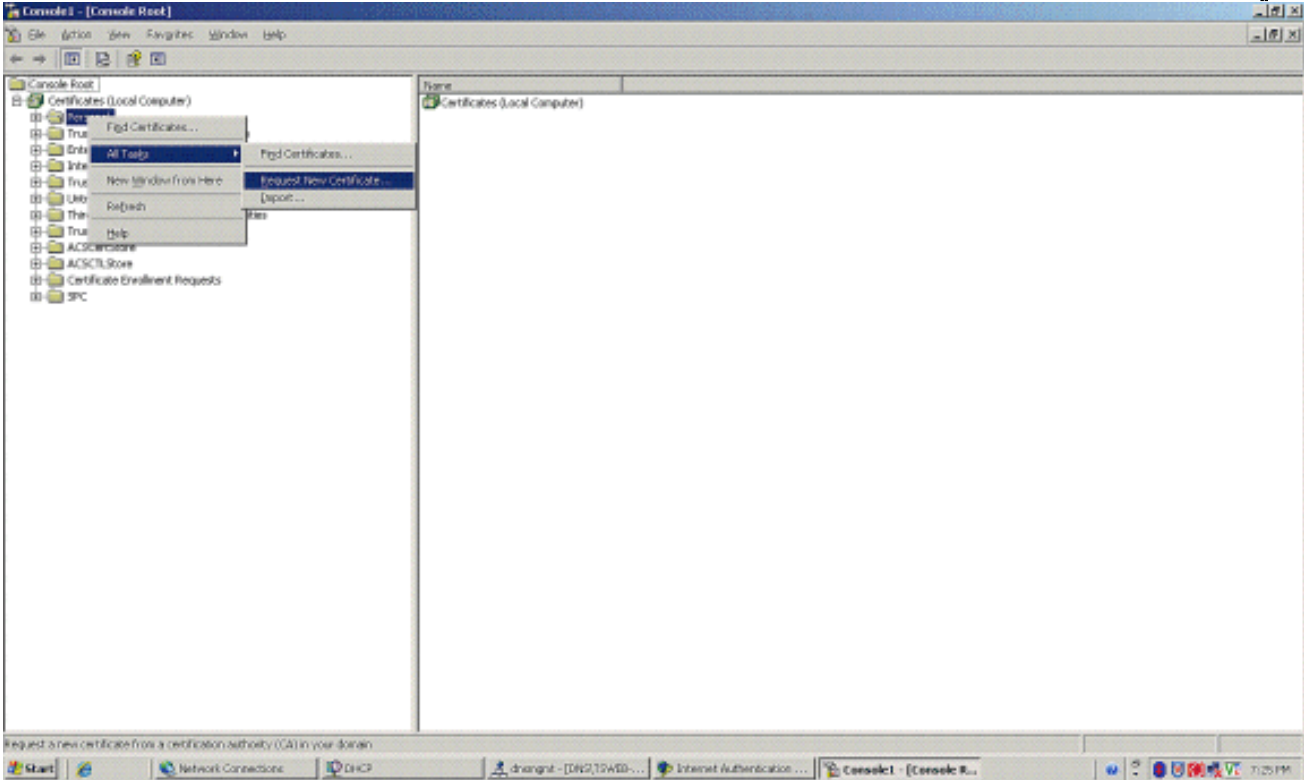


12. أختار كمبيوتر محلي، وانقر  
إنهاء.



13. طقطقة ختام، وطققة 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. أختار قالب شهادة وحدة التحكم بالمجال (إذا طلبت شهادة كمبيوتر على خادم غير وحدة التحكم بالمجال، أختار

قالب شهادة كمبيوتر، وانقر فوق  
التالي.

**Certificate Request Wizard**

**Certificate Types**

A certificate type contains preset properties for certificates.

---

Select a certificate type for your request. You can access only certificate types that you have permissions for and that are available from a trusted CA.

Certificate types:

- Directory Email Replication
- Domain Controller**
- Domain Controller Authentication

To select a cryptographic service provider and a CA, select Advanced.

Advanced

---

< Back   Next >   Cancel

17. اكتب اسما ووصف  
للشهادة.



## Certificate Request Wizard



### Certificate Friendly Name and Description

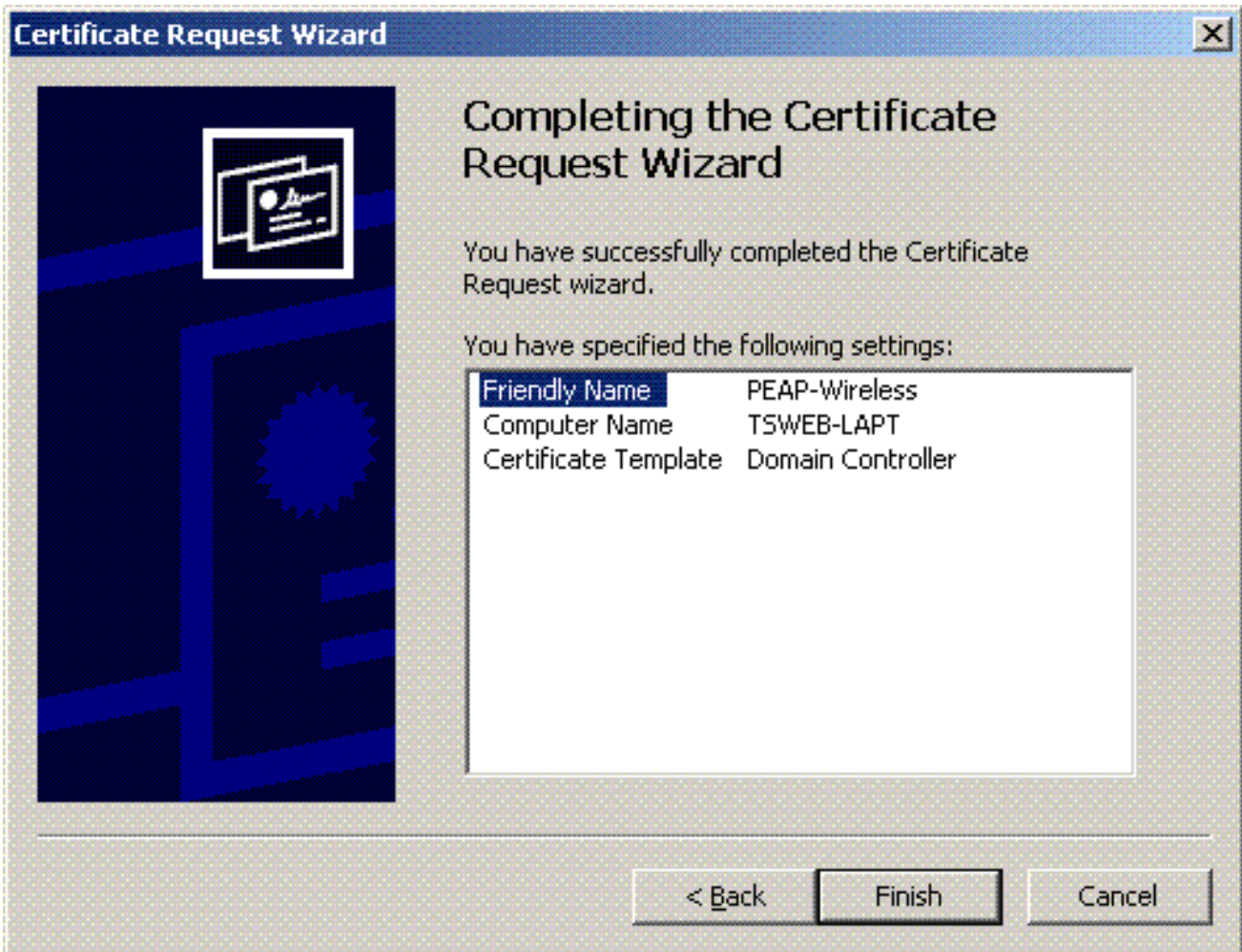
You can provide a name and description that help you quickly identify a specific certificate.

Type a friendly name and description for the new certificate.

Friendly name:

Description:

18. انقر فوق إنهاء " لإكمال معالج طلب الاعتماد.

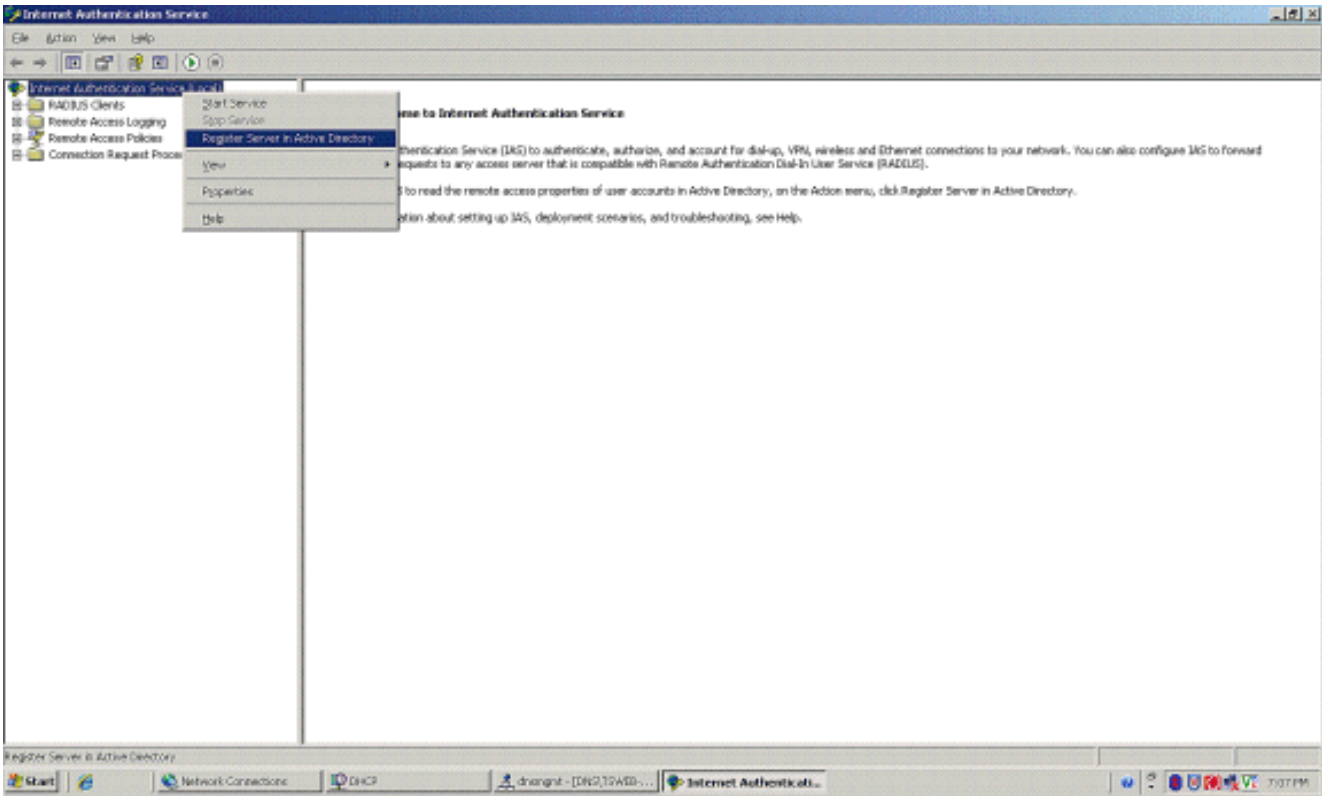


### تكوين خدمة مصادقة الإنترنت لمصادقة PEAP-MS-CHAP v2

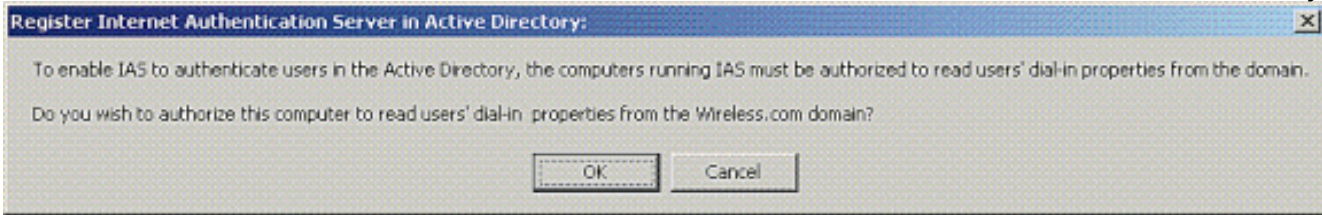
الآن بعد أن قمت بتثبيت طلب شهادة ل IAS، قم بتكوين IAS للمصادقة.

أكمل الخطوات التالية:

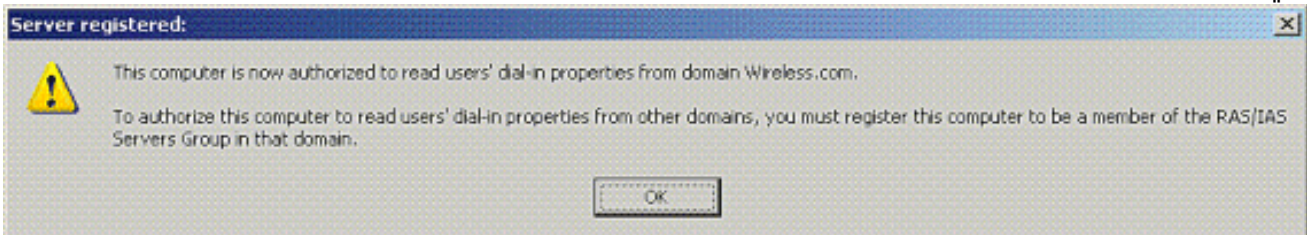
1. انقر على ابدأ < برامج < أدوات إدارية، وانقر فوق الأداة الإضافية لخدمة مصادقة الإنترنت.
2. انقر بزر الماوس الأيمن فوق خدمة مصادقة الإنترنت (IAS)، ثم انقر فوق تسجيل الخدمة في Active Directory.



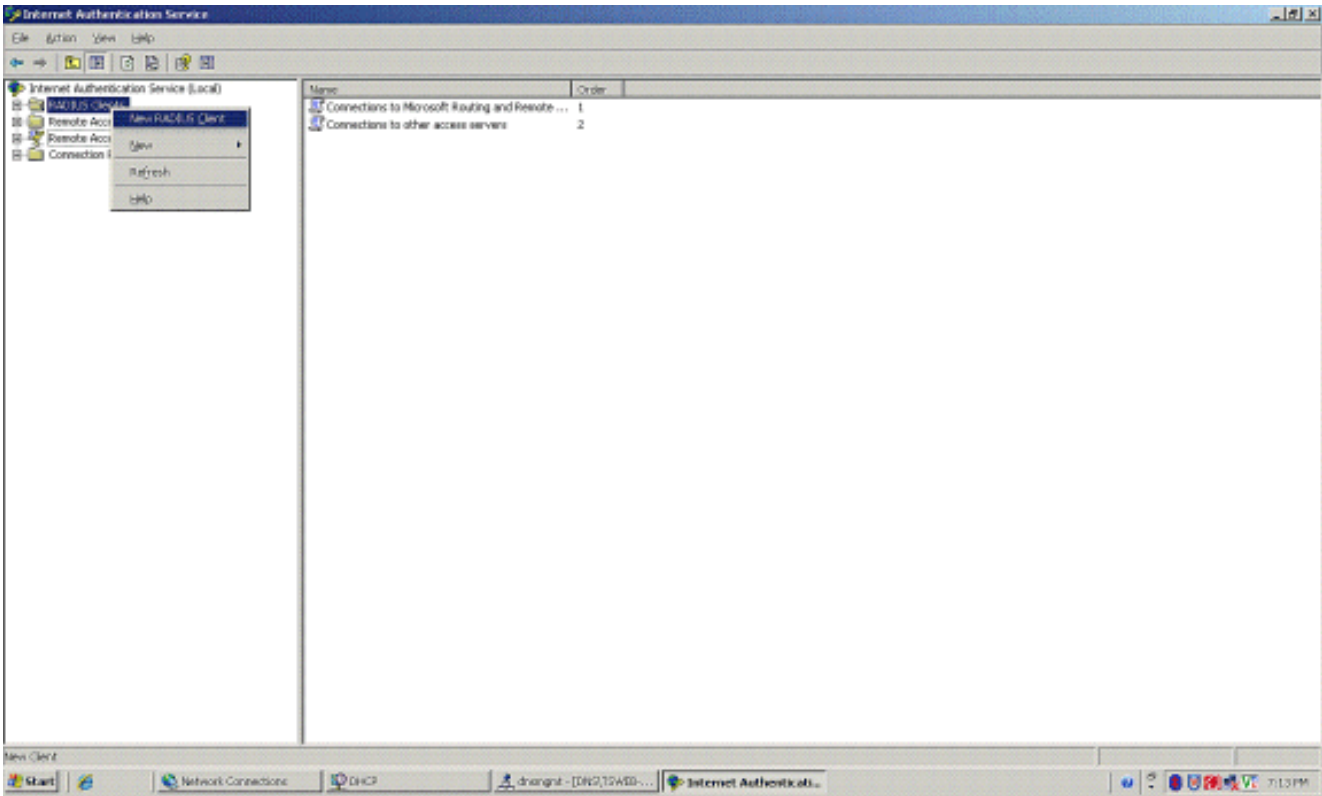
3. يظهر مربع الحوار تسجيل خدمة مصادقة الإنترنت في Active Directory، انقر موافق. هذا يمكن IAS من مصادقة المستخدمين في Active Directory.



4. طقطقة ok في الشاشة التالية.

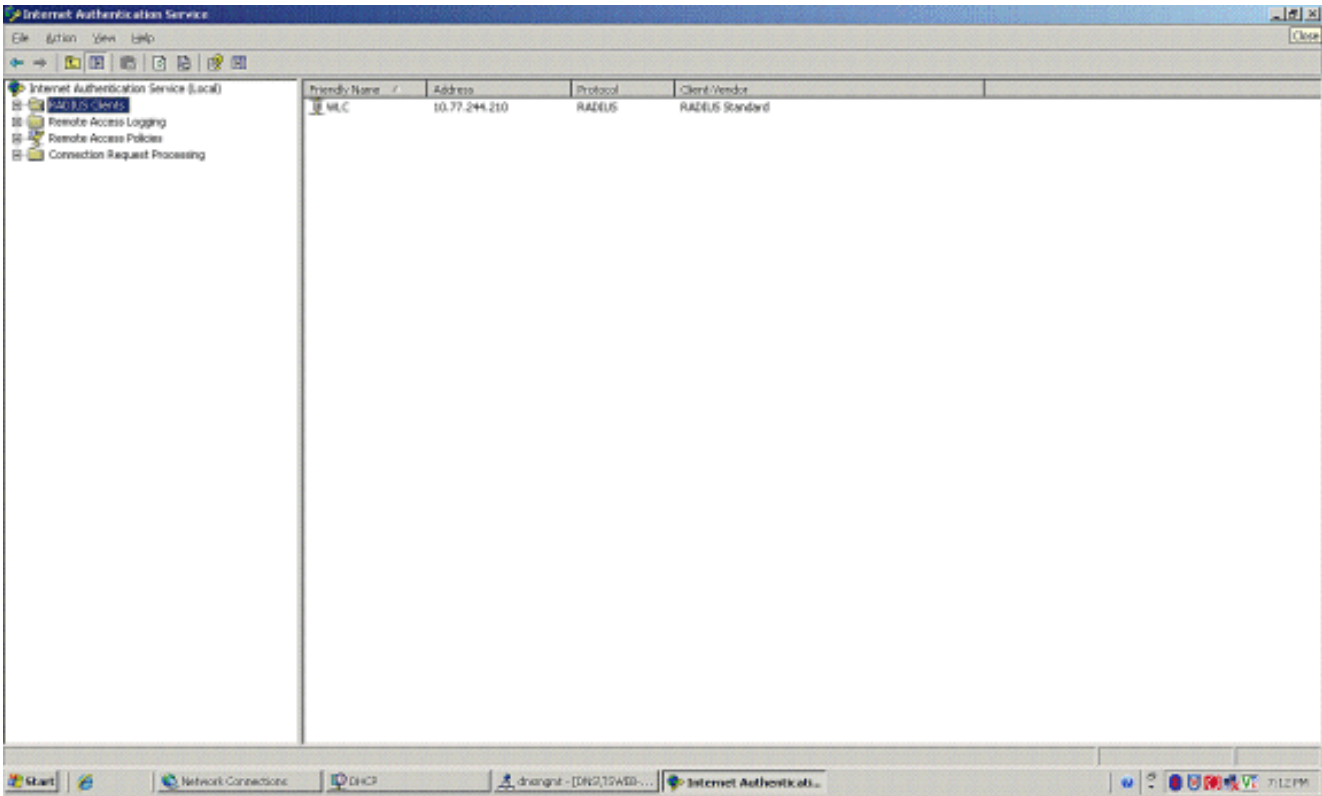


5. إضافة وحدة التحكم في شبكة LAN اللاسلكية كعميل AAA على خادم MS IAS.  
6. انقر بزر الماوس الأيمن فوق عملاء RADIUS، واختر عميل RADIUS الجديد.

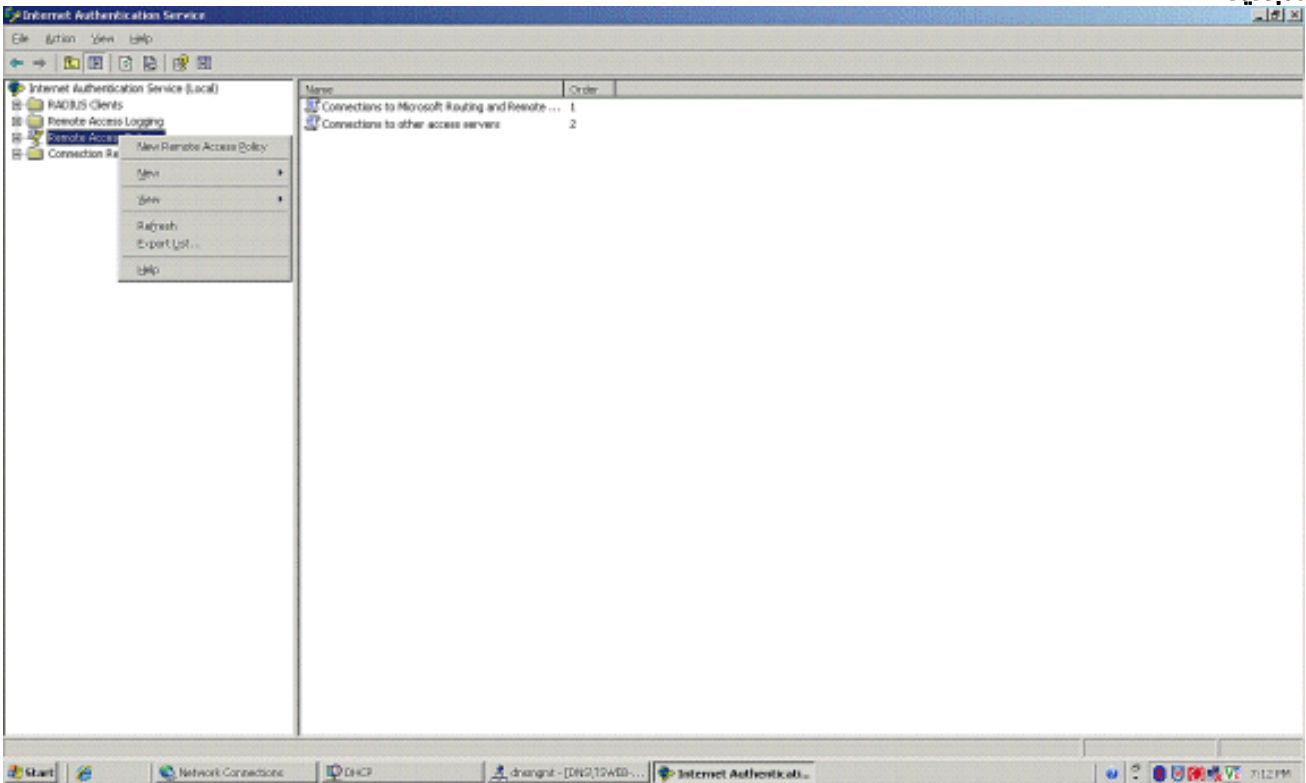


7. اكتب اسم العميل (WLC في هذه الحالة)، وأدخل عنوان IP الخاص بـ WLC. انقر فوق **Next** (التالي).

8. أخترت في الصفحة التالية، تحت زبون-بائع، **RADIUS معياري**؛ دخلت ال يشارك سر؛ وطققة 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.

**New Remote Access Policy Wizard** [X]

**Policy Configuration Method**

The wizard can create a typical policy, or you can create a custom policy.



How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

Type a name that describes this policy.

Policy name:

Example: Authenticate all VPN connections.

< Back   Next >   Cancel

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

## New Remote Access Policy Wizard



### Access Method

Policy conditions are based on the method used to gain access to the network.



Select the method of access for which you want to create a policy.

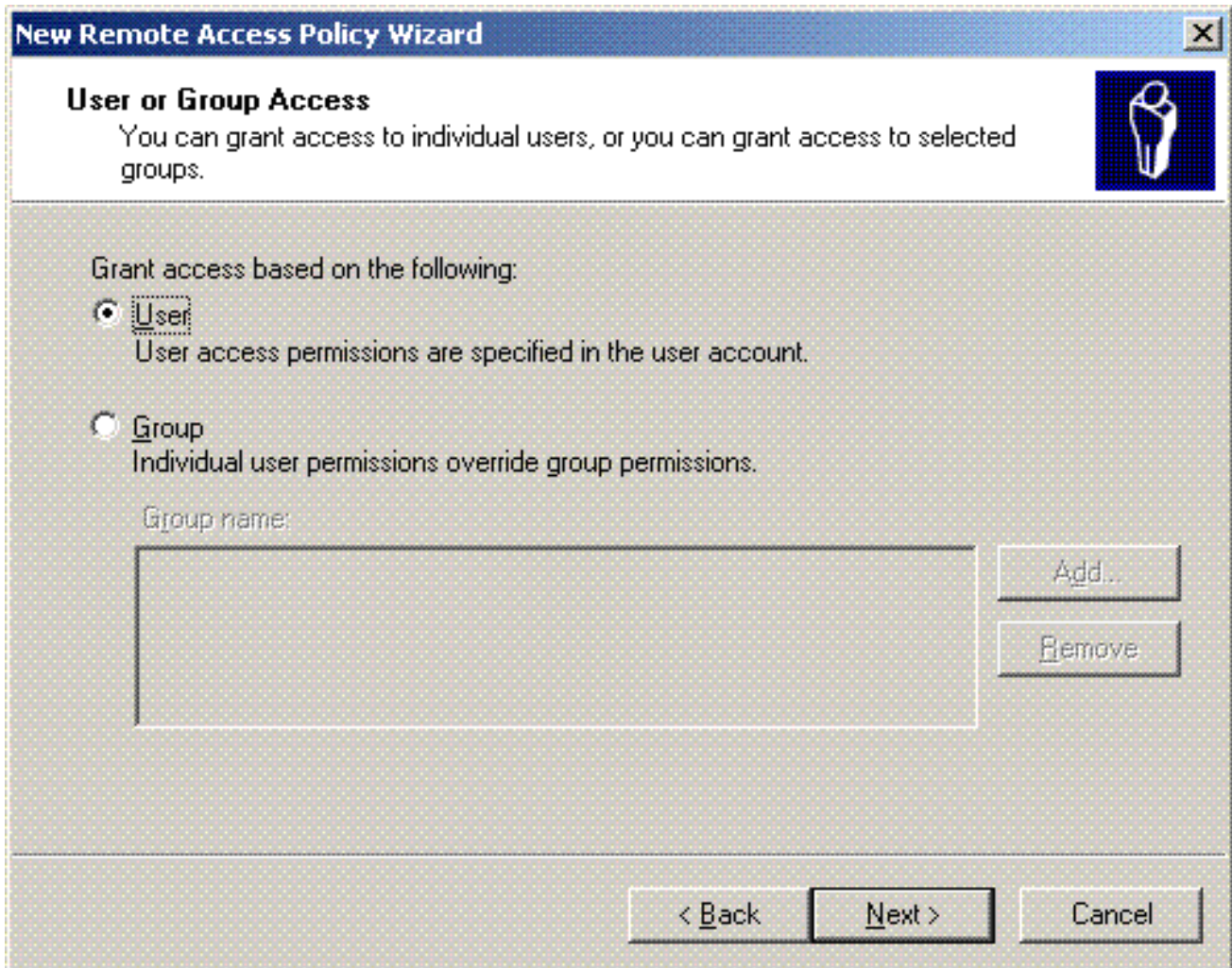
- V**PN  
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
- D**ial-up  
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
- W**ireless  
Use for wireless LAN connections only.
- E**thernet  
Use for Ethernet connections, such as connections that use a switch.

< **B**ack

**N**ext >

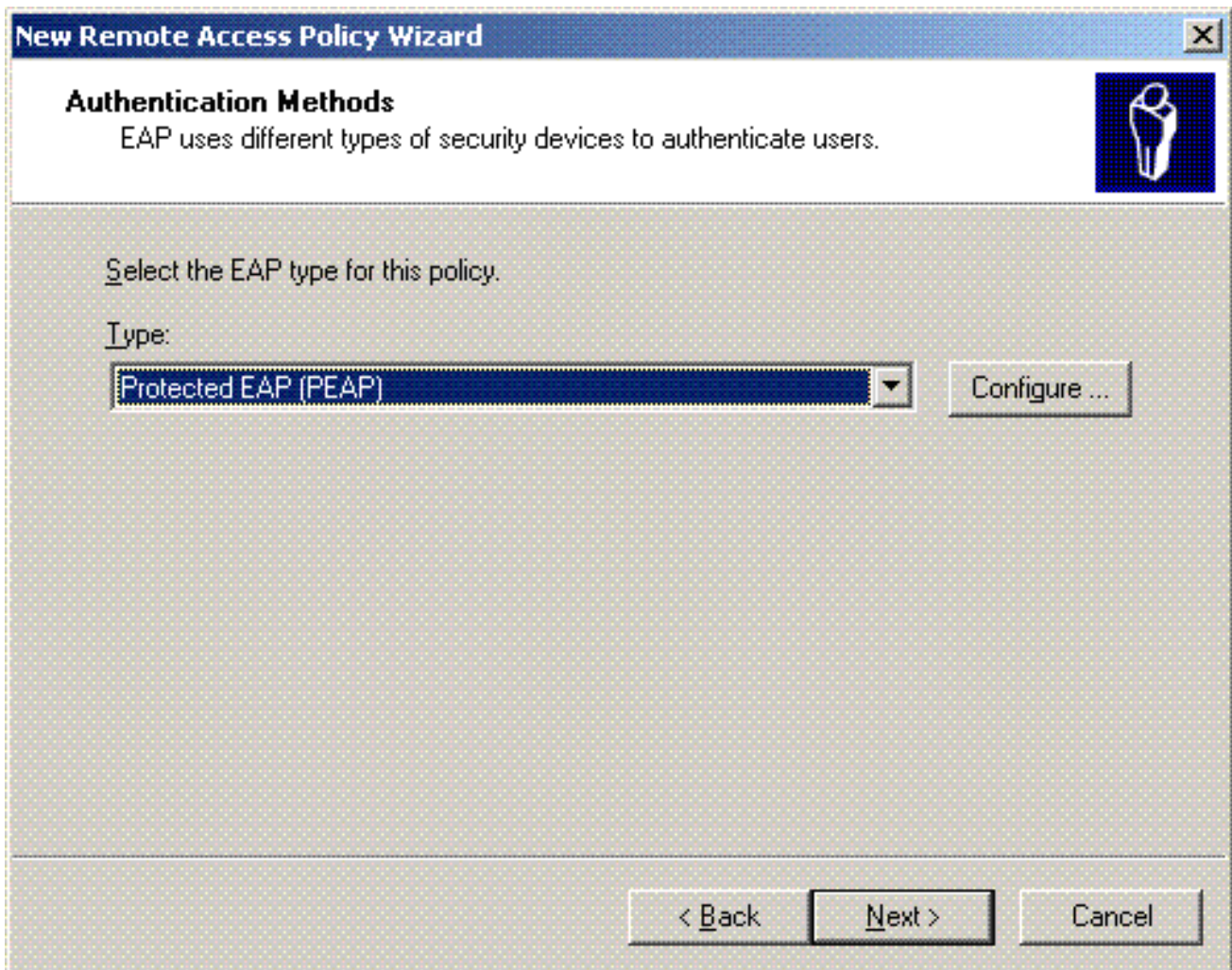
Cancel

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

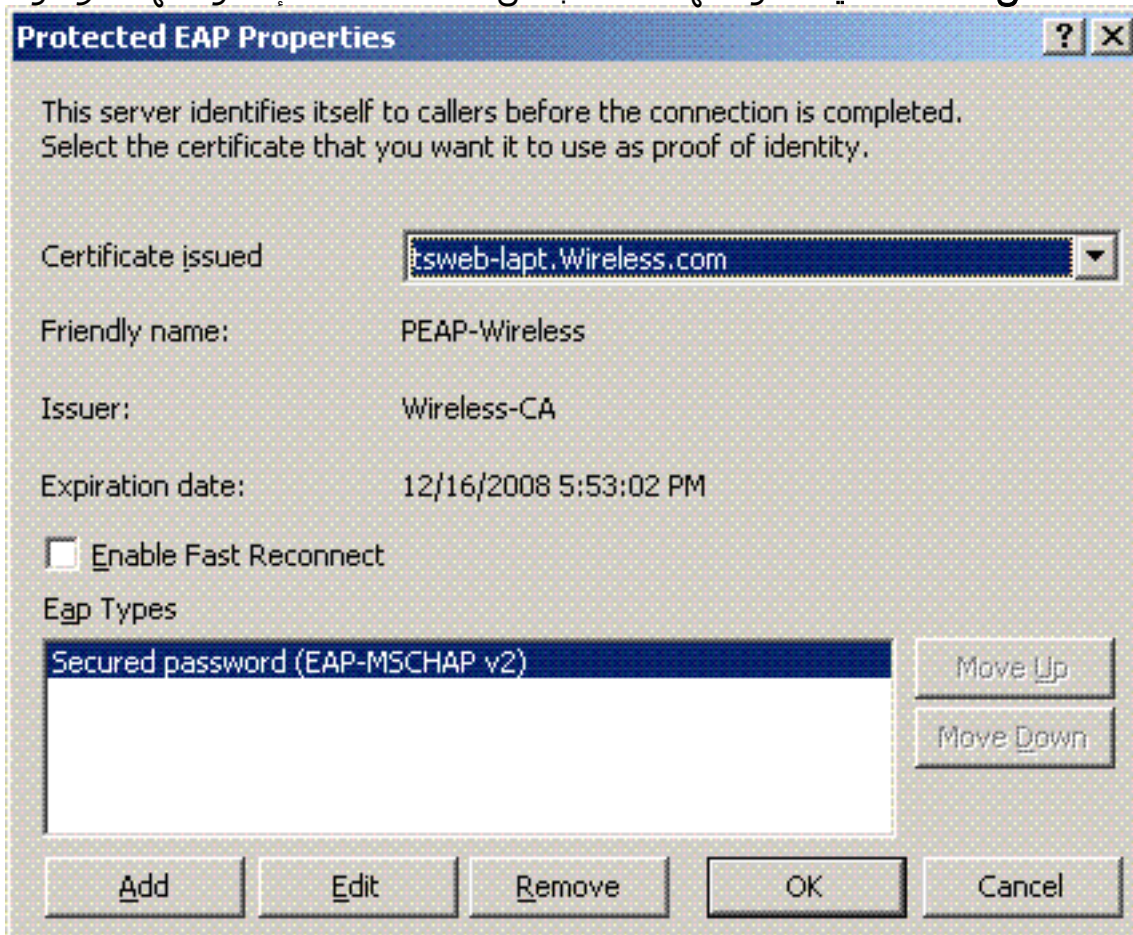


15. اخترت تحت أسلوب صحة هوية، محمي (PEAP) (EAP)، وطققة  
يشكل.



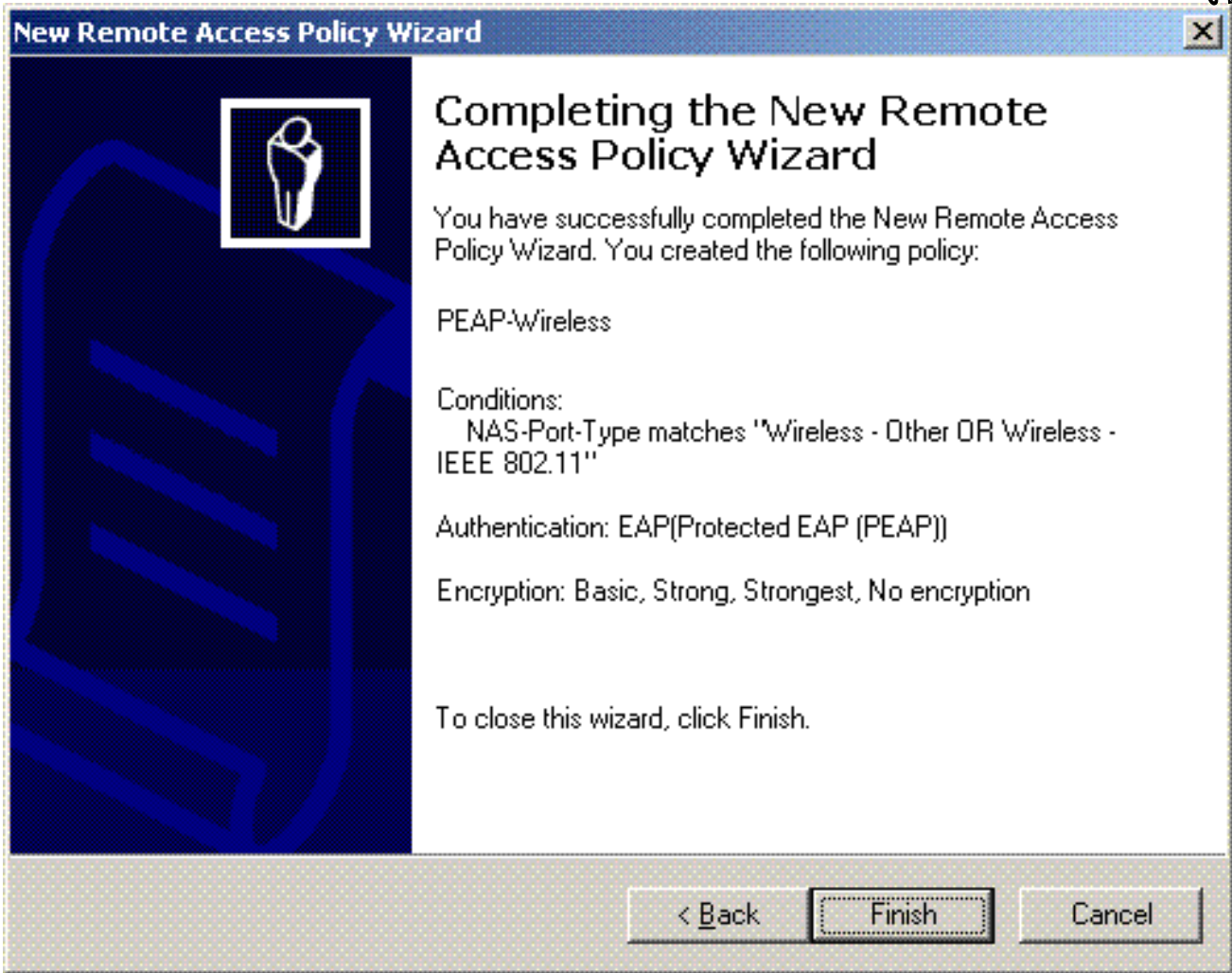


16. في صفحة خصائص EAP المحمية، أختار الشهادة المناسبة من القائمة المنسدلة إصدار الشهادة، وانقر على

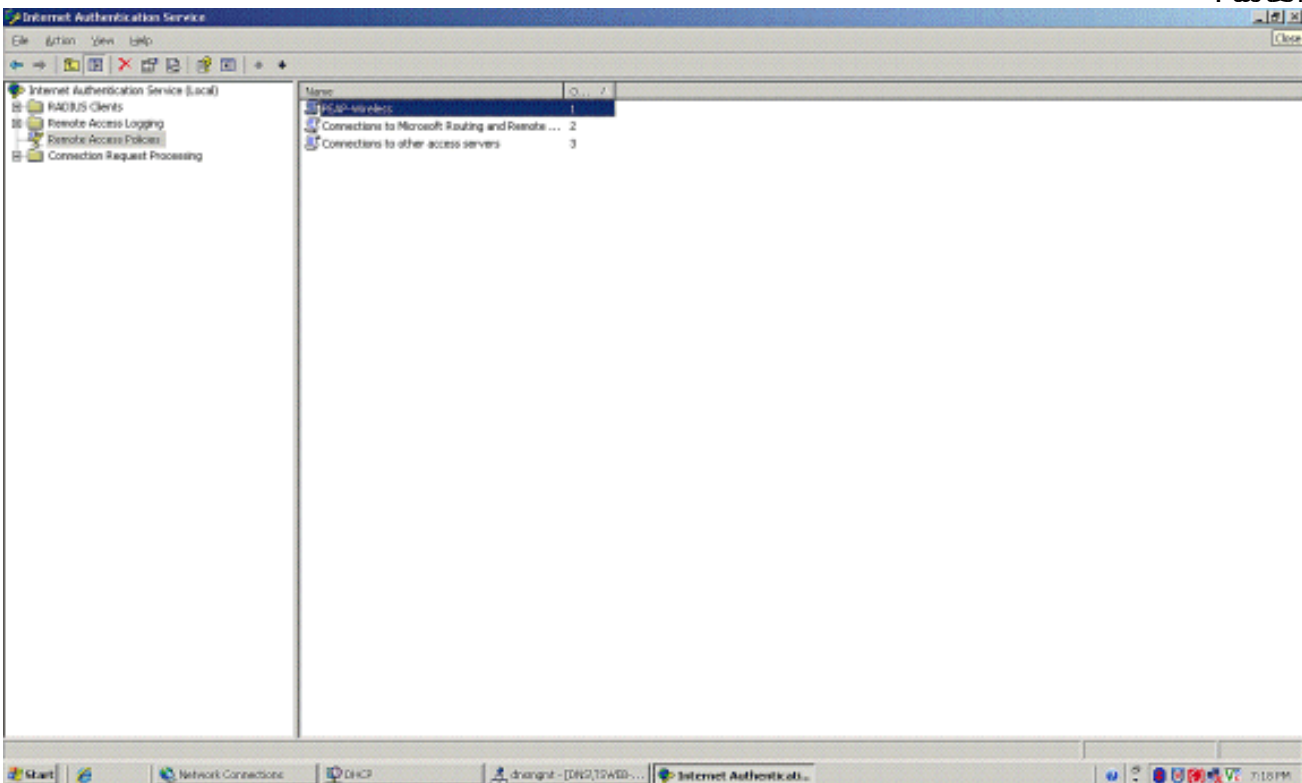


موافق.

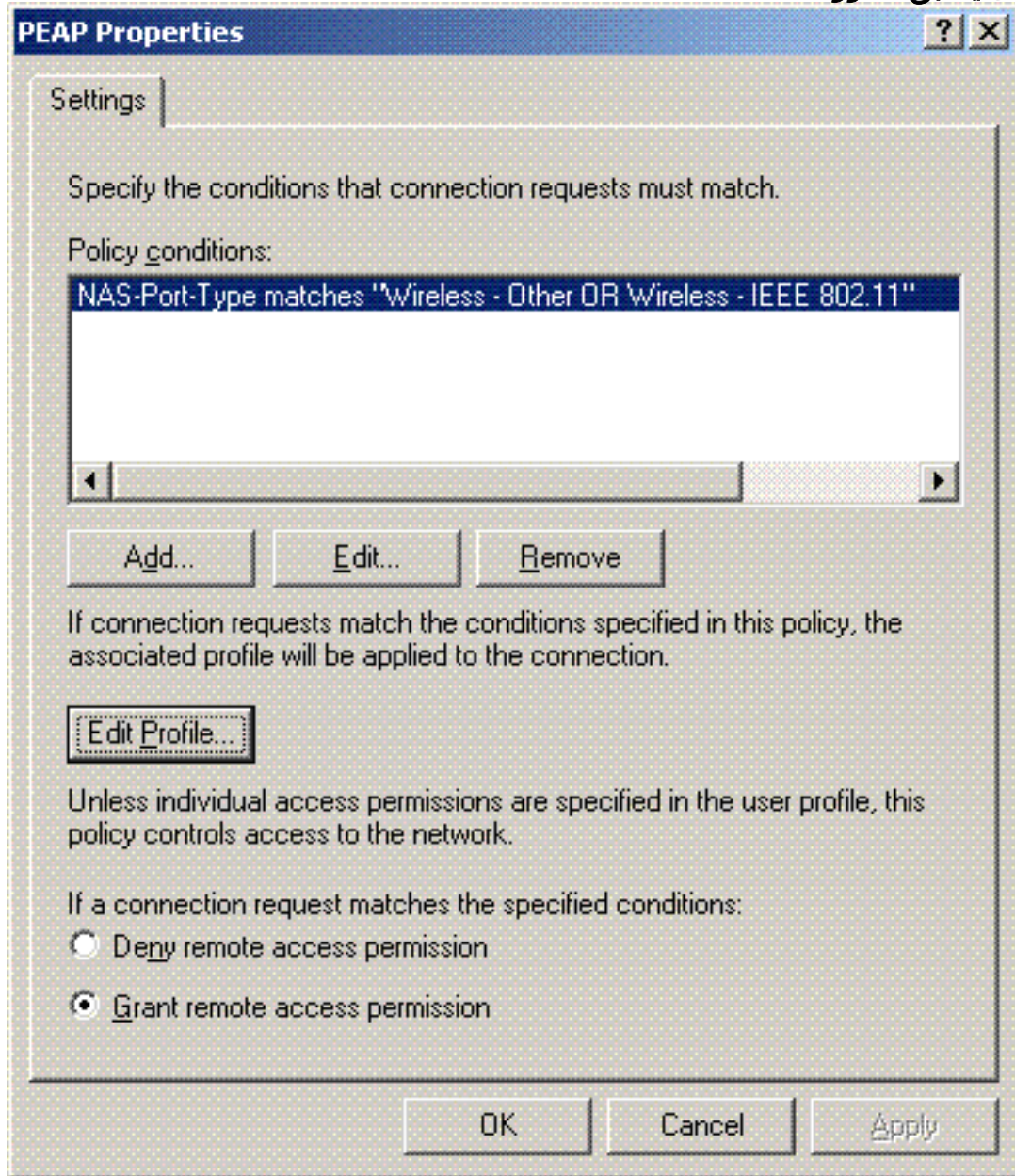
17. تحقق من تفاصيل نهج الوصول عن بعد، ثم انقر فوق إنهاء.



18. تمت إضافة نهج الوصول عن بعد إلى القائمة.



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



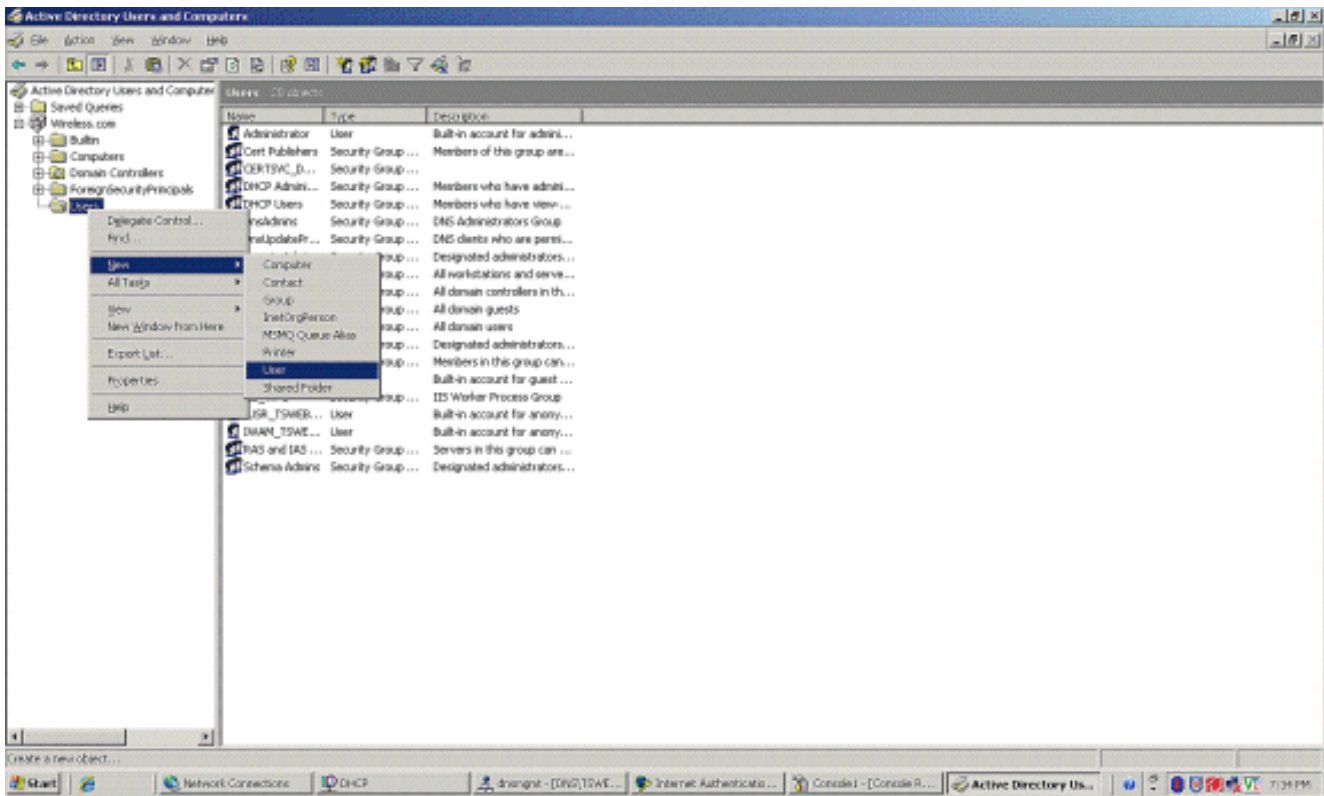
المحددة".

### [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**

The 'New Object - User' dialog box is shown. The 'Create in' field is set to 'Wireless.com/Users'. The 'First name' field contains 'Client 1', and the 'Initials' field is empty. The 'Last name' field is empty. The 'Full name' field contains 'Client 1'. The 'User logon name' field contains 'Client1' and the domain dropdown is set to '@Wireless.com'. The 'User logon name (pre-Windows 2000)' field contains 'WIRELESS\'. The 'Client 1' text is also present in the second part of this field. The 'Back <' button is disabled, and the 'Next >' button is highlighted. The 'Cancel' button is also visible.

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**.

**New Object - User** [X]

 Create in: Wireless.com/Users

---

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled


---

< Back   Next >   Cancel

التالي.

4. في شاشة كائن جديد - مستخدم، انقر

**New Object - User** [X]

 Create in: Wireless.com/Users

---

When you click Finish, the following object will be created:

Full name: Client 1

User logon name: Client1@Wireless.com

---

< Back   Finish   Cancel

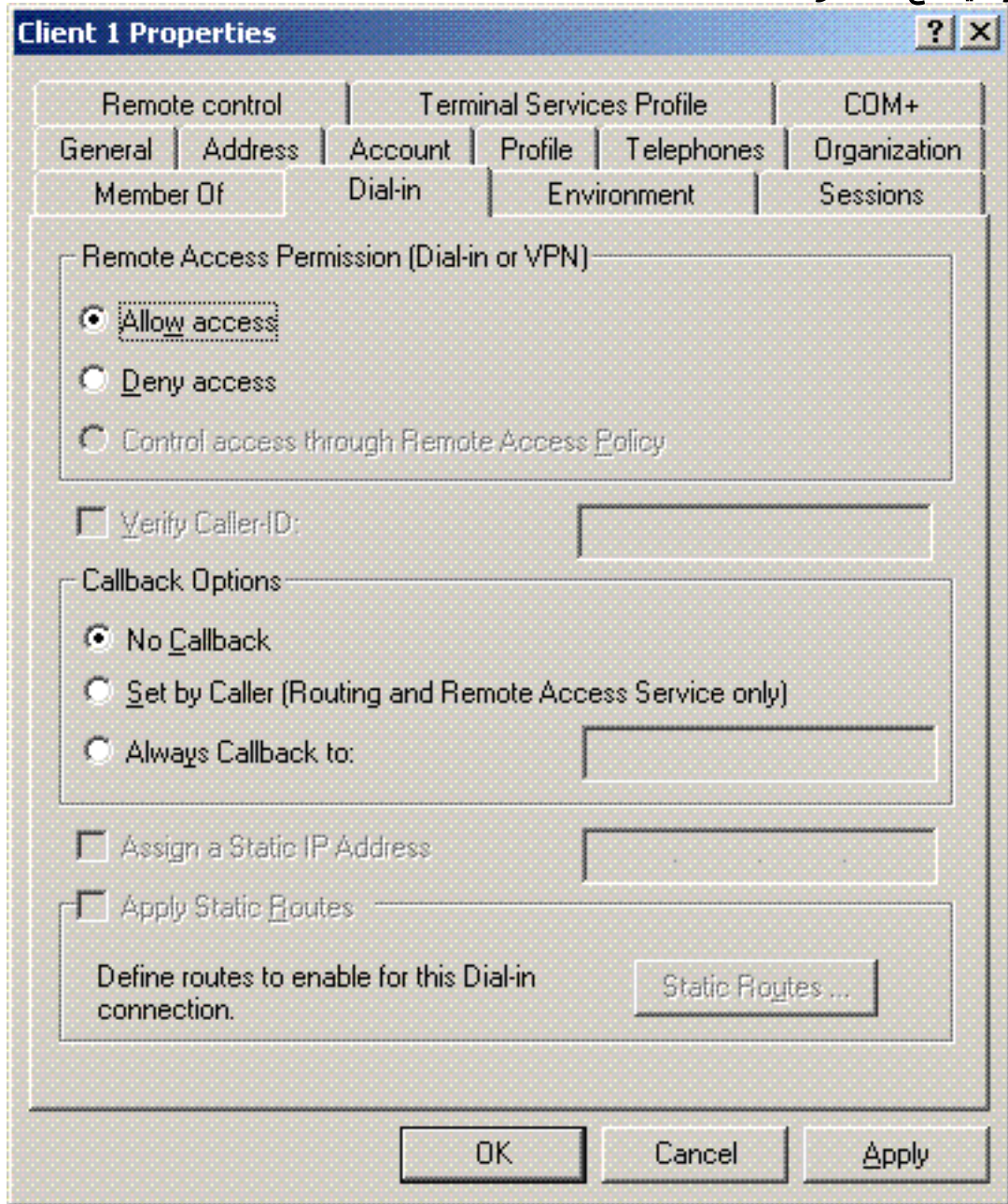
إنهاء.

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**، وطققة



.ok

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

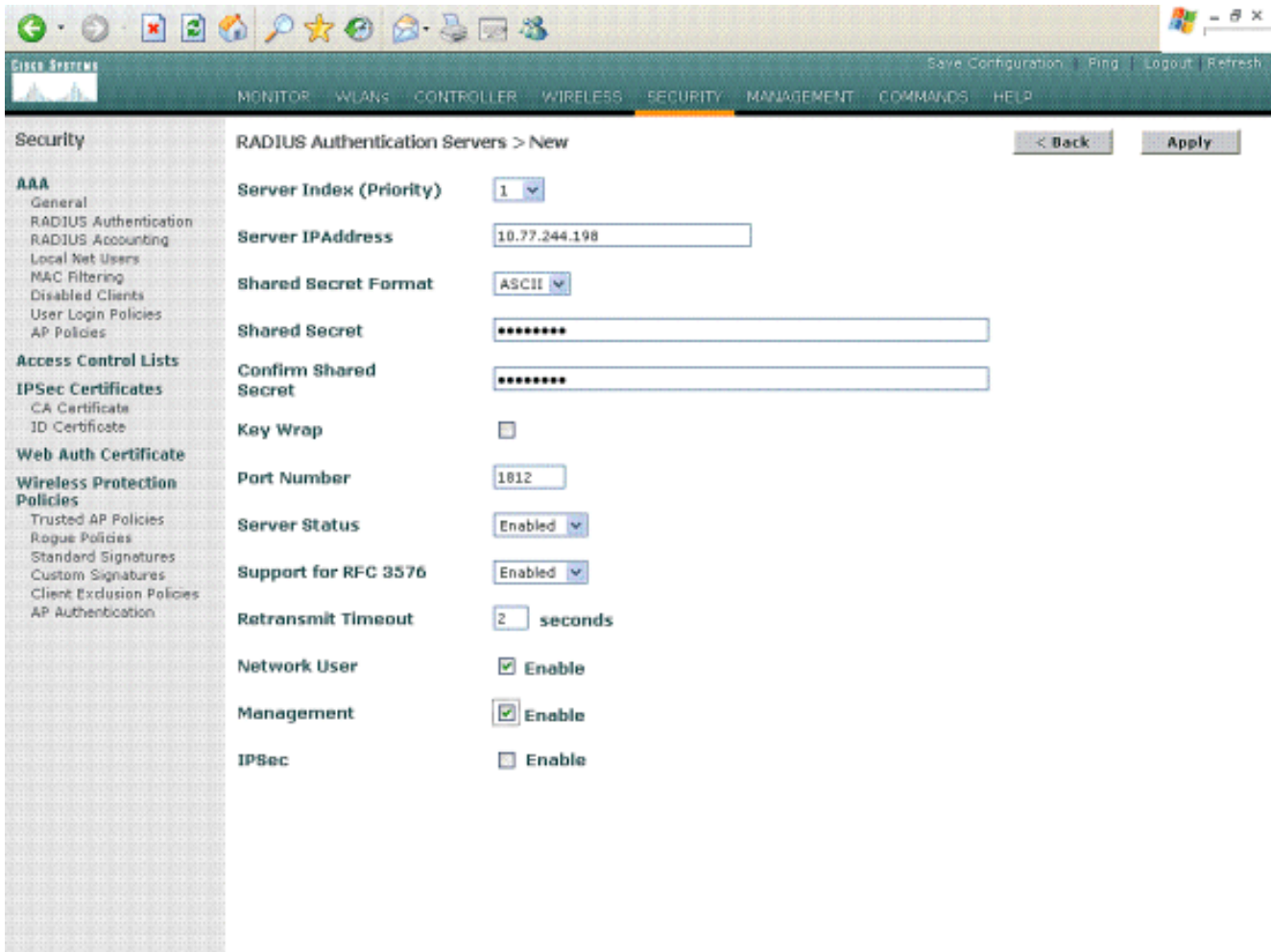
قم الآن بتكوين الأجهزة اللاسلكية لهذا الإعداد. وهذا يتضمن تكوين وحدات التحكم في الشبكة المحلية اللاسلكية ونقاط الوصول في الوضع Lightweight والعملاء اللاسلكيين.

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

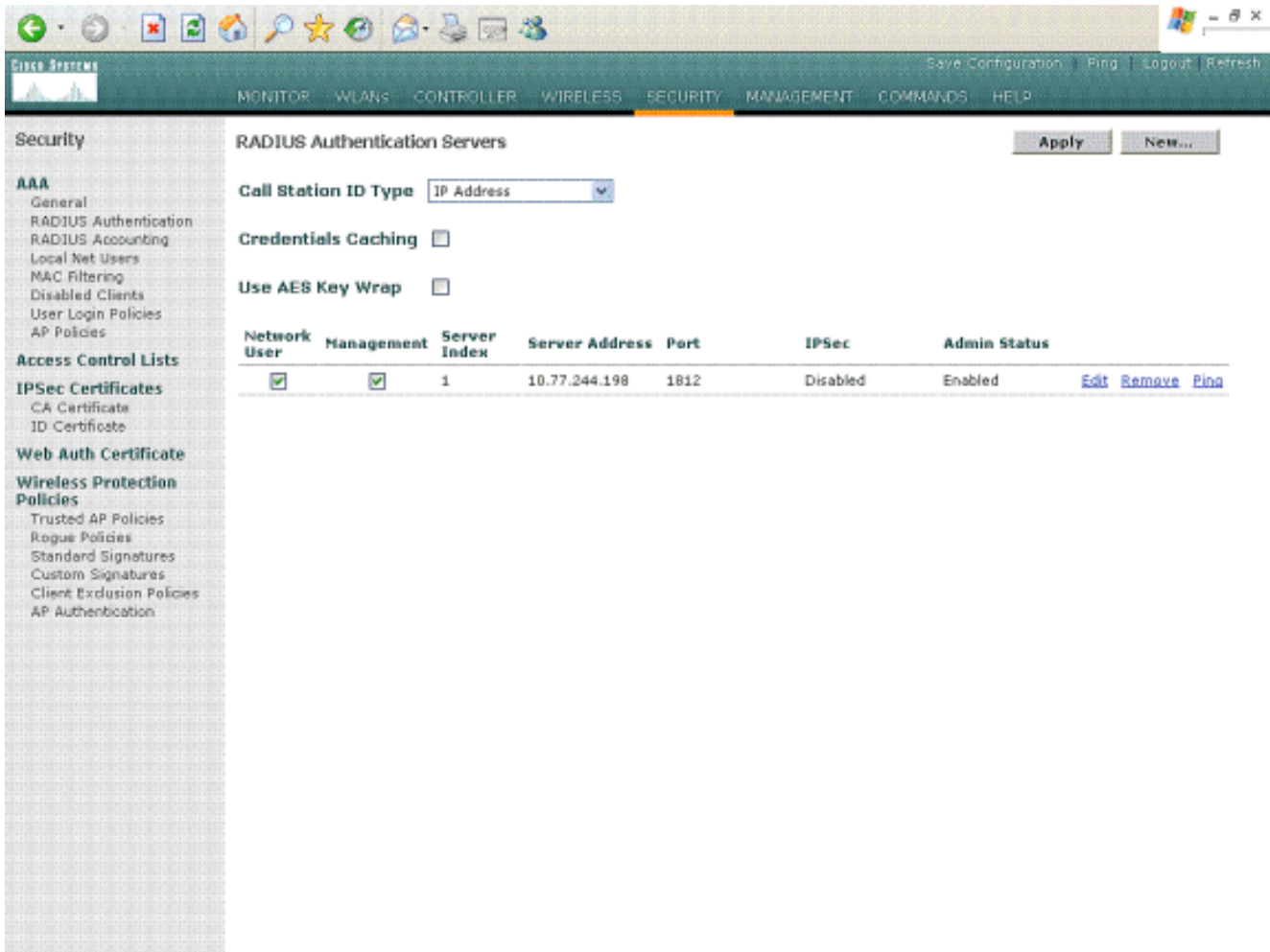
قم أولاً بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لاستخدام MS IAS كخادم مصادقة. يلزم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإعادة توجيه بيانات اعتماد المستخدم إلى خادم RADIUS خارجي. ثم يتحقق خادم RADIUS الخارجي من مسوغات المستخدم ويوفر الوصول إلى عملاء اللاسلكي. للقيام بذلك، 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 خانة 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 استخدامه لمصادقة العملاء اللاسلكيين.

### تكوين شبكة WLAN للعملاء

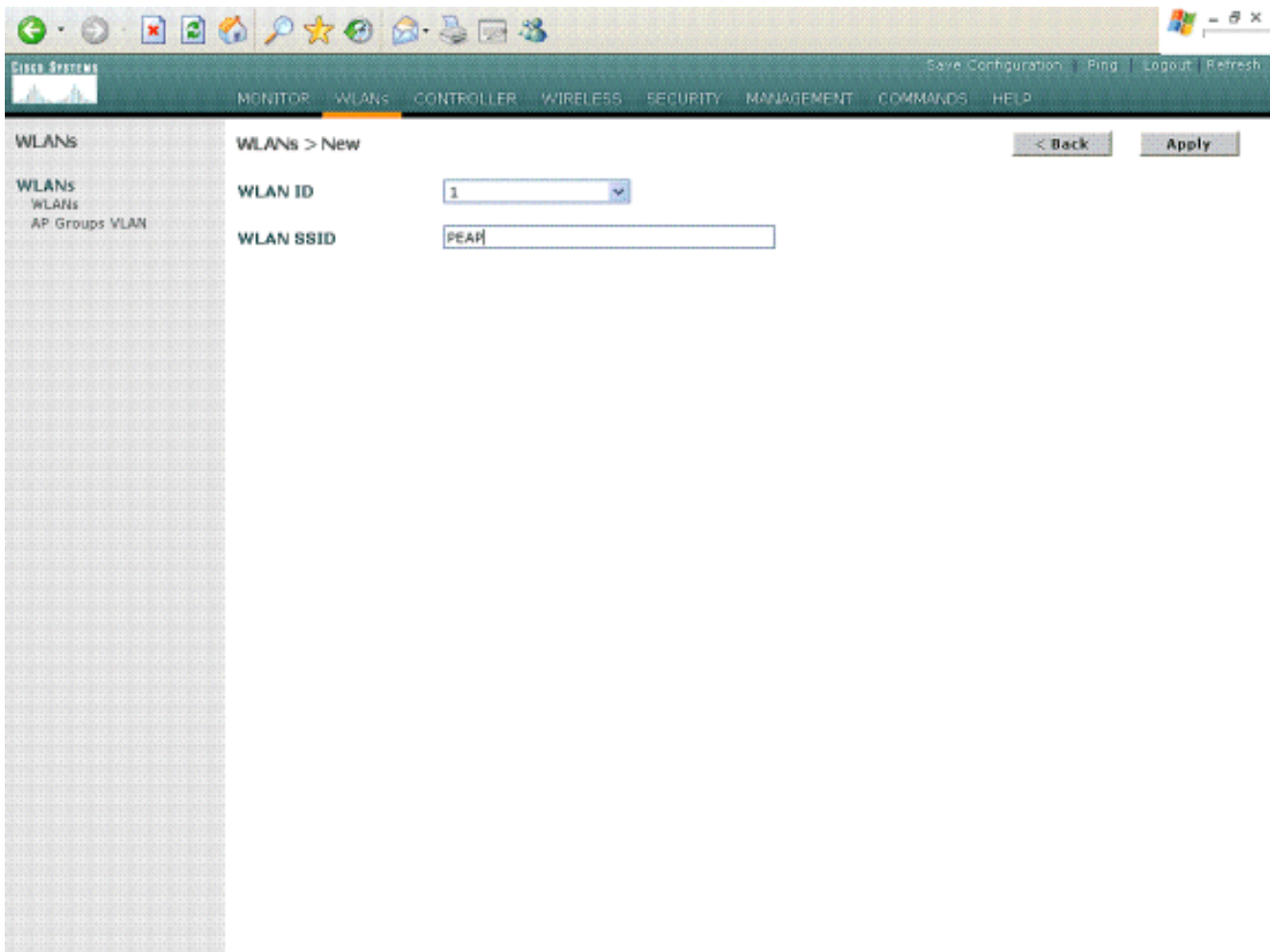
تكوين (WLAN) SSID الذي يتصل به العملاء اللاسلكيين. في هذا المثال، قم بإنشاء SSID، وقم بتسميته PEAP. قم بتعريف مصادقة الطبقة 2 على أنها WPA2 حتى يقوم العملاء بإجراء مصادقة تستند إلى PEAP (EAP MSCHAPv2 في هذه الحالة) واستخدم AES كآلية تشفير. أترك كل القيم الأخرى عند وضعها الافتراضي.

**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.](#)

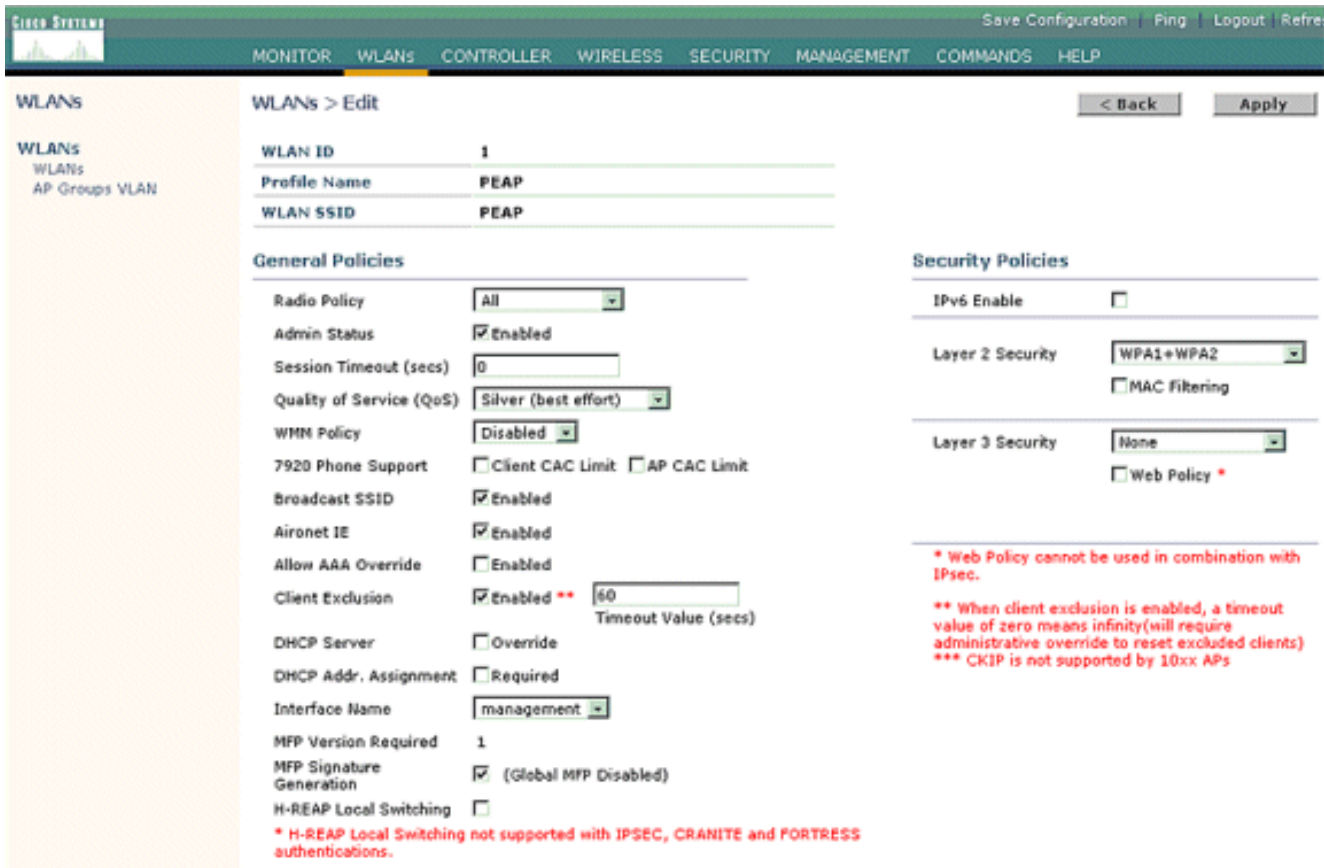
أتمت in order to شكلت WLAN على ال WLC هذا steps:

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، فتتحقق من بث SSID.
5. تحت تأمين الطبقة 2، اختر WPA1+WPA2. هذا يمكن WPA على ال WLAN. انزلق إلى أسفل الصفحة واختر سياسة WPA. يستخدم هذا المثال تشفير WPA2 و AES. اختر خادم RADIUS المناسب من القائمة المنسدلة تحت خوادم RADIUS. في هذا المثال، استخدم 10.77.244.198 (عنوان IP الخاص بخادم MS IAS). يمكن تعديل المعلمات الأخرى استنادا إلى متطلبات شبكة WLAN.



6. طقطقة

يطبق.



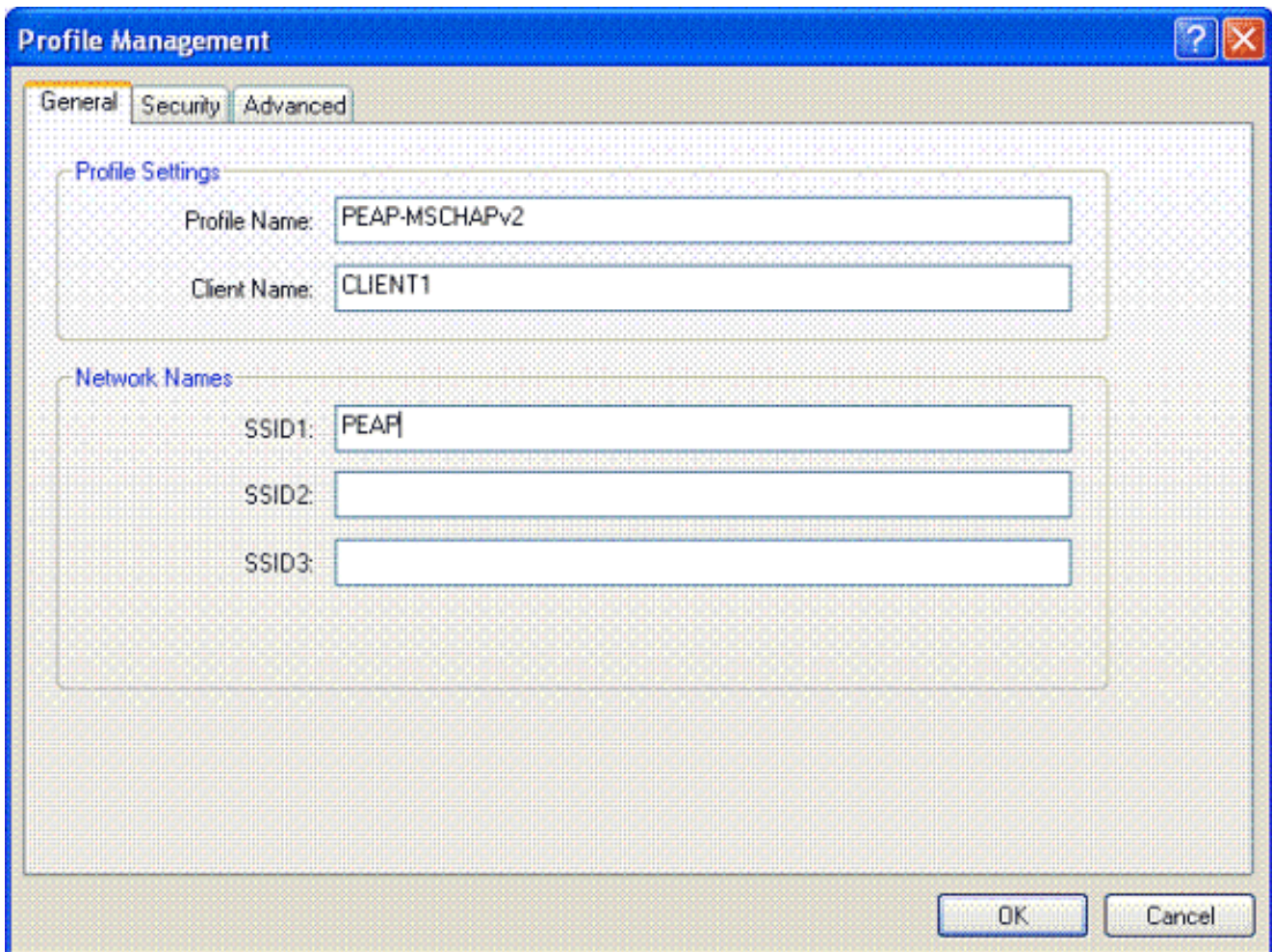
## تكوين عملاء اللاسلكي

### تكوين عملاء اللاسلكي لمصادقة PEAP-MS CHAPv2

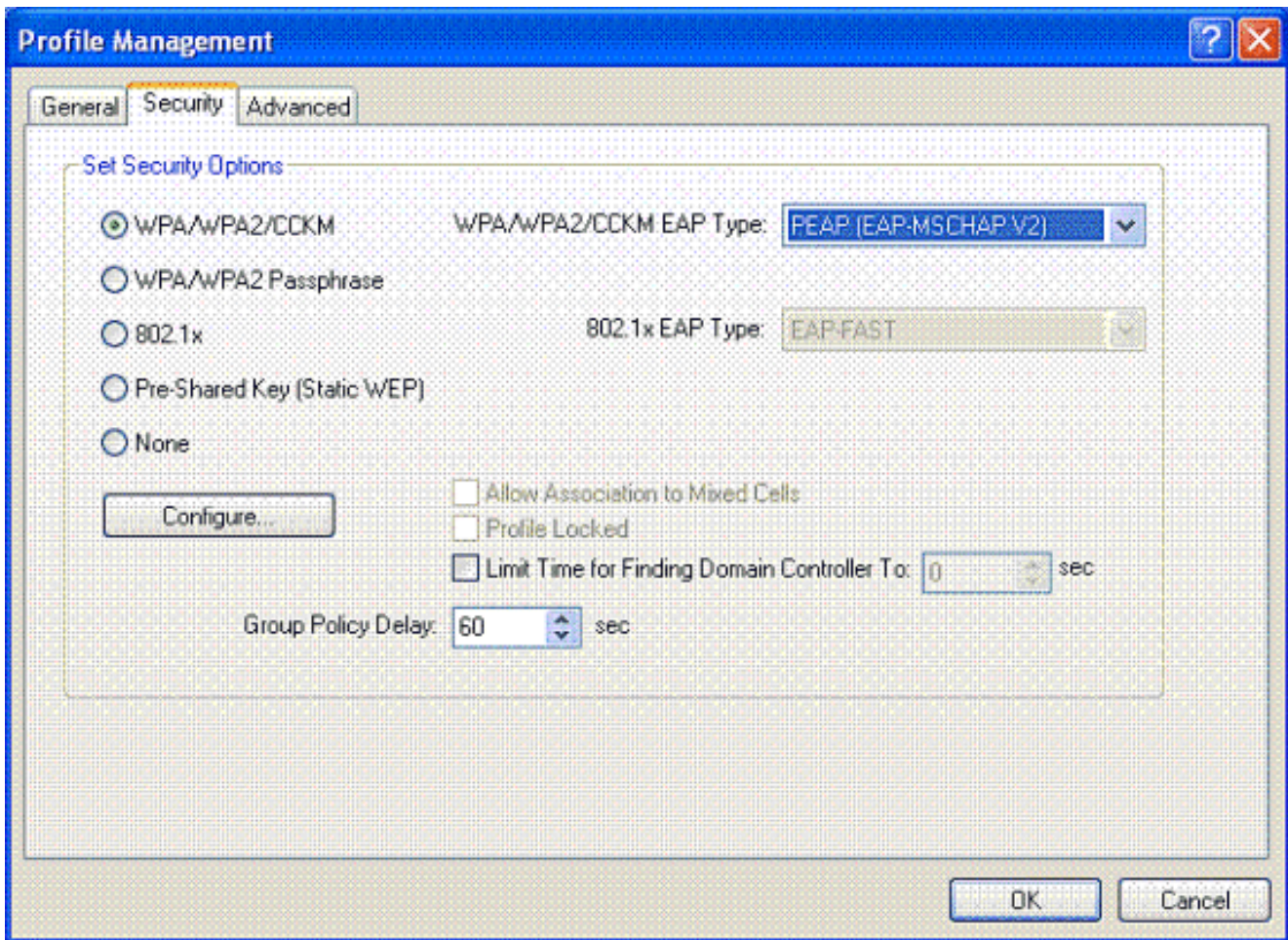
يقدم هذا المثال معلومات حول كيفية تكوين العميل اللاسلكي باستخدام أداة Cisco Aironet Desktop Utility المساعدة. قبل تكوين مهائى العميل، تأكد من استخدام أحدث إصدار من البرامج الثابتة والأداة المساعدة. ابحث عن أحدث إصدار من البرامج الثابتة والأدوات المساعدة في صفحة تنزيلات الشبكات اللاسلكية على موقع الويب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

لتكوين مهائى 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، استخدم معرف SSID الذي قمت بتكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية ((WLC)) ((PEAP)).



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



5. أختَرِ التَّحَقُّقَ مِنْ شَهَادَةِ الخَادِمِ، وَاخْتَرِ Wireless-CA ضمن القائمة المنسدلة مراجع التصديق الجذر الموثوق

**Configure PEAP (EAP-MSCHAP V2)**

Use Machine Information for Domain Logon

Validate Server Identity

Trusted Root Certification Authorities

Wireless-CA

When connecting, use:

Certificate

User Name and Password

Select a Certificate

Use Windows User Name and Password

User Information for PEAP (EAP-MSCHAP V2) Authentication

User Name: Administrator

Password:

Confirm Password:

Advanced... OK Cancel

فيها. 6. انقر على موافق، وقم بتنشيط ملف التخصيص. ملاحظة: عند استخدام بروتوكول المصادقة لتأكيد اتصال EAP- Microsoft مع التحدي المحمي الإصدار 2 (PEAP-MSCHAPv2) مع Microsoft XP SP2، تتم إدارة البطاقة اللاسلكية بواسطة (WZC) Microsoft Wireless Zero Configuration، 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.



**(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  
(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 PLUMBFASPATH: 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 التوصليل الأولي بنجاح، لكن محاولات مصادقة التوصليل 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](#)

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 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