

ACS عم ةءءوم ةيكلسال ةكبش ءءء EAP-TLS 4.0 و Windows 2003

المءءوءاء

[المءءوءة](#)

[المءءوءاء الأساسفة](#)

[المءءوءاء](#)

[المءوءاء المءءءوءة](#)

[الرسم الءءءبء للءءءة](#)

[الاصءلاءاء](#)

[إءءاء Windows Enterprise 2003 باءءءءام IIS ومرءء الشءءاء و DNS و CA و DHCP\)](#)

[DC CA \(ءءءة WirelessDemoca\)](#)

[إءءاء Windows Standard 2003 مع Cisco Secure ACS 4.0](#)

[الءءبء وءءوءوء الأساسفاء](#)

[ءءبء Cisco Secure ACS 4.0](#)

[ءءوءوء وءءة الءءءء Cisco LWAPP Controller](#)

[ءءءء الءءءءل ضرورف ل WPA2/WPA](#)

[مصادءة EAP-TLS](#)

[ءءبء الأءاءة الإءءافة لءوءب الشءءاء](#)

[ءم بانءشاء ءالب الشءءاءة لءءءم وءب ACS](#)

[ءمءءن ءالب شءءاءة لءءءم وءب ACS الءءءء](#)

[إءءاء شءءاءة ACS 4.0](#)

[ءءوءوء الشءءاءة الءالبة للءءءءءر ل ACS](#)

[ءءبء الشءءاءة فف برنامء ACS 4.0](#)

[ءءوءوء العمبل ل EAP-TLS باءءءءام Windows Zero Touch](#)

[إءءاء عمبلة ءءبء وءءبءة أساسفة](#)

[ءءوءوء ءوءبل الشءءة اللاسلكفة](#)

[مءءوءاء ءاء صلة](#)

المءءوءة

فصف هءا المءءءء ءففة ءءوءوء الوصول اللاسلكف الآمن باءءءءام وءءاء الءءءءم فف الشءءة المءءفة اللاسلكفة (WLCs) وبرنامء Microsoft Windows 2003 و Cisco Secure Access Control Server (ACS) 4.0 عبر بروءوءوءوء المصادءة المءوءسع - أمان طبءة النقل (EAP-TLS).

ملاءءة: للءءوءوء على مزفء من المءءوءوءاء ءوء نشر الءءءءال اللاسلكف الآمن، ارءء إلى [موءء Microsoft Wi-Fi](#) على الوب ومءءء Cisco SAFE اللاسلكف.

المءءوءاء الأساسفة

المتطلبات

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

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](#). للحصول على معلومات التثبيت الأولى ومعلومات التكوين لوحدة التحكم من السلسلة Cisco 2000 Series، ارجع إلى [دليل البدء السريع: سلسلة وحدات التحكم في الشبكة المحلية اللاسلكية Cisco 2000 Series](#).

قبل البدء، قم بتثبيت Windows Server 2003 باستخدام نظام التشغيل Service Pack (SP)1 على كل خادم في مختبر الاختبار وقم بتحديث جميع حزم الخدمة. قم بتثبيت وحدات التحكم ونقاط الوصول (AP) وتأكد من تكوين آخر تحديثات البرامج.

هام: في الوقت الذي تمت فيه كتابة هذا المستند، يكون SP1 هو آخر تحديث لنظام التشغيل Windows Server 2003، كما أن SP2 المزود بتصحيحات تحديث هو أحدث برنامج لنظام التشغيل Windows XP Professional.

يستخدم Windows Server 2003 Enterprise Edition المزود بحزمة الخدمة Enterprise Edition، SP1 لتكوين التسجيل التلقائي لشهادات المستخدم ومحطة العمل لمصادقة EAP-TLS. وهذا موضح في قسم [مصادقة EAP-TLS](#) في هذا المستند. يعمل التسجيل التلقائي للشهادة والتجديد التلقائي على تسهيل نشر الشهادات وتحسين الأمان من خلال إنهاء الشهادات وتجديدها تلقائياً.

المكونات المستخدمة

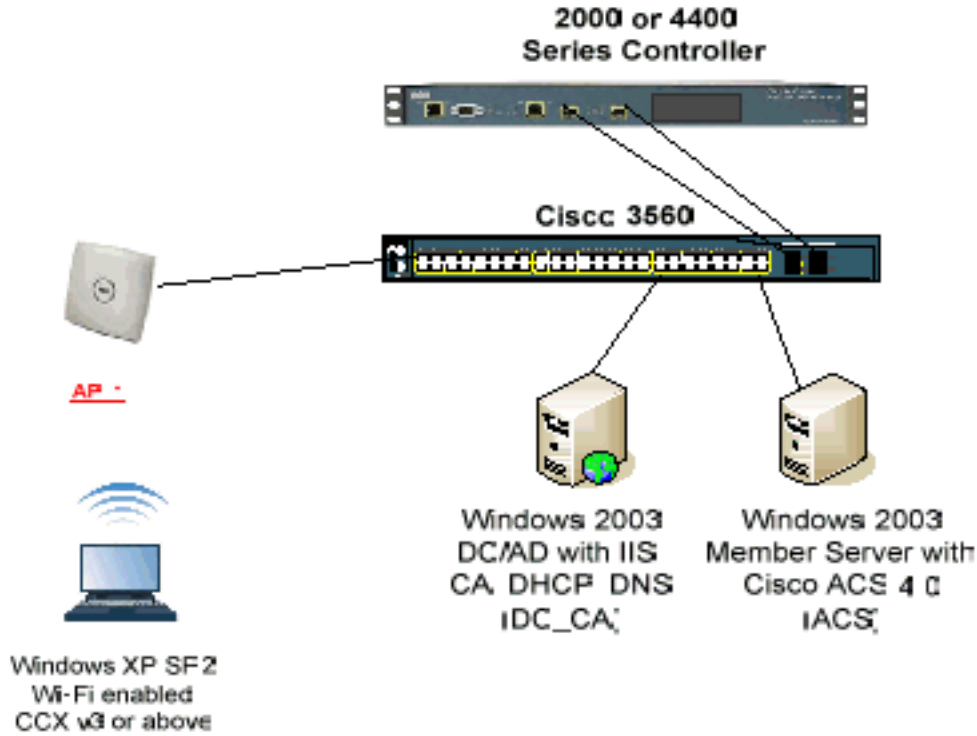
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة التحكم من السلسلة Cisco 2006 أو Series 4400 التي تشغل الإصدار 3.2.116.21
- نقطة الوصول AP Cisco 1131 Lightweight Access Point Protocol (LWAPP)
- Windows 2003 Enterprise مع تثبيت Internet Information Server (IIS) و Certificate Authority (CA) و DHCP ونظام اسم المجال (DNS)
- Windows 2003 Standard مع خادم التحكم في الوصول (ACS)، الإصدار 4.0
- Windows XP Professional مع SP (وحزم الخدمة المحدثة) وبطاقة واجهة الشبكة اللاسلكية (NIC) (مع دعم CCX v3) أو طالب من طرف ثالث.
- المحول Cisco 3560 Switch

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

طبولوجيا المختبرات اللاسلكية الآمنة من Cisco



الغرض الأساسي من هذا المستند هو توفير إجراء مفصل لتنفيذ EAP-TLS تحت شبكات لاسلكية موحدة مع ACS 4.0 و Windows 2003 Enterprise server. ينصب التركيز الرئيسي على التسجيل التلقائي للعميل حتى يتمكن العميل من التسجيل التلقائي وبأخذ الشهادة من الخادم.

ملاحظة: من أجل إضافة WPA/WPA2 (Wi-Fi Protected Access) مع بروتوكول سلامة المفاتيح المؤقتة (TKIP)/معيير التشفير المتقدم (AES) إلى Windows XP Professional مع SP، راجع [تحديث عنصر معلومات خدمات الإمداد اللاسلكي \(WPS IE\) ل Windows XP مع SP2](#).

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](#).

[إعداد Windows Enterprise 2003 باستخدام IIS ومرجع الشهادات و DNS و \(DC_CA\) DHCP](#)

[DC_CA \(تقنية WirelessDemoca\)](#)

DC_CA هو كمبيوتر يعمل بنظام التشغيل Windows Server 2003 المزود بحزمة الخدمة SP1، إصدار Enterprise، ويقوم بأداء الأدوار التالية:

- وحدة التحكم بالمجال للمجال اللاسلكي. local domain الذي يشغل IIS
 - خادم DNS لمجال WirelessDemo.DNS المحلي
 - خادم DHCP
 - المرجع المصدق الجذر للمؤسسة للمجال اللاسلكي. local
- أكمل الخطوات التالية لتكوين DC_CA لهذه الخدمات:

1. [إجراء عملية تثبيت وتهيئة أساسية.](#)
2. [قم بتكوين الكمبيوتر كوحدة تحكم بالمجال.](#)
3. [قم برفع مستوى وظائف المجال.](#)
4. [قم بتثبيت DHCP وتكوينه.](#)
5. [تثبيت خدمات الشهادات.](#)
6. [تحقق من أذونات المسؤول للشهادات.](#)
7. [إضافة أجهزة كمبيوتر إلى المجال.](#)
8. [السماح بالوصول اللاسلكي إلى أجهزة الكمبيوتر.](#)
9. [إضافة مستخدمين إلى المجال.](#)
10. [السماح بالوصول اللاسلكي إلى المستخدمين.](#)
11. [إضافة مجموعات إلى المجال.](#)
12. [إضافة مستخدمين إلى مجموعة WirelessUsers.](#)
13. [إضافة أجهزة كمبيوتر عميلة إلى مجموعة WirelessUsers.](#)

[الخطوة 1: إجراء التثبيت والتكوين الأساسيين](#)

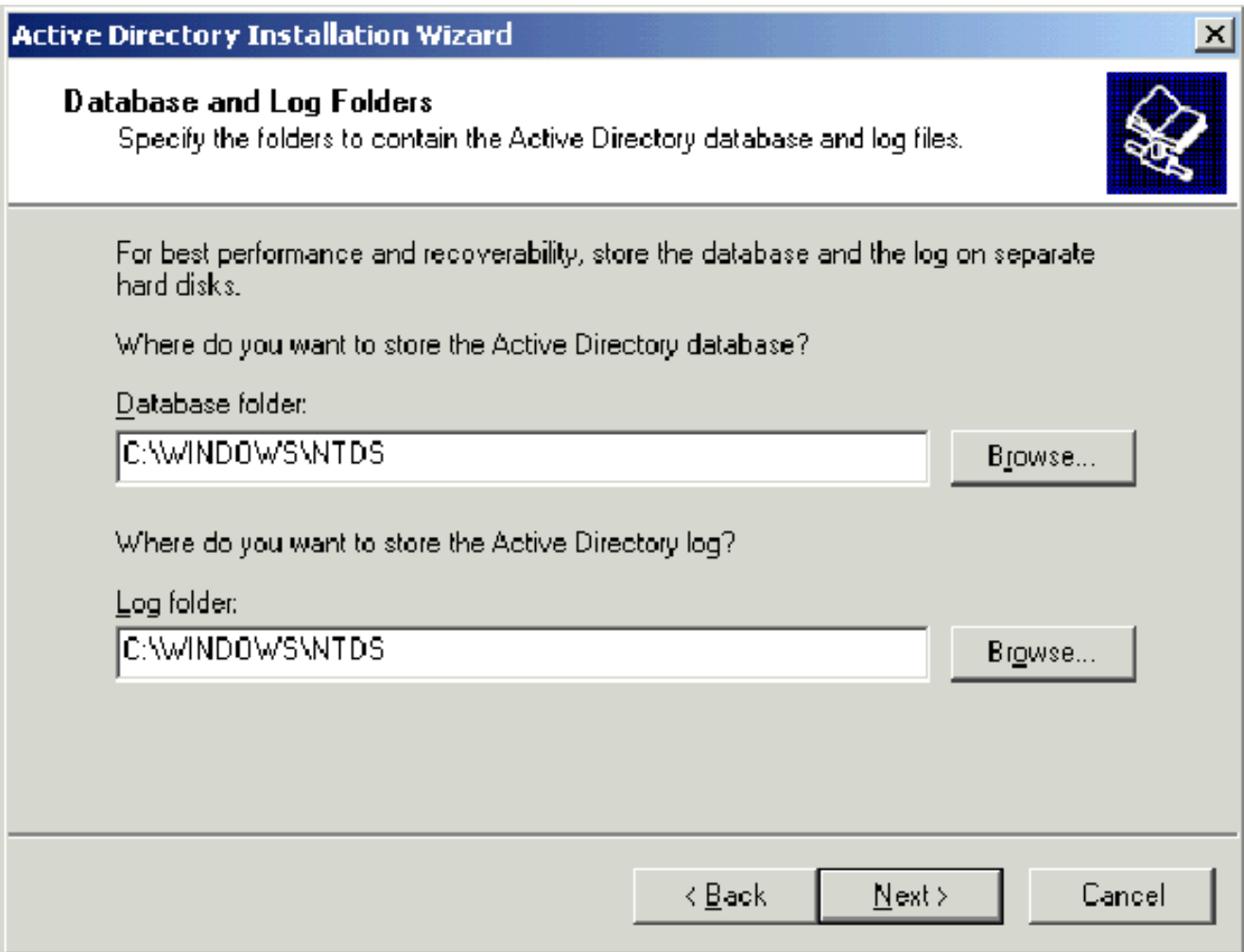
أكمل الخطوات التالية:

1. قم بتثبيت Windows Server 2003 Enterprise Edition باستخدام SP1، كخادم مستقل.
2. قم بتكوين بروتوكول TCP/IP باستخدام عنوان IP الخاص بـ 172.16.100.26 وقناع الشبكة الفرعية 255.255.255.0.

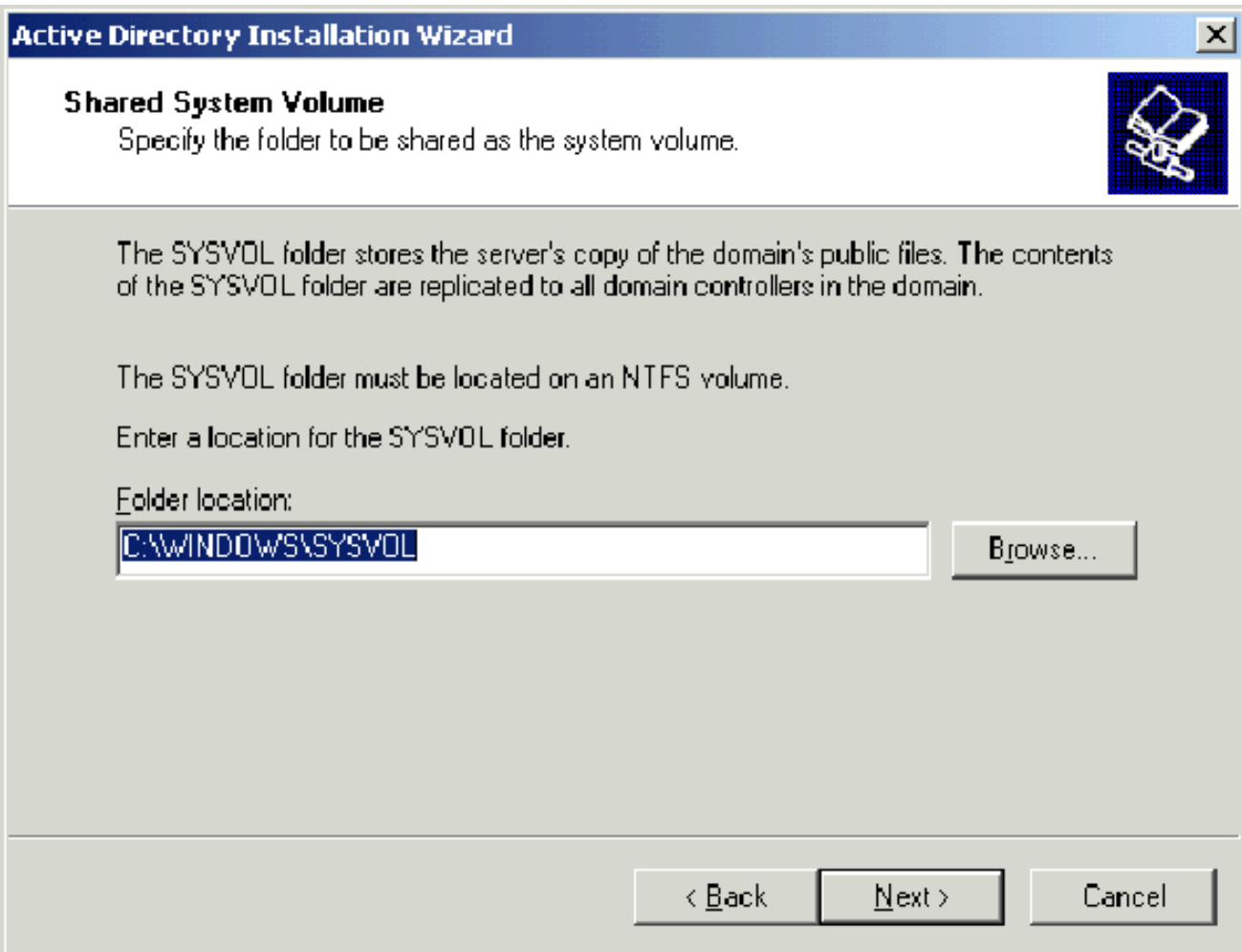
[الخطوة 2: تكوين الكمبيوتر كوحدة تحكم بالمجال](#)

أكمل الخطوات التالية:

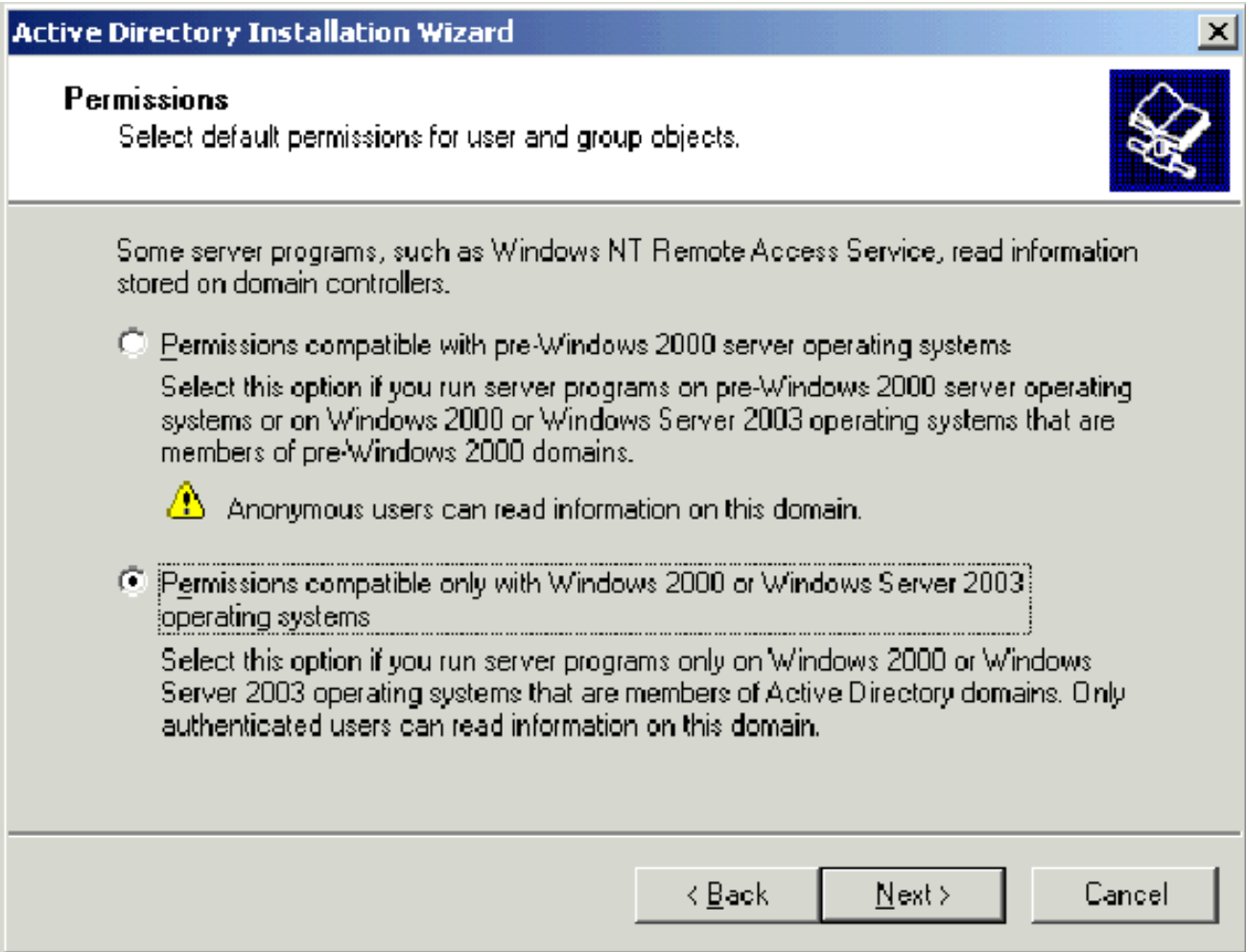
1. لبدء معالج تثبيت Active Directory، أختَر Start (البدء) < Run، واكتب dcpromo.exe، ثم انقر على موافق.
2. في صفحة معالج تثبيت Active Directory، انقر فوق التالي.
3. في صفحة "توافق نظام التشغيل"، انقر فوق التالي.
4. في صفحة "نوع وحدة التحكم بالمجال"، حدد وحدة التحكم بالمجال لمجال جديد وانقر فوق التالي.
5. في صفحة إنشاء مجال جديد، حدد مجال في غابة جديدة وانقر التالي.
6. في صفحة "تثبيت DNS أو تكوينه"، حدد لا، قم فقط بتثبيت DNS وتكوينه على هذا الكمبيوتر وانقر بعد ذلك.
7. في صفحة "اسم المجال الجديد"، اكتب wirelessdemo.local وانقر على التالي.
8. في صفحة اسم مجال NetBIOS، أدخل اسم المجال NetBIOS كاسم لاسلكي وانقر بعد ذلك.
9. في صفحة موقع "مجلدات قاعدة البيانات والسجل"، اقبل الدلائل الافتراضية لمجلدات "قاعدة البيانات" و"السجل" وانقر فوق التالي.



10. في شاشة وحدة تخزين النظام المشتركة، تحقق من صحة موقع المجلد الافتراضي ثم انقر فوق التالي.

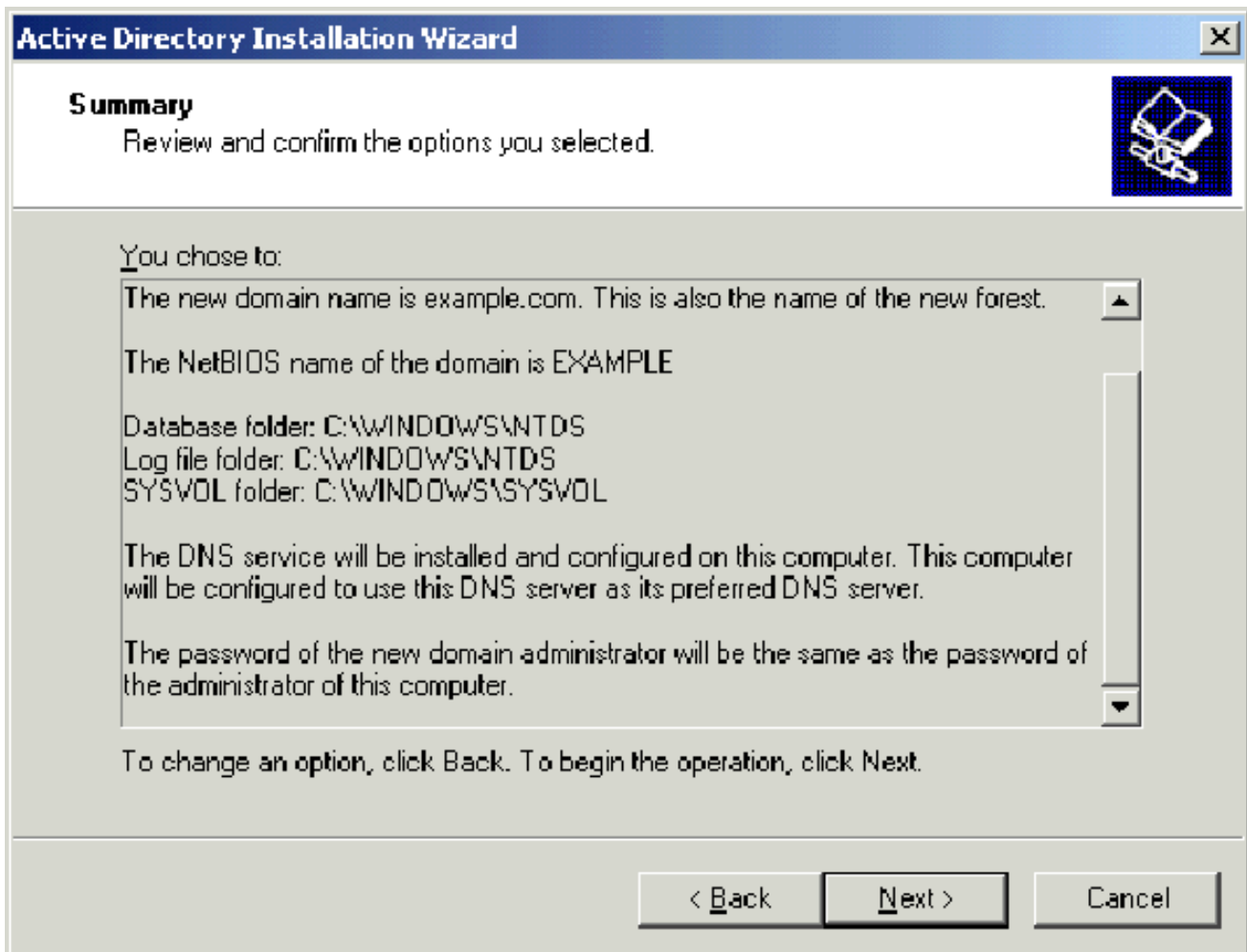


11. في الصفحة أذن، تحقق من تحديد الأذونات المتوافقة فقط مع أنظمة التشغيل Windows 2000 أو Windows Server 2003 وانقر فوق التالي.



12. في صفحة كلمة مرور "إستعادة وضع إدارة خدمات الدليل"، أترك مربعات كلمة المرور فارغة وانقر فوق التالي.

13. راجع المعلومات الموجودة في صفحة الملخص وانقر فوق التالي.

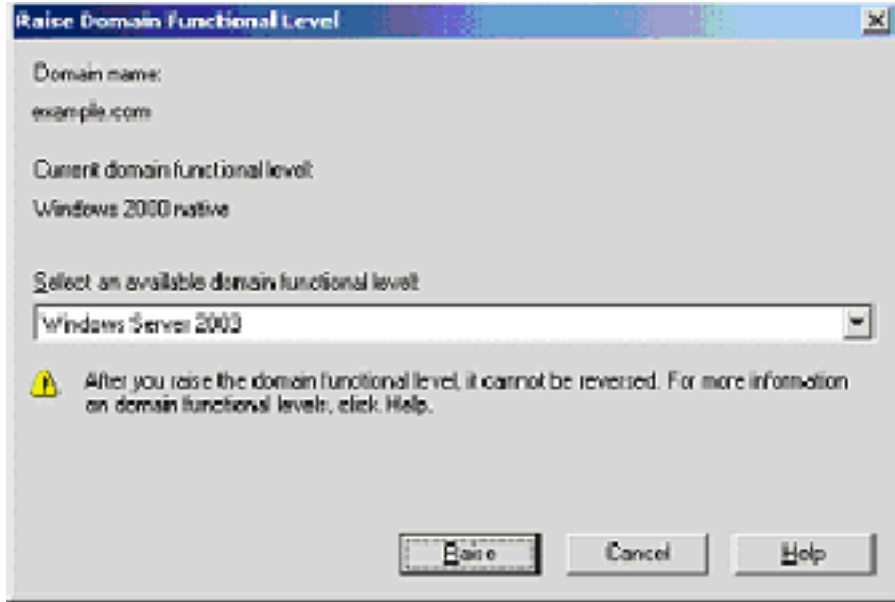


14. في صفحة إكمال معالج تثبيت Active Directory، انقر فوق إنهاء.
15. عند المطالبة بإعادة تشغيل الكمبيوتر، انقر فوق إعادة التشغيل الآن.

[الخطوة 3: رفع المستوى الوظيفي للمجال](#)

أكمل الخطوات التالية:

1. افتح "مجالات Active Directory" واتصل الأدوات الإضافية من مجلد الأدوات الإدارية (ابدأ < أدوات إدارية > مجالات Active Directory والوصايا)، ثم انقر بزر الماوس الأيمن فوق كمبيوتر المجال .dc_CA.wirelessdemo.local
2. انقر فوق رفع المستوى الوظيفي للمجال، ثم حدد Windows Server 2003 في صفحة رفع المستوى



الوظيفي للمجال.

3. انقر فوق رفع، انقر فوق موافق، ثم انقر فوق موافق مرة أخرى.

الخطوة 4: قم بتثبيت DHCP وتكوينه

أكمل الخطوات التالية:

1. قم بتثبيت بروتوكول التكوين الديناميكي للمضيف (DHCP) كمكون خدمة شبكة باستخدام إضافة أو إزالة البرامج في لوحة التحكم.
2. افتح الأداة الإضافية DHCP من مجلد الأدوات الإدارية (ابدأ > برامج > أدوات إدارية > DHCP)، ثم قم بإبراز خادم dc_CA.wirelessdemo.local، DHCP.
3. طقطقت إجراء، وبعد ذلك طقطقت يخلو in order to خولت ال DHCP خدمة.
4. على شجرة وحدة التحكم، انقر بزر الماوس الأيمن فوق dc_ca.wirelessdemo.local، ثم انقر فوق نطاق جديد.
5. في صفحة الترحيب الخاصة بمعالج "النطاق الجديد"، انقر فوق التالي.
6. في صفحة اسم النطاق، اكتب CorpNet في حقل الاسم.

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:

< Back Next > Cancel

7. انقر فوق التالي وقم بتعبئة هذه المعلومات: عنوان Start IP— 172.16.100.1 نهاية عنوان IP— 172.16.100.254 الطول — 24 قناع الشبكة الفرعية - 255.255.255.0

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:

End IP address:

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:

Subnet mask:

< Back

Next >

Cancel

8. طقطقت بعد ذلك وأدخل **172.16.100.1** ل بداية عنوان و **172.16.100.100** ل النهاية عنوان أن يكون استثيت. ثم انقر فوق التالي. يحجز هذا العنوان في النطاق من **172.16.100.1** إلى **172.16.100.100**. لم يتم تخصيص عناوين IP المحجوزة هذه من قبل خادم DHCP.

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:

Excluded address range:

9. في صفحة مدة التأجير، انقر فوق التالي.
10. اخترت على ال DHCP configure خيار، نعم، أنا أريد أن يشكل هذا 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

11. في صفحة الموجه (البوابة الافتراضية) أضف عنوان الموجه الافتراضي 172.16.100.1 وانقر على التالي.

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:

12. في صفحة اسم المجال وخوادم DNS، اكتب **wirelessdemo.local** في حقل المجال الرئيسي، اكتب **172.16.100.26** في حقل عنوان IP، ثم انقر فوق إضافة وانقر فوق التالي.

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:

Resolve

IP address:

172.16.100.26

Add

Remove

Up

Down

< Back

Next >

Cancel

13. في الصفحة خوادم WINS، انقر فوق التالي.
14. في صفحة "تنشيط النطاق"، اختر نعم، أريد تنشيط هذا 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

15. في صفحة "معالج إكمال نطاق جديد"، انقر فوق إنهاء.

الخطوة 5: تثبيت خدمات الشهادات

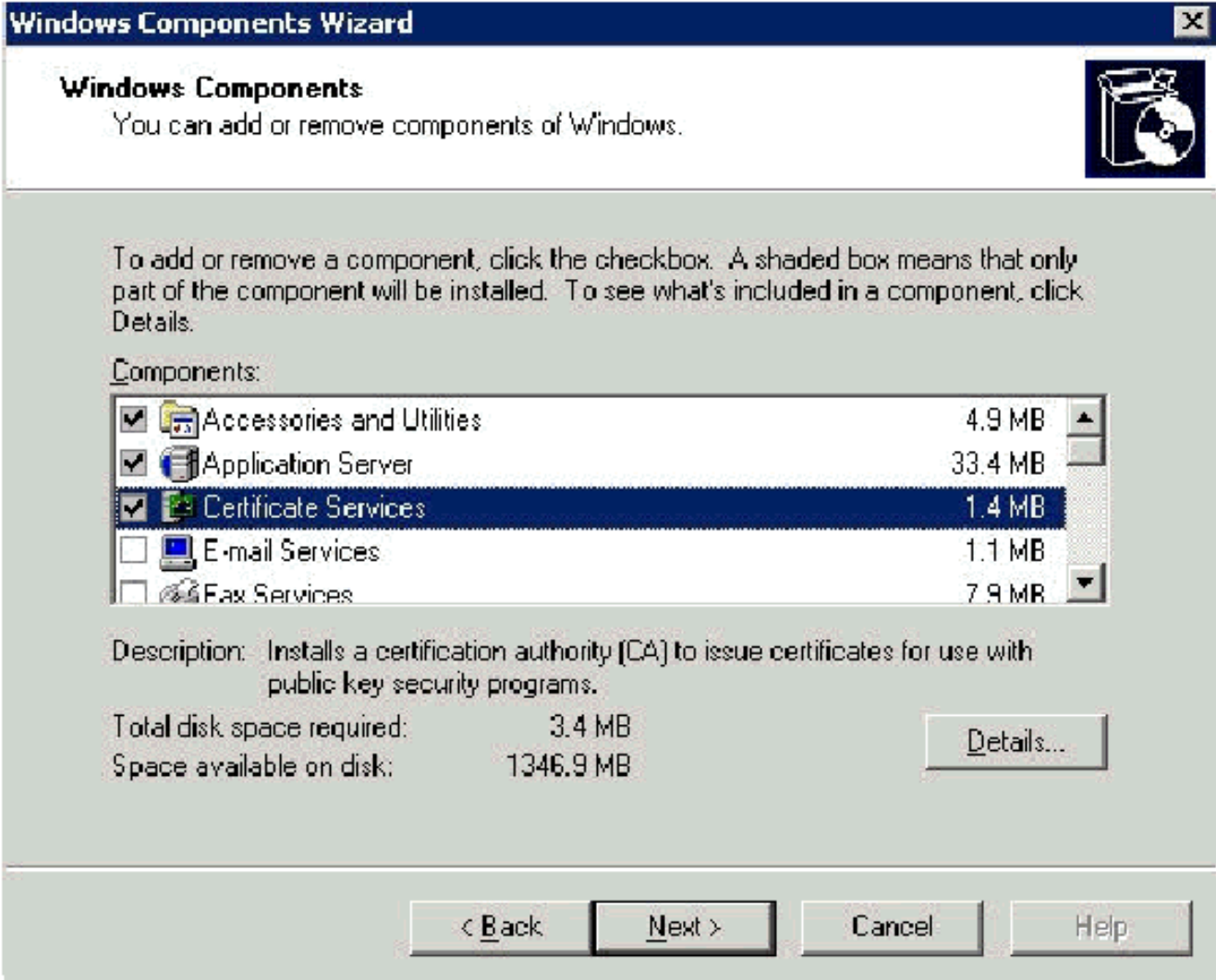
أكمل الخطوات التالية:

ملاحظة: يجب تثبيت IIS قبل تثبيت "خدمات الشهادات" ويجب أن يكون المستخدم جزءاً من "إدارة المؤسسة".

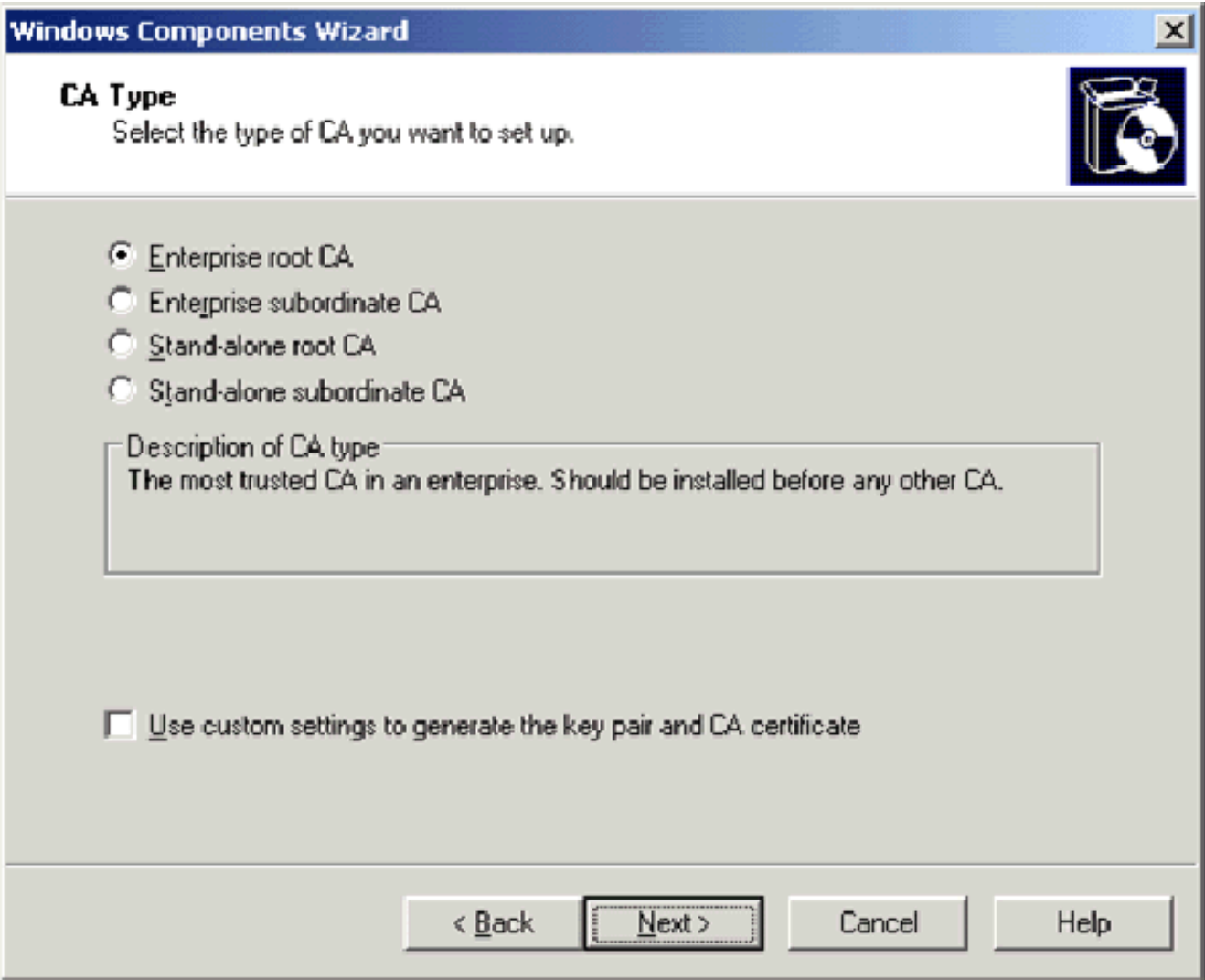
1. في لوحة التحكم، افتح إضافة أو إزالة برامج، ثم انقر فوق إضافة/إزالة مكونات Windows.

2. في صفحة معالج مكونات Windows، اختر خدمات الشهادات، ثم انقر فوق

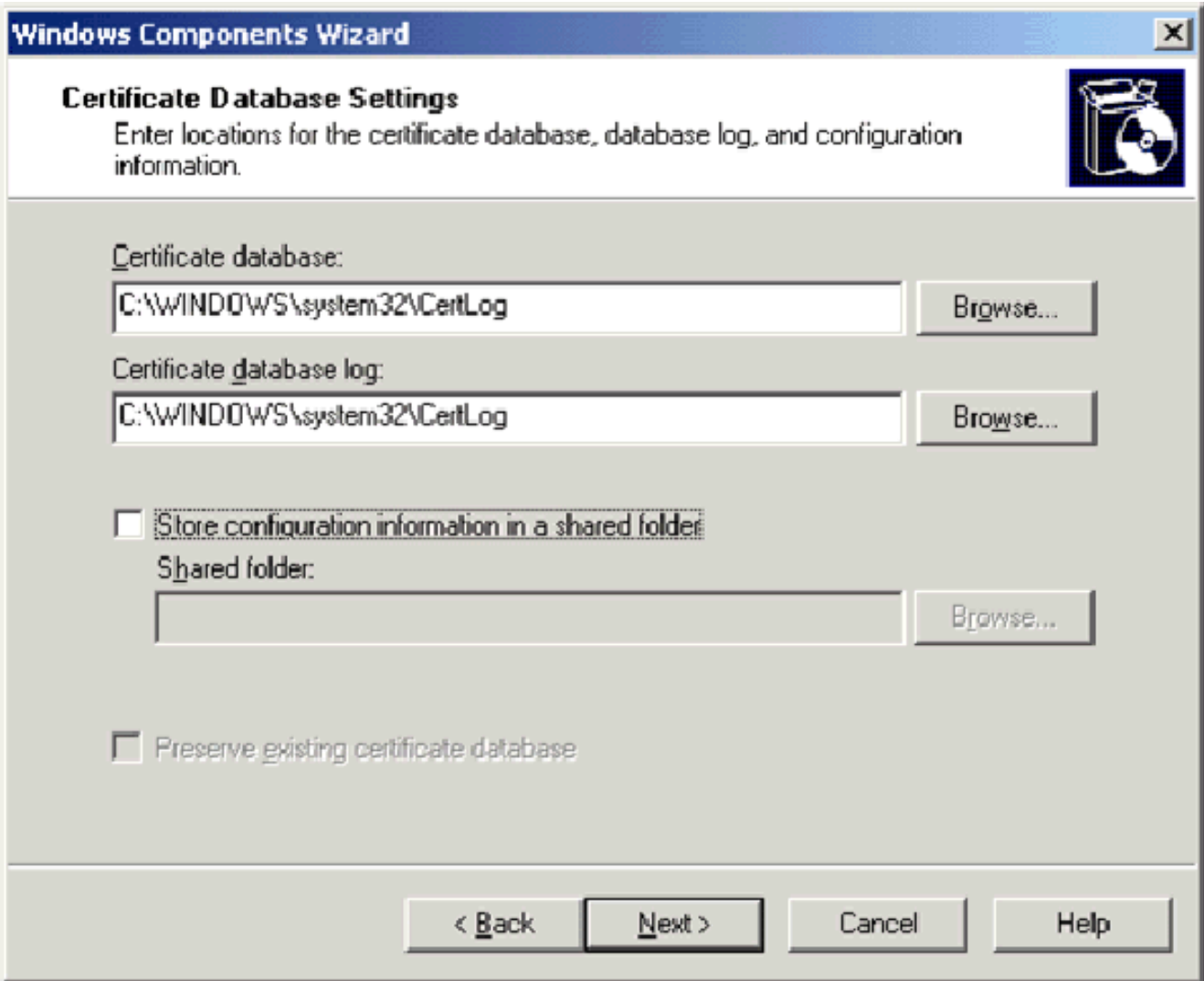
التالي.



3. في صفحة نوع المرجع المصدق، أختار المرجع المصدق الجذر للمؤسسة وانقر بعد ذلك.



4. في صفحة معلومات تعريف CA، اكتب **wirelessdemoca** في الاسم العام لمربع CA هذا. يمكنك إدخال التفاصيل الاختيارية الأخرى ثم انقر فوق التالي. قبول الافتراضيات على صفحة إعدادات قاعدة بيانات الشهادات.

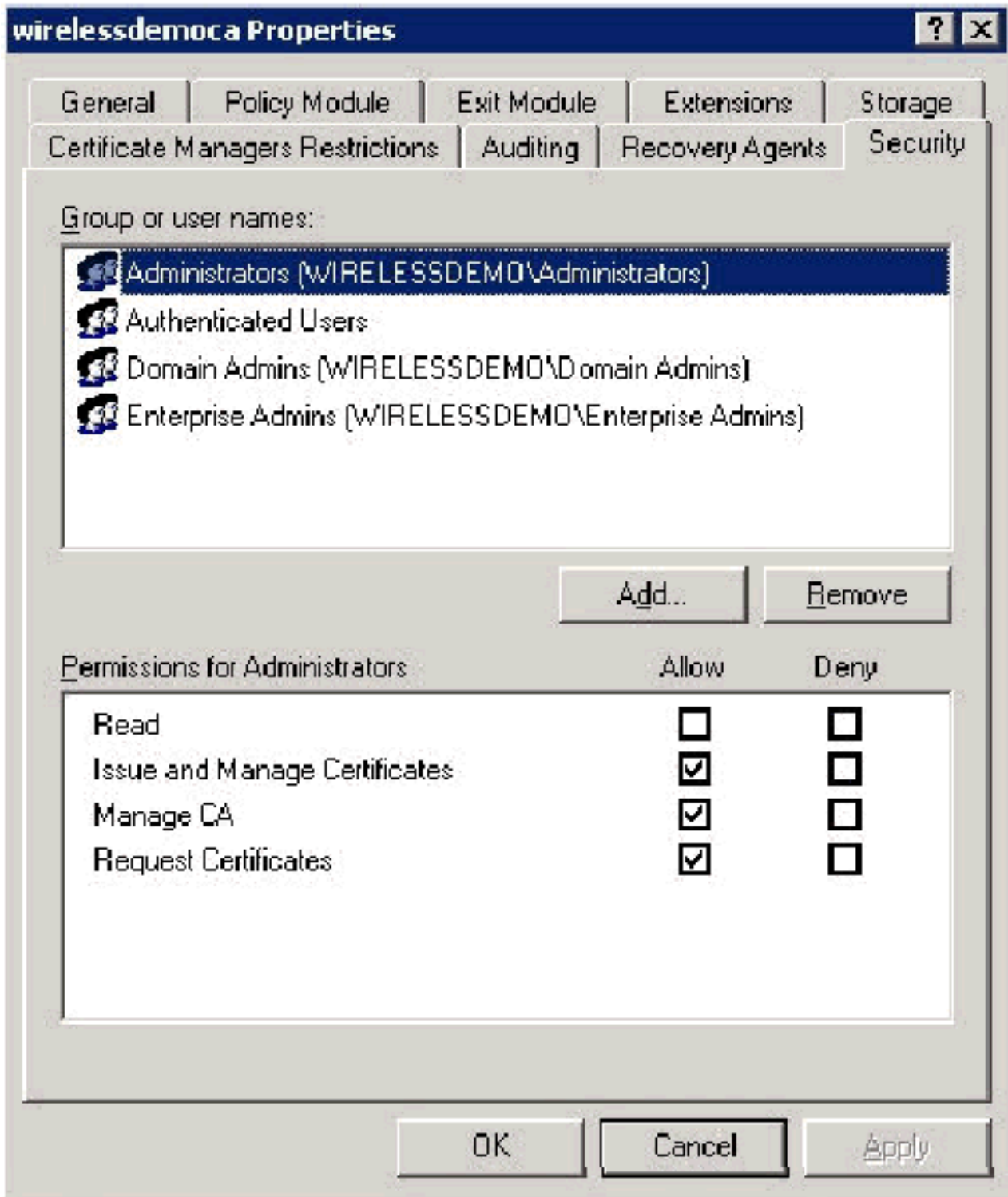


5. انقر فوق **Next** (التالي). بعد اكتمال التثبيت، انقر فوق **إنهاء**.
6. انقر فوق **موافق** بعد قراءة التحذير حول تثبيت IIS.

[الخطوة 6: التحقق من أذونات المسؤول للشهادات](#)

أكمل الخطوات التالية:

1. اختر **ابدأ < أدوات إدارية > المرجع المصدق**.
2. انقر بزر الماوس الأيمن فوق **WirelessDemoca CA** ثم انقر فوق **خصائص**.
3. في علامة التبويب "الأمان"، انقر فوق **Administrators** في قائمة "المجموعة" أو أسماء المستخدمين.
4. في قائمة الأذون أو المسؤولين، تحقق من تعيين هذه الخيارات على **السماح**: إصدار الشهادات وإدارتها لإدارة CA طلب الشهادات إذا تم تعيين أي من هذه إلى رفض أو لم يتم تحديده، قم بتعيين الإذن **للسماح**.



5. انقر فوق موافق لإغلاق مربع حوار خصائص المرجع المصدق اللاسلكي، ثم قم بإغلاق مرجع التصديق.

[الخطوة 7: إضافة أجهزة كمبيوتر إلى المجال](#)

أكمل الخطوات التالية:

ملاحظة: إذا كان الكمبيوتر قد تمت إضافته بالفعل إلى المجال، فقم بالمتابعة [لإضافة مستخدمين إلى المجال](#).

1. فتح الأداة الإضافية "مستخدمو Active Directory وأجهزة الكمبيوتر".
2. في شجرة وحدة التحكم، قم بتوسيع WirelessDemo.local.
3. انقر بزر الماوس الأيمن فوق المستخدمين، ثم انقر فوق جديد، ثم انقر فوق الكمبيوتر.
4. في شاشة كائن جديد - كمبيوتر، اكتب اسم الكمبيوتر في حقل اسم الكمبيوتر وانقر التالي. يستخدم هذا المثال عميل اسم

New Object - Computer

Create in: wirelessdemo.local/Users

Computer name:
Client

Computer name (pre-Windows 2000):
CLIENT

The following user or group can join this computer to a domain.
User or group:
Default: Domain Admins Change...

Assign this computer account as a pre-Windows 2000 computer
 Assign this computer account as a backup domain controller

< Back Next > Cancel

5. في شاشة الإدارة، انقر التالي.
6. في شاشة كائن-كمبيوتر جديد، انقر إنهاء.
7. كرر الخطوات من 3 إلى 6 لإنشاء حسابات كمبيوتر إضافية.

[الخطوة 8: السماح بالوصول اللاسلكي إلى أجهزة الكمبيوتر](#)

أكمل الخطوات التالية:

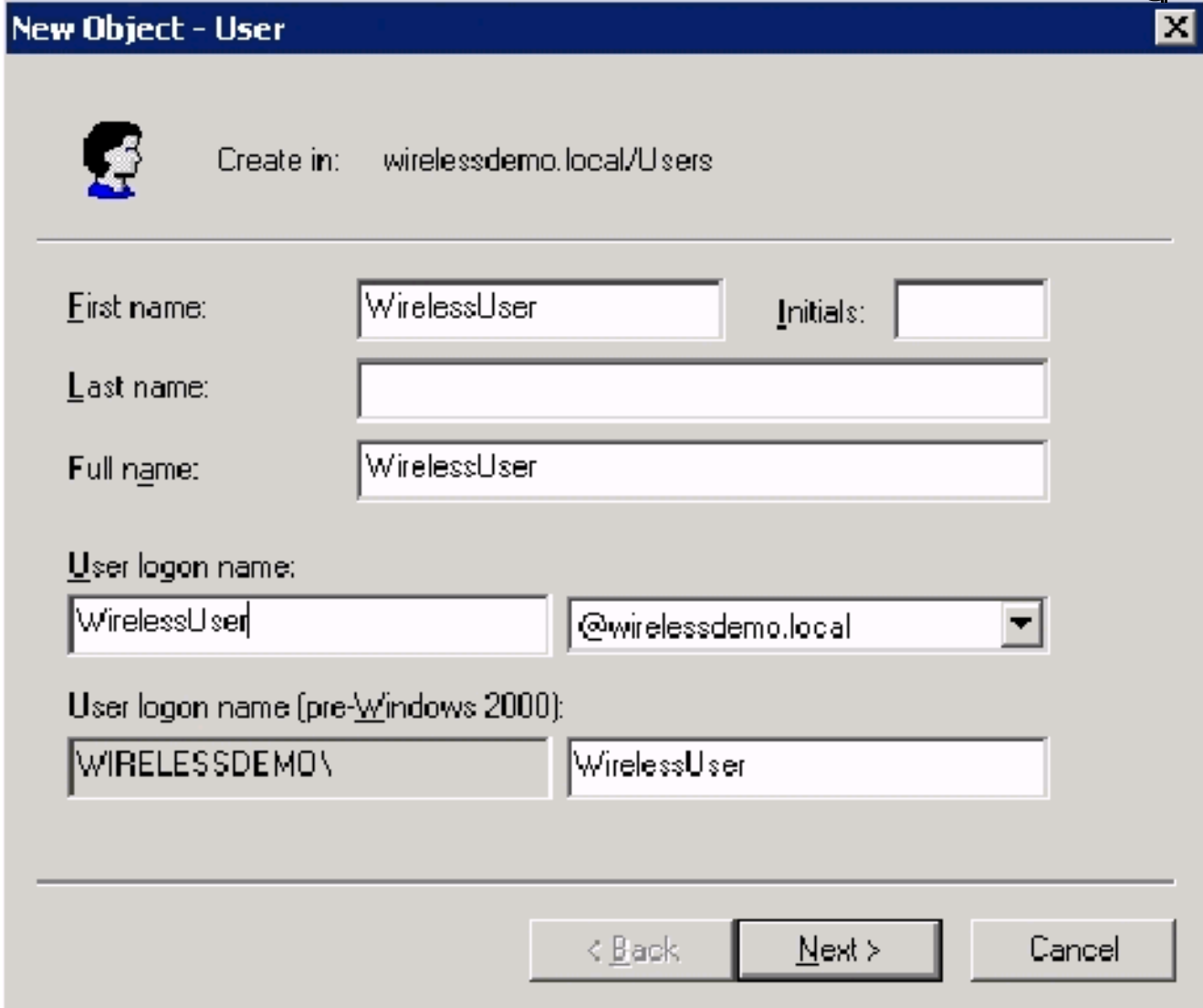
1. في شجرة وحدة تحكم مستخدمي Active Directory وأجهزة الكمبيوتر، انقر فوق المجلد أجهزة الكمبيوتر وانقر بزر الماوس الأيمن فوق الكمبيوتر الذي تريد تعيين وصول لاسلكي له. يوضح هذا المثال الإجراء مع عميل الكمبيوتر الذي أضفته في الخطوة 7.
2. انقر فوق خصائص، ثم انتقل إلى علامة التبويب "الطلب الهاتفي".
3. اخترت يسمح منفذ وطققة ok.

[الخطوة 9: إضافة مستخدمين إلى المجال](#)

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 مربع الحوار كائن جديد - مستخدم، اكتب WirelessUser في حقل الاسم الأول، واكتب WirelessUser في حقل اسم تسجيل دخول المستخدم وانقر فوق التالي.



New Object - User

Create in: wirelessdemo.local/Users

First name: WirelessUser Initials:

Last name:

Full name: WirelessUser

User logon name: WirelessUser @wirelessdemo.local

User logon name (pre-Windows 2000): WIRELESSDEMO\WirelessUser

< Back Next > Cancel

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 التالي لتسجيل الدخول، ثم انقر فوق التالي.



Create in: wirelessdemo.local/Users

Password:

•••••

Confirm password:

•••••

- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

< Back

Next >

Cancel

4. في شاشة كائن جديد - مستخدم، انقر إنهاء.
5. كرر الخطوات من 2 إلى 4 لإنشاء حسابات مستخدمين إضافية.

[الخطوة 10: السماح بالوصول اللاسلكي إلى المستخدمين](#)

أكمل الخطوات التالية:


1. في شجرة وحدة تحكم مستخدمي Active Directory وأجهزة الكمبيوتر، انقر فوق المجلد **Users**، وانقر بزر الماوس الأيمن فوق **WirelessUser**، ثم انقر فوق **خصائص**، ثم انتقل إلى علامة التبويب **Dial-in**.
2. أخترت **يسمح منفذ وطققة ok**.

[الخطوة 11: إضافة مجموعات إلى المجال](#)

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 **مجموعة**.
2. في شاشة كائن جديد - مجموعة، اكتب اسم المجموعة في حقل اسم المجموعة وانقر **موافق**. يستخدم هذا المستند اسم المجموعة **WirelessUsers**.

New Object - Group [X]

 Create in: wirelessdemo.local/Users

Group name:

Group name (pre-Windows 2000):

Group scope:

- Domain local
- Global
- Universal

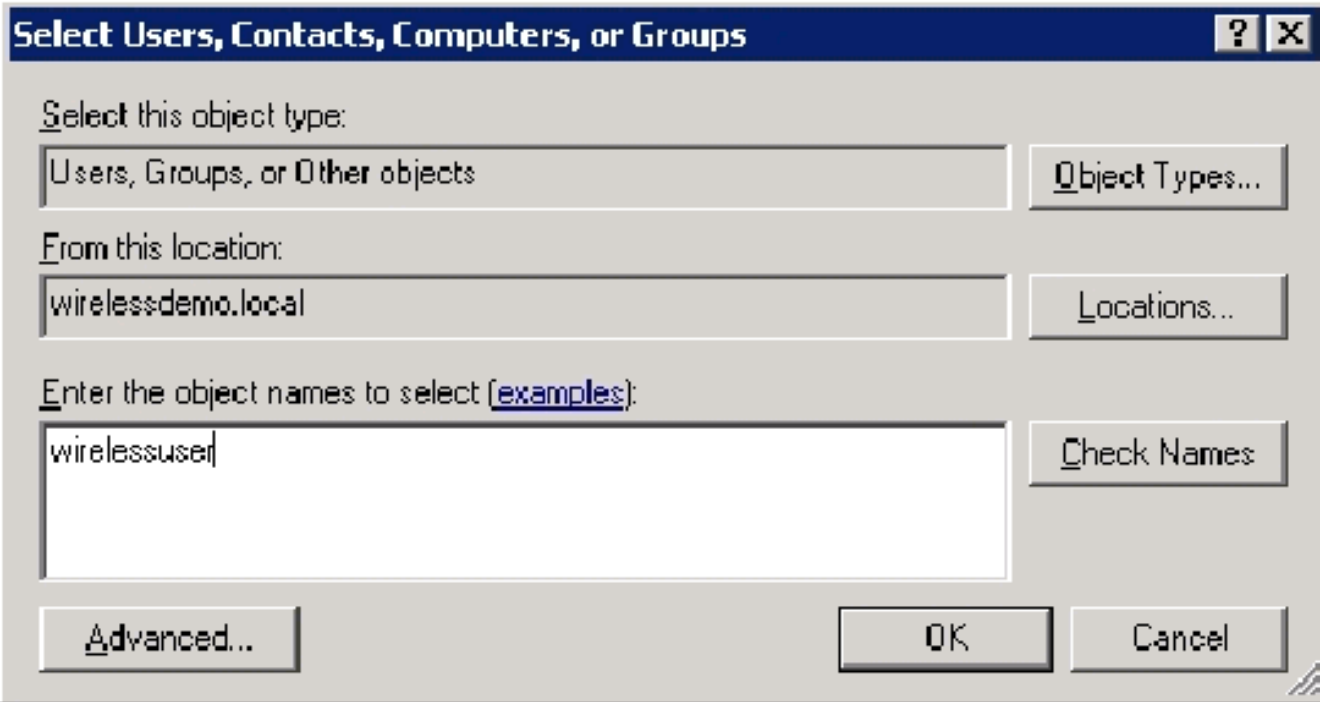
Group type:

- Security
- Distribution

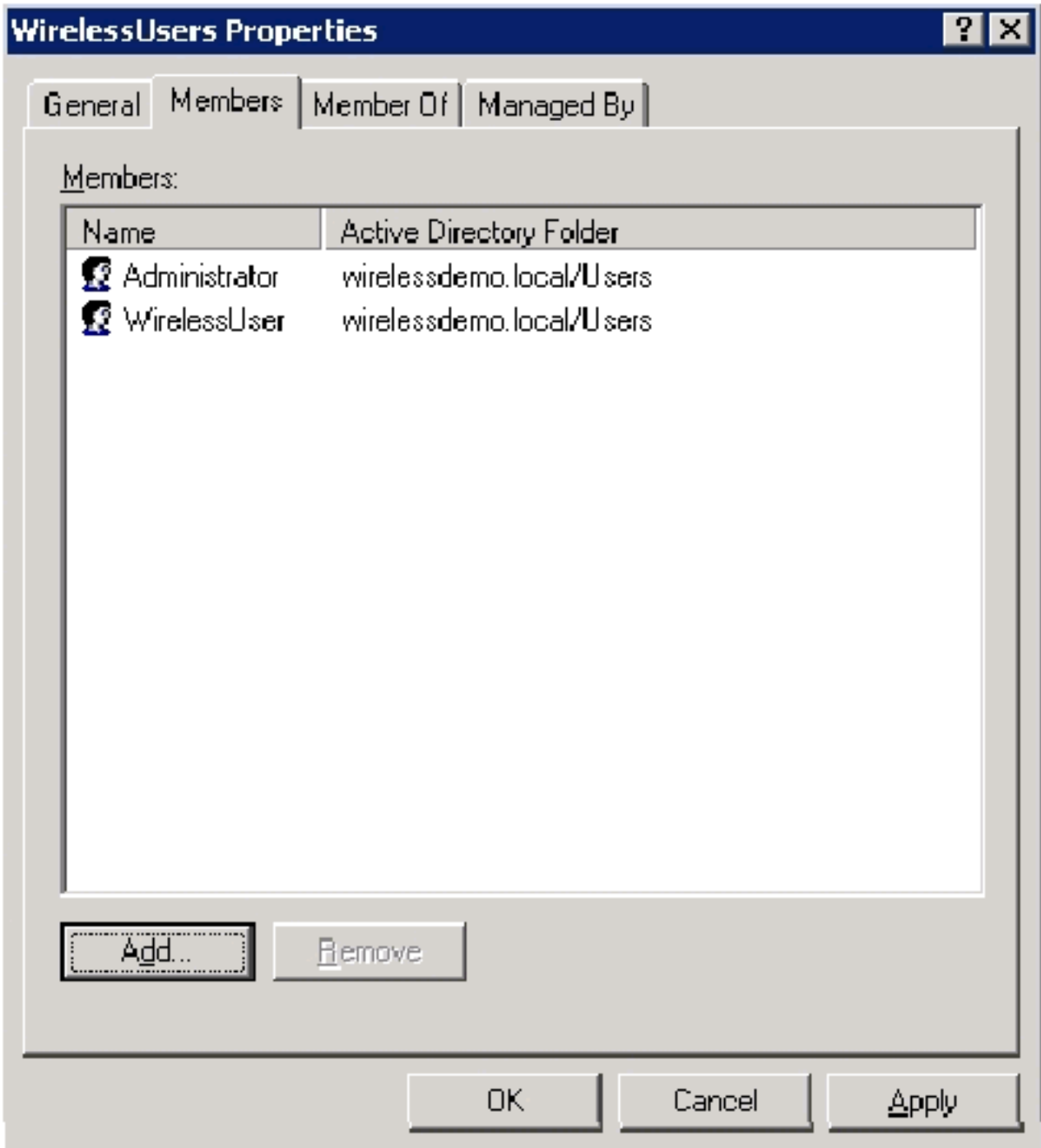
[الخطوة 12: إضافة مستخدمين إلى مجموعة WirelessUsers](#)

أكمل الخطوات التالية:

1. في جزء التفاصيل الخاص بـ Active Directory Users and Computers، انقر نقرًا مزدوجًا فوق Group WirelessUsers.
2. انتقل إلى علامة التبويب "أعضاء" وانقر فوق إضافة.
3. في شاشة تحديد مستخدمين، جهات اتصال، أجهزة كمبيوتر، أو مجموعات، اكتب اسم المستخدمين الذين تريد إضافتهم إلى المجموعة. يوضح هذا المثال كيفية إضافة المستخدم اللاسلكي إلى المجموعة. وانقر فوق OK.



4. في شاشة الأسماء المتعددة التي تم العثور عليها، انقر موافق. تتم إضافة حساب مستخدم WirelessUser إلى مجموعة WirelessUsers.

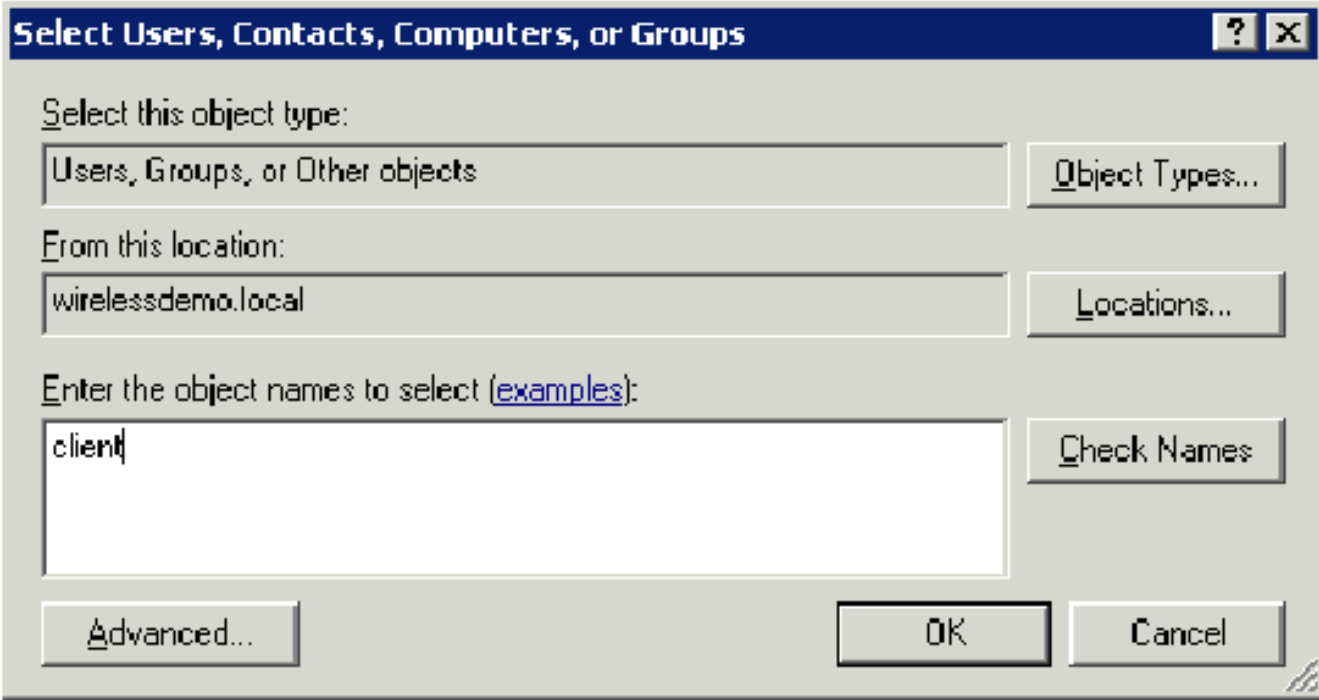


5. انقر على **موافق** لحفظ التغييرات في مجموعة WirelessUsers.
6. كرر هذا الإجراء لإضافة المزيد من المستخدمين إلى المجموعة.

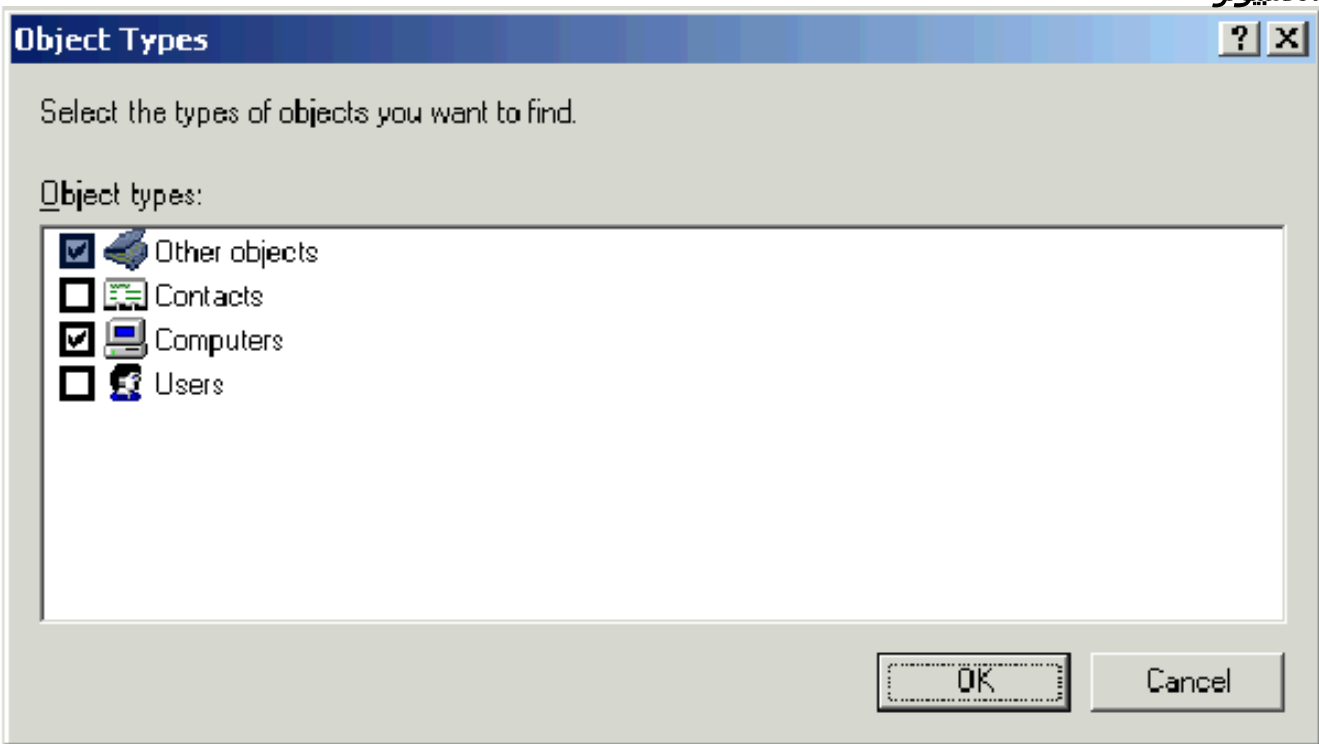
[الخطوة 13: إضافة أجهزة كمبيوتر عميلة إلى مجموعة WirelessUsers](#)

أكمل الخطوات التالية:

1. كرر الخطوات 1 و 2 في قسم [إضافة مستخدمين إلى مجموعة WirelessUsers](#) في هذا المستند
2. في شاشة تحديد المستخدمين أو جهات الاتصال أو أجهزة الكمبيوتر، اكتب اسم الكمبيوتر الذي تريد إضافته إلى المجموعة. يوضح هذا المثال كيفية إضافة الكمبيوتر المسمى **عميل** إلى المجموعة.



3. انقر فوق أنواع الكائن، وقم بإلغاء تحديد خانة الاختيار المستخدمين، ثم حدد أجهزة الكمبيوتر.



4. طقطقت ok مرتين. تتم إضافة حساب الكمبيوتر العميل إلى مجموعة WirelessUsers.
5. كرر الإجراء لإضافة المزيد من أجهزة الكمبيوتر إلى المجموعة.

[إعداد Windows Standard 2003 مع Cisco Secure ACS 4.0](#)

Cisco Secure ACS هو كمبيوتر يعمل بنظام التشغيل Windows Server 2003 المزود بحزمة الخدمة SP1، الإصدار Standard Edition، الذي يوفر مصادقة RADIUS والتحويل لوحدة التحكم. أتمت الإجراء في هذا قسم in order to شكلت ACS ك RADIUS نادل:

[الثبت والتكوين الأساسيان](#)

أكمل الخطوات التالية:

1. قم بتثبيت Windows Server 2003 Standard Edition باستخدام SP1، كخادم **عضو** يسمى **ACS** في مجال **wirelessdemo.local**. ملاحظة: يظهر اسم خادم ACS على هيئة **cisco_w2003** في التكوينات المتبقية. إستبدال ACS أو **Cisco_w2003** على إعداد المختبر المتبقي.
2. بالنسبة لاتصال المنطقة المحلية، قم بتكوين بروتوكول TCP/IP باستخدام عنوان **IP 172.16.100.26**، وقناع الشبكة الفرعية **255.255.255.0**، وعنوان IP لخادم DNS ل **127.0.0.1**.

تثبيت Cisco Secure ACS 4.0

ملاحظة: راجع [دليل التثبيت ل Cisco Secure ACS 4.0 ل Windows](#) للحصول على مزيد من المعلومات حول كيفية تكوين ACS 4.0 الآمن من Windows ل Cisco.

أكمل الخطوات التالية:

1. باستخدام حساب مسؤول مجال، قم بتسجيل الدخول إلى الكمبيوتر المسمى ACS إلى ACS الآمن من Cisco. **ملاحظة:** يتم دعم عمليات التثبيت التي يتم تنفيذها على الكمبيوتر حيث تقوم بتثبيت ACS الآمن من Cisco. لا يتم اختبار التثبيت البعيدة التي يتم تنفيذها باستخدام خدمات أو منتجات Windows الطرفية مثل حوسبة الشبكة الظاهرية (VNC) ولا يتم دعمها.
2. أدخل القرص المضغوط ل Cisco Secure ACS في محرك أقراص مضغوطة على الكمبيوتر.
3. إذا كان محرك الأقراص المضغوطة يدعم ميزة التشغيل التلقائي ل Windows، يظهر مربع الحوار "مصدر المحتوى الإضافي الآمن من Cisco ل Windows Server". **ملاحظة:** في حالة عدم تثبيت حزمة الخدمة المطلوبة على الكمبيوتر، يظهر مربع حوار. يمكن تطبيق حزم خدمة Windows قبل تثبيت Cisco Secure ACS أو بعد تثبيته. يمكنك متابعة التثبيت، ولكن يجب تطبيق حزمة الخدمة المطلوبة بعد اكتمال التثبيت. وإلا، قد لا يعمل مصدر المحتوى الإضافي الآمن من Cisco بشكل موثوق.
4. قم بتنفيذ واحدة من هذه المهام: إذا ظهر مربع الحوار "مصدر المحتوى الإضافي الآمن من Cisco" ل Windows Server، فانقر على **تثبيت**. إذا لم يظهر مربع الحوار "مصدر المحتوى الإضافي الآمن من Cisco" ل Windows Server، فقم بتشغيل **setup.exe**، الموجود في الدليل الجذر لقرص ACS الآمن من Cisco.
5. يعرض مربع الحوار "إعداد ACS الآمن من Cisco" إتفاقية ترخيص البرامج.
6. اقرأ إتفاقية ترخيص البرامج. إذا قمت بقبول إتفاقية ترخيص البرامج، فانقر فوق **قبول**. تعرض شاشة الترحيب المعلومات الأساسية حول برنامج الإعداد.
7. بعد قراءة المعلومات في شاشة الترحيب، انقر **التالي**.
8. تسرد شاشة قبل البدء العناصر التي يجب عليك إكمالها قبل متابعة التثبيت. إذا قمت بإكمال كل العناصر المسرودة في شاشة قبل البدء، حدد المربع المقابل لكل عنصر وانقر **التالي**. **ملاحظة:** إذا لم تكن قد أكملت كافة العناصر المدرجة في المربع قبل البدء، انقر فوق **إلغاء الأمر** ثم انقر فوق **إنهاء الإعداد**. بعد أن تقوم بإكمال كل العناصر المدرجة في شاشة قبل البدء، قم بإعادة تشغيل التثبيت.
9. سوف يظهر مربع الحوار إختيار موقع الوجهة. تحت مجلد الوجهة، يظهر موقع التثبيت. هذا هو محرك الأقراص والمسار حيث يقوم برنامج الإعداد بتثبيت ACS الآمن من Cisco.
10. إذا أردت تغيير موقع التثبيت، أكمل الخطوات التالية: انقر على **إستعراض**. سوف يظهر مربع الحوار إختيار مجلد. يحتوي مربع المسار على موقع التثبيت. تغيير موقع التثبيت. يمكنك إما كتابة الموقع الجديد في مربع المسار أو إستخدام قوائم محركات الأقراص والدلائل لتحديد محرك أقراص ودليل جديدين. يجب أن يكون موقع التثبيت على محرك أقراص محلي للكمبيوتر. **ملاحظة:** لا تقم بتحديد مسار يحتوي على حرف نسبة مئوية، "%". إذا قمت بذلك، قد يظهر التثبيت للمتابعة بشكل صحيح لكنه يفشل قبل اكتماله. وانقر فوق **OK**. **ملاحظة:** إذا قمت بتحديد مجلد غير موجود، فإن برنامج الإعداد يعرض مربع حوار لتأكيد إنشاء المجلد. للمتابعة، انقر فوق **نعم**.
11. في شاشة إختيار موقع الوجهة، يظهر موقع التثبيت الجديد تحت مجلد الوجهة.
12. انقر فوق **Next (التالي)**.
13. يسرد مربع حوار تكوين قاعدة بيانات المصادقة خيارات مصادقة المستخدمين. يمكنك المصادقة مع قاعدة بيانات المستخدم الآمن من Cisco فقط، أو أيضا مع قاعدة بيانات مستخدم Windows. **ملاحظة:** بعد تثبيت

- Cisco Secure ACS، يمكنك تكوين دعم المصادقة لجميع أنواع قواعد بيانات المستخدم الخارجي بالإضافة إلى قواعد بيانات مستخدمي Windows.
14. إن يريد أنت أن يصادق مستعمل مع ال Cisco يأمن قاعدة معطيات فقط، يختار ال Cisco يأمن قاعدة معطيات خيار فقط.
15. إذا كنت ترغب في مصادقة المستخدمين باستخدام قاعدة بيانات مستخدم "إدارة الوصول إلى الأمان ل (SAM) Windows) أو قاعدة بيانات مستخدم Active Directory بالإضافة إلى قاعدة بيانات المستخدم الآمنة من Cisco، أكمل الخطوات التالية: اخترت أيضا فحصت ال Windows مستعمل قاعدة معطيات خيار يصبح خانة الاختيار نعم، ارجع إلى خانة الاختيار منح إذن الطلب للمستخدم" متوفرة. ملاحظة: ينطبق خانة الاختيار نعم، ارجع إلى خانة الاختيار "منح إذن للمستخدم من خلال الطلب" على جميع أشكال الوصول التي يتم التحكم فيها بواسطة ACS الآمن من Cisco، وليس فقط الوصول إلى الطلب الهاتفي. على سبيل المثال، لا يتصل المستخدم الذي يصل إلى الشبكة من خلال نفق VPN بخادم وصول إلى الشبكة. ومع ذلك، إذا تم تحديد نعم، ارجع إلى مربع الإعداد منح إذن إلى المستخدم"، فإن مصدر المحتوى الإضافي الآمن من Cisco يطبق أذونات طلب اتصال مستخدم Windows لتحديد ما إذا كان سيتم منح المستخدم حق الوصول إلى الشبكة أم لا. إذا كنت ترغب في السماح بالوصول إلى المستخدمين الذين تمت مصادقتهم بواسطة قاعدة بيانات مستخدم مجال Windows فقط عندما يكون لديهم إذن الطلب الهاتفي في في حساب Windows الخاص بهم، فتتحقق من نعم، ارجع إلى مربع إعداد "منح إذن الطلب إلى المستخدم".
16. انقر فوق Next (التالي).
17. يقوم برنامج الإعداد بتثبيت ACS الآمن من Cisco وتحديث سجل Windows.
18. تسرد شاشة الخيارات المتقدمة العديد من ميزات Cisco Secure ACS التي لا يتم تمكينها بشكل افتراضي. لمزيد من المعلومات حول هذه الميزات، ارجع إلى [دليل المستخدم ل Cisco Secure ACS ل Windows Server](#)، الإصدار 4.0. ملاحظة: تظهر الميزات المدرجة في واجهة HTML الآمنة من Cisco فقط إذا قمت بتمكينها. بعد التثبيت، يمكنك تمكينها أو تعطيلها في صفحة الخيارات المتقدمة في قسم تكوين الواجهة.
19. لكل ميزة تريد تمكينها، حدد المربع المرادف.
20. انقر فوق Next (التالي).
21. يظهر مربع الحوار "مراقبة الخدمة النشطة". ملاحظة: بعد التثبيت، يمكنك تكوين ميزات مراقبة الخدمة النشطة على صفحة إدارة الخدمة النشطة في قسم تكوين النظام.
22. إذا كنت تريد من Cisco تأمين ACS أن يراقب خدمات مصادقة المستخدم، حدد مربع تمكين مراقبة تسجيل الدخول. من قائمة البرنامج النصي إلى التنفيذ، اختر الخيار الذي تريد تطبيقه في حالة فشل خدمة المصادقة: لا يوجد إجراء علاجي—لا يشغل ACS الآمن من Cisco برنامج نصي. ملاحظة: يكون هذا الخيار مفيدا إذا قمت بتمكين إعلانات بريد الحدث. Cisco reboot—reboot يأمن ACS يركض نص تنفيذي أن يركض الكومبيوتر أن يركض Cisco يأمن ACS إعادة تشغيل الكل—يعيد Cisco Secure ACS تشغيل جميع خدمات Cisco Secure ACS إعادة تشغيل RADIUS/TACACS+—يعيد ACS الآمن من Cisco تشغيل خدمات RADIUS و TACACS+ فقط.
23. إذا كنت تريد من Cisco Secure ACS أن يرسل رسالة بريد إلكتروني عند اكتشاف مراقبة الخدمة لحدث، فتتحقق من مربع إعلام البريد.
24. انقر فوق Next (التالي).
25. يظهر مربع الحوار تشفير كلمة مرور قاعدة البيانات. ملاحظة: يتم تشفير كلمة مرور تشفير قاعدة البيانات وتخزينها في سجل ACS. قد تحتاج إلى إعادة استخدام كلمة المرور هذه عند ظهور مشاكل خطيرة وضرورة الوصول إلى قاعدة البيانات يدويا. احتفظ بكلمة المرور هذه في المتناول حتى يتمكن الدعم الفني من الوصول إلى قاعدة البيانات. يمكن تغيير كلمة المرور كل فترة انتهاء صلاحية.
26. أدخل كلمة مرور لتشغيل قاعدة البيانات. يجب أن يكون طول كلمة المرور ثمانية أحرف على الأقل ويجب أن تحتوي على كل من الأحرف والأرقام. لا توجد أحرف غير صحيحة. انقر فوق Next (التالي).
27. ينتهي برنامج الإعداد وتظهر مربع الحوار "بدء خدمة ACS الآمنة من Cisco".
28. لكل خيار بدء خدمات ACS الآمنة من Cisco الذي تريده، حدد المربع المقابل. تحدث الإجراءات المرتبطة بالخيارات بعد انتهاء برنامج الإعداد. نعم، أريد بدء تشغيل خدمة ACS الآمنة من Cisco الآن—تبدأ خدمات Windows التي تشكل ACS الآمن من Cisco. إن لا ينتقى أنت هذا خيار، ال Cisco يأمن HTML acs قارن لا يتوفر ما لم أنت reboot الكومبيوتر أو يبدأ ال CSAdmin خدمة. نعم، أريد من برنامج الإعداد تشغيل مسؤول ACS الآمن من Cisco من المستعرض الخاص بي بعد التثبيت—يفتح واجهة HTML ل Cisco ACS الآمنة

- في مستعرض الويب الافتراضي لحساب مستخدم Windows الحالي. نعم، أريد عرض ملف Readme—يفتح ملف README.txt في Windows Notepad.
29. انقر فوق Next (التالي).
30. إذا قمت بتحديد خيار، فسيبدأ تشغيل خدمات ACS الآمنة من Cisco. تعرض شاشة اكتمال الإعداد معلومات حول واجهة HTML ل ACS الآمن من Cisco.
31. انقر فوق إنهاء. ملاحظة: يتم توثيق بقية التكوين ضمن القسم الخاص بنوع EAP الذي تم تكوينه.

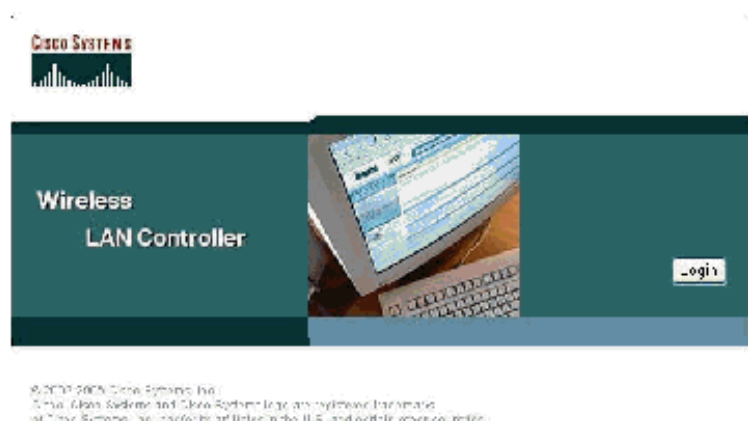
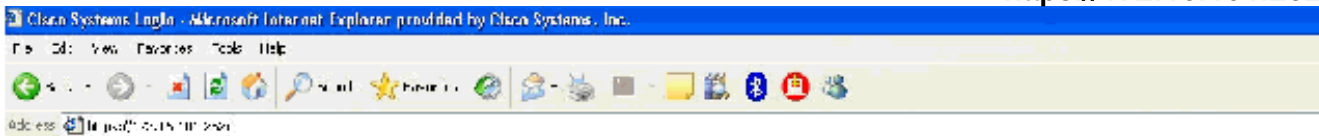
تكوين وحدة التحكم Cisco LWAPP Controller

خلقت التشكيل ضروري ل WPA2/WPA

أكمل الخطوات التالية:

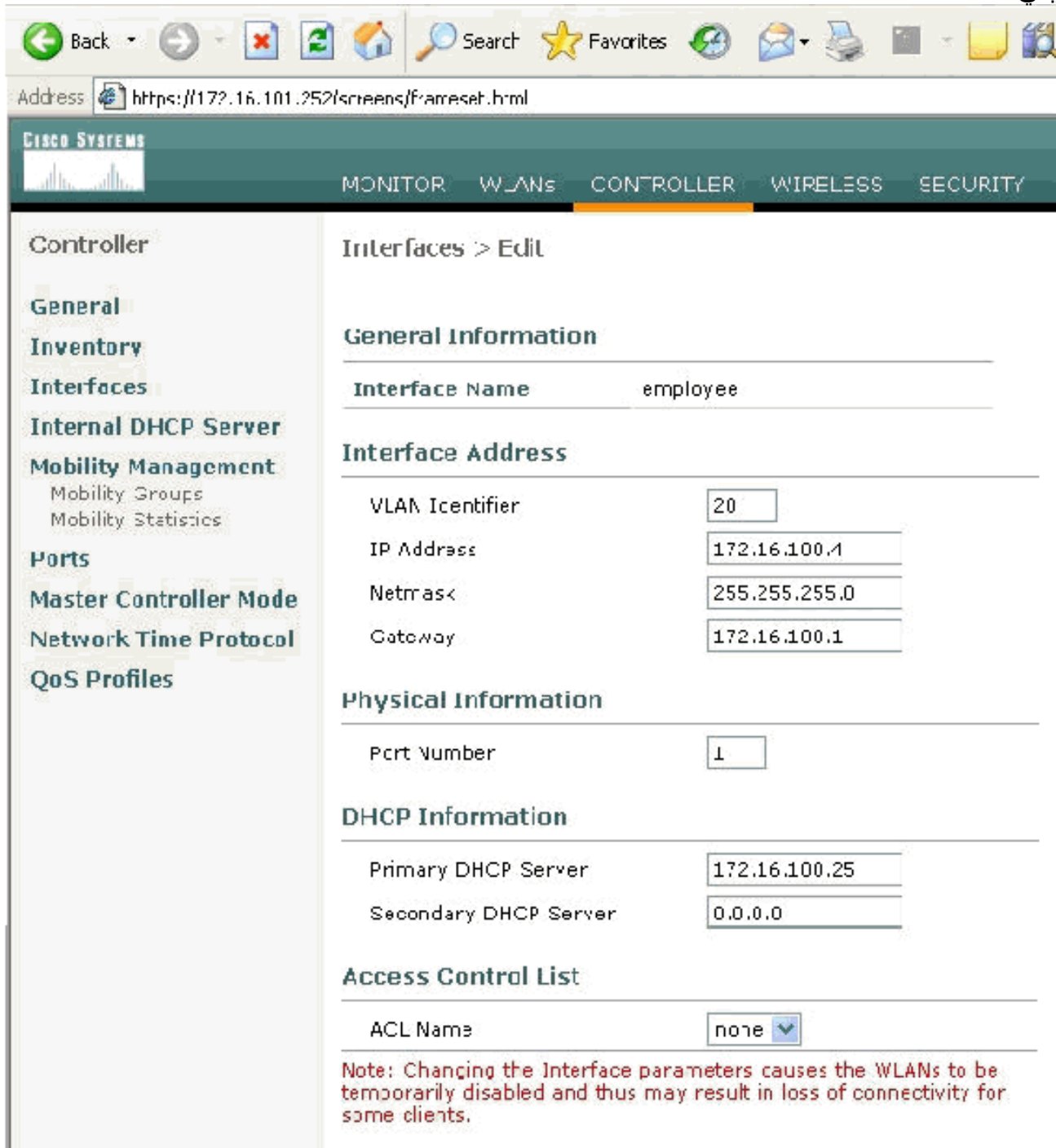
ملاحظة: من المفترض أن يكون لوحدة التحكم اتصال أساسي بالشبكة وأن تكون قابلية الوصول إلى IP لواجهة الإدارة ناجحة.

1. قم بتسجيل الدخول إلى وحدة التحكم عن طريق الاستعراض إلى <https://172.16.101.252>



2. انقر على تسجيل الدخول.
3. قم بتسجيل الدخول باستخدام مسؤول المستخدم الافتراضي وكلمة المرور الافتراضية admin.
4. خلقت القارن VLAN يخطط تحت الجهاز تحكم قائمة.
5. طقطقة قارن.
6. طقطقت جديد.
7. في نوع حقل اسم الواجهة موظف. (يمكن أن يكون هذا الحقل أي قيمة تحبها).

8. في حقل معرف شبكة VLAN نوع 20. (يمكن أن يكون هذا الحقل أي شبكة VLAN يتم نقلها في الشبكة).
 9. طقطقة يطبق.
 10. شكلت المعلومة بما أن هذا قارن < حرر نافذة بيدي.



Controller

General Information

Interface Name	employee
----------------	----------

Interface Address

VLAN Identifier	20
IP Address	172.16.100.1
Netmask	255.255.255.0
Gateway	172.16.100.1

Physical Information

Port Number	1
-------------	---

DHCP Information

Primary DHCP Server	172.16.100.25
Secondary DHCP Server	0.0.0.0

Access Control List

ACL Name	מסוח
----------	------

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

11. طقطقة يطبق.
 12. طقطقت WLAN.
 13. طقطقت جديد.
 14. في نوع حقل SSID الخاص بشبكة WLAN الموظف.
 15. طقطقة يطبق.
 16. قم بتكوين المعلومات مثل هذه الشبكات المحلية اللاسلكية (WLANs) < تحرير عروض الإطارات. ملاحظة:
 WPA2 هو طريقة تشفير الطبقة 2 المختارة لهذا المختبر. للسماح ل WPA مع عملاء TKIP-MIC بالاقتران
 بمعرف SSID هذا، يمكنك أيضا تحديد مربعات وضع توافق WPA والسماح لعملاء WPA2 TKIP أو العملاء
 الذين لا يؤيدون أسلوب تشفير 802.11i AES.

WLAN6 > Edit

WLAN ID	1
WLAN SSID	Employee

General Policies

Radio Policy	All
Admin Status	<input checked="" type="checkbox"/> Enabled
Session Timeout (secs)	1800
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Power Support	<input type="checkbox"/> Client CAC Limit <input type="checkbox"/> AP CAC Limit
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
Allow AAA Override	<input type="checkbox"/> Enabled
Client Exclusion	<input checked="" type="checkbox"/> Enabled ** 60 Timeout Value (secs)
DHCP Server	<input type="checkbox"/> Override
DHCP Addr. Assignment	<input checked="" type="checkbox"/> Required
Interface Name	employee

Security Policies

Layer 2 Security	WPA2
	<input type="checkbox"/> MAC Filtering
Layer 3 Security	None
	<input type="checkbox"/> Web Policy **

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:172.16.100.25, Port:1812	none
Server 2	none	none
Server 3	none	none

WPA2 Parameters

WPA Compatibility Mode	<input checked="" type="checkbox"/> Enable
Allow WPA2 TKIP Clients	<input checked="" type="checkbox"/> Enable
Pre-Shared Key	<input type="checkbox"/> Enabled (WPA2 passphrase has been set)

17. طقطقة يطبق.
18. انقر فوق قائمة الأمان وأضف خادم RADIUS.
19. طقطقت جديد.
20. إضافة عنوان IP لخادم (RADIUS) 172.16.100.25 وهو خادم ACS الذي تم تكوينه مسبقاً.
21. تأكد من تطابق المفتاح المشترك مع عميل AAA الذي تم تكوينه في خادم ACS.
22. طقطقة يطبق.



Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

RADIUS Authentication Servers > New

Server Index (Priority)	1 <input type="button" value="v"/>
Server IP Address	<input type="text" value="172.16.100.25"/>
Keys Format	ASCII <input type="button" value="v"/>
Shared Secret	<input type="password" value="....."/>
Confirm Shared Secret	<input type="password" value="....."/>
Key Wrap	<input type="checkbox"/>
Port Number	<input type="text" value="1812"/>
Server Status	Enabled <input type="button" value="v"/>
Support for RFC 3576	Enabled <input type="button" value="v"/>
Retransmit Timeout	<input type="text" value="2"/> seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable

CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.

File Edit View Favorites Tools Help

Address http://172.16.100.25:3052/index2.htm

CISCO SYSTEMS Network Configuration

Edit

User Setup
 Interface Setup
 Shared Profile Components
 Network Configuration
 System Configuration
 Interface Configuration
 Administration Control
 External User Database
 Profile Validation
 Network Access Profiles
 Features and

AAA Client Setup For DEMO_2006_1

AAA Client IP Address: 172.16.100.252

Key: shared secret

Authentication Using: RADIUS (Cisco Airesis)

Single Connect TACACS+ AAA Client (Record step in accounting on failure).

Coq Update/Watchdog Packets from this AAA Client

Coq RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

23. اكتمل التكوين الأساسي الآن ويمكنك البدء في اختبار EAP-TLS.

مصادقة EAP-TLS

تتطلب مصادقة EAP-TLS وجود شهادات كمبيوتر ومستخدم على العميل اللاسلكي، وإضافة EAP-TLS كنوع EAP إلى سياسة الوصول عن بعد للوصول اللاسلكي، وإعادة تكوين توصيل الشبكة اللاسلكية.

لتكوين DC_CA لتوفير التسجيل التلقائي لشهادات الكمبيوتر والمستخدمين، أكمل الإجراءات الواردة في هذا القسم.

ملاحظة: قامت Microsoft بتغيير قالب خادم الويب من خلال إصدار Windows 2003 Enterprise CA حتى لا تعود المفاتيح قابلة للتصدير ويتم تحديد الخيار بدقة. لا توجد قوالب شهادات أخرى مزودة بخدمات شهادات لمصادقة الخادم وتعطي القدرة على وضع علامة على المفاتيح قابلة للتصدير المتوفرة في القائمة المنسدلة بحيث يتعين عليك إنشاء قالب جديد يقوم بذلك.

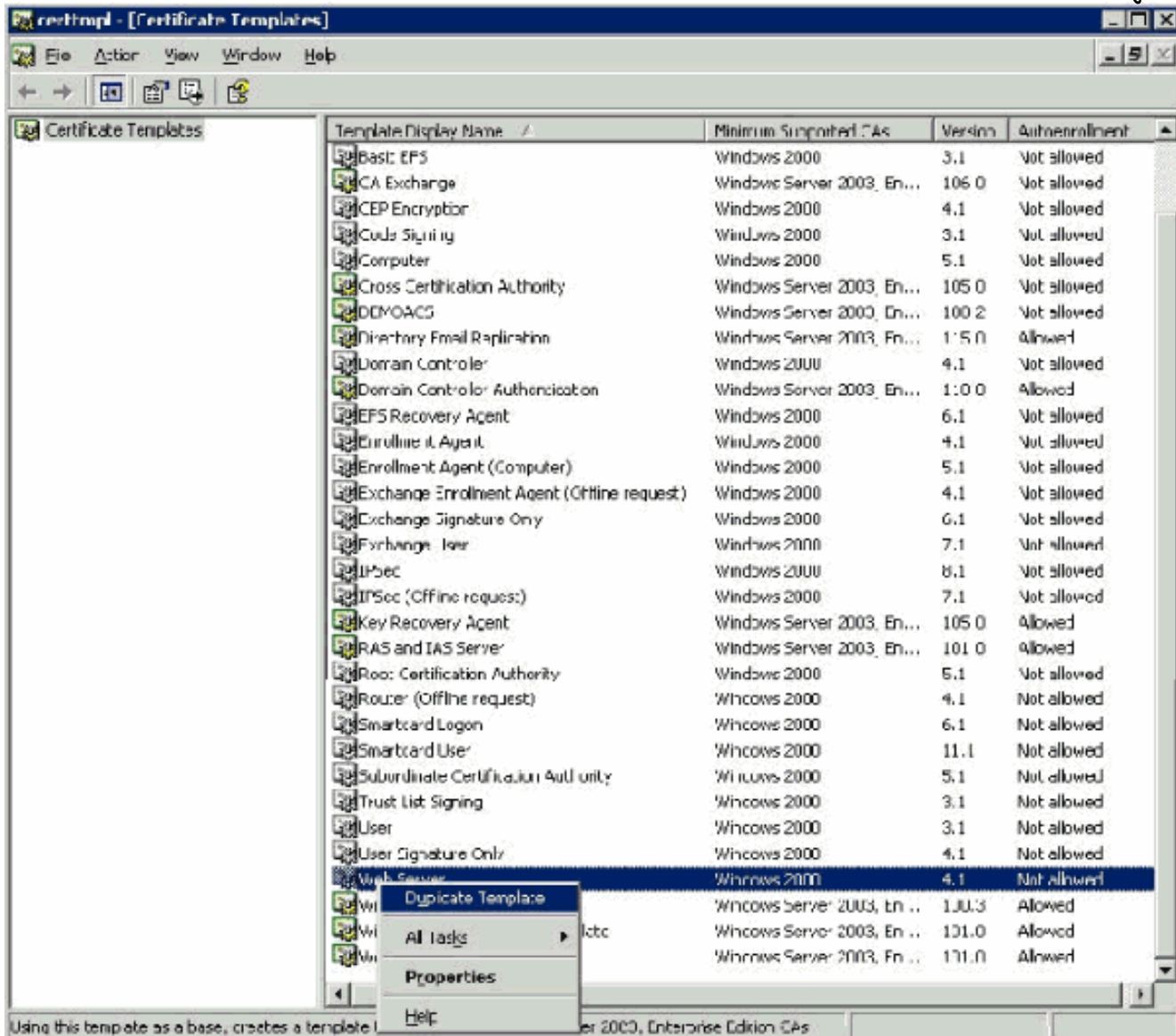
ملاحظة: يسمح نظام التشغيل Windows 2000 باستخدام مفاتيح قابلة للتصدير، ولا يلزم اتباع هذه الإجراءات إذا كنت تستخدم نظام التشغيل Windows 2000.

تثبيت الأداة الإضافية لقوالب الشهادات

أكمل الخطوات التالية:

1. أختار ابدأ < تشغيل، واكتب mmc، وانقر فوق موافق.
2. من القائمة "ملف"، انقر فوق إضافة/إزالة الأداة الإضافية ثم انقر فوق إضافة.

3. تحت الأداة الإضافية، انقر نقرًا مزدوجًا على **قوالب الترخيص**، ثم انقر على **إغلاق**، ثم انقر على **موافق**.
4. في شجرة وحدة التحكم، انقر فوق **قوالب الشهادات**. تظهر كل قوالب الشهادات في جزء التفاصيل.
5. لتخطي الخطوات من 2 إلى 4، اكتب **certtmpl.msc** الذي يفتح الأداة الإضافية "قوالب الشهادات".



قم بإنشاء قالب الشهادة لخدمة ويب ACS

أكمل الخطوات التالية:

1. في جزء التفاصيل من الأداة الإضافية "قوالب الشهادات"، انقر فوق قالب خادم الويب.
2. في قائمة الإجراء، انقر فوق **مضاعفة**.

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:
Copy of Web Server

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:
Copy of Web Server

Validity period: 2 years
Renewal period: 6 weeks

Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

قالب.
3. في حقل اسم عرض القالب ، اكتب

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:
[ACS]

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:
[ACS]

Validity period: [2] [years] [v] Renewal period: [6] [weeks] [v]

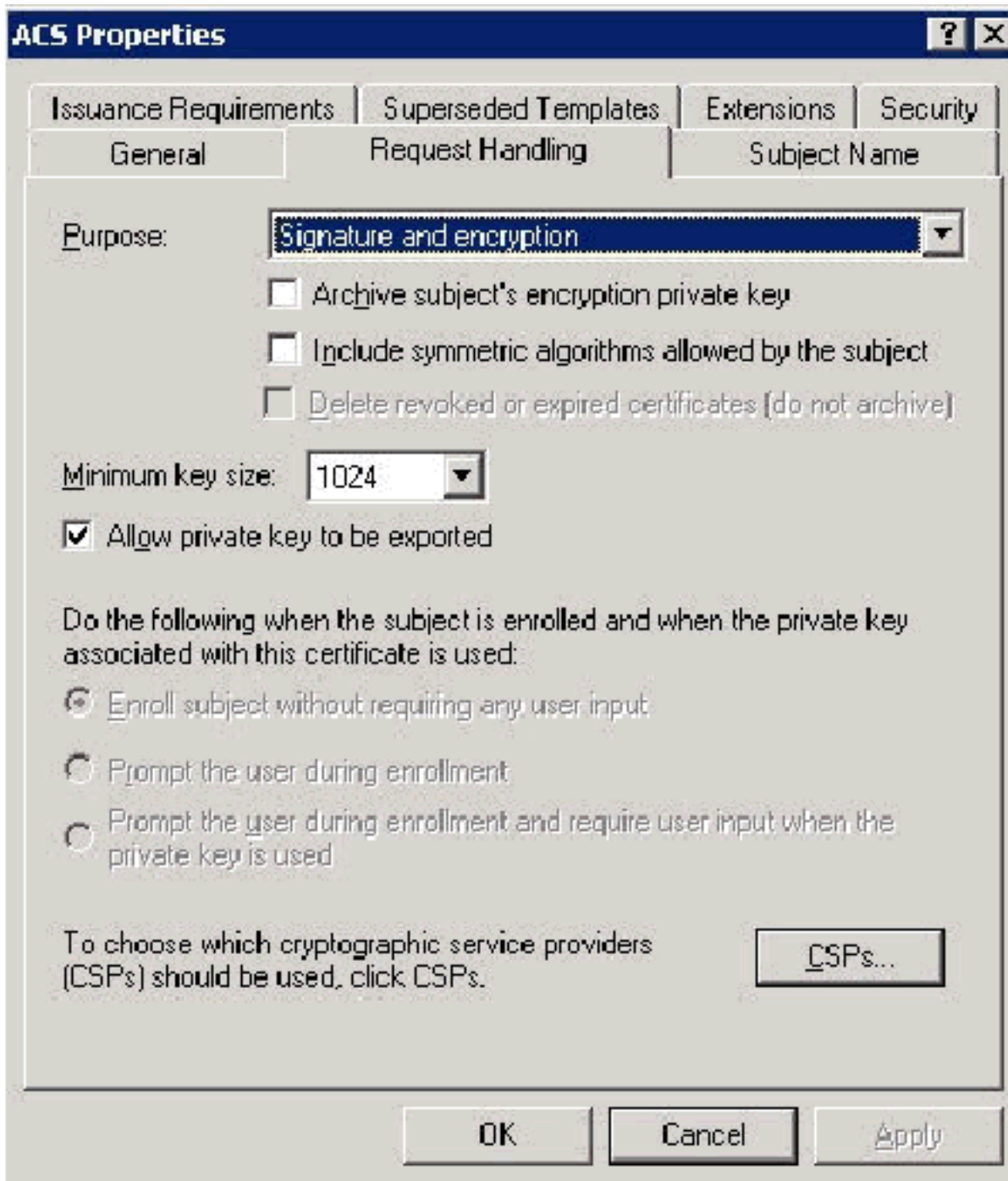
Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

[OK] [Cancel] [Apply]

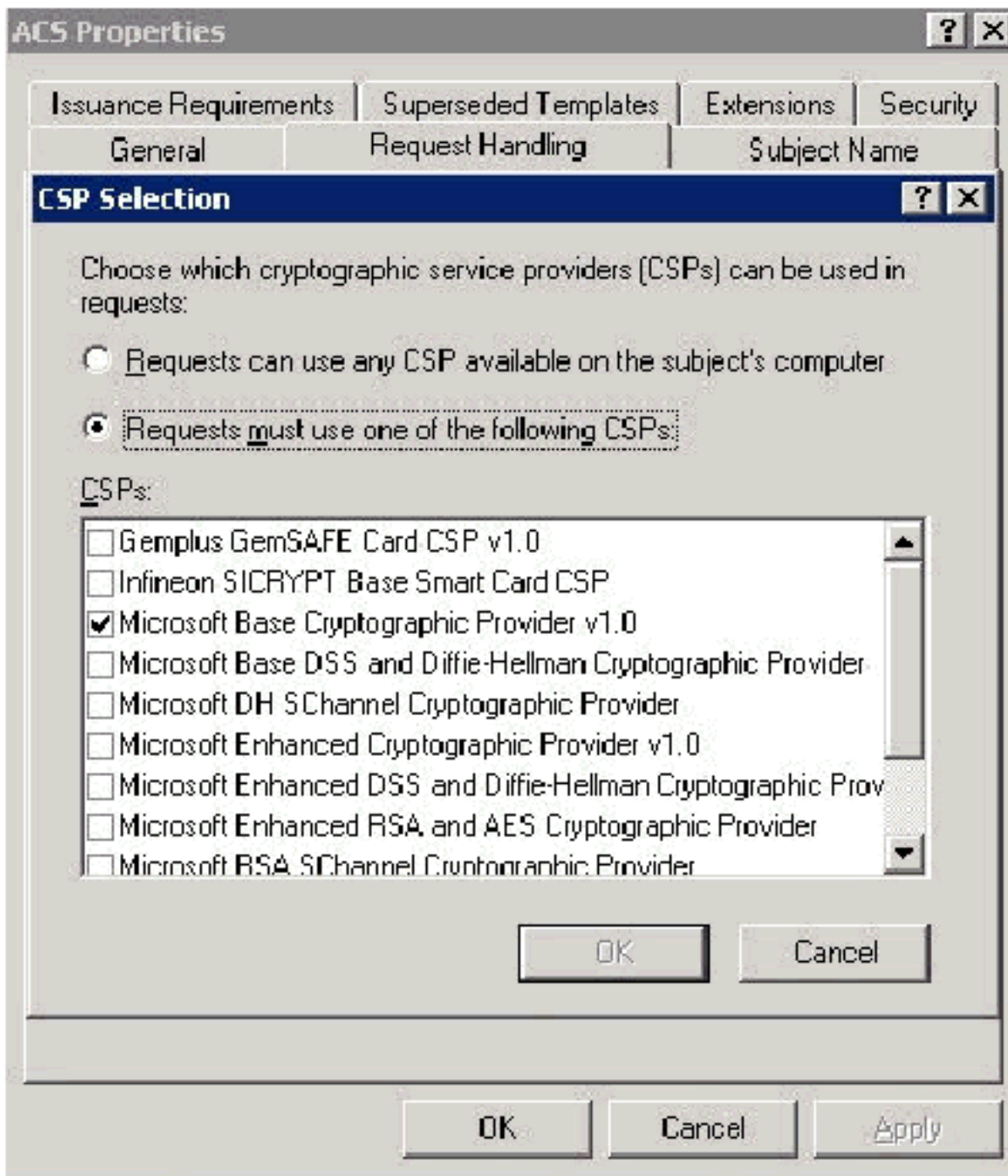
.acs

4. انتقل إلى علامة التبويب "معالجة الطلب" وحدد السماح بتصدير المفتاح



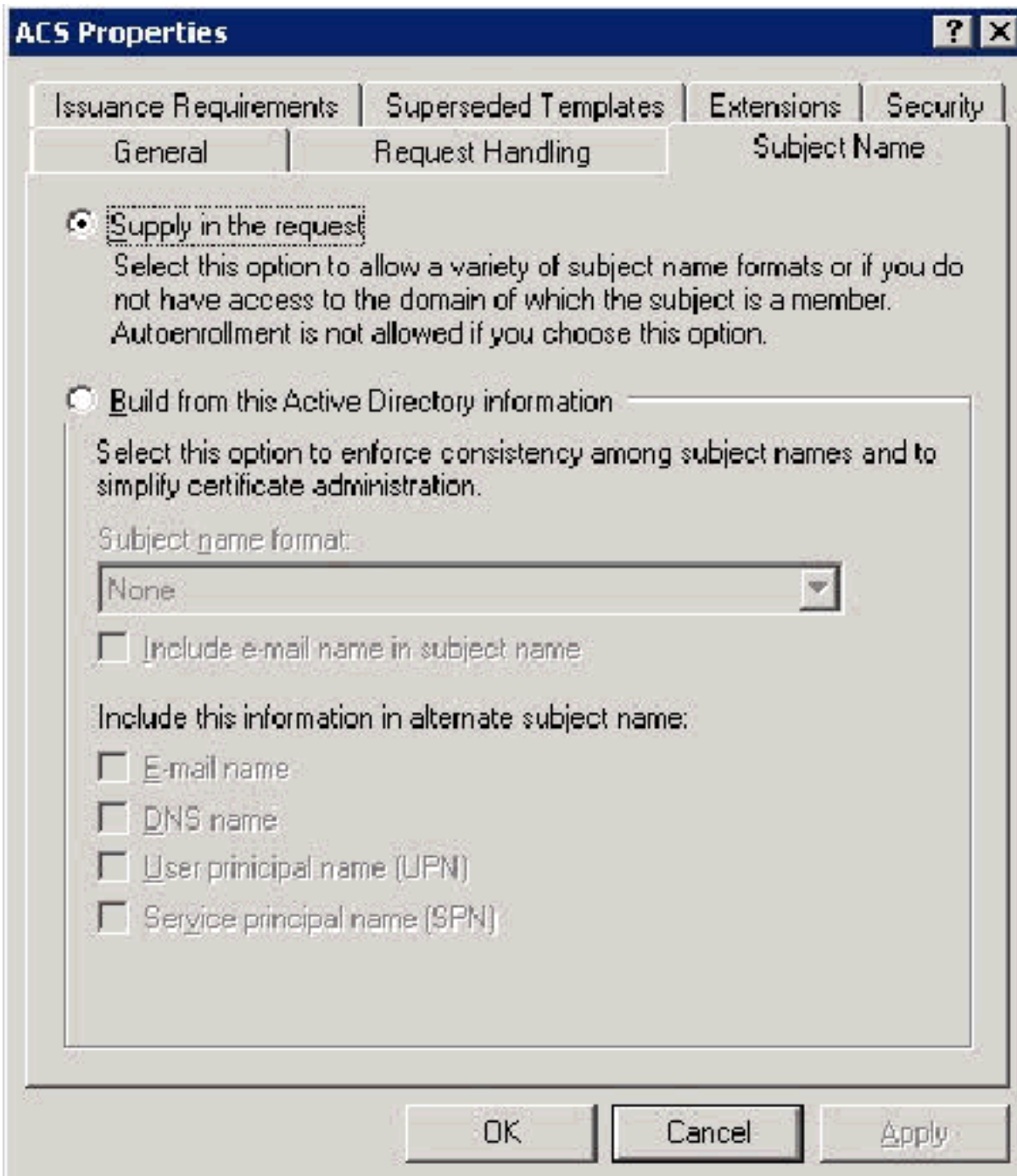
الخاص.

5. اختر طلبات يجب أن تستخدم أحد CSP التالية وفحص موفر التشفير الأساسي Microsoft v1.0. قم بإلغاء تحديد أي CSPs أخرى تم تحديدها ثم انقر فوق



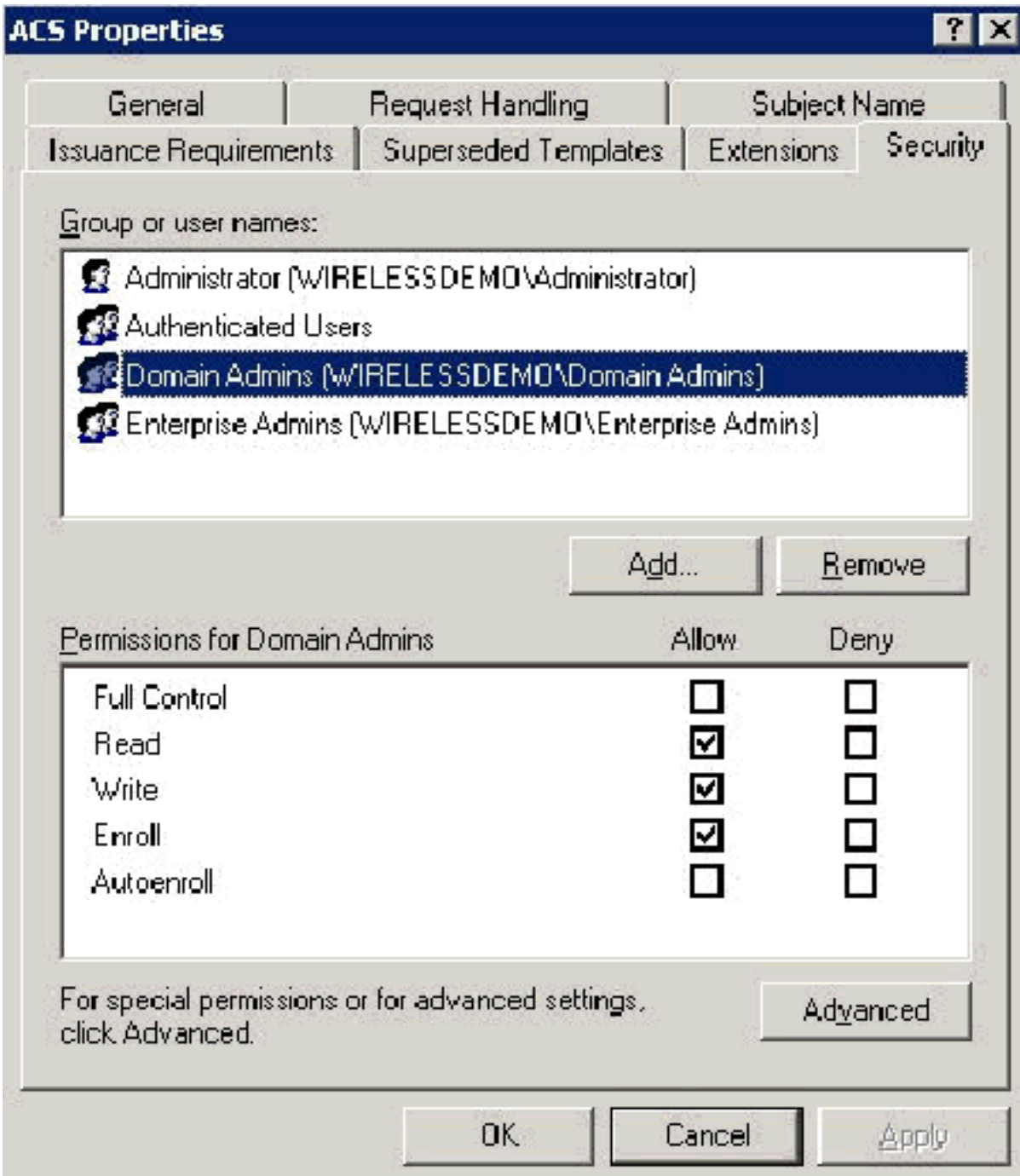
موافق.

6. انتقل إلى علامة التبويب اسم الموضوع، واختر التزويد في الطلب وانقر فوق



موافق.

7. انتقل إلى علامة التبويب "أمان"، وأبرز مجموعة مسؤولي المجال وتأكد من تحديد خيار التسجيل ضمن "مسموح به". هام: إذا اخترت الإنشاء من معلومات Active Directory هذه فقط، فتتحقق من اسم المستخدم الأساسي (UPN) وألغي تحديد اسم تضمين البريد الإلكتروني في اسم الموضوع واسم البريد الإلكتروني لأنه لم يتم إدخال اسم بريد إلكتروني لحساب WirelessUser في الأداة الإضافية Active Directory Users and Computers. إذا لم تقم بتعطيل هذين الخيارين، فسيحاول التسجيل التلقائي استخدام البريد الإلكتروني، مما ينتج عنه خطأ في التسجيل



التلقائي.

8. هناك إجراءات أمان إضافية إذا لزم الأمر لمنع دفع الشهادات تلقائياً. ويمكن العثور على هذه العناصر ضمن علامة التبويب متطلبات الإصدار. لم يتم مناقشة هذا الأمر في هذه

ACS Properties [?] [X]

General Request Handling Subject Name
 Issuance Requirements Superseded Templates Extensions Security

Require the following for enrollment:

CA certificate manager approval

This number of authorized signatures:

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Add...
 Remove

Require the following for reenrollment:

Same criteria as for enrollment

Valid existing certificate

OK Cancel Apply

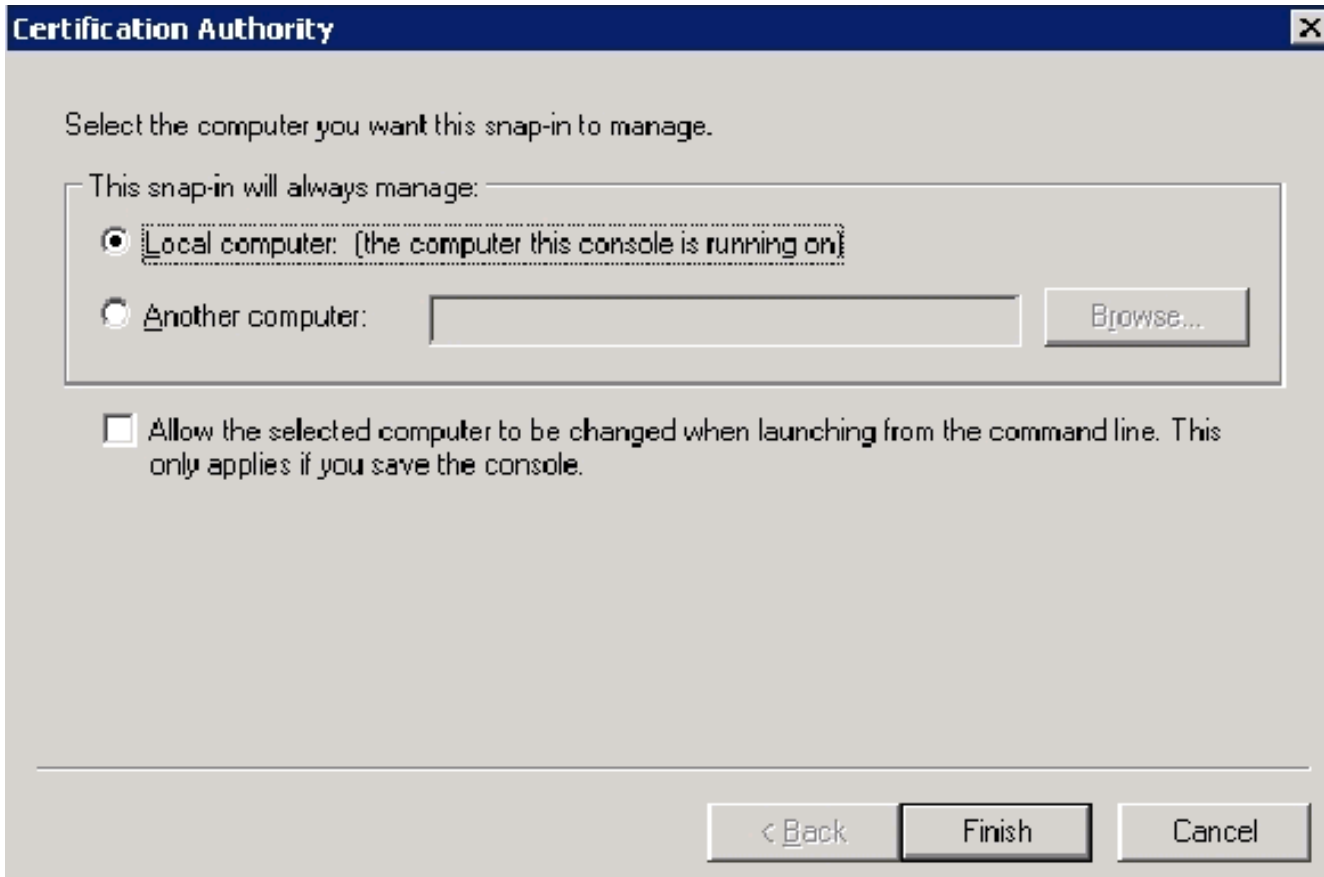
الوثيقة.

9. انقر فوق موافق لحفظ القالب والانتقال إلى إصدار هذا القالب من الأداة الإضافية "مرجع الشهادات".

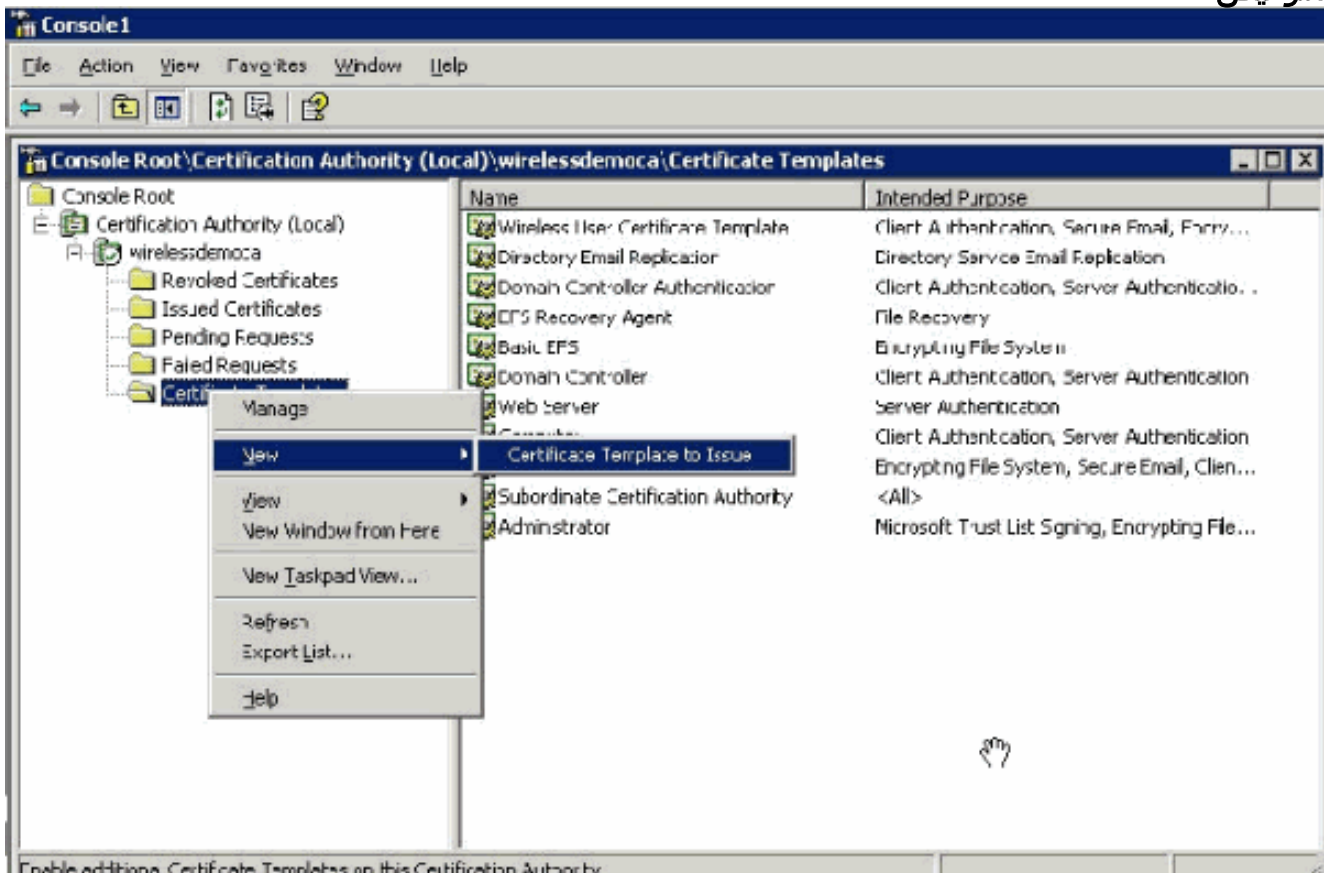
تمكين قالب شهادة خادم ويب ACS الجديد

أكمل الخطوات التالية:

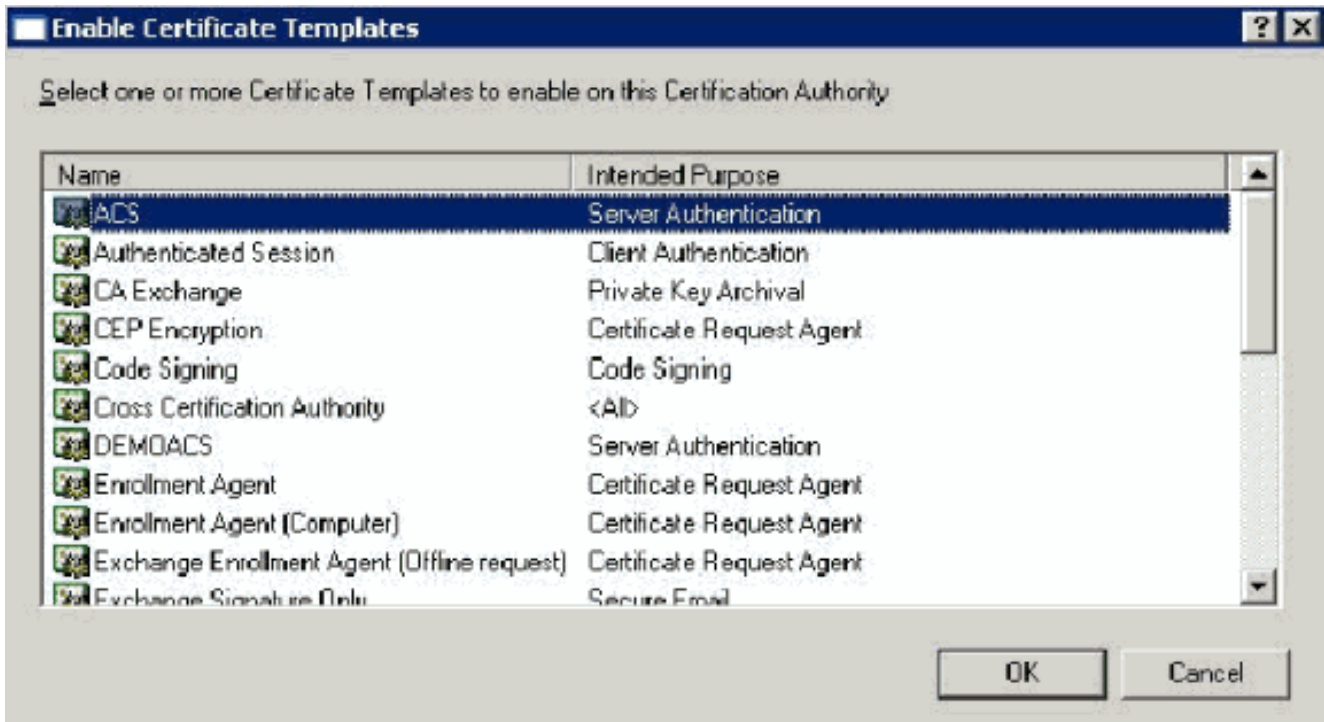
1. فتح الأداة الإضافية المرجع المصدق. اتبع الخطوات 1-3 في قسم إنشاء قالب الشهادة لخادم ويب ACS، واختر مرجع الشهادة، واختر الكمبيوتر المحلي وانقر فوق إنهاء.



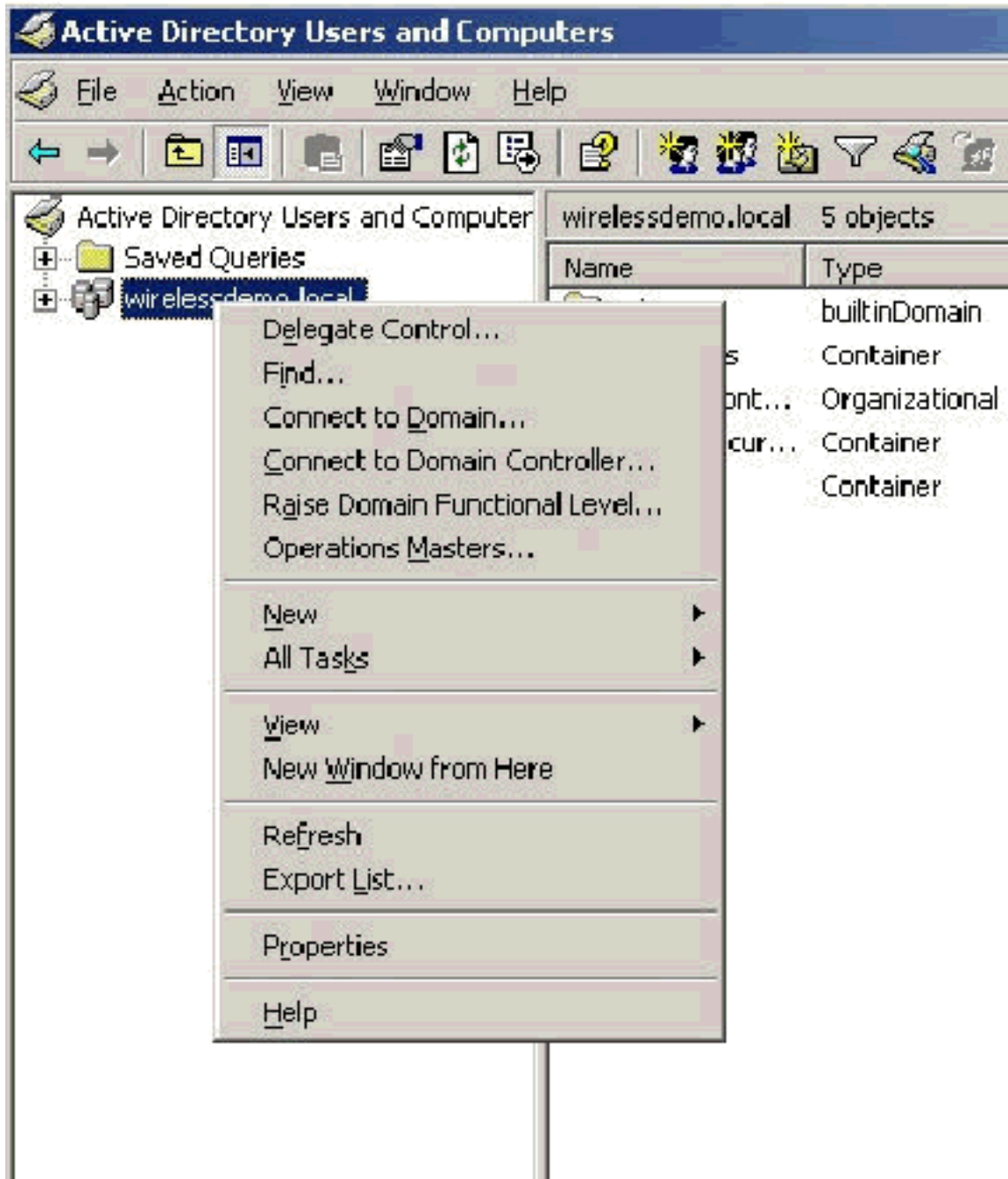
2. في شجرة وحدة التحكم، قم بتوسيع WirelessDemoca، ثم انقر بزر الماوس الأيمن فوق قوالب الترخيص.



3. أختار جديد < قالب الشهادة لإصداره.
4. انقر على قالب شهادة ACS.

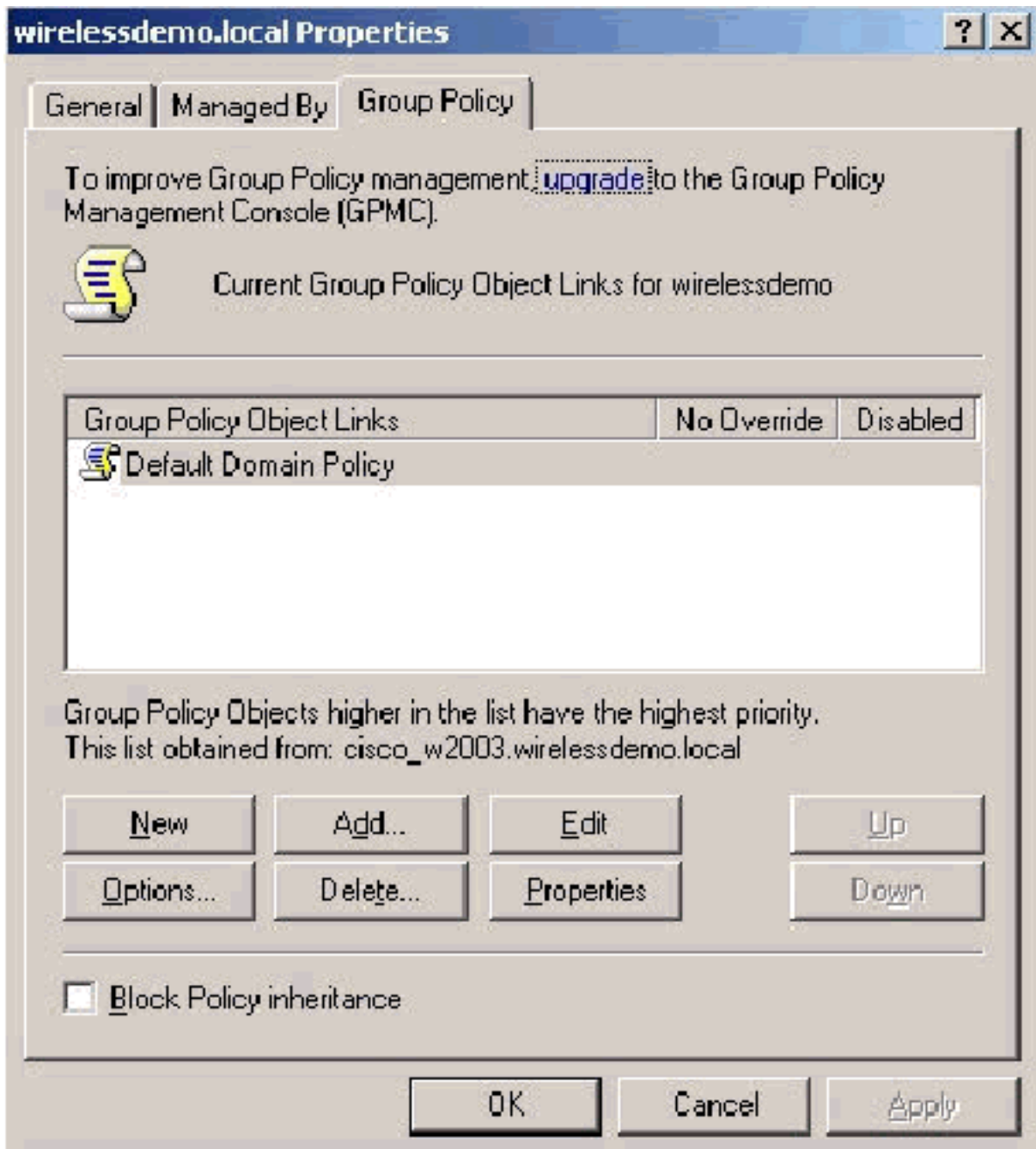


5. انقر فوق **موافق** وافتح الأداة الإضافية **Active Directory Users and Computers**. ثم انقر بزر
6. في شجرة وحدة التحكم، انقر نقرًا مزدوجًا فوق **Active Directory Users and Computers**. ثم انقر بزر
الماوس الأيمن فوق **WirelessDemo.local domain**. ثم انقر فوق

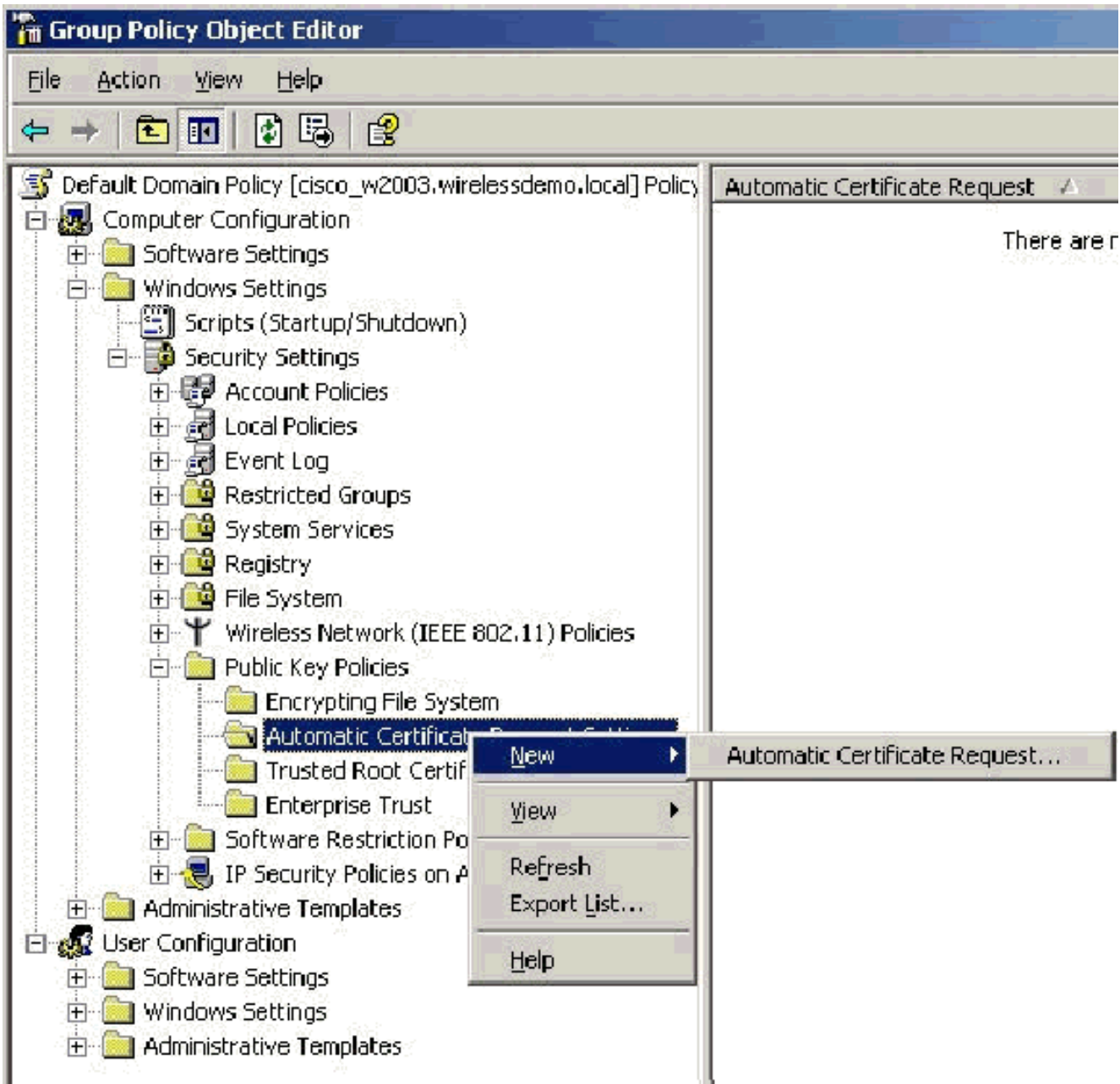


خصائص.

7. في علامة التبويب "نهج المجموعة"، انقر فوق نهج المجال الافتراضي، ثم انقر فوق تحرير. يؤدي ذلك إلى فتح الأداة الإضافية "محرر كائنات نهج المجموعة".



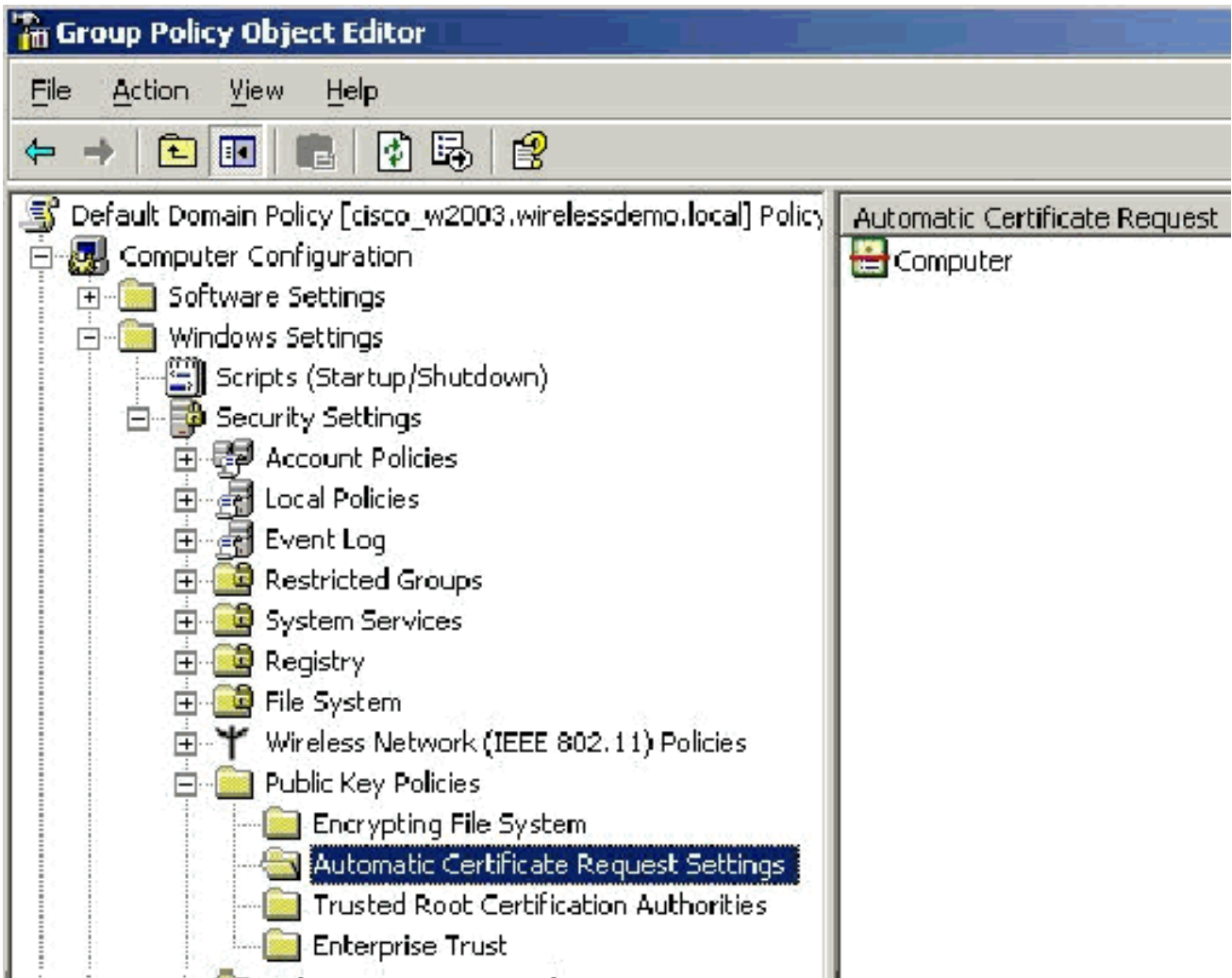
8. في شجرة وحدة التحكم، قم بتوسيع تكوين جهاز الكمبيوتر < إعدادات Windows > إعدادات التأمين < سياسات المفتاح العام، ثم حدد إعدادات طلب الترخيص الأبي.



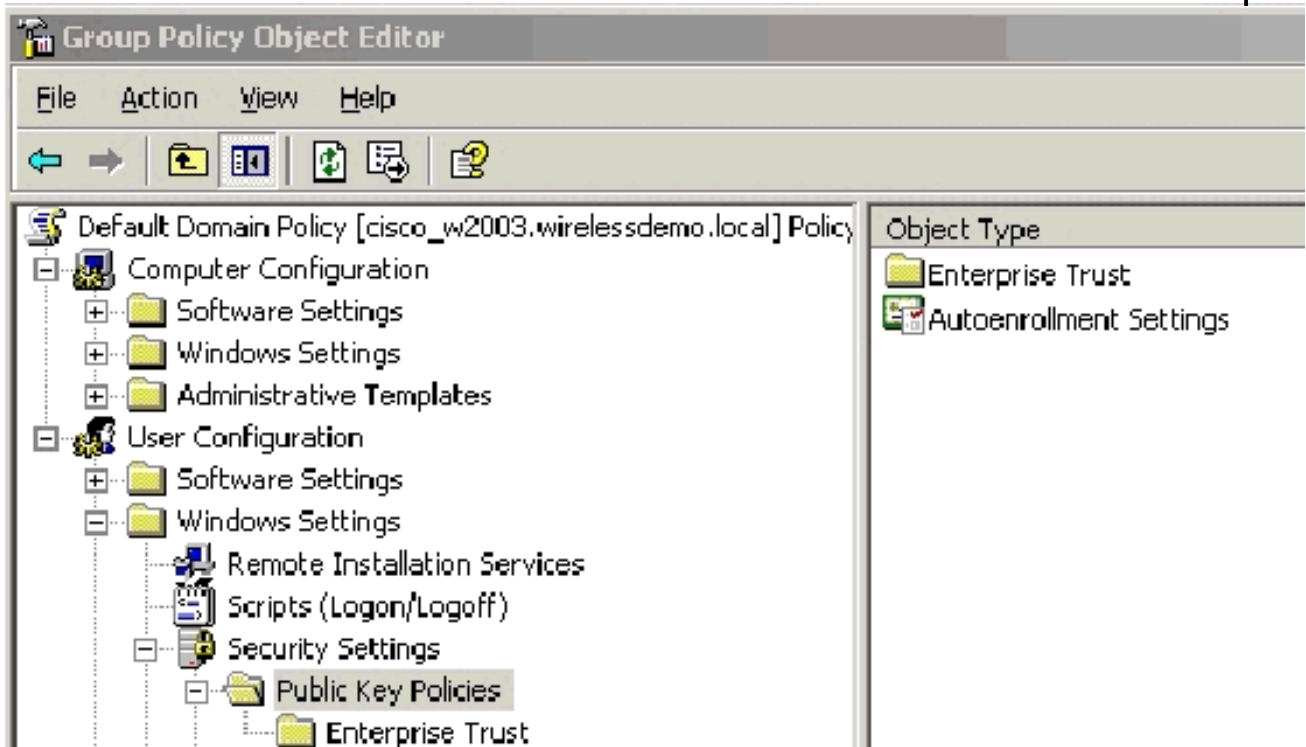
9. انقر بزر الماوس الأيمن على إعدادات طلب الترخيص الآلي واختر جديد < طلب الترخيص التلقائي.
10. في صفحة "معالج إعداد طلب الشهادة التلقائي"، انقر فوق التالي.
11. في صفحة "قالب الشهادة"، انقر على الكمبيوتر وانقر فوق التالي.



12. في صفحة إكمال معالج إعداد طلب الشهادة التلقائي، انقر فوق إنهاء. يظهر الآن نوع شهادة الكمبيوتر في جزء التفاصيل الخاص بالأداة الإضافية "محرر كائنات نهج المجموعة".

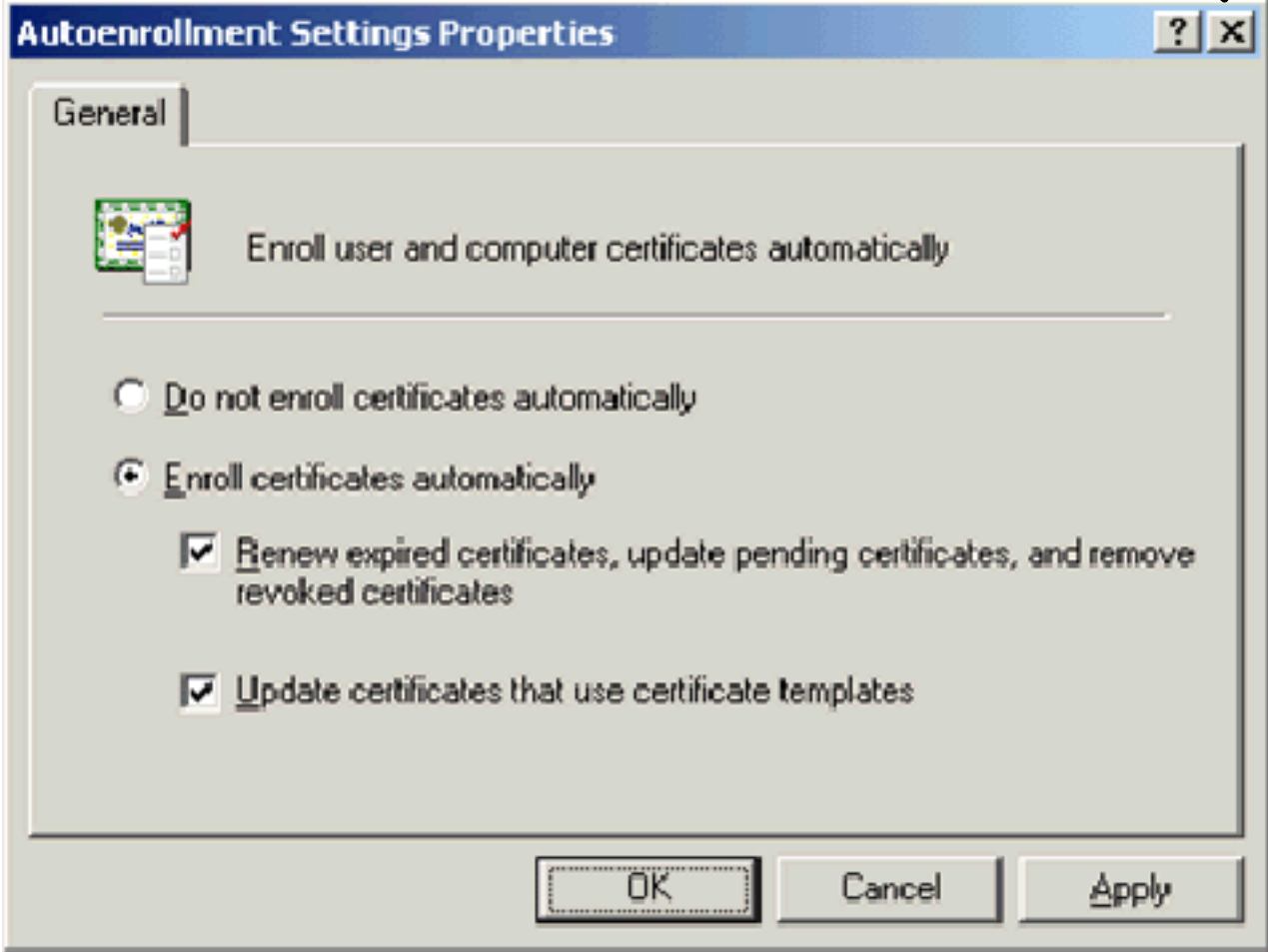


13. في شجرة وحدة التحكم، قم بتوسيع تكوين المستخدم < إعدادات Windows > إعدادات التأمين < سياسات المفتاح العام.



14. في جزء التفاصيل، انقر نقرًا مزدوجًا على إعدادات التسجيل التلقائي.
 15. أختَر تسجيل الشهادات تلقائياً وافحص تجديد الشهادات متتهية الصلاحية وتحديث الشهادات المعلقة وإزالة

الشهادات الملغاة وتحديث الشهادات التي تستخدم قوالب
الشهادات.



16. وانقر فوق OK.

إعداد شهادة ACS 4.0

تكوين الشهادة القابلة للتصدير ل ACS

هام: يجب أن يحصل خادم ACS على شهادة خادم من خادم CA الجذر للمؤسسة لمصادقة عميل-WLAN EAP-TLS.

هام: تأكد من عدم فتح إدارة IIS أثناء عملية إعداد الشهادة لأنها تتسبب في حدوث مشاكل مع المعلومات المخزنة مؤقتا.

1. قم بتسجيل الدخول إلى خادم ACS باستخدام حساب له حقوق Enterprise Admin.
2. على جهاز ACS المحلي، قم بتوجيه المستعرض إلى خادم مرجع مصدق Microsoft على <http://IP-address-of-Root-CA/certsrv>. في هذه الحالة، يكون عنوان IP 172.16.100.26.
3. قم بتسجيل الدخول كمسؤول.



4. أختار طلب شهادة وانقر التالي.



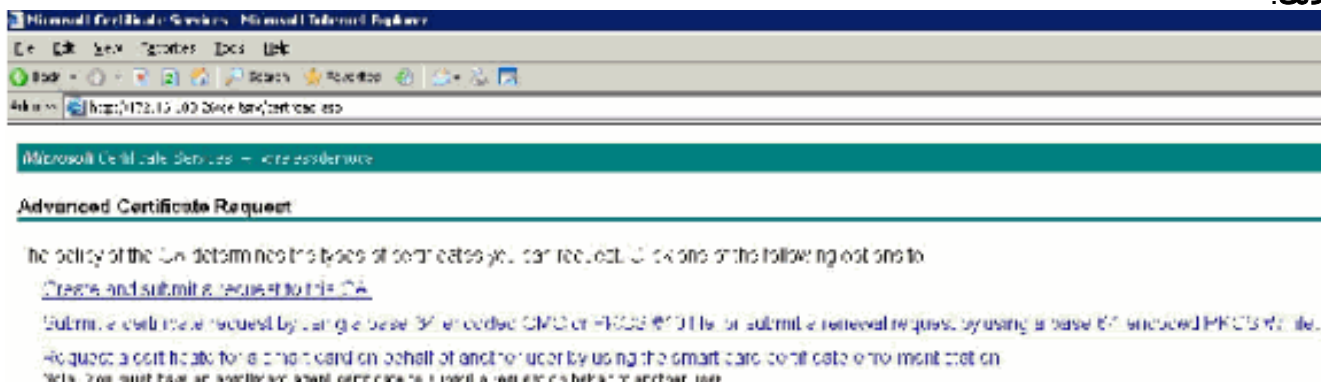
Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

5. أختارت طلب متقدم وطقطقة بعد ذلك.



6. أختار إنشاء طلب وإرساله إلى المرجع المصدق هذا وانقر فوق التالي. هام: يرجع السبب وراء هذه الخطوة إلى أن Windows 2003 لا يسمح بالمفاتيح القابلة للتصدير وأنت تحتاج إلى إنشاء طلب شهادة استنادا إلى شهادة ACS التي قمت بإنشائها مسبقا والتي تسمح

Address: http://172.16.1.10:2544/certs/wirelessdemo/

Microsoft Certificate Services - wirelessdemo.local

Advanced Certificate Request

Certificate Template:

Administra...
 Administrator
 Basic EFS
 EFS Recovery Agent
 User
 Wireless User Certificate Template
 User
 S_Lordine Certification Authority
 Web Server

Key Options:

CSP: Microsoft Base Cryptographic Provider
 Key Usage: Code Signing
 Key Storage: My
 Max: 15360
 Automatic key container name User specified key container name
 Mark keys as exportable
 Export keys to file
 Enable strong private key protection
 Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10
 Hash Algorithm: SHA-1
Only used to sign request.
 Save request to file
 Affiliates:
 Friendly Name:

بذلك.

7. من "قوالب الشهادات"، حدد قالب الشهادة الذي تم إنشاؤه سابقا باسم ACS. تتغير الخيارات بعد أن تقوم بتحديد القالب.

8. قم بتكوين الاسم ليكون اسم المجال المؤهل بالكامل ل خادم ACS. في هذه الحالة يكون اسم خادم ACS هو cisco_w2003.wirelessdemo.local. تأكد من أن شهادة المتجر في مخزن شهادات الكمبيوتر المحلي تم فحصها وانقر على

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Deck Back Forward Stop Search Favorites

Address http://172.16.100.25/certsrv/certreq.asp

Certificate Template:

ACS

Identifying Information For Offline Template:

Name: cisco_w2003_wirelessdemo.local

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Key Options:

Create new key set Use existing key set

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: Exchange

Key Size: 1024 Min:1024 Max:1024 (common key sizes: 1024)

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm: SHA-1
Only used to sign request.

Save request to a file

Attributes:

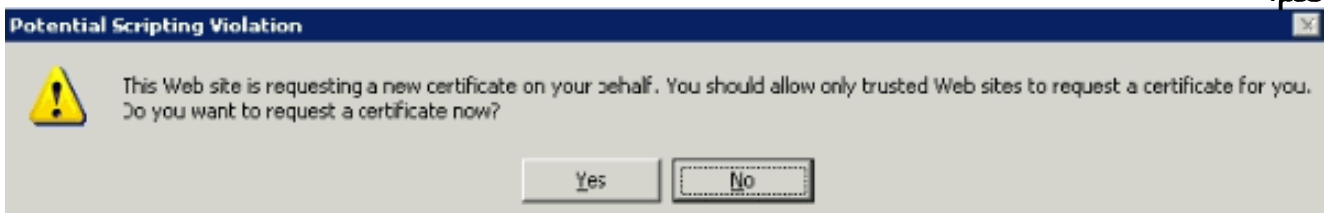
Friendly Name:

Submit >

إرسال.

9. تظهر نافذة مبنقة تحذر من إخلال محتمل للبرمجة النصية. طقطقة

نعم.



10. انقر على تثبيت هذه الشهادة.



Microsoft Certificate Services -- wirelessdemoca

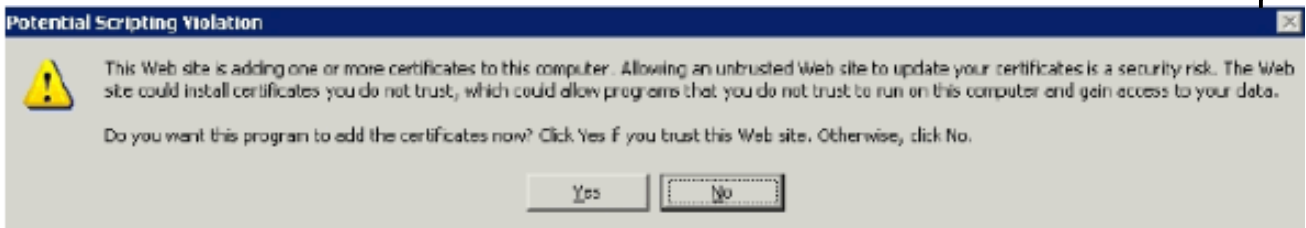
Certificate Issued

The certificate you requested was issued to you.

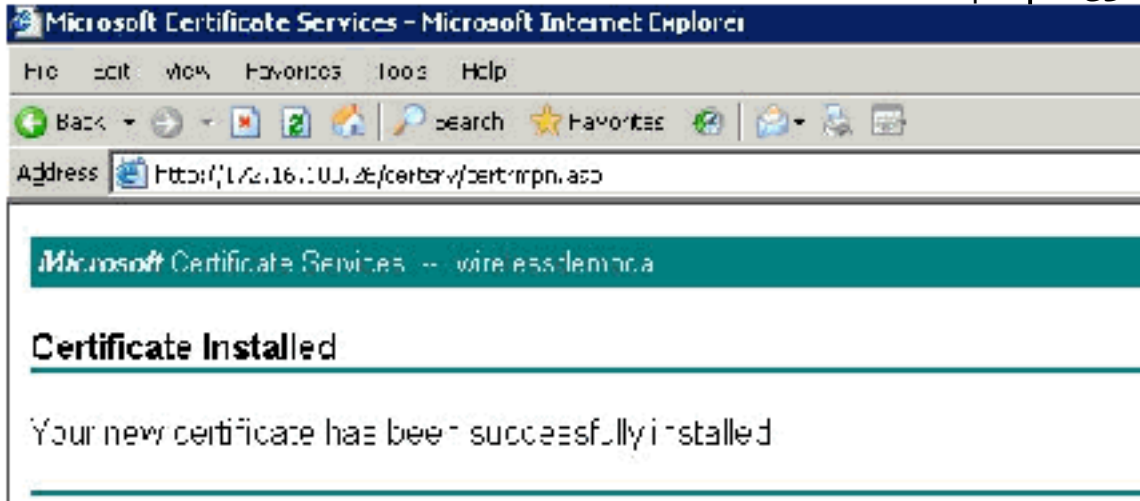


[Install this certificate](#)

11. تظهر نافذة منبثقة مرة أخرى وتحذر من انتهاك محتمل للبرمجة النصية. طققة نعم.

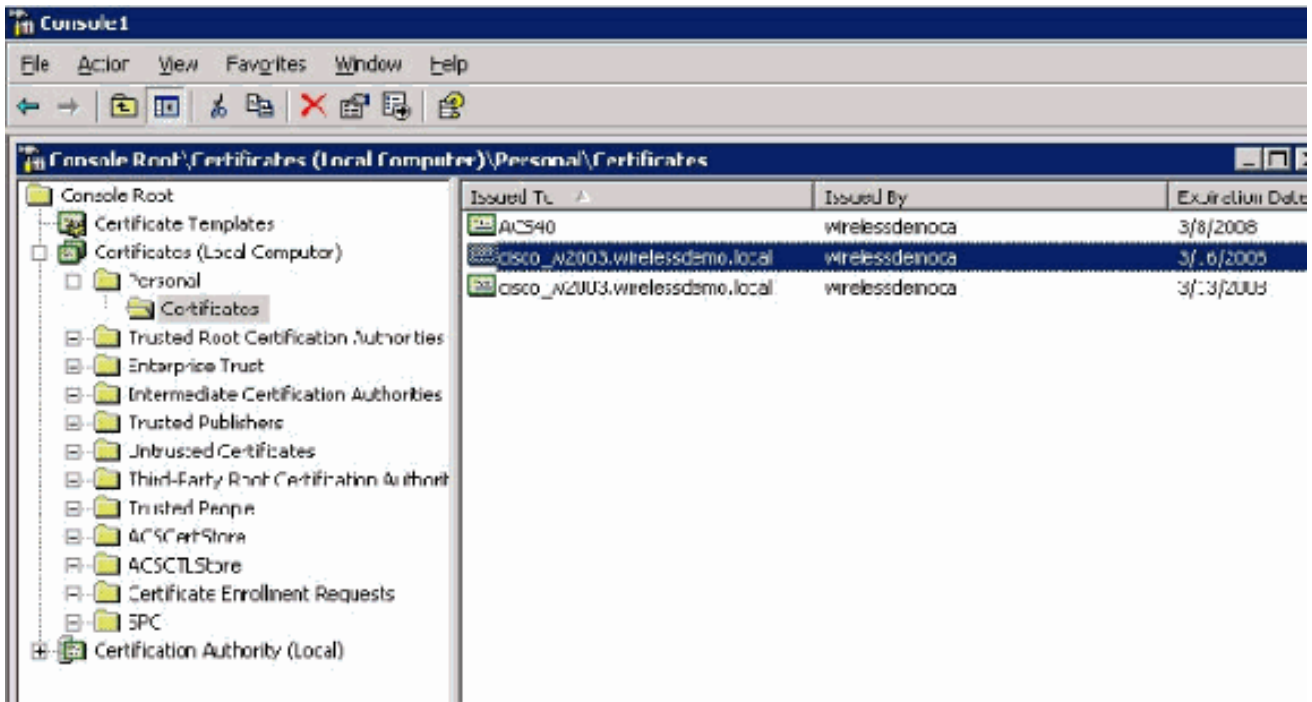


12. بعد النقر فوق نعم، يتم تثبيت



الشهادة.

13. عند هذه النقطة، يتم تثبيت الشهادة في مجلد الشهادات. للوصول إلى هذا المجلد، اختر بدء < تشغيل، واكتب mmc، واضغط على إدخال، واختر شخصي < شهادات.



14. الآن بعد أن تم تثبيت الشهادة على الكمبيوتر المحلي (ACS أو Cisco_w2003 في هذا المثال)، يلزمك إنشاء ملف شهادة (.cer) لتكوين ملف شهادة ACS 4.0.
15. على خادم ACS (Cisco_w2003 في هذا المثال)، وجه المتصفح في خادم مرجع مصدق Microsoft إلى <http://172.16.100.26/certsrv>.

تثبيت الشهادة في برنامج ACS 4.0

أكمل الخطوات التالية:

1. على خادم ACS (Cisco_w2003 في هذا المثال)، قم بتوجيه المستعرض في خادم Microsoft CA إلى <http://172.16.100.26/certsrv>.
2. من خيار تحديد مهمة اختر تنزيل شهادة CA أو سلسلة شهادات أو CRL.
3. اخترت القاعدة 64 ترميز أسلوب وطققة download ca شهادة.



Microsoft Certificate Services -- wirelessdemoca

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method:

CA certificate:

Content type: wirelessdemoca

Encoding method:

- DER
- Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

4. يظهر إطار تحذير أمان تنزيل الملفات. قطعة

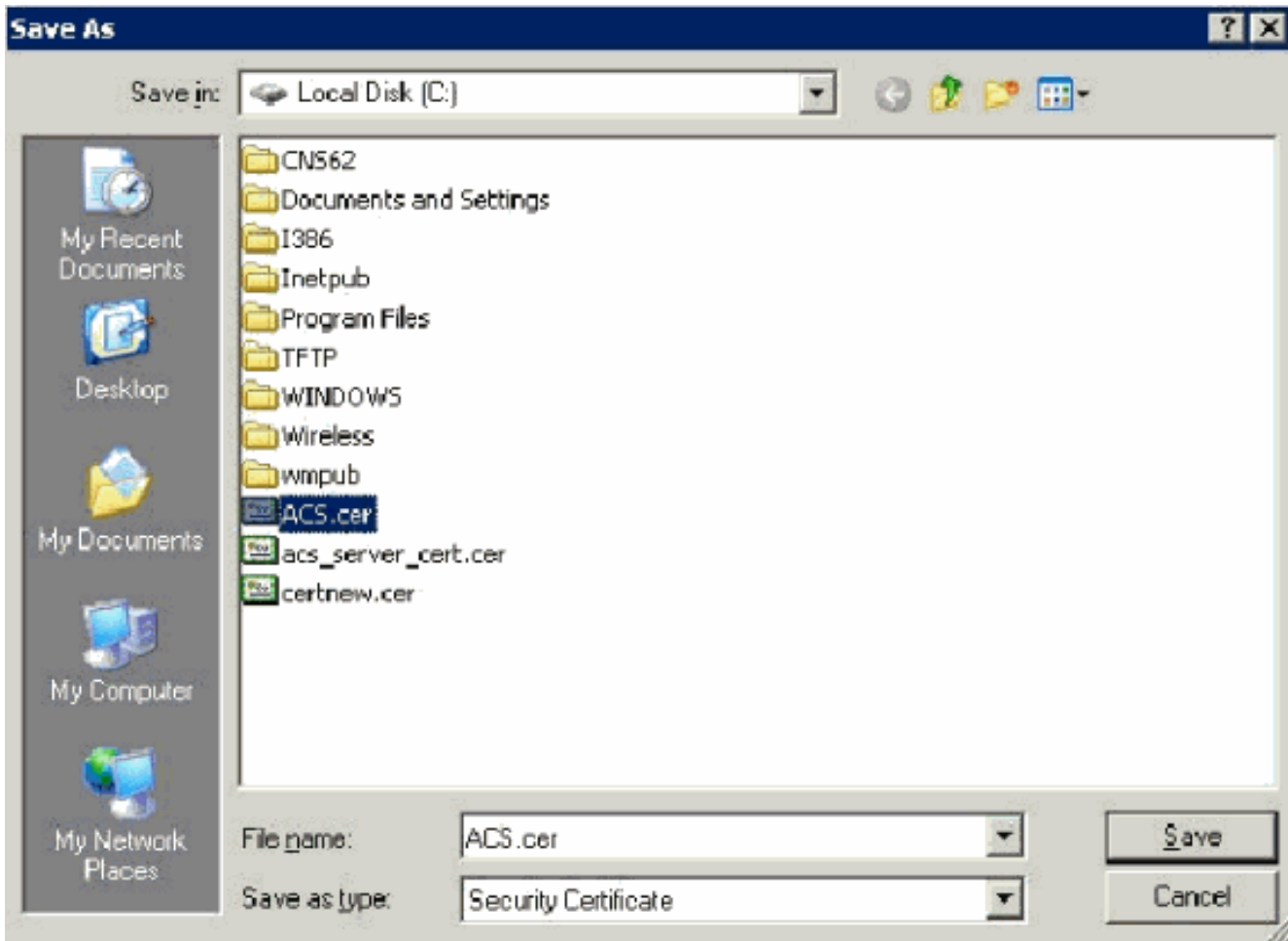


حفظ.

5. احفظ الملف باسم مثل ACS.CER أو أي اسم تريده. تذكر هذا الاسم لأنك تستخدمه أثناء إعداد "مرجع شهادة

ACS" في ACS

4.0

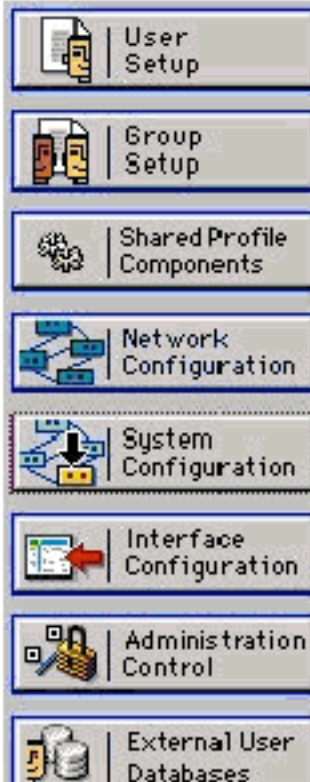


6. افتح مسؤول ACS من إختصار سطح المكتب الذي تم إنشاؤه أثناء التثبيت.
7. طقطقة نظام



System Configuration

Select



-  [Service Control](#)
-  [Logging](#)
-  [Date Format Control](#)
-  [Local Password Management](#)
-  [ACS Internal Database Replication](#)
-  [ACS Backup](#)
-  [ACS Restore](#)
-  [ACS Service Management](#)
-  [VoIP Accounting Configuration](#)
-  [ACS Certificate Setup](#)
-  [Global Authentication Setup](#)

تشكيل.
8. انقر على إعداد شهادة
.ACS

System Configuration

Select

ACS Certificate Setup

-  [Install ACS Certificate](#)
-  [ACS Certification Authority Setup](#)
-  [Edit Certificate Trust List](#)
-  [Certificate Revocation Lists](#)
-  [Generate Certificate Signing Request](#)
-  [Generate Self-Signed Certificate](#)

Cancel

9. انقر على تثبيت شهادة ACS.

System Configuration

Edit

Install ACS Certificate

Install new certificate 

Read certificate from file

Certificate file

Use certificate from storage

Certificate CN

Private key file

Private key password

10. اختر استخدام الشهادة من التخزين واكتب اسم المجال المؤهل بالكامل ل Cisco_w2003.wirelessdemo.local (أو ACS.wirelessdemo.local إذا كنت تستخدم ACS كاسم).

System Configuration

Edit

Install ACS Certificate


Install new certificate 	
<input type="radio"/> Read certificate from file	
Certificate file	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
Certificate CN	<input type="text" value="cisco_w2003.wirelessdemo.local"/>
Private key file	<input type="text"/>
Private key password	<input type="text"/>

11. انقر على إرسال.

System Configuration

Edit

Install ACS Certificate


Installed Certificate Information 	
Issued to:	cisco_w2003.wirelessdemo.local
Issued by:	wirelessdemoca
Valid from:	March 17 2006 at 08:33:25
Valid to:	March 16 2008 at 08:33:25
Validity:	OK


The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.


12. طقطقة نظام تشكيل.
13. انقر فوق التحكم في الخدمة ثم انقر فوق إعادة

System Configuration

Select

CiscoSecure ACS on cisco_w2003 
Is Currently Running

Services Log File Configuration 
<p>Level of detail</p> <p><input type="radio"/> None</p> <p><input checked="" type="radio"/> Low</p> <p><input type="radio"/> Full</p> <p>Generate New File</p> <p><input checked="" type="radio"/> Every day</p> <p><input type="radio"/> Every week</p> <p><input type="radio"/> Every month</p> <p><input type="radio"/> When size is greater than <input type="text" value="2048"/> KB</p> <p><input type="checkbox"/> Manage Directory</p> <p><input type="radio"/> Keep only the last <input type="text" value="7"/> files</p> <p><input checked="" type="radio"/> Delete files older than <input type="text" value="7"/> days</p>

 [Back to Help](#)

14. طقطقة نظام تشكيل.
15. انقر على إعداد المصادقة العامة.
16. حدد السماح ب EAP-TLS وجميع المربعات التي تحته.

System Configuration

Global Authentication Setup

EAP Configuration

PEAP

Allow EAP-MSCHAPV2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

17. انقر فوق إرسال + إعادة تشغيل.

18. طقطقة نظام تشكيل.

19. انقر على إعداد مرجع مصدق ACS.

20. تحت نافذة "إعداد مرجع مصدق ACS"، اكتب اسم وموقع ملف cer.* الذي تم إنشاؤه سابقاً. في هذا المثال،

ملف cer.* الذي تم إنشاؤه هو ACS.CER في الدليل الجذر c:\.

21. اكتب c:\acs.cer في حقل ملف شهادة CA وانقر

إرسال.

System Configuration

Edit

ACS Certification Authority Setup

CA Operations	
Add new CA certificate to local certificate storage	
CA certificate file	<input type="text" value="c:\acs.cer"/>

System Configuration

ACS Certification Authority Setup	
CA Operations	
Add new CA certificate to local certificate storage	
CA certificate file	<input type="text" value="c:\acs.cer"/>
The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.	

New CA certificate is successfully added into the global system certificate storage.	
CA certificate common name	wirelessdemo.ca

22. أعد تشغيل خدمة ACS.

تكوين العميل ل EAP-TLS باستخدام Windows Zero Touch

العميل هو كمبيوتر يعمل بنظام التشغيل Windows XP Professional باستخدام SP2 الذي يعمل كعميل لاسلكي ويحصل على حق الوصول إلى موارد إنترنت من خلال نقطة الوصول اللاسلكية. أكمل الإجراءات الواردة في هذا القسم لتكوين العميل كعميل لاسلكي.

إجراء عملية تثبيت وتهيئة أساسية

أكمل الخطوات التالية:

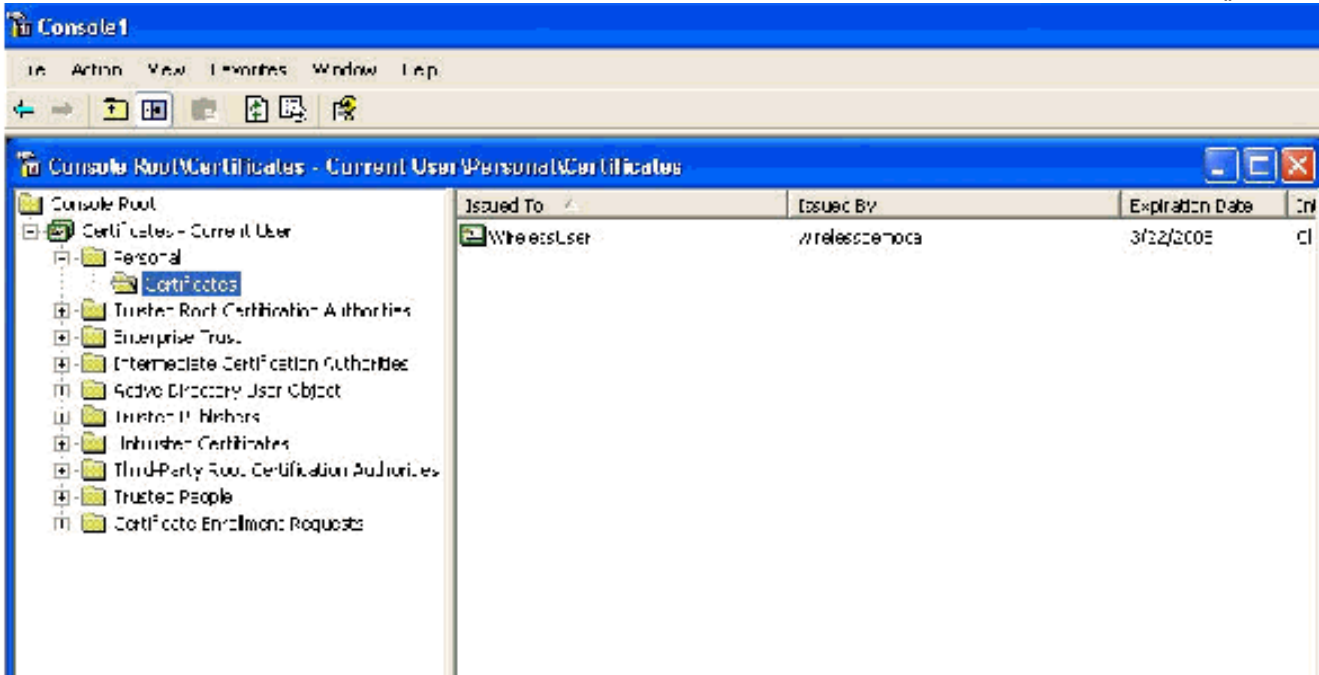
1. توصيل Client بمقطع شبكة إنترنت باستخدام كبل إيثرنت متصل بالمحول.
2. على العميل، قم بتثبيت Windows XP Professional مع SP2 ككمبيوتر عضو يسمى Client على المجال wirelessdemo.local.
3. قم بتثبيت Windows XP Professional مع SP2. يجب تثبيت هذا للحصول على دعم EAP-TLS و PEAP. ملاحظة: يتم تشغيل جدار حماية Windows تلقائياً في Windows XP Professional مع SP2. عدم إيقاف تشغيل جدار الحماية.

تكوين توصيل الشبكة اللاسلكية

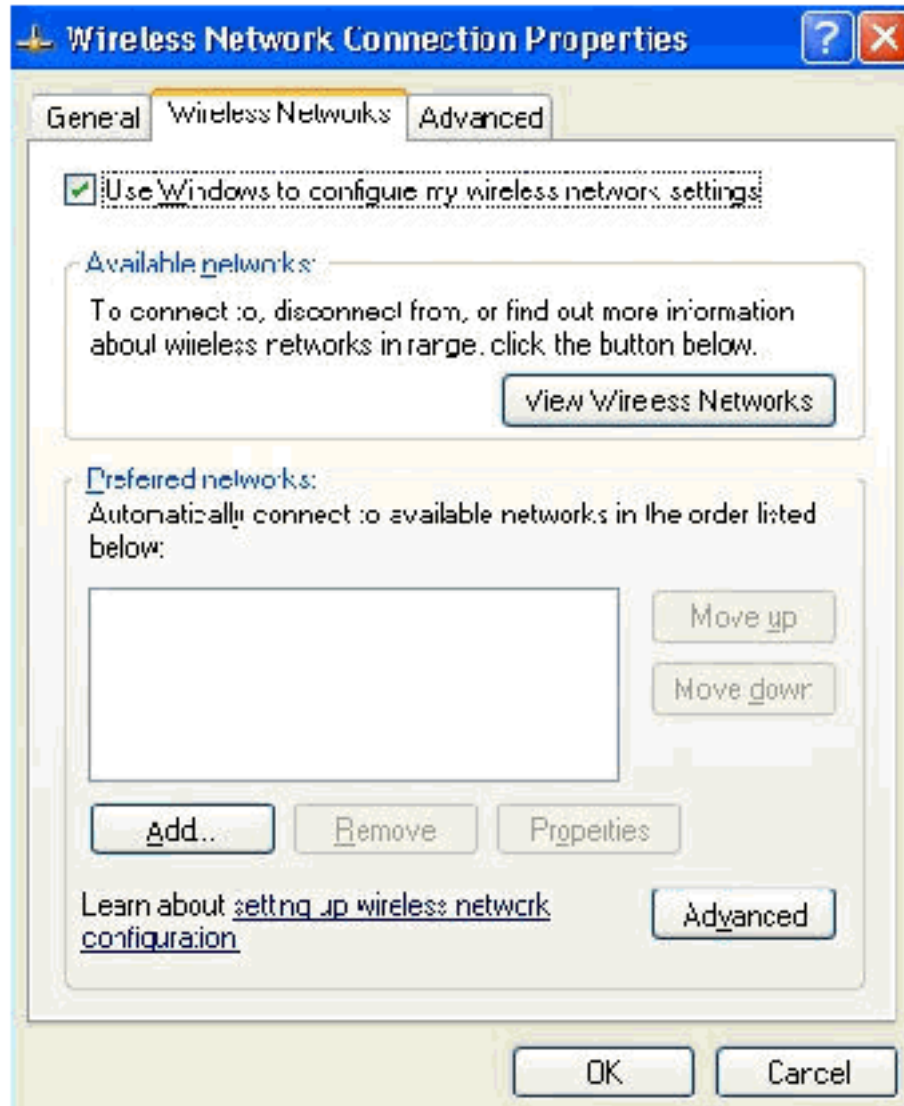
أكمل الخطوات التالية:

1. قم بتسجيل الخروج ثم تسجيل الدخول باستخدام حساب WirelessUser في المجال WirelessDemo.local. ملاحظة: تحديث إعدادات نهج مجموعة تكوين الكمبيوتر والمستخدمين والحصول على

شهادة كمبيوتر وشهادة مستخدم لكمبيوتر العميل اللاسلكي فوراً، وذلك بكتابة **Gpupdate** في موجه الأوامر. وإلا، عندما تقوم بتسجيل الخروج ثم تسجيل الدخول، فإنه يؤدي نفس وظيفة **Gpupdate**. يجب تسجيل الدخول إلى المجال من خلال الاتصال عبر السلك. ملاحظة: للتحقق من تثبيت الشهادة تلقائياً على العميل، افتح MMC للشهادة وتحقق من توفر شهادة WirelessUser في مجلد الشهادات الشخصية.

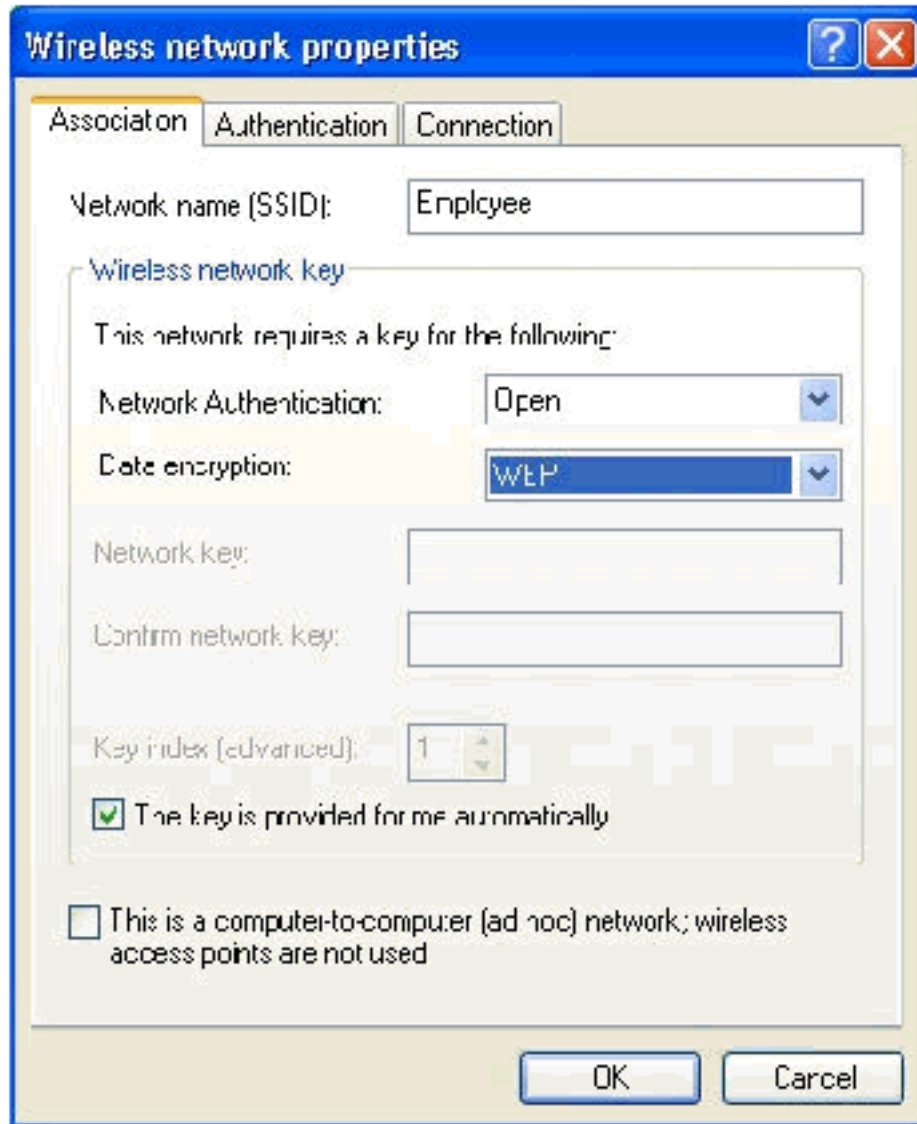


2. أختار ابدأ < لوحة التحكم، وانقر نقرًا مزدوجًا فوق إتيصالات الشبكة، ثم انقر بزر الماوس الأيمن على اتصال الشبكة اللاسلكية.
3. انقر على خصائص، انتقل إلى علامة التبويب الشبكات اللاسلكية، وتأكد من أن Windows الخاص بالمستخدم لتكوين إعدادات الشبكة اللاسلكية



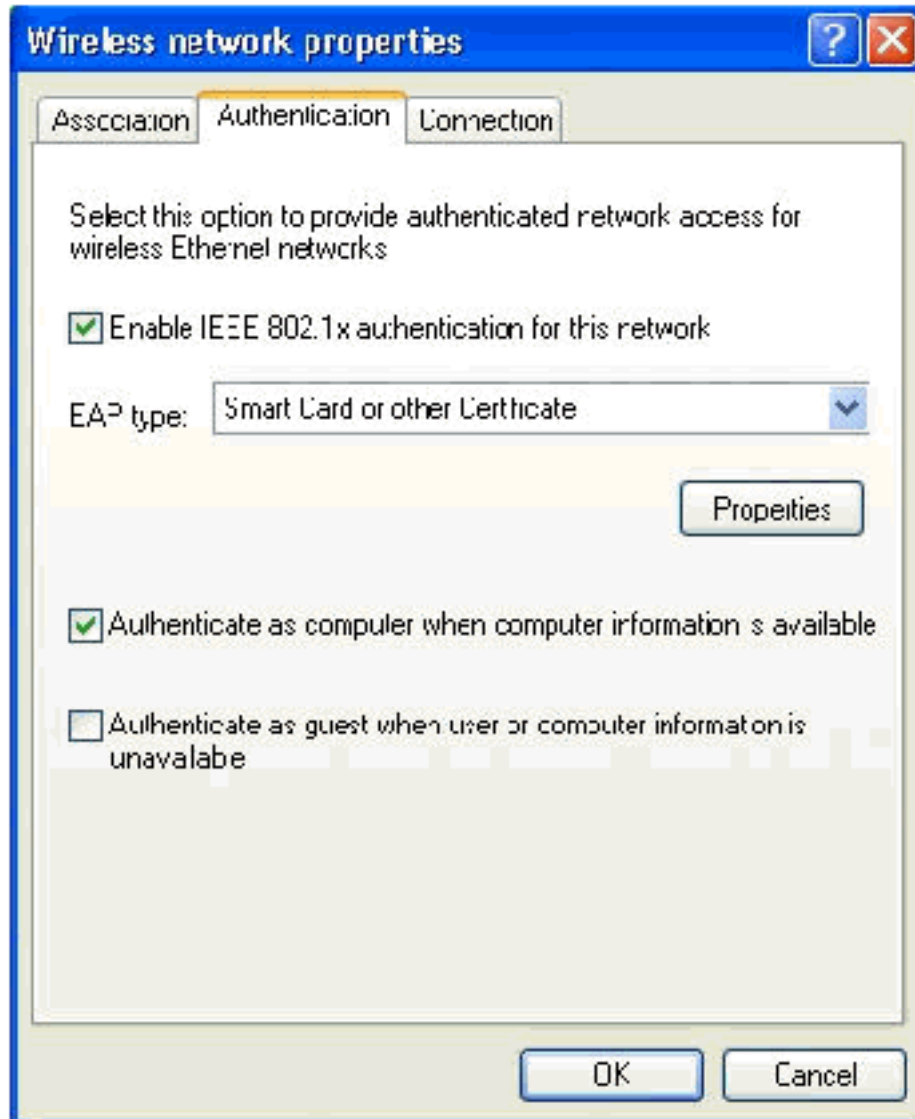
محدد.

4. انقر فوق إضافة (Add).
5. انتقل إلى علامة تبويب الاقتران، واكتب الموظف في حقل اسم الشبكة (SSID).
6. تأكد من تعيين تشفير البيانات على WEP ومن توفير المفتاح لي



تلقائياً.

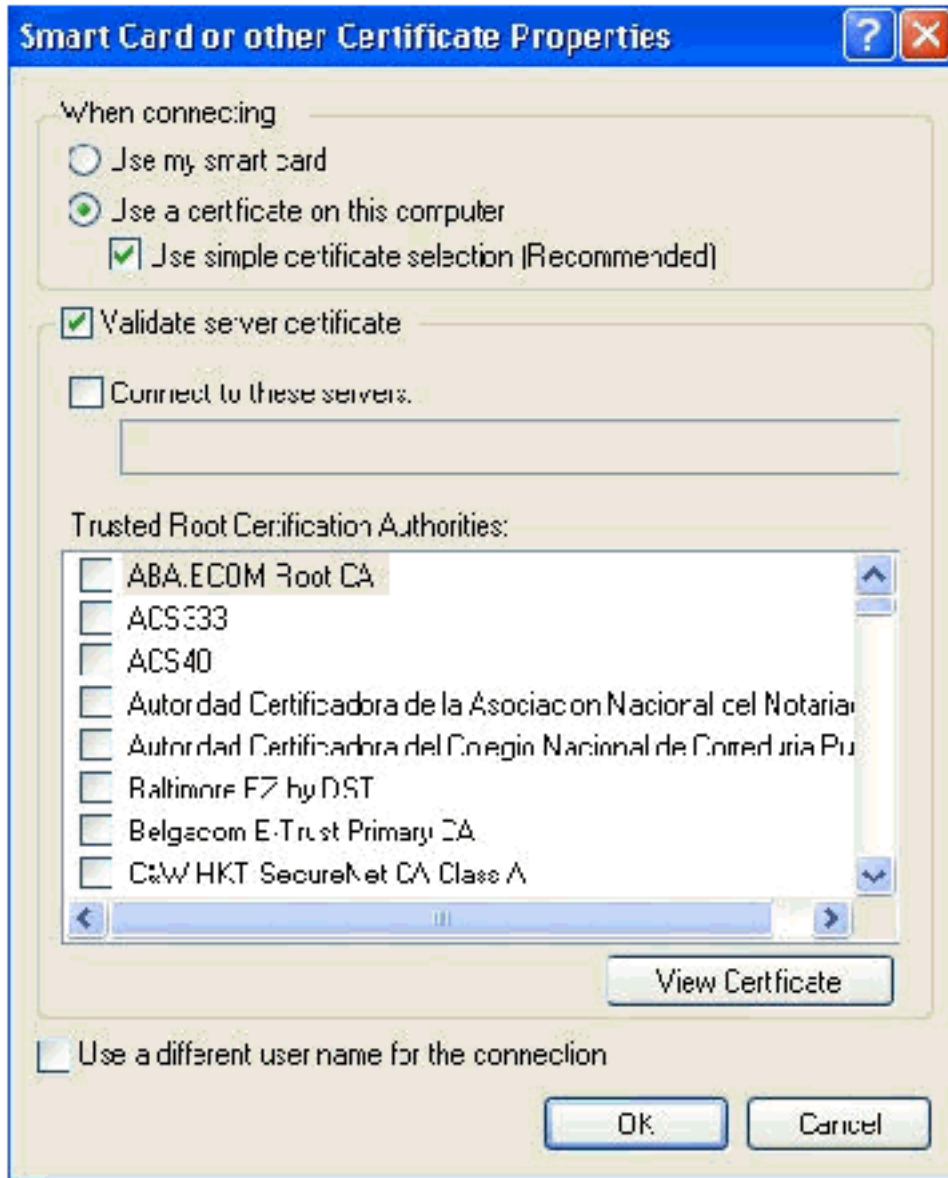
7. انتقل إلى علامة تبويب المصادقة.
8. تحقق من تكوين نوع EAP لاستخدام البطاقة الذكية أو شهادة أخرى. إذا لم يكن كذلك، فحدده من القائمة المنسدلة.
9. إذا كنت تريد مصادقة الجهاز قبل تسجيل الدخول (مما يسمح بتطبيق برامج تسجيل الدخول النصية أو نهج المجموعة) اختر الخيار مصادقة كجهاز كمبيوتر عند توفر معلومات



الكمبيوتر.

10. انقر فوق خصائص.

11. تأكد من تحديد المربعات الموجودة في هذه

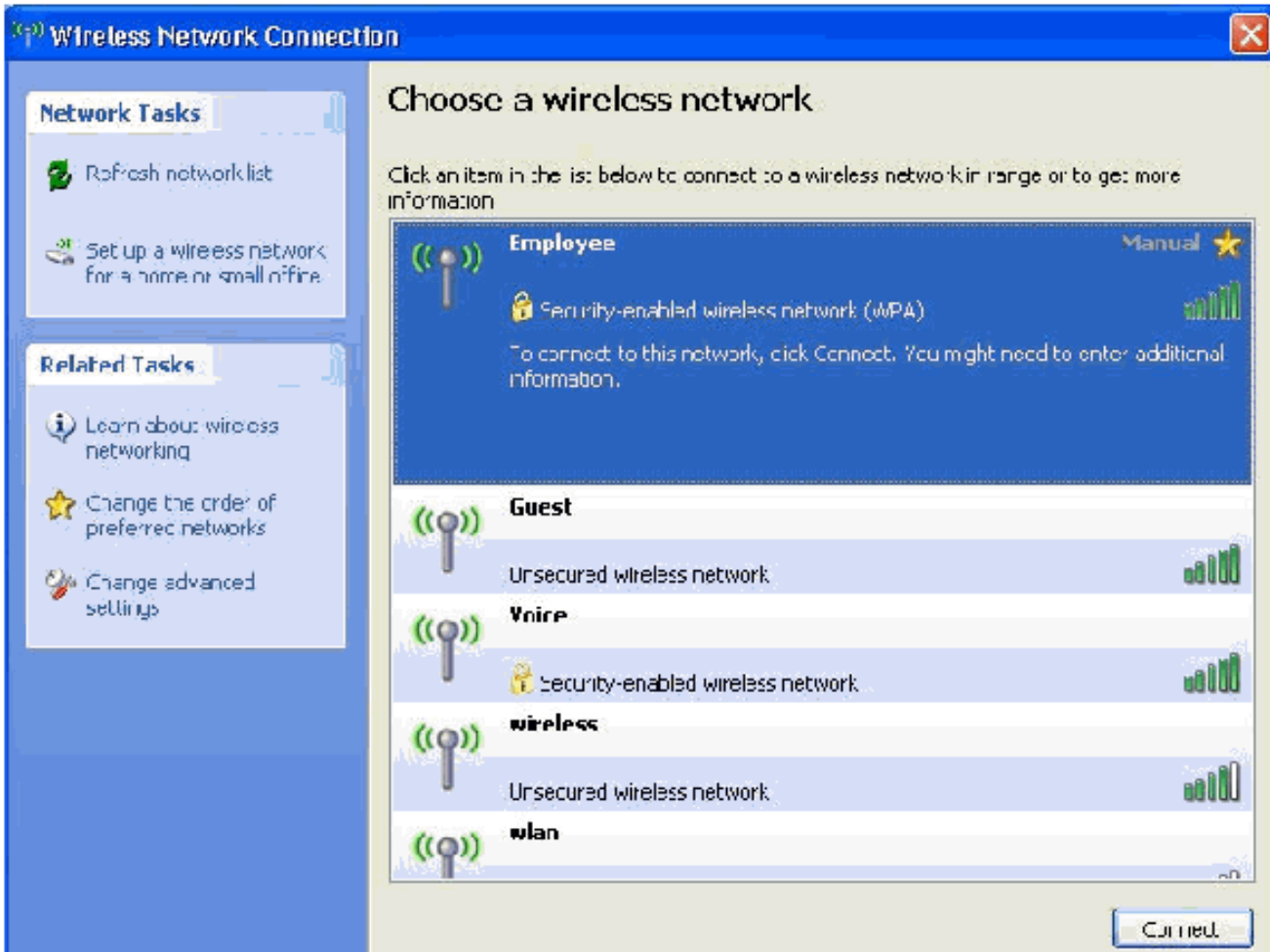


النافذة.

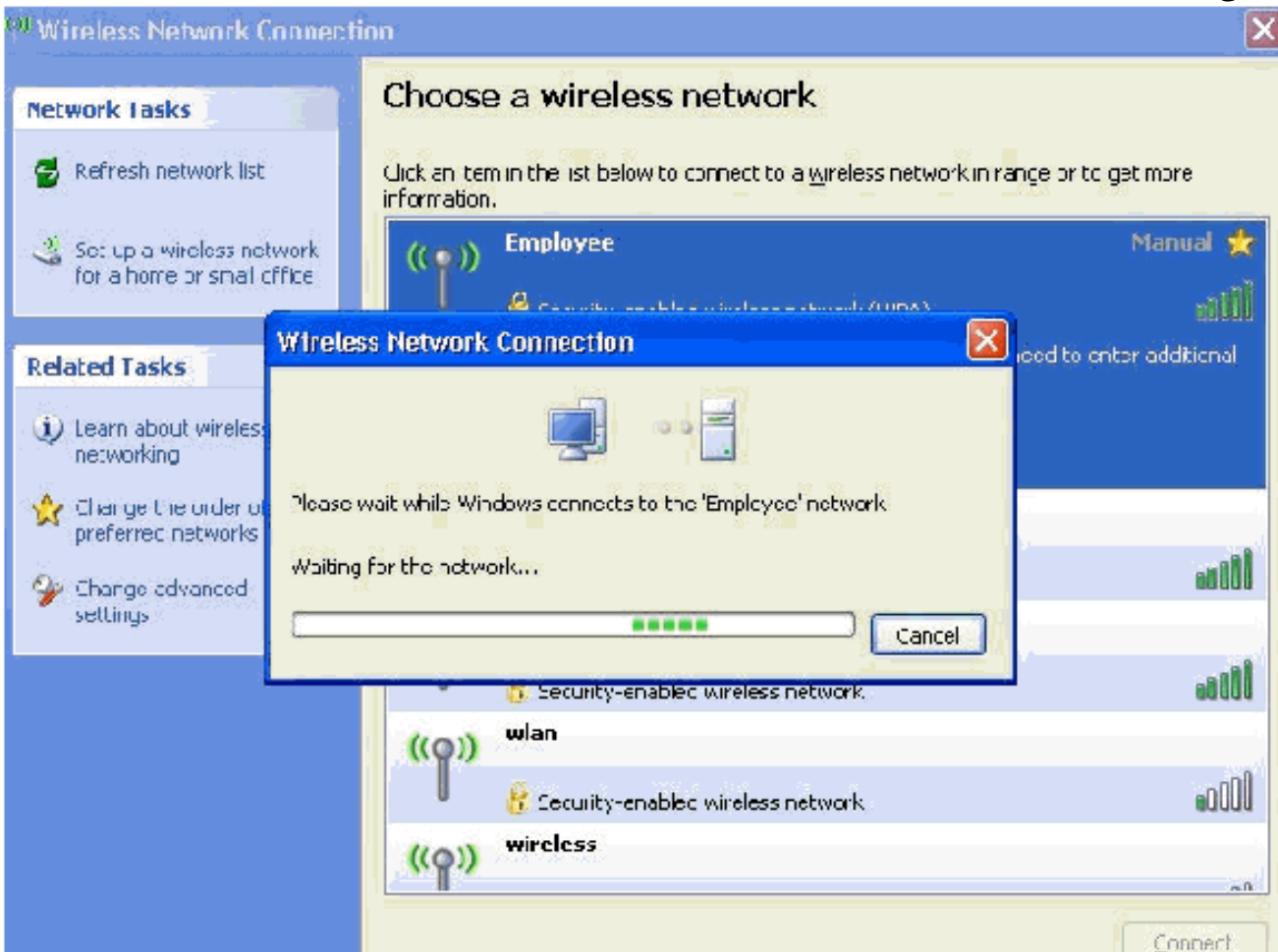
12. وانقر فوق OK ثلاث مرات.

13. انقر بزر الماوس الأيمن على رمز توصيل الشبكة اللاسلكية في النظام ثم انقر على عرض الشبكات اللاسلكية المتاحة.

14. انقر على شبكة الموظف اللاسلكية ثم انقر على توصيل.



تشير لقطات الشاشة هذه إلى ما إذا تم إكمال الاتصال بنجاح.



Wireless Network Connection

Choose a wireless network

Click on an item in the list below to connect to a wireless network in range or to get more information.

Employee Attempting to authenticate

Security-enabled wireless network

wlan Security-enabled wireless network

wireless Security-enabled wireless network

Disconnect

Wireless Network Connection

Please wait while Windows connects to the 'Employee' network.

Waiting for network to be ready...

Cancel

Wireless Network Connection

Choose a wireless network

Click on an item in the list below to connect to a wireless network in range or to get more information.

Employee Acquiring network address

Security-enabled wireless network (WPA)

wireless Unsecured wireless network

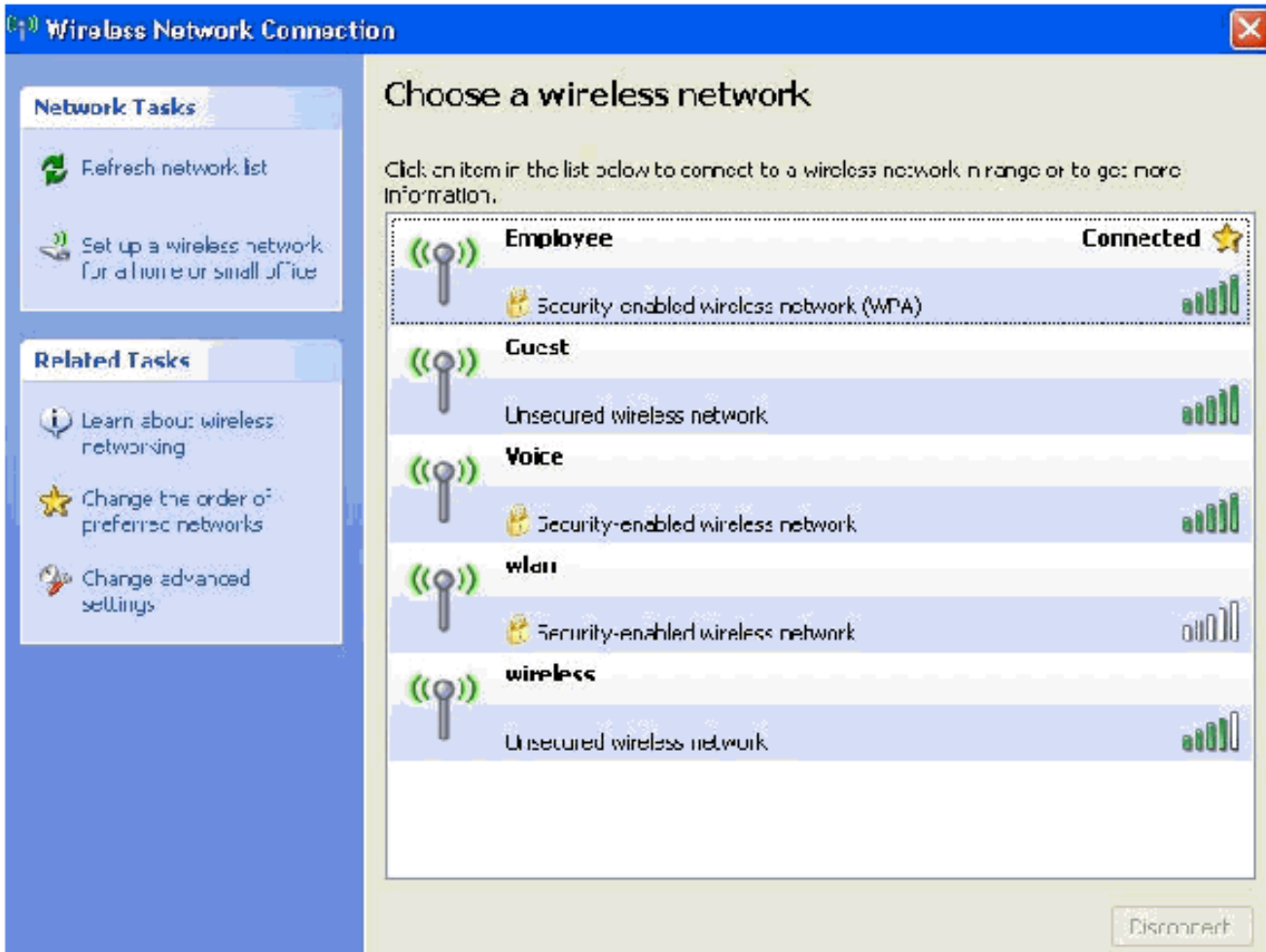
Disconnect

Wireless Network Connection

Please wait while Windows connects to the 'Employee' network.

Waiting for network to be ready...

Cancel



15. بعد نجاح المصادقة، تحقق من تكوين TCP/IP للمهايئ اللاسلكي باستخدام توصيلات الشبكة. يجب أن يكون له نطاق عنوان 172.16.100.100-172.16.100.254 من نطاق DHCP أو النطاق الذي تم إنشاؤه للعملاء اللاسلكي.

16. لاختبار الوظائف، افتح متصفح وتصفح حتى <http://wirelessdemo.ca> (أو عنوان IP الخاص بخادم (Enterprise CA).

معلومات ذات صلة

- مصادقة EAP باستخدام مثال تكوين وحدات التحكم في الشبكة المحلية اللاسلكية (WLC)
- دليل تكوين وحدة تحكم في الشبكة المحلية (LAN) اللاسلكية
- مثال التكوين الأساسي لنقطة الوصول في الوضع Lightweight ووحدة تحكم الشبكة المحلية (LAN) اللاسلكية
- مثال على تكوين شبكات VLAN على وحدات تحكم الشبكة المحلية اللاسلكية
- مجموعة AP VLANs مع لاسلكي lan جهاز تحكم تشكيل مثال
- 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 ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال 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 ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه 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