Windows 2003 و ACS 5.1 عم UWNs تحت PEAP Server

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين الوصول اللاسلكي الآمن باستخدام وحدات التحكم في الشبكة المحلية اللاسلكية

وبرنامج Microsoft Windows 2003 وخادم التحكم في الوصول الآمن (ACS 5.1) من Cisco عبر بروتوكول المصادقة المتوسع المحمي (PEAP) مع بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي ل Microsoft (MS-CHAP) الإصدار 2.

ملاحظة: للحصول على معلومات حول نشر الاتصال اللاسلكي الآمن، راجع موقع Microsoft Wi-Fi على الويب ومخطط Cisco SAFE اللاسلكي.

المتطلبات الأساسية

المتطلبات

هناك افتراض بأن المثبت لديه معرفة بتثبيت Windows 2003 الأساسي وتثبيت Cisco Wireless LAN Controller حيث إن هذا المستند يغطي فقط التكوينات المحددة لتسهيل الاختبارات.

للحصول على معلومات التثبيت الأولي ومعلومات التكوين لوحدات التحكم من السلسلة Cisco 5508 Series، ارجع إلى دليل تثبيت وحدة التحكم اللاسلكية من السلسلة Cisco 5500 Series. للحصول على معلومات التثبيت الأولي ومعلومات التكوين لوحدات التحكم من السلسلة Cisco 2100 Series، ارجع إلى دليل البدء السريع: وحدة التحكم في الشبكة المحلية اللاسلكية من السلسلة Cisco 2100 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.

يستخدم Windows Server 2003 المزود بحزمة الخدمة Enterprise Edition، SP1 لتكوين التسجيل التلقائي لشهادات المستخدم ومحطة العمل لمصادقة PEAP. يعمل التسجيل التلقائي للشهادة والتجديد التلقائي على تسهيل نشر الشهادات وتحسين الأمان من خلال إنهاء الشهادات وتجديدها تلقائيا.

المكونات المستخدمة

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

- وحدة التحكم Cisco 2106 أو Series Controller 5508 التي تشغل الإصدار 7.0.98.0
- نقطة الوصول Cisco 1142 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise مع تثبيت Internet Information Server (IIS) و Certificate Authority (CA) و DHCP ونظام اسم المجال (DNS)
- جهاز نظام التحكم بالوصول الآمن (ACS 5.1121) من Cisco
- Windows XP Professional مع SP (وحزم الخدمة المحدثة) وبطاقة واجهة الشبكة اللاسلكية (NIC) (مع دعم CCX v3) أو طالب من طرف ثالث.
- المحول Cisco 3750 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.

التكوين

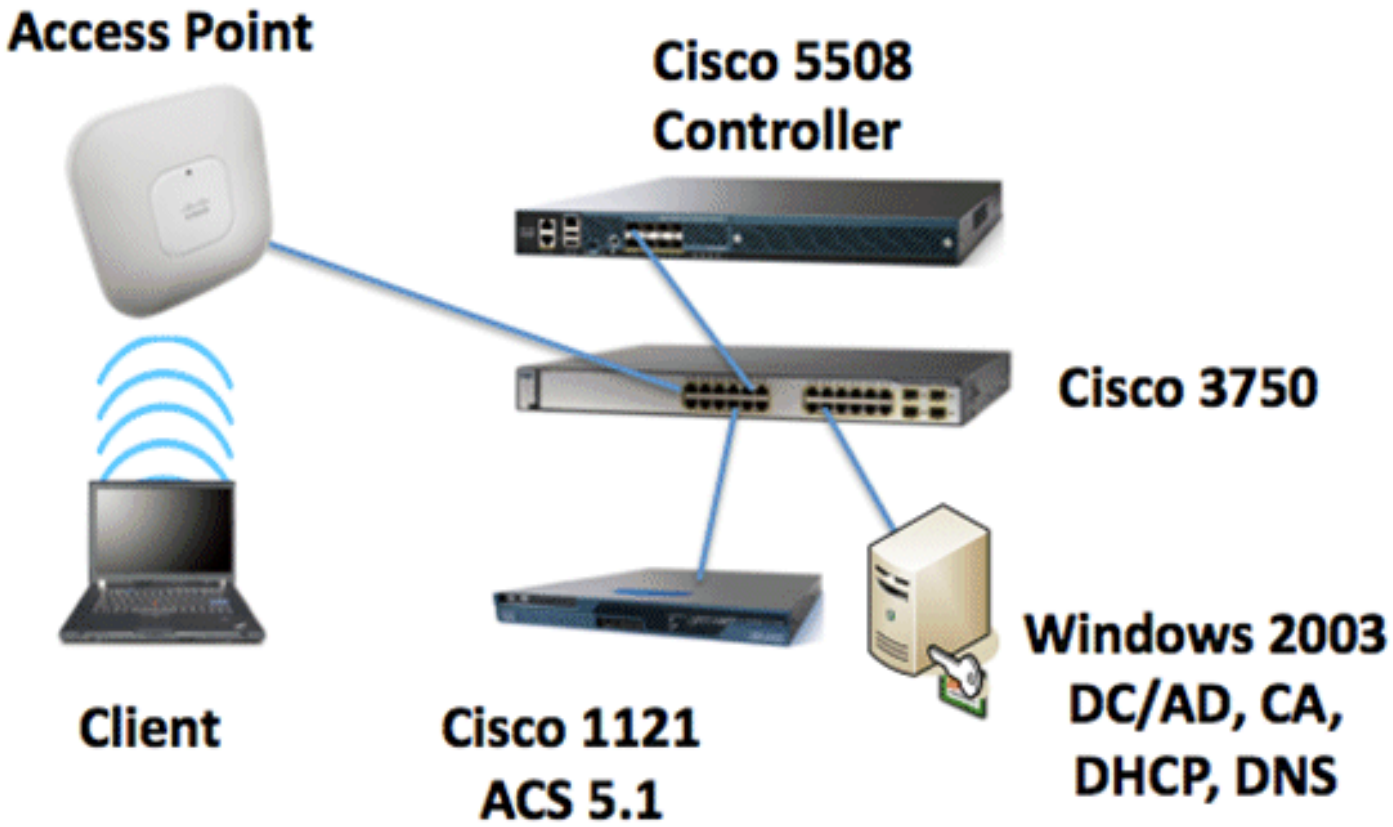
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

طبولوجيا المختبرات اللاسلكية الآمنة من Cisco



الغرض الأساسي من هذا المستند هو توفير إجراء مفصل خطوة بخطوة لتنفيذ PEAP تحت شبكات لاسلكية موحدة مع ACS 5.1 و Windows 2003 Enterprise Server. ينصب التركيز الرئيسي على التسجيل التلقائي للعميل حتى يتمكن العميل من التسجيل التلقائي ويأخذ الشهادة من الخادم.

ملاحظة: من أجل إضافة Wi-Fi Protected Access (WPA)/WPA2 مع بروتوكول سلامة المفاتيح المؤقتة (TKIP)/معيار التشفير المتقدم (AES) إلى Windows XP Professional مع SP، راجع تحديث عنصر معلومات خدمات الإمداد اللاسلكي (WPS IE) ل Windows XP مع Service Pack 2 .

إعداد Windows Enterprise 2003 باستخدام IIS ومرجع الشهادات و DNS و DHCP (CA)

CA (ديموكا)

CA هو كمبيوتر يعمل بنظام التشغيل Windows Server 2003 المزود بحزمة الخدمة SP2، Enterprise Edition، ويقوم بأداء الأدوار التالية:

- وحدة تحكم بالمجال لمجال **العرض التوضيحي.local** الذي يشغل IIS
- خادم DNS لمجال DNS **التجريبي**.local
- خادم DHCP
- المرجع المصدق الجذر للمؤسسة لمجال **العرض التوضيحي.local**

أنجزت هذا steps in order to شكلت CA ل هذا خدمة:

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 المستخدمين السلكين.
13. إضافة أجهزة كمبيوتر عميلة إلى مجموعة المستخدمين السلكين.

إجراء عمليات التثبيت والتكوين الأساسية

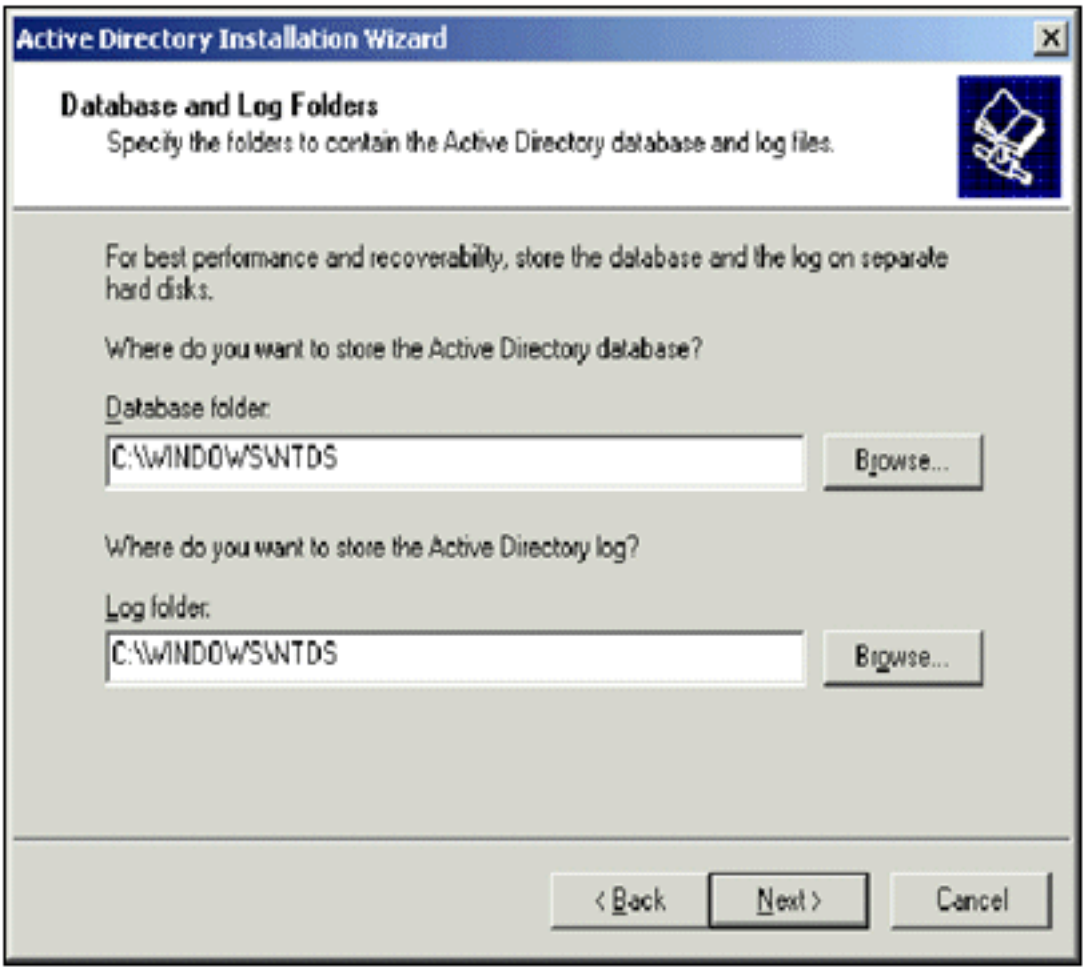
قم بإجراء هذه الخطوات:

1. قم بتثبيت Windows Server 2003 باستخدام Enterprise Edition، SP2 كخادم مستقل.
2. قم بتكوين بروتوكول TCP/IP باستخدام عنوان *10.0.10.10* IP وقناع الشبكة الفرعية *255.255.255.0*.

تكوين الكمبيوتر كوحدة تحكم بالمجال

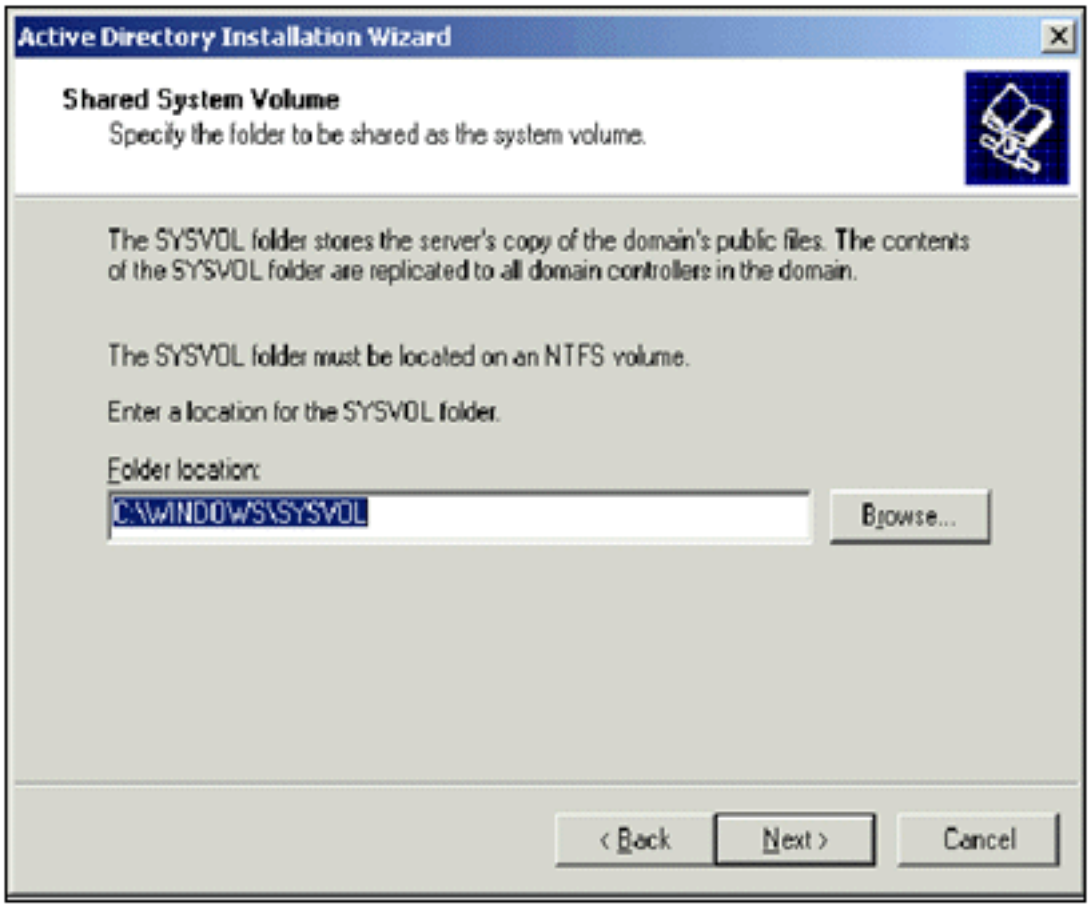
قم بإجراء هذه الخطوات:

1. لبدء معالج تثبيت Active Directory، أختر **Start > Run**، **اكتب dcpromo.exe**، وانقر فوق **OK**.
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 **التالي**.
7. في صفحة اسم المجال الجديد، اكتب **demo.local** وانقر **بعد ذلك**.
8. في صفحة اسم مجال NetBIOS، أدخل اسم المجال NetBIOS كعرض **توضيحي** وانقر **بعد ذلك**.
9. في صفحة مواقع "قاعدة البيانات" و"مجلدات السجل"، اقبل الدلائل الافتراضية "لمجلدات قاعدة البيانات" و"السجل" وانقر فوق



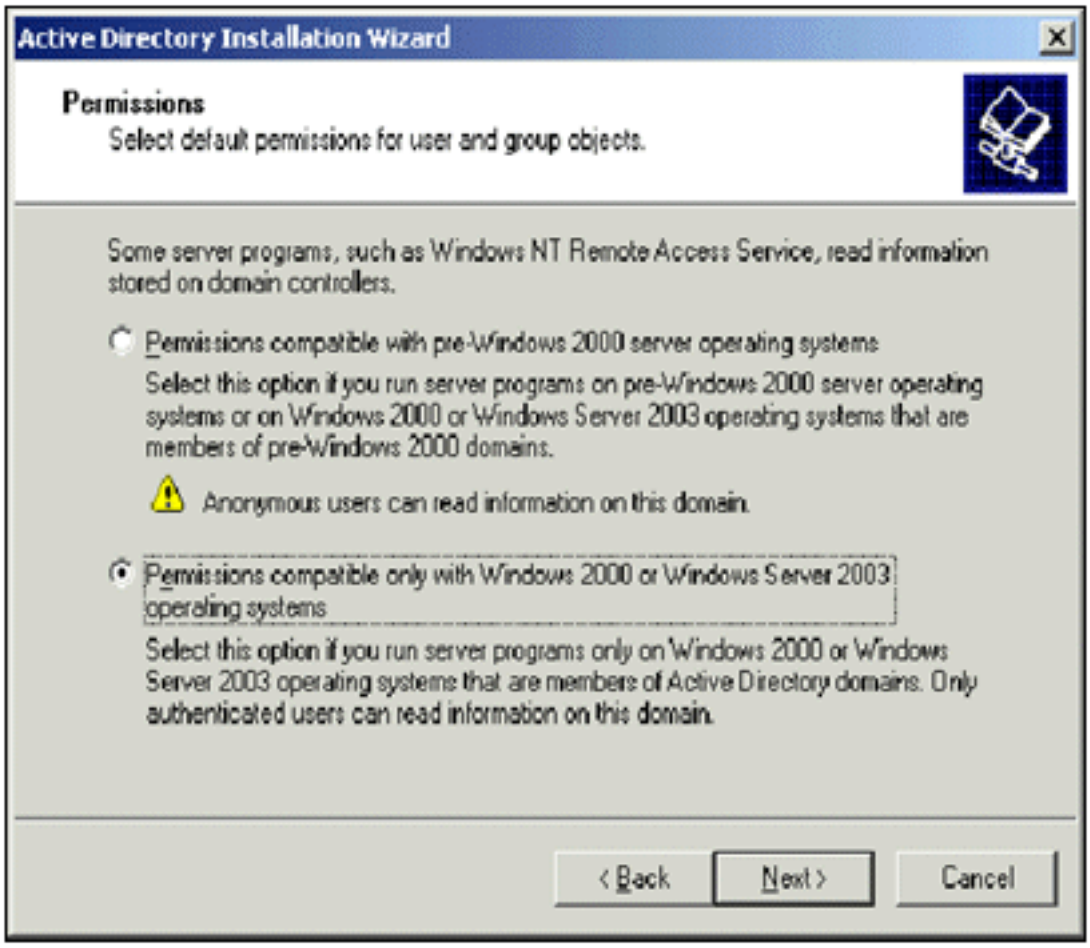
التالي.

10. في صفحة "وحدة تخزين النظام المشتركة"، تحقق من صحة موقع المجلد الافتراضي وانقر فوق



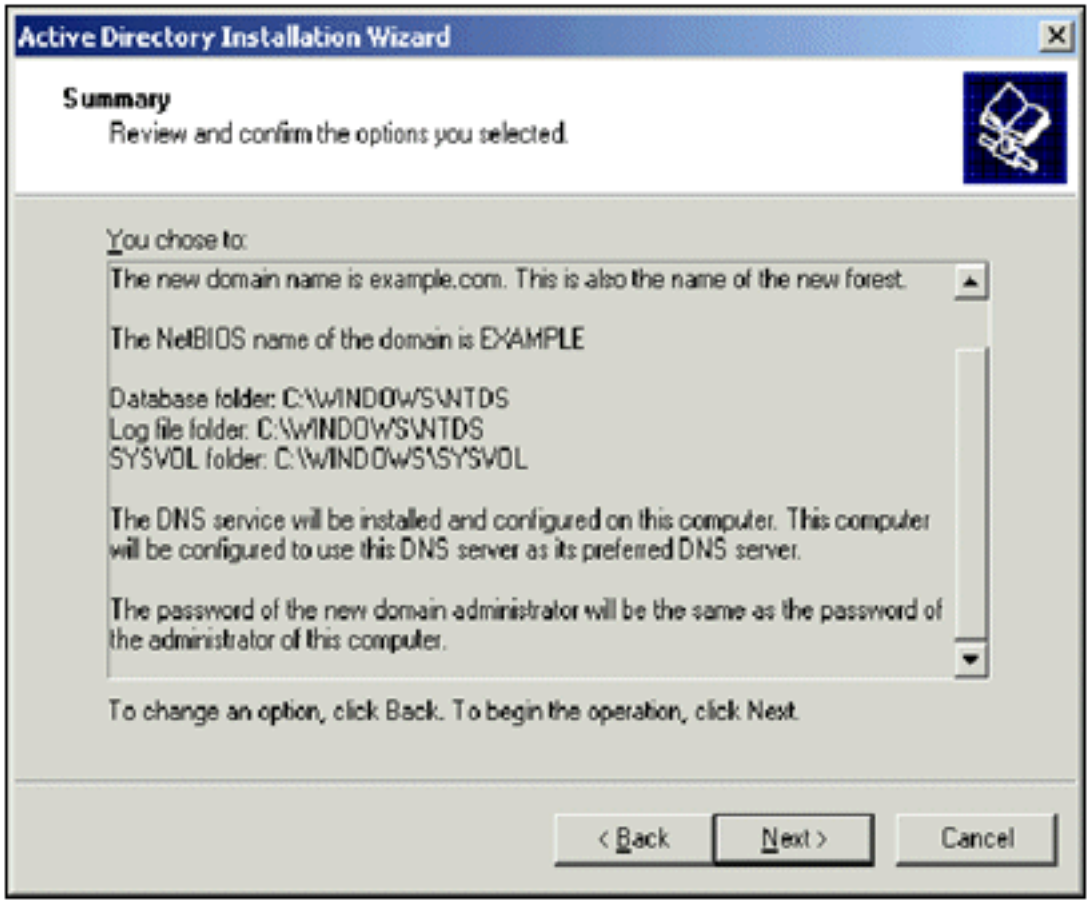
التالي.

11. في الصفحة أذون، تأكد 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.

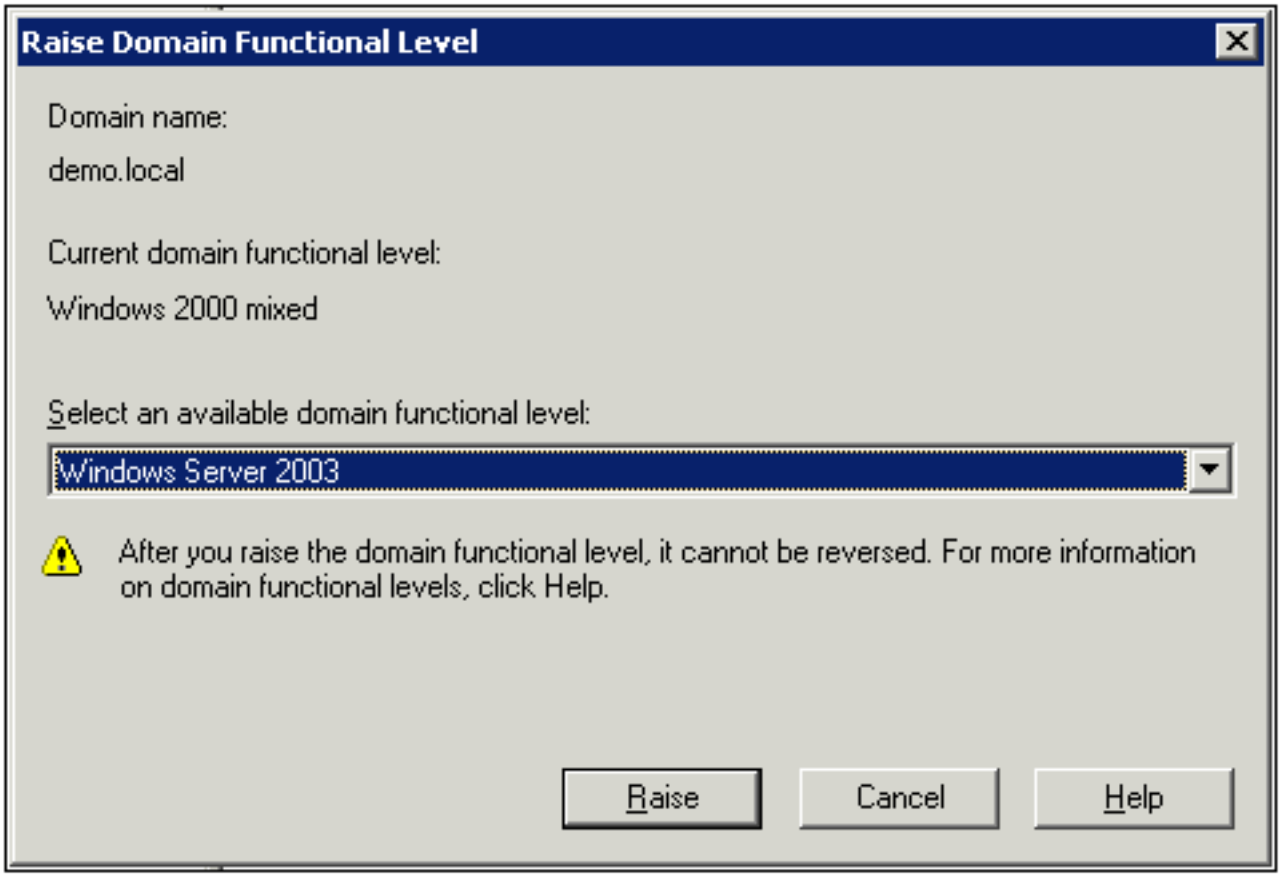
14. عند الانتهاء من تثبيت Active Directory، انقر فوق **إنهاء**.

15. عند المطالبة بإعادة تشغيل الكمبيوتر، انقر فوق **إعادة التشغيل الآن**.

رفع مستوى وظائف المجال

قم بإجراء هذه الخطوات:

1. افتح الأداة الإضافية Active Directory Domain و Trust من مجلد الأدوات الإدارية (ابدأ > برامج > أدوات إدارية > **مجالات Active Directory و Trust**)، ثم انقر بزر الماوس الأيمن فوق كمبيوتر المجال CA.Demo.Local.
2. انقر فوق **رفع المستوى الوظيفي للمجال**، ثم حدد **Windows Server 2003** في صفحة رفع المستوى الوظيفي للمجال.

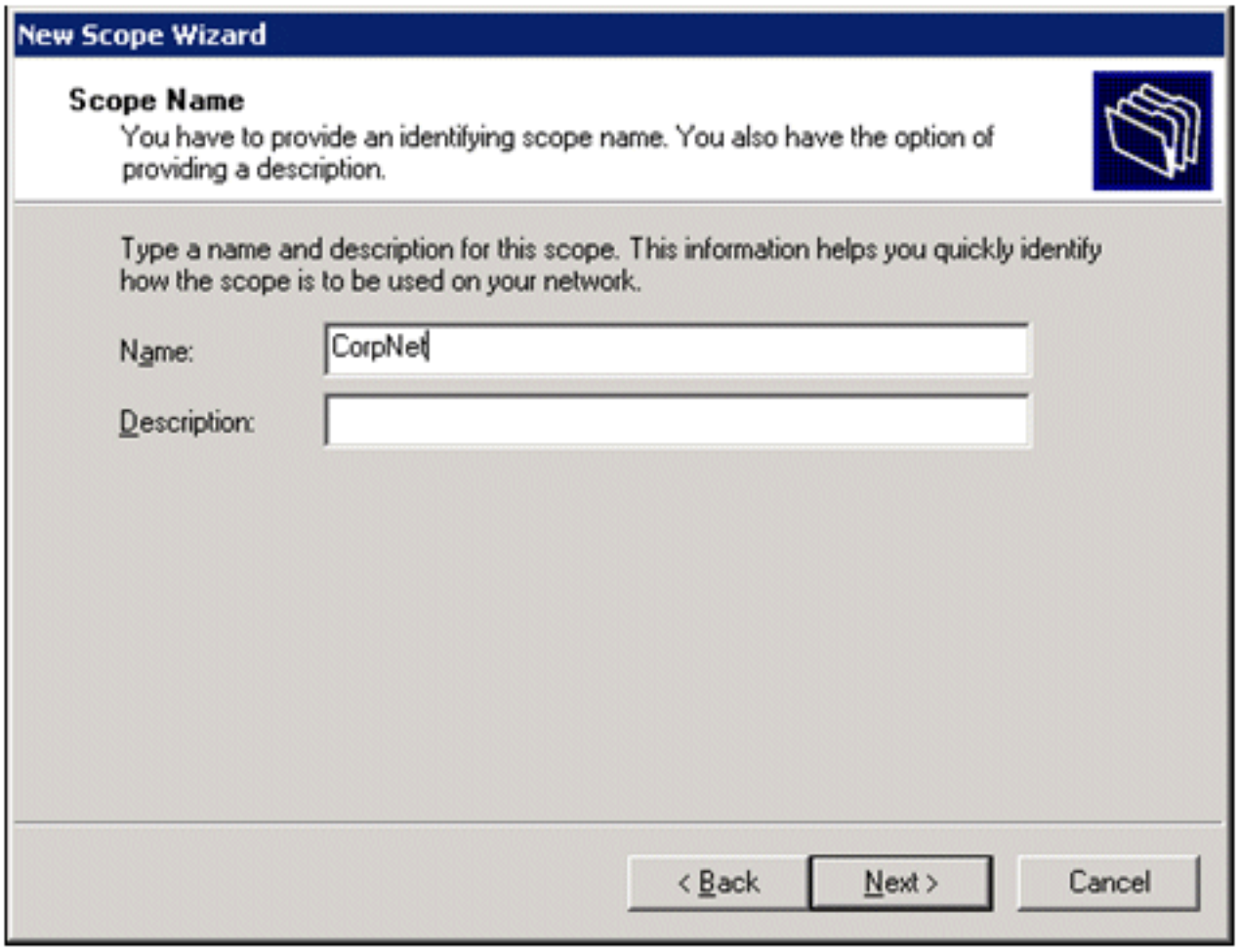


3. انقر فوق **رفع**، انقر فوق **موافق**، ثم انقر فوق **موافق** مرة أخرى.

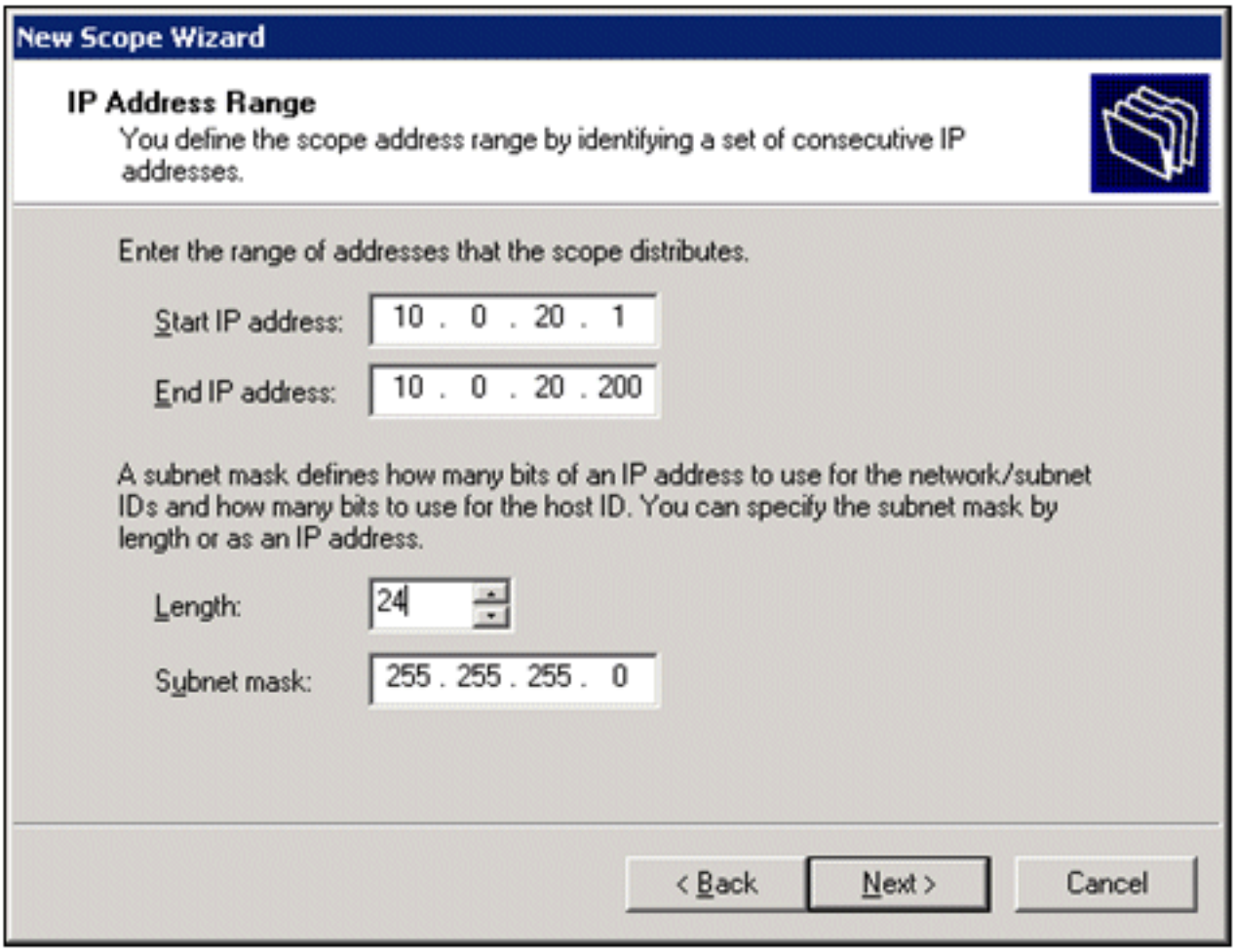
تثبيت DHCP وتكوينه

قم بإجراء هذه الخطوات:

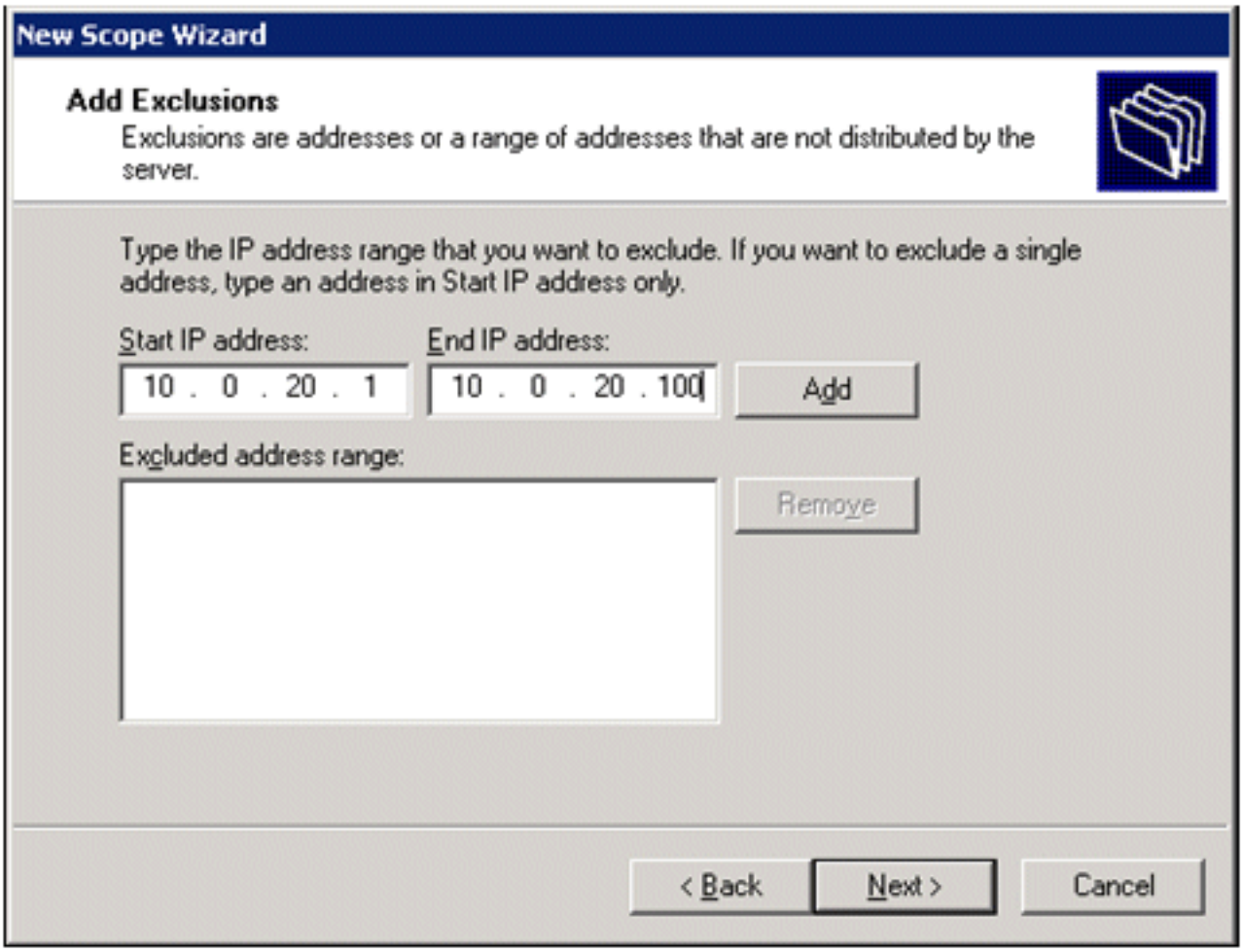
1. قم بتثبيت **بروتوكول التكوين الديناميكي للمضيف (DHCP)** كمكون **خدمة شبكة** باستخدام **إضافة أو إزالة برامج** في لوحة التحكم.
2. افتح الأداة الإضافية DHCP من مجلد الأدوات الإدارية (ابدأ > برامج > أدوات إدارية > **DHCP**)، ثم قم بتمييز خادم CA.demo.local، DHCP.
3. طقطقت **إجراء**، وبعد ذلك طقطقت **يخول** in order to خولت ال DHCP خدمة.
4. في شجرة وحدة التحكم، انقر بزر الماوس الأيمن فوق **CA.demo.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.



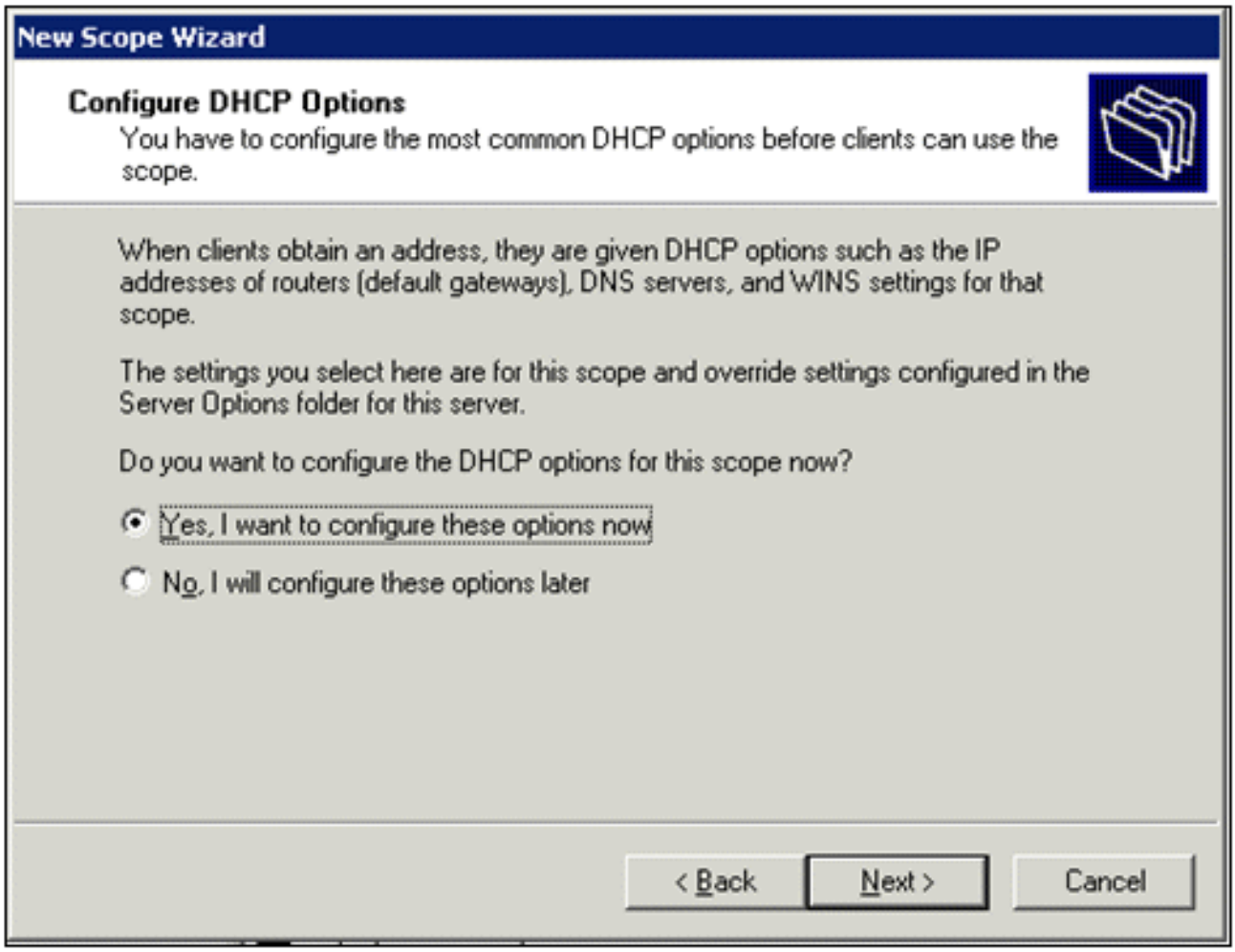
7. انقر فوق **التالي** وقم بتعبئة هذه المعلمات:عنوان Start IP - **10.0.20.1**نهاية عنوان IP - **10.0.20.200**الطول - **24**قناع الشبكة الفرعية - **255.255.255.0**



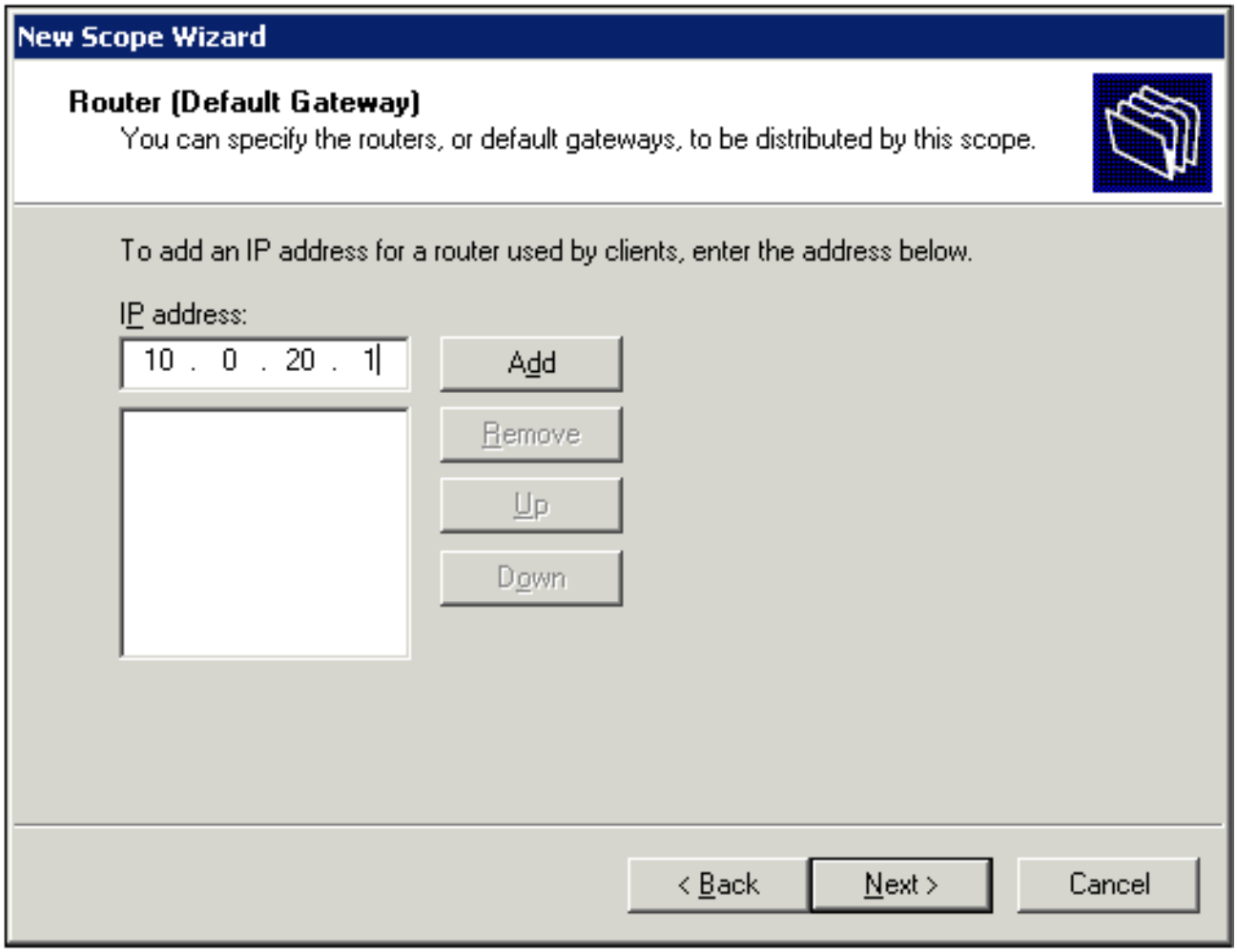
8. طقطقت **بعد ذلك** وأدخل *10.0.20.1* ل بداية عنوان و *10.0.20.100* ل النهاية عنوان أن يكون استثنيت. ثم انقر فوق **التالي**. يحجز هذا العنوان في النطاق من 10.0.20.1 إلى 10.0.20.100. لم يتم تخصيص عناوين IP الاحتياطية هذه من قبل خادم DHCP.



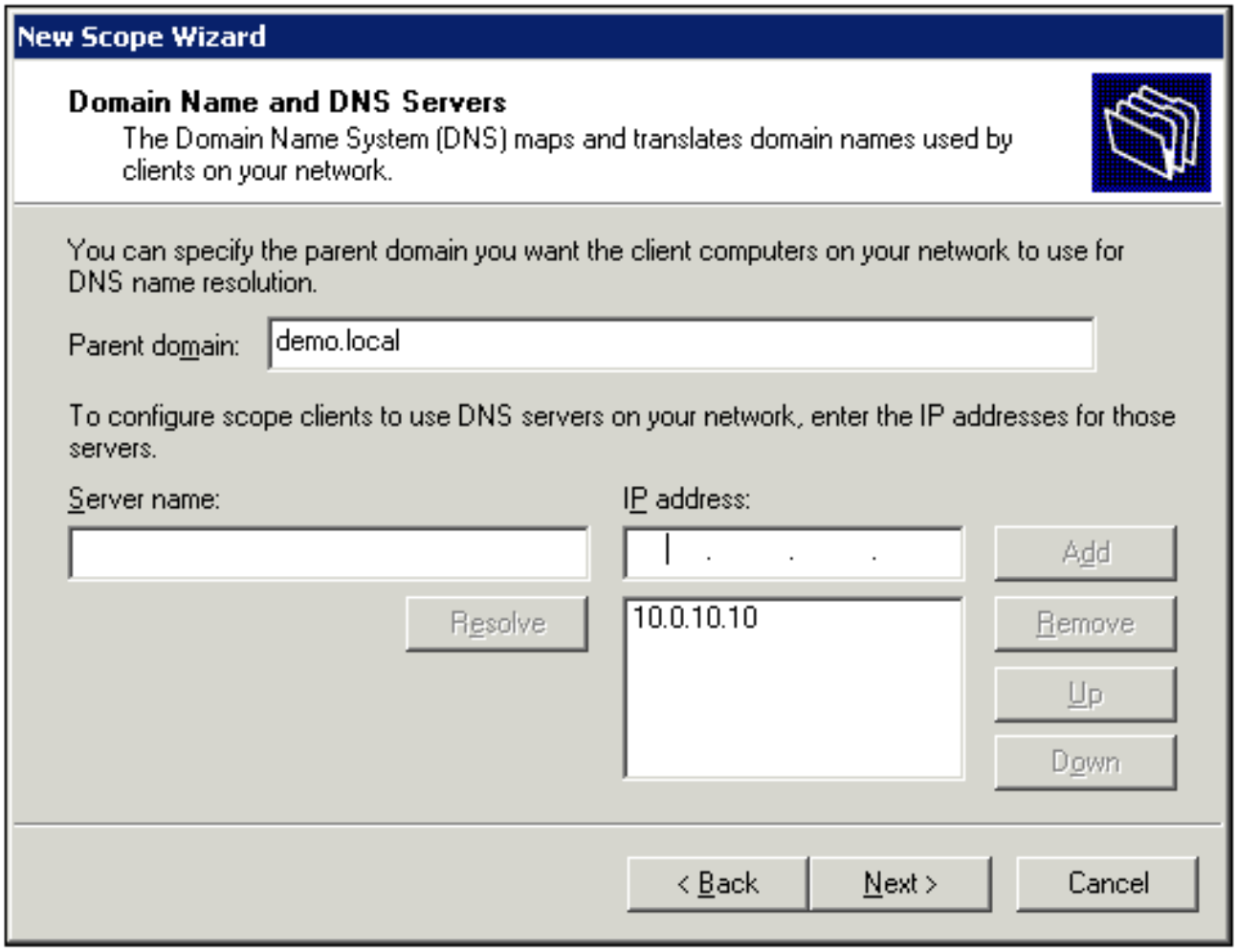
9. في صفحة مدة التأجير، انقر فوق **التالي**.
10. أخترت على ال configure DHCP خيار، **نعم، أنا أريد أن يشكل هذا خيار الآن** وطقطقة **بعد ذلك**.



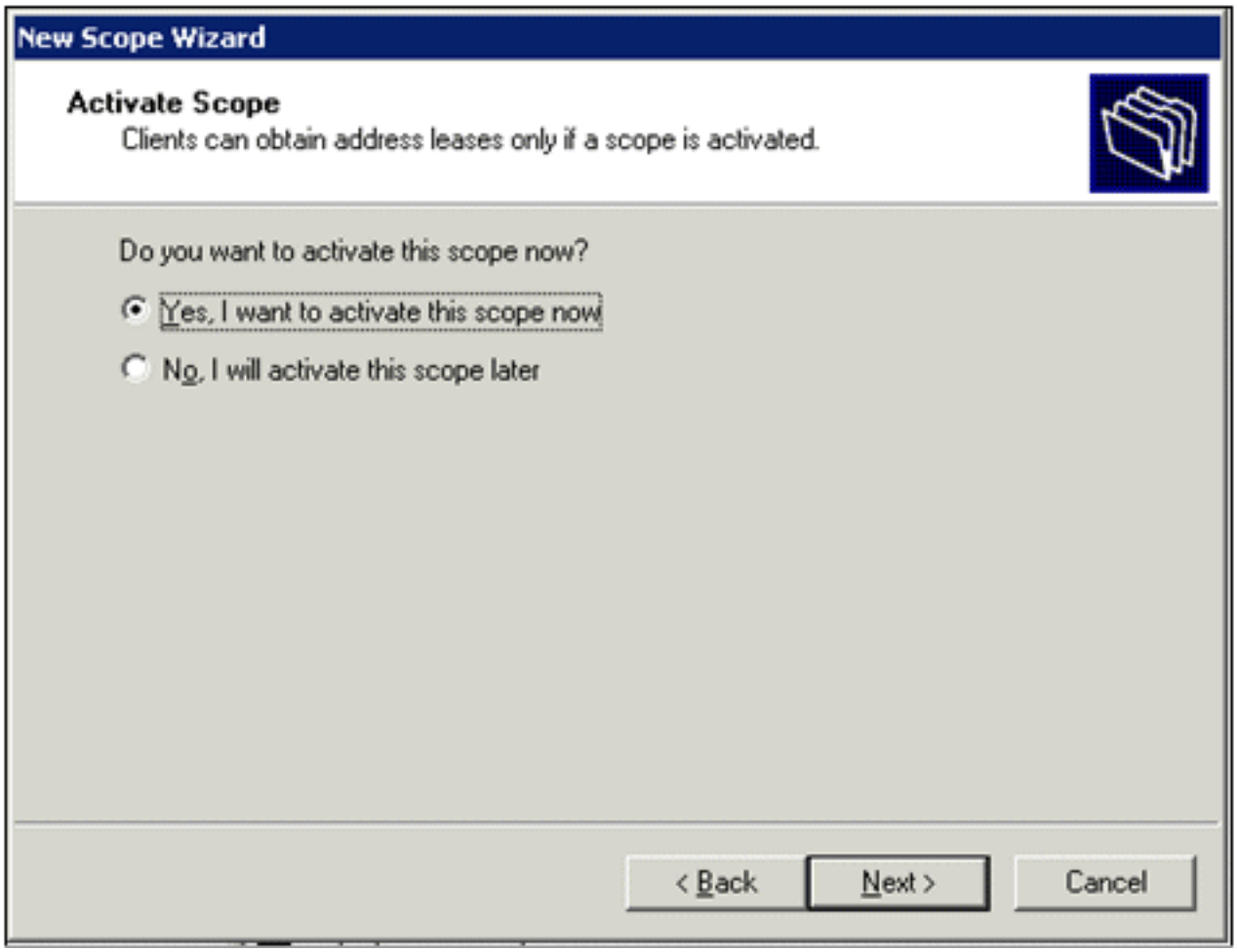
11. في صفحة الموجه (البوابة الافتراضية) أضف عنوان الموجه الافتراضي *10.0.20.1* وانقر على **التالي**.



12. في صفحة اسم المجال وخوادم DNS، اكتب *demo.local* في حقل المجال الرئيسي، اكتب *10.0.10.10* في حقل عنوان IP، ثم انقر فوق **إضافة** وانقر فوق **التالي**.



13. في الصفحة خوادم WINS، انقر فوق **التالي**.
14. في صفحة "تنشيط النطاق"، أختر **نعم، أريد تنشيط هذا النطاق الآن** وانقر فوق **التالي**.



15. عندما تنتهي بصفحة معالج نطاق جديد، انقر فوق **إنهاء**.

تثبيت خدمات الشهادات

قم بإجراء هذه الخطوات:

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

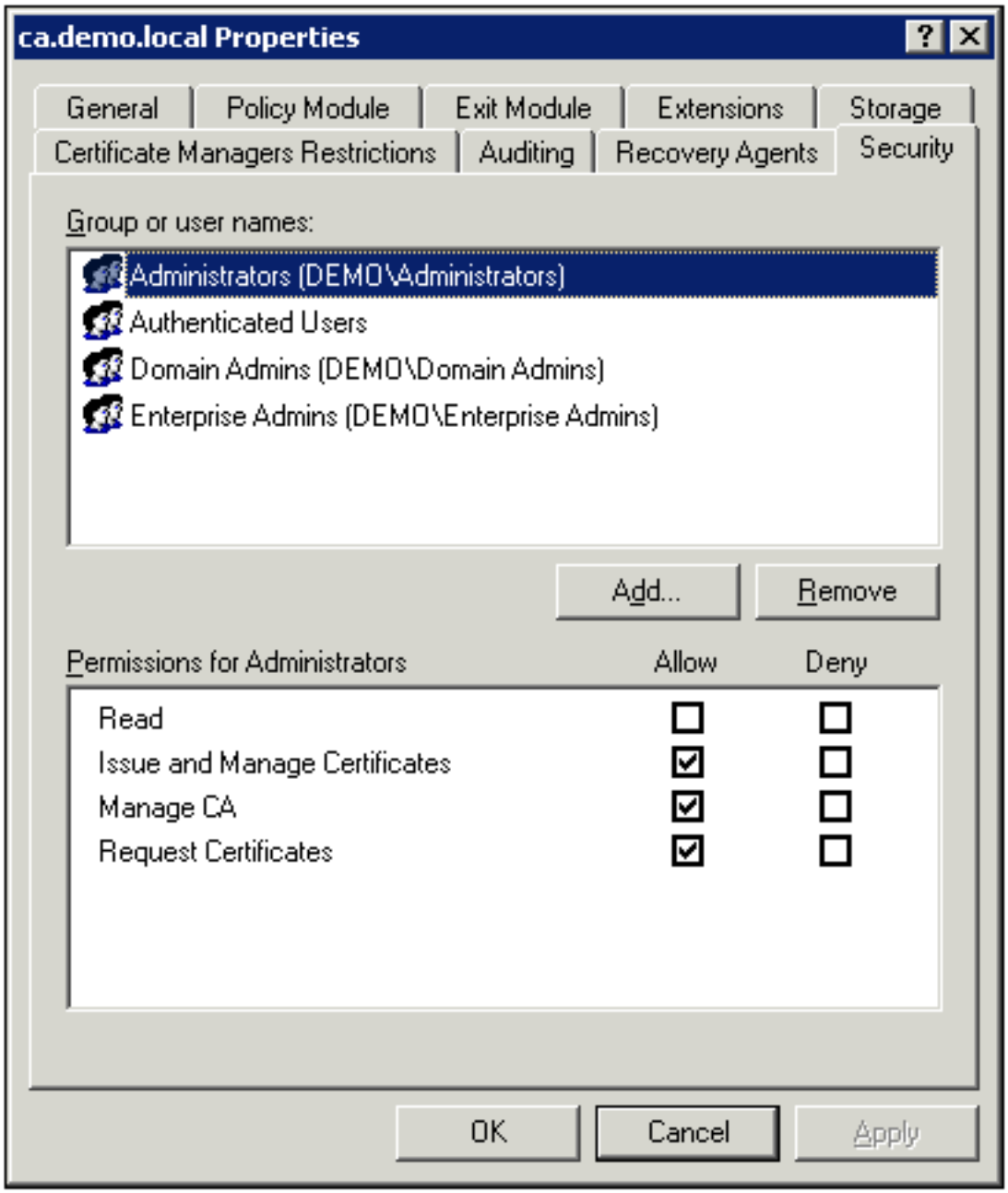
1. في "لوحة التحكم"، افتح **إضافة أو إزالة برامج**، ثم انقر فوق **إضافة/إزالة مكونات Windows**.
2. في صفحة معالج مكونات Windows، أختر خدمات الشهادات، ثم انقر فوق التالي.
3. في صفحة نوع المرجع المصدق، أختر المرجع المصدق الجذر للمؤسسة وانقر فوق التالي.
4. في صفحة معلومات تعريف المرجع المصدق، اكتب *democa* في الاسم العام لمربع المرجع المصدق هذا. يمكنك أيضا إدخال التفاصيل الاختيارية الأخرى. ثم انقر على **التالي** واقبل الافتراضيات على صفحة إعدادات قاعدة بيانات الشهادات.
5. انقر فوق **Next (التالي)**. بعد اكتمال التثبيت، انقر فوق **إنهاء**.
6. انقر فوق **موافق** بعد قراءة رسالة التحذير حول تثبيت IIS.

التحقق من أذونات المسؤول للشهادات

قم بإجراء هذه الخطوات:

1. أختر **ابدأ > أدوات إدارية > المرجع المصدق**.
2. انقر بزر الماوس الأيمن فوق **Democa CA** ثم انقر فوق **خصائص**.
3. في علامة التبويب "الأمان"، انقر فوق **Administrators** في قائمة "المجموعة" أو أسماء المستخدمين.
4. في القائمة أذون للمسئولين، تحقق من تعيين هذه الخيارات على **السماح**:إصدار الشهادات وإدارتهاإدارة

CAطلب الشهاداتإذا تم تعيين أي من هذه إلى رفض أو لم يتم تحديده، قم بتعيين الأذونات إلى



السماح.

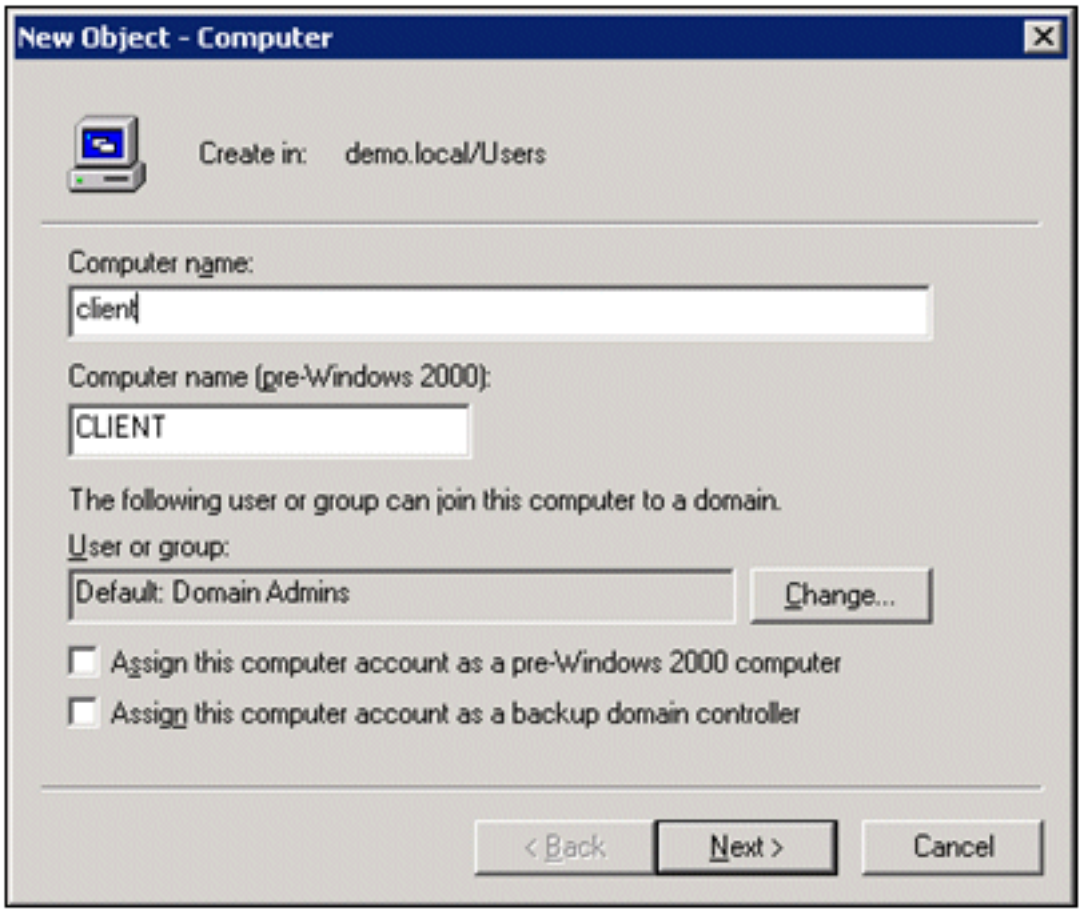
5. انقر فوق **موافق** لإغلاق مربع حوار خصائص المرجع المصدق Democa، ثم قم بإغلاق مرجع التصديق.

إضافة أجهزة كمبيوتر إلى المجال

قم بإجراء هذه الخطوات:

ملاحظة: إذا كان الكمبيوتر قد تمت إضافته بالفعل إلى المجال، فقم بالمتابعة لإضافة مستخدمين إلى المجال.

1. افتح الأداة الإضافية **لمستخدمي Active Directory وأجهزة الكمبيوتر**.
2. في شجرة وحدة التحكم، قم بتوسيع **العرض التوضيحي.local**.
3. انقر بزر الماوس الأيمن فوق **أجهزة الكمبيوتر**، وانقر فوق **جديد**، ثم انقر فوق **جهاز الكمبيوتر**.
4. في شاشة كائن جديد - كمبيوتر، اكتب اسم الكمبيوتر في حقل اسم الكمبيوتر وانقر **التالي**. يستخدم هذا المثال *عميل* اسم



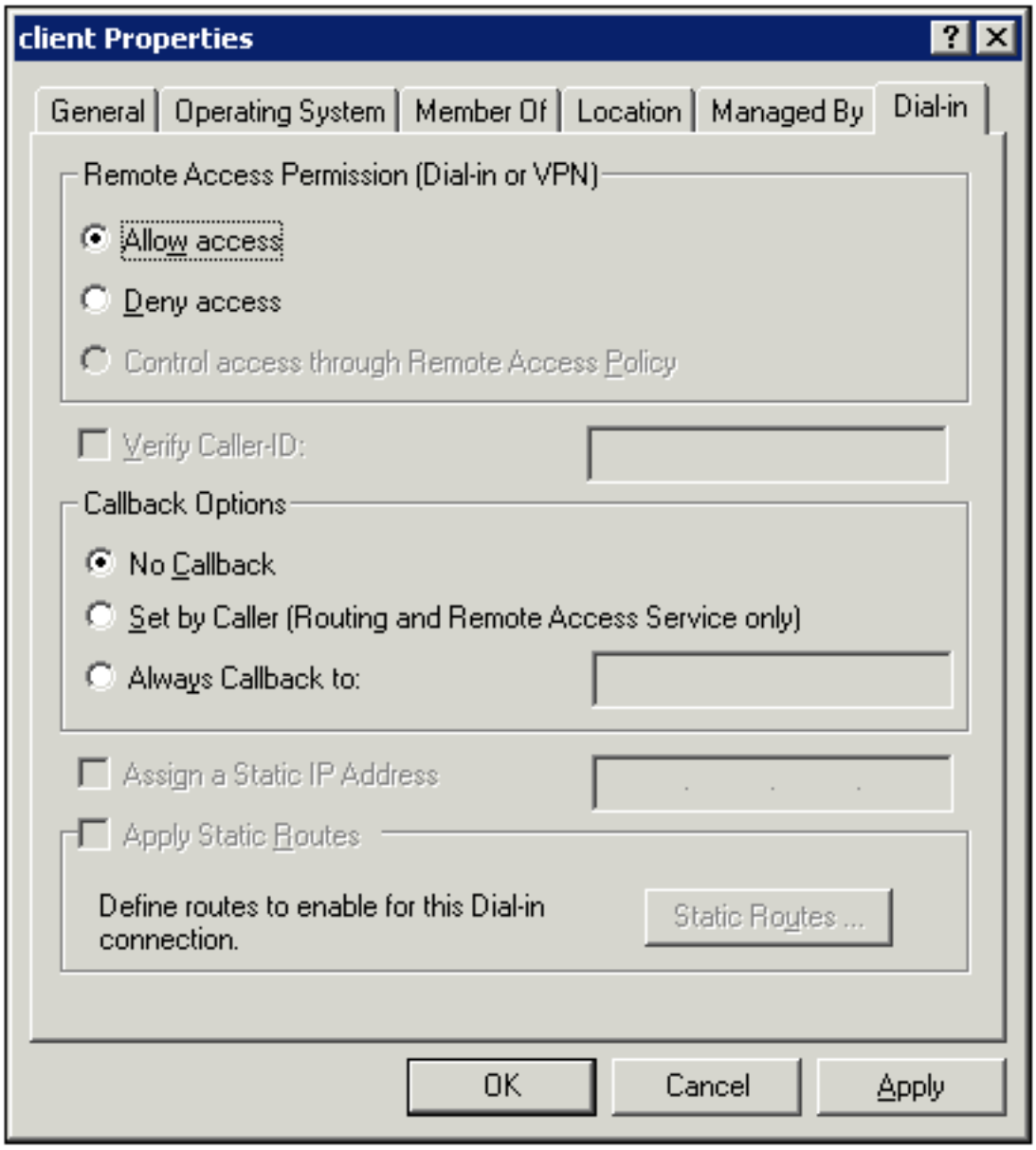
الكمبيوتر.

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

السماح بالوصول اللاسلكي إلى أجهزة الكمبيوتر

قم بإجراء هذه الخطوات:

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. انقر فوق **خصائص**، ثم انتقل إلى علامة التبويب **الطلب الهاتفي**.
2. في "إذن الوصول عن بعد"، أختر **السماح بالوصول** وانقر فوق

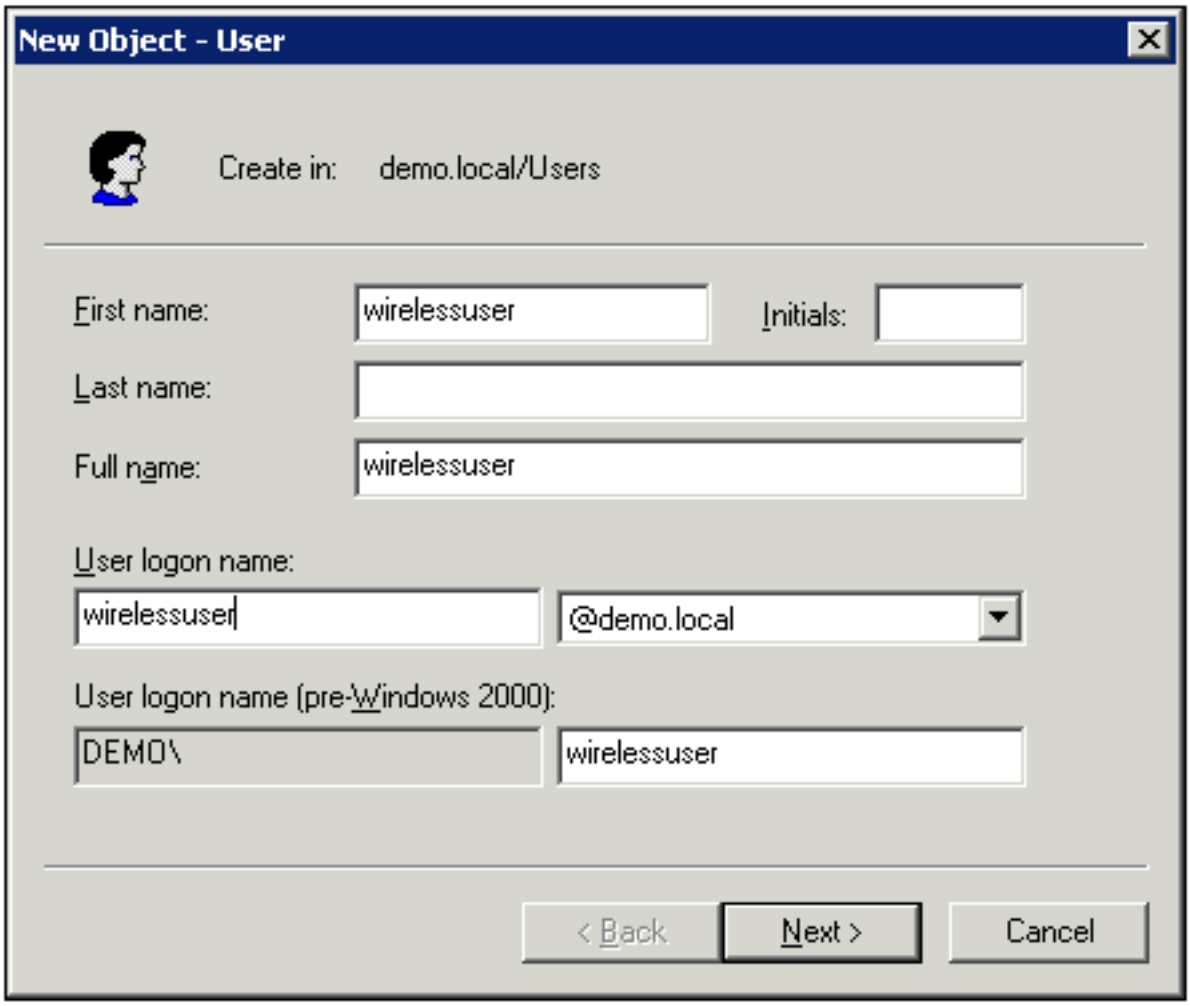


موافق.

إضافة مستخدمين إلى المجال

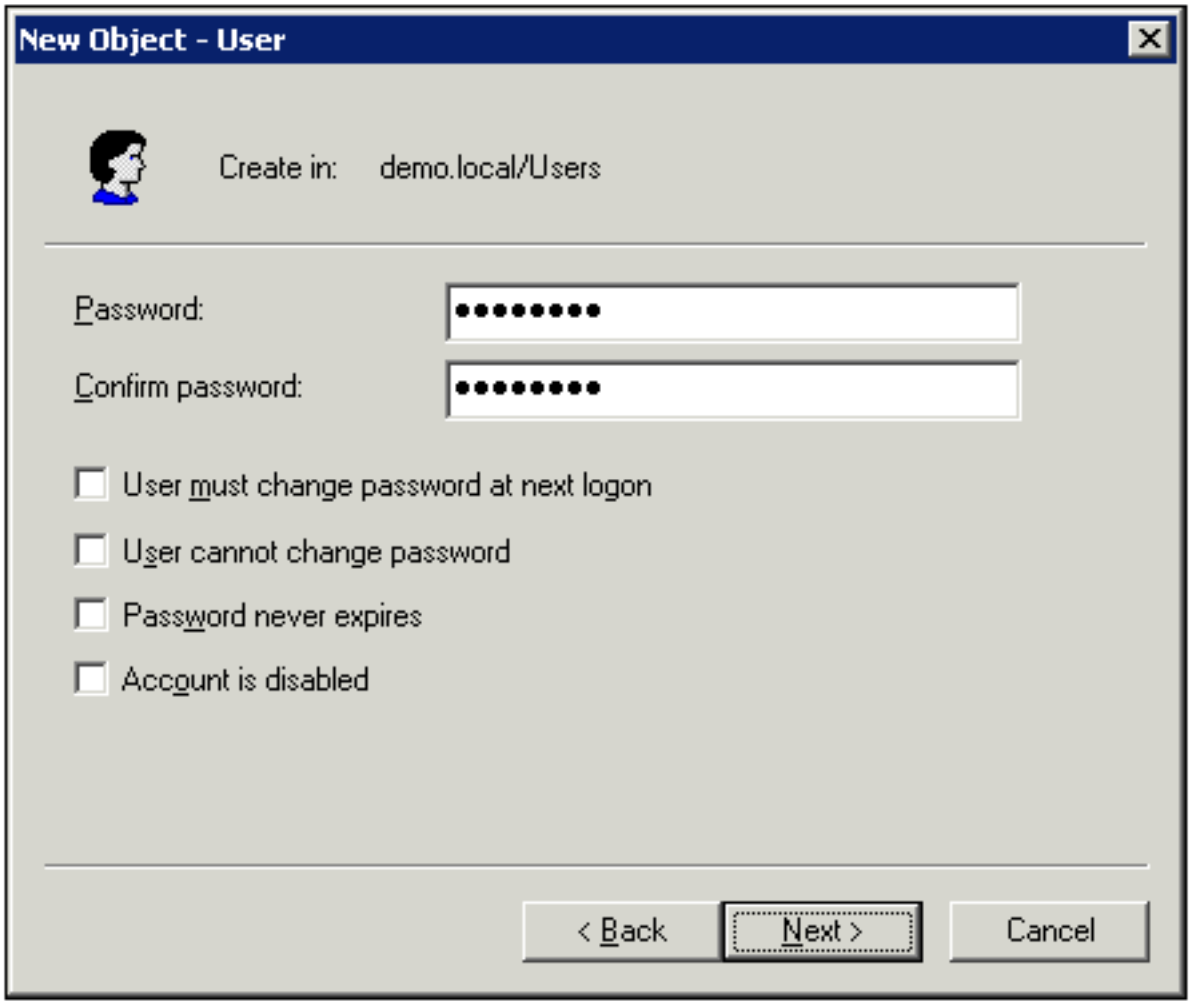
قم بإجراء هذه الخطوات:

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 الاسم *wirelessuser* في حقل "الاسم الأول" و*wirelessuser* في حقل اسم تسجيل دخول المستخدم. انقر فوق **Next**



(التالي).

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



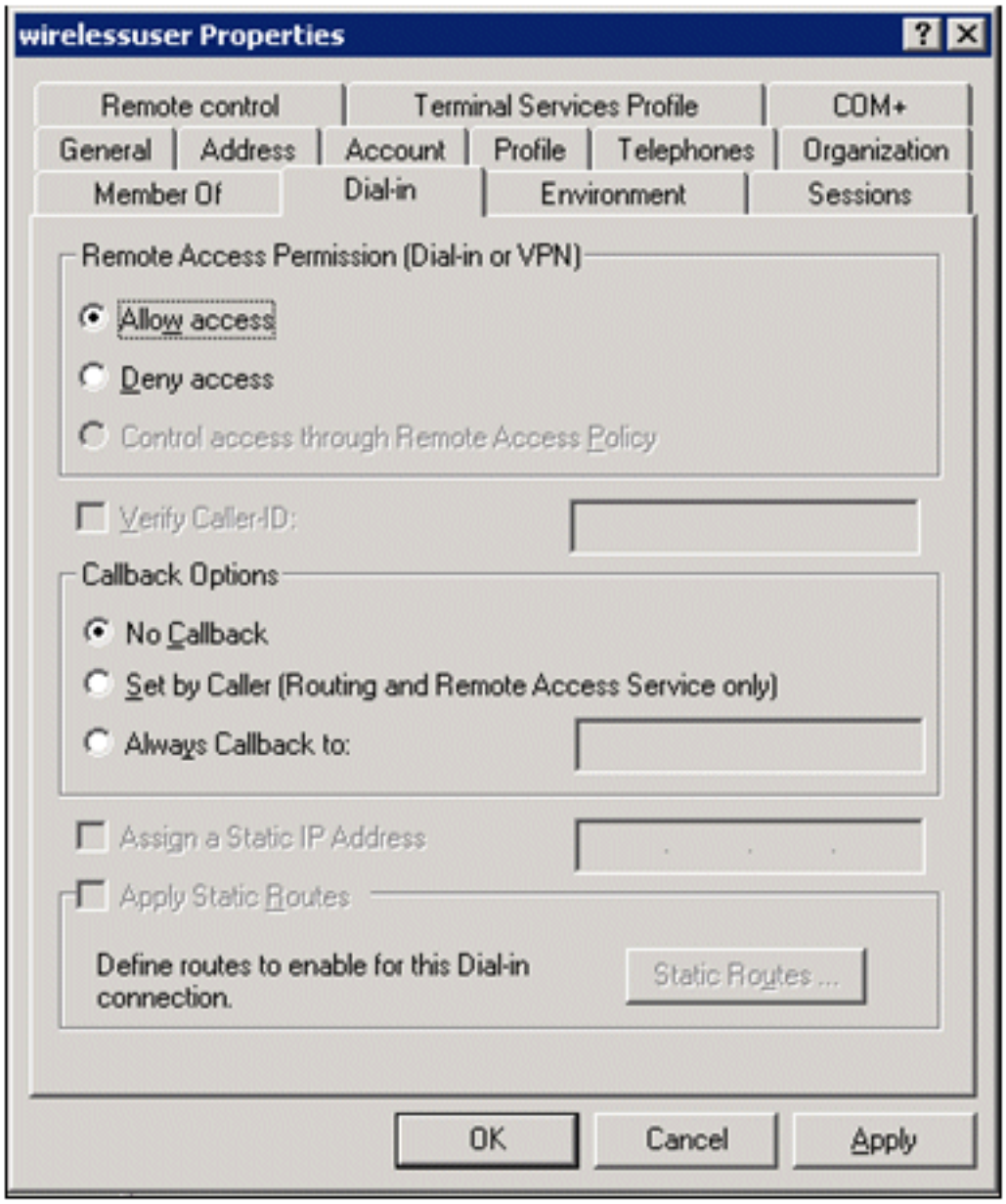
التالي.

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

السماح بالوصول اللاسلكي للمستخدمين

قم بإجراء هذه الخطوات:

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 **طلب** الدخول.
2. في "إذن الوصول عن بعد"، أختر **السماح بالوصول** وانقر فوق

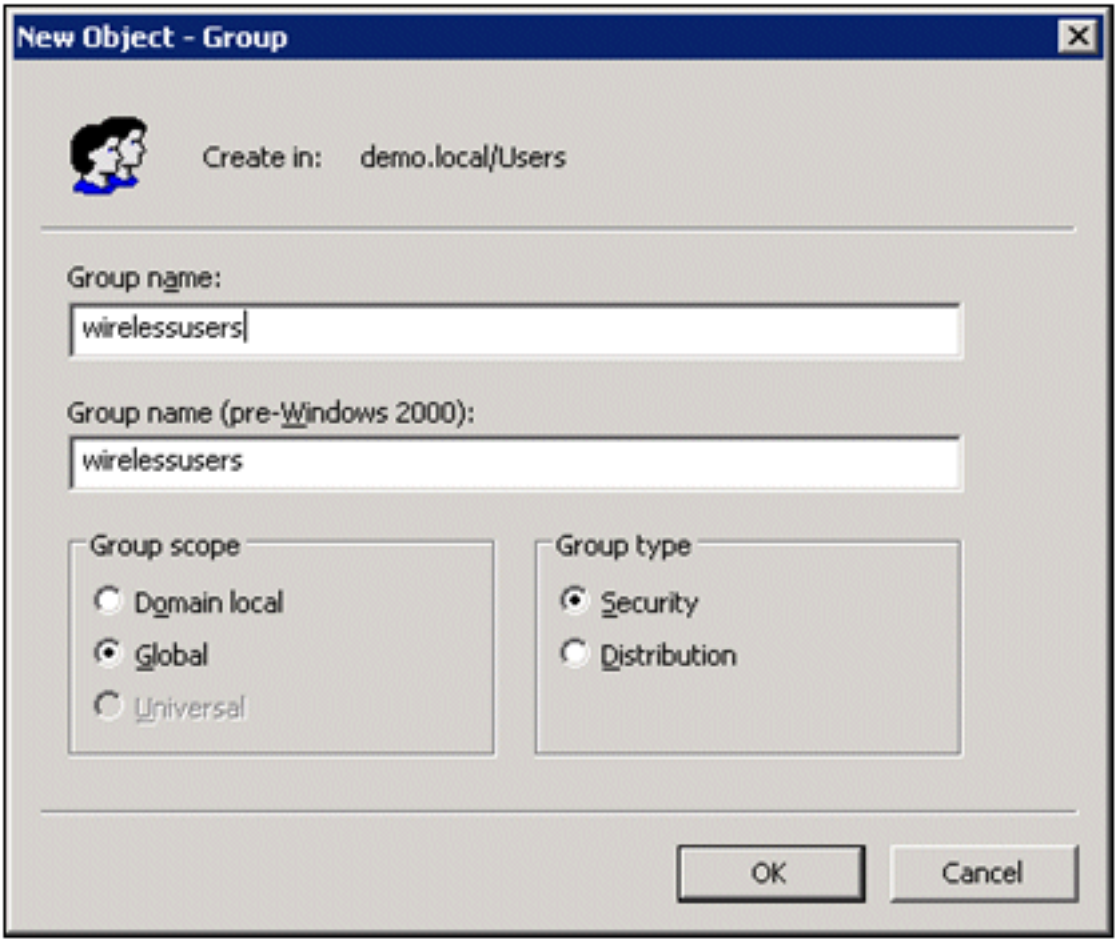


موافق.

إضافة مجموعات إلى المجال

قم بإجراء هذه الخطوات:

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 *المستخدمين اللاسلكيين* لاسم

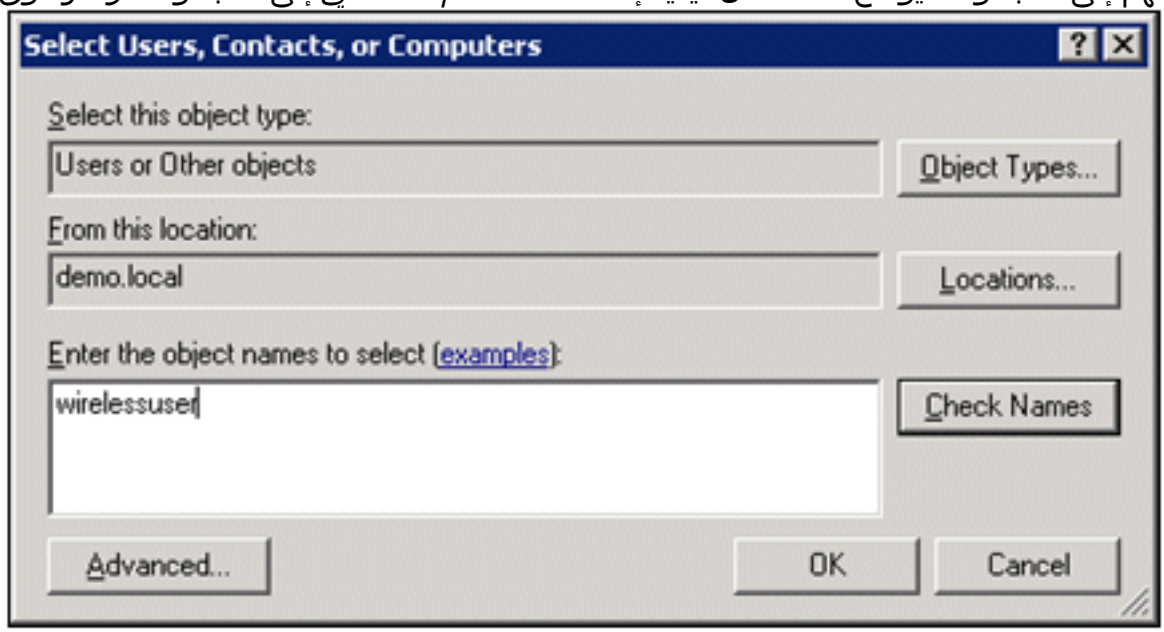


المجموعة.

إضافة مستخدمين إلى مجموعة المستخدمين السلكيين

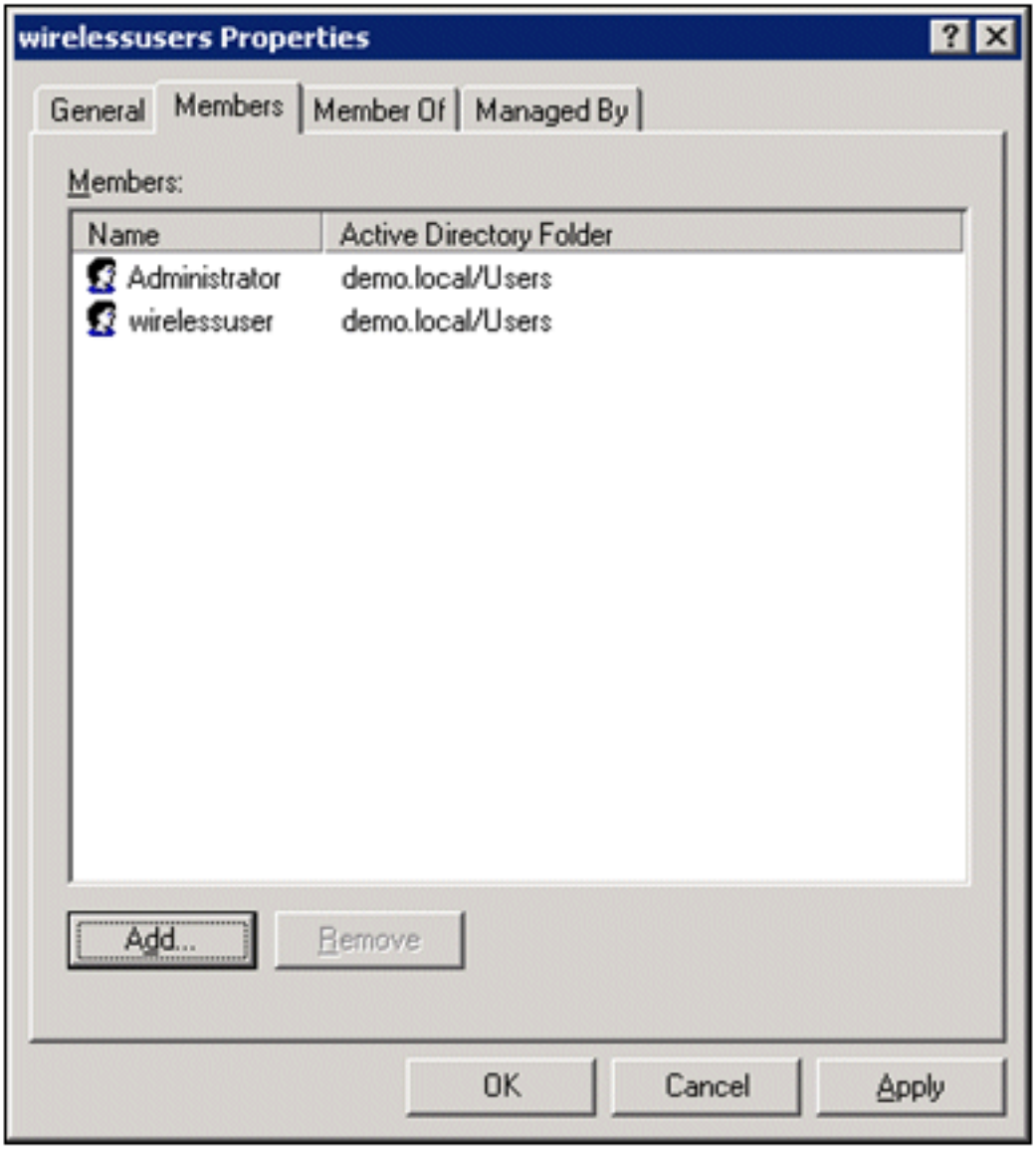
قم بإجراء هذه الخطوات:

1. في جزء التفاصيل الخاص بمستخدمي Active Directory وأجهزة الكمبيوتر، انقر نقرا مزدوجا فوق المجموعة *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 المستخدم اللاسلكي إلى مجموعة المستخدمين



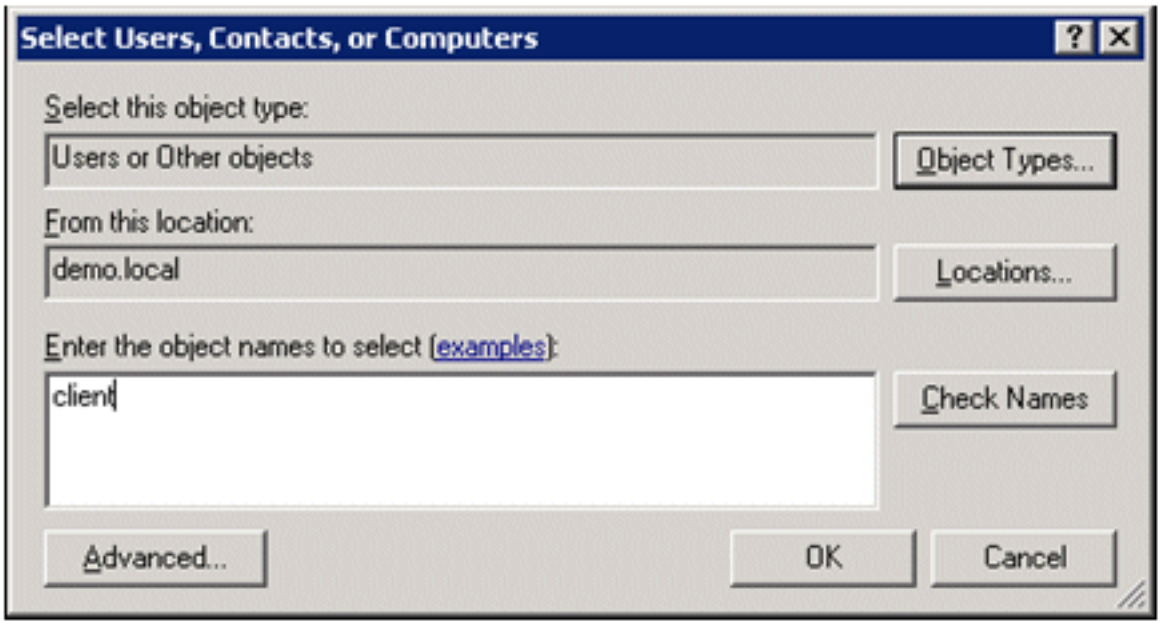
السلكيين.

5. طقطقة **ok** in order to أنقذت تغير إلى ال wirelessusers مجموعة.
6. كرر هذا الإجراء لإضافة المزيد من المستخدمين إلى المجموعة.

إضافة أجهزة كمبيوتر عميلة إلى مجموعة المستخدمين السلكيين

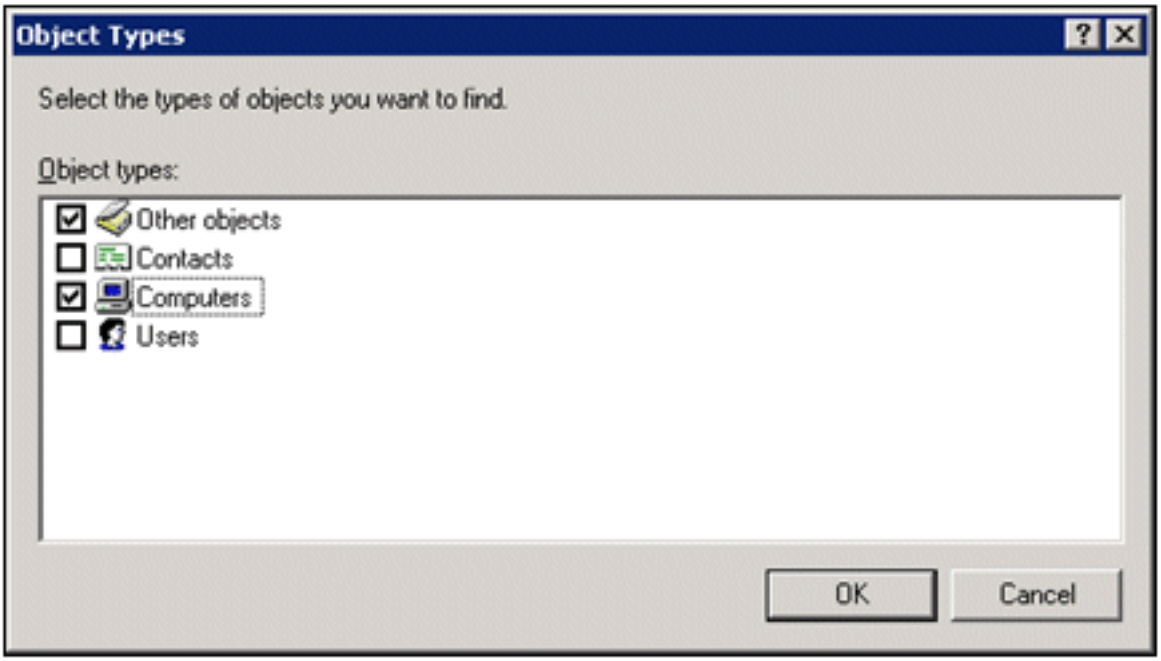
قم بإجراء هذه الخطوات:

1. كرر الخطوات 1 و 2 في قسم إضافة مستخدمين إلى مجموعة المستخدمين السلكيين 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



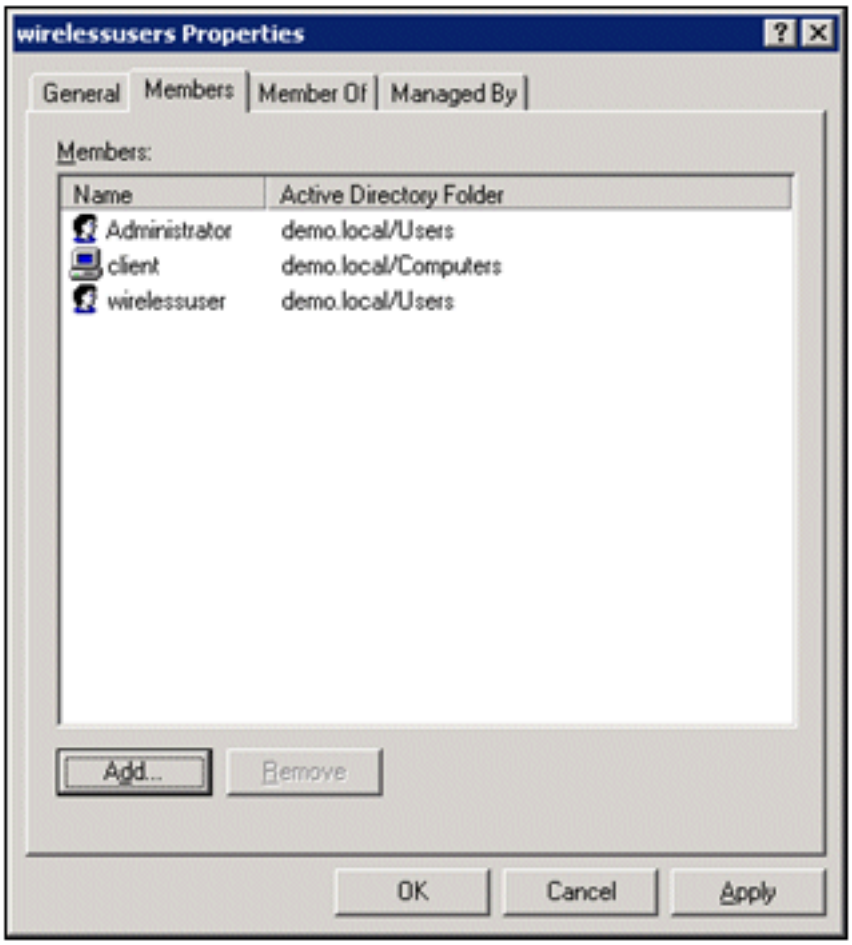
المجموعة.

3. انقر فوق **أنواع الكائن**، وقم بإلغاء تحديد خانة الاختيار **المستخدمون**، ثم حدد **أجهزة**



الكمبيوتر.

4. طقطقت **ok** مرتين. تتم إضافة حساب الكمبيوتر العميل إلى مجموعة المستخدمين



السلكيين.

5. كرر الإجراء لإضافة المزيد من أجهزة الكمبيوتر إلى المجموعة.

Cisco 1121 Secure ACS 5.1

التثبيت باستخدام جهاز CSACS-1121 Series

يتم تثبيت جهاز CSACS-1121 مسبقا مع برنامج ACS 5.1. يمنحك هذا القسم نظرة عامة على عملية التثبيت والمهام التي يجب عليك تنفيذها قبل تثبيت ACS.

1. توصيل CSACS-1121 بالشبكة ووحدة تحكم الجهاز. انظر الفصل الرابع، "توصيل الكبلات."
2. قم بتشغيل جهاز CSACS-1121. انظر الفصل 4، "تشغيل جهاز CSACS-1121 Series."
3. قم بتشغيل الأمر **setup** في نافذة مطالبة واجهة سطر الأوامر (CLI) لتكوين الإعدادات الأولية لخادم ACS. راجع تشغيل برنامج الإعداد.

تثبيت خادم ACS

يصف هذا القسم عملية التثبيت لخادم ACS على جهاز CSACS-1121 Series.

- تشغيل برنامج الإعداد
- التحقق من عملية التثبيت
- مهام ما بعد التثبيت

للحصول على معلومات تفصيلية حول تثبيت خادم Cisco Secure ACS، ارجع إلى دليل التثبيت والترقية لنظام التحكم في الوصول الآمن من Cisco 5.1.

تكوين وحدة التحكم Cisco WLC5508

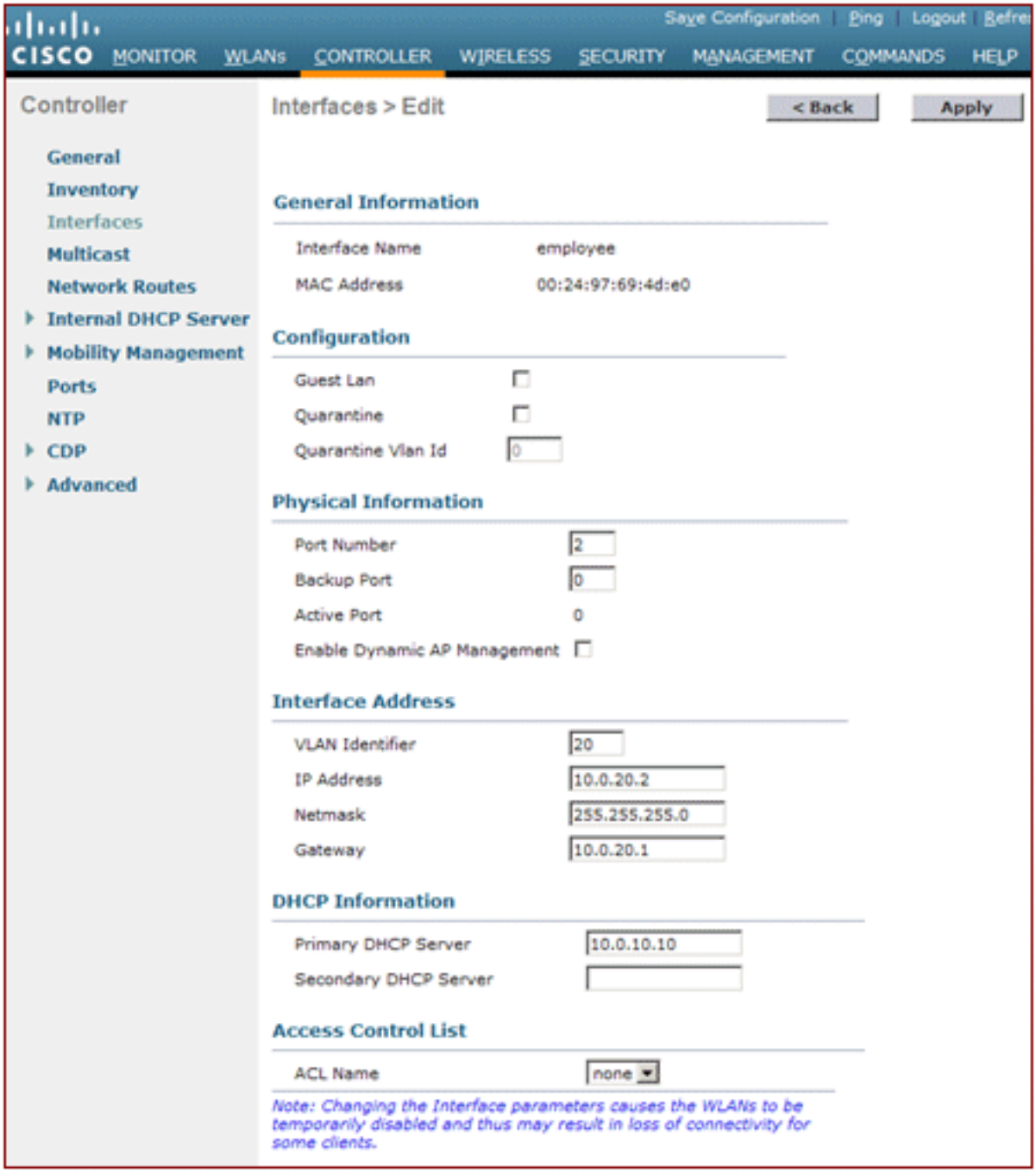
قم بإنشاء التكوين اللازم ل WPAv2/WPA

قم بإجراء هذه الخطوات:

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

1. استعرض للوصول إلى **https://10.0.1.10** لتسجيل الدخول إلى وحدة

التحكم.
2. انقر على **تسجيل الدخول**.
3. قم بتسجيل الدخول باستخدام *مسؤول* المستخدم الافتراضي وكلمة المرور الافتراضية *admin*.
4. قم بإنشاء واجهة جديدة لتعيين شبكة VLAN تحت قائمة **وحدة التحكم**.
5. طقطقة **قارن**.
6. طقطقت **جديد**.
7. دخلت في القارن إسم مجال، *موظف*. (يمكن أن يكون هذا الحقل أي قيمة تحبها.)
8. في حقل معرف شبكة VLAN، أدخل *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 يبدي:عنوان IP للواجهة - - 10.0.20.2NetMask - 255.255.255.0البوابة - 10.0.10.1بروتوكول DHCP الأساسي - 10.0.10.10

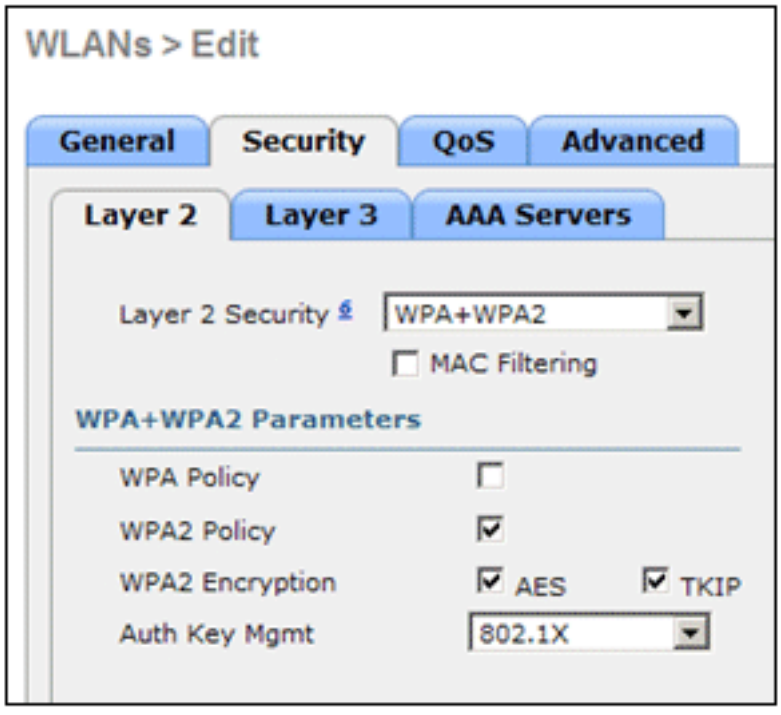


11. طقطقة **يطبق**.
12. انقر فوق علامة التبويب **شبكات WLAN**.
13. أختر **إنشاء جديد**، وانقر **انتقال**.
14. أدخل اسم توصيف، وأدخل *الموظف* في حقل WLAN SSID.

15. أختر معرف للشبكة المحلية اللاسلكية (WLAN)، وانقر فوق **تطبيق**.

16. قم بتكوين المعلومات لشبكة WLAN هذه عندما تظهر نافذة WLANs > Edit (تحرير).**ملاحظة:** WPAv2 هو طريقة تشفير الطبقة 2 المختارة لهذا المختبر. للسماح ل WPA مع عملاء TKIP-MIC بالاقتران بمعرف SSID هذا، يمكنك أيضا التحقق من **وضع توافق WPA** و**السماح** بصناديق **عملاء WPA2 TKIP** أو العملاء الذين لا يدعمون أسلوب تشفير AES 802.11i.
17. في شاشة WLANs > تحرير، انقر صفحة **عام**.
18. تأكد من أنه قد تم تحديد مربع الحالة **للتمكين** ومن إختيار **الواجهة** المناسبة (الموظف). تأكد أيضا من تحديد خانة الاختيار **تمكين** ل Broadcast SSID.

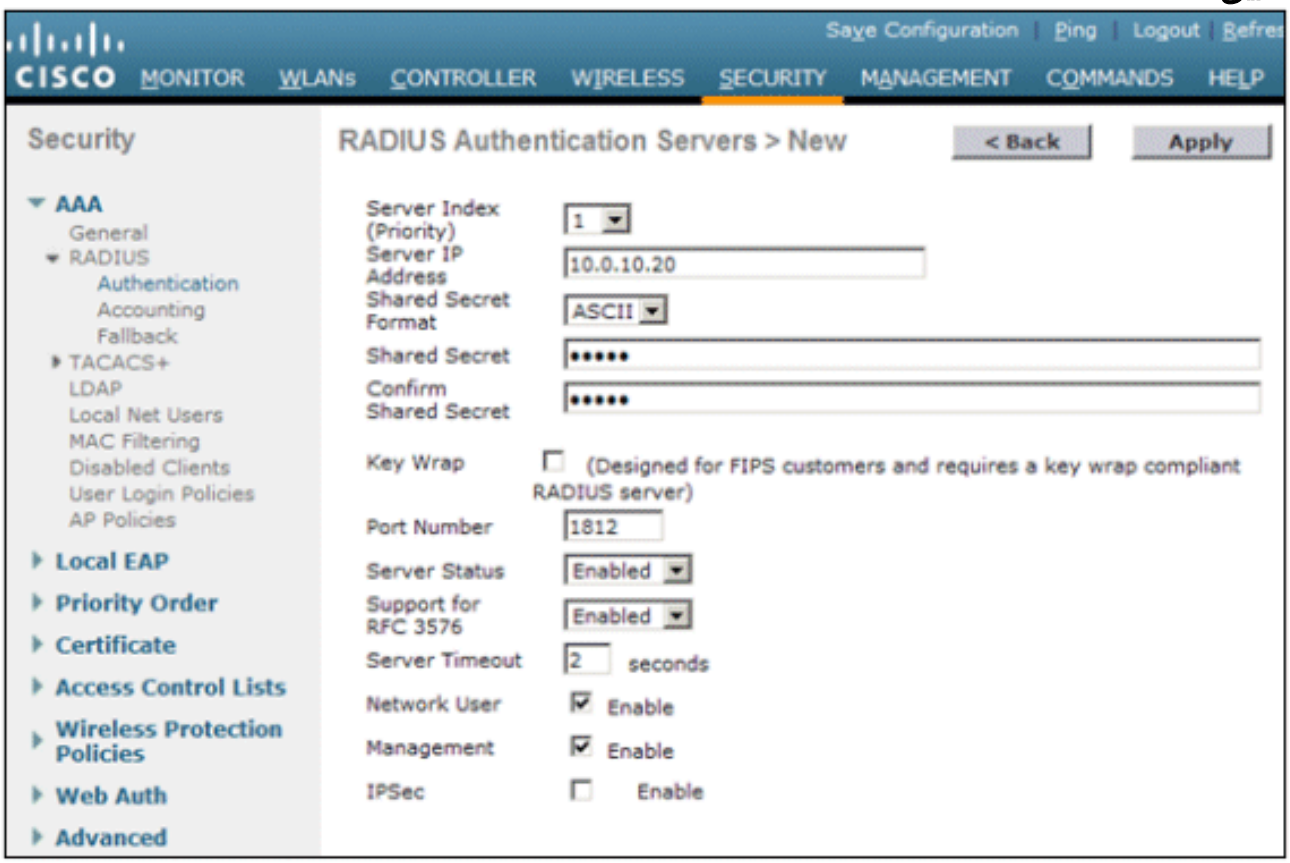
19. انقر فوق علامة التبويب **أمان**.
20. تحت الطبقة 2 قائمة فرعية، تدقيق **WPA + WPA2** لتأمين الطبقة 2. لتشفير WPA2، تحقق من **AES +** **TKIP** للسماح لعملاء TKIP.



21. أختر **802.1x** كطريقة مصادقة.
22. تخطي القائمة الفرعية للطبقة 3 لأنها غير مطلوبة. وبمجرد تكوين خادم RADIUS، يمكن إختيار الخادم

المناسب من قائمة المصادقة.

23. يمكن ترك علامات التبويب **جودة الخدمة** و**المتقدم** في الوضع الافتراضي ما لم تكن هناك حاجة إلى أي تكوينات خاصة.
24. انقر فوق قائمة **الأمان** لإضافة خادم RADIUS.
25. تحت القائمة الفرعية RADIUS، انقر على **المصادقة**. ثم انقر فوق **جديد**.
26. إضافة عنوان IP لخادم RADIUS (10.0.10.20) وهو خادم ACS الذي تم تكوينه مسبقا.
27. تأكد من تطابق المفتاح المشترك مع عميل AAA الذي تم تكوينه في خادم ACS. تأكد من أن مربع **مستخدم الشبكة** محددا وانقر **تطبيق**.



28. اكتملت الآن التهيئة الأساسية ويمكنك البدء في إختبار PEAP.

مصادقة PEAP

يتطلب PEAP مع MS-CHAP الإصدار 2 شهادات على خوادم ACS وليس على العملاء اللاسلكيين. يمكن إستخدام التسجيل التلقائي لشهادات الكمبيوتر لخوادم ACS لتبسيط عملية النشر.

لتكوين خادم CA لتوفير التسجيل التلقائي لشهادات الكمبيوتر والمستخدم، أكمل الإجراءات الواردة في هذا القسم.

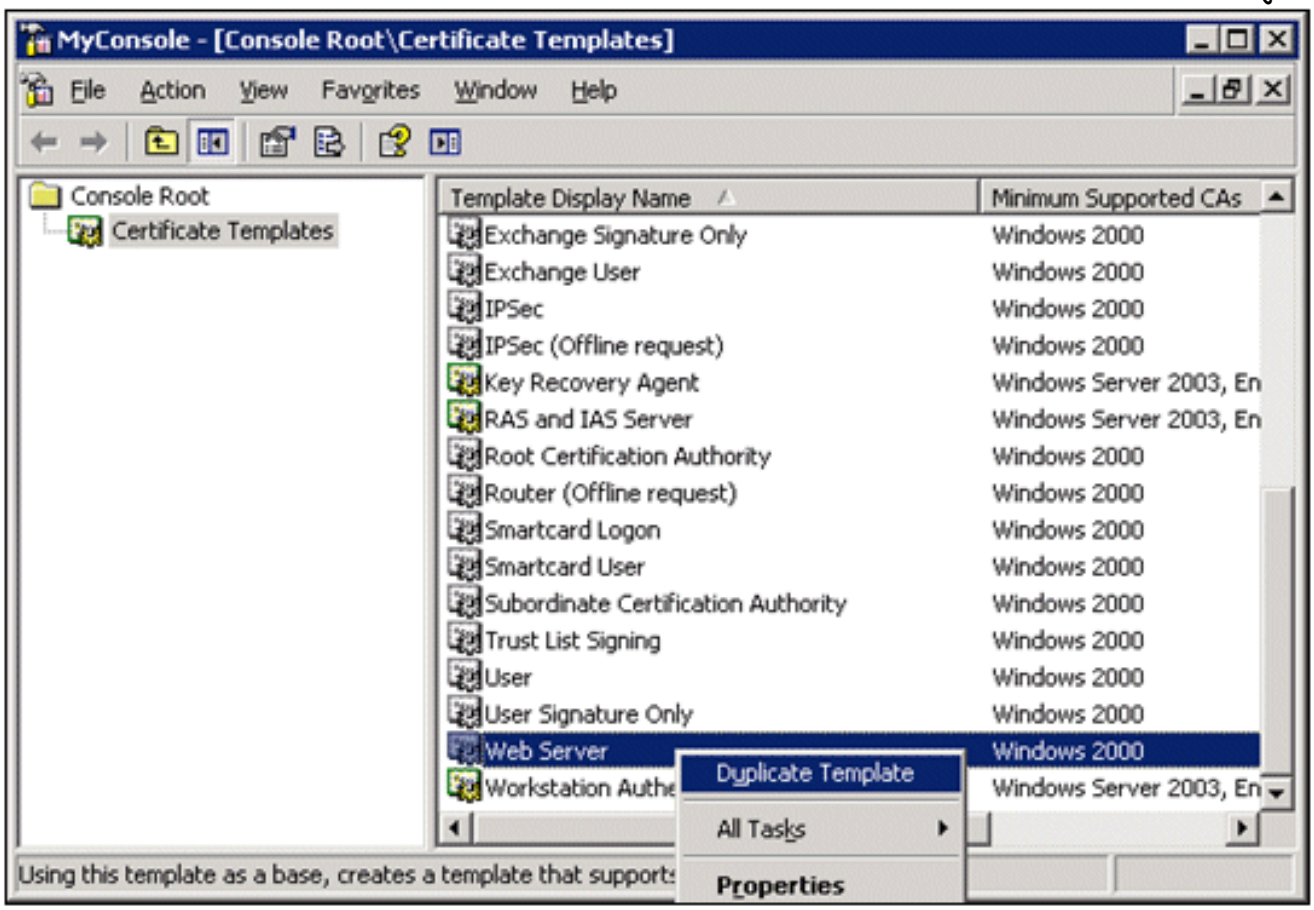
ملاحظة: قامت Microsoft بتغيير قالب خادم الويب من خلال إصدار Windows 2003 Enterprise CA حتى لا تعود المفاتيح قابلة للتصدير ويتم تحديد الخيار بدقة. لا توجد قوالب شهادات أخرى مزودة بخدمات شهادات لمصادقة الخادم وتعطي القدرة على وضع علامة على المفاتيح قابلة للتصدير المتوفرة في القائمة المنسدلة بحيث يتعين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

قم بإجراء هذه الخطوات:

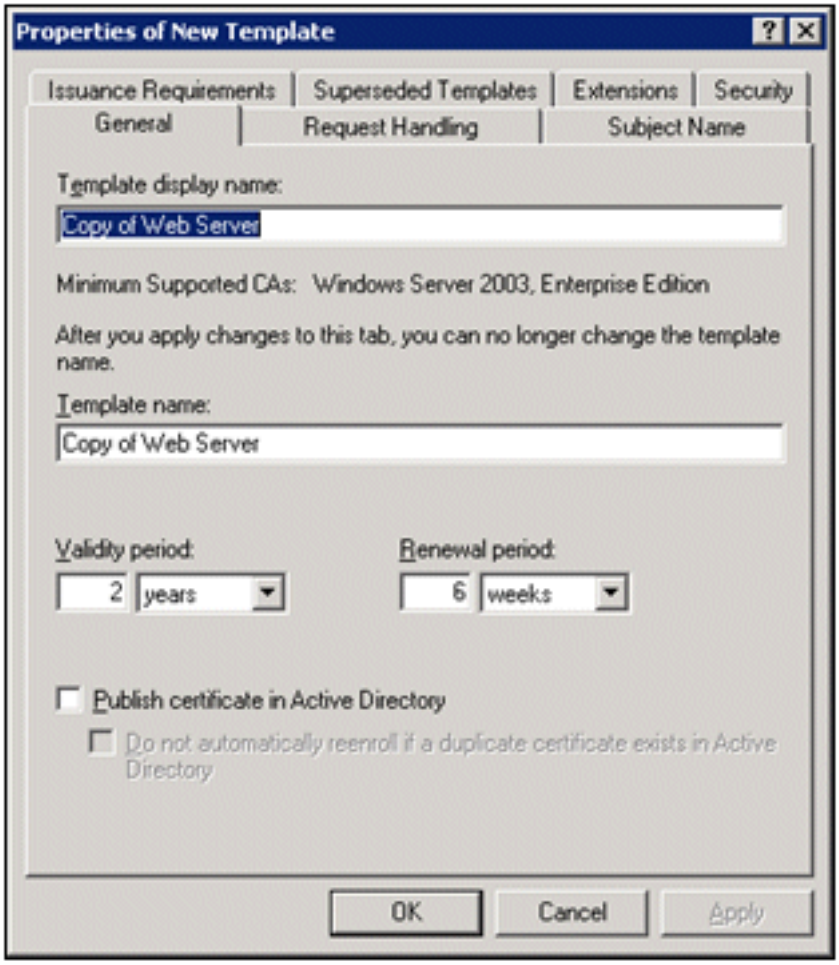
1. أخترت **يبدأ>يركض**، دخلت *mmc*، وطقطقة **ok**.
2. من القائمة "ملف"، انقر فوق **إضافة/إزالة الأداة الإضافية**، ثم انقر فوق **إضافة**.
3. تحت الأداة الإضافية، انقر نقرا مزدوجا على **قوالب الترخيص**، ثم انقر على **إغلاق**، ثم انقر على **موافق**.
4. في شجرة وحدة التحكم، انقر فوق **قوالب الشهادات**. تظهر كل قوالب الشهادات في جزء التفاصيل.
5. لتخطي الخطوات من 2 إلى 4، أدخل *certtmpl.msc* الذي يفتح الأداة الإضافية "قوالب الشهادات".



قم بإنشاء قالب الشهادة لخادم ويب ACS

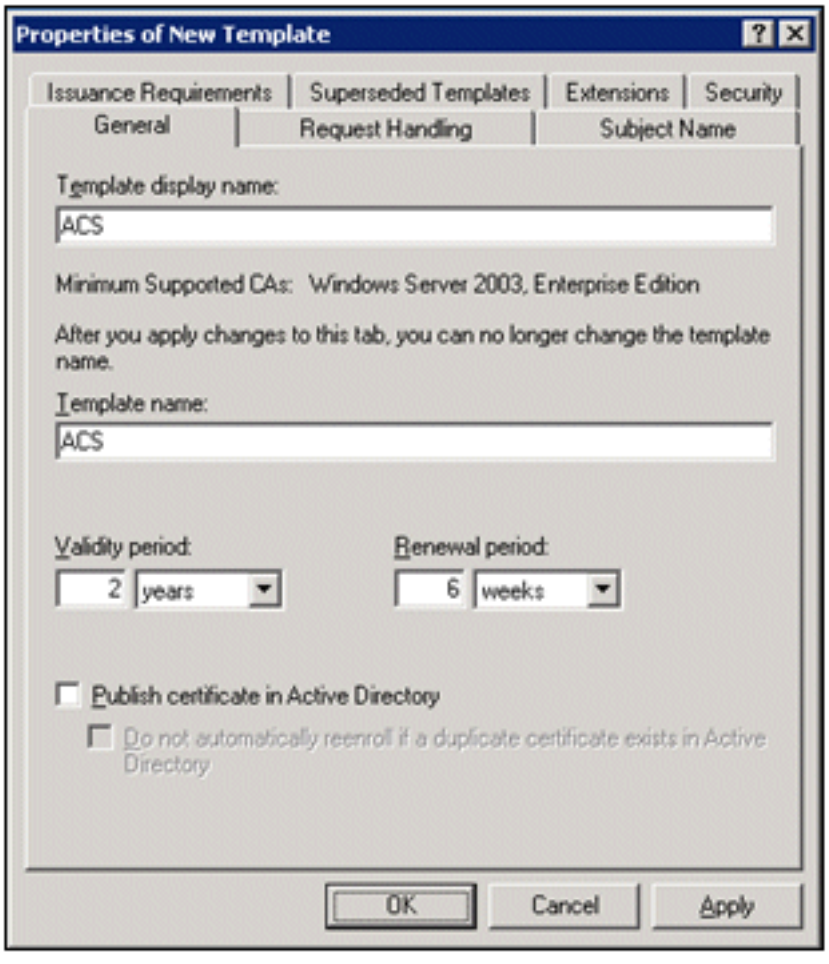
قم بإجراء هذه الخطوات:

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



قالب.

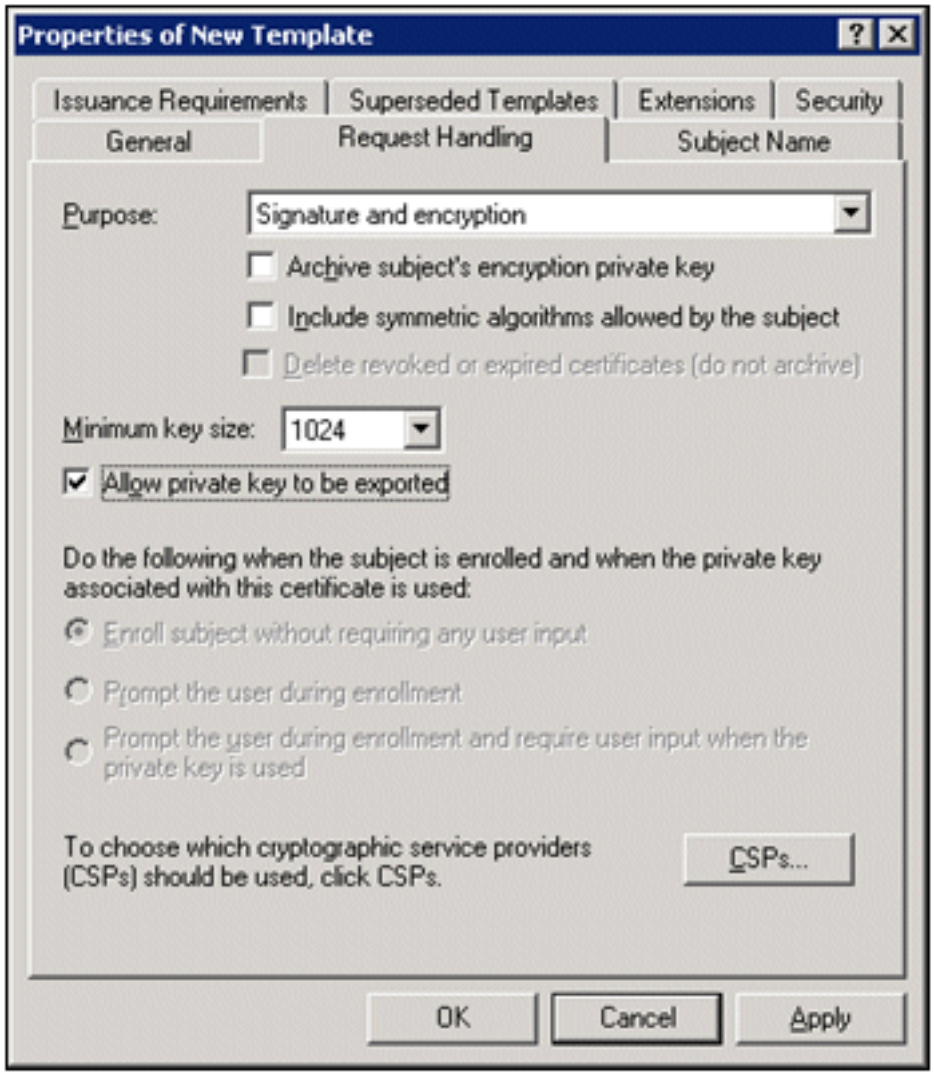
3. دخلت في القالب عرض إسم مجال،



ACS.

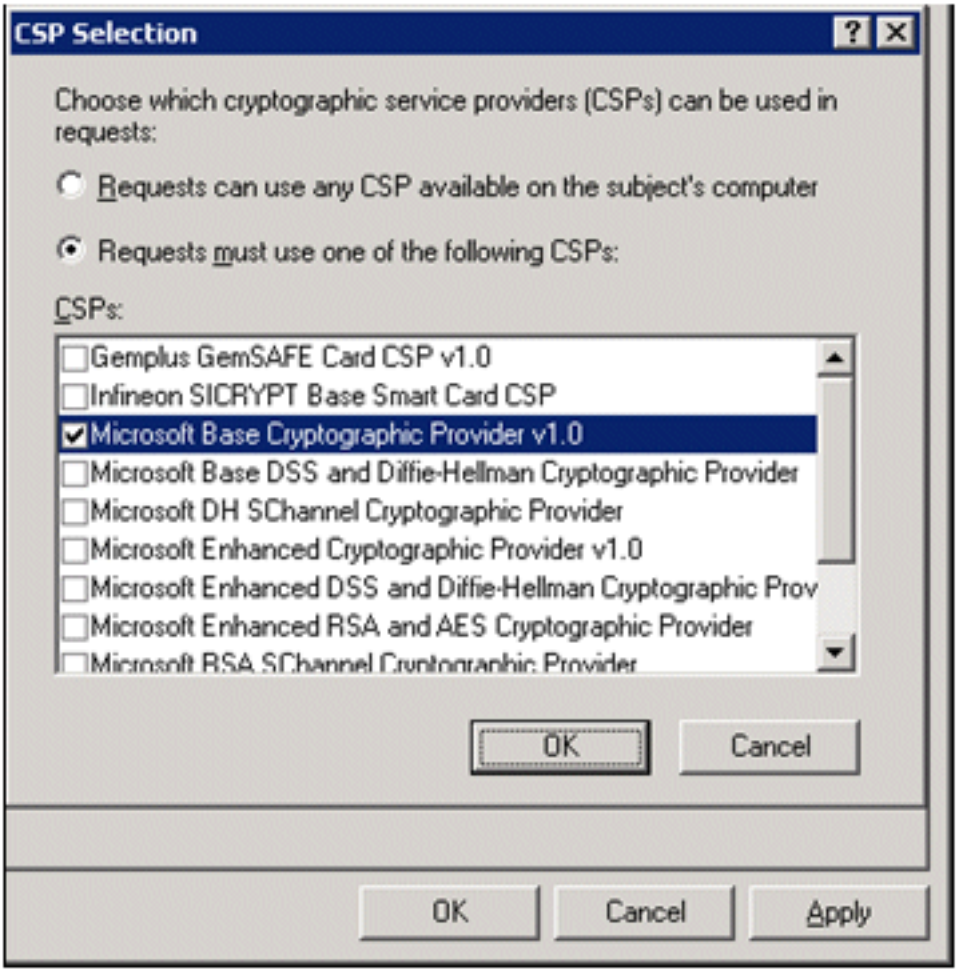
4. انتقل إلى علامة التبويب **معالجة الطلب** وحدد **السماح بتصدير المفتاح الخاص**. تأكد أيضا من تحديد **التوقيع**

والتشفير من القائمة المنسدلة



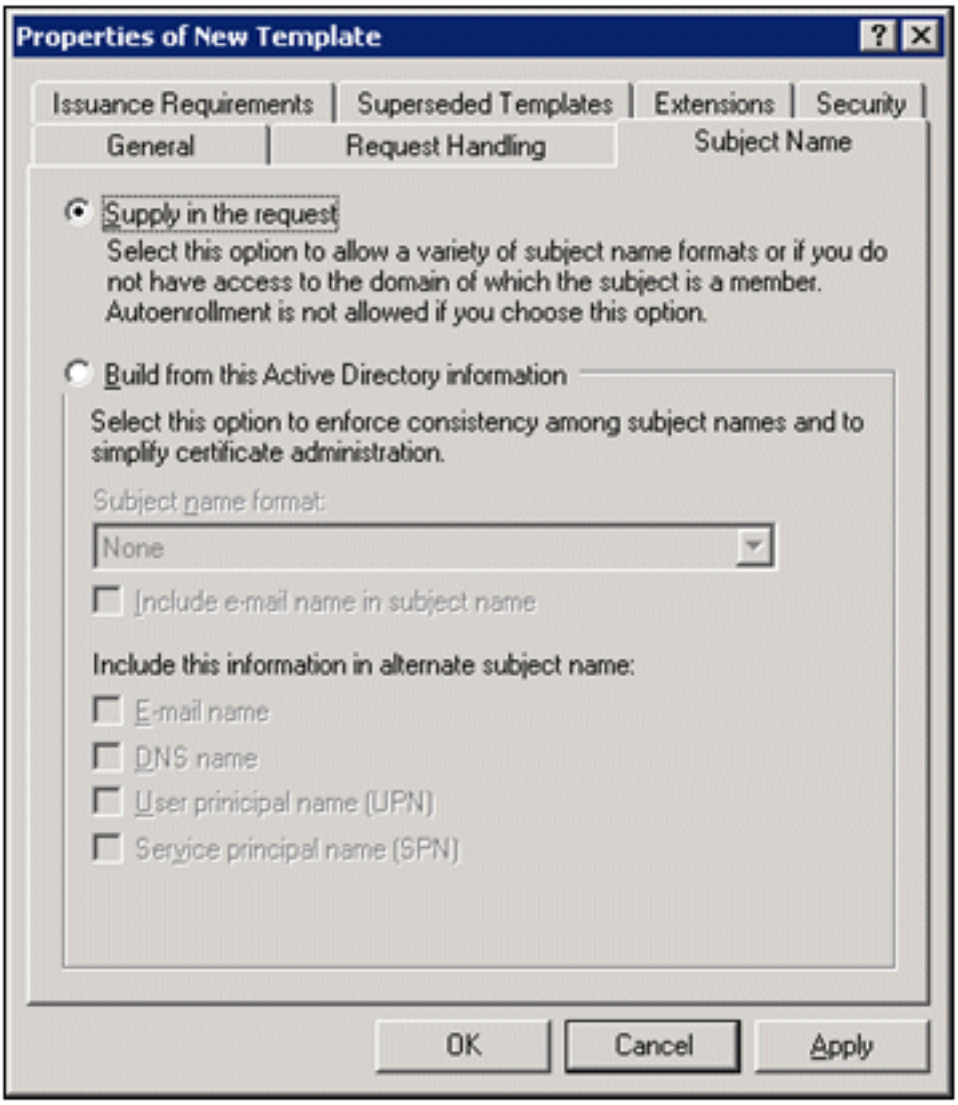
الغرض.

5. أختر **طلبات يجب أن تستخدم أحد CSP التالية** وفحص **موفر التشفير الأساسي Microsoft v1.0**. قم بإلغاء تحديد أي CSPs أخرى تم تحديدها، وانقر



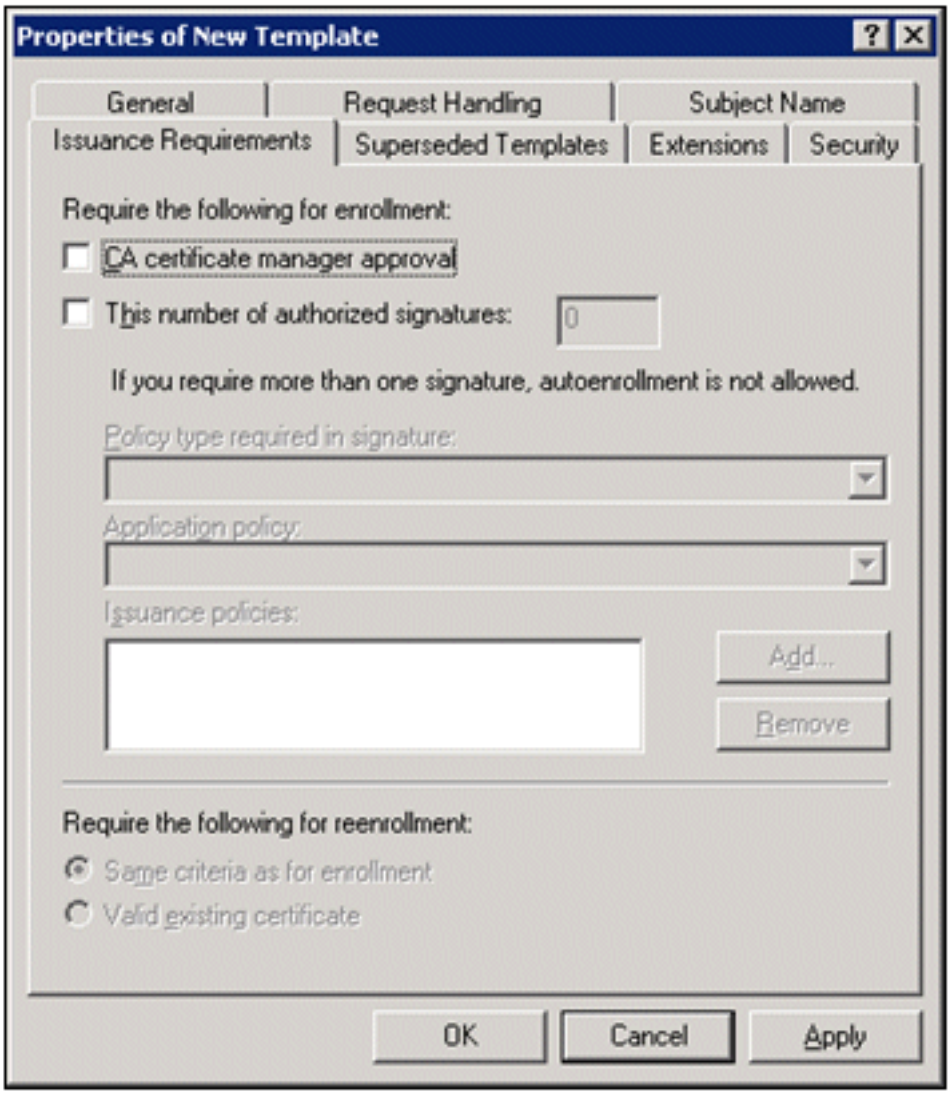
موافق.

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



موافق.

7. انتقل إلى علامة التبويب **الأمان**، وأبرز **مجموعة مسؤولي المجال**، وتأكد من تحديد خيار **التسجيل** ضمن "مسموح به".**ملاحظة:** إذا أخترت الإنشاء من معلومات Active Directory هذه، فتحقق فقط من **اسم المستخدم الأساسي (UPN)** وألغي تحديد اسم **تضمين البريد الإلكتروني** في اسم الموضوع واسم البريد الإلكتروني بسبب عدم إدخال اسم بريد إلكتروني لحساب المستخدم اللاسلكي في الأداة الإضافية لمستخدمي Active Directory وأجهزة الكمبيوتر. إذا لم تقم بتعطيل هذين الخيارين، فسيحاول التسجيل التلقائي إستخدام البريد الإلكتروني، مما ينتج عنه خطأ في التسجيل التلقائي.
8. هناك إجراءات أمان إضافية إذا لزم الأمر لمنع دفع الشهادات تلقائيا. ويمكن العثور على هذه العناصر ضمن علامة التبويب متطلبات الإصدار. لم يتم مناقشة هذا الأمر في هذه



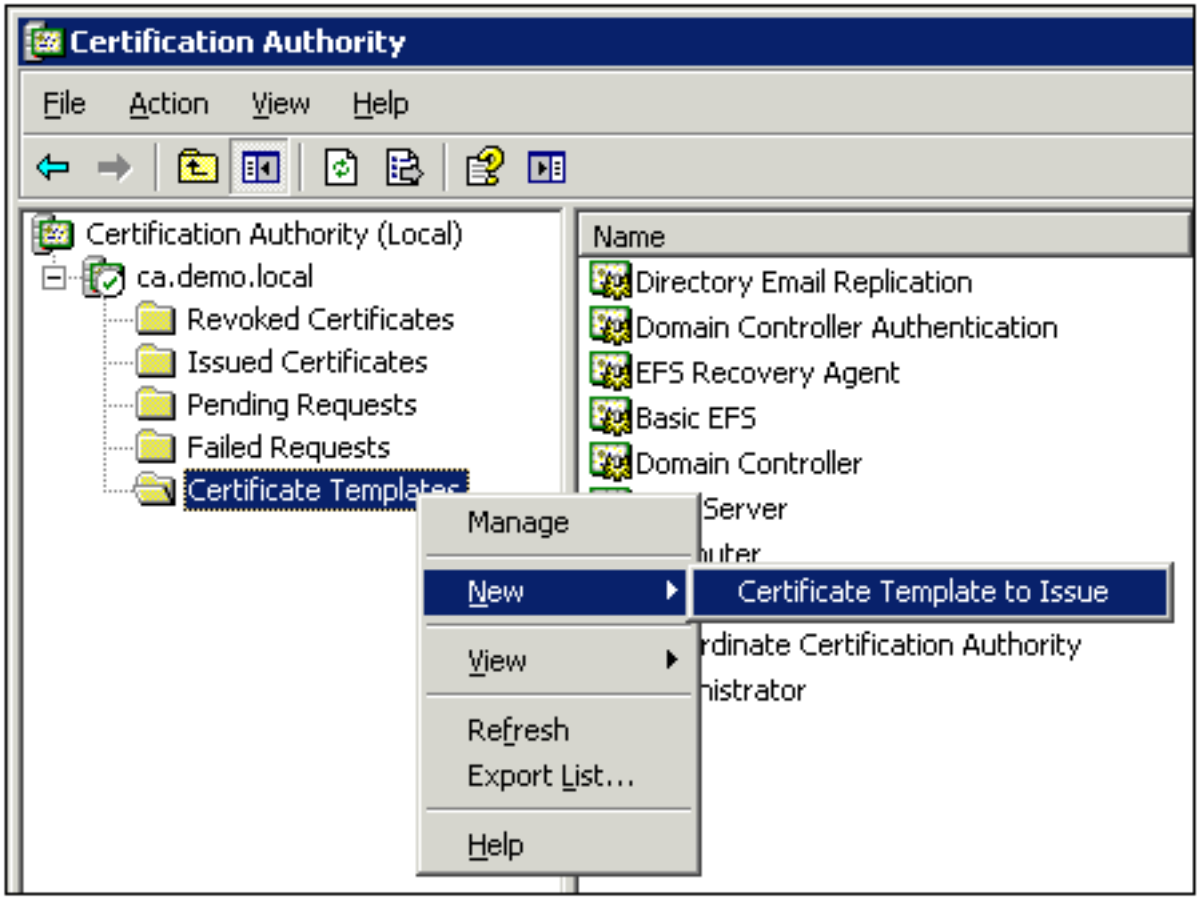
الوثيقة.

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

تمكين قالب شهادة خادم ويب ACS الجديد

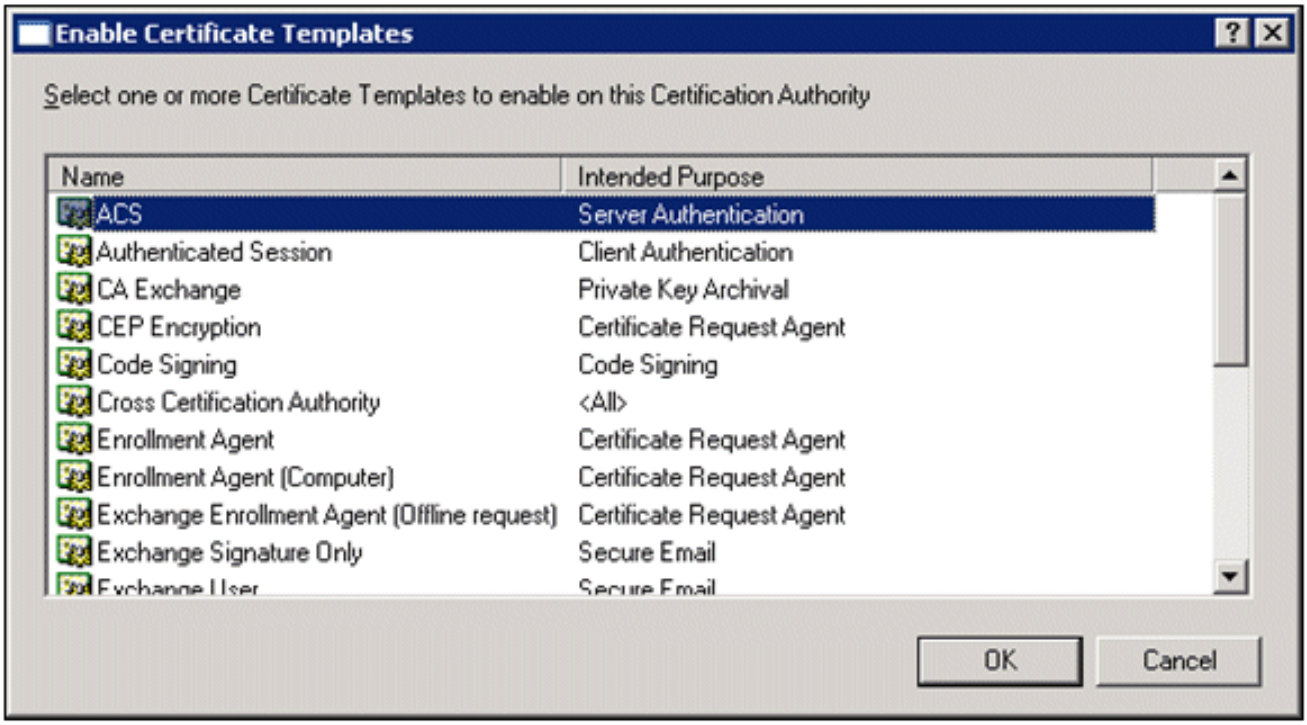
قم بإجراء هذه الخطوات:

1. فتح الأداة الإضافية "مرجع الشهادات". أنجزت الخطوات من 1 إلى 3 في ال create الشهادة قالب ل ال ACS ويب نادل قسم، **يختار المرجع مصدق** خيار، يختار **حاسوب محلي**، وطقطقة **إنجاز**.
2. في شجرة وحدة تحكم المرجع المصدق، قم بتوسيع **ca.demo.local**، ثم انقر بزر الماوس الأيمن على **قوالب الترخيص**.
3. انتقل إلى **جديد** > **قالب الشهادة المراد**

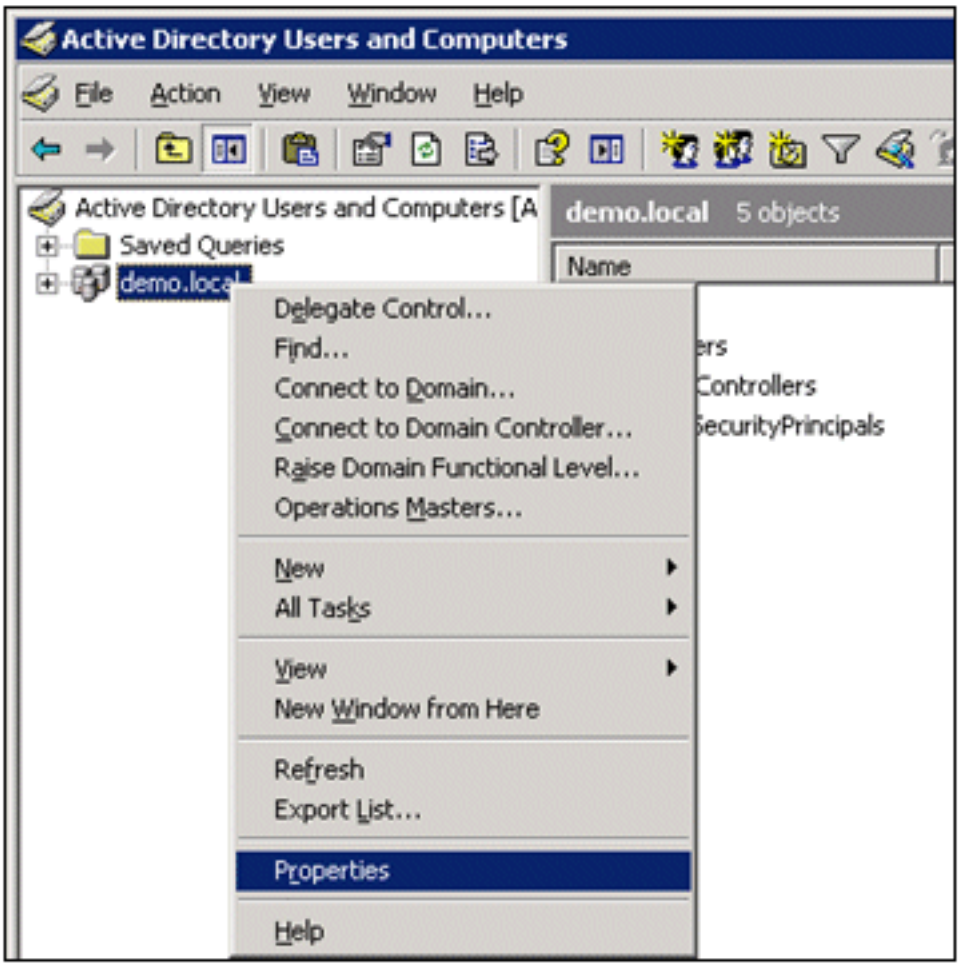


إصداره.

4. انقر على **قالب شهادة** **ACS**.

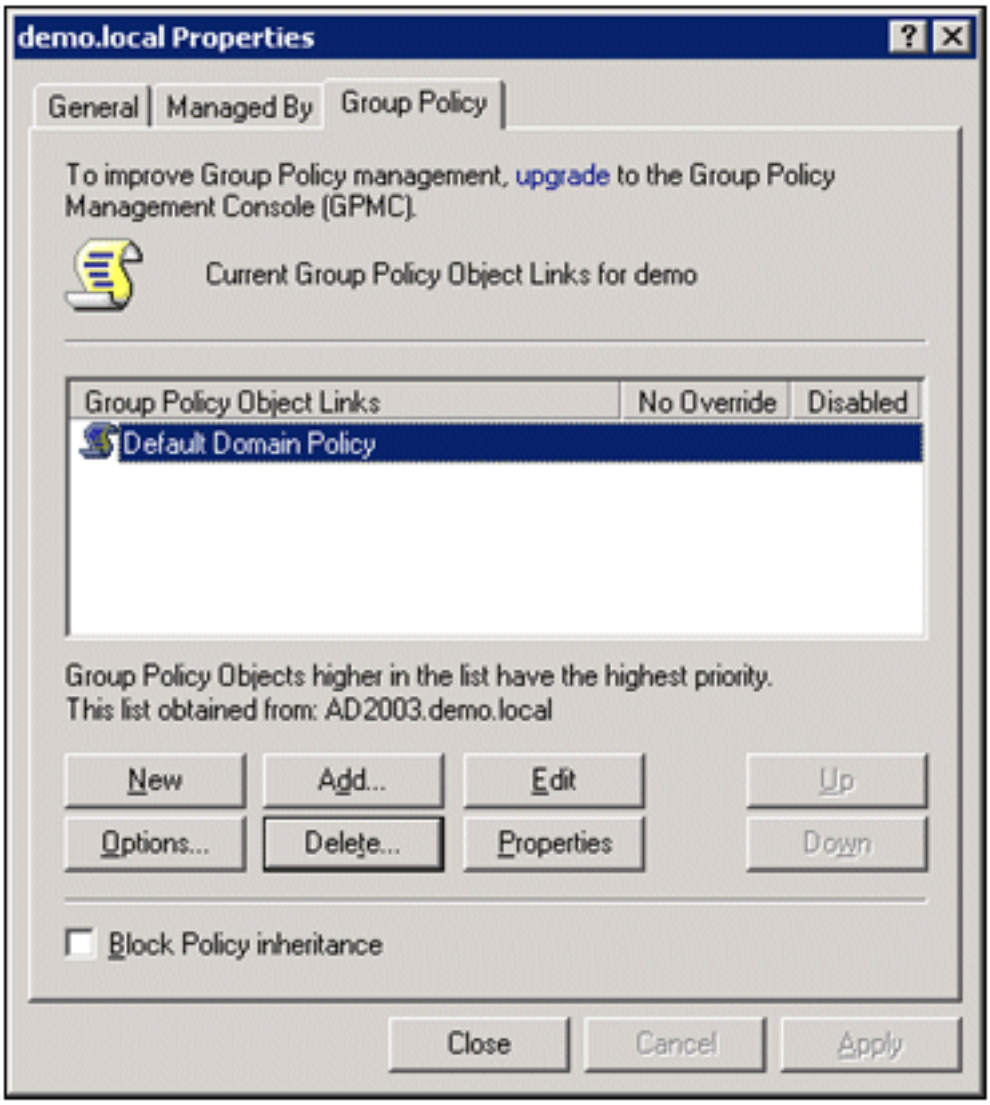


5. انقر فوق **موافق** وافتح الأداة الإضافية **Active Directory Users and Computers**.
6. في شجرة وحدة التحكم، انقر نقرا مزدوجا فوق **Active Directory Users and Computers**، ثم انقر بزر الماوس الأيمن فوق **الإصدار التجريبي.local**، ثم انقر فوق



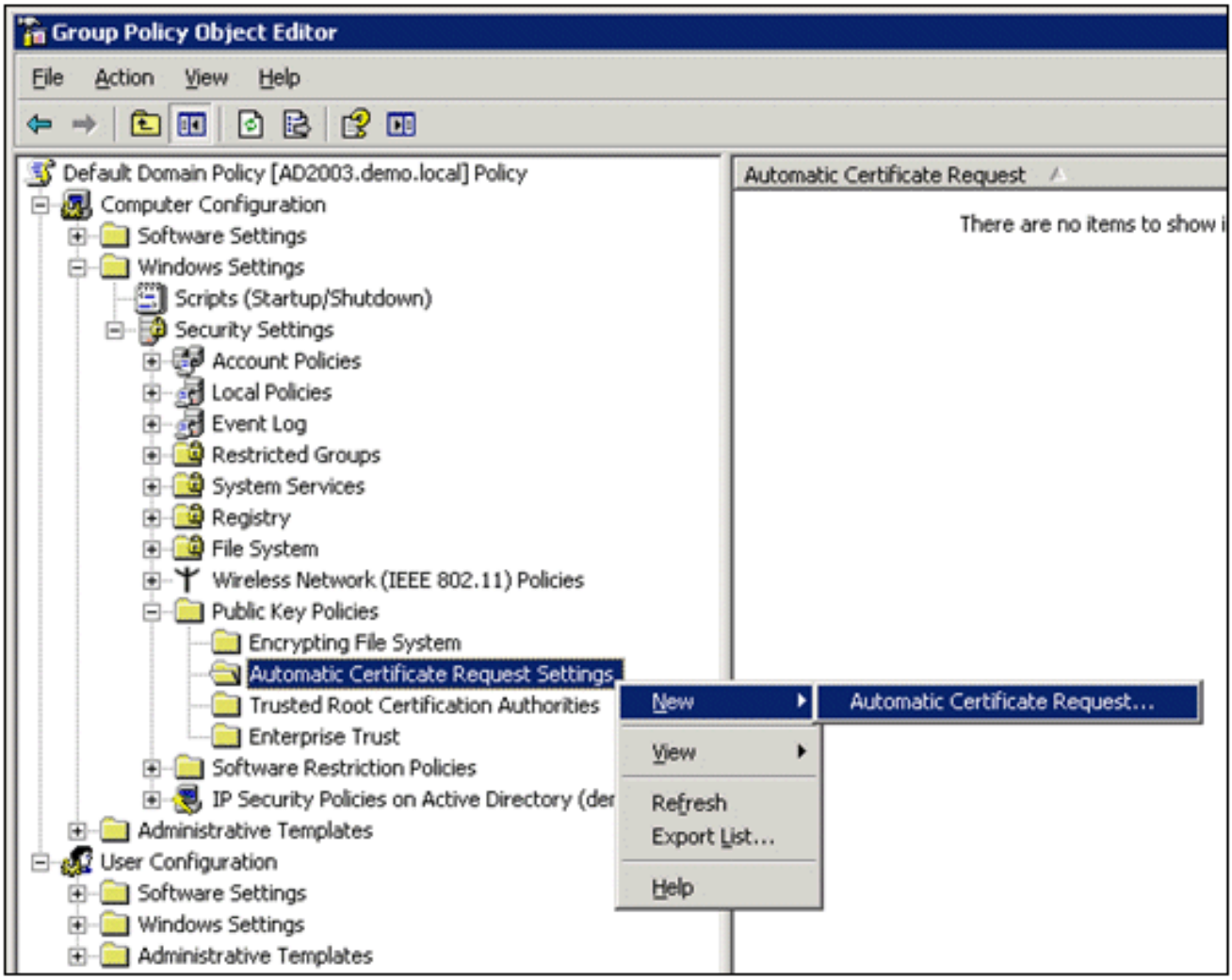
خصائص.

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".

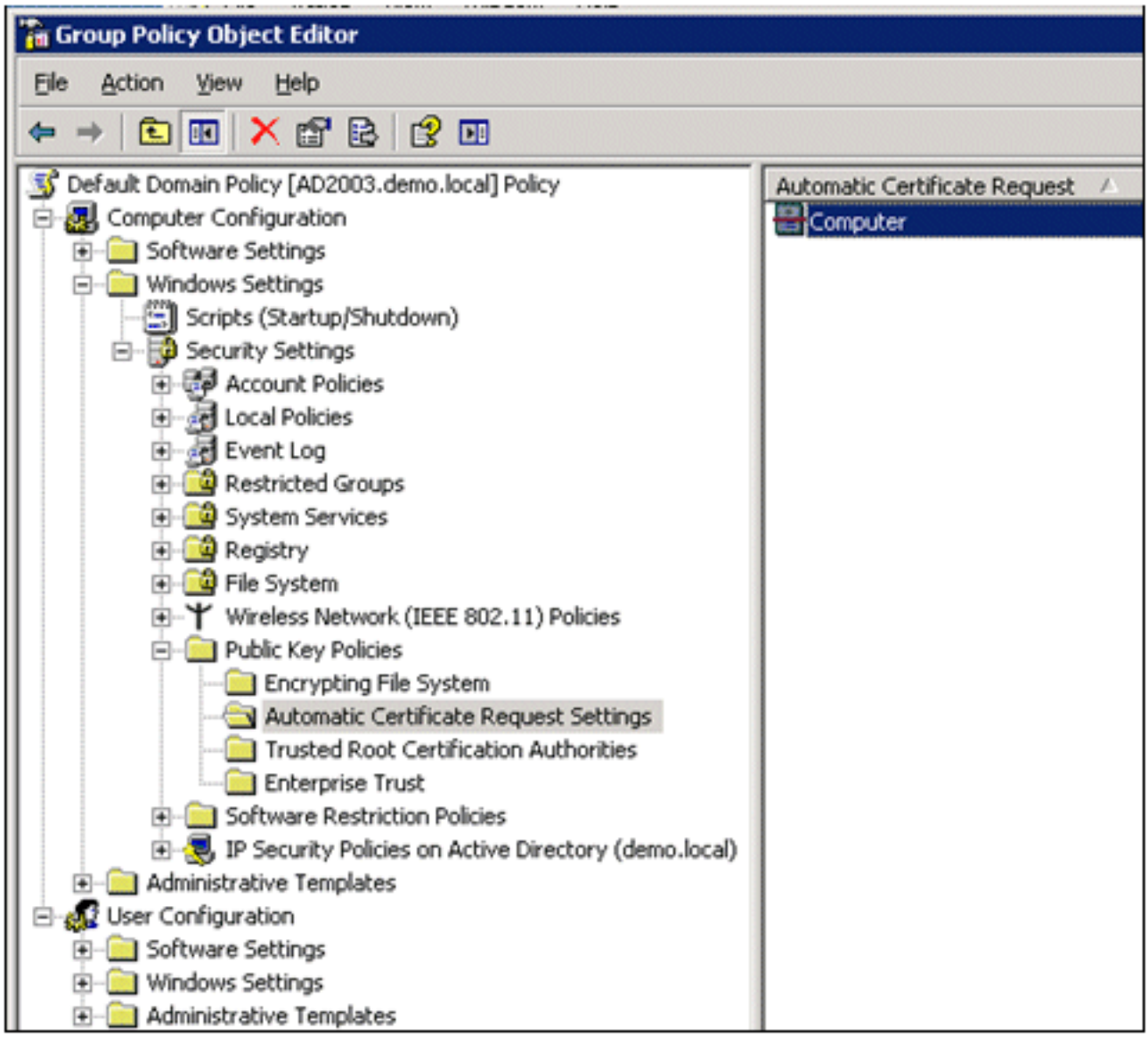
8. في شجرة وحدة التحكم، قم بتوسيع تكوين جهاز الكمبيوتر > **إعدادات Windows** > **إعدادات التأمين** > **سياسات المفتاح العام**، ثم أختر إعدادات طلب الترخيص الآلي.



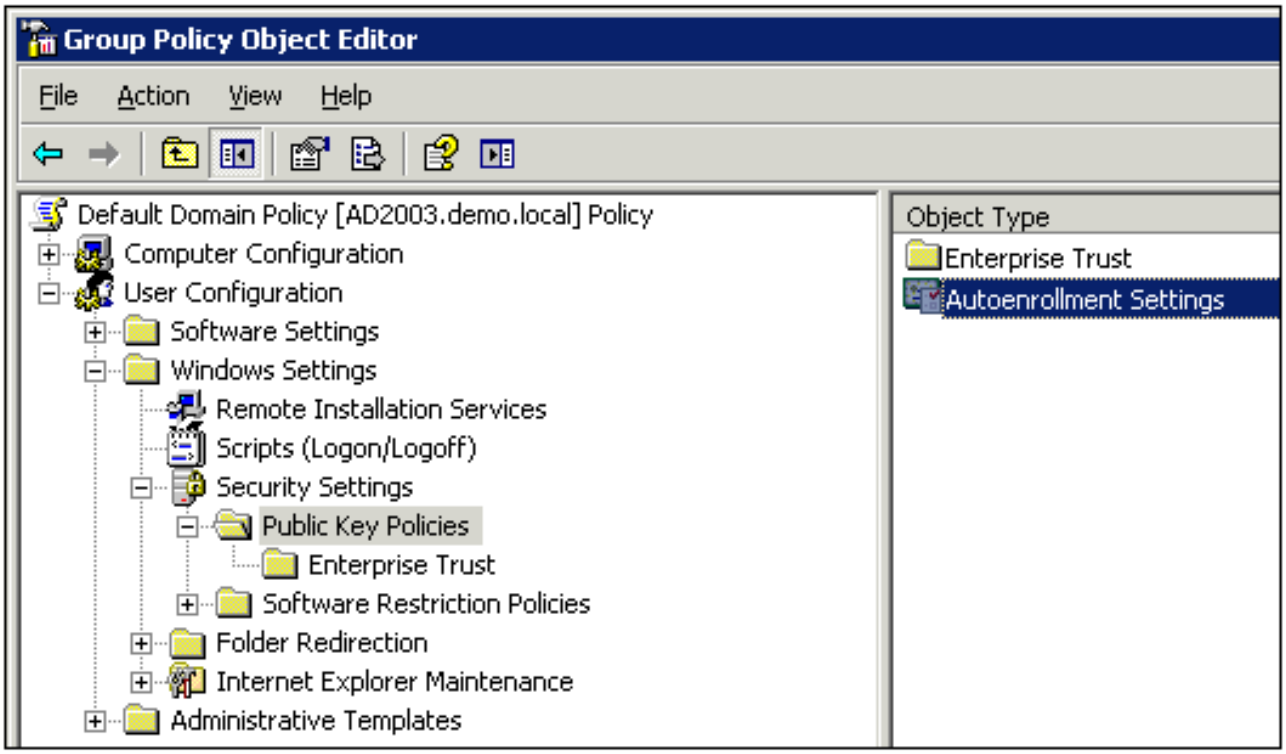
9. انقر بزر الماوس الأيمن على **إعدادات طلب الترخيص الآلي**، واختر **جديد > طلب الترخيص التلقائي**.
10. في صفحة "معالج إعداد طلب الشهادة التلقائي"، انقر فوق **التالي**.
11. في صفحة "قالب الشهادة"، انقر على **الكمبيوتر**، ثم انقر على

التالي.

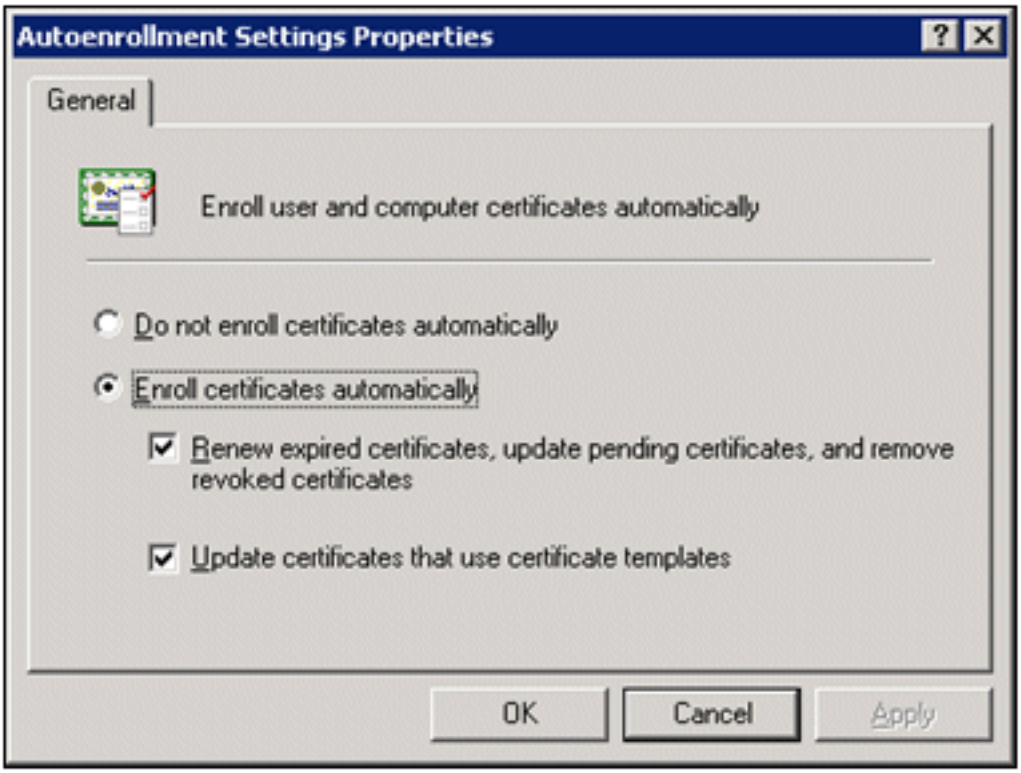
12. عند إتمام صفحة معالج إعداد طلب الشهادة التلقائي، انقر فوق **إنهاء**. يظهر الآن نوع شهادة الكمبيوتر في جزء التفاصيل الخاص بالأداة الإضافية "محرر كائنات نهج المجموعة".



13. في شجرة وحدة التحكم، قم بتوسيع **تكوين المستخدم>إعدادات Windows>إعدادات الأمان>سياسات المفتاح العام**.
14. في جزء التفاصيل، انقر نقرا مزدوجا على **إعدادات التسجيل التلقائي**.



15. أختر **تسجيل الشهادات تلقائيا** وافحص **تجديد الشهادات منتهية الصلاحية وتحديث الشهادات المعلقة وإزالة الشهادات الملغاة وتحديث الشهادات التي تستخدم قوالب**



الشهادات.

16. وانقر فوق **OK**.

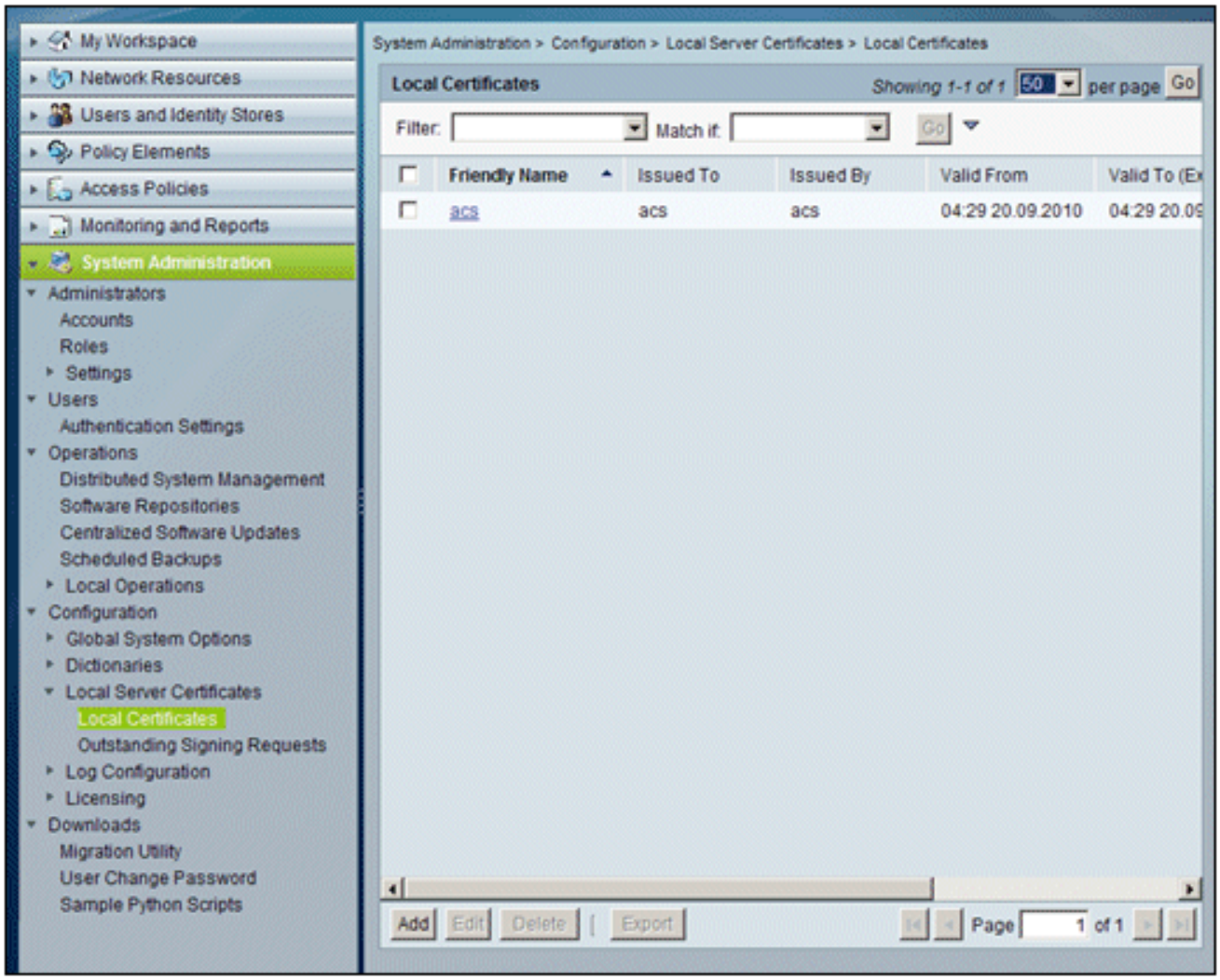
إعداد شهادة ACS 5.1

تكوين الشهادة القابلة للتصدير ل ACS

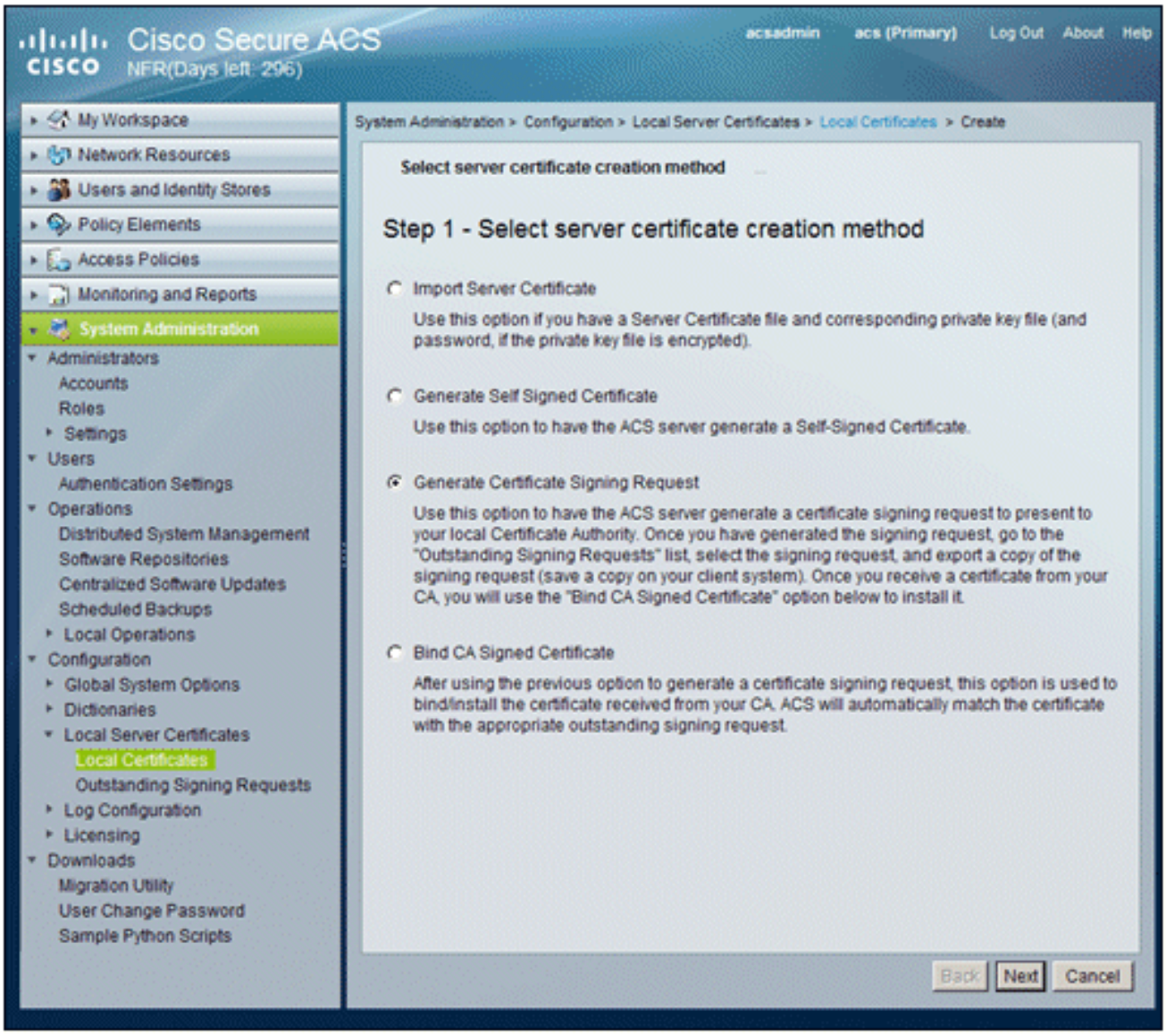
ملاحظة: يجب أن يحصل خادم ACS على شهادة خادم من خادم CA الجذر للمؤسسة لمصادقة عميل WLAN PEAP.

ملاحظة: تأكد من عدم فتح إدارة IIS أثناء عملية إعداد الشهادة كسبب لمشاكل في المعلومات المخزنة مؤقتا.

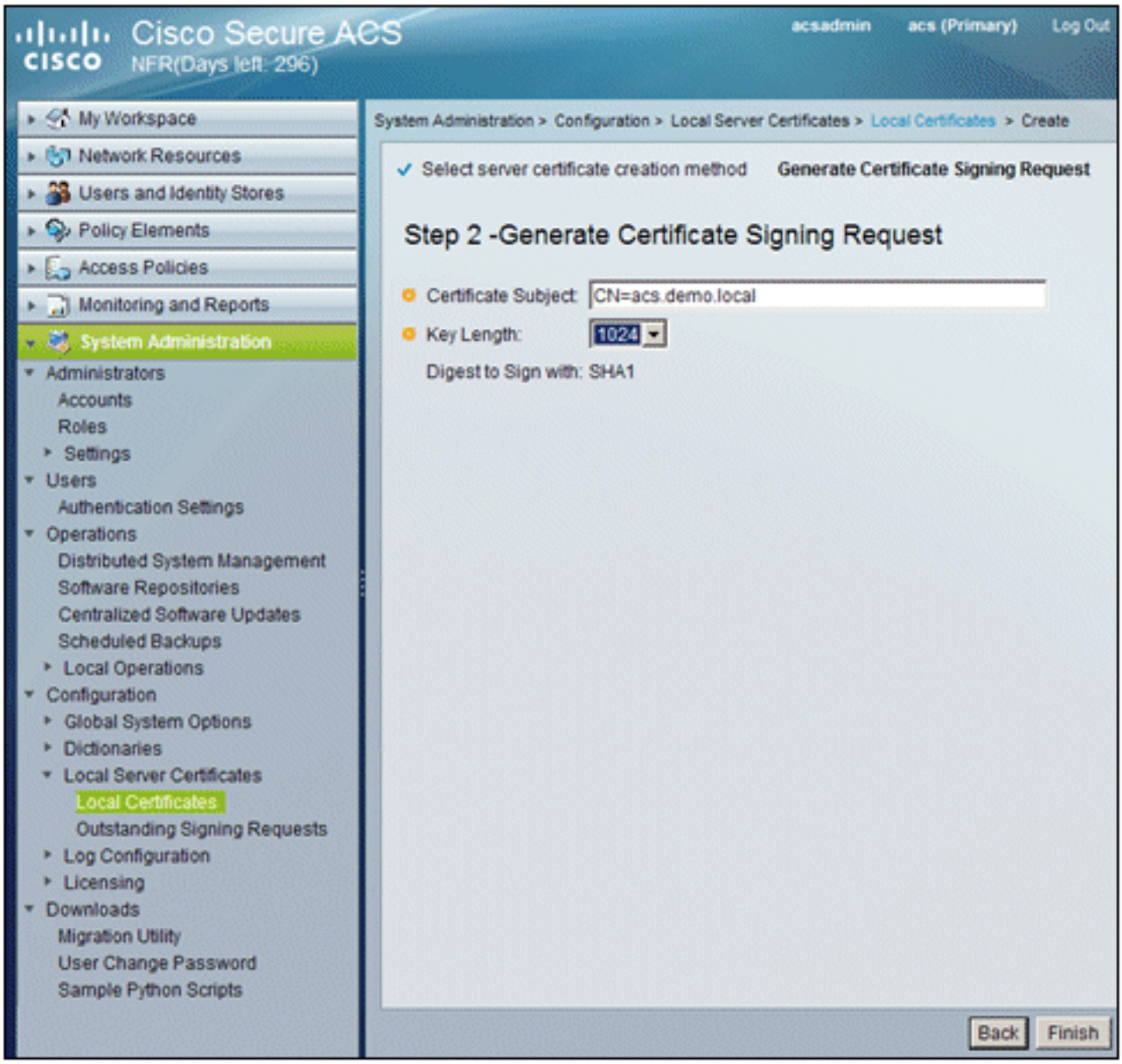
1. قم بتسجيل الدخول إلى خادم ACS باستخدام حقوق مسؤول الحساب.
2. انتقل إلى **إدارة النظام > التكوين > شهادات الخادم المحلي**. انقر فوق **إضافة (Add)**.



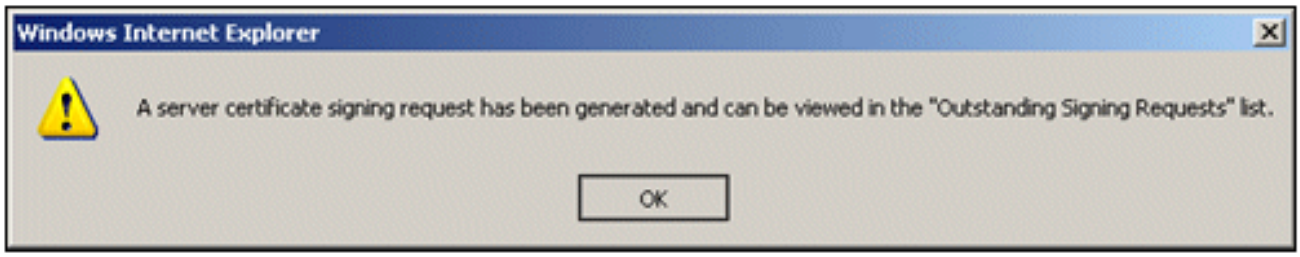
3. عندما تختار طريقة إنشاء شهادة خادم، أختر **إنشاء طلب توقيع شهادة**. انقر فوق **Next (التالي)**.



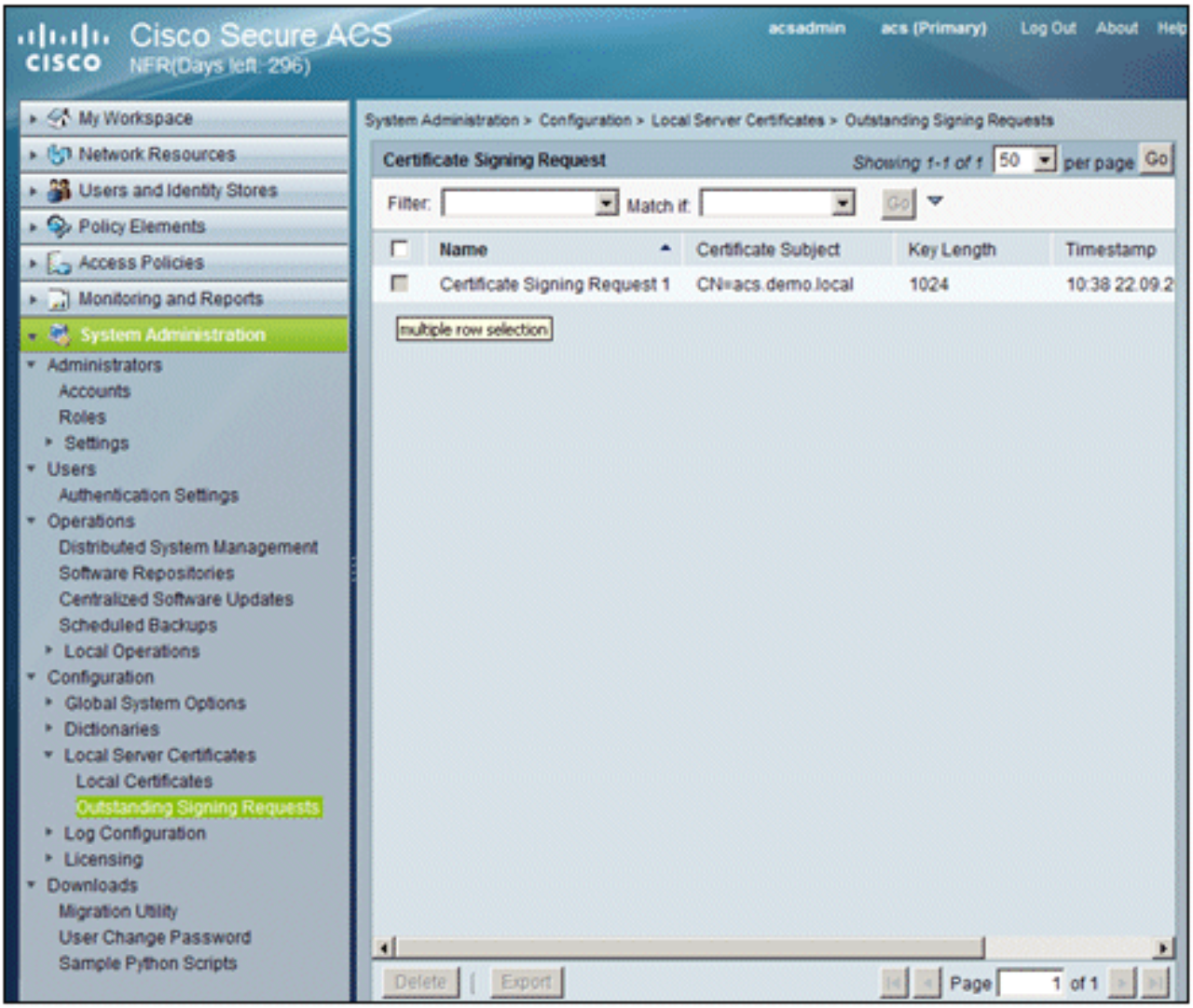
4. أدخل موضوع الشهادة وطول المفتاح كمثال، ثم انقر على **إنهاء**:موضوع الشهادة - **CN=acs.demo.local**طول المفتاح - **1024**



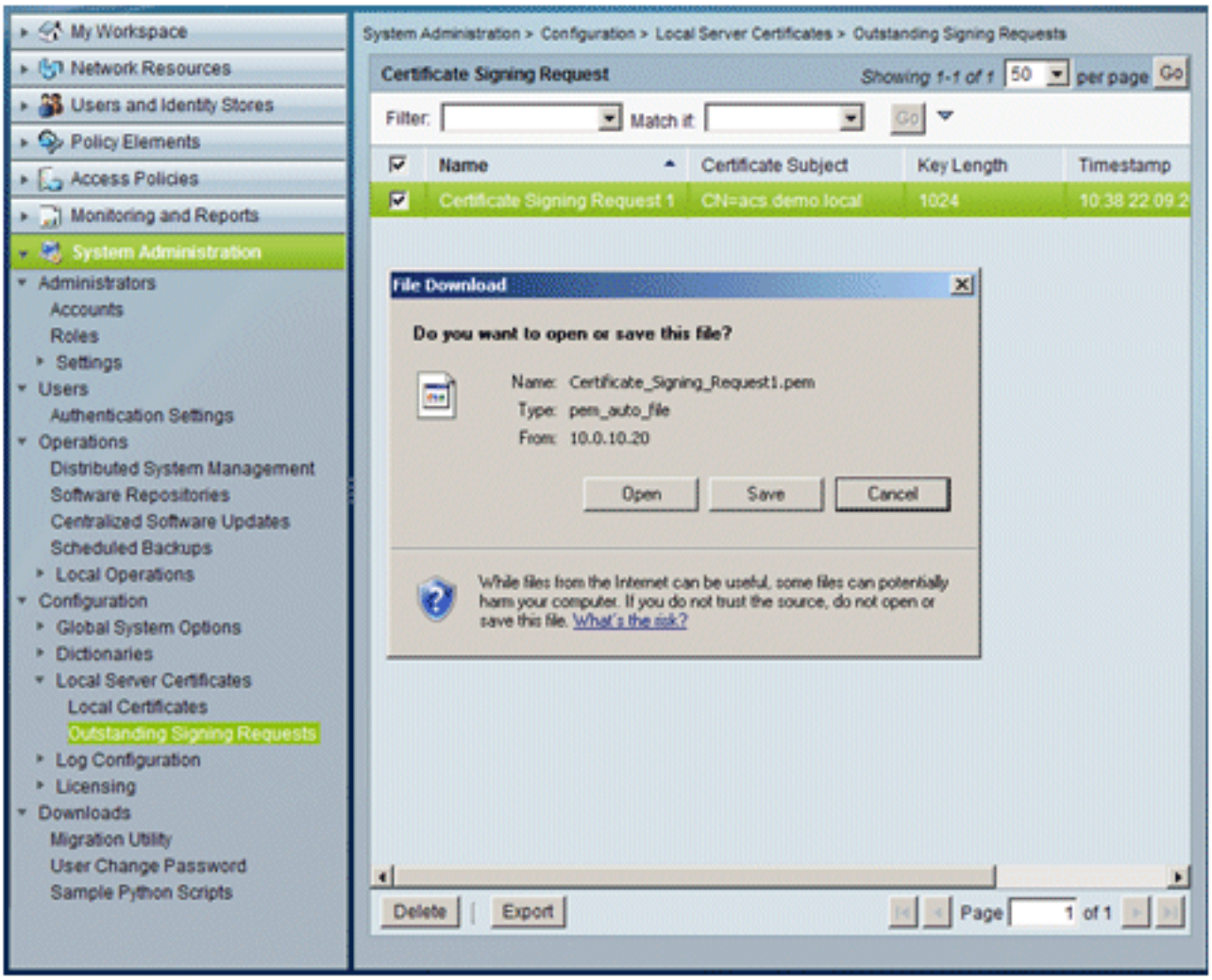
5. سيطالبك ACS بإنشاء طلب توقيع شهادة. وانقر فوق **OK**.



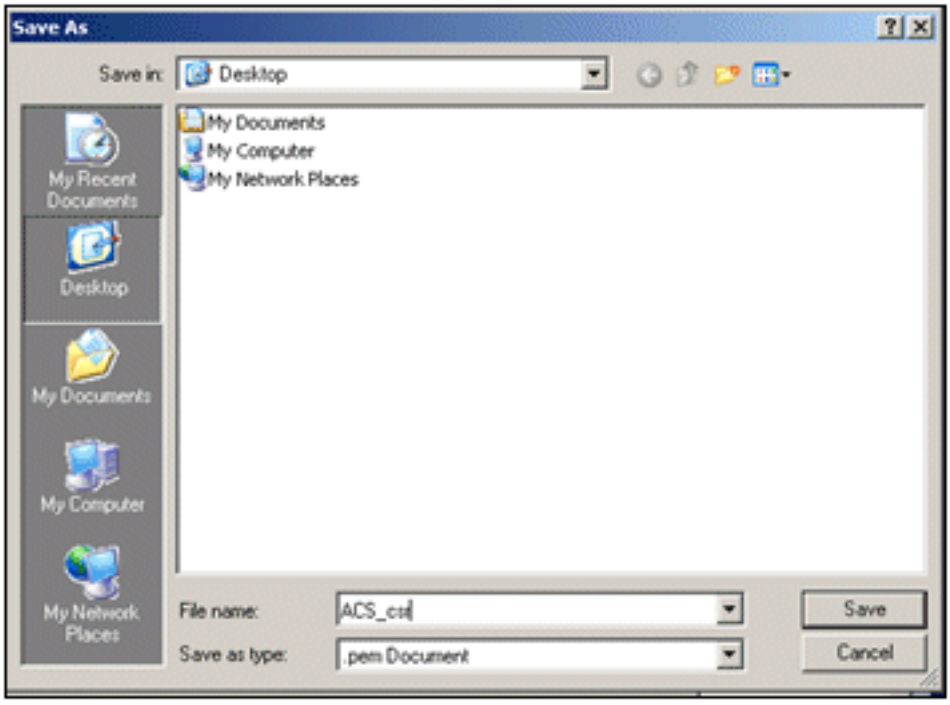
6. تحت إدارة النظام، انتقل إلى **التكوين > شهادات الخادم المحلي > طلبات التوقيع المعلقة.ملاحظة:** السبب وراء هذه الخطوة هو أن Windows 2003 لا يسمح بالمفاتيح القابلة للتصدير وأنك تحتاج إلى إنشاء طلب شهادة استنادا إلى شهادة ACS التي قمت بإنشائها سابقا والتي تسمح بذلك.



7. أختر إدخال **طلب توقيع الشهادة**، وانقر **تصدير**.



8. احفظ ملف شهادة **pem.** ACS إلى سطح

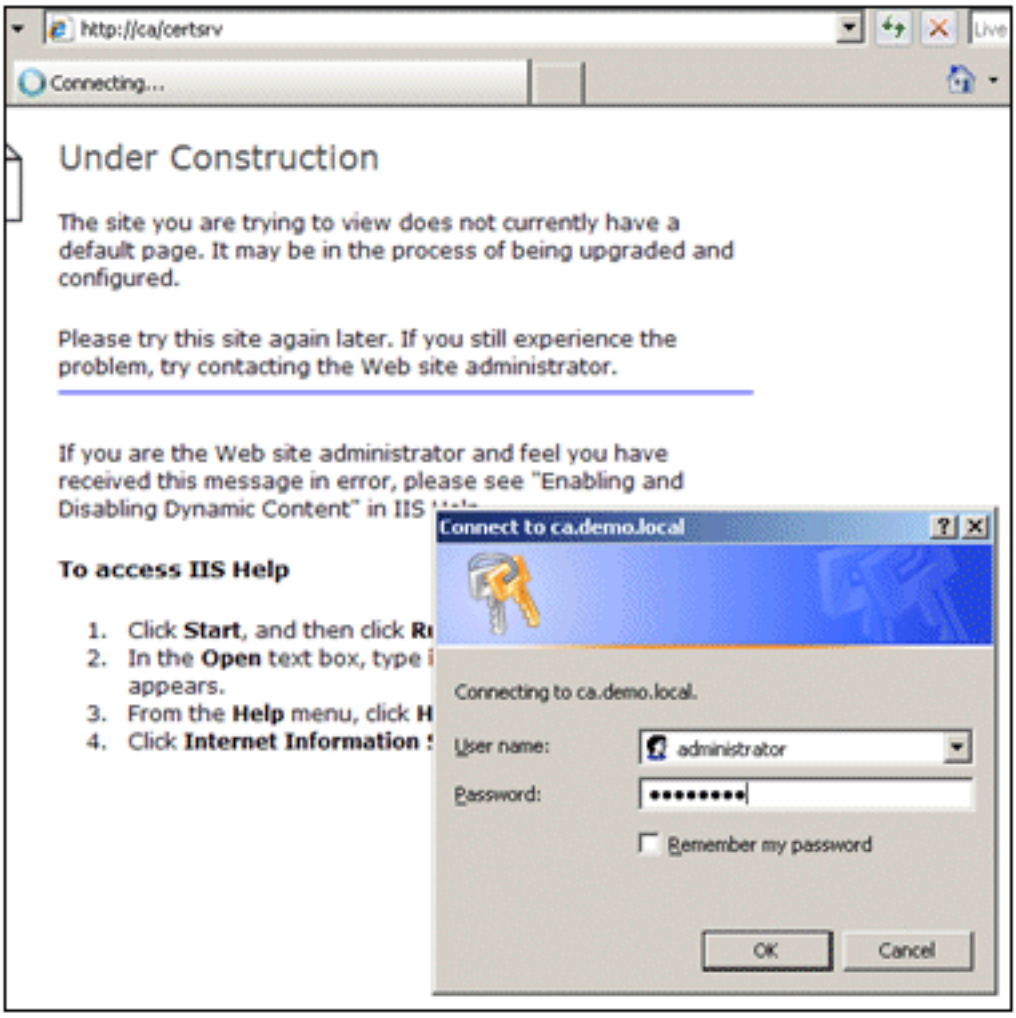


المكتب.

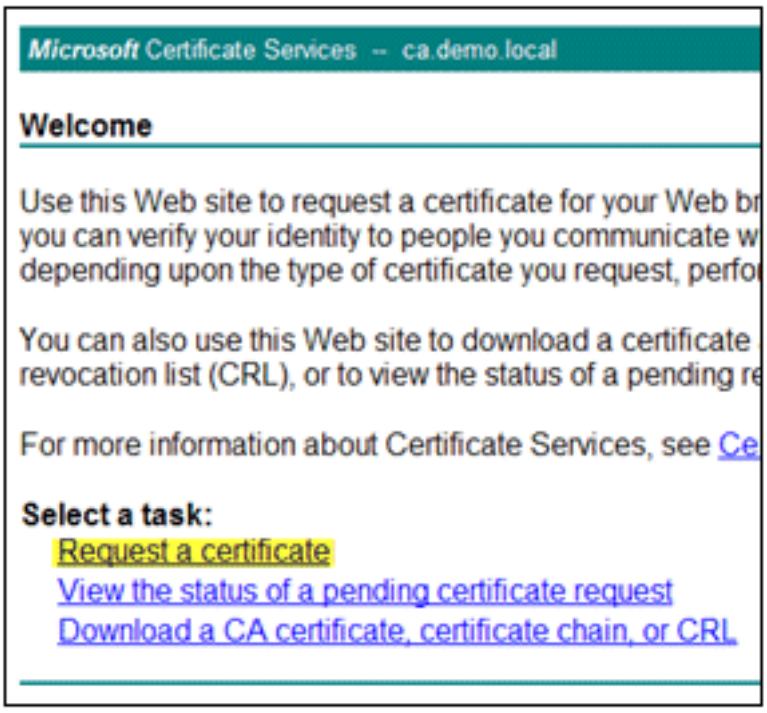
[تثبيت الشهادة في برنامج ACS 5.1]

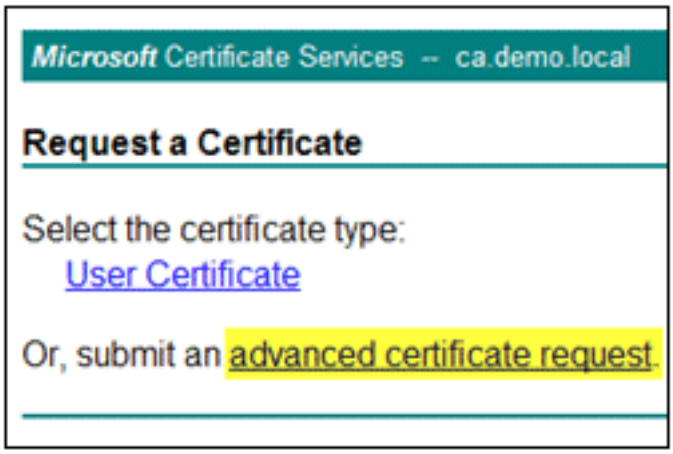
قم بإجراء هذه الخطوات:

1. افتح متصفح واتصل بعنوان URL لخادم CA
http://10.0.10.10/certsrv.

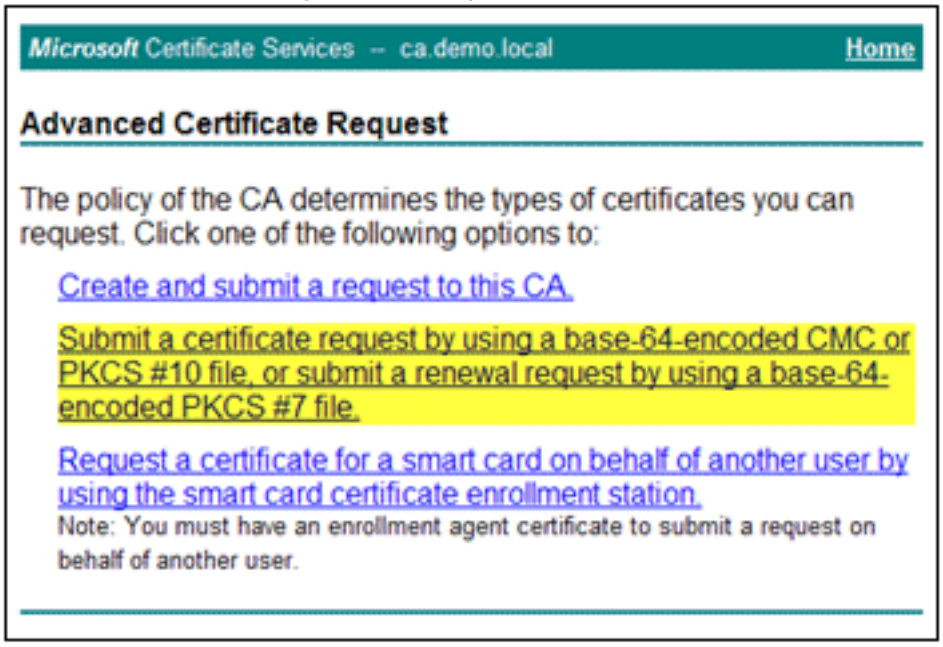


2. يظهر إطار Microsoft Certificate Services. أختر **طلب شهادة**.

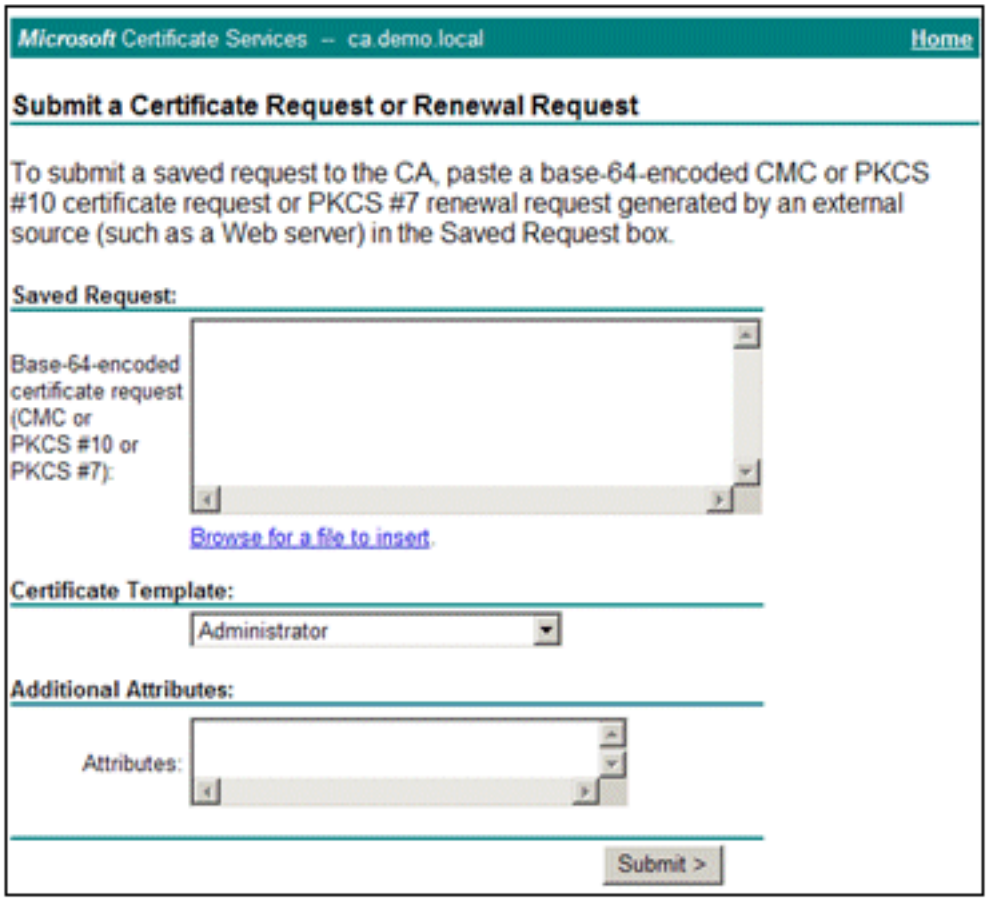




3. انقر لإرسال **طلب شهادة متقدم**.
4. في الطلب المتقدم، انقر فوق **إرسال طلب شهادة باستخدام مرمز -base** 64...

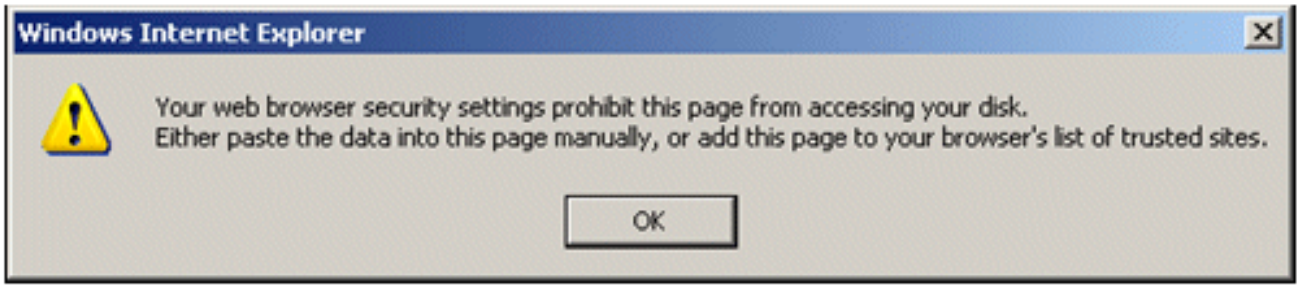


5. في حقل "الطلب المحفوظ"، إذا كان أمان المستعرض يسمح بذلك، استعرض إلى ملف طلب شهادة ACS

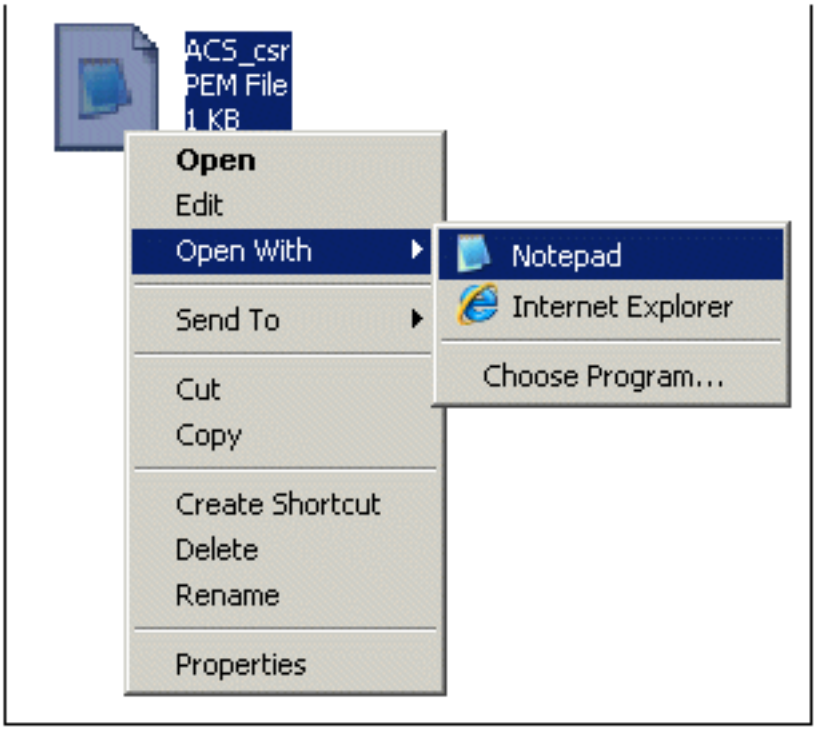


السابق وقم بالإدراج.

6. قد لا تسمح إعدادات أمان المستعرض بالوصول إلى الملف الموجود على قرص. إذا كان الأمر كذلك، فانقر فوق **موافق** لإجراء لصق يدوي.

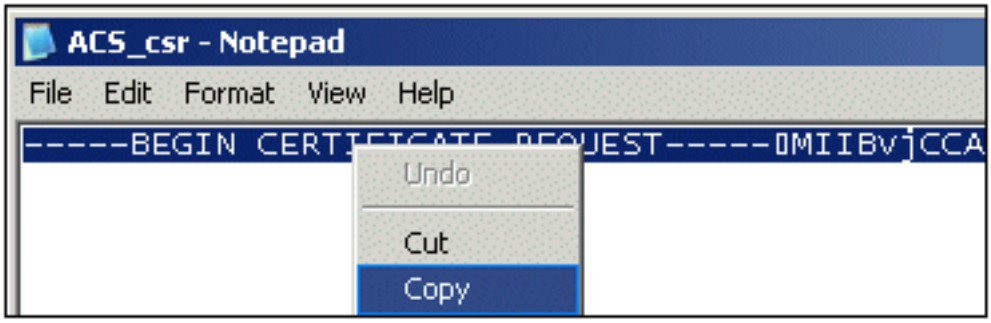


7. حدد موقع ملف ACS *.pem من مصدر ACS السابق. افتح الملف باستخدام محرر نصوص (على سبيل المثال،



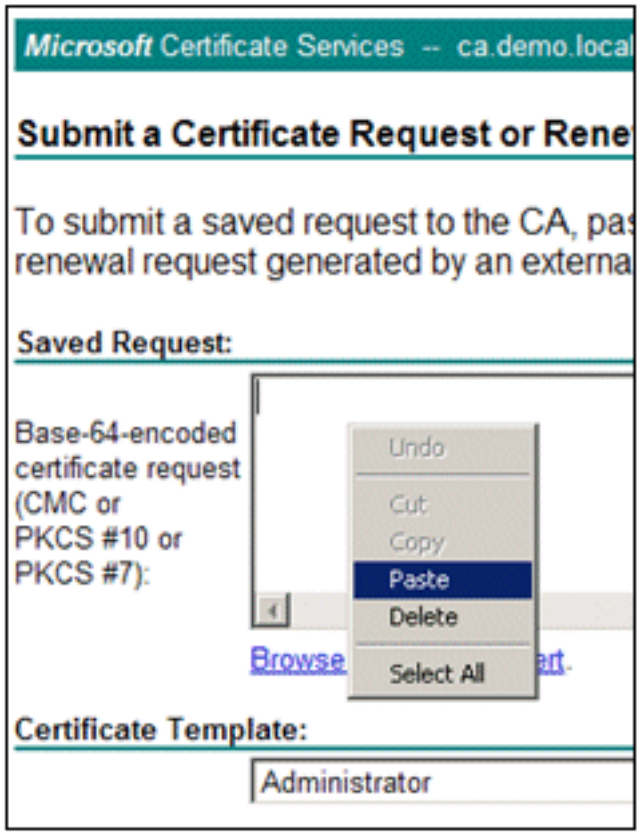
(Notepad).

8. قم بتمييز محتوى الملف بالكامل، وانقر



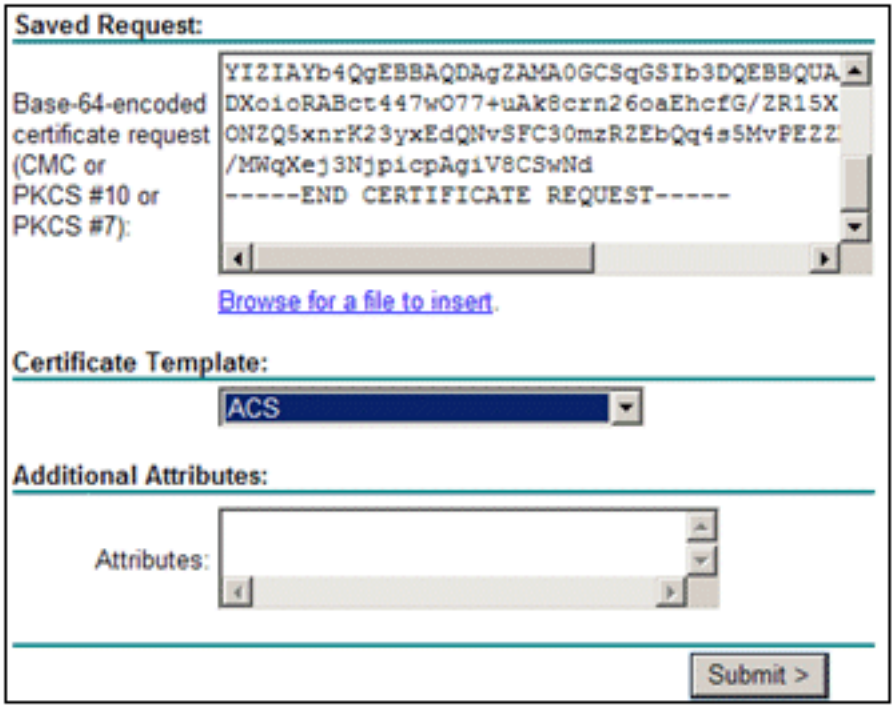
نسخ.

9. العودة إلى نافذة طلب شهادة Microsoft. **الصق** المحتوى المنسوخ في حقل الطلب



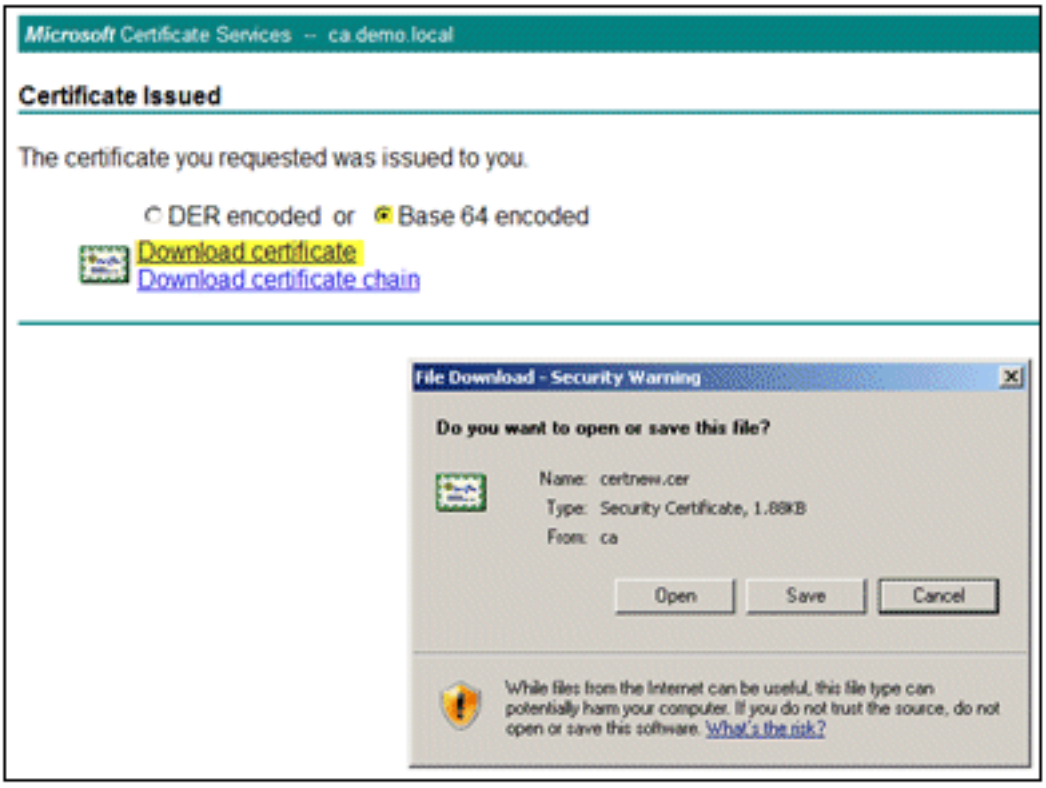
المحفوظ.

10. أختر **ACS** كقالب الشهادة، وانقر



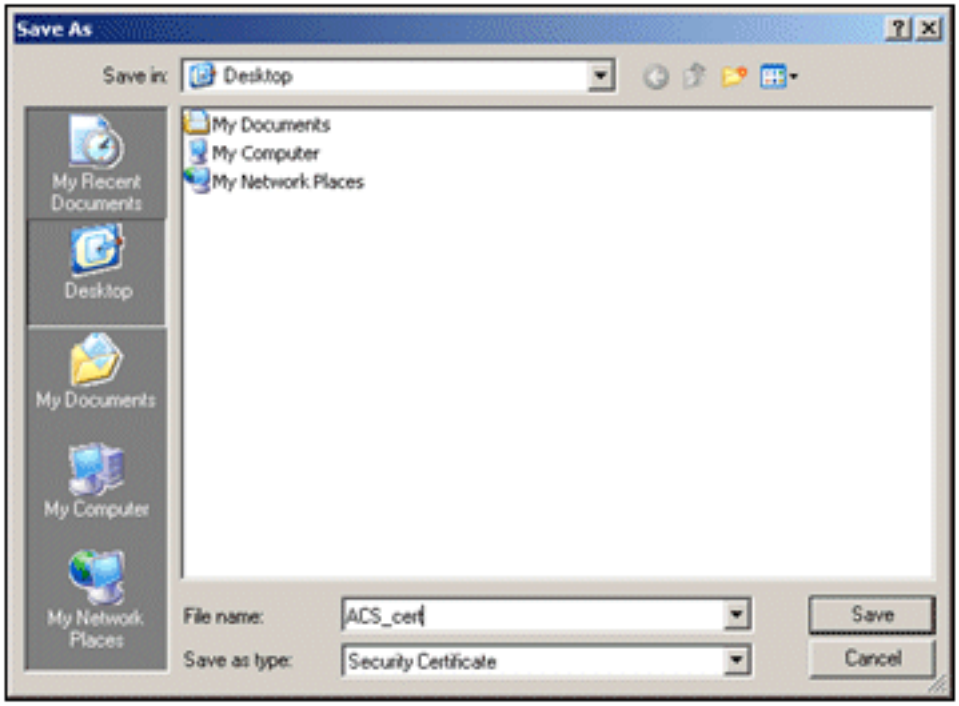
إرسال.

11. بمجرد إصدار الشهادة، أختر **Base 64 المشفر**، وانقر **تنزيل**



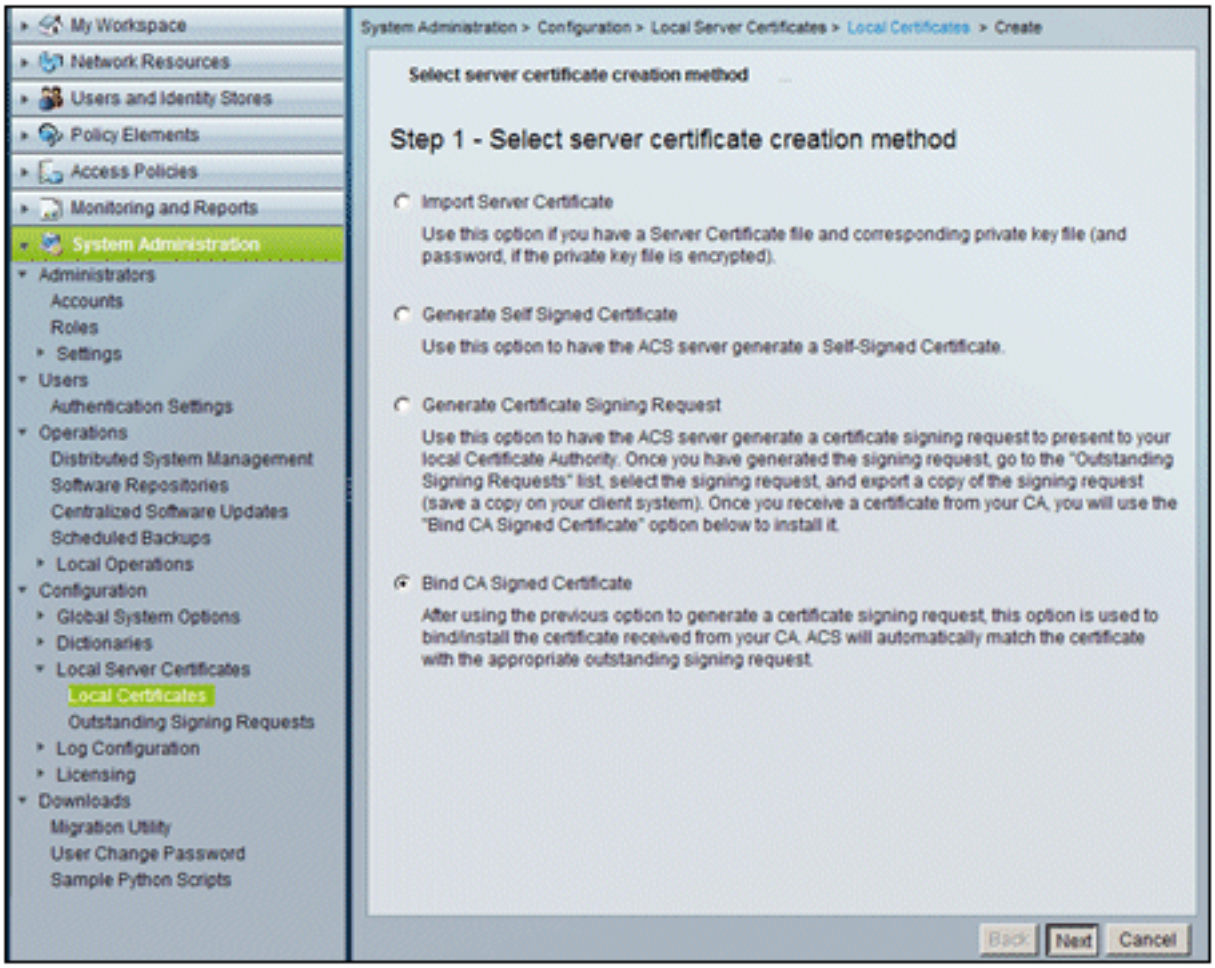
الشهادة.

12. انقر على **حفظ** لحفظ الشهادة على سطح

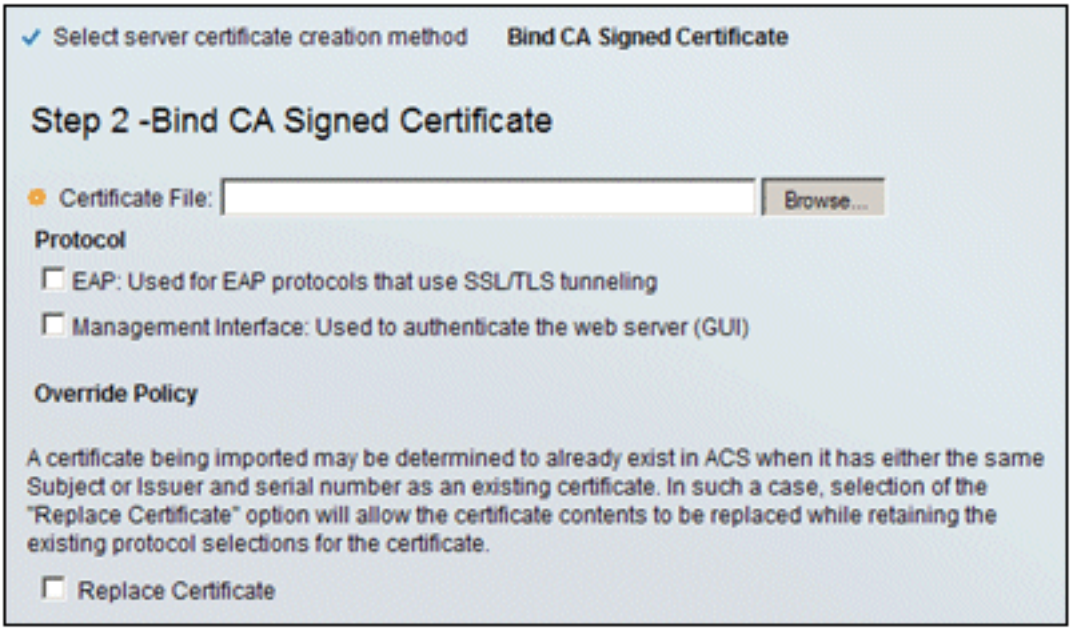


المكتب.

13. انتقل إلى **ACS>إدارة النظام>التكوين>شهادات الخادم المحلي**. أختر **ربط الشهادة الموقعة من المرجع المصدق**، وانقر **التالي**.

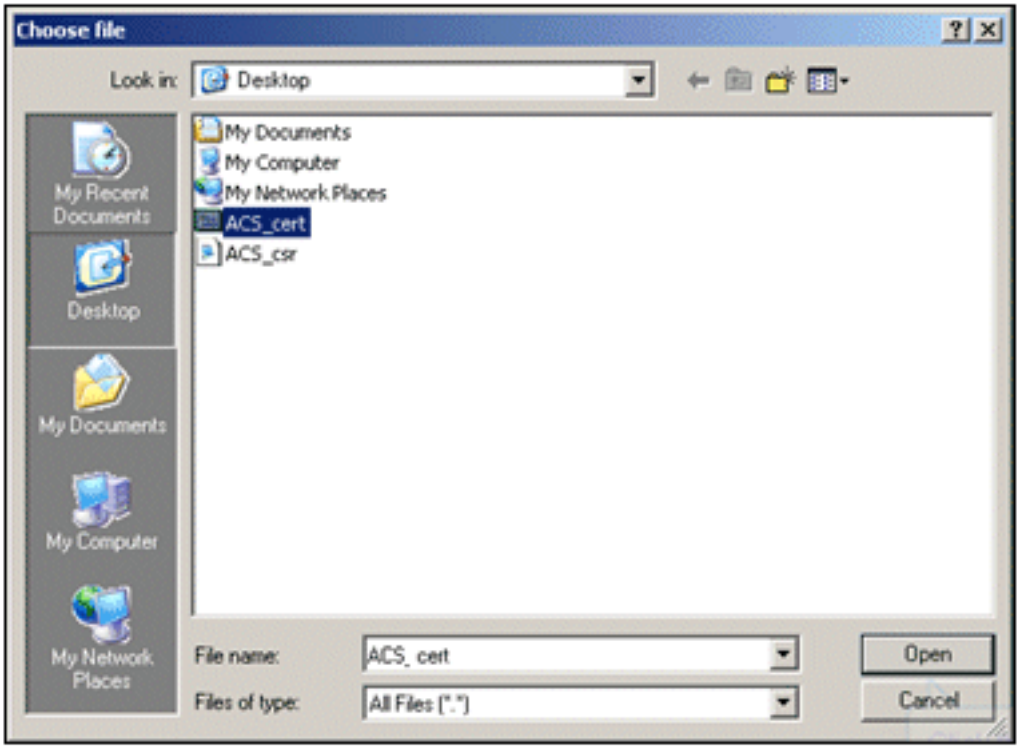


14. انقر على **إستعراض**، وحدد مكان الشهادة



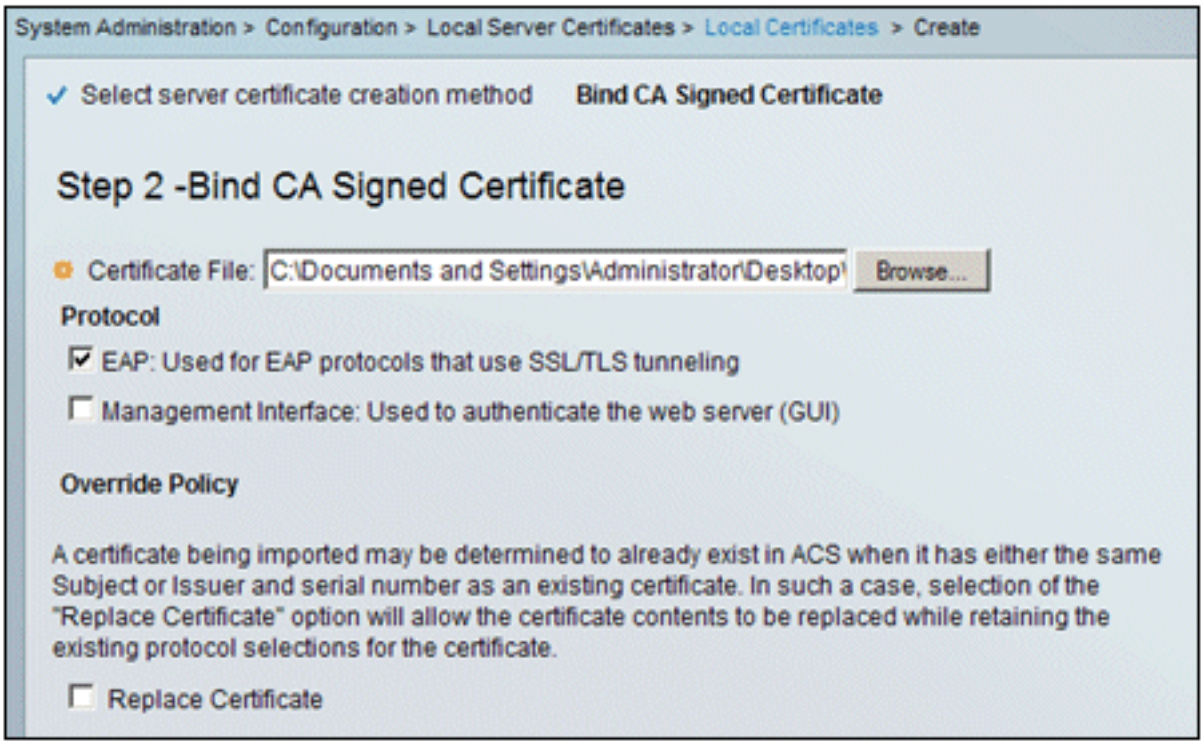
المحفوظة.

15. أختر شهادة ACS التي تم إصدارها بواسطة خادم CA، وانقر فوق



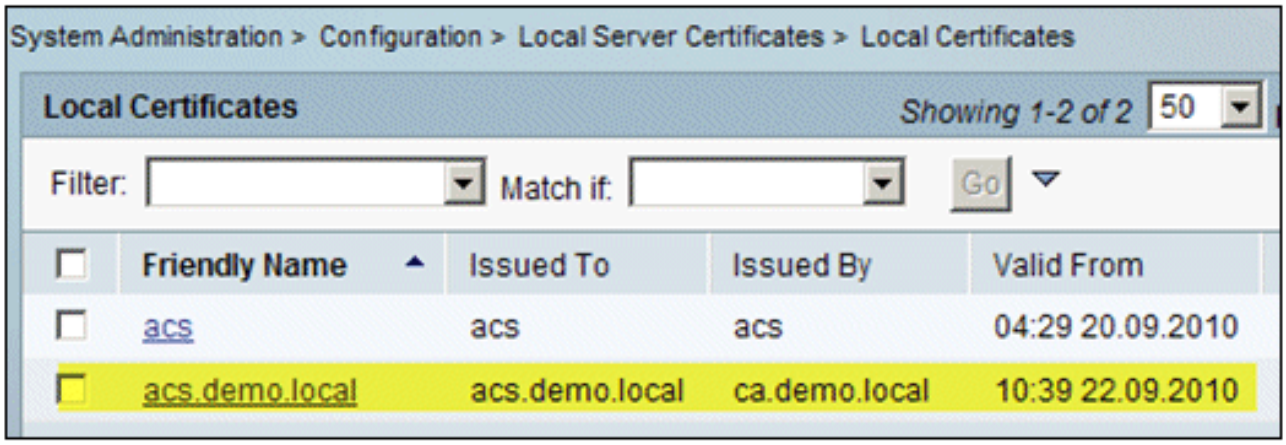
فتح.

16. تحقق أيضا من مربع البروتوكول ل **EAP**، وانقر



إنهاء.

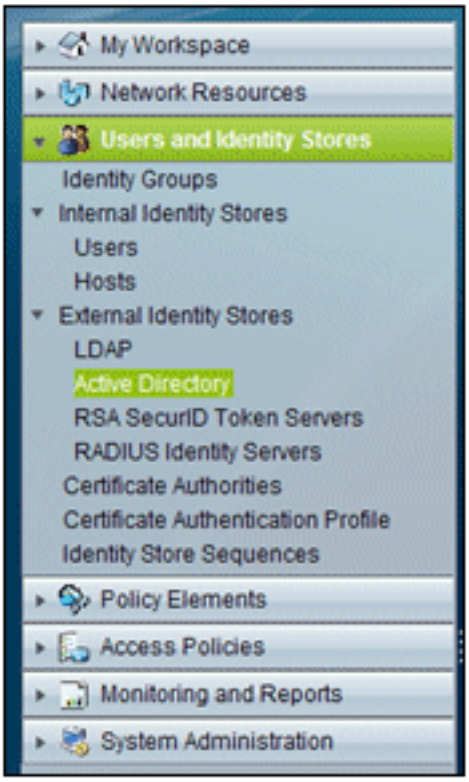
17. سوف تظهر شهادة ACS الصادرة عن CA في الشهادة المحلية ل ACS.



تكوين مخزن تعريف ACS ل Active Directory

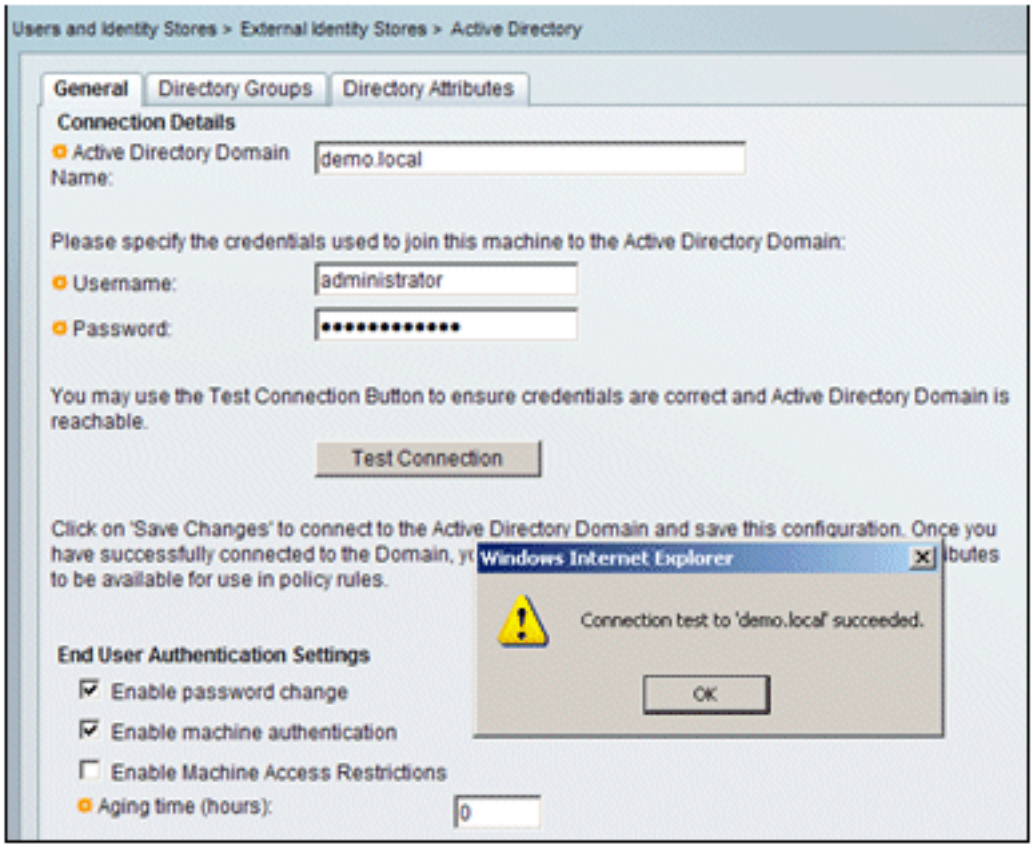
قم بإجراء هذه الخطوات:

1. اتصل ب ACS وسجل الدخول باستخدام حساب Admin.
2. انتقل إلى **Users and Identity Stores (المستخدمين ومتاجر الهويات) > مخازن الهويات الخارجية > Active**



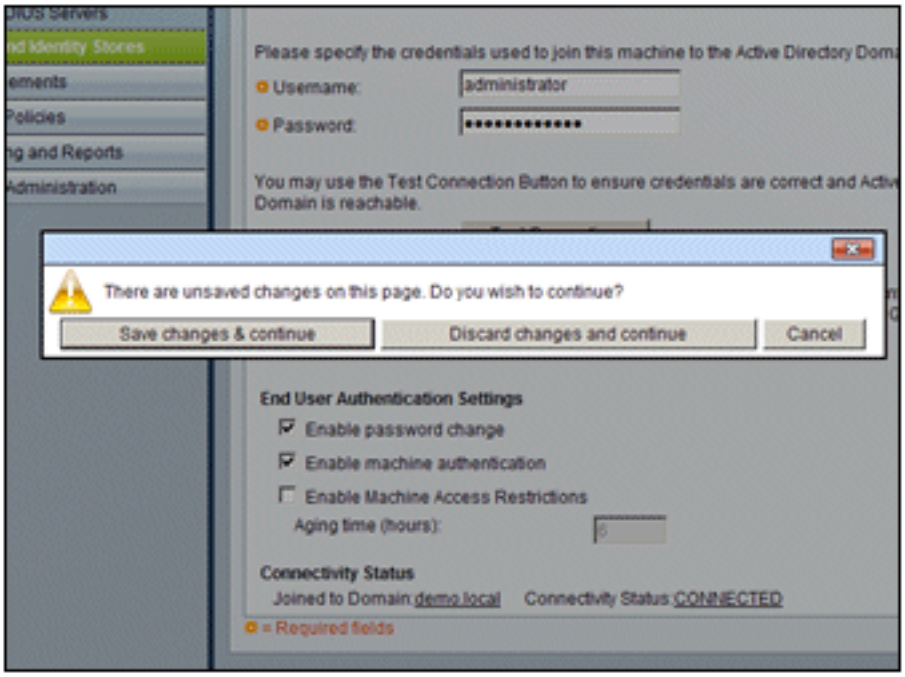
Directory.

3. أدخل *العرض التوضيحي* الخاص بمجال *local*.Active Directory، وأدخل كلمة المرور الخاصة بالخادم، وانقر فوق **إختبار الاتصال**. طقطقة ok in order to



تابعت.

4. انقر فوق **حفظ**



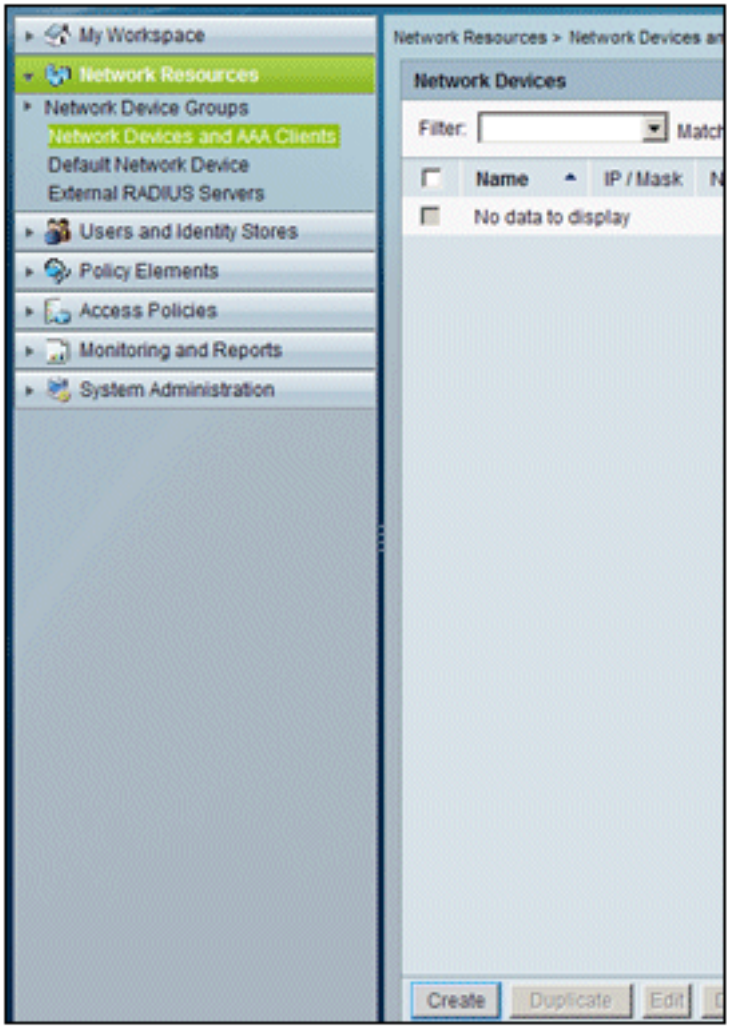
التغييرات.

ملاحظة: للحصول على مزيد من المعلومات حول إجراء التكامل مع ACS 5.x ارجع إلى ACS 5.x والإصدارات الأحدث: الدمج مع مثال تكوين Microsoft Active Directory.

إضافة وحدة تحكم إلى ACS كعميل AAA

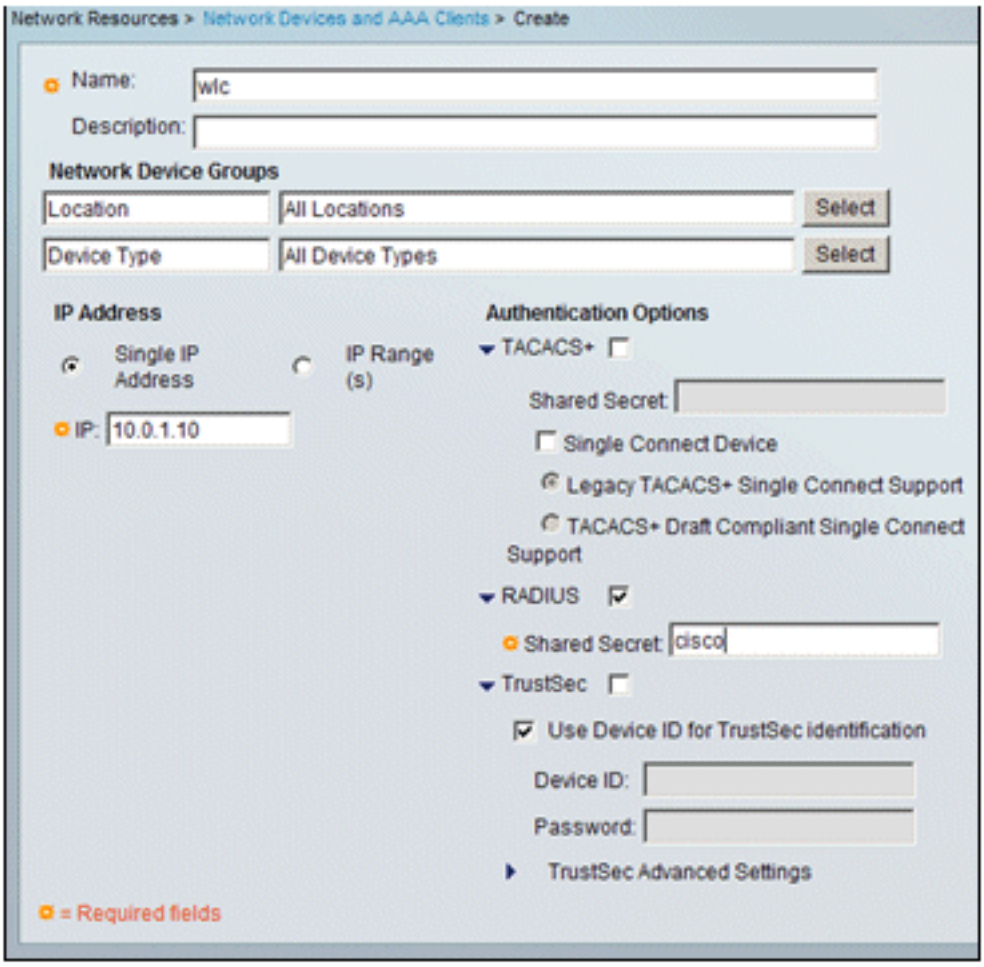
قم بإجراء هذه الخطوات:

1. قم بالاتصال ب ACS، وانتقل إلى **موارد الشبكة > أجهزة الشبكة وعملاء AAA**. طقطقة



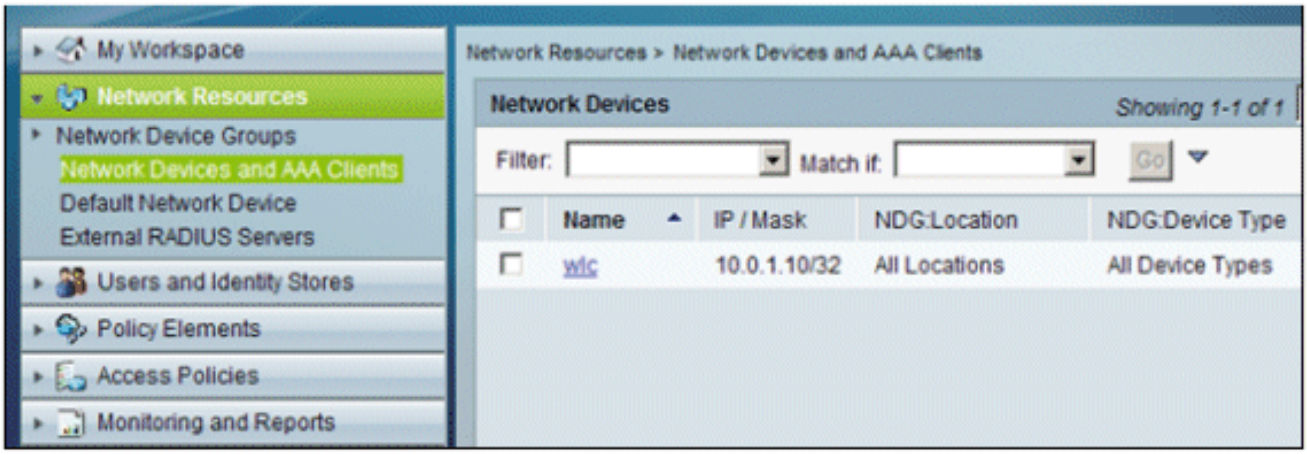
يخلق.

2. أدخل إلى هذه الحقول:الاسم - **10.0.1.10** - IP**WLC**خانة إختيار RADIUS - **محددة**سر مشترك -



Cisco

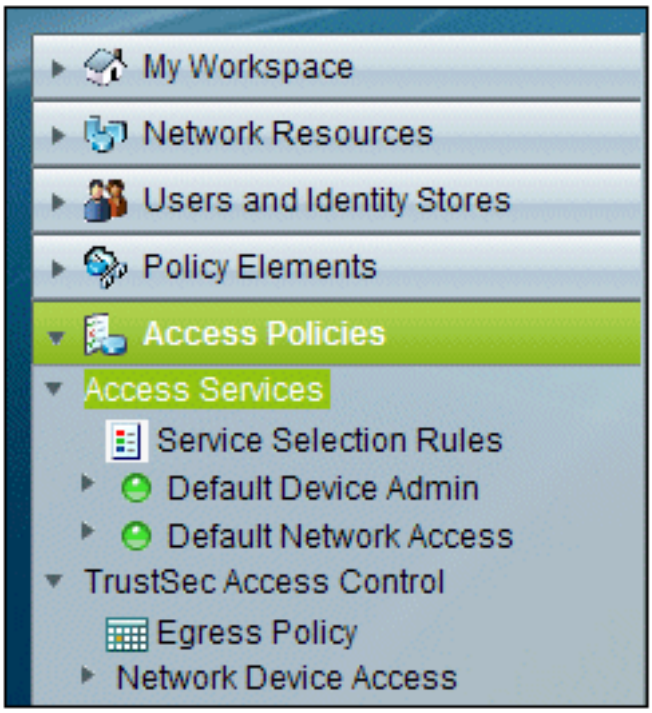
3. انقر فوق **إرسال** عند الانتهاء. ستظهر وحدة التحكم كإدخال في قائمة أجهزة شبكة ACS.



تكوين سياسات الوصول إلى ACS للشبكة اللاسلكية

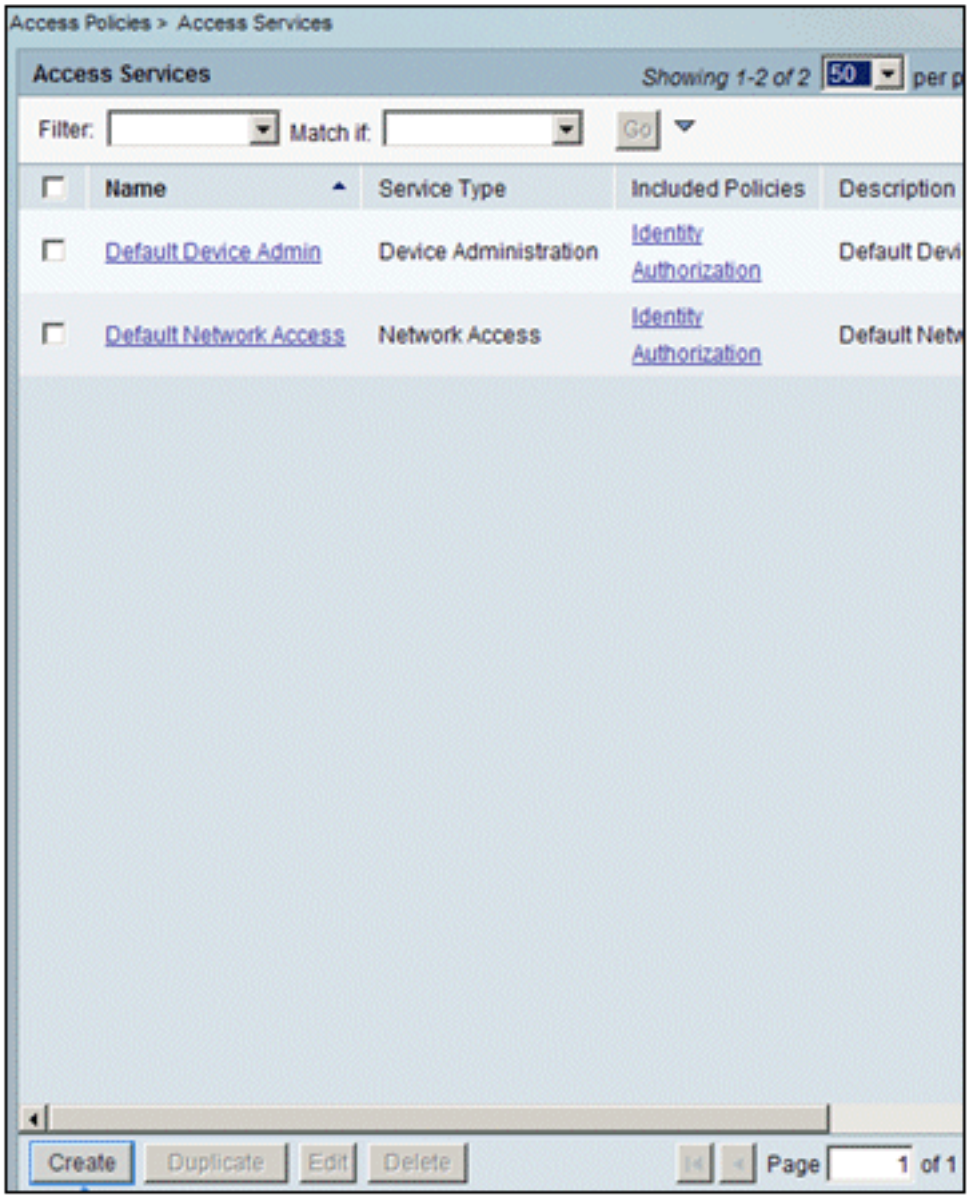
قم بإجراء هذه الخطوات:

1. في ACS، انتقل إلى **سياسات الوصول > خدمات**



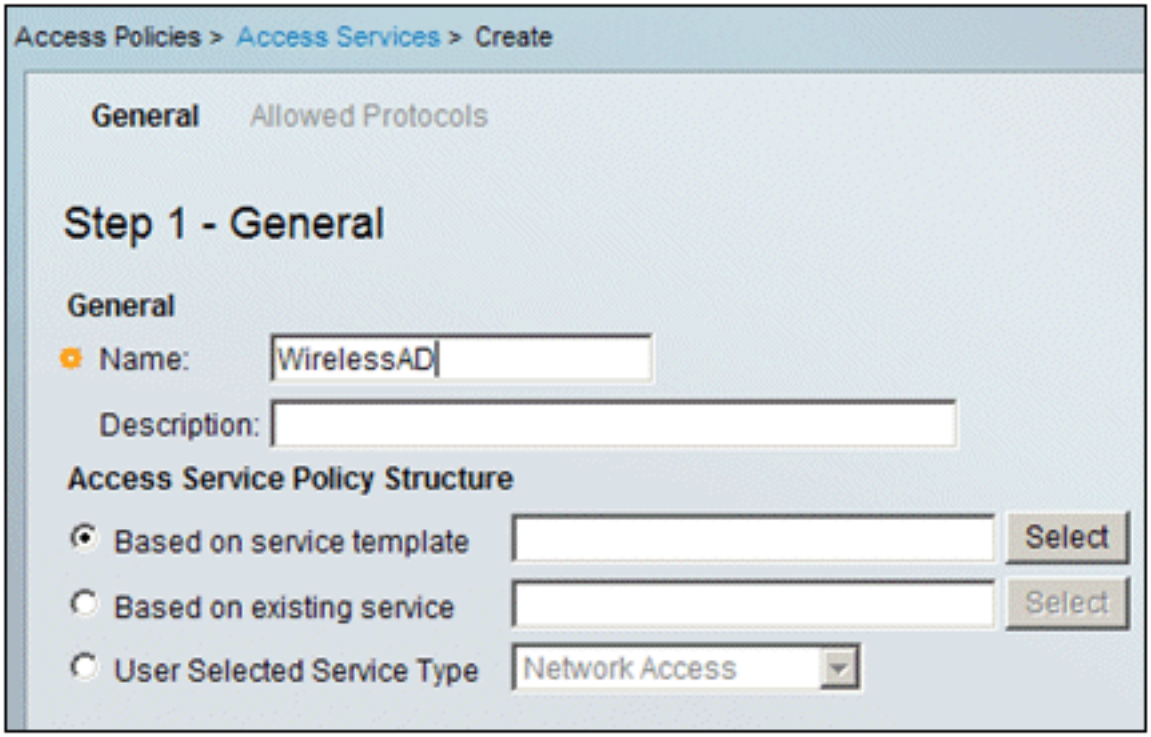
الوصول.

2. في نافذة "خدمات الوصول"، انقر فوق



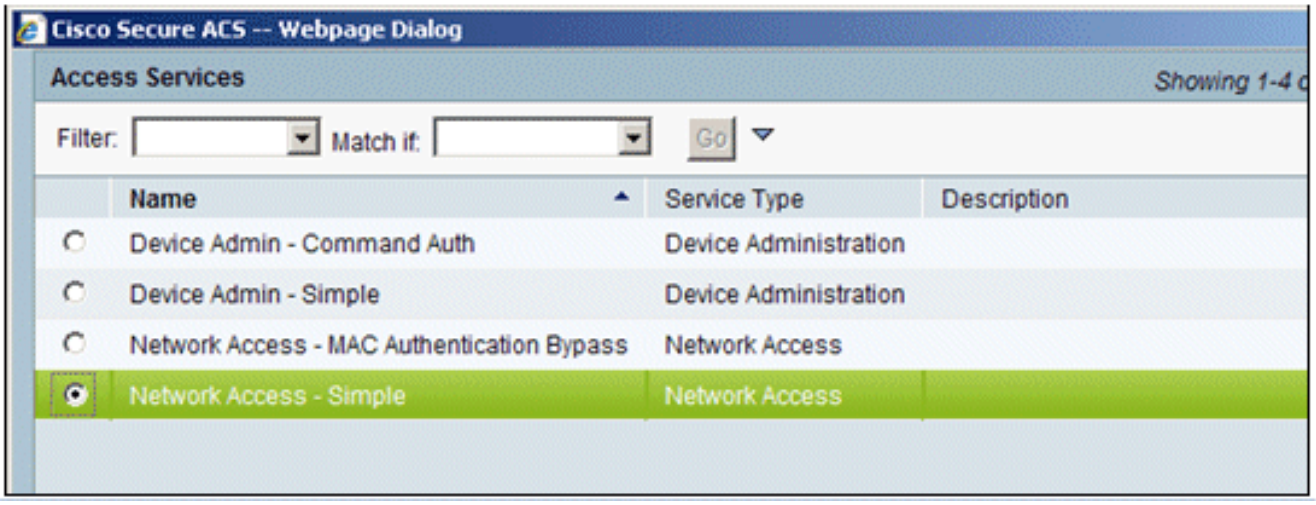
إنشاء.

3. قم بإنشاء خدمة وصول وأدخل اسما (مثل WirelessAD). أختر **استنادا إلى قالب الخدمة**، وانقر فوق

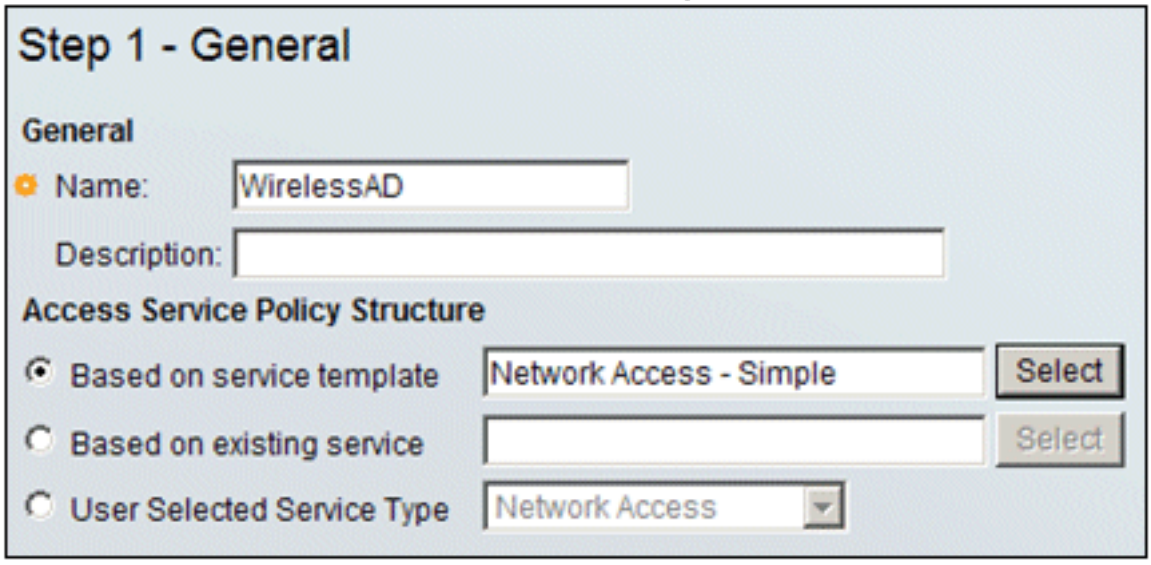


تحديد.

4. في مربع حوار صفحة الويب، أختر **الوصول إلى الشبكة - بسيط**. وانقر فوق **OK**.

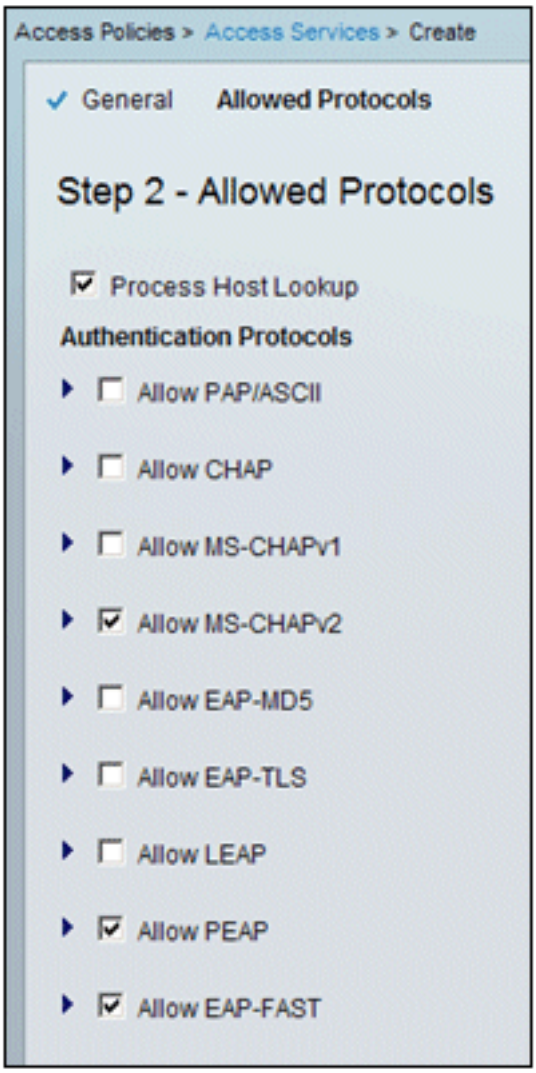


5. في مربع حوار صفحة الويب، أختر **الوصول إلى الشبكة - بسيط**. وانقر فوق **OK**. بمجرد تحديد القالب، انقر فوق



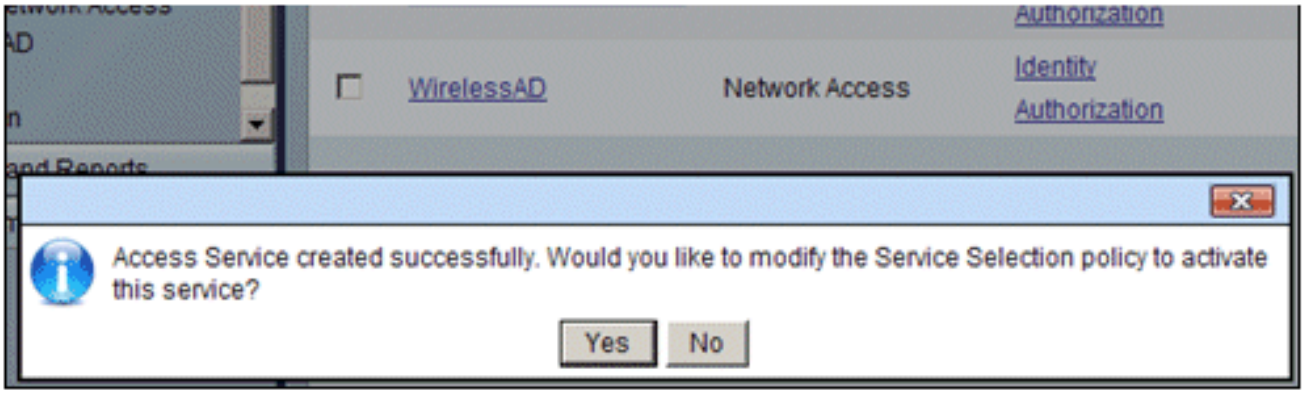
التالي.

6. تحت البروتوكولات المسموح بها، حدد خانات **السماح ب MS-CHAPv2** و **السماح PEAP**. انقر فوق

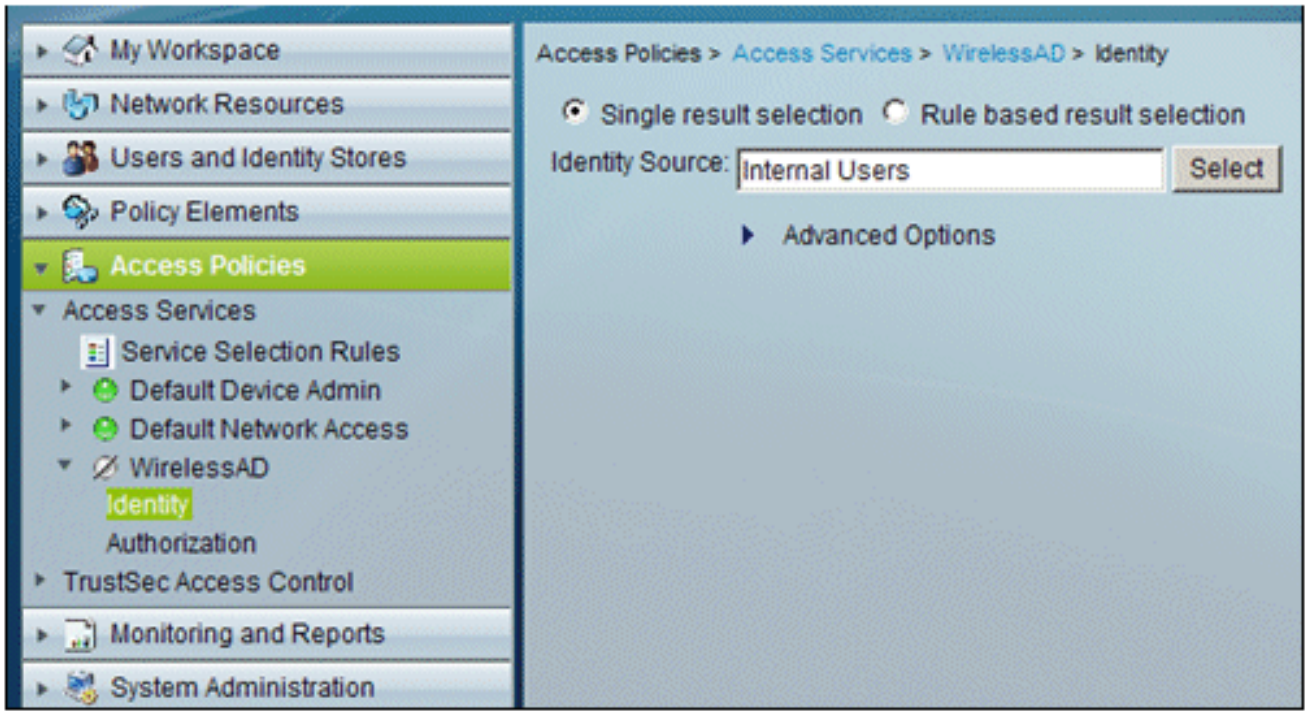


إنهاء.

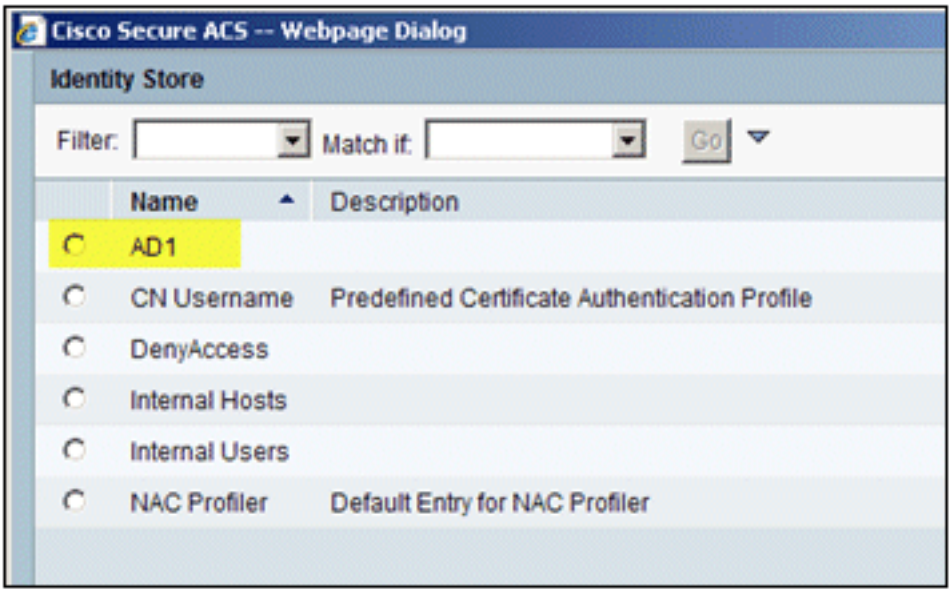
7. عندما يطالبك ACS بتنشيط الخدمة الجديدة، انقر فوق **نعم**.



8. في خدمة الوصول الجديدة التي تم إنشاؤها/تنشيطها للتو، قم بالتوسيع واختر **الهوية**. لمصدر الهوية، انقر على **تحديد**.



9. أخترت **AD1** ل Active Directory أن كان شكلت في ACS، طقطقة



ok.

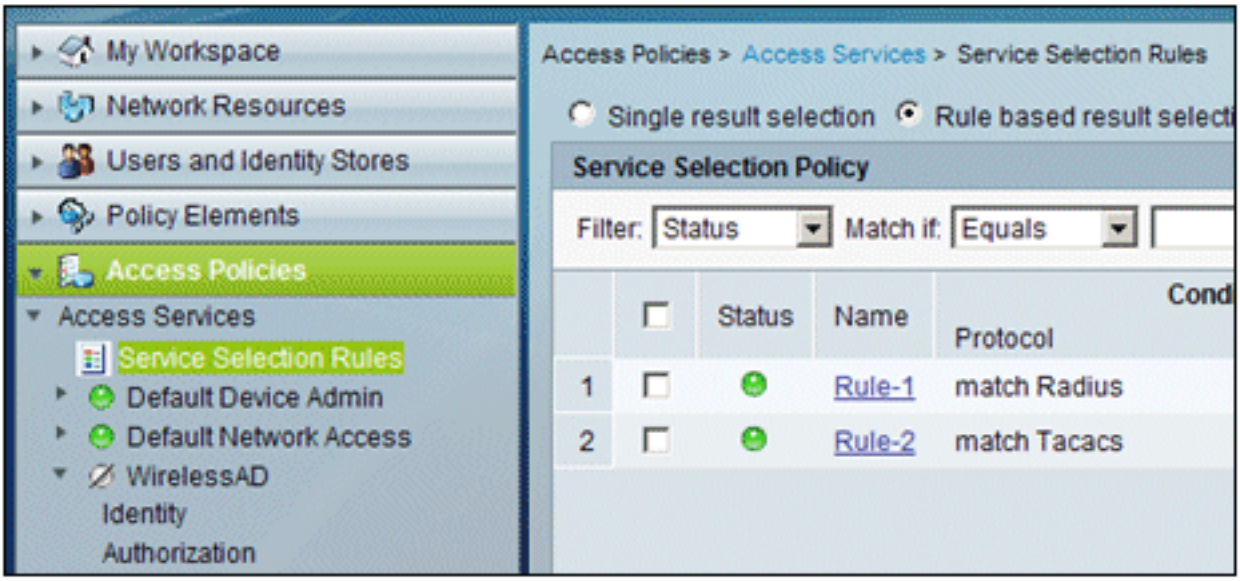
10. تأكد من أن مصدر الهوية هو AD1، وانقر **حفظ**

التغييرات.

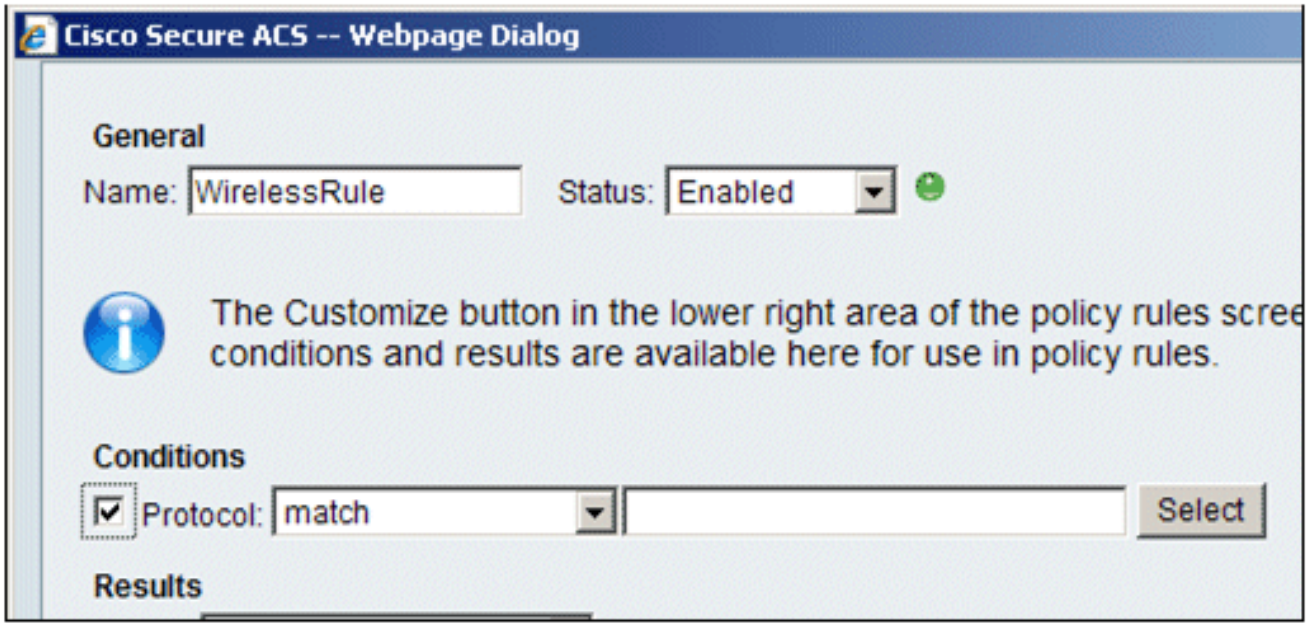
إنشاء سياسة الوصول إلى ACS وقاعدة الخدمة

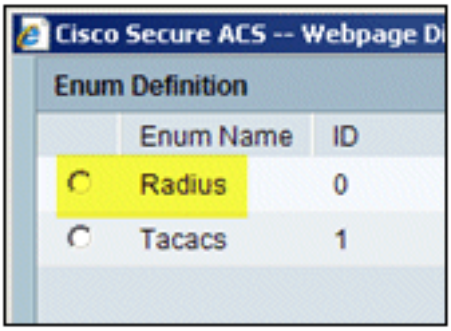
قم بإجراء هذه الخطوات:

1. انتقل إلى **سياسات الوصول > قواعد تحديد الخدمة**.

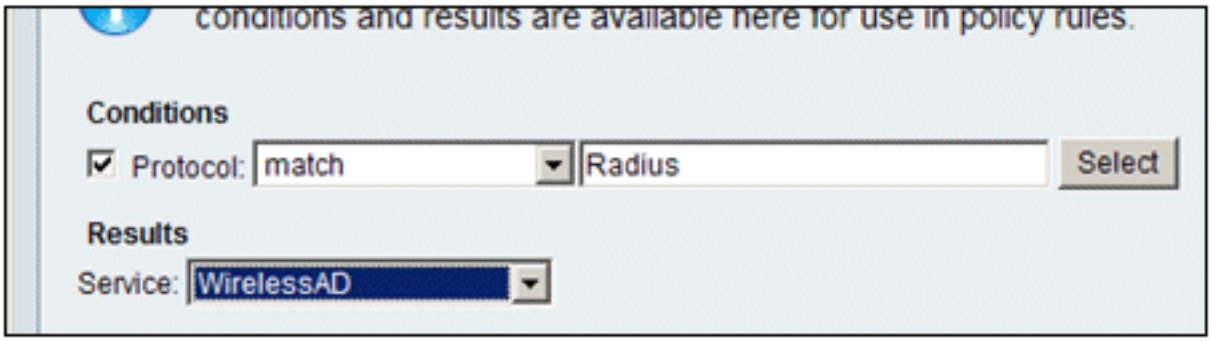


2. انقر فوق **إنشاء** في الإطار "نهج تحديد الخدمة". امنح القاعدة الجديدة اسما (على سبيل المثال، *WirelessRule*). حدد المربع الخاص **بالبروتوكول** لمطابقة **RADIUS**.

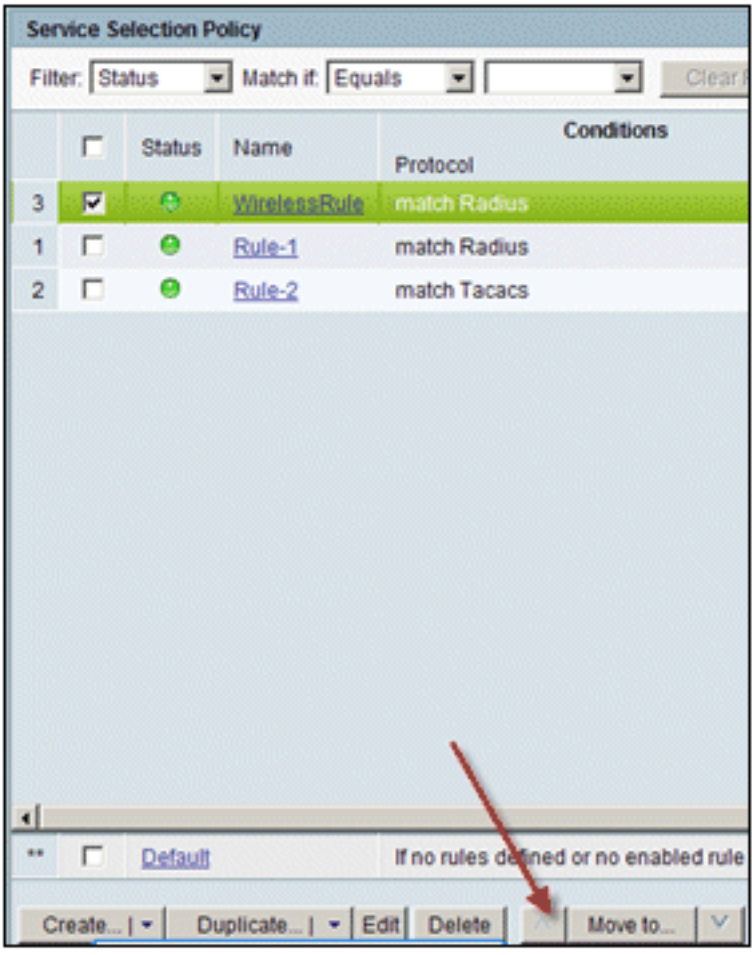




3. أخترت **Radius**، وطقطقة **ok**.
4. تحت النتائج، أختر **WirelessAD** للخدمة (تم إنشاؤه في الخطوة السابقة).



5. بمجرد إنشاء القاعدة اللاسلكية الجديدة، أختر هذه القاعدة وقم **بنقلها** إلى الأعلى، وستكون هذه القاعدة القاعدة الأولى في التعرف على مصادقة نصف القطر اللاسلكي باستخدام Active Directory.



تكوين العميل ل PEAP باستخدام Windows Zero Touch

في المثال الذي نقدمه، Client هو كمبيوتر يعمل بنظام التشغيل Windows XP Professional باستخدام SP يعمل كعميل لاسلكي ويحصل على إمكانية الوصول إلى موارد إنترانت من خلال نقطة الوصول اللاسلكية. أكمل الإجراءات الواردة في هذا القسم لتكوين العميل كعميل لاسلكي.

إجراء عملية تثبيت وتكوين أساسية

قم بإجراء هذه الخطوات:

1. توصيل Client بمقطع شبكة إنترانت باستخدام كبل إيثرنت متصل بالموجه.
2. على العميل، قم بتثبيت Windows XP Professional مع SP2 ككمبيوتر عضو يسمى Client الخاص بالمجال التجريبي.المحلي.
3. قم بتثبيت Windows XP Professional مع SP2. يجب تثبيت ذلك للحصول على دعم PEAP.**ملاحظة:** يتم

تشغيل جدار حماية Windows تلقائيا في Windows XP Professional مع SP2. عدم إيقاف تشغيل جدار الحماية.

تثبيت محول الشبكة اللاسلكية

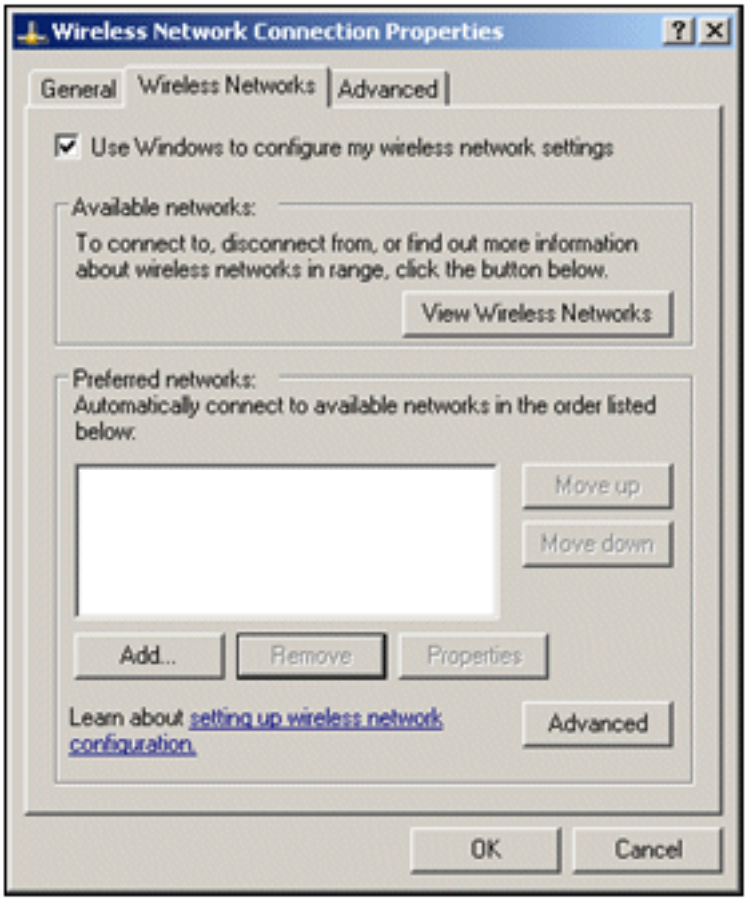
قم بإجراء هذه الخطوات:

1. قم بإيقاف تشغيل الكمبيوتر العميل.
2. قطع اتصال كمبيوتر العميل بمقطع شبكة إنترانت.
3. قم بإعادة تشغيل كمبيوتر العميل، ثم قم بتسجيل الدخول باستخدام حساب المسؤول المحلي.
4. قم بتثبيت محول الشبكة اللاسلكية.**ملاحظة** لا تقم بتثبيت برنامج تكوين الصانع للمحول اللاسلكي. قم بتثبيت برامج تشغيل محول الشبكة اللاسلكية باستخدام معالج إضافة أجهزة. وكذلك، عند المطالبة بذلك، قم بتزويد القرص المضغوط الذي قامت الشركة المصنعة بتوفيره أو قرص يحتوي على برامج تشغيل محدثة للاستخدام مع Windows XP Professional مع SP2.

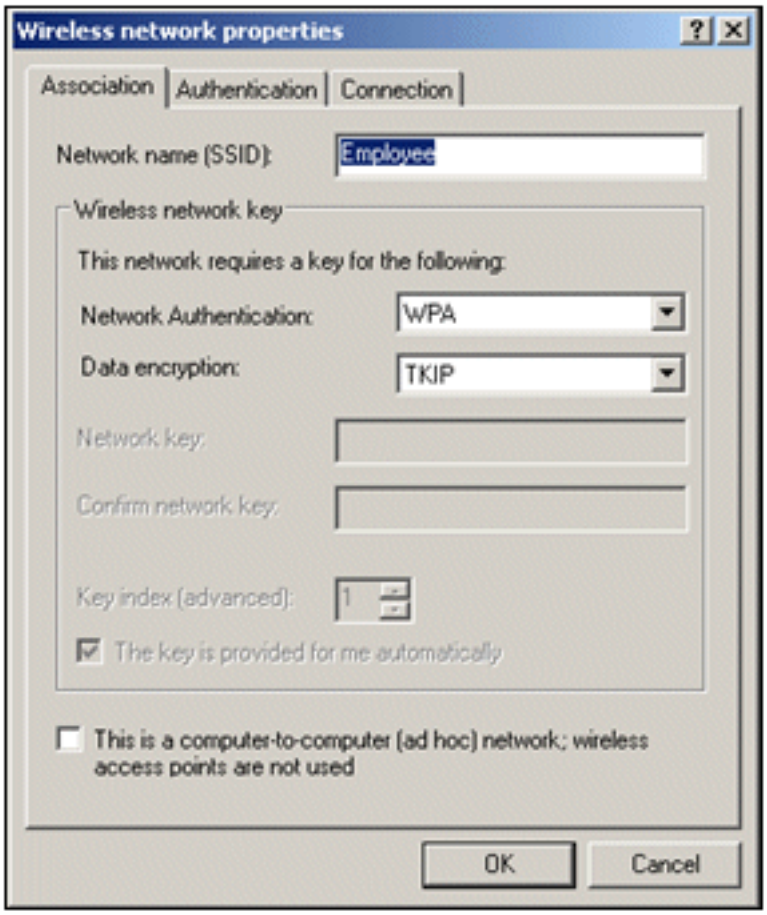
تكوين توصيل الشبكة اللاسلكية

قم بإجراء هذه الخطوات:

1. قم بتسجيل الخروج ثم قم بتسجيل الدخول باستخدام حساب **WirelessUser** في المجال **demo.local**.
2. أختر **ابدأ** > **لوحة التحكم**، وانقر نقرا مزدوجا فوق **إتصالات الشبكة**، ثم انقر بزر الماوس الأيمن فوق **اتصال الشبكة اللاسلكية**.
3. انقر على **خصائص**، انتقل إلى علامة التبويب **الشبكات اللاسلكية**، وتأكد من أن **إستخدام Windows لتكوين**

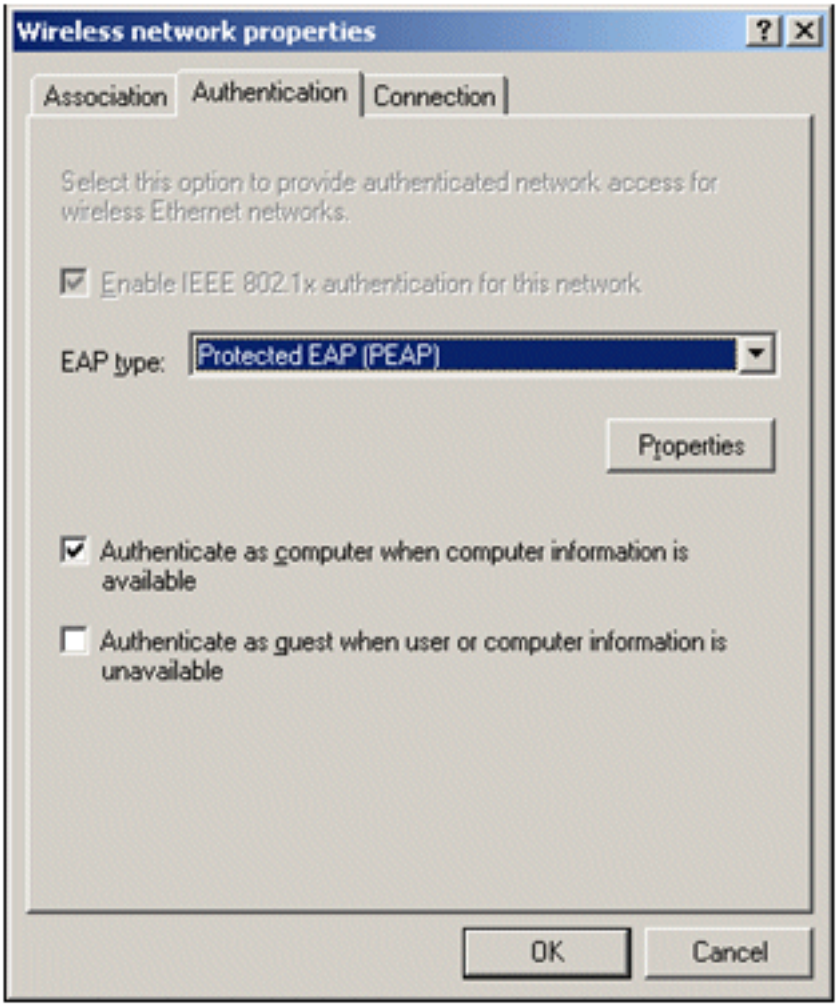


إعدادات الشبكة اللاسلكية محددة.
4. انقر فوق **إضافة (Add)**.
5. تحت علامة التبويب الاقتران، أدخل *الموظف* في حقل اسم الشبكة (SSID).
6. أختر **WPA** لمصادقة الشبكة، وتأكد من تعيين تشفير البيانات على



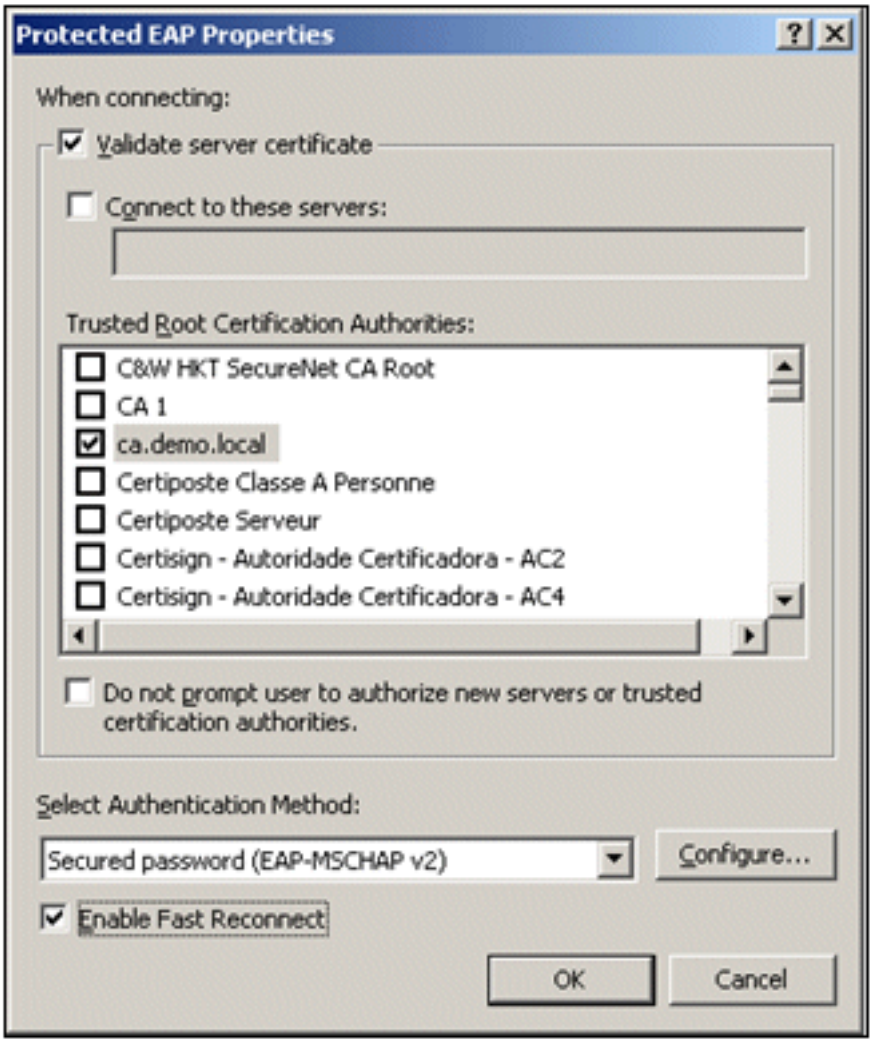
.**TKIP**

7. انقر فوق علامة التبويب **مصادقة**.
8. تحقق من تكوين نوع EAP لاستخدام **EAP المحمي (PEAP)**. إذا لم يكن كذلك، فإختاره من القائمة المنسدلة.
9. إذا كنت تريد مصادقة الجهاز قبل تسجيل الدخول (مما يسمح بتطبيق برامج تسجيل الدخول النصية أو نهج المجموعة)، فتحقق من **المصادقة كجهاز كمبيوتر عند توفر معلومات**



الكمبيوتر.

10. انقر فوق **خصائص**.
11. بما أن PEAP يتضمن مصادقة الخادم من قبل العميل، تأكد من أن **شهادة خادم التحقق** محددة. تأكد أيضا من فحص المرجع المصدق الذي أصدر شهادة ACS تحت قائمة مراجع التصديق الجذر الموثوق فيها.
12. أختر **كلمة مرور مؤمنة (EAP-MSCHAP v2)** تحت أسلوب المصادقة كما يتم إستخدامها للمصادقة



الداخلية.

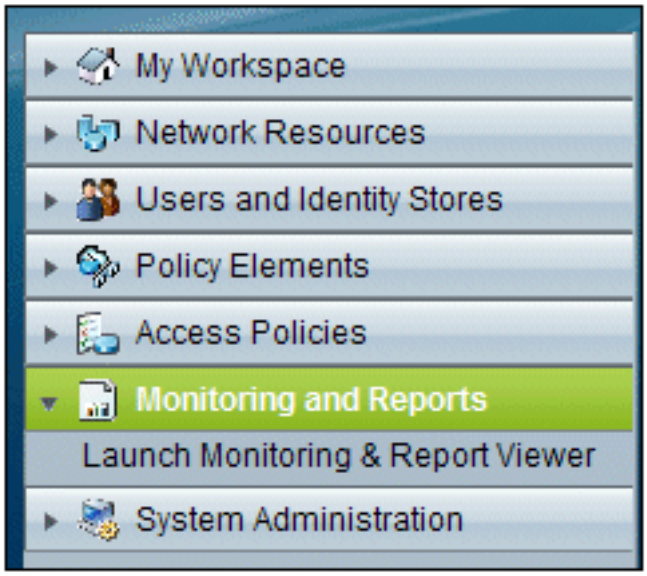
13. تأكد من تحديد خانة الاختيار **تمكين إعادة الاتصال السريع**. ثم انقر فوق **موافق** ثلاث مرات.
14. انقر بزر الماوس الأيمن على رمز توصيل الشبكة اللاسلكية في النظام ثم انقر على **عرض الشبكات اللاسلكية المتاحة**.
15. انقر على الشبكة اللاسلكية للموظف ثم انقر على **توصيل**. سيظهر العميل اللاسلكي **متصلا** إذا نجح الاتصال.

16. بعد نجاح المصادقة، تحقق من تكوين TCP/IP للمهايئ اللاسلكي باستخدام توصيلات الشبكة. يجب أن يكون له نطاق عنوان من 10.0.20.100-10.0.20.200 من نطاق DHCP أو النطاق الذي تم إنشاؤه لعملاء CorpNet اللاسلكي.
17. لاختبار الوظائف، افتح متصفح وتصفح إلى **http://10.0.10.10** (أو عنوان IP الخاص بخادم CA).

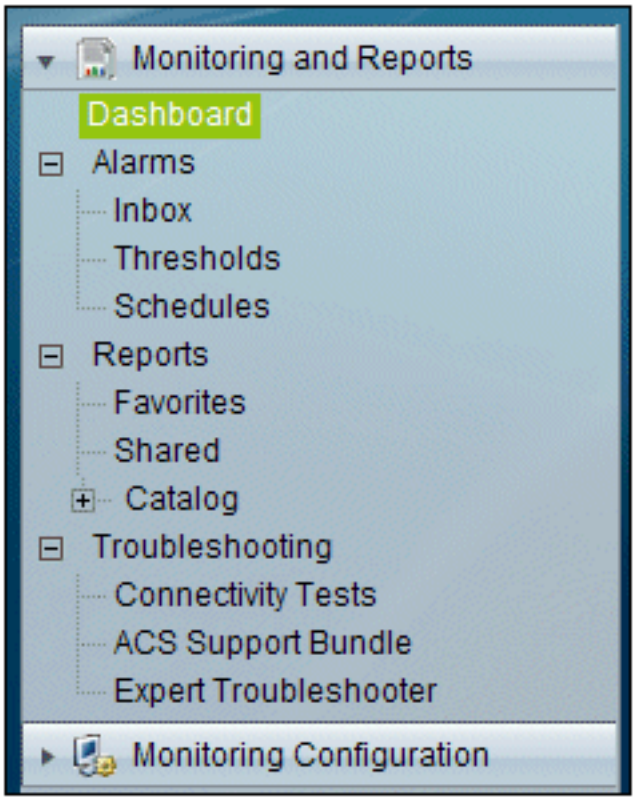
أستكشاف أخطاء المصادقة اللاسلكية وإصلاحها باستخدام ACS

قم بإجراء هذه الخطوات:

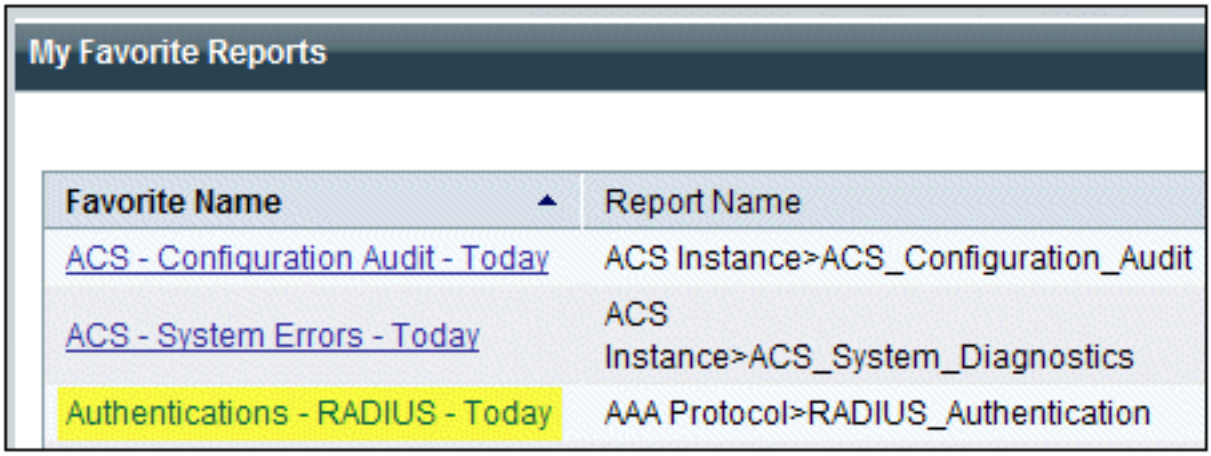
1. انتقل إلى **ACS > المراقبة والتقارير**، وانقر فوق **تشغيل المراقبة وعارض التقارير**.



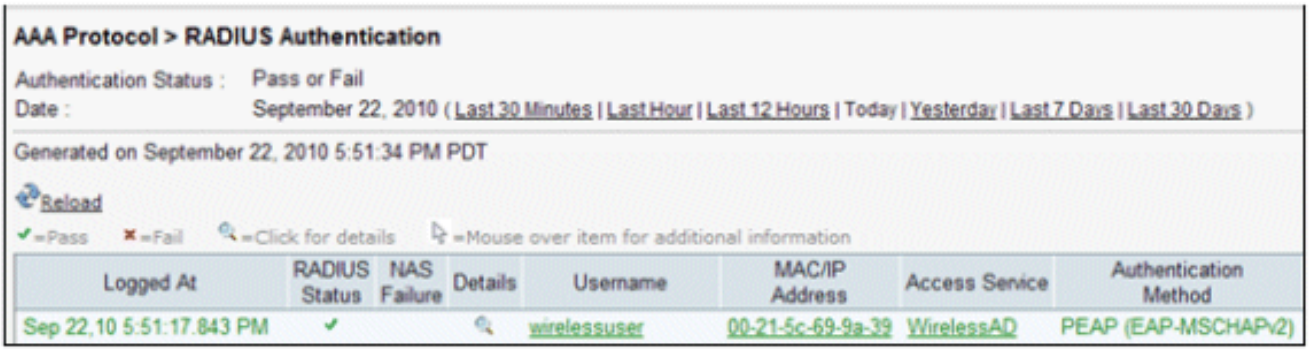
2. سيتم فتح نافذة ACS منفصلة. انقر فوق **لوحة المعلومات**.



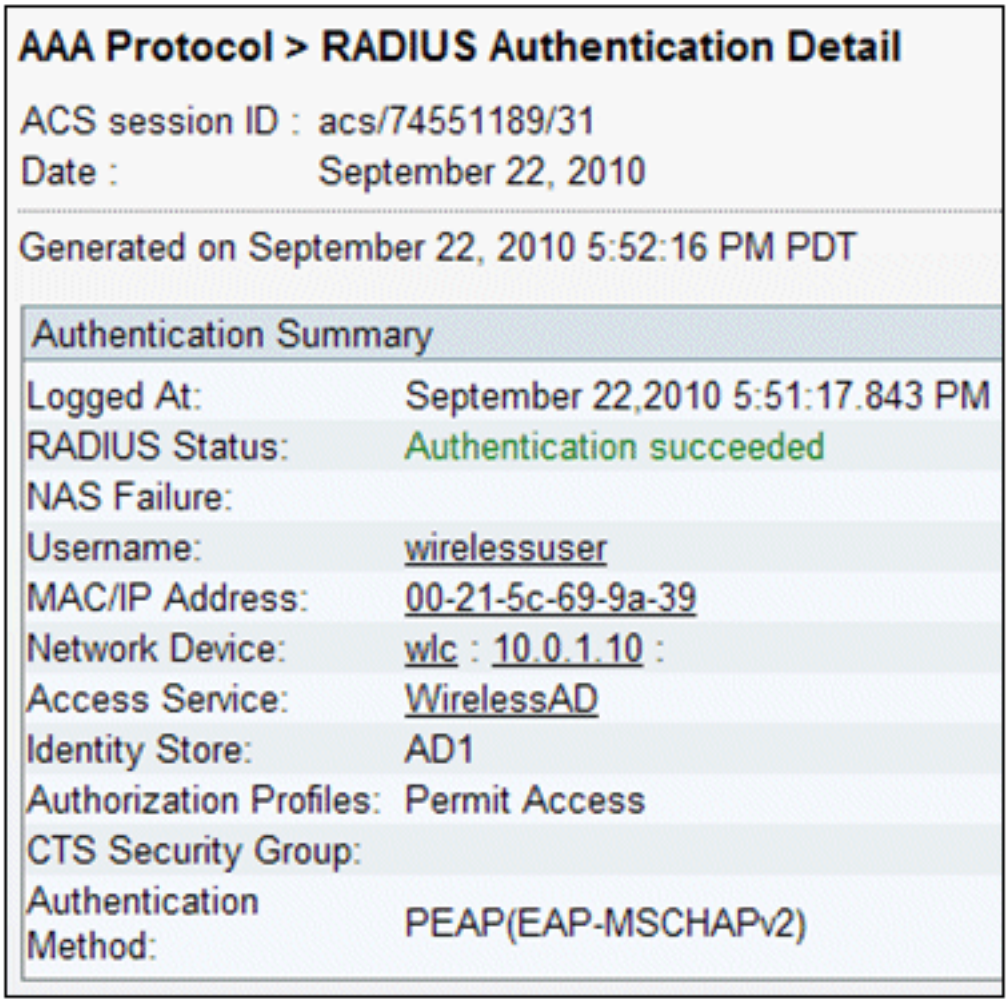
3. في قسم "التقارير المفضلة لدي"، انقر فوق **مصادقة - RADIUS - اليوم**.



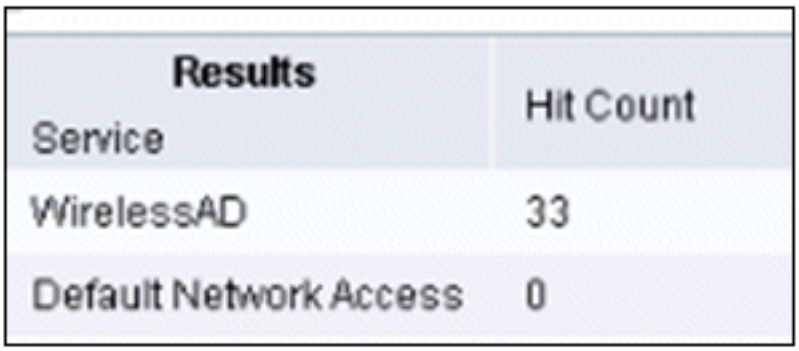
4. سيظهر السجل جميع مصادقة RADIUS إما على أنها عملية مرور أو فشل. ضمن مدخل مسجل، انقر على **أيقونة العدسة المكبرة** في عامود التفاصيل.



5. ستوفر تفاصيل مصادقة RADIUS الكثير من المعلومات حول المحاولات المسجلة.



6. يمكن أن يوفر "عدد مرات الوصول إلى خدمة ACS" نظرة عامة على المحاولات التي تطابق القاعدة (القواعد) التي تم إنشاؤها في ACS. انتقل إلى **ACS>سياسات الوصول>خدمات الوصول**، وانقر فوق **قواعد تحديد الخدمة**.



يفشل مصادقة PEAP مع خادم ACS

عندما يفشل العميل في مصادقة PEAP مع خادم ACS، تحقق مما إذا كنت تجد رسالة خطأ NAS في خيار **المحاولات الفاشلة** ضمن قائمة **التقرير والنشاط** الخاصة ب ACS.

قد تتلقى رسالة الخطأ هذه عندما يكون Microsoft Windows XP SP2 مثبتا على جهاز العميل ويصادق Windows XP SP2 على خادم جهة خارجية بخلاف خادم Microsoft IAS. وعلى وجه الخصوص، يستخدم خادم Cisco ACS (RADIUS) طريقة مختلفة لحساب معرف بروتوكول المصادقة المتوسع النوع:الطول:تنسيق القيمة (EAP-TLV) عن الطريقة التي يستخدمها Windows XP. وقد حددت Microsoft هذا كعيب في ملتمس XP SP2.

للحصول على إصلاح عاجل، اتصل ب Microsoft وأرجع إلى المقالة مصادقة PEAP غير ناجحة عند إتصالك بخادم RADIUS للجهة الخارجية . المشكلة الأساسية هي أنه على جانب العميل، مع الأداة المساعدة ل Windows، يتم تعطيل خيار إعادة الاتصال السريع ل PEAP بشكل افتراضي. ومع ذلك، يتم تمكين هذا الخيار بشكل افتراضي على جانب الخادم (ACS). لحل هذه المشكلة، قم بإلغاء تحديد خيار إعادة الاتصال السريع على خادم ACS (تحت خيارات النظام العام). بدلا من ذلك، يمكنك تمكين خيار إعادة الاتصال السريع على جانب العميل لحل المشكلة.

نفذ هذه الخطوات لتمكين إعادة الاتصال السريع بالعميل الذي يعمل بنظام التشغيل Windows XP باستخدام الأداة المساعدة ل Windows:

1. انتقل إلى **ابدأ > إعدادات > لوحة التحكم**.
2. انقر نقرا مزدوجا على أيقونة **إتصالات الشبكة**.
3. انقر بزر الماوس الأيمن على رمز **اتصال الشبكة اللاسلكية**، ثم انقر على **خصائص**.
4. انقر على علامة تبويب **الشبكات اللاسلكية**.
5. أختر **إستخدام Windows لتكوين إعدادات الشبكة اللاسلكية** لتمكين Windows من تكوين محول العميل.
6. إذا كنت قد انتهيت من تكوين SSID بالفعل، فاختر SSID وانقر فوق **خصائص**. إذا لم تكن هناك مساحة، انقر فوق **جديد** لإضافة شبكة WLAN جديدة.
7. أدخل SSID ضمن علامة التبويب الاقتران. تأكد من أن مصادقة الشبكة **مفتوحة** ومن تعيين تشفير البيانات على **WEP**.
8. انقر على **المصادقة**.
9. أخترت **ال enable IEEE 802.1x صحة هوية ل هذا شبكة** خيار.
10. أختر **PEAP** ليكون هو نوع EAP ثم انقر على **خصائص**.
11. أختر خيار **تمكين إعادة الاتصال السريع** في أسفل الصفحة.

معلومات ذات صلة

- PEAP تحت شبكات لاسلكية موحدة مع ACS 4.0 و Windows 2003
- مثال تكوين (WLC) Cisco Wireless LAN Controller و (TACACS+) Cisco ACS 5.x لمصادقة الويب
- دليل التثبيت والترقية لنظام التحكم بالوصول الآمن من Cisco 5.1
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).