مصادقة EAP المحلية على وحدة تحكم الشبكة المحلية اللاسلكية باستخدام LDAP وتكوين خادم EAP-FAST كمثال

المحتويات

المقدمة

يشرح هذا المستند كيفية تكوين بروتوكول المصادقة المتوسع (EAP) - المصادقة المرنة عبر مصادقة EAP المحلية الآمنة (FAST) على وحدة تحكم في الشبكة المحلية اللاسلكية (WLC). يشرح هذا المستند أيضا كيفية تكوين خادم البروتوكول الخفيف للوصول إلى الدليل (LDAP) كقاعدة بيانات خلفية لـ EAP المحلي لاسترداد بيانات اعتماد المستخدم ومصادقة المستخدم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- Cisco 4400 Series WLC الذي يشغل البرنامج الثابت 4.2
- نقطة الوصول في الوضع (Lightweight (LAP من سلسلة Cisco Aironet 1232AG
- تم تكوين خادم Microsoft Windows 2003 على أنه وحدة تحكم بالمجال وخادم LDAP بالإضافة إلى خادم مرجع الشهادات.
- مهايئ عميل Cisco Aironet 802.11 a/b/g الذي يشغل البرنامج الثابت الإصدار 4.2
- أداة (Cisco Aironet Desktop Utility (ADU التي تشغل الإصدار 4.2 من البرنامج الثابت

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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.

معلومات أساسية

تم تقديم مصادقة EAP المحلية على وحدات التحكم في الشبكة المحلية اللاسلكية باستخدام الإصدار 4.1.171.0 من وحدة التحكم في الشبكة المحلية اللاسلكية.

EAP المحلي هو أسلوب مصادقة يسمح للمستخدمين والعملاء اللاسلكيين بالمصادقة محليا على وحدة التحكم. وقد تم تصميمه للاستخدام في المكاتب البعيدة التي ترغب في الحفاظ على الاتصال بالعملاء اللاسلكيين عند تعطل النظام الخلفي أو تعطل خادم المصادقة الخارجي. عندما تقوم بتمكين EAP المحلي، فإن وحدة التحكم تعمل كخادم المصادقة وقاعدة بيانات المستخدم المحلية، بحيث تزيل الاعتماد على خادم مصادقة خارجي. يسترجع EAP المحلي مسوغات المستخدم من قاعدة بيانات المستخدم المحلية أو قاعدة بيانات خلفية LDAP لمصادقة المستخدمين. يدعم EAP المحلي مصادقة LEAP و EAP-FAST و EAP-TLS و P EAPv0/MSCHAPv2 و PEAPv1/GTC بين وحدة التحكم والعملاء اللاسلكيين.

يمكن ل EAP المحلي إستخدام خادم LDAP كقاعدة بيانات خلفية لاسترداد بيانات اعتماد المستخدم.

تسمح قاعدة بيانات LDAP الخلفية لوحدة التحكم بالاستعلام عن خادم LDAP لبيانات الاعتماد (اسم المستخدم وكلمة المرور) الخاصة بمستخدم معين. ثم يتم إستخدام بيانات الاعتماد هذه لمصادقة المستخدم.

تدعم قاعدة بيانات الطرف الخلفي ل LDAP طرق EAP المحلية التالية:

- EAP-FAST/GTC
- EAP-TLS
- PEAPv1/GTC.

كما يتم دعم LEAP و EAP-FAST/MSCHAPv2 و PEAPv0/MSCHAPv2، **ولكن فقط في حالة إعداد خادم LDAP لإرجاع كلمة مرور نص واضح**. على سبيل المثال، Microsoft Active Directory غير معتمد لأنه لا يرجع كلمة مرور نص واضح. إذا تعذر تكوين خادم LDAP لإرجاع كلمة مرور نص واضح، فإن LEAP و EAP-FAST/MSCHAPv2 و PEAPv0/MSCHAPv2 غير مدعومة.

ملاحظة: في حالة تكوين أي من خوادم RADIUS على وحدة التحكم، تحاول وحدة التحكم مصادقة العملاء اللاسلكيين باستخدام خوادم RADIUS أولا. لا يتم محاولة EAP المحلي إلا في حالة عدم العثور على خوادم RADIUS، إما بسبب انتهاء مهلة خوادم RADIUS أو بسبب عدم تكوين خوادم RADIUS. إذا تم تكوين أربعة خوادم RADIUS، تحاول وحدة التحكم مصادقة العميل باستخدام خادم RADIUS الأول، ثم خادم RADIUS الثاني، ثم EAP المحلي. وإذا حاول العميل إعادة المصادقة يدويا، فإن وحدة التحكم تحاول إستخدام خادم RADIUS الثالث، ثم خادم RADIUS الرابع، ثم EAP المحلي.

يستخدم هذا المثال EAP-FAST كأسلوب EAP المحلي على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، والذي يتم تكوينه بدوره للاستعلام عن قاعدة بيانات خلفية LDAP لبيانات اعتماد المستخدم الخاصة بعميل لاسلكي.

التكوين

يستخدم هذا المستند EAP-FAST بشهادات على كل من العميل والخادم. لهذا الغرض، يستخدم الإعداد خادم **مرجع شهادات Microsoft (CA)** لإنشاء شهادات العميل والخادم.

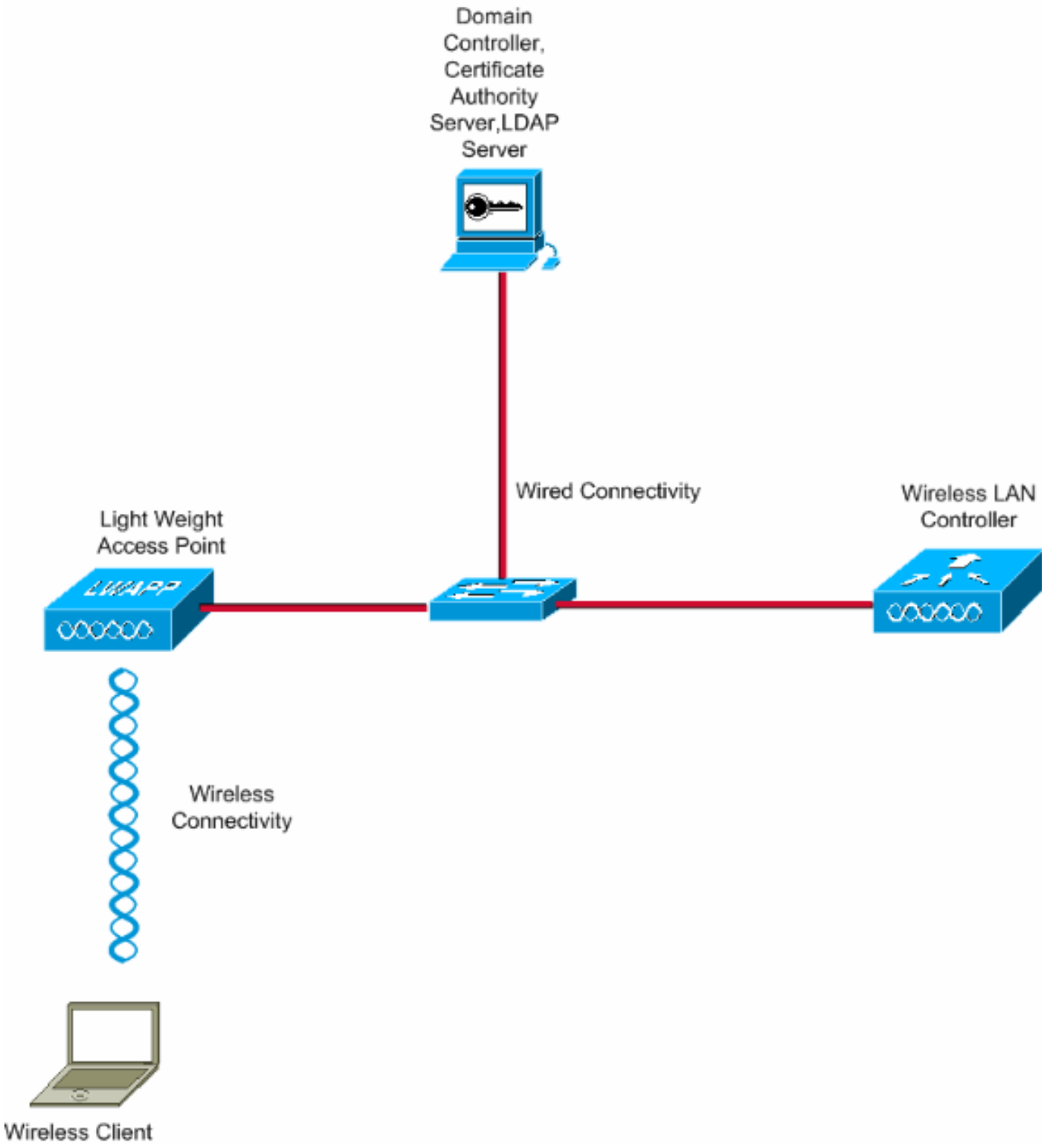
يتم تخزين بيانات اعتماد المستخدم في خادم LDAP حتى يستعلم جهاز التحكم عن خادم LDAP في التحقق من صحة الشهادة الناجحة لاسترداد بيانات اعتماد المستخدم ومصادقة العميل اللاسلكي.

يفترض هذا المستند أن هذه التكوينات موجودة بالفعل:

- تم تسجيل نقطة وصول (LAP) في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). راجع تسجيل نقطة الوصول في الوضع (Lightweight (LAP إلى وحدة تحكم شبكة محلية لاسلكية (WLC) للحصول على مزيد من المعلومات حول عملية التسجيل.
- تم تكوين خادم DHCP لتعيين عنوان IP إلى العملاء اللاسلكيين.
- تم تكوين خادم Microsoft Windows 2003 كوحدة تحكم بالمجال وكذلك كخادم CA. يستخدم هذا المثال **wireless.com** كمجال.ارجع إلى تكوين Windows 2003 كوحدة تحكم بالمجال للحصول على مزيد من المعلومات حول تكوين خادم Windows 2003 كوحدة تحكم بالمجال.ارجع إلى تثبيت خادم Microsoft Windows 2003 وتكوينه كخادم مرجع مصدق (CA) لتكوين خادم Windows 2003 كخادم مرجع مصدق للمؤسسة.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

أتمت هذا steps in order to نفذت هذا تشكيل:

- تكوين EAP-FAST كأسلوب مصادقة EAP محلي على WLC
- تكوين خادم LDAP
- تكوين عميل لاسلكي

تكوين EAP-FAST كأسلوب مصادقة EAP محلي على WLC

كما ذكر سابقا، يستخدم هذا المستند EAP-FAST بشهادات على كل من العميل والخادم كأسلوب مصادقة EAP المحلي. تتمثل الخطوة الأولى في تنزيل الشهادات التالية وتثبيتها على الخادم (WLC، في هذه الحالة) والعميل.

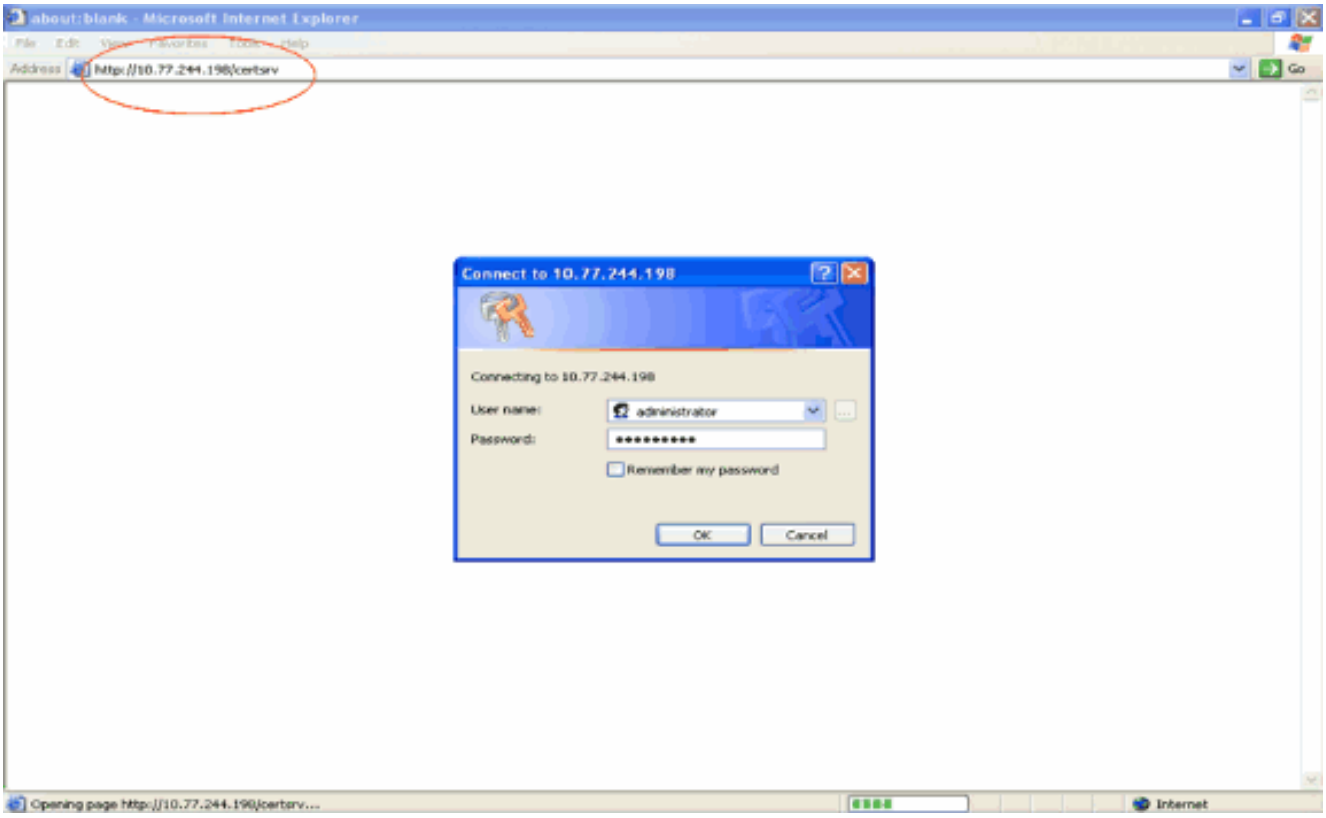
يحتاج كل من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) والعميل إلى تنزيل هذه الشهادات من خادم CA:

- "شهادة الجهاز" (شهادة ل WLC وأخرى للعميل)
- الشهادة الجذر للبنية الأساسية للمفتاح العام (PKI) لمركز التحكم في الشبكة المحلية اللاسلكية (WLC) وشهادة CA للعميل

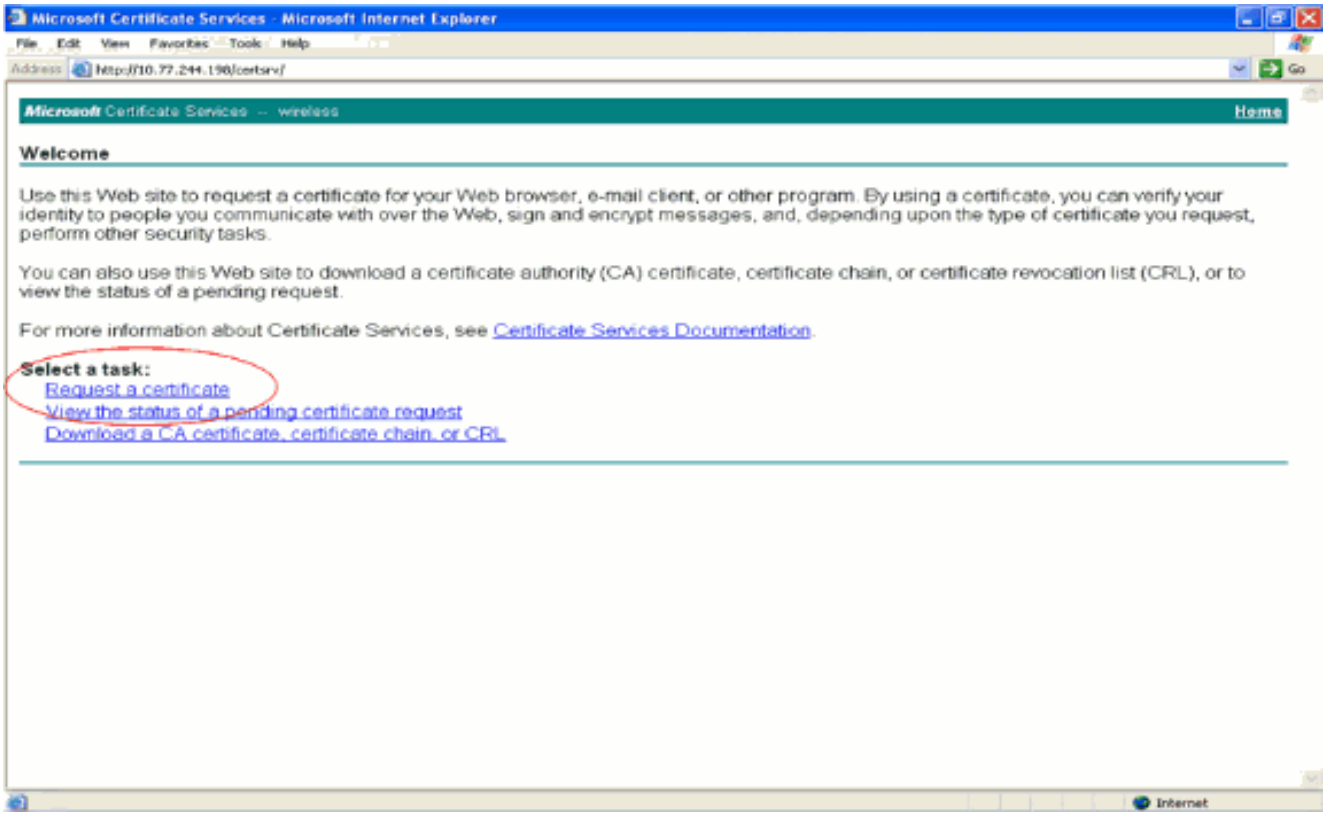
إنشاء شهادة جهاز ل WLC

قم بإجراء هذه الخطوات لإنشاء شهادة جهاز ل WLC من خادم CA. يتم إستخدام شهادة الجهاز هذه من قبل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للمصادقة على العميل.

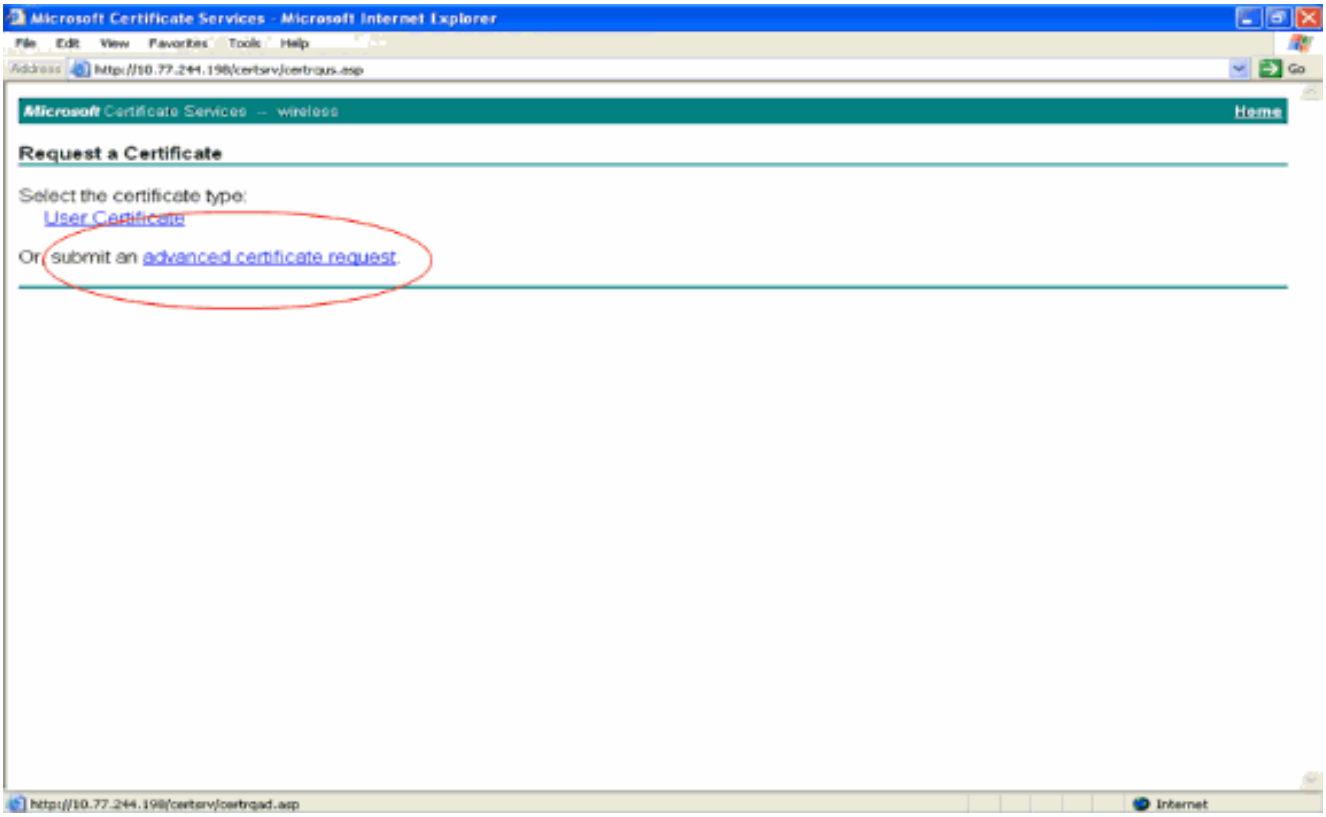
1. انتقل إلى **http://<IP عنوان CA Server>/certsrv** من pc الخاص بك الذي له اتصال شبكة بخادم CA. سجل الدخول كمسؤول عن خادم CA.



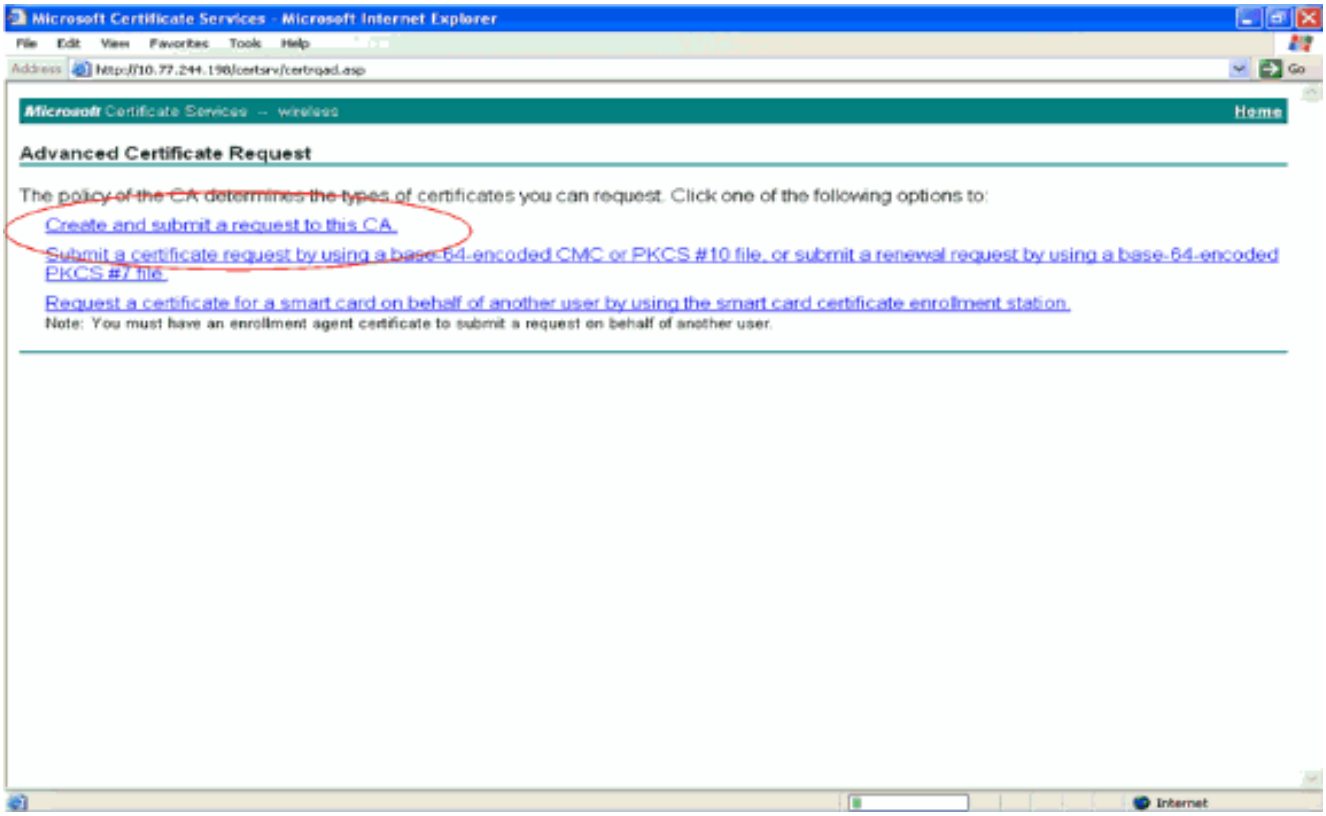
2. حدد **طلب شهادة**.



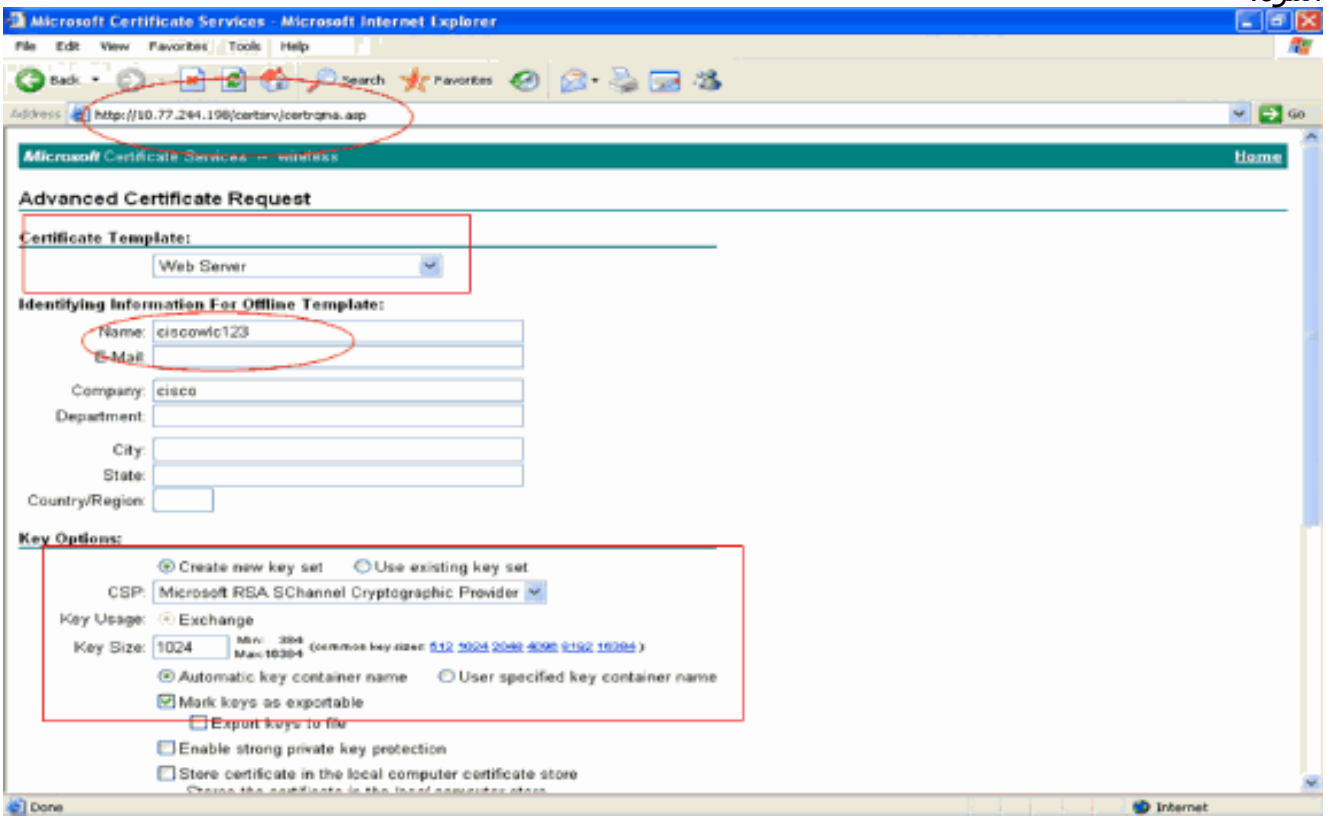
3. في صفحة طلب شهادة، انقر على **طلب شهادة متقدمة**.



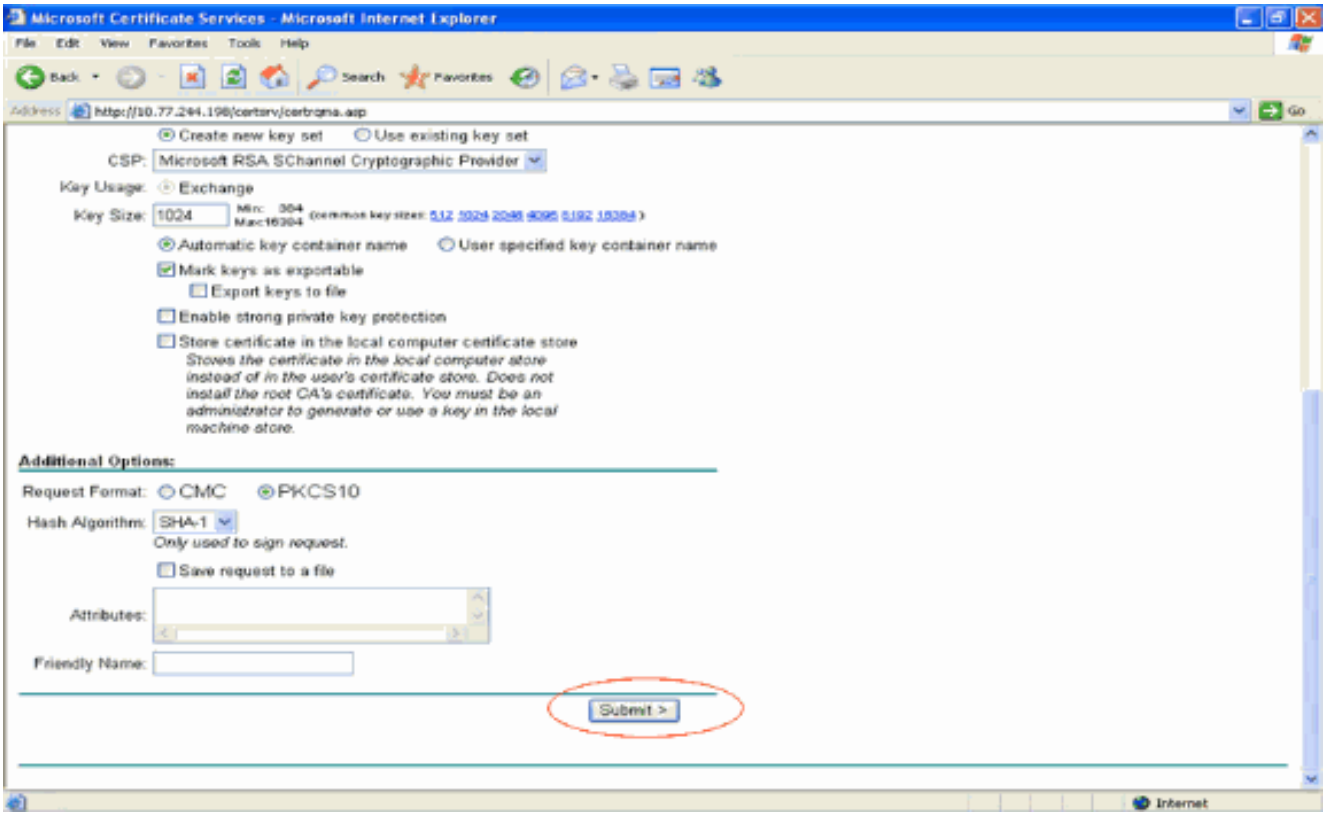
4. في صفحة طلب الشهادة المتقدمة، انقر على **إنشاء طلب وإرساله إلى المرجع المصدق هذا**. ينقلك هذا إلى نموذج طلب الشهادة
المتقدمة.



5. في نموذج طلب الشهادة المتقدمة، أختر **خادم ويب** كقالب شهادة. ثم حدد اسما لشهادة الجهاز هذه.يستخدم هذا المثال اسم الشهادة على هيئة CiscoWLC123. املأ معلومات التعريف الأخرى حسب متطلباتك.
6. تحت قسم **خيارات المفاتيح**، حدد **خيار تمييز المفاتيح كقابلة للتصدير**. في بعض الأحيان، سيتم تصنيف هذا الخيار المحدد بشكل إجمالي ويتعذر تمكينه أو تعطيله إذا قمت باختيار قالب خادم ويب. في مثل هذه الحالات، انقر فوق **الخلف** من قائمة المستعرض للعودة صفحة واحدة والعودة مرة أخرى إلى هذه الصفحة. يجب توفر خيار وضع علامة "مفاتيح" كقابلة للتصدير هذه المرة.

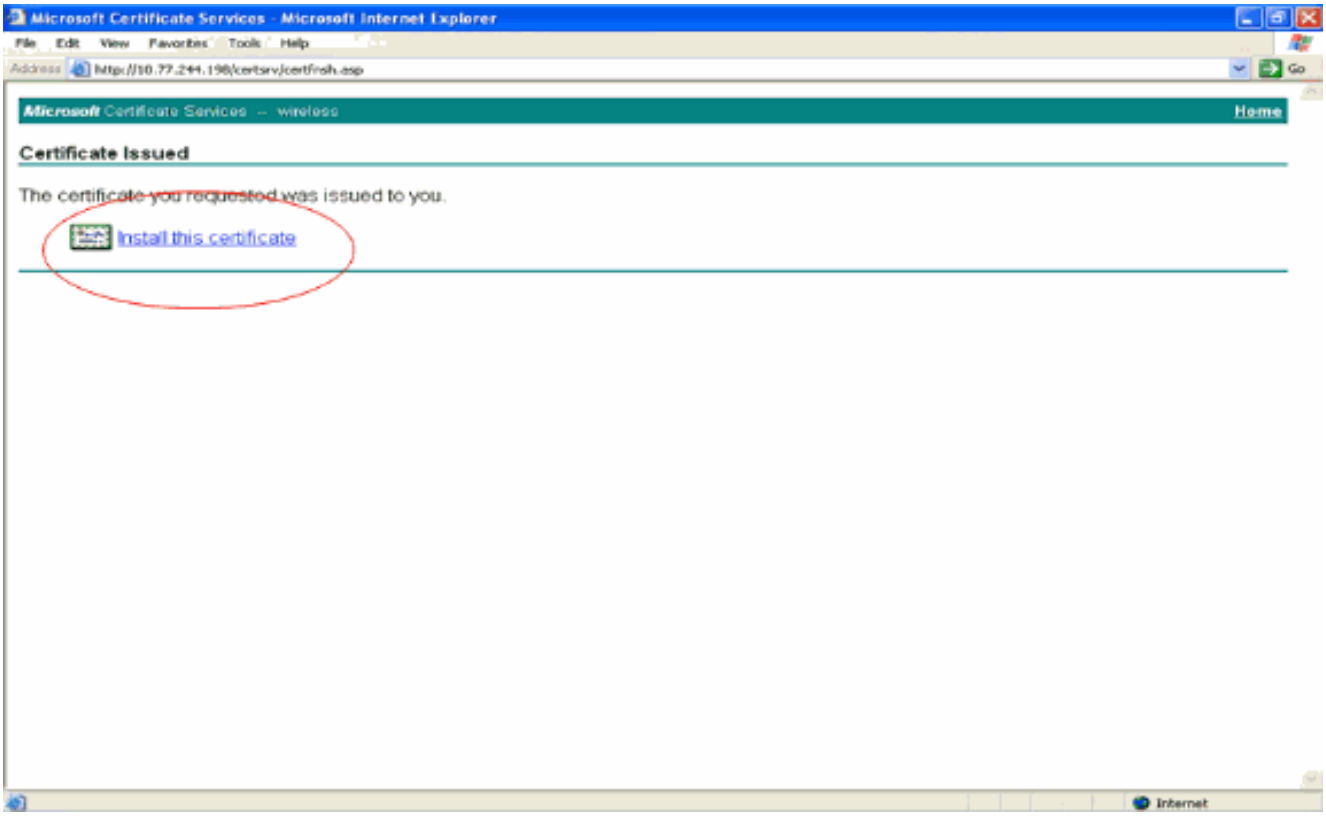


7. قم بتكوين كافة الحقول الضرورية الأخرى وانقر فوق **إرسال**.

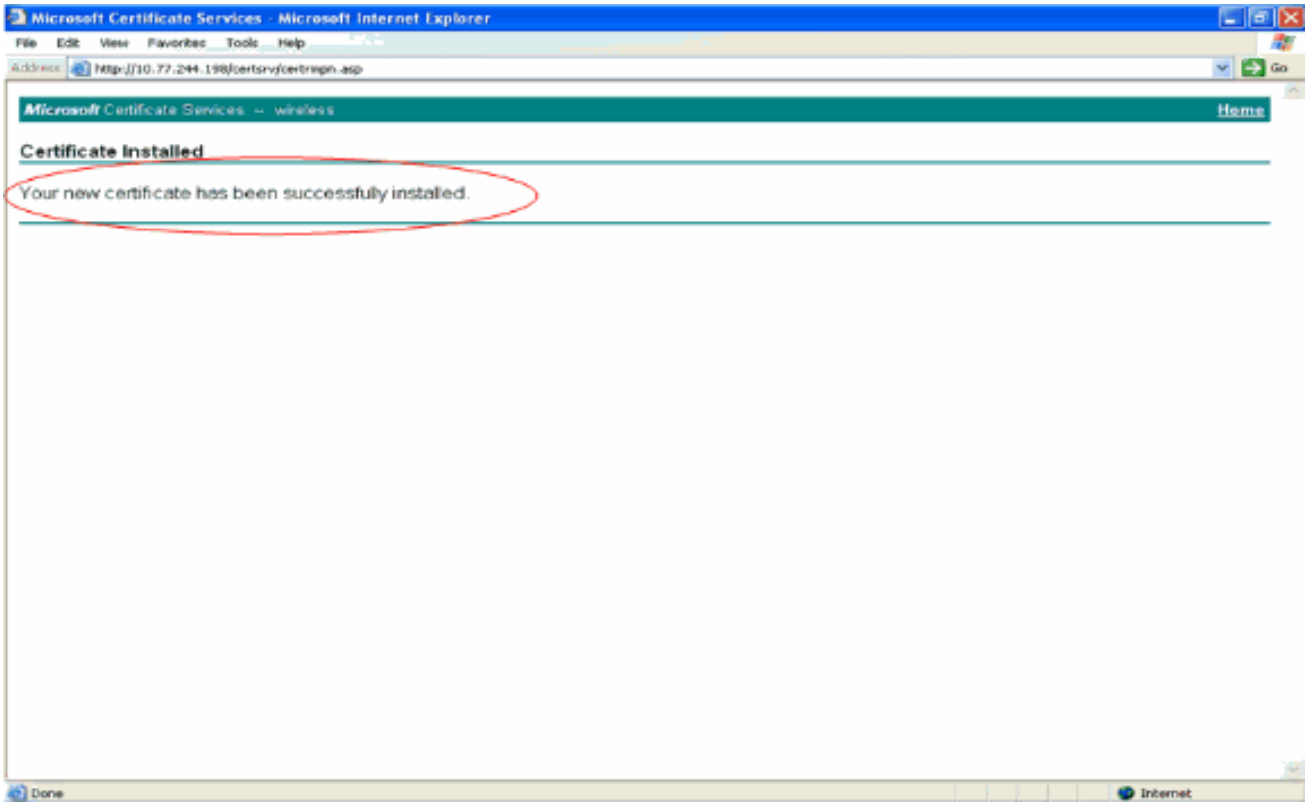


8. انقر على **نعم** في الإطار التالي للسماح بعملية طلب الشهادة.

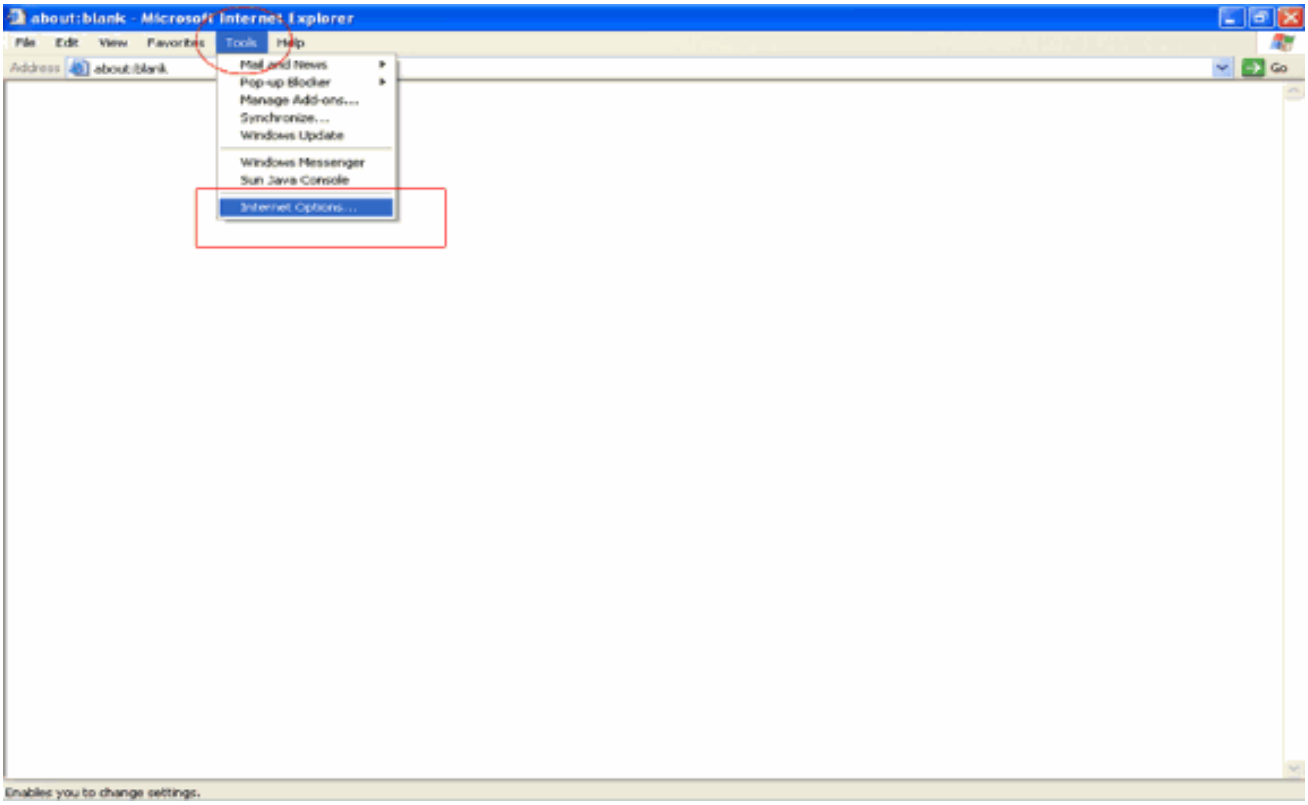
9. يظهر الإطار "إصدار الشهادة" الذي يشير إلى نجاح عملية طلب الشهادة. تتمثل الخطوة التالية في تثبيت الشهادة الصادرة في مخزن الشهادات الخاص بهذا الكمبيوتر. انقر على **تثبيت هذه الشهادة**.



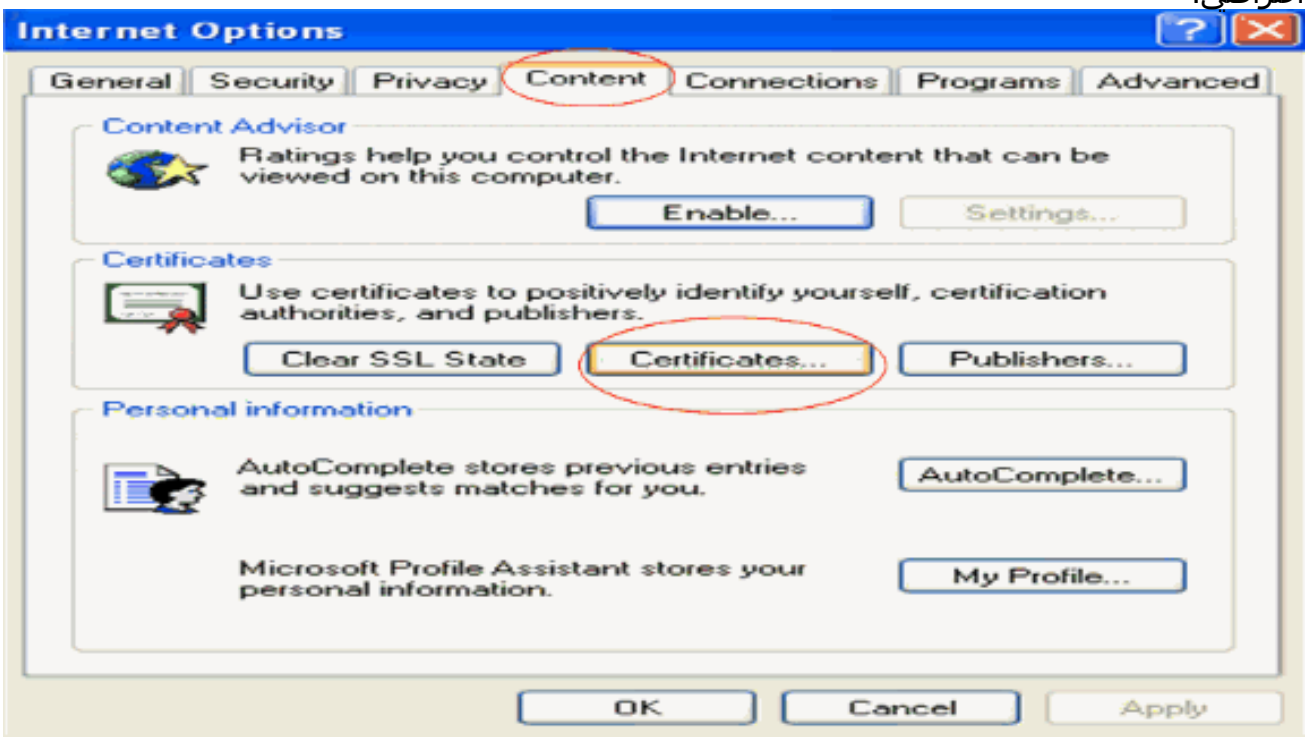
10. تم تثبيت الشهادة الجديدة بنجاح على الكمبيوتر من حيث تم إنشاء الطلب إلى خادم CA.



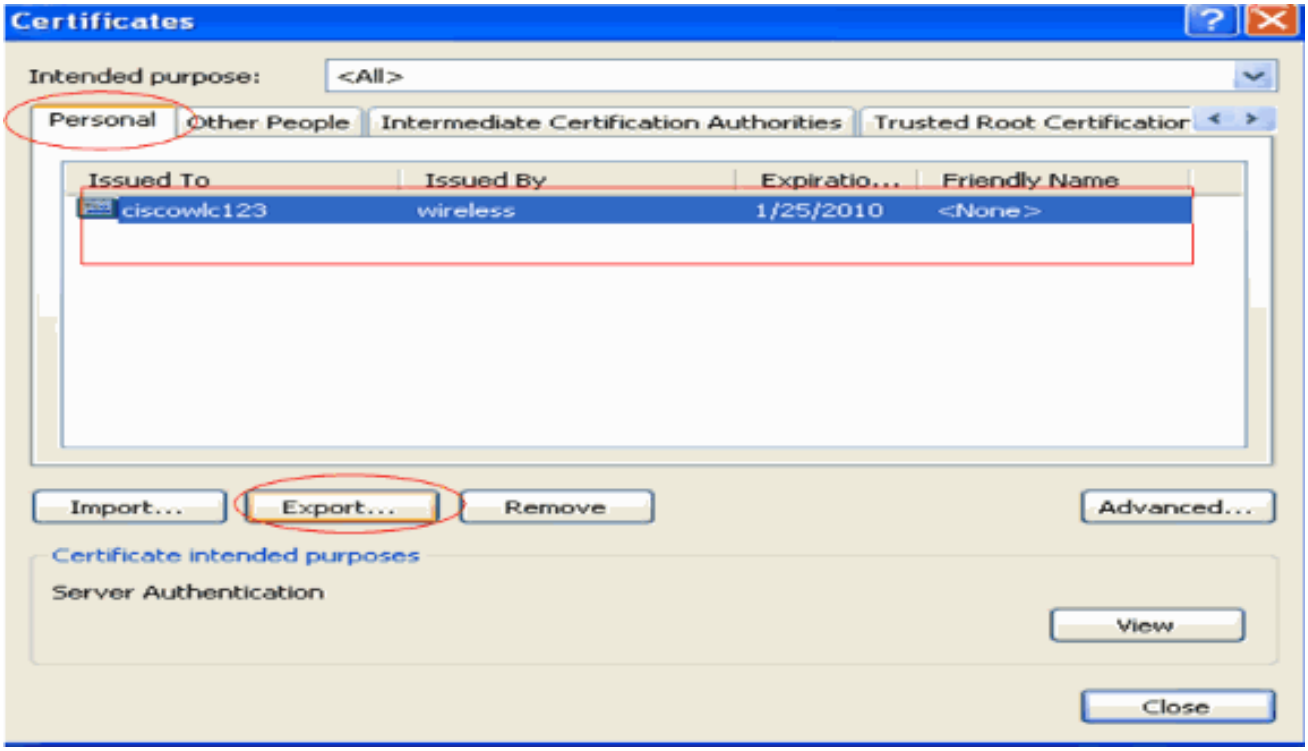
11. تتمثل الخطوة التالية في تصدير هذه الشهادة من مخزن الشهادات إلى القرص الثابت كملف. سيتم إستخدام ملف الشهادة هذا لاحقا لتنزيل الشهادة إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).لتصدير الشهادة من مخزن الشهادات، افتح مستعرض Internet Explorer، ثم انقر فوق **أدوات > خيارات إنترنت**.



12. انقر على **المحتوى** > **الشهادات** للانتقال إلى مخزن الشهادات حيث يتم تثبيت الشهادات بشكل افتراضي.

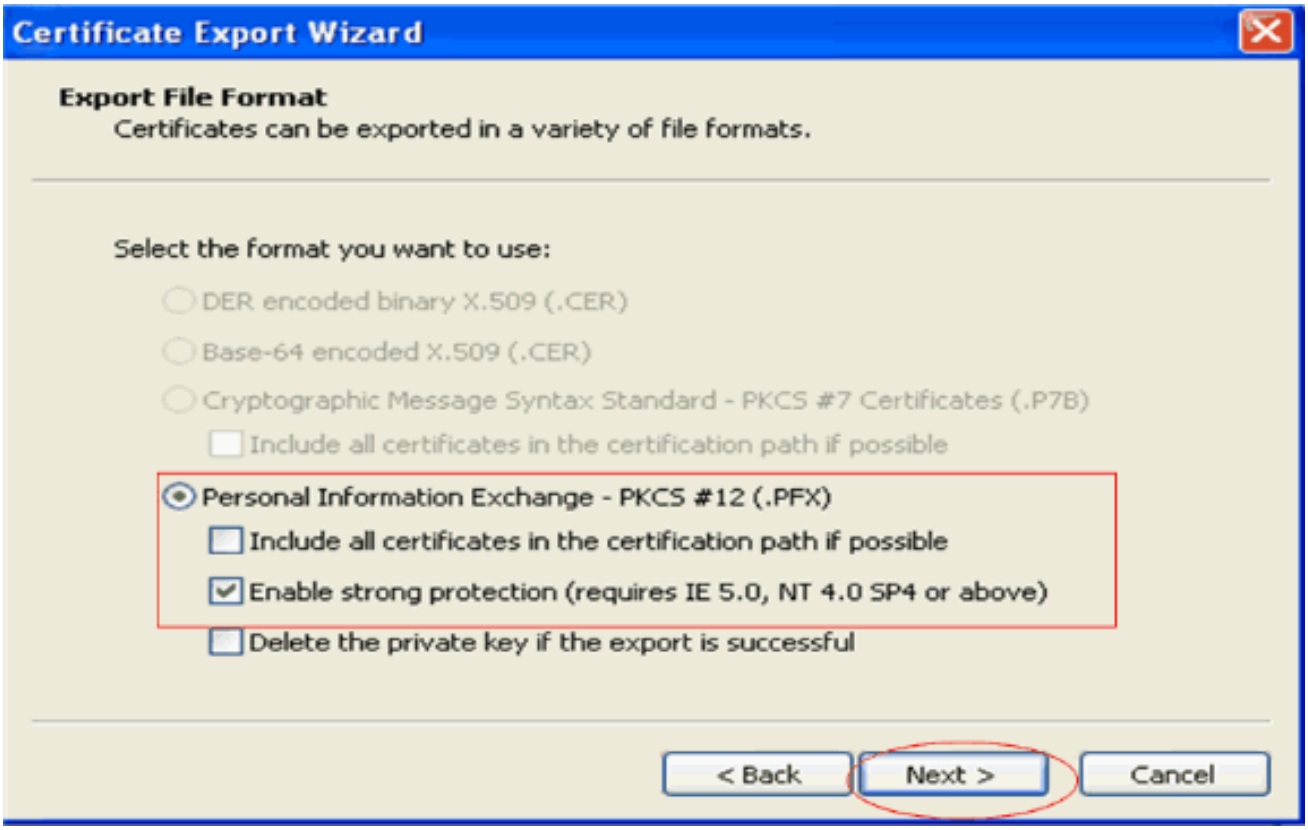


13. يتم تثبيت شهادات الجهاز عادة تحت قائمة الشهادات **الشخصية**. هنا، يجب أن ترى الشهادة المثبتة حديثا. حدد الشهادة وانقر على **تصدير**.



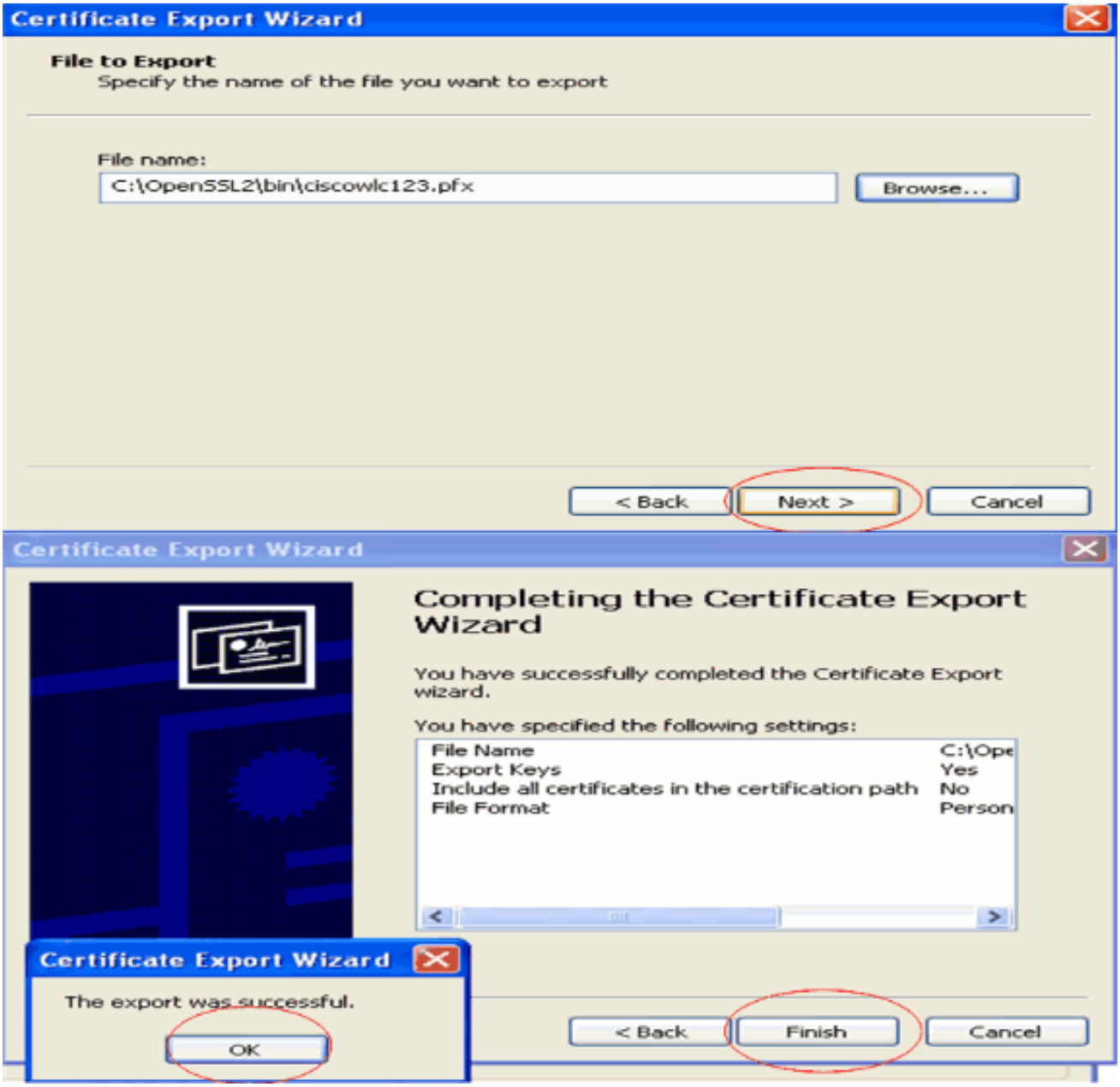
14. طقطقت **بعد ذلك** في النافذة التالي. أختر **نعم، تصدير** خيار **المفتاح الخاص** في نافذة **معالج تصدير الشهادات**. انقر فوق **Next (التالي)**.

15. أختر تنسيق ملف التصدير على هيئة **.PFX** واختر خيار **تمكين الحماية القوية**. انقر فوق **Next (التالي)**.



16. دخلت في الكلمة نافذة، كلمة. يستخدم هذا المثال **Cisco** ككلمة مرور.

17. احفظ ملف الترخيص (.PFX) على قرصك الصلب. طقطقت **بعد ذلك** وأنهيت عملية التصدير بنجاح.



تنزيل شهادة الجهاز على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

الآن بما أن شهادة جهاز WLC متوفرة كملف .PFX، فإن الخطوة التالية هي تنزيل الملف إلى وحدة التحكم. تقبل Cisco WLCs الشهادات بتنسيق .PEM فقط. لذلك، تحتاج أولا لتحويل ملف تنسيق .PFX أو PKCS12 إلى ملف PEM باستخدام برنامج OpenSSL.

تحويل الشهادة بتنسيق PFX إلى تنسيق PEM باستخدام برنامج OpenSSL

يمكنك نسخ الشهادة إلى أي كمبيوتر تم تثبيت OpenSSL فيه لتحويلها إلى تنسيق PEM. أدخل هذه الأوامر على ملف OpenSSL.exe في مجلد الحاويات الخاص ببرنامج OpenSSL:

ملاحظة: يمكنك تنزيل OpenSSL من موقع OpenSSL على الويب.

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem
ciscowlc123 is the name used in this example for the exported file. !--- You can specify ---!
any name to your certificate file. Enter Import Password : cisco
This is the same password that is mentioned in step 16 of the previous section. MAC ---!
verified Ok Enter PEM Pass phrase : cisco
```

```
Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM ---!
pass phrase : cisco
```

يتم تحويل ملف الشهادة إلى تنسيق PEM. تتمثل الخطوة التالية في تنزيل شهادة جهاز تنسيق PEM إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

ملاحظة: قبل ذلك، كنت بحاجة إلى برنامج خادم TFTP على الكمبيوتر الشخصي من حيث سيتم تنزيل ملف PEM. يجب أن يحتوي هذا الكمبيوتر على اتصال ب WLC. يجب أن يكون لخادم TFTP دليله الحالي والأساسي المحدد مع الموقع حيث يتم تخزين ملف PEM.

تنزيل شهادة جهاز تنسيق PEM المحولة إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

يشرح هذا المثال عملية التنزيل من خلال CLI (واجهة سطر الأوامر) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC).

1. تسجيل الدخول إلى واجهة سطر الأوامر (CLI) لوحدة التحكم.
2. أدخل الأمر **transfer download dataType eapdevcert**.
3. أدخل الأمر **transfer download server** 10.77.244.196.10.77.244.196 هو عنوان IP الخاص بخادم TFTP.
4. أدخل الأمر **transfer download filename** ciscoWLC.pem.CiscoWLC123.pem هو اسم الملف المستخدم في هذا المثال.
5. أدخل الأمر **transfer download certpassword** لتعيين كلمة المرور للشهادة.
6. أدخل الأمر **transfer download start** لعرض الإعدادات المحدثة.بعد ذلك، أجب **y** عند مطالبتك بتأكيد الإعدادات الحالية وبدء عملية التنزيل.يوضح هذا المثال إخراج أمر التنزيل:

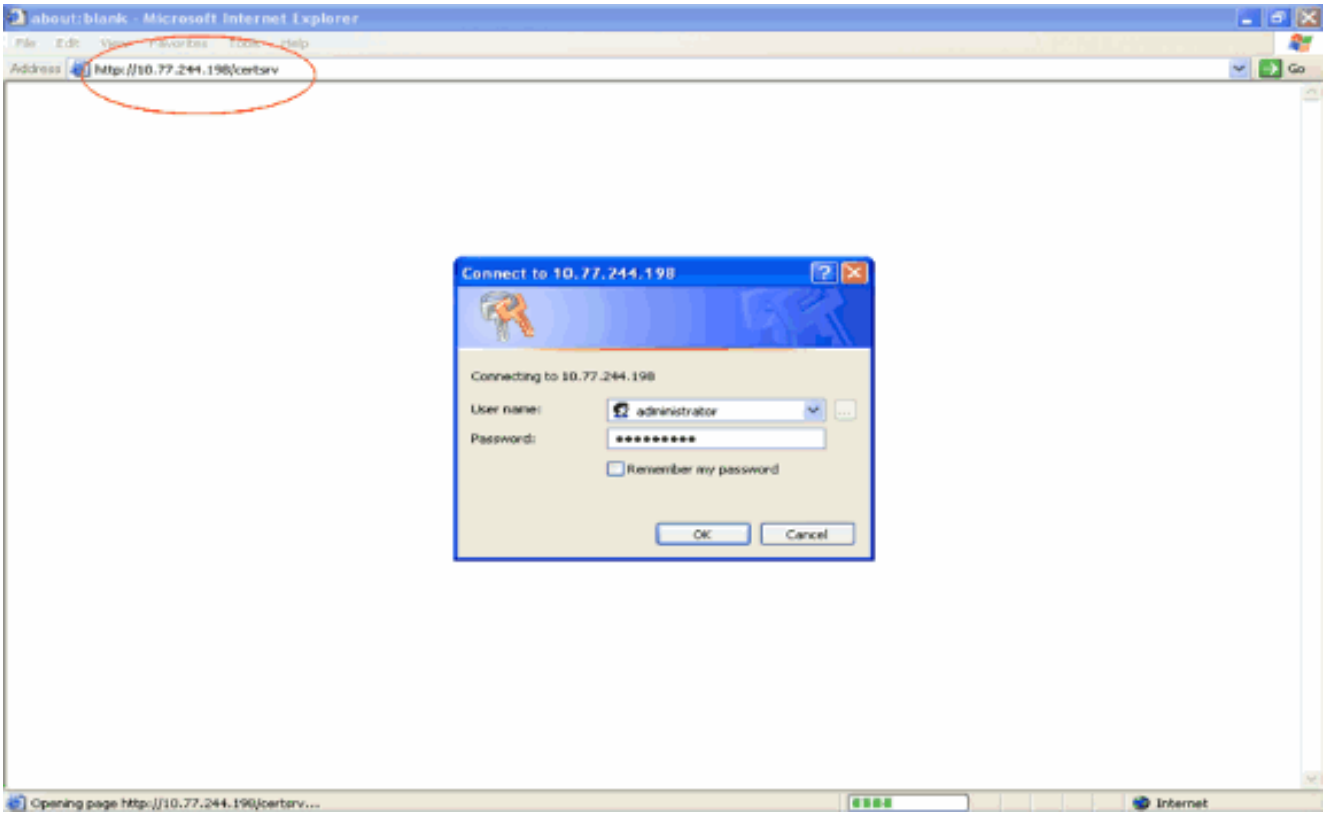
```
Cisco Controller) >transfer download start)

                                    Mode..... TFTP
                    Data Type..... Vendor Dev Cert
                  TFTP Server IP..... 10.77.244.196
                      TFTP Packet Timeout..... 6
                    TFTP Max Retries..... 10
                                    .....TFTP Path
                  TFTP Filename..... ciscowlc.pem

                                    .This may take some time
                  Are you sure you want to start? (y/N) y
                      .TFTP EAP CA cert transfer starting
                                    .Certificate installed
                .Reboot the switch to use the new certificate
            .Enter the reset system command to reboot the controller
        .The controller is now loaded with the device certificate
```

7. أدخل الأمر **reset system** لإعادة تشغيل وحدة التحكم. تم تحميل وحدة التحكم الآن بشهادة الجهاز.

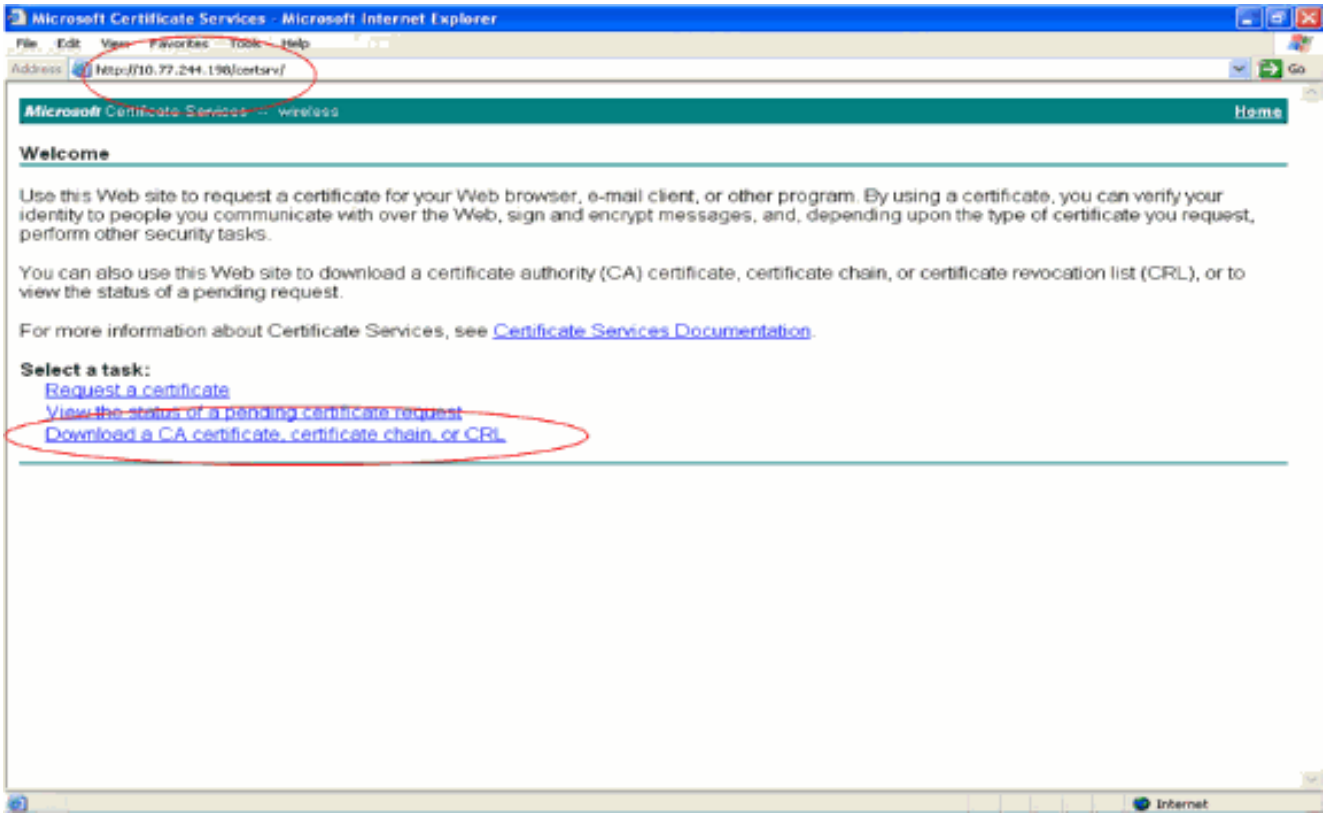
تثبيت شهادة جذر PKI في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

الآن وقد تم تثبيت شهادة الجهاز في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فإن الخطوة التالية هي تثبيت شهادة الجذر الخاصة بمكون التحكم في الشبكة المحلية اللاسلكية (PKI) إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من خادم CA. قم بإجراء هذه الخطوات :

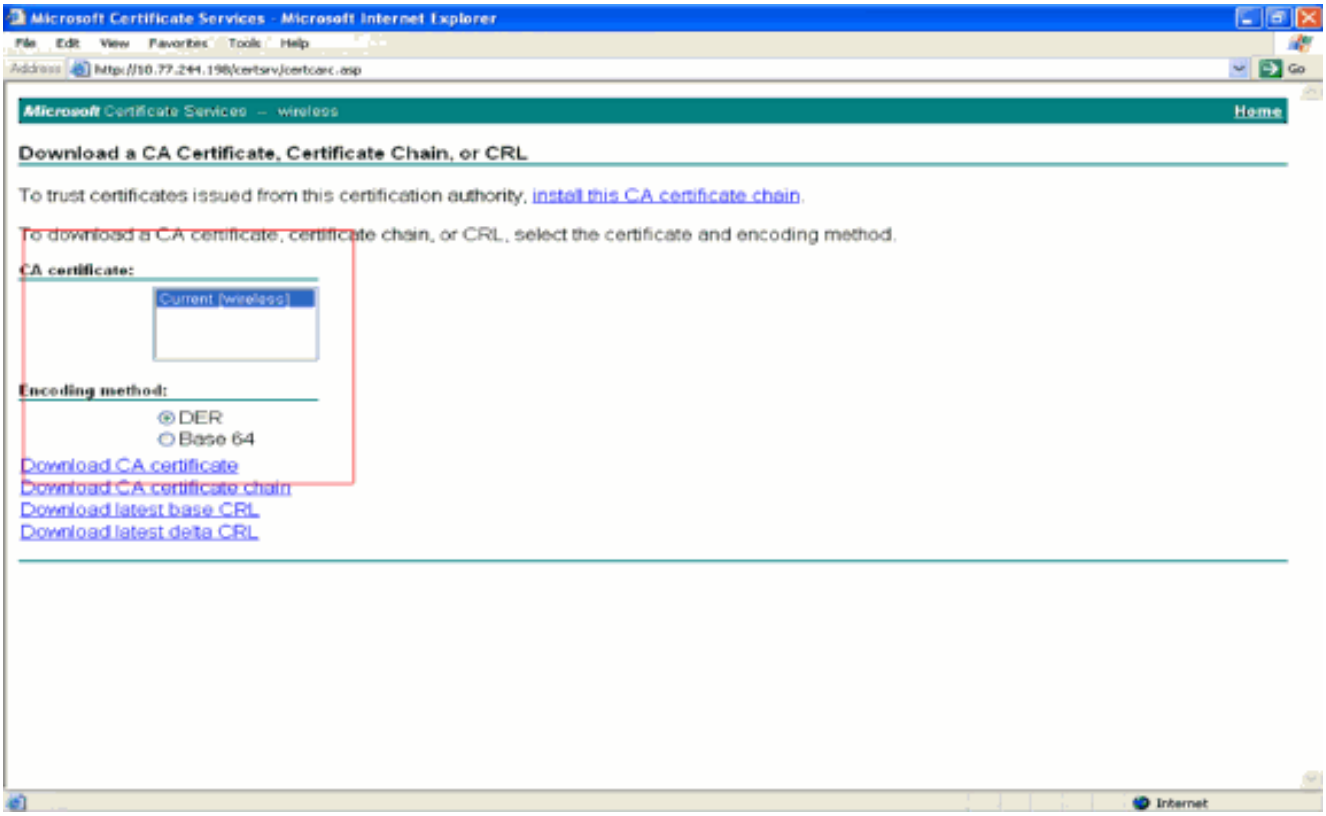
1. انتقل إلى **http://<IP عنوان CA Server>/certsrv** من pc الخاص بك الذي له اتصال شبكة بخادم CA. تسجيل الدخول كمسؤول عن خادم CA.



2. انقر على **تنزيل شهادة CA أو سلسلة شهادات أو CRL**.



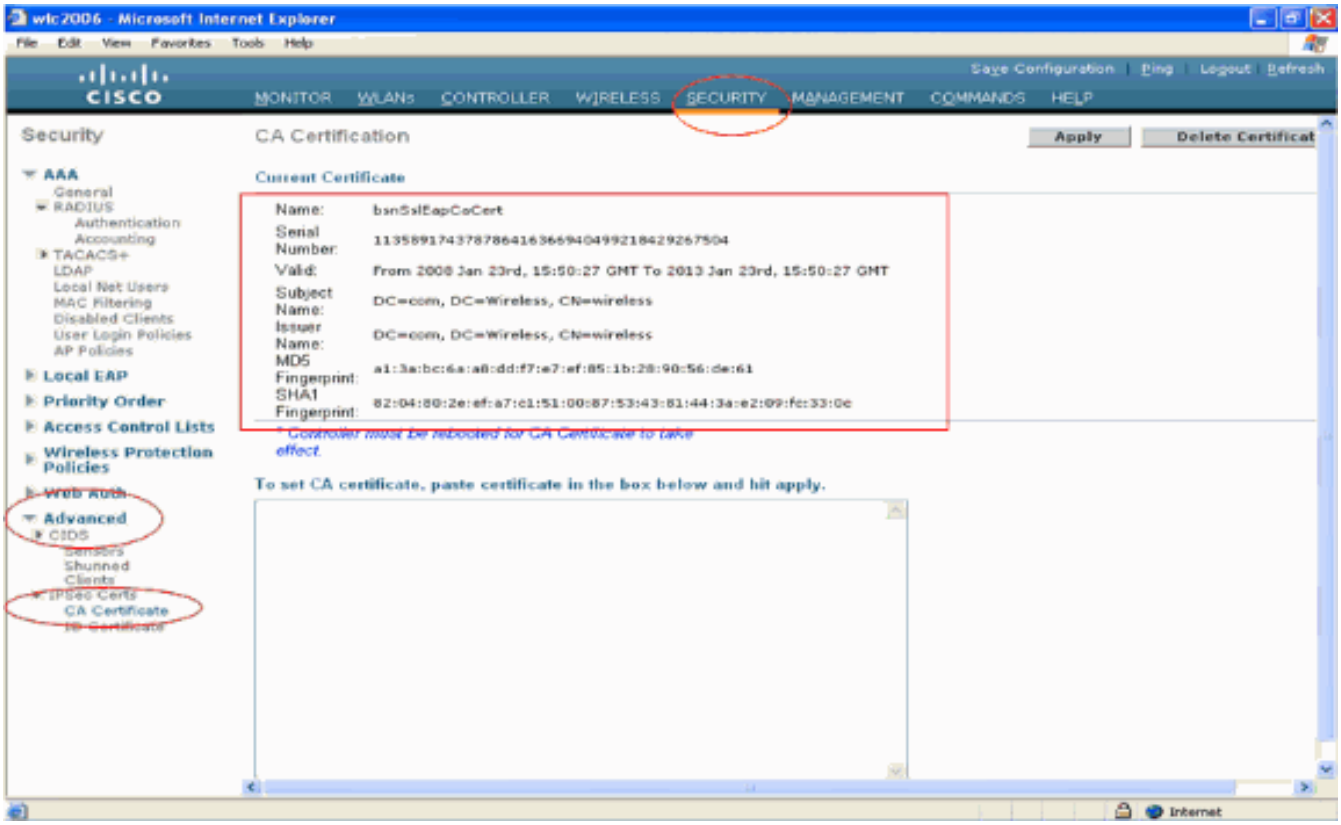
3. في الصفحة الناتجة، يمكنك أن ترى شهادات CA الحالية المتاحة على خادم CA تحت مربع **شهادة CA**. أختر **DER** كالترميز طريقة وطقطقة **تنزيل مرجع مصدق**.



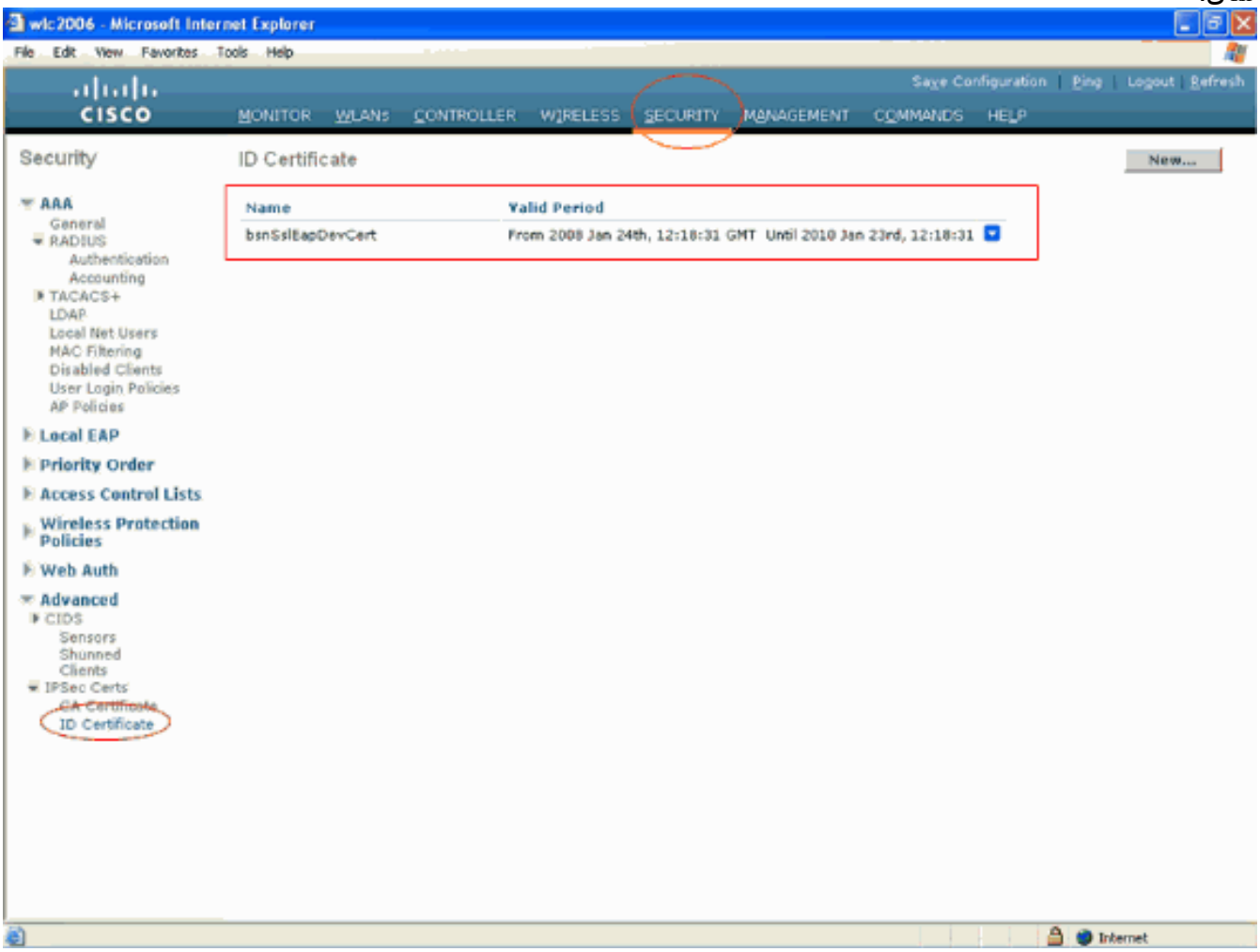
4. احفظ الشهادة كملف **.cer**. يستخدم هذا المثال **certnew.cer** كاسم الملف.
5. تتمثل الخطوة التالية في تحويل ملف .cer إلى تنسيق PEM وتنزيله إلى وحدة التحكم. للقيام بهذه الخطوات، كرر نفس الإجراء الموضح في قسم تنزيل شهادة الجهاز إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مع هذه التغييرات:إن الملفات "OpenSSL -in" و "-out" هي **certnew.cer** و**certnew.pem**.كما لا يلزم وجود عبارة مرور PEM أو كلمات مرور الاستيراد في هذه العملية.أيضا، أمر OpenSSL لتحويل ملف **cer.** إلى ملف **.pem** هو*certnew.cer* **-in X509 - إعلام PEM-** *DER -out certnew.pem* **خارجي**في الخطوة 2 من تنزيل شهادة الجهاز بتنسيق PEM المحول إلى قسم WLC، يكون الأمر لتنزيل الشهادة إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC):(وحدة التحكم من Cisco)>**نقل تنزيل البيانات**الملف المطلوب تنزيله إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) هو **certnew.pem**.

أنت يستطيع دققت ما إذا كانت الشهادات ركبت على ال WLC من الجهاز تحكم gui كما يلي:

- من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق **الأمان**. في صفحة الأمان، انقر فوق **خيارات متقدمة > عناصر IPSec** من المهام التي تظهر على اليسار. انقر على **شهادة المرجع المصدق** لعرض شهادة المرجع المصدق المثبتة. هنا مثال:



- للتحقق من تثبيت شهادة الجهاز على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق **الأمان**. في صفحة الأمان، انقر فوق **خيارات متقدمة > عناصر IPSec** من المهام التي تظهر على اليسار. انقر على **شهادة المعرف** لعرض شهادة الجهاز المثبتة. هنا
مثال:

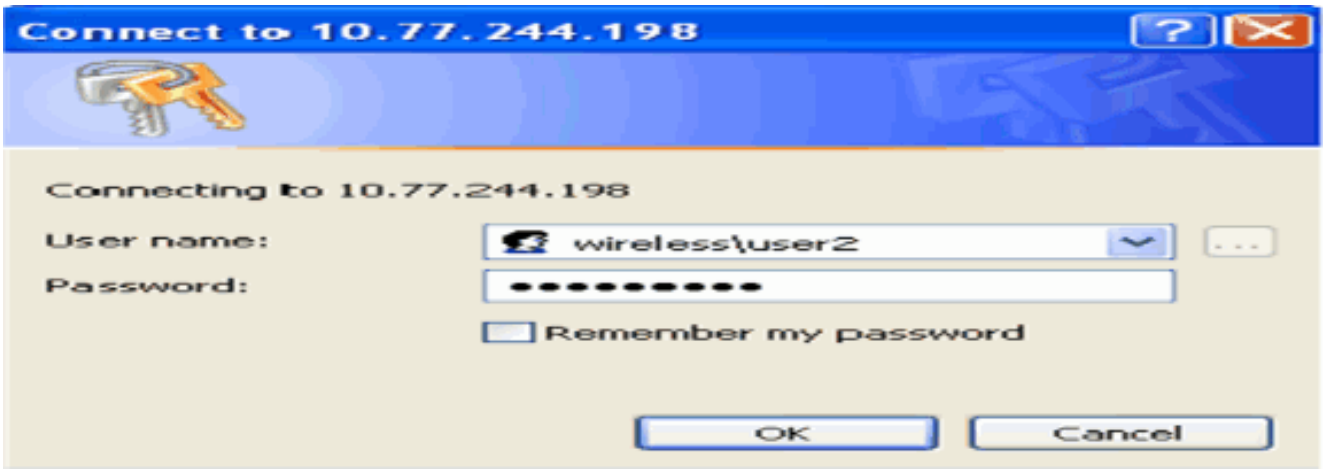


إنشاء شهادة جهاز للعميل

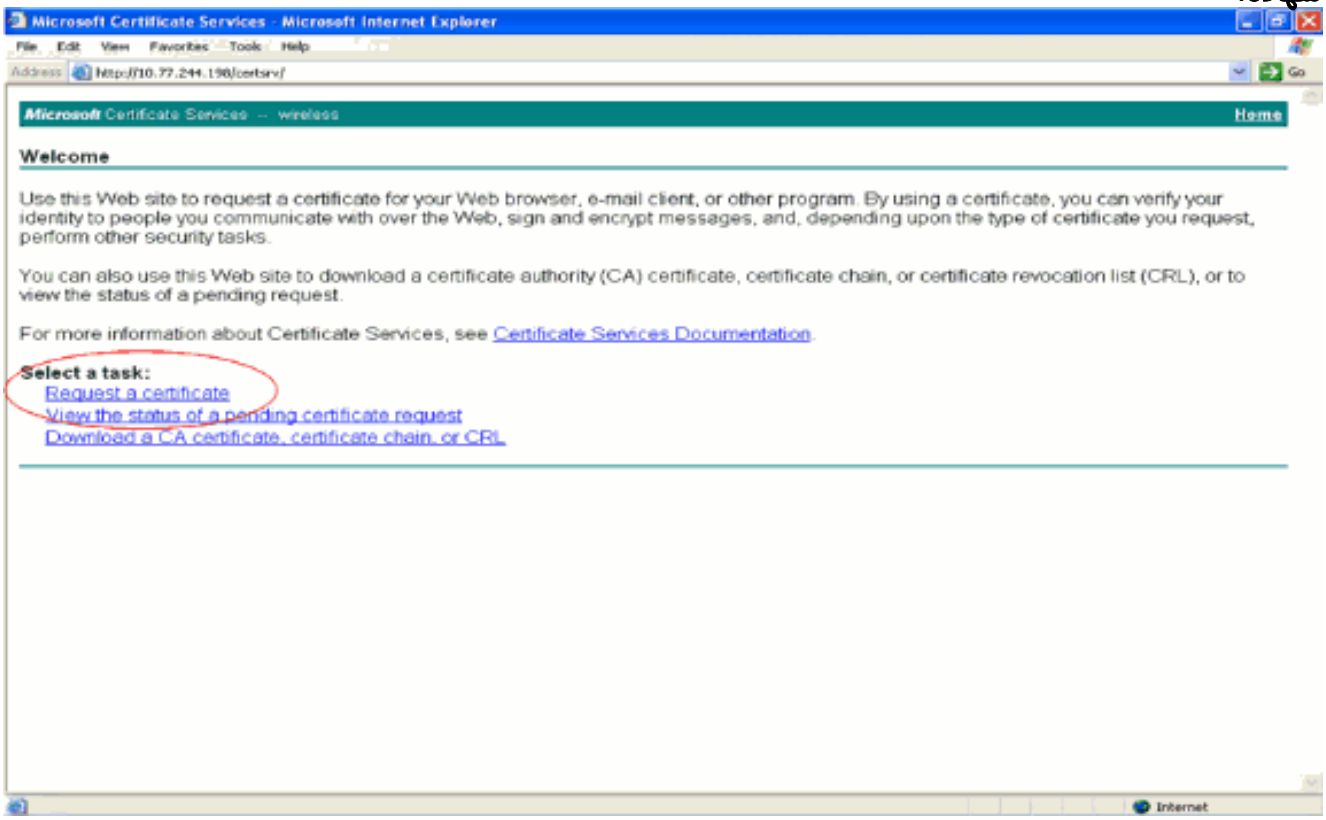
الآن وقد تم تثبيت شهادة الجهاز وشهادة CA على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فإن الخطوة التالية هي إنشاء هذه الشهادات للعميل.

قم بإجراء هذه الخطوات لإنشاء شهادة الجهاز للعميل. سيستخدم العميل هذه الشهادة للمصادقة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يشرح هذا المستند الخطوات المعنية بإنشاء شهادات عميل Windows XP Professional.

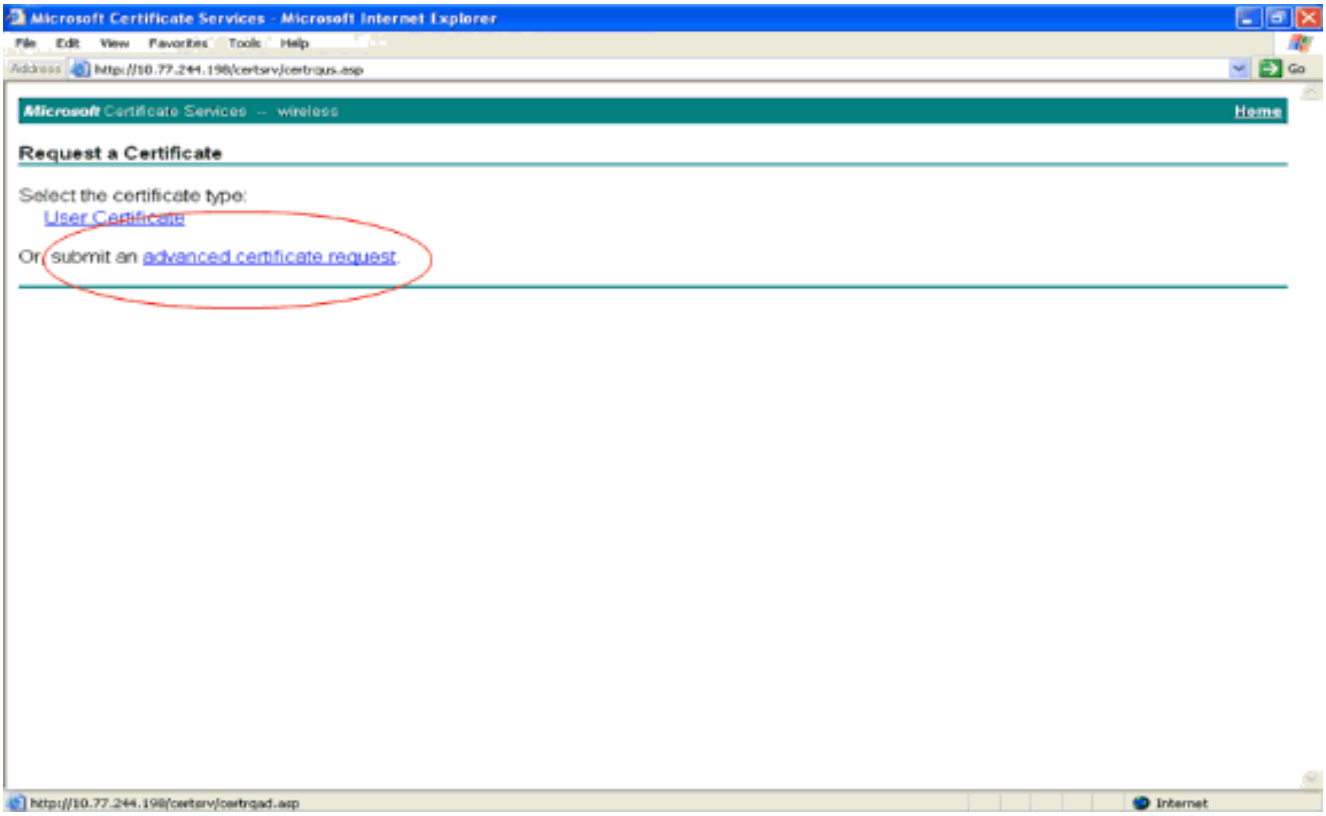
1. انتقل إلى **http://<IP address of CA server>/certsrv** من العميل الذي يتطلب تثبيت الشهادة. قم بتسجيل الدخول باسم المجال\اسم المستخدم إلى خادم CA. يجب أن يكون اسم المستخدم هو اسم المستخدم الذي يستخدم جهاز XP هذا، ويجب تكوين المستخدم بالفعل كجزء من نفس المجال مثل خادم CA.



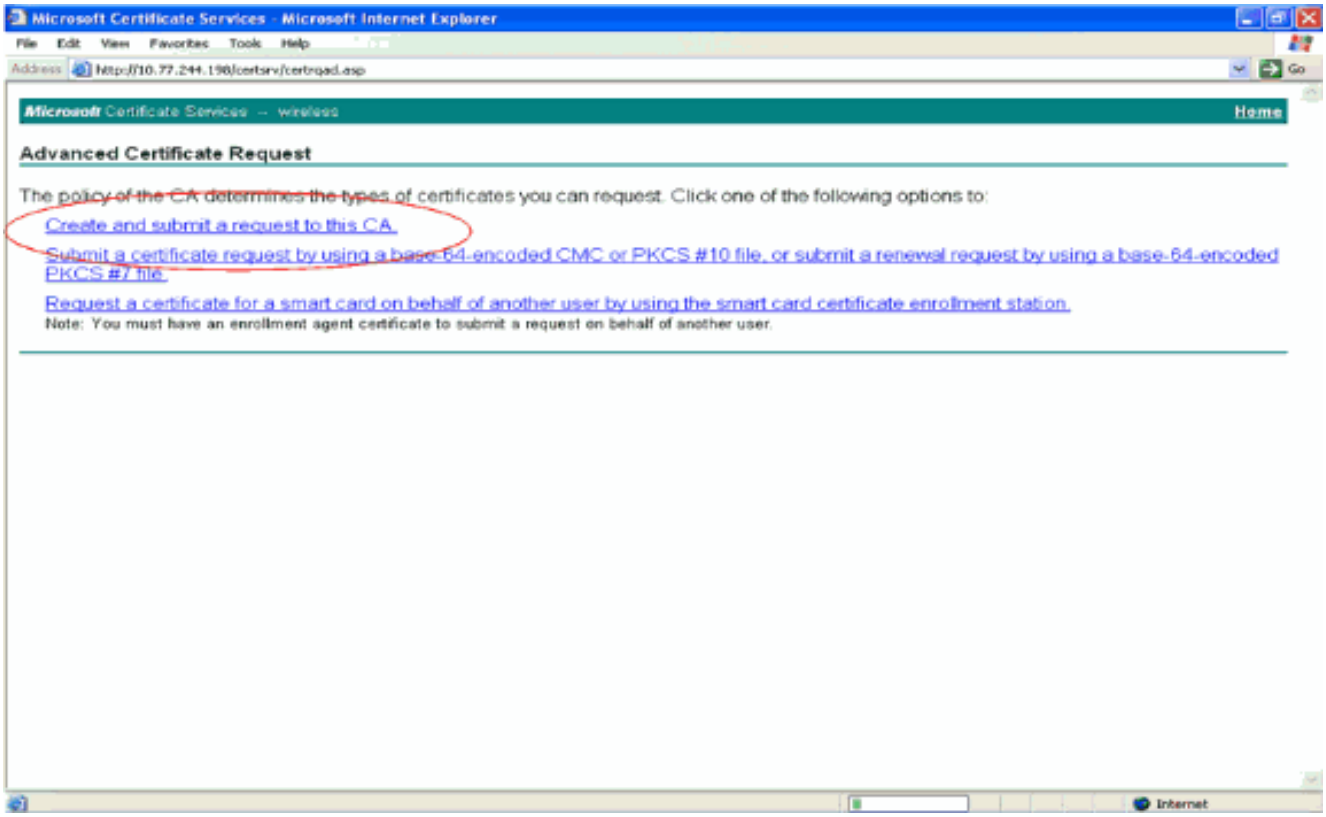
2. حدد **طلب شهادة**.



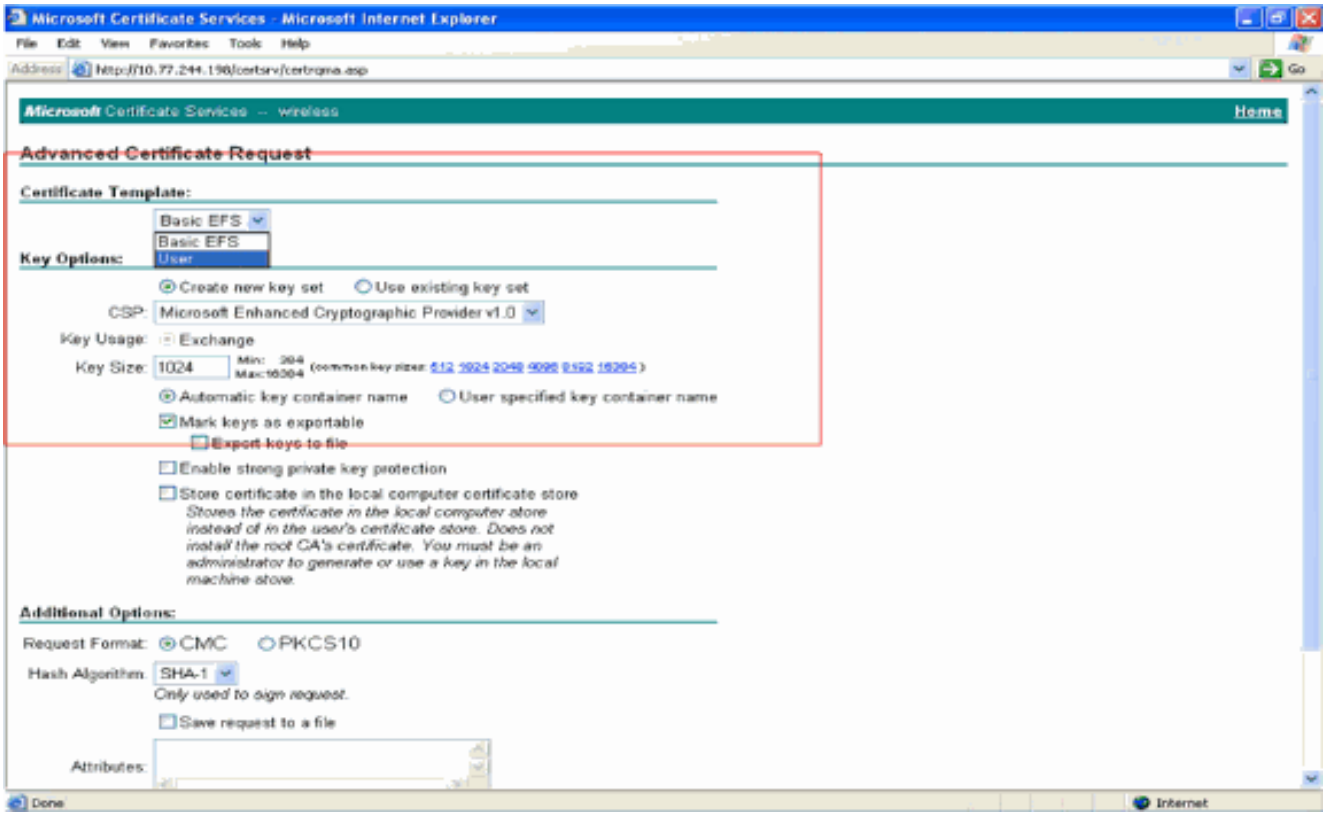
3. في صفحة طلب شهادة، انقر على **طلب شهادة متقدمة**.



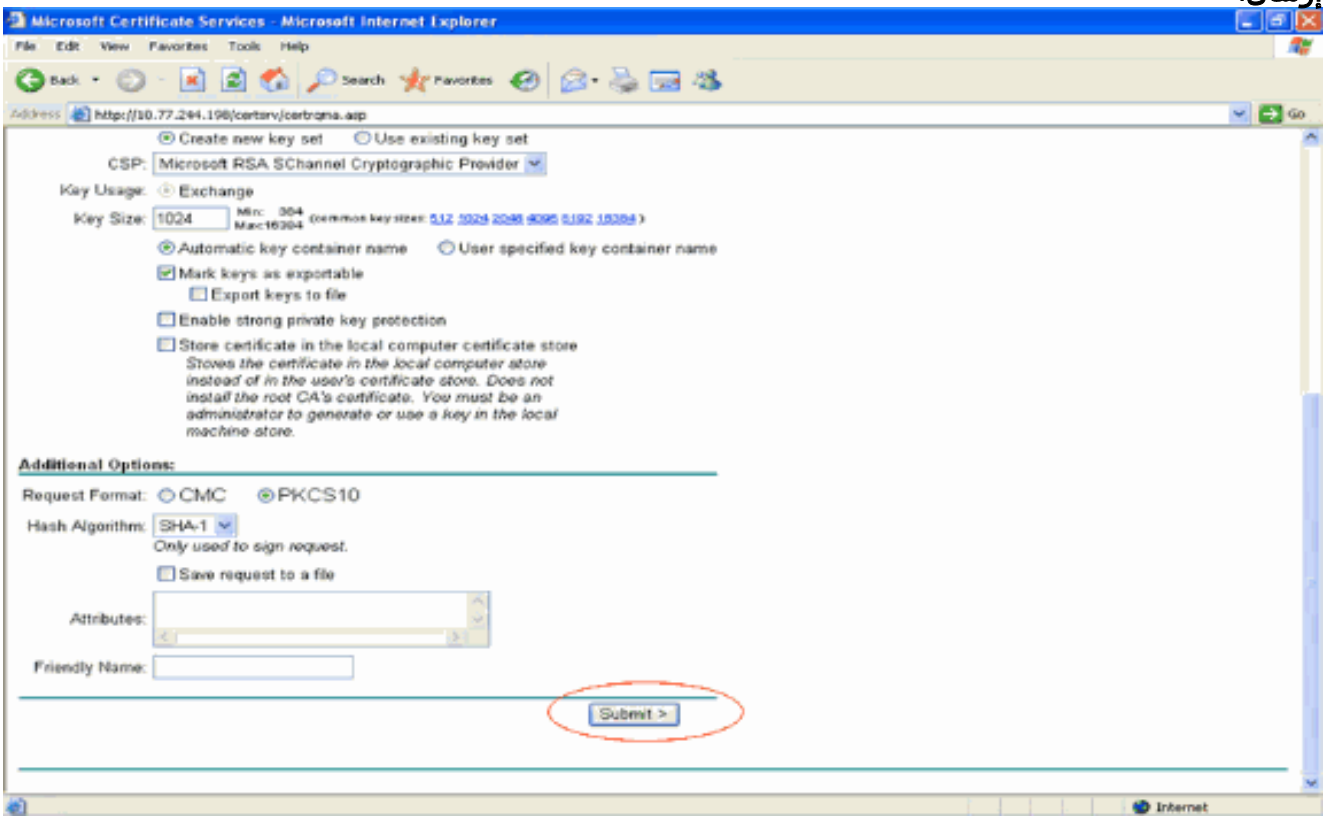
4. في صفحة طلب الشهادة المتقدمة، انقر على **إنشاء طلب وإرساله إلى المرجع المصدق هذا**. ينقلك هذا إلى نموذج طلب الشهادة
المتقدمة.



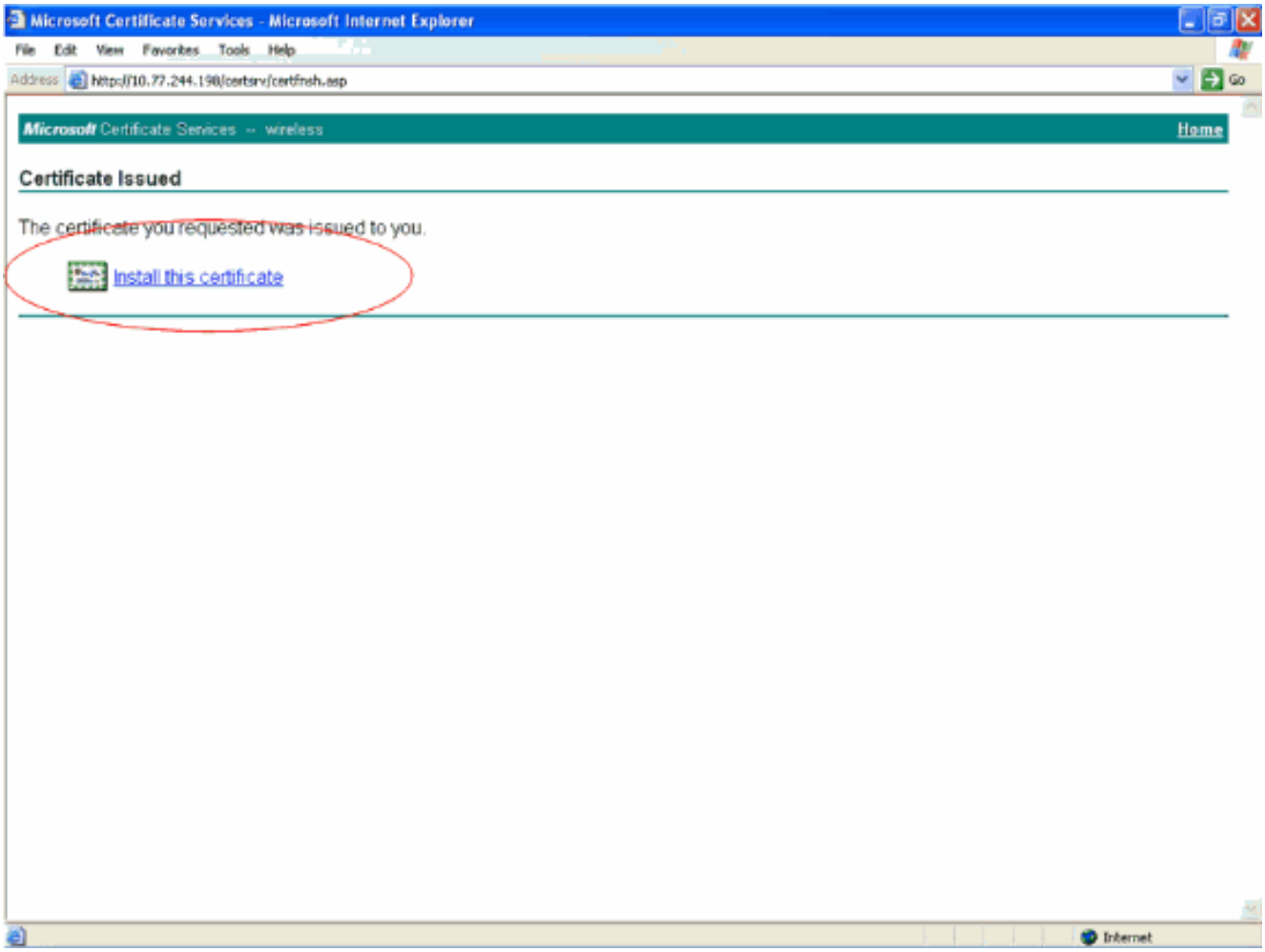
5. في نموذج طلب الشهادة المتقدمة، أختر **مستخدم** من القائمة المنسدلة قالب الشهادة.تحت قسم خيارات المفتاح، أختر المعاملات التالية:أدخل حقل حجم المفتاح. يستخدم هذا المثال **1024**.حدد خيار **وضع علامة على المفاتيح كقابلة للتصدير**.



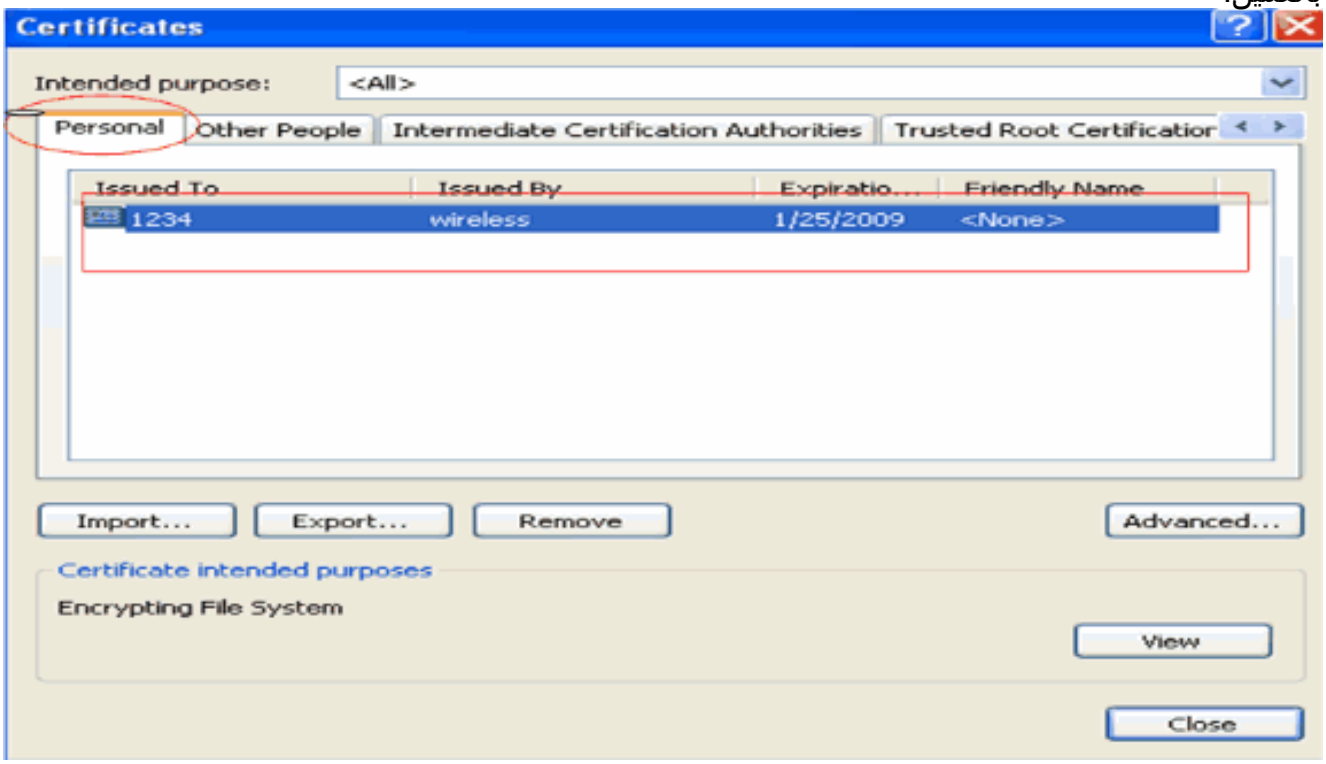
6. قم بتكوين كافة الحقول الضرورية الأخرى وانقر فوق **إرسال**.



7. يتم الآن إنشاء شهادة جهاز العميل وفقا للطلب. انقر على **تثبيت الشهادة** لتثبيت الشهادة في مخزن الشهادات.



8. يجب أن تكون قادرا على العثور على شهادة جهاز العميل مثبتة ضمن قائمة الشهادات الشخصية تحت **أدوات > خيارات الإنترنت > المحتوى > الشهادات** على مستعرض IE الخاص بالعميل.

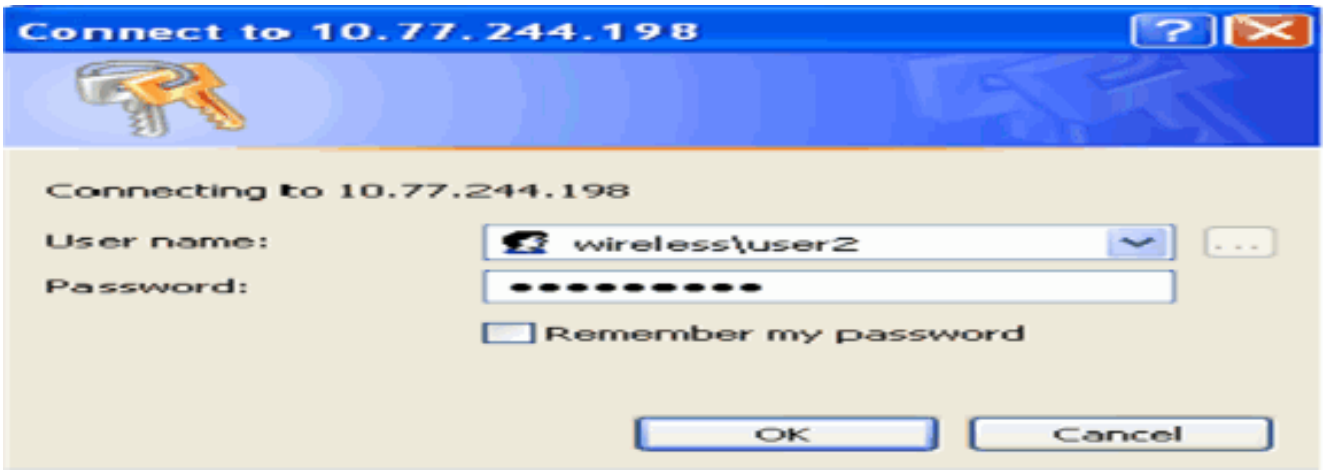


شهادة الجهاز الخاصة بالعميل مثبتة على العميل.

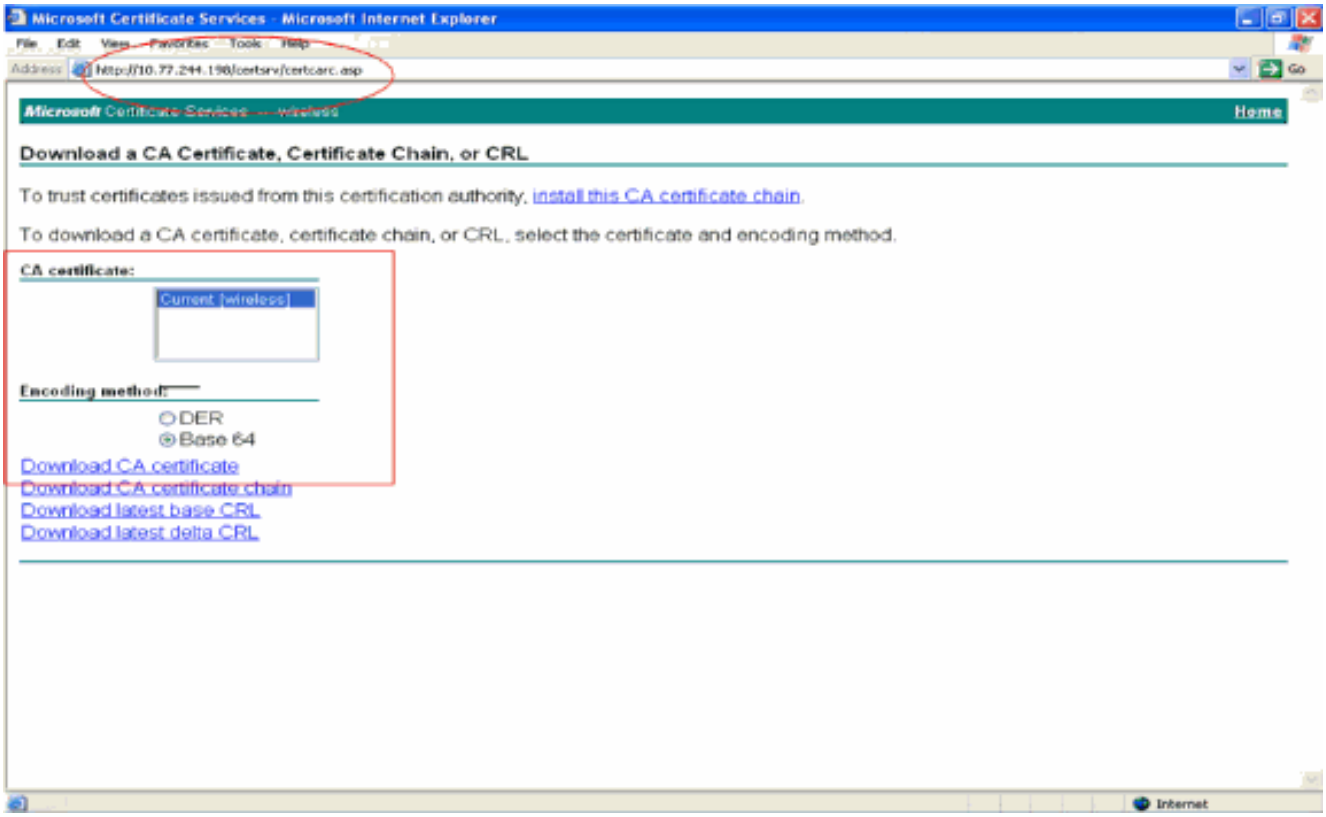
إنشاء شهادة المرجع المصدق الجذر للعميل

تتمثل الخطوة التالية في إنشاء شهادة CA للعميل. أكمل الخطوات التالية من كمبيوتر العميل:

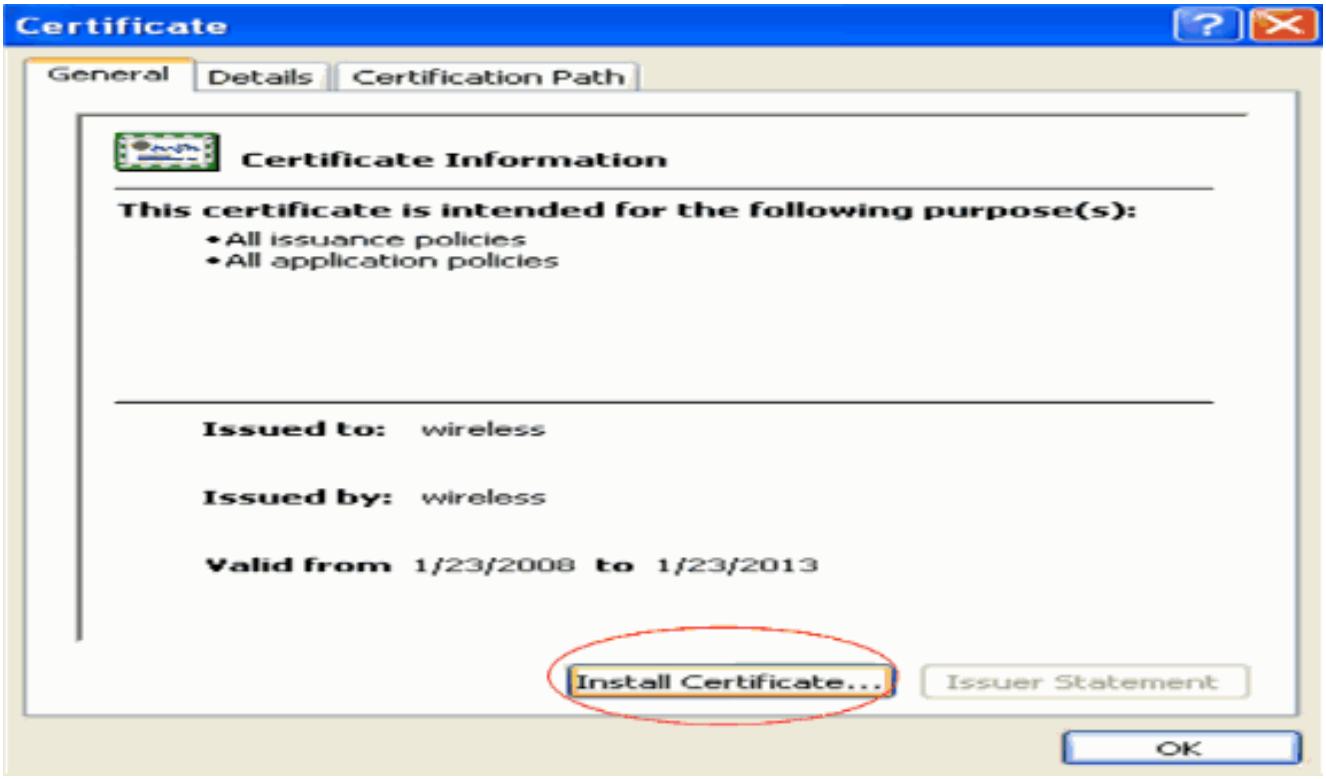
1. انتقل إلى **http://<IP address of CA server>/certsrv** من العميل الذي يتطلب تثبيت الشهادة. قم بتسجيل الدخول باسم المجال\اسم المستخدم إلى خادم CA. يجب أن يكون اسم المستخدم هو اسم المستخدم الذي يستخدم جهاز XP هذا، ويجب تكوين المستخدم بالفعل كجزء من نفس المجال مثل خادم CA.



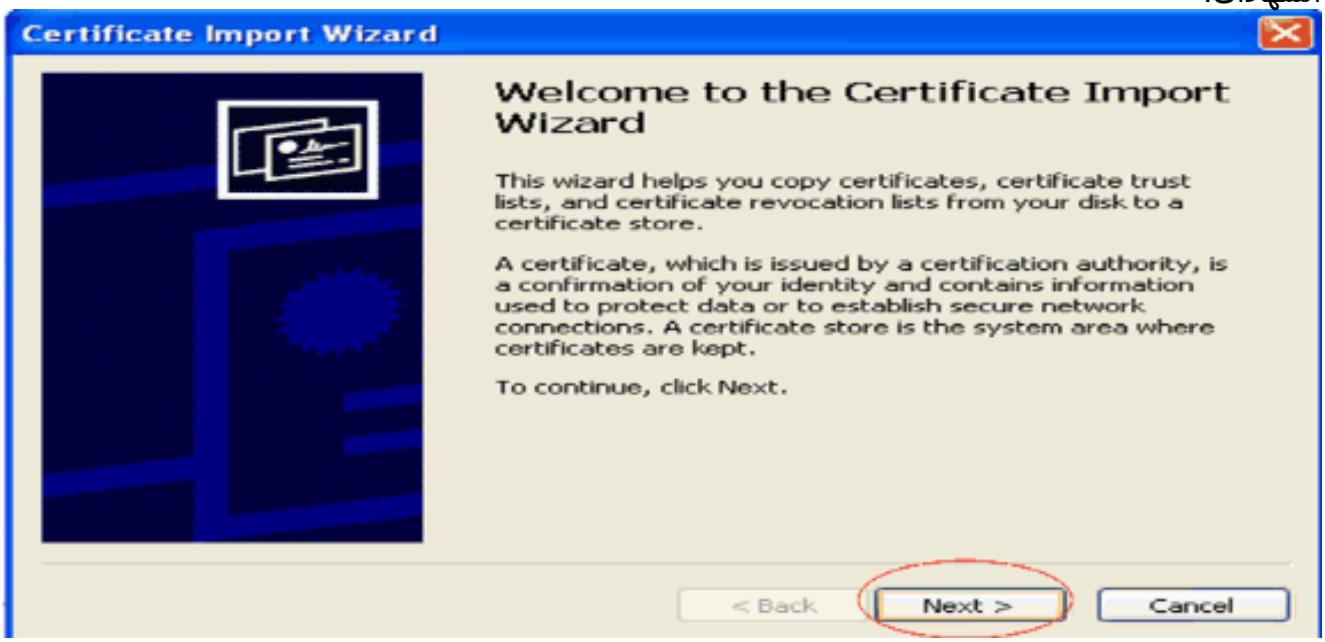
2. في الصفحة الناتجة، يمكنك أن ترى شهادات CA الحالية المتاحة على خادم CA تحت مربع **شهادة CA**. أختر **Base 64** كطريقة تشفير. ثم انقر على **تنزيل شهادة CA** واحفظ الملف على كمبيوتر العميل كملف **.cer**. يستخدم هذا المثال **rootca.cer** كاسم الملف.



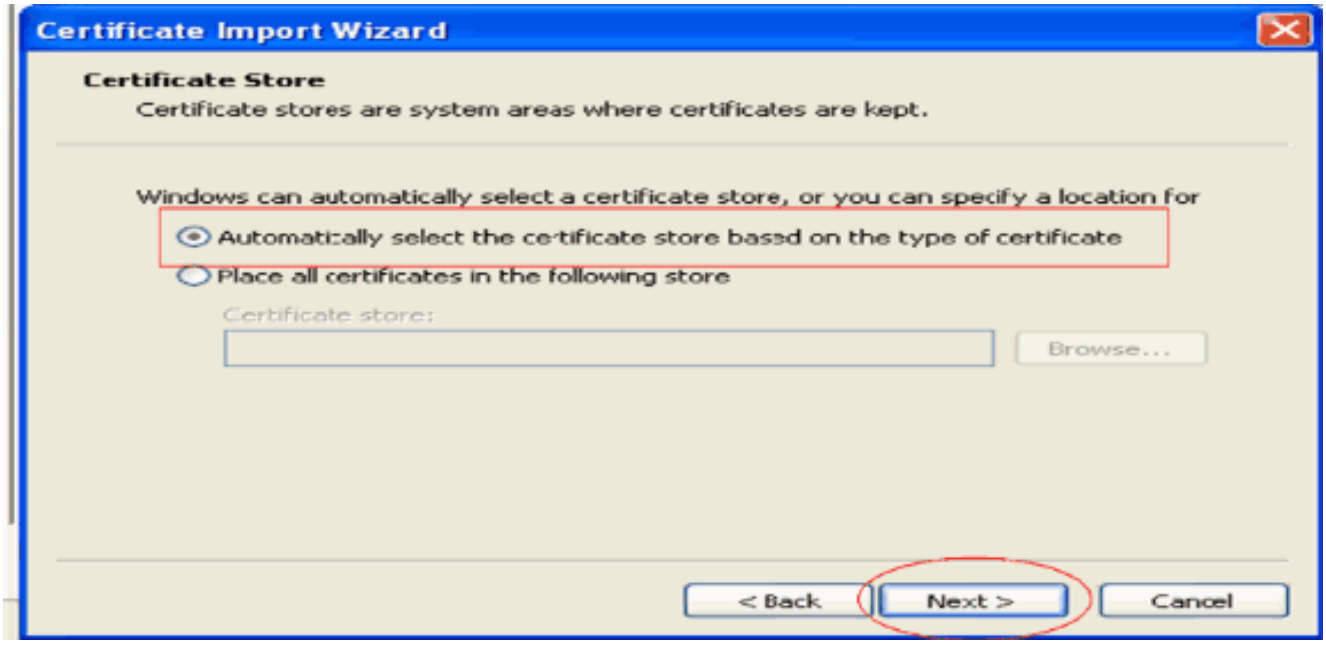
3. بعد ذلك، قم بتثبيت شهادة المرجع المصدق المحفوظة بتنسيق .cer إلى مخزن شهادات العميل. انقر نقرا مزدوجا على ملف rootca.cer وانقر فوق **تثبيت الشهادة**.



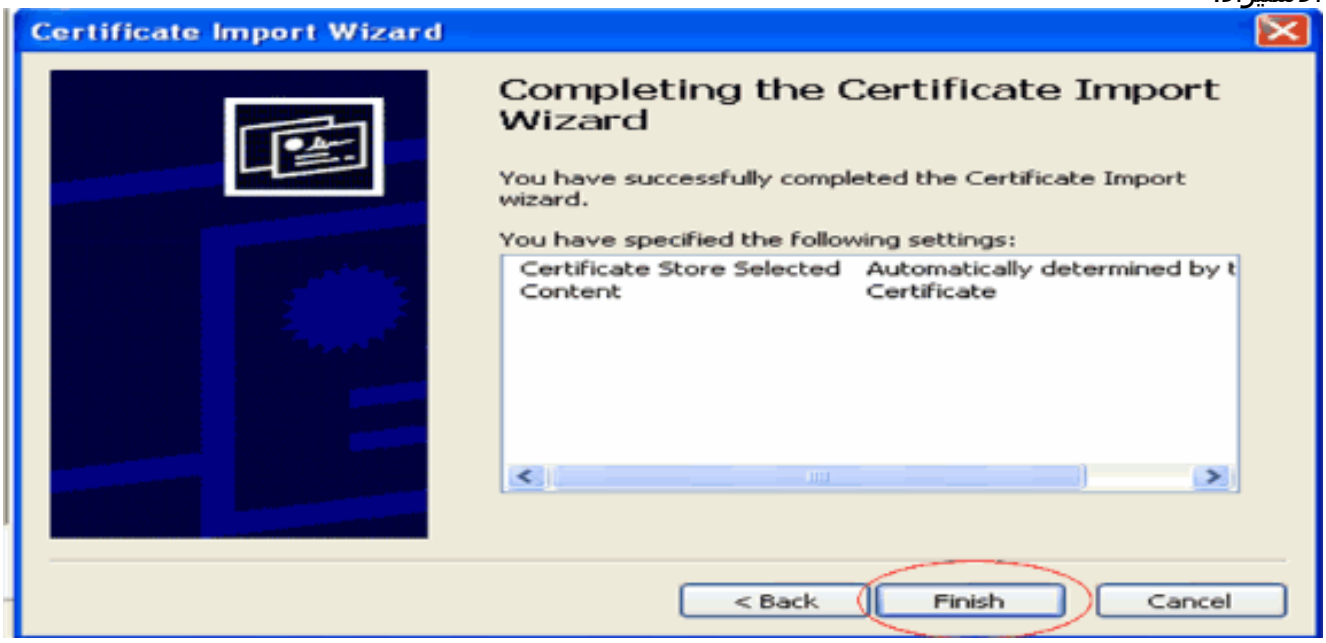
4. انقر على **التالي** لاستيراد الشهادة من قرص العميل الثابت إلى مخزن الشهادات.



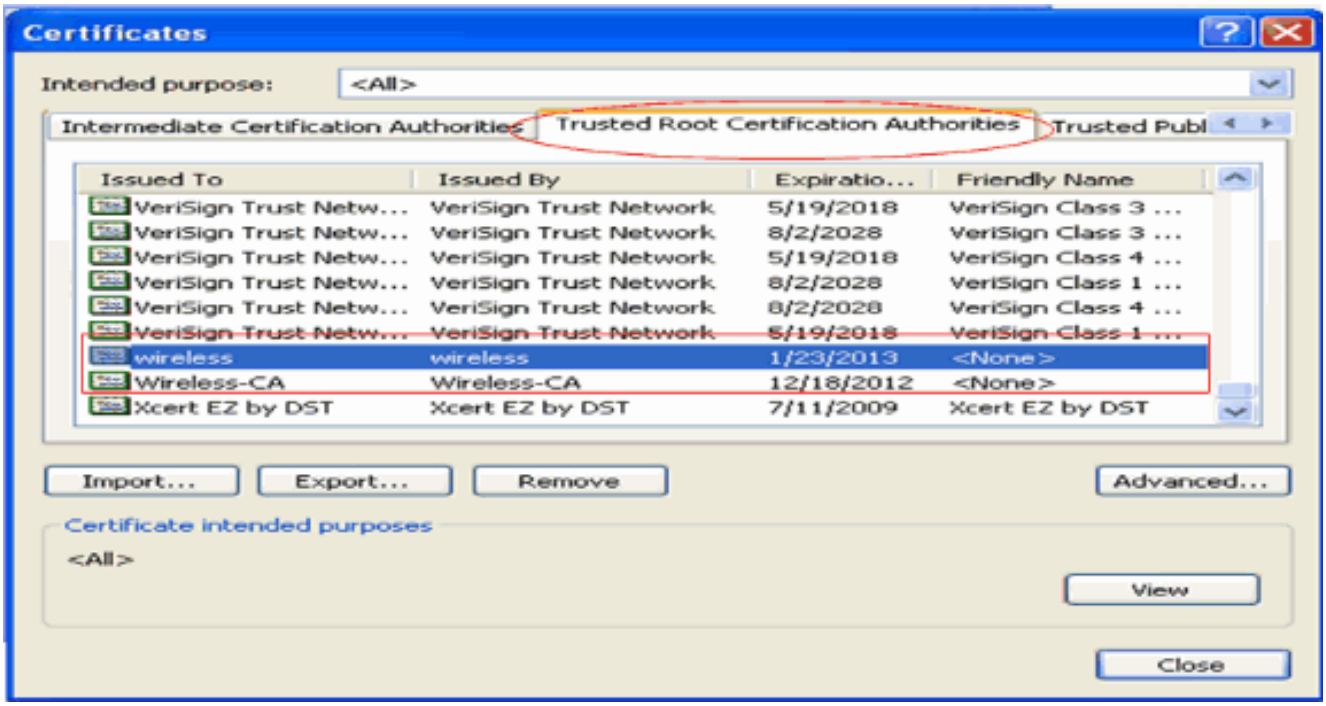
5. أختر **تحديد مخزن الشهادات تلقائيا بناء على نوع الشهادة** وانقر **التالي**.



6. طقطقة **إنجاز** in order to أنهيت عملية الاستيراد.



7. وبشكل افتراضي، يتم تثبيت شهادات المرجع المصدق تحت قائمة مراجع التصديق الجذر الموثوق بها في مستعرض IE الخاص بالعميل تحت **أدوات > خيارات الإنترنت > المحتوى > الشهادات**. هنا مثال:

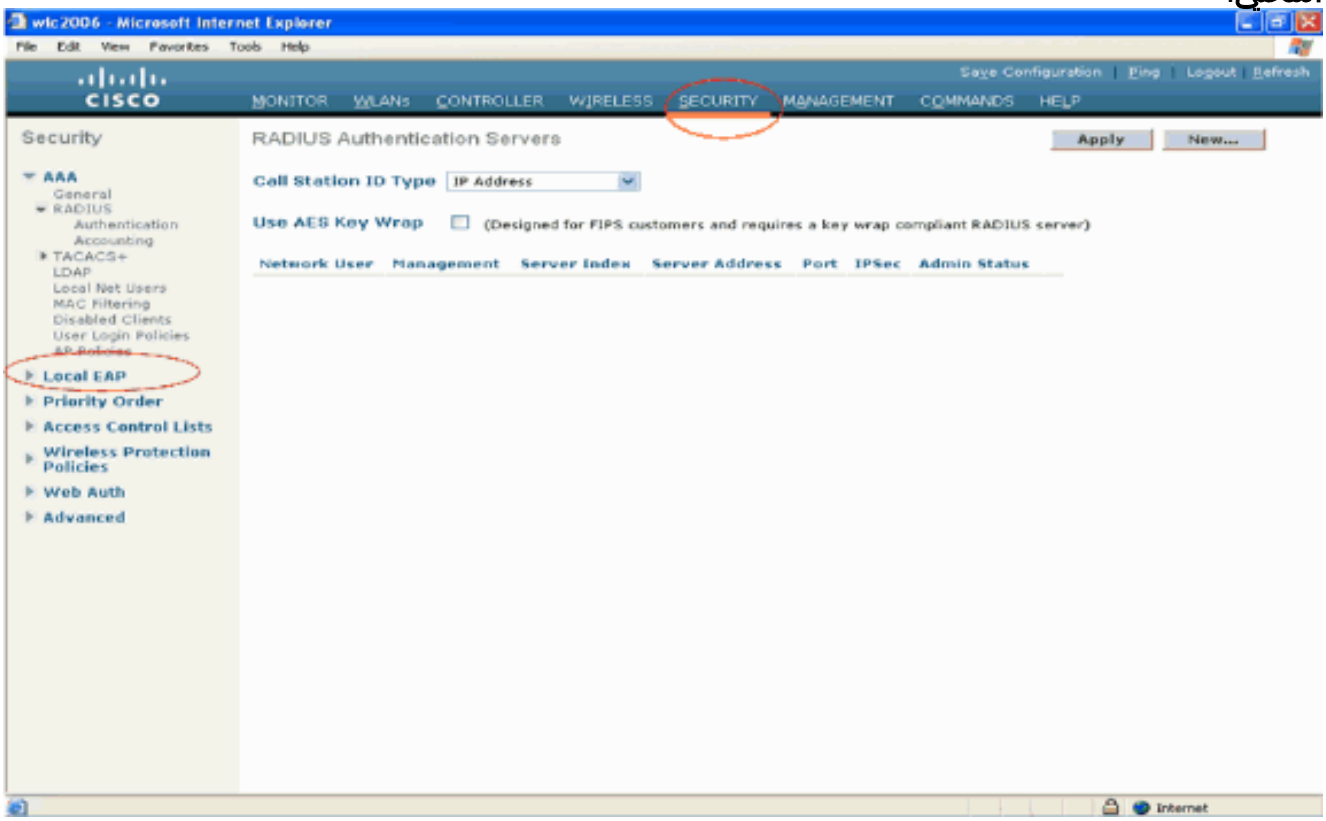


تثبت جميع الشهادات المطلوبة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وكذلك على العميل لمصادقة EAP-FAST المحلية. تتمثل الخطوة التالية في تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة EAP المحلية.

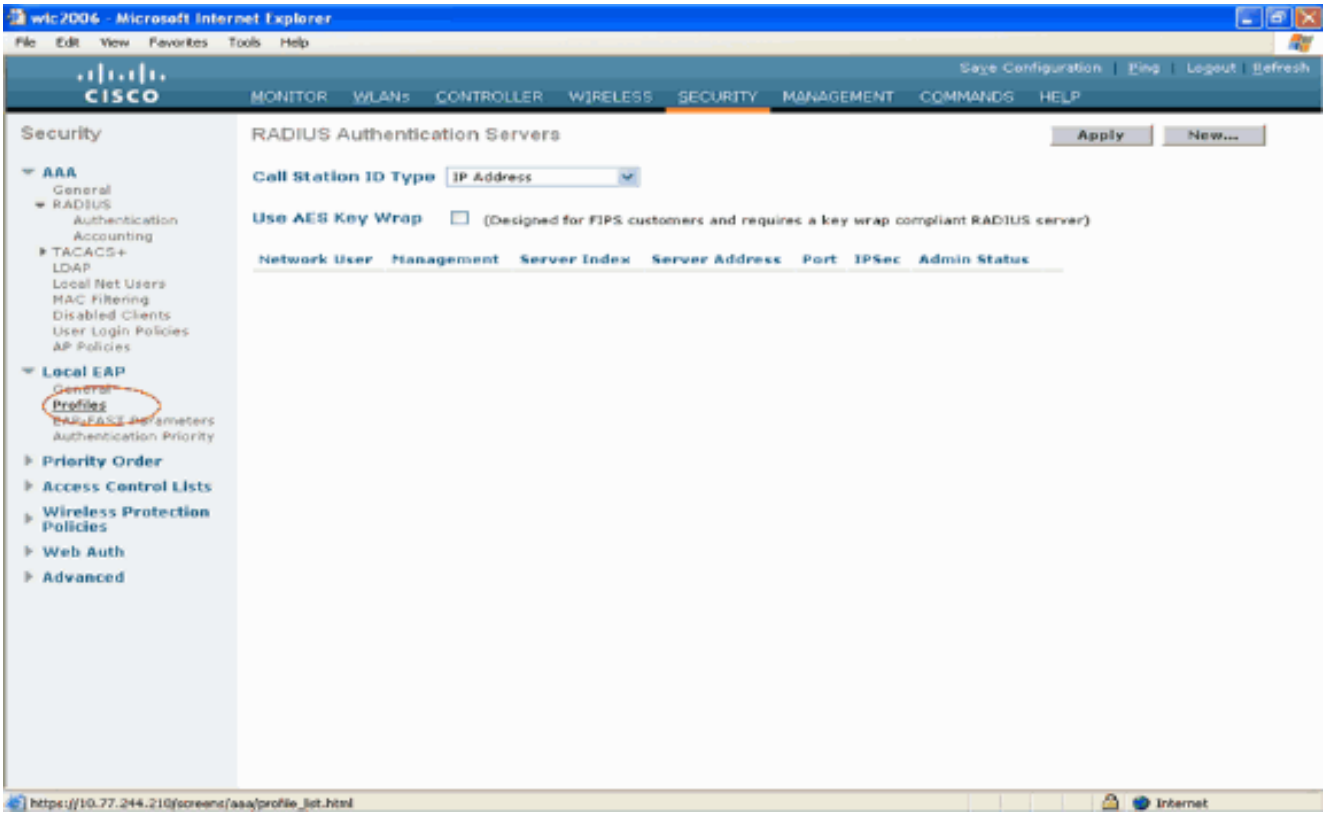
تكوين EAP المحلي على WLC

أتمت هذا steps من **ال WLC GUI أسلوب** in order to شكلت محلي EAP مصادقة على ال WLC:

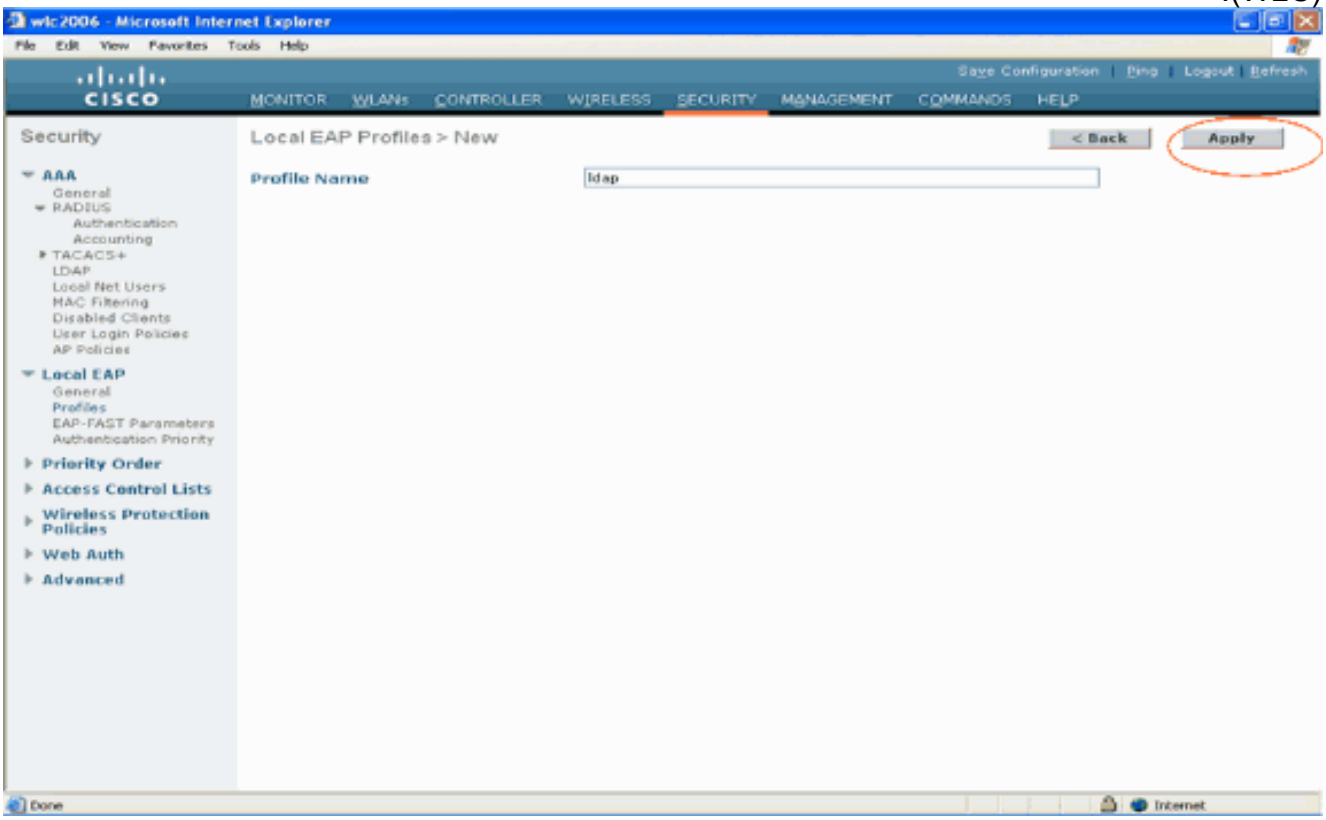
1. انقر على **التأمين > EAP المحلي**.



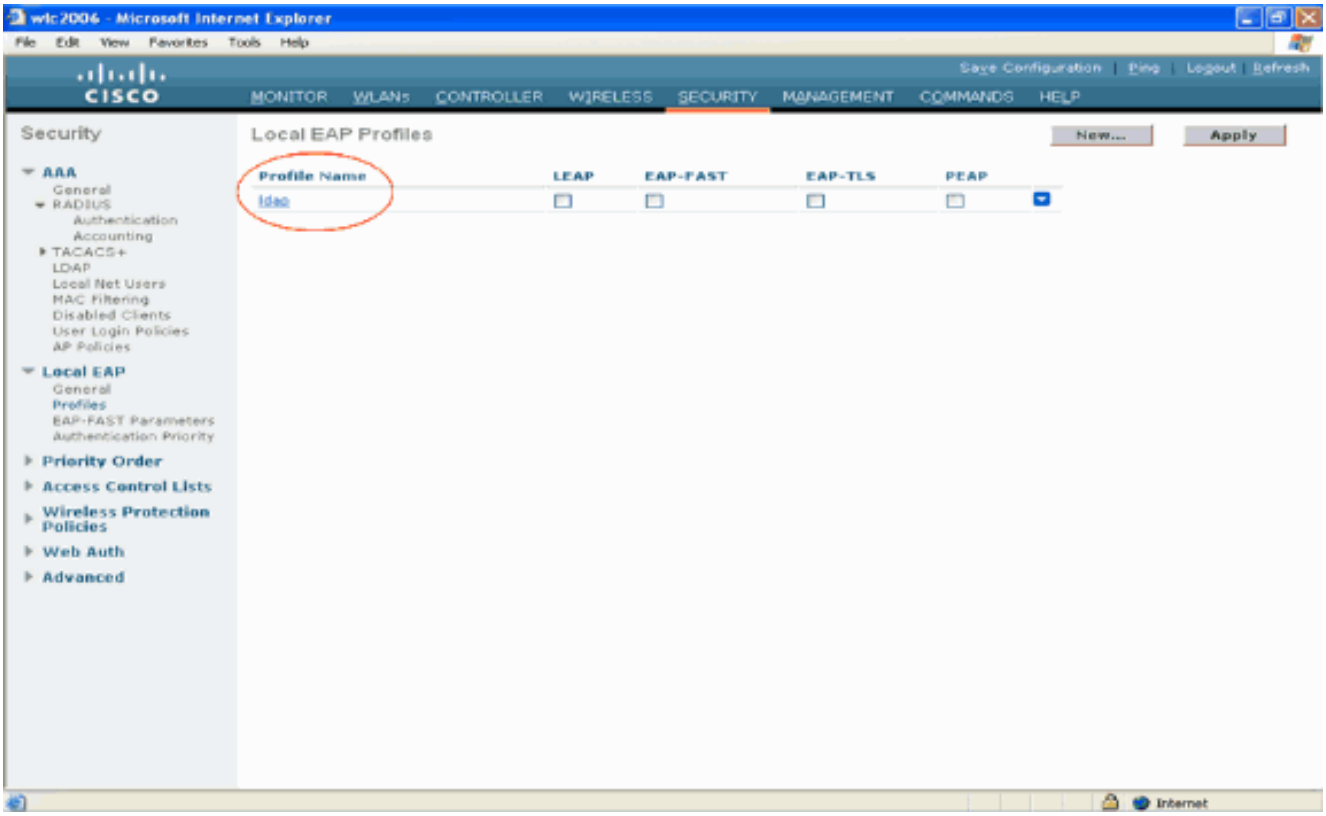
2. تحت EAP المحلي، انقر على **توصيفات** لتكوين ملف تعريف EAP المحلي.



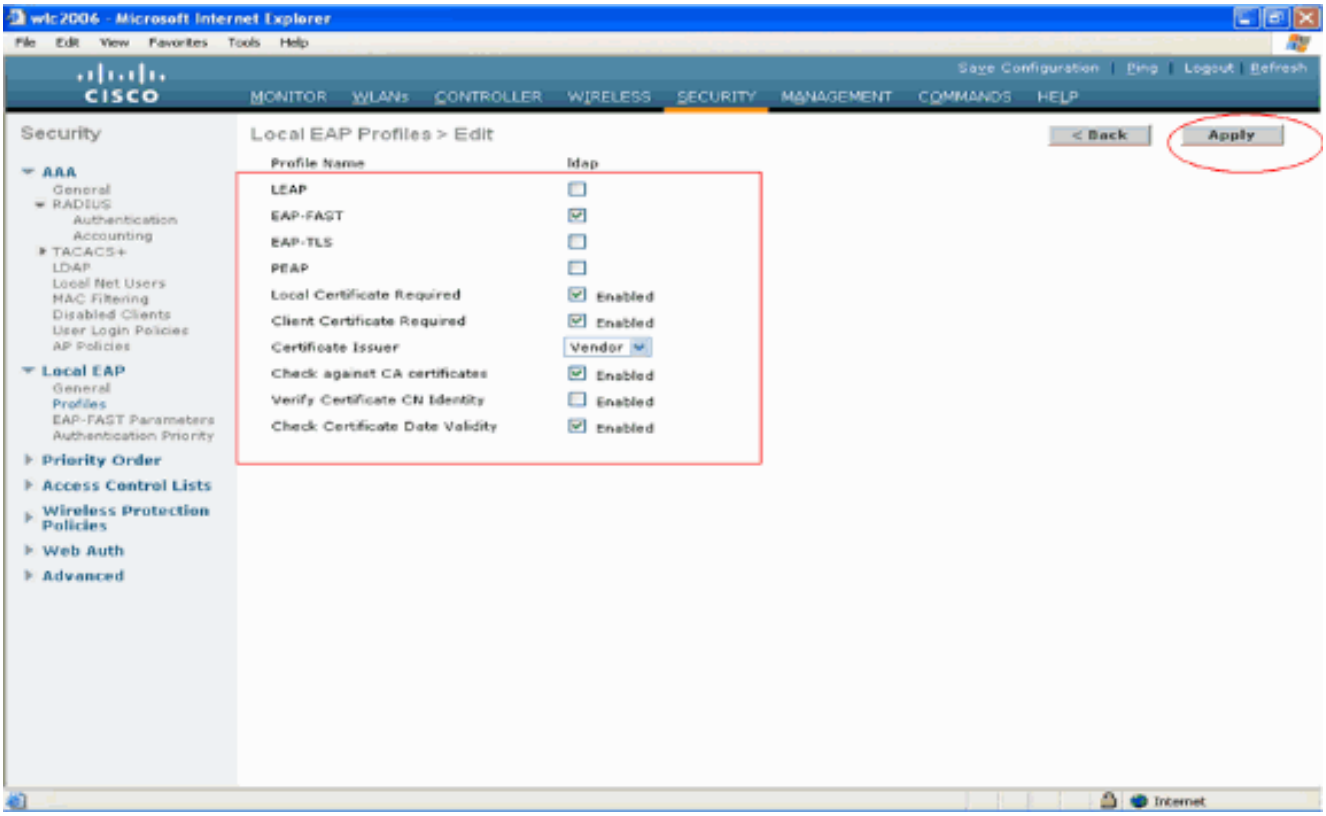
3. انقر على **جديد** لإنشاء توصيف EAP محلي جديد.
4. قم بتكوين اسم لملف التعريف هذا وانقر على **تطبيق**. في هذا المثال، اسم ملف التعريف هو **ldap**. ينقلك ذلك إلى توصيفات EAP المحلية التي تنشأ على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).



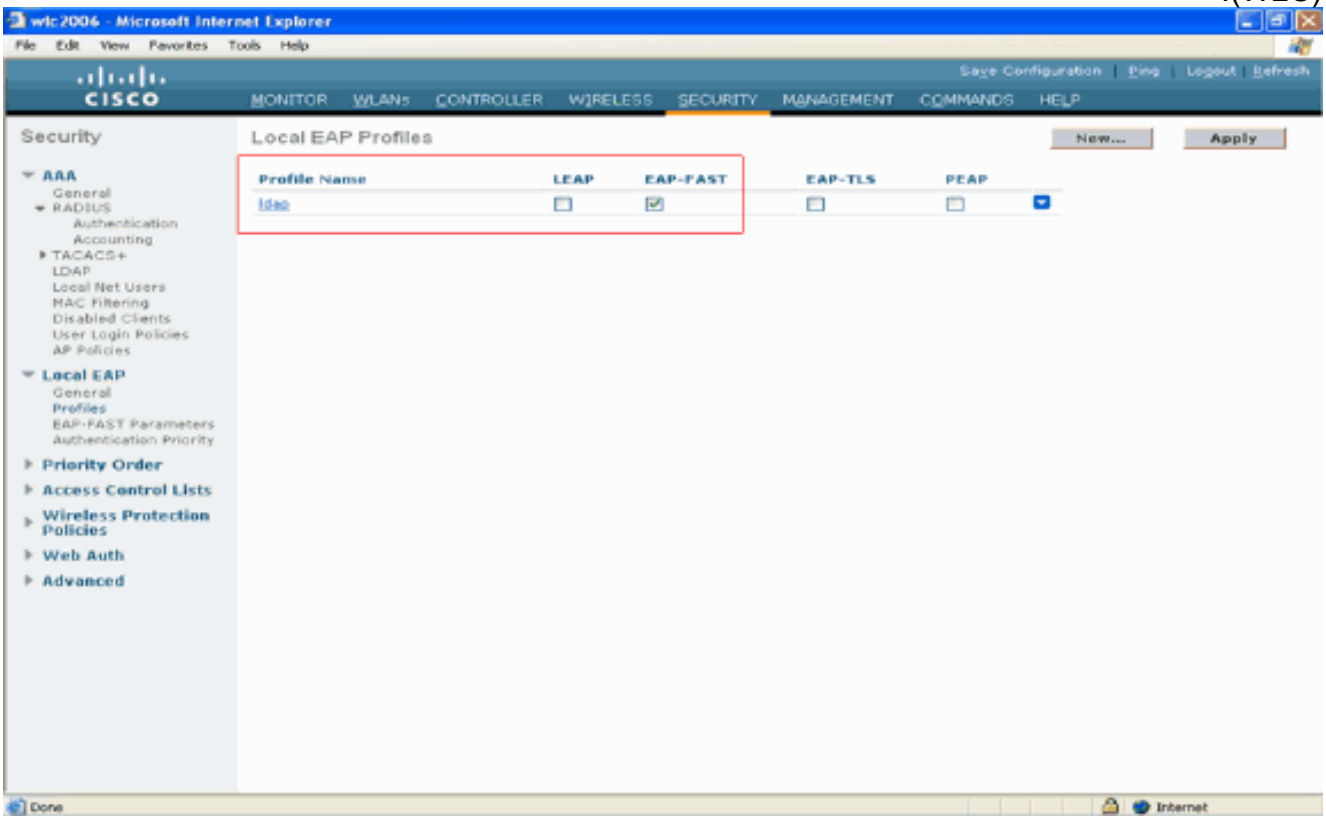
5. انقر على ملف تخصيص **ldap** الذي تم إنشاؤه للتو والذي يظهر تحت حقل اسم ملف التخصيص في صفحة ملفات تعريف EAP المحلية. ينقلك هذا إلى **توصيفات EAP المحلية > تحرير** الصفحة.



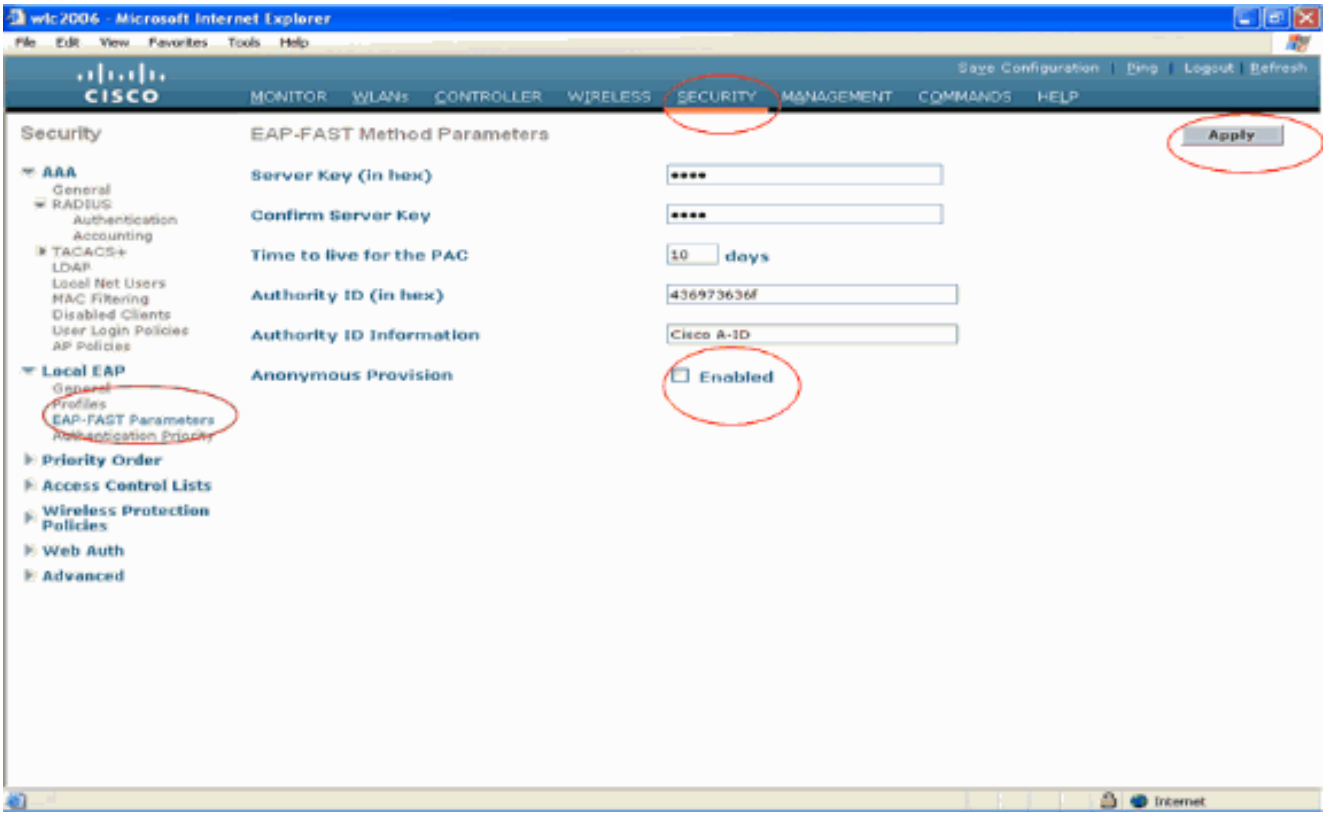
6. قم بتكوين المعلمات الخاصة بهذا التوصيف على **توصيفات EAP المحلية > تحرير** الصفحة.أختر **EAP-FAST** كأسلوب مصادقة EAP المحلي.تمكين خانات الاختيار المجاورة **للشهادة المحلية المطلوبة** و**شهادة العميل المطلوبة**.أختر **بائع** كمصدر شهادات لأن هذا المستند يستخدم خادم CA لجهة خارجية.قم بتمكين خانة الاختيار المجاورة **للتدقيق مقابل شهادات CA** للسماح بالتحقق من صحة الشهادة الواردة من العميل مقابل شهادات CA الموجودة على وحدة التحكم.إذا كنت تريد التحقق من صحة الاسم الشائع (CN) في الشهادة الواردة مقابل CA Certificates's CN على وحدة التحكم، فتحقق من خانة الاختيار **Verify Certificate CN Identity**. الإعداد الافتراضي معطل. للسماح لوحدة التحكم بالتحقق من أن شهادة الجهاز الوارد لا تزال صالحة ولم تنتهي صلاحيتها، تحقق من خانة الاختيار **التحقق من صحة تاريخ الشهادة**.**ملاحظة:** يتم التحقق من صحة تاريخ الشهادة مقابل وقت (GMT) UTC الحالي الذي تم تكوينه على وحدة التحكم. يتم تجاهل إزاحة المنطقة الزمنية.طقطقة **يطبق**.



7. ينشأ الآن توصيف EAP المحلي بمصادقة EAP-FAST على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).



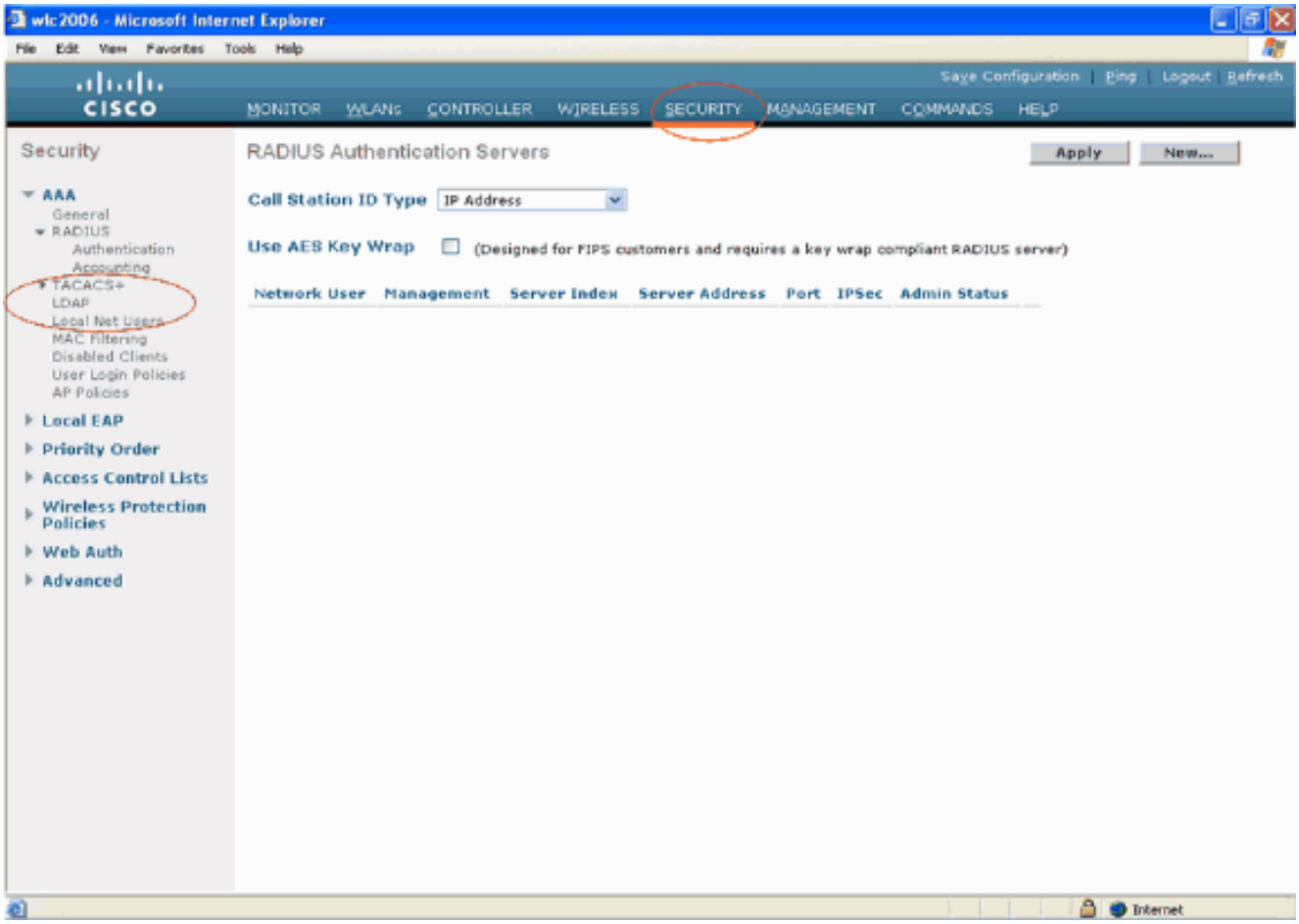
8. تتمثل الخطوة التالية في تكوين معلمات EAP-FAST المحددة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). في صفحة أمان WLC، انقر **EAP المحلي > معلمات EAP-FAST** للانتقال إلى صفحة معلمات أسلوب EAP-FAST.قم بإلغاء تحديد خانة الاختيار **تزويد مجهول** لأن هذا المثال يشرح EAP-FAST باستخدام الشهادات. أترك كافة المعلمات الأخرى عند إعداداتها الافتراضية. طقطقة **يطبق**.



تكوين WLC مع تفاصيل خادم LDAP

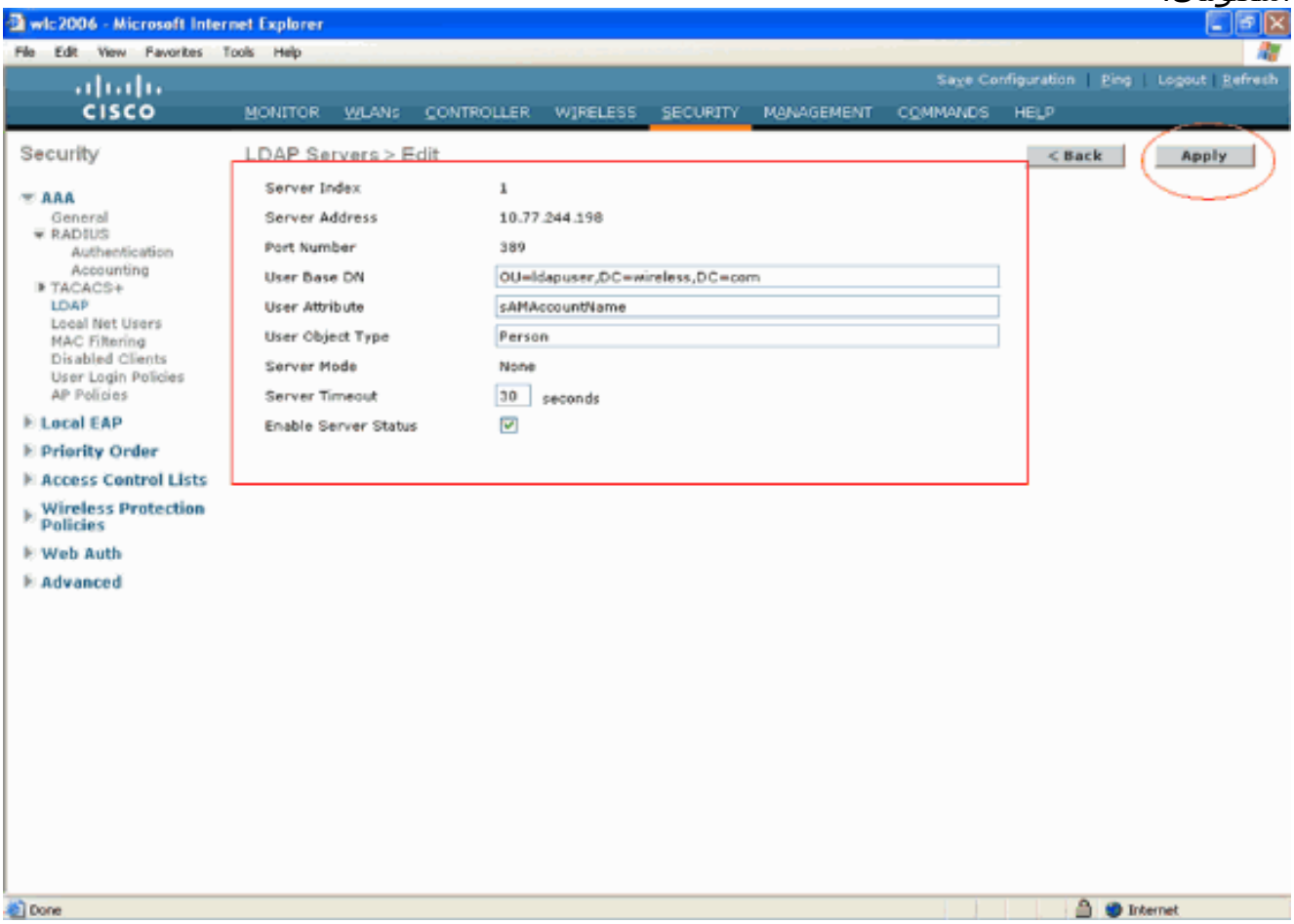
الآن بعد تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام ملف تعريف EAP المحلي والمعلومات ذات الصلة، فإن الخطوة التالية هي تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مع تفاصيل خادم LDAP. أتمت هذا steps على ال WLC:

1. في صفحة **الأمان** الخاصة بعنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، حدد **AAA > LDAP** من جزء المهام الموجود على الجانب الأيسر للنقل إلى صفحة تكوين خادم LDAP. لإضافة خادم LDAP، انقر فوق **جديد**. تظهر الصفحة **خوادم LDAP > جديد**.



2. في صفحة تحرير خوادم LDAP، حدد تفاصيل خادم LDAP مثل عنوان IP الخاص بخادم LDAP، ورقم المنفذ، وتمكين حالة الخادم وهكذا.أختر رقما من المربع المنسدل **لفهرس الخادم (الأولوية)** لتحديد ترتيب أولوية هذا الخادم فيما يتعلق بأي خوادم LDAP تم تكوينها أخرى. يمكنك تكوين ما يصل إلى سبعة عشر خادما. إذا تعذر على وحدة التحكم الوصول إلى الخادم الأول، فستحاول إستخدام الخادم الثاني في القائمة وما إلى ذلك.دخلت العنوان من ال LDAP نادل في **الخادم عنوان** مجال.أدخل رقم منفذ TCP الخاص بخادم LDAP في حقل **رقم المنفذ**. النطاق الصالح هو من 1 إلى 65535، والقيمة الافتراضية هي **389**.في حقل **قاعدة المستخدم DN**، أدخل الاسم المميز (DN) للشجرة الفرعية في خادم LDAP الذي يحتوي على قائمة بجميع المستخدمين. على سبيل المثال، أنت=وحدة تنظيمية، .ou=الوحدة التنظيمية التالية، و o=corporation.com. إذا كانت الشجرة التي تحتوي على مستخدمين هي DN الأساسي، فأدخل o=corporation.com أو dc=corporation، dc=com.في هذا المثال، يوجد المستخدم ضمن **مستخدم الحد الأدنى** (OU) للوحدة التنظيمية الذي يتم إنشاؤه بدوره كجزء من مجال **Wireless.com**.يجب أن يشير DN الخاص بقاعدة المستخدم إلى المسار الكامل حيث توجد معلومات المستخدم (بيانات اعتماد المستخدم طبقا لأسلوب مصادقة EAP-FAST). في هذا المثال، يوجد المستخدم ضمن OU=ldapuser DN الأساسي، DC=COM، DC=Wireless.يتم شرح المزيد من التفاصيل حول OU، بالإضافة إلى تكوين المستخدم، في قسم إنشاء مستخدمين في وحدة التحكم بالمجال في هذا المستند.في حقل **سمة المستخدم**، أدخل اسم السمة في سجل المستخدم الذي يحتوي على اسم المستخدم.في حقل **نوع كائن المستخدم**، أدخل قيمة سمة كائنType ل LDAP التي تعرف السجل كمستخدم. غالبا ما يكون لسجلات المستخدم عدة قيم للسمة objectType، بعضها فريد للمستخدم وبعضها مشترك مع أنواع كائن أخرى.**ملاحظة:** يمكنك الحصول على قيمة هذين الحقلين من خادم الدليل الخاص بك باستخدام الأداة المساعدة مستعرض LDAP، والتي تأتي كجزء من أدوات دعم Windows 2003. **تسمى أداة مستعرض Microsoft LDAP هذه LDP.** بمساعدة هذه الأداة، يمكنك التعرف على الحقول DN الخاصة بقاعدة المستخدم وسمة المستخدم ونوع كائن المستخدم لهذا المستخدم المعين. وتتم مناقشة المعلومات التفصيلية حول إستخدام LDP لمعرفة سمات المستخدم المحددة هذه في قسم إستخدام LDP لتحديد سمات المستخدم في هذا المستند.أختر **Secure** من المربع المنسدل لوضع الخادم إذا كنت تريد أن تستخدم جميع حركات LDAP نفق TLS آمن. وإلا، أختر **بلا**، وهو الإعداد الافتراضي.في حقل **مهلة الخادم**، أدخل عدد الثواني بين عمليات إعادة الإرسال. النطاق الصحيح هو من 2 إلى 30 ثانية، والقيمة الافتراضية هي 2 ثانية.حدد خانة الاختيار **تمكين حالة الخادم** لتمكين خادم LDAP هذا، أو قم بإلغاء تحديده لتعطيله. تم تعطيل القيمة الافتراضية.انقر فوق

تطبيق لتنفيذ التغييرات.فيما يلي مثال تم تكوينه بالفعل باستخدام هذه المعلومات:

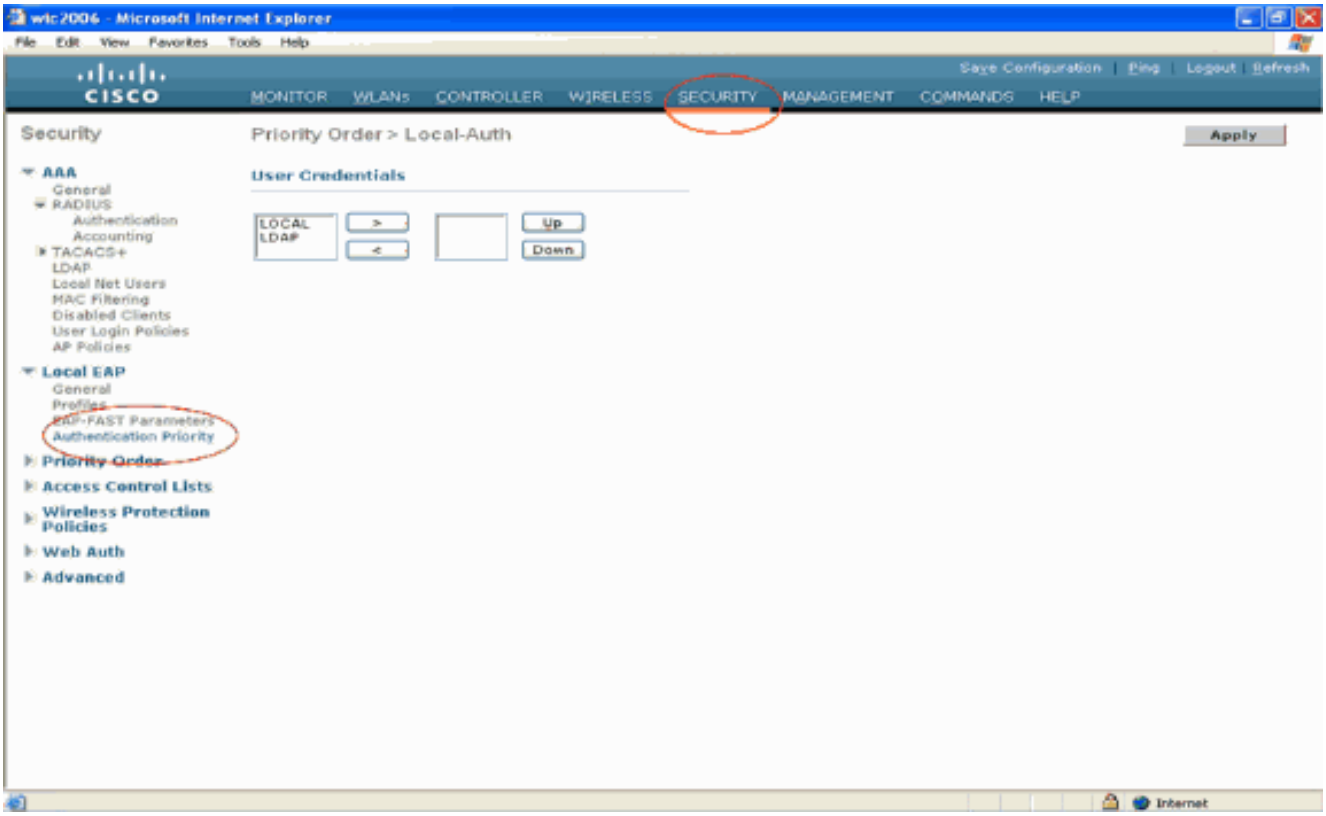


الآن بعد تكوين تفاصيل حول خادم LDAP على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فإن الخطوة التالية هي تكوين LDAP كقاعدة بيانات خلفية ذات أولوية حتى تبحث عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) أولا عن قاعدة بيانات LDAP لبيانات اعتماد المستخدم بدلا من أي قواعد بيانات أخرى.

تكوين LDAP كقاعدة بيانات خلفية ذات أولوية

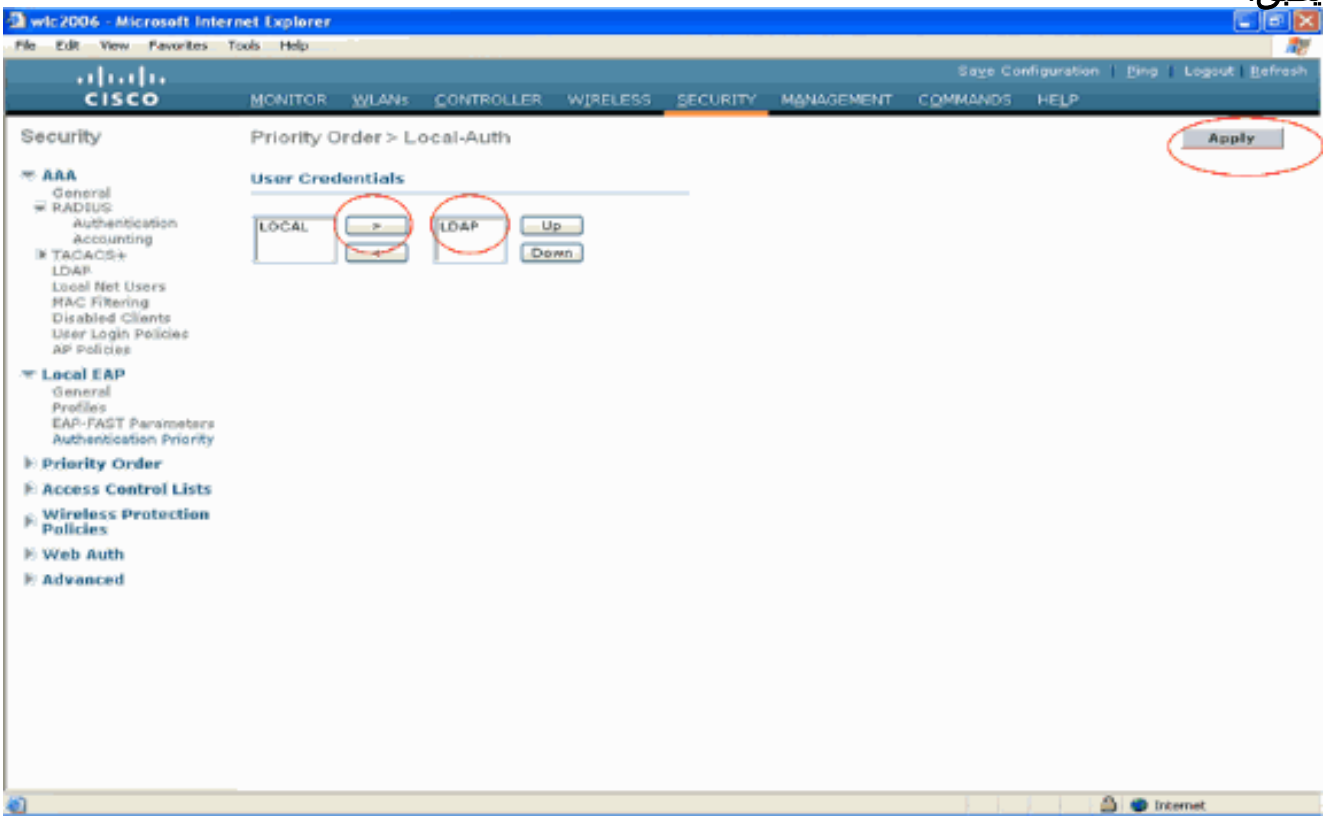
أتمت هذا steps على الـ WLC in order to شكلت LDAP كأولوية خلفي قاعدة معطيات:

1. في صفحة التأمين انقر على **EAP المحلي > أولوية المصادقة**. في صفحة ترتيب الأولوية > المصادقة المحلية، يمكنك العثور على قاعدتي بيانات (محليتين و LDAP) يمكنهما تخزين بيانات اعتماد المستخدم.لتجعل LDAP قاعدة بيانات أولوية، أختر **LDAP** من مربع بيانات اعتماد المستخدم الموجود على الجانب الأيسر وانقر فوق > زر لنقل LDAP إلى مربع ترتيب الأولوية الموجود على الجانب الأيمن.



2. يوضح هذا المثال بوضوح أنه يتم إختيار LDAP على المربع الأيسر ويتم تحديد الزر >. ونتيجة لذلك، ينقل LDAP إلى المربع الموجود على الجانب الأيمن الذي يقرر الأولوية. يتم إختيار قاعدة بيانات LDAP كقاعدة بيانات أولوية المصادقة.طقطقة

يطبق.

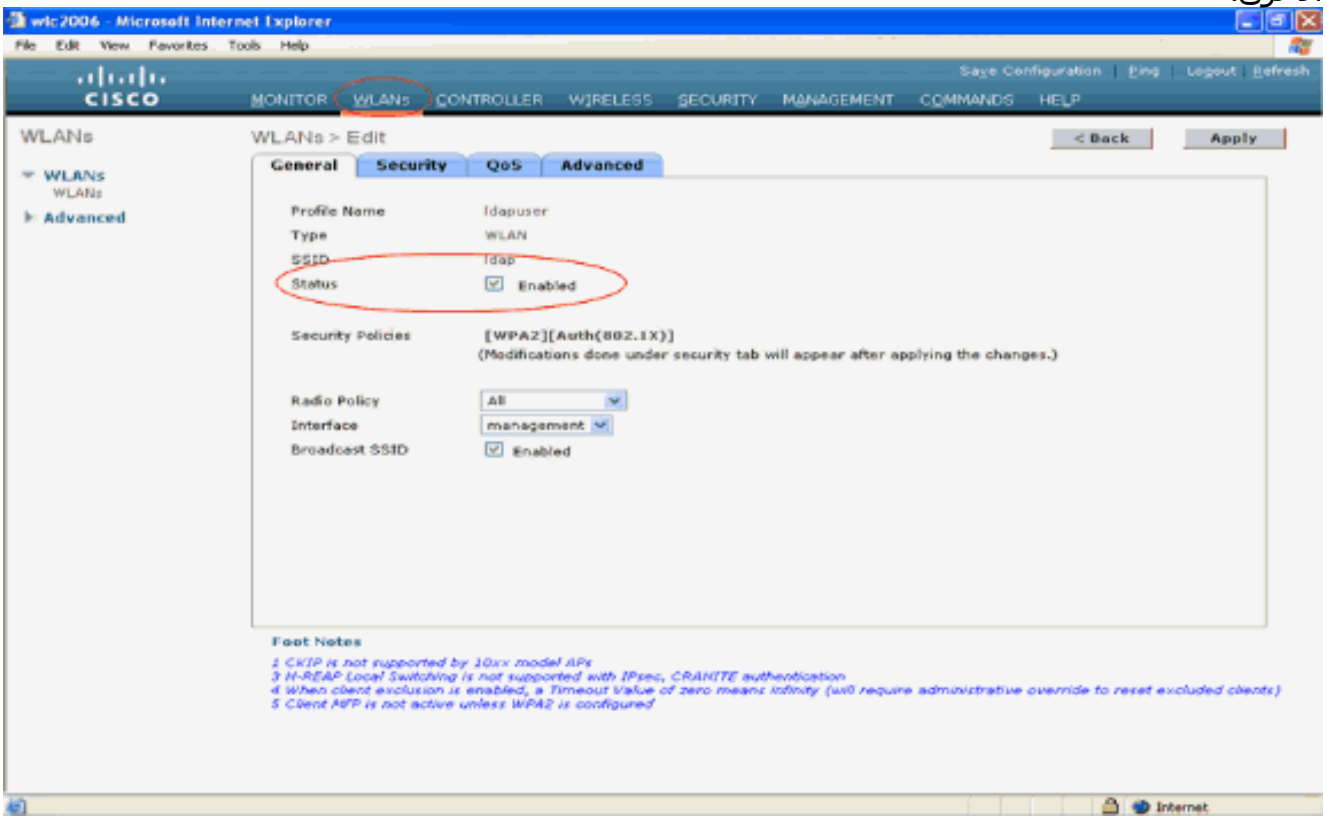


ملاحظة: إذا ظهر كل من LDAP و LOCAL في مربع مسوغات المستخدم الأيمن مع LDAP في الأعلى والمحلي في الأسفل، يحاول EAP المحلي مصادقة العملاء باستخدام قاعدة بيانات الطرف الخلفي LDAP ويفشل في الوصول إلى قاعدة بيانات المستخدم المحلي إذا لم تكن خوادم LDAP قابلة للوصول. في حالة عدم العثور على المستخدم، يتم رفض محاولة المصادقة. إذا كان EAP المحلي في الأعلى يحاول المصادقة باستخدام قاعدة بيانات المستخدم المحلي فقط. لا يفشل إلى قاعدة بيانات LDAP الخلفية.

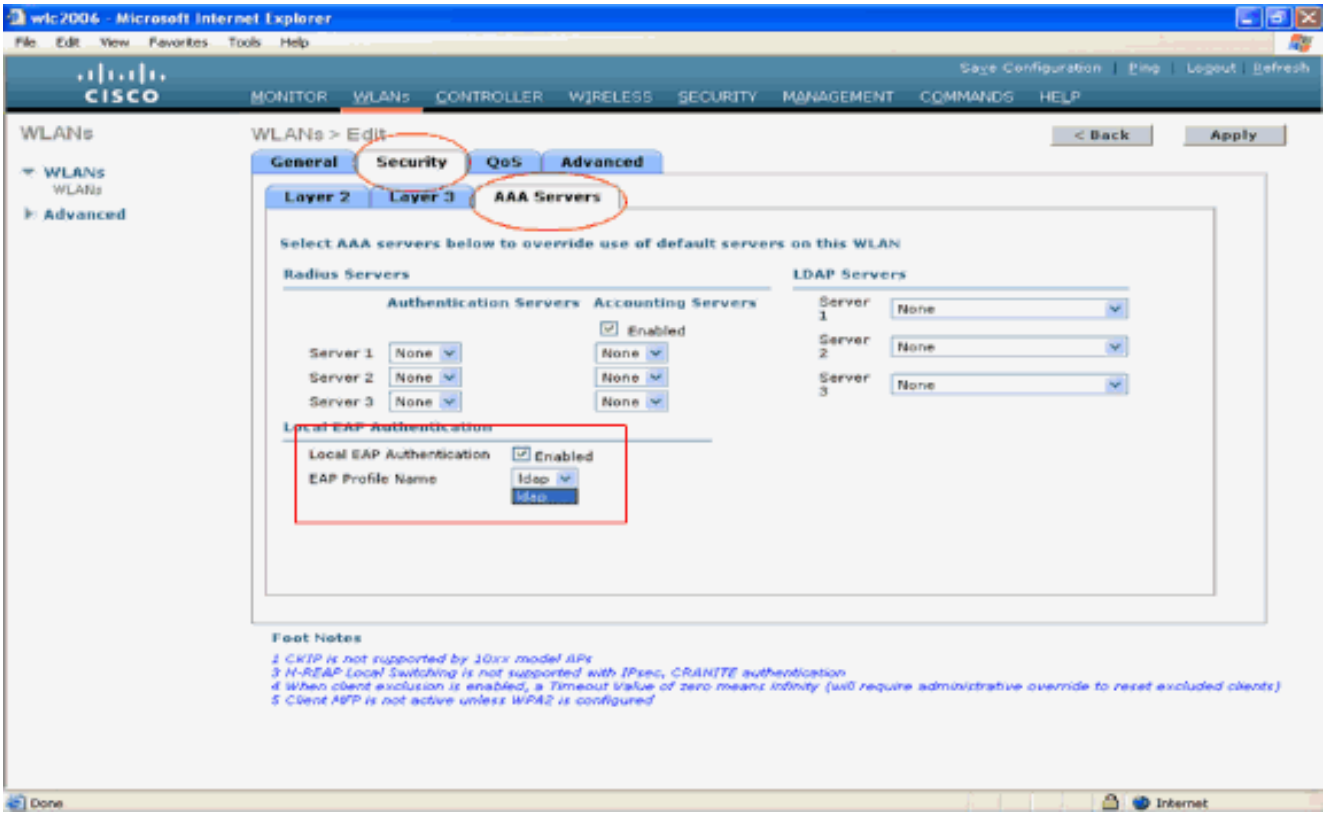
تكوين WLAN على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام مصادقة EAP المحلية

تتمثل الخطوة الأخيرة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في تكوين شبكة WLAN تستخدم EAP المحلي كطريقة مصادقة لها مع LDAP كقاعدة بيانات طرفية خلفية لها. قم بإجراء هذه الخطوات:

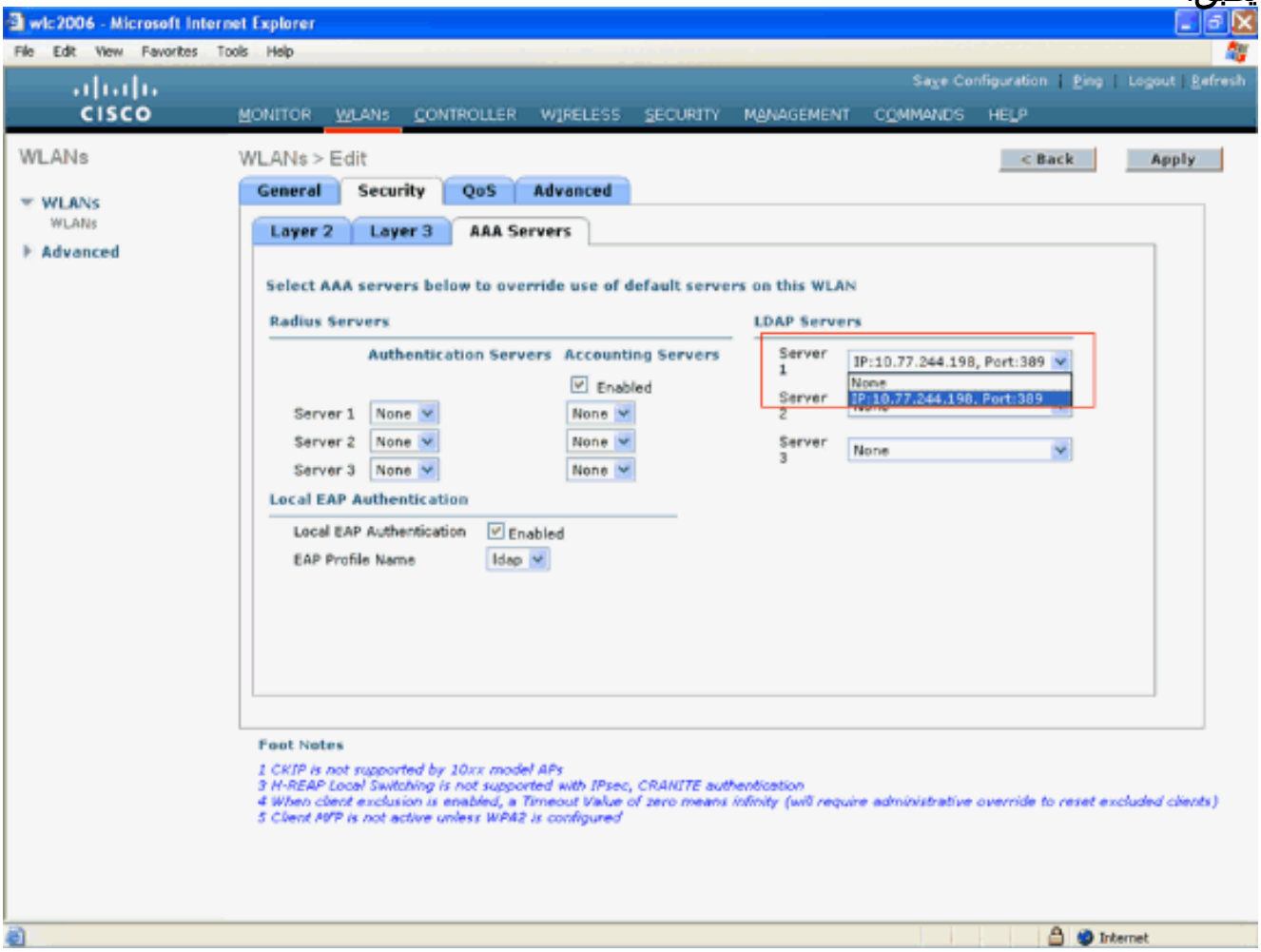
1. من القائمة الرئيسية لوحدة التحكم، انقر فوق **شبكات WLAN** للنقل إلى صفحة تكوين شبكات WLAN. في صفحة شبكات WLAN، انقر فوق **جديد** لإنشاء شبكة WLAN جديدة. يقوم هذا المثال بإنشاء **LDAP** جديد لشبكة WLAN.طقطقة **يطبق** الخطوة تالي أن يشكل ال WLAN معلم في ال WLANs > تحرير صفحة .
2. في صفحة تحرير شبكة WLAN، قم بتمكين حالة شبكة WLAN هذه. قم بتكوين كافة المعلمات الضرورية الأخرى.



3. انقر فوق **الأمان** لتكوين المعلمات ذات الصلة بالأمان لشبكة WLAN هذه. يستخدم هذا المثال تأمين الطبقة 2 على هيئة 802.1x مع 104 بت WEP ديناميكي.**ملاحظة:** يستخدم هذا المستند 802.1x مع WEP الديناميكي كمثال. يوصى باستخدام أساليب مصادقة أكثر أمانا، مثل WPA2 /WPA.
4. في صفحة تكوين أمان شبكة WLAN، انقر فوق علامة التبويب **خوادم AAA**. في صفحة خوادم AAA، قم بتمكين أسلوب مصادقة EAP المحلي واختر **ldap** من المربع المنسدل الذي يتوافق مع معلمة اسم ملف تعريف EAP. هذا هو ملف تعريف EAP المحلي الذي تم إنشاؤه في هذا المثال.

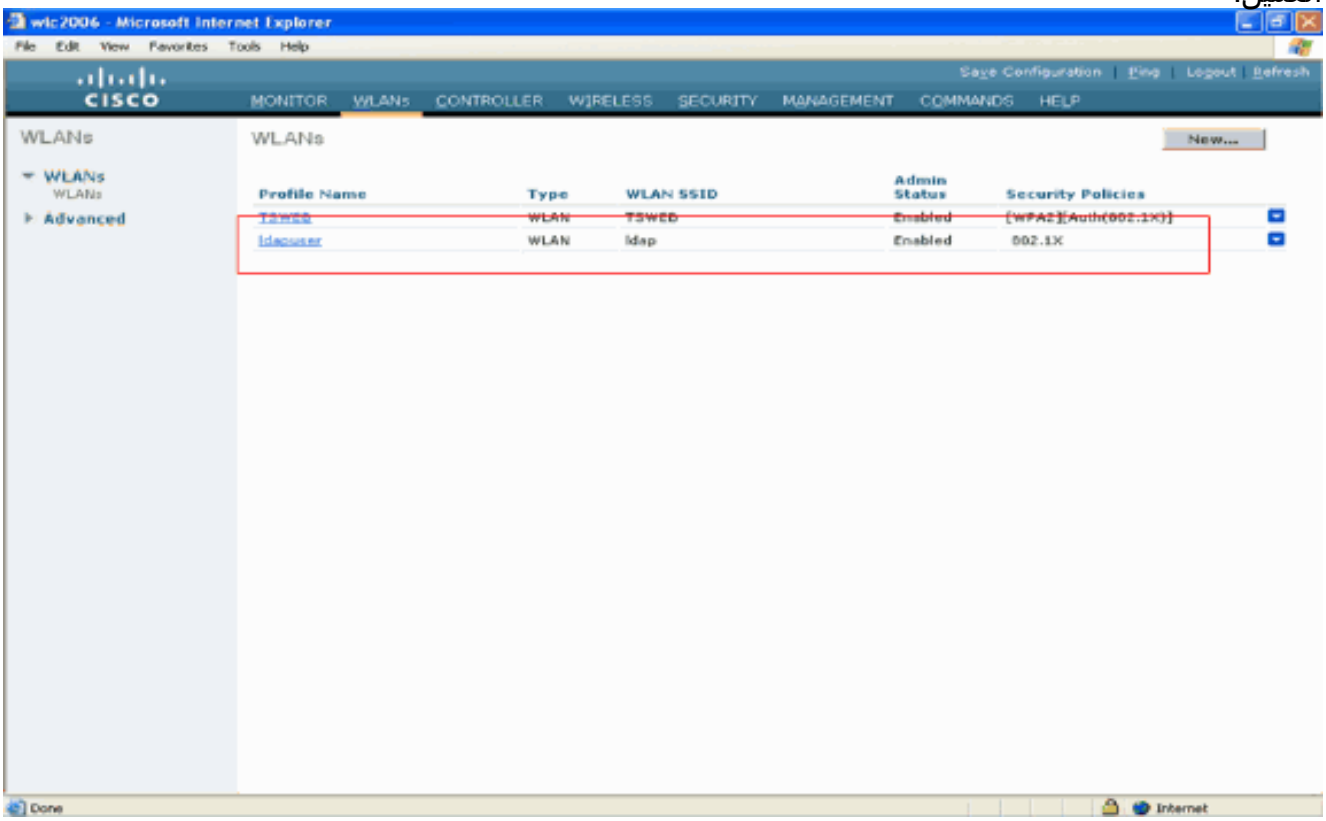


5. أختر خادم LDAP (الذي تم تكوينه مسبقا على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)) من المربع المنسدل . تأكد من إمكانية الوصول إلى خادم LDAP من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).طقطقة
يطبق.



6. تم تكوين WLAN الجديد على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تصادق شبكة WLAN هذه

العملاء بمصادقة EAP المحلية (EAP-FAST في هذه الحالة) وتستعلم عن قاعدة بيانات خلفية LDAP للتحقق من صحة بيانات اعتماد
العميل.



تكوين خادم LDAP

الآن وقد تم تكوين EAP المحلي على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فإن الخطوة التالية هي تكوين خادم LDAP الذي يعمل كقاعدة بيانات خلفية لمصادقة العملاء اللاسلكيين عند التحقق من صحة الشهادة بنجاح.

الخطوة الأولى في تكوين خادم LDAP هي إنشاء قاعدة بيانات مستخدم على خادم LDAP حتى يمكن ل WLC الاستعلام عن قاعدة البيانات هذه لمصادقة المستخدم.

إنشاء مستخدمين على وحدة التحكم بالمجال

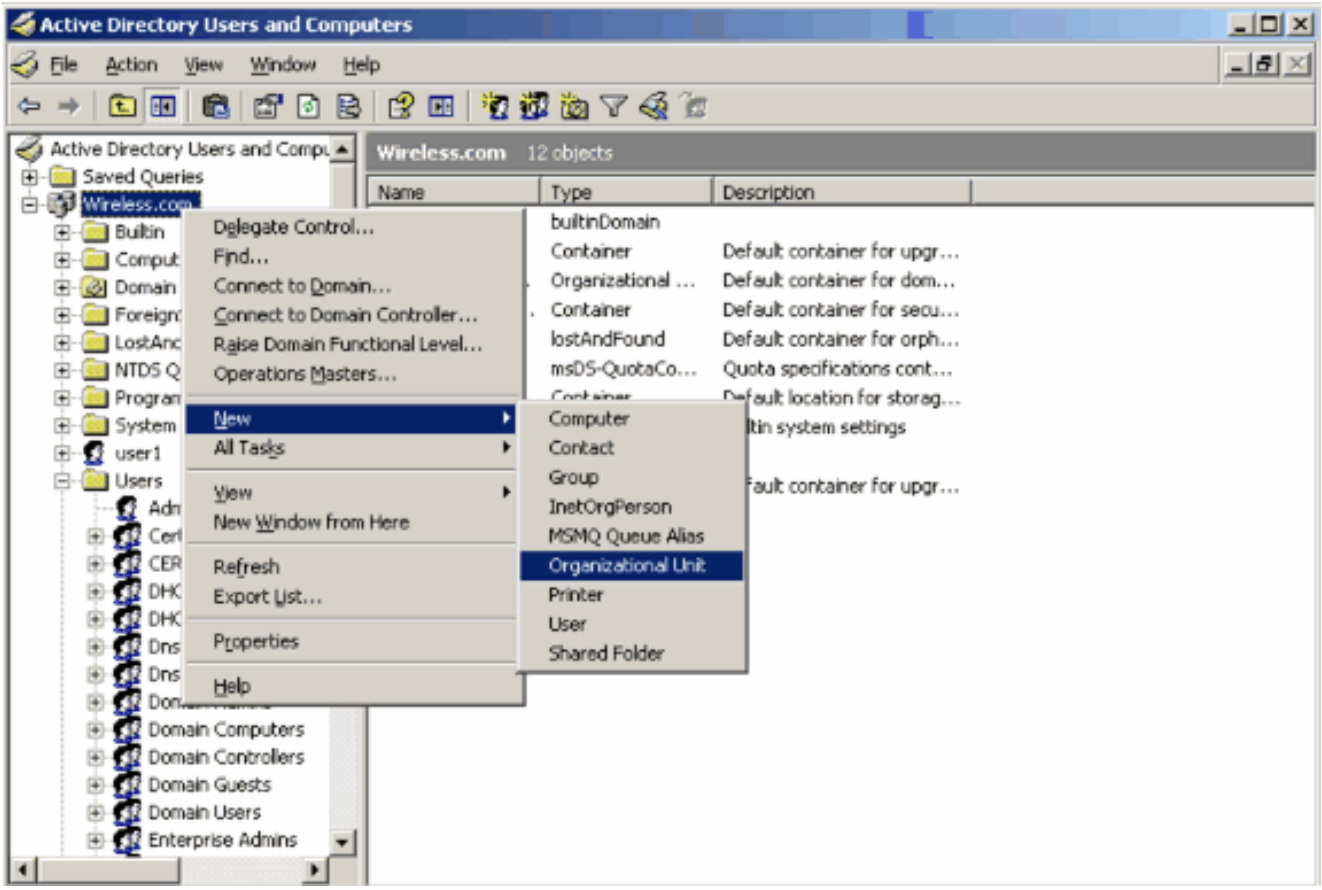
في هذا مثال، خلقت جديد **ldapuser** OU و المستعمل **user2** يكون تحت هذا OU. من خلال تكوين هذا المستخدم للوصول إلى LDAP، يمكن ل WLC الاستعلام عن قاعدة بيانات LDAP هذه لمصادقة المستخدم.

المجال المستخدم في هذا المثال هو **wireless.com**.

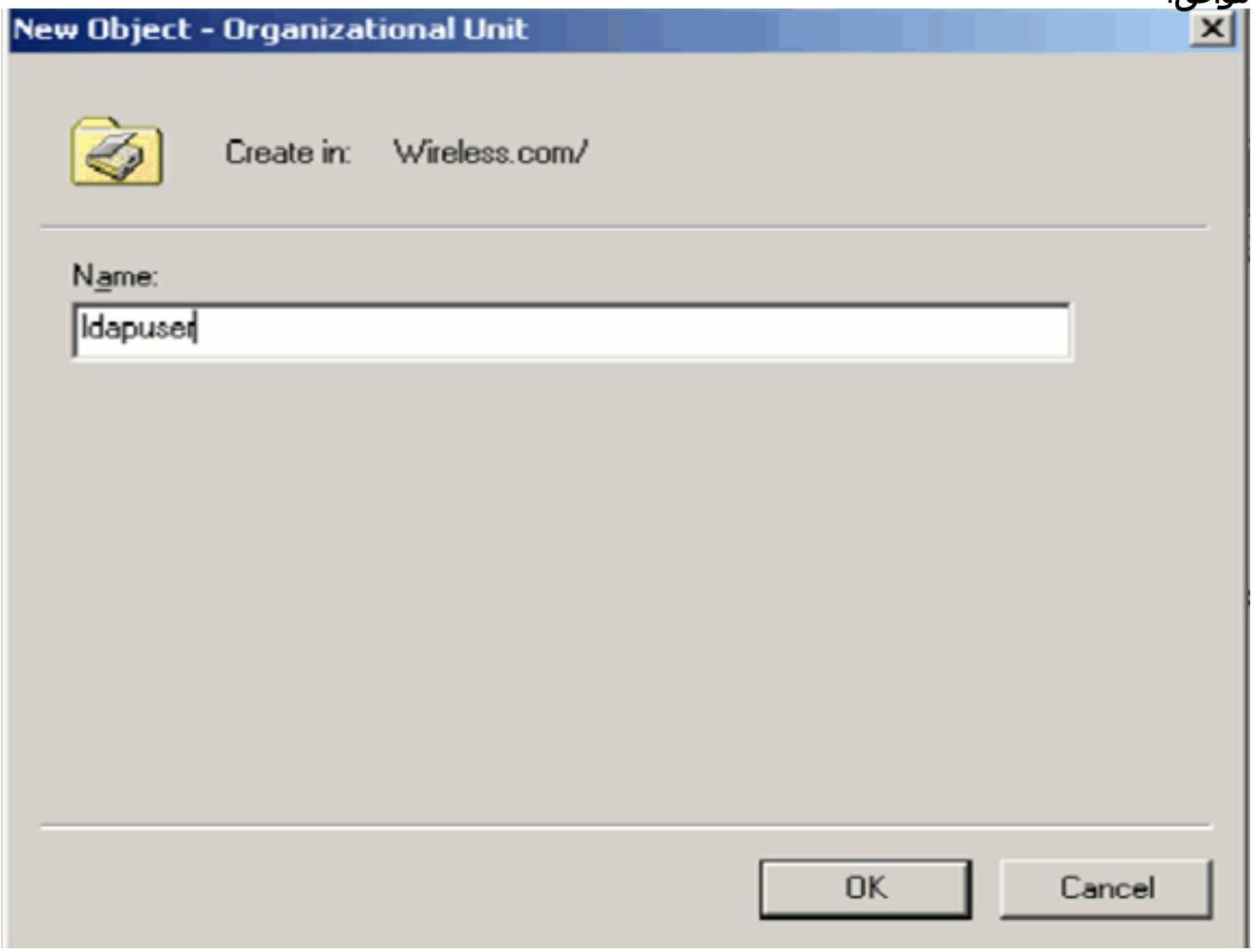
إنشاء قاعدة بيانات مستخدم تحت OU

يشرح هذا القسم كيفية إنشاء OU جديد في مجالك وإنشاء مستخدم جديد على OU هذا.

1. في وحدة التحكم بالمجال، انقر فوق **بدء > برامج > أدوات إدارية > مستخدمي Active Directory وأجهزة الكمبيوتر** لتشغيل وحدة التحكم في إدارة **مستخدمي Active Directory وأجهزة الكمبيوتر**.
2. انقر بزر الماوس الأيمن فوق اسم المجال الخاص بك (wireless.com، في هذا المثال)، ثم حدد **جديد > وحدة تنظيمية** من قائمة السياق لإنشاء قيمة
جديدة.

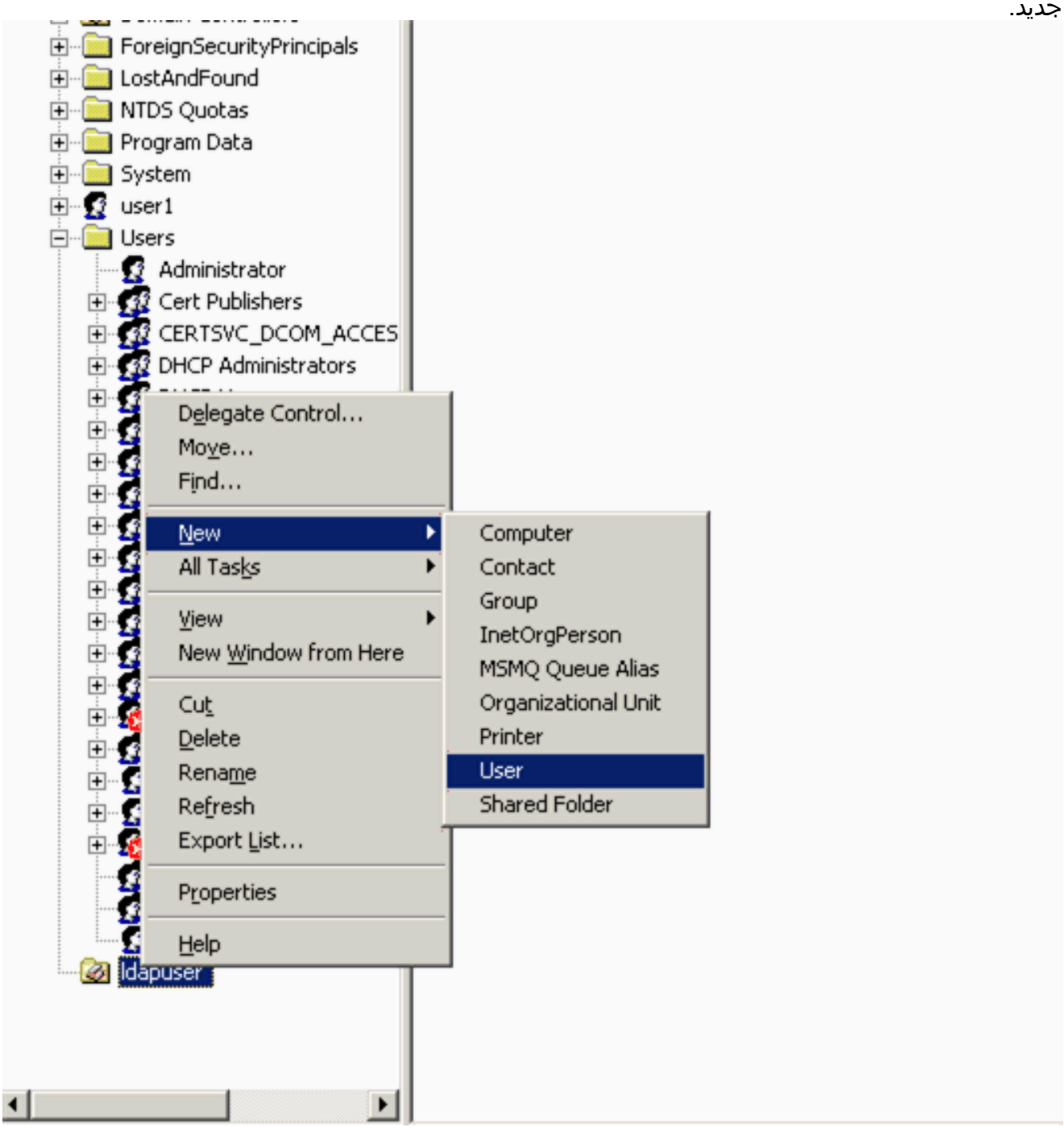


3. قم بتعيين اسم لهذه الوحدة الخاصة بك وانقر فوق **موافق**.

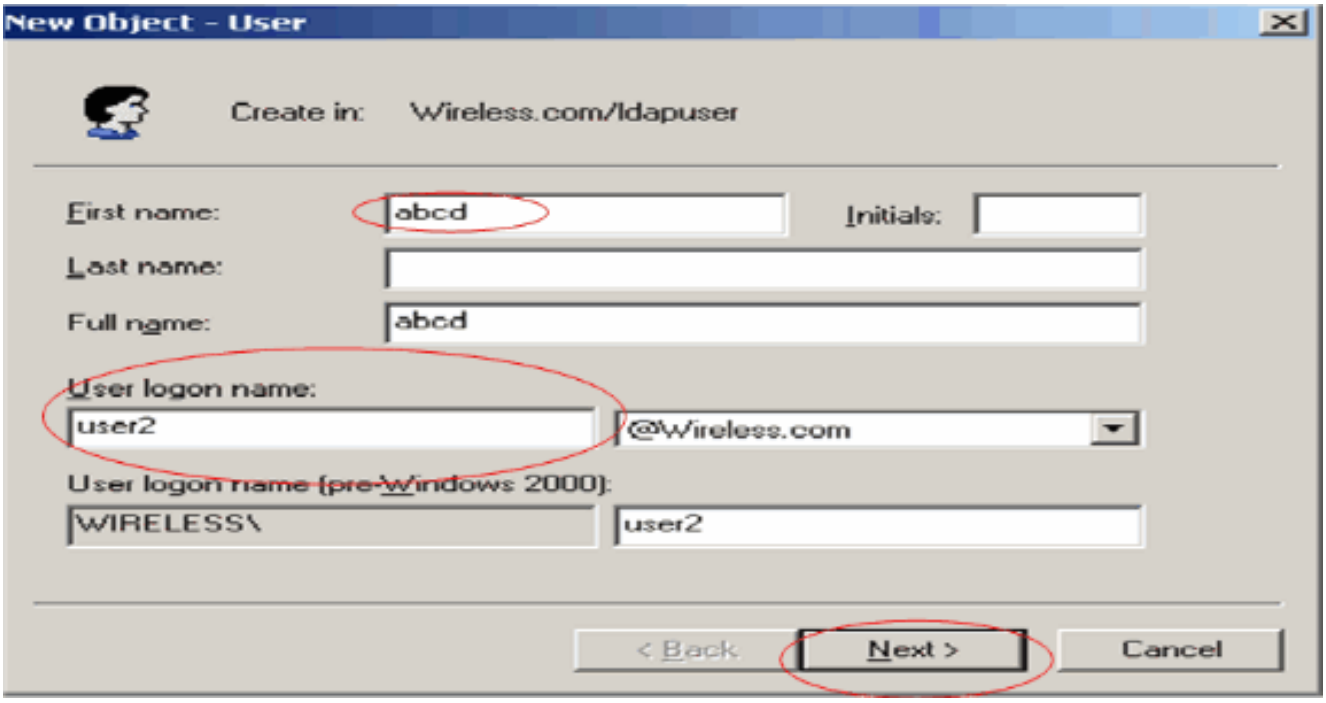


الآن يتم إنشاء **ldapuser** OU الجديد على خادم LDAP، الخطوة التالية هي إنشاء مستخدم **user2** ضمن هذه OU. ومن أجل تحقيق ذلك، أكمل الخطوات التالية:

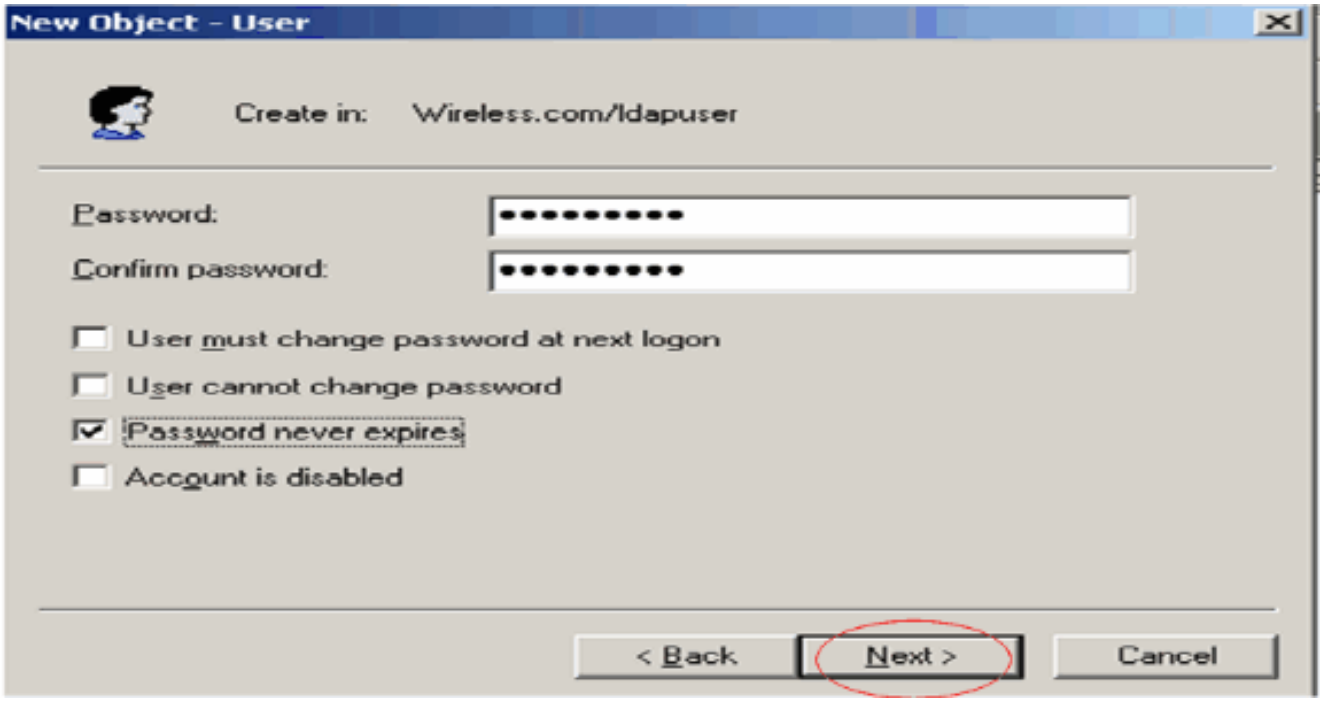
1. انقر بزر الماوس الأيمن فوق ما تم إنشاؤه حديثا. حدد **جديد > مستخدم** من قوائم السياق الناتجة لإنشاء مستخدم
جديد.



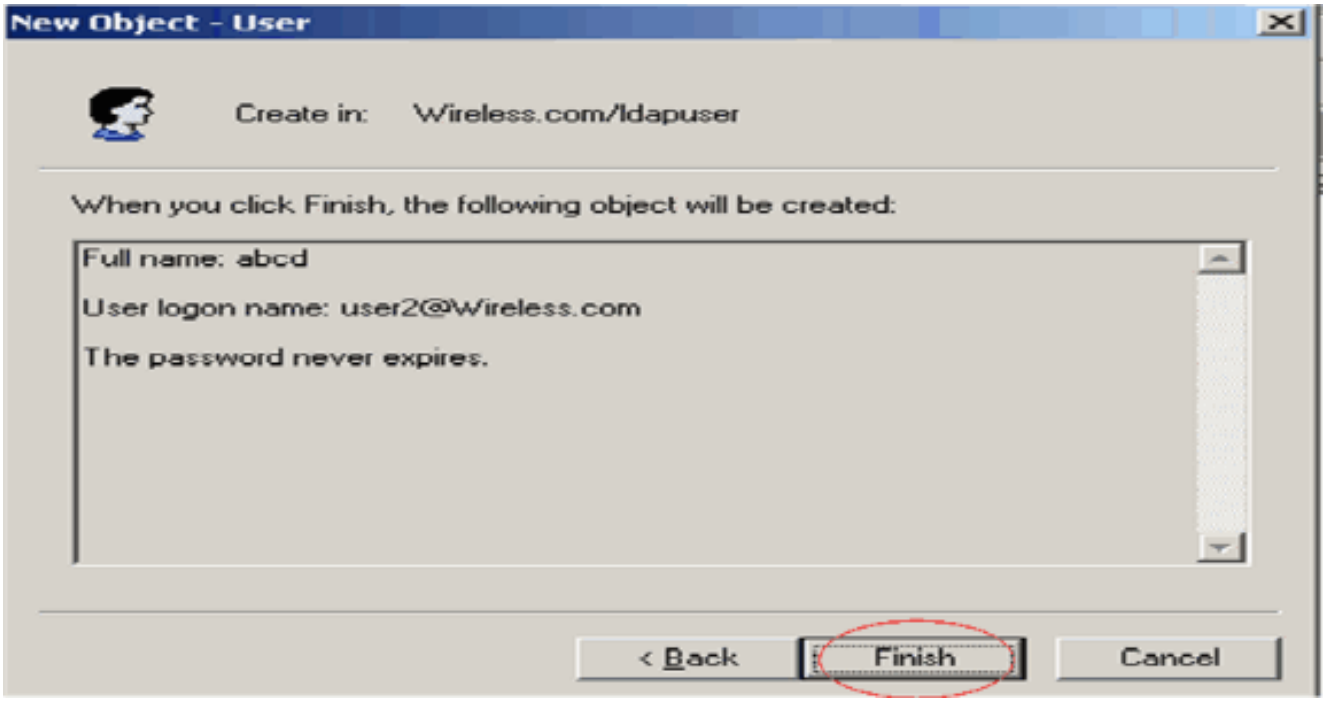
2. في صفحة إعداد المستخدم، قم بتعبئة الحقول المطلوبة كما هو موضح في هذا المثال. يتضمن هذا المثال **user2** كاسم تسجيل دخول المستخدم.هذا هو اسم المستخدم الذي سيتم التحقق منه في قاعدة بيانات LDAP لمصادقة العميل. يستخدم هذا المثال **كاسم** أول واسم العائلة. انقر فوق **Next (التالي)**.



3. أدخل كلمة مرور وقم بتأكيد كلمة المرور. أخترت **الكلمة أبدا تنتهي** خيار وطقطقة **بعد ذلك**.



4. انقر فوق إنهاء.يتم إنشاء مستخدم جديد **user2** ضمن **ldapuser** OU. مسوغات المستخدم هي:اسم المستخدم: **user2**كلمة المرور: **الكمبيوتر المحمول 123**



الآن بعد إنشاء المستخدم تحت OU، فإن الخطوة التالية هي تكوين هذا المستخدم للوصول إلى LDAP.

تكوين المستخدم للوصول إلى LDAP

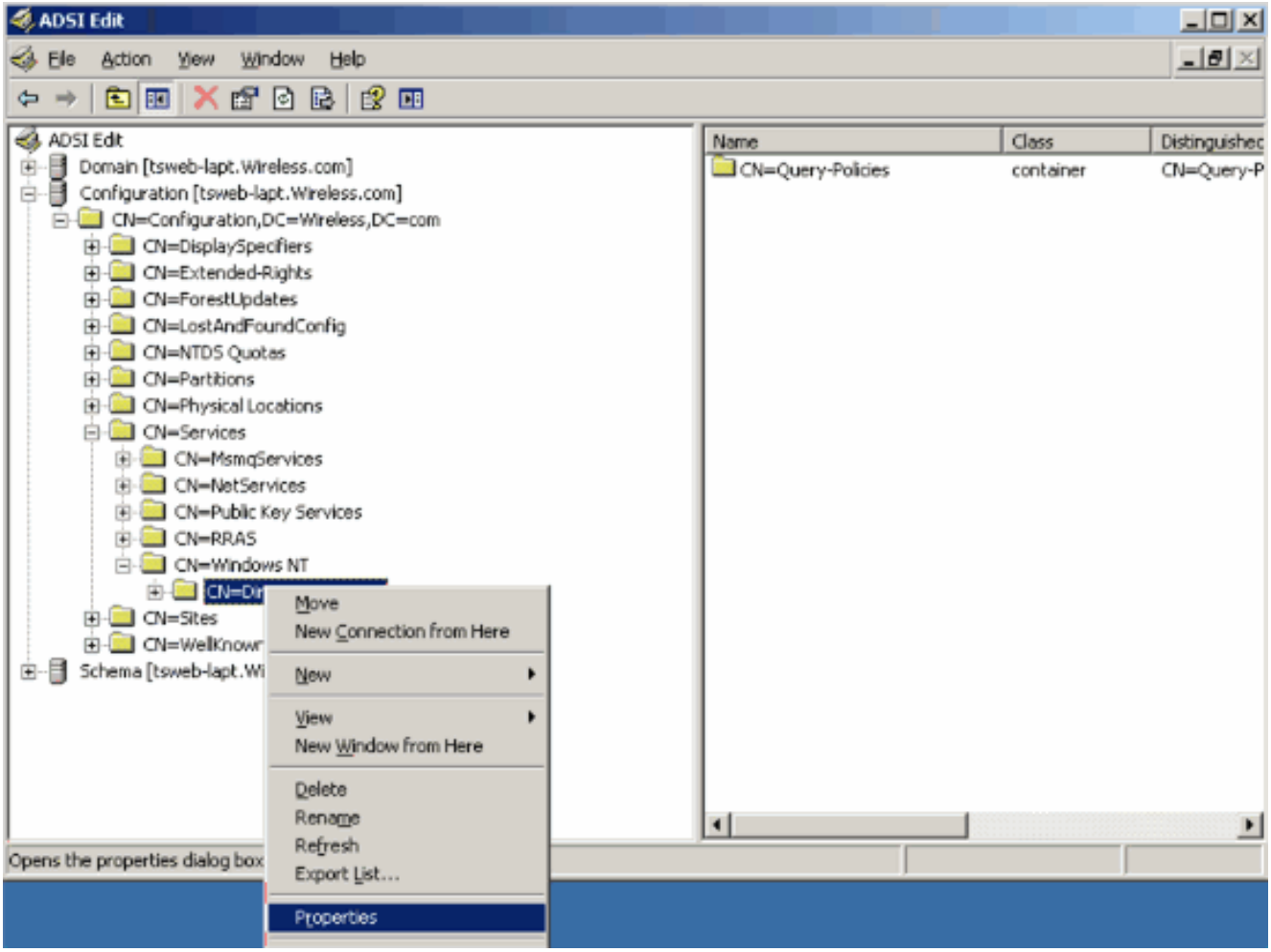
أنجزت ال steps في هذا قسم in order to شكلت مستعمل ل LDAP منفذ.

تمكين ميزة الربط المجهول على خادم Windows 2003

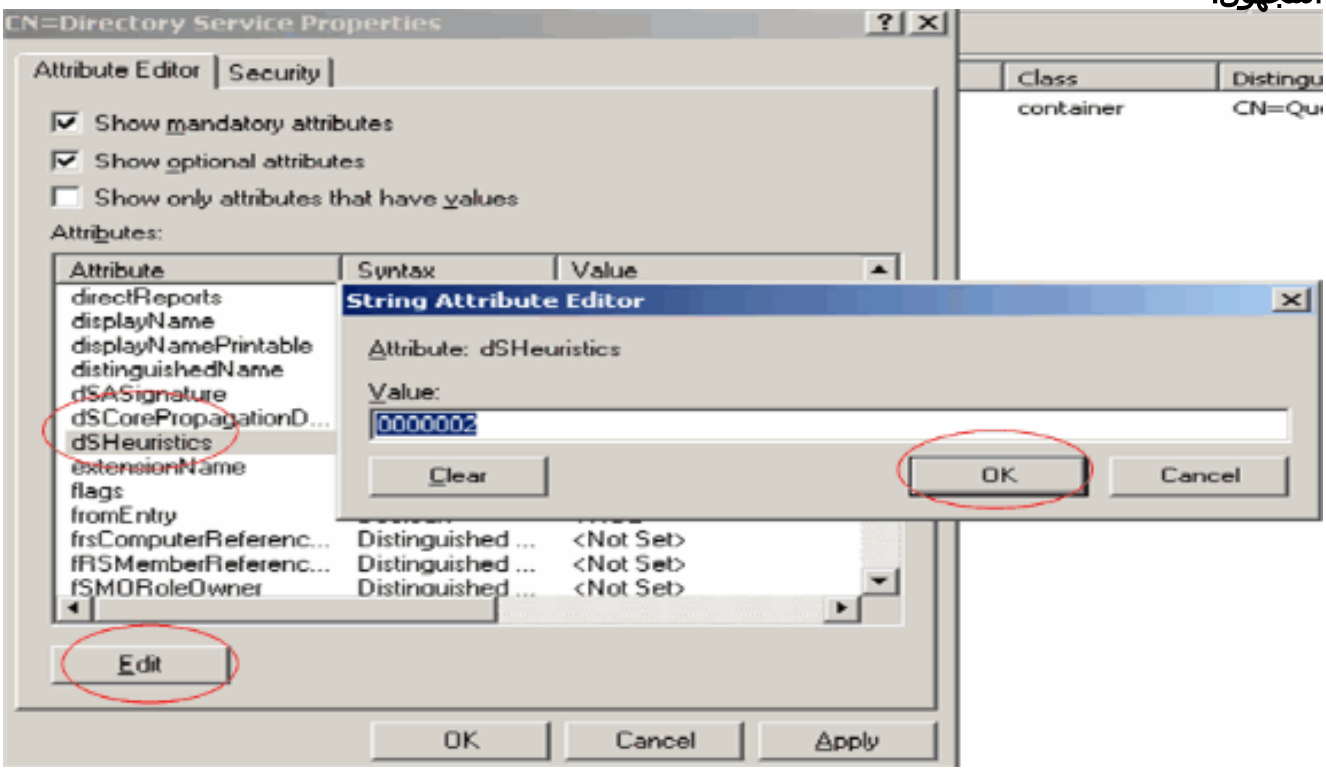
بالنسبة لأي تطبيقات جهات خارجية للوصول إلى Windows 2003 AD على LDAP، يجب تمكين ميزة الربط المجهول على Windows 2003. بشكل افتراضي، لا يسمح بعمليات LDAP المجهولة على وحدات التحكم بالمجال ل Windows 2003.

أنجزت هذا steps in order to مكنت مجهول ربط سمة:

1. قم بتشغيل أداة **تحرير ADSI** من الموقع بدء > تشغيل > الكتابة: **ADSI Edit.msc**. تعد هذه الأداة جزءا من أدوات دعم نظام التشغيل Windows 2003.
2. في نافذة تحرير ADSI، قم بتوسيع المجال الجذر (التكوين [tsweb-lapt.wireless.com]).توسيع **CN=الخدمات > CN=Windows NT > CN=خدمة الدليل**. انقر بزر الماوس الأيمن فوق حاوية **CN=Directory Service** وحدد **خصائص** من قائمة السياق.



3. في الإطار **CN=خصائص خدمة الدليل**، انقر فوق سمة **DSheuristics** تحت حقل السمة واختر **Edit**. في نافذة **محرر سمة السلسلة** لهذه السمة، أدخل القيمة **000002** وانقر فوق **تطبيق** و**موافق**. تم تمكين ميزة الربط المجهول على خادم Windows 2003.**ملاحظة:** الحرف الأخير (السابع) هو الذي يتحكم في طريقة الربط بخدمة LDAP. "0" أو عدم وجود حرف سابع يعني تعطيل عمليات LDAP المجهولة. **تعيين الحرف السابع إلى "2" يمكن ميزة الربط المجهول.**



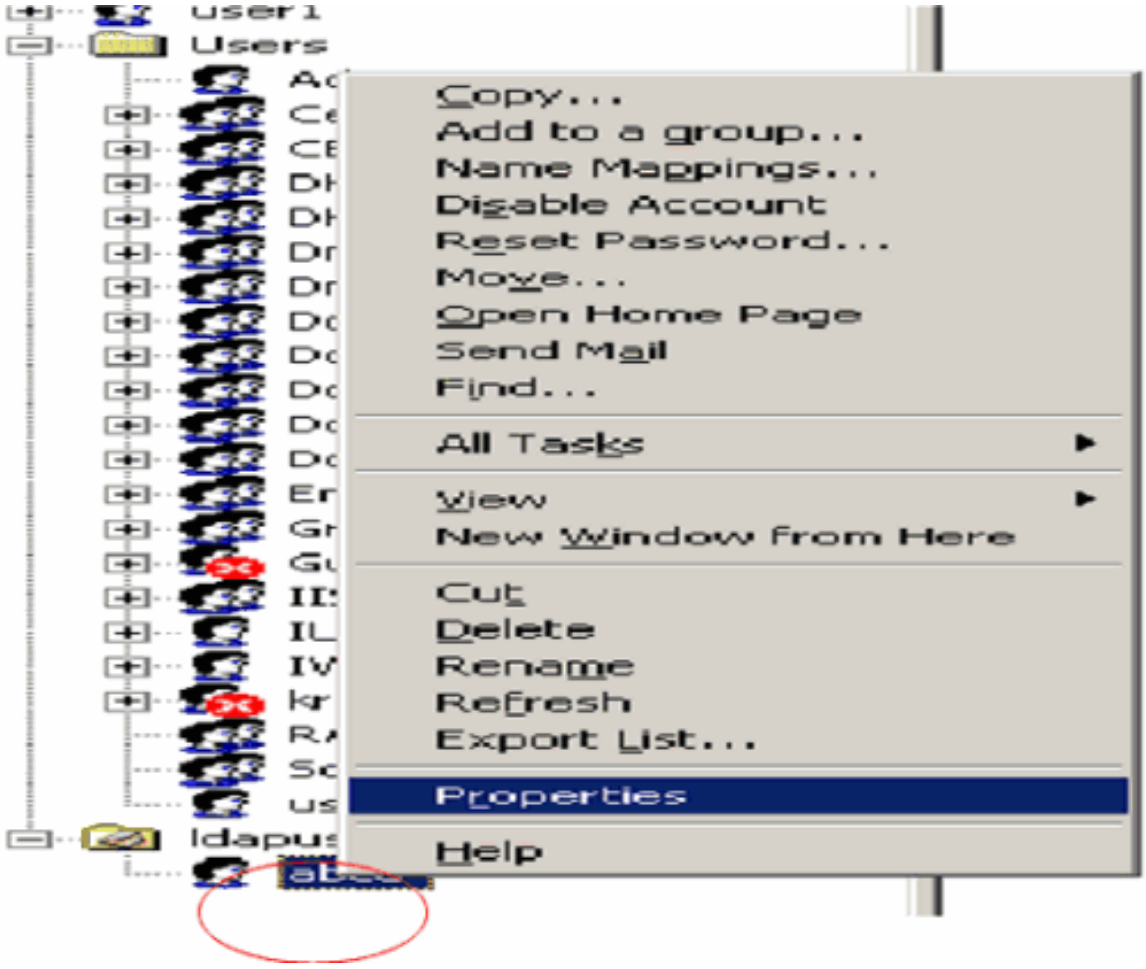
ملاحظة: إذا كانت هذه السمة تحتوي بالفعل على قيمة، فتأكد من تغيير الحرف السابع فقط من اليسار. هذا هو

الحرف الوحيد الذي يجب تغييره لتمكين الروابط المجهولة. على سبيل المثال، إذا كانت القيمة الحالية هي "0010000"، ستحتاج إلى تغييرها إلى "0010002". إذا كانت القيمة الحالية أقل من سبعة أحرف، ستحتاج إلى وضع أصفار في الأماكن غير المستخدمة: "001" ستصبح "0010002".

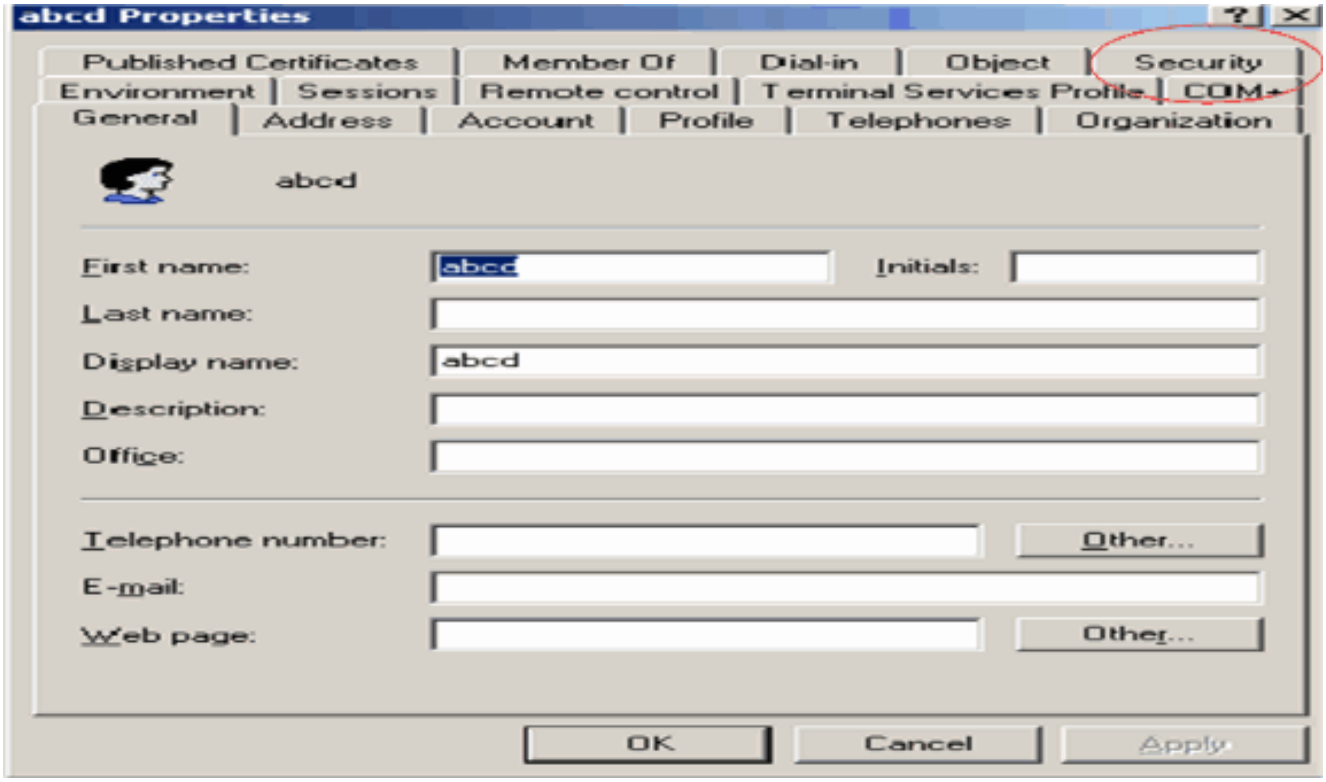
منح "مستخدم2" وصول تسجيل دخول مجهول

تتمثل الخطوة التالية في منح وصول **تسجيل دخول مجهول** للمستخدم **user2**. أتمت هذا steps in order to حققت هذا:

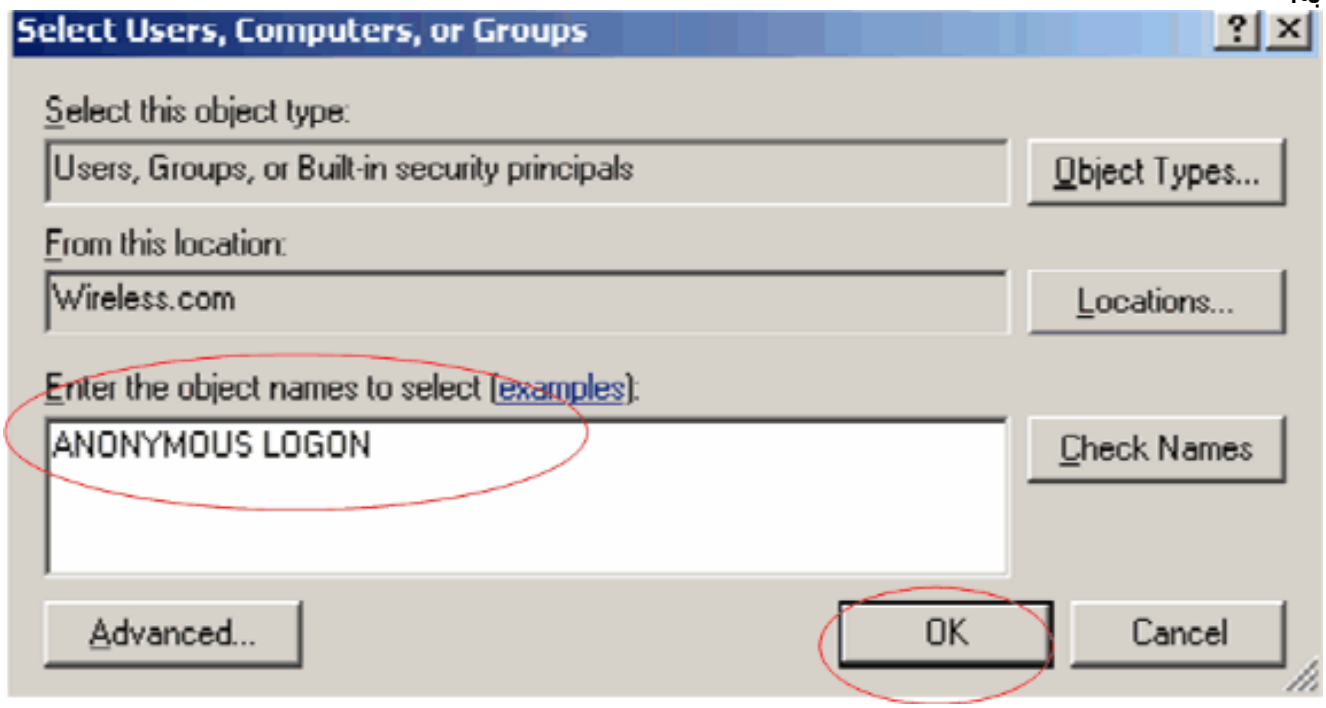
1. فتح **مستخدمي Active Directory** و**أجهزة الكمبيوتر**.
2. تأكد من تحديد **عرض الميزات المتقدمة**.
3. انتقل إلى المستخدم **user2** وانقر فوقه بزر الماوس الأيمن. حدد **خصائص** من قائمة السياق. يتم تعريف هذا المستخدم بالاسم الأول "ABCD".



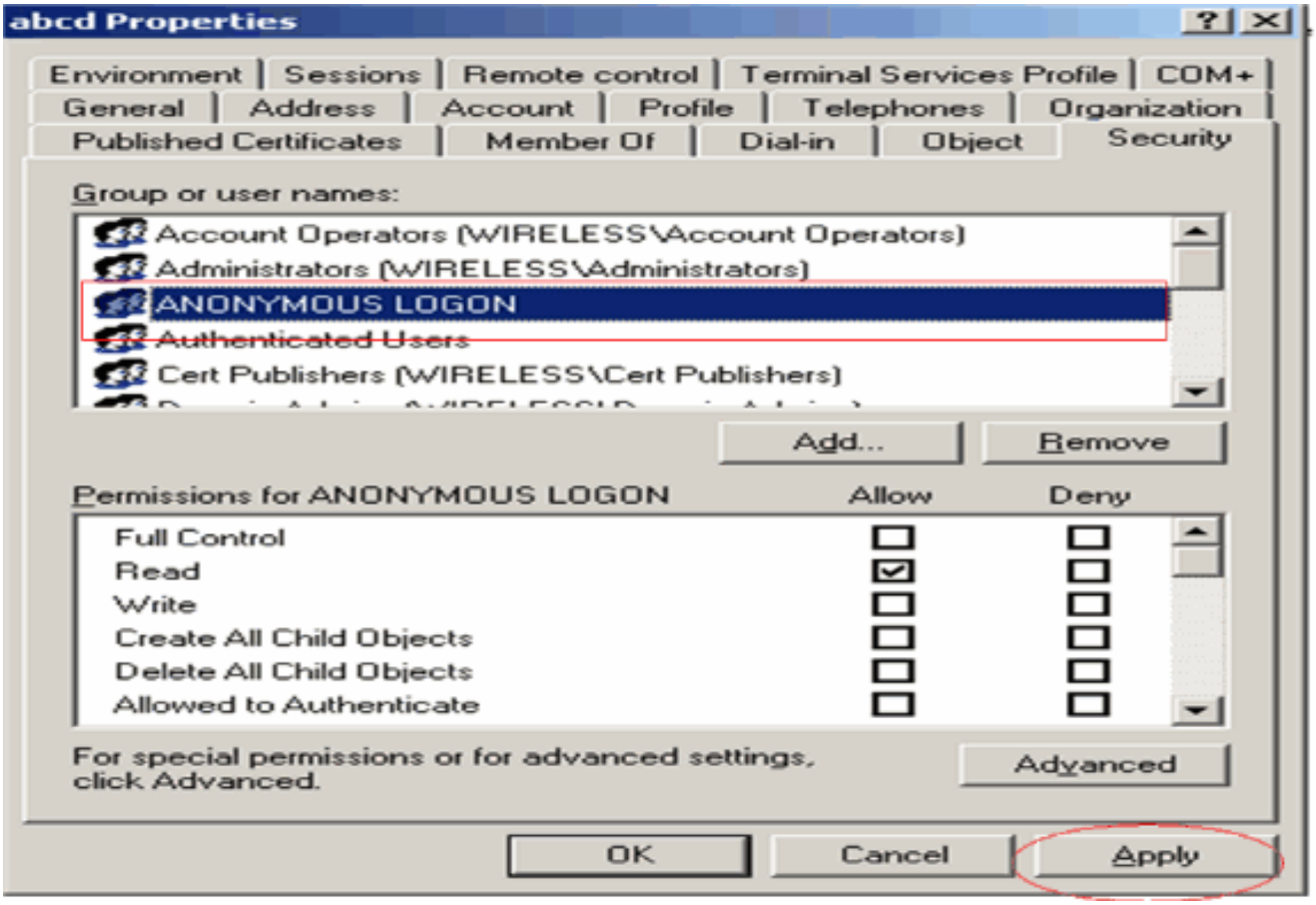
4. انتقل إلى **الأمان** في نافذة الخصائص.



5. انقر فوق **إضافة** في النافذة الناتجة.
6. أدخل **تسجيل الدخول المجهول** ضمن **مربع إدخال أسماء الكائنات لتحديد** مربع الحوار والإقرار به.



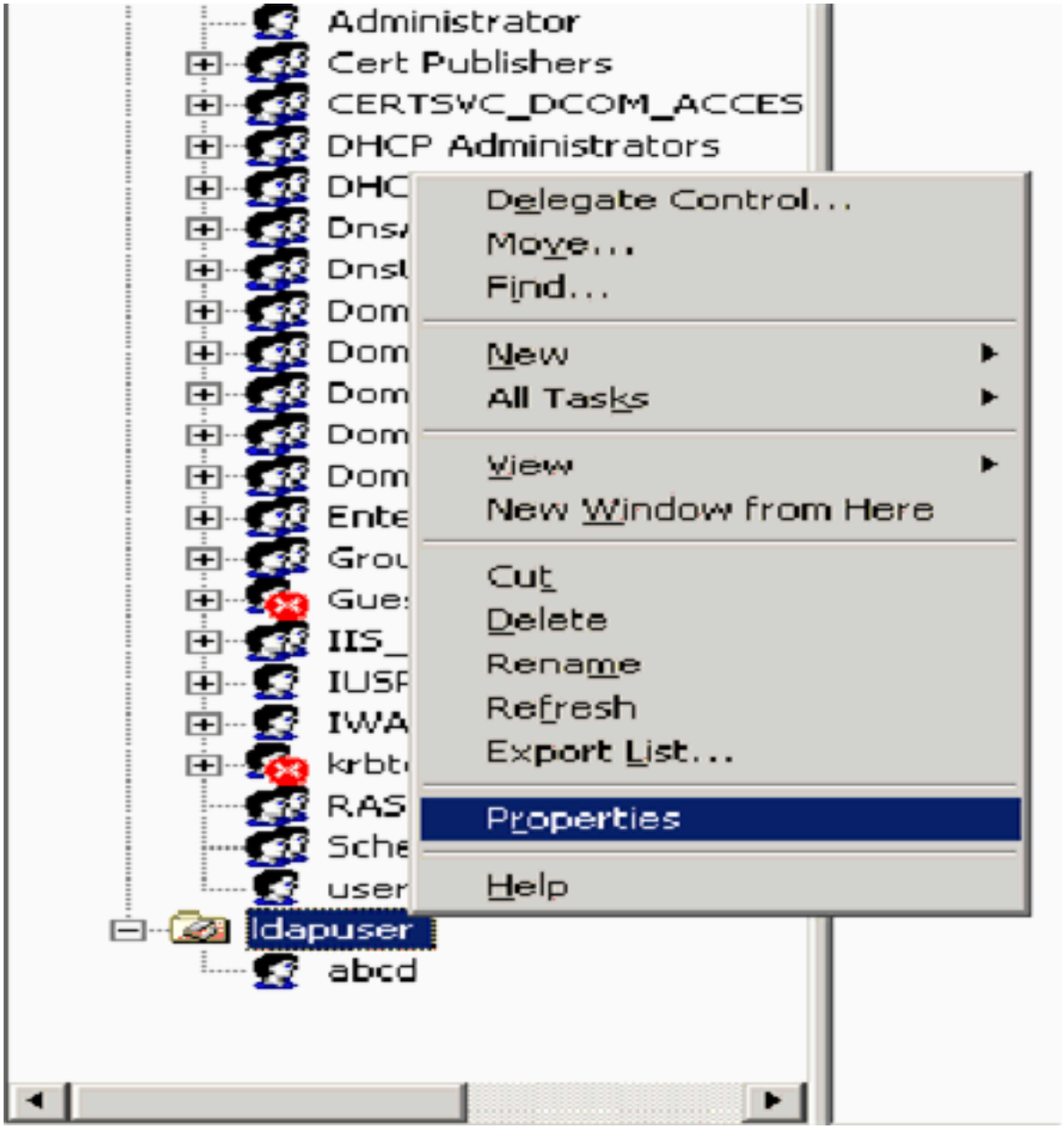
7. في قائمة التحكم بالوصول (ACL)، ستلاحظ أن **تسجيل الدخول المجهول** لديه حق الوصول إلى بعض مجموعات خصائص المستخدم. وانقر فوق **OK**. تم منح وصول تسجيل الدخول المجهول لهذا المستخدم.



منح إذن محتويات القائمة في OU

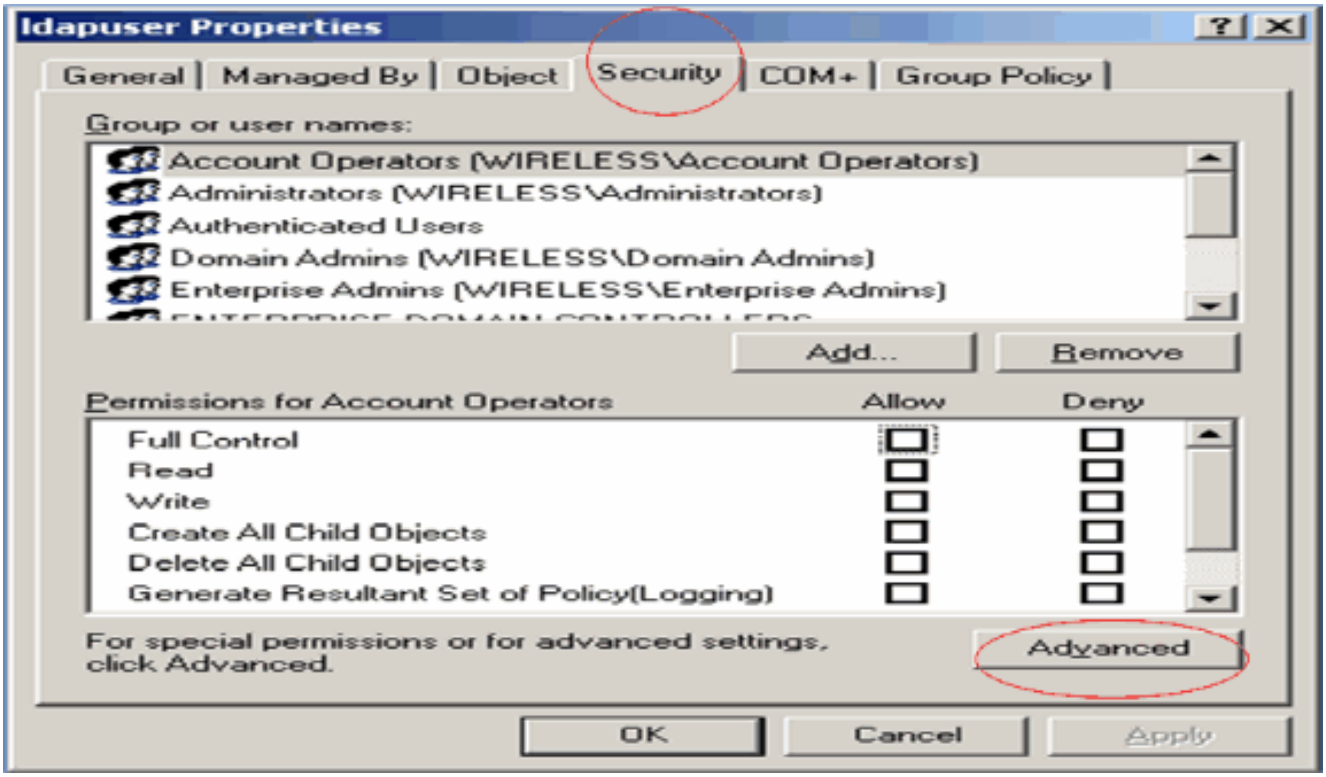
تتمثل الخطوة التالية في منح إذن **محتويات القائمة** على الأقل إلى **تسجيل الدخول المجهول** في الأمر الذي يقع فيه المستخدم. في هذا المثال، يوجد "user2" في "ldapuser OU". أتمت هذا steps in order to حققت هذا:

1. في Active Directory Users and Computers، انقر بزر الماوس الأيمن فوق **Ldapuser** Ou واختر

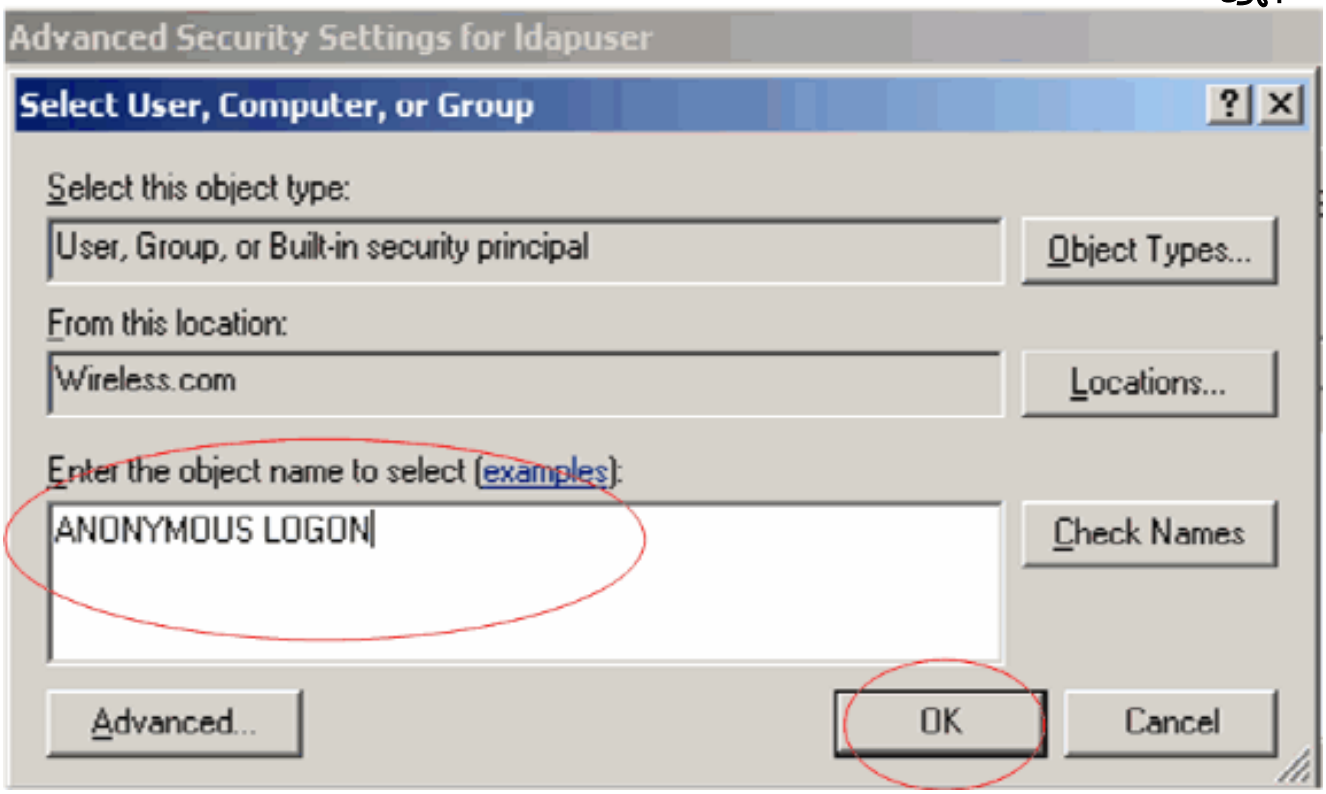


خصائص.

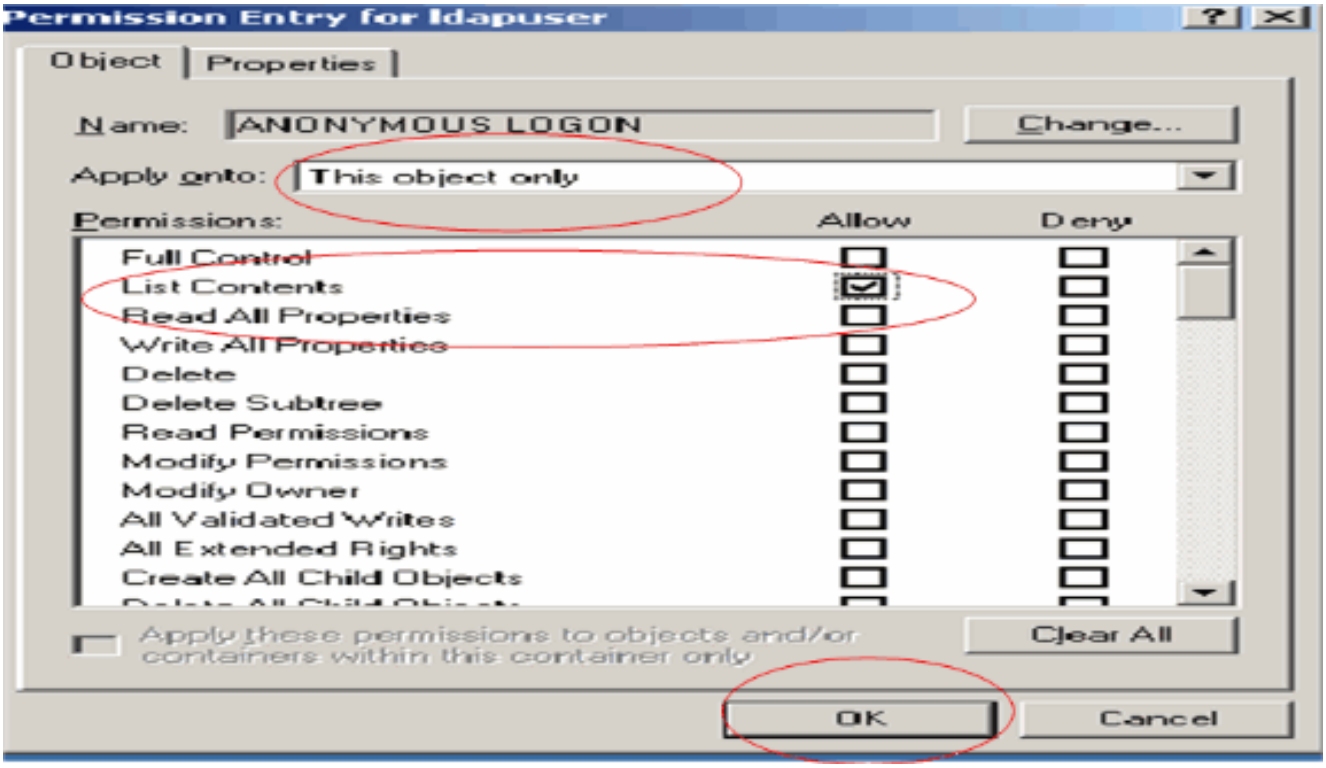
2. انقر فوق **الأمان** ثم **خيارات متقدمة**.



3. انقر فوق **إضافة (Add)**. في مربع الحوار الذي يتم فتحه، أدخل **تسجيل الدخول المجهول**.



4. الاعتراف بالحوار. يؤدي هذا إلى فتح نافذة حوار جديدة.
5. في المربع **تطبيق على** القائمة المنسدلة، أختر **هذا الكائن فقط** وقم بتمكين خانة الاختيار **محتويات القائمة** السماح.

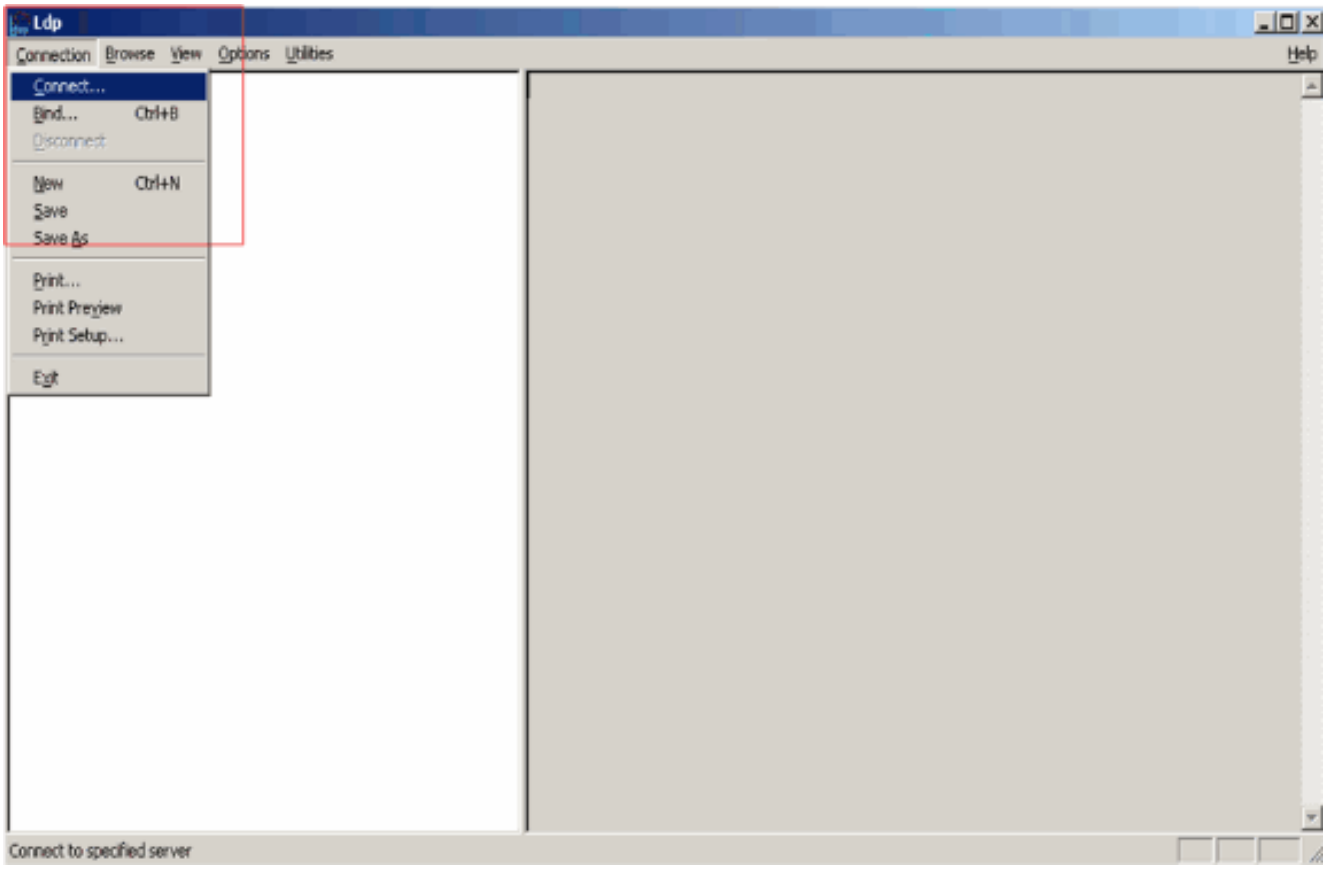


إستخدام LDP لتعريف سمات المستخدم

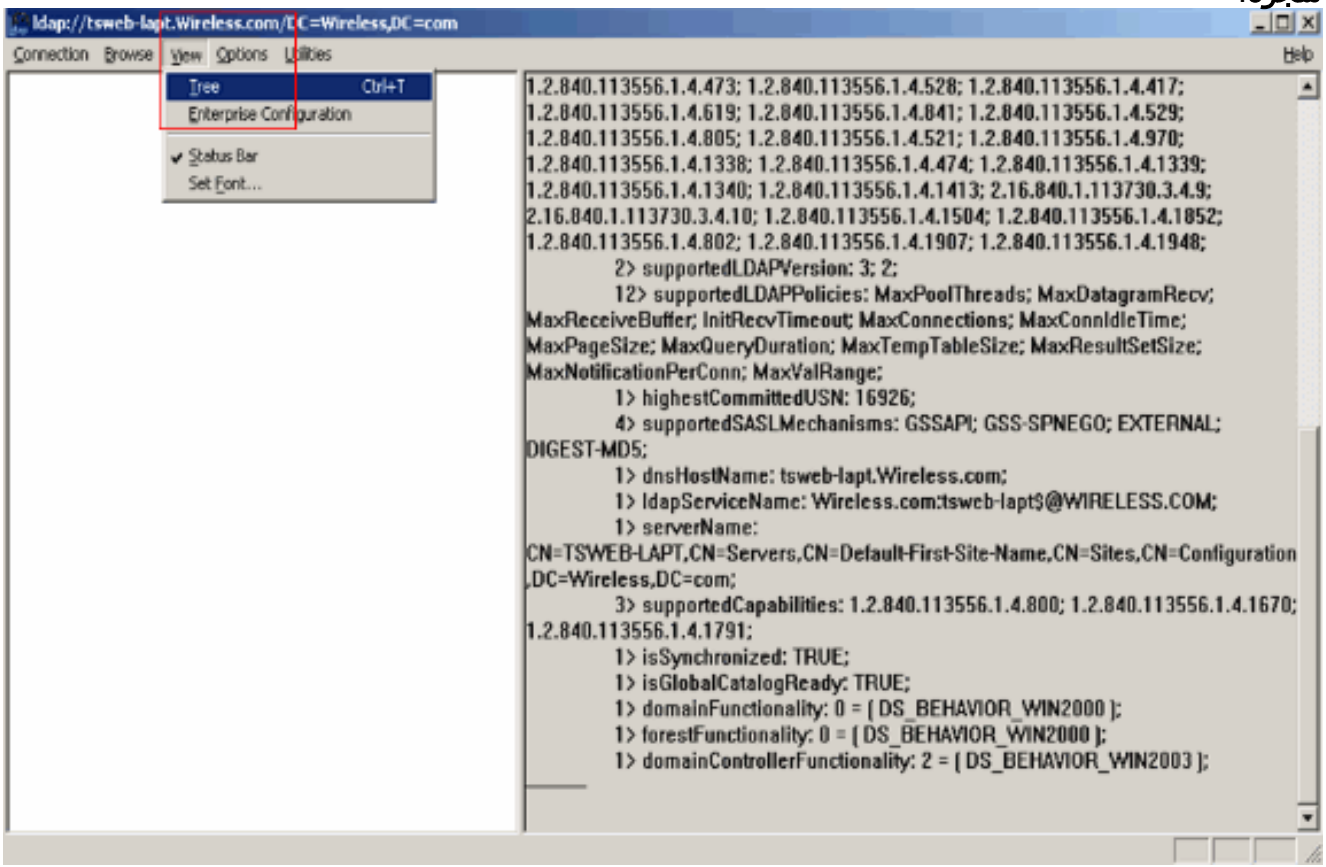
أداة واجهة المستخدم الرسومية هذه هي عميل LDAP الذي يسمح للمستخدمين بإجراء عمليات (مثل الاتصال، الربط، البحث، التعديل، الإضافة، الحذف) مقابل أي دليل متوافق مع LDAP، مثل Active Directory. يتم إستخدام LDP لعرض الكائنات المخزنة في Active Directory مع بيانات التعريف الخاصة بها، مثل واصفات الأمان وبيانات التعريف الخاصة بالنسخ المتماثل.

يتم تضمين أداة واجهة المستخدم الرسومية (GUI) عبر بروتوكول LDP عند تثبيت أدوات دعم نظام التشغيل Windows Server 2003 من القرص المضغوط الخاص بالمنتج. يشرح هذا القسم إستخدام الأداة المساعدة LDP لتحديد السمات المحددة المقترنة **بالمستخدم2**. يتم إستخدام بعض هذه السمات لتعبئة معلمات تكوين خادم LDAP على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، مثل نوع سمة المستخدم ونوع كائن المستخدم.

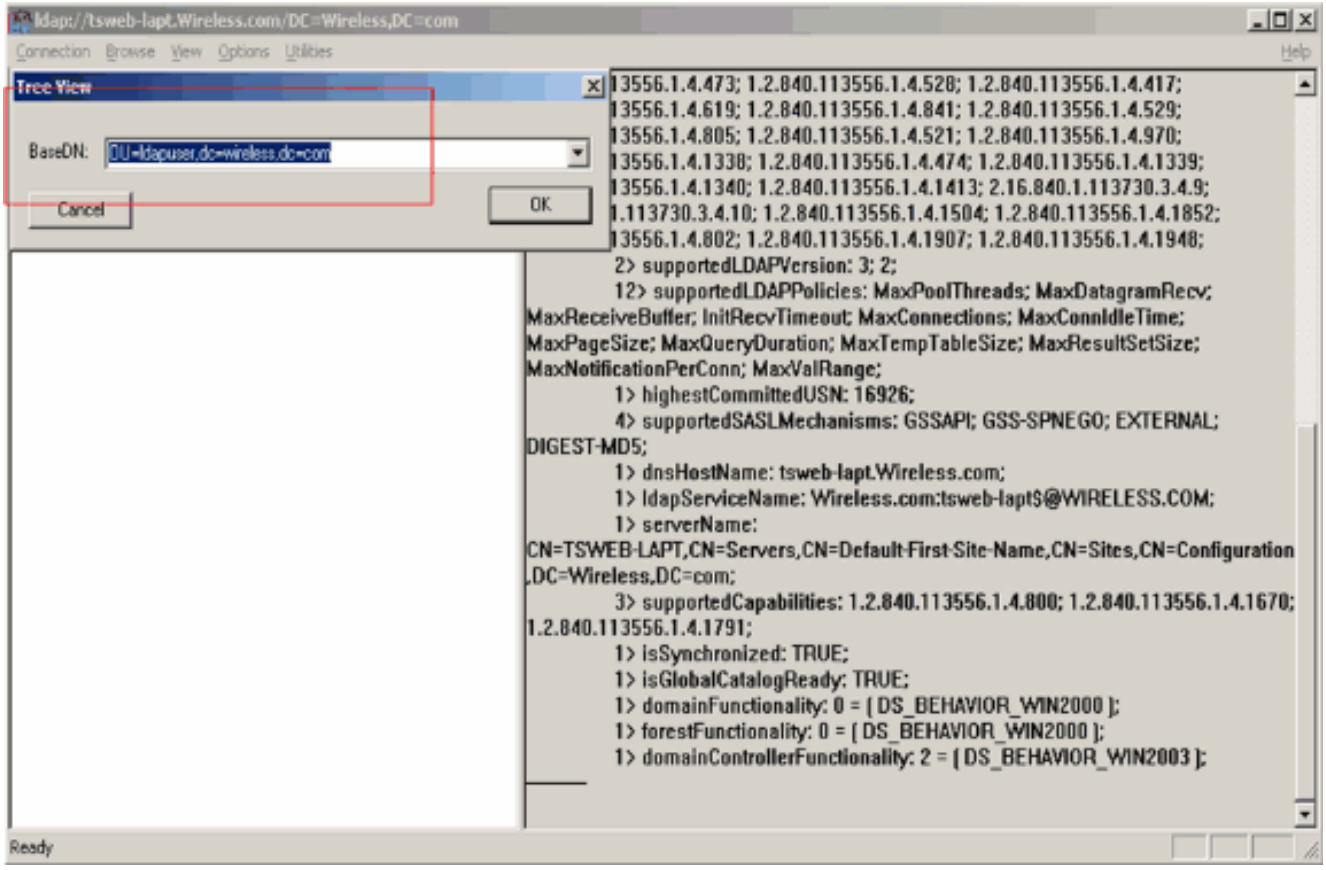
1. على خادم Windows 2003 (حتى على خادم LDAP نفسه)، انقر فوق **ابدأ > تشغيل** وأدخل **LDP** للوصول إلى مستعرض LDP.
2. في الإطار الرئيسي ل LDP، انقر فوق **اتصال** > توصيل وتوصيل بخادم LDAP من خلال إدخال عنوان IP الخاص بخادم LDAP.



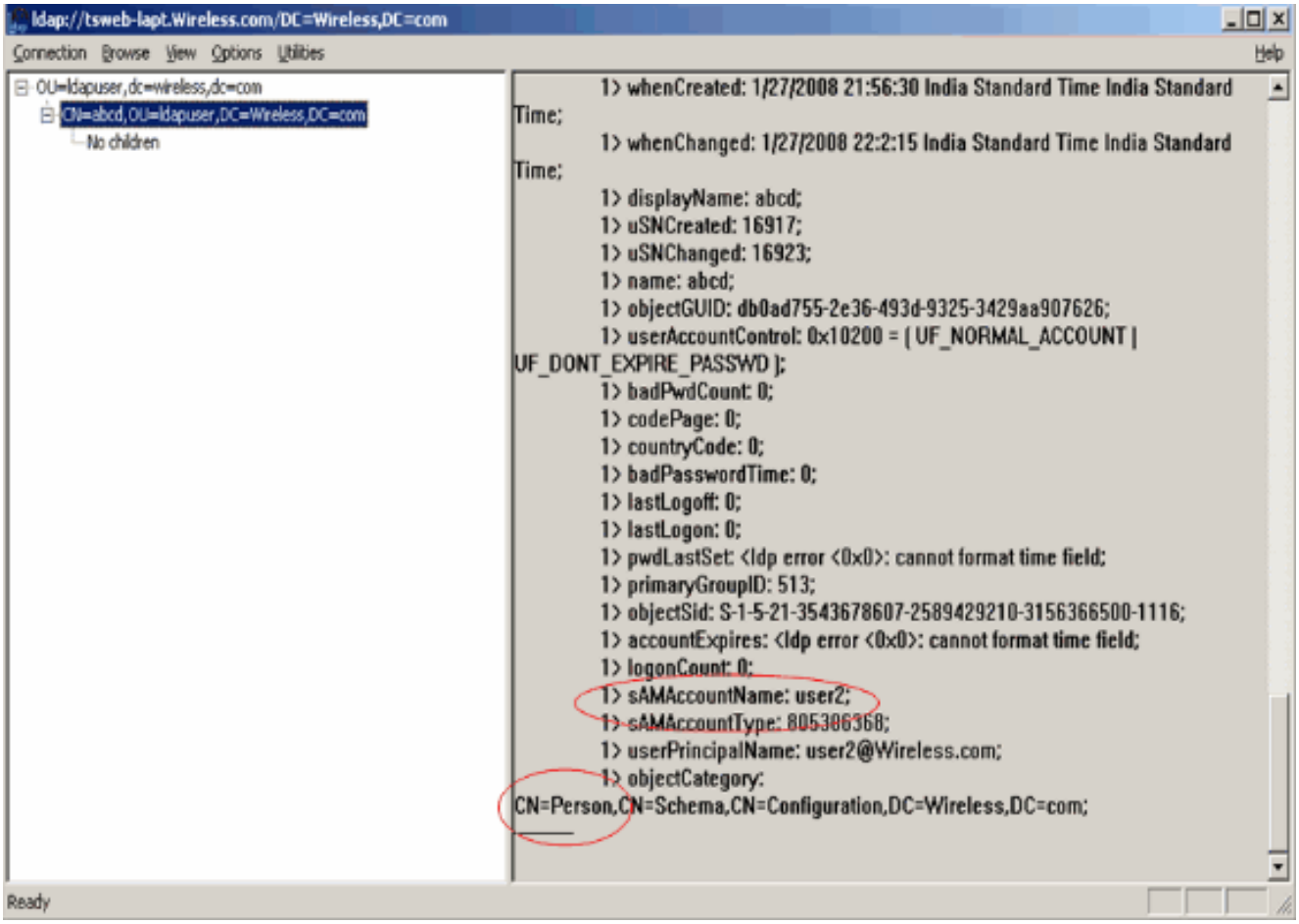
3. بمجرد الاتصال بخادم LDAP، حدد **عرض** من القائمة الرئيسية وانقر فوق **شجرة**.



4. في نافذة "عرض الشجرة الناتجة"، أدخل BaseDN الخاص بالمستخدم. في هذا المثال، **يقع user2 ضمن OU "ldapuser" ضمن المجال Wireless.com**. لذلك، فإن BaseDN **للمستخدم**2 هو **OU=ldapuser، dc=com، dc=wireless**. وانقر فوق **OK**.



5. يعرض الجانب الأيسر من مستعرض LDP الشجرة بأكملها التي تظهر أسفل BaseDN المحدد (**OU=LDAPUSER، dc=wireless، dc=com**). قم بتوسيع الشجرة لتحديد موقع **المستخدم 2**. يمكن تعريف هذا المستخدم بقيمة CN التي تمثل الاسم الأول للمستخدم. في هذا المثال، ستكون **CN=CN**. انقر نقرا مزدوجا على **CN=CN**. في الجزء الأيمن من المستعرض LDP، **سيعرض LDP جميع السمات المرتبطة بالمستخدم2**. يشرح هذا المثال هذه الخطوة:



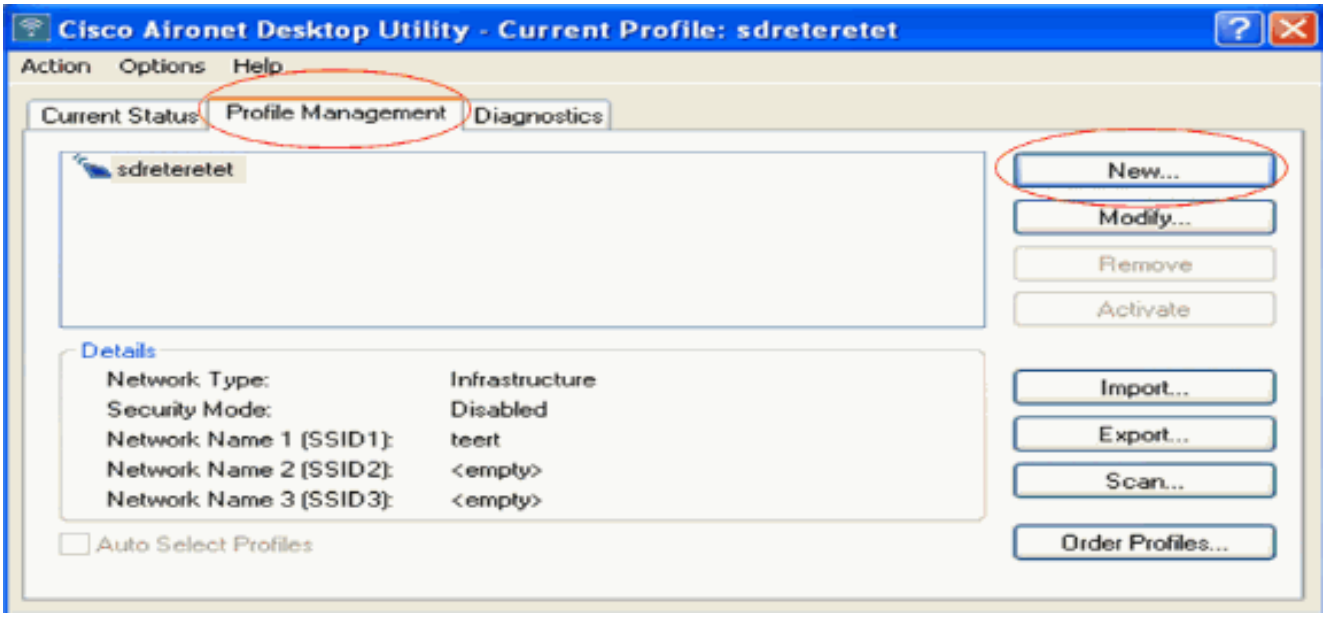
في هذا المثال، لاحظ الحقول المحاطة على اليمين.

6. كما هو مذكور في قسم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مع تفاصيل قسم خادم LDAP في هذا المستند، أدخل في حقل **سمة المستخدم** اسم السمة في سجل المستخدم الذي يحتوي على اسم المستخدم.من هذا الإخراج LDP، يمكنك أن ترى أن **sAMAccountName** هي سمة واحدة تحتوي على اسم المستخدم "user2". لذلك، أدخل سمة **sAMAccountName** المطابقة لحقل **سمة المستخدم** على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
7. في حقل **نوع كائن المستخدم**، أدخل قيمة سمة كائنType ل LDAP التي تعرف السجل كمستخدم. غالبا ما يكون لسجلات المستخدم عدة قيم للسمة objectType، بعضها فريد للمستخدم وبعضها مشترك مع أنواع كائن أخرى.في إخراج بروتوكول LDP، تكون **CN=Person** إحدى القيم التي تحدد السجل كمستخدم. لذلك، حدد **شخص** كسمة **نوع كائن المستخدم** على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

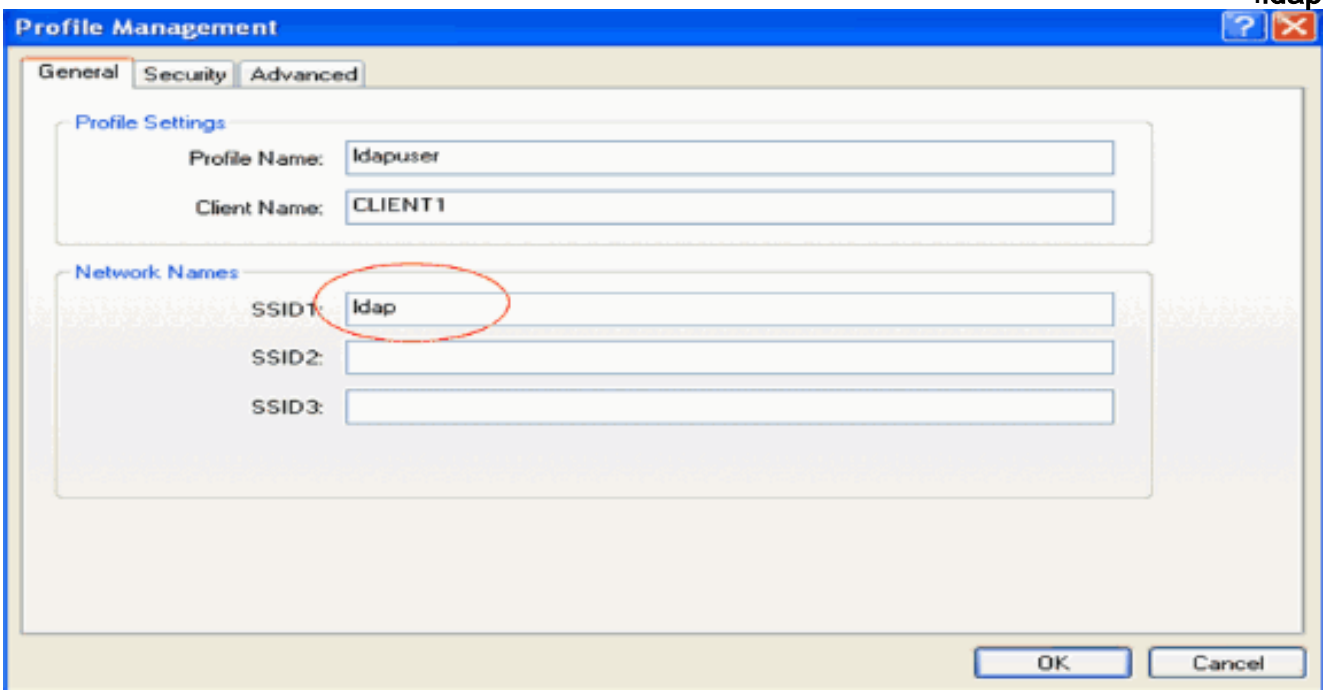
تكوين عميل لاسلكي

تتمثل الخطوة الأخيرة في تكوين العميل اللاسلكي لمصادقة EAP-FAST باستخدام شهادات العميل والخادم. أتمت هذا steps in order to حققت:

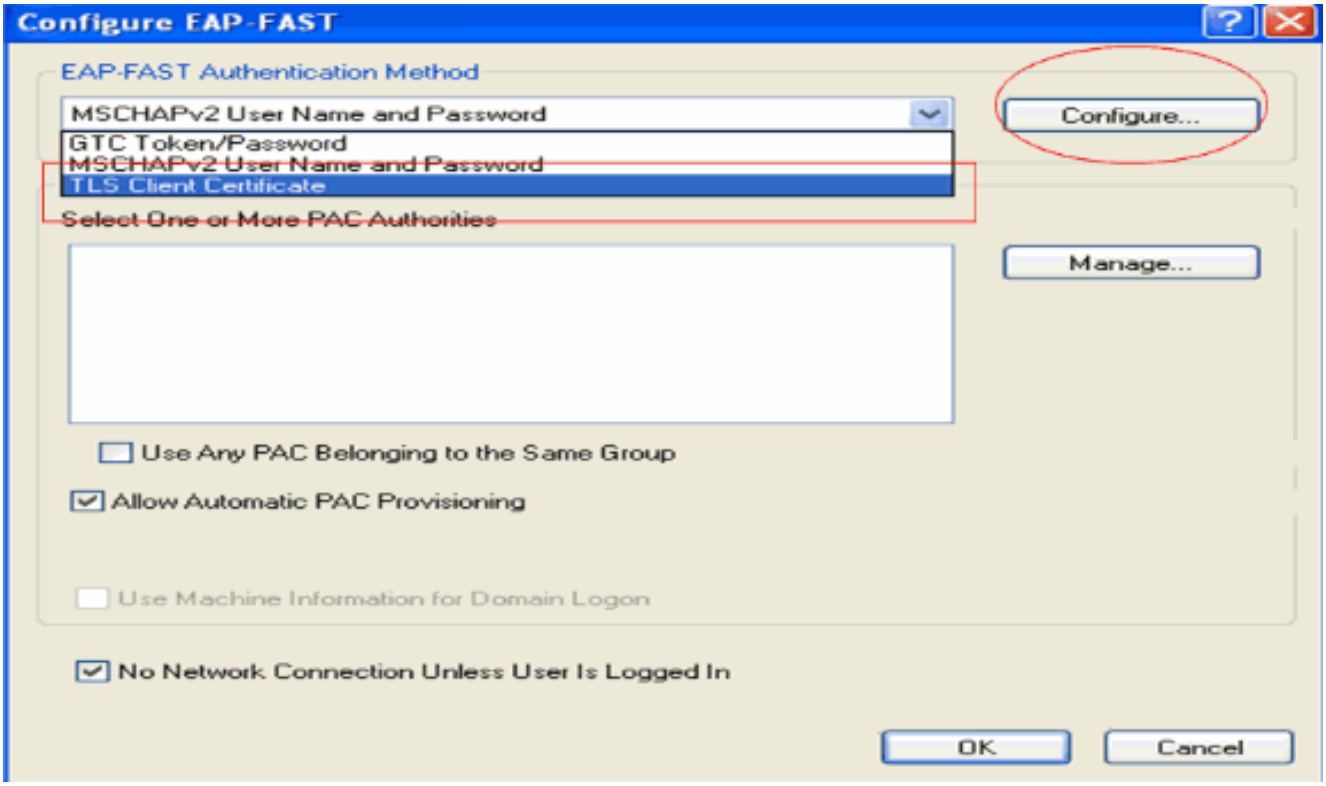
1. قم بتشغيل **أداة** ADU) **Cisco Aironet Desktop Utility**). في الإطار الرئيسي لوحدة المعالجة المركزية، انقر على **إدارة التوصيفات > جديد** لإنشاء توصيف عميل لاسلكي جديد.



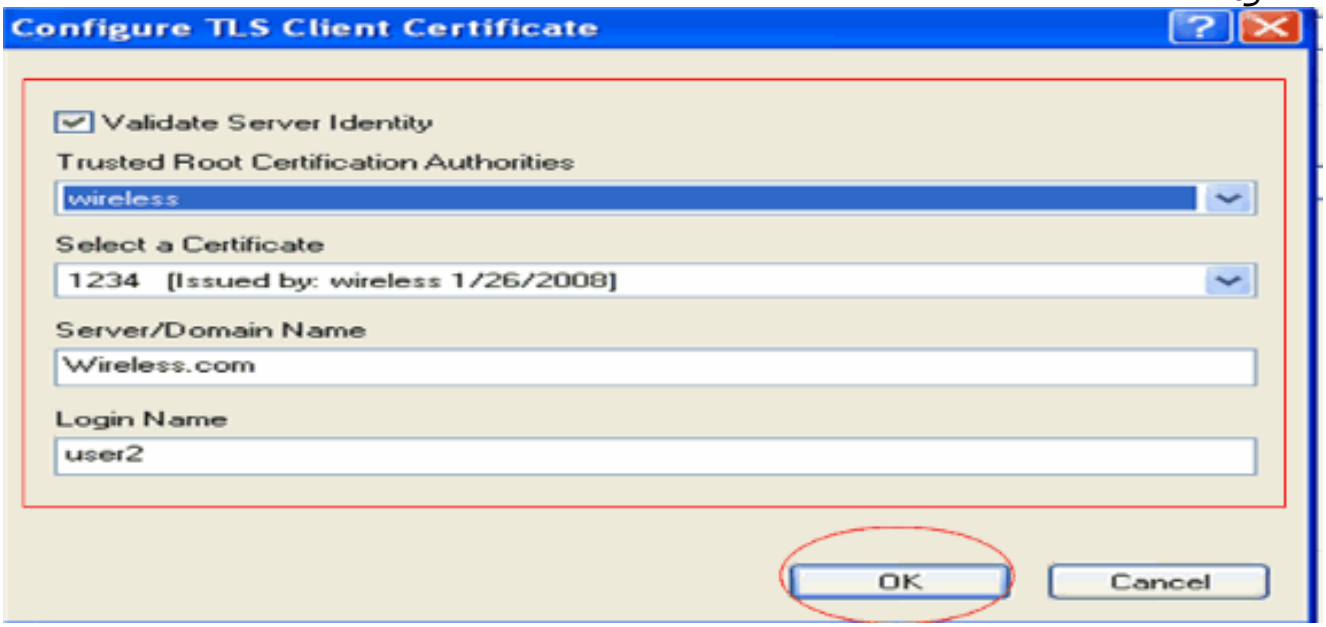
2. حدد اسم توصيف وقم بتعيين اسم SSID لهذا التوصيف. يجب أن يكون اسم SSID هذا هو نفسه الذي تم تكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). في هذا المثال، اسم SSID هو **ldap**.



3. انقر على صفحة **التأمين** واختر **802.1x/EAP** كتأمين من الطبقة 2. أخترت **EAP-FAST** كأسلوب EAP وطقطقة **يشكل**.
4. في صفحة تكوين EAP-FAST، أختر **شهادة عميل TLS** من المربع المنسدل لأسلوب مصادقة EAP-FAST وانقر على **تكوين**.



5. في نافذة تكوين شهادة عميل TLS:قم بتمكين خانة الاختيار **التحقق من هوية الخادم** وحدد شهادة المرجع المصدق المثبتة على العميل (الموضحة في قسم إنشاء شهادة المرجع المصدق الجذر لقسم العميل بهذا المستند) كمرجع مصدق جذري موثوق به.حدد شهادة الجهاز المثبتة على العميل (الموضحة في قسم إنشاء شهادة جهاز لقسم العميل بهذا المستند) كشهادة عميل.وانقر فوق **OK**.يشرح هذا المثال هذه الخطوة:



يتم إنشاء ملف تعريف العميل اللاسلكي.

التحقق من الصحة

أنجزت هذا steps in order to دققت ما إذا تشكيلك يعمل بشكل صحيح.

1. قم بتنشيط **LDAP** SSID على وحدة التحكم في الوصول المتقدمة.
2. انقر فوق **نعم** أو **موافق** كما هو مطلوب على الإطارات التالية. يجب أن تكون قادرا على رؤية جميع خطوات مصادقة العميل بالإضافة إلى الاقتران لتكون ناجحة على وحدة التحكم في الوصول (ADU).

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح. أستخدم وضع واجهة سطر أوامر (CLI) عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

- in order to دققت ما إذا WLC يستطيع اتصلت مع ال LDAP نادل وحدد المستعمل، عينت **ال debug aaa ldap enable** أمر من ال WLC CLI. يشرح هذا المثال عملية LDAP للاتصال الناجح:**ملاحظة:** تم نقل بعض الناتج في هذا القسم إلى السطر الثاني بسبب مراعاة المساحة.(وحدة التحكم من Cisco) >**تمكين تصحيح الأخطاء AAA ldap**

```
                    Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008:       Callback.....................................0x8
                                                                        344900
Sun Jan 27 09:23:46 2008:       protocolType.................................0x0
                                                                       0100002
:Sun Jan 27 09:23:46 2008:       proxyState...................................00
                                                              AC:E6:57-00:00:40:96
                (Sun Jan 27 09:23:46 2008:       Packet contains 2 AVPs (not shown
(Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1
                    Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
(Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success
(Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success
                Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
                                Sun Jan 27 09:23:46 2008: LDAP server 1 now active
,Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser,DC=wireless
                    ((DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2
                    Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64
Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus
er,DC=wireless,DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0
                                                                    (Success -
Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com
                                                                    (size 38)
                            Sun Jan 27 09:23:46 2008: Handling LDAP response Success
```

من المعلومات المميزة في إخراج تصحيح الأخطاء هذا، من الواضح أن خادم LDAP يتم الاستعلام عنه بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مع تحديد سمات المستخدم على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وأن عملية LDAP ناجحة.

- للتحقق مما إذا كانت مصادقة EAP المحلية ناجحة أم لا، حدد الأمر **debug aaa local-auth method events enable** من واجهة سطر أوامر (CLI) عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). فيما يلي مثال:(وحدة التحكم من Cisco) > **تمكين أحداث طريقة EAP المحلية** المتصلة **بالتصحيح والمحاسبة (AAA)**

```
                                Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context
                                                    (EAP handle = 0x1B000009)

                Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
                                                    (handle = 0x22000009)

                    Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
                                                    (EAP handle = 0x1B000009)

                **Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity**

                Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV
                                    (436973636f000000000000000000000000)

                    Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start

            Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

                    Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
                                                    (EAP handle = 0x1B000009)

                **:Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT**
```

Received TLS record type: Handshake in state: Start

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake

:Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT
...TLS_DHE_RSA_AES_128_CBC_SHA proposed

:(Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA

:Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello

:Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT
... Starting Diffie Hellman phase 1

:Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT
Diffie Hellman phase 1 complete

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello

Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required

:()Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet
(EAP Fast NoData (0x2b

:()Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet
(EAP Fast NoData (0x2b

:()Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet
(EAP Fast NoData (0x2b

Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack

.....

.....

.....

:Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT
Received TLS record type: Handshake in state: Sent provisioning Server Hello

:Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT
Reading Client Certificate handshake

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate

:Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID
EAP-FAST I-ID" from Peer Cert"

:Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT
Reading Client Key Exchange handshake

:Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT
... Starting Diffie Hellman phase 2

:Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT
.Diffie Hellman phase 2 complete

:Sun **Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:**
Reading Client Certificate Verify handshake

:Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
(Sign certificate verify succeeded (compare

.....

.....

.....

.....
.

- كما أن الأمر **debug aaa local-auth db enable** مفيد للغاية. فيما يلي مثال:(وحدة التحكم من Cisco)
>تمكين تصحيح أخطاء AAA المحلي المصادقة

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context

'Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
id 2) to EAP subsys)

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential
request username 'user2' to LDAP

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8

.....

.....

.....

.....

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
id 12) to EAP subsys)

```
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Processing keys success
```

- لعرض الشهادات المثبتة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) التي سيتم إستخدامها للمصادقة المحلية، قم بإصدار الأمر **show local-auth certificates** من واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC). فيما يلي مثال:(وحدة التحكم من Cisco) > **إظهار شهادات المصادقة المحلية**

```
:Certificates available for Local EAP authentication


Certificate issuer ..... vendor

:CA certificate

Subject: DC=com, DC=Wireless, CN=wireless

Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

:Device certificate

Subject: O=cisco, CN=ciscowlc123

Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT


Certificate issuer ..... cisco

:CA certificate

Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

:Device certificate

.Not installed
```

لعرض تكوين المصادقة المحلية على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من وضع واجهة سطو الأوامر (CLI)، قم بإصدار الأمر **show local-auth config**. فيما يلي مثال:(وحدة التحكم من Cisco) > **إظهار التكوين المحلي المصادقة**

```
:User credentials database search order

Primary ..... LDAP
```

```
:Timer
Active timeout ............................. 300

:Configured EAP profiles
Name ....................................... ldapuser
Certificate issuer ........................ vendor
:Peer verification options
Check against CA certificates ........... Enabled
Verify certificate CN identity .......... Disabled
Check certificate date validity ......... Disabled
:EAP-FAST configuration
Local certificate required .............. Yes
Client certificate required ............. Yes
Enabled methods ........................... fast
Configured on WLANs ....................... 2

:EAP Method configuration
:EAP-FAST
More-- or (q)uit--
<Server key ................................ <hidden
TTL for the PAC ........................... 10
Anonymous provision allowed ............... No
.............................................
.............................................
Authority Information .................... Cisco A-ID
```

استكشاف الأخطاء وإصلاحها

يمكنك إستخدام هذه الأوامر لاستكشاف أخطاء التكوين وإصلاحها:

- **تمكين أحداث أسلوب EAP المحلي-المصادقة ل debug aaa**
- **debug aaa all enable**
- **enable ربط debug dot1x**

معلومات ذات صلة

- مصادقة EAP-FAST مع وحدات تحكم الشبكة المحلية اللاسلكية ومثال تكوين خادم RADIUS الخارجي
- PEAP تحت شبكات لاسلكية موحدة مع خدمة مصادقة الإنترنت من Microsoft (IAS)
- تعيين شبكة VLAN الديناميكية مع WLCs استنادا إلى ACS إلى مثال تكوين تعيين مجموعة Active Directory
- دليل تكوين وحدة تحكم الشبكة المحلية (LAN) اللاسلكية من Cisco - تكوين حلول الأمان
- دليل تكوين وحدة التحكم في شبكة LAN اللاسلكية من Cisco - إدارة برامج وحدة التحكم وتكويناتها
- مصادقة EAP باستخدام مثال تكوين وحدات التحكم في الشبكة المحلية اللاسلكية (WLC)
- تصميم وحدة التحكم في شبكة LAN اللاسلكية (WLC) والميزات المتداولة
- Cisco Secure Services Client مع مصادقة EAP-FAST
- الأسئلة المتداولة حول وحدة التحكّم في الشبكة المحلية اللاسلكية (WLC)
- أخطاء وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية (WLC) ورسائل النظام المتداولة
- 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).