مكحت ةدحو ىلع ةيلحملا EAP ةقداصم مادختساب ةيكلساللا ةيلحملا ةكبشلا EAP-FAST مداخ نيوكت لاثمو EAP-FAST

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المتطلبات الم<u>كونات المستخدمة</u> الاصطلاحات معلومات أساسية التكوين الرسم التخطيطي للشبكة التكوينات تكوين EAP-FAST كأسلوب مصادقة EAP محلي على WLC إنشاء شهادة جهاز ل WLC تنزيل شهادة الجهاز على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تثبيت شهادة جذر PKI في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إنشاء شهادة جهاز للعميل إنشاء شهادة المرجع المصدق الجذر للعميل <u>تكوين EAP المحلي على WLC</u> تكوين خادم LDAP إنشاء مستخدمين على وحدة التحكم بالمجال تكوين المستخدم للوصول إلى LDAP إستخدام LDP لتعريف سمات المستخدم تكوين عميل لاسلكي التحقق من الصحة استكشاف الأخطاء وإصلاحها معلومات ذات صلة

<u>المقدمة</u>

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 ل EAP المحلي لاسترداد بيانات اعتماد المستخدم ومصادقة المستخدم.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

لا توجد متطلبات خاصة لهذا المستند.

<u>المكونات المستخدمة</u>

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 تشغّل 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.

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

<u>معلومات أساسية</u>

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. عندماً 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 حارجي. يسترجع EAP المحلي EAP المحلي مصادقة الحارجي و EAP-FAS و EAP-TLS و PEAPv0/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 في 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 خاول التقادم تكوين أربعة خوادم 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.

<u>التكوين</u>

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 <u>تسجيل نقطة</u> <u>الوصول في الوضع Lightweight (LAP) إلى وحدة تحكم شبكة محلية لاسلكية (WLC)</u> للحصول على مزيد من المعلومات حول عملية التسجيل.
 - تم تكوين خادم DHCP لتعيين عنوان IP إلى العملاء اللاسلكيين.
 - تم تكوين خادم CA. يستخدم هذا المثال كوحدة تحكم بالمجال وكذلك كخادم CA. يستخدم هذا المثال Windows 2003. يستخدم هذا المثال wireless.com كمجال.ارجع إلى <u>تكوين Windows 2003 كوحدة تحكم بالمجال</u> للحصول على مزيد من المعلومات حول تكوين خادم Windows 2003 كوحدة تحكم بالمجال.ارجع إلى <u>تثبيت خادم Microsoft المعلومات حول تكوين خادم Windows 2003</u> للمعلومات حول تكوين خادم Windows 2003 كوحدة تحكم بالمجال.ارجع إلى <u>تثبيت خادم Microsoft لمعلومات حول تكوين Windows 2003</u> للمعلومات مول تكوين خادم Microsoft كوحدة تحكم بالمجال.ارجع إلى مرجع مصدق (CA) للمعلومات حول تكوينه كخادم مرجع مصدق (CA) للمؤسسة.

<u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي:



<u>التكوينات</u>

أتمت هذا steps in order to نفذت هذا تشكيل:

- <u>تكوين EAP-FAST كأسلوب مصادقة EAP محلي على WLC</u>
 - <u>تكوين خادم LDAP</u>
 - <u>تكوين عميل لاسلكي</u>

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 <u>ل WLC</u>

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 ^^

eng page Mgs/J10-77.244.199(gettry			.07
emp pep Mtg://10.77.244.199(jettrv	bout:blank - Microsoft Internet Explorer		
erron page Mapu/J10.77.244.198(pertarv	Edit View Favorites Totale stelp		
ening page http://10.77.244.190/certarv	Inter//10.77.244.198/certsrv	Connect to 10, 77, 244, 198 Connecting to 10, 77, 244, 198 User name: Password: Remember my password OK: Cancel	
	paring same http://10.77.244.190/partery		amat
	sening page http://10.77.244.1940certorv	C104	ernet

شهادة.

Microsoft Certificate Services - Microsoft Internet Explorer	
Address 🕘 http://10.77.244.190/certarv/	
Microsoft Certificate Services wireless	Home
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify yo identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you reperform other security tasks.	ur Juest,
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), view the status of a pending request.	or to
For more information about Certificate Services, see Certificate Services Documentation.	
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
Internet	<u>. (9</u>
، طلب شهادة، انقر على طلب شهادة	3. في صفحا
	متقدمة.
Microsoft Certificate Services - Microsoft Internet Explorer	
Address 🕘 http://10.77.244.198/certsrv/certraus.asp	💌 🎒 Go
Microsoft Certificate Services wireless	Home
Request a Certificate	
Select the certificate type: User Cathfronte	
Or submit an advanced certificate request.	

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

icrosoft Certificate Services - Microsoft Internet Explorer	
Edit View Favorites Tools Help	4
🚥 🕘 http://10.77.244.190/certsrv/certsrgad.asp	🗹 🛃 G
Icroaoff Certificate Services witeless	Heme
luanced Certificate Dequest	
Walload Celuinate Reduest	
e policy of the CA determines the types of certificates you can request. Click one of the following options to:	
Create and submit a request to this CA.	
Submit a certificate request by using a base 64-encoded CMC or PKCS #10 file, or submit a renewal request by using PKCS #7 file.	a base-64-encoded
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrolment station. Note: You must have an enrolment agent certificate to submit a request on behalf of another user.	
	Internet

- 5. في نموذج طلب الشهادة المتقدمة، اختر **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 الم

	ىمرە.
Microsoft Certificate Services - Microsoft Internet Explorer	
nle Edit View Pavoritiel Tools Help	A1
Charles of the Charles Structure (C) Co. 2. 7 3	
Can the state of t	
sidvess 🛃 http://10.77.244.198/cartisry/certrigns.asp)	🛩 🛃 GO
Microsoff Certificate Services with this	Home
Advanced Certificate Request	
Certificate Template:	
Web Server	
Identifying Information For Offline Template:	
Name: ciscowic123	
B-Mail	
Company Alego	
Company, Citto	
Department:	
City:	
State:	
Country/Region	
Key Options:	
Oreste new key set Ouse existing key set Ouse existin	
CSP. Microsoft RSA SChannel Cryptographic Provider 🛩	
Key Usage: @ Exchange	
Key Size: 1024 Max. 304 (common key date: 512 1024 2049 6192 10204.)	
1.13 0.14 100 Mac 10304	
O User specified key container name	
Mark koys as exportable	
Enable strong private key protection	
Store certificate in the local computer certificate store	1
Done	Internet

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

Microsoft Certificate Services - Microsoft Internet Explorer	
le Edit View Favorites Tools Help	A
🕽 Back + 🕥 - 📧 🗟 🐔 🔎 Search 🤺 Pavortes 🥝 🔗•	😓 🖼 🚳
(kess 🕘 http://10.77.244.198/certary/certrana.asp	💌 🛃 😡
Create new key set Use existing key set	A
CSP: Microsoft RSA SChannel Cryptographic Previder 💌	
Kay Usage: 🛞 Exchange	
Key Size: 1024 Min: 004 (common key size: 512 5029 2048 5085 5192) Marc16204	15356 >
Automatic key container name	container name
Mark keys as exportable	
Export keys to the	
Enable strong private key procession Store pertificate in the local computer certificate store	
Store centricate in the local computer centricate store Stores the certificate in the local computer store	
instead of in the user's certificate store. Does not instead the cost CA's catilicate. View must be an	
administrator to generate or use a key in the local	
machine store.	
dditional Options:	
lequest Format: O CMC	
Hash Algorithm: SHA-1 M	
Only used to sign request.	
Save request to a file	
Attributes:	
()	
Friendly Name:	
	Submit >
	🕐 Internet
	انقرعا نعم في الإطار التال السماح يعملية طلب
	العراجين فعكم في الإصار التاني مستنتاع بمسيد مشب
	الشهادة.

Potentia	al Scripting Violation	X
⚠	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request certificate for you. Do you want to request a certificate now?	a
	Yes No	

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**.

Alicrosoft Certificate Services - Microsoft Internet Explorer	
File Edit View Pavortisi Tools Help	
Addxiss and http://10.77.244.198/certsrv/certfinsh-asp	💌 🛃 🖘 🚬
Microsoft Certificate Services - wireless	Home
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
	C Televent
1	Troemer

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

	.0/
Nicrosoft Certificate Services - Microsoft Internet Explorer	
Edit: Week Favorites Tools Help	<i>A</i>
<< ali http://10.77.244.198/bertsrv/certringn.asp	💌 🛃 🚥
prosoff Certificate Services wireless	Home
tificate Installed	
r new certificate has been successfully installed.	

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**.

about:blank - Microsoft Internet Explorer	
File Edit View Pavorites Toxis Help	
about:blank - Microsoft Internet Lxplorer Ple Edit View Pavorite Address about:blank Poy-up Bioder Manage Addrons Sinchronite Windows UpSate Windows UpSate Windows UpSate Sun Java Console Sunered Opticits	
Enables you to change settings.	

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

فتراضي.
nternet Options 💦 🚬 🔀
General Security Privacy Content Connections Programs Advanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer.
Enable Settings
Certificates
Use certificates to positively identify yourself, certification authorities, and publishers.
Clear SSL State Certificates Publishers
Personal information
AutoComplete stores previous entries and suggests matches for you. AutoComplete
Microsoft Profile Assistant stores your My Profile
OK Cancel Apply

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

Certificates			<u>?</u> 🔀
Intended purpose:	<all></all>		~
Personal Other Pe	ople Intermediate Certification	Authorities Trusted Root Cert	ification 🔨 🚬
Issued To	Issued By	Expiratio Friendly Nam	
🔤 ciscowlc123	wireless	1/25/2010 <none></none>	
Import	xport Remove	0	Advanced
Server Authenticat	1 purposes		
Joi toi hadhanalad			View
		0	Close

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

- Wessels Freesel Wessel	الي).
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page. Do you want to export the private key with the certificate?	
 Yes, export the private key No, do not export the private key 	
< Back Next > Car	cel

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

icate Export Wizard	
port File Format Certificates can be exported in a varie	ety of file formats.
Select the format you want to use:	
O DER encoded binary X.509 (.C	ER)
O Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax	Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the	e certification path if possible
Personal Information Exchange	e - PKCS #12 (.PFX)
Include all certificates in the	e certification path if possible
Enable strong protection (r	equires IE 5.0, NT 4.0 SP4 or above)
Delete the private key if the	e export is successful
	< Back Next > Cancel
امة	ات في الكلمة نافذة، كلمة يستخدم هذا المثلا، Cisco كك
	ور.
ificate Export Wizard	ور.
ificate Export Wizard	ور. 2
ificate Export Wizard assword To maintain security, you must protec	ور. کا Lt the private key by using a password.
ificate Export Wizard assword To maintain security, you must protee	ور. کا ct the private key by using a password.
ificate Export Wizard assword To maintain security, you must protec	t the private key by using a password.
ificate Export Wizard assword To maintain security, you must protec Type and confirm a password.	ر. t the private key by using a password.
ificate Export Wizard assword To maintain security, you must protec Type and confirm a password. Password:	ر. t the private key by using a password.
ificate Export Wizard assword To maintain security, you must protec Type and confirm a password. Password:	ر. t the private key by using a password.
ificate Export Wizard assword To maintain security, you must protect Type and confirm a password. Password: ******** Confirm password:	ct the private key by using a password.
ificate Export Wizard assword To maintain security, you must protect Type and confirm a password. Password: ******** Confirm password: *****	ct the private key by using a password.
ificate Export Wizard assword To maintain security, you must protect Type and confirm a password. Password: ******** Confirm password: *******	t the private key by using a password.
ificate Export Wizard assword To maintain security, you must protect Type and confirm a password. Password: ******** Confirm password: *******	ct the private key by using a password.
ificate Export Wizard assword To maintain security, you must protect Type and confirm a password. Password: ******** Confirm password: *******	t the private key by using a password.
ificate Export Wizard assword To maintain security, you must protect Type and confirm a password. Password: ******** Confirm password: *******	ct the private key by using a password.
ificate Export Wizard assword To maintain security, you must protect Type and confirm a password. Password: ******** Confirm password: *******	ct the private key by using a password.
ificate Export Wizard assword To maintain security, you must protect Type and confirm a password. Password: ******** Confirm password: *******	t the private key by using a password.
ificate Export Wizard assword To maintain security, you must protect Type and confirm a password. Password: ******** Confirm password: *******	ct the private key by using a password.

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

Certificate Export Wizard	
File to Export Specify the name of the file	you want to export
File name:	
C:\OpenSSL2\bin\ciscowlc1	23.pfx Browse
	< Back Next > Cancel
Certificate Export Wizard	
	Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings: File Name C:\Opt Yes Export Keys C:\Opt Yes Include all certificates in the certification path File Format No Person Person
Certificate Export Wizard	X
The export was successful.	< Back Finish Cancel

<u>تنزيل شهادة الجهاز على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)</u>

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.

<u>تحويل الشهادة بتنسيق PFX إلى تنسيق PEM باستخدام برنامج OpenSSL</u>

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 <u>OpenSSL</u> 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.

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

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.
- د. 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: (transfer download start> (Cisco Controller)

.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.

<u>تثبيت شهادة جذر PKI في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)</u>

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://<I**P عنوان CA Server>/certsrv** من pc الخاص بك الذي له اتصال شبكة بخادم CA. تسجيل الدخول كمسؤول عن خادم CA.



2. انقر علی **تنزیل شهادة CA أو سلسلة شهادات أو** CRL

	.ORL
Microsoft Certificate Services - Microsoft Internet Explorer	
in Lar Year Parotes Look leep	2 2 0
Microsoff Contribute Services	Home
Nelcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify y identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you re perform other security tasks.	vour equest,
(ou can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL) iew the status of a pending request.), or to
For more information about Certificate Services, see Certificate Services Documentation.	
Select a task: Request a certificate View the steture of a pending certificate request Download a CA certificate, certificate chain, or CRL	
	<u>v</u>
	396
ة الناتجة، يمكنك ان ترى شهادات CA الحالية المتاحة على خادم CA تحت مربع شهادة CA . اخترت	. في الصفح
ميز طريقة وطقطقة تنزيل مرجع	DER کالتر
	مصدق.

Microsoft Certificate Services - Microsoft Internet Explorer	C 8 🛛
Pile Edit View Pavortisk Tools Help	
Addinus 🕘 http://10.77.244.198/certsrv/joertoerc.esp	aa 🛃 🐱
Microsoft Certificate Services - wireless	Home
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
© Base 64 Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL	
Ø	Internet

- 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" و "-openSSL" هي certnew.cer و @WLC) رولال (WLC) مع هذه التغييرات:إن الملفات openSSL" و "-out" هي certnew.cer و @WLC) و (WLC) مع هذه التغييرات:إن الملفات openSSL" و "-out" هي certnew.cer و @WLC) مع هذه التغييرات:إن الملفات openSSL" و "-out" هي certnew.cer و @WLC) (WLC) مع هذه التغييرات:إن الملفات openSSL" و "-out" هي certnew.cer و @WLC) و (WLC) مع هذه التغييرات:إن الملفات n مرور الاستيراد في هذه العملية.أيضا، أمر OpenSSL لحويل ملف .certnew.cer إلى ملف .certnew.cer و @WLC الحويل ملف .certnew.cer و @WLC لحمل .ger out certnew.cer و @WLC لحمل .ger NEO لتحويل ملف .cer من <u>openSSL مرور معارة مرور PEM مرور NEC و @WLC و @WLC</u> و ".ser out certnew.cer و @WLC و WLC و @WLC و @WLC و @WLC و @WLC و WLC و @WLC و

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

									ﺎﻝ:
wic2006 - Microsoft Inter	net Explorer								
ı. cısco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	Saxe Co C <u>C</u> MMANDS	nfiguration Ping HELP	Logout <u>R</u> efres
Security	ID Certific	ate			\smile				New
 AAA Ganeral RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies E Local EAP Priority Order Access Control Lists Wireless Protection Policies Web Auth Advanced Clos Sensors Shunned Clients ID Certificate 	Name bsnSslEapOr	twCert	Fo	ilid Period	Heh, 12:10:31 (GMT Until 2010 Jan	n 23rd, 12:18:31		
à								A 🖷 1	nternet

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
Connect to 10.77	. 244.198 🛛 🖓 🔀
Connecting to 10.77.	244.198
User name:	😰 wireless\user2
Password:	•••••
	Remember my password
	OK Cancel
	:. حدد طلب
	شهادة.
Microsoft Certificate Services - Microsoft Internet Exp Pie Edit View Envortes Tools Help	lorer 🗧 🖬 🗶
Address Attp://10.77.244.198/certary/	v 🛃 😡
Microsoft Certificate Services wireless	Home
Welcome	
Use this Web site to request a certificate for your identity to people you communicate with over the perform other security tasks.	Web browser, e-mail client, or other program. By using a certificate, you can verify your Web, sign and encrypt messages, and, depending upon the type of certificate you request,
You can also use this Web site to download a cent view the status of a pending request.	tificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to
For more information about Certificate Services,	see Centificate Services Documentation.
Select a task: Request a certificate View the status of a pending certificate reques Download a CA certificate, certificate chain, or	t CRL
e)	Internet

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

Microsoft Certificate Services - Microsoft Internet Explorer	
e Edit Wew Pavorites Tools Help	
inni 🕘 Milpu//10.77.244.198/certsrv/certrigus.esp	🗹 🛃 Go
dicrosoft Certificate Services wireless	Heme
equest a Certificate	
elect the certificate type:	
User Certificate	
submit an advanced certificate request.	
tp://10.77.244.198/certsrv/certrqad.asp	S Internet
لتورياني. فر على إنشاء طلب وإرساله إلى المرجع المصدق هذا . ينقلك هذا إلى	و في صفحة طلب الشهادة المتقدمة، ان
ل لهيز//10.77.244.198/carter/ceetroad.app فر على إنشاء طلب وإرساله إلى المرجع المصدق هذ ا. ينقلك هذا إلى	و في صفحة طلب الشهادة المتقدمة، ان منابع المالية الم
^{یور} علی إنشاء طلب وإرساله إلی المرجع المصدق هذ ا. ينقلك هذا إلی	و في صفحة طلب الشهادة المتقدمة، ان نموذج طلب الشهادة
مرجع المصدق هذا. ينقلك هذا إلى فر على إنشاء طلب وإرساله إلى المرجع المصدق هذ ا. ينقلك هذا إلى	في صفحة طلب الشهادة المتقدمة، ان موذج طلب الشهادة لمتقدمة.
تفتر على إنشاء طلب وإرساله إلى المرجع المصدق هذا . ينقلك هذا إلى Microsoft Certificate Services - Microsoft Internet Explorer	التعامية في صفحة طلب الشهادة المتقدمة، ان لمتقدمة. المتقدمة.
فلمرجع المصدق هذا. ينقلك هذا إلى فر على إنشاء طلب وإرساله إلى المرجع المصدق هذ ا. ينقلك هذا إلى Alcrosoft Certificate Services - Microsoft Internet Explorer	لي صفحة طلب الشهادة المتقدمة، ان نموذج طلب الشهادة لمتقدمة. ها ■ ■
فلمرجع المصدق هذا. ينقلك هذا إلى فر على إنشاء طلب وإرساله إلى المرجع المصدق هذا. ينقلك هذا إلى Alcrosoft Certificate Services Microsoft Internet Explorer Edt: Veen Feverlass Took Help	المتقدمة، ان في صفحة طلب الشهادة المتقدمة، ان موذج طلب الشهادة لمتقدمة. هو ي
فتر على إنشاء طلب وإرساله إلى المرجع المصدق هذا. ينقلك هذا إلى هذر على إنشاء طلب وإرساله إلى المرجع المصدق هذا. ينقلك هذا إلى Microsoft Certificate Services - Microsoft Internet Explorer قط العور(10.77.244.190)(estav/certrogad.asp	المتقدمة، ان متقدمة، ان موذج طلب الشهادة المتقدمة، ان لمتقدمة. كانا المتقلية
etp://10.77.244.19#/certerv/certrqad.acp فر علی إنشاء طلب وإرساله إلی المرجع المصدق هذا . ينقلك هذا إلی Microsoft Certificate Services - Microsoft Internet Explorer قط Vers Pavortes Tools Help الاتور: الموري(10.77.244.198)certsry/certrqad.asp	موذج طلب الشهادة المتقدمة، ان لموذج طلب الشهادة لمتقدمة. کا تا با الاعتلال الاعتلال
ttp://10.77.244.198/certsrv/certrgad.asp فر على إنشاء طلب وإرساله إلى المرجع المصدق هذا . ينقلك هذا إلى Microsoft Certificate Services - Microsoft Internet Explorer Edit Vers Favorites Took العلي	في صفحة طلب الشهادة المتقدمة، ان نموذج طلب الشهادة لمتقدمة. ◙ ₪ ₪ الاطلا
للمحمد المحمد المحم المحمد المحمد المحمد المحمد المحمد المحمد المحمد المحمد المحمد المحم المحمد المحمد المحمد المحمد المحمد المحم محمد المحمد المحم المحمد المحمد المحمد المحمد المحمد المحمد المحمد ا	في صفحة طلب الشهادة المتقدمة، ان موذج طلب الشهادة لمتقدمة. الاقتتاع الاقتتاع الاقتتاع

Submit a certificate request by using a base 64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #116.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrolment station. Note: You must have an enrolment agent certificate to submit a request on behalf of another user.

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.

Internet

Microsoft Certi	ficate Services - Microsoft Internet Explorer		
File Edit View	Pavorites Tools Help	-	
Address 🔕 http://10). 77. 244. 196/certsrv/certroma.asp		💌 🔁 Go 🚽
Microsoft Certifi	cate Services wheleas		Home
Advanced Ce	rtificate Request		
Certificate Tem	date:		
Key Options:	Basic EFS V Basic EFS User		
CSP	Create new key set Ouse existing key set Microsoft Enhanced Cryptographic Provider v1.0		
Key Usage:	Exchange		
Key Size:	1024 Min: 384 (common key size: <u>\$12,1924,2248,4998,8552,15294</u> .)		
	Automatic key container name OUser specified key container name		
	Mark keys as exportable Export keys to file		
	Enable strong private key protection		
	Store certificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root GA's certificate. You must be an administrator to generate or use a key in the local machine store.		
Additional Optio	05		
Request Format:	CMC OPKCS10		
Hash Algorithm	SHA-1 Confy used to sign request.		
	Save request to a file		
Attributes:			
Done Done			 Internet

6. قم بتكوين كافة الحقول الضرورية الأخرى وانقر فوق ارسال

	ېرسان.
Microsoft Certificate Services - Microsoft Internet Explorer	
Ne Edit View Pavorites Tools Help	
🔇 Back + 🕥 - 🖹 🗟 🐔 🔎 Search 👷 Pavortes 🤣 🎯 🏂 🖼 🖄	
60+55 🍓 http://10.77.294.198/centsrv/centroma.asp	💌 🔁 😡
Create new key set	
CSP: Microsoft RSA SChannel Cryptographic Previder 💌	
Key Usage:	
Key Size: 1024 Min: 304 (common key size: 512 1028 2048 6085 5192 15384)	
Automatic key container name	
Mark keys as exportable	
Export keys to file	
Enable strong private key protection	
State centricate in the local computer centricate store Stores the certificate in the local computer atore instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.	
Additional Options:	
Request Format: OCMC	
Hash Algorithm: SHA-1 Contract and the sign request.	
Save remeat to a file	
Attributes:	
Friendly Name:	
Submit >	
	(A) Internet

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

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	At
Address a http://10.77.244.190/oertsrv/certfinsh.asp	💌 🄁 Go
Manual Carlo ata Sariana windana	Alama 🖄
MHERESUM CONTINUES OF WITHOUS	nome
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
8)	😨 Internet

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

nded purpose:	<all></all>		
sonal Other Pe	ople Intermediate Certification	Authorities Truste	d Root Certification
Issued To	Issued By	Expiratio	Friendly Name
······································	wireless	1/25/2009 <	None>
nport E	xport Remove		Advanc
nport E	export Remove		Advanc
nport E	xport Remove		Advanc
nport E rtificate intendec rrypting File Syst	em		Advanc

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

Connect to 10.77.	244.198
Connecting to 10.77.2	244.198
User name:	🛃 wireless\user2
Password:	••••••
	Remember my password
	OK Cancel

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.
B Microsoft Certificate Services - Microsoft Internet Explorer	
Min. Edit Wass Preventions Tools Help	
Address Whitpol/10.77.244.196/centsrv/centcarc.asp	🐱 🔁 🐱
Alterosoft Contraste Service Vervices	Home
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, instal this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Current (wireless)	
Encoding method:	
ODER CONTRACTOR	
© Base 64	
Download CA certificate chain	
Download latest base CRI	
Download latest delta CRL	
	(M
	Tobaccat

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



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

Cert	tificate Import Wizard	×
G	Certificate Store Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for Automatically select the certificate store based on the type of certificate	
	O Place all certificates in the following store Certificate store: Browse	
-		

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

	الاستيراد.
Certificate Import Wizard	
	Completing the Certificate Import Wizard Vou have successfully completed the Certificate Import wizard. You have specified the following settings: Certificate Store Selected Automatically determined by t Content Certificate
	< Back Finish Cancel

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:

rtificates				?
tended purpose: <all></all>				~
Intermediate Certification Au	thorities Trusted Root C	ertification Aut	horities Trusted Pub	< >
Issued To	Issued By	Expiratio	Friendly Name	-
VeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 3	
VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 3	
VeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 4	
VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 1	
VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 4	
VeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 1	
EE wireless	wireless	1/23/2013	<none></none>	
Wireless-CA	Wireless-CA	12/18/2012	<none></none>	in the second se
Xcert EZ by DST	Xcert EZ by DST	7/11/2009	Xcert EZ by DST	~
Import Export Certificate intended purpose	Remove		Advan	ced
<ali></ali>			View	
				se

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.

<u>تكوين EAP المحلي على WLC</u>

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

1. انقر على **التأمين > EAP**

Vic2006 - Microsoft Inter Edit. View Pavorites 1	net Explorer
 cisco	Sage Configuration Eing Legaut Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
AAA	Call Station ID Type IP Address
Authentication Authentication Accounting TACACS+ LDAP Local Net Users	Use AES Key Wrop (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Network User Management Server Index Server Address Port IPSec Admin Status
MAC Filtering Disabled Clients User Login Policies AP Policies	
Priority Order Access Control Lists Wireless Protection	
folicies Web Auth Advanced	
	حت 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 **Idap**. ينقلك ذلك إلى توصيفات EAP المحلية التي تنشأ على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

Wic2006 - Microsoft Inter Ple Edit View Pavorites T	net Explorer ools Help							
ababa						Sage Co	nfiguration <u>P</u> ing	Logout Befresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EAP Profile	s≻New					< Back	Apply
AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Cocol EAP General	Profile Name		ld ap					
Profiles EAP-FAST Parameters Authentication Priority								
▶ Priority Order								
Access Control Lists								
 Wireless Protection Policies 								
▶ Web Auth								
▶ Advanced								
() Done							۵.	Internet

5. انقر على ملف تخصيص **Idap** 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.

Wic2006 - Microsoft Inter	rnet Explorer							
	Tools Help					Sage Co	infiguration <u>P</u> i	ng Logout <u>R</u> efresh
CISCO	MONITOR	WLANS CONTROLLER	W]RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EAI	P Profiles	LEAP	CAP-PAST	EAP-TLS	PEAP	New	Apply
Ceneral Authentication Accounting TACACS+ Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Idae						•	
 Local EAP General Profiles EAP-FAST Parameters Authentication Priority 								
E Priority Order								
Access Control Lists								
Wireless Protection Policies								
Web Auth								
▶ Advanced								
 a) 	_						- A -	Internet

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 وشهادة العميل كأسلوب مصادقة EAP المحلي.تمكين خانات الاختيار المجاورة للشهادة المحلية المطلوبة وشهادة الاختيار المطلوبة.أختر بائع كمصدر شهادات لأن هذا المستند يستخدم خادم CA لجهة خارجية.قم بتمكين خانة الاختيار المجاورة للتدقيق مقابل شهادات لأن هذا المستند يستخدم خادم CA لجهة خارجية.قم بتمكين خانة الاختيار المجاورة للتدقيق مقابل شهادات لأن هذا المستند يستخدم خادم CA لجهة خارجية.قم بتمكين خانة الاختيار المجاورة للتدقيق مقابل 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 الموجودة على وحدة التحكم.إذا كنت تريد التحقق من ضحة الاسم الشائع (CN) في الشهادة الواردة مقابل الموجودة الموجودة على وحدة التحكم، فتحقق من خانة الاختيار (CN) في الشهادة الواردة مقابل الموجودة على وحدة الحكم.إذا كنت تريد التحقق من خانة الاختيار وCN) في الشهادة الوارد لا تزال صالحة ولم تنتهي 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 ضادة الإعداء الورد لا تزال صالحة ولم تنتهي صلاحيتها، تحقق من خانة الاختيار التحقق من صحة تاريخ الشهادة.ملاحظة: يتم التحقق من ضاد شهادة الجاز ولي من صحة تاريخ الشهادة مقابل وقت UTC (GMT) الحالي الذي تم تكوينه على وحدة التحكم. يتم تجاهل إزاحة المنطقة الشهادة مقابل وقت UTC (GMT) الحالي الذي تم تكوينه على وحدة التحكم. يتم تجاهل إزاحة المنطقة الرمنية.طقطقة الرمنية.طقطقة



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

wic2006 - Microsoft Inter	rnet Explorer							
le Edit View Pavorites T	Tools Help							4
cisco	MONITOR WEANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Logout Hefres
Security	Local EAP Profile	10	11,122200	geoord 1		0200000	New	Apply
	Readily Maria							
General	Ideo		EAP EA	I I I I I I I I I I I I I I I I I I I	EAP-ILS	PEAP		
Authentication	Look .		L 2				-	
Accounting								
LDAP								
Local Net Users MAC Filtering								
Disabled Clients								
AP Policies								
Local EAP								
General								
EAP-FAST Parameters Authentication Priority								
Priority Order								
Access Control Lists								
Wireless Protection Policies								
Web Auth								
Advanced								
Dana							A	- to

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 ي**طبق**.

a wic2006 - Microsoft Intern	et Explorer		
He Edit view Pavorites To	us Hep		Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS CONTROLLER WIRELESS		COMMANDS HELP
Security	EAP-FAST Method Parameters	\bigcirc	Apply
T AAA General	Server Key (in hex)	****	
RADIUS Authentication	Confirm Server Key	••••	
IN TACACS+	Time to live for the PAC	10 days	
NAC Filtering	Authority ID (in hex)	436973636f	
User Login Policies AP Policies	Authority ID Information	Cieco A-ID	
T Local EAP	Anonymous Provision	Enabled	
Profiles EAP-FAST Parameters Romantication Princip		\bigcirc	
E Priority Order			
Access Control Lists			
F Wireless Protection Policies			
E Web Auth			
E Advanced			
0			🚔 🖷 Internet

<u>تكوين WLC مع تفاصيل خادم LDAP</u>

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 DN OU=Idapuser الأساسي، DC=Wireless، DC=COM.يتم شرح المزيد من التفاصيل حول OU، بالإضافة إلى تكوين المستخدم، في قسم <u>إنشاء مستخدمين في وحدة التحكم بالمجال</u> 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 <u>إستخدام LDP لتحديد سمات المستخدم</u> 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

								لمعلومات:
wic2006 - Microsoft Inte	rnet Explorer							
File Edit View Favorites	Tools Help							
aludo						Sage Co	nfiguration Eing	Logout Refresh
CISCO	MONITOR WU	INS CONTROLLER	WIRELESS :	SECURITY	MANAGEMENT	COMMANDS	HELP	
CISCO Security CAAA General CAAPUUS Authentication Accounting TACACS+ LOAP Local Net Users MAC Fitering Disabled Clients User Login Policies AP Policies E Local EAP E Priority Order E Access Control Lists Wireless Protection Policies E Web Auth E Advanced	MONITOR WLA Server Index Server Index Server Address Port Number User Base DN User Attribute User Object Ty Server Mode Server Timeoul Enable Server 3	NIS CONTROLLER	WIRELESS 2244.198 depuser,DC=wirel ccountName in seconds	ESS, DC=cor	MANAGEMENT		HELP < Back	Apply
Done								Internet

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.

<u>تكوين LDAP كقاعدة بيانات خلفية ذات أولوية</u>

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

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

1. في صفحة التأمين انقر على EA**P 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.

Wic2006 - Microsoft Intern File File View Favorites To	et Explorer vis Helo								
ll							Saye Co	nfiguration Ping	Logout Befresh
cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Priority Or	rder > Lo	cal-Auth		\bigcirc	-			Apply
Ceneral General	User Crede	entials							
AADIUS Authentication Accounting Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	LOCAL LDA#	*		P wn					
Ceneral Profiles RRP-FAST Parameters Authentication Priority									
E Priority Order									
E Access Control Lists									
Wireless Protection Policies									
I: Web Auth									
Rdvanced									
- E								🙆 🍏 D	vternet

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.
wic2006 - Microsoft Inter	net Explorer								
File Edit View Favorites 1	Fools Help								
ahaha									Ping Logout Befrash
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Priority O	rder > L	o-cal-Auth						Apply
 ♥ AAA General ♥ RADEUS Authentication Accounting № TacACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies 	User Cred	entials		p wn					
T Local EAP General Profiles EAP-PAST Parameters Authentication Priority									
E Priority Order									
E Access Control Lists									
F Wireless Protection Policies									
E Web Auth									
F Advanced									
()								1 1 14	🕽 🔿 Internet

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 الصلا

<u>تكوين WLAN على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام مصادقة EAP المحلية</u>

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 WPA/ WPA2.
- 4. في صفحة تكوين أمان شبكة WLAN، انقر فوق علامة التبويب **خوادم AAA**. في صفحة خوادم AAA، قم بتمكين أسلوب مصادقة EAP المحلي واختر **Idap** من المربع المنسدل الذي يتوافق مع معلمة اسم ملف تعريف EAP. هذا هو ملف تعريف EAP المحلي الذي تم إنشاؤه في هذا المثال.

Wic2006 - Microsoft Inte	ternet Explorer	
	Sage Configuration Ping Legout B MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	fresh
WLANS WLANS WLANS IN Advanced	VLAND > Edit < Back	a di seconda di s
100 -		

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

WE Note Microsoft internet Export a E& Yew Paretes Tolk Hep			بق.
CISCO MONITOR WEAKS CONTROLLER WIFELESS SECURITY MANAGEMENT COMMANDS HEAR VILANS WLANS - Edit Apply * WLANS WLANS - Edit Apply * WLANS WLANS - Edit Apply * WLANS Security Qos Advanced	WE2006 - Microsoft Int le Edit View Favorites	ternet Explorer Tools Help	
CISCO MONITOR WANS CONTROLLER WIPELESS SECURITY MANAGEMENT COMMANDS HEIP	ahaha	Sage Configuration Bing	Logout Befre
VLANS VLANS <th< td=""><td>CISCO</td><td>MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP</td><td></td></th<>	CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
	WLANS WLANS WLANS Advanced	WLANS > Edit C Back General Security QoS Advanced Loyer 2 Layer 3 AAA Servers Select AAA servers below to override use of default servers on this WLAN Radius Servers LDAP Servers Authentication Servers Accounting Servers Server 1 None None Server 1 Server 1 None None Server 2 None None Server 3 None None Server 3 None None Server 3 None None Server 3 None Server Local EAP Authentication Server Server None Server Server Server Server 3 None Server Server Local EAP Authentication Server Server Server Local EAP Authentication Server Server Server Read	Apply

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

							مىل.
wic2006 - Microsoft Inte	rnet Explorer						
e Edit View Favorites	Tools Help						
		CO17001170 101		MANAGEMENT	001114	ve computation Eng	Logout Betre
CISCO	MONTIOR WEAKS	CONTROLLER W	RELESS DECORDITY	MENAGEMENT	COMMO	NDS HEDP	
VLANs	WLANs						New
WEANS					Admin		
WLANs	Profile Name	Туре	WLAN SSID		Status	Security Policies	_
Advanced	Ideouser	WLAN	Idao		Enabled	002.1X	
	Lasherana.	The second se	and b		crossred	CONC. LEVI	-
							_
00						🙆 🐡 Inte	rnet

<mark>تکوین خادم LDAP</mark>

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 OU **Idapuser** 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

						فق.	مواه
Ne	w Object ·	• Organizal	ional Unit			2	×Ц
	Ø	Create in:	Wireless.com/				
	N <u>a</u> me:						
	Idapuser						
1							
				0	IK	Cancel	

الآن يتم إنشاء OU **Idapuser** 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



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).

New Object - User	
Create in: Wireles	s.com/ldapuser
<u>F</u> irst name:abcd	
Last name:	
Full ngme: abcd	
User logon name:	
user2	@Wireless.com
User logon name (pre-Windows	2000):
WIRELESS\	user2
	< Back Next > Cancel

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

Password:	•••••	
Confirm password:	•••••	
User <u>m</u> ust change	e password at next logon	
User cannot char	nge password	
Password never e	xpires	
Account is disable	bd	

4. انقر فوق إنهاء.يتم إنشاء مستخدم جديد user2 ضمن OU Idapuser. مسوغات المستخدم هي:اسم المستخدم: user2كلمة المرور: **الكمبيوتر المحمول** 123

ew Object	- User				×
S	Create in:	Wireless.c	om/Idapuser		
When yo	u click Finish	, the following	g object will be	e created:	
Full name	e: abcd				<u>^</u>
User logo	on name: use	r2@Wireless	com		
The pass	sword never e	expires.			
1					T
			< <u>B</u> ack	(Finish)	Cancel

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

<u>تكوين المستخدم للوصول إلى LDAP</u>

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 Edit.msc** 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 > CN =خدمة الدليل. انقر بزر الماوس الأيمن فوق حاوية وحدد **خصائص** من قائمة السياق.

🐗 ADSI Edit				
SEle Action Yew Win	dow Help			
⇔ ⇒ 🗈 🖬 🗙 🗳	0 🗟 😫 💷			
📣 ADSI Edit		 Name	Class	Distinguished
Domain [tsweb-lapt. Wire Configuration [tsweb-lap CN=Configuration,D CN=DisplaySpec CN=Extended-R CN=Extended-R CN=ForestUpda CN=CN=NTDS Quota CN=NTDS Quota CN=Partitions CN=Physical Loc CN=Physical Loc CN=Stress CN=Window CN=Sites CN=Window CN=Sites CN=Window CN=Sites CN=Window CN=Sites CN=Window CN=Sites CN=Window CN=Sites CN=Window CN=Sites CN=Window CN=Sites	eless.com] ct.Wireless,DC=com ifiers ights tes indConfig as ations rvices ices ey Services s NT Move New Connection from Here New Mindow from Here Rename	CN=Query-Policies	container	CN=Query-P
Opens the properties dialog box	Refresh			
	Export List	,		
	Properties			

3. في الإطار C**N=خصائص خدمة الدليل**، انقر فوق سمة DSheuristics تحت حقل السمة واختر Edit. في نافذة محرر سمة السلسلة لهذه السمة، أدخل القيمة 00000 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 0" LDAP." أو عدم وجود حرف سابع يعني تعطيل عمليات LDAP المجهولة. **تعيين الحرف السابع إلى** "2" يمكن ميزة الربط

					المجهول.
CN=Directory Service Pro	operties		<u>?</u> ×		- •
Attribute Editor Security				Class	Distingu
Show mandatory attrib	outes			container	CN=Qu
Show optional attribut	es				
Show only attributes th	hat have values				
Attributes:					
Attribute	Suntax	Value	<u> </u>		
directReports displayName displayNamePrintable distinguishedName dSASignature dSCorePropagationD dSHeuristics extensionName flags fromEntry frsComputerReferenc fRSMemberReferenc fSMOBoleOwner	String Attribute Attribute: dSHee Value: COCCCC2 Clear Distinguished Distinguished Distinguished	<not set=""> <not set=""> <not set=""> <not set=""></not></not></not></not>		ОК	Cancel
Edit		Cancel			

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 "0010000". إذا كانت القيمة الحالية أقل من سبعة أحرف، ستحتاج إلى وضع أصفار في الأماكن غير المستخدمة: "001" ستصبح "001000".

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 وأجهزة 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.

cd Properties	
Published Certificates Environment Session General Address	8 Member Of Dial-in Object Security ns Remote control Terminal Services Profile COM+ Account Profile Telephones Organization
S abod	
Eirst name:	abcd Initials:
Last name:	
Digplay name:	abcd
Description:	
Offi <u>c</u> e:	
<u>I</u> elephone number:	
E- <u>m</u> ail:	
∭eb page:	Other
	OK Cancel Apply

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

Select Users, Computers, or Groups	<u> </u>
Select this object type:	
Users, Groups, or Built-in security principals	<u>O</u> bject Types
From this location:	
Wireless.com	Locations
Enter the object names to select (examples):	
ANONYMOUS LOGON	<u>C</u> heck Names
Advanced	OK Cancel

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.

abcd Properties	<u>? ×</u>
Environment Sessions Remote control Terminal Servi General Address Account Profile Telephone Published Certificates Member Of Dial-in Ob	ces Profile COM+ es Organization oject Security
<u>G</u> roup or user names:	
Account Operators (WIRELESS Account Operators)	
ANONYMOUS LOGON	
Authenticated Users	Conservation of the second sec
Cert Publishers (WIRELESS\Cert Publishers)	-
A <u>d</u> d	<u>R</u> emove
Permissions for ANONYMOUS LOGON Allow	Deny
Full Control	
Read 🗹	
Write 🗖	
Create All Child Objects	
Delete All Child Objects	
Allowed to Authenticate	
For special permissions or for advanced settings, click Advanced.	Advanced
OK Cancel	

<u>منح إذن محتويات القائمة في OU</u>

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 OU "Idapuser". أتمت هذا steps in order to حققت هذا:

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



Idapuser Properties	? ×
General Managed By Object Security COM+ Group Policy	
Group or user names:	
Account Operators (WIRELESS \Account Operators)	<u> </u>
Administrators (WIRELESS Administrators)	
🛃 Authenticated Users	
🖅 Domain Admins (WIRELESS\Domain Admins)	
Enterprise Admins (WIRELESS\Enterprise Admins)	-1
Add <u>B</u> em	ove
Permissions for Account Operators Allow Den	v l
Full Control	
Read 🗌 🗖	
Write 🗖 🗖	
Create All Child Objects	
Delete All Child Objects	
Generate Resultant Set of Policy(Logging)	-
For special permissions or for advanced settings, Advanced.	iced
OK Cancel	Apply

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

Advanced Security Settings for Idapuser	
Select User, Computer, or Group	? ×
Select this object type:	
User, Group, or Built-in security principal	Object Types
From this location:	
Wireless.com	Locations
Enter the object name to select (<u>examples</u>):	
ANONYMOUS LOGON	<u>C</u> heck Names
Advanced	OK Cancel

- 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.

Permission Entry for Idapuser		<u>?</u> ×
Object Properties		
Name: ANONYMOUS LOGON		<u>C</u> hange
Apply onto: This object only		-
Permissions:	Allow	Deny
Full Control List Contents Read All Properties Write All Properties Delete Delete Subtree Read Permissions Modify Permissions Modify Owner All Validated Writes All Validated Rights Create All Child Objects		
Apply these permissions to objects an containers within this container only	id/ior	Clear All
	οκ	Cancel

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 LDA 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

شجره.
Help

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

Midap://tsweb-lapt.Wireless.com/DC=Wireless,DC=com		_ 🗆 🗵
Connection Browse View Options Utilities		Help
Tree View BaseDN: DU-Idapuser.do-wireless.do-com Cancel	X 3556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 13556.1.4.619; 1.2.840.113556.1.4.841; 1.2.840.113556.1.4.970; 13556.1.4.805; 1.2.840.113556.1.4.971; 1.2.840.113556.1.4.1339; 13556.1.4.1338; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 13556.1.4.1340; 1.2.840.113556.1.4.1413; 2.16.840.1.113730.3.4.9; 1.113730.3.4.10; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1852; 33556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1852; 33556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: 3; 2; 13556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: 3; 2; 13> highestCommittedUSN: 16926; 4> supportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1> dnsHostName: tsweb-lapt.Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 1> serverName: CN=TSWEB-LAPT,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configu ,DC=Wireless,DC=com; 3> supportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4. 1.2.840.113556.1.4.1791; 1> isSilobalCatalogReady: TRUE; 1> isGlobalCatalogReady: TRUE; 1> domainFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1> forestFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1> domainControllerFunctionality: 2 = [DS_BEHAVIOR_WIN2000];	ration .1670;
Ready		

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:

🚰 ldap://tsweb-lapt.Wireless.com/DC=Wireless,DC=com		×
Connection Browse View Options Utilities	Be	łp –
Connection Browse View Options Utilities ⊡-OU=Idapuser,dc=wireless,dc=con ⊡-No children UN=abcd,OU=Idapuser,DC=Wireless,DC=com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=Wireless,DC=Com UN=Abcd,OU=Idapuser,DC=W	Line: 1> whenCreated: 1/27/2008 21:56:30 India Standard Time India Standard Time; 1> whenChanged: 1/27/2008 22:2:15 India Standard Time India Standard Time; 1> displayName: abcd; 1> uSNCreated: 16917; 1> uSNChanged: 16923; 1> name: abcd; 1> objectGUID: db0ad755-2e36-493d-9325-3429aa907626; 1> userAccountControl: 0x10200 = (UF_NORMAL_ACCOUNT UF_DONT_EXPIRE_PASSWD); 1> badPwdCount: 0; 1> codePage: 0; 1> countryCode: 0; 1> lastLogoft: 0; 1> absLogoft: 0; 1> pwdLastSet 1> primaryGroupID: 513; 1> objectSid: S-1-5-21-3543678607-2589429210-3156366500-1116; 1> accountExpires: 1> sAMAccountName: user2; 1> sAMAccountName: user2;	1 4 X
	CN=Person, CN=Schema, CN=Configuration, DC=Wireless, DC=com;	
		•
Ready		11.

في هذا المثال، لاحظ الحقول المحاطة على اليمين.

- 6. كما هو مذكور في قسم <u>تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مع تفاصيل</u> قسم<u>خادم للح</u> 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).

<u>تكوين عميل لاسلكي</u>

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

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

retet 🔹 💽 🔀
New
Modify
Remove
Activate
Import
Export
Sean
Scart
Order Profiles

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 حملا

		luap
Profile Management		2 🔀
General Security Advance	ed	
Profile Settings		_
Profile Name:	Idapuser	
Client Name:	CLIENT1	
Network Names	\frown	
SSIDT	Idap	in states and
SSID2:		
SSID3:		
	·	
	ок	Cancel

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

تكوين.

Configure EAP-FAST
EAP-FAST Authentication Method MSCHAPv2 User Name and Password Configure GTC Token/Password Configure MSCHAPv2 User Name and Password Configure TLS Client Certificate Manage
Use Any PAC Belonging to the Same Group
Allow Automatic PAC Provisioning
Use Machine Information for Domain Logon
OK Cancel

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

onfigure TLS Client Certificate	· · · · · · · · · · · · · · · · · · ·
✓ Validate Server Identity	
Trusted Root Certification Authorities	
wireless	✓
Select a Certificate	
1234 [Issued by: wireless 1/26/2008]	~
Server/Domain Name	
Wireless.com	
Login Name	
user2	
	OK Cancel

يتم إنشاء ملف تعريف العميل اللاسلكي.

<u>التحقق من الصحة</u>

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

- 1. قم بتنشيط SSID LDAP 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** WLC نعن in order to idap 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 Idap** 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 EAP المحلية ناجحة أم لا، حدد الأمر 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_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_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

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

Reading Client Certificate handshake

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) Received success event

• 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 :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

_

:EAP-FAST

More-- or (q)uit--

<server <hidden<="" key="" th=""></server>
TTL for the PAC 10
Anonymous provision allowed No
Authority Information Cisco A-ID

<u>استكشاف الأخطاء وإصلاحها</u>

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 •

<u>معلومات ذات صلة</u>

- <u>مصادقة EAP-FAST مع وحدات تحكم الشبكة المحلية اللاسلكية ومثال تكوين خادم RADIUS الخارجي</u>
 - 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
 - <u>دليل تكوين وحدة تحكم الشبكة المحلية (LAN) اللاسلكية من Cisco تكوين حلول الأمان</u>
 - <u>دليل تكوين وحدة التحكم في شبكة LAN اللاسلكية من Cisco إدارة برامج وحدة التحكم وتكويناتها</u>
 - <u>مصادقة EAP باستخدام مثال تكوين وحدات التحكم في الشبكة المحلية اللاسلكية (WLC)</u>
 - <u>تصميم وحدة التحكم في شبكة LAN اللاسلكية (WLC) والميزات المتداولة</u>
 - <u>EAP-FAST مع مصادقة Cisco Secure Services Client</u>
 - <u>الأسئلة المتداولة حول وحدة التحكّم في الشبكة المحلية اللاسلكية (WLC)</u>
 - <u>أخطاء وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية (WLC) ورسائل النظام المتداولة</u>
 - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما