

# دليل لاثم في (WPA) يمحمل Wi-Fi لوصو نم ةدحوم لةيكل لاللة كةبش لال نيوكت Cisco

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[دعم WPA و WPA2](#)

[Network Setup \(إعداد الشبكة\)](#)

[تكوين الأجهزة لوضع WPA2 مؤسسي](#)

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

[شكلت ال WLAN ل WPA2 مشروع أسلوب التشغيل](#)

[تكوين خادم RADIUS لمصادقة وضع WPA2 المؤسسي \(EAP-FAST\)](#)

[تكوين العميل اللاسلكي لوضع التشغيل WPA2 Enterprise](#)

[تكوين الأجهزة لوضع WPA2 الشخصي](#)

[استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

## المقدمة

يصف هذا وثيقة كيف أن يشكل (WPA (Wi-Fi Protected Access في cisco شبكة لاسلكية موحدة.

## المتطلبات الأساسية

### المتطلبات

تأكد من أن لديك معرفة أساسية بهذه الموضوعات قبل محاولة هذا التكوين:

- WPA
- حلول أمان شبكة LAN اللاسلكية (WLAN) ملاحظة: راجع [نظرة عامة على أمان شبكة LAN اللاسلكية من Cisco](#) للحصول على معلومات حول حلول أمان Cisco WLAN.

### المكونات المستخدمة

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

- نقطة الوصول في الوضع (LAP Lightweight) سلسلة Cisco 1000
  - وحدة التحكم في شبكة LAN اللاسلكية (WLC) طراز 4404 من Cisco التي تشغل البرنامج الثابت 4.2.61.0
  - مهائى عميل Cisco 802.11a/b/g الذي يشغل البرنامج الثابت 4.1
  - أداة (Aironet Desktop Utility) (ADU) التي تشغل البرنامج الثابت 4.1
  - خادم ACS الآمن من Cisco، الإصدار 4.1
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## دعم WPA و WPA2

تتضمن شبكة Cisco اللاسلكية الموحدة دعم لشهادات تحالف WPA و Wi-Fi WPA2. وقد طرح تحالف الواي - فاي WPA في عام 2003. تم تقديم WPA2 من قبل تحالف Wi-Fi في عام 2004. يلزم أن تكون جميع منتجات Wi-Fi المعتمدة لـ WPA2 قابلة للتشغيل البيئي مع المنتجات المعتمدة لـ Wi-Fi لـ WPA.

يقدم WPA و WPA2 مستوى عال من الضمان للمستخدمين النهائيين ومسؤولي الشبكة بأن بياناتهم ستبقى خاصة وأن الوصول إلى شبكاتهم سيكون مقصوراً على المستخدمين المخولين. وكل منهما له طرق عمل شخصية وأسلوب عمل خاص بالمؤسسات تفي بالاحتياجات المتميزة لجزأي السوق. يستخدم وضع المؤسسة لكل منها IEEE 802.1X و EAP للمصادقة. يستخدم الوضع الشخصي لكل واحد مفتاح مشترك مسبقاً (PSK) للمصادقة. لا توصي Cisco بوضع شخصي لعمليات نشر الشركات أو الحكومات لأنها تستخدم PSK لمصادقة المستخدم. لا يكون PSK آمناً لبيئات المؤسسات.

يعالج WPA جميع نقاط الضعف المعروفة في WEP في تنفيذ تأمين IEEE 802.11 الأصلي مما يوفر حلاً آمناً فوراً لشبكات WLAN في بيئات المؤسسات والمكاتب الصغيرة/المكاتب المنزلية (SOHO) على حد سواء. يستخدم WPA TKIP للتشفير.

يمثل WPA2 الجيل التالي من تأمين Wi-Fi. إنه التطبيق البيئي من قبل تحالف Wi-Fi لمقياس IEEE 802.11i المصدق عليه. وهو يطبق خوارزمية تشفير AES الموصى بها من المعهد الوطني للمعايير والتكنولوجيا باستخدام وضع العداد مع بروتوكول مصادقة رمز رسالة توصيل مجموعات التشفير (CCMP). يسهل WPA2 التوافق مع الحكومة وفق FIPS 140-2.

### مقارنة أنواع وضع WPA و WPA2

WPA2	WPA	
<ul style="list-style-type: none"> <li>المصادقة: IEEE 802.1X/EAP</li> <li>التشفير: AES-CCMP</li> </ul>	<ul style="list-style-type: none"> <li>المصادقة: IEEE 802.1X/EAP</li> <li>التشفير: TKIP/MIC</li> </ul>	وضع المؤسسة (الأعمال والحكومة والتعليم)
<ul style="list-style-type: none"> <li>المصادقة: PSK</li> <li>التشفير: AES-CCMP</li> </ul>	<ul style="list-style-type: none"> <li>المصادقة: PSK</li> <li>التشفير: TKIP/MIC</li> </ul>	الوضع الشخصي (SOHO، المنزل/الشخصي)

في الوضع المؤسسي للتشغيل يستخدم كلا من WPA و WPA2 802.1X/EAP للمصادقة. يوفر معيار 802.1X

شبكات WLAN مصادقة قوية ومتبادلة بين عميل وخادم مصادقة. بالإضافة إلى ذلك، يوفر الطراز 802.1X مفاتيح تشفير ديناميكية لكل مستخدم ولكل جلسة عمل، مما يعمل على إزالة الأعباء الإدارية ومشكلات الأمان التي تحيط بمفاتيح التشفير الثابتة.

مع معيار 802.1X، لا يتم إرسال بيانات الاعتماد المستخدمة للمصادقة أبداً، مثل كلمات مرور تسجيل الدخول، في الخفاء أو دون تشفير، عبر الوسط اللاسلكي. في حين توفر أنواع مصادقة 802.1X مصادقة قوية للشبكات المحلية اللاسلكية، فإن TKIP أو AES مطلوبة للتشفير بالإضافة إلى 802.1X حيث أن التشفير القياسي 802.11 WEP معرض لهجمات الشبكة.

توجد عدة أنواع لمصادقة 802.1X، يوفر كل منها نهجاً مختلفاً للمصادقة مع الاعتماد على نفس الإطار وعلى EAP للاتصال بين العميل ونقطة وصول. تدعم منتجات Cisco Aironet أنواع مصادقة EAP 802.1X أكثر من أي منتجات أخرى للشبكة المحلية اللاسلكية (WLAN). تتضمن الأنواع المدعومة:

#### • [Cisco LEAP](#)

#### • [مصادقة EAP المرنة عبر الاتصال النفقي الآمن \(EAP-FAST\)](#)

• أمان طبقة النقل (EAP-TLS) (EAP)

• [بروتوكول المصادقة المتوسع المحمي \(PEAP\)](#)

• (EAP-Tunneled TLS) (EAP-TTLS)

• وحدة تعريف (EAP-SIM) (EAP-Subscriber)

ومن المزايا الأخرى لمصادقة 802.1X الإدارة المركزية لمجموعات مستخدمي الشبكة المحلية اللاسلكية (WLAN)، بما في ذلك تدوير المفاتيح القائم على السياسات وتعيين المفاتيح الديناميكية وتعيين الشبكة المحلية الظاهرية (VLAN) الديناميكية وتقييد SSID. تقوم هذه الميزات بتدوير مفاتيح التشفير.

في الوضع الشخصي للعملية، يتم استخدام مفتاح مشترك مسبقاً (كلمة مرور) للمصادقة. لا يتطلب الوضع الشخصي إلا نقطة وصول وجهاز عميل، بينما يتطلب وضع Enterprise عادةً خادم مصادقة RADIUS أو غيره على الشبكة.

يقدم هذا المستند أمثلة لتكوين WPA2 (وضع المؤسسة) و WPA2-PSK (الوضع الشخصي) في شبكة Cisco اللاسلكية الموحدة.

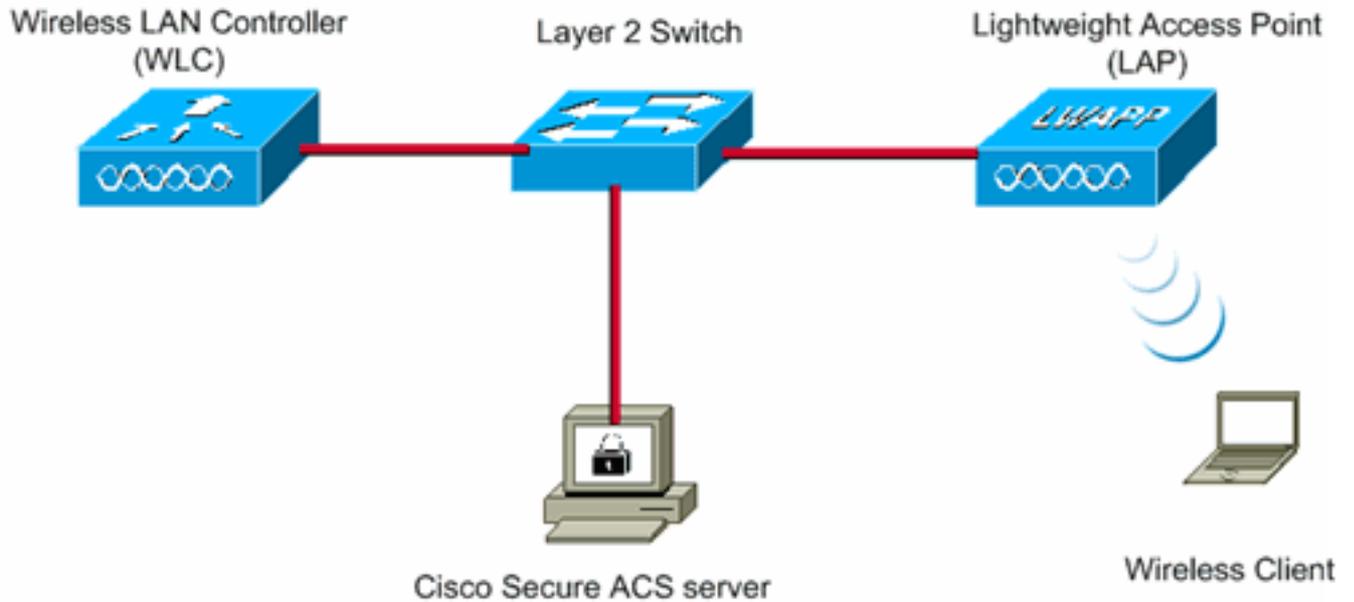
### [Network Setup \(إعداد الشبكة\)](#)

في هذا الإعداد، يتم توصيل وحدة تحكم في الشبكة المحلية اللاسلكية (WLC) من Cisco 4404 نقطة وصول من السلسلة Cisco 1000 Series من خلال محول من الطبقة 2. كما يتم توصيل خادم RADIUS الخارجي (Cisco Secure ACS) بنفس المحول. توجد جميع الأجهزة في الشبكة الفرعية نفسها. يتم تسجيل نقطة الوصول (LAP) في البداية إلى وحدة التحكم. هناك حاجة إلى إنشاء شبكتي محلية لاسلكية، واحدة لوضع WPA2 Enterprise والأخرى لوضع WPA2 الشخصي.

يستخدم EAP-FAST (SSID: WPA2-Enterprise) WLAN (WPA2-Enterprise Mode) لمصادقة العملاء اللاسلكيين و AES للتشفير. سيتم استخدام خادم ACS الآمن من Cisco كخادم RADIUS الخارجي لمصادقة العملاء اللاسلكيين.

WPA2-Enterprise الشخصي تستخدم WPA2-PSK (SSID: WPA2-PSK) WLAN للمصادقة مع المفتاح المشترك مسبقاً "WPA2-PSK".

يجب تكوين الأجهزة لهذا الإعداد:



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

## تكوين الأجهزة لوضع WPA2 مؤسسي

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

أجزت هذا steps in order to شكلت الأداة ل WPA2 مشروع أسلوب التشغيل:

1. تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة RADIUS من خلال خادم RADIUS خارجي
2. تكوين شبكة WLAN لمصادقة وضع WPA2 المؤسسي (EAP-FAST)
3. تشكيل العميل اللاسلكي لوضع WPA2 مؤسسي

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

يلزم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإعادة توجيه بيانات اعتماد المستخدم إلى خادم RADIUS خارجي. ثم يتحقق خادم RADIUS الخارجي من مسوغات المستخدم باستخدام EAP-FAST ويوفر الوصول إلى العملاء اللاسلكيين.

أتمت هذا steps in order to شكلت ال WLC لخادم خارجي RADIUS:

1. أختبرت تأمين ومصادقة RADIUS من الجهاز تحكم gui أن يعرض ال RADIUS صحة هوية نادل صفحة. ثم انقر فوق جديد لتحديد خادم RADIUS.
2. قم بتعريف معلمات خادم RADIUS على خوادم مصادقة RADIUS < صفحة جديدة. وتتضمن هذه المعلمات ما يلي: عنوان IP لخادم RADIUS، سر مشترك رقم المنفذ حالة الخادم يستعمل هذا وثيقة ال ACS نادل مع عنوان

Security

RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address 10.77.244.196

Shared Secret Format ASCII

Shared Secret \*\*\*\*\*

Confirm Shared Secret \*\*\*\*\*

Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User  Enable

Management  Enable

IPsec  Enable

3. قطعة يطبق.

### شبكة ال WLAN ل WPA2 مشروع أسلوب التشغيل

بعد ذلك، قم بتكوين شبكة WLAN التي سيستخدمها العملاء للاتصال بالشبكة اللاسلكية. سيكون WLAN SSID لوضع WPA2 مؤسسي -WPA2 مؤسسي. يعين هذا مثال هذا WLAN إلى الإدارة قارن.

أكمل هذه الخطوات لتكوين شبكة WLAN والمعلومات المرتبطة بها:

1. طقطقت WLANs من ال gui من الجهاز تحكم in order to عرضت WLANs صفحة. تسرد هذه الصفحة شبكات WLAN الموجودة على وحدة التحكم.
2. طقطقت جديد in order to خلقت WLAN جديد.
3. أدخل اسم SSID لشبكة WLAN واسم التوصيف على شبكات WLAN < صفحة جديدة. بعد ذلك، انقر فوق تطبيق. يستخدم هذا المثال -WPA2 مؤسسي كمعرف SSID.

WLANs

WLANs > New

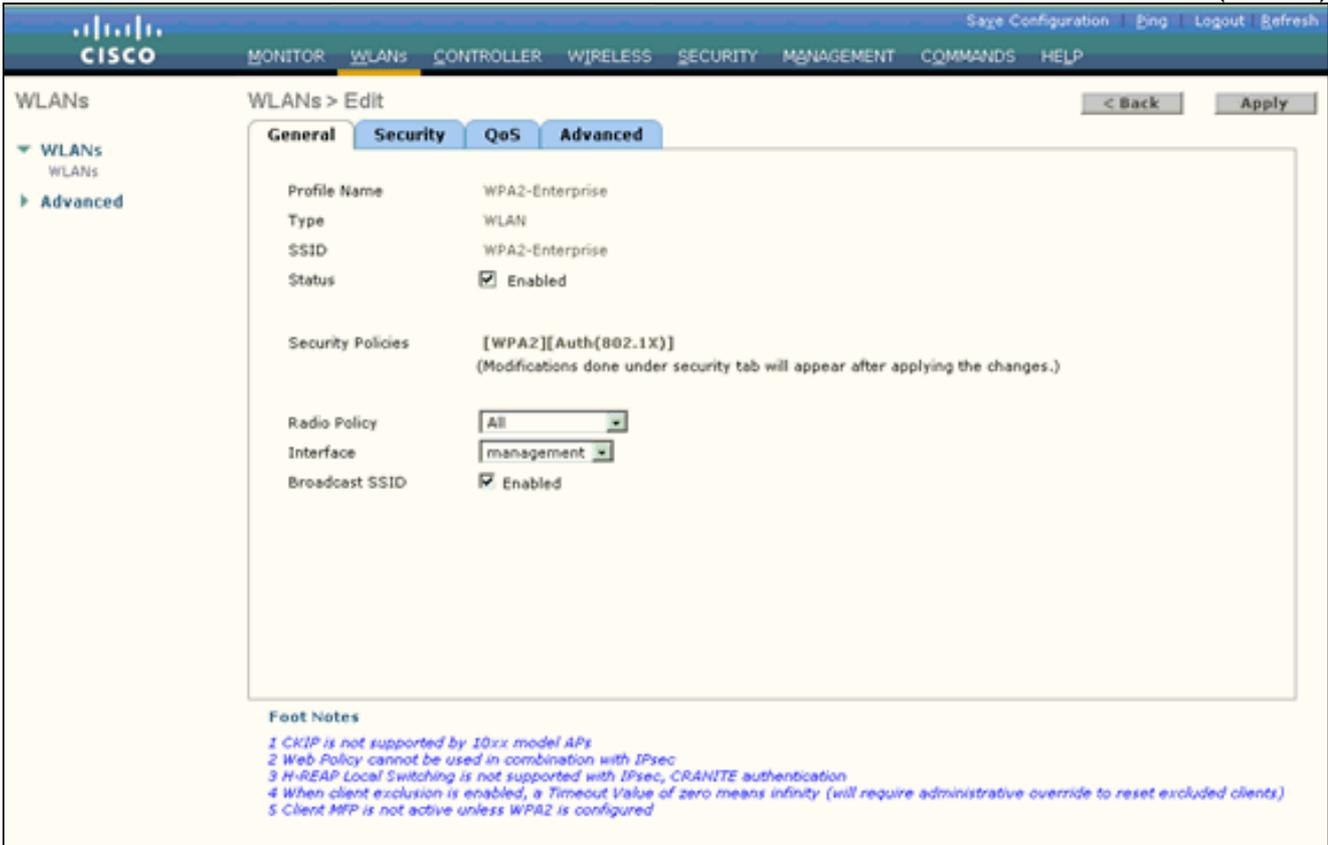
Type WLAN

Profile Name WPA2-Enterprise

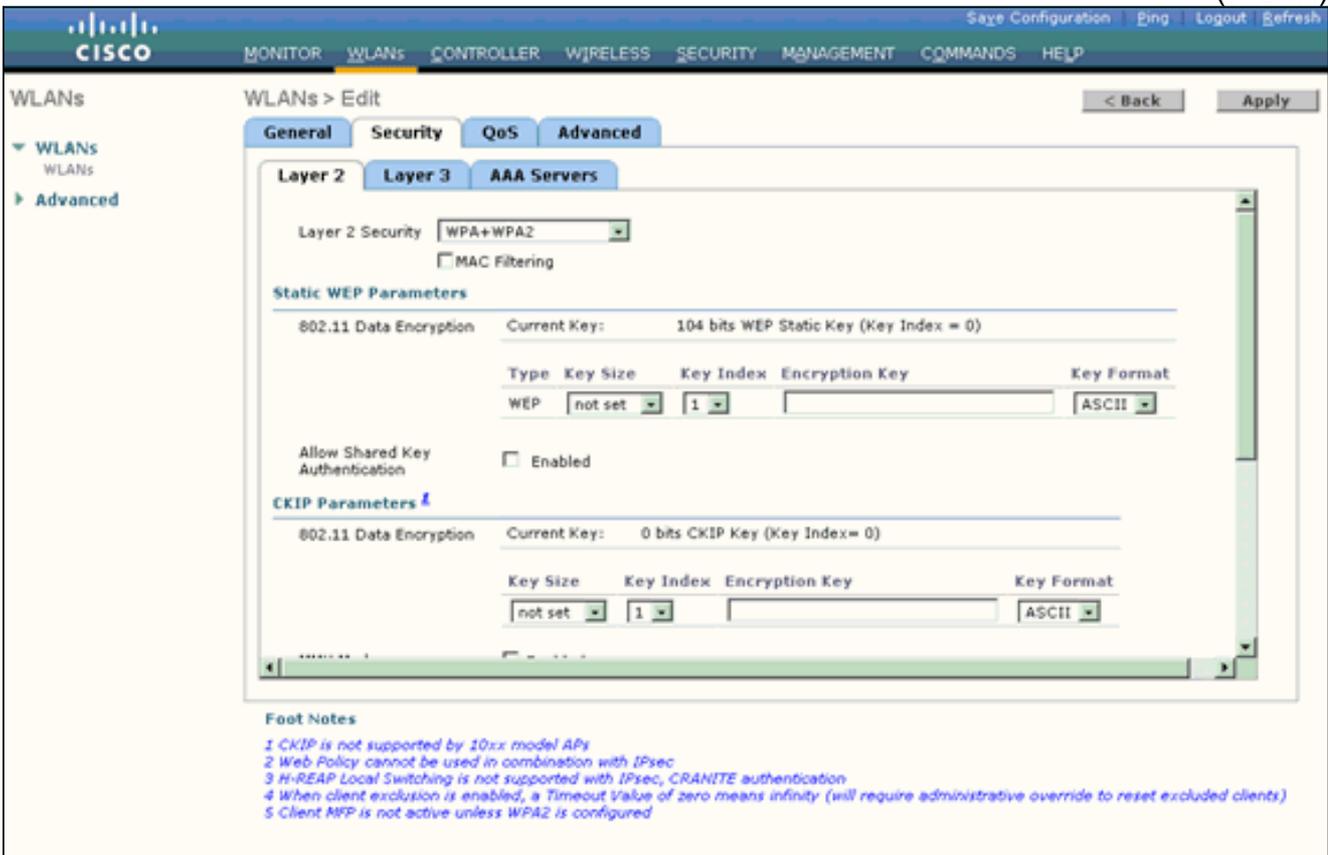
WLAN SSID WPA2-Enterprise

4. ما إن يخلق أنت WLAN جديد، ال WLAN < تحرير صفحة ل WLAN جديد يظهر. في هذه الصفحة، يمكنك تحديد معلومات مختلفة خاصة بشبكة WLAN هذه. ويتضمن ذلك السياسات العامة ونهج الأمان ونهج جودة الخدمة والمعلومات المتقدمة.

5. تحت سياسات عامة، حدد خانة الاختيار الحالة لتمكين الشبكة المحلية اللاسلكية (WLAN).



6. إذا أردت لنقطة الوصول أن تبث SSID في إطارات المنارة الخاصة بها، حدد خانة الاختيار بث SSID.  
7. انقر فوق علامة التبويب أمان. تحت تأمين الطبقة 2، اختر WPA+WPA2. هذا يمكن مصادقة WPA للشبكة المحلية اللاسلكية (WLAN).



8. انزلق إلى أسفل الصفحة لتعديل معلمات WPA+WPA2. في هذا المثال، يتم تحديد تشفير سياسة WPA2 و

The screenshot shows the Cisco WLAN configuration interface. The 'Security' tab is selected, and the '802.11 Data Encryption' section is expanded. The 'Current Key' is set to '0 bits CKIP Key (Key Index= 0)'. Below this, there are fields for 'Key Size' (set to 'not set'), 'Key Index' (set to '1'), 'Encryption Key' (empty), and 'Key Format' (set to 'ASCII'). There are also checkboxes for 'MMH Mode' and 'Key Permutation', both of which are currently disabled. The '802.1X Parameters' section shows '802.11 Data Encryption' set to 'WEP' with a 'Key Size' of '104 bits'. The 'WPA+WPA2 Parameters' section shows 'WPA Policy' disabled, 'WPA2 Policy' checked, 'WPA2 Encryption' set to 'AES' (with 'TKIP' also checked), and 'Auth Key Mgmt' set to '802.1X'. At the bottom, there are 'Foot Notes' providing additional information about CKIP, Web Policy, H-REAP, and client exclusion.

9. تحت إدارة مفتاح المصادقة، أختار 802.1x. ويتيح ذلك استخدام مصادقة 802.1x/EAP وتشفير AES للشبكة المحلية اللاسلكية (WLAN).
10. انقر فوق علامة التبويب خوادم AAA. تحت خوادم المصادقة، أختار عنوان IP الخاص بالخادم. في هذا المثال، يتم استخدام 10.77.244.196 كخادم RADIUS.

The screenshot shows the Cisco WLAN configuration interface. The 'AAA Servers' tab is selected. The 'Select AAA servers below to override use of default servers on this WLAN' section is expanded. It shows 'Radius Servers' and 'LDAP Servers'. Under 'Radius Servers', there are 'Authentication Servers' and 'Accounting Servers'. 'Accounting Servers' is checked as 'Enabled'. There are three 'Server' entries. 'Server 1' has an IP of '10.77.244.196, Port:1812' and 'None' for the accounting server. 'Server 2' and 'Server 3' have 'None' for both authentication and accounting servers. Under 'LDAP Servers', there are three 'Server' entries, all set to 'None'. The 'Local EAP Authentication' section shows 'Local EAP Authentication' disabled. At the bottom, there are 'Foot Notes' providing additional information about CKIP, Web Policy, H-REAP, and client exclusion.

11. قطعة يطبق. ملاحظة: هذا هو إعداد EAP الوحيد الذي يلزم تكوينه على وحدة التحكم لمصادقة EAP. كل

التكوينات الأخرى الخاصة ب EAP-FAST تحتاج أن تتم على خادم RADIUS والعملاء الذين يحتاجون إلى المصادقة.

## تكوين خادم RADIUS لمصادقة وضع WPA2 المؤسسي (EAP-FAST)

في هذا المثال، يتم استخدام مصدر المحتوى الإضافي الآمن من Cisco كخادم RADIUS الخارجي. أنجزت هذا steps in order to RADIUS نادل لمصادقة EAP-FAST:

1. [إنشاء قاعدة بيانات مستخدم لمصادقة العملاء](#)
2. [إضافة عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\) كعميل AAA إلى خادم RADIUS](#)
3. [تكوين مصادقة EAP-FAST على خادم RADIUS باستخدام إمداد PAC مجهول داخل النطاق ملاحظة: يمكن تكوين EAP-FAST إما بإمداد PAC غير معروف داخل النطاق أو توفير PAC داخل النطاق مصادق عليه. يستخدم هذا المثال توفير مسوغ وصول محمي \(PAC\) داخل النطاق مجهول. أحلت لمعلومات وأمثلة مفصلة على تكوين EAP FAST مع مجهول داخل النطاق يزود PAC ومصادقة داخل النطاق، \[EAP-FAST صحة هوية مع لاسلكي lan جهاز تحكم ومثال خارجي RADIUS نادل تشكيل.\]\(#\)](#)

## إنشاء قاعدة بيانات مستخدم لمصادقة عملاء EAP-FAST

أكمل هذه الخطوات لإنشاء قاعدة بيانات مستخدم لعملاء EAP-FAST على ACS. يقوم هذا المثال بتكوين اسم المستخدم وكلمة المرور لعميل EAP-FAST ك user1 و user1، على التوالي.

1. من واجهة المستخدم الرسومية (GUI) ل ACS في شريط التنقل، حدد إعداد المستخدم. قم بإنشاء مستخدم لاسلكي جديد، ثم انقر فوق إضافة/تحرير للانتقال إلى صفحة تحرير هذا المستخدم.

The screenshot shows the CiscoSecure ACS User Setup interface. The browser window title is "CiscoSecure ACS - Microsoft Internet Explorer". The address bar shows "http://127.0.0.1:1005/". The page title is "User Setup". The left sidebar contains a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is divided into two sections: "Select" and "Help". The "Select" section has a "User:" input field with "User1" entered, "Find" and "Add/Edit" buttons, and a list of users beginning with "U". Below the list are buttons for "List all users" and "Remove Dynamic Users", and a "Back to Help" button. The "Help" section contains a list of links and text explaining the User Setup functionality and notes.

2. من صفحة تحرير إعداد المستخدم، قم بتكوين الاسم والوصف الحقيقيين بالإضافة إلى إعدادات كلمة المرور كما هو موضح في هذا المثال. يستخدم هذا المستند قاعدة بيانات ACS الداخلية لمصادقة كلمة المرور.

The screenshot shows the CiscoSecure ACS User Setup web interface. The page is titled "User Setup" and is accessed via a Microsoft Internet Explorer browser. The address bar shows "http://127.0.0.1:1065/". The interface is divided into several sections:

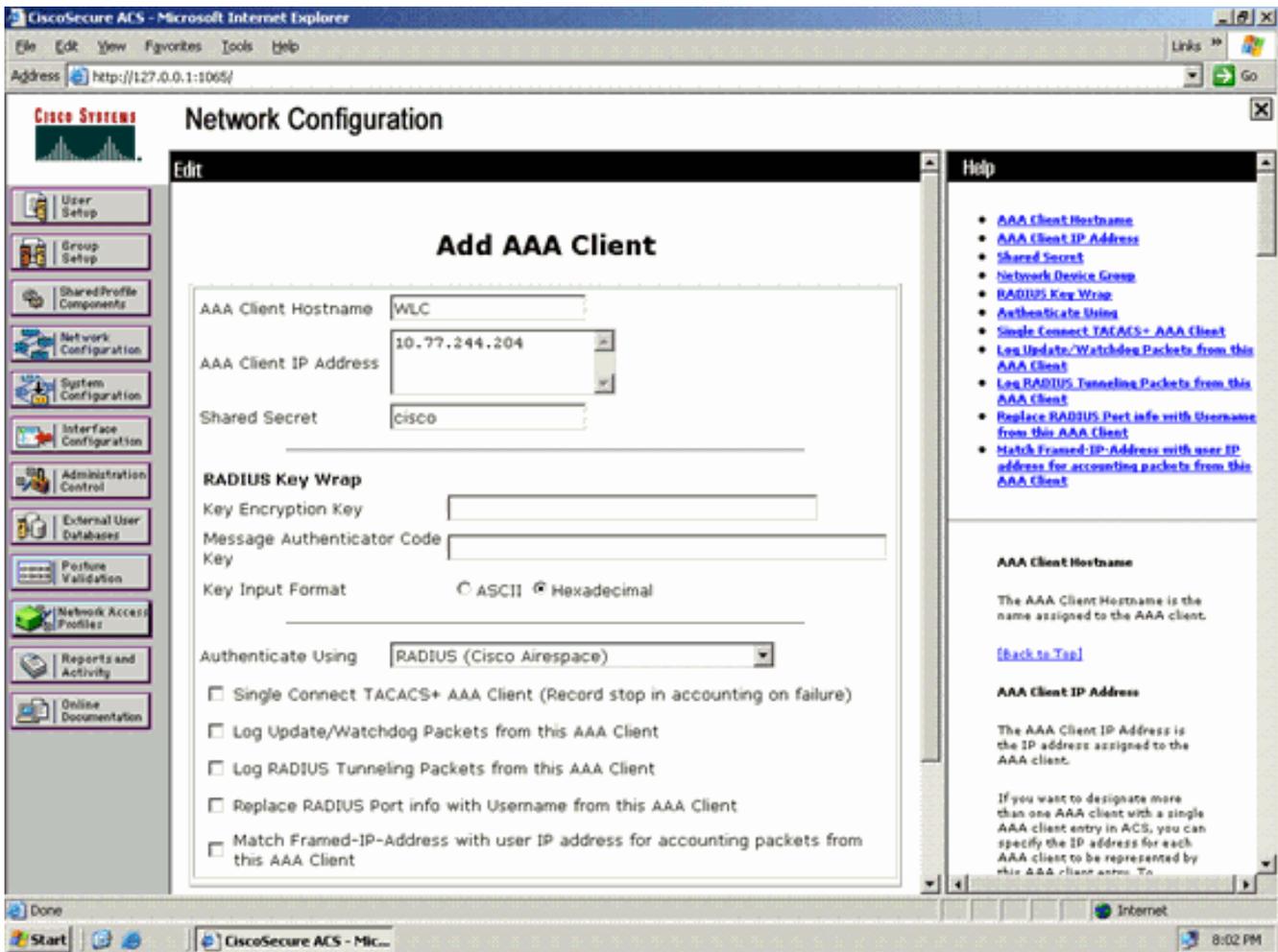
- Edit:** This section contains the main configuration form for the user. It includes:
  - User: User1 (New User):** A checkbox for "Account Disabled".
  - Supplementary User Info:** Fields for "Real Name" and "Description".
  - User Setup:** A section for "Password Authentication" with a dropdown menu set to "ACS Internal Database". Below this are fields for "Password" and "Confirm Password", and a checkbox for "Separate (CHAP/MS-CHAP/ARAP)".
- Help:** A sidebar on the right containing a list of links for various configuration options, such as "Account Disabled", "Deleting a Username", "Supplementary User Info", "Password Authentication", "Group to which the user is assigned", "Callback", "Client IP Address Assignment", "Advanced Settings", "Network Access Restrictions", "Max Sessions", "Usage Quotas", "Account Disable", "Downloadable ACLs", "Advanced TACACS+ Settings", "TACACS+ Enable Control", "TACACS+ Enable Password", "TACACS+ Outbound Password", "TACACS+ Shell Command Authorization", "Command Authorization for Network Device Management Applications", "TACACS+ Unknown Services", "TFT RADIUS Attributes", and "RADIUS Vendor-Specific Attributes".

3. أخترت ACS قاعدة معطيات داخلي من الكلمة صحة هوية مدخل صندوق.  
4. قم بتكوين كافة المعلمات المطلوبة الأخرى وانقر فوق إرسال.

### إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA إلى خادم RADIUS

أكمل الخطوات التالية لتعريف وحدة التحكم كعميل AAA على خادم ACS:

1. طقطقت شبكة تشكيل من ال ACS gui. تحت قسم إضافة عميل AAA من صفحة تكوين الشبكة، انقر فوق إضافة إدخال لإضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA إلى خادم RADIUS.
2. من صفحة عميل AAA، قم بتحديد اسم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وعنوان بروتوكول الإنترنت (IP) والسر المشترك وطريقة المصادقة (RADIUS/Cisco Airespace). ارجع إلى الوثائق من الشركة المصنعة الخاصة بخوادم المصادقة الأخرى غير الخاصة ب ACS.



ملاحظة: يجب أن يتطابق المفتاح السري المشترك الذي تقوم بتكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وخادم ACS. السر المشترك حساس لحالة الأحرف. 3. انقر فوق إرسال+تطبيق.

### تكوين مصادقة EAP-FAST على خادم RADIUS باستخدام إمداد PAC مجهول داخل النطاق

#### إمداد مجهول داخل النطاق

هذه إحدى طريقتي الإمداد داخل النطاق اللتين يقوم فيهما ACS بإنشاء اتصال آمن مع عميل المستخدم النهائي بغرض تزويد العميل بمسوغ وصول محمي جديد. يتيح هذا الخيار تبادل TLS مجهول بين عميل المستخدم النهائي و ACS.

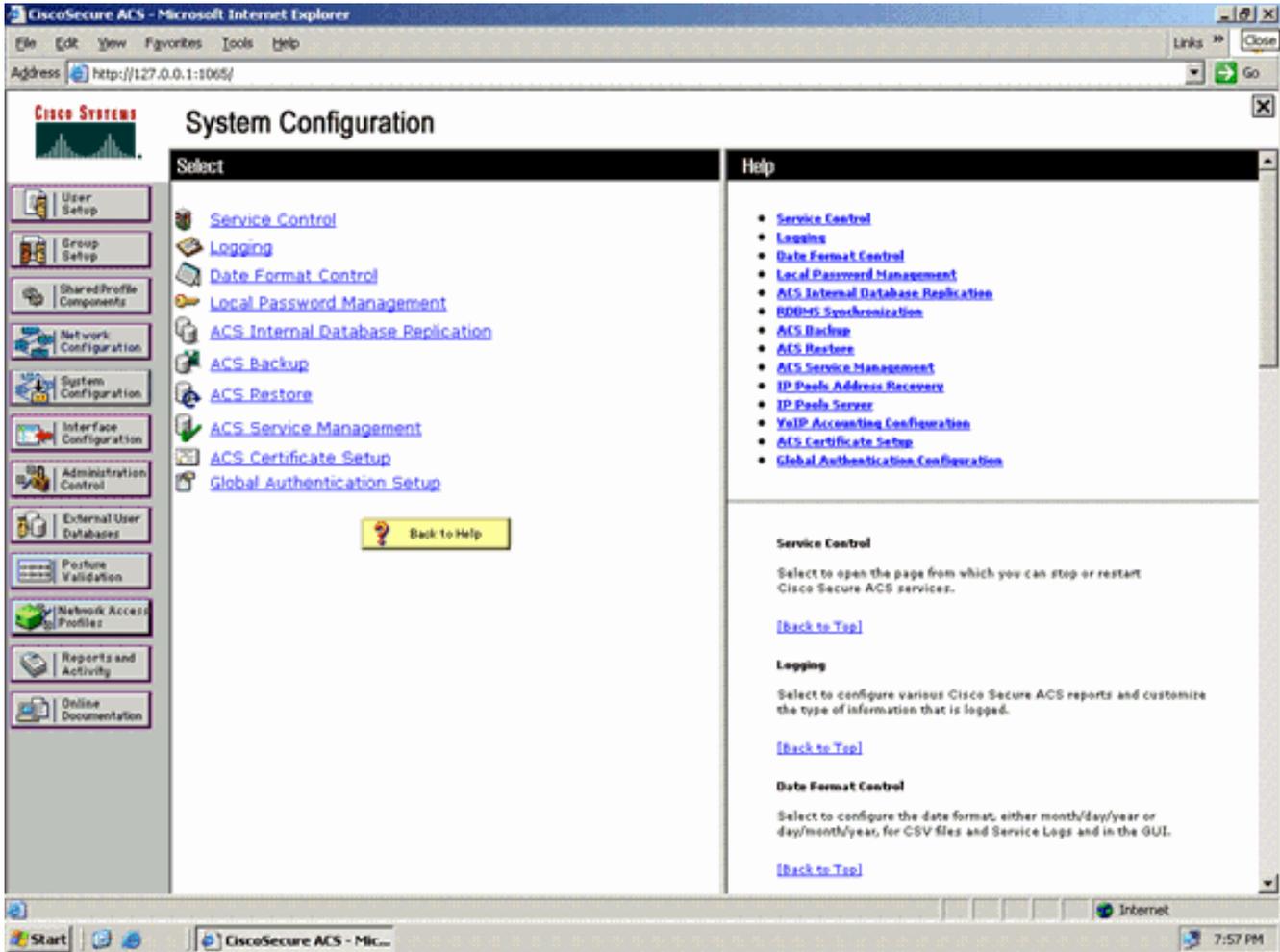
تعمل هذه الطريقة داخل نفق بروتوكول إتفاقية (ADHP) (Diffie-HellmanKey) المصادق عليه قبل أن يقوم النظرير بمصادقة خادم ACS.

ثم يتطلب ACS مصادقة EAP-MS-CHAPv2 للمستخدم. في مصادقة المستخدم الناجحة، يؤسس ACS نفق Diffie-Hellman مع عميل المستخدم النهائي. يقوم ACS بإنشاء مسوغ وصول محمي (PAC) للمستخدم وإرساله إلى عميل المستخدم النهائي في هذا النفق، بجانب معلومات حول ACS هذا. يستخدم أسلوب التقديم هذا EAP-MSCHAPv2 كطريقة مصادقة في المرحلة صفر و EAP-GTC في المرحلة الثانية.

نظرا لأنه يتم توفير خادم غير مصدق عليه، فلا يمكن استخدام كلمة مرور نص عادي. لذلك، يمكن استخدام بيانات اعتماد MS-CHAP فقط داخل النفق. يستخدم MS-CHAPv2 لإثبات هوية النظرير واستلام مسوغ وصول محمي (PAC) لجلسات المصادقة الإضافية (سيتم استخدام EAP-MS-CHAP كأسلوب داخلي فقط).

أتمت هذا steps in order to مصادقة EAP-FAST في RADIUS نادل لمجهول داخل النطاق:

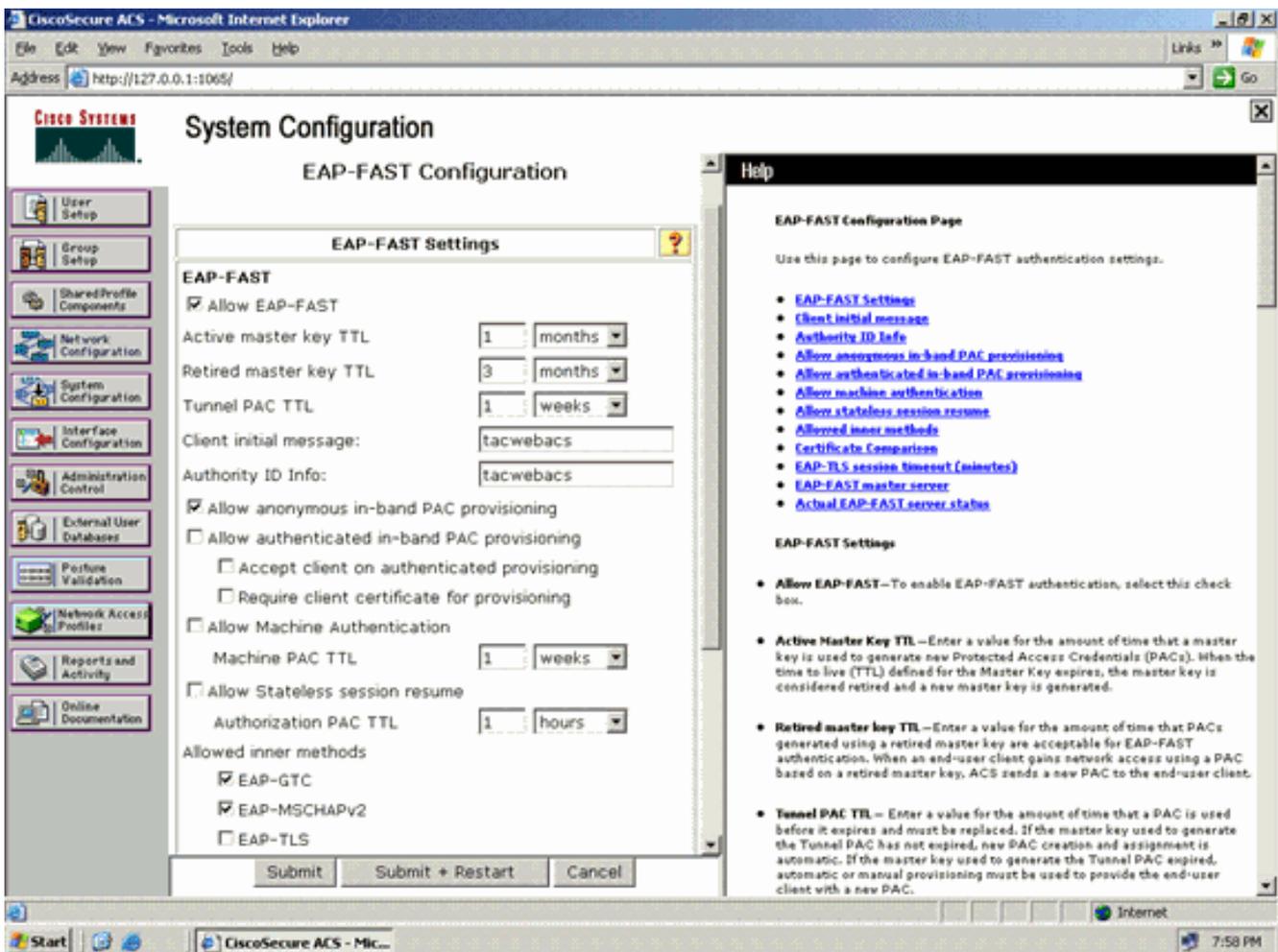
1. انقر فوق تكوين النظام من واجهة المستخدم الرسومية (GUI) الخاصة بخادم RADIUS. من صفحة "تكوين النظام"، اختر إعداد المصادقة العامة.



2. من صفحة إعداد المصادقة العامة، انقر على تكوين EAP-FAST للانتقال إلى صفحة إعدادات EAP-FAST.

The screenshot shows the CiscoSecure ACS System Configuration page. The left sidebar contains navigation links for various configuration areas. The main content area is titled 'EAP Configuration' and is divided into three sections: PEAP, EAP-FAST, and EAP-TLS. The EAP-FAST section is currently selected, and a link for 'EAP-FAST Configuration' is visible. The help window on the right provides detailed information about EAP and PEAP protocols.

3. من صفحة إعدادات EAP-FAST، حدد خانة الاختيار السماح EAP-FAST لتمكين EAP-FAST في خادم RADIUS.



4. قم بتكوين قيم مدة البقاء (TTL) للمفتاح الرئيسي النشط/المتقاعد كما هو مطلوب، أو قم بتعيينها على القيمة الافتراضية كما هو موضح في هذا المثال. ارجع إلى المفاتيح الرئيسية للحصول على معلومات حول المفاتيح الرئيسية النشطة والمتقاعدة. راجع أيضا "المفاتيح الرئيسية" و PAC TTLs للحصول على مزيد من المعلومات. يمثل حقل معلومات معرف المرجع الهوية النصية لخدم ACS هذا، والتي يمكن للمستخدم النهائي استخدامها لتحديد خادم ACS الذي ستم المصادقة عليه. ملء هذا الحقل إلزامي. يحدد حقل رسالة العرض الأولية للعميل الرسالة التي سيتم إرسالها إلى المستخدمين الذين يقومون بالمصادقة مع عميل EAP-FAST. الحد الأقصى للطول هو 40 حرفا. لن يرى المستخدم الرسالة الأولية إلا إذا كان عميل المستخدم النهائي يدعم العرض.

5. إذا كنت تريد أن يقوم ACS بتنفيذ تزويد PAC غير معروف داخل النطاق، حدد خانة الاختيار السماح بإمداد PAC داخل النطاق المجهول.

6. الطرق الداخلية المسموح بها— يحدد هذا الخيار أي طرق EAP داخلية يمكن أن تعمل داخل نفق EAP-FAST TLS. من أجل التقديم مجهول النطاق، يجب عليك تمكين EAP-GTC و EAP-MS-CHAP من أجل التوافق مع الإصدارات السابقة. إذا حددت السماح بتقديم مسوغات الوصول المحمي (PAC) المغفل داخل النطاق، فيجب عليك تحديد EAP-MS-CHAP (المرحلة صفر) و EAP-GTC (المرحلة الثانية).

## [تكوين العميل اللاسلكي لوضع التشغيل WPA2 Enterprise](#)

تتمثل الخطوة التالية في تكوين العميل اللاسلكي لوضع التشغيل WPA2 Enterprise.

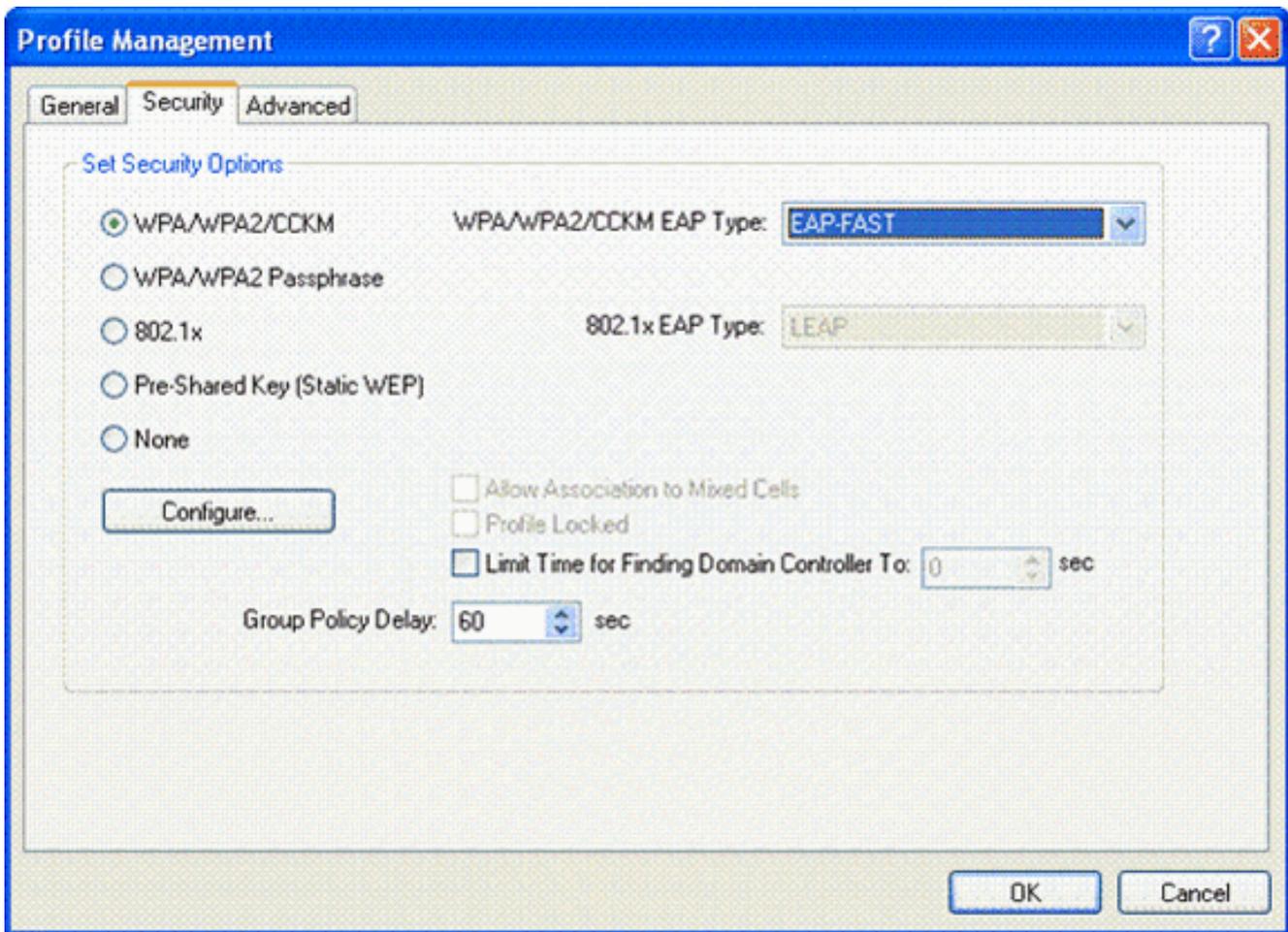
أكمل هذه الخطوات لتكوين العميل اللاسلكي لوضع WPA2 Enterprise.

1. من نافذة Aironet Desktop Utility، انقر على إدارة التوصيفات < جديد لإنشاء توصيف لمستخدم WPA2-Enterprise WLAN. كما ذكر سابقا، يستخدم هذا المستند اسم الشبكة المحلية اللاسلكية (WLAN/SSID) على هيئة WPA2-مؤسسي للعميل اللاسلكي.
2. من إطار إدارة التوصيفات، انقر على علامة التبويب عام وقم بتكوين اسم التوصيف واسم العميل واسم SSID

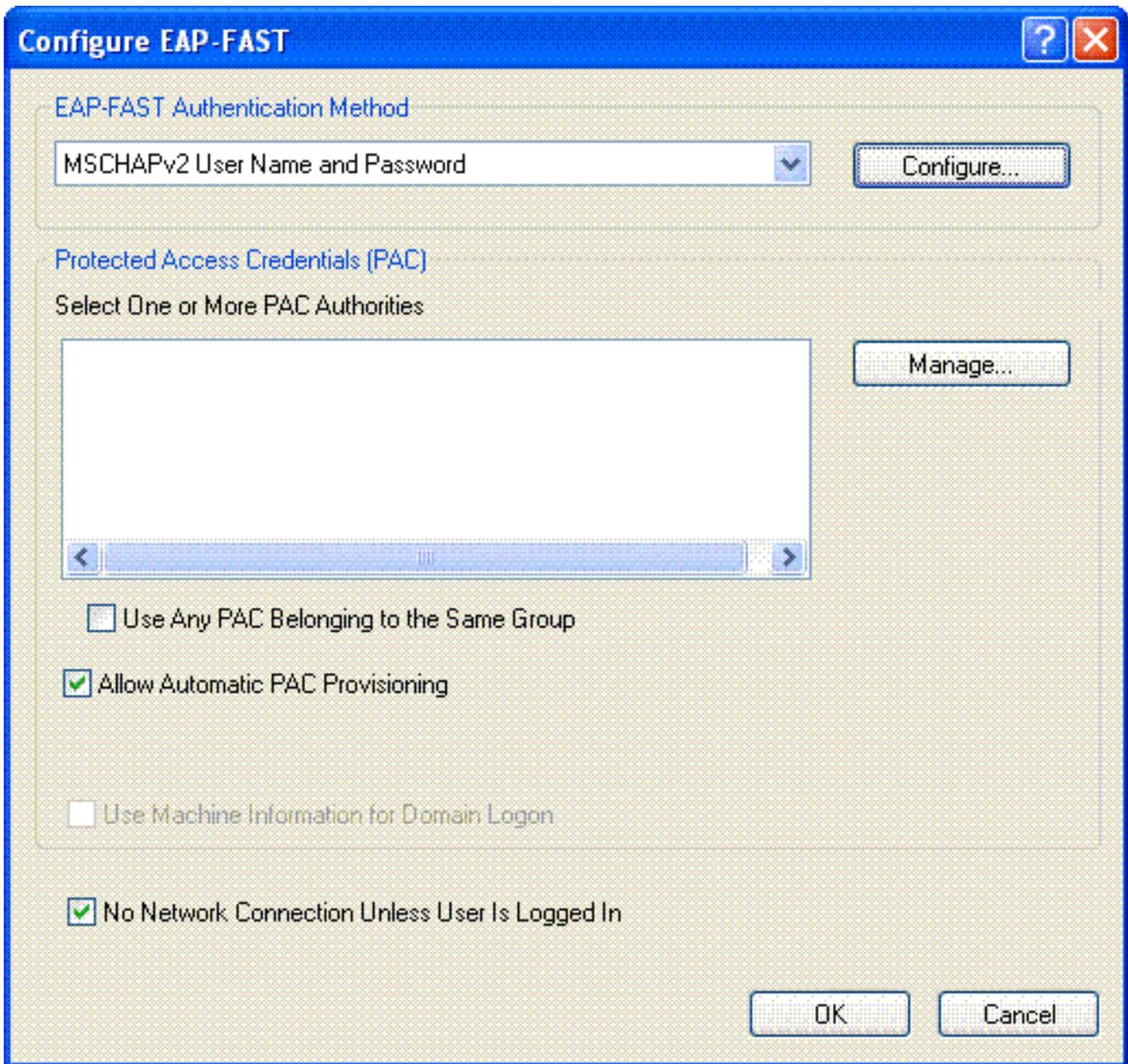
كما هو موضح في هذا المثال. ثم انقر فوق  
OK

The image shows a 'Profile Management' dialog box with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected. Under 'Profile Settings', there are two text boxes: 'Profile Name' containing 'WPA2-Enterprise' and 'Client Name' containing 'Wireless-Client1'. Under 'Network Names', there are three text boxes: 'SSID1' containing 'WPA2-Enterprise', 'SSID2' which is empty, and 'SSID3' which is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

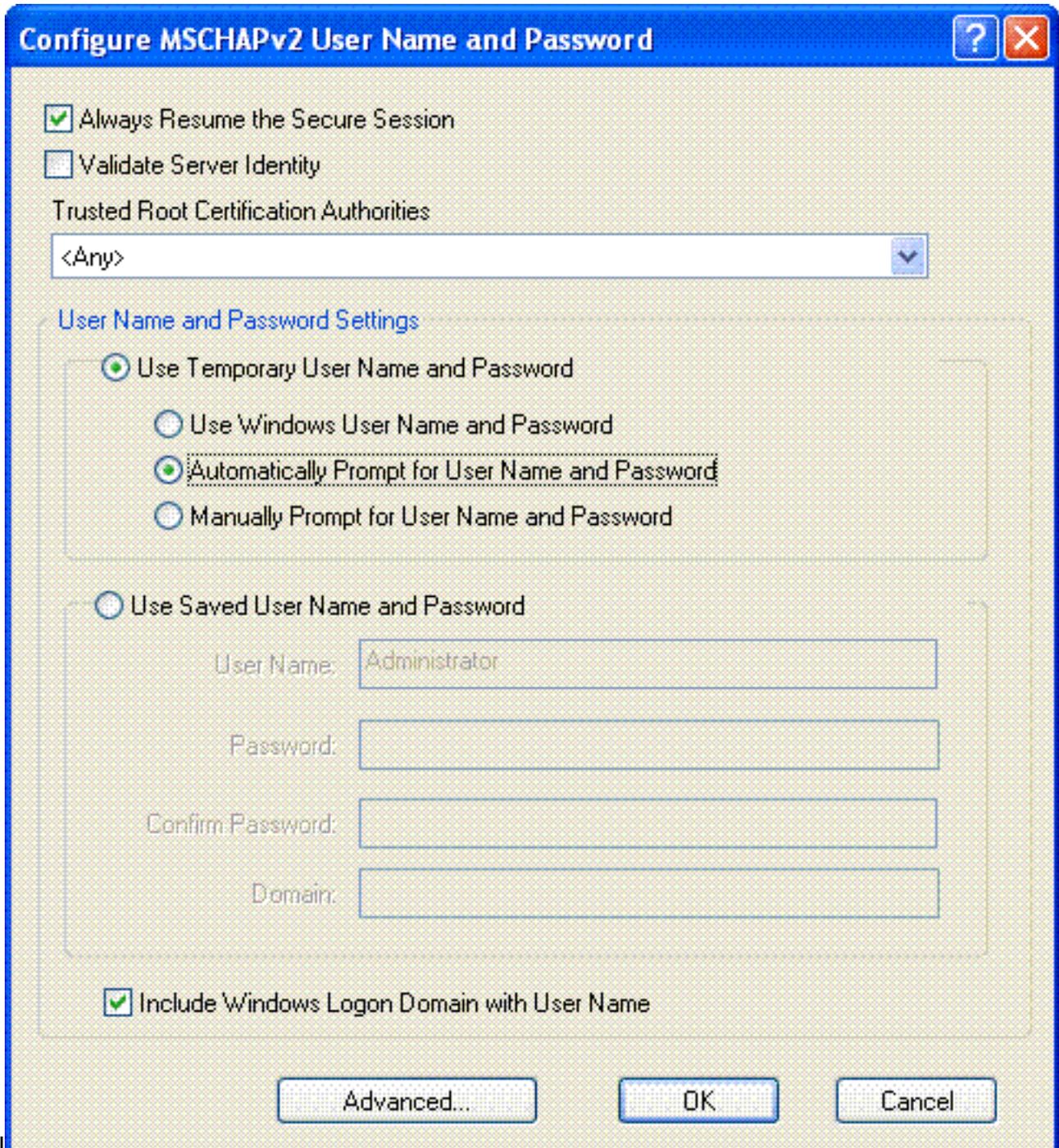
3. انقر على علامة التبويب تأمين واختر WPA/WPA2/CCKM لتمكين وضع التشغيل WPA2. تحت نوع EAP WPA/WPA2/CCKM، اختر EAP-FAST. انقر على تكوين لتكوين إعداد EAP-FAST.



4. من نافذة تكوين EAP-FAST، حدد خانة الاختيار السماح بإمداد PAC التلقائي. إذا أردت تكوين إعداد مسوغ وصول محمي مجهول، فسيتم استخدام EAP-MS-CHAP كطريقة داخلية وجيدة في المرحلة صفر.



5. أختار اسم مستخدم وكلمة مرور MSCHAPv2 كطريقة مصادقة من المربع المنسدل لأسلوب مصادقة EAP-FAST. طقطقة يشكل.
6. من نافذة تكوين اسم المستخدم وكلمة المرور MSCHAPv2، أختار إعدادات اسم المستخدم وكلمة المرور المناسبة. يختار هذا مثال تلقائياً رسالة حدث ل مستعمل إسم وكلمة.



ال

نفسه username وكلمة ينبغي كنت سجلت في ال ACS. كما تمت الإشارة سابقا، يستخدم هذا المثال User1 و User1 على التوالي كاسم المستخدم وكلمة المرور. لاحظ أيضا أن هذا ترويد مجهول داخل النطاق. لذلك، يتعذر على العميل التحقق من صحة شهادة الخادم. يجب أن تتأكد من إلغاء تحديد خانة الاختيار التحقق من هوية الخادم.  
7. وانقر فوق OK.

### التحقق من وضع تشغيل WPA2 على مستوى المؤسسة

أتمت هذا steps in order to إن ك WPA2 مشروع أسلوب تشكيل يعمل بشكل صحيح:

1. من نافذة أداة Aironet Desktop Utility، حدد التوصيف WPA2-Enterprise وانقر **تنشيط** من أجل تنشيط توصيف العميل اللاسلكي.
2. إذا قمت بتمكين MS-CHAP الإصدار 2 كمصادقة لك، سيقوم العميل بالمطالبة باسم المستخدم وكلمة

**Enter Wireless Network Password**

Please enter your EAP-FAST username and password to log on to the wireless network.

User Name :

Password :

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

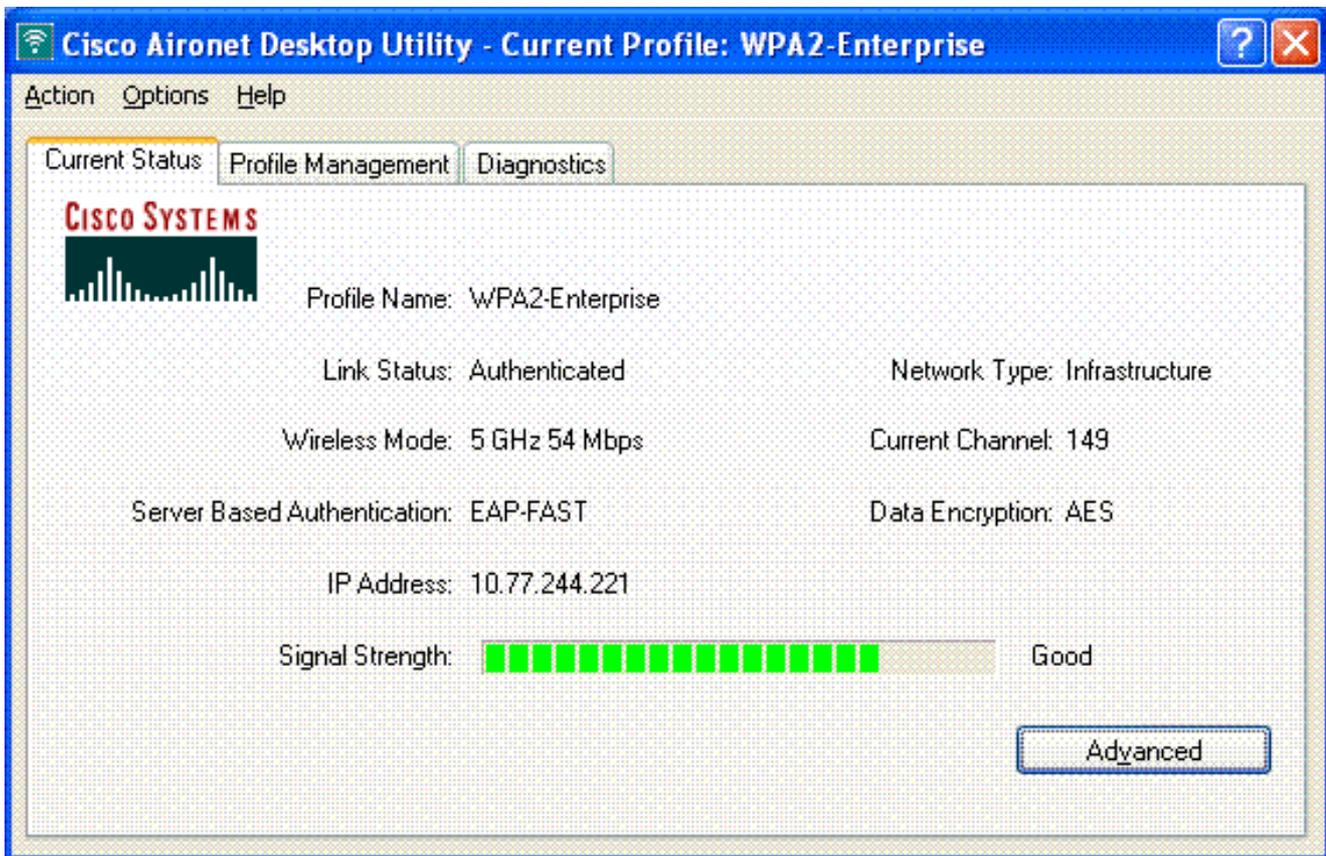
Profile Name : WPA-Enterprise

المروور.  
3. أثناء معالجة EAP-FAST للمستخدم، سيطالبك العميل بطلب PAC من خادم RADIUS. عند النقر فوق نعم، يبدأ توفير مسوغات الوصول المحمي (PAC).

**EAP-FAST Authentication**

You do not have a valid PAC from the authentication server. Do you want to proceed and request automatic provisioning?

4. بعد توفير مسوغات الوصول المحمي (PAC) بنجاح في المرحلة صفر، تتبع المرحلة الأولى والثانية ويتم إجراء المصادقة بنجاح. عند المصادقة الناجحة، يقترن العميل اللاسلكي بالشبكة المحلية اللاسلكية (WPA2- WLAN) Enterprise. هنا لقطة الشاشة:



كما يمكنك التحقق من تلقي خادم RADIUS لطلب المصادقة من العميل اللاسلكي والتحقق من صحته. تحقق من المصادقة التي تم تمريرها والمحاولات الفاشلة على خادم ACS للقيام بذلك. وهذه التقارير متاحة في إطار التقارير والأنشطة على خادم ACS.

## تكوين الأجهزة لوضع WPA2 الشخصي

أنجزت هذا steps in order to شكلت الأداة ل-WPA2 شخصي أسلوب عملية:

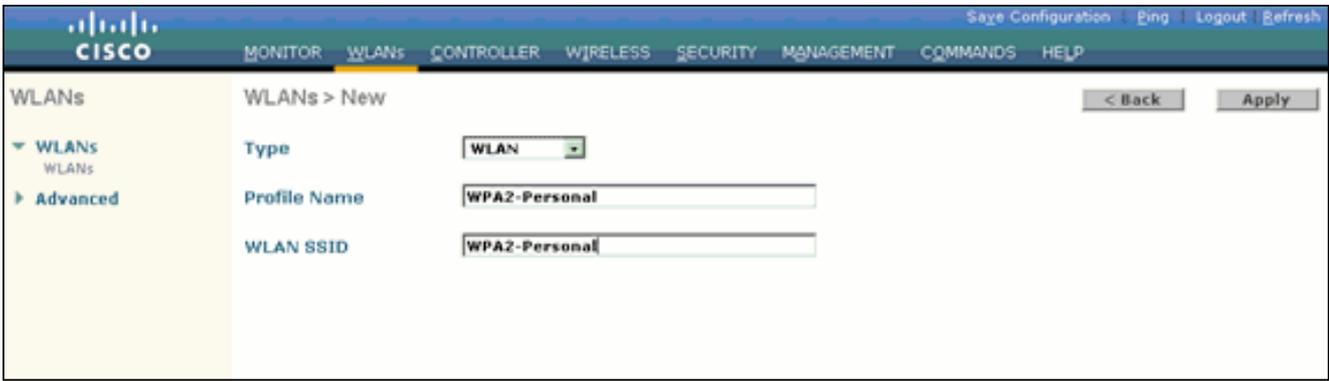
1. تكوين شبكة WLAN لمصادقة الوضع الشخصي WPA2
2. تكوين العميل اللاسلكي لوضع WPA2 الشخصي

### شكلت ال WLAN ل WPA2 شخصي أسلوب عملية

أنت تحتاج إلى تكوين شبكة WLAN التي سيستخدمها العملاء للاتصال بالشبكة اللاسلكية. سيكون WLAN SSID للوضع الشخصي WPA2- WPA2 شخصي. يعين هذا مثال هذا WLAN إلى الإدارة قارن.

أكمل هذه الخطوات لتكوين شبكة WLAN والمعلومات المرتبطة بها:

1. طقطقت WLANs من ال gui من الجهاز تحكم in order to عرضت WLANs صفحة. تسرد هذه الصفحة شبكات WLAN الموجودة على وحدة التحكم.
2. طقطقت جديد in order to خلقت WLAN جديد.
3. أدخل اسم SSID لشبكة WLAN واسم ملف التعريف ومعرف WLAN على شبكات WLAN < صفحة جديدة. بعد ذلك، انقر فوق تطبيق. يستخدم هذا المثال -WPA2 شخصي كمعرف SSID.

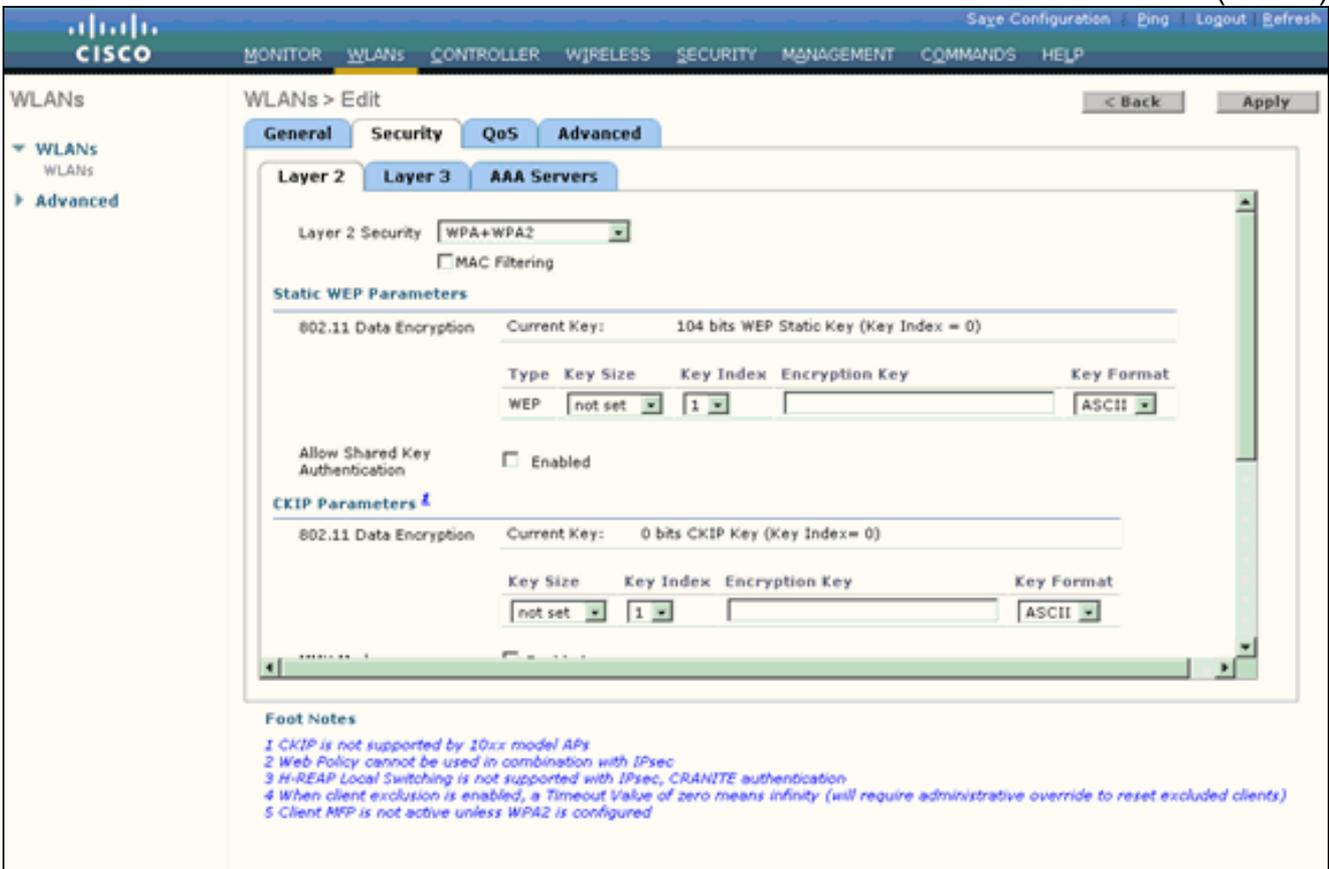


4. ما إن يخلق أنت WLAN جديد، ال WLAN < تحرير صفحة ل WLAN جديد يظهر. في هذه الصفحة، يمكنك تحديد معالم مختلفة خاصة بشبكة WLAN هذه. ويتضمن ذلك السياسات العامة ونهج الأمان ونهج جودة الخدمة والمعلومات المتقدمة.

5. تحت سياسات عامة، حدد خانة الاختيار الحالة لتمكين الشبكة المحلية اللاسلكية (WLAN).

6. إذا أردت لنقطة الوصول أن تبث SSID في إطارات المنارة الخاصة بها، حدد خانة الاختيار بث SSID.

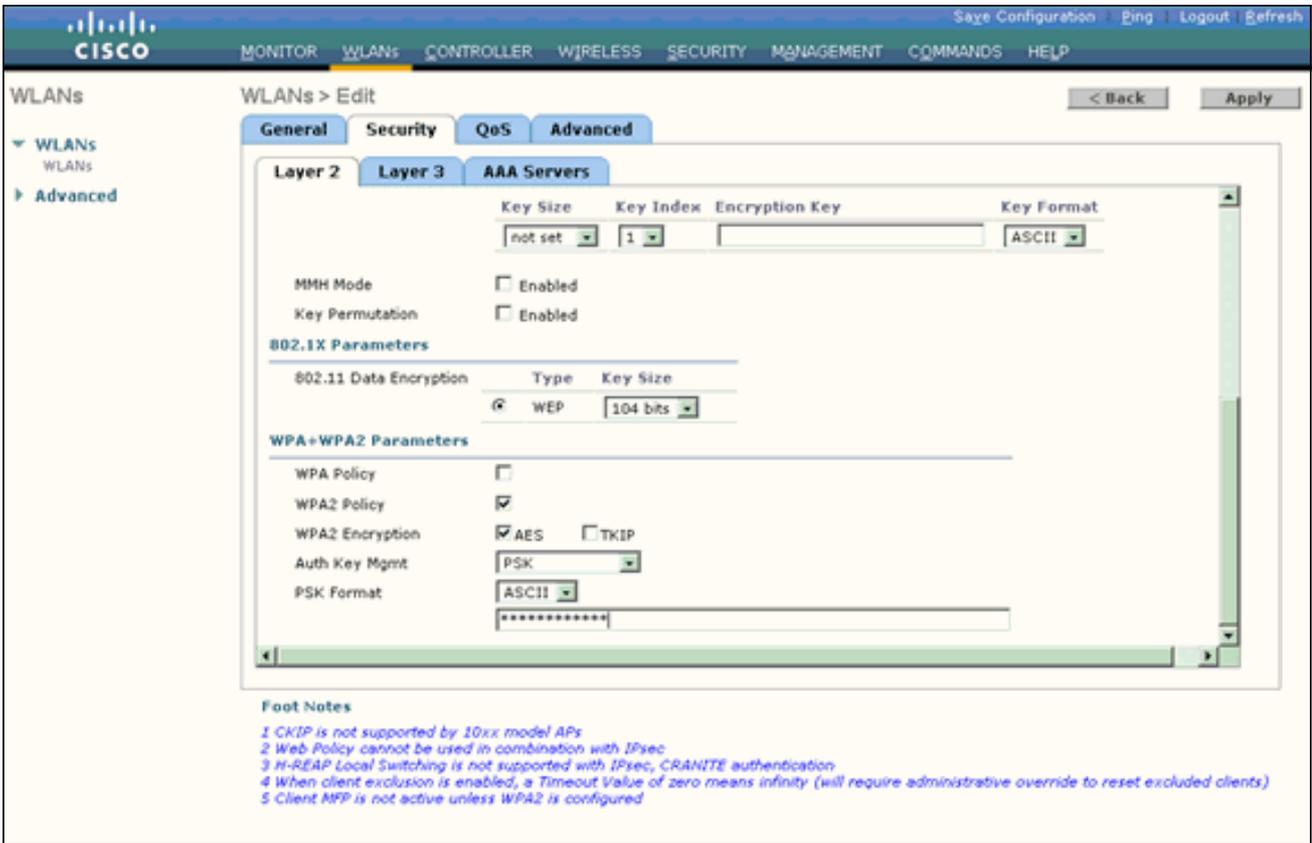
7. انقر فوق علامة التبويب أمان. تحت تأمين الطبقة، اختر WPA+WPA2. هذا يمكن مصادقة WPA للشبكة المحلية اللاسلكية (WLAN).



8. انزلق إلى أسفل الصفحة لتعديل معالم WPA+WPA2. في هذا المثال، يتم تحديد تشفير سياسة WPA2 و AES.

9. تحت إدارة مفتاح المصادقة، اختر PSK لتمكين WPA2-PSK.

10. أدخل المفتاح المشترك مسبقا في الحقل المناسب كما هو موضح.



**ملاحظة:** يجب أن يتطابق المفتاح المشترك مسبقا المستخدم على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مع المفتاح الذي تم تكوينه على العملاء اللاسلكيين.  
11. قطعة يطبق.

### تكوين العميل اللاسلكي لوضع WPA2 الشخصي

تتمثل الخطوة التالية في تكوين العميل اللاسلكي لوضع التشغيل -WPA2 الشخصي.

أتمت هذا steps in order to شكلت الزبون لاسلكي ل -WPA2 شخصي أسلوب:

1. من نافذة Aironet Desktop Utility، انقر على إدارة التوصيف < جديد لإنشاء توصيف لمستخدم WPA2-PSK.
2. من إطار إدارة التوصيفات، انقر على علامة التبويب عام وقم بتكوين اسم التوصيف واسم العميل واسم SSID كما هو موضح في هذا المثال. ثم انقر فوق .OK

**Profile Management** [?] [X]

General Security Advanced

**Profile Settings**

Profile Name: WPA2-Personal

Client Name: Wireless-Client2

**Network Names**

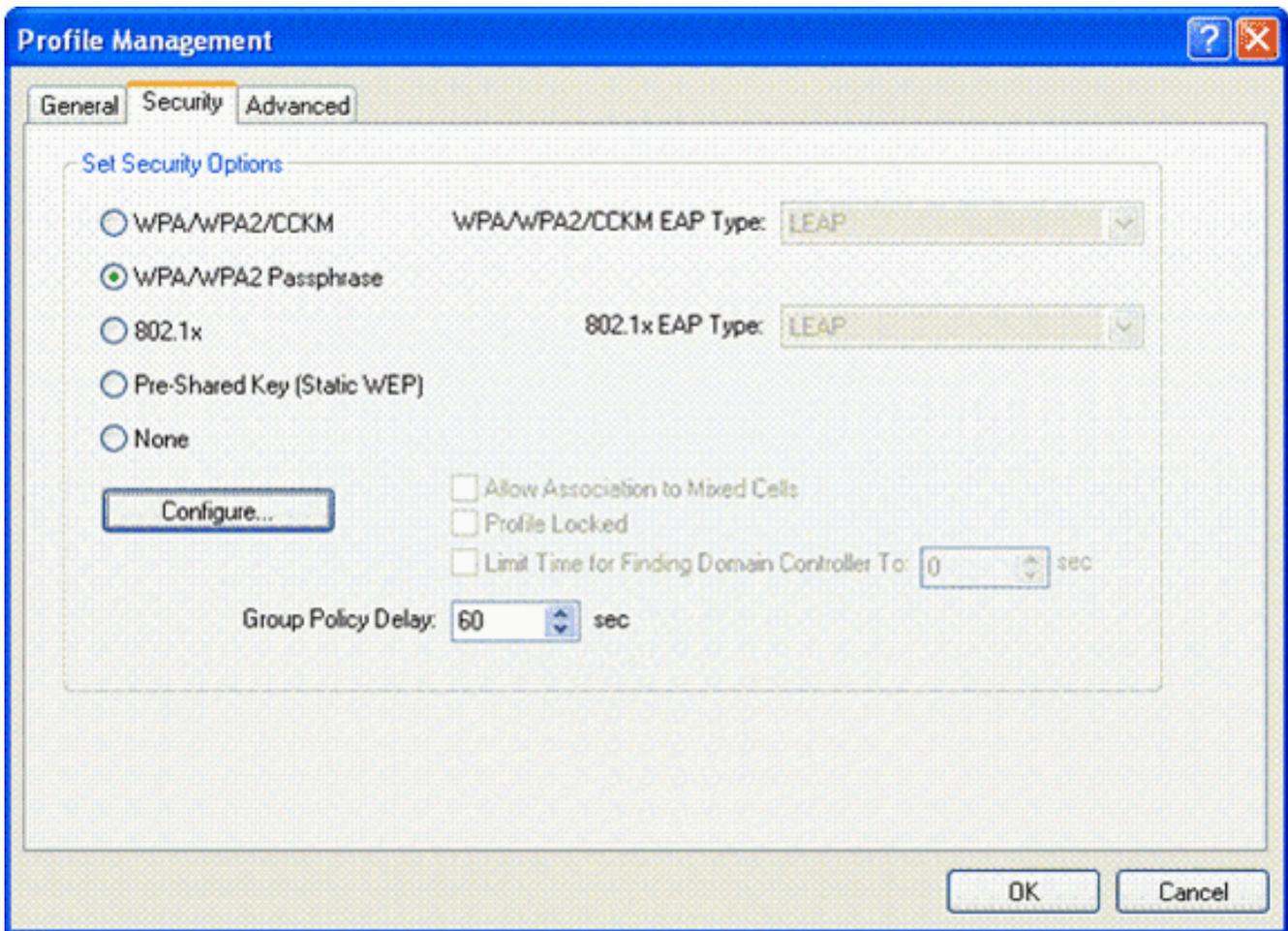
SSID1: WPA2-Personal

SSID2:

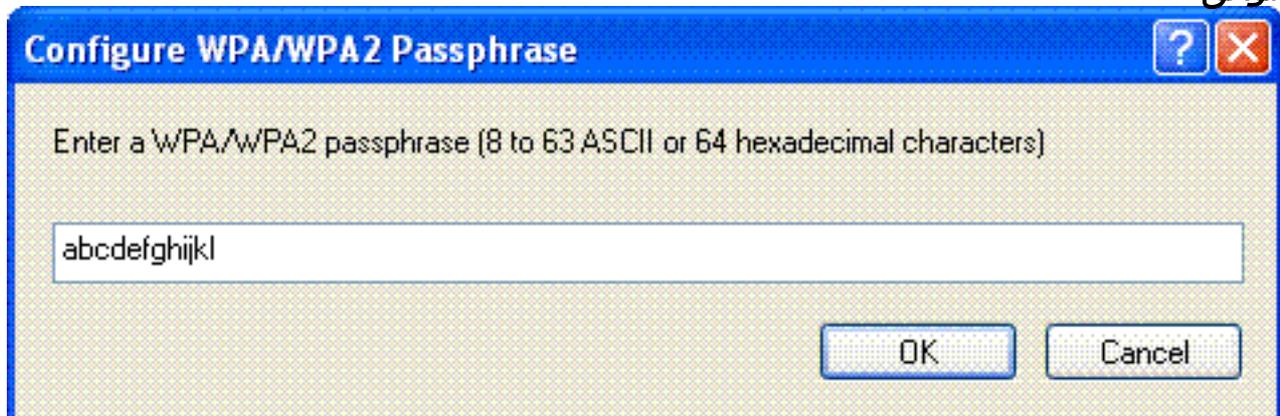
SSID3:

OK Cancel

3. انقر على علامة التبويب تأمين واختر عبارة مرور WPA/WPA2 لتمكين وضع التشغيل WPA2-PSK. انقر على تكوين لتكوين مفتاح WPA-PSK المشترك مسبقاً.



4. أدخل المفتاح المشترك مسبقا وانقر موافق.



التحقق من وضع التشغيل -WPA2 شخصي

أتمت هذا steps in order to دقت إن ك -WPA2 مؤسسي أسلوب تشكيل يعمل بشكل صحيح:

1. من إطار أداة Aironet Desktop Utility، حدد التوصيف -WPA2 شخصي وانقر تنشيط من أجل تنشيط توصيف العميل اللاسلكي.
2. بمجرد تنشيط التوصيف يرتبط العميل اللاسلكي بالشبكة المحلية اللاسلكية (WLAN) عند المصادقة الناجحة. هنا لقطة الشاشة:



for mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA  
(to mobile 00:40:96:af:3e:93 (EAP Id 20  
Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43  
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0  
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on  
AP 00:0b:85:91:c3:c0  
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1  
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on  
AP 00:0b:85:91:c3:c0  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to  
(mobile 00:40:96:af:3e:93 (EAP Id 22  
(Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3  
from mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
<=== Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22  
for STA 00:40:96:af:3e:93 19  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 19  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 20  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 21  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 22  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 23  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 24  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 25  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to

(mobile 00:40:96:af:3e:93 (EAP Id 26  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 27  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for  
mobile00:40:96:af:3e:93  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to  
(mobile 00:4096:af:3e:93 (EAP Id 27  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds  
for mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to  
(mobile 00:40:96:af:3e:93 (EAP Id 1  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to  
(mobile 00:40:96:af:3e:93 (EAP Id 1  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to  
(mobile 00:40:96:af:3e:93 (EAP Id 2  
(Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2  
from mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
<=== Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2  
for STA 00:40:96:af:3e:93 20  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 20  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 21  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 22  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for  
mobile 00:40:96:af:3e:93  
<=== Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22  
for STA 00:40:96:af:3e:93 24  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to  
(mobile 00:40:96:af:3e:93 (EAP Id 24  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Challenge  
for mobile 00:40:96:af:3e:93**  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA  
(to mobile 00:40:96:af:3e:93 (EAP Id 25**  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Received EAP Response from  
(mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43**  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Accept for  
mobile 00:40:96:af:3e:93**  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Creating a new PMK Cache Entry for  
(tation 00:40:96:af:3e:93 (RSN 0**  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP-Success to**

```
(mobile 00:40:96:af:3e:93 (EAP Id 25
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in
Authenticating state for mobile 00:40:96:af:3e:93
```

- debug dot1x ربط enable—يمكن ال debug من 802.1x ربط رسالة.
- debug aaa events enable—يمكن إخراج تصحيح الأخطاء لجميع أحداث AAA.

## معلومات ذات صلة

- WPA2 - Wi-Fi Protected Access 2
- مصادقة EAP-FAST مع وحدات تحكم الشبكة المحلية اللاسلكية ومثال تكوين خادم RADIUS الخارجي
- مصادقة EAP باستخدام مثال تكوين وحدات التحكم في الشبكة المحلية اللاسلكية (WLC)
- نظرة عامة على تكوين WPA
- دعم المنتج اللاسلكي
- الدعم التقني والمستندات - Cisco Systems

