مثال على تكوين وصول WiFi المحمي 2 (WPA 2)

المحتويات

المقدمة

يشرح هذا المستند مزايا استخدام WPA 2 (Wi-Fi Protected Access 2) في شبكة LAN اللاسلكية (WLAN). يوفر المستند مثالين للتكوين حول كيفية تنفيذ WPA 2 على الشبكة المحلية اللاسلكية (WLAN). يوضّح المثال الأول كيفية تكوين WPA 2 في وضع المؤسسة، ويوضّح المثال الثاني تكوين WPA 2 في الوضع الشخصي.

ملاحظة: يعمل WPA مع بروتوكول المصادقة المتوسع (EAP).

المتطلبات الأساسية

المتطلبات

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

- WPA
- حلول أمان WLAN**ملاحظة:** راجع نظرة عامة على أمان شبكة LAN اللاسلكية Cisco Aironet للحصول على معلومات حول حلول أمان Cisco WLAN.

المكونات المستخدمة

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

- نقطة وصول (AP)/جسر Cisco Aironet 1310g التي تعمل ببرنامج Cisco IOS® الإصدار JA(2)12.3
- مهايئ عميل Aironet 802.11a/b/g CB21AG الذي يشغل البرنامج الثابت 2.5
- أداة Aironet Desktop Utility (ADU) التي تشغل البرنامج الثابت 2.5

ملاحظة: برنامج مهايئ عميل Aironet CB21AG و PI21AG غير متوافق مع برامج مهايئ عميل Aironet الأخرى. يجب عليك إستخدام وحدة المعالجة المركزية (ADU) مع بطاقات CB21AG و PI21AG، ويجب عليك إستخدام أداة Aironet Client Utility (ACU) لجميع مهايئات عميل Aironet الأخرى. ارجع إلى تثبيت مهايئ العميل للحصول على مزيد من المعلومات حول كيفية تثبيت بطاقة CB21AG و ADU.

ملاحظة: يستخدم هذا المستند نقطة وصول/جسر يحتوي على هوائي مدمج. إذا كنت تستخدم نقطة وصول/جسر يتطلب هوائي خارجي، تأكد من توصيل الهوائيات بنقطة الوصول/الجسر. وإلا فإن نقطة الوصول/الجسر غير قادرة على الاتصال بالشبكة اللاسلكية. تأتي بعض نماذج نقاط الوصول (AP)/الجسور مع هوائيات مدمجة، في حين تحتاج طرازات أخرى إلى هوائي خارجي للتشغيل العام. أحلت لمعلومة على ال AP/Bridge نموذج أن يأتي مع هوائيات داخلية أو خارجية، دليل طلب شراء/دليل إنتاج للجهاز المناسب.

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.

معلومات أساسية

WPA هو حل تأمين قياسي من تحالف Wi-Fi يعالج نقاط الضعف في شبكات WLAN الأصلية. يوفر WPA حماية محسنة للبيانات والتحكم في الوصول لأنظمة WLAN. يعالج WPA جميع نقاط الضعف المعروفة المتعلقة بالخصوصية المكافئة للتوصيل السلكي (WEP) في تنفيذ أمان IEEE 802.11 الأصلي ويقدم حل أمان فوري لشبكات WLAN في بيئات المؤسسات والمكاتب الصغيرة والمكاتب المنزلية (SOHO) على حد سواء.

يمثل WPA 2 الجيل التالي من تأمين Wi-Fi. WPA 2 هو التطبيق البيني لتحالف Wi-Fi لمقياس IEEE 802.11i المصدق عليه. يطبق WPA 2 خوارزمية التشفير المتقدم المستحسنة (AES) الخاصة بالمعهد الوطني للمعايير والتكنولوجيا باستخدام وضع العداد مع بروتوكول مصادقة رسائل ربط التشفير (CCMP). يعد وضع عداد AES تشفير كتل يقوم بتشفير كتل بيانات 128 بت في كل مرة باستخدام مفتاح تشفير 128 بت. تنتج خوارزمية CCMP رمز تكامل الرسالة (MIC) الذي يوفر مصادقة أصل البيانات وسلامة البيانات للإطار اللاسلكي.

ملاحظة: يشار أيضا إلى CCMP باسم CBC-MAC.

يوفر WPA 2 مستوى تأمين أعلى من WPA لأن AES يوفر تشفيرا أقوى من بروتوكول سلامة المفاتيح المؤقتة (TKIP). TKIP هو خوارزمية التشفير التي يستخدمها WPA. ينشئ WPA 2 مفاتيح جلسات جديدة على كل اقتران. تكون مفاتيح التشفير المستخدمة لكل عميل على الشبكة فريدة ومحددة لذلك العميل. وفي نهاية المطاف، يتم تشفير كل حزمة يتم إرسالها عبر الهواء باستخدام مفتاح فريد. يتم تحسين الأمان باستخدام مفتاح تشفير جديد وفريد لعدم وجود إعادة إستخدام للمفتاح. لا يزال WPA يعتبر آمنا ولم يتم كسر TKIP. ومع ذلك، توصي Cisco بانتقال العملاء

إلى WPA 2 في أقرب وقت ممكن.

يدعم كلا WPA و WPA 2 وضعي التشغيل:

- وضع المؤسسة
- الوضع الشخصي

يناقش هذا المستند تنفيذ هذين الوضعين باستخدام WPA 2.

دعم WPA 2 مع أجهزة Cisco Aironet

يتم دعم WPA 2 على هذا الجهاز:

- سلسلة نقطة الوصول Aironet 1130AG و 1230AG AP Series
- سلسلة Aironet 1100 AP
- Aironet 1200 AP Series
- سلسلة Aironet 1300 AP

ملاحظة: قم بتجهيز نقاط الوصول هذه بأجهزة لاسلكي 802.11g واستخدم برنامج Cisco IOS الإصدار 12.3(2)JA أو إصدار أحدث.

كما يتم دعم WPA 2 و AES في:

- الوحدات النمطية للراديو Aironet 1200 Series مع أرقام الأجزاء AIR-RM21A و AIR-RM22A**ملاحظة:** لا تدعم الوحدة النمطية اللاسلكية Aironet 1200 المزودة برقم الجزء WPA 2 AIR-RM20a.
- مهايئات عميلة Aironet 802.11a/b/g مع برنامج ثابت، الإصدار 2.5

ملاحظة: لا تدعم منتجات Cisco Aironet 350 Series WPA 2 لأن أجهزة الراديو الخاصة بها تفتقر إلى دعم AES.

ملاحظة: لا تدعم الجسور اللاسلكية Cisco Aironet 1400 Series WPA 2 أو AES.

التكوين في وضع المؤسسة

يشير مصطلح **وضع المؤسسة** إلى المنتجات التي يتم إختبارها لتكون قابلة للتشغيل البيني في كل من وضعي تشغيل المفتاح المشترك مسبقا (PSK) و IEEE 802.1x للمصادقة. يعد الطراز 802.1x أكثر أمانا من أي إطار من أطر المصادقة القديمة نظرا لمرونته في دعم مجموعة متنوعة من آليات المصادقة وخوارزميات تشفير أقوى. يجري WPA 2 في وضع المؤسسة المصادقة على مرحلتين. يحدث تكوين المصادقة المفتوحة في المرحلة الأولى. المرحلة الثانية هي مصادقة 802. 1x بإحدى طرق EAP. يوفر AES آلية التشفير.

في وضع المؤسسة، يقوم العملاء وخوادم المصادقة بمصادقة بعضهم البعض باستخدام طريقة مصادقة EAP، ويقوم العميل والخادم بإنشاء مفتاح أساسي قياسي (PMK). باستخدام WPA 2، يقوم الخادم بإنشاء PMK ديناميكيا ويمرر PMK إلى AP.

يناقش هذا قسم التشكيل أن يكون ضروري أن يطبق WPA 2 في المؤسسة أسلوب العملية.

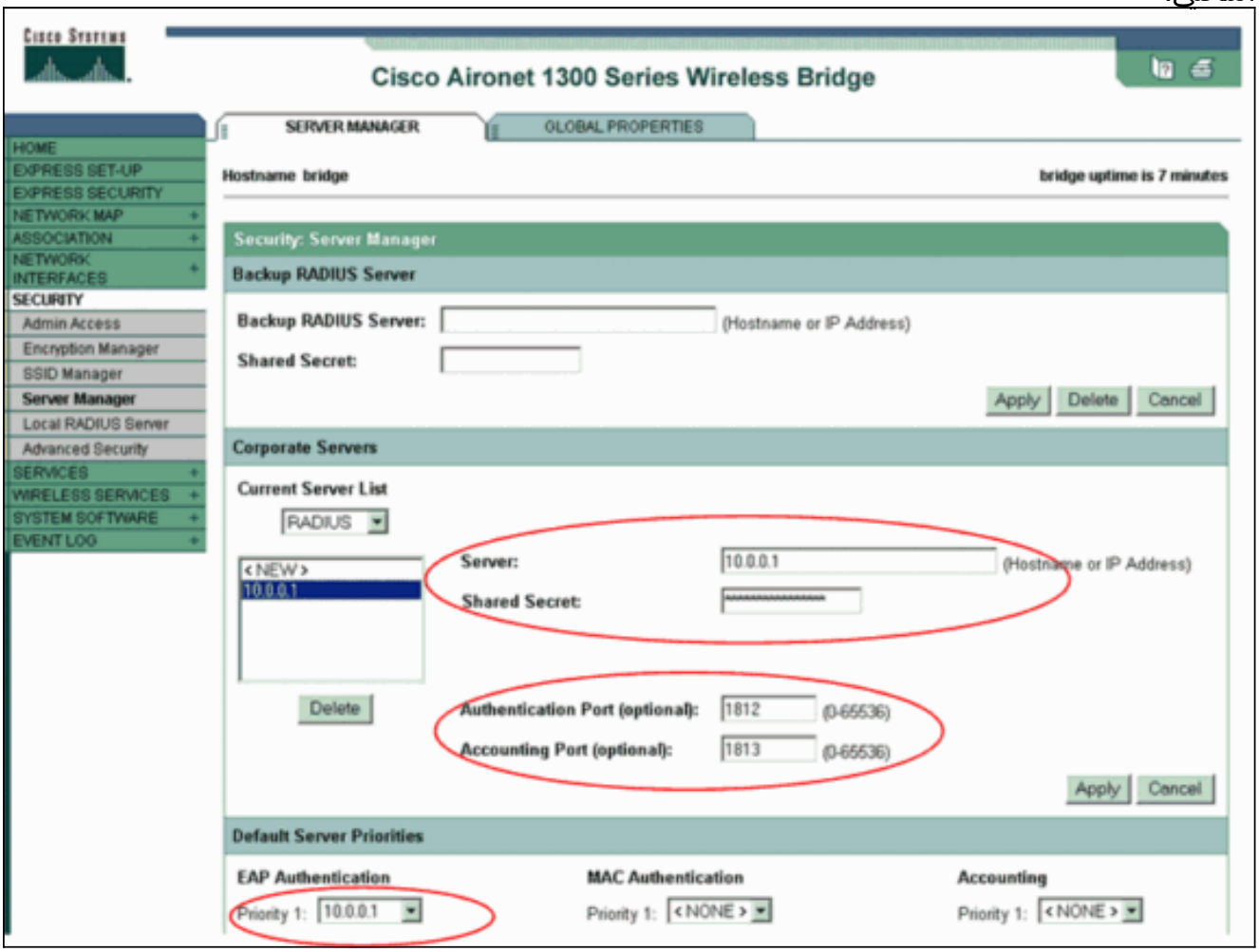
Network Setup (إعداد الشبكة)

في هذا الإعداد، يقوم نقطة الوصول/الجسر Aironet 1310g AP/Bridge الذي يشغل بروتوكول المصادقة المتوسع (LEAP) من Cisco بمصادقة مستخدم باستخدام مهايئ عميل متوافق مع WPA 2. تحدث إدارة المفاتيح باستخدام WPA 2، الذي يتم فيه تكوين تشفير AES-CCMP. تم تكوين نقطة الوصول كخادم RADIUS محلي يقوم بتشغيل مصادقة LEAP. يجب تكوين محول العميل و AP من أجل تنفيذ هذا الإعداد. الأقسام تكوين نقطة الوصول وتكوين مهايئ العميل عرض التكوين على نقطة الوصول ومهايئ العميل.

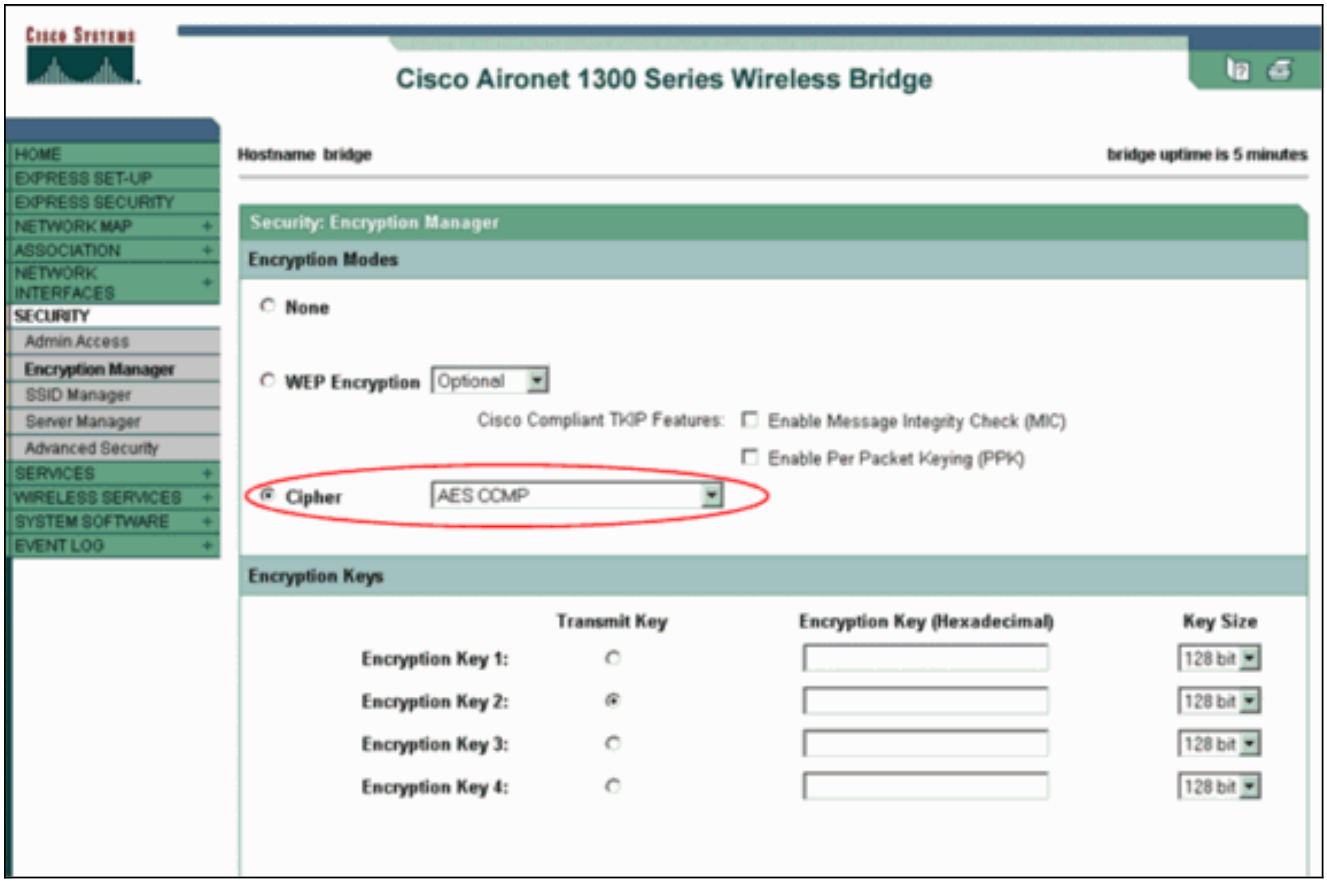
قم بتكوين نقطة الوصول

أتمت هذا steps أن يشكل ال ap يستعمل GUI:

1. قم بتكوين نقطة الوصول كخادم RADIUS محلي يقوم بتشغيل مصادقة LEAP.أختر **التأمين > مدير الخادم** في القائمة الموجودة على اليسار وحدد عنوان IP، المنافذ، والسر المشترك لخادم RADIUS.لأن هذا تشكيل يقوم بتكوين نقطة الوصول كخادم RADIUS محلي، أستخدم عنوان IP الخاص بنقطة الوصول. أستخدم المنافذ 1812 و 1813 لتشغيل خادم RADIUS المحلي.في منطقة "أولويات الخادم الافتراضي"، قم بتعريف أولوية مصادقة EAP الافتراضية ك 10.0.0.1.**ملاحظة:** 10.0.0.1 هو خادم RADIUS المحلي.

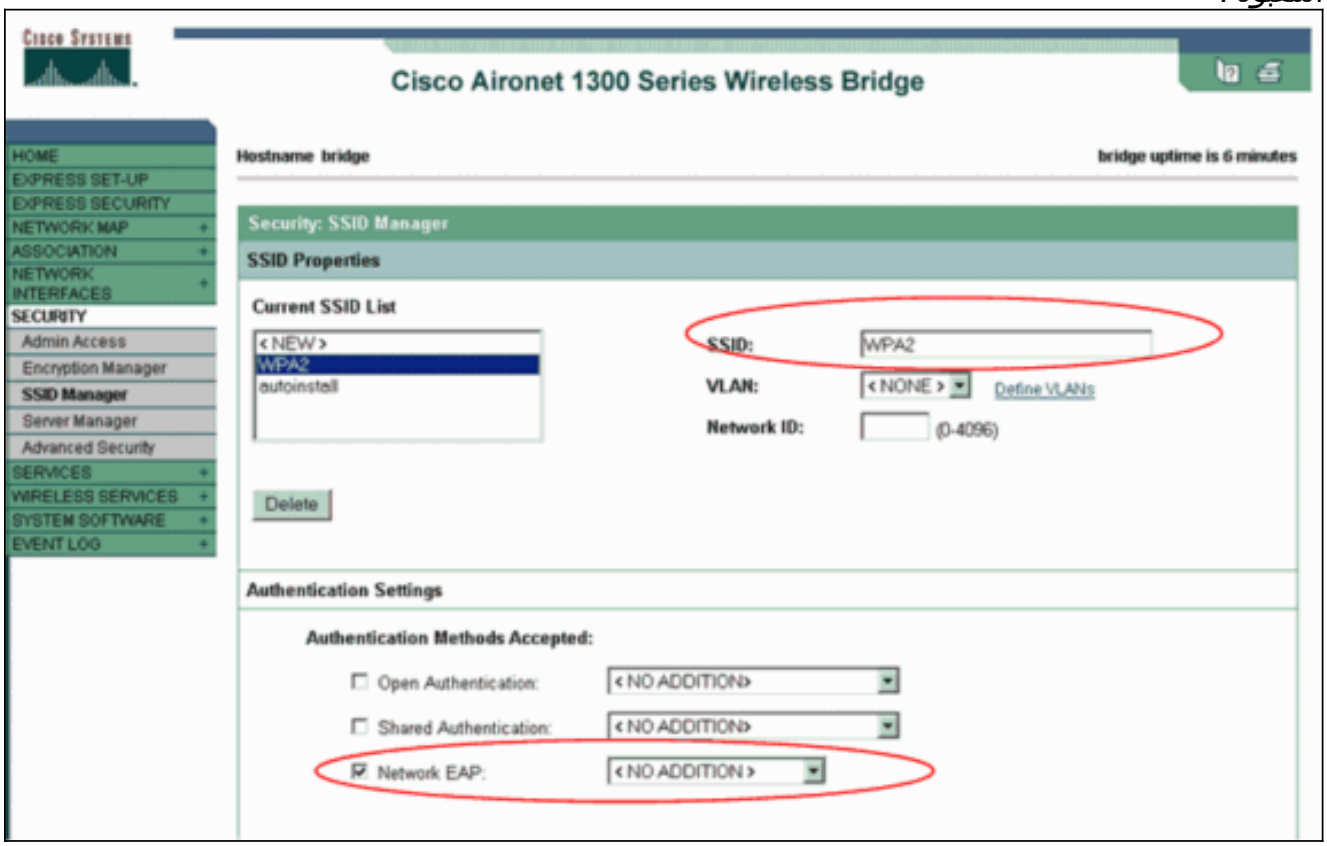


2. أختر **التأمين > مدير التشفير** من القائمة الموجودة على اليسار وأكمل الخطوات التالية:من قائمة التشفير، أختر **AES CCMP**.يتيح هذا الخيار تشفير AES باستخدام وضع العداد مع CBC-MAC.



طقطقة **يطبق**.

3. أختر **تأمين > إدارة SSID** وقم بإنشاء معرف مجموعة خدمة جديد (SSID) للاستخدام مع WPA 2.حدد خانة الاختيار **Network EAP** في منطقة طرق المصادقة المقبولة.



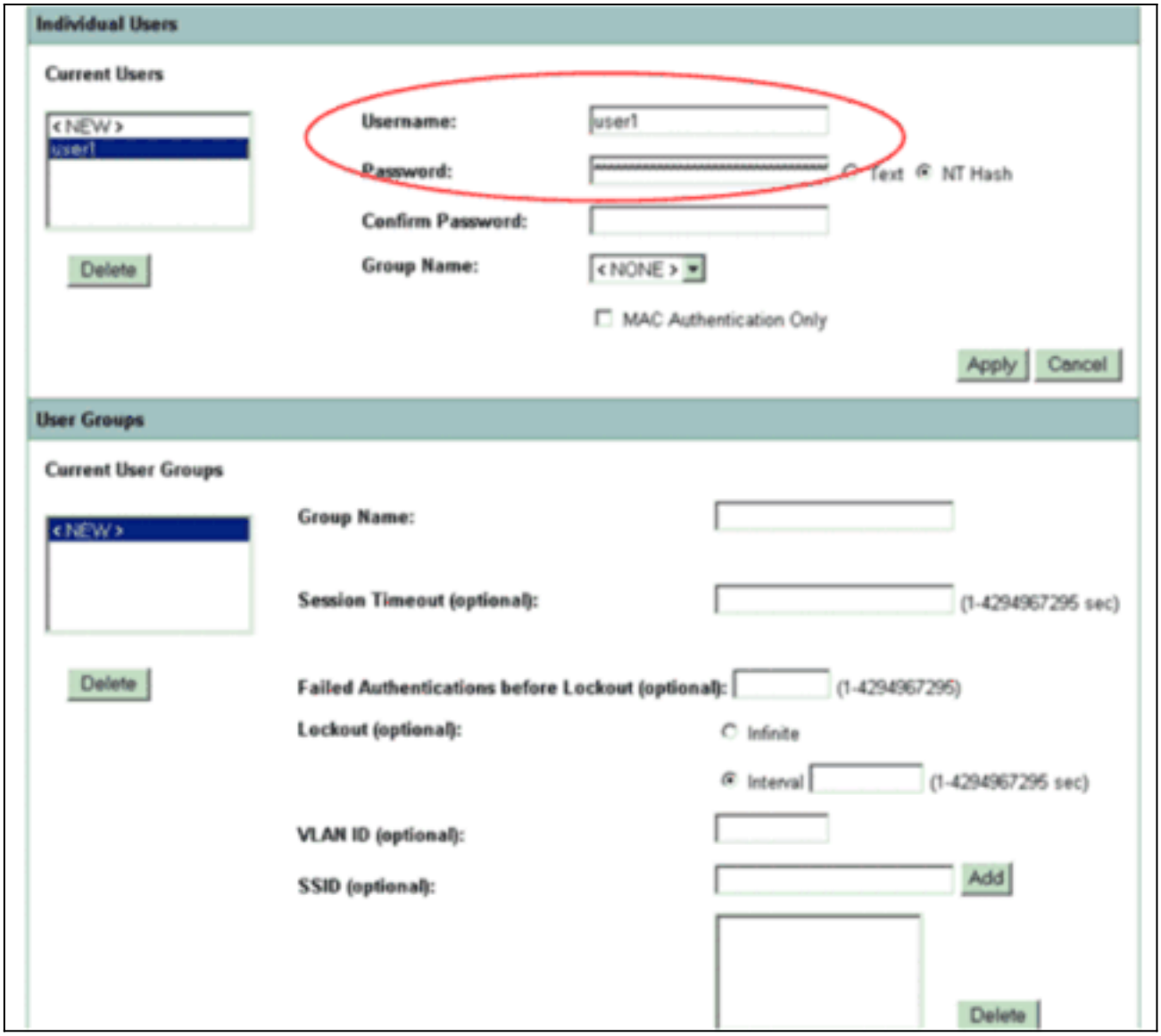
ملاحظة: أستخدم هذه الإرشادات عند تكوين نوع المصادقة على واجهة الراديو:إستخدام عملاء Cisco ل EAP الشبكة.عملاء الطرف الثالث (والتي تتضمن ملحقات متوافقة مع سيسكو [CCX] منتجات متوافقة مع EAP)- إستخدام المصادقة المفتوحة مع EAP.مزيج من كل من عملاء Cisco والأطراف الخارجية - أختر كلا من EAP

للشبكة والمصادقة المفتوحة مع EAP.قم بالتمرير لأسفل في نافذة "مدير SSID للأمان" إلى منطقة "إدارة المفاتيح المصدق عليها" وأكمل الخطوات التالية:من قائمة إدارة المفاتيح، أختر **إلزامي**.حدد خانة الاختيار **WPA** الموجودة على اليمين.طقطقة **يطبق**.**ملاحظة:** تعريف شبكات VLAN إختياري. إن يعين أنت VLANs، زبون أداة أن يربط مع إستعمال من هذا SSID يجمع داخل ال VLAN. راجع تكوين شبكات VLAN للحصول على مزيد من المعلومات حول كيفية تنفيذ شبكات VLAN.

4. أختر **التأمين > خادم RADIUS المحلي** وأكمل الخطوات التالية:انقر على علامة التبويب **إعداد عام** الموجودة أعلى النافذة.حدد خانة الاختيار **LEAP** وانقر **تطبيق**.في منطقة "خوادم الوصول إلى الشبكة"، حدد عنوان IP والسر المشترك لخادم RADIUS.بالنسبة لخادم RADIUS المحلي، أستخدم عنوان IP الخاص بنقطة الوصول.

طقطقة **يطبق**.

5. قم بالتمرير لأسفل في نافذة إعداد عام إلى منطقة "المستخدمين المنفردين" وقم بتعريف المستخدمين المنفردين.تعريف مجموعات المستخدمين
إختياري.



يحدد هذا التكوين مستخدم باسم "user1" وكلمة مرور. كما يحدد التكوين تجزئة NT لكلمة المرور. بعد اكتمال الإجراء الوارد في هذا القسم، تكون نقطة الوصول (AP) جاهزة لقبول طلبات المصادقة من العملاء. تتمثل الخطوة التالية في تكوين محول العميل.

تكوين واجهة سطر الأوامر (CLI)

نقطة الوصول
ap#**show running-config** ...Building configuration . . . **aaa new-model** *!--- This command reinitializes the authentication, !--- authorization and accounting functions.* ! ! **aaa group server radius rad_eap server 10.0.0.1 auth-port 1812 acct-port 1813** *A server group for RADIUS is created called ---! "rad_eap" !--- that uses the server at 10.0.0.1 on ports 1812 and 1813.* . . . **aaa authentication login eap_methods group rad_eap** *Authentication [user validation] is to be done for ---! !--- users in a group called "eap_methods" who use server group "rad_eap".* . . . ! bridge irb ! interface Dot11Radio0 no ip address no ip route-cache !

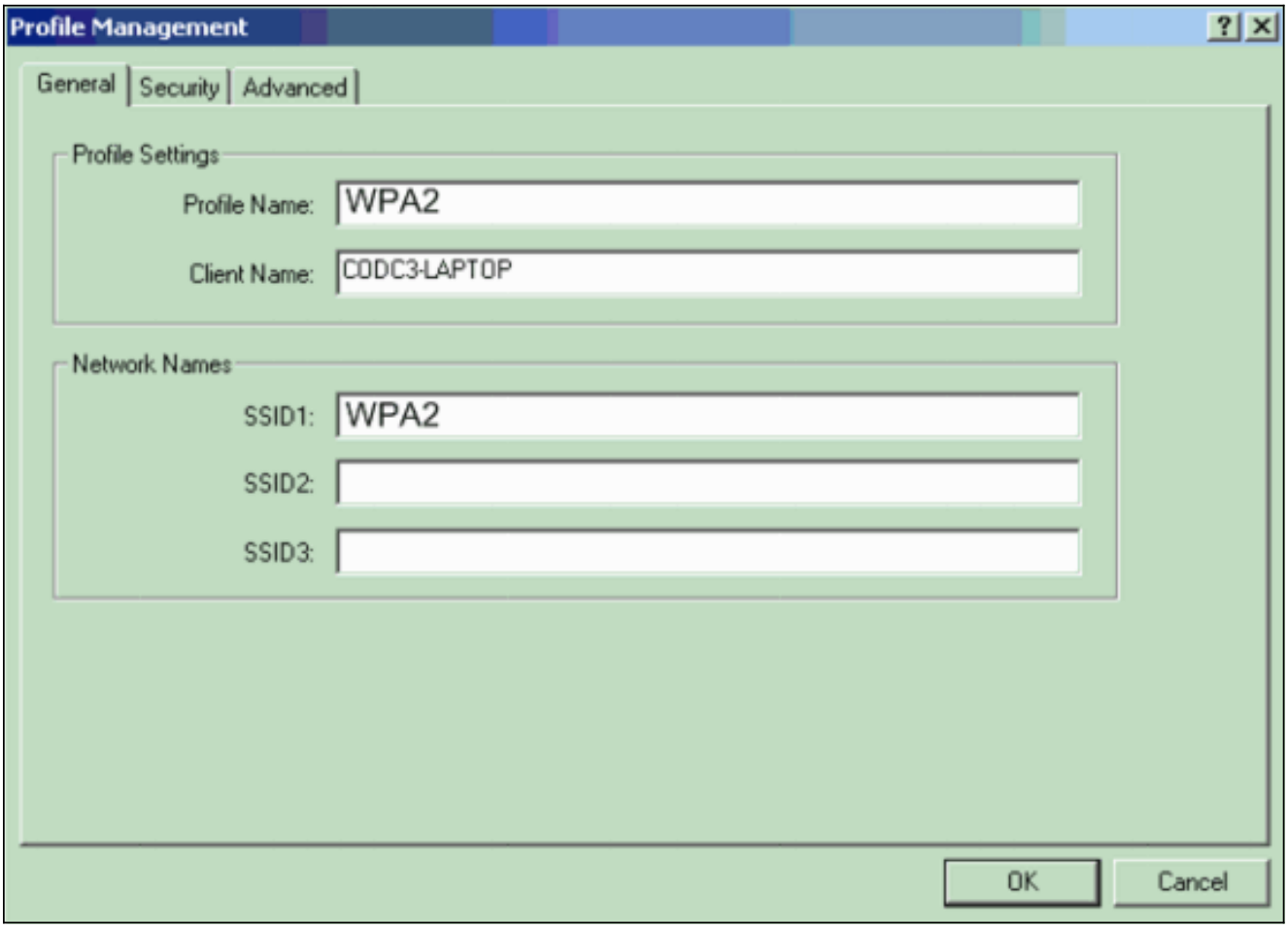
```
encryption vlan 1 key 1 size 128bit
transmit-key 12345678901234567890123456
This step is optional !--- This value seeds the---!
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory
This defines the policy for the use of Wired ---!
Equivalent Privacy (WEP). !--- If more than one VLAN is
used, !--- the policy must be set to mandatory for each
VLAN. broadcast-key vlan 1 change 300
You can also enable Broadcast Key Rotation for ---!
each vlan and Specify the time after which Brodacst key
is changed. If it is disabled Broadcast Key is still
used but not changed. ssid cisco vlan 1
Create a SSID Assign a vlan to this SSID ---!
authentication open eap eap_methods
authentication network-eap eap_methods
Expect that users who attach to SSID "cisco" !--- ---!
request authentication with the type 128 Open EAP and
Network EAP authentication !--- bit set in the headers
of those requests, and group those users into !--- a
group called "eap_methods." ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local
Engages the Local RADIUS Server feature. nas ---!
10.0.0.1 key shared_secret
Identifies itself as a RADIUS server, reiterates !- ---!
-- "localness" and defines the key between the server
(itself) and the access point(itself). ! group testuser
!--- Groups are optional. ! user user1 nthash password1
group testuser
Individual user user user2 nthash password2 group ---!
testuser
Individual user !--- These individual users ---!
comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port
key shared_secret 1813
Defines where the RADIUS server is and the key ---!
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end
```

تكوين محول العميل

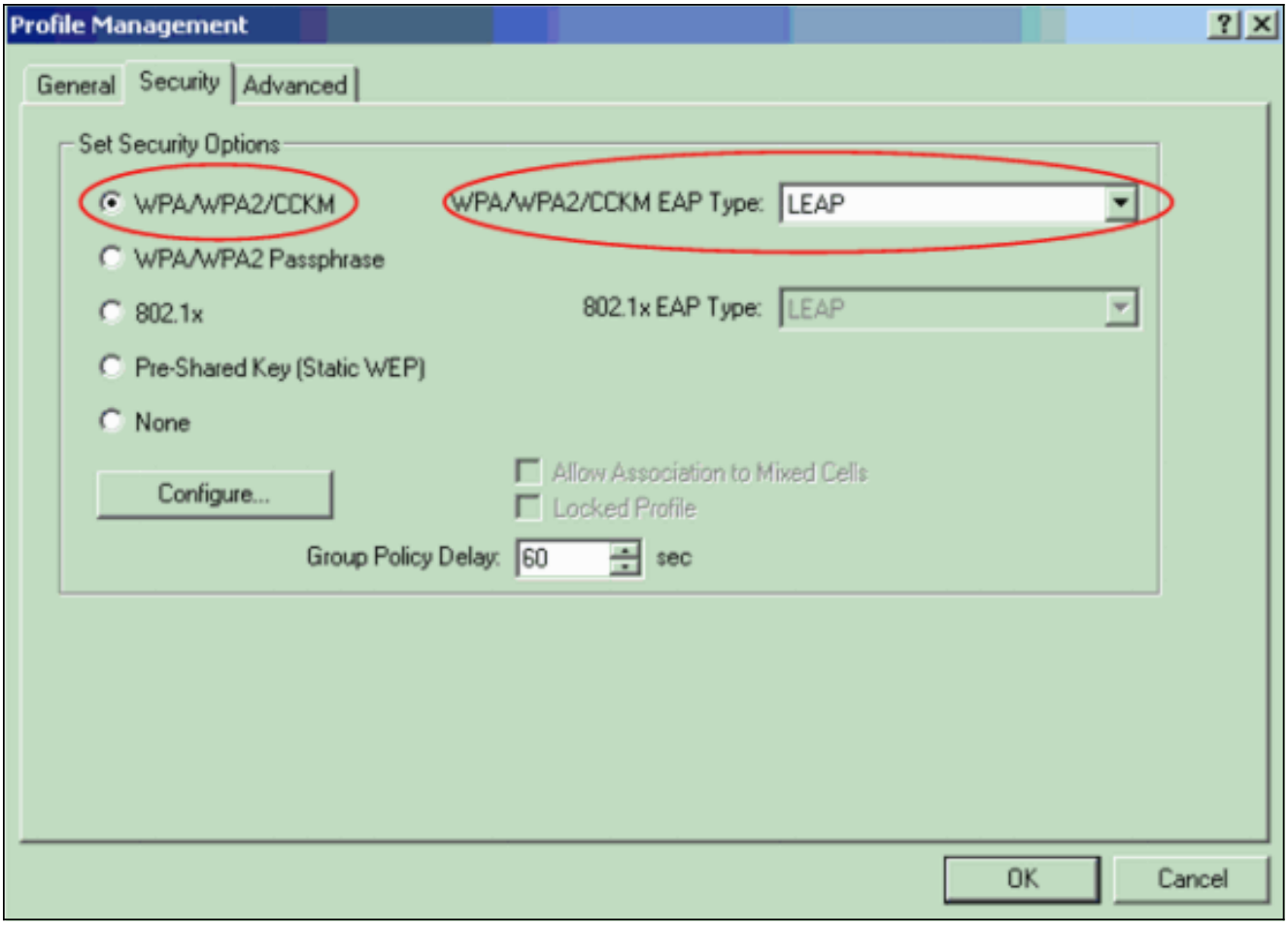
أكمل الخطوات التالية:

ملاحظة: يستخدم هذا المستند مهايئ عميل Aironet 802.11a/b/g يشغل البرنامج الثابت 2.5 ويشرح تكوين مهايئ العميل باستخدام الإصدار 2.5 من ADU.

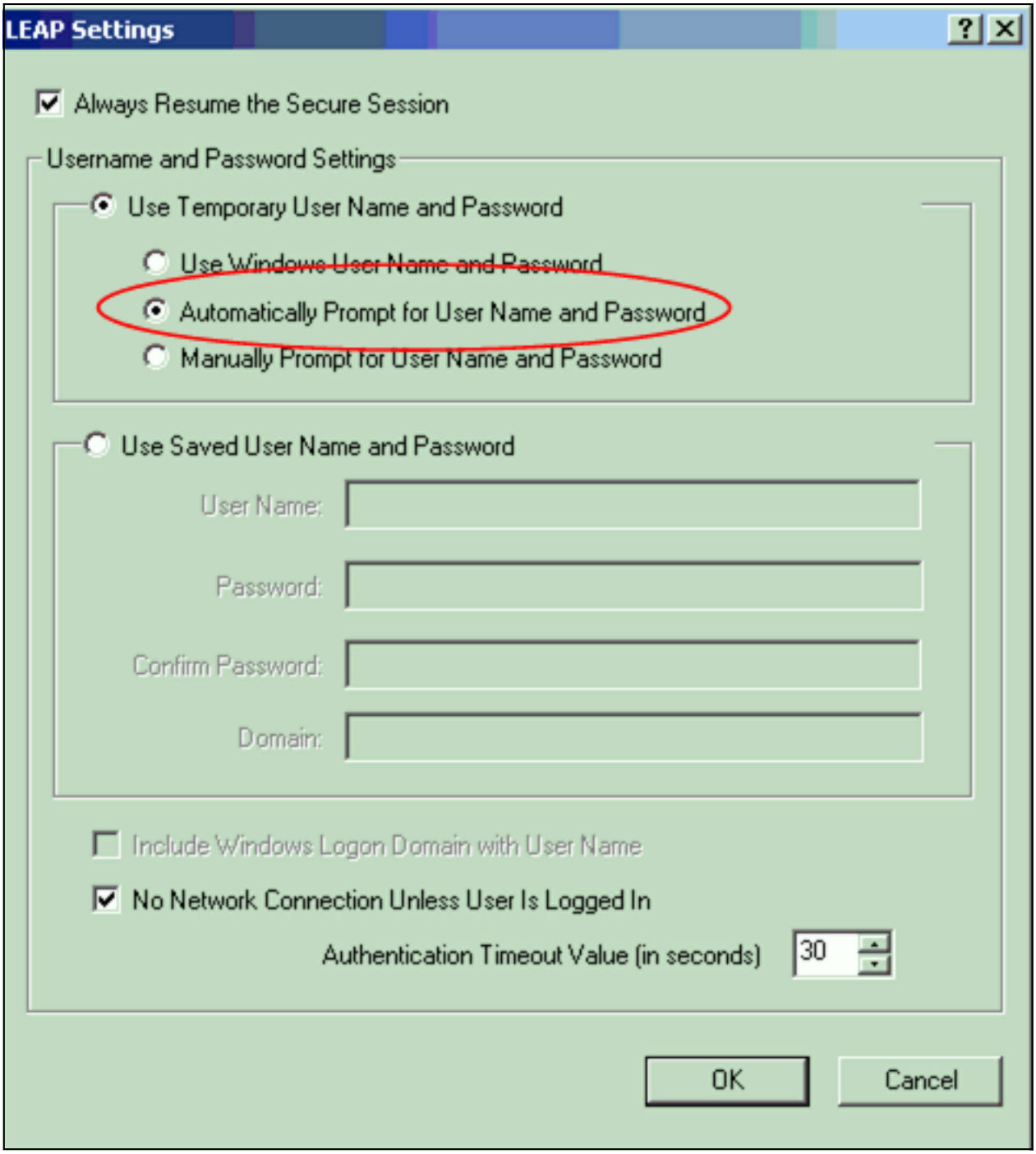
1. في إطار إدارة التوصيفات الموجود على وحدة التحكم في الوصول، انقر على **جديد** لإنشاء توصيف جديد.تظهر نافذة جديدة حيث يمكنك ضبط التكوين لعملية وضع WPA 2 على مستوى المؤسسة. تحت علامة التبويب عام أدخل اسم التوصيف واسم SSID الذي سيستخدمه محول العميل.في هذا المثال، يكون اسم التوصيف واسم SSID هما WPA2:**ملاحظة:** يجب أن يتطابق SSID مع SSID الذي قمت بتكوينه على نقطة الوصول ل WPA 2.



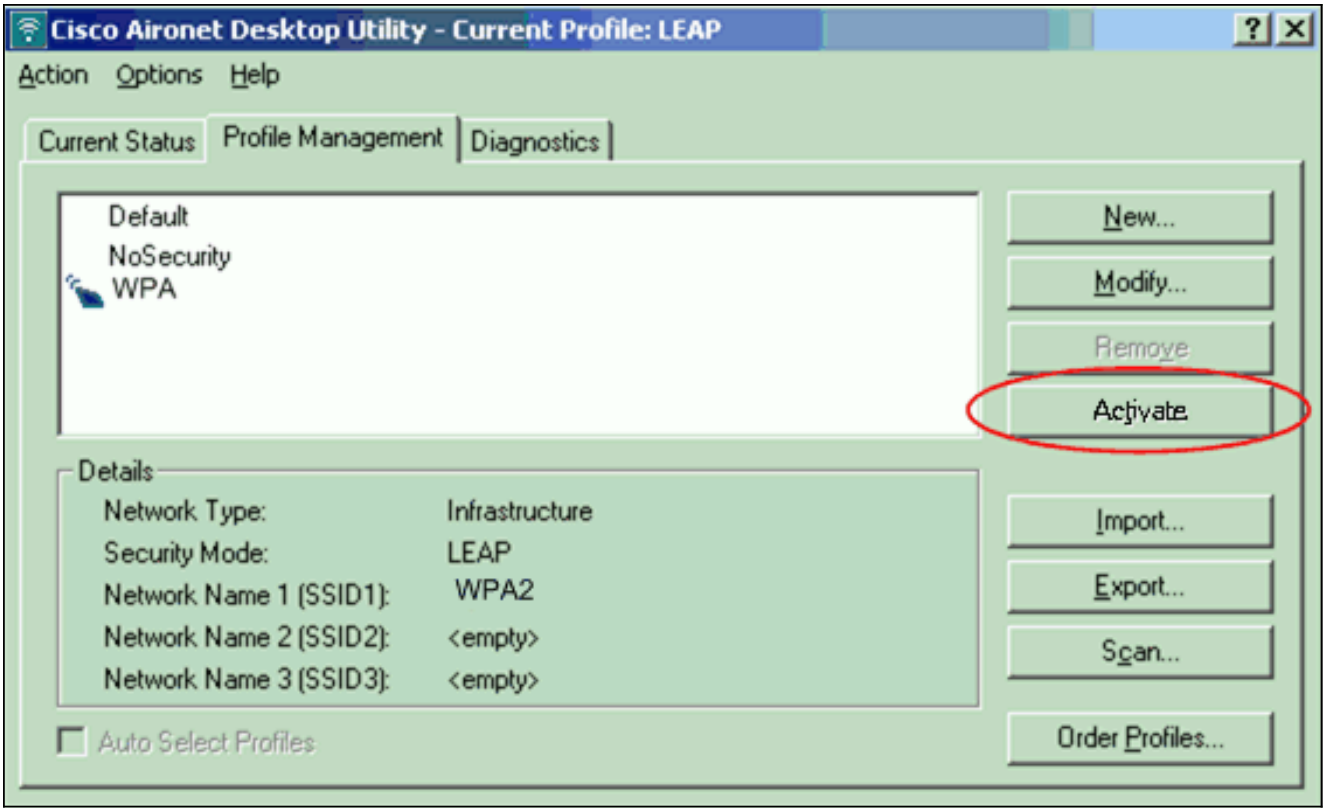
2. انقر على علامة التبويب **تأمين**، وانقر فوق **WPA/WPA2/CCKM**، واختر **LEAP** من قائمة نوع WPA/WPA2/CCKM EAP.يمكن هذا الإجراء إما WPA أو 2 WPA، أيهما تقوم بالتكوين على نقطة الوصول.



3. انقر على **تكوين** لتحديد إعدادات LEAP.
4. أخترت المناسب username وكلمة عملية إعداد، يؤسس على المتطلب، وطقطقة **ok**.يختار هذا تشكيل الخيار تلقائيا رسالة حث ل مستعمل إسم وكلمة. يتيح لك هذا الخيار إدخال اسم المستخدم وكلمة المرور يدويا عند إجراء مصادقة LEAP.



5. انقر على **موافق** للخروج من إطار إدارة التوصيفات.
6. انقر على **تنشيط** لتمكين هذا التوصيف على محول العميل.

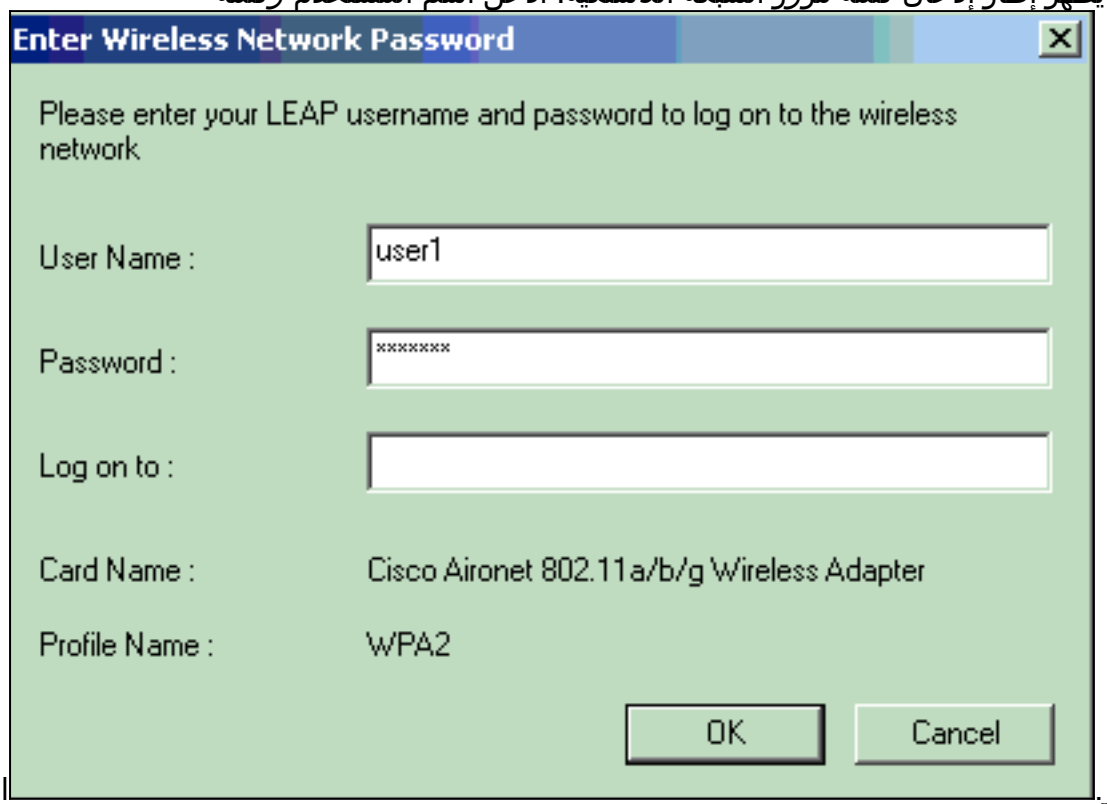


ملاحظة: إذا كنت تستخدم Microsoft Wireless Zero Configuration (WZC) لتكوين محول العميل، فإن WPA 2 غير متاح افتراضيا مع WZC. لذلك، للسماح للعملاء الذين تم تمكين WZC عليهم بتشغيل WPA 2، يجب تثبيت إصلاح سريع ل Microsoft Windows XP. ارجع إلى مركز التنزيل في Microsoft - تحديث (Windows XP (KB893357 للتثبيت.بعد تثبيت الإصلاح الساخن، يمكنك تكوين WPA 2 مع WZC.

التحقق من الصحة

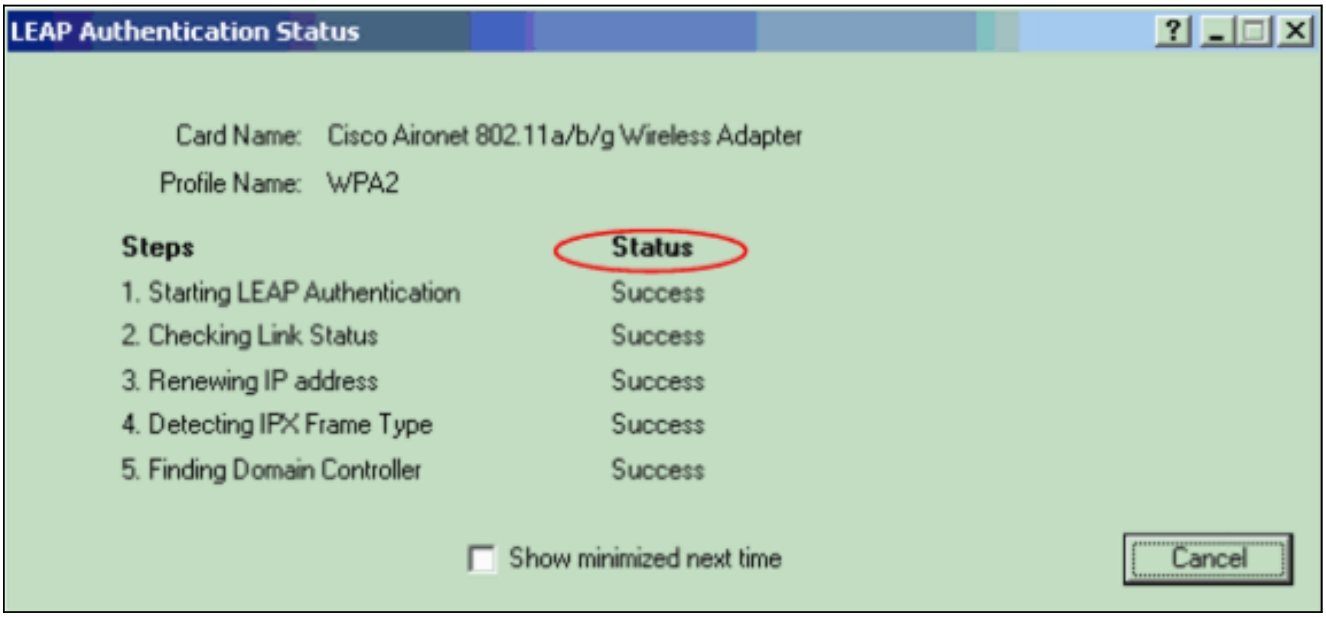
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

1. عندما يظهر إطار إدخال كلمة مرور الشبكة اللاسلكية، أدخل اسم المستخدم وكلمة المرور.الإطار التالي



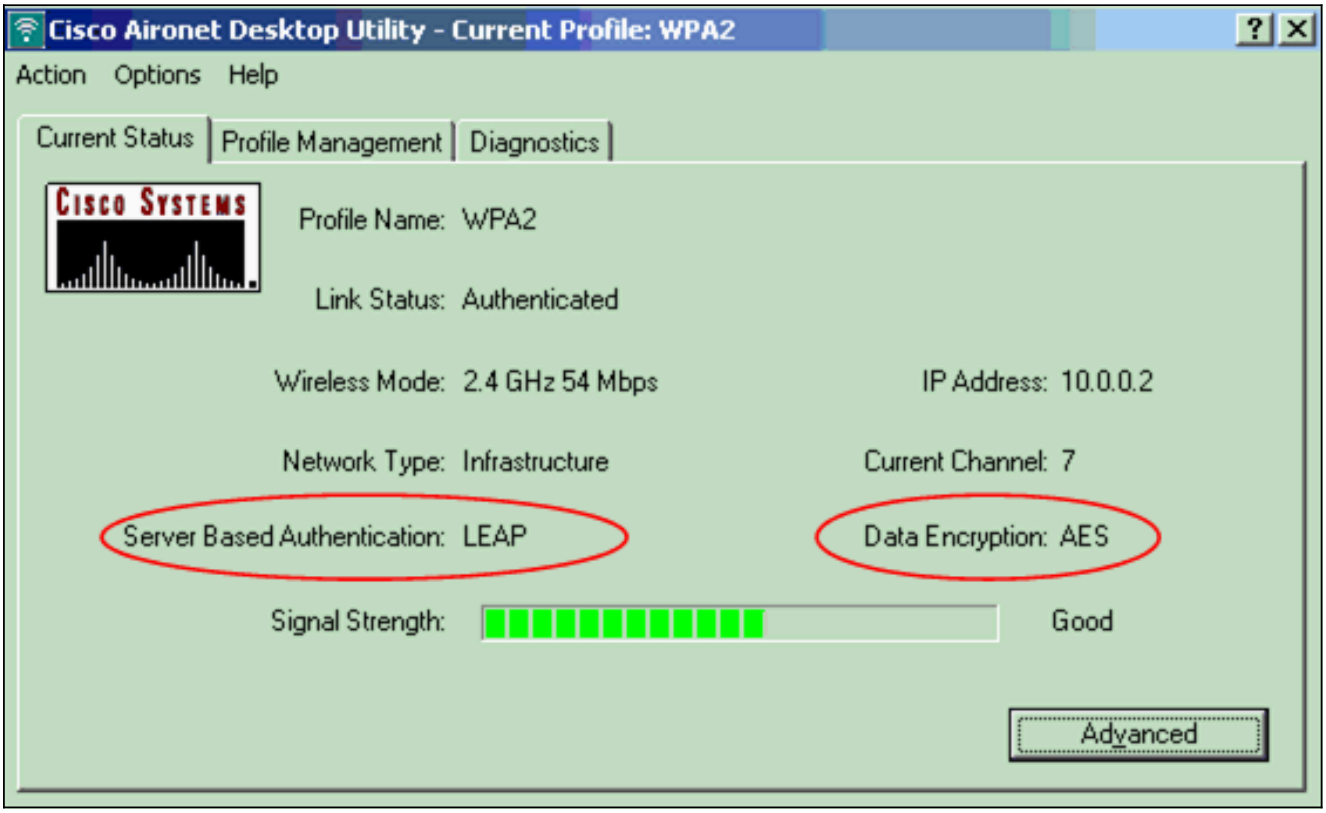
هو حالة مصادقة LEAP. تتحقق هذه المرحلة من بيانات اعتماد المستخدم مقابل خادم RADIUS المحلي.

2. تحقق من منطقة الحالة للاطلاع على نتيجة المصادقة.



في حالة نجاح المصادقة، يتصل العميل بشبكة LAN اللاسلكية.

3. تحقق من حالة ADU الحالية للتحقق من أن العميل يستخدم تشفير AES ومصادقة LEAP.هذا يظهر أنك طبقت WPA 2 بمصادقة LEAP وتشفير AES في WLAN.



4. تحقق من سجل أحداث AP/Bridge للتحقق من مصادقة العميل بنجاح مع WPA 2.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

التكوين في الوضع الشخصي

يشير مصطلح **الوضع الشخصي** إلى المنتجات التي يتم إختبارها لتكون قابلة للتشغيل البيني في وضع تشغيل PSK فقط للمصادقة. يتطلب هذا الوضع التكوين اليدوي لبطاقة PSK على نقطة الوصول والعملاء. يصادق PSK المستخدمين عبر كلمة مرور أو رمز تعريف على كل من محطة العميل و AP. لا يلزم وجود خادم مصادقة. يمكن للعميل الوصول إلى الشبكة فقط إذا كانت كلمة مرور العميل تطابق كلمة مرور AP. كما توفر كلمة المرور مادة الكبلات التي يستخدمها TKIP أو AES لإنشاء مفتاح تشفير لتشفير حزم البيانات. يستهدف الوضع الشخصي بيئات SOHO ولا يعتبر آمنا لبيئات المؤسسات. يزود هذا قسم التشكيل أن أنت تحتاج أن يطبق WPA 2 في الشخصي أسلوب عملية.

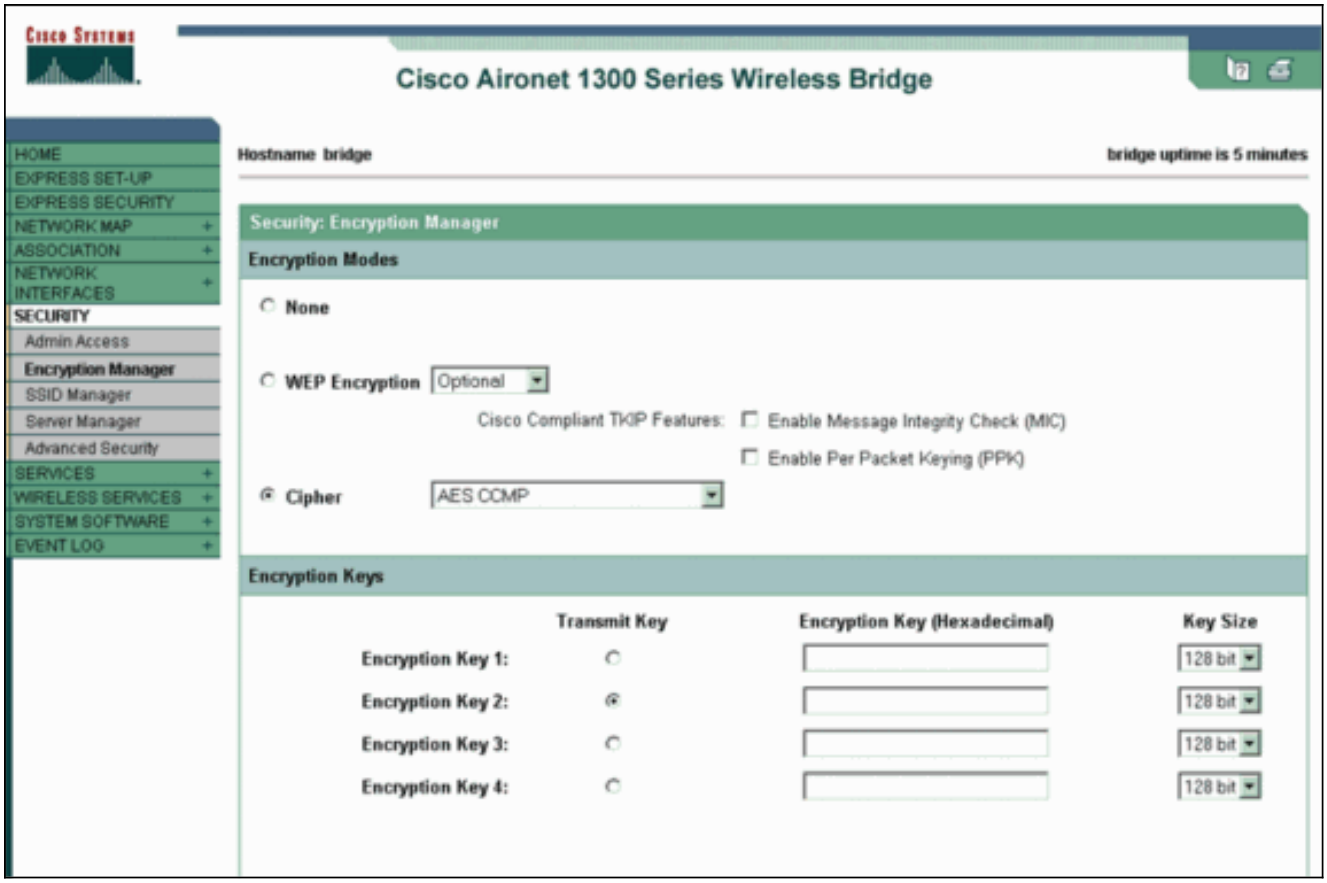
Network Setup (إعداد الشبكة)

في هذا الإعداد، يصدق مستخدم لديه مهايئ عميل متوافق مع WPA 2 على نقطة وصول/جسر Aironet 1310g. تتم إدارة المفاتيح باستخدام WPA 2 PSK، مع تكوين تشفير AES-CCMP. الأقسام تكوين نقطة الوصول وتكوين مهايئ العميل عرض التكوين على نقطة الوصول ومهايئ العميل.

قم بتكوين نقطة الوصول

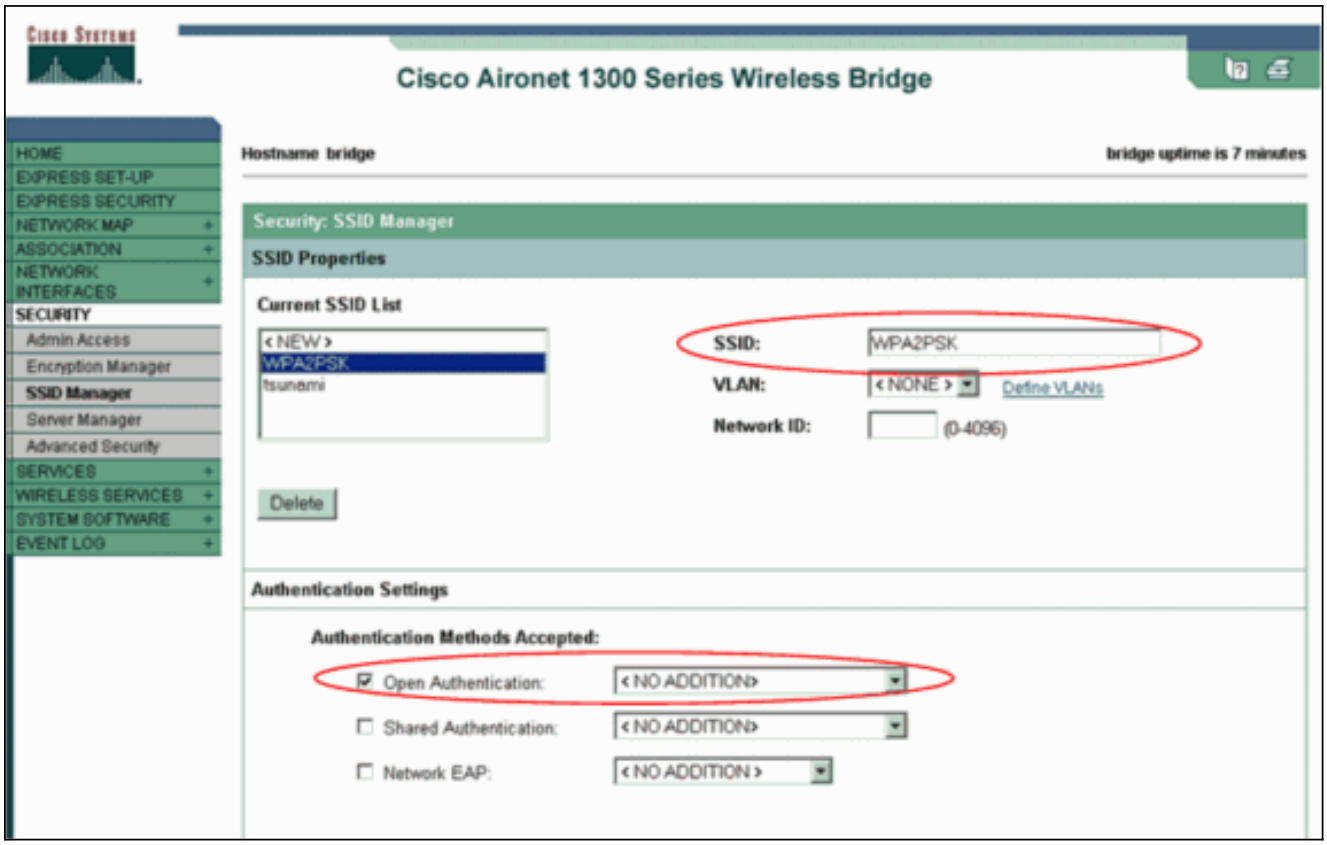
أكمل الخطوات التالية:

1. أختر **التأمين > مدير التشفير** في القائمة على اليسار وأكمل الخطوات التالية:من قائمة التشفير، أختر **AES CCMP**.يتيح هذا الخيار تشفير AES باستخدام وضع العداد مع CCMP.

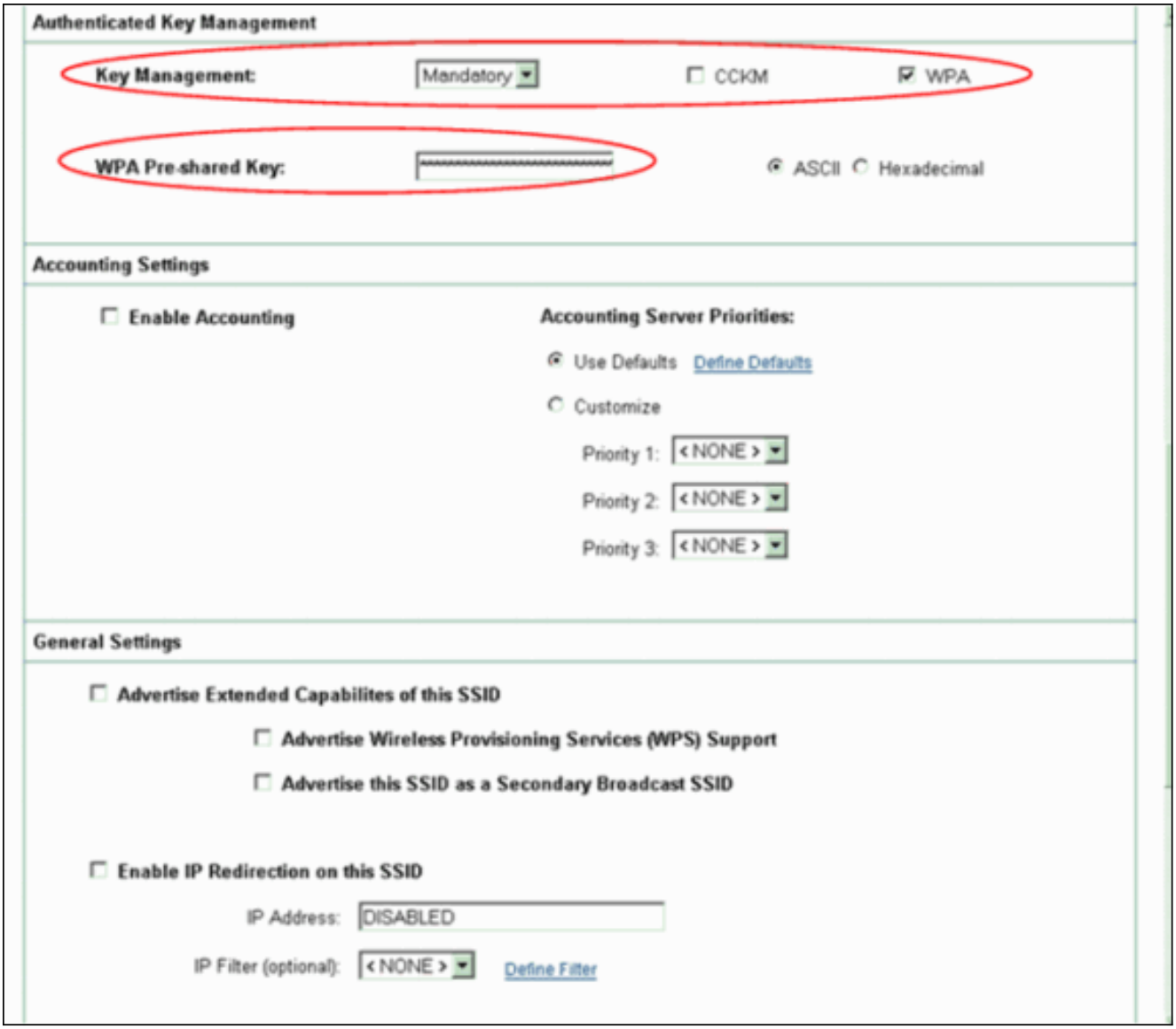


طقطقة **يطبق**.

2. أختر **تأمين > إدارة SSID** وقم بإنشاء SSID جديد للاستخدام مع WPA 2.حدد خانة الاختيار **فتح المصادقة**.



انزلق لأسفل الأمان: إطار مدير SSID إلى منطقة إدارة المفاتيح المصدق عليها وإكمال الخطوات التالية:من قائمة إدارة المفاتيح، أختر **إلزامي**.حدد خانة الاختيار **WPA** الموجودة على اليمين.



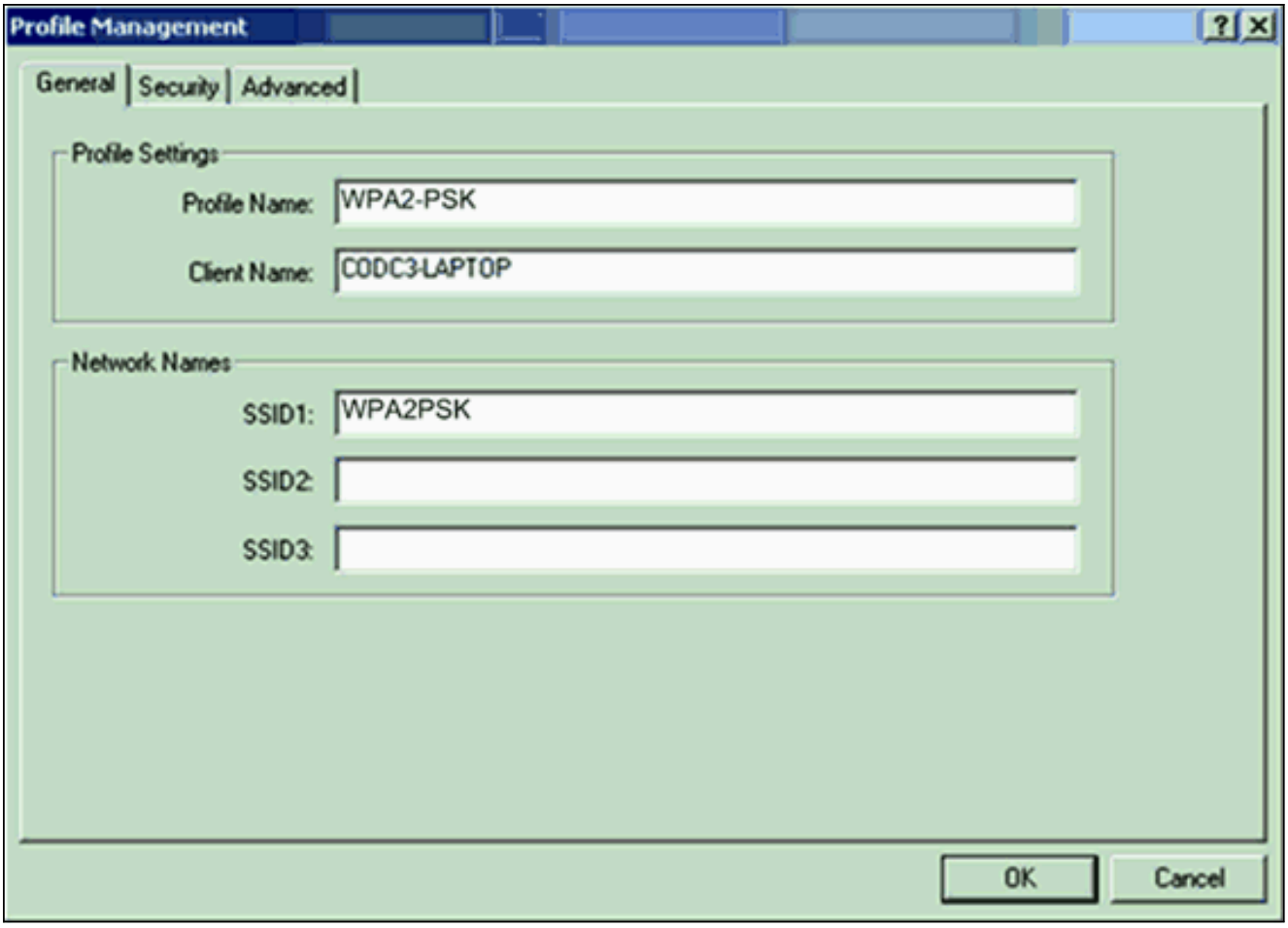
أدخل المفتاح السري المشترك WPA PSK أو مفتاح عبارة المرور WPA PSK.يجب أن يتطابق هذا المفتاح مع مفتاح WPA PSK الذي تقوم بتكوينه على محول العميل.طقطقة **يطبق**.

يمكن لنقطة الوصول الآن تلقي طلبات المصادقة من العملاء اللاسلكيين.

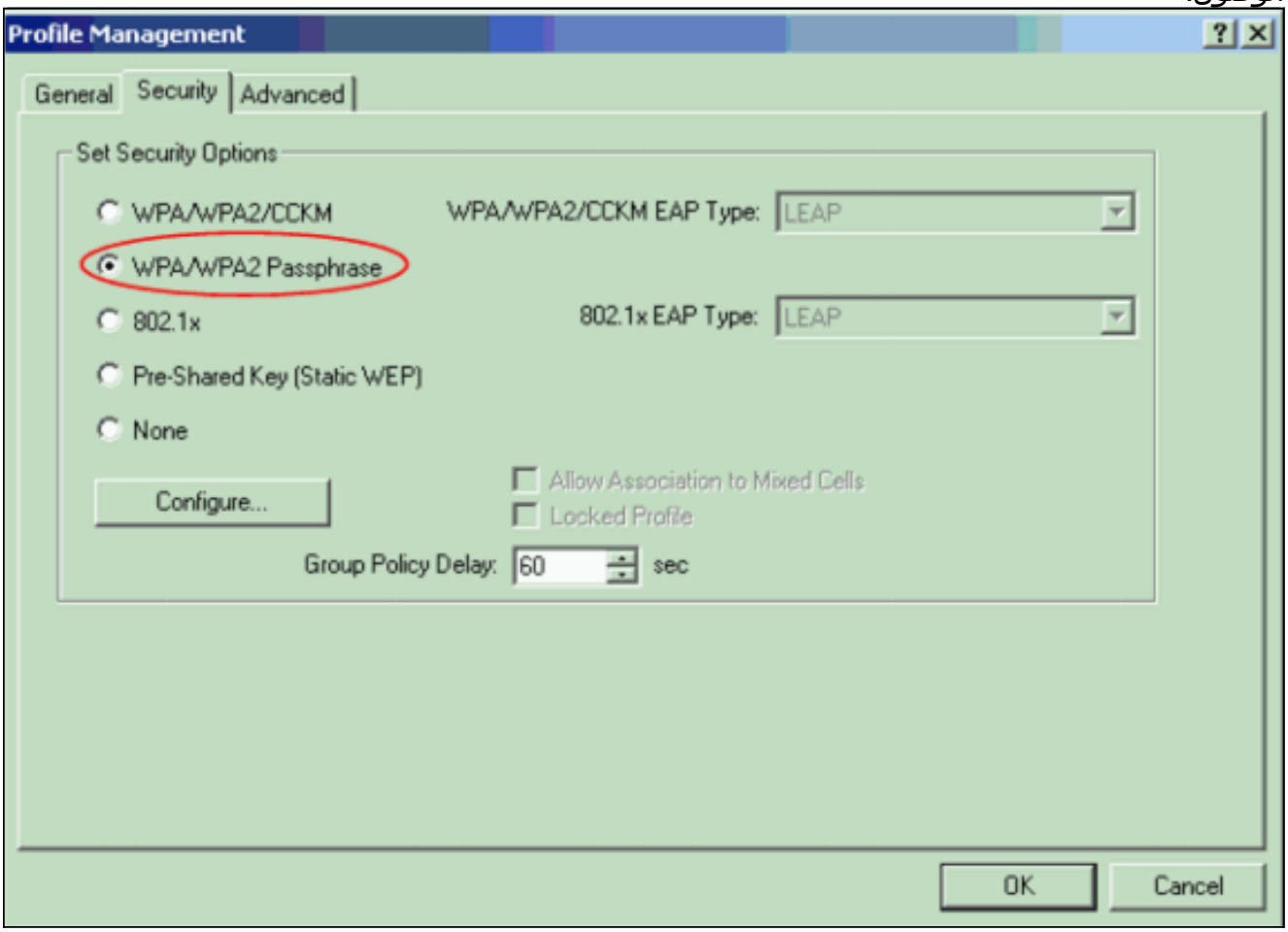
تكوين محول العميل

أكمل الخطوات التالية:

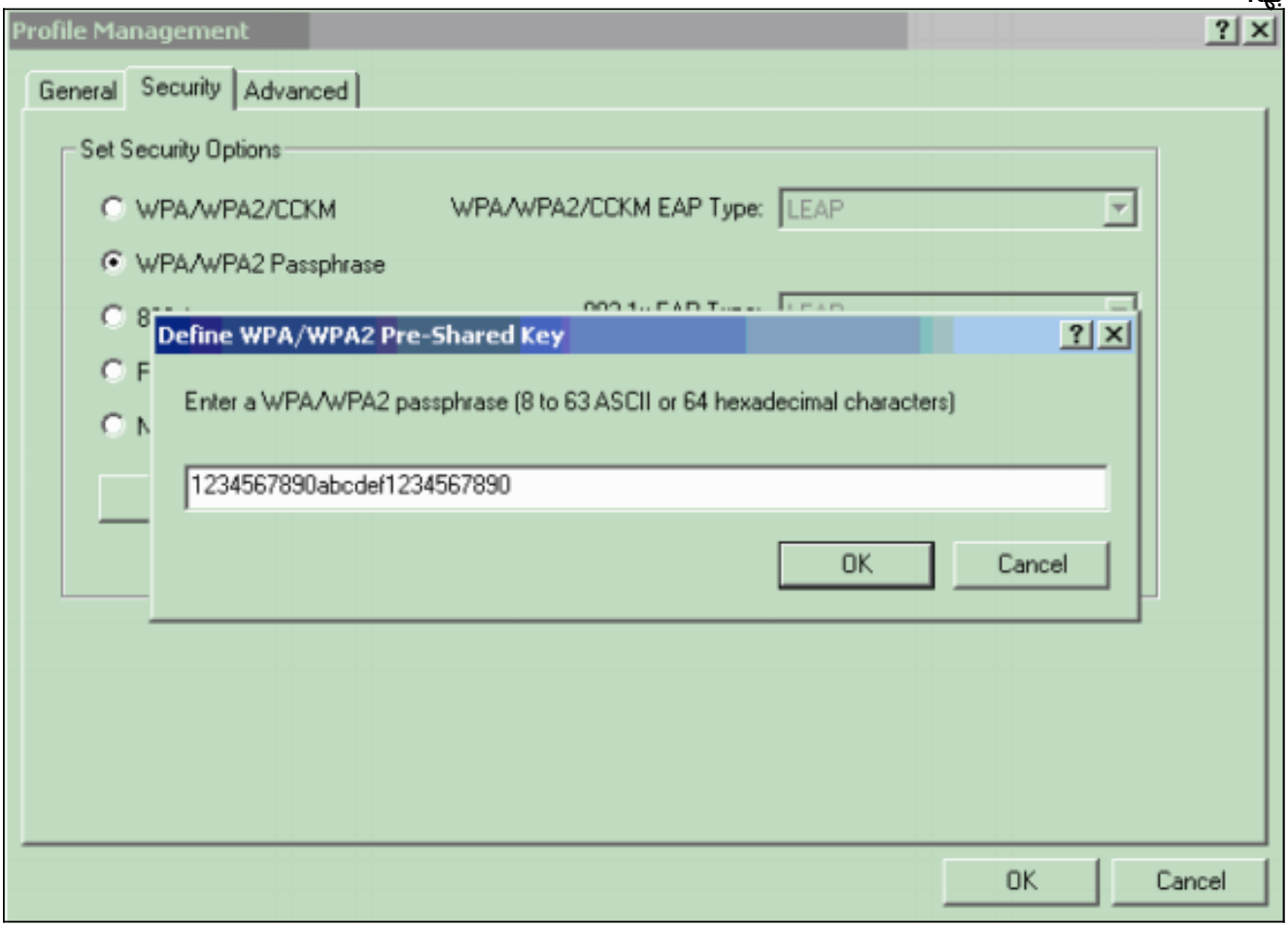
1. في إطار إدارة التوصيفات الموجود على وحدة التحكم في الوصول، انقر على **جديد** لإنشاء توصيف جديد.تعرض نافذة جديدة حيث يمكنك ضبط التكوين لوضع التشغيل WPA 2 PSK. تحت علامة التبويب عام أدخل اسم التوصيف واسم SSID الذي سيستخدمه محول العميل.في هذا المثال، اسم التوصيف هو WPA2-PSK و SSID هو WPA2PSK:**ملاحظة:** يجب أن يتطابق SSID مع SSID الذي قمت بتكوينه على نقطة الوصول ل WPA 2 PSK.



2. انقر على علامة التبويب **تأمين** وانقر فوق **عبارة مرور WPA/WPA2**.يمكن هذا الإجراء إما WPA PSK أو WPA 2 PSK، أيهما تقوم بالتكوين على نقطة الوصول.



3. طقطقة **يشكل**.تعريف نافذة مفاتيح WPA/WPA2 المشتركة مسبقا.
4. احصل على عبارة مرور WPA/WPA2 من مسؤول النظام وأدخل عبارة المرور في حقل عبارة المرور WPA/WPA2.احصل على عبارة المرور لنقطة الوصول في شبكة بنية أساسية أو عبارة المرور لعملاء آخرين في شبكة أقران.أستخدم هذه الإرشادات لإدخال عبارة مرور:يجب أن تحتوي عبارات مرور WPA/WPA2 على ما بين 8 و 63 حرف نص ASCII أو 64 حرف سادس عشري.يجب أن تطابق عبارة مرور WPA/WPA2 لمهايئ العميل عبارة مرور نقطة الوصول التي تخطط للاتصال بها.



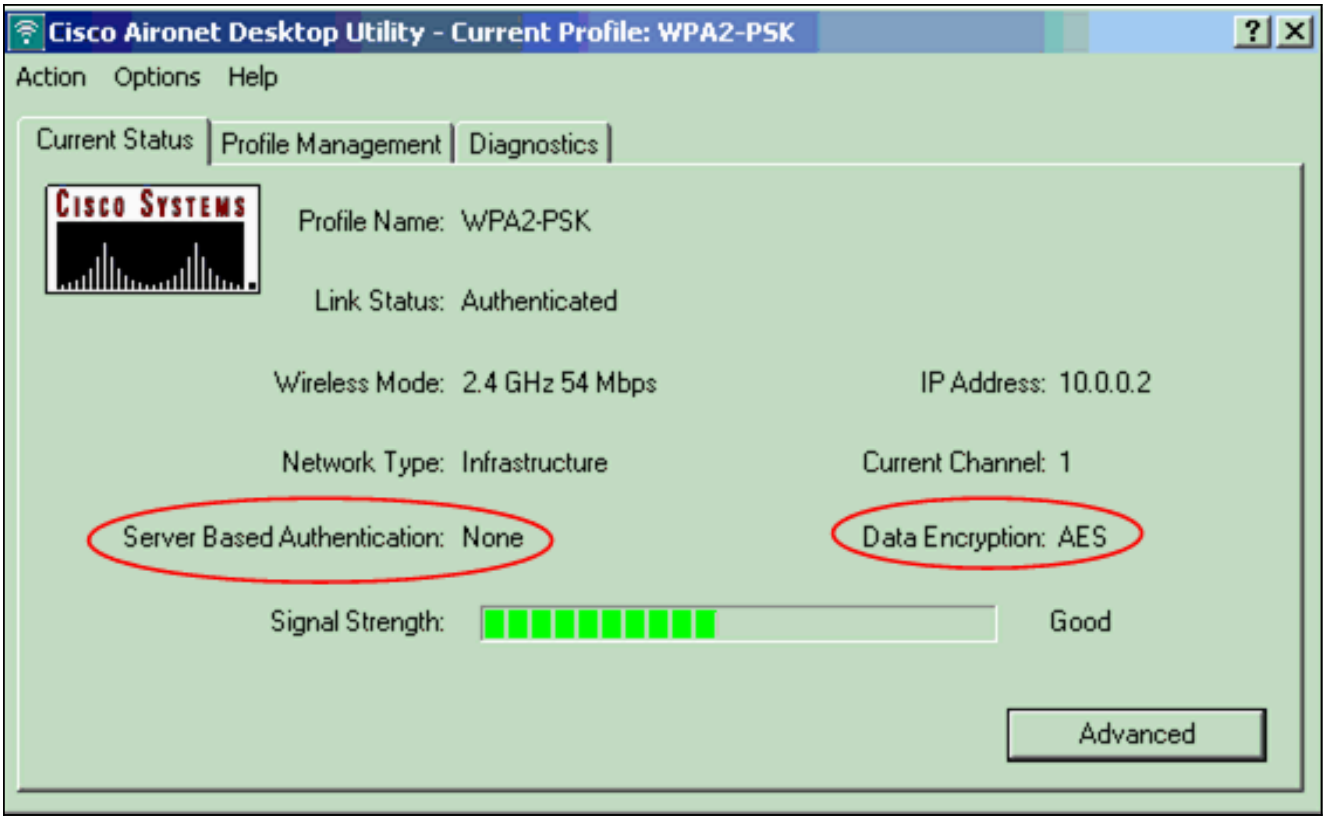
5. طقطقة **ok** in order to أنقذت عبارة المرور ورجعت إلى التوصيف إدارة نافذة.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

بعد تنشيط ملف تعريف WPA 2 PSK، تصادق نقطة الوصول على العميل استنادا إلى عبارة مرور PSK) WPA 2) وتوفر الوصول إلى شبكة WLAN.

1. تحقق من حالة ADU الحالية للتحقق من المصادقة الناجحة.تقدم هذه النافذة مثالا. يوضح الإطار أن التشفير المستخدم هو AES وأنه لا يتم إجراء مصادقة مستندة إلى الخادم:



2. تحقق من سجل أحداث نقطة الوصول/الجسر للتحقق من مصادقة العميل بنجاح مع وضع المصادقة WPA 2 PSK.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- تكوين مجموعات التشفير و WEP
- تكوين أنواع المصادقة

- نظرة عامة على تكوين WPA
- WPA2 - Wi-Fi Protected Access 2
- ما هي عملية وضع WPA المختلط، وكيف يمكنني تكوينها في نقطة الوصول الخاصة بي
- صفحة الدعم اللاسلكي
- الدعم التقني والمستندات - Cisco Systems

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