مثال تكوين إعادة توجيه صفحة ويب لوحدة تحكم شبكة LAN اللاسلكية

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين ميزة إعادة توجيه صفحة البداية على وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- معرفة حلول أمان LWAPP
- معرفة كيفية تكوين ACS الآمن من Cisco

المكونات المستخدمة

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

- وحدة التحكم في شبكة LAN اللاسلكية (WLC) من Cisco 4400 Series التي تشغل الإصدار 5.0 من البرنامج الثابت

- نقطة الوصول (LAP) خفيفة الوزن للسلسلة Cisco 1232 Series
- مهايئ العميل اللاسلكي Cisco Aironet 802.a/b/g الذي يشغل الإصدار 4.1 من البرنامج الثابت
- خادم ACS الآمن من Cisco الذي يشغل الإصدار 4.1
- أي خادم ويب خارجي تابع لجهة خارجية

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

إعادة توجيه صفحة البداية على الويب هي ميزة مقدمة مع وحدة التحكم في الشبكة المحلية اللاسلكية الإصدار 5.0. باستخدام هذه الميزة، تتم إعادة توجيه المستخدم إلى صفحة ويب معينة بعد اكتمال مصادقة 802.1x. تحدث عملية إعادة التوجيه عندما يفتح المستخدم متصفح (تم تكوينه بصفحة رئيسية افتراضية) أو يحاول الوصول إلى URL. بعد اكتمال عملية إعادة التوجيه إلى صفحة الويب، يصبح للمستخدم حق الوصول الكامل إلى الشبكة.

يمكنك تحديد صفحة إعادة التوجيه على خادم خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS). يجب تكوين خادم RADIUS لإرجاع سمة RADIUS الخاصة ب Cisco AV-pair url-redirect إلى وحدة التحكم في الشبكة المحلية اللاسلكية عند مصادقة 802.1x الناجحة.

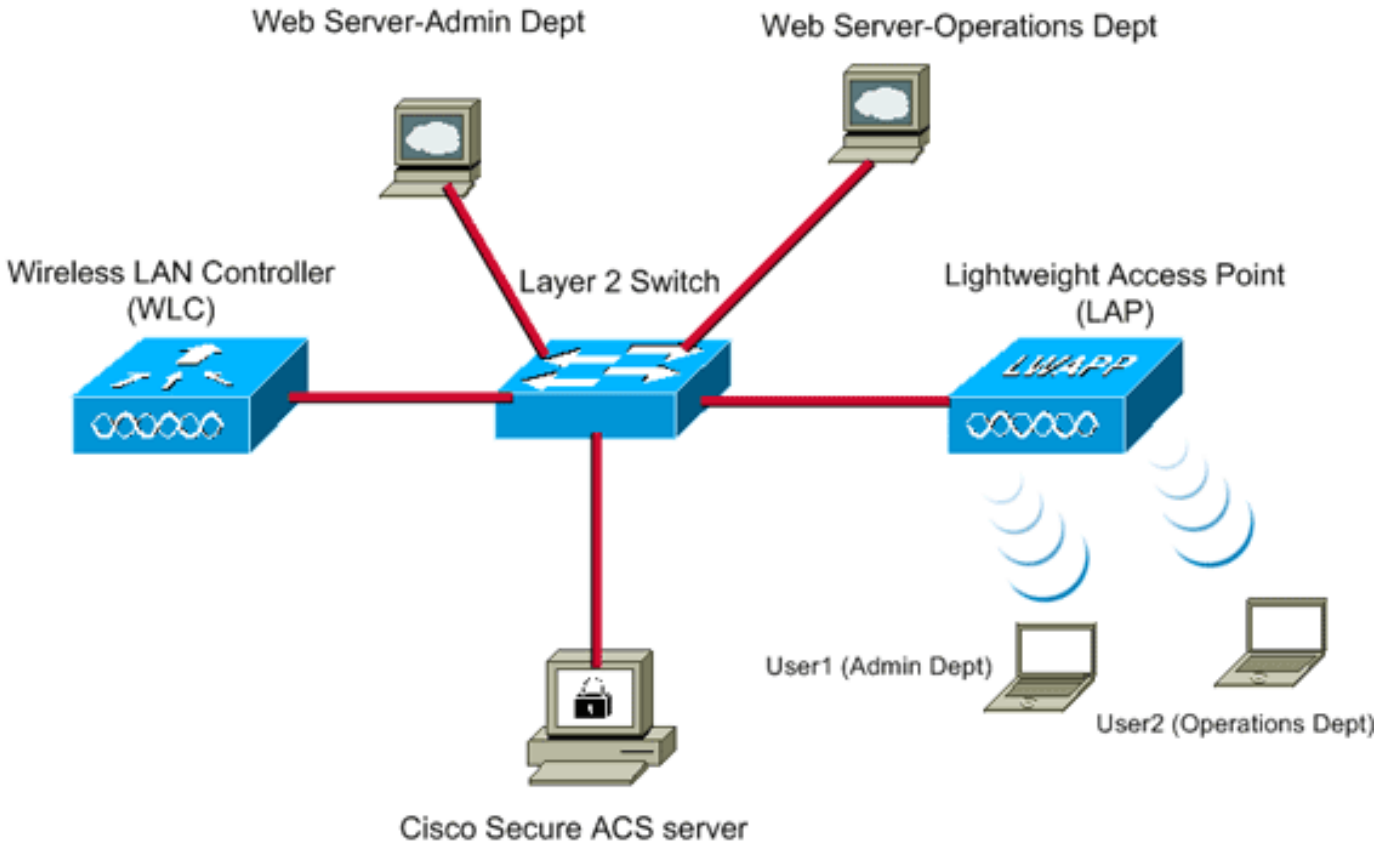
تتوفر ميزة إعادة توجيه صفحة البداية للشبكة المحلية اللاسلكية (WLANs) فقط للشبكات المحلية اللاسلكية (WLANs) التي تم تكوينها لتأمين 802.1x أو تأمين WPA/WPA2 من الطبقة 2.

Network Setup (إعداد الشبكة)

في هذا مثال، cisco 4404 WLC و {upper}lap cisco 1232 sery ربطت من خلال طبقة 2 مفتاح. كما يتم توصيل خادم Cisco Secure ACS (الذي يعمل كخادم RADIUS خارجي) بنفس المحول. توجد جميع الأجهزة في الشبكة الفرعية نفسها.

يتم تسجيل نقاط الوصول في الوضع Lightweight (LAP) في البداية إلى وحدة التحكم. يجب إنشاء شبكتي WLAN: واحدة لمستخدمي **قسم** الإدارة والأخرى لمستخدمي **قسم العمليات**. تستخدم كلا شبكتي الشبكة المحلية اللاسلكية WPA2/ AES (يستخدم EAP-FAST للمصادقة). تستخدم كلتا شبكتي WLAN ميزة إعادة توجيه صفحة البداية من أجل إعادة توجيه المستخدمين إلى عناوين URL المناسبة للصفحة الرئيسية (على خوادم الويب الخارجية).

يستخدم هذا المستند إعداد الشبكة التالي:



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

يشرح القسم التالي كيفية تكوين الأجهزة لهذا الإعداد.

التكوين

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

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

أتمت هذا steps in order to شكلت الأداة أن يستعمل الطفرة صفحة redirect سمة:

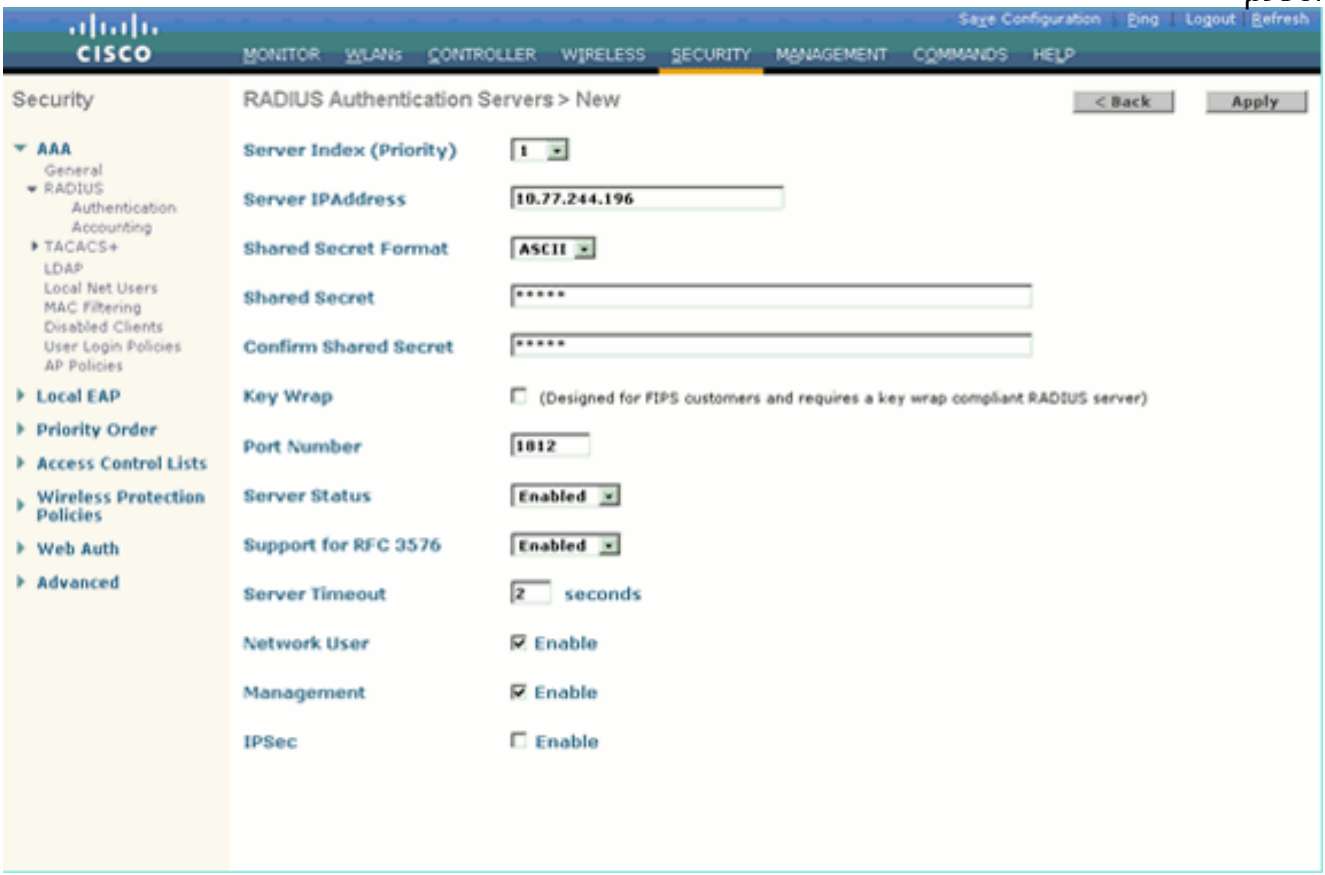
1. قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة RADIUS من خلال خادم ACS الآمن من Cisco.
2. قم بتكوين شبكات WLAN لقسم "الإدارة" وقسم "العمليات".
3. قم بتكوين ACS الآمن من Cisco لدعم ميزة إعادة توجيه صفحة البداية.

الخطوة 1. قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة RADIUS من خلال خادم ACS الآمن من Cisco.

يلزم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإعادة توجيه بيانات اعتماد المستخدم إلى خادم RADIUS خارجي.

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

1. أخترت **أمن** و**RADIUS صحة هوية** من الجهاز تحكم gui in order to عرضت ال RADIUS صحة هوية نادل صفحة.
2. انقر فوق **جديد** لتحديد خادم RADIUS.
3. قم بتعريف معلمات خادم RADIUS على خوادم مصادقة RADIUS > صفحة جديدة.وتتضمن هذه المعلمات ما يلي:عنوان IP لخادم RADIUSسر مشتركرقم المنفذحالة الخادم



يستعمل هذا وثيقة ال ACS نادل مع عنوان 10.77.244.196.

4. طقطقة **يطبق**.

الخطوة 2. قم بتكوين شبكات WLAN لقسم "الإدارة" و"العمليات".

في هذه الخطوة، تقوم بتكوين شبكتي WLAN (واحدة لقسم "الإدارة" وأخرى لقسم "العمليات") اللتين سيستخدمهما العملاء للاتصال بالشبكة اللاسلكية.

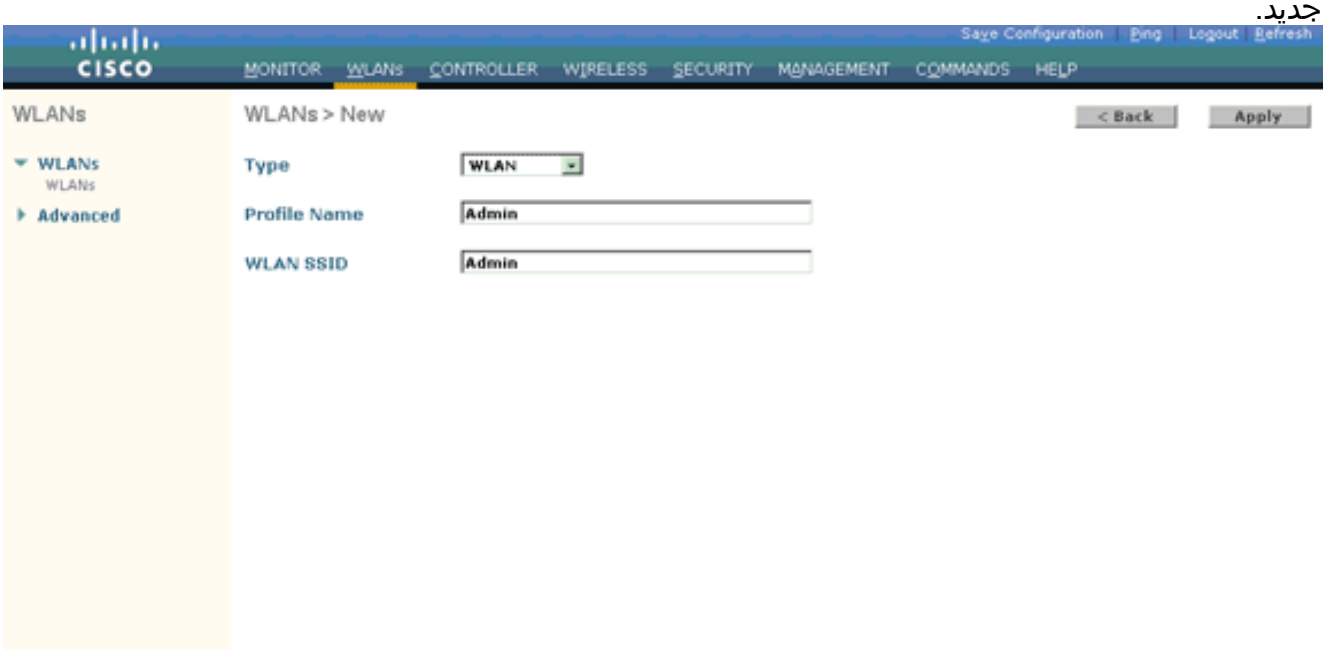
سيكون WLAN SSID لقسم "الإدارة" هو *Admin*. ستكون SSID WLAN لقسم "العمليات" هي "العمليات".

أستخدم مصادقة EAP-FAST لتمكين WPA2 كآلية تأمين الطبقة 2 على كل من شبكات WLAN ونهج الويب - ميزة إعادة توجيه صفحة البداية للويب كطريقة تأمين الطبقة 3.

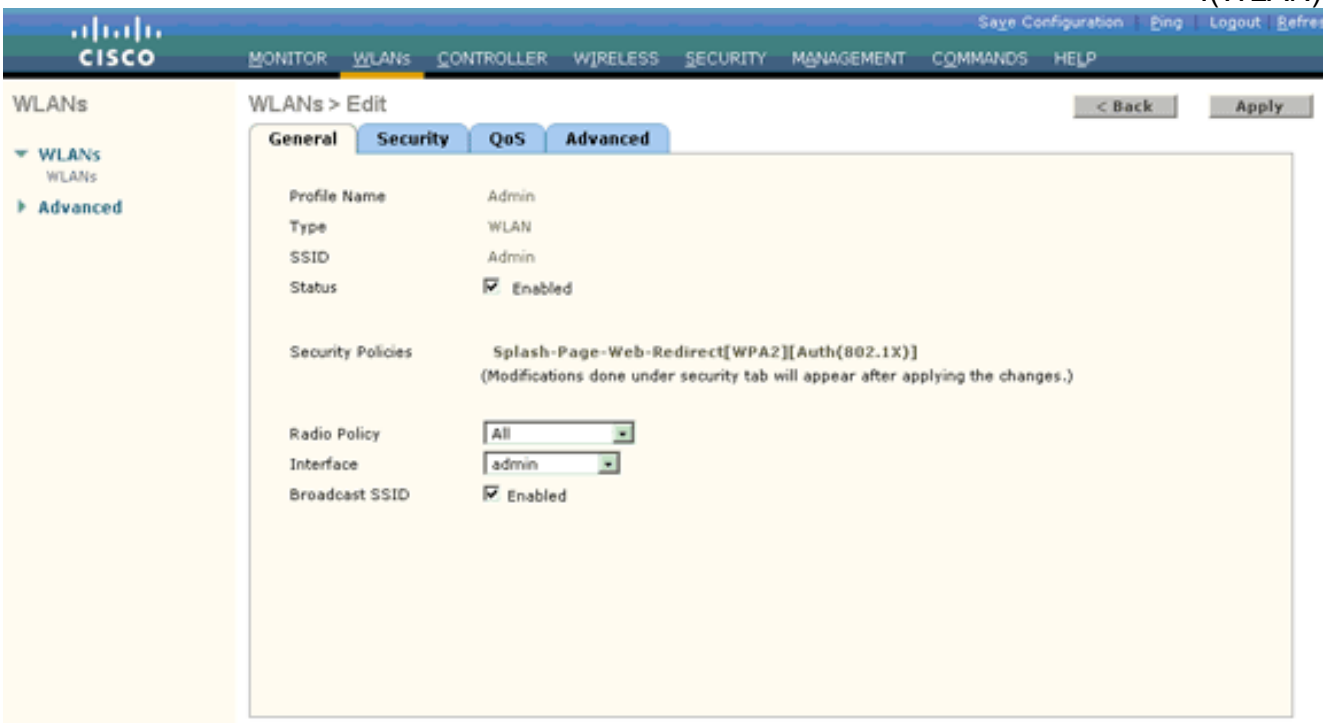
أكمل هذه الخطوات لتكوين شبكة WLAN والمعلمات المرتبطة بها:

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

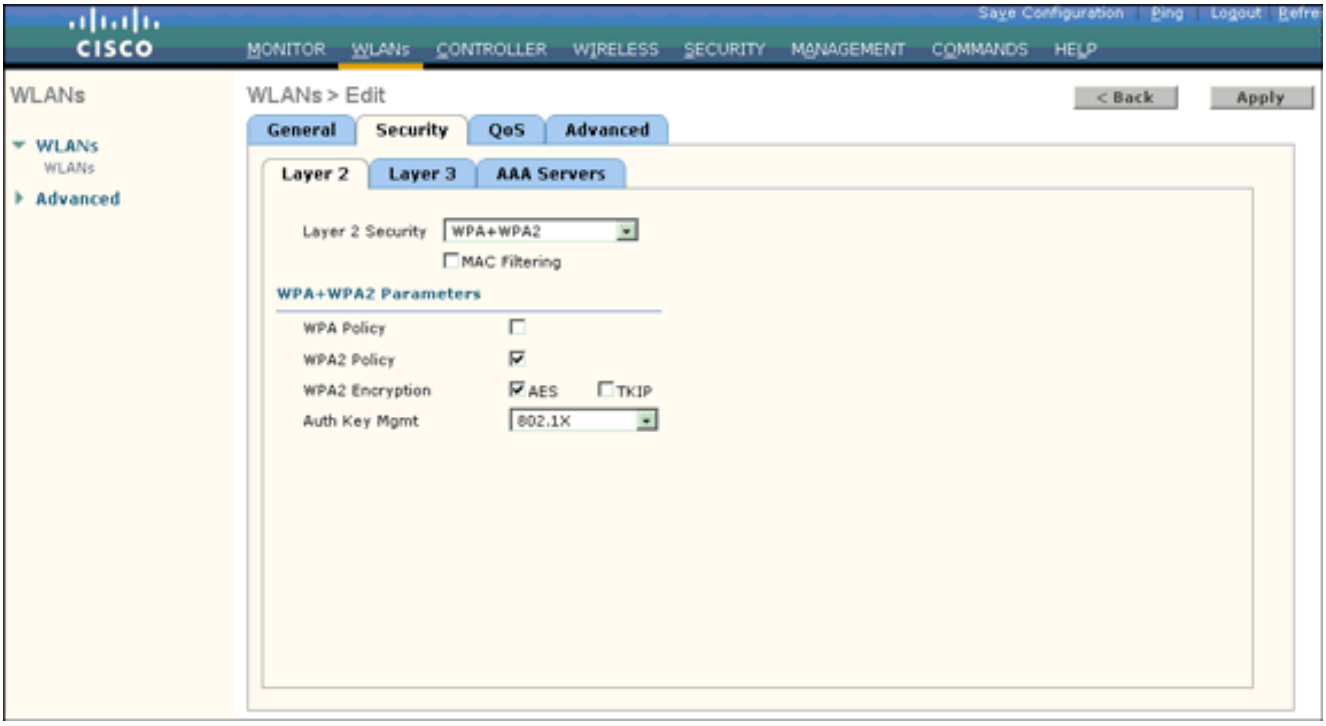
جديد.



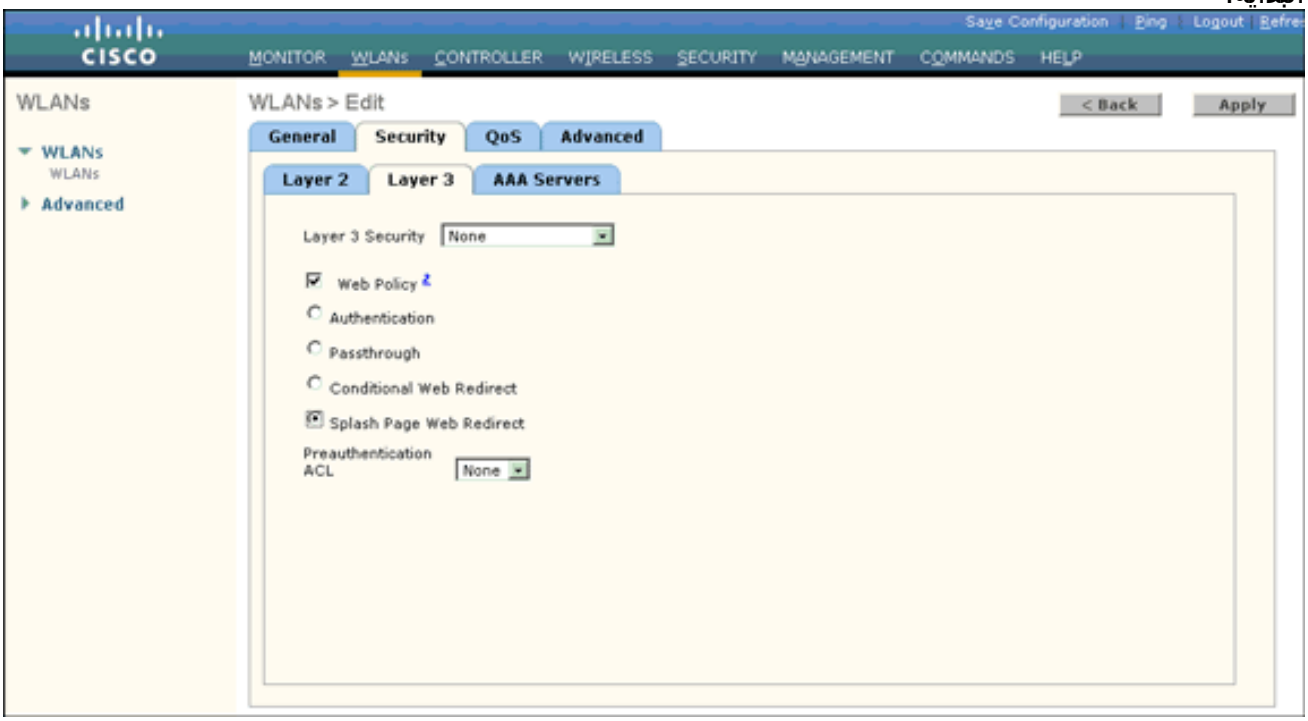
3. أدخل اسم SSID الخاص بشبكة WLAN واسم التوصيف على شبكات WLAN > صفحة جديدة.
4. طقطقة **يطبق**.
5. أولا، فلنقم بإنشاء شبكة WLAN لقسم "الإدارة".ما إن يخلق أنت WLAN جديد، ال WLAN > تحرير صفحة ل ال WLAN جديد يظهر. في هذه الصفحة، يمكنك تحديد معلمات مختلفة خاصة بشبكة WLAN هذه. ويتضمن ذلك السياسات العامة، وسياسات الأمان، ونهج جودة الخدمة، والمعلمات المتقدمة.
6. تحت سياسات عامة، حدد خانة الاختيار **الحالة** لتمكين الشبكة المحلية اللاسلكية (WLAN).



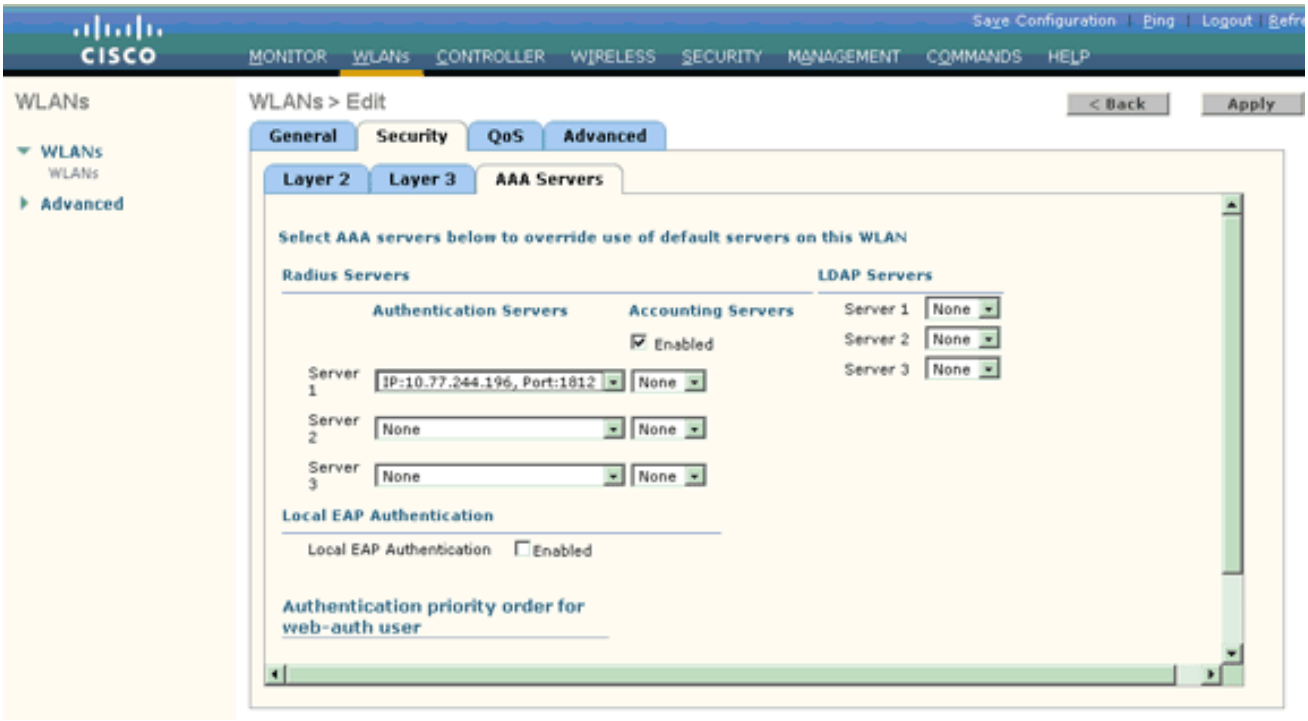
7. انقر صفحة **التأمين**، ثم انقر صفحة **الطبقة 2**.
8. أختر **WPA+WPA2** من القائمة المنسدلة تأمين الطبقة 2.تمكن هذه الخطوة مصادقة WPA للشبكة المحلية اللاسلكية (WLAN).
9. تحت معلمات WPA+WPA2، تحقق من خانات تأشير **سياسة WPA2** و**تشفير AES**.



10. أختر **802.1x** من القائمة المنسدلة إدارة مفتاح المصادقة. يتيح هذا الخيار WPA2 مع مصادقة 802.1x/EAP وتشفير AES للشبكة المحلية اللاسلكية (WLAN).
11. انقر صفحة **تأمين الطبقة 3**.
12. حدد مربع **نهج الويب**، ثم انقر فوق الزر **إعادة توجيه صفحة البداية** على الويب.يتيح هذا الخيار ميزة إعادة توجيه صفحة
البداية.

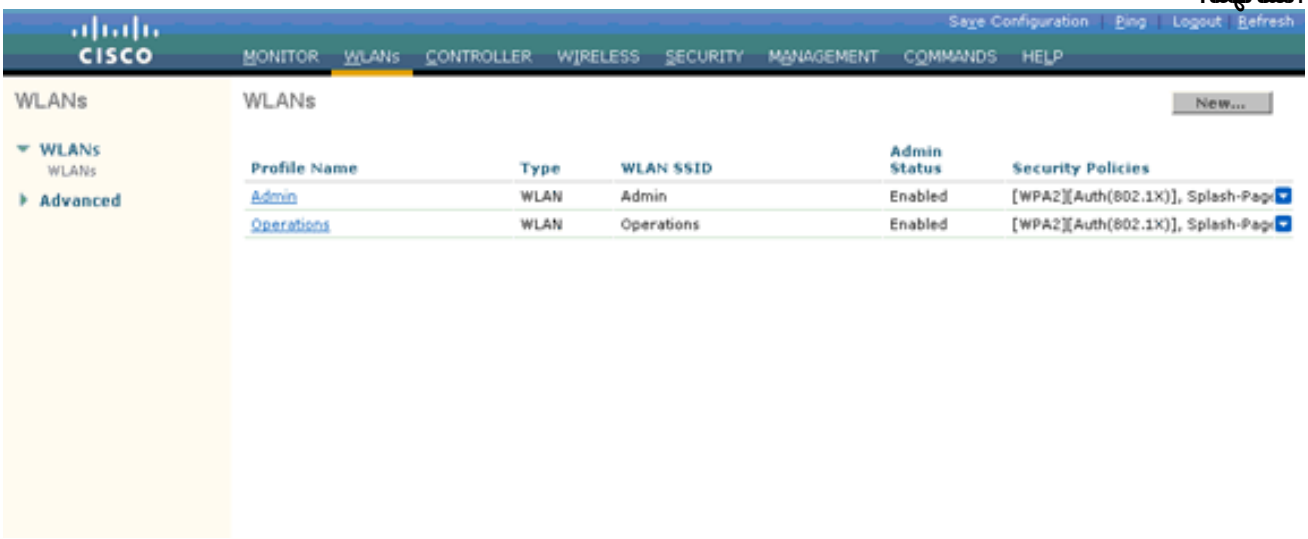


13. انقر فوق علامة التبويب **خوادم AAA**.
14. تحت مصادقة الخادم، أختر عنوان IP المناسب للخادم من القائمة المنسدلة الخادم
.1



في هذا المثال، يتم إستخدام 10.77.244.196 كخادم RADIUS.

15. طقطقة **يطبق**.
16. كرر الخطوات من 2 إلى 15 لإنشاء شبكة WLAN لقسم "العمليات".تسرد صفحة شبكات WLAN شبكتي WLAN اللتين أنشأتهما.



لاحظ أن سياسات التأمين تتضمن إعادة توجيه صفحة البداية.

الخطوة 3. قم بتكوين ACS الآمن من Cisco لدعم ميزة إعادة توجيه صفحة Splash.

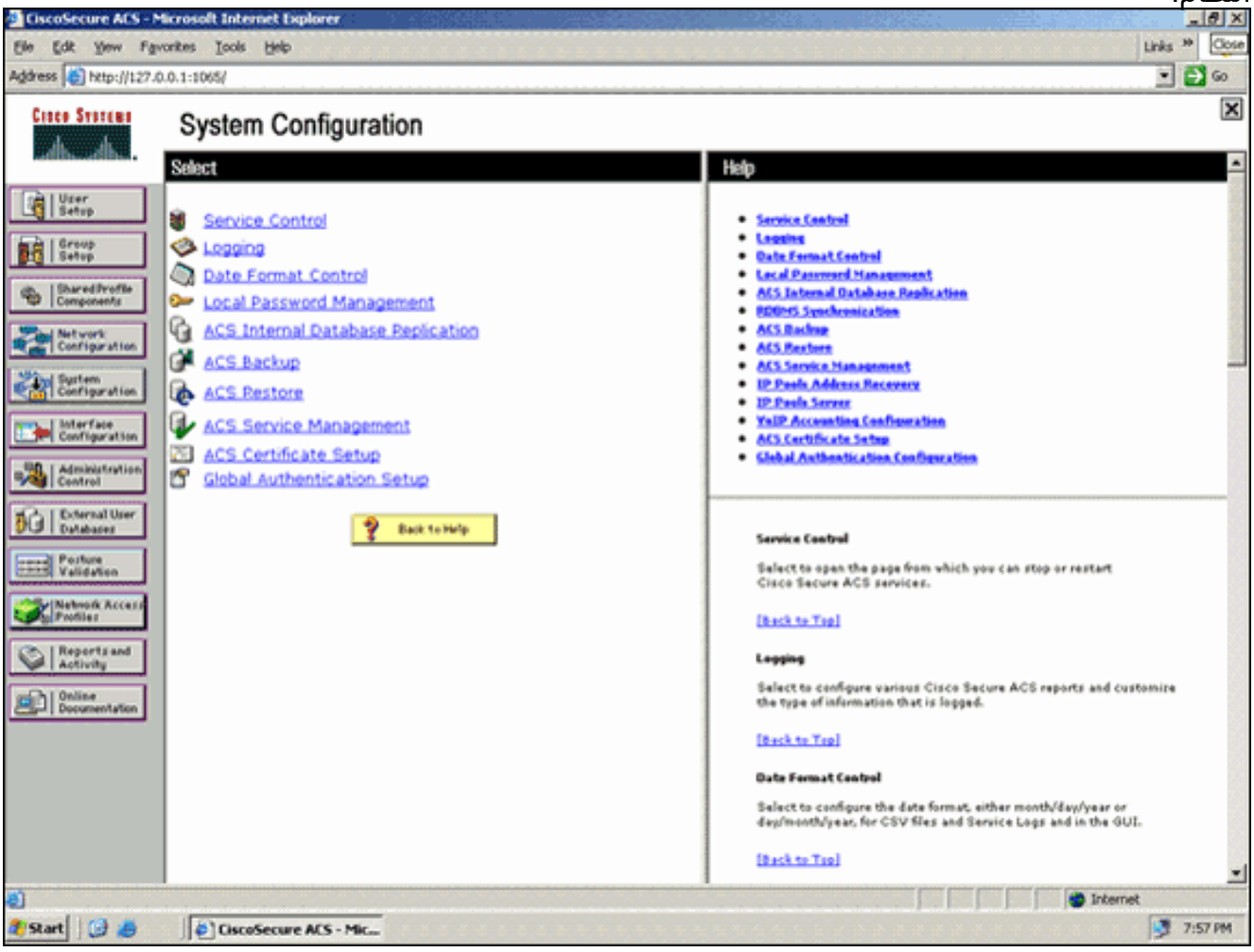
تتمثل الخطوة التالية في تكوين خادم RADIUS لهذه الميزة. يحتاج خادم RADIUS إلى إجراء مصادقة EAP-FAST للتحقق من مسوغات العميل، وعند نجاح المصادقة، لإعادة توجيه المستخدم إلى URL (على خادم الويب الخارجي) المحدد في سمة RADIUS ***لإعادة توجيه عنوان URL*** مزدوج من Cisco.

تكوين مصدر المحتوى الإضافي الآمن من Cisco لمصادقة EAP-FAST

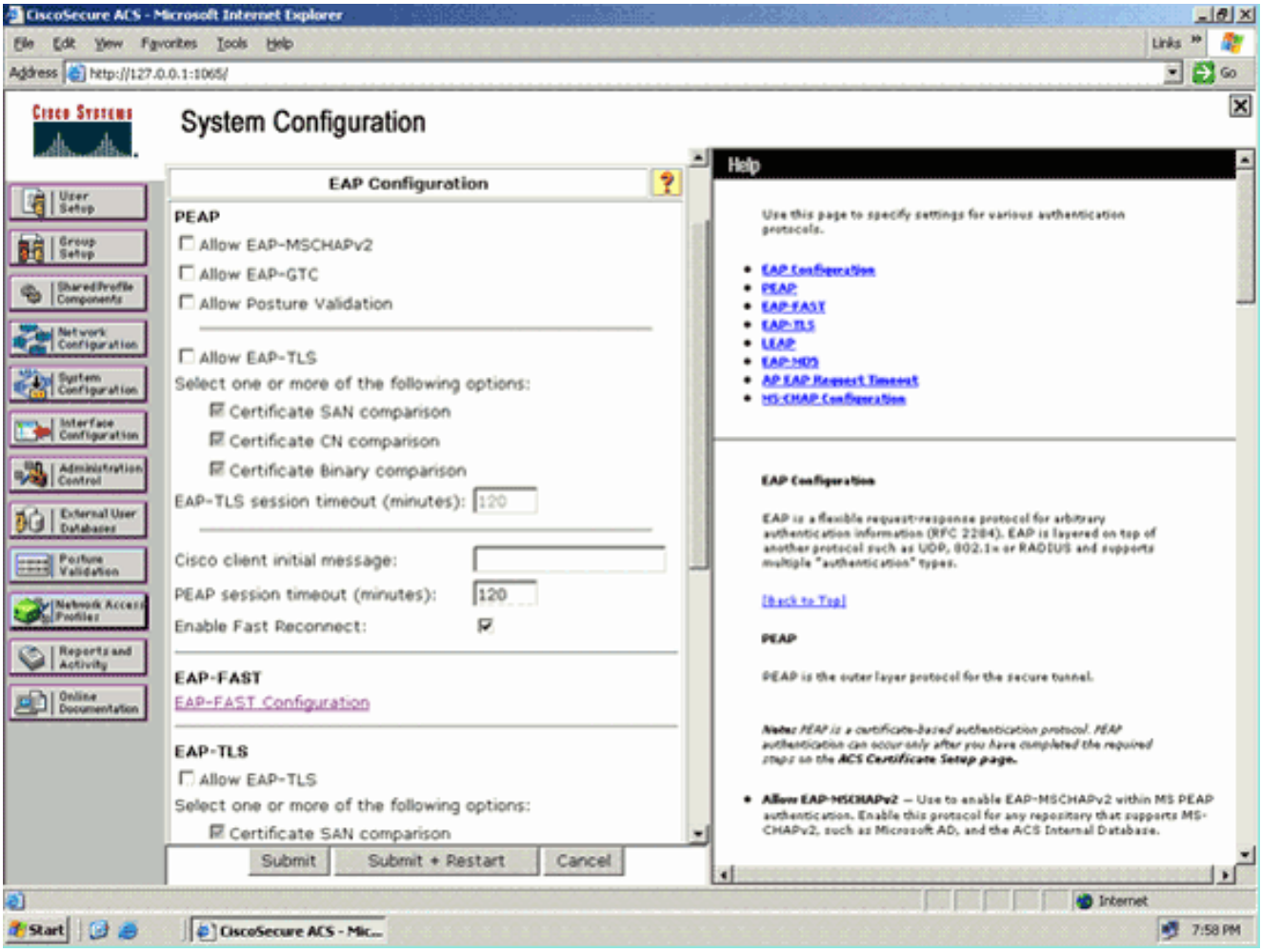
ملاحظة: يفترض هذا المستند إضافة وحدة التحكم في الشبكة المحلية اللاسلكية إلى Cisco ACS الآمن كعميل AAA.

أكمل هذه الخطوات لتكوين مصادقة EAP-FAST في خادم RADIUS:

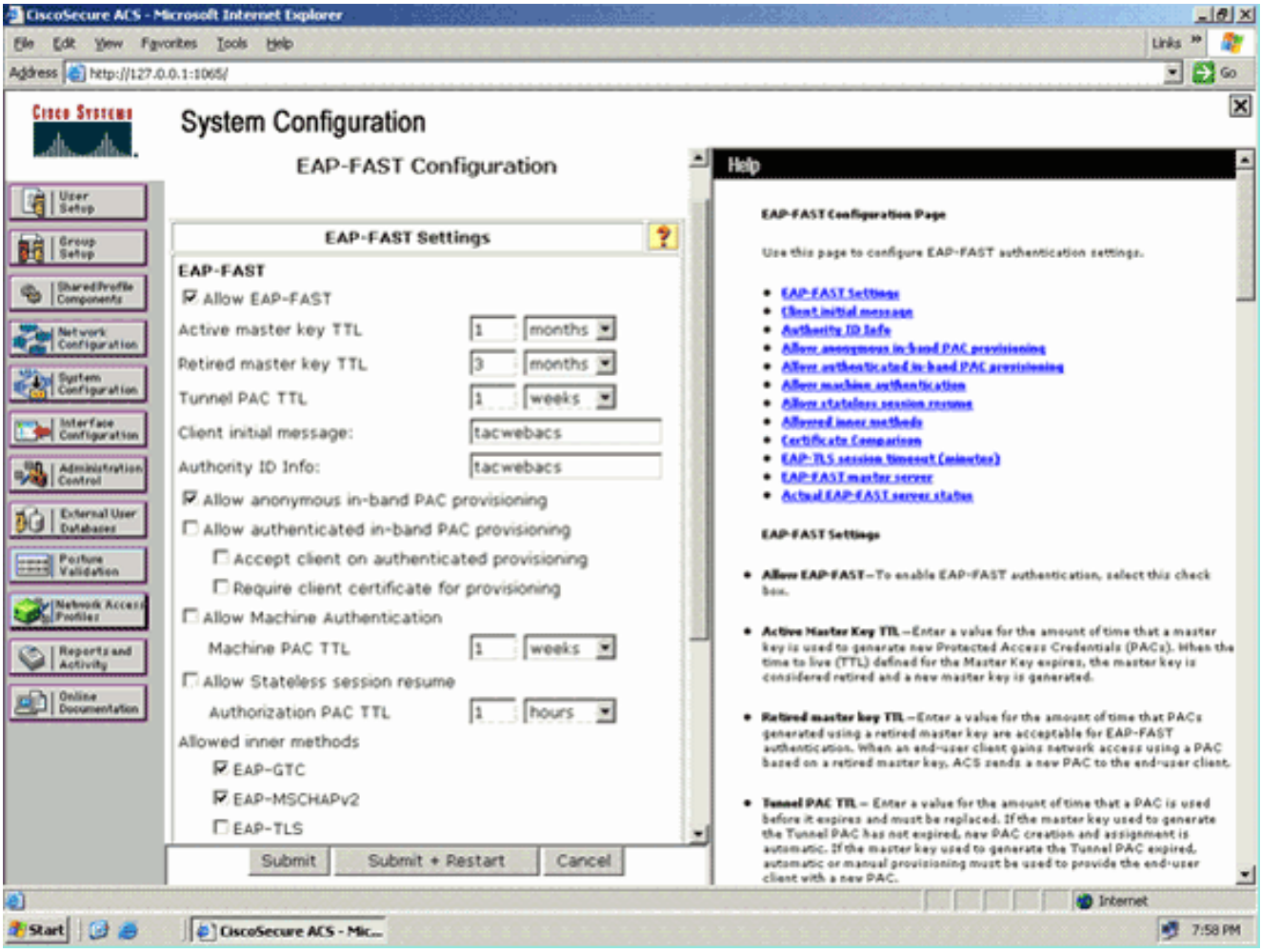
1. انقر فوق **تكوين النظام** من واجهة المستخدم الرسومية (GUI) لخادم RADIUS، ثم أختر **إعداد المصادقة العامة** من صفحة تكوين
النظام.



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



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



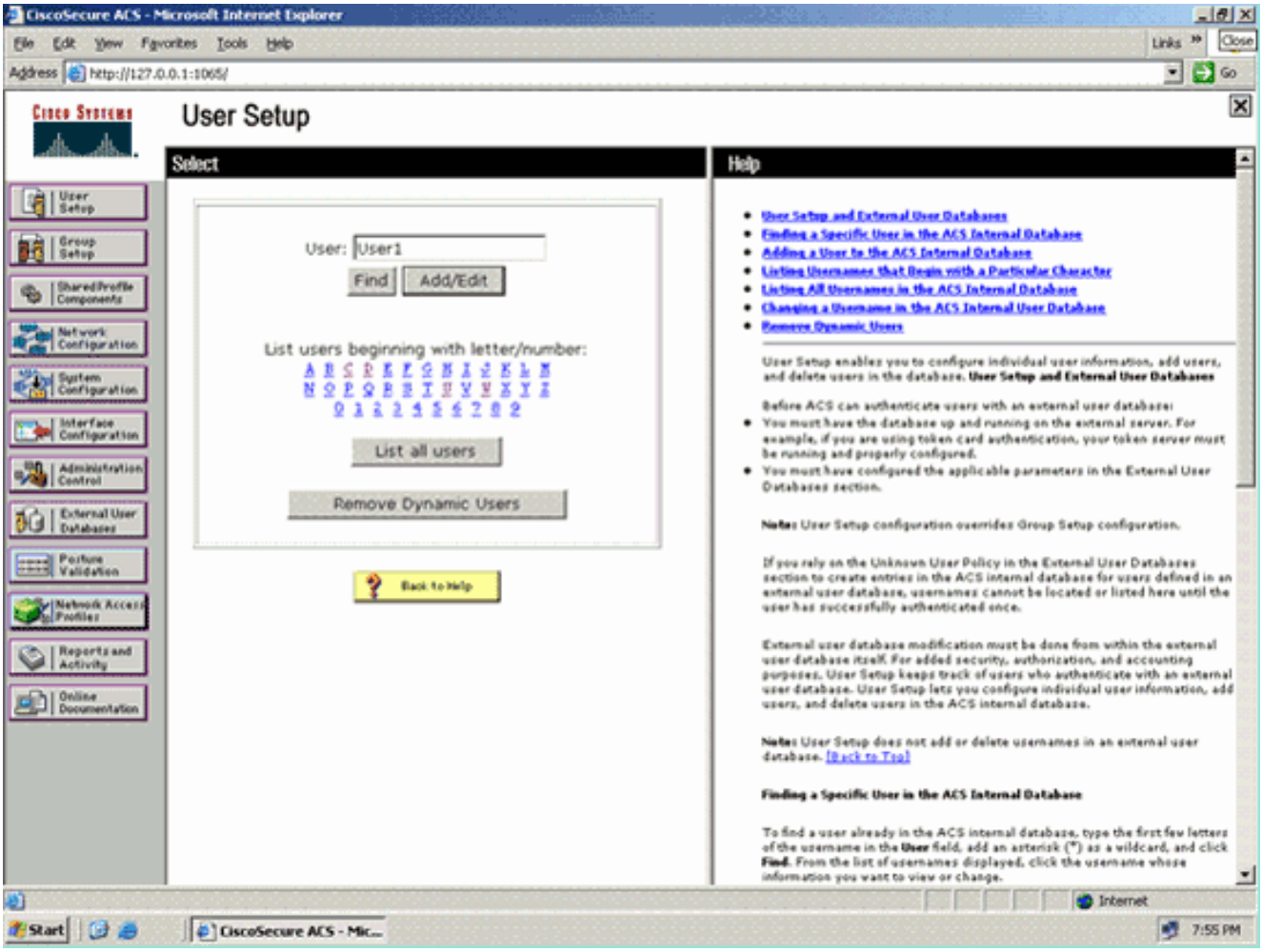
4. قم بتكوين قيم مدة البقاء (TTL) للمفتاح الرئيسي النشط/المتقاعد كما هو مطلوب، أو قم بتعيينها على القيمة الافتراضية كما هو موضح في هذا المثال.يمثل حقل معلومات معرف المرجع الهوية النصية لخادم ACS هذا، والتي يمكن للمستخدم النهائي إستخدامها لتحديد خادم ACS الذي ستتم المصادقة عليه. ملء هذا الحقل إلزامي.يحدد 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. يحدد خيار *الأساليب الداخلية المسموح بها* 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).
7. انقر على **إرسال**.**ملاحظة:** للحصول على معلومات وأمثلة مفصلة حول كيفية تكوين EAP FAST باستخدام تزويد PAC غير معروف داخل النطاق وإمداد معتمد داخل النطاق، راجع مصادقة EAP-FAST مع وحدات تحكم الشبكة المحلية اللاسلكية ومثال تكوين خادم RADIUS الخارجي.

قم بتكوين قاعدة بيانات المستخدم وحدد سمة RADIUS *لإعادة توجيه عنوان URL*

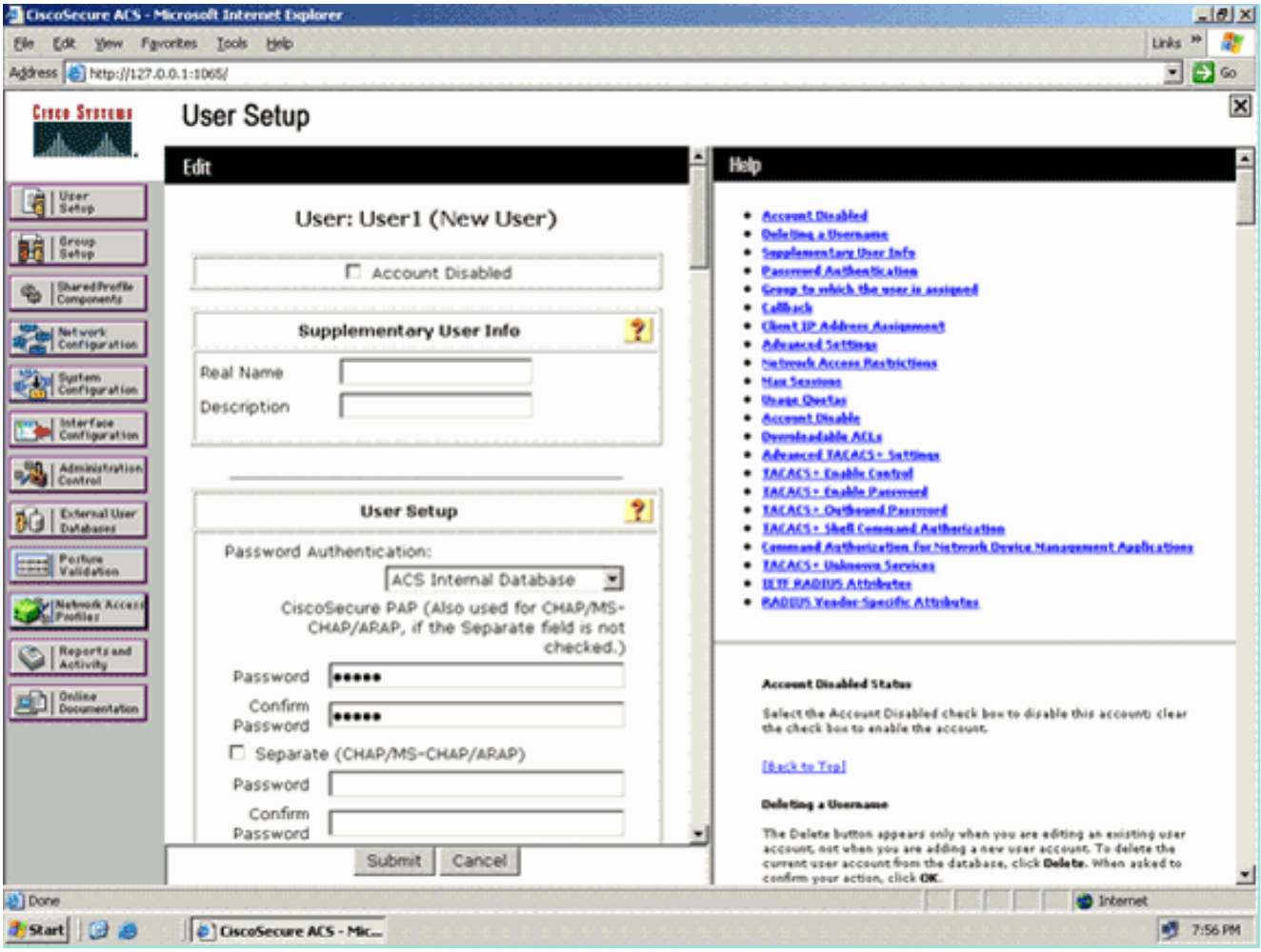
يقوم هذا المثال بتكوين اسم المستخدم وكلمة المرور للعميل اللاسلكي ك User1 و User1، على التوالي.

أتمت هذا steps in order to خلقت مستعمل قاعدة بيانات:

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



3. 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.



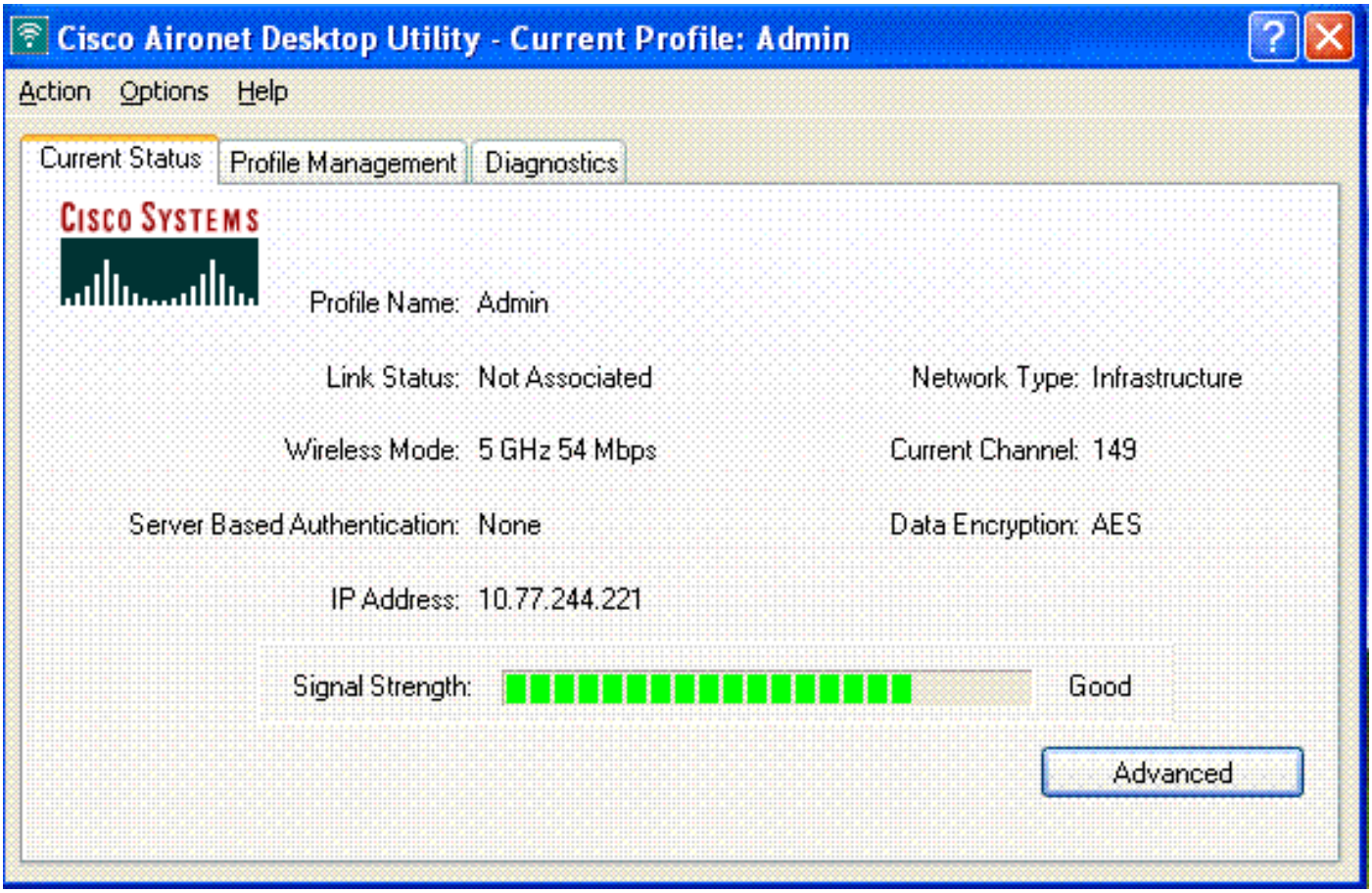
4. انزلق إلى أسفل الصفحة لتعديل خصائص RADIUS.
5. حدد خانة الاختيار **Cisco-AV-pair [001\009]**.
6. أدخل أزواج Cisco الظاهرية هذه في مربع تحرير [001\009] Cisco-av-pair لتحديد عنوان URL الذي يتم إعادة توجيه المستخدم إليه:-url-redirect=http://10.77.244.196/Admin Login.html

هذه هي الصفحة الرئيسية لمستخدمي قسم "الإدارة".
7. انقر على **إرسال**.
8. كرر هذا الإجراء لإضافة User2 (مستخدم قسم العمليات).
9. كرر الخطوات من 1 إلى 6 لإضافة المزيد من مستخدمي قسم الإدارة ومستخدمي قسم العمليات إلى قاعدة البيانات.**ملاحظة:** يمكن تكوين سمات RADIUS على مستوى المستخدم أو مستوى المجموعة على مصدر المحتوى الإضافي الآمن من Cisco.

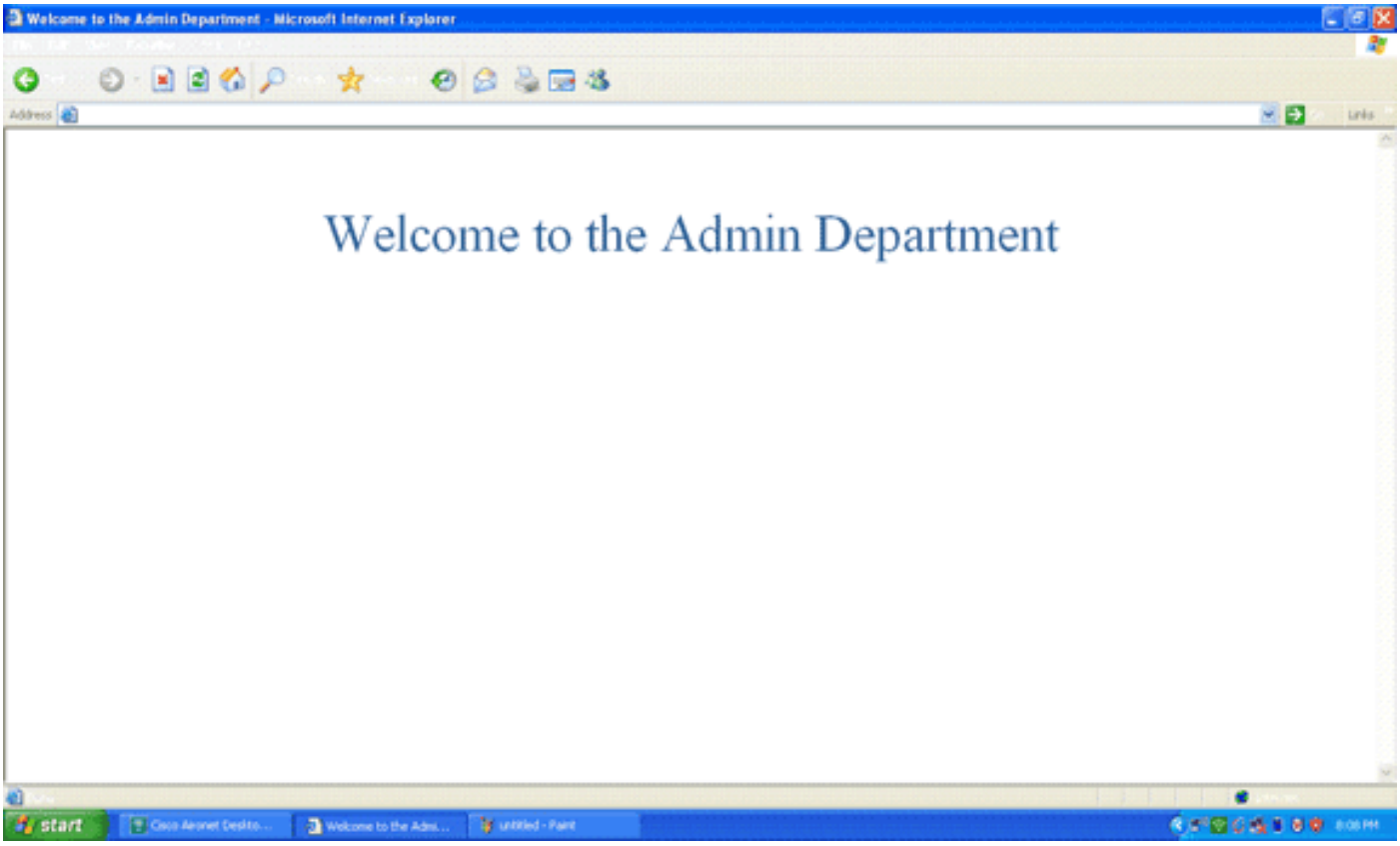
التحقق من الصحة

للتحقق من التكوين، قم بإقران عميل شبكات WLAN من قسم "الإدارة" وقسم "العمليات" بشبكات WLAN المناسبة الخاصة بهم.

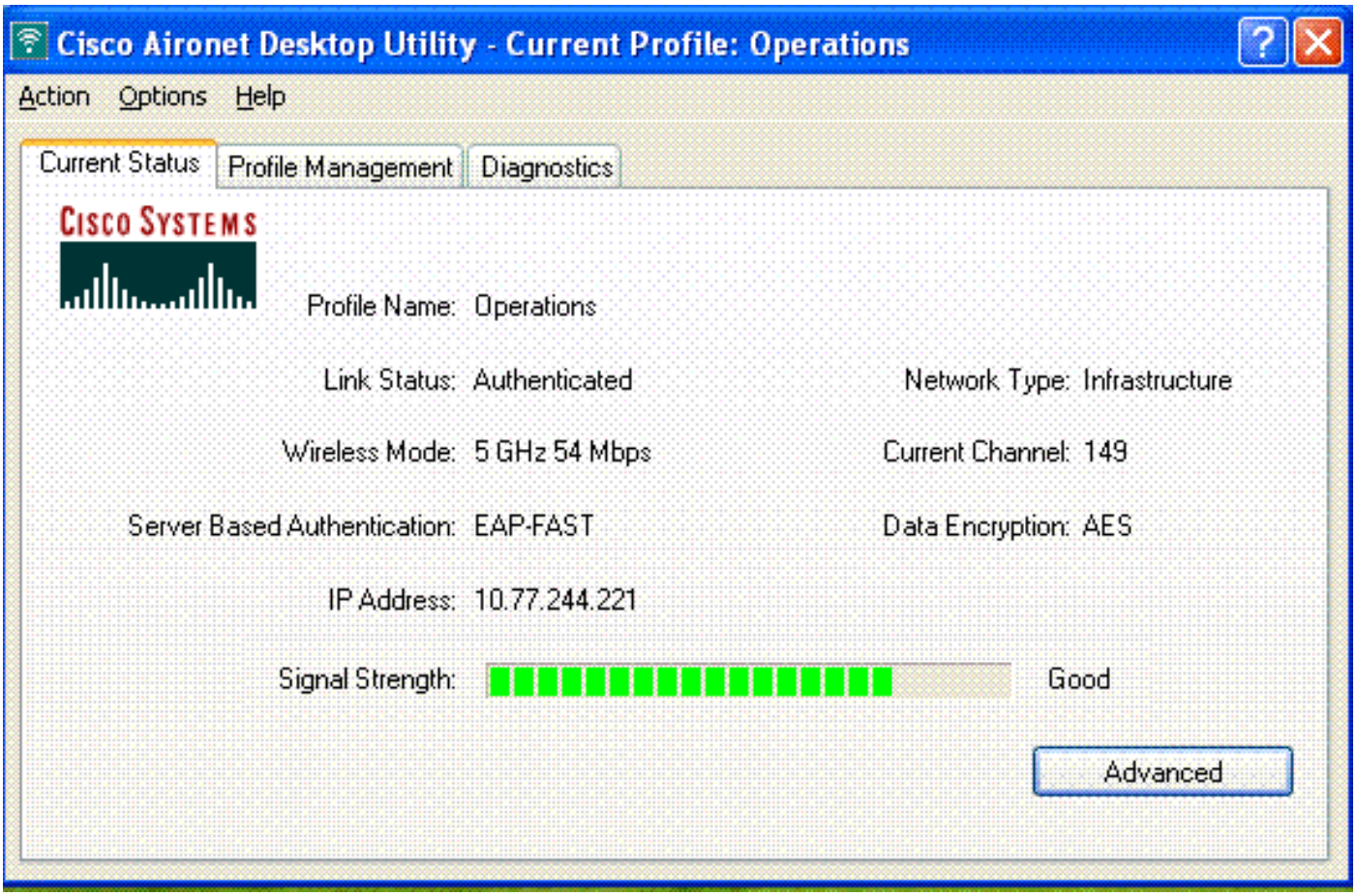
عندما يتصل مستخدم من قسم الإدارة بمسؤول الشبكة المحلية اللاسلكية، يوعز للمستخدم بإدخال بيانات اعتماد 802.1x (بيانات اعتماد EAP-FAST في حالتنا). بمجرد أن يوفر المستخدم بيانات الاعتماد، يقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بتمرير بيانات الاعتماد هذه إلى خادم ACS الآمن من Cisco. يتحقق خادم Cisco Secure ACS من مسوغات المستخدم مقابل قاعدة البيانات، وعند نجاح المصادقة، يرجع سمة url-redirect إلى وحدة التحكم في الشبكة المحلية اللاسلكية. تكتمل المصادقة في هذه المرحلة.

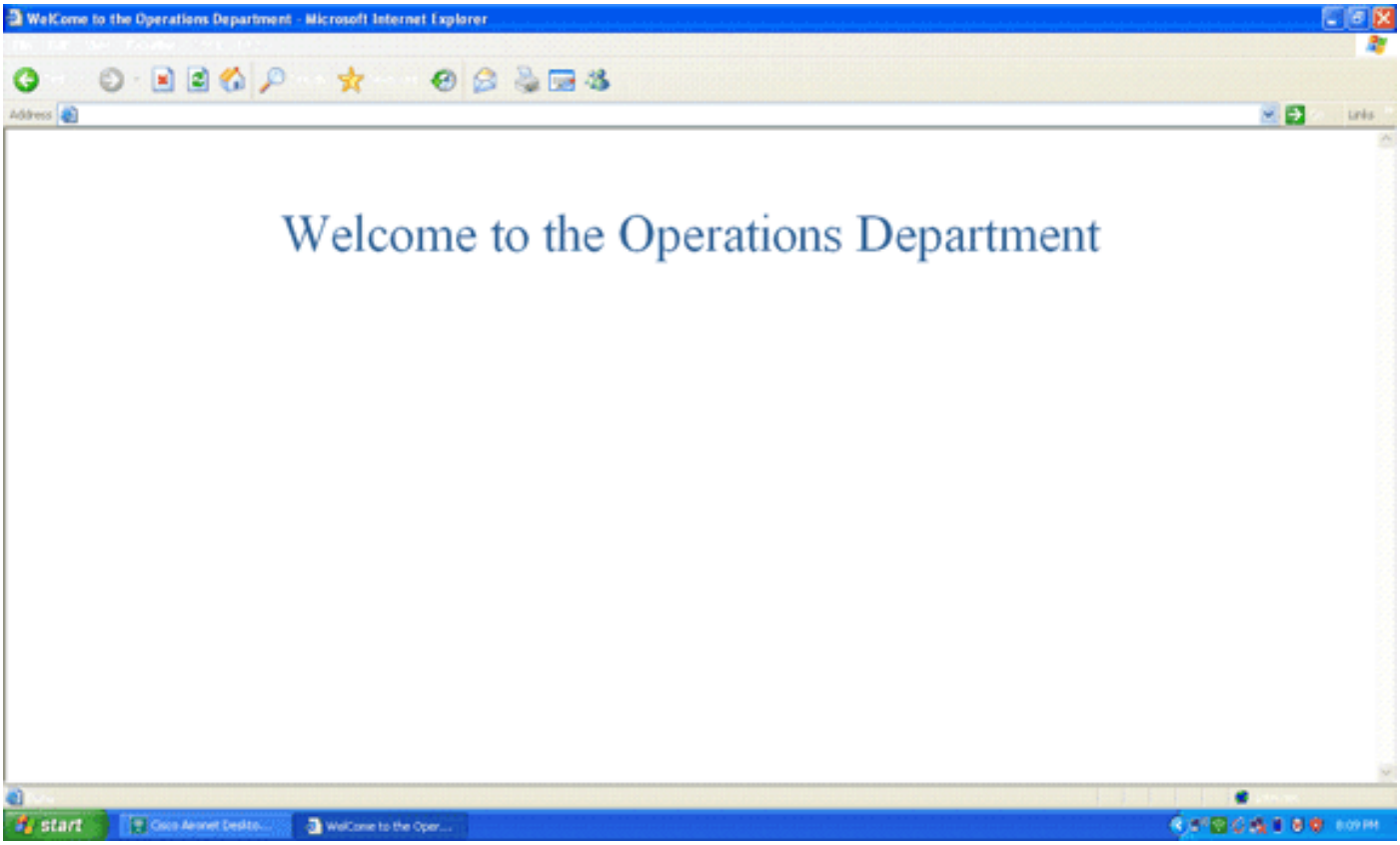


عندما يقوم المستخدم بفتح مستعرض ويب، تتم إعادة توجيه المستخدم إلى عنوان URL الخاص بالصفحة الرئيسية لقسم "الإدارة". (يتم إرجاع عنوان URL هذا إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من خلال سمة زوج-الصوت من Cisco). بعد إعادة التوجيه، يتمتع المستخدم بحق الوصول الكامل إلى الشبكة. هنا اللقطات:



يحدث نفس تسلسلات الأحداث عندما يتصل مستخدم من قسم العمليات بعمليات شبكة WLAN.





استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

يمكنك إستخدام الأوامر التالية لاستكشاف أخطاء التكوين وإصلاحها.

- **show wlan wlan_id**— يعرض حالة ميزات إعادة توجيه الويب لشبكة WLAN معينة.فيما يلي مثال:

```
WLAN Identifier.................................. 1
Profile Name..................................... Admin
Network Name (SSID).............................. Admin
                                                  ...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
```

- **debug dot1x events enable**—يمكن ال debug من 802.1x ربط رسالة.فيما يلي مثال:

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
                                    (mobile 00:40:96:ac:dd:05 (EAP Id 16
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
                                    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
                                (mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for
                                    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
                                        .seconds, got from WLAN config
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
                                        setting dot1x reauth timeout = 1800
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
                                    (for station 00:40:96:ac:dd:05 (RSN 2
```

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
                                to PMKID cache for station 00:40:96:ac:dd:05
                                       (Fri Feb 29 10:27:16 2008: New PMKID: (16
 Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
                                                                 fb fa 8e 3c
   Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
                                                 .lifetime can take care of same
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
                                                      (ac:dd:05 (EAP Id 17:00:40:96
                                (Fri Feb 29 10:27:16 2008: Including PMKID in M1  (16
 Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
                                                                 fb fa 8e 3c
  Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
                                                          mobile 00:40:96:ac:dd:05
    state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
  Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
                                 in Authenticating state for mobile 00:40:96:ac:dd:05
```

- debug aaa events enable— يمكن إخراج تصحيح الأخطاء لجميع أحداث AAA.فيما يلي مثال:

```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
                           Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
                                                                ac:dd:05-00:00:00:40:96
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
  Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
   RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
      Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
                           Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
                                                                ac:dd:05-00:00:00:40:96
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
    Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
   RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
      Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
                                  http://10.77.244.196/Admin-login.html' set'
  Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
                                                       station 00:40:96:ac:dd:05
    Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
                                                                ac:dd:05:00:40:96
                                                source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
                dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                ' :vlanIfName: '', aclName
```

معلومات ذات صلة

- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية، الإصدار 5.0 من Cisco
- مثال تكوين مصادقة الويب لوحدة تحكم الشبكة المحلية (LAN) اللاسلكية
- مثال تكوين المصادقة الخارجية للويب مع وحدات تحكم الشبكة المحلية (LAN) اللاسلكية
- 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).