مصادقة ويب خارجية باستخدام خادم RADIUS

المحتويات

المقدمة

يشرح هذا المستند كيفية إجراء مصادقة ويب خارجية باستخدام خادم RADIUS خارجي.

المتطلبات الأساسية

المتطلبات

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

- معرفة أساسية بتكوين نقاط الوصول في الوضع Lightweight (LAPs) و Cisco WLCs
- معرفة كيفية إعداد خادم ويب الخارجي وتكوينه
- معرفة كيفية تكوين ACS الآمن من Cisco

المكونات المستخدمة

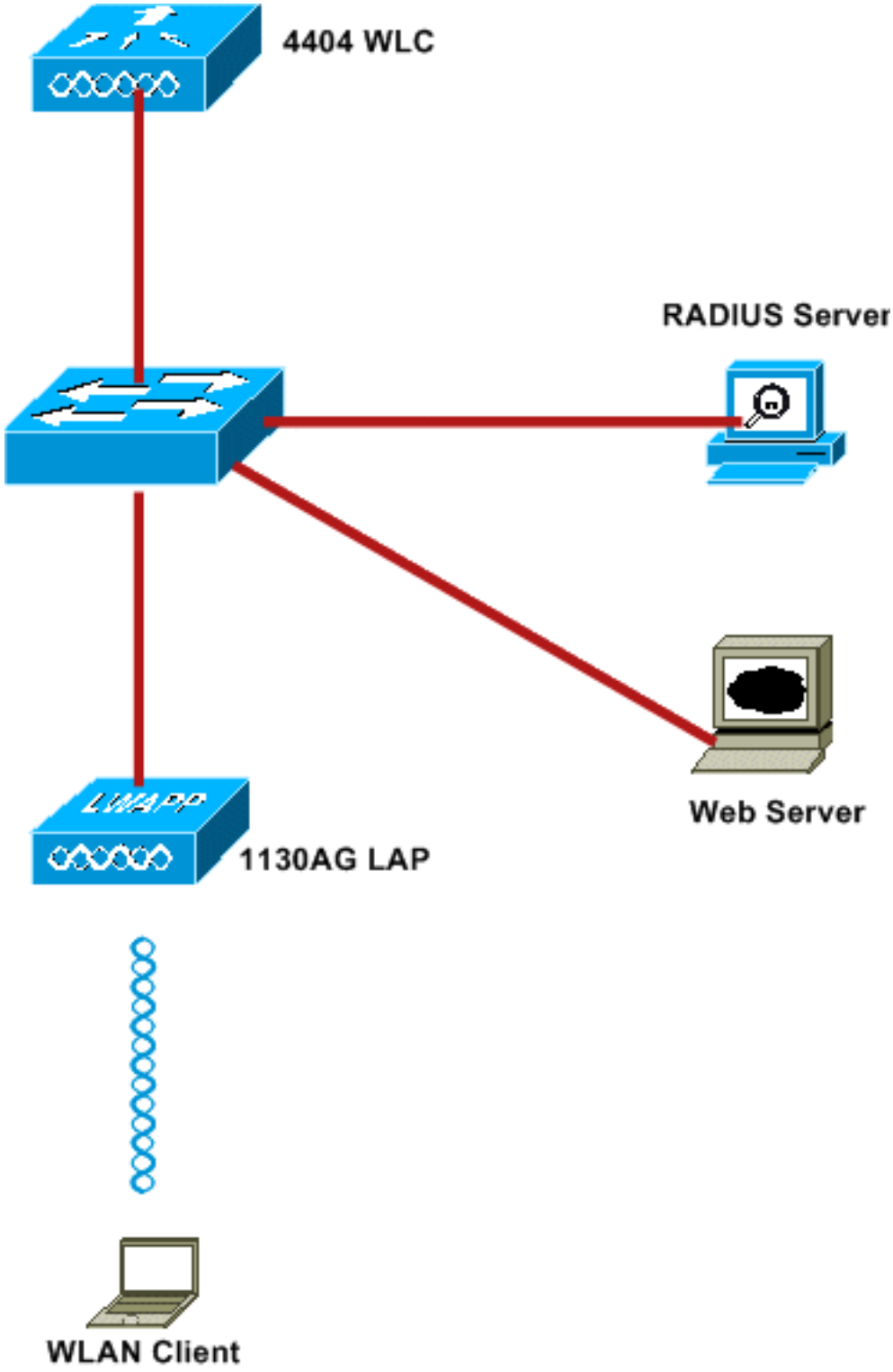
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة التحكم في شبكة LAN اللاسلكية التي تشغل الإصدار 5.0.148.0 من البرنامج الثابت
- نقطة الوصول في الوضع Lightweight من السلسلة Cisco 1232 Series LAP
- مهايئ العميل اللاسلكي 3.6.0.61 802.11a/b/g من Cisco
- خادم ويب الخارجي الذي يستضيف صفحة تسجيل الدخول لمصادقة الويب
- Cisco Secure ACS الإصدار 4.1.1.24 من البرنامج الثابت

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.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



هذه هي عناوين IP المستخدمة في هذا المستند:

- يستخدم WLC عنوان IP 10.77.244.206
- LAP مسجل إلى WLC مع عنوان IP 10.77.244.199
- يستخدم خادم الويب عنوان IP 10.77.244.210
- يستخدم خادم Cisco ACS عنوان IP 10.77.244.196
- يستلم العميل عنوان IP من واجهة الإدارة التي تم تعيينها على الشبكة المحلية اللاسلكية (WLAN) - 10.77.244.208

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

مصادقة الويب الخارجية

مصادقة الويب هي آلية مصادقة من الطبقة 3 تستخدم لمصادقة المستخدمين الضيوف للوصول إلى الإنترنت. لن يتمكن المستخدمون الذين تمت مصادقتهم باستخدام هذه العملية من الوصول إلى الإنترنت حتى يستكملوا عملية المصادقة بنجاح. للحصول على معلومات كاملة حول عملية مصادقة الويب الخارجية، اقرأ القسم عملية مصادقة الويب الخارجية الخاصة بالمستند مصادقة الويب الخارجية مع مثال تكوين وحدات تحكم الشبكة المحلية اللاسلكية.

في هذا المستند، ننظر إلى مثال تكوين، يتم فيه إجراء مصادقة الويب الخارجية باستخدام خادم RADIUS خارجي.

تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

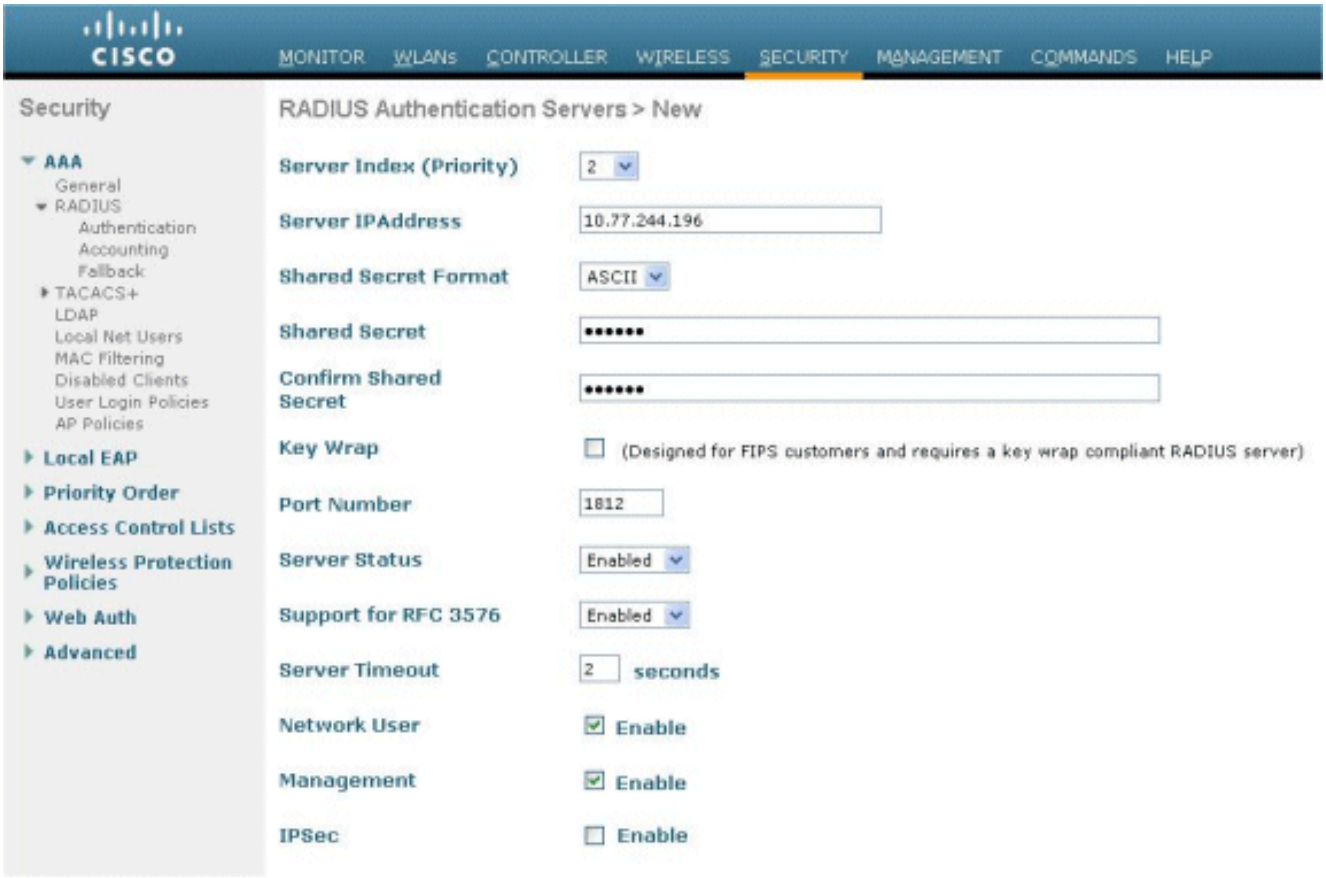
في هذا المستند، نفترض أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تم تكوينه بالفعل ولديه نقطة وصول (LAP) مسجلة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يفترض هذا المستند كذلك أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تم تكوينه للتشغيل الأساسي وأن نقاط الوصول في الوضع Lightweight تم تسجيلها إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). إذا كنت مستخدما جديدا يحاول إعداد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للعملية الأساسية باستخدام نقاط الوصول في الوضع Lightweight (LAP)، فارجع إلى تسجيل نقطة الوصول في الوضع Lightweight (LAP) إلى وحدة تحكم شبكة محلية لاسلكية (WLC). لعرض نقاط الوصول في الوضع Lightweight (LAPs) المسجلة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى **لاسلكي > جميع نقاط الوصول (APs)**.

بمجرد تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للتشغيل الأساسي وتزويده بنقطة وصول واحدة أو أكثر مسجلة إليه، يمكنك تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة الويب الخارجية باستخدام خادم ويب خارجي. في مثالنا، نستخدم إصدار Cisco ACS الآمن 4.1.1.24 كخادم RADIUS. أولا، سنقوم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لخادم RADIUS هذا، ومن ثم سنبحث عن التكوين المطلوب على مصدر المحتوى الإضافي الآمن من Cisco لهذا الإعداد.

تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لـ Cisco Secure ACS

أنجزت هذا steps in order to أضفت ال RADIUS نادل على ال WLC:

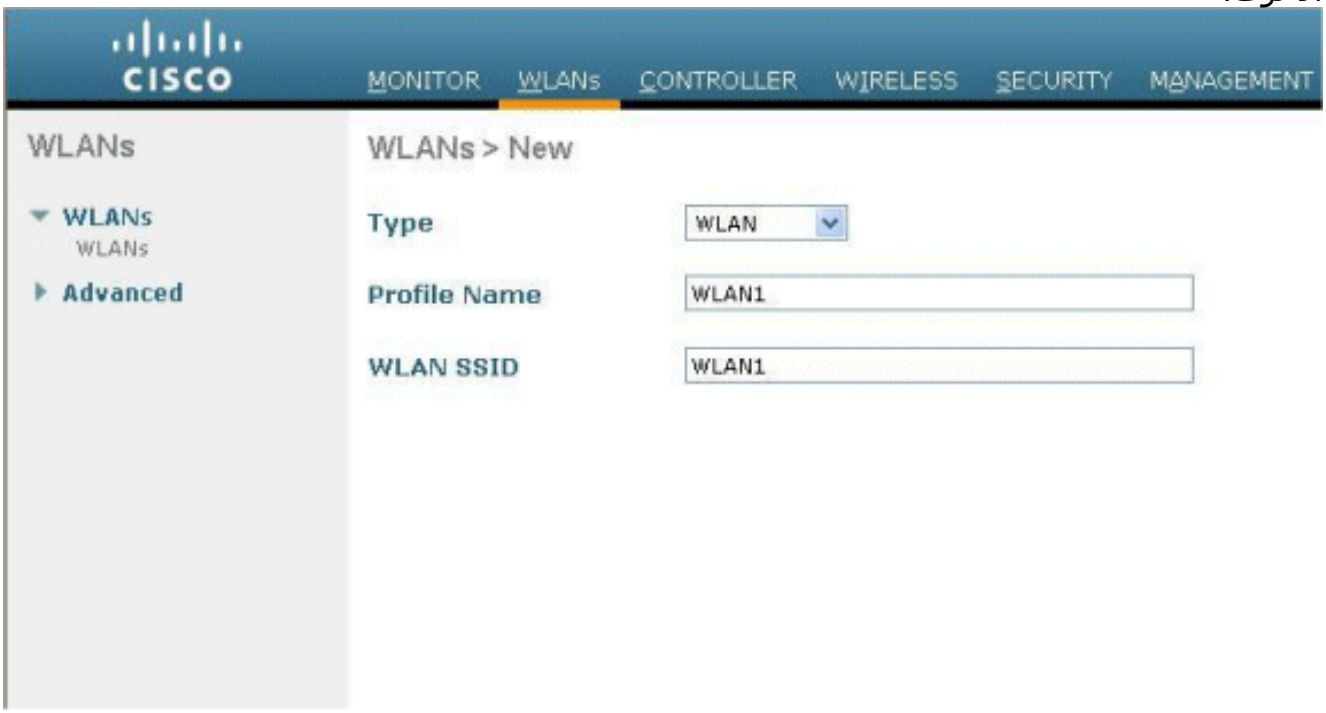
1. من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق قائمة **الأمان**.
2. تحت قائمة **AAA**، انتقل إلى القائمة الفرعية **RADIUS > المصادقة**.
3. انقر فوق **جديد**، وأدخل عنوان IP الخاص بخادم RADIUS. في هذا المثال، عنوان IP الخاص بالخادم هو *10.77.244.196*.
4. دخلت ال يشارك سر في ال WLC. يجب تكوين "السر المشترك" نفسه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
5. أختر إما **ASCII** أو **hex** لتنسيق سري مشترك. يجب إختيار نفس التنسيق على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
6. **1812** هو رقم المنفذ المستخدم لمصادقة RADIUS.
7. تأكد من تعيين خيار حالة الخادم إلى **ممكن**.
8. حدد مربع **تمكين** مستخدم الشبكة لمصادقة مستخدمي الشبكة.
9. طقطقة
يطبق.



تكوين شبكة WLAN على WLC لمصادقة الويب

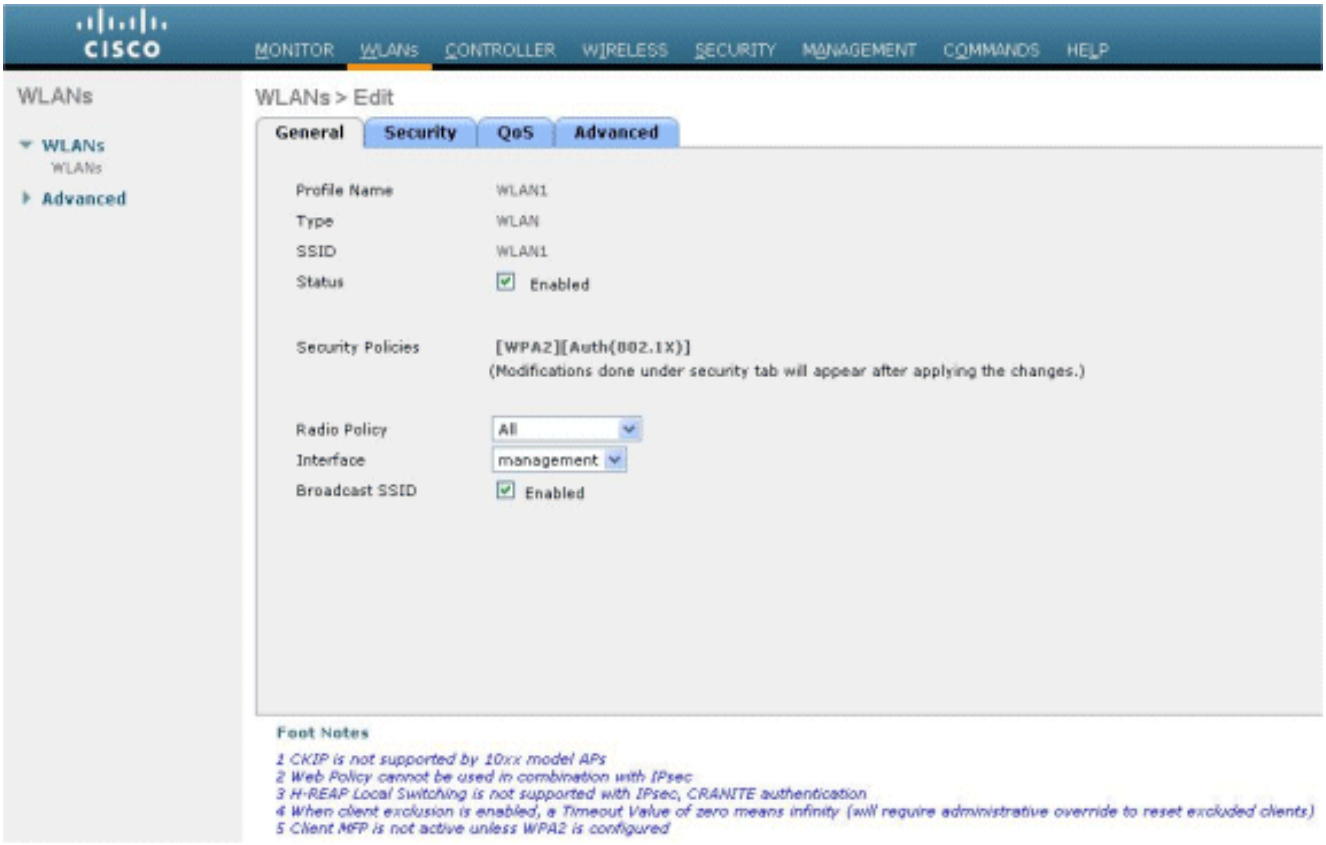
تتمثل الخطوة التالية في تكوين شبكة WLAN لمصادقة الويب على WLC. أنجزت هذا steps in order to شكلت ال WLAN على WLC:

1. انقر فوق قائمة **شبكات WLAN** من واجهة المستخدم الرسومية (GUI) لوحدة التحكم، واختر **جديد**.
2. أختر **WLAN** للنوع.
3. أدخل اسم توصيف ومعرف WLAN SSID من إختيارك، وانقر **تطبيق**.**ملاحظة:** WLAN SSID حساس لحالة الأحرف.

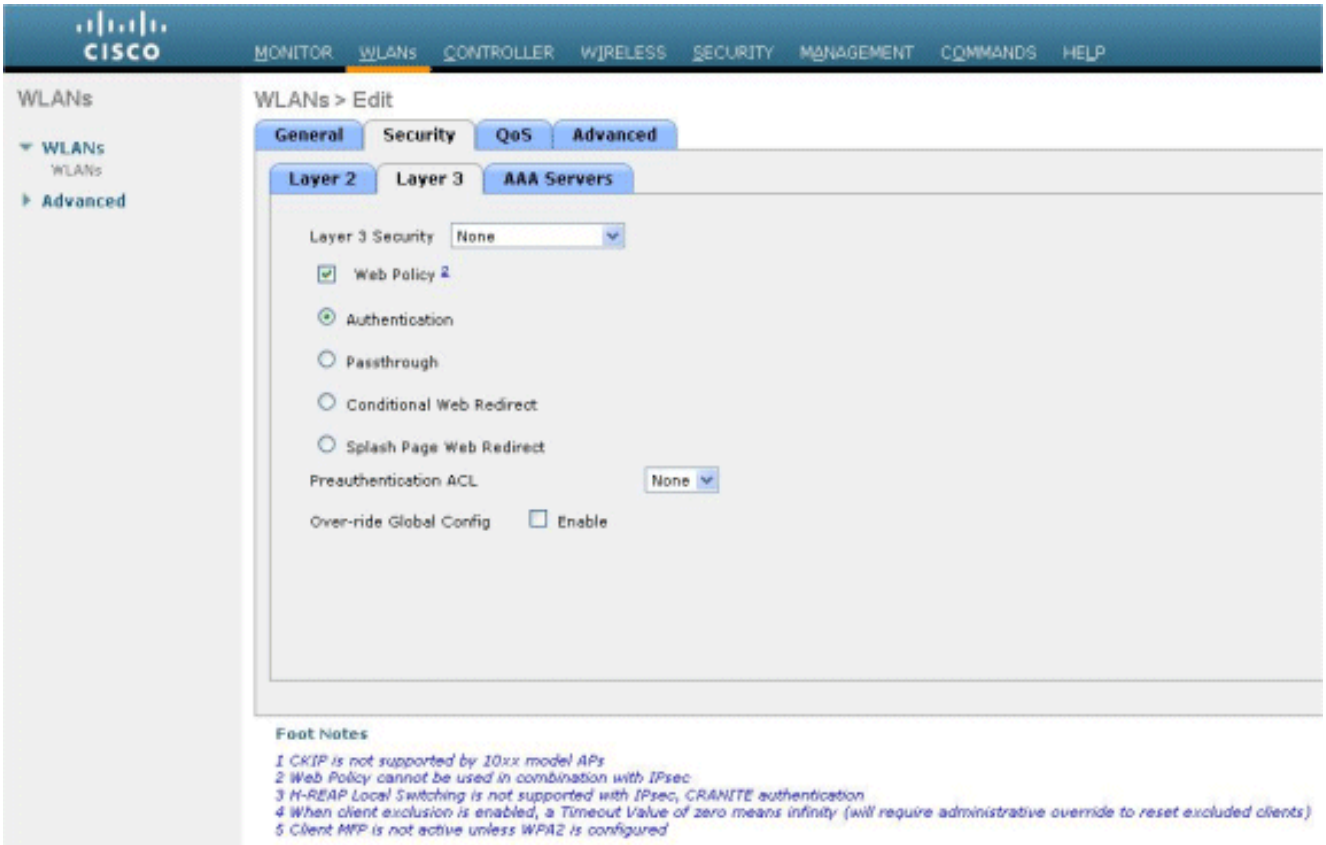


4. تحت علامة التبويب **عام**، تأكد من أن خيار **تمكين** محدد لكل من الحالة و Broadcast SSID.**تكوين شبكة**

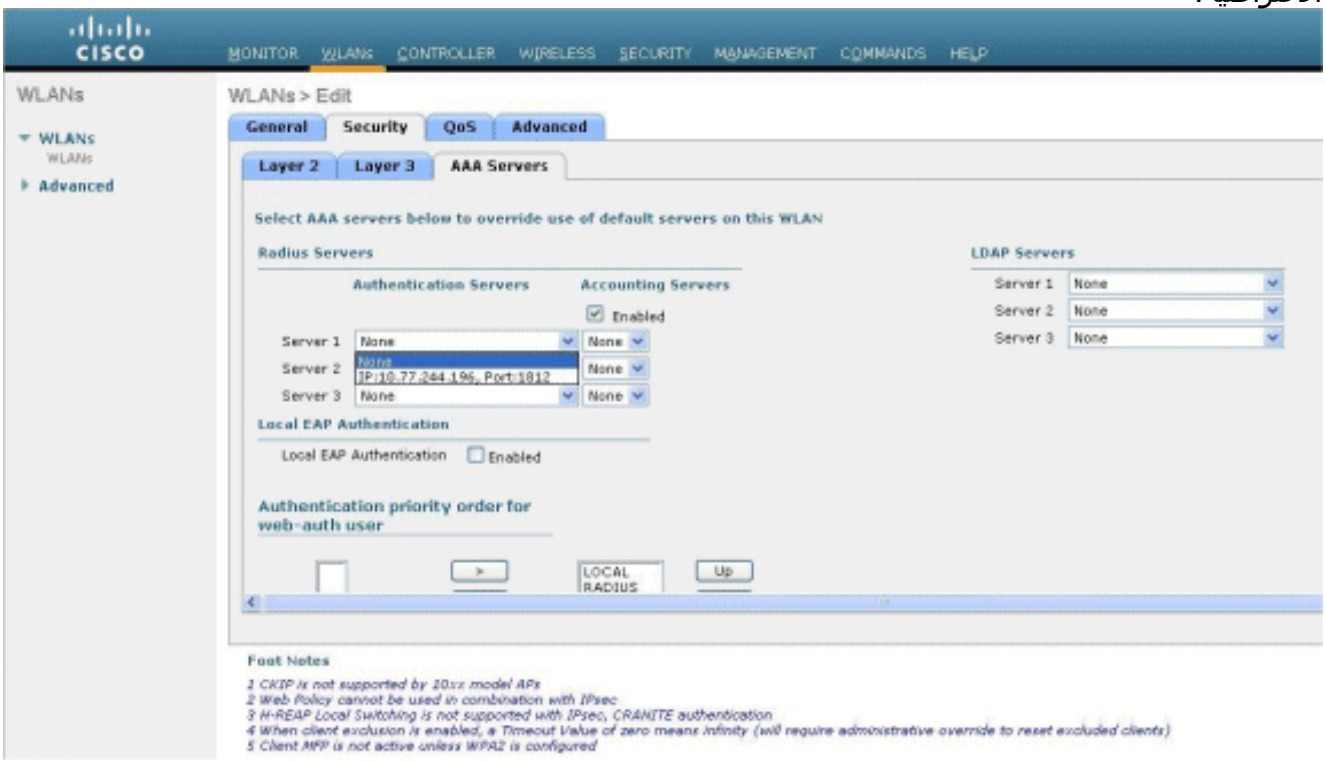
WLAN



5. أخترت قارن ل ال WLAN. بشكل خاص، يتم تعيين واجهة تم تكوينها في شبكة VLAN فريدة على الشبكة المحلية اللاسلكية (WLAN) حتى يستلم العميل عنوان IP في شبكة VLAN هذه. في هذا المثال، نستخدم *الإدارة* للواجهة.
6. أختر علامة التبويب **أمان**.
7. تحت قائمة **الطبقة 2**، أختر **لا شيء** لأمان الطبقة 2.
8. تحت قائمة **الطبقة 3**، أختر **لا شيء** لأمان الطبقة 3. حدد خانة الاختيار **نهج الويب**، واختر **المصادقة**.



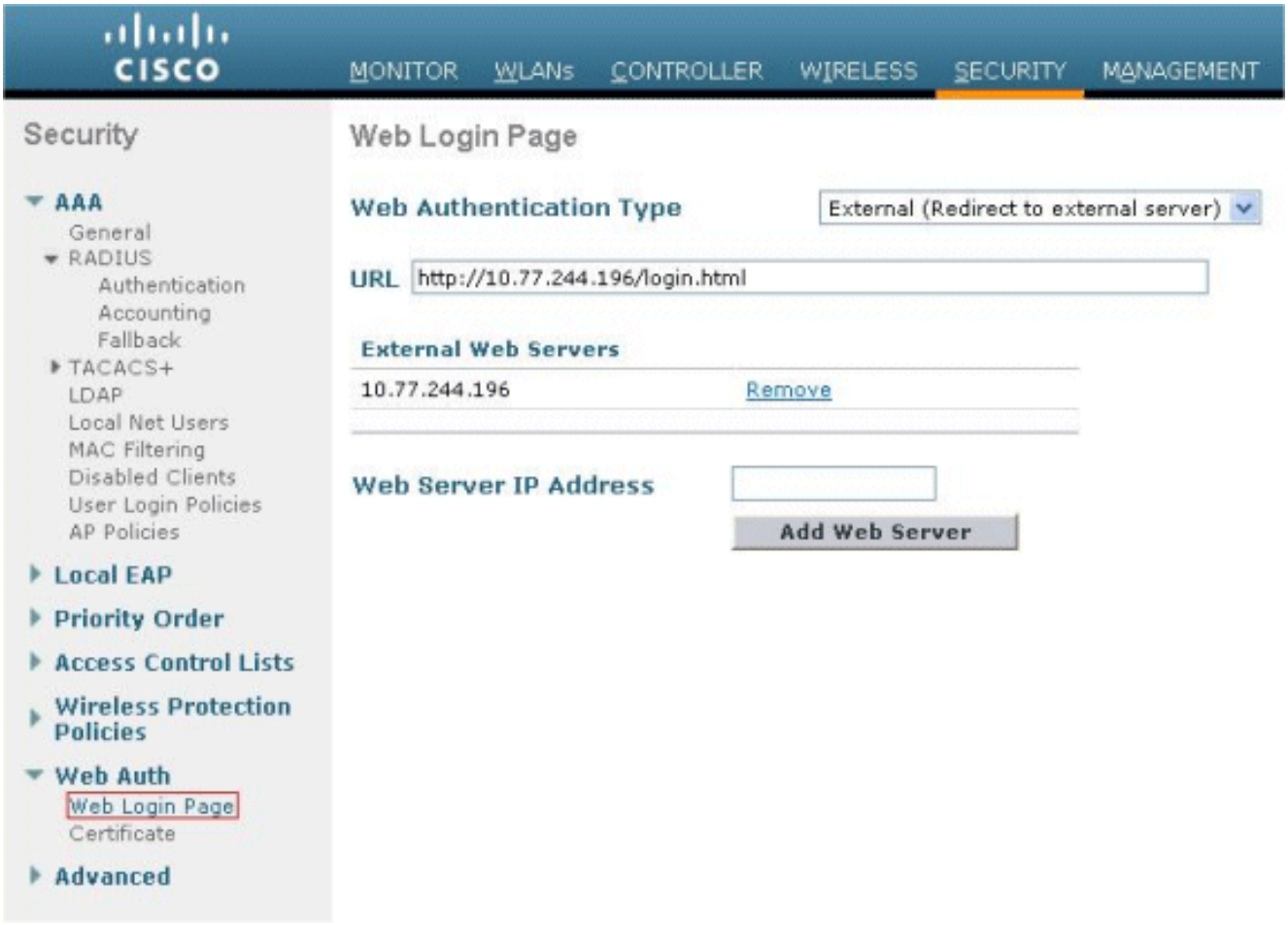
9. تحت قائمة **خوادم AAA**، لخادم المصادقة، أختر خادم RADIUS الذي تم تكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) هذا. يجب أن تظل القوائم الأخرى بالقيم الافتراضية.



تكوين معلومات خادم الويب على WLC

يجب تكوين خادم ويب الذي يستضيف صفحة مصادقة الويب على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). قم بإجراء هذه الخطوات لتكوين خادم الويب:

1. انقر فوق علامة التبويب **أمان**. انتقل إلى **مصادقة الويب > صفحة تسجيل الدخول إلى الويب**.
2. تعيين نوع مصادقة الويب على أنه **خارجي**.
3. في حقل عنوان IP لخادم الويب، أدخل عنوان IP الخاص بالخادم الذي يستضيف صفحة مصادقة الويب، وانقر فوق **إضافة خادم ويب**. في هذا المثال، عنوان IP هو *10.77.244.196*، والذي يظهر تحت خوادم الويب الخارجية.
4. أدخل عنوان URL لصفحة مصادقة الويب (في هذا المثال، *http://10.77.244.196/login.html*) في حقل عنوان URL.



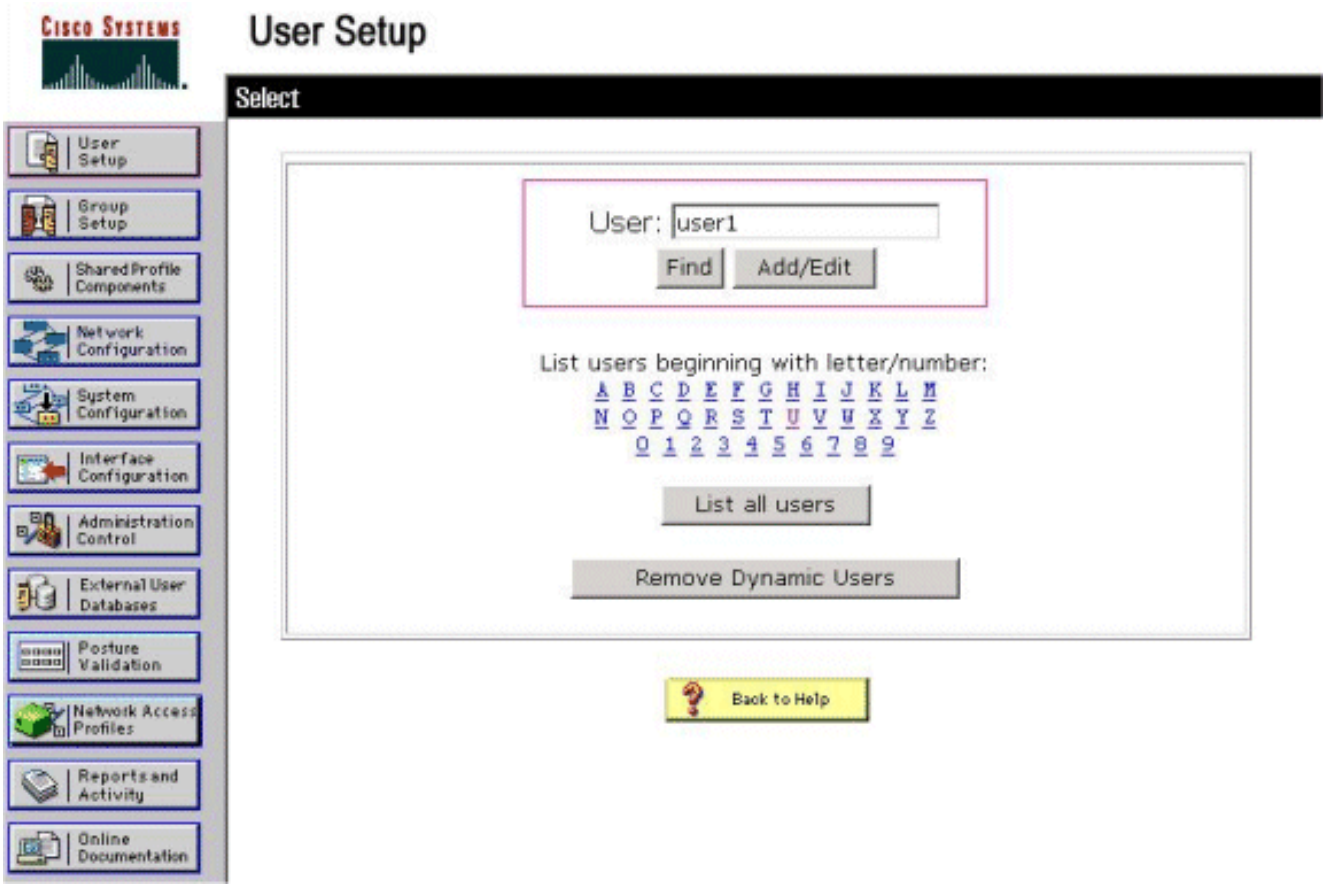
تكوين مصدر المحتوى الإضافي الآمن من Cisco

في هذا المستند نفترض أن خادم ACS الآمن من Cisco مثبت بالفعل وأنه قيد التشغيل على جهاز. للحصول على مزيد من المعلومات حول كيفية إعداد Cisco Secure ACS، ارجع إلى دليل التكوين ل Cisco Secure ACS 4.2.

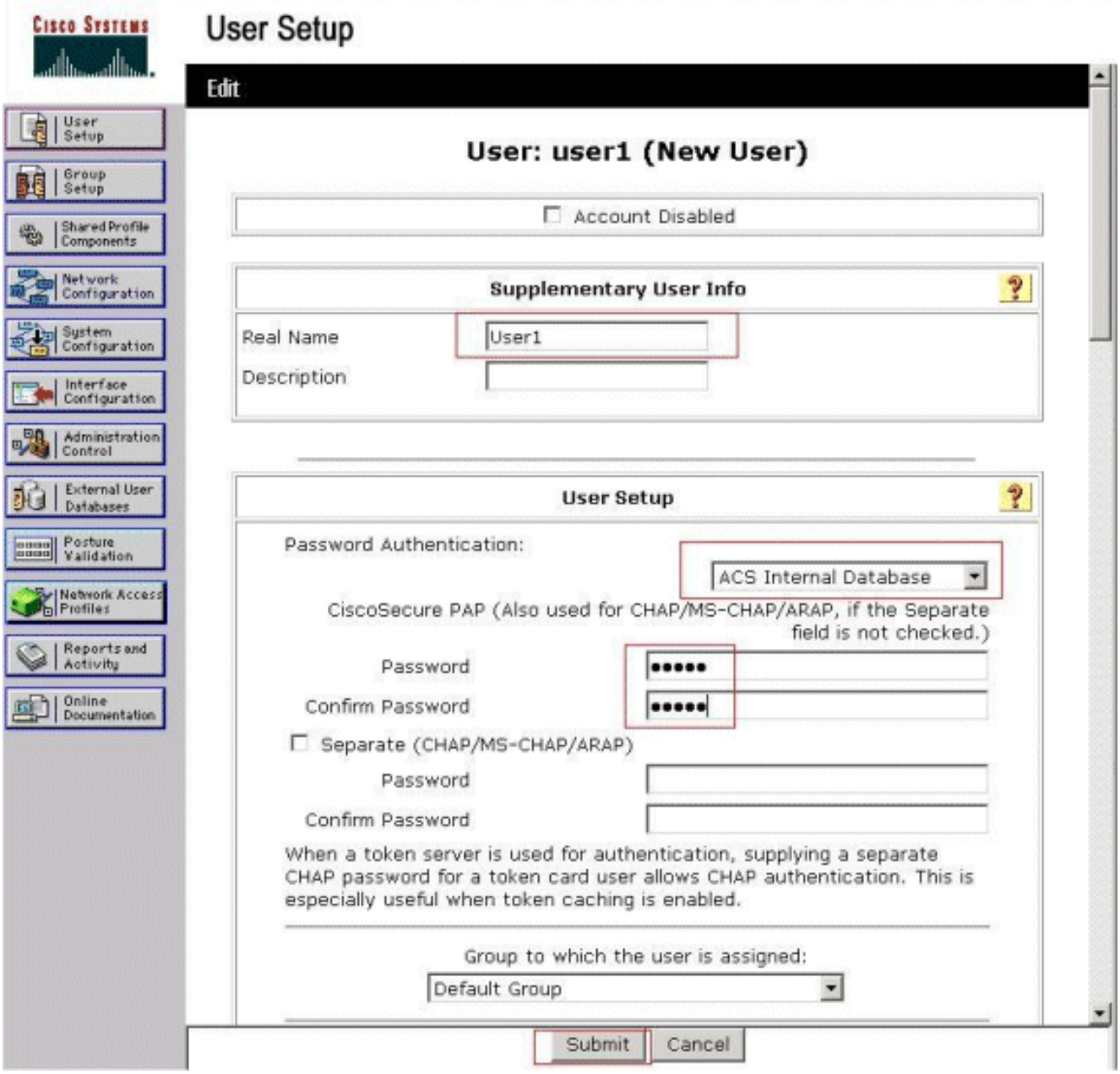
تكوين معلومات المستخدم على ACS الآمن من Cisco

أنجزت هذا steps in order to شكلت مستعمل على ال cisco يأمن ACS:

1. أخترت **مستعمل setup** من ال cisco يأمن ACS gui، دخلت username، وطقطقة **يضيف/يحرر**. في هذا المثال، المستخدم هو *user1*.



2. بشكل افتراضي، يتم إستخدام PAP لمصادقة العملاء. يتم إدخال كلمة المرور الخاصة بالمستخدم ضمن **إعداد المستخدم > مصادقة كلمة المرور > Cisco PAP الآمن**. تأكد من إختيار **قاعدة بيانات ACS الداخلية** لمصادقة كلمة
المرور.



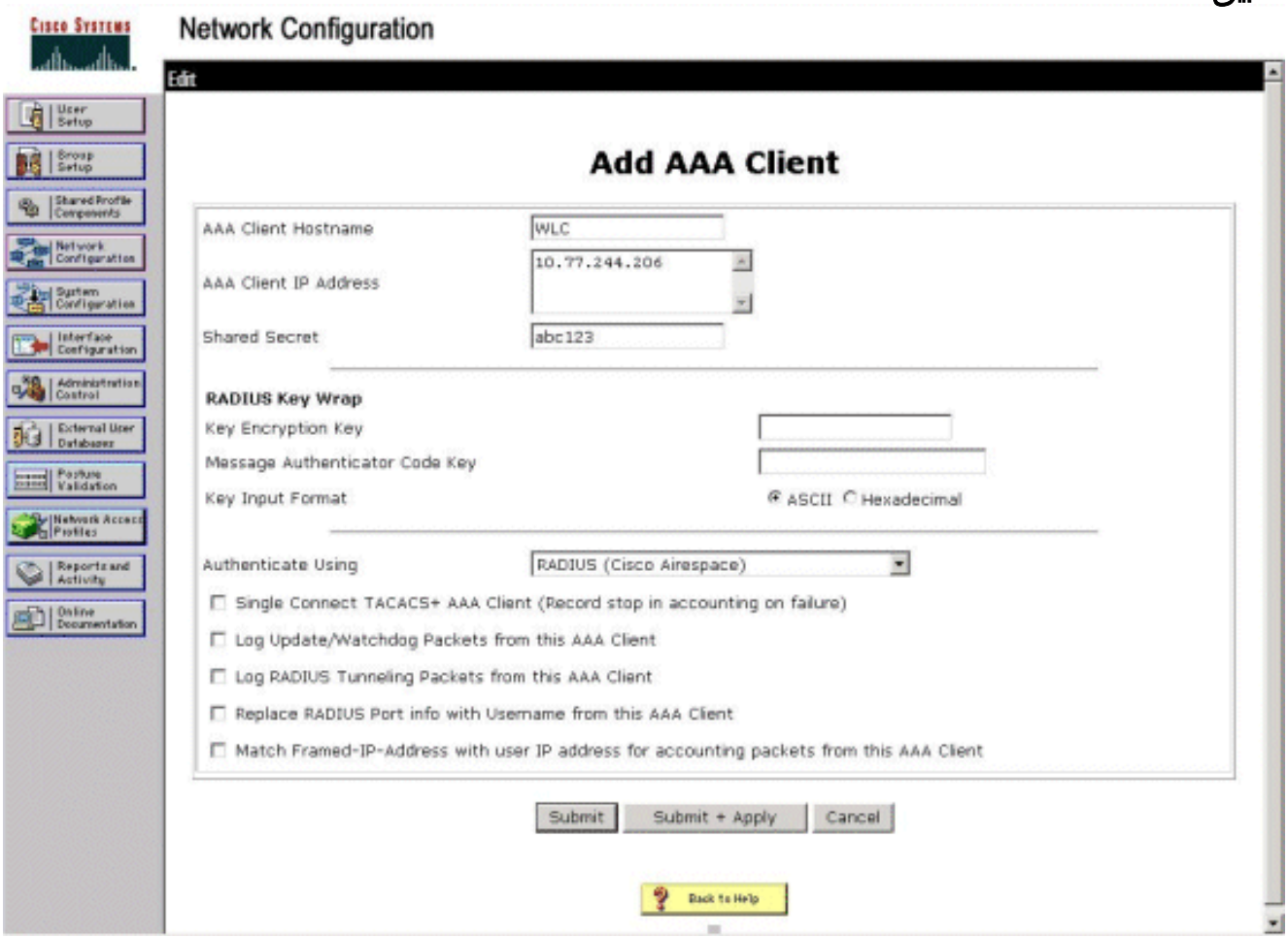
3. يجب تعيين مجموعة إلى المستخدم ينتمي إليها المستخدم. أختر **المجموعة الافتراضية**.
4. انقر على **إرسال**.

تكوين معلومات WLC على ACS الآمن من Cisco

أنجزت هذا steps in order to شكلت WLC معلومة على cisco يأمن ACS:

1. في واجهة المستخدم الرسومية (ACS)، انقر فوق علامة التبويب **تكوين الشبكة**، وانقر فوق **إضافة إدخال**.
2. تظهر الشاشة إضافة عميل AAA.
3. أدخل اسم العميل. في هذا المثال، نستخدم عنصر التحكم في الشبكة المحلية اللاسلكية (*WLC*).
4. أدخل عنوان IP الخاص بالعميل. عنوان IP الخاص بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) هو *10.77.244.206*.
5. أدخل مفتاح "سر مشترك" وتنسيق المفتاح. يجب أن يتطابق هذا مع الإدخال الذي تم إجراؤه في قائمة **أمان** WLC.
6. أخترت **ASCII** ل المفتاح مدخل تنسيق، أي ينبغي كنت ال نفس على ال WLC.
7. أخترت **RADIUS (cisco Airespace)** ل يصادق يستعمل in order to ثبتت البروتوكول يستعمل بين ال WLC و RADIUS نادل.
8. انقر فوق **إرسال +**

تطبيق.

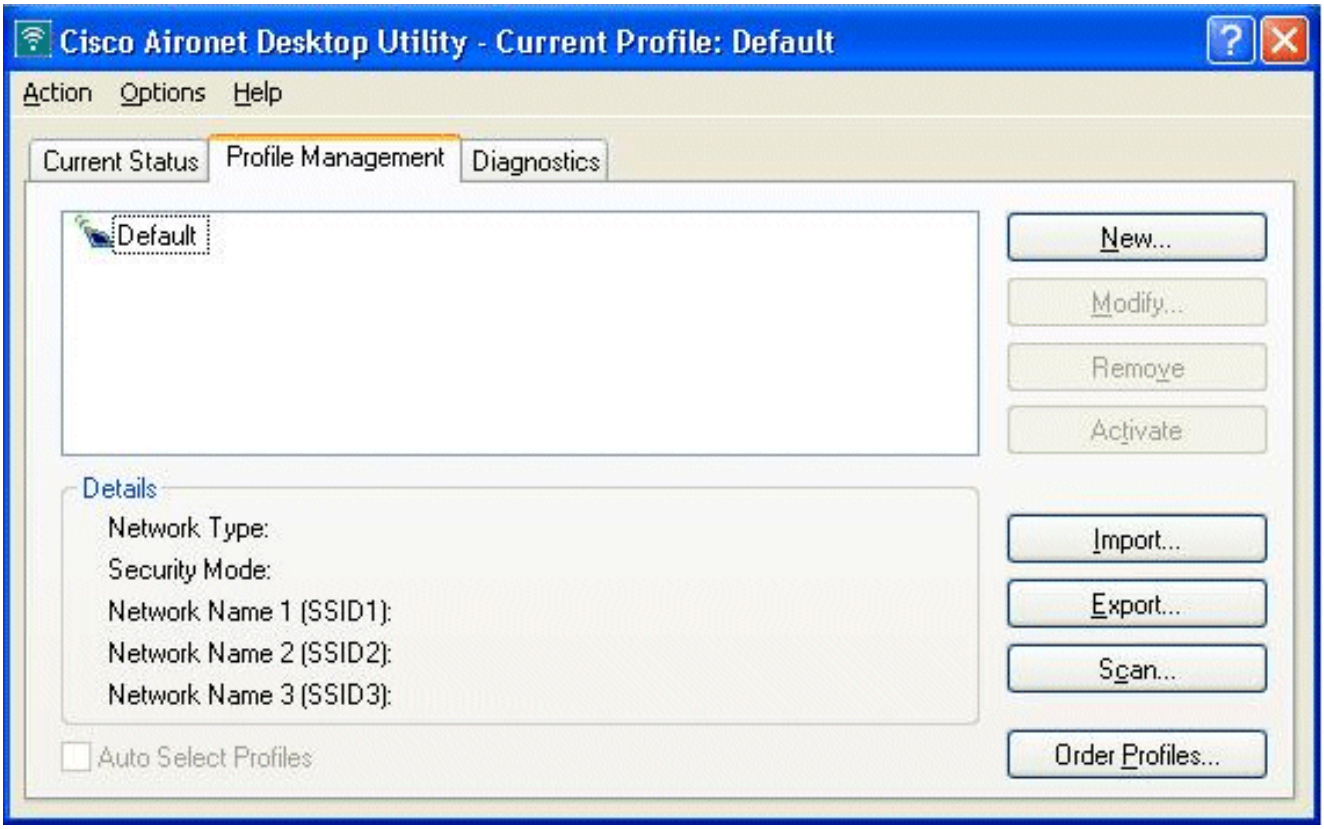


عملية مصادقة العميل

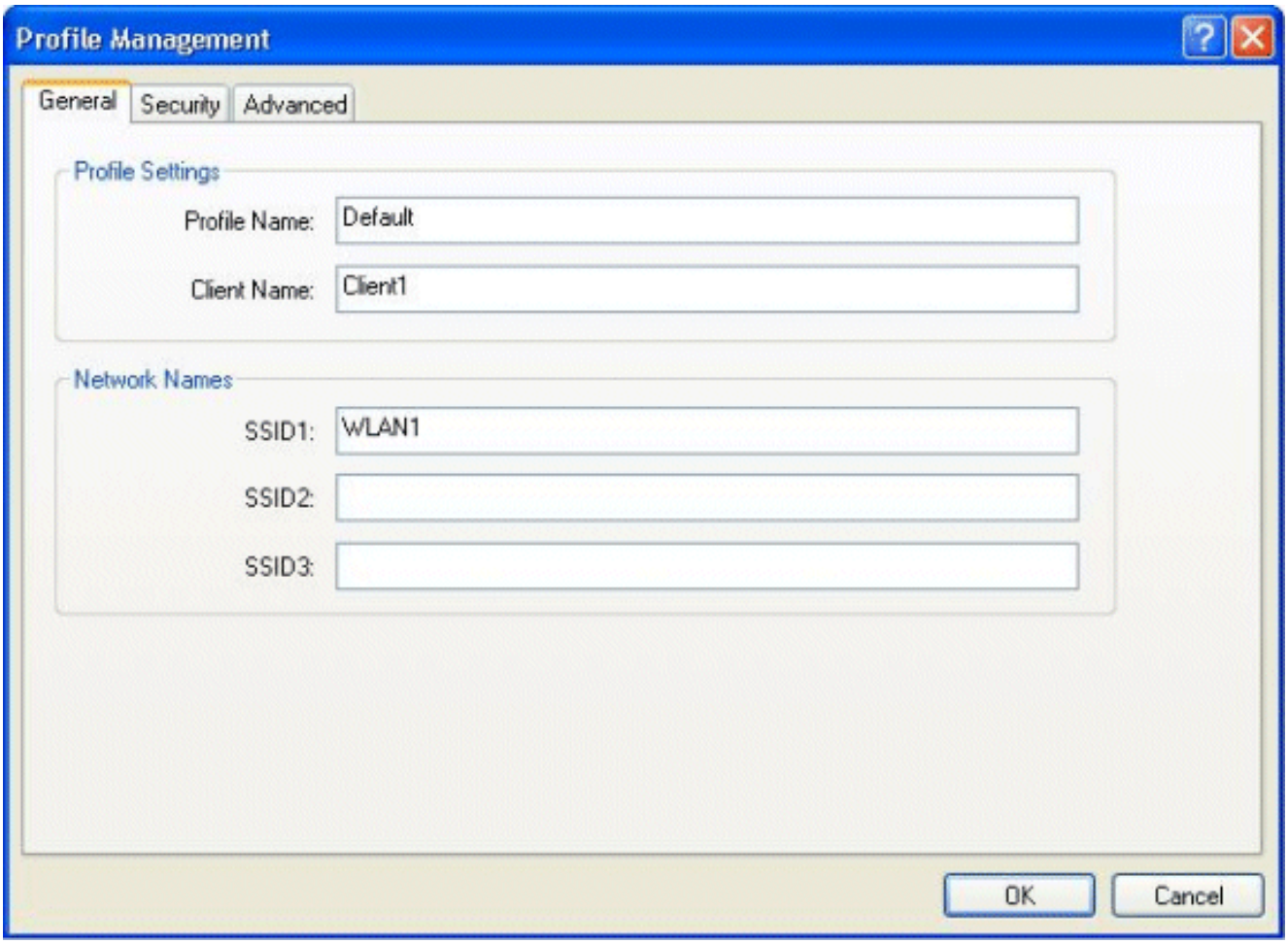
تكوين العميل

في هذا المثال، نستخدم الأداة المساعدة لسطح المكتب Cisco Aironet Desktop Utility لإجراء مصادقة الويب. قم بإجراء هذه الخطوات لتكوين الأداة المساعدة لسطح المكتب Aironet.

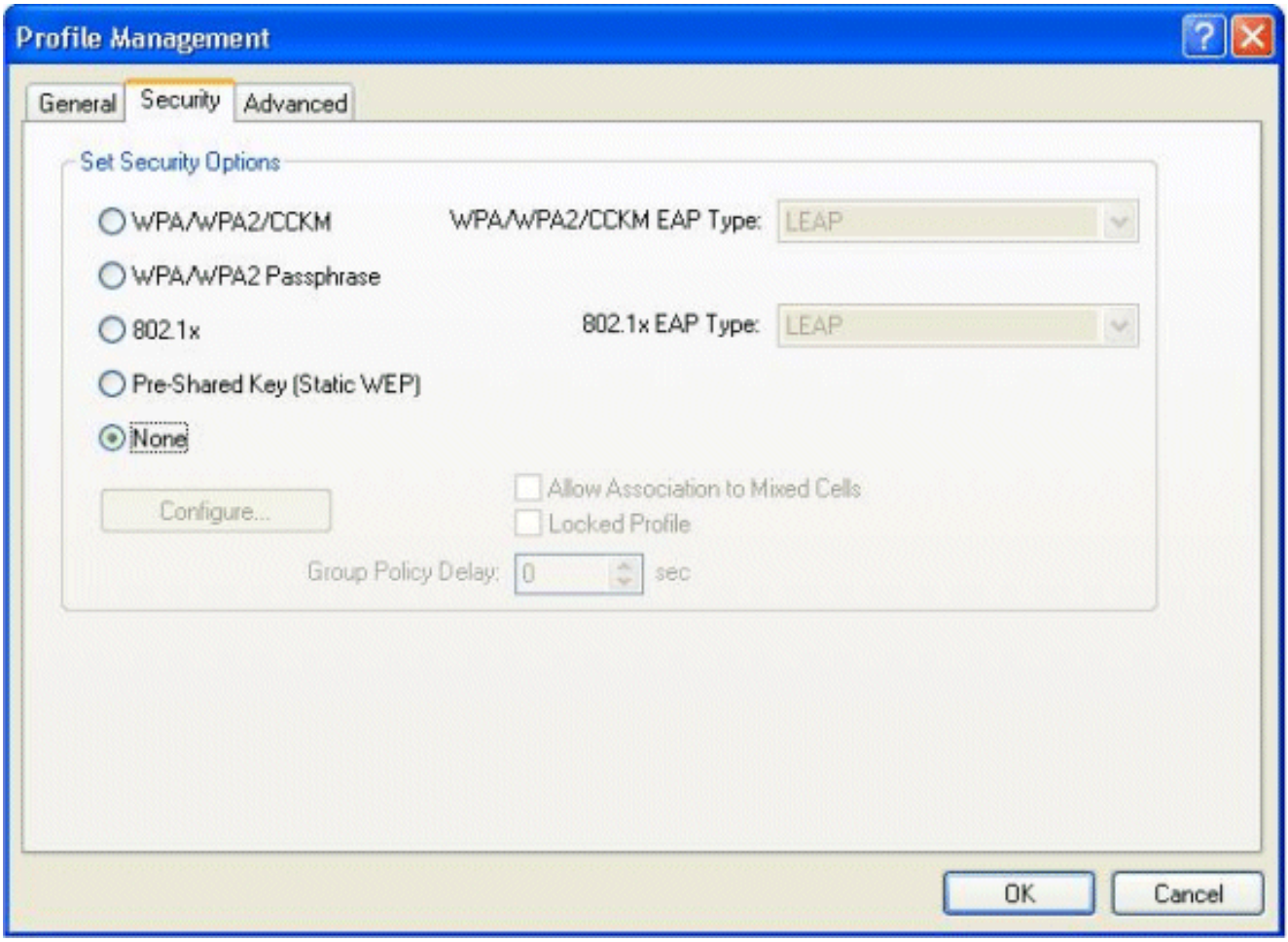
1. افتح أداة Aironet Desktop Utility من **البداية** > **Cisco Aironet** > **أداة Aironet Desktop Utility**.
2. انقر على علامة تبويب **إدارة التوصيفات**.



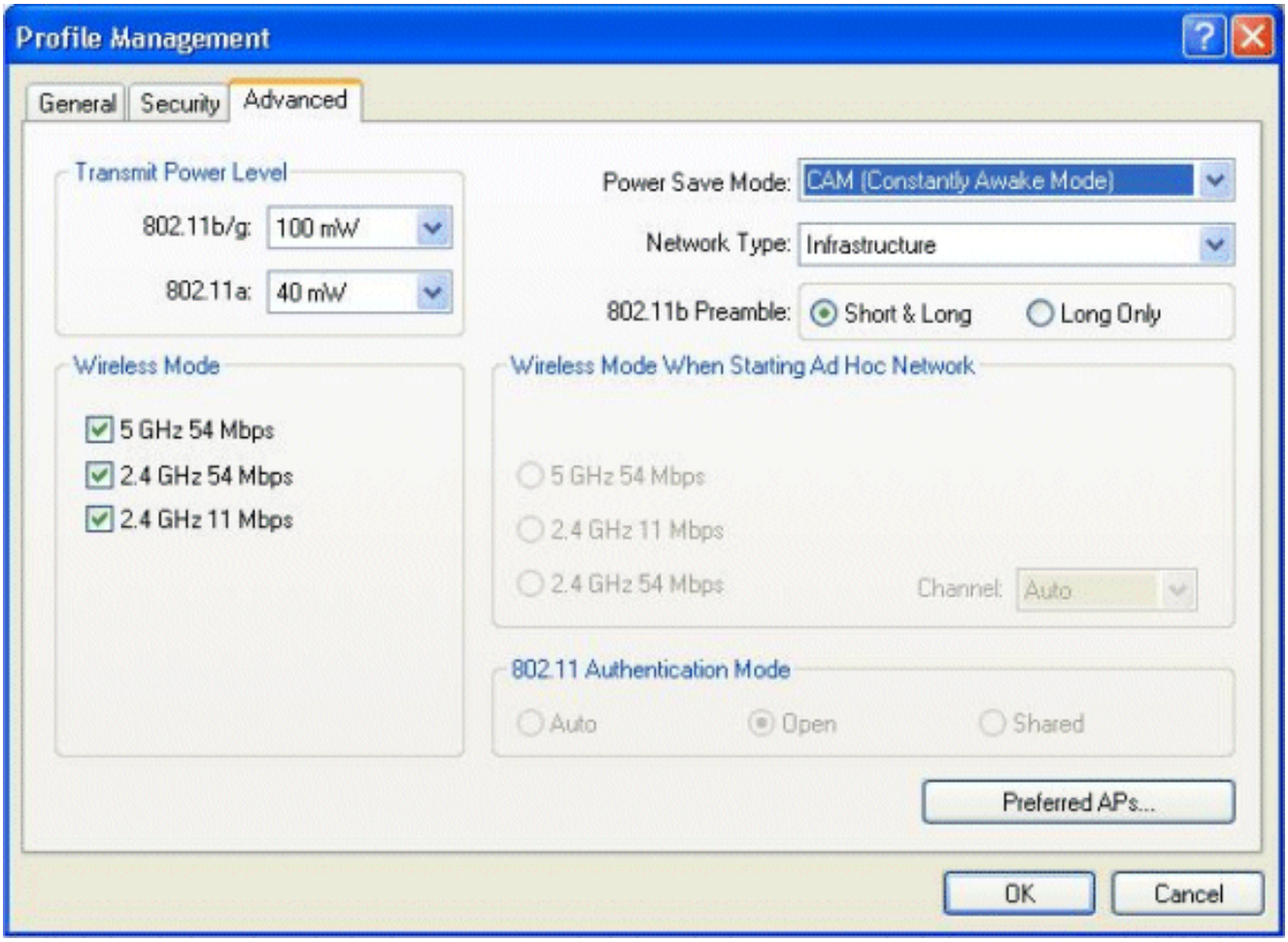
3. أختر ملف التخصيص **الافتراضي**، وانقر **تعديل**.انقر فوق علامة التبويب **عام**.تشكيل اسم توصيف. في هذا المثال، يتم إستخدام *الافتراضي*.قم بتكوين SSID تحت أسماء الشبكة. في هذا المثال، يتم إستخدام *WLAN1*.



ملاحظة: SSID حساس لحالة الأحرف ويجب أن يطابق شبكة WLAN التي تم تكوينها على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).انقر فوق علامة التبويب **أمان**.أختر **بلا** كأمان لمصادقة الويب.



انقر فوق علامة التبويب **خيارات متقدمة**.تحت قائمة **الوضع اللاسلكي**، أختر التردد الذي يتصل عنده العميل اللاسلكي بنقطة الوصول في الوضع اللاسلكي (LAP).أخترت تحت **ال transmit طاقة مستوى**، الطاقة أن يكون شكلت على ال WLC.أترك القيمة الافتراضية لوضع حفظ الطاقة.أختر **بنية أساسية** كنوع الشبكة.تعيين دياجة 802.11b على أنها **قصيرة وطويلة** لتحقيق توافق أفضل.وانقر فوق **OK**.

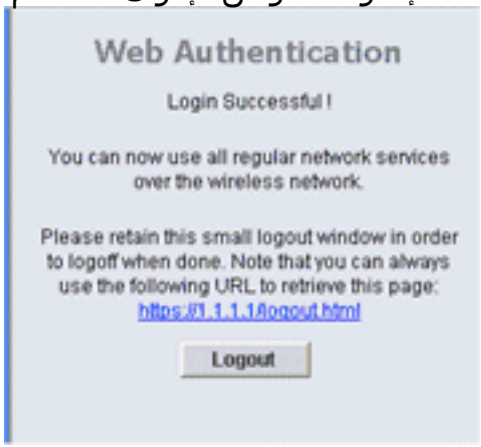


4. بمجرد تكوين ملف التعريف على برنامج العميل، يتم اقتران العميل بنجاح ويستلم عنوان IP من تجمع VLAN الذي تم تكوينه لواجهة الإدارة.

عملية تسجيل دخول العميل

يشرح هذا القسم كيفية حدوث تسجيل دخول العميل.

1. افتح نافذة المستعرض وأدخل أي عنوان URL أو عنوان IP. يؤدي هذا إلى جلب صفحة مصادقة الويب إلى العميل. إذا كانت وحدة التحكم تقوم بتشغيل أي إصدار أقدم من 3.0، فيجب على المستخدم إدخال *https://1.1.1.1/login.html* لإظهار صفحة مصادقة الويب. تظهر نافذة تنبيه أمان.
2. طقطقة **نعم** in order to باشرت.
3. عندما تظهر نافذة تسجيل الدخول، أدخل اسم المستخدم وكلمة المرور اللذين تم تكوينهما على خادم RADIUS. إذا نجح تسجيل دخولك، فسترى نافذتي مستعرض. الإطار الأكبر يشير إلى تسجيل دخول ناجح، ويمكنك هذا الإطار لاستعراض الإنترنت. أستخدم الإطار الأصغر لتسجيل الخروج عند اكتمال إستخدامك لشبكة



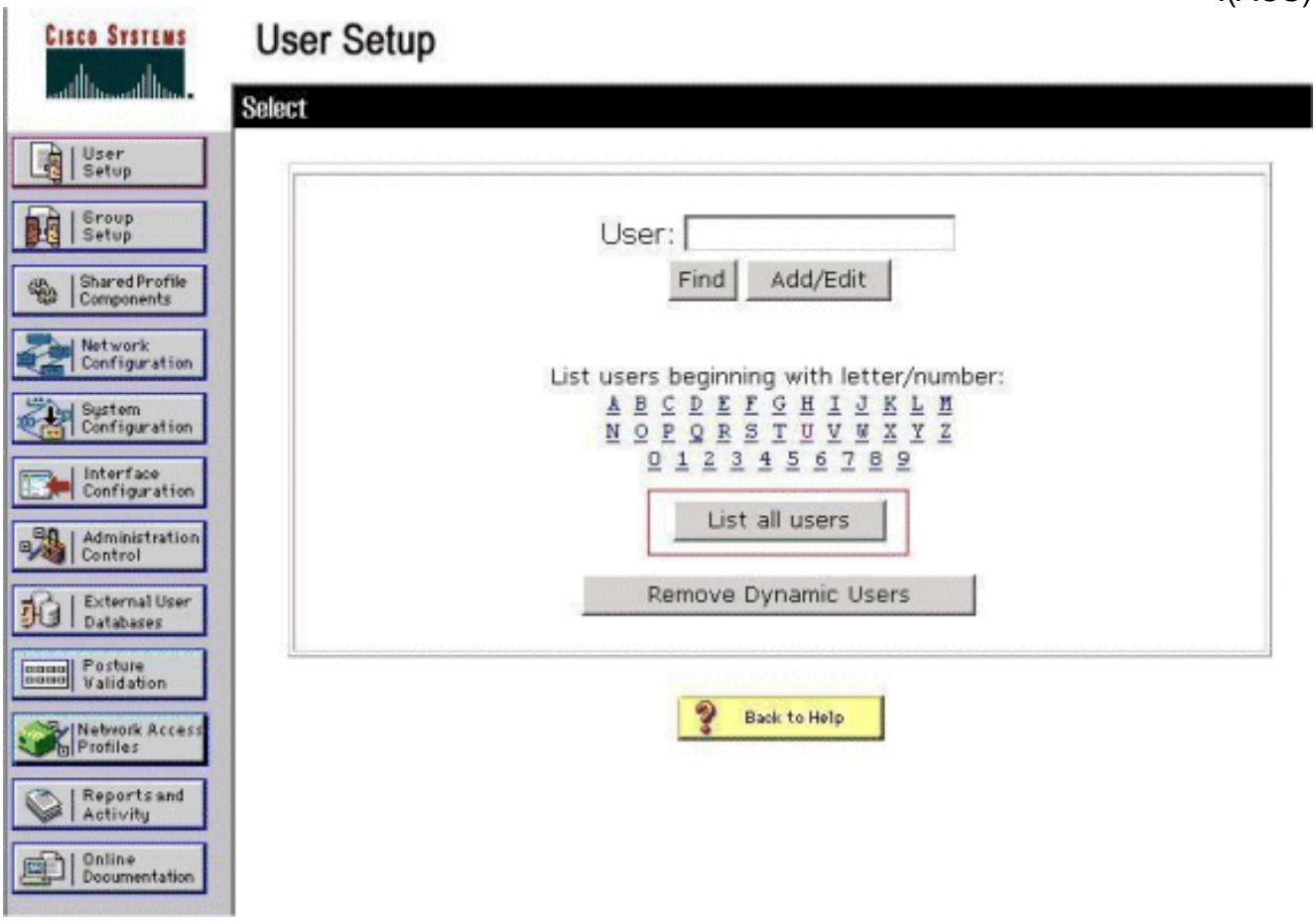
الضيوف.

التحقق من الصحة

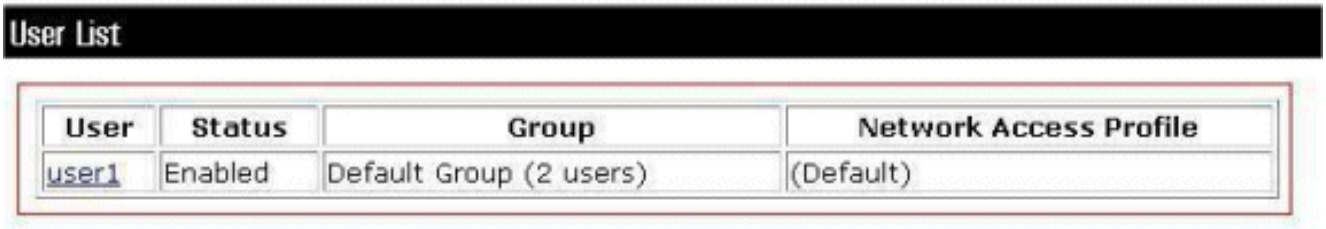
من أجل مصادقة ويب ناجحة، تحتاج إلى التحقق من تكوين الأجهزة بطريقة مناسبة. يشرح هذا القسم كيفية التحقق من الأجهزة المستخدمة في العملية.

التحقق من مصدر المحتوى الإضافي

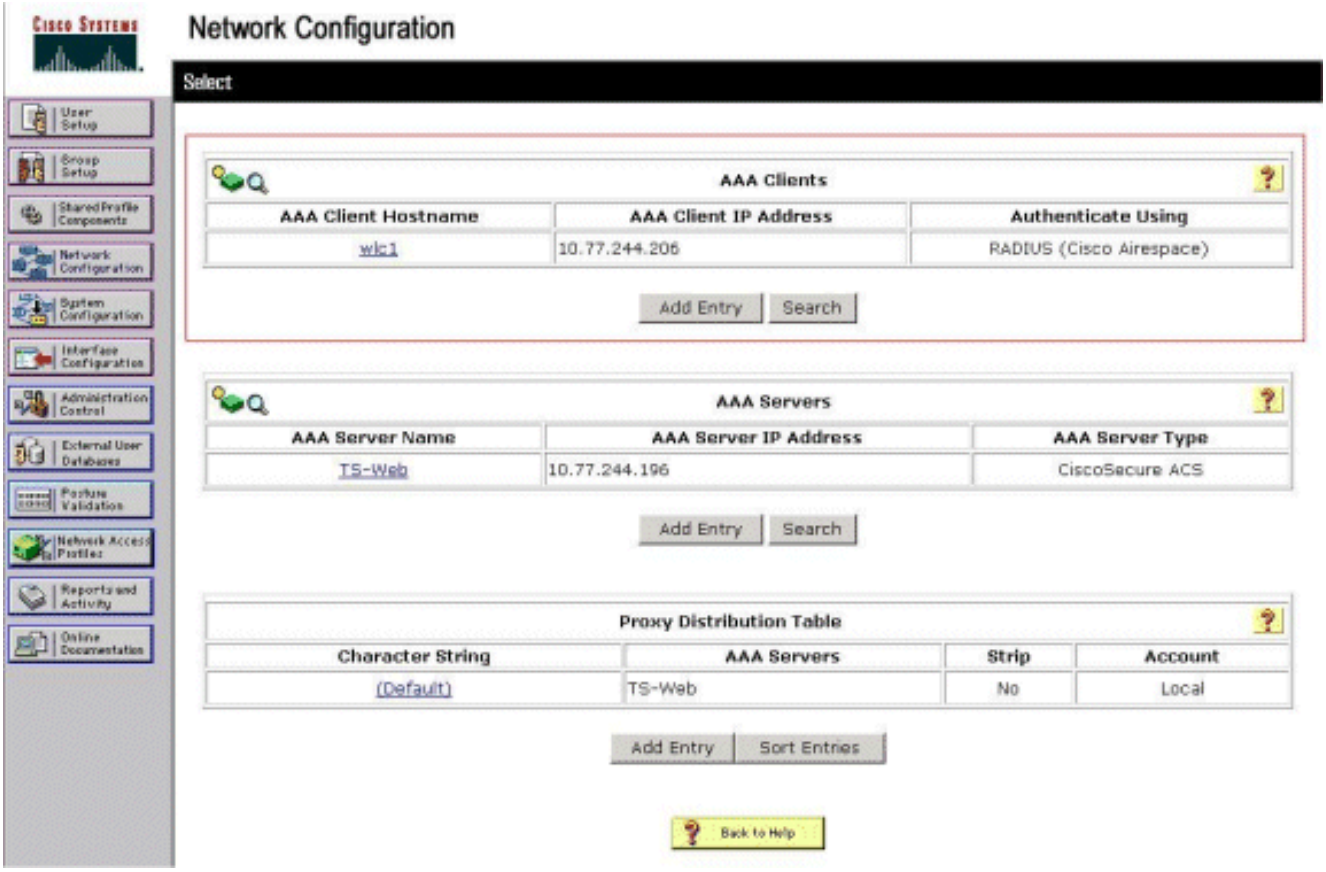
1. انقر فوق **إعداد المستخدم**، ثم انقر فوق **سرد جميع المستخدمين** في واجهة المستخدم الرسومية (ACS).



تأكد من تمكين حالة المستخدم ومن تعيين المجموعة الافتراضية للمستخدم.



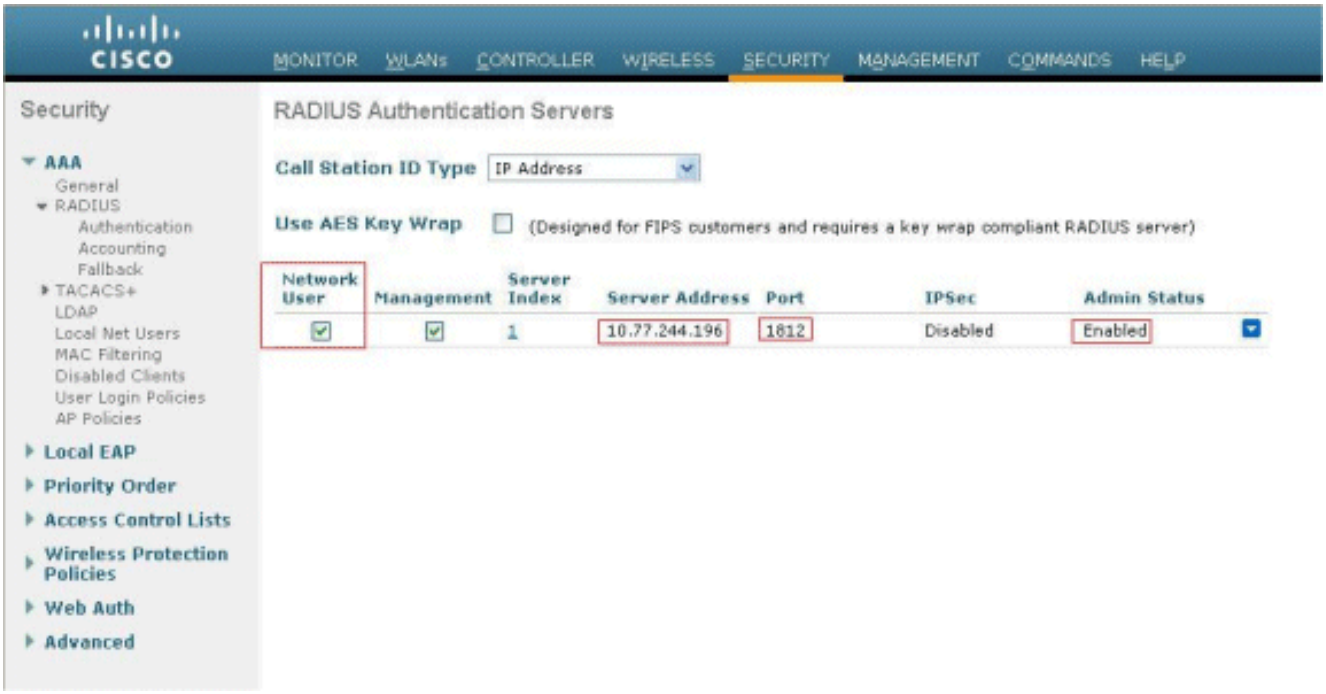
2. انقر فوق علامة التبويب **تكوين الشبكة**، وابحث في جدول **عملاء AAA** للتحقق من تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA.



التحقق من WLC

1. طقطقت ال **WLANs** قائمة من ال WLC GUI.تأكد من إدراج شبكة WLAN المستخدمة لمصادقة الويب في الصفحة.تأكد من *تمكين* حالة المسؤول لشبكة WLAN.تأكد من أن سياسة الأمان للشبكة المحلية اللاسلكية (WLAN) تعرض مصادقة *الويب*.

2. انقر فوق قائمة **الأمان** من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC).تأكد من إدراج مصدر المحتوى الإضافي الآمن من 10.77.244.196) Cisco) في الصفحة.تأكد من تحديد مربع مستخدم الشبكة.تأكد من أن المنفذ هو *1812* وأن حالة المسؤول ممكنة.



استكشاف الأخطاء وإصلاحها

هناك العديد من الأسباب التي تجعل مصادقة ويب غير ناجحة. يشرح المستند أستكشاف أخطاء مصادقة الويب وإصلاحها على وحدة تحكم شبكة محلية لاسلكية (WLC) بشكل واضح هذه الأسباب بالتفصيل.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر **debug** هذه.

Telnet في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وأصدر هذه الأوامر لاستكشاف أخطاء المصادقة وإصلاحها:

- **debug aaa all enable**

```
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
  ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00  00 00 00 00 00 00 0
                                                 ............s...  00 0
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73  65 72 31 02 12 93 c
                                                 user1....f......  66 3
                          Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
                                                               user1
    Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
      Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
                  erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
                     Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
 Fri Sep 24 13:59:52 2010:       structureSize.............................89
  Fri Sep 24 13:59:52 2010:       resultCode.................................0
Fri Sep 24 13:59:52 2010:       protocolUsed..............................0x0
                                                                    0000001
:Fri Sep 24 13:59:52 2010:       proxyState................................00
                                                          AC:DD:05-00:00:40:96
                        :Fri Sep 24 13:59:52 2010:       Packet contains 2 AVPs
.................Fri Sep 24 13:59:52 2010:           AVP[01] Framed-IP-Address
                                                (0xffffffff (-1) (4 bytes.....
.............................Fri Sep 24 13:59:52 2010:           AVP[02] Class
                                          (CACS:0/5183/a4df4ce/user1 (25 bytes.....
```

```
      Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio
                                                                  n 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
                                                                      ac:dd:05:
                                        source: 48, valid bits: 0x1
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

                          dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
 ,'' :vlanIfName
                                                                          :aclName
 Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
                       station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
                                                                 tation 00:40:96:ac:dd:05
        Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
                          :Fri Sep 24 13:59:52 2010:       Packet contains 12 AVPs
.........................Fri Sep 24 13:59:52 2010:           AVP[01] User-Name
                                                                (user1 (5 bytes.....
.............................Fri Sep 24 13:59:52 2010:           AVP[02] Nas-Port
                                                        (0x00000002 (2) (4 bytes.....
.....................Fri Sep 24 13:59:52 2010:           AVP[03] Nas-Ip-Address
                                                    (0x0a4df4ce (172881102) (4 bytes.....
...................Fri Sep 24 13:59:52 2010:           AVP[04] Framed-IP-Address
                                                    (0x0a4df4c7 (172881095) (4 bytes.....
```

- enable debug aaa detail

يتم سرد محاولات المصادقة الفاشلة في القائمة الموجودة في **التقارير والنشاط > محاولات فاشلة**.

معلومات ذات صلة

- مثال تكوين مصادقة الويب لوحدة تحكم الشبكة المحلية (LAN) اللاسلكية
- أستكشاف أخطاء مصادقة الويب وإصلاحها على وحدة تحكم شبكة محلية لاسلكية (WLC)
- مثال تكوين المصادقة الخارجية للويب مع وحدات تحكم الشبكة المحلية (LAN) اللاسلكية
- مصادقة الويب باستخدام LDAP على مثال تكوين وحدات تحكم الشبكة المحلية (LAN) اللاسلكية (WLCs)
- 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).