قائمة التحكم في الوصول (ACL) لكل مستخدم مع وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية ومثال تكوين Cisco الآمن من ACS

المحتويات

المقدمة

يشرح هذا المستند من خلال مثال كيفية إنشاء قوائم التحكم في الوصول (ACLs) على قوائم التحكم في الوصول (WLCs) وتطبيقها على المستخدمين الذين يعتمدون على تفويض RADIUS.

المتطلبات الأساسية

المتطلبات

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

- معرفة أساسية بكيفية تكوين خادم Cisco Secure ACS لمصادقة العملاء اللاسلكيين
- معرفة تكوين نقاط الوصول في الوضع (Lightweight (LAPs و Cisco Wireless LAN Controllers ((WLCs
- معرفة حلول الأمان اللاسلكية الموحدة من Cisco

المكونات المستخدمة

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

- وحدة التحكم في شبكة LAN اللاسلكية Cisco 4400 Series التي تشغل الإصدار 5.0.148.0
- نقاط الوصول في الوضع (Lightweight (LAPs من سلسلة Cisco Aironet 1231
- مهايئ عميل شبكة LAN اللاسلكية من Cisco Wireless LAN Client Cisco Aironet 802.11 a/b/g Adapter الذي يشغل الإصدار 3.6
- Cisco Aironet Desktop Utility، الإصدار 3.6
- خادم ACS الآمن من Cisco، الإصدار 4.1
- موجه الخدمات المتكاملة Cisco 2800 Series Integrated Services Router الذي يعمل بنظام التشغيل IOS®، الإصدار T(11)12.4
- cisco مادة حفازة 2900xl sery مفتاح أن يركض صيغة WC3b(5)12.0

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.

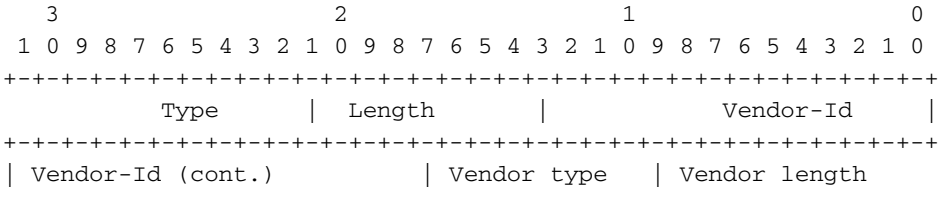
معلومات أساسية

قائمة التحكم في الوصول لكل مستخدم (ACL) هي جزء من شبكة هوية Cisco. يدعم حل Cisco Wireless LAN شبكات الهوية، والتي تسمح للشبكة بالإعلان عن معرف SSID واحد، كما تسمح لمستخدمين محددين بتوريث سياسات مختلفة استنادا إلى ملفات تعريف المستخدمين الخاصة بهم.

توفر ميزة قائمة التحكم في الوصول (ACL) لكل مستخدم إمكانية تطبيق قائمة تحكم في الوصول (ACL) تم تكوينها على وحدة التحكم في الشبكة المحلية اللاسلكية على مستخدم استنادا إلى تفويض RADIUS. ويتم تحقيق ذلك باستخدام السمة المحددة للمورد (VSA) ل Airespace-ACL-Name.

تشير هذه السمة إلى اسم قائمة التحكم في الوصول (ACL) المطلوب تطبيقه على العميل. عندما تكون سمة قائمة التحكم في الوصول (ACL) موجودة في "قبول الوصول إلى RADIUS"، يطبق النظام اسم قائمة التحكم في الوصول (ACL) على محطة العميل بعد مصادقته. يتخطى هذا الإجراء أي قوائم تحكم في الوصول (ACL) يتم تعيينها إلى الواجهة. فهو يتجاهل قائمة التحكم في الوصول (ACL) الخاصة بالواجهة المعينة ويطبق القائمة الجديدة.

يوجد أدناه ملخص لتنسيق سمة اسم قائمة التحكم في الوصول (ACL). يتم إرسال الحقول من اليسار إلى اليمين



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
ACL Name...                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

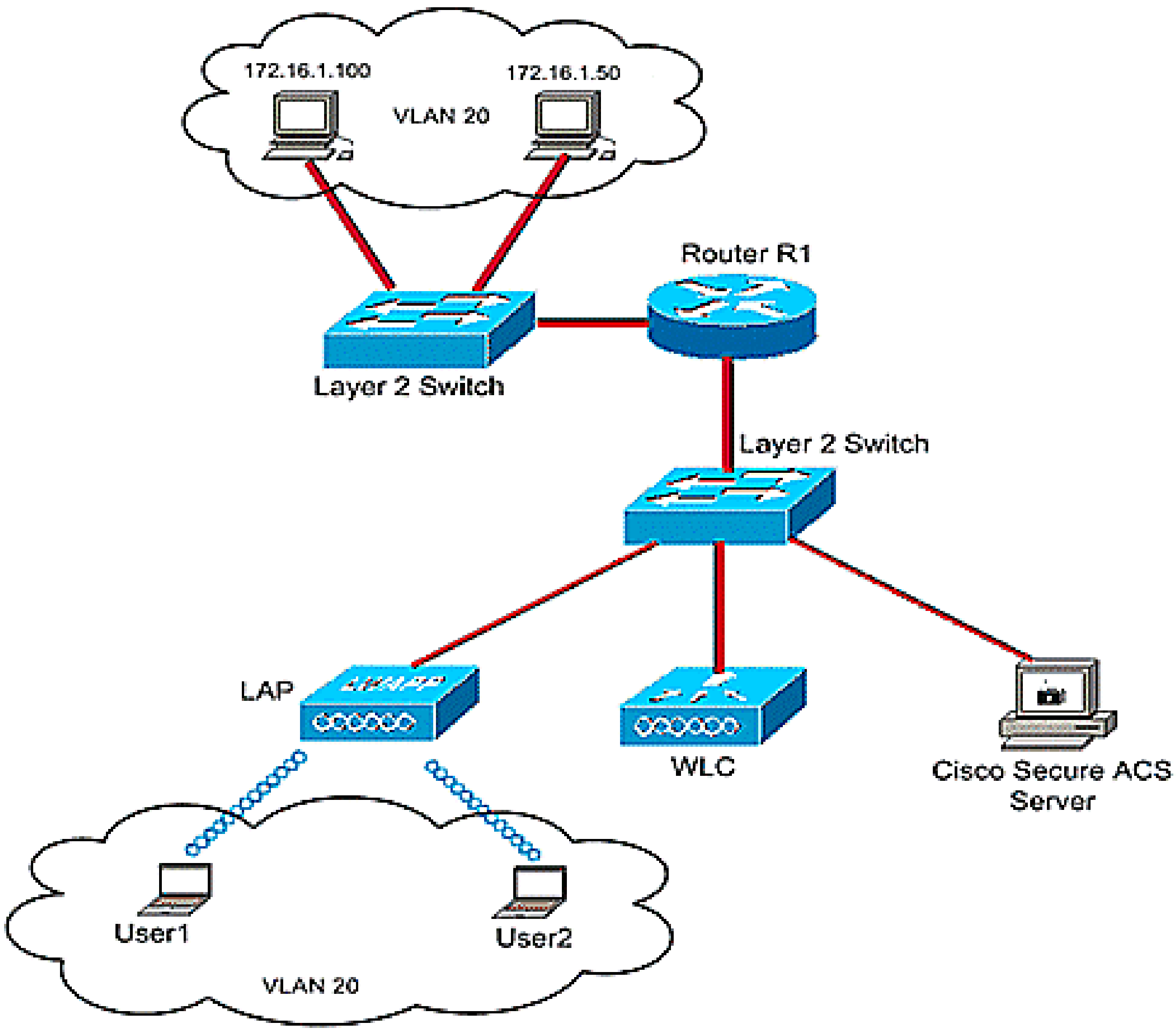
- Type - 26 for Vendor-Specific
- Length - >7
- Vendor-Id - 14179
- Vendor type - 6
- Vendor length - >0
- Value - A string that includes the name of the ACL to use for the client. The string is case sensitive.

لمزيد من المعلومات حول شبكة معرف الشبكة اللاسلكية الموحدة من Cisco، ارجع إلى قسم تكوين شبكات الهوية في المستند تكوين حلول الأمان.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

في هذا الإعداد، يتم إستخدام وحدة تحكم الشبكة المحلية اللاسلكية (LAN) ووحدة التحكم في الشبكة المحلية اللاسلكية (WLC) ونقطة الوصول في الوضع (LAP (Lightweight لتوفير الخدمات اللاسلكية للمستخدمين في القسم A والقسم B. يستخدم جميع المستخدمين اللاسلكيين مكتب شبكة (WLAN (SSID مشتركة للوصول إلى الشبكة وهم في شبكة VLAN Office-VLAN.



يتم إستخدام خادم ACS الآمن من Cisco لمصادقة المستخدمين اللاسلكيين. تستخدم مصادقة EAP لمصادقة

المستخدمين. يتم توصيل خادم WLC و LAP و Cisco ACS الآمن بمحول الطبقة 2 كما هو موضح.

يعمل الموجه R1 على توصيل الخوادم على الجانب السلكي من خلال محول الطبقة 2 كما هو موضح. يعمل الموجه R1 أيضا كخادم DHCP، الذي يوفر عناوين IP إلى عملاء اللاسلكي من الشبكة الفرعية 16/172.16.0.0.

أنت تحتاج أن يشكل الأداة أن هذا يقع:

المستخدم1 من القسم A لديه حق الوصول إلى الخادم 172.16.1.100 فقط

المستخدم 2 من القسم ب لديه حق الوصول إلى الخادم 172.16.1.50 فقط

ومن أجل تحقيق ذلك، تحتاج إلى إنشاء 2 قائمة تحكم في الوصول (ACL) على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC): واحدة للمستخدم1، والأخرى للمستخدم 2. بمجرد إنشاء قوائم التحكم في الوصول، يلزمك تكوين خادم Cisco Secure ACS لإرجاع سمة اسم قائمة التحكم في الوصول إلى عنصر التحكم في الوصول (WLC) عند المصادقة الناجحة للمستخدم اللاسلكي. تطبق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بعد ذلك قائمة التحكم في الوصول (ACL) على المستخدم، وبالتالي يتم تقييد الشبكة بناء على ملف تعريف المستخدم.

ملاحظة: يستخدم هذا المستند مصادقة LEAP لمصادقة المستخدمين. تكون تقنية LEAP من Cisco عرضة لهجمات القاموس. في شبكات الوقت الفعلي، يجب إستخدام أساليب مصادقة أكثر أمانا مثل EAP FAST. بما أن تركيز الوثيقة ينصب على شرح كيفية تكوين ميزة قائمة التحكم بالوصول لكل مستخدم، فإنه يتم إستخدام LEAP من أجل التبسيط.

يوفر القسم التالي إرشادات خطوة بخطوة لتكوين الأجهزة لهذا الإعداد.

التكوين

قبل تكوين ميزة قوائم التحكم في الوصول (ACL) لكل مستخدم، يجب تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للعملية الأساسية وتسجيل نقاط الوصول في الوضع Lightweight إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يفترض هذا المستند أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تم تكوينه للعملية الأساسية وأن نقاط الوصول في الوضع Lightweight تم تسجيلها إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). إذا كنت مستخدما جديدا، والذي 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).

بمجرد تسجيل نقاط الوصول في الوضع Lightweight، أكمل الخطوات التالية لتكوين الأجهزة الخاصة بهذا الإعداد:

1. قم بتكوين وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية.
2. قم بتكوين خادم ACS الآمن من Cisco.
3. التحقق من التكوين.

ملاحظة: يناقش هذا المستند التكوين المطلوب على الجانب اللاسلكي. يفترض المستند أن التكوين السلكي في موضعه.

تكوين وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية

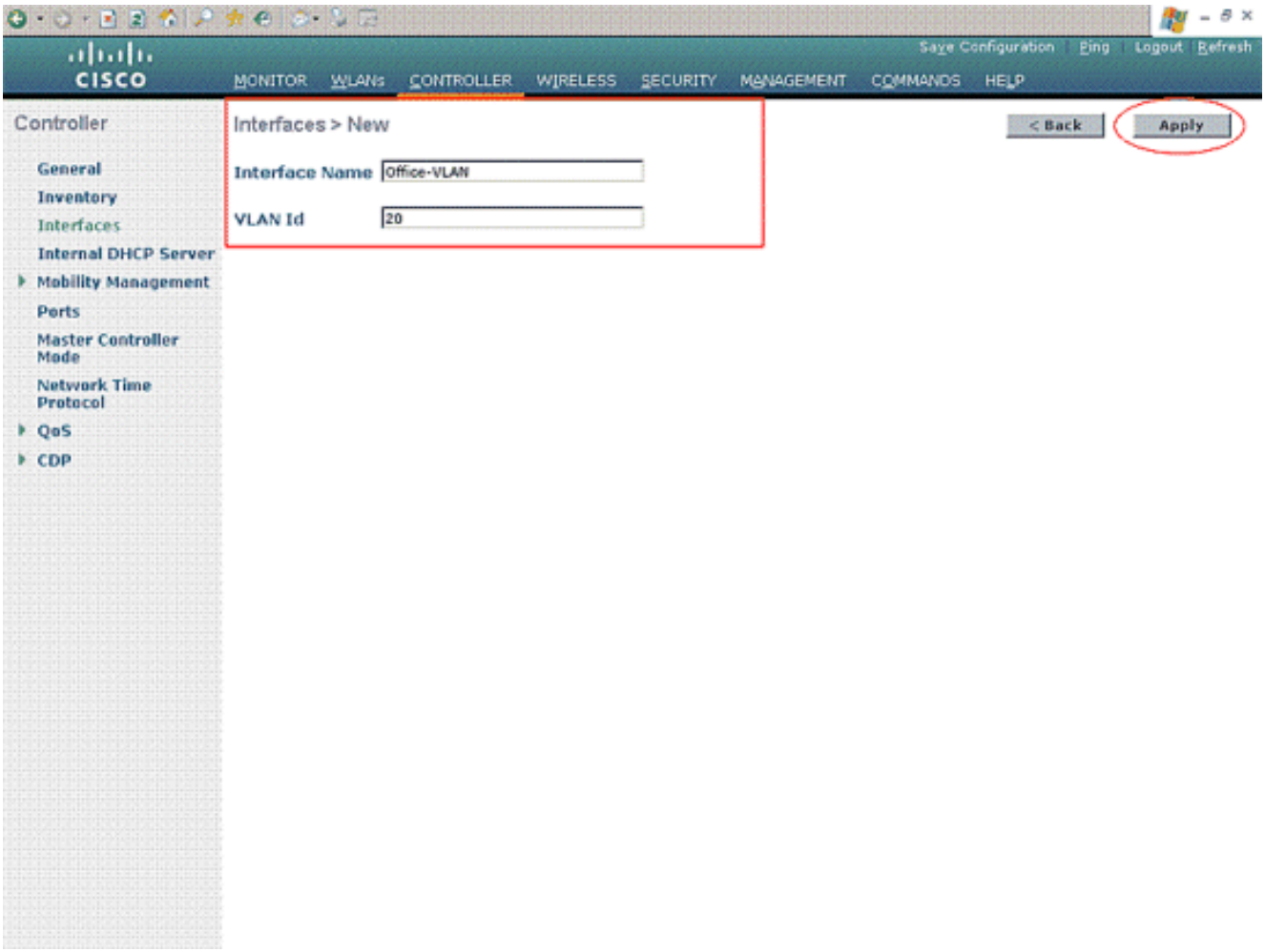
على وحدة التحكم في الشبكة المحلية اللاسلكية، يجب القيام بما يلي:

- خلقت VLAN للمستخدمين اللاسلكي.
- قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة المستخدمين اللاسلكيين مع Cisco Secure ACS.
- إنشاء شبكة WLAN جديدة للمستخدمين اللاسلكيين.
- تحديد قوائم التحكم في الوصول (ACL) للمستخدمين اللاسلكيين.

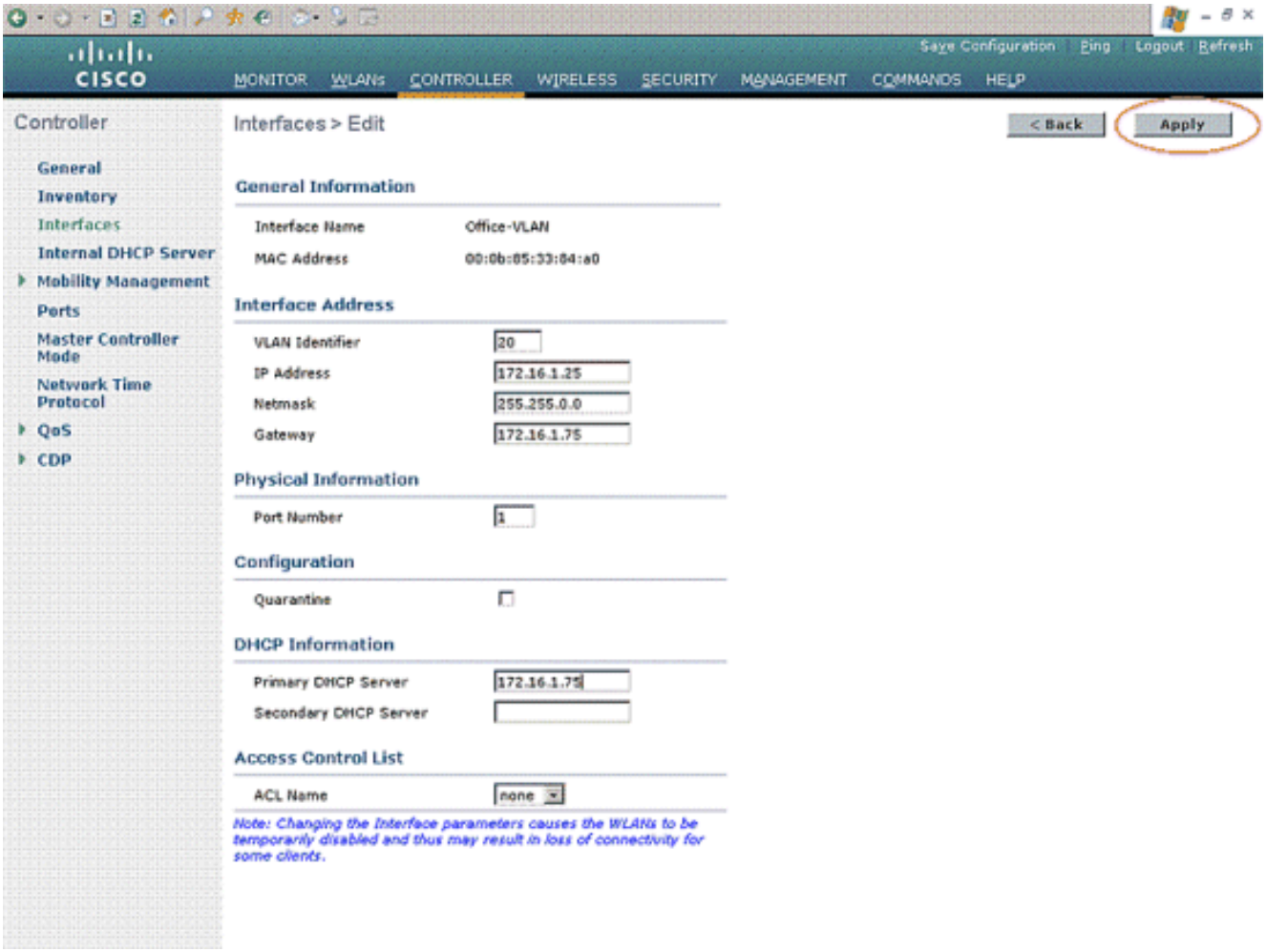
خلقت VLAN للمستخدمين اللاسلكي

أتمت in order to خلقت VLAN للمستخدمين اللاسلكي، هذا steps.

1. انتقل إلى واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) واختر **وحدة التحكم > الواجهات**. تظهر نافذة الواجهات. تسرد هذه النافذة الواجهات التي تم تكوينها على وحدة التحكم.
2. انقر فوق **جديد** لإنشاء واجهة ديناميكية جديدة.
3. دخلت في **القارن > جديد** نافذة، القارن إسم وال VLAN id. ثم انقر فوق تطبيق. في هذا المثال، يتم تسمية الواجهة الديناميكية باسم Office-VLAN، ويتم تعيين معرف شبكة VLAN على 20.



4. في نافذة **الواجهات > تحرير**، أدخل عنوان IP وقناع الشبكة الفرعية والبوابة الافتراضية للواجهة الديناميكية. عينت هو إلى ميناء طبيعي على ال WLC، وأدخل العنوان من ال DHCP نادل. ثم انقر فوق **تطبيق**.



على سبيل المثال، يتم إستخدام هذه المعلمات لواجهة Office-VLAN:

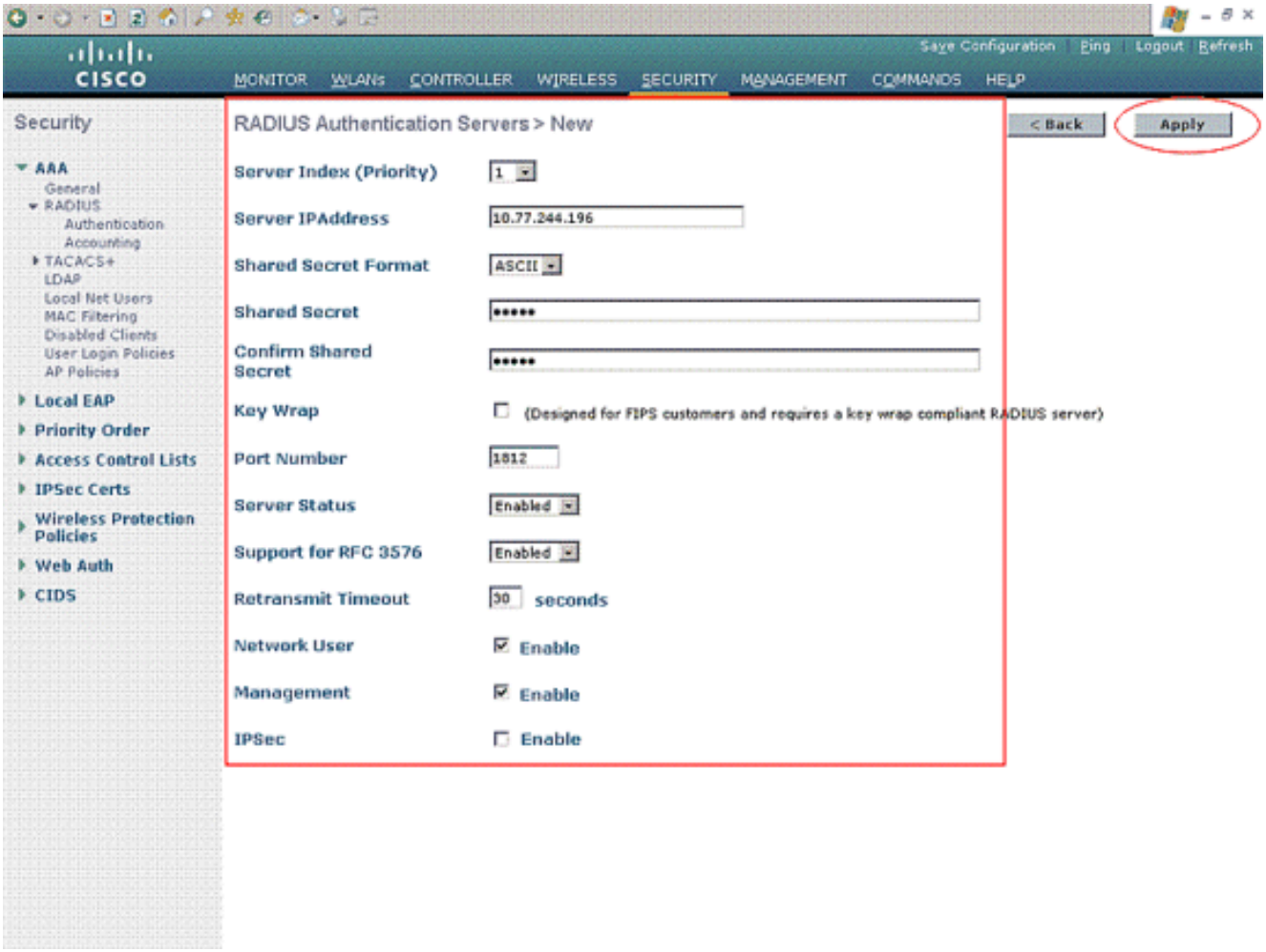
```
Office-VLAN
IP address: 172.16.1.25
Netmask: 255.255.0.0
(Default gateway: 172.16.1.75 (sub-interface on Router R1
Port on WLC: 1
DHCP server: 172.16.1.75
```

قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للمصادقة مع Cisco Secure ACS

يلزم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإعادة توجيه بيانات اعتماد المستخدم إلى خادم RADIUS خارجي (في هذه الحالة، مصدر المحتوى الإضافي الآمن من Cisco). يتحقق خادم RADIUS بعد ذلك من مسوغات المستخدم ويعيد سمة اسم قائمة التحكم بالوصول (ACL) إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) عند نجاح مصادقة المستخدم اللاسلكي.

أتمت هذا steps in order to شكلت ال WLC لنادل RADIUS:

1. أخترت **أمن** و**RADIUS مصادقة** 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 في **خوادم مصادقة RADIUS >** صفحة **جديدة**. وتتضمن هذه المعلمات عنوان IP لخادم RADIUS والسر المشترك ورقم المنفذ وحالة الخادم.

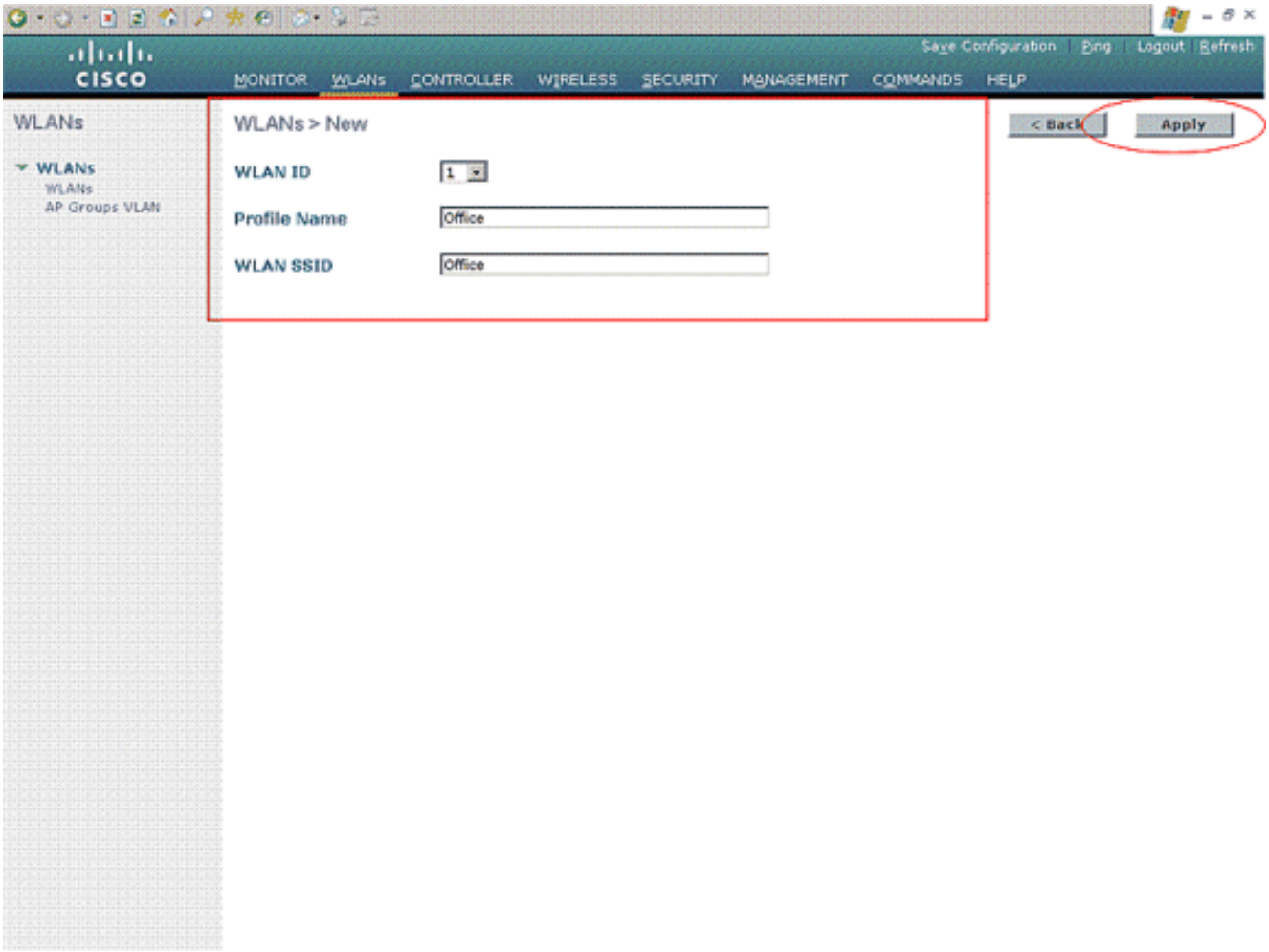


3. تحدد خانات الاختيار **Network User** and **Management** ما إذا كانت المصادقة المستندة إلى RADIUS تنطبق على الإدارة ومستخدمي الشبكة. يستعمل هذا مثال ال cisco يأمن ACS كخادم RADIUS مع عنوان 10.77.244.196. طقطقة **يطبق**.

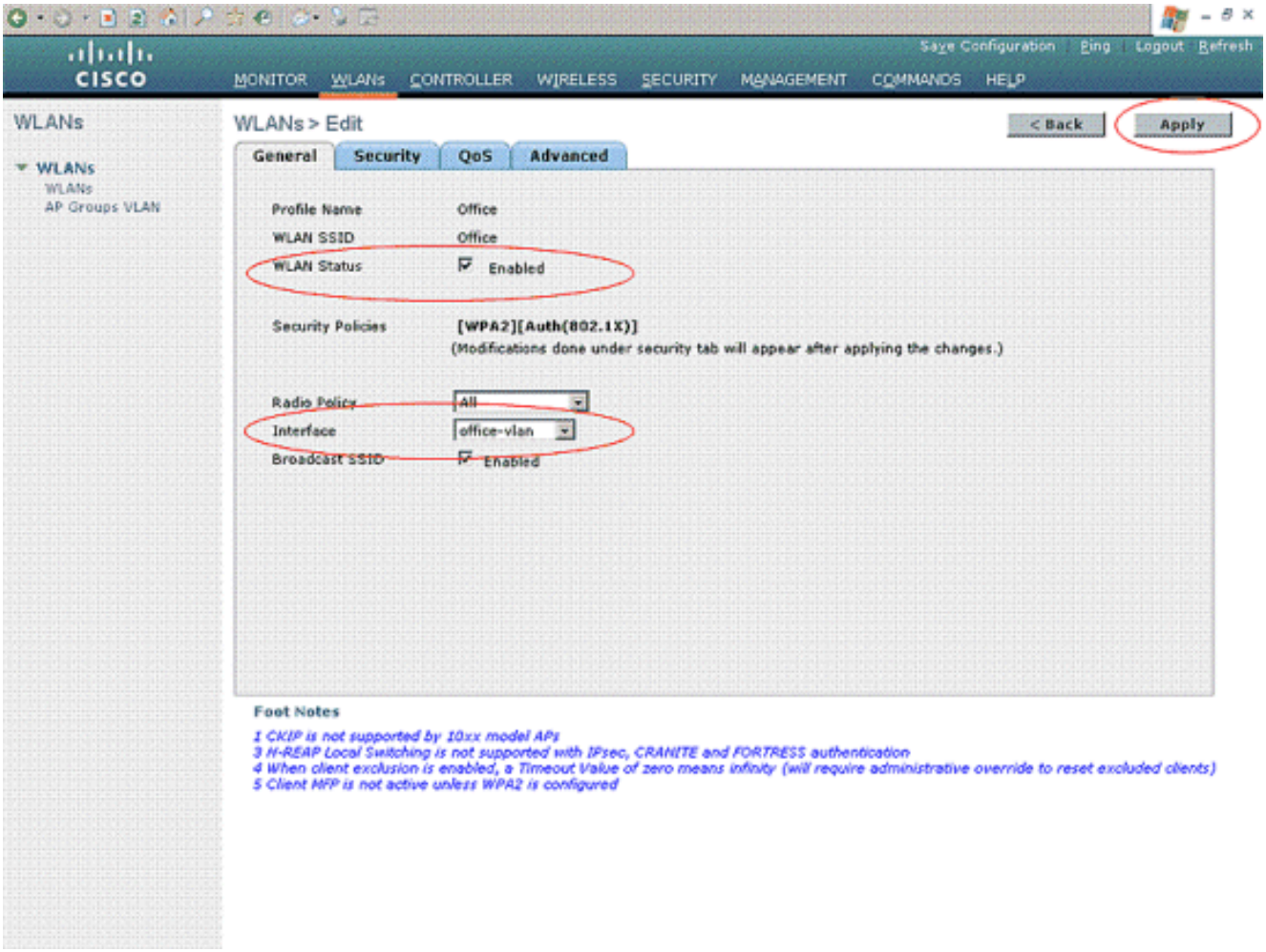
إنشاء شبكة WLAN جديدة للمستخدمين اللاسلكيين

بعد ذلك، يلزمك إنشاء شبكة WLAN يمكن للمستخدمين اللاسلكيين الاتصال بها. أتمت in order to خلقت WLAN جديد، هذا steps:

1. من واجهة المستخدم الرسومية (GUI) لوحدة تحكم الشبكة المحلية اللاسلكية، انقر على **شبكات WLAN**. تسرد هذه الصفحة شبكات WLAN الموجودة على وحدة التحكم.
2. أخترت **جديد** in order to خلقت WLAN جديد. أدخل معرف الشبكة المحلية اللاسلكية (WLAN) واسم ملف التعريف واسم شبكة WLAN للشبكة المحلية اللاسلكية (WLAN)، ثم انقر على **تطبيق**. لهذا الإعداد، قم بإنشاء **Office** لشبكة WLAN.

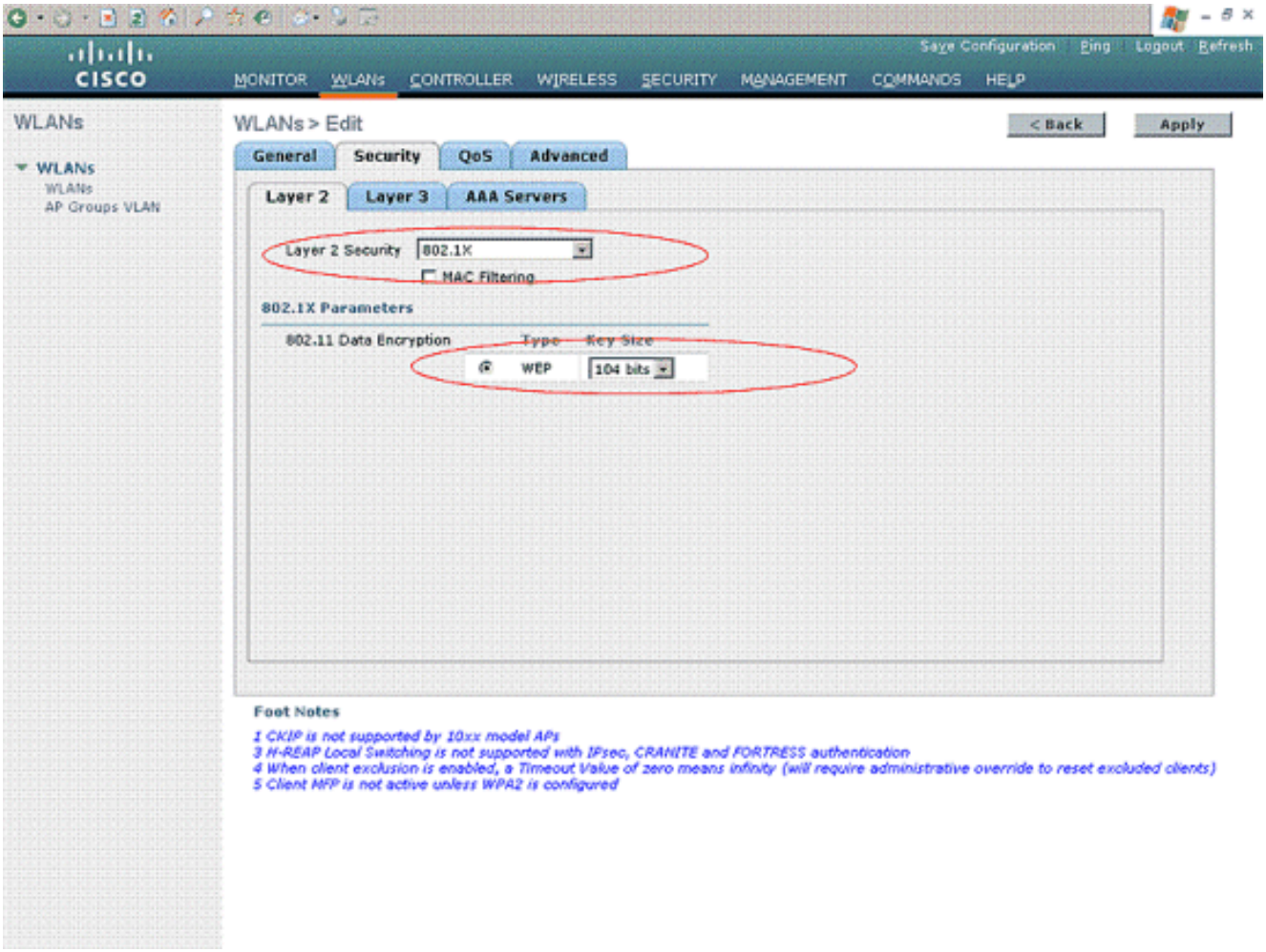


3. ما إن يخلق أنت WLAN جديد، ال **WLAN > تحرير** صفحة ل WLAN جديد يظهر. في هذه الصفحة، يمكنك تحديد معلمات مختلفة خاصة بشبكة WLAN هذه تتضمن السياسات العامة والأمان وجودة الخدمة والمعلمات المتقدمة.

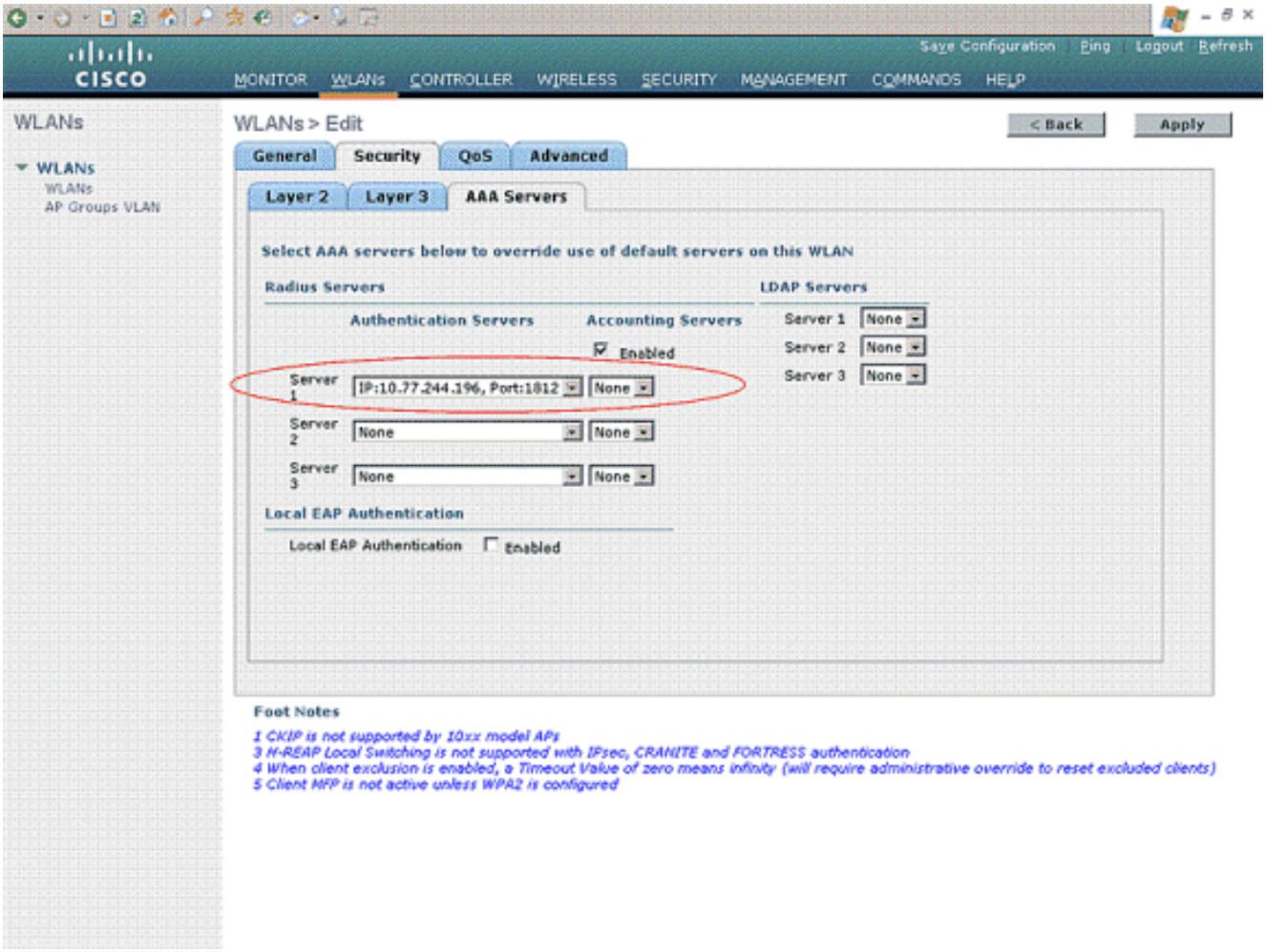


تحقق من **حالة شبكة WLAN** ضمن السياسات العامة لتمكين شبكة WLAN. أختر الواجهة المناسبة من القائمة المنسدلة. في هذا المثال، أستخدم الواجهة **Office-VLAN**. يمكن تعديل المعلمات الأخرى في هذه الصفحة استنادا إلى متطلبات شبكة WLAN.

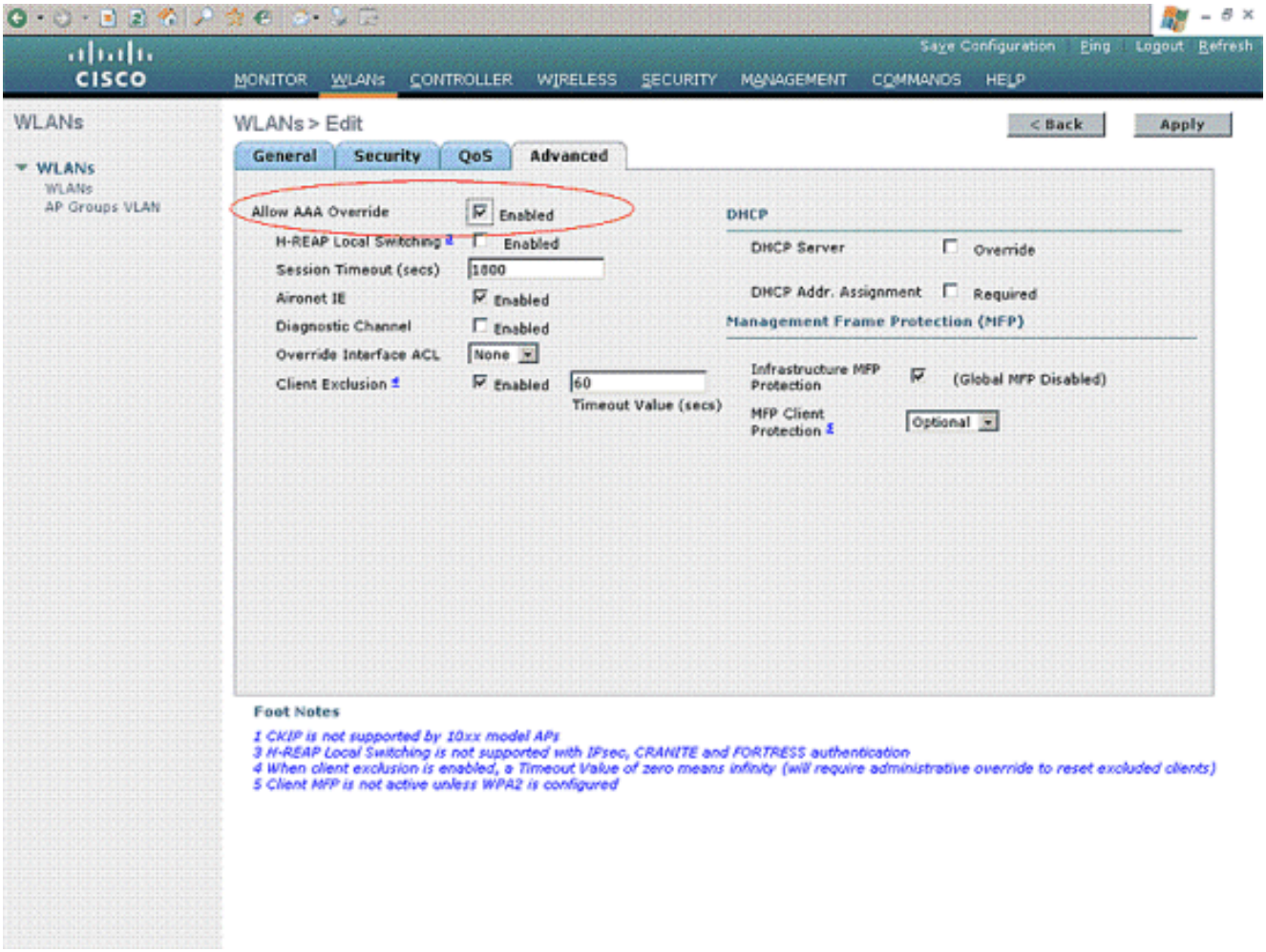
4. أختر **علامة التبويب تأمين**. أختر **802.1x** من قائمة المنسدلة أمان الطبقة 2 (لأنها مصادقة LEAP). أختر حجم مفتاح WEP المناسب تحت معاملات 802.1x.



5. تحت علامة التبويب تأمين، أختر علامة التبويب الفرعية **AAA server**. أختر خادم AAA الذي يتم إستخدامه لمصادقة العملاء اللاسلكيين. في هذا المثال، أستخدم خادم ACS 10.77.244.196 لمصادقة العملاء اللاسلكيين.



6. أختر علامة التبويب **خيارات متقدمة**. تحقق من **السماح بتجاوز AAA** لتكوين تجاوز سياسة المستخدم من خلال AAA على شبكة LAN لاسلكية.



عند تمكين تجاوز AAA، ولدى العميل معلمات مصادقة AAA متعارضة مع وحدة تحكم الشبكة المحلية (LAN) اللاسلكية من Cisco ووحدة تحكم الشبكة المحلية اللاسلكية من Cisco، يتم إجراء مصادقة العميل بواسطة خادم AAA. كجزء من هذه المصادقة، ينقل نظام التشغيل العملاء من حل شبكة LAN اللاسلكية الافتراضي من Cisco إلى شبكة VLAN اللاسلكية إلى شبكة VLAN التي يتم إرجاعها بواسطة خادم AAA والمحددة مسبقا في تكوين واجهة وحدة التحكم في شبكة LAN اللاسلكية من Cisco، والتي تحدث فقط عند تكوينها لتصفية MAC، و/أو 802.1X، و/أو عملية WPA. وفي جميع الحالات، يستخدم نظام التشغيل أيضا قيم الأولوية لجودة الخدمة (QoS) و DSCP وقيم علامات الأولوية المتوافقة مع معيار 802.1p وقوائم التحكم في الوصول (ACL) المقدمة من خادم AAA، طالما تم تعريفها مسبقا في تكوين واجهة وحدة التحكم في الشبكة المحلية اللاسلكية من Cisco.

7. أختر المعلمات الأخرى استنادا إلى متطلبات الشبكة. طقطقة **يطبق**.

تحديد قوائم التحكم في الوصول (ACL) للمستخدمين

تحتاج إلى إنشاء قوائم التحكم في الوصول (ACL) لهذا الإعداد:

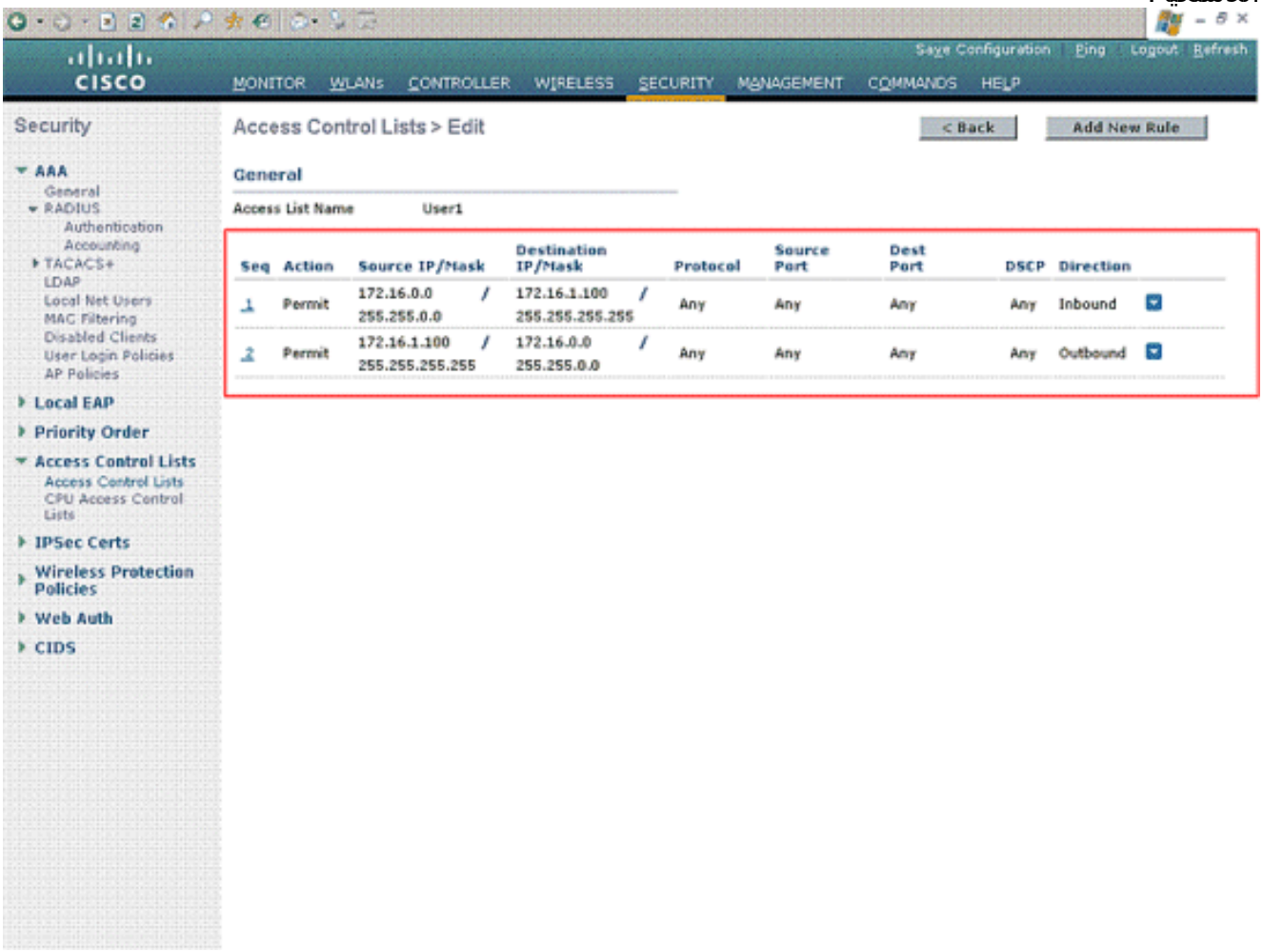
- ACL1: لتوفير الوصول إلى User1 إلى الخادم 172.16.1.100 فقط
- ACL2: لتوفير الوصول إلى User2 إلى الخادم 172.16.1.50 فقط

أتمت هذا steps أن يشكل ال ACLs على ال WLC:

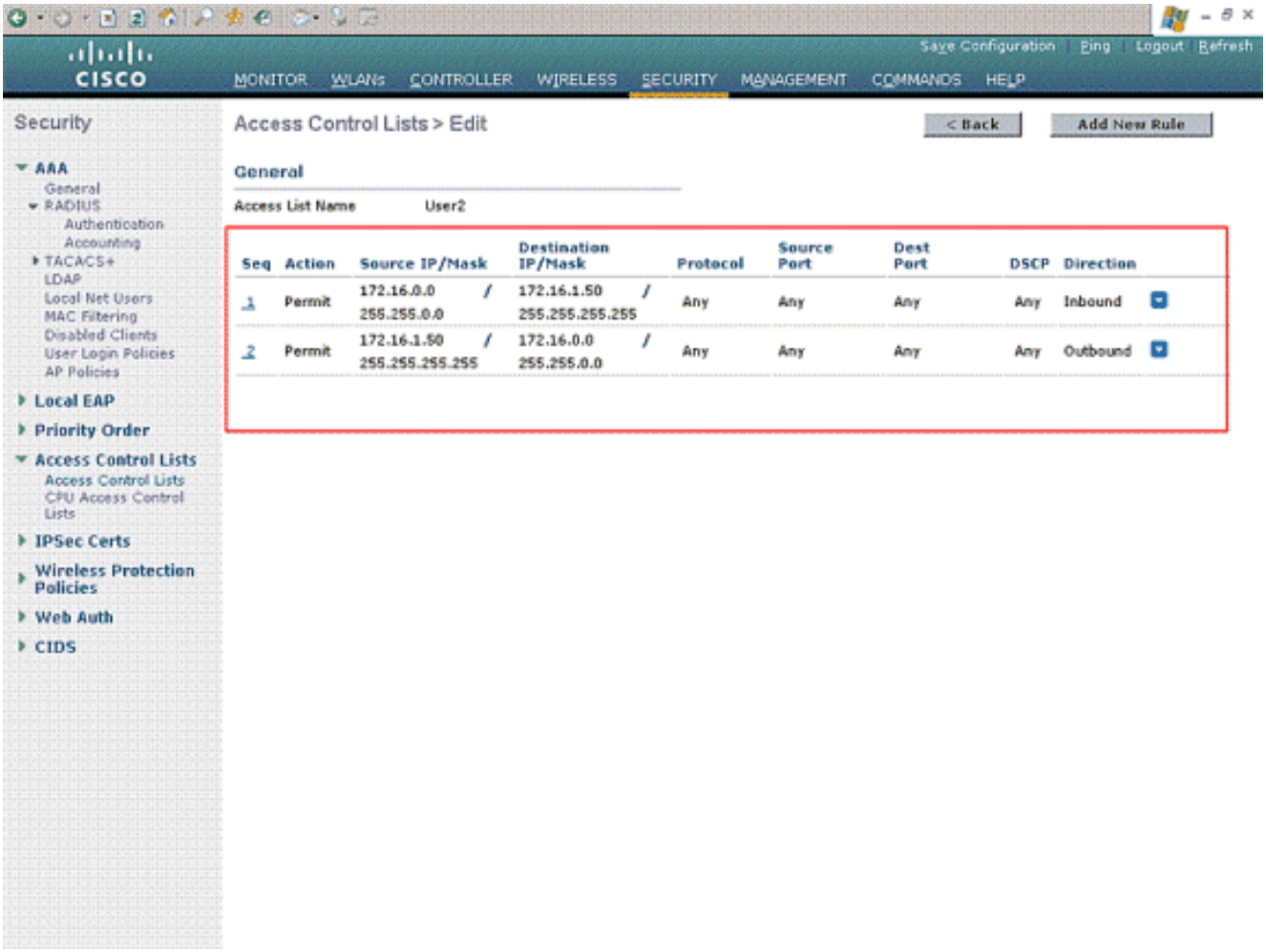
1. من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الوصول اللاسلكية (WLC)، أختر **الأمان > قوائم التحكم في الوصول**. تظهر صفحة قوائم التحكم في الوصول. تسرد هذه الصفحة قوائم التحكم في الوصول (ACL) التي تم تكوينها على عنصر التحكم في الوصول (WLC). كما يتيح لك تحرير أي من قوائم التحكم في الوصول (ACL) أو إزالته. لإنشاء قائمة تحكم في الوصول (ACL) جديدة، انقر فوق **جديد**.
2. تسمح لك هذه الصفحة بإنشاء قوائم التحكم في الوصول (ACL) جديدة. أدخل اسم قائمة التحكم في الوصول (ACL) وانقر فوق **تطبيق**. بمجرد إنشاء قائمة التحكم في الوصول (ACL)، انقر فوق **تحرير** لإنشاء قواعد

لقائمة التحكم في الوصول (ACL).

3. يجب أن يكون المستخدم1 قادرا على الوصول إلى الخادم 172.16.1.100 فقط ويجب رفضه من الوصول إلى جميع الأجهزة الأخرى. لهذا، تحتاج إلى تعريف هذه القواعد.راجع قوائم التحكم في الوصول (ACL) على مثال تكوين وحدة تحكم الشبكة المحلية اللاسلكية للحصول على مزيد من المعلومات حول كيفية تكوين قوائم التحكم في الوصول (ACL) على وحدات التحكم في الشبكة المحلية اللاسلكية.



4. وبالمثل، يلزمك إنشاء قائمة تحكم في الوصول (ACL) للمستخدم 2، والتي تتيح للمستخدم 2 إمكانية الوصول إلى الخادم 172.16.1.50 فقط. هذه هي قائمة التحكم في الوصول (ACL) المطلوبة للمستخدم 2.



لقد انتهيت الآن من تكوين وحدة التحكم في الشبكة المحلية اللاسلكية لهذا الإعداد. تتمثل الخطوة التالية في تكوين خادم التحكم في الوصول الآمن من Cisco لمصادقة العملاء اللاسلكي وإعادة سمة اسم قائمة التحكم في الوصول (ACL) إلى عنصر التحكم في الوصول الآمن (WLC) عند المصادقة الناجحة.

تكوين خادم ACS الآمن من Cisco

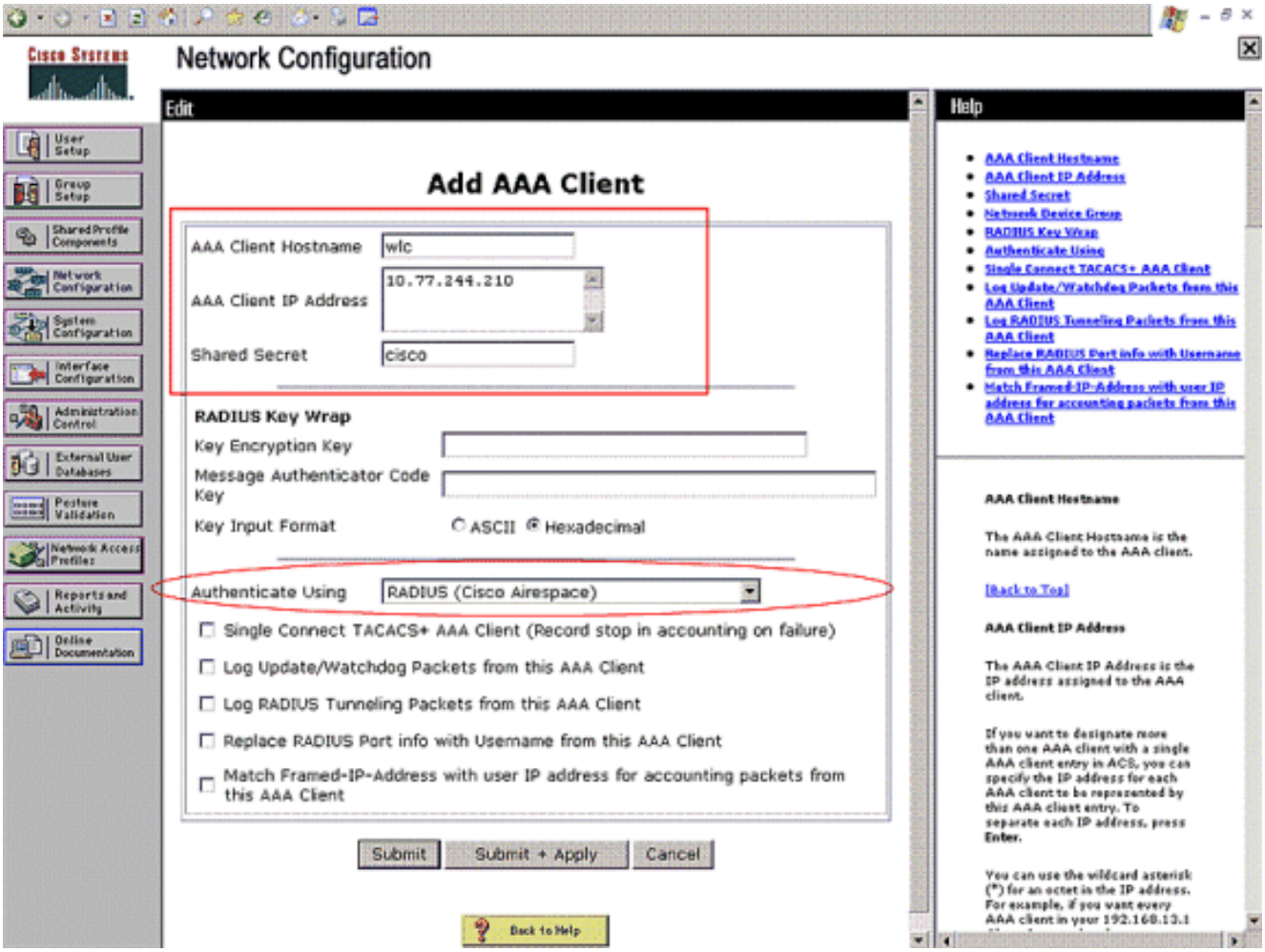
لكي يتمكن ACS الآمن من Cisco من مصادقة الأجهزة اللاسلكية العميلة، يلزمك استكمال الخطوات التالية:

- قم بتكوين وحدة التحكم في الشبكة المحلية اللاسلكية كعميل AAA على Cisco Secure ACS.
- قم بتكوين المستخدمين وملفات تعريف المستخدمين على ACS الآمن من Cisco.

تكوين وحدة التحكم في الشبكة المحلية اللاسلكية كعميل AAA على Cisco Secure ACS

لتكوين وحدة التحكم في الشبكة المحلية اللاسلكية كعميل AAA على Cisco ACS الآمن، أكمل الخطوات التالية:

1. انقر فوق **تكوين الشبكة > إضافة عميل AAA**. تظهر صفحة **إضافة عميل AAA**. في هذه الصفحة، قم بتعريف اسم نظام WLC وعنوان IP لواجهة الإدارة والسر المشترك والمصادقة باستخدام **Radius Airespace**. فيما يلي
مثال:



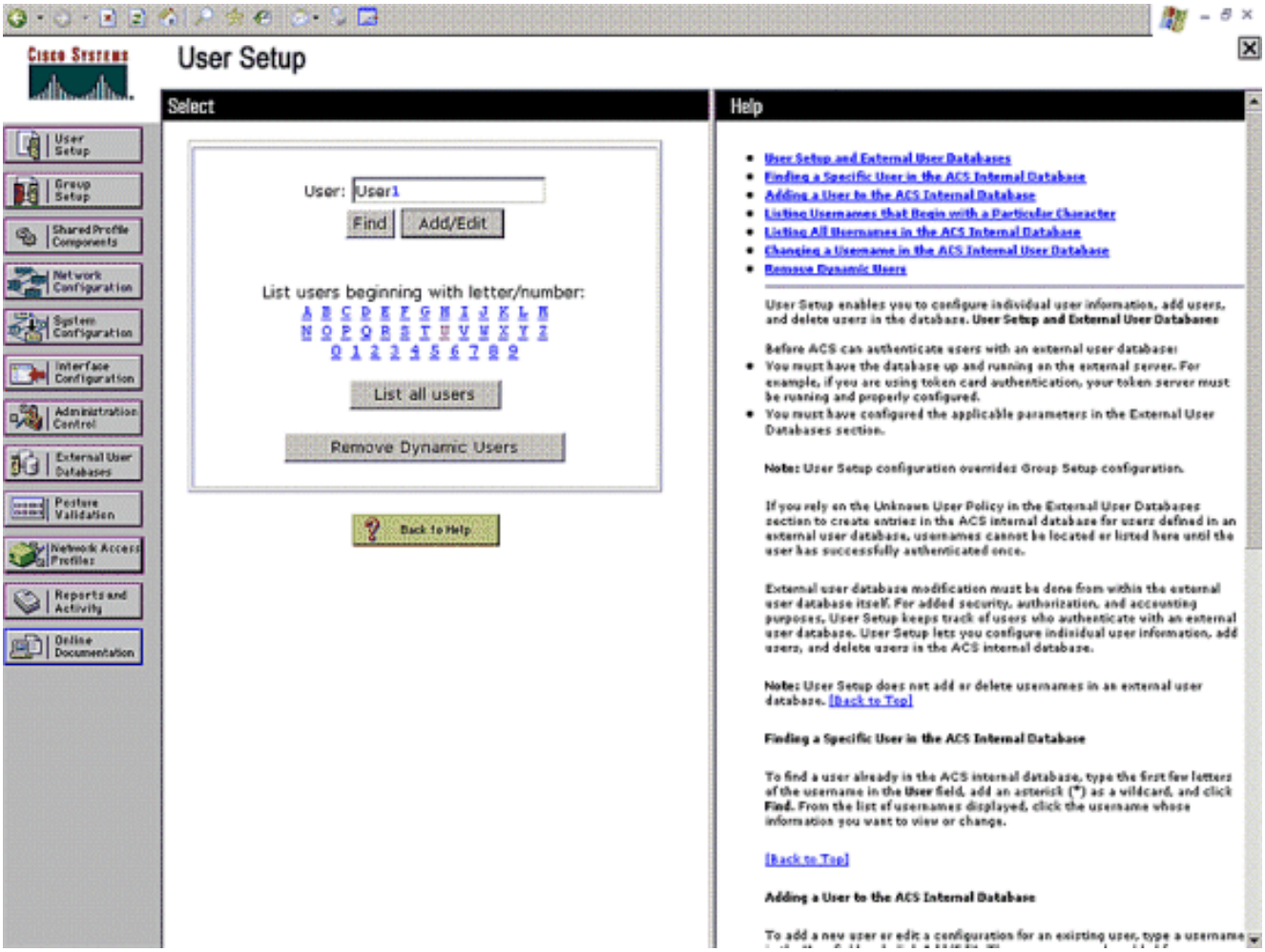
ملاحظة: يجب أن يتطابق السر المشترك الذي تم تكوينه على Cisco Secure ACS مع السر المشترك الذي تم تكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تحت **خوادم مصادقة RADIUS > جديد**.

2. انقر فوق **إرسال+تطبيق**.

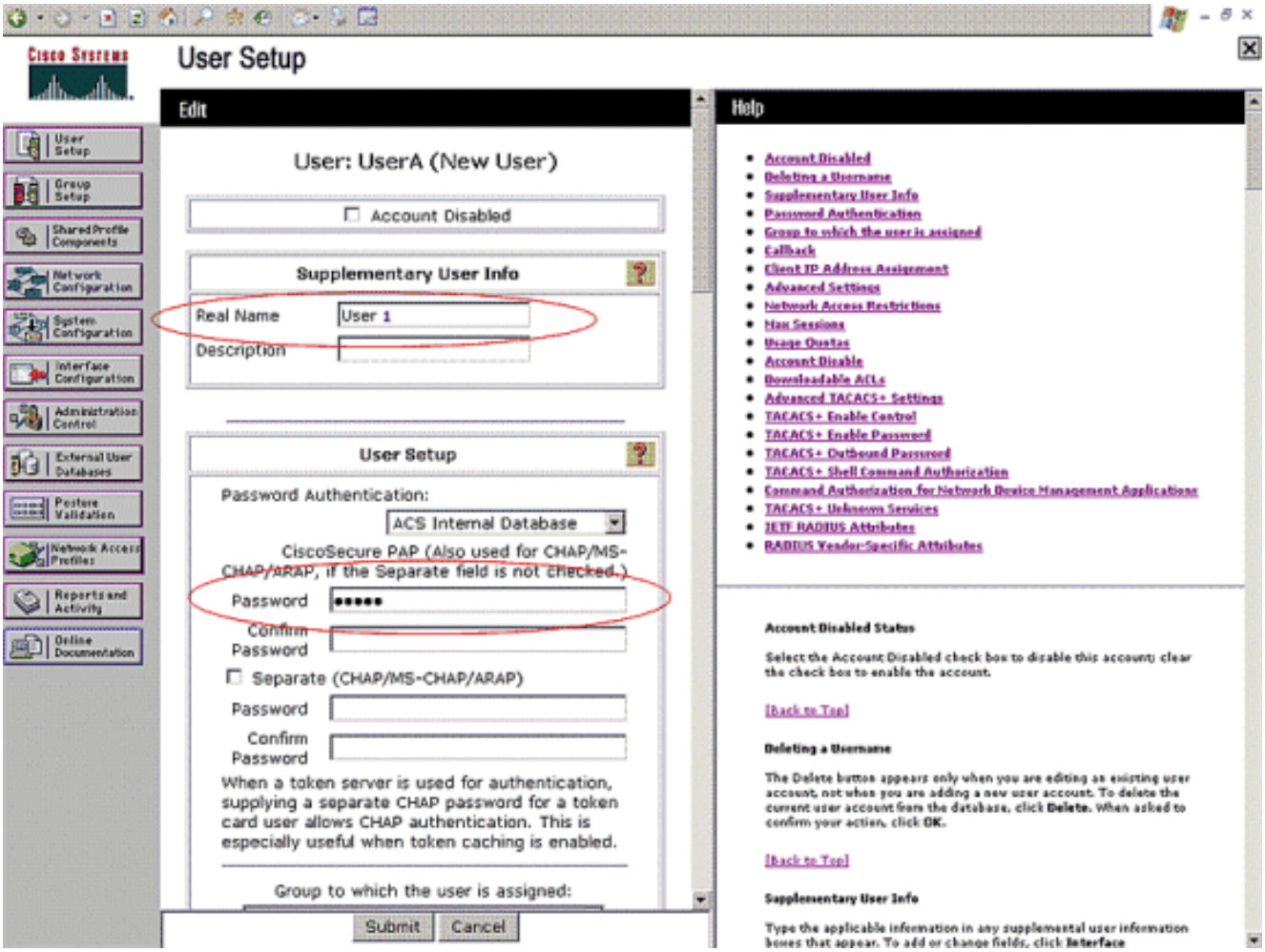
تكوين المستخدمين وملف تعريف المستخدم على ACS الآمن من Cisco

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

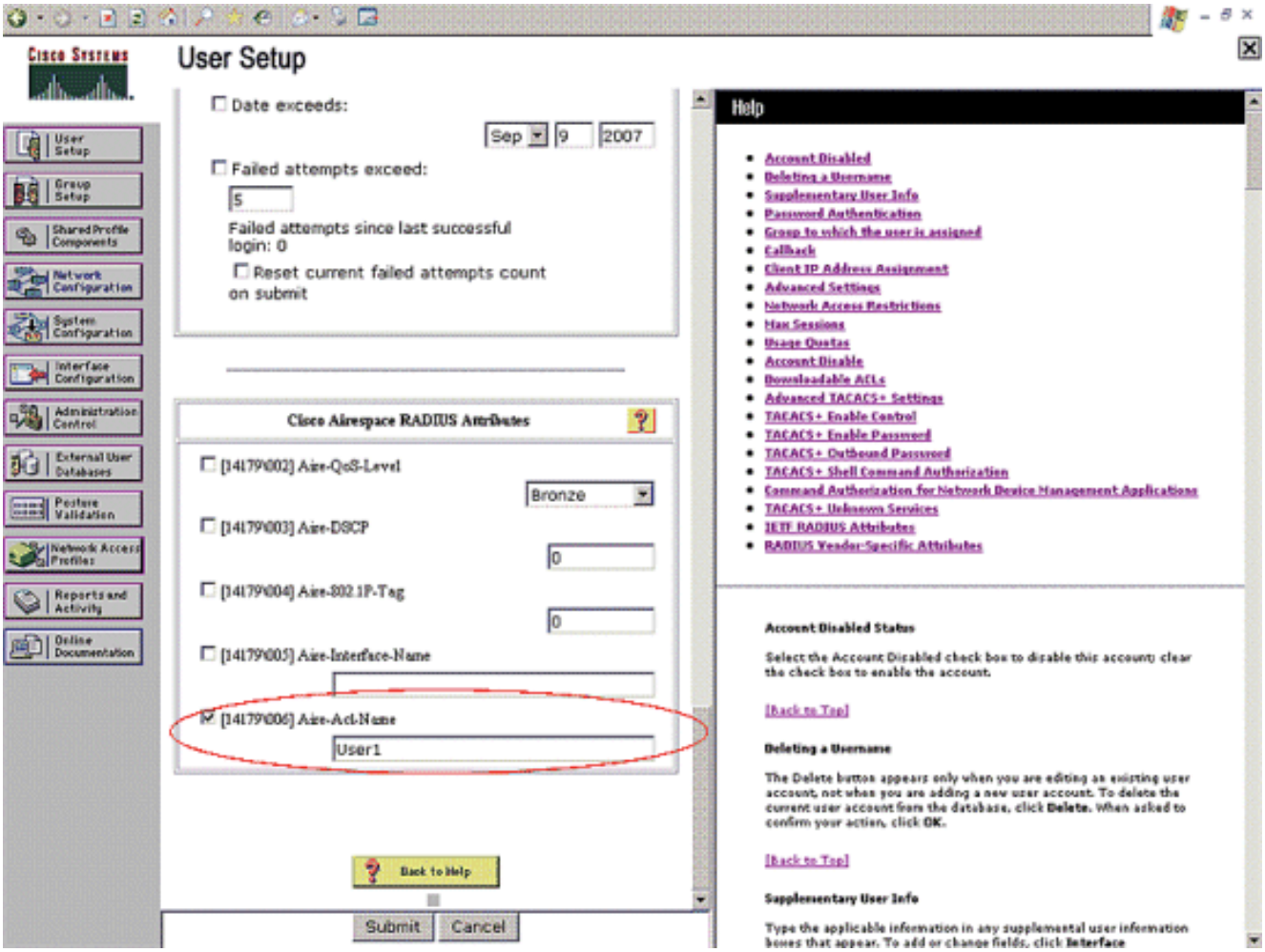
1. أخترت **مستعمل setup** من ال ACS gui، دخلت ال username، وطقطقة **يضيف/يحرر**. في هذا المثال، المستخدم هو **User1**.



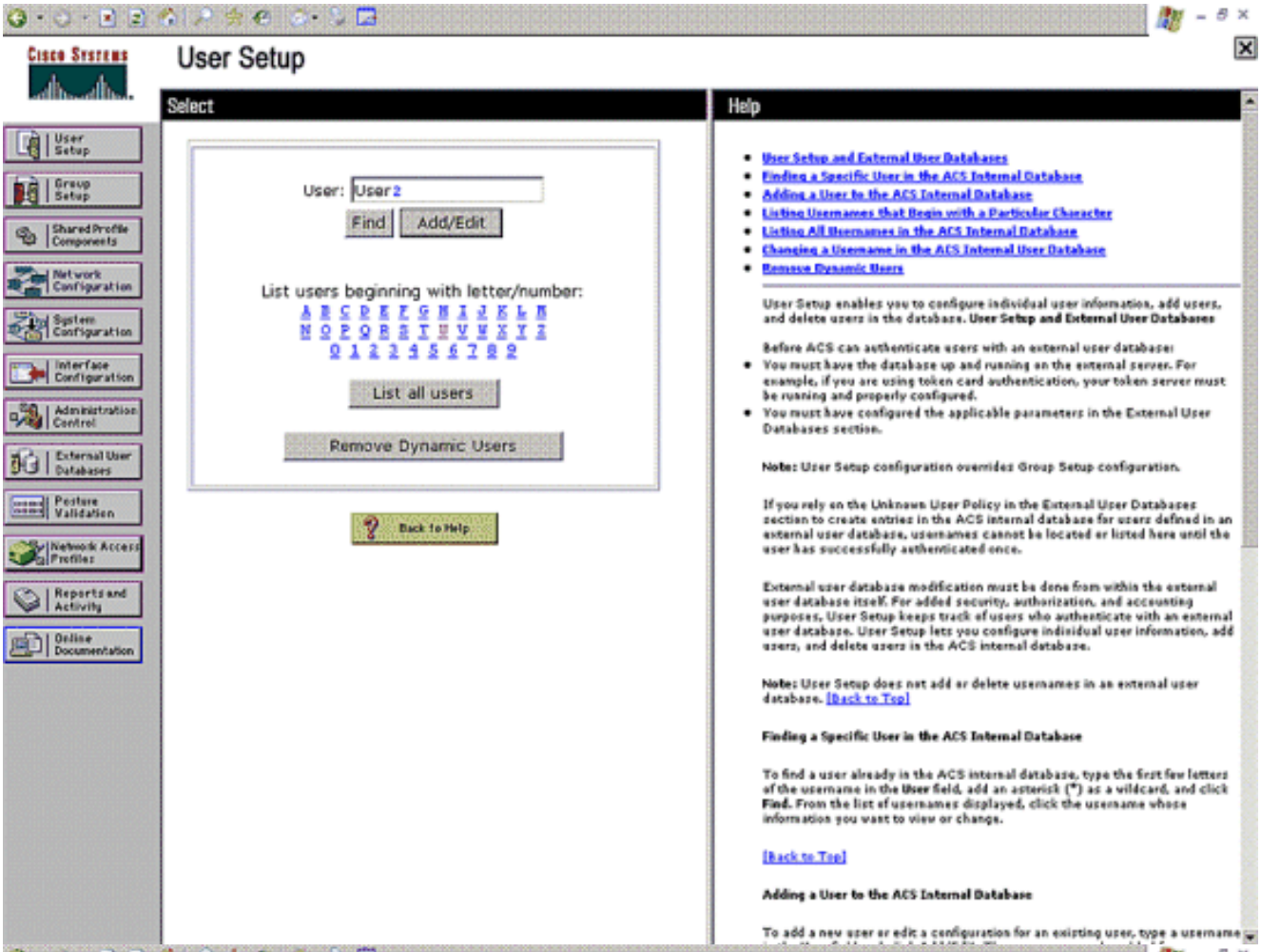
2. عندما تظهر صفحة **إعداد المستخدم**، قم بتعريف كافة المعلمات الخاصة بالمستخدم. في هذا المثال، يتم تكوين اسم المستخدم وكلمة المرور ومعلومات المستخدم التكميلية وسمات RADIUS لأنك تحتاج فقط إلى هذه المعلمات لمصادقة EAP.

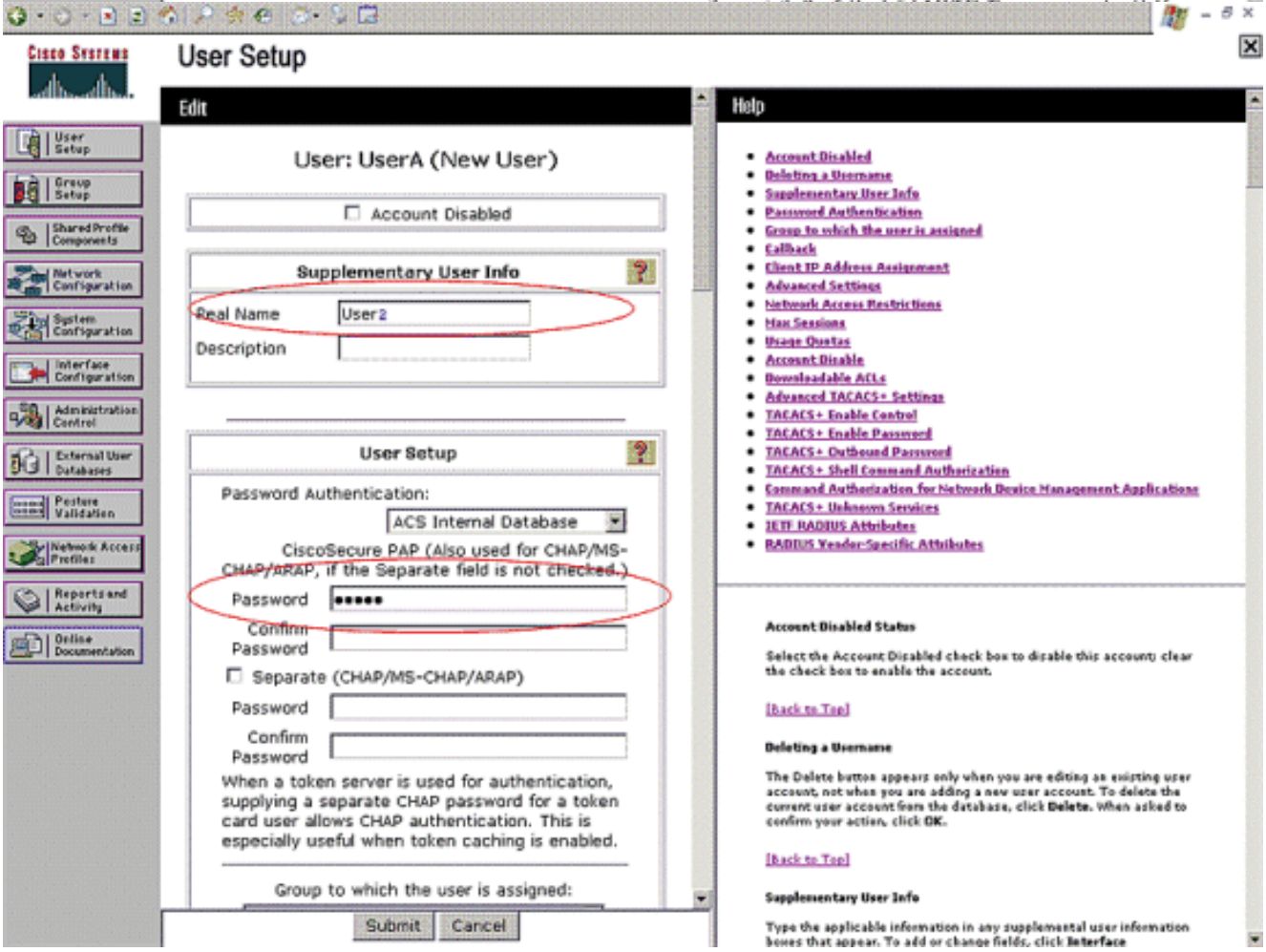


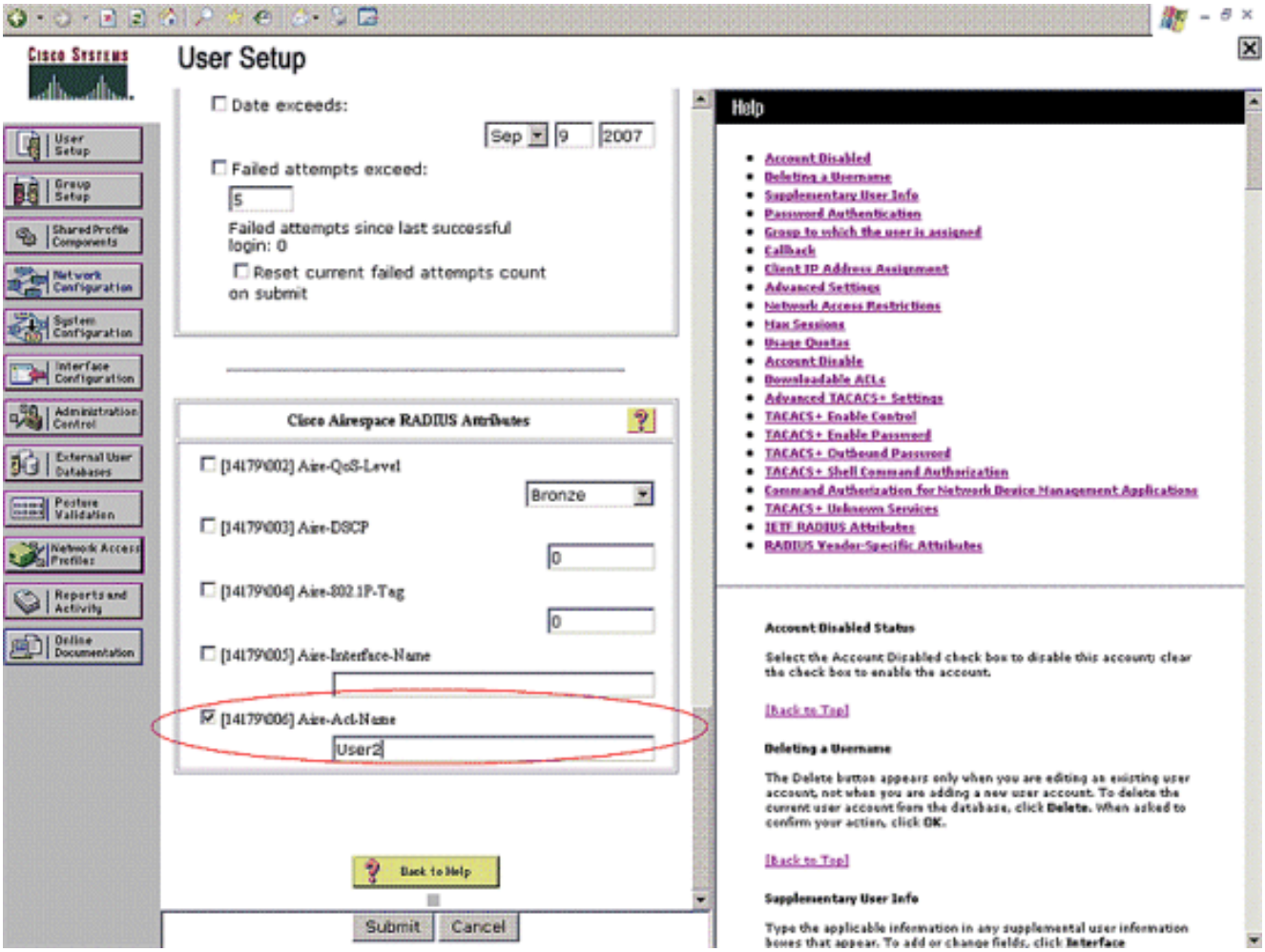
قم بالتمرير إلى أسفل حتى ترى سمات Cisco Airespace RADIUS الخاصة بالمستخدم. تحقق من **اسم قائمة التحكم في الوصول** (**AIRE-ACL**) لتمكين ACS لإعادة اسم قائمة التحكم في الوصول (ACL) إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مع إستجابة المصادقة الناجحة. بالنسبة للمستخدم 1، قم بإنشاء مستخدم قائمة تحكم في الوصول (1 (ACL على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). أدخل اسم قائمة التحكم في الوصول (ACL) ك User1.



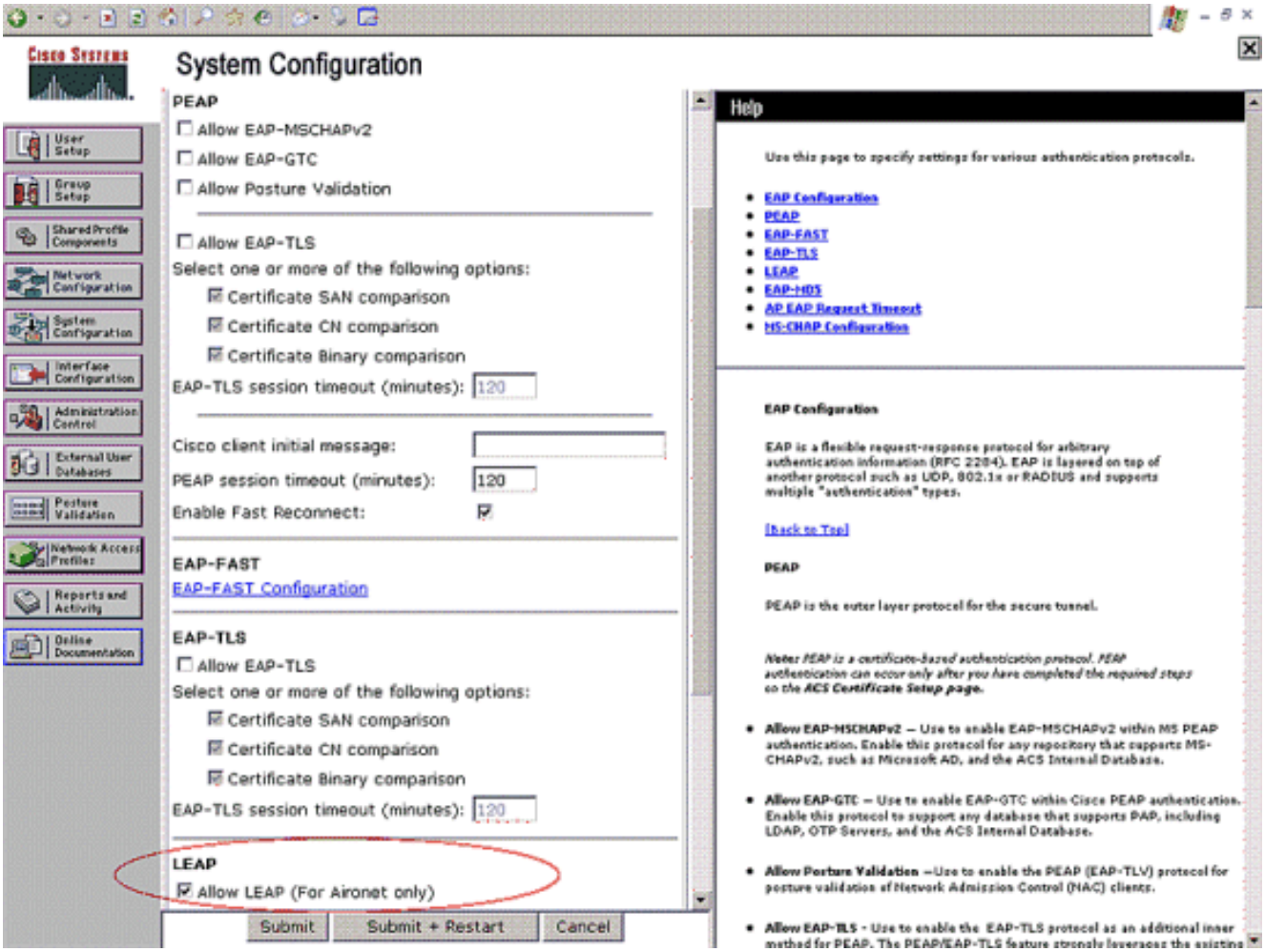
3. كرر نفس الإجراء لإنشاء User2 كما هو موضح هنا.


Cisco Systems
User Setup
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
Online Documentation
Select
User: User2
Find
Add/Edit
List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
List all users
Remove Dynamic Users
Back to Help
Help
User Setup and External User Databases
Finding a Specific User in the ACS Internal Database
Adding a User to the ACS Internal Database
Listing Usernames that Begin with a Particular Character
Listing All Usernames in the ACS Internal Database
Changing a Username in the ACS Internal User Database
Remove Dynamic Users
User Setup enables you to configure individual user information, add users, and delete users in the database. User Setup and External User Databases
Before ACS can authenticate users with an external user database:
You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
You must have configured the applicable parameters in the External User Databases section.
Note: User Setup configuration overrides Group Setup configuration.
If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.
External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.
Note: User Setup does not add or delete usernames in an external user database. [Back to Top]
Finding a Specific User in the ACS Internal Database
To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an asterisk (*) as a wildcard, and click Find. From the list of usernames displayed, click the username whose information you want to view or change.
[Back to Top]
Adding a User to the ACS Internal Database


Cisco Systems
User Setup
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
Online Documentation
Edit
User: UserA (New User)
Account Disabled
Supplementary User Info
Real Name
User2
Description
User Setup
Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Password
Confirm Password
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
Group to which the user is assigned:
Submit
Cancel
Help
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
IETF RADIUS Attributes
RADIUS Vendor-Specific Attributes
Account Disabled Status
Select the Account Disabled check box to disable this account; clear the check box to enable the account.
[Back to Top]
Deleting a Username
The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action, click OK.
[Back to Top]
Supplementary User Info
Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click Interface



4. انقر على **تكوين النظام** و**إعداد المصادقة العامة** لضمان تكوين خادم المصادقة لتنفيذ أسلوب مصادقة EAP المطلوب. تحت إعدادات تكوين EAP، أختر أسلوب EAP المناسب. يستخدم هذا المثال مصادقة LEAP. انقر فوق **إرسال** عند
الانتهاء.



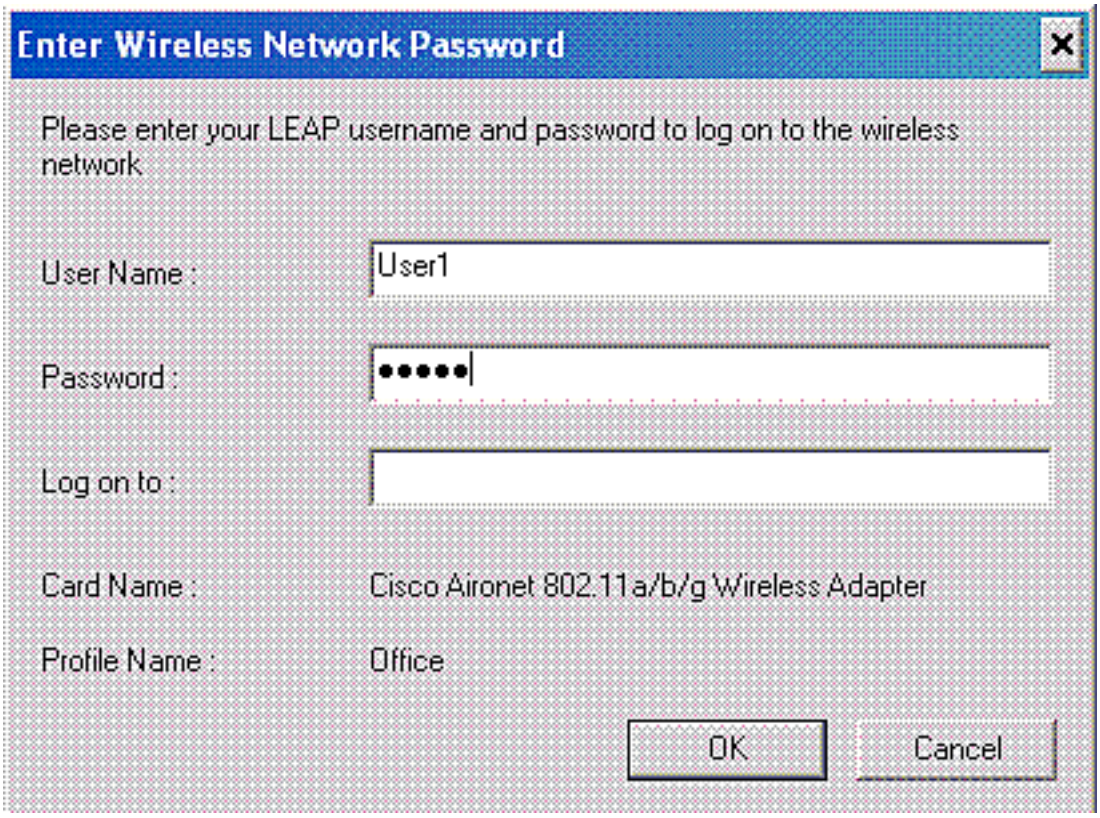
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

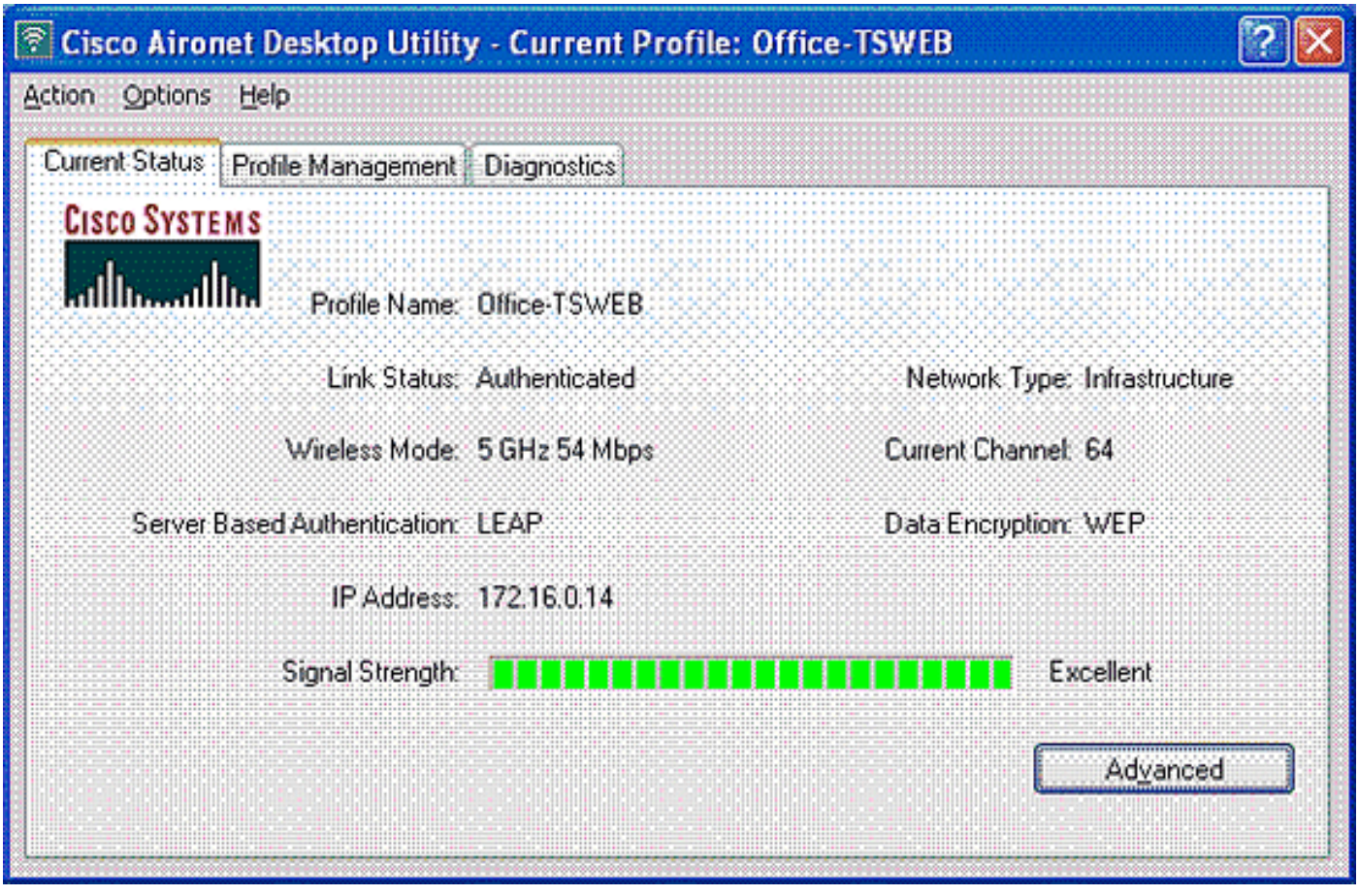
حاول إقران عميل لاسلكي مع نقطة الوصول في الوضع Lightweight مع مصادقة LEAP للتحقق مما إذا كان التكوين يعمل كما هو متوقع.

ملاحظة: يفترض هذا المستند تكوين ملف تعريف العميل لمصادقة LEAP. ارجع إلى إستخدام مصادقة EAP للحصول على مزيد من المعلومات حول كيفية تكوين مهايئ العميل اللاسلكي 802.11 a/b/g لمصادقة LEAP.

بمجرد تنشيط توصيف العميل اللاسلكي يطلب من المستخدم توفير اسم المستخدم/كلمة المرور لمصادقة LEAP. هذا ما يحدث عندما يحاول User1 المصادقة على نقطة الوصول في الوضع Lightweight (LAP).



تمرر نقطة الوصول في الوضع Lightweight ثم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بيانات اعتماد المستخدم إلى خادم RADIUS الخارجي (Cisco Secure ACS) للتحقق من بيانات الاعتماد. يقوم خادم RADIUS بمقارنة البيانات بقاعدة بيانات المستخدم، وبعد نجاح المصادقة، يرجع اسم قائمة التحكم في الوصول (ACL) الذي تم تكوينه للمستخدم إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). في هذه الحالة، يرجع قائمة التحكم في الوصول (ACL User1) إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

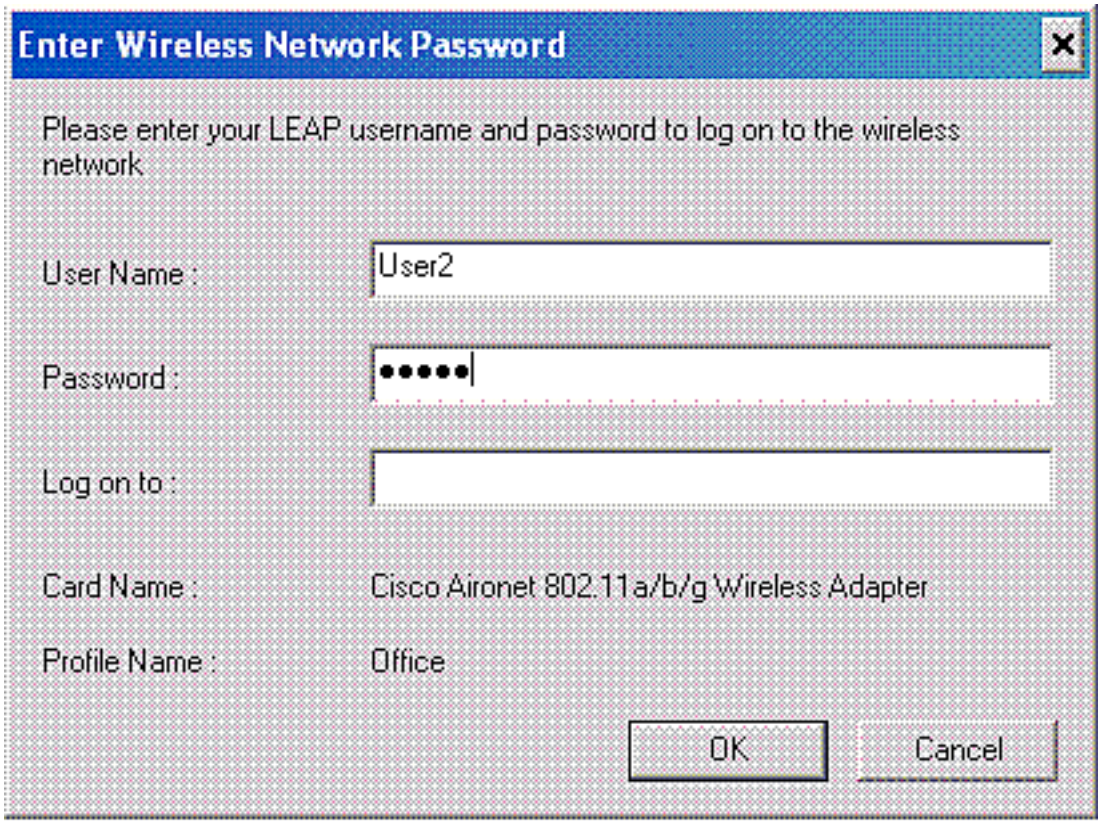


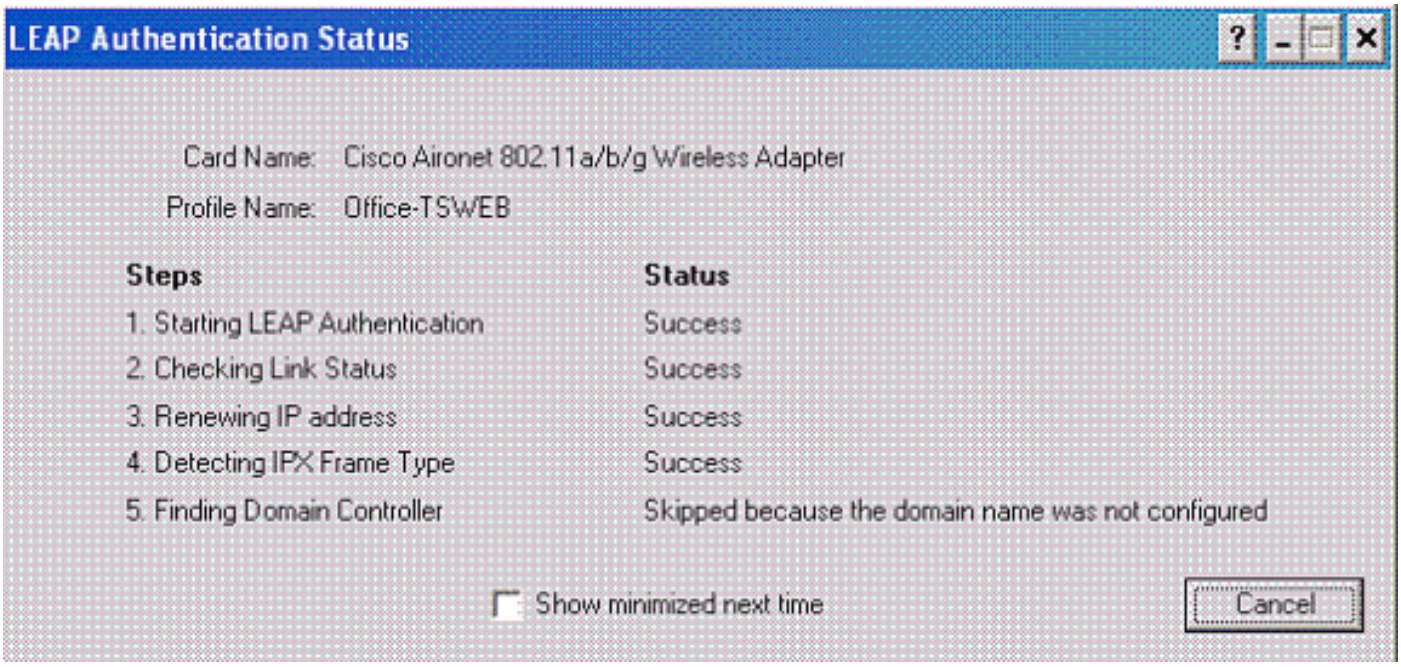
تقوم وحدة التحكم في الشبكة المحلية اللاسلكية بتطبيق قائمة التحكم في الوصول (ACL) هذه على المستخدم 1.

يوضح إخراج إختبار الاتصال هذا أن User1 قادر على الوصول إلى الخادم 172.16.1.100 فقط، وليس إلى أي جهاز آخر.

```
D:\Documents and Settings\Administrator>ping 172.16.1.100

:Pinging 172.16.1.100 with 32 bytes of data

Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255

:Ping statistics for 172.16.1.100
,(Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
:Approximate round trip times in milli-seconds
Minimum = 1ms, Maximum = 3ms, Average = 1ms

D:\Documents and Settings\Administrator>ping 172.16.1.50

:Pinging 172.16.1.50 with 32 bytes of data

.Request timed out
.Request timed out
.Request timed out
.Request timed out

:Ping statistics for 172.16.1.50
,(Packets: Sent = 4, Received = 0, Lost = 4 (100% loss
```

بالمثل، عندما يحاول User2 الوصول إلى الشبكة المحلية اللاسلكية (WLAN)، يرجع خادم RADIUS، عند المصادقة الناجحة، مستخدم ACL2 إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).





تقوم وحدة التحكم في الشبكة المحلية اللاسلكية بتطبيق قائمة التحكم في الوصول (ACL) هذه على المستخدم 2. يوضح إخراج إختبار الاتصال هذا أن User2 قادر على الوصول إلى الخادم 172.16.1.50 فقط، وليس إلى أي جهاز آخر.

```
D:\Documents and Settings\Administrator>ping 172.16.1.50

:Pinging 172.16.1.50 with 32 bytes of data

Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255

:Ping statistics for 172.16.1.50
,(Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
:Approximate round trip times in milli-seconds
Minimum = 1ms, Maximum = 18ms, Average = 5ms

D:\Documents and Settings\Administrator>ping 172.16.1.100

:Pinging 172.16.1.100 with 32 bytes of data

.Request timed out
.Request timed out
.Request timed out
.Request timed out

:Ping statistics for 172.16.1.100
,(Packets: Sent = 4, Received = 0, Lost = 4 (100% loss
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

على وحدة التحكم في الشبكة المحلية اللاسلكية، يمكنك أيضا إستخدام أوامر تصحيح الأخطاء هذه لاستكشاف أخطاء مصادقة AAA وإصلاحها

- **debug aaa all enable**—يشكل تصحيح أخطاء جميع رسائل AAA
- **debug dot1x ربط enable**— يمكن ال debug لكل ربط dot1x
- **تصحيح أخطاء العميل <MAC Address>**—تمكين تصحيح أخطاء العميل اللاسلكي

هنا مثال من **ال debug aaa all enable** أمر

ملاحظة: تم نقل بعض البنود في الناتج إلى السطر الثاني بسبب قيود المساحة.

```
                    Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
                  Thu Aug 16 14:42:54 2007:       Callback.................0x85ed228
                Thu Aug 16 14:42:54 2007:       protocolType.............0x00140001
      Thu Aug 16 14:42:54 2007:       proxyState..............00:40:96:AF:3E:93-03:01
                (Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown
                                     Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
                                   Successful transmission of Authentication Packet
                id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00)
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99  b4 19 27 28 eb 5f 35 9c
                                                                    .5_.)'....-4....
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73  65 72 31 1f 13 30 30 2d
                                                                    user1..00-......
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
                                                                    ..40-96-AF-3E-93
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
                                                                    00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
                                                                    ..Office-TSWEB:0
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
                                                                    .M....wlc.......
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
                                                                    ...........7c...
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
                                                                    ..@.....=.......
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 27 02
                                                                    .'A.....Q.20O...
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d  87 9d 0b f9 dd e5 39 0d
                                                                    .9..........%..
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96  dc c3 55 ff 7c 51 4e 75
                                                                    U.|QNu....#.....
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
                                                                    .ser1..SVC=0.1;P
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0  c6 2f 5e f5 65 e9 3e 2d
                                                                    -<.e.^/....^5;..
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4  27 e6 d4 0e 1b 8e 5d 19
                                                                    .[.....'.6.1j...
Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01  00 04 18 0a 53 56 43 3d
                                                                     =O.......SVC...
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb  90 ec 48 9b fb d7 ce ca
                                                                    .....P.l...H;0.1
                    ....Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09      ;d
          Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11
            Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11
                                     Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
                                   Access-Challenge received from RADIUS server
                              for mobile 00:40:96:af:3e:93 receiveId = 3 10.77.244.196
                            Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
                          Thu Aug 16 14:42:54 2007:       structureSize............104
                          Thu Aug 16 14:42:54 2007:       resultCode..............255
                  Thu Aug 16 14:42:54 2007:       protocolUsed............0x00000001
                           ..............Thu Aug 16 14:42:54 2007:       proxyState
                                                  AF:3E:93-03:01:00:40:96
                  (Thu Aug 16 14:42:54 2007:       Packet contains 3 AVPs (not shown
```

```
                        Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
                  Thu Aug 16 14:42:54 2007:       Callback.................0x85ed228
                  Thu Aug 16 14:42:54 2007:       protocolType.............0x00140001
                 ........................Thu Aug 16 14:42:54 2007:       proxyState
                                                        AF:3E:93-03:02:00:40:96
                 (Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown
                                      Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
      ,Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812
                                                    proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20  ff 5b f2 16 64 df 02 61
                                                                d..a..]....8....
Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73  65 72 31 1f 13 30 30 2d
                                                                K..User1..00-...
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
                                                                ..40-96-AF-3E-93
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
                                                                00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
                                                                    ..Office:0
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
                                                                .M.... wlc.....
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
                                                                ...........7c...
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
                                                                ..@.....=.......
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 17 01
                                                                ..A.....Q.20O...
Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f  14 05 65 1b 28 61 c9 75
                                                                e.(a.u..........
Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
                                                                .ser1..SVC=0.1;P
Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1  a2 94 f8 39 80 ca 3c 96
                                                                .>..k........9..
Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8  6c 07 8e fb 58 84 8d f6
                                                                ...l...X.[=.....
Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff  ff ff 4f 27 02 01 00 25
                                                                %...'3m.!......O
Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e  33 b5 4e 69 90 e7 84 25
                                                                %...Ni.1.3......
Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87  ca dc c9 b3 75 73 65 72
                                                                B....3......user
Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01  35 6c 65 61 70 3a 73 65
                                                                5leap:se.....;.1
Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65  79 3d 29 80 1d 2c 1c 85
                                                                ..,..(=ssion-key
Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93  69 2a 55 d2 e5 46 89 8b
                                                                ..i*U..F...@~(..
Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e  95 29 47 54 1a 1f 00 00
                                                                ....eI>D.~.)GT;,
Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68  2d 61 6c 67 6f 2d 74 79
                                                                auth-algo-ty....
Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c  65 61 70 1a 0d 00 00 37
                                                                pe=eap-leap....7
Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31  19 14 43 41 43 53 3a 30
                                                                c..User1..CACS:0
Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34  64 32 2f 31 50 12 9a 71
                                                                a4df4d2/1P..q/9/
      Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5  c8 b1 71 94 97 d1
                                                                  ...t......q{..
        Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2
          Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2
                                      Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
                                        Access-Accept received from RADIUS server
                                for mobile 00:40:96:af:3e:93 receiveId = 3 10.77.244.196
```

```
                                Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
                              Thu Aug 16 14:42:54 2007:       structureSize............236
                                Thu Aug 16 14:42:54 2007:       resultCode.....0
                              Thu Aug 16 14:42:54 2007:       protocolUsed.....0x0
                                                                              0000001
                              :Thu Aug 16 14:42:54 2007:       proxyState.....00
                                                                      AF:3E:93-03:02:40:96
                                          :Thu Aug 16 14:42:54 2007:  Packet contains 6 AVPs
   (Thu Aug 16 14:42:54 2007:  AVP[01] Framed-IP-Address.....0xffffffff (-1
                                                                        (bytes 4)
   (Thu Aug 16 14:42:54 2007:  AVP[02] EAP-Message.....DATA (37 bytes
   (Thu Aug 16 14:42:54 2007:  AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes
   (Thu Aug 16 14:42:54 2007:  AVP[04] Airespace / ACL-Name.....User1 (5 bytes
Thu Aug 16 14:42:54 2007:  AVP[05] Class.....CACS:0/9/a4df4d2/1
                                                                        (bytes 18)
   (Thu Aug 16 14:42:54 2007:  AVP[06] Message-Authenticator.....DATA (16 bytes
          Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override
                                                for station 00:40:96:af:3e:93
                        Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values
                                                for station 00:40:96:af:3e:93
                                      source: 4, valid bits: 0x400
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

                           dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
          ,'' :vlanIfName
                                                                      aclName:User1
                                        Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
    Inserting new RADIUS override into chain for station 00:40:96:af:3e:93
```

يمكنك إستخدام مجموعة من الأمر **show wlan summary** للتعرف علي أي من شبكات WLAN تستخدم مصادقة خادم RADIUS. ثم يمكنك عرض الأمر **show client summary** لترى أي عناوين MAC (العملاء) تتم مصادقتها بنجاح على شبكات WLAN RADIUS. يمكنك أيضا ربط هذا مع Cisco Secure ACS يمر بمحاولات أو محاولات فاشلة سجل.

توصي Cisco باختبار تكوينات قائمة التحكم في الوصول (ACL) باستخدام عميل لاسلكي لضمان تكوينها بشكل صحيح. إذا فشلت في العمل بشكل صحيح، فتحقق من قوائم التحكم في الوصول (ACL) على صفحة ويب قائمة التحكم في الوصول والتحقق من تطبيق تغييرات قائمة التحكم في الوصول (ACL) على واجهة وحدة التحكم.

أنت يستطيع أيضا استعملت هذا عرض أمر in order to دققت تشكيلك:

- **show acl summary** — لعرض قوائم التحكم في الوصول (ACL) التي تم تكوينها على وحدة التحكم، أستخدم الأمر **show acl summary**.

فيما يلي مثال:

```
Cisco Controller) >show acl summary)

ACL Name                                 Applied
------- ---------------------------------
User1                                    Yes
User2                                    Yes
```

- **إظهار قائمة التحكم في الوصول (ACL) التفصيلية** <ACL_Name> — يعرض معلومات تفصيلية حول قوائم التحكم في الوصول (ACL) التي تم تكوينها.فيما يلي مثال:**ملاحظة:** تم نقل بعض البنود في الناتج إلى السطر الثاني بسبب قيود المساحة.

```
Cisco Controller) >show acl detailed User1
```

```
                Source                      Destination
                                                Source Port   Dest Port
       I  Dir       IP Address/Netmask              IP Address/Netmask
                          Prot    Range       Range    DSCP   Action
------------------------------ ------------------------------ --- --
                              ------    ---- ----------- ----------- ----
In      172.16.0.0/255.255.0.0        172.16.1.100/255.255.255.255  1
                          Any  0-65535       0-65535   Any    Permit
    Out    172.16.1.100/255.255.255.255      172.16.0.0/255.255.0.0 2
                          Any  0-65535       0-65535   Any    Permit


                            Cisco Controller) >show acl detailed User2)

                Source                      Destination
                                                Source Port   Dest Port
       I  Dir       IP Address/Netmask              IP Address/Netmask
                          Prot    Range       Range    DSCP Action
------------------------------ ------------------------------ --- --
                              ------ ---- ----------- ----------- ----
 In      172.16.0.0/255.255.0.0         172.16.1.50/255.255.255.255  1
                          Any   0-65535       0-65535    Any  Permit
     Out     172.16.1.50/255.255.255.255      172.16.0.0/255.255.0.0 2
                          Any   0-65535       0-65535    Any  Permit
```

- **إظهار تفاصيل العميل** <MAC Address الخاص بالعميل> - يعرض معلومات تفصيلية حول العميل اللاسلكي.

تلميحات استكشاف المشكلات وإصلاحها

استعملت هذا طرف أن يتحرى:

- تحقق من وحدة التحكم أن خادم RADIUS في حالة نشطة، وليس في وضع الاستعداد أو معطل.
- على وحدة التحكم، تحقق مما إذا تم إختيار خادم RADIUS من القائمة المنسدلة للشبكة المحلية اللاسلكية (WLAN) (SSID).
- تحقق 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.

معلومات ذات صلة

- قوائم التحكم في الوصول على وحدات التحكم في الشبكة المحلية اللاسلكية: القواعد والحدود والأمثلة
- مثال على تكوين ACL على وحدة تحكّم الشبكة المحلية اللاسلكية
- مثال على تكوين عوامل تصفية MAC المزوّدة بوحدات التحكّم في شبكة LAN اللاسلكية (WLC)
- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 5.2
- 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).