مثال تكوين خادم Cisco Airespace VSAs على Microsoft IAS RADIUS Server

المحتويات

المقدمة

يبدي هذا وثيقة أنت كيف أن يشكل Microsoft إنترنت صحة هوية خدمة (IAS) نادل أن يساند cisco Airespace بائع شعار خاص (VSAs). كود المورد ل **14179** Cisco Airespace VSAs.

المتطلبات الأساسية

المتطلبات

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

- معرفة كيفية تكوين خادم IAS
- معرفة تكوين نقاط الوصول في الوضع Lightweight (LAPs) ووحدات التحكم في الشبكة المحلية (LAN) اللاسلكية من Cisco (WLCs)
- معرفة حلول الأمان اللاسلكية الموحدة من Cisco

المكونات المستخدمة

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

- خادم Microsoft Windows 2000 مع IAS
- Cisco 4400 WLC أن يركض برمجية صيغة 4.0.206.0

- نقاط الوصول في الوضع Cisco 1000 Series LAPs
- مهايئ عميل لاسلكي 802.11 a/b/g مع برنامج ثابت 2.5
- Aironet Desktop Utility (ADU)، الإصدار 2.5

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.

ملاحظة: يهدف هذا المستند إلى إعطاء القارئ مثالا على التكوين المطلوب على خادم IAS لدعم Cisco Airespace VSAs. تم إختبار تكوين خادم IAS المقدم في هذا المستند في المعمل ويعمل كما هو متوقع. إذا واجهت مشكلة في تكوين خادم IAS، فاتصل ب Microsoft للحصول على تعليمات. لا يدعم Cisco TAC تكوين Microsoft Windows Server.

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 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 LAP) Lightweight) إلى وحدة تحكم شبكة LAN لاسلكية (WLC).

الاصطلاحات

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

معلومات أساسية

في معظم أنظمة الشبكة المحلية اللاسلكية (WLAN)، تحتوي كل شبكة محلية لاسلكية (WLAN) على سياسة ثابتة تنطبق على جميع العملاء المرتبطين بمعرف مجموعة الخدمة (SSID). وعلى الرغم من أنها فعالة، إلا أن هذه الطريقة لها قيود لأنها تتطلب من العملاء الاقتران ب SSIDs مختلفة لوراثة جودة الخدمة (QoS) ونهج الأمان المختلفة.

ومع ذلك، يدعم حل شبكة LAN اللاسلكية من Cisco شبكات الهوية، والتي تسمح للشبكة بالإعلان عن معرف خدمة (SSID) واحد ومستخدمين معينين لوراثة جودة الخدمة (QoS) المختلفة أو سياسات الأمان استنادا إلى ملفات تعريف المستخدمين الخاصة بهم. وتتضمن السياسات المحددة التي يمكنك التحكم فيها باستخدام شبكات الهوية ما يلي:

- **جودة الخدمة**- عند وجودها في "قبول الوصول إلى RADIUS"، تتخطى قيمة مستوى جودة الخدمة قيمة جودة الخدمة المحددة في ملف تعريف WLAN.
- **ACL**—عندما تكون سمة قائمة التحكم في الوصول (ACL) موجودة في قبول الوصول إلى RADIUS، يقوم النظام بتطبيق اسم قائمة التحكم في الوصول (ACL) على محطة العميل بعد مصادقته. يتخطى هذا الإجراء أي قوائم تحكم في الوصول (ACL) يتم تعيينها إلى الواجهة.
- **VLAN**— عندما يكون اسم واجهة شبكة VLAN أو VLAN-Tag موجودا في "قبول الوصول إلى RADIUS"، يضع النظام العميل على واجهة معينة.
- **معرف WLAN**—عندما تكون سمة معرف الشبكة المحلية اللاسلكية (WLAN) موجودة في "قبول الوصول إلى RADIUS"، يقوم النظام بتطبيق معرف الشبكة المحلية اللاسلكية (SSID) (WLAN) على محطة العميل بعد مصادقته. يتم إرسال معرف شبكة WLAN بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في جميع مثيلات المصادقة باستثناء IPSec. في حالة مصادقة الويب، إذا تلقت وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) سمة معرف الشبكة المحلية اللاسلكية (WLAN) في إستجابة المصادقة من خادم AAA، ولم تطابق معرف شبكة WLAN، يتم رفض المصادقة. لا تقوم أنواع أخرى من طرق الأمان بذلك.
- **قيمة DSCP**- عندما تكون موجودة في قبول الوصول إلى RADIUS، تتجاوز قيمة DSCP قيمة DSCP المحددة في ملف تعريف WLAN.
- **802.1p-tag**—عندما تكون موجودة في "قبول الوصول إلى RADIUS"، تتجاوز قيمة 802.1p القيمة الافتراضية

المحددة في ملف تعريف WLAN.

ملاحظة: تدعم ميزة شبكة VLAN تصفية MAC، و 802.1X، و WPA (Wi-Fi Protected Access) فقط. لا تدعم ميزة شبكة VLAN مصادقة الويب أو IPSec. تم توسيع قاعدة بيانات عامل تصفية MAC المحلي لنظام التشغيل لتضمين اسم الواجهة. وهذا يسمح لعوامل تصفية MAC المحلية بتحديد الواجهة التي يجب تعيين العميل لها. كما يمكن إستخدام خادم RADIUS منفصل، ولكن يجب تعريف خادم RADIUS باستخدام قوائم الأمان.

راجع تكوين شبكة الهوية للحصول على مزيد من المعلومات حول شبكات الهوية.

شكلت ال IAS ل Airespace VSAs

in order to شكلت ال IAS ل Airespace VSAs، أنت تحتاج أن يتم هذا steps:

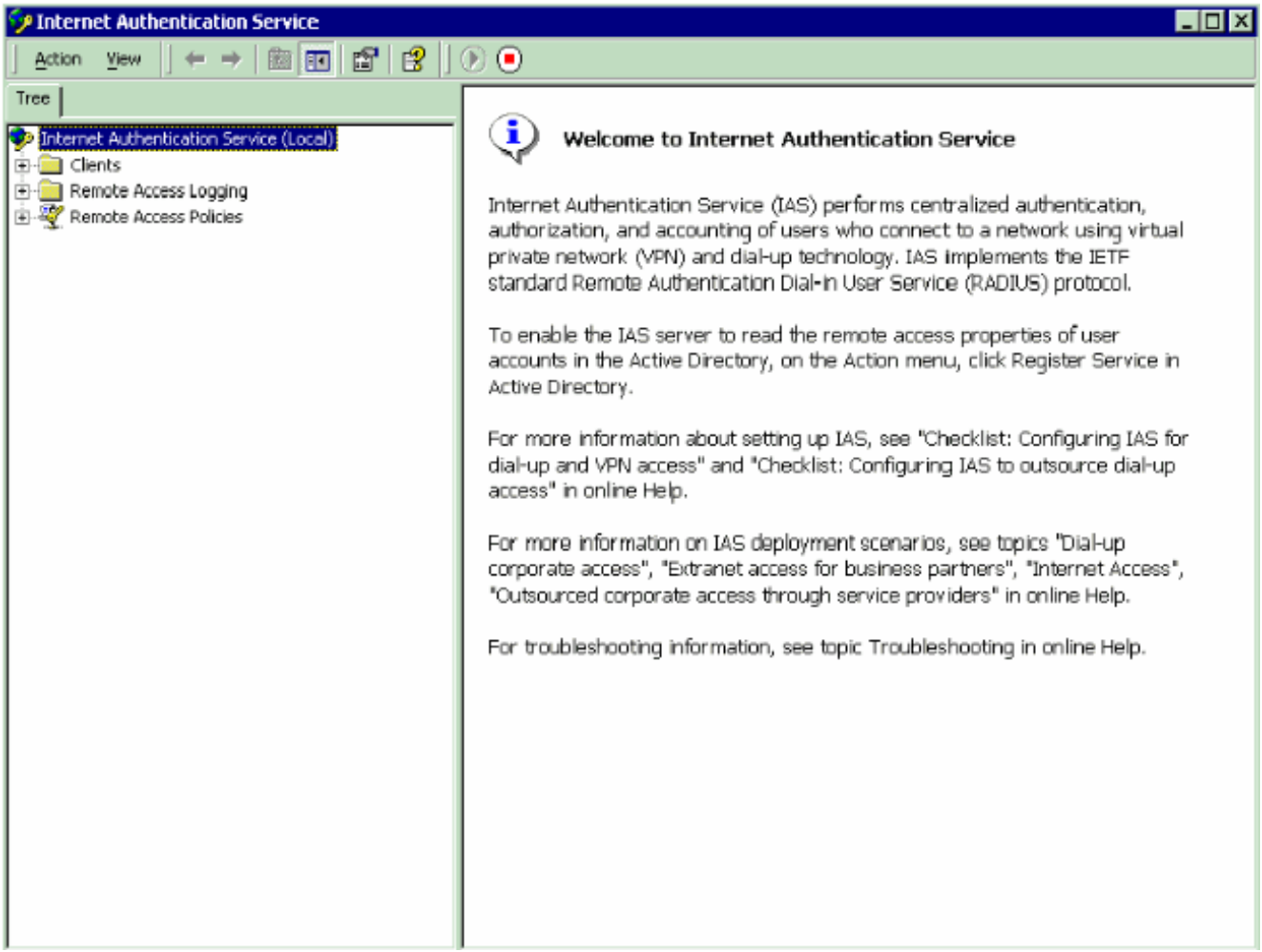
1. تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA على IAS
2. تكوين نهج الوصول عن بعد على IAS

ملاحظة: يتم تكوين شبكات VSA بموجب نهج الوصول عن بعد.

تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA على IAS

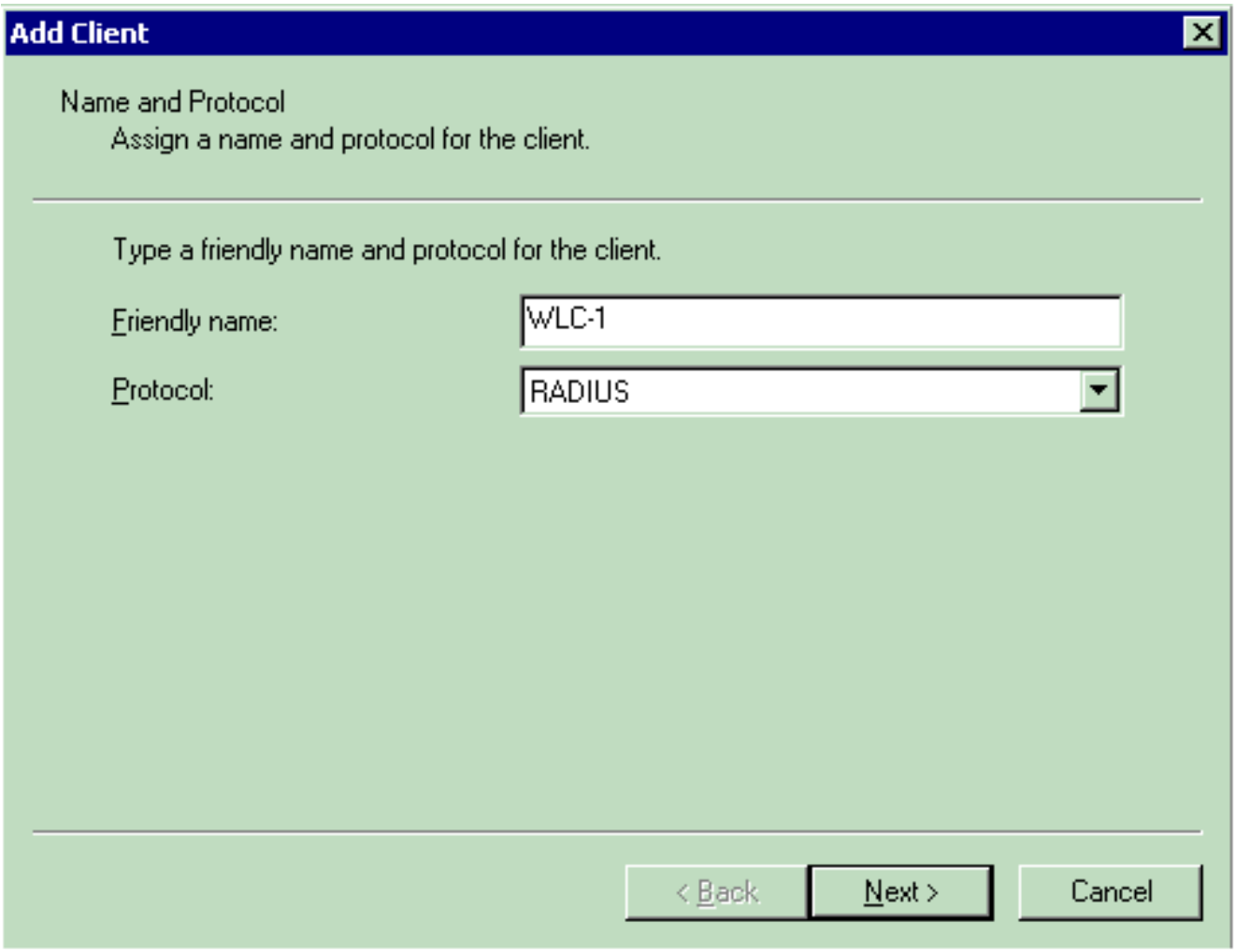
أتمت هذا steps in order to شكلت ال WLC كعميل AAA على ال IAS:

1. انقر على **برامج > أدوات إدارية > خدمة مصادقة الإنترنت** لتشغيل IAS على خادم Microsoft 2000.

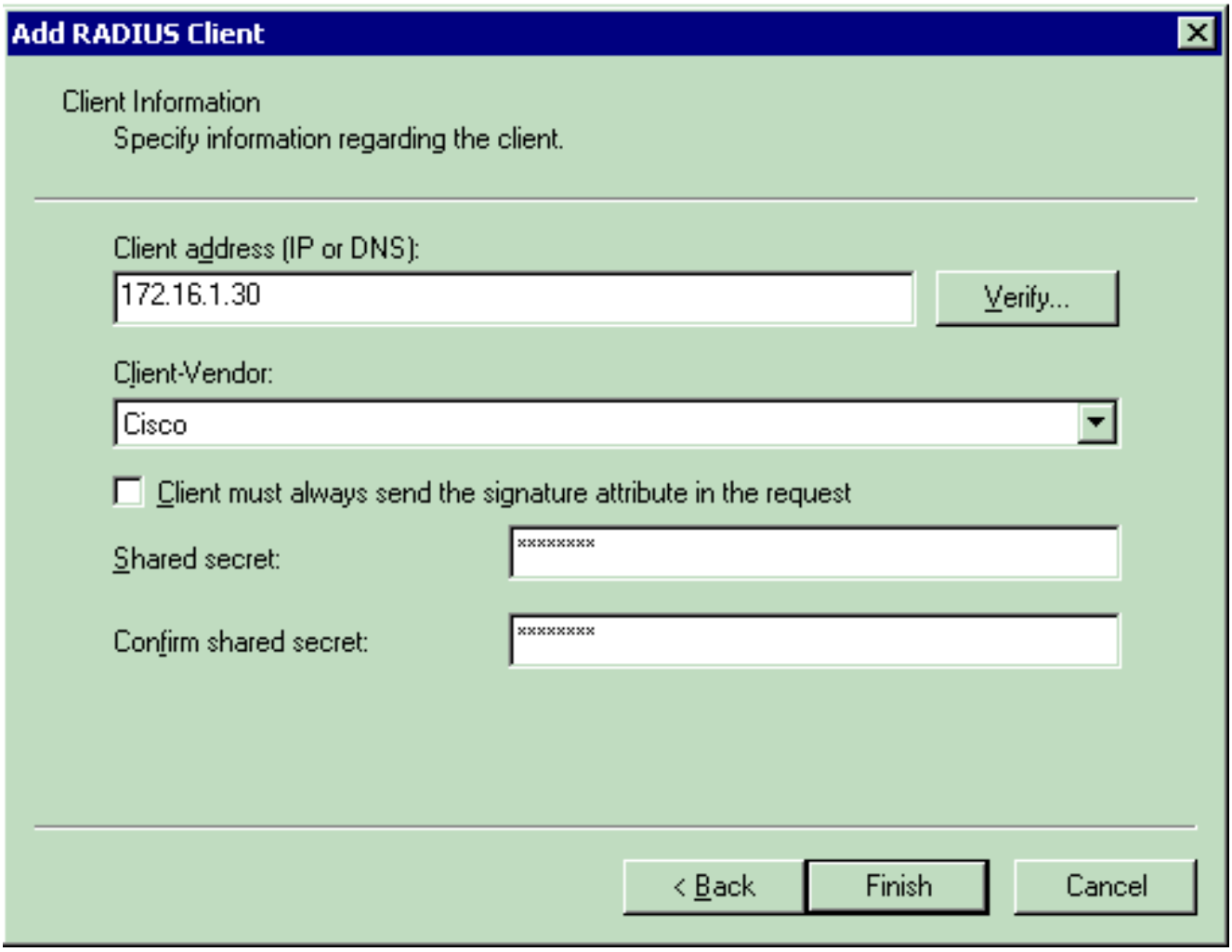


2. انقر بزر الماوس الأيمن فوق المجلد **العملاء** واختر **عميل جديد** لإضافة عميل RADIUS جديد.
3. في نافذة "إضافة عميل"، أدخل اسم العميل واختر **RADIUS** كبروتوكول. ثم انقر فوق **التالي**.في هذا المثال،

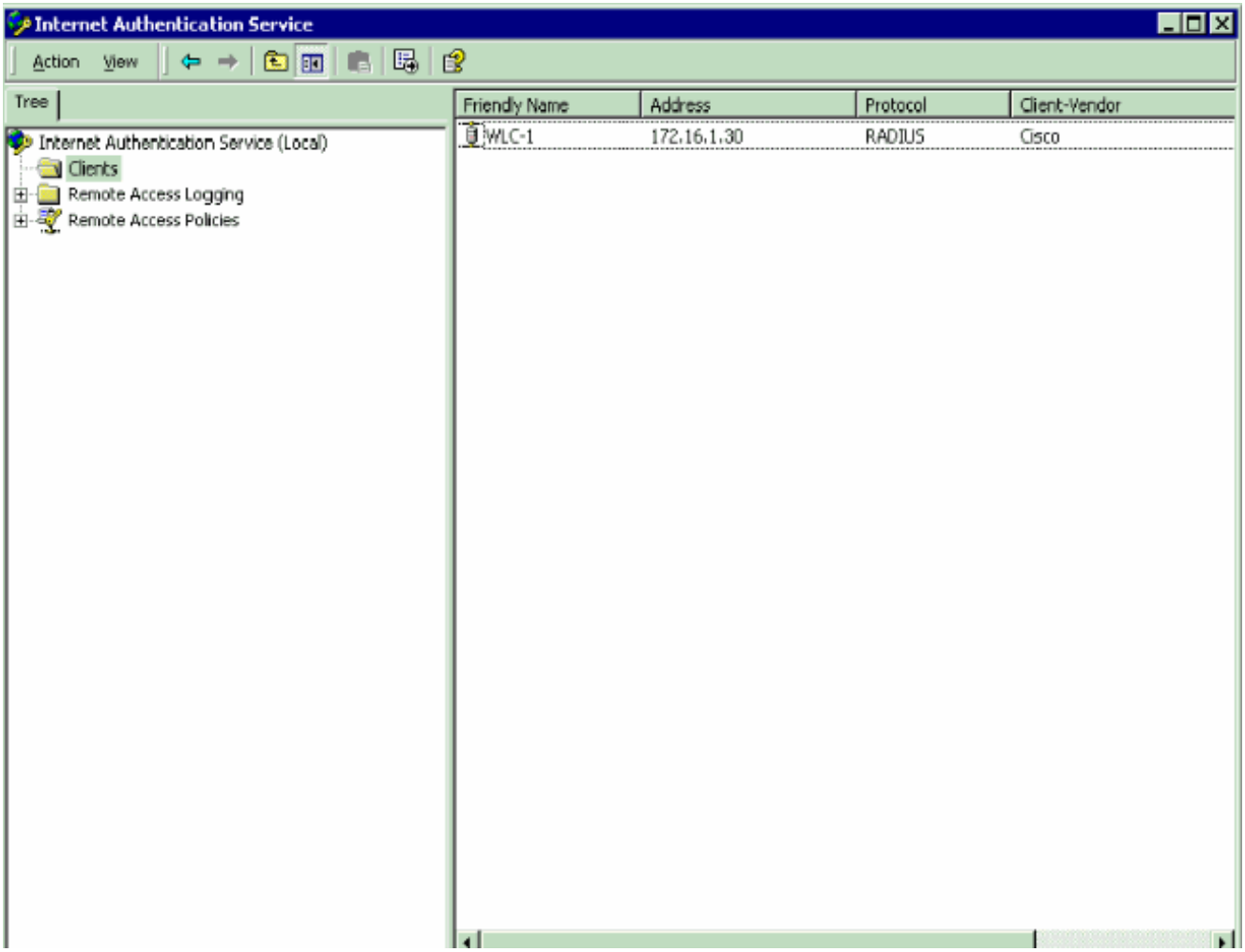
اسم العميل هو *WLC-1*.**ملاحظة:** بشكل افتراضي، يتم تعيين البروتوكول على RADIUS.



4. في نافذة Add RADIUS Client، أدخل **عنوان IP للعميل**، و**client-vendor**، و**السر المشترك**. بعد إدخال معلومات العميل، انقر فوق **إنهاء**.يبدي هذا مثال زبون يعين *WLC-1* مع عنوان *172.16.1.30*، الزبون-بائع ثبتت إلى *cisco*، والسر مشترك *cisco123*:



مع هذه المعلومات، تتم إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) المسمى WLC-1 كعميل AAA لخادم IAS.

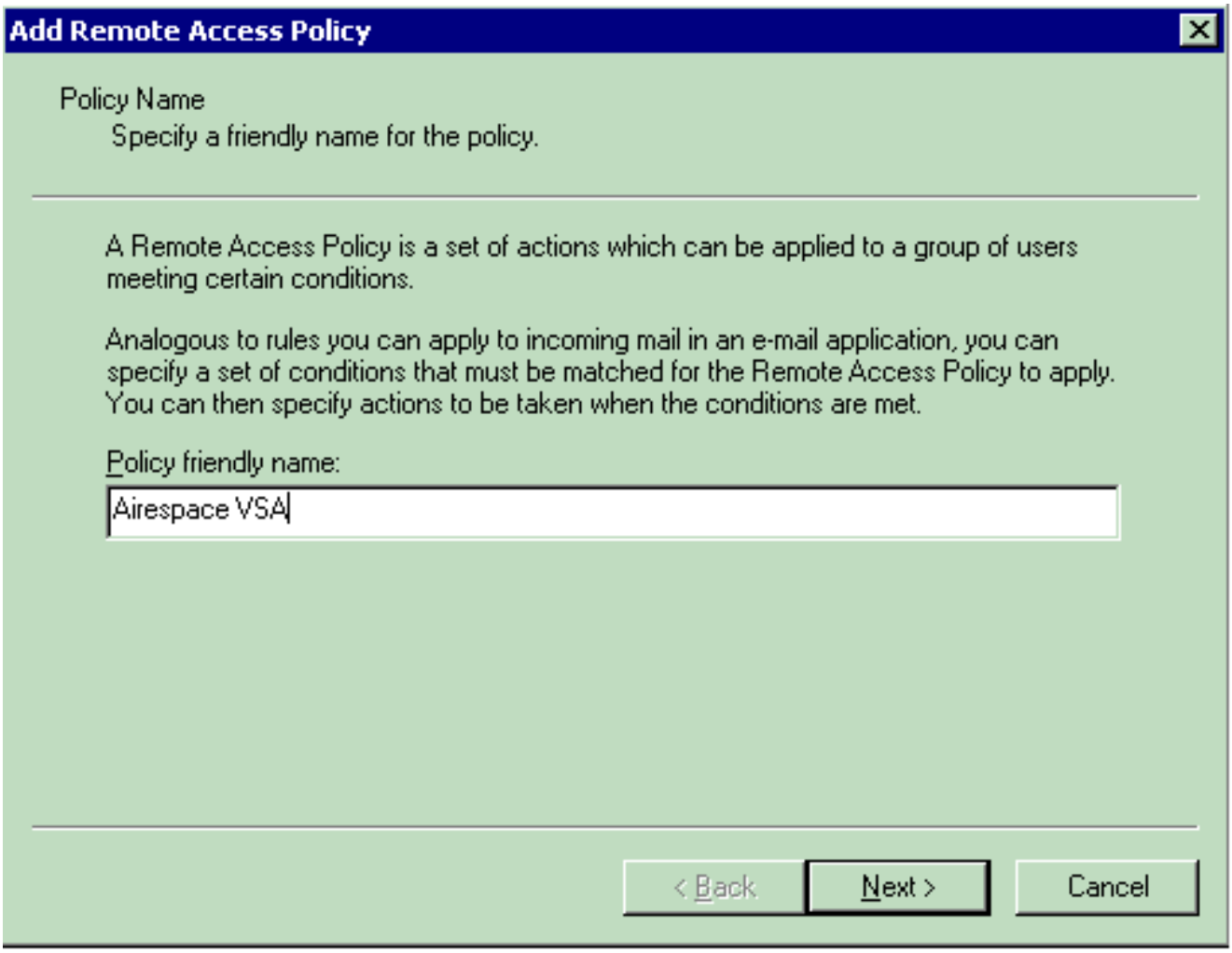


تتمثل الخطوة التالية في إنشاء سياسة الوصول عن بعد وتكوين شبكات VSA.

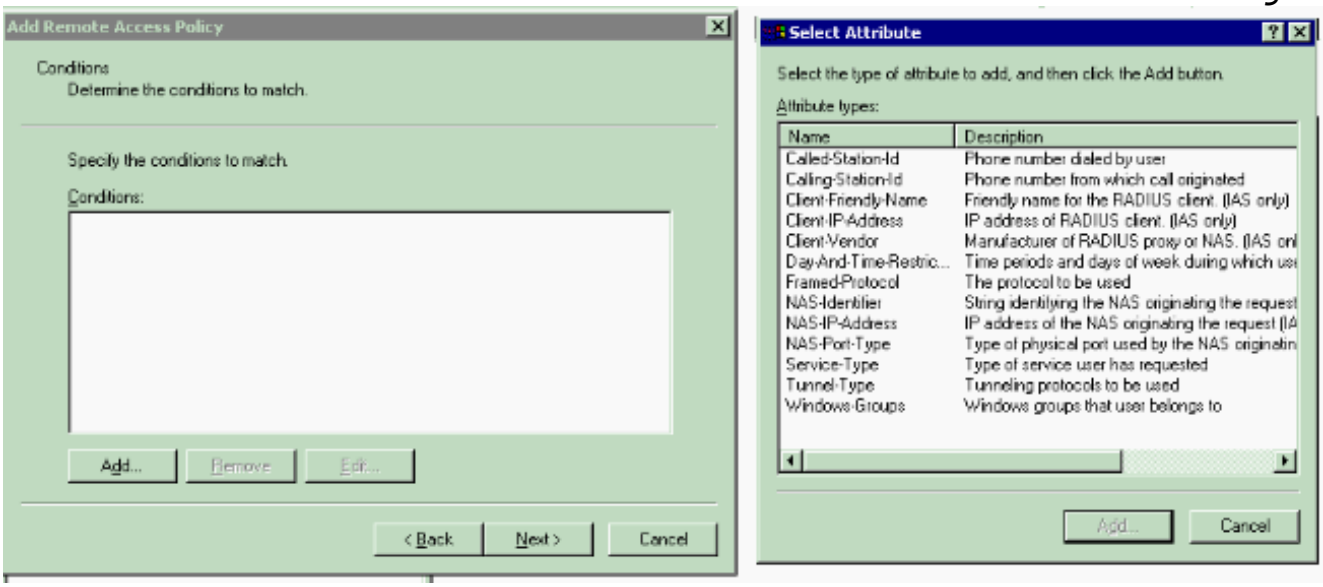
تكوين نهج الوصول عن بعد على IAS

أكمل الخطوات التالية لتكوين نهج وصول عن بعد جديد على IAS:

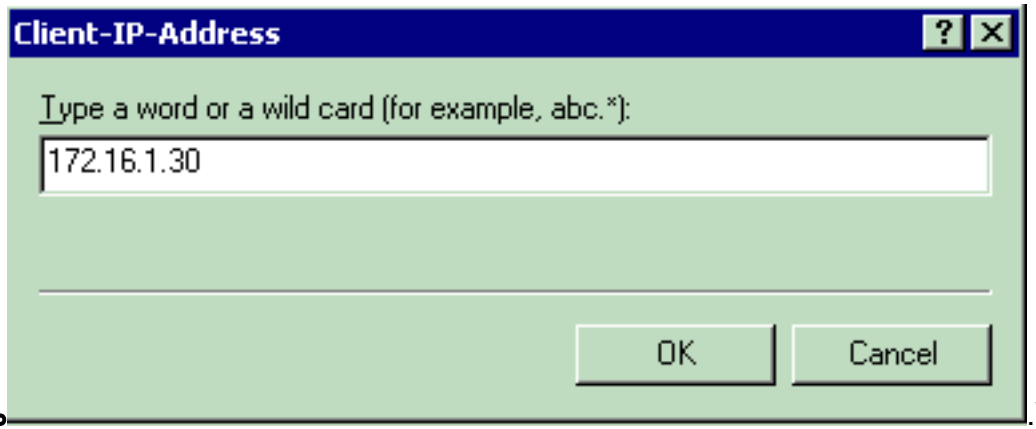
1. انقر بزر الماوس الأيمن فوق **نهج الوصول عن بعد** واختر **نهج AcceMS الجديد عن بعد**.يظهر إطار اسم النهج.
2. أدخل اسم النهج وانقر فوق **التالي**.



3. في الإطار التالي، حدد الشروط التي سيتم تطبيق نهج الوصول عن بعد عليها. طقطقة **يضيف** in order to حددت
الشرط.

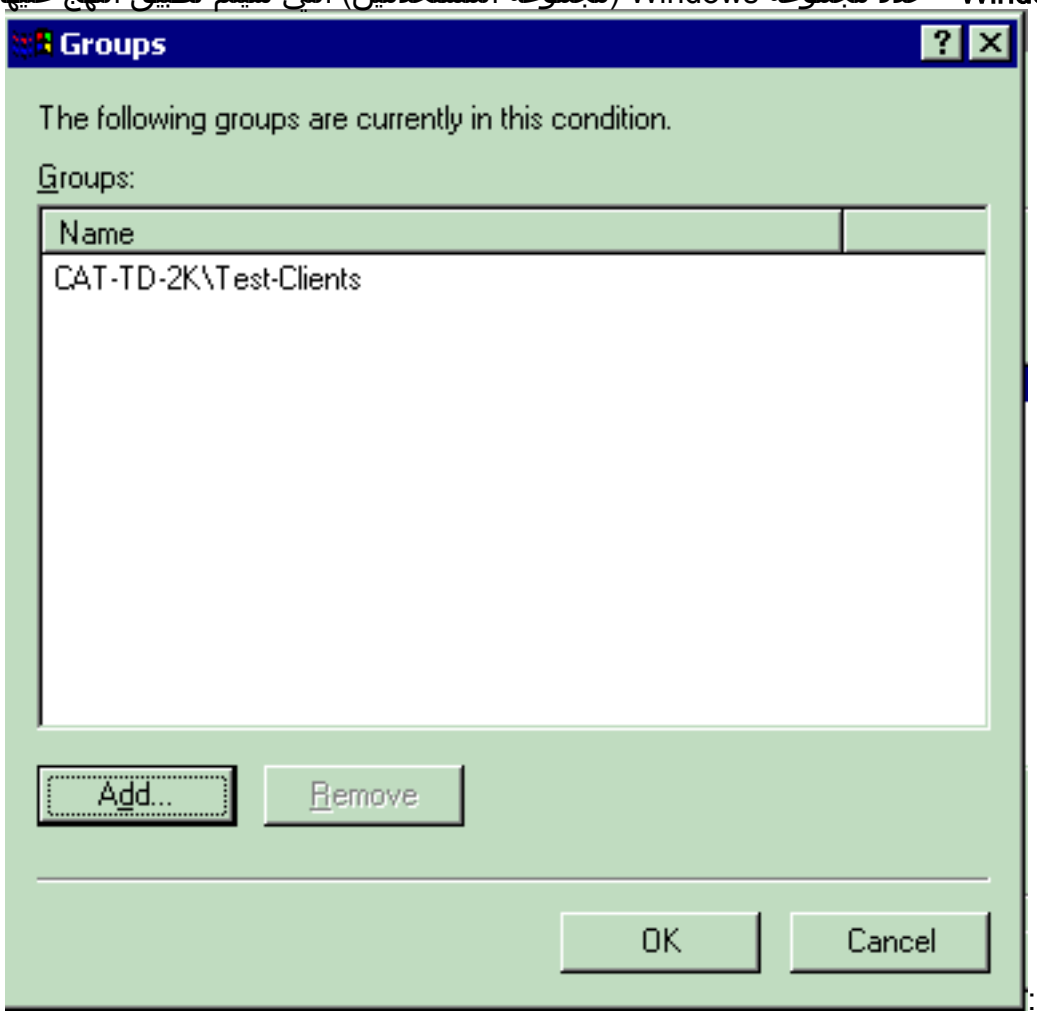


4. من قائمة أنواع السمات ، حدد السمات التالية:**client-ip-address**—أدخل عنوان IP الخاص بعميل AAA. في هذا مثال، ال WLCs عنوان دخلت لذلك السياسة يطبق إلى ربط من ال

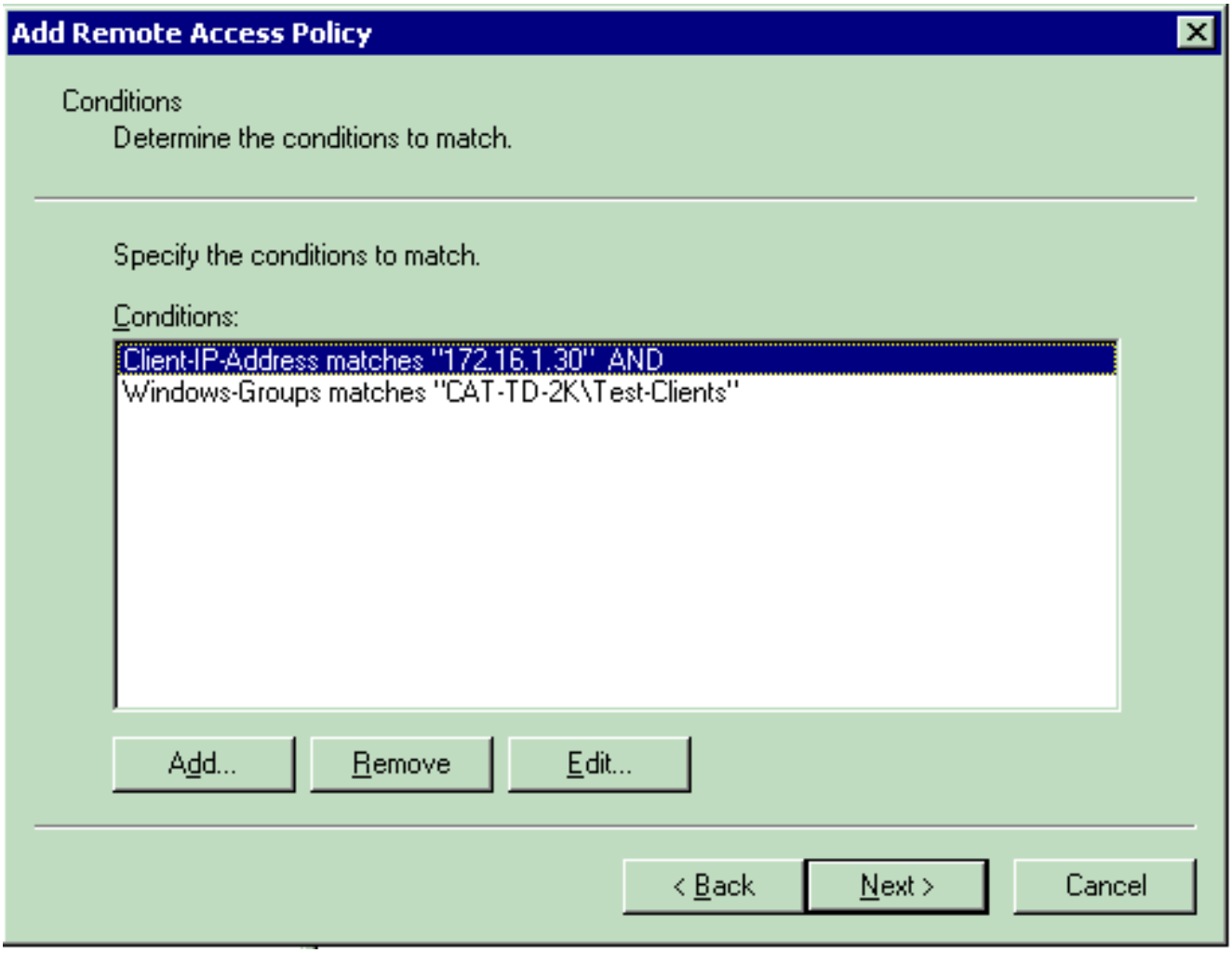


مجموعات WLC.

Windows—حدد مجموعة Windows (مجموعة المستخدمين) التي سيتم تطبيق النهج عليها. فيما يلي

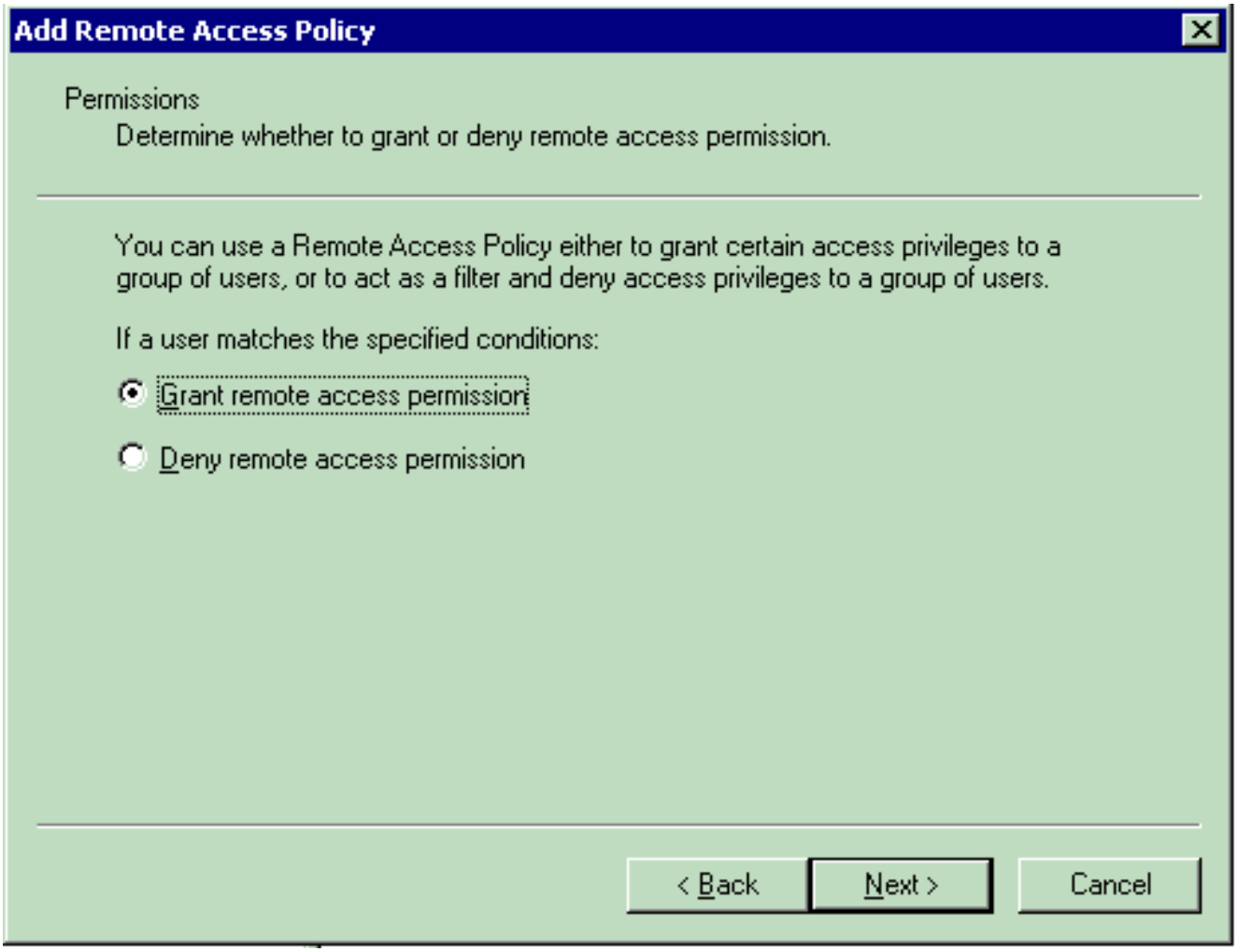


مثال:

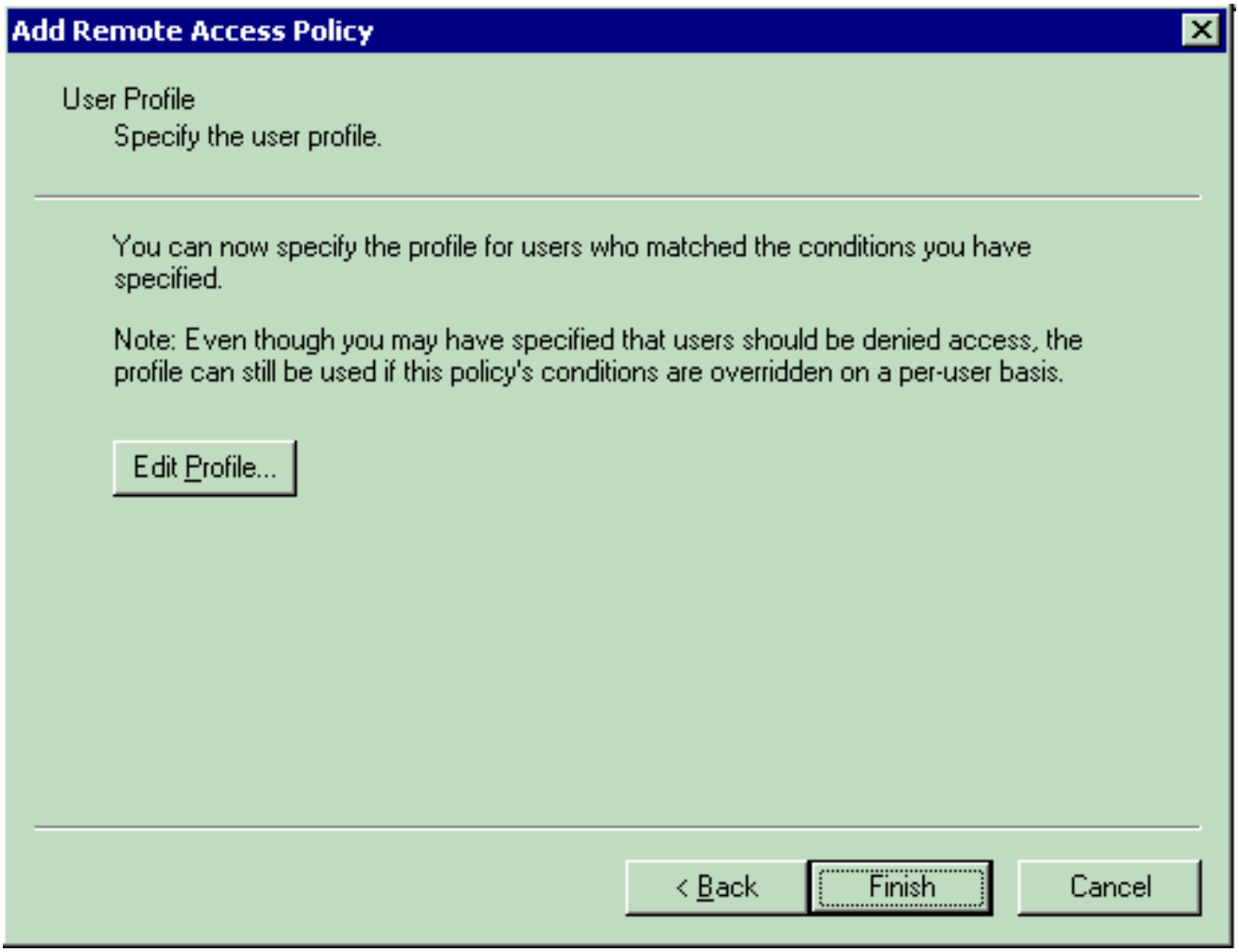


يوضح هذا المثال شرطين فقط. إذا كان هناك المزيد من الشروط، فقم بإضافة هذه الشروط أيضا وانقر فوق **التالي**.يظهر إطار الأذون.

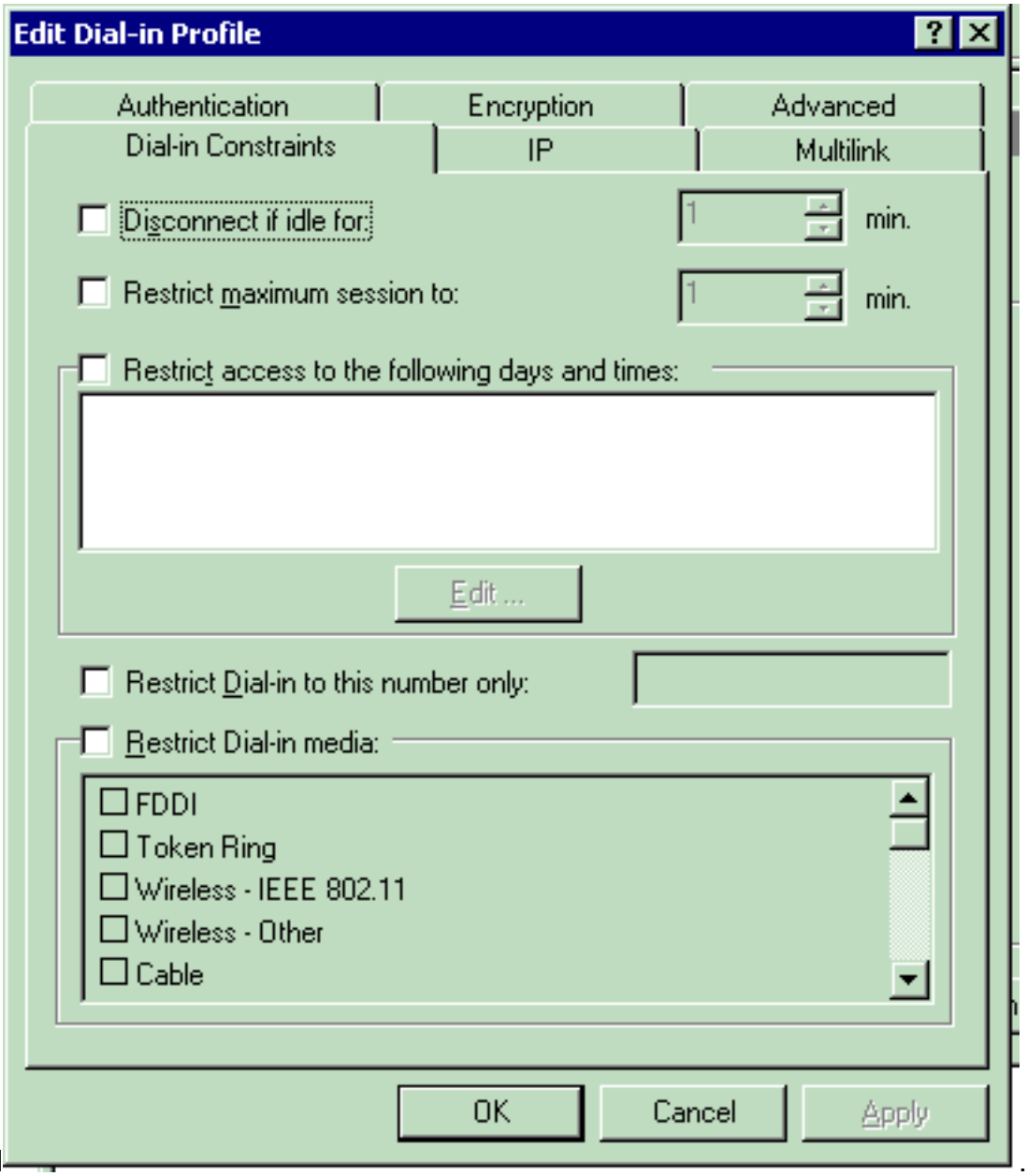
5. في الإطار أذون ، أختر **منح إذن الوصول عن بعد**.بعد إختيار هذا الخيار، يتم منح المستخدم حق الوصول، على أن يطابق المستخدم الشروط المحددة (من الخطوة 2).



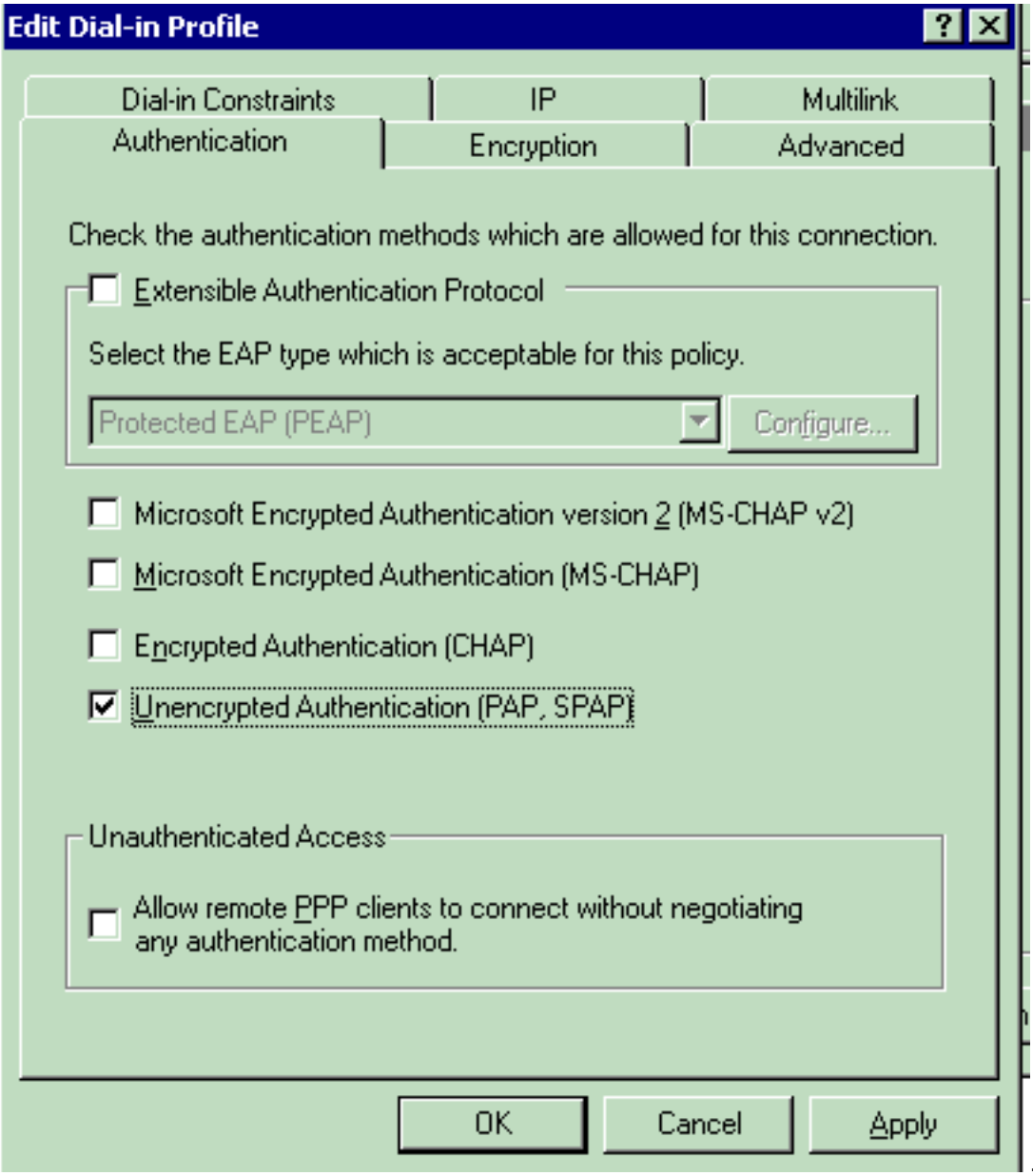
6. انقر فوق **Next (التالي)**.
7. تتمثل الخطوة التالية في إعداد ملف تعريف المستخدم.على الرغم من أنه قد تكون قد حددت أنه يجب رفض المستخدمين أو منحهم حق الوصول بناء على الشروط، إلا أنه لا يزال من الممكن إستخدام ملف التعريف إذا تم تجاوز شروط هذا النهج على أساس كل
مستخدم.



طقطقة in order to شكلت المستعمل توصيف، **يحرر توصيف** على نافذة المستعمل التوصيف.تظهر نافذة "تحرير ملف تعريف الطلب

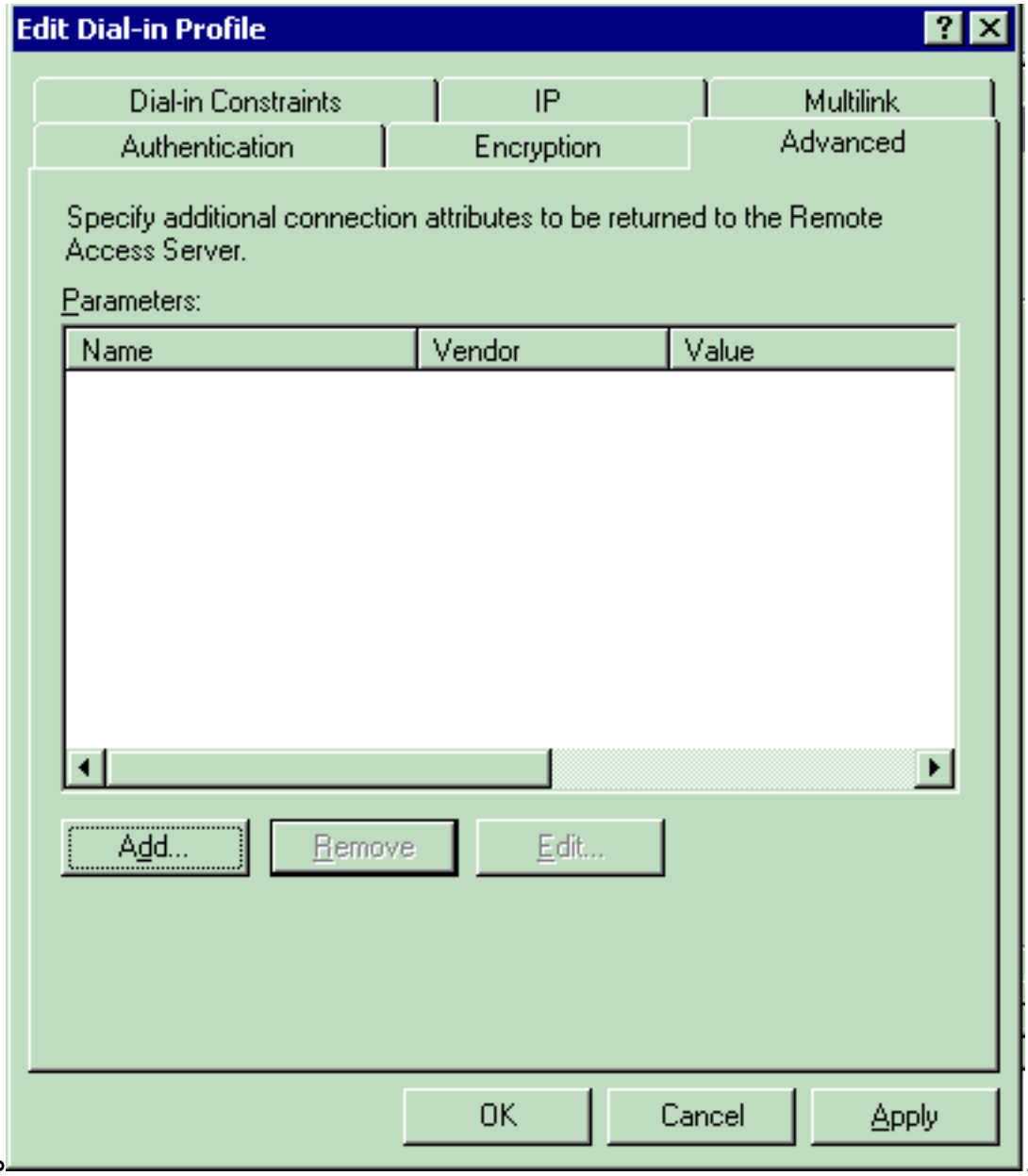


الهاتفي".انقر فوق علامة التبويب **المصادقة**، ثم أختر طريقة المصادقة المستخدمة في الشبكة المحلية اللاسلكية (WLAN).يستخدم هذا المثال مصادقة غير مشفرة (PAP،



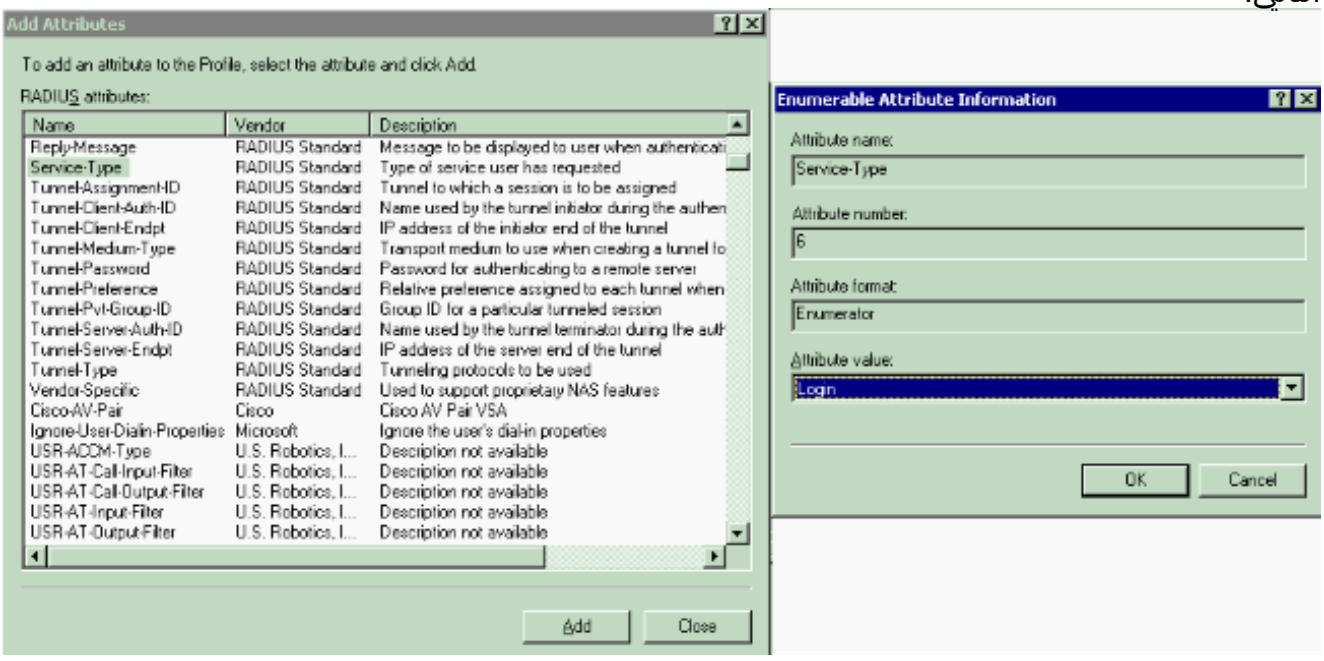
انقر فوق SPAP).

علامة التبويب **خيارات متقدمة**. قم بإزالة كافة المعلمات الافتراضية وانقر فوق



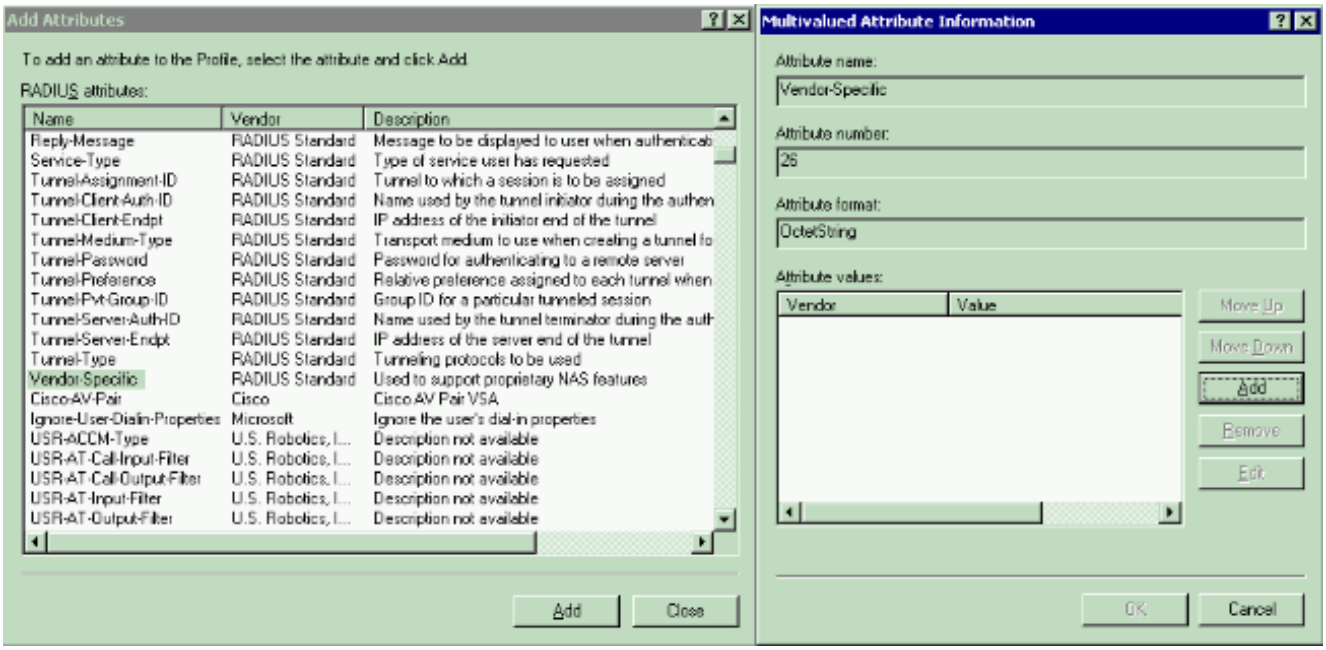
إضافة.من نافذة

إضافة سمات، حدد **نوع الخدمة**، ثم أختر قيمة **تسجيل الدخول** من الإطار التالي.

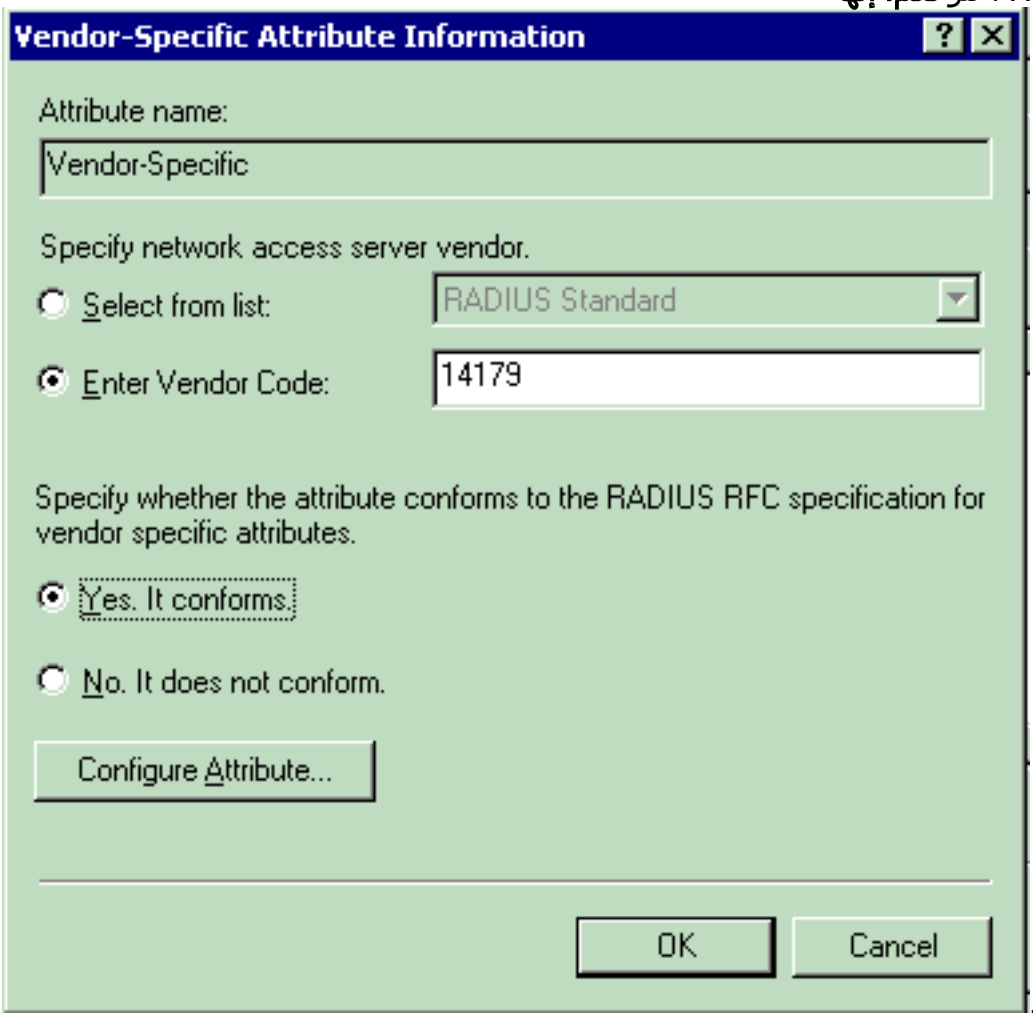


بعد ذلك، يلزمك تحديد السمة **الخاصة بالمورد** من قائمة سمات

.RADIUS

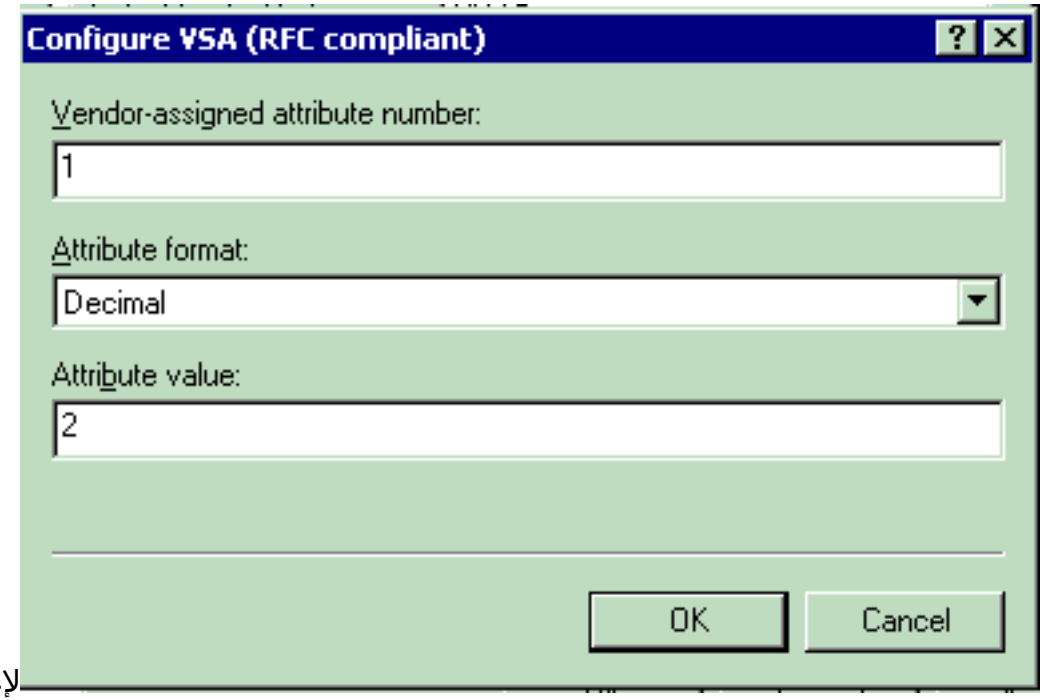


في الإطار التالي، طقطقت **يضيف** in order to حددت VSA جديد.يظهر نافذة معلومات السمة الخاصة بالمورد.تحت تحديد مورد خادم الوصول إلى الشبكة، أختر **إدخال رمز المورد**.دخلت البائع رمز ل Airespace VSAs. كود المورد ل **14179** Cisco Airespace VSAs.لأن هذه السمة تتفق مع مواصفات RADIUS RFC ل VSAs، أختر **نعم. إنها**

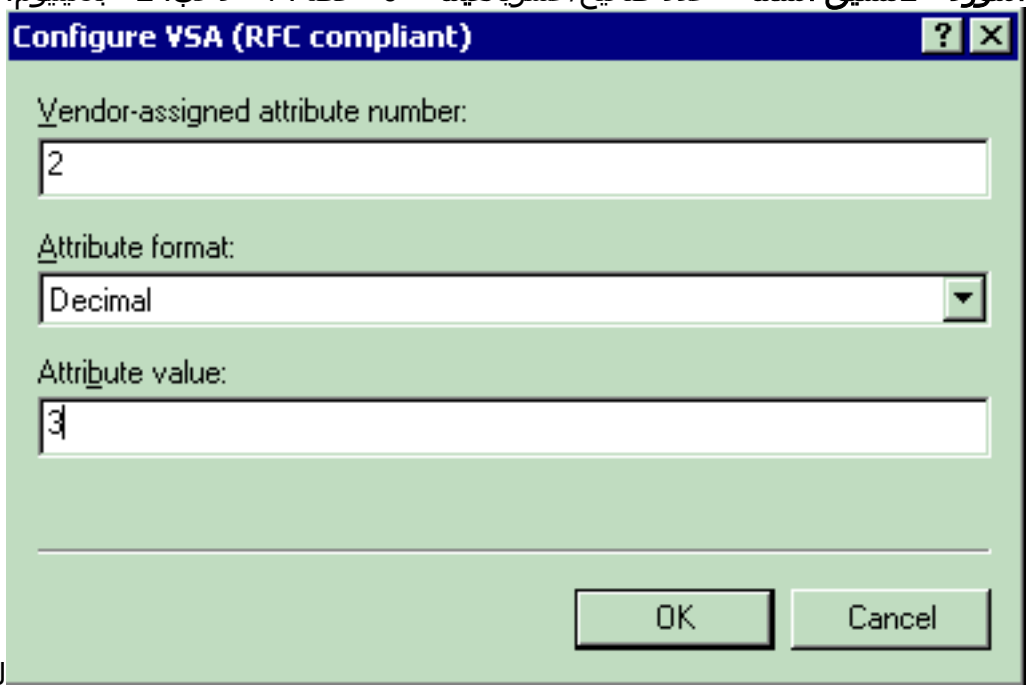


تتوافق.. انقر فوق **تكوين**

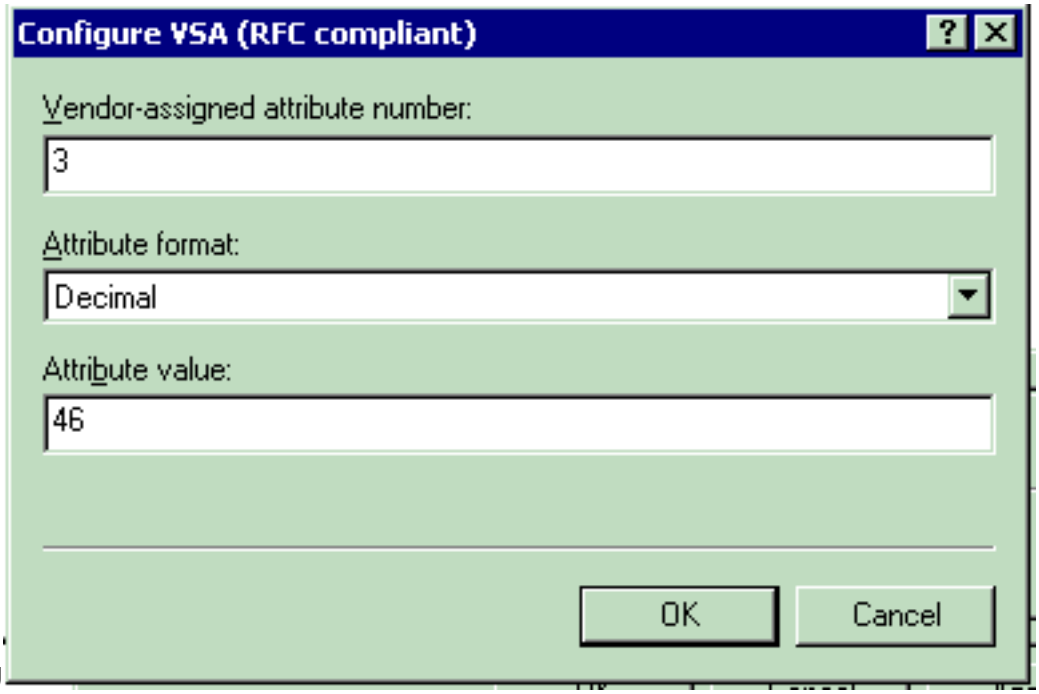
السمة.دخلت في ال configure VSA (متوافق مع RFC) نافذة، البائع يعين سمة رقم، السمة شكل والسمة قيمة، أي يعتمد على ال VSA أن أنت تريد أن يستعمل.لإعداد معرف WLAN على أساس كل مستخدم:**اسم السمة**—Airespace-WLAN-id**رقم السمة المعين من قبل المورد**—1**تنسيق السمة**—عدد صحيح/عشري**value**—wlan-id**مثال 1**



لإعداد ملف تعريف جودة الخدمة على أساس كل مستخدم:**اسم السمة** — Airespace-QoS-level**رقم السمة المعين من قبل المورد**—2**تنسيق السمة**—عدد صحيح/عشري**القيمة**—0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ 3 - برونز**مثال 2**

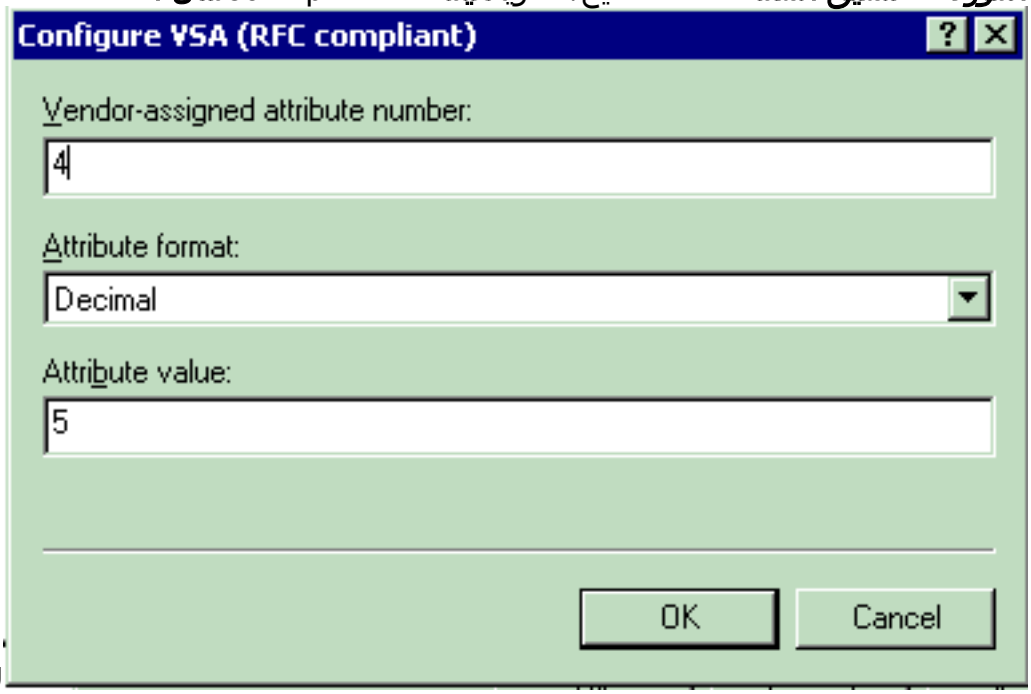


لتعيين قيمة DSCP على أساس كل مستخدم:**اسم السمة** — Airespace-DSCP**ترقيم السمة المعين من قبل المورد**—3**تنسيق السمة**—عدد صحيح/عشري**القيمة**—قيمة DSCP**مثال 3**



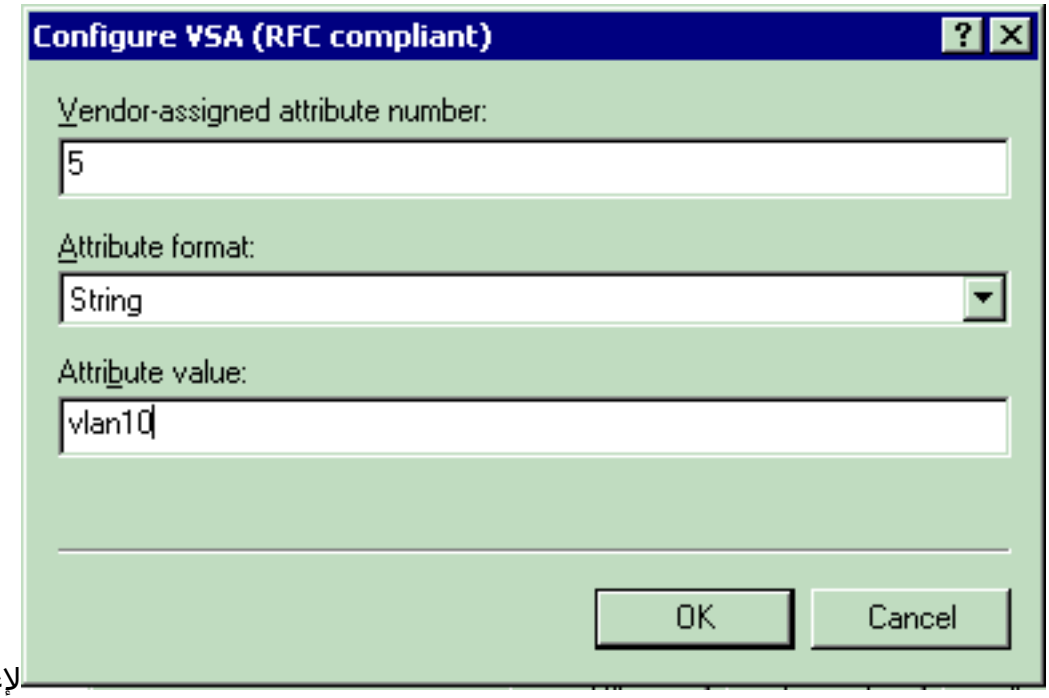
لإعداد علامة 802. 1p

على أساس كل مستخدم:**اسم السمة** — Airespace-802.1p-tag**رقم السمة المعين من قبل المورد**—4**تنسيق السمة**—عدد صحيح/عشري**القيمة**—علامة 802.1p**مثال 4**

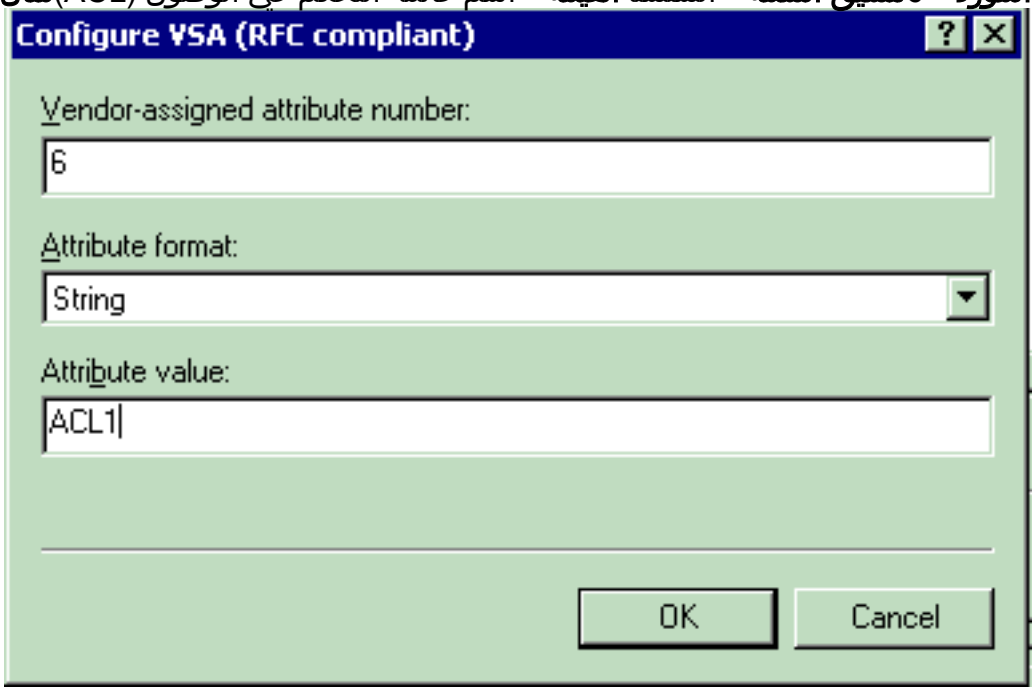


لإعداد الواجهة (VLAN)

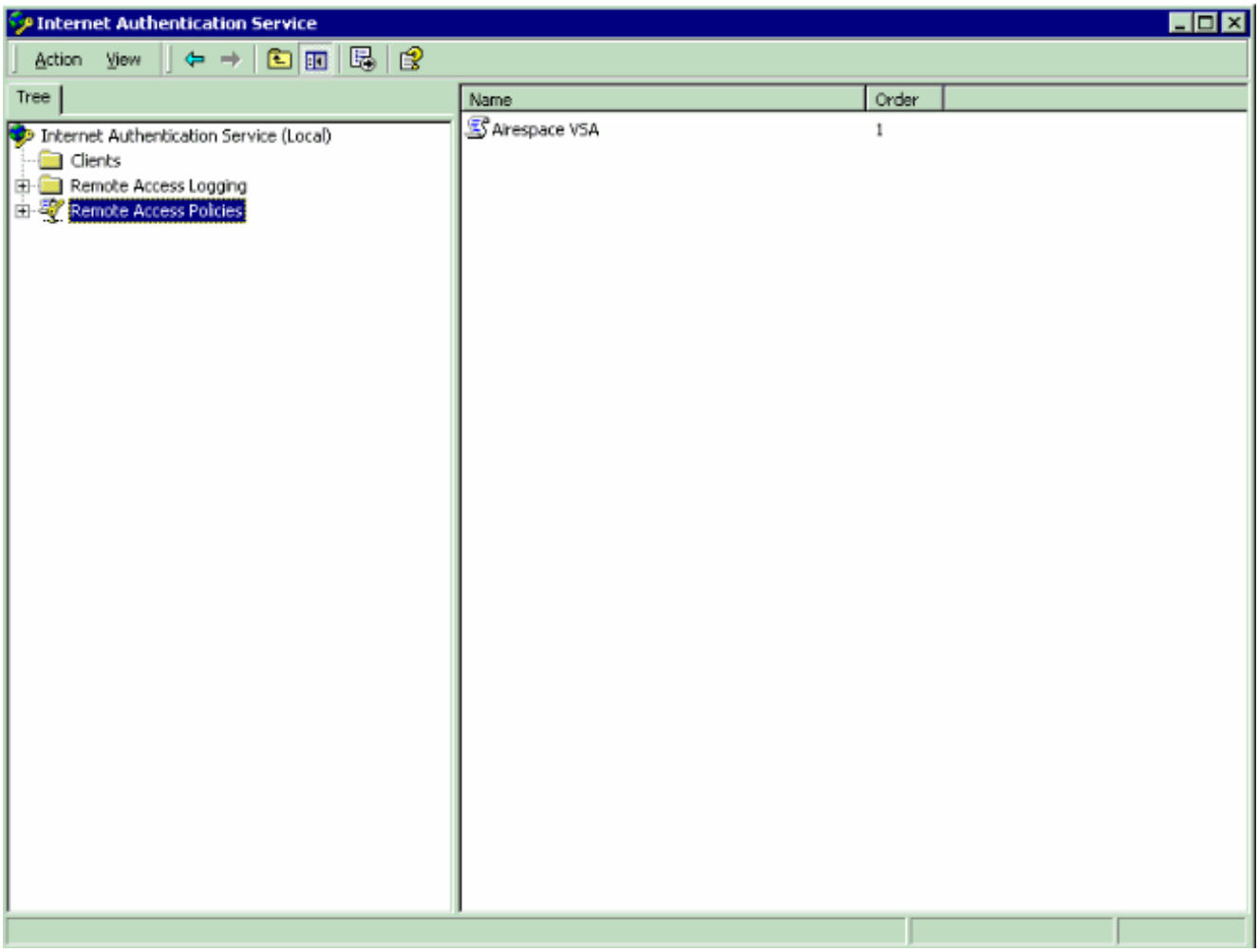
على أساس كل مستخدم:**اسم السمة**—Airespace-interface-name**رقم السمة المعين من قبل المورد**—5**تنسيق السمة**—السلسلة**القيمة**—interface-name**مثال 5**



لإعداد قائمة التحكم في الوصول (ACL) على أساس كل مستخدم:**اسم السمة** — اسم Airespace-ACL**رقم السمة المعين من قبل المورد**—6**تنسيق السمة**—السلسلة**القيمة**—اسم قائمة التحكم في الوصول (ACL)**مثال 6**

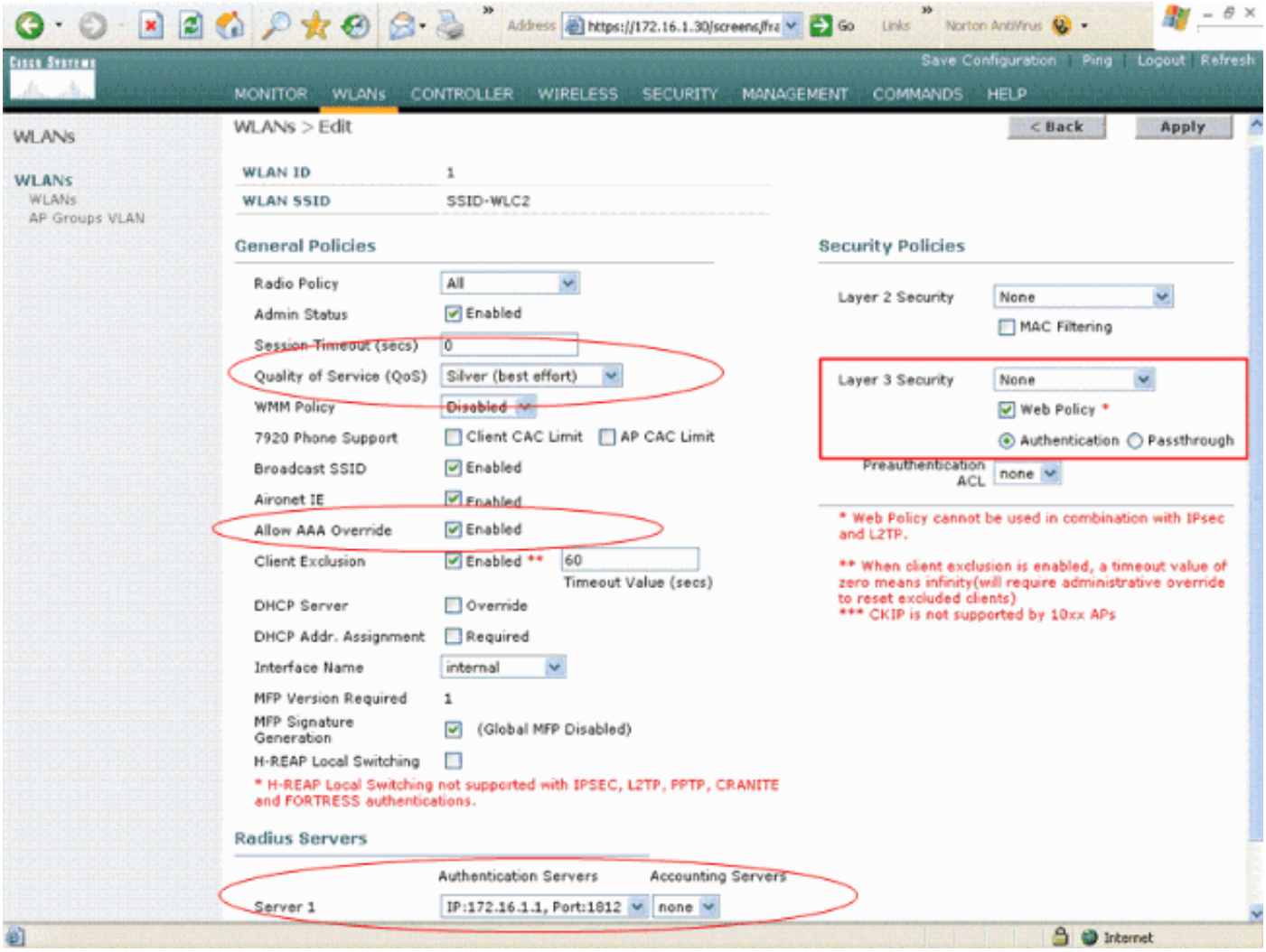


8. ما إن يشكل أنت ال VSAs، طقطقت **ok** إلى أن أنت ترى المستعمل مرجع نافذة.
9. بعد ذلك، انقر فوق **إنهاء** لإكمال التكوين.يمكنك مشاهدة النهج الجديد ضمن نهج الوصول عن بعد.



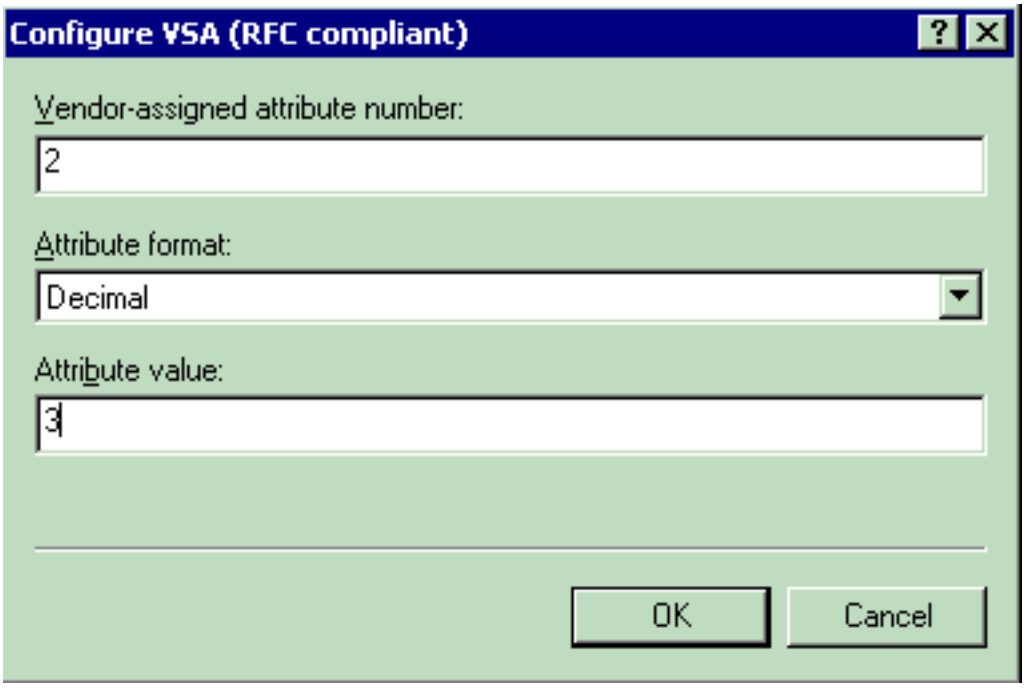
مثال على التكوين

في هذا المثال، يتم تكوين شبكة WLAN لمصادقة الويب. تتم مصادقة المستخدمين بواسطة خادم IAS RADIUS، ويتم تكوين خادم RADIUS لتخصيص نهج جودة الخدمة (QoS) على أساس كل مستخدم.



كما يمكنك أن ترى من هذا الإطار، يتم تمكين مصادقة الويب، وخادم المصادقة هو 172.16.1.1، كما يتم تمكين تجاوز AAA على شبكة WLAN. تم تعيين إعداد جودة الخدمة الافتراضي لشبكة WLAN هذه إلى Silver.

على خادم IAS RADIUS، يتم تكوين سياسة وصول عن بعد تقوم بإرجاع السمة البرونزية لجودة الخدمة في طلب قبول RADIUS. ويتم القيام بذلك عند تكوين معرف فئة المورد (VSA) الخاص بسمة جودة الخدمة.



راجع قسم تكوين نهج الوصول عن بعد على IAS في هذا المستند للحصول على معلومات تفصيلية حول كيفية تكوين نهج الوصول عن بعد على خادم IAS.

بمجرد تكوين خادم IAS و WLC و LAP لهذا الإعداد، يمكن للعملاء اللاسلكيين إستخدام مصادقة الويب للاتصال.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

عندما يتصل المستخدم بشبكة WLAN بمعرف مستخدم وكلمة مرور، يقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بتمرير بيانات الاعتماد إلى خادم IAS RADIUS الذي يصادق المستخدم في مقابل الشروط وملف تعريف المستخدم الذي تم تكوينه في نهج الوصول عن بعد. إذا نجحت مصادقة المستخدم، يرجع خادم RADIUS طلب قبول RADIUS الذي يحتوي أيضا على قيم تجاوز AAA. في هذه الحالة، يتم إرجاع سياسة جودة الخدمة الخاصة بالمستخدم.

يمكنك إصدار الأمر **debug aaa all enable** لعرض تسلسل الأحداث التي تحدث أثناء المصادقة. هنا نموذج للمخرجات:

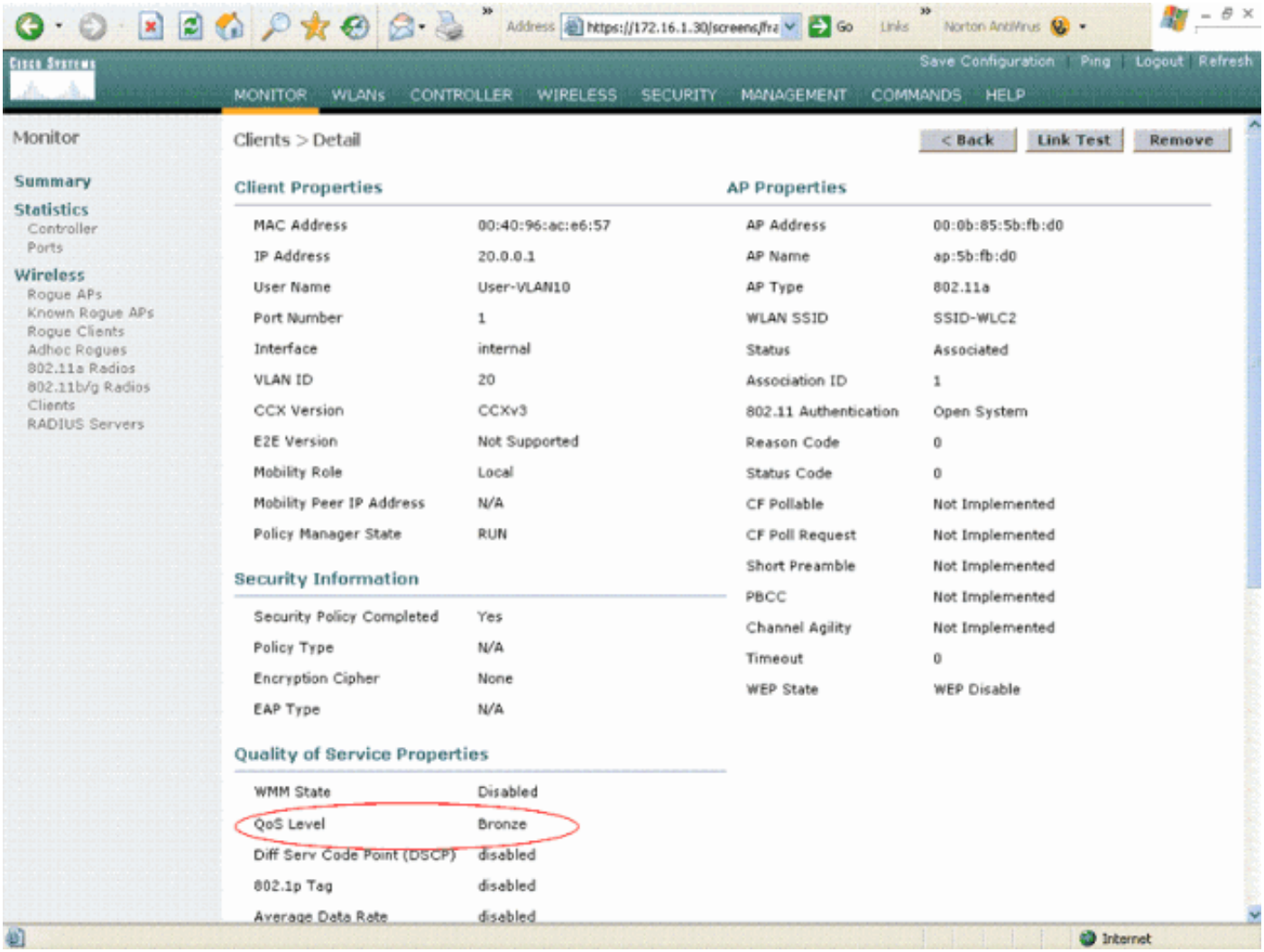
```
                                                Cisco Controller) > debug aaa all enable)
                                        Wed Apr 18 18:14:24 2007: User admin authenticated
      Wed Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for
                                        mobile 28:1f:00:00:00:00
                              Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c
        Wed Apr 18 18:14:24 2007:       structureSize.............................70
         Wed Apr 18 18:14:24 2007:       resultCode.................................0
Wed Apr 18 18:14:24 2007:       protocolUsed..............................0x00000008
          .................................Wed Apr 18 18:14:24 2007:       proxyState
                                28:1F:00:00:00:00-00:00
                                :Wed Apr 18 18:14:24 2007:       Packet contains 2 AVPs
  ..........................Wed Apr 18 18:14:24 2007:           AVP[01] Service-Type
                           (0x00000006 (6) (4 bytes
  ............Wed Apr 18 18:14:24 2007:           AVP[02] Airespace / WLAN-Identifier
                           (0x00000000 (0) (4 bytes
                                        Wed Apr 18 18:14:24 2007: User admin authenticated
      Wed Apr 18 18:14:24 2007: 29:1f:00:00:00:00 Returning AAA Error 'Success' (0) for
                                        mobile 29:1f:00:00:00:00
                              Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c
        Wed Apr 18 18:14:24 2007:       structureSize.............................70
         Wed Apr 18 18:14:24 2007:       resultCode.................................0
Wed Apr 18 18:14:24 2007:       protocolUsed..............................0x00000008
          .................................Wed Apr 18 18:14:24 2007:       proxyState
                                29:1F:00:00:00:00-00:00
                                :Wed Apr 18 18:14:24 2007:       Packet contains 2 AVPs
  ..........................Wed Apr 18 18:14:24 2007:           AVP[01] Service-Type
                           (0x00000006 (6) (4 bytes
  ............Wed Apr 18 18:14:24 2007:           AVP[02] Airespace / WLAN-Identifier
                           (0x00000000 (0) (4 bytes
          Wed Apr 18 18:15:08 2007: Unable to find requested user entry for User-VLAN10
                            Wed Apr 18 18:15:08 2007: AuthenticationRequest: 0xa64c8bc
 Wed Apr 18 18:15:08 2007:       Callback.....................................0x8250c40
Wed Apr 18 18:15:08 2007:       protocolType..............................0x00000001
          .................................Wed Apr 18 18:15:08 2007:       proxyState
                                AC:E6:57-00:00:00:40:96
                     (Wed Apr 18 18:15:08 2007:       Packet contains 8 AVPs (not shown
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Successful transmission of Authentication Packet
   id 26) to 172.16.1.1:1812, proxy state 00:40:96:ac:e6:57-96:ac)
     Wed Apr 18 18:15:08 2007: 00000000: 01 1a 00 68 00 00 00 00  00 00 00 00 00 00 00 00
                                          .............h...
```

```
Wed Apr 18 18:15:08 2007: 00000010: 00 00 00 00 01 0d 55 73  65 72 2d 56 4c 41 4e 31
                                          User-VLAN1......
Wed Apr 18 18:15:08 2007: 00000020: 30 02 12 fa 32 57 ba 2a  ba 57 38 11 bc 9a 5d 59
                                          2W.*.W8...]Y...0
Wed Apr 18 18:15:08 2007: 00000030: ed ca 23 06 06 00 00 00  01 04 06 ac 10 01 1e 20
                                          .............#..
Wed Apr 18 18:15:08 2007: 00000040: 06 57 4c 43 32 1a 0c 00  00 37 63 01 06 00 00 00
                                          .....WLC2....7c.
Wed Apr 18 18:15:08 2007: 00000050: 01 1f 0a 32 30 2e 30 2e  30 2e 31 1e 0d 31 37 32
                                          172..20.0.0.1...
                  Wed Apr 18 18:15:08 2007: 00000060: 2e 31 36 2e 31 2e 33 30 .16.1.30
Wed Apr 18 18:15:08 2007: 00000000: 02 1a 00 46 3f cf 1b cc  e4 ea 41 3e 28 7e cc bc
                                          ..~)<F?.....A...
Wed Apr 18 18:15:08 2007: 00000010: 00 e1 61 ae 1a 0c 00 00  37 63 02 06 00 00 00 03
                                          ......a.....7c..
Wed Apr 18 18:15:08 2007: 00000020: 06 06 00 00 00 01 19 20  37 d0 03 e6 00 00 01 37
                                          7......7........
Wed Apr 18 18:15:08 2007: 00000030: 00 01 ac 10 01 01 01 c7  7a 8b 35 20 31 80 00 00
                                          ...z.5.1........
                    ......      Wed Apr 18 18:15:08 2007: 00000040: 00 00 00 00 00 1b
          Wed Apr 18 18:15:08 2007: ****Enter processIncomingMessages: response code=2
            Wed Apr 18 18:15:08 2007: ****Enter processRadiusResponse: response code=2
  Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Access-Accept received from RADIUS server
       for mobile 00:40:96:ac:e6:57 receiveId = 0 172.16.1.1
                           Wed Apr 18 18:15:08 2007: AuthorizationResponse: 0x9802520
      Wed Apr 18 18:15:08 2007:       structureSize.............................114
        Wed Apr 18 18:15:08 2007:       resultCode.................................0
Wed Apr 18 18:15:08 2007:       protocolUsed.............................0x00000001
          .................................Wed Apr 18 18:15:08 2007:       proxyState
                                AC:E6:57-00:00:00:40:96
                                :Wed Apr 18 18:15:08 2007:       Packet contains 3 AVPs
  ...................Wed Apr 18 18:15:08 2007:           AVP[01] Airespace / QOS-Level
                           (0x00000003 (3) (4 bytes
  ............................Wed Apr 18 18:15:08 2007:           AVP[02] Service-Type
                           (0x00000001 (1) (4 bytes
  ................................Wed Apr 18 18:15:08 2007:           AVP[03] Class
                                    (DATA (30 bytes
     Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Applying new AAA override for station
                                                ac:e6:57:00:40:96
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57
                                                    source: 48, valid bits: 0x3
        qosLevel: 3, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
                     dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                     ' :vlanIfName: '', aclName
                 Wed Apr 18 18:15:12 2007: AccountingMessage Accounting Start: 0xa64c8bc
                                  :Wed Apr 18 18:15:12 2007:       Packet contains 13 AVPs
  ..............................Wed Apr 18 18:15:12 2007:           AVP[01] User-Name
                              (User-VLAN10 (11 bytes
  ................................Wed Apr 18 18:15:12 2007:           AVP[02] Nas-Port
                           (0x00000001 (1) (4 bytes
  ..........................Wed Apr 18 18:15:12 2007:           AVP[03] Nas-Ip-Address
                 (0xac10011e (-1408237282) (4 bytes
  ..........................Wed Apr 18 18:15:12 2007:           AVP[04] NAS-Identifier
                  (0x574c4332 (1464615730) (4 bytes
  ..............Wed Apr 18 18:15:12 2007:           AVP[05] Airespace / WLAN-Identifier
                           (0x00000001 (1) (4 bytes
  ........................Wed Apr 18 18:15:12 2007:           AVP[06] Acct-Session-Id
           (4626602c/00:40:96:ac:e6:57/16 (29 bytes
  ..........................Wed Apr 18 18:15:12 2007:           AVP[07] Acct-Authentic
                           (0x00000001 (1) (4 bytes
  ............................Wed Apr 18 18:15:12 2007:           AVP[08] Tunnel-Type
                          (0x0000000d (13) (4 bytes
  ......................Wed Apr 18 18:15:12 2007:           AVP[09] Tunnel-Medium-Type
                           (0x00000006 (6) (4 bytes
```

```
.........................Wed Apr 18 18:15:12 2007:          AVP[10] Tunnel-Group-Id
                          (0x3230 (12848) (2 bytes
.........................Wed Apr 18 18:15:12 2007:          AVP[11] Acct-Status-Type
                          (0x00000001 (1) (4 bytes
.......................Wed Apr 18 18:15:12 2007:          AVP[12] Calling-Station-Id
                            (bytes 8) 20.0.0.1
.......................Wed Apr 18 18:15:12 2007:          AVP[13] Called-Station-Id
                          (bytes 11) 172.16.1.30
```

كما يمكنك أن ترى من المخرجات، فإن المستخدم تتم مصادقته. ثم، يتم إرجاع قيم تجاوز AAA باستخدام رسالة قبول RADIUS. وفي هذه الحالة، يتم إعطاء المستخدم سياسة جودة الخدمة (QoS) البرونزية.

يمكنك التحقق من ذلك على واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) كذلك. فيما يلي مثال:



ملاحظة: ملف تعريف جودة الخدمة الافتراضي ل SSID هذا هو Silver. ومع ذلك، نظرا لتحديد تجاوز المصادقة والتفويض والمحاسبة (AAA) وتكوين المستخدم باستخدام ملف تعريف جودة الخدمة (QoS) البرونزي على خادم IAS، يتم تجاوز ملف تعريف جودة الخدمة الافتراضي.

استكشاف الأخطاء وإصلاحها

أنت يستطيع استعملت ال **debug aaa all enable** أمر على ال WLC أن يتحرى التشكيل. يتم عرض مثال على إخراج تصحيح الأخطاء هذا في شبكة عمل في قسم التحقق من هذا المستند.

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

معلومات ذات صلة

- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية، الإصدار 4.0 من Cisco
- تقييد الوصول إلى شبكة WLAN استنادا إلى SSID باستخدام WLC ومثال تكوين ACS الآمن من Cisco
- دعم المنتج 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).