تكوين تعيين VLAN الديناميكي باستخدام ACS 5.2 و NGWC

المحتويات

المقدمة

يصف هذا وثيقة مفهوم VLAN حركي تعيين. كما تصف كيفية تكوين وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وخادم RADIUS لتخصيص عملاء شبكة LAN اللاسلكية (WLAN) لشبكة VLAN معينة بشكل ديناميكي. في هذا المستند، يعد خادم RADIUS خادم تحكم في الوصول (ACS) يشغل نظام التحكم في الوصول الآمن من Cisco الإصدار 5.2.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بنقاط الوصول في الوضع Lightweight (LAPs) و WLC
- المعرفة الوظيفية لخادم المصادقة والتفويض والمحاسبة (AAA)

- معرفة دقيقة بالشبكات اللاسلكية ومشكلات الأمان اللاسلكي

المكونات المستخدمة

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

- وحدة التحكم في شبكة LAN اللاسلكية Cisco 5760 مع برنامج Cisco IOS® XE الإصدار 3.2.2 (خزانة أسلاك الجيل التالي، أو NGWC)
- نقطة وصول خفيفة الوزن للسلسلة Cisco Aironet 3602 Series
- Microsoft Windows XP مع عميل PROSet من Intel
- نظام التحكم بالوصول الآمن من Cisco، الإصدار 5.2
- المحول Cisco Catalyst 3560 Series Switch

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التعيين الديناميكي لشبكة VLAN مع خادم RADIUS

في معظم أنظمة WLAN، يكون لكل شبكة WLAN سياسة ثابتة تنطبق على جميع العملاء المرتبطين بمعرف مجموعة الخدمة (SSID) أو WLAN في مصطلحات وحدة التحكم. 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 Cisco WLAN شبكات الهوية. وهذا يسمح للشبكة بالإعلان عن معرف SSID واحد، ولكنه يسمح لمستخدمين محددين وراثة جودة الخدمة (QoS) المختلفة وسمات VLAN و/أو نهج الأمان المستندة إلى مسوغات المستخدم.

تعيين VLAN الديناميكي هو أحد تلك الميزات التي تضع مستخدم لاسلكي في شبكة VLAN معينة بناء على بيانات الاعتماد التي قدمها المستخدم. تتم معالجة هذه المهمة لتعيين المستخدم إلى شبكة VLAN معينة بواسطة خادم مصادقة RADIUS، مثل ACS الآمن من Cisco. يمكن إستخدام هذه الميزة، على سبيل المثال، للسماح للمضيف اللاسلكي بالبقاء على شبكة VLAN نفسها أثناء انتقالها داخل شبكة مجمع.

ونتيجة لذلك، عندما يحاول العميل الاقتران بنقطة وصول في الوضع Lightweight مسجلة مع وحدة تحكم، تقوم نقطة الوصول في الوضع Lightweight بتمرير بيانات اعتماد المستخدم إلى خادم RADIUS للتحقق من الصحة. وبمجرد نجاح المصادقة، يقوم خادم RADIUS بتمرير بعض سمات فريق عمل هندسة الإنترنت (IETF) إلى المستخدم. تحدد سمات RADIUS هذه معرف VLAN الذي يجب تعيينه للعميل اللاسلكي. لا يهم معرف SSID للعميل (الشبكة المحلية اللاسلكية (WLAN) من حيث عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لأنه يتم تعيين المستخدم دائما لمعرف VLAN هذا المحدد مسبقا.

سمات مستخدم RADIUS المستخدمة لتعيين معرف VLAN هي:

- IETF 64 (نوع النفق) - ضبط على VLAN.
- IETF 65 (نوع النفق المتوسط) - ضبط على 802.
- IETF 81 (Tunnel-Private-Group-ID) - تم تعيينه على معرف شبكة VLAN.

معرف شبكة VLAN هو 12 وحدة بت ويأخذ قيمة بين 1 و 4094، شاملة. لأن معرف Tunnel-Private-Group-ID هو من النوع خيط، كما هو معرف في RFC 2868، وسمات RADIUS لدعم بروتوكول النفق للاستخدام مع IEEE 802.1X، يتم تشفير قيمة العدد الصحيح لمعرف VLAN كسلسلة. عندما يتم إرسال سمات النفق هذه، فمن الضروري أن تملأ في حقل علامة التمييز.

وكما لوحظ في RFC2868، الباب 3-1:

"حقل العلامة عبارة عن نظام ثماني واحد في الطول ويقصد به توفير وسيلة لتجميع السمات في الحزمة نفسها التي تشير إلى نفس النفق."

القيم الصالحة لحقل العلامة هي 0x01 حتى 0x1F، شاملة. إذا كان حقل العلامة غير مستخدم، يجب أن يكون صفر (0x00). راجع RFC 2868 للحصول على مزيد من المعلومات حول جميع سمات RADIUS.

التكوين

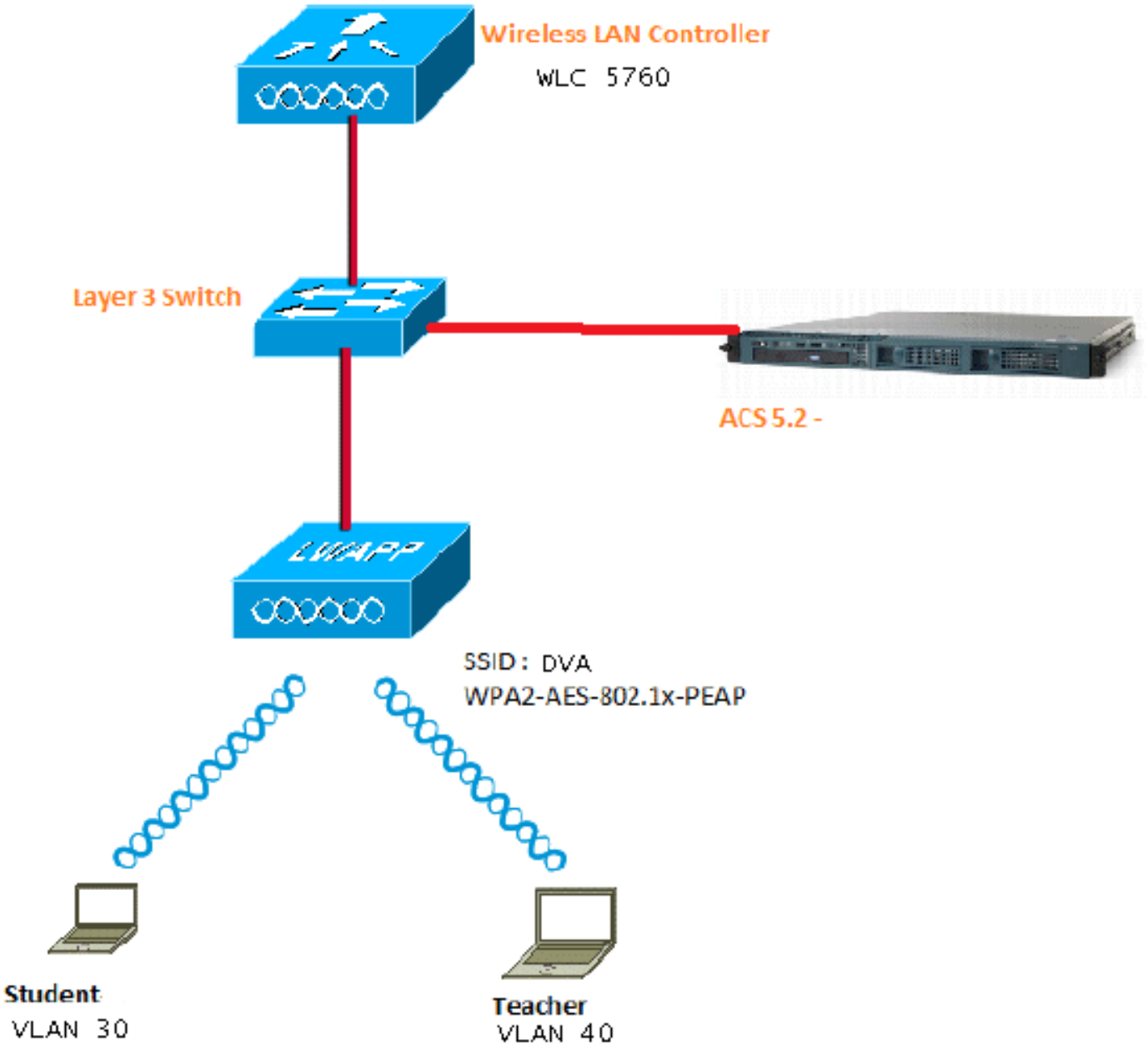
يتألف تكوين تعيين شبكة VLAN الديناميكية من خطوتين مميزتين:

1. شكلت ال WLC مع الأمر خط قارن (CLI) أو مع ال gui.
2. قم بتكوين خادم RADIUS.

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



يستخدم هذا المستند 802.1X مع بروتوكول المصادقة المتوسع المحمي (PEAP) كآلية تأمين.

إفتراضات

- يتم تكوين المحولات لجميع شبكات VLAN من الطبقة 3 (L3).
- تم تعيين نطاق DHCP لخادم DHCP.
- يوجد اتصال L3 بين جميع الأجهزة في الشبكة.
- نقطة الوصول (LAP) متصلة بالفعل بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC).
- تحتوي كل شبكة VLAN على قناع /24.
- يحتوي ACS 5.2 على شهادة موقعة ذاتيا مثبتة.

تكوين WLC باستخدام CLI

تكوين WLAN

هذا مثال على كيفية تكوين شبكة WLAN باستخدام SSID الخاص ب DVA:

```
wlan DVA 3 DVA
 aaa-override
 client vlan VLAN0020
security dot1x authentication-list ACS
 session-timeout 1800
 no shutdown
```

تكوين خادم RADIUS على WLC

هذا مثال من التشكيل من ال RADIUS نادل على ال WLC:

```
aaa new-model
!
!
aaa group server radius ACS
 server name ACS
!
aaa authentication dot1x ACS group ACS

radius server ACS
address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
 key Cisco123

dot1x system-auth-control
```

تكوين تجمع DHCP لشبكة VLAN الخاصة بالعميل

هذا مثال من التشكيل من ال DHCP بركة ل الزبون VLAN 30 و VLAN 40:

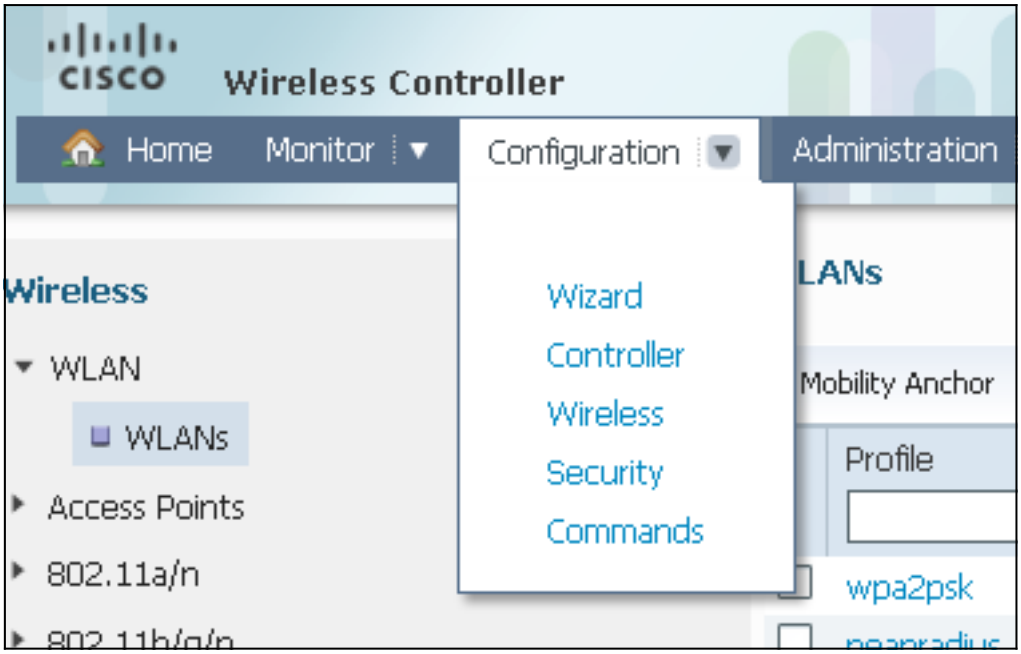
```
interface Vlan30
ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
ip address 40.40.40.1 255.255.255.0

ip dhcp pool vla30
network 30.30.30.0 255.255.255.0
 default-router 30.30.30.1
!
ip dhcp pool vlan40
network 40.40.40.0 255.255.255.0
 default-router 40.40.40.1

ip dhcp snooping vlan 30,40
ip dhcp snooping
```

تكوين WLC باستخدام GUI

تكوين WLAN

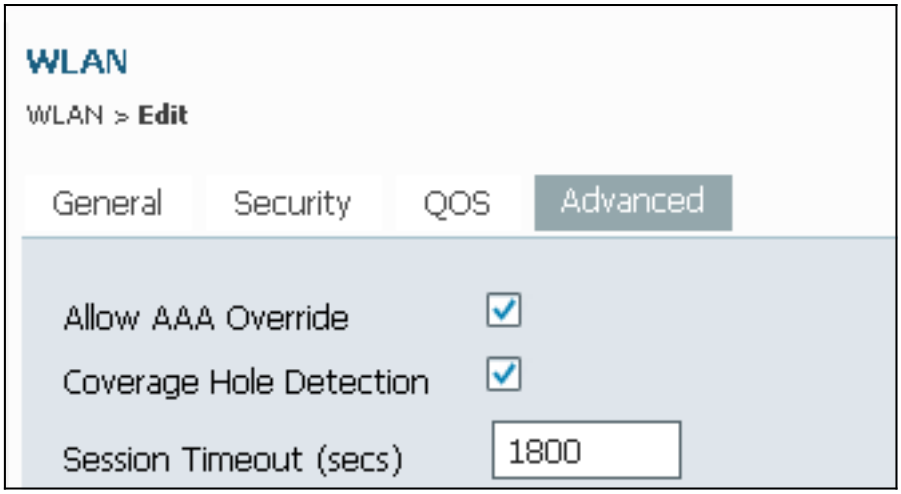
يصف هذا الإجراء كيفية تكوين شبكة WLAN.

1. انتقل إلى **التكوين** > **لاسلكي** > **WLAN** > علامة التبويب **جديد**.

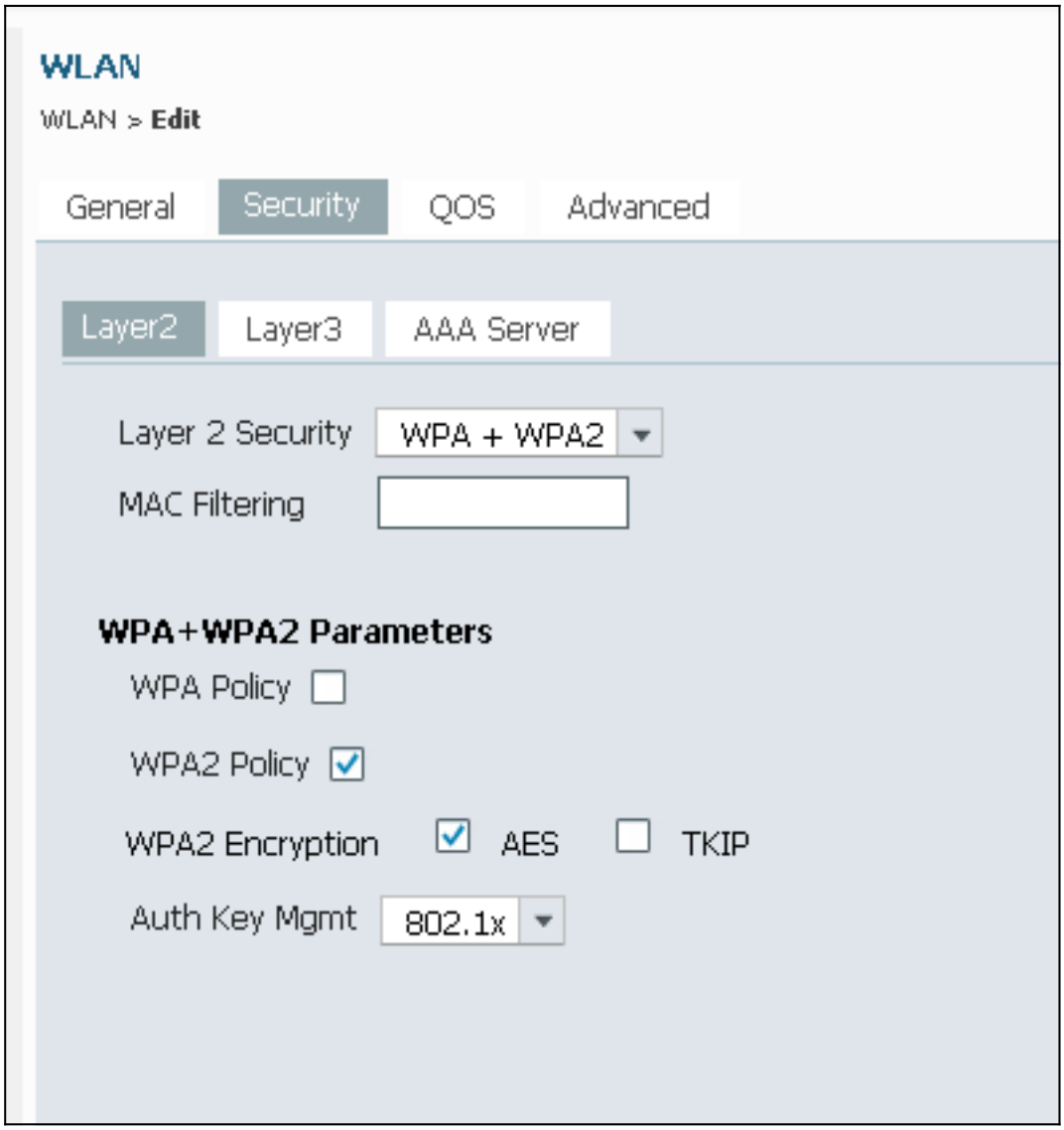


2. انقر فوق علامة التبويب **عام** لترى أن شبكة WLAN تم تكوينها ل WPA2-802.1X، وترجمة الواجهة/مجموعة (G) إلى شبكة VLAN رقم 20 (**VLAN0020**).

3. انقر فوق علامة التبويب **خيارات متقدمة**، وحدد خانة الاختيار **السماح بتجاوز AAA**. يجب تمكين التجاوز لهذه الميزة للعمل.



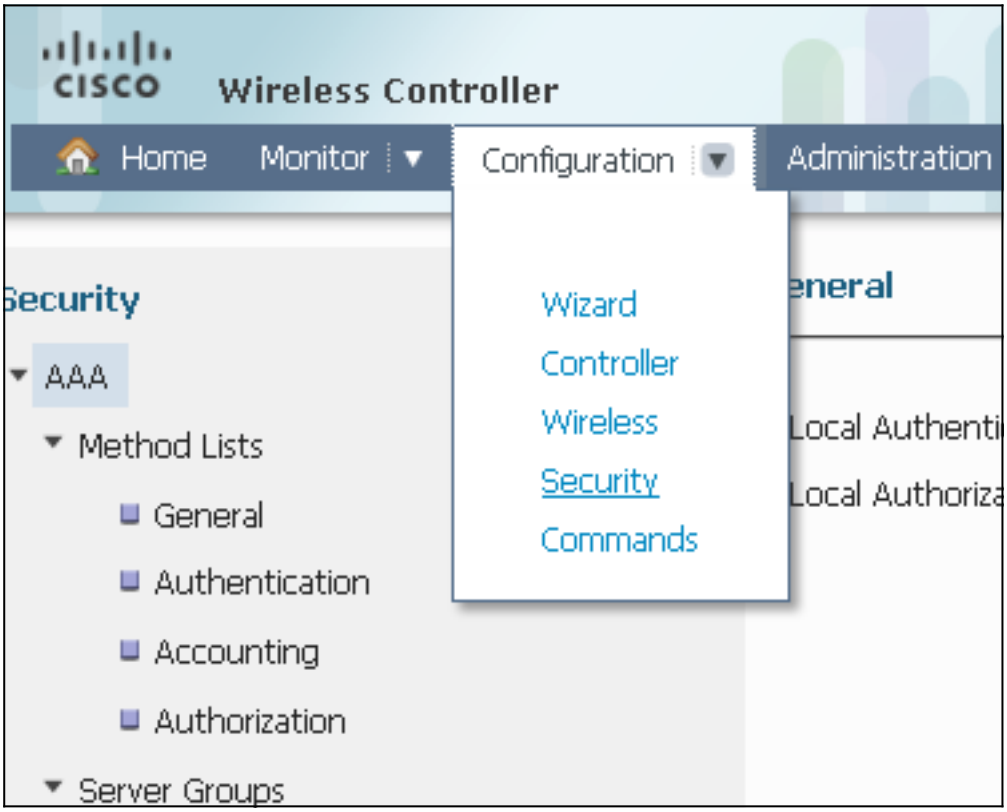
4. انقر فوق علامة التبويب **تأمين** وعلامة التبويب **الطبقة 2**، وحدد خانة الاختيار تشفير **AES** WPA2، وحدد **802.1x** من القائمة المنسدلة لإدارة مفاتيح المصادقة.



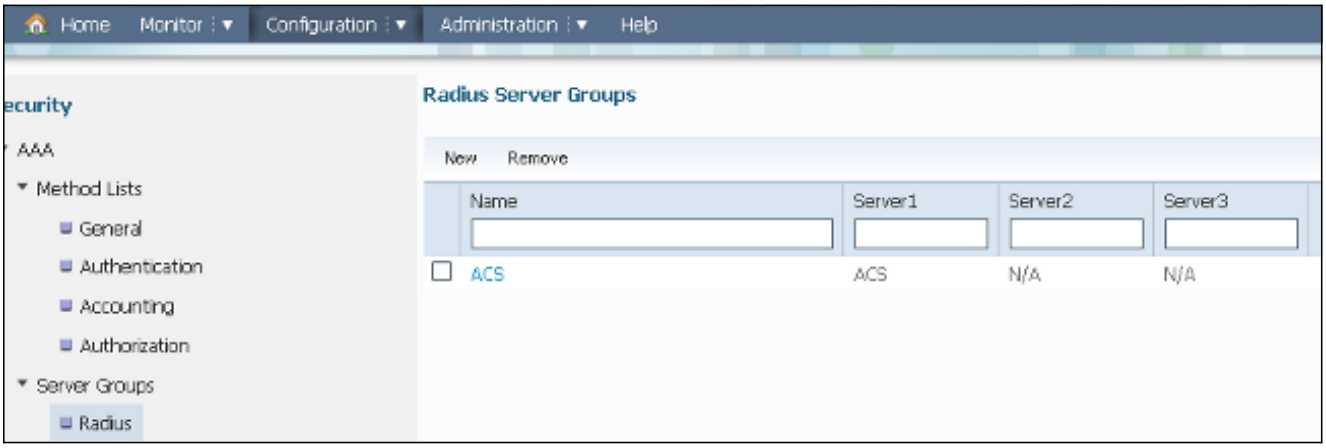
تكوين خادم RADIUS على WLC

يصف هذا الإجراء كيفية تكوين خادم RADIUS على WLC.

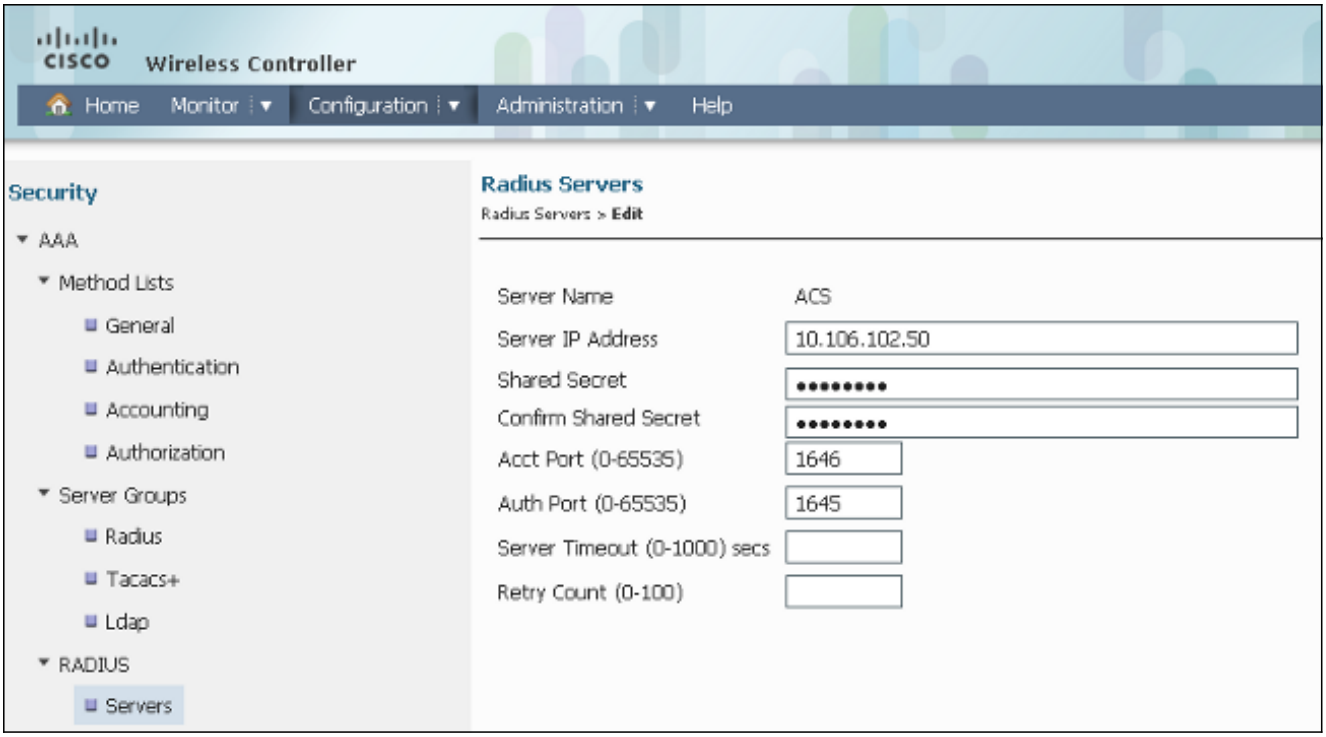
1. انتقل إلى **التكوين > علامة تبويب الأمان**.



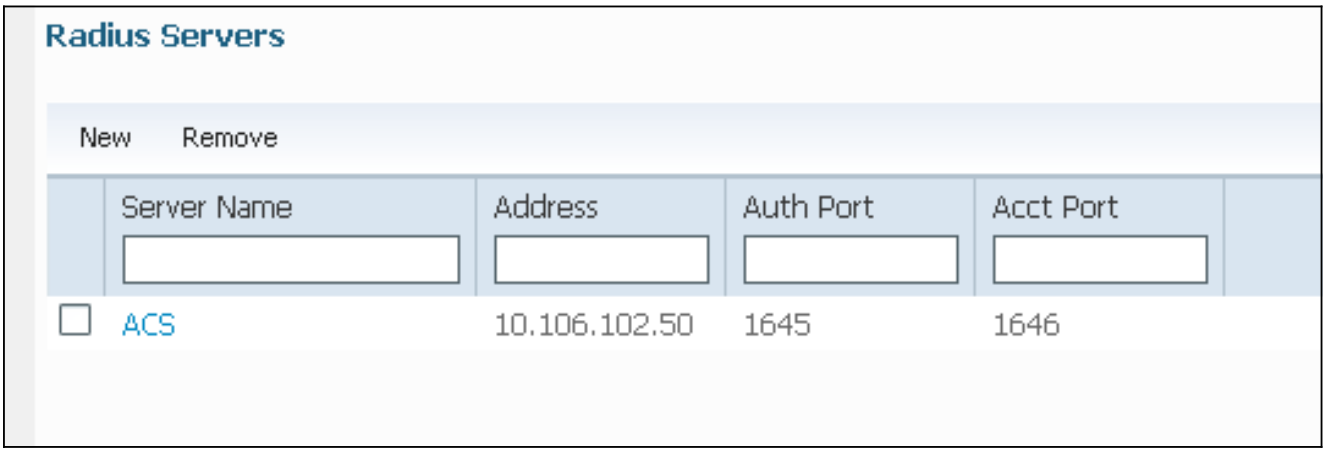
انتقل إلى **AAA > مجموعات الخوادم > RADIUS** لإنشاء مجموعات خوادم RADIUS. في هذا المثال، تسمى2 مجموعة خوادم RADIUS ACS.



قم بتحرير إدخال خادم RADIUS لإضافة عنوان IP الخاص بالخادم والسر المشترك. يجب أن يطابق هذا السر3. المشترك السر المشترك على ال WLC وخادم RADIUS.



هذا مثال على تكوين كامل:

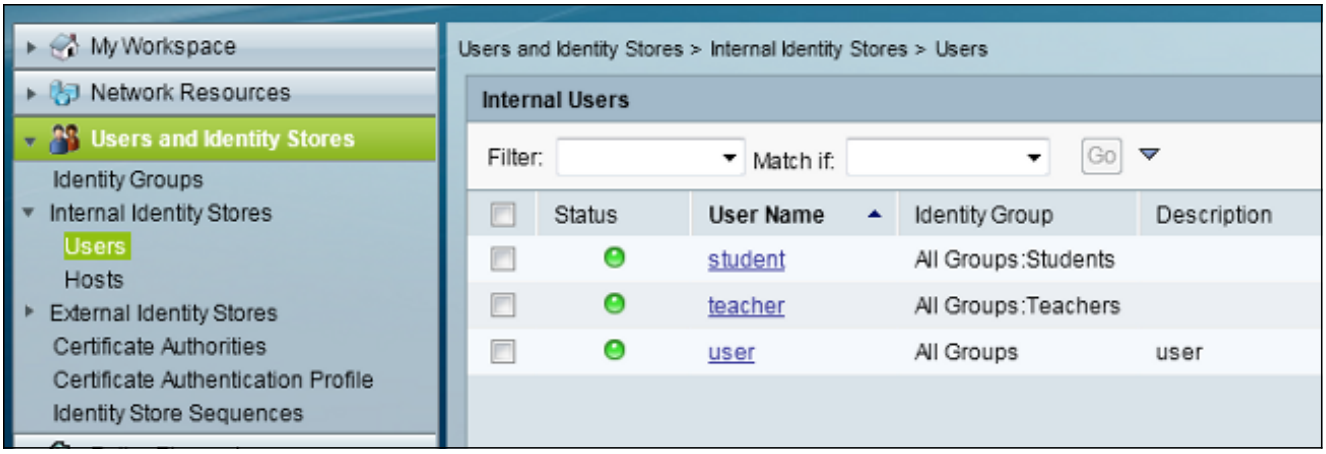


تكوين خادم RADIUS

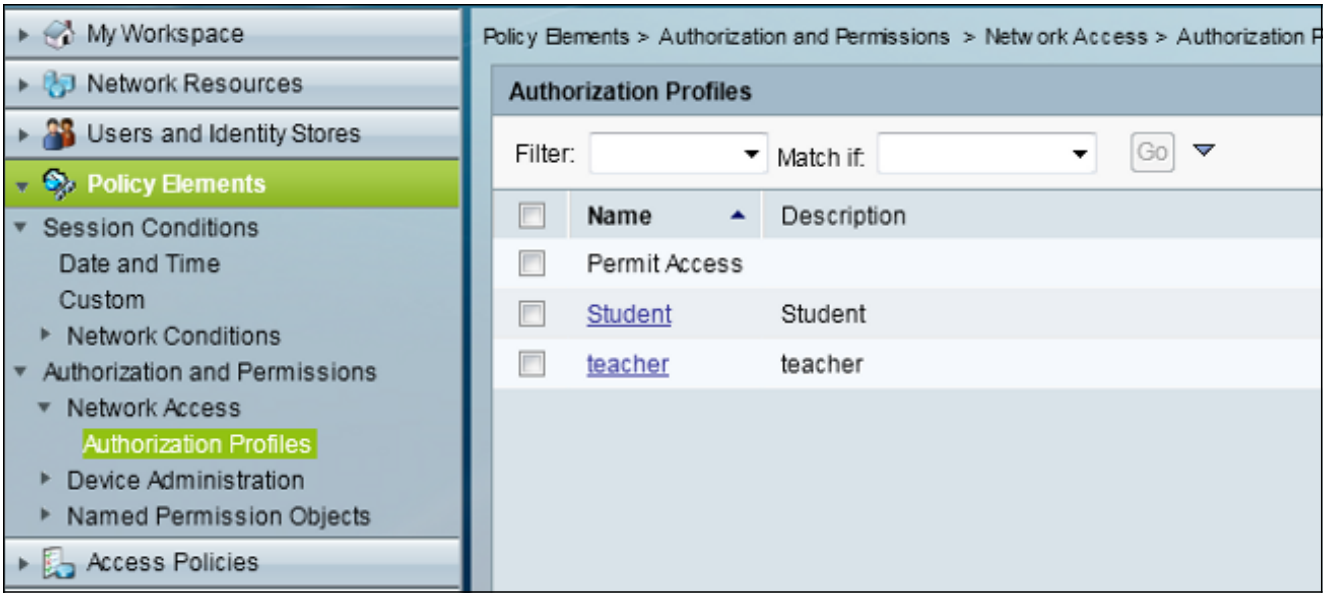
يوضح هذا الإجراء كيفية تكوين خادم RADIUS.

1. على خادم RADIUS، انتقل إلى **المستخدمين ومخازن الهوية > مخازن الهوية الداخلية > المستخدمين**.

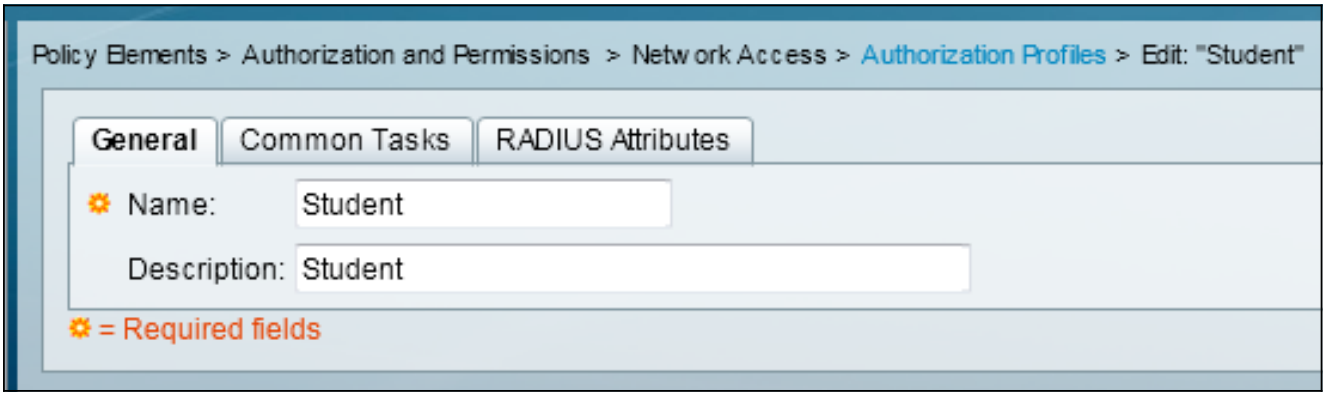
2. قم بإنشاء أسماء المستخدمين ومجموعات الهوية المناسبة. في هذا المثال، الطلاب والمجموعات كافة:الطلاب والمعلمين وكافة المجموعات:المعلمون.



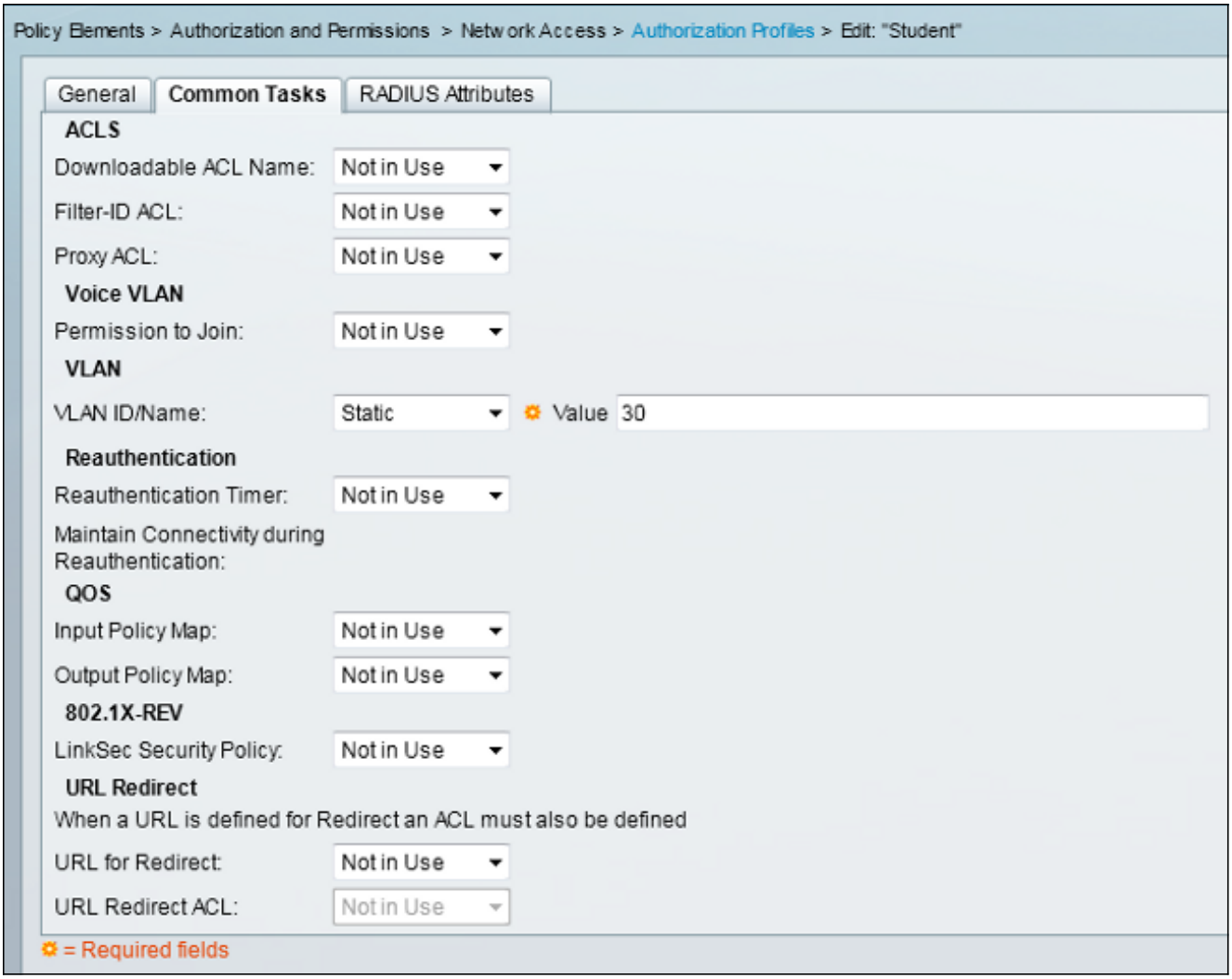
3. انتقل إلى **عناصر السياسة > التفويض والأذونات > الوصول إلى الشبكة>ملفات تعريف التفويض**، ثم قم بإنشاء ملفات تعريف التفويض لتجاوز AAA.



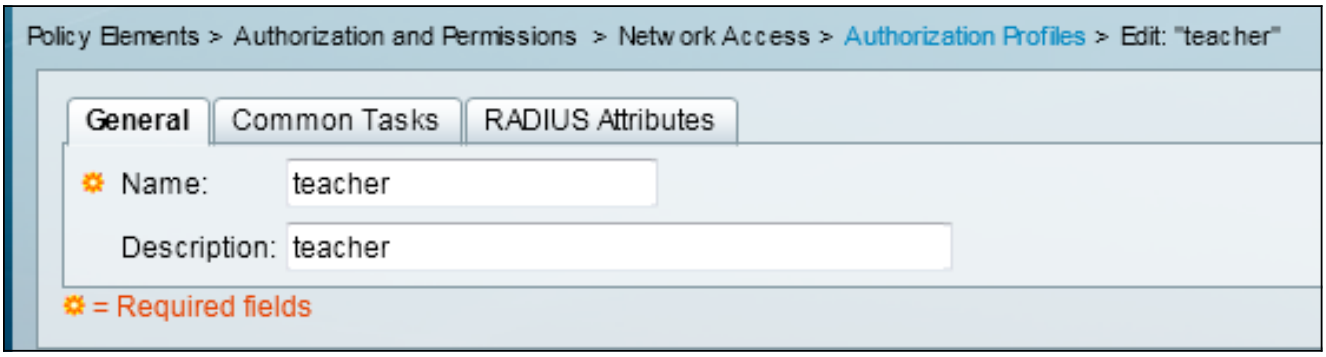
4. تحرير ملف تعريف التخويل للطالب.



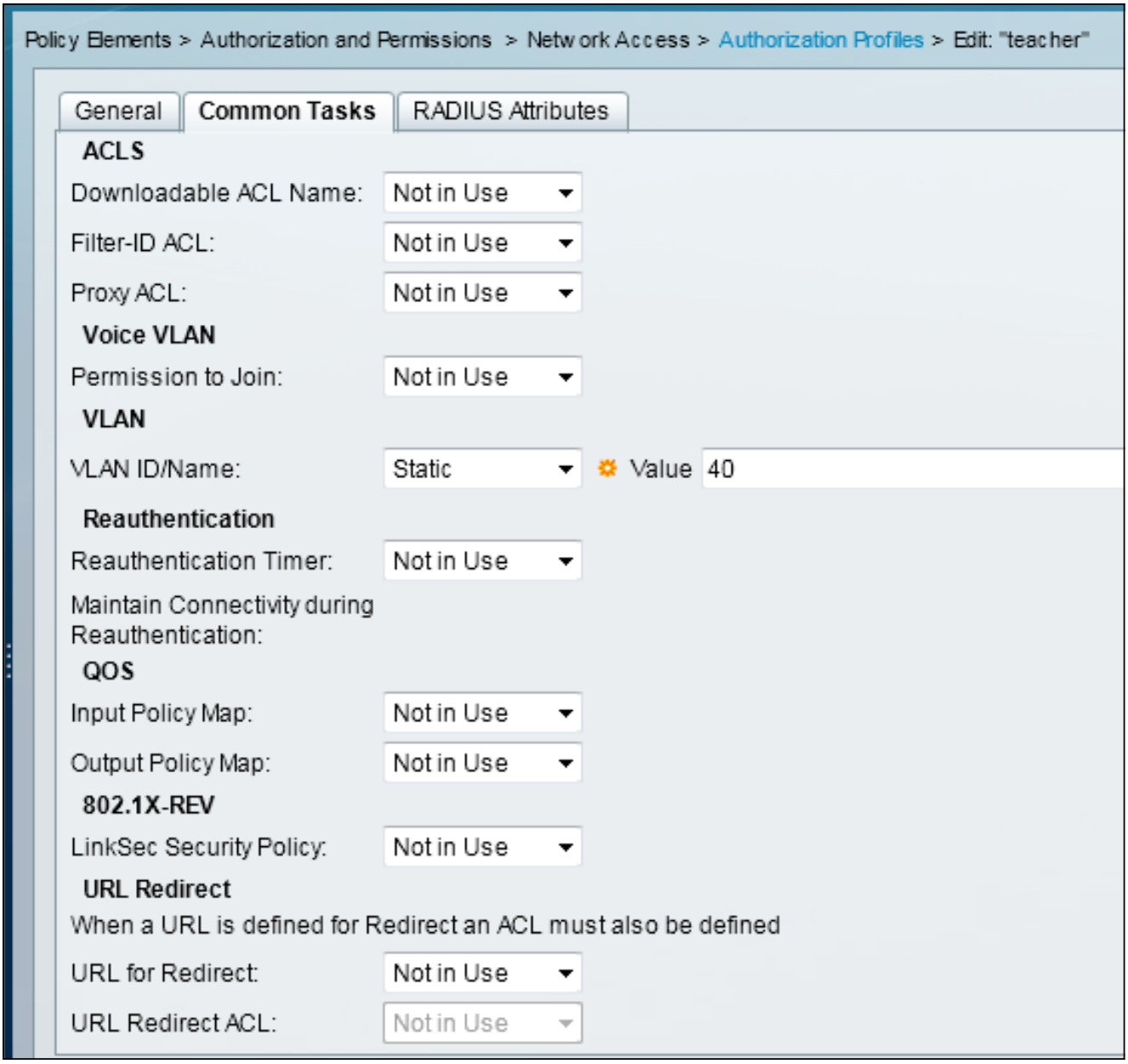
5. ثبت ال VLAN id/name **ساكن إستاتيكي** مع قيمة **30** (VLAN 30).



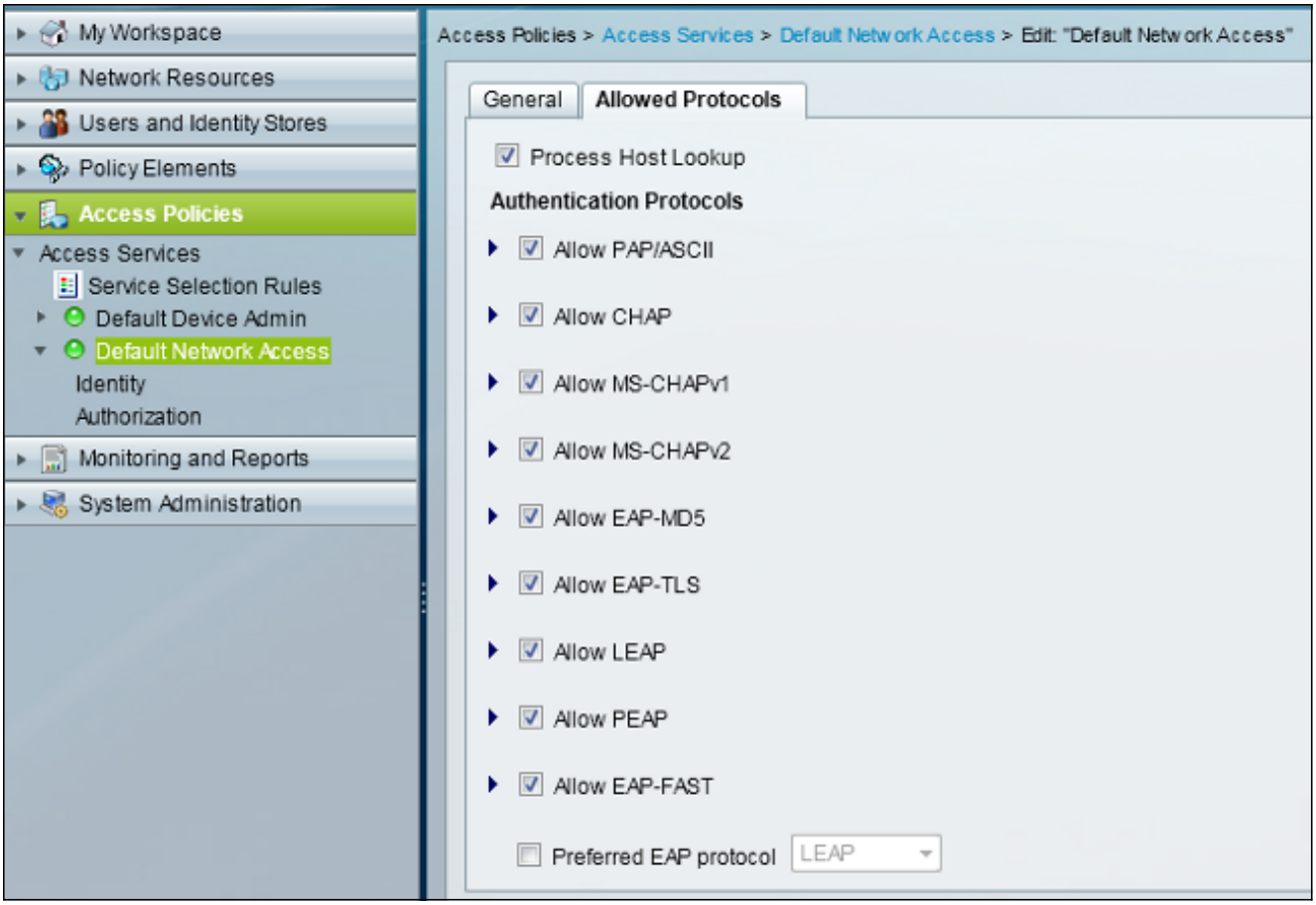
6. تحرير ملف تعريف التخويل للمعلم.



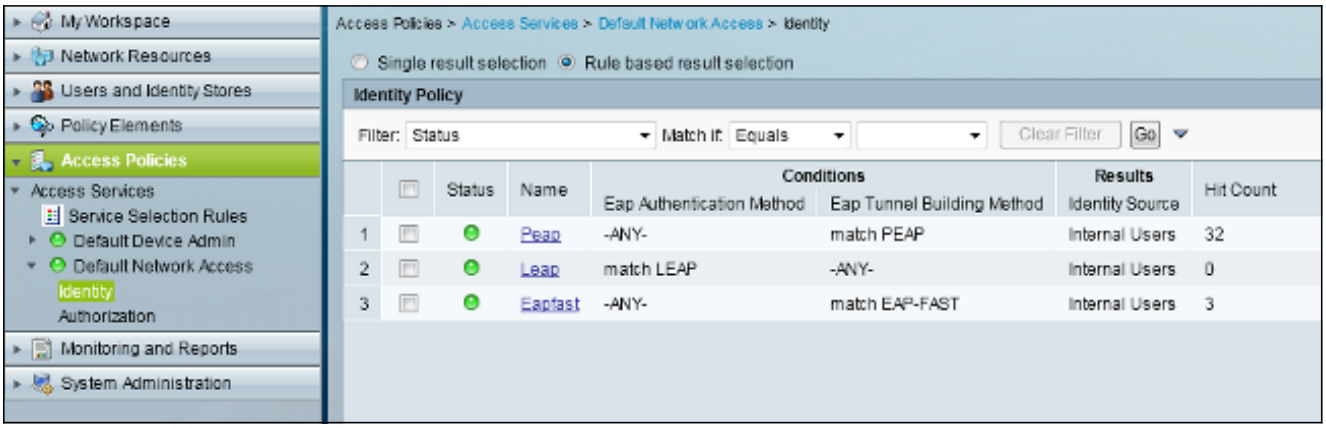
7. ثبت ال VLAN id/name **ساكن إستاتيكي** مع قيمة **40** (VLAN 40).



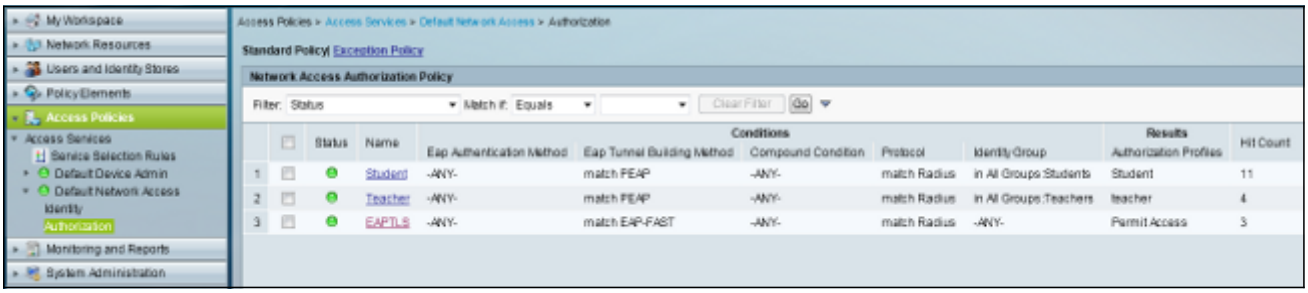
8. انتقل إلى **سياسات الوصول>خدمات الوصول>الوصول الافتراضي إلى الشبكة**، وانقر فوق علامة التبويب **البروتوكولات المسموح بها**. حدد خانة الاختيار **السماح PEAP**.



9. انتقل إلى **الهوية**، وحدد القواعد للسماح لمستخدمي PEAP.



10. انتقل إلى **التفويض**، وقم بتعيين الطالب والمعلم إلى سياسة التخويل؛ في هذا المثال، يجب أن يكون التخطيط طالبا لشبكة VLAN رقم 30 ومعلما لشبكة VLAN رقم 40.

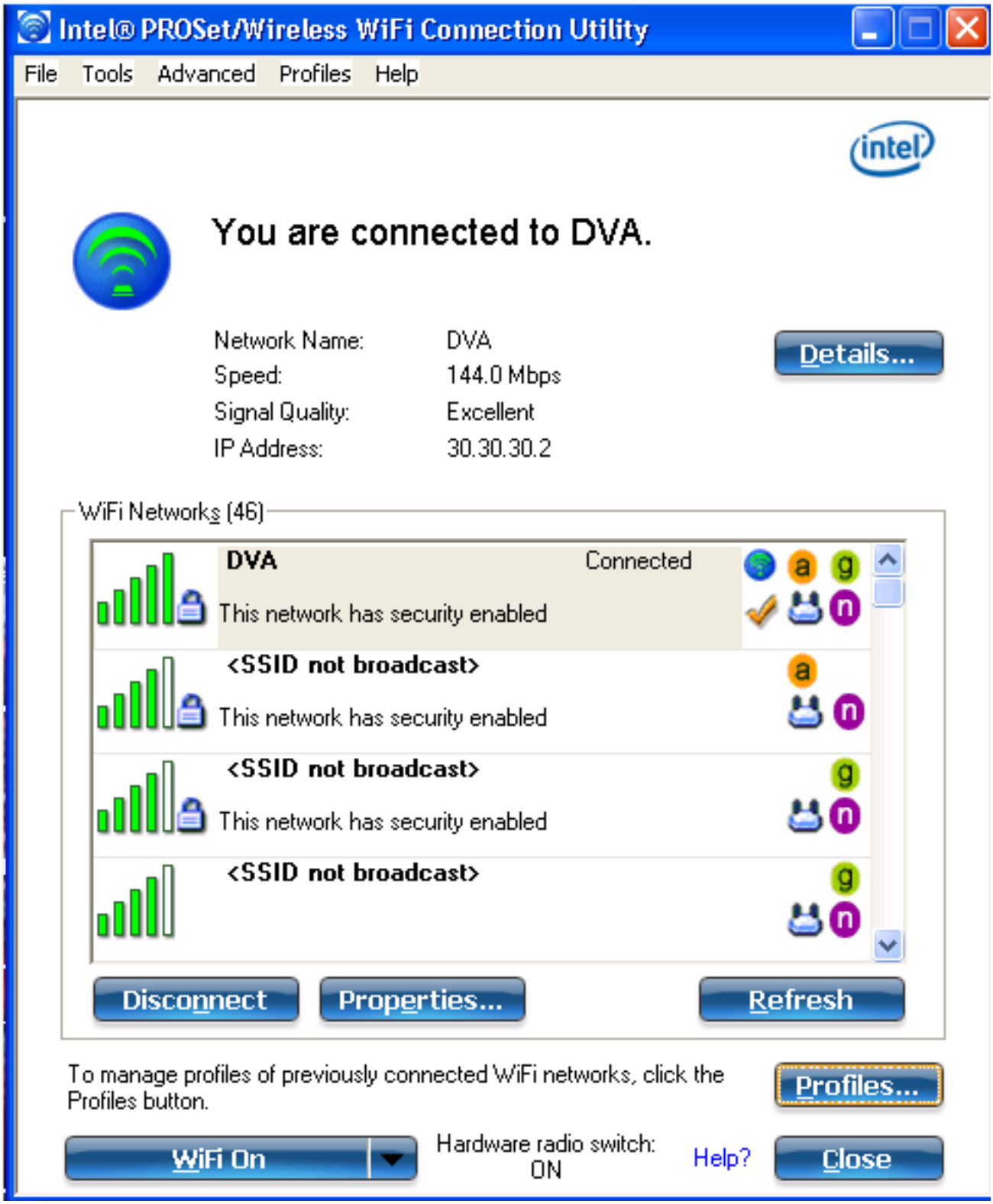


التحقق من الصحة

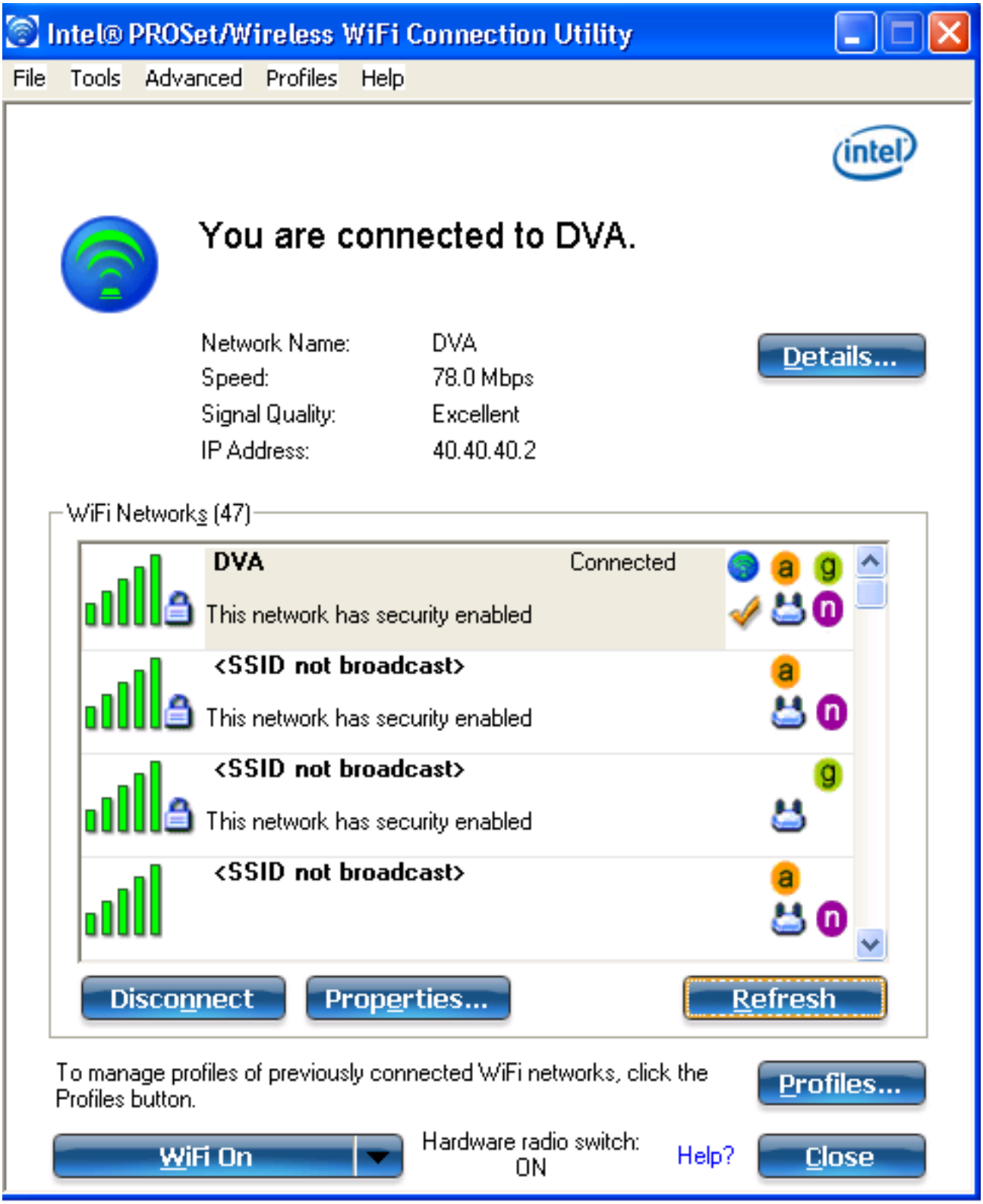
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح. وهذه هي عمليات التحقق:

- راقبت الصفحة على ال ACS أن يبدي أي زبون يكون مصدق.

- التوصيل بشبكة DVA WLAN مع مجموعة الطلاب، ومراجعة أداة توصيل WiFi المساعدة للعميل.



- اتصل بشبكة DVA WLAN مع مجموعة المعلم، وراجع أداة توصيل WiFi المساعدة للعميل.



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظات:

استخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المُستخدمة في هذا القسم.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

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

تتضمن تصحيح الأخطاء المفيدة **تصحيح أخطاء العميل** *mac* **mac-address**، بالإضافة إلى أوامر تتبع NGWC هذه:

- **تعيين تصحيح أخطاء مستوى مجموعة التتبع اللاسلكية-العميل**
- **تعيين مرشح مجموعة-لاسلكية-عميل** *xxxx.xxx.xxxx*
- **show trace sys-filtered-trace**

لا يتضمن تتبع NGWC dot1x/AAA، لذلك أستخدم قائمة التتبع المجمع هذه بالكامل ل dot1x/AAA:

- **تعيين تصحيح أخطاء مستوى مجموعة التتبع اللاسلكية-العميل**
- **set trace wcm-dot1x مستوى الحدث debug**
- **set trace wcm-dot1x aaa مستوى debug**
- **ضبط تصحيح أخطاء مستوى أحداث AAA اللاسلكية للتتبع**
- **تعيين تصحيح أخطاء مستوى SM الأساسي لجلسة وصول التتبع**
- **تعيين تتبع طريقة الوصول إلى جلسة عمل dot1x مستوى تصحيح الأخطاء**
- **تعيين مرشح مجموعة-لاسلكية-عميل** *xxxx.xxx.xxxx*
- **ضبط تتبع wcm-dot1x مرشح حدث** *xxxx.xxx.xxxx* **mac**
- **ضبط تتبع wcm-dot1x aaa مرشح** *xxxx.xxx.xxxx* **mac**
- **ضبط مرشح AAA لأحداث اللاسلكي** *xxxx.xxx.xxxx*
- **تعيين مرشح MAC لعامل تصفية** *xxxx.xxx.xxxx* **Trace Access-Session Core sm**
- **ضبط تتبع طريقة الوصول إلى جلسة عمل dot1x مرشح** *xxxx.xxx.xxxx* **mac**
- **show trace sys-filtered-trace**

عندما يعمل تعيين شبكة VLAN الديناميكية بشكل صحيح، يجب أن ترى هذا النوع من المخرجات من تصحيح الأخطاء:

```
(IST 1ccc 5933] 0021.5C8C.C761 1XA: Received Medium tag (0 12:13:28.598 09/01/13
            (Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13
                                                    (Tunnel-Private-Id (30
      IST 1ccd 5933] 0021.5C8C.C761 Tunnel-Group-Id is 30 12:13:28.598 09/01/13]
         IST 1cce 5933] 0021.5C8C.C761 Checking Interface 12:13:28.598 09/01/13]
          Change - Current VlanId: 40 Current Intf: VLAN0040 New Intf: VLAN0030 New
                                                  GroupIntf:  intfChanged: 1
             IST 1ccf 5933] 0021.5C8C.C761 Incrementing the 12:13:28.598 09/01/13]
                          (Reassociation Count 1 for client (of interface VLAN0040
        More--         [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761--
                                          Clearing Address 40.40.40.2 on mobile
   IST 1cd1 5933] 0021.5C8C.C761 Applying new AAA override 12:13:28.598 09/01/13]
                                                  for station  0021.5C8C.C761
    (..IST 1cd2 5933] 0021.5C8C.C761 Override values (cont 12:13:28.598 09/01/13]
                          dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                    '' :vlanIfName: 'VLAN0030', aclName

     IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for 12:13:28.598 09/01/13]
                                                          ---  station
   IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies 12:13:28.598 09/01/13]
                                                            to client
    IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for 12:13:28.598 09/01/13]
                                                (Wireless client in WCM(NGWC
      IST 1cd6 5933] 0021.5C8C.C761 Inserting AAA Override 12:13:28.598 09/01/13]
                                                        struct for mobile
                                    MAC:  0021.5C8C.C761 , source 4
```

IST 1cd7 5933] 0021.5C8C.C761 Inserting new RADIUS 12:13:28.598 09/01/13]
override into chain for station 0021.5C8C.C761
(..IST 1cd8 5933] 0021.5C8C.C761 Override values (cont 12:13:28.598 09/01/13]
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
'' :vlanIfName: 'VLAN0030', aclName

More-- [09/01/13 12:13:28.598 IST 1cd9 5933] 0021.5C8C.C761--
:Applying override policy from source Override Summation

(..IST 1cda 5933] 0021.5C8C.C761 Override values (cont 12:13:28.598 09/01/13]
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
'' :vlanIfName: 'VLAN0030', aclName

IST 1cdb 5933] 0021.5C8C.C761 Applying local bridging 12:13:28.598 09/01/13]
'Interface Policy for station 0021.5C8C.C761 - vlan 30, interface 'VLAN0030
IST 1cdc 5933] 0021.5C8C.C761 1XA: Setting reauth timeout 12:13:28.598 09/01/13]
to 1800 seconds from WLAN config
IST 1cdd 5933] 0021.5C8C.C761 1XA: Setting reauth timeout 12:13:28.598 09/01/13]
to 1800 seconds
IST 1cde 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID 12:13:28.598 09/01/13]
(Cache entry (RSN 1
IST 1cdf 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0 12:13:28.598 09/01/13]

(IST 1ae1 5933] 0021.5C8C.C761 1XA: Received Medium tag (0 12:08:59.553 09/01/13]
(Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13
(Tunnel-Private-Id (40
IST 1ae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40 12:08:59.553 09/01/13]
More-- [09/01/13 12:08:59.553 IST 1ae3 5933] 0021.5C8C.C761--
:Checking Interface Change - Current VlanId: 20 Current Intf: VLAN0020 New Intf
VLAN0040 New GroupIntf: intfChanged: 1
IST 1ae4 5933] 0021.5C8C.C761 Applying new AAA override for 12:08:59.553 09/01/13]
station 0021.5C8C.C761
(..IST 1ae5 5933] 0021.5C8C.C761 Override values (cont 12:08:59.553 09/01/13]
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
'' :vlanIfName: 'VLAN0040', aclName

IST 1ae6 5933] 0021.5C8C.C761 Clearing Dhcp state for 12:08:59.553 09/01/13]
--- station
IST 1ae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies 12:08:59.553 09/01/13]
to client
IST 1ae8 5933] 0021.5C8C.C761 No Interface ACL used for 12:08:59.553 09/01/13]
(Wireless client in WCM(NGWC
IST 1ae9 5933] 0021.5C8C.C761 Inserting AAA Override struct 12:08:59.553 09/01/13]
for mobile
MAC: 0021.5C8C.C761 , source 4

IST 1aea 5933] 0021.5C8C.C761 Inserting new RADIUS override 12:08:59.553 09/01/13]
into chain for station 0021.5C8C.C761
(..IST 1aeb 5933] 0021.5C8C.C761 Override values (cont 12:08:59.553 09/01/13]
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
'' :vlanIfName: 'VLAN0040', aclName
--More--
IST 1aec 5933] 0021.5C8C.C761 Applying override policy 12:08:59.553 09/01/13]
:from source Override Summation

(..IST 1aed 5933] 0021.5C8C.C761 Override values (cont 12:08:59.553 09/01/13]
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
'' :vlanIfName: 'VLAN0040', aclName

IST 1aee 5933] 0021.5C8C.C761 Applying local bridging 12:08:59.553 09/01/13]
'Interface Policy for station 0021.5C8C.C761 - vlan 40, interface 'VLAN0040
IST 1aef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout 12:08:59.553 09/01/13]
to 1800 seconds from WLAN config

IST 1af0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout 12:08:59.553 09/01/13]
to 1800 seconds
IST 1af1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID 12:08:59.553 09/01/13]
(Cache entry (RSN 1

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).