Configuration de l'affectation dynamique de VLAN avec NGWC et ACS 5.2

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Affectation de VLAN dynamique avec le serveur RADIUS](#)
[Configuration](#)
[Diagramme du réseau](#)
[Hypothèses](#)
[Configuration du WLC avec CLI](#)
[Configurer WLAN](#)
[Configurer le serveur RADIUS sur WLC](#)
[Configurer le pool DHCP pour le VLAN client](#)
[Configuration du WLC avec l'interface graphique utilisateur](#)
[Configurer WLAN](#)
[Configurer le serveur RADIUS sur WLC](#)
[Configurer le serveur RADIUS](#)
[Vérification](#)
[Dépannage](#)

Introduction

Ce document décrit le concept d'affectation de VLAN dynamique. Il décrit également comment configurer le contrôleur de réseau local sans fil (WLC) et un serveur RADIUS afin d'affecter des clients de réseau local sans fil (WLAN) à un VLAN spécifique de manière dynamique. Dans ce document, le serveur RADIUS est un serveur de contrôle d'accès (ACS) qui exécute Cisco Secure Access Control System Version 5.2.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base du WLC et des points d'accès légers (LAP)

- Connaissance fonctionnelle du serveur AAA (Authentication, Authorization and Accounting)
- Avoir une connaissance complète des réseaux sans fil et des problèmes liés à la sécurité sans fil

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur LAN sans fil Cisco 5760 avec logiciel Cisco IOS® XE version 3.2.2 (armoire de câblage nouvelle génération ou NGWC)
- Point d'accès allégé de la gamme Cisco Aironet 3602
- Microsoft Windows XP avec Intel Proset Supplicator
- Cisco Secure Access Control System version 5.2
- Commutateur de la gamme Cisco Catalyst 3560

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Affectation de VLAN dynamique avec le serveur RADIUS

Dans la plupart des systèmes WLAN, chaque WLAN a une stratégie statique qui s'applique à tous les clients associés à un SSID (Service Set Identifier), ou WLAN dans la terminologie du contrôleur. Bien que puissante, cette méthode a des limitations parce qu'elle exige que les clients soient associés à des SSID différents afin d'hériter de QoS et de stratégies de sécurité différentes.

Cependant, la solution WLAN de Cisco prend en charge la mise en réseau d'identités. Cela permet au réseau d'annoncer un SSID unique, mais permet à des utilisateurs spécifiques d'hériter de différentes QoS, attributs VLAN et/ou stratégies de sécurité en fonction des informations d'identification de l'utilisateur.

L'affectation de VLAN dynamique est une fonction qui place un utilisateur sans fil dans un VLAN spécifique en fonction des informations fournies par l'utilisateur. Cette tâche d'affectation des utilisateurs à un VLAN spécifique est gérée par un serveur d'authentification RADIUS, tel qu'un Cisco Secure ACS. Cette fonctionnalité peut être utilisée, par exemple, afin de permettre à l'hôte sans fil de rester sur le même VLAN qu'il se déplace au sein d'un réseau de campus.

Par conséquent, lorsqu'un client tente de s'associer à un LAP enregistré auprès d'un contrôleur, le LAP transmet les informations d'identification de l'utilisateur au serveur RADIUS pour validation. Une fois que l'authentification est réussie, le serveur RADIUS passe certains attributs de l'Internet Engineering Task Force (IETF) à l'utilisateur. Ces attributs RADIUS décident de l'ID de VLAN qui doit être affecté au client sans fil. Le SSID du client (le WLAN, en termes de WLC) n'a pas d'importance car l'utilisateur est toujours affecté à cet ID de VLAN prédéterminé.

Les attributs d'utilisateur RADIUS utilisés pour l'affectation de l'ID de VLAN sont :

- IETF 64 (Tunnel Type) : défini sur VLAN.
- IETF 65 (Tunnel Medium Type) : défini sur 802.
- IETF 81 (Tunnel-Private-Group-ID) - Défini sur l'ID VLAN.

L'ID de VLAN est de 12 bits et prend une valeur comprise entre 1 et 4 094, inclus. Étant donné que l'ID de groupe privé-tunnel est de type chaîne, comme défini dans RFC 2868, Attributs RADIUS pour la prise en charge du protocole de tunnel pour utilisation avec IEEE 802.1X, la valeur entière de l'ID de VLAN est codée en tant que chaîne. Quand ces attributs de tunnel sont envoyés, il est nécessaire de renseigner la zone Tag.

Comme observé dans RFC2868 , section 3.1 :

«Le champ Tag est d'un octet de longueur et est destiné à fournir un moyen de regrouper des attributs dans le même paquet qui font référence au même tunnel. »

Les valeurs valides pour le champ Tag sont 0x01 à 0x1F, inclusivement. Si la zone Tag est inutilisée, elle doit avoir pour valeur zéro (0x00). Référez-vous à RFC 2868 pour plus d'informations sur tous les attributs RADIUS.

Configuration

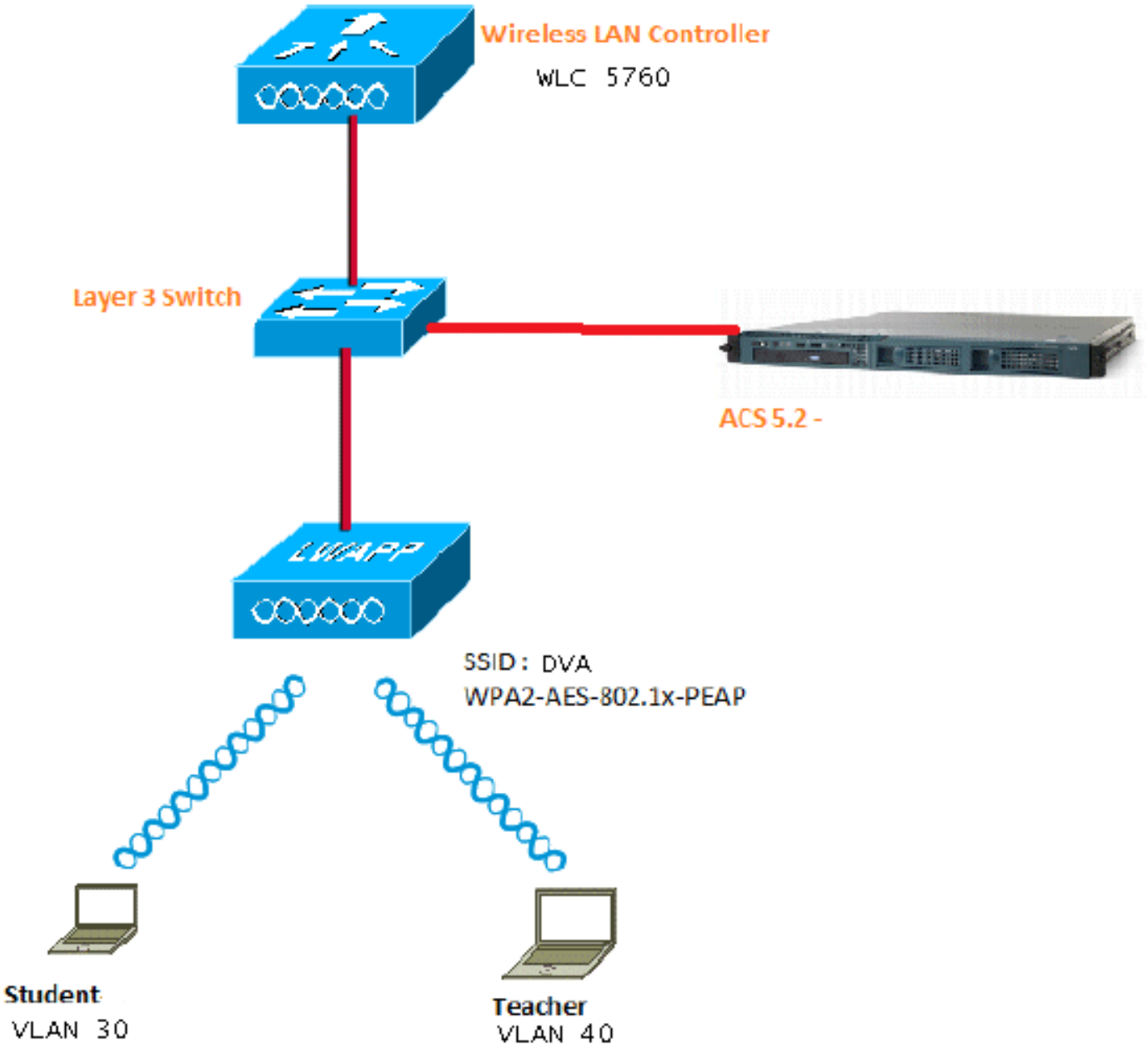
La configuration d'une affectation de VLAN dynamique se compose de deux étapes distinctes :

1. Configurez le WLC à l'aide de l'interface de ligne de commande (CLI) ou de l'interface utilisateur graphique.
2. Configurez le serveur RADIUS.

Note: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Ce document utilise 802.1X avec le protocole PEAP (Protected Extensible Authentication Protocol) comme mécanisme de sécurité.

Hypothèses

- Les commutateurs sont configurés pour tous les VLAN de couche 3 (L3).
- Une étendue DHCP est attribuée au serveur DHCP.
- La connectivité de couche 3 existe entre tous les périphériques du réseau.
- Le LAP est déjà joint au WLC.
- Chaque VLAN a un masque /24.
- ACS 5.2 possède un certificat auto-signé installé.

Configuration du WLC avec CLI

Configurer WLAN

Voici un exemple de configuration d'un WLAN avec le SSID de DVA :

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

Configurer le serveur RADIUS sur WLC

Voici un exemple de configuration du serveur RADIUS sur le 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
```

Configurer le pool DHCP pour le VLAN client

Voici un exemple de configuration du pool DHCP pour les VLAN 30 et 40 du client :

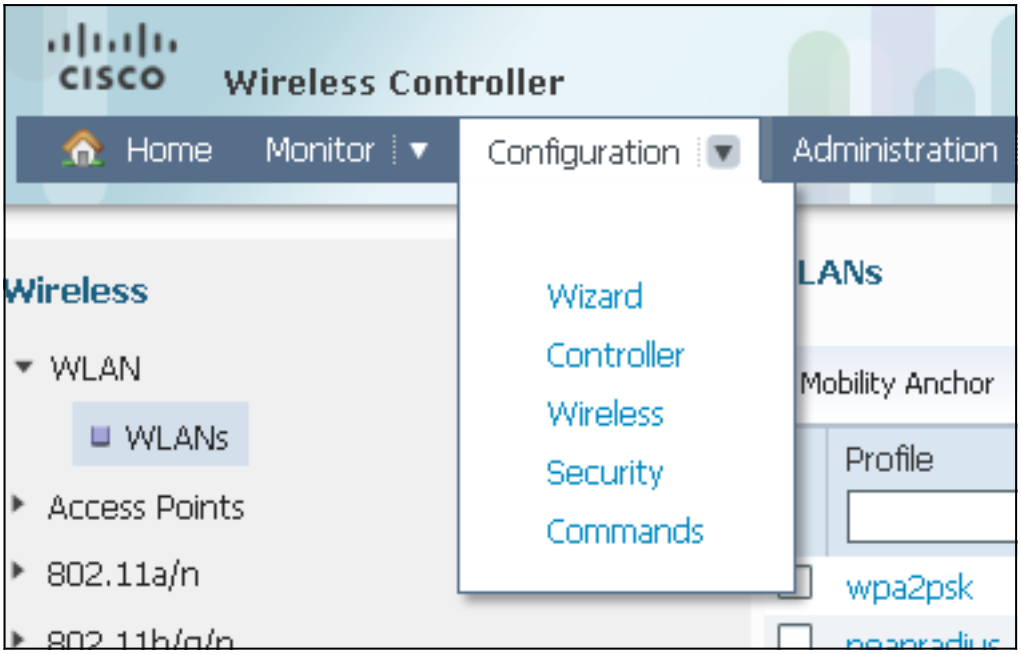
```
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0

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
```

Configuration du WLC avec l'interface graphique utilisateur

Configurer WLAN

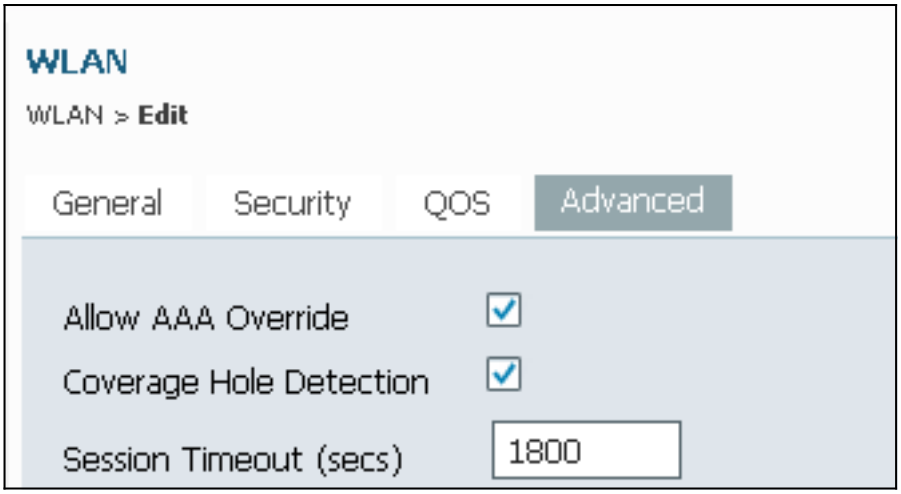
Cette procédure décrit comment configurer le WLAN.

1. Accédez à **Configuration > Wireless > WLAN > NEW** tab.

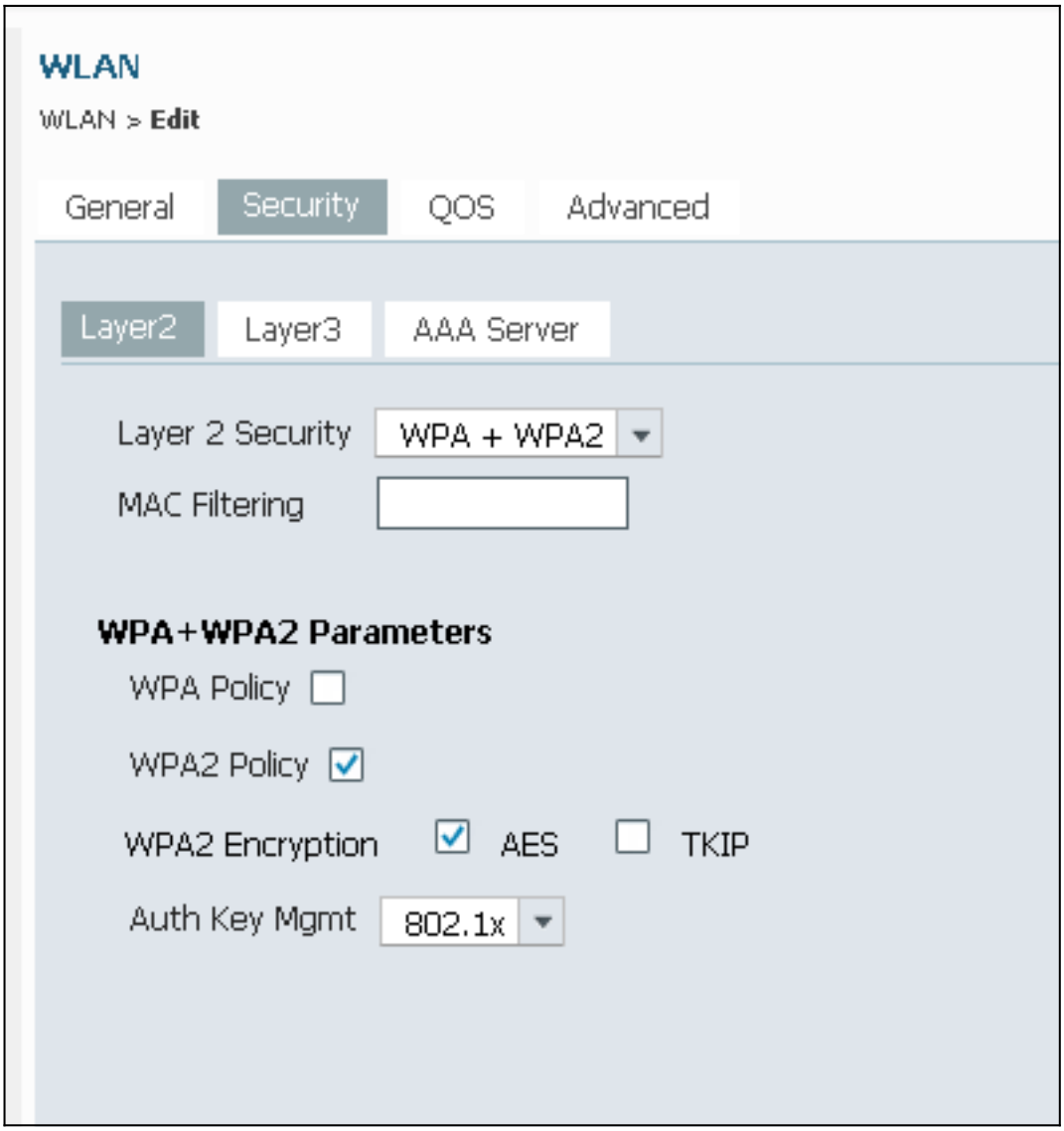


2. Cliquez sur l'onglet **General** afin de voir que le WLAN est configuré pour WPA2-802.1X et mappez l'interface/groupe d'interfaces(G) au VLAN 20 (**VLAN0020**).

3. Cliquez sur l'onglet **Avancé** et cochez la case **Autoriser le remplacement AAA**. La substitution doit être activée pour que cette fonctionnalité fonctionne.



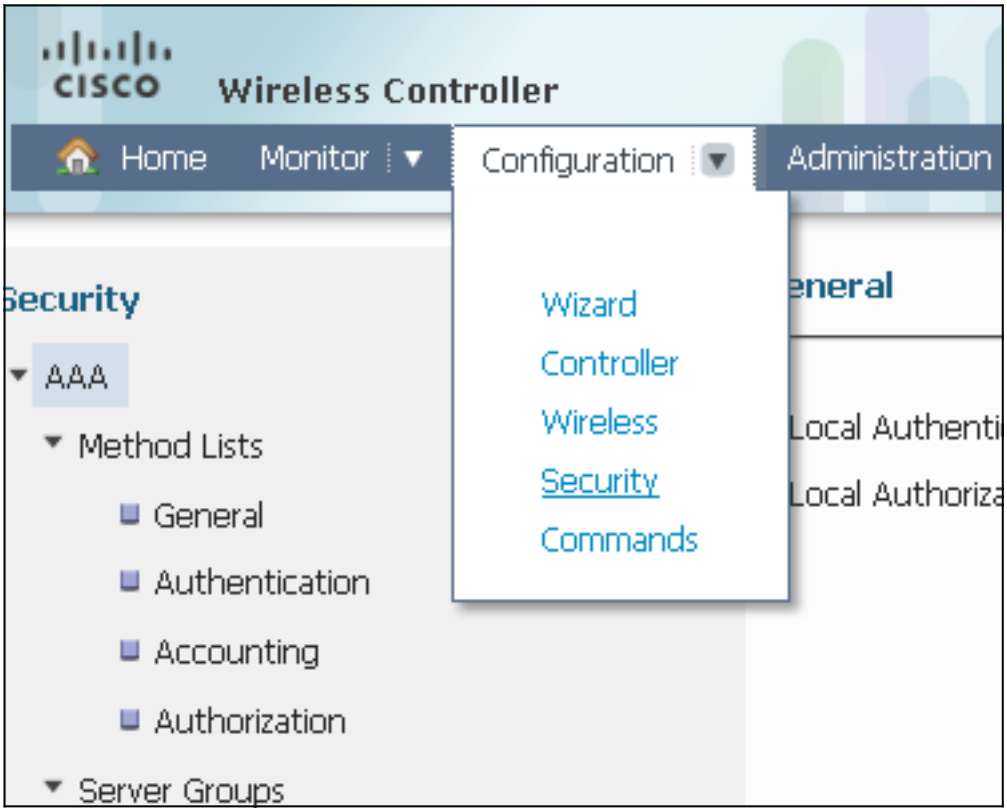
4. Cliquez sur l'onglet **Security** et l'onglet **Layer2**, cochez la case WPA2 Encryption **AES**, puis sélectionnez **802.1x** dans la liste déroulante Auth Key Mgmt.



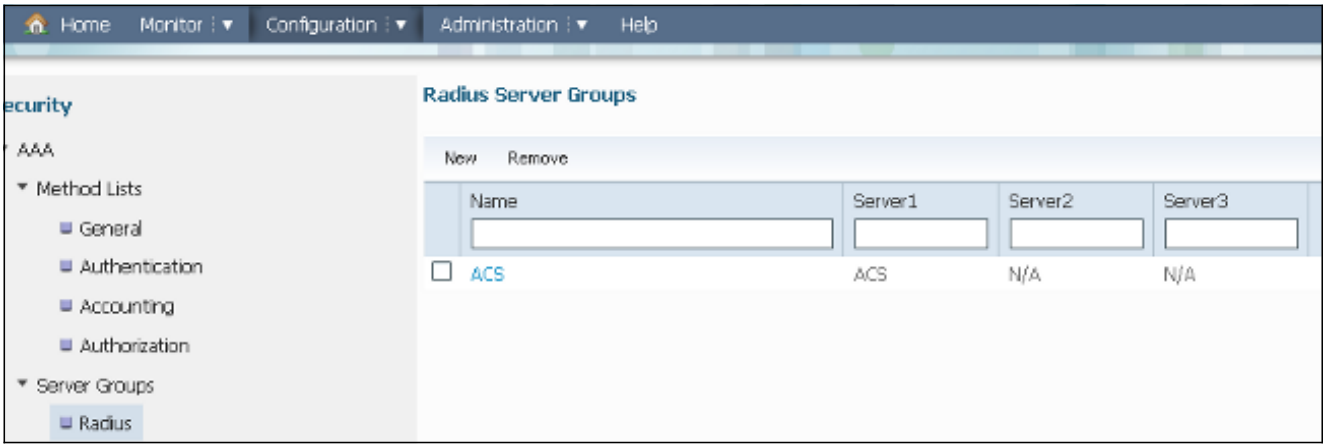
Configurer le serveur RADIUS sur WLC

Cette procédure décrit comment configurer le serveur RADIUS sur le WLC.

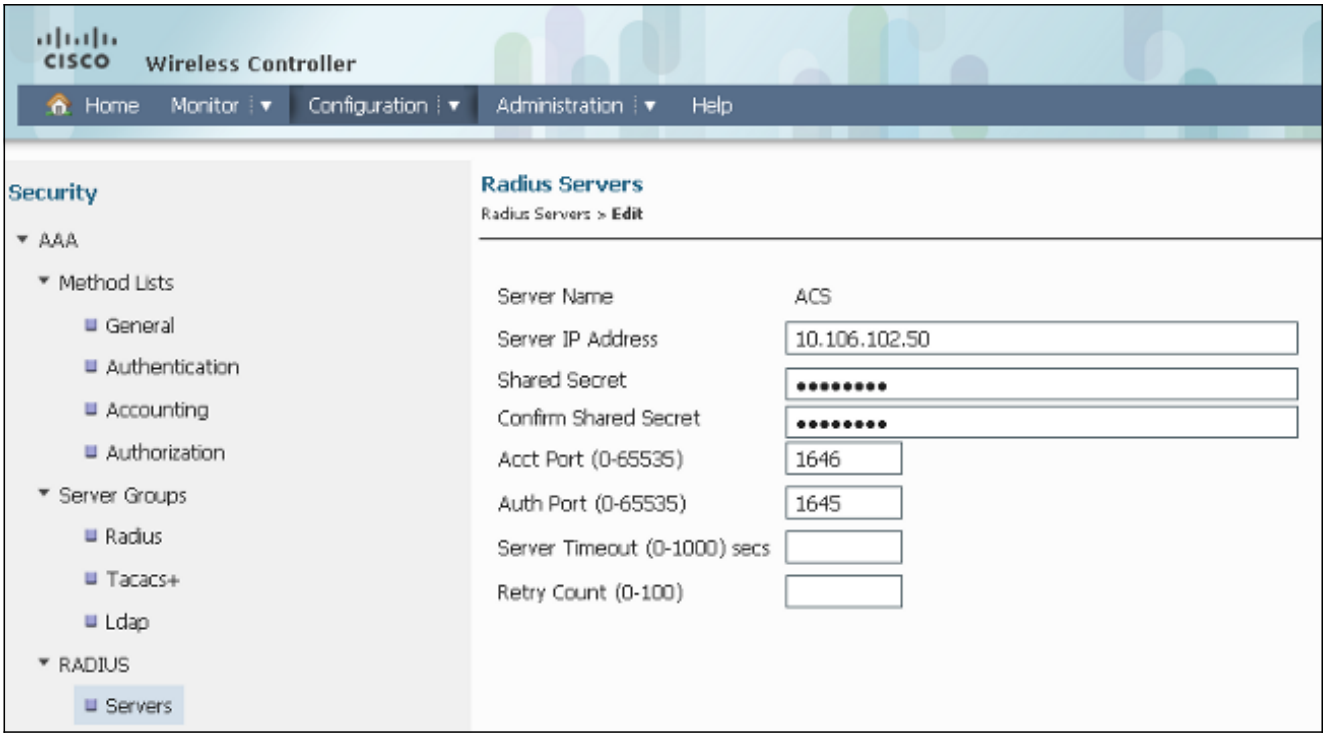
1. Accédez à l'onglet **Configuration > Sécurité**.



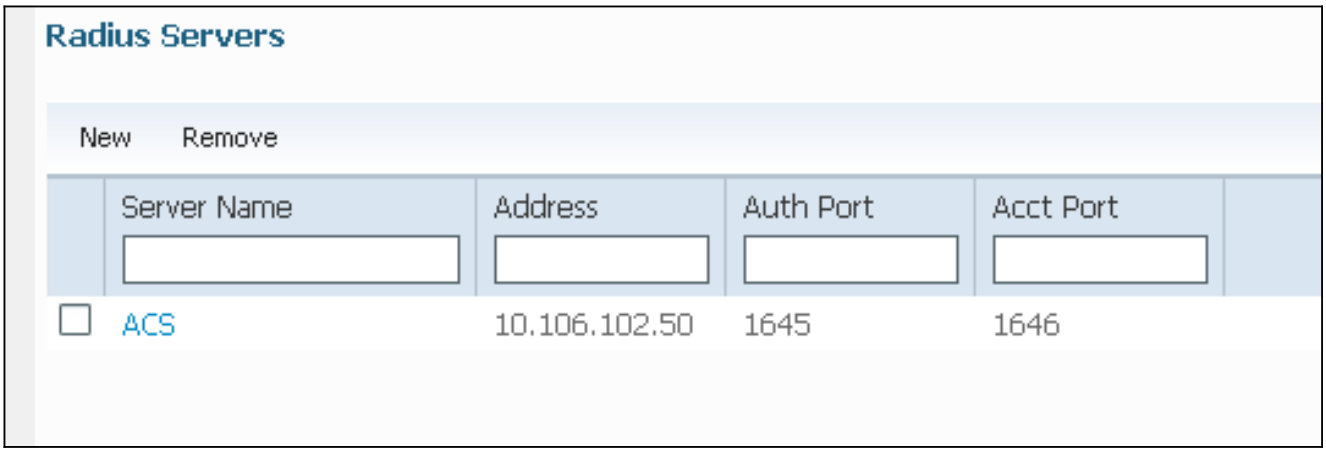
2. Accédez à **AAA > Groupes de serveurs > Radius** afin de créer les groupes de serveurs Radius. Dans cet exemple, le groupe de serveurs Radius est appelé ACS.



3. Modifiez l'entrée Radius Server afin d'ajouter l'adresse IP du serveur et le secret partagé. Ce secret partagé doit correspondre au secret partagé sur le WLC et le serveur RADIUS.



Voici un exemple de configuration complète :

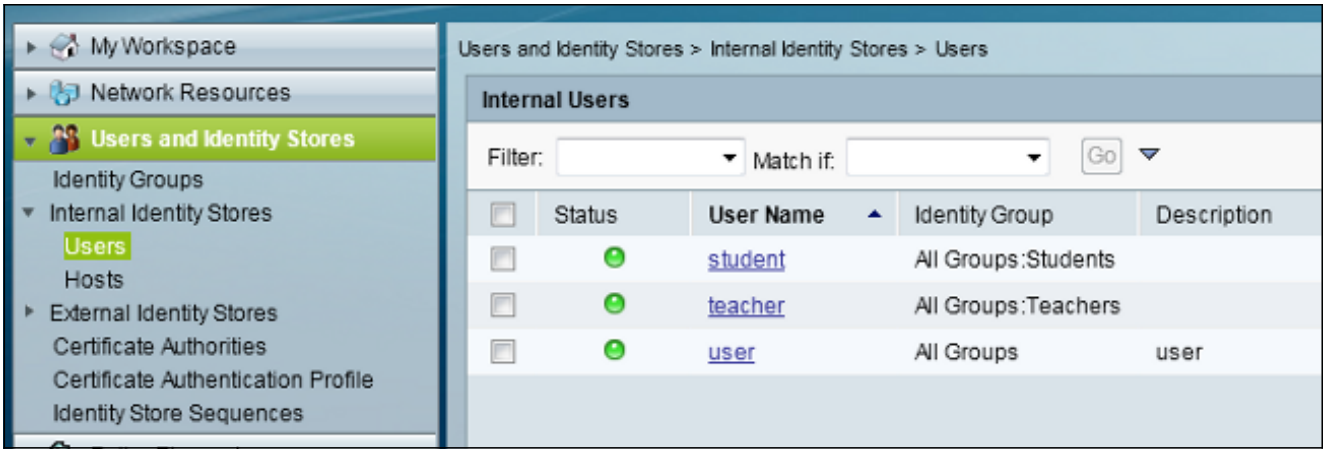


Configurer le serveur RADIUS

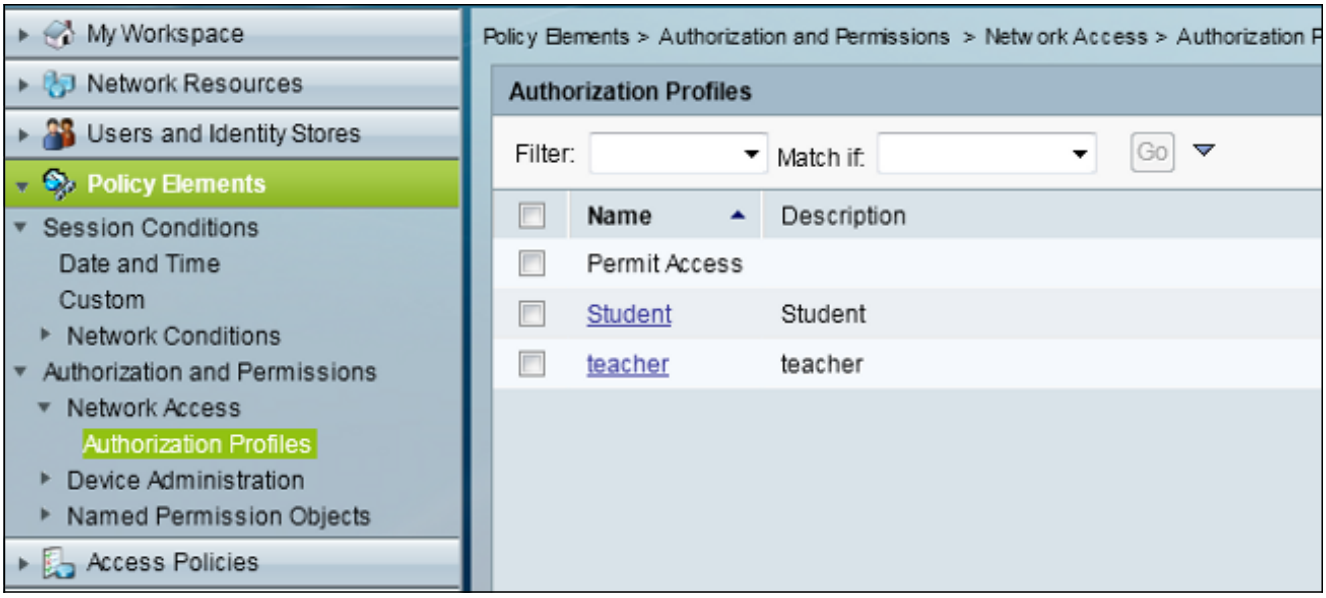
Cette procédure décrit comment configurer le serveur RADIUS.

1. Sur le serveur RADIUS, accédez à **Utilisateurs et magasins d'identités > Magasins d'identités internes > Utilisateurs**.

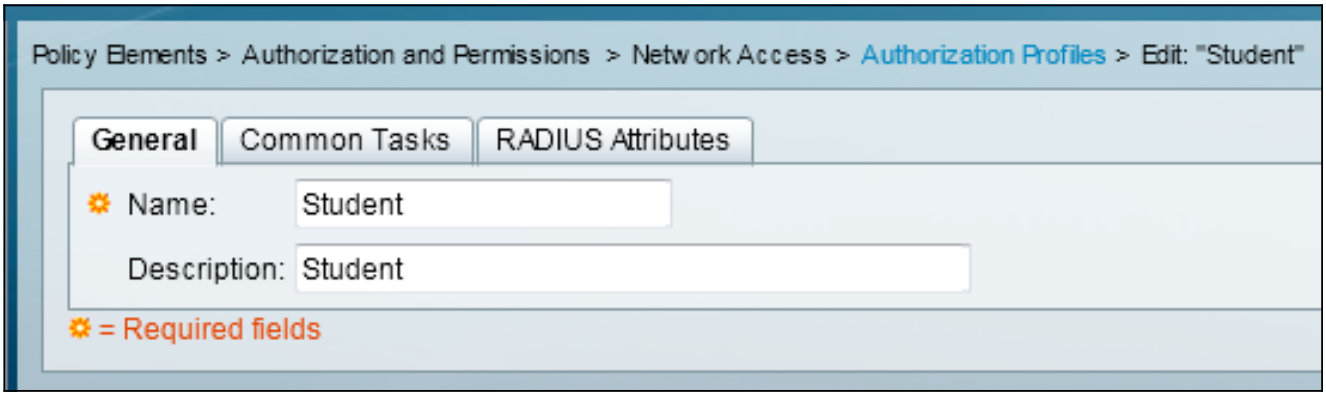
2. Créez les noms d'utilisateur et les groupes d'identités appropriés. Dans cet exemple, il s'agit de Student et All Groups:Students, et Teacher et AllGroups:Teachers.



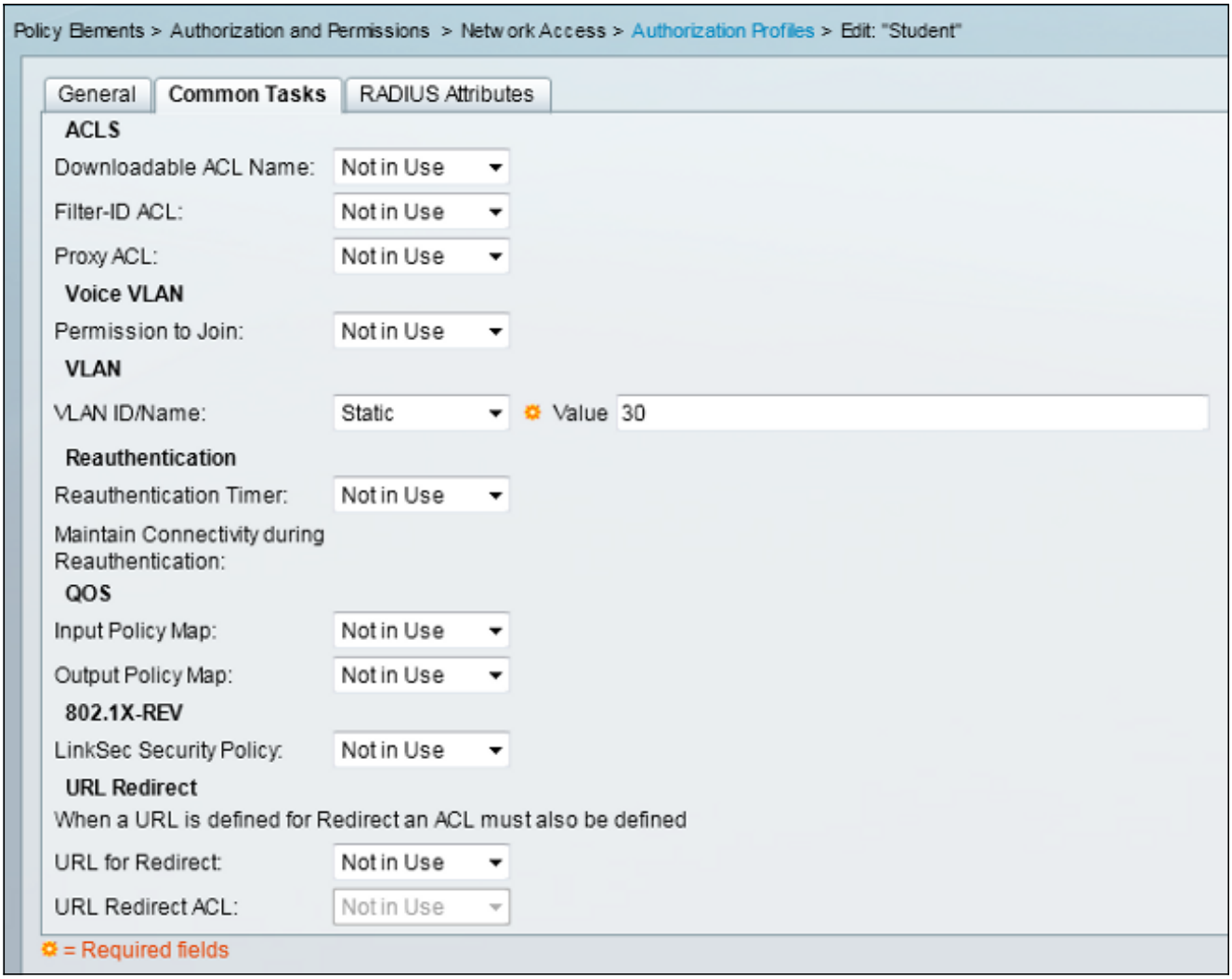
3. Accédez à **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles** et créez les profils d'autorisation pour AAA override.



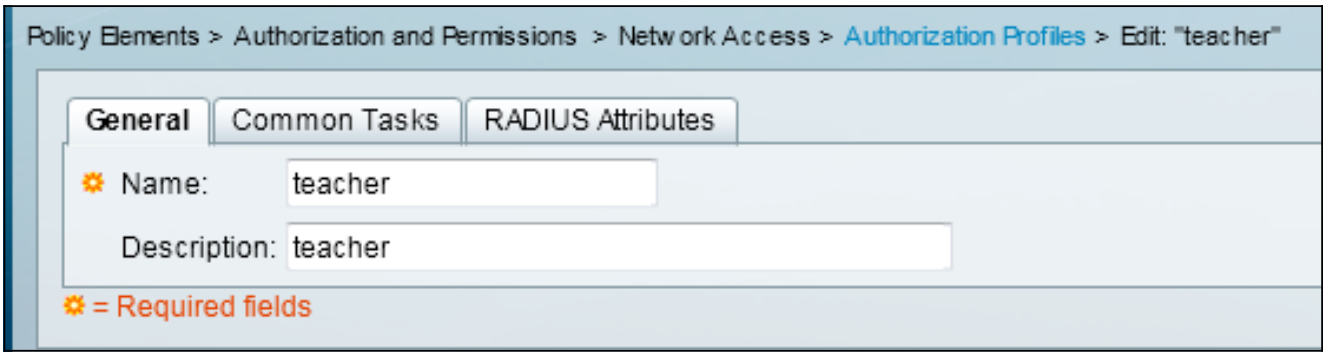
4. Modifiez le profil d'autorisation de l'étudiant.



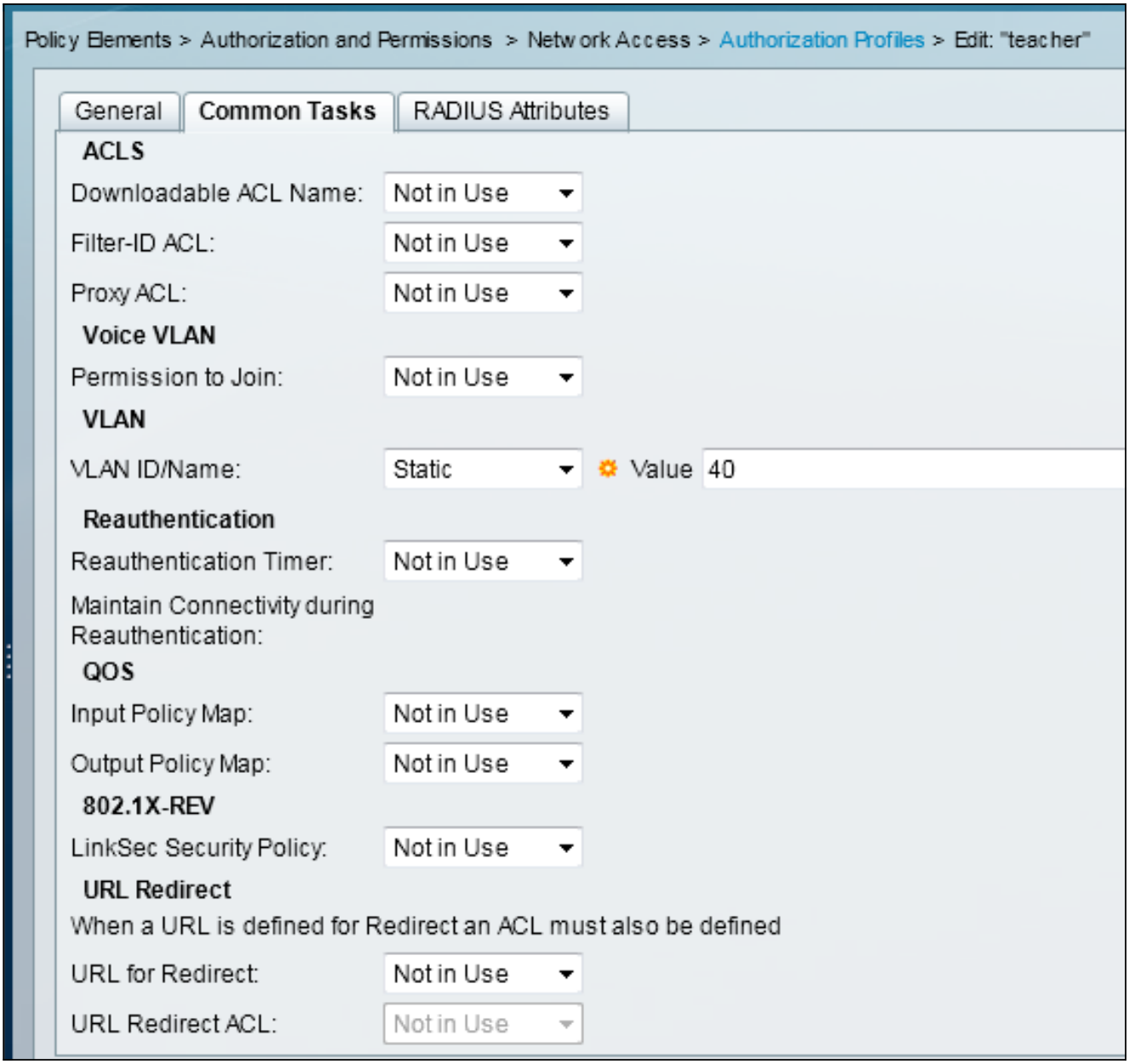
5. Définissez l'ID/nom du VLAN comme **Statique** avec une valeur de **30** (VLAN 30).



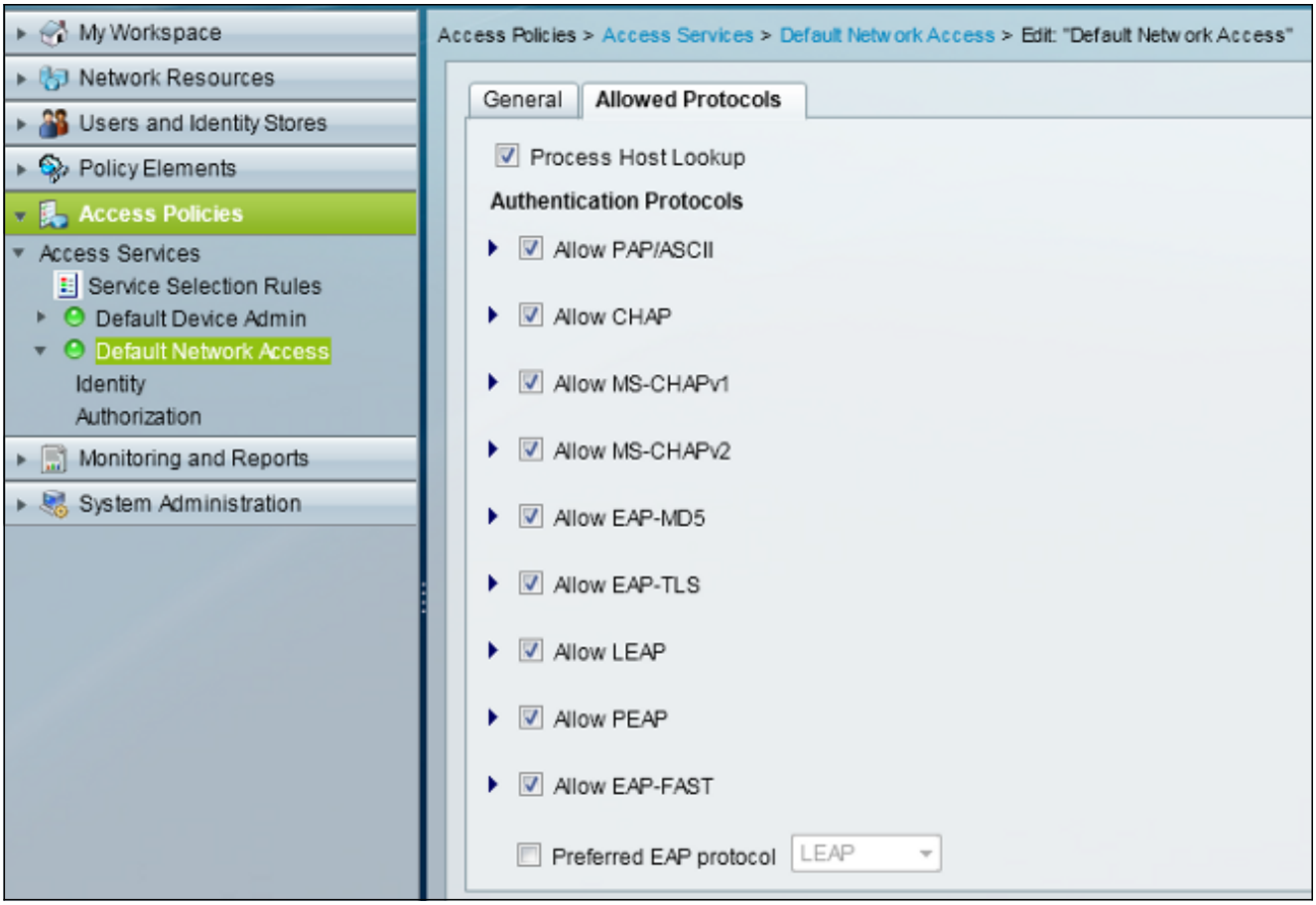
6. Modifiez le profil d'autorisation de l'enseignant.



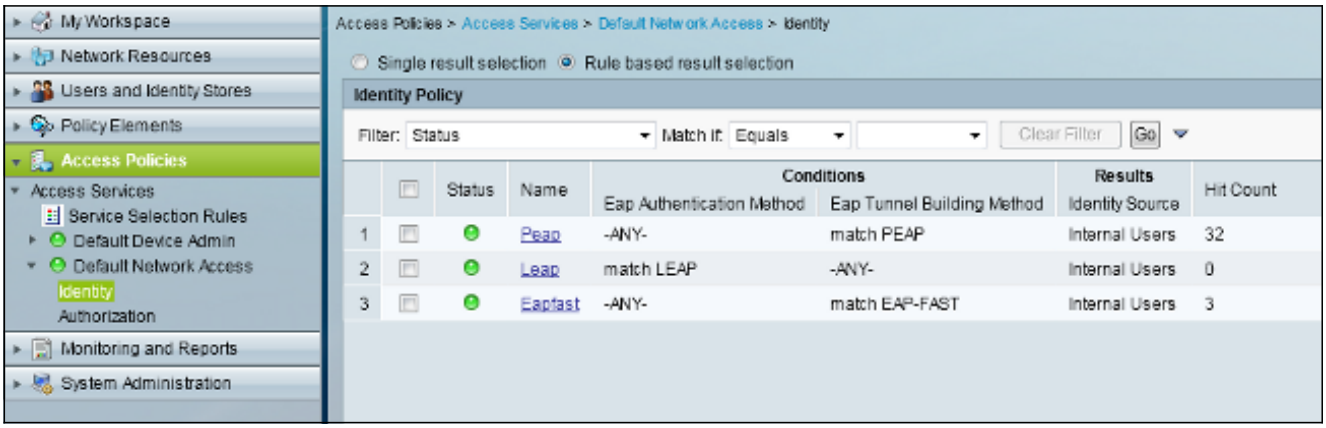
7. Définissez l'ID/nom du VLAN comme **Statique** avec une valeur de **40** (VLAN 40).



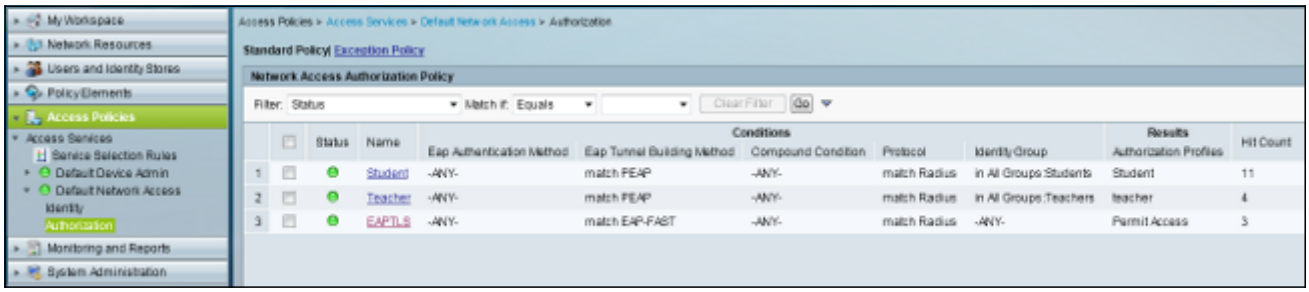
8. Naviguez jusqu'à **Access Policies > Access Services > Default Network Access**, puis cliquez sur l'onglet **Allowed Protocols**. Cochez la case **Autoriser PEAP**.



9. Accédez à **Identité** et définissez les règles afin d'autoriser les utilisateurs PEAP.



10. Naviguez jusqu'à **Autorisation**, et associez Étudiant et enseignant à la Politique d'autorisation ; dans cet exemple, le mappage doit être Student pour VLAN 30 et Teacher pour VLAN 40.



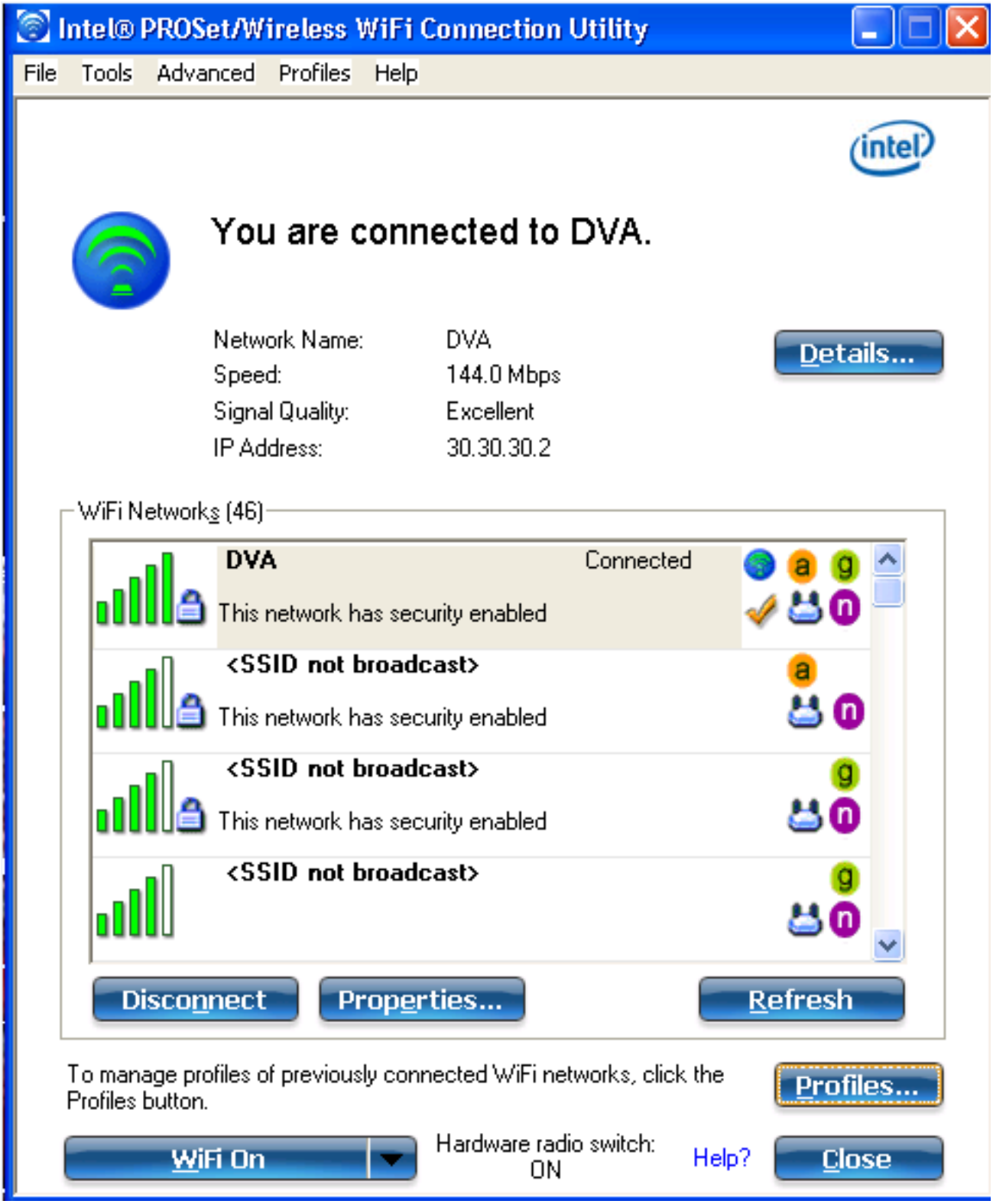
Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Voici les processus de vérification :

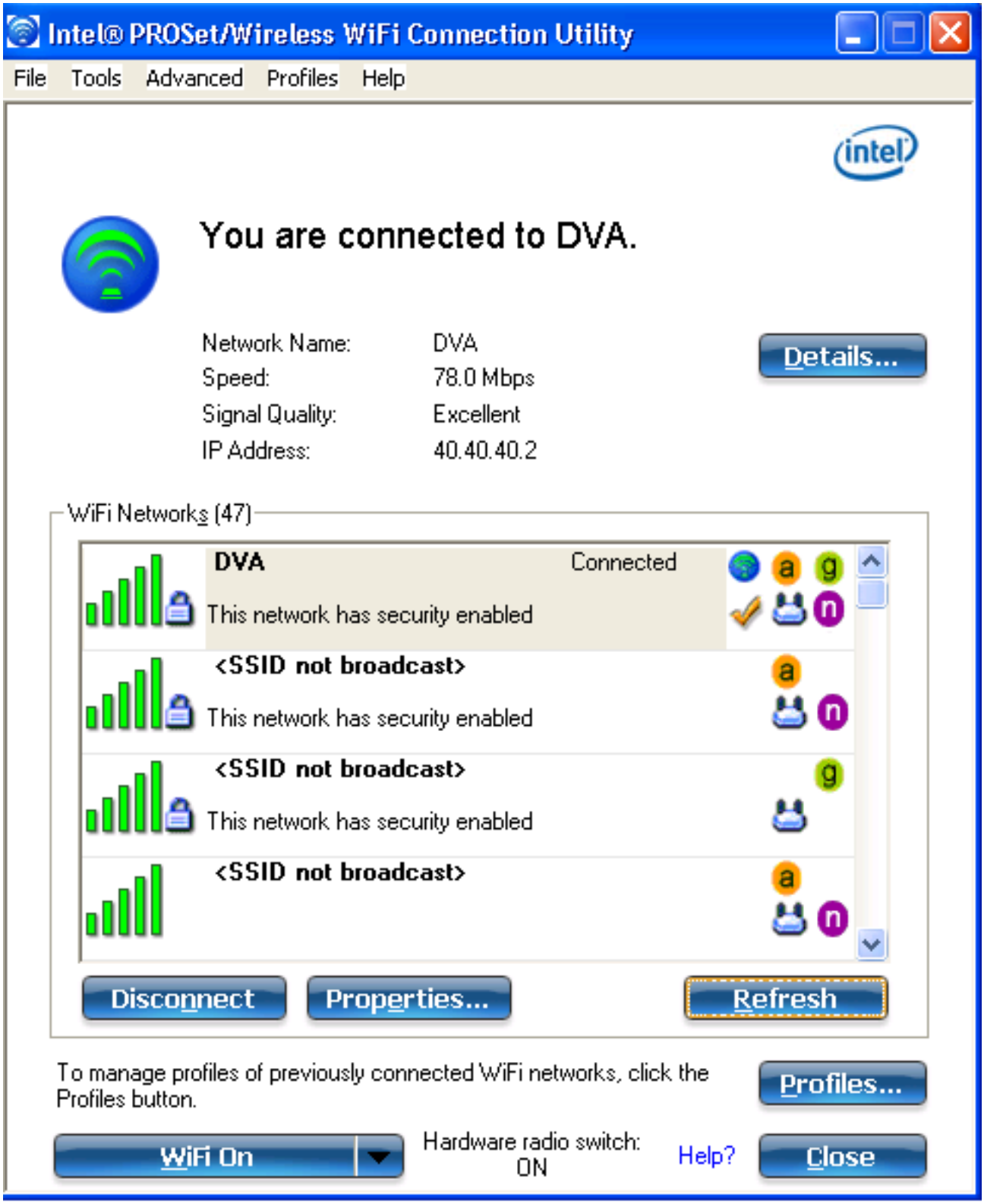
- Surveillez la page de l'ACS qui affiche les clients authentifiés.

Sep 1,13 4:56:49.220 AM	✔		teacher	00-21-5C-8C-C7-61	Default Network Access	PEAP (EAP-MSCHAPv2)	Default Network Device	10.105.135.176	Capwap1	acstemplate
Sep 1,13 4:50:54.483 AM	✔		student	00-21-5C-8C-C7-61	Default Network Access	PEAP (EAP-MSCHAPv2)	Default Network Device	10.105.135.176	Capwap1	acstemplate

- Connectez-vous au réseau local sans fil DVA avec le groupe d'étudiants et examinez l'utilitaire de connexion WiFi du client.



- Connectez-vous au réseau local sans fil DVA avec le groupe d'enseignants et examinez l'utilitaire de connexion WiFi du client.



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Remarques :

Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Les débogages utiles incluent **debug client mac-address** *mac*, ainsi que les commandes de trace NGWC suivantes :

- **set trace group-wireless-client level debug**
- **set trace group-wireless-client filter mac** *xxxx.xxxx.xxxx*
- **show trace sys-filtrtered-traces**

La trace de NGWC n'inclut pas dot1x/AAA. Utilisez donc cette liste complète de traces combinées pour dot1x/AAA :

- **set trace group-wireless-client level debug**
- **set trace wcm-dot1x event level debug**
- **set trace wcm-dot1x aaa level debug**
- **set trace aaa wireless events level debug**
- **set trace access-session core sm level debug**
- **set trace access-session méthode dot1x level debug**
- **set trace group-wireless-client filter mac** *xxxx.xxxx.xxxx*
- **set trace wcm-dot1x event filter mac** *xxxx.xxxx.xxxx*
- **set trace wcm-dot1x aaa filter mac** *xxxx.xxxx.xxxx*
- **set trace aaa wireless events filter mac** *xxxx.xxxx.xxxx*
- **set trace access-session core sm filter mac** *xxxx.xxxx.xxxx*
- **set trace access-session, méthode dot1x filter mac** *xxxx.xxxx.xxxx*
- **show trace sys-filtrtered-traces**

Lorsque l'affectation de VLAN dynamique fonctionne correctement, vous devriez voir ce type de sortie des débogages :

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

[09/01/13 12:13:28.598 IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for
station  ---
[09/01/13 12:13:28.598 IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
```

[09/01/13 12:13:28.598 IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for Wireless client in WCM(NGWC)
[09/01/13 12:13:28.598 IST 1cd6 5933] 0021.5C8C.C761 Inserting AAA Override struct for mobile
   MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:13:28.598 IST 1cd7 5933] 0021.5C8C.C761 Inserting new RADIUS override into chain for station 0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd8 5933] 0021.5C8C.C761 Override values (cont..)
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:

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

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

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

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

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

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

```
   vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST 1aee 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station  0021.5C8C.C761  - vlan 40, interface 'VLAN0040'
[09/01/13 12:08:59.553 IST 1aef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config
[09/01/13 12:08:59.553 IST 1af0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
[09/01/13 12:08:59.553 IST 1af1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)
```