Authentification Web externe à l'aide d'un serveur RADIUS

Table des matières

Introduction

Ce document explique comment effectuer l'authentification Web externe au moyen un serveur RADIUS externe.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance de base de la configuration des points d'accès légers (LAP) et des WLC Cisco

- Connaissance de la configuration d'un serveur Web externe
- Connaissance de la configuration de Cisco Secure ACS

Composants utilisés

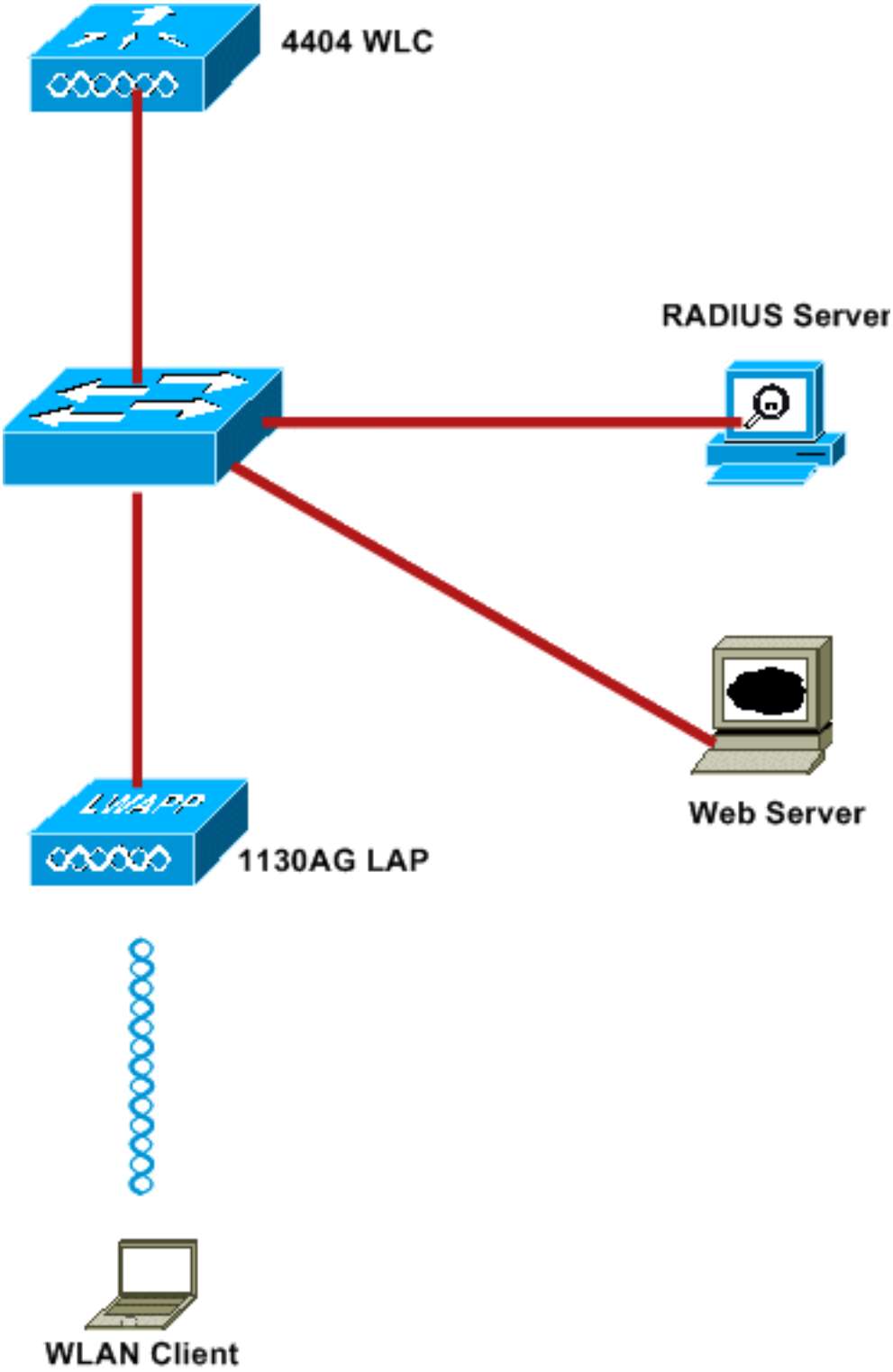
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur LAN sans fil qui exécute la version 5.0.148.0 du microprogramme
- LAP de la gamme Cisco 1232
- Adaptateur client sans fil Cisco 802.11a/b/g 3.6.0.61
- Serveur Web externe qui héberge la page de connexion d'authentification Web
- Version de Cisco Secure ACS qui exécute la version 4.1.1.24 du microprogramme

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Ce sont les adresses IP utilisées dans ce document :

- Le WLC utilise l'adresse IP 10.77.244.206
- Le LAP est enregistré auprès du WLC avec l'adresse IP 10.77.244.199
- Le serveur Web utilise l'adresse IP 10.77.244.210
- Le serveur Cisco ACS utilise l'adresse IP 10.77.244.196
- Le client reçoit une adresse IP de l'interface de gestion qui est mappée au WLAN - 10.77.244.208

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Authentification Web externe

L'authentification Web est un mécanisme d'authentification de couche 3 utilisé pour authentifier les utilisateurs invités pour l'accès à Internet. Les utilisateurs authentifiés à l'aide de ce processus ne pourront pas accéder à Internet tant qu'ils n'auront pas terminé le processus d'authentification. Pour obtenir des informations complètes sur le processus d'authentification Web externe, lisez la section Processus d'authentification Web externe du document Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil.

Dans ce document, nous examinons un exemple de configuration, dans lequel l'authentification Web externe est effectuée à l'aide d'un serveur RADIUS externe.

Configurer le WLC

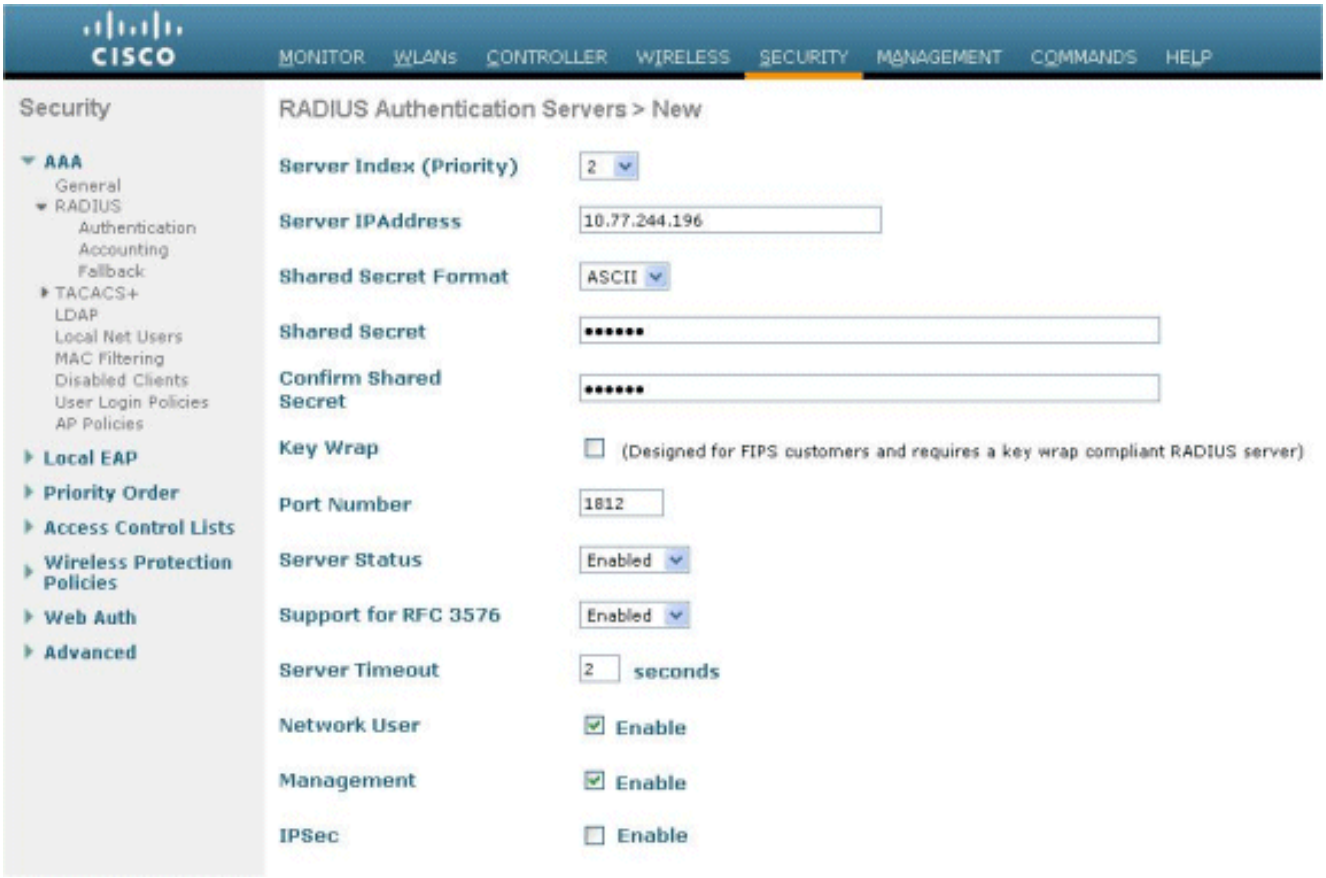
Dans ce document, nous supposons que le WLC est déjà configuré et a un LAP enregistré sur le WLC. Ce document suppose en outre que le WLC est configuré pour un fonctionnement de base et que les LAP sont enregistrés sur le WLC. Si vous êtes un nouvel utilisateur et tentez de configurer le WLC pour un fonctionnement de base avec les LAP, consultez la section Enregistrer un point d'accès léger (LAP) sur un contrôleur réseau local sans fil (WLC). Pour afficher les LAP qui sont enregistrés sur le WLC, accédez à **Wireless > All APs**.

Une fois que le WLC est configuré pour un fonctionnement de base et qu'un ou plusieurs LAP y sont inscrits, vous pouvez configurer le WLC pour l'authentification Web externe à l'aide d'un serveur Web externe. Dans notre exemple, nous utilisons un Cisco Secure ACS version 4.1.1.24 comme serveur RADIUS. Tout d'abord, nous allons configurer le WLC pour ce serveur RADIUS, puis nous allons examiner la configuration requise sur Cisco Secure ACS pour cette configuration.

Configurer le WLC pour Cisco Secure ACS

Effectuez ces étapes afin d'ajouter le serveur RADIUS sur le WLC :

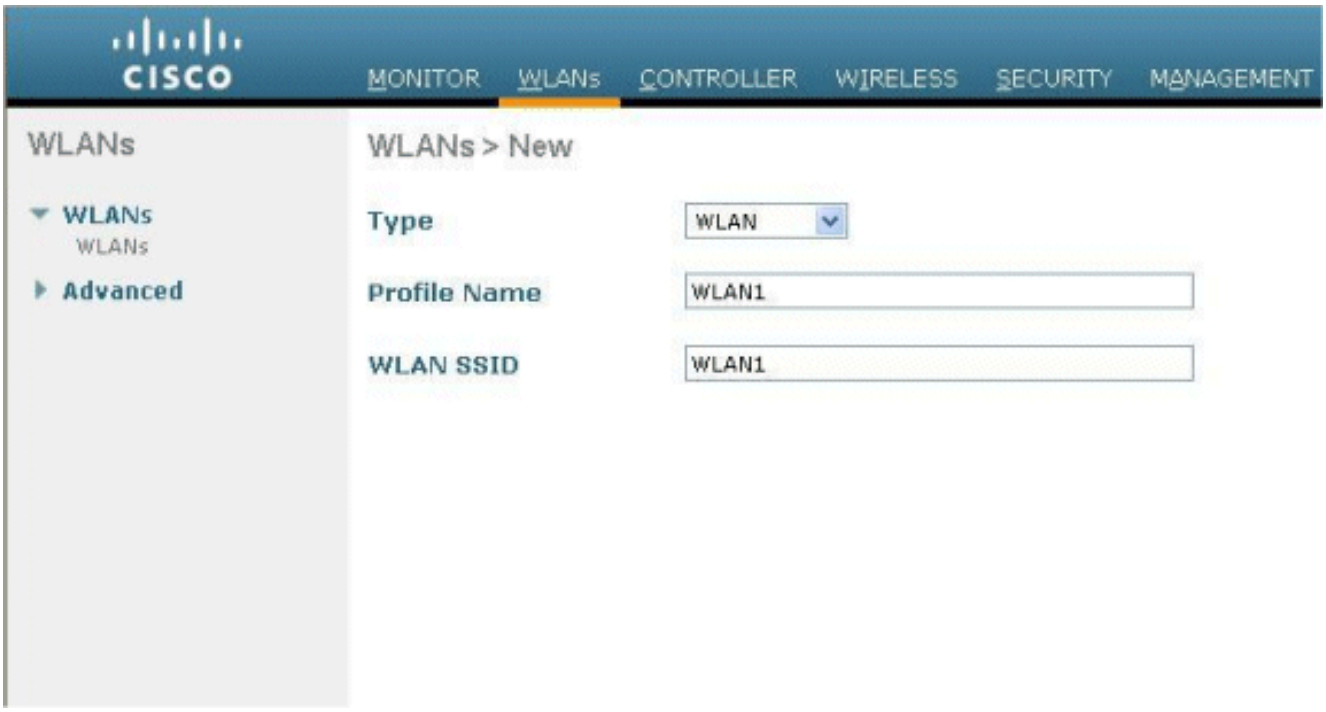
1. Dans l'interface graphique utilisateur du WLC, cliquez sur le menu **SECURITY**.
2. Sous le menu **AAA**, accédez au sous-menu **Radius > Authentication**.
3. Cliquez sur **New**, et entrez l'adresse IP du serveur RADIUS. Dans cet exemple, l'adresse IP du serveur est *10.77.244.196*.
4. Entrez le secret partagé dans le WLC. Le secret partagé doit être configuré de la même manière sur le WLC.
5. Choisissez **ASCII** ou **Hex** pour le format secret partagé. Le même format doit être choisi sur le WLC.
6. **1812** est le numéro de port utilisé pour l'authentification RADIUS.
7. Assurez-vous que l'option Server Status est définie sur **Enabled**.
8. Cochez la case Network User **Enable** pour authentifier les utilisateurs du réseau.
9. Cliquez sur
   Apply.



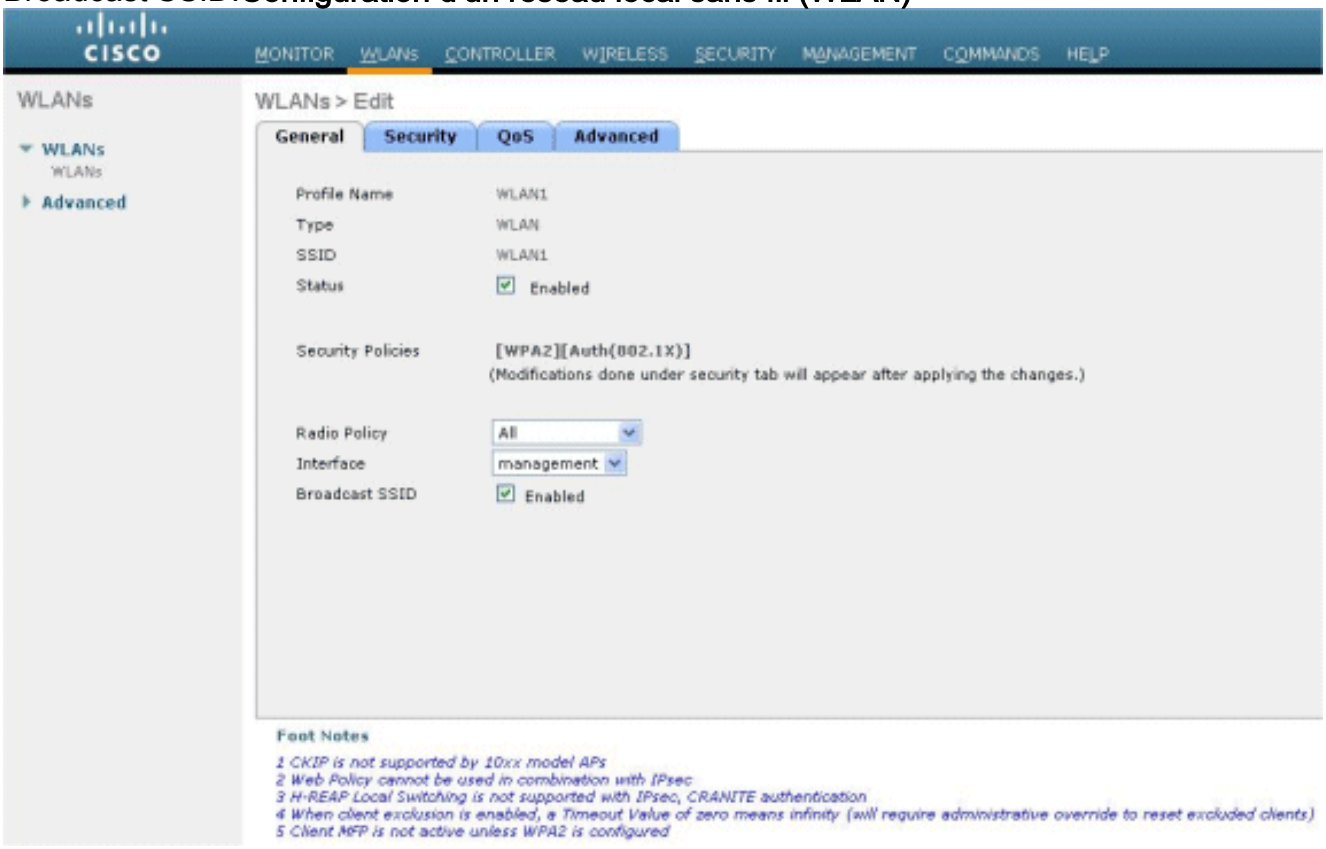
Configurer le WLAN sur le WLC pour l'authentification Web

L'étape suivante consiste à configurer le WLAN pour l'authentification Web sur le WLC. Suivez ces étapes afin de configurer le WLAN sur le WLC :

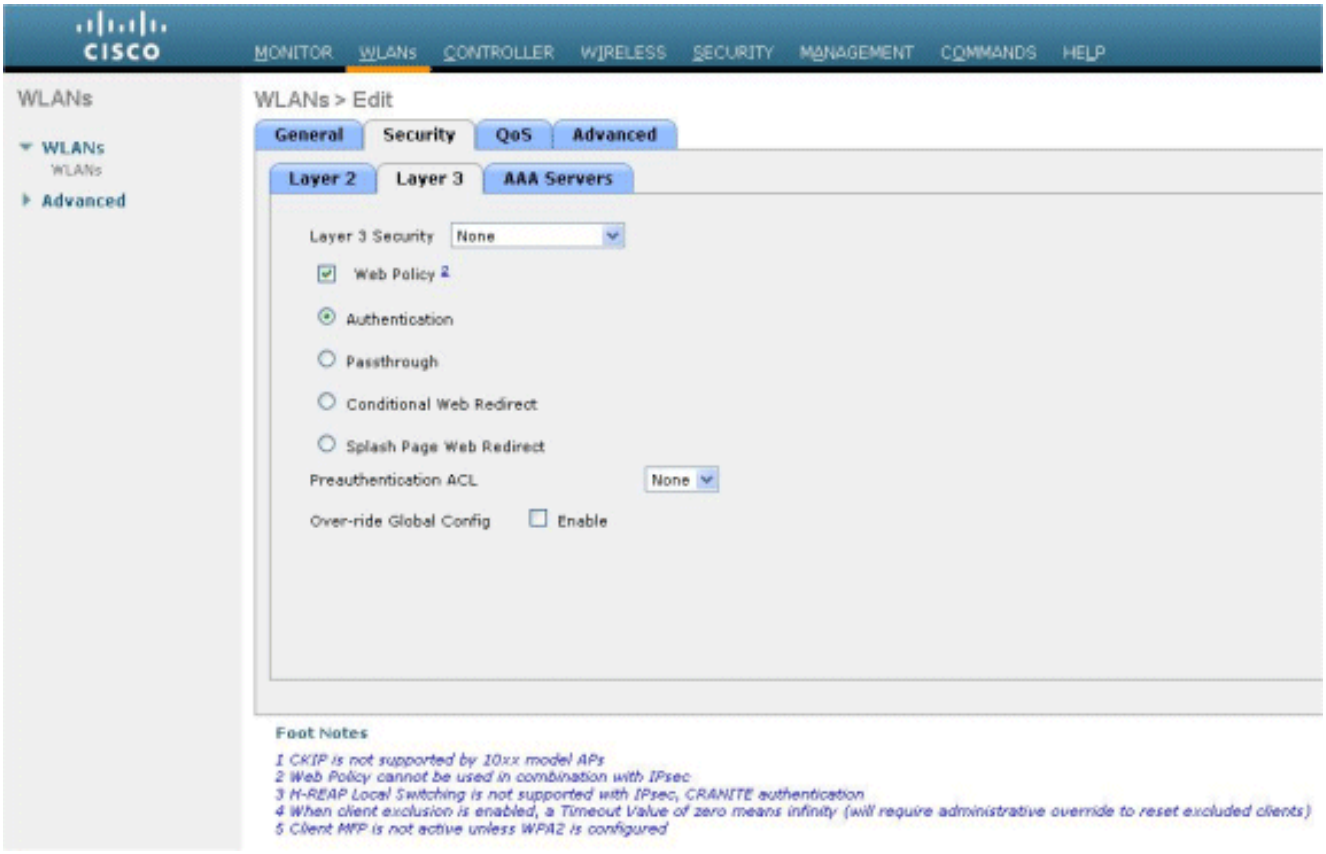
1. Cliquez sur le menu **WLANs** de l'interface graphique du contrôleur, et choisissez **New**.
2. Sélectionnez **WLAN** pour Type.
3. Saisissez un nom de profil et un SSID WLAN de votre choix, puis cliquez sur **Apply**.**Remarque :** le SSID du WLAN est sensible à la casse.



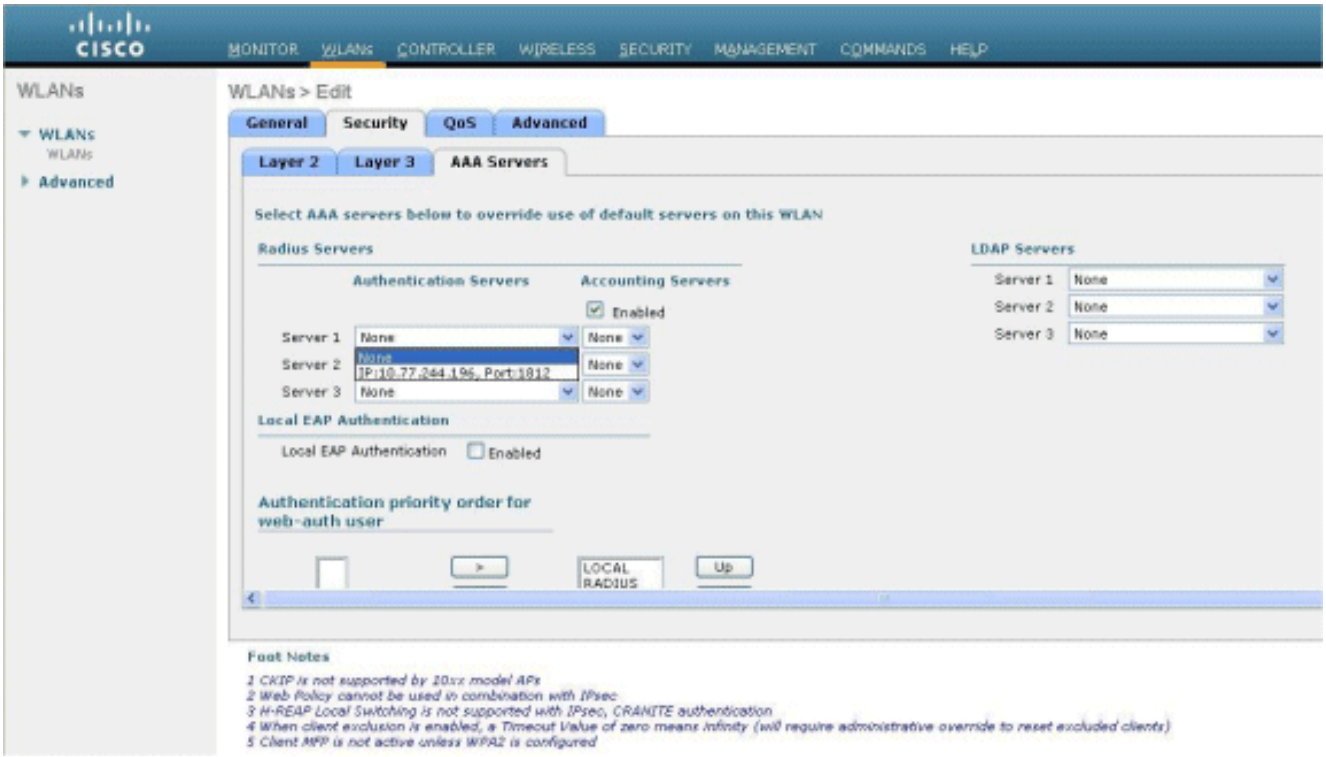
4. Sous l'onglet **General**, assurez-vous que l'option **Enabled** est cochée pour Status et Broadcast SSID.**Configuration d’un réseau local sans fil (WLAN)**



5. Choisissez une interface pour le WLAN. En général, une interface configurée dans un VLAN unique est mappée au WLAN de sorte que le client reçoive une adresse IP dans ce VLAN. Dans cet exemple, nous utilisons la *gestion* pour l'interface.
6. Sélectionnez l'onglet Security .
7. Dans le menu **Layer 2**, choisissez **None** pour Layer 2 Security.
8. Dans le menu **Layer 3**, choisissez **None** pour Layer 3 Security. Cochez la case **Web Policy** et choisissez
Authentication.



9. Dans le menu **AAA servers**, pour Authentication Server, choisissez le serveur RADIUS qui a été configuré sur ce WLC. Les autres menus doivent conserver leurs valeurs par défaut.

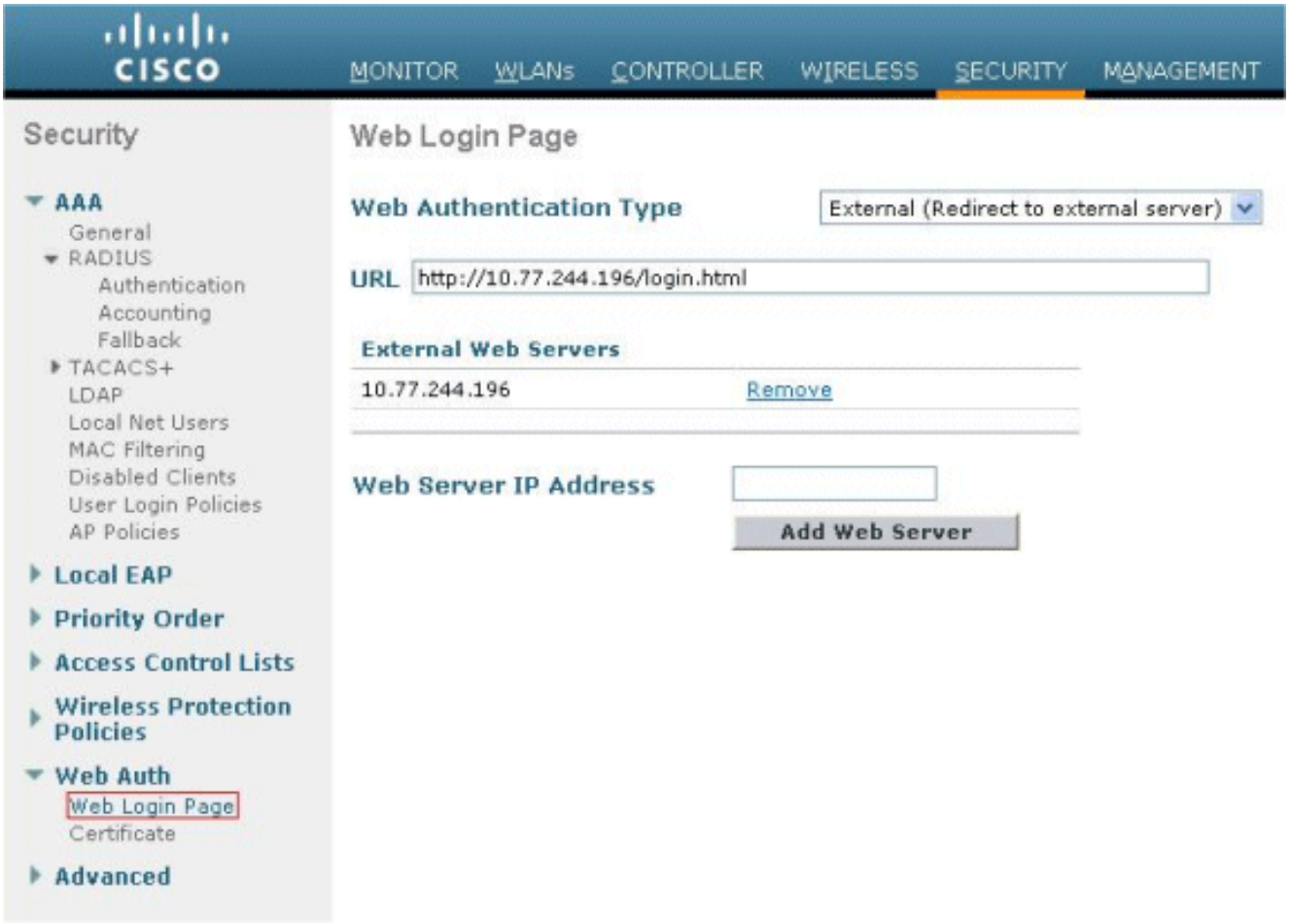


Configurer les informations du serveur Web sur le WLC

Le serveur Web qui héberge la page Web Authentication doit être configuré sur le WLC. Procédez comme suit pour configurer le serveur Web :

1. Cliquez sur l'onglet **Security.** Accédez à **Web Auth > Web Login Page**.

2. Définissez le type d'authentification Web sur **Externe**.
3. Dans le champ Web Server IP Address, entrez l'adresse IP du serveur qui héberge la page Web Authentication, puis cliquez sur **Add Web Server**. Dans cet exemple, l'adresse IP est *10.77.244.196*, qui apparaît sous Serveurs Web externes.
4. Entrez l'URL de la page Web Authentication (dans cet exemple, *http://10.77.244.196/login.html*) dans le champ URL.



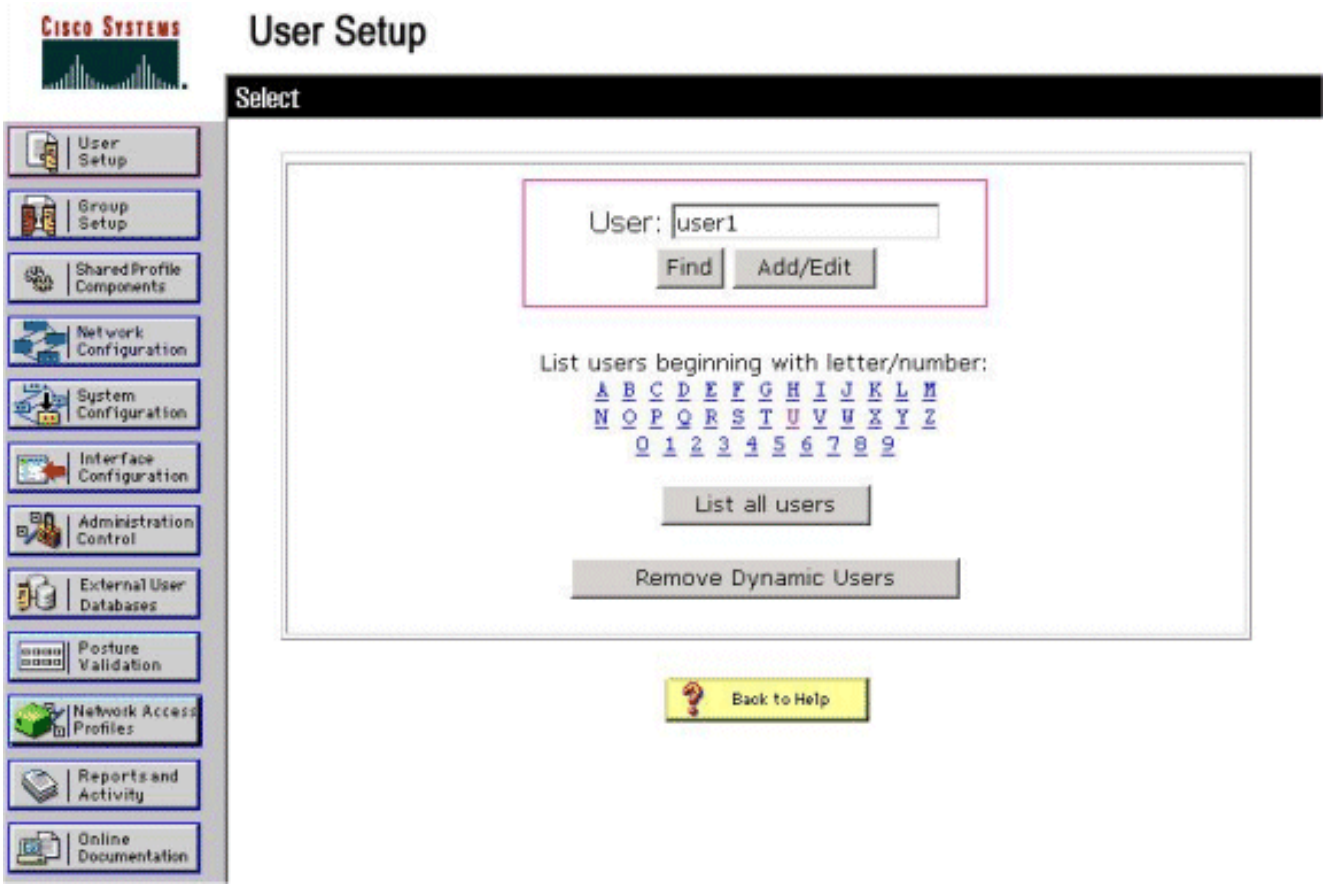
Configuration de Cisco Secure ACS

Dans ce document, nous supposons que Cisco Secure ACS Server est déjà installé et exécuté sur une machine. Pour plus d'informations sur la configuration de Cisco Secure ACS, reportez-vous au Guide de configuration de Cisco Secure ACS 4.2.

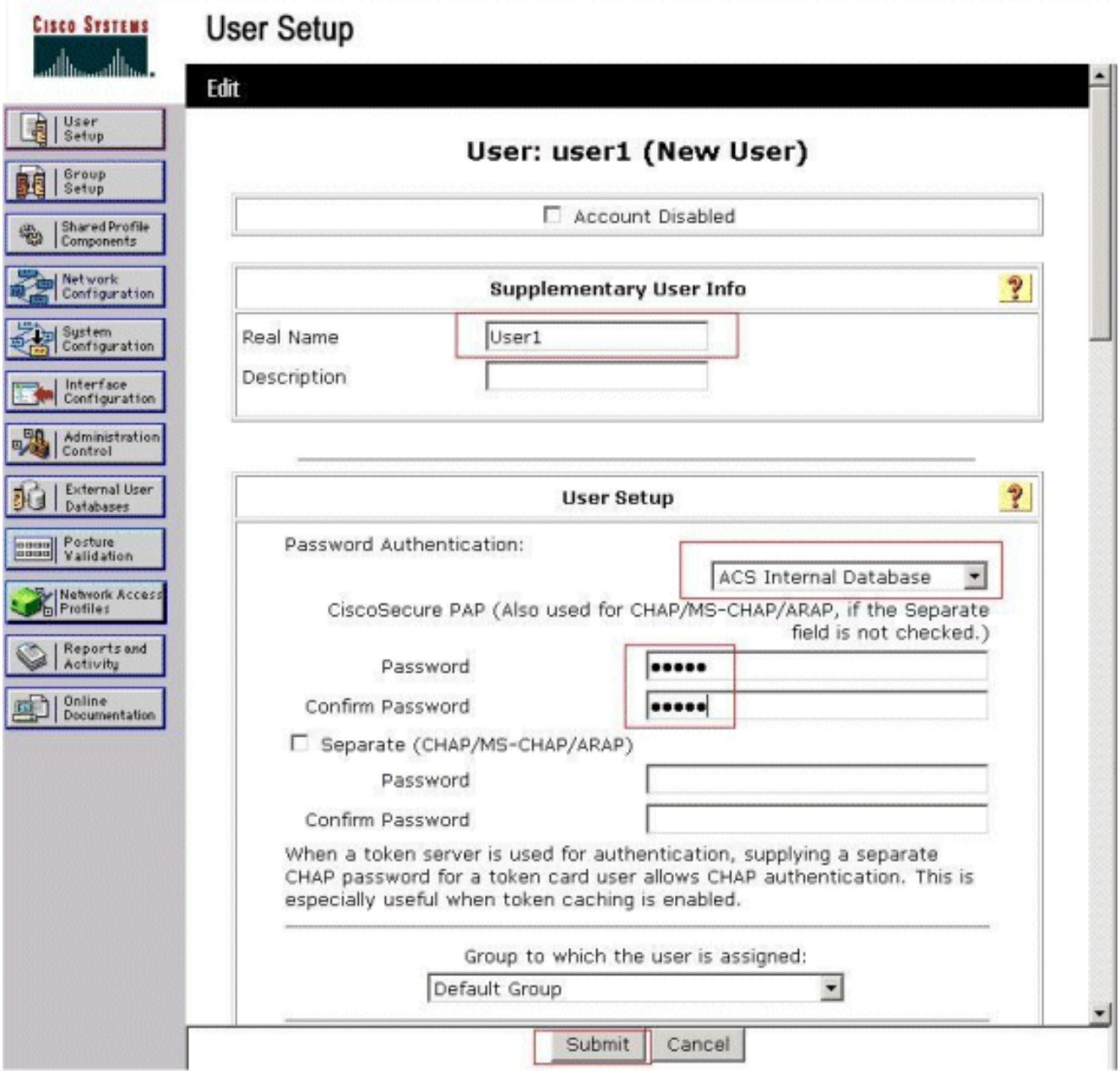
Configuration des informations utilisateur sur Cisco Secure ACS

Procédez comme suit afin de configurer les utilisateurs sur Cisco Secure ACS :

1. Choisissez **User Setup** dans l'interface graphique utilisateur de Cisco Secure ACS, entrez un nom d'utilisateur, puis cliquez sur **Add/Edit**. Dans cet exemple, l'utilisateur est *user1*.



2. Par défaut, le protocole PAP est utilisé pour authentifier les clients. Le mot de passe de l'utilisateur est entré sous **User Setup > Password Authentication > Cisco Secure PAP**. Assurez-vous de choisir **Base de données interne ACS** pour l'authentification par mot de passe.



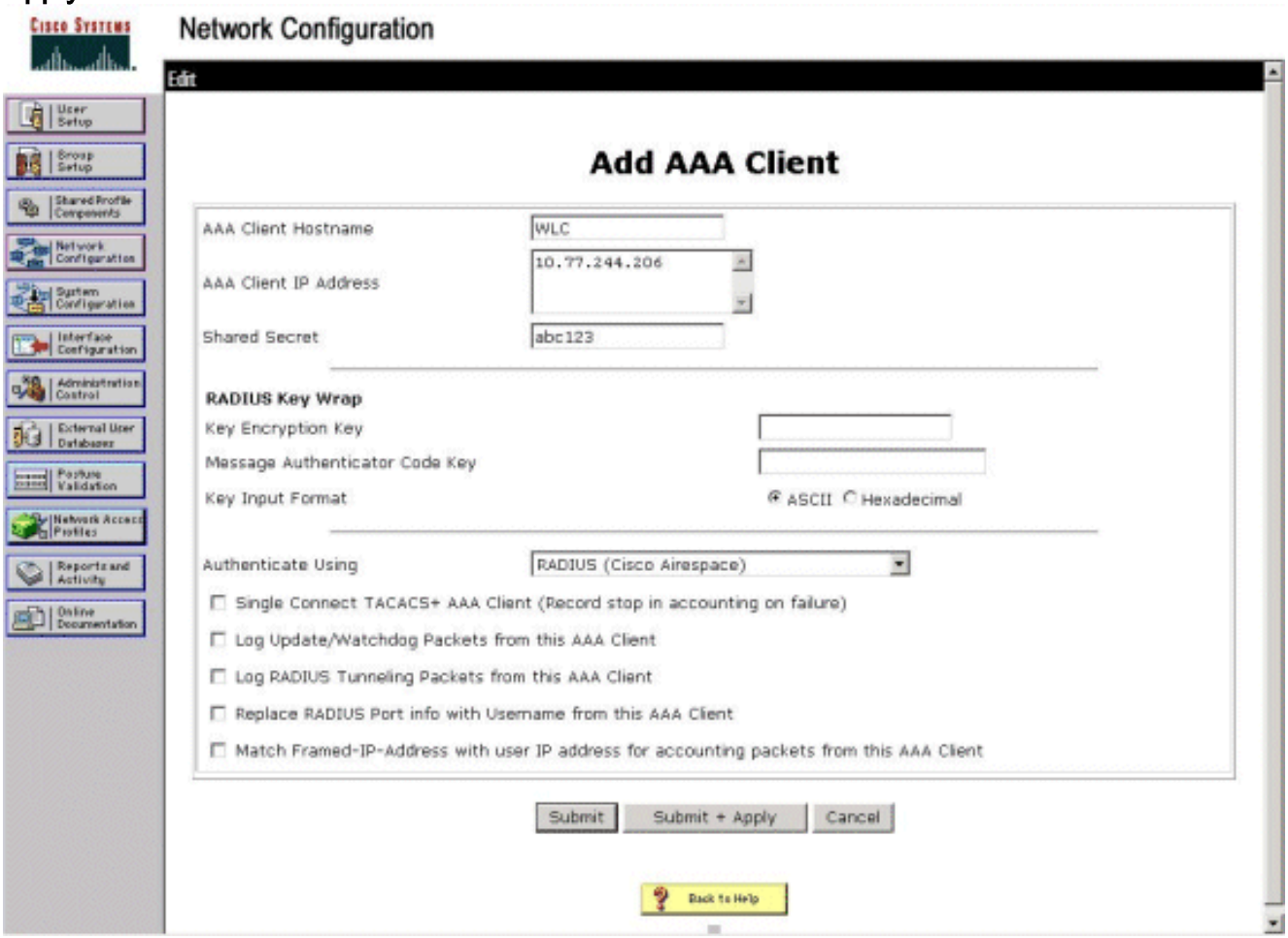
3. L'utilisateur doit se voir attribuer un groupe auquel il appartient. Sélectionnez le **groupe par défaut**.
4. Cliquez sur Submit.

Configurer les informations WLC sur Cisco Secure ACS

Suivez ces étapes afin de configurer les informations WLC sur Cisco Secure ACS :

1. Dans l'interface graphique utilisateur ACS, cliquez sur l'onglet **Network Configuration**, puis cliquez sur **Add Entry**.
2. L'écran Add AAA client apparaît.
3. Saisissez le nom du client. Dans cet exemple, nous utilisons *WLC*.
4. Saisissez l'adresse IP du client. L'adresse IP du WLC est *10.77.244.206*.
5. Saisissez la clé secrète partagée et le format de la clé. Cela devrait correspondre à l'entrée faite dans le menu **Sécurité** du WLC.
6. Choisissez **ASCII** pour le Key Input Format, qui devrait être le même sur le WLC.
7. Choisissez **RADIUS (Cisco Airespace)** pour Authenticate Using afin de définir le protocole utilisé entre le WLC et le serveur RADIUS.

8. Cliquez sur **Submit + Apply**.

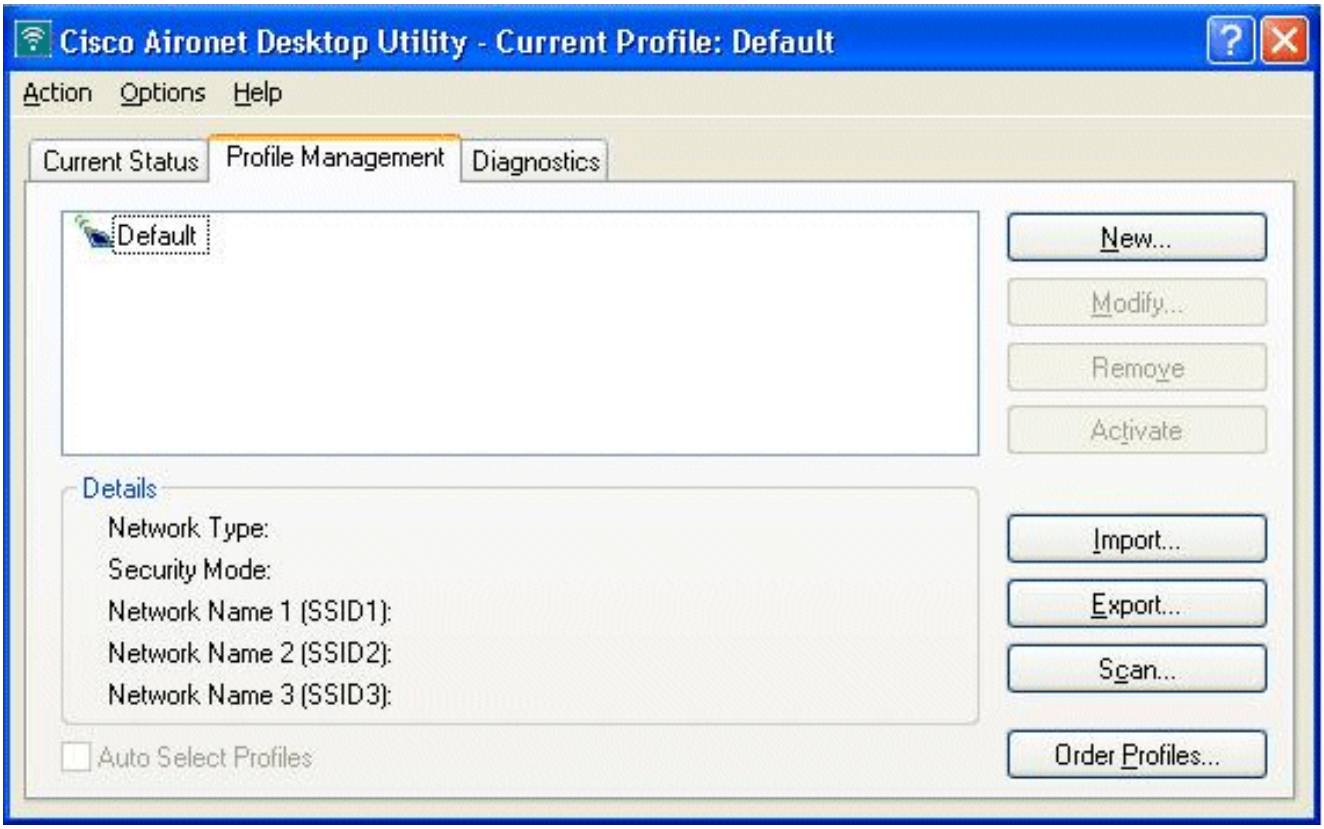


Processus d'authentification client

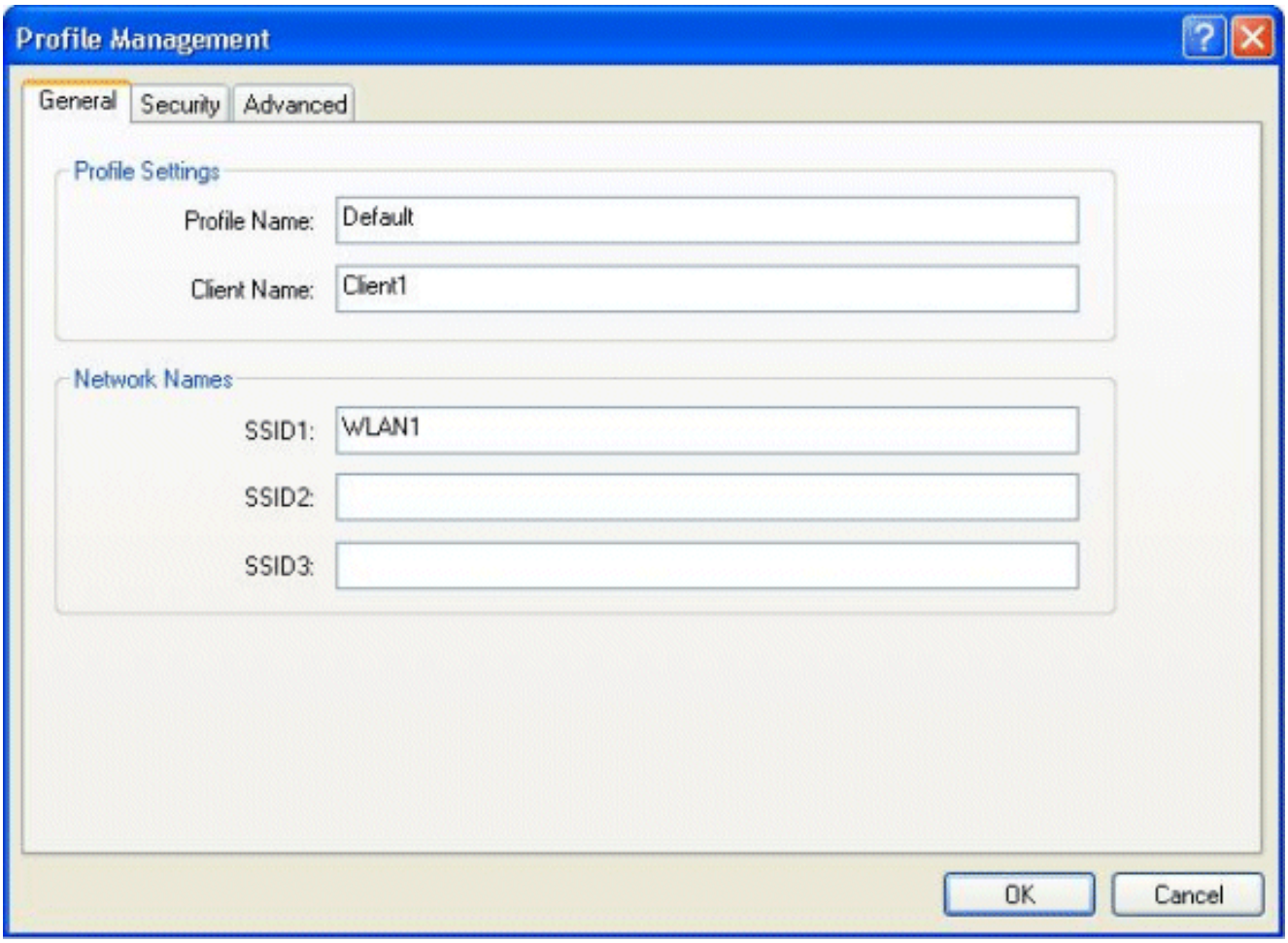
Configuration du client

Dans cet exemple, nous utilisons l'utilitaire Cisco Aironet Desktop Utility pour effectuer l'authentification Web. Suivez ces étapes afin de configurer l'utilitaire Aironet Desktop Utility.

1. Ouvrez l'utilitaire de bureau Aironet à partir de **Start > Cisco Aironet > Aironet Desktop Utility**.
2. Cliquez sur l'onglet **Profile Management**.

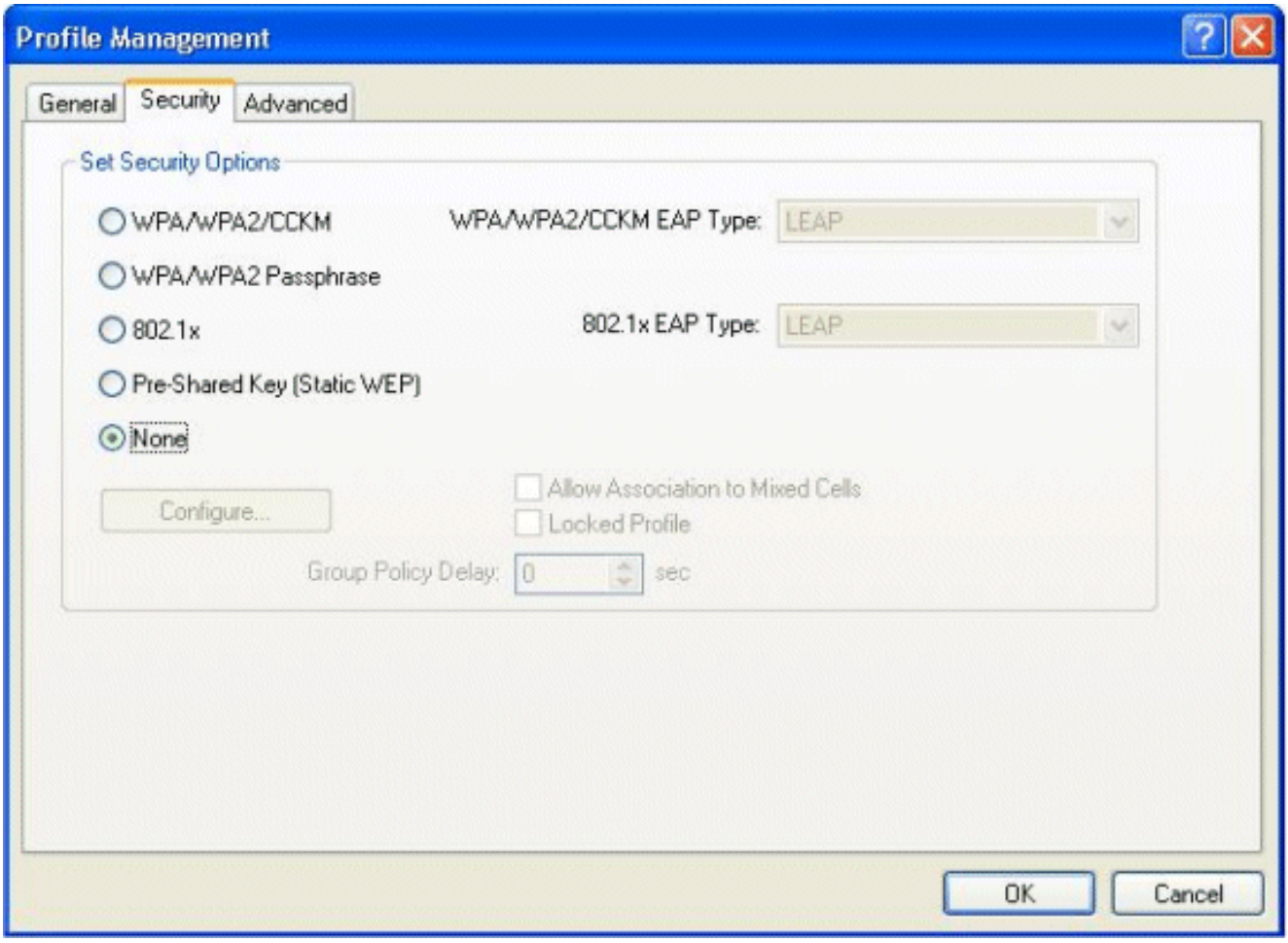


3. Sélectionnez le profil **par défaut**, puis cliquez sur **Modifier**.Cliquez sur l'**onglet General (Général).**Configurez un nom de profil. Dans cet exemple, *Default* est utilisé.Configurez le SSID sous Network Names. Dans cet exemple, *WLAN1* est utilisé.

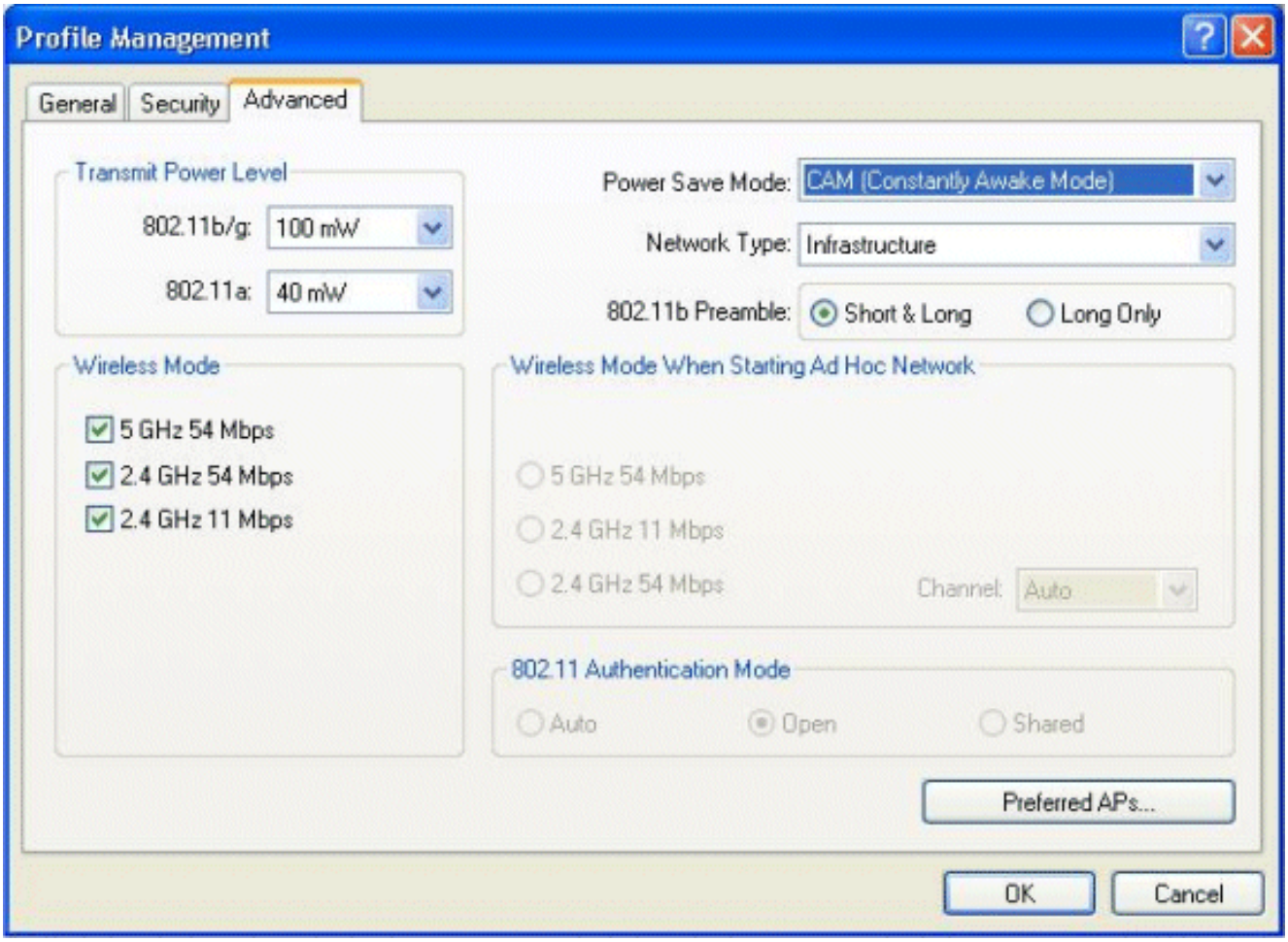


Remarque : le SSID est sensible à la casse et doit correspondre au WLAN configuré sur le WLC.Cliquez sur l'onglet **Security.**Sélectionnez **None** comme Security pour l'authentification

Web.



Cliquez sur l'onglet **Advanced.**Dans le menu **Wireless Mode**, choisissez la fréquence à laquelle le client sans fil communique avec le LAP.Sous **Transmit Power Level**, choisissez la puissance qui est configurée sur le WLC.Conservez la valeur par défaut du mode Power Save.Sélectionnez **Infrastructure** comme type de réseau.Définissez le préambule 802.11b sur **Short & Long** pour une meilleure compatibilité.Click
OK.



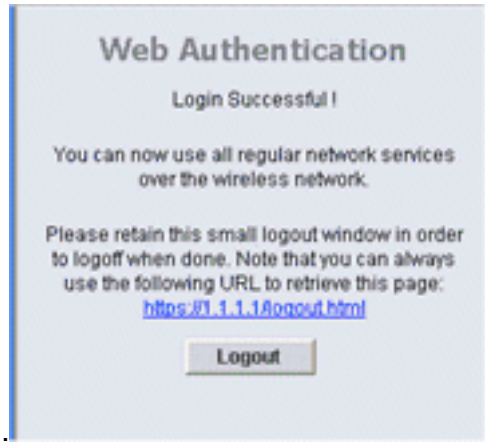
4. Une fois le profil configuré sur le logiciel client, le client est associé avec succès et reçoit une adresse IP du pool de VLAN configuré pour l'interface de gestion.

Processus de connexion client

Cette section explique comment se produit la connexion du client.

1. Ouvrez une fenêtre du navigateur et entrez n'importe quel URL ou adresse IP. La page d'authentification Web est alors affichée sur le client. Si le contrôleur exécute une version antérieure à la version 3.0, l'utilisateur doit entrer *https://1.1.1.1/login.html* pour afficher la page d'authentification Web. Une fenêtre d'alerte de sécurité s'affiche.
2. Cliquez sur **Yes pour poursuivre.**
3. Lorsque la fenêtre Login s'affiche, saisissez le nom d'utilisateur et le mot de passe configurés sur le serveur RADIUS. Si votre connexion est réussie, deux fenêtres de navigateur s'affichent. La fenêtre la plus grande indique une connexion réussie et vous pouvez utiliser cette fenêtre pour naviguer sur Internet. Utilisez la fenêtre plus petite pour vous déconnecter

une fois l'utilisation du réseau invité terminée.

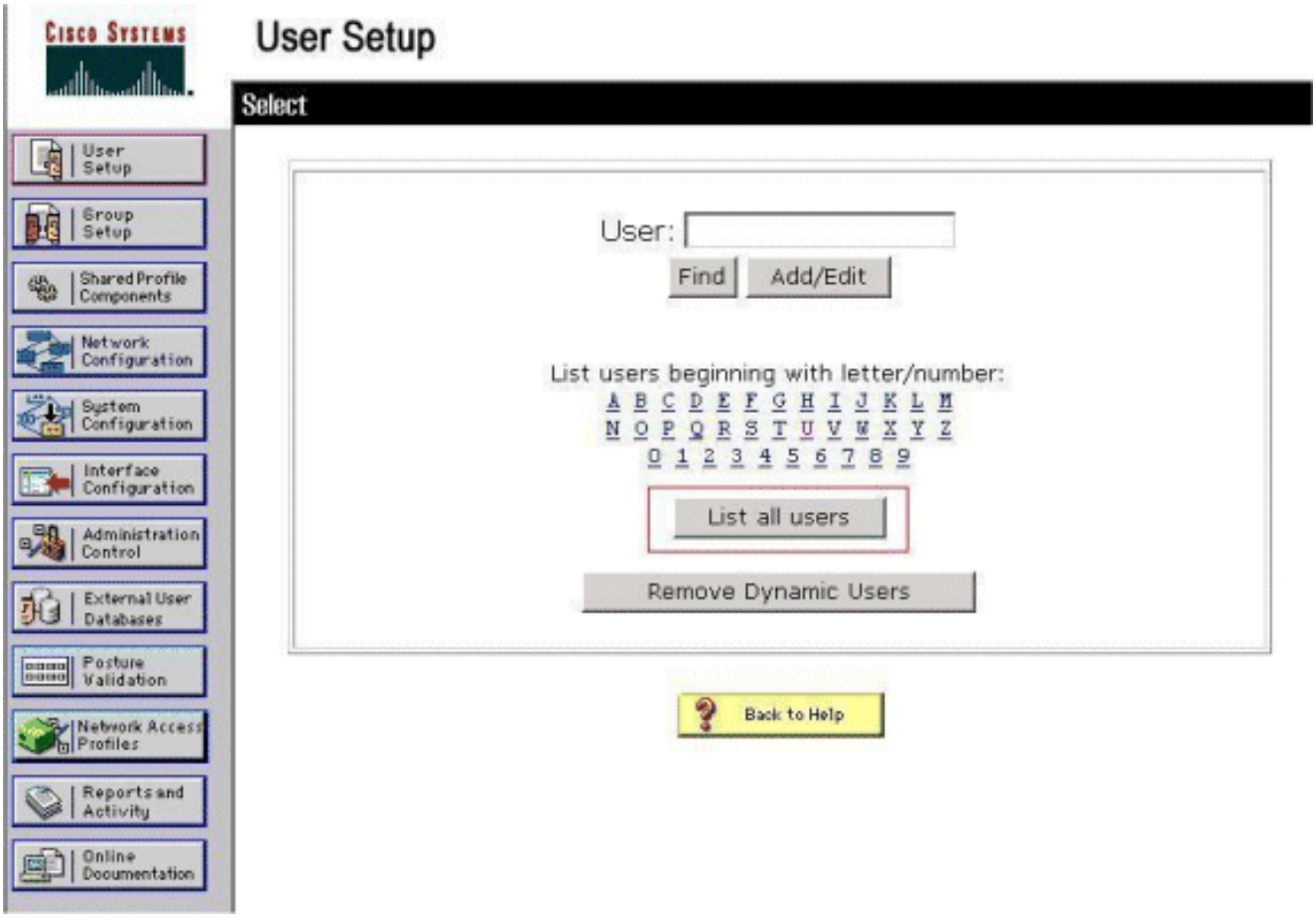


Vérifier

Pour une authentification Web réussie, vous devez vérifier si les périphériques sont configurés de manière appropriée. Cette section explique comment vérifier les périphériques utilisés dans le processus.

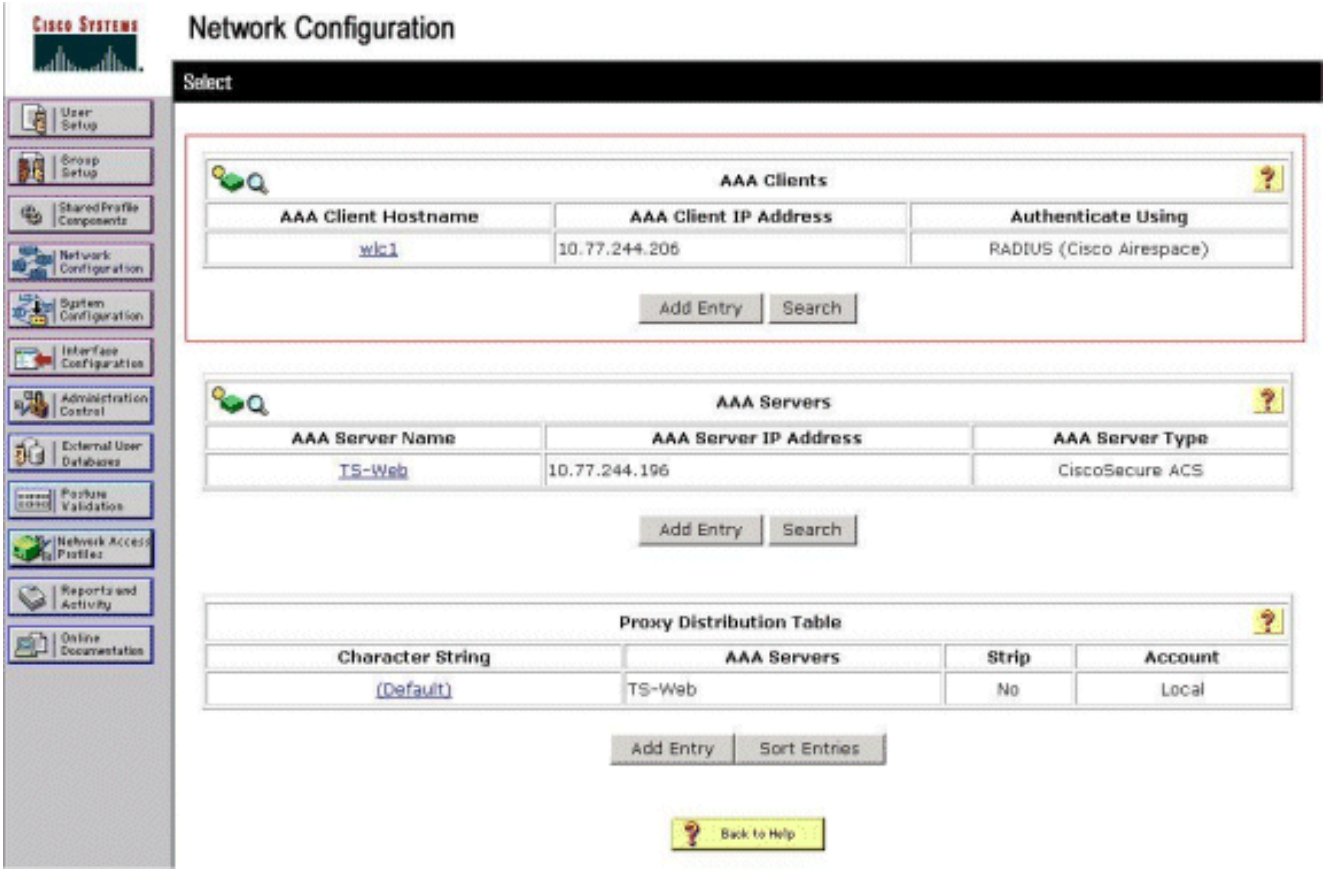
Vérifier ACS

1. Cliquez sur **User Setup**, puis sur **List All Users** sur l'interface graphique utilisateur ACS.



Assurez-vous que l'état de l'utilisateur est *Activé* et que le groupe par défaut est mappé à l'utilisateur.

2. Cliquez sur l'onglet **Network Configuration**, et regardez dans le tableau **AAA Clients** afin de vérifier que le WLC est configuré en tant que client AAA.

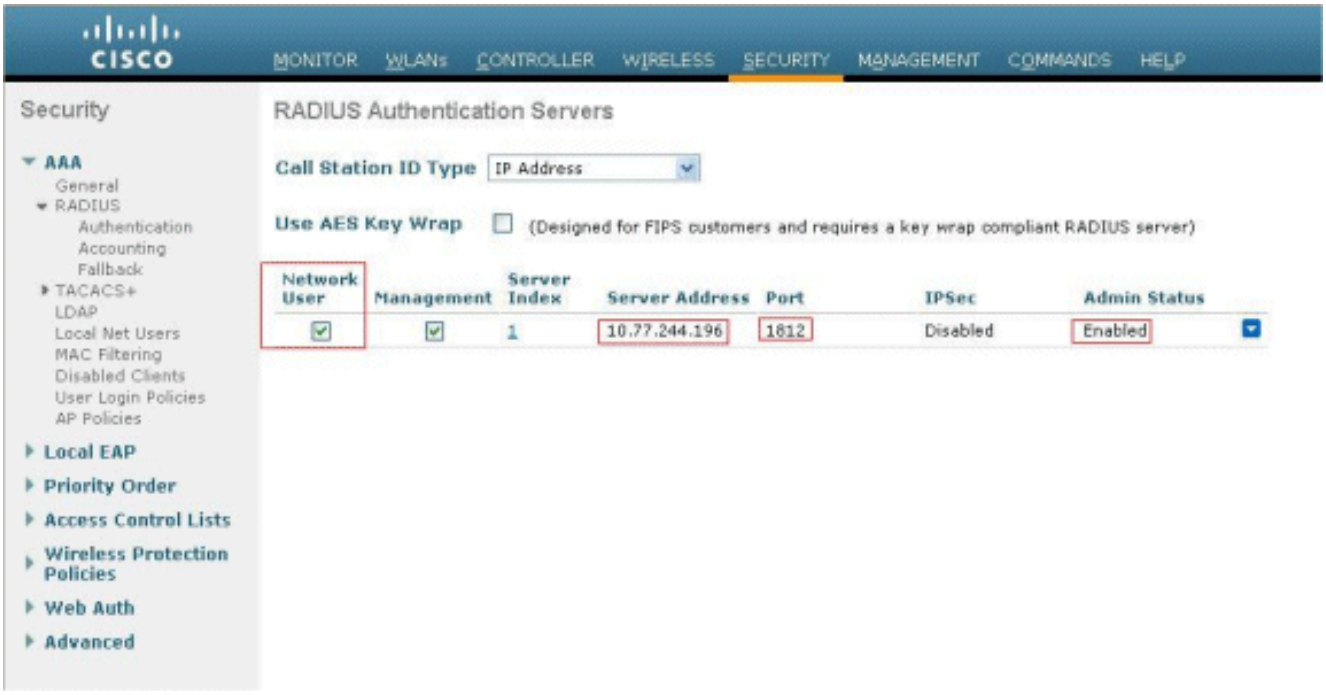


Vérifier le WLC

1. Cliquez sur le menu **WLANs** de l'interface graphique WLC.Assurez-vous que le WLAN utilisé pour l'authentification Web est répertorié sur la page.Assurez-vous que l'état Admin du WLAN est *Activé*.Assurez-vous que la stratégie de sécurité pour le WLAN affiche *Web-Auth*.

2. Cliquez sur le menu **SECURITY** de l'interface graphique WLC.Assurez-vous que Cisco

Secure ACS (10.77.244.196) est répertorié sur la page.Assurez-vous que la case Utilisateur réseau est cochée.Assurez-vous que le port est *1812* et que l'état Admin est *Enabled*.



Dépannage

Il existe de nombreuses raisons pour lesquelles une authentification Web échoue. Le document Troubleshooting Web Authentication on a Wireless LAN Controller (WLC) explique clairement ces raisons en détail.

Dépannage des commandes

Remarque : reportez-vous à Informations importantes sur les commandes de débogage avant d'utiliser ces commandes de **débogage**.

Établissez une connexion Telnet avec le WLC et exécutez ces commandes pour dépanner l'authentification :

- **debug aaa all enable**

```
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00  00 00 00 00 00 00 0
0 00  ...s............
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73  65 72 31 02 12 93 c
3 66  ......user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
      user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010:       structureSize.............................89
Fri Sep 24 13:59:52 2010:       resultCode................................0
Fri Sep 24 13:59:52 2010:       protocolUsed..............................0x0
0000001
```

```
Fri Sep 24 13:59:52 2010:       proxyState.................................00:
40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010:       Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] Framed-IP-Address..................
.....0xffffffff (-1) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Class..............................
.....CACS:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio
n 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
                source: 48, valid bits: 0x1
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

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

- **debug aaa detail enable**

Les tentatives d'authentification ayant échoué sont répertoriées dans le menu **Reports and Activity > Failed Attempts**.

Informations connexes

- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Dépannage de l'authentification Web sur un contrôleur de réseau local sans fil
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Exemple de configuration d'authentification Web avec LDAP sur les contrôleurs de réseau local sans fil
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.