Exemple de configuration d'une liste de contrôle d'accès par utilisateur avec des contrôleurs de réseau local sans fil et Cisco Secure ACS

Contenu

Introduction

Ce document explique, au moyen d'un exemple, comment créer des listes de contrôle d'accès (ACL) dans le WLC et les appliquer aux utilisateurs qui dépendent de l'autorisation RADIUS.

Conditions préalables

Conditions requises

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

- Connaissances de base sur la configuration d'un serveur Cisco Secure ACS pour authentifier les clients sans fil

- Connaissance de la configuration des points d'accès légers (LAP) Cisco Aironet et des contrôleurs de réseau local sans fil (WLC) Cisco
- Connaissance des solutions de sécurité sans fil unifiées Cisco

Components Used

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

- Contrôleur LAN sans fil de la gamme Cisco 4400 qui exécute la version 5.0.148.0
- Points d'accès légers (LAP) de la gamme Cisco Aironet 1231
- Adaptateur client LAN sans fil Cisco Aironet 802.11 a/b/g qui exécute la version 3.6
- Utilitaire Cisco Aironet Desktop Version 3.6
- Serveur Cisco Secure ACS version 4.1
- Routeur à services intégrés de la gamme Cisco 2800 qui exécute IOS® Version 12.4(11)T
- Commutateur de la gamme Cisco Catalyst 2900XL qui exécute la version 12.0(5)WC3b

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.

Conventions

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

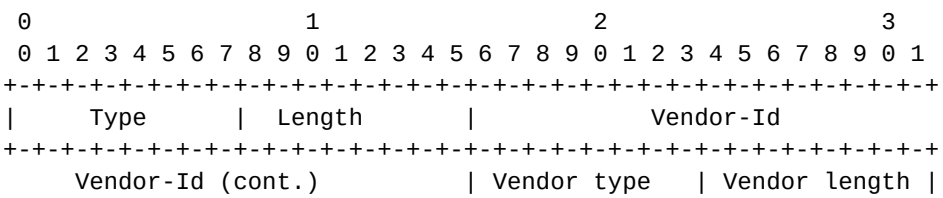
Informations générales

La liste de contrôle d'accès (ACL) par utilisateur fait partie du réseau Cisco Identity. La solution LAN sans fil de Cisco prend en charge la mise en réseau des identités, qui, tout en permettant au réseau d'annoncer un SSID unique, permet également à des utilisateurs spécifiques d'hériter de politiques différentes en fonction de leur profil utilisateur.

La fonction ACL par utilisateur permet d'appliquer une liste de contrôle d'accès configurée sur le contrôleur de réseau local sans fil à un utilisateur en fonction de l'autorisation RADIUS. Pour ce faire, vous devez utiliser l'attribut VSA (Airespace-ACL-Name Vendor Specific Attribute).

Cet attribut indique le nom de la liste de contrôle d'accès à appliquer au client. Lorsque l'attribut ACL est présent dans l'acceptation d'accès RADIUS, le système applique le nom ACL à la station cliente après son authentification. Ceci remplace les listes de contrôle d'accès qui sont affectées à l'interface. Il ignore la liste de contrôle d'accès d'interface attribuée et applique la nouvelle liste.

Un résumé du format d'attribut de nom de liste de contrôle d'accès est présenté ci-dessous. Les champs sont transmis de gauche à droite



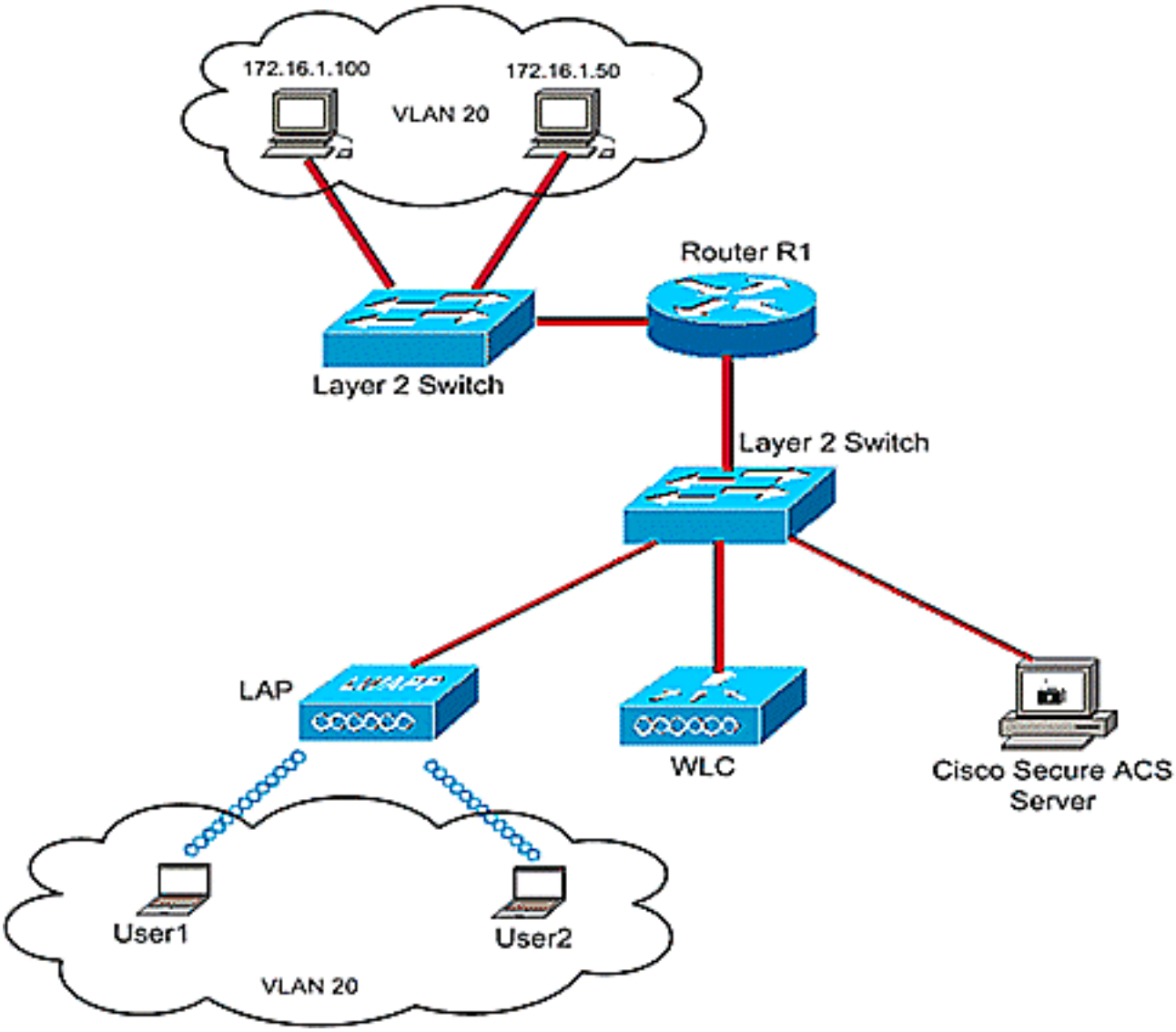
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        ACL Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
• Type - 26 for Vendor-Specific
• Length - >7
• Vendor-Id - 14179
• Vendor type - 6
• Vendor length - >0
• Value - A string that includes the name of the ACL to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

Pour plus d'informations sur Cisco Unified Wireless Network Identity Networking, reportez-vous à la section Configuration de la mise en réseau d'identité du document Configuration des solutions de sécurité.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Dans cette configuration, le contrôleur de réseau local sans fil WLC et le LAP sont utilisés pour fournir des services sans fil aux utilisateurs des services A et B. Tous les utilisateurs sans fil utilisent un bureau WLAN (SSID) commun pour accéder au réseau et se trouvent dans le VLAN Office-VLAN.



Le serveur Cisco Secure ACS sert à authentifier les utilisateurs sans fil. L'authentification EAP est utilisée pour authentifier les utilisateurs. Le WLC, le LAP et le serveur Cisco Secure ACS sont connectés à un commutateur de couche 2 comme indiqué.

Le routeur R1 connecte les serveurs du côté câblé via le commutateur de couche 2, comme indiqué. Le routeur R1 agit également en tant que serveur DHCP, qui fournit des adresses IP aux clients sans fil à partir du sous-réseau 172.16.0.0/16.

Vous devez configurer les périphériques de sorte que ceci se produise :

L'utilisateur 1 du service A n'a accès qu'au serveur 172.16.1.100

L'utilisateur2 du service B n'a accès qu'au serveur 172.16.1.50

Pour ce faire, vous devez créer 2 listes de contrôle d'accès sur le WLC : l'une pour l'utilisateur 1 et l'autre pour l'utilisateur 2. Une fois les listes de contrôle d'accès créées, vous devez configurer le serveur Cisco Secure ACS pour renvoyer l'attribut de nom de liste de contrôle d'accès au WLC une fois l'authentification de l'utilisateur sans fil réussie. Le WLC applique ensuite la liste de contrôle d'accès à l'utilisateur et, par conséquent, au réseau est limité en fonction du profil utilisateur.

Remarque : ce document utilise l'authentification LEAP pour authentifier les utilisateurs. Cisco LEAP est vulnérable aux attaques de dictionnaires. Dans les réseaux en temps réel, des méthodes d'authentification plus sécurisées telles que EAP FAST doivent être utilisées. Comme le document a pour objet d'expliquer comment configurer la fonction de liste de contrôle d'accès par utilisateur, LEAP est utilisé pour la simplicité.

La section suivante fournit les instructions pas à pas pour configurer les périphériques de cette configuration.

Configuration

Avant de configurer la fonctionnalité ACL par utilisateur, vous devez configurer le WLC pour le fonctionnement de base et enregistrer les LAP sur le WLC. Ce document suppose que WLC est configuré pour les opérations de base et que les LAP sont enregistrés au WLC. Si vous êtes un nouvel utilisateur, qui tente de configurer le WLC pour le fonctionnement de base avec les LAP, référez-vous à Enregistrement d'un LAP (Lightweight AP) à un contrôleur LAN sans fil (WLC).

Une fois les LAP enregistrés, procédez comme suit pour configurer les périphériques pour cette configuration :

1. Configurez le contrôleur de réseau local sans fil.
2. Configurez le serveur Cisco Secure ACS.
3. Vérifier la configuration

Remarque : Ce document traite de la configuration requise côté sans fil. Le document suppose que la configuration filaire est en place.

Configuration du contrôleur de réseau local sans fil

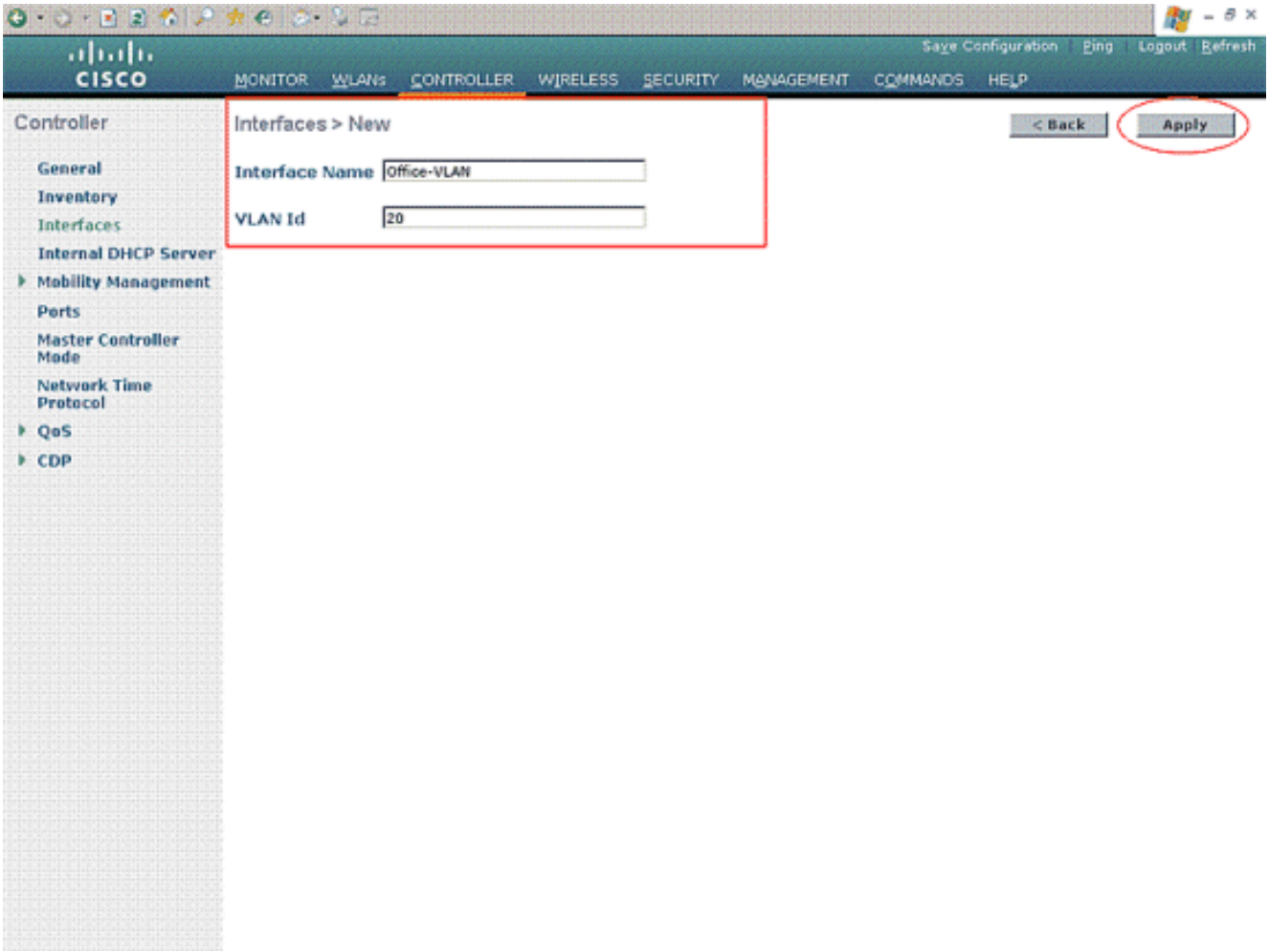
Sur le contrôleur de réseau local sans fil, procédez comme suit :

- Créez un VLAN pour les utilisateurs sans fil.
- Configurez le WLC pour authentifier les utilisateurs sans fil avec Cisco Secure ACS.
- Créez un nouveau WLAN pour les utilisateurs sans fil.
- Définissez les listes de contrôle d'accès pour les utilisateurs sans fil.

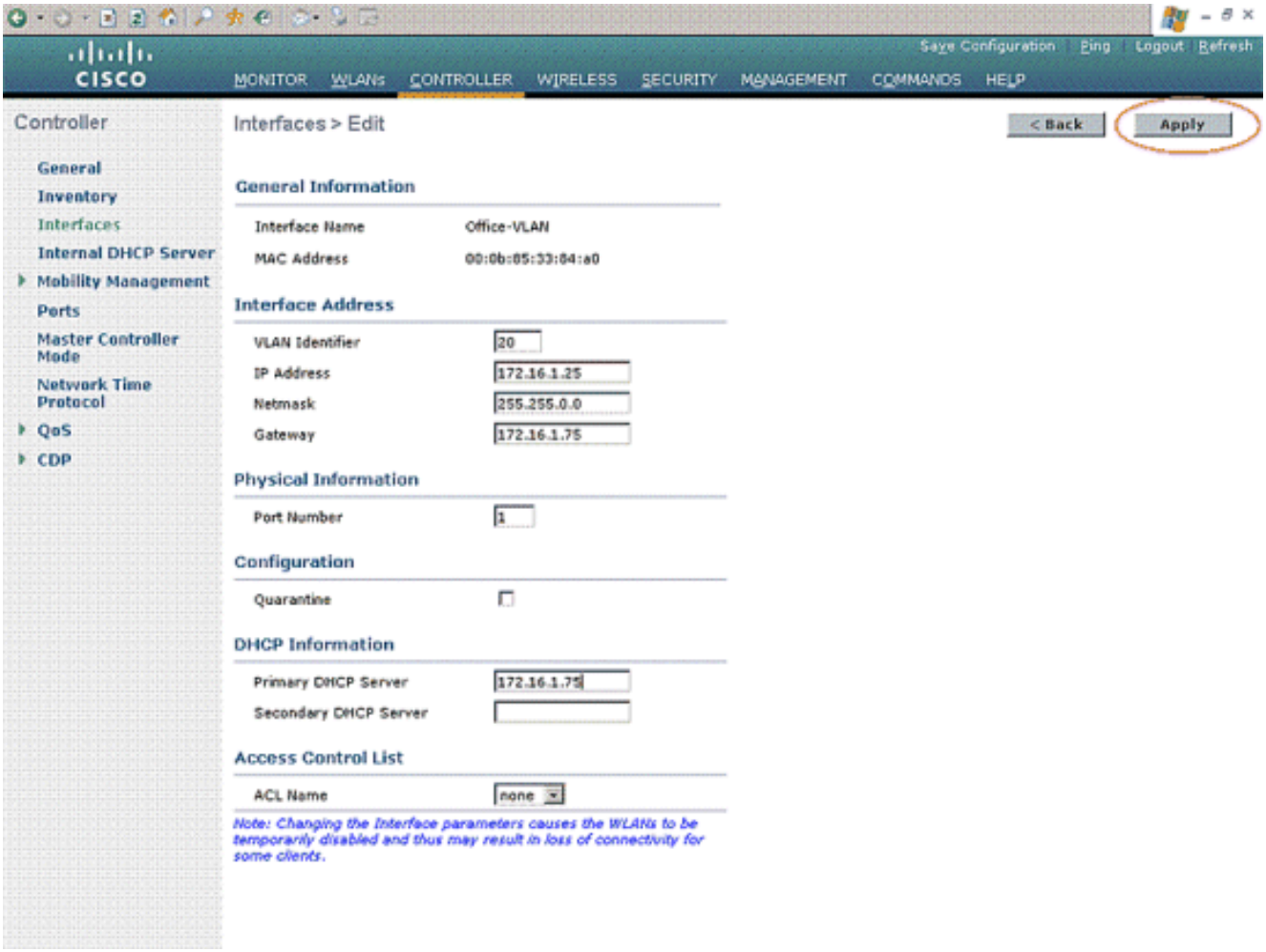
Créer un VLAN pour les utilisateurs sans fil

Afin de créer un VLAN pour les utilisateurs sans fil, complétez ces étapes.

1. Allez à l'interface graphique WLC et choisissez **Controller > Interfaces**. La fenêtre Interfaces apparaît. Cette fenêtre liste les interfaces qui sont configurées sur le contrôleur.
2. Afin de créer une nouvelle interface dynamique, cliquez sur **New.**
3. Dans la nouvelle fenêtre > Interfaces, entrez le nom de l'interface et l'ID VLAN. Cliquez ensuite sur Apply. Dans cet exemple, l'interface dynamique est nommée Office-VLAN et l'ID de VLAN est attribué à
   20.



4. Dans la fenêtre **Interfaces > Edit , entrez l'adresse IP, le masque de sous-réseau et la passerelle par défaut pour l'interface dynamique.** Attribuez-la à un port physique sur le WLC et entrez l'adresse IP sur le serveur DHCP. Cliquez ensuite sur
   Apply.



Pour cet exemple, ces paramètres sont utilisés pour l'interface Office-VLAN :

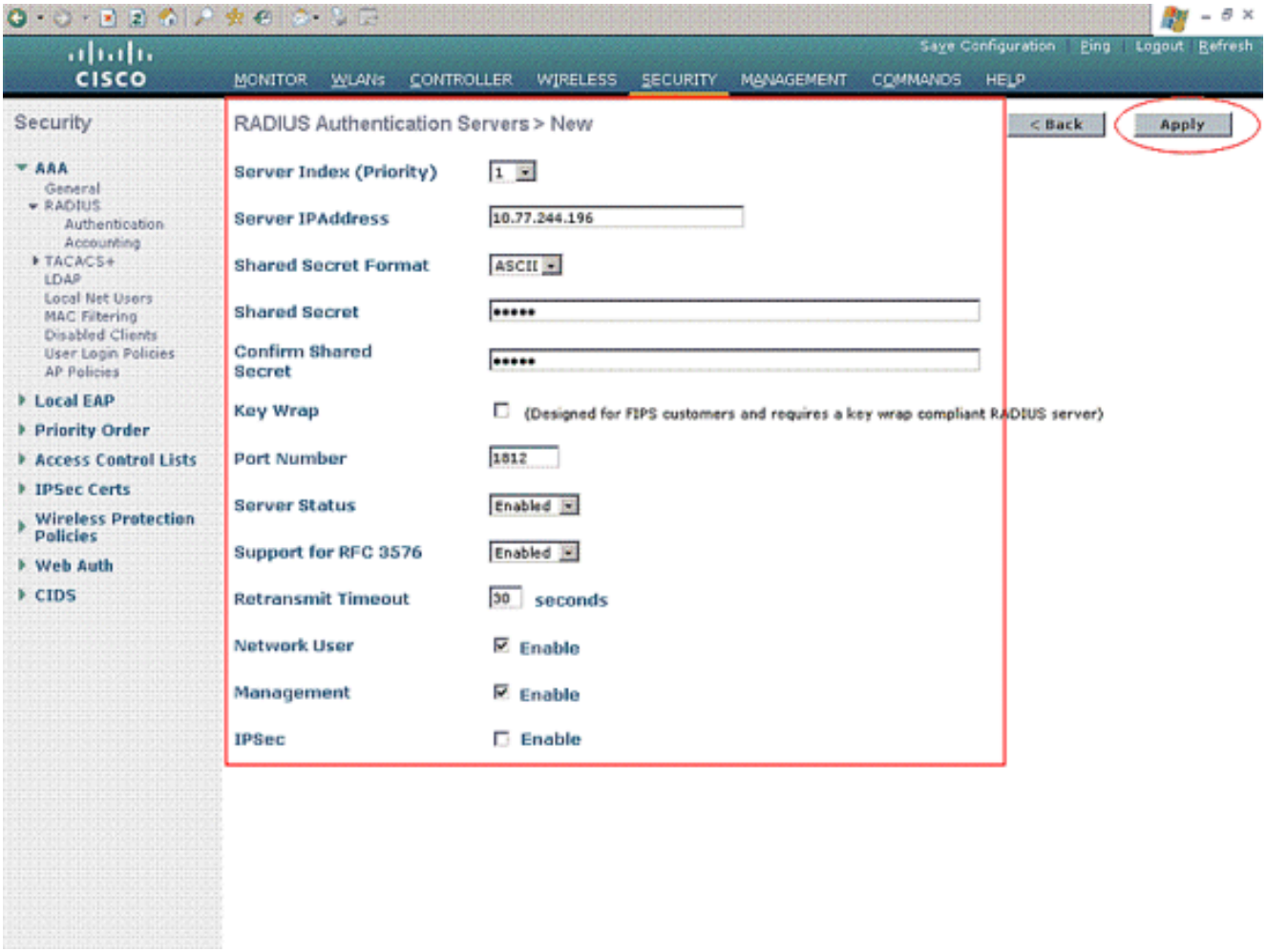
```
Office-VLAN
IP address: 172.16.1.25
Netmask: 255.255.0.0
Default gateway: 172.16.1.75 (sub-interface on Router R1)
Port on WLC: 1
DHCP server: 172.16.1.75
```

Configurer le WLC pour l'authentification avec Cisco Secure ACS

Le WLC doit être configuré pour transférer les informations d'identification de l'utilisateur à un serveur RADIUS externe (dans ce cas, Cisco Secure ACS). Le serveur RADIUS valide ensuite les informations d'identification de l'utilisateur et renvoie l'attribut de nom de la liste de contrôle d'accès au WLC une fois l'authentification de l'utilisateur sans fil réussie.

Complétez ces étapes afin de configurer le WLC pour le serveur RADIUS :

1. Sélectionnez **Security et RADIUS Authentication** depuis la GUI du contrôleur pour afficher la page des serveurs d'authentification RADIUS. Cliquez alors sur **New afin de définir un serveur RADIUS.**
2. Définissez les paramètres du serveur RADIUS sur la page **RADIUS Authentication Servers > New .** Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du
serveur.

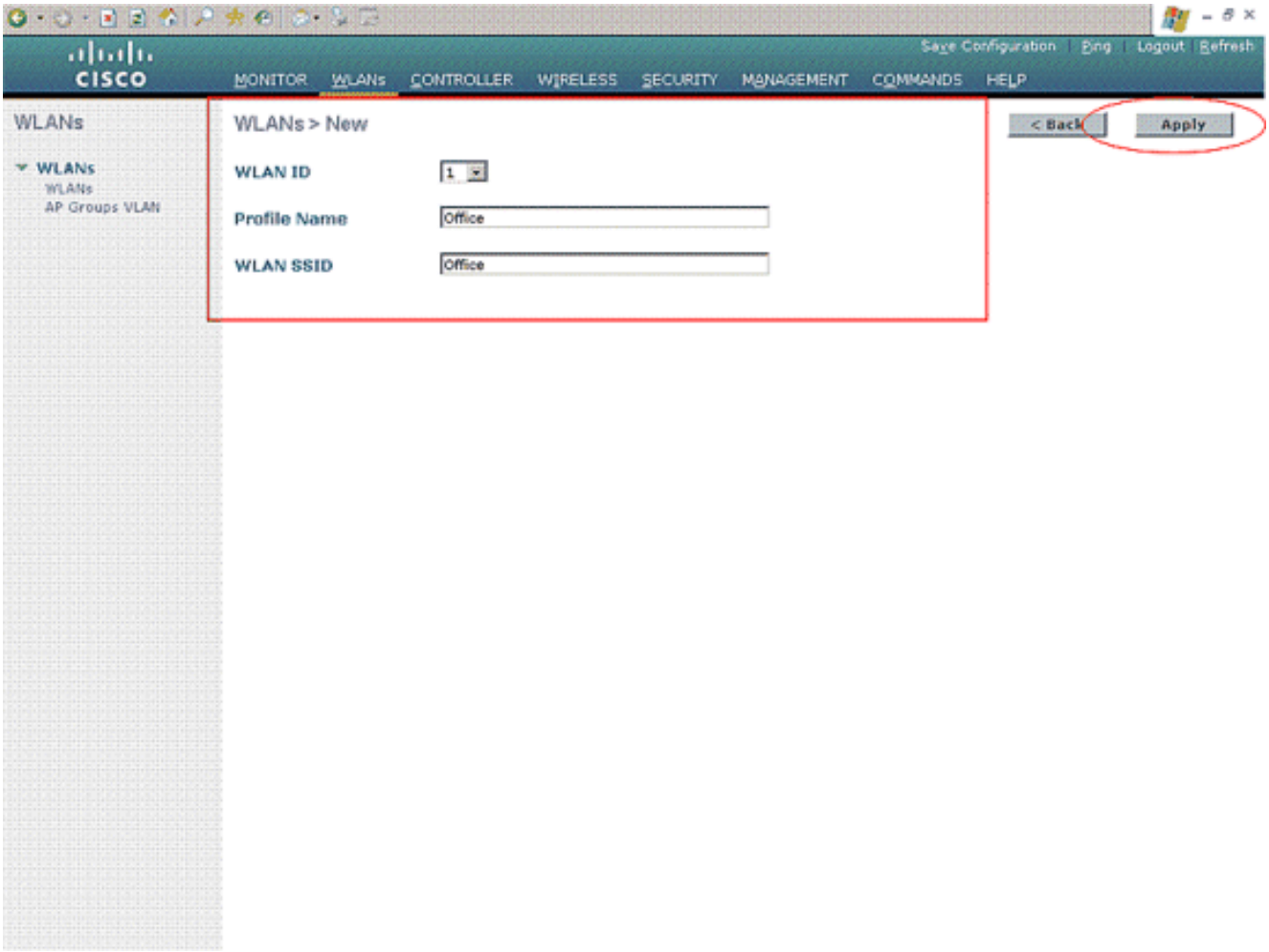


3. Les cases à cocher d'utilisateur du réseau et de gestion déterminent si l'authentification basée sur RADIUS s'applique pour la gestion et les utilisateurs du réseau. Cet exemple utilise Cisco Secure ACS comme serveur RADIUS avec l'adresse IP 10.77.244.196. Cliquez sur Apply.

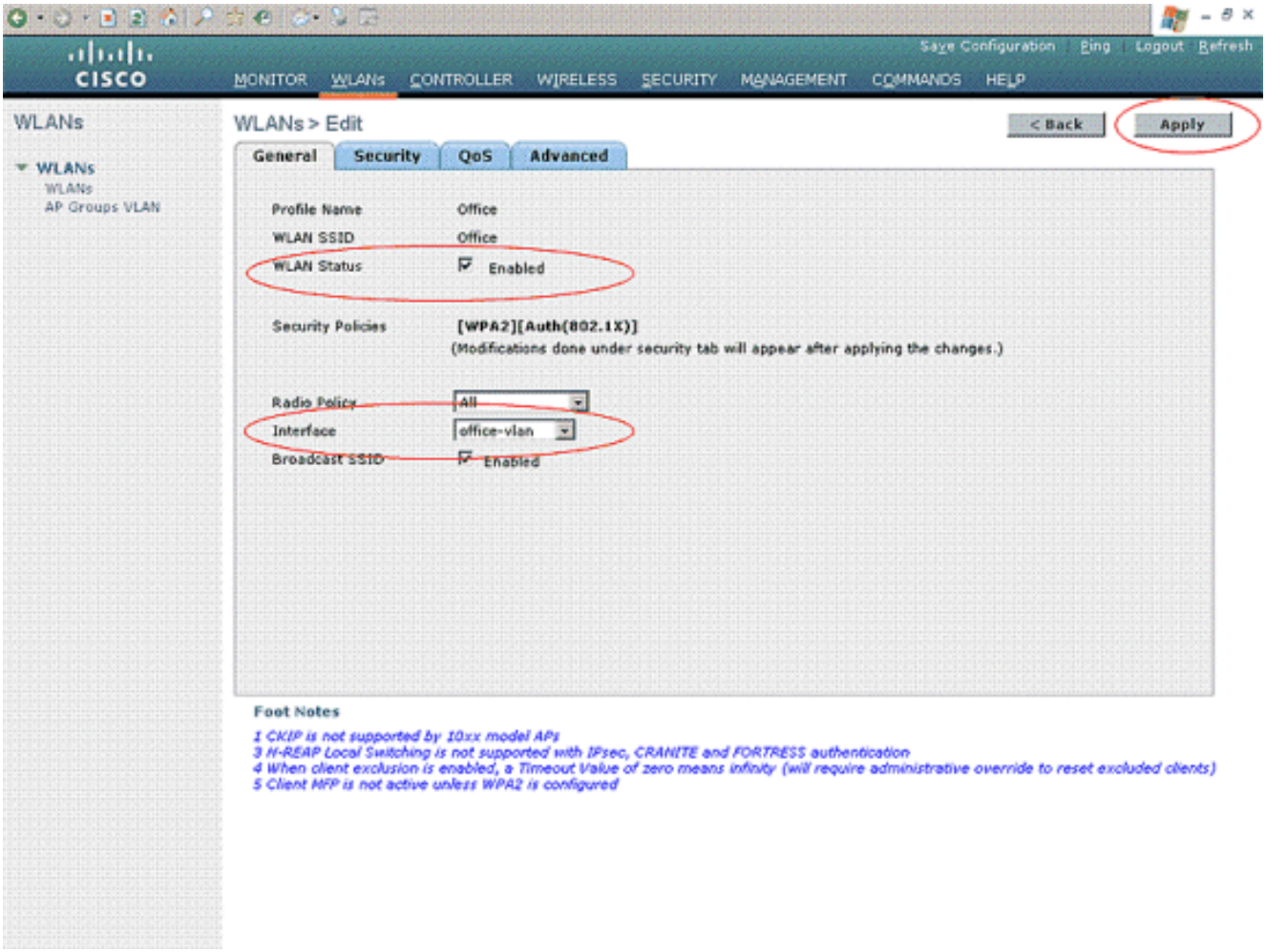
Créer un nouveau WLAN pour les utilisateurs sans fil

Ensuite, vous devez créer un WLAN auquel les utilisateurs sans fil peuvent se connecter. Pour créer un nouveau WLAN, procédez comme suit :

1. Dans l'interface utilisateur graphique du contrôleur de réseau local sans fil, cliquez sur **WLAN**. Cette page énumère les WLAN qui existent sur le contrôleur.
2. Sélectionnez **New afin de créer un nouveau WLAN.** Entrez l'ID WLAN, le nom de profil et le SSID WLAN pour le WLAN, puis cliquez sur **Apply**. Pour cette configuration, créez un WLAN **Office**.

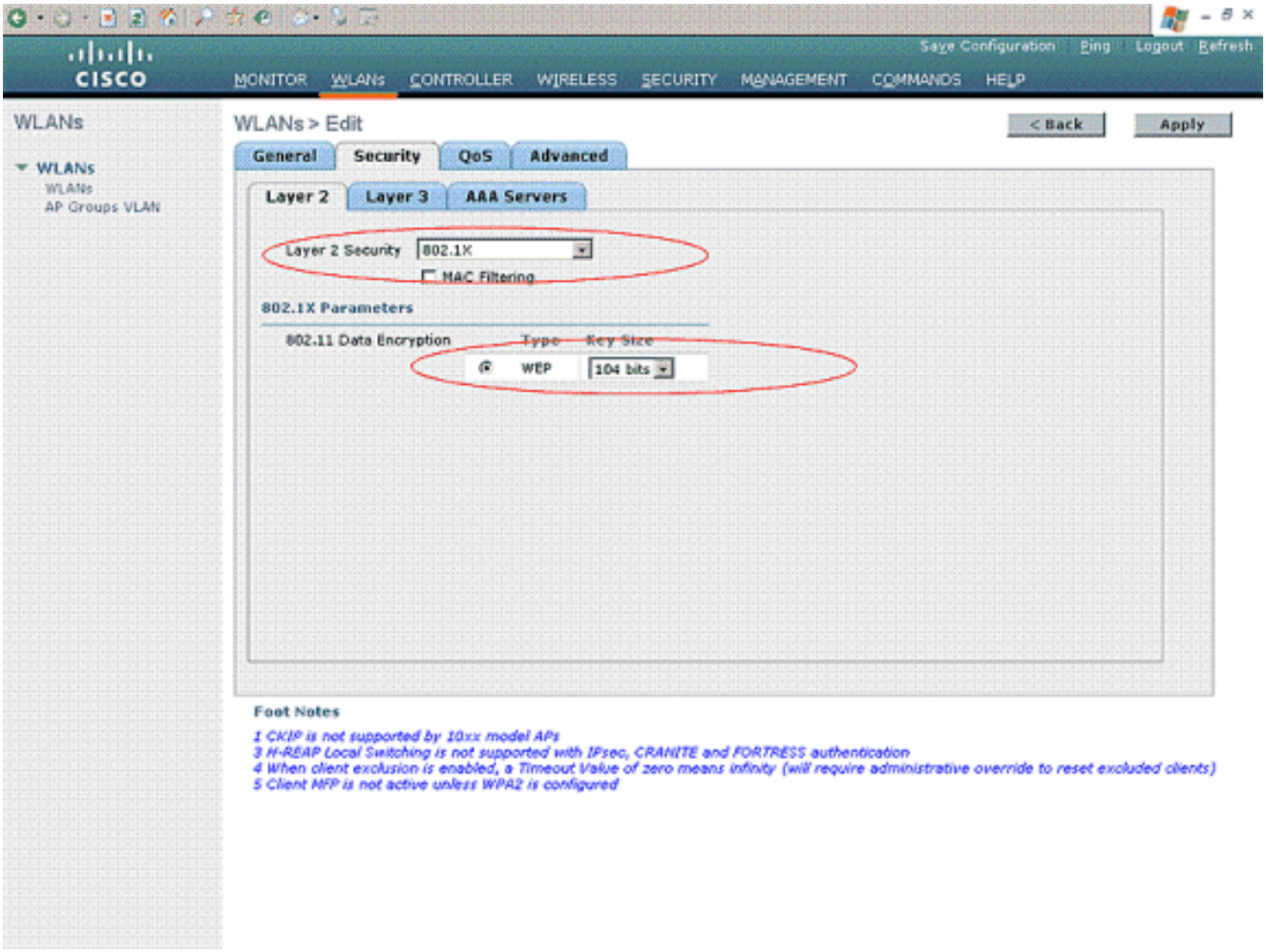


3. Une fois que vous avez créé un nouveau WLAN, la page **WLAN > Edit du nouveau WLAN apparaît.** Dans cette page, vous pouvez définir différents paramètres spécifiques à ce WLAN qui incluent les stratégies générales, la sécurité, la qualité de service et les paramètres avancés.

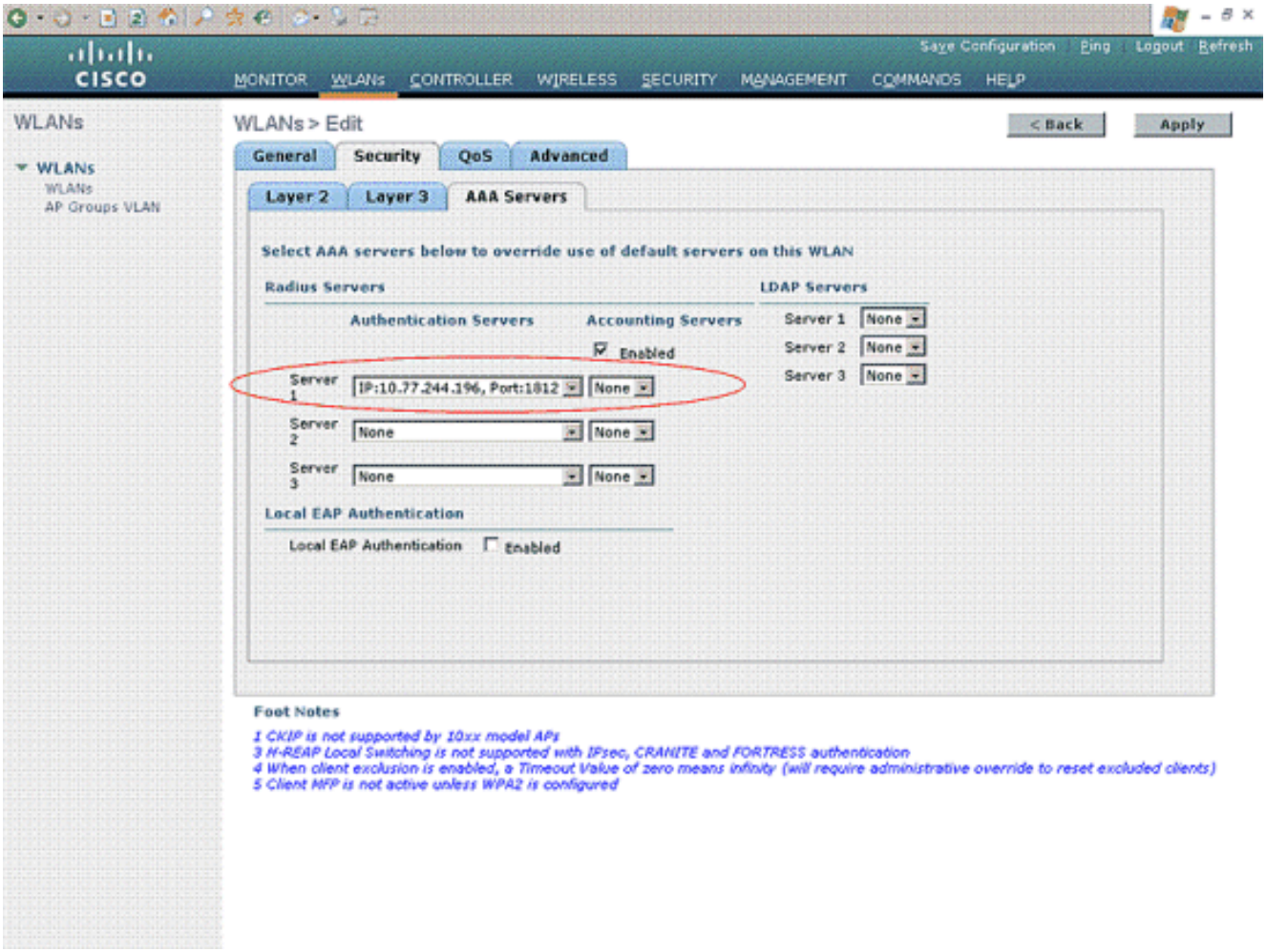


Vérifiez **l'état du WLAN** sous Stratégies générales afin d'activer le WLAN. Choisissez l'interface appropriée dans le menu déroulant. Dans cet exemple, utilisez l'interface **Office-vlan**. Les autres paramètres de cette page peuvent être modifiés en fonction des besoins du réseau WLAN.

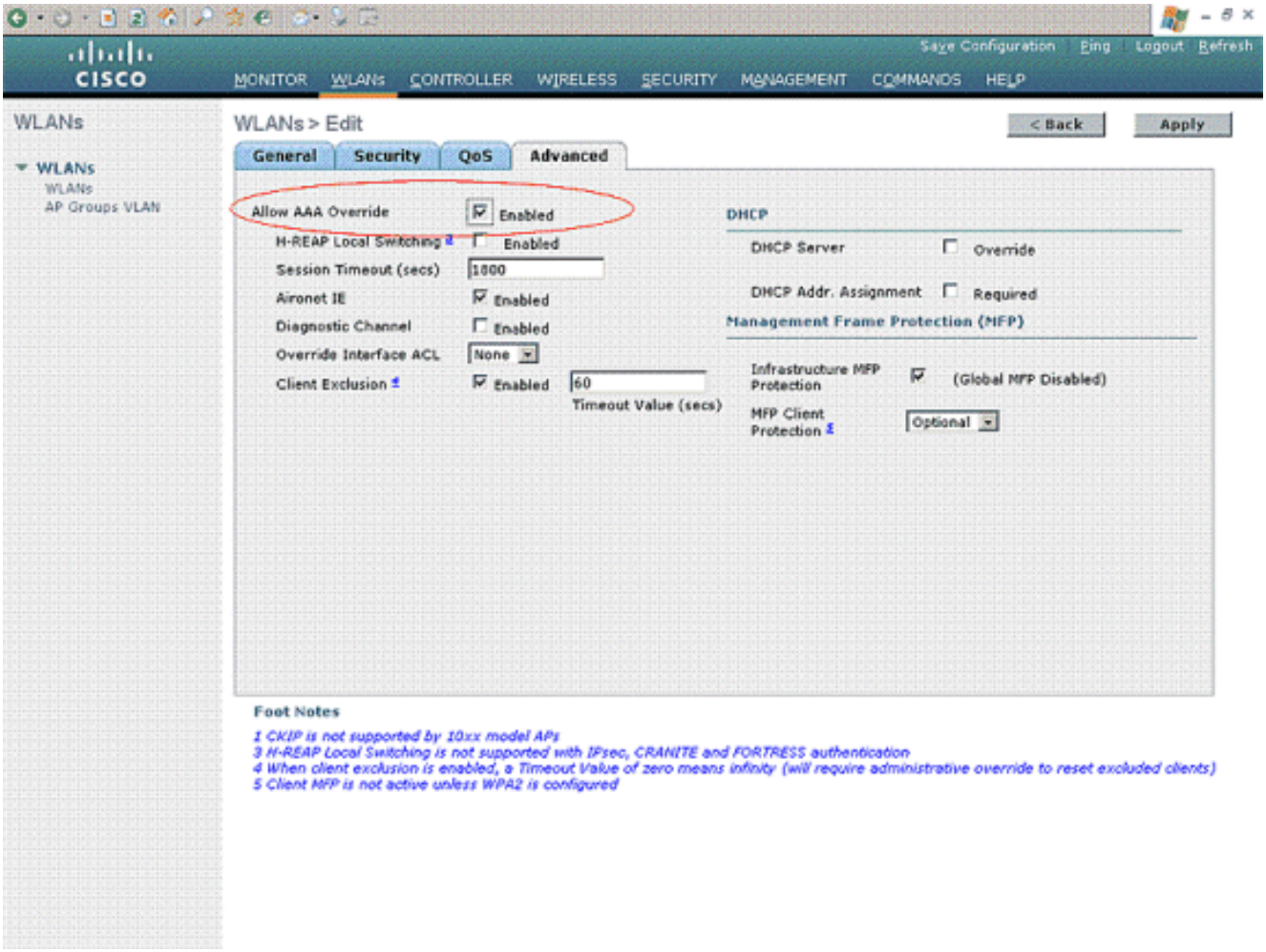
4. Sélectionnez l'onglet Security . Choisissez **802.1x** dans le menu déroulant de sécurité de couche 2 (car il s'agit d'une authentification LEAP). Sélectionnez la taille de clé WEP appropriée sous les paramètres
802.1x.



5. Sous l'onglet Sécurité, sélectionnez le sous-onglet **serveur AAA**. Sélectionnez le serveur AAA utilisé pour authentifier les clients sans fil. Dans cet exemple, utilisez le serveur ACS 10.77.244.196 pour authentifier les clients sans fil.



6. Sélectionnez l'onglet **Avancé**. Cochez **Allow AAA Override** pour configurer la substitution de stratégie utilisateur via AAA sur un réseau local sans fil.



Lorsque le remplacement AAA est activé et qu'un client a des paramètres d'authentification LAN sans fil AAA et contrôleur LAN sans fil Cisco en conflit, l'authentification du client est effectuée par le serveur AAA. Dans le cadre de cette authentification, le système d'exploitation déplace les clients du VLAN LAN sans fil de la solution de réseau local sans fil Cisco par défaut vers un VLAN retourné par le serveur AAA et prédéfini dans la configuration de l'interface du contrôleur LAN sans fil Cisco, qui ne se produit que lorsqu'il est configuré pour le filtrage MAC, le fonctionnement 802.1X et/ou WPA. Dans tous les cas, le système d'exploitation utilise également des valeurs de balise de priorité QoS, DSCP, 802.1p et ACL fournies par le serveur AAA, à condition qu'elles soient prédéfinies dans la configuration de l'interface du contrôleur LAN sans fil Cisco.

7. Choisissez les autres paramètres en fonction des besoins du réseau. Cliquez sur Apply.

Définir les listes de contrôle d'accès pour les utilisateurs

Vous devez créer deux listes de contrôle d'accès pour cette configuration :

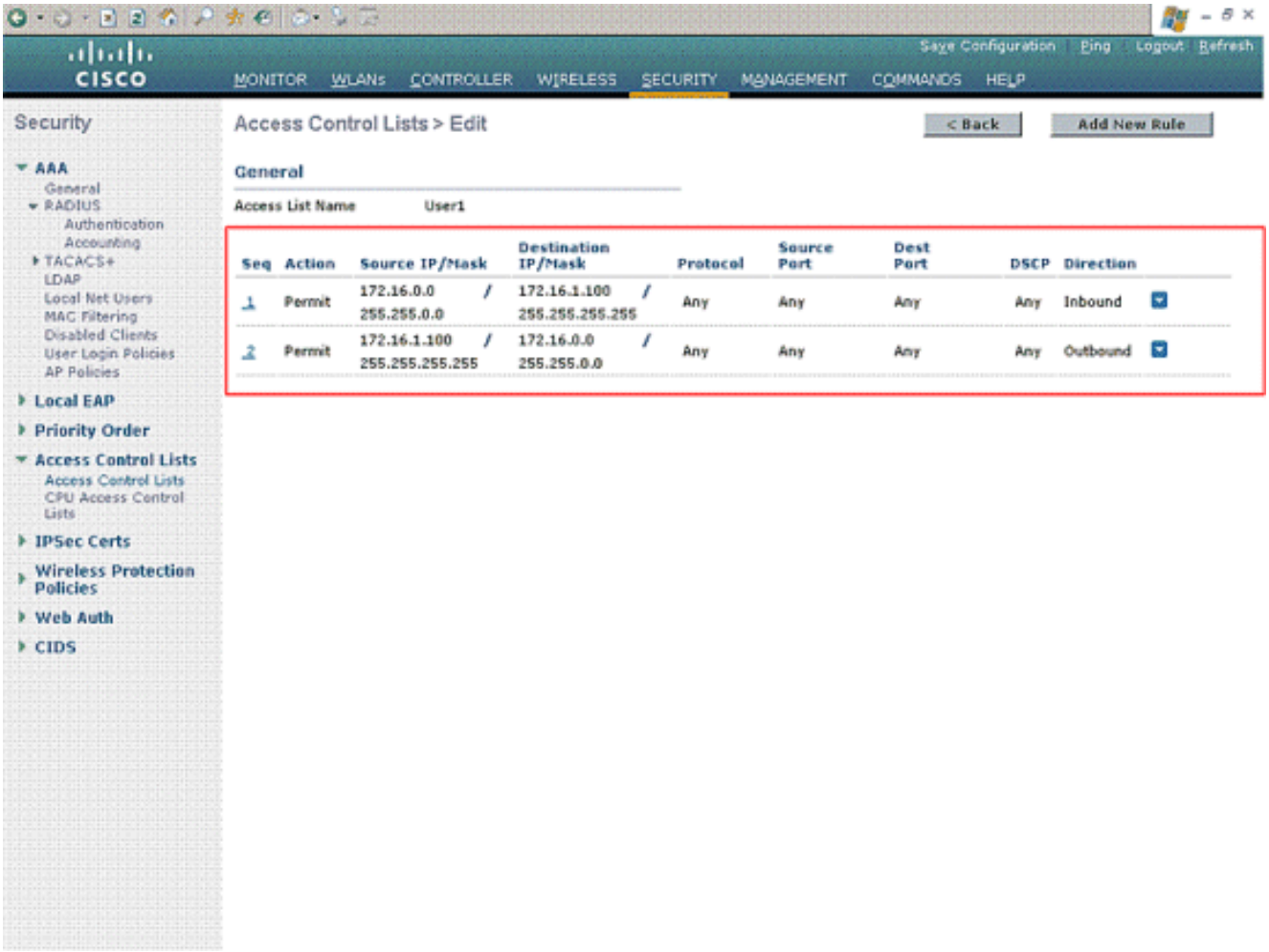
- ACL1 : Afin de fournir l'accès à User1 au serveur 172.16.1.100 uniquement
- ACL2 : Afin de fournir l'accès à User2 au serveur 172.16.1.50 uniquement

Complétez ces étapes pour configurer les listes de contrôle d'accès sur le WLC :

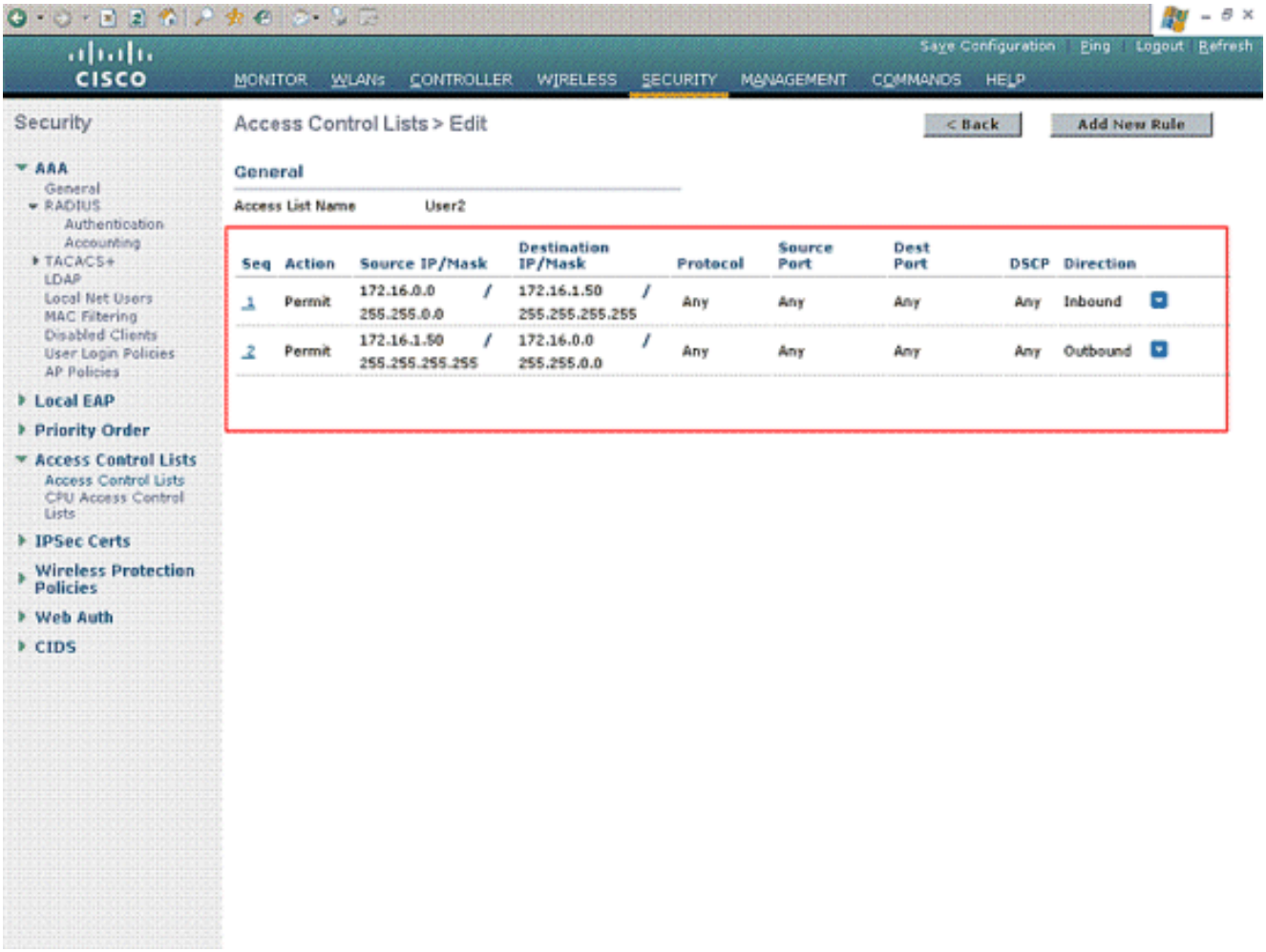
1. Dans l'interface graphique du WLC, sélectionnez **Security > Access Control Lists**. La page Listes de contrôle d'accès s'affiche. Cette page répertorie les listes de contrôle d'accès configurées sur le WLC. Il vous permet également de modifier ou de supprimer une liste de contrôle d'accès. Afin de créer une nouvelle liste de contrôle d'accès, cliquez sur **Nouveau**.
2. Cette page vous permet de créer de nouvelles listes de contrôle d'accès. Entrez le nom de la

liste de contrôle d'accès et cliquez sur **Apply**. Une fois la liste de contrôle d'accès créée, cliquez sur **Modifier** afin de créer des règles pour la liste de contrôle d'accès.

3. L'utilisateur 1 doit pouvoir accéder au serveur 172.16.1.100 uniquement et doit se voir refuser l'accès à tous les autres périphériques. Pour cela, vous devez définir ces règles.Référez-vous à Exemple de configuration des listes de contrôle d'accès sur un contrôleur de réseau local sans fil pour plus d'informations sur la façon de configurer des listes de contrôle d'accès sur des contrôleurs de réseau local sans fil.



4. De même, vous devez créer une liste de contrôle d'accès pour l'utilisateur 2, qui autorise l'accès de l'utilisateur 2 au serveur 172.16.1.50 uniquement. Il s'agit de la liste de contrôle d'accès requise pour l'utilisateur 2.



Vous avez maintenant configuré le contrôleur de réseau local sans fil pour cette configuration. L'étape suivante consiste à configurer le serveur Cisco Secure Access Control pour authentifier les clients sans fil et pour renvoyer l'attribut ACL Name au WLC une fois l'authentification réussie.

Configuration du serveur Cisco Secure ACS

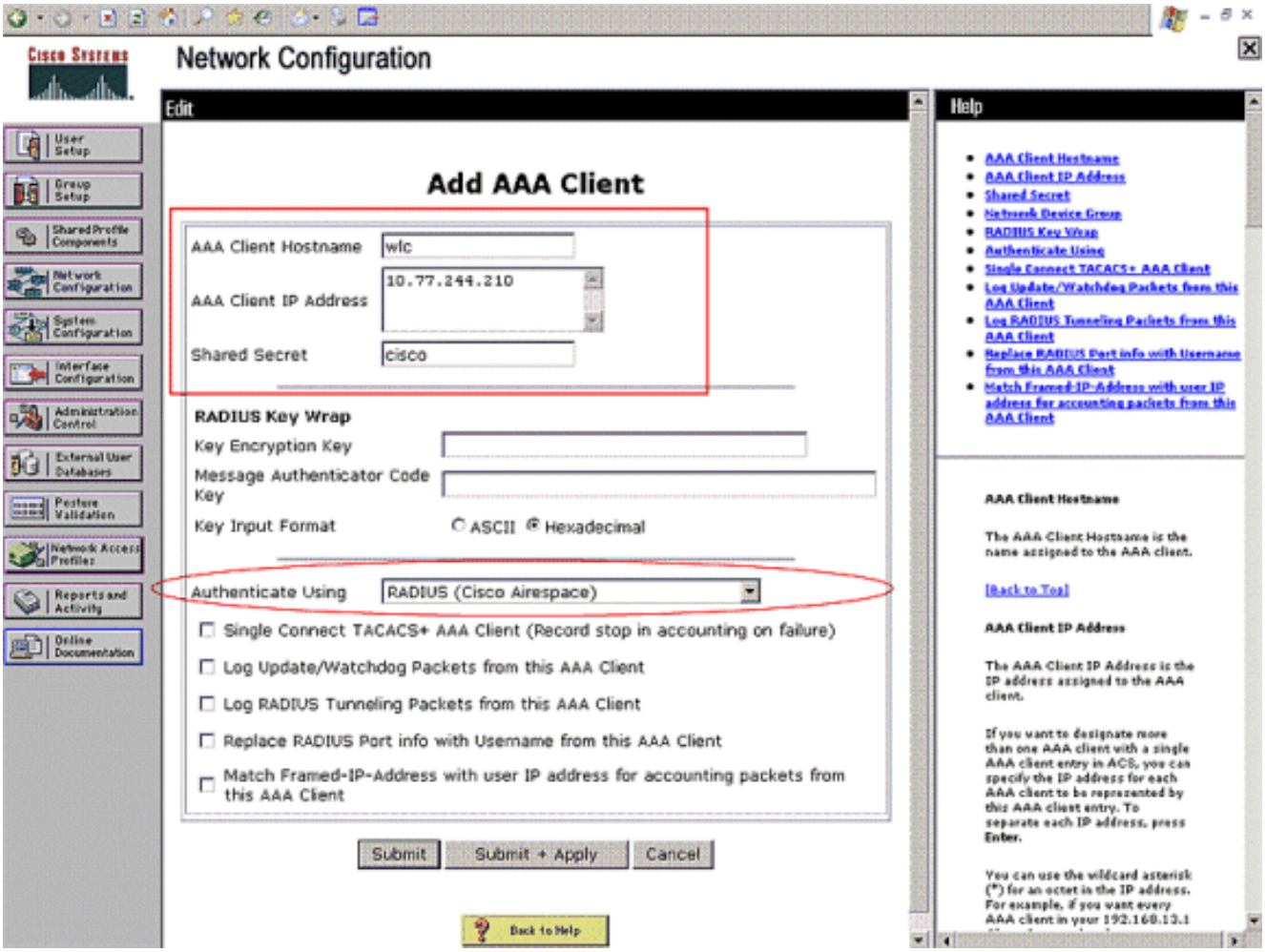
Pour que Cisco Secure ACS puisse authentifier les clients sans fil, procédez comme suit :

- Configurez le contrôleur de réseau local sans fil en tant que client AAA sur Cisco Secure ACS.
- Configurez les utilisateurs et les profils utilisateur sur Cisco Secure ACS.

Configurer le contrôleur de réseau local sans fil en tant que client AAA sur Cisco Secure ACS

Afin de configurer le contrôleur de réseau local sans fil en tant que client AAA sur Cisco Secure ACS, procédez comme suit :

1. Cliquez sur **Network Configuration > Add AAA client**. La page **Add AAA client** s'affiche. Dans cette page, définissez le nom du système WLC, l'adresse IP de l'interface de gestion, le secret partagé et l'authentification à l'aide de **Radius Airespace**. Voici un exemple :



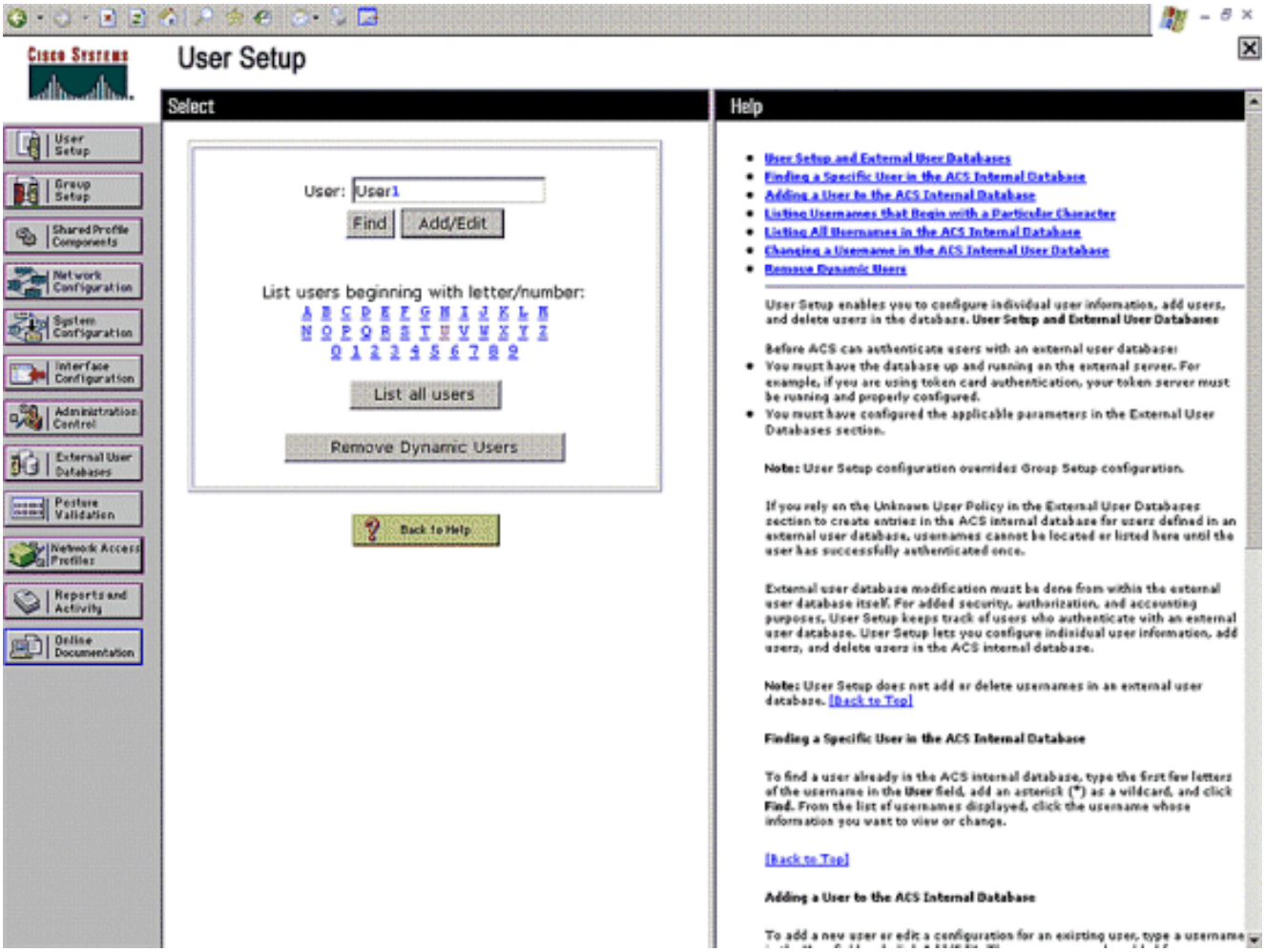
Remarque : Le secret partagé configuré sur Cisco Secure ACS doit correspondre au secret partagé configuré sur le WLC sous **RADIUS Authentication Servers > New**.

2. Cliquez sur **Soumettre+Appliquer**.

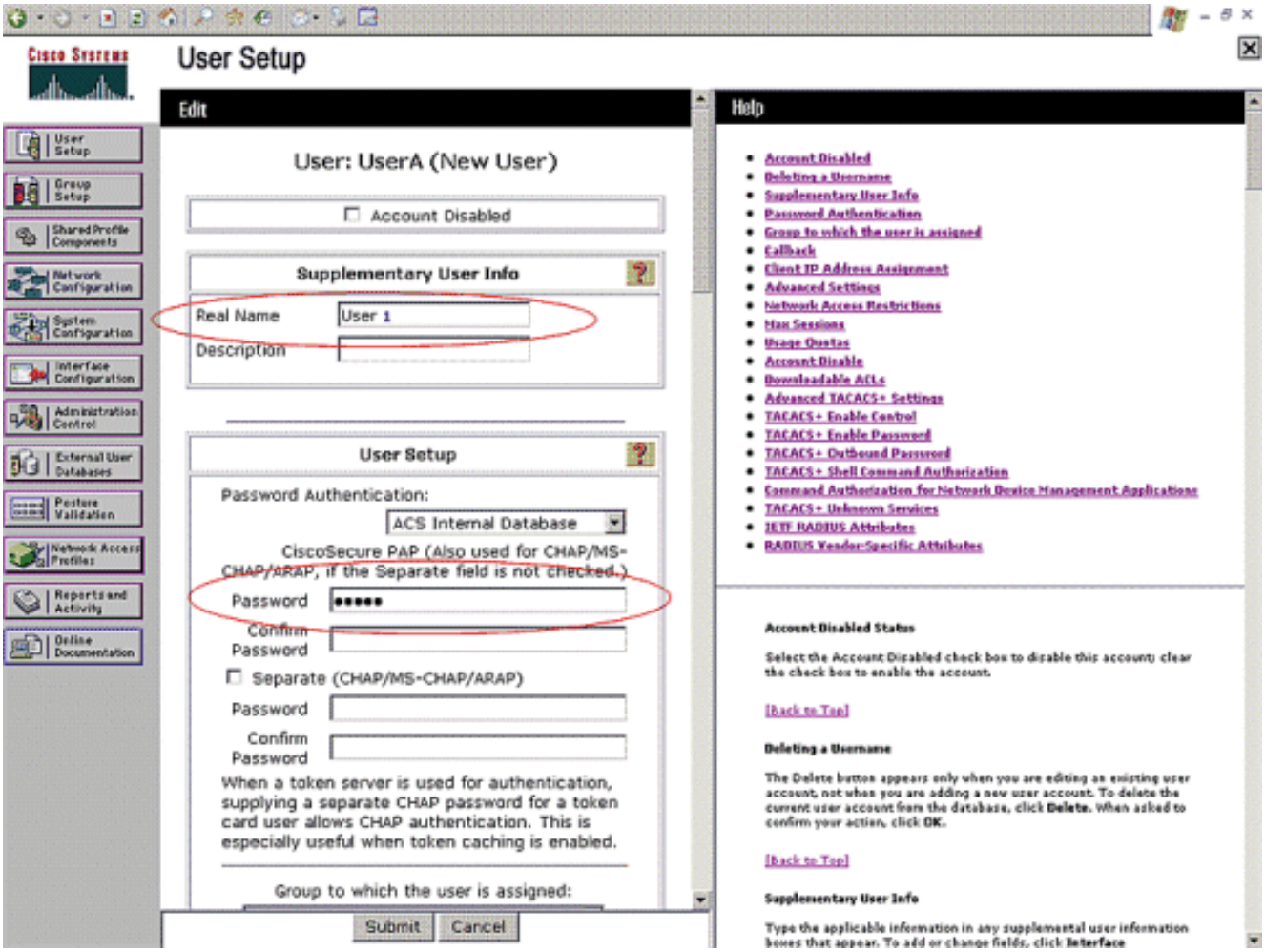
Configurer les utilisateurs et le profil utilisateur sur Cisco Secure ACS

Afin de configurer les utilisateurs sur Cisco Secure ACS, procédez comme suit :

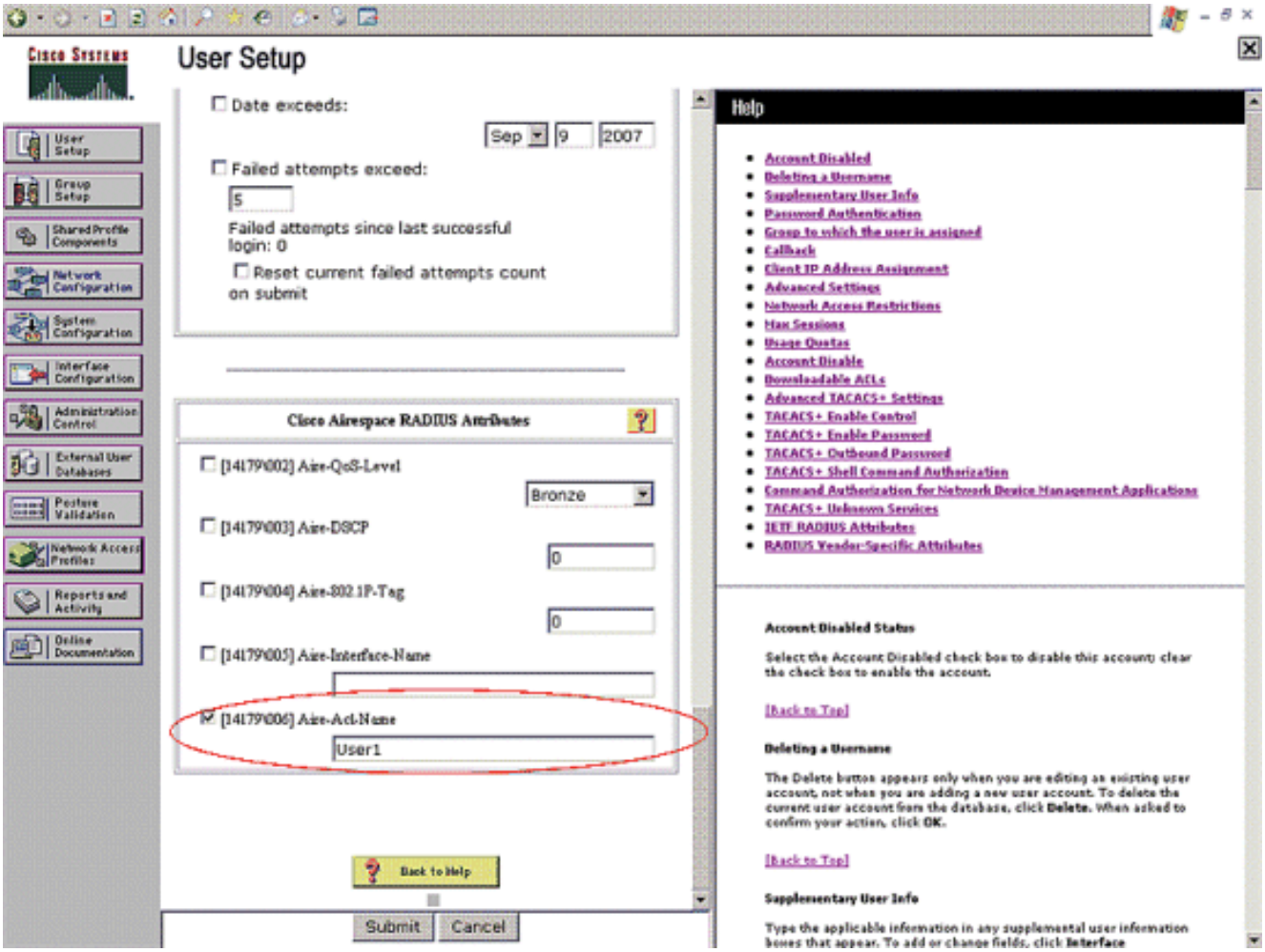
1. Choisissez **User Setup depuis l'interface graphique ACS, entrez le nom d'utilisateur et cliquez sur Add/Edit**. Dans cet exemple, l'utilisateur est **User1**.



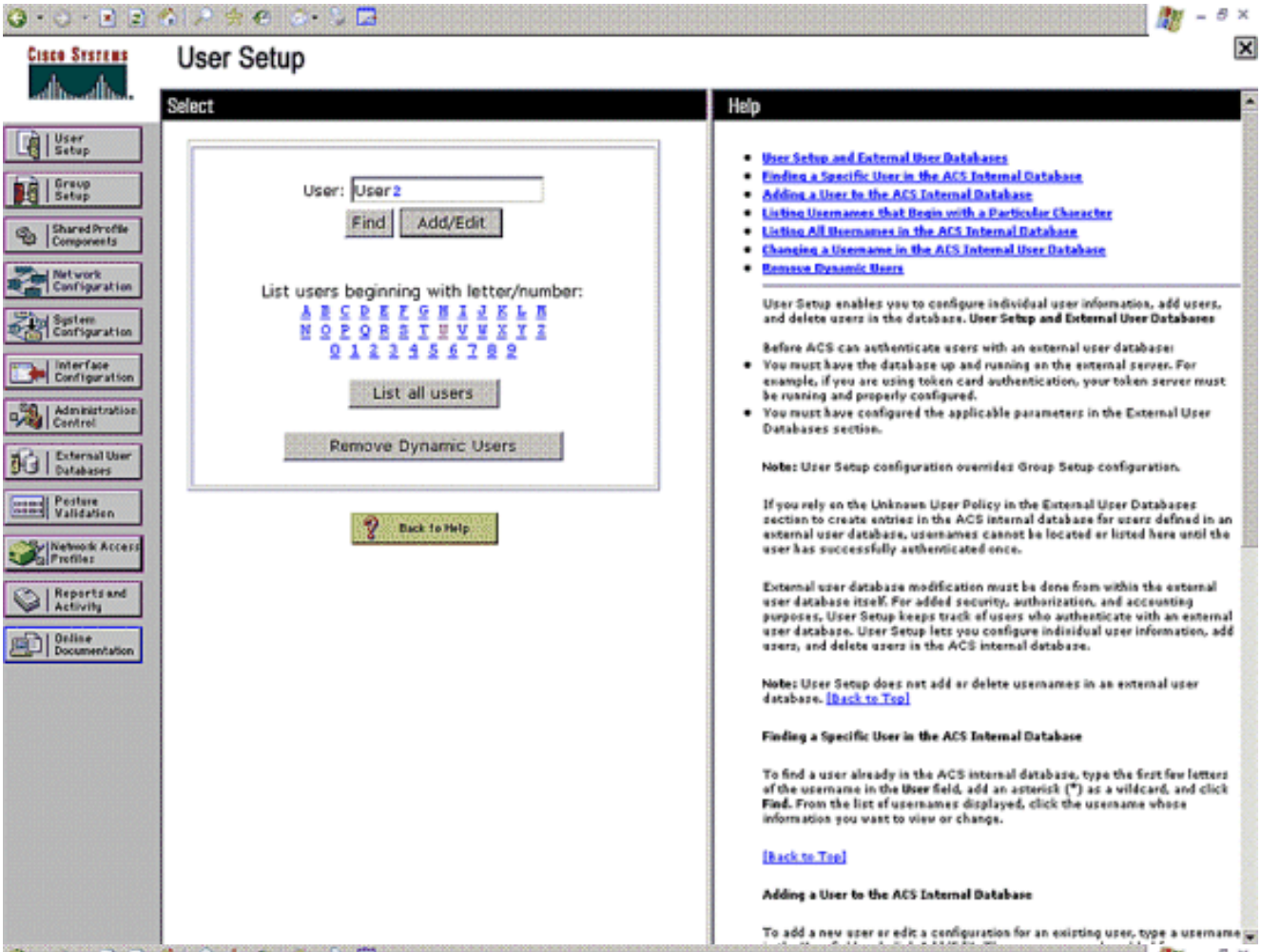
2. Lorsque la page **User Setup** apparaît, définissez tous les paramètres propres à l'utilisateur. Dans cet exemple, le nom d'utilisateur, le mot de passe, les informations utilisateur supplémentaires et les attributs RADIUS sont configurés car vous n'avez besoin que de ces paramètres pour l'authentification
EAP.

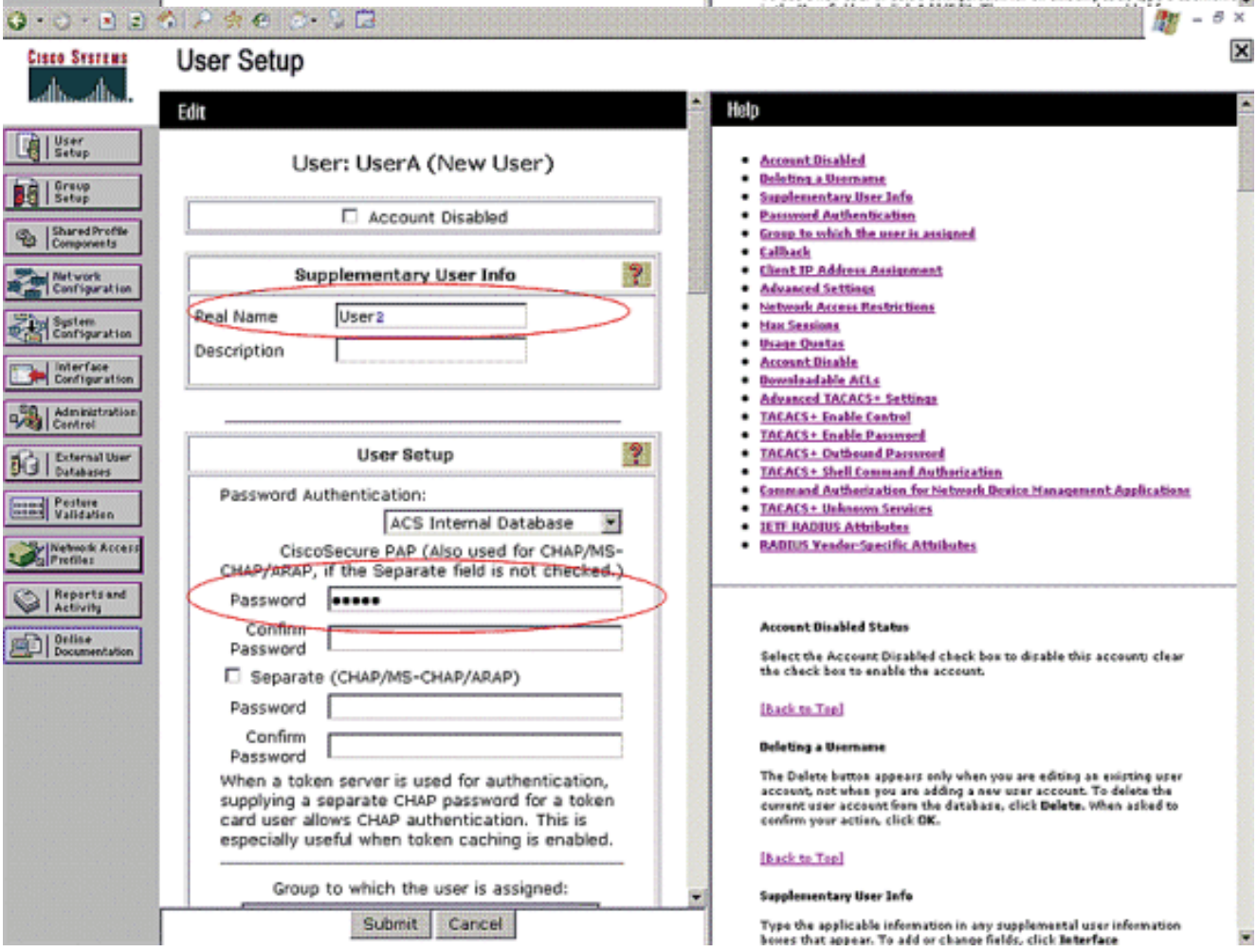


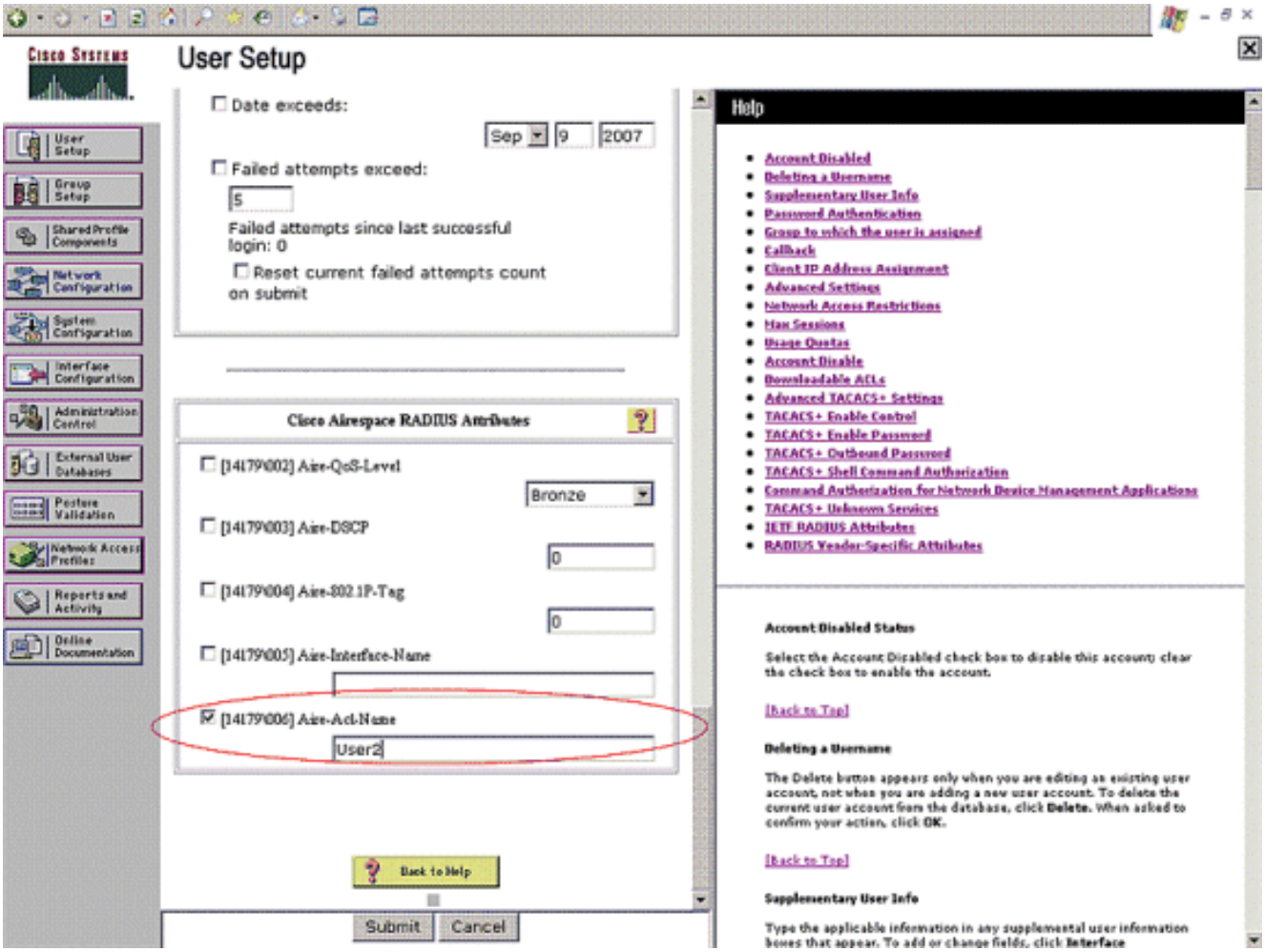
Faites défiler la page vers le bas jusqu'à ce que les attributs RADIUS Cisco Airespace soient spécifiques à l'utilisateur. Cochez la case **Aire-ACL-Name** pour permettre à ACS de renvoyer le nom de la liste de contrôle d'accès au WLC avec la réponse d'authentification réussie.
Pour User1, créez une liste de contrôle d'accès User1 sur le WLC. Entrez le nom de la liste de contrôle d’accès sous la forme
User1.



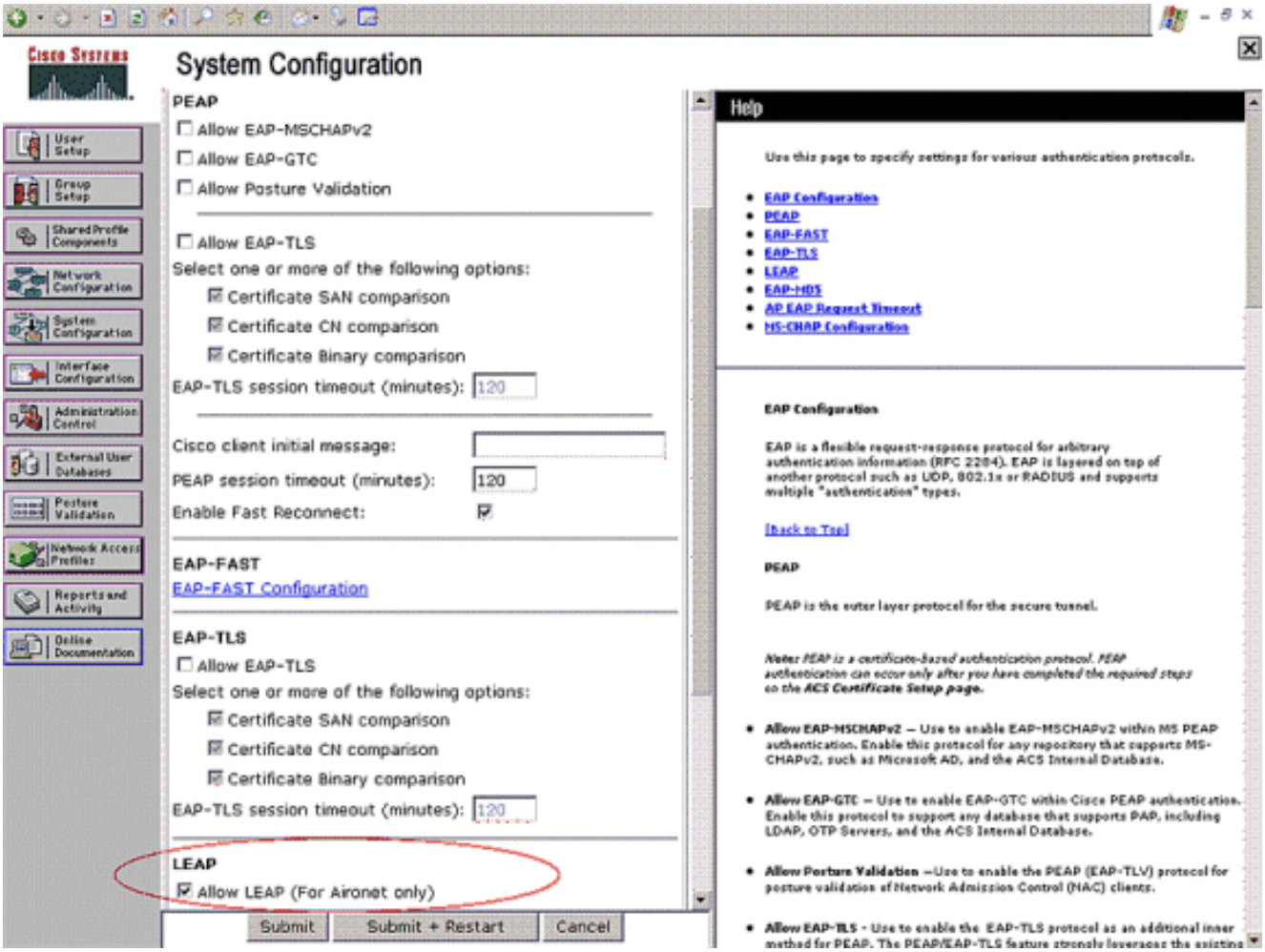
3. Répétez la même procédure pour créer User2 comme indiqué ici.


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


Cisco Systems
User Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Edit
User: UserA (New User)
Account Disabled
Supplementary User Info
Real Name
User2
Description
User Setup
Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Password
Confirm Password
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
Group to which the user is assigned:
Submit
Cancel
Help
Account Disabled
Deleting a Username
Supplementary User Info
Password Authentication
Group to which the user is assigned
Callback
Client IP Address Assignment
Advanced Settings
Network Access Restrictions
Max Sessions
Usage Quotas
Account Disable
Downloadable ACLs
Advanced TACACS+ Settings
TACACS+ Enable Control
TACACS+ Enable Password
TACACS+ Outbound Password
TACACS+ Shell Command Authorization
Command Authorization for Network Device Management Applications
TACACS+ Unknown Services
IETF RADIUS Attributes
RADIUS Vendor-Specific Attributes
Account Disabled Status
Select the Account Disabled check box to disable this account; clear the check box to enable the account.
[Back to Top]
Deleting a Username
The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action, click OK.
[Back to Top]
Supplementary User Info
Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click Interface



4. Cliquez sur **System Configuration et sur Global Authentication Setup, afin de vous assurer que le serveur d'authentification est configuré pour exécuter la méthode d'authentification EAP souhaitée.** Dans les paramètres de configuration EAP, sélectionnez la méthode EAP appropriée. Cet exemple utilise l'authentification LEAP. Cliquez sur **Submit lorsque vous avez**
terminé.



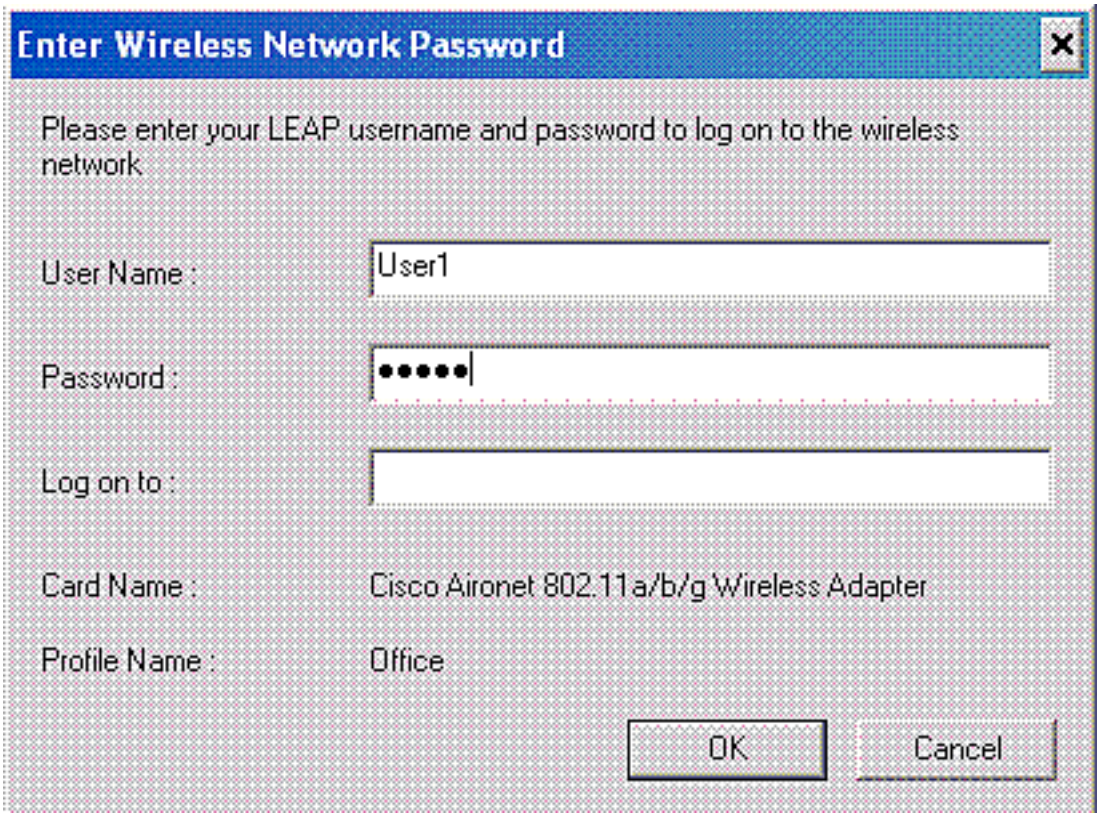
Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

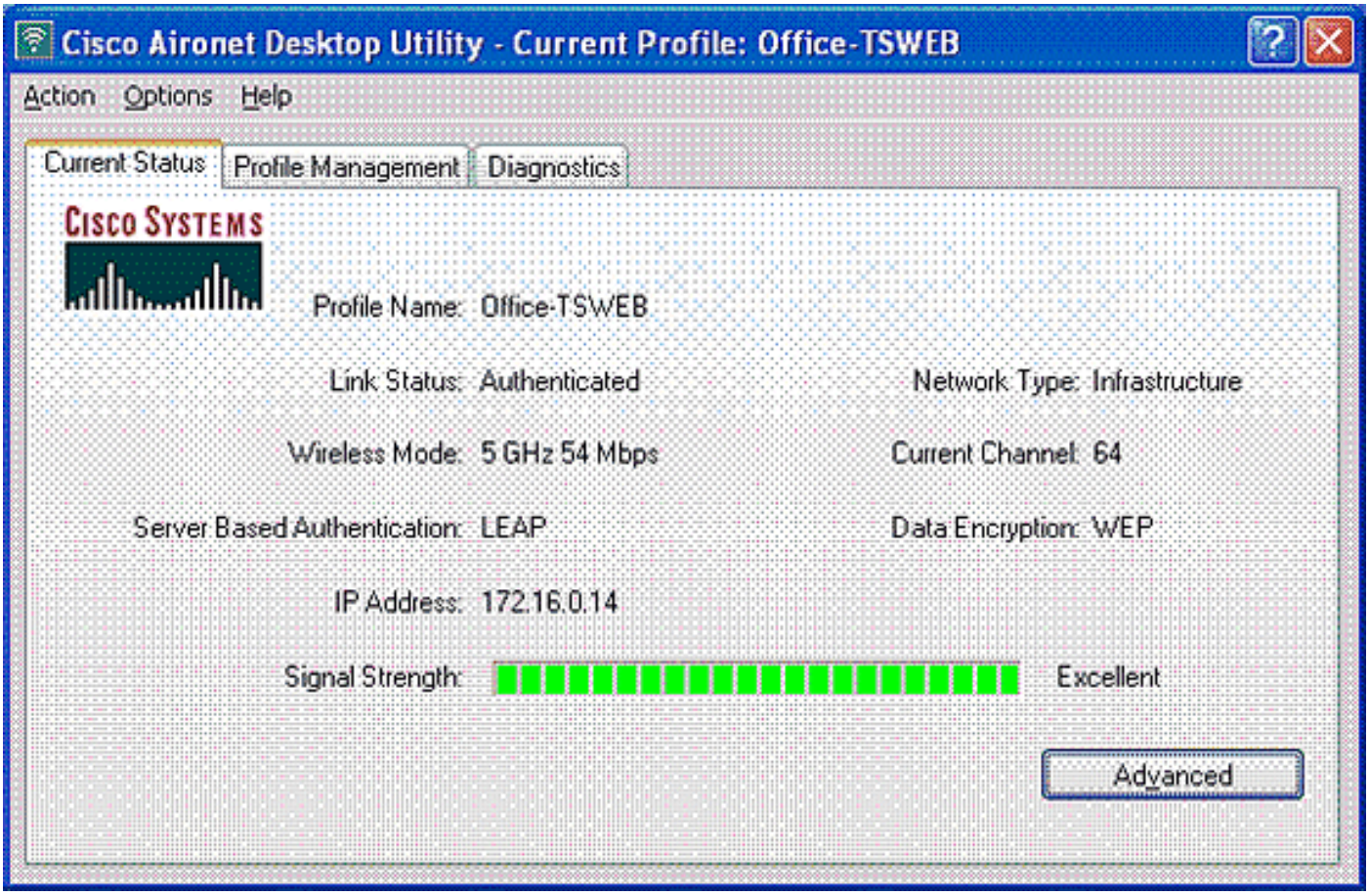
Essayez d'associer un client sans fil au point d'accès léger à l'authentification LEAP afin de vérifier si la configuration fonctionne comme prévu.

Remarque : ce document suppose que le profil client est configuré pour l'authentification LEAP. Reportez-vous à la section Utilisation de l'authentification EAP pour plus d'informations sur le mode de configuration de l'adaptateur client sans fil 802.11 a/b/g pour l'authentification LEAP.

Une fois le profil du client sans fil activé, l'utilisateur est invité à fournir le nom d'utilisateur/mot de passe pour l'authentification LEAP. C'est ce qui se passe lorsque l'utilisateur 1 tente de s'authentifier auprès du LAP.



Le point d'accès léger, puis le WLC, transmettent les identifiants de l'utilisateur au serveur RADIUS externe (Cisco Secure ACS) afin de valider les identifiants. Le serveur RADIUS compare les données à la base de données utilisateur et, une fois l'authentification réussie, renvoie le nom de la liste de contrôle d'accès configuré pour l'utilisateur au WLC. Dans ce cas, l'utilisateur 1 de la liste de contrôle d'accès est renvoyé au WLC.

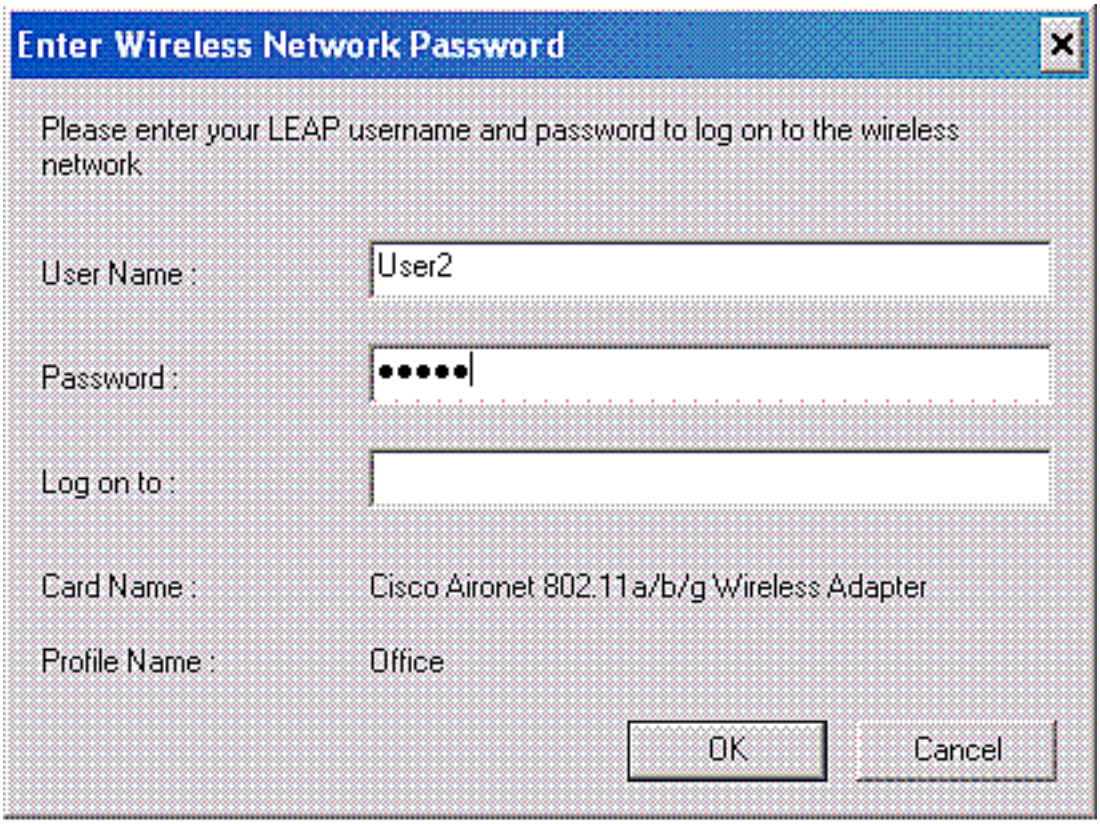


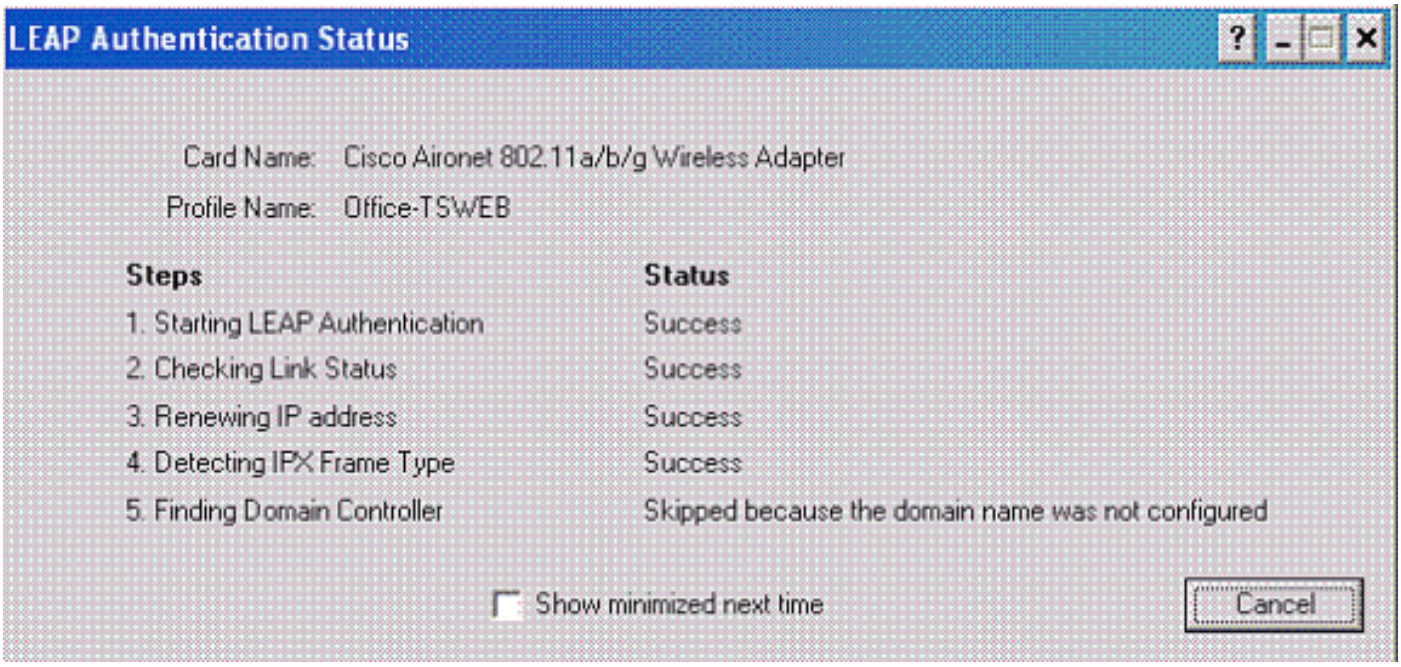
Le contrôleur de réseau local sans fil applique cette liste de contrôle d’accès à l’utilisateur 1. Ce

résultat de la requête ping indique que l'utilisateur 1 peut accéder uniquement au serveur 172.16.1.100, mais pas à tout autre périphérique.

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

Pinging 172.16.1.100 with 32 bytes of data:

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

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

D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

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

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

De même, lorsque l'utilisateur2 tente d'accéder au WLAN, le serveur RADIUS, une fois l'authentification réussie, retourne l'utilisateur ACL 2 au WLC.





Le contrôleur de réseau local sans fil applique cette liste de contrôle d'accès à l'utilisateur 2. Ce résultat de la requête ping montre que l'utilisateur2 peut accéder uniquement au serveur 172.16.1.50, mais pas à tout autre périphérique.

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

Pinging 172.16.1.50 with 32 bytes of data:

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

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

D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

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

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

Dépannage

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

Sur le contrôleur de réseau local sans fil, vous pouvez également utiliser ces commandes de débogage afin de dépanner l'authentification AAA

- **debug aaa all enable** - Configure le débogage de tous les messages AAA
- **debug dot1x packet enable** - Active le débogage de tous les paquets dot1x
- **debug client <MAC Address>** : active le débogage du client sans fil

Voici un exemple de la commande **debug aaa all enable**

Remarque : Certaines des lignes du résultat ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

```
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback.....0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType.....0x00140001
Thu Aug 16 14:42:54 2007:       proxyState.....00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet
   (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99  b4 19 27 28 eb 5f 35 9c
   ....-4....'(._5.
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73  65 72 31 1f 13 30 30 2d
   ......user1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 27 02
   ...A.....Q.20O'.
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d  87 9d 0b f9 dd e5 39 0d
   ..%...........9.
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96  dc c3 55 ff 7c 51 4e 75
   .....#....U.|QNu
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0  c6 2f 5e f5 65 e9 3e 2d
   ..;5^..../^.e.>-
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4  27 e6 d4 0e 1b 8e 5d 19
   ...6.1j.'.....].
Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01  00 04 18 0a 53 56 43 3d
   ...O.......SVC=
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb  90 ec 48 9b fb d7 ce ca
   0.1;P.l...H.....
Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09      ;d....
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Challenge received from RADIUS server
   10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize.....104
Thu Aug 16 14:42:54 2007:       resultCode.....255
Thu Aug 16 14:42:54 2007:       protocolUsed.....0x00000001
Thu Aug 16 14:42:54 2007:       proxyState.....
   00:40:96:AF:3E:93-03:01
```

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

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

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

Vous pouvez utiliser une combinaison de la commande **show wlan summary** afin de reconnaître lequel de vos WLAN utilise l'authentification serveur RADIUS. Vous pouvez ensuite afficher la commande **show client summary** afin de voir quelles adresses MAC (clients) sont authentifiées avec succès sur les WLAN RADIUS. Vous pouvez également comparer ces résultats avec vos journaux des tentatives réussies et échouées Cisco Secure ACS.

Cisco vous recommande de tester vos configurations ACL avec un client sans fil afin de vous assurer que vous les avez correctement configurées. S'ils ne fonctionnent pas correctement, vérifiez les listes de contrôle d'accès sur la page Web de la liste de contrôle d'accès et vérifiez que vos modifications de liste de contrôle d'accès ont été appliquées à l'interface du contrôleur.

Vous pouvez également utiliser ces commandes show afin de vérifier votre configuration :

- **show acl summary** - Afin d'afficher les listes de contrôle d'accès configurées sur le contrôleur, utilisez la commande **show acl summary**.

Voici un exemple :

```
(Cisco Controller) >show acl summary

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

- **show acl detail** <ACL_Name> : affiche des informations détaillées sur les listes de contrôle

d'accès configurées.Voici un exemple :**Remarque :** Certaines des lignes du résultat ont été déplacées vers la deuxième ligne en raison de contraintes d'espace.

```
Cisco Controller) >show acl detailed User1

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


(Cisco Controller) >show acl detailed User2

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

- **show client detail** <MAC Address of the client> - Affiche des informations détaillées sur le client sans fil.

Conseils de dépannage

Utilisez ces conseils pour dépanner :

- Vérifiez sur le contrôleur que le serveur RADIUS est en état actif et non en veille ou désactivé.
- Sur le contrôleur, vérifiez si le serveur RADIUS est sélectionné dans le menu déroulant du WLAN (SSID).
- Vérifiez que le serveur RADIUS reçoit et valide la demande d'authentification du client sans fil.
- Pour ce faire, vérifiez les rapports Passed Authentications et Failed Attempts sur le serveur ACS pour savoir si l'authentification a réussi ou échoué. Ces rapports sont disponibles sous l'option Reports and Activities sur le serveur ACS.

Informations connexes

- Listes de contrôle d'accès sur les contrôleurs de réseau local sans fil : Règles, limitations et exemples
- Exemple de configuration de listes de contrôle d'accès sur un contrôleur de réseau local sans fil
- Exemple de configuration de filtres MAC avec des contrôleurs de réseau local sans fil (WLC)
- Guide de configuration du contrôleur LAN sans fil Cisco, version 5.2
- Support et documentation techniques - Cisco Systems