Exemple de configuration de restriction de l'accès au réseau local sans fil sur SSID avec WLC et Cisco Secure ACS

Contenu

Introduction

Ce document fournit un exemple de configuration pour limiter l'accès de chaque utilisateur à un WLAN basé sur le Service Set Identifier (SSID).

Conditions préalables

Conditions requises

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

- Connaissance de la façon dont configurer le contrôleur LAN sans fil (WLC) et le point d'accès léger (LAP) pour le fonctionnement de base
- Connaissances de base sur la configuration de Cisco Secure Access Control Server (ACS)
- Connaissance du protocole LWAPP (Lightweight Access Point Protocol) et des méthodes de sécurité sans fil

Components Used

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

- Contrôleur de réseau sans fil de la gamme Cisco 2000 qui exécute le micrologiciel 4.0
- LAP de la gamme Cisco 1000
- Serveur Cisco Secure ACS version 3.2
- Carte client sans fil Cisco 802.11a/b/g qui exécute le micrologiciel 2.6
- Utilitaire de bureau Cisco Aironet (ADU) version 2.6

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

Avec l'utilisation d'un accès WLAN basé sur SSID, les utilisateurs peuvent être authentifiés en fonction du SSID qu'ils utilisent afin de se connecter au WLAN. Le serveur Cisco Secure ACS sert à authentifier les utilisateurs. L'authentification se déroule en deux étapes sur Cisco Secure ACS :

1. Authentification EAP
2. Authentification SSID basée sur les restrictions d'accès au réseau (NAR) sur Cisco Secure ACS

Si l'authentification EAP et SSID réussit, l'utilisateur est autorisé à accéder au WLAN ou l'utilisateur est disassocié.

Cisco Secure ACS utilise la fonction NAR pour restreindre l'accès utilisateur en fonction du SSID. Une NAR est une définition, que vous définissez dans Cisco Secure ACS, des conditions supplémentaires qui doivent être remplies avant qu'un utilisateur puisse accéder au réseau. Cisco Secure ACS applique ces conditions à l'aide d'informations provenant d'attributs envoyés par vos clients AAA. Bien qu'il existe plusieurs façons de configurer les NAR, elles sont toutes basées sur les informations d'attribut correspondantes envoyées par le client AAA. Par conséquent, vous devez comprendre le format et le contenu des attributs que vos clients AAA envoient si vous voulez utiliser des NAR efficaces.

Lorsque vous configurez un NAR, vous pouvez choisir si le filtre fonctionne de manière positive ou négative. En d'autres termes, dans la NAR, vous indiquez s'il faut autoriser ou refuser l'accès au réseau, en fonction d'une comparaison des informations envoyées par les clients AAA aux informations stockées dans la NAR. Cependant, si une NAR ne rencontre pas suffisamment d’informations pour fonctionner, elle refuse par défaut l’accès.

Vous pouvez définir une NAR pour un utilisateur ou un groupe d'utilisateurs spécifique et l'appliquer à un utilisateur ou à un groupe d'utilisateurs spécifique. Reportez-vous au Livre blanc sur les restrictions d'accès au réseau pour plus d'informations.

Cisco Secure ACS prend en charge deux types de filtres NAR :

1. **Filtres IP** - Les filtres NAR IP limitent l'accès en fonction des adresses IP du client utilisateur final et du client AAA. Référez-vous à À propos des filtres NAR basés sur IP pour plus d'informations sur ce type de filtre NAR.
2. **Filtres non basés sur IP** - Les filtres NAR non basés sur IP limitent l'accès en fonction d'une simple comparaison de chaînes d'une valeur envoyée par le client AAA. La valeur peut être le numéro d'ID de ligne appelante (CLI), le numéro DNIS (Dialed Number Identification Service), l'adresse MAC ou toute autre valeur provenant du client. Pour que ce type de NAR fonctionne, la valeur de la description NAR doit correspondre exactement à ce qui est envoyé du client, y compris le format utilisé. Par exemple, (217) 555-4534 ne correspond pas à 217-555-4534. Référez-vous à À propos des filtres NAR non basés sur IP pour plus d'informations sur ce type de filtre NAR.

Ce document utilise des filtres non basés sur IP pour effectuer l'authentification basée sur SSID. Un filtre NAR non basé sur IP (c'est-à-dire un filtre NAR basé sur DNIS/CLI) est une liste des emplacements d'appel/point d'accès autorisés ou refusés que vous pouvez utiliser dans la restriction d'un client AAA lorsque vous n'avez pas de connexion IP établie. La fonction NAR non basée sur IP utilise généralement le numéro CLI et le numéro DNIS. Il existe des exceptions dans l'utilisation des champs DNIS/CLI. Vous pouvez entrer le nom SSID dans le champ DNIS et effectuer une authentification basée sur SSID. En effet, le WLC envoie l'attribut DNIS, le nom SSID, au serveur RADIUS. Ainsi, si vous créez DNIS NAR dans l'utilisateur ou le groupe, vous pouvez créer des restrictions SSID par utilisateur.

Si vous utilisez RADIUS, les champs NAR répertoriés ici utilisent les valeurs suivantes :

- **Client AAA** - L'adresse IP NAS (attribut 4) ou, si l'adresse IP NAS n'existe pas, l'identificateur NAS (attribut RADIUS 32) est utilisé.
- **Port** : le port NAS (attribut 5) ou, si le port NAS n'existe pas, l'ID de port NAS (attribut 87) est utilisé.
- **CLI** - L'ID de la station appelante (attribut 31) est utilisé.
- **DNIS** : l'ID de station appelée (attribut 30) est utilisé.

Référez-vous à Restrictions d'accès au réseau pour plus d'informations sur l'utilisation de NAR.

Puisque le WLC envoie dans l'attribut DNIS et le nom SSID, vous pouvez créer des restrictions SSID par utilisateur. Dans le cas du WLC, les champs NAR ont les valeurs suivantes :

- **Client AAA** - Adresse IP du WLC
- **port** —*
- **CLI** —*
- **DNIS** —*ssidname

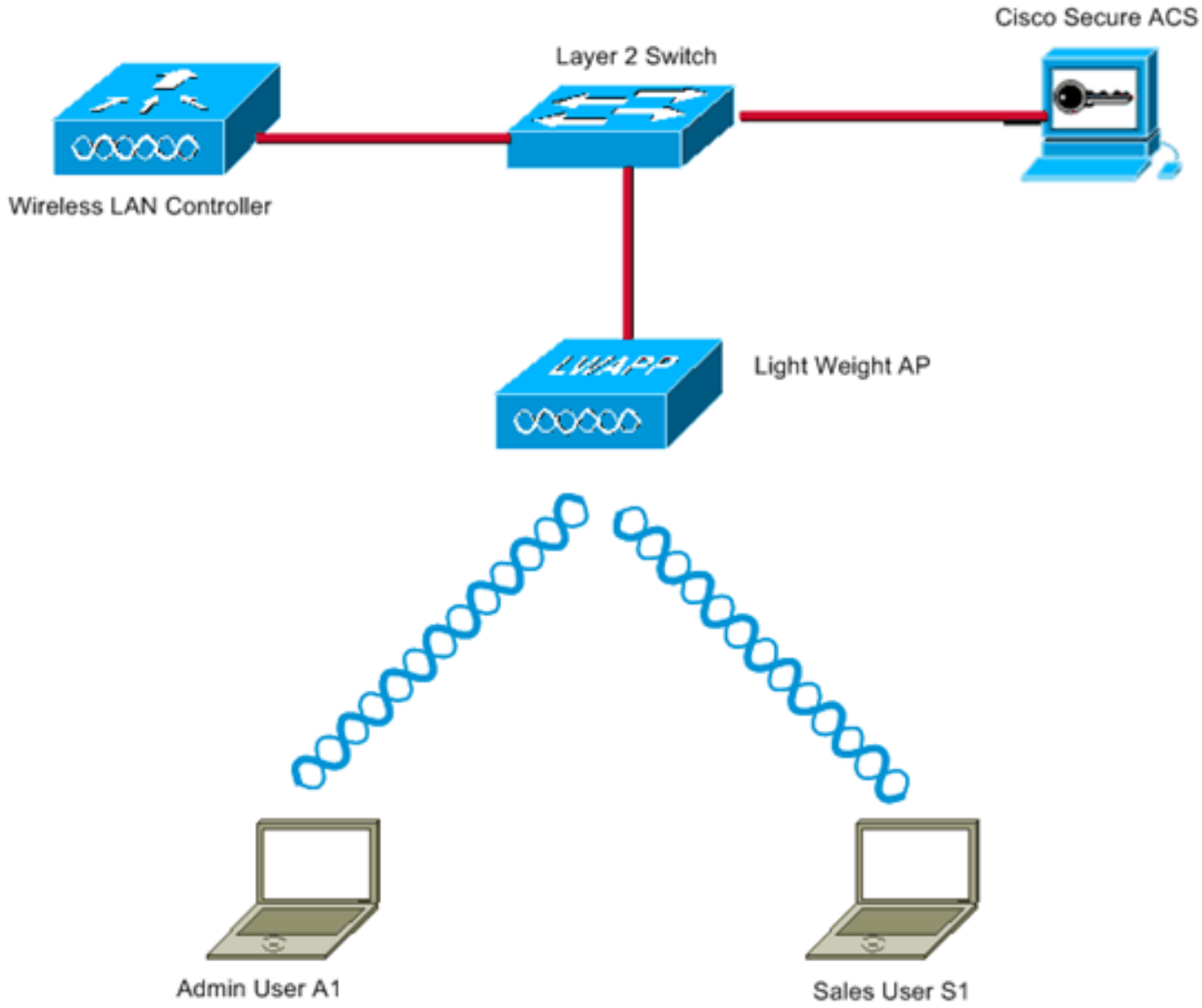
Le reste de ce document fournit un exemple de configuration sur la façon d'accomplir ceci.

Configuration du réseau

Dans cet exemple de configuration, le WLC est inscrit au LAP. Deux WLAN sont utilisés. Un WLAN est destiné aux utilisateurs du service d'administration et l'autre aux utilisateurs du service des ventes. Les clients sans fil A1 (utilisateur Admin) et S1 (utilisateur Sales) se connectent au réseau sans fil. Vous devez configurer le WLC et le serveur RADIUS de manière à ce que l'utilisateur Admin A1 puisse accéder uniquement à l'**administrateur** WLAN et qu'il ait un accès limité aux **ventes** WLAN et que l'utilisateur Sales S1 puisse accéder aux **ventes** WLAN et ait un accès limité à l'**administrateur** WLAN. Tous les utilisateurs utilisent l'authentification LEAP comme

méthode d'authentification de couche 2.

Note : Ce document suppose que le WLC est enregistré au contrôleur. Si vous n'êtes pas familier avec le WLC et que vous ne savez pas comment configurer le WLC pour le fonctionnement de base, référez-vous à Enregistrement du point d'accès léger (LAP) à un contrôleur de réseau local sans fil (WLC).



WLC Management Interface IP address : 172.16.1.30/16
WLC AP-Manager Interface IP address: 172.16.1.31/16
Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin
SSID for Sales department users: Sales

Configuration

Pour configurer les périphériques de cette configuration, vous devez :

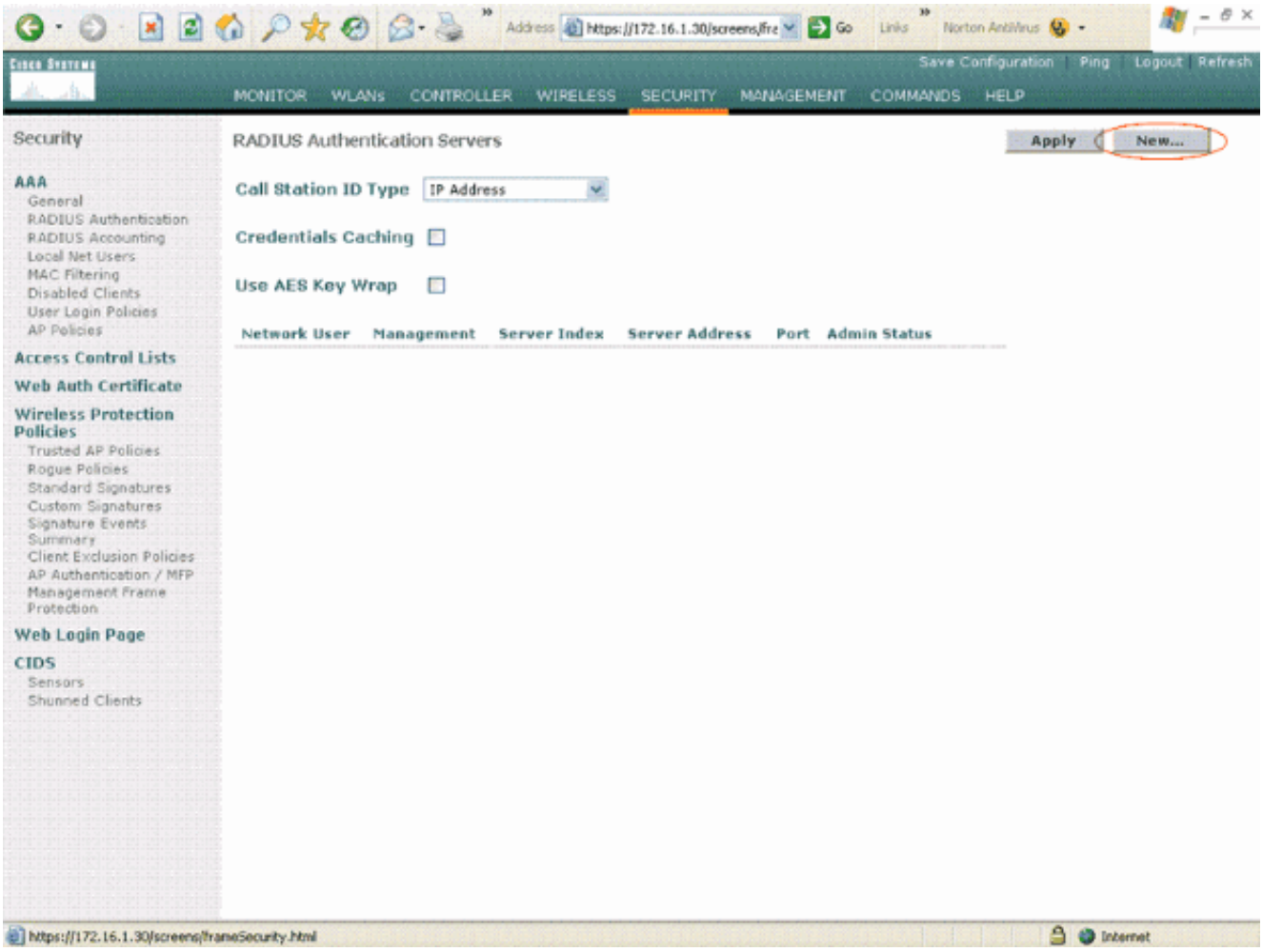
1. Configurez le WLC pour les deux WLAN et le serveur RADIUS.

2. Configurez Cisco Secure ACS.
3. Configurez les clients sans fil et vérifiez.

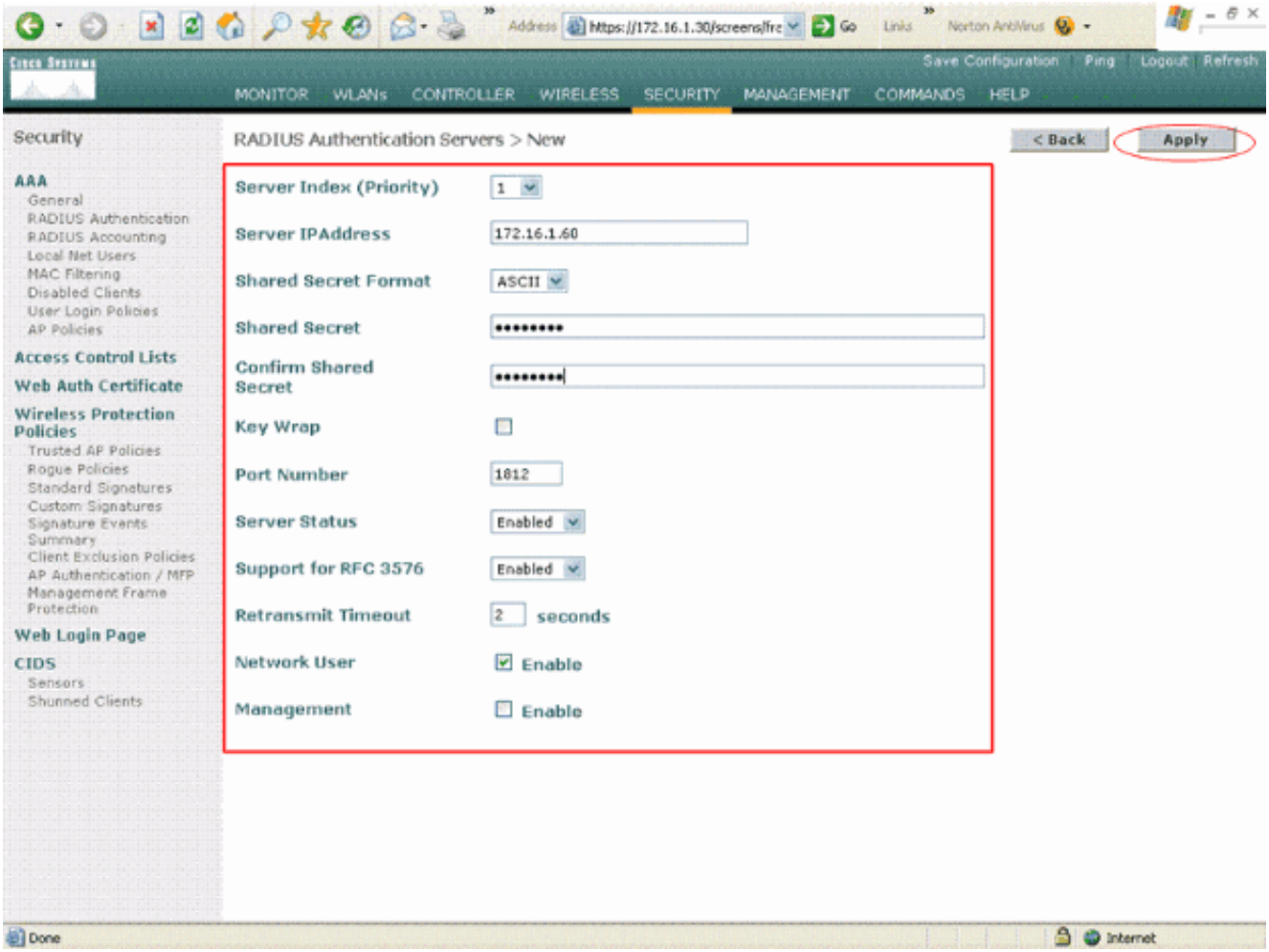
Configurer le WLC

Complétez ces étapes afin de définir le WLC pour cette configuration :

1. Le WLC doit être configuré pour transférer les informations d'identification de l'utilisateur à un serveur RADIUS externe. Le serveur RADIUS externe (Cisco Secure ACS dans ce cas) valide ensuite les informations d'identification de l'utilisateur et fournit l'accès aux clients sans fil. Procédez comme suit :Choisissez **Security > RADIUS Authentication** dans l'interface graphique du contrôleur afin d'afficher la page RADIUS Authentication Servers.

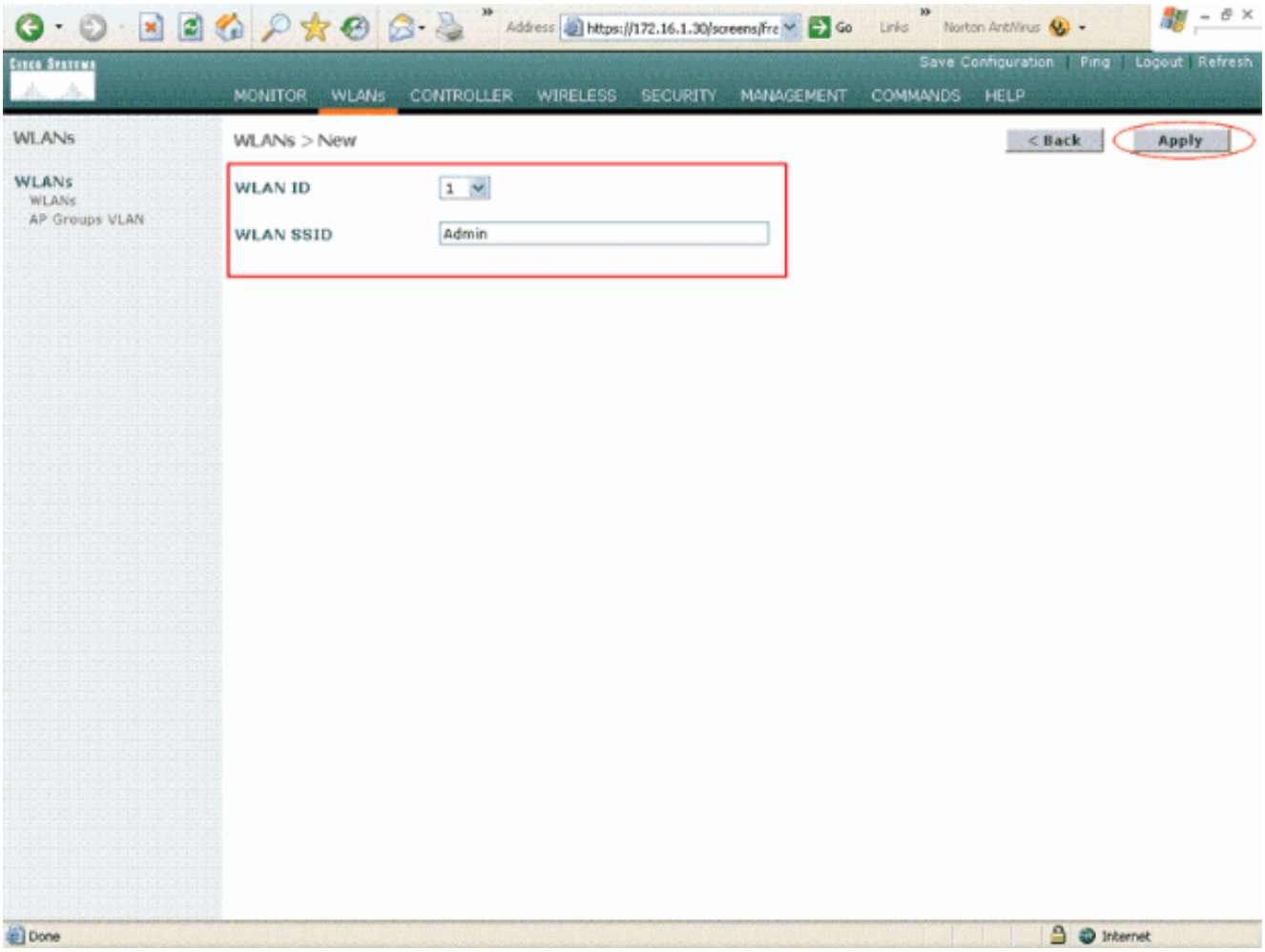


Cliquez sur **Nouveau** afin de définir les paramètres du serveur RADIUS.Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du serveur. Les cases à cocher d'utilisateur du réseau et de gestion déterminent si l'authentification basée sur RADIUS s'applique pour la gestion et les utilisateurs du réseau. Cet exemple utilise Cisco Secure ACS comme serveur RADIUS avec l'adresse IP 172.16.1.60.

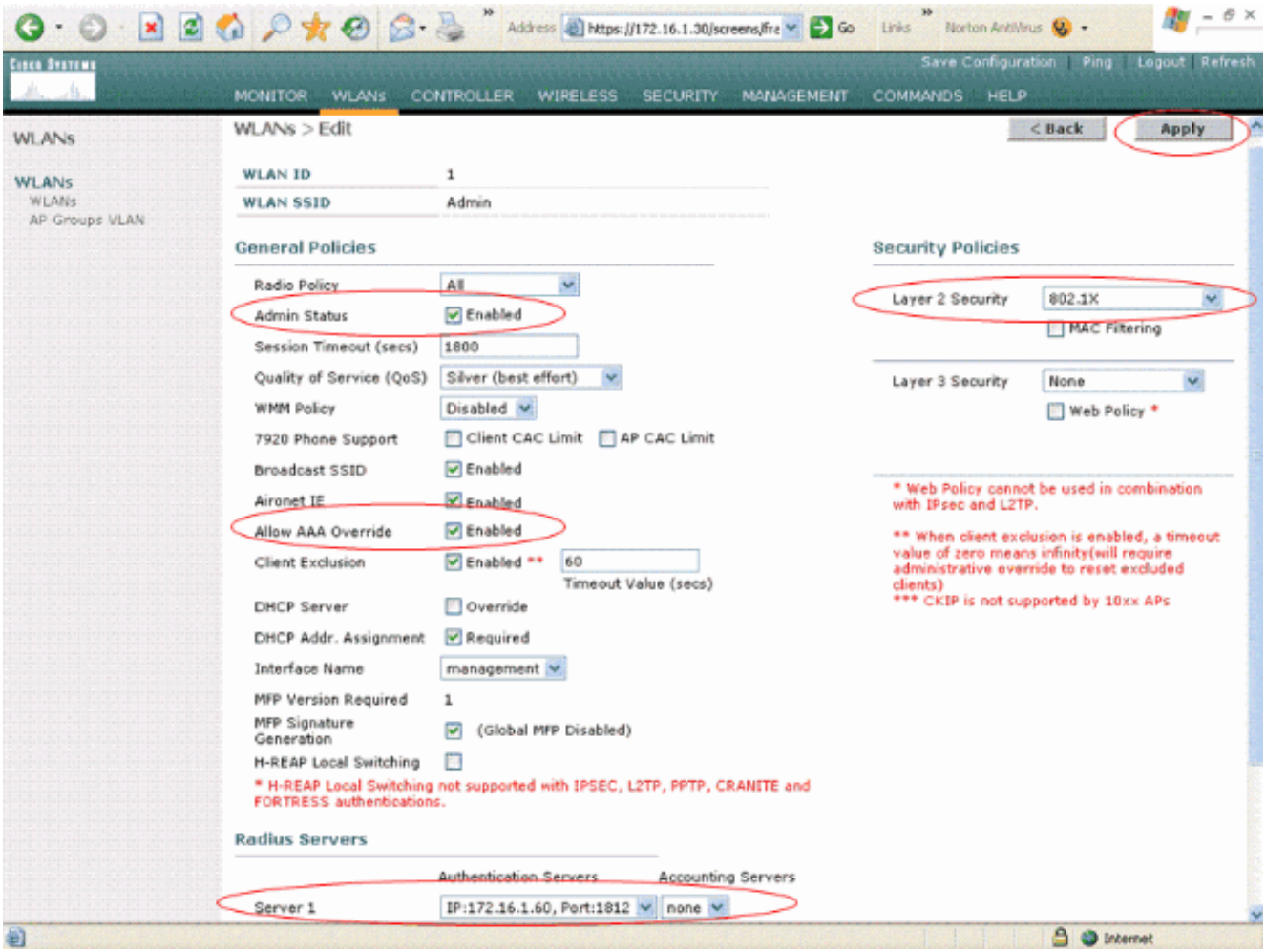


Cliquez sur Apply.

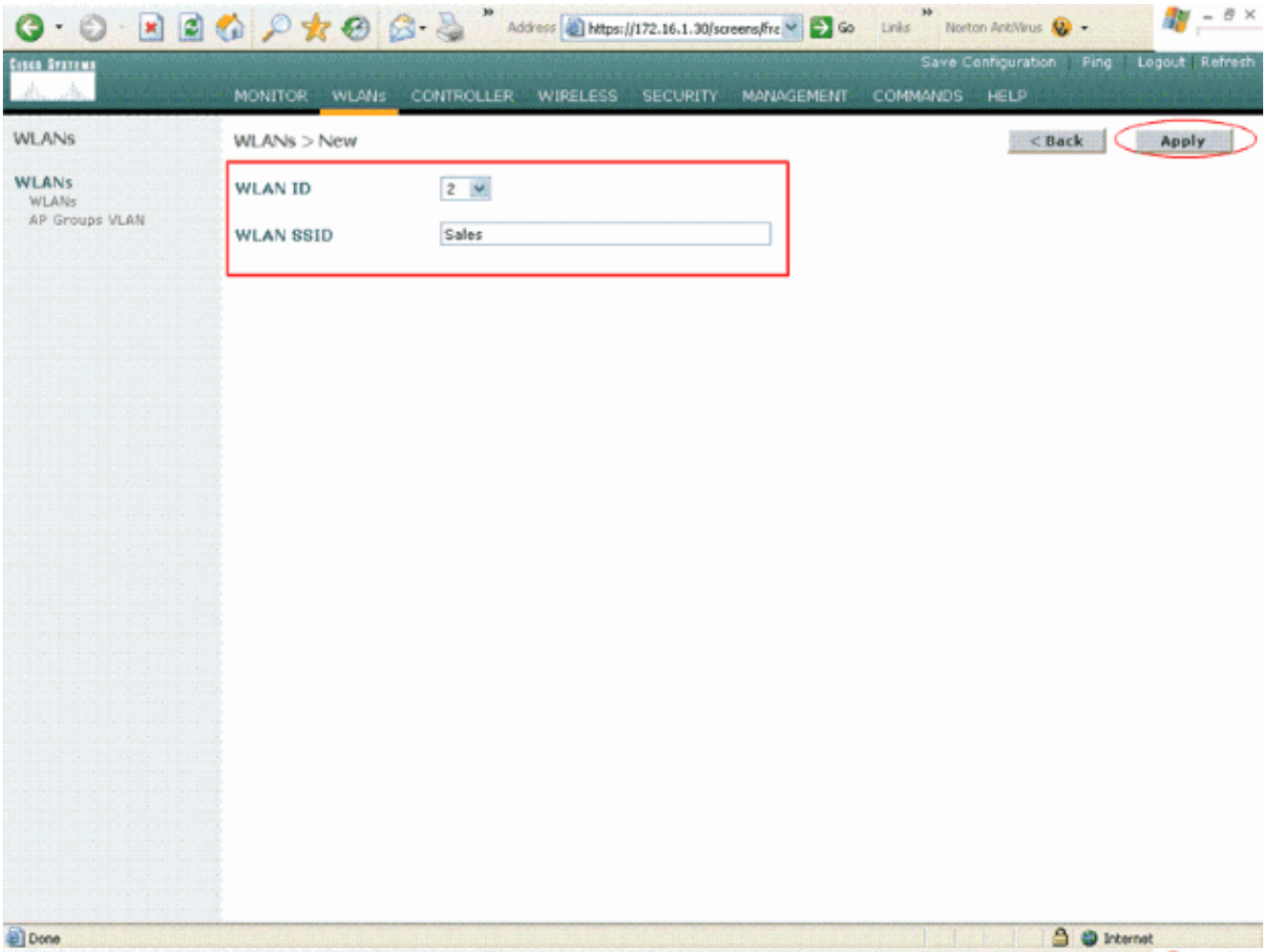
2. Configurez un WLAN pour le service Admin avec SSID **Admin** et l'autre WLAN pour le service Sales avec SSID **Sales**. Pour ce faire, exécutez ces étapes:Cliquez sur **WLANs depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.** La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.Cliquez sur **New pour configurer un nouveau WLAN.**Cet exemple crée un WLAN nommé **Admin** pour le service Admin et l'ID WLAN est **1**. Cliquez sur
Apply.

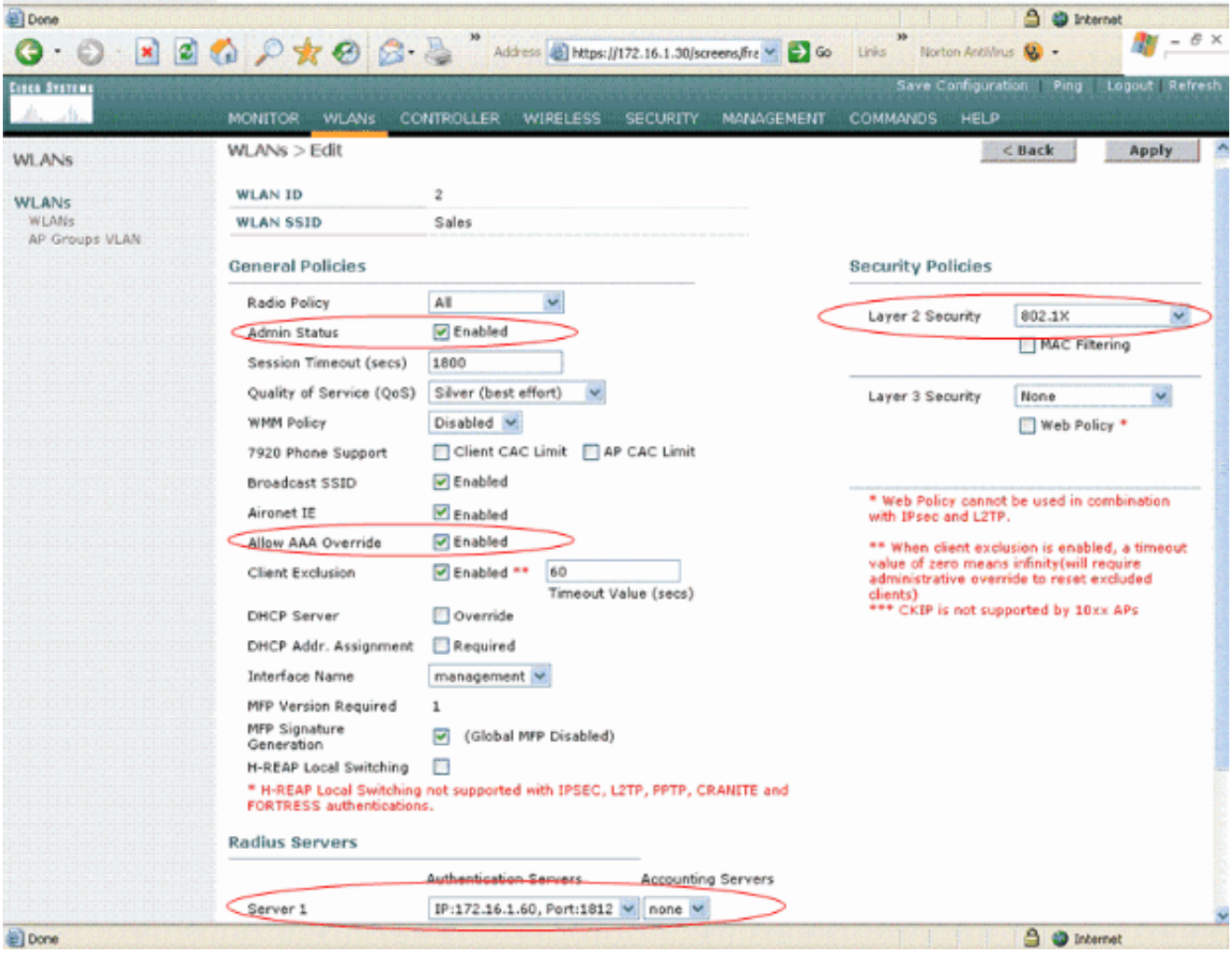


Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN:Dans le menu déroulant Sécurité de couche 2, sélectionnez **802.1x**. Par défaut, l'option de sécurité de couche 2 est 802.1x. Cela active l'authentification 802.1x/EAP pour le WLAN.Sous Stratégies générales, cochez la case **Remplacement AAA**. Lorsque le remplacement AAA est activé et qu'un client a des paramètres d'authentification AAA et WLAN du contrôleur en conflit, l'authentification du client est effectuée par le serveur AAA.Sélectionnez le serveur RADIUS approprié dans le menu déroulant sous Serveurs RADIUS. Les autres paramètres peuvent être modifiés sur les conditions requises du réseau WLAN. Cliquez sur Apply.



De même, afin de créer un WLAN pour le service Ventes, répétez les étapes b et c. Voici les captures
d'écran.


Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > New
< Back
Apply
WLAN ID
2
WLAN SSID
Sales


Done
Internet
Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > Edit
< Back
Apply
WLAN ID 2
WLAN SSID Sales
General Policies
Radio Policy All
Admin Status Enabled
Session Timeout (secs) 1800
Quality of Service (QoS) Silver (best effort)
WMM Policy Disabled
7920 Phone Support Client CAC Limit AP CAC Limit
Broadcast SSID Enabled
Aironet IE Enabled
Allow AAA Override Enabled
Client Exclusion Enabled ** 60
Timeout Value (secs)
DHCP Server Override
DHCP Addr. Assignment Required
Interface Name management
MFP Version Required 1
MFP Signature Generation (Global MFP Disabled)
H-REAP Local Switching
* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.
Security Policies
Layer 2 Security 802.1X
MAC Filtering
Layer 3 Security None
Web Policy *
* Web Policy cannot be used in combination with IPsec and L2TP.
** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)
*** CKIP is not supported by 10xx APs
Radius Servers
Authentication Servers
Accounting Servers
Server 1 IP:172.16.1.60, Port:1812 none
Done
Internet

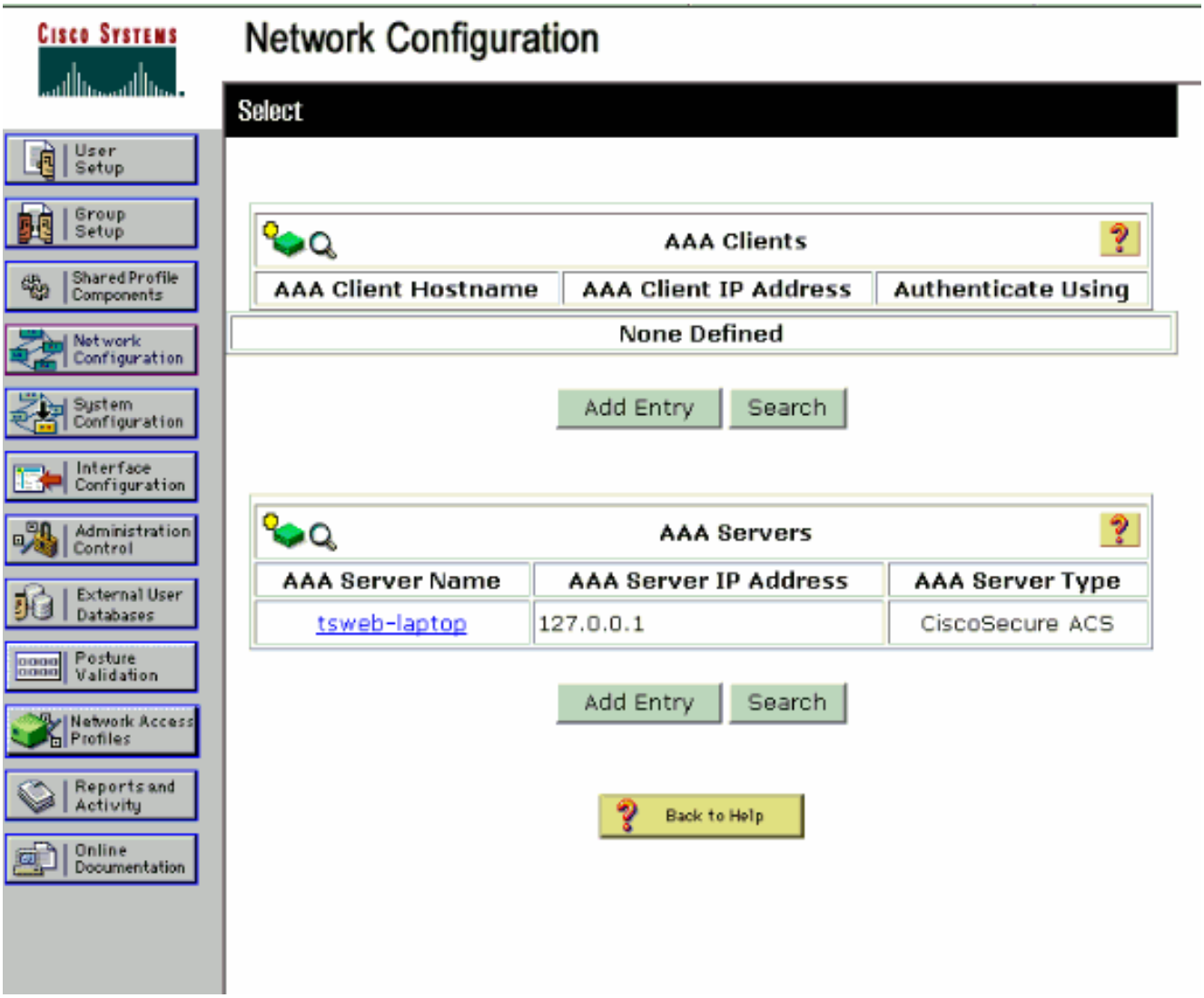
Configurer Cisco Secure ACS

Sur le serveur Cisco Secure ACS, vous devez :

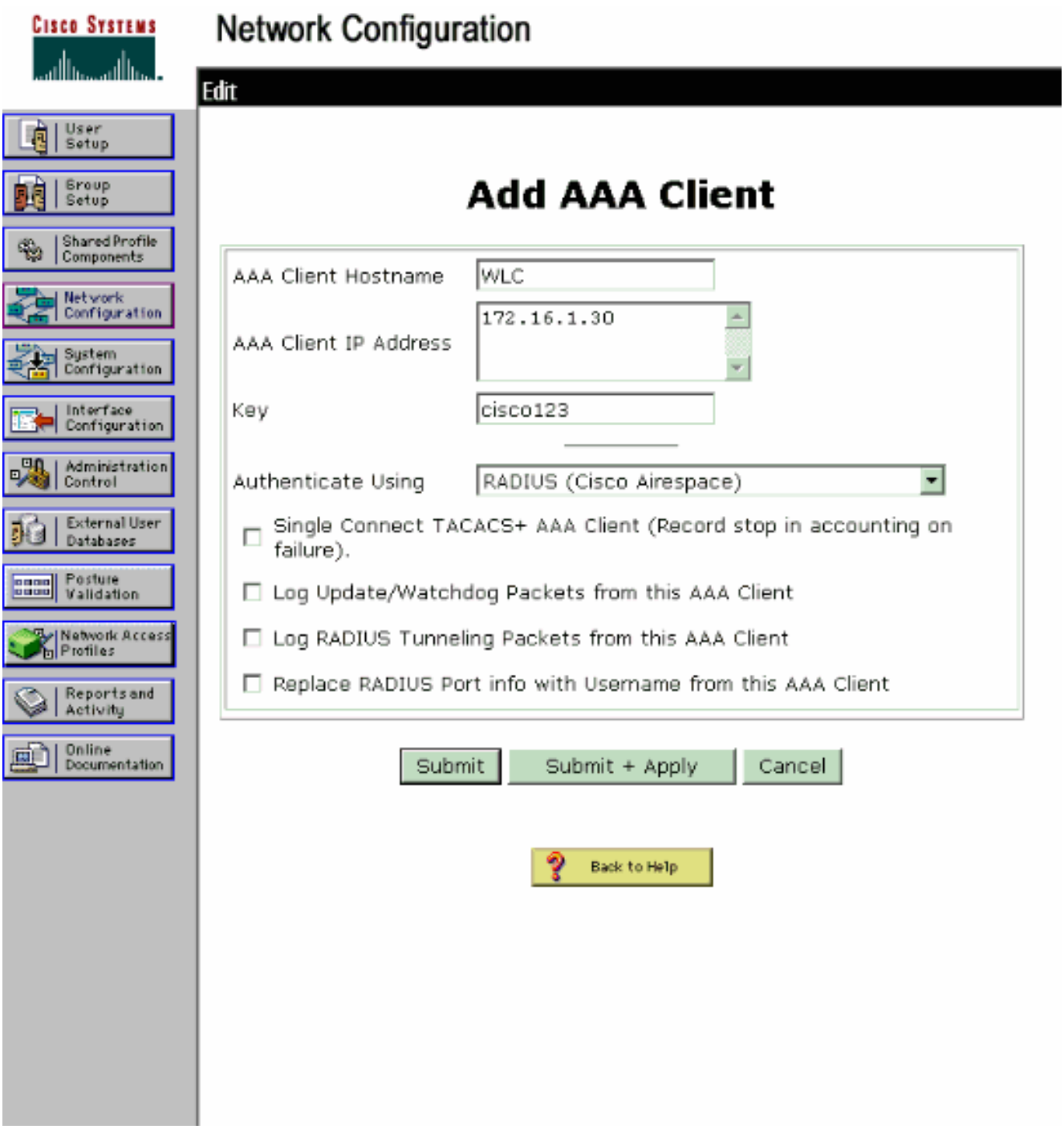
1. Configurez le WLC en tant que client AAA.
2. Créez la base de données User et définissez NAR pour l'authentification basée sur SSID.
3. Activez l'authentification EAP.

Suivez ces étapes sur Cisco Secure ACS :

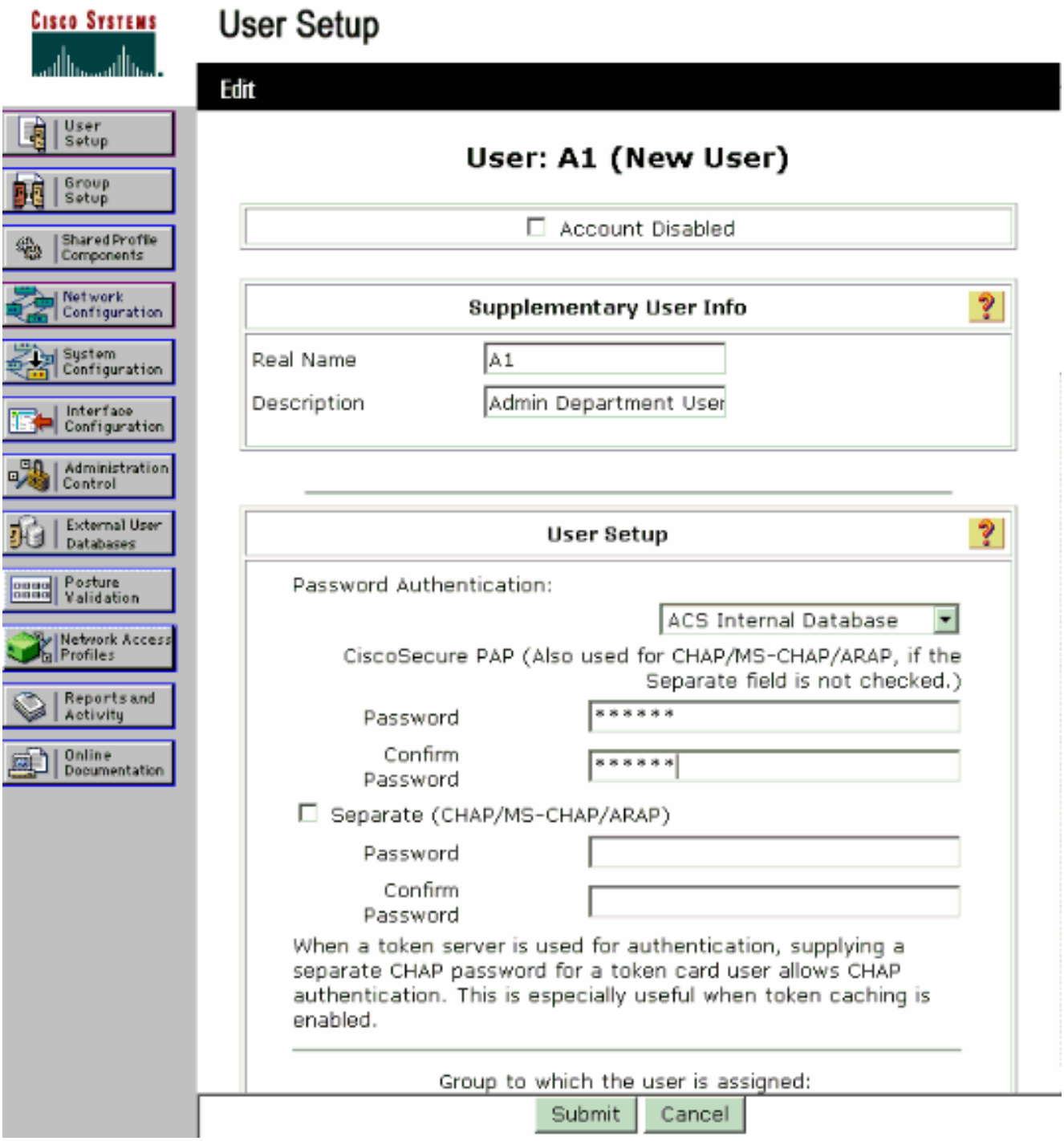
1. Afin de définir le contrôleur en tant que client AAA sur le serveur ACS, cliquez sur **Configuration réseau** dans l'interface utilisateur graphique ACS. Sous clients AAA, cliquez sur **Ajouter une entrée**.



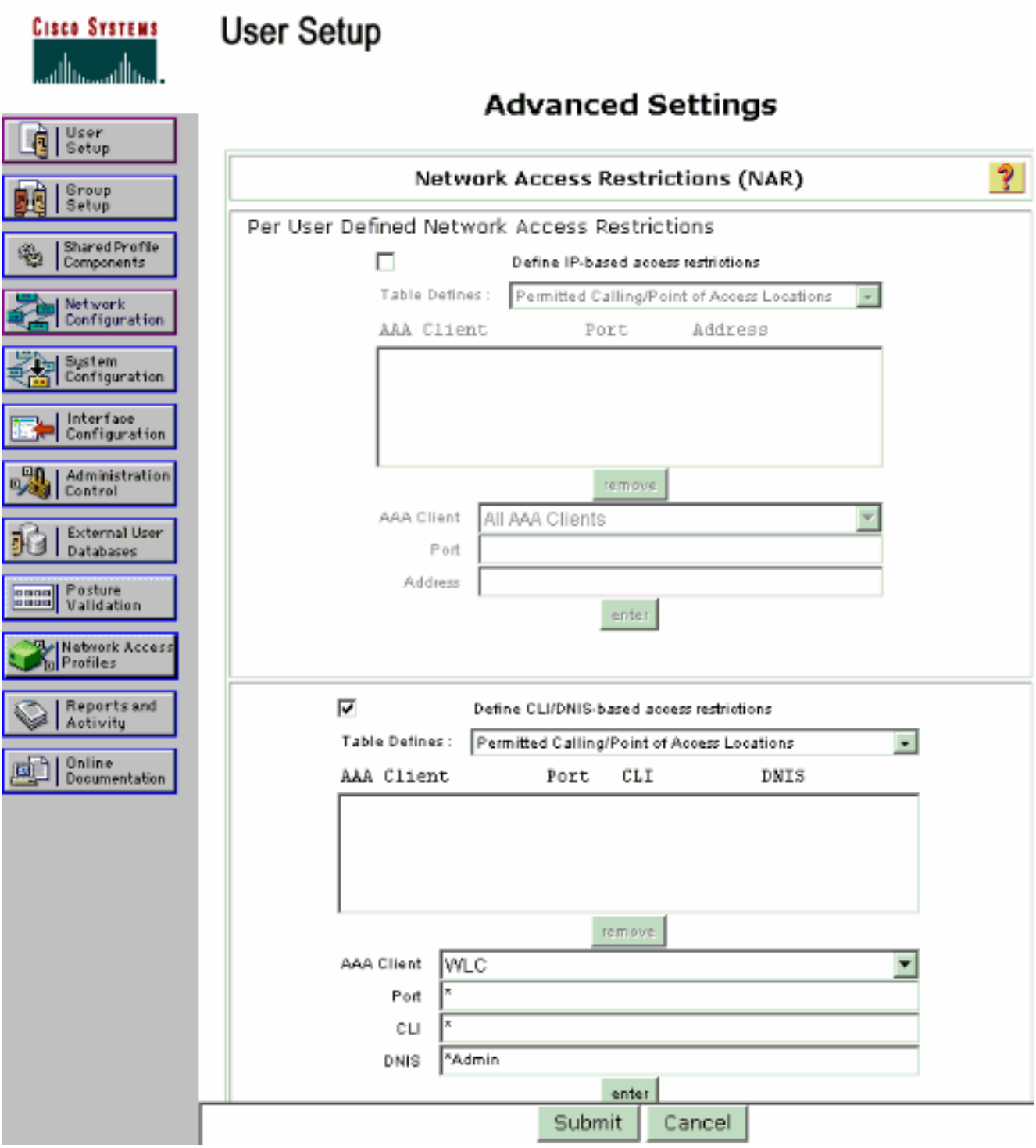
2. Lorsque la page de configuration réseau apparaît, définissez le nom du WLC, l'adresse IP, le secret partagé et la méthode d'authentification (RADIUS Cisco Airespace).



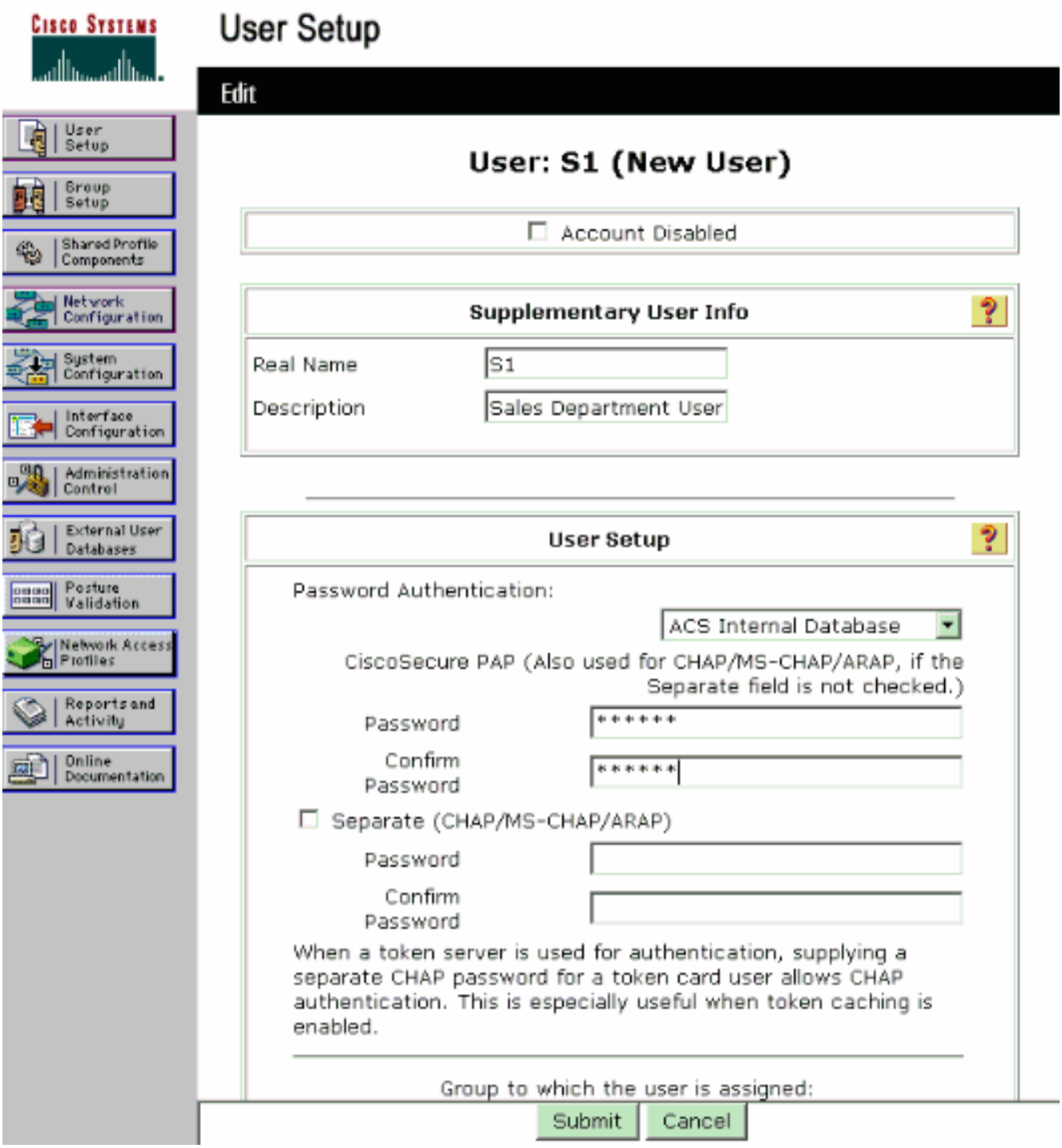
3. Cliquez sur **User Setup** dans l'interface utilisateur graphique ACS, saisissez le nom d'utilisateur et cliquez sur **Add/Edit**. Dans cet exemple, l'utilisateur est A1.
4. Lorsque la page d'installation utilisateur apparaît, définissez tous les paramètres spécifiques à l'utilisateur. Dans cet exemple, le nom d'utilisateur, le mot de passe et les informations utilisateur supplémentaires sont configurés car vous avez besoin de ces paramètres pour l'authentification
LEAP.

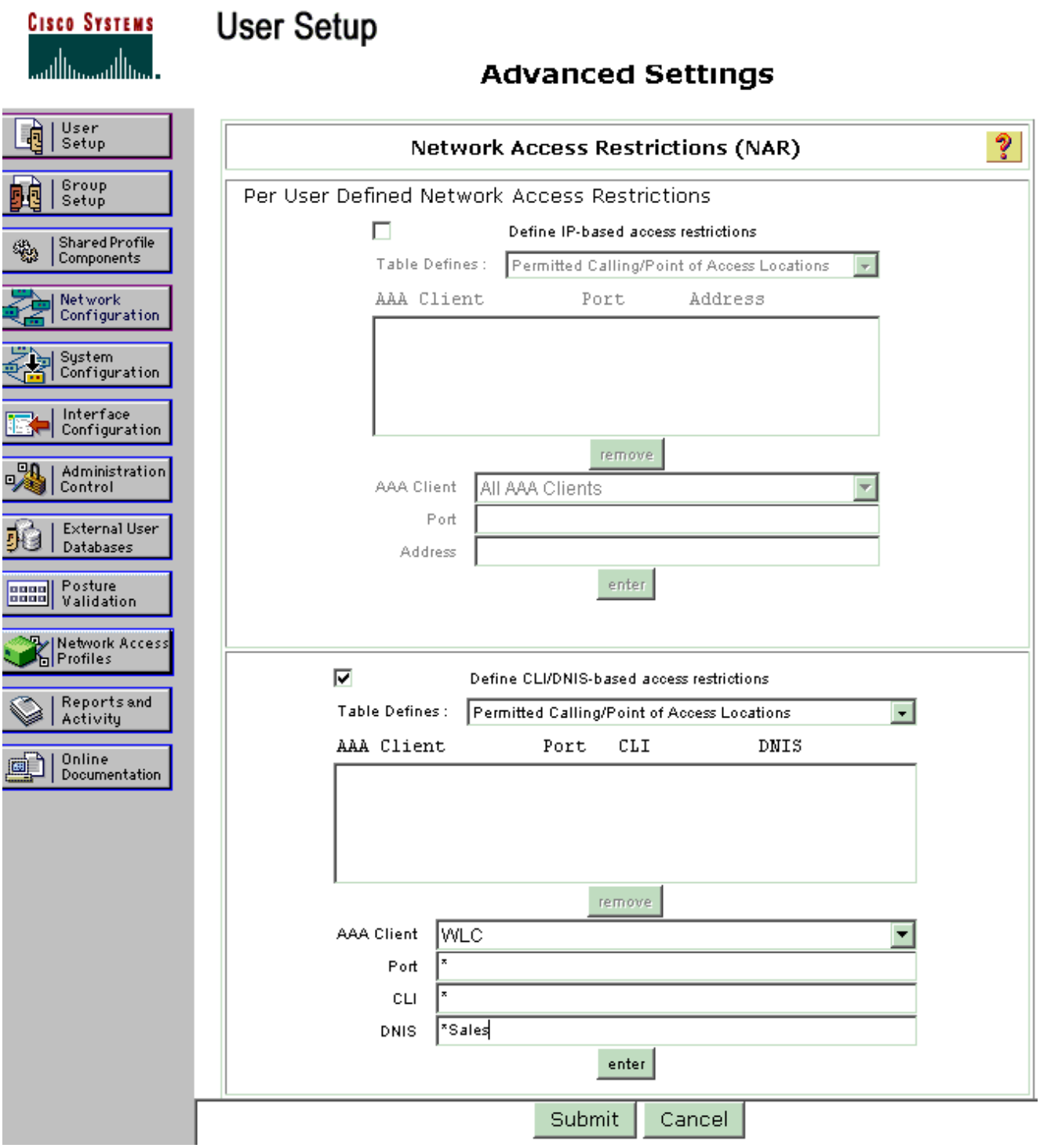


5. Faites défiler la page User Setup jusqu'à ce que la section Network Access Restrictions (Restrictions d'accès au réseau) s'affiche. Sous l'interface utilisateur de la restriction d'accès DNIS/CLI, sélectionnez **Appels autorisés/ Points d'accès** et définissez ces paramètres :**Client AAA** - Adresse IP du WLC (172.16.1.30 dans notre exemple)**Port** —***CLI** —***DNIS** —*ssidname
6. L'attribut DNIS définit le SSID auquel l'utilisateur est autorisé à accéder. Le WLC envoie le SSID dans l'attribut DNIS au serveur RADIUS.Si l'utilisateur doit accéder uniquement au WLAN nommé Admin, saisissez ***Admin** pour le champ DNIS. Cela garantit que l'utilisateur n'a accès qu'au WLAN nommé Admin. Cliquez sur **Entrée**.**Note :** Le SSID doit toujours être précédé de ***. Elle est
obligatoire.

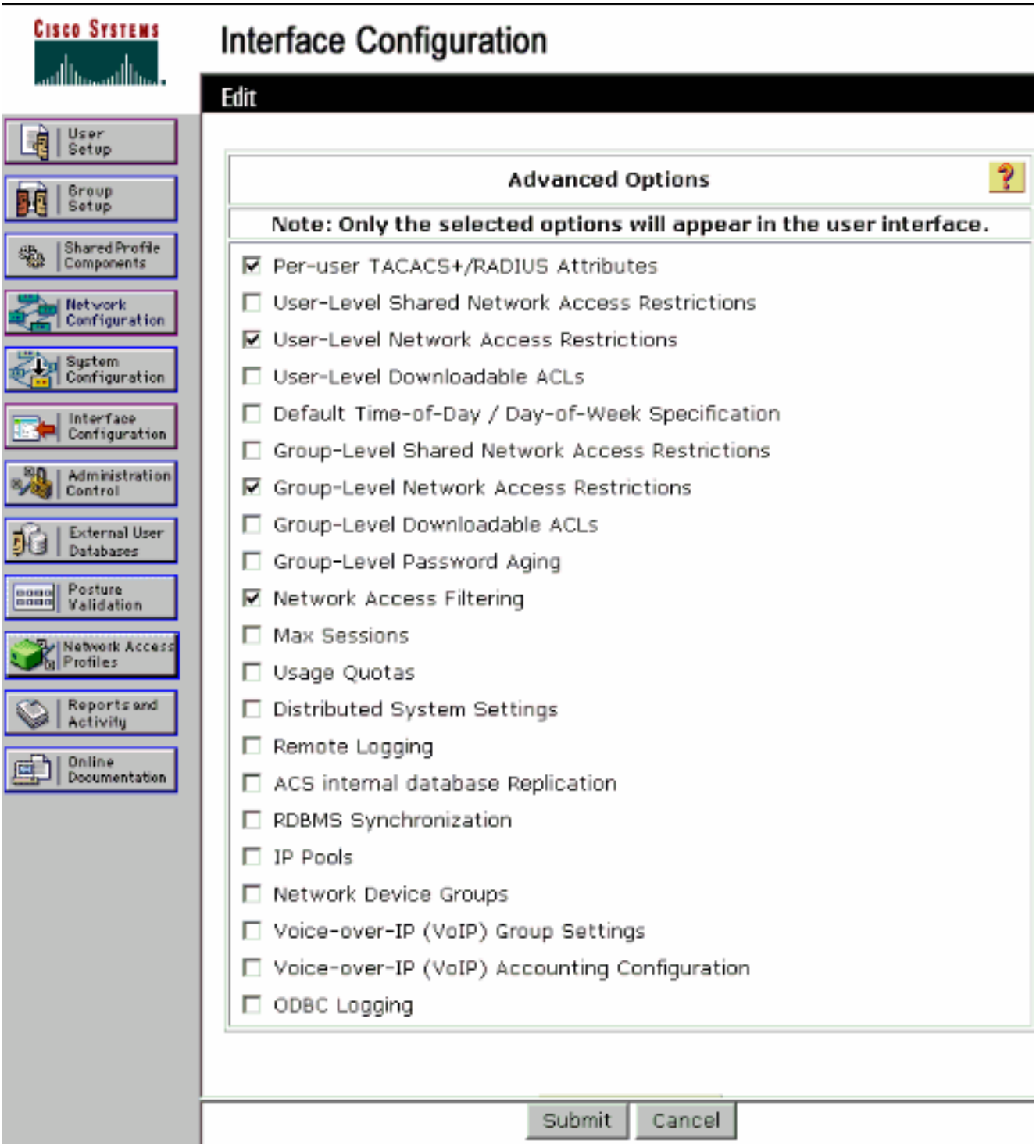


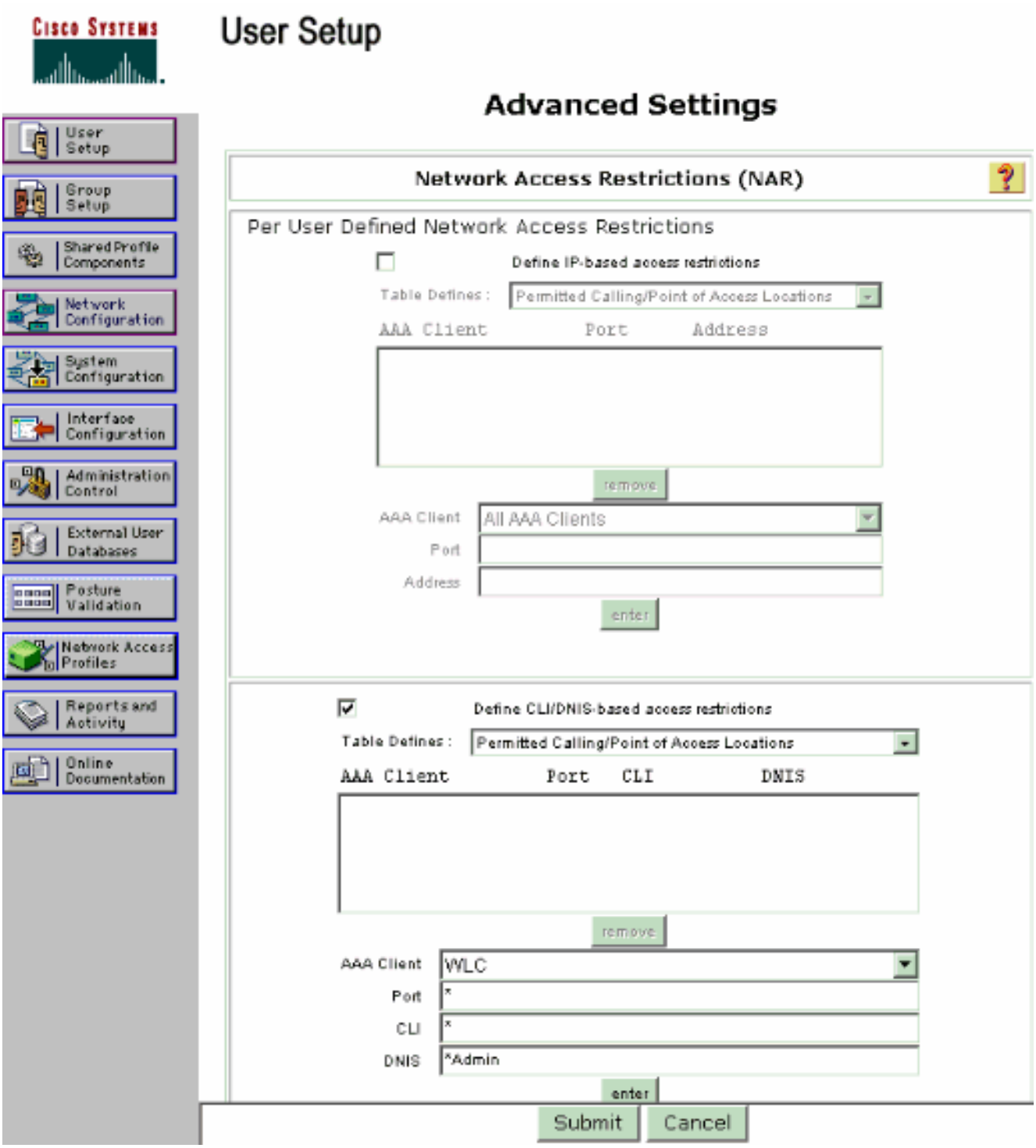
7. Cliquez sur Submit.
8. De même, créez un utilisateur pour l'utilisateur du service Ventes. Voici les captures d'écran.


Cisco Systems
User Setup
Edit
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
User: S1 (New User)
Account Disabled
Supplementary User Info
Real Name
S1
Description
Sales Department User
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

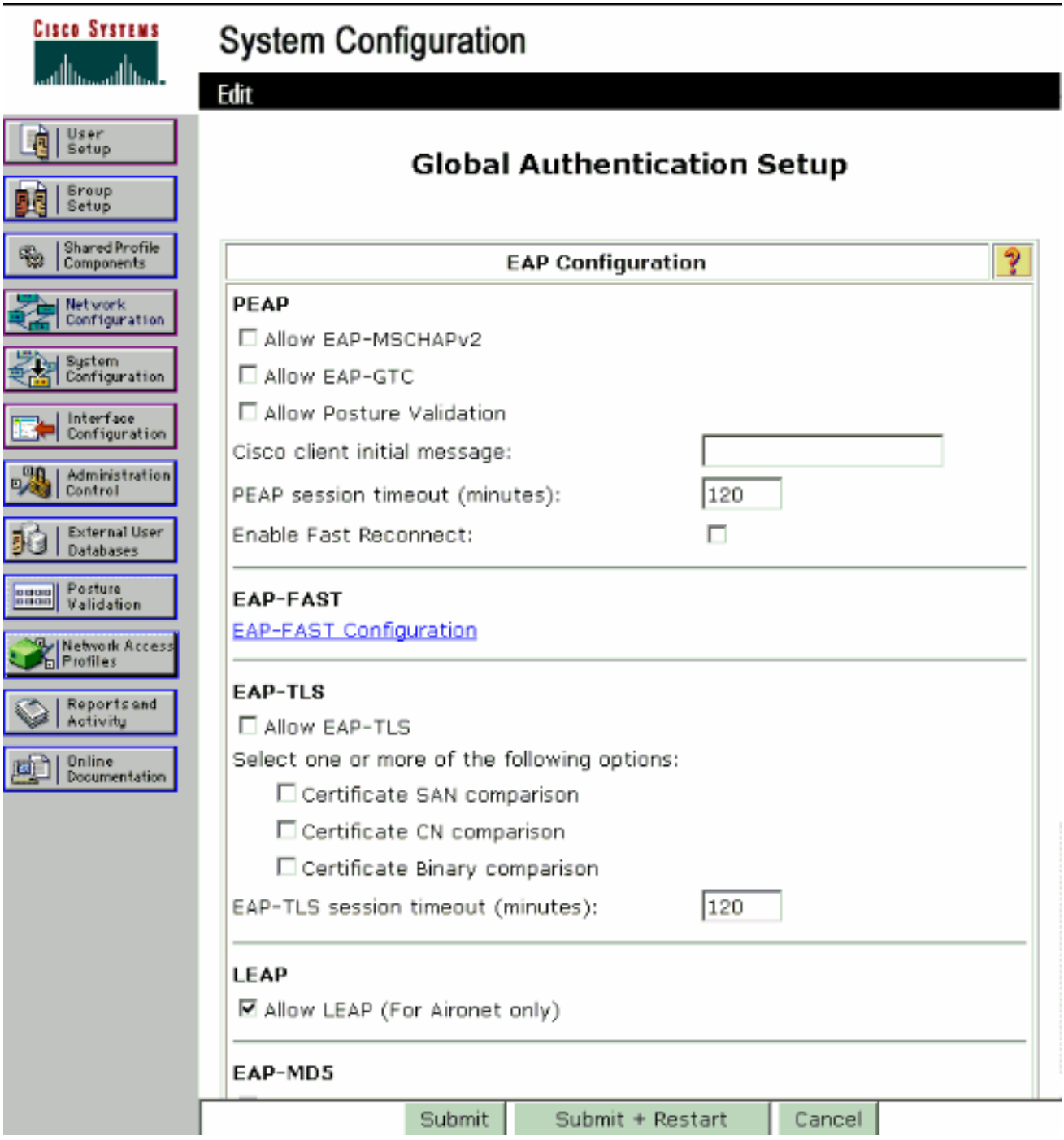


9. Répétez le même processus pour ajouter d'autres utilisateurs à la base de données.**Remarque :** par défaut, tous les utilisateurs sont regroupés sous le groupe par défaut. Si vous souhaitez affecter des utilisateurs spécifiques à différents groupes, reportez-vous à la section Gestion des groupes d'utilisateurs du Guide de l'utilisateur de Cisco Secure ACS pour Windows Server 3.2.**Remarque :** si la section Restrictions d'accès au réseau ne s'affiche pas dans la fenêtre User Setup (Configuration de l'utilisateur), cela peut être dû au fait qu'elle n'est pas activée. Afin d'activer les restrictions d'accès au réseau pour les utilisateurs, choisissez **Interfaces > Options avancées** dans l'interface utilisateur graphique ACS, sélectionnez **Restrictions d'accès au réseau au niveau de l'utilisateur** et cliquez sur **Soumettre**. Ceci active la NAR et apparaît dans la fenêtre User Setup.


Cisco Systems
Interface Configuration
Edit
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
Advanced Options
Note: Only the selected options will appear in the user interface.
Per-user TACACS+/RADIUS Attributes
User-Level Shared Network Access Restrictions
User-Level Network Access Restrictions
User-Level Downloadable ACLs
Default Time-of-Day / Day-of-Week Specification
Group-Level Shared Network Access Restrictions
Group-Level Network Access Restrictions
Group-Level Downloadable ACLs
Group-Level Password Aging
Network Access Filtering
Max Sessions
Usage Quotas
Distributed System Settings
Remote Logging
ACS internal database Replication
RDBMS Synchronization
IP Pools
Network Device Groups
Voice-over-IP (VoIP) Group Settings
Voice-over-IP (VoIP) Accounting Configuration
ODBC Logging
Submit
Cancel



10. Afin d'activer l'authentification EAP, cliquez sur **Configuration du système** et **Configuration de l'authentification globale** afin de vous assurer que le serveur d'authentification est configuré pour exécuter la méthode d'authentification EAP souhaitée.Sous les paramètres de configuration EAP, sélectionnez la méthode EAP appropriée. Cet exemple utilise l'authentification LEAP. Cliquez sur **Submit lorsque vous avez terminé.**

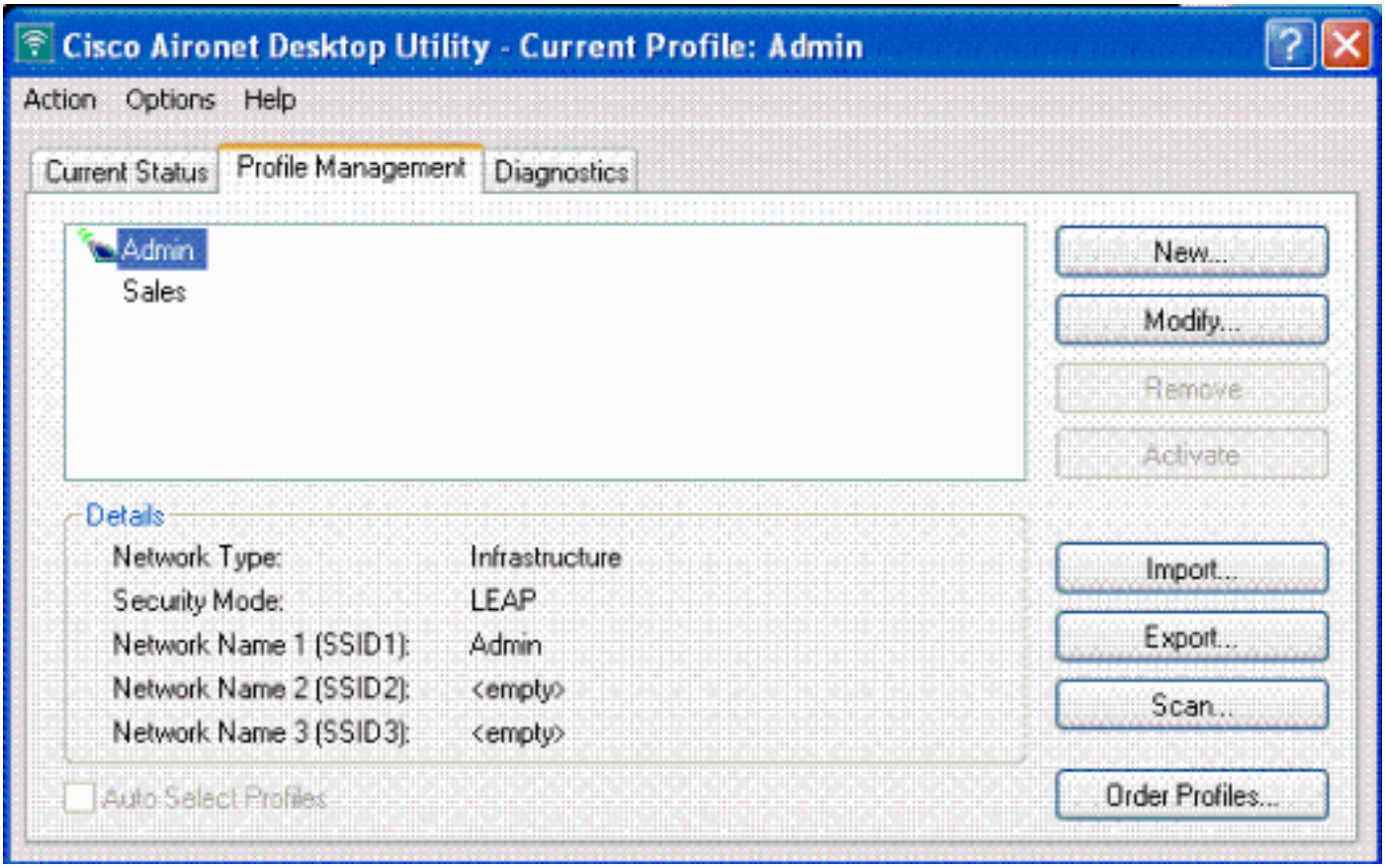


Configuration du client sans fil et vérification

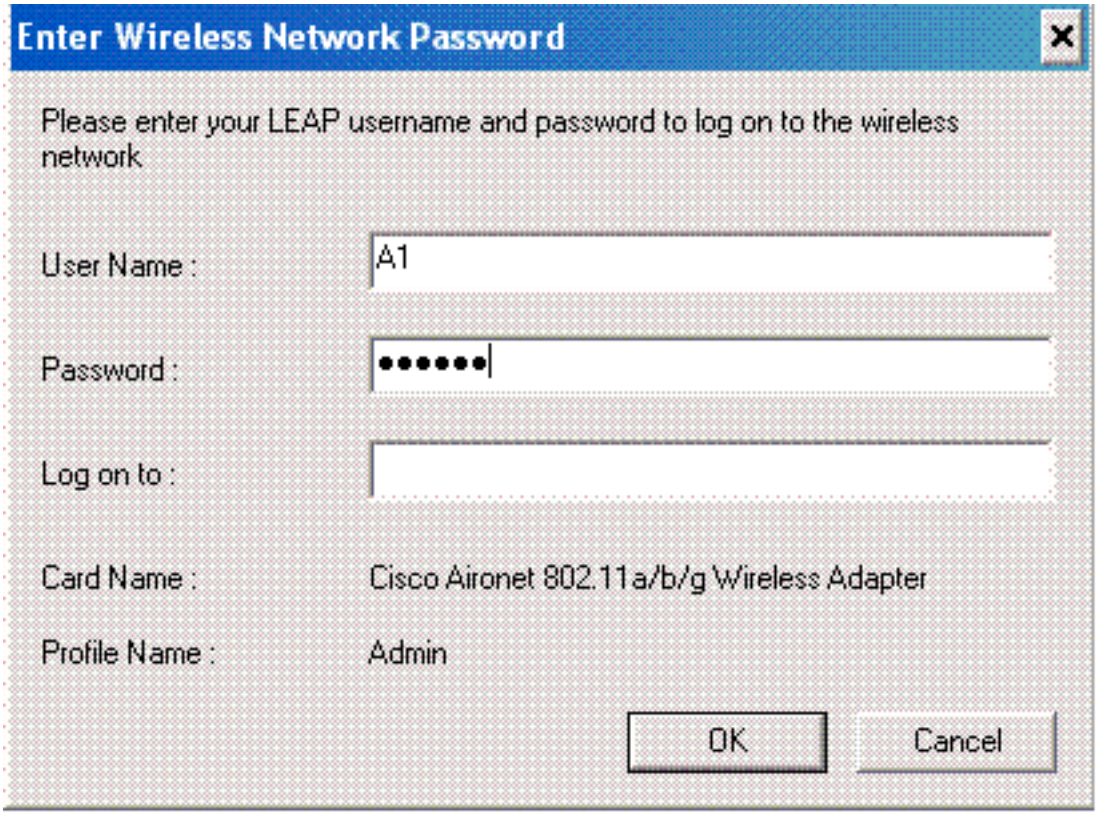
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Essayez d'associer un client sans fil au LAP à l'aide de l'authentification LEAP pour vérifier si la configuration fonctionne comme prévu.

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

Remarque : à partir de l'ADU, vous voyez que vous avez configuré deux profils client. L'un pour les utilisateurs du service Admin avec **Admin** SSID et l'autre pour les utilisateurs du service Sales avec SSID **Sales**. Les deux profils sont configurés pour l'authentification LEAP.



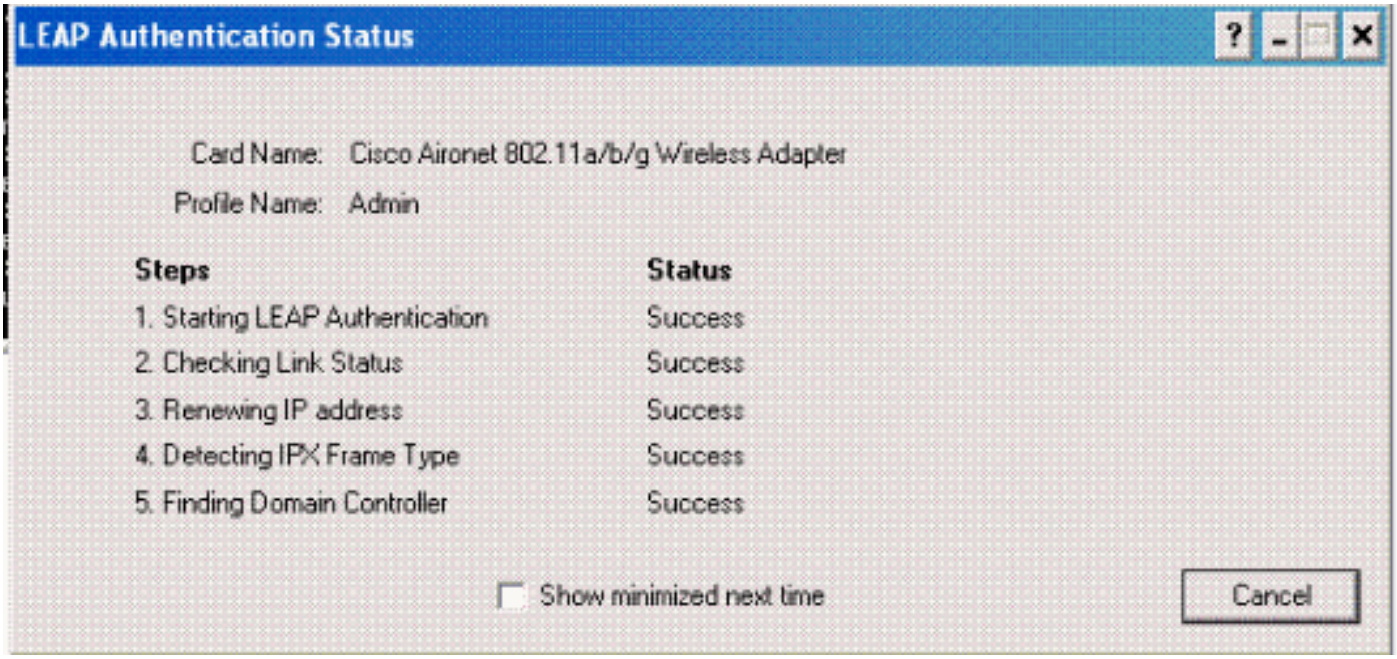
Lorsque le profil de l'utilisateur sans fil du service Admin est activé, l'utilisateur est invité à fournir le nom d'utilisateur/mot de passe pour l'authentification LEAP. Voici un exemple :



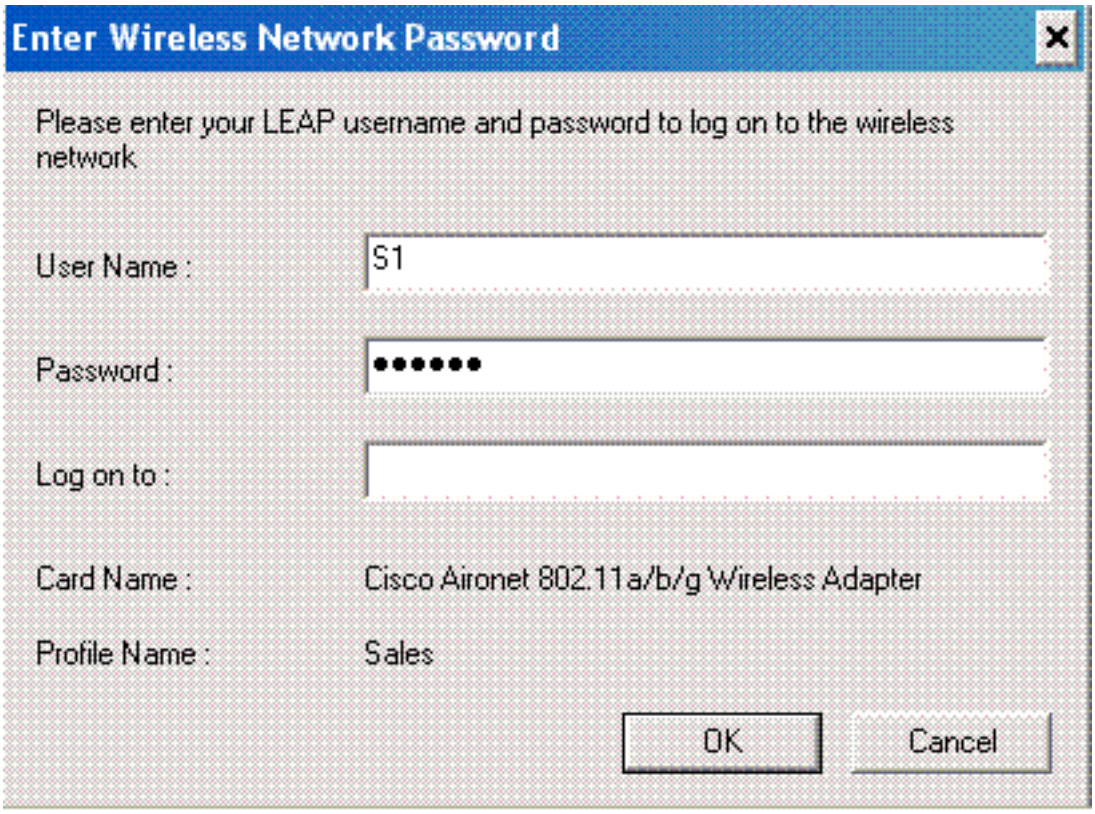
Le LAP, puis le WLC transmettent les informations d'identification de l'utilisateur au serveur RADIUS externe (Cisco Secure ACS) pour valider les informations d'identification. Le WLC transmet les informations d'identification, y compris l'attribut DNIS (nom SSID), au serveur RADIUS pour validation.

Le serveur RADIUS vérifie les informations d'identification de l'utilisateur en comparant les données à la base de données de l'utilisateur (et aux NAR) et fournit un accès au client sans fil chaque fois que les informations d'identification de l'utilisateur sont valides.

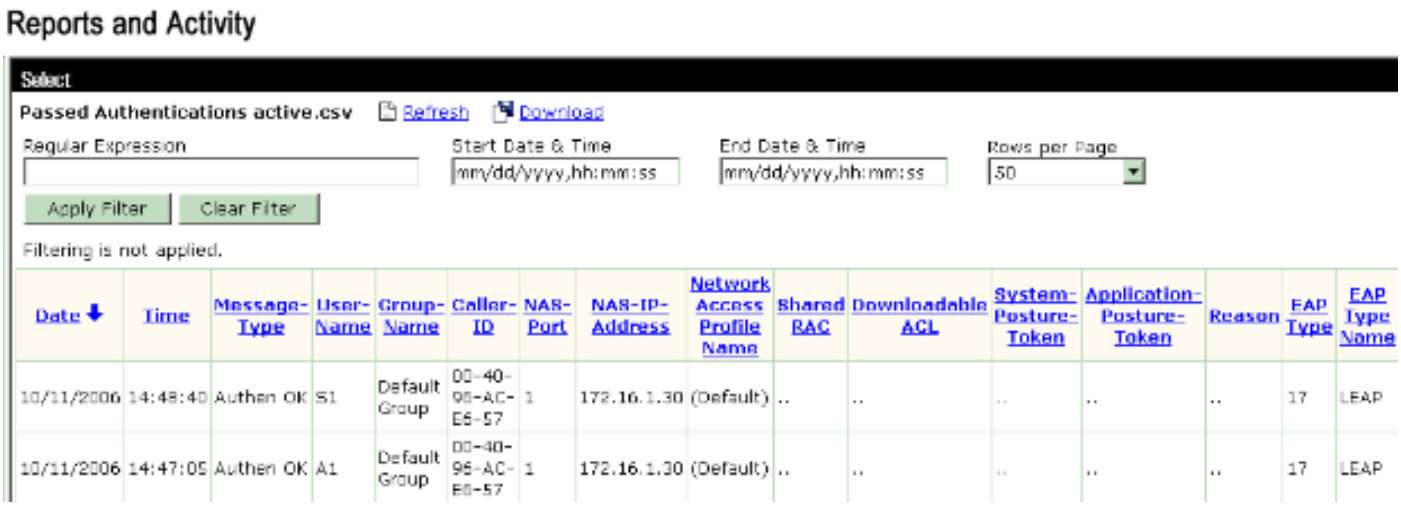
Une fois l'authentification RADIUS réussie, le client sans fil est associé au LAP.



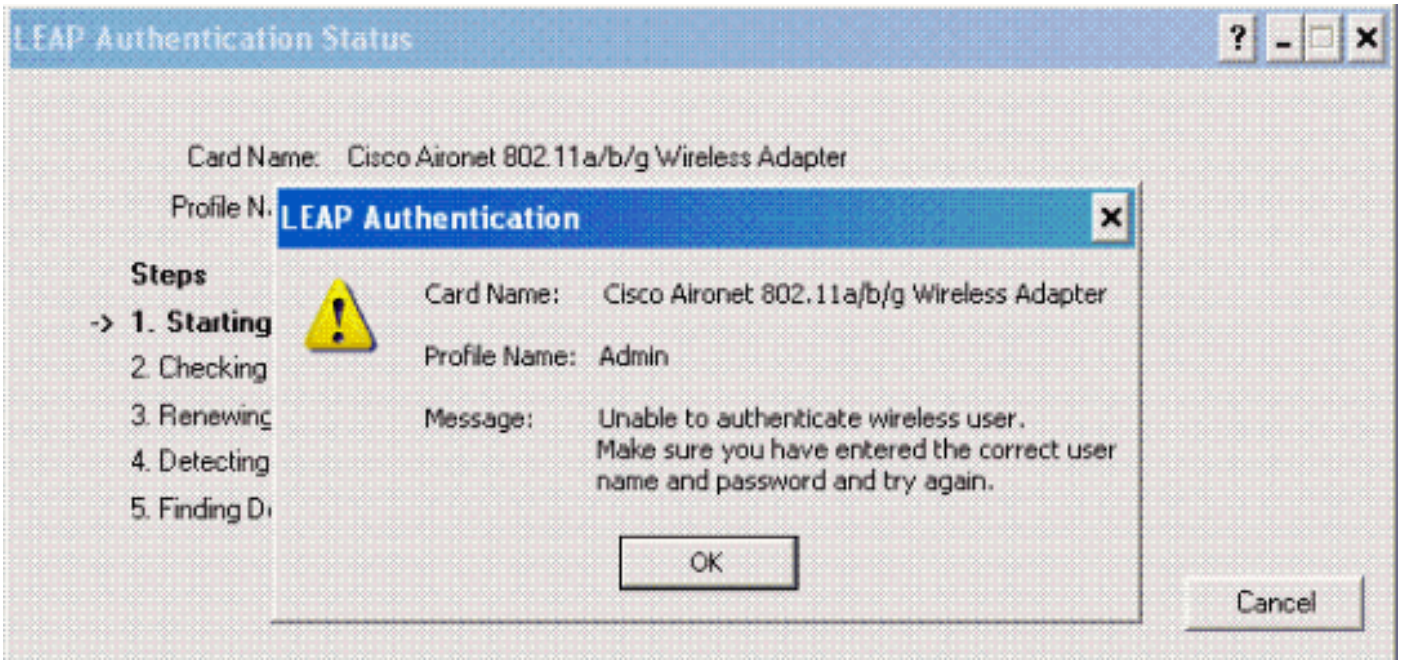
De même, lorsqu'un utilisateur du service Ventes active le profil Ventes, l'utilisateur est authentifié par le serveur RADIUS en fonction du nom d'utilisateur/mot de passe LEAP et du SSID.



Le rapport Passed Authentication sur le serveur ACS indique que le client a réussi l'authentification RADIUS (authentification EAP et authentification SSID). Voici un exemple :



Maintenant, si l'utilisateur Sales tente d'accéder au SSID **Admin**, le serveur RADIUS refuse à l'utilisateur l'accès au WLAN. Voici un exemple :



De cette façon, les utilisateurs peuvent être restreints d'accès en fonction du SSID. Dans un environnement d'entreprise, tous les utilisateurs qui font partie d'un service spécifique peuvent être regroupés en un seul groupe et l'accès au WLAN peut être fourni en fonction du SSID qu'ils utilisent, comme expliqué dans ce document.

Dépannage

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug dot1x aaa enable** - Active le débogage des interactions AAA 802.1x.
- **debug dot1x packet enable — Permet le débogage de tous les paquets dot1x.**

- **debug aaa all enable — Configure le débogage de tous les messages AAA.**

Vous pouvez également utiliser le rapport Passed Authentication et le rapport Failed Authentication sur le serveur Cisco Secure ACS afin de dépanner la configuration. Ces rapports se trouvent sous la fenêtre **Rapports et activité** de l'interface utilisateur graphique ACS.

Informations connexes

- Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil (WLC)
- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Exemple de configuration de réseaux VLAN de groupe de points d'accès avec des contrôleurs de réseau local sans fil
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems