

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

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configuration du réseau](#)

[Configurez](#)

[Configurez le WLC](#)

[Configurez le Cisco Secure ACS](#)

[Configurez le client sans fil et le vérifiez](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Informations connexes](#)

## [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 :

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

### [Composants utilisés](#)

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

- Gamme Cisco 2000 WLC qui exécute les micrologiciels 4.0
- RECOUVREMENT de gamme Cisco 1000
- Serveur Cisco Secure ACS version 3.2
- Adaptateur client sans fil de Cisco 802.11a/b/g qui exécute le micrologiciel 2.6
- Version 2.6 de Cisco Aironet Desktop Utility (ADU)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## 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 de l'accès WLAN basé sur SSID, les utilisateurs peuvent être authentifiés ont basé sur le SSID qu'ils les utilisent afin de connecter au WLAN. Le serveur de Cisco Secure ACS est utilisé pour authentifier les utilisateurs. L'authentification se produit dans deux étapes sur le Cisco Secure ACS :

1. Authentification EAP
2. Authentification SSID basée sur des restrictions d'accès au réseau (NARs) sur le Cisco Secure ACS

Si l'EAP et l'authentification basée sur SSID sont réussis, l'utilisateur est permis pour accéder au WLAN ou bien l'utilisateur est dissocié.

Le Cisco Secure ACS emploie la caractéristique de NARs pour limiter l'accès client basé sur le SSID. Un NAR est une définition, que vous faites dans le Cisco Secure ACS, des conditions supplémentaires qui doivent être remplies avant qu'un utilisateur puisse accéder au réseau. Le Cisco Secure ACS applique ces conditions utilisant les informations à partir des attributs envoyés par vos clients d'AAA. Bien qu'il y ait plusieurs manières que vous pouvez installer NARs, ils tous sont basés sur les informations d'attribut assorties envoyées par le client d'AAA. Par conséquent, vous devez comprendre que le format et le contenu des attributs que vos clients d'AAA envoient si vous voulez utiliser NARs efficace.

Quand vous installez un NAR, vous pouvez choisir si le filtre fonctionne franchement ou négativement. C'est-à-dire, dans le NAR vous spécifiez si permettre ou refuser l'accès au réseau, basé sur une comparaison des informations envoyée des clients d'AAA à l'information enregistrée dans le NAR. Cependant, si un NAR ne rencontre pas les informations suffisantes pour fonctionner, il se transfère sur l'accès refusé.

Vous pouvez définir un NAR pour, et appliquez lui, à un utilisateur ou un groupe d'utilisateurs spécifique. Référez-vous au pour en savoir plus de [Livre Blanc de restrictions d'accès au réseau](#).

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

1. **filtres basés sur IP** — le NAR basé sur IP filtre la limite accès basé sur sur les adresses IP du client d'utilisateur et du client d'AAA. Référez-vous [au sujet des filtres basés sur IP NAR](#) pour plus d'informations sur ce type de filtre NAR.
2. **filtres basés sur Non IP** — le NAR basé sur Non IP filtre la limite accès basé sur sur la comparaison simple de chaîne d'une valeur envoyée du client d'AAA. La valeur peut être le nombre de l'ID ligne appelant (CLI), le nombre de Service d'identification du numéro composé réacheminé (RDNIS), l'adresse MAC, ou toute autre valeur qui provient du client. Pour ce type de NAR à fonctionner, la valeur dans la description NAR doit exactement apparier y compris ce qui est envoyé du client, Qu'est ce que format est utilisé. Par exemple, (217) 555-4534 n'apparient pas 217-555-4534. Référez-vous [au sujet des filtres basés sur Non IP NAR](#) pour plus d'informations sur ce type de filtre NAR.

Ce document utilise les filtres basés sur non IP pour faire l'authentification basée sur SSID. Un filtre basé sur non IP NAR (c'est-à-dire, un filtre DNIS/CLI-based NAR) est une liste d'appeler permis ou refusé/point d'emplacements d'accès que vous pouvez utiliser dans la restriction d'un client d'AAA quand vous n'avez pas une connexion basée sur IP établie. La caractéristique basée sur non IP NAR utilise généralement le nombre CLI et le numéro de DNIS. Il y a des exceptions dans l'utilisation des champs DNIS/CLI. Vous pouvez écrire le nom SSID dans le domaine DNIS et faire l'authentification basée sur SSID. C'est parce que le WLC introduit l'attribut DNIS, le nom SSID, au serveur de RAYON. Ainsi si vous construisez DNIS NAR dans l'utilisateur ou le groupe, vous pouvez créer des restrictions du par-utilisateur SSID.

Si vous utilisez le RAYON, les champs NAR répertoriés ici utilisent ces valeurs :

- **Client d'AAA** — La Nas-IP-adresse (l'attribut 4) ou, si la Nas-IP-adresse n'existe pas, le Nas-identifiant (attribut RADIUS 32) est utilisé.
- **Port** — Le Nas-port (l'attribut 5) ou, si le Nas-port n'existe pas, le Nas-port-ID (attribut 87) est utilisé.
- **CLI** — Le calling-station-id (attribut 31) est utilisé.
- **DNIS** — L'appeler-station-ID (attribut 30) est utilisé.

Référez-vous aux [restrictions d'accès au réseau](#) pour plus d'informations sur l'utilisation du NAR.

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

- **Client d'AAA** — Adresse IP WLC
- **port** — \*
- **CLI** — \*
- **DNIS** — \*ssidname

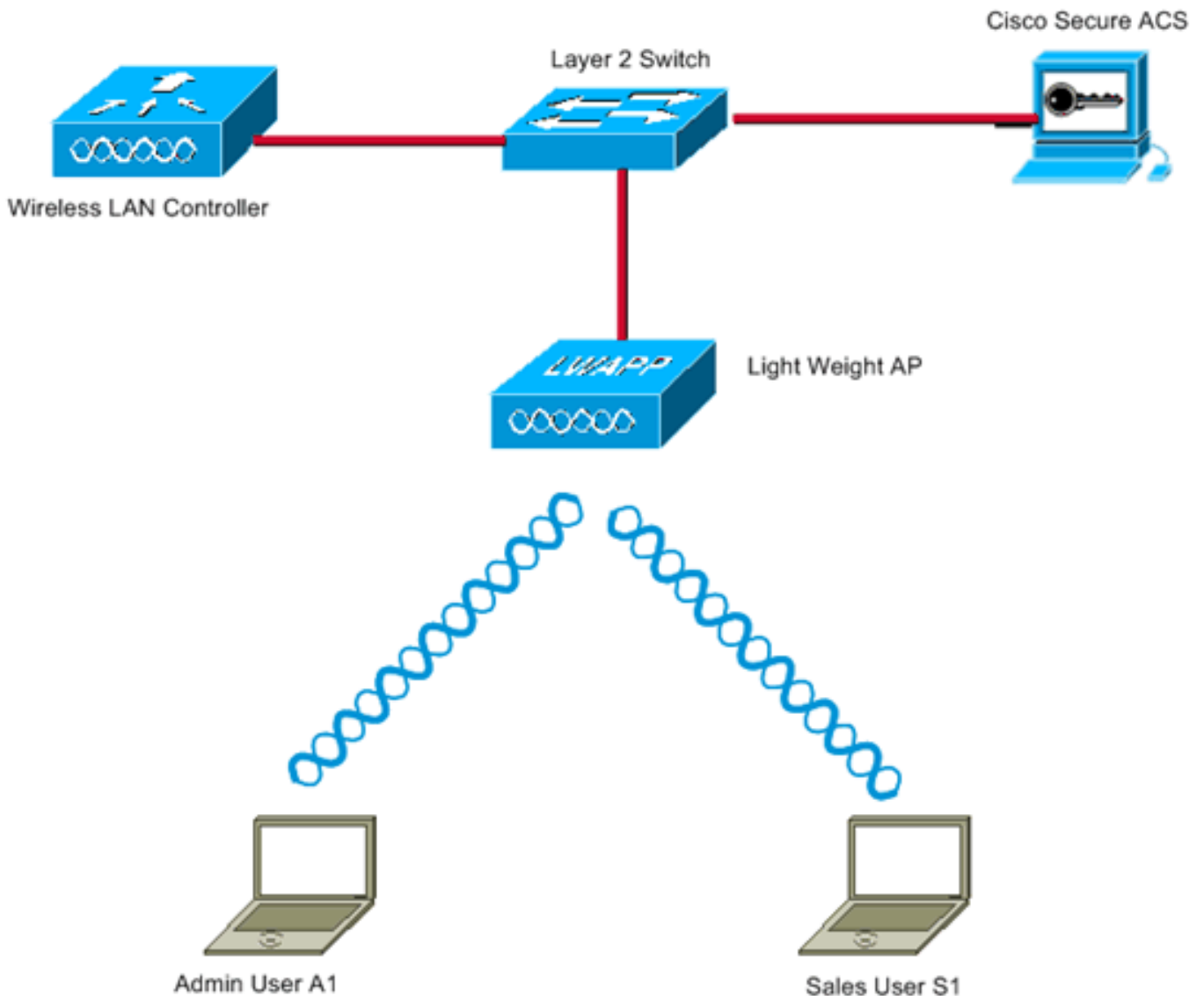
Le reste de ce document fournit un exemple de configuration sur la façon dont accomplir ceci.

## [Configuration du réseau](#)

Dans cette installation d'exemple, WLC est enregistré au RECOUVREMENT. Deux WLAN sont utilisés. Un WLAN est pour les utilisateurs de service d'admin et l'autre WLAN est pour les utilisateurs de service de vente. Le client sans fil A1 (utilisateur d'admin) et S1 (utilisateur de ventes) se connectent au réseau Sans fil. Vous devez configurer le WLC et le serveur de RAYON de telle manière que l'utilisateur A1 d'admin puisse accéder à seulement l'**admin** WLAN et soit accès limité aux **ventes** et à l'utilisateur S1 WLAN de ventes devrait pouvoir accéder aux **ventes** WLAN et devrait avoir limité l'accès à l'**admin** WLAN. Toute l'authentification de LEAP d'utilisation

d'utilisateurs comme méthode d'authentification de la couche 2.

**Remarque:** Ce document suppose que le WLC est enregistré au contrôleur. Si vous êtes nouveau à WLC et ne savez pas configurer le WLC pour le fonctionnement de base, vous rappelez à [l'enregistrement léger AP \(RECOUVREMENT\) à un contrôleur LAN 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

## Configurez

Afin de configurer les périphériques pour cette installation, vous avez besoin :

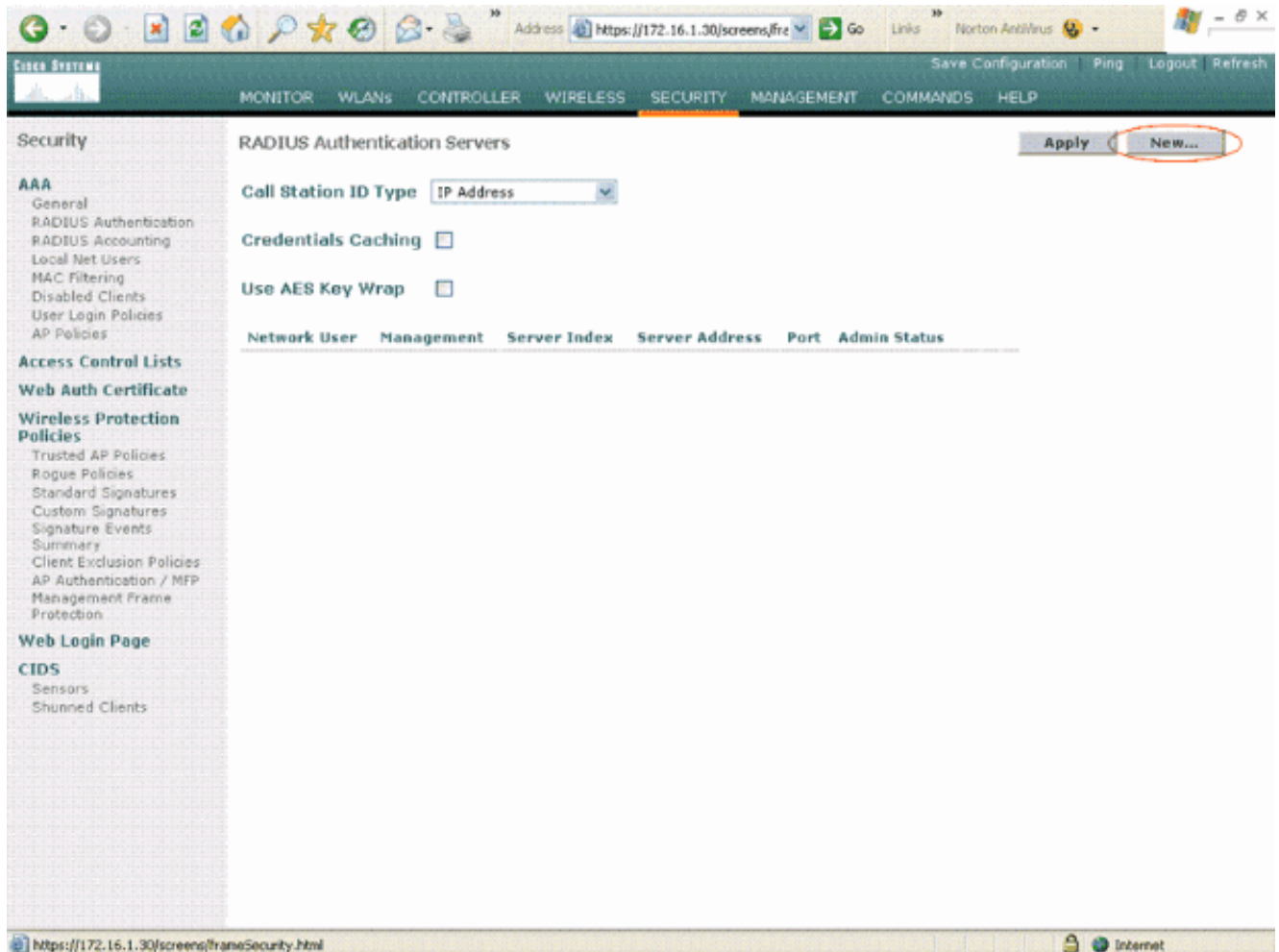
1. [Configurez le WLC pour les deux WLAN et serveurs de RAYON.](#)
2. [Configurez le Cisco Secure ACS.](#)

### 3. [Configurez les clients sans fil et les vérifiez.](#)

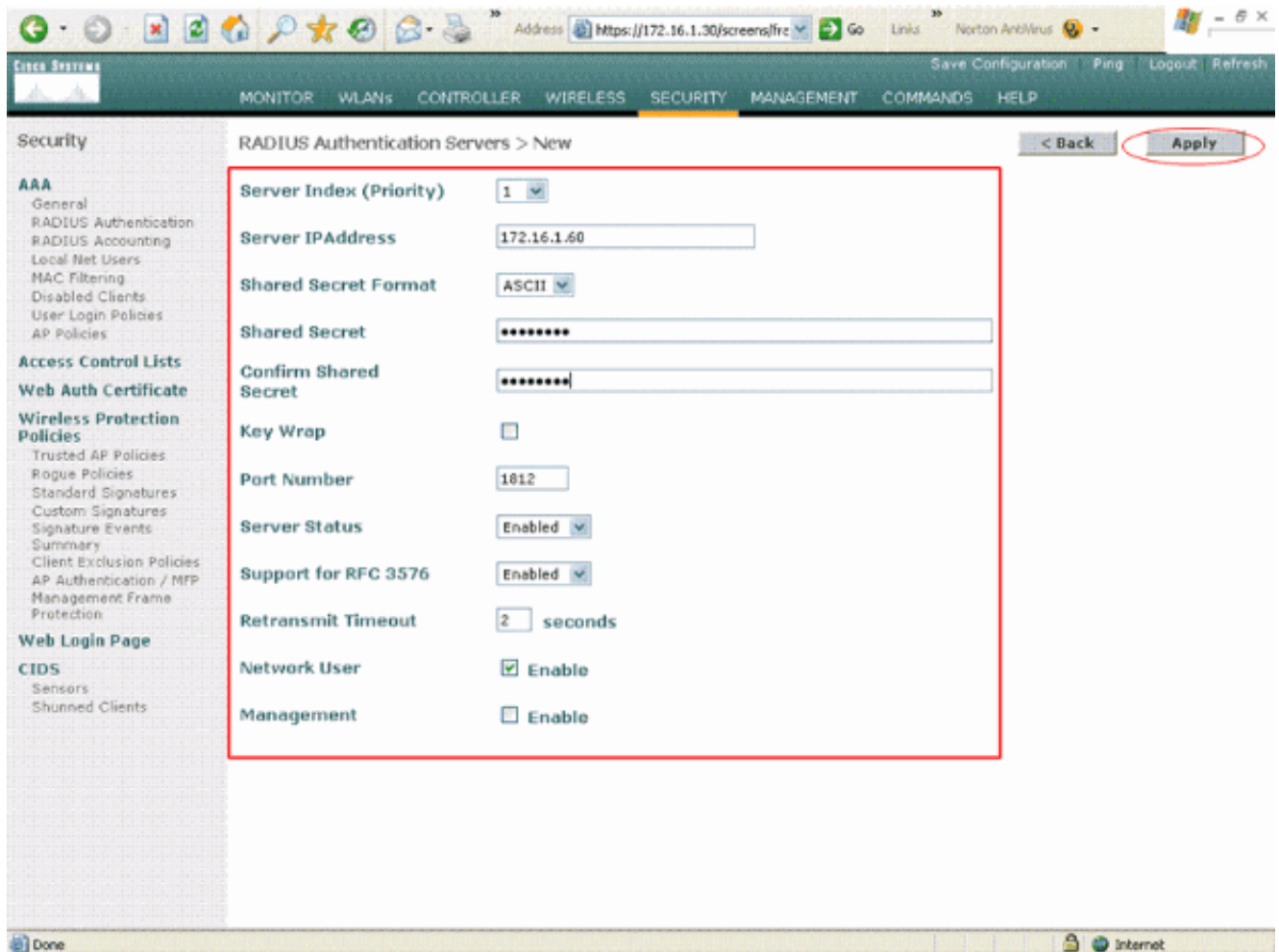
## [Configurez le WLC](#)

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

1. Le WLC doit être configuré pour expédier les identifiants utilisateurs à un serveur RADIUS externe. Le serveur RADIUS externe (Cisco Secure ACS dans ce cas) alors valide les identifiants utilisateurs et permet d'accéder aux clients sans fil. Procédez comme suit : Choisissez le **Security > RADIUS Authentication** du GUI de contrôleur afin d'afficher la page de serveurs d'authentification RADIUS.

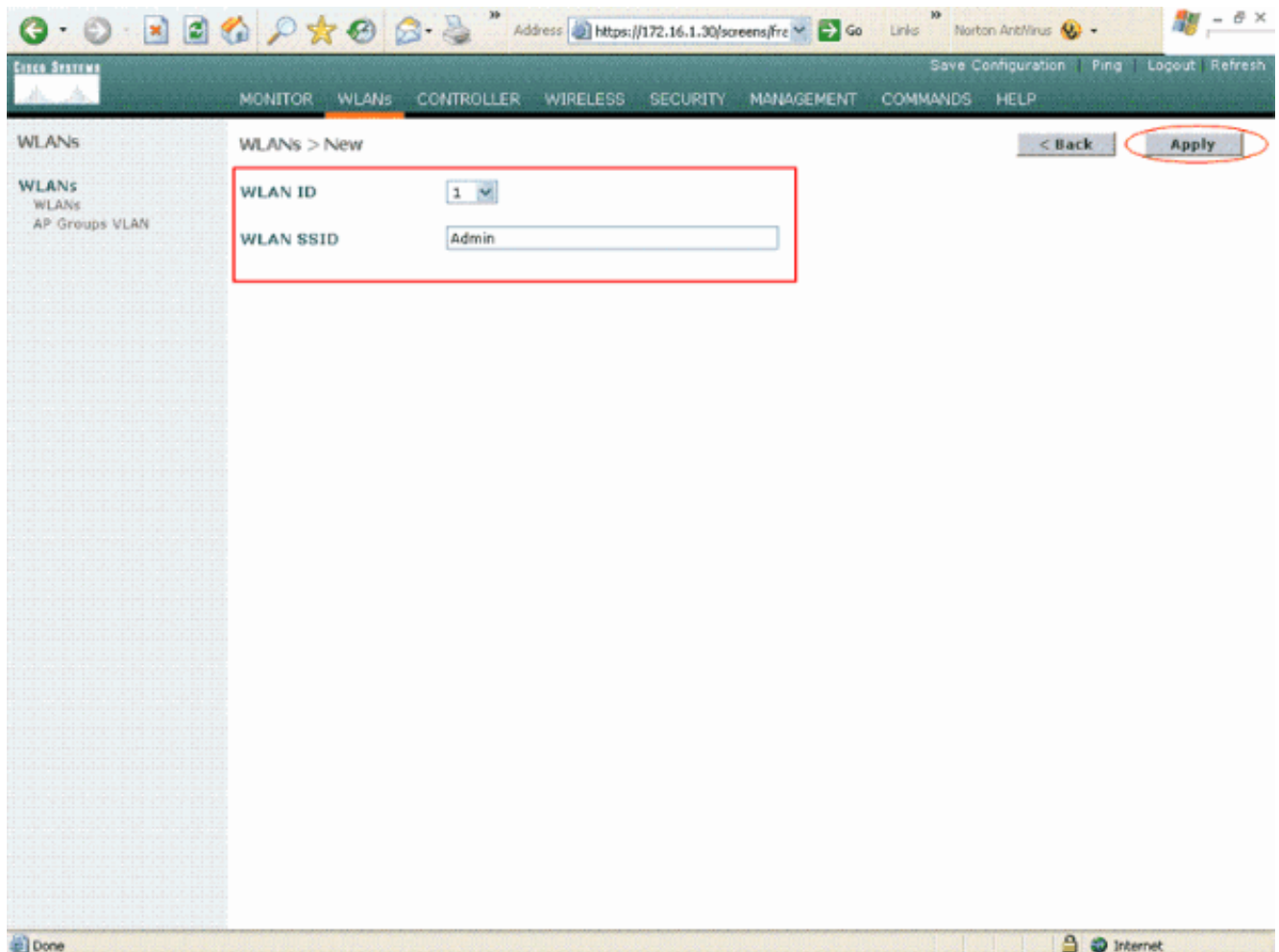


Cliquez sur New afin de définir les paramètres de serveur de RADIUS. Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du serveur. Les cases à cocher d'utilisateur du réseau et de gestion déterminent si l'authentification basée sur RADIUS s'applique pour la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



Cliquez sur **Apply**.

2. Configurez un WLAN pour le service d'admin avec l'**admin** SSID et l'autre WLAN pour le service de vente avec des **ventes** SSID. 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 **Admin** nommé par WLAN pour le service d'admin et l'ID de WLAN est 1. Cliquez sur **Apply**.



Dans la fenêtre de **WLAN > Edit**, définissez les paramètres spécifiques au WLAN : Du menu déroulant de degré de sécurité de la couche 2, **802.1x** choisi. Par défaut, l'option de degré de sécurité de la couche 2 est 802.1x. Ceci active l'authentification 802.1x/EAP pour le WLAN. Dans le cadre des stratégies générales, cochez la case de **priorité d'AAA**. Quand le dépassement d'AAA est activé, et un client a l'AAA et les paramètres contradictoires d'authentification du contrôleur WLAN, l'authentification client est exécutée par le serveur d'AAA. Sélectionnez le serveur compétent de RAYON du menu déroulant sous des serveurs de RAYON. Les autres paramètres peuvent être modifiés sur les conditions requises du réseau WLAN. Cliquez sur **Apply**.

WLAN ID 1  
WLAN SSID Admin

**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

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



Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs > New

WLAN ID: 2

WLAN SSID: Sales

< Back | **Apply**

WLANs

WLANs

AP Groups VLAN

Done | Internet

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs > Edit

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

## Configurez le Cisco Secure ACS

Sur le serveur de Cisco Secure ACS vous avez besoin :

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

Terminez-vous ces étapes sur le Cisco Secure ACS :

1. Afin de définir le contrôleur en tant que client d'AAA sur le serveur ACS, cliquez sur Network Configuration du GUI ACS. Sous l'AAA les clients cliquent sur en fonction l'**entrée Add**.

**CISCO SYSTEMS** Network Configuration

Select

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		













Add Entry Search

AAA Servers		
AAA Server Name	AAA Server IP Address	AAA Server Type
<a href="#">tsweb-laptop</a>	127.0.0.1	CiscoSecure ACS

Add Entry Search


Back to Help

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).

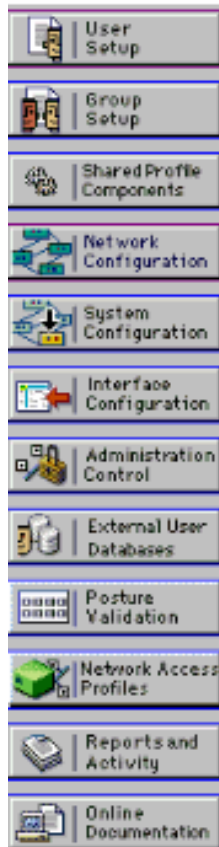
-  User Setup
-  Group Setup
-  Shared Profile Components
-  Network Configuration
-  System Configuration
-  Interface Configuration
-  Administration Control
-  External User Databases
-  Posture Validation
-  Network Access Profiles
-  Reports and Activity
-  Online Documentation

## Add AAA Client

AAA Client Hostname	<input type="text" value="WLC"/>
AAA Client IP Address	<input type="text" value="172.16.1.30"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco Airespace)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

 [Back to Help](#)

3. Cliquez sur User Setup du GUI ACS, écrivez le nom d'utilisateur, et cliquez sur Add//éditez. 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 parce que vous avez besoin de ces paramètres pour l'authentification de LEAP.



## User: A1 (New User)

Account Disabled

### Supplementary User Info

Real Name   
 Description

### User Setup

Password Authentication:

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:

5. Faites descendre l'écran la page d'installation utilisateur, jusqu'à ce que vous voyiez la section de restrictions d'accès au réseau. Sous l'interface utilisateur de la restriction DNIS/CLI Access, sélectionnez le **point appelant laissé des emplacements d'Access** et définissez ces paramètres : **Client d'AAA** — Adresse IP WLC (172.16.1.30 dans notre exemple) **Port** — \*CLI — \*DNIS — \*ssidname
6. L'attribut DNIS définit le SSID qu'on permet à l'utilisateur pour accéder à. Le WLC envoie le SSID dans l'attribut DNIS au serveur de RAYON. Si les besoins de l'utilisateur d'accéder à seulement le WLAN nommaient Admin, entrez dans le \*Admin pour le champ DNIS. Ceci s'assure que l'utilisateur a accès seulement à Admin nommé par WLAN. Le clic **entrent**. **Remarque:** Le SSID devrait toujours être précédé avec \*. C'est obligatoire.

## Advanced Settings

- 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

### Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	Address
<span style="border: 1px solid #ccc; padding: 2px 5px;">remove</span>		

AAA Client All AAA Clients

Port  

Address  

enter

---

Define CLI/DNIS-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS
<span style="border: 1px solid #ccc; padding: 2px 5px;">remove</span>			

AAA Client WLC

Port \*

CLI \*

DNIS \*Admin

enter

Submit
Cancel

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



# 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

- 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

### Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address
<span style="border: 1px solid gray; padding: 2px;">remove</span>		

AAA Client: All AAA Clients

Port:

Address:

enter

---

Define CLI/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS
<span style="border: 1px solid gray; padding: 2px;">remove</span>			

AAA Client: WLC

Port: \*

CLI: \*

DNIS: \*Sales

enter

Submit
Cancel

9. Répétez le même processus pour ajouter plus d'utilisateurs à la base de données. **Remarque:** Par défaut tous les utilisateurs sont groupés sous le groupe par défaut. Si vous voulez affecter les utilisateurs spécifiques à différents groupes, référez-vous à la [section Gestion de groupe d'utilisateurs du guide utilisateur pour le Cisco Secure ACS pour les Windows Server 3.2](#). **Remarque:** Si vous ne voyez pas la section de restrictions d'accès au réseau dans la fenêtre d'installation utilisateur, elle pourrait être parce qu'elle n'est pas activée. Afin d'activer les restrictions d'accès au réseau pour des utilisateurs, choisissez les interfaces > a avancé des options du GUI ACS, des restrictions choisies d'accès au réseau de niveau utilisateur et clique sur Submit. Ceci active le NAR et apparaît dans la fenêtre d'installation utilisateur.



# 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



## Advanced Settings

- 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

### Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	Address
<span style="border: 1px solid gray; padding: 2px;">remove</span>		

AAA Client All AAA Clients

Port  

Address  

enter

---

Define CLI/DNIS-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS
<span style="border: 1px solid gray; padding: 2px;">remove</span>			

AAA Client WLC

Port \*

CLI \*

DNIS \*Admin

enter

Submit
Cancel

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

- 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

## Global Authentication Setup

EAP Configuration ?

**PEAP**

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

---

**EAP-FAST**

[EAP-FAST Configuration](#)

---

**EAP-TLS**

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

---

**LEAP**

Allow LEAP (For Aironet only)

---

**EAP-MD5**

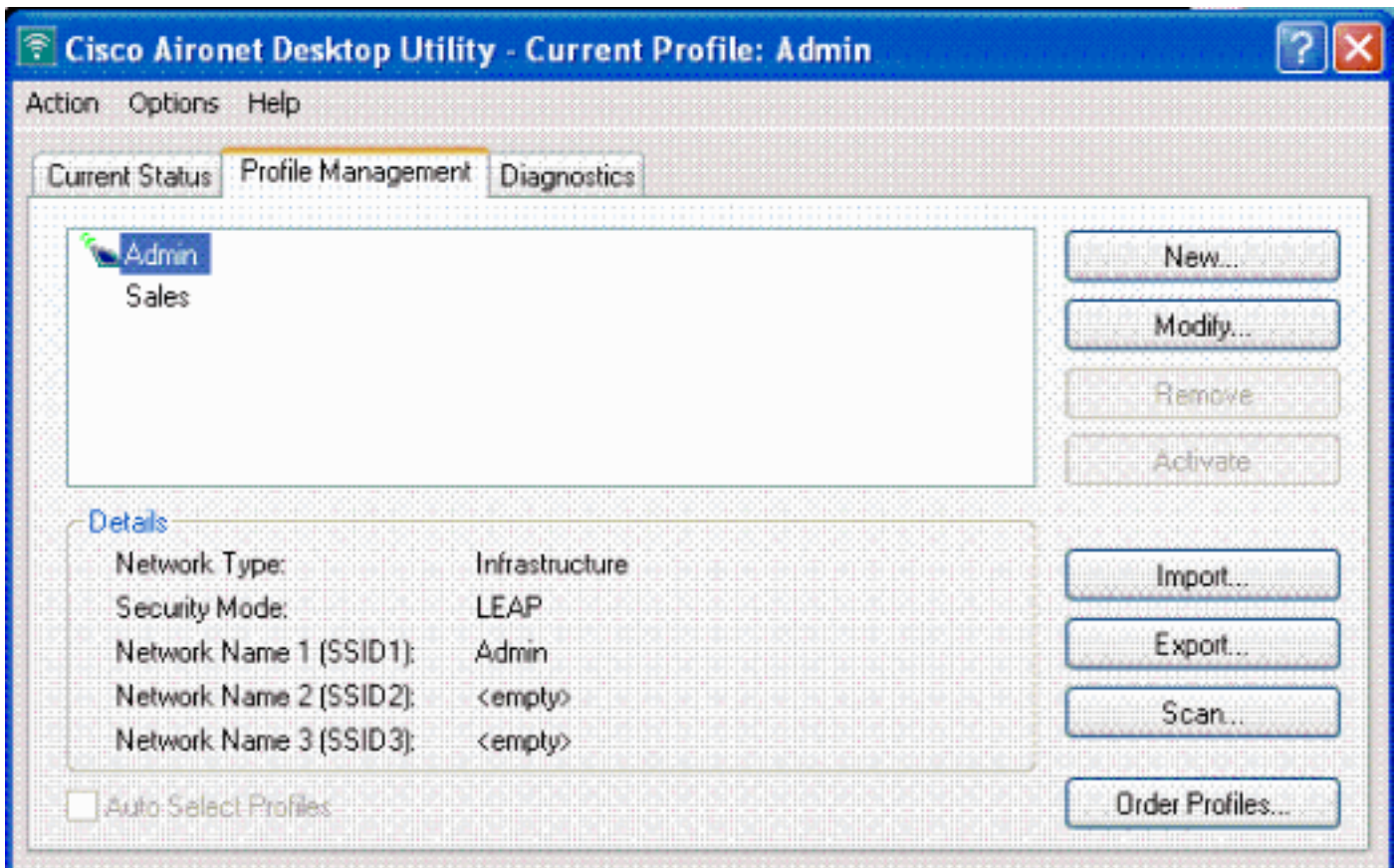
Submit
Submit + Restart
Cancel

## [Configurez le client sans fil et le vérifiez](#)

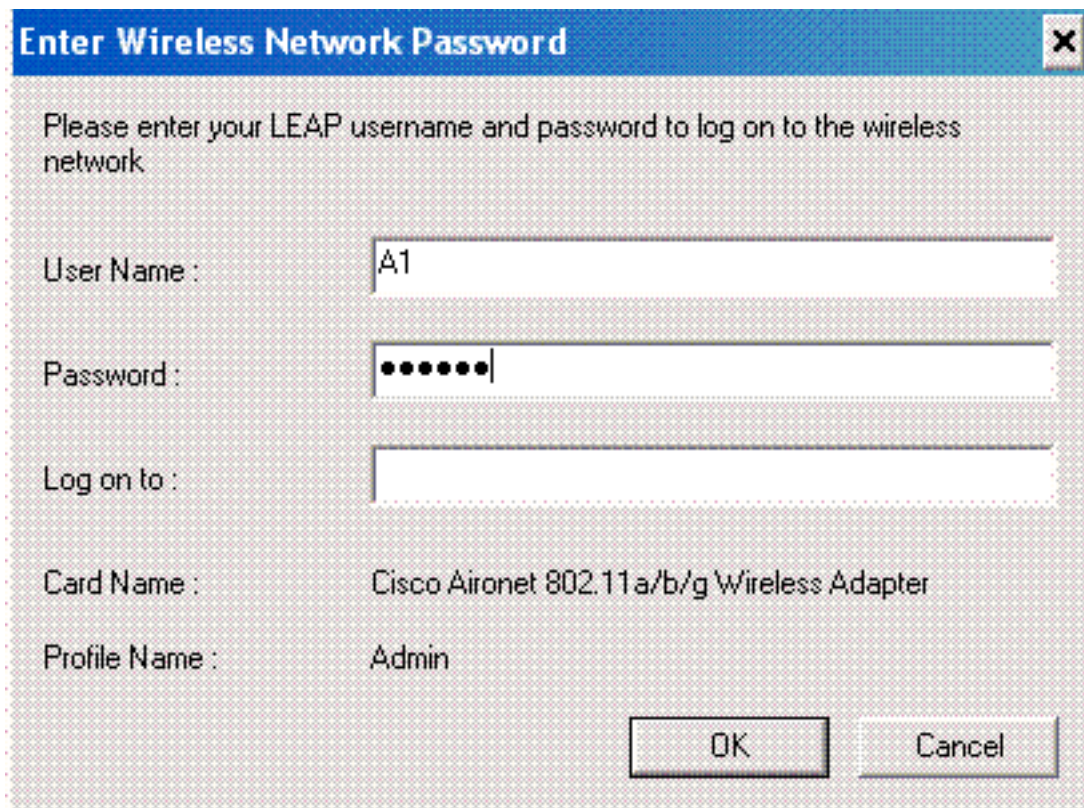
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Essayez d'associer un client sans fil avec le RECOUVREMENT utilisant l'authentification de LEAP pour vérifier si la configuration fonctionne comme prévu.

**Remarque:** ce document suppose que le profil client est configuré pour l'authentification LEAP. Référez-vous [en utilisant l'authentification EAP](#) pour les informations sur la façon dont configurer l'adaptateur client sans fil du 802.11 a/b/g pour l'authentification de LEAP.

**Remarque:** De l'ADU vous voyez que vous avez configuré deux profils de client. Un pour les utilisateurs de service d'admin avec l'**admin** SSID et l'autre profil pour les utilisateurs de service de vente avec des **ventes** SSID. Les deux profils sont configurés pour l'authentification de LEAP.



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

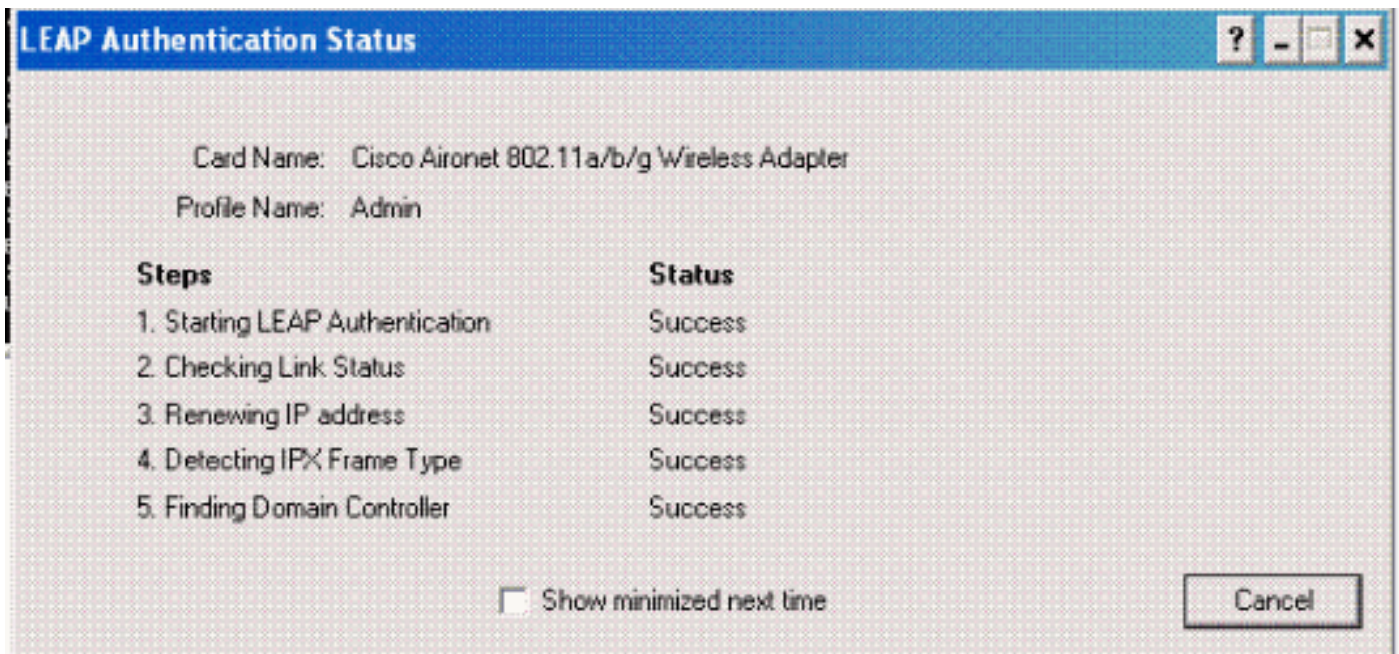


Le RECOUVREMENT et alors le WLC transmettent les identifiants utilisateurs au serveur RADIUS externe (Cisco Secure ACS) pour valider les qualifications. Le WLC passe en fonction les qualifications comprenant l'attribut DNIS (nom SSID) au serveur de RAYON pour la validation.

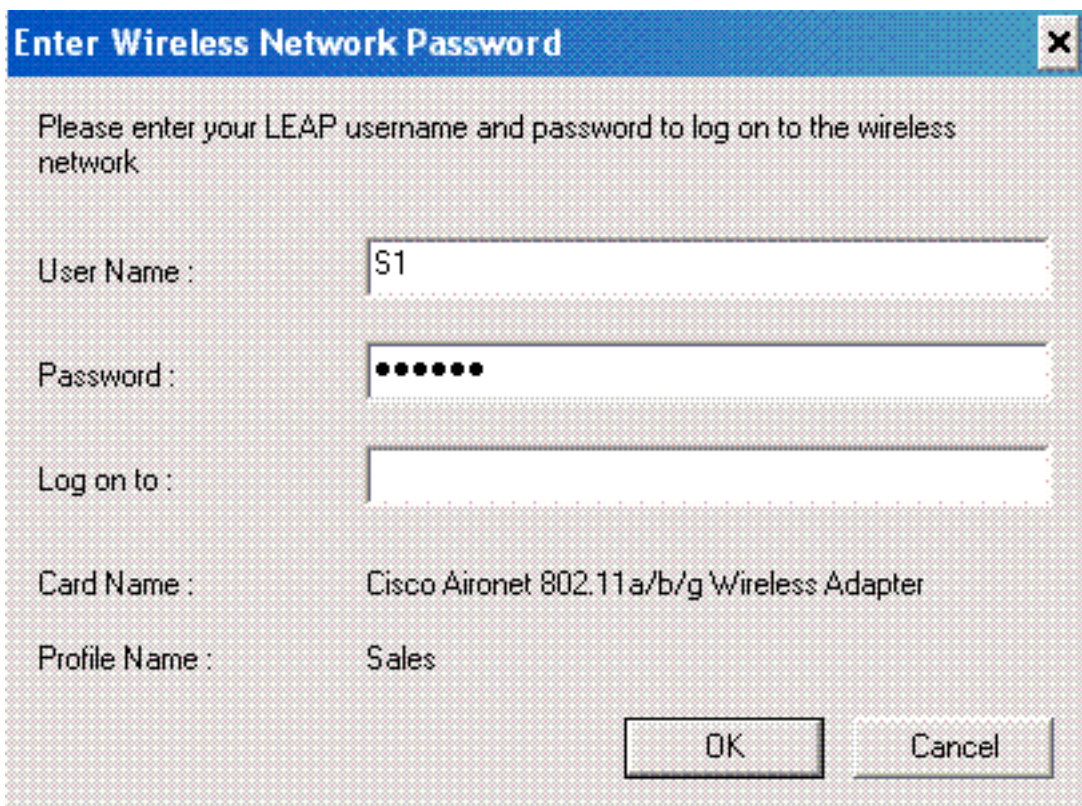
Le serveur de RAYON vérifie les identifiants utilisateurs en comparant les données à la base de

données utilisateur (et au NARs) et permet d'accéder au client sans fil toutes les fois que les identifiants utilisateurs sont valides.

Sur l'authentification réussie de RAYON le client sans fil s'associe avec le RECOUVREMENT.



De même quand un utilisateur du service de vente lance le profil de ventes, l'utilisateur est authentifié par le serveur de RAYON basé sur le nom d'utilisateur/mot de passe de LEAP et le SSID.



L'état passé d'authentification sur le serveur ACS prouve que le client a passé l'authentification de RAYON (authentification EAP et authentification SSID). Voici un exemple :

## Reports and Activity

Select

Passed Authentications active.csv Refresh Download

Regular Expression Start Date & Time End Date & Time Rows per Page

Apply Filter Clear Filter

Filtering is not applied.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAR-Port	NAR-IP-Address	Network Access Profile Name	Shared BAC	Downloadable ACL	System-Posture-Token	Application-Posture-Token	Reason	EAP Type	EAP Type Name
10/11/2006	14:48:40	Authen OK	S1	Default Group	00-40-9E-9E-57	1	172.16.1.30	(Default)	..	..	..	..	..	17	LEAP
10/11/2006	14:47:05	Authen OK	A1	Default Group	00-40-9E-9E-57	1	172.16.1.30	(Default)	..	..	..	..	..	17	LEAP

Maintenant, si les essais d'utilisateur de ventes pour accéder à l'**admin** SSID, le serveur de RAYON refuse l'accès client au WLAN. Voici un exemple :



De cette façon les utilisateurs peut être accès basé sur limité sur le SSID. Dans un environnement d'entreprise, tous les utilisateurs qui tombent dans un service spécifique peuvent être groupés dans un groupe et un accès simples au WLAN peuvent être fournis ont basé sur le SSID qu'ils les utilisent comme expliqué dans ce document.

## Dépannez

### 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:** Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de débogage.

- **enable d'AAA de debug dot1x** — Active le débogage des interactions d'AAA de 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 employer l'état passé d'authentification et l'état d'authentification défaillante sur le serveur de Cisco Secure ACS afin de dépanner la configuration. Ces états sont sous la fenêtre d'**états et d'activité** sur le GUI 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](#)