

Exemple de configuration d'une affectation de VLAN dynamique avec un serveur RADIUS et un contrôleur de réseau local sans fil

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Affectation de VLAN dynamique avec le serveur RADIUS](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configuration](#)

[Étapes de configuration](#)

[Configuration du serveur RADIUS](#)

[Configurer l'ACS avec les attributs VSA Cisco Airespace pour l'affectation de VLAN dynamique](#)

[Configurer la commutation pour plusieurs VLAN](#)

[Configuration WLC](#)

[Configuration de l'utilitaire du client sans fil](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document présente le concept d'affectation de VLAN dynamique. Le document décrit comment configurer le contrôleur LAN sans fil (WLC) et un serveur RADIUS pour affecter des clients LAN sans fil (WLAN) dans un VLAN spécifique de façon dynamique.

Conditions préalables

Conditions requises

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

- Avoir une connaissance de base du WLC et des points d'accès légers (LAP)
- Avoir une connaissance fonctionnelle du serveur AAA
- Avoir une connaissance complète des réseaux sans fil et des problèmes liés à la sécurité

sans fil

- Avoir une connaissance de base du protocole LWAPP (Lightweight AP Protocol)

Composants utilisés

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

- WLC Cisco 4400 exécutant la version de microprogramme 5.2
- LAP de la gamme Cisco 1130
- Adaptateur client sans fil Cisco 802.11a/b/g exécutant la version de microprogramme 4.4
- Utilitaire Cisco Aironet Desktop Utility (ADU) exécutant la version 4.4
- Serveur de contrôle d'accès CiscoSecure (ACS) exécutant la version 4.1
- Commutateur de la série Cisco 2950

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](#).

Affectation de VLAN dynamique avec le serveur RADIUS

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

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

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

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

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

- IETF 64 (Tunnel Type) — Définissez cette valeur sur VLAN.
- IETF 65 (Tunnel Medium Type) — Définissez cette valeur sur 802
- IETF 81 (Tunnel Private Group ID) — Définissez cette valeur sur l'ID du VLAN

L'ID du VLAN est de 12 bits et prend une valeur entre 1 et 4 094, inclus. Puisque Tunnel-Private-Group-ID est de type chaîne, comme défini dans [RFC2868](#) pour une utilisation avec IEEE 802.1X, la valeur entière de l'ID de VLAN est codée en tant que chaîne. [Quand ces attributs de tunnel sont envoyés, il est nécessaire de renseigner la zone Tag.](#)

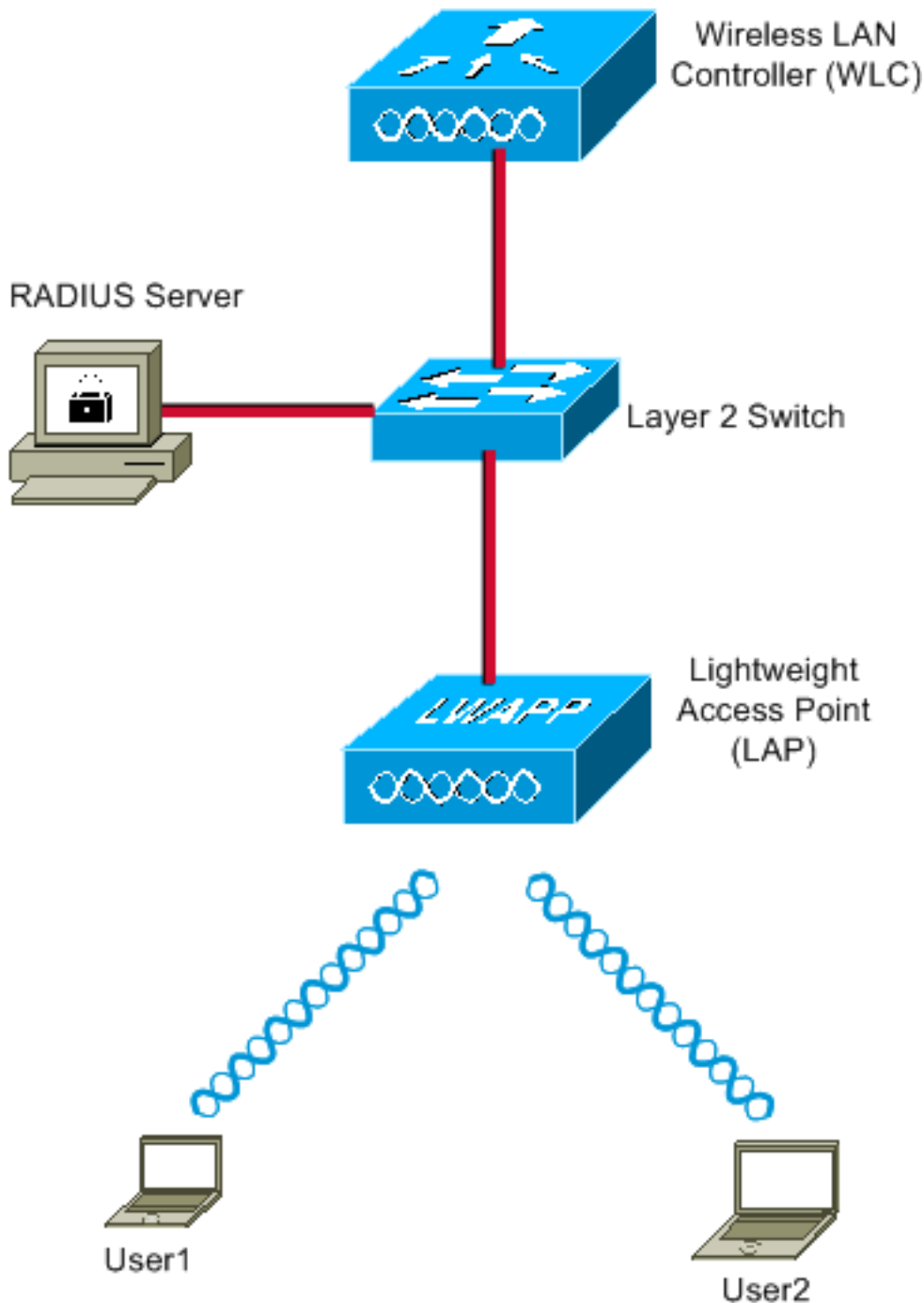
Comme observé dans [RFC2868](#), section 3.1 : **La zone Tag a une longueur d'un octet et sa fonction est de fournir un moyen de regrouper les attributs dans le même paquet qui fait référence au même tunnel.** Les valeurs valides pour cette zone sont comprises entre 0x01 et 0x1F, inclus. Si la zone Tag est inutilisée, elle doit avoir pour valeur zéro (0x00). Référez-vous à [RFC 2868](#) pour plus d'informations sur tous les attributs RADIUS.

[Configurez](#)

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

[Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :



Voici les détails de configuration des composants utilisés dans ce diagramme :

- L'adresse IP du serveur ACS (RADIUS) est 172.16.1.1.
- L'adresse de l'interface de gestion du WLC est 172.16.1.30.
- L'adresse de l'interface de gestionnaire AP du WLC est 172.16.1.31.
- L'adresse 172.16.1.1 de serveur DHCP est utilisée pour assigner des adresses IP au LWAPP. **Le serveur DHCP interne sur le contrôleur est utilisé pour affecter l'adresse IP aux clients sans fil.**
- VLAN10 et VLAN11 sont utilisés dans l'ensemble de cette configuration. L'utilisateur user1 est configuré pour être placé dans le VLAN10 et user2 est configuré pour être placé dans VLAN11 par le serveur RADIUS. **Remarque:** Ce document montre uniquement toutes les informations de configuration relatives à l'utilisateur user1. Complétez la même procédure expliquée dans ce document pour l'utilisateur user2.
- Ce document utilise 802.1x avec LEAP comme mécanisme de sécurité. **Remarque:** Cisco vous recommande d'utiliser des méthodes d'authentification avancées, telles que

l'authentification EAP-FAST et EAP-TLS, afin de sécuriser le WLAN. Ce document utilise LEAP seulement pour la simplicité.

Configuration

Avant de commencer la configuration, ce document suppose que le LAP est déjà enregistré auprès du WLC. Référez-vous à [Exemple de configuration de base du contrôleur de LAN sans fil \(WLC\) et des points d'accès légers](#) pour plus d'informations. Référez-vous à [Enregistrement des points d'accès légers \(LAP\) auprès d'un contrôleur de LAN sans fil \(WLC\)](#) pour des informations sur la procédure d'enregistrement impliquée.

Étapes de configuration

Cette configuration est divisée en trois catégories :

1. [Configuration du serveur RADIUS](#)
2. [Configurer la commutation pour plusieurs VLAN](#)
3. [Configuration WLC](#)
4. [Configuration de l'utilitaire du client sans fil](#)

Configuration du serveur RADIUS

Cette configuration requiert les étapes suivantes :

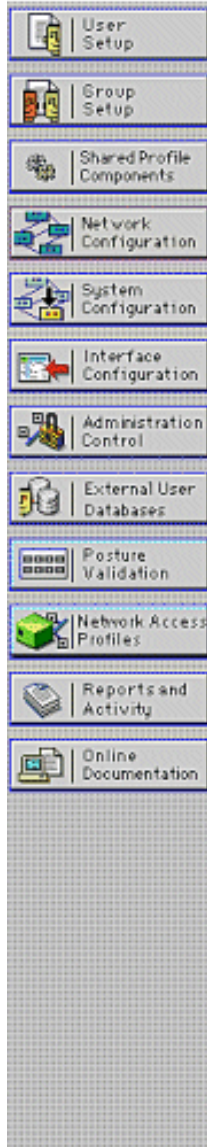
- [Configurez le WLC en tant que client d'AAA sur le serveur de RAYON](#)
- [Configurer les utilisateurs et les attributs RADIUS \(IETF\) utilisés pour l'affectation de VLAN dynamique sur le serveur RADIUS](#)

Configurer le client AAA pour le WLC sur le serveur RADIUS

Cette procédure explique comment ajouter le WLC comme client AAA sur le serveur RADIUS de sorte que le WLC puisse passer les informations d'identification des utilisateurs au serveur RADIUS.

Procédez comme suit :

1. Dans l'interface graphique ACS, cliquez sur **Network Configuration**.
2. Cliquez sur la section **Add Entry** en dessous de la zone AAA Client.
3. Entrez l'adresse IP et la clé du client AAA. L'adresse IP devrait être l'adresse IP de l'interface de gestion du WLC. Assurez-vous que la clé que vous entrez est la même que celle qui est configurée sur le WLC dans la fenêtre Security. Il s'agit de la clé secrète utilisée pour la communication entre le client AAA (WLC) et le serveur RADIUS.
4. Choisissez **RADIUS (Cisco Airespace)** dans la zone Authenticate Using pour le type d'authentification.



Add AAA Client

AAA Client Hostname	<input type="text" value="WLC4400"/>
AAA Client IP Address	<input type="text" value="172.16.1.30"/>
Shared Secret	<input type="text" value="cisco"/>

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format ASCII Hexadecimal

Authenticate Using

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

[Configurer les utilisateurs et les attributs RADIUS \(IETF\) utilisés pour l'affectation de VLAN dynamique sur le serveur RADIUS](#)

Cette procédure explique comment configurer les utilisateurs dans le serveur RADIUS et les attributs RADIUS (IETF) utilisés pour affecter des ID de VLAN à ces utilisateurs.

Procédez comme suit :

1. Dans l'interface graphique ACS, cliquez sur **User Setup**.
2. Dans la fenêtre User Setup, entrez un nom d'utilisateur dans la zone User et cliquez sur **Add/Edit**.



User Setup

Select

- 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:

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](#)

[Back to Help](#)

3. Dans la page Edit, entrez les informations utilisateur nécessaires comme montré ici :

- 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: User1

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.

Dans ce diagramme, notez que le mot de passe que vous fournissez sous la section User Setup doit être identique à celle qui a été fournie côté client pendant l'authentification de l'utilisateur.

- Faites défiler la page Edit vers le bas et recherchez la zone **IETF RADIUS Attributes**.
- Dans la zone IETF RADIUS Attributes, activez les case à cocher situées en regard des trois attributs Tunnel et configurez les valeurs d'attribut comme montré ici :



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

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

Downloadable ACLs

Assign IP ACL: VPN_Access

IETF RADIUS Attributes

[064] Tunnel-Type

Tag 1 Value VLAN

Tag 2 Value

[065] Tunnel-Medium-Type

Tag 1 Value 802

Tag 2 Value

[081] Tunnel-Private-Group-ID

Tag 1 Value 10

Tag 2 Value

Remarque: Dans la configuration initiale du serveur ACS, les attributs RADIUS IETF peuvent ne pas être affichés. Choisissez **Interface Configuration > RADIUS (IETF)** afin d'activer les attributs IETF dans la fenêtre de configuration utilisateur. Ensuite, activez les cases à cocher pour les attributs **64, 65 et 81** dans les colonnes User et Groupe.



Interface Configuration

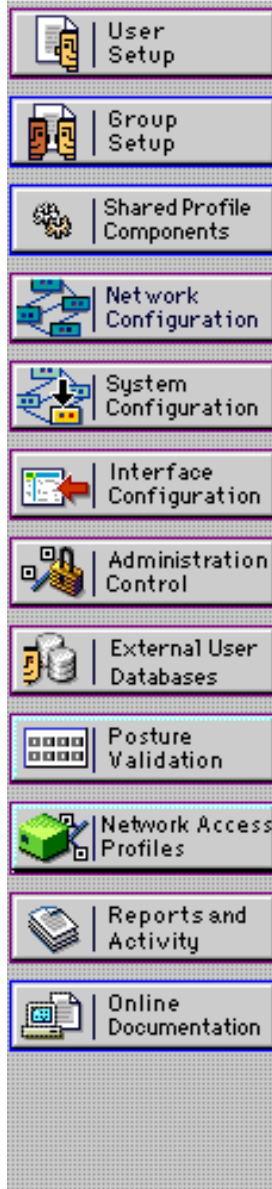
- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

- [029] Termination-Action
- [033] Proxy-State
- [034] Login-LAT-Service
- [035] Login-LAT-Node
- [036] Login-LAT-Group
- [037] Framed-AppleTalk-Link
- [038] Framed-AppleTalk-Network
- [039] Framed-AppleTalk-Zone
- [062] Port-Limit
- [063] Login-LAT-Port
- [064] Tunnel-Type
- [065] Tunnel-Medium-Type
- [066] Tunnel-Client-Endpoint
- [067] Tunnel-Server-Endpoint
- [069] Tunnel-Password
- [071] ARAP-Features
- [072] ARAP-Zone-Access
- [078] Configuration-Token
- [081] Tunnel-Private-Group-ID
- [082] Tunnel-Assignment-ID
- [083] Tunnel-Preference
- [085] Acct-Interim-Interval
- [090] Tunnel-Client-Auth-ID
- [091] Tunnel-Server-Auth-ID

Remarque: Pour que le serveur RADIUS affecte dynamiquement le client à un VLAN spécifique, il est nécessaire que les valeurs VLAN-ID configurées sous la zone IETF 81 (Tunnel-Private-Group-ID) du serveur RADIUS existent sur le WLC. Activez la case à cocher de l'attribut **Per User TACACS+/RADIUS** en dessous de Interface Configuration > Advanced Options afin d'activer le serveur RADIUS pour des configurations par utilisateur. Également, parce que LEAP est utilisé comme protocole d'authentification, assurez-vous que LEAP est activé dans la fenêtre de configuration système du serveur RADIUS, comme montré ici :



System Configuration



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

Allow EAP-MD5

AP EAP request timeout (seconds):

[Configurer l'ACS avec les attributs VSA Cisco Airespace pour l'affectation de VLAN dynamique](#)

Dans les dernières versions ACS, vous pouvez également configurer l'attribut Cisco Airespace [VSA (Vendor Specific Attribute)] pour affecter à un utilisateur correctement authentifié un nom d'interface VLAN (pas l'ID de VLAN) en fonction de la configuration utilisateur sur ACS. Afin d'accomplir cela, exécutez les étapes de cette section.

Remarque: Cette section utilise ACS version 4.1 pour configurer l'attribut VSA Cisco Airespace.

[Configurer le groupe ACS avec l'option d'attribut VSA Cisco Airespace](#)

Procédez comme suit :

1. Dans l'interface graphique ACS 4.1, cliquez sur **Interface Configuration** dans la barre de

navigation. Puis, sélectionnez **RADIUS (Cisco Airespace)** dans la page Interface Configuration afin de configurer l'option d'attribut Cisco Airespace.

2. Dans la fenêtre RADIUS (Cisco Airespace), activez la case à cocher User (et la case à cocher Group si nécessaire) à côté de **Aire-Interface-Name** afin de l'afficher dans la page User Edit. Puis, cliquez sur **Submit**.

CISCO SYSTEMS

Interface Configuration

Edit

RADIUS (Cisco Airespace)

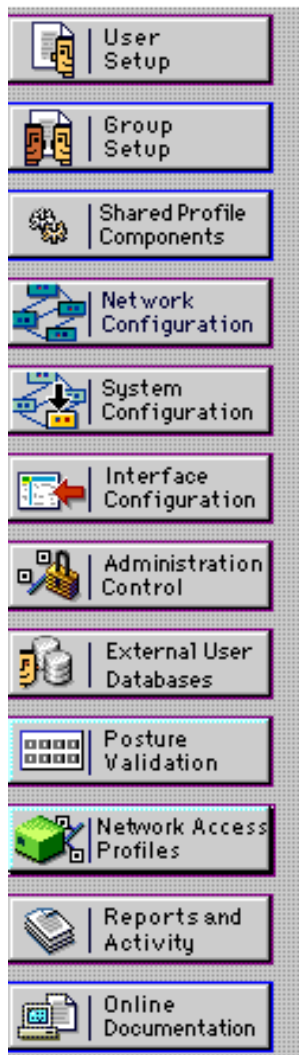
User	Group	Attribute
<input type="checkbox"/>	<input type="checkbox"/>	[026/14179/002] Aire-QoS-Level
<input type="checkbox"/>	<input type="checkbox"/>	[026/14179/003] Aire-DSCP
<input type="checkbox"/>	<input type="checkbox"/>	[026/14179/004] Aire-802.1P-Tag
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[026/14179/005] Aire-Interface-Name
<input type="checkbox"/>	<input type="checkbox"/>	[026/14179/006] Aire-Acl-Name

[Back to Help](#)

3. Accédez à la page Edit de l'utilisateur user1.
4. Dans la page User Edit, faites défiler la section **Cisco Airespace RADIUS Attributes** vers le bas. Activez la case à cocher situées à côté de l'attribut **Aire-Interface-Name** et spécifiez le nom de l'interface dynamique à affecter en cas de succès de l'authentification de l'utilisateur. Cet exemple affecte l'utilisateur au VLAN **admin**



User Setup



Date exceeds:

May 24 2009

Failed attempts exceed:

5

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

Downloadable ACLs

Assign IP ACL:

VPN_Access

Cisco Airespace RADIUS Attributes

[14179\005] Aire-Interface-Name

admin

5. Cliquez sur **Submit**.

[Configurer la commutation pour plusieurs VLAN](#)

Pour autoriser plusieurs VLAN à travers le commutateur, vous devez émettre ces commandes afin de configurer le port de commutation connecté au contrôleur :

1. Switch(config-if)#switchport mode trunk
2. Switch(config-if)#switchport trunk encapsulation dot1q

Remarque: Par défaut, la plupart des commutateurs autorisent tous les VLAN créés sur ce commutateur à travers le port de jonction.

Ces commandes varient pour un commutateur du système d'exploitation Catalyst (CatOS).

Si un réseau câblé est connecté au commutateur, alors cette même configuration peut être appliquée au port de commutation qui se connecte au réseau câblé. Cela active la communication entre les mêmes VLAN dans le réseau câble et sans fil.

Remarque: Ce document ne parle pas de la communication inter-VLAN. Ce sujet sort du cadre de ce document. Vous devez comprendre que pour le routage inter-VLAN, un commutateur de

couche 3 ou un routeur externe avec les configurations de VLAN et de jonction appropriées est nécessaire. Il existe plusieurs documents qui expliquent la configuration du routage inter-VLAN.

[Configuration WLC](#)

Cette configuration requiert les étapes suivantes :

- [Configurer le WLC avec les détails du serveur d'authentification](#)
- [Configurer les interfaces dynamiques \(VLAN\)](#)
- [Configurer les WLAN \(SSID\)](#)

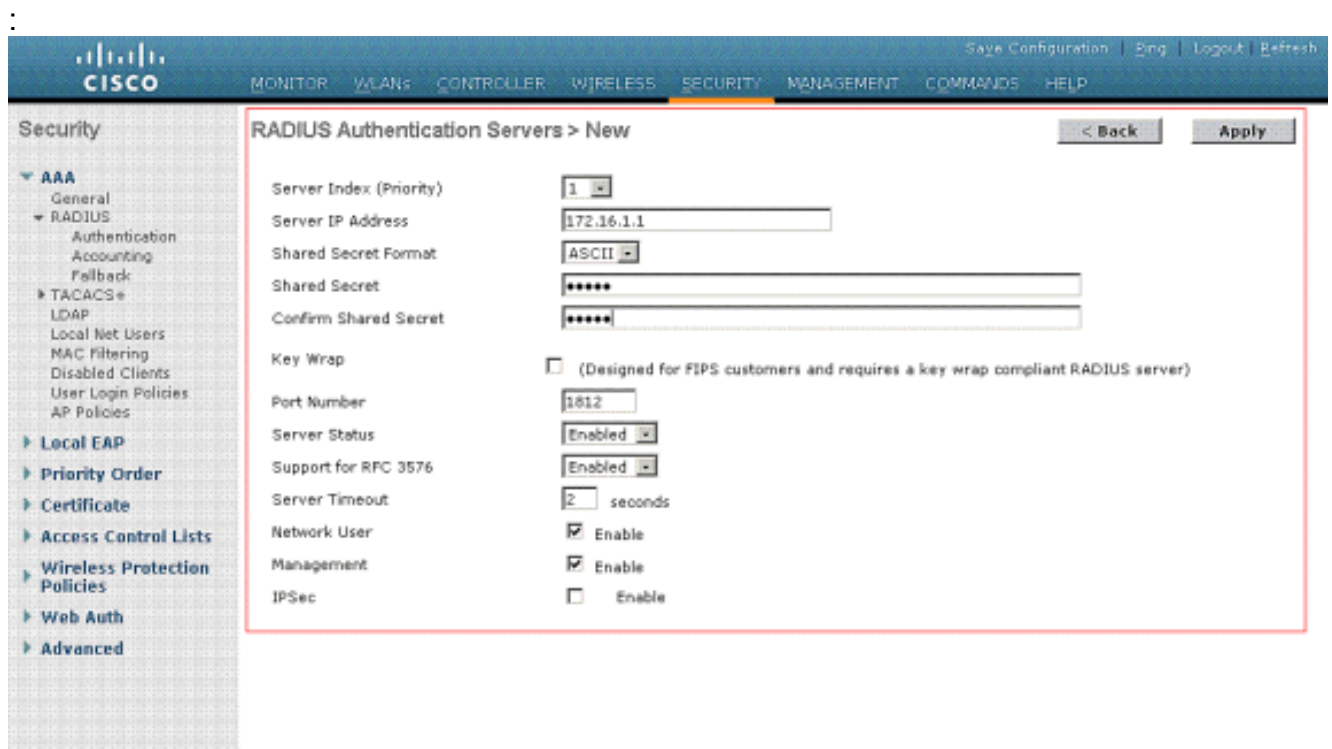
[Configurer le WLC avec les détails du serveur d'authentification](#)

Il est nécessaire de configurer le WLC pour qu'il puisse communiquer avec le serveur RADIUS afin d'authentifier les clients, et également pour toutes les autres transactions.

Procédez comme suit :

1. Dans l'interface graphique du contrôleur, cliquez sur **Security**.
2. Entrez l'adresse IP du serveur RADIUS et la clé Shared Secret utilisée entre le serveur RADIUS et le WLC. Cette clé de secret partagé (Shared Secret) doit être identique à celle qui est configurée dans le serveur RADIUS sous Network Configuration > AAA Clients > Add Entry. Voici un exemple de fenêtre du WLC

:



The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'SECURITY' tab is selected. On the left, a sidebar shows the 'Security' menu with 'AAA' expanded to 'RADIUS'. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

Server Index (Priority)	1
Server IP Address	172.16.1.1
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

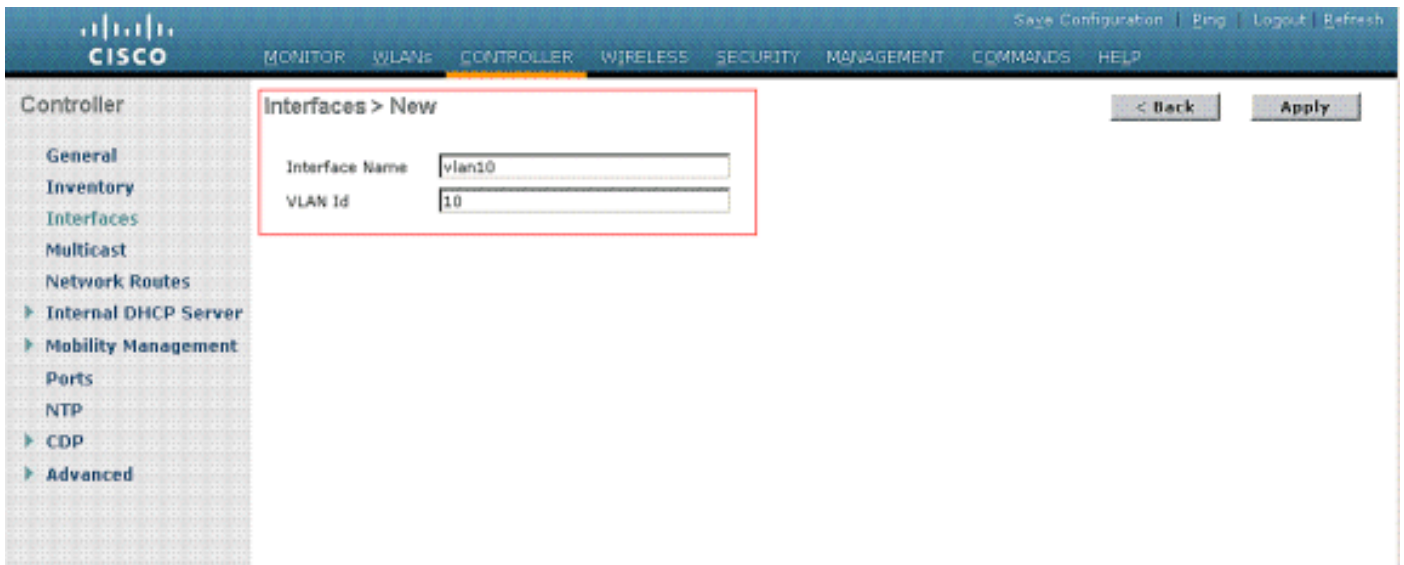
[Configurer les interfaces dynamiques \(VLAN\)](#)

Cette procédure explique comment configurer des interfaces dynamiques sur le WLC. Comme expliqué plus tôt dans ce document, l'ID de VLAN spécifié sous l'attribut Tunnel-Private-Group ID du serveur RADIUS doit également exister dans le WLC.

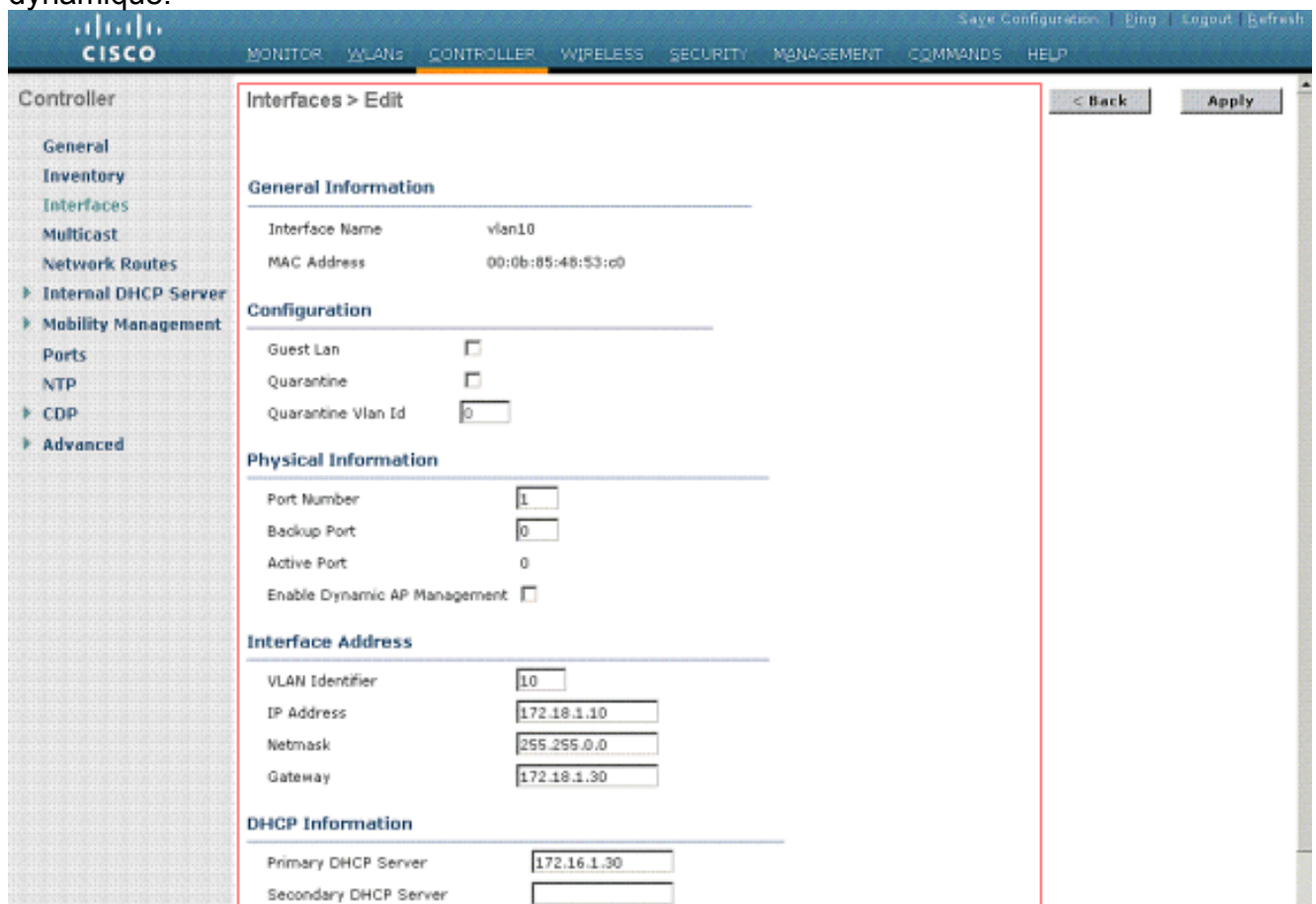
Dans l'exemple, l'utilisateur user1 est spécifié avec l'attribut **Tunnel-Private-Group ID** ayant pour

valeur 10 (VLAN =10) sur le serveur RADIUS. Voyez la section [Attributs RADIUS IETF](#) de la fenêtre User Setup de l'utilisateur user1.

Vous pouvez voir la même interface dynamique (VLAN=10) configurée dans le WLC dans cet exemple. Dans l'interface graphique du contrôleur, sous la fenêtre Controller > Interfaces, l'interface dynamique est configurée.



1. Cliquez sur **Apply** dans cette fenêtre. Cela vous mène à la fenêtre Edit de cette interface dynamique (VLAN 10 ici).
2. Entrez l'adresse IP et la passerelle par défaut de cette interface dynamique.



Remarque: Puisque ce document utilise un serveur DHCP interne sur le contrôleur, la zone du serveur DHCP primaire de cette fenêtre pointe vers l'interface de gestion du WLC. Vous

pouvez également utiliser un serveur DHCP externe, un routeur ou le serveur RADIUS lui-même comme serveur DHCP pour les clients sans fil. Dans ce cas, la zone du serveur DHCP primaire pointe vers l'adresse IP du périphérique utilisé comme serveur DHCP. Référez-vous à la documentation de votre serveur DHCP pour plus d'informations.

3. Cliquez sur **Apply**. Maintenant vous êtes configuré avec une interface dynamique dans votre WLC. De même, vous pouvez configurer plusieurs interfaces dynamiques dans votre WLC. Cependant, rappelez-vous que le même ID de VLAN ID doit également exister dans le serveur RADIUS pour que ce VLAN particulier soit affecté au client.

Configurer les WLAN (SSID)

Cette procédure explique comment configurer les WLAN dans le WLC.

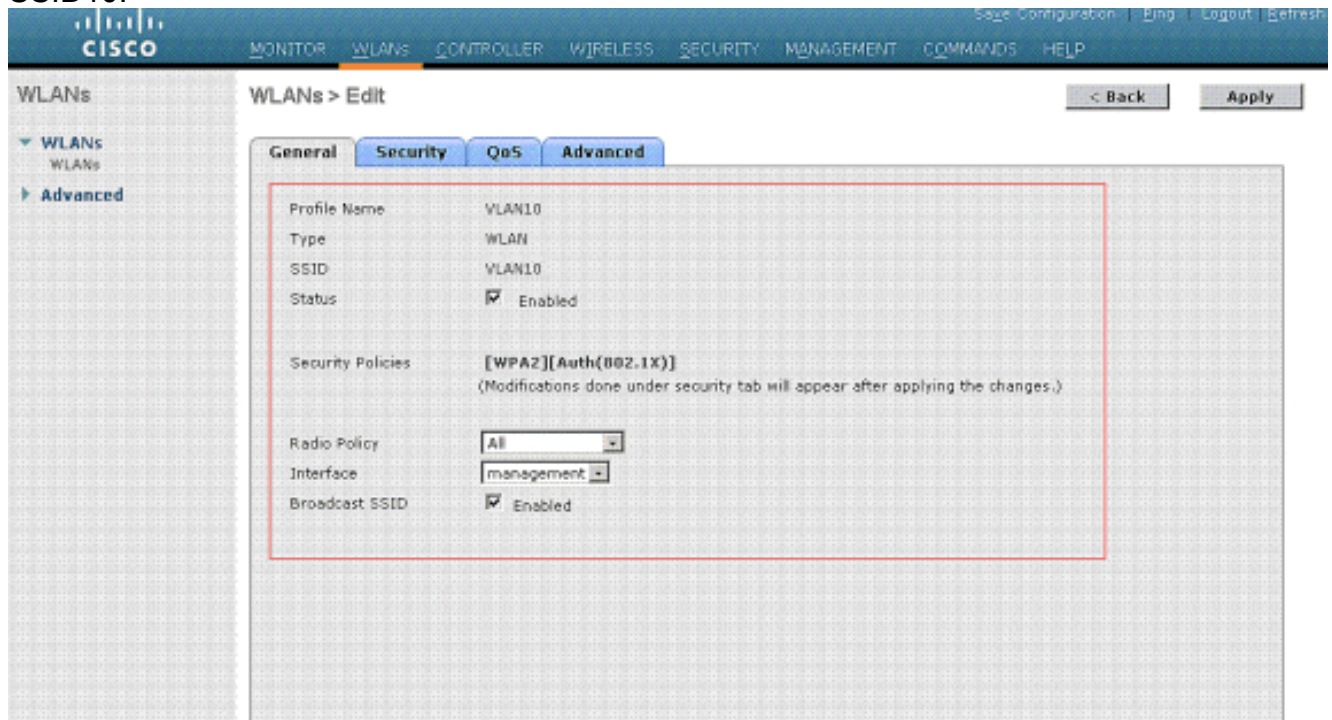
Procédez comme suit :

1. Dans l'interface graphique du contrôleur, choisissez **WLANs > New** pour créer un nouveau WLAN. La fenêtre New WLANs est affichée.
2. Entrez l'ID de WLAN et le SSID du WLAN. Vous pouvez entrer n'importe quel nom en tant que SSID du WLAN. Cet exemple utilise VLAN10 comme SSID du WLAN.

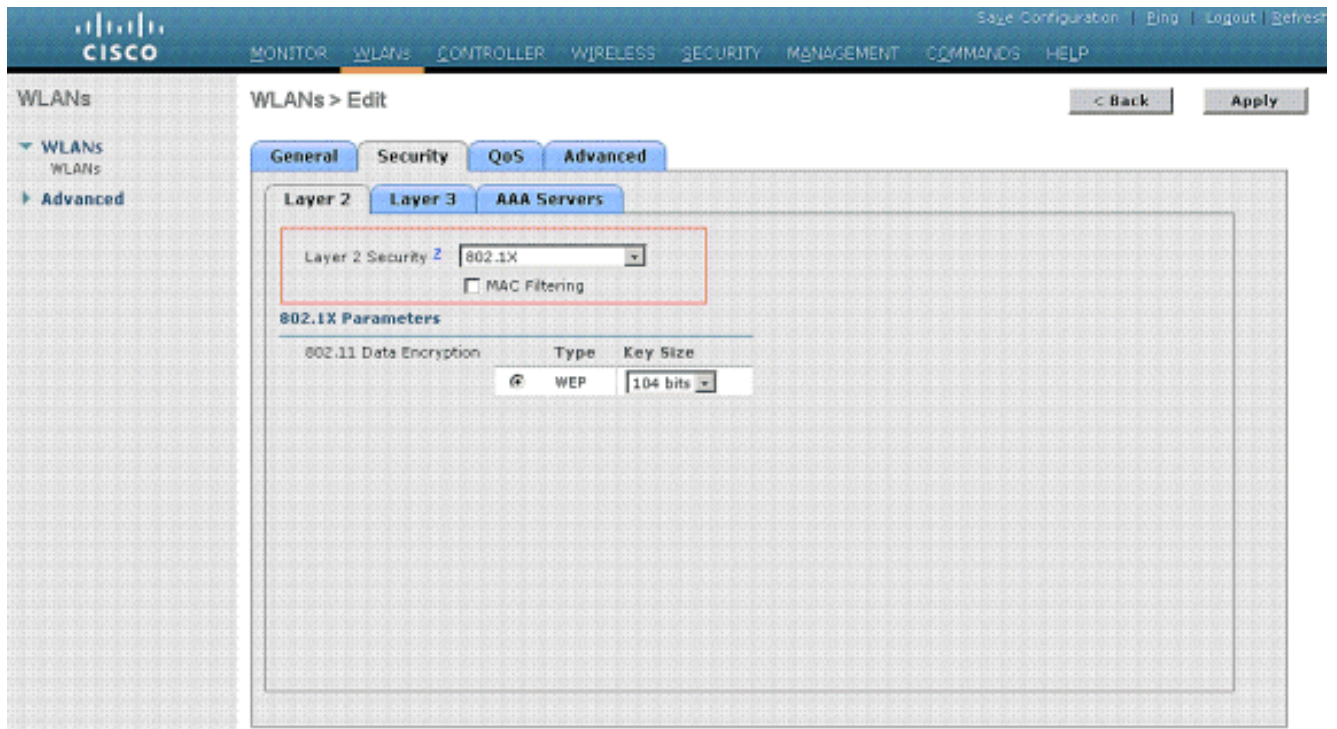


The screenshot shows the 'WLANs > New' configuration page in the Cisco WLC GUI. The page has a blue header with the Cisco logo and navigation tabs: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. On the left, there is a sidebar with 'WLANs' and 'Advanced' options. The main content area is titled 'WLANs > New' and contains a form with the following fields: Type (WLAN), Profile Name (VLAN10), SSID (VLAN10), and ID (3). A red box highlights the form fields. There are '< Back' and 'Apply' buttons at the top right of the form area.

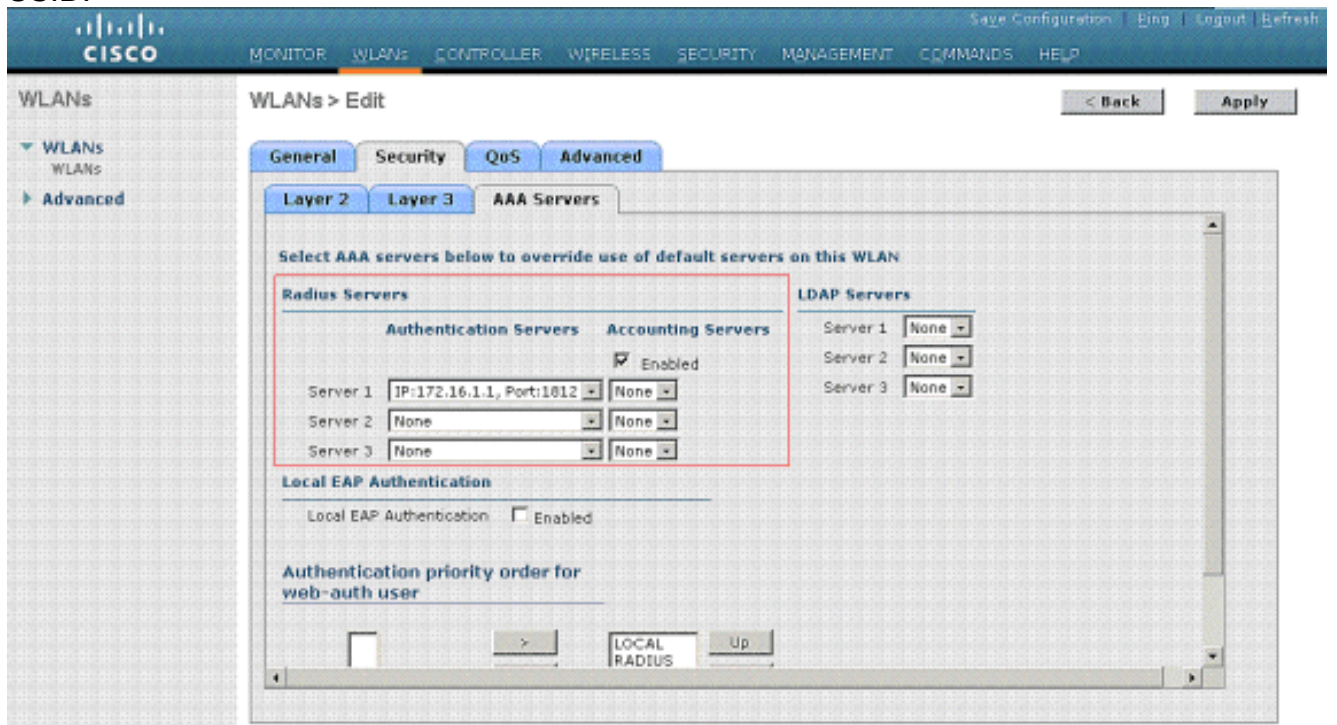
3. Cliquez sur **Apply** afin d'accéder à la fenêtre Edit du WLAN SSID10.



The screenshot shows the 'WLANs > Edit' configuration page in the Cisco WLC GUI. The page has a blue header with the Cisco logo and navigation tabs: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. On the left, there is a sidebar with 'WLANs' and 'Advanced' options. The main content area is titled 'WLANs > Edit' and contains a form with the following fields: Profile Name (VLAN10), Type (WLAN), SSID (VLAN10), Status (Enabled), Security Policies ([WPA2][Auth(802.1X)]), Radio Policy (All), Interface (management), and Broadcast SSID (Enabled). A red box highlights the main configuration area. There are '< Back' and 'Apply' buttons at the top right of the form area.



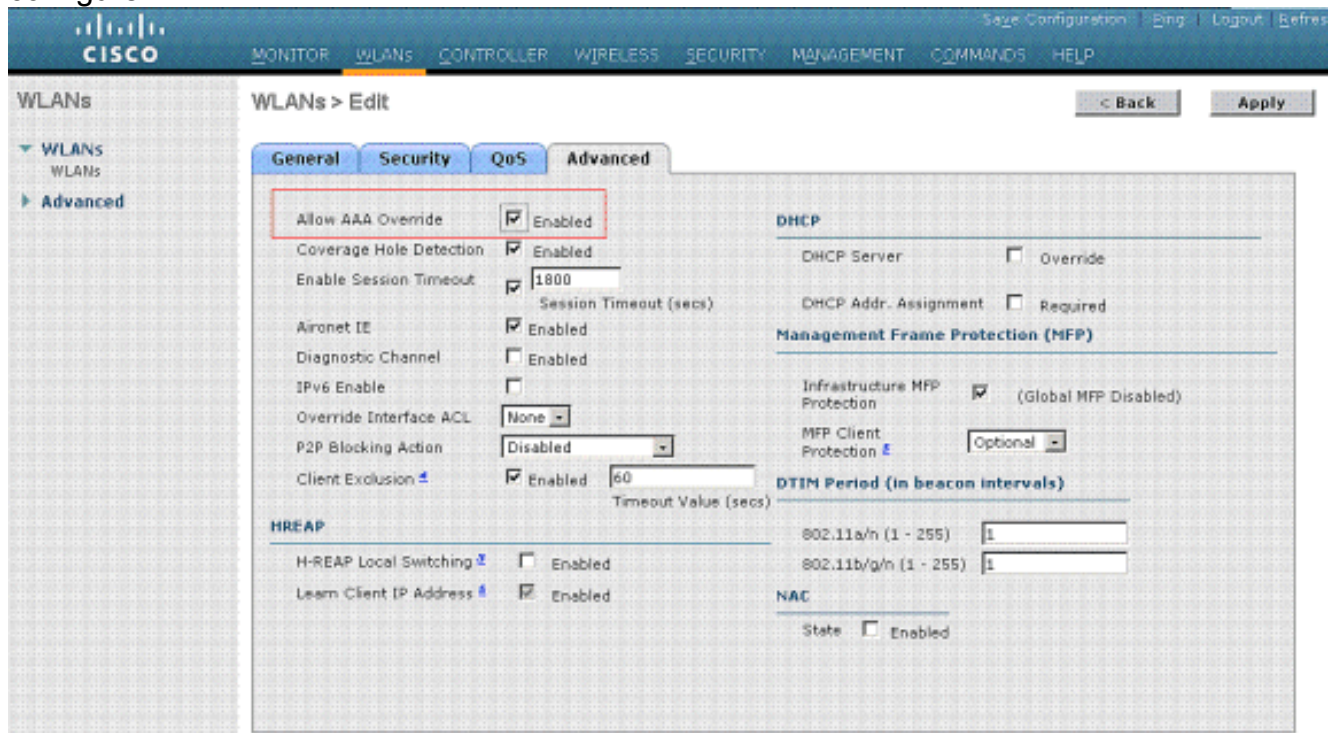
Normalement, dans un contrôleur LAN sans fil, chaque WLAN est mappé à un VLAN (SSID) spécifique de sorte qu'un utilisateur particulier qui appartient à ce WLAN soit placé dans le VLAN spécifique mappé. Ce mappage est normalement effectué sous la zone Interface Name de la fenêtre WLAN SSID.



Dans l'exemple fourni, c'est le travail du serveur RADIUS d'assigner un client sans fil à un VLAN spécifique après une authentification réussie. Les WLAN n'ont pas besoin d'être mappés à une interface dynamique spécifique sur le WLC. Ou, bien que le mappage du WLAN à une interface dynamique soit effectué sur le WLC, le serveur RADIUS ignore ce mappage et affecte l'utilisateur qui arrive à travers ce WLAN au VLAN spécifié sous la zone **Tunnel-Group-Private-ID** de l'utilisateur dans le serveur RADIUS.

4. Activez la case à cocher **Allow AAA Override** pour que le serveur RADIUS substitue les configurations WLC.

5. Activez l'option Allow AAA Override dans le contrôleur pour chaque WLAN (SSID) configuré.



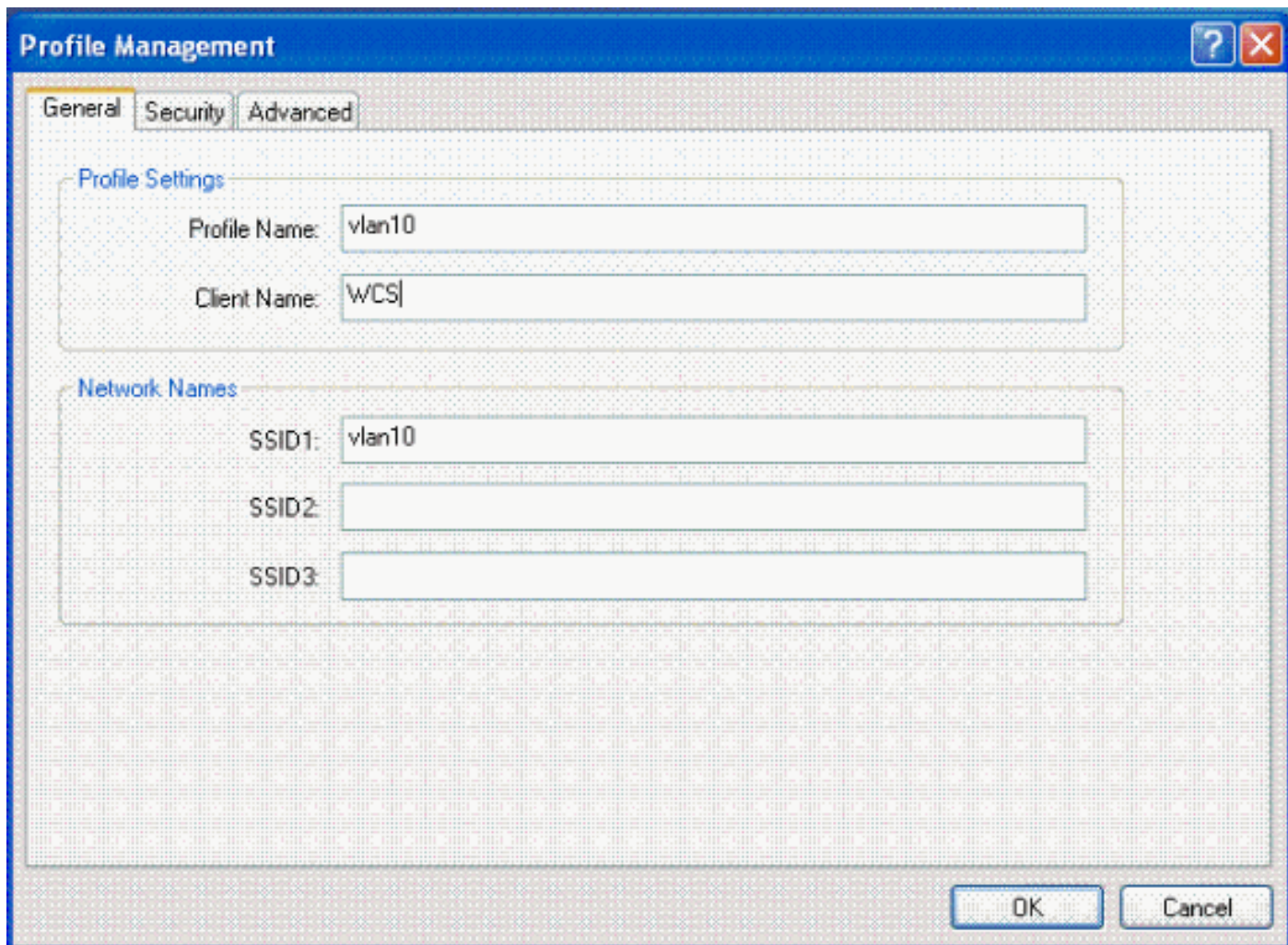
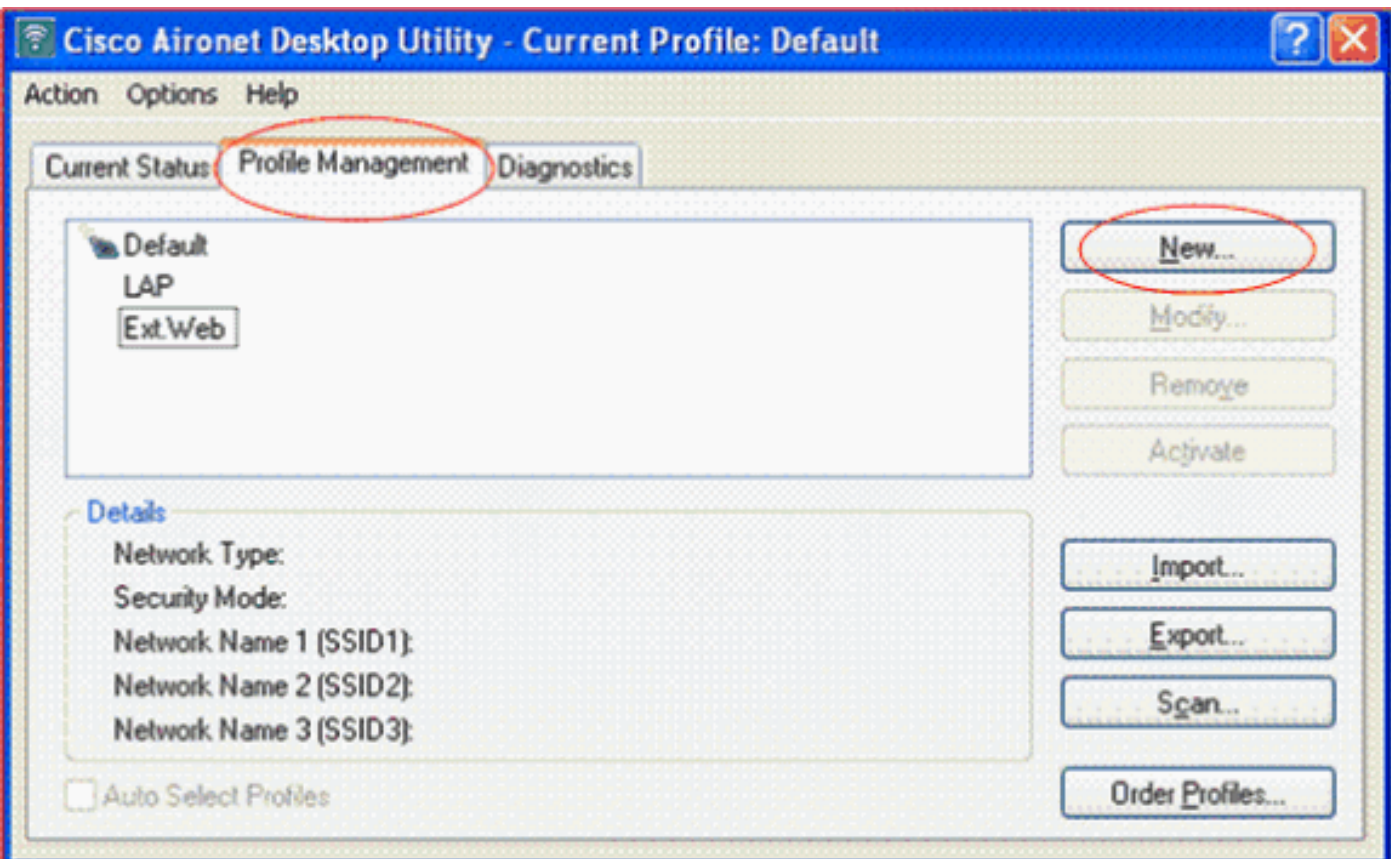
Quand l'option Allow AAA Override est activée, et que les paramètres d'authentification AAA et WLAN du contrôleur sont en conflit, l'authentification du client est exécutée par le serveur AAA (RADIUS). Dans le cadre de cette authentification, le système d'exploitation déplace les clients vers un VLAN retourné par le serveur AAA. Cela est prédéfini dans la configuration de l'interface du contrôleur. Par exemple, si le WLAN d'entreprise utilise principalement une interface de gestion assignée au VLAN 2, et si l'option d'AAA Override retourne une redirection vers VLAN 100, le système d'exploitation redirige toutes les transmissions de client à VLAN 100 même si le port physique auquel VLAN 100 est affecté. Quand l'option AAA Override est désactivée, l'authentification de tous les clients adopte par défaut les valeurs des paramètres d'authentification du contrôleur, et l'authentification est seulement effectuée par le serveur AAA si le WLAN du contrôleur ne contient aucun paramètre d'authentification spécifique au client.

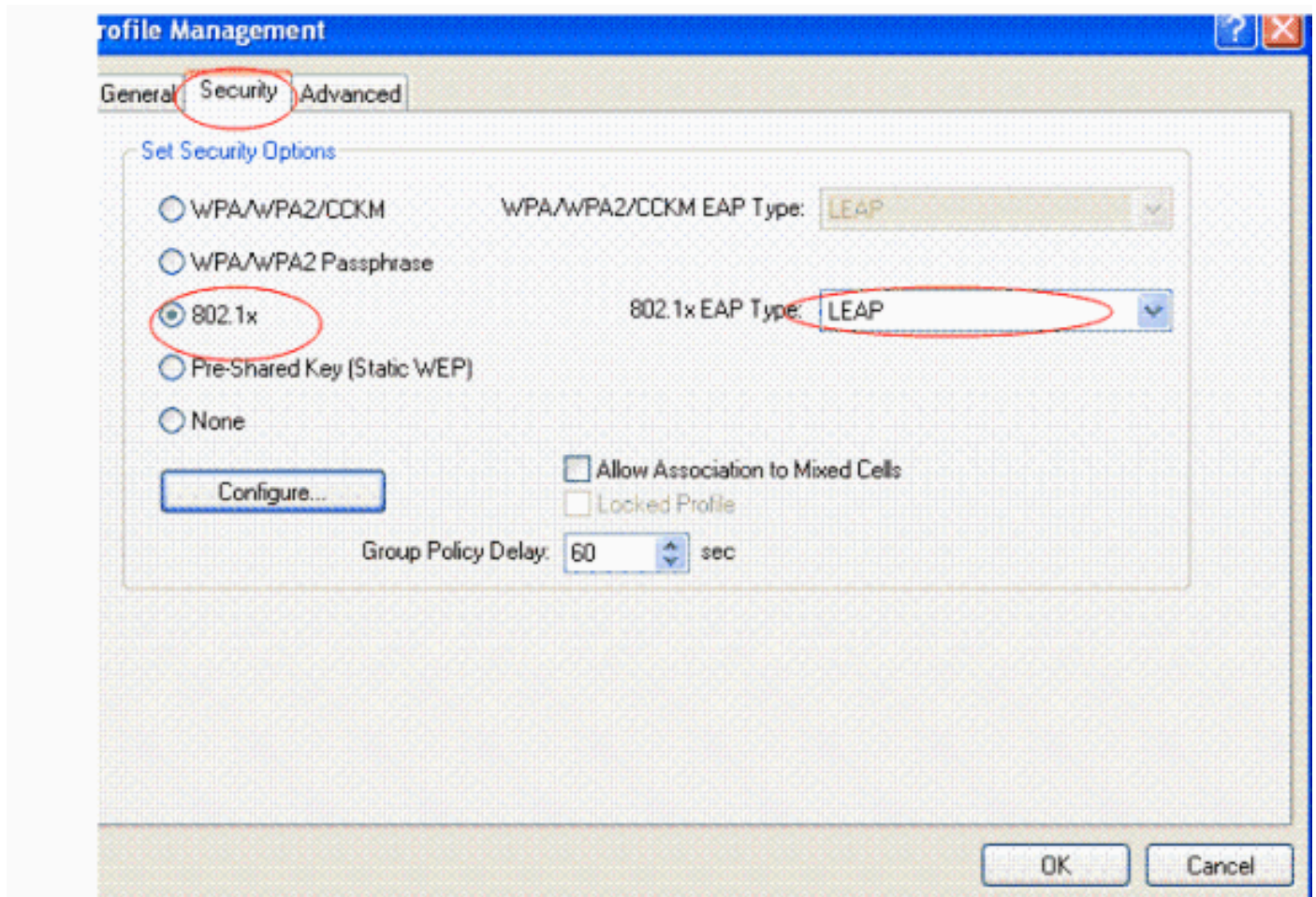
[Configuration de l'utilitaire du client sans fil](#)

Ce document utilise l'ADU comme utilitaire client pour la configuration des profils d'utilisateur. Cette configuration utilise également LEAP comme protocole d'authentification. Configurez l'ADU comme indiqué dans l'exemple de cette section.

Dans la barre de menu de l'ADU, choisissez **Profile Management > New** pour créer un nouveau profil.

Le client de l'exemple est configuré pour faire partie de SSID VLAN10. Ces diagrammes montrent comment configurer un profil d'utilisateur sur un client :





Vérifiez

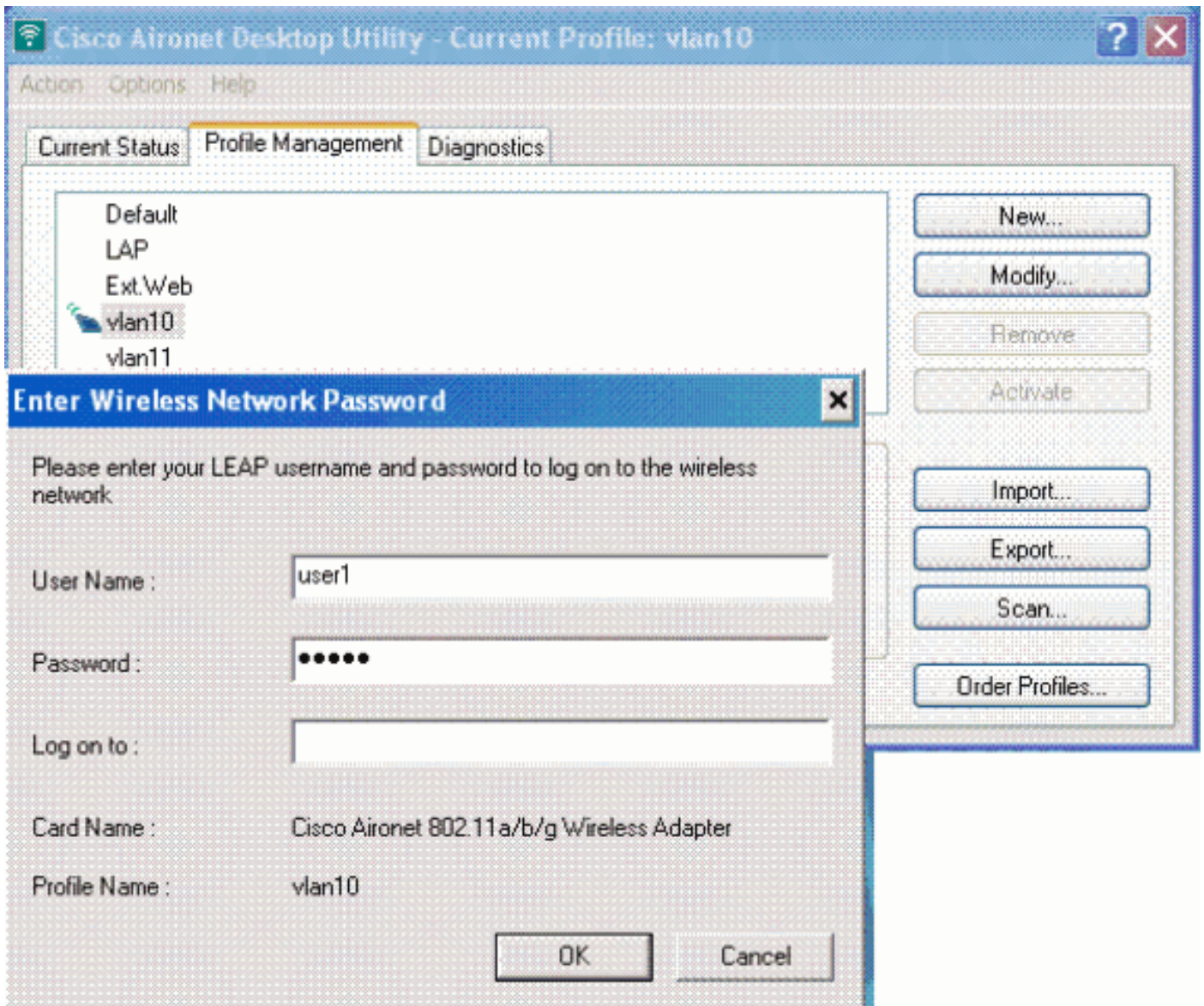
Activez le profil d'utilisateur que vous avez configuré dans l'ADU. En fonction de la configuration, vous êtes invité à entrer un nom d'utilisateur et un mot de passe. Vous pouvez également demander à l'ADU d'utiliser le nom d'utilisateur et le mot de passe Windows pour l'authentification. Il existe un certain nombre d'options à partir desquelles le client peut recevoir l'authentification. Vous pouvez configurer ces options sous l'onglet Security > Configure du profil d'utilisateur que vous avez créé.

Dans l'exemple précédent, notez que l'utilisateur user1 est assigné au VLAN10 comme spécifié dans le serveur RADIUS.

Cet exemple utilise le nom d'utilisateur et le mot de passe du côté client pour recevoir l'authentification et pour être assigné à un VLAN par le serveur RADIUS :

- Nom d'utilisateur = user1
- Mot de passe = user1

Cet exemple montre comment le SSID VLAN10 est invité à indiquer le nom d'utilisateur et le mot de passe. Le nom d'utilisateur et le mot de passe sont entrés dans cet exemple :



Une fois l'authentification et la validation correspondante réussies, vous recevez un message d'état indiquant la réussite.

Puis, vous devez vérifier que votre client est assigné au VLAN approprié conformément aux attributs RADIUS envoyés. Complétez ces étapes afin d'accomplir ceci :

1. Dans l'interface graphique du contrôleur, choisissez **Wireless > AP**.
2. Cliquez sur **Clients**, qui apparaît sur le coin gauche de la fenêtre Access Points (APs). Les statistiques du client sont affichées.

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:21:5c:09:08:dd	AP1130	Unknown	802.11a	Probing	No	2	No
00:21:5c:50:3a:1f	AP1130	VLAN10	802.11g	Associated	Yes	2	No

3. Cliquez sur **Details** afin d'identifier les informations complètes concernant le client, comme l'adresse IP, le VLAN auquel il est assigné, et ainsi de suite. Cet exemple affiche ces détails

concernant le client,
user1 :

The screenshot shows the Cisco AireSpace configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar shows a navigation menu with 'Monitor' selected, and sub-items like 'Summary', 'Access Points', 'Statistics', 'CDP', 'Rogues', 'Clients', and 'Multicast'. The main content area is titled 'Clients > Detail' and contains three sections:

- Client Properties:**
 - MAC Address: 00:21:50:50:3a:1f
 - IP Address: 17.18.1.35
 - Client Type: Regular
 - User Name: User1
 - Port Number: 2
 - Interface: **vlan10** (highlighted with a red box)
 - VLAN ID: 10
 - CCX Version: CCXv4
 - E2E Version: E2Ev1
 - Mobility Role: Local
 - Mobility Peer IP Address: N/A
 - Policy Manager State: RUN
 - Mirror Mode:
 - Management Frame Protection: No
- AP Properties:**
 - AP Address: 00:15:c7:7a:b1:55:90
 - AP Name: AP1130
 - AP Type: 802.11g
 - WLAN Profile: VLAN10
 - Status: Associated
 - Association ID: 1
 - 802.11 Authentication: Open System
 - Reason Code: 0
 - Status Code: 0
 - CF Pollable: Not Implemented
 - CF Poll Request: Not Implemented
 - Short Preamble: Implemented
 - PBCC: Not Implemented
 - Channel Agility: Not Implemented
 - Timeout: 1800
 - WEP State: WEP Disable
- Security Information:**
 - Security Policy Completed: Yes
 - Policy Type: 802.1X
 - Encryption Cipher: WEP (104 bits)
 - EAP Type: LEAP
 - NAC State: Access

Dans cette fenêtre, vous pouvez observer que ce client est assigné à VLAN10 conformément aux attributs RADIUS configurés sur le serveur RADIUS. **Remarque:** Si l'affectation de VLAN dynamique est basée sur la définition de **Cisco Airespace VSA Attribute** , le **nom de l'interface l'affichera comme admin** , comme dans cet exemple, dans la page des détails du client.

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

- **debug aaa events enable** - Cette commande peut être utilisée pour s'assurer du transfert réussi des attributs RADIUS au client par l'intermédiaire du contrôleur. Cette partie de la sortie de débogage assure une transmission réussie des attributs RADIUS :

```

Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
.....J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
.....44 a9 da 6c 36 94 0a f3 <D..l6...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]: attribute 1, vendorId 9,
valueLen 16 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]: attribute 25,
vendorId 0, valueLen 28 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-
Type 16777229 should be 13 for STA 00:40:96:ac:e6:57 Fri Jan 20 02:25:08 2006:
00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222 should be 6 for STA 00:40:96:ac:e6:57 Fri Jan

```

```
20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57 setting dot1x reauth timeout = 1800
```

- Ces commandes peuvent également être utiles :**debug dot1x aaa enabledebug aaa packets enable**

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Remarque: L'affectation dynamique VLAN ne fonctionne pas pour l'authentification Web d'un WLC.

Informations connexes

- [Authentification EAP avec le serveur RADIUS](#)
- [Cisco SAUTENT](#)
- [Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0](#)
- [Support et documentation techniques - Cisco Systems](#)