# Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil

## Contenu



# Introduction

Ce document explique comment Cisco met en application l'authentification Web et affiche comment configurer un contrôleur réseau local de radio de gamme Cisco 4400 (WLAN) (WLC) prendre en charge une authentification de Web interne.

# Conditions préalables

## Conditions requises

Ce document suppose que vous avez déjà une configuration initiale sur les WLC 4400.

## Composants utilisés

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

logiciel suivantes :

- Une gamme 4400 WLC qui exécute la version 7.0.116.0
- La version 4.2 du Cisco Secure Access Control Server (ACS) a installé sur un serveur de Microsoft® Windows 2003
- Point d'accès léger de gamme de Cisco Aironet 1131AG
- Adaptateur sans fil CardBus Cisco Aironet 802.11 a/b/g qui exécute la version 4.0

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.

## Authentification Web

L'authentification Web est une fonctionnalité de sécurité de la couche 3 qui fait ne pas permettre le contrôleur le trafic IP (excepté à paquets liés DHCP et de DN) d'un client particulier jusqu'à ce que ce client ait correctement fourni un nom d'utilisateur valide et un mot de passe. Il s'agit d'une méthode d'authentification simple qui ne requiert aucun utilitaire demandeur ou client. L'authentification Web est généralement utilisée par les clients qui veulent déployer un réseau d'accès invité. En général, les déploiements peuvent inclure des hotspots tels que T-Mobile ou Starbucks.

Gardez présent à l'esprit que l'authentification Web ne fournit pas le chiffrement des données. L'authentification Web est généralement utilisée en tant qu'accès invité simple pour un hotspot ou une atmosphère de campus où la seule préoccupation est la connectivité.

L'authentification Web peut être exécutée utilisant :

- Fenêtre de connexion par défaut sur le WLC
- Version modifiée de la fenêtre de connexion par défaut sur le WLC
- Une fenêtre de connexion personnalisée que vous configurez sur un web server externe (l'authentification de Web externe)
- Une fenêtre de connexion personnalisée que vous téléchargez au contrôleur

Dans ce document, le contrôleur LAN Sans fil pour l'authentification de Web interne est configuré.

## Procédé d'authentification Web

C'est ce qui se produit quand un utilisateur se connecte à un WLAN configuré pour l'authentification Web :

- L'utilisateur ouvre un navigateur Web et écrit un URL, par exemple, http://www.cisco.com. Le client envoie une demande de DN de cet URL d'obtenir l'IP pour la destination. Le WLC saute la demande de DN au serveur DNS et le serveur DNS répond de retour avec des DN répondent, qui contient l'adresse IP de la destination www.cisco.com. Ceci, consécutivement,

est expédié aux clients sans fil.

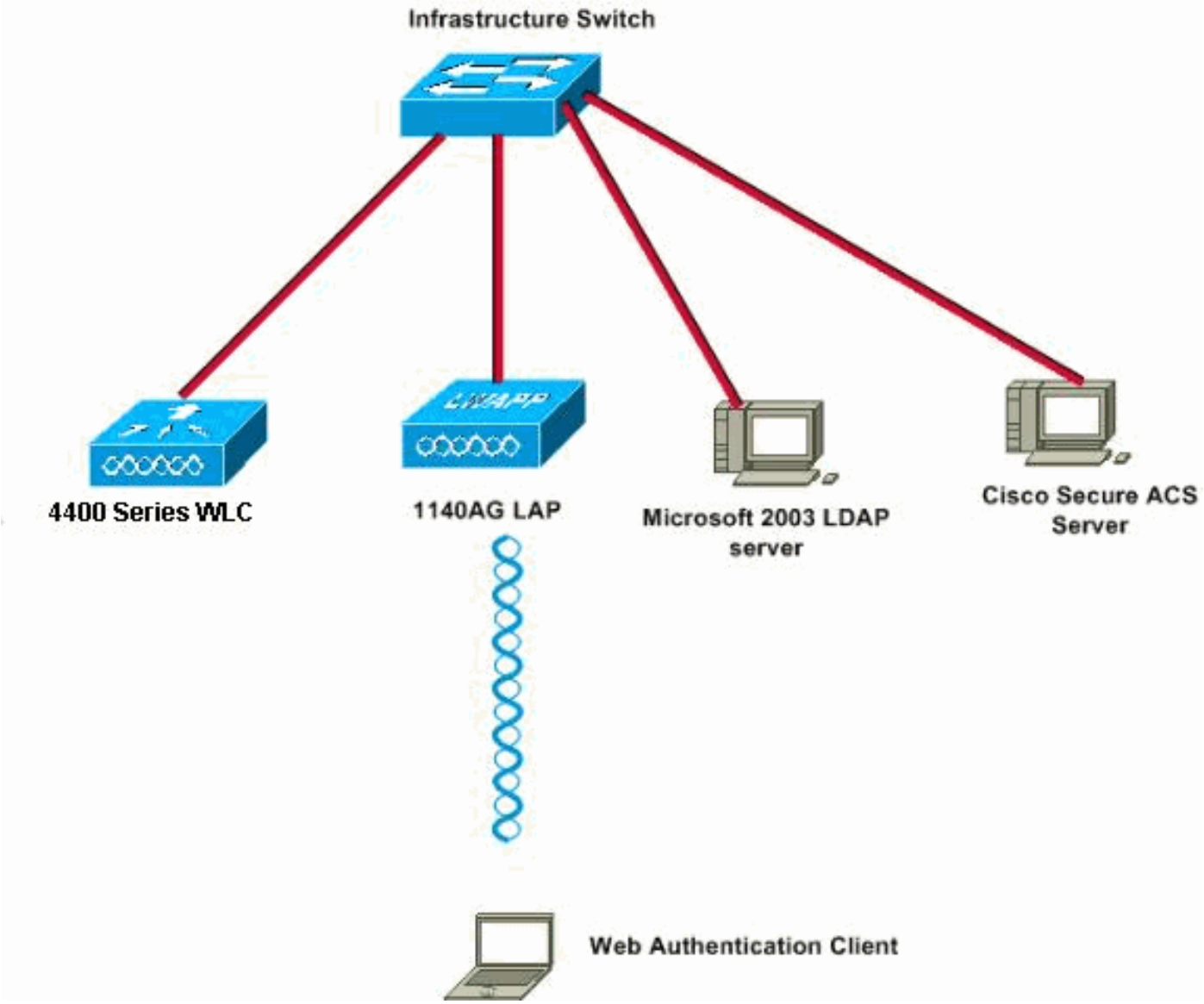
- Les essais de client puis pour ouvrir une connexion TCP avec l'adresse IP de destination. Il envoie un paquet de synchronisation de TCP destiné à l'adresse IP de www.cisco.com.
- Le WLC a des règles configurées pour le client et par conséquent peut agir en tant que proxy pour www.cisco.com. Il renvoie un paquet du TCP SYN-ACK au client avec la source comme adresse IP de www.cisco.com. Le client renvoie un paquet du TCP ACK afin de se terminer la prise de contact à trois voies de TCP et la connexion TCP est entièrement établie.
- Le client envoie un HTTP OBTIENNENT le paquet destiné à www.cisco.com. Le WLC intercepte ce paquet et l'envoie pour la manipulation de redirection. La passerelle d'application de HTTP prépare un corps HTML et le renvoie comme réponse au HTTP GET demandé par le client. Ce HTML incite le client à aller à l'URL par défaut de page Web du WLC, par exemple, http:// <Virtual-Server-IP>/login.html.
- Le client ferme la connexion TCP avec l'adresse IP, par exemple, www.cisco.com.
- Maintenant le client veut aller à http://1.1.1.1/login.html. Par conséquent, les essais de client pour ouvrir une connexion TCP avec l'adresse IP virtuelle du WLC. Il envoie un paquet de synchronisation de TCP pour 1.1.1.1 au WLC.
- Le WLC répond de retour avec un TCP SYN-ACK et le client renvoie un TCP ACK au WLC afin de se terminer la prise de contact.
- Le client envoie un HTTP OBTIENNENT pour /login.html a destiné à 1.1.1.1 afin de demander pour la page de connexion.
- Cette demande est permise jusqu'au serveur Web du WLC, et le serveur répond de retour avec la page de connexion par défaut. Le client reçoit la page de connexion sur la fenêtre du navigateur où l'utilisateur peut avancer et procédure de connexion.

Voici un lien à un vidéo sur la Communauté de support de Cisco qui explique le procédé d'authentification Web :

Authentification Web sur les contrôleurs LAN Sans fil de Cisco (WLCs)

## Configuration du réseau

Ce document utilise la configuration réseau suivante :




## Configurer le contrôleur pour l'authentification Web

Dans ce document, un WLAN est configuré pour l'authentification Web et mappé à un VLAN dédié. Ce sont les étapes permettant de configurer un WLAN pour l'authentification Web :

- Créer une interface VLAN
- Configurez WLC pour l'authentification de Web interne
- Ajouter une instance WLAN
- Configurer le type d'authentification (trois façons d'authentifier des utilisateurs dans l'authentification Web)

Cette section présente les informations permettant de configurer le contrôleur pour l'authentification Web.

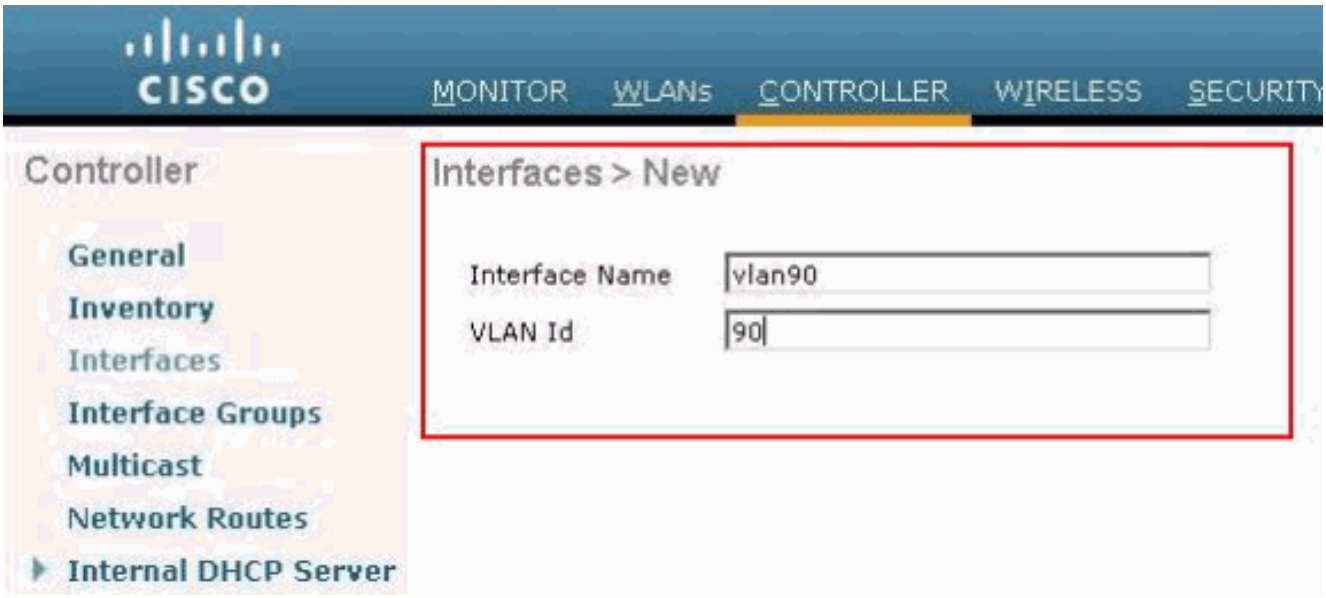
**Ce sont les adresses IP utilisées dans ce document :**

- L'adresse IP du WLC est 10.77.244.204.
- L'adresse IP du serveur ACS est is 10.77.244.196.

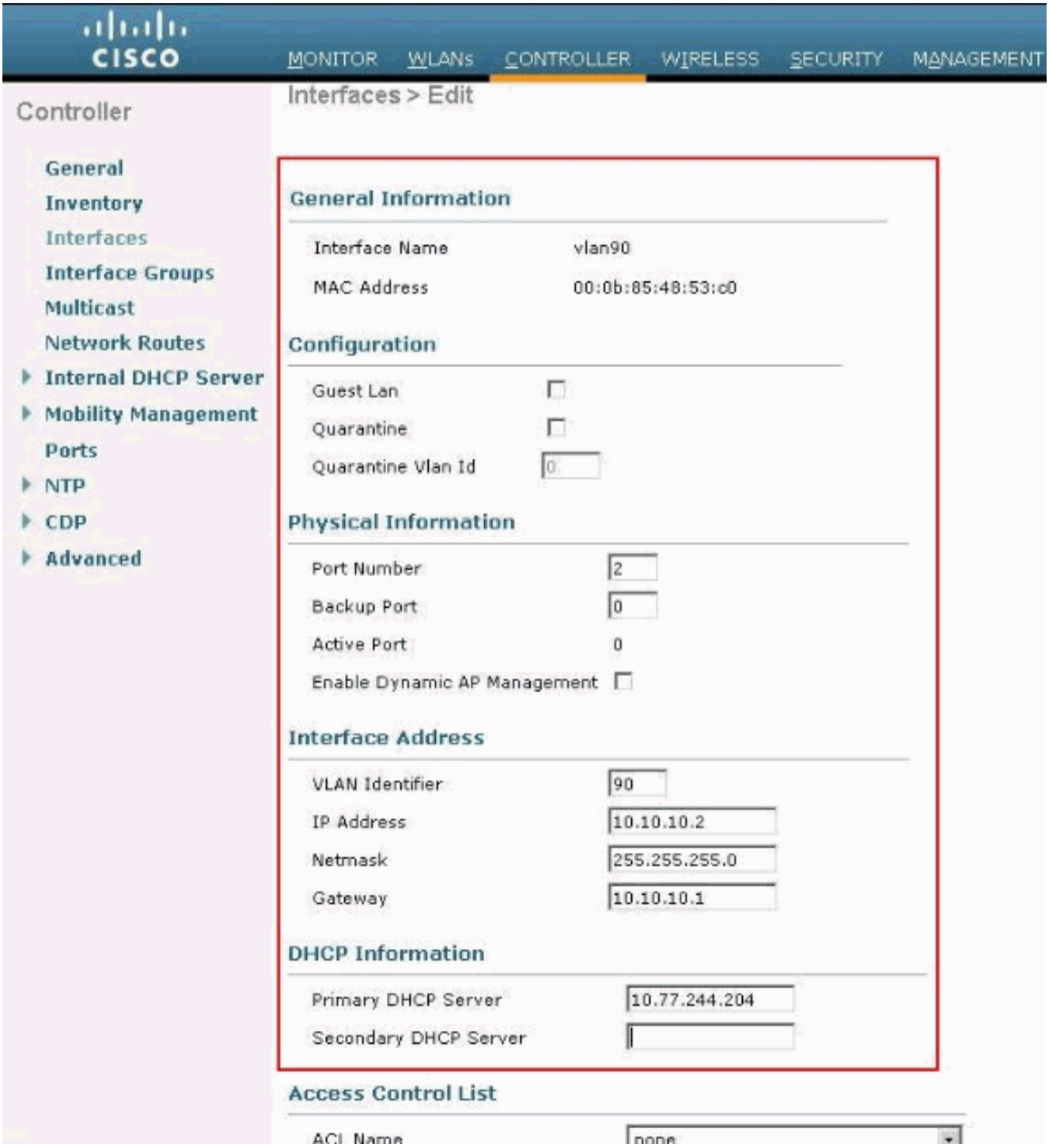
## Créer une interface VLAN

Procédez comme suit :

1. Du GUI Sans fil de contrôleur LAN, choisissez le **contrôleur du** menu au dessus, choisissez les **interfaces du** menu du côté gauche, et cliquez sur New du côté droit supérieur de la fenêtre pour créer une nouvelle interface dynamique.**Les interfaces > nouvelle** fenêtre apparaît. Cet exemple utilise le nom d'interface *vlan90* avec un ID VLAN de *90* :




2. Cliquez sur **Apply** pour créer l'interface VLAN.La fenêtre d'**Interfaces > Edit** apparaît qui te demande de remplir informations de particularité d'interface.
3. Ce document utilise ces paramètres :Adresse IP — 10.10.10.2Masque de réseau - 255.255.255.0 (24 bits)Passerelle — 10.10.10.1Numéro de port — 2Serveur DHCP principal — 10.77.244.204**Note**: Ce paramètre devrait être l'adresse IP de votre serveur RADIUS ou DHCP. Dans cet exemple, l'adresse de gestion du WLC est utilisée comme serveur DHCP parce que la portée DHCP interne est configurée sur le WLC.Serveur DHCP secondaire — 0.0.0.0**Note**: L'exemple n'a pas de serveur DHCP secondaire et utilise donc 0.0.0.0. Si votre configuration a un serveur DHCP secondaire, ajoutez l'adresse IP de celui-ci dans ce champ.Nom de l'ACL Name —
   Aucun



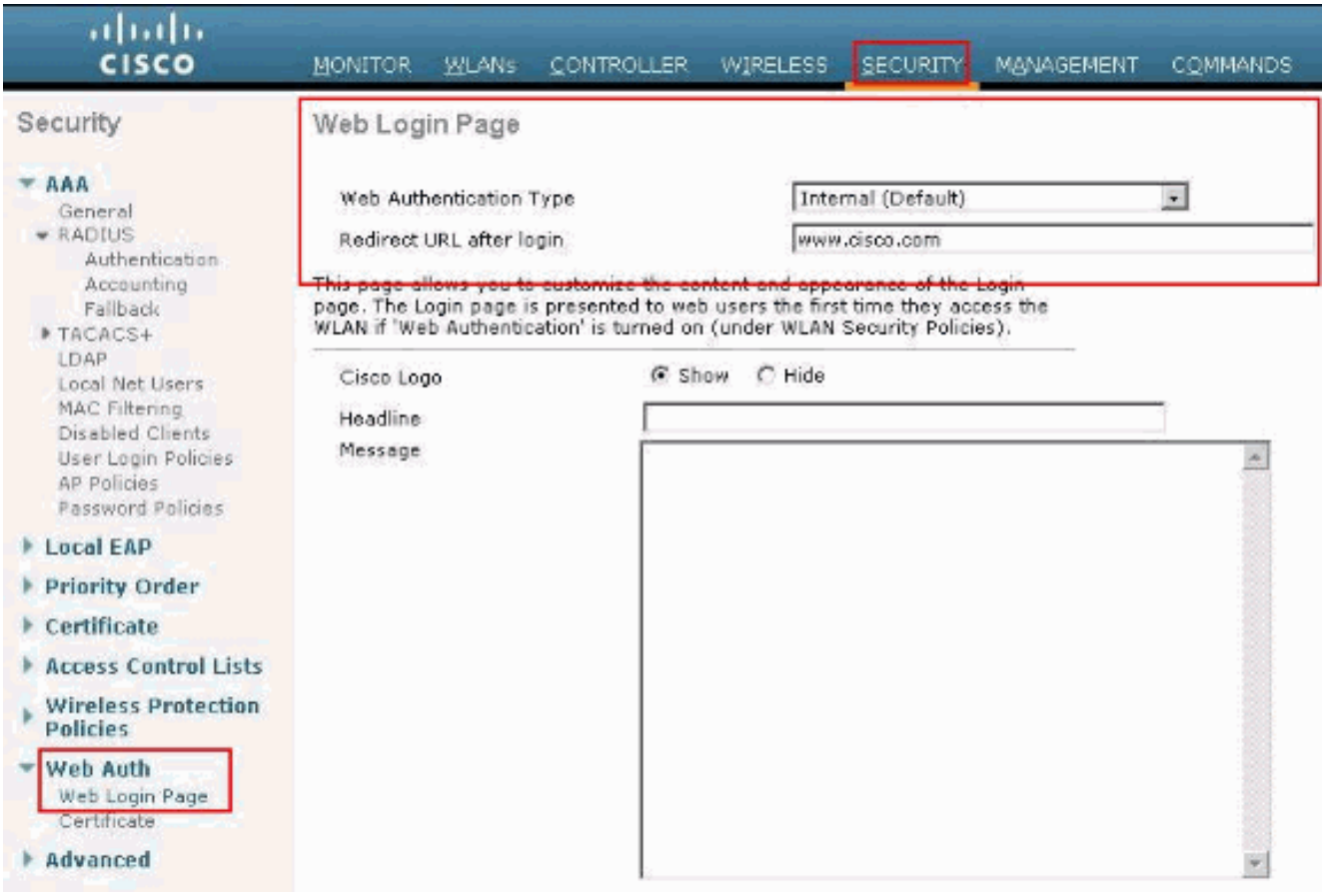

4. Cliquez sur **Apply** afin de sauvegarder les modifications.

## Configurez WLC pour l'authentification de Web interne

L'étape suivante est de configurer le WLC pour l'authentification de Web interne. L'authentification de Web interne est le type d'authentification de web par défaut sur WLCs. Si ce paramètre n'a pas été changé, aucune configuration n'est exigée pour activer l'authentification de Web interne. Si le paramètre d'authentification Web était changé précédemment, terminez-vous ces étapes pour configurer le WLC pour l'authentification de Web interne :

1. Du GUI de contrôleur, choisissez la **Sécurité** > le **Web authentiques** > **page Web Login** afin d'accéder à la page Web Login.
2. De la liste déroulante de type d'authentification Web, choisissez l'**authentification de Web interne**.

3. Dans l'**URL de réorientation après que le** champ de **procédure de connexion**, écrivent l'URL de la page à laquelle l'utilisateur final sera réorienté à après l'authentification réussie.



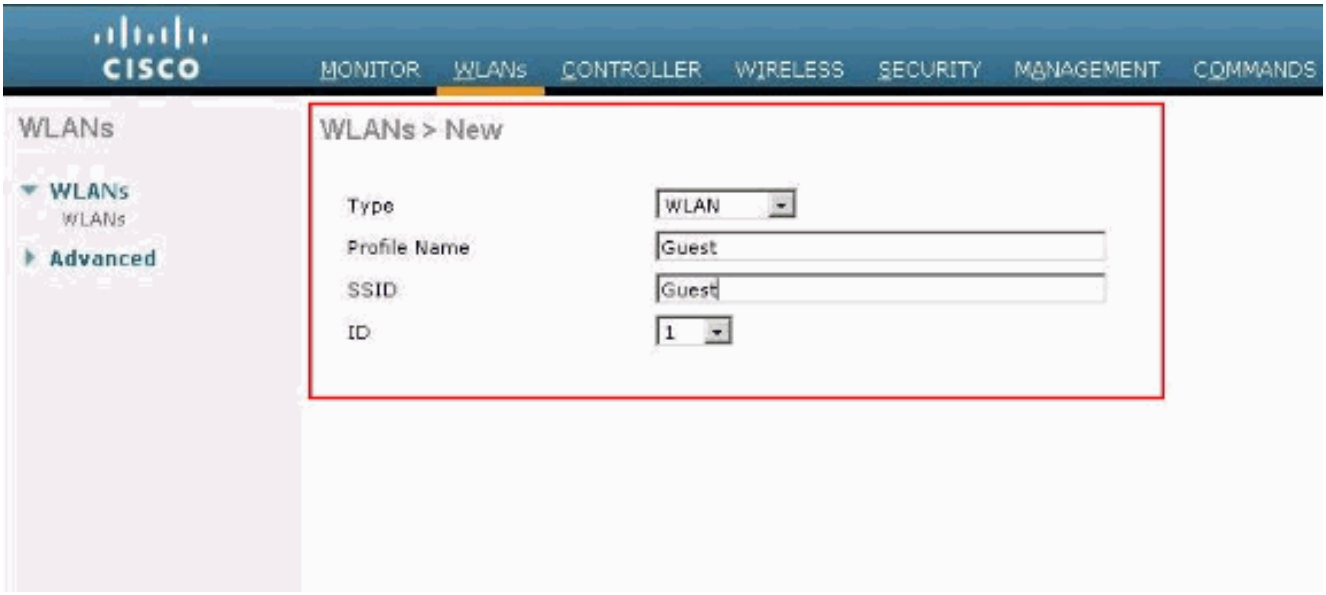

**Note**: Dans des versions 5.0 et ultérieures WLC, la page de déconnexion pour l'authentification Web peut également être personnalisée. Référez-vous à la panne de procédure de connexion, de procédure de connexion d'assigner et aux pages de déconnexion par section WLAN de la *configuration Sans fil Guide,5.2 de contrôleur LAN* pour plus d'informations sur la façon la configurer.

## Ajouter une instance WLAN

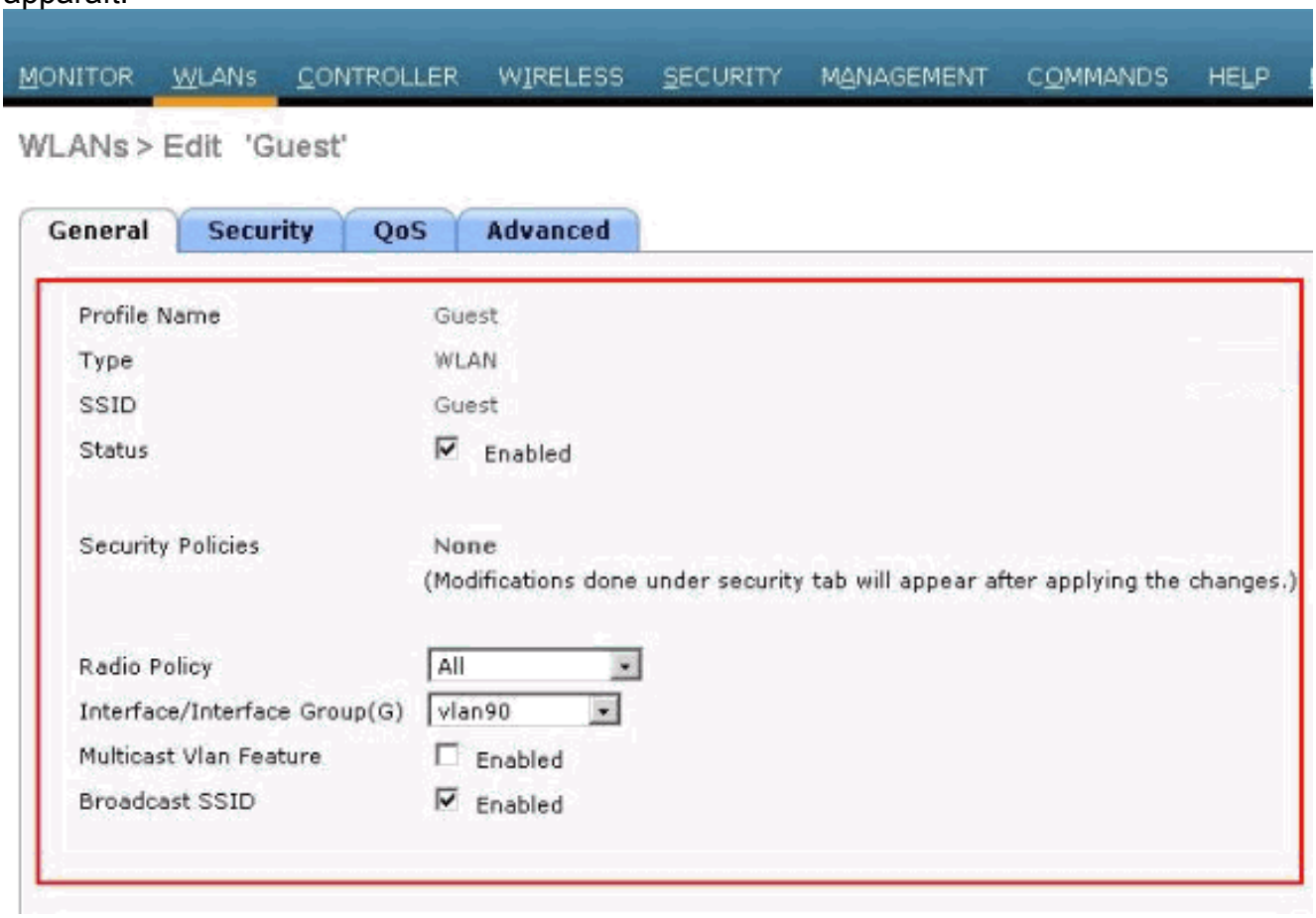
Maintenant que l'authentification de Web interne a été activée et il y a une interface VLAN dédiée pour l'authentification Web, vous devez fournir un nouveau WLAN/SSID afin de prendre en charge les utilisateurs d'authentification Web.

Exécutez les étapes suivantes pour créer un nouveau WLAN/SSID :

1. Du GUI WLC, cliquez sur le **WLAN** dans le menu au dessus, et cliquez sur New en fonction le côté droit supérieur.Choisissez le type **WLAN**. Choisissez un nom de profil et le SSID WLAN pour l'authentification Web. Cet exemple utilise **Guest** comme nom du profil et SSID WLAN.

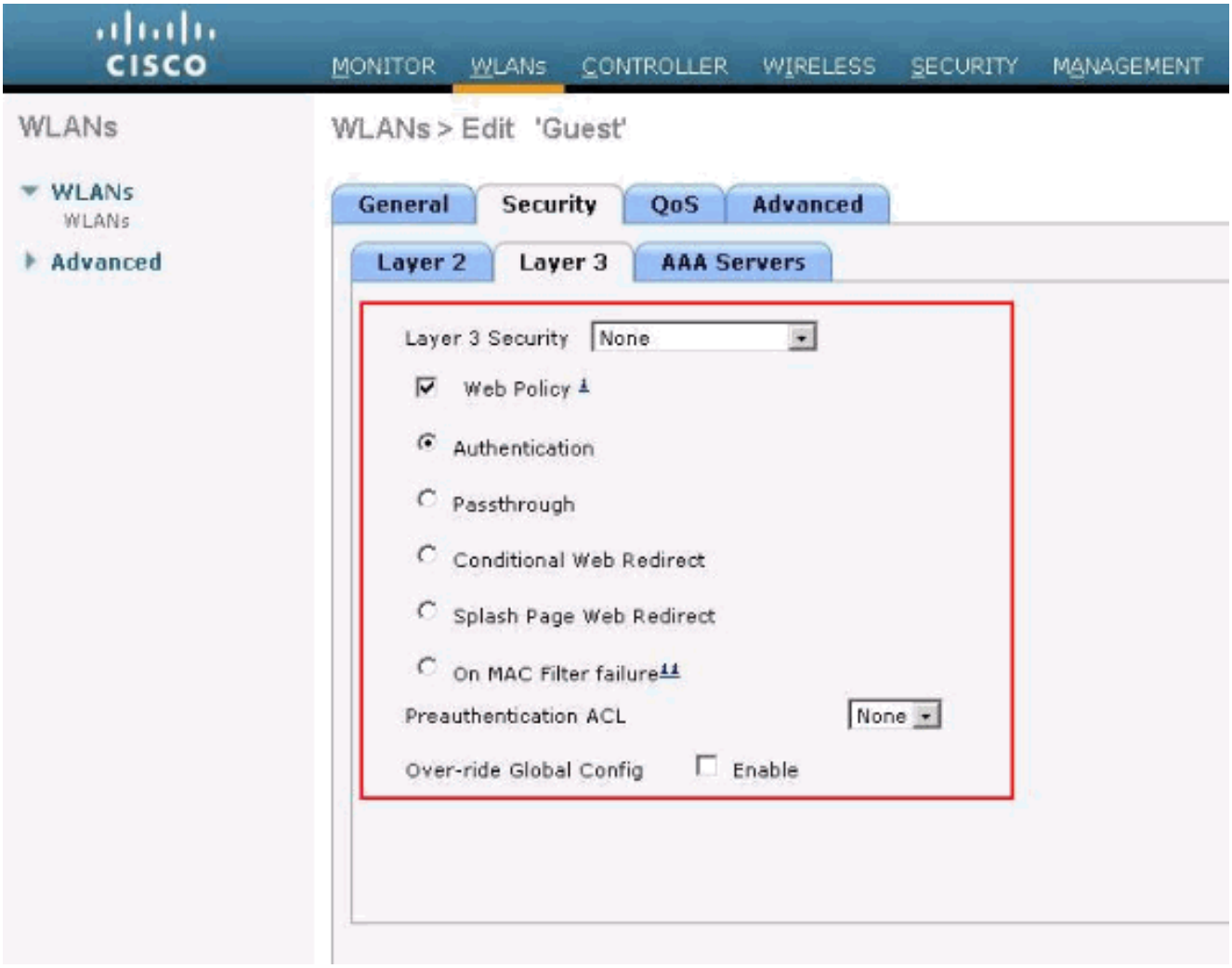



2. Cliquez sur **Apply**.Une nouvelle fenêtre de WLANs > Edit apparaît.




3. Cochez la case d'état du WLAN afin d'activer celui-ci. Dans le menu Interface, sélectionnez le nom de l'interface VLAN que vous avez créée précédemment. Dans cet exemple, le nom de l'interface est *vlan90*.**Note**: Conservez la valeur par défaut des autres paramètres de cet écran.
4. Cliquez sur l'onglet **Security**.Exécutez ces étapes pour configurer l'authentification Web :Cliquez sur l'onglet **Layer 2** et définissez la sécurité sur ***None***.**Note**: Vous ne pouvez pas configurer le transit Web comme sécurité de couche 3 avec 802.1x ou WPA/WPA2 comme sécurité de couche 2 pour un WLAN. Consultez Matrice de compatibilité de la sécurité des couches 2 et 3 pour le contrôleur LAN sans fil pour plus d'informations sur la compatibilité de la sécurité des couches 2 et 3 du contrôleur LAN sans fil.Cliquez sur l'onglet

**Layer 3**. Cochez la case de **stratégie de Web** et choisissez l'option d'***authentification***, comme affiché ici
:




Cliquez sur **Apply** pour sauvegarder le WLAN.Vous revenez à la fenêtre de résumé WLAN. Assurez-vous que Web-Auth est activé sous la colonne Security Policies de la table WLAN pour l'invité SSID.

## Trois façons d'authentifier des utilisateurs dans l'authentification Web

Il y a trois façons d'authentifier des utilisateurs quand vous utilisez l'authentification Web. L'authentification locale permet d'authentifier l'utilisateur dans le WLC Cisco. Vous pouvez également utiliser un serveur RADIUS externe ou un serveur LDAP comme base de données principale afin d'authentifier les utilisateurs.

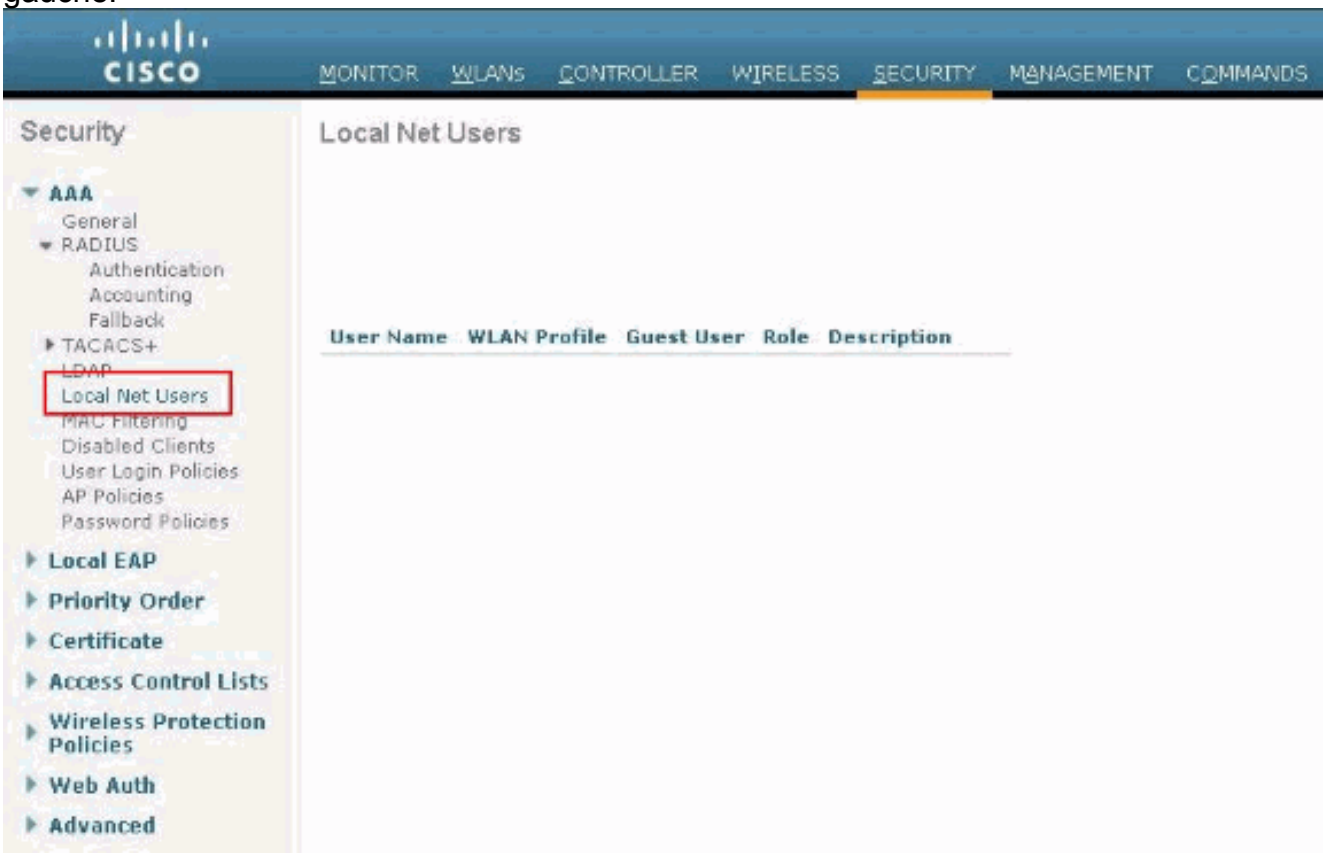
Ce document fournit un exemple de configuration pour chacune des trois méthodes.

### Authentification locale

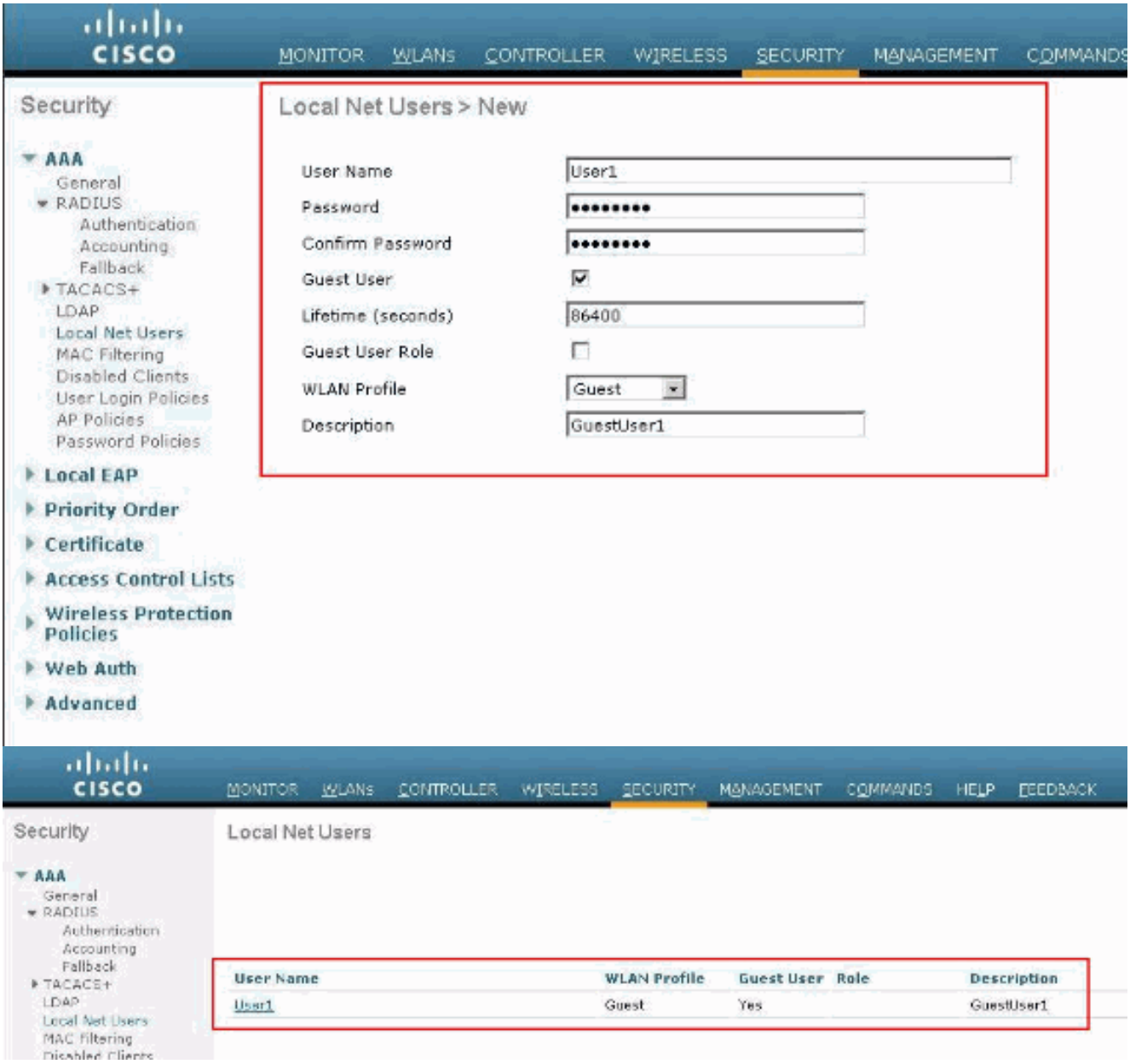
La base de données utilisateur pour les utilisateurs d'invité sont enregistrées sur la base de données locale du WLC. Des utilisateurs sont authentifiés par le WLC contre cette base de données.

1. Du GUI WLC, choisissez la **Sécurité**.
2. Cliquez sur les **utilisateurs du réseau locaux du** menu d'AAA du côté

gauche.




3. Cliquez sur New afin de créer un nouvel utilisateur.D'une nouvelle affichages fenêtre qui demande les informations de nom d'utilisateur et mot de passe.
4. Entrez un nom d'utilisateur et un mot de passe afin de créer un nouvel utilisateur, puis confirmez le mot de passe que vous voulez utiliser.Cet exemple crée l'utilisateur nommé **User1**.
5. Ajoutez une description, le cas échéant.Cet exemple utilise l'**invité User1**.
6. Cliquez sur **Apply** pour sauvegarder la nouvelle configuration utilisateur.




7. Répétez les étapes 3-6 pour ajouter plus d'utilisateurs à la base de données.

## Serveur RADIUS pour l'authentification Web

Ce document utilise un ACS sans fil sur Windows 2003 Server comme serveur RADIUS. Vous pouvez utiliser n'importe quel serveur RADIUS disponible que vous déployez actuellement sur votre réseau.

**Note**: ACS peut être installé sur Windows NT ou Windows 2000 Server. Pour télécharger ACS à partir de Cisco.com, consultez Centre logiciel (téléchargements) - Logiciel sécurisé Cisco (clients enregistrés uniquement). Vous avez besoin d'un compte Web Cisco Web pour télécharger le logiciel.

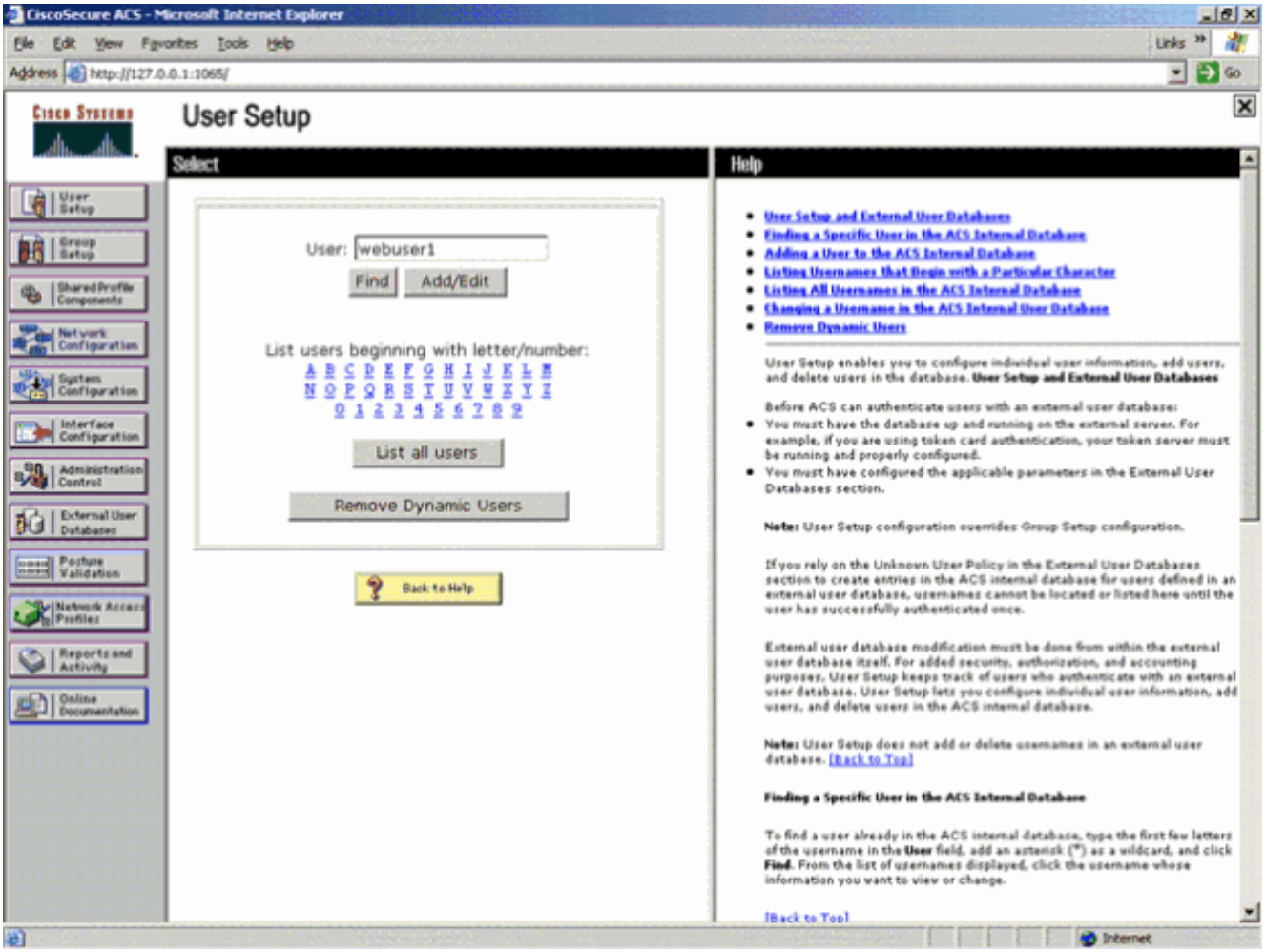
La section Configurer ACS explique comment configurer ACS pour RADIUS. Vous devez avoir un réseau totalement fonctionnel avec un système de noms de domaine (DNS) et un serveur RADIUS.

## Configurer ACS

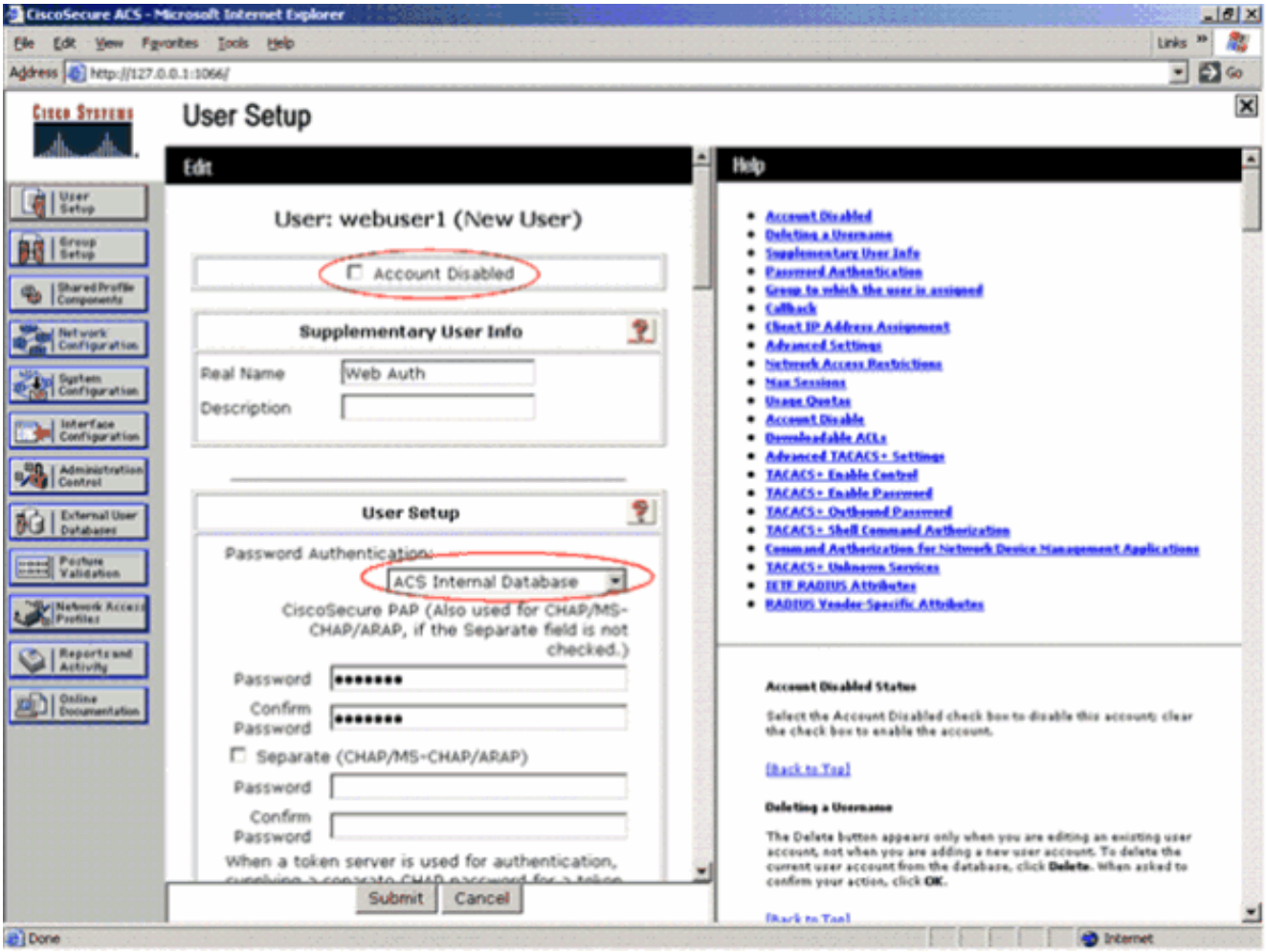
Cette section présente la configuration d'ACS pour RADIUS.

Configurez ACS sur votre serveur, puis effectuez ces étapes afin de créer un utilisateur pour l'authentification :

1. Quand ACS demande si vous voulez ouvrir ACS dans une fenêtre de navigateur pour la configuration, cliquez sur **yes**.**Note**: Une fois que vous avez configuré ACS, vous avez également une icône sur votre bureau.
2. Dans le menu de gauche, cliquez sur **User Setup**.Cette action vous porte à l'écran User Setup comme affiché ici :




3. Entrez l'utilisateur dont vous souhaitez vous servir pour l'authentification Web, puis cliquez sur **Add/Edit**.Après que l'utilisateur soit créé, une deuxième fenêtre s'ouvre comme affiché ici :

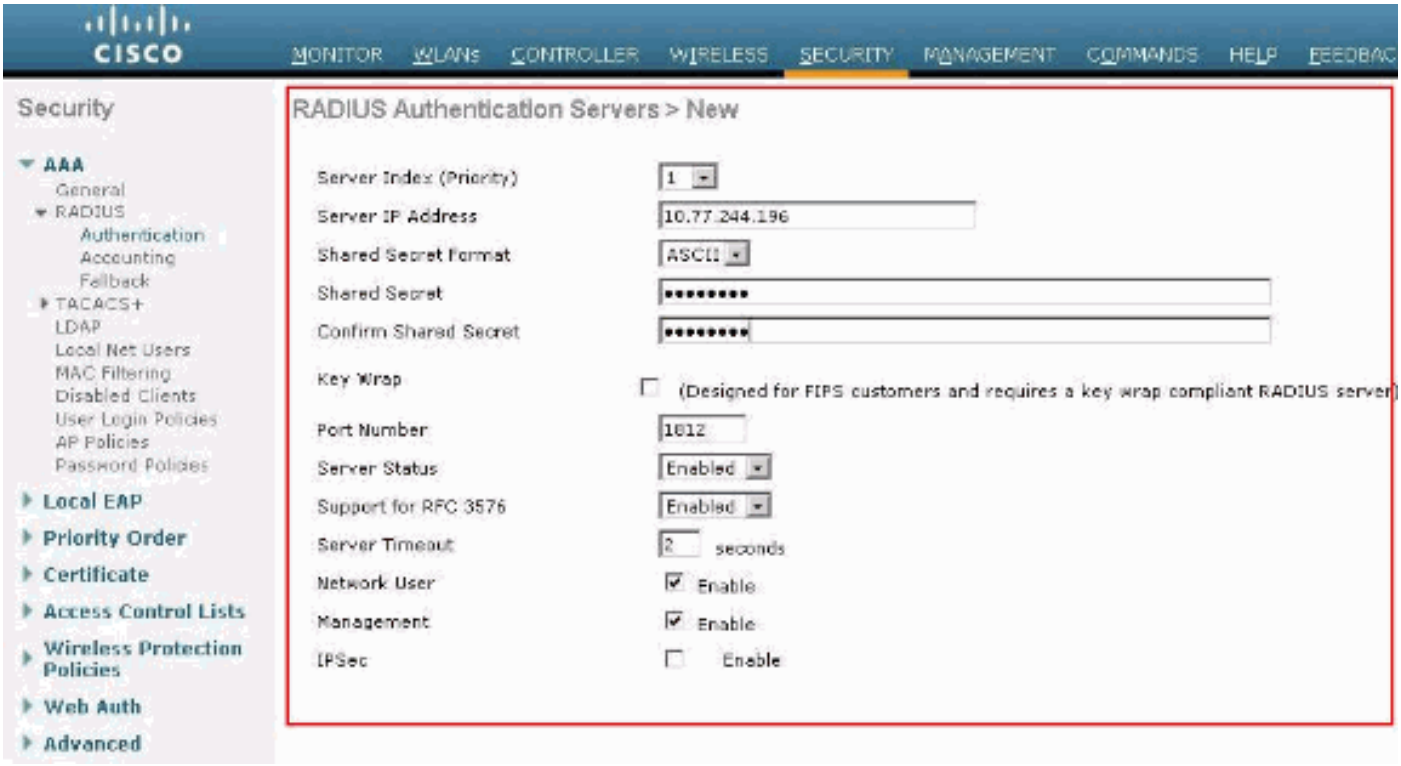



4. Assurez-vous que la **case Account Disabled au** dessus n'est pas cochée.
5. Choisissez **ACS Internal Database** pour l'option Password Authentication.
6. Entrez le mot de passe. L'administrateur dispose d'une option pour configurer l'authentification PAP/CHAP ou MD5-CHAP tout en ajoutant un utilisateur dans la base de données interne ACS. PAP est le type d'authentification par défaut pour les utilisateurs de l'authentification Web sur les contrôleurs. L'administrateur peut remplacer la méthode d'authentification par chap/md5-chap en utilisant cette commande CLI :
   `config custom-web radiusauth <auth method>`
7. Cliquez sur **Submit**.

## Entrer les informations du serveur RADIUS dans le WLC Cisco

Procédez comme suit :

1. Cliquez sur **Security** dans le menu situé en haut.
2. Cliquez sur **RADIUS Authentication** dans le menu de gauche.
3. Cliquez sur **New**, puis entrez l'adresse IP de votre serveur ACS/RADIUS. Dans cet exemple, l'adresse IP du serveur ACS est **10.77.244.196**.
4. Entrez le secret partagé du serveur RADIUS. Assurez-vous que cette clé secrète est identique à celle que vous avez entrée dans le serveur RADIUS pour le WLC.
5. Conservez le numéro de port par défaut, 1812.
6. Assurez-vous que l'option **Server Status** est activée.
7. Cochez la case de **Network User Enable** de sorte que ce serveur de RADIUS soit utilisé pour authentifier des utilisateurs de votre réseau Sans fil.
8. Cliquez sur **Apply**.

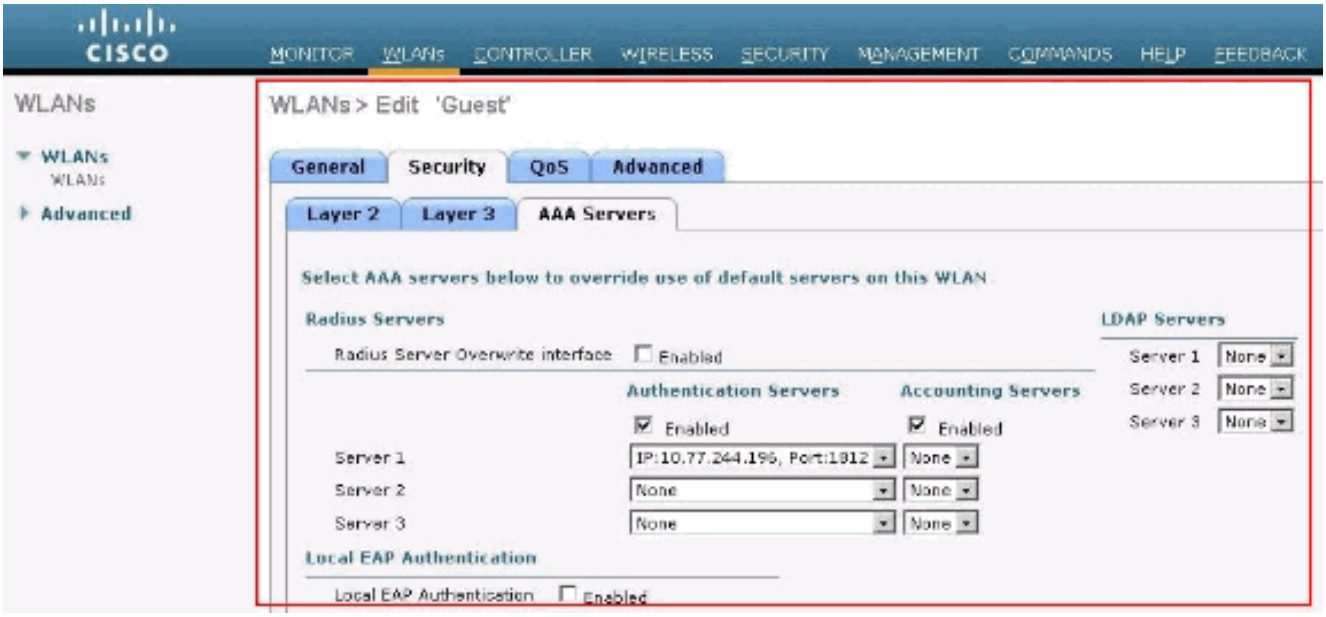



Assurez-vous que la case *Network User* est cochée et que l'option *Admin Status* est activée.


## Configuration du WLAN avec le serveur RADIUS

Maintenant que le serveur RADIUS est configuré sur le WLC, vous devez configurer le WLAN afin d'utiliser ce serveur RADIUS pour l'authentification Web. Effectuez ces étapes afin de configurer le WLAN avec le serveur RADIUS.

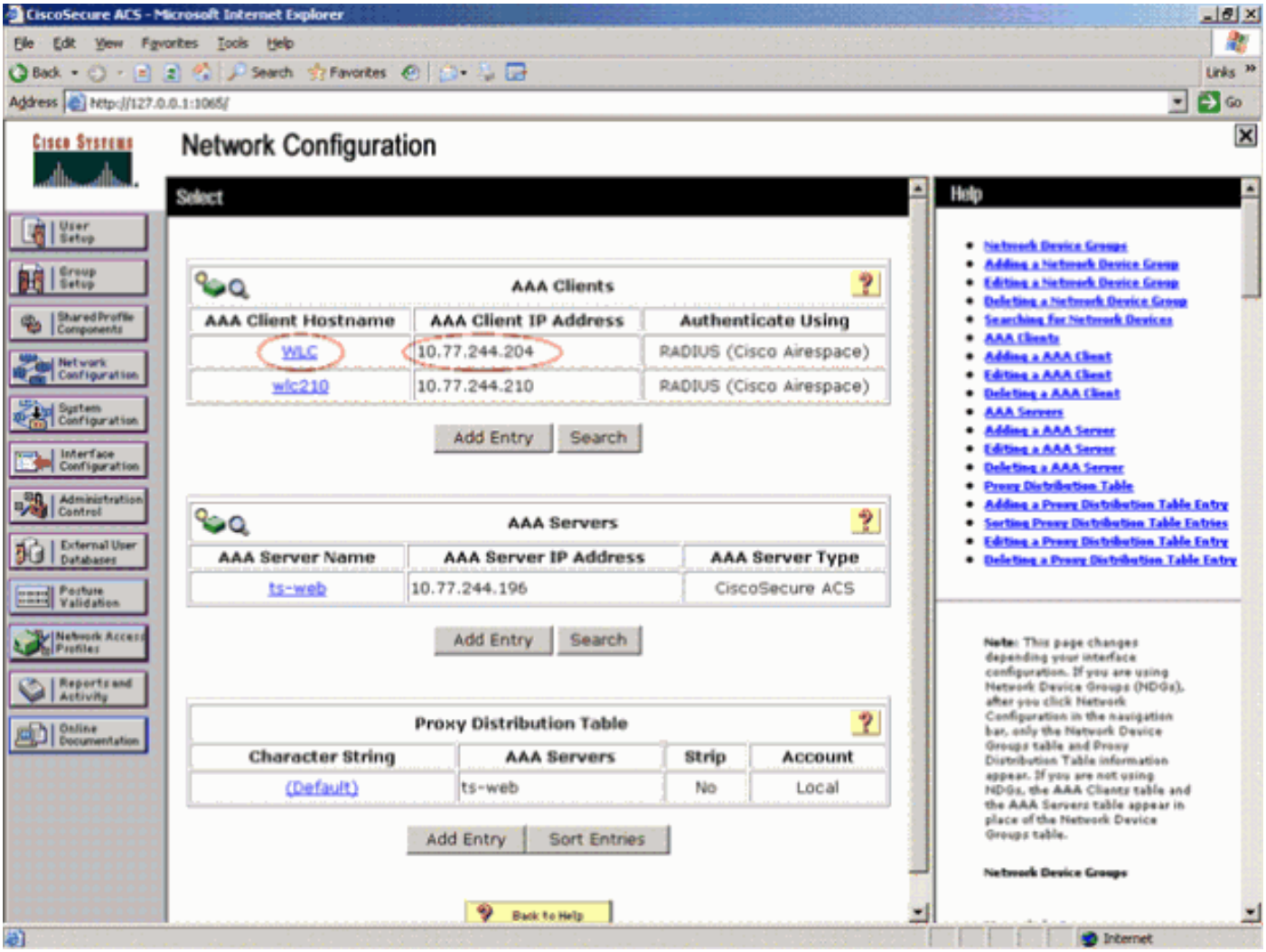
1. Ouvrez votre navigateur WLC et cliquez sur **WLANs**. La liste des WLAN configurés sur le WLC s'affiche alors. Cliquez sur l'**invité** WLAN qui a été créé pour l'authentification Web.
2. Dans la page **WLANs>Edit**, cliquez sur le menu **Security**. Cliquez sur l'onglet **AAA Servers** sous Security. Puis, choisissez le serveur de RADIUS qui est 10.77.244.196 dans cet exemple
   :



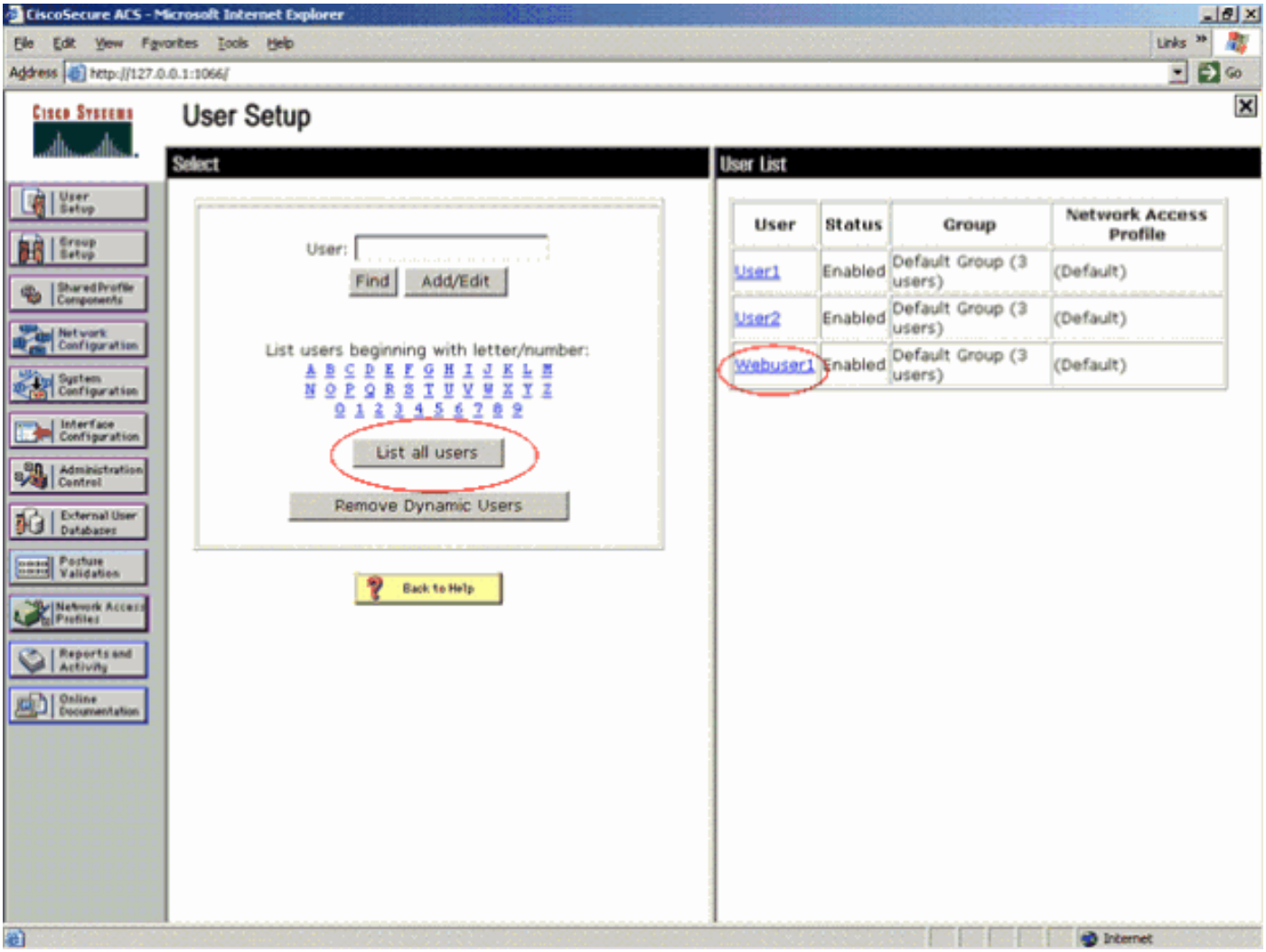

3. Cliquez sur **Apply**.

## Vérifier ACS

Quand vous installez l'ACS, souvenez-vous pour télécharger tous les correctifs en cours et dernier code. Ceci devrait résoudre les prochains problèmes. Au cas où vous utiliseriez l'authentification de RADIUS assurez-vous que votre WLC est répertorié en tant qu'un des clients d'AAA. Cliquez sur le **menu Network Configuration du** côté gauche pour vérifier ceci. Cliquez sur le client AAA, puis vérifiez le mot de passe et le type d'authentification configurés. Consultez la section Configuration des clients AAA du Guide de l'utilisateur de Cisco Secure Access Control Server 4.2 pour plus d'informations sur la configuration d'un client AAA.




Quand vous choisissez User Setup, vérifiez à nouveau que les utilisateurs existent réellement. Cliquez sur **List All Users**. Une fenêtre comme affichée apparaît. Assurez-vous que l'utilisateur qui a été créé existe dans la liste.

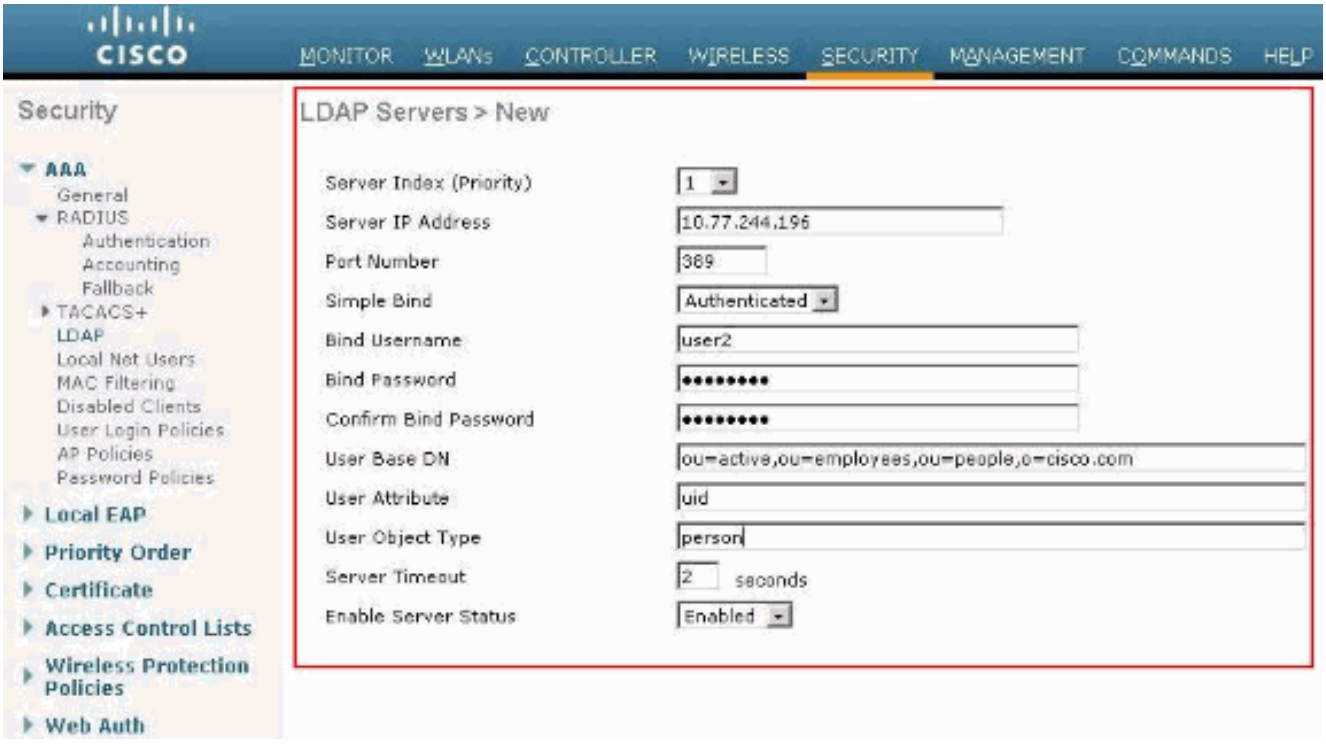



## Serveur LDAP

Cette section explique comment configurer un serveur Protocole d'accès aux annuaires allégé (LDAP) comme base de données principale, semblable à une base de données RADIUS ou des utilisateurs locaux. Une base de données principale LDAP permet au contrôleur de demander à un serveur LDAP les informations d'identification (nom d'utilisateur et mot de passe) d'un utilisateur particulier. Ces informations d'identification sont ensuite utilisées pour authentifier l'utilisateur.

Effectuez ces étapes pour configurer le LDAP en utilisant l'interface graphique du contrôleur :

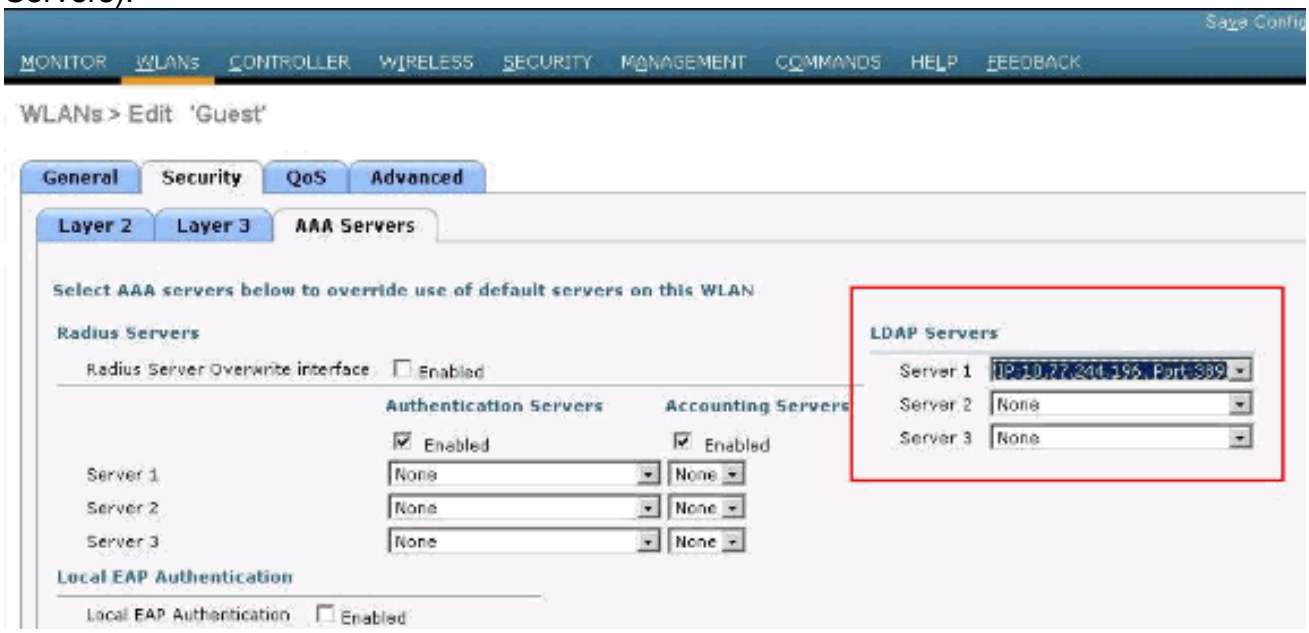
1. Cliquez sur Security > **AAA** > **LDAP** afin d'ouvrir les serveurs LDAP.Cette page dresse une liste de tous les serveurs LDAP qui ont été déjà configurés.Si vous voulez supprimer un serveur LDAP existant, déplacez votre curseur au-dessus de la flèche bleue pour ce serveur et choisissez **Remove**.Si vous voulez vous assurer que le contrôleur peut atteindre un serveur particulier, faites passer votre curseur au-dessus de la flèche bleue de ce serveur et choisissez **Ping**.
2. Effectuez une des opérations suivantes :Pour modifier un serveur LDAP existant, cliquez sur son numéro d'index. La page LDAP Servers > Edit apparaît.Pour ajouter un serveur LDAP, cliquez sur **New**. La page LDAP Servers > New
apparaît.




3. Si vous ajoutez un nouveau serveur, choisissez un numéro dans la zone de liste déroulante Server Index (Priority) pour spécifier la priorité de ce serveur par rapport à tous les autres serveurs LDAP configurés. Vous pouvez configurer jusqu'à dix-sept serveurs. Si le contrôleur ne peut pas atteindre le premier serveur, il essaie le deuxième de la liste et ainsi de suite.
4. Si vous ajoutez un nouveau serveur, entrez l'adresse IP du serveur LDAP dans le champ Server IP Address.
5. Si vous ajoutez un nouveau serveur, entrez le numéro de port TCP du serveur LDAP dans le champ Numéro de port. La plage valide s'étend de 1 à 65535, et la valeur par défaut est 389.
6. Cochez la case **Enable Server Status** pour activer ce serveur LDAP ou décochez-la pour le désactiver. Par défaut, cette option est désactivée.
7. Dans la zone de liste déroulante Simple Bind, choisissez **Anonymous** ou **Authenticated** pour spécifier la méthode de liaison d'authentification locale pour le serveur LDAP. La méthode Anonymous permet l'accès anonyme au serveur LDAP, tandis que la méthode Authenticated requiert la saisie d'un nom d'utilisateur et d'un mot de passe pour sécuriser l'accès. La valeur par défaut est Anonymous.
8. Si vous avez choisi Authenticated au cours de l'étape 7, effectuez les opérations suivantes :Dans le champ Bind Username, entrez le nom d'utilisateur à utiliser pour l'authentification locale auprès du serveur LDAP.Dans les champs Bind Password et Confirm Bind Password, entrez le mot de passe à utiliser pour l'authentification locale auprès du serveur LDAP.
9. Dans le champ User Base DN, entrez le nom distinctif (DN) du sous-arbre dans le serveur LDAP qui contient une liste de tous les utilisateurs. Par exemple, ou=unité organisationnelle, .ou=unité organisationnelle suivante et o=corporation.com. Si l'arborescence contenant les utilisateurs est le DN de la base, entrez o=corporation.com ou dc=corporation de base, dc=com.
10. Dans le champ User Attribute, entrez le nom de l'attribut dans l'enregistrement utilisateur contenant le nom d'utilisateur. Vous pouvez obtenir cet attribut à partir de votre serveur d'annuaire.
11. Dans le champ User Object Type, entrez la valeur de l'attribut LDAP objectType qui identifie l'enregistrement comme utilisateur. Souvent, les enregistrements utilisateur ont plusieurs

valeurs pour l'attribut objectType, certains étant propres à l'utilisateur et certains étant partagés avec d'autres types d'objet.

12. Dans le champ Server Timeout, entrez le nombre de secondes entre les retransmissions. La plage valide s'étend de 2 à 30 secondes, et la valeur par défaut est de 2 secondes.
13. Cliquez sur **Apply** pour valider les modifications.
14. Cliquez sur **Save Configuration** pour sauvegarder les modifications.
15. Terminez-vous ces étapes si vous souhaitez affecter les serveurs LDAP spécifiques à un WLAN :Cliquez sur **WLANs** pour ouvrir la page WLANs.Cliquez sur le numéro d'identification du WLAN souhaité.Lorsque la page WLANs > Edit apparaît, cliquez sur les onglets **Security > AAA Servers** pour ouvrir la page WLANs > Edit (Security > AAA Servers).




Dans les zones de liste déroulante LDAP Servers, choisissez le ou les serveurs LDAP que vous voulez utiliser avec ce WLAN. Vous pouvez choisir jusqu'à trois serveurs LDAP, qui sont essayés par ordre de priorité.Cliquez sur **Apply** pour valider les modifications.Cliquez sur **Save Configuration** pour sauvegarder les modifications.

## Configurez votre client WLAN pour utiliser l'authentification Web

Une fois le WLC configuré, le client doit être configuré de façon appropriée pour l'authentification Web. Cette section présente les informations permettant de configurer votre système Windows pour l'authentification Web.

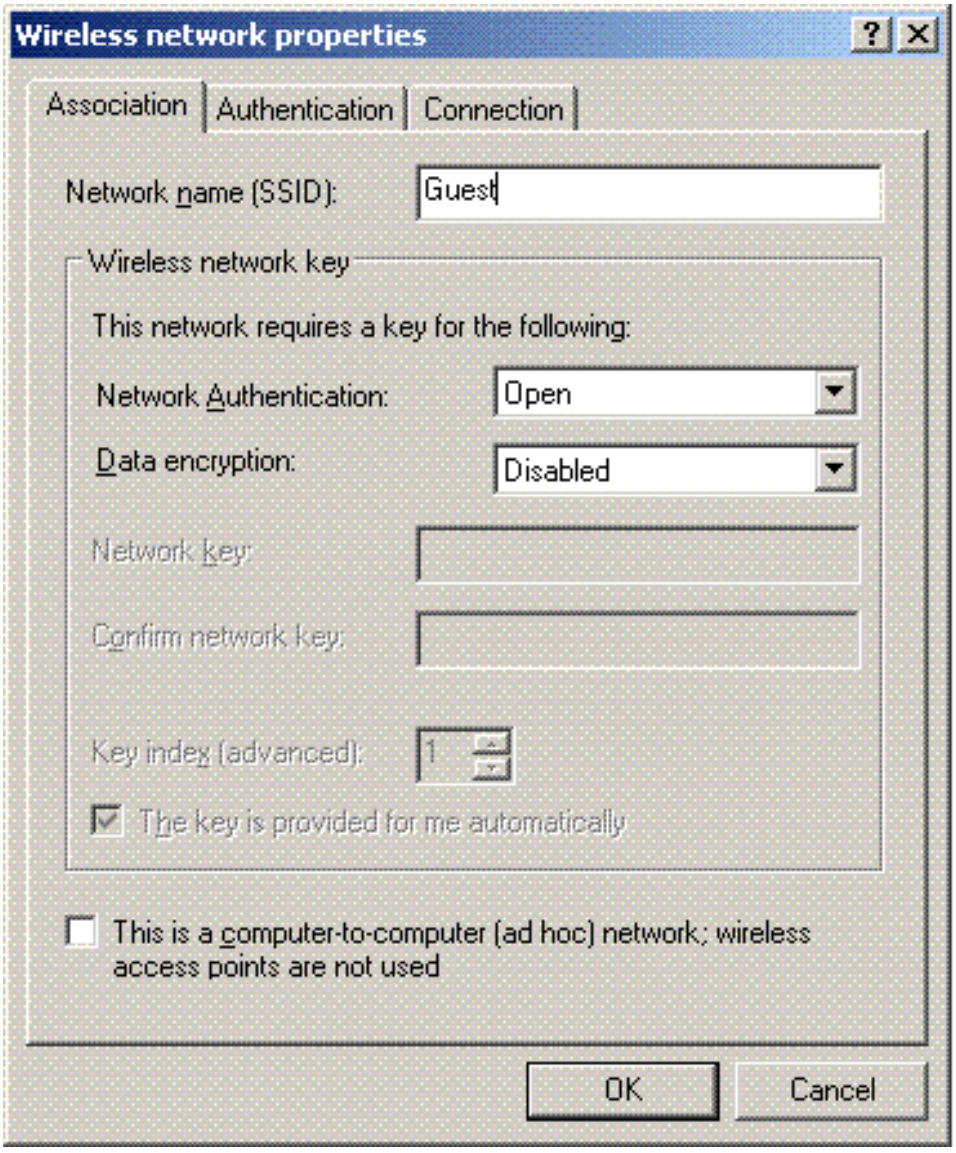
### Configuration du client

La configuration du client sans fil de Microsoft demeure en grande partie inchangée pour cet abonné. Vous devez seulement ajouter les informations de configuration appropriées pour WLAN/SSID. Procédez comme suit :

1. Dans le menu Windows **Start**, choisissez **Settings > Control Panel > Network et Internet Connections**.
2. Cliquez sur l'icône **Connexions réseau**.
3. Cliquez avec le bouton droit de la souris sur l'icône **LAN Connection**, puis choisissez **Disable**.
4. Cliquez avec le bouton droit de la souris sur l'icône **Wireless Connection**, puis choisissez

**Enable**.

5. Cliquez avec le bouton droit de la souris sur l'icône **Wireless Connection**, puis choisissez **Properties**.
6. Dans la fenêtre Propriétés de Connexion au réseau sans fil, cliquez sur l'onglet **Réseaux sans fil**.
7. Sous les réseaux préférés, cliquez sur **Add** pour configurer le SSID de l'authentification Web.
8. Sous l'onglet Association, entrez le nom du réseau (WLAN/SSID) que vous voulez utiliser pour l'authentification
   Web.




   **Note**: Par défaut, le cryptage des données est Wired Equivalent Privacy (WEP). Désactivez le cryptage des données pour que l'authentification Web fonctionne.
9. Cliquez sur **OK** en bas de la fenêtre afin de sauvegarder la configuration.Quand vous communiquez avec le WLAN, vous voyez l'icône d'une balise dans la zone du réseau préféré.

Ceci affiche une connexion Sans fil réussie à l'authentification Web. Le WLC a fourni à votre client Windows sans fil une adresse IP.


**Note**: Si votre client sans fil est également un point de terminaison VPN et que l'authentification Web est configurée comme fonction de sécurité pour le WLAN, le tunnel VPN n'est pas établi tant que vous n'avez pas suivi le processus d'authentification Web expliqué ici. Pour établir un tunnel VPN, le client doit d'abord suivre le processus d'authentification Web avec succès. C'est seulement à partir de là que le tunnel VPN est réussi.

**Note**: Après une connexion réussie, si les clients sans fil sont inactifs et ne communiquent pas avec les autres périphériques, l'authentification du client est annulée après une période de délai d'inactivité. Ce délai d'inactivité est de 300 secondes par défaut et il peut être modifié à l'aide de cette commande CLI : config network usertimeout <secondes>. Quand ceci se produit, l'entrée du client est supprimée du contrôleur. Si le client est associé à nouveau, il retrouve l'état Webauth_Reqd.

**Note**: Si les clients sont actifs après une connexion réussie, leur authentification est annulée et l'entrée peut être supprimée du contrôleur après la période d'inactivité de session configurée sur ce WLAN (par exemple, 1 800 secondes par défaut, qui peuvent être modifiées à l'aide de cette commande CLI : config wlan session-timeout <WLAN ID> <secondes>). Quand ceci se produit, l'entrée du client est supprimée du contrôleur. Si le client est associé à nouveau, il retrouve l'état Webauth_Reqd.

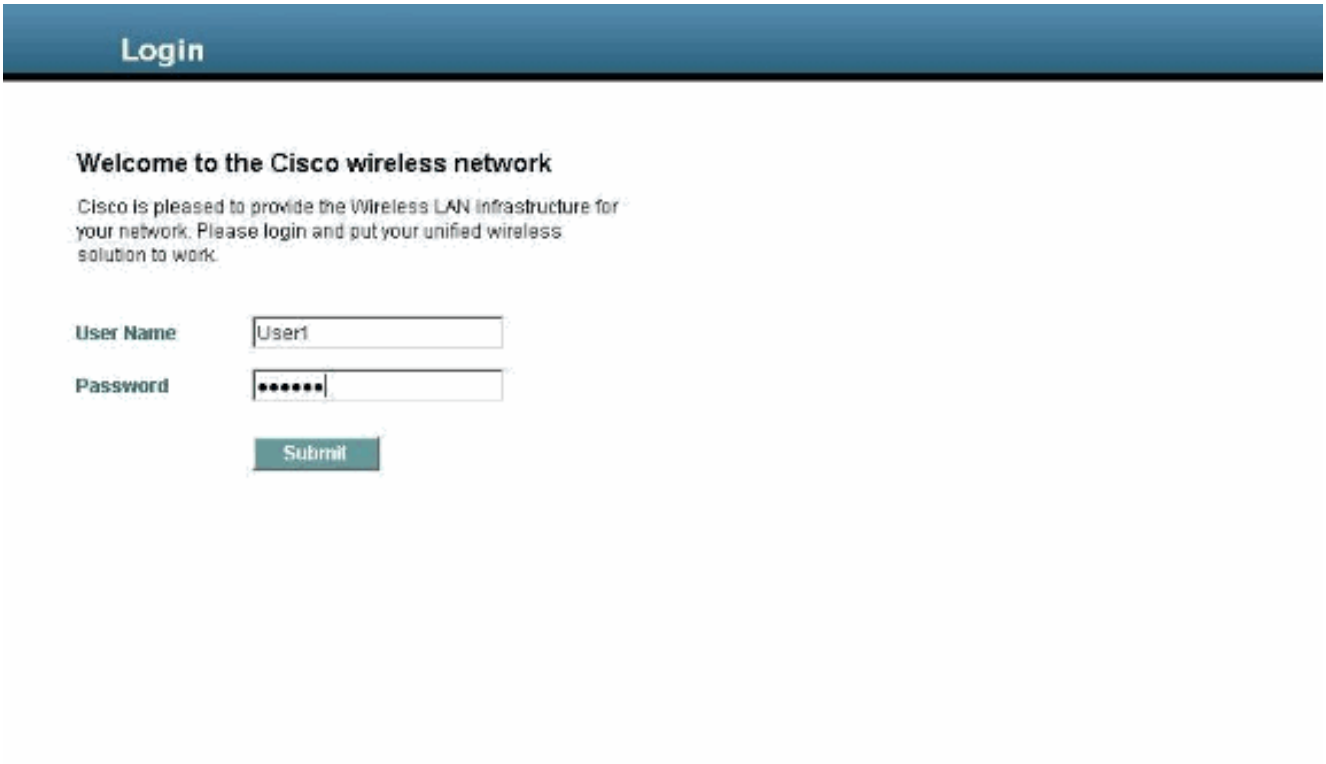
Si les clients sont associés à l'état Webauth_Reqd, qu'ils soient actifs ou inactifs, leur authentification sera annulée **après une période d'inactivité obligatoire web-auth** (par exemple, 300 secondes et ce délai n'est pas configurable par l'utilisateur). Tout le trafic du client (autorisé via l'ACL de pré-authentification) sera perturbé. Si le client est associé à nouveau, il retrouve l'état Webauth_Reqd.

## Connexion du client

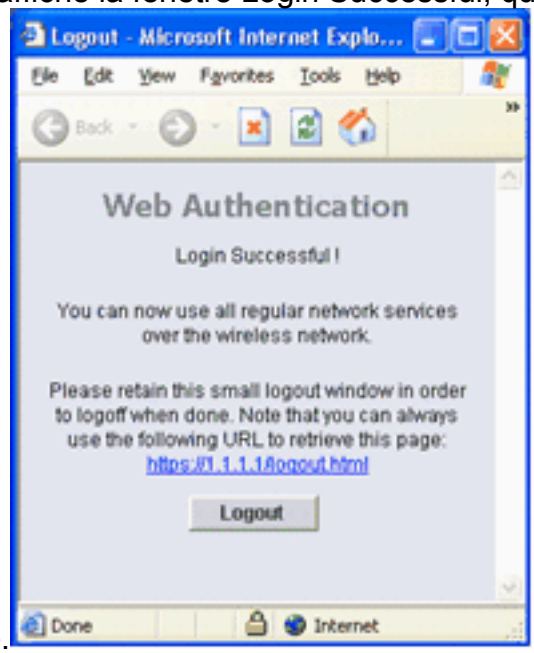
Procédez comme suit :

1. Ouvrez une fenêtre du navigateur et entrez n'importe quel URL ou adresse IP. La page d'authentification Web est alors affichée sur le client.Si le contrôleur exécute une version antérieure à 3,0, l'utilisateur doit entrer dans https://1.1.1.1/login.html pour afficher la page d'authentification Web.Une fenêtre d'alerte de sécurité s'affiche.
2. Cliquez sur **Yes** pour poursuivre.

3. Quand la fenêtre de connexion apparaît, entrez le nom d'utilisateur et le mot de passe de l'utilisateur du réseau local que vous avez
créé.




Si votre connexion est réussie, vous voyez deux fenêtres du navigateur. La fenêtre la plus grande indique une connexion réussie et vous pouvez l'utiliser pour parcourir Internet. Utilisez la fenêtre plus petite pour vous déconnecter une fois l'utilisation du réseau invité terminée.Le tir d'écran affiche qu'un réussi réoriente pour l'authentification Web.Le tir d'écran suivant affiche la fenêtre Login Successful, qui affiche quand l'authentification s'est produite.



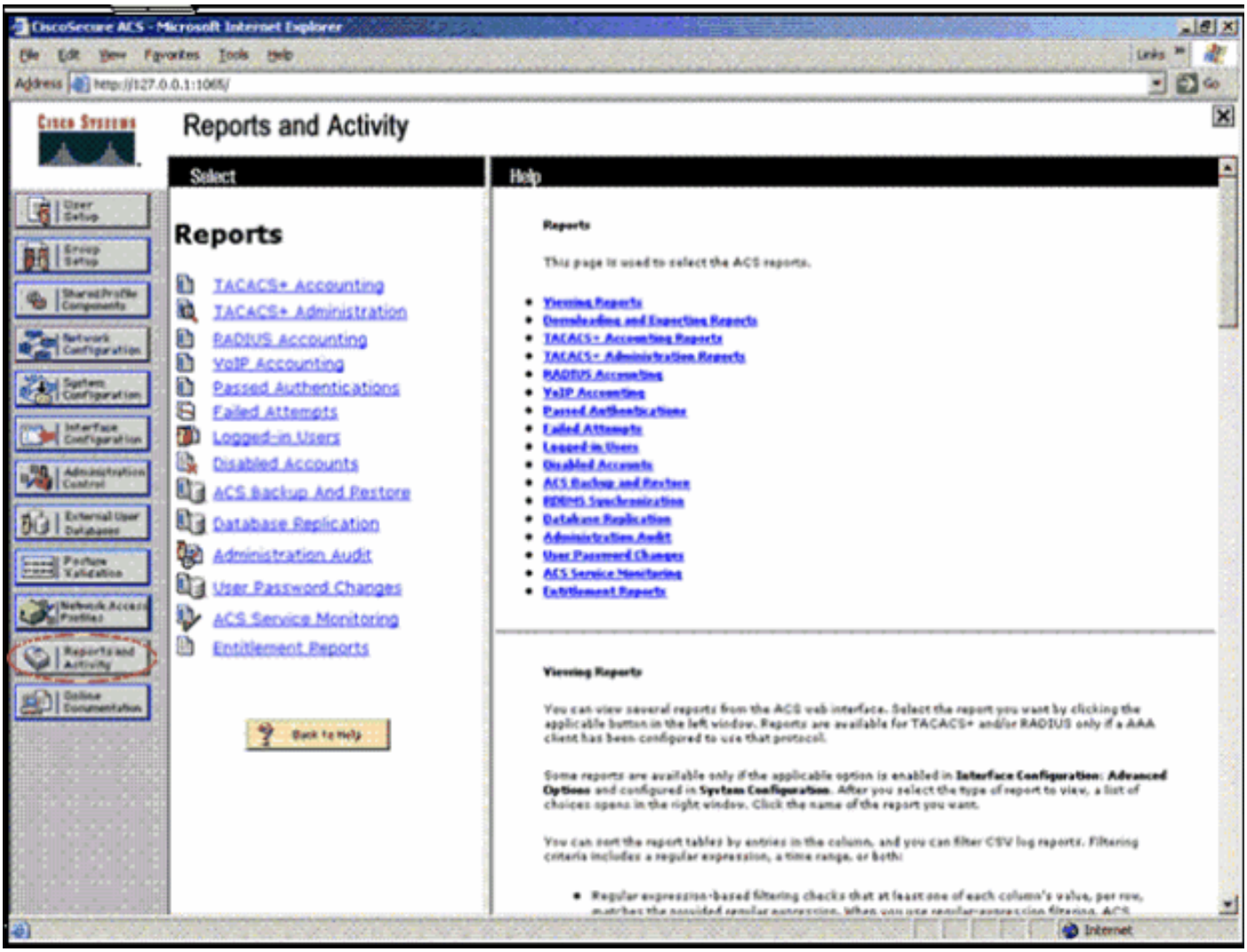

Les contrôleurs Cisco 4404/WiSM peuvent prendre en charge 125 connexions simultanées d'utilisateurs de l'authentification Web et évaluer jusqu'à 5 000 clients d'authentification Web.

Les contrôleurs Cisco 5500 peuvent prendre en charge 150 connexions simultanées des utilisateurs de l'authentification Web.

# Dépanner l'authentification Web

## Dépanner ACS

Si vous rencontrez des problèmes avec l'authentification du mot de passe, cliquez sur **Reports and Activity** dans la partie inférieure gauche pour ouvrir tous les rapports disponibles. Une fois la fenêtre des rapports ouverte, vous pouvez notamment ouvrir les rapports RADIUS Accounting, Failed Attempts for login, Passed Authentications, Logged-in Users, etc. Ces rapports sont des fichiers .csv que vous pouvez ouvrir localement sur votre machine. Les rapports aident à découvrir des problèmes d'authentification, tels qu'un nom d'utilisateur et/ou un mot de passe incorrects. ACS est également livré avec la documentation en ligne. Si vous n'êtes pas connecté à un réseau en activité et que vous n'avez pas défini le port de service, ACS utilise l'adresse IP de votre port Ethernet pour le port de service. Si votre réseau n'est pas connecté, vous obtiendrez très certainement l'adresse IP par défaut Windows 169.254.x.x.



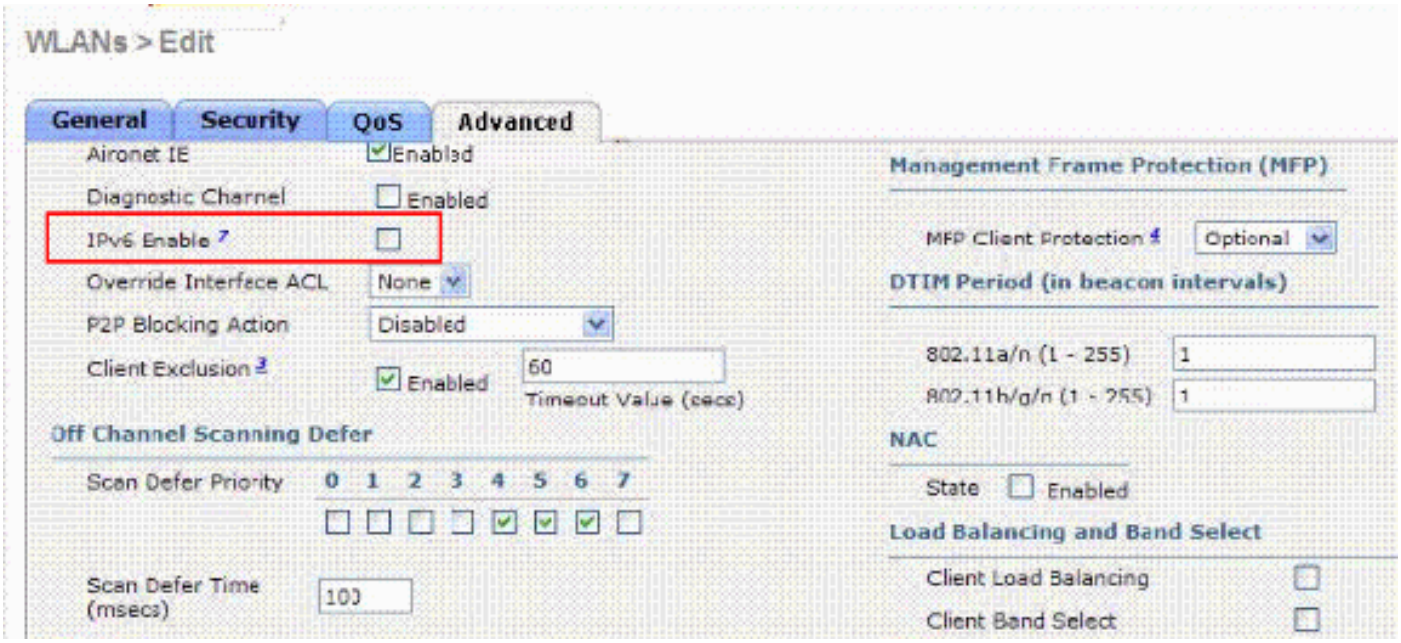

**Note**: Si vous entrez une URL externe, le WLC vous connecte automatiquement à la page d'authentification Web interne. Si la connexion automatique ne fonctionne pas, vous pouvez entrer l'adresse IP de gestion du WLC dans la barre d'URL afin d'effectuer le dépannage. Recherchez en haut du navigateur le message indiquant une redirection vers l'authentification Web.

Consultez la section Dépannage de l'authentification Web sur un contrôleur de réseau local sans fil (WLC) pour plus d'informations sur le dépannage de l'authentification Web.

# Authentification Web avec pont IPv6

Afin de configurer un WLAN pour l'IPv6 jetant un pont sur, du GUI de contrôleur, naviguez vers des **WLAN**. Puis, sélectionnez le WLAN désiré et choisissez **avancé de la** page de **WLANs > Edit**.

Sélectionnez la case d'**ipv6 enable** si vous voulez activer les clients qui se connectent à ce WLAN pour recevoir des paquets d'IPv6. Autrement, laissez la case non sélectionnée, qui est la valeur par défaut. Si vous désactivez (ou décochez) la case d'IPv6, on permettra l'IPv6 seulement après authentification. L'activation de l'IPv6 signifie que le contrôleur peut passer le trafic d'IPv6 sans authentification client.




Pour plus d'informations détaillées sur la transition d'IPv6 et les **instructions pour l'usage de cette caractéristique**, référez-vous à l'IPv6 de configuration jetant un pont sur la section du guide de configuration Sans fil de contrôleur LAN de Cisco, version 7.0.

# Informations connexes

- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Dépannage de l'authentification Web sur un contrôleur de réseau local sans fil
- LAN sans fil Cisco
- Exemple de configuration d'un accès invité filaire à l'aide de contrôleurs de réseau local sans fil Cisco
- Guide de configuration du contrôleur de réseau local sans fil Cisco, version 7.0 - Gérer des comptes utilisateurs
- Authentification de l'administrateur de salle d'attente du contrôleur de réseau local sans fil via un serveur RADIUS
- Support et documentation techniques - Cisco Systems