

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Authentification Web](#)

[Procédé d'authentification Web](#)

[Configuration du réseau](#)

[Configurer le contrôleur pour l'authentification Web](#)

[Créer une interface VLAN](#)

[Configurer un contrôleur WLC pour l'authentification Web interne](#)

[Ajouter une instance WLAN](#)

[Trois façons d'authentifier des utilisateurs dans l'authentification Web](#)

[Configurer votre client WLAN afin de procéder à l'authentification Web](#)

[Configuration du client](#)

[Connexion du client](#)

[Dépanner l'authentification Web](#)

[Dépanner ACS](#)

[Authentification Web avec pont IPv6](#)

[Informations connexes](#)

[Introduction](#)

Ce document explique comment Cisco implante l'authentification Web et présente la manière de configurer un contrôleur LAN sans fil (WLAN) Cisco de gamme 4400 (WLC) pour prendre en charge une authentification 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 :

- Un contrôleur WLC de gamme 4400 qui exécute la version 7.0.116.0
- Version 4.2 du Cisco Secure Access Control Server (ACS) installée sur un serveur Microsoft® Windows 2003
- Point d'accès léger Cisco de gamme 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 troisième couche faisant en sorte que le contrôleur empêche le trafic IP (à l'exception des paquets liés au protocole DHCP et au DNS) provenant d'un client particulier jusqu'à ce que le client ait fourni un nom d'utilisateur et un mot de passe valides. 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 se faire par les moyens suivants :

- Fenêtre de connexion par défaut sur le WLC
- Version modifiée de la fenêtre de connexion par défaut sur le WLC
- Fenêtre de connexion personnalisée, que vous configurez sur un serveur Web externe (authentification Web externe)
- Fenêtre de connexion personnalisée que vous téléchargez vers le contrôleur

Dans ce document, le contrôleur LAN sans fil pour authentification Web interne est configuré.

Procédé d'authentification Web

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

- L'utilisateur ouvre un navigateur Web et saisit une adresse URL, par exemple : <http://www.cisco.com>. Le client envoie une demande DNS liée à cet URL afin d'obtenir l'IP pour la destination. Le WLC fait dévier la demande DNS vers le serveur DNS, qui réplique par une réponse DNS contenant l'adresse IP de la destination www.cisco.com. Cette réponse est

ensuite transmise aux clients sans fil.

- Le client tente alors d'établir une connexion TCP avec l'adresse IP de destination. Il envoie un paquet TCP SYN destiné à l'adresse IP de www.cisco.com.
- Le WLC a configuré des règles pour le client, donc peut agir en tant que serveur mandataire pour www.cisco.com. Il renvoie un paquet TCP SYN-ACK au client, avec l'adresse IP de www.cisco.com comme source. Le client renvoie un paquet TCP ACK afin de se terminer la connexion TCP en trois temps. Une fois cela terminé, la connexion TCP est entièrement établie.
- Le client envoie un paquet HTTP GET destiné à www.cisco.com. Le WLC intercepte ce paquet et l'envoie pour redirection. La passerelle d'application HTTP prépare un corps en HTML et le renvoie comme réponse au HTTP GET demandé par le client. Ce HTML incite le client à se rendre à l'URL de page Web par défaut du WLC, par exemple : http://<Virtual-Server-IP>/login.html.
- Le client désactive la connexion TCP avec l'adresse IP, par exemple, www.cisco.com.
- Le client souhaite maintenant accéder à http://1.1.1.1/login.html. Par conséquent, le client essaie d'établir une connexion TCP avec l'adresse IP virtuelle du WLC. Il envoie un paquet TCP SYN au WLC pour 1.1.1.1.
- Le WLC répond par un TCP SYN-ACK, et le client renvoie un TCP ACK au WLC afin de terminer la liaison.
- Le client envoie une requête HTTP GET pour /login.html destiné à 1.1.1.1 en vue d'accéder à la page de connexion.
- Cette demande est permise jusqu'au serveur Web du WLC, qui répond avec la page de connexion par défaut. Le client reçoit la page de connexion sur la fenêtre du navigateur, d'où l'utilisateur peut procéder à la connexion.

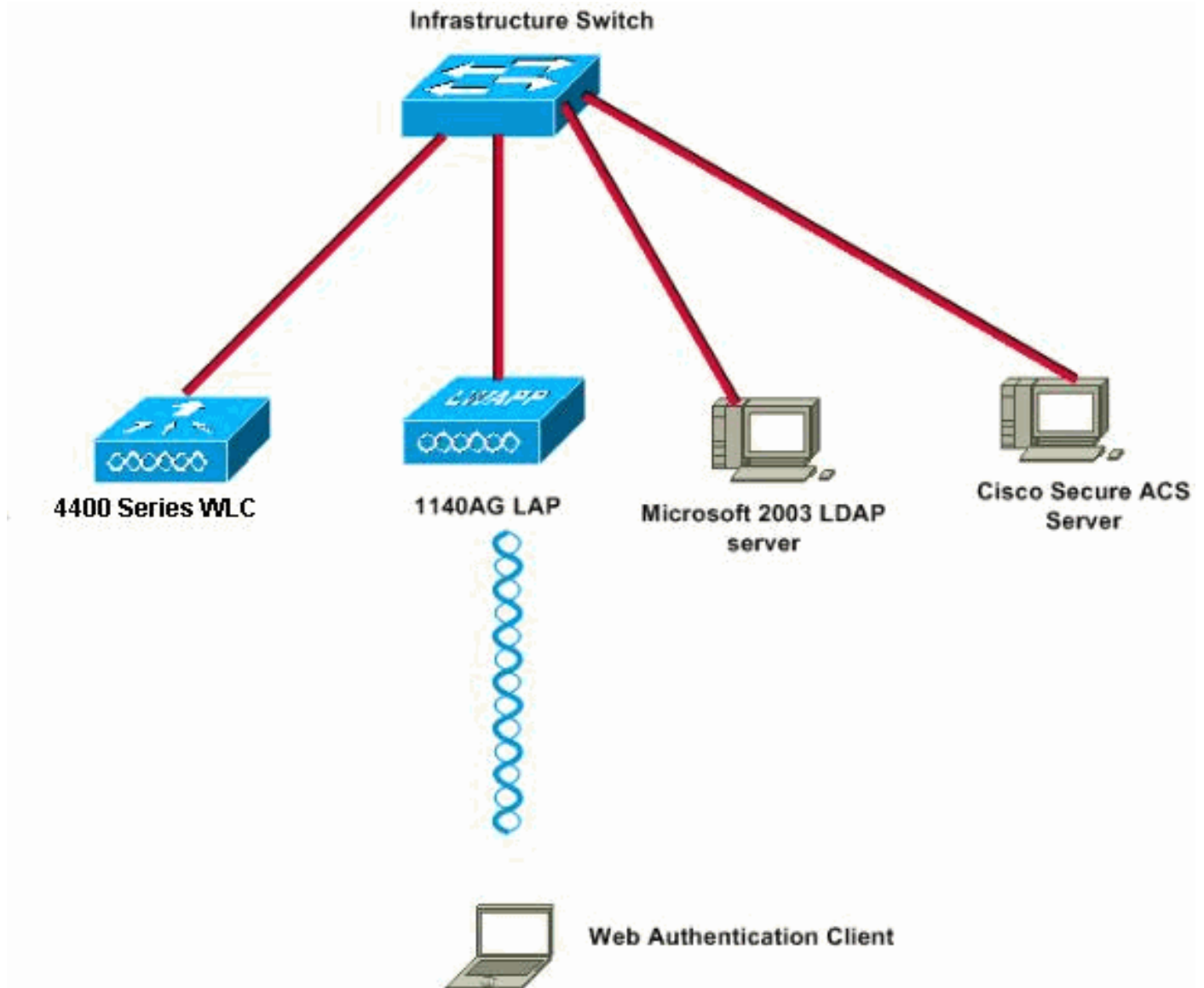
Voici un lien vers une vidéo de la [communauté de soutien de Cisco](#) qui explique le procédé d'authentification Web :

[Authentification Web sur les contrôleurs LAN sans fil de Cisco \(WLC\)](#)



[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](#)
- [Configurer un contrôleur WLC pour l'authentification 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.

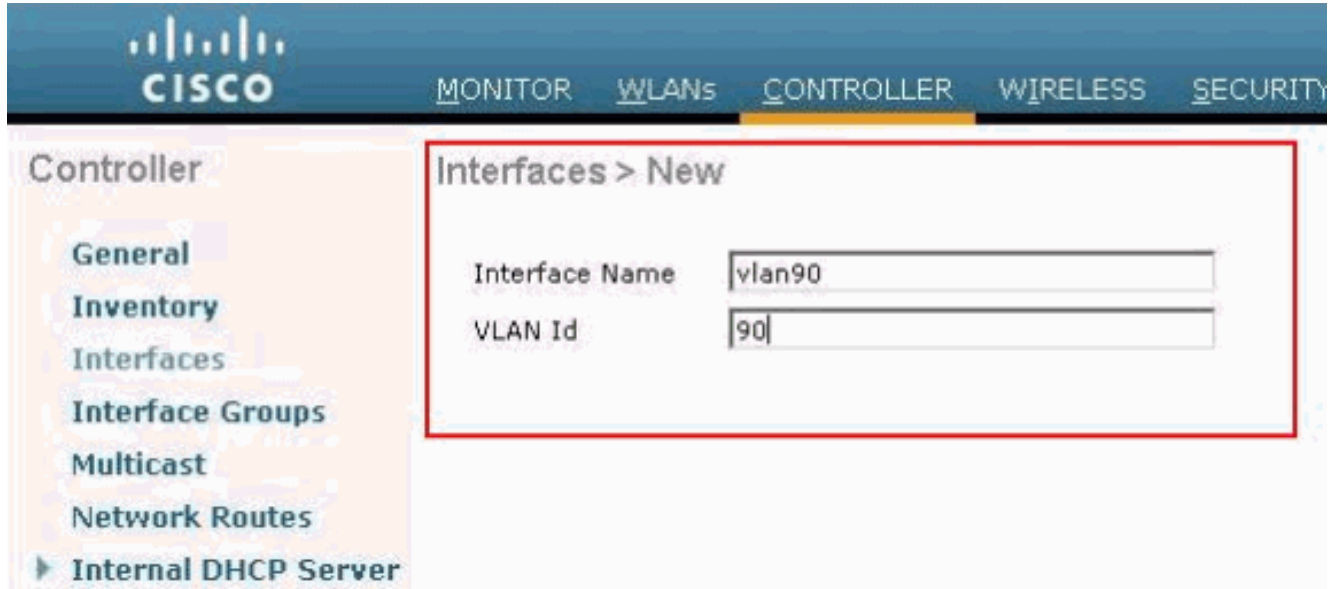
Ce sont les adresses IP utilisées dans ce document :

- 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. À partir de l'interface GUI du contrôleur LAN, sélectionnez **Contrôleur** dans le menu supérieur, puis **Interfaces** dans le menu de gauche, et cliquez sur Nouveau, du côté droit supérieur de la fenêtre, pour créer une interface dynamique. La fenêtre **Interfaces > Nouveau** s'affiche. Cet exemple utilise le nom d'interface *vlan90* avec un ID VLAN de *90* :



The screenshot shows the Cisco GUI for a LAN controller. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The 'CONTROLLER' tab is active. On the left, a sidebar lists various configuration options: 'General', 'Inventory', 'Interfaces', 'Interface Groups', 'Multicast', 'Network Routes', and 'Internal DHCP Server'. The main content area is titled 'Interfaces > New' and contains two input fields: 'Interface Name' with the value 'vlan90' and 'VLAN Id' with the value '90'. A red box highlights this configuration area.

2. Cliquez sur **Apply** pour créer l'interface VLAN. La fenêtre **Interfaces > Modifier** apparaît et demande de saisir des renseignements spécifiques à l'interface.
3. Ce document utilise ces paramètres : Adresse IP — 10.10.10.2 Masque de réseau - 255.255.255.0 (24 bits) Passerelle — 10.10.10.1 Numéro de port — 2 Serveur DHCP principal — 10.77.244.204 **Remarque:** 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 **Remarque:** 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

The screenshot shows the Cisco WLC GUI configuration page for interface 'vlan90'. The page is organized into several sections:

- General Information:** Interface Name (vlan90), MAC Address (00:0b:85:48:53:c0).
- Configuration:** Guest Lan (checkbox), Quarantine (checkbox), Quarantine Vlan Id (text field with value 0).
- Physical Information:** Port Number (text field with value 2), Backup Port (text field with value 0), Active Port (text field with value 0), Enable Dynamic AP Management (checkbox).
- Interface Address:** VLAN Identifier (text field with value 90), IP Address (text field with value 10.10.10.2), Netmask (text field with value 255.255.255.0), Gateway (text field with value 10.10.10.1).
- DHCP Information:** Primary DHCP Server (text field with value 10.77.244.204), Secondary DHCP Server (text field).
- Access Control List:** ACL Name (dropdown menu with value none).

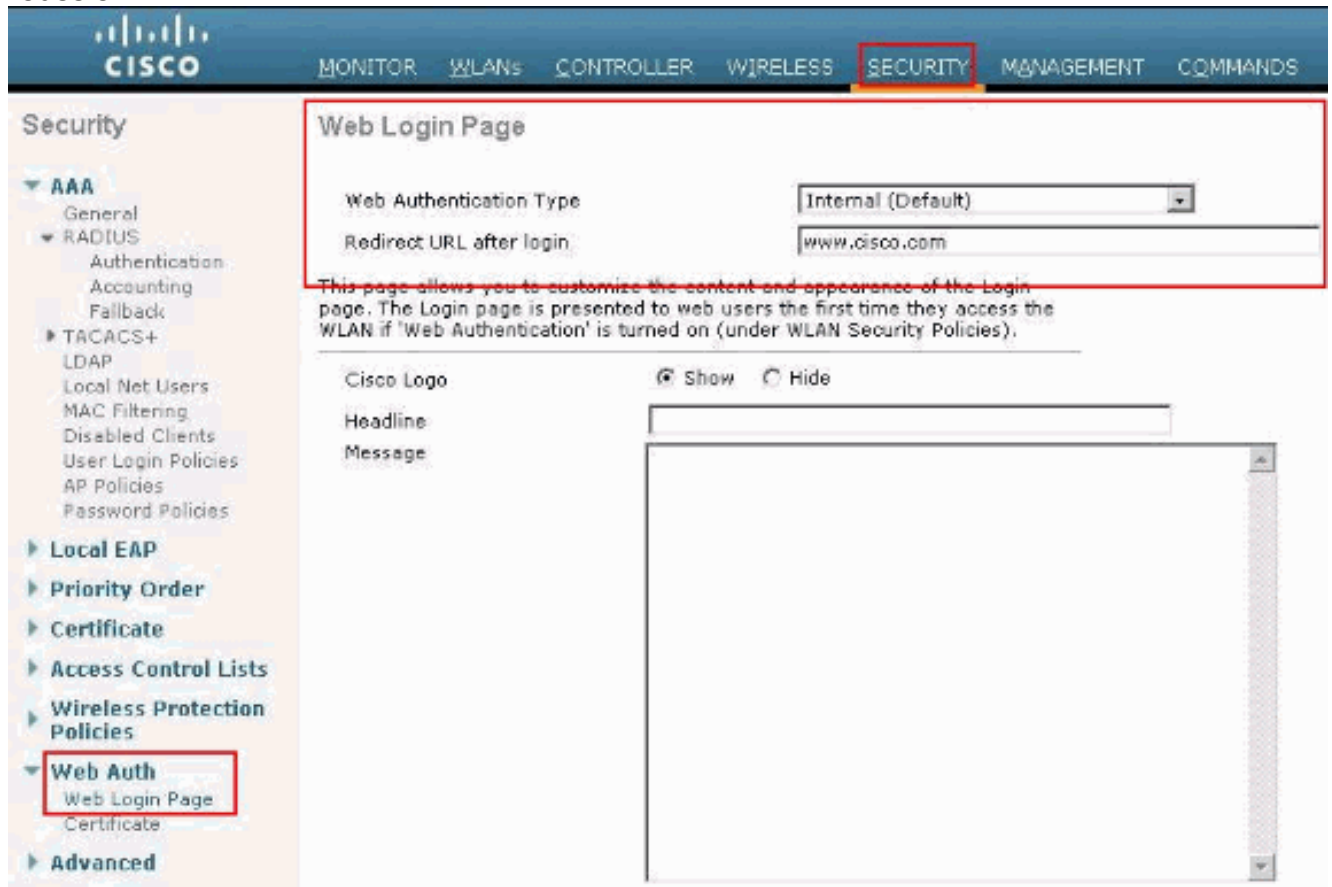
4. Cliquez sur **Apply** afin de sauvegarder les modifications.

[Configurer un contrôleur WLC pour l'authentification Web interne](#)

L'étape suivante est de configurer le WLC pour l'authentification Web interne. L'authentification Web interne est le type d'authentification Web par défaut pour les WLC. Si ce paramètre n'a pas été changé, aucune configuration n'est exigée pour permettre l'authentification Web interne. Si le paramètre d'authentification Web a été changé précédemment, terminez ces étapes afin de configurer le WLC pour l'authentification Web interne :

1. À partir de l'interface GUI de contrôleur, sélectionnez **Sécurité > Authentification Web > Page de connexion Web** afin d'accéder à la page de connexion.
2. À partir de la liste déroulante de types d'authentification Web, choisissez **Authentification Web interne**.

3. Dans le champ **Redirigez l'URL après la connexion**, entrez l'URL de la page à laquelle l'utilisateur final sera réorienté après l'authentification réussie.



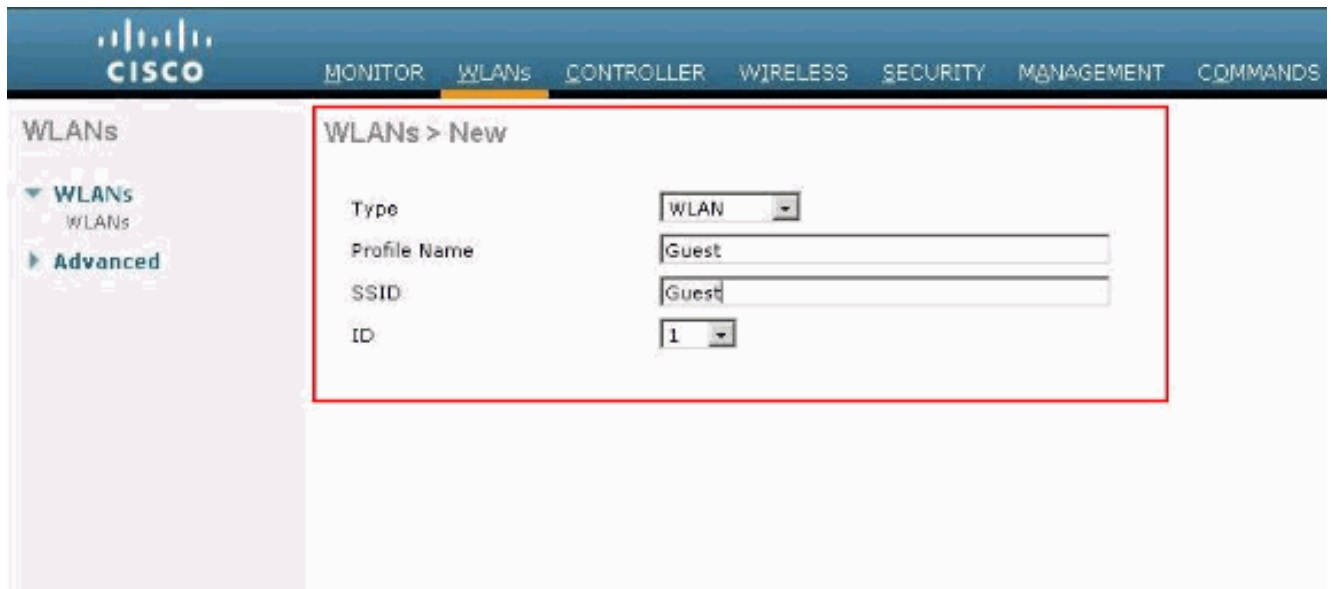
Remarque: Dans les versions 5.0 et ultérieures du WLC, la page de déconnexion pour l'authentification Web peut également être personnalisée. Reportez-vous aux [pages d'assignation de connexion, d'échec de connexion et de déconnexion dans la section WLAN du Guide de configuration du contrôleur LAN sans fil 5.2](#) pour plus d'informations sur le mode de configuration.

[Ajouter une instance WLAN](#)

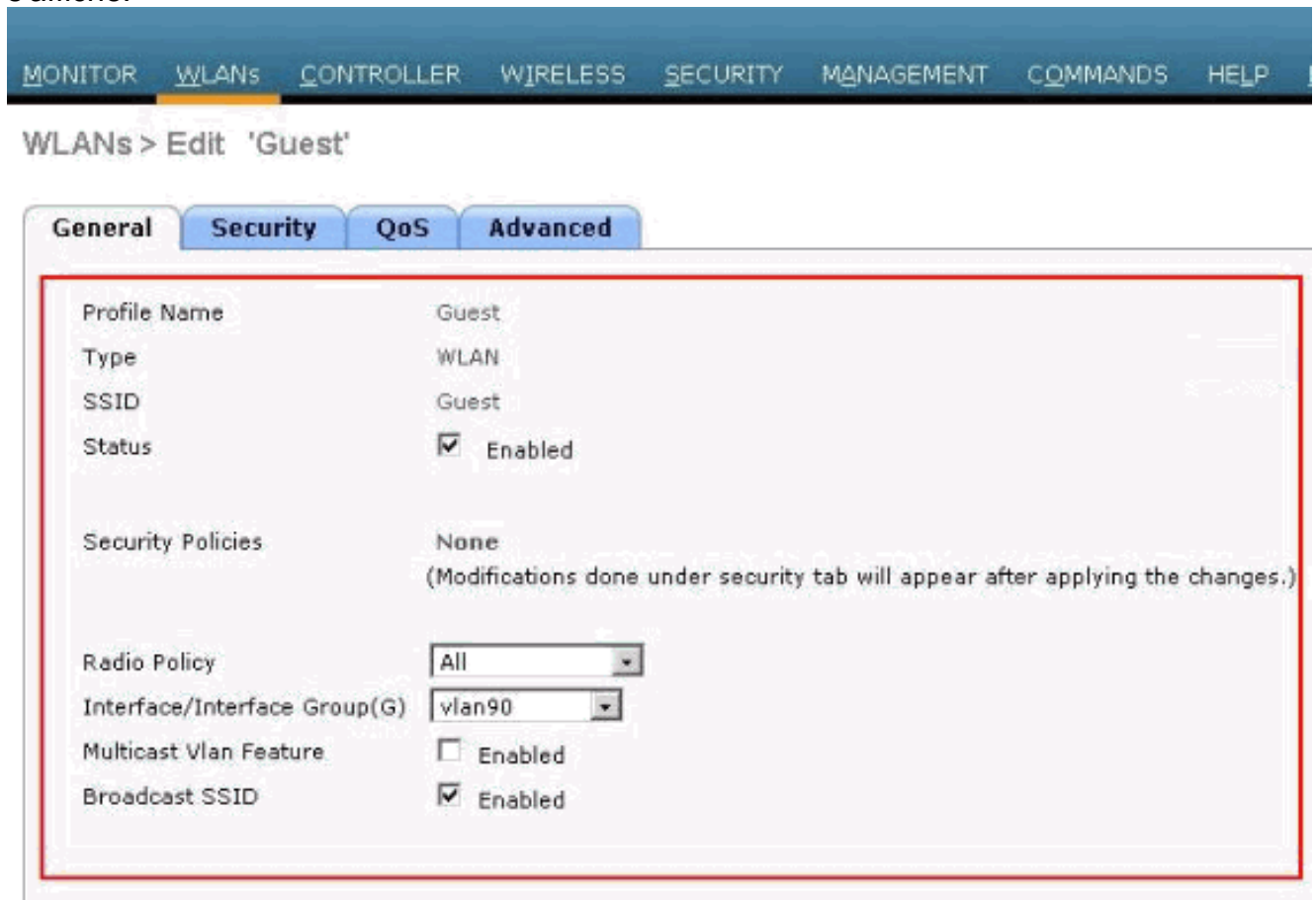
Maintenant que l'authentification Web interne a été activée et qu'il y a une interface VLAN dédiée à l'authentification Web, vous devez fournir un nouveau WLAN/SSID afin de prendre en charge les utilisateurs d'authentification Web.

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

1. À partir de l'interface GUI du WLC, cliquez sur **WLAN** dans le menu supérieur, puis sur **Nouveau**, du 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.



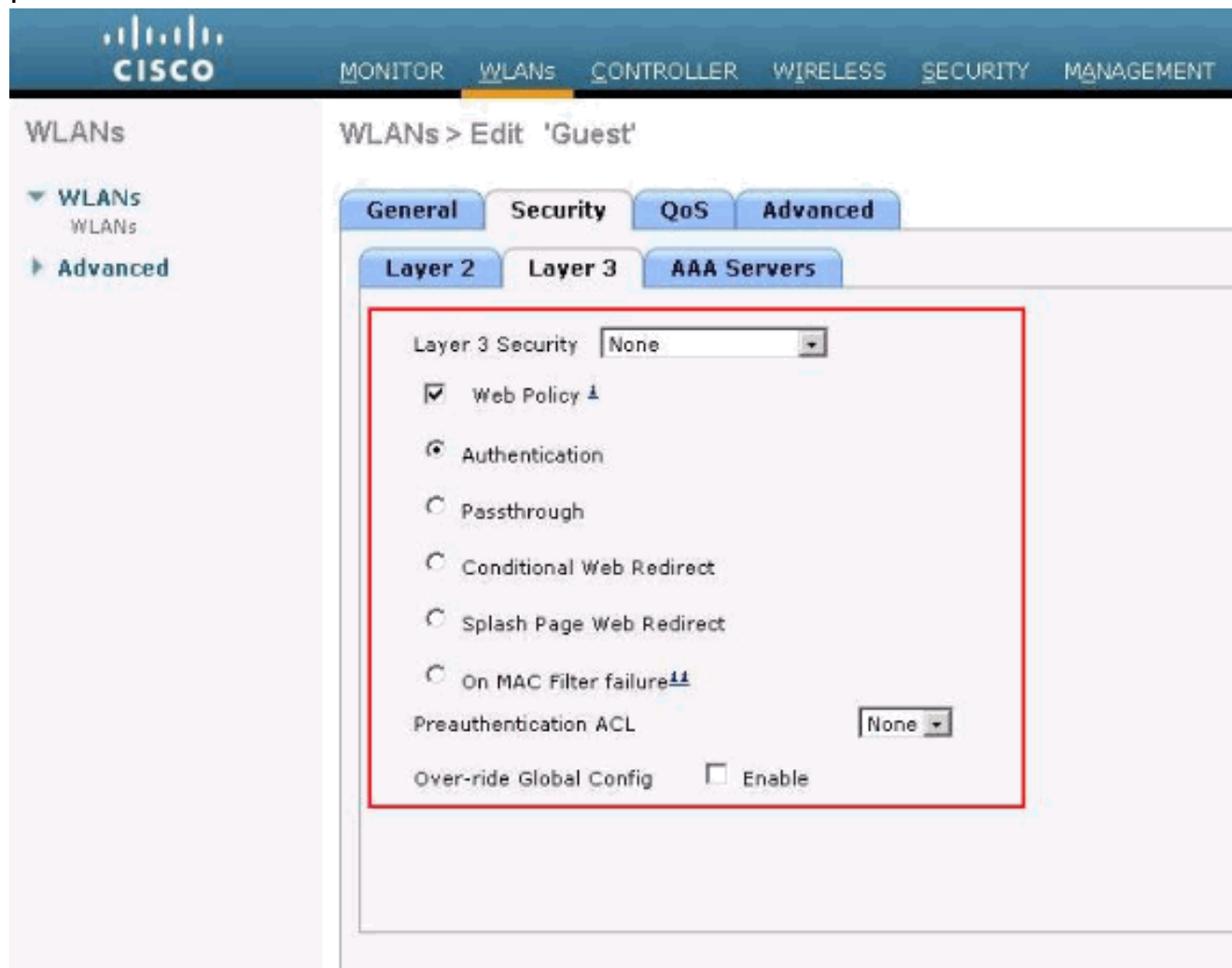
2. Cliquez sur **Apply**. Une nouvelle fenêtre WLAN > Modifier s'affiche.



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*. **Remarque:** 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**. **Remarque:** 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 **Politique Web** et choisissez l'option **Authentification**, comme démontré 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 d'utilisateurs invités s'enregistre dans la base de données locale du WLC. Les utilisateurs sont authentifiés par le WLC dans cette base de données.

1. À partir de l'interface GUI du WLC, sélectionnez **Sécurité**.
2. Cliquez sur **Utilisateurs du réseau local** dans le menu AAA à gauche.

The screenshot shows the Cisco Security configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, and COMMANDS. The left sidebar shows the Security menu with various options, and 'Local Net Users' is highlighted with a red box. The main content area is titled 'Local Net Users' and contains a table with the following headers: User Name, WLAN Profile, Guest User, Role, and Description.

3. Cliquez sur Nouveau afin de créer un utilisateur. Une nouvelle fenêtre s'affiche, qui demande les informations de nom d'utilisateur et de 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 **Utilisateur1**.
5. Ajoutez une description, le cas échéant. Cet exemple se sert de l'**utilisateur invité 1**.
6. Cliquez sur **Apply** pour sauvegarder la nouvelle configuration utilisateur.

The screenshot shows the Cisco Security configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COMMANDS. The left sidebar shows the 'Security' menu with options like AAA, RADIUS, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, and Advanced.

The main content area displays the 'Local Net Users > New' form with the following fields:

- User Name: User1
- Password: [Redacted]
- Confirm Password: [Redacted]
- Guest User:
- Lifetime (seconds): 86400
- Guest User Role:
- WLAN Profile: Guest
- Description: GuestUser1

Below the form, a table lists the created users:

User Name	WLAN Profile	Guest User	Role	Description
User1	Guest	Yes		GuestUser1

7. Répétez les étapes 3 à 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.

Remarque: 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.

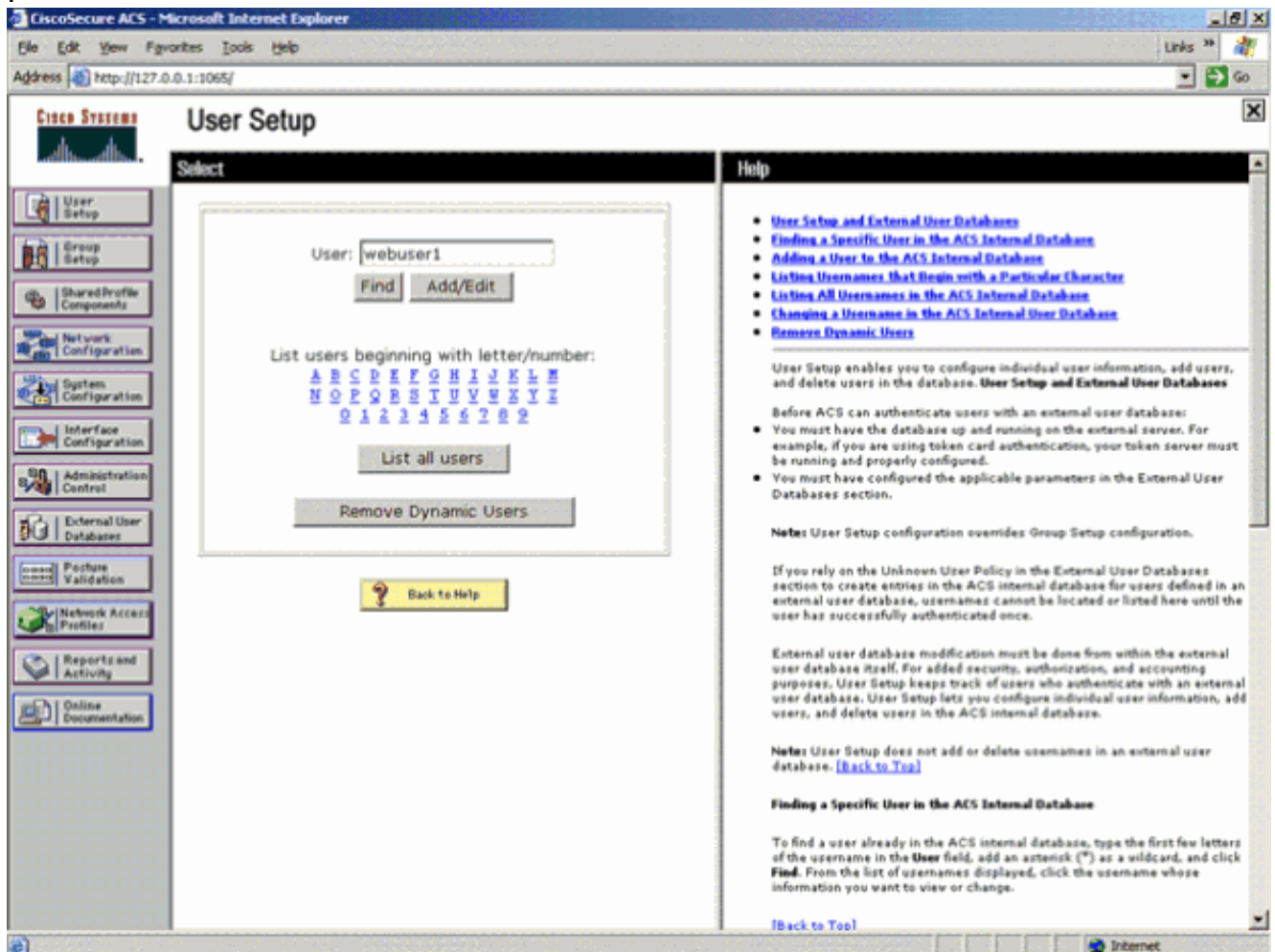
La section [Configurer ACS](#) explique comment configurer ACS pour RADIUS. Vous devez avoir un réseau totalement fonctionnel avec un système de noms de domaine (DNS) et un serveur RADIUS.

[Configurer ACS](#)

Cette section présente la configuration d'ACS pour RADIUS.

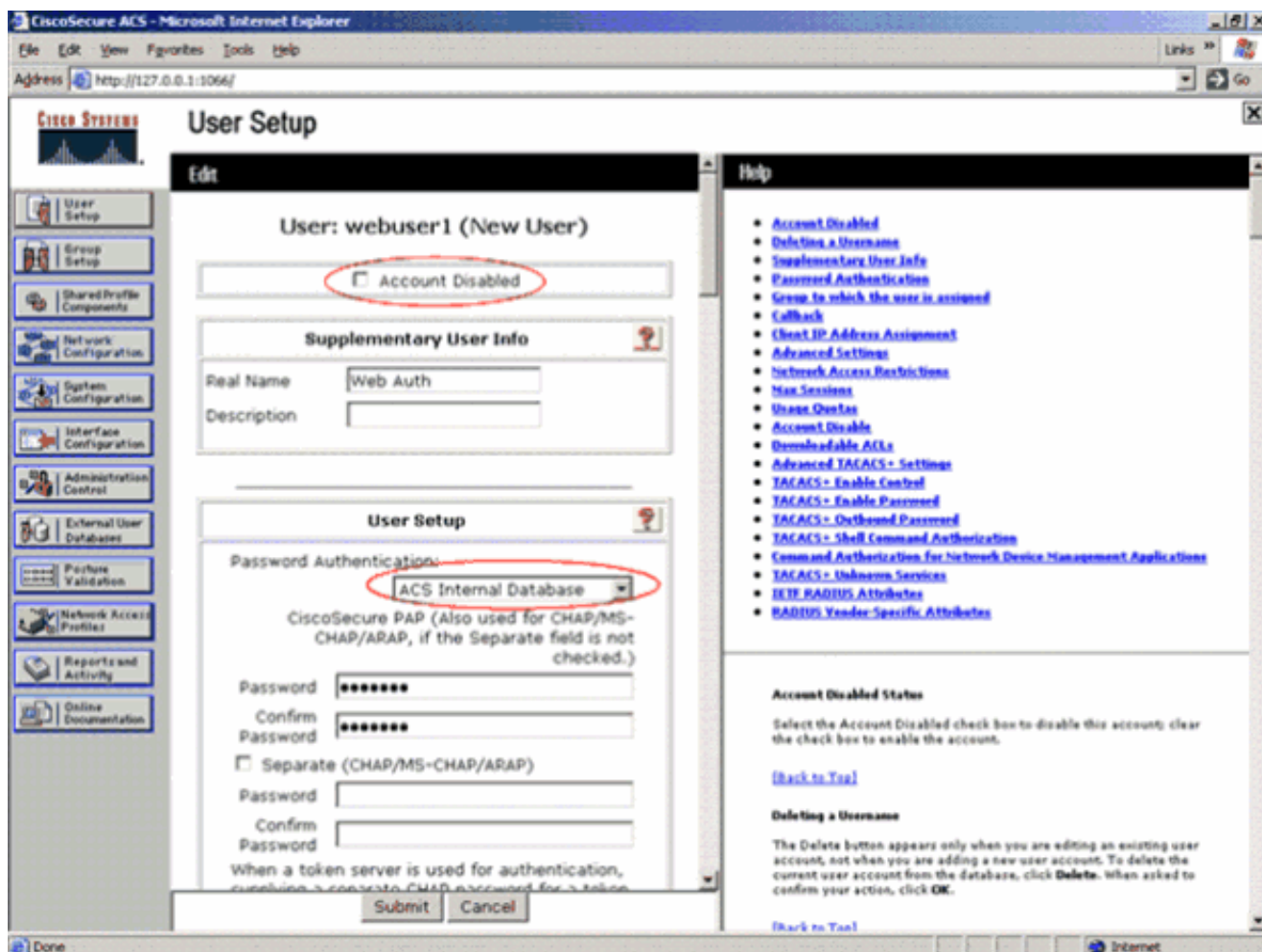
Configurez ACS sur votre serveur, puis effectuez ces étapes afin de créer un utilisateur pour l'authentification :

1. Quand ACS demande si vous voulez ouvrir ACS dans une fenêtre de navigateur pour la configuration, cliquez sur **yes**. **Remarque:** 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 amène à l'écran de réglage d'utilisateur, comme affiché ici



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

:



4. Assurez-vous que la case **Compte désactivé** au haut de la fenêtre 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 **Autoriser les utilisateurs réseau** de sorte que le serveur RADIUS soit utilisé pour authentifier les utilisateurs de votre réseau sans fil.
8. Cliquez sur **Apply**.

RADIUS Authentication Servers > New

Server Index (Priority): 1

Server IP Address: 10.77.244.196

Shared Secret Format: ASCII

Shared Secret: [Redacted]

Confirm Shared Secret: [Redacted]

Key Wrap: (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: Enable

Management: Enable

IPSec: Enable

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

RADIUS Authentication Servers

Call Station ID Type: IP Address

Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.77.244.196	1812	Disabled	Enabled

1. Call Station ID Type will be applicable only for non-802.1x authentication only.

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. Ensuite, choisissez le serveur RADIUS, représenté par 10.77.244.196 dans cet exemple

:

The screenshot shows the Cisco WLAN configuration interface for a 'Guest' WLAN. The 'AAA Servers' tab is selected, and the 'Layer 2' sub-tab is active. The configuration includes:

- Radius Servers:** A checkbox for 'Radius Server Overwrite interface' is unchecked. Below it, there are three rows for 'Server 1', 'Server 2', and 'Server 3'. Each row has a dropdown menu for the server name and a dropdown menu for the server IP and port. Server 1 is configured with 'IP:10.77.244.196, Port:1812'.
- Authentication Servers:** A checkbox for 'Enabled' is checked. Below it, there are three rows for 'Server 1', 'Server 2', and 'Server 3', each with a dropdown menu for the server name.
- Accounting Servers:** A checkbox for 'Enabled' is checked. Below it, there are three rows for 'Server 1', 'Server 2', and 'Server 3', each with a dropdown menu for the server name.
- LDAP Servers:** Three rows for 'Server 1', 'Server 2', and 'Server 3', each with a dropdown menu for the server name.
- Local EAP Authentication:** A checkbox for 'Enabled' is unchecked.

3. Cliquez sur **Apply**.

[Vérifier ACS](#)

Quand vous installez ACS, souvenez-vous de télécharger tous les correctifs actuels et le code le plus récent. Ceci devrait résoudre les prochains problèmes. Au cas où vous utiliseriez l'authentification RADIUS, assurez-vous que votre WLC est répertorié en tant qu'un des clients AAA. Cliquez sur le **menu de configuration réseau** à votre gauche pour vérifier cela. 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.

CiscoSecure ACS - Microsoft Internet Explorer

Address: http://127.0.0.1:1065/

Network 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

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
wlc	10.77.244.204	RADIUS (Cisco Airespace)
wlc210	10.77.244.210	RADIUS (Cisco Airespace)

Add Entry Search

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
ts-web	10.77.244.196	CiscoSecure ACS

Add Entry Search

Proxy Distribution Table

Character String	AAA Servers	Strip	Account
(Default)	ts-web	No	Local

Add Entry Sort Entries

[Back to Help](#)

Help

- Network Device Groups
- Adding a Network Device Group
- Editing a Network Device Group
- Deleting a Network Device Group
- Searching for Network Devices
- AAA Clients
- Adding a AAA Client
- Editing a AAA Client
- Deleting a AAA Client
- AAA Servers
- Adding a AAA Server
- Editing a AAA Server
- Deleting a AAA Server
- Proxy Distribution Table
- Adding a Proxy Distribution Table Entry
- Sorting Proxy Distribution Table Entries
- Editing a Proxy Distribution Table Entry
- Deleting a Proxy Distribution Table Entry

Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.

Network Device Groups

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

The screenshot shows the CiscoSecure ACS User Setup interface. The browser window is titled 'CiscoSecure ACS - Microsoft Internet Explorer' and the address bar shows 'http://127.0.0.1:1066/'. The page title is 'User Setup'. On the left is a navigation menu with options like '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', and 'Online Documentation'. The main area is split into two panes: 'Select' and 'User List'. The 'Select' pane contains a search form with a 'User:' field, 'Find', and 'Add/Edit' buttons. Below it is a keyboard layout with letters and numbers, and a 'List all users' button circled in red. The 'User List' pane shows a table with columns: User, Status, Group, and Network Access Profile. The table contains three rows: 'User1', 'User2', and 'Webuser1'. The 'Webuser1' row is circled in red.

User	Status	Group	Network Access Profile
User1	Enabled	Default Group (3 users)	(Default)
User2	Enabled	Default Group (3 users)	(Default)
Webuser1	Enabled	Default Group (3 users)	(Default)

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 Sécurité > **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.

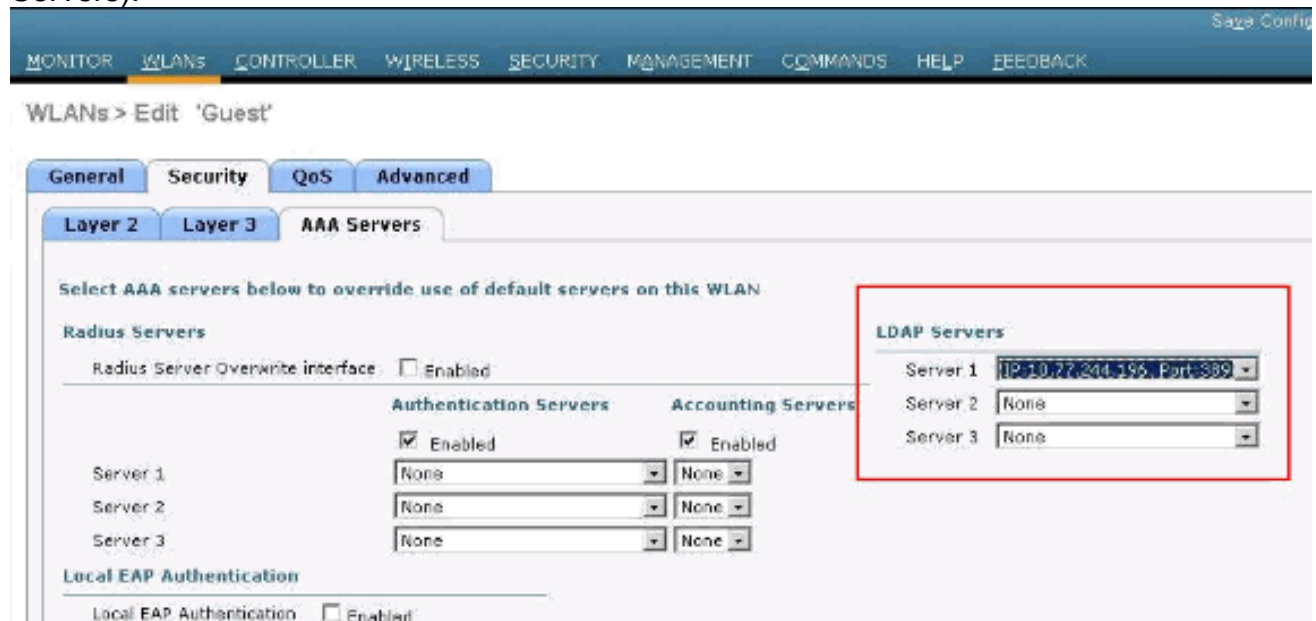
The screenshot shows the Cisco Security configuration interface for adding a new LDAP server. The page is titled "LDAP Servers > New". The left sidebar contains a navigation menu with the following items: AAA (General, RADIUS, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies), Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, and Web Auth. The main form contains the following fields:

Server Index (Priority)	1
Server IP Address	10.77.244.196
Port Number	389
Simple Bind	Authenticated
Bind Username	user2
Bind Password	*****
Confirm Bind Password	*****
User Base DN	ou=active,ou=employees,ou=people,o=cisco.com
User Attribute	uid
User Object Type	person
Server Timeout	2 seconds
Enable Server Status	Enabled

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 ces étapes si vous souhaitez affecter des serveurs LDAP précis 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.

[Configurer votre client WLAN afin de procéder à l'authentification Web](#)

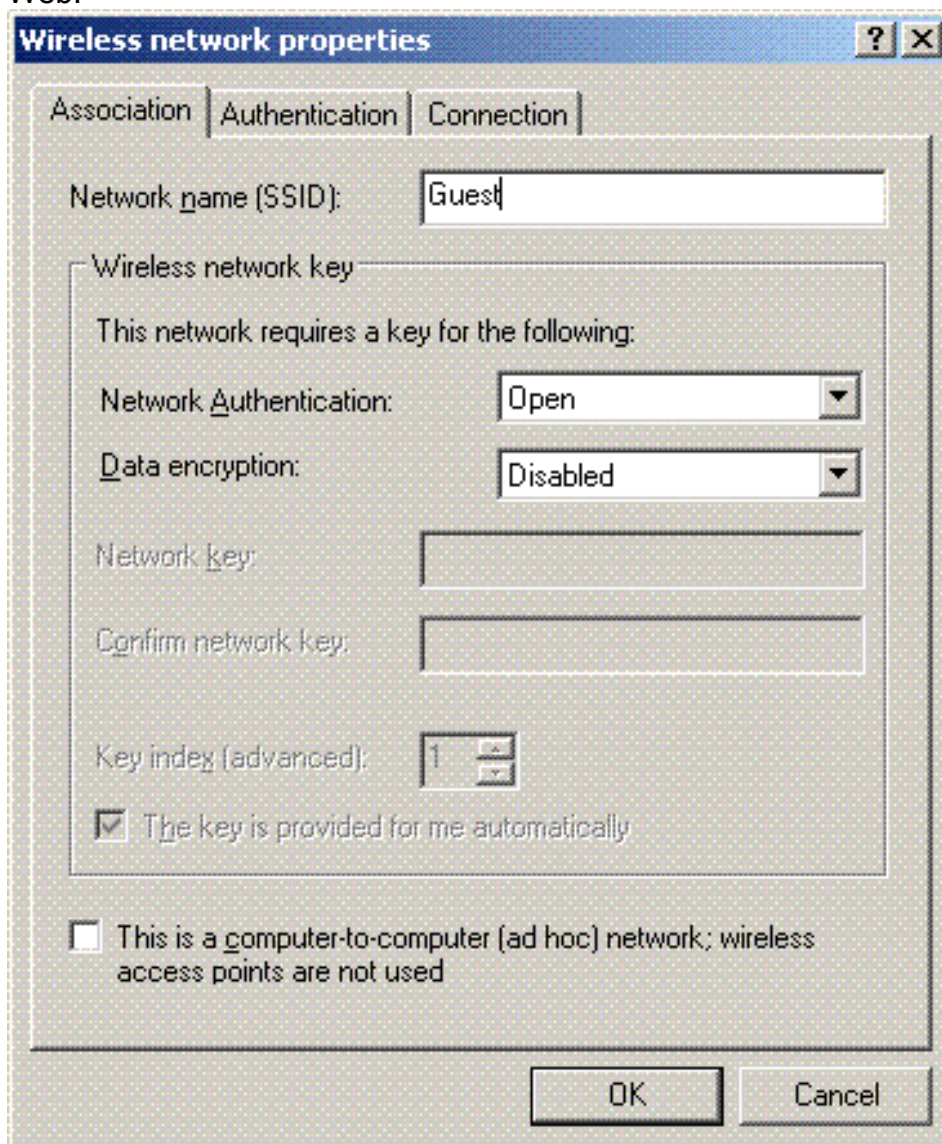
Une fois le WLC configuré, le client doit être configuré de façon appropriée pour l'authentification Web. Cette section présente les informations permettant de configurer votre système Windows pour l'authentification Web.

[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.



Remarque: 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.

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



Remarque: 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.

Remarque: 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`.

Remarque: 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`.

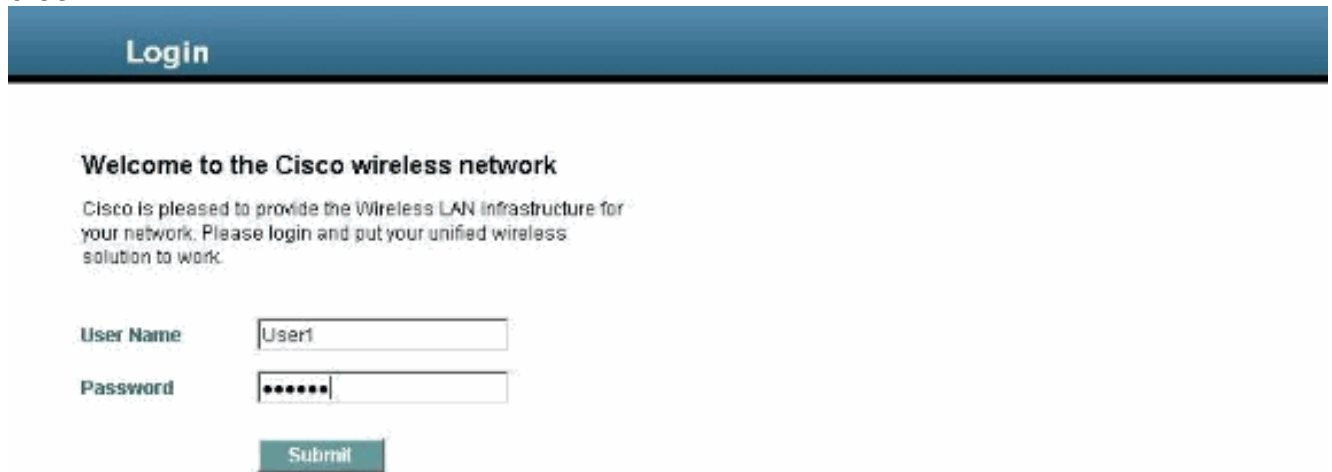
Si les clients sont associés à l'état `Webauth_Reqd`, qu'ils soient actifs ou inactifs, leur authentification sera annulée **après une période d'inactivité obligatoire web-auth** (par exemple, 300 secondes et ce délai n'est pas configurable par l'utilisateur). Tout le trafic du client (autorisé via l'ACL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



Login

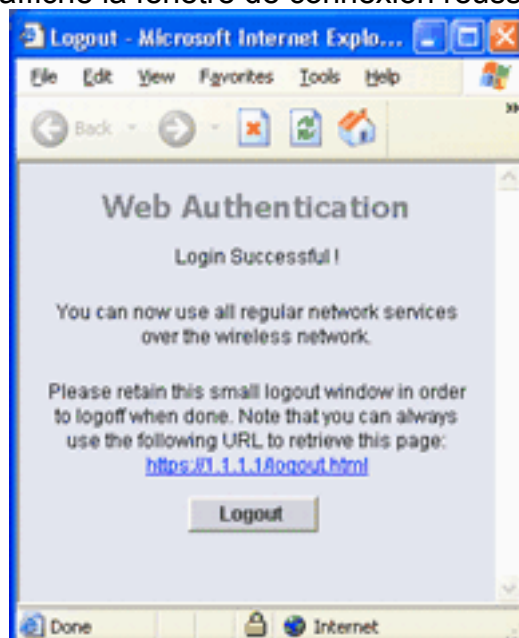
Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name:

Password:

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. La capture d'écran démontre une redirection réussie pour l'authentification Web. La capture d'écran suivante affiche la fenêtre de connexion réussie, qui indique lorsque



l'authentification a eu lieu.

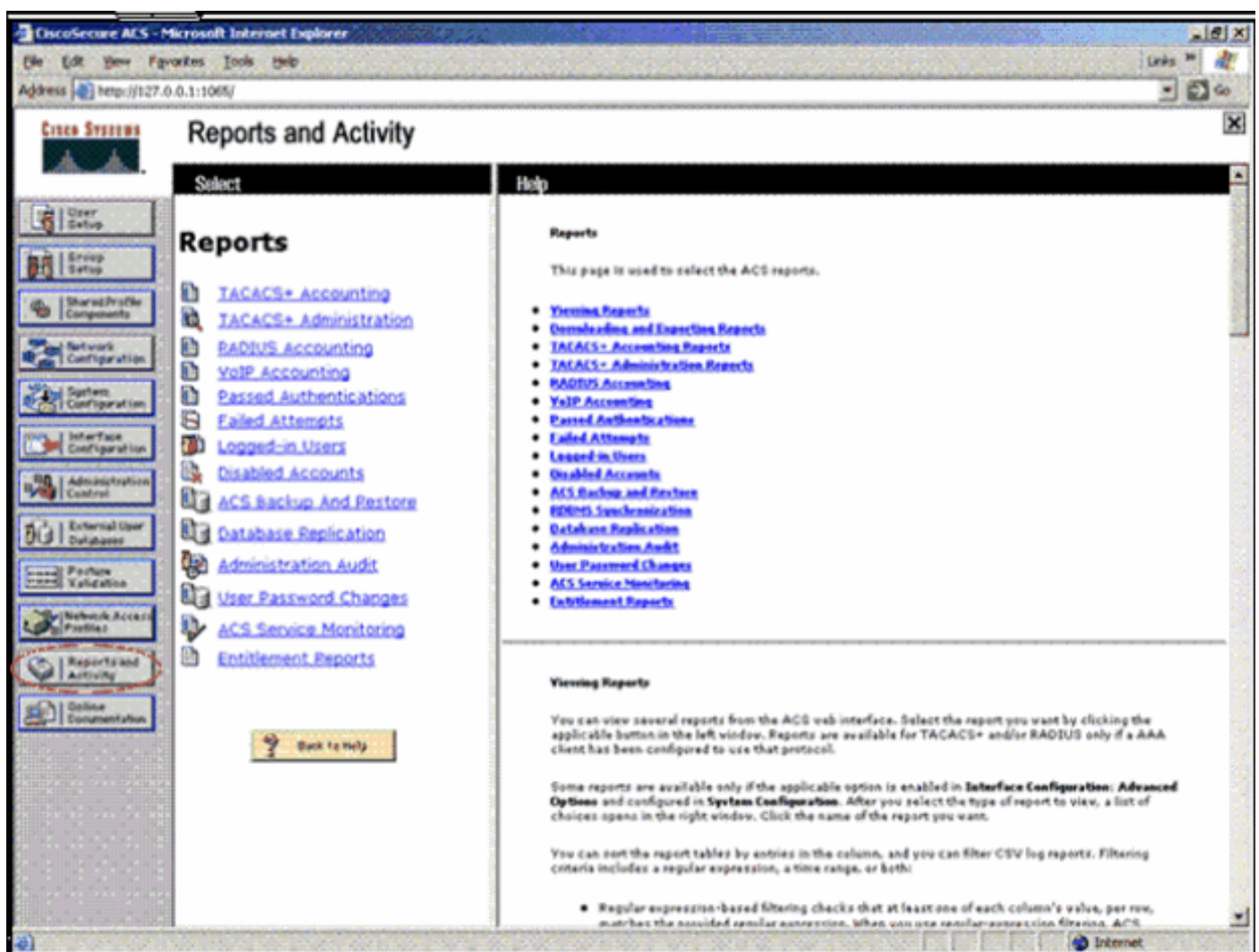
Les contrôleurs Cisco 4404/WiSM peuvent prendre en charge 125 connexions simultanées d'utilisateurs de l'authentification Web et évaluer jusqu'à 5 000 clients d'authentification Web.

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.



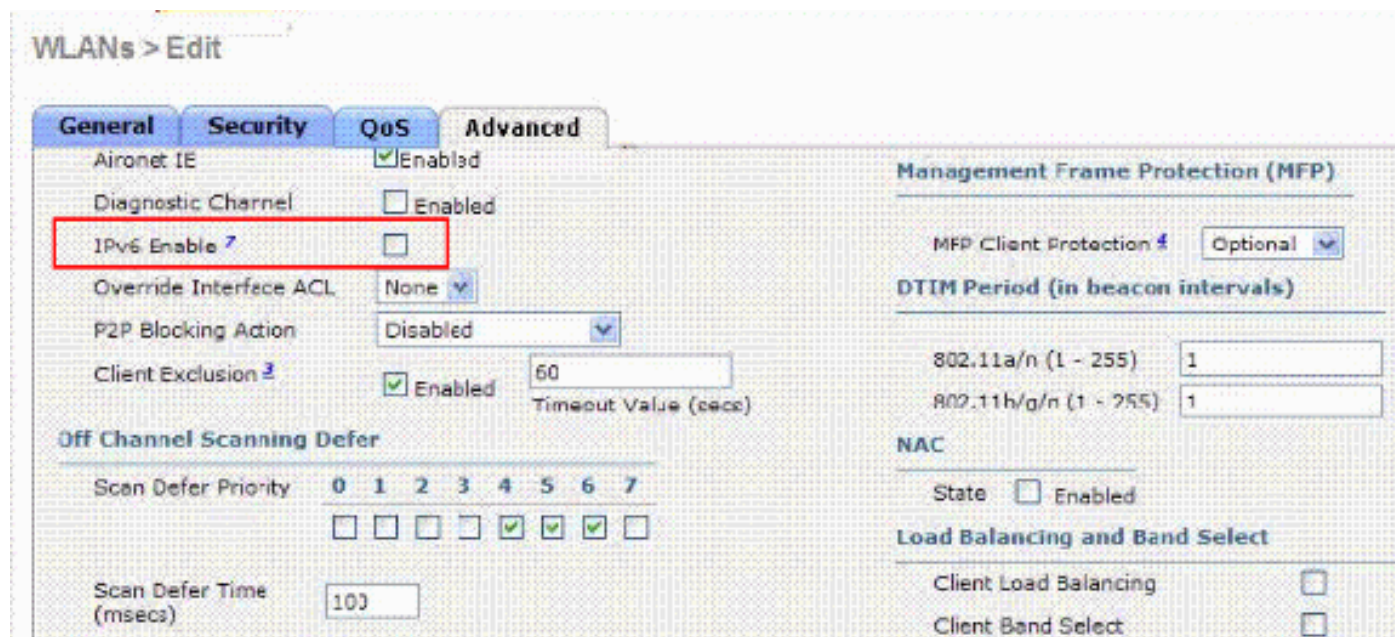
Remarque: Si vous entrez une URL externe, le WLC vous connecte automatiquement à la page d'authentification Web interne. Si la connexion automatique ne fonctionne pas, vous pouvez entrer l'adresse IP de gestion du WLC dans la barre d'URL afin d'effectuer le dépannage. Recherchez en haut du navigateur 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 réseau WLAN pour le pontage IPv6, depuis l'interface GUI du contrôleur, rendez-vous à la section **WLAN**. Puis, sélectionnez le WLAN désiré et choisissez **Avancé** dans la page **WLAN > Modifier**.

Sélectionnez la case d'**IPv6 autorisé** si vous voulez autoriser les clients qui se connectent à ce WLAN pour recevoir des paquets IPv6. Autrement, laissez la case non sélectionnée, ce qui est la valeur par défaut. Si vous désactivez (ou décochez) la case IPv6, l'autorisation d'IPv6 aura lieu seulement après l'authentification. L'activation d'IPv6 signifie que le contrôleur peut laisser circuler le trafic IPv6 sans authentification du client.



Pour plus d'informations sur le pontage d'IPv6 et les **directives pour l'utilisation de cette caractéristique**, référez-vous à la section sur [la configuration de pontage d'IPv6](#) du [guide de configuration du contrôleur LAN sans fil 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](#)