Exemple de configuration de redirection de page de démarrage sur les contrôleurs de réseau local sans fil

Table des matières

Introduction

Ce document décrit comment configurer la fonction de redirection de la page d'accueil sur les contrôleurs de réseau local sans fil.

Conditions préalables

Exigences

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

- Connaissance des solutions de sécurité LWAPP
- Connaissance de la configuration de Cisco Secure ACS

Composants utilisés

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

- Contrôleur LAN sans fil (WLC) de la gamme Cisco 4400 qui exécute la version 5.0 du microprogramme
- Point d'accès léger Cisco 1232 (LAP)
- Adaptateur client sans fil Cisco Aironet 802.a/b/g qui exécute la version 4.1 du microprogramme
- Serveur Cisco Secure ACS qui exécute la version 4.1
- Tout serveur Web externe tiers

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

La redirection Web de la page d'accueil est une fonctionnalité introduite avec le contrôleur LAN sans fil version 5.0. Grâce à cette fonctionnalité, l'utilisateur est redirigé vers une page Web particulière une fois l'authentification 802.1x terminée. La redirection se produit lorsque l'utilisateur ouvre un navigateur (configuré avec une page d'accueil par défaut) ou tente d'accéder à une URL. Une fois la redirection vers la page Web terminée, l'utilisateur a un accès complet au réseau.

Vous pouvez spécifier la page de redirection sur le serveur RADIUS (Remote Authentication Dial-In User Service). Le serveur RADIUS doit être configuré pour renvoyer l'attribut RADIUS de redirection d'URL de Cisco av-pair au contrôleur LAN sans fil après une authentification 802.1x réussie.

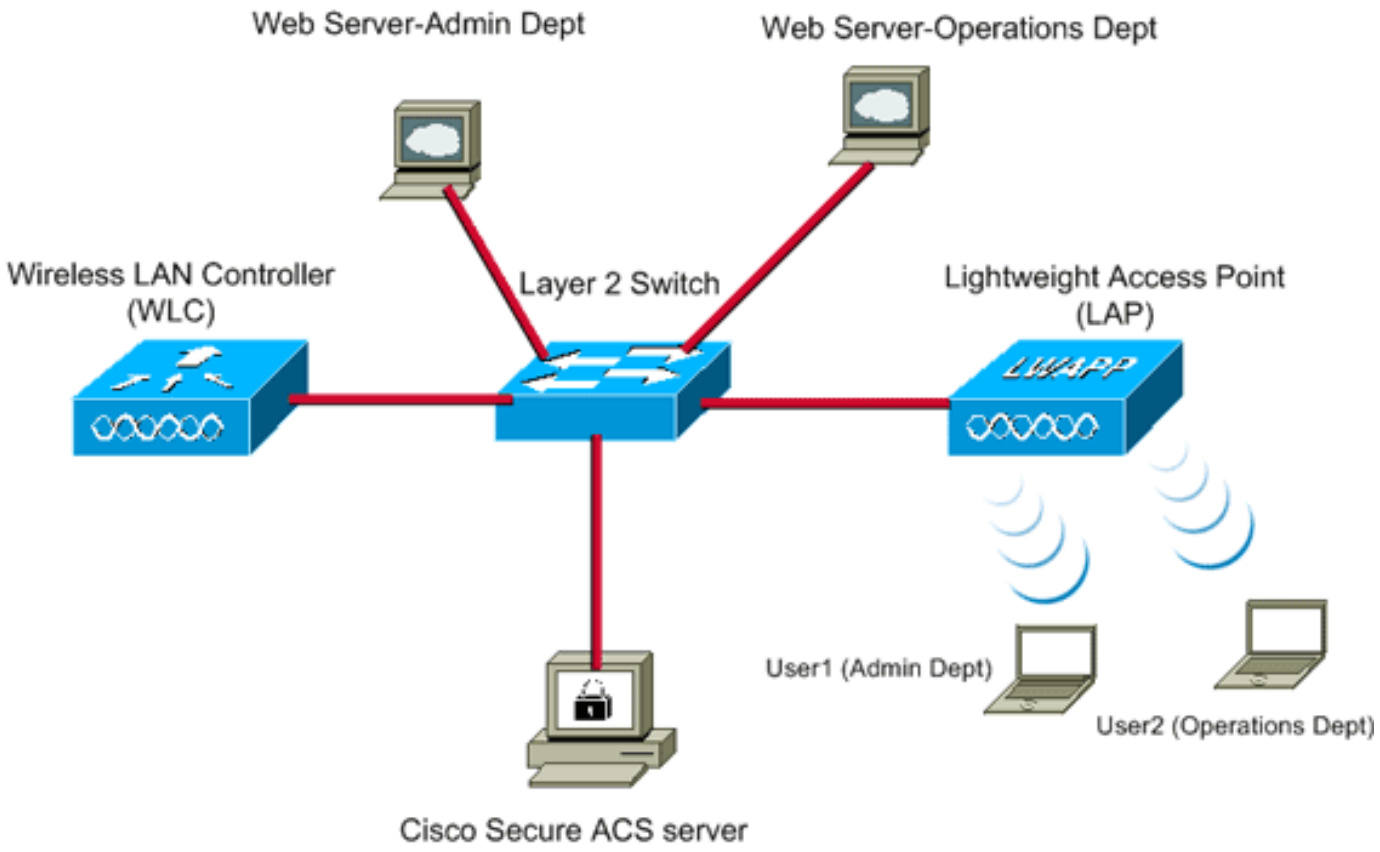
La fonction de redirection Web de la page de démarrage est disponible uniquement pour les réseaux locaux sans fil configurés pour la sécurité de couche 2 802.1x ou WPA/WPA2.

Configuration du réseau

Dans cet exemple, un WLC Cisco 4404 et un LAP Cisco 1232 sont connectés via un commutateur de couche 2. Le serveur Cisco Secure ACS (qui fait office de serveur RADIUS externe) est également connecté au même commutateur. Tous les périphériques se trouvent dans le même sous-réseau.

Le LAP est initialement enregistré auprès du contrôleur. Vous devez créer deux WLAN : l'un pour les utilisateurs du **service d'administration** et l'autre pour les utilisateurs du **service des opérations**. Les deux réseaux locaux sans fil utilisent WPA2/AES (EAP-FAST est utilisé pour l'authentification). Les deux WLAN utilisent la fonctionnalité de redirection de page d'accueil afin de rediriger les utilisateurs vers les URL de page d'accueil appropriées (sur des serveurs Web externes).

Ce document utilise la configuration réseau suivante :



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

La section suivante explique comment paramétrer les périphériques pour cette configuration.

Configurer

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

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Complétez ces étapes afin de configurer les périphériques pour utiliser la fonctionnalité de redirection de la page de démarrage :

1. Configurez le WLC pour l'authentification RADIUS via le serveur Cisco Secure ACS.
2. Configurez les réseaux locaux sans fil pour les services Admin et Operations.
3. Configurez Cisco Secure ACS pour prendre en charge la fonction de redirection de la page de démarrage.

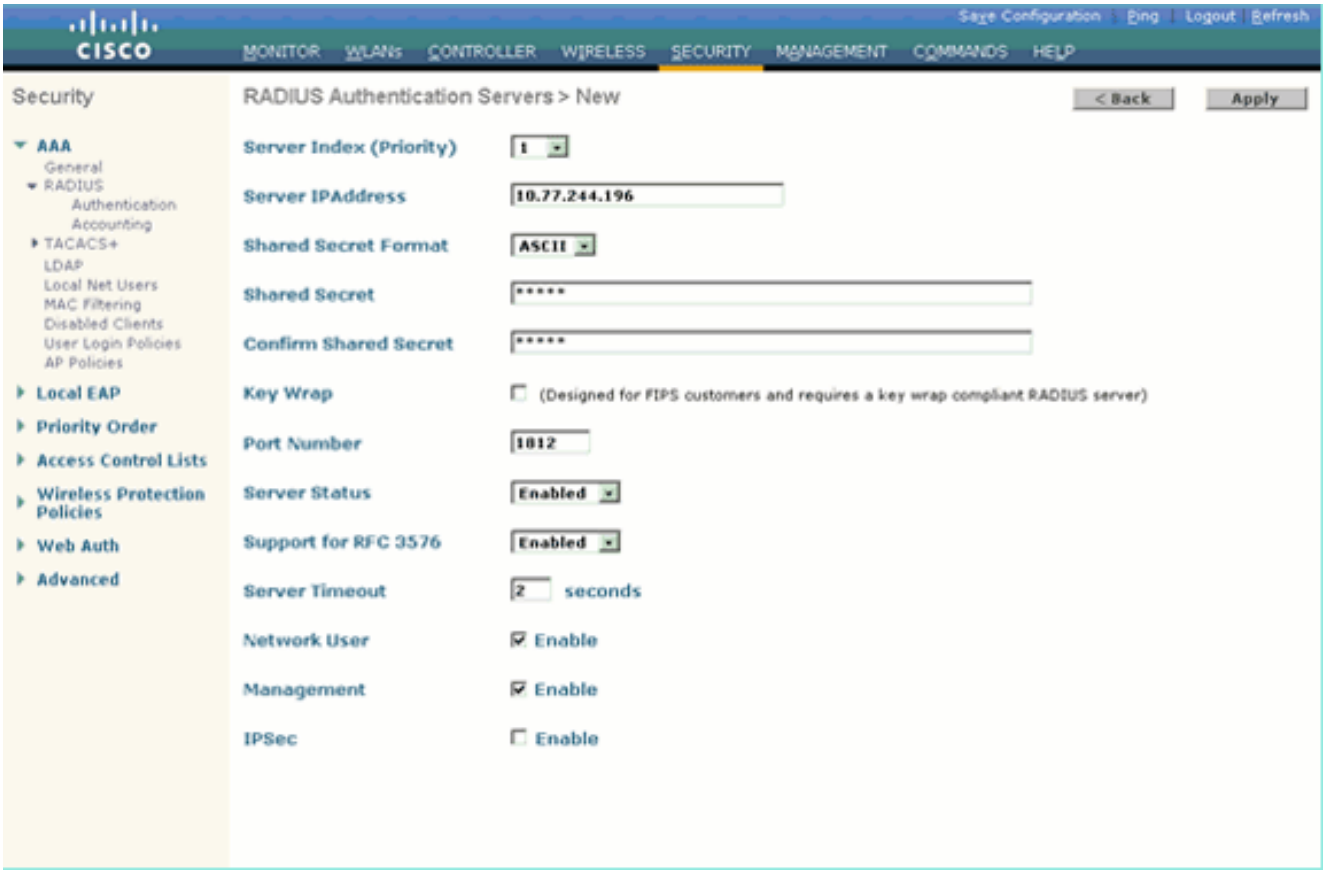
Étape 1. Configurez le WLC pour l'authentification RADIUS via le serveur Cisco

Secure ACS.

WLC doit être configuré afin de transférer les identifiants de l'utilisateur à un serveur RADIUS externe.

Complétez ces étapes pour configurer le WLC pour un serveur RADIUS externe :

1. Choisissez **Security** and **RADIUS Authentication** dans la GUI du contrôleur afin d'afficher la page RADIUS Authentication Servers.
2. Cliquez sur **New** afin de définir un serveur RADIUS.
3. Définissez les paramètres du serveur RADIUS sur la page RADIUS Authentication Servers > New.Ces paramètres incluent :Adresse IP du serveur RADIUSSecret partagéPort number (numéro de port) État du serveur



Ce document utilise le serveur ACS avec l'adresse IP 10.77.244.196.

4. Cliquez sur **Apply**.

Étape 2. Configurez les réseaux locaux sans fil pour le service Admin et Operations.

Au cours de cette étape, vous allez configurer les deux réseaux locaux sans fil (un pour le service Admin et l'autre pour le service Operations) que les clients utiliseront pour se connecter au réseau sans fil.

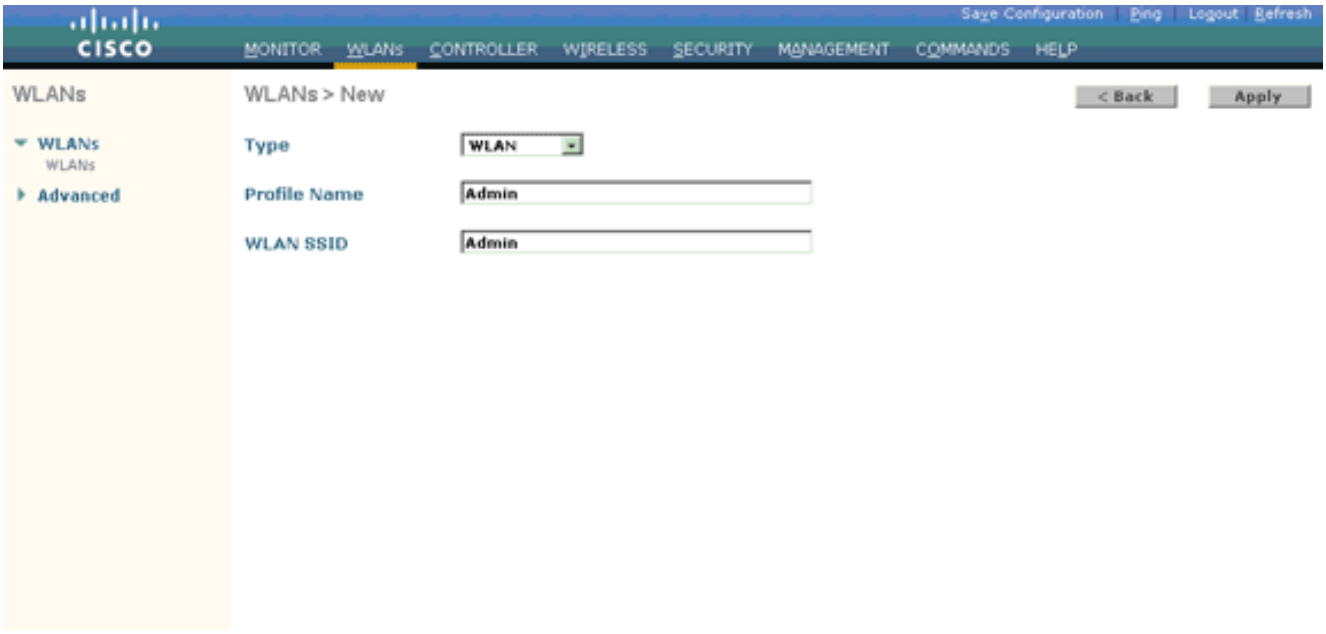
Le SSID du WLAN pour le service Admin sera *Admin*. Le SSID WLAN du service des opérations sera Operations (Opérations).

Utilisez l'authentification EAP-FAST afin d'activer WPA2 en tant que mécanisme de sécurité de couche 2 sur les WLAN et la politique Web - fonction de redirection Web de page d'accueil en tant

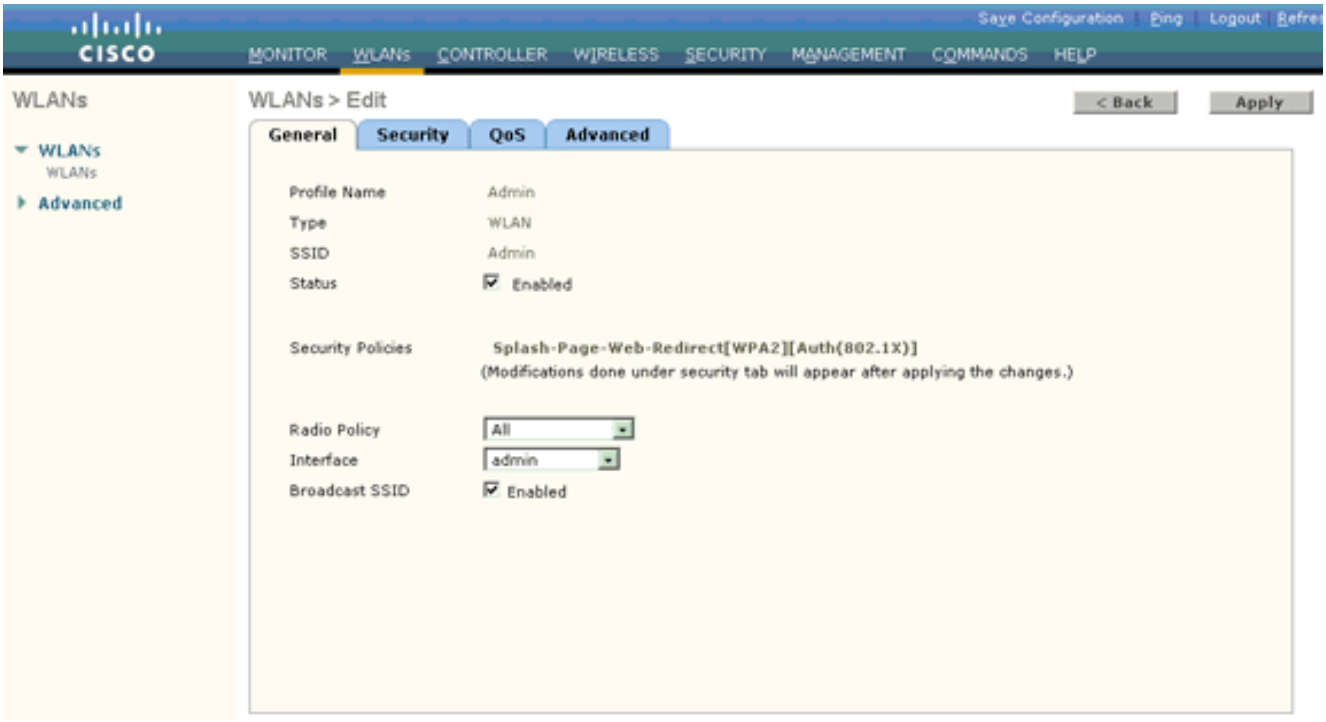
que méthode de sécurité de couche 3.

Complétez ces étapes afin de configurer le WLAN et ses paramètres associés :

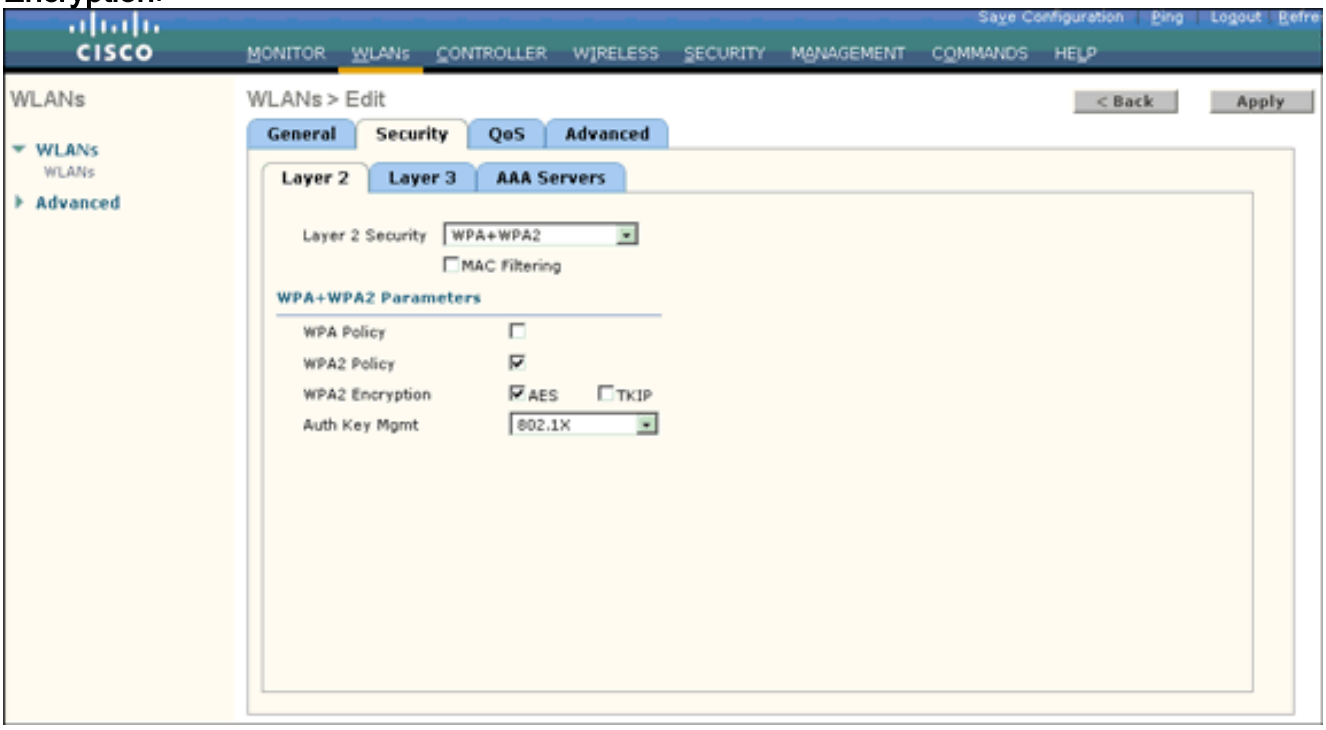
1. Cliquez sur les **WLAN de la GUI du contrôleur afin d'afficher la page des WLAN.**Cette page énumère les WLAN qui existent sur le contrôleur.
2. Cliquez sur New [nouveau] pour créer un autre WLAN.



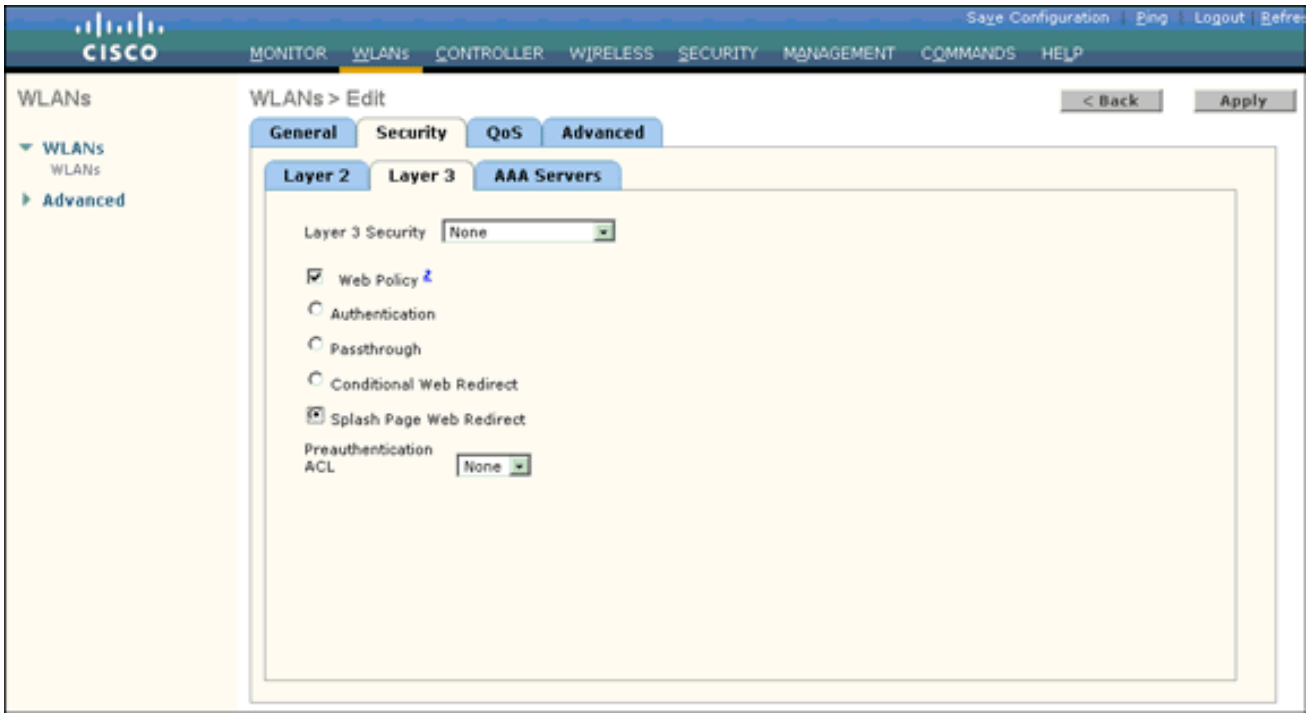
3. Saisissez le nom SSID du WLAN et le nom du profil sur la page WLANs > New.
4. Cliquez sur **Apply**.
5. Commençons par créer le WLAN pour le service Admin.Une fois que vous avez créé un nouveau WLAN, la page WLAN > Edit du nouveau WLAN apparaît. Sur cette page, vous pouvez définir divers paramètres spécifiques à ce WLAN. Cela inclut les stratégies générales, les stratégies de sécurité, les stratégies QOS et les paramètres avancés.
6. Sous General Policies, cochez la case **Status** afin d'activer le WLAN.



7. Cliquez sur l'onglet **Security**, puis sur l'onglet **Layer 2**.
8. Choisissez **WPA+WPA2** dans la liste déroulante Layer 2 Security.Cette étape active l'authentification WPA pour le WLAN.
9. Sous WPA+WPA2 Parameters, cochez les cases **WPA2 Policy** et **AES Encryption**.

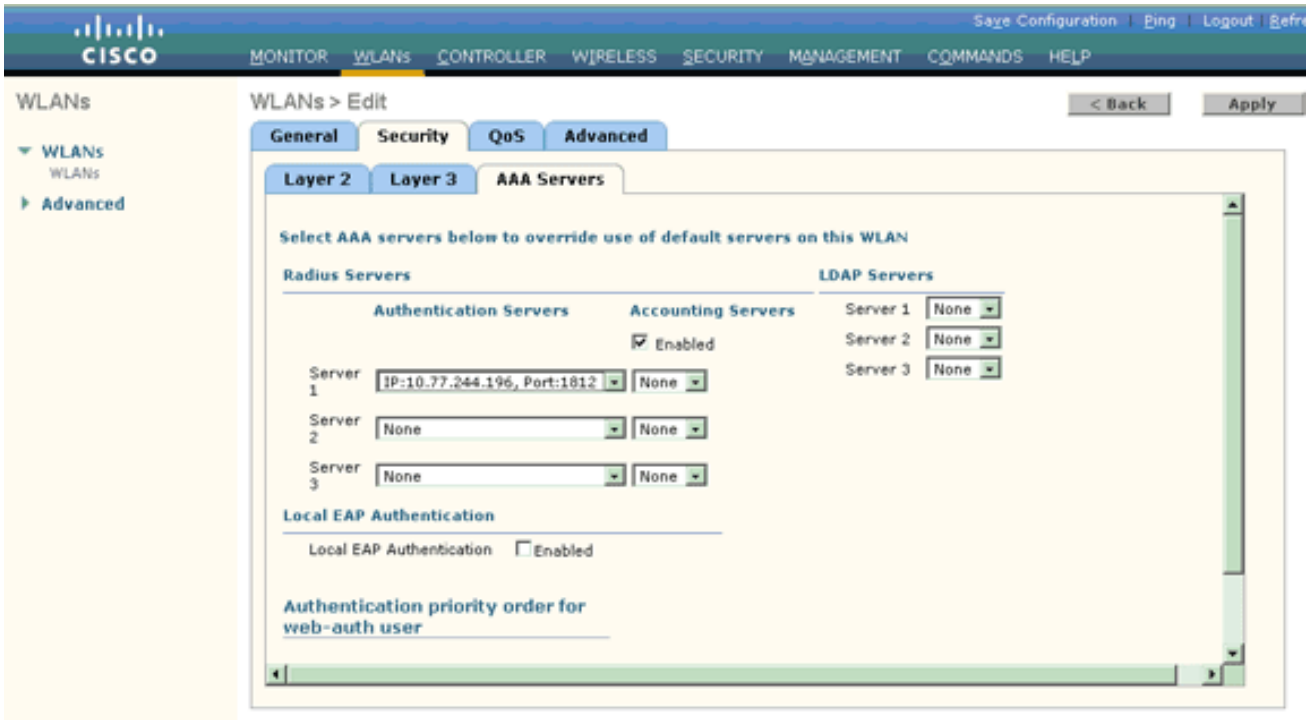


10. Choisissez **802.1x** dans la liste déroulante Auth Key Mgmt. Cette option active WPA2 avec authentification 802.1x/EAP et cryptage AES pour le WLAN.
11. Cliquez sur l'onglet **Layer 3 Security**.
12. Cochez la case **Web Policy**, puis cliquez sur la case d'option **Splash Page Web Redirect**.Cette option active la fonction de redirection Web de la page d'accueil.



13. Cliquez sur l'onglet **AAA Servers**.
14. Sous Authentication Servers, choisissez l'adresse IP du serveur approprié dans la liste déroulante Server

1.



Dans cet exemple, 10.77.244.196 est utilisé comme serveur RADIUS.

15. Cliquez sur **Apply**.
16. Répétez les étapes 2 à 15 afin de créer le WLAN pour le service des opérations.La page WLANs répertorie les deux WLAN que vous avez créés.

Notez que les stratégies de sécurité incluent la redirection de la page de démarrage.

Étape 3. Configurez Cisco Secure ACS pour prendre en charge la fonction de redirection de la page de démarrage.

L'étape suivante consiste à configurer le serveur RADIUS pour cette fonctionnalité. Le serveur RADIUS doit effectuer l'authentification EAP-FAST afin de valider les informations d'identification du client, et après une authentification réussie, pour rediriger l'utilisateur vers l'URL (sur le serveur Web externe) spécifiée dans l'attribut Cisco av-pair ***url-redirect*** RADIUS.

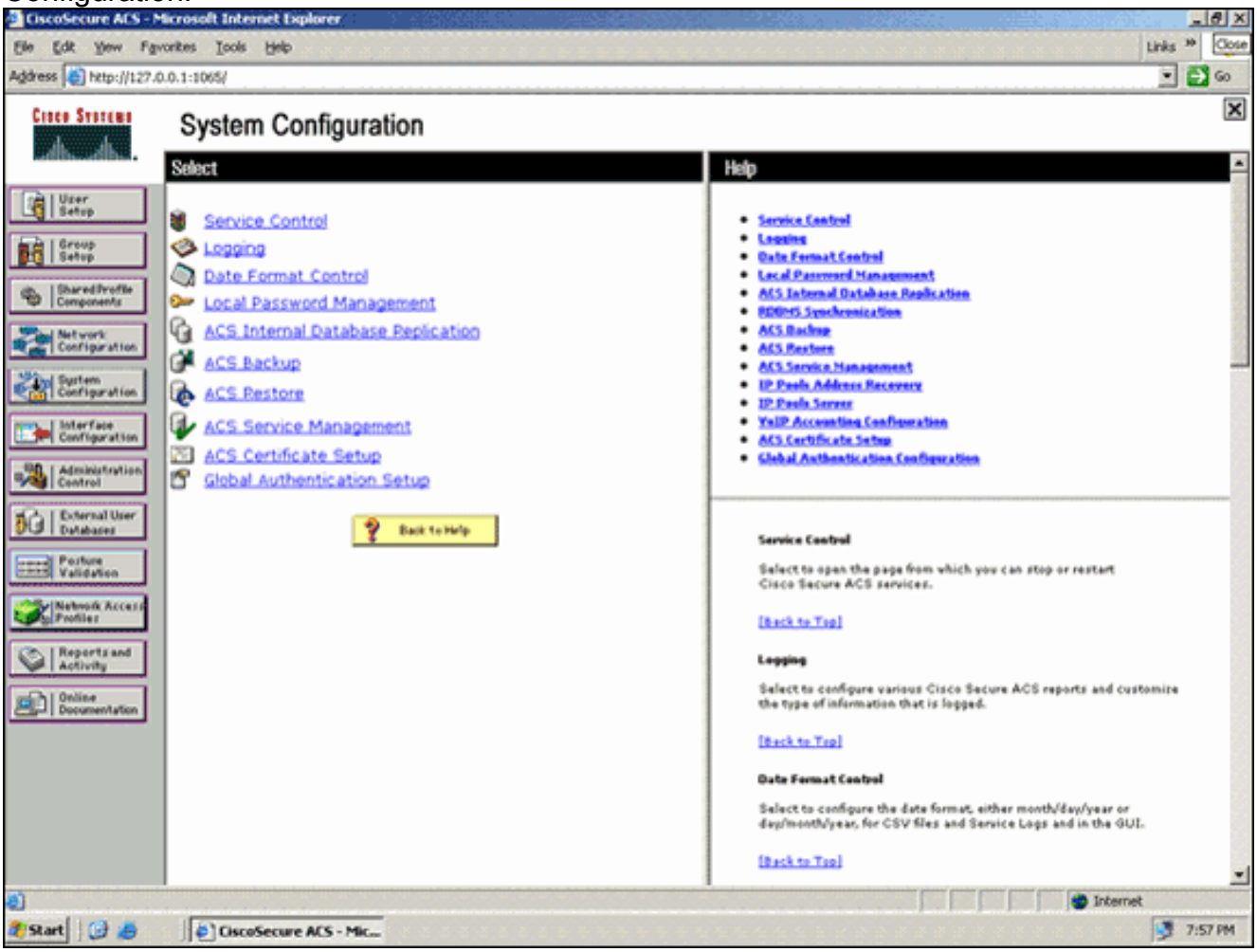
Configuration de Cisco Secure ACS pour l'authentification EAP-FAST

Remarque : ce document suppose que le contrôleur LAN sans fil est ajouté à Cisco Secure ACS

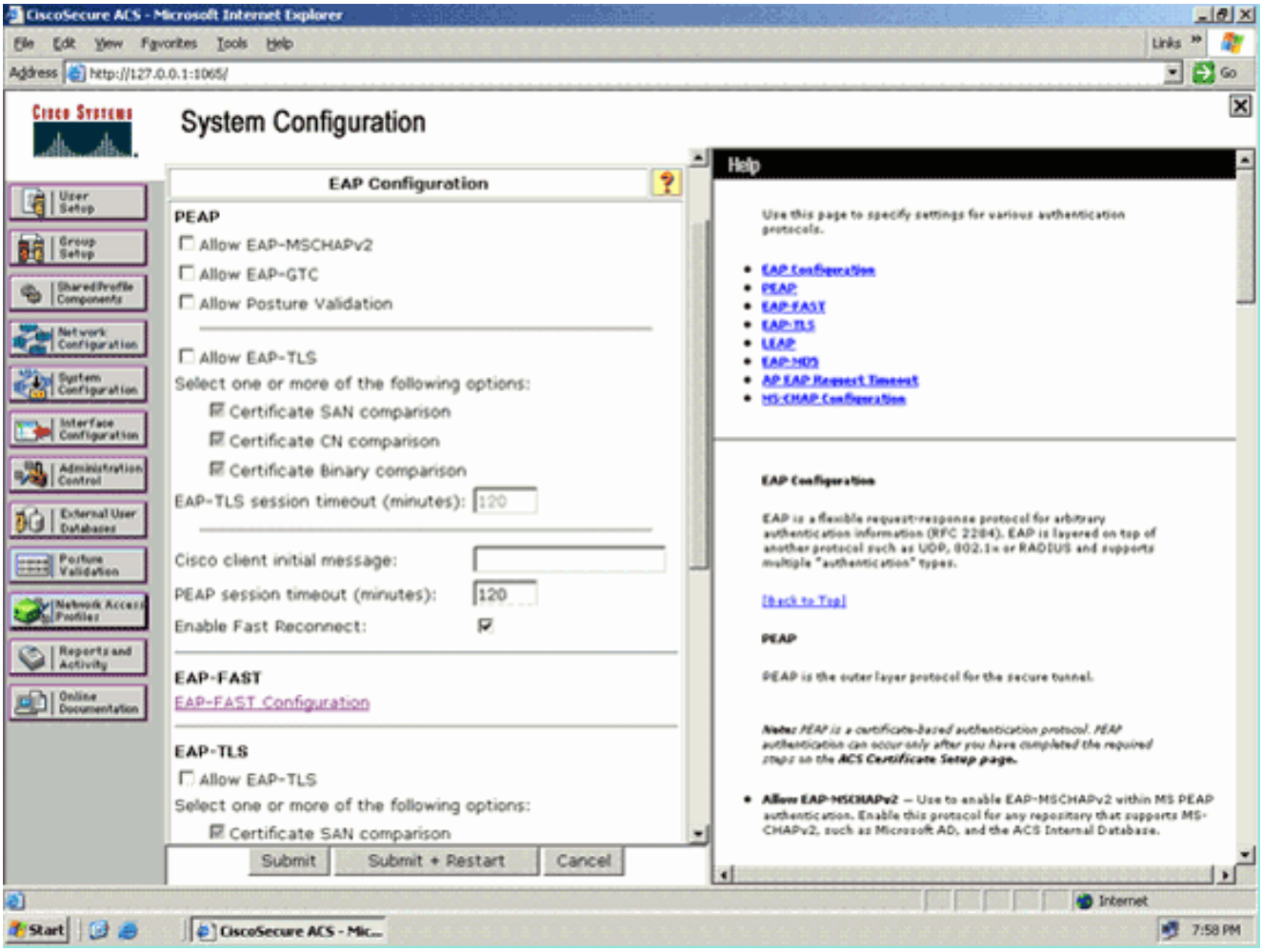
en tant que client AAA.

Complétez ces étapes afin de configurer l'authentification EAP-FAST dans le serveur RADIUS :

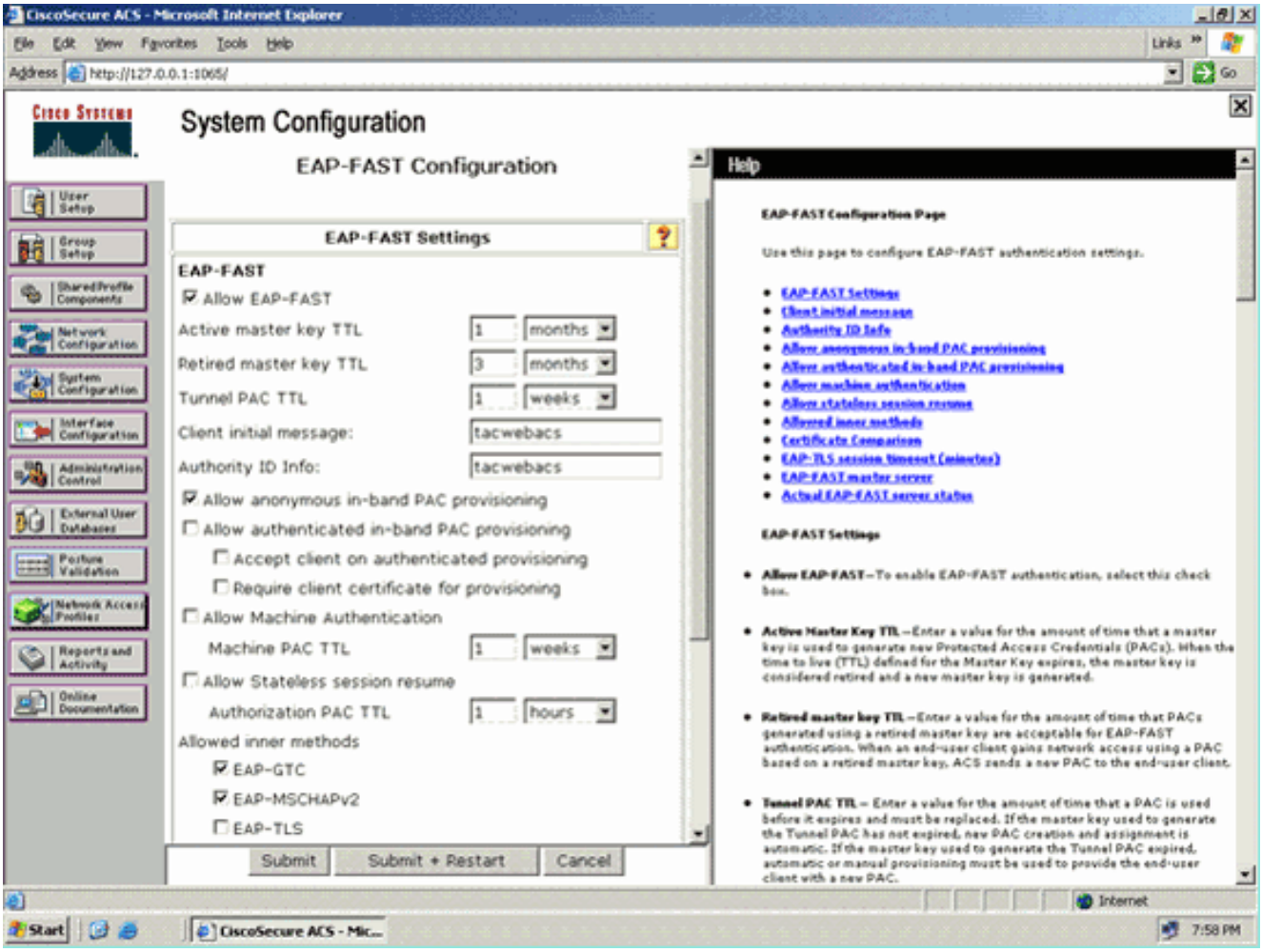
1. Cliquez sur **System Configuration** dans l'interface utilisateur graphique du serveur RADIUS, puis choisissez **Global Authentication Setup** dans la page System Configuration.



2. Dans la page de configuration de l'authentification globale, cliquez sur **EAP-FAST Configuration** afin d'accéder à la page des paramètres EAP-FAST.



3. Dans la page EAP-FAST Settings, cochez la case **Allow EAP-FAST** afin d'activer EAP-FAST dans le serveur
RADIUS.



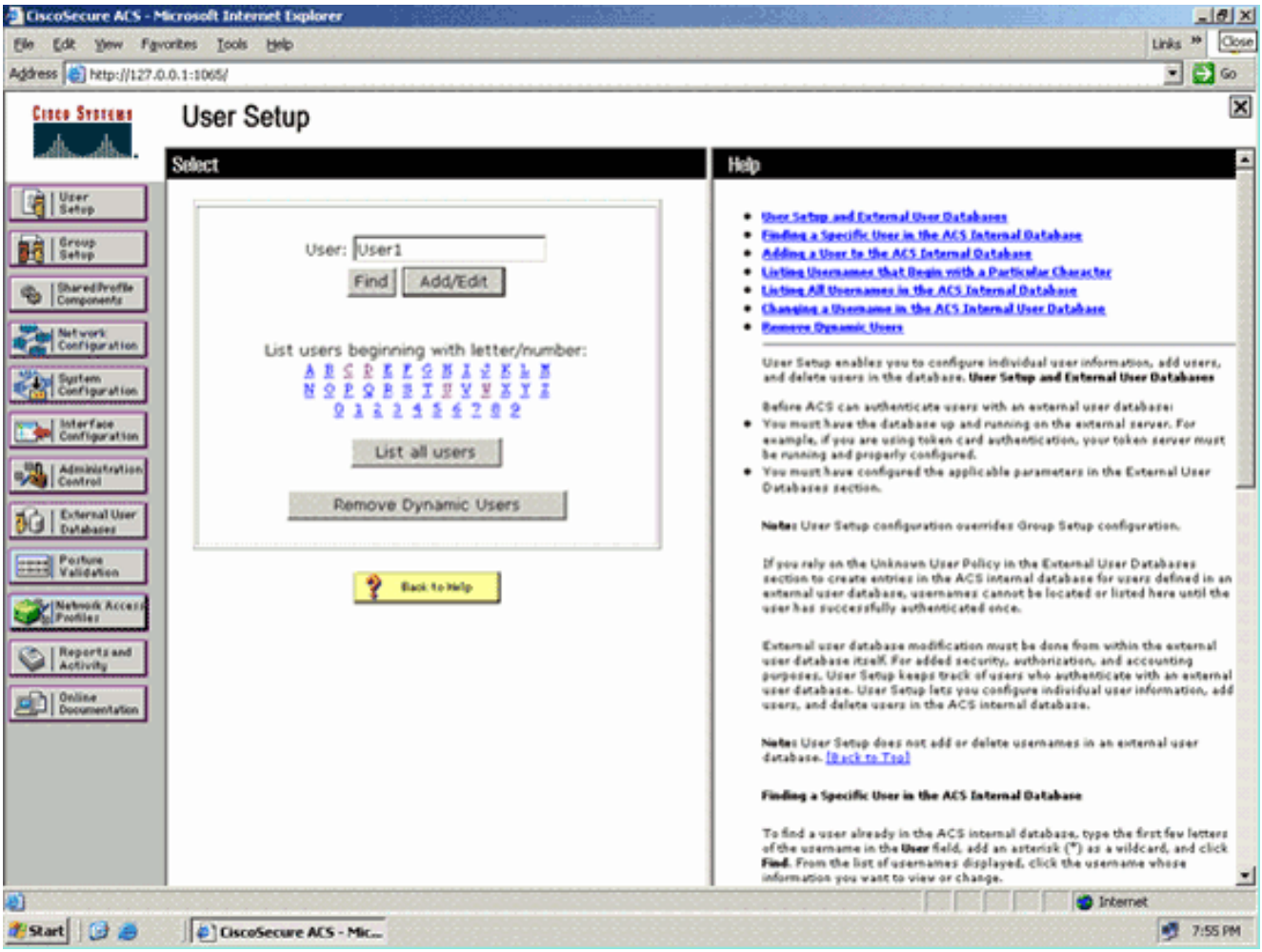
4. Configurez les valeurs TTL (Time-to-Live) de la clé principale active/retirée comme vous le souhaitez, ou définissez-la sur la valeur par défaut, comme indiqué dans cet exemple.Le champ ID d'autorité Info représente l'identité textuelle de ce serveur ACS, qu'un utilisateur final peut utiliser pour déterminer le serveur ACS à authentifier. Il est obligatoire de renseigner ce champ.Le champ Client initial display message spécifie un message à envoyer aux utilisateurs qui s'authentifient auprès d'un client EAP-FAST. La longueur maximale est de 40 caractères. Un utilisateur ne verra le message initial que si le client de l'utilisateur final prend en charge l'affichage.
5. Si vous voulez que l'ACS effectue le provisionnement PAC dans la bande anonyme, cochez la case **Autoriser le provisionnement PAC dans la bande anonyme**.
6. L'option *Allowed inner methods* détermine quelles méthodes EAP internes peuvent s'exécuter à l'intérieur du tunnel EAP-FAST TLS. Pour l'approvisionnement en bande anonyme, vous devez activer EAP-GTC et EAP-MS-CHAP pour la rétrocompatibilité. Si vous sélectionnez Allow anonymous in-band PAC provisioning, vous devez sélectionner EAP-MS-CHAP (phase zéro) et EAP-GTC (phase deux).
7. Cliquez sur Submit.**Remarque :** pour obtenir des informations détaillées et des exemples sur la façon de configurer EAP FAST avec la mise en service PAC intrabande anonyme et la mise en service intrabande authentifiée, reportez-vous à Exemple de configuration d'authentification EAP-FAST avec des contrôleurs LAN sans fil et un serveur RADIUS externe.

Configurez la base de données User et définissez l'attribut *url-redirect* RADIUS

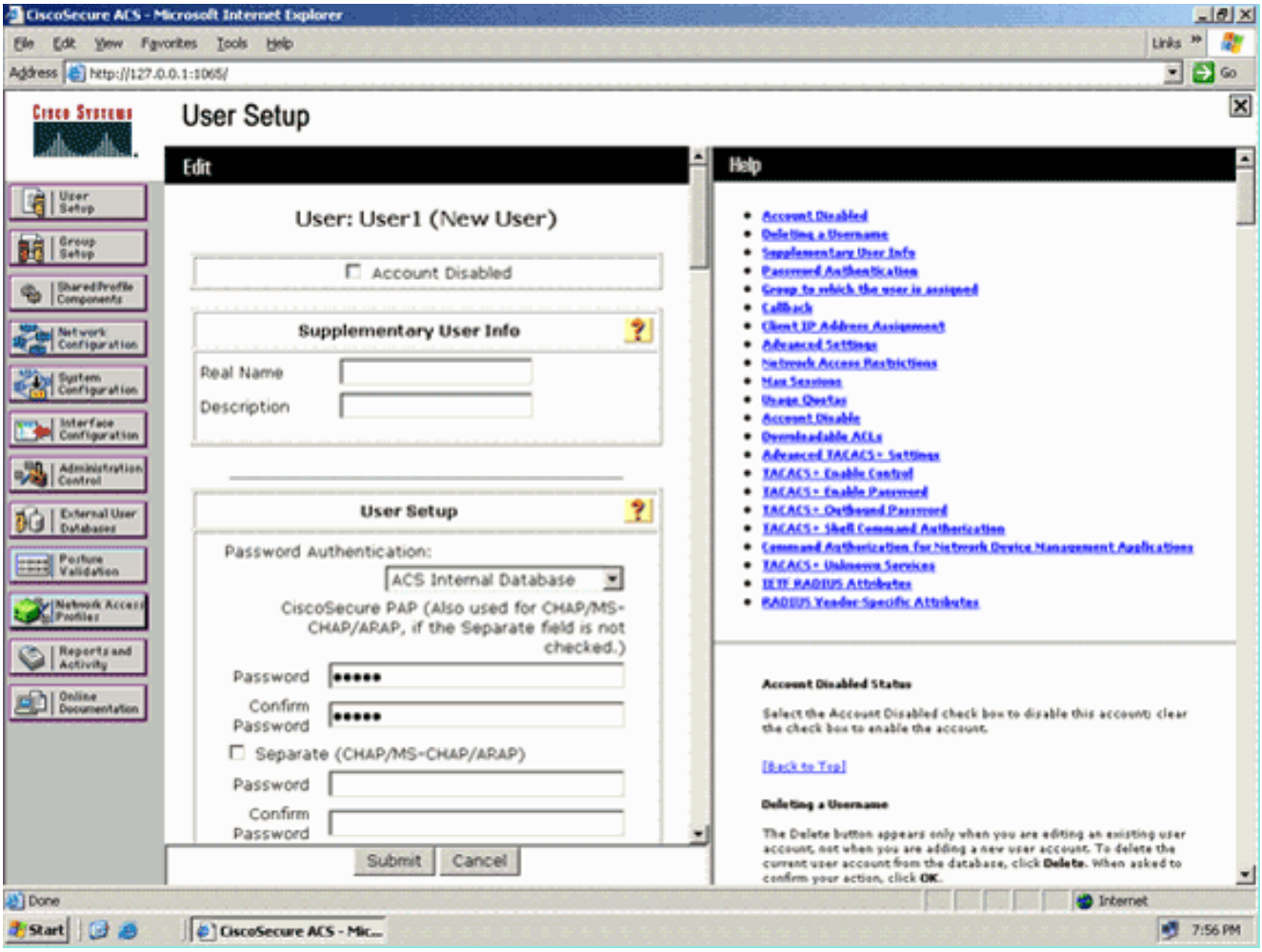
Cet exemple configure le nom d'utilisateur et le mot de passe du client sans fil en tant qu'Utilisateur1 et Utilisateur1, respectivement.

Complétez ces étapes afin de créer une base de données utilisateur :

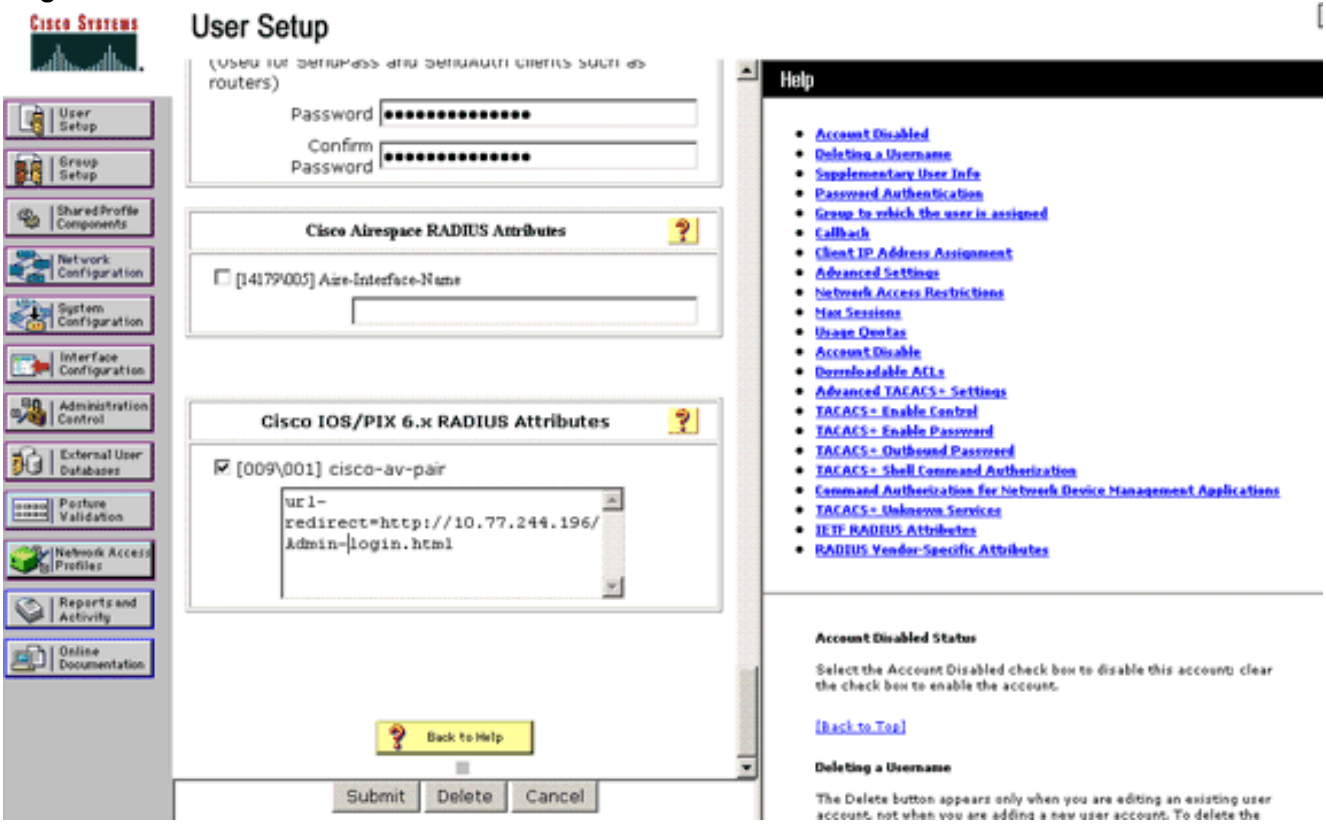
1. Dans la barre de navigation de l'interface graphique utilisateur ACS, sélectionnez **User Setup**.
2. Créez un nouvel utilisateur sans fil, puis cliquez sur **Add/Edit** afin d'accéder à la page Edit de cet
   utilisateur.



3. Dans la page User Setup Edit, configurez Real Name et Description, ainsi que les paramètres Password, comme indiqué dans cet exemple.Ce document utilise la base de données interne ACS pour l'authentification par mot de
   passe.



4. Faites défiler la page vers le bas pour modifier les attributs RADIUS.
5. Cochez la case **[009\001] cisco-av-pair**.
6. Entrez ces paires av Cisco dans la zone d'édition [009\001] cisco-av-pair afin de spécifier l'URL vers laquelle l'utilisateur est redirigé :url-redirect=http://10.77.244.196/Admin-Login.html



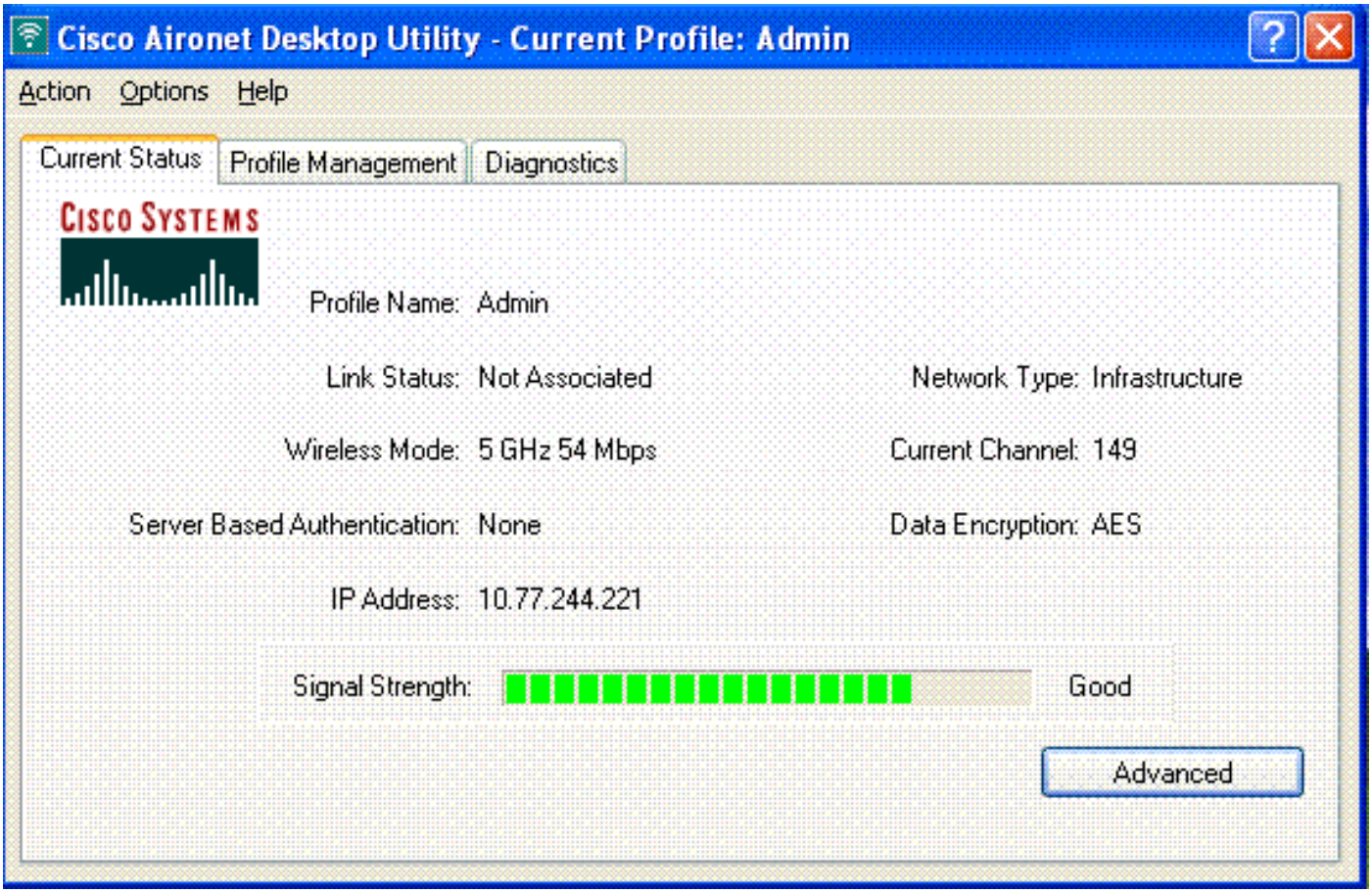
Il s'agit de la page d'accueil des utilisateurs du service Admin.

7. Cliquez sur Submit.
8. Répétez cette procédure afin d'ajouter User2 (utilisateur du service Opérations).
9. Répétez les étapes 1 à 6 afin d'ajouter d'autres utilisateurs du service d'administration et du service des opérations à la base de données.**Remarque :** les attributs RADIUS peuvent être configurés au niveau utilisateur ou au niveau groupe sur Cisco Secure ACS.

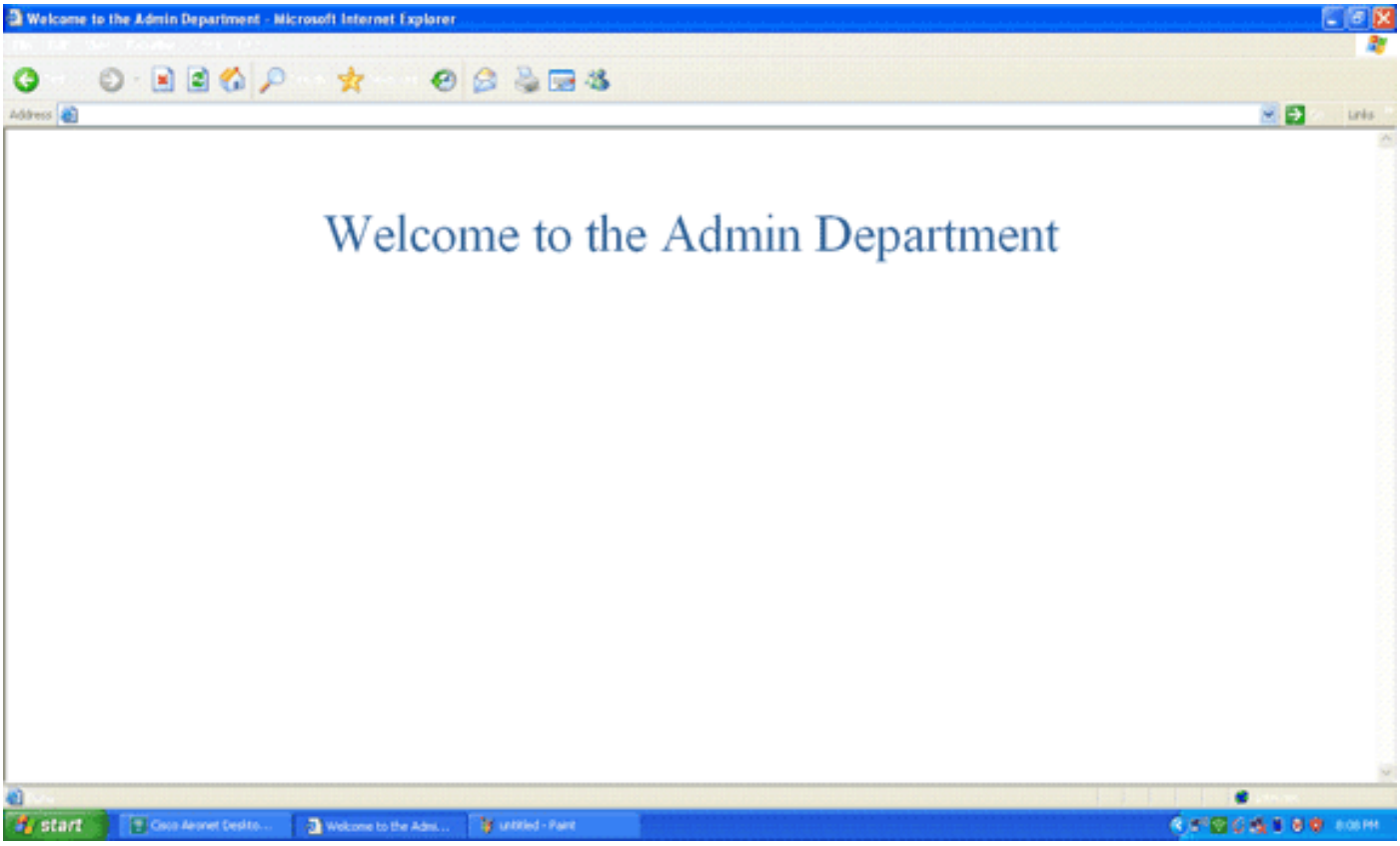
Vérifier

Afin de vérifier la configuration, associez un client WLAN du service Admin et du service Operations à leurs WLAN appropriés.

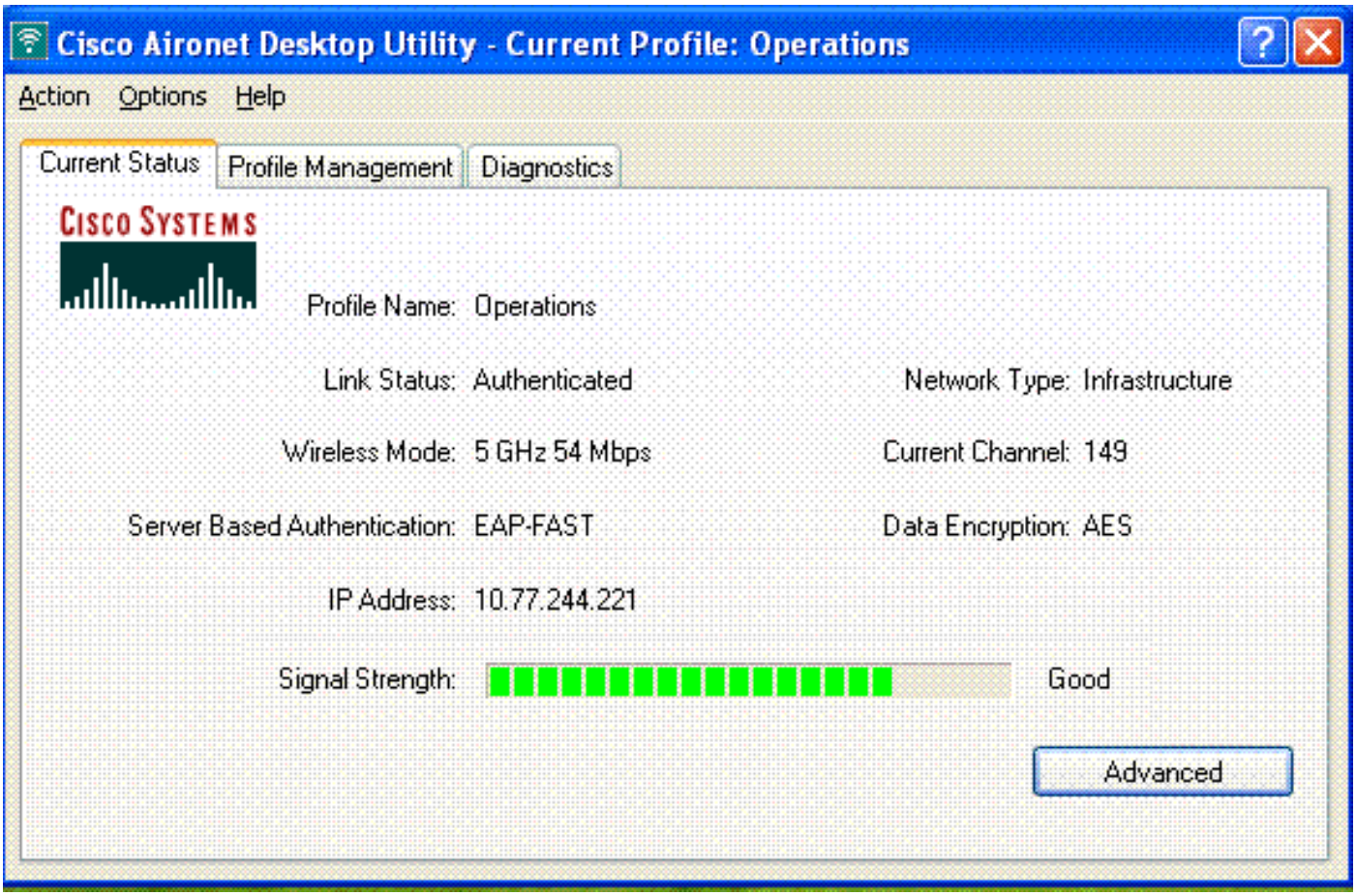
Lorsqu'un utilisateur du service Admin se connecte à l'administrateur du réseau local sans fil, il est invité à fournir des informations d'identification 802.1x (dans notre cas, des informations d'identification EAP-FAST). Une fois que l'utilisateur a fourni les informations d'identification, le WLC les transmet au serveur Cisco Secure ACS. Le serveur Cisco Secure ACS valide les informations d'identification de l'utilisateur par rapport à la base de données et, après authentification réussie, renvoie l'attribut url-redirect au contrôleur de réseau local sans fil. L'authentification est terminée à ce stade.

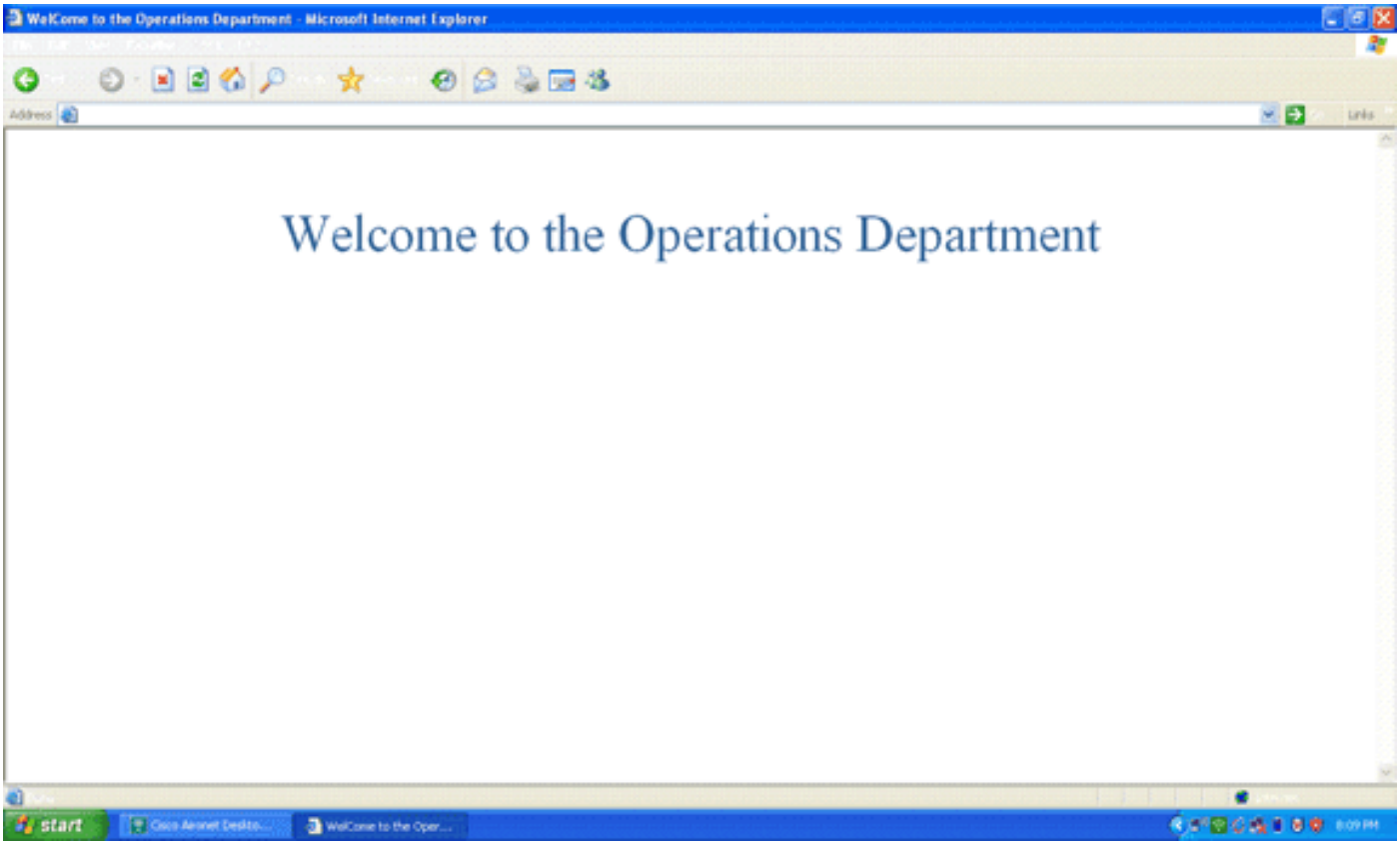


Lorsque l'utilisateur ouvre un navigateur Web, il est redirigé vers l'URL de la page d'accueil du service Admin. (Cette URL est retournée au WLC via l'attribut cisco-av-pair). Une fois la redirection effectuée, l'utilisateur dispose d'un accès complet au réseau. Voici les captures d'écran :



Les mêmes séquences d'événements se produisent lorsqu'un utilisateur du service des opérations se connecte au service des opérations du réseau local sans fil.





Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

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

Vous pouvez utiliser les commandes suivantes pour dépanner votre configuration.

- **show wlan wlan_id** : affiche l'état des fonctions de redirection Web pour un WLAN particulier.Voici un exemple :

```
WLAN Identifier.................................. 1
Profile Name..................................... Admin
Network Name (SSID).............................. Admin
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
```

- **debug dot1x events enable** : active le débogage des messages de paquets 802.1x.Voici un exemple :

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
    mobile 00:40:96:ac:dd:05 (EAP Id 16)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
    mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
    seconds, got from WLAN config.
```

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
    setting dot1x reauth timeout = 1800
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
    for station 00:40:96:ac:dd:05 (RSN 2)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
    to PMKID cache for station 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: New PMKID: (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
    lifetime can take care of same.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
    00:40:96:ac:dd:05 (EAP Id 17)
Fri Feb 29 10:27:16 2008: Including PMKID in M1  (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
    mobile 00:40:96:ac:dd:05
    state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
    in Authenticating state for mobile 00:40:96:ac:dd:05
```

- **debug aaa events enable** : active la sortie de débogage de tous les événements aaa.Voici un exemple :

```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
    'http://10.77.244.196/Admin-login.html' set
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
    station 00:40:96:ac:dd:05
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
    00:40:96:ac:dd:05
       source: 4, valid bits: 0x0
       qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
       dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
       vlanIfName: '', aclName: '
```

Informations connexes

- Guide de configuration du contrôleur de réseau local sans fil Cisco, version 5.0
- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Page de prise en charge du mode sans fil
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.