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

Contenu

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

Conditions requises

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

- La connaissance des solutions de sécurité LWAPP
- La connaissance de la façon configurer le Cisco Secure ACS

Composants utilisés

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

- Le contrôleur LAN sans fil de la gamme Cisco 2100 (WLC) ce exécute la version 5.0 de micrologiciels
- Point d'accès léger (LAP) de gamme Cisco 1232
- Adaptateur client sans fil de Cisco Aironet 802.a/b/g qui exécute la version 4.1 de micrologiciels
- Serveur de Cisco Secure ACS qui exécute la version 4.1
- Tout tiers web server externe

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

Conventions

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

Informations générales

Le Web de page de splash réorientent est une fonctionnalité introduite avec la version 5.0 Sans fil de contrôleur LAN. Avec cette configuration, l'utilisateur est réorienté à une page Web particulière après que l'authentification de 802.1x se soit terminée. La réorientation se produit quand l'utilisateur ouvre un navigateur (configuré avec une page d'accueil par défaut) ou des essais pour accéder à un URL. Après le redirect to que la page Web est complète, l'utilisateur a l'accès complet au réseau.

Vous pouvez spécifier la page de réorientation sur le serveur de Service RADIUS (Remote Authentication Dial-In User Service). Le serveur de RADIUS devrait être configuré pour renvoyer les poids du commerce-paires de Cisco URL-réorientent l'attribut RADIUS au contrôleur LAN Sans fil sur l'authentification réussie de 802.1x.

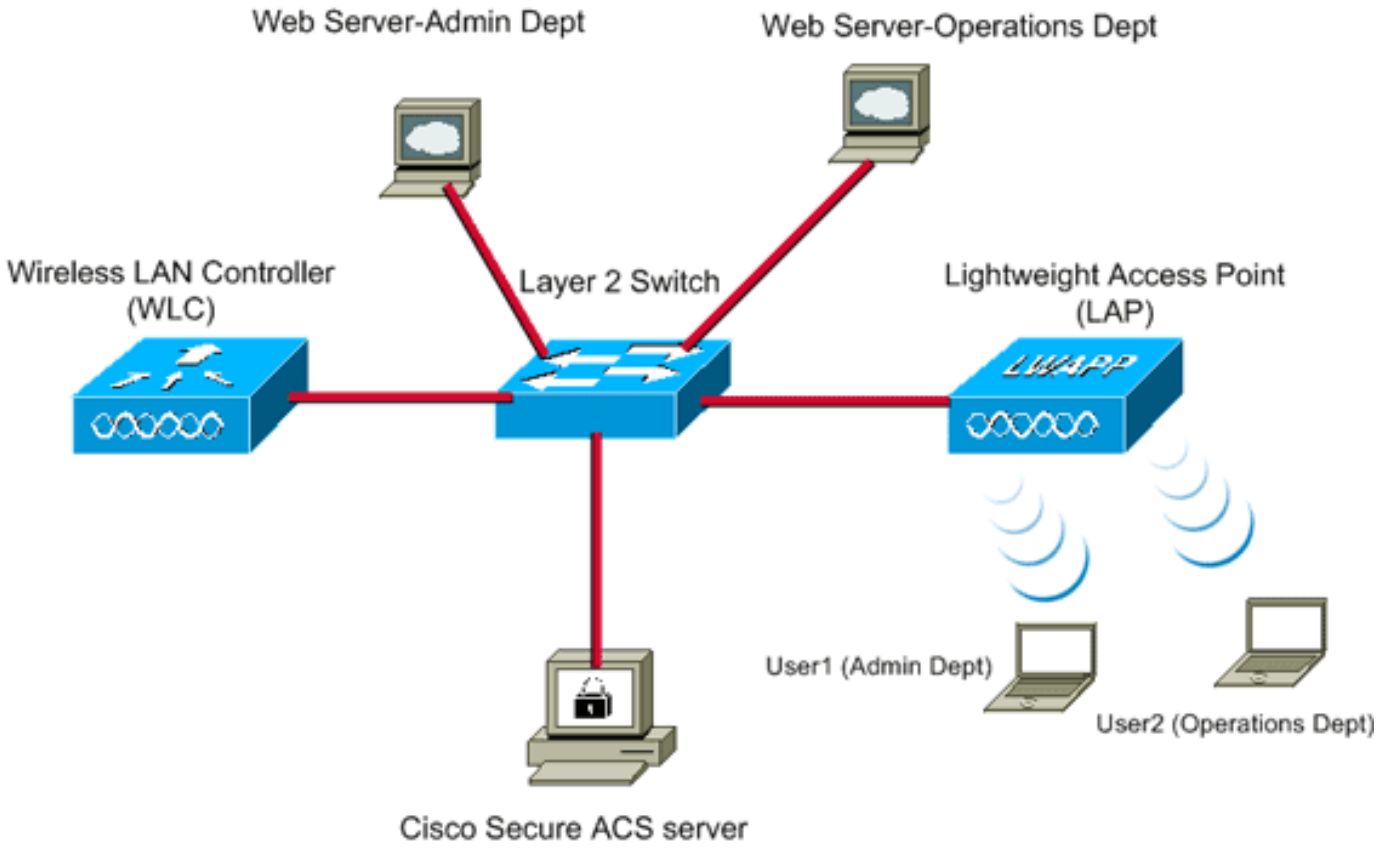
Le Web de page de splash réorientent la caractéristique est disponible seulement pour des WLAN configurés pour le 802.1x ou WPA/WPA2 le degré de sécurité de la couche 2.

Configuration du réseau

Dans cet exemple, un Cisco 4404 WLC et un RECOUVREMENT de gamme Cisco 1232 sont connectés par un commutateur de la couche 2. Le serveur de Cisco Secure ACS (qui agit en tant que serveur RADIUS externe) est également connecté au même commutateur. Tous les périphériques se trouvent dans le même sous-réseau.

Le RECOUVREMENT est au commencement enregistré au contrôleur. Vous devez créer deux WLAN : un pour les utilisateurs de **service d'admin** et l'autre pour les utilisateurs de **service d'exécutions**. Utilisation Sans fil WPA2/ AES de les deux réseaux locaux (l'EAP-FAST est utilisé pour l'authentification). Les deux WLAN utilisent la page de splash réorientent la caractéristique afin de réorienter des utilisateurs à la page d'accueil appropriée URLs (sur des web server 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 Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Terminez-vous ces étapes afin de configurer les périphériques pour utiliser la page de splash réorientent la caractéristique :

1. Configurez le WLC pour l'authentification de RADIUS par le serveur de Cisco Secure ACS.
2. Configurez les WLAN pour les services d'admin et d'exécutions.
3. Configurez le Cisco Secure ACS pour prendre en charge la page de splash réorientent la caractéristique.

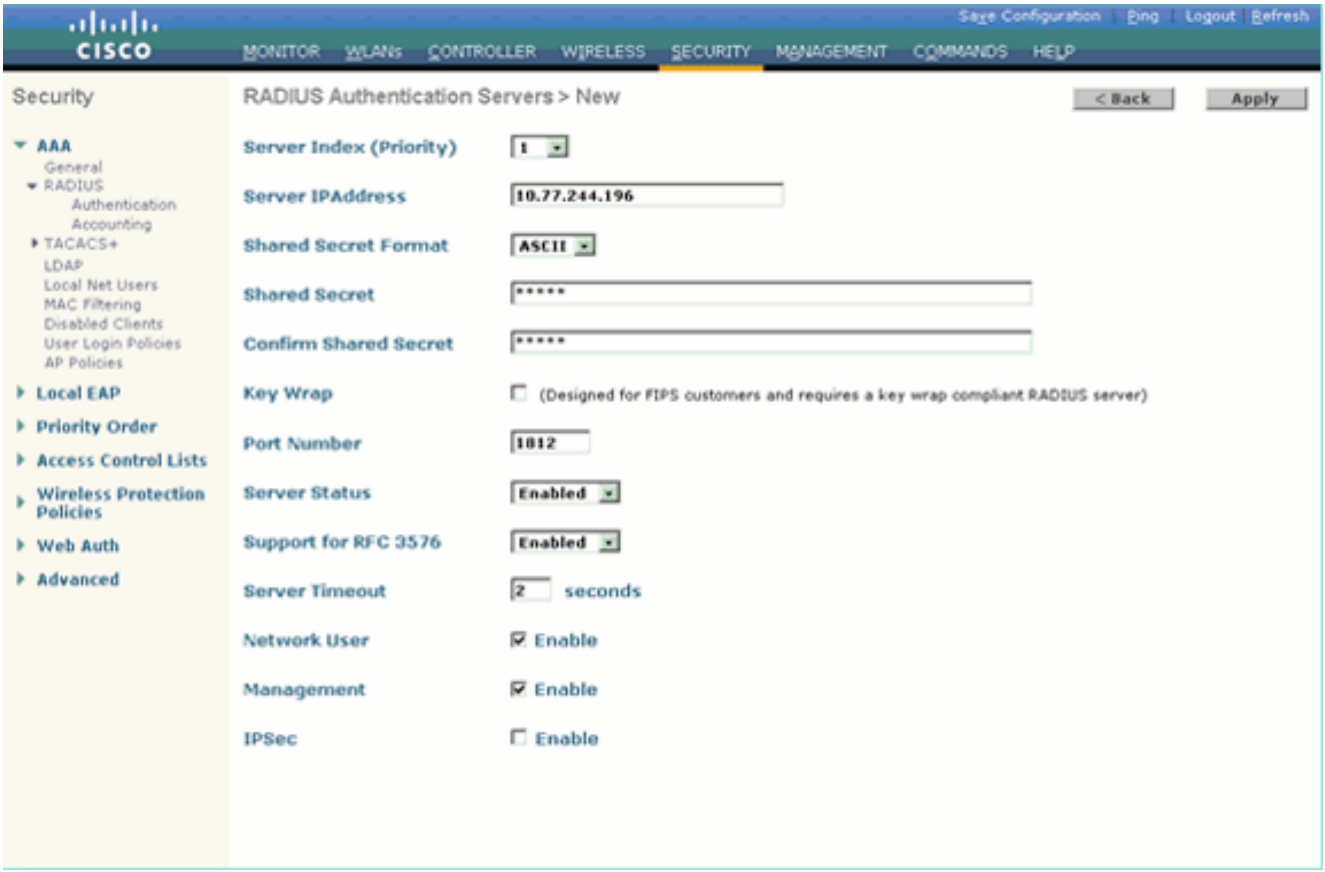
Étape 1. Configurez le WLC pour l'authentification de RADIUS par le serveur de

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 la **Sécurité** et l'**authentification de RADIUS du** GUI de contrôleur afin d'afficher la page de serveurs d'authentification RADIUS.
2. Cliquez sur New afin de définir un serveur de RADIUS.
3. Définissez les paramètres de serveur de RADIUS sur le RADIUS Authentication Servers > New page.Ces paramètres incluent :Adresse IP du serveur RADIUSSecret partagéNuméro de portÉtat de serveur



Ce document utilise le serveur ACS avec une adresse IP de 10.77.244.196.

4. Cliquez sur **Apply**.

Étape 2. Configurez les WLAN pour le service d'admin et d'exécutions.

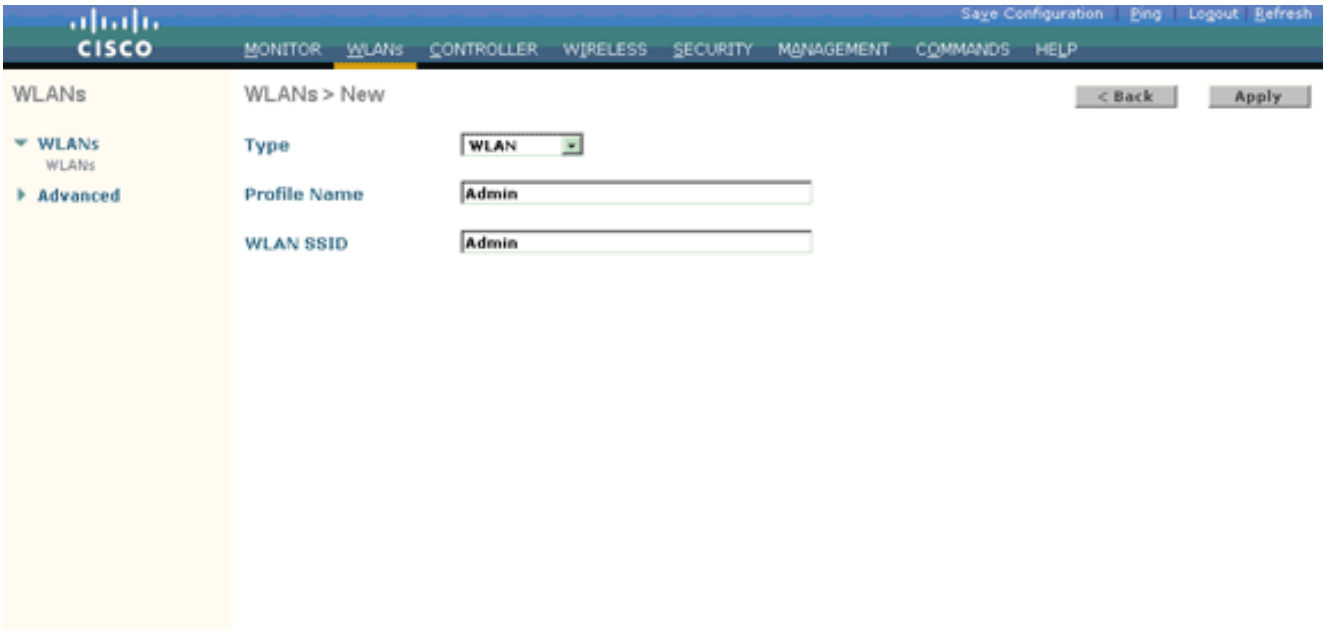
Dans cette étape, vous configurez les deux WLAN (un pour le service d'admin et l'autre pour le service d'exécutions) que les clients emploieront afin de se connecter au réseau Sans fil.

Le WLAN SSID pour le service d'admin sera *admin*. Le WLAN SSID pour le service d'exécutions sera des exécutions.

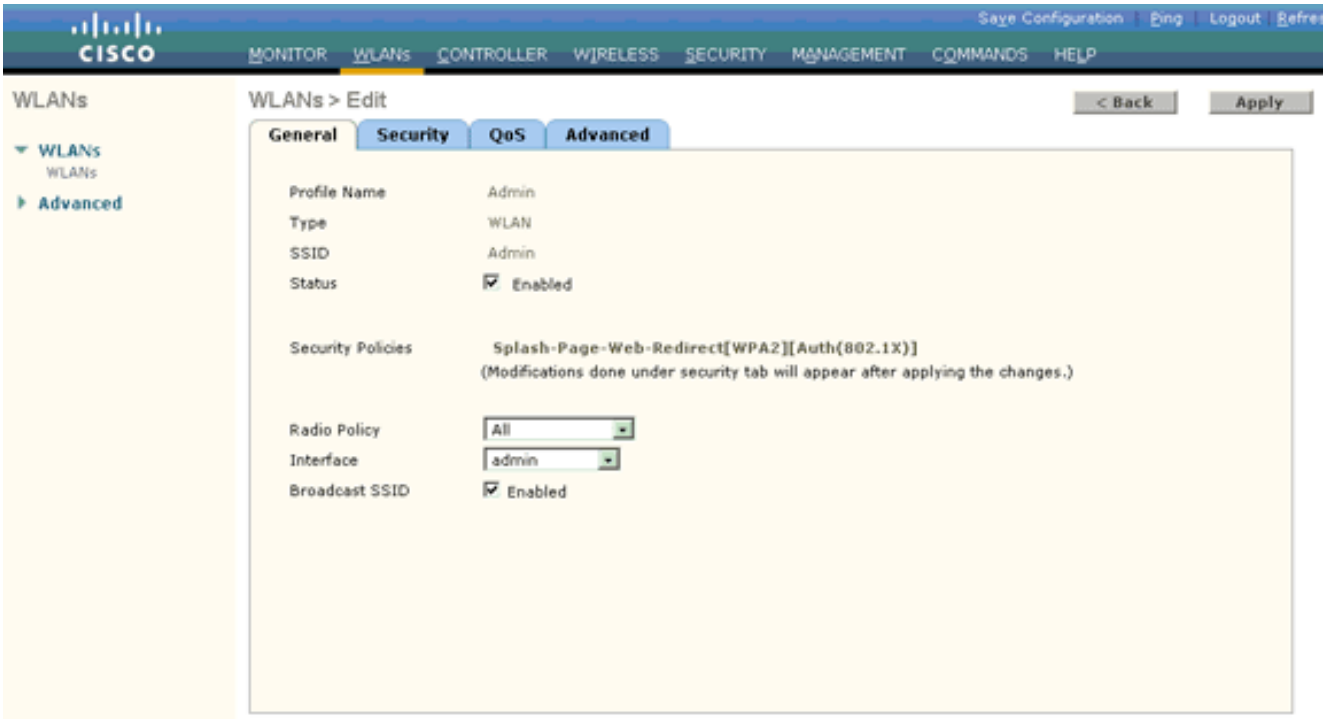
Employez l'authentification d'EAP-FAST afin d'activer le WPA2 comme mécanisme de sécurité de la couche 2 sur les deux WLAN et la stratégie de Web - le Web de page de splash réorientent la caractéristique comme méthode de degré de sécurité de la couche 3.

Terminez-vous ces étapes afin de configurer le WLAN et ses paramètres relatifs :

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 afin de créer un nouveau WLAN.



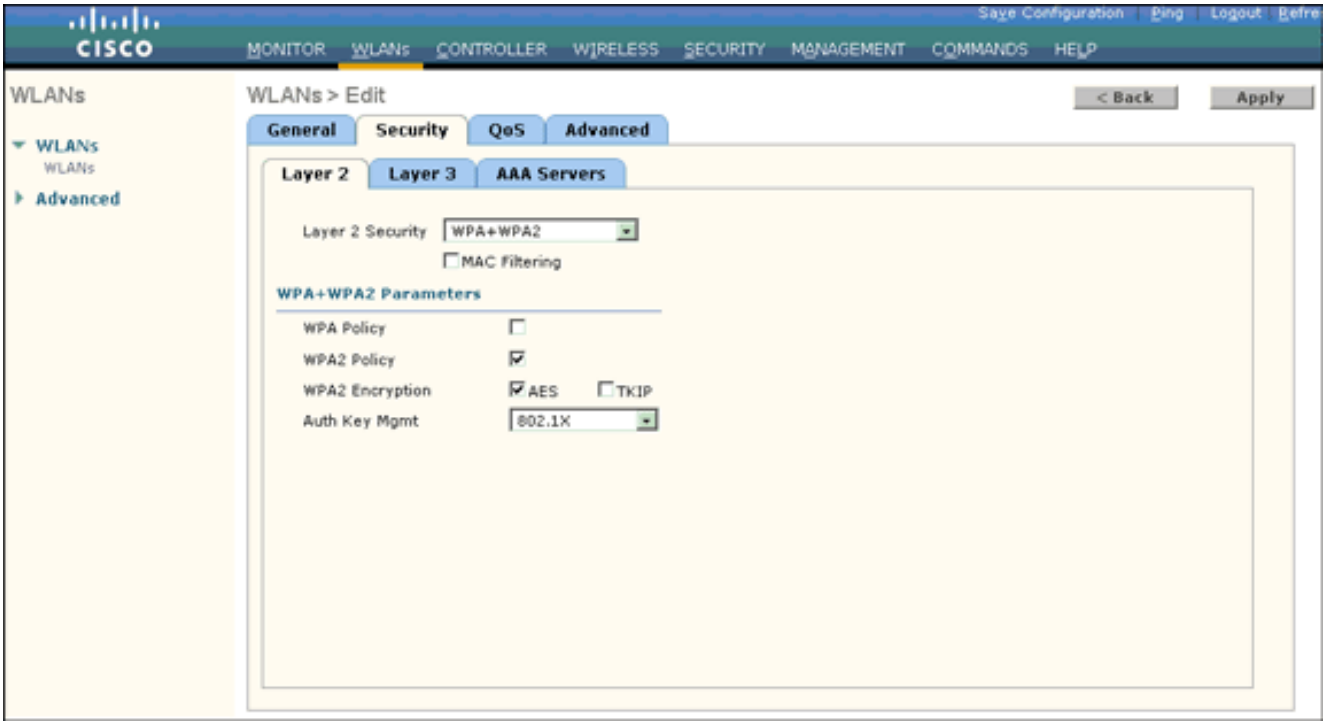
3. Écrivez le nom WLAN SSID et le nom de profil à la page de WLANs > New.
4. Cliquez sur **Apply**.
5. Permettez-d'abord nous créent le WLAN pour le service d'admin.Une fois que vous avez créé un nouveau WLAN, la page WLAN > Edit du nouveau WLAN apparaît. À cette page, vous pouvez définir de divers paramètres spécifiques à ce WLAN. Ceci inclut des stratégies générales, des stratégies de sécurité, des stratégies QoS, et des paramètres avancés.
6. Dans le cadre des stratégies générales, cochez la case d'**état** afin d'activer le WLAN.



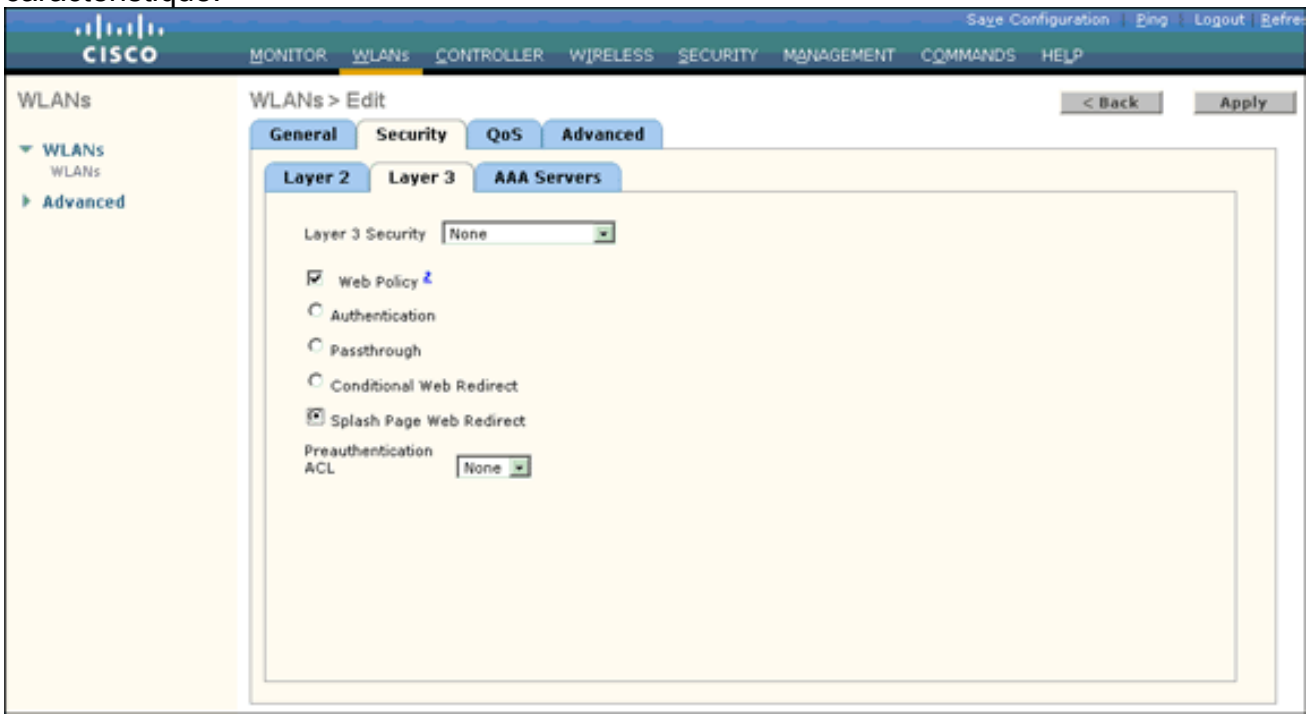
7. Cliquez sur l'**onglet Sécurité**, et puis cliquez sur l'onglet de la **couche 2**.
8. Choisissez **WPA+WPA2 de la** liste déroulante de degré de sécurité de la couche 2.Cette

étape active l'authentification WPA pour le WLAN.

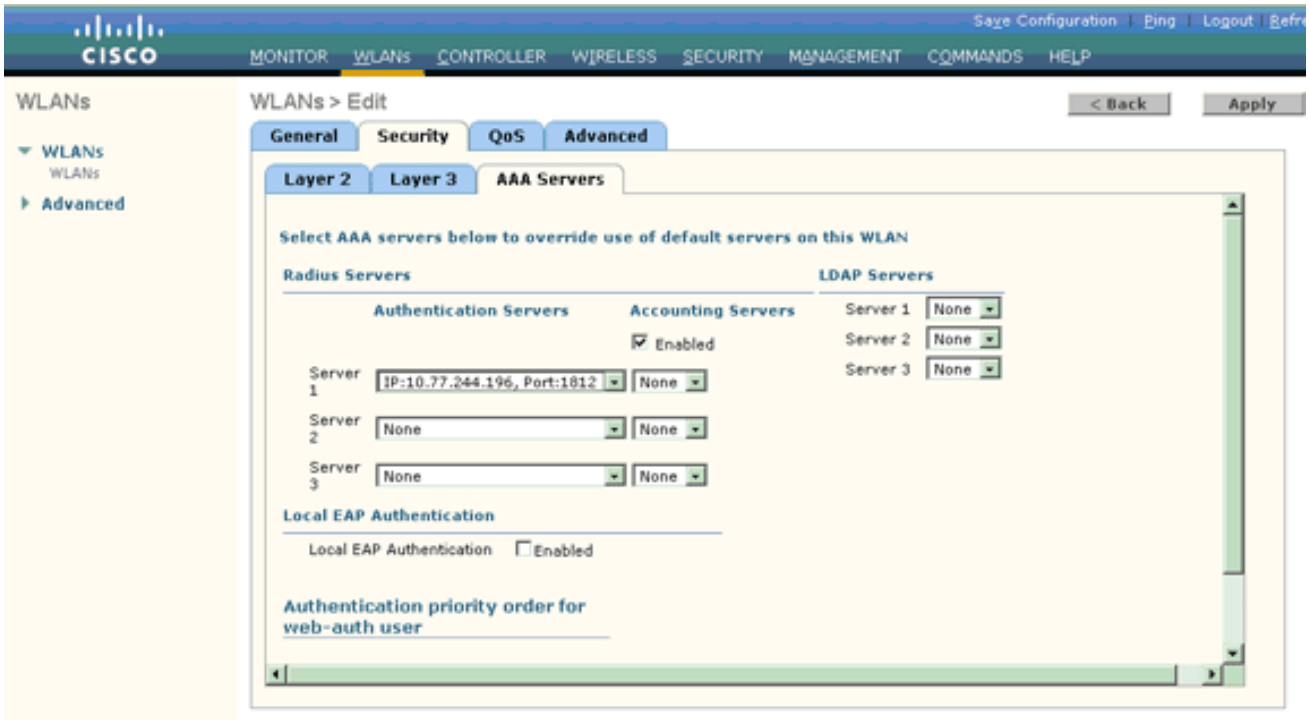
9. Sous les paramètres WPA+WPA2, vérifiez les cases de la **stratégie WPA2** et du **cryptage AES**.



10. Choisissez le **802.1x de la** liste déroulante authentique de clé gestion. Cette option active le WPA2 avec l'authentification 802.1x/EAP et le cryptage AES pour le WLAN.
11. Cliquez sur l'**onglet Sécurité de la couche 3**.
12. Cochez la case de **stratégie de Web**, et puis cliquez sur le **Web de page de splash réorientent la** case d'option.Cette option active le Web de page de splash réorientent la caractéristique.



13. Cliquez sur l'**onglet AAA Servers**.
14. Sous des serveurs d'authentification, choisissez l'adresse IP du serveur appropriée de la liste déroulante du serveur
    1.



Dans cet exemple, 10.77.244.196 est utilisé en tant que serveur de RADIUS.

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

Notez que les stratégies de sécurité incluent la page de splash réorientent.

Étape 3. Configurez le Cisco Secure ACS pour prendre en charge la page de splash réorientent la caractéristique.

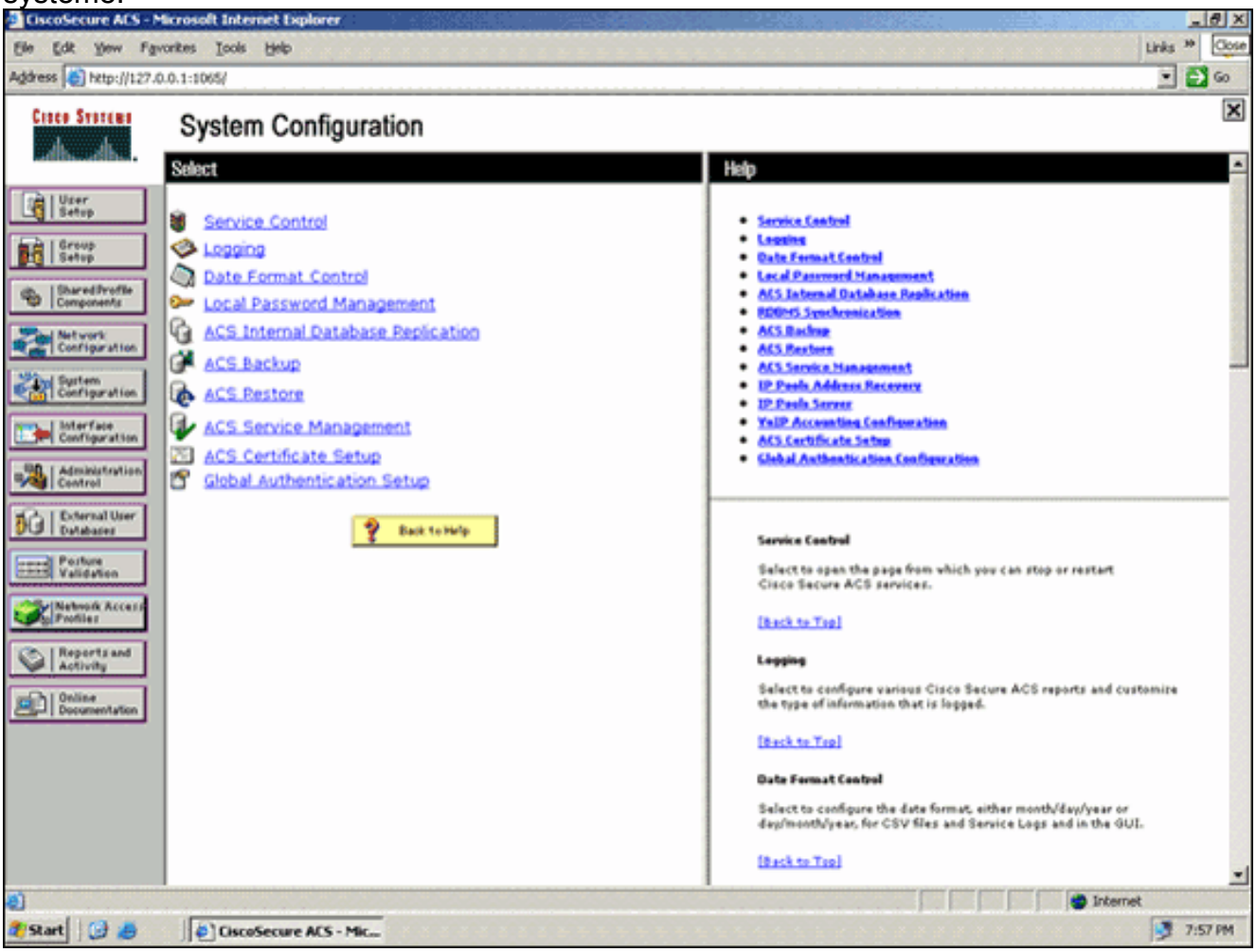
L'étape suivante est de configurer le serveur de RADIUS pour cette caractéristique. Le serveur de RADIUS doit exécuter l'authentification d'EAP-FAST afin de valider les qualifications de client, et sur l'authentification réussie, pour réorienter l'utilisateur à l'URL (sur le web server externe) spécifié dans les poids du commerce-paires de Cisco URL-***réorientez l'***attribut RADIUS.

Configurez le Cisco Secure ACS pour l'authentification d'EAP-FAST

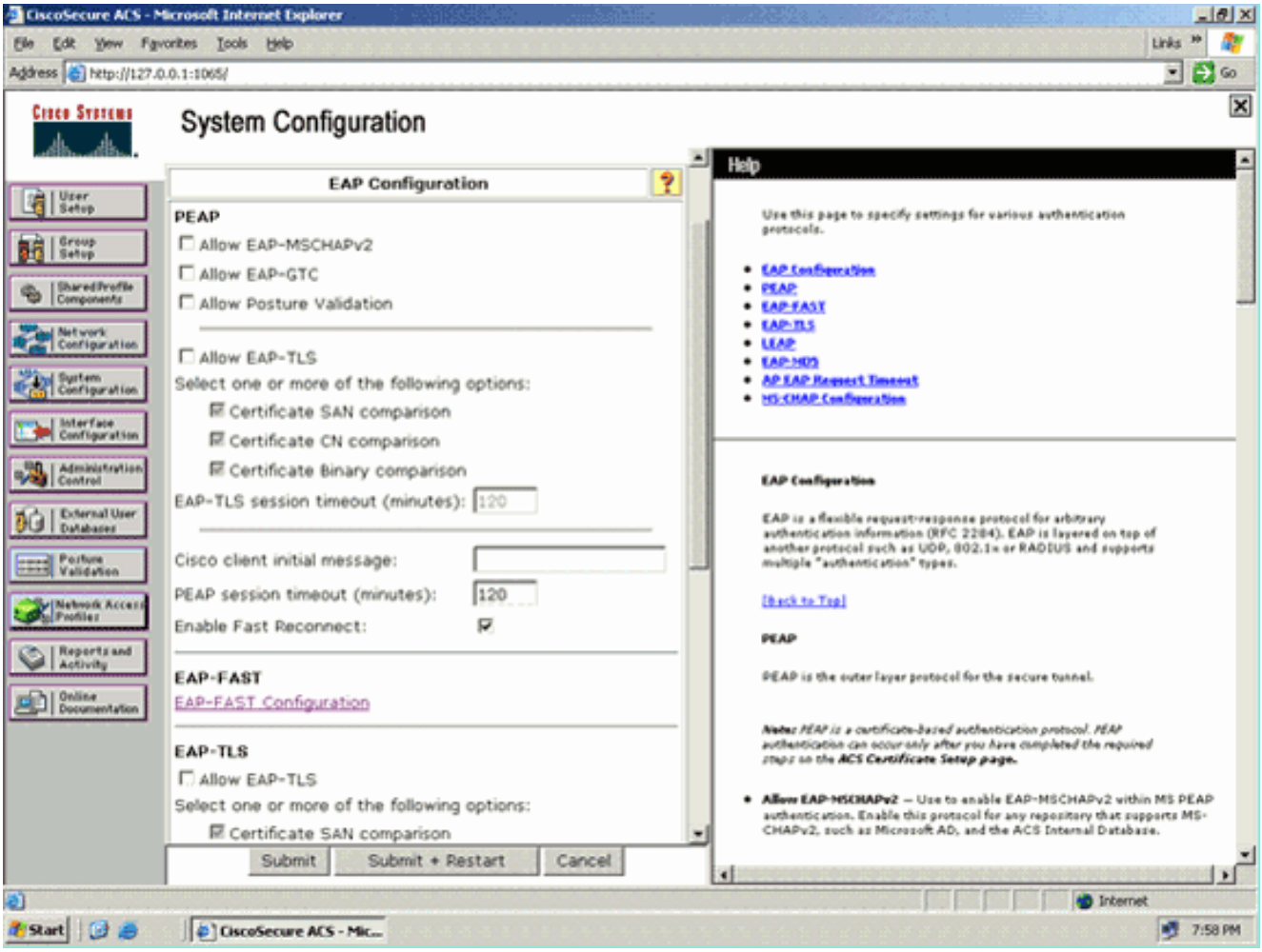
Remarque: Ce document suppose que le contrôleur LAN Sans fil est ajouté au Cisco Secure ACS en tant que client d'AAA.

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

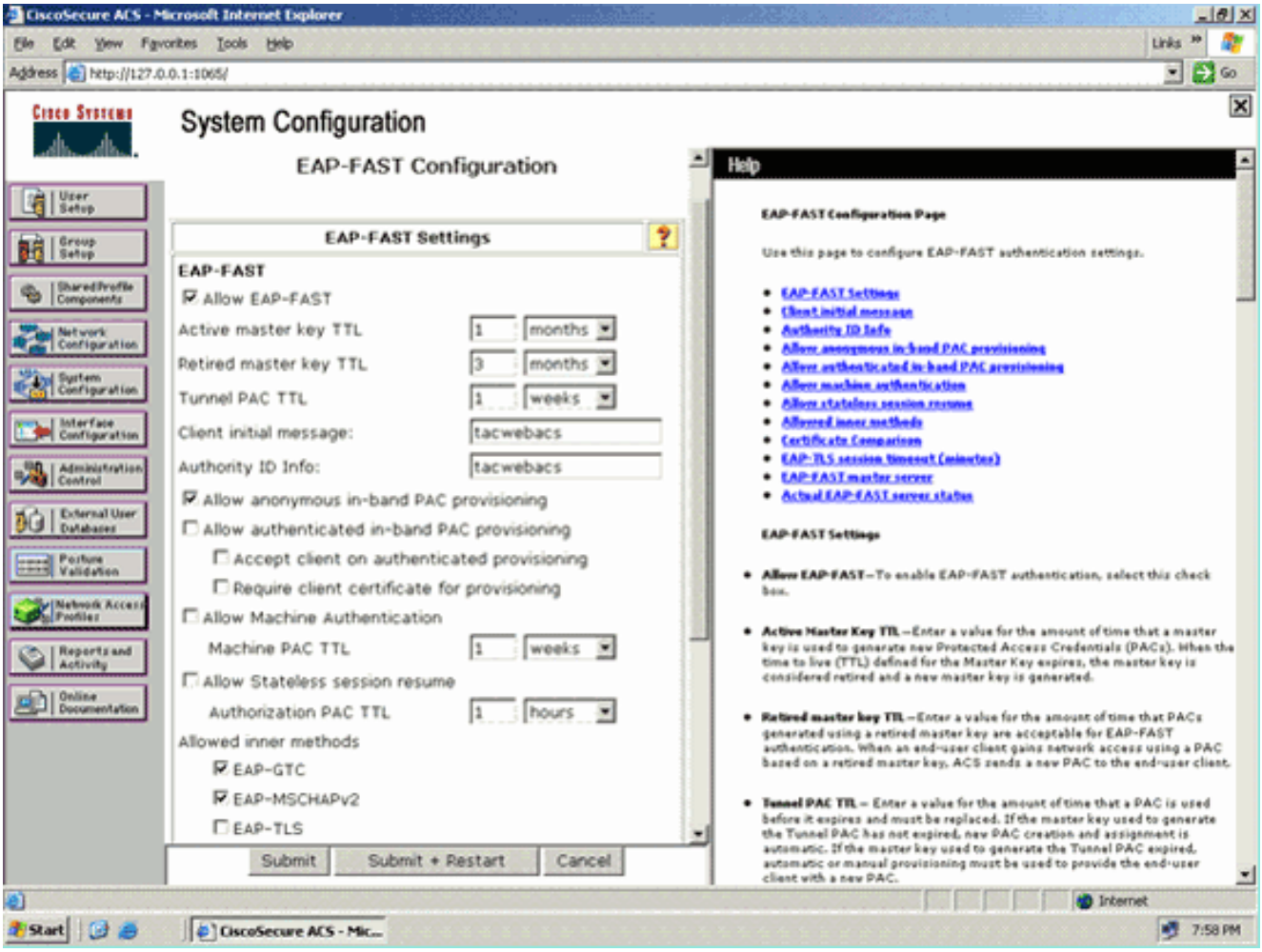
1. Cliquez sur la **configuration système du** GUI de serveur de RADIUS, et puis choisissez choisissent l'**authentification globale installée de la** page de configuration système.



2. De la page globale d'installation d'authentification, **configuration d'EAP-FAST de** clic afin d'aller aux configurations d'EAP-FAST la page.



3. De la page Settings d'EAP-FAST, cochez la case d'**EAP-FAST d'autoriser** afin d'activer l'EAP-FAST dans le serveur de RADIUS.



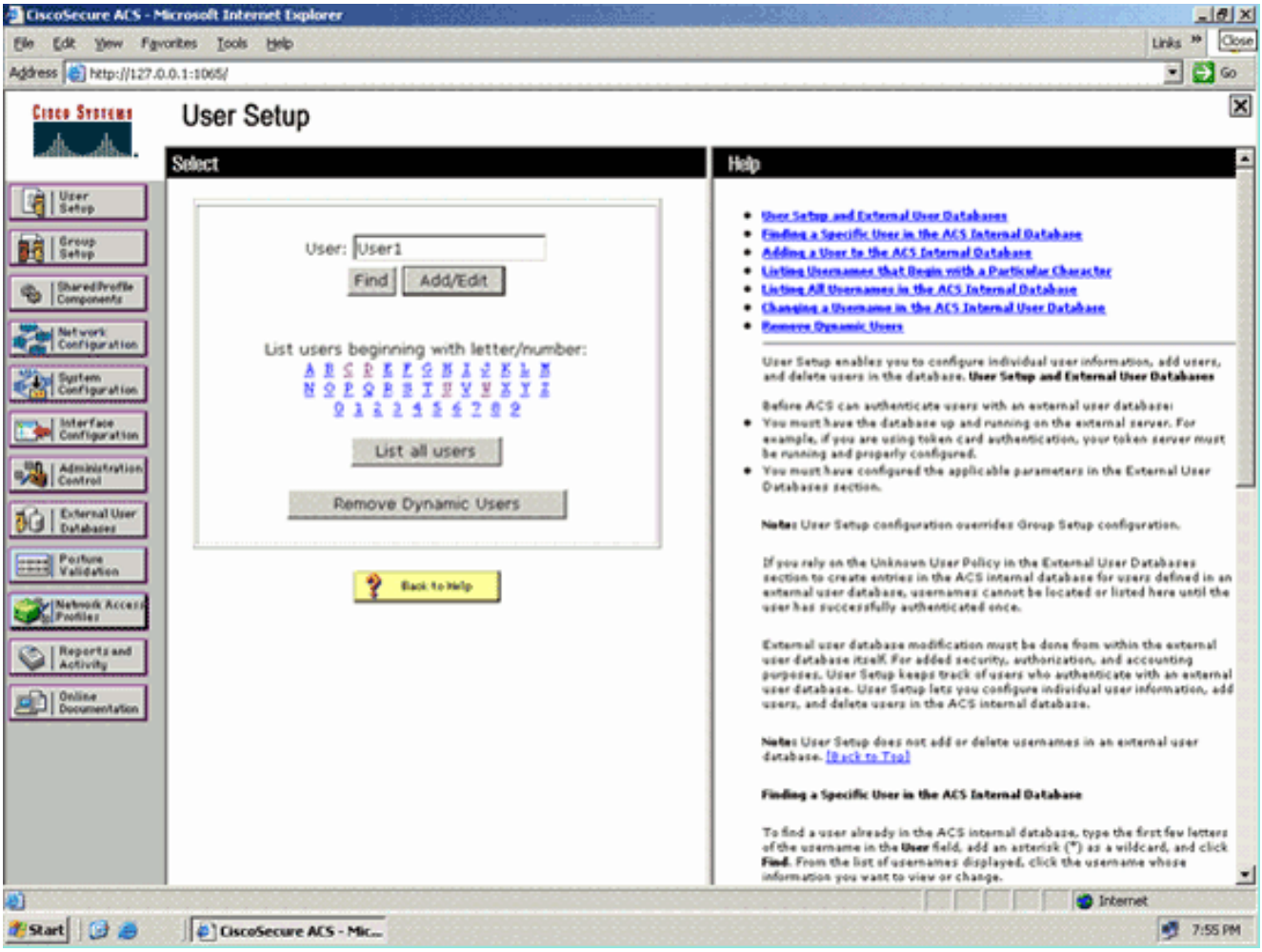
4. Configurez l'Active/valeurs retirées de la clé principale TTL (Time to Live) comme désirées, ou placez-les à la valeur par défaut suivant les indications de cet exemple.La zone d'informations d'ID d'autorité représente l'identité textuelle de ce serveur ACS, qu'un utilisateur final peut employer pour déterminer contre quel serveur ACS à authentifier. Compléter ce champ est obligatoire.Le champ de message d'affichage d'initiale de client spécifie un message à envoyer aux utilisateurs qui authentifient avec un client d'EAP-FAST. La longueur maximale est 40 caractères. Un utilisateur verra le message initial seulement si le client d'utilisateur prend en charge l'affichage.
5. Si vous voulez que l'ACS effectue le ravitaillement anonyme PAC d'intrabande, cochez la case **anonyme de ravitaillement PAC d'intrabande d'autoriser**.
6. L'option *intérieure permise de méthodes* détermine quelles méthodes intérieures d'EAP peuvent fonctionner à l'intérieur du tunnel de TLS d'EAP-FAST. Pour le ravitaillement anonyme d'intrabande, vous devez activer EAP-GTC et EAP-MS-CHAP pour la compatibilité ascendante. Si vous sélectionnez permettez le ravitaillement anonyme PAC d'intrabande, vous devez sélectionner EAP-MS-CHAP (phase zéro) et EAP-GTC (phase deux).
7. Cliquez sur **Submit**.**Remarque:** Pour les informations détaillées et des exemples au sujet de la façon configurer l'EAP RAPIDE avec le ravitaillement anonyme PAC d'intrabande et le ravitaillement authentifié d'intrabande, référez-vous à l'authentification d'EAP-FAST avec l'exemple Sans fil de contrôleurs LAN et de configuration de serveur RADIUS externe.

Configurez la base de données utilisateur et définissez l'attribut RADIUS d'URL-*réorientation*

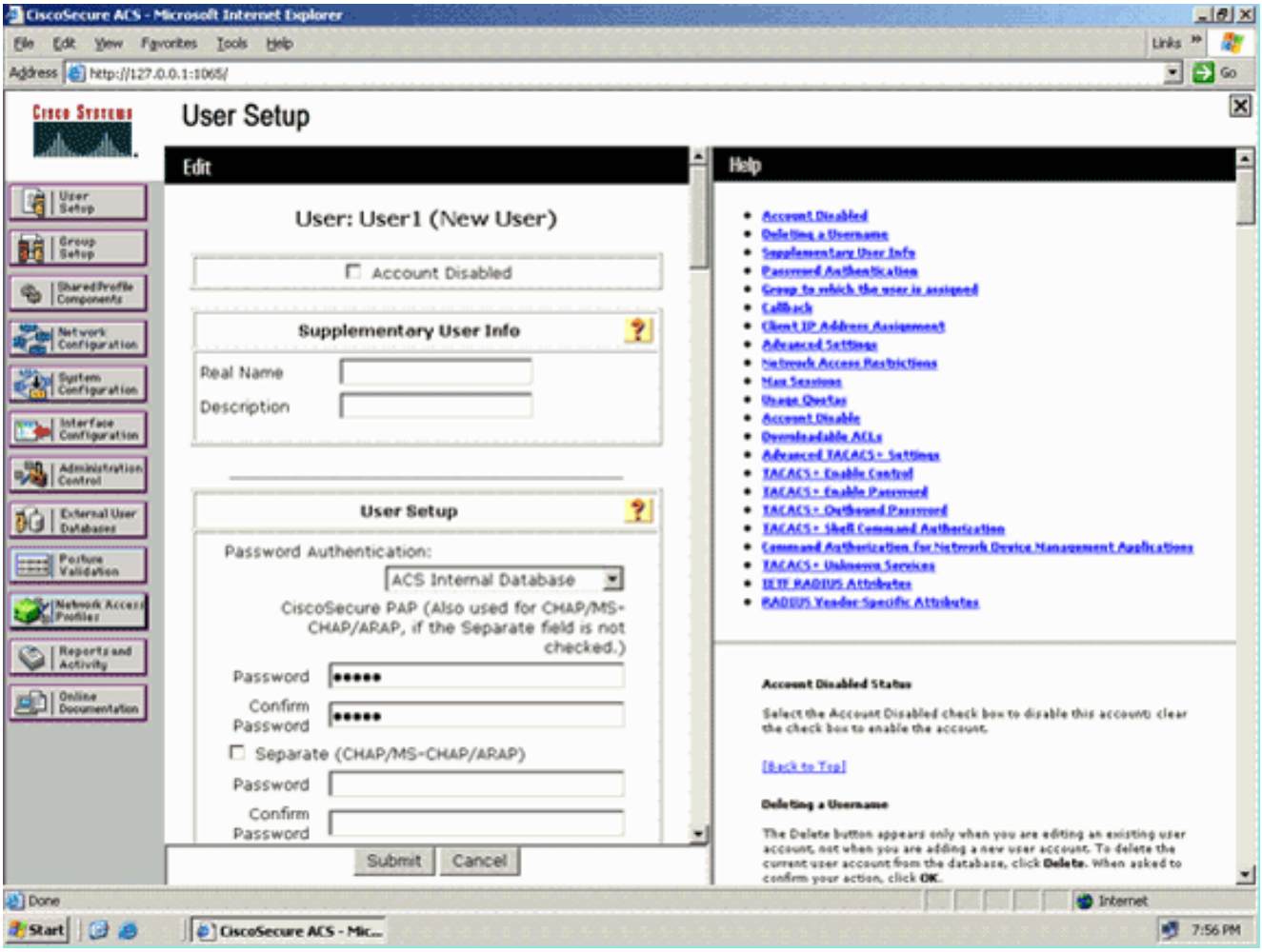
Cet exemple configure le nom d'utilisateur et mot de passe du client sans fil comme User1 et User1, respectivement.

Terminez-vous ces étapes afin de créer une base de données utilisateur :

1. Du GUI ACS dans la barre de navigation, choisissez User Setup.
2. Créez une nouvelle radio d'utilisateur, et puis cliquez sur Add/**l'éditez** afin d'aller à la page d'éditer de cet
   utilisateur.



3. De l'installation utilisateur éditez la page, configurez le nom réel et la description, aussi bien que les paramètres du mot de passe, suivant les indications de cet exemple.Ce document utilise des ACS Internal Database pour l'authentification de mot de
   passe.



4. Faites descendre l'écran la page pour modifier les attributs RADIUS.
5. Cochez la case de Cisco-poids du commerce-**paires [009\001]**.
6. Écrivez ce les poids du commerce-paires de Cisco dans la case d'éditer de Cisco-poids du commerce-paires [009\001] afin de spécifier l'URL auquel l'utilisateur est réorienté :url-redirect=http://10.77.244.196/Admin-Login.html

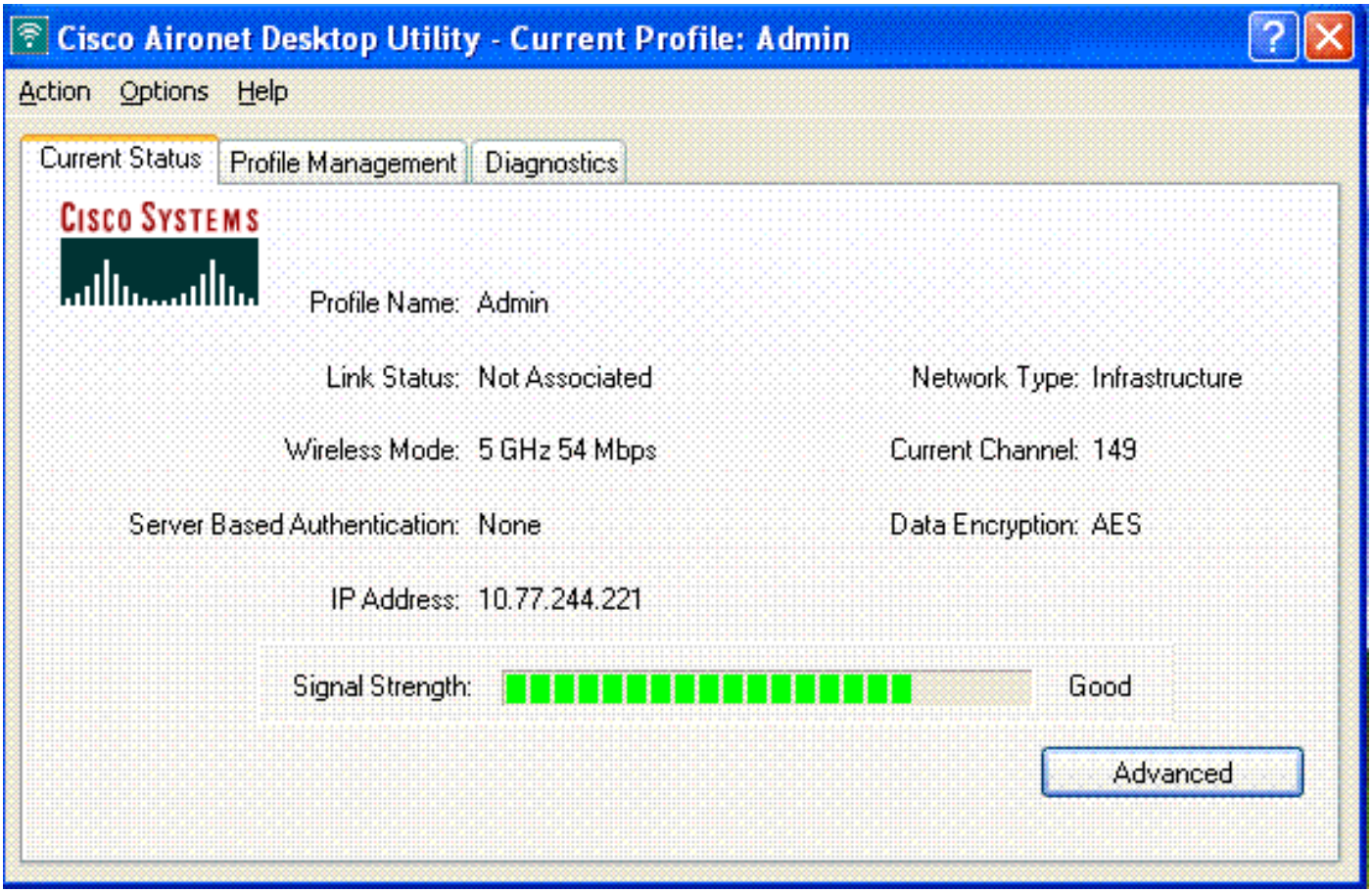
C'est la page d'accueil des utilisateurs de service d'admin.

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

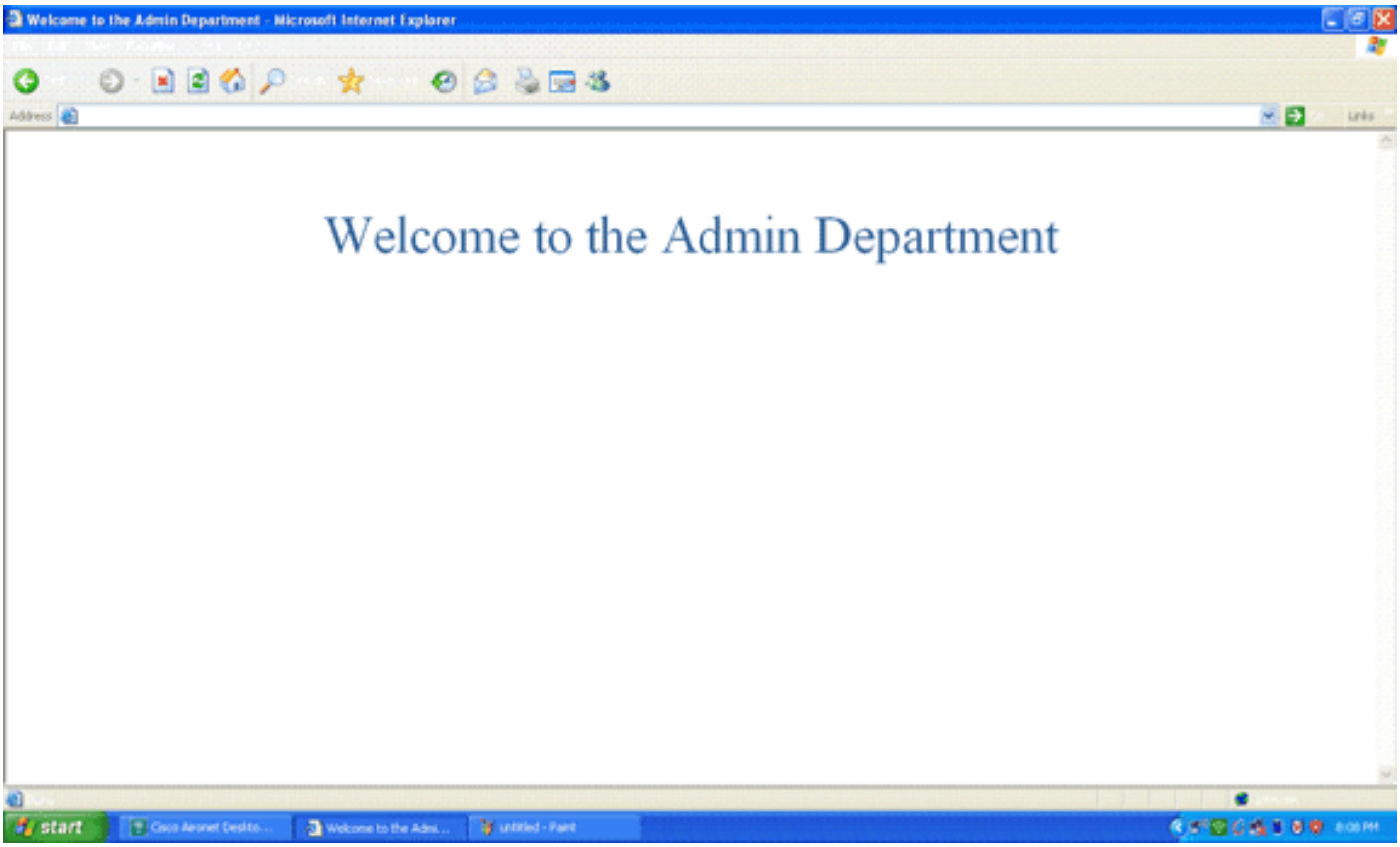
Vérifier

Afin de vérifier la configuration, associez un client WLAN du service d'admin et du service d'exécutions à leurs WLAN appropriés.

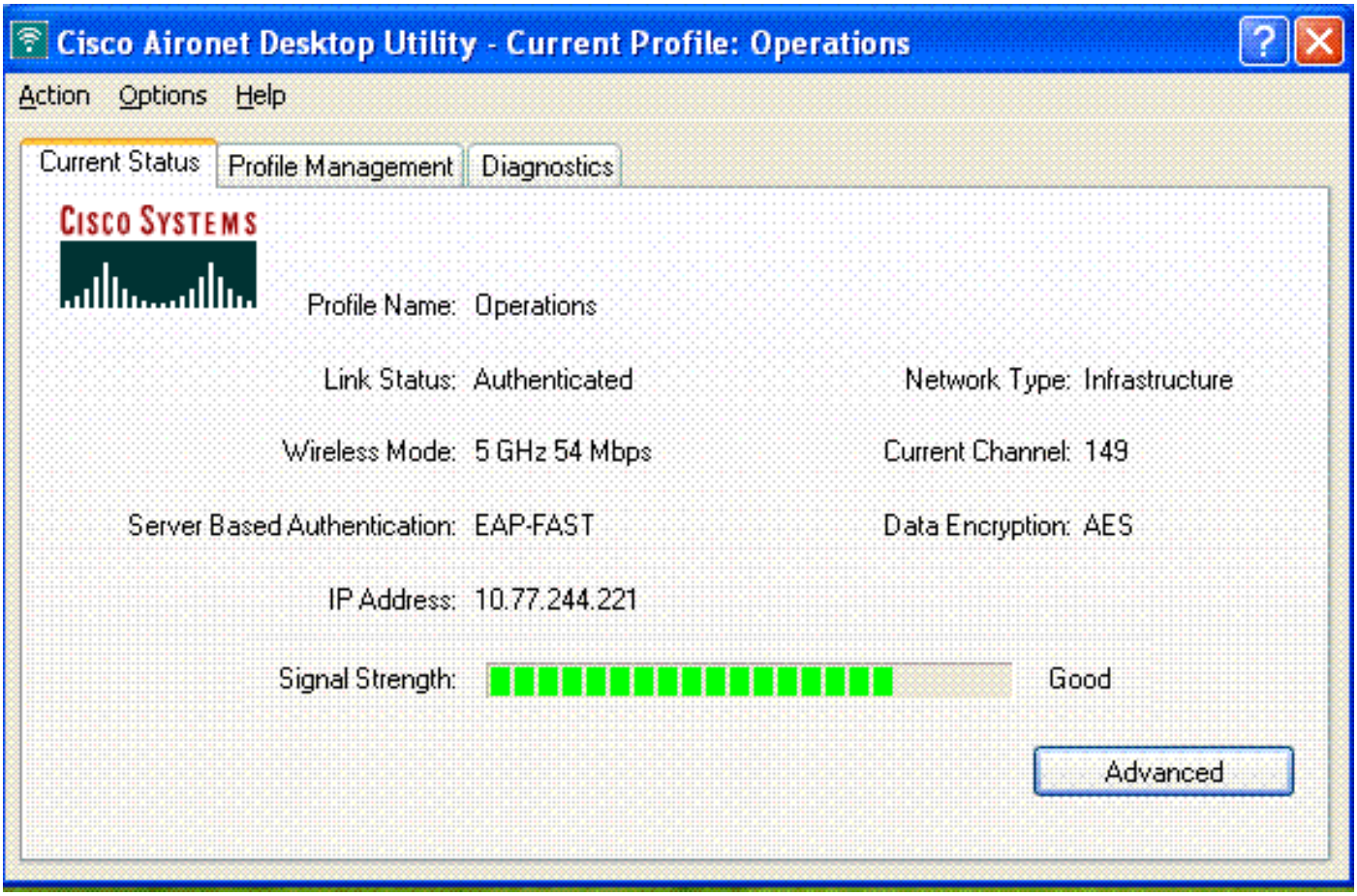
Quand un utilisateur du service d'admin se connecte à l'admin Sans fil de RÉSEAU LOCAL, l'utilisateur est incité pour les qualifications de 802.1x (qualifications d'EAP-FAST dans notre cas). Une fois que l'utilisateur fournit les qualifications, le WLC passe ces qualifications au serveur de Cisco Secure ACS. Le serveur de Cisco Secure ACS valide les qualifications de l'utilisateur contre la base de données, et sur l'authentification réussie, renvoie l'attribut d'URL-réorientation au contrôleur LAN Sans fil. L'authentification est complète à ce stade.

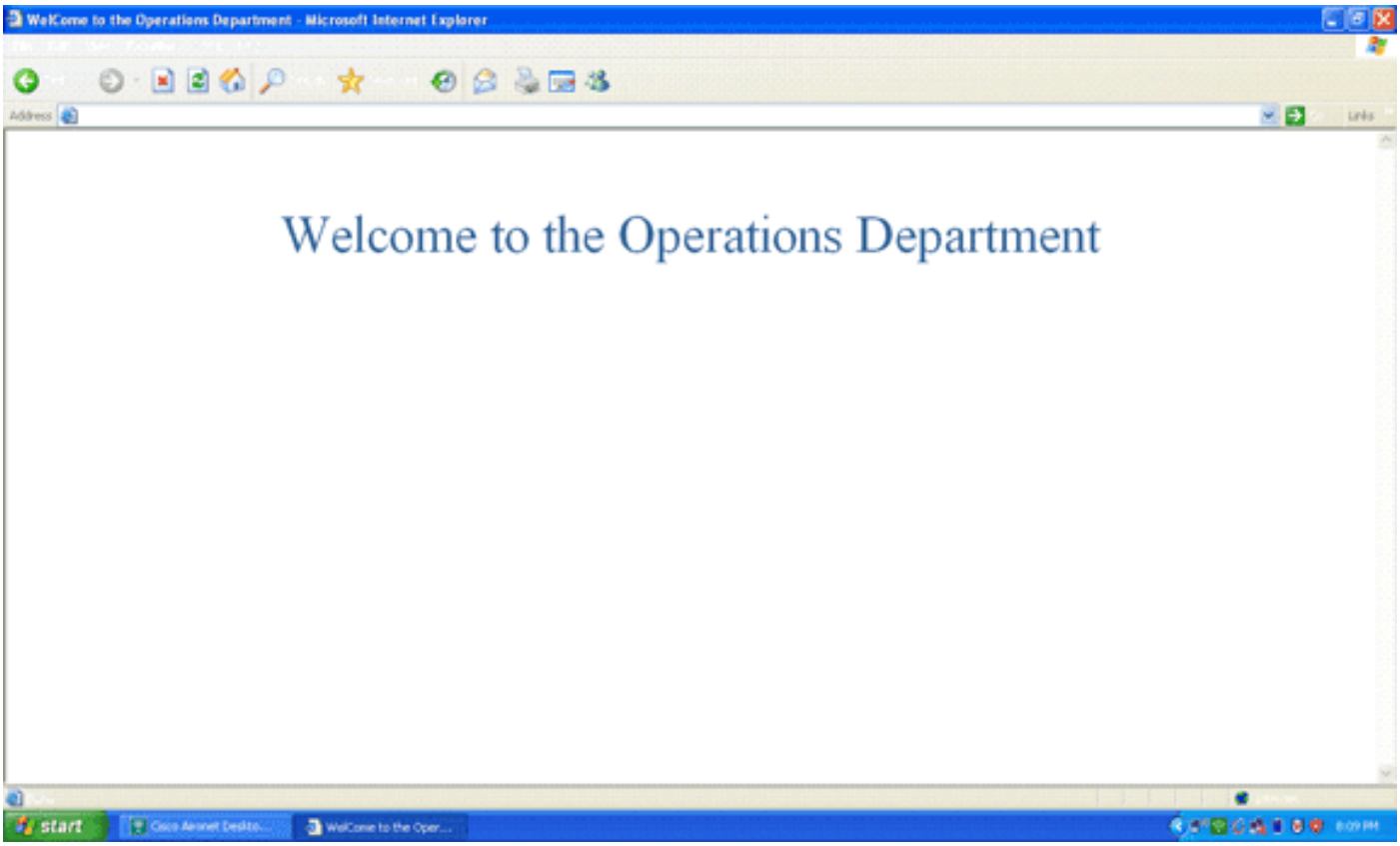


Quand l'utilisateur ouvre un navigateur Web, l'utilisateur est réorienté à l'URL de page d'accueil du service d'admin. (Cet URL est retourné au WLC par l'attribut de Cisco-poids du commerce-paires). Après que la réorientation, l'utilisateur ait l'accès complet au réseau. Voici les captures d'écran :



Les mêmes séquences d'opérations se produisent quand un utilisateur du service d'exécutions se connecte aux exécutions WLAN.





Dépanner

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

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant

d'utiliser les commandes de **débogage**.

Vous pouvez utiliser les commandes suivantes de dépanner votre configuration.

- **wlan_id de show wlan** — Affiche le statut du Web réorientent des caractéristiques 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
```

- **enable d'événements de debug dot1x** — Active le débogage des messages de paquet de 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
```

- **enable d'événements de debug aaa** — Active la sortie de débogage de tous les événements d'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 Sans fil de contrôleur LAN de 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
- Support et documentation techniques - Cisco Systems