Exemple de configuration de l'accès WPA (Wi-Fi Protected Access) dans un réseau sans fil unifié Cisco

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Conventions
Prise en charge WPA et WPA2
Configuration du réseau
Configuration des périphériques en mode WPA2 entreprise
Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe
Configurer le WLAN pour le mode de fonctionnement WPA2 Enterprise
Configurer le serveur RADIUS pour l'authentification en mode entreprise WPA2 (EAP-FAST)
Configuration du client sans fil pour le mode de fonctionnement WPA2 Enterprise
Configuration des périphériques pour le mode WPA2 Personal
Dépannage
Informations connexes

Introduction

Ce document décrit comment configurer le Wi-Fi Protected Access (WPA) dans un réseau sans fil unifié Cisco.

Conditions préalables

Exigences

Assurez-vous d´avoir une connaissance de base de ces sujets avant de tenter cette configuration :

- WPA
- Solutions de sécurité LAN sans fil (WLAN)**Remarque :** reportez-vous à Présentation de la sécurité LAN sans fil Cisco pour obtenir des informations sur les solutions de sécurité WLAN Cisco.

Composants utilisés

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

- Point d'accès allégé (LAP) Cisco, série 1000
- Contrôleur LAN sans fil (WLC) Cisco 4404 qui exécute le microprogramme 4.2.61.0
- Adaptateur client Cisco 802.11a/b/g qui exécute le microprogramme 4.1
- Aironet Desktop Utility (ADU) qui exécute le microprogramme 4.1
- Serveur Cisco Secure ACS version 4.1

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 aux Conventions relatives aux conseils techniques Cisco.

Prise en charge WPA et WPA2

Le réseau sans fil unifié Cisco prend en charge les certifications WPA et WPA2 de la Wi-Fi Alliance. La norme WPA a été introduite par la Wi-Fi Alliance en 2003. WPA2 a été introduit par la Wi-Fi Alliance en 2004. Tous les produits certifiés Wi-Fi pour WPA2 doivent être interopérables avec les produits certifiés Wi-Fi pour WPA.

Les protocoles WPA et WPA2 offrent aux utilisateurs finaux et aux administrateurs réseau un niveau élevé d'assurance que leurs données resteront privées et que l'accès à leurs réseaux sera limité aux utilisateurs autorisés. Les deux modes de fonctionnement, personnel et entreprise, répondent aux besoins distincts des deux segments de marché. Le mode Entreprise de chaque utilise IEEE 802.1X et EAP pour l'authentification. Le mode personnel de chaque utilise la clé prépartagée (PSK) pour l'authentification. Cisco ne recommande pas le mode personnel pour les déploiements professionnels ou gouvernementaux, car il utilise une clé prépartagée pour l'authentification des utilisateurs. PSK n'est pas sécurisé pour les environnements d'entreprise.

WPA résout toutes les vulnérabilités WEP connues dans la mise en oeuvre de la sécurité IEEE 802.11 d'origine, apportant ainsi une solution de sécurité immédiate aux WLAN dans les environnements d'entreprise et de petits bureaux/bureaux à domicile (SOHO). WPA utilise TKIP pour le cryptage.

WPA2 est la nouvelle génération de sécurité Wi-Fi. Il s'agit de la mise en oeuvre interopérable de la norme IEEE 802.11i ratifiée par la Wi-Fi Alliance. Il implémente l'algorithme de chiffrement AES recommandé par le National Institute of Standards and Technology (NIST) à l'aide du mode compteur avec le protocole CCMP (Cipher Block Chaining Message Authentication Code Protocol). WPA2 facilite la conformité à la norme FIPS 140-2 du gouvernement.

Comparaison des types de modes WPA et WPA2

	WPA	WPA2
Mode entreprise (entreprise, gouvernement, éducation)	• Authentification : IEEE 802.1X/EA	• Authentification : IEEE 802.1X/EA

	P • Cryptage : TKIP/MIC	P • Cryptage : AES-CCMP
Mode personnel (SOHO, domicile/personnel)	• Authentification : PSK • Cryptage : TKIP/MIC	• Authentification : PSK • Cryptage : AES-CCMP

En mode Entreprise, WPA et WPA2 utilisent tous deux la norme 802.1X/EAP pour l'authentification. La norme 802.1X fournit aux réseaux locaux sans fil une authentification mutuelle solide entre un client et un serveur d'authentification. En outre, la norme 802.1X fournit des clés de cryptage dynamiques par utilisateur et par session, éliminant ainsi la charge administrative et les problèmes de sécurité liés aux clés de cryptage statiques.

Avec la norme 802.1X, les informations d'identification utilisées pour l'authentification, telles que les mots de passe d'ouverture de session, ne sont jamais transmises en clair, ou sans chiffrement, sur le support sans fil. Alors que les types d'authentification 802.1X fournissent une authentification forte pour les réseaux locaux sans fil, TKIP ou AES sont nécessaires pour le cryptage en plus de la norme 802.1X, car le cryptage WEP 802.11 standard est vulnérable aux attaques réseau.

Il existe plusieurs types d'authentification 802.1X, chacun offrant une approche différente de l'authentification tout en s'appuyant sur le même cadre et le même EAP pour la communication entre un client et un point d'accès. Les produits Cisco Aironet prennent en charge plus de types d'authentification EAP 802.1X que tous les autres produits WLAN. Les types pris en charge sont :

- LEAP Cisco
- EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
- EAP-TLS (EAP-Transport Layer Security)
- Protocole PEAP (Protected Extensible Authentication Protocol)
- EAP-TTLS (EAP-TTLS)
- Module EAP-SIM (Subscriber Identity Module)

Un autre avantage de l'authentification 802.1X est la gestion centralisée pour les groupes d'utilisateurs WLAN, y compris la rotation des clés basée sur des politiques, l'attribution de clés dynamiques, l'attribution de VLAN dynamiques et la restriction SSID. Ces fonctions font pivoter les clés de cryptage.

En mode de fonctionnement Personnel, une clé pré-partagée (mot de passe) est utilisée pour l'authentification. Le mode Personnel ne nécessite qu'un point d'accès et un périphérique client, tandis que le mode Entreprise requiert généralement un serveur RADIUS ou un autre serveur d'authentification sur le réseau.

Ce document fournit des exemples de configuration de WPA2 (mode Entreprise) et de WPA2-PSK (mode Personnel) dans un réseau sans fil unifié Cisco.

Configuration du réseau

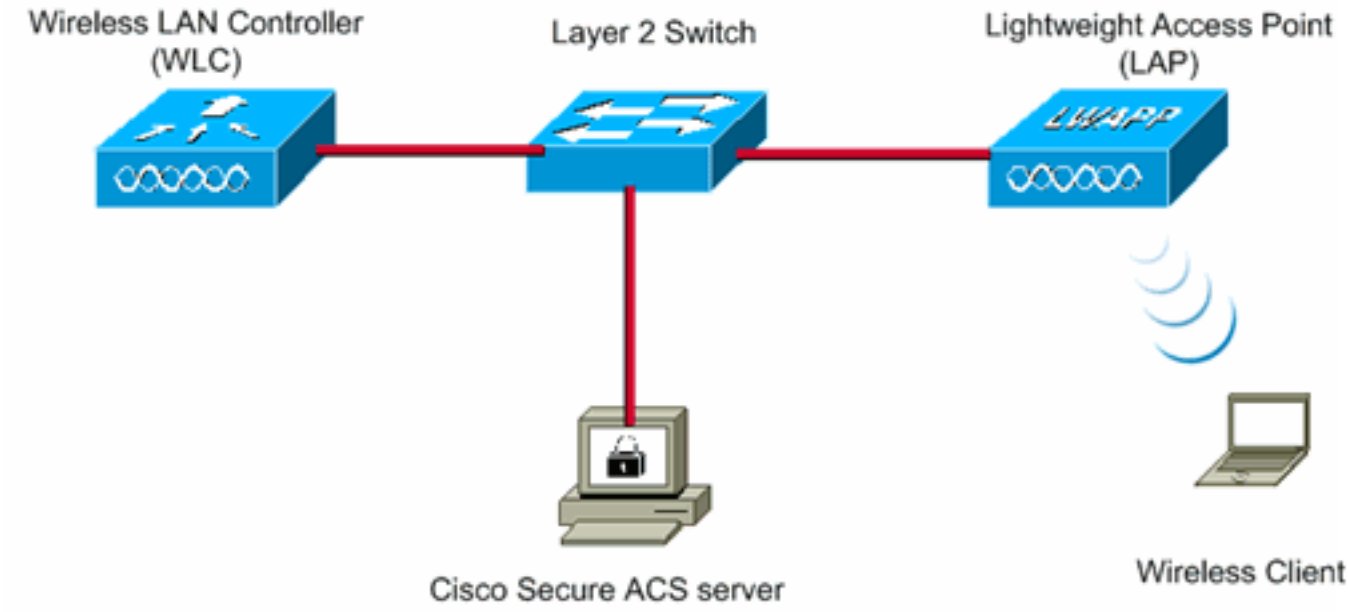
Dans cette configuration, un WLC Cisco 4404 et un LAP Cisco 1000 sont connectés via un

commutateur de couche 2. Un serveur RADIUS externe (Cisco Secure ACS) est également connecté au même commutateur. Tous les périphériques se trouvent dans le même sous-réseau. Le point d'accès (LAP) est initialement enregistré auprès du contrôleur. Deux réseaux locaux sans fil doivent être créés, l'un pour le mode WPA2 entreprise et l'autre pour le mode WPA2 personnel.

WLAN en mode WPA2 entreprise (SSID : WPA2 entreprise) utilise EAP-FAST pour authentifier les clients sans fil et AES pour le cryptage. Le serveur Cisco Secure ACS sera utilisé comme serveur RADIUS externe pour l'authentification des clients sans fil.

WPA2-Personal mode WLAN (SSID : WPA2-PSK) utilise WPA2-PSK pour l'authentification avec la clé prépartagée « abcdefghijk ».

Vous devez configurer les périphériques pour cette configuration :



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

Configuration des périphériques en mode WPA2 entreprise

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

Suivez ces étapes afin de configurer les périphériques pour le mode de fonctionnement WPA2 Entreprise :

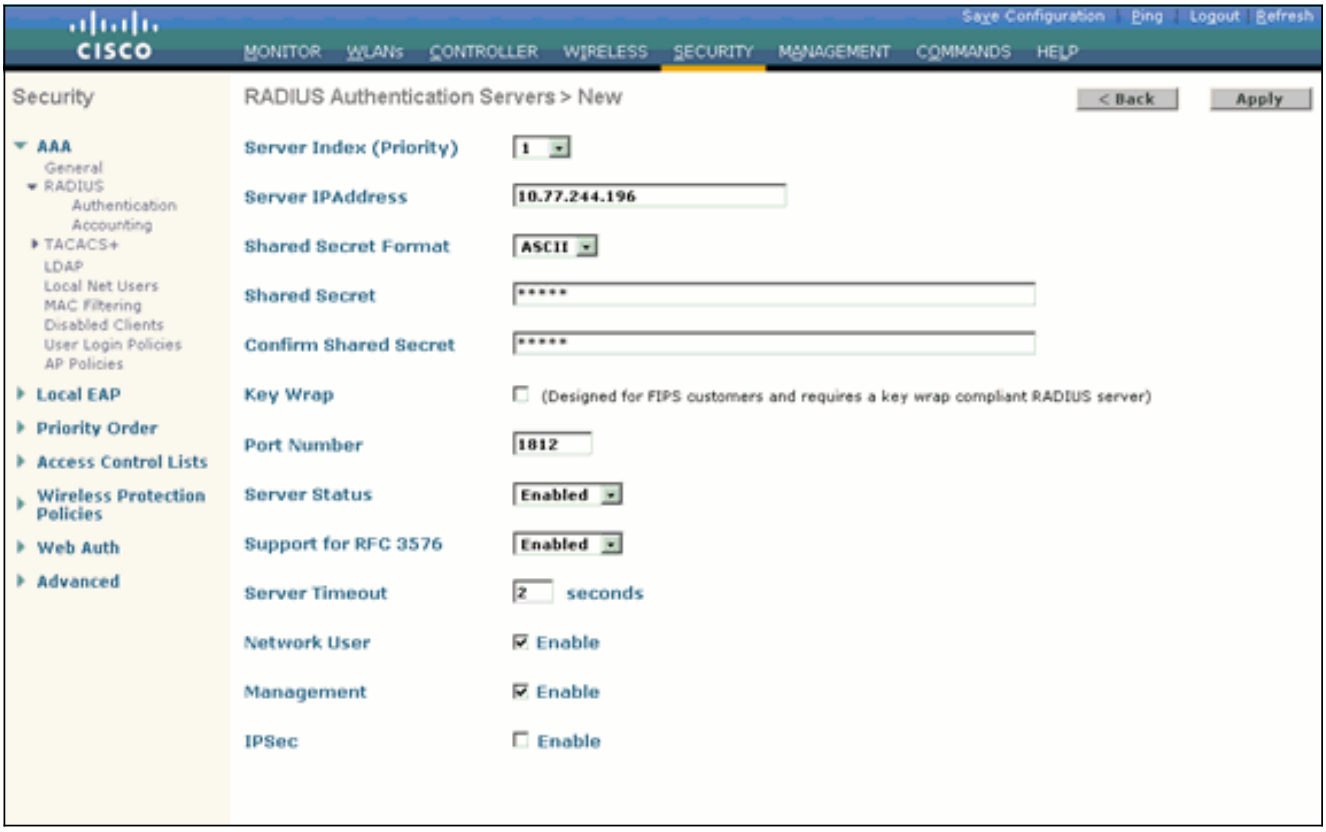
1. Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe
2. Configurer le WLAN pour l'authentification WPA2 en mode entreprise (EAP-FAST)
3. Configuration du client sans fil pour le mode WPA2 entreprise

Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe

WLC doit être configuré afin de transférer les identifiants de l'utilisateur à un serveur RADIUS externe. Le serveur RADIUS externe valide ensuite les informations d'identification de l'utilisateur à l'aide d'EAP-FAST et fournit l'accès aux clients sans fil.

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

1. Sélectionnez **Security et RADIUS Authentication depuis la GUI du contrôleur pour afficher la page des serveurs d'authentification RADIUS.** Cliquez ensuite sur **New** afin de définir un serveur RADIUS.
2. 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 serveurCe document utilise le serveur ACS avec l'adresse IP 10.77.244.196.



3. Cliquez sur **Apply**.

Configurer le WLAN pour le mode de fonctionnement WPA2 Enterprise

Configurez ensuite le WLAN que les clients utiliseront pour se connecter au réseau sans fil. Le SSID WLAN pour le mode WPA2 entreprise sera WPA2-Enterprise. Cet exemple attribue ce WLAN à l'interface de gestion.

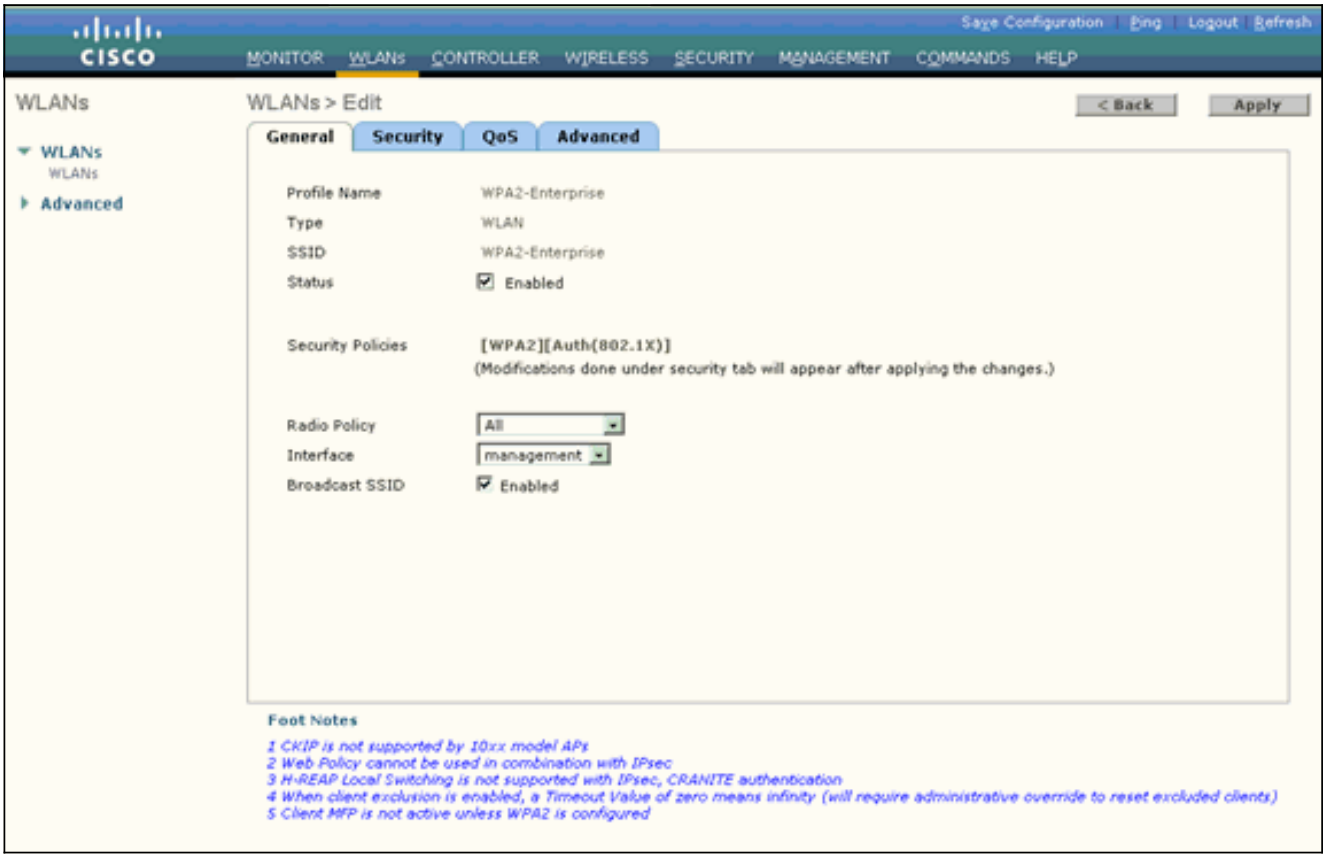
Complétez ces étapes afin de configurer le WLAN et ses paramètres associés :

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**. Cliquez

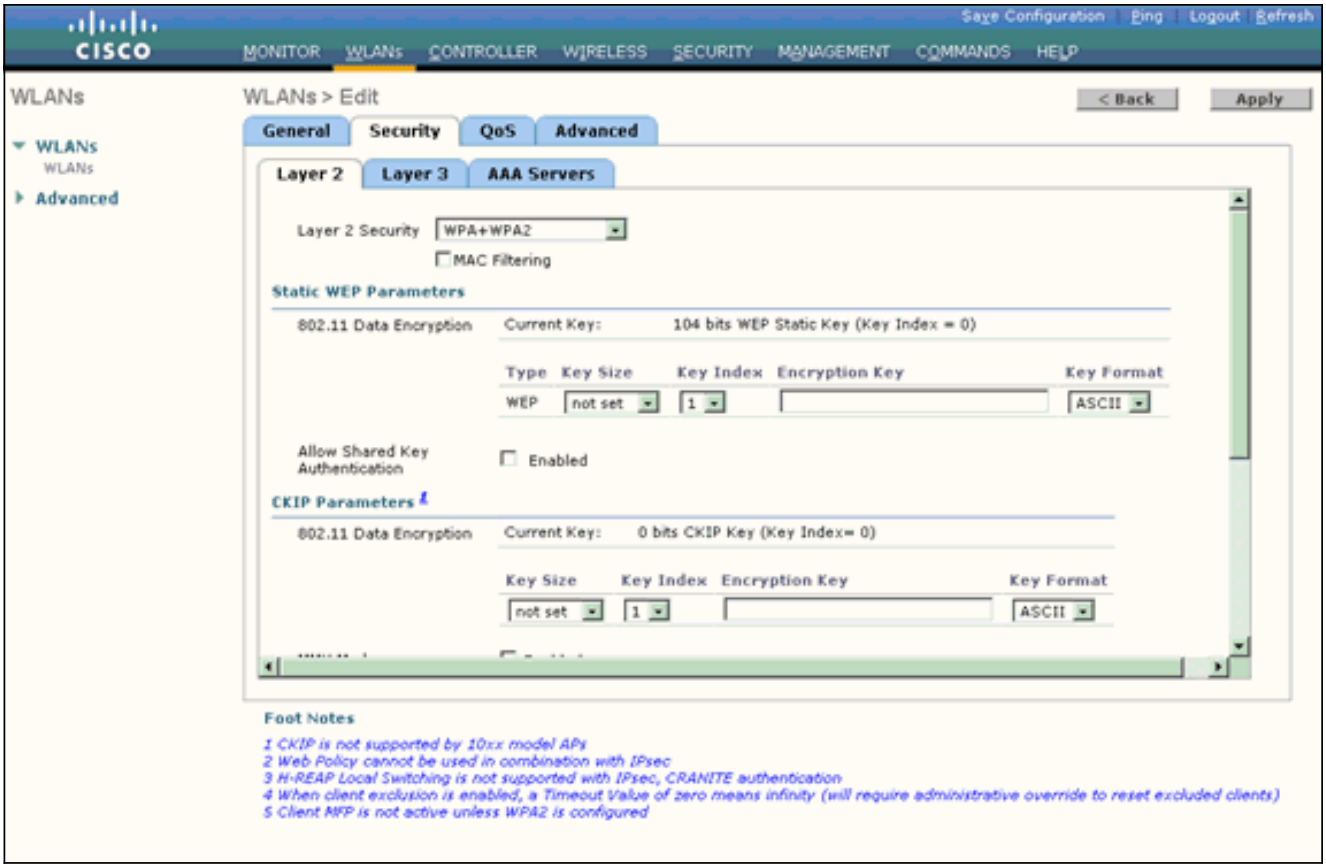
ensuite sur **Apply**.Cet exemple utilise **WPA2-Enterprise** comme SSID.



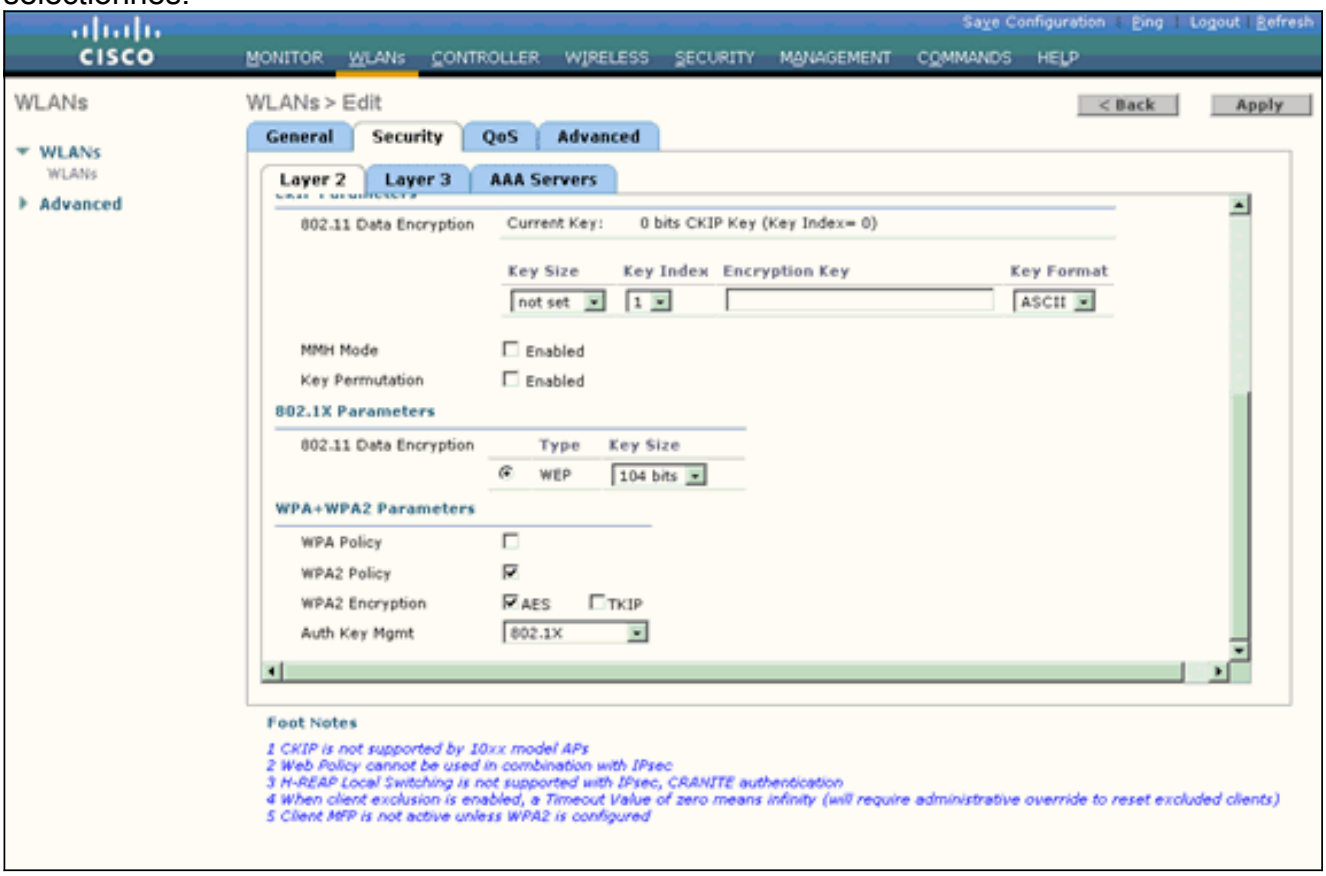
4. Une fois que vous avez créé un nouveau WLAN, la page **WLAN > Edit du nouveau WLAN apparaît.** Sur cette page, vous pouvez définir divers paramètres spécifiques à ce WLAN. Cela inclut les stratégies générales, les stratégies de sécurité, les stratégies QOS et les paramètres avancés.
5. Sous General Policies, cochez la case **Status** afin d'activer le WLAN.



6. Si vous voulez que le point d'accès diffuse le SSID dans ses trames de balise, cochez la case **Broadcast SSID**.
7. Cliquez sur l'onglet **Security.** Sous Layer 2 Security, sélectionnez **WPA+WPA2**.Cela active l'authentification WPA pour le WLAN.

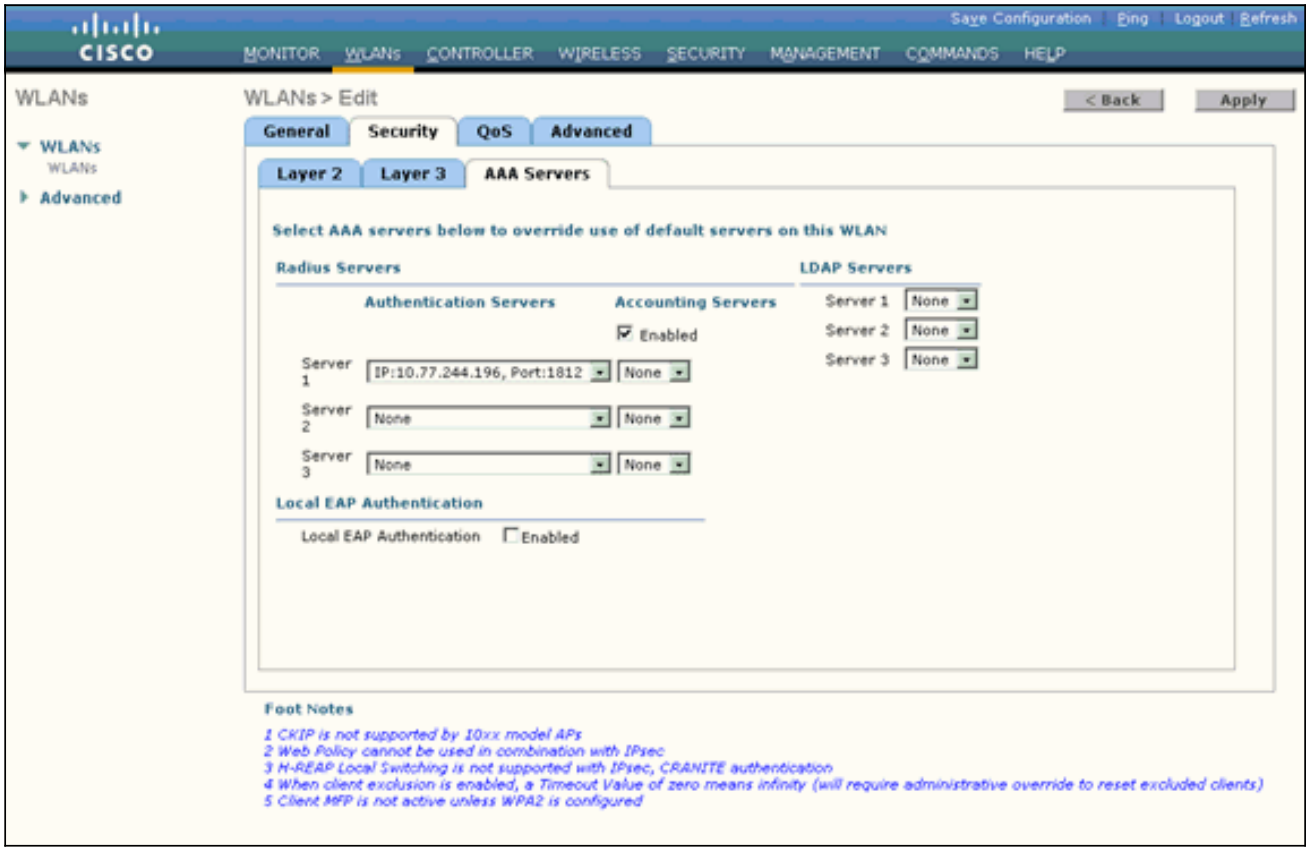


8. Faites défiler la page vers le bas pour modifier les paramètres **WPA+WPA2**.Dans cet exemple, la stratégie WPA2 et le cryptage AES sont sélectionnés.



9. Sous Auth Key Mgmt, sélectionnez **802.1x**.Cela active le WPA2 à l'aide de l'authentification 802.1x/EAP et du cryptage AES pour le WLAN.
10. Cliquez sur l'onglet **AAA Servers**. Sous Authentication Servers, sélectionnez l'adresse IP du serveur approprié.Dans cet exemple, 10.77.244.196 est utilisé comme serveur

RADIUS.



11. Cliquez sur **Apply**.**Remarque :** il s'agit du seul paramètre EAP qui doit être configuré sur le contrôleur pour l'authentification EAP. Toutes les autres configurations spécifiques à EAP-FAST doivent être effectuées sur le serveur RADIUS et les clients qui doivent être authentifiés.

Configurer le serveur RADIUS pour l'authentification en mode entreprise WPA2 (EAP-FAST)

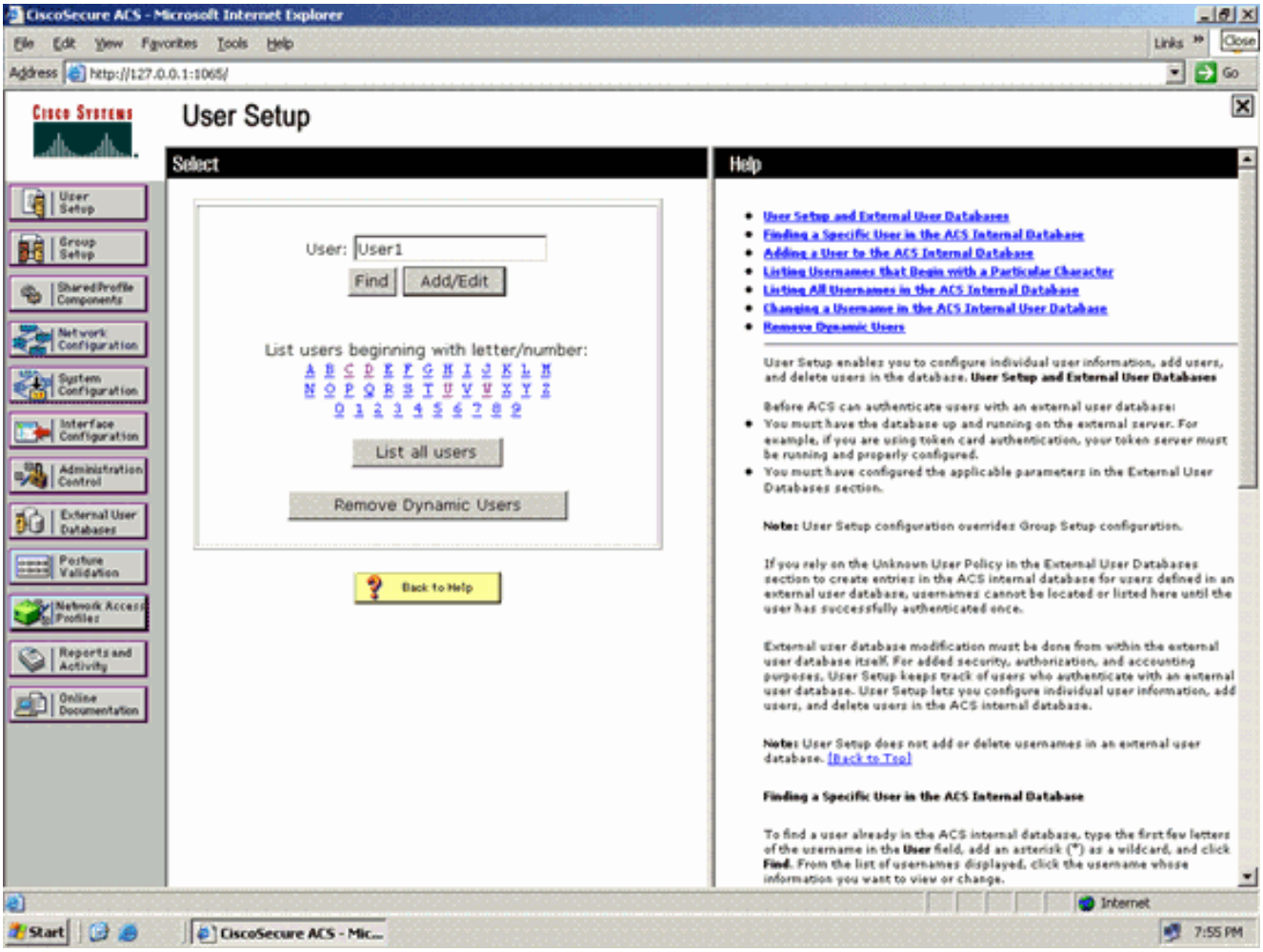
Dans cet exemple, Cisco Secure ACS est utilisé comme serveur RADIUS externe. Procédez comme suit afin de configurer le serveur RADIUS pour l'authentification EAP-FAST :

1. Créer une base de données utilisateur pour authentifier les clients
2. Ajouter le WLC en tant que client AAA au serveur RADIUS
3. Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement PAC intrabande anonyme**Remarque :** EAP-FAST peut être configuré avec l'approvisionnement PAC intrabande anonyme ou l'approvisionnement PAC intrabande authentifié. Cet exemple utilise le provisionnement PAC intrabande anonyme. Pour obtenir des informations détaillées et des exemples sur la configuration d'EAP FAST avec la mise en service PAC intrabande anonyme et la mise en service intrabande authentifiée, référez-vous à Exemple de configuration d'authentification EAP-FAST avec des contrôleurs LAN sans fil et un serveur RADIUS externe.

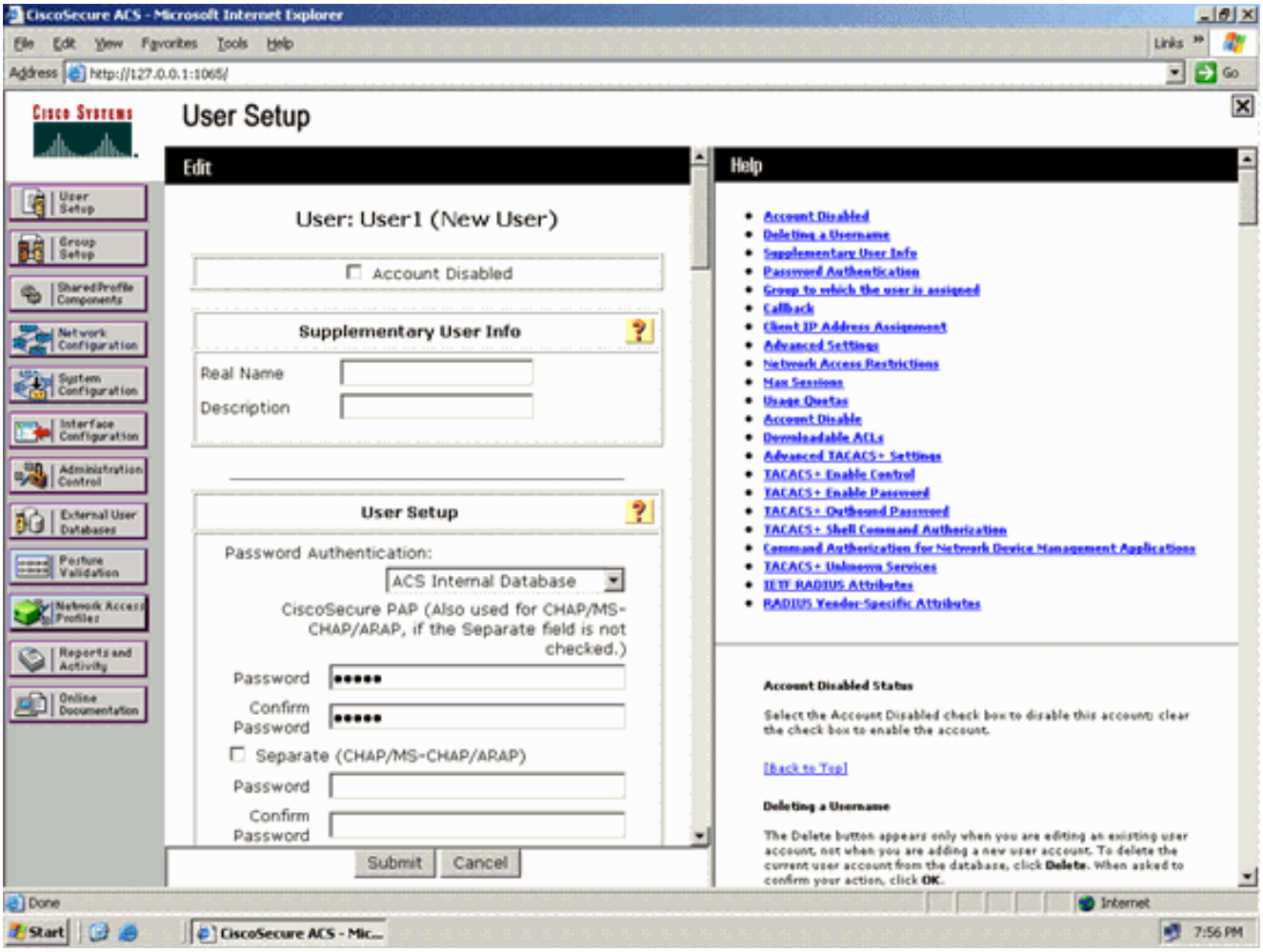
Créer une base de données utilisateur pour authentifier les clients EAP-FAST

Complétez ces étapes afin de créer une base de données utilisateur pour les clients EAP-FAST sur l'ACS. Cet exemple configure le nom d'utilisateur et le mot de passe du client EAP-FAST comme User1 et User1, respectivement.

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



2. 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 de mot de
passe.

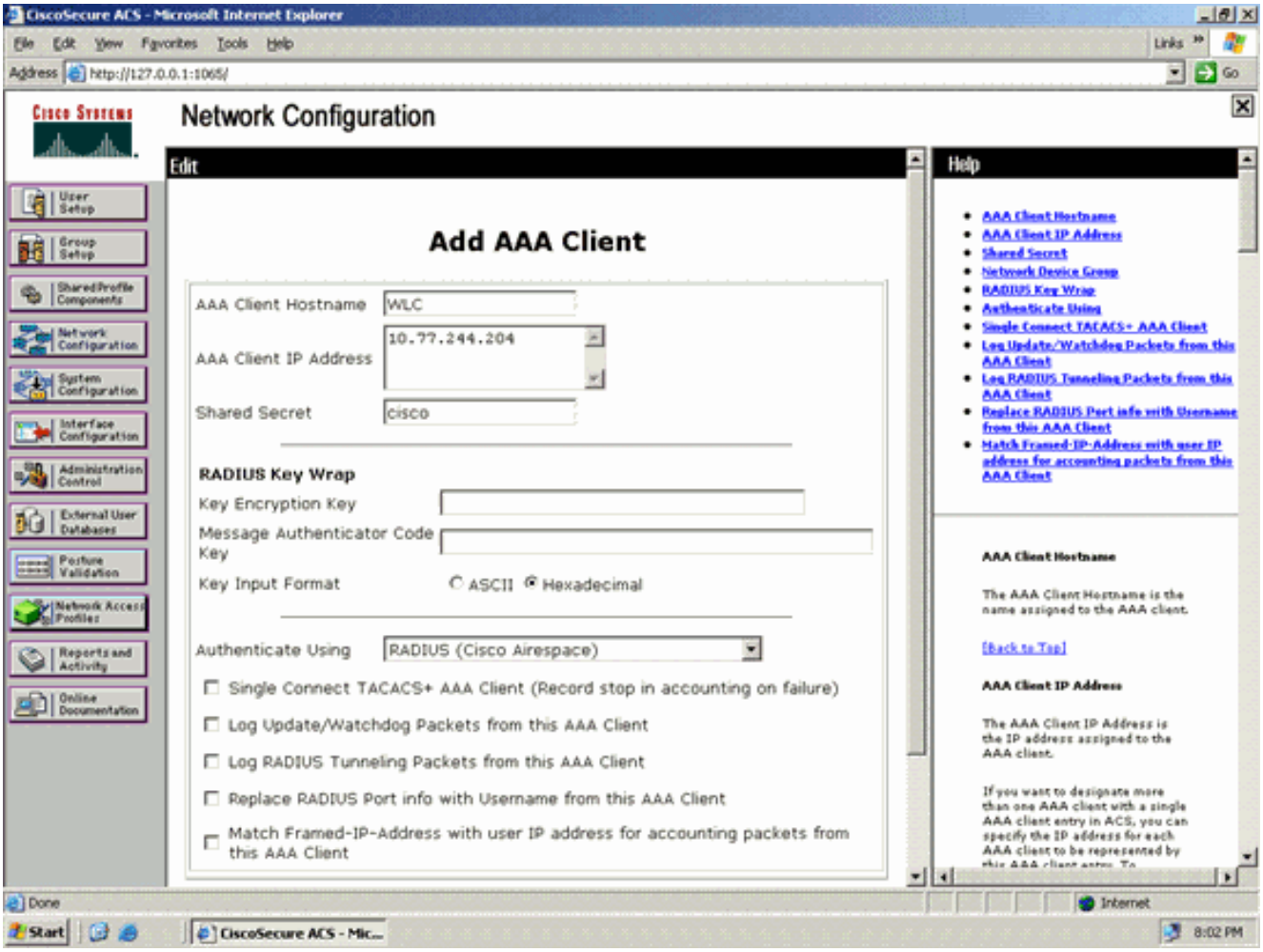


3. Choisissez **ACS Internal Database** dans la liste déroulante Password Authentication.
4. Configurez tous les autres paramètres requis et cliquez sur **Submit**.

Ajouter le WLC en tant que client AAA au serveur RADIUS

Complétez ces étapes afin de définir le contrôleur en tant que client AAA sur le serveur ACS :

1. Cliquez sur **Network Configuration depuis l'interface graphique ACS.** Dans la section Add AAA client de la page Network Configuration, cliquez sur **Add Entry** afin d'ajouter le WLC comme client AAA au serveur RADIUS.
2. Sur la page AAA Client, définissez le nom du WLC, l'adresse IP, le secret partagé et la méthode d'authentification (RADIUS/Cisco Airespace). Référez-vous à la documentation du constructeur pour d'autres serveurs d'authentification non-ACS.



Remarque : la clé secrète partagée que vous configurez sur le WLC et le serveur ACS doit correspondre. Le secret partagé distingue les majuscules et minuscules.

3. Cliquez sur **Envoyer+Appliquer**.

Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement PAC intrabande anonyme

Approvisionnement en bande anonyme

Il s'agit de l'une des deux méthodes de mise en service intrabande selon lesquelles l'ACS établit une connexion sécurisée avec le client de l'utilisateur final dans le but de fournir au client un nouveau PAC. Cette option permet une connexion TLS anonyme entre le client de l'utilisateur final et ACS.

Cette méthode fonctionne à l'intérieur d'un tunnel ADHP (Authenticated Diffie-HellmanKey Agreement Protocol) avant que l'homologue authentifie le serveur ACS.

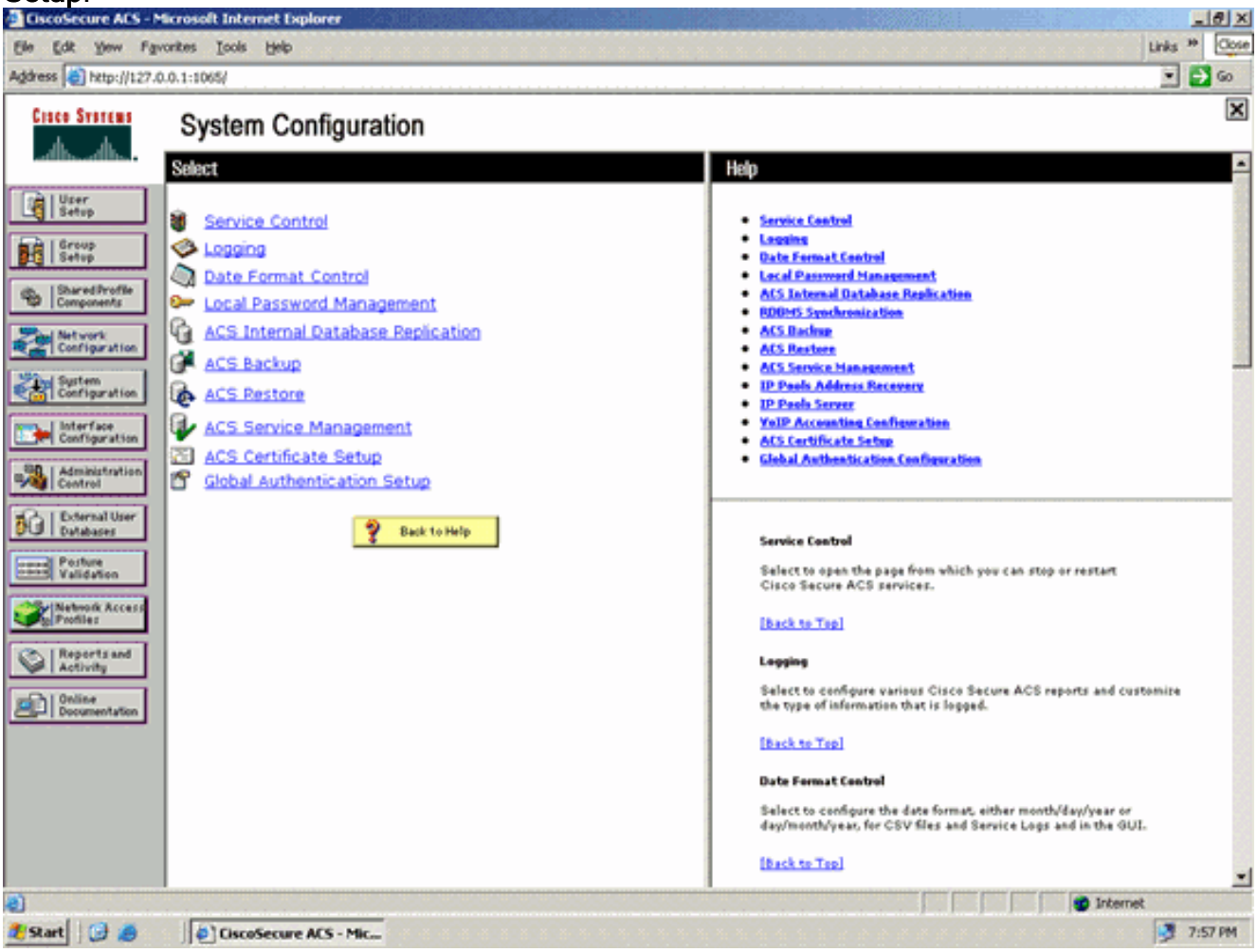
Ensuite, l'ACS requiert l'authentification EAP-MS-CHAPv2 de l'utilisateur. Une fois l'authentification utilisateur réussie, l'ACS établit un tunnel Diffie-Hellman avec le client utilisateur final. L'ACS génère un PAC pour l'utilisateur et l'envoie au client de l'utilisateur final dans ce tunnel, avec des informations sur cet ACS. Cette méthode d'approvisionnement utilise EAP-MSCHAPv2 comme méthode d'authentification dans la phase zéro et EAP-GTC dans la phase deux.

Étant donné qu'un serveur non authentifié est configuré, il n'est pas possible d'utiliser un mot de passe en texte clair. Par conséquent, seules les informations d'identification MS-CHAP peuvent

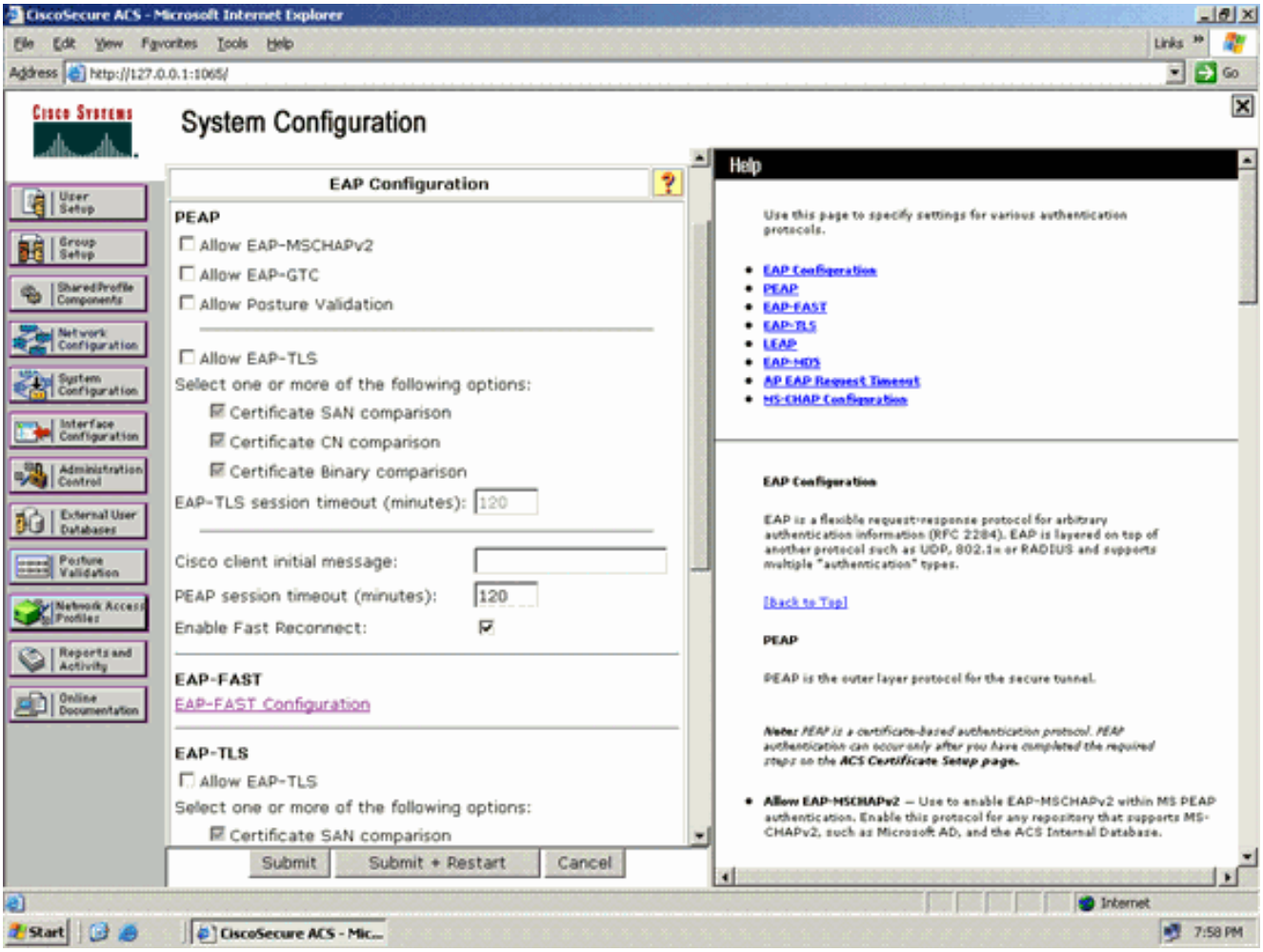
être utilisées à l'intérieur du tunnel. MS-CHAPv2 est utilisé pour prouver l'identité de l'homologue et recevoir un PAC pour d'autres sessions d'authentification (EAP-MS-CHAP sera utilisé comme méthode interne uniquement).

Complétez ces étapes afin de configurer l'authentification EAP-FAST dans le serveur RADIUS pour l'approvisionnement en bande anonyme :

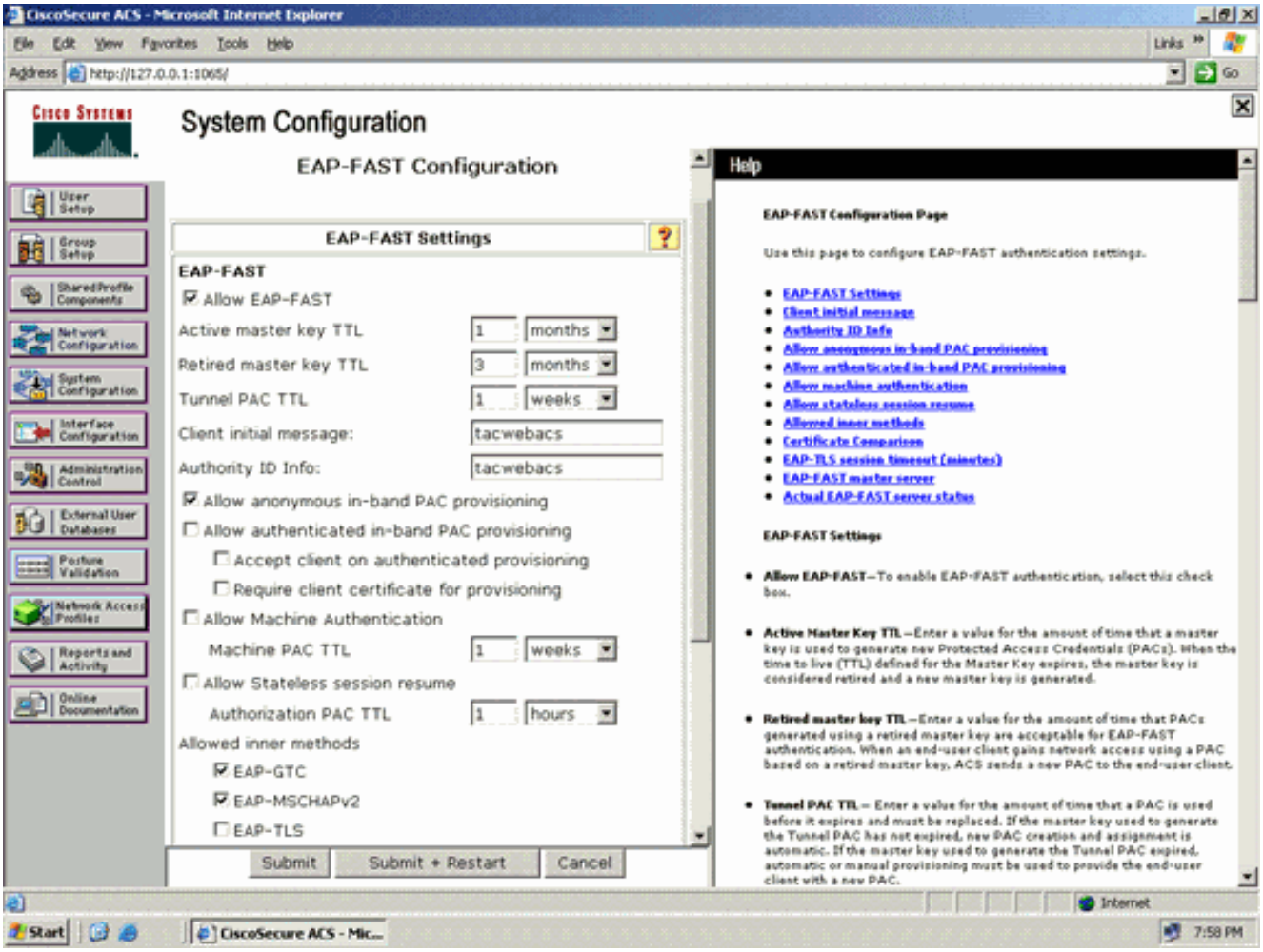
1. Cliquez sur **System Configuration** dans l'interface utilisateur graphique du serveur RADIUS. Dans la page System Configuration, sélectionnez **Global Authentication Setup**.



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. Sur la page EAP-FAST Settings, cochez la case **Allow EAP-FAST** pour activer EAP-FAST dans le serveur
RADIUS.



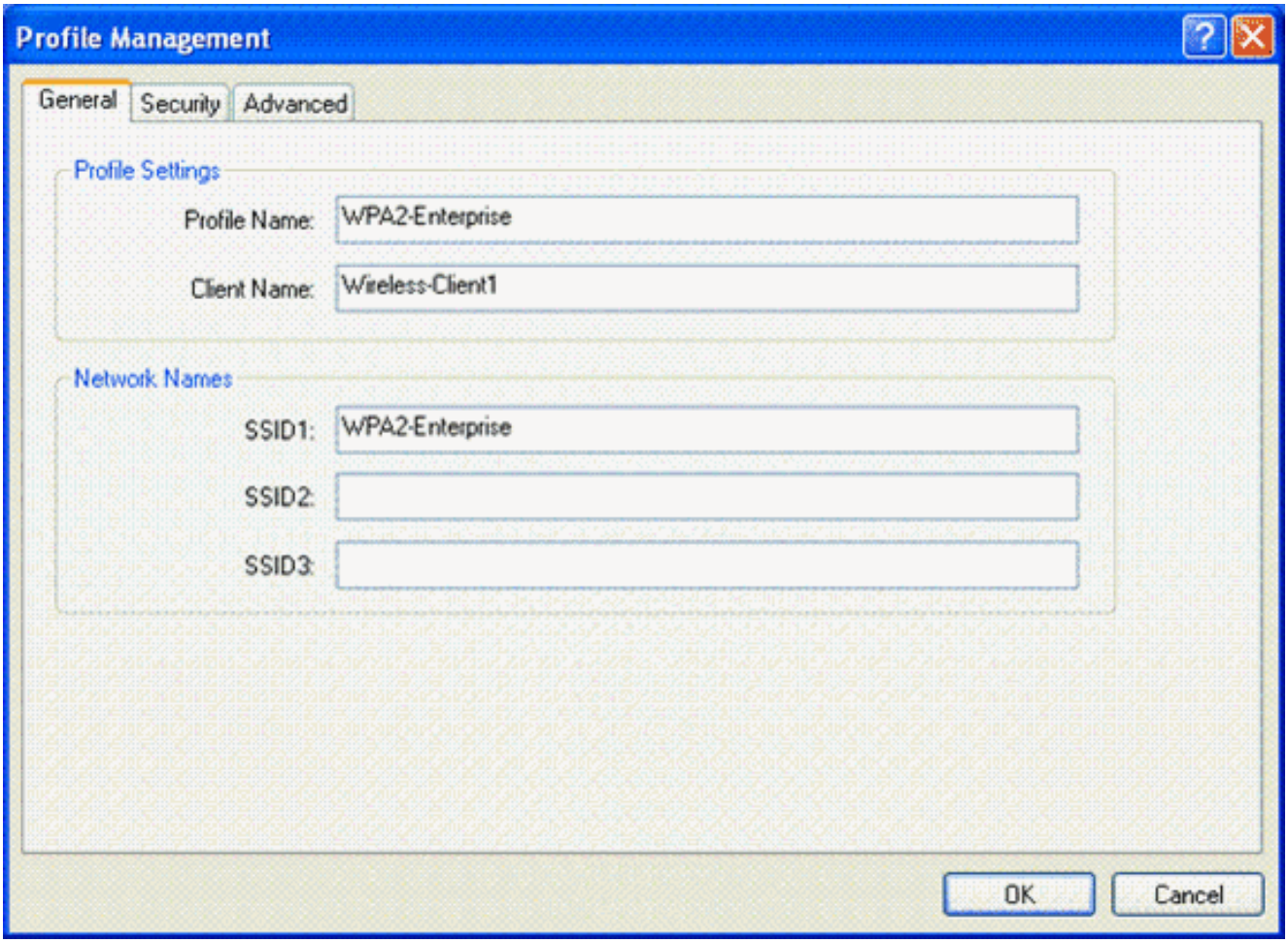
4. Configurez les valeurs TTL (Time-to-Live) de la clé principale active/retirée comme vous le souhaitez, ou définissez-la sur la valeur par défaut, comme indiqué dans cet exemple.Référez-vous à Clés maîtres pour des informations sur les clés maîtres actives et retirées. Consultez également Clés principales et TTL PAC pour plus d'informations.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. **Allowed inner methods** : cette option détermine quelles méthodes EAP internes peuvent être exécutées dans le 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).

Configuration du client sans fil pour le mode de fonctionnement WPA2 Enterprise

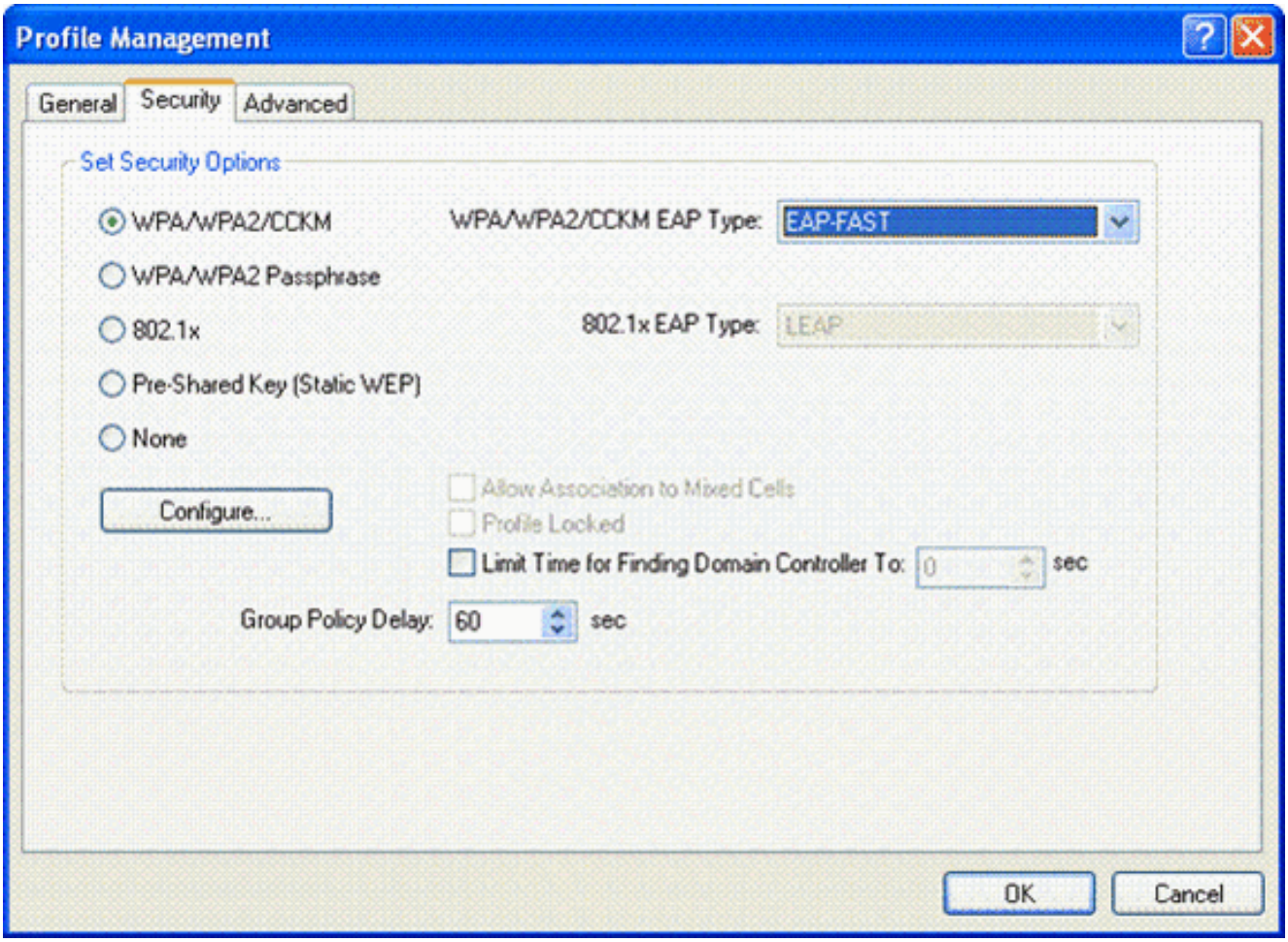
L'étape suivante consiste à configurer le client sans fil pour le mode de fonctionnement WPA2 Entreprise.

Complétez ces étapes afin de configurer le client sans fil pour le mode WPA2 Entreprise.

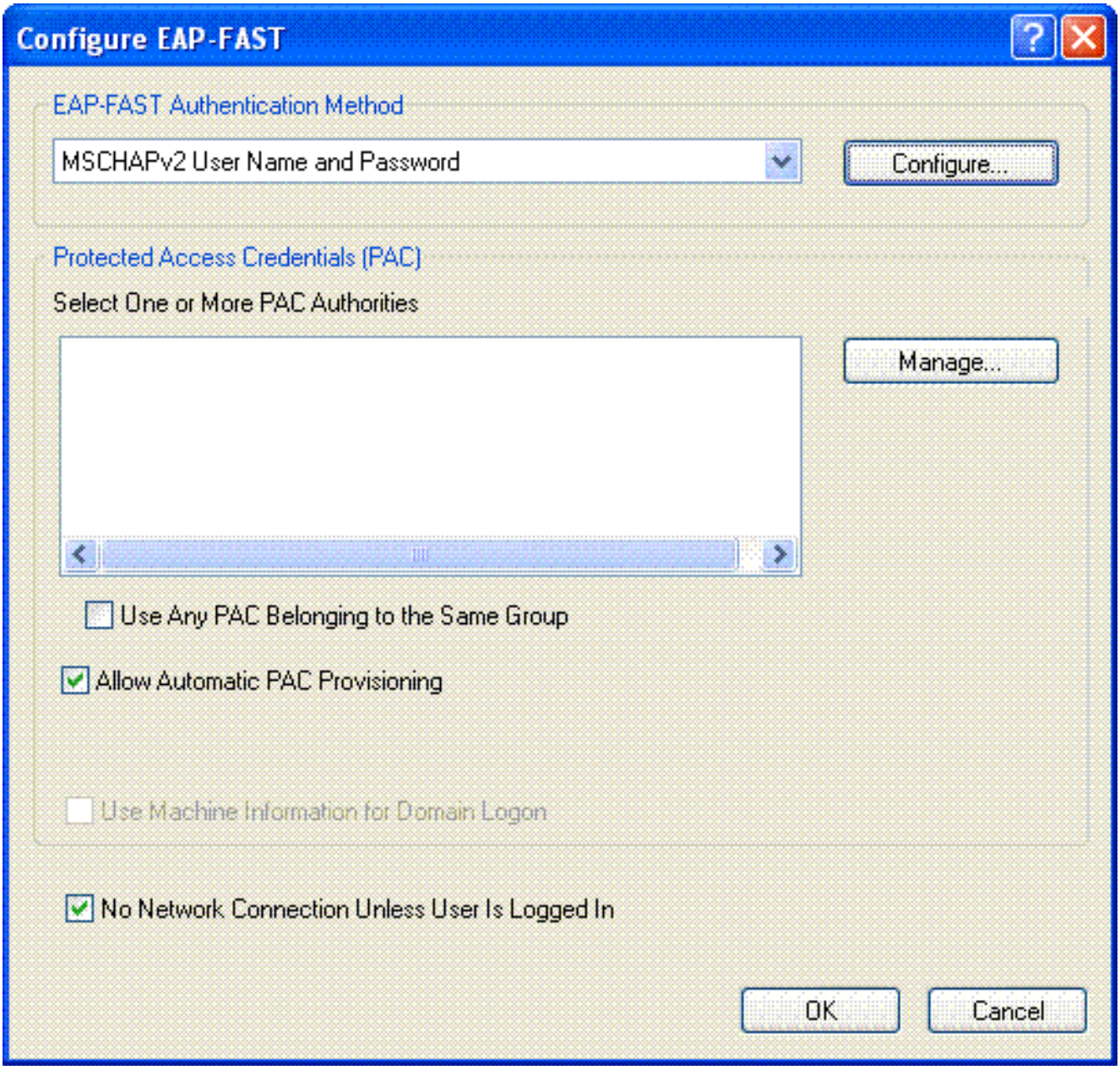
1. Dans la fenêtre Aironet Desktop Utility, cliquez sur **Profile Management > New** afin de créer un profil pour l'utilisateur WLAN WPA2-Enterprise.Comme mentionné précédemment, ce document utilise le nom WLAN/SSID comme **WPA2-Enterprise** pour le client sans fil.
2. Dans la fenêtre Profile Management, cliquez sur l'onglet **General** et configurez le nom du profil, le nom du client et le nom du SSID comme indiqué dans cet exemple. Cliquez ensuite sur
OK



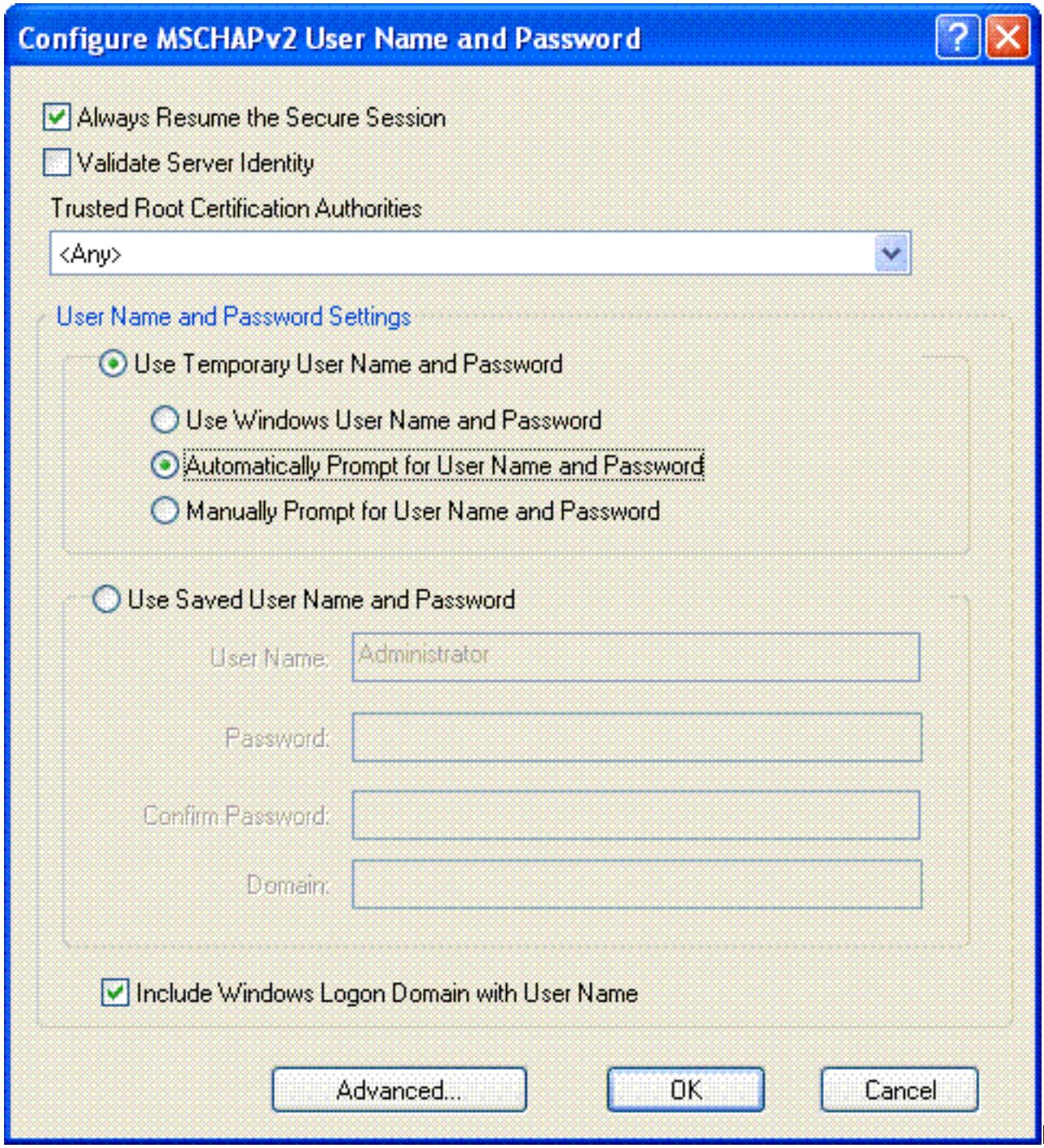
3. Cliquez sur l'onglet **Security** et choisissez **WPA/WPA2/CCKM** pour activer le mode de fonctionnement WPA2. Sous WPA/WPA2/CCKM EAP Type, sélectionnez **EAP-FAST**. Cliquez sur **Configure** afin de configurer le paramètre EAP-
FAST.



4. Dans la fenêtre Configure EAP-FAST, cochez la case **Allow Automatic PAC Provisioning**. Si vous souhaitez configurer le provisionnement PAC anonyme, EAP-MS-CHAP sera utilisé comme seule méthode interne de la phase
zéro.



5. Sélectionnez Nom d'utilisateur et mot de passe MSCHAPv2 comme méthode d'authentification dans la liste déroulante Méthode d'authentification EAP-FAST. Cliquez sur **Configure**.
6. Dans la fenêtre Configurer le nom d'utilisateur et le mot de passe MSCHAPv2, sélectionnez les paramètres de nom d'utilisateur et de mot de passe appropriés.Cet exemple choisit **Automatically Prompt for User Name and Password**.



Le même nom d'utilisateur et le même mot de passe doivent être enregistrés auprès de l'ACS. Comme mentionné précédemment, cet exemple utilise respectivement User1 et User1 comme nom d'utilisateur et mot de passe. Notez également qu'il s'agit d'une mise en service intrabande anonyme. Par conséquent, le client ne peut pas valider le certificat du serveur. Vous devez vous assurer que la case Valider l'identité du serveur est décochée.

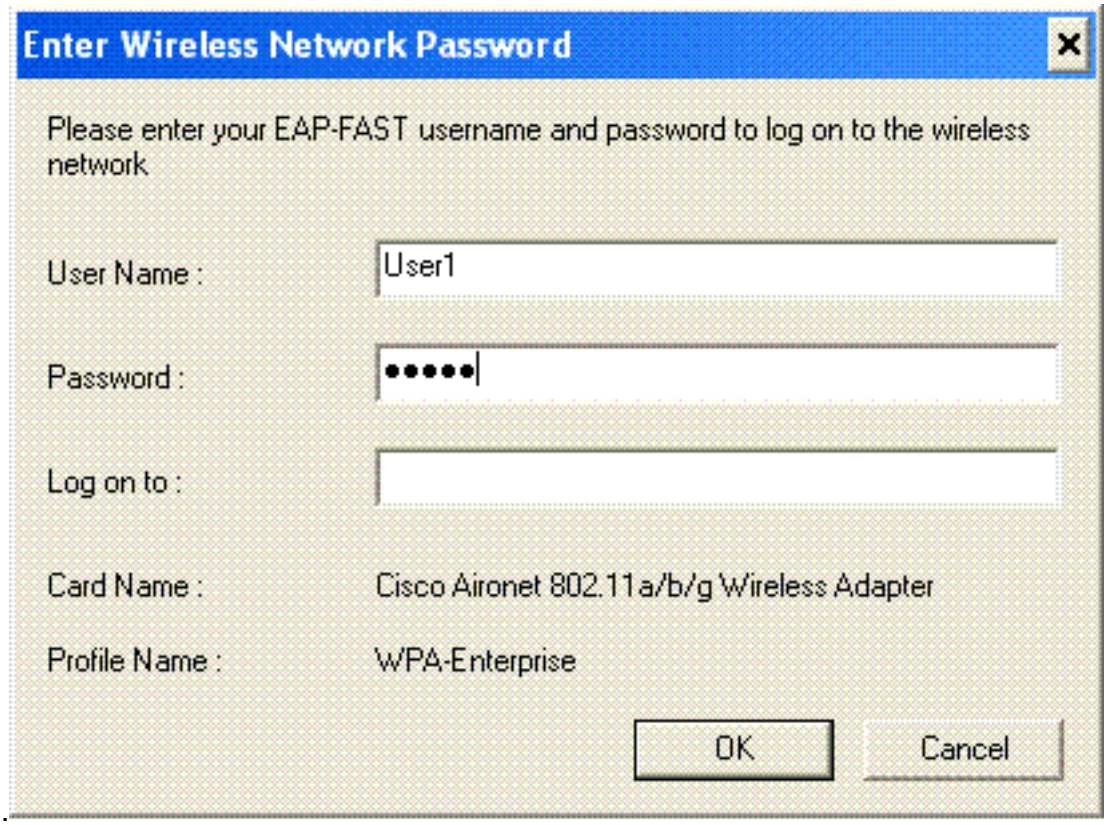
7. Click OK.

Vérification du mode de fonctionnement WPA2 Enterprise

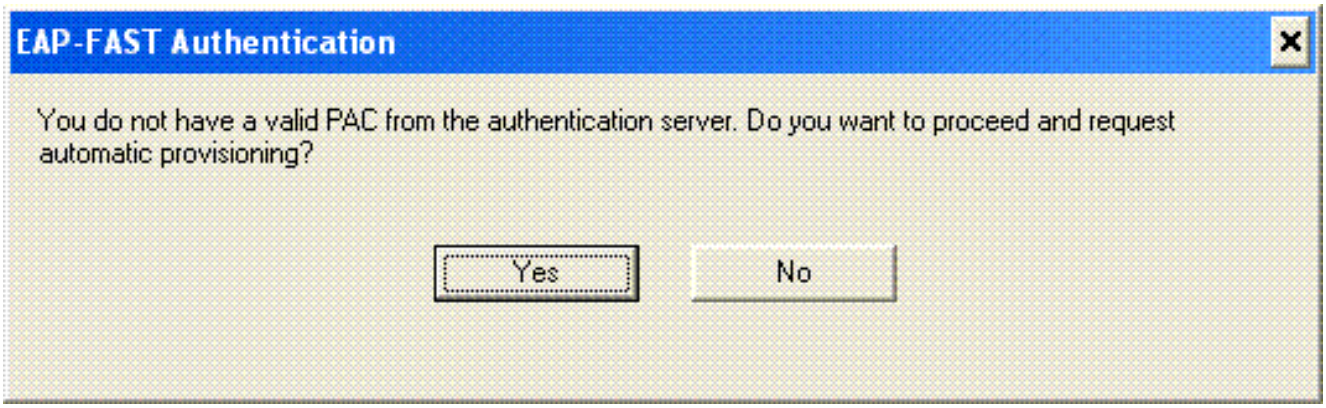
Complétez ces étapes afin de vérifier si votre configuration du mode WPA2 Entreprise fonctionne correctement :

1. Dans la fenêtre Aironet Desktop Utility, sélectionnez le profil **WPA2-Enterprise** et cliquez sur **Activate** afin d'activer le profil client sans fil.
2. Si vous avez activé l'authentification MS-CHAP ver2, le client vous demandera le nom

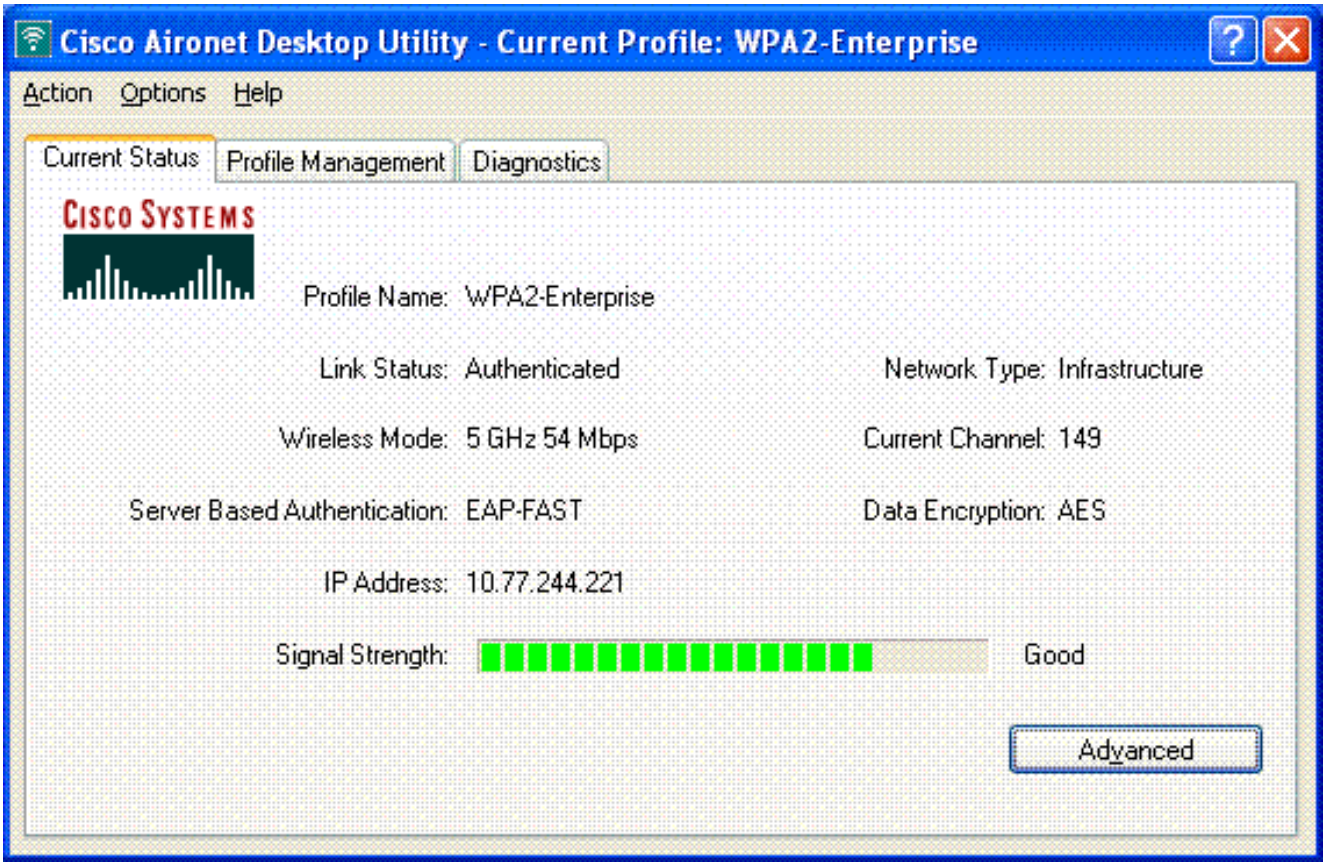
d'utilisateur et le mot de passe.



3. Pendant le traitement EAP-FAST de l'utilisateur, le client vous demandera de demander PAC au serveur RADIUS. Lorsque vous cliquez sur **Yes**, l'approvisionnement PAC démarre.



4. Une fois le provisionnement PAC réussi dans la phase zéro, les phases un et deux suivent et une procédure d'authentification réussie a lieu.Une fois l'authentification réussie, le client sans fil est associé au WLAN WPA2-Enterprise. Voici la capture d'écran :



Vous pouvez également vérifier si le serveur RADIUS reçoit et valide la demande d'authentification du client sans fil. Pour ce faire, vérifiez les rapports Passed Authentications et Failed Attempts sur le serveur ACS pour savoir si l'authentification a réussi ou échoué. Ces rapports sont disponibles sous l'option Reports and Activities sur le serveur ACS.

Configuration des périphériques pour le mode WPA2 Personal

Procédez comme suit afin de configurer les périphériques pour le mode de fonctionnement WPA2-Personal :

1. Configuration du WLAN pour l'authentification en mode personnel WPA2
2. Configuration du client sans fil pour le mode WPA2 personnel

Configuration du WLAN pour le mode de fonctionnement personnel WPA2

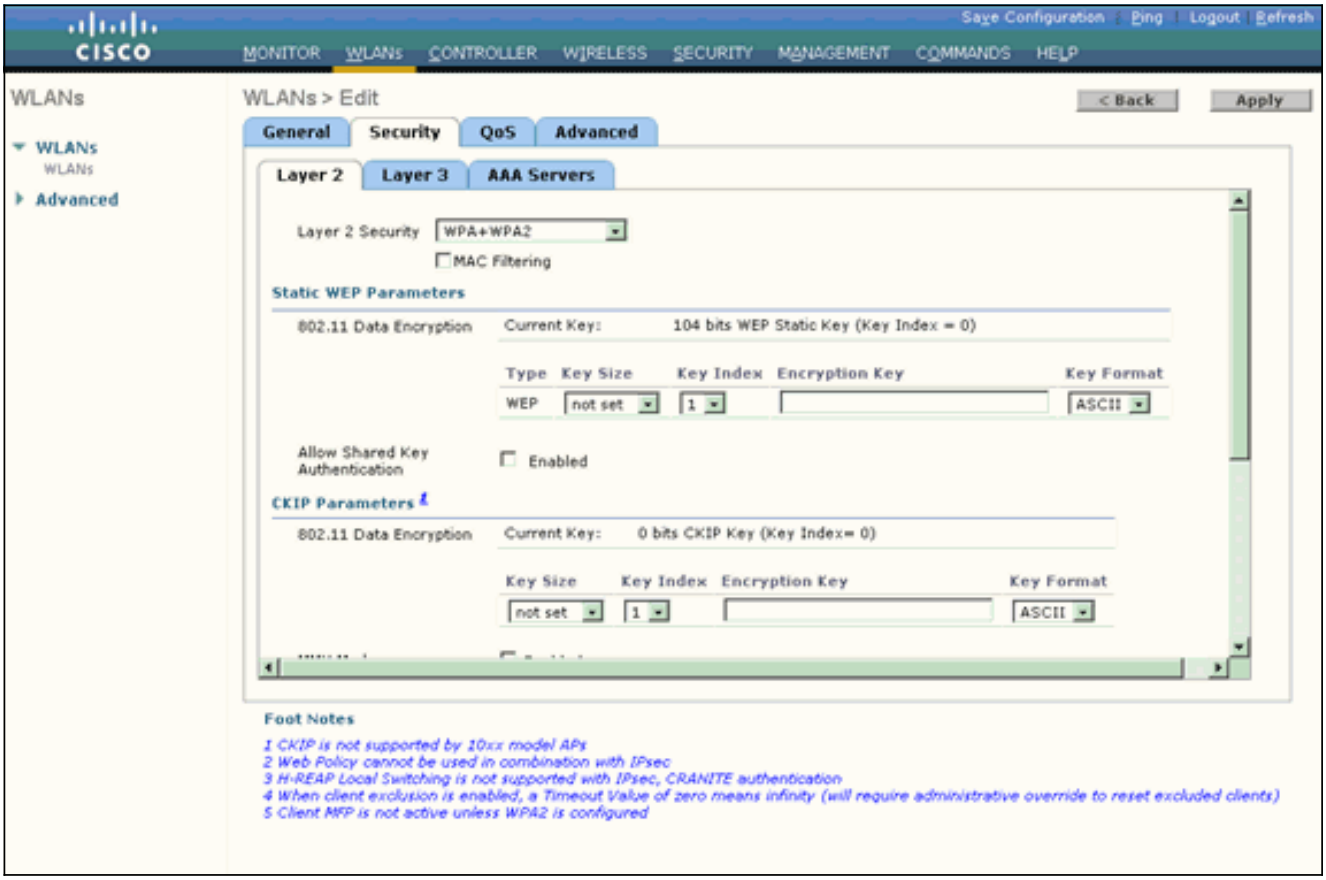
Vous devez configurer le WLAN que les clients utiliseront pour se connecter au réseau sans fil. Le SSID WLAN du mode WPA2 personnel est WPA2 personnel. Cet exemple attribue ce WLAN à l'interface de gestion.

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

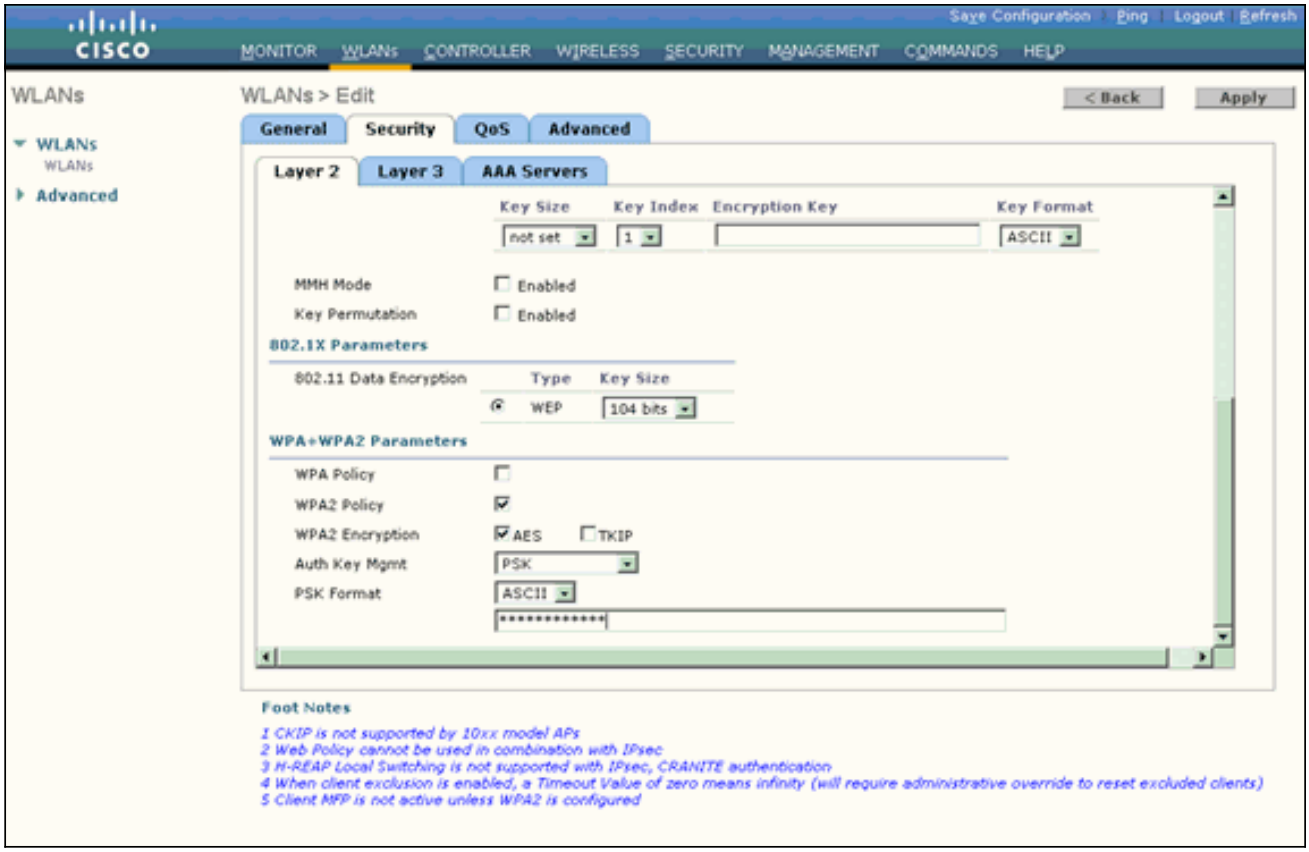
1. Cliquez sur les **WLAN de la GUI du contrôleur afin d'afficher la page des WLAN.**Cette page énumère les WLAN qui existent sur le contrôleur.
2. Cliquez sur New [nouveau] pour créer un autre WLAN.
3. Saisissez le nom SSID WLAN, le nom du profil et l'ID WLAN dans la page WLANs > New. Cliquez ensuite sur **Apply**.Cet exemple utilise **WPA2-Personal** comme SSID.



4. 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.
5. Sous General Policies, cochez la case **Status** afin d'activer le WLAN.
6. Si vous voulez que le point d'accès diffuse le SSID dans ses trames de balise, cochez la case **Broadcast SSID**.
7. Cliquez sur l'onglet **Security.** Sous Layer Security, sélectionnez **WPA+WPA2**.Cela active l'authentification WPA pour le WLAN.



8. Faites défiler la page vers le bas pour modifier les paramètres **WPA+WPA2**.Dans cet exemple, la stratégie WPA2 et le cryptage AES sont sélectionnés.
9. Sous Auth Key Mgmt, choisissez **PSK** afin d'activer WPA2-PSK.
10. Saisissez la clé pré-partagée dans le champ approprié, comme indiqué.



Remarque : la clé pré-partagée utilisée sur le WLC doit correspondre à celle configurée sur les clients sans fil.

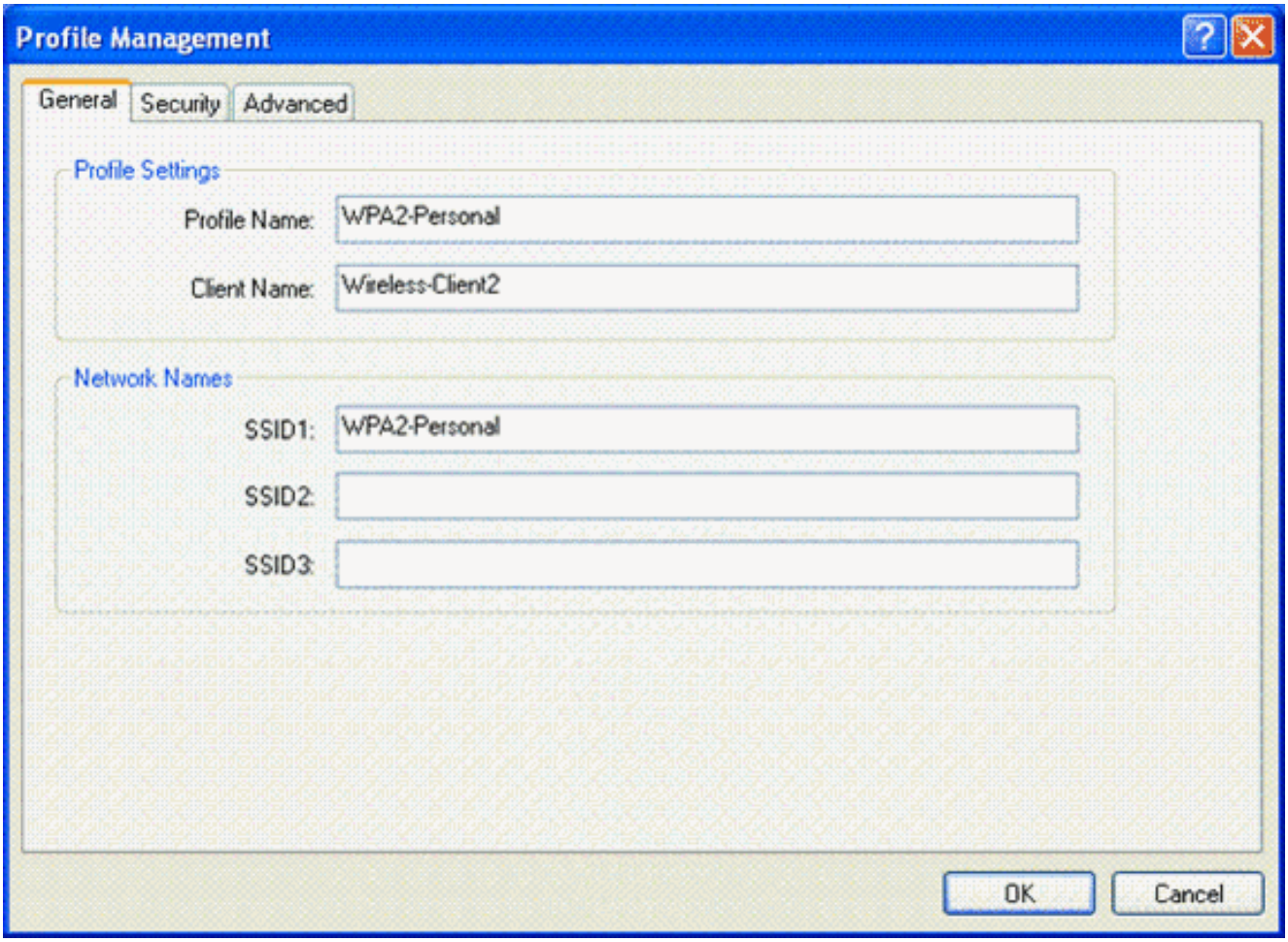
11. Cliquez sur **Apply**.

Configuration du client sans fil pour le mode WPA2 personnel

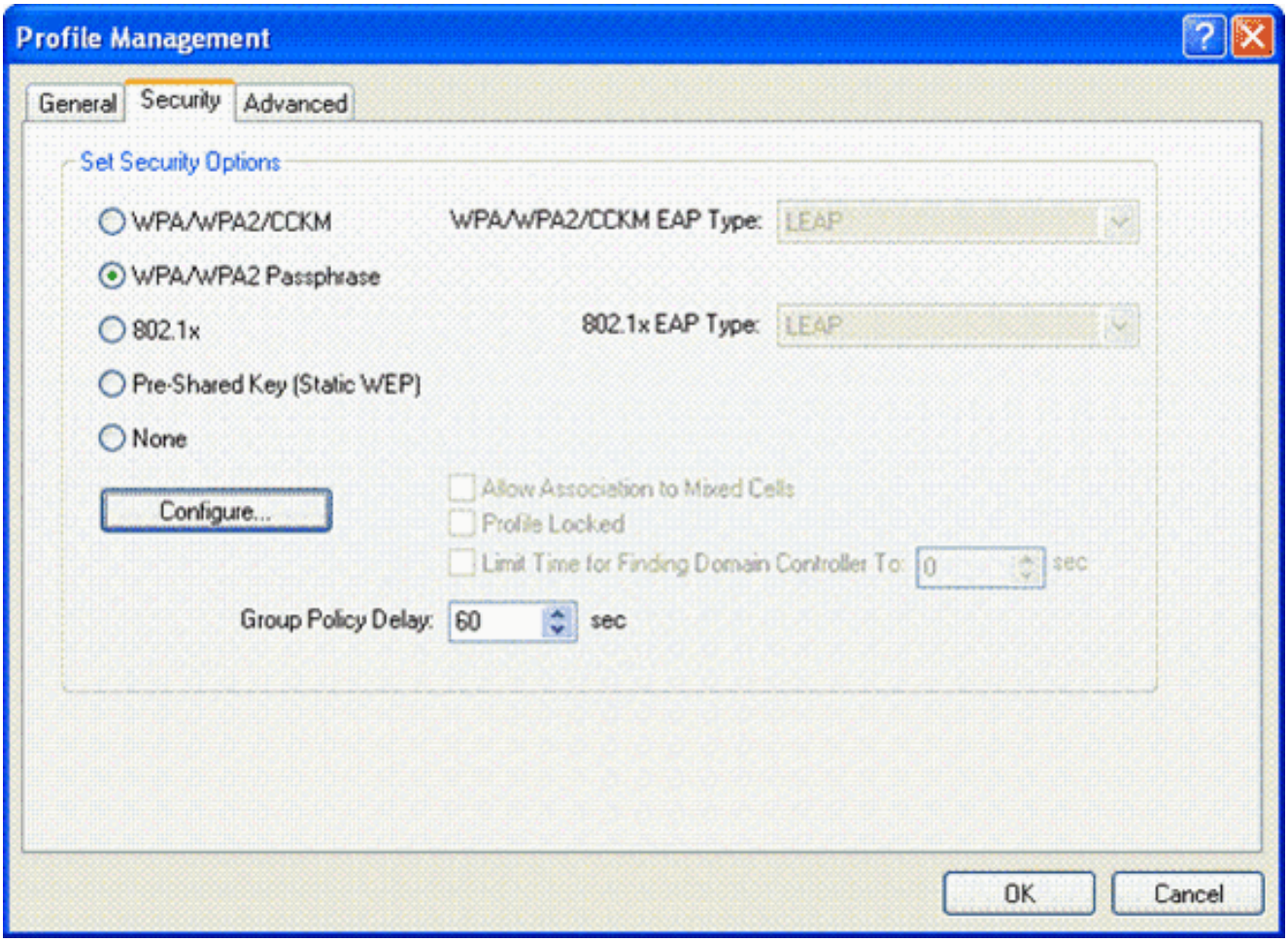
L'étape suivante consiste à configurer le client sans fil pour le mode de fonctionnement WPA2-Personal.

Complétez ces étapes afin de configurer le client sans fil pour le mode WPA2-Personal :

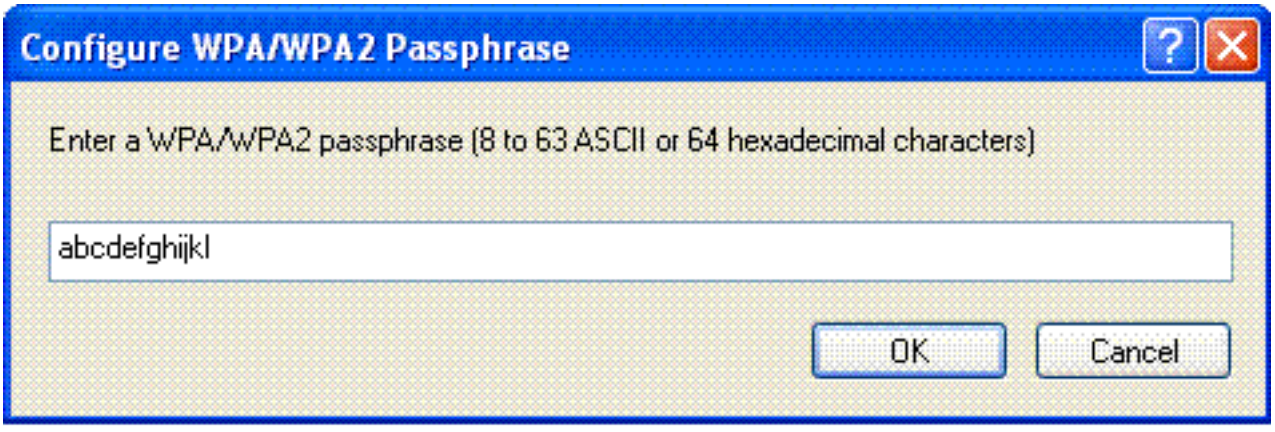
1. Dans la fenêtre Aironet Desktop Utility, cliquez sur **Profile Management > New** afin de créer un profil pour l'utilisateur WLAN WPA2-PSK.
2. Dans la fenêtre Profile Management, cliquez sur l'onglet **General** et configurez le nom du profil, le nom du client et le nom du SSID comme indiqué dans cet exemple. Cliquez ensuite sur
OK.



3. Cliquez sur l'onglet **Security** et choisissez **WPA/WPA2 Passphrase** pour activer le mode de fonctionnement WPA2-PSK. Cliquez sur **Configure** afin de configurer la clé pré-partagée WPA-
PSK.



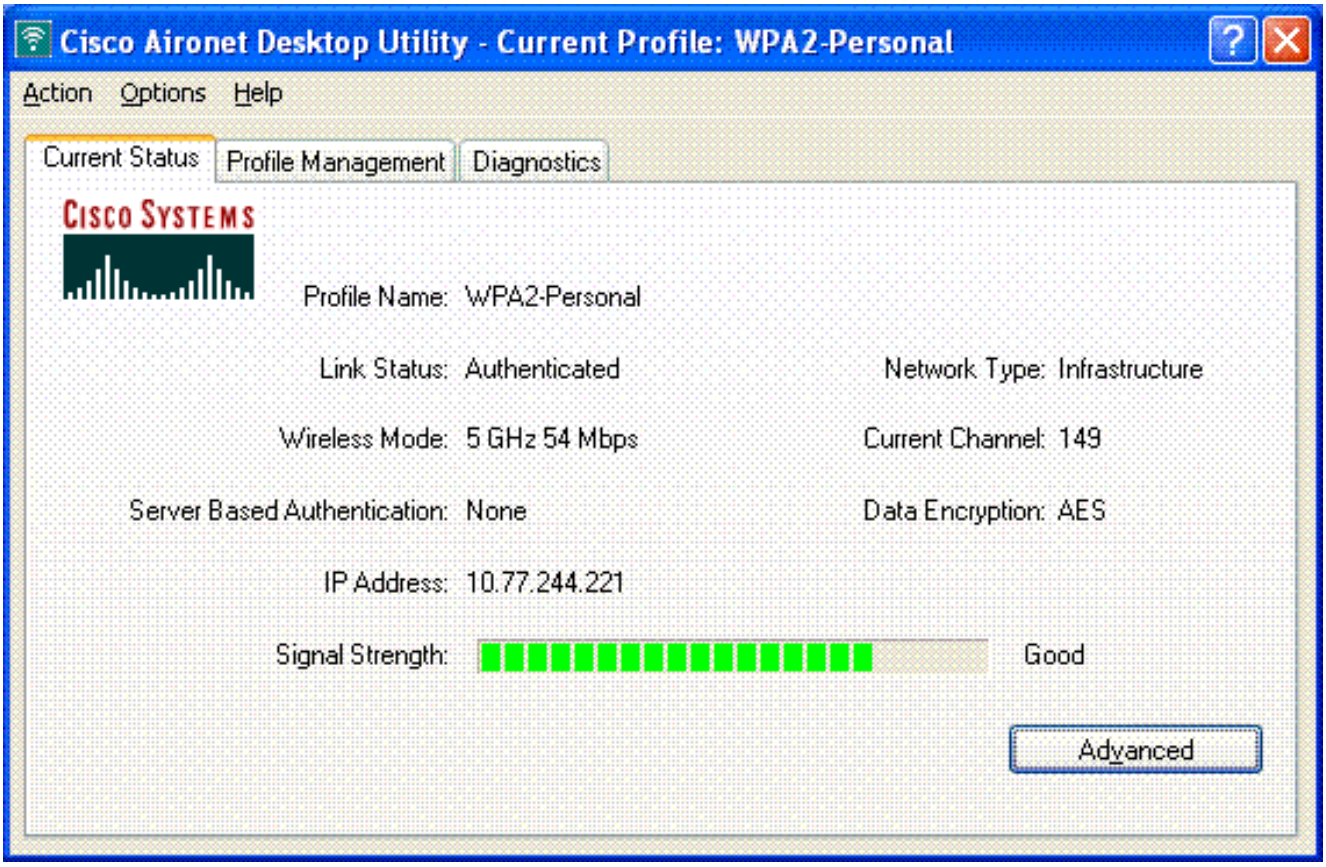
4. Entrez la clé pré-partagée et cliquez sur **OK**.



Vérification du mode de fonctionnement WPA2-Personal

Complétez ces étapes afin de vérifier si votre configuration du mode WPA2-Enterprise fonctionne correctement :

1. Dans la fenêtre Aironet Desktop Utility, sélectionnez le profil **WPA2-Personal** et cliquez sur **Activate** afin d'activer le profil client sans fil.
2. Une fois le profil activé, le client sans fil s'associe au WLAN après une authentification réussie.Voici la capture d'écran :



Dépannage

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

Ces commandes **debug** seront utiles pour dépanner la configuration :

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

- **debug dot1x events enable** : active le débogage de tous les événements dot1x. Voici un exemple de résultat de débogage basé sur une authentification réussie :**Remarque :** certaines des lignes de cette sortie ont été déplacées vers des secondes lignes en raison de limitations d'espace.

```
(Cisco Controller)>debug dot1x events enable
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with
mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response
(count=2) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
.....
.....
.....
.....

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from
```

mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93**
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)**
Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)**
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for

```
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 26)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for
mobile00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to
mobile 00:4096:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2)
from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===>
20 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===>
24 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry for
```

```
tation 00:40:96:af:3e:93 (RSN 0)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in
Authenticating state for mobile 00:40:96:af:3e:93
```

- **debug dot1x packet enable** : active le débogage des messages de paquets 802.1x.
- **debug aaa events enable** : active la sortie de débogage de tous les événements aaa.

Informations connexes

- WPA2 - Wi-Fi Protected Access 2
- Exemple de configuration d'authentification EAP-FAST avec des contrôleurs de réseau local sans fil et un serveur RADIUS externe
- Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil (WLC)
- Présentation de la configuration WPA
- Assistance produit 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.

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.