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

Contenu

Introduction

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

Conditions préalables

Conditions requises

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

- WPA
- Solutions de sécurité Sans fil du RÉSEAU LOCAL (WLAN)**Remarque:** Référez-vous à l'aperçu Sans fil de Sécurité LAN de Cisco pour les informations sur des solutions de sécurité de WLAN Cisco.

Composants utilisés

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

- Point d'accès léger (LAP) de gamme Cisco 1000
- Le contrôleur LAN sans fil Cisco 4404 (WLC) ce exécute le micrologiciel 4.2.61.0
- Adaptateur de client de Cisco 802.11a/b/g qui exécute le micrologiciel 4.1
- Aironet Desktop Utility (ADU) ce exécute le micrologiciel 4.1
- Version 4.1 de serveur de Cisco Secure ACS

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.

Support WPA et WPA2

Le réseau sans fil unifié Cisco inclut le soutien des certifications WPA et WPA2 de Wi-Fi Alliance. Le WPA a été introduit par le Wi-Fi Alliance en 2003. Le WPA2 a été introduit par le Wi-Fi Alliance en 2004. Tout le WiFi de Produits certifié pour le WPA2 sont exigés pour être interopérable avec les Produits qui sont WiFi certifié pour le WPA.

Le WPA et le WPA2 offrent un haut niveau d'assurance pour des utilisateurs finaux et des administrateurs réseau que leurs données demeureront privées et que l'accès à leurs réseaux sera limité aux utilisateurs autorisés. Chacun des deux ont des modes de fonctionnement personnels et d'entreprise qui répondent aux besoins distincts des deux segments de marché. La mode entreprise de chacune utilise le 802.1X et l'EAP d'IEEE pour l'authentification. Le mode personnel de chacun utilise la clé pré-partagée (PSK) pour l'authentification. Cisco ne recommande pas le mode personnel pour des déploiements d'affaires ou de gouvernement parce qu'il utilise un PSK pour l'authentification de l'utilisateur. PSK n'est pas sécurisé pour des environnements d'entreprise.

Le WPA adresse toutes les vulnérabilités connues WEP dans la mise en œuvre d'un système de sécurité d'origine d'IEEE 802.11 apportant une solution de sécurité immédiate aux WLAN dans l'entreprise et les petits environnements de bureau/bureau à domicile (SOHO). Le WPA utilise le TKIP pour le cryptage.

Le WPA2 est la nouvelle génération de sécurité wifi. C'est l'implémentation interopérable d'Alliance de WiFi de la norme ratifiée d'IEEE 802.11i. Il implémente l'algorithme de chiffrement recommandé du National Institute of Standards and Technology (NIST) AES utilisant le contre-mode avec le Cipher Block Chaining Message Authentication Code Protocol (CCMP). Le WPA2 facilite la conformité PAP 140-2 de gouvernement.

Comparaison des types du mode WPA et WPA2

	WPA	WPA2

Mode entreprise (entreprise, gouvernement, formation)	• Authentification : IEEE 802.1X/EAP • Cryptage : TKIP/MIC	• Authentification : IEEE 802.1X/EAP • Cryptage : AES-CCMP
Mode personnel (SOHO, maison/personnel)	• Authentification : PSK • Cryptage : TKIP/MIC	• Authentification : PSK • Cryptage : AES-CCMP

Dans le mode de fonctionnement WPA et WPA2 d'entreprise utilisez 802.1X/EAP pour l'authentification. le 802.1X fournit à des WLAN fort, à l'authentification mutuelle entre un client et un serveur d'authentification. En outre, le 802.1X fournit le par-utilisateur dynamique, des clés de chiffrement de par-session, retirant la charge administrative et les problèmes de sécurité entourant les clés de chiffrement statiques.

Avec le 802.1X, les qualifications utilisées pour l'authentification, telle que des mots de passe de connexion, ne sont en clair jamais transmises, ou sans cryptage, au-dessus du support Sans fil. Tandis que les types d'authentification de 802.1X fournissent l'authentification poussée pour des réseaux locaux Sans fil, le TKIP ou les AES sont nécessaires pour le cryptage en plus du 802.1X depuis le cryptage WEP standard de 802.11, est vulnérable aux attaques réseau.

Plusieurs types d'authentification de 802.1X existent, chacun qui fournit une approche différente à l'authentification tout en comptant sur le mêmes cadre et EAP pour la transmission entre un client et un Point d'accès. Les Produits de Cisco Aironet prennent en charge plus de types d'authentification EAP de 802.1X que tous les autres Produits WLAN. Les types pris en charge incluent :

- Cisco SAUTENT
- EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
- EAP-Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol (PEAP)
- EAP-Tunneled TLS (EAP-TTLS)
- Module d'identité d'Eap-abonné (EAP-SIM)

Un autre avantage de l'authentification de 802.1X est Gestion centralisée pour des groupes d'utilisateurs WLAN, y compris la rotation principale basée sur la politique, le transfert principal dynamique, l'affectation dynamique VLAN, et la restriction SSID. Ces caractéristiques tournent les clés de chiffrement.

Dans le mode de fonctionnement personnel, une clé pré-partagée (mot de passe) est utilisée pour l'authentification. Le mode personnel exige un périphérique seulement de Point d'accès et de client, alors que la mode entreprise exige typiquement un RAYON ou tout autre serveur d'authentification sur le réseau.

Ce document fournit des exemples pour configurer WPA2 (mode entreprise) et WPA2-PSK (mode personnel) dans un réseau de Cisco Unified Wireless.

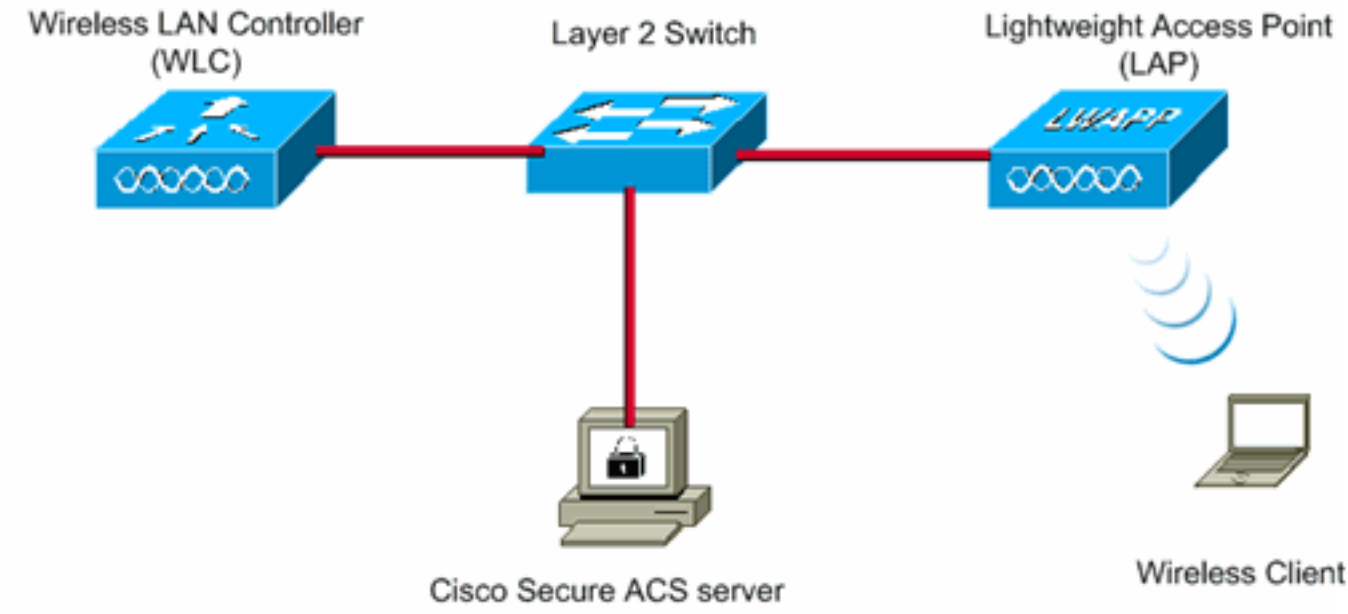
Configuration du réseau

Dans cette installation, un Cisco 4404 WLC et un RECOUVREMENT de gamme Cisco 1000 sont connectés par un commutateur de la 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 (RECOUVREMENT) est au commencement enregistré au contrôleur. Deux réseaux locaux Sans fil, un pour le mode de WPA2 Enterprise et l'autre pour le mode WPA2 personnel, doivent être créés.

Mode WLAN (SSID de WPA2 Enterprise : Le WPA2 Enterprise) utilisera l'EAP-FAST pour authentifier les clients sans fil et l'AES pour le cryptage. Le serveur de Cisco Secure ACS sera utilisé en tant que serveur RADIUS externe pour authentifier les clients sans fil.

Mode WLAN (SSID WPA2-Personal : WPA2-PSK) utilisera WPA2-PSK pour l'authentification avec le « abcdefghijk » principal pré-partagé.

Vous devez configurer les périphériques pour cette installation :



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

Configurez les périphériques pour le mode de WPA2 Enterprise

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

Exécutez ces étapes afin de configurer les périphériques pour le mode de fonctionnement de WPA2 Enterprise :

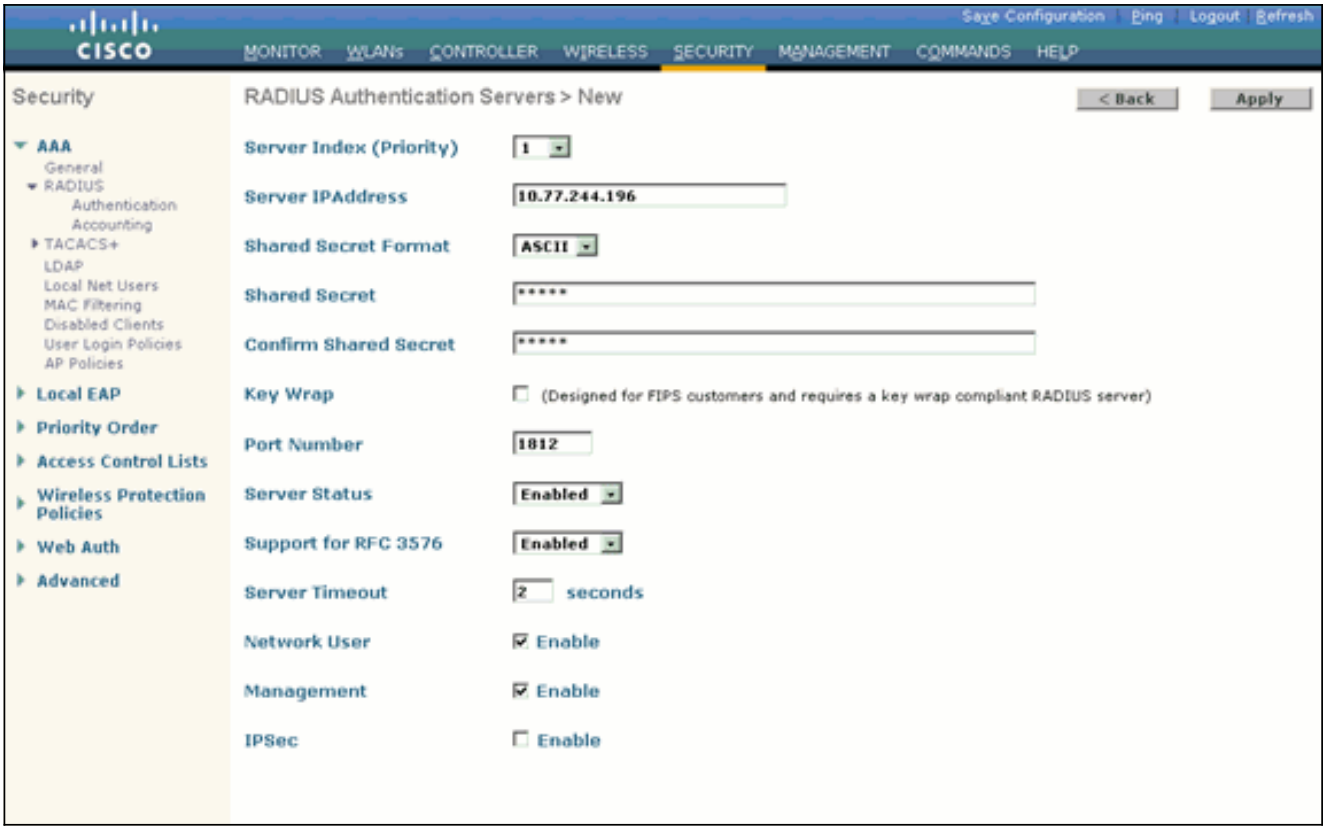
1. Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe
2. Configurez le WLAN pour l'authentification de mode de WPA2 Enterprise (l'EAP-FAST)
3. Configurez le client sans fil pour le mode de WPA2 Enterprise

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 alors valide les identifiants utilisateurs utilisant l'EAP-FAST et permet d'accéder 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. Puis, cliquez sur New afin de définir un serveur de RAYON.
2. Définissez les paramètres de serveur de RAYON sur le **RADIUS Authentication Servers > New page**. Ces paramètres incluent :Adresse IP du serveur RADIUSSecret partagéNuméro de portÉtat de serveurCe document utilise le serveur ACS avec une adresse IP de 10.77.244.196.



3. Cliquez sur **Apply**.

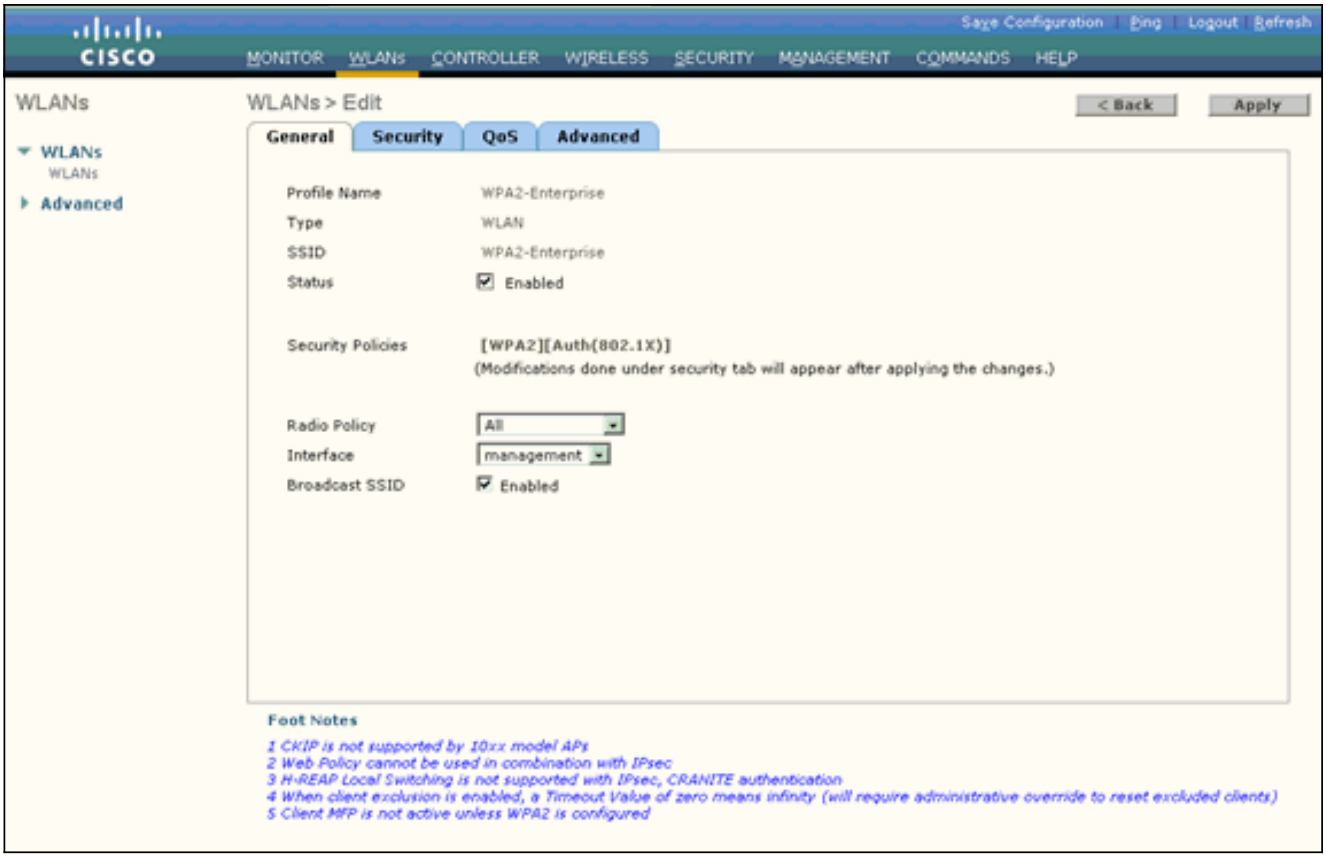
Configurez le WLAN pour le mode de fonctionnement de WPA2 Enterprise

Ensuite, configurez le WLAN que les clients les utiliseront pour connecter au réseau Sans fil. Le WLAN SSID pour la mode entreprise WPA2 sera WPA2 Enterprise. Cet exemple assigne ce WLAN à l'interface de gestion.

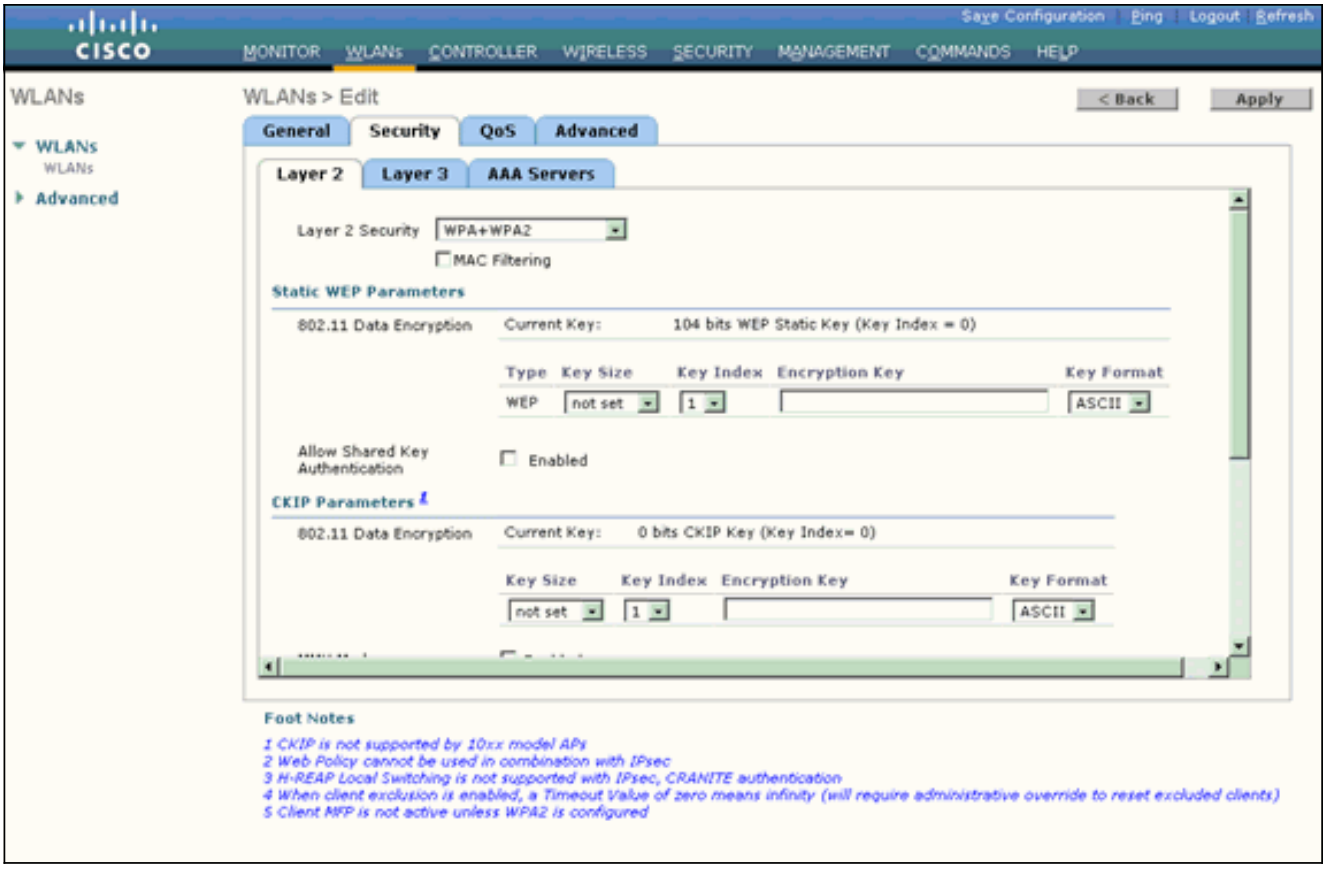
Terminez-vous ces étapes afin de configurer le WLAN et ses paramètres relatifs :

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

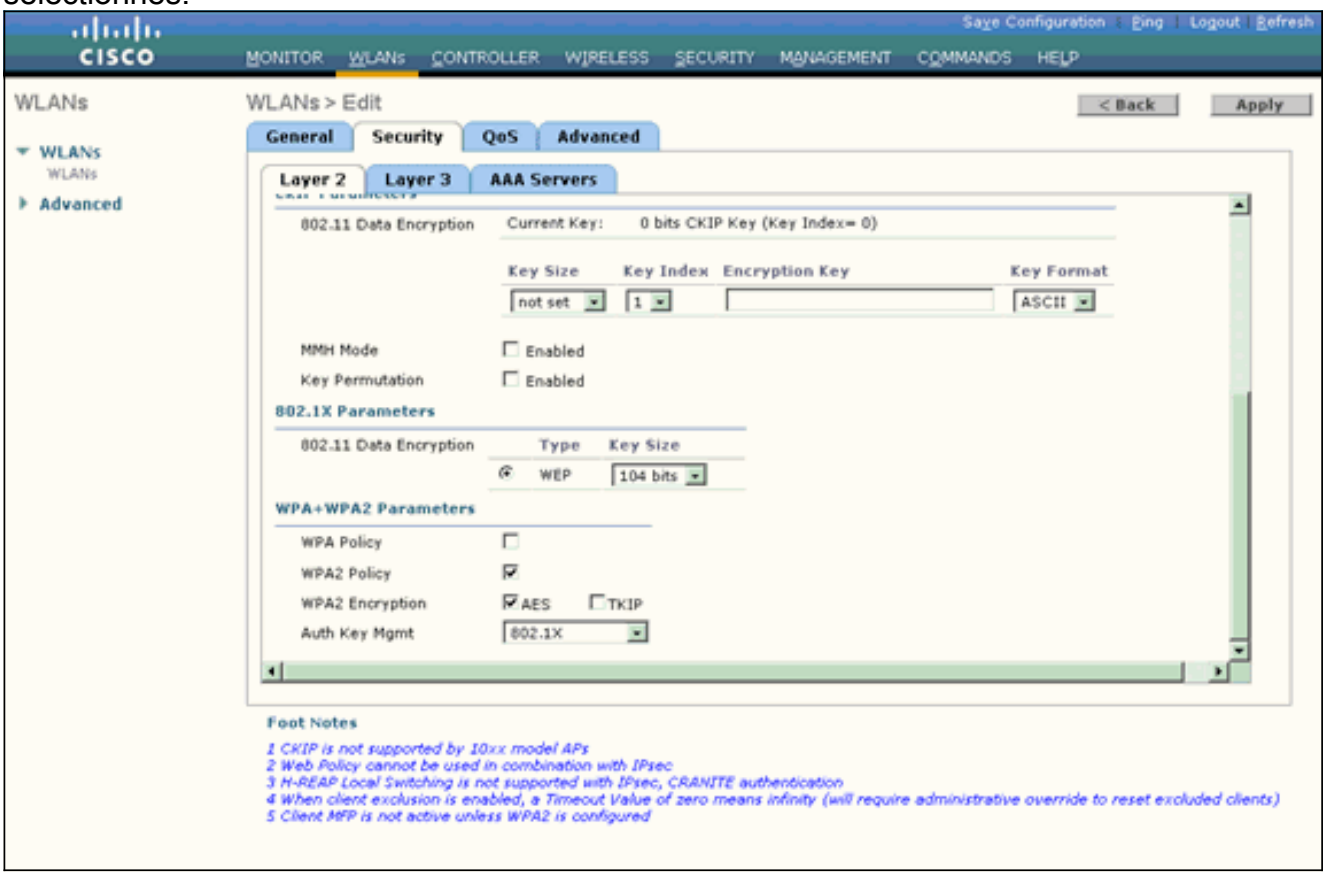
4. Une fois que vous avez créé un nouveau WLAN, la page **WLAN > Edit** du nouveau WLAN apparaît. À cette page, vous pouvez définir de divers paramètres spécifiques à ce WLAN. Ceci inclut des stratégies générales, des stratégies de sécurité, des stratégies QoS et des paramètres avancés.
5. Dans le cadre des stratégies générales, cochez la case d'**état** afin d'activer le WLAN.



6. Si vous voulez qu'AP annonce le SSID dans des ses trames balise, cochez la case de **Broadcast SSID**.
7. Cliquez sur l'onglet **Security**. Sous le degré de sécurité de la couche 2, choisissez **WPA+WPA2**.Ceci active l'authentification WPA pour le WLAN.

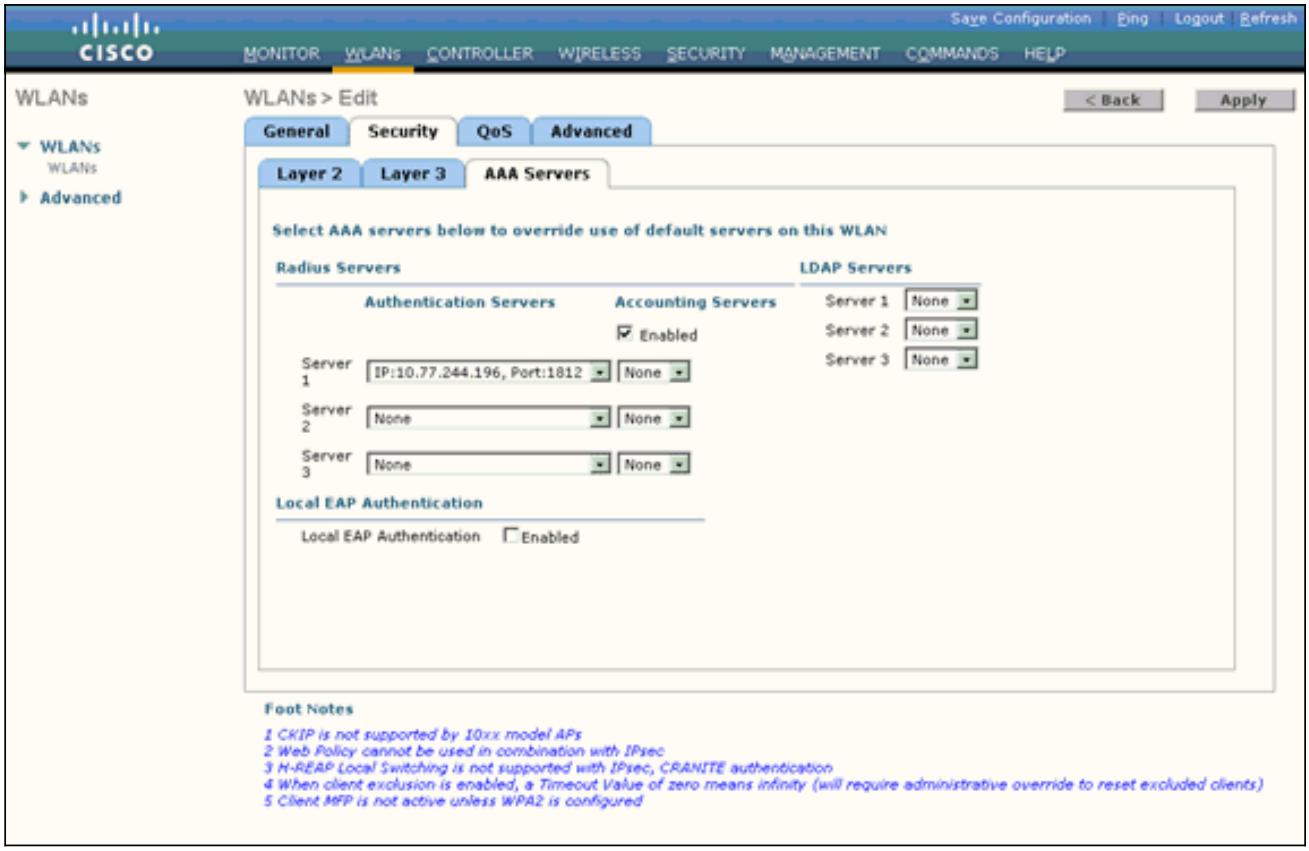


8. Faites descendre l'écran la page pour modifier les **paramètres WPA+WPA2**.Dans cet exemple, la stratégie WPA2 et le cryptage AES sont sélectionnés.



9. Sous la clé authentique gestion, choisissez le **802.1x**.Ceci active le WPA2 utilisant l'authentification 802.1x/EAP et le cryptage AES pour le WLAN.
10. Cliquez sur l'**onglet AAA Servers**. Sous des serveurs d'authentification, choisissez l'adresse IP du serveur appropriée.Dans cet exemple, 10.77.244.196 est utilisé en tant que serveur

de
RAYON.



11. Cliquez sur **Apply**.**Remarque:** C'est la seule configuration d'EAP qui doit être configurée sur le contrôleur pour l'authentification EAP. Toutes autres configurations spécifiques à l'EAP-FAST doivent être faites sur le serveur de RAYON et les clients qui doivent être authentifiées.

Configurez le serveur de RAYON pour l'authentification de mode de WPA2 Enterprise (l'EAP-FAST)

Dans cet exemple, le Cisco Secure ACS est utilisé en tant que serveur RADIUS externe. Exécutez ces étapes afin de configurer le serveur de RAYON pour l'authentification d'EAP-FAST :

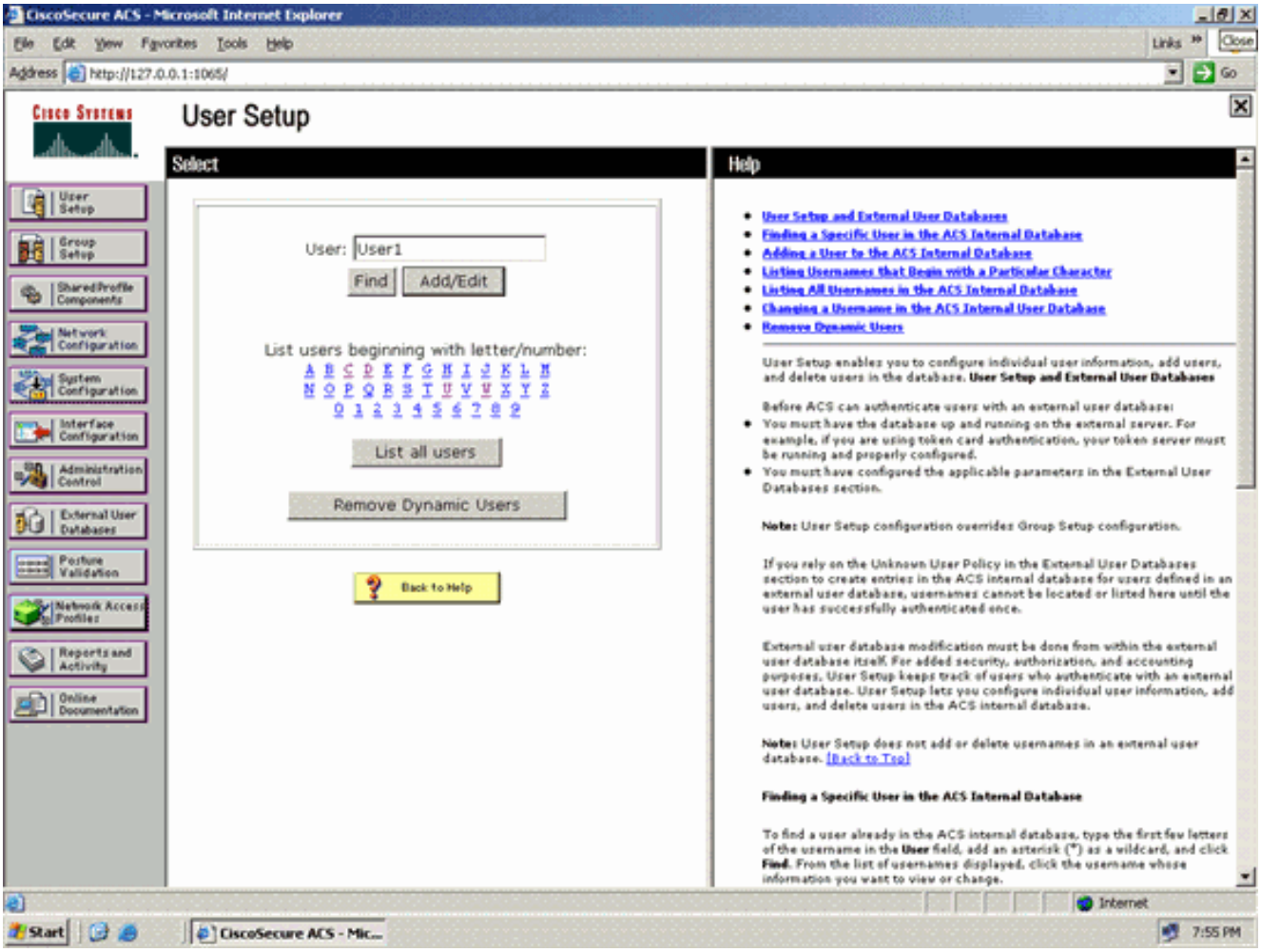
1. Créez une base de données utilisateur pour authentifier des clients
2. Ajoutez le WLC comme client d'AAA au serveur de RAYON
3. Configurez l'authentification d'EAP-FAST sur le serveur de RAYON avec le ravitaillement anonyme PAC d'intrabande**Remarque:** L'EAP-FAST peut être configuré avec le ravitaillement anonyme PAC d'intrabande ou le ravitaillement authentifié PAC d'intrabande. Cet exemple utilise le ravitaillement anonyme PAC d'intrabande. Pour les informations détaillées et des exemples sur 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.

Créez une base de données utilisateur pour authentifier des clients d'EAP-FAST

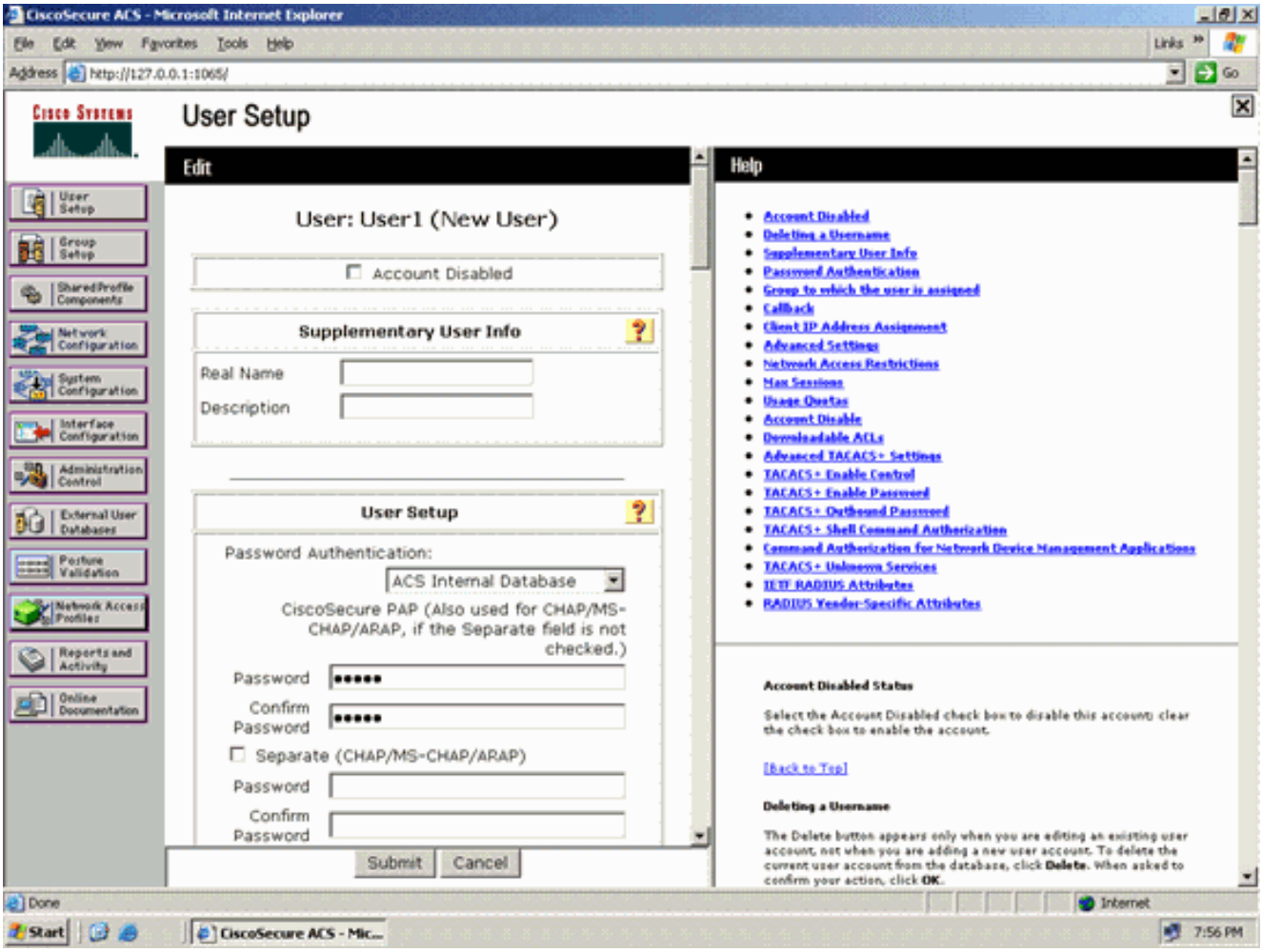
Terminez-vous ces étapes afin de créer une base de données utilisateur pour des clients d'EAP-FAST sur l'ACS. Cet exemple configure le nom d'utilisateur et mot de passe du client d'EAP-FAST

comme User1 et User1, respectivement.

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



2. 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.

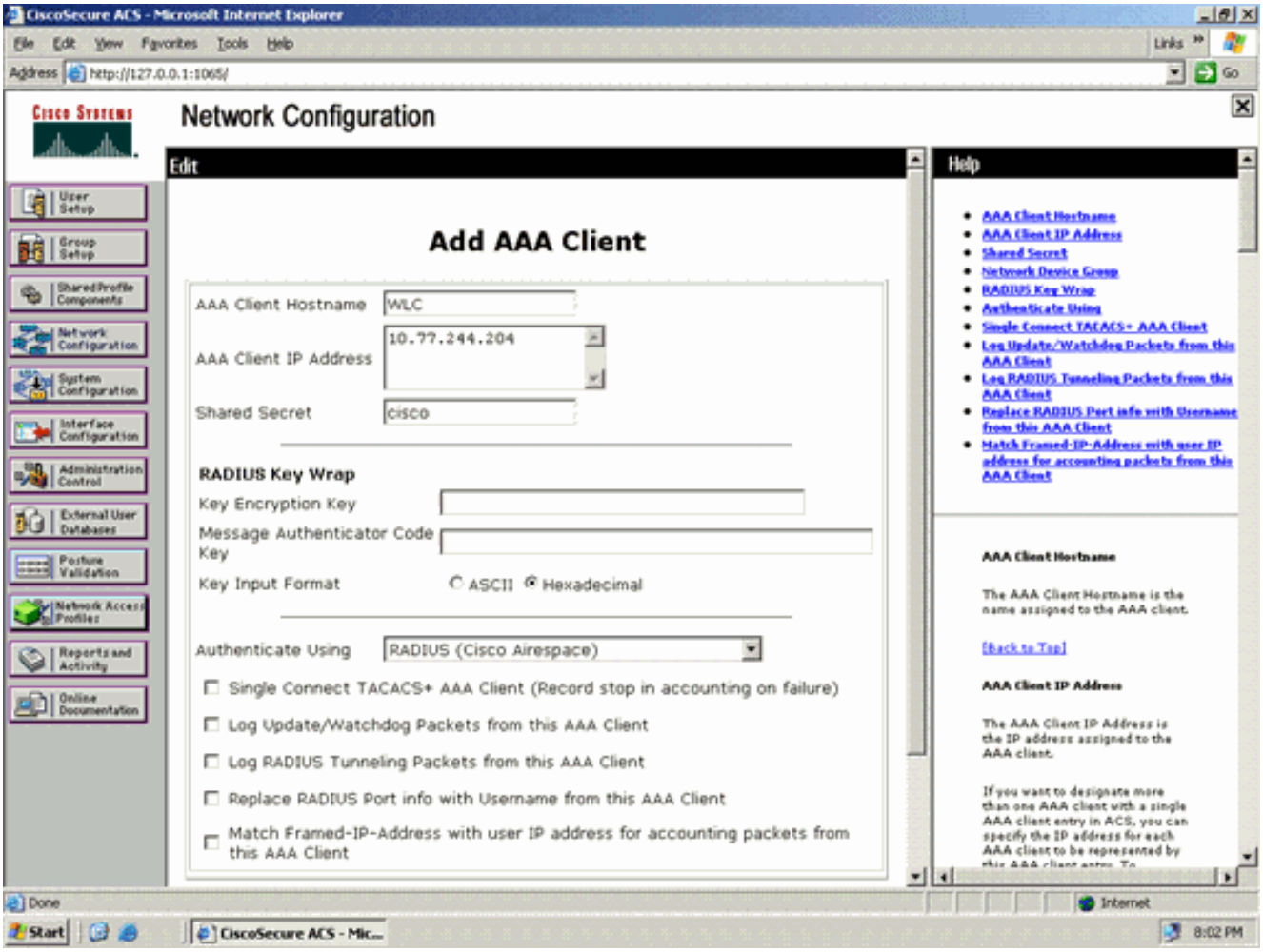


3. Choisissez les **ACS Internal Database de la** liste déroulante d'authentification de mot de passe.
4. Configurez tous les autres paramètres requis et cliquez sur Submit.

Ajoutez le WLC comme client d'AAA au serveur de RAYON

Terminez-vous ces étapes afin de définir le contrôleur en tant que client d'AAA sur le serveur ACS :

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



Remarque: les clés secrètes partagées que vous configurez sur le WLC et le serveur ACS doivent correspondre. Le secret partagé distingue les majuscules et minuscules.

3. Clic **Submit+Apply**.

Configurez l'authentification d'EAP-FAST sur le serveur de RAYON avec le ravitaillement anonyme PAC d'intrabande

Ravitaillement anonyme d'intrabande

C'est l'une des deux méthodes de ravitaillement d'intrabande dans lesquelles l'ACS établit une connexion sécurisée avec le client d'utilisateur afin de fournir au client un nouveau PAC. Cette option permet une prise de contact anonyme de TLS entre le client d'utilisateur et l'ACS.

Cette méthode actionne l'intérieur un tunnel authentifié de Protocol d'accord de Diffie-HellmanKey (ADHP) avant que le pair authentifie le serveur ACS.

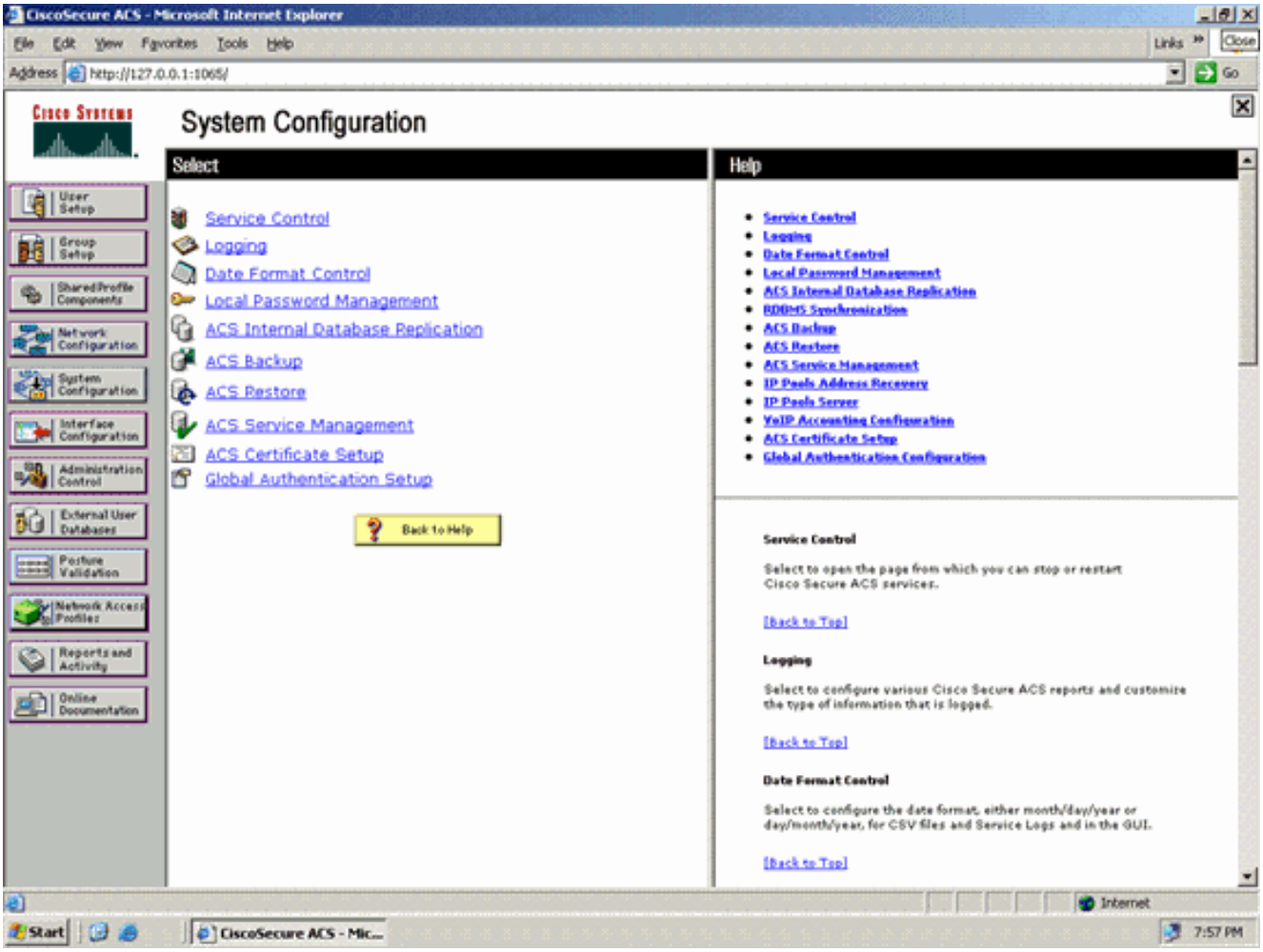
Puis, l'ACS exige l'authentification EAP-MS-CHAPv2 de l'utilisateur. À l'authentification de l'utilisateur réussie, l'ACS établit un tunnel de Diffie-Hellman avec le client d'utilisateur. L'ACS génère un PAC pour l'utilisateur et l'envoie au client d'utilisateur dans ce tunnel, avec des informations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

Puisqu'un serveur unauthenticated provisioned, il n'est pas possible d'utiliser un mot de passe de texte brut. Par conséquent, seulement des qualifications MS-CHAP peuvent être utilisées à l'intérieur du tunnel. MS-CHAPv2 est utilisé pour prouver l'identité du pair et pour recevoir un PAC pour d'autres sessions d'authentification (EAP-MS-CHAP sera utilisé en tant que méthode

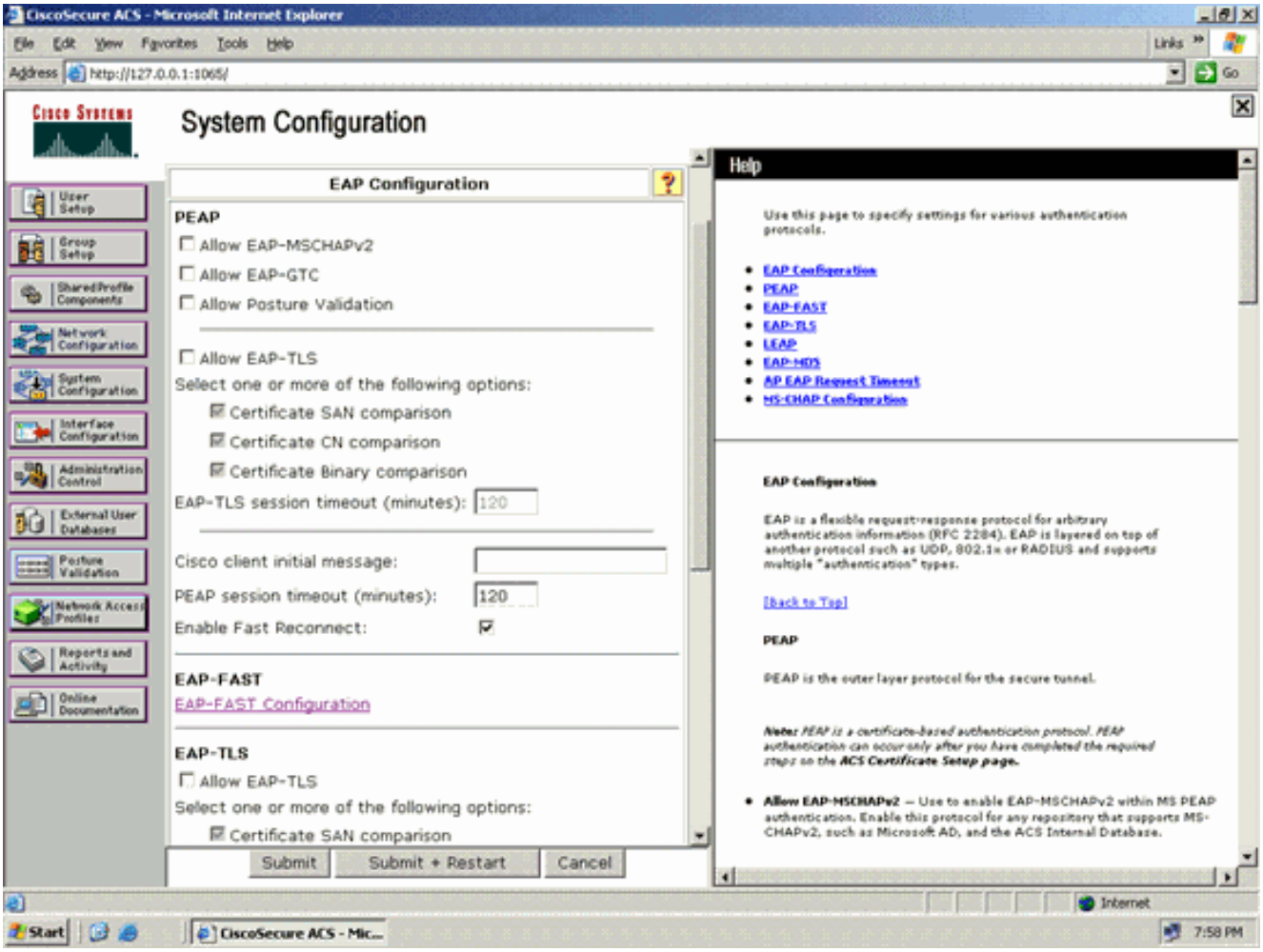
intérieure seulement).

Terminez-vous ces étapes afin de configurer l'authentification d'EAP-FAST dans le serveur de RAYON pour le ravitaillement anonyme d'intrabande :

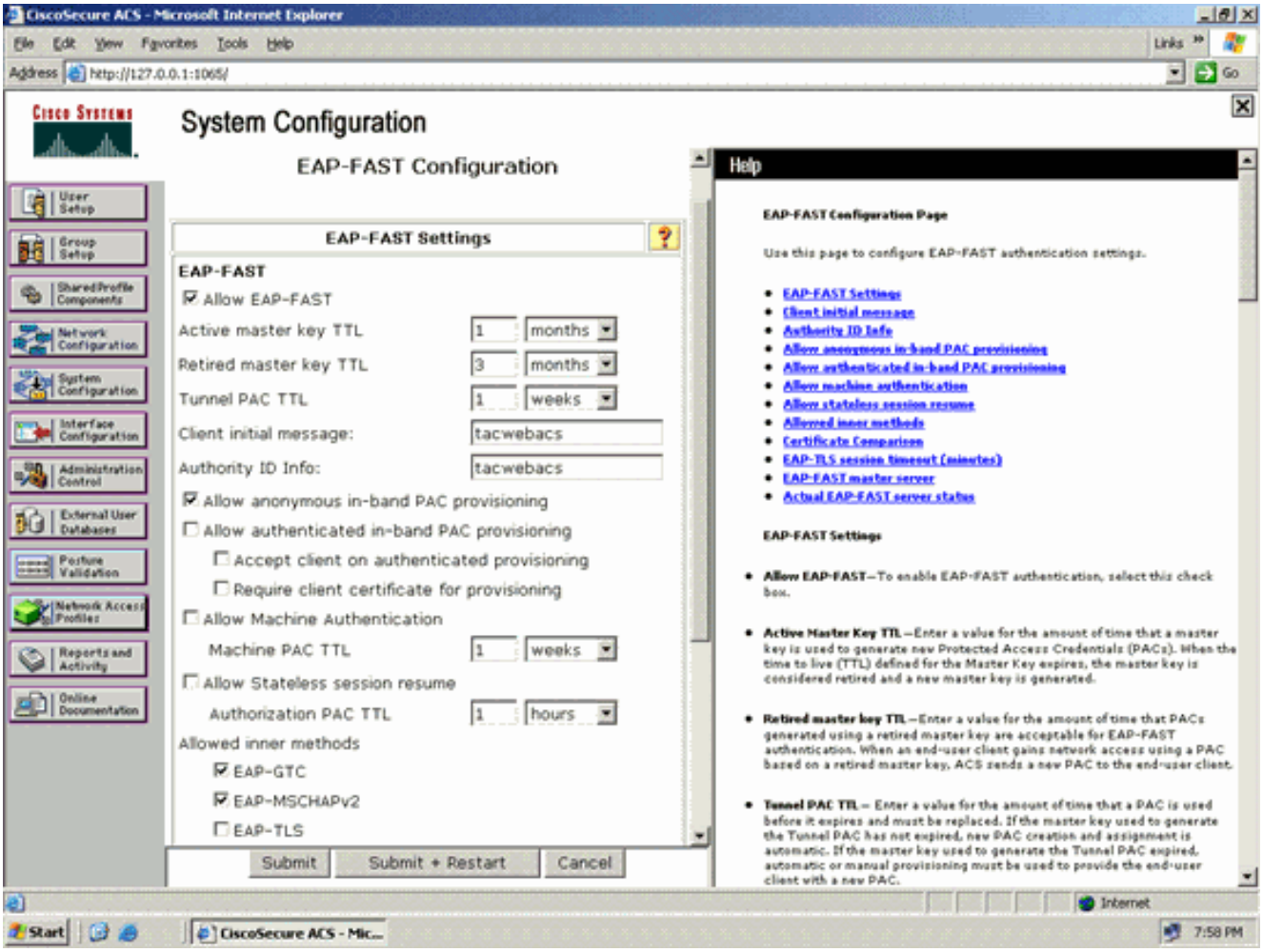
1. **Configuration système de** clic du GUI de serveur de RAYON. De la page de configuration système, choisissez l'**installation globale d'authentification**.



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** pour activer l'EAP-FAST dans le serveur de
RAYON.



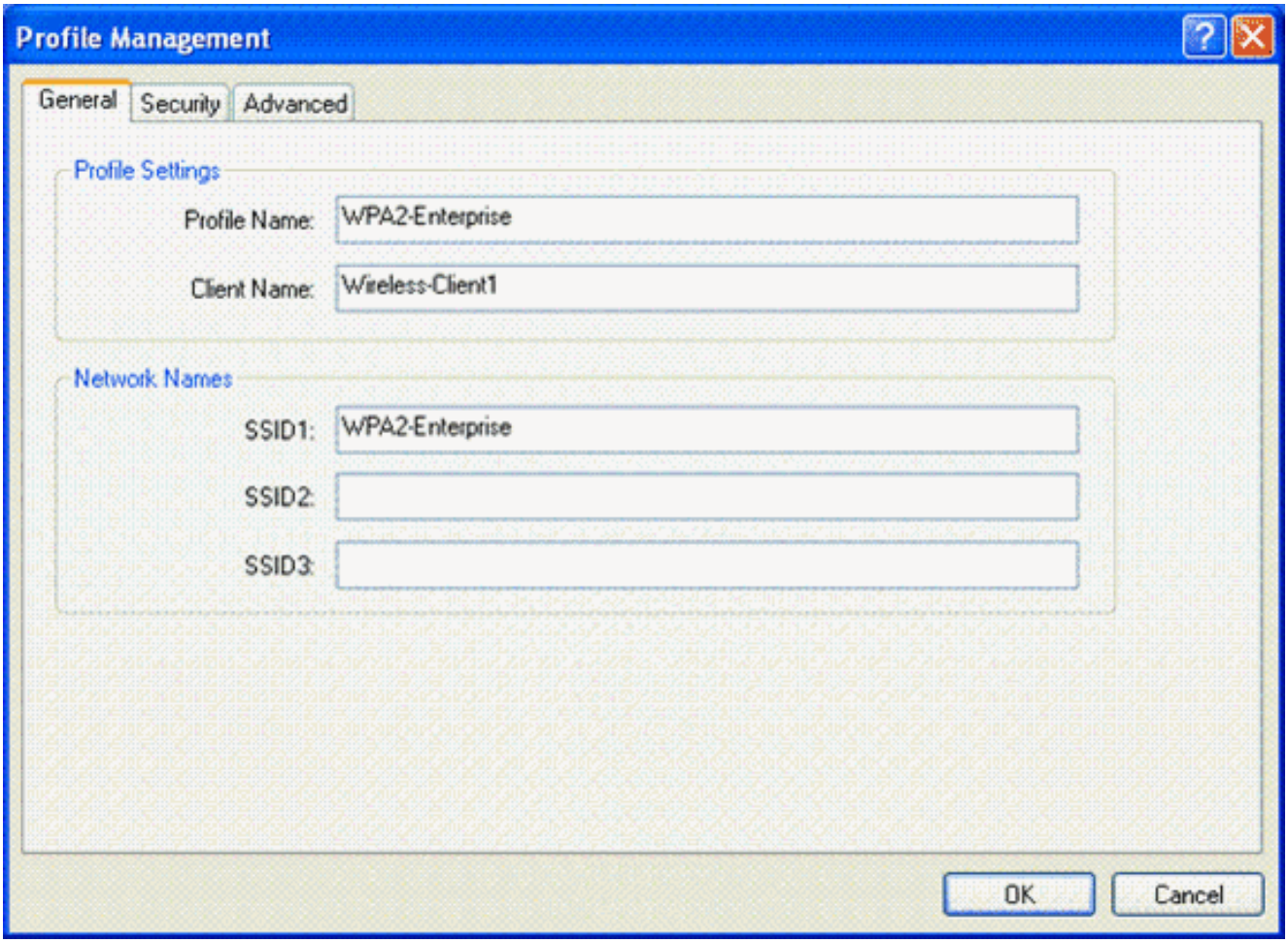
4. Configurez l'Active/valeurs retirées de la clé principale TTL (Time to Live) comme désirées, ou placez-les à la valeur par défaut suivant les indications de cet exemple.Référez-vous aux clés principales pour des informations sur l'Active et les clés principales retirées. En outre, référez-vous aux clés principales et au pour en savoir plus PAC TTL.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. **Méthodes intérieures permises** — Cette option 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).

Configurez le client sans fil pour le mode de fonctionnement de WPA2 Enterprise

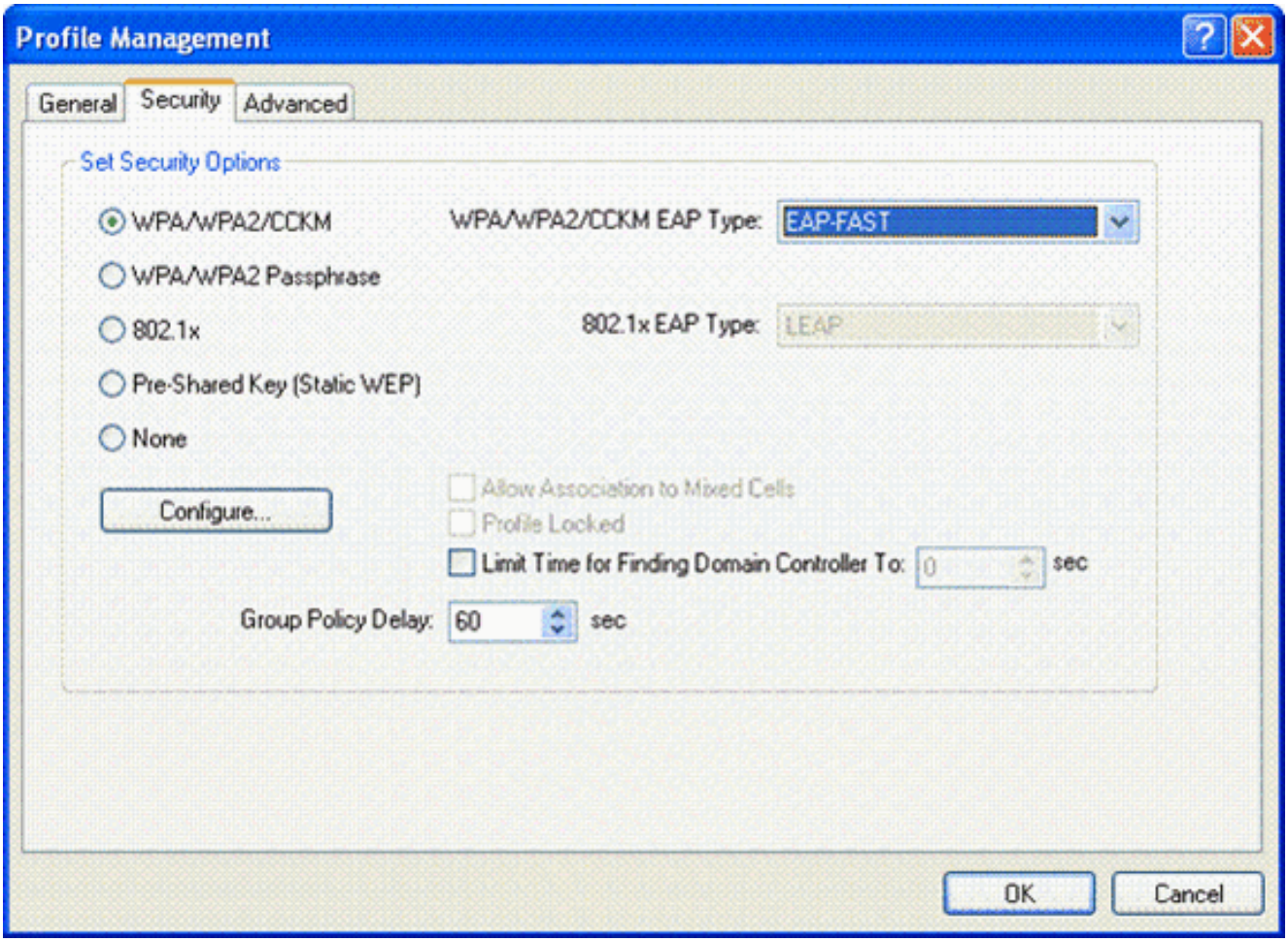
L'étape suivante est de configurer le client sans fil pour le mode de fonctionnement de WPA2 Enterprise.

Terminez-vous ces étapes afin de configurer le client sans fil pour le mode de WPA2 Enterprise.

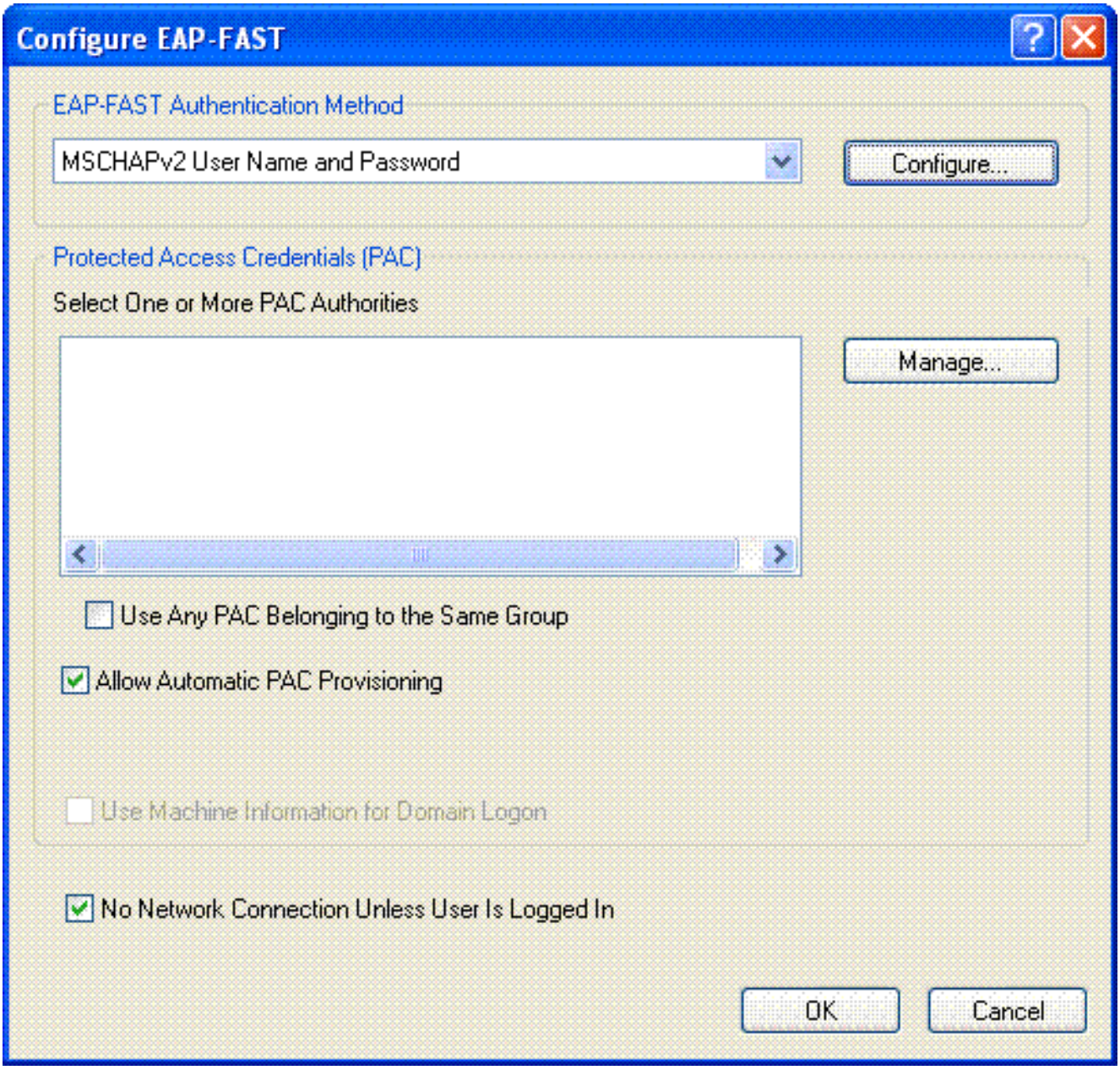
1. De la fenêtre d'Aironet Desktop Utility, **Profile Management > New de** clic afin de créer un profil pour l'utilisateur du WPA2 Enterprise WLAN.Comme cité précédemment, ce document utilise le nom WLAN/SSID comme **WPA2 Enterprise** pour le client sans fil.
2. De la fenêtre Profile Management, cliquez sur l'**onglet Général** et configurez le nom de profil, le nom de client et le nom SSID suivant les indications de cet exemple. Puis, cliquez sur OK



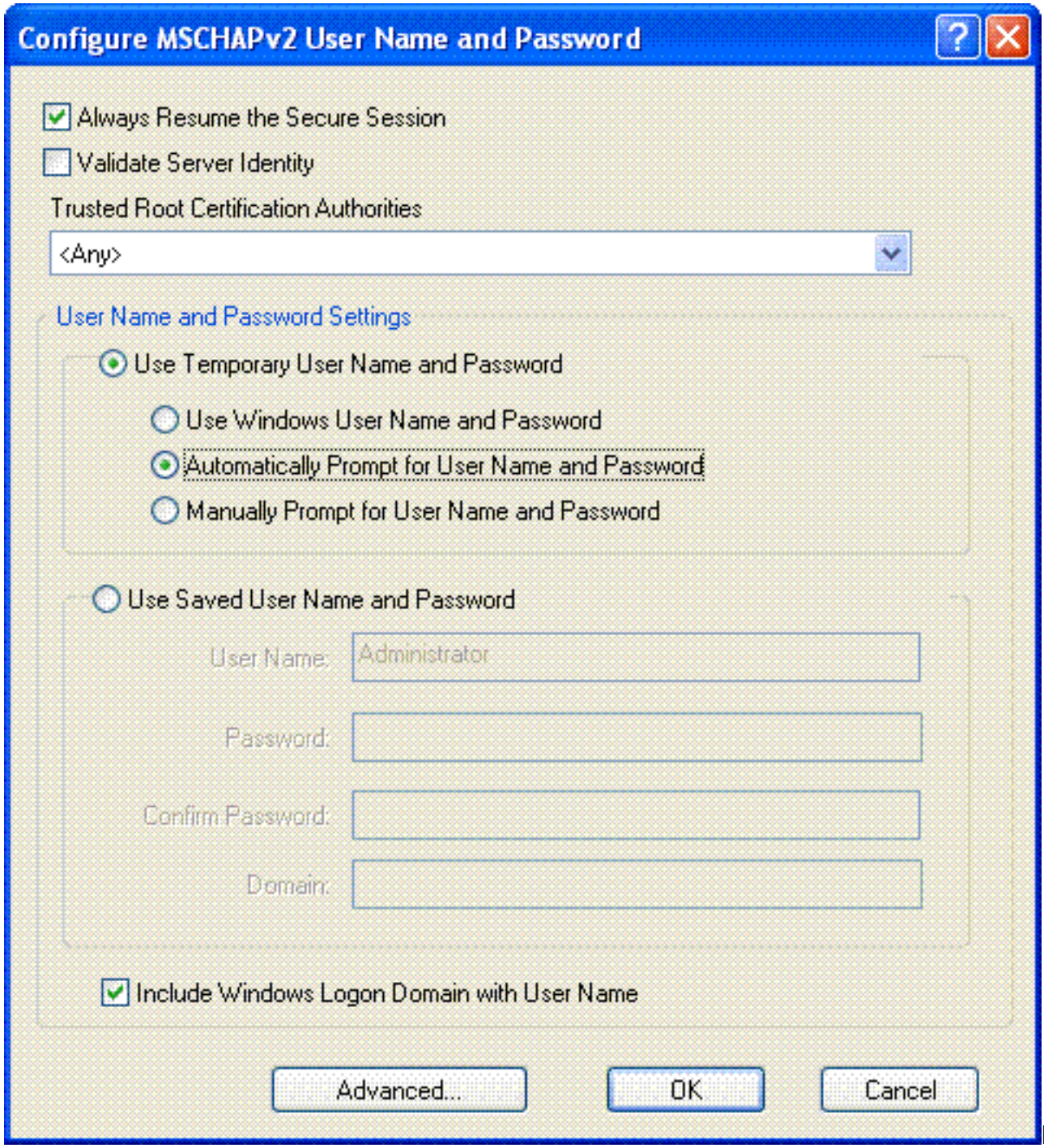
3. Cliquez sur l'**onglet Sécurité** et choisissez **WPA/WPA2/CCKM** pour activer le mode de fonctionnement WPA2. Sous le type d'EAP WPA/WPA2/CCKM, choisissez l'**EAP-FAST**. Cliquez sur Configure afin de configurer la configuration d'EAP-FAST.



4. De la fenêtre d'EAP-FAST de configurer, cochez la case **automatique de ravitaillement PAC d'autoriser**. Si vous voulez configurer le ravitaillement anonyme PAC, EAP-MS-CHAP sera utilisé comme seule méthode intérieure dans la phase
zéro.



5. Choisissez le nom d'utilisateur MSCHAPv2 et le mot de passe comme méthode d'authentification de la liste déroulante de méthode d'authentification d'EAP-FAST. Cliquez sur **Configure**.
6. De la fenêtre de nom d'utilisateur et de mot de passe du configurer MSCHAPv2, choisissez les configurations appropriées de nom d'utilisateur et mot de passe.Cet exemple choisit **automatiquement la demande pour le nom d'utilisateur et le mot de passe**.



Le même nom d'utilisateur et mot de passe devrait être enregistré à l'ACS. Comme cité précédemment, cet exemple utilise User1 et User1 respectivement comme nom d'utilisateur et mot de passe. En outre, notez que c'est un ravitaillement anonyme d'intrabande. Par conséquent, le client ne peut pas valider le certificat de serveur. Vous devez s'assurer que la case d'identité de serveur de validation est décochée.

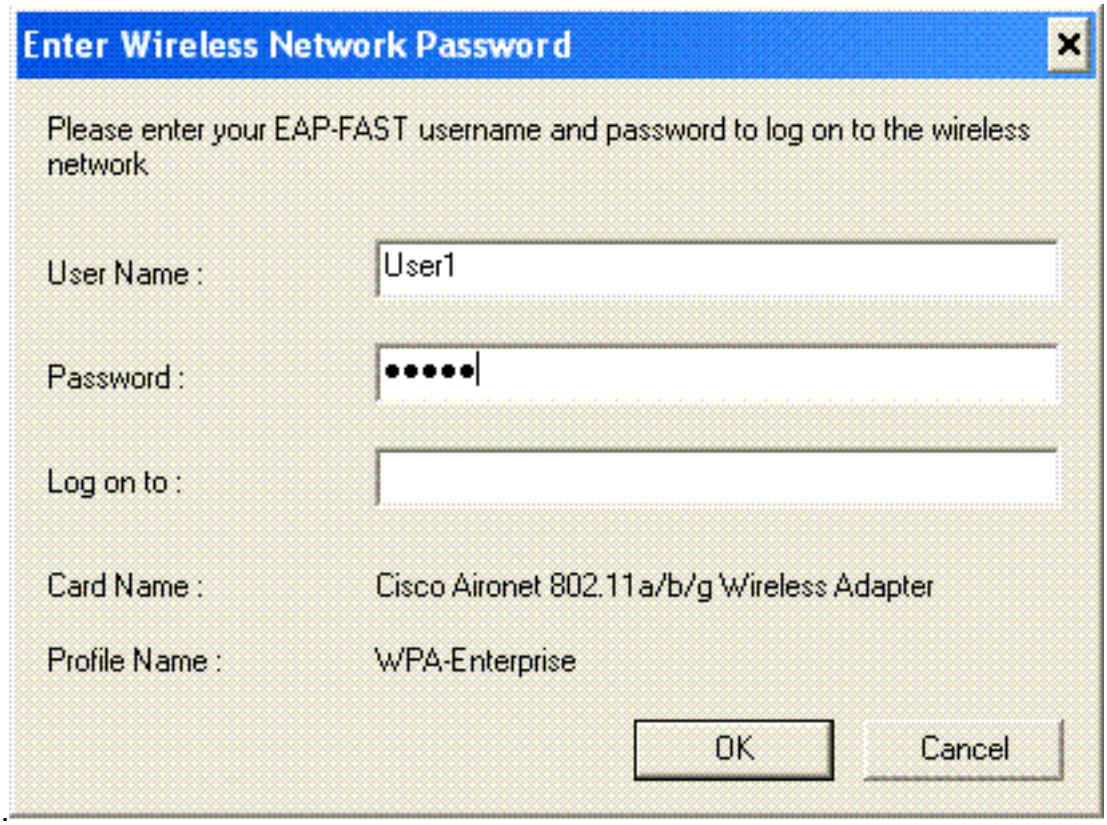
7. Cliquez sur **OK**.

Vérifiez le mode de fonctionnement de WPA2 Enterprise

Terminez-vous ces étapes afin de vérifier si votre configuration de mode de WPA2 Enterprise fonctionne correctement :

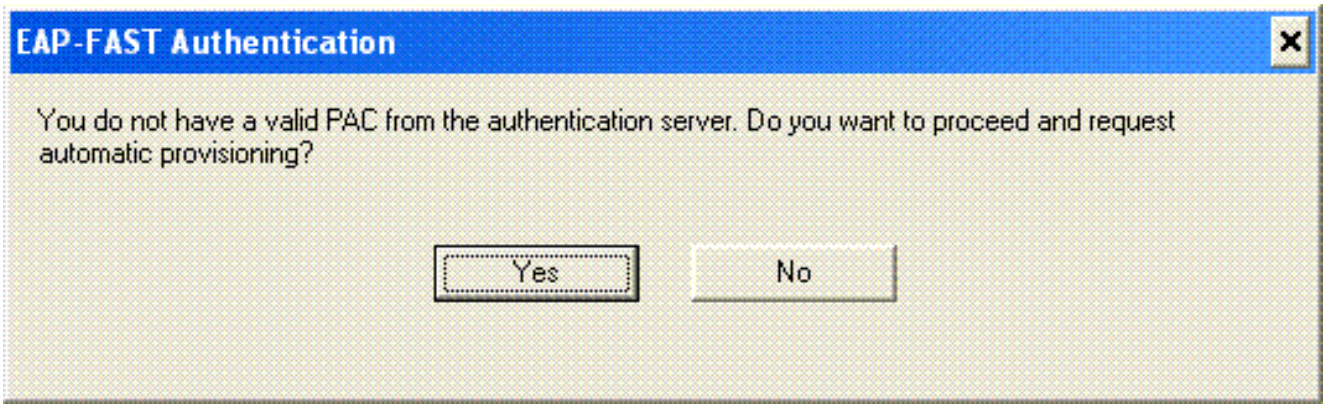
1. De la fenêtre d'Aironet Desktop Utility, sélectionnez le **WPA2 Enterprise de** profil et le clic **lancent** afin de lancer le profil de client sans fil.
2. Si vous avez activé MS-CHAP ver2 en tant que votre authentification, alors le client incitera

pour le nom d'utilisateur et mot de

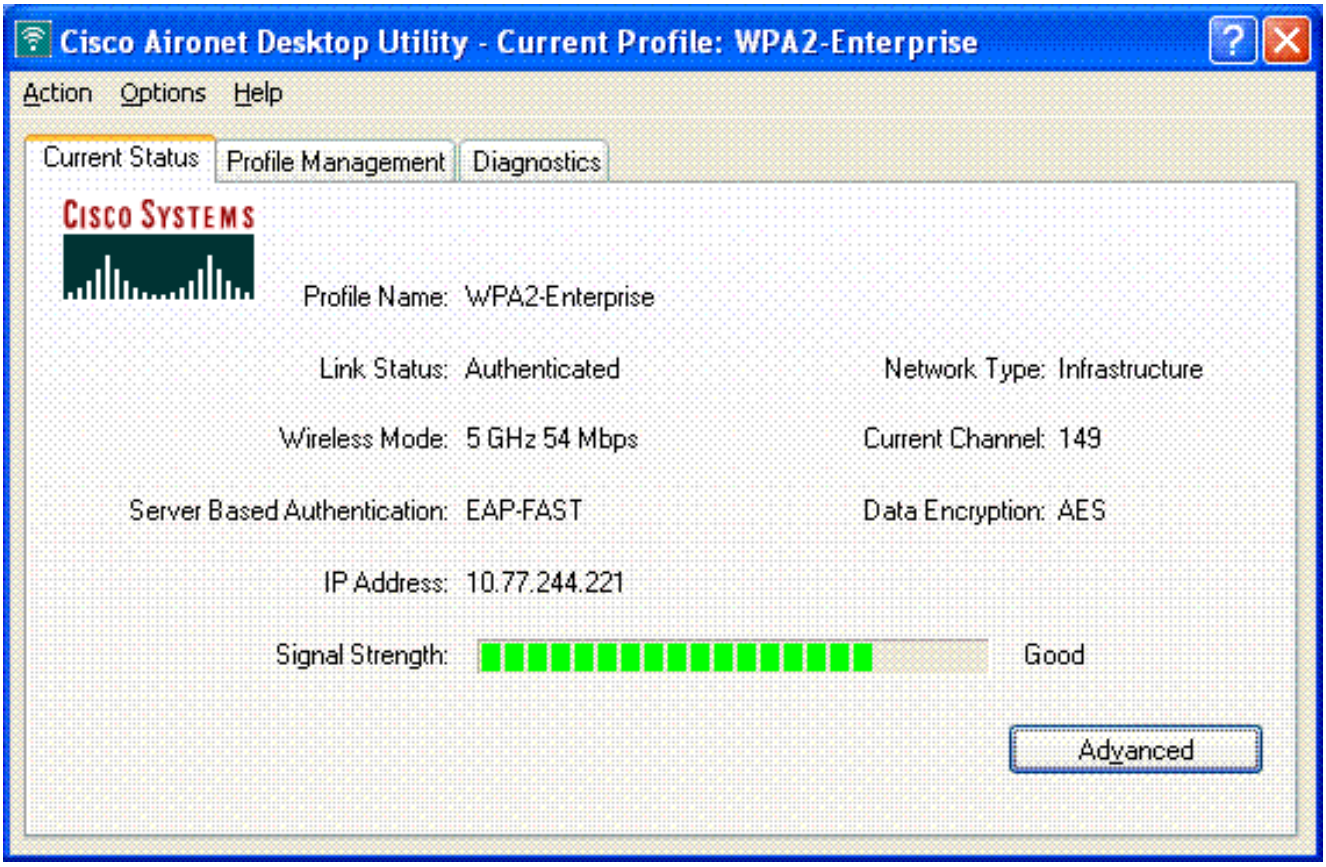


passe.

3. Pendant le traitement d'EAP-FAST de l'utilisateur, vous serez incité par le client à demander le PAC du serveur de RAYON. Quand vous cliquez sur **oui**, des débuts de ravitaillement PAC.



4. Après ravitaillement réussi PAC dans la phase zéro, la phase une et deux suivent et une procédure réussie d'authentification a lieu.Sur l'authentification réussie le client sans fil obtient associé au WPA2 Enterprise WLAN. Voici le tir d'écran
:



Vous pouvez également vérifier si le serveur de RAYON 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.

Configurez les périphériques pour le mode WPA2 personnel

Exécutez ces étapes afin de configurer les périphériques pour le mode de fonctionnement WPA2-Personal :

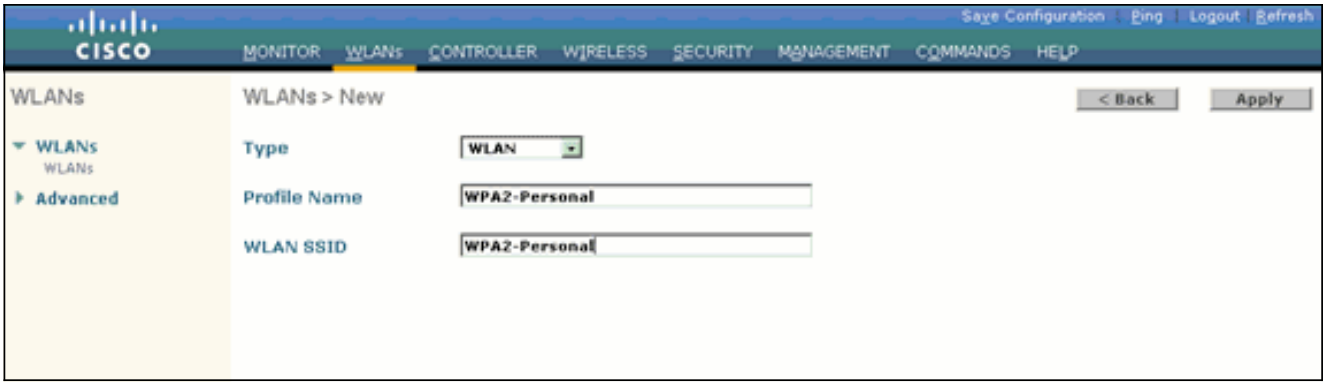
1. Configurez le WLAN pour l'authentification personnelle du mode WPA2
2. Configurez le client sans fil pour le mode WPA2 personnel

Configurez le WLAN pour le mode de fonctionnement WPA2 personnel

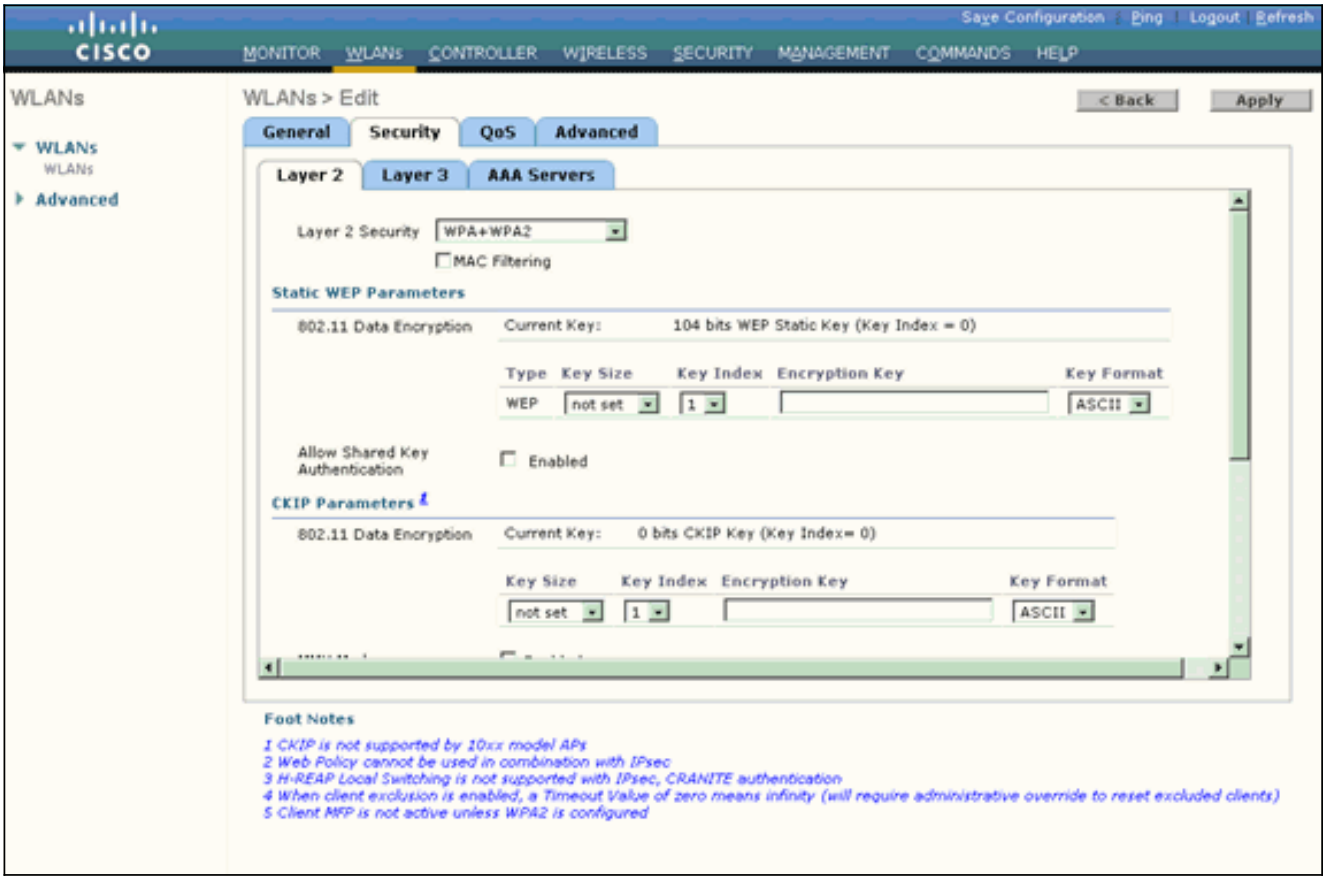
Vous devez configurer le WLAN que les clients les utiliseront pour connecter au réseau Sans fil. Le WLAN SSID pour le mode WPA2 personnel sera WPA2-Personal. Cet exemple assigne ce WLAN à l'interface de gestion.

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

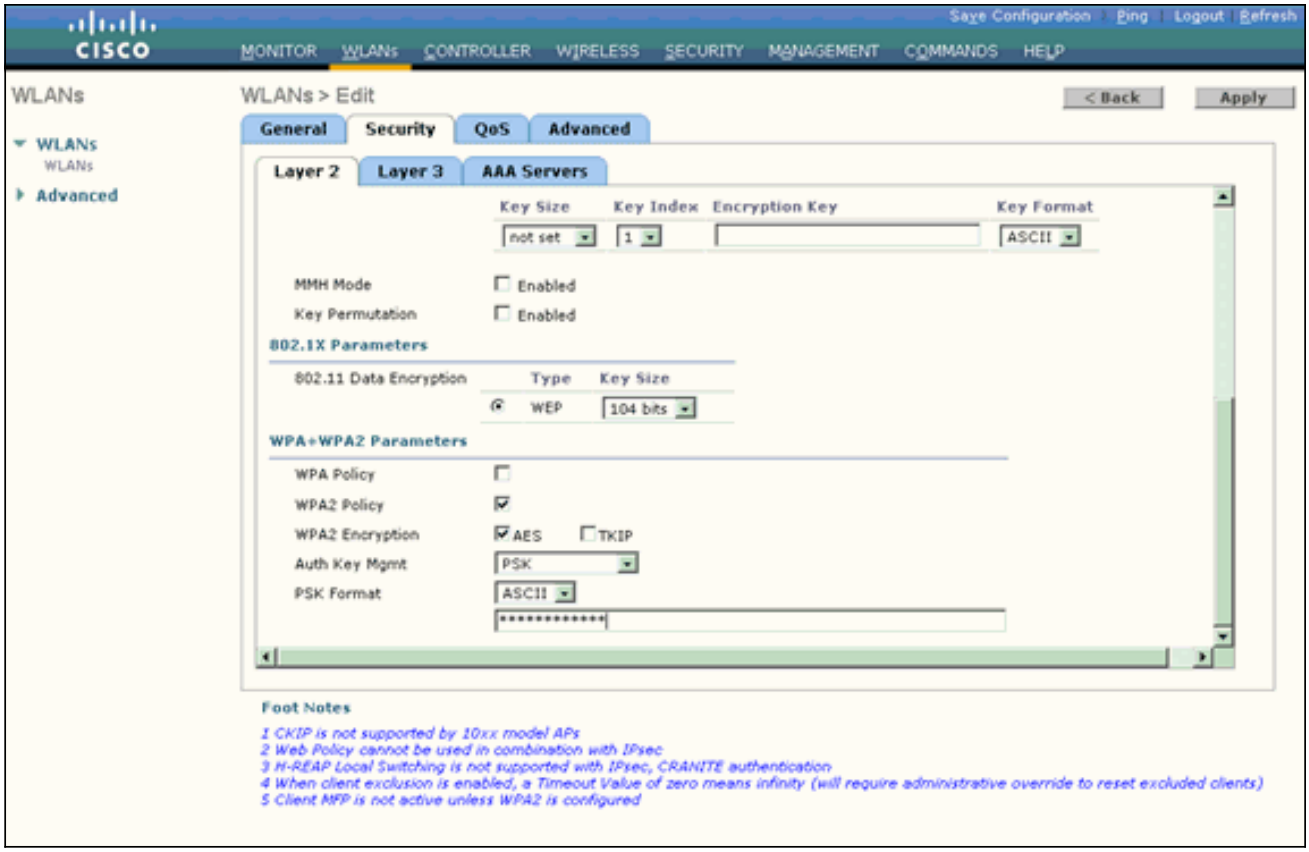
1. Cliquez sur les **WLAN** de la GUI du contrôleur afin d'afficher la page des WLAN.Cette page énumère les WLAN qui existent sur le contrôleur.
2. Cliquez sur New afin de créer un nouveau WLAN.
3. Écrivez le nom, le nom de profil et l'ID de WLAN WLAN SSID à la page de WLANs > New. Cliquez ensuite sur **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. 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.
5. Dans le cadre des stratégies générales, cochez la case d'**état** afin d'activer le WLAN.
6. Si vous voulez qu'AP annonce le SSID dans des ses trames balise, cochez la case de **Broadcast SSID**.
7. Cliquez sur l'onglet **Security**. Sous Layer Security, choisissez **WPA+WPA2**.Ceci active l'authentification WPA pour le WLAN.



8. Faites descendre l'écran la page pour modifier les **paramètres WPA+WPA2**.Dans cet exemple, la stratégie WPA2 et le cryptage AES sont sélectionnés.
9. Sous la clé authentique gestion, choisissez **PSK** afin d'activer WPA2-PSK.
10. Introduisez la clé pré-partagée dans le champ approprié comme affiché.



Remarque: La clé pré-partagée utilisée sur le WLC doit s'assortir avec celui configuré sur les clients sans fil.

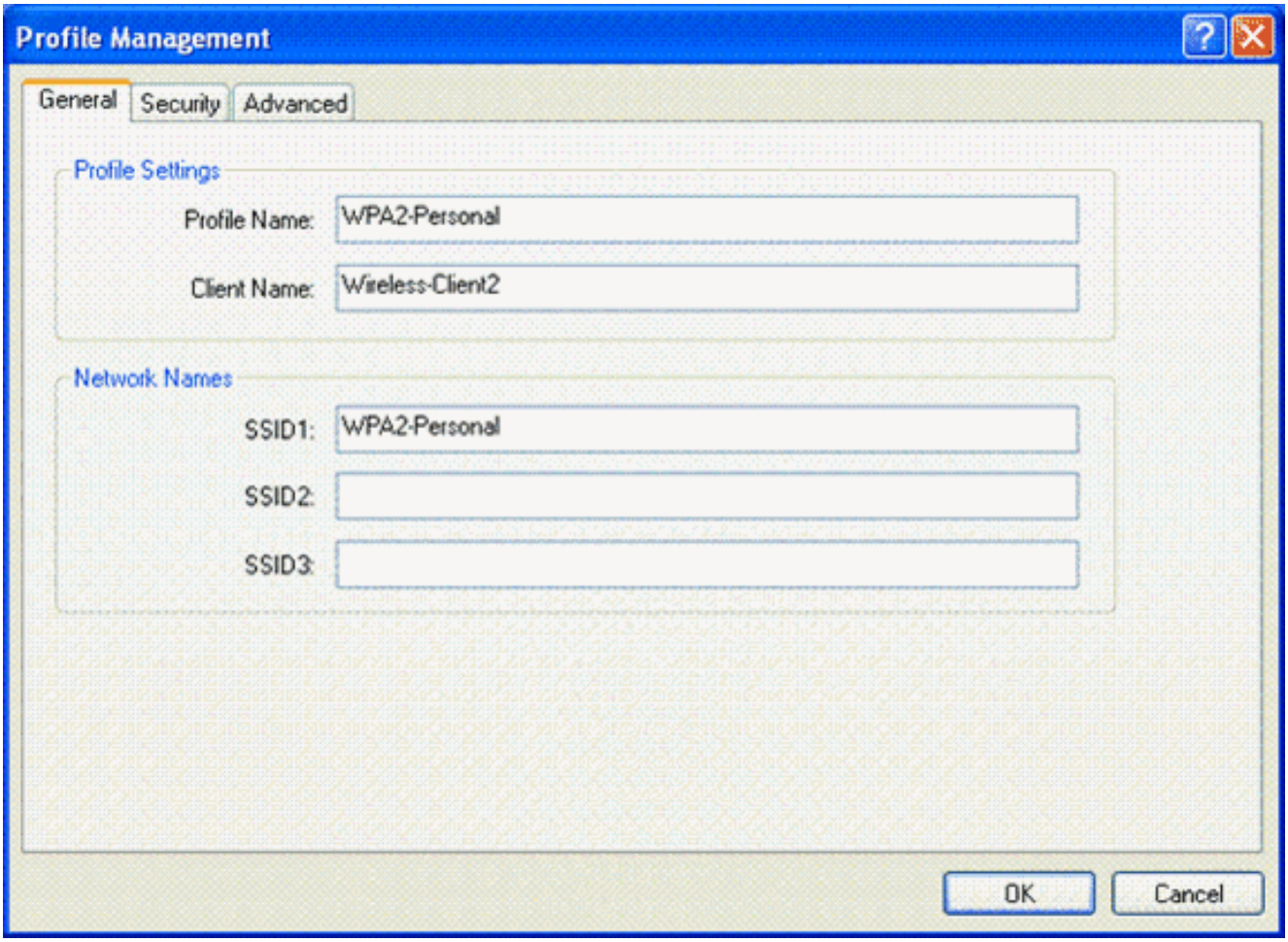
11. Cliquez sur **Apply**.

Configurez le client sans fil pour le mode WPA2 personnel

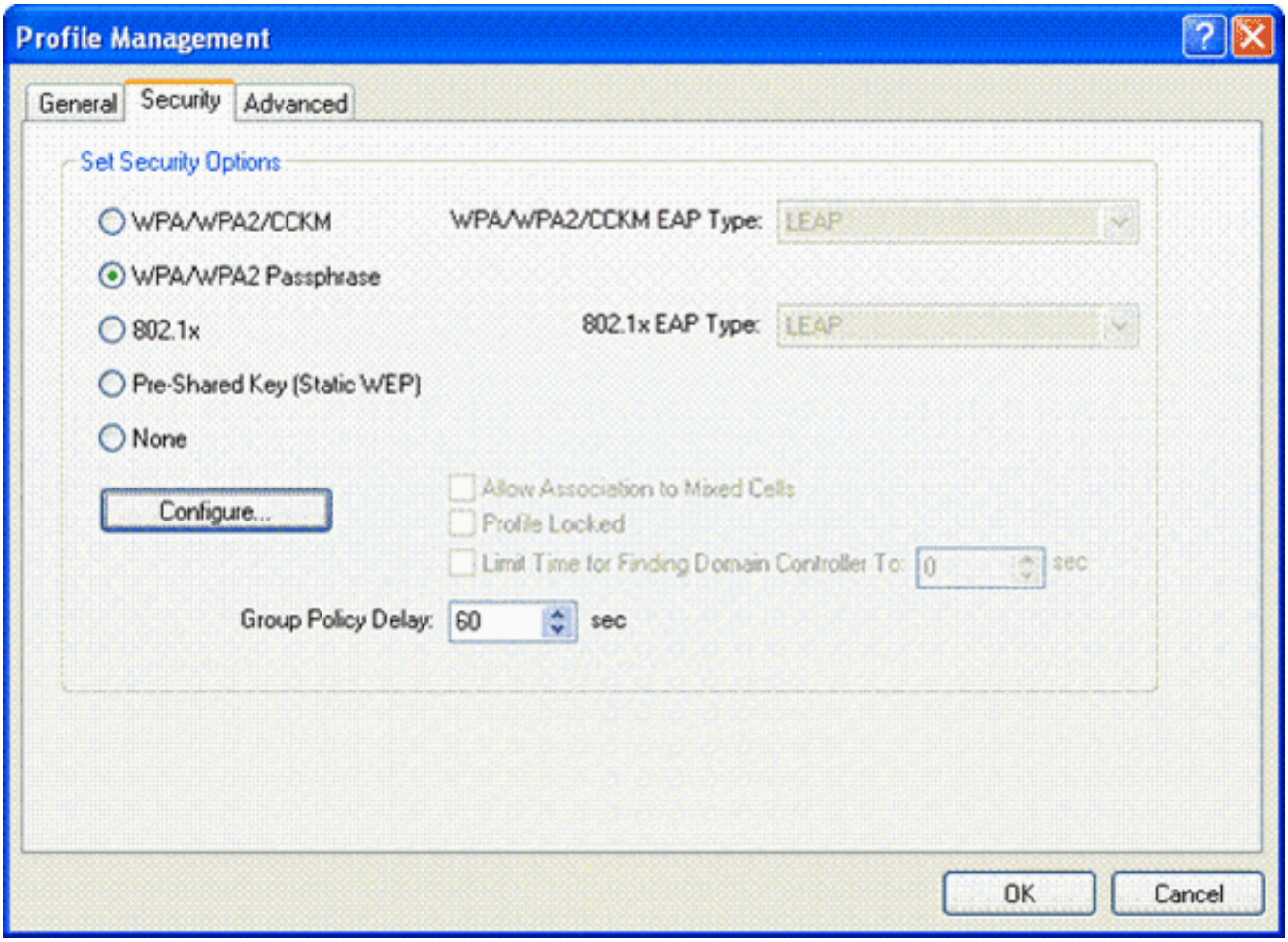
L'étape suivante est de configurer le client sans fil pour le mode de fonctionnement WPA2-Personal.

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

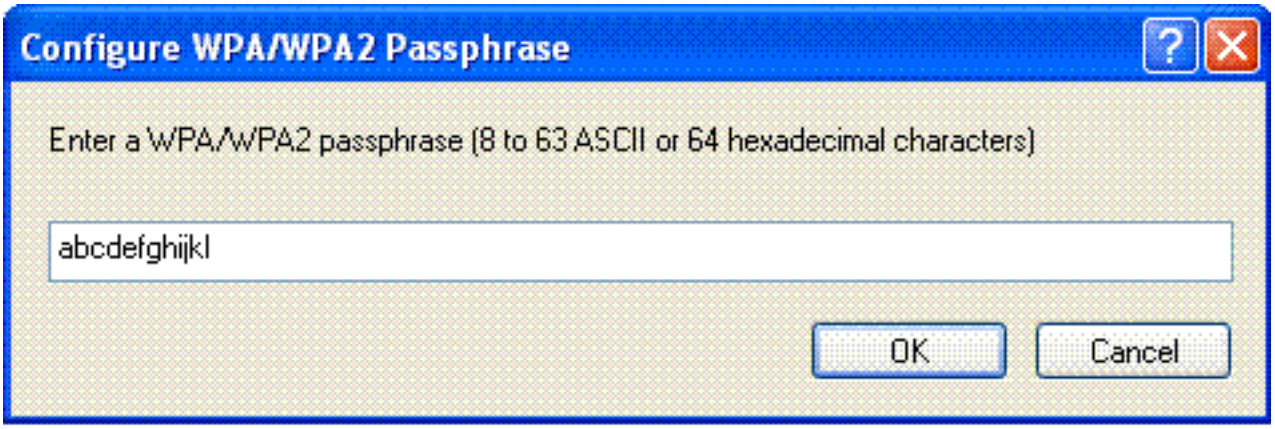
1. De la fenêtre d'Aironet Desktop Utility, **Profile Management > New de** clic afin de créer un profil pour l'utilisateur WPA2-PSK WLAN.
2. De la fenêtre Profile Management, cliquez sur l'**onglet Général** et configurez le nom de profil, le nom de client et le nom SSID suivant les indications de cet exemple. Puis, cliquez sur OK.



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



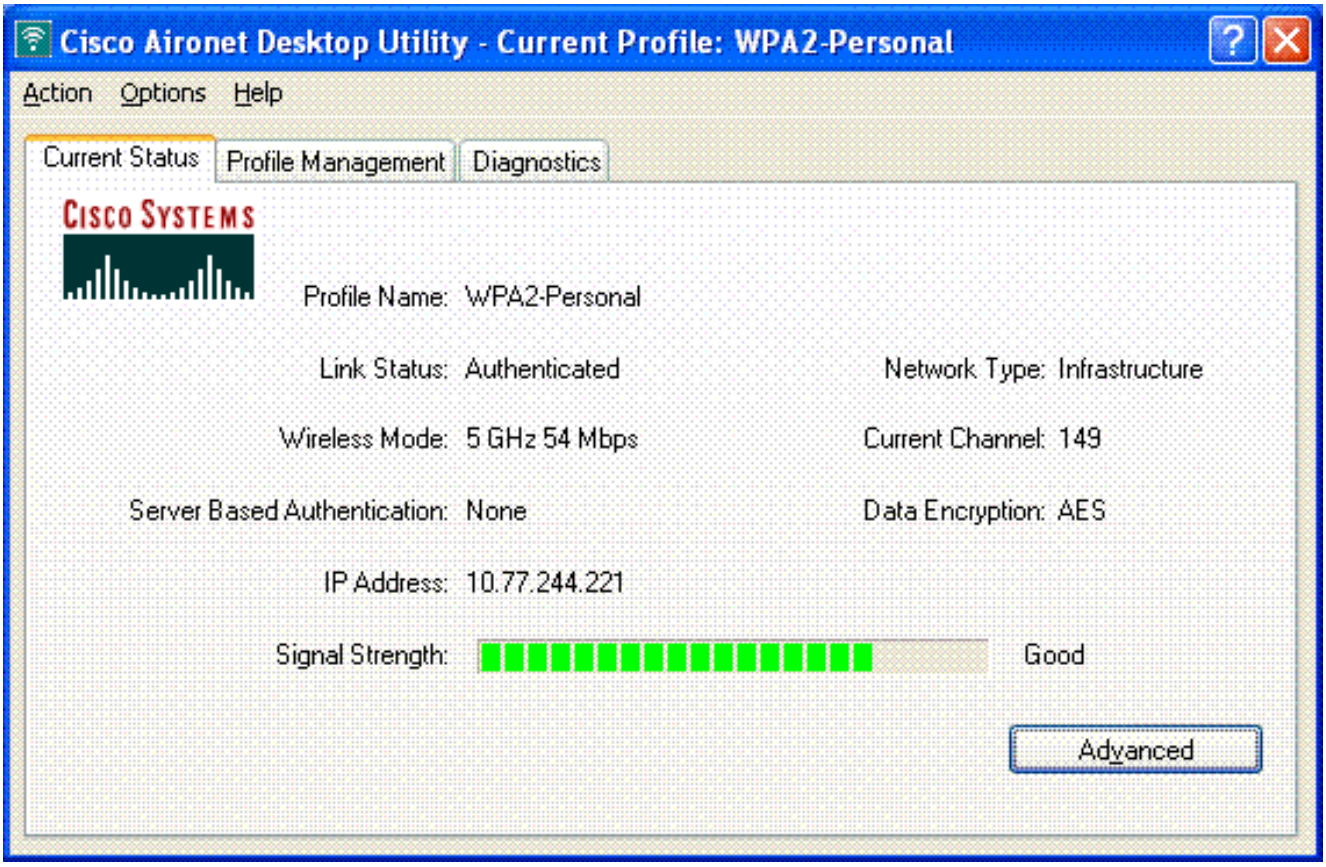
4. Introduisez la clé pré-partagée et cliquez sur OK.



Vérifiez le mode de fonctionnement WPA2-Personal

Terminez-vous ces étapes afin de vérifier si votre configuration de mode de WPA2 Enterprise fonctionne correctement :

1. De la fenêtre d'Aironet Desktop Utility, sélectionnez le profil **WPA2-Personal** et le clic **lancent** afin de lancer le profil de client sans fil.
2. Une fois que le profil est lancé, le client sans fil s'associe au WLAN sur l'authentification réussie.Voici le tir d'écran :



Dépannez

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

Ces commandes de **débogage** seront utiles pour dépanner la configuration :

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **enable d'événements de debug dot1x** — Active le débogage de tous les événements de dot1x. Voici une sortie de débogage d'exemple basée sur l'authentification réussie :**Remarque:** Certaines des lignes de cette sortie ont été les deuxièmes lignes déplacées dues aux limites de l'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
```

- **enable de paquet de debug dot1x** — Active le débogage des messages de paquet de 802.1x.
- **enable d'événements de debug aaa** — Active la sortie de débogage de tous les événements d'AAA.

Informations connexes

- WPA2 - Accès protégé par Wi-Fi 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
- Support et documentation techniques - Cisco Systems