Exemple de configuration WPA 2 (Wi-Fi Protected Access 2)

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Informations générales
Support WPA 2 avec l'équipement Cisco Aironet
Configurez en mode entreprise
Configuration du réseau
Configurez AP
Configuration CLI
Configurez l'adaptateur client
Vérification
Dépannage
Configurez en mode personnel
Configuration du réseau
Configurez AP
Configurez l'adaptateur client
Vérification
Dépannage
Informations connexes

Introduction

Ce document explique les avantages de l'utilisation de l´accès protégé par Wi-Fi 2 (WPA 2) dans un LAN Sans fil (WLAN). Le document fournit deux exemples de configuration sur la façon dont mettre en application WPA 2 sur un WLAN. Le premier exemple montre comment configurer WPA 2 en mode entreprise, et le deuxième exemple configure WPA 2 en mode personnel.

Remarque : WPA fonctionne avec le protocole EAP (Extensible Authentication Protocol).

Conditions préalables

Conditions requises

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

configuration :

- WPA
- Solutions de sécurité WLAN**Remarque :** reportez-vous à Présentation de la sécurité LAN sans fil Cisco Aironet pour plus d'informations sur les solutions de sécurité WLAN Cisco.

Components Used

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

- Point d'accès (AP)/Pont Cisco Aironet 1310G qui exécute le logiciel Cisco IOS® Version 12.3(2)JA
- Adaptateur client de l'Aironet 802.11a/b/g CB21AG qui exécute le microprogramme 2.5
- Aironet Desktop Utility (ADU) qui exécute le microprogramme 2.5

Remarque : Le logiciel d'adaptateur client Aironet CB21AG et PI21AG est incompatible avec d'autres logiciels d'adaptateur client Aironet. Vous devez utiliser l'ADU avec des cartes CB21AG et PI21AG, et vous devez utiliser l'utilitaire de client Aironet (ACU) tous les autres adaptateurs client Aironet. Référez-vous à Installation de l'adaptateur client pour plus d'informations sur la façon d´installer la carte CB21AG et l'ADU.

Remarque : Ce document utilise un point d'accès/pont qui possède une antenne intégrée. Si vous utilisez un AP/pont qui exige une antenne externe, assurez-vous que les antennes sont connectées à l´AP/pont. Autrement, l´AP/pont ne peut pas se connecter au réseau sans fil. Certains modèles d´AP/pont comportent des antennes intégrées, tandis que d'autres ont besoin d'une antenne externe pour le fonctionnement général. Pour informations sur les modèles d´AP/pont qui comportent des antennes internes ou externes, référez-vous au guide de commande/guide de produit du périphérique approprié.

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

Conventions

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

Informations générales

WPA est une solution de sécurisation basée sur standard de l'alliance de Wi-Fi qui traite des vulnérabilités dans les WLAN natifs. Le WPA fournit la protection des données améliorée et le contrôle d'accès pour des systèmes WLAN. WPA aborde toutes les vulnérabilités connues de Wired Equivalent Privacy (WEP) dans l'implémentation originale de la sécurité IEEE 802.11 et apporte une solution de sécurisation immédiate aux WLAN dans les environnements d'entreprises, de petites entreprises et de bureau à domicile (SOHO).

WPA 2 est la prochaine génération de sécurité Wi-Fi. WPA 2 est la mise en œuvre interopérable de Wi-Fi Alliance de la norme ratifiée IEEE 802.11i. WPA 2 met en œuvre le National Institute of Standards and Technology (NIST) - algorithme de cryptage Advanced Encryption Standard (AES)

recommandé avec utilisation du Counter Mode avec Cipher Block Chaining Message Authentication Code Protocol (CCMP). Le mode compteur AES est un cryptage par blocs qui crypte les blocs de données de 128 bits à la fois avec une clé de cryptage de 128 bits. L'algorithme CCMP produit un code d'intégrité de message (MIC) qui fournit l'authentification des données d'origine et l'intégrité des données pour le cadre sans fil.

Remarque : CCMP est également appelé CBC-MAC.

WPA 2 offre un de plus haut niveau de sécurité que WPA parce qu'AES offre un cryptage plus fort que le Temporal Key Integrity Protocol (TKIP). TKIP est l'algorithme de cryptage que WPA utilise. WPA2 crée des clés de session fraîches à chaque association. Les clés de cryptage qui sont utilisées pour chaque client sur le réseau sont uniques et spécifiques à ce client. Finalement, chaque paquet qui est envoyé sans fil est crypté avec une clé unique. La Sécurité est améliorée avec l'utilisation d'une nouvelle et unique clé de cryptage parce qu'il n'y a aucune réutilisation de la clé. WPA est encore considéré sécurisé et TKIP n'a pas été percé. Cependant, Cisco recommande que les clients transitionnent à WPA 2 dès que possible.

WPA et WPA2 supportent chacun deux modes de fonctionnement :

- Mode entreprise
- Mode personnel

Ce document discute la mise en œuvre de ces deux modes avec WPA 2.

Support WPA 2 avec l'équipement Cisco Aironet

WPA 2 est supporté sur ce matériel :

- AP de la gamme Aironet 1130AG et AP de la gamme 1230AG
- AP de la gamme Aironet 1100
- AP de la gamme Aironet 1200
- AP de la gamme Aironet 1300

Remarque : équipez ces points d'accès de radios 802.11g et utilisez le logiciel Cisco IOS Version 12.3(2)JA ou ultérieure.

WPA 2 et AES sont également supportés sur :

- Modules radio de la gamme Aironet 1200 avec les numéros de pièce AIR-RM21A et AIR-RM22A**Remarque :** Le module radio Aironet 1200 avec la référence AIR-RM20A ne prend pas en charge WPA 2.
- Les adaptateurs client de l'Aironet 802.11a/b/g avec la version de microprogramme 2.5

Remarque : les produits de la gamme Cisco Aironet 350 ne prennent pas en charge WPA 2, car leurs radios ne prennent pas en charge AES.

Remarque : Les ponts sans fil de la gamme Cisco Aironet 1400 ne prennent pas en charge WPA 2 ou AES.

Configurez en mode entreprise

Le terme **mode entreprise se rapporte aux produits qui sont testés pour être interopérables en modes clé pré-partagée (PSK) et IEEE 802.1x de fonctionnement pour authentification.** Le 802.1x

est considéré comme étant mieux sécurisé que tous les cadres d'authentification existant en raison de sa flexibilité à l'appui d'un grand choix de mécanismes d'authentification et d'algorithmes de cryptage plus forts. WPA 2 en mode entreprise exécute l'authentification en deux phases. La configuration de l'authentification ouverte se produit pendant la première phase. La deuxième phase est l´authentification 802.1x avec l´une des méthodes EAP. AES fournit le mécanisme de cryptage.

En mode entreprise, les clients et les serveurs d'authentification s'authentifient mutuellement avec l'utilisation d'une méthode d'authentification EAP, et le client et le serveur produisent une Pairwise Master Key (PMK). Avec WPA 2, le serveur produit la PMK dynamiquement et passe la PMK à l´AP.

Cette section discute la configuration qui est nécessaire pour mettez en œuvre WPA 2 dans le mode de fonctionnement d'entreprise.

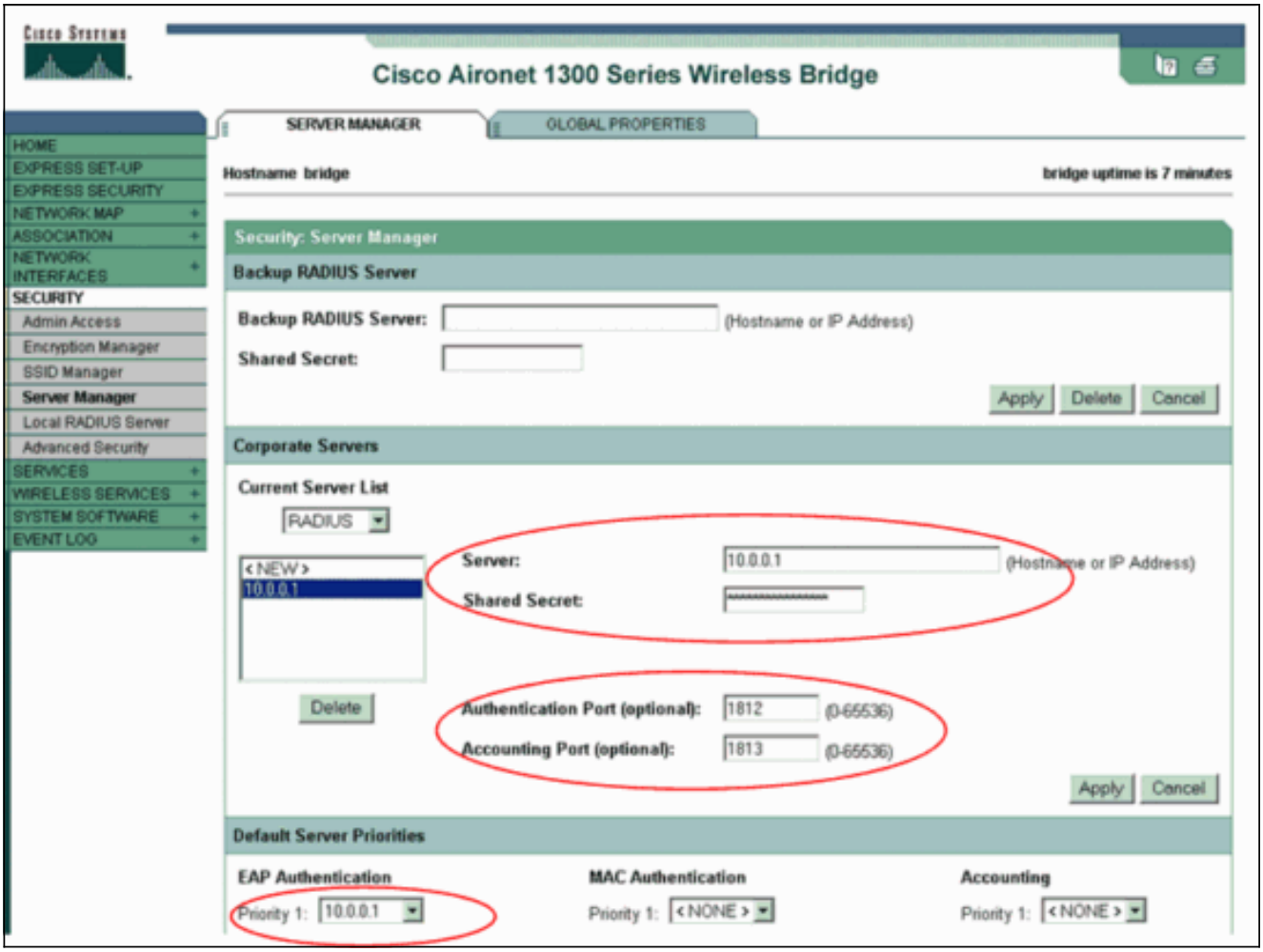
Configuration du réseau

Dans cette configuration, un AP/Bridge de la gamme Aironet 1310G qui exécute Cisco Lightweight Extensible Authentication Protocol (LEAP) authentifie un utilisateur avec un adaptateur client compatible WPA 2. La gestion des clés se produit avec l'utilisation de WPA 2, sur lequel le cryptage AES-CCMP est configuré. AP est configuré en tant que serveur RADIUS local qui exécute l'authentification LEAP. Vous devez configurer l'adaptateur client et l'AP afin de mettre en œuvre cette installation. Les sections Configurer l´AP et Configurer l'adaptateur client montrent la configuration sur l´AP et l'adaptateur client.

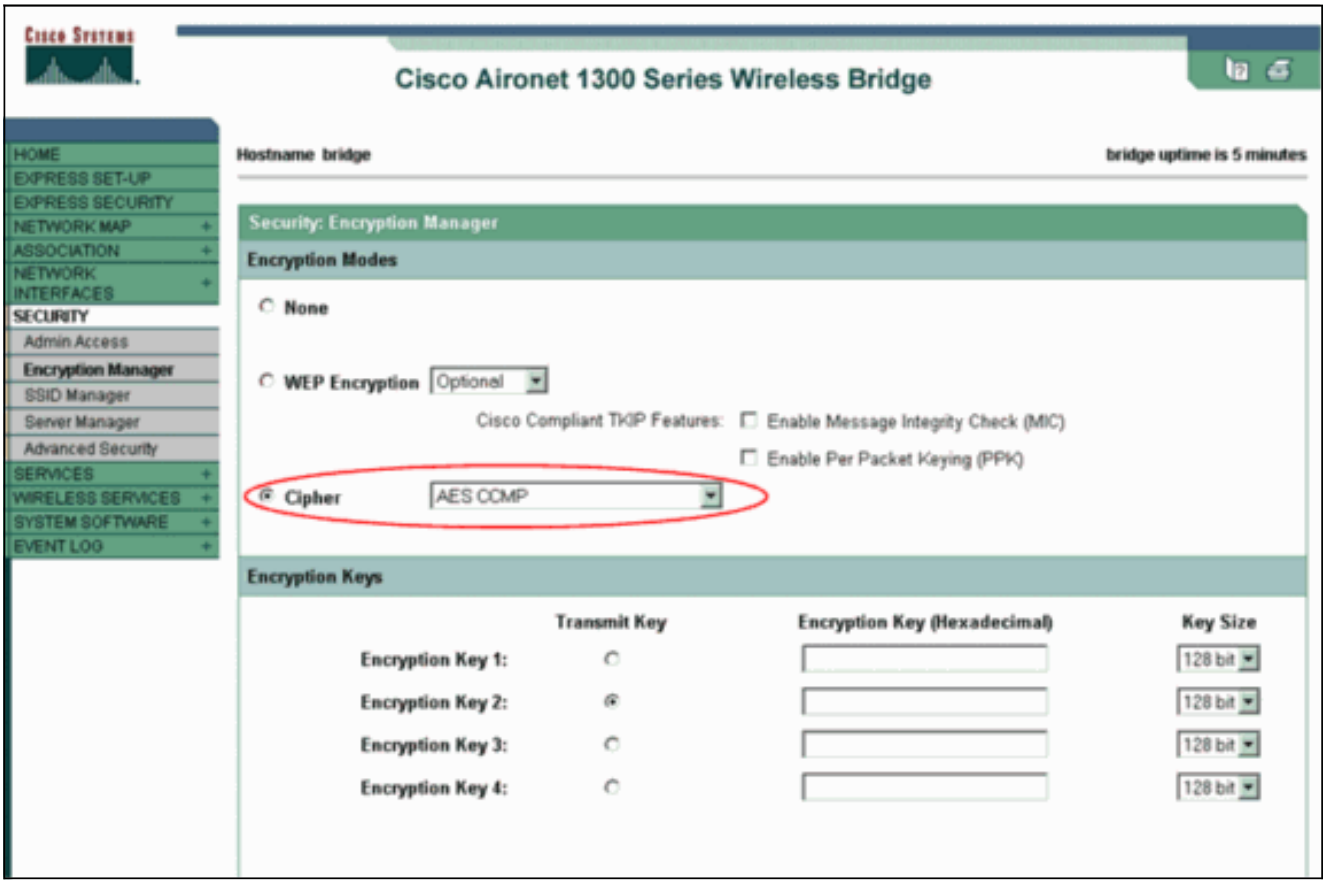
Configurez AP

Complétez ces étapes pour configurer l´AP en utilisant le GUI :

1. Configurez AP en tant que serveur RADIUS local qui exécute l'authentification LEAP.Choisissez **Security > Server Manager dans le menu du côté gauche et définissez l'adresse IP, les ports, et le secret partagé du serveur RADIUS.**Puisque cette configuration configure AP en tant que serveur RADIUS local, utilisez l'adresse IP de l'AP. Utilisez les ports 1812 et 1813 pour le fonctionnement du serveur RADIUS local.Dans la section Default Server Priorities, définissez la priorité d'authentification EAP par défaut à 10.0.0.1.**Remarque :** 10.0.0.1 est le serveur RADIUS
   local.

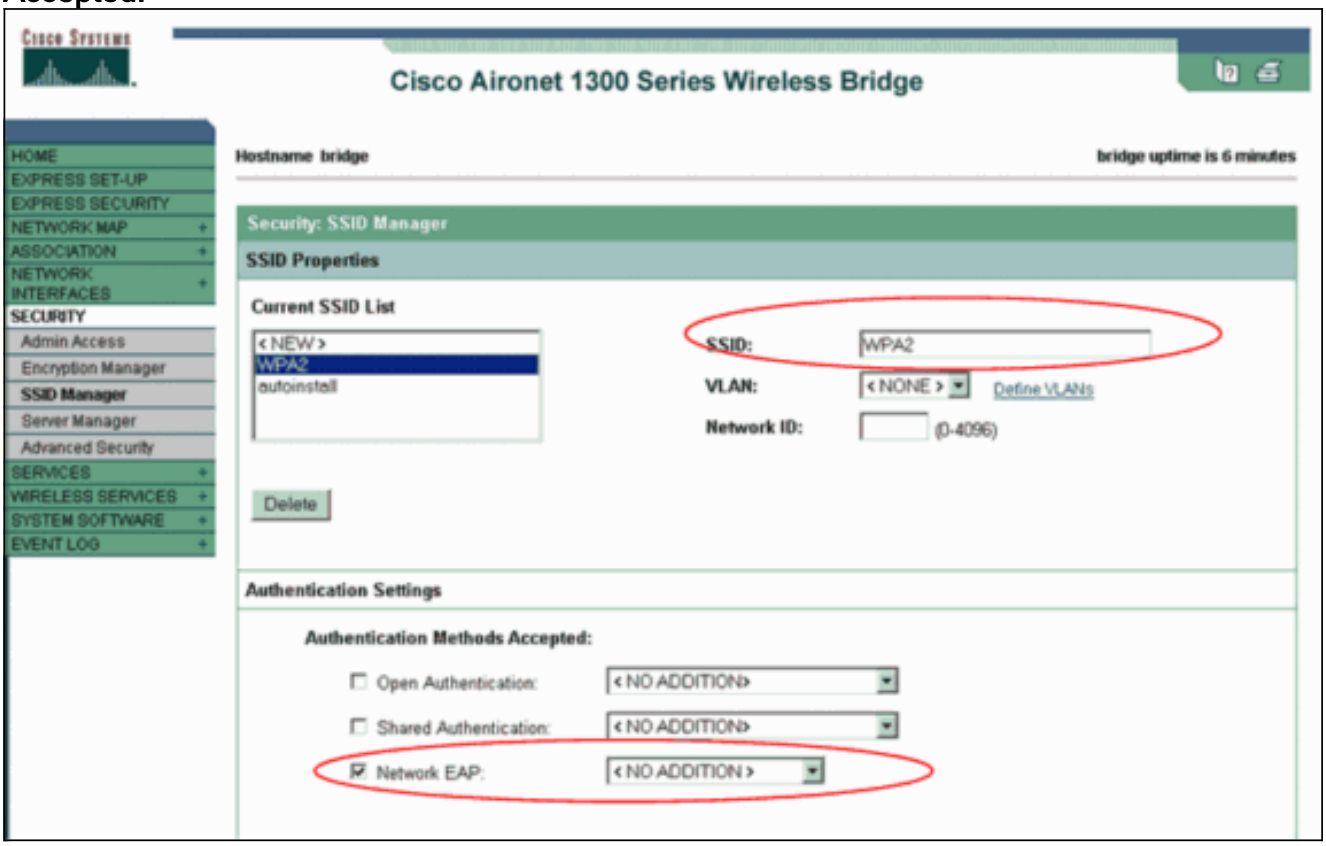


2. Choisissez **Security > Encryption Manager dans le menu du côté gauche et complétez ces étapes :**Dans la menu Cipher, choisissez **AES CCMP**.Cette option active le cryptage AES avec l'utilisation du mode compteur avec CBC-MAC.



Cliquez sur Apply.

3. Choisissez **Security > SSID Manager et créez un nouveau Service Set Identifier (SSID) pour usage avec WPA 2.**Cochez la case à cocher **Network EAP dans la section Authentication Methods Accepted.**

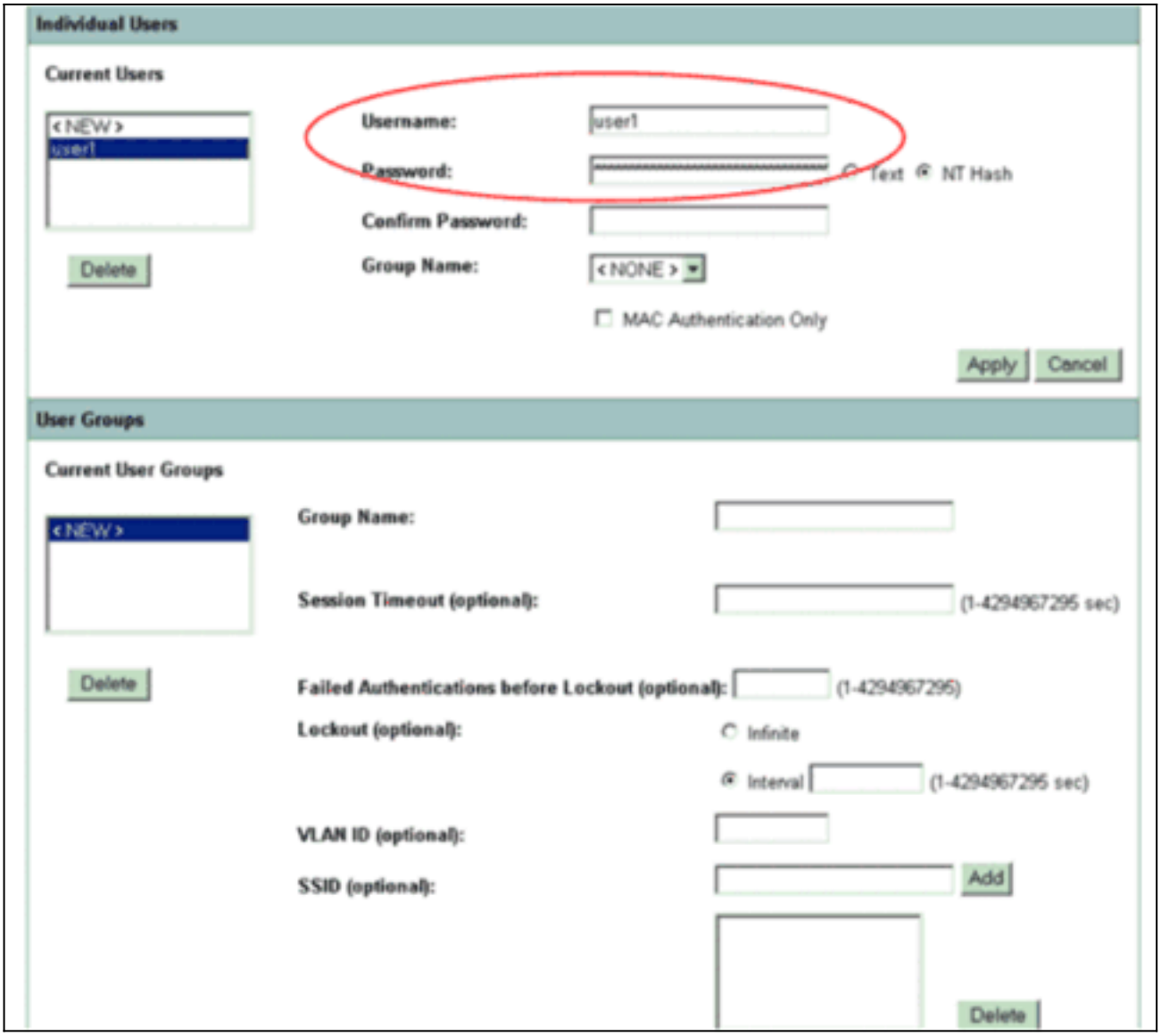


Remarque : Utilisez ces instructions lorsque vous configurez le type d'authentification sur l'interface radio :Clients Cisco - Utilisez Network EAP.Clients tiers (qui incluent les produits conformes Cisco Compatible Extensions [CCX]) - utilisez l'authentification ouverte avec EAP.Une combinaison de clients Cisco et clients tiers - choisissez Network EAP et authentification ouverte avec EAP.Faites défiler vers le bas la fenêtre Security SSID Manager jusqu´au secteur Authenticated Key Management et complétez ces étapes :Dans le menu Key Management, choisissez **Mandatory**.Cochez la case à cocher **WPA du côté droit.**Cliquez sur Apply.**Remarque :** La définition des VLAN est facultative. Si vous définissez les VLAN, les périphériques client qui s´associent avec l'utilisation de ce SSID sont groupés dans le VLAN. Référez-vous à Configuration des VLAN pour plus d'informations sur la façon de mettre en œuvre des
VLAN.

4. Choisissez **Security > Local Radius Server et complétez ces étapes :**Cliquez sur l'onglet **General Set-Up situé en haut de la fenêtre.**Cochez la case à cocher **LEAP et cliquez sur Apply**.Dans le secteur Network Access Servers, définissez l'adresse IP et le secret partagé du serveur RADIUS.Pour le serveur RADIUS local, utilisez l'adresse IP de l'AP.

Cliquez sur Apply.

5. Faites défiler vers le bas la fenêtre General Set-Up jusqu´au secteur Individual Users et définissez les utilisateurs individuels.La définition des groupes d'utilisateurs est facultative.



Cette configuration définit un utilisateur avec le nom « user1 » et un mot de passe. En outre, la configuration sélectionne le hachage de NT pour le mot de passe. Après l'achèvement de la procédure dans cette section, l´AP est prêt à accepter les requêtes d'authentification des clients. L'étape suivante est de configurer l'adaptateur client.

Configuration CLI

Point d'accès

```
ap#show running-config
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap
 server 10.0.0.1 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"rad_eap" !--- that uses the server at 10.0.0.1 on ports
1812 and 1813. . . . aaa authentication login
eap_methods group rad_eap
!--- Authentication [user validation] is to be done for
!--- users in a group called "eap_methods" who use
server group "rad_eap". . . . ! bridge irb ! interface
```

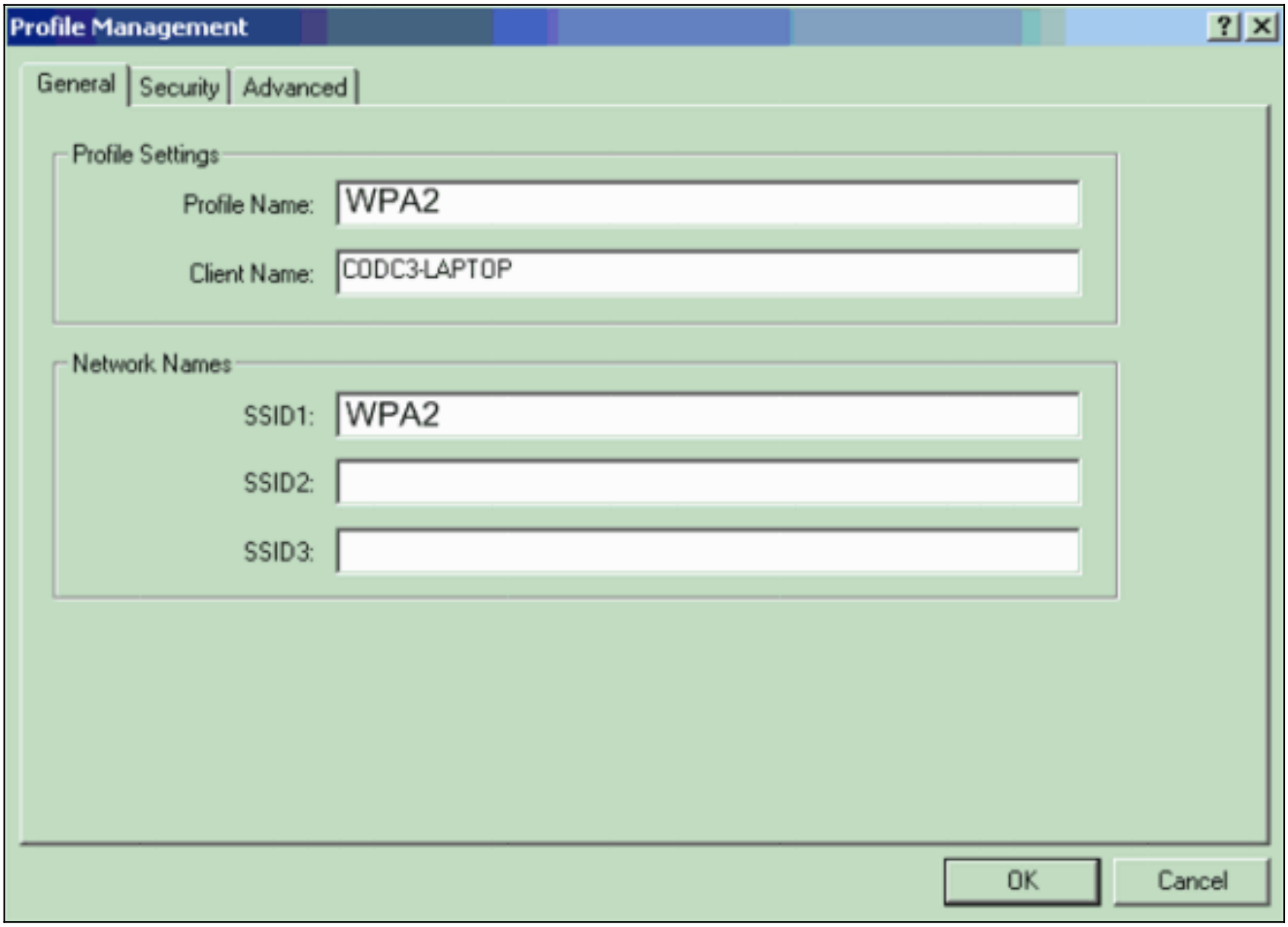
```
Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
   12345678901234567890123456 transmit-key
!---This step is optional !--- This value seeds the
initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory
!--- This defines the policy for the use of Wired
Equivalent Privacy (WEP). !--- If more than one VLAN is
used, !--- the policy must be set to mandatory for each
VLAN. broadcast-key vlan 1 change 300
  !--- You can also enable Broadcast Key Rotation for
each vlan and Specify the time after which Brodacst key
is changed. If it is disabled Broadcast Key is still
used but not changed. ssid cisco vlan 1
!--- Create a SSID Assign a vlan to this SSID
authentication open eap eap_methods
 authentication network-eap eap_methods
 !--- Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and
Network EAP authentication !--- bit set in the headers
of those requests, and group those users into !--- a
group called "eap_methods." ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local
!--- Engages the Local RADIUS Server feature. nas
10.0.0.1 key shared_secret
!--- Identifies itself as a RADIUS server, reiterates !-
-- "localness" and defines the key between the server
(itself) and the access point(itself). ! group testuser
!--- Groups are optional. ! user user1 nthash password1
group testuser
!--- Individual user user user2 nthash password2 group
testuser
!--- Individual user !--- These individual users
comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port
   1813 key shared_secret
!--- Defines where the RADIUS server is and the key
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end
```

Configurez l'adaptateur client

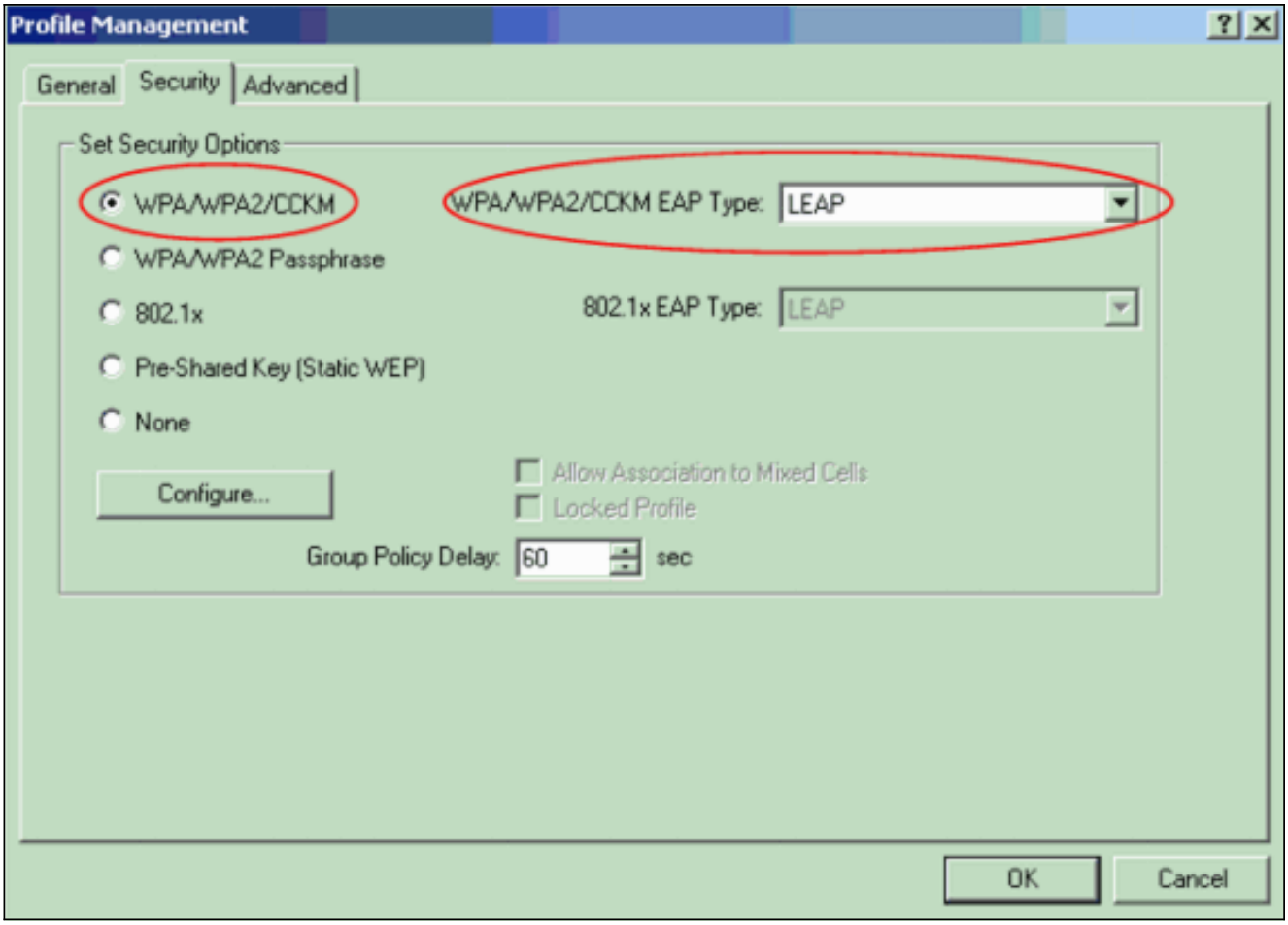
Procédez comme suit :

Remarque : Ce document utilise un adaptateur client Aironet 802.11a/b/g qui exécute le microprogramme 2.5 et explique la configuration de l'adaptateur client avec ADU version 2.5.

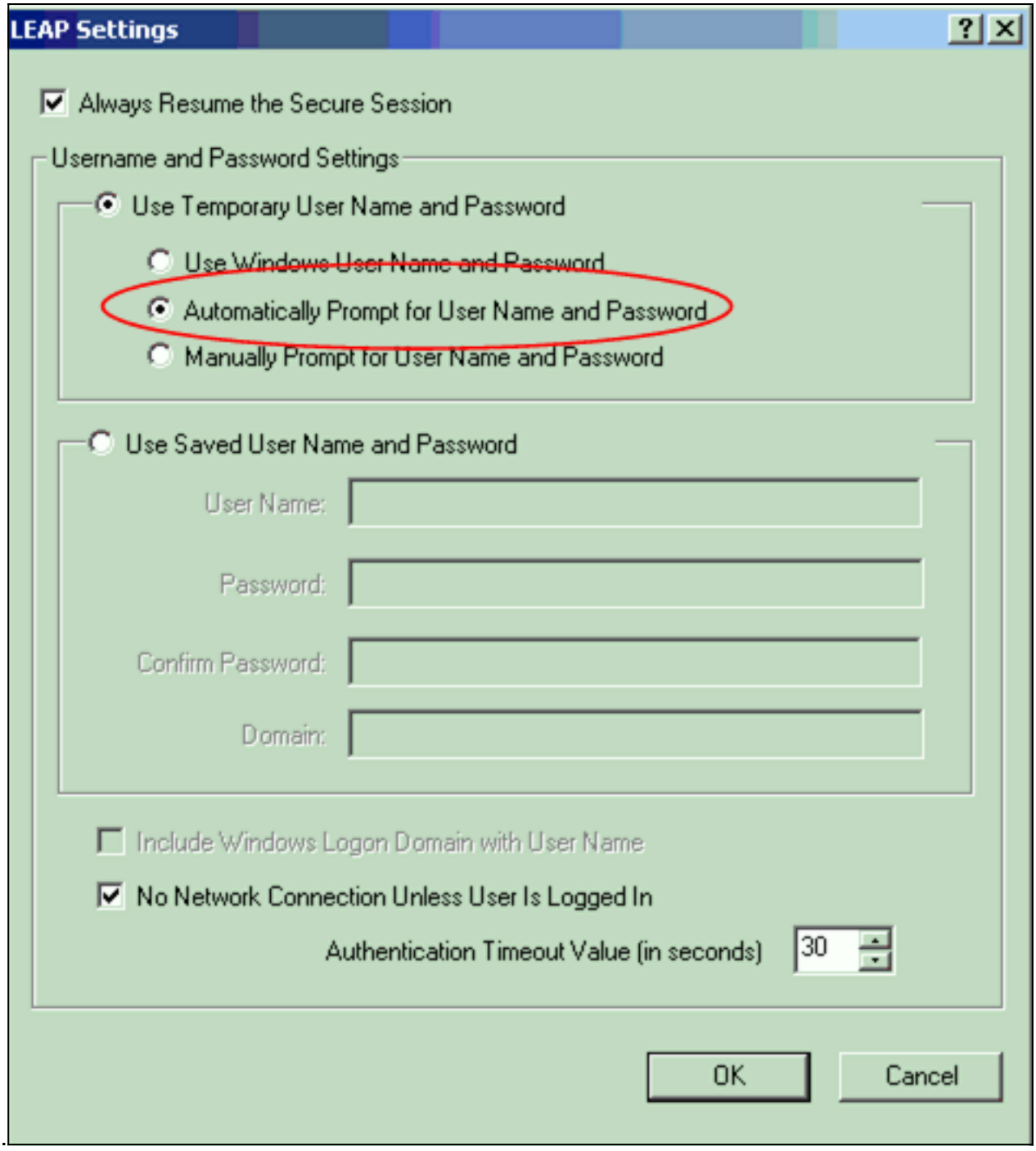
1. Dans la fenêtre Profile Management sur l'ADU, cliquez sur **New afin de créer un nouveau profil.**Une nouvelle fenêtre s´affiche où vous pouvez définir la configuration pour le mode de fonctionnement entreprise de WPA 2. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilisera.Dans cet exemple, le nom de profil et le SSID sont WPA2 :**Remarque :** Le SSID doit correspondre au SSID que vous avez configuré sur l'AP pour WPA
2.



2. Cliquez sur **Security tab, cliquez sur WPA/WPA2/CCKM**, et choisissez **LEAP dans le menu WPA/WPA2/CCKM EAP Type.**Cette action active WPA ou WPA 2, selon celui que vous configurez sur
l´AP.

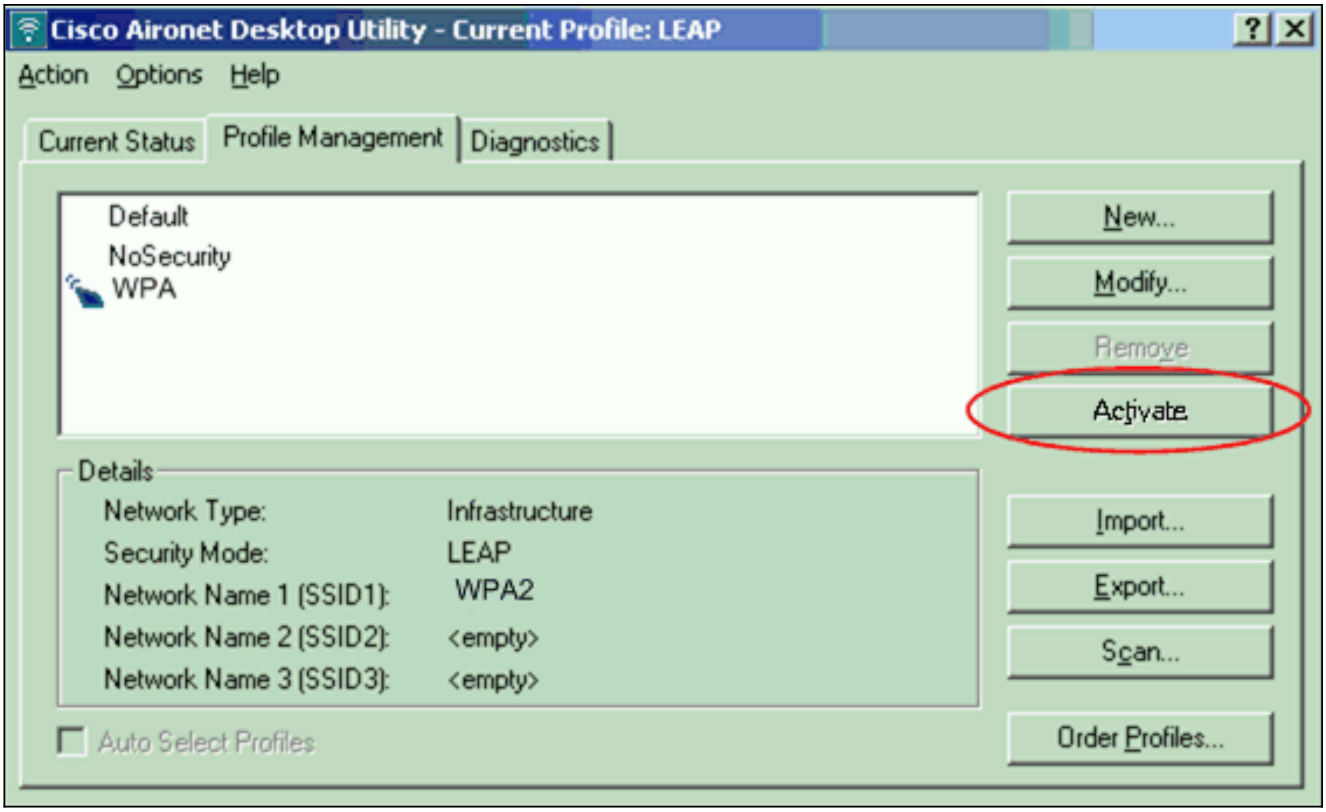


3. Cliquez sur **Configure afin de définir les paramètres LEAP.**
4. Choisissez les paramètres Username et Password appropriés, basés sur les exigences, et cliquez sur **OK**.Cette configuration choisit l'option Automatically Prompt for User Name and Password. Cette option vous permet de saisir manuellement le nom de l'utilisateur et le mot de passe quand l'authentification de LEAP a



lieu.

5. Cliquez sur **OK afin de quitter la fenêtre Profile Management.**
6. Cliquez sur **Activate afin d'activer ce profil sur l'adaptateur client.**

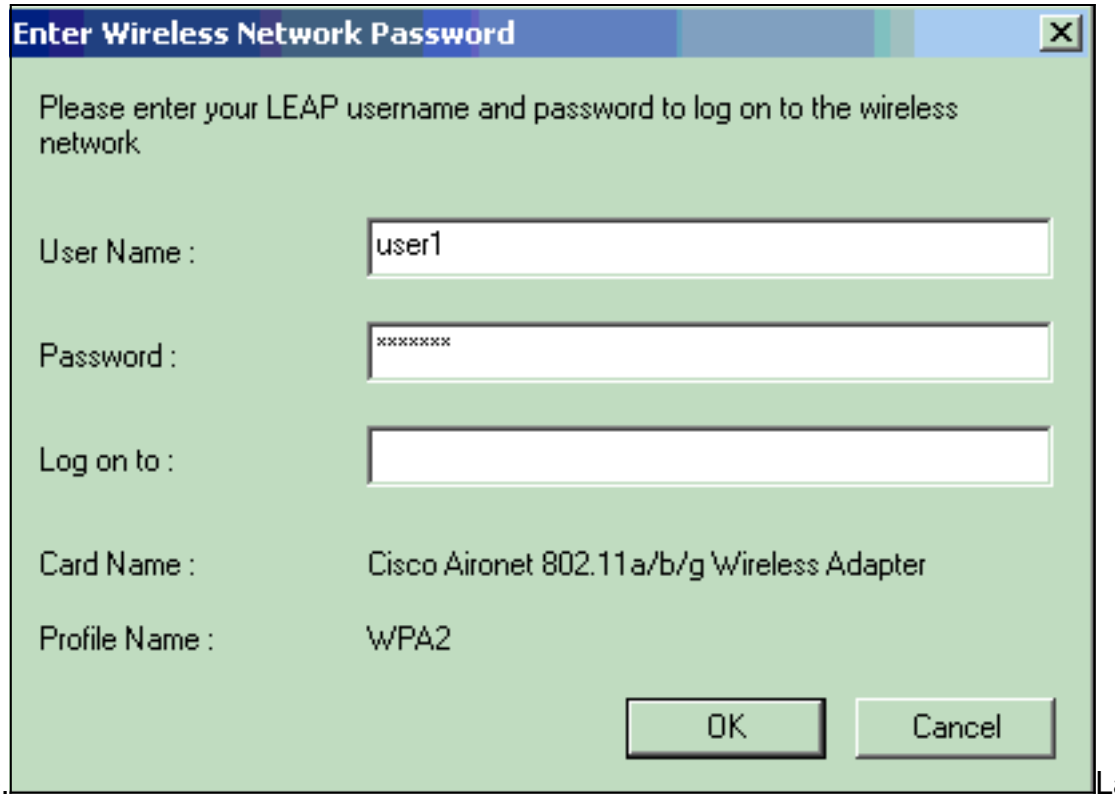


Remarque : si vous utilisez la configuration automatique de réseau sans fil (WZC) de Microsoft pour configurer l'adaptateur client, par défaut, WPA 2 n'est pas disponible avec WZC. Ainsi, afin de permettre aux clients activés WZC d´exécuter WPA 2, vous devez installer un hot fix pour Microsoft Windows XP. Référez-vous à Microsoft Download Center - Update for Windows XP (KB893357) pour l'installation.Après avoir installé le hot fix, vous pouvez configurer WPA 2 avec WZC.

Vérification

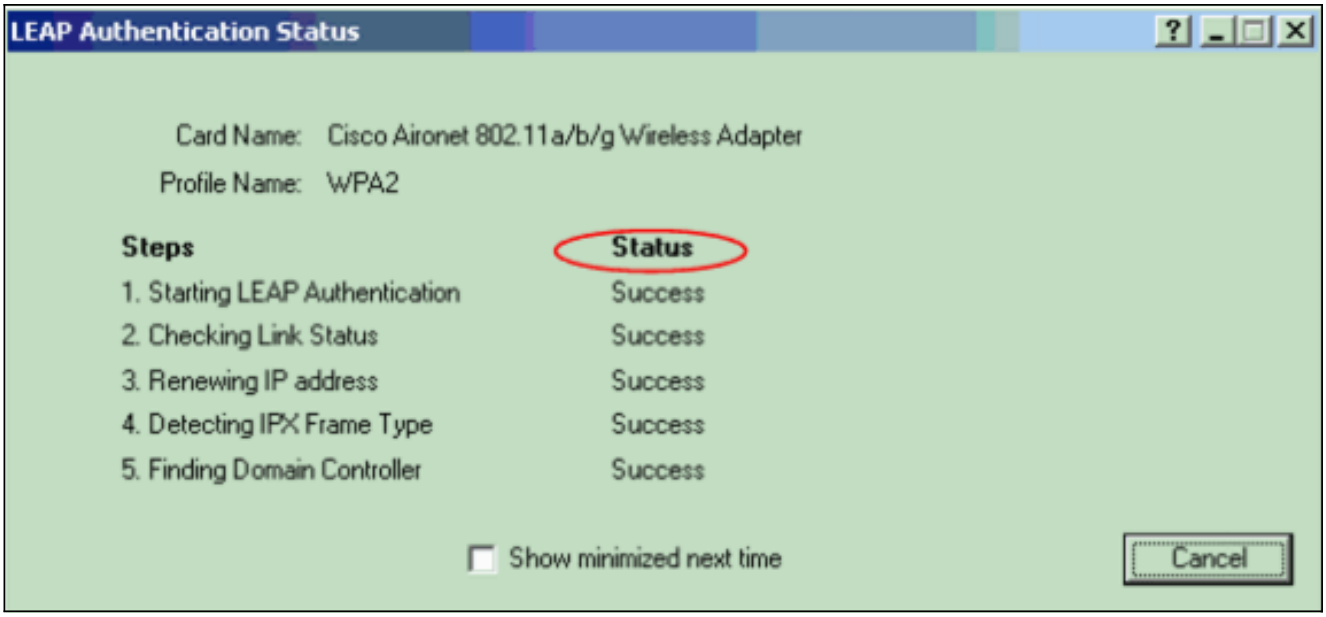
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

1. Quand la fenêtre Enter Wireless Network Password s´affiche, saisissez le nom de l'utilisateur et le mot de



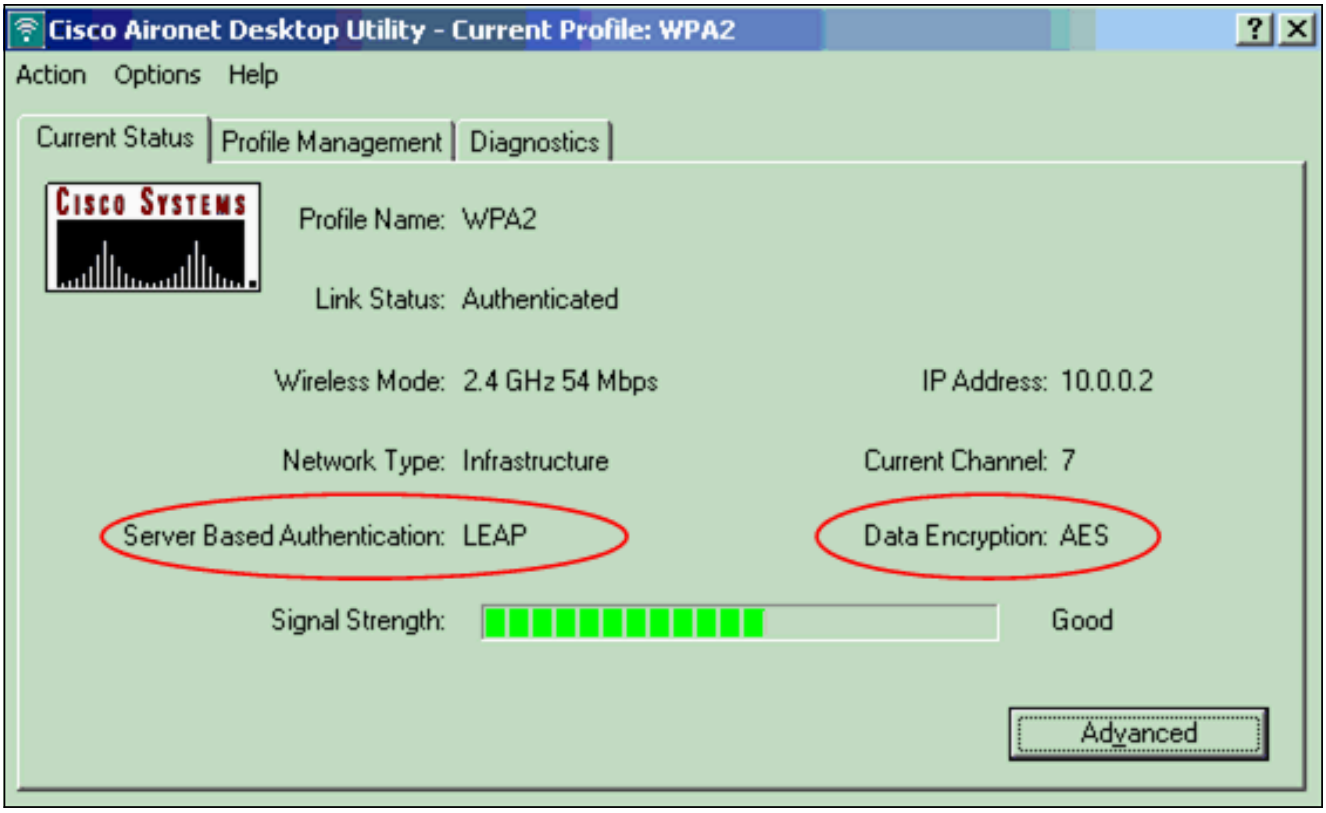
passe.La prochaine fenêtre est LEAP Authentication Status. Cette phase vérifie les qualifications de l'utilisateur contre le serveur RADIUS local.

2. Consultez le secteur Status afin de voir le résultat de l'authentification.



Quand l'authentification est réussie, le client se connecte au LAN sans fil.

3. Contrôlez l'état actuel de l´ADU afin de vérifier que le client utilise le cryptage AES et l'authentification LEAP.Ceci montre que vous avez mis en œuvre WPA 2 avec l'authentification LEAP et le cryptage AES dans le WLAN.



4. Consultez le journal d'événements AP/bridge pour vérifier que le client a été authentifié avec succès avec WPA
   2.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Configurez en mode personnel

Le terme **mode personnel se rapporte aux produits qui sont testés pour être interopérables dans le mode de fonctionnement PSK seul pour l'authentification.** Ce mode exige la configuration

manuelle d'un PSK sur l´AP et les clients. PSK authentifie les utilisateurs par l'intermédiaire d'un mot de passe, ou code d'identification, à la fois sur la station client et l´AP. Aucun serveur d'authentification n'est nécessaire. A client peut accéder au réseau seulement si le mot de passe du client correspond au mot de passe de l´AP. Le mot de passe fournit également le matériel de clé que TKIP ou AES utilise pour produire une clé de cryptage pour le cryptage des paquets de données. Le mode personnel est ciblé pour les environnements SOHO et n'est pas considéré sécurisé pour les environnements d'entreprise. Cette section fournit la configuration dont vous avez besoin pour mettre en œuvre WPA 2 en mode de fonctionnement personnel.

Configuration du réseau

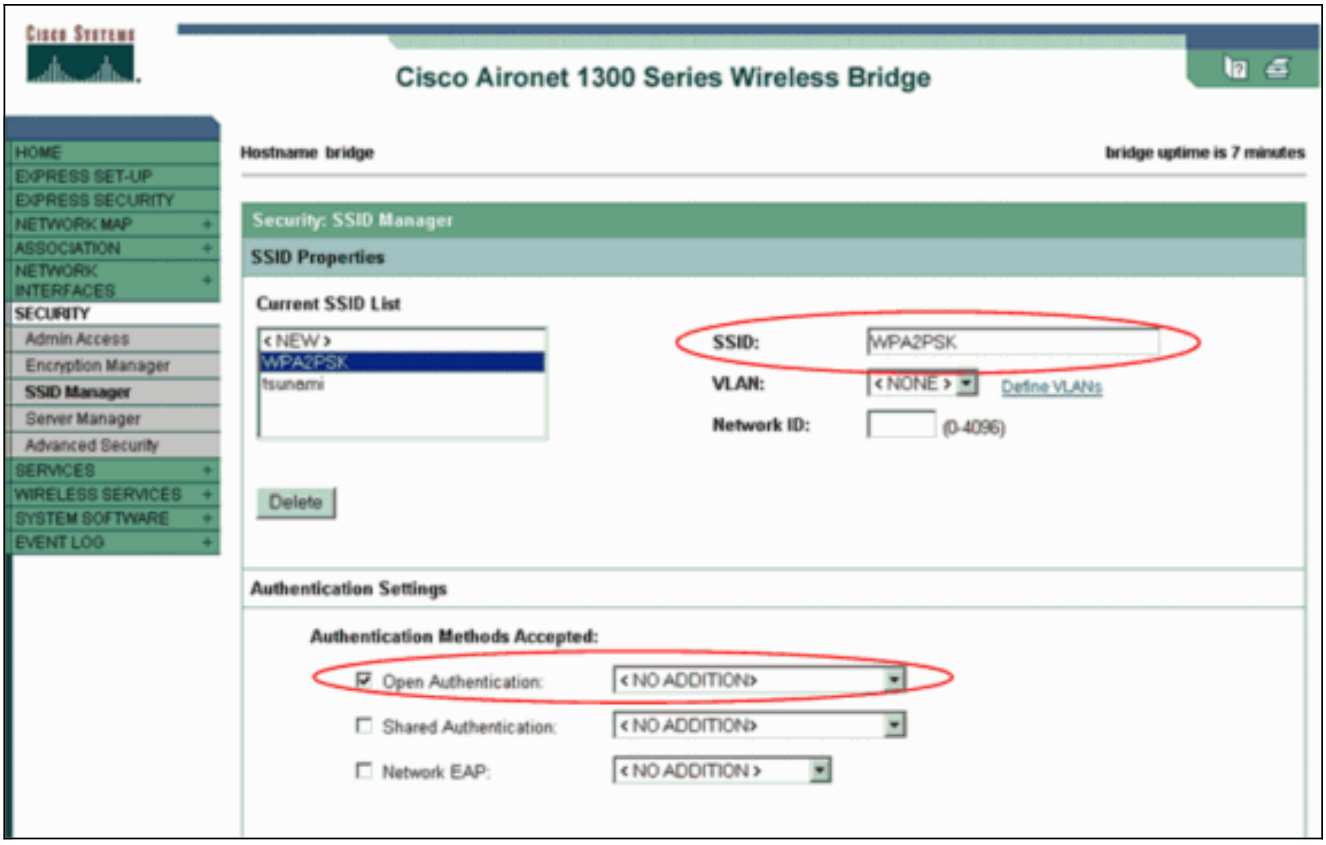
Dans cette configuration, un utilisateur avec un adaptateur client compatible WPA 2 s´authentifie à un AP/Bridge d´Aironet 1310G. La gestion des clés se produit avec l'utilisation de WPA 2 PSK, avec le cryptage AES-CCMP configuré. Les sections Configurer l´AP et Configurer l'adaptateur client montrent la configuration sur l´AP et l'adaptateur client.

Configurez AP

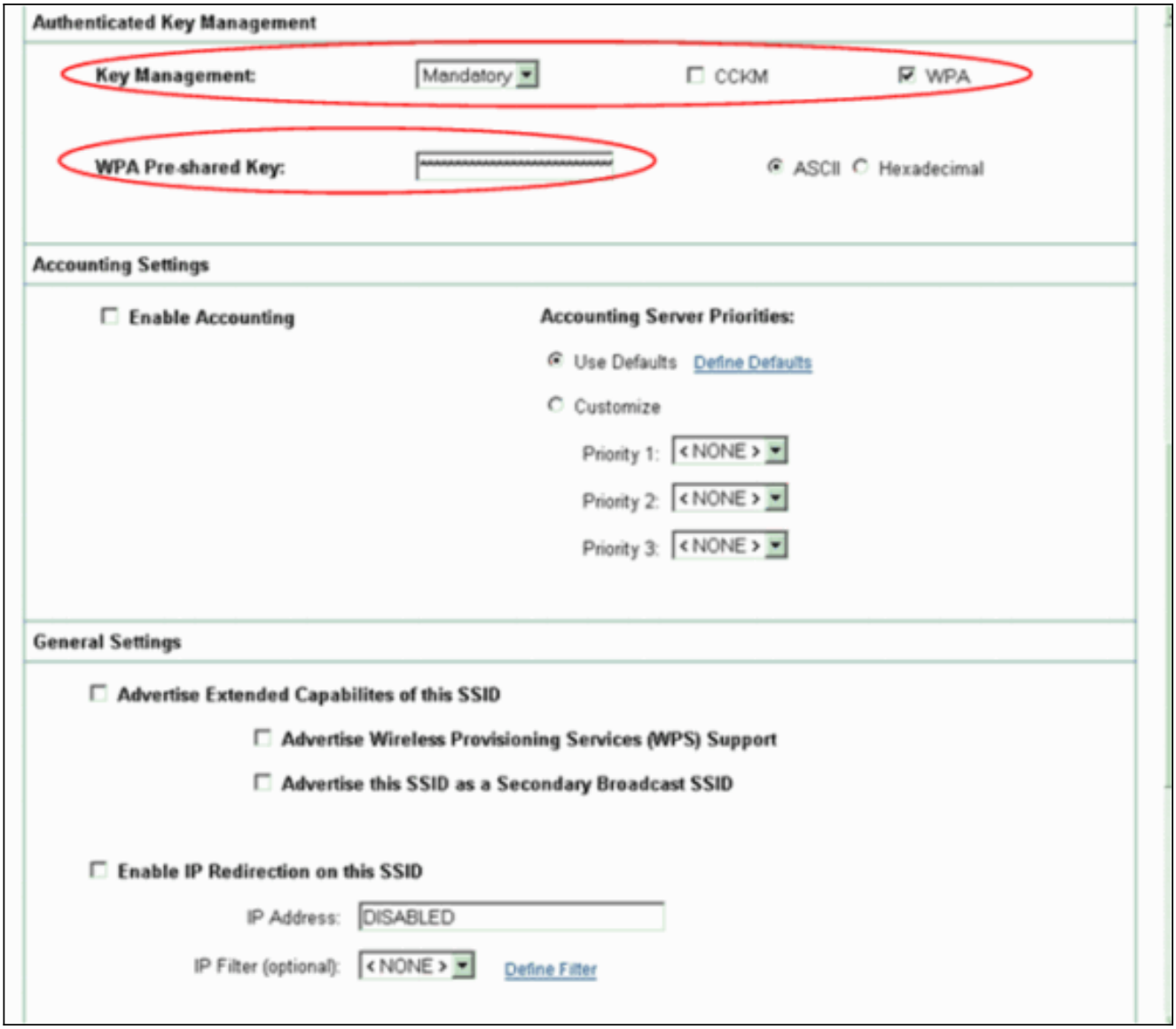
Procédez comme suit :

1. Choisissez **Security > Encryption Manager dans le menu du côté gauche et complétez ces étapes :**Dans la menu Cipher, choisissez **AES CCMP**.Cette option active le cryptage AES avec l'utilisation du mode compteur avec
   CCMP.

   Cliquez sur Apply.
2. Choisissez **Security > SSID Manager et créez un nouveau SSID pour usage avec WPA 2.**Cochez la case à cocher **Open Authentication**
   .



Faites défiler la Sécurité vers le bas : La fenêtre SSID Manager au secteur Authenticated Key Management et complétez ces étapes :Dans le menu Key Management, choisissez **Mandatory**.Cochez la case à cocher **WPA du côté droit.**



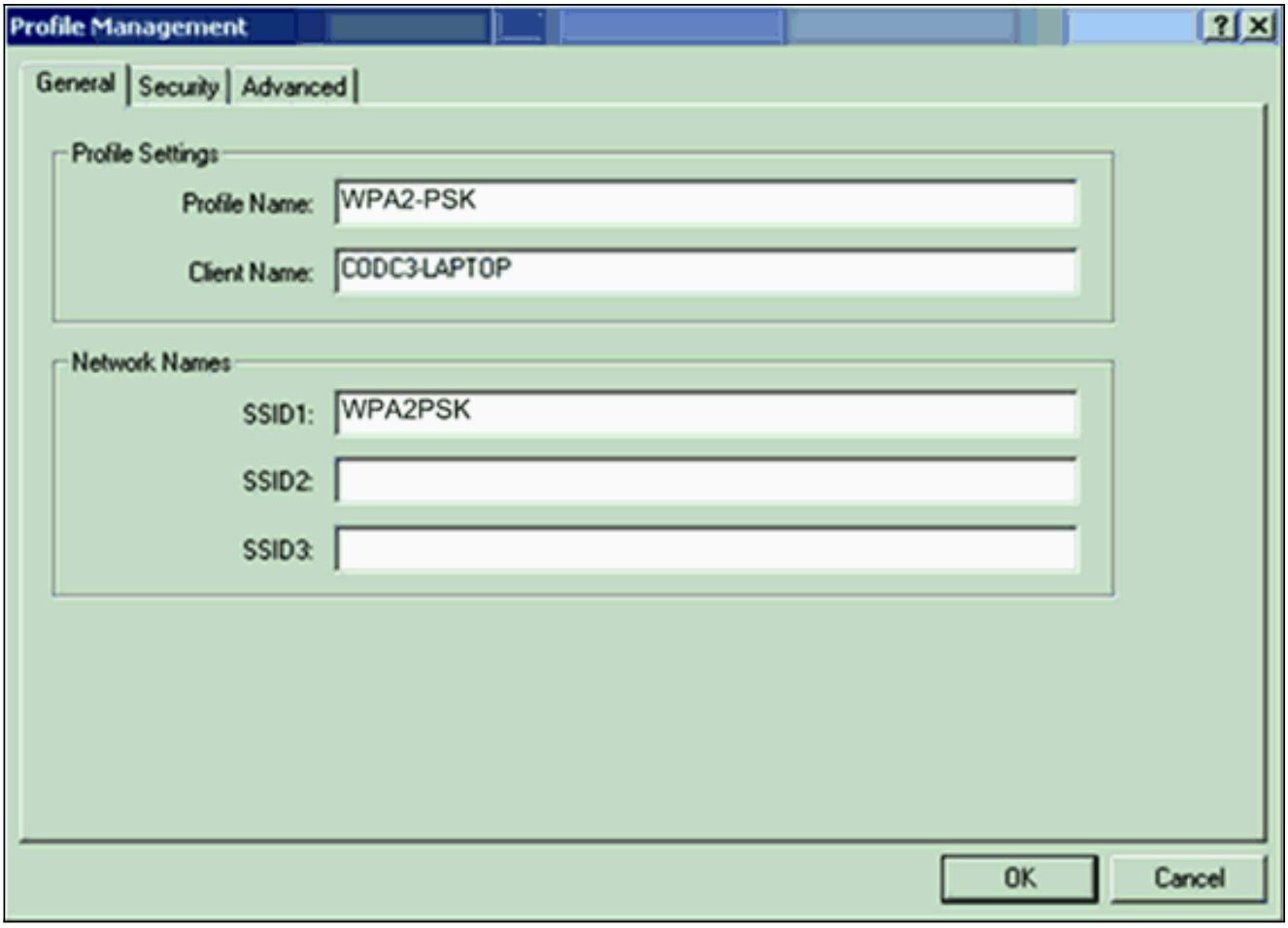
Saisissez la clé secrète partagée PSK WPA ou la clé phrase de passe WPA PSK.Cette clé doit correspondre à la clé WPA PSK que vous configurez sur l'adaptateur client.Cliquez sur Apply.

AP peut maintenant recevoir des requêtes d'authentification des clients sans fil.

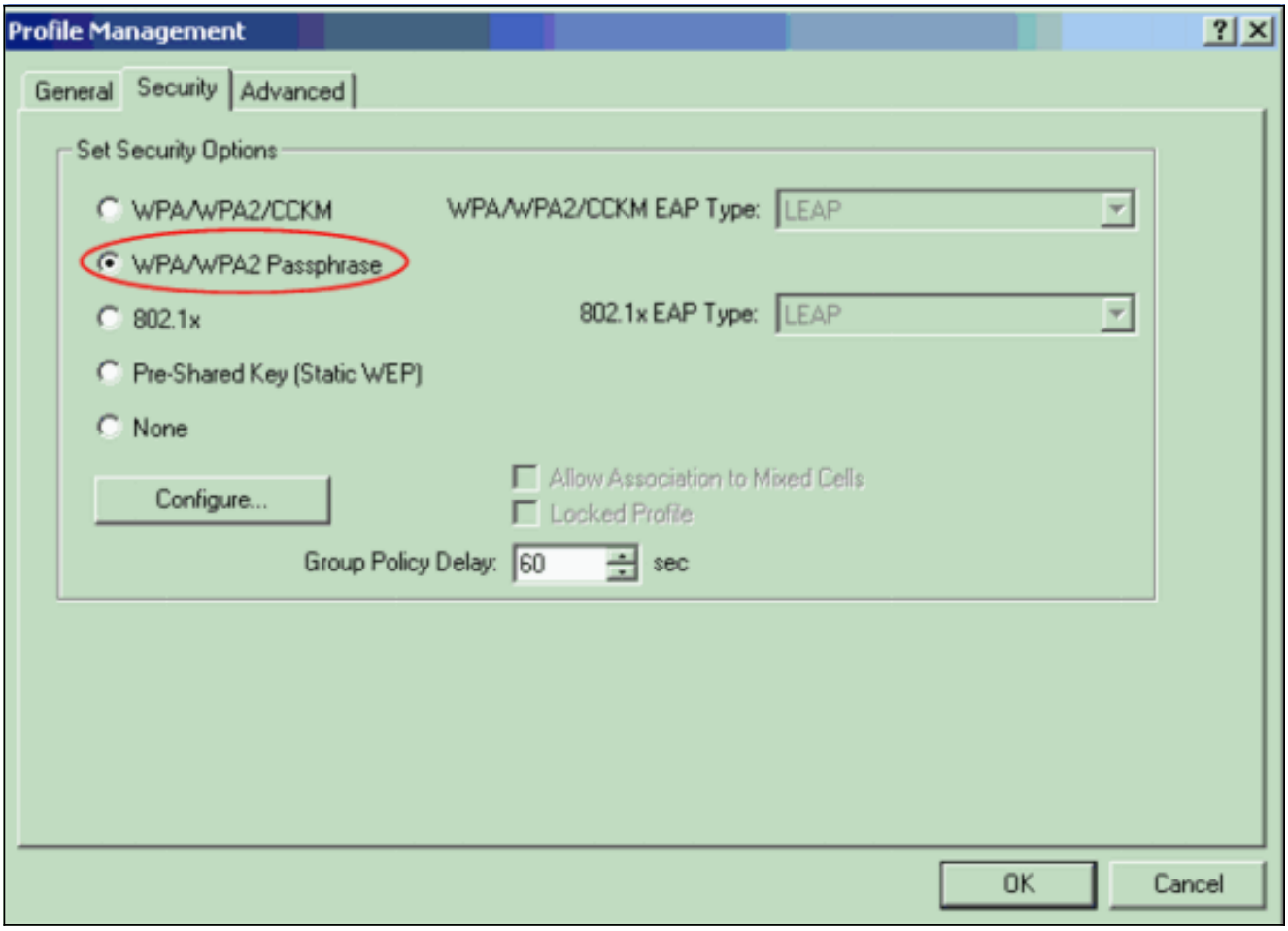
Configurez l'adaptateur client

Procédez comme suit :

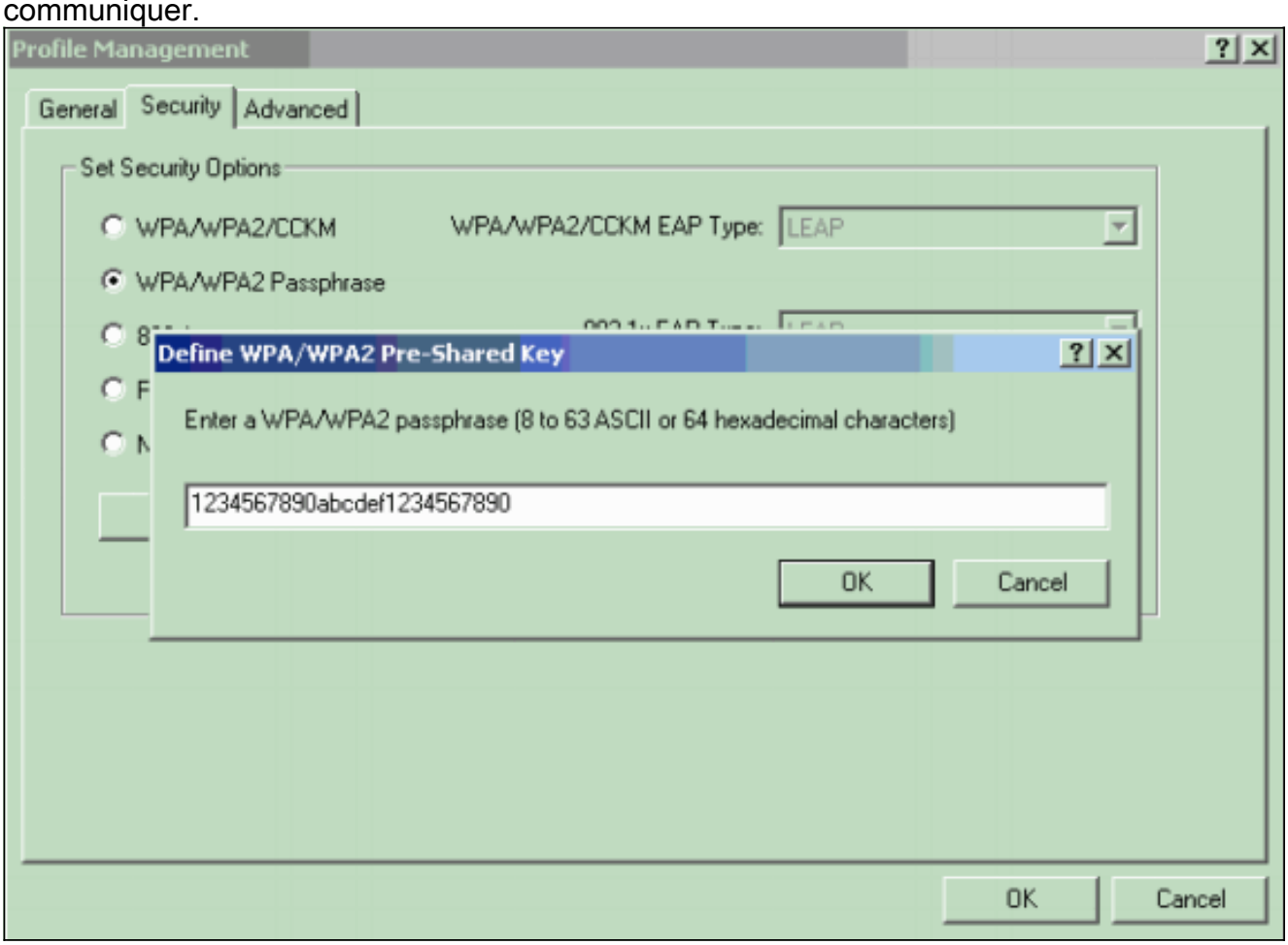
1. Dans la fenêtre Profile Management sur l'ADU, cliquez sur **New afin de créer un nouveau profil.**Une nouvelle fenêtre s´affiche où vous pouvez définir la configuration pour le mode de fonctionnement PSK de WPA 2. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilisera.Dans cet exemple, le nom de profil est WPA2-PSK et le SSID est WPA2PSK :**Remarque :** Le SSID doit correspondre au SSID que vous avez configuré sur l'AP pour WPA 2
PSK.



2. Cliquez sur l´onglet **Security et cliquez sur WPA/WPA2 Passphrase**.Cette action active WPA PSK ou WPA 2 PSK, selon celui que vous configurez sur l´AP.



3. Cliquez sur **Configure**.La fenêtre Define WPA/WPA2 Pre-Shared Key s´affiche.
4. Obtenez la phrase de passe WPA/WPA2 auprès de votre administrateur système et saisissez la phrase de passe dans le champ phrase de passe WPA/WPA2.Obtenez la phrase de passe pour AP dans une infrastructure réseau ou la phrase de passe pour d'autres clients dans un réseau ad-hoc.Employez ces directives afin d'entrer une phrase de passe :Les phrases de passe WPA/WPA2 doivent contenir entre 8 et 63 caractères de texte ASCII ou 64 caractères hexadécimaux.La phrase de passe WPA/WPA2 de votre adaptateur client doit correspondre à la phrase de passe de l'AP avec lequel vous prévoyez de communiquer.



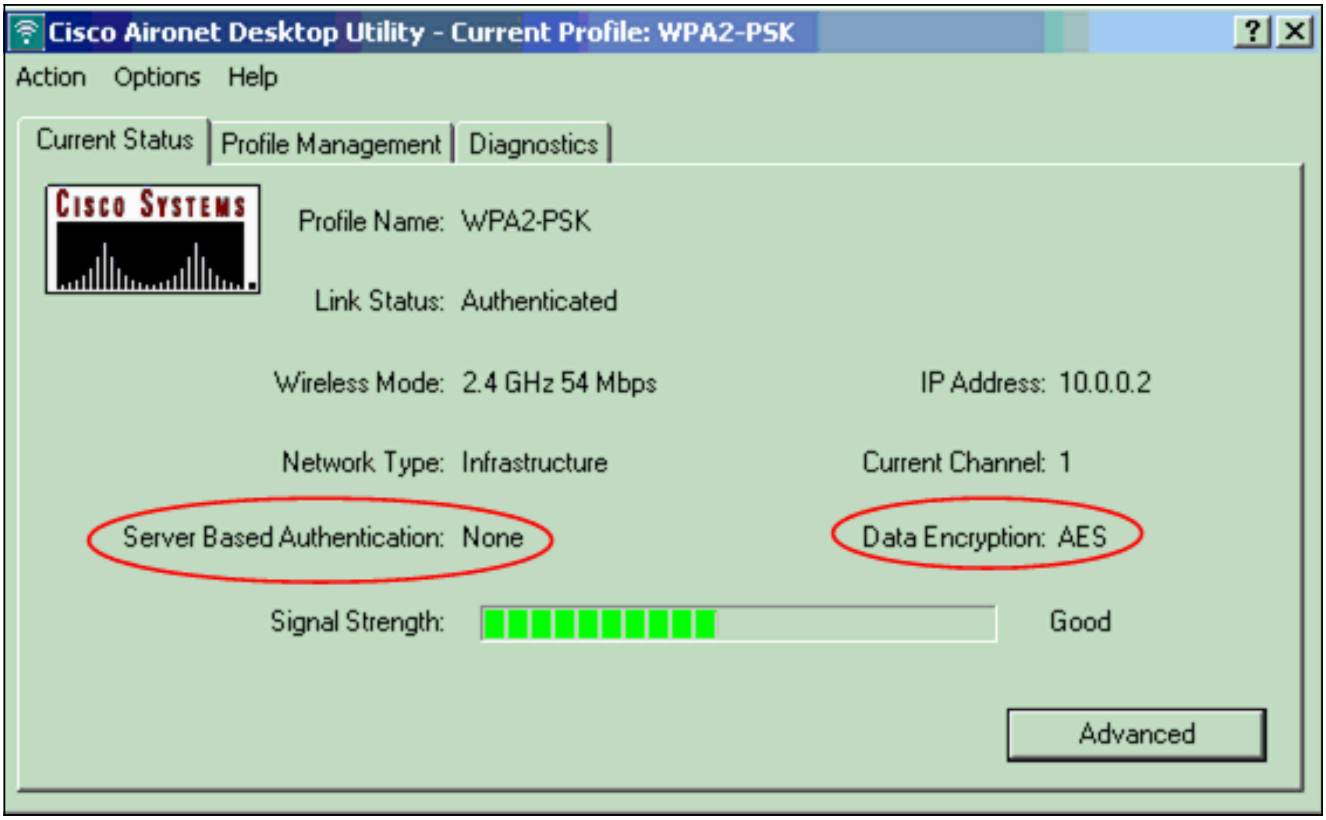
5. Cliquez sur **OK afin de sauvegarder la phrase de passe et retourner à la fenêtre Profile Management.**

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Après avoir activé le profil WPA 2 PSK, AP authentifie le client sur la base de la phrase de passe WPA 2 (PSK) et permet d'accéder au WLAN.

1. Contrôlez l'état actuel de l´ADU afin de vérifier l'authentification réussie.Cette fenêtre fournit un exemple : La fenêtre montre que le cryptage qui est utilisé est AES et qu´aucune authentification basée sur serveur n'est exécutée
   :



2. Consultez le journal d'événements AP/pont pour vérifier que le client a été authentifié avec succès avec le mode d'authentification WPA 2
   PSK.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Configuration des suites de chiffre et de WEP

- Configuration des types d'authentification
- Présentation de la configuration WPA
- WPA2 - Wi-Fi Protected Access 2
- Qu'est-ce que le fonctionnement en mode mixte WPA et comment le configurer dans mon point d'accès
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems