Configurer les types d’authentification sans fil sur un ISR fixe

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Conventions
Informations générales
Configurer
Diagramme du réseau
Configurer l'authentification ouverte
Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
Configuration de l'interface virtuelle pontée (BVI)
Configurer le SSID pour l'authentification ouverte
Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN
Configuration de l'authentification 802.1x/EAP
Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
Configuration de l'interface virtuelle pontée (BVI)
Configurer le serveur RADIUS local pour l'authentification EAP
Configurez le SSID pour l'authentification 802.1x/EAP
Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN
Gestion des clés WPA
Configuration de WPA-PSK
Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
Configuration de l'interface virtuelle pontée (BVI)
Configuration du SSID pour l'authentification WPA-PSK
Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN
Configuration de l'authentification WPA (avec EAP)
Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
Configuration de l'interface virtuelle pontée (BVI)
Configurer le serveur RADIUS local pour l'authentification WPA
Configuration du SSID pour WPA avec authentification EAP
Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN
Configuration du client sans fil pour l'authentification
Configuration du client sans fil pour l'authentification ouverte
Configuration du client sans fil pour l'authentification 802.1x/EAP
Configuration du client sans fil pour l'authentification WPA-PSK
Configuration du client sans fil pour l'authentification WPA (avec EAP)
Dépannage
Dépannage des commandes

[Informations connexes]

Introduction

Ce document donne un exemple de configuration qui explique comment configurer différents types d'authentification de couche 2 sur un routeur à configuration fixe intégré Cisco Wireless pour la connectivité sans fil avec les commandes CLI.

Conditions préalables

Exigences

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

- Connaissance de la configuration des paramètres de base du routeur à services intégrés Cisco (ISR)
- Connaissance de la configuration de l'adaptateur client sans fil 802.11a/b/g avec l'utilitaire de bureau Aironet (ADU)

Composants utilisés

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

- ISR Cisco 877W qui exécute le logiciel Cisco IOS® version 12.3(8)YI1
- Ordinateur portable avec Aironet Desktop Utility version 3.6
- Adaptateur client 802.11 a/b/g qui exécute la version 3.6 du micrologiciel

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.

Informations générales

Les routeurs à configuration fixe à services intégrés Cisco prennent en charge une solution LAN sans fil sécurisée, abordable et facile à utiliser qui allie mobilité et flexibilité aux fonctionnalités professionnelles requises par les professionnels des réseaux. Avec un système de gestion basé sur la plate-forme logicielle Cisco IOS, les routeurs Cisco agissent comme des points d'accès et sont des émetteurs-récepteurs LAN sans fil certifiés Wi-Fi et conformes à la norme IEEE

802.11a/b/g.

Vous pouvez configurer et surveiller les routeurs à l'aide de l'interface de ligne de commande (CLI), du système de gestion basé sur navigateur ou du protocole SNMP (Simple Network Management Protocol). Ce document décrit comment configurer le routeur de service intégré pour la connectivité sans fil à l'aide des commandes CLI.

Configurer

Cet exemple montre comment configurer ces types d'authentification sur un routeur à configuration fixe intégré sans fil Cisco avec des commandes CLI.

- Authentification ouverte
- Authentification 802.1x/EAP (Extensible Authentication Protocol)
- Authentification WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)
- Authentification WPA (avec EAP)

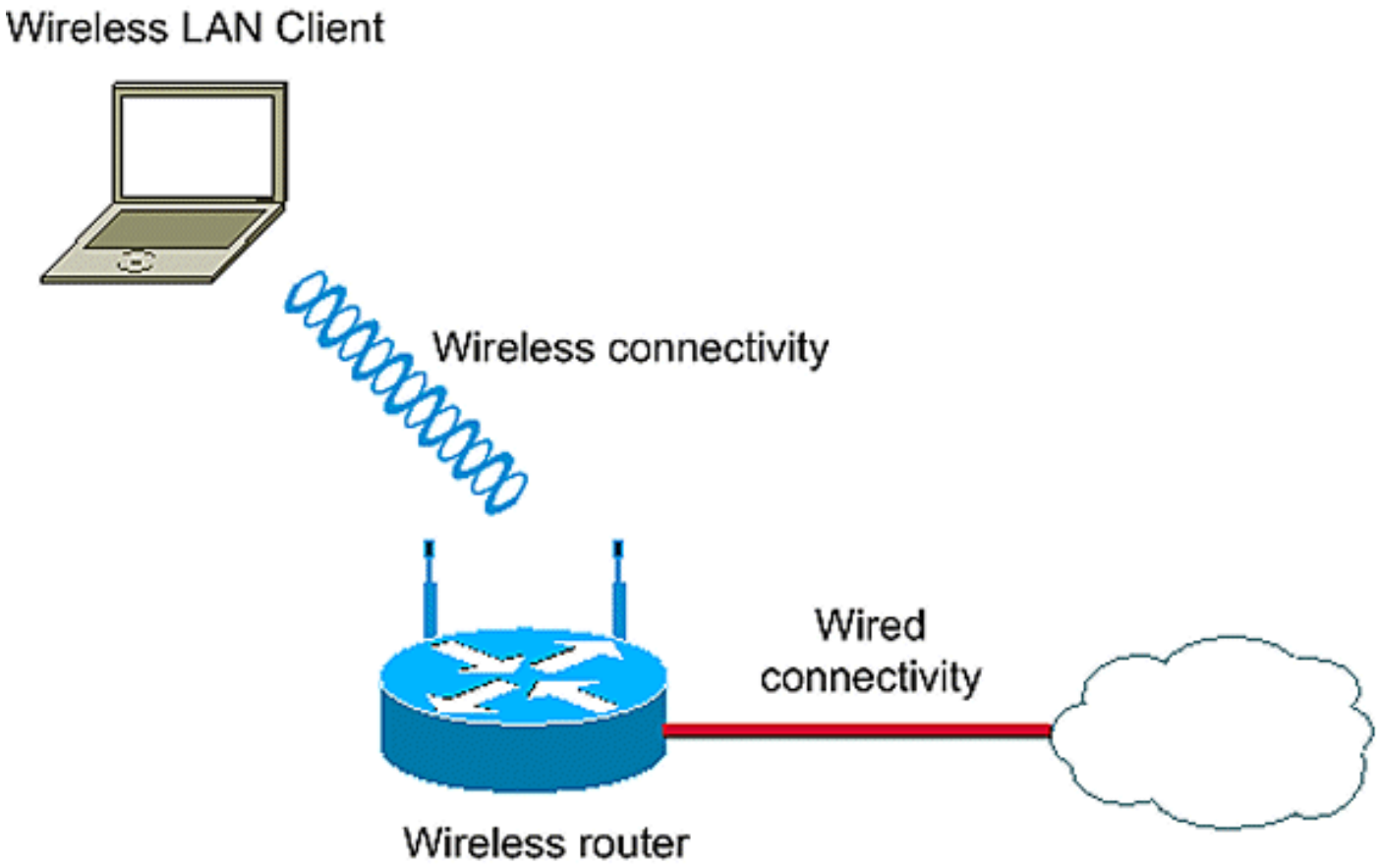
Remarque : ce document ne se concentre pas sur l'authentification partagée, car il s'agit d'un type d'authentification moins sécurisé.

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

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Cette configuration utilise le serveur RADIUS local sur le routeur de service intégré sans fil pour authentifier les clients sans fil avec l'authentification 802.1x.

Configurer l'authentification ouverte

L'authentification ouverte est un algorithme d'authentification nul. Le point d'accès autorise toute demande d'authentification. L'authentification ouverte autorise l'accès au réseau de tous les périphériques. Si aucun chiffrement n'est activé sur le réseau, tout périphérique qui connaît le SSID du point d'accès peut accéder au réseau. Lorsque le cryptage WEP est activé sur un point d'accès, la clé WEP devient elle-même un moyen de contrôle d'accès. Si un périphérique ne dispose pas de la clé WEP correcte, même si l'authentification réussit, il ne peut pas transmettre de données via le point d'accès. Il ne peut pas non plus déchiffrer les données envoyées depuis le point d'accès.

Cet exemple de configuration explique simplement une authentification ouverte. La clé WEP peut être rendue obligatoire ou facultative. Cet exemple configure la clé WEP comme étant facultative afin que tout périphérique qui n'utilise pas WEP puisse également s'authentifier et s'associer à ce point d'accès.

Référez-vous à Authentification ouverte pour plus d'informations.

Cet exemple utilise cette configuration pour configurer l'authentification ouverte sur le routeur de service intégré.

- Nom SSID : "open"

- VLAN 1
- Plage de serveurs DHCP internes : 10.1.0.0/16

Remarque : par souci de simplicité, cet exemple n'utilise aucune technique de cryptage pour les clients authentifiés.

Exécutez les actions suivantes sur le routeur :

1. Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
2. Configuration de l'interface virtuelle pontée (BVI)
3. Configurer le SSID pour l'authentification ouverte
4. Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN

Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont

Effectuez les actions suivantes :

1. Activez IRB dans le routeur.

   router<configure>#bridge irb

   Remarque : si tous les types de sécurité doivent être configurés sur un seul routeur, il suffit d'activer IRB une seule fois globalement sur le routeur. Il n'est pas nécessaire de l'activer pour chaque type d'authentification individuel.

2. Définissez un groupe de ponts.

   Cet exemple utilise le groupe de pontage numéro 1.

   router<configure>#bridge 1

3. Sélectionnez le protocole Spanning Tree pour le groupe de pontage.

   Ici, le protocole Spanning Tree IEEE est configuré pour ce groupe de ponts.

   router<configure>#bridge 1 protocol ieee

4. Permettez à une BVI d'accepter et d'acheminer les paquets routables reçus de son groupe de pontage correspondant.

   Cet exemple permet à l'interface BVI d'accepter et d'acheminer le paquet IP.

   router<configure>#bridge 1 route ip

Configuration de l'interface virtuelle pontée (BVI)

Effectuez les actions suivantes :

1. Configurez le BVI.

   Configurez l'interface BVI lorsque vous attribuez le numéro correspondant du groupe de pontage à l'interface BVI. Chaque groupe de ponts ne peut avoir qu'une seule interface BVI correspondante. Cet exemple attribue le groupe de pontage numéro 1 à la BVI.

   router<configure>#interface BVI <1>

2. Attribuez une adresse IP à l'interface BVI.

   router<config-if>#ip address 10.1.1.1 255.255.0.0

   router<config-if>#no shut

Référez-vous à Configurer le pontage pour des informations détaillées sur le pontage.

Configurer le SSID pour l'authentification ouverte

Effectuez les actions suivantes :

1. Activer l'interface radio

   Afin d'activer l'interface radio, passez en mode de configuration d'interface radio DOT11 et attribuez un SSID à l'interface.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid open

   Le type d'authentification ouverte peut être configuré en association avec l'authentification d'adresse MAC. Dans ce cas, le point d'accès force tous les périphériques clients à effectuer une authentification d'adresse MAC avant d'être autorisés à se connecter au réseau.

   L'authentification ouverte peut également être configurée avec l'authentification EAP. Le point d'accès force tous les périphériques clients à effectuer l'authentification EAP avant d'être autorisés à se connecter au réseau. Pour list-name, spécifiez la liste de méthodes d'authentification.

   Un point d'accès configuré pour l'authentification EAP force tous les périphériques clients associés à effectuer l'authentification EAP. Les périphériques clients qui n'utilisent pas EAP ne peuvent pas utiliser le point d'accès.

2. Liez le SSID à un VLAN.

   Afin d'activer le SSID sur cette interface, liez le SSID au VLAN en mode de configuration SSID.

   router<config-ssid>vlan 1

3. Configurez le SSID avec l'authentification ouverte.

   router<config-ssid>#authentication open

4. Configurez l'interface radio pour la clé WEP (facultatif).

   router<config>#encryption vlan 1 mode WEP facultatif

5. Activez le VLAN sur l'interface radio.

   router<config>#interface Dot11Radio 0.1

   router<config-subif>#encapsulation dot1Q 1

   router<config-subif>#bridge-group 1

Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN

Tapez ces commandes en mode de configuration globale pour configurer le serveur DHCP interne pour les clients sans fil de ce VLAN :

- ip dhcp excluded-address 10.1.1.1 10.1.1.5
- ip dhcp pool open

En mode de configuration du pool DHCP, tapez ces commandes :

- réseau 10.1.0.0 255.255.0.0
- default-router 10.1.1.1

Configuration de l'authentification 802.1x/EAP

Ce type d'authentification offre le niveau de sécurité le plus élevé pour votre réseau sans fil. Avec le protocole EAP (Extensible Authentication Protocol) utilisé pour interagir avec un serveur RADIUS compatible EAP, le point d'accès aide un périphérique client sans fil et le serveur RADIUS à effectuer une authentification mutuelle et à dériver une clé WEP de monodiffusion dynamique. Le serveur RADIUS envoie la clé WEP au point d'accès, qui l'utilise pour tous les signaux de données de monodiffusion qu'il envoie ou reçoit du client.

Référez-vous à Authentification EAP pour plus d'informations.

Cet exemple utilise la configuration suivante :

- Nom SSID : saut
- VLAN 2
- Plage de serveurs DHCP internes : 10.2.0.0/16

Cet exemple utilise l'authentification LEAP comme mécanisme d'authentification du client sans fil.

Remarque : référez-vous à Cisco Secure ACS pour Windows v3.2 avec authentification de machine EAP-TLS pour configurer EAP-TLS.

Remarque : reportez-vous à Configuration de Cisco Secure ACS pour Windows v3.2 avec l'authentification de machine PEAP-MS-CHAPv2 pour configurer PEAP-MS-CHAPv2.

Remarque : comprenez que toutes les configurations de ces types EAP impliquent principalement les modifications de configuration côté client et côté serveur d'authentification. La configuration au niveau du routeur sans fil ou du point d'accès reste plus ou moins la même pour tous ces types d'authentification.

Remarque : comme indiqué précédemment, cette configuration utilise le serveur RADIUS local sur le routeur de service intégré sans fil pour authentifier les clients sans fil avec l'authentification 802.1x.

Exécutez les actions suivantes sur le routeur :

1. Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
2. Configuration de l'interface virtuelle pontée (BVI)
3. Configurer le serveur RADIUS local pour l'authentification EAP
4. Configurez le SSID pour l'authentification 802.1x/EAP
5. Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN

Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont

Effectuez les actions suivantes :

1. Activez IRB dans le routeur.

   router<configure>#bridge irb

   Remarque : si tous les types de sécurité doivent être configurés sur un seul routeur, il suffit d'activer IRB une seule fois globalement sur le routeur. Il n'est pas nécessaire de l'activer pour chaque type d'authentification individuel.

2. Définissez un groupe de ponts.

   Cet exemple utilise le groupe de pontage numéro 2.

   router<configure>#bridge 2

3. Sélectionnez le protocole Spanning Tree pour le groupe de pontage.

   Ici, le protocole Spanning Tree IEEE est configuré pour ce groupe de ponts.

router<configure>#bridge 2 protocol ieee

4. Sélectionnez le protocole Spanning Tree pour le groupe de pontage.

   Ici, le protocole Spanning Tree IEEE est configuré pour ce groupe de ponts.

   router<configure>#bridge 2 protocol ieee

5. Activez une interface BVI pour accepter et router les paquets routables reçus de son groupe de pontage correspondant.

   Cet exemple permet à l'interface BVI d'accepter et d'acheminer des paquets IP.

   router<configure>#bridge 2 route ip

Configuration de l'interface virtuelle pontée (BVI)

Effectuez les actions suivantes :

1. Configurez le BVI.

   Configurez l'interface BVI lorsque vous attribuez le numéro correspondant du groupe de pontage à l'interface BVI. Chaque groupe de pontage ne peut avoir qu'une seule interface BVI correspondante. Cet exemple attribue le groupe de pontage numéro 2 à la BVI.

   router<configure>#interface BVI <2>

2. Attribuez une adresse IP à l'interface BVI.

   router<config-if>#ip address 10.2.1.1 255.255.0.0

   router<config-if>#no shut

Configurer le serveur RADIUS local pour l'authentification EAP

Comme mentionné précédemment, ce document utilise le serveur RADIUS local sur le routeur reconnaissant le sans fil pour l'authentification EAP.

1. Activez le modèle de contrôle d'accès AAA (Authentication, Authorization, and Accounting).

   router<configure>#aaa new-model

2. Créez un groupe de serveurs rad-eap pour le serveur RADIUS.

   router<configure>#aaa group server radius rad-eap server 10.2.1.1 auth-port 1812 acct-port 1813

3. Créez une liste de méthodes eap_methods qui répertorie la méthode d'authentification utilisée pour authentifier l'utilisateur de connexion AAA. Attribuez la liste de méthodes à ce groupe de serveurs.

router<configure>#aaa authentication login eap_methods group rad-eap

4. Activez le routeur en tant que serveur d'authentification local et passez en mode de configuration pour l'authentificateur.

   router<configure>#radius-server local

5. En mode de configuration du serveur Radius, ajoutez le routeur en tant que client AAA du serveur d'authentification local.

   router<config-radsrv>#nas 10.2.1.1 clé Cisco

6. Configurez user user1 sur le serveur RADIUS local.

   router<config-radsrv>#user user1 password user1 group rad-eap

7. Spécifiez l'hôte du serveur RADIUS.

   router<config-radsrv>#radius-server host 10.2.1.1 auth-port 1812 acct-port 1813 key cisco

   Remarque : cette clé doit être identique à celle spécifiée dans la commande nas en mode de configuration radius-server.

Configurez le SSID pour l'authentification 802.1x/EAP

La configuration de l'interface radio et du SSID associé pour 802.1x/EAP implique la configuration de divers paramètres sans fil sur le routeur, notamment le SSID, le mode de cryptage et le type d'authentification. Cet exemple utilise le SSID appelé leap.

1. Activez l'interface radio.

   Afin d'activer l'interface radio, passez en mode de configuration d'interface radio DOT11 et attribuez un SSID à l'interface.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid leap

2. Liez le SSID à un VLAN.

   Afin d'activer le SSID sur cette interface, liez le SSID au VLAN en mode de configuration SSID.

   router<config-ssid>#vlan 2

3. Configurez le SSID avec l'authentification 802.1x/LEAP.

   router<config-ssid>#authentication network-eap eap_methods

4. Configurez l'interface radio pour la gestion dynamique des clés.

   router<config>#encryption mode vlan 2 ciphers wep40

5. Activez le VLAN sur l'interface radio.

   router<config>#interface Dot11Radio 0.2

   router<config-subif>#encapsulation dot1Q 2

   router<config-subif>#bridge-group 2

Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN

Tapez ces commandes en mode de configuration globale pour configurer le serveur DHCP interne pour les clients sans fil de ce VLAN :

- ip dhcp excluded-address 10.2.1.1 10.2.1.5
- ip dhcp pool leapauth

En mode de configuration du pool DHCP, tapez ces commandes :

- réseau 10.2.0.0 255.255.0.0
- default-router 10.2.1.1

Gestion des clés WPA

Wi-Fi Protected Access est une amélioration de la sécurité interopérable basée sur des normes qui augmente fortement le niveau de protection des données et de contrôle d'accès pour les systèmes LAN sans fil actuels et futurs.

Référez-vous à Gestion des clés WPA pour plus d'informations.

La gestion des clés WPA prend en charge deux types de gestion mutuellement exclusifs : WPA-Pre-Shared key (WPA-PSK) et WPA (avec EAP).

Configuration de WPA-PSK

WPA-PSK est utilisé comme type de gestion de clé sur un réseau local sans fil où l'authentification 802.1x n'est pas disponible. Dans de tels réseaux, vous devez configurer une clé pré-partagée sur le point d'accès. Vous pouvez saisir la clé prépartagée sous forme de caractères ASCII ou hexadécimaux. Si vous entrez la clé sous forme de caractères ASCII, vous entrez entre 8 et 63 caractères et le point d'accès développe la clé selon le processus décrit dans la norme de cryptographie par mot de passe (RFC2898). Si vous entrez la clé sous forme de caractères hexadécimaux, vous devez entrer 64 caractères hexadécimaux.

Cet exemple utilise la configuration suivante :

- Nom SSID : wpa-shared
- VLAN 3
- Plage de serveurs DHCP internes : 10.3.0.0/16

Exécutez les actions suivantes sur le routeur :

1. Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
2. Configuration de l'interface virtuelle pontée (BVI)
3. Configuration du SSID pour l'authentification WPA-PSK
4. Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN

Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont

Effectuez les actions suivantes :

1. Activez IRB dans le routeur.

   router<configure>#bridge irb

   Remarque : si tous les types de sécurité doivent être configurés sur un seul routeur, il suffit d'activer IRB une seule fois globalement sur le routeur. Il n'est pas nécessaire de l'activer pour chaque type d'authentification individuel.

2. Définissez un groupe de ponts.

   Cet exemple utilise le groupe de pontage numéro 3.

   router<configure>#bridge 3

3. Sélectionnez le protocole Spanning Tree pour le groupe de pontage.

   Le protocole Spanning Tree IEEE est configuré pour ce groupe de ponts.

   router<configure>#bridge 3 protocol ieee

4. Permettez à une BVI d'accepter et d'acheminer les paquets routables reçus de son groupe de pontage correspondant.

   Cet exemple permet à l'interface BVI d'accepter et d'acheminer des paquets IP.

   router<configure>#bridge 3 route ip

Configuration de l'interface virtuelle pontée (BVI)

Effectuez les actions suivantes :

1. Configurez le BVI.

   Configurez l'interface BVI lorsque vous attribuez le numéro correspondant du groupe de pontage à l'interface BVI. Chaque groupe de pontage ne peut avoir qu'une seule interface BVI correspondante. Cet exemple montre comment affecter le groupe de raccordements numéro 3 à l'interface BVI.

   router<configure>#interface BVI <2>

2. Attribuez une adresse IP à l'interface BVI.

   router<config-if>#ip address 10.3.1.1 255.255.0.0

   router<config-if>#no shut

Configuration du SSID pour l'authentification WPA-PSK

Effectuez les actions suivantes :

1. Activez l'interface radio.

   Afin d'activer l'interface radio, passez en mode de configuration d'interface radio DOT11 et attribuez un SSID à l'interface.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-shared

2. Afin d'activer la gestion de clé WPA, configurez d'abord le chiffrement de cryptage WPA pour l'interface VLAN. Cet exemple utilise tkip comme chiffre de chiffrement..

   Entrez cette commande pour spécifier le type de gestion de clé WPA sur l'interface radio.

   router<config>#interface dot11radio0

   router(config-if)#encryption mode vlan 3 ciphers tkip

3. Liez le SSID à un VLAN.

   Afin d'activer le SSID sur cette interface, liez le SSID au VLAN en mode de configuration SSID.

   router<config-ssid>vlan 3

4. Configurez le SSID avec l'authentification WPA-PSK.

   Vous devez d'abord configurer l'authentification EAP ouverte ou réseau en mode de configuration SSID pour activer la gestion des clés WPA. Cet exemple configure l'authentification ouverte.

router<config>#interface dot11radio0

router<config-if>#ssid wpa-shared

router<config-ssid>#authentication open

Activez maintenant la gestion des clés WPA sur le SSID. Le chiffrement de gestion de clé tkip est déjà configuré pour ce VLAN.

router(config-if-ssid)#authentication key-management wpa

Configurez l'authentification WPA-PSK sur le SSID.

router(config-if-ssid)#wpa-psk ascii 1234567890 ! — 1234567890 est la valeur de clé pré-partagée pour ce SSID. Assurez-vous que la même clé est spécifiée pour ce SSID côté client.

5. Activez le VLAN sur l'interface radio.

   router<config>#interface Dot11Radio 0.3

   router<config-subif>#encapsulation dot1Q 3

   router<config-subif>#bridge-group 3

Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN

Tapez ces commandes en mode de configuration globale pour configurer le serveur DHCP interne pour les clients sans fil de ce VLAN :

- ip dhcp excluded-address 10.3.1.1 10.3.1.5
- ip dhcp pool wpa-psk

En mode de configuration du pool DHCP, tapez ces commandes :

- réseau 10.3.0.0 255.255.0.0
- default-router 10.3.1.1

Configuration de l'authentification WPA (avec EAP)

Il s'agit d'un autre type de gestion de clé WPA. Dans ce cas, les clients et le serveur d'authentification s'authentifient mutuellement à l'aide d'une méthode d'authentification EAP, et le client et le serveur génèrent une clé principale par paire (PMK). Avec WPA, le serveur génère la clé PMK dynamiquement et la transmet au point d'accès, mais avec WPA-PSK, vous configurez une clé pré-partagée à la fois sur le client et sur le point d'accès, et cette clé pré-partagée est utilisée comme clé PMK.

Référez-vous à WPA avec authentification EAP pour plus d'informations.

Cet exemple utilise la configuration suivante :

- Nom SSID : wpa-dot1x
- VLAN 4
- Plage de serveurs DHCP internes : 10.4.0.0/16

Exécutez les actions suivantes sur le routeur :

1. Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
2. Configuration de l'interface virtuelle pontée (BVI)
3. Configurez le serveur RADIUS local pour l'authentification WPA.
4. Configuration du SSID pour WPA avec authentification EAP
5. Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN

Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont

Effectuez les actions suivantes :

1. Activez IRB dans le routeur.

   router<configure>#bridge irb

   Remarque : si tous les types de sécurité doivent être configurés sur un seul routeur, il suffit d'activer IRB une seule fois globalement sur le routeur. Il n'est pas nécessaire de l'activer pour chaque type d'authentification individuel.

2. Définissez un groupe Bridge.

   Cet exemple utilise le groupe de ponts numéro 4.

   router<configure>#bridge 4

3. Sélectionnez le protocole Spanning Tree pour le groupe de pontage.

   Ici, le protocole Spanning Tree IEEE est configuré pour ce groupe de ponts.

   router<configure>#bridge 4 protocol ieee

4. Activez une interface BVI pour accepter et acheminer les paquets routables reçus de son groupe de pontage correspondant.

   Cet exemple permet à l'interface BVI d'accepter et d'acheminer des paquets IP.

   router<configure>#bridge 4 route ip

Configuration de l'interface virtuelle pontée (BVI)

Effectuez les actions suivantes :

1. Configurez le BVI.

   Configurez l'interface BVI lorsque vous attribuez le numéro correspondant du groupe de pontage à l'interface BVI. Chaque groupe de ponts ne peut avoir qu'une seule interface BVI correspondante. Cet exemple attribue le groupe de pontage numéro 4 à la BVI.

   router<configure>#interface BVI <4>

2. Attribuez une adresse IP à l'interface BVI.

   router<config-if>#ip address 10.4.1.1 255.255.0.0

   router<config-if>#no shut

Configurer le serveur RADIUS local pour l'authentification WPA

Référez-vous à la section sous Authentification 802.1x/EAP pour la procédure détaillée.

Configuration du SSID pour WPA avec authentification EAP

Effectuez les actions suivantes :

1. Activez l'interface radio.

   Afin d'activer l'interface radio, passez en mode de configuration d'interface radio DOT11 et attribuez un SSID à l'interface.

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-dot1x

2. Afin d'activer la gestion de clé WPA, configurez d'abord le chiffrement de cryptage WPA pour l'interface VLAN. Cet exemple utilise tkip comme chiffre de chiffrement..

   Entrez cette commande pour spécifier le type de gestion de clé WPA sur l'interface radio.

   router<config>#interface dot11radio0

   router(config-if)#encryption mode vlan 4 ciphers tkip

3. Liez le SSID à un VLAN.

   Afin d'activer le SSID sur cette interface, liez le SSID au VLAN dans le mode de configuration SSID.

vlan 4

4. Configurez le SSID avec l'authentification WPA-PSK.

   Afin de configurer l'interface radio pour WPA avec l'authentification EAP, configurez d'abord le SSID associé pour le réseau EAP.

   router<config>#interface dot11radio0

   router<config-if>#ssid wpa-shared

   router<config-ssid>#authentication réseau eap eap_methods

5. Activez maintenant la gestion des clés WPA sur le SSID. Le chiffrement de gestion de clé tkip est déjà configuré pour ce VLAN.

   router(config-if-ssid)#authentication key-management wpa

6. Activez le VLAN sur l'interface radio.

   router<config>#interface Dot11Radio 0.4

   router<config-subif>#encapsulation dot1Q 4

   router<config-subif>#bridge-group 4

Configurer le serveur DHCP interne pour les clients sans fil de ce VLAN

Tapez ces commandes en mode de configuration globale pour configurer le serveur DHCP interne pour les clients sans fil de ce VLAN :

- ip dhcp excluded-address 10.4.1.1 10.4.1.5
- ip dhcp pool wpa-dot1shared

En mode de configuration du pool DHCP, tapez ces commandes :

- réseau 10.4.0.0 255.255.0.0
- default-router 10.4.1.1

Configuration du client sans fil pour l'authentification

Après avoir configuré le routeur de service intégré, configurez le client sans fil pour différents types d'authentification, comme expliqué, afin que le routeur puisse authentifier ces clients sans fil et fournir l'accès au réseau WLAN. Ce document utilise l'utilitaire Cisco Aironet Desktop Utility (ADU) pour la configuration côté client.

Configuration du client sans fil pour l'authentification ouverte

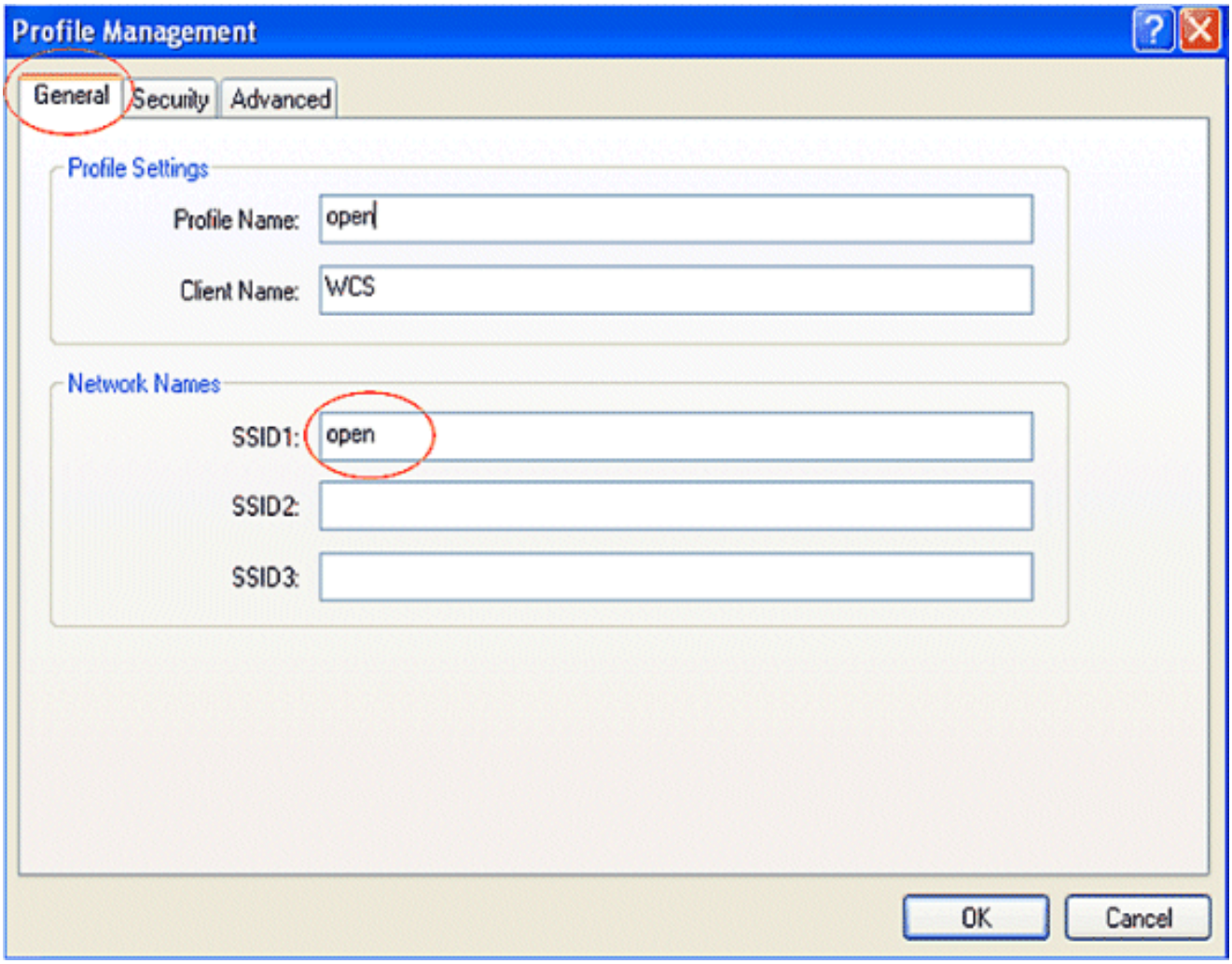
Procédez comme suit :

1. Dans la fenêtre de gestion de profil sur l'ADU, cliquez sur New pour créer un nouveau profil.

   Une nouvelle fenêtre s'affiche dans laquelle vous pouvez définir la configuration de l'authentification ouverte. Sous l'onglet General, entrez le nom du profil et le SSID que l'adaptateur client utilise.

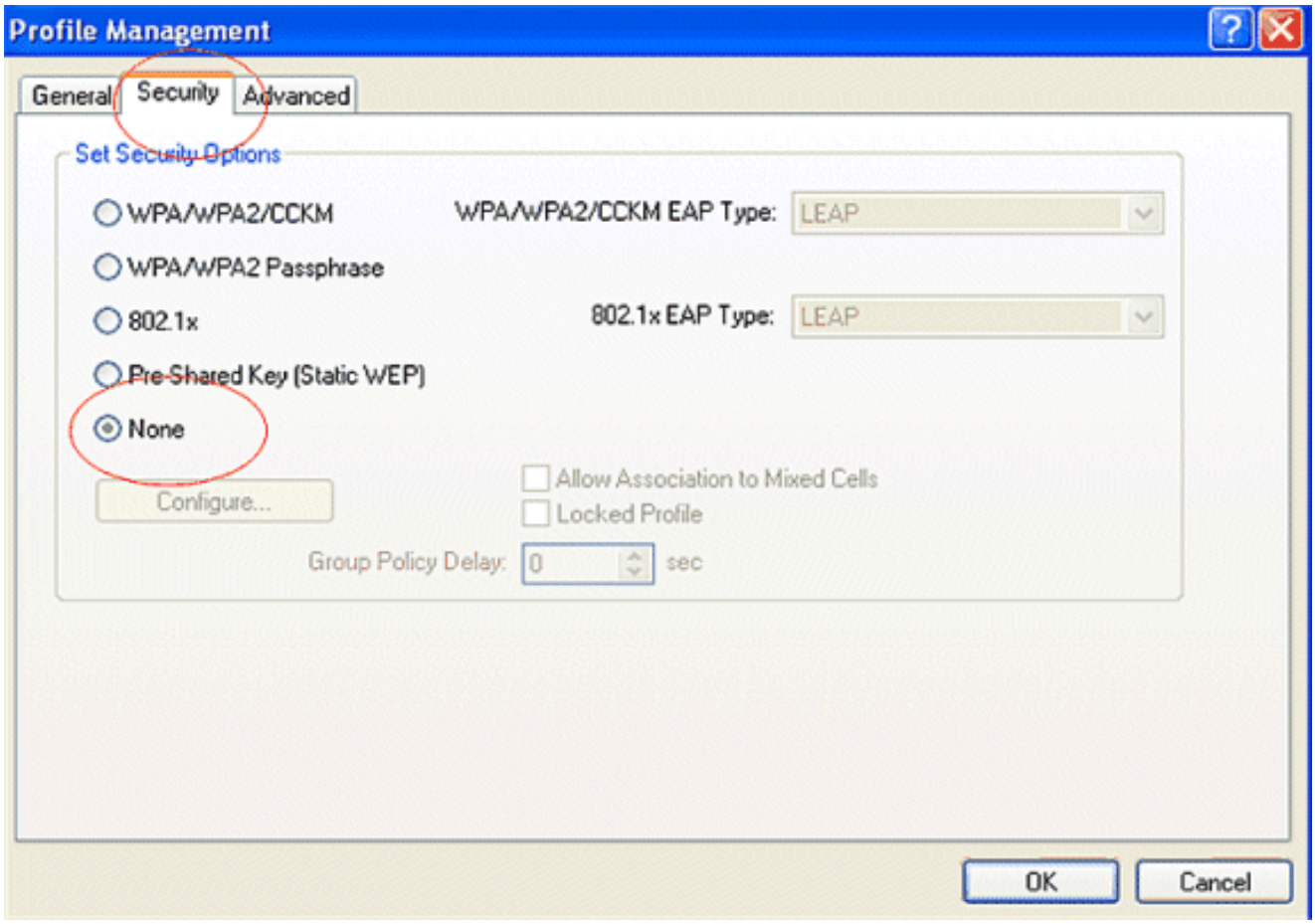
   Dans cet exemple, le nom du profil et le SSID sont ouverts.

   Remarque : le SSID doit correspondre au SSID que vous avez configuré sur l'ISR pour l'authentification ouverte.

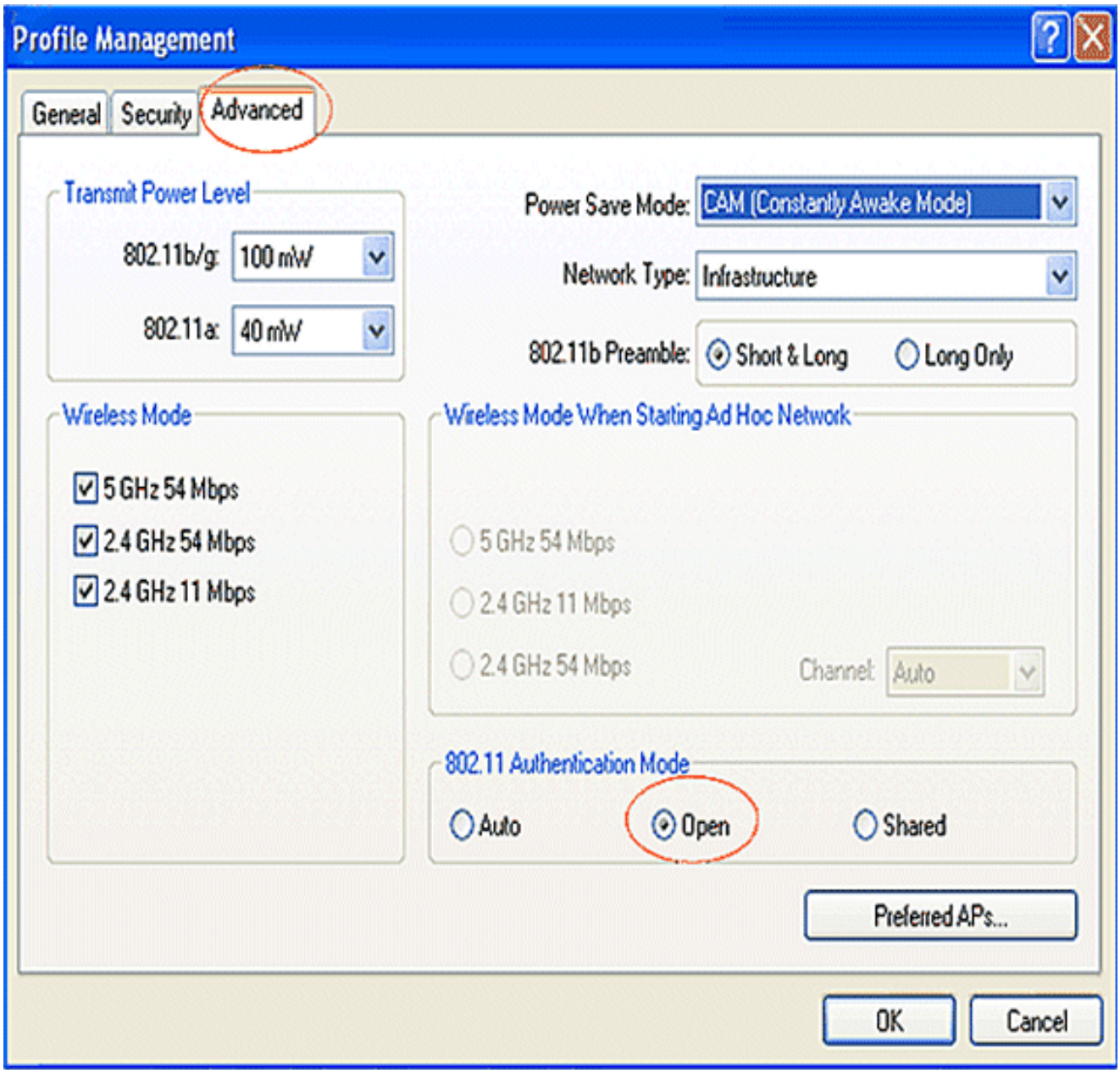


2. Cliquez sur l'onglet Security et conservez l'option de sécurité None pour le cryptage WEP. Comme cet exemple utilise le protocole WEP comme option, l'attribution de la valeur None à cette option permettra au client de s'associer et de communiquer avec le réseau WLAN.

   Click OK

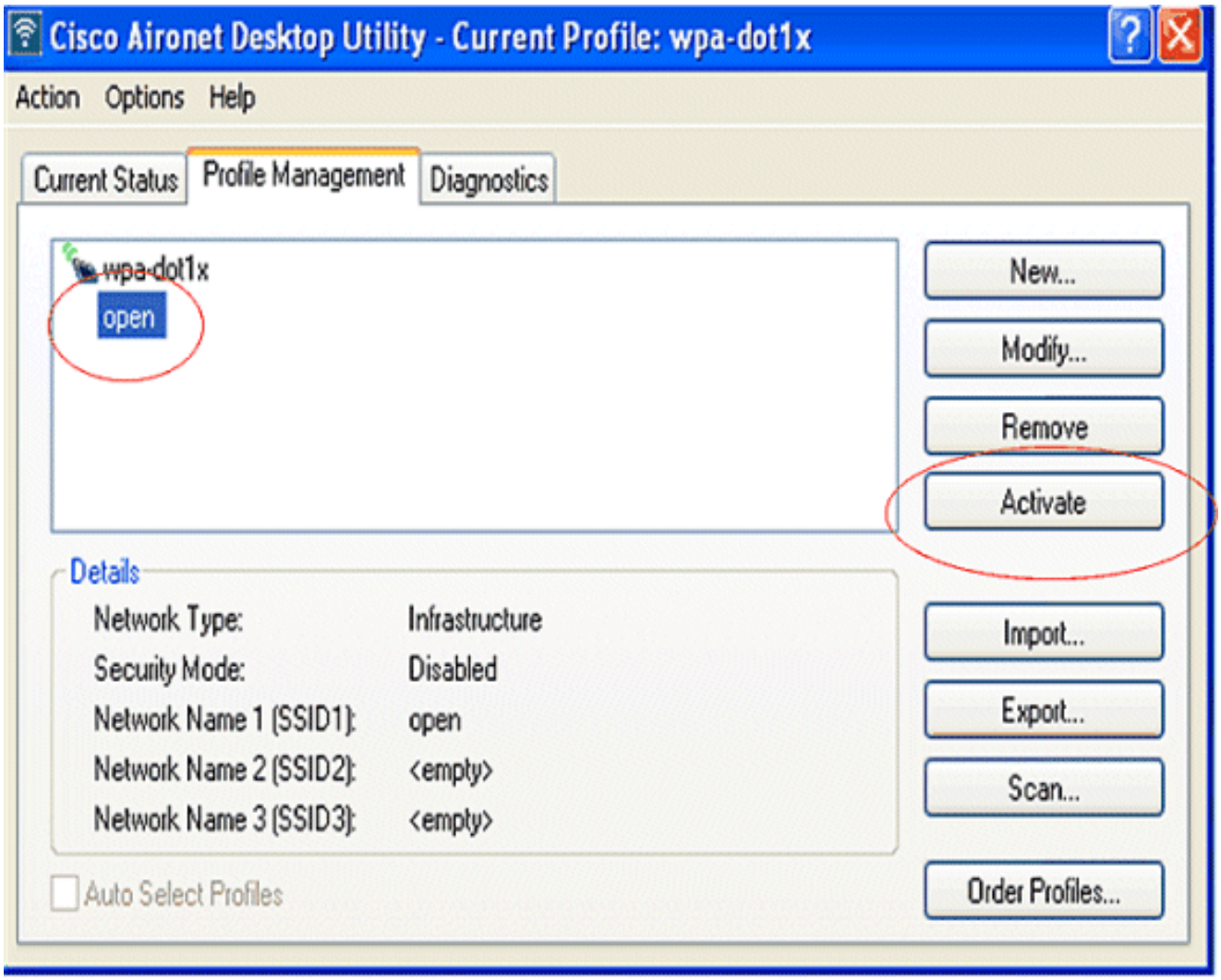


3. Sélectionnez Advanced window dans l'onglet Profile Management et définissez le mode d'authentification 802.11 sur Open pour l'authentification ouverte.

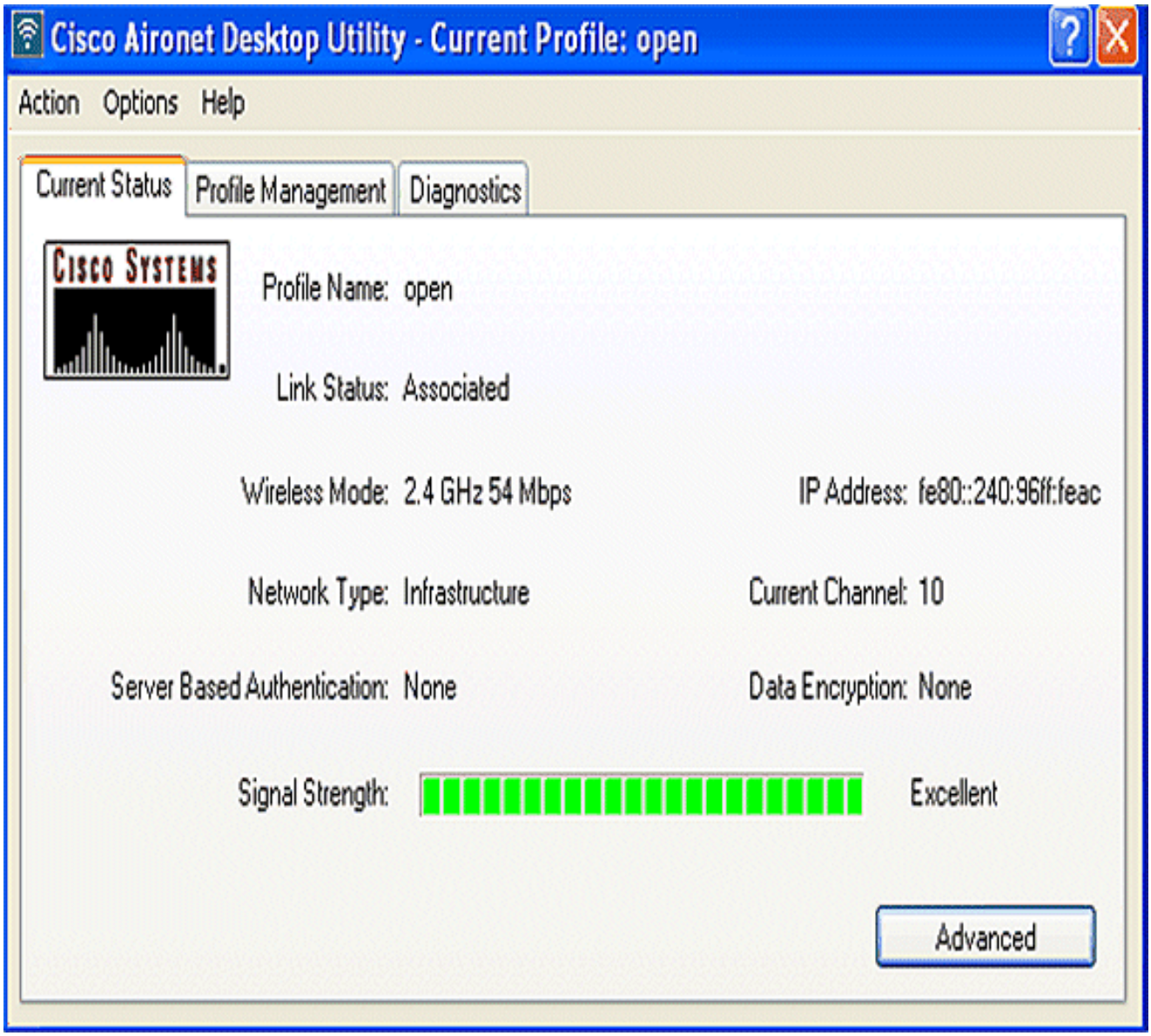


Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

1. Une fois le profil client créé, cliquez sur Activate sous l'onglet Profile Management pour activer le profil.



2. Vérifiez l'état ADU pour une authentification réussie.



Configuration du client sans fil pour l'authentification 802.1x/EAP

Procédez comme suit :

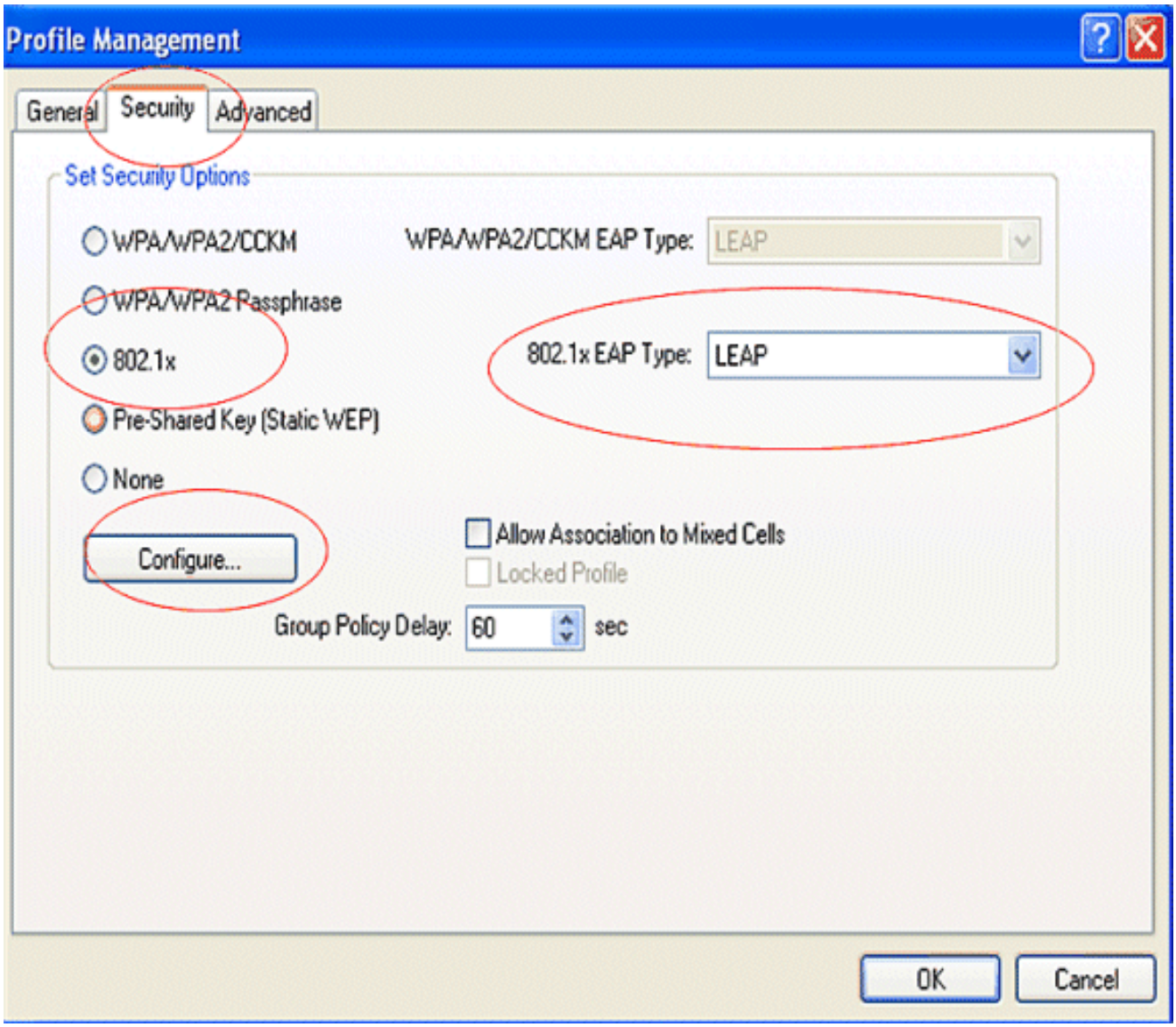
1. Dans la fenêtre de gestion de profil sur l'ADU, cliquez sur New pour créer un nouveau profil.

   Une nouvelle fenêtre s'affiche dans laquelle vous pouvez définir la configuration de l'authentification ouverte. Sous l'onglet General, entrez le nom du profil et le SSID que l'adaptateur client utilise.

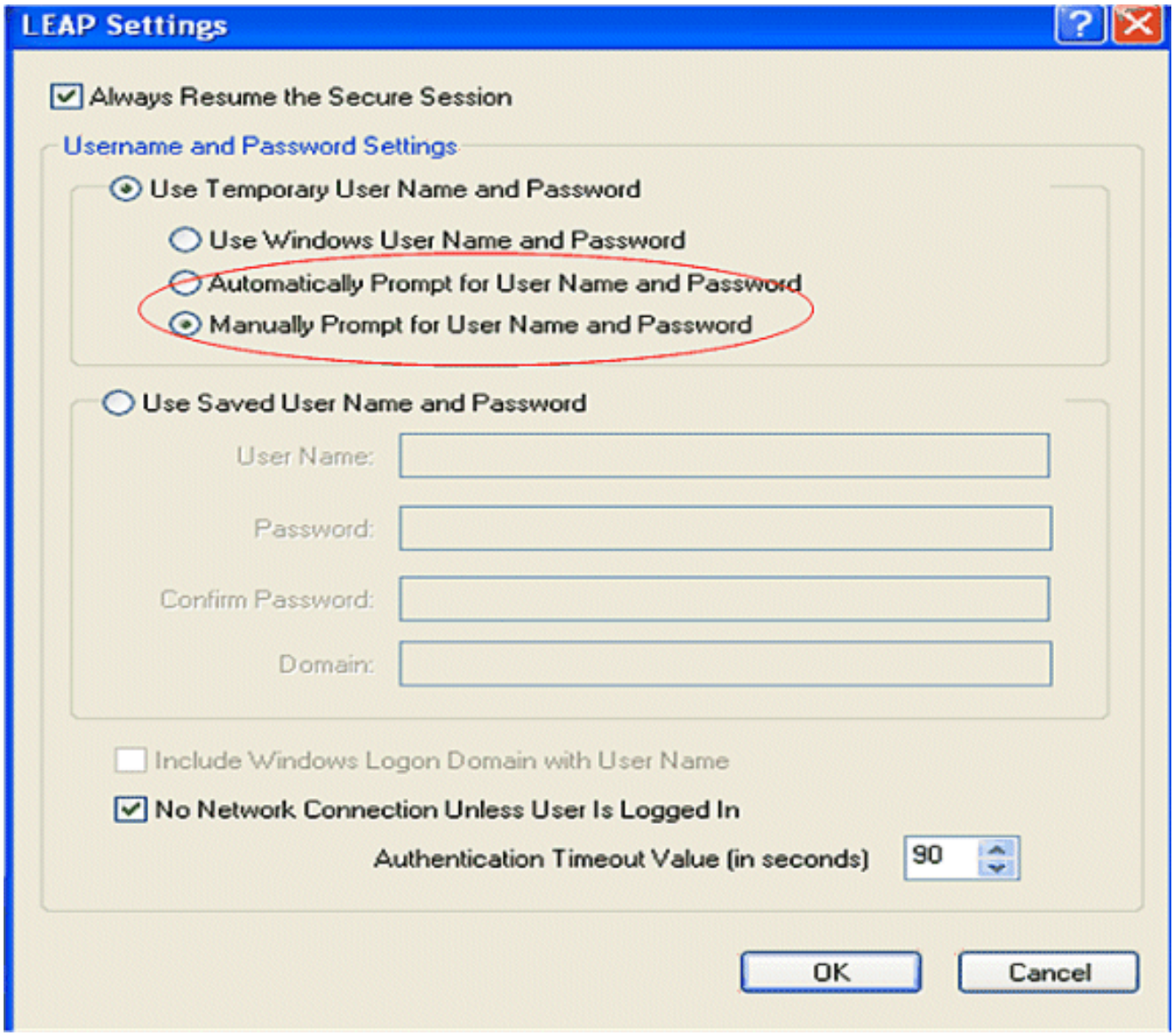
   Dans cet exemple, le nom du profil et le SSID sont bissextiles.

2. Sous Profile Management, cliquez sur l'onglet Security, définissez l'option de sécurité sur 802.1x et choisissez le type EAP approprié. Ce document utilise LEAP comme type d'EAP pour l'authentification. Cliquez à présent sur Configure pour configurer les paramètres de nom d'utilisateur et de mot de passe LEAP.

   Remarque : Remarque : le SSID doit correspondre au SSID que vous avez configuré sur l'ISR pour l'authentification 802.1x/EAP.

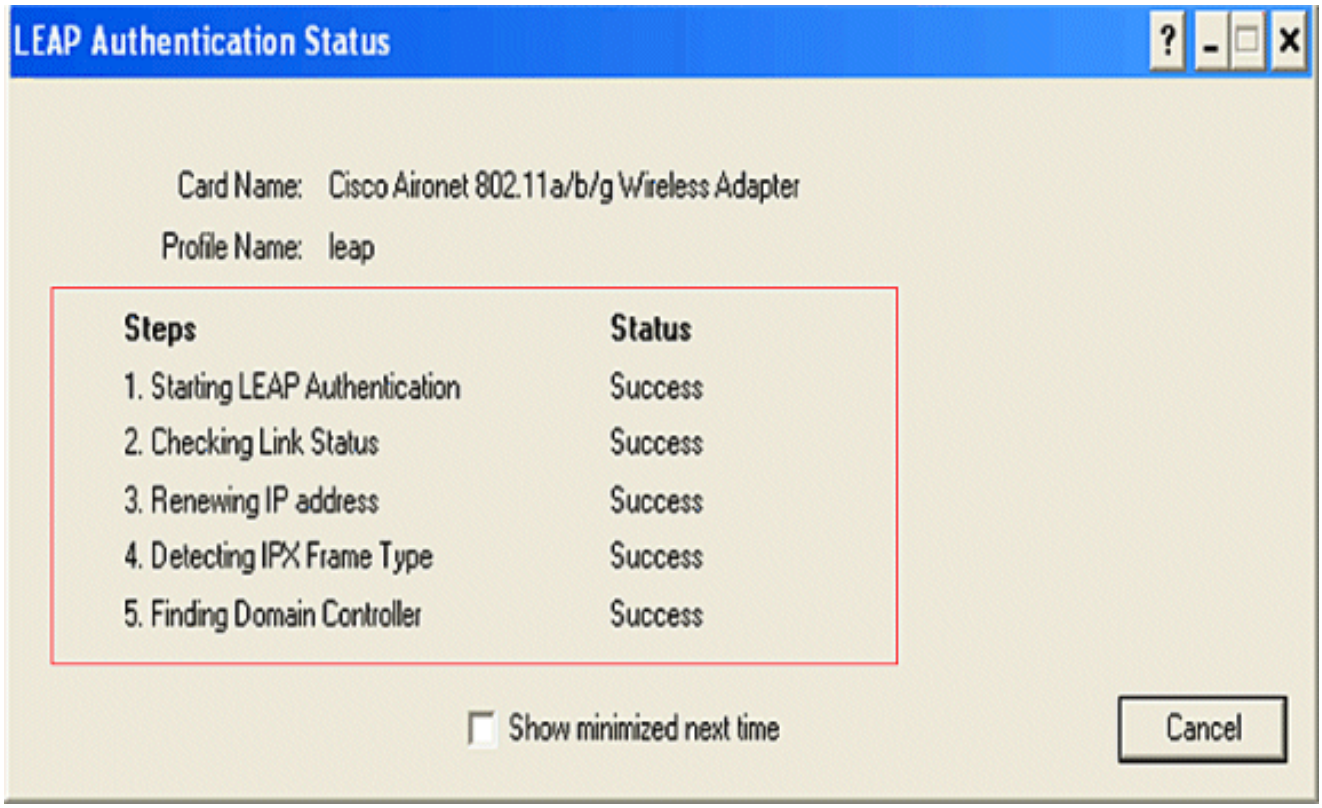


3. Dans les paramètres de nom d'utilisateur et de mot de passe, cet exemple choisit de demander manuellement le nom d'utilisateur et le mot de passe afin que le client soit invité à entrer le nom d'utilisateur et le mot de passe corrects pendant que le client tente de se connecter au réseau. Click OK.



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

- Une fois le profil client créé, cliquez sur Activate sous l'onglet Profile Management pour activer le saut de profil. Vous êtes invité à saisir le nom d'utilisateur et le mot de passe saut. Cet exemple utilise le nom d'utilisateur et le mot de passe user1. Click OK.
- Vous pouvez voir le client s'authentifier correctement et se voir attribuer une adresse IP à partir du serveur DHCP configuré sur le routeur.



Configuration du client sans fil pour l'authentification WPA-PSK

Procédez comme suit :

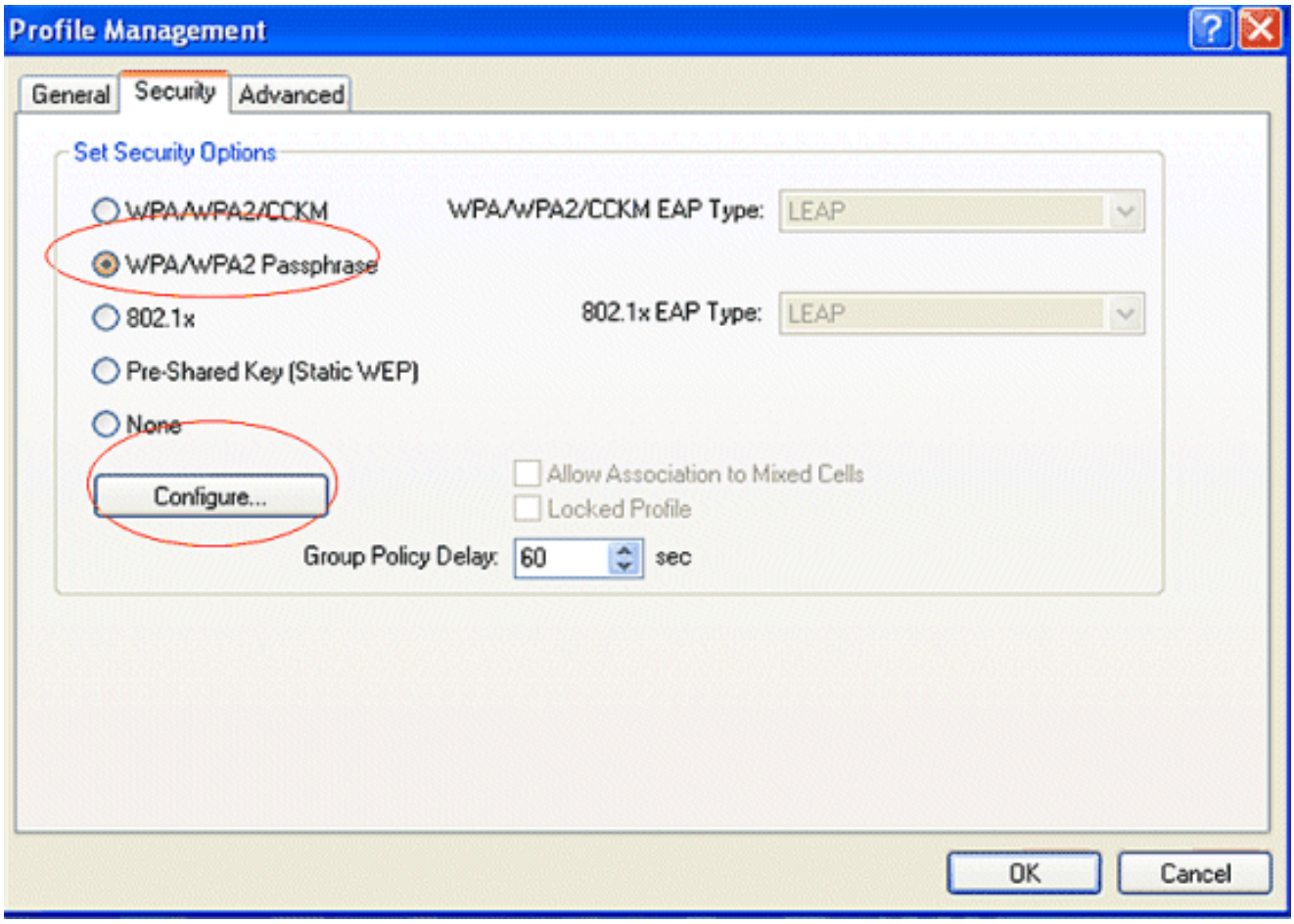
1. Dans la fenêtre de gestion de profil sur l'ADU, cliquez sur New pour créer un nouveau profil.

   Une nouvelle fenêtre s'affiche dans laquelle vous pouvez définir la configuration de l'authentification ouverte. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilise.

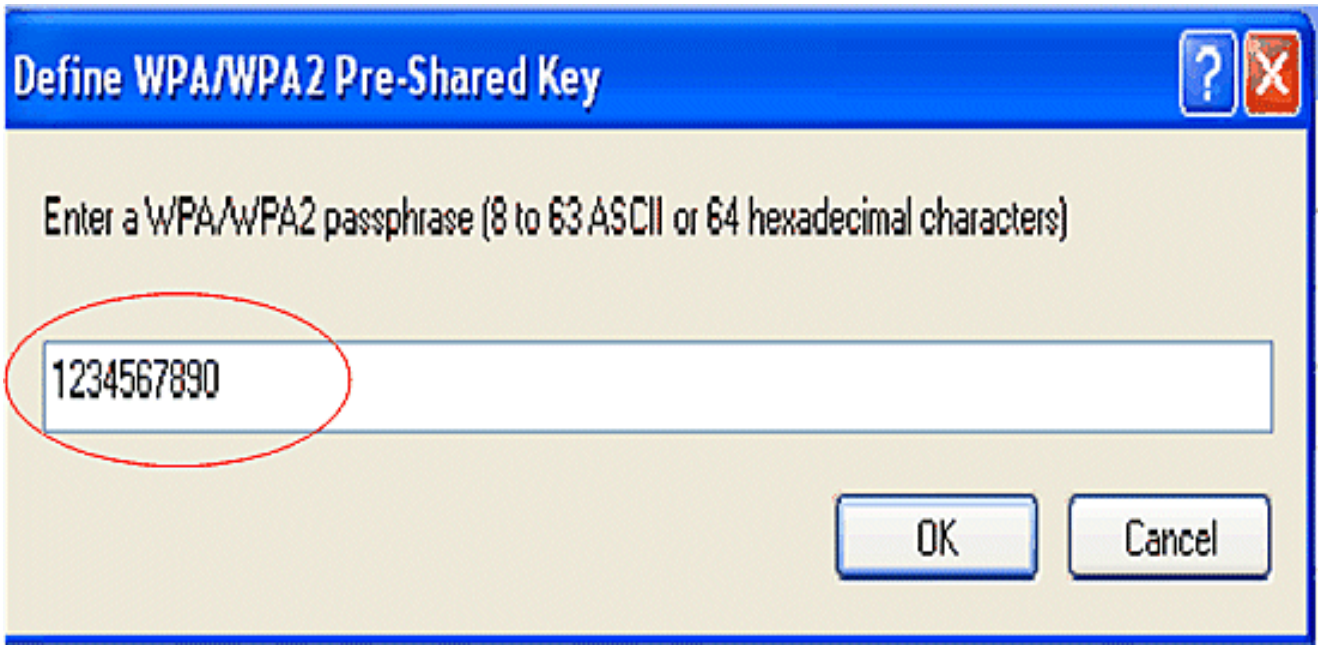
   Dans cet exemple, le nom de profil et le SSID sont wpa-shared.

   Remarque : le SSID doit correspondre au SSID que vous avez configuré sur l'ISR pour l'authentification WPA-PSK.

2. Sous Profile Management, cliquez sur l'onglet Security et définissez l'option de sécurité sur WPA/WPA2 Passphrase. Cliquez à présent sur Configure pour configurer la phrase de passe WPA.



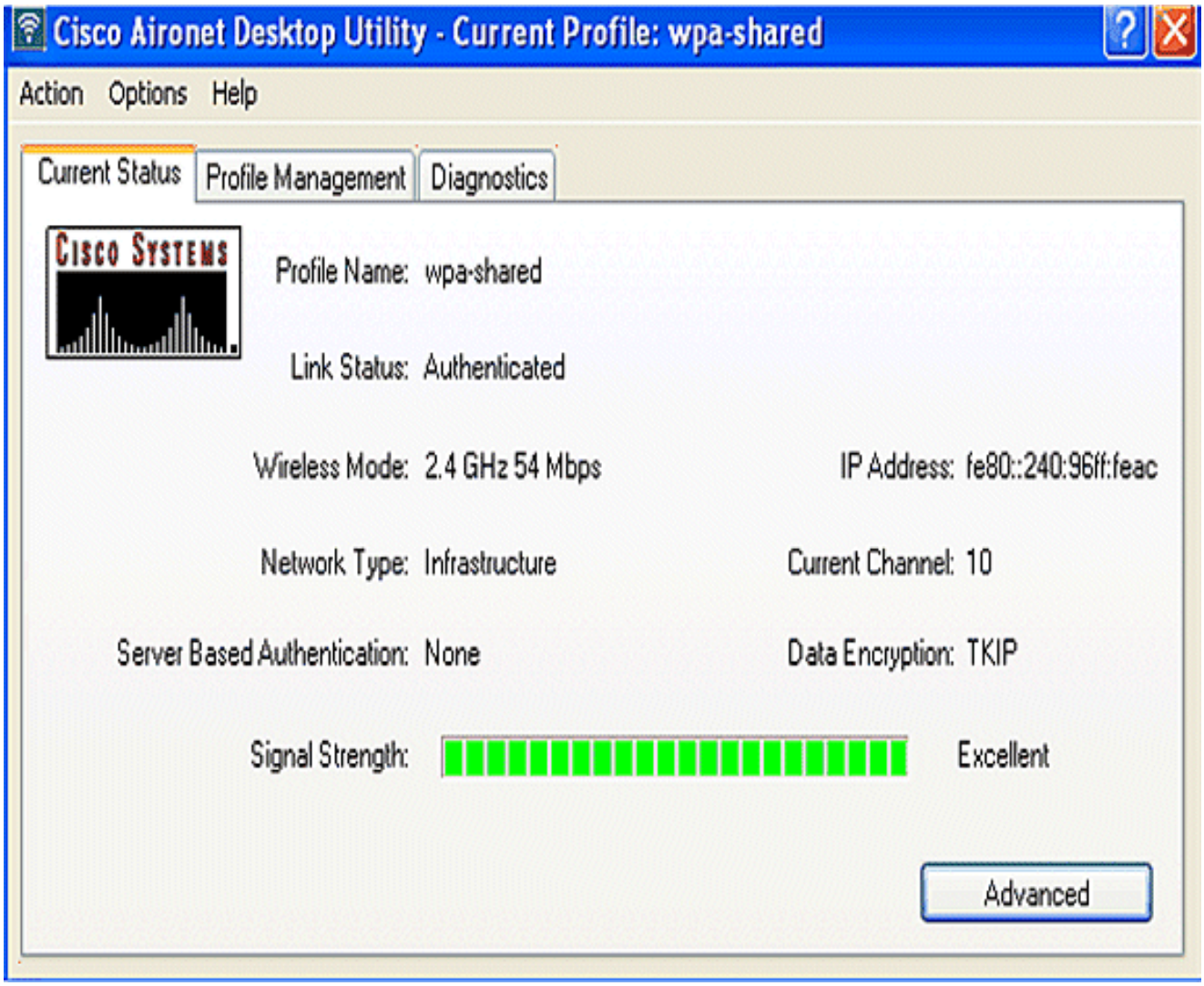
3. Définissez une clé prépartagée WPA. La clé doit comporter entre 8 et 63 caractères ASCII. Click OK.



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

- Une fois le profil client créé, cliquez sur Activate sous l'onglet Profile Management pour activer le profil wpa-shared.

- Vérifiez l'ADU pour une authentification réussie.



Configuration du client sans fil pour l'authentification WPA (avec EAP)

Procédez comme suit :

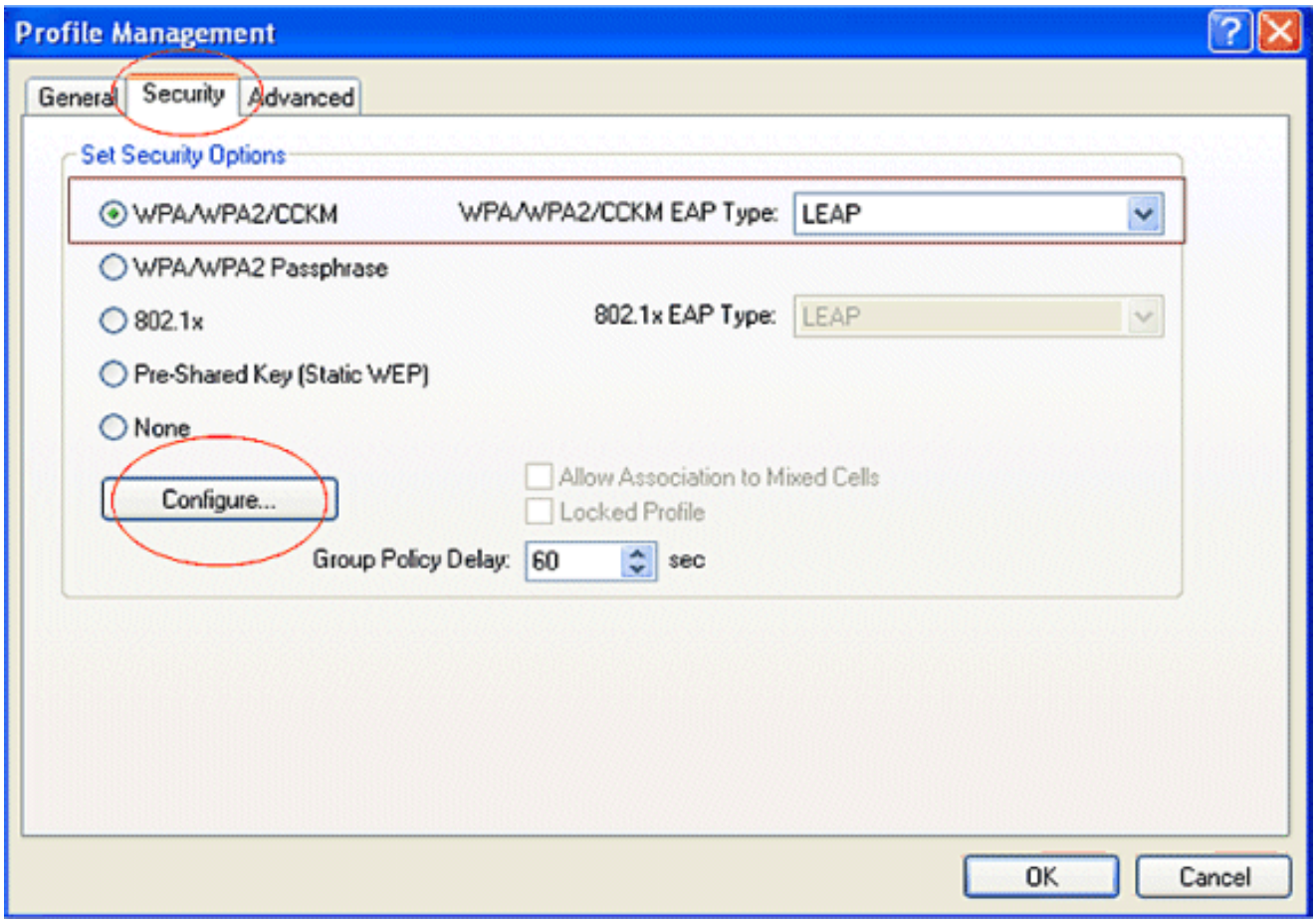
1. Dans la fenêtre de gestion de profil sur l'ADU, cliquez sur New pour créer un nouveau profil.

   Une nouvelle fenêtre s'affiche dans laquelle vous pouvez définir la configuration de l'authentification ouverte. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilise.

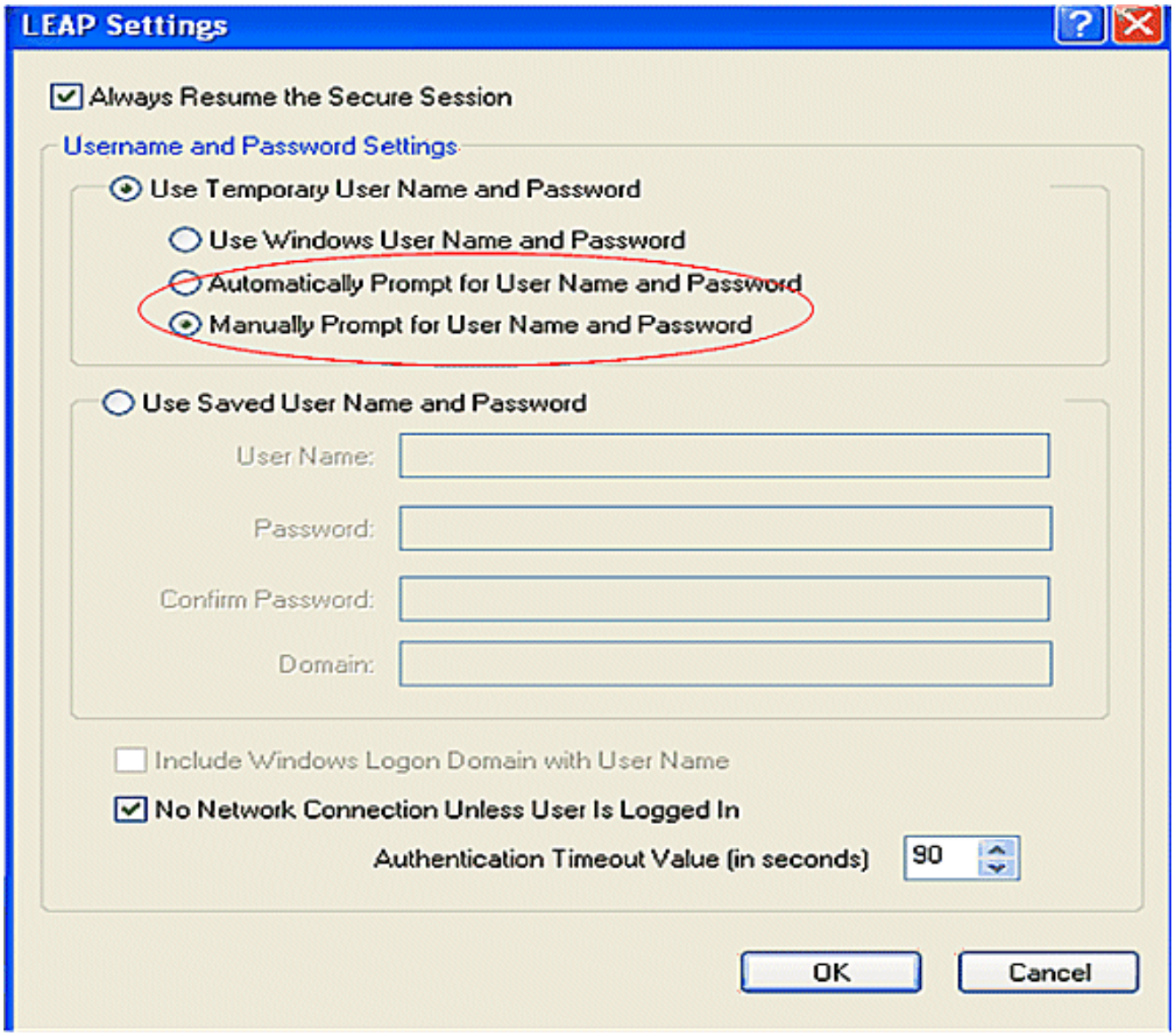
   Dans cet exemple, le nom de profil et le SSID sont wpa-dot1x.

   Remarque : le SSID doit correspondre au SSID que vous avez configuré sur l'ISR pour l'authentification WPA (avec EAP).

2. Sous Profile Management, cliquez sur l'onglet Security, définissez l'option de sécurité sur WPA/WPA2/CCKM, puis sélectionnez le type EAP WPA/WPA2/CCKM approprié. Ce document utilise LEAP comme type d'EAP pour l'authentification. Cliquez à présent sur Configure pour configurer les paramètres de nom d'utilisateur et de mot de passe LEAP.

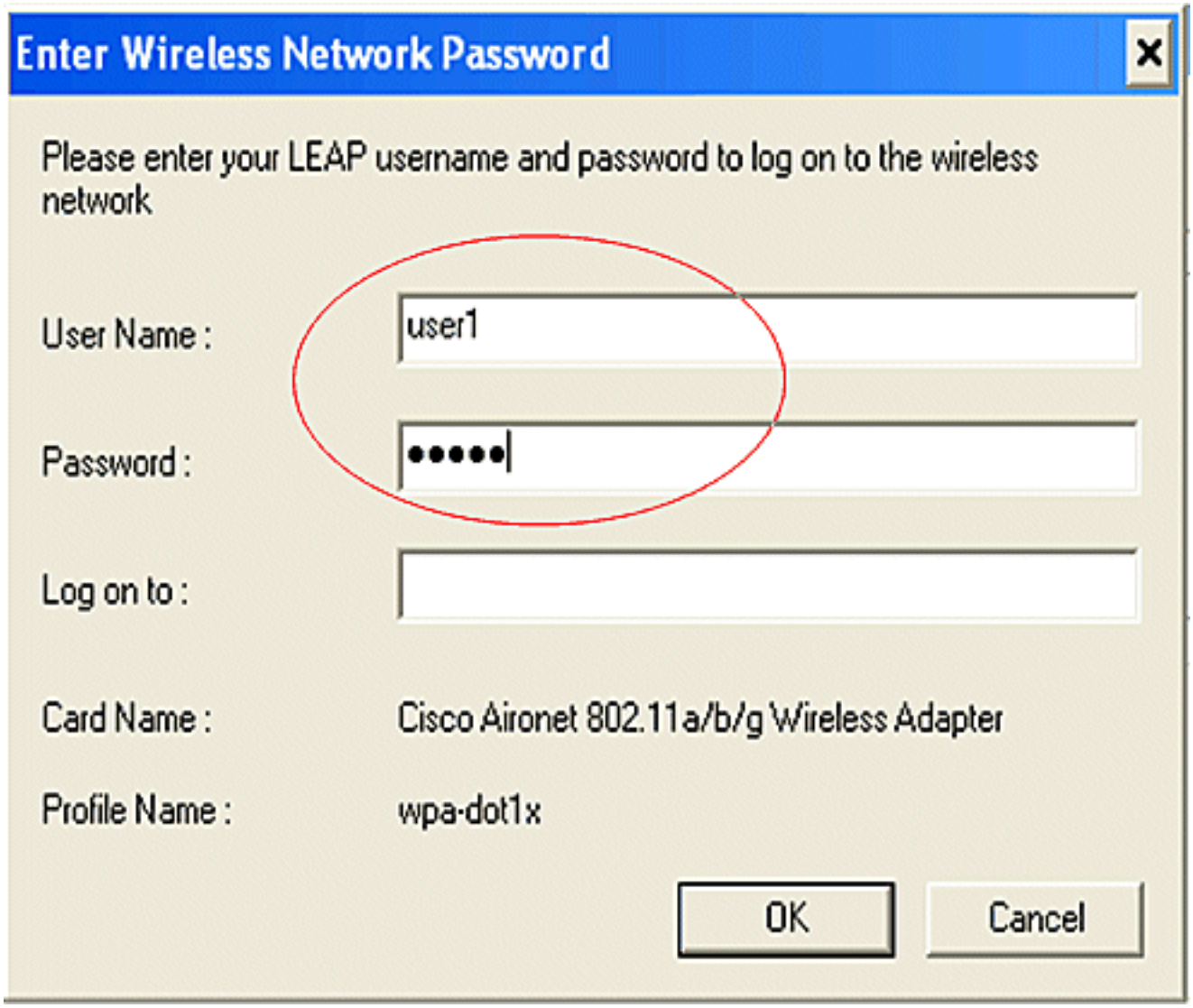


3. Dans la zone Paramètres de nom d'utilisateur et de mot de passe, cet exemple choisit de demander manuellement le nom d'utilisateur et le mot de passe afin que le client soit invité à entrer le nom d'utilisateur et le mot de passe corrects lorsque le client tente de se connecter au réseau. Click OK.

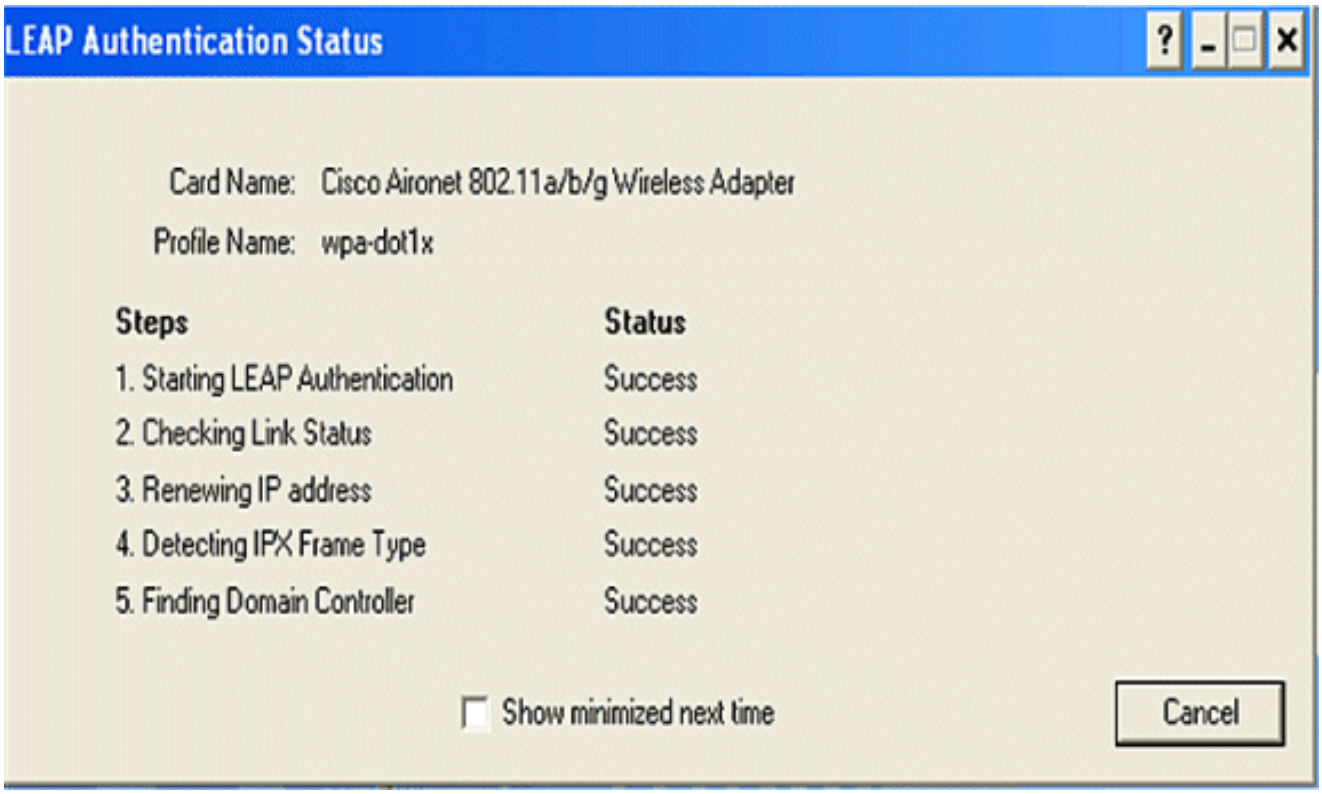


Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

1. Une fois le profil client créé, cliquez sur Activate sous l'onglet Profile Management pour activer le profil wpa-dot1x. Vous êtes invité à saisir le nom d'utilisateur et le mot de passe LEAP. Cet exemple utilise le nom d'utilisateur et le mot de passe user1. Click OK.



2. Vous pouvez voir le client s'authentifier correctement.



La commande show dot11 associations de l'interface de ligne de commande du routeur affiche des détails complets sur l'état de l'association du client. Voici un exemple.

Routeur#show dot11 associations

<#root>

```
802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 10.3.0.2        CB21AG/PI21AG WCS             self         EAP-Assoc


SSID [open] :

SSID [pre-shared] : DISABLED, not associated with a configured VLAN

SSID [wpa-dot1x] :

SSID [wpa-shared] :


Others:  (not related to any ssid)
```

Dépannage

Dépannage des commandes

Vous pouvez utiliser ces commandes debug pour dépanner votre configuration.

- debug dot11 aaa authenticator all : active le débogage des paquets d'authentification MAC et EAP.
- debug radius authentication : affiche les négociations RADIUS entre le serveur et le client.
- debug radius local-server packets : affiche le contenu des paquets RADIUS envoyés et reçus.
- debug radius local-server client : affiche des messages d'erreur sur les échecs d'authentification client.

Informations connexes

- Exemples de configuration de l'authentification sur des contrôleurs de réseau local sans fil
- Configuration des VLAN sur les points d'accès
- Exemple de configuration d'un routeur sans fil ISR 1800 avec DHCP interne et authentification ouverte
- Guide de configuration des points d'accès Cisco Wireless ISR et HWIC
- Exemple de configuration de la connectivité LAN sans fil à l'aide d'un ISR avec chiffrement WEP et authentification LEAP
- Assistance et documentation techniques - Cisco Systems
- Configuration des types d'authentification
- Exemple de configuration de la connectivité LAN sans fil à l'aide d'un ISR avec chiffrement WEP et authentification LEAP

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.