Exemple de configuration de la connectivité LAN sans fil à l'aide d'un ISR avec chiffrement WEP et authentification LEAP

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Diagramme du réseau
Conventions
Configuration du routeur 871W
Configuration de l'adaptateur client
Vérification
Dépannage
Informations connexes

Introduction

Ce document explique comment configurer un routeur à services intégrés (ISR) de la gamme Cisco 870 pour la connectivité LAN sans fil avec cryptage WEP et authentification LEAP.

La même configuration s'applique à tous les autres modèles de la gamme Cisco ISR Wireless.

Conditions préalables

Conditions requises

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

- Connaissance des paramètres de base du routeur de service intégré de la gamme Cisco 870.
- Connaissance de la configuration de l'adaptateur client sans fil 802.11a/b/g à l'aide de l'utilitaire de bureau Aironet (ADU).

Reportez-vous au Guide d'installation et de configuration des adaptateurs client LAN sans fil Cisco Aironet 802.11a/b/g (CB21AG et PI21AG), version 2.5 pour plus d'informations sur la configuration de l'adaptateur client 802.11a/b/g.

Components Used

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

logiciel suivantes :

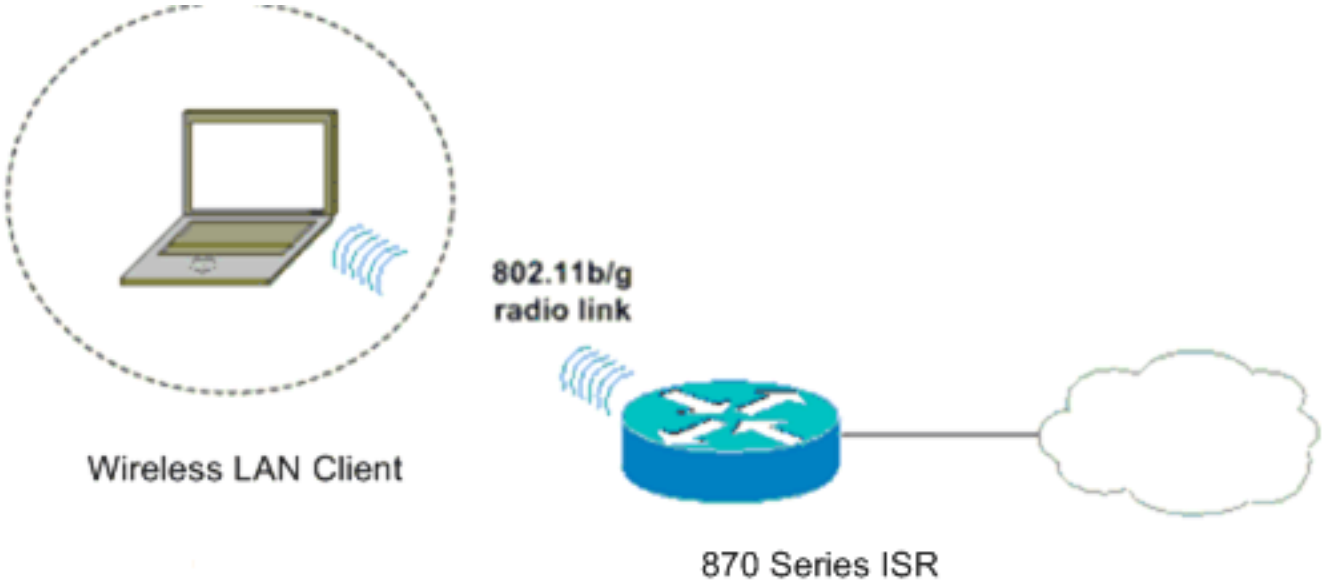
- Cisco 871W ISR qui exécute le logiciel Cisco IOS® version 12.3(8)YI1
- Ordinateur portable avec Aironet Desktop Utility version 2.5
- Adaptateur client 802.11 a/b/g qui exécute le microprogramme version 2.5

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.

Diagramme du réseau

Ce document utilise cette configuration du réseau.

Dans cette configuration, le client LAN sans fil est associé au routeur 870. Le serveur DHCP (Dynamic Host Configuration Protocol) interne du routeur 870 est utilisé pour fournir une adresse IP aux clients sans fil. Le cryptage WEP est activé sur le routeur de service intégré 870 et le client WLAN. L'authentification LEAP est utilisée pour authentifier les utilisateurs sans fil et la fonctionnalité de serveur RADIUS local sur le routeur 870 est utilisée pour valider les informations d'identification.



Conventions

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

Configuration du routeur 871W

Complétez ces étapes pour configurer le routeur de service intégré 871W en tant que point d'accès pour accepter les demandes d'association des clients sans fil.

1. Configurez l'IRB (Integrated Routing and Bridging) et configurez le groupe de pontage.Tapez ces commandes en mode de configuration globale afin d'activer IRB.

```
WirelessRouter<config>#bridge irb
!--- Enables IRB. WirelessRouter<config>#bridge 1 protocol ieee  !--- Defines the type of
Spanning Tree Protocol as ieee. WirelessRouter<config>#bridge 1 route ip
!--- Enables the routing of the specified protocol in a bridge group.
```

2. Configurez l'interface virtuelle pontée (BVI).Attribuez une adresse IP à l'interface BVI. Tapez ces commandes en mode de configuration globale.

```
WirelessRouter<config>#interface bvi1
!--- Enter interface configuration mode for the BVI. WirelessRouter<config-if>#ip address
172.16.1.100 255.255.0.0
```

   Référez-vous à la section *Configuration du groupe de ponts sur les points d'accès et les ponts de* l'utilisation de VLAN avec l'équipement sans fil Cisco Aironet pour plus d'informations sur la fonctionnalité des groupes de ponts dans les points d'accès.
3. Configurez la fonction de serveur DHCP interne sur le routeur de service intégré 871W.La fonction de serveur DHCP interne du routeur peut être utilisée pour attribuer des adresses IP aux clients sans fil qui s'associent au routeur. Exécutez ces commandes en mode de configuration globale.

```
WirelessRouter<config>#ip dhcp excluded-address 172.16.1.100 172.16.1.100
!--- Excludes IP addresses from the DHCP pool. !--- This address is used on the BVI
interface, so it is excluded. WirelessRouter<config>#ip dhcp pool 870-ISR
WirelessRouter<dhcp-config>#network 172.16.1.0 255.255.0.0
```

   Remarque : La carte client doit également être configurée pour accepter les adresses IP d'un serveur DHCP.
4. Configurez le routeur de service intégré 871W en tant que serveur RADIUS local.En mode de configuration globale, tapez ces commandes pour configurer le routeur de service intégré 871W en tant que serveur RADIUS local.

```
WirelessRouter<config>#aaa new-model
!--- Enable the authentication, authorization, and accounting !--- (AAA) access control
model. WirelessRouter<config>#radius-server local
!--- Enables the 871 wireless-aware router as a local !--- authentication server and enters
into configuration !--- mode for the authenticator. WirelessRouter<config-radsrv)#nas
172.16.1.100 key Cisco
!--- Adds the 871 router to the list of devices that use !--- the local authentication
server. WirelessRouter<config-radsrv>#user ABCD password ABCD
WirelessRouter<config-radsrv)#user XYZ password XYZ
!--- Configure two users ABCD and XYZ on the local RADIUS server. WirelessRouter<config-
radsrv)#exit
WirelessRouter<config>#radius-server host 172.16.1.100 auth-port 1812 acct-port 1813 key
Cisco
!--- Specifies the RADIUS server host.
```

   Remarque : utilisez les ports 1812 et 1813 pour l'authentification et la comptabilité du serveur RADIUS local.

```
WirelessRouter<config>#aaa group server radius rad_eap
!--- Maps the RADIUS server to the group rad_eap
.
WirelessRouter<config-sg-radius>#server 172.16.1.100 auth-port 1812 acct-port 1813
!--- Define the server that falls in the group rad_eap. WirelessRouter<config>#aaa
authentication login eap_methods group rad_eap
!--- Enable AAA login authentication.
```

5. Configurer l'interface radio.La configuration de l'interface radio implique la configuration de différents paramètres sans fil sur le routeur, notamment le SSID, le mode de chiffrement, le type d'authentification, la vitesse et le rôle du routeur sans fil. Cet exemple utilise le SSID appelé **Test**.Tapez ces commandes pour configurer l'interface radio en mode de

configuration globale.

```
WirelessRouter<config>#interface dot11radio0
!--- Enter radio interface configuration mode. WirelessRouter<config-if>#ssid Test
!--- Configure an SSID test. irelessRouter<config-ssid>#authentication open eap eap_methods
WirelessRouter<config-ssid>#authentication network-eap eap_methods
!--- Expect that users who attach to SSID 'Test' !--- are requesting authentication with
the type 128 !--- Network Extensible Authentication Protocol (EAP) !--- authentication bit
set in the headers of those requests. !--- Group these users into a group called
'eap_methods'. WirelessRouter<config-ssid>#exit
!--- Exit interface configuration mode. WirelessRouter<config-if>#encryption mode wep
mandatory
!--- Enable WEP encryption. WirelessRouter<config-if>#encryption key 1 size 128
1234567890ABCDEF1234567890
!--- Define the 128-bit WEP encryption key. WirelessRouter<config-if>#bridge-group 1
WirelessRouter<config-if>#no shut
!--- Enables the radio interface.
```

Le routeur 870 accepte les demandes d'association des clients sans fil une fois cette procédure effectuée.Lorsque vous configurez le type d'authentification EAP sur le routeur, il est recommandé de choisir **Network-EAP et Open with EAP** comme types d'authentification afin d'éviter tout problème d'authentification.

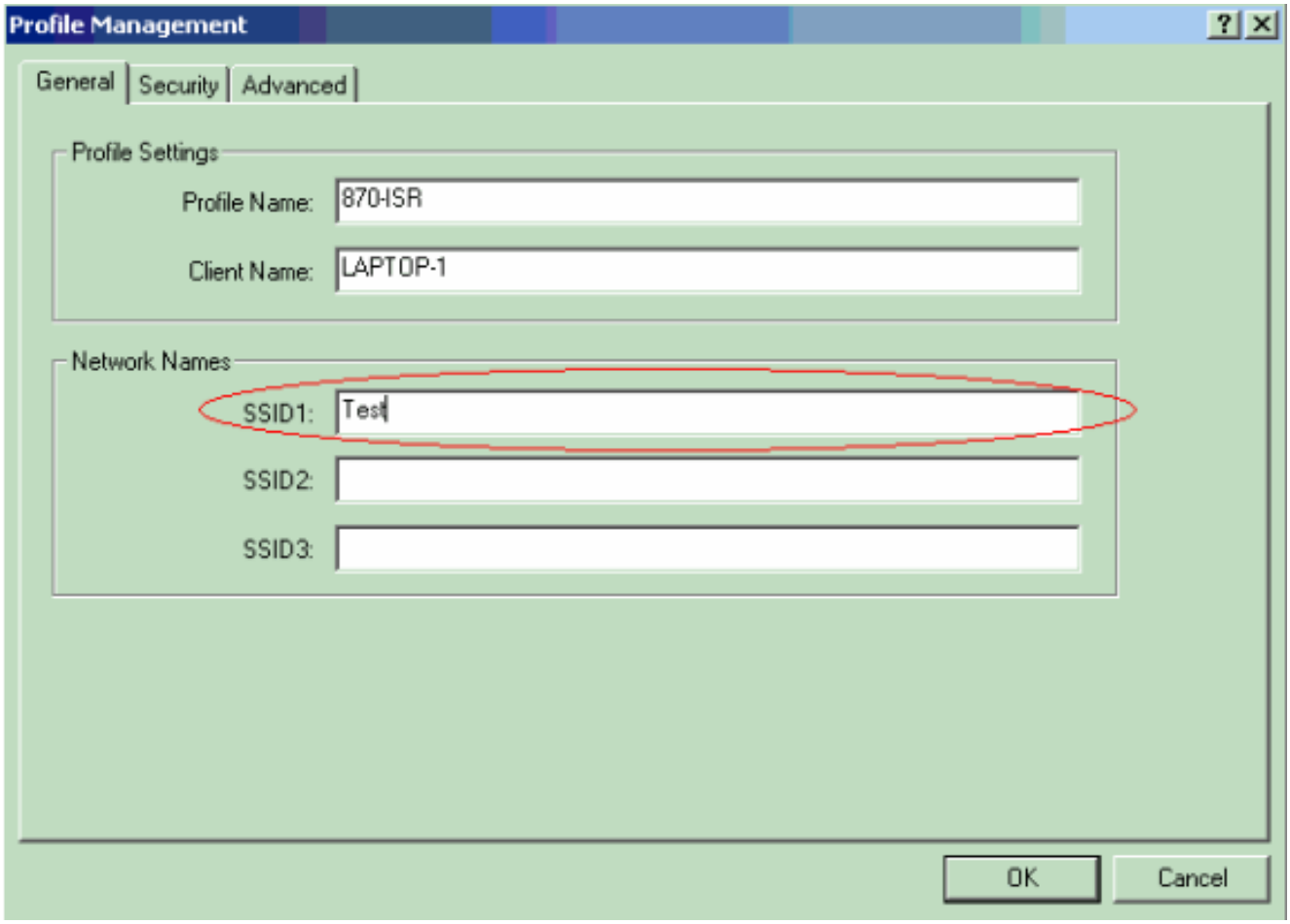
```
WirelessRouter<config-ssid>#authentication network-eap eap_methods
WirelessRouter<config-ssid>#authentication open eap eap_methods
```

Remarque : Ce document suppose que le réseau ne possède que des clients sans fil Cisco.**Remarque :** Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

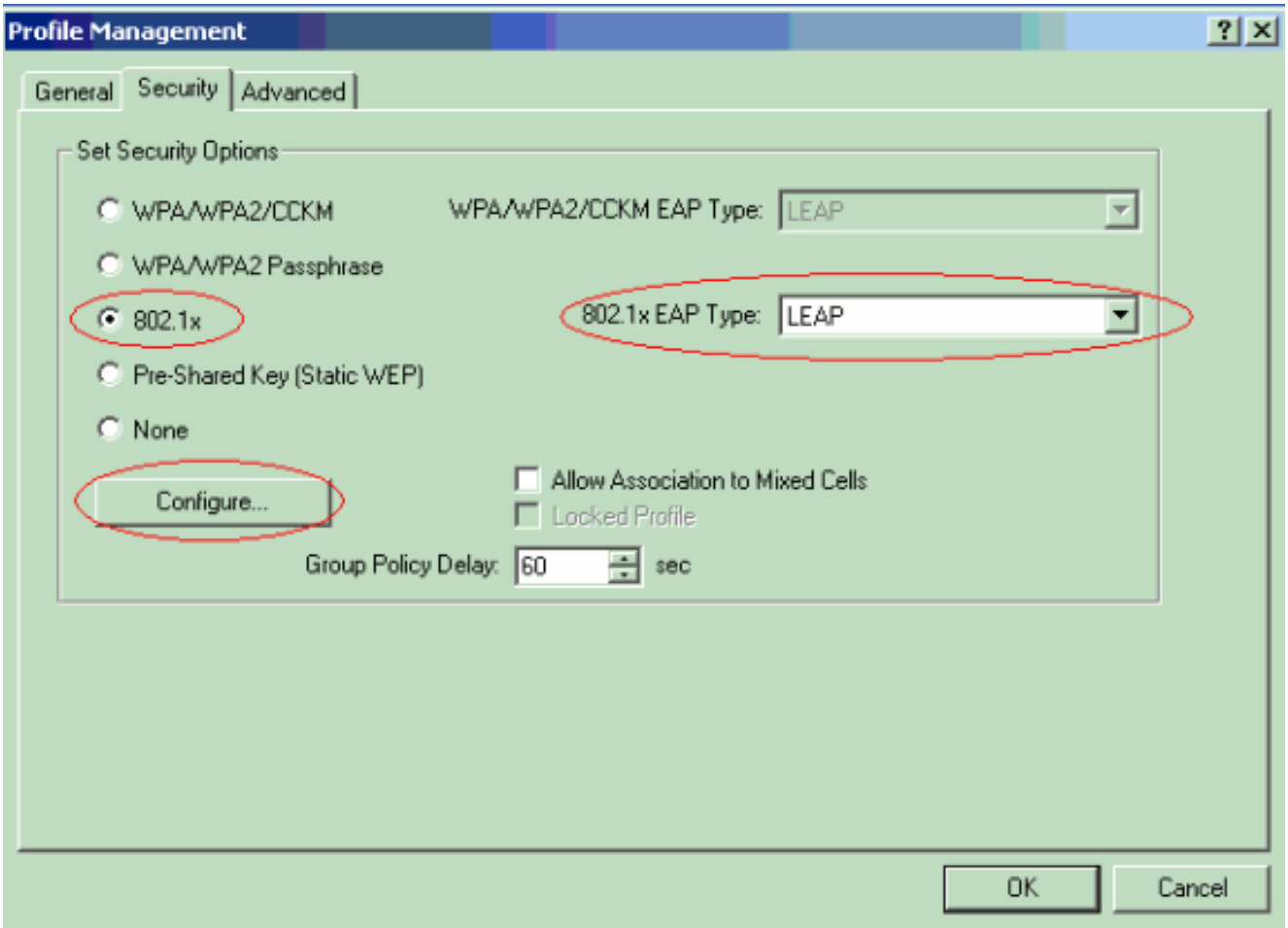
Configuration de l'adaptateur client

Complétez ces étapes afin de configurer l'adaptateur client. Cette procédure crée un nouveau profil appelé **870-ISR** sur l'ADU, par exemple. Cette procédure utilise également Test comme SSID et active l'authentification LEAP sur l'adaptateur client.

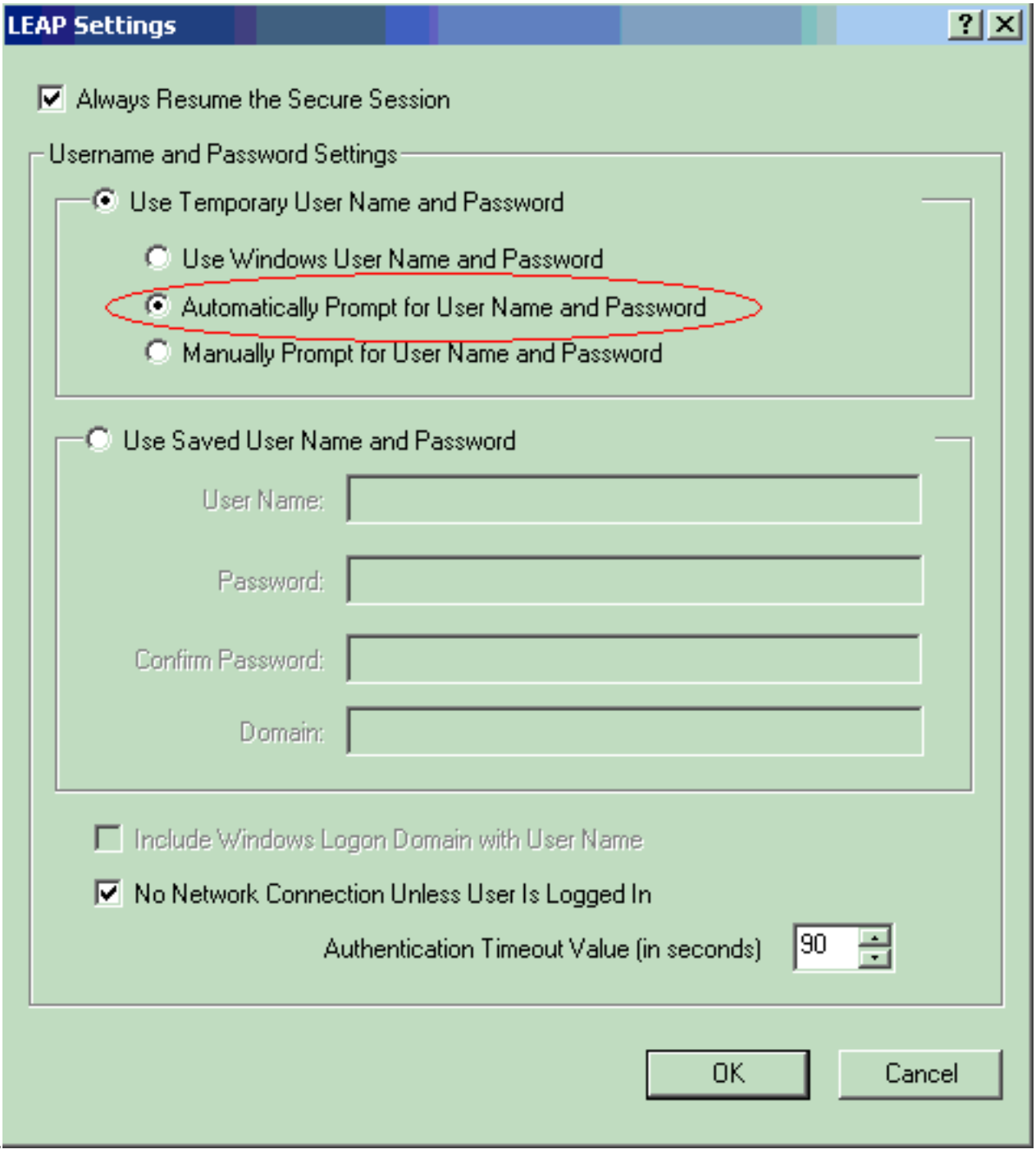
1. Cliquez sur **Nouveau** pour créer un nouveau profil dans la fenêtre Gestion des profils de l'ADU. Saisissez le nom du profil et le SSID que l'adaptateur client utilise sous l'onglet Général.Dans cet exemple, le nom du profil est **870-ISR** et le SSID est **Test**.**Remarque :** Le SSID doit correspondre exactement au SSID que vous avez configuré sur le routeur de service intégré 871W. Le SSID est sensible à la casse.



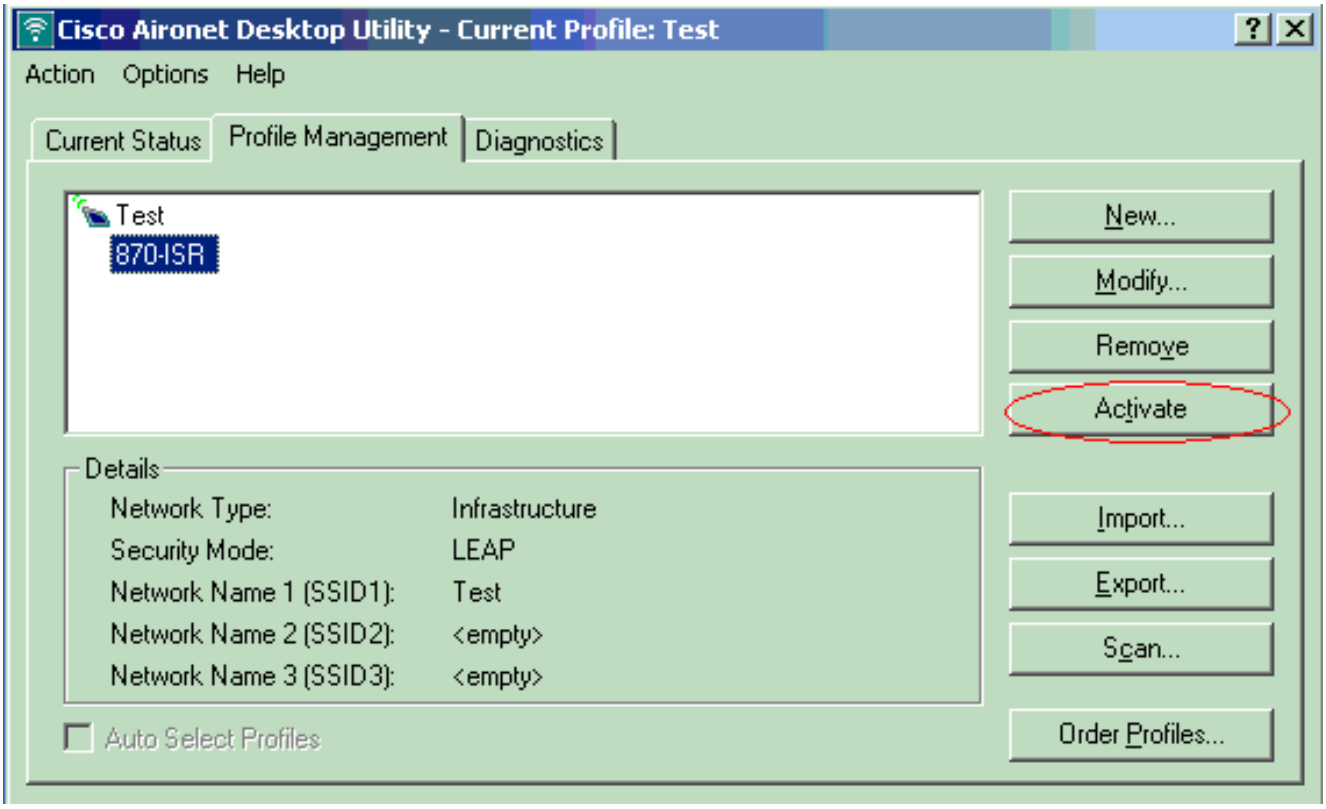
2. Accédez à l'onglet Sécurité, sélectionnez **802.1x** et choisissez **LEAP** dans le menu Type EAP 802.1x.Cette action active l'authentification LEAP sur la carte client.



3. Cliquez sur **Configurer** pour définir les paramètres LEAP.Cette configuration choisit l'option **Demander automatiquement le nom d'utilisateur et le mot de passe**. Cette option vous permet de saisir manuellement le nom de l'utilisateur et le mot de passe quand l'authentification de LEAP a lieu.



4. Cliquez sur **OK** pour quitter la fenêtre Gestion des profils.
5. Cliquez sur **Activer** pour activer ce profil sur l'adaptateur client.

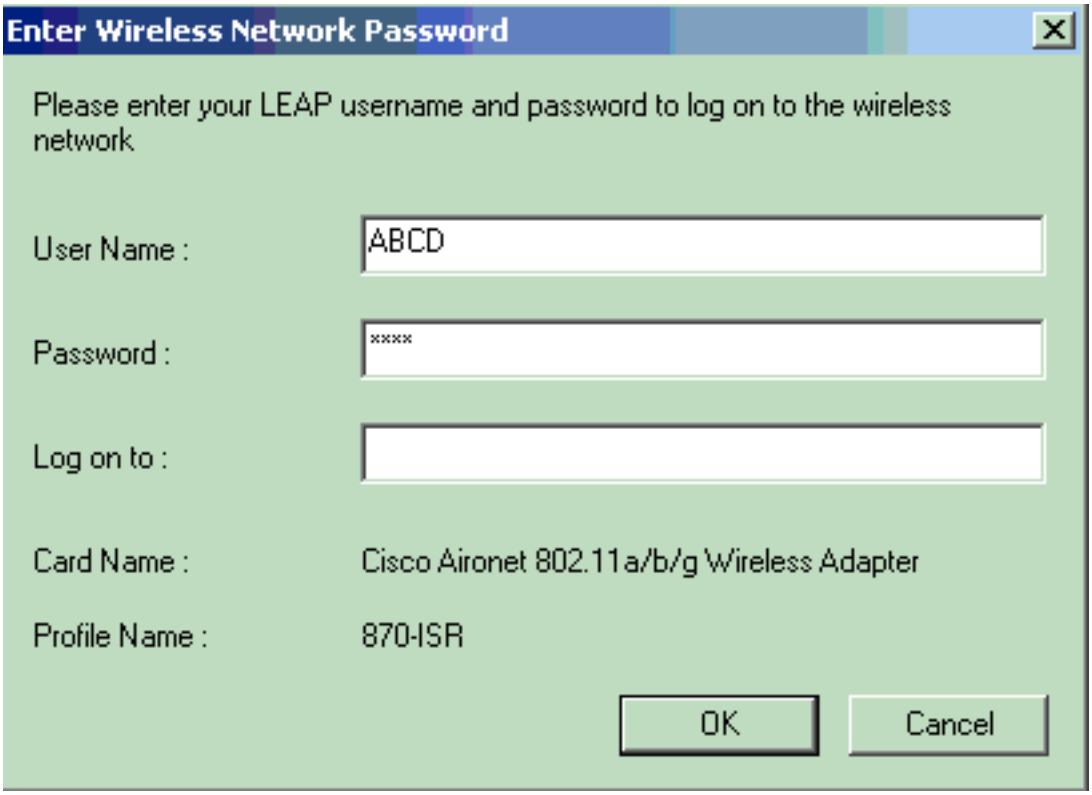


Vérification

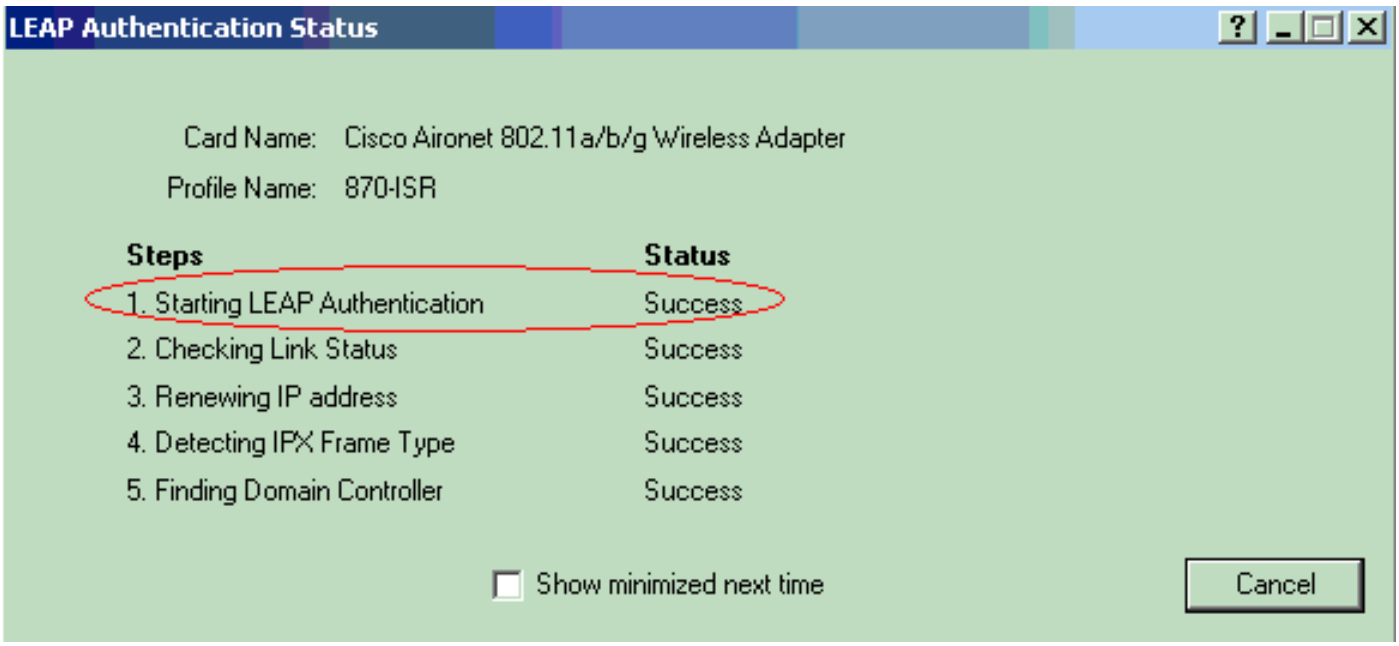
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Une fois l'adaptateur client et le routeur 870 configurés, activez le profil 870-ISR sur l'adaptateur client pour vérifier la configuration.

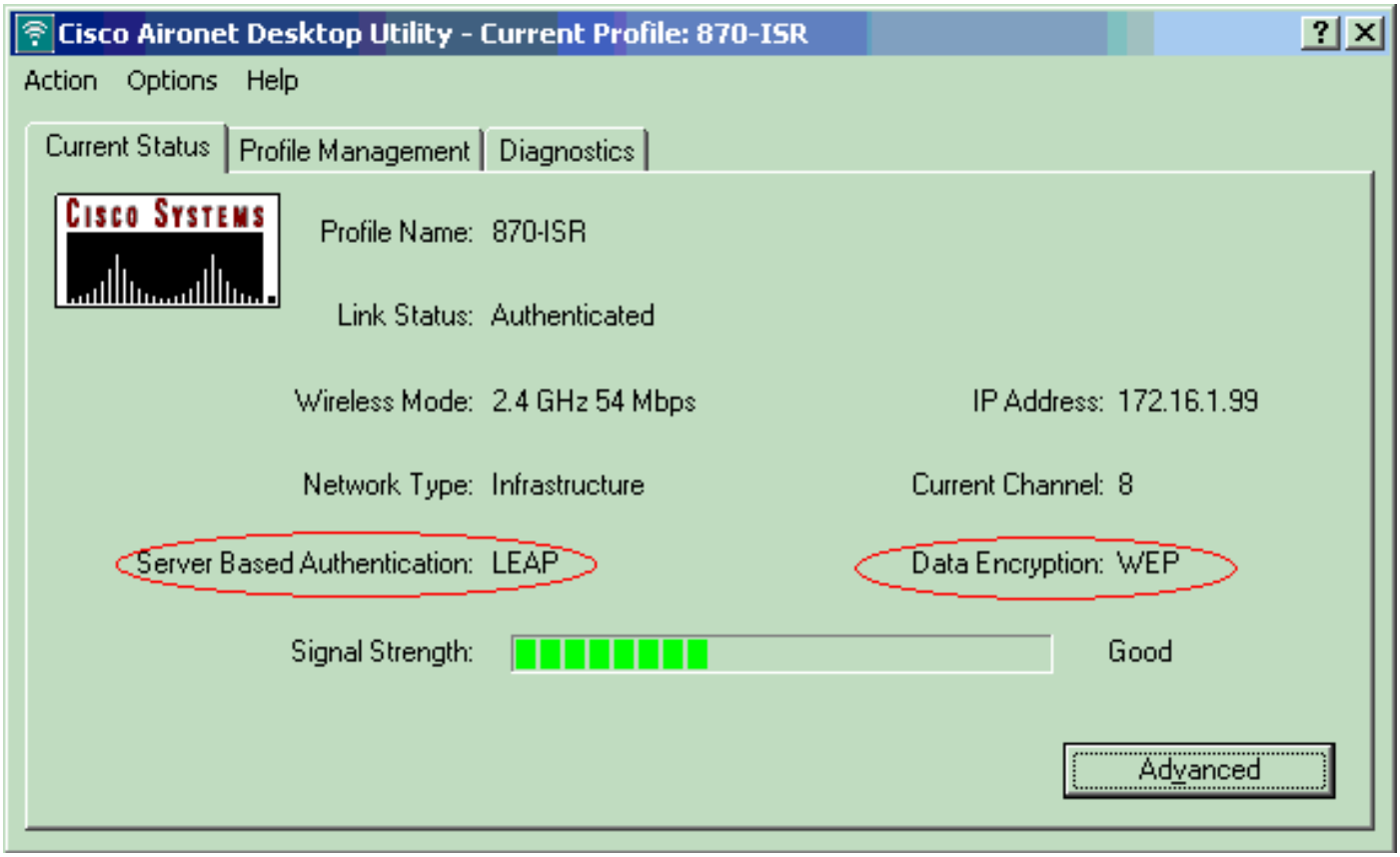
Entrez le nom d'utilisateur et le mot de passe lorsque la fenêtre Enter Wireless Network Password (Saisir le mot de passe du réseau sans fil) s'affiche. Celles-ci doivent correspondre à celles configurées dans le routeur de service intégré 871W. L'un des profils utilisés dans cet exemple est User Name **ABCD** et Password **ABCD**.



La fenêtre LEAP Authentication Status s'affiche. Cette fenêtre vérifie les informations d'identification de l'utilisateur par rapport au serveur RADIUS local.



Vérifiez l'état actuel de l'ADU afin de vérifier que le client utilise le chiffrement WEP et l'authentification LEAP.



L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show dot11 association** - Vérifie la configuration sur le routeur 870.

```
WirelessRouter#show dot11 association

802.11 Client Stations on Dot11Radio0:

SSID [Test]:

MAC Address     IP Address     Device          Name     Parent    State
0040.96ac.dd05   172.16.1.99   CB21AG/PI21AG   LAPTOP-1  self    EAP-Associated

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

- **show ip dhcp binding** - Vérifie que le client a une adresse IP via le serveur DHCP.

```
WirelessRouter#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/       Lease expiration      Type
                 Hardware address/
                 User name
172.16.1.99      0040.96ac.dd05     Feb 6 2006 10:11 PM  Automatic
```

Dépannage

Cette section fournit des informations de dépannage relatives à cette configuration.

1. Définissez la méthode sur le SSID sur **Open** afin de désactiver temporairement l'authentification.Cela élimine la possibilité de problèmes de radiofréquence (RF) empêchant une authentification réussie.Utilisez les commandes **no authentication open eap eap_method**, **no authentication network-eap eap_method** et **authentication open** depuis l'interface de ligne de commande.Si le client s'associe avec succès, alors RF ne contribue

pas au problème d'association
2. Vérifiez si les clés WEP configurées sur le routeur sans fil correspondent aux clés WEP configurées sur les clients.Si les clés WEP ne correspondent pas, les clients ne peuvent pas communiquer avec le routeur sans fil.
3. Vérifiez que les mots de passe secrets partagés sont synchronisés entre le routeur sans fil et le serveur d'authentification.

Vous pouvez également utiliser ces commandes de débogage 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 qui sont envoyés et reçus.
- **debug radius local-server client** - Affiche les messages d'erreur sur les authentifications de client ayant échoué.

Informations connexes

- Algorithmes de chiffrement et types d'authentification
- Exemple de configuration des types d'authentification sans fil sur un routeur ISR fixe via SDM
- Exemple de configuration des types d'authentification sans fil sur un routeur ISR fixe
- Guide de configuration sans fil du routeur d'accès Cisco
- Exemple de configuration d'un routeur sans fil ISR 1800 avec DHCP interne et authentification ouverte
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems