Exemples de configuration de l'authentification sur des contrôleurs de réseau local sans fil

Contenu

Introduction

Ce document fournit les exemples de configuration qui expliquent comment configurer différents types de méthodes d'authentification de couche 1, couche 2 et couche 3 sur des contrôleurs de réseau local sans fil (WLC).

Conditions préalables

Conditions requises

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

- Connaissance de la configuration des points d'accès légers (LAP) et des WLC Cisco
- Connaissance des normes de sécurité 802.11i

Composants utilisés

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

- WLC Cisco 4400 exécutant la version de microprogramme 6.0.182.0
- LAP de la gamme Cisco 1000
- Adaptateur client sans fil Cisco 802.11a/b/g exécutant la version de microprogramme 2.6
- Serveur Cisco Secure ACS version 3.2

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.

Authentification sur des WLC

La solution de sécurité du réseau sans fil unifié (UWN) Cisco regroupe des composants de sécurité de point d'accès (AP) 802.11 de couche 1, couche 2 et couche 3 potentiellement compliqués en un gestionnaire des stratégies simple qui personnalise les stratégies de sécurité au niveau du système par réseau local sans fil (WLAN). La solution de sécurité UWN Cisco fournit des outils de gestion de la sécurité simples, unifiés et systématiques.

Ces mécanismes de sécurité peuvent être mis en application sur les WLC.

Solutions de la couche 1

Restreignez l'accès client selon le nombre de tentatives consécutives ayant échoué.

Solutions de la couche 2

None Authentication — Quand cette option est sélectionnée dans la liste déroulante de sécurité de la couche 2, aucune authentification de la couche 2 n'est exécutée sur le WLAN. Cette option est identique à l'authentification ouverte de la norme 802.11.

Static WEP — Avec le WEP (Wired Equivalent Privacy) statique, tous les AP et NIC radio client sur un WLAN particulier doivent utiliser la même clé de chiffrement. Chaque station émettrice chiffre le corps de chaque trame avec une clé WEP avant transmission et la station réceptrice le déchiffre à l'aide d'une clé identique à la réception.

802.1x — Configure le WLAN pour utiliser l'authentification basée sur 802.1x. L'utilisation de l'authentification IEEE 802.1X offre un cadre pertinent afin d'authentifier et de contrôler le trafic utilisateur vers un réseau protégé, aussi bien que de varier dynamiquement des clés de chiffrement. 802.1X attache un protocole appelé EAP (Extensible Authentication Protocol) à la fois aux supports câblé et WLAN, et prend en charge plusieurs méthodes d'authentification.

Static WEP + 802.1x — Ce paramètre de sécurité de couche 2 active à la fois 802.1x et le WEP statique. Les clients peuvent employer l'authentification WEP statique ou 802.1x afin de se connecter au réseau.

Wi-Fi Protected Access (WPA) — WPA ou WPA1 et WPA2 sont des solutions de sécurité

standard de Wi-Fi Alliance qui fournissent la protection des données et le contrôle d'accès pour des systèmes WLAN. WPA1 est compatible avec la norme IEEE 802.11i mais a été mis en application avant la ratification de la norme. WPA2 est la mise en œuvre de Wi-Fi Alliance de la norme ratifiée IEEE 802.11i.

Par défaut, WPA1 utilise le protocole TKIP (Temporal Key Integrity Protocol) et MIC (Message Integrity Check) pour la protection des données. WPA2 utilise l'algorithme de chiffrement plus fort AES (Advanced Encryption Standard) avec l'utilisation du mode compteur avec le protocole de code d'authentification de message de chaînage de chiffrement de blocs (AES-CCMP). WPA1 et WPA2 utilisent tous deux 802.1X pour la gestion des clés authentifiée par défaut. Cependant, ces options sont également disponibles : PSK, CCKM et CCKM+802.1x. Si vous sélectionnez CCKM, Cisco autorise seulement les clients qui prennent en charge CCKM. Si vous sélectionnez CCKM+802.1x, Cisco autorise également des clients non-CCKM.

CKIP — Le Cisco Key Integrity Protocol (CKIP) est un protocole de Sécurité de propre à Cisco pour chiffrer des medias de 802.11. CKIP améliore la sécurité 802.11 dans le mode infrastructure avec la permutation de clés, MIC et le numéro de séquence du message. La version de logiciel 4.0 prend en charge CKIP avec la clé statique. Pour que cette fonctionnalité opère correctement, vous devez activer les éléments d'information Aironet pour le WLAN. Les paramètres CKIP spécifiés dans un WLAN sont obligatoires pour n'importe quel client qui essaye une association. Si le WLAN est configuré pour la permutation de clés CKIP et MMH MIC, le client doit prendre en charge chacun des deux. Si le WLAN est configuré pour seulement une de ces fonctionnalités, le client doit prendre en charge seulement cette fonctionnalité CKIP. Les WLC ne prennent en charge que le CKIP statique (comme le WEP statique). Les WLC ne prennent pas en charge CKIP avec 802.1x (CKIP dynamique).

Solutions de la couche 3

None — Quand cette option est sélectionnée dans la liste déroulante de sécurité de la couche 3, aucune authentification de la couche 3 n'est exécutée sur le WLAN.

Remarque: L'exemple de configuration pour l'absence d'authentification de la couche 3 et l'absence d'authentification de la couche 2 est expliqué dans la section Aucune authentification.

Web Policy (Web Authentication and Web Passthrough) — L'authentification Web est typiquement utilisée par les clients qui veulent déployer un réseau d'accès invité. Dans un réseau d'accès invité, il y a une authentification initiale de nom d'utilisateur et mot de passe, mais la sécurité n'est pas requise pour le trafic ultérieur. En général, les déploiements peuvent inclure des hotspots tels que T-Mobile ou Starbucks.

L'authentification Web pour le WLC Cisco est faite localement. Vous créez une interface, puis associez un WLAN/SSID (Service Set Identifier) à cette interface.

L'authentification Web fournit une authentification simple sans demandeur ou client. Gardez présent à l'esprit que l'authentification Web ne fournit pas le chiffrement des données. L'authentification Web est généralement utilisée en tant qu'accès invité simple pour un hotspot ou une atmosphère de campus où la seule préoccupation est la connectivité.

Le relais Web est une solution par laquelle des utilisateurs sans fil sont redirigés vers une page acceptable de stratégie d'utilisation sans devoir s'authentifier quand ils se connectent à Internet. Cette redirection est assurée par le WLC lui-même. La seule condition requise est de configurer le WLC pour le relais Web, qui est fondamentalement l'authentification Web sans devoir entrer des

informations d'identification.

VPN Passthrough — VPN Passthrough est une fonctionnalité qui permet à un client d'établir un tunnel seulement avec un serveur VPN spécifique. Par conséquent, si vous devez accéder en toute sécurité au serveur VPN configuré aussi bien qu'à un autre serveur VPN ou Internet, ce n'est pas possible avec l'option VPN Passthrough activée sur le contrôleur.

Dans les sections suivantes, des exemples de configuration sont donnés pour chacun des mécanismes d'authentification.

Exemples de configuration

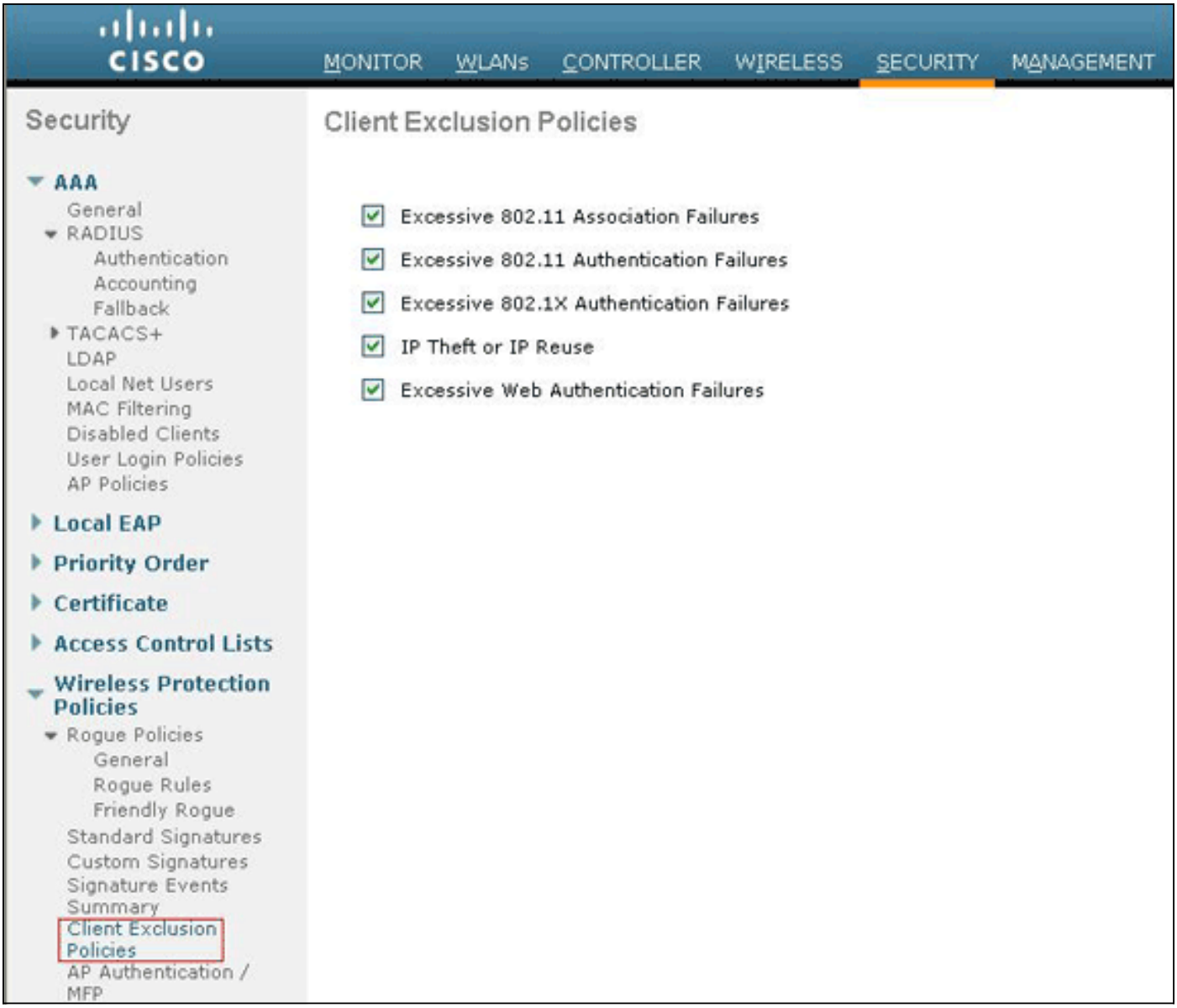
Avant de configurer les WLAN et les types d'authentification, vous devez configurer le WLC pour l'opération de base et enregistrer les LAP sur le WLC. Ce document suppose que WLC est configuré pour les opérations de base et que les LAP sont enregistrés au WLC. Si vous êtes un nouvel utilisateur qui essaie d'installer le WLC pour l'opération de base avec les LAP, consultez l'Enregistrement léger AP (LAP) sur un contrôleur LAN sans fil (WLC).

Solutions de sécurité de la couche 1

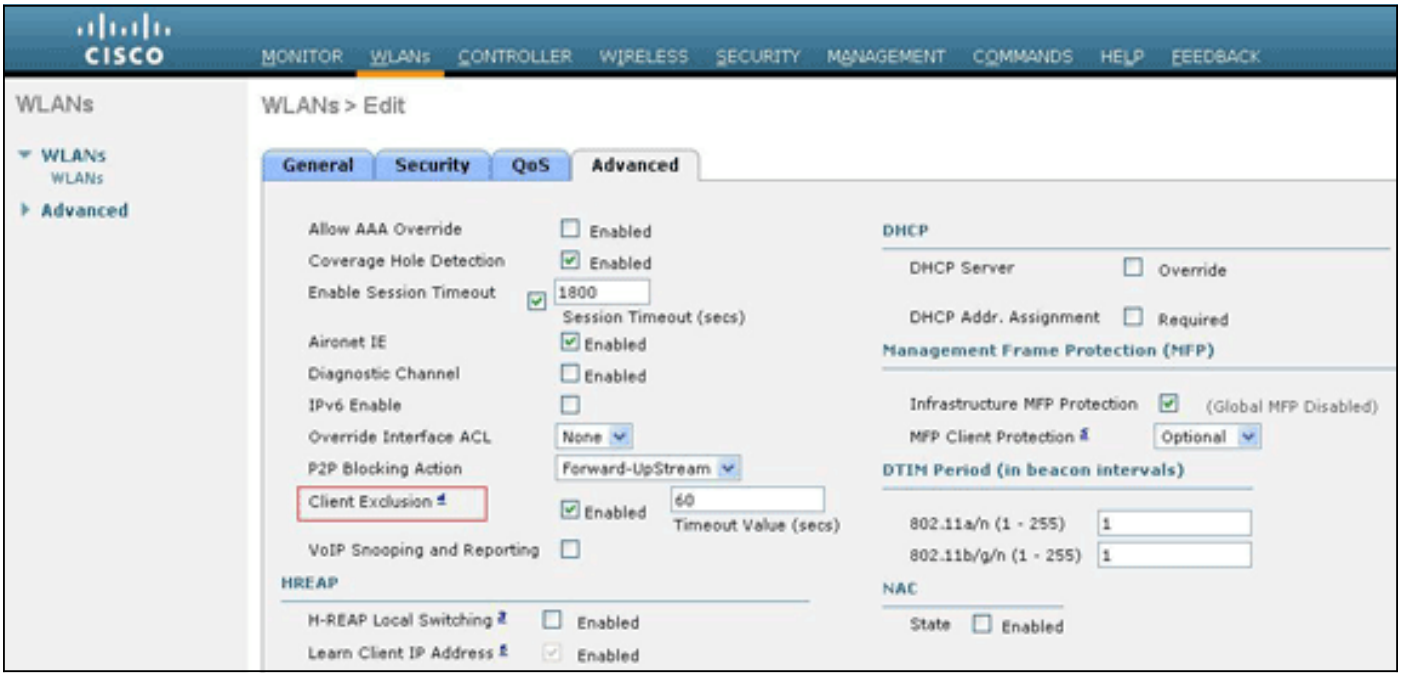
L'accès peut être limité pour les clients sans fil selon le nombre de tentatives consécutives d'accès au réseau WLAN ayant échoué. L'exclusion de client se produit dans ces conditions par défaut. Ces valeurs ne peuvent pas être modifiées.

- Échec d'authentification 802.11 consécutif (5 fois consécutives, le 6ème essai est exclu)
- Échecs d'association 802.11 consécutifs (5 fois consécutives, le 6ème essai est exclu)
- Échecs d'authentification 802.1x consécutifs (3 fois consécutives, le 4ème essai est exclu)
- Échec de serveur de stratégie externe
- Tentative d'utiliser l'adresse IP déjà attribuée à un autre périphérique (vol d'IP ou réutilisation d'IP)
- Échecs d'authentification Web consécutifs (3 fois consécutives, le 4ème essai est exclu)

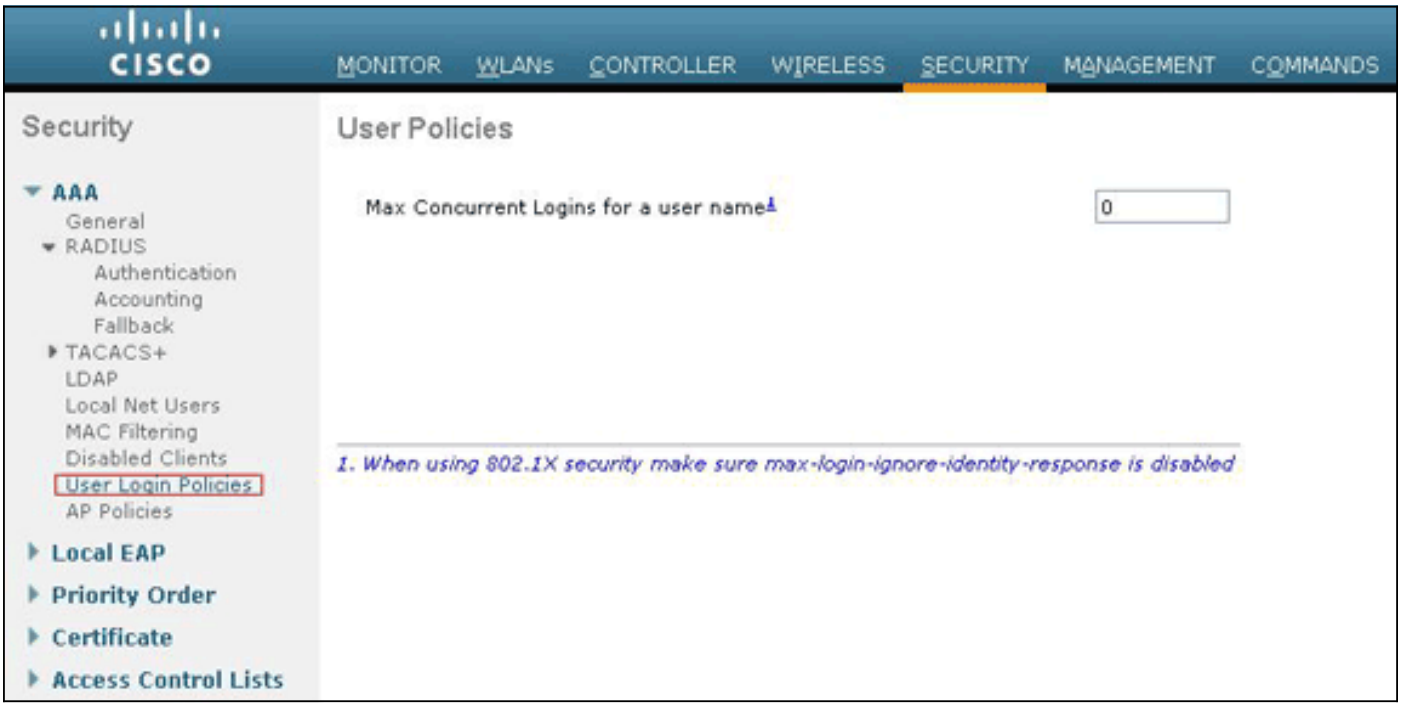
Afin de localiser les stratégies d'exclusion de client, cliquez sur **Security** dans le menu principal, puis choisissez **Wireless Protection Policies > Client Exclusion Policies** sur le côté gauche de la page.



Le compteur d'exclusion peut être configuré. Des options d'exclusion peuvent être activées ou désactivées par contrôleur. Le compteur d'exclusion peut être activé ou désactivé par WLAN.



Le nombre maximal de connexions simultanées pour un seul nom d'utilisateur par défaut est 0. Vous pouvez entrer n'importe quelle valeur entre 0 et 8. Ce paramètre peut être défini sur **SECURITY > AAA > User Login Policies** et vous permet de spécifier le nombre maximal de connexions simultanées pour un seul nom de client, entre un et huit, ou 0 = illimité. Voici un exemple :

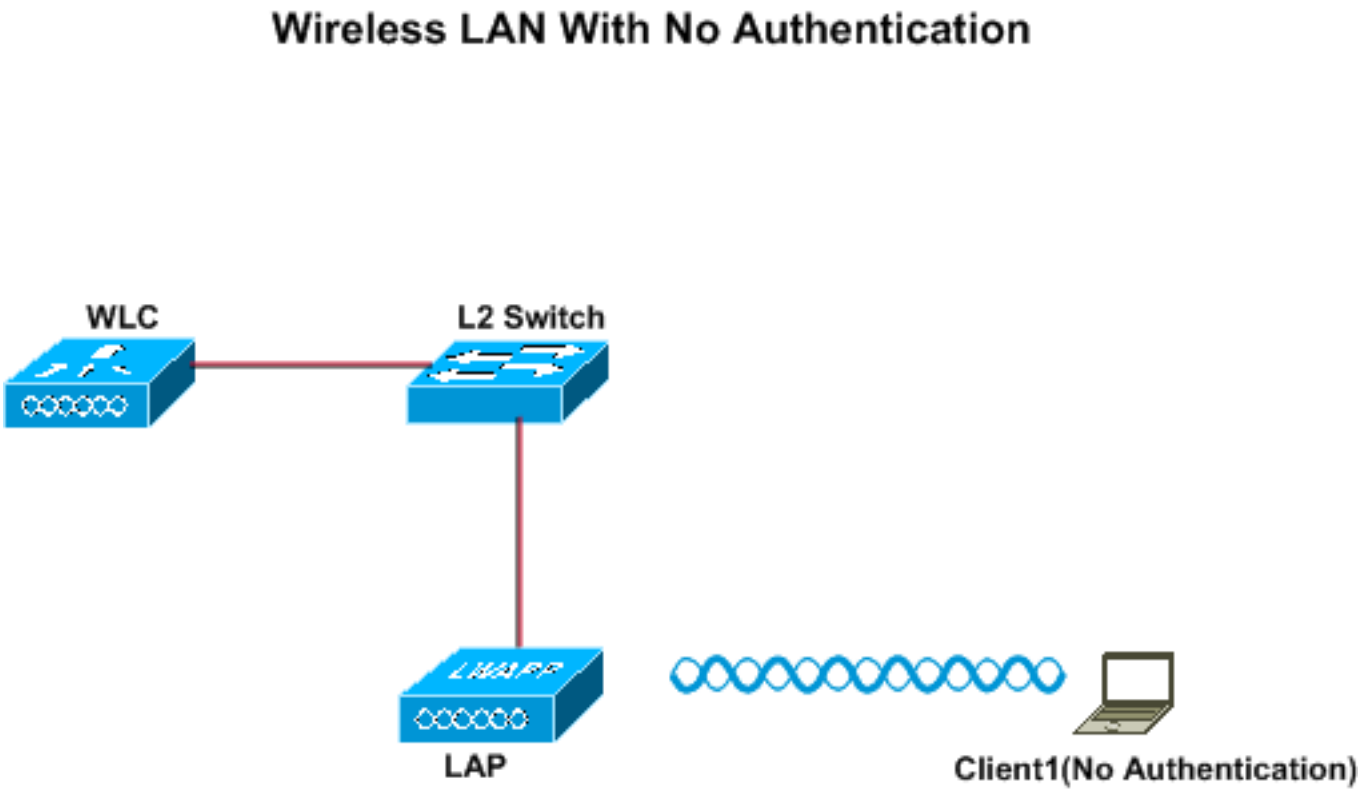


Solutions de sécurité de la couche 2

Aucune authentification

Cet exemple montre un WLAN configuré sans authentification.

Remarque: Cet exemple fonctionne également pour l'absence d'authentification de la couche 3.



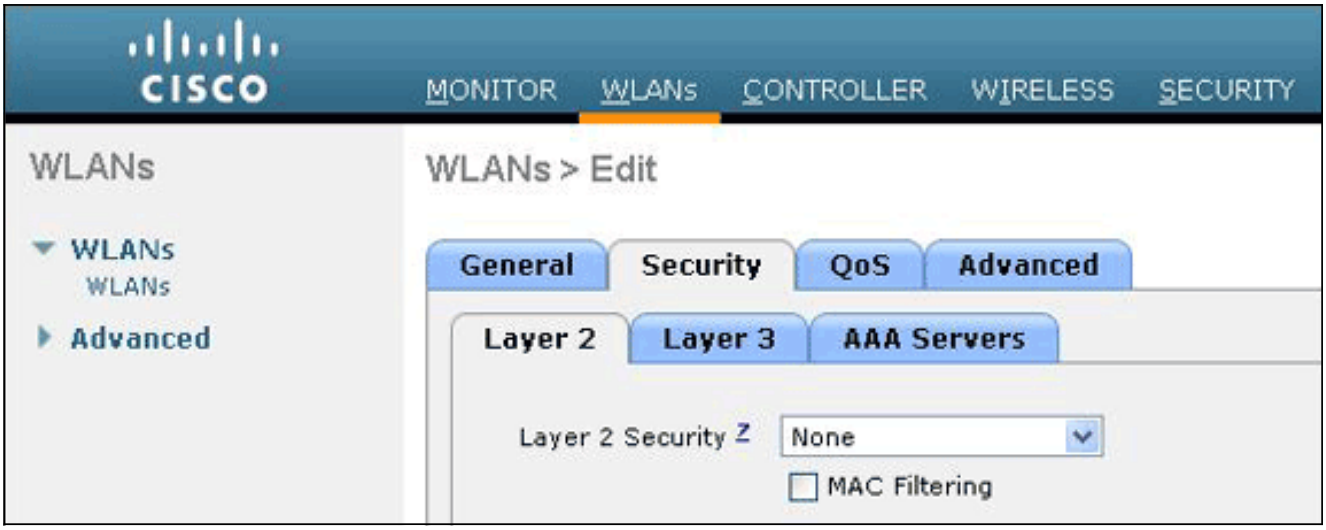
Configurer WLC pour l'absence d'authentification

Complétez ces étapes afin de définir le WLC pour cette configuration :

1. Cliquez sur **WLANs** depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **Go** pour configurer un nouveau WLAN.
3. Entrez les paramètres pour le WLAN. Cet exemple montre la configuration pour ce WLAN.

4. Cliquez sur **Apply**.
5. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.

6. Cliquez sur l'onglet **Security**, puis choisissez **None** pour la sécurité de couche 2 et de couche 3.



Remarque: Pour qu'un WLAN devienne actif, l'état doit être activé. Pour l'activer, activez la case à cocher **Status** sous l'onglet General.Ceci active l'absence d'authentification pour ce WLAN.

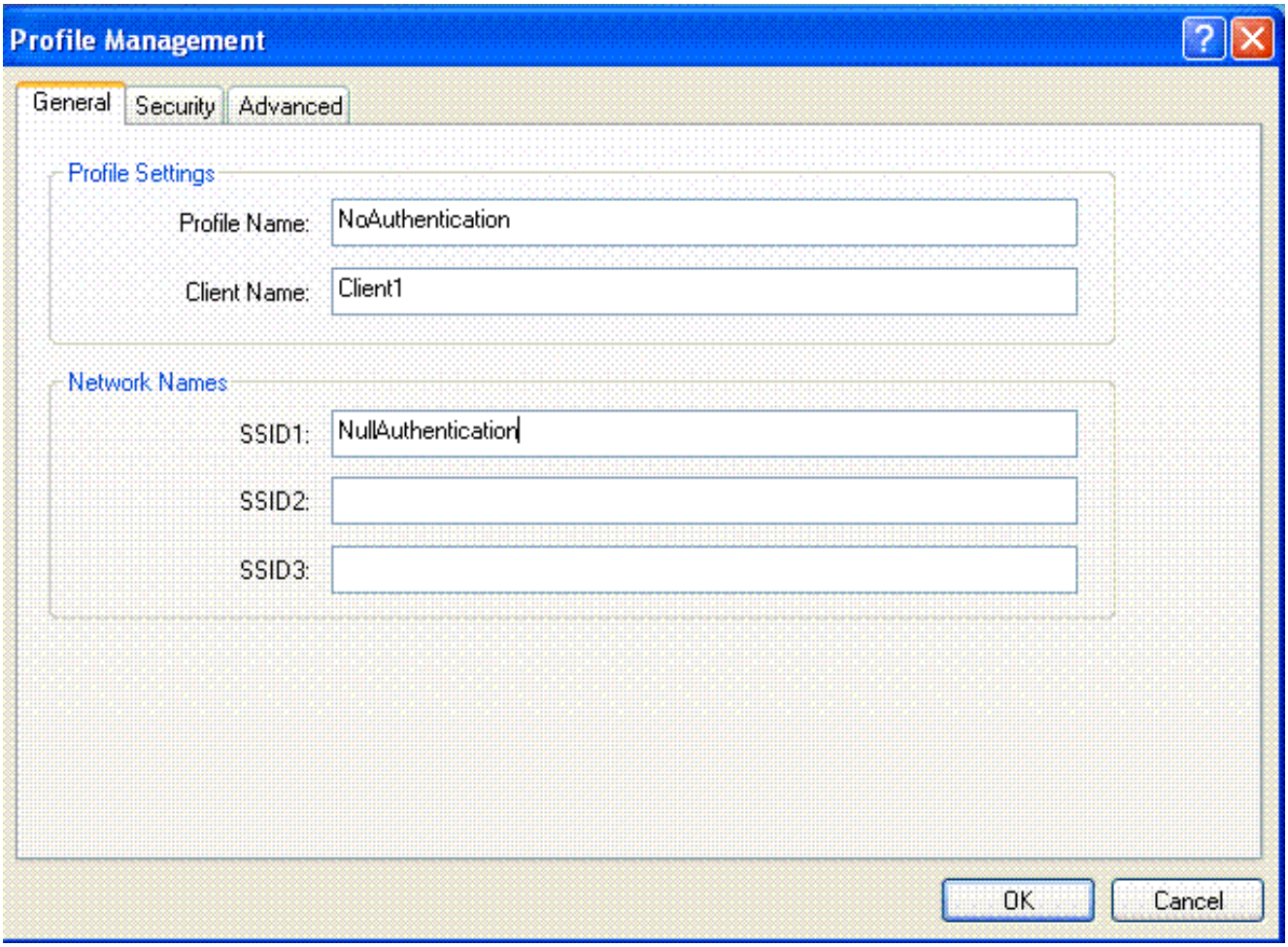
7. Choisissez d'autres paramètres selon vos exigences en termes de conception. Cet exemple utilise les valeurs par défaut.
8. Cliquez sur **Apply**.

Configurer le client sans fil pour l'absence d'authentification

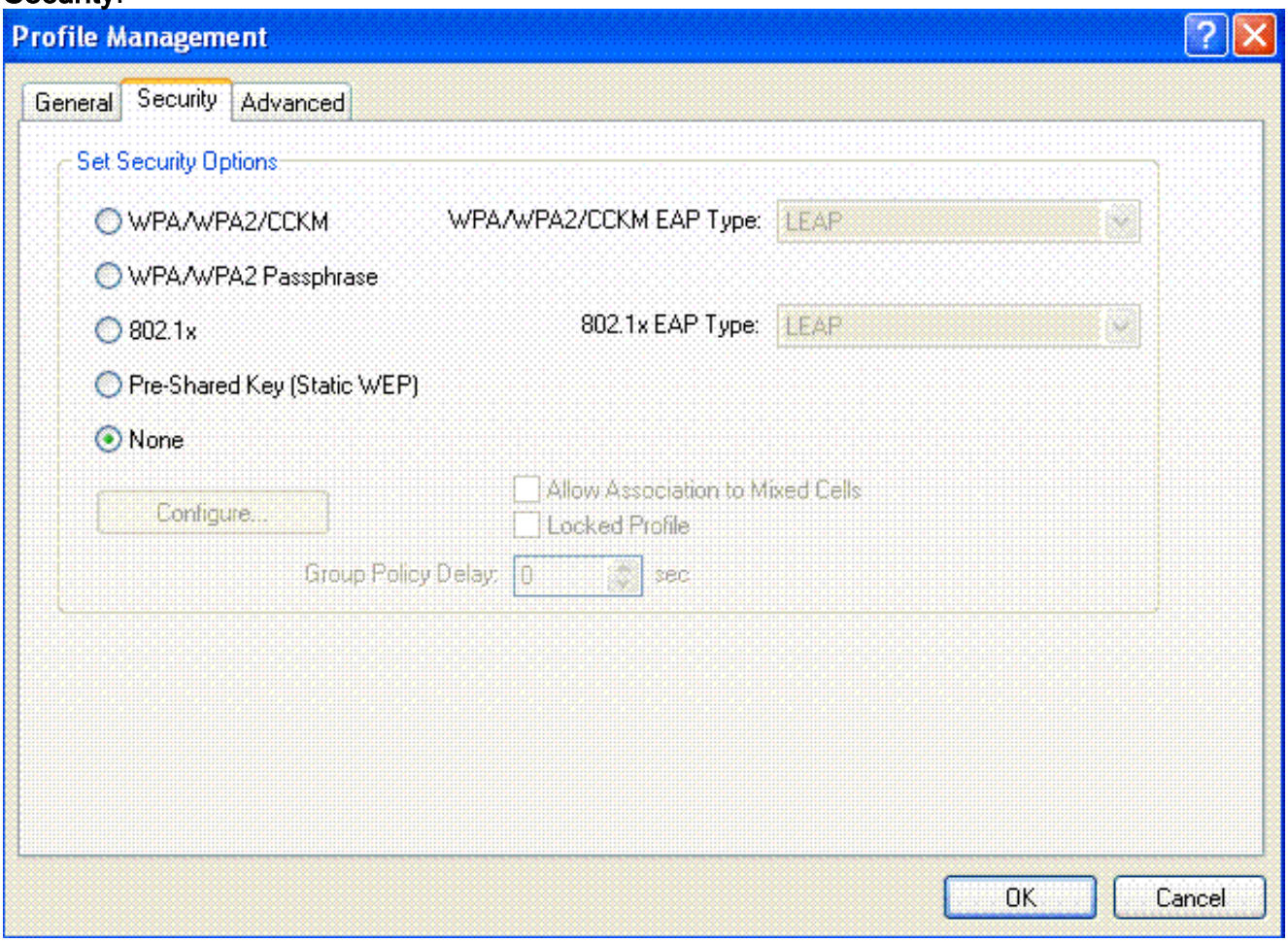
Terminez-vous ces étapes afin de configurer le client Sans fil de RÉSEAU LOCAL pour cette installation :

Remarque: Ce document utilise un adaptateur client Aironet 802.11a/b/g qui exécute le microprogramme 3.5 et explique la configuration de l'adaptateur client avec ADU version 3.5.

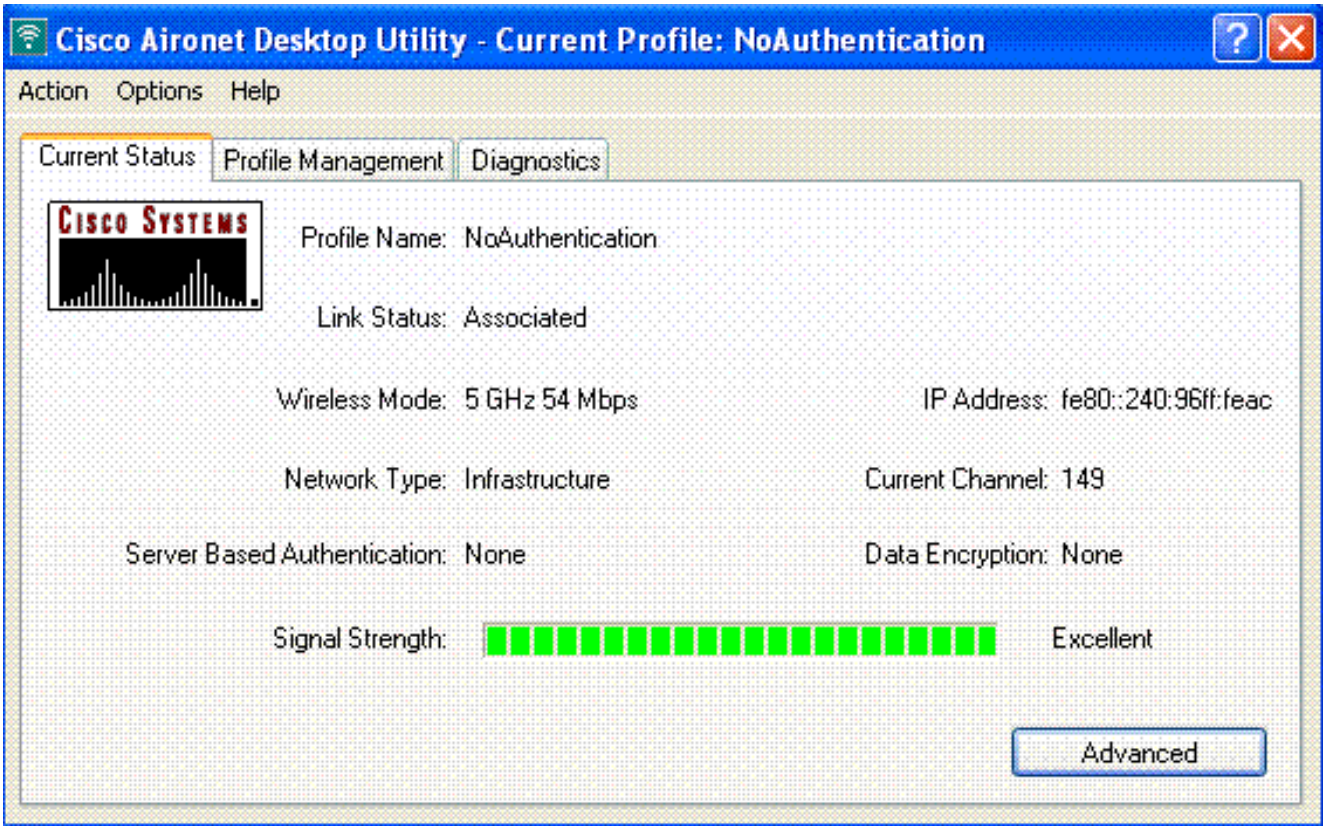
1. Afin de créer un nouveau profil, cliquez sur l'onglet **Profile Management** sur l'ADU.
2. Cliquez sur **New**.
3. Quand les affichages de fenêtre de Profile Management (général), se terminent ces étapes afin de placer le nom de profil, le nom de client, et le SSID :Saisissez le nom du profil dans le champ Profile Name.Cet exemple utilise *NoAuthentication* comme nom de profil.Saisissez le nom du client dans le champ Client Name.Le nom du client est utilisé pour identifier le client sans fil dans le réseau WLAN. Cette configuration utilise *Client 1* pour le nom du client.Sous des noms de réseau, écrivez le SSID qui doit être utilisé pour ce profil.Le SSID est identique au SSID que vous avez configuré sur le WLC. Le SSID dans cet exemple est *NullAuthentication.*



4. Cliquez sur l'onglet **Security**.

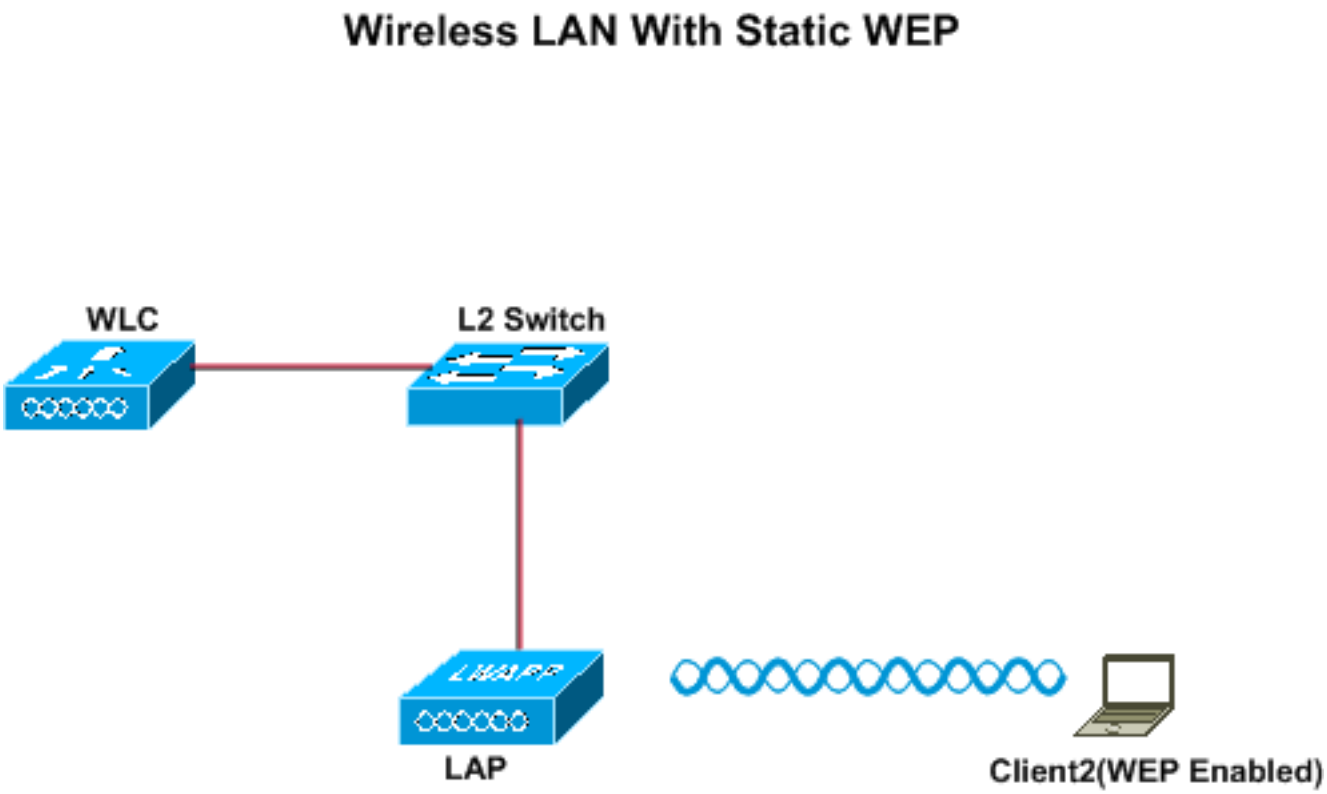


5. Cliquez sur la case d'option **None** sous Set Security Options, puis sur **OK**.Quand le SSID est activé, le client sans fil se connecte au WLAN sans aucune authentification.



WEP statique

Cet exemple montre un WLAN configuré avec le WEP statique.

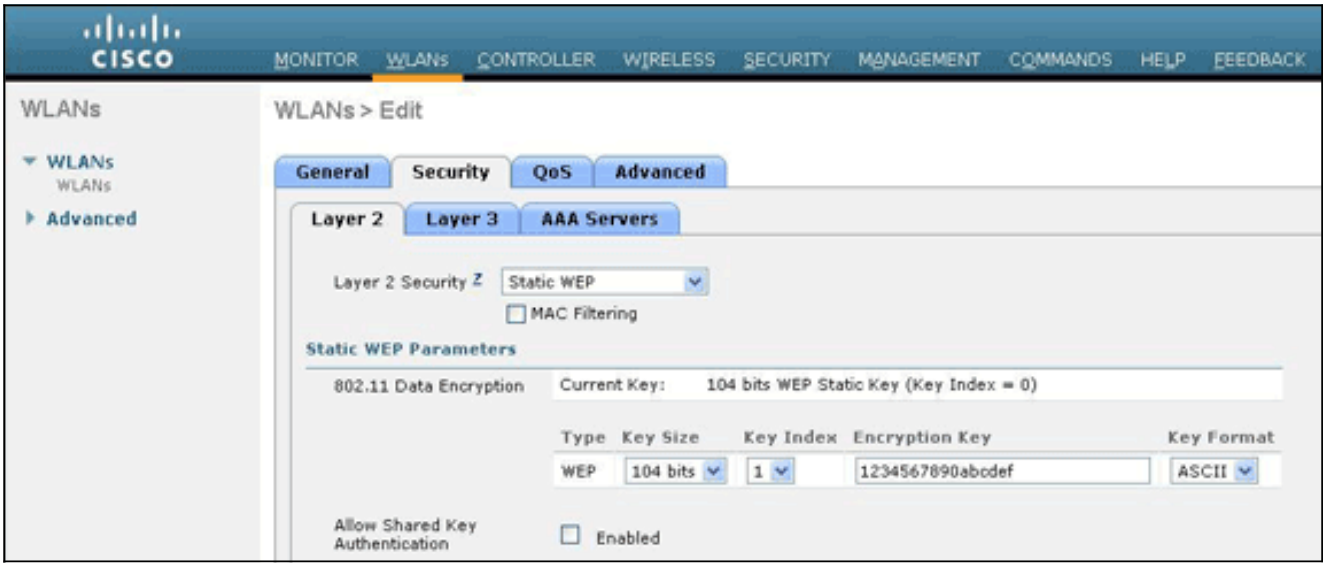


Configurer WLC pour le WEP statique

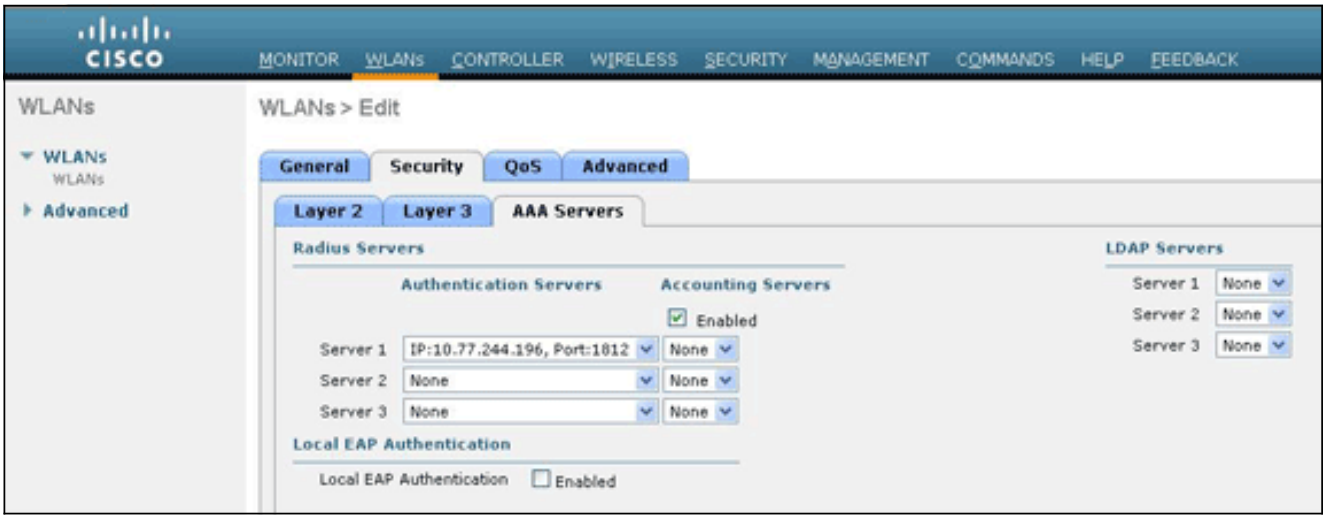
Complétez ces étapes afin de définir le WLC pour cette configuration :

1. Cliquez sur **WLANs** depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **New** pour configurer un nouveau WLAN.
3. Entrez l'ID de WLAN et le SSID de WLAN.Dans cet exemple, le WLAN est nommé *StaticWEP* et l'ID de WLAN est *2*.

4. Cliquez sur **Apply**.
5. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.Dans la liste déroulante de la couche 2, choisissez **Static WEP**.Ceci active le WEP statique pour ce WLAN.Sous les paramètres de WEP statique, choisissez la taille et l'index de clé WEP et entrez la clé de chiffrement WEP statique.La taille de la clé peut être de 40 bits ou 104 bits. L'index de clé peut être entre 1 et 4. Un seul index de clé WEP peut être appliqué à chaque WLAN. Puisqu'il y a seulement quatre index de clé WEP, seuls quatre WLAN peuvent être configurés pour le chiffrement WEP statique de couche 2. Dans cet exemple, le WEP 104 bits est utilisé et la clé WEP utilisée est 1234567890abcdef.



Vérifiez si le serveur RADIUS est configuré pour l'authentification. Le serveur RADIUS peut être configuré sur l'onglet **Security** situé à **AAA > Radius > Authentication**. Une fois configuré, le serveur RADIUS devrait être attribué au WLAN pour l'authentification. Allez à **WLANs > Security > AAA Servers** afin d'affecter le serveur RADIUS au WLAN pour l'authentification.Dans cet exemple, 10.77.244.196 est le serveur RADIUS.



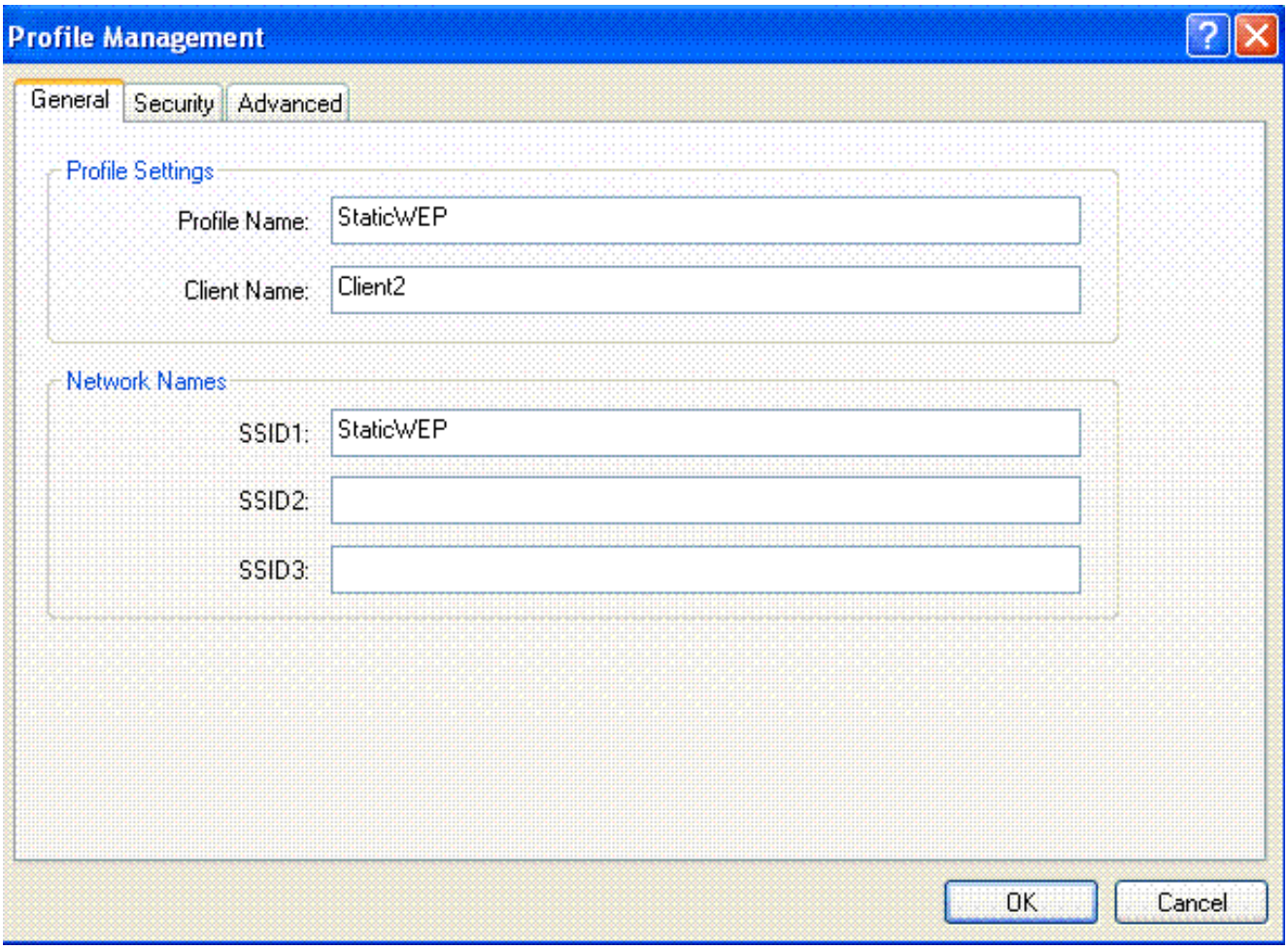
6. Choisissez d'autres paramètres selon vos exigences en termes de conception.Cet exemple utilise les valeurs par défaut.
7. Cliquez sur **Apply**.**Remarque:** WEP est toujours représenté au format hexadécimal (hex). Quand vous entrez la clé WEP en mode ASCII, la chaîne WEP ASCII est convertie au format hexadécimal, qui est utilisé pour chiffrer le paquet. Il n'y a aucune méthode standard que les fournisseurs exécutent pour convertir le format hexadécimal en ASCII, car certains

effectueront un remplissage et d'autres non. Par conséquent, pour une compatibilité maximale entre fournisseurs, utilisez le format hexadécimal pour les clés WEP.**Remarque:** Si vous voulez activer l'authentification par clé partagée pour le WLAN, activez la case à cocher **Allow Shared-Key Authentication** sous les paramètres de WEP statique. De cette façon, si le client est également configuré pour l'authentification par clé partagée, l'authentification par clé partagée suivie du chiffrement WEP des paquets aura lieu dans le WLAN.

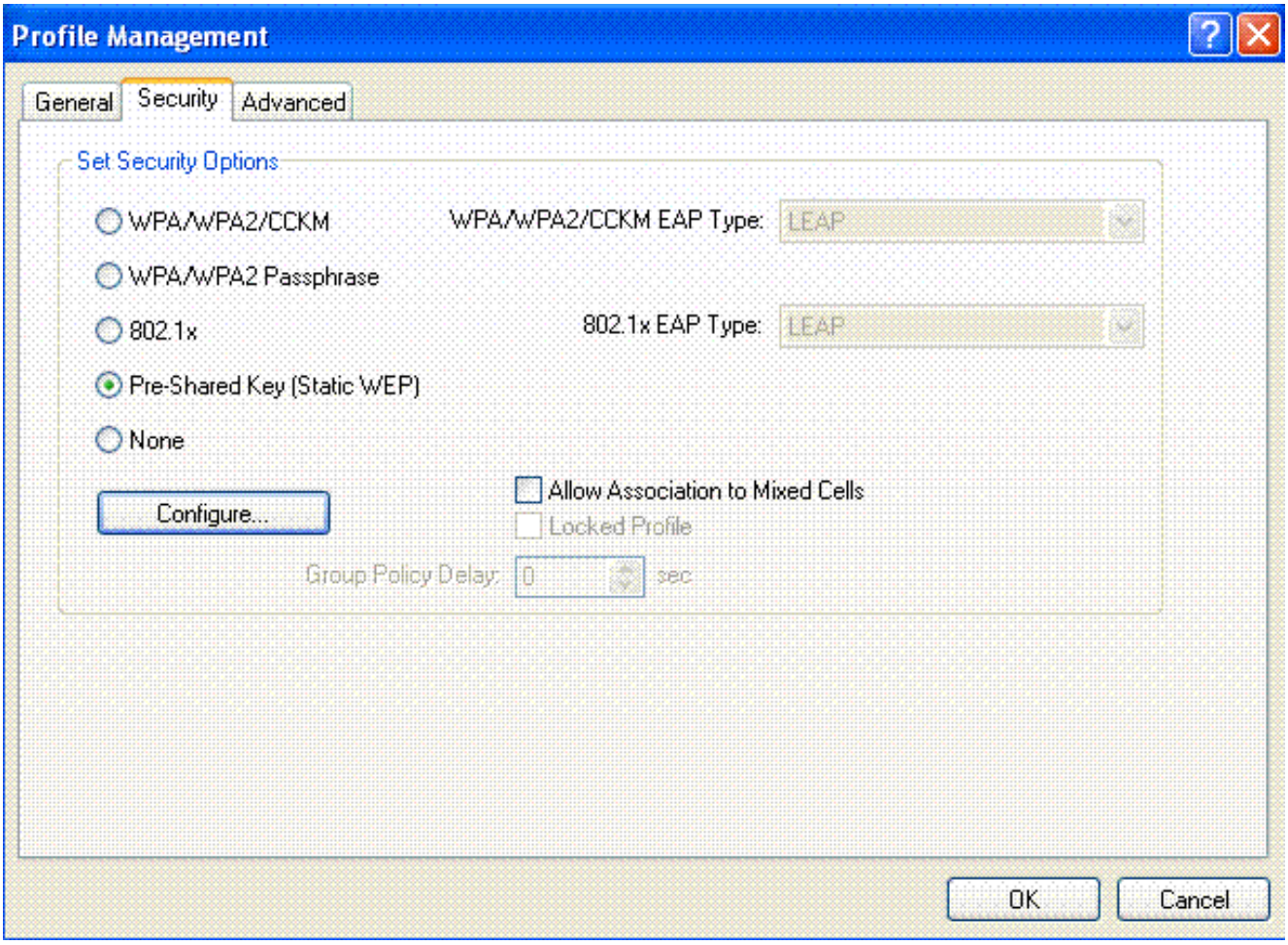
Configurer le client sans fil pour le WEP statique

Effectuez ces étapes afin de définir le client LAN sans fil pour cette configuration :

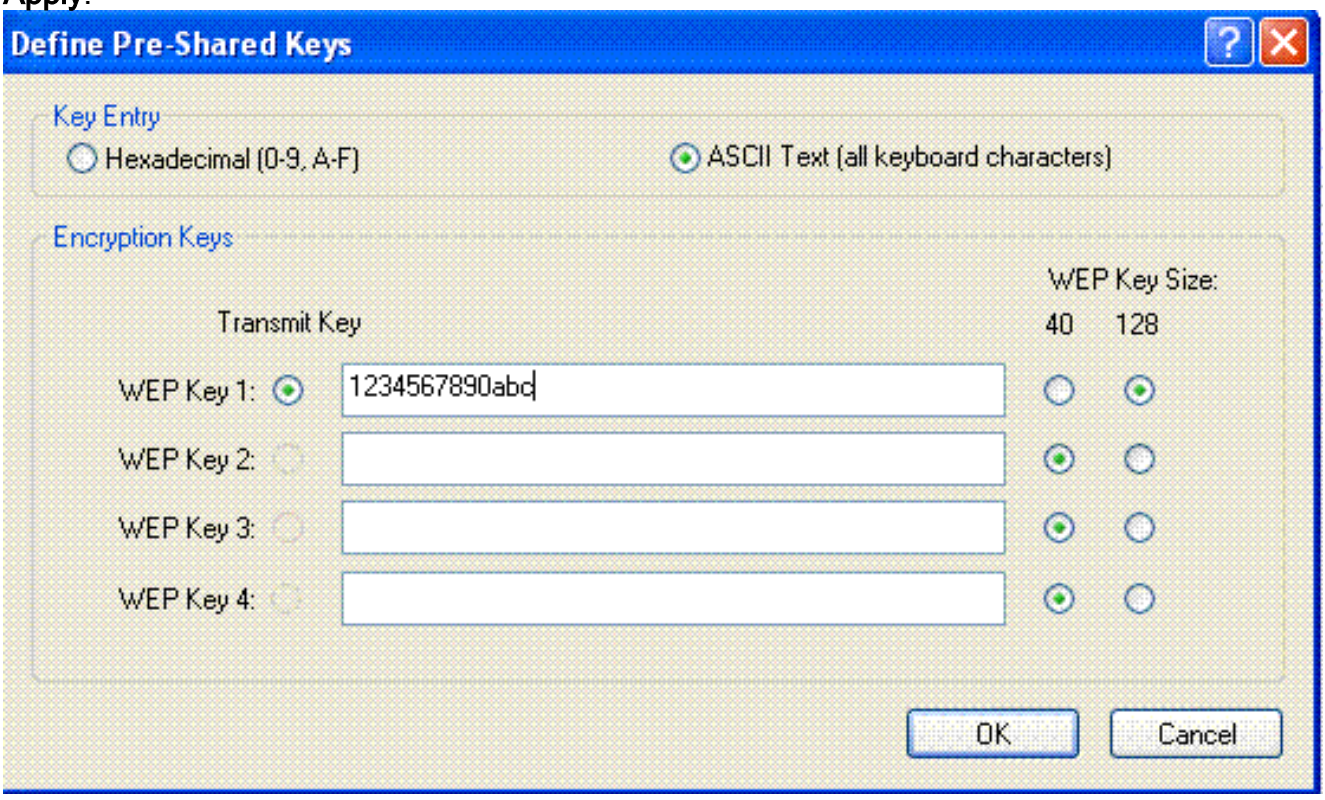
1. Afin de créer un nouveau profil, cliquez sur l'onglet **Profile Management** sur l'ADU.
2. Cliquez sur **New**.
3. Quand les affichages de fenêtre de Profile Management (général), se terminent ces étapes afin de placer le nom de profil, le nom de client, et le SSID :Saisissez le nom du profil dans le champ Profile Name.Cet exemple utilise *StaticWEP* comme nom de profil.Saisissez le nom du client dans le champ Client Name.Le nom du client est utilisé pour identifier le client sans fil dans le réseau WLAN. Cette configuration utilise *Client 2* pour le nom du client.Sous des noms de réseau, écrivez le SSID qui doit être utilisé pour ce profil.Le SSID est identique au SSID que vous avez configuré sur le WLC. Le SSID dans cet exemple est *StaticWEP*.



4. Cliquez sur l'onglet **Security**.

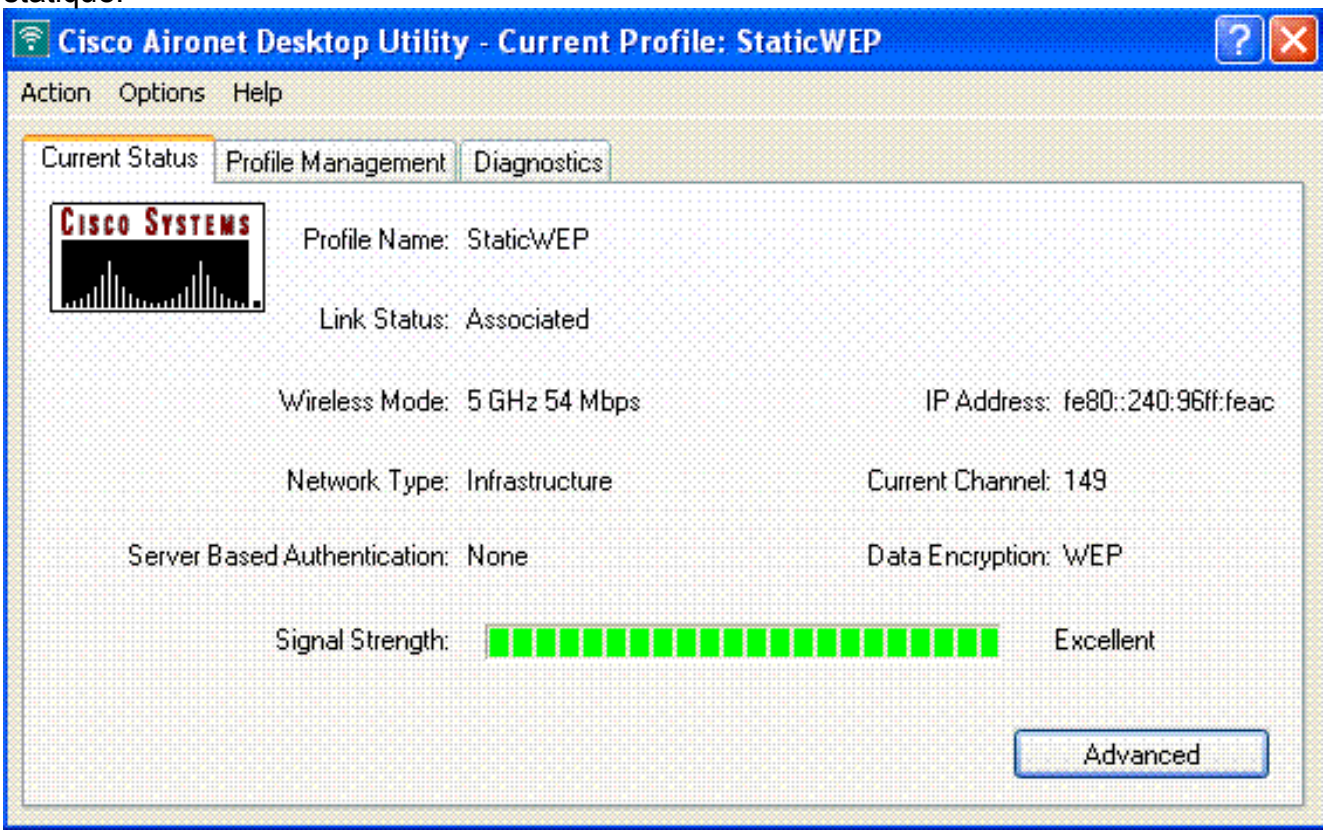


5. Choisissez **Pre-Shared Key (Static WEP)** sous Set Security Options.
6. Cliquez sur **Configure** et définissez la taille de clé WEP et la clé WEP.Ceci doit correspondre à la clé WEP configurée sur le WLC pour ce WLAN.
7. Cliquez sur **Apply**.



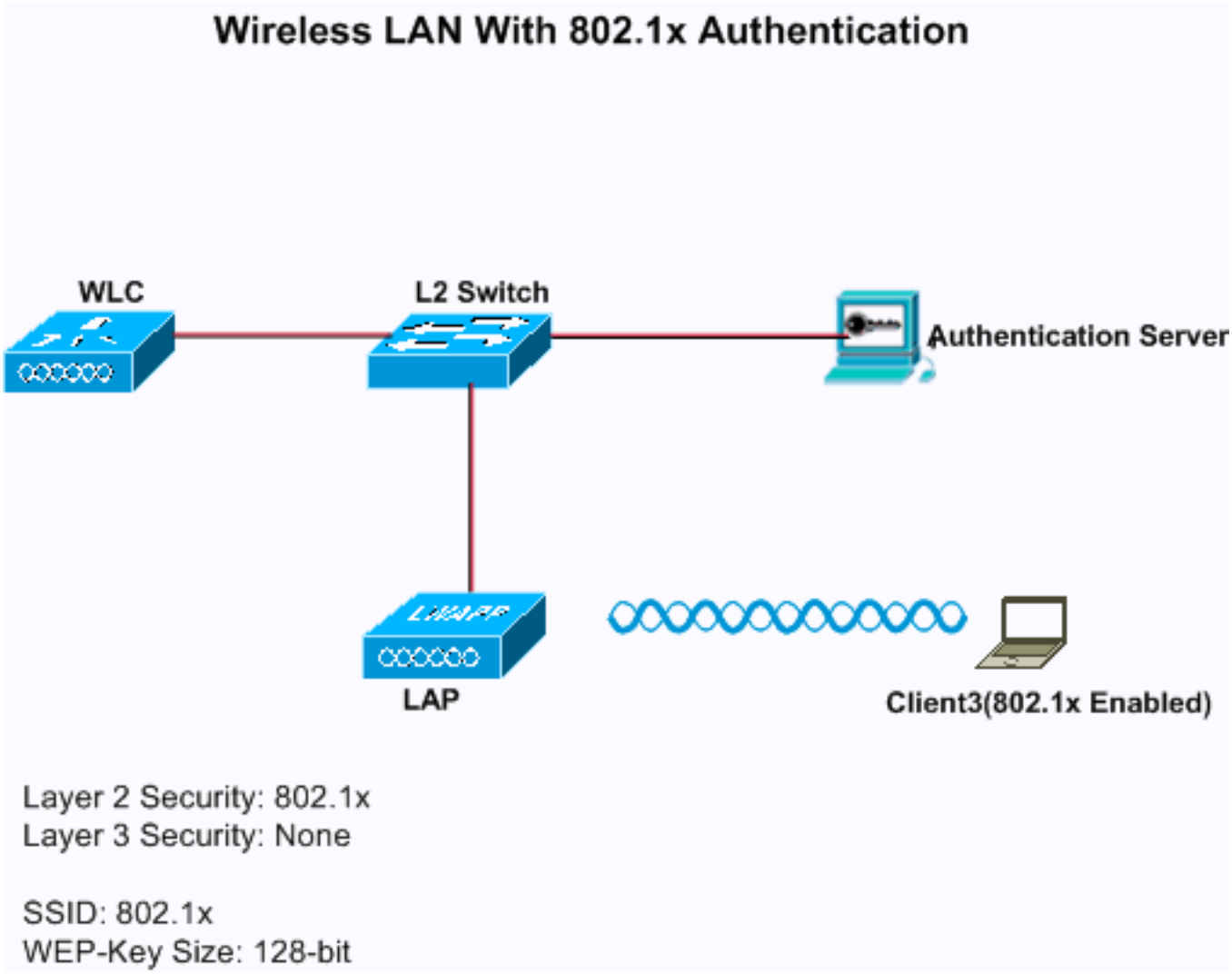
Quand le SSID est activé, le client sans fil se connecte au WLAN et les paquets sont chiffrés à l'aide de la clé WEP

statique.



Authentification 802.1x

Cet exemple montre un WLAN configuré avec l'authentification 802.1x.



Configurer WLC pour l'authentification 802.1x

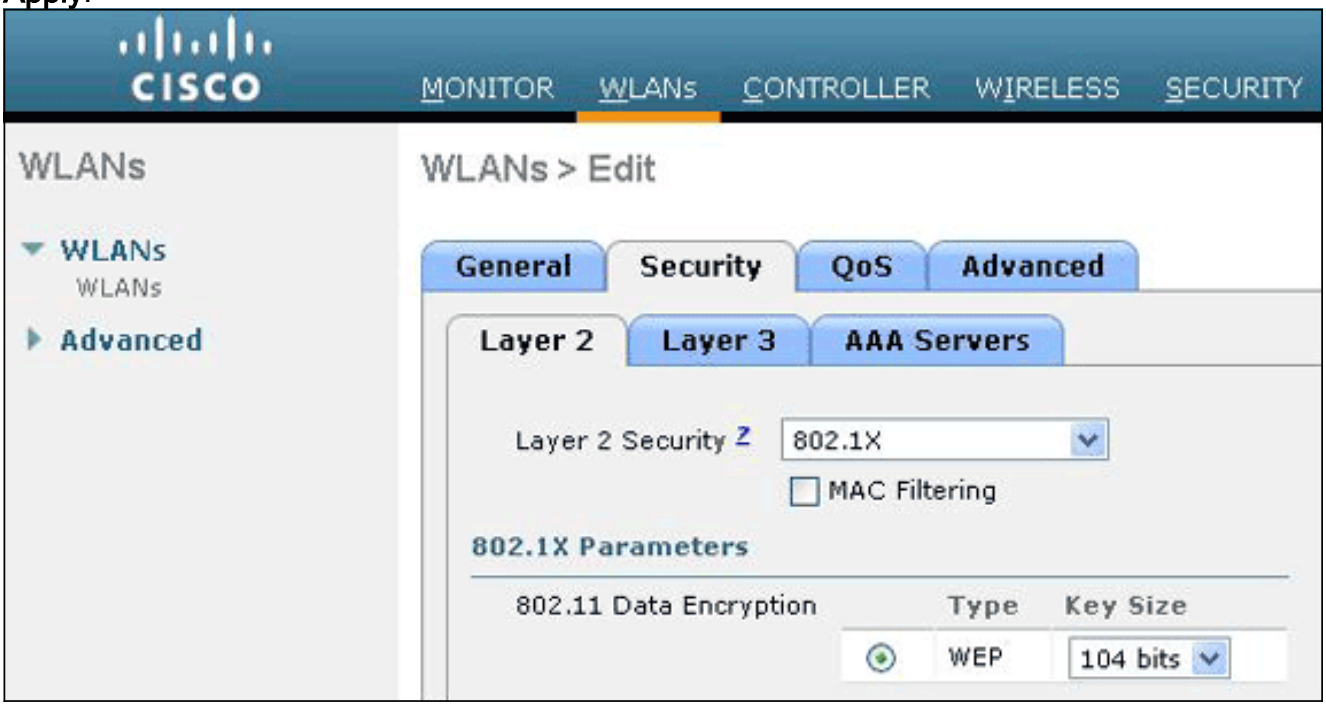
Complétez ces étapes afin de définir le WLC pour cette configuration :

1. Cliquez sur **WLANs** depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **New** pour configurer un nouveau WLAN.Dans cet exemple, le WLAN est nommé *802.1x* et l'ID de WLAN est *3.* Un nom de profil doit également être ajouté.

3. Cliquez sur **Apply**.
4. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.Dans la liste

déroulante de la couche 2, choisissez **802.1x**.**Remarque:** Seul le chiffrement WEP est disponible avec 802.1x. Choisissez 40 bits ou 104 bits pour le chiffrement et assurez-vous que la sécurité de la couche 3 est définie sur None.Ceci active l'authentification 802.1x pour ce WLAN.Sous les paramètres de serveur RADIUS, sélectionnez le serveur RADIUS qui sera utilisé pour authentifier les informations d'identification du client.Choisissez d'autres paramètres selon vos exigences en termes de conception.Cet exemple utilise les valeurs par défaut.

5. Cliquez sur **Apply**.

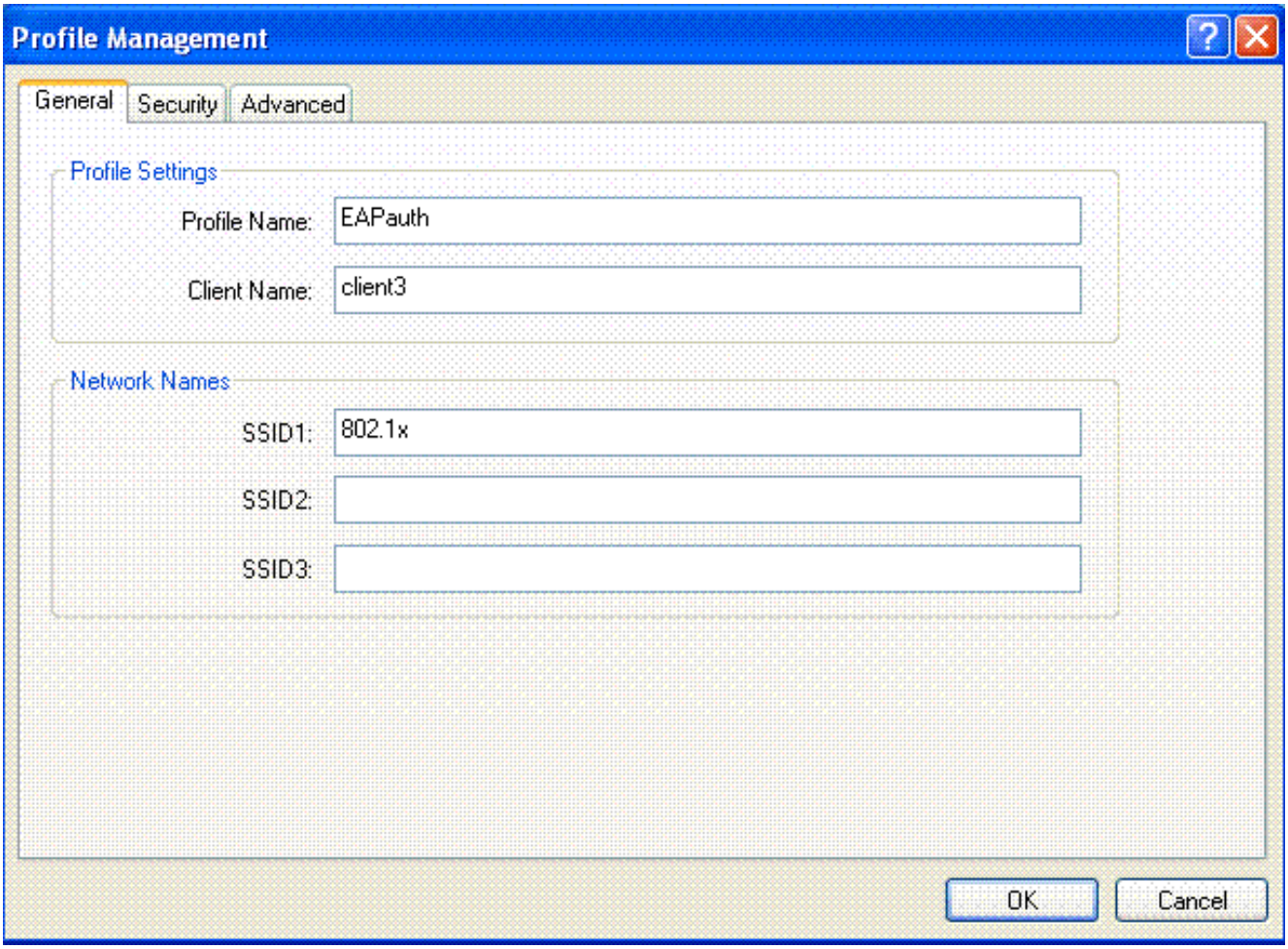


Remarques : Si vous choisissez *802.1x* pour la sécurité de la couche 2, CCKM ne peut pas être utilisé.Si vous choisissez *WPA 1* ou *WPA 2* pour la sécurité de la couche 2, ces options apparaissent sous Auth Key Management :*802.1x+CCKM* — Si vous choisissez cette option, CCKM ou les clients non-CCKM sont tous deux pris en charge (CCKM facultatif).*802.1x* — Si vous choisissez cette option, seuls les clients 802.1x sont pris en charge.*CCKM* — Si vous choisissez cette option, seulement des clients CCKM sont pris en charge, où des clients sont dirigés vers un serveur externe pour l'authentification.*PSK* — Si vous choisissez cette option, une clé pré-partagée est utilisée pour le WLC et le client. En outre, toutes les normes sont définies pour être utilisées avant les prénormes ; par exemple, WPA/WPA2 est prioritaire sur CCKM lorsqu'ils sont utilisés simultanément.Le type d'authentification EAP utilisé pour valider les clients dépend du type d'EAP configuré sur le serveur RADIUS et les clients sans fil. Une fois que 802.1x est activé sur le WLC, le WLC permet à tous les types de paquets EAP de circuler entre le LAP, le client sans fil et le serveur RADIUS.Ces documents fournissent des exemples de configuration sur certains des types d'authentification EAP :PEAP sous des réseaux sans fil unifiés avec ACS 4.0 et Windows 2003EAP-TLS sous un réseau sans fil unifié avec ACS 4.0 et Windows 2003Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil (WLC)

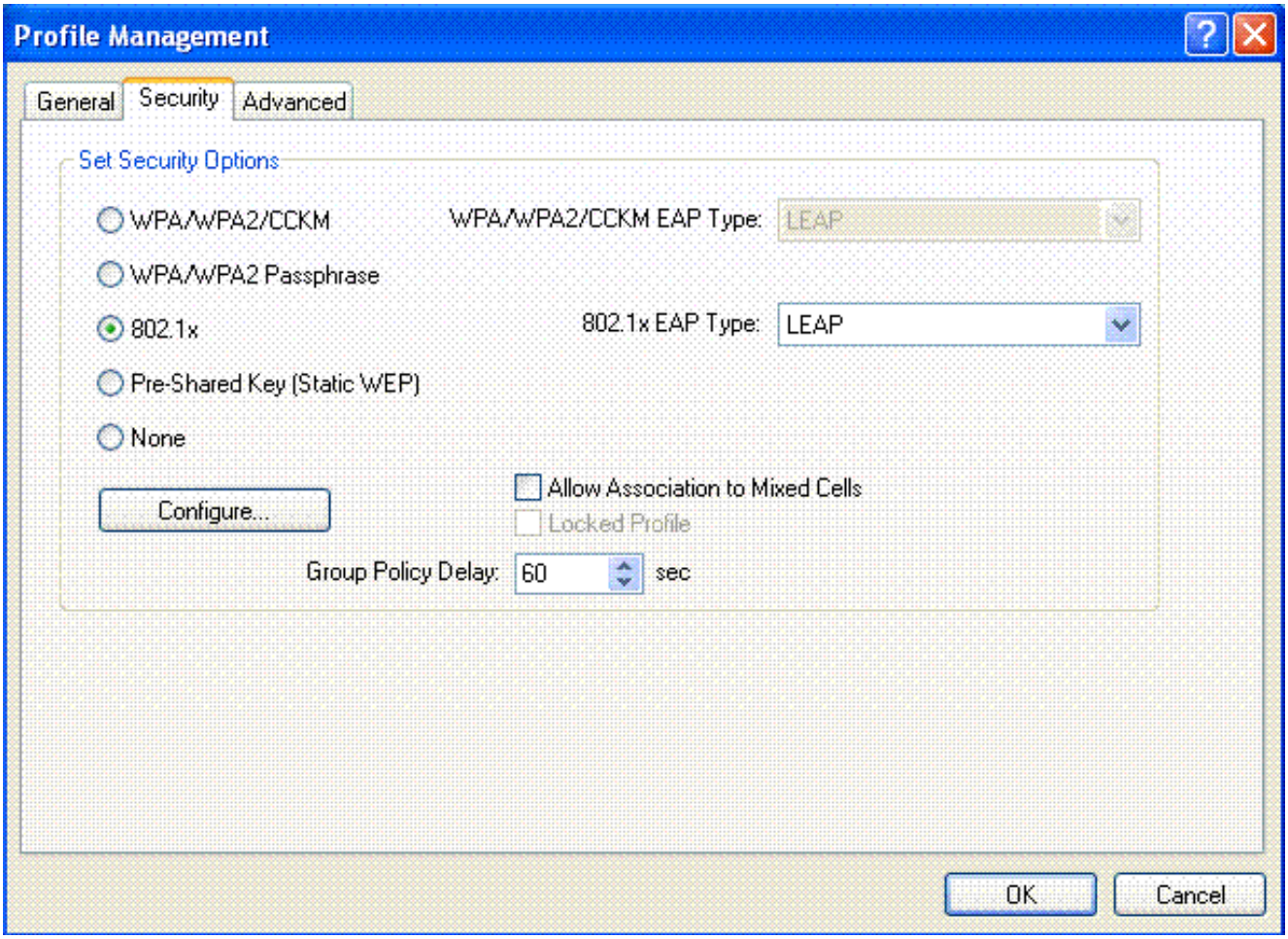
Configurer le client sans fil pour l'authentification 802.1x

Effectuez ces étapes afin de définir le client LAN sans fil pour cette configuration :

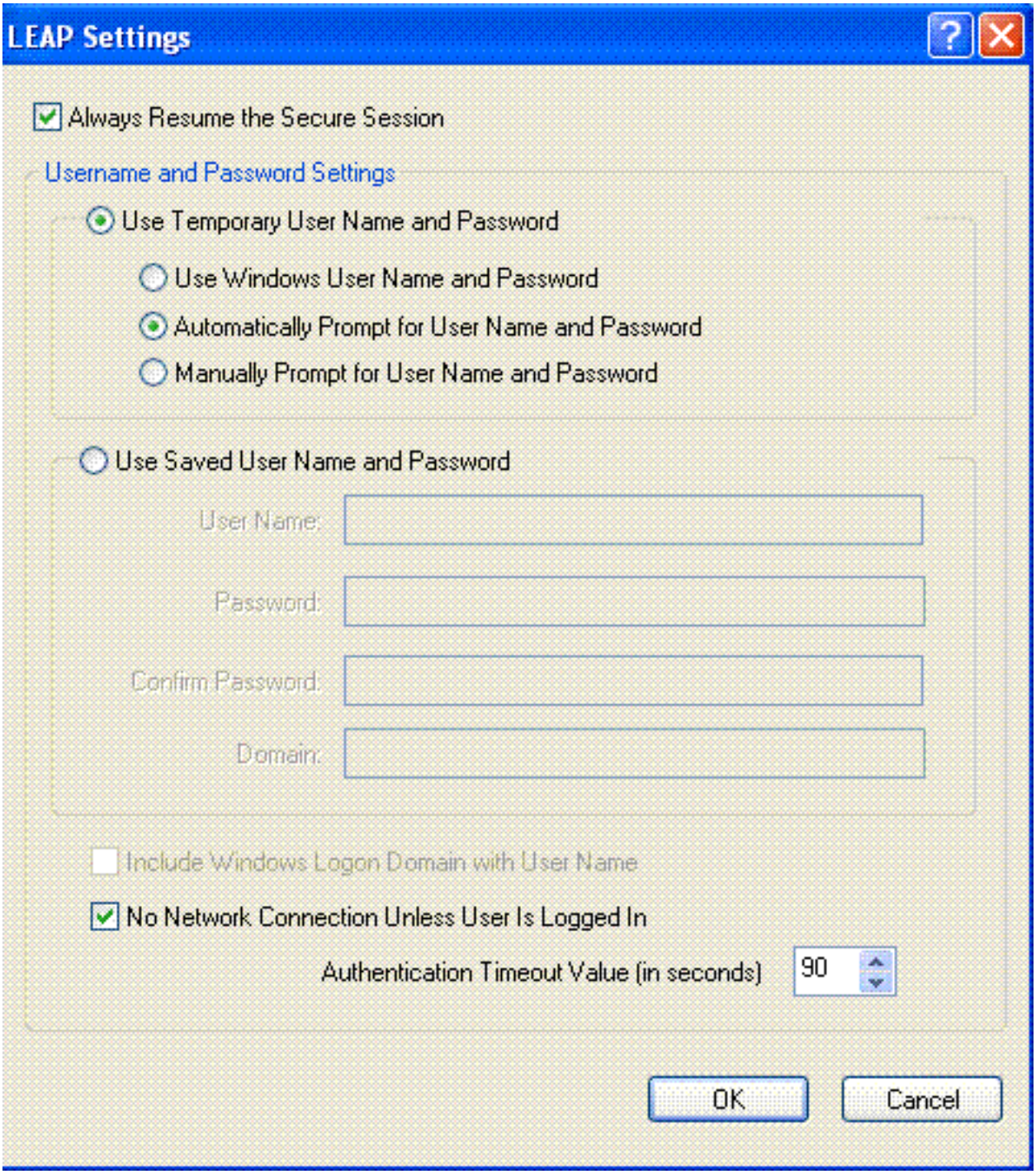
1. Afin de créer un nouveau profil, cliquez sur l'onglet **Profile Management** sur l'ADU.
2. Cliquez sur **New**.
3. Quand les affichages de fenêtre de Profile Management (général), se terminent ces étapes afin de placer le nom de profil, le nom de client, et le SSID :Saisissez le nom du profil dans le champ Profile Name.Cet exemple utilise *EAPAuth* comme nom de profil.Saisissez le nom du client dans le champ Client Name.Le nom du client est utilisé pour identifier le client sans fil dans le réseau WLAN. Cette configuration utilise *Client 3* pour le nom du client.Sous des noms de réseau, écrivez le SSID qui doit être utilisé pour ce profil.Le SSID est identique au SSID que vous avez configuré sur le WLC. Le SSID dans cet exemple est *802.1x*.



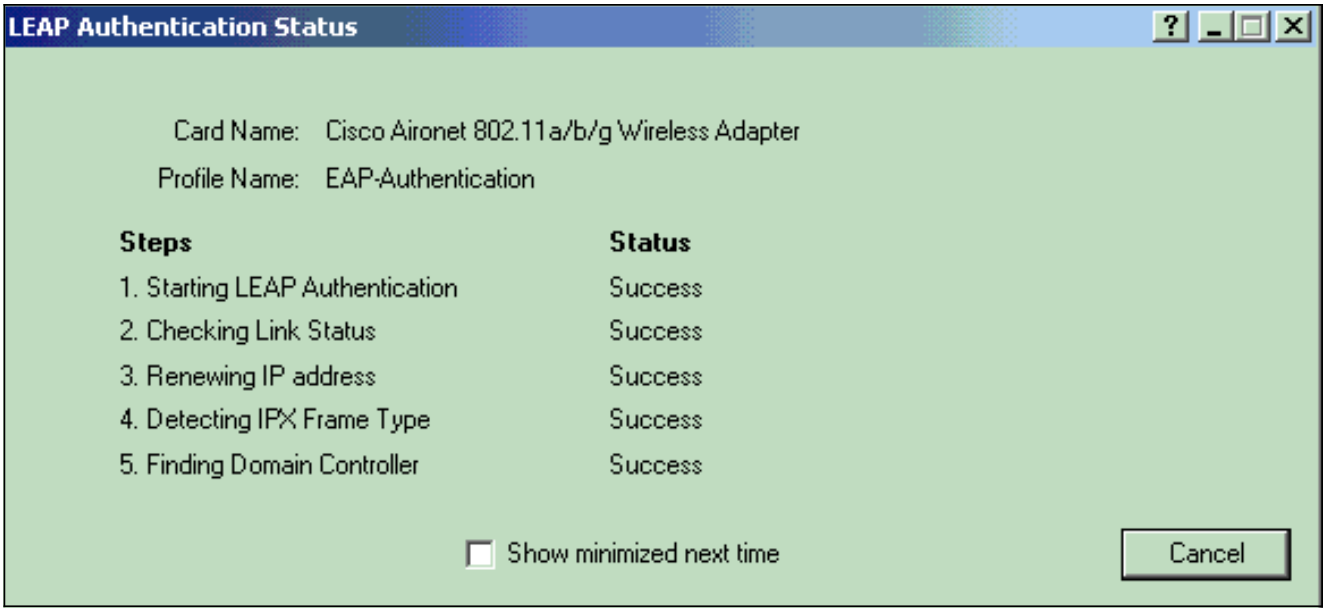
4. Cliquez sur l'onglet **Security**.



5. Cliquez sur la case d'option **802.1x**.
6. Dans la liste déroulante des types d'EAP 802.1x, choisissez le type d'EAP utilisé.
7. Cliquez sur **Configure** afin de configurer des paramètres spécifiques au type d'EAP sélectionné.

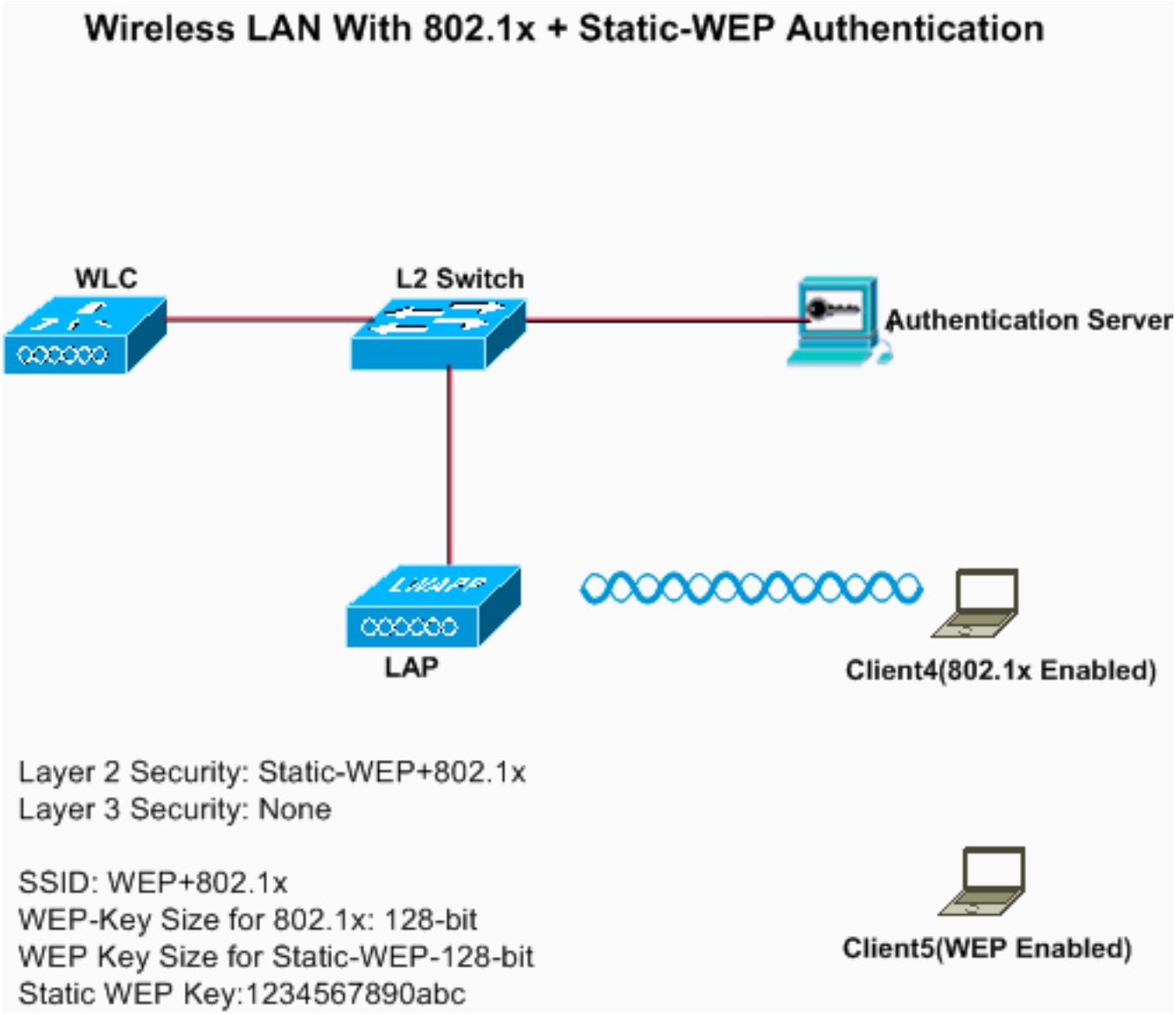


8. Cliquez sur **Apply**.Quand le SSID est activé, le client sans fil se connecte au WLAN à l'aide de l'authentification 802.1x. Des clés WEP dynamiques sont utilisées pour les sessions.



Authentification WEP statique et 802.1x

Cet exemple montre un WLAN configuré avec l'authentification WEP statique et 802.1x.



Complétez ces étapes afin de définir le WLC pour cette configuration :

1. Cliquez sur **WLANs** depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **New** pour configurer un nouveau WLAN.
3. Entrez l'ID de WLAN et le SSID de WLAN.Dans cet exemple, le WLAN est nommé *WEP+802.1x* et l'ID de WLAN est *4*.

4. Cliquez sur **Apply**.
5. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.Dans la liste déroulante de la couche 2, choisissez **Static-WEP+802.1x**.Ceci active l'authentification WEP statique et 802.1x pour ce WLAN.Sous les paramètres de serveur RADIUS, sélectionnez le serveur RADIUS qui sera utilisé pour authentifier les informations d'identification du client à l'aide de 802.1x et configurez le serveur RADIUS suivant les indications de l'exemple précédent.Sous les paramètres de WEP statique, sélectionnez la taille et l'index de clé WEP et entrez la clé de chiffrement WEP statique suivant les indications de l'image précédente.Choisissez d'autres paramètres selon vos exigences en termes de conception.Cet exemple utilise les valeurs par défaut.

Configurer le client sans fil pour WEP statique et 802.1x

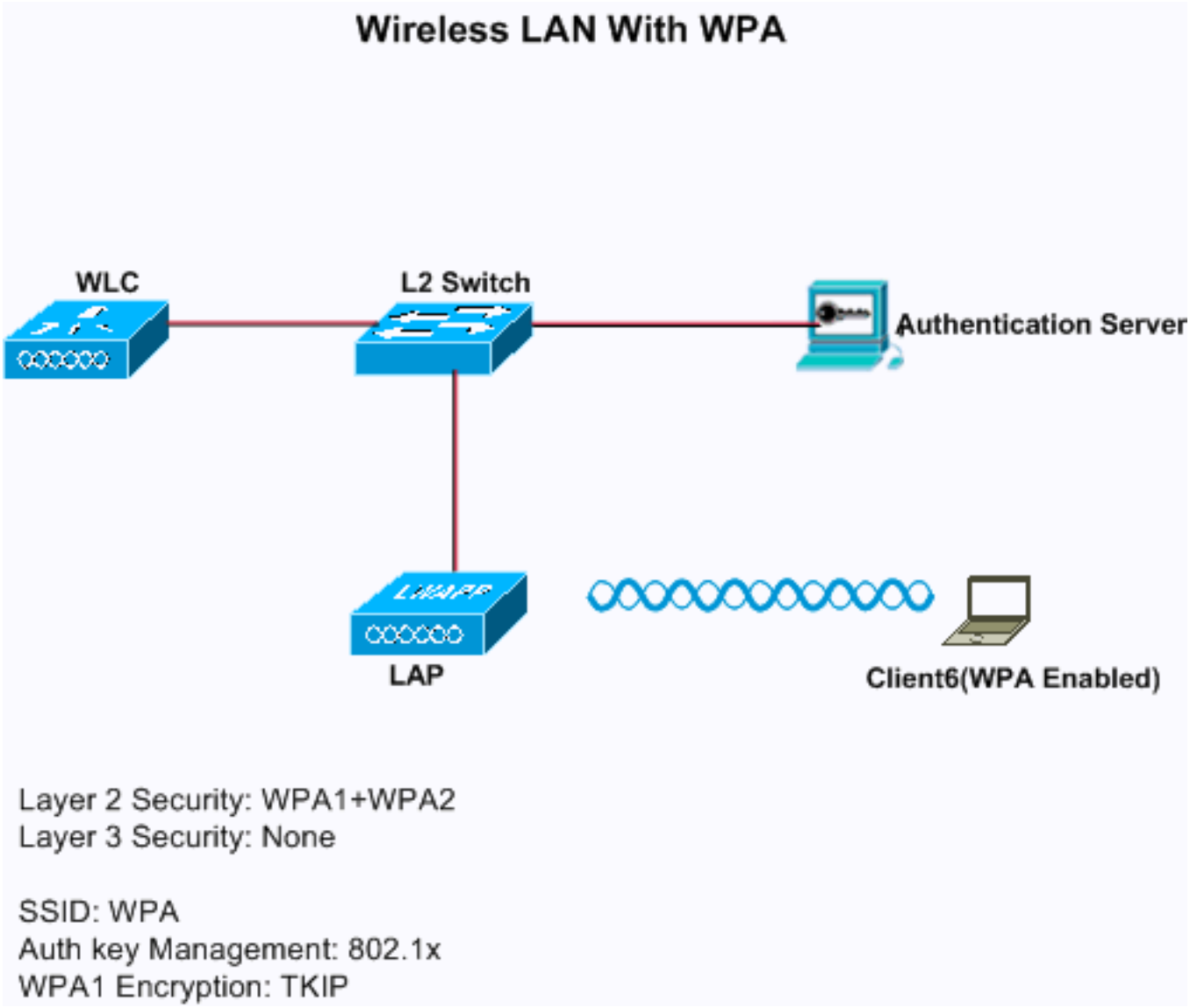
Consultez les sections Configurer le client sans fil pour l'authentification 802.1x et Configurer le client sans fil pour le WEP statique pour plus d'informations sur la façon de configurer le client sans fil.

Une fois que les profils de client sont créés, les clients qui sont configurés pour le WEP statique sont associés au LAP. Employez le SSID WEP+802.1x afin de vous connecter au réseau.

De même, les clients sans fil qui sont configurés pour utiliser l'authentification 802.1x sont authentifiés avec EAP et accèdent au réseau avec le même SSID WEP+802.1x.

Wi-Fi Protected Access

Cet exemple montre un WLAN qui est configuré avec WPA avec 802.1x.



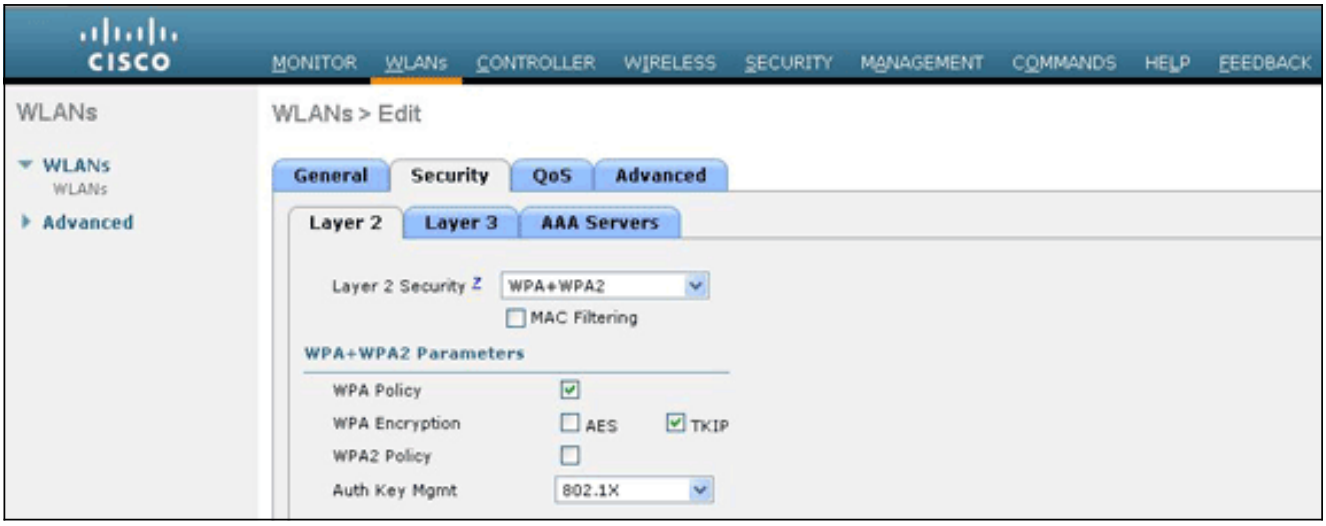
Configurer le WLC pour le WPA

Complétez ces étapes afin de définir le WLC pour cette configuration :

1. Cliquez sur **WLANs** depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **Go** pour configurer un nouveau WLAN.Choisissez le type et le nom du profil. Dans cet exemple, le WLAN est nommé *WPA* et l'ID de WLAN est *5*.

3. Cliquez sur **Apply**.

4. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.



Cliquez sur l'onglet **Security**, sur l'onglet **Layer 2** et choisissez **WPA1+WPA2** dans la liste déroulante de sécurité de la couche 2.Sous les paramètres WPA1+WPA2, activez la case à cocher **WPA1 Policy** afin d'activer WPA1, activez la case à cocher **WPA2 Policy** afin d'activer WPA2, ou activez les deux cases à cocher afin d'activer WPA1 et WPA2.La valeur par défaut est désactivée pour WPA1 et WPA2. Si vous laissez WPA1 et WPA2 désactivés, les points d'accès sont annoncés dans leurs balises et éléments d'informations de réponse de la sonde seulement pour la méthode de gestion des clés d'authentification que vous choisissez.Activez la case à cocher **AES** pour activer le chiffrement des données AES ou la case à cocher **TKIP** pour activer le chiffrement des données TKIP pour WPA1, WPA2, ou les deux.Les valeurs par défaut sont TKIP pour WPA1 et AES pour WPA2.Choisissez une de ces méthodes de gestion des clés dans la liste déroulante Auth Key Mgmt :*802.1X* — Si vous choisissez cette option, seuls les clients 802.1x sont pris en charge.*CCKM* — Si vous choisissez cette option, seulement des clients CCKM sont pris en charge, où des clients sont dirigés vers un serveur externe pour l'authentification.*PSK* — Si vous choisissez cette option, une clé pré-partagée est utilisée pour le WLC et le client. En outre, toutes les normes sont définies pour être utilisées avant les prénormes ; par exemple, WPA/WPA2 est prioritaire sur CCKM lorsqu'ils sont utilisés simultanément.*802.1X+CCKM* — Si vous choisissez cette option, CCKM ou clients de non-CCKM sont pris en charge (CCKM facultatif).Cet exemple utilise
802.1x.

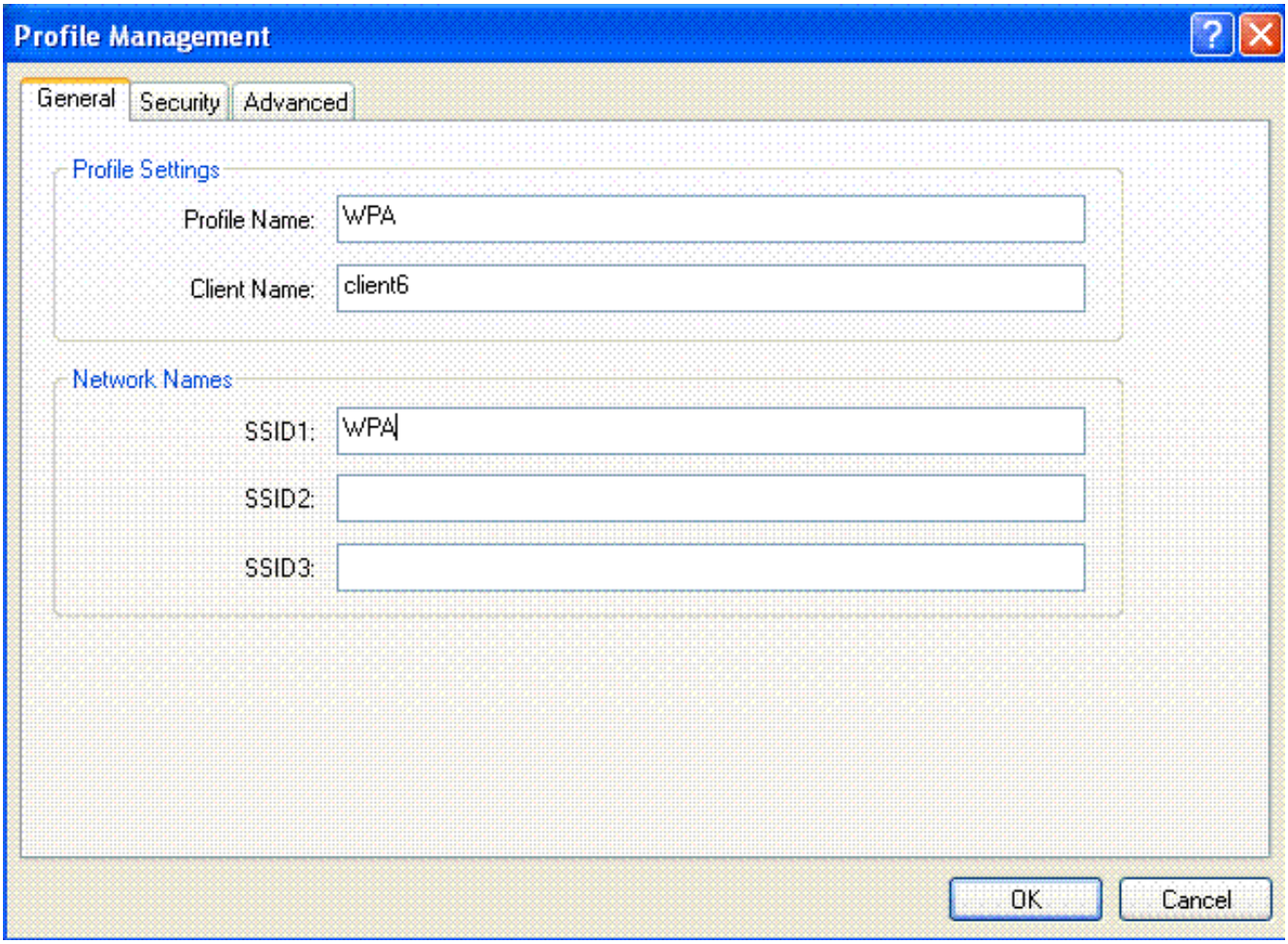
Remarque: Si vous choisissez PSK, choisissez **ascii** ou **hex** dans la liste déroulante de format PSK, puis entrez une clé prépartagée dans le champ vide. Les clés prépartagées WPA doivent contenir 8 à 63 caractères de texte ASCII ou 64 caractères hexadécimaux.

5. Cliquez sur **Apply** pour appliquer les modifications.

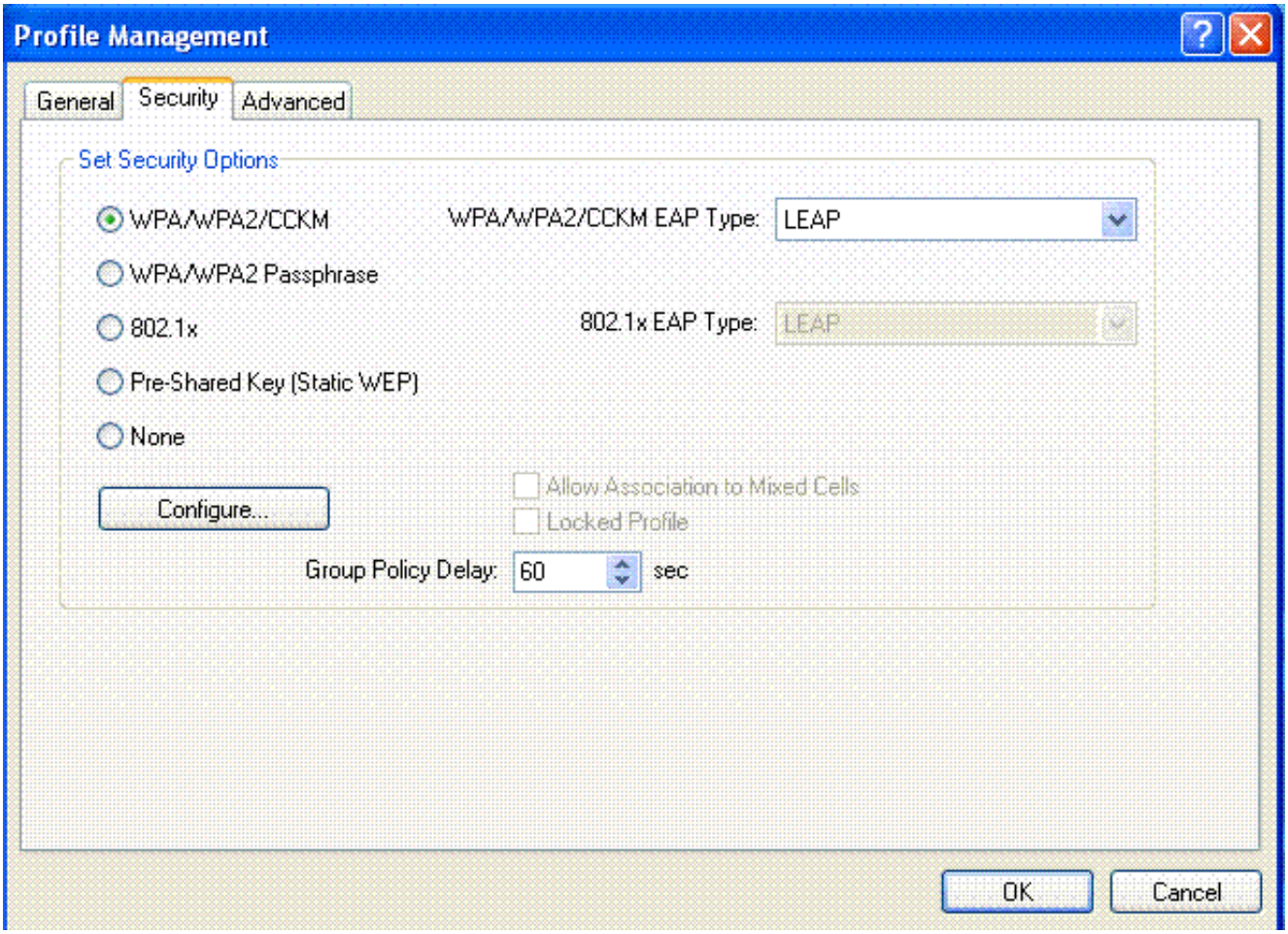
Configurer le client sans fil pour WPA

Terminez-vous ces étapes afin de configurer le client Sans fil de RÉSEAU LOCAL pour cette installation :

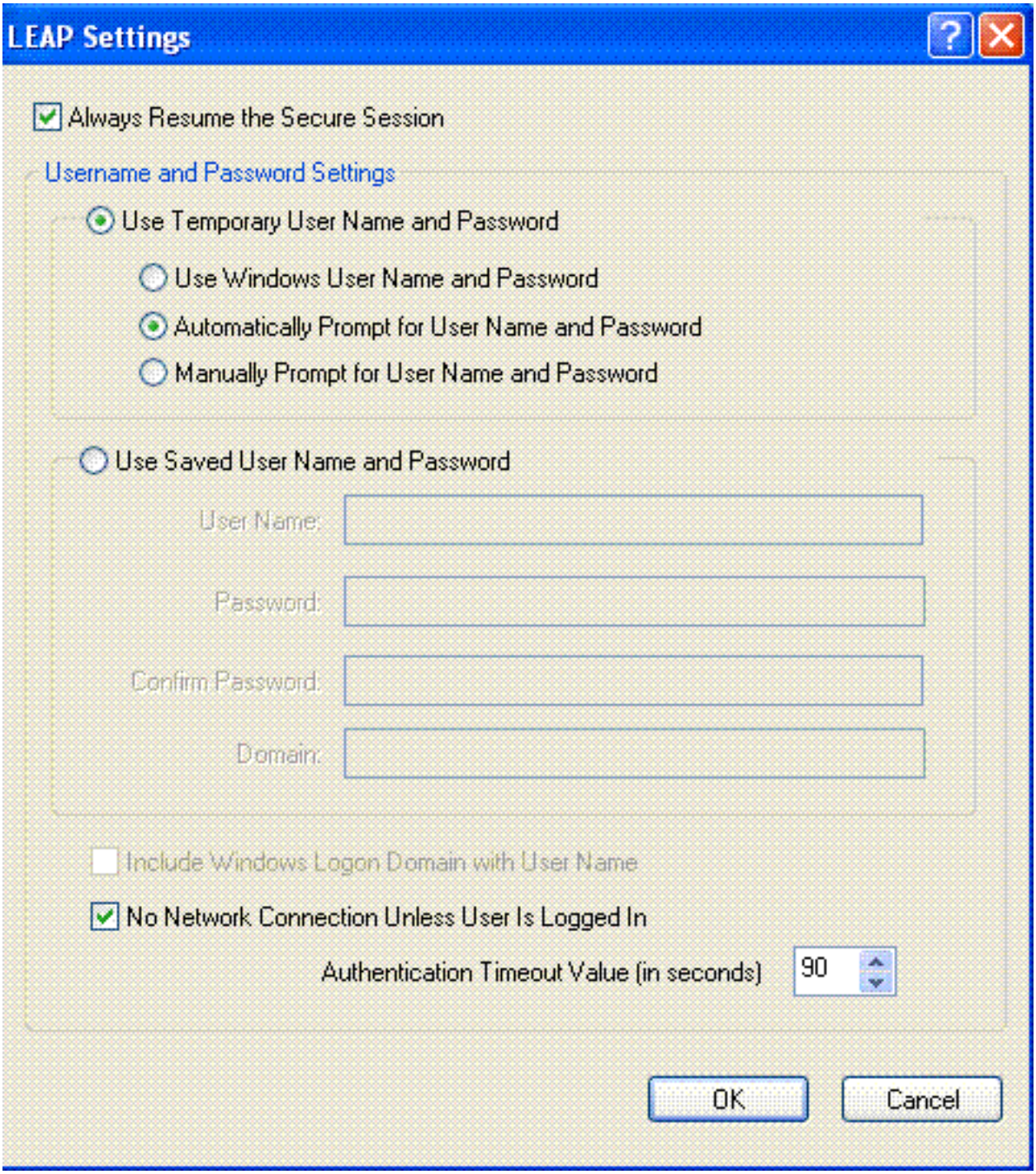
1. Dans la fenêtre Profile Management sur l'ADU, cliquez sur **New** afin de créer un nouveau profil.
2. Cliquez sur l'onglet **General** et entrez le nom de profil et le SSID que l'adaptateur client utilisera.Dans cet exemple, le nom de profil et le SSID sont *WPA*. Le SSID doit correspondre au SSID que vous avez configuré sur le WLC pour
WPA.



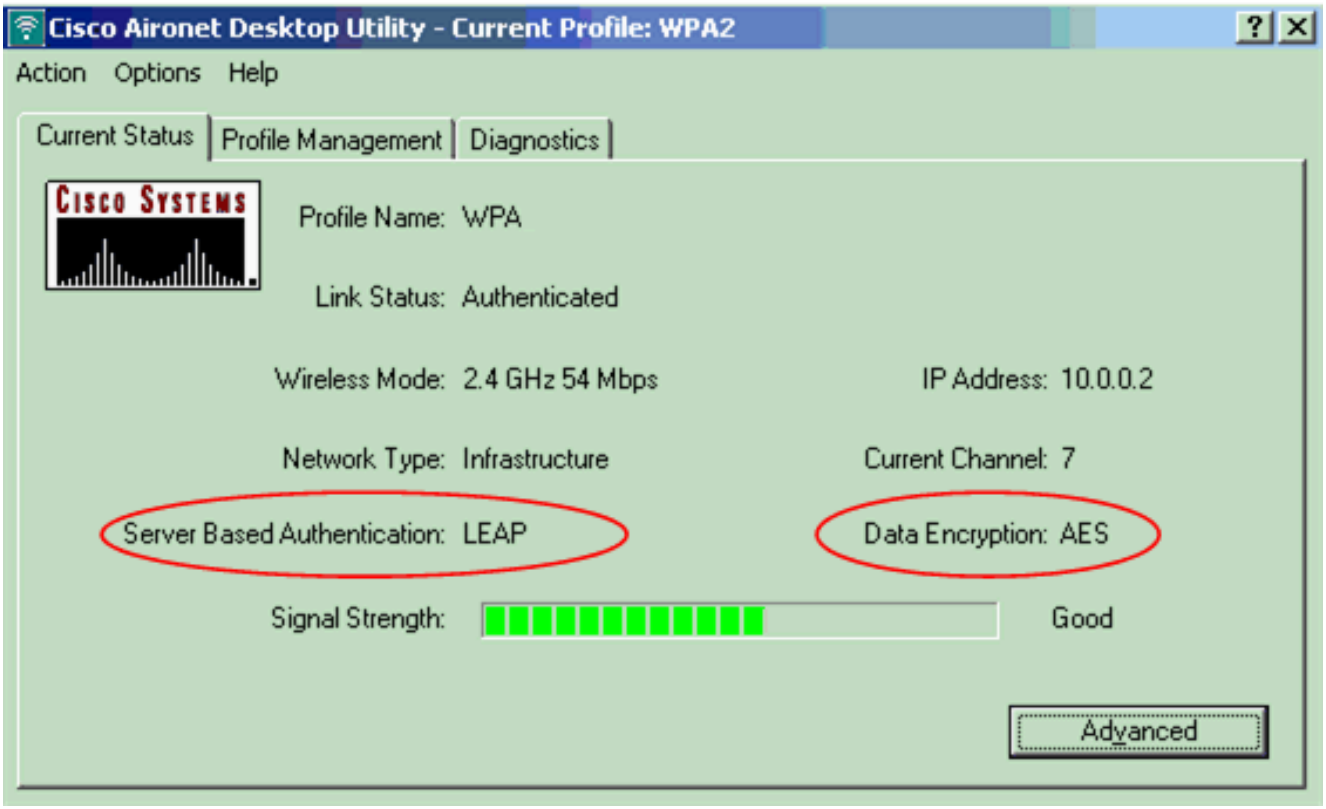
3. Sur l'onglet Security, cliquez sur la case d'option **WPA/WPA2/CCKM** et choisissez le type approprié d'EAP dans la liste déroulante des types d'EAP WPA/WPA2/CCKM. Cette étape active
WPA.



4. Cliquez sur **Configure** afin de définir les paramètres EAP spécifiques au type d'EAP sélectionné.

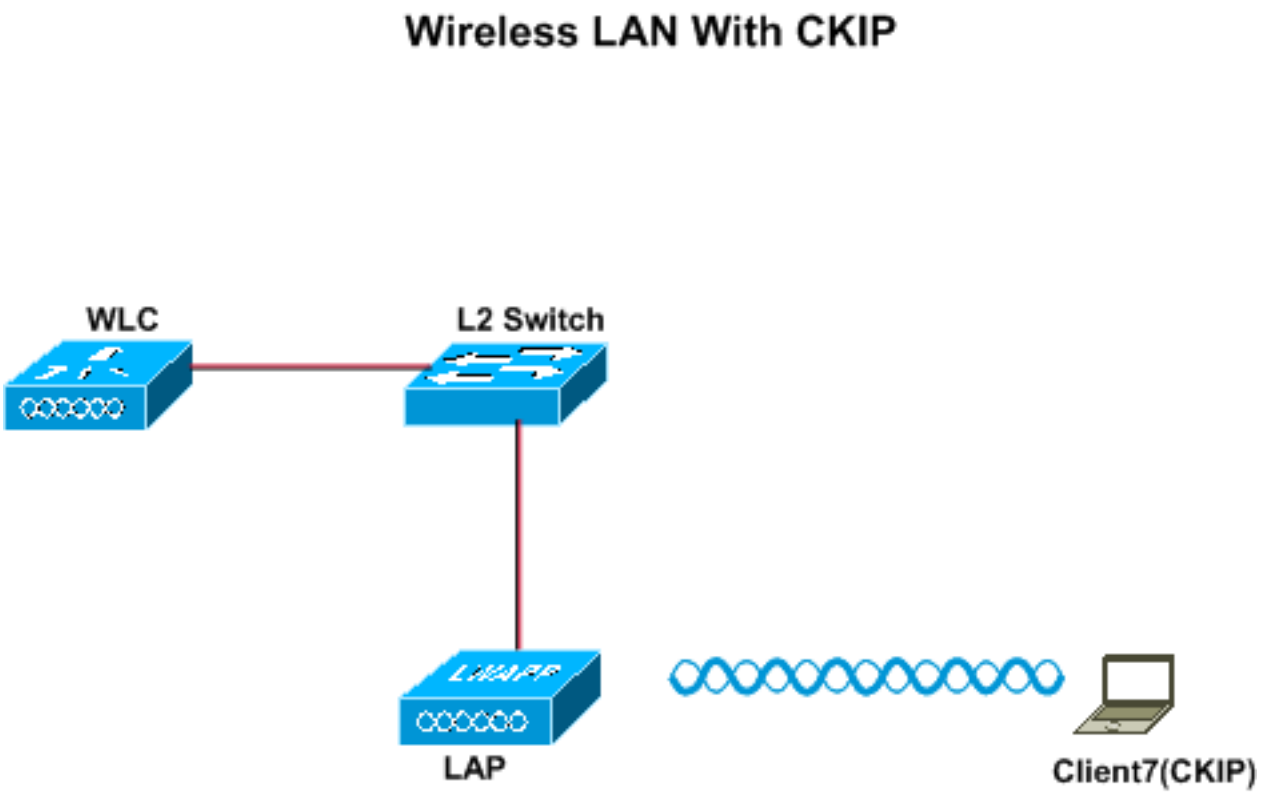


5. Cliquez sur **OK**.**Remarque:** Quand ce profil est activé, le client est authentifié à l'aide de 802.1x et quand l'authentification est réussie, le client se connecte au WLAN. Vérifiez l'état actuel de l'ADU afin de vérifier que le client utilise le chiffrement TKIP (chiffrement par défaut utilisé par WPA1) et l'authentification
EAP.



CKIP

Cet exemple montre un WLAN configuré avec CKIP.



Layer 2 Security: CKIP
Layer 3 Security: None
SSID: CKIP

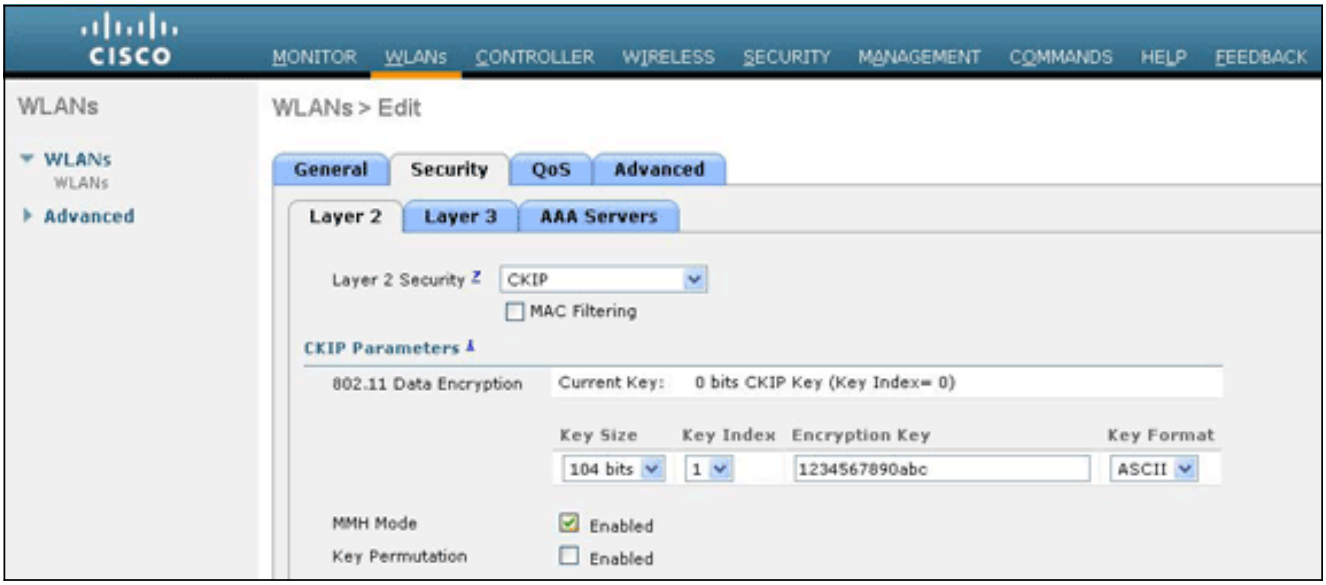
Configurer le WLC pour le CKIP

Complétez ces étapes afin de définir le WLC pour cette configuration :

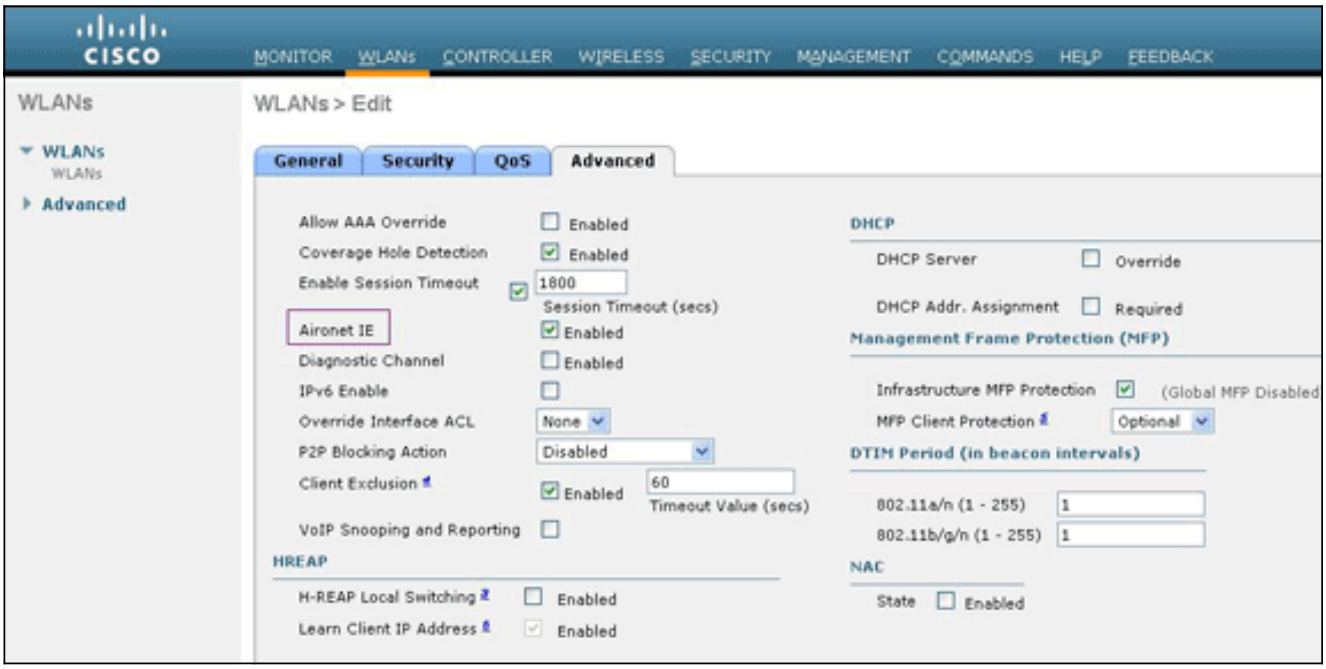
1. Cliquez sur **WLANs** depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **New** pour configurer un nouveau WLAN.Choisissez le type et le nom du profil. Dans cet exemple, le WLAN est nommé *CKIP* et l'ID de WLAN est *6*.

3. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.Dans la liste déroulante de la couche 2, choisissez **CKIP**.Cette étape active CKIP pour ce WLAN.Sous les paramètres CKIP, sélectionnez la taille et l'index de clé et entrez la clé de chiffrement

statique.La taille de la clé peut être de 40 bits, 104 bits ou 128 bits. L'index de clé peut être entre 1 et 4. Un seul index de clé WEP peut être appliqué à chaque WLAN. Puisqu'il y a seulement quatre index de clé WEP, seulement quatre WLAN peuvent être configurés pour le cryptage statique de la couche 2 WEP.Pour CKIP, choisissez l'option **MMH Mode**, l'option **Key Permutation**, ou les deux.**Remarque:** Un de ces paramètres ou chacun des deux devrait être sélectionné pour que CKIP fonctionne comme prévu. Si ces paramètres ne sont pas sélectionnés, le WLAN reste dans l'état désactivé.Dans cet exemple, la clé 104 bits est utilisée et la clé est
1234567890abc.



4. Choisissez d'autres paramètres selon vos exigences en termes de conception.Cet exemple utilise les valeurs par
défaut.

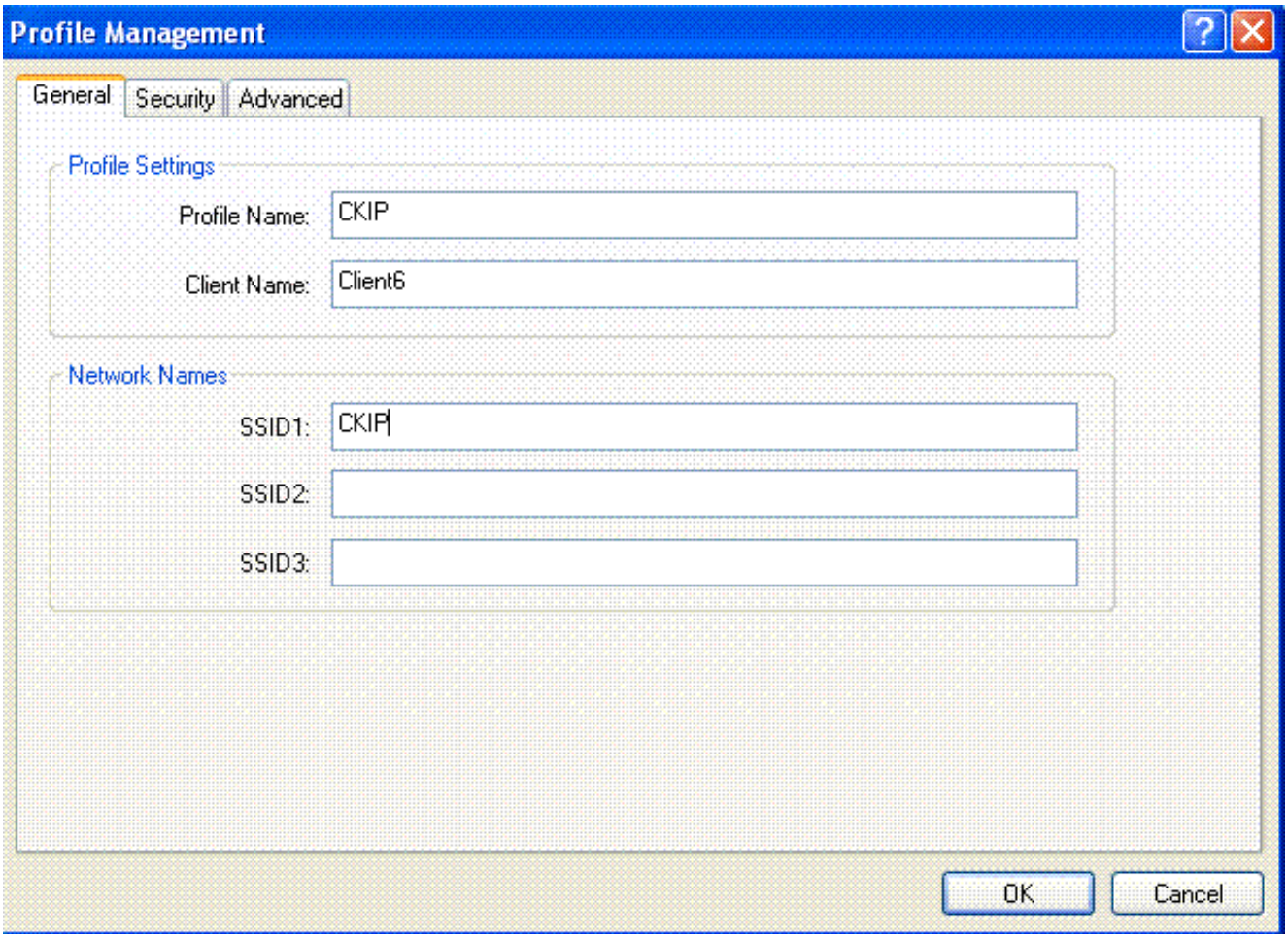


5. Cliquez sur **Apply**.**Remarque:** CKIP est fonctionnel sur les AP 1100, 1130 et 1200, mais pas 1000. L'élément d'information Aironet doit être activé pour que cette fonctionnalité fonctionne. CKIP développe les clés de chiffrement à 16 octets.

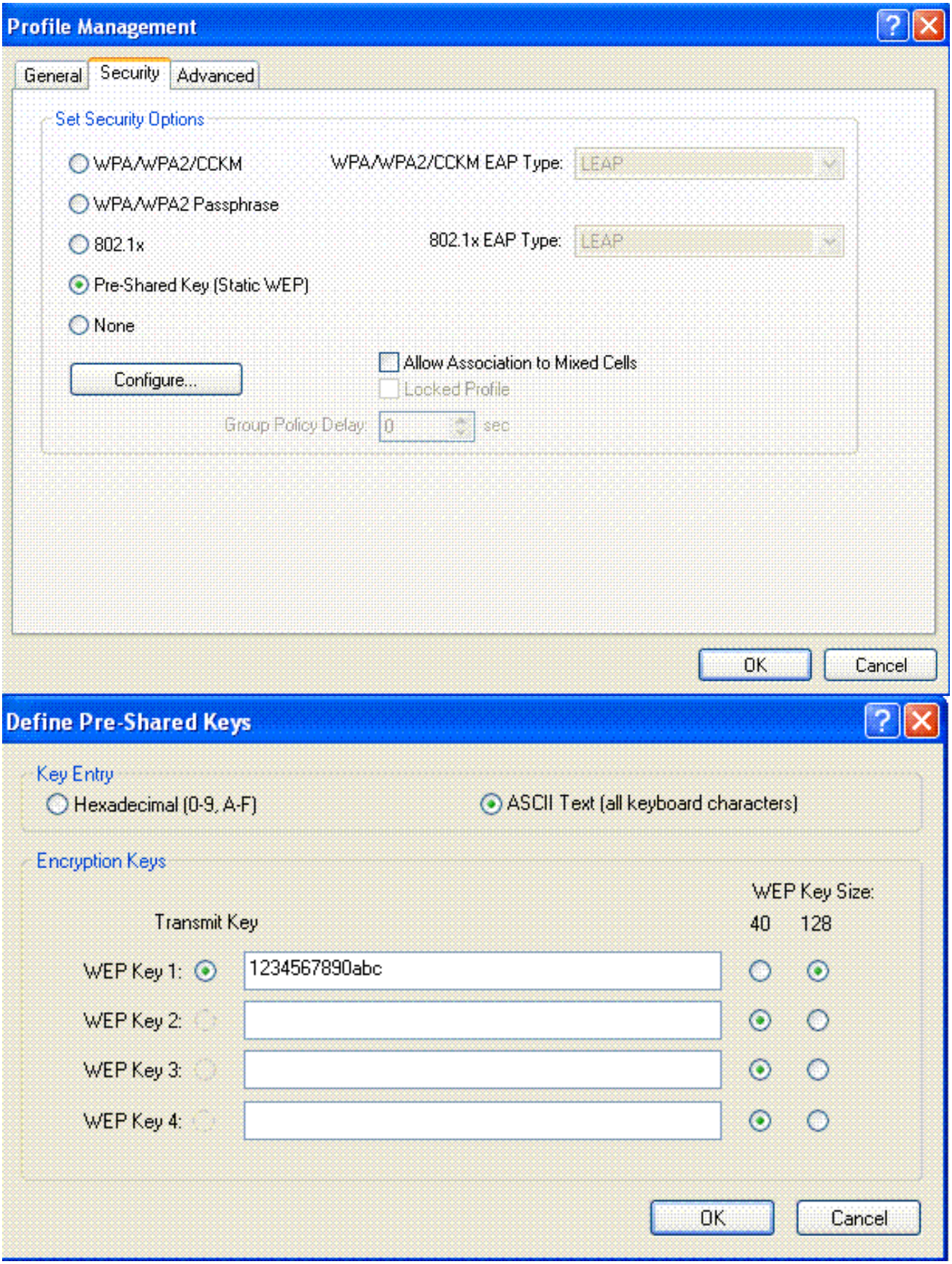
Configurer le client sans fil pour CKIP

Effectuez ces étapes afin de définir le client LAN sans fil pour cette configuration :

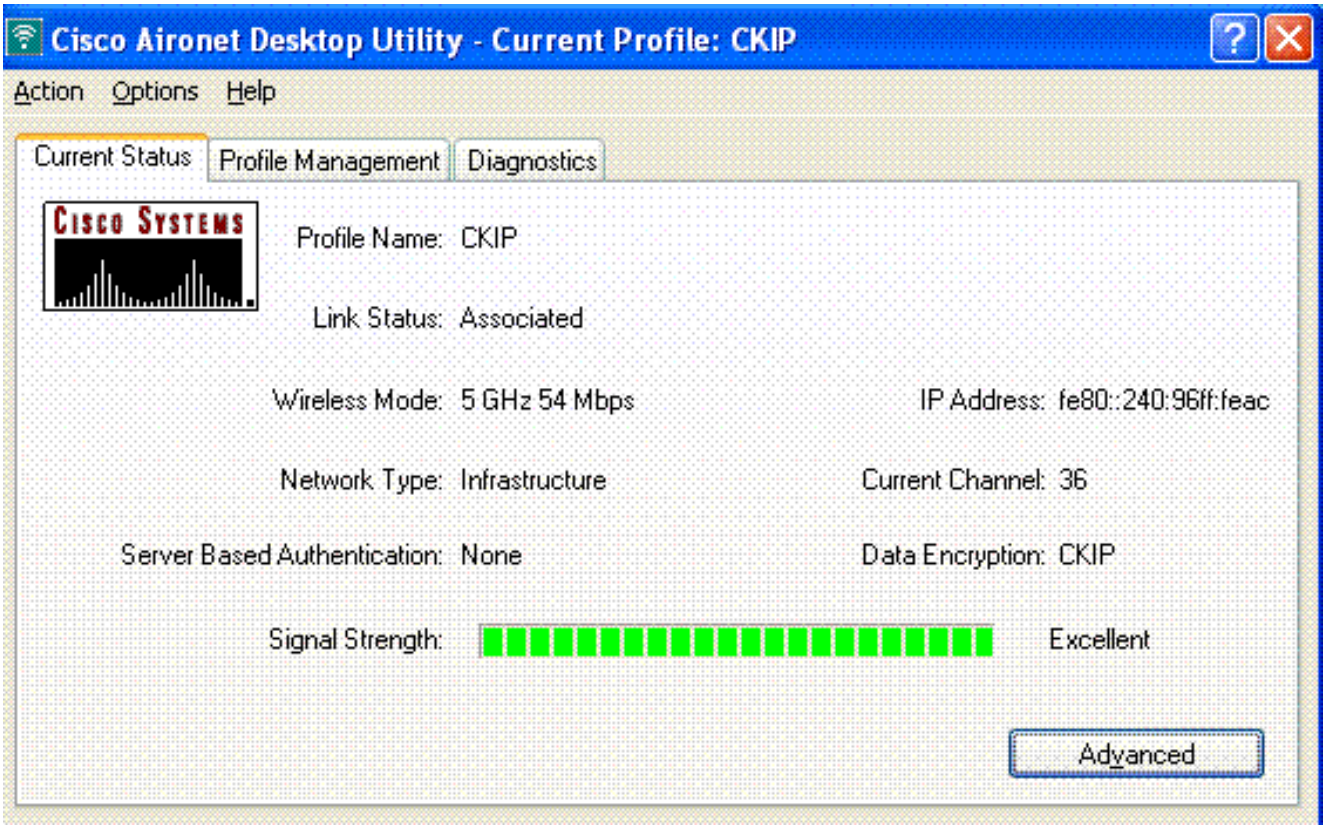
1. Afin de créer un nouveau profil, cliquez sur l'onglet **Profile Management** sur l'ADU, puis cliquez sur **New**.
2. Quand les affichages de fenêtre de Profile Management (général), se terminent ces étapes afin de placer le nom de profil, le nom de client, et le SSID :Saisissez le nom du profil dans le champ Profile Name.Cet exemple utilise *CKIP* comme nom de profil.Saisissez le nom du client dans le champ Client Name.Le nom du client est utilisé pour identifier le client sans fil dans le réseau WLAN. Cette configuration utilise *Client6* pour le nom du client.Sous Network Names, entrez le SSID qui doit être utilisé pour ce profil.Le SSID est identique au SSID que vous avez configuré sur le WLC. Le SSID dans cet exemple est *CKIP*.



3. Cliquez sur l'onglet **Security**.
4. Choisissez **Pre-Shared Key (Static WEP)** sous Set Security Options, cliquez sur **Configure** et définissez la taille de clé WEP et la clé WEP.Ces valeurs doivent correspondre à la clé WEP configurée sur le WLC pour ce WLAN.



5. Cliquez sur **OK**.Quand le SSID est activé, le client sans fil négocie avec le LAP et le WLC pour utiliser CKIP pour le chiffrement des paquets.



Solutions de sécurité de la couche 3

Stratégie Web (authentification Web et relais Web)

Consultez Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil pour plus d'informations sur la façon d'activer l'authentification Web dans un réseau WLAN.

Consultez Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil pour plus d'informations sur la façon de configurer l'authentification Web externe et l'authentification de relais Web dans un WLAN.

Consultez Exemple de configuration du relais Web sur un contrôleur de réseau local sans fil pour plus d'informations sur la façon d'activer le relais Web dans un réseau WLAN.

Le mécanisme de page de démarrage est un mécanisme de sécurité de la couche 3 introduit dans la version WLC 5.0 utilisée pour l'authentification du client. Consultez Exemple de configuration de redirection de page de démarrage sur les contrôleurs de réseau local sans fil pour plus d'informations.

Relais VPN

Consultez Exemple de configuration d'un VPN client sur un réseau local sans fil avec WLC pour plus d'informations sur la façon de configurer le relais VPN dans un WLAN.

Dépanner

Dépannage des commandes

Vous pouvez utiliser ces commandes **debug** pour dépanner votre configuration.

Commandes debug pour l'authentification Web :

- **debug mac addr <adresse-MAC-client xx:** *xx : xx : xx : xx :* ***xx>*** — Configure le débogage d'adresse MAC pour le client.
- **debug aaa all enable** — Configure le débogage de tous les messages AAA.
- **debug pem state enable** — Configure le débogage de l'ordinateur d'état de gestionnaire des stratégies
- **debug pem events enable** — Configure le débogage des événements de gestionnaire des stratégies.
- **debug dhcp message enable** — Employez cette commande afin d'afficher les informations de débogage sur les activités de client de protocole de configuration dynamique d'hôte (DHCP) et contrôler l'état des paquets DHCP.
- **debug dhcp packet enable** — Employez cette commande afin d'afficher les informations de niveau de paquet DHCP.
- **debug pm ssh-appgw enable** — Configure le débogage des passerelles d'application.
- **debug pm ssh-tcp enable** — Configure le débogage de la gestion TCP de gestionnaire des stratégies

Commandes debug pour WEP : Aucun débogage pour le WEP parce qu'il est effectué au niveau de l'AP, activez **debug dot11 all enable**.

Commandes debug pour la mise en cache 802.1X/WPA/RSN/PMK :

- **debug mac addr <adresse-MAC-client xx:** *xx : xx : xx : xx :* ***xx>*** — Configure le débogage d'adresse MAC pour le client.
- **debug dot1x all enable** — Employez cette commande afin d'afficher les informations de débogage 802.1X.
- **debug dot11 all enable** — Employez cette commande afin d'activer le débogage des fonctions radio.
- **debug pem events enable** — Configure le débogage des événements de gestionnaire des stratégies.
- **debug pem state enable** — Configure le débogage de l'ordinateur d'état de gestionnaire des stratégies.
- **debug dhcp message enable** — Employez cette commande afin d'afficher les informations de débogage sur les activités de client de protocole de configuration dynamique d'hôte (DHCP) et contrôler l'état des paquets DHCP.
- **debug dhcp packet enable** — Employez cette commande afin d'afficher les informations de niveau de paquet DHCP.
- **debug mobility handoff enable (for intra-switch roaming)** — Configure le débogage des paquets de mobilité.
- **show client detail <mac>** — Affiche les informations détaillées pour un client par adresse MAC. Vérifiez la configuration du délai d'expiration de session WLAN et RADIUS.

Informations connexes

- Exemple de configuration de restriction de l'accès au réseau local sans fil sur SSID avec WLC et Cisco Secure ACS

- Exemple de configuration de listes de contrôle d'accès sur un contrôleur de réseau local sans fil
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems