Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil (WLC)

Contenu

Introduction

Ce document explique comment configurer le contrôleur de réseau local sans fil (WLC) pour l'authentification Extensible Authentication Protocol (EAP) avec un serveur RADIUS externe. Cet exemple de configuration utilise Cisco Secure Access Control Server (ACS) comme serveur RADIUS externe pour valider les identifiants de l'utilisateur.

Conditions préalables

Conditions requises

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

- Connaissance de base de la configuration des points d'accès légers (AP) et des WLC Cisco.
- Connaissance de base du protocole LWAPP (Lightweight AP Protocol).
- Connaissance du mode de configuration d'un serveur RADIUS externe comme Cisco Secure ACS.

Composants utilisés

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

- AP légers de la gamme Cisco Aironet 1232AG
- WLC de la gamme Cisco 4400 qui exécute le firmware 5.1
- Cisco Secure ACS exécutant la version 4.1
- Adaptateur client Cisco Aironet 802.11 a/b/g
- Cisco Aironet Desktop Utility (ADU) exécutant le microprogramme 4.2

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.

Configurez

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

Remarque: Utilisez l'outil de recherche de commande (réservé aux clients inscrits) pour plus d'informations sur les commandes utilisées dans ce document.

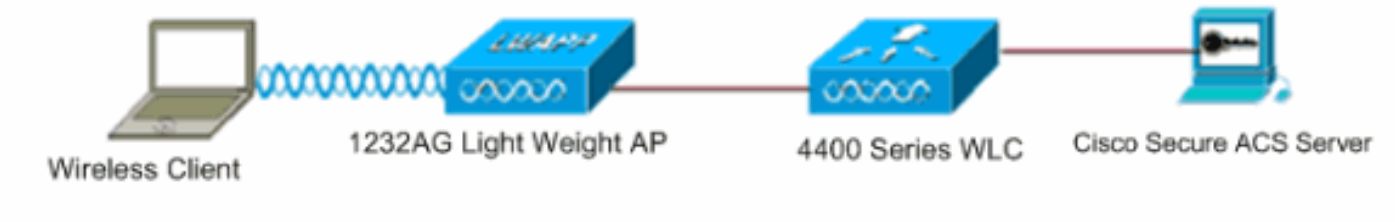
Complétez ces étapes pour configurer les périphériques pour l'authentification EAP :

1. Configurer le WLC pour l'opération de base et enregistrer les points d'accès légers sur le contrôleur.
2. Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe.
3. Configurer les paramètres WLAN.
4. Configurer Cisco Secure ACS en tant que serveur RADIUS externe et créer une base de données utilisateur pour l'authentification des clients.

Diagramme du réseau

Dans cette configuration, un WLC Cisco 4400 et un point d'accès léger sont connectés via un concentrateur. Un serveur RADIUS externe (Cisco Secure ACS) est également connecté au même concentrateur. Tous les périphériques se trouvent dans le même sous-réseau. Le point d'accès est d'abord enregistré sur le contrôleur. Vous devez configurer le WLC et le point d'accès pour l'authentification Lightweight Extensible Authentication Protocol (LEAP). Les clients qui se

connectent au point d'accès utilisent une authentification LEAP pour réaliser l'association. Cisco Secure ACS sert à l'exécution de l'authentification RADIUS.



Configurer le WLC pour l'opération de base et enregistrer les points d'accès légers sur le contrôleur

Pour configurer le WLC pour l'opération de base, utilisez l'assistant de configuration de démarrage sur l'interface de ligne de commande (CLI). Pour configurer le WLC, vous pouvez également utiliser l'interface graphique (GUI). Ce document explique comment configurer le WLC avec l'assistant de configuration de démarrage sur le CLI.

Lors du premier démarrage du WLC, celui-ci ouvre directement l'assistant de configuration de démarrage. Utilisez l'assistant de configuration pour configurer des paramètres de base. Vous pouvez exécuter l'assistant sur le CLI ou l'interface graphique (GUI). Ce résultat montre un exemple d'assistant de configuration de démarrage sur le CLI :

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1 Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): ***** Management Interface IP Address:
10.77.244.204 Management Interface Netmask: 255.255.255.224 Management Interface Default Router:
10.77.244.220 Management Interface VLAN Identifier (0 = untagged): Management Interface Port Num
[1 to 4]: 1 Management Interface DHCP Server IP Address: 10.77.244.220 AP Manager Interface IP
Address: 10.77.244.205 AP-Manager is on Management subnet, using same values AP Manager
Interface DHCP Server (10.77.244.220): Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group
Name: Test Network Name (SSID): Cisco123 Allow Static IP Addresses [YES][no]: yes Configure a
RADIUS Server now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS
server. Please see documentation for more details. Enter Country Code (enter 'help' for a list
of countries) [US]: Enable 802.11b Network [YES][no]: yes Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes Enable Auto-RF [YES][no]: yes Configuration saved!
Resetting system with new configuration..
```

Ces paramètres configurent le WLC pour l'opération de base. Dans cet exemple de configuration, le WLC utilise **10.77.244.204** comme adresse IP de l'interface de gestion et **10.77.244.205** comme adresse IP de l'interface du gestionnaire des points d'accès.

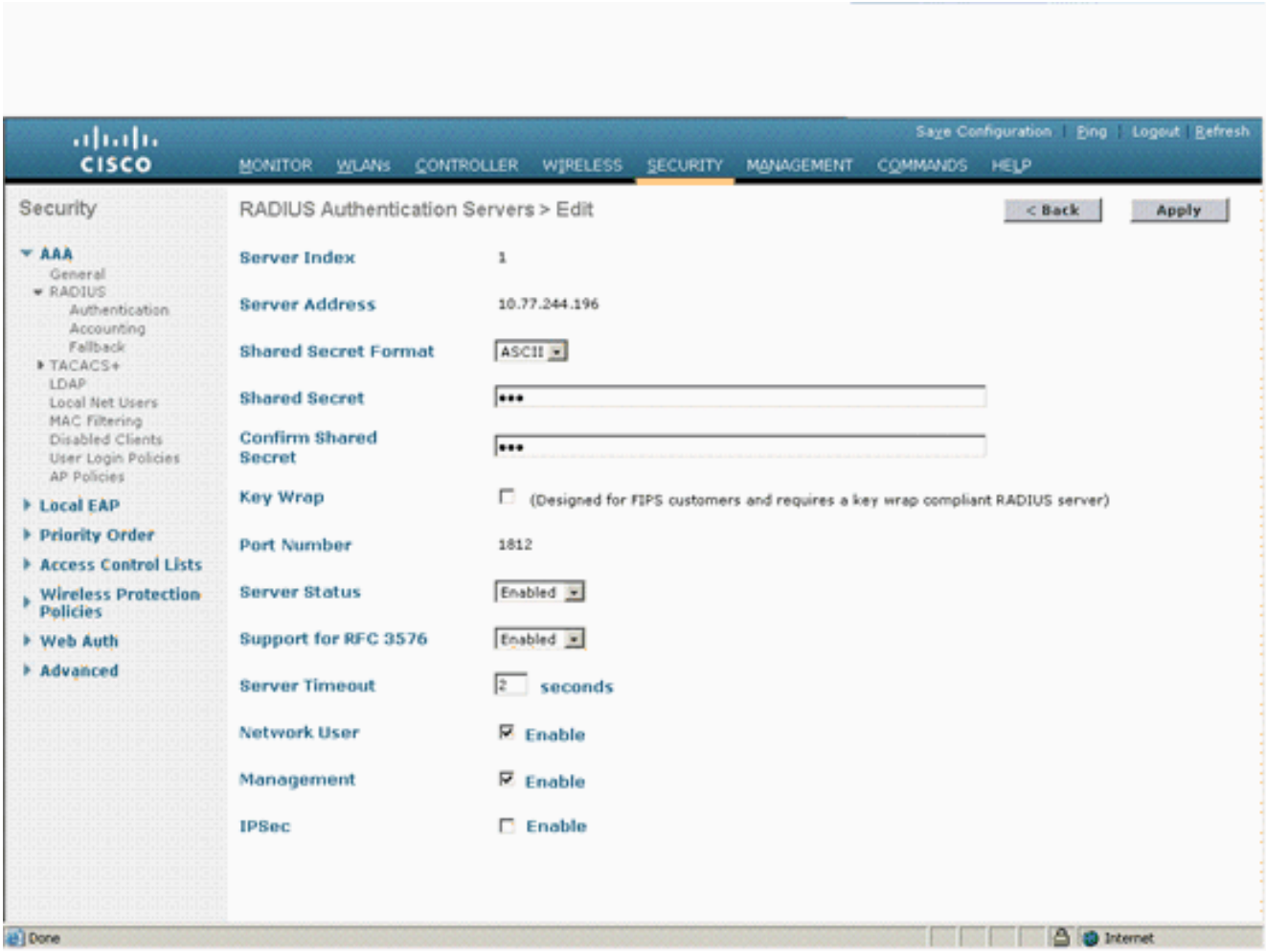
Avant que toutes les autres fonctionnalités ne puissent être configurées sur le WLC, les points d'accès légers doivent être enregistrés sur le WLC. Ce document suppose que les points d'accès légers sont enregistrés sur le WLC. Pour plus d'informations, consultez la section Enregistrement d'un point d'accès léger (LAP) sur un contrôleur de réseau local sans fil (WLC).

Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe

WLC doit être configuré afin de transférer les identifiants de l'utilisateur à un serveur RADIUS externe. Le serveur RADIUS externe alors valide les identifiants utilisateurs et permet d'accéder aux clients sans fil.

Complétez ces étapes pour configurer le WLC pour un serveur RADIUS externe :

1. Sélectionnez **Security** et **RADIUS Authentication** depuis la GUI du contrôleur pour afficher la page des serveurs d'authentification RADIUS. Cliquez alors sur **New** afin de définir un serveur
RADIUS.



2. Définissez les paramètres du serveur RADIUS sur la page RADIUS Authentication Servers > New. Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du serveur.Les cases à cocher Network User et Management déterminent si l'authentification RADIUS s'applique aux utilisateurs réseau et à la gestion WLC. Cet exemple utilise Cisco Secure ACS comme serveur RADIUS avec l'adresse IP 10.77.244.196.
3. Le serveur RADIUS peut maintenant être utilisé par le WLC pour l'authentification. Vous pouvez rechercher le serveur RADIUS répertorié en choisissant **Security > Radius > Authentication**.

RFC 3576 est pris en charge sur le serveur RADIUS Cisco CNS Access Registrar (CAR), mais pas sur la version 4.0 ni les versions antérieures du serveur Cisco Secure ACS.Vous

pouvez également utiliser la fonctionnalité du serveur RADIUS local afin d'authentifier des utilisateurs. Le serveur RADIUS local a été commercialisé avec le code de version 4.1.171.0. Les WLC qui exécutent les versions précédentes n'ont pas la fonctionnalité de serveur RADIUS local. L'authentification EAP locale est une méthode qui permet d'authentifier localement des utilisateurs et des clients sans fil. Cette méthode est conçue pour une utilisation dans les bureaux distants qui veulent conserver la connectivité avec les clients sans fil lorsque le système principal est perturbé ou que le serveur d'authentification externe est en panne. L'authentification EAP locale récupère les identifiants de l'utilisateur à partir de la base de données des utilisateurs locaux ou de la base de données LDAP principale pour authentifier les utilisateurs. Elle prend en charge les authentifications LEAP, EAP-FAST avec PAC, EAP-FAST avec certificats et EAP-TLS entre le contrôleur et les clients sans fil.Cette méthode est conçue comme un système d'authentification de secours. Si des serveurs RADIUS sont configurés sur le contrôleur, le contrôleur tente d'abord d'authentifier les clients sans fil avec les serveurs RADIUS. L'authentification EAP locale est utilisée uniquement si aucun serveur RADIUS n'est détecté, soit parce que les serveurs RADIUS ont expiré, soit parce qu'aucun serveur RADIUS n'a été configuré.Pour plus d'informations, consultez la section Exemple de configuration d'authentification EAP locale sur le contrôleur de réseau local sans fil avec un serveur EAP-FAST et LDAP.

Configurer les paramètres WLAN

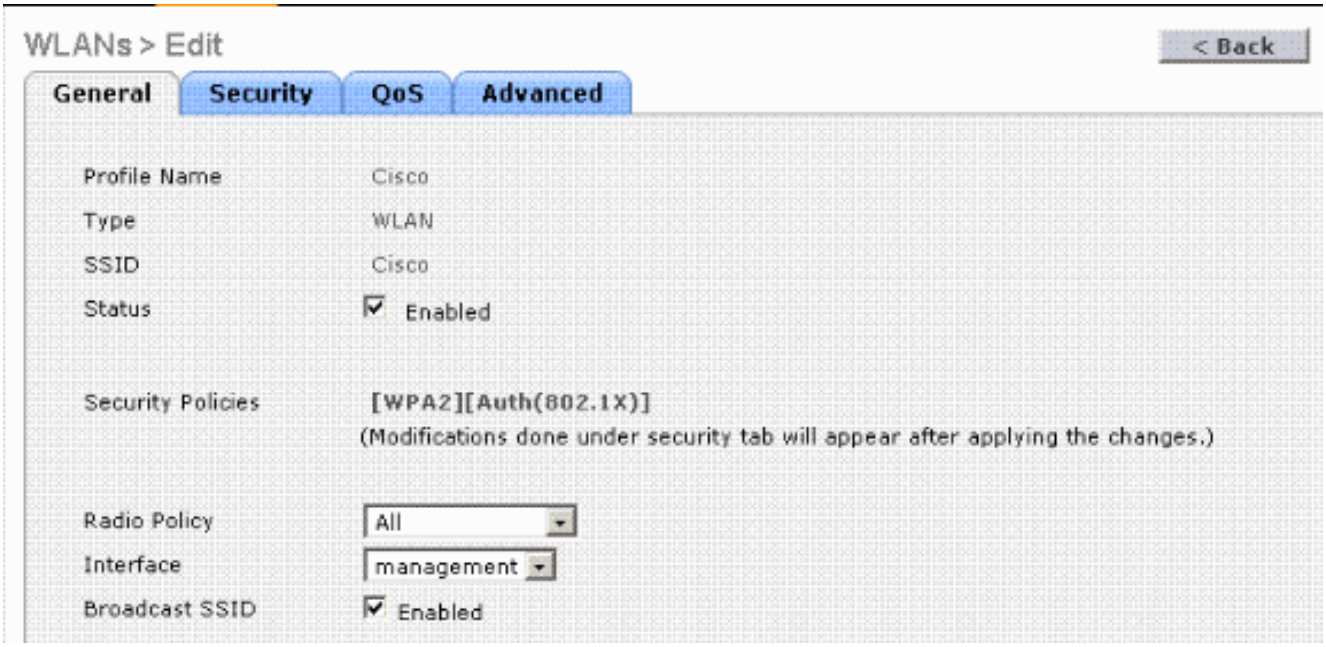
Configurez ensuite le WLAN que les clients utilisent pour se connecter au réseau sans fil. Une fois les paramètres de base pour le WLC configurés, le SSID du WLAN est également configuré. Vous pouvez utiliser ce SSID pour le WLAN ou créer un nouveau SSID. Dans cet exemple, vous créez un nouveau SSID.

Remarque: vous pouvez configurer jusqu'à seize WLAN sur le contrôleur. La solution WLAN de Cisco peut contrôler jusqu'à seize WLAN pour les points d'accès légers. Des stratégies de sécurité uniques peuvent être affectées à chacun des WLAN. Les points d'accès légers diffusent tous les SSID WLAN actifs de la solution WLAN de Cisco et appliquent les stratégies que vous définissez pour chaque WLAN.

Complétez ces étapes pour configurer un nouveau WLAN et ses paramètres associés :

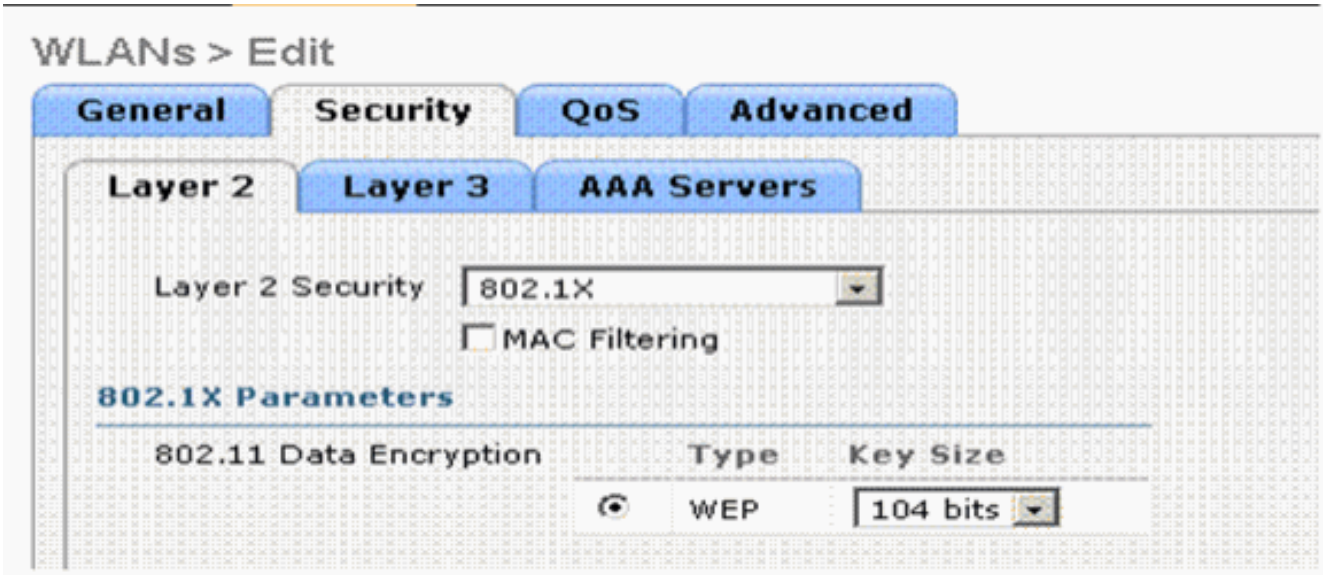
1. Cliquez sur les **WLAN** de la GUI du contrôleur afin d'afficher la page des WLAN.Cette page répertorie les WLAN qui existent sur le contrôleur.
2. Sélectionnez **New** afin de créer un nouveau WLAN. Entrez le nom du profil et le SSID du WLAN, puis cliquez sur **Apply**. Cet exemple utilise Cisco comme SSID.

3. Une fois que vous avez créé un nouveau WLAN, la page WLAN > Edit du nouveau WLAN apparaît. Sur cette page, vous pouvez définir divers paramètres spécifiques à ce WLAN, comme des stratégies générales, des stratégies de sécurité, des stratégies de qualité de service (QoS) et d'autres paramètres
avancés.

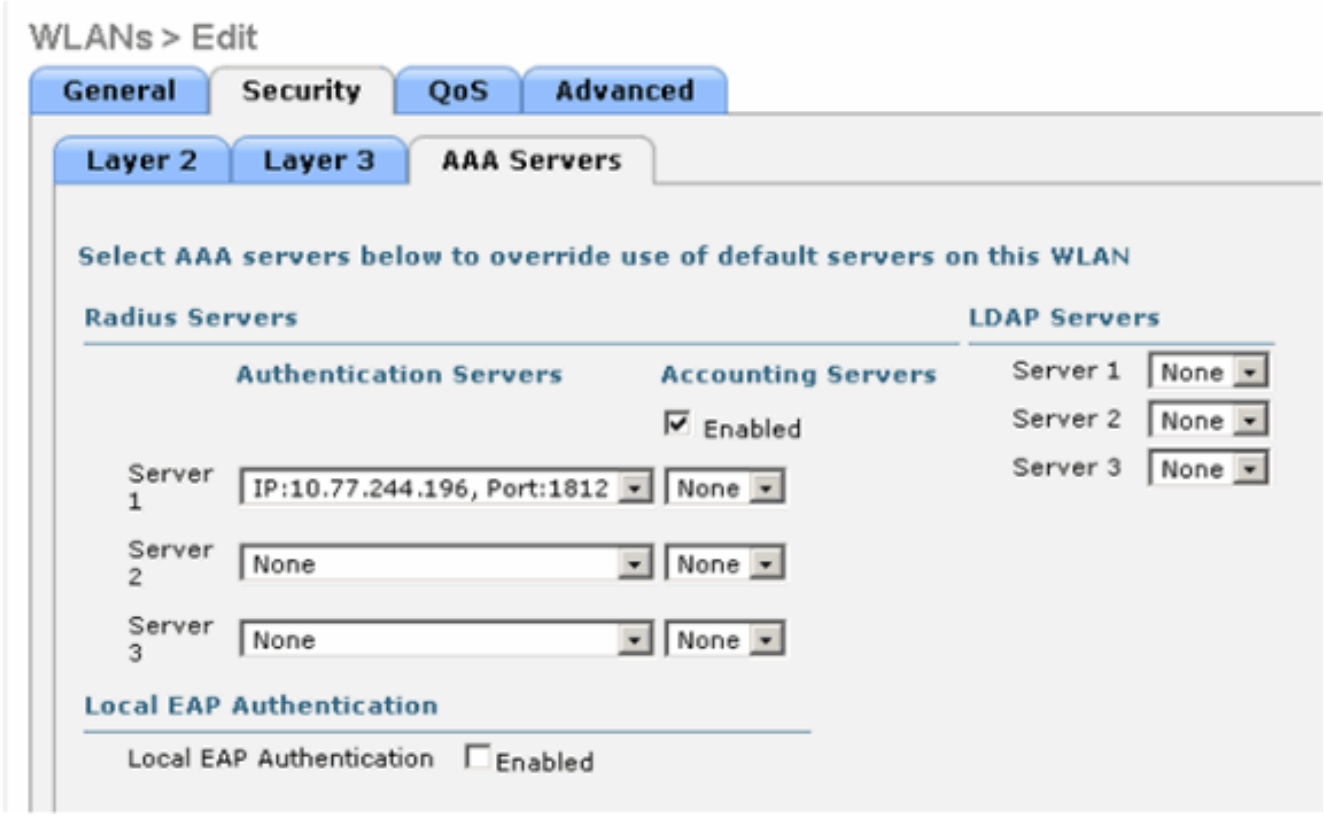


Choisissez l'interface appropriée dans le menu déroulant. Les autres paramètres peuvent être modifiés sur les conditions requises du réseau WLAN.Cochez la case **Status** sous l'option General Policies afin d'activer le WLAN.

4. Cliquez sur l'onglet **Security** et sélectionnez **Layer 2 Security**. Dans le menu déroulant Layer 2 Security, sélectionnez **802.1x**. Dans les paramètres 802.1x, choisissez la taille de clé WEP. Cet exemple utilise une clé WEP de 128 bits, qui est la clé WEP de 104 bits plus le vecteur d'initialisation de
24 bits.



5. Cliquez sur l'onglet **AAA Servers**. Dans le menu déroulant Authentication Servers (RADIUS), sélectionnez le serveur RADIUS approprié. Ce serveur est utilisé pour authentifier les clients sans
fil.

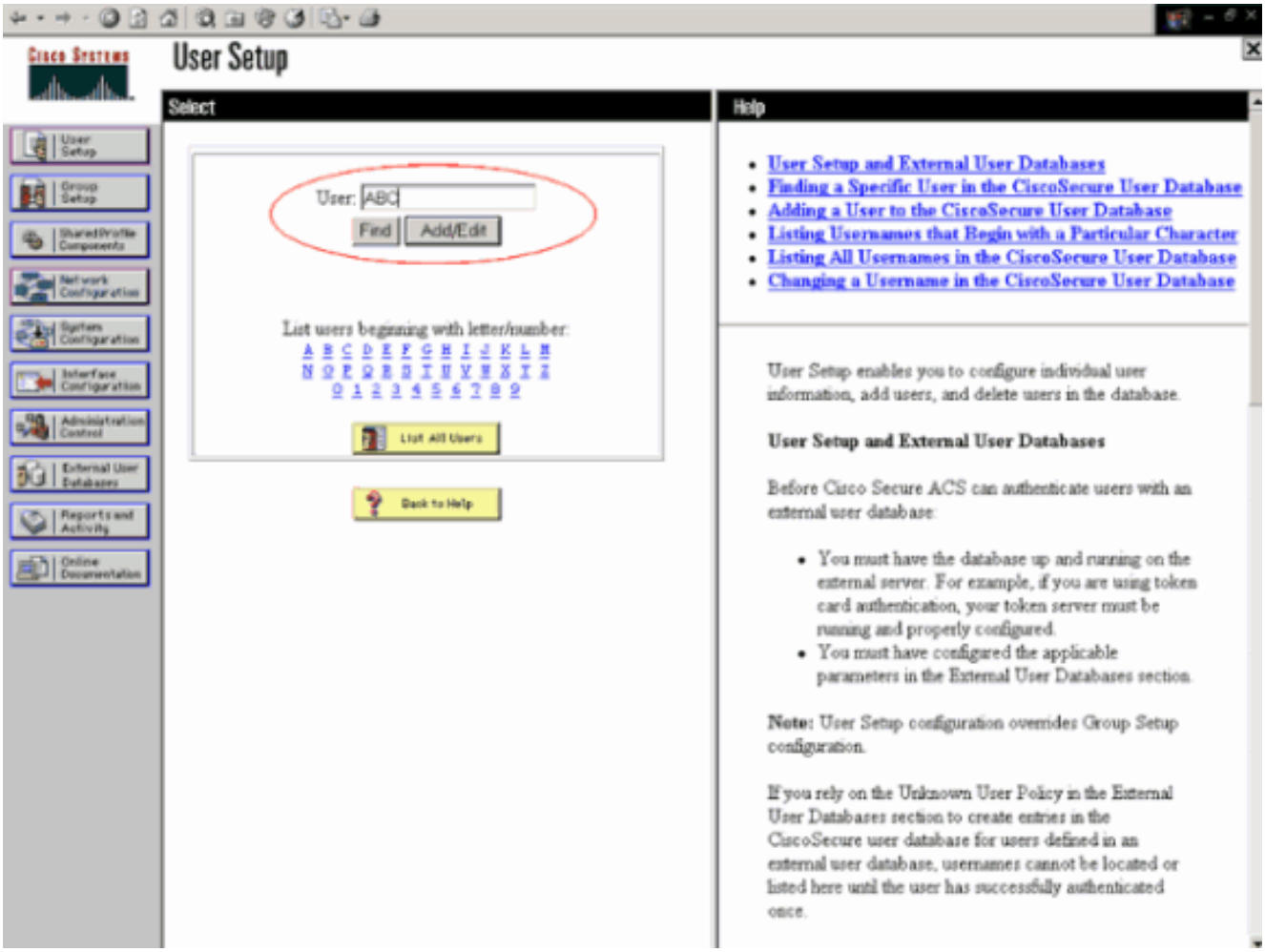


6. Cliquez sur **Apply** afin d'enregistrer la configuration.

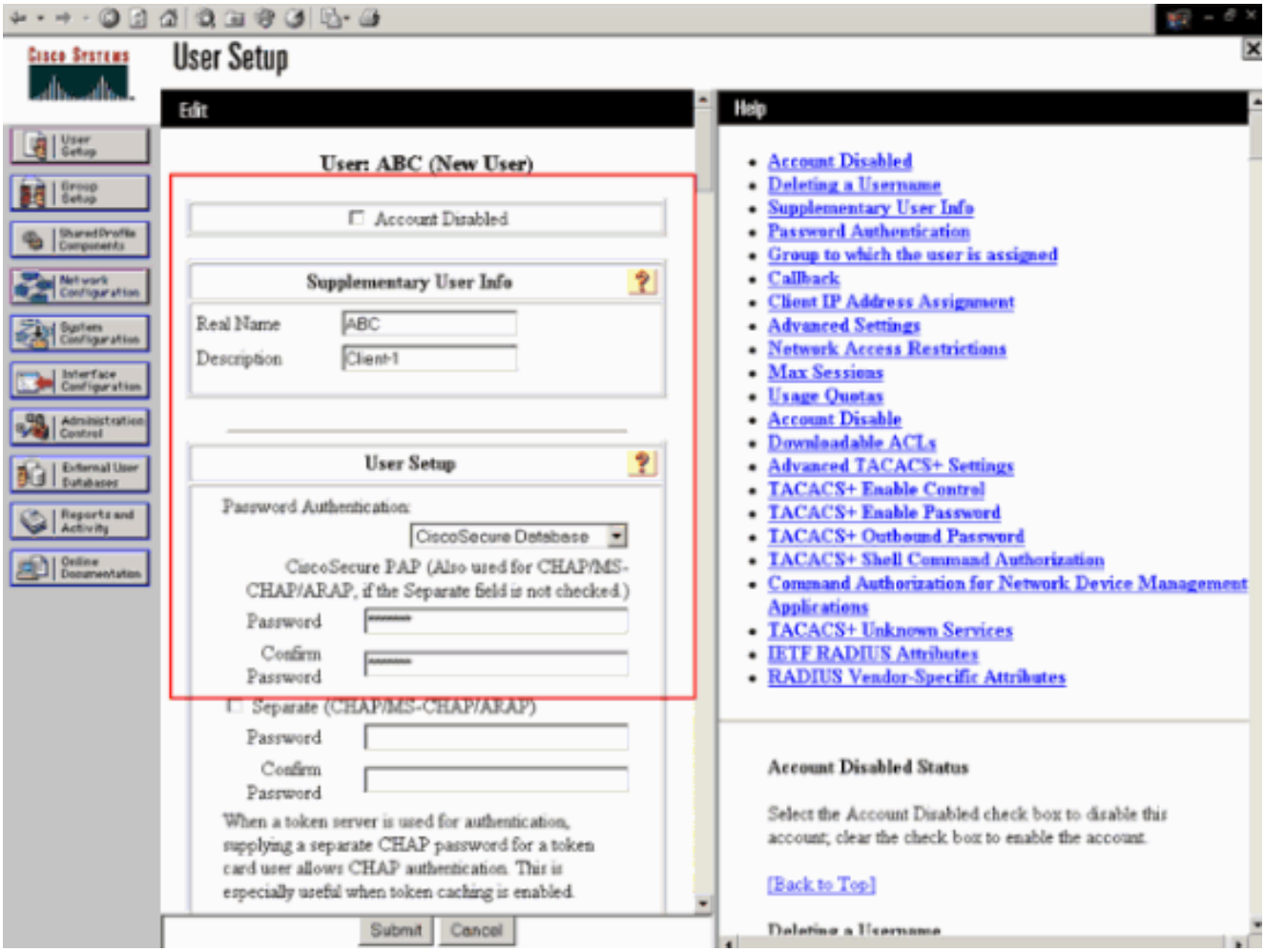
Configurer Cisco Secure ACS en tant que serveur RADIUS externe et créer une base de données utilisateur pour des authentifications client

Complétez ces étapes pour créer la base de données utilisateur et activer l'authentification EAP sur Cisco Secure ACS :

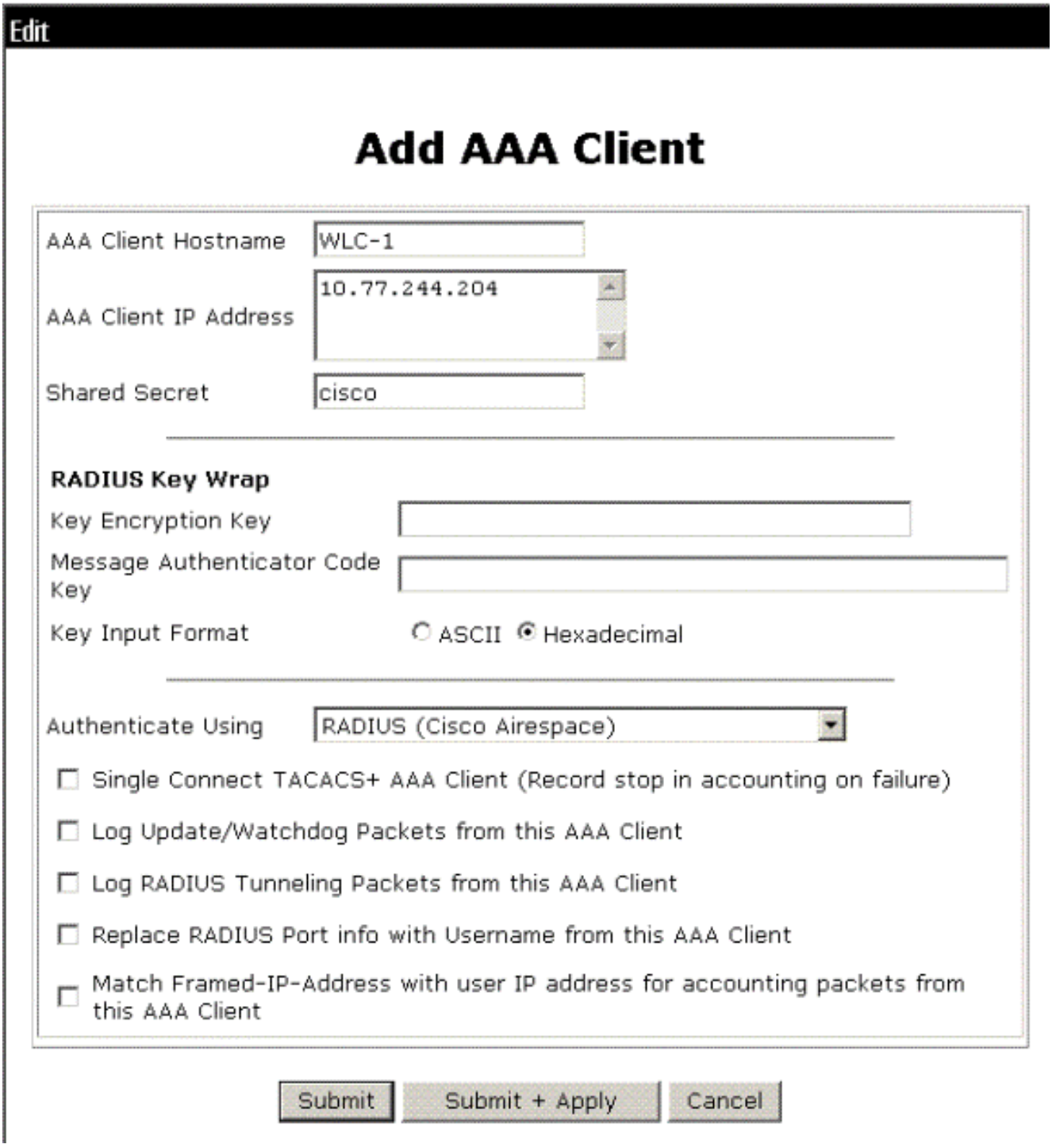
1. Choisissez **User Setup** depuis l'interface graphique ACS, entrez le nom d'utilisateur et cliquez sur **Add/Edit**. Dans cet exemple, l'utilisateur est
ABC.



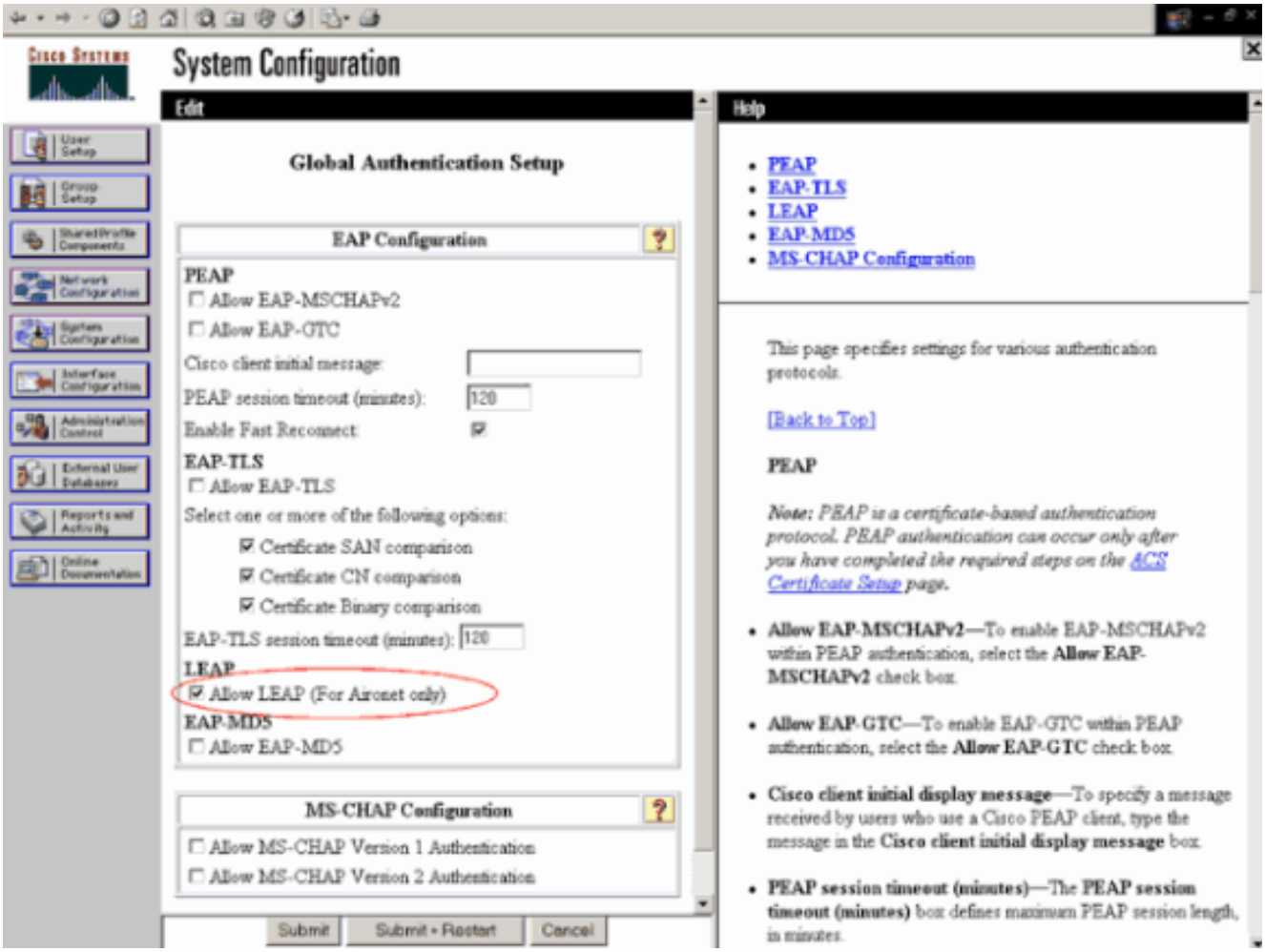
2. Lorsque la page d'installation utilisateur apparaît, définissez tous les paramètres spécifiques à l'utilisateur. Dans cet exemple, le nom d'utilisateur, le mot de passe et les informations utilisateur supplémentaires sont configurés parce que vous avez besoin de ces paramètres uniquement pour l'authentification EAP.Cliquez sur **Submit** et répétez la même procédure afin d'ajouter d'autres utilisateurs à la base de données. Par défaut, tous les utilisateurs sont regroupés sous le groupe par défaut et reçoivent la même stratégie que celle définie pour le groupe. Consultez la section Gestion de groupes d'utilisateurs du Guide de l'utilisateur Cisco Secure ACS pour Windows Server 3.2 pour plus d'informations sur l'affectation d'utilisateurs spécifiques à différents
groupes.



3. Définissez le contrôleur en tant que client AAA sur le serveur ACS. Cliquez sur **Network Configuration** depuis l'interface graphique ACS.Lorsque la page de configuration réseau apparaît, définissez le nom du WLC, l'adresse IP, le secret partagé et la méthode d'authentification (RADIUS Cisco Airespace). Référez-vous à la documentation du constructeur pour d'autres serveurs d'authentification non-ACS.**Remarque:** les clés secrètes partagées que vous configurez sur le WLC et le serveur ACS doivent correspondre. Le secret partagé distingue les majuscules et minuscules.



4. Cliquez sur **System Configuration** et sur **Global Authentication Setup**, afin de vous assurer que le serveur d'authentification est configuré pour exécuter la méthode d'authentification EAP souhaitée. Dans les paramètres de configuration EAP, sélectionnez la méthode EAP appropriée. Cet exemple utilise l'authentification LEAP. Cliquez sur **Submit** lorsque vous avez
terminé.

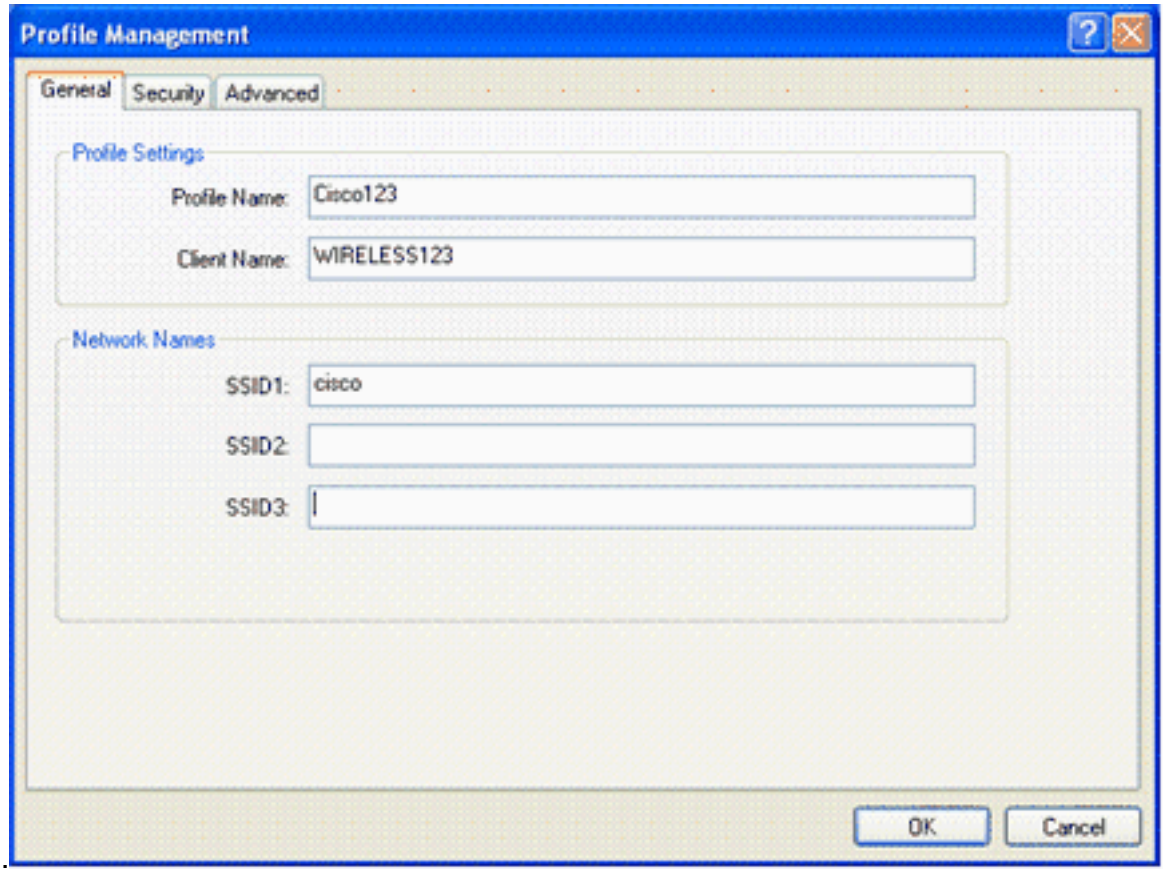


Configurer le client

Le client doit également être configuré pour le type d'EAP approprié. Le client propose le type d'EAP au serveur lors de la procédure de négociation EAP. Si le serveur prend en charge le type d'EAP, celui-ci sera immédiatement reconnu. Si le type d'EAP n'est pas pris en charge, il envoie un accusé de réception négatif et le client négocie de nouveau avec une méthode EAP différente. Cette procédure continue jusqu'à ce qu'un type d'EAP pris en charge soit négocié. Cet exemple utilise LEAP comme type d'EAP.

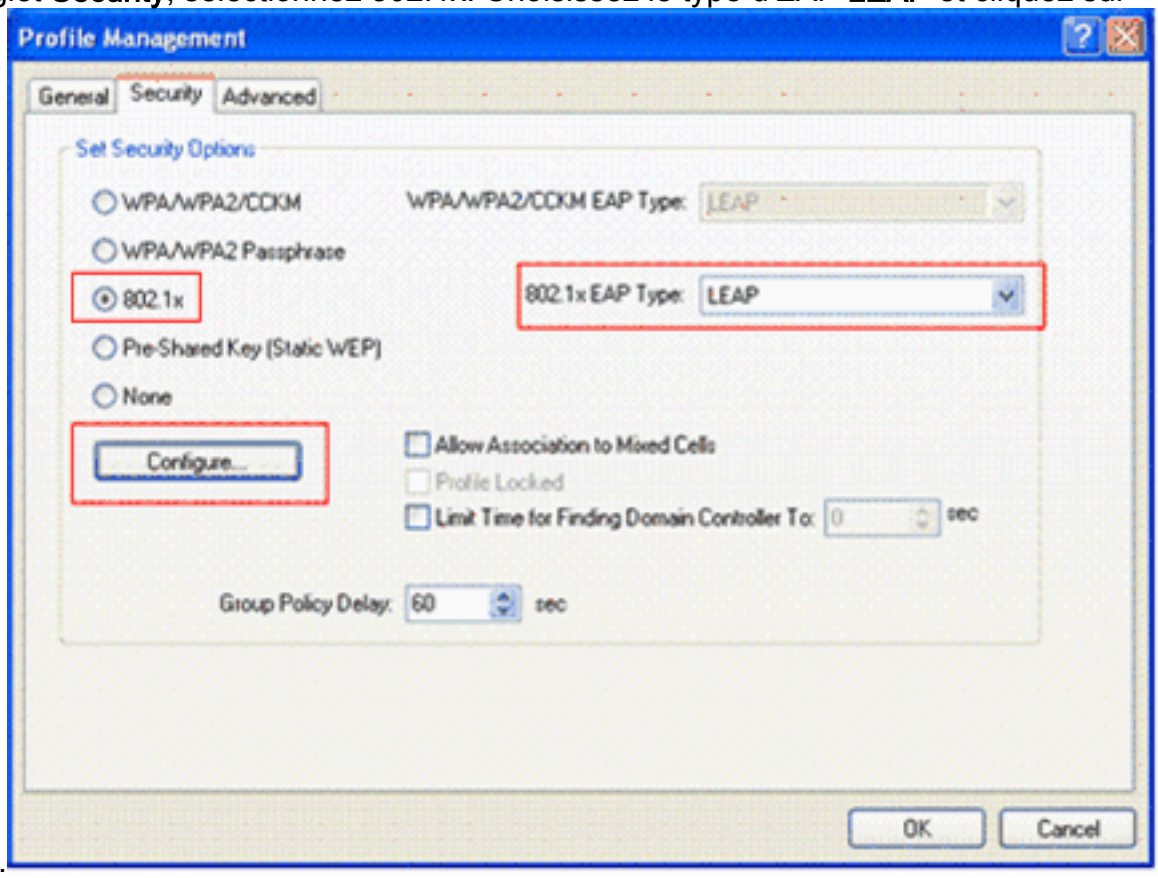
Complétez ces étapes afin de configurer LEAP sur le client avec Aironet Desktop Utility.

1. Double-cliquez sur l'icône **Aironet Utility** afin de l'ouvrir.
2. Cliquez sur l'onglet **Profile Management**.
3. Cliquez sur un profil et sélectionnez **Modify**.
4. Dans l'onglet General, sélectionnez un *nom de profil*. Entrez le **SSID** du



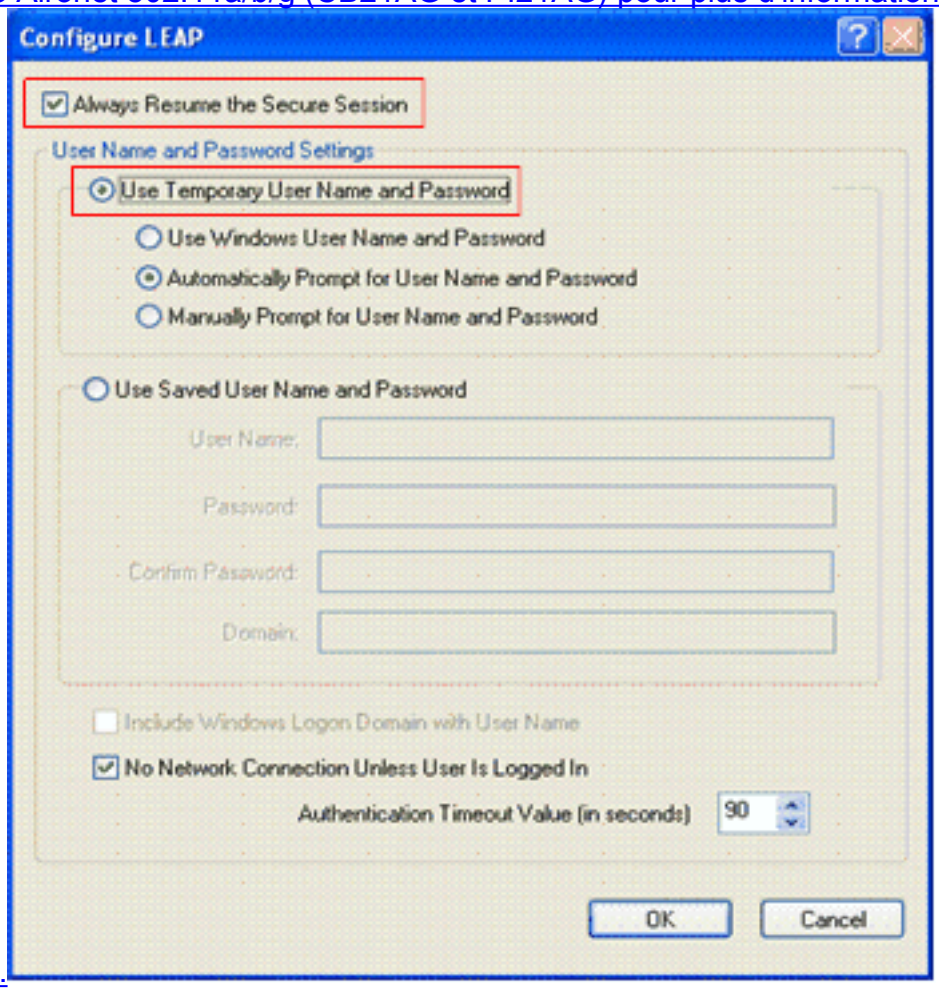
WLAN.**Remarque:** le SSID distingue les majuscules et minuscules et il doit correspondre exactement au SSID configuré sur le WLC.

5. Sous l'onglet **Security**, sélectionnez *802.1x*. Choisissez le type d'EAP **LEAP** et cliquez sur **Configure**.



6. Sélectionnez **Use Temporary Username and Password**, qui vous invite à entrer les identifiants de l'utilisateur chaque fois que l'ordinateur redémarre.Cochez l'une des trois cases fournies. Cet exemple utilise l'option **Automatically Prompt for Username and Password**, qui requiert que vous entriez les identifiants de l'utilisateur *LEAP* en plus des *nom*

d'utilisateur et mot de passe Windows avant de vous connecter sous Windows.Cochez la case **Always Resume the Secure Session** en haut de la fenêtre si vous voulez que le demandeur LEAP tente toujours de reprendre la session précédente sans vous demander d'entrer de nouveau vos identifiants chaque fois que le serveur client se déplace et s'associe de nouveau au réseau.**Remarque:** Reportez-vous à la section Configuration de l'adaptateur client du document Guide d'installation et de configuration des adaptateurs client LAN sans fil Cisco Aironet 802.11a/b/g (CB21AG et PI21AG) pour plus d'informations sur les autres options.



7. Sous l'onglet **Advanced**, vous pouvez configurer le préambule, l'extension Aironet et d'autres options 802.11 telles que la puissance, la fréquence, etc.
8. Cliquez sur **OK**. Le client tente maintenant de s'associer aux paramètres configurés.

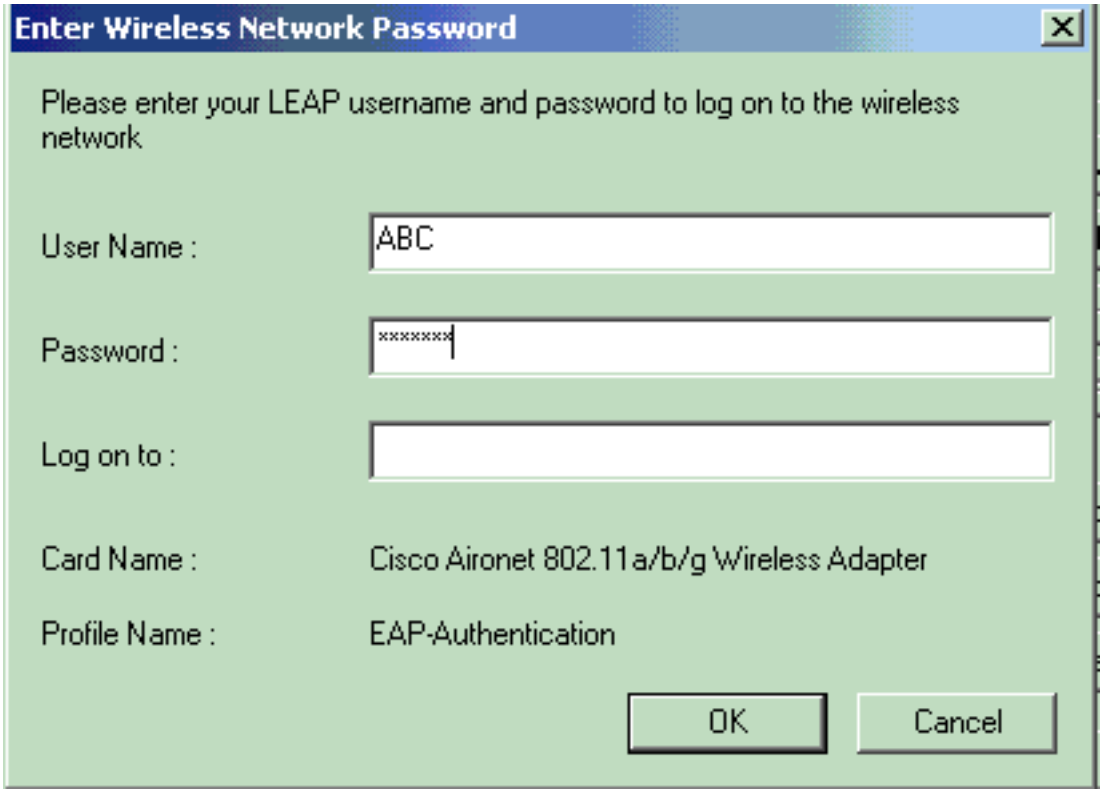
Vérifiez

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

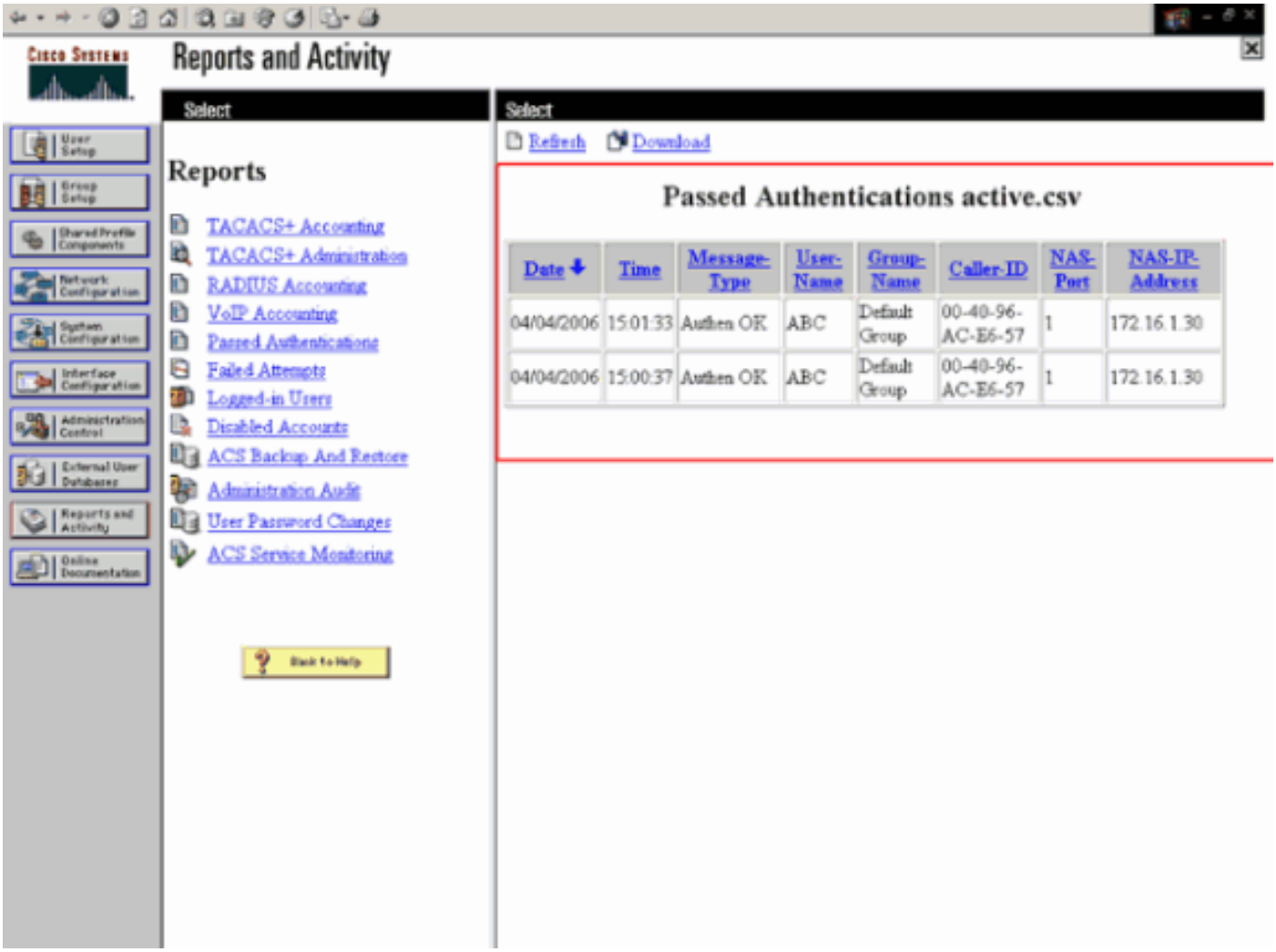
Essayez d'associer un client sans fil au point d'accès léger à l'aide de l'authentification LEAP, afin de vérifier que la configuration fonctionne comme prévu.

Remarque: ce document suppose que le profil client est configuré pour l'authentification LEAP. Reportez-vous à la section Utilisation de l'authentification EAP pour plus d'informations sur le mode de configuration de l'adaptateur client sans fil 802.11 a/b/g pour l'authentification LEAP.

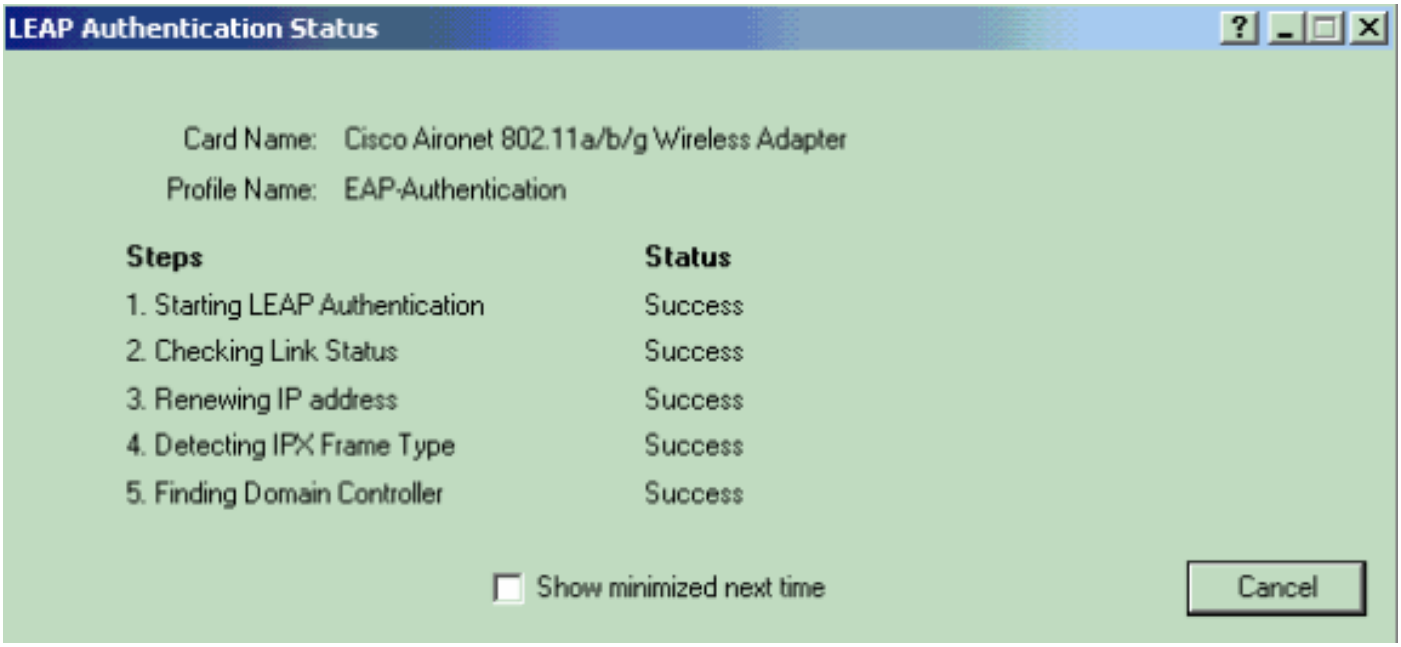
Une fois le profil du client sans fil activé, l'utilisateur est invité à fournir le nom d'utilisateur/mot de passe pour l'authentification LEAP. Voici un exemple :



Le point d'accès léger, puis le WLC, transmettent les identifiants de l'utilisateur au serveur RADIUS externe (Cisco Secure ACS) afin de valider les identifiants. Le serveur RADIUS compare les données à la base de données utilisateur et fournit l'accès au client sans fil chaque fois que les identifiants de l'utilisateur sont valides, afin de vérifier les identifiants de l'utilisateur. Le rapport Passed Authentication du serveur ACS montre que le client a réussi l'authentification RADIUS. Voici un exemple :



Lors de la réussite de l'authentification RADIUS, le client sans fil s'associe à au point d'accès léger.

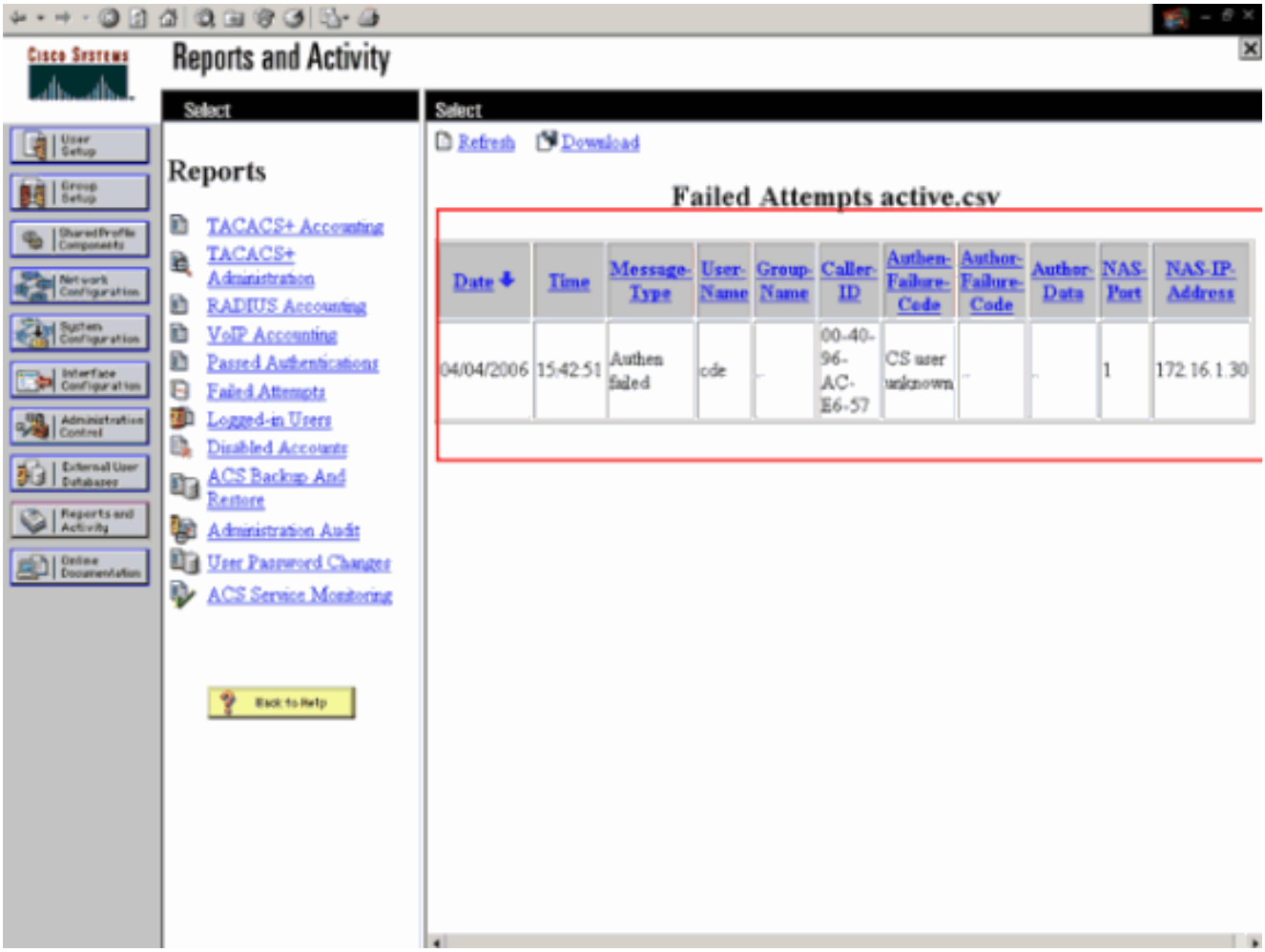


Ceci peut également être vérifié sous l'onglet **Monitor** de l'interface graphique WLC. Choisissez **Monitor > Clients** et recherchez l'adresse MAC du client.

Dépannez

Complétez ces étapes pour dépanner les configurations :

1. Utilisez la commande **debug lwapp events enable** afin de vérifier que le point d'accès s'enregistre sur le WLC.
2. Vérifiez que le serveur RADIUS reçoit et valide la demande d'authentification du client sans fil. Vérifiez l'adresse, la date et l'heure NAS-IP, afin de vérifier que le WLC a pu atteindre le serveur RADIUS.Pour ce faire, vérifiez les rapports Passed Authentications et Failed Attempts sur le serveur ACS pour savoir si l'authentification a réussi ou échoué. Ces rapports sont disponibles sous l'option Reports and Activities sur le serveur ACS. Voici un exemple d'échec d'authentification du serveur RADIUS :



Remarque: Reportez-vous à la section Obtention d'informations de version et de débogage AAA pour Cisco Secure ACS pour Windows pour plus d'informations sur le dépannage et l'obtention des informations de débogage sur Cisco Secure ACS.

3. Vous pouvez également utiliser les commandes de **débogage** suivantes afin de résoudre les problèmes d'authentification AAA :**debug aaa all enable** — Configure le débogage de tous les messages AAA.**debug dot1x packet enable** — Permet le débogage de tous les paquets dot1x.Voici un exemple de réponse de la commande **debug 802.1x aaa enable** :

```
(Cisco Controller) >debug dot1x aaa enable *Sep 23 15:15:43.792: 00:40:96:ac:dd:05
Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding
AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding
AAA_ATT_MESS_AUTH(80) index=11 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet
created request = 0x1533a288.. !!!! *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP
Attribute (code=2, length=8, id=2) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.794:
00000000: 02 02 00 08 01 41 42 43 .....ABC *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req]
Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.799: 00:40:96:ac:dd:05
[BE-resp] AAA response 'Interim Response' *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp]
Returning AAA response *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim
Response' received for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.799: 00:40:96:ac:dd:05
Received EAP Attribute (code=1, length=19,id=3, dot1xcb->id = 2) for mobile
00:40:96:ac:dd:05 *Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08 42 3a 8e d1 18 24
e8 9f ........B:... *Sep 23 15:15:43.799: 00000010: 41 42 43 ABC *Sep 23 15:15:43.799:
00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.901:
00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05
Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding
AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding
AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding
AAA_ATT_RAD_STATE(24) index=11 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding
AAA_ATT_MESS_AUTH(80) index=12 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet
created request = 0x1533a288.. !!!! *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP
Attribute (code=2, length=35, id=3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.902:
00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed ...#......[2.e.. *Sep 23
15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13 ..O...5..k..WP..
*Sep 23 15:15:43.904: 00000020: 41 42 43 ABC *Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-
req] Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.907:
00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response' *Sep 23 15:15:43.907:
00:40:96:ac:dd:05 [BE-resp] Returning AAA response *Sep 23 15:15:43.907: 00:40:96:ac:dd:05
AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.907:
00:40:96:ac:dd:05 Received EAP Attribute (code=3, length=4,id=3, dot1xcb->id = 3) for
mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.907: 00000000: 03 03 00 04 .... *Sep 23
15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05 *Sep 23
15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.912:
```

```
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.912:
00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05
Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding
AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding
AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding
AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding
AAA_ATT_RAD_STATE(24) index=11 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding
AAA_ATT_MESS_AUTH(80) index=12 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet
created request = 0x1533a288.. !!!! *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP
Attribute (code=1, length=19, id=3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.915:
00000000: 01 03 00 13 11 01 00 08 29 23 be 84 e1 6c d6 ae ........)#...l.. *Sep 23
15:15:43.915: 00000010: 41 42 43 ABC *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req]
Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.918: 00:40:96:ac:dd:05
[BE-resp] AAA response 'Success' *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp]
Returning AAA response *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success'
received for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing
avps[0]: attribute 8, vendorId 0, valueLen 4 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05
processing avps[1]: attribute 79, vendorId 0, valueLen 35 *Sep 23 15:15:43.918:
00:40:96:ac:dd:05 Received EAP Attribute (code=2, length=35,id=3) for mobile
00:40:96:ac:dd:05 *Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18 03 66 2c 6a b3 a6
c3 4c ...#.....f,j...L *Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2 29 eb 56 d6
92 ce 60 a6 ..i.....).V...`. *Sep 23 15:15:43.918: 00000020: 41 42 43 ABC *Sep 23
15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1, vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25, vendorId 0,
valueLen 21 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
vendorId 0, valueLen 16
```

Remarque: certaines des lignes du résultat du débogage ont été renvoyées à la ligne à cause des contraintes d'espace.

4. Surveillez les journaux sur le WLC, afin de vérifier que le serveur RADIUS reçoit les identifiants de l'utilisateur. Cliquez sur **Monitor** pour vérifier les journaux depuis l'interface graphique WLC. Dans le menu gauche, cliquez sur **Statistics** et sur **Radius server** dans la liste d'options.Cette étape est très importante car, dans certains cas, le serveur RADIUS ne reçoit jamais les identifiants de l'utilisateur si la configuration du serveur RADIUS sur le WLC est incorrecte.Voici comment les journaux se présentent sur le WLC si les paramètres RADIUS sont configurés de manière
incorrecte :

Vous pouvez utiliser une combinaison de la commande **show wlan summary** afin d'identifier lequel de vos WLAN utilise l'authentification du serveur RADIUS. Vous pouvez ensuite afficher la commande **show client summary** afin de voir les adresses MAC (clients) correctement authentifiées sur les WLAN RADIUS. Vous pouvez également comparer ces résultats avec vos journaux des tentatives réussies et échouées Cisco Secure ACS.

Conseils de dépannage

- Vérifiez sur le contrôleur que le serveur RADIUS est à l'état active et non standby ou disabled.
- Utilisez la **commande ping** afin de vérifier que le serveur RADIUS est accessible depuis le WLC.
- Vérifiez que le serveur RADIUS est sélectionné dans le menu déroulant du WLAN (SSID).
- Si vous utilisez WPA, vous devez installer le dernier correctif logiciel WPA Microsoft pour Windows XP SP2. Le pilote de votre demandeur client doit également être mis à niveau à la dernière version.
- Si vous utilisez PEAP, par exemple, des certificats avec XP, SP2, où les cartes sont gérées par l'utilitaire Microsoft wireless-0, vous devez obtenir le correctif KB885453 de Microsoft.Si vous utilisez Windows Zero Config/demandeur client, désactivez **Enable Fast Reconnect**. Pour ce faire, choisissez **Wireless Network Connection Properties > Wireless Networks > Preferred networks**. Sélectionnez ensuite **SSID > Properties > Open > WEP > Authentication > EAP type > PEAP > Properties > Enable Fast Reconnect**. Vous trouverez l'option d'activation ou de désactivation au bas de la fenêtre.
- Si vous utilisez des cartes Intel 2200 ou 2915, reportez-vous aux instructions sur le site Web d'Intel concernant les problèmes identifiés sur leurs cartes :Connexion réseau Intel® PRO/Wireless 2200BGConnexion réseau Intel® PRO/Wireless 2915ABGTéléchargez les pilotes Intel les plus récents, afin d'éviter tout problème. Vous pouvez télécharger les pilotes Intel sur http://downloadcenter.intel.com/
- Si la fonctionnalité de basculement agressif est activée sur le WLC, le WLC est trop agressif pour signaler que le serveur AAA ne répond pas (mode not responding). Mais cela ne devrait pas se produire, car il est probable que le serveur AAA ne réponde pas uniquement à un client donné, si vous sélectionnez l'annulation silencieuse. Il peut s'agir d'une réponse à d'autres clients valides avec des certificats valides. Cependant, le WLC peut continuer à signaler que le serveur AAA ne répond pas (not responding) et ne fonctionne pas (not functional).Afin de résoudre ce problème, désactivez la fonctionnalité de basculement agressif. Pour ce faire, lancez la commande **config radius aggressive-failover disable** depuis l'interface graphique du contrôleur. Si cette fonctionnalité est désactivée, le contrôleur bascule sur le serveur AAA suivant uniquement si 3 clients consécutifs ne reçoivent pas de réponse du serveur RADIUS.

Manipulation des compteurs EAP

Pendant l'authentification 802.1x, l'utilisateur peut voir apparaître le message d'erreur DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE: `MAX EAPOL-Key M1 retransmissions reached for mobile xx: xx : xx : xx : xx`.

Ces messages d'erreur indiquent que le client de routage n'a pas répondu à temps au contrôleur lors de la négociation de clé WPA (802.1x). Le contrôleur définit un compteur pour une réponse lors de la négociation de clé. Généralement, si ce message apparaît, il s'agit d'un problème avec le demandeur. Assurez-vous que vous exécutez les dernières versions des pilotes client et du microprogramme. Le WLC comporte quelques compteurs EAP que vous pouvez manipuler pour aider l'authentification client. Ces compteurs EAP incluent les fonctions suivantes :

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

Avant de pouvoir manipuler ces valeurs, vous devez comprendre ce qu'elles font et comment leur modification affectera le réseau :

- **EAP-Identity-Request Timeout :**Ce compteur affecte la durée d'attente entre les demandes d'identité EAP. Par défaut, la durée d'attente est d'une seconde (versions 4.1 et antérieures) et de 30 secondes (versions 4.2 et ultérieures). La raison de cette modification est due au fait que certains clients, terminaux sans fil, téléphones, scanners etc., ont du mal à répondre suffisamment rapidement. Les périphériques comme les ordinateurs portables ne requièrent généralement pas la manipulation de ces valeurs. Les valeurs disponibles sont comprises entre 1 et 120.Que se produit-il donc quand cet attribut est défini sur une valeur de 30 ? Quand le client se connecte la première fois, il envoie un message EAPOL Start au réseau et le WLC renvoie un paquet EAP, demandant l'identité de l'utilisateur ou de la machine. Si le WLC ne reçoit pas de réponse d'identification, il envoie une nouvelle demande d'identité 30 secondes plus tard. Ceci se produit lors de la connexion initiale et en cas d'itinérance du client.Que se produit-il si nous augmentons ce compteur ? Si tout est correct, il n'y a pas d'impact. Cependant, en cas de problème réseau (comme avec des clients, des points d'accès ou des fréquences radio), cela peut entraîner des retards de connectivité. Par exemple, si vous définissez le compteur sur une valeur maximale de 120 secondes, le WLC attend 2 minutes entre chaque demande d'identification. Si le client est en mode d'itinérance et si le WLC ne reçoit aucune réponse, cela peut avoir entraîné une panne de deux minutes minimum pour ce client.La valeur recommandée pour ce compteur est de *5.* Pour le moment, il n'y a aucune raison de définir ce compteur sur sa valeur maximale.
- **EAP-Identity-Request Max Retries :**La valeur Max Retries correspond au nombre de fois où le WLC envoie la demande d'identification au client avant de supprimer son entrée dans la MSCB. Une fois cette valeur atteinte, le WLC envoie une trame de désauthentification au client, l'obligeant à recommencer la procédure EAP. Les valeurs disponibles sont comprises entre 1 et 20. Nous nous pencherons davantage sur ce point ultérieurement.La valeur Max Retries fonctionne avec l'option Identity Timeout. Si vous définissez l'option Identity Timeout sur 120 et la valeur Max Retries sur 20, cela prend 2 400 secondes (soit 120 * 20). Ceci signifie que cela prendrait 40 minutes pour supprimer le client et recommencer la procédure EAP. Si vous définissez l'option Identity Timeout sur 5, avec une valeur Max Retries de 12, cela prendra alors 60 secondes (soit 5 * 12). Contrairement à l'exemple précédent, il s'écoule une minute avant la suppression du client et la relance de la procédure EAP.La valeur recommandée pour l'option Max Retries est *12*.
- **EAPOL-Key Timeout :**Pour la valeur de temporisation de la clé EAPOL, le routage par défaut est d'1 seconde ou 1 000 millisecondes. Ceci signifie que lorsque les clés EAPOL sont permutées entre le point d'accès et le client, le point d'accès envoie la clé et attend la réponse du client pendant 1 seconde maximum par défaut. Une fois la valeur temporelle définie, le point d'accès retransmet la clé. Vous pouvez utiliser la commande **config advanced eap eapol-key-timeout <time>** pour modifier ce réglage. Les valeurs disponibles dans la version 6.0 sont comprises entre 200 et 5 000 millisecondes, alors que les codes des versions antérieures à la version 6.0 acceptent des valeurs comprises entre 1 et 5 secondes. N'oubliez pas que si vous avez un client qui ne répond pas à une demande de clé, vous pouvez augmenter la durée d'attente des compteurs, pour lui accorder plus de temps pour répondre. Cependant, cela risque également de prolonger le temps qu'il faut au WLC et/ou au point d'accès pour désauthentifier le client et recommencer la procédure 802.1x.
- **EAPOL-Key Max Retries :**La valeur EAPOL-Key Max Retries par défaut est 2. Ceci signifie que la tentative de demande de clé d'origine sera envoyée deux fois au client. Ce paramètre

peut être modifié à l'aide de la commande **config advanced eap eapol-key-retries <retries>**. Les valeurs disponibles sont comprises entre 0 et 4 tentatives. Si vous utilisez la valeur EAPOL-Key Timeout par défaut (c'est-à-dire, 1 seconde) et la valeur EAPOL-Key Retry par défaut (2 secondes), et si le client ne répond pas à la demande de clé initiale, la procédure sera comme suit :Le point d'accès envoie une tentative de demande de clé au client.Il attend la réponse pendant une seconde.S'il ne reçoit aucune réponse, il envoie la première tentative de demande de clé EAPOL.Il attend la réponse pendant une seconde.S'il ne reçoit aucune réponse, il envoie la seconde tentative.S'il ne reçoit toujours pas de réponse du client et si le nombre maximal de tentatives est atteint, le client est désauthentifié. Comme avec l'option EAPOL-Key Timeout, le fait d'augmenter la valeur EAPOL-Key Retry peut, dans certains cas, présenter des avantages. Cependant, la définir à sa valeur maximale peut également être néfaste, car cela risque de prolonger le message de désauthentification.

Extraction du fichier de package du serveur ACS RADIUS pour le dépannage

Si vous utilisez ACS en tant que serveur RADIUS externe, cette section peut vous aider à dépanner votre configuration. Le fichier package.cab est un fichier zip qui contient tous les fichiers nécessaires requis pour dépanner ACS de manière efficace. Vous pouvez utiliser l'utilitaire CSSupport.exe pour créer le fichier package.cab ou collecter les fichiers manuellement.

Référez-vous à créer une section de fichier package.cab des *informations d'*ObtainingVersion *et de debug d'AAA pour le Cisco Secure ACS pour Windows pour plus d'informations sur* la façon créer et extraire le fichier de package de WCS.

Informations connexes

- Exemple de configuration du basculement du contrôleur de réseau local sans fil pour les points d'accès légers
- Mise à niveau logicielle du contrôleur LAN sans fil (WLC)
- Références des commandes du contrôleur de réseau local sans fil Cisco
- Support et documentation techniques - Cisco Systems