Cisco Secure Services Client avec authentification EAP-FAST

Contenu

Introduction

Ce document décrit comment configurer le Cisco Secure Services Client (CSSC) avec le logiciel du® Sans fil de contrôleurs LAN, de Microsoft Windows 2000, et le Cisco Secure Access Control Server (ACS) 4.0 par l'EAP-FAST. Ce document introduit l'architecture d'EAP-FAST et fournit des exemples de déploiement et de configuration. CSSC est le composant de logiciel client qui fournit la transmission des identifiants utilisateurs à l'infrastructure afin d'authentifier un utilisateur au réseau et assigner l'accès approprié.

Ce sont certains des avantages de la solution CSSC conformément à ce document :

- Authentification de chaque utilisateur (ou de périphérique) avant la permission d'accès au

WLAN/LAN avec le Protocole EAP (Extensible Authentication Protocol)
- Solution de bout en bout de Sécurité WLAN avec le serveur, l'authentificateur, et les composants de client
- Solution commune pour l'authentification de câble et Sans fil
- Dynamique, par clés de chiffrement d'utilisateur dérivées dans la procédure d'authentification
- Aucune condition requise pour l'Infrastructure à clés publiques (PKI) ou les Certificats (vérification de certificat facultative)
- Affectation de stratégie d'Access et/ou cadre NAC-activé d'EAP

Remarque: Référez-vous à Cisco le plan détaillé Sans fil que SÛR pour des informations sur le déploiement de sécurisent la radio.

Le cadre d'authentification de 802.1x a été incorporé en tant qu'élément (Sécurité LAN Sans fil) de la norme 802.11i pour activer l'authentification, l'autorisation, et les fonctions de traçabilité basées par layer-2 dans un réseau LAN sans fil de 802.11. Aujourd'hui, il y a plusieurs protocoles d'EAP disponibles pour le déploiement dans les réseaux de câble et Sans fil. Les protocoles généralement déployés d'EAP incluent le LEAP, le PEAP, et l'EAP-TLS. En plus de ces protocoles, Cisco a défini et authentification flexible mise en application d'EAP par le protocole sécurisé de tunnel (EAP-FAST) comme protocole basé sur des standards d'EAP disponible pour le déploiement dans de câble et des réseaux LAN sans fil. La spécification de protocole d'EAP-FAST est publiquement - disponible sur le site Web IETF .

Comme avec quelques autres protocoles d'EAP, l'EAP-FAST est une architecture de degré de sécurité de client-serveur qui chiffre des transactions d'EAP dans un tunnel de TLS. Tandis que semblable au PEAP ou à l'EAP-TTLS à cet égard, il diffère dans cet établissement de tunnel d'EAP-FAST est basé sur les clés secrètes partagées fortes qui sont seules à chaque utilisateur contre PEAP/EAP-TTLS (qui emploient un certificat du serveur X.509 pour protéger la session d'authentification). Ces clés secrètes partagées s'appellent les qualifications de Protected Access (PACs) et peuvent être distribuées automatiquement (ravitaillement automatique ou d'intrabande) ou manuellement (ravitaillement manuel ou hors bande) aux périphériques de client. Puisque les prises de contact basées sur des secrets partagés sont plus efficaces que des prises de contact basées sur une infrastructure de PKI, l'EAP-FAST est le type le plus rapide et moins processeur-intensif d'EAP de ceux qui fournissent des échanges d'authentification protégés. L'EAP-FAST est également conçu pour la simplicité du déploiement puisqu'il n'exige pas un certificat sur le client Sans fil de RÉSEAU LOCAL ou sur l'infrastructure de RADIUS pourtant incorpore un mécanisme intégré de ravitaillement.

Ce sont certaines des principales capacités du protocole d'EAP-FAST :

- Ouverture de session simple (SSO) avec le nom d'utilisateur/mot de passe de Windows
- Soutien d'exécution de script de connexion
- Support de Protocole WPA (Wi-Fi Protected Access) sans suppliant de tiers (Windows 2000 et XP seulement)
- Déploiement simple sans la condition requise pour l'infrastructure de PKI
- Vieillissement de mot de passe de Windows (c'est-à-dire, soutien de l'expiration du mot de passe basée sur un serveur)
- Intégration avec le Cisco Trust Agent pour le contrôle d'admission au réseau avec le logiciel client approprié

Conditions préalables

Condition requise

Il y a une supposition que l'installateur a la connaissance de l'installation de base de Windows 2003 et de l'installation de Cisco WLC puisque ce document couvre seulement les configurations spécifiques pour faciliter les tests.

Pour l'installation initiale et les informations de configuration pour les contrôleurs de la gamme Cisco 4400, consultez le Guide de démarrage rapide : Contrôleurs de réseau local sans fil de la gamme Cisco 4400 Pour l'installation initiale et les informations de configuration pour les contrôleurs de gamme Cisco 2000, référez-vous au guide de démarrage rapide : Contrôleurs de réseau local sans fil de la gamme Cisco 2000.

Avant que vous commenciez, installez la Microsoft Windows Server 2000 avec le dernier logiciel de pack de services. Installez les contrôleurs et les points d'accès léger (LAP) et assurez-vous que les dernières mises à jour logicielles sont configurées.

Composants utilisés

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

- Contrôleur de gamme Cisco 2006 ou 4400 qui passages 4.0.155.5
- Cisco 1242 LWAPP AP
- Windows 2000 avec le Répertoire actif
- Commutateur de Cisco Catalyst 3750G
- Windows XP avec la carte adaptateur CB21AG et la version 4.05 de Cisco Secure Services Client

Conventions

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

Paramètres de conception

Base de données

Quand vous déployez un réseau WLAN et recherchez un protocole d'authentification, on le désire généralement pour utiliser une base de données en cours pour l'utilisateur/authentification de machine. Les bases de données typiques qui peuvent être utilisées sont Répertoire actif de Windows, LDAP, ou une base de données du mot de passe d'une fois (OTP) (c'est-à-dire, RSA ou SecureID). Toutes ces bases de données sont compatibles avec le protocole d'EAP-FAST, mais quand vous prévoyez pour le déploiement, il y a quelques conditions requises de compatibilité qui doivent être considérées. Le déploiement initial d'un fichier PAC aux clients fait par l'approvisionnement automatique anonyme, le ravitaillement authentifié (par le certificat en cours de client X.509), ou le ravitaillement manuel. Afin de ce document, l'approvisionnement automatique et le ravitaillement anonymes de manuel sont considérés.

Le ravitaillement automatique PAC utilise l'accord authentifié Protocol (ADHP) de clé de Diffie-Hellman d'établir un tunnel sécurisé. Le tunnel sécurisé peut être établi anonyme ou par un

mécanisme d'authentification de serveur. Dans la connexion de tunnel établi, MS-CHAPv2 est utilisé pour authentifier le client et, sur l'authentification réussie, pour distribuer le fichier PAC au client. Après que le PAC provisioned avec succès, le fichier PAC peut être utilisé pour initier une nouvelle session d'authentification d'EAP-FAST afin de gagner l'accès de réseau sécurisé.

Le ravitaillement automatique PAC est approprié à la base de données en service parce que, puisque le mécanisme d'approvisionnement automatique compte sur MSCHAPv2, la base de données utilisée pour authentifier des utilisateurs doit être compatible avec ce format de mot de passe. Si vous utilisez l'EAP-FAST avec une base de données qui ne prend en charge pas le format MSCHAPv2 (tel qu'OTP, Novell, ou LDAP), on l'exige pour utiliser un autre mécanisme (c'est-à-dire, ravitaillement manuel ou ravitaillement authentifié) pour déployer des fichiers PAC d'utilisateur. Ce document donne un exemple de ravitaillement automatique avec une base de données d'utilisateur Windows.

Cryptage

L'authentification d'EAP-FAST n'exige pas l'utilisation un type de cryptage de la particularité WLAN. Le type de cryptage WLAN à utiliser est déterminé par les capacités de carte NIC de client. Il est recommandé pour utiliser le cryptage WPA2 (AES-CCM) ou WPA(TKIP), dépendant sur les capacités de carte NIC dans le déploiement spécifique. Notez que la solution WLAN de Cisco permet la coexistence des périphériques WPA2 et WPA de client sur un SSID commun.

Si les périphériques de client ne prennent en charge pas le WPA2 ou le WPA, il est possible de déployer l'authentification de 802.1X avec les clés WEP dynamiques, mais, dues aux exploits réputées contre des clés WEP, ce mécanisme de chiffrement WLAN n'est pas recommandé. Si on l'exige pour prendre en charge les clients réservés à la WEP, il est recommandé d'utiliser un intervalle de session-timeout, qui exige que les clients dérivent une nouvelle clé WEP sur un intervalle fréquent. Trente minutes est l'intervalle recommandé de session pour les débits de données typiques WLAN.

Qualifications simples d'ouverture de session et d'ordinateur

L'ouverture de session simple se rapporte à la capacité d'une ouverture de session de seul utilisateur ou à l'entrée des qualifications d'authentification d'être utilisé pour accéder à des applications multiples ou des périphériques de multiple. Aux fins de ce document, l'ouverture de session simple se rapporte à l'utilisation des qualifications qui sont utilisées pour ouvrir une session à un PC pour l'authentification au WLAN.

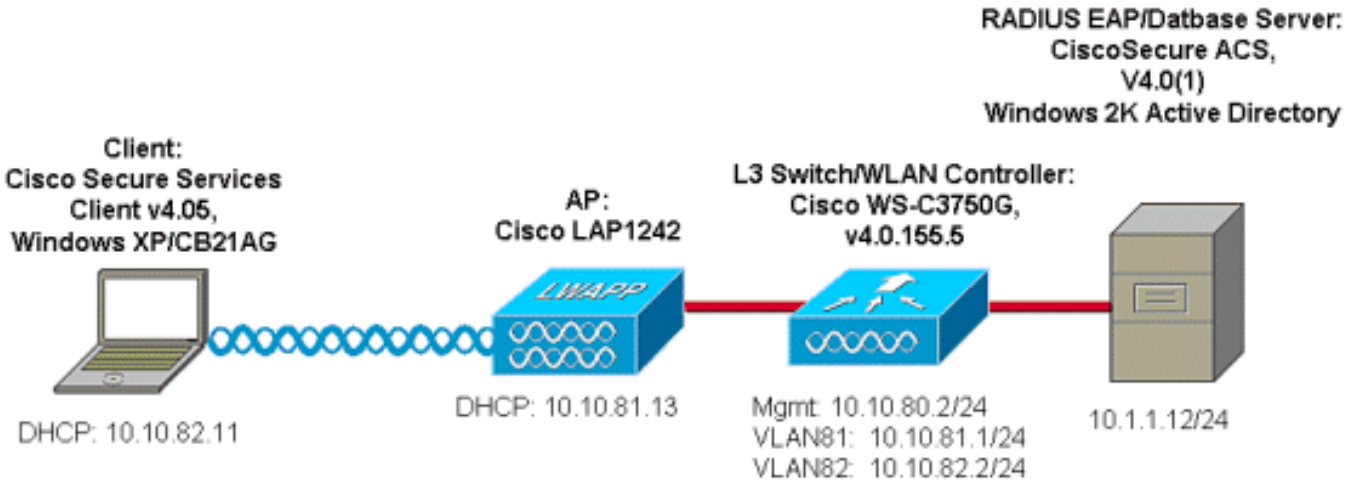
Avec le Cisco Secure Services Client, il est possible d'employer les qualifications de connexion d'un utilisateur pour authentifier également au réseau WLAN. Si on le désire pour authentifier un PC au réseau avant la connexion d'utilisateur au PC, on l'exige pour utiliser les identifiants utilisateurs enregistrés ou les qualifications attachés à un profil d'ordinateur. L'un ou l'autre de ces méthodes est utile dans les cas où on le désire pour exécuter des scripts de connexion ou pour tracer des lecteurs quand les amorces PC, par opposition à quand un utilisateur ouvre une session.

Diagramme du réseau

C'est le schéma de réseau utilisé dans ce document. Dans ce réseau, il y a quatre sous-réseaux utilisés. Notez qu'il n'est pas nécessaire de segmenter ces périphériques dans différents réseaux, mais ceci a les moyens la plupart de flexibilité pour l'intégration avec les réseaux réels. Le

contrôleur sans fil LAN intégré du Catalyst 3750G fournit des switchports des Over Ethernet d'alimentation (POE), la commutation L3, et la capacité de contrôleur WLAN sur un châssis commun.

1. Le réseau 10.1.1.0 est le réseau serveur où l'ACS réside.
2. Le réseau 10.10.80.0 est le réseau de gestion utilisé par le contrôleur WLAN.
3. Le réseau 10.10.81.0 est le réseau où les aps résident.
4. Le réseau 10.10.82.0 est utilisé pour les clients WLAN.



Configurez le serveur de contrôle d'accès (ACS)

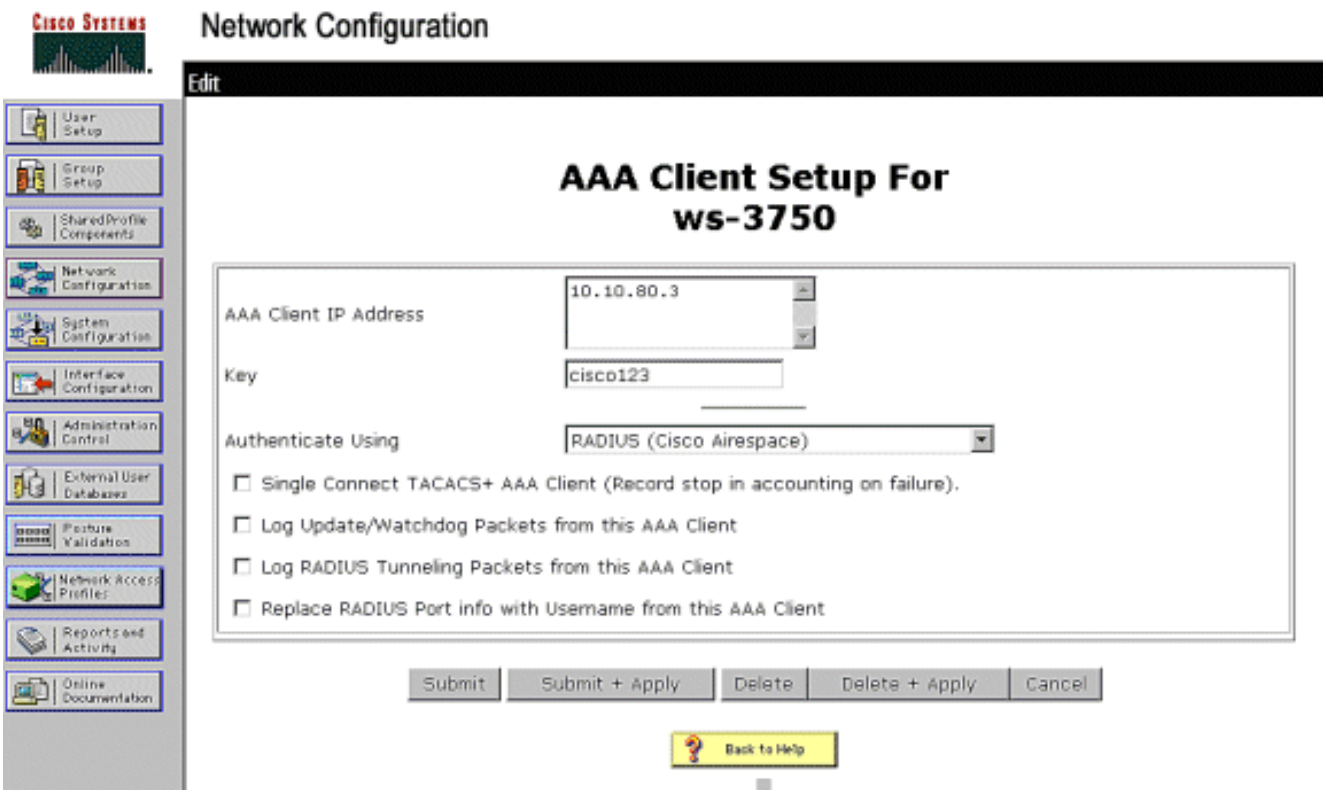
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Ajoutez le Point d'accès comme AAA-client (NAS) dans ACS

Cette section décrit comment configurer ACS pour l'EAP-FAST avec le ravitaillement PAC d'intrabande avec le Répertoire actif de Windows comme base de données externe.

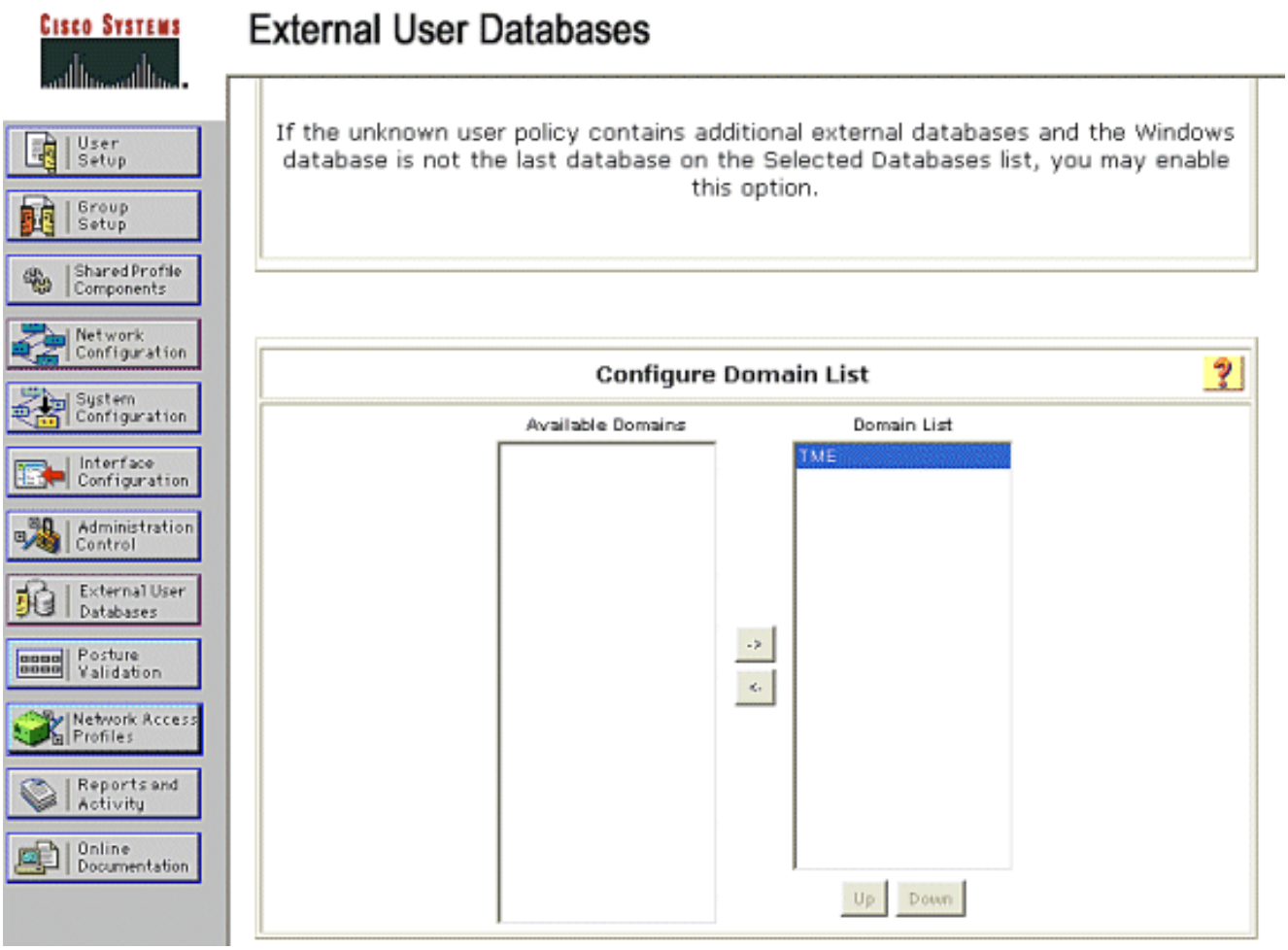
1. Ouvrez une session à **ACS > configuration réseau** et cliquez sur Add l'**entrée**.
2. Complétez le nom de contrôleur WLAN, adresse IP, la clé secrète partagée, et dessous l'authentifiez utilisant, choisissez RADIUS (Cisco Airespace), qui inclut également des attributs IETF de RADIUS.**Remarque:** Si les groupes de périphériques réseau (NDG) sont activés, d'abord choisissez le NDG approprié et ajoutez le contrôleur WLAN à lui. Référez-vous au guide de configuration ACS pour des informations sur le NDG.
3. **Reprise du** clic **Submit+**.



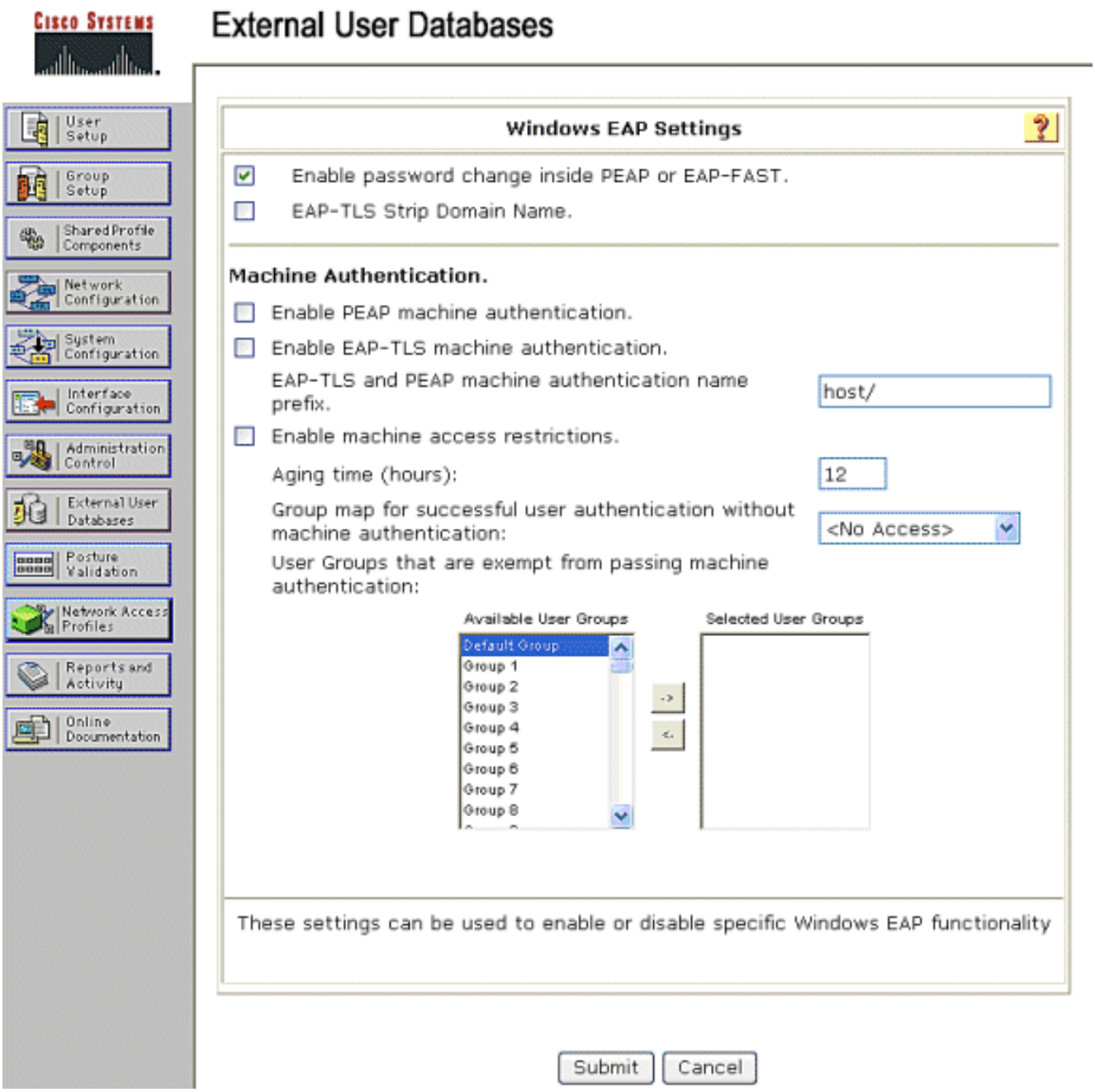
Configurez ACS afin de questionner la base de données externe

Cette section décrit comment configurer l'ACS afin de questionner la base de données externe.

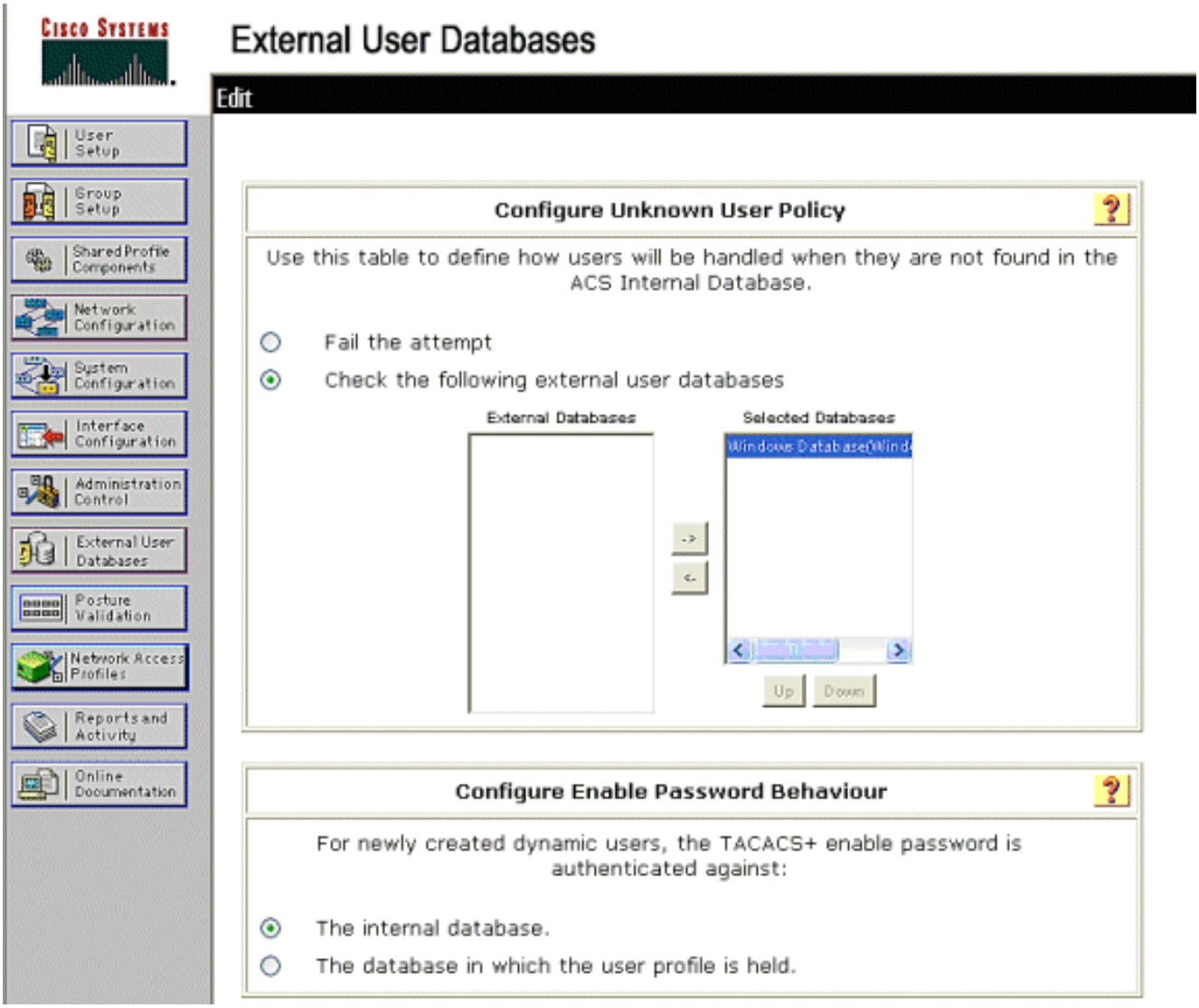
1. **La base de données d'utilisateur externe de** clic **> la configuration de base de données > la base de données de Windows > configurent**.
2. Sous configurez le domain list, des **domaines de** mouvement des domaines disponibles au domain list.**Remarque:** Le serveur qui exécute l'ACS doit avoir la connaissance de ces domaines pour que l'application ACS détecte et pour utilise ces domaines pour l'authentification.



3. Sous les configurations d'EAP de Windows, configurez l'option de permettre la modification de mot de passe à l'intérieur de la session PEAP ou d'EAP-FAST. Référez-vous au guide de configuration pour le Cisco Secure ACS 4.1 afin d'obtenir plus de détails au sujet d'EAP-FAST et de vieillissement de mot de passe de Windows.
4. Cliquez sur **Submit**.**Remarque:** Vous pouvez également permettre à la caractéristique d'autorisation de Dialin pour l'EAP-FAST sous la configuration de base de données d'utilisateur Windows afin de permettre à la base de données externe de Windows pour contrôler la permission d'accès. Les configurations MS-CHAP pour la modification de mot de passe à la page de configuration de base de données de Windows s'appliquent seulement à l'authentification du non-EAP MS-CHAP. Afin d'activer la modification de mot de passe en même temps que l'EAP-FAST, il est nécessaire d'activer la modification de mot de passe sous les configurations d'EAP de
Windows.



5. Cliquez sur la **base de données d'utilisateur externe > stratégie inconnue d'utilisateur** et choisissez le **contrôle la** case d'option **suivante de bases de données d'utilisateur externe**.
6. Déplacez la base de données de Windows des **bases de données externes aux bases de données sélectionnées**.
7. Cliquez sur **Submit**.**Remarque:** À partir de là, l'ACS vérifie le DB de Windows. Si l'utilisateur n'est pas trouvé dans la base de données locale ACS, elle place l'utilisateur au groupe par défaut ACS. Référez-vous à la documentation ACS pour plus de détails au sujet des mappages de groupe de base de données.**Remarque:** Car l'ACS questionne la base de données de Microsoft Active Directory pour vérifier des identifiants utilisateurs, des configurations supplémentaires de droits d'accès doivent être configurées sur Windows. Référez-vous au [guide d'installation pour le Cisco Secure ACS pour des Windows Server] pour des
détails.

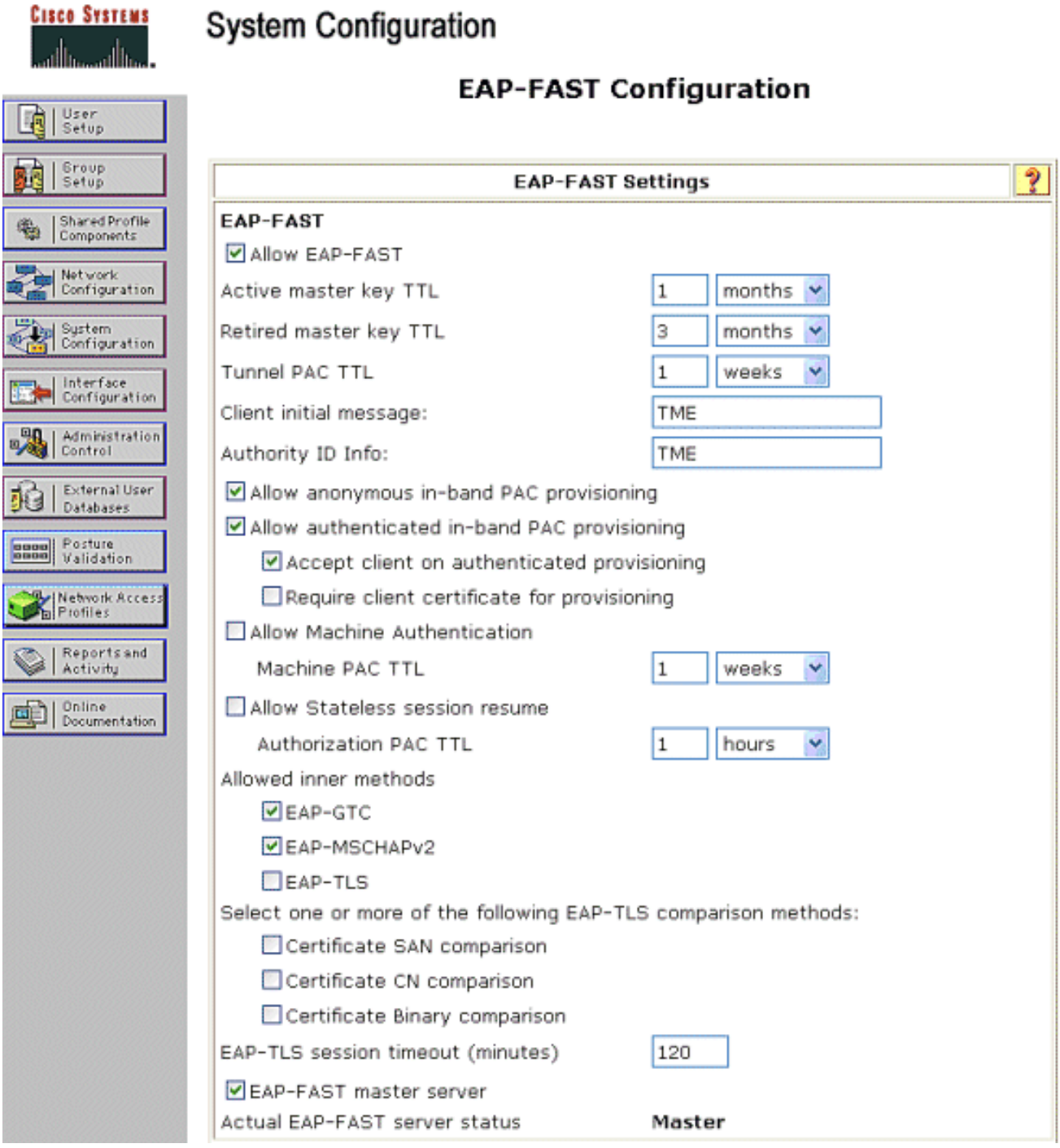


Support d'EAP-FAST d'enable sur l'ACS

Cette section décrit comment activer le support d'EAP-FAST sur l'ACS.

1. Allez à la **configuration système > authentification globale installée > configuration d'EAP-FAST**.
2. Choisissez **permettent l'EAP-FAST**.
3. Configurez ces recommandations : Clé principale retirée par TTL TTL PAC TTL de clé principale. Ces configurations sont configurées par défaut dans le Cisco Secure ACS :Mois de la clé principale TTL:1TTL principal retiré : 3 moisPAC TTL : 1 semaine
4. Complétez la zone d'informations d'**ID d'autorité**. Ce texte est affiché sur du logiciel client d'EAP-FAST où la sélection de l'autorité PAC est le contrôleur.**Remarque:** Le Cisco Secure Services Client n'utilise pas ce texte descriptif pour l'autorité PAC.
5. Choisissez le champ de **ravitaillement PAC d'intrabande d'autoriser**. Ce champ active le ravitaillement automatique PAC pour les clients approprié-activés d'EAP-FAST. Pour cet exemple, l'approvisionnement automatique est utilisé.
6. Choisissez les **méthodes intérieures permises** : EAP-GTC et EAP-MSCHAP2. Ceci permet l'exécution des clients de l'EAP-FAST v1 et de l'EAP-FAST v1a. (Le Cisco Secure Services Client prend en charge l'EAP-FAST v1a.) S'il n'est pas nécessaire de prendre en charge des clients de l'EAP-FAST v1, il est seulement nécessaire d'activer EAP-MSCHAPv2 comme méthode intérieure.

7. Choisissez la case à cocher de **serveur de maître d'EAP-FAST** pour activer ce serveur d'EAP-FAST comme maître. Ceci permet à d'autres serveurs ACS pour utiliser ce serveur comme autorité PAC de maître pour éviter la fourniture de seules clés pour chaque ACS dans un réseau. Référez-vous au guide de configuration ACS pour des détails.
8. Clic **Submit+Restart**.



Contrôleur de WLAN Cisco

Aux fins de ce guide de déploiement, un contrôleur sans fil LAN intégré de Cisco WS3750G (WLC) est utilisé avec Cisco AP1240 aps légers (RECOUVREMENT) pour fournir l'infrastructure WLAN pour des tests CSSC. La configuration s'applique pour n'importe quel contrôleur de WLAN Cisco. La version de logiciel utilisée est 4.0.155.5.

Configurez le contrôleur LAN Sans fil

Fonctionnement de base et enregistrement de RECOUVREMENT au 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). Alternativement, vous pouvez utiliser le GUI afin de configurer le WLC. Ce document explique comment configurer le WLC avec l'assistant de configuration de démarrage sur le CLI.

Après que le WLC démarre pour la première fois, il entre dans l'assistant de démarrage de configuration. Utilisez l'assistant de configuration pour configurer des paramètres de base. Vous pouvez accéder à l'assistant par le CLI ou le 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]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
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. En cet exemple de configuration, le WLC utilise **10.10.80.3** comme adresse IP d'interface de gestion et **10.10.80.4** comme adresse IP d'interface d'AP-gestionnaire.

Avant que toutes les autres caractéristiques puissent être configurées sur le WLCs, les recouvrements doivent s'inscrire au WLC. Ce document suppose que le RECOUVREMENT est enregistré au WLC. Référez-vous au registre AP léger à la section de WLCs de Basculement de contrôleur WLAN pour l'exemple de configuration de Point d'accès léger pour les informations sur la façon dont les aps légers s'inscrivent au WLC. Pour la référence avec cet exemple de configuration, les AP1240s sont déployés sur un sous-réseau distinct (10.10.81.0/24) du contrôleur WLAN (10.10.80.0/24), et l'option 43 DHCP est utilisée de prévoir la détection de contrôleur.

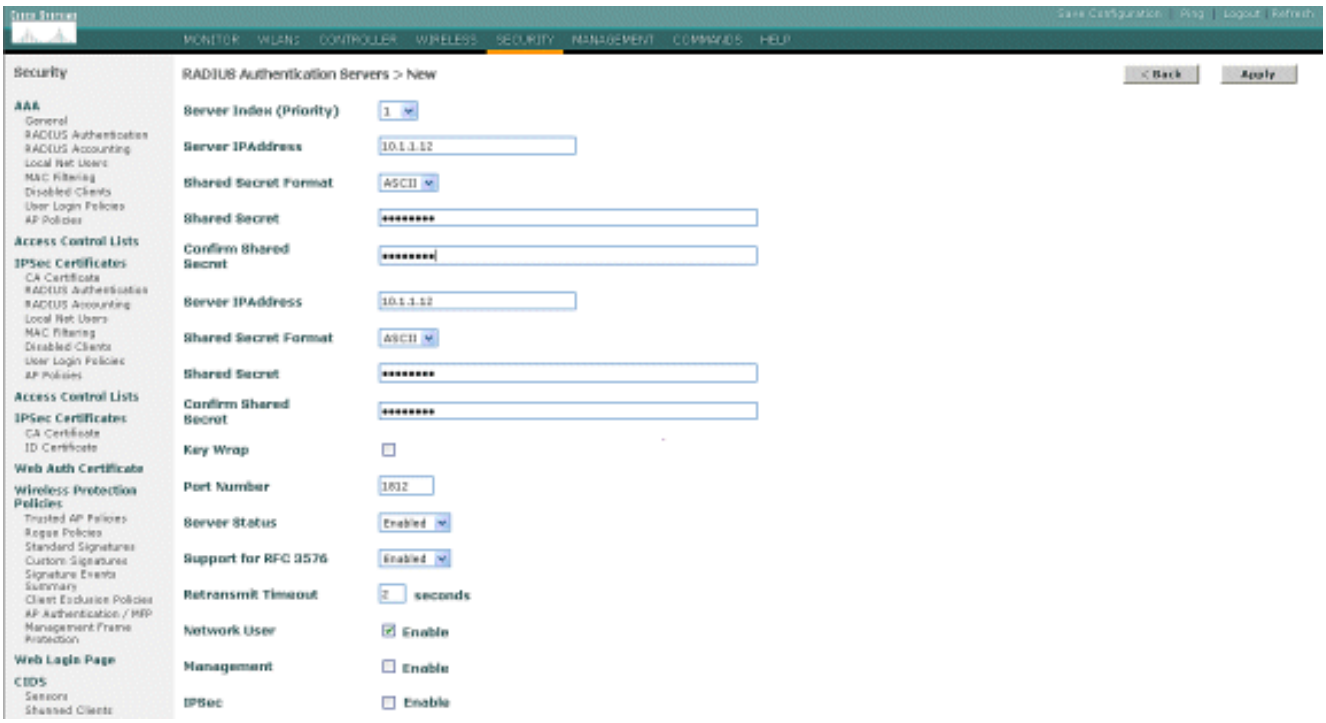
Authentification de RADIUS par le Cisco Secure ACS

Le WLC doit être configuré pour expédier les identifiants utilisateurs au serveur de Cisco Secure ACS. Le serveur ACS alors valide les identifiants utilisateurs (par la base de données configurée de Windows) et permet d'accéder aux clients sans fil.

Terminez-vous ces étapes pour configurer le WLC pour la transmission au serveur ACS :

1. Cliquez sur Security et **authentification de RADIUS du** GUI de contrôleur pour afficher la page de serveurs d'authentification RADIUS. Cliquez sur New alors pour définir le serveur ACS.

2. Définissez les paramètres de serveur ACS dans le RADIUS Authentication Servers > New page. Ces paramètres incluent l'adresse IP ACS, le secret partagé, le numéro de port, et l'état de serveur.**Remarque:** Les numéros de port 1645 ou 1812 sont compatibles avec ACS pour l'authentification de RADIUS.Les cases d'utilisateur du réseau et de Gestion déterminent si l'authentification basée sur RADIUS s'applique pour les utilisateurs du réseau (par exemple, des clients WLAN) et la Gestion (c'est-à-dire, utilisateurs administratifs). L'exemple de configuration utilise le Cisco Secure ACS en tant que serveur de RADIUS avec l'adresse IP 10.1.1.12
:



Configuration des paramètres WLAN

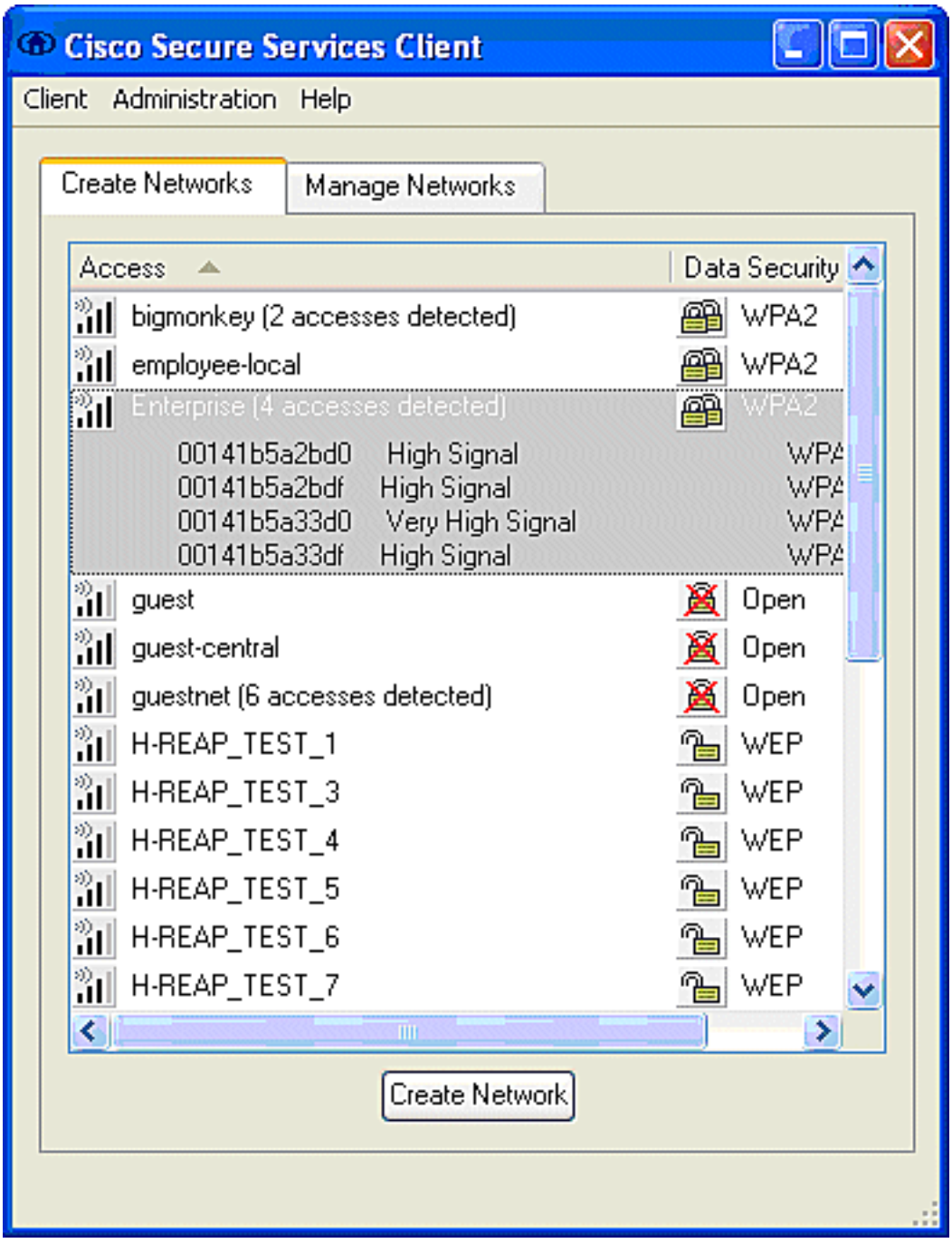
Cette section décrit la configuration du Cisco Secure Services Client. Dans cet exemple, CSSC

v4.0.5.4783 est utilisé avec un adaptateur de client de Cisco CB21AG. Avant l'installation du logiciel CSSC, vérifiez que seulement les gestionnaires pour le CB21AG sont installés, pas Aironet Desktop Utility (ADU).

Une fois que le logiciel est installé et il fonctionne comme service, il balaye pour les réseaux disponibles et affiche ceux disponibles.

Remarque: CSSC désactive le config de Windows Zero.

Remarque: Seulement ces le SSID qui sont activés pour l'émission sont visible.



Remarque: Le contrôleur WLAN, par défaut, annonce le SSID, ainsi on lui affiche dans la liste de réseaux de création de SSID balayé. Afin de créer un profil réseau, vous pouvez simplement cliquer sur le **SSID** dans la liste (entreprise) et la case d'option de **réseau de création**.

Si l'infrastructure WLAN est configurée avec l'émission SSID désactivée, vous devez manuellement ajouter le SSID ; cliquez sur la case d'option d'**ajouter** sous des périphériques

d'Access et écrivez manuellement le **SSID** approprié (par exemple, entreprise). Configurez le comportement actif de sonde pour le client, c.-à-d., où le client sonde activement pour son SSID configuré ; spécifiez **recherchent activement ce périphérique d'accès** après que vous écriviez le SSID sur la fenêtre de périphérique d'Access d'ajouter.

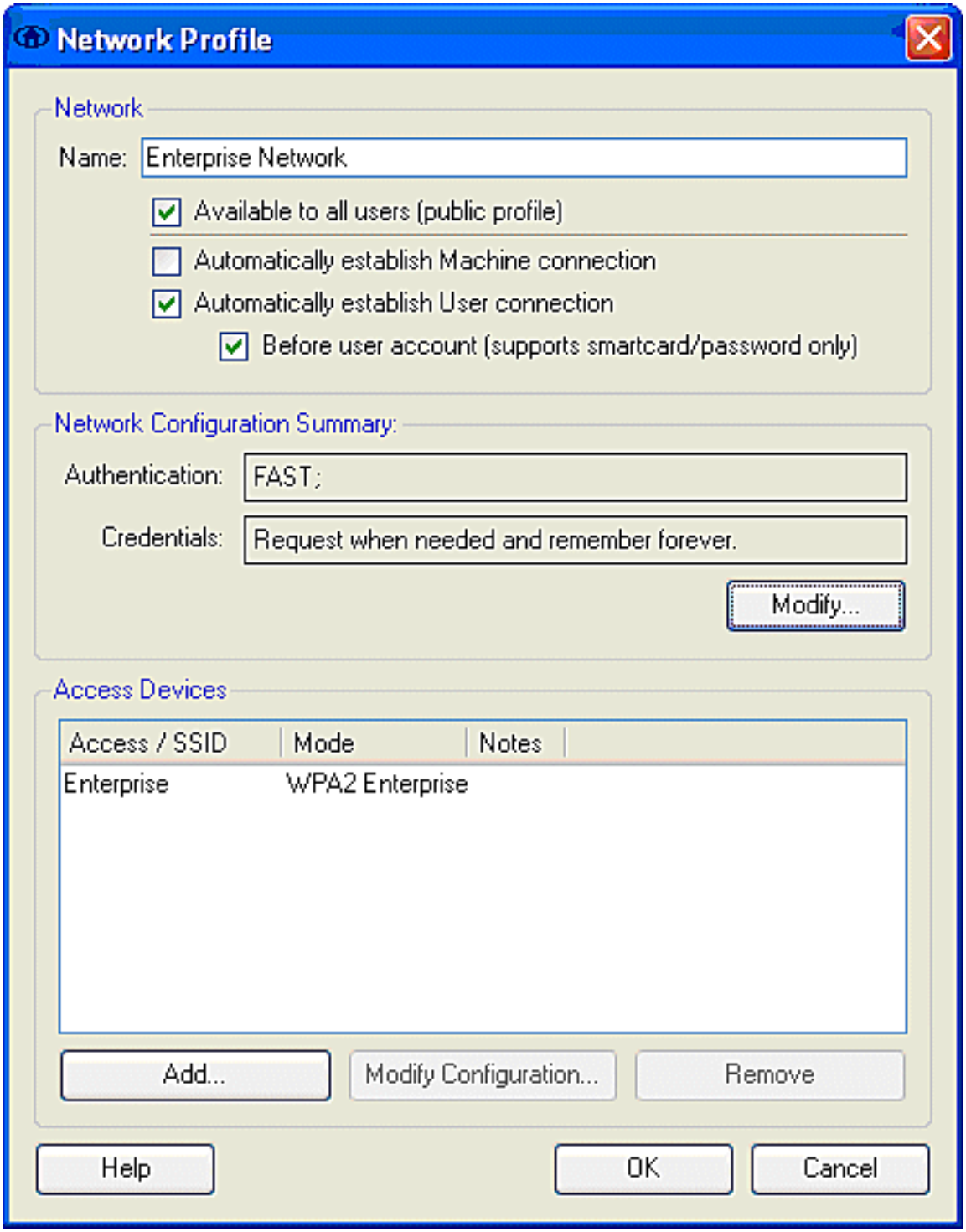
Remarque: Les configurations de port ne permettent pas des modes entreprises (802.1X) si les configurations d'authentification EAP ne sont pas des premières configurées pour le profil.

La case d'option de **réseau de création** lance la fenêtre de profil réseau, qui te permet pour associer (ou configuré) le SSID choisi avec un mécanisme d'authentification. Assignez un nom descriptif pour le profil.

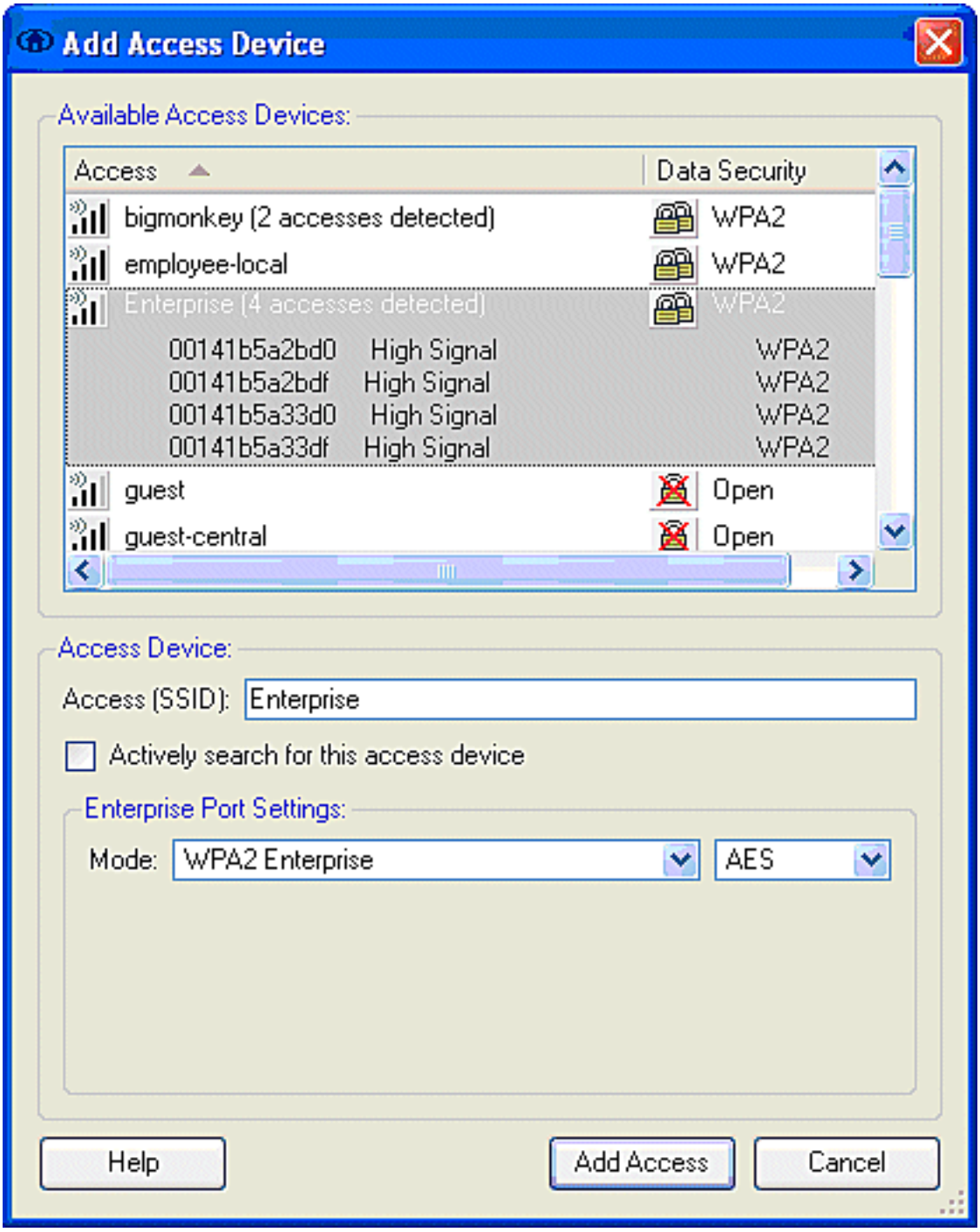
Remarque: La plusieurs Sécurité WLAN tape et/ou le SSID peut être associé sous ce profil d'authentification.

Afin d'avoir le client à connecter automatiquement au réseau quand dans la plage de couverture rf, choisissez **établissent automatiquement la connexion utilisateur**. Décochez **disponible à tous les utilisateurs** s'il n'est pas desirable d'utiliser ce profil avec d'autres comptes utilisateurs sur l'ordinateur. Si **établissez automatiquement** n'est pas choisi, il est que l'utilisateur ouvrir la fenêtre CSSC et initie manuellement la connexion WLAN avec la case d'option de **connecter**.

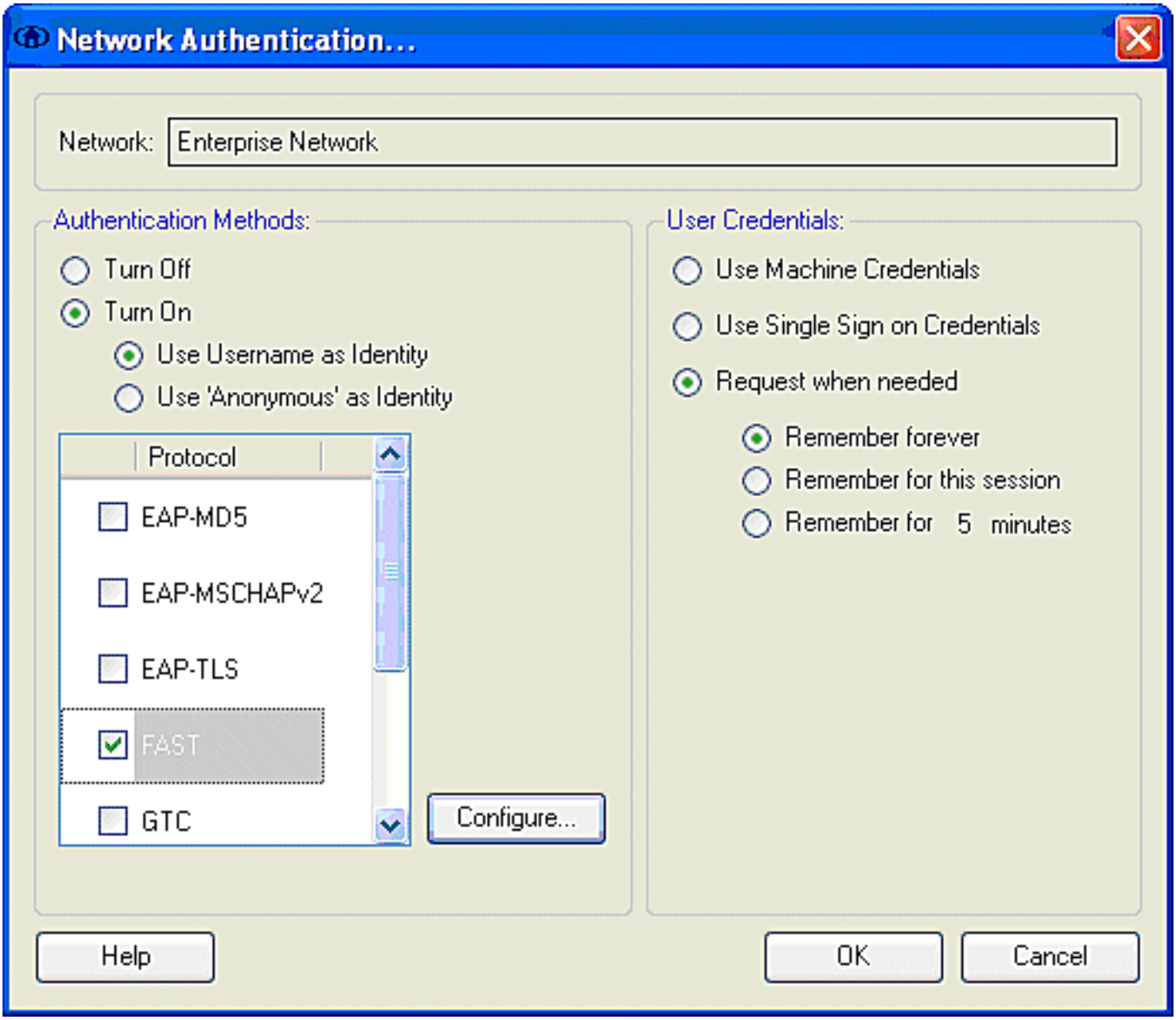
Si on le désire pour initier la connexion WLAN avant le login d'utilisateur, choisissez **avant le compte utilisateur**. Ce autorisations Simple-Signe-sur l'exécution avec les identifiants utilisateurs enregistrés (mot de passe ou certificat/carte à puce quand vous utilisez le TLS dans l'EAP-FAST).



Remarque: Pour l'exécution WPA/TKIP avec l'adaptateur de client de Gamme Cisco Aironet 350, il est nécessaire de désactiver la validation de prise de contact WPA puisqu'il y a actuellement une incompatibilité entre le client CSSC et 350 gestionnaires en ce qui concerne la prise de contact WPA hachez la validation. Ceci est désactivé sous le **client > les paramètres avancés > la validation de la prise de contact WPA/WPA2**. La validation handicapée de prise de contact permet toujours les fonctionnalités de sécurité inhérentes à WPA (introduction et Message Integrity Check de par-paquet TKIP), mais désactive l'authentification initiale de clé WPA.



Sous le résumé de configuration réseau, le clic **modifient** pour configurer l'EAP/configurations de qualifications. Spécifiez **activent l'**authentification, choisissent Protocol de dessous **RAPIDE**, et choisissent **« anonyme » comme identité** (afin de n'utiliser aucun nom d'utilisateur dans la demande initiale d'EAP). Il est possible d'utiliser le **nom d'utilisateur d'utilisation comme Identityas l'**identité externe d'EAP, mais beaucoup de clients ne souhaitent pas exposer les user-id dans la demande décryptée initiale d'EAP. Spécifiez l'**utilisation simple se connectent des qualifications** pour utiliser des qualifications de login pour l'authentification de réseau. Cliquez sur Configure pour installer des paramètres d'EAP-FAST.



Sous les configurations RAPIDES, il est possible de spécifier **valident le certificat de serveur**, qui permet au client pour valider le certificat du serveur d'EAP-FAST (ACS) avant l'établissement d'une session d'EAP-FAST. Ceci assure la protection pour les périphériques de client contre la connexion à un serveur d'EAP-FAST d'inconnu ou d'escroc et la soumission négligente de leurs qualifications d'authentification à une source non approuvée. Ceci exige que le serveur ACS font installer un certificat et le client fait également installer le certificat correspondant d'autorité de certification de racine. Dans cet exemple, la validation de certificat de serveur n'est pas activée.

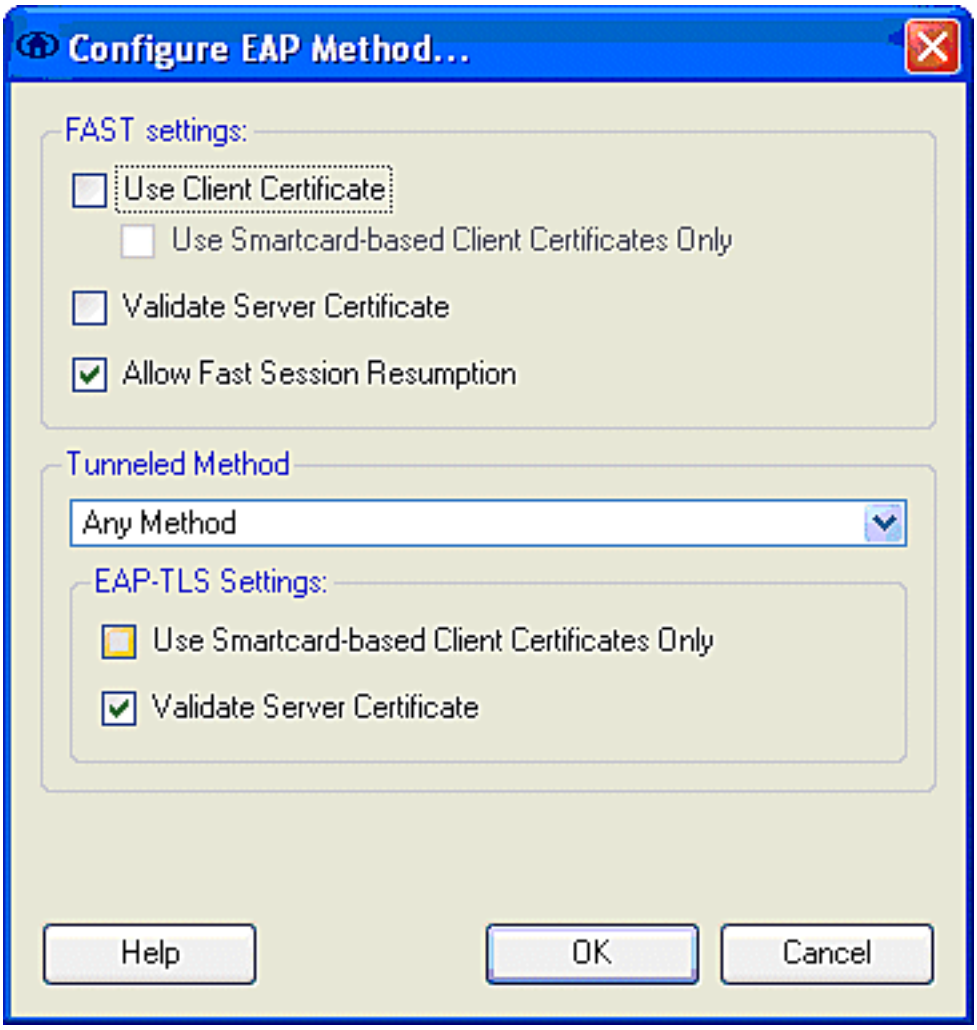
Sous les configurations RAPIDES, il est possible de spécifier **permettent la reprise rapide de session**, qui permet la reprise d'une session d'EAP-FAST basée sur les informations de tunnel (session de TLS) plutôt que la condition requise d'une pleine réauthentification d'EAP-FAST. Si le serveur et le client d'EAP-FAST ont la notoriété publique des informations de session de TLS négociées dans l'échange d'authentification initial d'EAP-FAST, la reprise de session peut se produire.

Remarque: Le serveur et le client d'EAP-FAST doivent être configurés pour la reprise de session d'EAP-FAST.

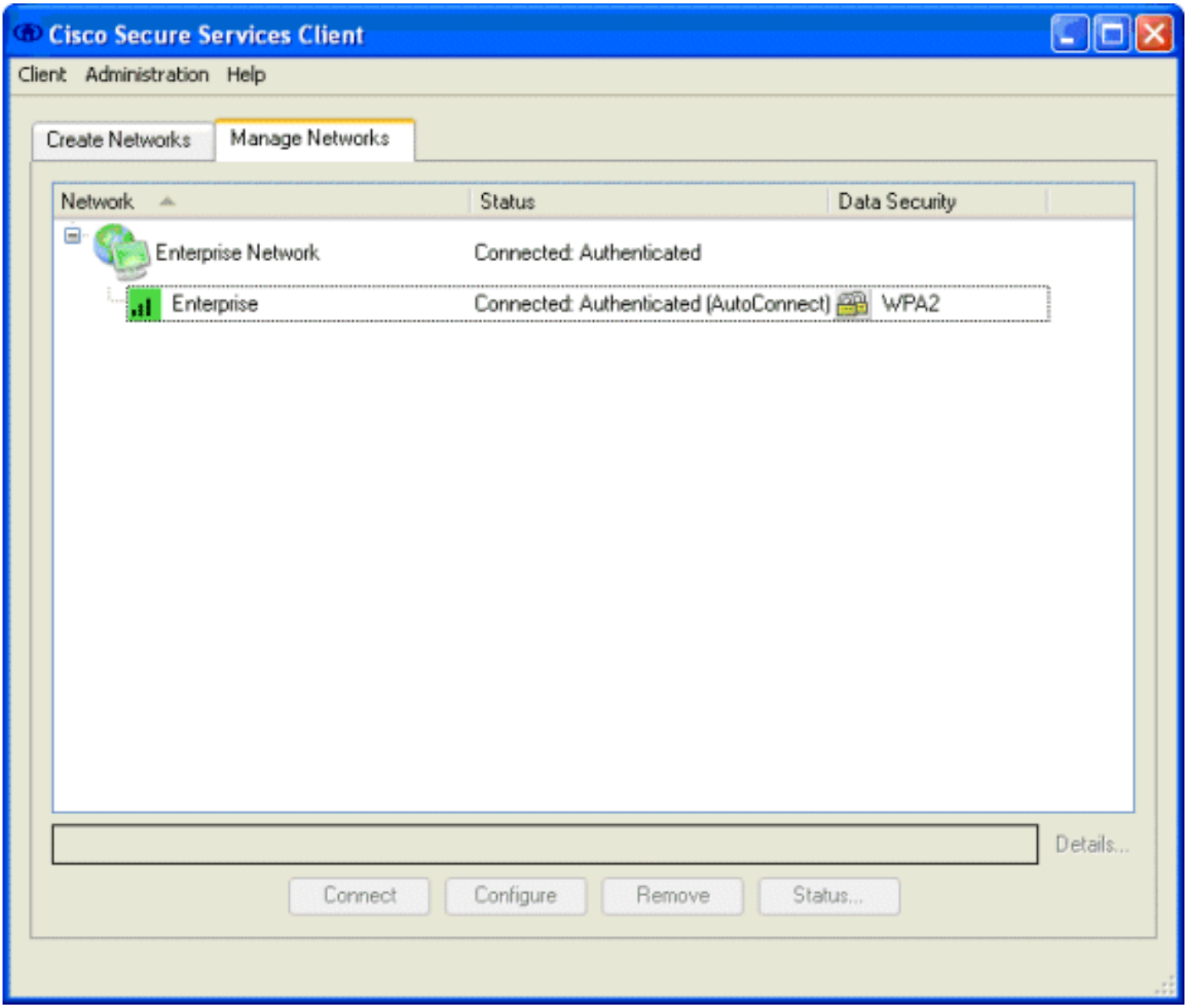
Sous la méthode > les configurations percées un tunnel d'EAP-TLS, spécifiez **n'importe quelle méthode** pour permettre l'EAP-MSCHAPv2 pour l'automatique-disposition PAC et EAP-GTC pour l'authentification. Si vous utilisez une base de données de Microsoft-format, telle que le Répertoire

actif, et si si ne prend en charge aucun client de l'EAP-FAST v1 sur le réseau, vous pouvez également spécifier l'utilisation de **MSCHAPv2** seulement comme méthode percée un tunnel.

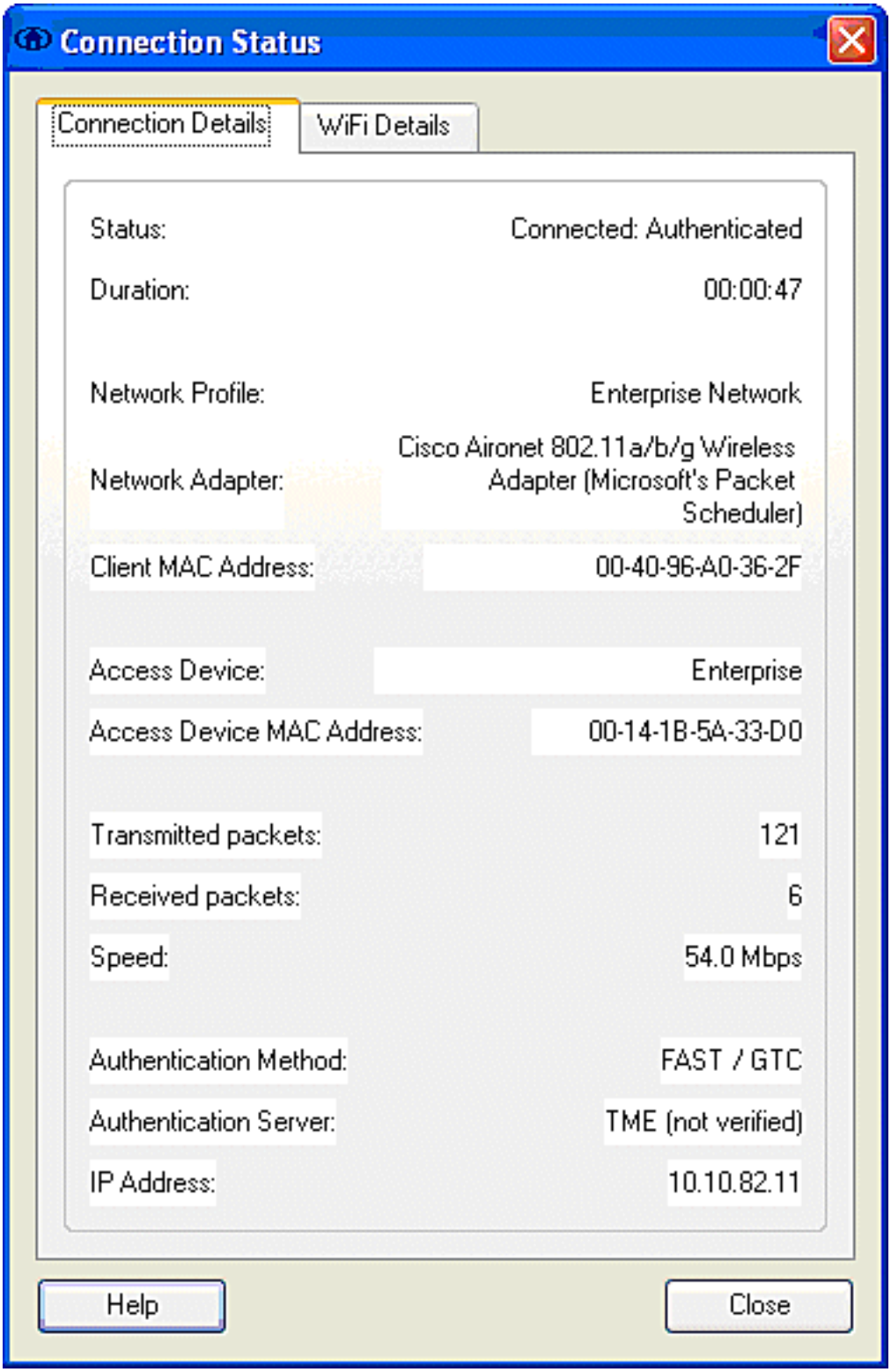
Remarque: Validez le certificat de serveur est activé par défaut sous les configurations d'EAP-TLS sur cette fenêtre. Puisque l'exemple n'utilise pas l'EAP-TLS comme méthode d'authentification intérieure, ce champ s'applique pas applicable. Si ce champ est activé, il permet au client de valider le certificat de serveur en plus de la validation de serveur du certificat client dans l'EAP-TLS.

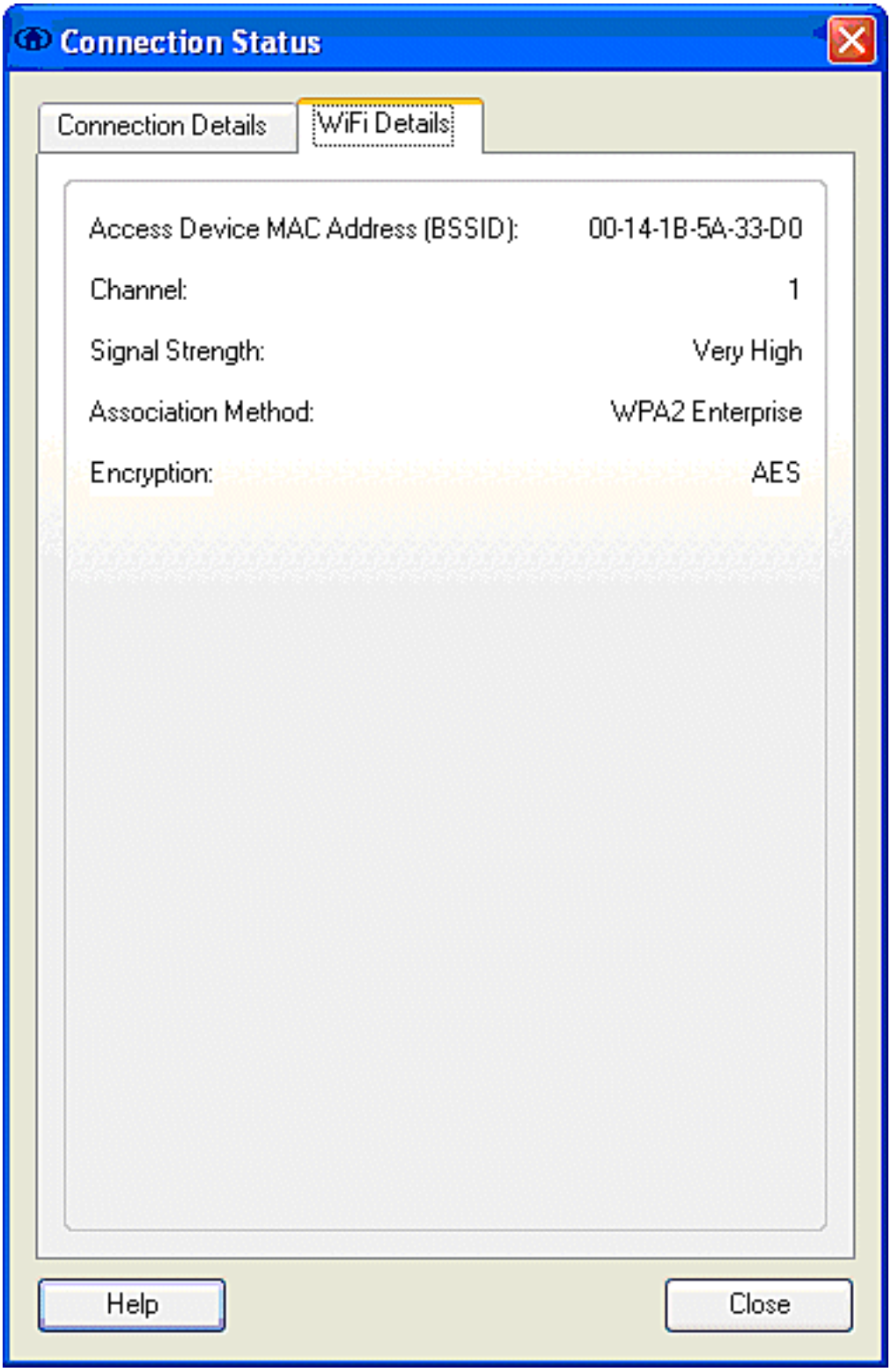


Cliquez sur OK pour sauvegarder les configurations d'EAP-FAST. Puisque le client est configuré pour « automatiquement établissez » sous le profil, il initie automatiquement l'association/authentification avec le réseau. De l'onglet de réseaux de gérer, les champs de réseau, d'état, et de protection des données indiquent l'état de la connexion du client. De l'exemple, on le voit que le réseau d'entreprise de profil est en service, et le périphérique d'accès au réseau est l'entreprise SSID, qui indique connecté : Authentifié et les utilisations Autoconnect. Le champ de protection des données indique le type de cryptage de 802.11 qui est utilisé, qui, pour cet exemple, est WPA2.



Après que le client authentifie, choisissez le **SSID** sous le profil dans l'onglet de réseaux de gérer et cliquez sur l'**état** pour questionner des détails de connexion. La fenêtre de détails de connexion fournit des informations sur le périphérique de client, l'état de la connexion et les statistiques, et la méthode d'authentification. L'onglet de détails de WiFi fournit des détails sur l'état de la connexion de 802.11, qui inclut le RSSI, le canal de 802.11, et l'authentification/cryptage.


Connection Status
Connection Details
WiFi Details
Status:
Connected: Authenticated
Duration:
00:00:47
Network Profile:
Enterprise Network
Network Adapter:
Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:
00-40-96-A0-36-2F
Access Device:
Enterprise
Access Device MAC Address:
00-14-1B-5A-33-D0
Transmitted packets:
121
Received packets:
6
Speed:
54.0 Mbps
Authentication Method:
FAST / GTC
Authentication Server:
TME (not verified)
IP Address:
10.10.82.11
Help
Close



En tant qu'administrateur système, vous avez droit à l'utilitaire diagnostique, l'état de système de Cisco Secure Services Client, qui est disponible avec la distribution standard CSSC. Cet utilitaire est dès le début menu disponible ou à partir du répertoire CSSC. Afin d'obtenir des données, le clic **collectent les données > la copie au presse-papier > localisent le fichier de rapport**. Ceci dirige une fenêtre d'explorateur de fichiers de Microsoft vers le répertoire avec le fichier de rapport fermé la fermeture éclair. Dans le fichier fermé la fermeture éclair, les la plupart des informations utiles se trouvent sous le log (log_current).

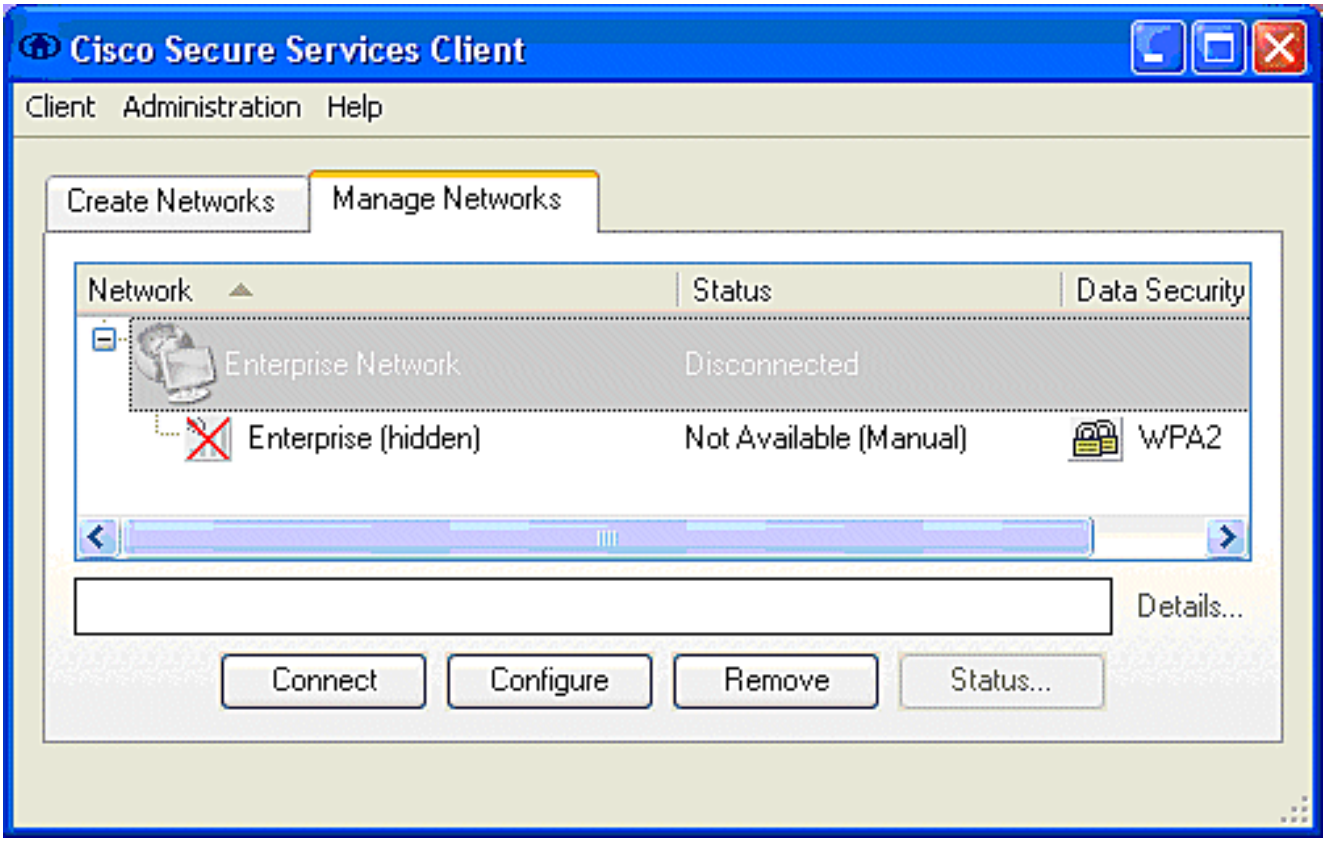
L'utilitaire donne l'état actuel de CSSC, interface, et détails de gestionnaire, avec les informations WLAN (SSID détecté, état d'association, etc.). Ceci peut être utile, particulièrement diagnostiquer des problèmes de connectivité entre CSSC et l'adaptateur WLAN.

Vérifiez l'exécution

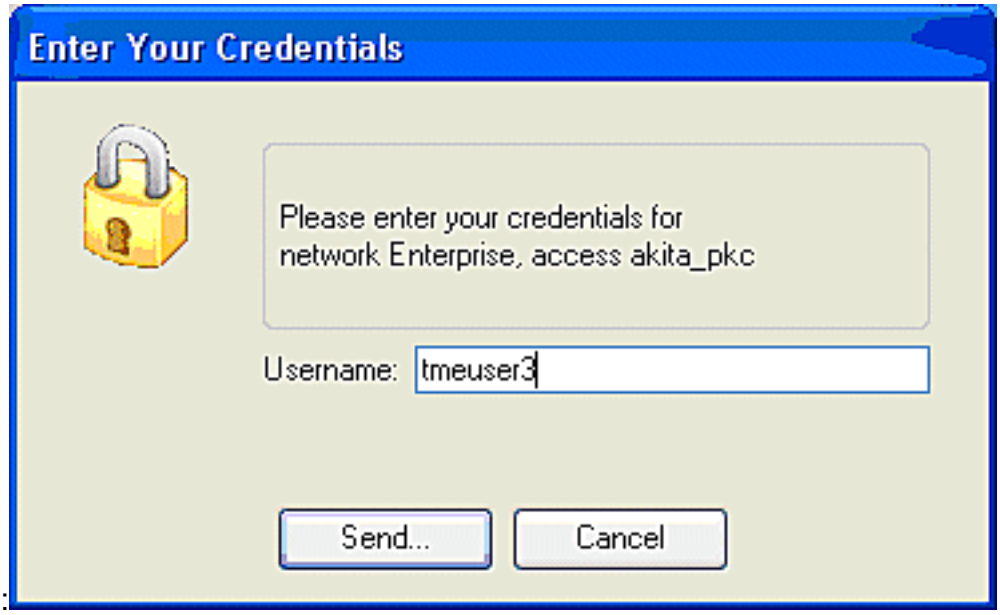
Après la configuration du serveur de Cisco Secure ACS, du contrôleur WLAN, du client CSSC, et vraisemblablement de la population de configuration correcte et de base de données, le réseau WLAN est configuré pour l'authentification d'EAP-FAST et la communication client sécurisée. Il y a de nombreux points qui peuvent être surveillés pour vérifier la progression/erreurs pour une session sécurisée.

Afin de tester la configuration, tentative d'associer un client sans fil avec le contrôleur WLAN avec l'authentification d'EAP-FAST.

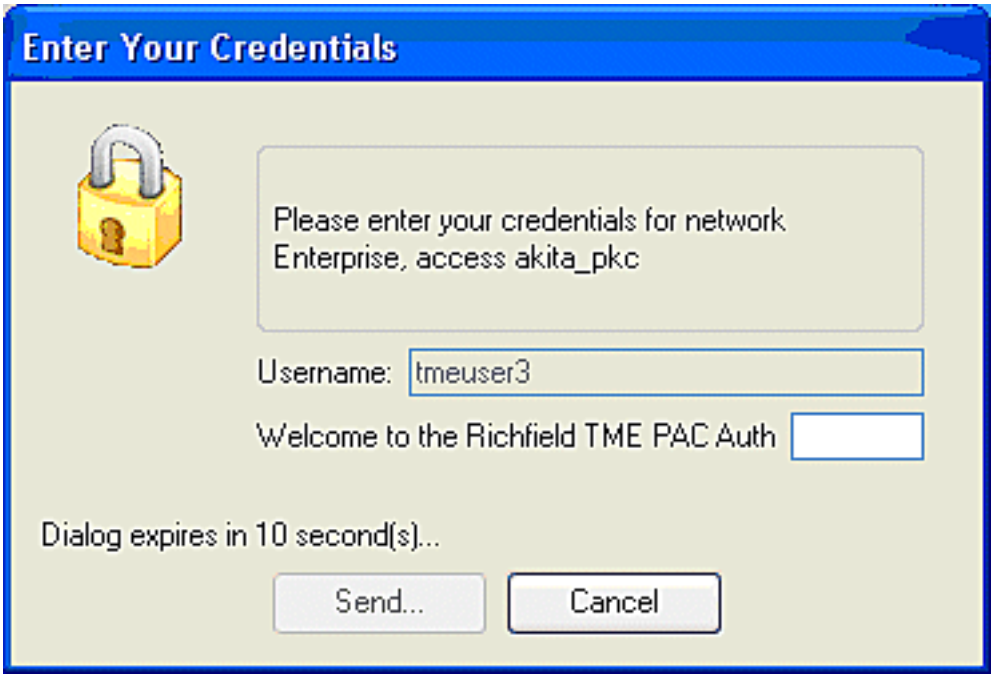
1. Si CSSC est configuré pour l'autoconnexion, le client tente cette connexion automatiquement. S'il n'est pas configuré pour l'autoconnexion et l'exécution simple d'ouverture de session, l'utilisateur doit initier la connexion WLAN par la case d'option de **connecter**. Ceci initie le processus d'association de 802.11 au-dessus dont l'authentification EAP se produit.Voici un exemple
   :



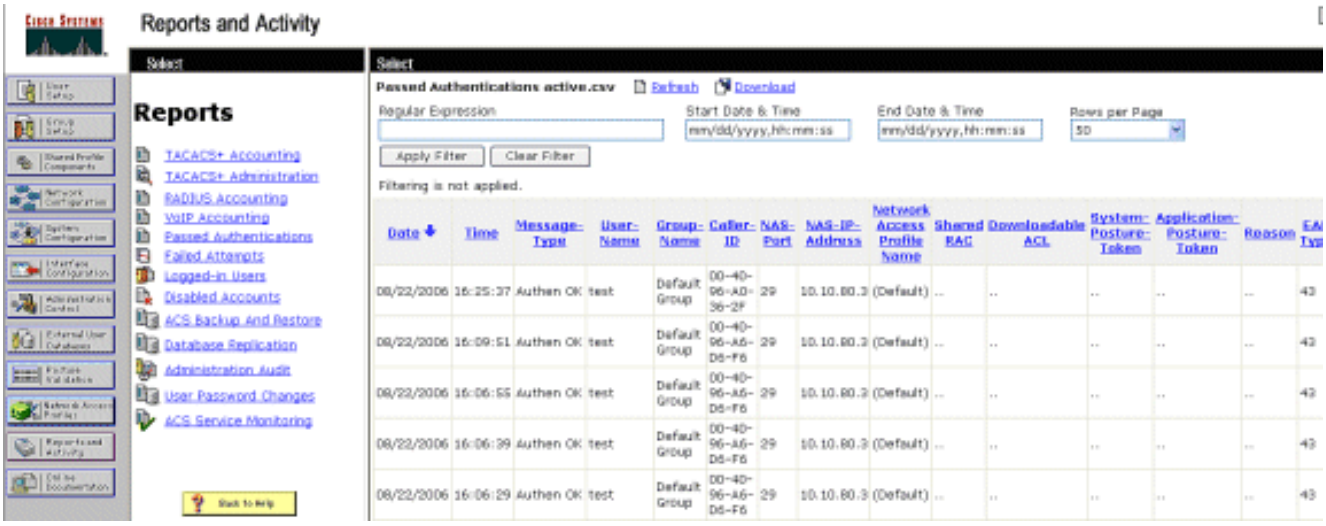
2. L'utilisateur est ultérieurement incité à fournir le nom d'utilisateur et puis le mot de passe pour l'authentification d'EAP-FAST (de l'autorité PAC d'EAP-FAST ou de l'ACS).Voici un exemple



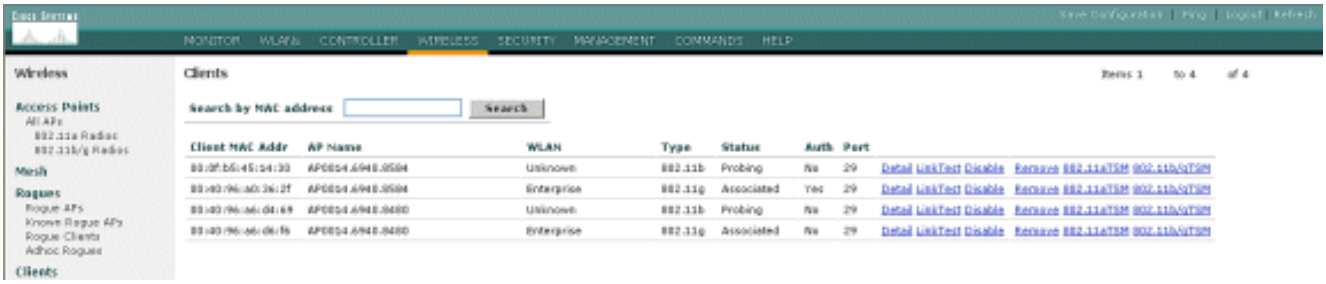
:



3. Le client CSSC, par le WLC, passe alors les identifiants utilisateurs au serveur de RADIUS (Cisco Secure ACS) afin de valider les qualifications. ACS vérifie les identifiants utilisateurs avec une comparaison des données et de la base de données configurée (en exemple de configuration, la base de données externe est Répertoire actif de Windows) et permet d'accéder au client sans fil toutes les fois que les identifiants utilisateurs sont valides. L'état passé d'authentifications sur le serveur ACS prouve que le client a passé l'authentification RADIUS/EAP.Voici un exemple
:



4. Sur l'authentification réussie RADIUS/EAP, le client sans fil (00:40:96:ab:36:2f dans cet exemple) est authentifié avec le contrôleur WLAN AP.



Annexe

En plus du diagnostic et des informations d'état, qui sont disponibles au contrôleur de Cisco Secure ACS et de WLAN Cisco, il y a des points supplémentaires qui peuvent être utilisés pour diagnostiquer l'authentification d'EAP-FAST. Bien que la majorité de questions d'authentification puisse être diagnostiquée sans utilisation d'un renifleur WLAN ou échanges d'EAP d'élimination des imperfections au contrôleur WLAN, ce manuel de référence est inclus pour aider à dépanner.

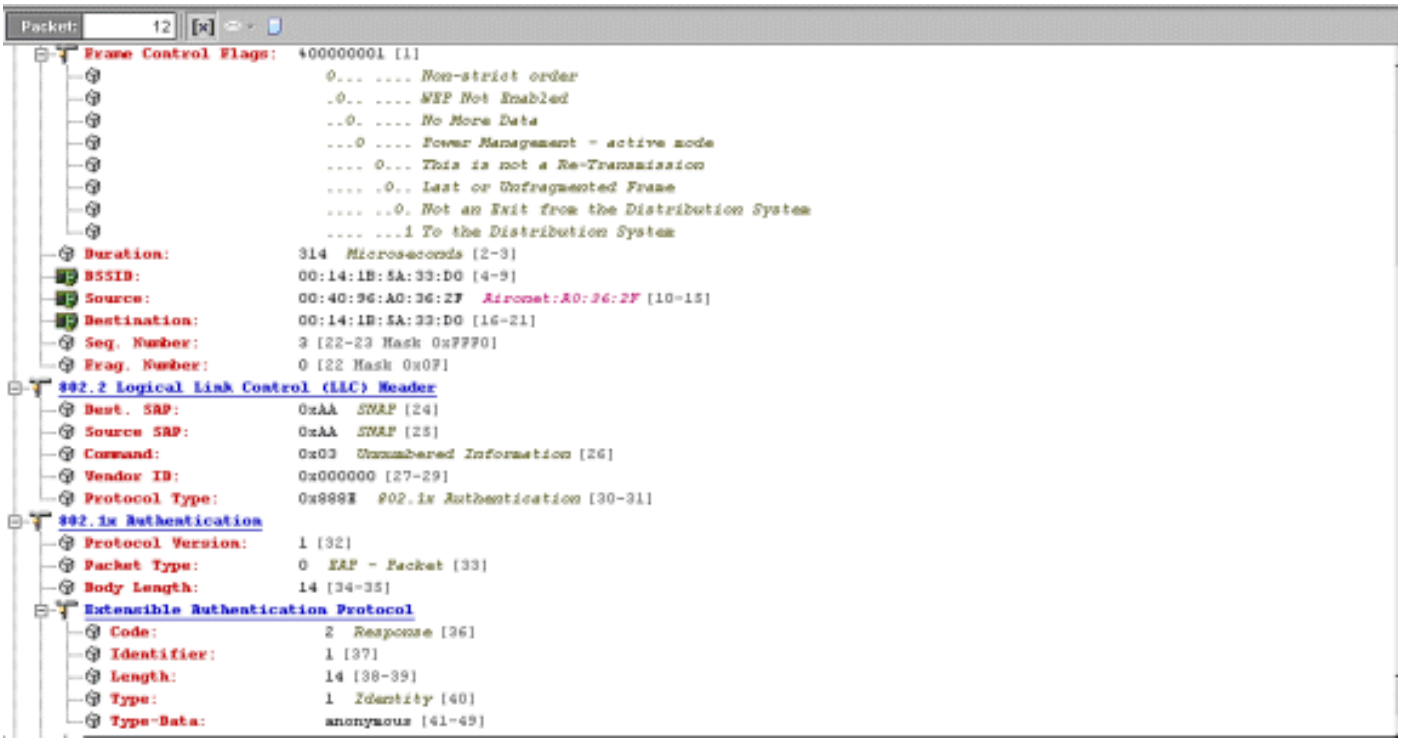
Capture de renifleur pour l'échange d'EAP-FAST

Cette capture de renifleur de 802.11 affiche l'échange d'authentification.

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F......,SN=2868,FN= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.......,SN= 3,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.123517	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	65	00.165611	802.1x	FC=.F......,SN=2870,FN= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.......,SN= 4,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.174228	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F......,SN=2871,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.......,SN= 5,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T..R....,SN= 5,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.203639	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	70%	54.0	188	00.207634	802.1x	FC=.F......,SN=2872,FN= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.......,SN= 6,FN= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T..R....,SN= 6,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.217754	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F......,SN=2874,FN= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.......,SN= 7,FN= 0
00:14:1B:5A:33:D0	#	11	68%	1.0	14	00.254499	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R....,SN=2875,FN= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.......,SN= 8,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.318383	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F......,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F......,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T.......,SN= 9,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.334019	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	65%	54.0	207	00.340467	802.1x	FC=.F......,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R....,SN=2879,FN= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T.......,SN= 10,FN= 0

Ce paquet affiche la réponse initiale d'EAP d'EAP-FAST.

Remarque: Comme configuré au client CSSC, anonyme est utilisé comme identité externe d'EAP dans la réponse initiale d'EAP.



Debug au contrôleur WLAN

Ces commandes de débogage peuvent être utilisées au contrôleur WLAN pour surveiller la progression de l'échange d'authentification :

- **enable d'événements de debug aaa**
- **enable de détail de debug aaa**

- enable d'événements de debug dot1x
- enable d'états de debug dot1x

C'est un exemple du début d'une transaction d'authentification entre le client CSSC et l'ACS comme surveillé au contrôleur WLAN avec met au point :

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
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.
```

C'est la réussite de l'échange d'EAP du contrôleur mettent au point (avec authentification WPA2) :

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
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.
```

Informations connexes

- Guide d'installation pour le Cisco Secure ACS pour des Windows Server
- Guide de configuration pour le Cisco Secure ACS 4.1
- Exemple de configuration de restriction de l'accès au réseau local sans fil sur SSID avec WLC et Cisco Secure ACS
- EAP-TLS sous un réseau sans fil unifié avec ACS 4.0 et Windows 2003
- Exemple de configuration d'une affectation de VLAN dynamique avec un serveur RADIUS et un contrôleur de réseau local sans fil
- Support et documentation techniques - Cisco Systems