

Cisco Secure Services Client avec authentification EAP-FAST

Contenu

[Introduction](#)

[Conditions préalables](#)

[Exigence](#)

[Components Used](#)

[Conventions](#)

[Paramètres de conception](#)

[Base de données](#)

[Chiffrement](#)

[Authentification unique et informations d'identification de la machine](#)

[Diagramme du réseau](#)

[Configuration du serveur de contrôle d'accès \(ACS\)](#)

[Ajouter un point d'accès en tant que client AAA \(NAS\) dans ACS](#)

[Configurer ACS afin d'interroger la base de données externe](#)

[Activer la prise en charge EAP-FAST sur ACS](#)

[Contrôleur WLAN Cisco](#)

[Configuration du contrôleur de réseau local sans fil](#)

[Fonctionnement de base et enregistrement du LAP au contrôleur](#)

[Authentification RADIUS via Cisco Secure ACS](#)

[Configuration des paramètres WLAN](#)

[Vérifier le fonctionnement](#)

[Annexe](#)

[Capture de renifleur pour EAP-FAST Exchange](#)

[Déboguer au niveau du contrôleur WLAN](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer Cisco Secure Services Client (CSSC) avec les contrôleurs LAN sans fil, le logiciel Microsoft Windows 2000[®] et Cisco Secure Access Control Server (ACS) 4.0 via EAP-FAST. Ce document présente l'architecture EAP-FAST et fournit des exemples de déploiement et de configuration. CSSC est le composant logiciel client qui fournit la communication des informations d'identification des utilisateurs à l'infrastructure afin d'authentifier un utilisateur sur le réseau et d'attribuer un accès approprié.

Voici quelques-uns des avantages de la solution CSSC, comme indiqué dans ce document :

- Authentification de chaque utilisateur (ou périphérique) avant l'autorisation d'accès au

- WLAN/LAN avec le protocole EAP (Extensible Authentication Protocol)
- Solution de sécurité WLAN de bout en bout avec composants serveur, authentificateur et client
 - Solution commune pour l'authentification filaire et sans fil
 - Clés de chiffrement dynamiques par utilisateur dérivées du processus d'authentification
 - Aucune exigence pour les infrastructures à clé publique (PKI) ou les certificats (vérification des certificats facultative)
 - Affectation de stratégie d'accès et/ou cadre EAP NAC

Remarque : Reportez-vous au [Plan d'action Cisco SAFE Wireless](#) pour obtenir des informations sur le déploiement d'un réseau sans fil sécurisé.

La structure d'authentification 802.1x a été intégrée dans la norme 802.11i (Wireless LAN Security) pour activer les fonctions d'authentification, d'autorisation et de comptabilité de couche 2 dans un réseau LAN sans fil 802.11. Aujourd'hui, plusieurs protocoles EAP sont disponibles pour le déploiement dans les réseaux filaires et sans fil. Les protocoles EAP couramment déployés incluent LEAP, PEAP et EAP-TLS. En plus de ces protocoles, Cisco a défini et mis en oeuvre le protocole EAP Flexible Authentication through Secure Tunnel (EAP-FAST) en tant que protocole EAP normalisé disponible pour le déploiement dans les réseaux LAN filaires et sans fil. La spécification du protocole EAP-FAST est accessible au public sur le [site de l'IETF](#).

Comme pour d'autres protocoles EAP, EAP-FAST est une architecture de sécurité client-serveur qui chiffre les transactions EAP dans un tunnel TLS. Bien que similaire à PEAP ou EAP-TTLS à cet égard, il diffère en ce sens que l'établissement du tunnel EAP-FAST est basé sur des clés secrètes partagées fortes qui sont uniques à chaque utilisateur par rapport à PEAP/EAP-TTLS (qui utilisent un certificat de serveur X.509 pour protéger la session d'authentification). Ces clés secrètes partagées sont appelées PAC (Protected Access Credential) et peuvent être distribuées automatiquement (Automatic ou In-band Provisioning) ou manuellement (Manual ou Out-of-band Provisioning) aux périphériques clients. Étant donné que les échanges basés sur des secrets partagés sont plus efficaces que les échanges basés sur une infrastructure PKI, EAP-FAST est le type EAP le plus rapide et le moins gourmand en processeurs de ceux qui fournissent des échanges d'authentification protégés. EAP-FAST est également conçu pour simplifier le déploiement car il ne nécessite pas de certificat sur le client LAN sans fil ou sur l'infrastructure RADIUS, mais intègre un mécanisme de provisionnement intégré.

Voici quelques-unes des principales fonctionnalités du protocole EAP-FAST :

- Authentification unique (SSO) avec nom d'utilisateur/mot de passe Windows
- Prise en charge de l'exécution du script de connexion
- Prise en charge du Wi-Fi Protected Access (WPA) sans demandeur tiers (Windows 2000 et XP uniquement)
- Déploiement simple sans infrastructure PKI requise
- Vieillessement du mot de passe Windows (c'est-à-dire prise en charge de l'expiration du mot de passe basé sur le serveur)
- Intégration avec Cisco Trust Agent pour le contrôle des admissions au réseau avec le logiciel client approprié

[Conditions préalables](#)

[Exigence](#)

Il est supposé que le programme d'installation connaît l'installation de base de Windows 2003 et l'installation de Cisco WLC, car ce document ne couvre que 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 la gamme Cisco 2000, consultez le Guide de démarrage rapide : [Contrôleurs de réseau local sans fil de la gamme Cisco 2000](#)

Avant de commencer, installez Microsoft Windows Server 2000 à l'aide du dernier logiciel Service Pack. Installez les contrôleurs et les points d'accès léger (LAP) et assurez-vous que les dernières mises à jour logicielles sont configurées.

Components Used

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

- Contrôleur de la gamme Cisco 2006 ou 4400 qui exécute 4.0.155.5
- Point d'accès LWAPP Cisco 1242
- Windows 2000 avec Active Directory
- Commutateur Cisco Catalyst 3750G
- Windows XP avec carte adaptateur CB21AG et Cisco Secure Services Client Version 4.05

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

Lorsque vous déployez un réseau WLAN et recherchez un protocole d'authentification, il est généralement recommandé d'utiliser une base de données actuelle pour l'authentification utilisateur/machine. Les bases de données typiques qui peuvent être utilisées sont Windows Active Directory, LDAP ou une base de données OTP (One Time Password) (RSA ou SecureID). Toutes ces bases de données sont compatibles avec le protocole EAP-FAST, mais lorsque vous planifiez un déploiement, certaines exigences de compatibilité doivent être prises en compte. Le déploiement initial d'un fichier PAC vers les clients s'effectue par le biais d'un provisionnement automatique anonyme, d'un provisionnement authentifié (via le certificat X.509 du client actuel) ou d'un provisionnement manuel. Pour les besoins de ce document, le provisionnement automatique anonyme et le provisionnement manuel sont pris en compte.

Le provisionnement automatique PAC utilise le protocole ADHP (Authentication Diffie-Hellman Key Agreement Protocol) pour établir un tunnel sécurisé. Le tunnel sécurisé peut être établi de manière anonyme ou via un mécanisme d'authentification du serveur. Dans la connexion de tunnel établie, MS-CHAPv2 est utilisé pour authentifier le client et, une fois l'authentification réussie, pour distribuer le fichier PAC au client. Une fois le PAC correctement provisionné, le

fichier PAC peut être utilisé pour lancer une nouvelle session d'authentification EAP-FAST afin d'obtenir un accès réseau sécurisé.

Le provisionnement automatique des PAC est pertinent pour la base de données en cours d'utilisation car, puisque le mécanisme d'approvisionnement automatique repose sur MSCHAPv2, la base de données utilisée pour authentifier les utilisateurs doit être compatible avec ce format de mot de passe. Si vous utilisez EAP-FAST avec une base de données qui ne prend pas en charge le format MSCHAPv2 (comme OTP, Novell ou LDAP), il est nécessaire d'utiliser un autre mécanisme (c'est-à-dire le provisionnement manuel ou authentifié) pour déployer des fichiers PAC utilisateur. Ce document donne un exemple de mise en service automatique avec une base de données utilisateur Windows.

Chiffrement

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

Si les périphériques clients ne prennent pas en charge WPA2 ou WPA, il est possible de déployer l'authentification 802.1X avec des clés WEP dynamiques, mais en raison des exploits connus contre les clés WEP, ce mécanisme de cryptage WLAN n'est pas recommandé. S'il est nécessaire de prendre en charge des clients WEP uniquement, il est recommandé d'utiliser un intervalle de temporisation de session, qui nécessite que les clients dérivent une nouvelle clé WEP sur un intervalle fréquent. L'intervalle de session recommandé pour les débits de données WLAN standard est de trente minutes.

Authentification unique et informations d'identification de la machine

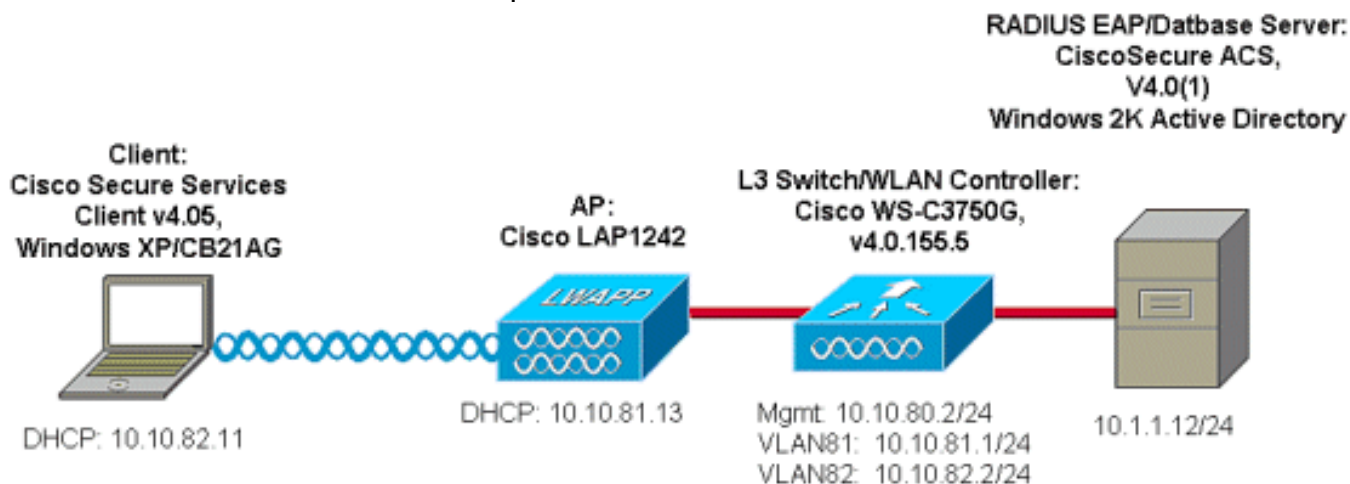
L'authentification unique désigne la capacité d'un utilisateur unique à se connecter ou à entrer des informations d'identification d'authentification pour accéder à plusieurs applications ou périphériques. Pour les besoins de ce document, l'authentification unique fait référence à l'utilisation des informations d'identification utilisées pour se connecter à un PC en vue de l'authentification au WLAN.

Avec Cisco Secure Services Client, il est possible d'utiliser les informations d'identification d'un utilisateur pour s'authentifier également sur le réseau WLAN. Si vous souhaitez authentifier un PC sur le réseau avant que l'utilisateur ne se connecte au PC, vous devez utiliser les informations d'identification stockées ou les informations d'identification liées à un profil de machine. L'une ou l'autre de ces méthodes est utile dans les cas où il est souhaitable d'exécuter des scripts d'ouverture de session ou des lecteurs de mappage au démarrage de l'ordinateur, par opposition à lorsqu'un utilisateur se connecte.

Diagramme du réseau

Il s'agit du diagramme de réseau utilisé dans ce document. Dans ce réseau, quatre sous-réseaux sont utilisés. Notez qu'il n'est pas nécessaire de segmenter ces périphériques en différents réseaux, mais cela offre la plus grande flexibilité pour l'intégration aux réseaux réels. Le contrôleur LAN sans fil intégré Catalyst 3750G fournit des ports de commutation PoE (Power Over Ethernet), une commutation de couche 3 et des fonctionnalités de contrôleur WLAN sur un châssis commun.

1. Le réseau 10.1.1.0 est le réseau du serveur sur lequel réside ACS.
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 résident les points d'accès.
4. Le réseau 10.10.82.0 est utilisé pour les clients WLAN.



Configuration du serveur de contrôle d'accès (ACS)

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

Remarque : Utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement) pour en savoir plus sur les commandes figurant dans le présent document.

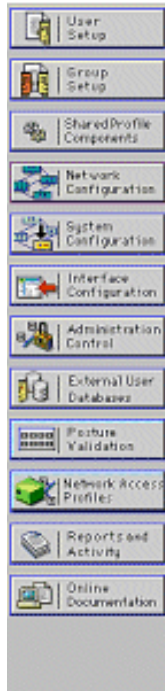
Ajouter un point d'accès en tant que client AAA (NAS) dans ACS

Cette section décrit comment configurer ACS pour EAP-FAST avec le provisionnement PAC intrabande avec Windows Active Directory en tant que base de données externe.

1. Connectez-vous à **ACS > Network Configuration** et cliquez sur **Add Entry**.
2. Complétez le nom du contrôleur WLAN, l'adresse IP, la clé secrète partagée et sous Authentifier à l'aide, choisissez RADIUS (Cisco Airespace), qui inclut également les attributs RADIUS IETF. **Remarque :** si les groupes de périphériques réseau (NDG) sont activés, choisissez d'abord le NDG approprié et ajoutez-y le contrôleur WLAN. Reportez-vous au Guide de configuration ACS pour plus de détails sur le NDG.
3. Cliquez sur **Soumettre+**
Redémarrer.



Edit



AAA Client Setup For ws-3750

AAA Client IP Address	<input type="text" value="10.10.80.3"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco Airespace)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

[Back to Help](#)

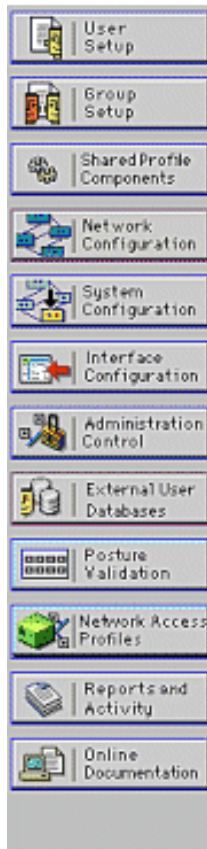
[Configurer ACS afin d'interroger la base de données externe](#)

Cette section décrit comment configurer ACS afin d'interroger la base de données externe.

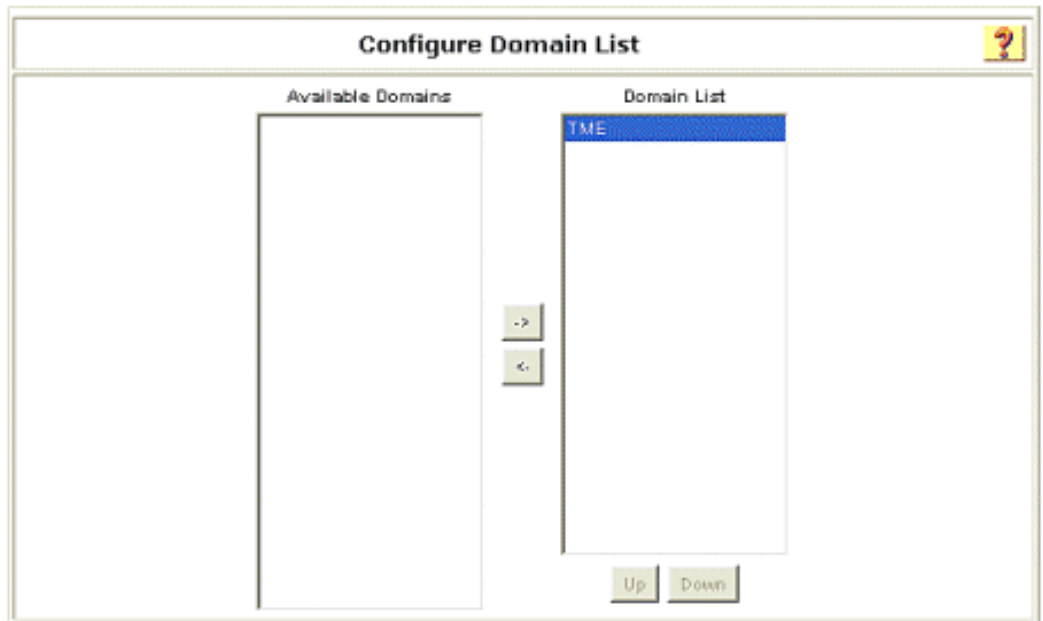
1. Cliquez sur **Base de données utilisateur externe > Configuration de base de données > Base de données Windows > Configurer**.
2. Sous Configurer la liste de domaines, déplacez **les domaines** des domaines disponibles vers la liste de domaines. **Remarque** : le serveur qui exécute ACS doit connaître ces domaines pour que l'application ACS puisse détecter et utiliser ces domaines à des fins d'authentification.



External User Databases



If the unknown user policy contains additional external databases and the Windows database is not the last database on the Selected Databases list, you may enable this option.



3. Sous Paramètres EAP de Windows, configurez l'option pour autoriser le changement de mot de passe dans la session PEAP ou EAP-FAST. Reportez-vous au [Guide de configuration de Cisco Secure ACS 4.1](#) afin d'obtenir plus de détails sur l'obsolescence des mots de passe EAP-FAST et Windows.
4. Cliquez sur Submit. **Remarque** : Vous pouvez également activer la fonctionnalité d'autorisation de numérotation pour EAP-FAST sous Configuration de la base de données utilisateur Windows afin d'autoriser la base de données externe Windows à contrôler l'autorisation d'accès. Les paramètres MS-CHAP pour la modification du mot de passe sur la page de configuration de la base de données Windows ne s'appliquent qu'à l'authentification MS-CHAP non EAP. Afin d'activer la modification de mot de passe en conjonction avec EAP-FAST, il est nécessaire d'activer la modification de mot de passe sous les paramètres EAP de Windows.

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Windows EAP Settings ?

Enable password change inside PEAP or EAP-FAST.
 EAP-TLS Strip Domain Name.

Machine Authentication.

Enable PEAP machine authentication.
 Enable EAP-TLS machine authentication.
 EAP-TLS and PEAP machine authentication name prefix:

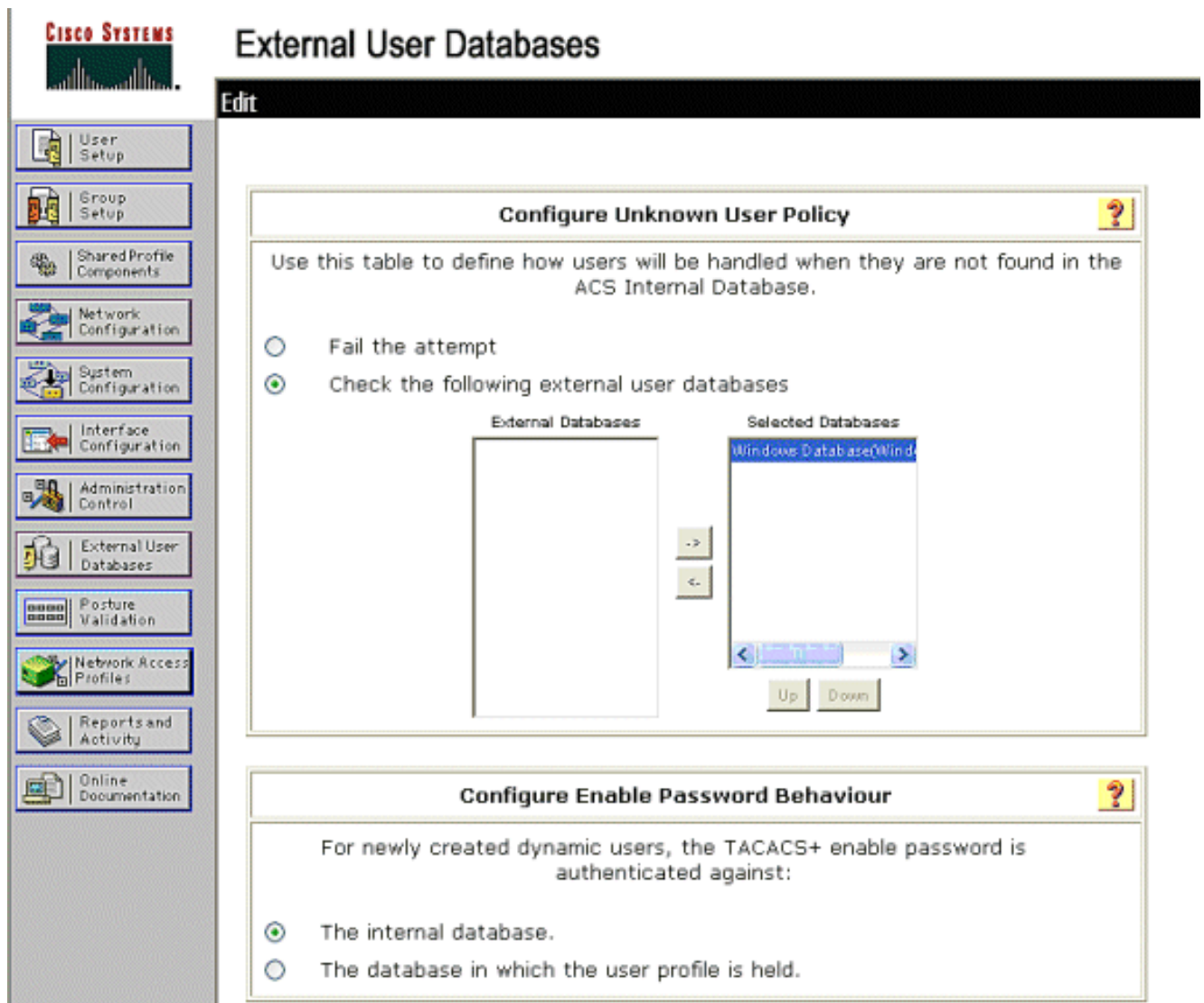
Enable machine access restrictions.
 Aging time (hours):
 Group map for successful user authentication without machine authentication:

User Groups that are exempt from passing machine authentication:

Available User Groups		Selected User Groups
Default Group	->	
Group 1	->	
Group 2	->	
Group 3	->	
Group 4	->	
Group 5	->	
Group 6	->	
Group 7	->	
Group 8	->	

These settings can be used to enable or disable specific Windows EAP functionality

5. Cliquez sur **Base de données des utilisateurs externes > Stratégie des utilisateurs inconnus** et sélectionnez la case d'option **Vérifier les bases de données des utilisateurs externes suivantes**.
6. Déplacez la base de données Windows des **bases de données externes** vers les **bases de données sélectionnées**.
7. Cliquez sur **Submit**. **Remarque** : À partir de ce point, ACS vérifie la base de données Windows. Si l'utilisateur est introuvable dans la base de données locale ACS, il le place dans le groupe par défaut ACS. Reportez-vous à la documentation ACS pour plus de détails sur les mappages de groupes de bases de données. **Remarque** : lorsque ACS interroge la base de données Microsoft Active Directory pour vérifier les informations d'identification des utilisateurs, des paramètres de droits d'accès supplémentaires doivent être configurés sous Windows. Reportez-vous au [Guide d'installation de Cisco Secure ACS pour Windows Server](#) pour plus de détails.



External User Databases

Edit

Configure Unknown User Policy

Use this table to define how users will be handled when they are not found in the ACS Internal Database.

Fail the attempt
 Check the following external user databases

External Databases: [Empty List]

Selected Databases: Windows Database@Wind

Up Down

Configure Enable Password Behaviour

For newly created dynamic users, the TACACS+ enable password is authenticated against:

The internal database.
 The database in which the user profile is held.

[Activer la prise en charge EAP-FAST sur ACS](#)

Cette section décrit comment activer la prise en charge EAP-FAST sur ACS.

1. Accédez à **Configuration du système > Configuration de l'authentification globale > Configuration EAP-FAST.**
2. Sélectionnez **Autoriser EAP-FAST.**
3. Configurez ces recommandations : TTL/TTL/TTL/TTL PAC/TTL de la clé principale retraitée. Ces paramètres sont configurés par défaut dans Cisco Secure ACS :Durée de vie de la clé principale : 1 moisDurée de vie de la clé retraitée : 3 moisTTL PAC : 1 semaine
4. Remplissez le champ **Informations sur l'ID d'autorité.** Ce texte est affiché sur certains logiciels clients EAP-FAST où la sélection de l'autorité PAC est le contrôleur.**Remarque :** Cisco Secure Services Client n'utilise pas ce texte descriptif pour l'autorité PAC.
5. Sélectionnez le champ **Autoriser le provisionnement PAC intrabande.** Ce champ active le provisionnement PAC automatique pour les clients EAP-FAST correctement activés. Dans cet exemple, le provisionnement automatique est utilisé.
6. Choisissez **les méthodes internes autorisées** : EAP-GTC et EAP-MSCHAP2. Cela permet le fonctionnement des clients EAP-FAST v1 et EAP-FAST v1a. (Cisco Secure Services Client prend en charge EAP-FAST v1a.) S'il n'est pas nécessaire de prendre en charge les clients EAP-FAST v1, il est seulement nécessaire d'activer EAP-MSCHAPv2 comme méthode interne.

7. Cochez la case **Serveur maître EAP-FAST** pour activer ce serveur EAP-FAST en tant que serveur maître. Cela permet aux autres serveurs ACS d'utiliser ce serveur en tant qu'autorité PAC maître afin d'éviter la fourniture de clés uniques pour chaque ACS d'un réseau. Reportez-vous au Guide de configuration ACS pour plus de détails.
8. Cliquez sur **Soumettre+Redémarrer**.

The screenshot displays the Cisco System Configuration web interface. On the left is a navigation sidebar with various configuration categories. The main content area is titled "EAP-FAST Configuration" and contains a form for "EAP-FAST Settings".

System Configuration

EAP-FAST Configuration

EAP-FAST Settings

EAP-FAST

- Allow EAP-FAST
- Active master key TTL: 1 months
- Retired master key TTL: 3 months
- Tunnel PAC TTL: 1 weeks
- Client initial message: TME
- Authority ID Info: TME
- Allow anonymous in-band PAC provisioning
- Allow authenticated in-band PAC provisioning
 - Accept client on authenticated provisioning
 - Require client certificate for provisioning
- Allow Machine Authentication
 - Machine PAC TTL: 1 weeks
- Allow Stateless session resume
 - Authorization PAC TTL: 1 hours
- Allowed inner methods
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS
- Select one or more of the following EAP-TLS comparison methods:
 - Certificate SAN comparison
 - Certificate CN comparison
 - Certificate Binary comparison
- EAP-TLS session timeout (minutes): 120
- EAP-FAST master server
- Actual EAP-FAST server status: **Master**

[Contrôleur WLAN Cisco](#)

Pour les besoins de ce guide de déploiement, un contrôleur LAN sans fil intégré (WLC) Cisco WS3750G est utilisé avec les points d'accès légers (LAP) Cisco AP1240 pour fournir l'infrastructure WLAN pour les tests CSSC. La configuration est applicable à tout contrôleur WLAN Cisco. La version logicielle utilisée est 4.0.155.5.

Configuration du contrôleur de réseau local sans fil

Fonctionnement de base et enregistrement du LAP 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). Vous pouvez également utiliser l'interface utilisateur graphique afin de configurer le WLC. Ce document explique comment configurer le WLC avec l'assistant de configuration de démarrage sur le CLI.

Une fois que le WLC a démarré pour la première fois, il entre dans l'assistant de configuration de démarrage. Utilisez l'assistant de configuration pour configurer les paramètres de base. Vous pouvez accéder à l'assistant via l'interface de ligne de commande ou l'interface utilisateur graphique. 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. Dans cet exemple de configuration, le WLC utilise **10.10.80.3** comme adresse IP de l'interface de gestion et **10.10.80.4** comme adresse IP de l'interface du gestionnaire AP.

Avant de pouvoir configurer d'autres fonctionnalités sur les WLC, les LAP doivent s'enregistrer auprès du WLC. Ce document suppose que le LAP est inscrit au WLC. Référez-vous à la section [Register the Lightweight AP to the WLCs](#) de [WLAN Controller Failover for Lightweight Access Points Configuration Exemple](#) pour obtenir des informations sur la façon dont les AP légers s'enregistrent auprès du WLC. Pour référence dans cet exemple de configuration, les AP1240 sont déployés sur un sous-réseau distinct (10.10.81.0/24) à partir du contrôleur WLAN (10.10.80.0/24), et l'option DHCP 43 est utilisée pour fournir une détection de contrôleur.

[Authentication RADIUS via Cisco Secure ACS](#)

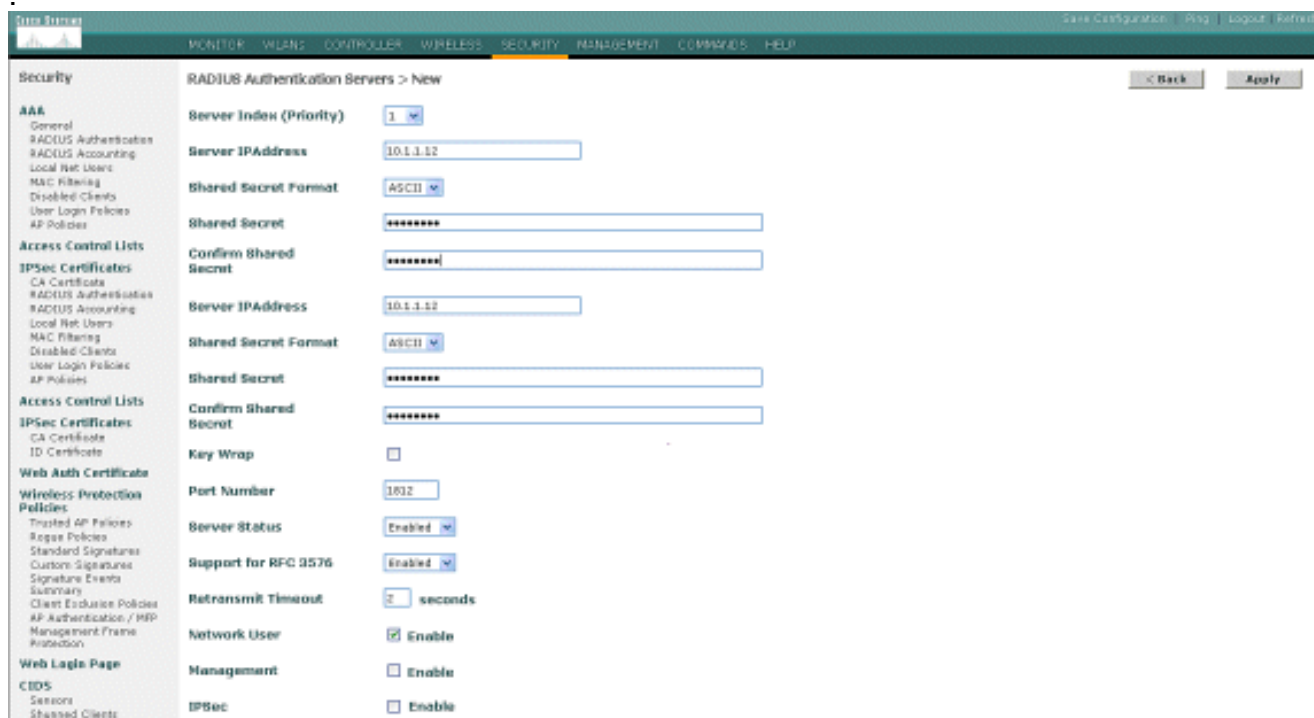
Le WLC doit être configuré pour transférer les informations d'identification de l'utilisateur au serveur Cisco Secure ACS. Le serveur ACS valide ensuite les informations d'identification de l'utilisateur (via la base de données Windows configurée) et fournit l'accès aux clients sans fil.

Complétez ces étapes pour configurer le WLC pour la communication au serveur ACS :

1. Cliquez sur **Security and RADIUS Authentication** à partir de l'interface graphique du contrôleur pour afficher la page RADIUS Authentication Servers. Cliquez ensuite sur **Nouveau** pour définir le serveur ACS.



2. Définissez les paramètres du serveur ACS dans la page RADIUS Authentication Servers > New. Ces paramètres incluent l'adresse IP ACS, le secret partagé, le numéro de port et l'état du serveur. **Remarque** : Les numéros de port 1645 ou 1812 sont compatibles avec ACS pour l'authentification RADIUS. Les cases à cocher Network User and Management (Utilisateur réseau et gestion) déterminent si l'authentification RADIUS s'applique aux utilisateurs du réseau (par exemple, les clients WLAN) et à la gestion (c'est-à-dire les utilisateurs administratifs). L'exemple de configuration utilise Cisco Secure ACS comme serveur RADIUS avec l'adresse IP 10.1.1.12



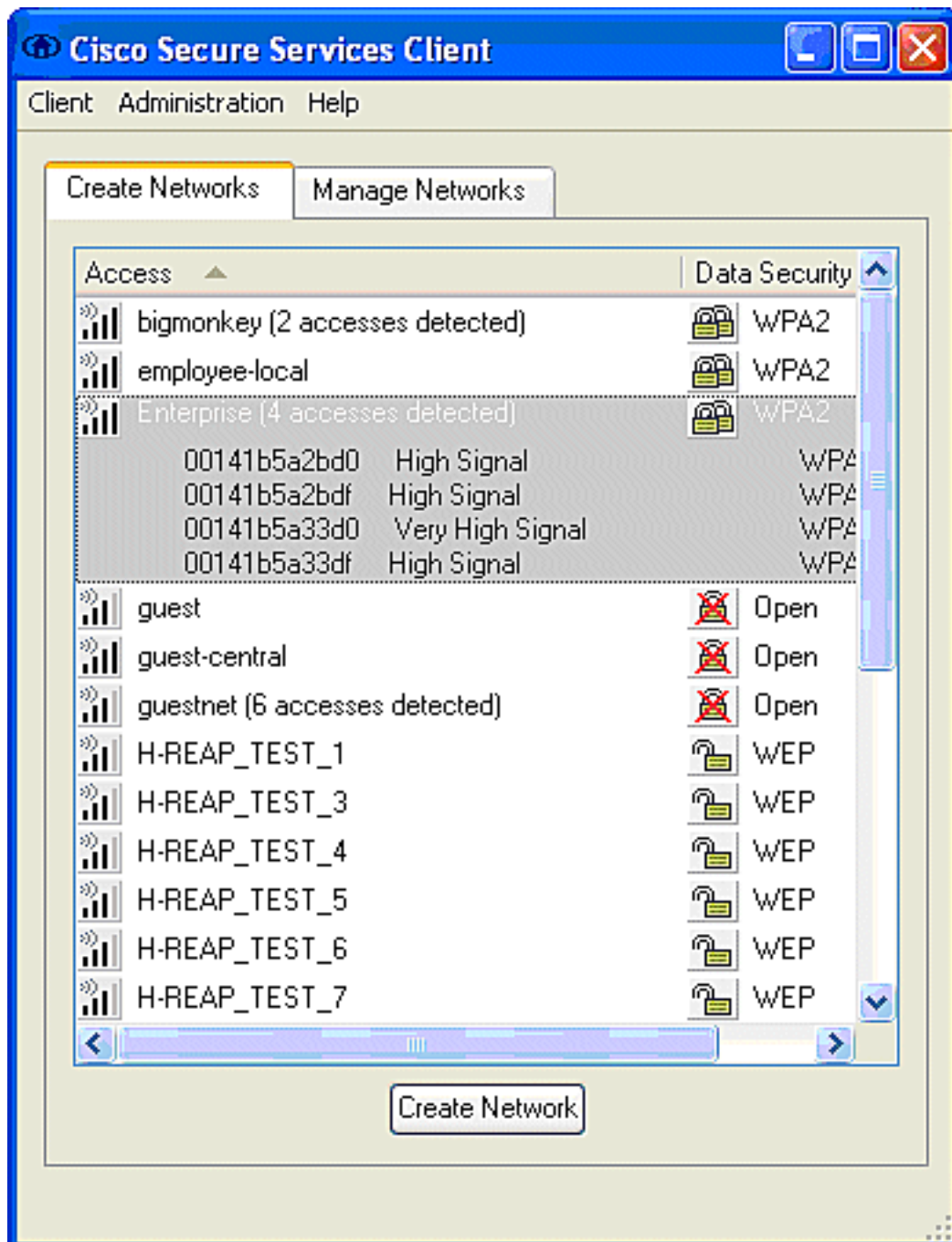
[Configuration des paramètres WLAN](#)

Cette section décrit la configuration du client Cisco Secure Services. Dans cet exemple, CSSC v4.0.5.4783 est utilisé avec un adaptateur client Cisco CB21AG. Avant d'installer le logiciel CSSC, vérifiez que seuls les pilotes du CB21AG sont installés, et non l'utilitaire de bureau Aironet (ADU).

Une fois le logiciel installé et exécuté en tant que service, il analyse les réseaux disponibles et les affiche.

Remarque : CSSC désactive la configuration automatique de Windows.

Remarque : Seuls les SSID activés pour la diffusion sont visibles.



Remarque : Par défaut, le contrôleur WLAN diffuse le SSID, de sorte qu'il figure dans la liste Create Networks des SSID analysés. Afin de créer un profil réseau, vous pouvez simplement cliquer sur le **SSID** dans la liste (Entreprise) et sur la case d'option **Créer un réseau**.

Si l'infrastructure WLAN est configurée avec le SSID de diffusion désactivé, vous devez ajouter manuellement le SSID ; cliquez sur la case d'option **Add** sous Access Devices et entrez

manuellement le **SSID** approprié (par exemple Enterprise). Configurez le comportement de la sonde active pour le client, c'est-à-dire, où le client recherche activement son SSID configuré ; spécifiez la **recherche active de ce périphérique d'accès** après avoir entré le SSID dans la fenêtre Ajouter un périphérique d'accès.

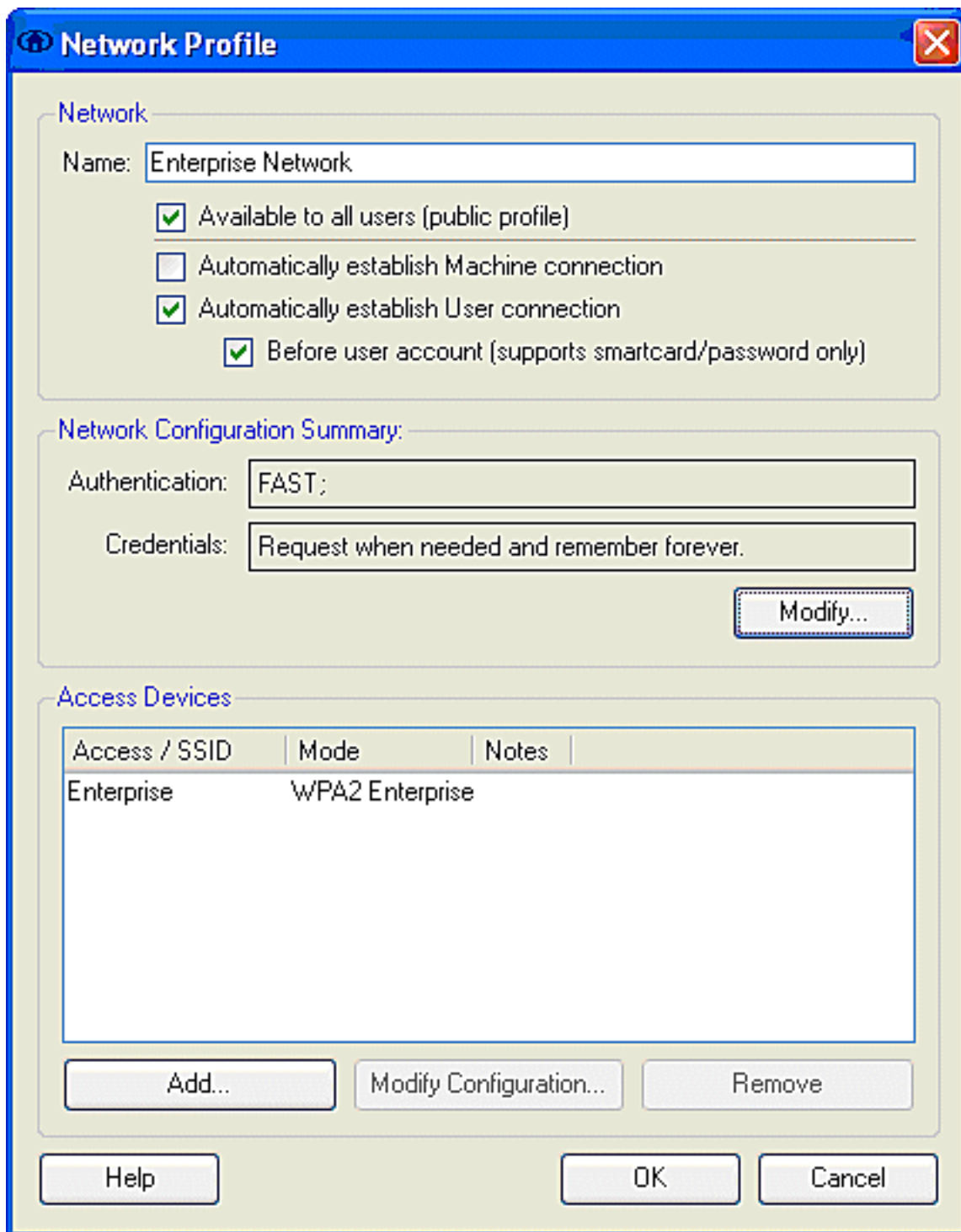
Remarque : Les paramètres de port ne permettent pas les modes d'entreprise (802.1X) si les paramètres d'authentification EAP ne sont pas configurés pour le profil.

La case d'option **Créer un réseau** lance la fenêtre Profil réseau, qui vous permet d'associer le SSID choisi (ou configuré) à un mécanisme d'authentification. Attribuez un nom descriptif au profil.

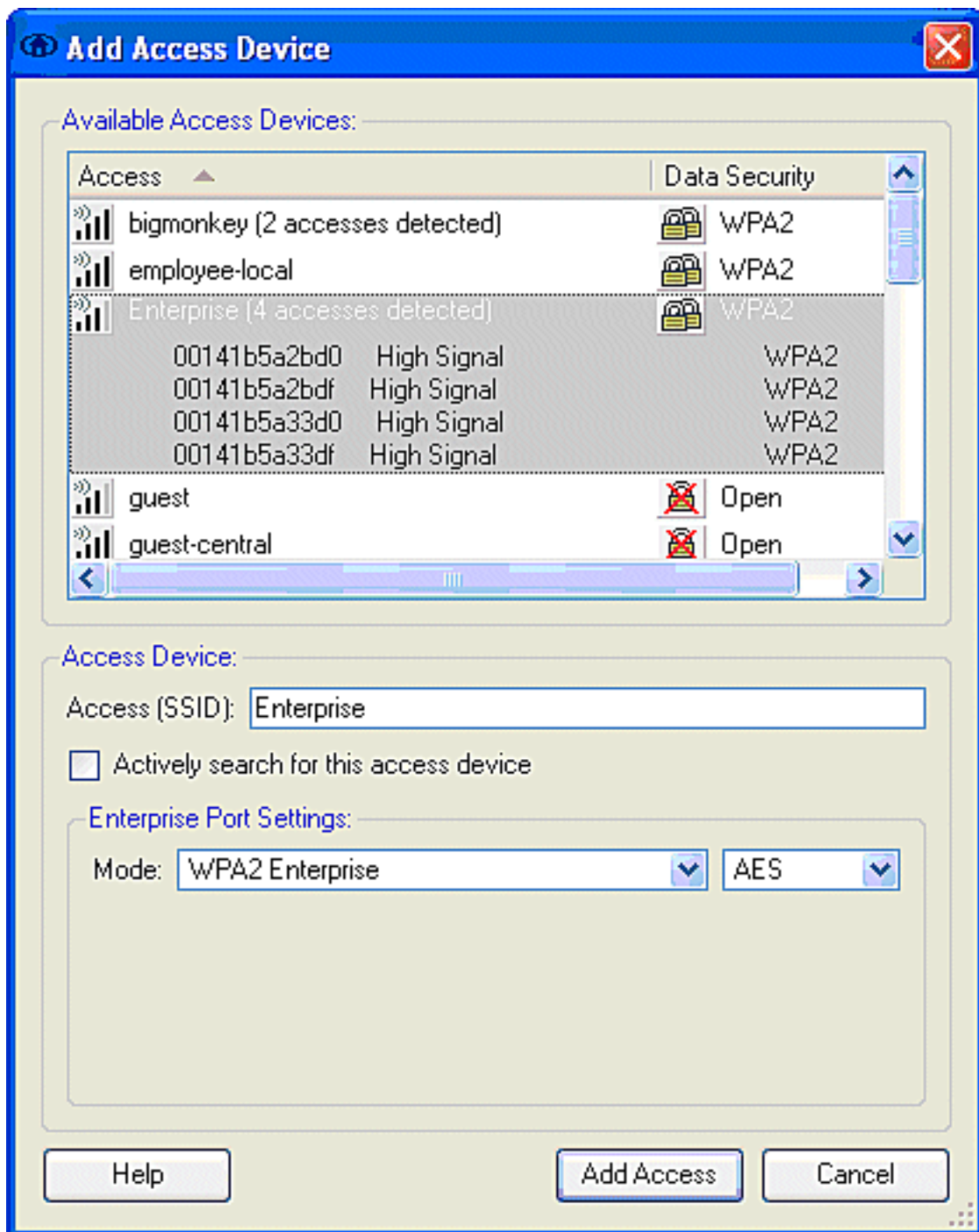
Remarque : Plusieurs types de sécurité WLAN et/ou SSID peuvent être associés sous ce profil d'authentification.

Pour que le client se connecte automatiquement au réseau dans la plage de couverture RF, sélectionnez **Établir automatiquement la connexion utilisateur**. Décochez **Disponible pour tous les utilisateurs** s'il n'est pas souhaitable d'utiliser ce profil avec d'autres comptes d'utilisateurs sur l'ordinateur. Si l'option **Établir automatiquement** n'est pas sélectionnée, l'utilisateur doit ouvrir la fenêtre CSSC et lancer manuellement la connexion WLAN à l'aide du bouton radio **Connect**.

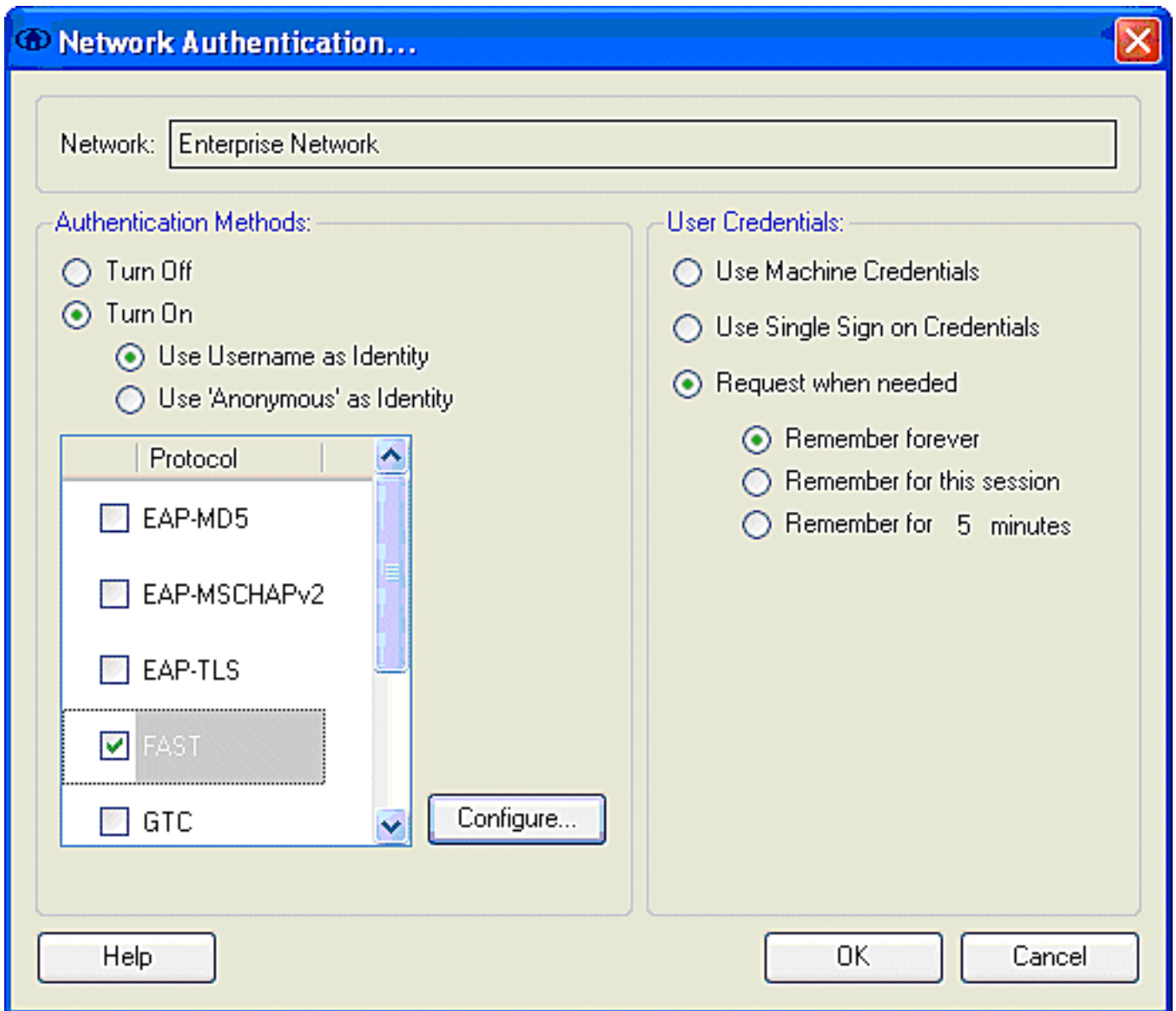
Si vous souhaitez établir la connexion WLAN avant de vous connecter, sélectionnez **Avant le compte d'utilisateur**. Cela permet une connexion unique avec des informations d'identification utilisateur enregistrées (mot de passe ou certificat/carte à puce lorsque vous utilisez TLS dans EAP-FAST).



Remarque : pour le fonctionnement de WPA/TKIP avec l'adaptateur client de la gamme Cisco Aironet 350, il est nécessaire de désactiver la validation de la connexion WPA, car il existe actuellement une incompatibilité entre le client CSSC et 350 pilotes en ce qui concerne la validation du hachage de la connexion WPA. Ceci est désactivé sous **Client > Advanced Settings > WPA/WPA2 Handshake Validation**. La validation de la connexion désactivée autorise toujours les fonctions de sécurité inhérentes à WPA (TKIP par paquet et vérification de l'intégrité des messages), mais désactive l'authentification de clé WPA initiale.



Sous Network Configuration Summary, cliquez sur **Modify** pour configurer les paramètres EAP / des informations d'identification. Spécifiez **Activer** l'authentification, Choisissez **EXPRES** sous Protocole, et choisissez '**Anonyme comme Identité** (afin d'utiliser aucun nom d'utilisateur dans la demande EAP initiale). Il est possible d'utiliser **Use Username as Identity** as comme identité EAP externe, mais de nombreux clients ne souhaitent pas exposer les ID utilisateur dans la demande EAP non chiffrée initiale. Spécifiez **Utiliser les informations d'identification de connexion unique** pour utiliser les informations d'identification de connexion pour l'authentification réseau. Cliquez sur **Configurer** pour configurer les paramètres EAP-FAST.



Dans les paramètres FAST, il est possible de spécifier **Valider le certificat de serveur**, qui permet au client de valider le certificat de serveur EAP-FAST (ACS) avant l'établissement d'une session EAP-FAST. Cela protège les périphériques clients de la connexion à un serveur EAP-FAST inconnu ou non autorisé et de la soumission par inadvertance de leurs informations d'identification à une source non fiable. Pour cela, un certificat doit être installé sur le serveur ACS et le certificat d'autorité de certification racine correspondant doit également être installé sur le client. Dans cet exemple, la validation du certificat de serveur n'est pas activée.

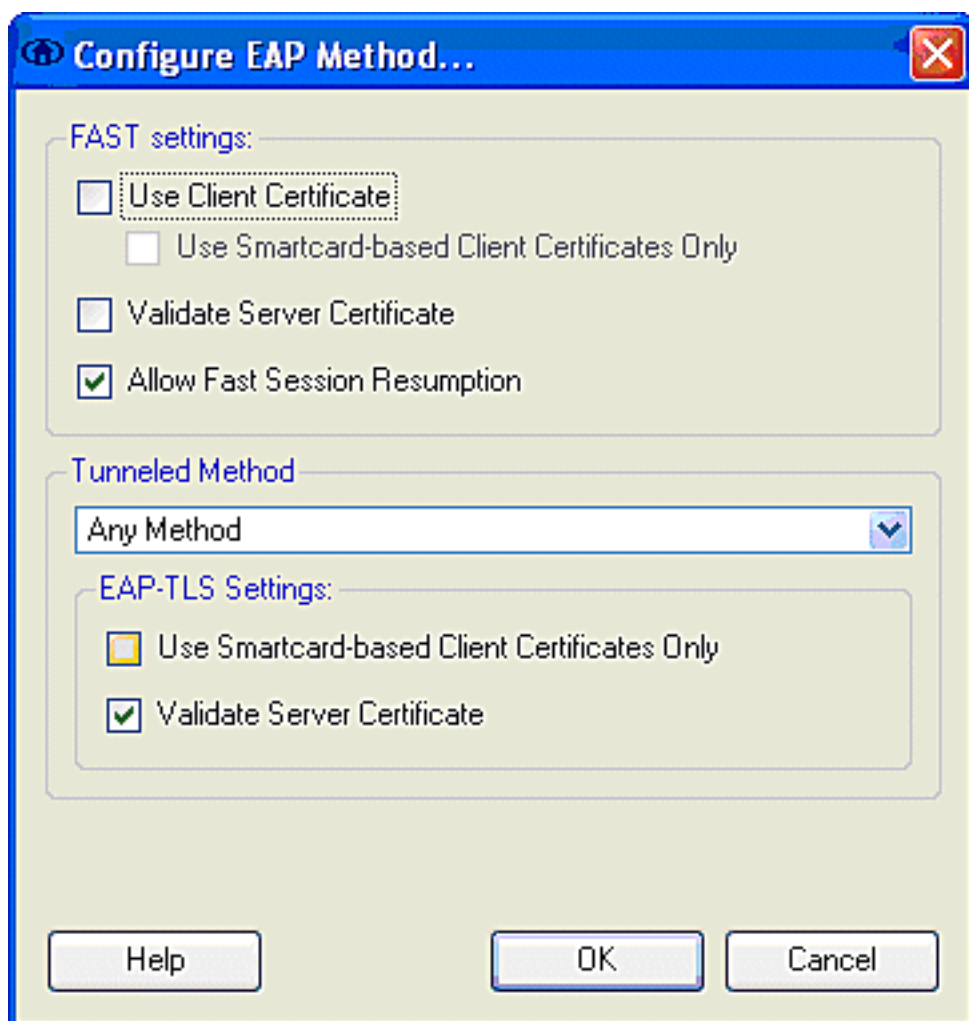
Dans les paramètres FAST, il est possible de spécifier **Allow Fast Session Resumption**, qui permet la reprise d'une session EAP-FAST basée sur les informations du tunnel (session TLS) plutôt que sur la nécessité d'une réauthentification EAP-FAST complète. Si le serveur et le client EAP-FAST ont une connaissance commune des informations de session TLS négociées dans l'échange d'authentification EAP-FAST initial, la reprise de session peut se produire.

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

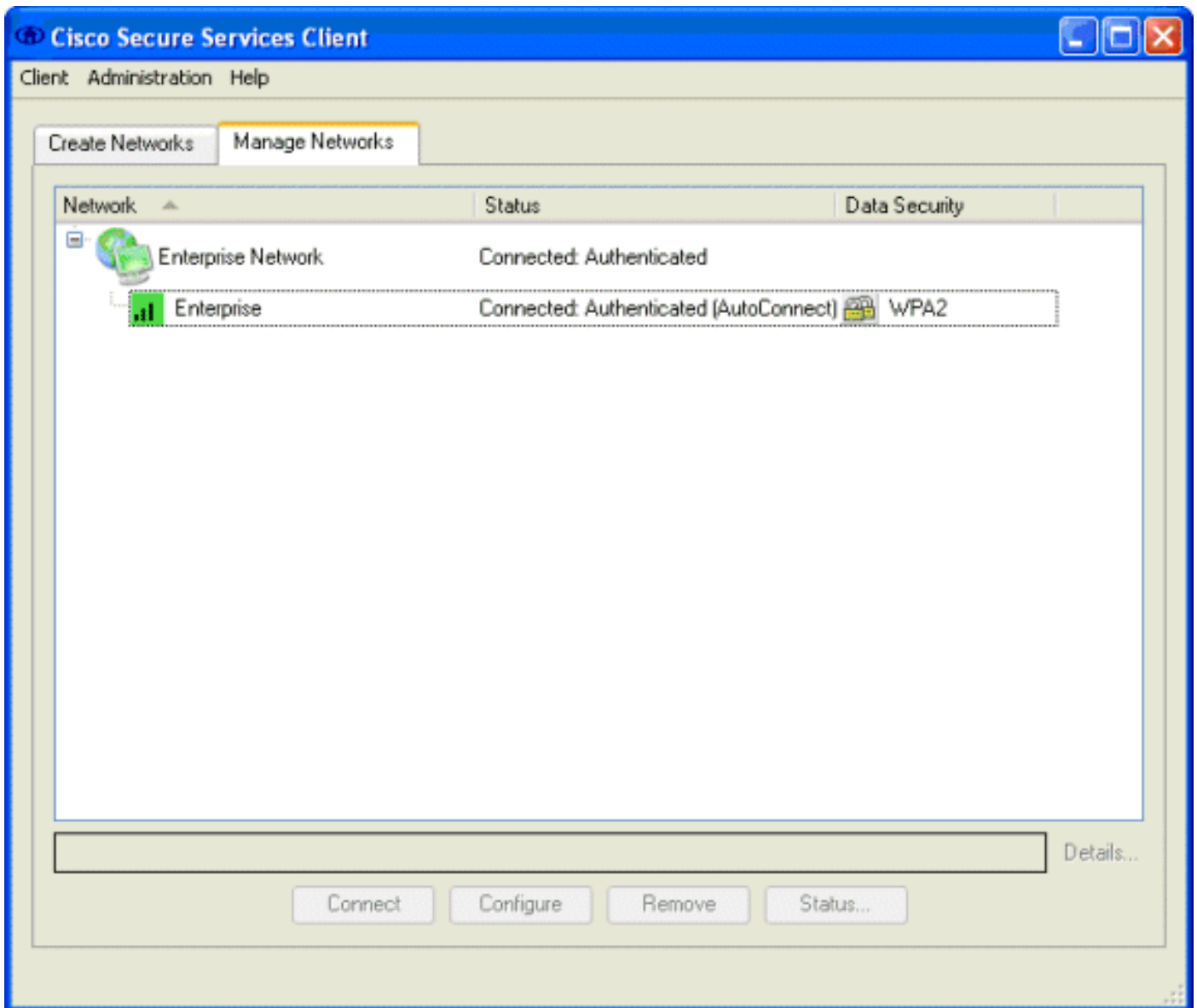
Sous Tunneled Method > EAP-TLS Settings, spécifiez **Any Method** pour autoriser l'EAP-MSCHAPv2 pour la fourniture automatique PAC et EAP-GTC pour l'authentification. Si vous utilisez une base de données au format Microsoft, telle qu'Active Directory, et si ne prend pas en charge aucun client EAP-FAST v1 sur le réseau, vous pouvez également spécifier l'utilisation de

MSCHAPv2 uniquement comme méthode tunnelée.

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



Cliquez sur **OK** pour enregistrer les paramètres EAP-FAST. Puisque le client est configuré pour « établir automatiquement » sous le profil, il initie automatiquement l'association/authentification avec le réseau. Dans l'onglet Gérer les réseaux, les champs Réseau, État et Sécurité des données indiquent l'état de connexion du client. À partir de cet exemple, on voit que le réseau Profile Enterprise est utilisé et que le périphérique d'accès réseau est le SSID Enterprise, qui indique Connected : Authenticated et utilise Autoconnect. Le champ Sécurité des données indique le type de chiffrement 802.11 utilisé, qui, par exemple, est WPA2.



Une fois le client authentifié, sélectionnez **SSID** sous Profil dans l'onglet Gérer les réseaux et cliquez sur **État** pour interroger les détails de connexion. La fenêtre Détails de la connexion fournit des informations sur le périphérique client, l'état et les statistiques de la connexion, ainsi que la méthode d'authentification. L'onglet WiFi Details (Détails WiFi) fournit des détails sur l'état de la connexion 802.11, qui inclut le RSSI, le canal 802.11 et l'authentification/chiffrement.

Connection Status



Connection Details

WiFi Details

Status: Connected: Authenticated

Duration: 00:00:47

Network Profile: Enterprise Network

Network Adapter: Cisco Aironet 802.11 a/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

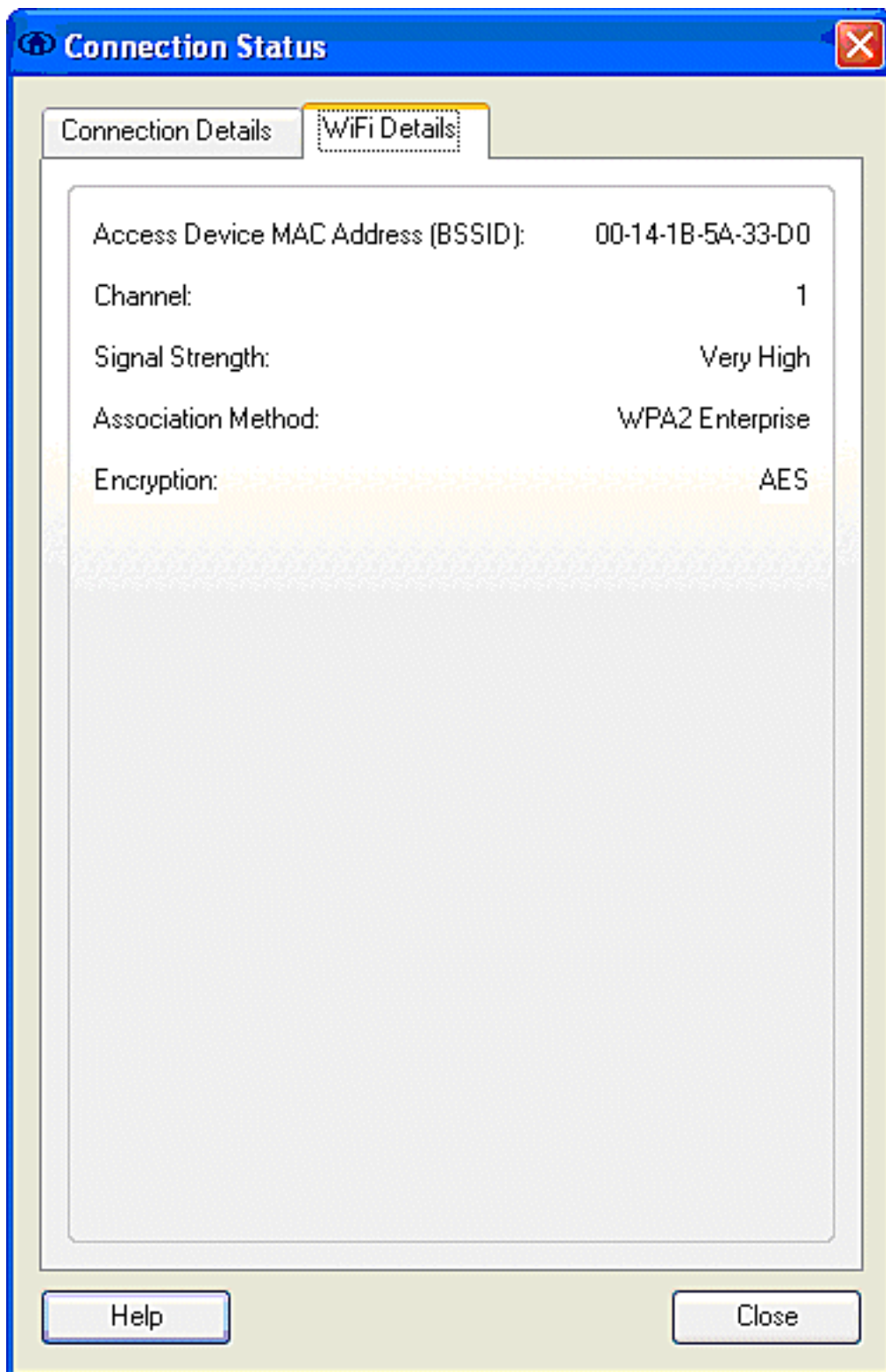
Authentication Method: FAST / GTC

Authentication Server: TME (not verified)

IP Address: 10.10.82.11

Help

Close



En tant qu'administrateur système, vous avez droit à l'utilitaire de diagnostic Cisco Secure Services Client System Report, qui est disponible avec la distribution CSSC standard. Cet utilitaire est disponible à partir du menu Démarrer ou du répertoire CSSC. Pour obtenir des données, cliquez sur **Collecter des données > Copier dans le Presse-papiers > Rechercher le fichier de rapport**. Cette opération dirige une fenêtre de l'Explorateur de fichiers Microsoft vers le répertoire contenant le fichier de rapport compressé. Dans le fichier compressé, les données les plus utiles se trouvent sous log (log_current).

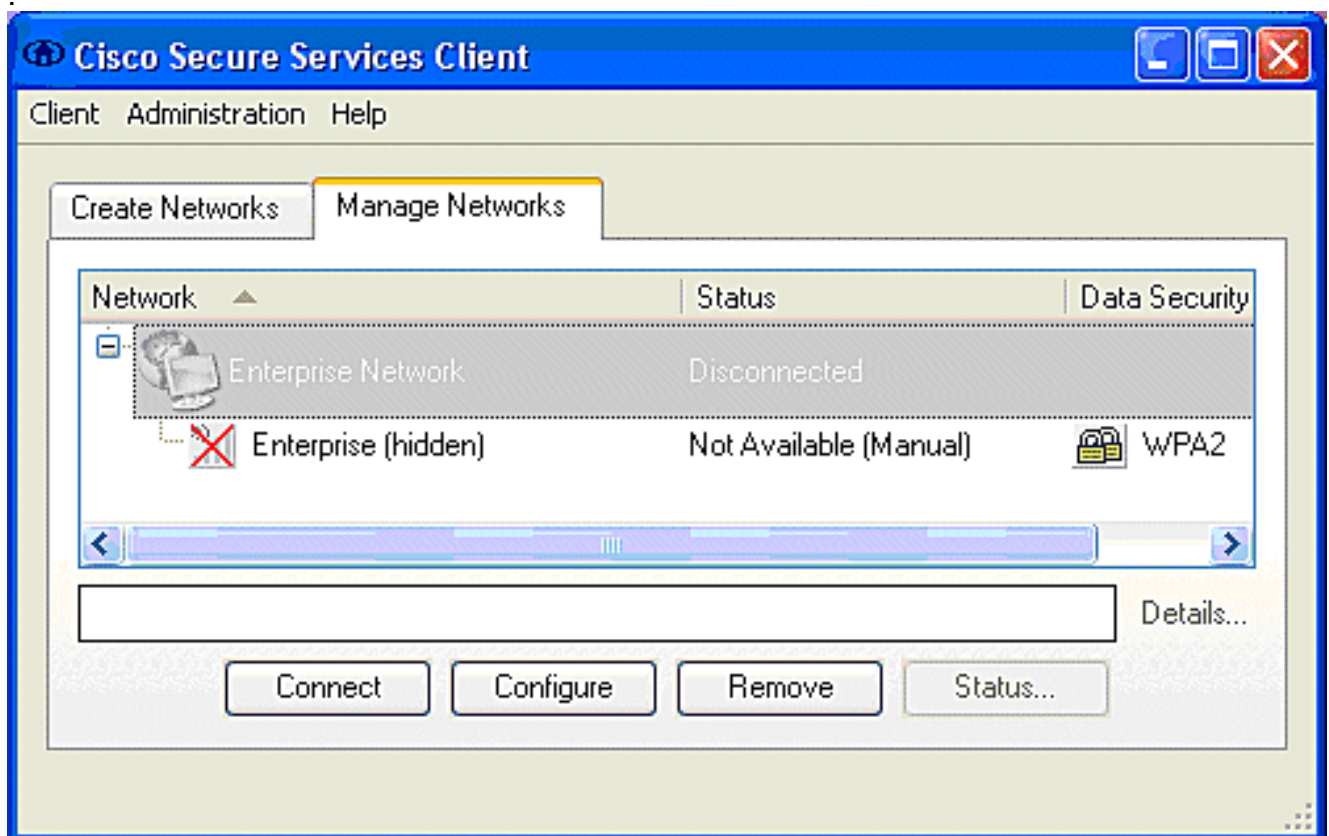
L'utilitaire fournit l'état actuel des informations CSSC, de l'interface et du pilote, ainsi que les informations WLAN (SSID détecté, état de l'association, etc.). Cela peut être utile, en particulier pour diagnostiquer les problèmes de connectivité entre CSSC et la carte WLAN.

Vérifier le fonctionnement

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


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

1. Si CSSC est configuré pour la connexion automatique, le client tente cette connexion automatiquement. S'il n'est pas configuré pour les opérations de connexion automatique et d'authentification unique, l'utilisateur doit lancer la connexion WLAN via la case d'option **Connect**. Ceci initie le processus d'association 802.11 sur lequel se produit l'authentification EAP. Voici un exemple



2. L'utilisateur est ensuite invité à fournir le nom d'utilisateur, puis le mot de passe pour l'authentification EAP-FAST (de l'Autorité PAC EAP-FAST ou ACS). Voici un exemple


Enter Your Credentials



Please enter your credentials for network Enterprise, access akita_pkc

Username:

Enter Your Credentials



Please enter your credentials for network Enterprise, access akita_pkc

Username:

Welcome to the Richfield TME PAC Auth

Dialog expires in 10 second(s)...

3. Le client CSSC, via le WLC, transmet ensuite les informations d'identification de l'utilisateur au serveur RADIUS (Cisco Secure ACS) afin de valider les informations d'identification. ACS vérifie les informations d'identification de l'utilisateur avec une comparaison des données et de la base de données configurée (dans l'exemple de configuration, la base de données externe est Windows Active Directory) et fournit un accès au client sans fil lorsque les informations d'identification de l'utilisateur sont valides. Le rapport Passed Authentications sur le serveur ACS indique que le client a réussi l'authentification RADIUS/EAP. Voici un exemple

:

The screenshot shows the Cisco ACS Reports and Activity interface. The left sidebar contains various report categories like TACACS+ Accounting, RADIUS Accounting, and Failed Authentications. The main area displays a table of authentication events for the file 'Passed Authentications active.csv'.

Date	Time	Message- Type	User- Name	Group- Name	CoRr- ID	NAS- Port	NAS- IP- Address	Network Access Profile Name	Shared BAC	Downloadable ACL	System- Posture- Token	Application- Posture- Token	Reason	EA Typ
08/22/2006	16:25:37	Authn OK	test	Default Group	00-40-96-a0-36-2f	29	10.10.80.3	(Default)	43
08/22/2006	16:09:51	Authn OK	test	Default Group	00-40-96-a5-d5-f6	29	10.10.80.3	(Default)	43
08/22/2006	16:06:55	Authn OK	test	Default Group	00-40-96-a5-d5-f6	29	10.10.80.3	(Default)	43
08/22/2006	16:06:29	Authn OK	test	Default Group	00-40-96-a5-d5-f6	29	10.10.80.3	(Default)	43
08/22/2006	16:06:29	Authn OK	test	Default Group	00-40-96-a6-d5-f6	29	10.10.80.3	(Default)	43

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

The screenshot shows the Cisco WLAN Controller GUI. The 'Clients' tab is active, displaying a table of connected clients. The table includes columns for Client MAC Addr, AP Name, WLAN, Type, Status, and Auth Port.

Client MAC Addr	AP Name	WLAN	Type	Status	Auth Port
88:0f:05:45:04:30	AP0504/948.9504	Unknown	882.11b	Probing	No 29
88:00:76:a0:36:2f	AP0504/948.9504	Enterprise	882.11g	Associated	Yes 29
88:00:76:ab:d1:89	AP0504/948.9480	Unknown	882.11b	Probing	No 29
88:00:76:ab:06:1b	AP0504/948.9480	Enterprise	882.11g	Associated	Yes 29

Annexe

Outre les informations de diagnostic et d'état disponibles sur Cisco Secure ACS et Cisco WLAN Controller, des points supplémentaires peuvent être utilisés pour diagnostiquer l'authentification EAP-FAST. Bien que la plupart des problèmes d'authentification puissent être diagnostiqués sans l'utilisation d'un analyseur WLAN ou d'échanges EAP de débogage au niveau du contrôleur WLAN, ce document de référence est inclus pour aider au dépannage.

[Capture de renifleur pour EAP-FAST Exchange](#)

Cette capture de renifleur 802.11 montre 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 Req	FC=...R...,SN=2867,FM= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Req	FC=...R...,SN=2867,FM= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F.,...,SN=2868,FM= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.,...,SN= 3,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.,...,SN= 4,FM= 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,FM= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.,...,SN= 5,FM= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T.,...,SN= 5,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.,...,SN= 6,FM= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T.,...,SN= 6,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.,...,SN= 7,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.,...,SN= 8,FM= 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,FM= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R.,...,SN=2877,FM= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R.,...,SN=2877,FM= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F.,...,SN=2878,FM= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAPOL-Key	FC=T.,...,SN= 9,FM= 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,FM= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R.,...,SN=2879,FM= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAPOL-Key	FC=T.,...,SN= 10,FM= 0

Ce paquet montre la réponse EAP-FAST initiale.

Remarque : tel que configuré sur le client CSSC, anonymous est utilisé comme identité EAP externe dans la réponse EAP initiale.

Packet: 12

Frame Control Flags: 00000001 [11]

- 0... .. Non-strict order
- .0... .. WEP Not Enabled
- ..0... .. No More Data
-0... .. Power Management - active mode
-0... .. This is not a Re-Transmission
-0... .. Last or Unfragmented Frame
-0... .. Not an Exit from the Distribution System
-1... .. To the Distribution System

Duration: 314 Microseconds [2-3]

BSSID: 00:14:1B:5A:33:D0 [4-9]

Source: 00:40:96:A0:36:2F Aironet:A0:36:2F [10-15]

Destination: 00:14:1B:5A:33:D0 [16-21]

Seq. Number: 3 [22-23 Hash 0x7770]

Frag. Number: 0 [22 Hash 0x07]

IEEE 802.2 Logical Link Control (LLC) Header

- Dest. SRP:** 0xAA SNAP [24]
- Source SRP:** 0xAA SNAP [25]
- Command:** 0x03 Unnumbered Information [26]
- Vendor ID:** 0x000000 [27-29]
- Protocol Type:** 0x888E 802.1x Authentication [30-31]

IEEE 802.1x Authentication

- Protocol Version:** 1 [32]
- Packet Type:** 0 EAP - Packet [33]
- Body Length:** 14 [34-35]

Extensible Authentication Protocol

- Code:** 2 Response [36]
- Identifier:** 1 [37]
- Length:** 14 [38-39]
- Type:** 1 Identity [40]
- Type-Data:** anonymous [41-49]

Débugger au niveau du contrôleur WLAN

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

- debug aaa events enable
- debug aaa detail enable

- debug dot1x events enable
- debug dot1x states enable

Voici un exemple du début d'une transaction d'authentification entre le client CSSC et ACS, tel qu'il est surveillé au niveau du contrôleur WLAN avec les débogages :

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
(count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006: Callback.....0x10372764
Thu Aug 24 18:20:54 2006: protocolType...0x00040001
Thu Aug 24 18:20:54 2006: proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006: Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006: structureSize..147
Thu Aug 24 18:20:54 2006: resultCode.....255
Thu Aug 24 18:20:54 2006: protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006: proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006: Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
(id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
updated EAP-Identifer 1 ==> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

Il s'agit de la réussite de l'échange EAP à partir du débogage du contrôleur (avec l'authentification WPA2) :

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-
Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
override for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
```

00:40:96:a0:36:2f source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout:
-1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, r1'
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
for station 00:40:96:a0:36:2f (RSN 2)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: New PMKID: (16)
Thu Aug 24 18:20:54 2006: [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
to mobile 00:40:96:a0:36:2f (EAP Id 0)
Thu Aug 24 18:20:54 2006: Including PMKID in M1 (16)
Thu Aug 24 18:20:54 2006:
[0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
while in Authenticating state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
moving mobile 00:40:96:a0:36:2f into Authenticated state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-
Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
(1) in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission
timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messal
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
EAPOL-Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1)
in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
Accounting Interim: 0x138dd764
Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs:
Thu Aug 24 18:20:54 2006:
AVP[01] User-Name.....enterprise (10 bytes)
Thu Aug 24 18:20:54 2006: AVP[02]
Nas-Port.....0x0000001d (29) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[03]
Nas-Ip-Address.....0x0a0a5003 (168448003) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[04]
Class.....CACs:0/28b5/a0a5003/29 (22 bytes)
Thu Aug 24 18:20:54 2006: AVP[05]
NAS-Identifier.....ws-3750 (7 bytes)
Thu Aug 24 18:20:54 2006: AVP[06]
Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[07]
Acct-Session-Id.....44ede3b0/00:40:
96:a0:36:2f/14 (29 bytes)
Thu Aug 24 18:20:54 2006: AVP[08]
Acct-Authentic.....0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[09]
Tunnel-Type.....0x0000000d (13) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[10]

```
Tunnel-Medium-Type.....0x00000006 (6) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[11]
Tunnel-Group-Id.....0x3832 (14386) (2 bytes)
Thu Aug 24 18:20:54 2006: AVP[12]
Acct-Status-Type.....0x00000003 (3) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[13]
Acct-Input-Octets.....0x000b99a6 (760230) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[14]
Acct-Output-Octets.....0x00043a27 (277031) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[15]
Acct-Input-Packets.....0x0000444b (17483) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[16]
Acct-Output-Packets.....0x0000099b (2459) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[17]
Acct-Session-Time.....0x00000a57 (2647) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[18]
Acct-Delay-Time.....0x00000000 (0) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[19]
Calling-Station-Id.....10.10.82.11 (11 bytes)
Thu Aug 24 18:20:54 2006: AVP[20]
Called-Station-Id.....10.10.80.3 (10 bytes)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated
```

[Informations connexes](#)

- [Guide d'installation de Cisco Secure ACS pour Windows Server](#)
- [Guide de configuration de 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](#)