# EAP-FAST 認証を使用する Cisco Secure Services Client

## 目次



## 概要

このドキュメントでは、EAP-FAST により、ワイヤレス LAN コントローラ、Microsoft Windows 2000(R) ソフトウェア、および Cisco Secure Access Control Server ( ACS ) 4.0 で Cisco Secure Services Client ( CSSC ) を設定する方法について説明します。 このドキュメントでは EAP-FAST のアーキテクチャを紹介し、展開と設定の例を示します。 CSSC はクライアント ソフトウェア コンポーネントで、ユーザをネットワークに対して認証し、適切なアクセス権を割り当てるために、ユーザのクレデンシャルのインフラストラクチャへのコミュニケーションを実現します。

このドキュメントで概要が示されている CSSC ソリューションには、次のような利点があります。

- Extensible Authentication Protocol（EAP）を使用した、WLAN/LAN へのアクセス権限に先行する各ユーザ（またはデバイス）の認証
- サーバ、Authenticator、およびクライアント コンポーネントを使用したエンドツーエンドの WLAN セキュリティ ソリューション
- 有線と無線の認証に共通のソリューション
- 認証プロセスで取得される動的なユーザごとの暗号化キー
- Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）または証明書が不要（証明書検証はオプション）
- アクセス ポリシー割り当て/NAC 対応の EAP フレームワーク

**注:** セキュアな無線の展開については、『Cisco SAFE ワイヤレス計画』を参照してください。

802.1x 認証フレームワークは、802.11 ワイヤレス LAN ネットワークにおけるレイヤ 2 ベースの認証、許可、およびアカウンティング（AAA）機能を有効にするために、802.11i（無線 LAN のセキュリティ）標準の一部として組み込まれています。 今日では、有線と無線両方のネットワークにおける展開で使用できる EAP プロトコルがいくつか存在します。 一般的に展開される EAP プロトコルには、LEAP、PEAP、および EAP-TLS があります。 これらのプロトコルに加えて、Cisco では、有線と無線両方の LAN ネットワークでの配備に使用できる標準規格ベースの EAP プロトコルとして、EAP Flexible Authentication through Secured Tunnel（EAP-FAST）プロトコルを定義および実装しています。 EAP-FAST プロトコルの仕様は、IETF の Web サイトで一般に公開されています。

その他の EAP プロトコルと同じように、EAP-FAST は、TLS トンネル内部での EAP トランザクションを暗号化するクライアント/サーバ型のセキュリティ アーキテクチャです。 この点では PEAP や EAP-TTLS に似ていますが、（サーバ X.509 証明書を使用して認証セッションを保護する）PEAP/EAP-TTLS と対比すると、EAP-FAST トンネル確立は各ユーザに固有の強力な共有秘密キーに基づくという点において、EAP-FAST は異なります。 これらの共有秘密キーは Protected Access Credential（PAC）と呼ばれ、クライアント デバイスに自動（Automatic または In-band Provisioning）または手動（Manual または Out-of-band Provisioning）で配布できます。 共有秘密に基づくハンドシェイクは PKI インフラストラクチャに基づくハンドシェイクよりも効率的なので、保護された認証交換を実現するプロトコルの中では、EAP-FAST が最速でプロセッサの負荷が少ない EAP タイプになります。 さらに EAP-FAST は、ワイヤレス LAN クライアント上または RADIUS インフラストラクチャ上で証明書を必要とせず、組み込み型のプロビジョニング メカニズムを備えているため、展開を簡単にする設計になっています。

次に、EAP-FAST プロトコルの主要な機能の一部を示します。

- Windows のユーザ名/パスワードを使用した Single Sign-On（SSO; シングル サインオン）
- ログイン スクリプト実行のサポート
- サードパーティ製サプリカントを必要としない Wi-Fi Protected Access（WPA）のサポート（Windows 2000 および XP のみ）
- PKI インフラストラクチャを必要としない簡単な展開
- Windows パスワード エージング（つまり、サーバベースのパスワード期限切れのサポート）
- 適切なクライアント ソフトウェアを使用した Network Admission Control 用の Cisco Trust Agent との統合

# 前提条件

## 要件

このドキュメントではテストを行うための特定の設定のみがカバーされているため、インストー

ルを実行するユーザには基本的な Windows 2003 のインストールと Cisco WLC のインストールの知識があることが前提となっています。

Cisco 4400 シリーズ コントローラ用の初期インストールおよび構成情報に関しては、クイックスタートガイドを参照して下さい: Cisco 4400 シリーズ ワイヤレス LAN コントローラ。 Cisco 2000 シリーズ コントローラ用の初期インストールおよび構成情報に関しては、クイックスタートガイドを参照して下さい: Cisco 2000 シリーズ ワイヤレス LAN コントローラ。

作業を始める前に、最新のサービス パック ソフトウェアが含まれる Microsoft Windows Server 2000 をインストールします。 コントローラと Lightweight Access Point（LAP; Lightweight アクセス ポイント）をインストールし、最新のソフトウェア更新プログラムが設定されていることを確認します。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 4.0.155.5 が稼働する Cisco 2006 または 4400 シリーズ コントローラ
- Cisco 1242 LWAPP AP
- Active Directory を搭載した Windows 2000
- Cisco Catalyst 3750G スイッチ
- CB21AG アダプタ カードと Cisco Secure Services Client バージョン 4.05 を伴う Windows XP

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 設計パラメータ

## データベース

WLAN ネットワークを展開して、認証プロトコルを決定する場合、通常はユーザ/マシンの認証用に現在のデータベースを使用するのが望まれます。 使用できる一般的なデータベースは、Windows Active Directory、LDAP、または One-Time Password（OTP; ワンタイム パスワード）データベース（つまり RSA や SecureID）です。 これらすべてのデータベースが EAP-FAST プロトコルと互換性がありますが、展開を計画する際には、考慮する必要がある互換性の要件がいくつか存在します。 クライアントへの PAC ファイルの最初の展開は、匿名自動プロビジョニング、（現行のクライアント X.509 証明書を介した）認証済みプロビジョニング、または手動プロビジョニングで実行されます。 このドキュメントの目的に合わせて、匿名自動プロビジョニングと手動プロビジョニングを検討します。

自動 PAC プロビジョニングでは、Authenticated Diffie-Hellman Key Agreement Protocol（ADHP）を使用してセキュアなトンネルが確立されます。 セキュアなトンネルは、匿名で、またはサーバ認証メカニズムを介して確立できます。 確立されたトンネル接続内では、クライアントの認証に MS-CHAPv2 が使用され、認証が成功するとクライアントに PAC ファイルが配布されます。 PAC が正しくプロビジョニングされた後、セキュアなネットワーク アクセスを実現するために、PAC ファイルを使用して新しい EAP-FAST 認証セッションを開始できます。

自動プロビジョニング メカニズムは MSCHAPv2 に依存していることから、ユーザの認証に使用されるデータベースは使用されるデータベースのパスワード形式と互換性がある必要があるため、自動 PAC プロビジョニングは、使用されるデータベースと関連することになります。 EAP-FAST と、MSCHAPv2 形式をサポートしないデータベース（OTP、Novell、LDAP など）を併用する場合、ユーザ PAC ファイルを展開するために別のメカニズム（つまり手動プロビジョニングや認証済みプロビジョニング）を採用する必要があります。 このドキュメントでは、Windows のユーザ データベースを使用した自動プロビジョニングの例を示します。

## Encryption

EAP-FAST 認証は、特定の WLAN 暗号化タイプの使用を必要としません。 使用されるべき WLAN 暗号化タイプはクライアント NIC カード機能によって判別されます。 特定の展開における NIC カードの機能に応じて、WPA2（AES-CCM）または WPA（TKIP）の暗号化を採用することをお勧めします。 Cisco WLAN ソリューションでは、共通の SSID 上に WPA2 クライアント デバイスと WPA クライアント デバイスの両方が共存できることに注意してください。

クライアント デバイスで WPA2 や WPA がサポートされていない場合、ダイナミックな WEP キーを使用した 802.1X 認証を展開できますが、WEP キーに対する有名な悪用があるため、この WLAN 暗号化メカニズムはお勧めできません。 WEP 専用クライアントサポートする必要がある場合、クライアントが短い間隔で新しい WEP キーを取得する必要があるセッションタイムアウト間隔を採用することをお勧めします。 一般的な WLAN データ レートに対しては 30 分が推奨されるセッション間隔です。

## シングル サインオンとマシンのクレデンシャル

シングル サインオンとは、認証のためのクレデンシャルの 1 回のユーザ サインオンまたは入力が、複数のアプリケーションまたは複数のデバイスにアクセスするために使用できることを指しています。 このドキュメントの目的に合わせると、シングル サインオンとは、WLAN に対する認証のために PC への口グオンに使用されるクレデンシャルを使用することを指します。

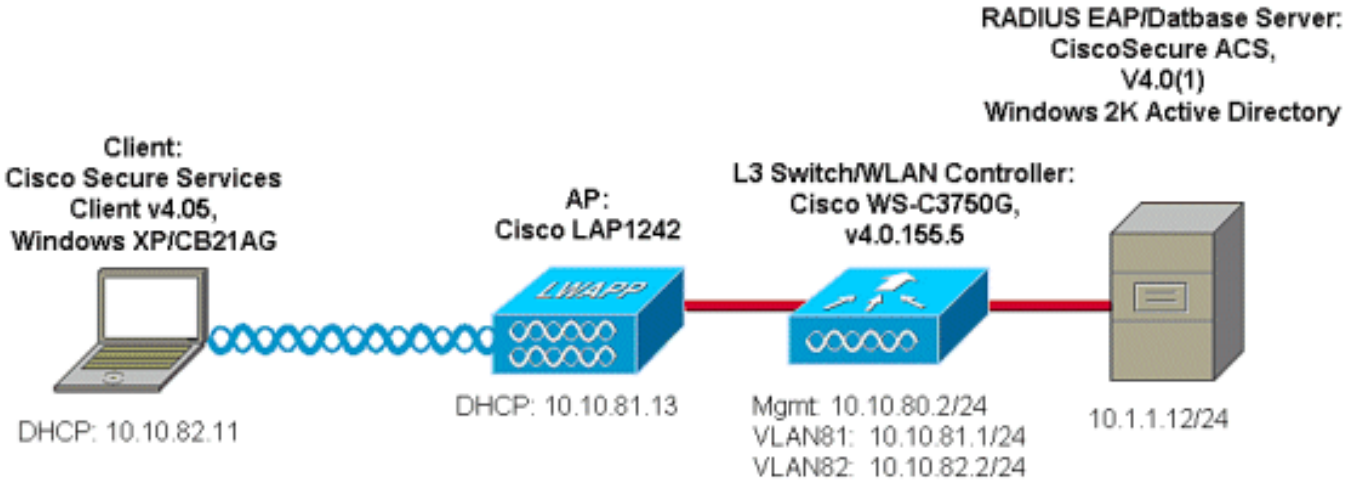
Cisco Secure Services Client を使用すると、あるユーザのログオン クレデンシャルを使用して、WLAN ネットワークに対して認証することも可能です。 PC へのユーザ ログオンの前に PC をネットワークに対して認証することが望ましい場合、保存されたユーザ クレデンシャルか、マシン プロファイルと結び付けられたクレデンシャルのいずれかを使用する必要があります。 ユーザのログオン時ではなく、PC の起動時にログオン スクリプトを実行するかドライブをマッピングすることが望ましいケースでは、これらの方式のどちらも有用です。

# ネットワーク図

このドキュメントでは、次のネットワーク ダイアグラムを使用します。 このネットワークでは、4 つのサブネットが使用されます。 以下に示すデバイスを異なるネットワークにセグメント化する必要はありませんが、このようにすると実際のネットワークとの統合に関して最高の柔軟性が利用可能になります。 Catalyst 3750G Integrated Wireless LAN Controller では、通常のシャーシ上で Power Over Ethernet（POE）スイッチポート、L3 スイッチング、および WLAN コントローラ機能が実現されます。

1. ネットワーク 10.1.1.0 は、ACS が存在するサーバ ネットワークです。
2. ネットワーク 10.10.80.0 は、WLAN コントローラにより使用される管理ネットワークです。
3. ネットワーク 10.10.81.0 は、AP が存在するネットワークです。

4. ネットワーク 10.10.82.0 は、WLAN クライアント用に使用されます。




## Access Control Server ( ACS ) の設定

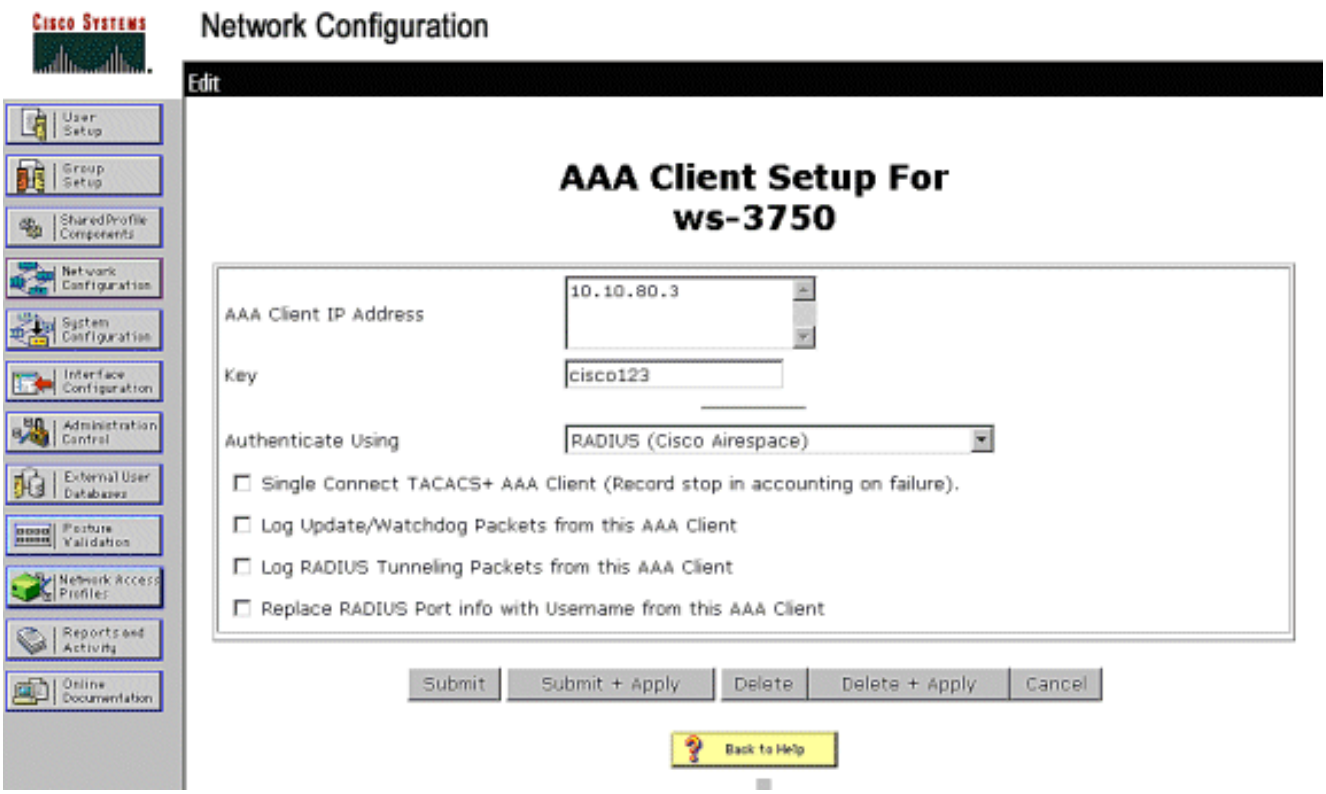
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

**注:** このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool ( 登録ユーザ専用 ) を使用してください。

### ACS でアクセス ポイントを AAA クライアント ( NAS ) として追加する

このセクションでは、外部データベースとして、Windows Active Directory によるインバンド PAC プロビジョニングを使用して EAP-FAST 用に ACS を設定する方法について説明します。

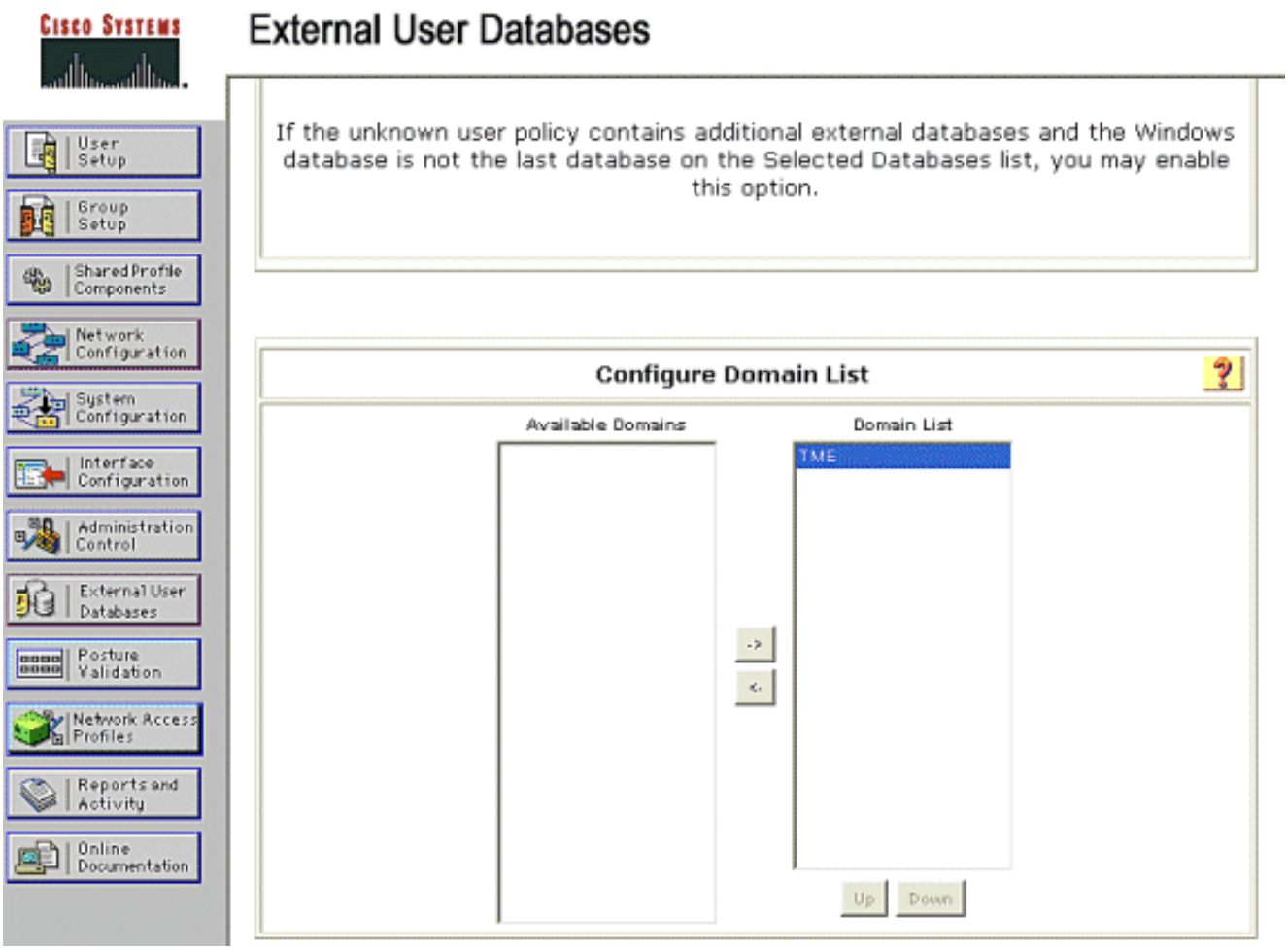
1. **ACS > ネットワークコンフィギュレーション**にログオンし、『Add Entry』 をクリック して下さい。
2. WLAN コントローラ名、IP アドレス、共有秘密キーを入力し、Authenticate Using の下で RADIUS (Cisco Airespace) を選択します ( これには RADIUS IETF 属性も含まれます )。**注**: Network Device Groups (NDG) が有効である場合、まず適切な NDG を選択してからそれに WLAN コントローラを追加します。 NDG の詳細については、『ACS 設定ガイド』を参照してください。
3. [Submit + Restart] をクリックします。



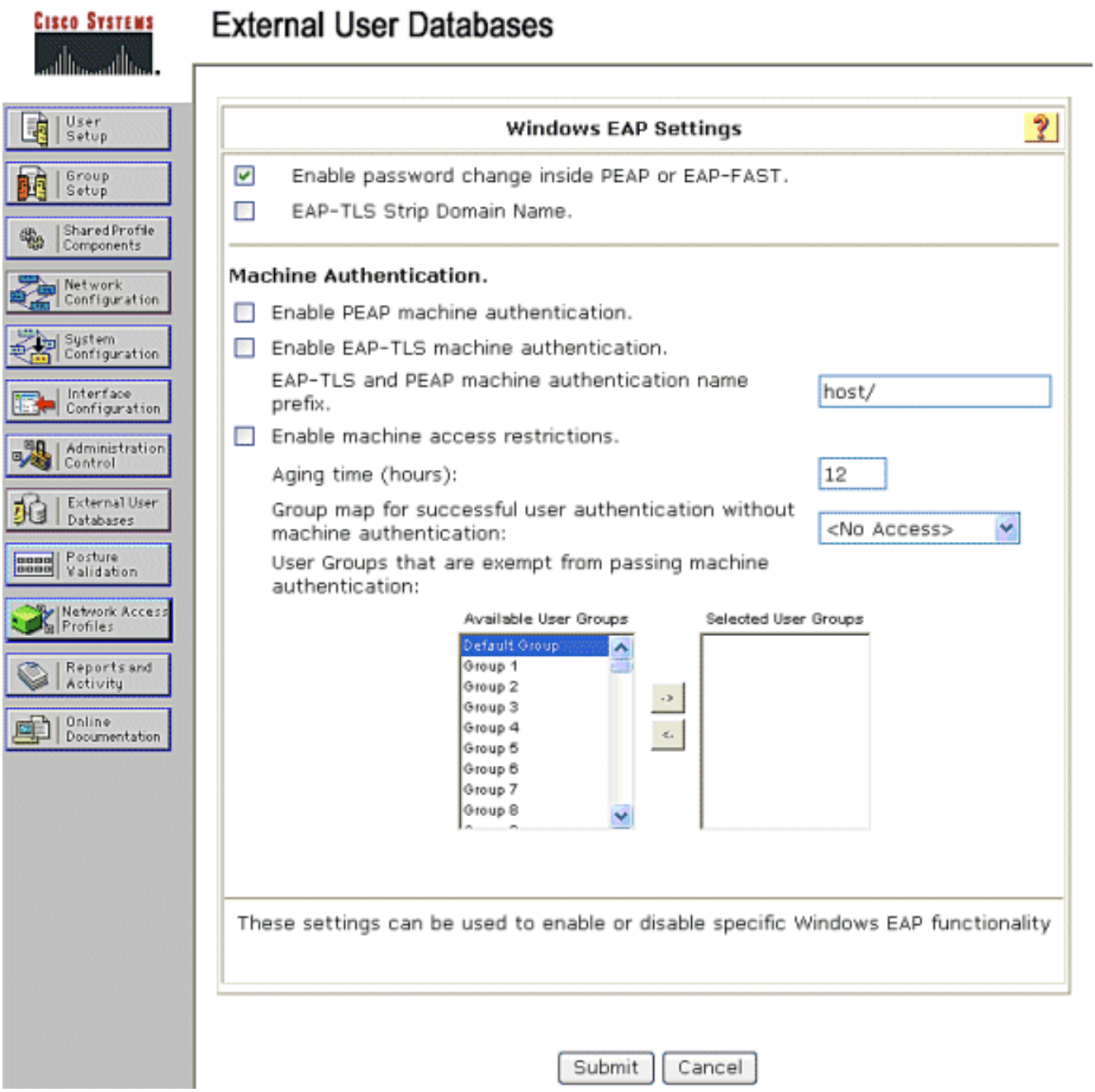

## 外部データベースに照会するため ACS を設定する

このセクションでは、外部データベースを照会するために ACS を設定する方法について説明します。

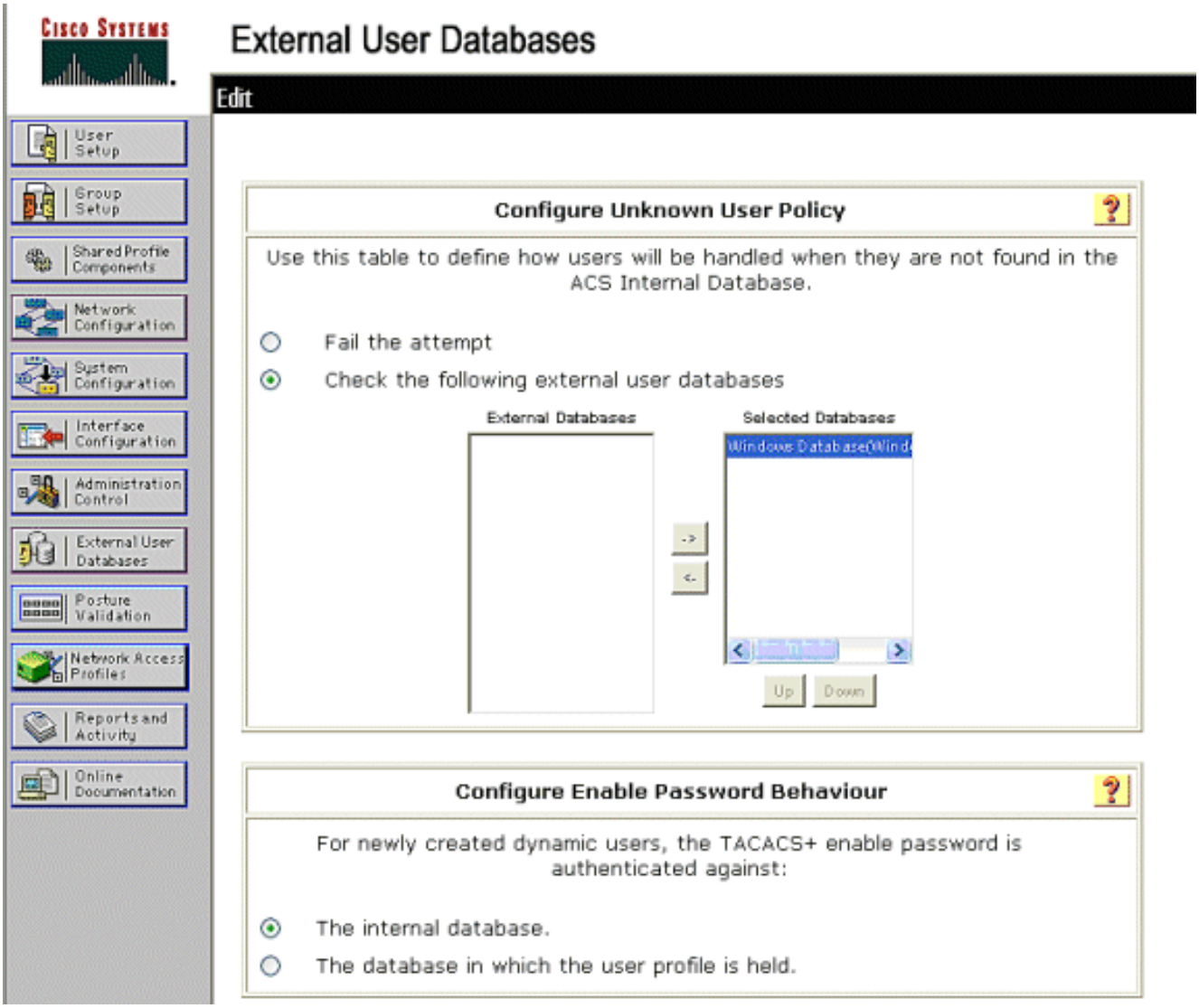
1. **ユーザデータベース > データベースコンフィギュレーション > ウィンドウ データベース > 設定** 『External』 をクリック して下さい。
2. Configure Domain List の下で、Domains を、Available Domains から Domain List へ移動させます。**注:** ACS アプリケーションが認証のためにこれらのドメインを検出および使用するために、ACS を実行するサーバではこれらのドメインが認識されている必要があります。




3. Windows EAP Settings の下で、PEAP または EAP-FAST セッション内部でのパスワード変更を許可するオプションを設定します。 EAP-FAST と Windows パスワードのエージングの詳細については、『Cisco Secure ACS 4.1 の設定ガイド』を参照してください。
4. [Submit] をクリックします。**注:** Windows の外部データベースがアクセス許可を制御することを許可するために、Windows User Database Configuration の下で EAP-FAST 用の Dialin Permission 機能を有効にすることもできます。 Windows database configuration ページのパスワード変更用の MS-CHAP Settings は、非 EAP MS-CHAP 認証にのみ適用可能です。 EAP-FAST と組み合わせたパスワード変更を有効にするには、Windows EAP Settings の下でパスワード変更を有効にする必要があります。




5. **ユーザデータベース > Unknown User Policy を**『External』 をクリック し、**チェックを次の外部ユーザデータベース** オプション ボタン選択して下さい。
6. Windows データベースを、External Databases から Selected Databases へ移動させます。
7. [Submit] をクリックします。**注:** これ以降、ACS は Windows のデータベースをチェックします。 ユーザが ACS ローカル データベース内に見つからない場合、ユーザは ACS のデフォルト グループ内に配置されます。 データベース グループ マッピングの詳細については、ACS のドキュメントを参照してください。**注:** ユーザのクレデンシャルを確認するために ACS が Microsoft Active Directory データベースに照会するため、Windows で追加のアクセス権設定を設定する必要があります。 詳細は、『Cisco Secure ACS for Windows Server のインストール ガイド』を参照してください。



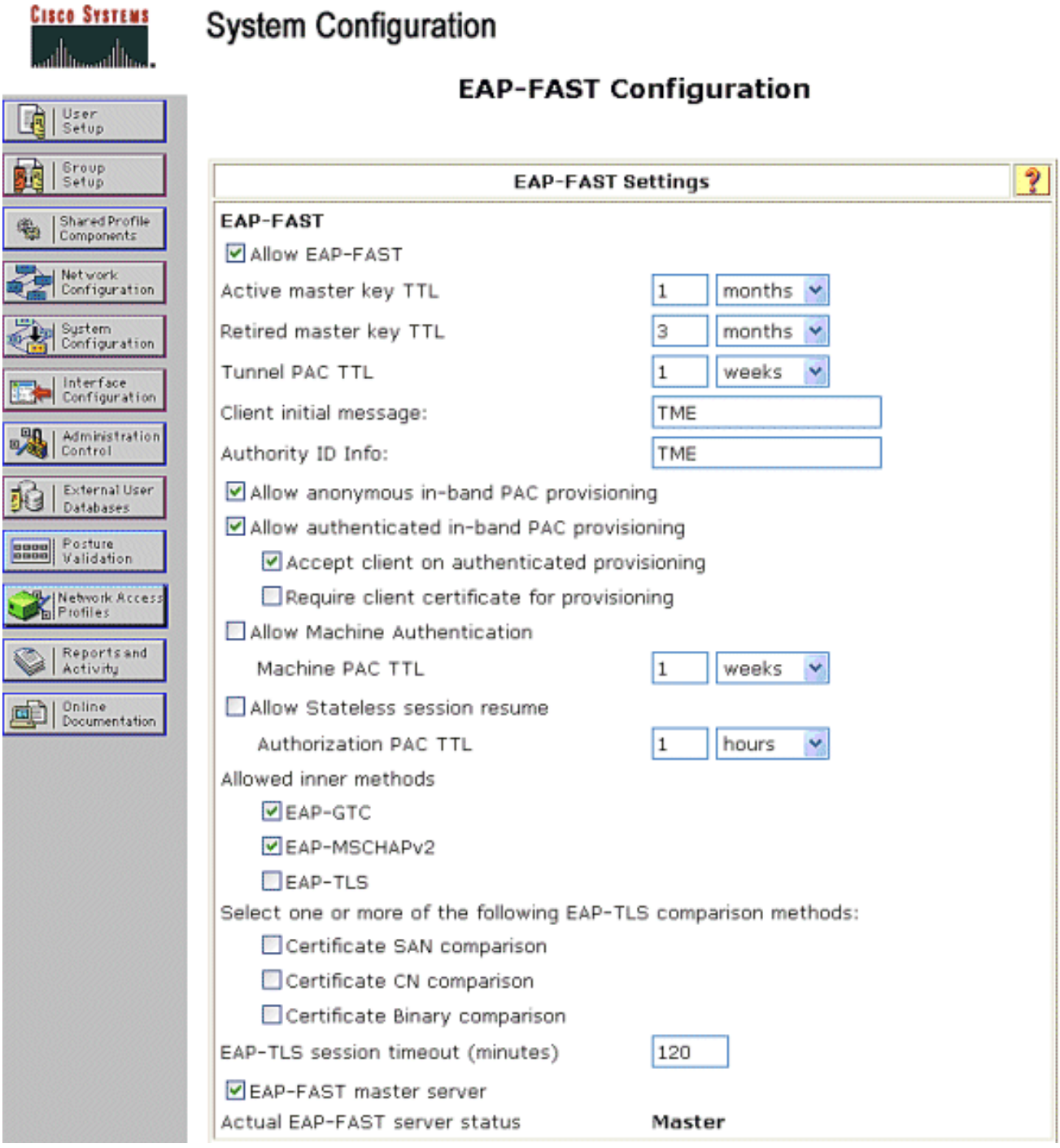

## ACS で EAP-FAST サポートを有効にする

このセクションでは、ACS で EAP-FAST サポートを有効にする方法について説明します。

1. **> EAP-FAST な 設定** System Configuration > Global Authentication Setup の順に進んで下さい。
2. Allow EAP-FAST を選択します。
3. これらの推奨事項を設定して下さい: マスタ鍵 TTL によって終了させまされる マスタ鍵 TTL PAC TTL。 これらの設定は、Cisco Secure ACS のデフォルトでは次のように設定されています。Master Key TTL：1 か月終了させまされたキー TTL: 3 か月PAC TTL: 1 週
4. Authority ID Info フィールドに入力します。 このテキストは、PAC Authority にコントローラが選択されている場合に、一部の EAP-FAST クライアント ソフトウェア上で表示されます。**注:** Cisco Secure Services Client では、PAC Authority 用のこの説明文は採用されていません。
5. Allow in-band PAC provisioning フィールドを選択します。 このフィールドにより、適切に有効にされた EAP-FAST クライアント用の自動 PAC プロビジョニングが有効になります。この例では、自動プロビジョニングが採用されています。
6. **許可された内部メソッドを**選択して下さい: EAP-GTC および EAP-MSCHAP2。 これにより、EAP-FAST v1 クライアントと EAP-FAST v1a クライアント両方の動作が許可されます Cisco Secure Services Client では EAP-FAST v1a をサポートしています ）。 EAP-FAST v1 クライアントをサポートする必要がない場合は、内部方式として EAP-MSCHAPv2 のみを有

効にする必要があります。

7. EAP-FAST Master Server チェックボックスを選択し、この EAP-FAST サーバをマスターとして有効にします。 これにより、ネットワーク内の各 ACS の一意のキーのプロビジョンを避けるために、その他の ACS サーバがこのサーバをマスター PAC Authority として利用できるようになります。 詳細は、『ACS 設定ガイド』を参照してください。
8. [Submit + Restart] をクリックします。




## Cisco WLAN コントローラ

展開ガイドとしてのこのドキュメントの目的に合わせて、CSSC テスト用の WLAN インフラストラクチャを提供するために、Cisco WS3750G Integrated Wireless LAN Controller（WLC）が、Cisco AP1240 Lightweight AP（LAP）とともに使用されます。 この設定は任意の Cisco WLAN コントローラに適用できます。 採用されているソフトウェアのバージョンは 4.0.155.5 です。

# ワイヤレス LAN コントローラの設定

## LAP の基本動作およびコントローラへの LAP の登録

WLC を基本動作用に設定するには、Command-Line Interface ( CLI; コマンドライン インターフェイス ) 上でスタートアップ コンフィギュレーション ウィザードを使用します。 または、WLC を設定するために GUI を使用することもできます。 このドキュメントでは、CLI 上でスタートアップ コンフィギュレーション ウィザードを使用した、WLC 上の設定について説明します。

WLC が初めて起動すると、スタートアップ コンフィギュレーション ウィザードに入ります。 基本設定を設定するには、コンフィギュレーション ウィザードを使用します。 このウィザードには CLI または GUI からアクセスできます。 次の出力は、CLI 上でのスタートアップ コンフィギュレーション ウィザードの例を示します。

```
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.
```

これらのパラメータにより、WLC が基本動作用に設定されます。 この設定例では、WLC は管理インターフェイス IP アドレスとして 10.10.80.3 を使用し、AP マネージャ インターフェイス IP アドレスとして 10.10.80.4 を使用しています。

その他の機能を WLC 上で設定する前に、WLC で LAP を登録する必要があります。 このドキュメントでは、LAP が WLC に登録されていることが前提となっています。 Lightweight AP の登録がどのように WLC で行われるかの詳細については、『Lightweight アクセス ポイントのための WLAN コントローラのフェールオーバーの設定例』の「Lightweight AP を WLC に登録する」のセクションを参照してください。 この設定例では、AP1240 は WLAN コントローラ ( 10.10.80.0/24 ) からは独立したサブネット ( 10.10.81.0/24 ) に展開され、コントローラ検出を行うため DHCP オプション 43 が使用されています。

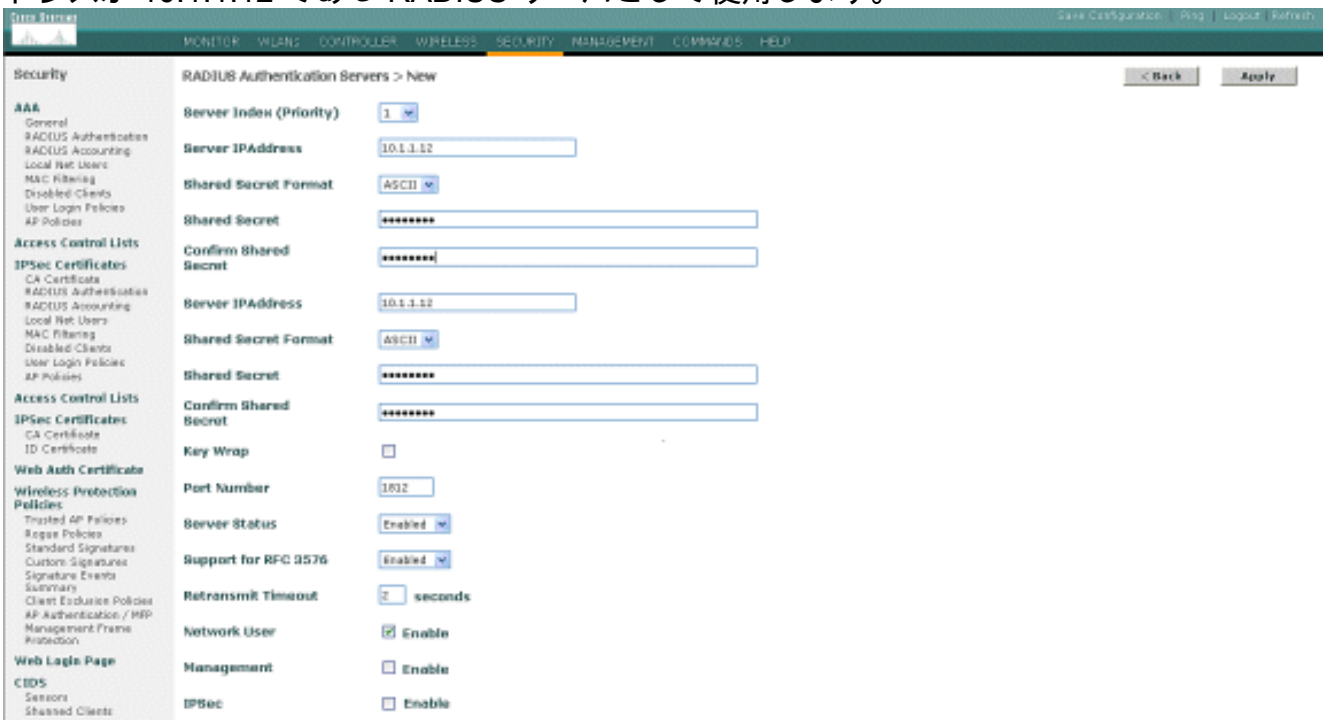
## Cisco Secure ACS を介した RADIUS 認証

WLC は、Cisco Secure ACS サーバへユーザのクレデンシャルを転送するように設定する必要があります。 そうすると、ACS サーバは ( 設定済みの Windows データベースを介して ) ユーザのクレデンシャルを検証し、ワイヤレス クライアントにアクセス権を提供します。

ACS サーバへのコミュニケーション用に WLC を設定するには、次の手順を実行します。

1. コントローラの GUI から Security と RADIUS Authentication をクリックして、RADIUS Authentication Servers ページを表示します。 続いて New をクリックして ACS サーバを定義します。


2. RADIUS認証サーバの ACS サーバ パラメータを > New ページ定義して下さい。 これらのパラメータには、ACS IP Address、Shared Secret、Port Number、および Server Status が含まれます。**注:** ポート番号 1645 または 1812 は、RADIUS 認証用に ACS と互換性があります。Network User チェック ボックスと Management チェック ボックスでは、ネットワーク ユーザ（WLAN クライアントなど）と管理（つまり管理ユーザ）に RADIUS ベースの認証を適用することを指定します。 設定例では、次のように、Cisco Secure ACS を IP アドレスが 10.1.1.12 である RADIUS サーバとして使用します。



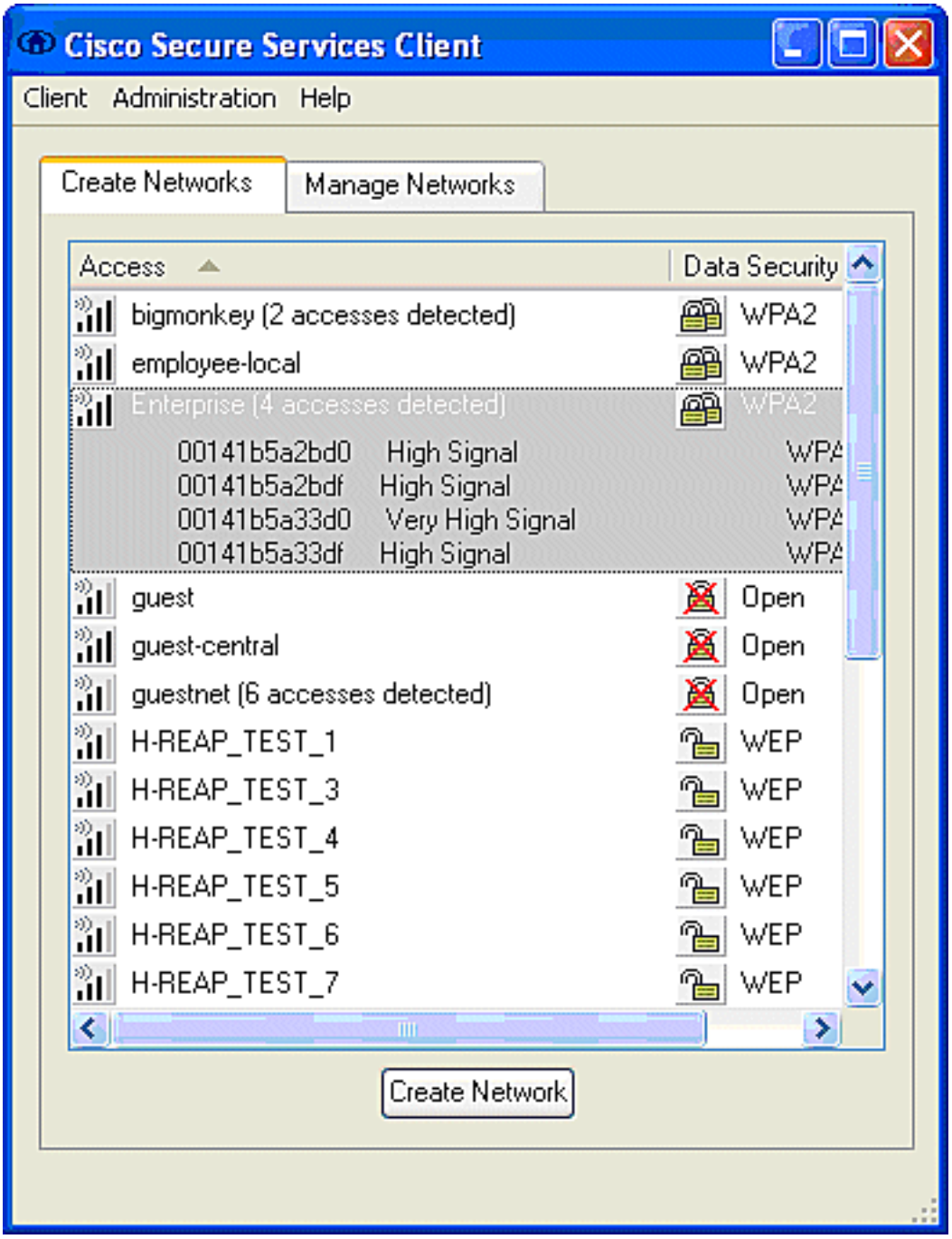

## WLAN パラメータの設定

このセクションでは、Cisco Secure Services Client の設定について説明します。 このドキュメントの例では、CSSC v4.0.5.4783 が Cisco CB21AG クライアント アダプタとともに使用されています。 CSSC ソフトウェアをインストールする前に、CB21AG 用のドライバのみがインストールされ、Aironet Desktop Utility（ADU）がインストールされていないことを確認してください。

このソフトウェアがインストールされ、サービスとして動作するようになると、そのサービスは使用可能なネットワークをスキャンし、使用可能なネットワークを表示します。

**注:** CSSC により Windows Zero Config が無効にされます。

**注:** ブロードキャストに対して有効になっている SSID のみが可視になります。




**注:** デフォルトでは WLAN コントローラは SSID をブロードキャストするため、その SSID が、スキャンされた SSID の Create Networks リストに表示されます。 Network Profile を作成するには、リスト（Enterprise）の SSID および Create Network オプション ボタンをクリックするだけで済みます。

WLAN インフラストラクチャがディセーブルにされるブロードキャスト SSID で設定される場合手動で SSID を追加して下さい; **Addオプション・ ボタンを**アクセスデバイスの下でクリックし、手動で適切な **SSID を**入力して下さい（たとえば、企業）。 クライアントのためのアクティブなプローブ 動作を、すなわち、ところで設定された SSID のためのクライアント アクティブにプローブ設定して下さい; 追加アクセスデバイス ウィンドウの SSID を入力した後**このアクセスデバイスのための検索をアクティブに** 規定 して下さい。

**注:** EAP 認証設定がプロファイルに対して設定されていない場合、ポート設定ではエンタープライズ モード（802.1X）は許可されません。

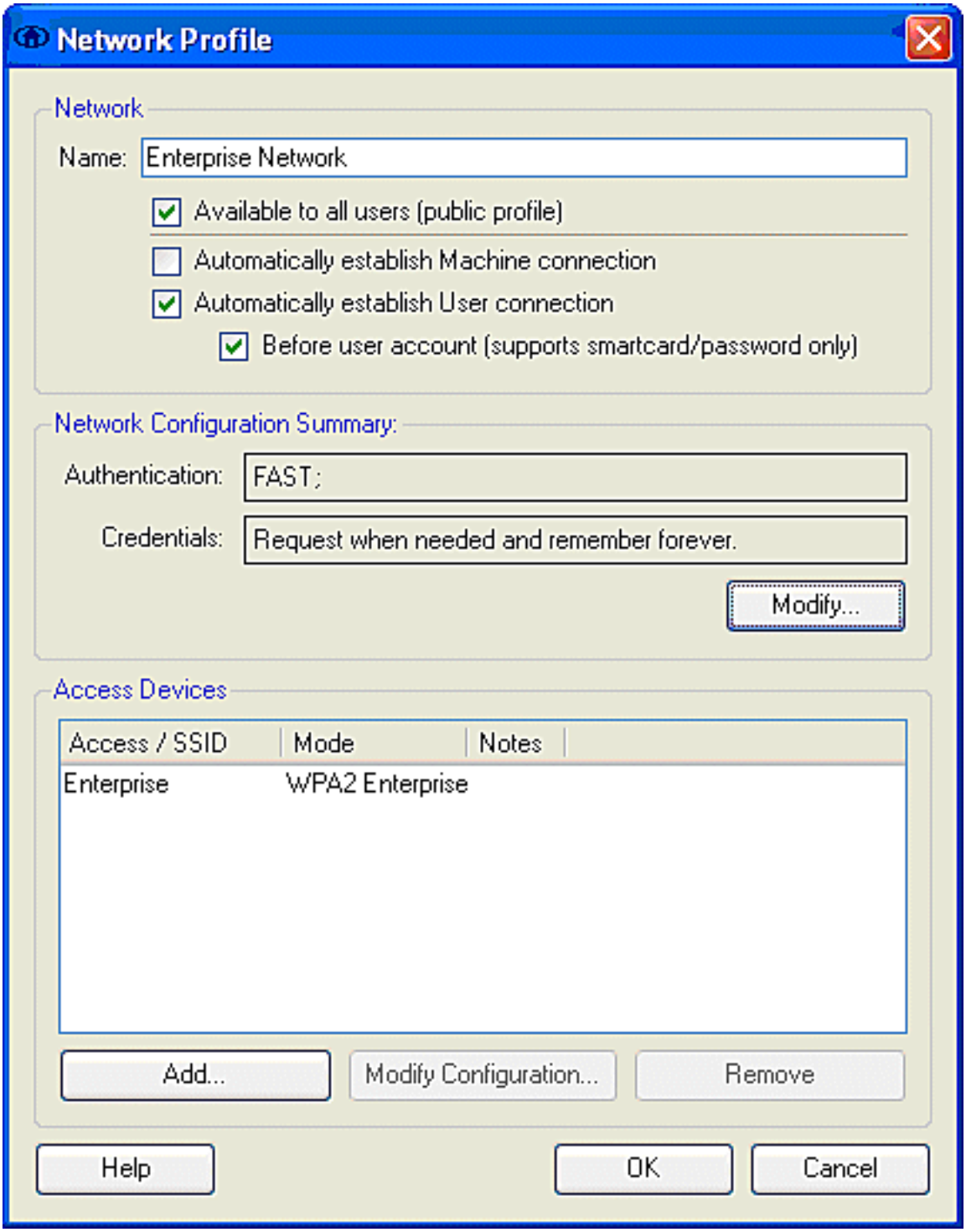
Create Network オプション ボタンを押すと Network Profile ウィンドウが表示され、このウィンドウでは選択済み（または設定済み）の SSID を認証メカニズムと関連付けることができます。

プロファイルに説明的な名前を割り当てます。

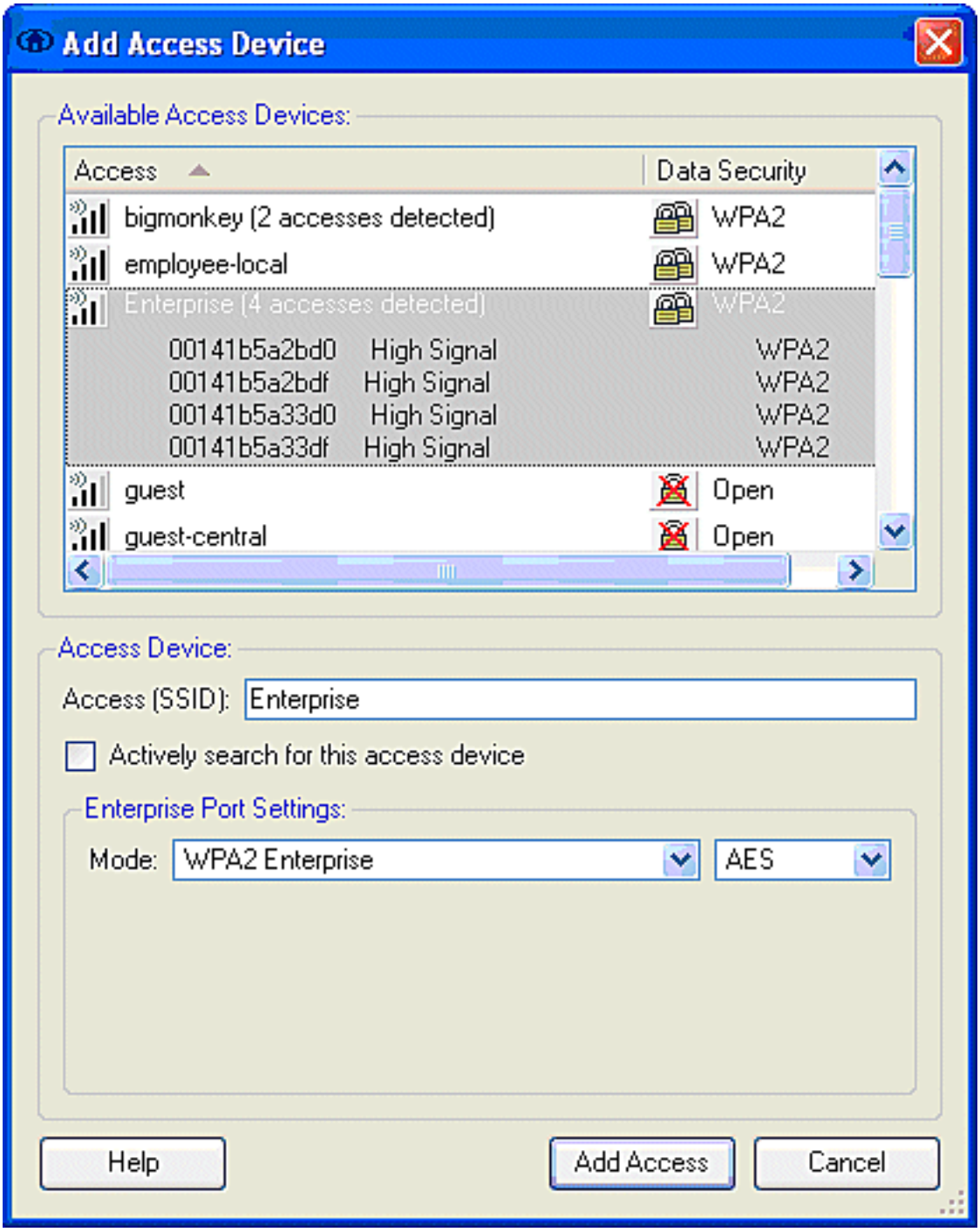
**注:** この認証プロファイルの下では、複数の WLAN セキュリティ タイプや SSID をアソシエーションすることができます。

RF カバー範囲内にある際にクライアントを自動的にネットワークに接続させるには、Automatically establish User connection を選択します。 このプロファイルをマシン上の他のユーザ アカウントとともに使用することが望ましくない場合、Available to all users のチェックを外します。 Automatically establish が選択されていない場合、ユーザが CSSC ウィンドウを開き、Connect オプション ボタンで WLAN 接続を手動で開始する必要があります。

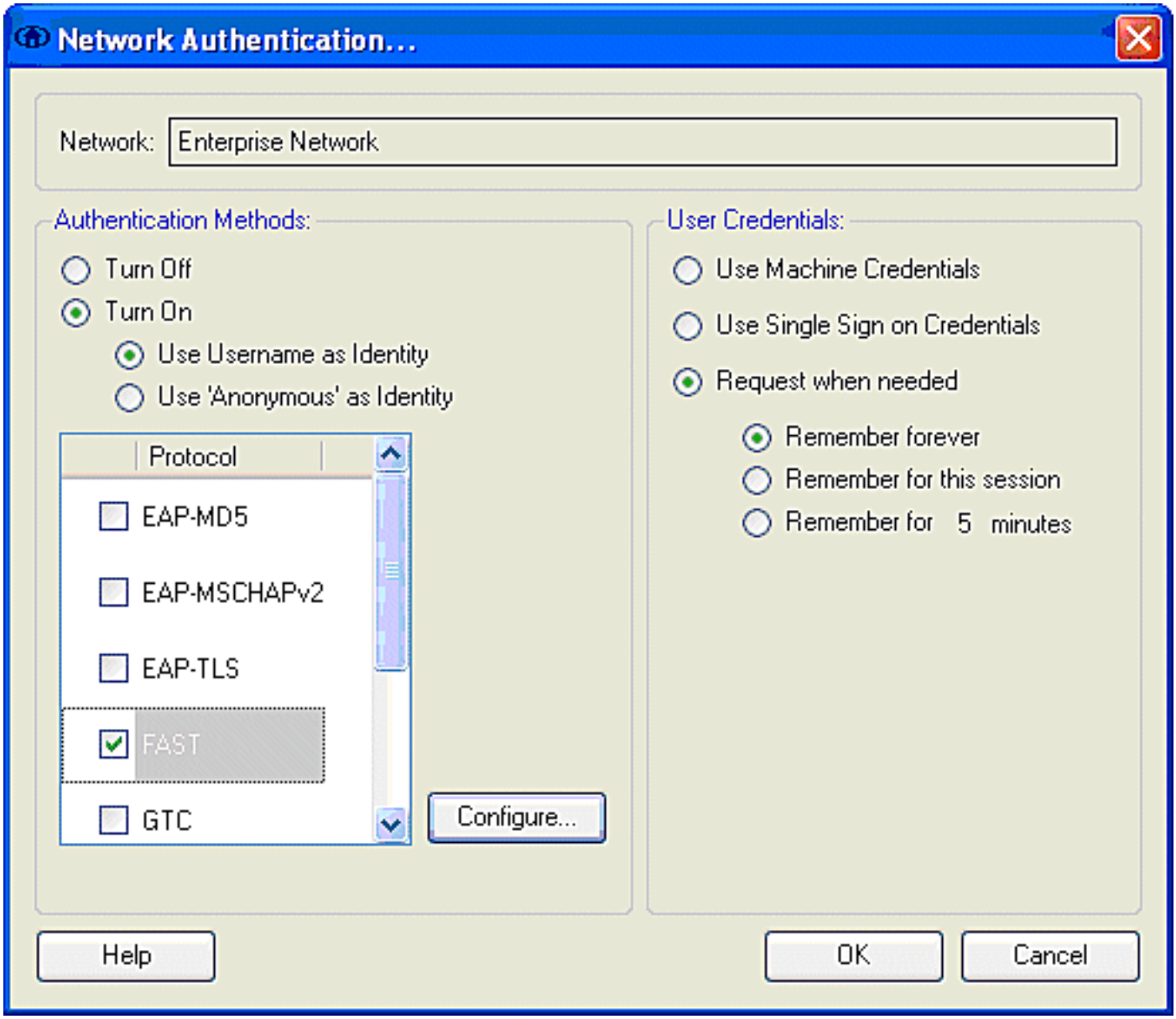
ユーザ ログオンの前に WLAN 接続を開始することが望ましい場合は、Before user account を選択します。 これにより、保存されたユーザのクレデンシャルを使用したシングル サインオン動作が可能になります ( パスワードまたは証明書/EAP-FAST 内で TLS を使用する場合はスマートカード ) 。




**注:** Cisco Aironet 350 シリーズ クライアント アダプタでの WPA/TKIP の動作に関しては、WPA ハンドシェイク ハッシュ検証に関して CSSC クライアントと 350 ドライバとの間には現時点で互換性がないため、WPA ハンドシェイク検証を無効にする必要があります。 これは**クライアント > 詳細設定 > WPA/WPA2 ハンドシェイク 検証**の下で無効です。 無効にされたハンドシェイク検証では依然として WPA に固有のセキュリティ機能（TKIP のパケットごとのキー生成および Message Integrity Check）は許可されますが、最初の WPA キー認証が無効にされます。




Network Configuration Summary の下で Modify をクリックして EAP/クレデンシャルの設定を設定します。 Turn On 認証を指定し、Protocol の下で FAST を選択し、（最初の EAP 要求でユーザ名を使用しないために）'Anonymous' as Identity を選択します。 Use Username as Identity を外部 EAP 識別情報として使用することは可能ですが、お客様の多くでは最初の暗号化されていない EAP 要求でユーザ ID を提示することは希望されません。 ネットワーク認証用のログオン クレデンシャルを使用するには、Use Single Sign on Credentials を指定します。 Configure をクリックして EAP-FAST のパラメータを設定します。




FAST 設定の下では、EAP-FAST セッションの確立の前に EAP-FAST サーバ（ACS）証明書をクライアントが検証できるようにする Validate Server Certificate を指定できます。 これにより、未知のまたは不正な EAP-FAST サーバへの接続や、信頼できないソースへ不用意に認証のためのクレデンシャルを発行してしまうことから、クライアント デバイスを保護できます。 これには、ACS サーバに証明書がインストールされている必要はなく、またクライアントには対応する Root Certificate Authority 証明書がインストールされている必要もありません。 この例では、サーバ証明書の検証は有効ではありません。

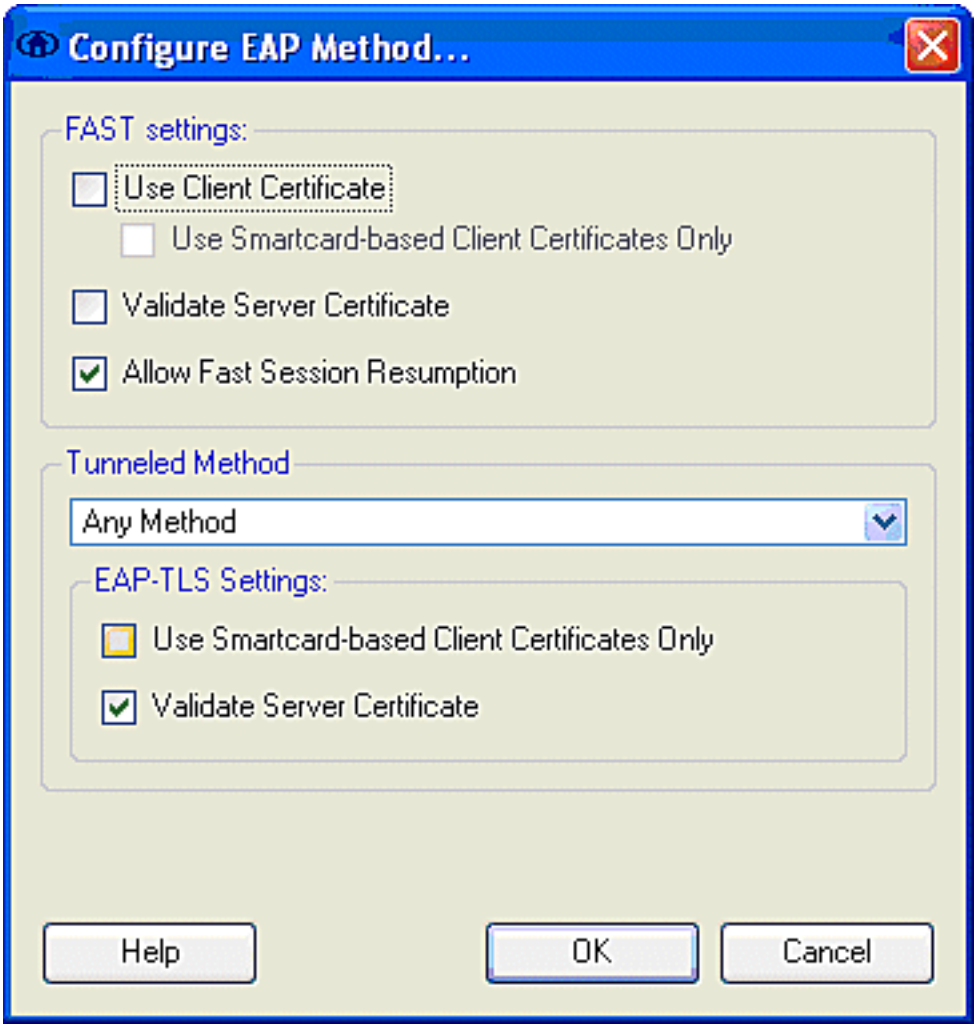
FAST 設定の下では Allow Fast Session Resumption を指定することが可能です。これにより、完全な EAP-FAST の再認証を必要とせずに、トンネル（TLS セッション）情報に基づく EAP-FAST セッションの再開が可能になります。 EAP-FAST サーバとクライアントが最初の EAP-FAST 認証交換内でネゴシエートされる TLS セッション情報を共通して認識している場合、セッションの再開が可能になります。

**注:** EAP-FAST サーバとクライアントの両方が EAP-FAST セッション再開用に設定されている必要があります。

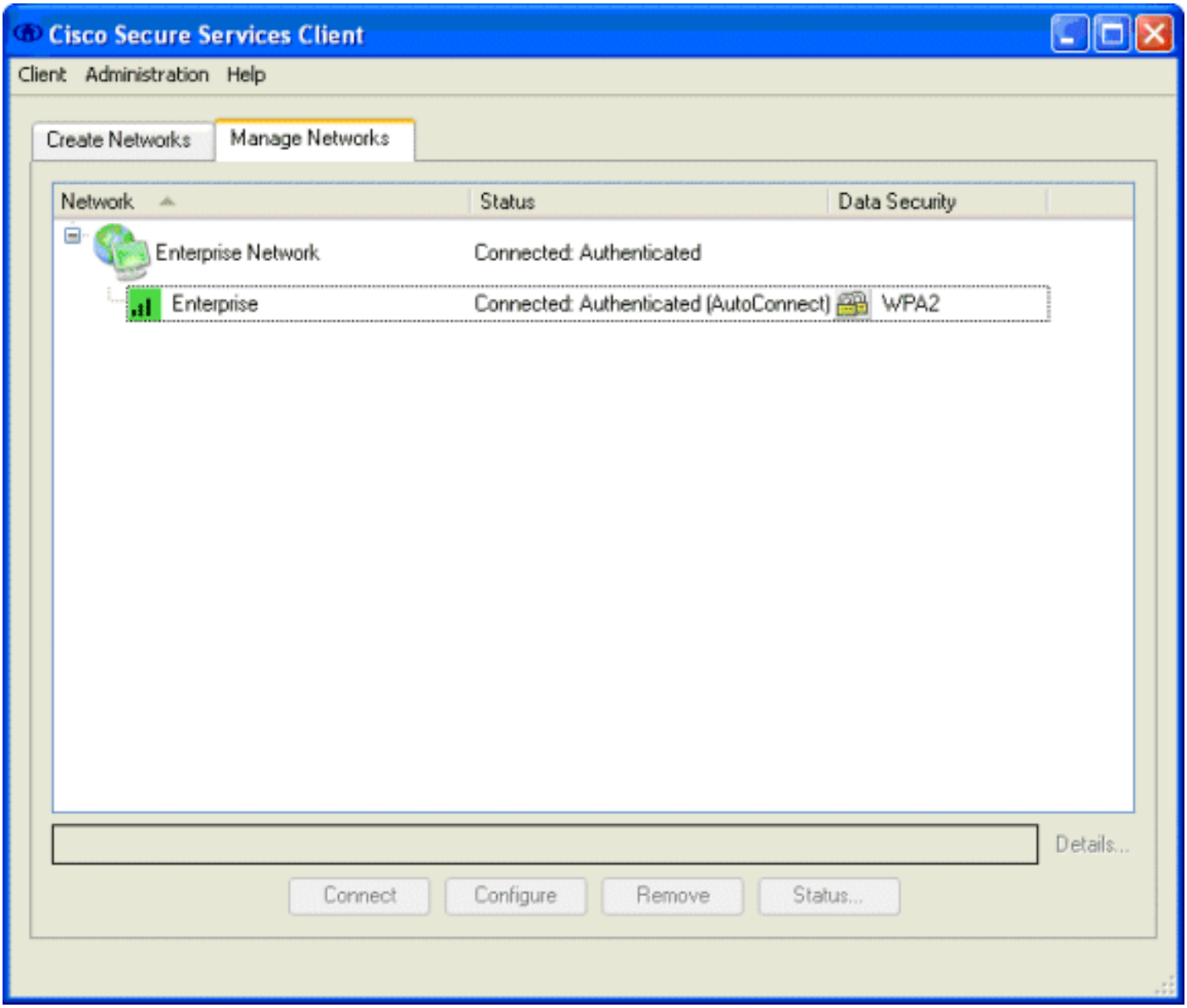
トンネル伝送された方式 > EAP-TLS 設定の下で、割り当てに**方式を** PAC 自動プロビジョニングするための EAP-MSCHAPv2 および認証のための EAP-GTC 規定 して下さい。 Active Directory などの Microsoft 形式のデータベースを使用していて、そのデータベースでネットワーク上の EAP-FAST v1 クライアントがサポートされていない場合、Tunneled Method としては

MSCHAPv2 のみの使用を指定することもできます。

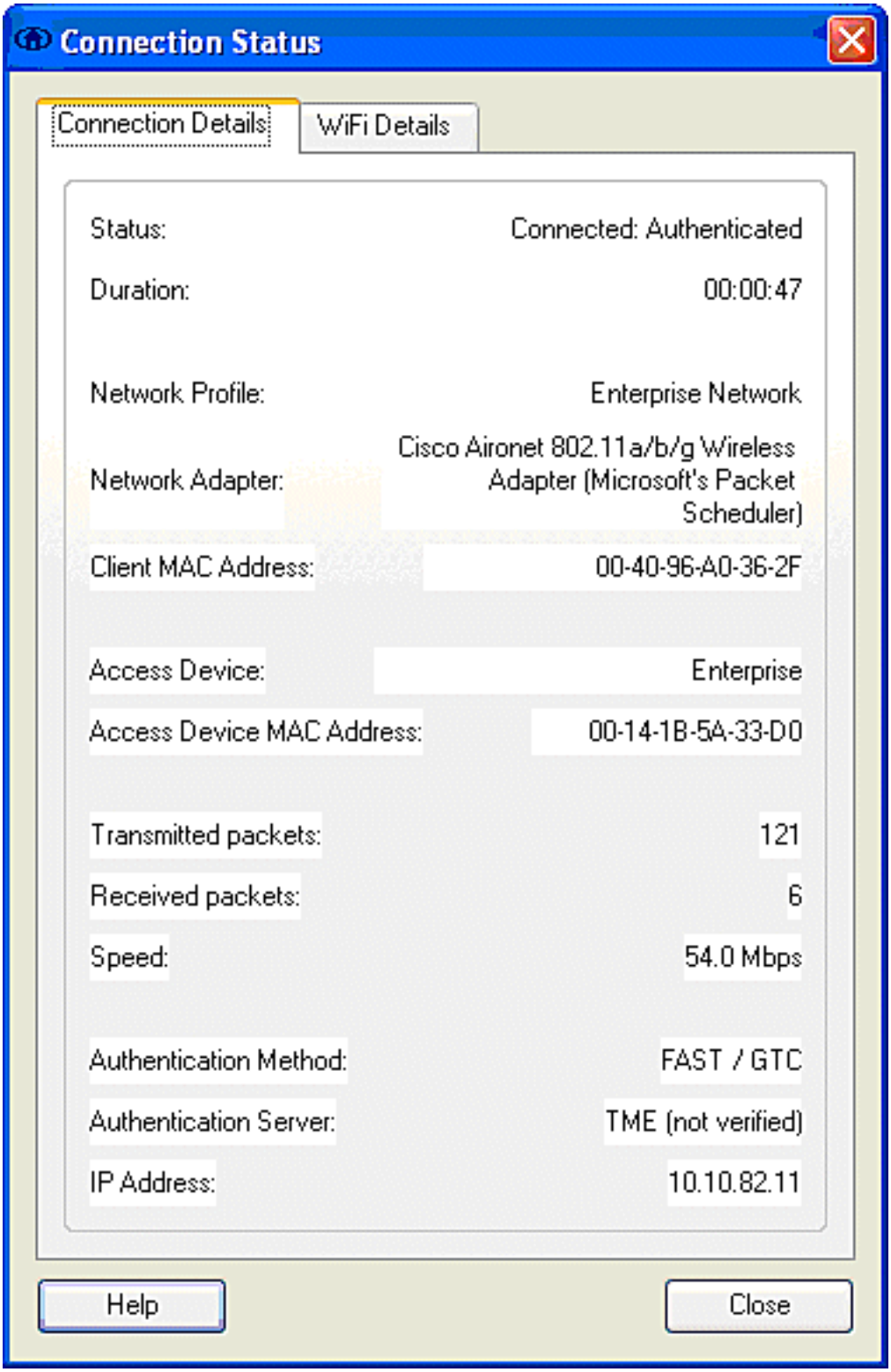
**注:** Validate Server Certificate は、このウィンドウ上の EAP-TLS 設定の下でデフォルトで有効になっています。 この例では内部認証方式として EAP-TLS を使用していないため、このフィールドは適用できません。 このフィールドが有効である場合、EAP-TLS 内でのクライアント証明書のサーバによる検証に加えて、クライアントがサーバ証明書を検証することもできます。

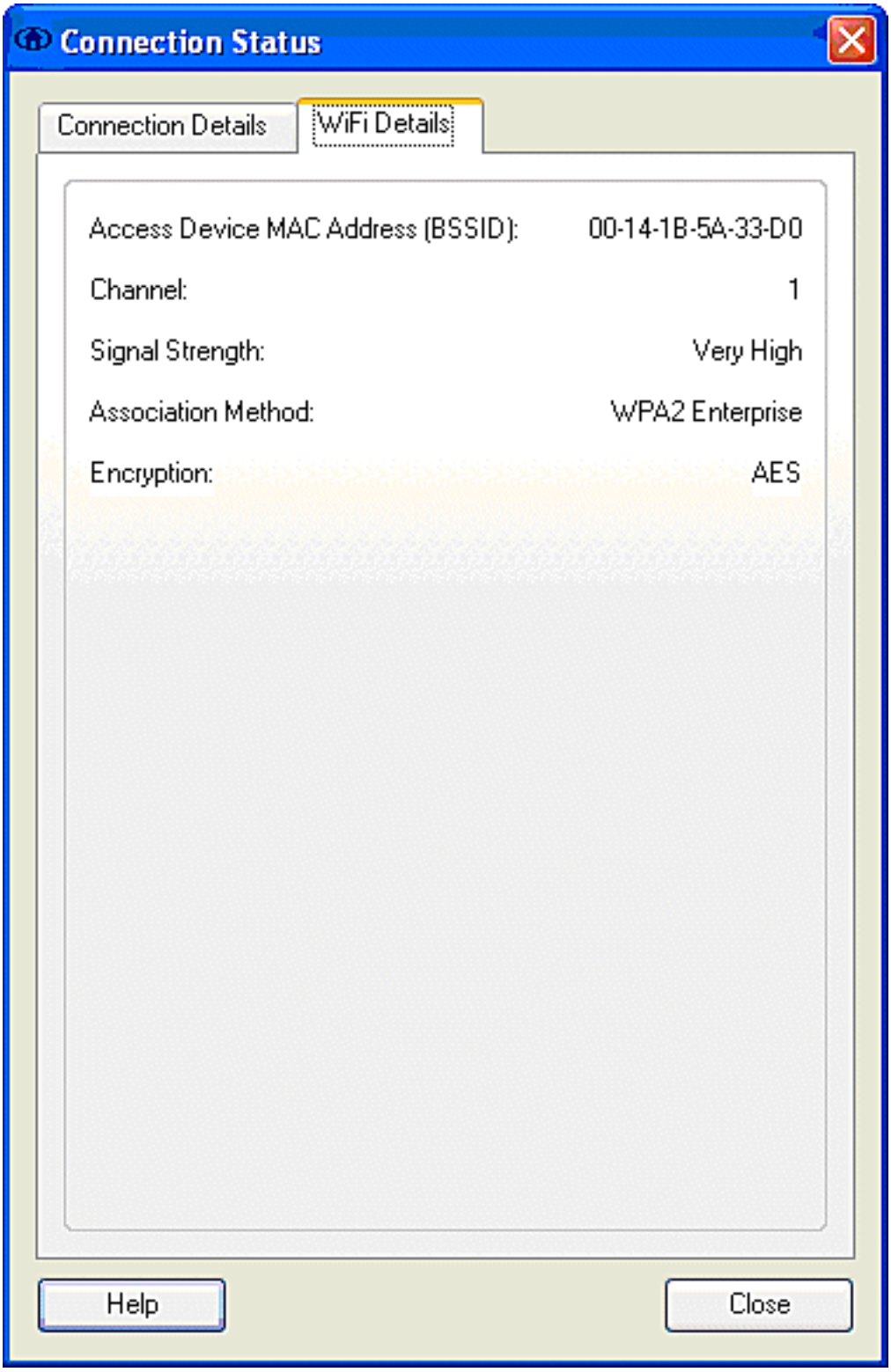



EAP-FAST の設定を保存するには OK をクリックします。 クライアントはプロファイルの下で「automatically establish」用に設定されているため、自動的にネットワークとのアソシエーション/認証が開始されます。 Manage Networks タブの、Network、Status、および Data Security フィールドはクライアントの接続状態を示しています。 例から、プロファイル エンタープライズ ネットワークが使用中である、ネットワーク アクセス デバイスは接続されて示す SSID 企業ですことが見られ、: 認証されて使用は自動接続し。 Data Security フィールドは、採用されている 802.11 暗号化タイプを示しています ( この例では WPA2 ) 。




クライアントが認証を行った後、接続の詳細情報を照会するには、[Manage Networks] タブの [Profile] の下で [SSID] を選択し、[Status] をクリックします。 [Connection Details] ウィンドウには、クライアント デバイス、接続の状態と統計、および認証方式に関する情報が表示されます。 [WiFi Details] タブには、802.11 の接続状態に関する詳細情報が表示されますが、これには RSSI、802.11 チャネル、および認証/暗号化が含まれます。


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




システム管理者であるユーザは、標準の CSSC ディストリビューションで利用可能な診断ユーティリティである Cisco Secure Services Client System Report を使用する資格があります。 このユーティリティはスタート メニューまたは CSSC ディレクトリから使用できます。 データを得るために、**集めますクリップボードにデータ > コピーを > 取付けますレポートファイルを**クリックして下さい。 これにより、Microsoft File Explorer ウィンドウでは、zip 圧縮されたレポート ファイルがあるディレクトリが表示されます。 zip 圧縮されたファイル内では、log ( log_current ) の下に最も有用なデータがあります。

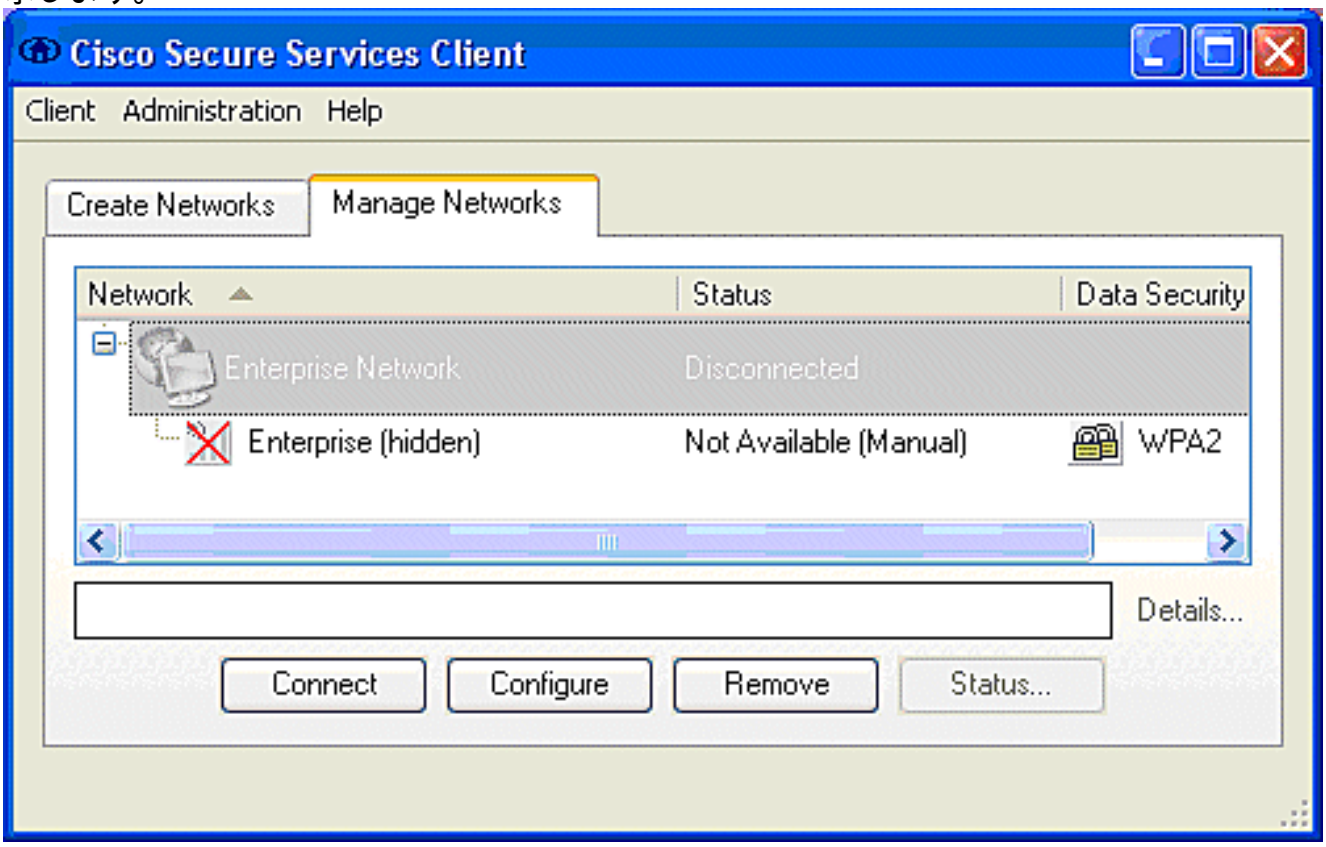
このユーティリティからは、CSSC、インターフェイス、およびドライバの詳細情報の現在の状態だけでなく、WLAN の情報 ( 検出された SSID、アソシエーション状態など ) が分かります。 このユーティリティは、特に CSSC と WLAN アダプタの間の接続の問題を診断するのに便利です。

# 動作の確認

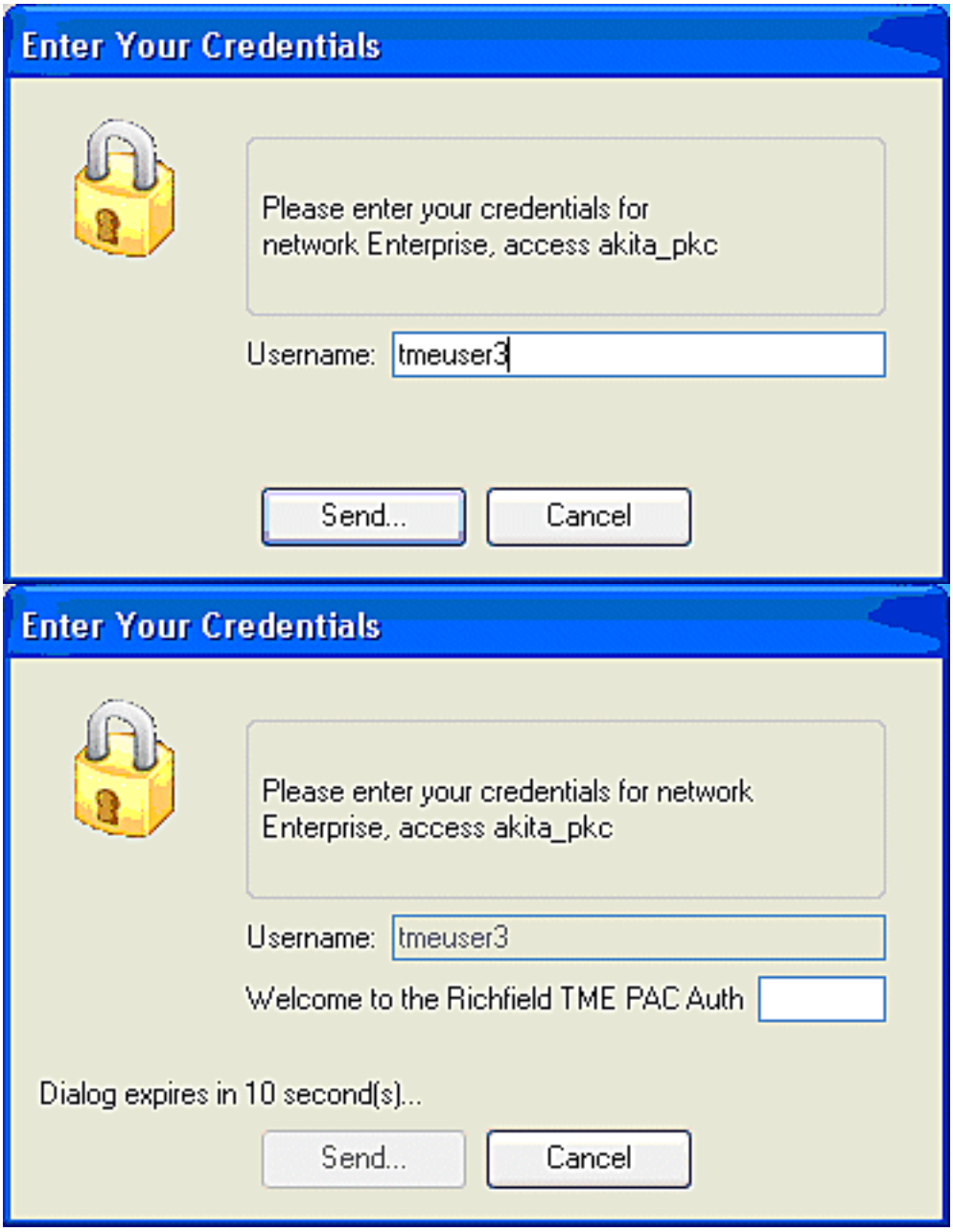
Cisco Secure ACS サーバ、WLAN コントローラ、CSSC クライアントの設定、およびおそらく正しい設定とデータベース ポピュレーションの後、WLAN ネットワークは EAP-FAST 認証および安全なクライアント通信用に設定されます。 セキュアなセッションのためには、進行状況/エラーをチェックするために監視可能な数多くのポイントがあります。

設定をテストするには、EAP-FAST 認証を使用してワイヤレス クライアントと WLAN コントローラを関連付けてみます。

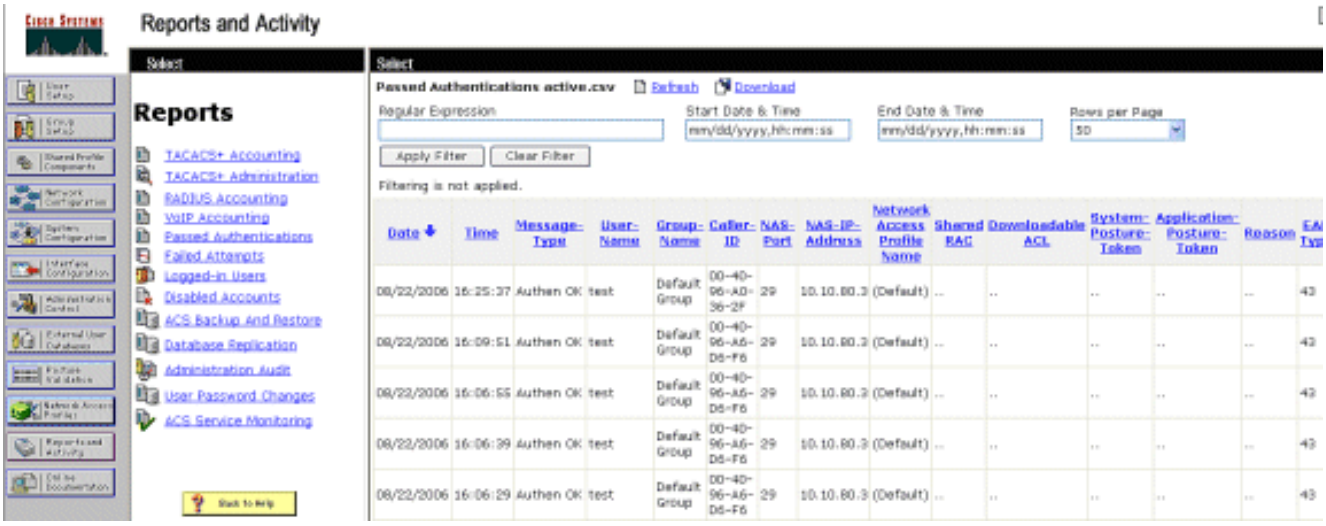
1. CSSC が Auto-Connection に設定されている場合、クライアントはこの接続を自動的に試行します。 CSSC が Auto-Connection とシングル サインオン動作に設定されていない場合、ユーザは Connect オプション ボタンにより WLAN 接続を開始する必要があります。 これにより、EAP 認証が行われる 802.11 アソシエーション プロセスが開始されます。次に例を示します。



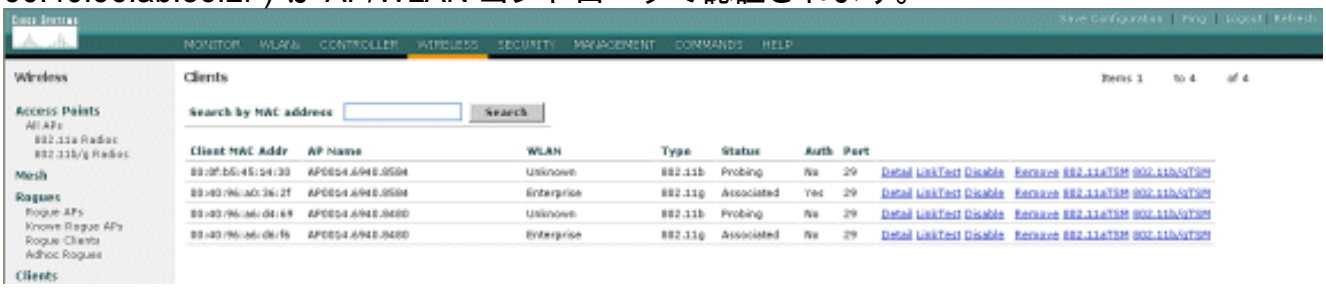

2. 続いてユーザは（EAP-FAST PAC Authority または ACS から）EAP-FAST 認証用のユーザ名、続いてパスワードを入力するよう求められます。次に例を示します。




3. CSSC クライアントは続いて、クレデンシャルを検証するために、WLC を使用してユーザのクレデンシャルを RADIUS サーバ（Cisco Secure ACS）に渡します。 ACS は、データと設定済みのデータベース（設定例では外部データベースは Windows Active Directory）の比較によりユーザのクレデンシャルを確認し、ユーザのクレデンシャルが有効である場合は常にワイヤレス クライアントにアクセス権を提供します。 ACS サーバ上の Passed Authentications レポートには、クライアントが RADIUS/EAP 認証をパスしたことが示されます。次に例を示します。




4. RADIUS/EAP 認証に成功した時点で、ワイヤレス クライアント（この例では 00:40:96:ab:36:2f）は AP/WLAN コントローラで認証されます。




# 付録

Cisco Secure ACS および Cisco WLAN コントローラで使用可能な診断およびステータス情報に加えて、EAP-FAST 認証の診断に使用可能な追加ポイントが存在します。 認証の問題の大部分は、WLAN スニファを使用したり WLAN コントローラで EAP 交換をデバッグすることなく診断できますが、トラブルシューティングに役立つように、この参照資料が収録されています。

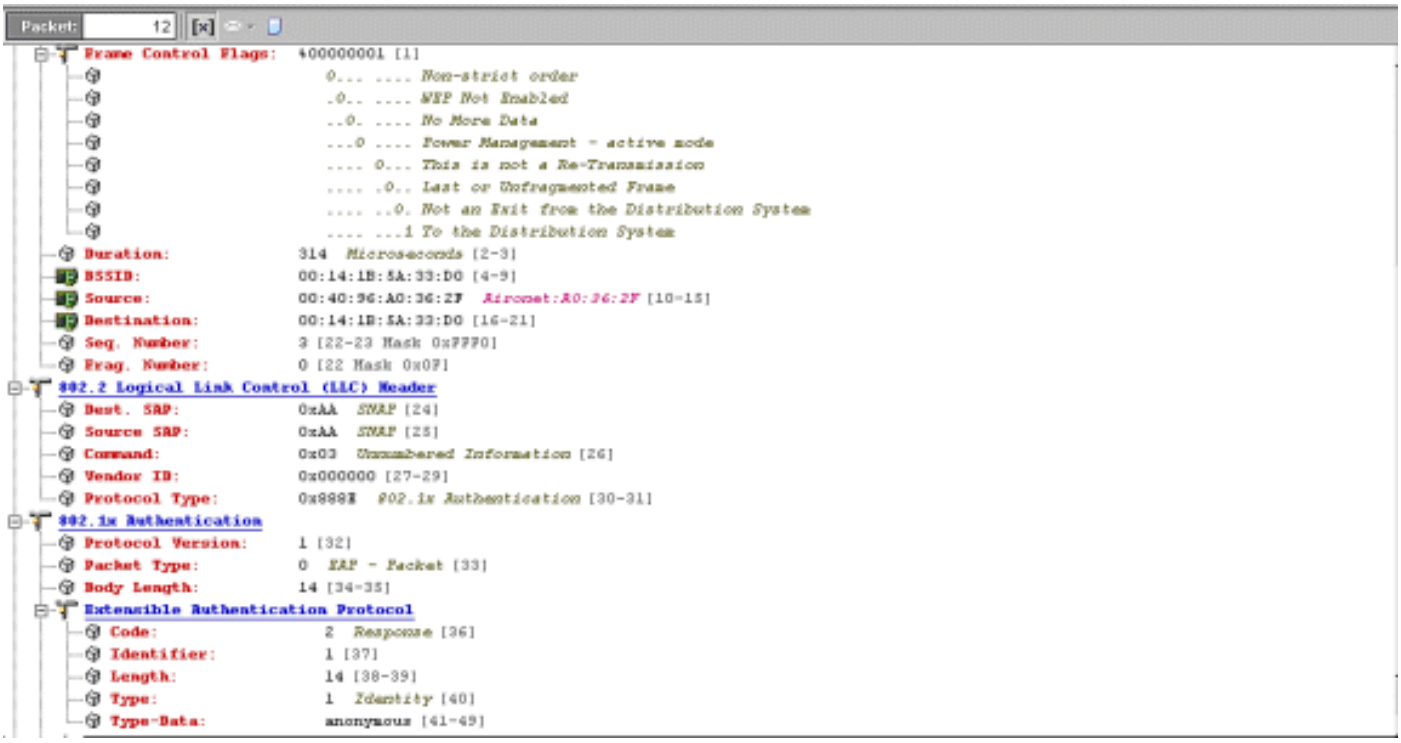
## EAP-FAST Exchange のスニファ キャプチャ

次の 802.11 スニファ キャプチャは、認証交換を示しています。

| 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 |

このパケットは、最初の EAP-FAST EAP 応答を示しています。

**注:** CSSC クライアントで設定されているように、最初の EAP 応答では外部 EAP 識別情報として「anonymous」が使用されています。




## WLAN コントローラでのデバッグ

認証交換の進行状況を監視するために、WLAN コントローラでは次の debug コマンドが使用できます。

- debug aaa events enable
- debug aaa detail enable

- debug dot1x events enable
- debug dot1x states enable

デバッグを使用して WLAN コントローラで監視された、CSSC クライアントと ACS の間の認証トランザクションの開始の例を次に示します。

```
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)
```

次に、( WPA2 認証を使用した ) コントローラ デバッグからの成功した EAP 交換完了を示します。

```
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 (messa1
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
```

# 関連情報

- Cisco Secure ACS for Windows Server のインストール ガイド
- Cisco Secure ACS 4.1 の設定ガイド
- WLC と Cisco Secure ACS を使用した SSID に基づく WLAN アクセス制限の設定例
- ACS 4.0 と Windows 2003 を使用した Unified Wireless Network 環境での EAP-TLS
- RADIUS **LAN VLAN** 設定例
- テクニカルサポートとドキュメント - Cisco Systems