CHAPTER 4

Profile Settings タブ

この章では、ACAT プロファイル オプションについて説明します。この章では、次の項目について説明します。

プロファイルの追加

ACAT を使用すると、既存の構成プロファイルのインポートや、新しいプロファイルの作成ができます。ACAT の File メニューには、次の 2 つのプロファイル オプションがあります。

- Create/Manage Profile：このオプションでは、新しいプロファイル名を追加、削除、または変更できます。プロファイル名を定義すると、ACAT の Profile Settings タブで各プロファイルを設定できます。
- Load from Registry：このオプションでは、PC のレジストリから ACAT コンフィギュレーション ファイルに既存のプロファイルをインポートまたはロードできます。

ACU を使用すると、プロファイルを作成し、確認してから、他のユーザに配布できます。ACU で作成したプロファイルは、PC のレジストリに保存されます。プロファイルが正しく機能することを確認した後、ACAT の Load from Registry オプションを使用して、特定のクライアント アダプタ タイプのプロファイルを ACAT コンフィギュレーション ファイルにインポートします。

プロファイルは、クライアント アダプタ ドライバ用に予約されたレジストリの一部として保存されるので、特定の無線タイプに関連付けられます。したがって、350 シリーズ PC カードのプロファイルを設定し、後でクライアント アダプタを CB20A PC カードにアップグレードした場合、これらのプロファイルはすべて新しいクライアント アダプタで使用できなくなります。

一般的な推奨事項

複数のタイプのクライアント アダプタを設定する必要がある場合は、次の推奨事項に従ってください。

- ユーザ全員がアクセスできるサーバで、各クライアント アダプタ用にディレクトリを作成して名前を付けます。
- 各クライアント アダプタ ディレクトリに、すべての Install Wizard ファイルおよびサブディレクトリのコピーを置きます。
- クライアント アダプタのタイプごとに、必要なプロファイルと設定パラメータを持つ ACAT コンフィギュレーション ファイルを作成します。各 ACAT コンフィギュレーション ファイルを、Install Wizard のファイルとともに該当のクライアント アダプタ ディレクトリに保存します。

（注）　すべての ACAT コンフィギュレーション ファイルには同じファイル名（CiscoAdminConfig.dat）が使用されるため、それぞれ異なるフォルダに保存する必要があります。

- ユーザが特定のタイプのクライアント アダプタのプロファイルをインストールするには、該当のクライアント アダプタ ディレクトリで Install Wizard（IWSetup.exe）を実行します。

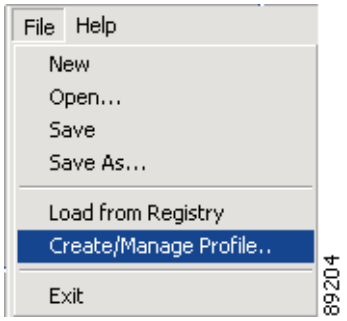
Create/Manage Profile

ACAT でプロファイルを設定する前に、各プロファイルの新しいプロファイル名を作成する必要があります。File メニューの Create/Manage Profile オプションを使用すると、新しいプロファイル名を追加、削除、または変更できます。最大 16 個のプロファイルを作成できます。

新しいプロファイル名を作成する手順は、次のとおりです。

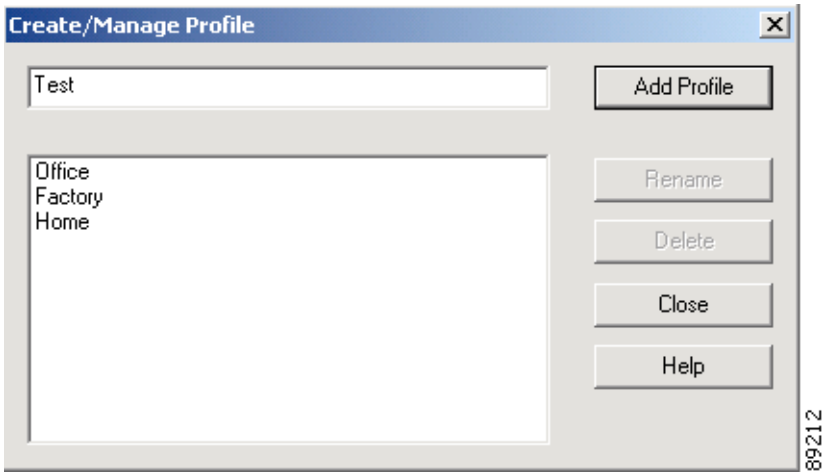
ステップ 1　ACAT の File メニューで **Create/Manage Profile** を選択します（図 4-1 を参照）。

図 4-1　Create/Manage Profile オプション



このオプションを選択すると、Create/Manage Profile ウィンドウが表示されます（図 4-2 を参照）。

図 4-2　Create/Manage Profile ウィンドウ



ステップ 2　入力フィールドに新しいプロファイルの名前（1 ～ 79 文字の American Standard Code for Information Interchange（ASCII; 米国規格協会情報交換標準コード）文字）を入力し、**Add Profile** をクリックします。

ステップ 3　プロファイル名を変更するには、プロファイル名をクリックして **Rename** をクリックします。また、削除するには、**Delete** をクリックします。

ステップ 4　新しいプロファイルの名前を入力した後、**Close** をクリックします。

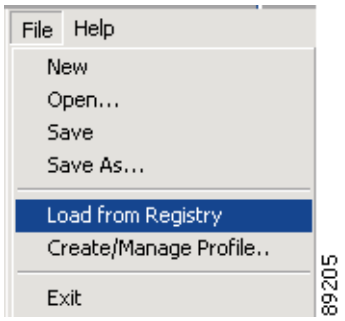
（注）　最大 16 個のプロファイルを作成できます。

プロファイル設定パラメータの入力方法は、「Profile Settings タブでのプロファイルの編集」の項（P. 4-5）を参照してください。

Load From Registry

ACAT ユーティリティでは、File メニューの Load from Registry オプション（図 4-3 を参照）を使用して、PC のレジストリから既存のプロファイルをインポートできます。

図 4-3　Load from Registry オプション



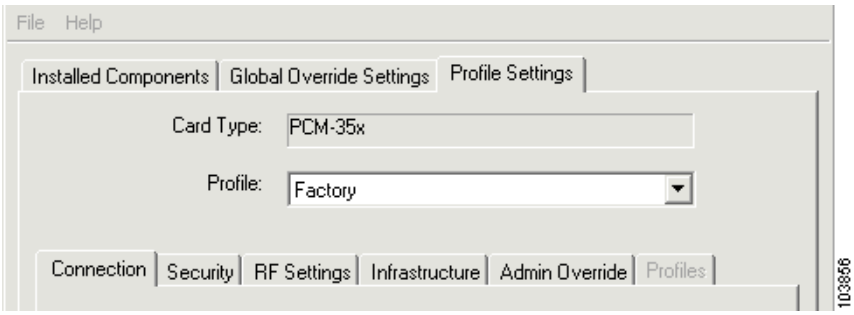
このオプションを選択する前に、ACU を使用して新しいプロファイルを作成しておく必要があります。これらのプロファイルは、PC のレジストリに保存されます。

インポートしたプロファイル パラメータの表示方法および編集方法は、「Profile Settings タブでのプロファイルの編集」の項（P. 4-5）を参照してください。

Profile Settings タブでのプロファイルの編集

ACAT Profile Settings タブでは、既存のプロファイルや作成中の新しいプロファイルを編集できます（図 4-4 を参照）。

図 4-4　Profile Settings タブ ウィンドウ



この項では、次の項目について説明します。

- Card Type（P. 4-5）
- Profile（P. 4-6）
- Connection タブ（P. 4-6）
- Security タブ（P. 4-10）
- RF Settings タブ（P. 4-27）
- Infrastructure タブ（P. 4-34）
- Ad Hoc タブ（P. 4-37）
- Admin Override タブ（P. 4-40）
- Auto Profile Selection（P. 4-41）

Card Type

Card Type フィールドには、プロファイルで使用されているクライアント アダプタ カードのタイプが示されます。カード タイプは、File メニューで New オプションを選択したときに指定します。ACAT では、デフォルトでカードタイプとして 350 シリーズ PCMCIA（PCM-35x）が設定されます次のカード タイプがサポートされています。

- PCM-35x：Cisco Aironet 350 シリーズ PCMCIA カード
- MPI-35x：Cisco Aironet 350 シリーズ mini-PCI カード
- PCI-35x：Cisco Aironet 350 シリーズ PCI カード
- CB20A：Cisco Aironet 5GHz Cardbus PC カード

（注）　ACAT 1.6 と互換性があるのは、Install Wizard 1.6 のみです。

（注）　ACAT 1.6 は、Cisco Aironet 340 および 4800 シリーズのクライアント アダプタや Cisco Aironet Institute of Electrical and Electronics Engineers（IEEE; 電気電子学会）802.11a/b/g ワイヤレス LAN クライアント アダプタ（CB21AG および PI21AG）をサポートしていません。

Profile

Profile フィールドでは、設定するプロファイルを選択できます。フィールドの右側の矢印をクリックすると、プロファイルのリストが表示されます。

Connection タブ

Connection タブを使用すると、接続固有のパラメータとクライアント アダプタのパワー セーブ モードを指定できます。このウィンドウを図 4-5 に示します。

図 4-5　Connection タブ ウィンドウ

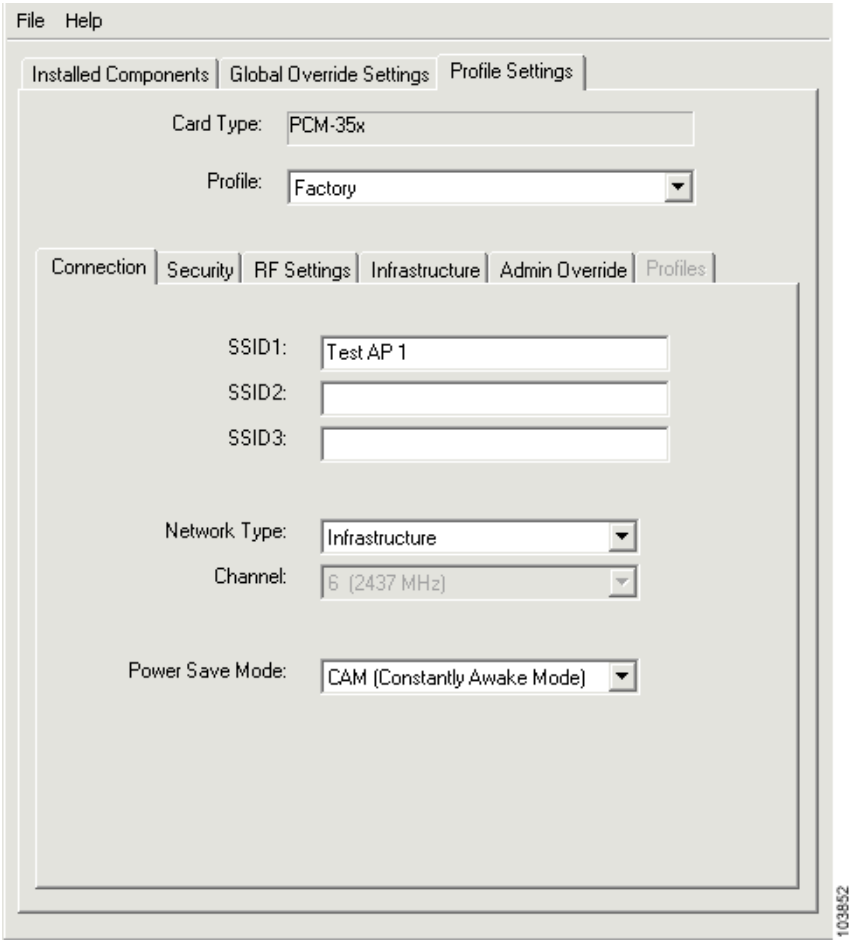


表 4-1 は、Connection タブのパラメータとその説明を示しています。

表 4-1　Connection タブのパラメータ

パラメータ	説明
SSID1	service set identifier（SSID; サービス セット ID）は、アクセスする個々の無線ネットワークを特定します。 **値の範囲：**最大で 32 文字の ASCII 文字（大文字 / 小文字が区別されます） **デフォルト：**空白 （注）　このパラメータを空白のままにすると、クライアント アダプタは、ブロードキャスト SSID を使用できるように設定されているネットワーク上のあらゆるアクセス ポイントにアソシエートできます（アクセス ポイントの資料を参照してください）。クライアント アダプタが通信するアクセス ポイントがブロードキャスト SSID を使用できるよう設定されていない場合は、このパラメータの値がアクセス ポイントの SSID と一致している必要があります。そうでない場合は、クライアント アダプタはネットワークにアクセスできません。
SSID2	クライアント アダプタを再設定しなくても、2 つ目の別のネットワークを識別して、そのネットワークにローミングできるようにするオプションの SSID。 （注）　複数の SSID を持つプロファイルは、自動プロファイル切り替えでは使用できません。 **値の範囲：**最大で 32 文字の ASCII 文字（大文字 / 小文字が区別されます） **デフォルト：**空白
SSID3	クライアント アダプタを再設定しなくても、3 つ目の別のネットワークを識別して、そのネットワークにローミングできるようにするオプションの SSID。 （注）　複数の SSID を持つプロファイルは、自動プロファイル切り替えでは使用できません。 **値の範囲：**最大で 32 文字の ASCII 文字（大文字 / 小文字が区別されます） **デフォルト：**空白

表 4-1　Connection タブのパラメータ（続き）

<table>
<tr><th>パラメータ</th><th>説明</th></tr>
<tr><td>Network Type</td><td>クライアント アダプタをインストールするネットワークのタイプを指定します。

オプション：Ad Hoc または Infrastructure
デフォルト：Infrastructure

Network Type ／ 説明
Ad Hoc ／ ピア ツー ピアと呼ばれることもあります。無線ネットワークが、アクセス ポイント経由で有線イーサネット ネットワークに接続されていない少数の無線デバイスから構成されていることを示します。たとえば、会議室のコンピュータ間にアドホック ネットワークを設定すれば、会議の情報をユーザ間で共有できます。
Infrastructure ／ 無線ネットワークがアクセス ポイント経由で有線イーサネット ネットワークに接続されていることを示します。</td></tr>
<tr><td>Channel</td><td>クライアント アダプタで通信チャネルとして使用する周波数を指定します。これらのチャネルは、規制地域の IEEE 802.11 規格に準拠しています。

• インフラストラクチャ モードでは、このパラメータは自動的に設定されるため、変更できません。クライアント アダプタはスペクトラム全体をリスンして、最適なアソシエート先アクセス ポイントを選択し、そのアクセス ポイントと同じ周波数を使用します。
• アドホック モードでは、クライアント アダプタのチャネルは、無線ネットワーク内の他のクライアントが使用しているチャネルと一致するように設定する必要があります。

値の範囲：クライアント アダプタの無線および規制地域により異なる
2.4GHz クライアント アダプタでの例
北米では 1 ～ 11（2412 ～ 2462 Megahertz（MHz; メガヘルツ））
5GHz クライアント アダプタでの例
北米では 36、40、44、48、52、56、60、および 64（5180、5200、5220、5240、5260、5280、5300、および 5320 MHz）
デフォルト：クライアント アダプタの無線および規制地域により異なる
2.4GHz クライアント アダプタでの例
北米では 6（2437MHz）
5GHz クライアント アダプタでの例
北米では 36（5180MHz）</td></tr>
</table>

表 4-1　Connection タブのパラメータ（続き）

<table>
<tr><th>パラメータ</th><th>説明</th></tr>
<tr><td>Power Save Mode</td><td>クライアント アダプタを最適な電力消費モードに設定します。

オプション：CAM、Max PSP、Fast PSP
デフォルト：CAM（Constantly Awake Mode）

<table><tr><th>Power Save Mode</th><th>説明</th></tr><tr><td>CAM（Constantly Awake Mode）</td><td>メッセージの応答時間に遅延が発生しないように、クライアント アダプタを常に電源が投入された状態にしておきます。

最も電力を消費しますが、最高のスループットを実現します。このオプションは、デスクトップ コンピュータおよび AC 電源を使用するデバイスにお勧めします。</td></tr><tr><td>Max PSP（Max Power Savings）</td><td>クライアント アダプタ宛ての着信メッセージをアクセス ポイントでバッファリングします。クライアント アダプタは定期的に起動してアクセス ポイントをポーリングし、バッファに待機中のメッセージがないかどうかを確認します。アダプタはそれぞれのメッセージを要求してから、スリープ モードに戻ります。

電力を最も節約できますが、スループットは最も低くなります。このオプションは、電力消費を抑えることが重要なデバイス（バッテリ駆動のデバイスなど）にお勧めします。

（注）　Max PSP モードに設定して ACU を閉じると、次に ACU を起動したときに、「Maximum Power Save mode is temporarily disabled while you are running this application.」というメッセージが表示されます。ACU 起動中は、Fast PSP モードが有効になります。ACU を閉じると、カードは Max PSP モードに戻ります。</td></tr><tr><td>Fast PSP（Power Save Mode）</td><td>ネットワーク トラフィックに応じて、PSP モードと CAM モードを切り替えます。大量のパケットを受信するときは CAM モードに切り替わり、パケットの受信が完了すると PSP モードに戻ります。

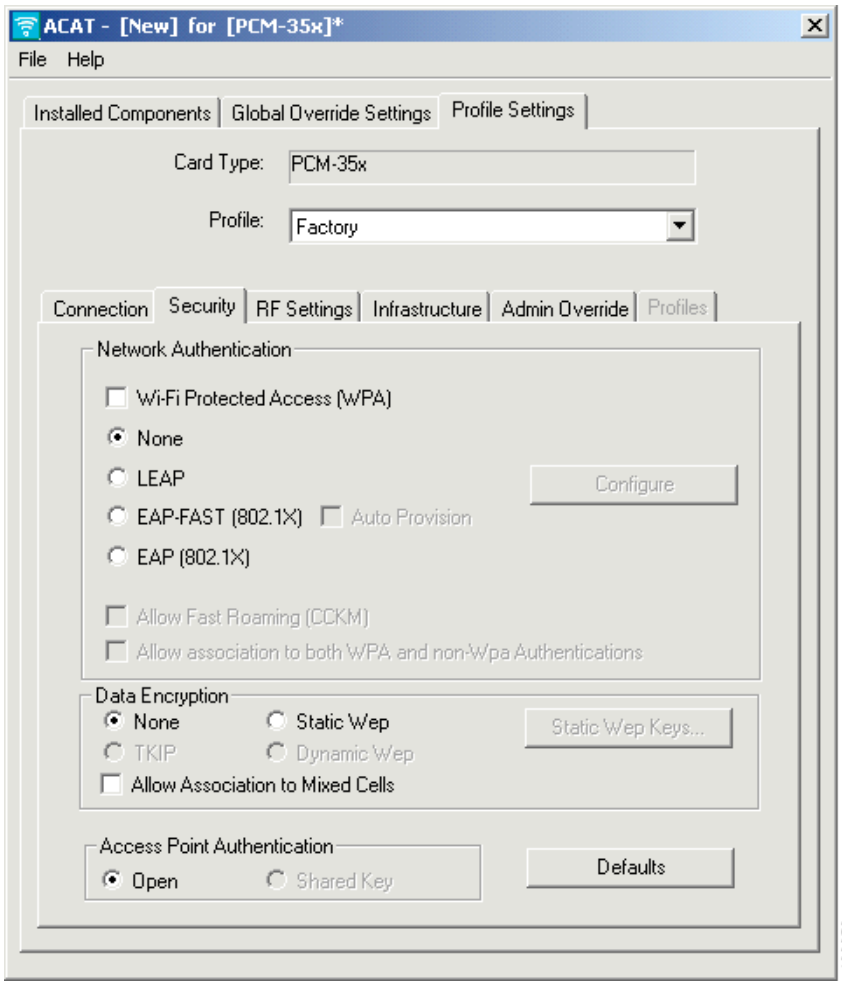
このオプションは、電力消費を抑えつつ、Max PSP モードよりも高いスループットを必要とする場合にお勧めします。</td></tr></table></td></tr>
</table>

Security タブ

Security タブ ウィンドウ（図 4-6 を参照）では、クライアント アダプタのアクセス ポイントとのアソシエート方法、無線ネットワークでの認証方法、データの暗号化および復号化方法を制御するパラメータを設定できます。Security タブ ウィンドウは、次の 3 つのセクションに分かれています。

- Network Authentication：ネットワーク認証オプションを指定します。
- Data Encryption：データ暗号化オプションを指定します。
- Access Point Authentication：アクセス ポイント認証オプションを指定します。

図 4-6　Security タブ ウィンドウ



このウィンドウではセキュリティ機能をいくつか設定できますが、各機能を設定するにはいくつかの手順を実行する必要があります。また、セキュリティ機能自体も複雑なので、設定する前によく理解しておく必要があります。セキュリティ機能の概要は、第 5 章「セキュリティ機能」で説明します。

Network Authentication

Network Authentication セクションでは、使用しているクライアント アダプタで利用できるネットワーク認証オプションを指定します。表 4-2 は、パラメータのオプションを説明しています。

表 4-2　Network Authentication パラメータ

パラメータ	説明
Wi-Fi Protected Access (WPA)	クライアント アダプタで WPA 認証を使用するかどうかを指定します。 （注）　WPA を選択すると、TKIP データ暗号化パラメータが自動的に設定されます。その他のデータ暗号化オプションは使用できません。 （注）　WPA を選択した場合は、LEAP（WPA）認証、EAP-FAST（WPA）認証、または EAP（WPA）認証も選択できます。 **値の範囲**：オンまたはオフ **デフォルト**：オフ
None	このオプションを選択した場合、ネットワーク認証は使用されません。 **値の範囲**：オンまたはオフ **デフォルト**：オン
LEAP	クライアント アダプタで LEAP 認証を使用するかどうかを指定します。 （注）　LEAP を選択すると、動的 WEP データ暗号化オプションが自動的に設定されます。WPA も選択した場合は、TKIP データ暗号化オプションが自動的に設定されます。その他のデータ暗号化オプションは使用できず、Configure ボタンは LEAP 設定の入力用としてアクティブになります。 （注）　WPA を選択すると、このパラメータは LEAP から LEAP（WPA）に変わります。 **値の範囲**：オンまたはオフ **デフォルト**：オフ

表 4-2　Network Authentication パラメータ（続き）

パラメータ	説明
EAP-FAST (802.1X)	クライアント アダプタで EAP-FAST 認証を使用するかどうかを指定します。 （注）　EAP-FAST を選択すると、動的 WEP データ暗号化オプションが自動的に設定され、Configure ボタンは EAP-FAST 設定の入力用としてアクティブになります。WPA も選択した場合は、TKIP データ暗号化オプションが自動的に設定されます。その他のデータ暗号化オプションは使用できません。 （注）　この機能は、350 シリーズまたは CB20A カードとクライアント アダプタを使用する場合にのみ利用できます。 （注）　WPA を選択すると、このパラメータは EAP-FAST（802.1X）から EAP-FAST （WPA）に変わります。 （注）　この機能は、Windows 2000 または Windows XP オペレーティング システムを実行している PC にのみインストールできます。サポート対象でないオペレーティング システムで、EAP-FAST を指定したプロファイルのインストールに失敗しても、Install Wizard からエラー メッセージは返されません。 **値の範囲**：オンまたはオフ **デフォルト**：オフ
Auto Provision	EAP-FAST 認証で、Protected Authentication Credentials（PAC）プロビジョニングに自動的にアクセスするか、手動で指定するかを指定します。 （注）　プロビジョニングは、PAC ファイルを特定のユーザまたはユーザ グループにアソシエートするプロセスです。 （注）　自動プロビジョニングを選択していないときは、ACU を使用してプロビジョニング情報を入力する必要があります。 **値の範囲**：オンまたはオフ **デフォルト**：オフ

表 4-2　Network Authentication パラメータ（続き）

パラメータ	説明
EAP (802.1X)	使用している PC のオペレーティング システムでサポートされている 802.1X 認証をクライアント アダプタで使用するかどうかを指定します。 （注）　WPA を選択すると、このパラメータは EAP （802.1X）から EAP （WPA）に変わります。 **値の範囲：**オンまたはオフ **デフォルト：**オフ
Allow Fast Roaming (CCKM)	いくつかのアクセス ポイントで使用可能な CCKM 機能をクライアント アダプタで使用できるようにするかどうかを指定します。 （注）　このオプションは、LEAP または EAP-FAST が選択されている場合にのみ使用できます。 （注）　このオプションを選択した場合、クライアント アダプタは、CCKM 機能をサポートしているアクセス ポイントに対してのみ CCKM を使用しますが、CCKM をサポートしていないアクセス ポイントにアソシエートすることはできます。 **値の範囲：**オンまたはオフ **デフォルト：**オフ
Allow association to both WPA and non-WPA Authentications	WPA をサポートしているアクセス ポイント、またはサポートしていないアクセス ポイントにクライアント アダプタがアソシエートできるかどうかを指定します。 （注）　このオプションは、WPA が選択されている場合にのみ使用できます。 **値の範囲：**オンまたはオフ **デフォルト：**オフ

Data Encryption

Data Encryption セクションでは、クライアント アダプタで使用する暗号化オプション（表 4-3 を参照）を指定します。

表 4-3　Data Encryption オプション

パラメータ	説明
None	クライアント アダプタでデータ暗号化を使用しないように指定します。 **値の範囲**：オンまたはオフ **デフォルト**：オン
Static WEP	クライアント アダプタで静的 WEP 暗号化を使用するように指定します。 **値の範囲**：オンまたはオフ **デフォルト**：オフ
TKIP	クライアント アダプタで Temporal Key Integrity Protocol（TKIP）を使用するように指定します。 （注）　TKIP は、WPA を選択すると自動的に使用可能になります。 **値の範囲**：オンまたはオフ **デフォルト**：オフ
Dynamic WEP	クライアント アダプタで動的 WEP 暗号化を使用するように指定します。 （注）　動的 WEP は、LEAP または EAP-FAST を選択すると自動的に使用可能になります。 **値の範囲**：オンまたはオフ **デフォルト**：オフ
Allow Association to Mixed Cells	クライアント アダプタが、WEP アソシエーションと非 WEP アソシエーションの両方が有効なアクセス ポイントにアソシエートできるようにするかどうかを指定します。 **値の範囲**：オンまたはオフ **デフォルト**：オフ

Allow Association To Mixed Cells パラメータ

Allow Association To Mixed Cells パラメータは、クライアント アダプタが、WEP 対応と WEP 非対応の両方のアクセス ポイントにアソシエートできるかどうかを示します。このパラメータを設定する際は、次のガイドラインに従ってください。

- クライアント アダプタのアソシエート先のアクセス ポイントで WEP が Optional に設定されており、クライアント アダプタで WEP が有効になっている場合は、**Allow Association To Mixed Cells** チェックボックスをオンにします。そうしないと、クライアントは、アクセス ポイントとの接続を確立できません。
- クライアント アダプタのアソシエート先のアクセス ポイントで WEP が Optional に設定されていない場合は、**Allow Association To Mixed Cells** チェックボックスをオフにします。

（注）　セキュリティ上の理由により、同じセルに WEP 対応クライアントと WEP 非対応クライアントの双方を混在させることはお勧めできません。これは、WEP を使用しているクライアントにも、暗号化されていないブロードキャスト パケットが送信されてしまうためです。

（注）　このパラメータは、アドホック モードでは使用できません。

（注）　WPA を選択した場合は、*Allow association to both WPA and non-WPA Authentications* パラメータも選択しないと、このパラメータを使用できません。

Access Point Authentication

Access Point Authentication セクションでは、クライアント アダプタがアクセス ポイントの認証を受ける方法を指定します。

- **Open Authentication**：WEP の設定に関係なく、クライアント アダプタは、アクセス ポイントにアソシエートし、通信を確立しようとします。Open Authentication はデフォルト設定です。

（注）　クライアント アダプタがデータ フレームを正常に送信できるのは、アクセス ポイントと同じ WEP キーを持っている場合のみです。

- **Shared Key Authentication**：クライアント アダプタが、同じ WEP キーを持つアクセス ポイントとのみ通信できるようにします。

  Shared Key 認証では、アクセス ポイントは既知の暗号化されていない身元証明要求パケットをクライアント アダプタに送信します。クライアント アダプタはそのパケットを暗号化して、アクセス ポイントに返送します。アクセス ポイントは暗号化されたパケットの復号化を試み、その成功または失敗を通知する認証応答パケットをクライアント アダプタに返送します。パケットが正常に暗号化および復号化された場合、ユーザは認証されたと見なされます。

  （注）　共有キー認証にはセキュリティ上のリスクがあるので、使用しないことをお勧めします。

  （注）　共有キー認証は、データ暗号化方式として静的 WEP が選択されている場合にのみ使用できます。

新しい静的 WEP キーの入力

このプロファイルに対して新しい静的 WEP キーを入力する手順は、次のとおりです。

ステップ 1　Security タブ ウィンドウの Network Associations セクションで **None** をオンにします。

ステップ 2　Data Encryption で **Static WEP** をオンにします。

（注）　Security タブ ウィンドウの Network Association セクションで **LEAP** を選択すると、自動的に静的 WEP が無効になり、動的 WEP が有効になります。

ステップ 3　**Static WEP Keys** をクリックすると、WEP Key Setting ウィンドウが表示されます。

ステップ 4　ドロップダウン メニューで、WEP キーの入力方法を次のいずれかから選択します。

- **Hexadecimal** : 0 ～ 9、A ～ F、a ～ f を使用した 16 進文字で WEP キーを入力するように指定します。
- **ASCII Text** : 英数字と句読点を含む ASCII テキストで WEP キーが入力されるよう指定します。

（注）　ASCII テキスト WEP キーは、VxWorks ソフトウェアを実行している Cisco Aironet 1200 シリーズ アクセス ポイントではサポートされていません。したがって、これらのアクセス ポイントでクライアント アダプタを使用する場合は、Hexadecimal（0 ～ 9、A ～ F、a ～ f）オプションを選択してください。

ステップ 5　入力する静的 WEP キー（1、2、3、4）に対し、ドロップダウン メニューから WEP キーのサイズとして 40 ビットまたは 128 ビットを選択します。128 ビットのクライアント アダプタでは 40 ビットまたは 128 ビットのキーが使用できますが、40 ビットのアダプタで使用できるのは 40 ビットのキーだけです。

ステップ 6　システム管理者から静的 WEP キーを入手し、作成するキーの空白フィールドに入力します。新しい静的 WEP キーを入力するには、次のガイドラインに従ってください。

- WEP キーは、次の文字数で構成する必要があります。
  - 40 ビットのキーでは 10 個の 16 進文字または 5 個の ASCII テキスト文字
    例：5A5A313859（16 進文字）または ZZ18Y（ASCII 文字）
  - 128 ビットのキーでは 26 個の 16 進文字または 13 個の ASCII テキスト文字
    例：5A583135333554595549333534（16 進文字）または ZX1535TYUI354（ASCII 文字）
- クライアント アダプタの WEP キーは、インフラストラクチャ モードの場合は通信先のアクセス ポイントと同じキーに、アドホック モードの場合は通信先のクライアントと同じキーに設定する必要があります。
- 複数の WEP キーを設定する場合は、割り当てるキーの WEP キー番号がすべてのデバイスで一致している必要があります。たとえば、WEP キー 2 は、すべてのデバイスで WEP キー番号 2 に割り当てられていなければなりません。複数の WEP キーを設定する場合は、それらのキーがすべてのデバイスで同じ順序になっている必要があります。

ステップ 7　パケットの送信に使用するキーの左側にある **Transmit Key** ボタンをクリックします。送信キーとして選択できる WEP キーは 1 つだけです。

ステップ 8　次に示すアクセス ポイント認証オプションのうちいずれかを選択します。このオプションは、クライアント アダプタがアクセス ポイントに認証を求める方法を定義します。

- **Open** : WEP の設定に関係なく、クライアント アダプタは、アクセス ポイントとの認証を行い、そこと通信しようとします。Open Authentication はデフォルト設定です。
- **Shared Key** : クライアント アダプタが、同じ WEP キーを持つアクセス ポイントとだけ通信できるようにします。このオプションは、静的 WEP が選択されている場合にのみ使用できます。

（注）　Shared Key 認証はセキュリティ上のリスクがあるので、使用しないことをお勧めします。

ステップ 9　**OK** をクリックして Security タブ ウィンドウに戻ります。

（注）　WEP キーを設定すると、新しいキー値を入力できますが、元のキーの表示や削除はできません。

静的 WEP の無効化

特定のプロファイルの静的 WEP を無効にするには、Security タブ ウィンドウの Data Encryption で **None** をオンにします。

（注）　Security タブ ウィンドウの Network Association セクションで **LEAP** を選択すると、自動的に静的 WEP が無効になり、動的 WEP が有効になります。

LEAP の有効化

LEAP 認証を有効にするには、ネットワーク デバイスが次の要件に一致している必要があります。

- クライアント アダプタは、WEP をサポートし、Install Wizard ファイル内のファームウェア、ドライバ、ユーティリティ、およびセキュリティ モジュールを使用する必要があります。
- WPA を使用するには、350 シリーズおよび CB20A クライアント アダプタで、Install Wizard 1.2 以降に付属しているソフトウェアを Windows 2000 または XP オペレーティング システムを実行するコンピュータ上で使用する必要があります。
- LEAP 認証に失敗したアクセスポイントの報告機能と高速ローミング機能を使用するには、クライアント アダプタが、Install Wizard 1.2 以降に含まれているクライアント アダプタ ファームウェアを使用している必要があります。
- クライアント アダプタが認証を試みるアクセス ポイントでは、VxWorks 11.23T 以降（340 および 350 シリーズ アクセス ポイント）、11.54T 以降（1200 シリーズ アクセス ポイント）、または Cisco IOS リリース 12.2(4)JA 以降（1100 シリーズ アクセス ポイント）のソフトウェア リリースを使用している必要があります。

（注）　WPA を使用するには、アクセス ポイントで Cisco IOS リリース 12.2(11)JA 以降を使用している必要があります。LEAP 認証に失敗したアクセス ポイントの報告機能と高速で安全なローミング機能を使用するには、アクセス ポイントが、VxWorks リリース 12.00T（340、350、および 1200 シリーズ アクセス ポイント）、または Cisco IOS リリース 12.2(4)JA（1100 シリーズ アクセス ポイント）を使用している必要があります。

- LEAP 認証に必要なすべてのインフラストラクチャ デバイス（アクセス ポイント、サーバなど）が正しく設定されていなければなりません。

選択したプロファイルに対し LEAP 認証を有効にする手順は次のとおりです。

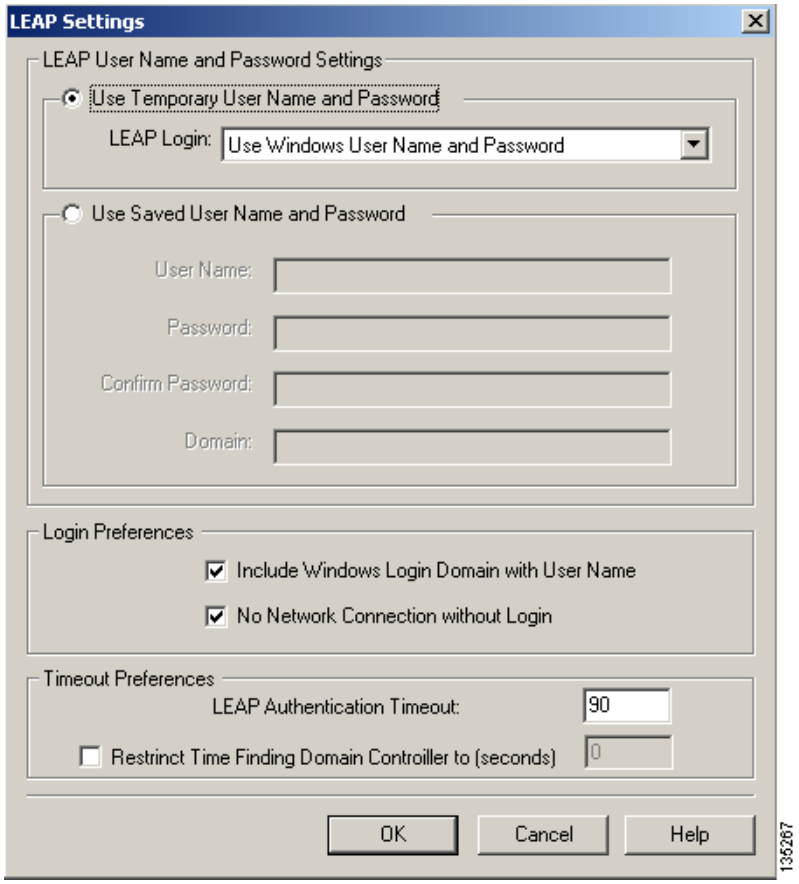
ステップ 1　WPA を有効にする場合は、Security タブ ウィンドウの Network Authentication セクションで **Wi-Fi Protected Access (WPA)** をオンにします。このパラメータを有効にすると、クライアント アダプタは、WPA を使用してアクセス ポイントにアソシエートできるようになります（詳細は、「Wi-Fi Protected Access（WPA）」の項（P. 5-8）を参照）。

ステップ 2　Security タブ ウィンドウの Network Authentication セクションで **LEAP** をオンにします。

（注）　このオプションをオンにすると、動的 WEP が自動的に有効になります。WPA も選択すると、TKIP が有効になります。

ステップ 3　**Configure** をクリックすると、LEAP Settings ウィンドウが表示されます（図 4-7 を参照）。

図 4-7　LEAP Settings ウィンドウ



ステップ 4　次に示す LEAP ユーザ名およびパスワードの設定オプションのいずれかを選択します。

- **Use Temporary User Name and Password**：ユーザはコンピュータを再度ブートするたびに LEAP ユーザ名とパスワードを入力し、ネットワークへのアクセスに対する認証を受ける必要があります。
- **Use Saved User Name and Password**：コンピュータを再度ブートするたびに、ACU によってコンピュータのレジストリに保存された LEAP ユーザ名とパスワードが使用されます。認証は、保存されているユーザ名とパスワード（RADIUS サーバに登録されている）を使用して自動的に行われます。

（注）　このオプションを選択する場合は、PC 上で ACU を使用して LEAP を設定する必要があります。この設定のためには、*Use Saved User Name and Password* オプションを選択し、適切な LEAP ユーザ名とパスワードを入力します。ACAT では、オプション フィールドは使用できません。

（注）　Use Saved User Name and Password オプションを使用できるのは、Installed Components タブで Allow Saved LEAP User Name and Password オプションが有効になっている場合のみです（詳細は、「Installed Components タブ ウィンドウ」の項（P. 2-2）を参照してください）。

ステップ 5　ステップ 4 で Use Temporary User Name and Password を選択した場合は、ドロップダウン メニューを使用して次のいずれかのオプションを選択します。

- **Use Windows User Name and Password**：Windows のユーザ名とパスワードが LEAP のユーザ名とパスワードとしても使用されるので、ユーザは 1 組のクレデンシャルを覚えるだけで済みます。ログイン後、LEAP 認証プロセスが自動的に開始されます。このオプションはデフォルト設定です。
- **Automatically Prompt for LEAP User Name and Password**：通常の Windows ログインとは別の、RADIUS サーバに登録されている LEAP ユーザ名とパスワードを入力して、LEAP 認証プロセスを開始する必要があります。
- **Manually Prompt for LEAP User Name and Password**：ACU Commands ドロップダウン メニューから Manual LEAP Login オプションを使用し、必要に応じて手動で LEAP 認証プロセスを開始する必要があります。Windows のログイン時に LEAP ユーザ名とパスワードの入力は求められません。このオプションは、ソフトウェア トークン ワンタイム パスワード システムなど、ログイン時には使用できない別のソフトウェアを必要とするシステムをサポートするために使用できます。

ステップ 6　別のユーザが自分のクレデンシャルを使用して無線ネットワークにアクセスできないようにするために、ログオフ後、強制的にクライアント アダプタのアソシエーションを解除する場合は、**No Network Connection without Login** チェックボックスをオンにします。デフォルト設定はオフです。

ステップ 7　複数のドメインを使用する環境で作業しており、Windows ログイン ドメインをユーザ名とともに RADIUS サーバに渡す場合は、**Include Windows Login Domain With User Name** チェックボックスをオンにします。デフォルト設定はオフです。

ステップ 8　別のユーザが自分のクレデンシャルを使用して無線ネットワークにアクセスできないようにするために、ログオフ後、強制的にクライアント アダプタのアソシエーションを解除する場合は、**No Network Connection without Login** チェックボックスをオンにします。デフォルト設定はオンです。

ステップ 9　LEAP Authentication Timeout Value フィールドに、LEAP 認証が失敗したと見なされてエラー メッセージが表示されるまでの時間を秒単位で入力します。

値の範囲：45 ～ 300 秒

デフォルト：90 秒

ステップ 10　認証プロセス中にドメイン コントローラの検出所要時間を制限する手順は、次のとおりです。

a. **Restrict Time Finding the Domain Controller to (seconds)** チェックボックスをオンにします。

デフォルト：オフ

b. 認証プロセス中、ドメイン コントローラの検出に掛ける所要時間を秒単位で入力します。ドメイン コントローラの検出は、認証プロセス中最後に行われるシーケンスです。

値の範囲：0 ～ 300 秒

デフォルト：0 秒

（注）　「0」の値を入力すると、認証プロセスで「Finding Domain Controller」手順全体が省略されます。

（注）　ドメイン コントローラ検出のタイムアウト値は、全体的な LEAP 認証タイムアウト値に含まれます。たとえば、認証タイムアウト値が 60 秒でドメイン コントローラの検出タイムアウト値が 10 秒の場合、クライアント アダプタは最大 60 秒間掛けてすべての認証プロセスを完了しますが、そのうちの最大 10 秒間はドメイン コントローラの検出に割り当てられます。

（注）　ログイン スクリプトやローミング デスクトップなどのドメイン サービスが必要な場合は、Restrict Time Finding Domain Controller to (seconds) チェックボックスをオンにしないことをお勧めします。

（注）　チェックボックスのオン / オフ設定にかかわらず、Windows に一度ログインしているか、またはドメインにではなくローカル　マシンにログインしていれば、「Finding Domain Controller」手順は省略されます。

ステップ 11　**OK** をクリックして LEAP Settings ウィンドウを終了し、Security タブ ウィンドウに戻ります。

ステップ 12　クライアント アダプタで高速ローミングを有効にする場合は、Security タブ ウィンドウの Network Authentication セクションで **Allow Fast Roaming （CCKM）**をオンにします。

- このオプションをオンにすると、クライアント アダプタが、CCKM を使用するアクセス ポイントにアソシエートしたときに CCKM を使用できます。このオプションを使用すると、クライアント アダプタは、CCKM を使用しないアクセス ポイントにもアソシエートできます。
- このオプションをオンにしないと、CCKM を使用するアクセス ポイントにアソシエートしても、クライアント アダプタでは CCKM を使用できません。

デフォルト：オフ

（注）　このオプションは、WPA が有効になっている場合にのみ使用できます。

（注）　コンピュータで Microsoft 802.1X サプリカントを使用していて、高速ローミング機能を使用する場合は、Microsoft の資料を参照してください。

ステップ 13　WPA をサポートしているアクセス ポイントだけでなく、サポートしていないアクセス ポイントにもアソシエートする場合は、**Allow Association to both WPA and non-WPA authentication** をオンにします。このオプションをオンにしない場合、クライアント アダプタがアソシエートできるのは、WPA を使用しているアクセス ポイントのみです。

デフォルト：オフ

EAP-FAST の有効化

EAP-FAST 認証を有効にする前に、ネットワーク デバイスが次の要件を満足している必要があります。

- クライアント アダプタは、WEP をサポートし、Install Wizard ファイル内のファームウェア、ドライバ、ユーティリティ、およびセキュリティ モジュールを使用する必要があります。
- 350 シリーズおよび CB20A クライアント アダプタで、Install Wizard 1.3 以降に付属しているソフトウェアを Windows 2000 または XP オペレーティング システムを実行するコンピュータ上で使用する必要があります。
- EAP-FAST　認証に失敗したアクセスポイントの報告機能と高速ローミング機能を使用するには、クライアント アダプタが、Install Wizard 1.3 以降に含まれているクライアント アダプタ ファームウェアを使用している必要があります。
- クライアント アダプタが認証を試みるアクセス ポイントでは、VxWorks 11.23T 以降（340 および 350 シリーズ アクセス ポイント）、11.54T 以降（1200 シリーズ アクセス ポイント）、または Cisco IOS リリース 12.2(4)JA 以降（1100 シリーズ アクセス ポイント）のソフトウェア リリースを使用している必要があります。

（注）　WPA を使用するには、アクセス ポイントで Cisco IOS リリース 12.2(11)JA 以降を使用している必要があります。EAP-FAST 認証に失敗したアクセス ポイントの報告機能と高速で安全なローミング機能を使用するには、アクセス ポイントが、VxWorks リリース 12.00T（340、350、および 1200 シリーズ アクセス ポイント）、または Cisco IOS リリース 12.2(4)JA（1100 シリーズ アクセス ポイント）を使用している必要があります。

- EAP-FAST 認証に必要なすべてのインフラストラクチャ デバイス（アクセス ポイント、サーバなど）が正しく設定されていなければなりません。

選択したプロファイルに対して EAP-FAST 認証を有効にする手順は、次のとおりです。

ステップ 1　WPA を有効にする場合は、Security タブ ウィンドウの Network Authentication セクションで **Wi-Fi Protected Access (WPA)** をオンにします。このパラメータを有効にすると、クライアント アダプタは、WPA を使用してアクセス ポイントにアソシエートできるようになります（詳細は、「Wi-Fi Protected Access（WPA）」の項（P. 5-8）を参照してください）。

ステップ 2　Security タブ ウィンドウの Network Authentication セクションで **EAP-FAST** をオンにします。

（注）　このオプションをオンにすると、動的 WEP が自動的に有効になります。WPA も選択すると、TKIP が有効になります。

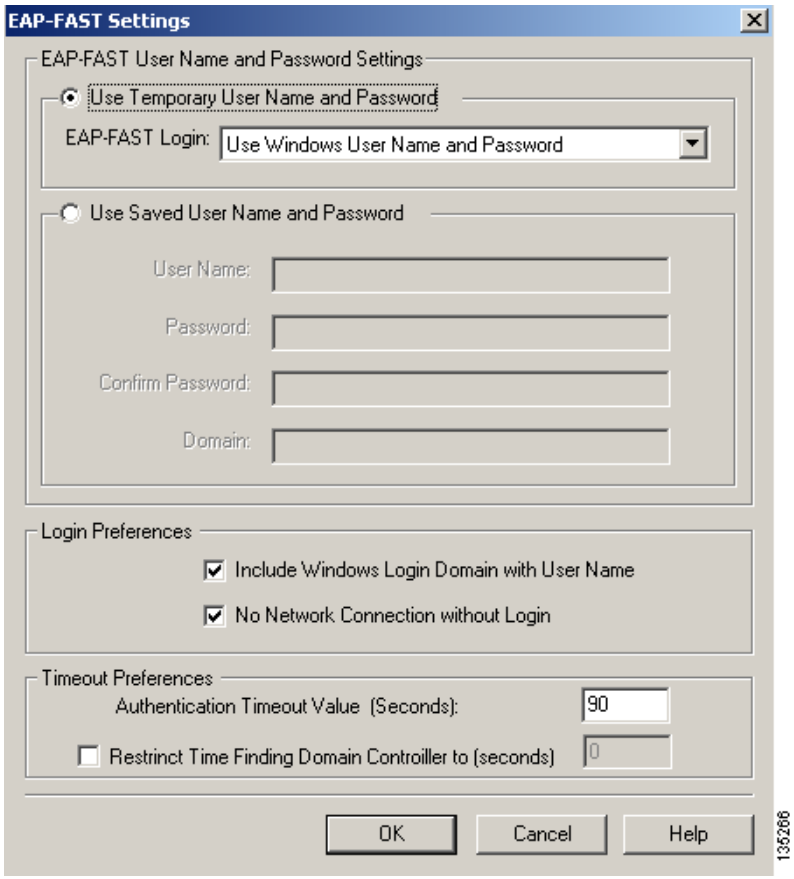
ステップ 3　**Auto Provision** をオンにすると、EAP-FAST プロトコルによって EAP-FAST サーバにユーザ名とパスワードが送信され、自動的に PAC プロビジョニングを取得できるようになります。

（注）　Auto Provision オプションは、Installed Components タブで Allow Auto Provisioning オプションが有効になっている場合にのみ使用できます（詳細は「Installed Components タブ ウィンドウ」の項（P. 2-2）を参照してください）。

（注）　Auto Provision オプションがオフの場合は、ACU を使用して、このプロファイルの PAC を手動で設定する必要があります。

ステップ 4　**Configure** をクリックすると、EAP-FAST Settings ウィンドウが表示されます（図 4-8 を参照してください）。

図 4-8　EAP-FAST Settings ウィンドウ



ステップ 5　次に示す EAP-FAST ユーザ名とパスワードの設定オプションのいずれかをオンにします。

- **Use Temporary User Name and Password**：ユーザはコンピュータを再度ブートするたびに EAP-FAST ユーザ名とパスワードを入力し、ネットワークへのアクセスに対する認証を受ける必要があります。このオプションはデフォルト設定です。
- **Use Saved User Name and Password**：コンピュータを再度ブートするたびに、ACU によってコンピュータのレジストリに保存された EAP-FAST ユーザ名とパスワードが使用されます。認証は、保存されているユーザ名とパスワード（EAP-FAST サーバに登録されている）を使用して自動的に行われます。

（注）　このオプションを選択する場合は、ACU を使用して EAP-FAST を設定する必要があります。この設定のためには、*Use Saved User Name and Password* オプションを選択し、適切な EAP-FAST ユーザ名とパスワードを入力します。ACAT では、オプション フィールドは使用できません。

（注）　Use Saved User Name and Password オプションを使用できるのは、Installed Components タブで Allow Saved EAP-FAST User Name and Password オプションが有効になっている場合のみです（詳細は「Installed Components タブ ウィンドウ」の項（P. 2-2）を参照してください）。

ステップ 6　ステップ 4 で Use Temporary User Name and Password を選択した場合は、ドロップダウン メニューを使用して次のいずれかのオプションを選択します。

- **Use Windows User Name and Password** : Windows のユーザ名とパスワードが EAP-FAST のユーザ名とパスワードとしても使用されるので、ユーザは 1 組のクレデンシャルを覚えるだけで済みます。ログイン後、LEAP 認証プロセスが自動的に開始されます。このオプションはデフォルト設定です。
- **Automatically Prompt for User Name and Password** : 通常の Windows ログインとは別の EAP-FAST ユーザ名とパスワード（EAP-FAST サーバに登録されている）を入力し、EAP-FAST 認証プロセスを開始する必要があります。
- **Manually Prompt for User Name and Password** : ACU Commands ドロップダウン メニューから Manual EAP-FAST Login オプションを使用して、必要に応じて手動で EAP-FAST 認証プロセスを開始する必要があります。Windows のログイン時に EAP-FAST ユーザ名とパスワードの入力は求められません。このオプションは、ソフトウェア トークン ワンタイム パスワード システムなど、ログイン時には使用できない別のソフトウェアを必要とするシステムをサポートするために使用できます。

ステップ 7　別のユーザが自分のクレデンシャルを使用して無線ネットワークにアクセスできないようにするために、ログオフ後、強制的にクライアント アダプタのアソシエーションを解除する場合は、**No Network Connection without Login** チェックボックスをオンにします。デフォルト設定はオフです。

ステップ 8　複数のドメインを使用する環境で作業しており、Windows ログイン ドメインをユーザ名とともに EAP-FAST サーバに渡す必要がある場合は、**Include Windows Login Domain With User Name** チェックボックスをオンにします。デフォルト設定はオフです。

ステップ 9　別のユーザが自分のクレデンシャルを使用して無線ネットワークにアクセスできないようにするために、ログオフ後、強制的にクライアント アダプタのアソシエーションを解除する場合は、**No Network Connection without Login** チェックボックスをオンにします。デフォルト設定はオンです。

ステップ 10　Authentication Timeout Value フィールドに、EAP-FAST 認証が失敗したと見なされてエラー メッセージが表示されるまでの時間を秒単位で入力します。

値の範囲：45 ～ 300 秒

デフォルト：90 秒

ステップ 11　認証プロセス中にドメイン コントローラの検出所要時間を制限する手順は、次のとおりです。

a. **Restrict Time Finding the Domain Controller to (seconds)** チェックボックスをオンにします。

   デフォルト：オフ

b. 認証プロセス中、ドメイン コントローラの検出に掛ける所要時間を秒単位で入力します。ドメイン コントローラの検出は、認証プロセス中最後に行われるシーケンスです。

   値の範囲：0 ～ 300 秒

   デフォルト：0 秒

（注）　「0」の値を入力すると、認証プロセスで「Finding Domain Controller」手順全体が省略されます。

（注）　ドメイン コントローラ検出のタイムアウト値は、全体的な EAP-FAST 認証タイムアウト値に含まれます。たとえば、認証タイムアウト値が 60 秒でドメイン コントローラの検出タイムアウト値が 10 秒の場合、クライアント アダプタは最大 60 秒間掛けてすべての認証プロセスを完了しますが、そのうちの最大 10 秒間はドメイン コントローラの検出に割り当てられます。

（注）　ログイン スクリプトやローミング デスクトップなどのドメイン サービスが必要な場合は、Restrict Time Finding Domain Controller to (seconds) チェックボックスをオンにしないことをお勧めします。

（注）　チェックボックスのオン / オフ設定にかかわらず、Windows に一度ログインしているか、またはドメインにではなくローカル　マシンにログインしていれば、「Finding　Domain Controller」手順は省略されます。

ステップ 12　**OK** をクリックして EAP-FAST Settings ウィンドウを終了し、Security タブ ウィンドウに戻ります。

ステップ 13　クライアント アダプタで高速ローミングを有効にする場合は、Security タブ ウィンドウの Network Authentication セクションで **Allow Fast Roaming （CCKM）**をオンにします。

- このオプションをオンにすると、クライアント アダプタが、CCKM を使用するアクセス ポイントにアソシエートしたときに CCKM を使用できます。このオプションを使用すると、クライアント アダプタは、CCKM を使用しないアクセス ポイントにもアソシエートできます。
- このオプションをオンにしないと、CCKM を使用するアクセス ポイントにアソシエートしても、クライアント アダプタでは CCKM を使用できません。

デフォルト：オフ

（注）　このオプションは、WPA が有効になっている場合にのみ使用できます。

（注）　コンピュータで Microsoft 802.1X サプリカントを使用していて、高速ローミング機能を使用する場合は、Microsoft の資料を参照してください。

ステップ 14　WPA をサポートしているアクセス ポイントだけでなく、サポートしていないアクセス ポイントにもアソシエートする場合は、**Allow Association to both WPA and non-WPA authentication** をオンにします。このオプションをオンにしない場合、クライアント アダプタがアソシエートできるのは、WPA を使用しているアクセス ポイントのみです。

デフォルト：オフ

ホストベース EAP の有効化

ホストベース EAP を有効にする前に、ネットワーク デバイスが次の要件に一致していなければなりません。

- EAP 認証をサポートしているのは、VxWorks リリース 11.06 以降を実行している 340 シリーズおよび 350 シリーズ アクセス ポイント、VxWorks リリース 11.40T 以降を実行している 1200 シリーズ アクセス ポイント、または 1100 シリーズ アクセス ポイントのみです。
- MIC、TKIP、PEAP、ブロードキャスト キー ローテーション、および EAP-SIM 認証をサポートしているのは、VxWorks リリース 11.23T 以降を実行している 340 シリーズおよび 350 シリーズ アクセス ポイント、VxWorks リリース 11.54T 以降を実行している 1200 シリーズ アクセス ポイント、または 1100 シリーズ アクセス ポイントのみです。
- Windows を実行している、ユーザの PC に Microsoft 802.1X サプリカントをインストールしておく必要があります。
- WPA または WPA-PSK を使用するには、Windows 2000 または XP を実行するコンピュータ上で、350 シリーズまたは CB20A クライアント アダプタを Install Wizard 1.2 以降に付属のソフトウェアとともに使用する必要があります。また、次のいずれかのホスト サプリカントをインストールしておく必要もあります。これらのサプリカントは次のサイトからダウンロードできます。
  - Funk Odyssey Client サプリカント リリース 2.2（Windows 2000 の場合）
    http://www.funk.com/radius/wlan/wlan_c_radius.asp
  - Windows XP Service Pack 1 および Microsoft サプリカント Q815485（Windows XP 用）
    http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp
    http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&DisplayLang=en

（注）　WPA を使用するには、アクセス ポイントで Cisco IOS リリース 12.2(11)JA 以降を使用している必要があります。

（注）　Microsoft Windows PC で WPA または WPA-PSK を設定する方法の詳細は、Microsoft の資料および Cisco Aironet 350/CB20A ワイヤレス LAN クライアント アダプタ インストレーション コンフィギュレーション ガイド Windows 版を参照してください。

- クライアントで有効にする予定の認証タイプに対しては、すべての必要なインフラストラクチャ デバイス（アクセス ポイント、サーバ、ゲートウェイ、ユーザ データベースなど）を正しく設定する必要があります。

このプロファイルに対して該当のホストベース EAP 認証（EAP-TLS、PEAP、または EAP-SIM）を有効にする手順は、次のとおりです。

（注）　EAP-TLS、PEAP、および EAP-SIM 認証は、オペレーティング システムでは有効、ACU では無効になっているので、ACU でプロファイルを切り替えることによってこれらの認証タイプを切り替えることはできません。ホストベース EAP を使用するプロファイルを作成できますが、Windows で特定の認証タイプを有効にする必要があります（Windows で Microsoft 802.1X サプリカントが使用されている場合）。また、Windows で一度に設定できるのは、1 つの認証タイプだけです。ホストベース EAP を使用するプロファイルが複数ある場合に別の認証タイプを使用するには、ACU でプロファイルを切り替えた後、Windows で認証タイプを変更する必要があります。

ステップ 1　WPA を有効にする場合は、Security タブ ウィンドウの Network Authentication で、**Wi-Fi Protected Access (WPA)** をオンにします。このパラメータを有効にすると、クライアント アダプタは、WPA を使用するアクセス ポイントにアソシエートできます。

ステップ 2　Security タブ ウィンドウの Network Authentication で **Host Based EAP** をオンにします。

ステップ 3　動的 WEP キーは、アクセス ポイントに EAP-TLS、PEAP、および EAP-SIM 認証を設定する場合に使用します。WPA が無効になっている場合は、**Dynamic WEP** をクリックします。

（注）　Windows 2000 または XP を実行している PC を設定する方法の詳細は、Microsoft の資料および『Cisco Aironet 350/CB20A ワイヤレス LAN クライアント アダプタ インストレーション コンフィギュレーション ガイド Windows 版』を参照してください。

RF Settings タブ

RF Settings タブ ウィンドウ（図 4-9 を参照）では、クライアント アダプタのデータの送受信方法とタイミングを制御するパラメータを設定できます。

図 4-9　RF Settings タブ ウィンドウ

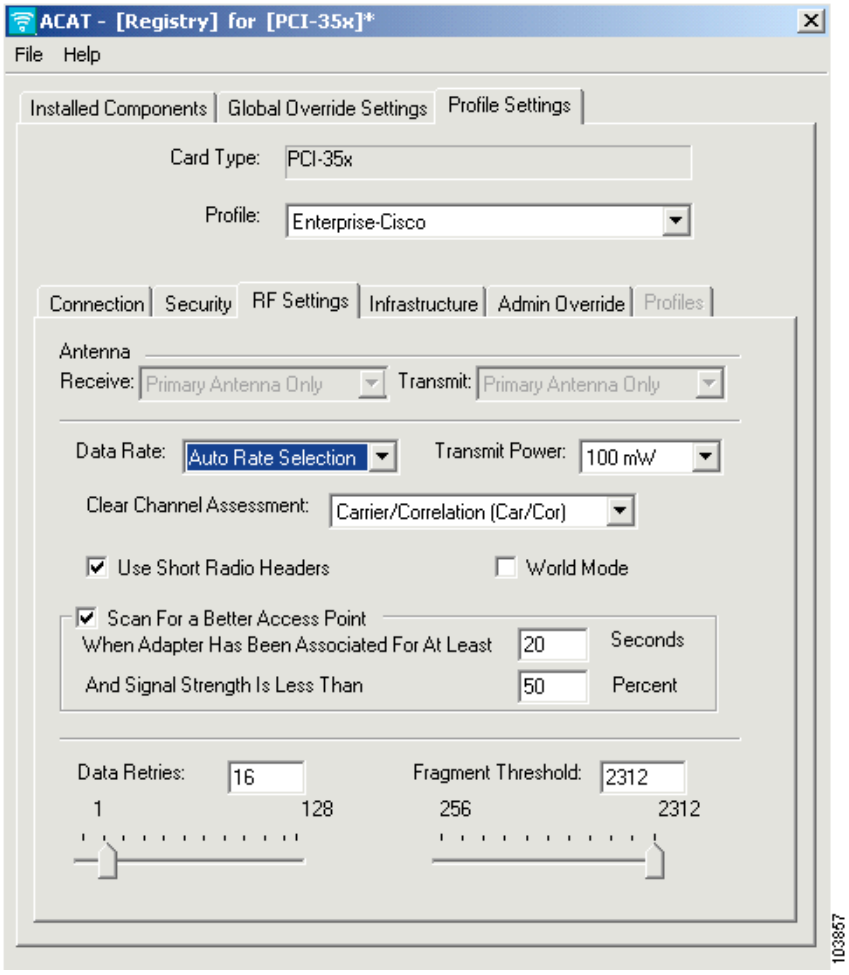


表 4-4 は、クライアント アダプタの Radio Frequency（RF; 無線周波数）ネットワーク パラメータとその説明を示しています。パラメータを変更する場合は、表の指示に従ってください。

表 4-4　RF ネットワーク パラメータ

パラメータ	説明
Antenna（Receive）	クライアント アダプタがデータの受信に使用するアンテナを指定します。 • PCM and CB20A cards：内蔵の常設アンテナは、ダイバーシティ モードで使用する場合に最高の性能を発揮します。ダイバーシティ モードにすると、カードの 2 つのアンテナ ポートのうち、状態の良い方の信号が使用されます。 **オプション：** Diversity (Both)、Primary Antenna Only、Secondary Antenna Only **デフォルト：** Diversity (Both) • PCI card：PCI カードは、Primary Antenna Only オプションを使用する必要があります。 **デフォルト：** Primary Antenna Only • MPI card：1 つまたは 2 つのアンテナで使用できる mini-PCI カードは、ダイバーシティ モードで使用する場合に最高の性能を発揮します。ダイバーシティ モードにすると、カードの 2 つのアンテナ コネクタのうち、状態の良い方の信号が使用されます。 **オプション：** Diversity (Both)、Primary Antenna Only、Secondary Antenna Only **デフォルト：** Diversity (Both) （注）　このパラメータは 2.4GHz クライアント アダプタだけで利用可能です。
Antenna（Transmit）	クライアント アダプタがデータの送信に使用するアンテナを指定します。クライアント アダプタに使用できるオプションは、上記の Antenna（Receive）パラメータを参照してください。 （注）　このパラメータは 2.4GHz クライアント アダプタだけで利用可能です。

表 4-4　RF ネットワーク パラメータ（続き）

<table>
<tr><th>パラメータ</th><th>説明</th></tr>
<tr><td>Data Rate</td><td>
クライアント アダプタがアクセス ポイント（インフラストラクチャ モードの場合）または他のクライアント（アドホック モードの場合）との間でパケットを送受信する速度を指定します。

インフラストラクチャ モードの場合は Auto Rate Selection を選択し、アドホック モードの場合は特定のデータ レートを設定することをお勧めします。

オプション：Auto Rate Selection、1Mbps Only、2Mbps Only、5.5Mbps Only、11Mbps Only（2.4GHz クライアント アダプタ）
Auto Rate Selection、6Mbps Only、9Mbps Only、12Mbps Only、18Mbps Only、24Mbps Only、36Mbps Only、48Mbps Only、または 54Mbps Only（5GHz クライアント アダプタ）

デフォルト：Auto Rate Selection
<table>
<tr><th colspan="2">データ レート</th><th rowspan="2">説明</th></tr>
<tr><th>2.4GHz クライアント アダプタ</th><th>5GHz クライアント アダプタ</th></tr>
<tr><td>Auto Rate Selection</td><td>Auto Rate Selection</td><td>可能な場合は 11 Megabits per second（Mbps; メガビット / 秒）（2.4GHz クライアント アダプタの場合）または 54Mbps（5GHz クライアント アダプタの場合）のデータ転送を行いますが、必要に応じてデータ レートを下げます。</td></tr>
<tr><td>1Mbps Only</td><td>6Mbps Only</td><td>無線範囲は最大ですが、スループットは最も低くなります。</td></tr>
<tr><td>2Mbps Only および 5.5Mbps Only</td><td>9Mbps Only から 48Mbps Only</td><td>1Mbps Only（2.4GHz クライアント アダプタの場合）または 6Mbps Only（5GHz クライアント アダプタの場合）オプションよりも通信範囲はやや狭くなりますが、スループットは高くなります。</td></tr>
<tr><td>11Mbps Only</td><td>54Mbps Only</td><td>スループットは最大ですが、無線範囲は最も狭くなります。</td></tr>
</table>

（注）　クライアント アダプタのデータ レートは、Auto Rate Selection に設定するか、通信先のアクセス ポイントと同じレート（インフラストラクチャ モードの場合）または他のクライアントと同じレート（アドホック モードの場合）にする必要があります。そうでない場合、クライアント アダプタが通信先とアソシエートできない可能性があります。
</td></tr>
</table>

表 4-4　RF ネットワーク パラメータ（続き）

<table>
<tr><th>パラメータ</th><th>説明</th></tr>
<tr><td>Transmit Power</td><td>クライアント アダプタの送信時の電力レベルを定義します。この値を、各国の規制機関（米国では FCC、カナダでは DOC、ヨーロッパでは European Telecommunication Standards Institute（ETSI; 欧州通信規格協会）、日本では MKK）で許可されている値より高くすることはできません。

オプション：クライアント アダプタにプログラミングされている電力テーブルによる（下記の表を参照）

デフォルト：クライアント　アダプタにプログラミングされているレベルのうち、アダプタを使用する国の規制当局で許可される最大レベル

<table>
<tr><th>使用可能な電力レベル</th><th>クライアント アダプタのタイプ</th></tr>
<tr><td>100mW、50mW、30mW、20mW、5mW、または 1mW</td><td>350 シリーズ クライアント アダプタ</td></tr>
<tr><td>20mW、10mW、または 5mW</td><td>PC Cardbus カード（5GHz クライアント アダプタ）</td></tr>
</table>

（注）　送信電力レベルを下げると、バッテリの電力を節約できますが、無線範囲が狭まります。

（注）　World Mode を有効にした場合は、クライアント アダプタを使用する国の規制機関で許可されている最大送信電力レベルだけが利用可能になります。

（注）　旧バージョンの 350 シリーズ クライアント アダプタを使用している場合は、電力レベルがここに記載されているものと異なる場合があります。</td></tr>
</table>

表 4-4　RF ネットワーク パラメータ（続き）

<table>
<tr><th>パラメータ</th><th>説明</th></tr>
<tr><td>Clear Channel Assessment</td><td>クライアント アダプタが動作するチャネルに輻輳が発生していないかどうかをデータの転送前に判断する手段を指定します。

オプション：Firmware Default (xxx)、Carrier/Correlation (Car/Cor)、Energy Detect (ED)、または ED or Car/Cor

デフォルト：Firmware Default (xxx)

<table>
<tr><th>方法</th><th>説明</th></tr>
<tr><td>Firmware Default (xxx)</td><td>Clear Channel Assessment（CCA）機構では、クライアント アダプタのファームウェアのデフォルト値に基づいてチャネルの混雑が報告されます。ファームウェアの CCA デフォルト値は、括弧内に示されます。

（注）　PCM、LMC、PCI カード ファームウェアの CCA デフォルト xxx 値は Car/Cor、mini-PCI カード ファームウェアのデフォルト値は ED です。</td></tr>
<tr><td>Carrier/Correlation（Car/Cor）</td><td>CCA 機構では、Direct-Sequence Spread Spectrum（DSSS; ダイレクトシーケンススペクトラム拡散方式）信号の検出時にチャネルの混雑が報告されます。この信号は ED しきい値を上回ることも下回ることもあります。</td></tr>
<tr><td>Energy Detect（ED）</td><td>CCA 機構では、ED しきい値を上回るエネルギーの検出時にチャネルの混雑が報告されます。</td></tr>
<tr><td>ED or Car/Cor</td><td>CCA 機構では、DSSS 信号または ED しきい値を上回るエネルギーの検出時にチャネルの混雑が報告されます。</td></tr>
</table>
（注）　このパラメータは 2.4GHz クライアント アダプタだけで利用可能です。</td></tr>
</table>

表 4-4　RF ネットワーク パラメータ（続き）

パラメータ	説明
Use Short Radio Headers	このチェックボックスをオンにすると、クライアント アダプタが短い無線ヘッダーを使用するように設定されます。ただし、アダプタが短い無線ヘッダーを使用できるのは、アクセス ポイントもそれらをサポートするように設定され、使用している場合だけです。アクセス ポイントにアソシエートするクライアントのいずれかが長いヘッダーを使用している場合は、クライアントとアクセス ポイントの両方で短い無線ヘッダーが使用可能になっていても、そのセル内の *すべての*クライアントが長いヘッダーを使用する必要があります。 短い無線ヘッダーを使用するとスループットの効率が高まり、長い無線ヘッダーを使用すると、短い無線ヘッダーに対応していないクライアントやアクセス ポイントとの互換性が確保されます。 **デフォルト：**オン （注）　このパラメータは、インフラストラクチャ モードの 2.4GHz クライアント アダプタのみで利用可能です。 （注）　このパラメータを、アクセス ポイント ウィンドウの *プリアンブル* といいます。
World Mode	アソシエート先のアクセス ポイントもワールド モードに設定されていれば、このチェックボックスをオンにすることによって、そのアクセス ポイントの最大送信電力レベルおよび周波数範囲をクライアント アダプタで受け入れることが可能になります。このパラメータは、海外出張の多いユーザが、異なる規制地域のアクセス ポイントにクライアント アダプタをアソシエートできるようにするためのもので、インフラストラクチャ モードでしか使用できません。 **デフォルト：**オフ （注）　このパラメータは 2.4GHz クライアント アダプタだけで利用可能です。 （注）　World Mode を有効にした場合は、クライアント アダプタを使用する国の規制機関で許可されている最大送信電力レベルだけが利用可能になります。

表 4-4　RF ネットワーク パラメータ（続き）

パラメータ	説明
Periodically Scan For a Better Access Point	このチェックボックスをオンにすると、アソシエートしているアクセス ポイントで指定時間が経過した後の信号強度が指定値より低い場合、クライアント アダプタは、より適したアクセス ポイントを探し、それを見つけた場合はアソシエートを切り替えます。 **例：**20 秒と 50% というデフォルト値が使用されている場合、クライアント アダプタは、アソシエート後 20 秒で、アソシエートしているアクセス ポイントから受信した信号強度の監視を開始します。監視は 1 秒あたり 1 回の頻度で続けられます。クライアントが 50% を下回る信号強度を検出すると、より適したアクセス ポイントをスキャンします。 **値の範囲：**5 ～ 255 秒、0 から 75% の信号強度 **デフォルト：**オン、20 秒、50 % の信号強度
Data Retries	最初の送信が失敗した場合に、パケットが再送信される回数を指定します。 **値の範囲：**1 ～ 128 **デフォルト：**16（2.4GHz クライアント アダプタの場合）または 32（5GHz クライアント アダプタの場合） **（注）** ネットワーク プロトコルに独自の再試行回数が設定されている場合は、このパラメータをデフォルト値より小さい値に設定してください。これにより、不良パケットの通知がプロトコル スタックに速やかに送信されるため、アプリケーションで必要に応じてパケットを再送信できます。
Fragment Threshold	RF データ パケットを分割（断片化）するしきい値を定義します。断片化されたパケットの 1 つが送信中に干渉を受けた場合は、そのパケットを再送するだけで済みます。 断片化されたパケットでは、固定パケット オーバーヘッドによって RF 帯域幅が大量に消費されるため、一般にスループットは低くなります。 **値の範囲：**256 ～ 2312 **デフォルト：**2312

Infrastructure タブ

Infrastructure タブ ウィンドウ（図 4-10 を参照）では、インフラストラクチャ ネットワークでのクライアント アダプタの動作を制御するパラメータを設定できます。

（注）　インフラストラクチャ パラメータを設定できるのは、クライアント アダプタをインフラストラクチャ ネットワークで動作するように設定している場合のみです。表 4-1 の Network Type パラメータを参照してください。

図 4-10　Infrastructure タブ ウィンドウ

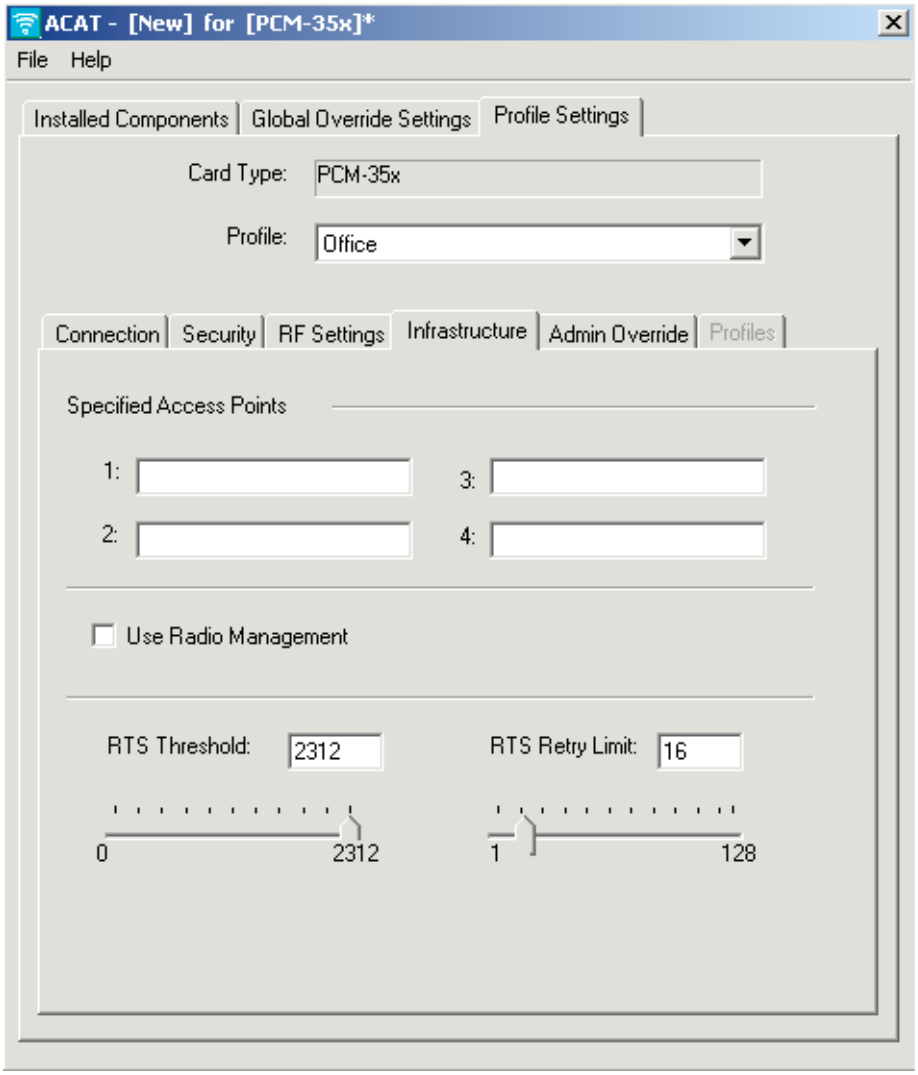


表 4-5 は、クライアント アダプタのインフラストラクチャ パラメータとその説明を示しています。パラメータを変更する場合は、表の指示に従ってください。

表 4-5　Infrastructure タブのパラメータ

パラメータ	説明
Specified Access Points 1-4	クライアント アダプタがアソシエート可能な最大 4 個のアクセス ポイントの Media Access Control（MAC; メディア アクセス制御）アドレスを指定します。指定したアクセス ポイントが見つからない場合やクライアント アダプタが無線範囲外にローミングした場合、アダプタは別のアクセス ポイントにアソシエートすることがあります。 編集ボックスにアクセス ポイントの MAC アドレスを入力します。また、ボックスを空白にしたままアクセス ポイントを指定しないことも可能です。 **デフォルト：**空白 （注）　このパラメータは、リピータ モードのアクセス ポイントだけに使用します。アクセス ポイントを指定するとローミング プロセスの速度が遅くなるので、通常の操作ではこのフィールドをブランクのままにしておいてください。
Use Radio Management	このパラメータをオンにすると、クライアント アダプタがアソシエートされているアクセス ポイントで無線管理（RM）が有効になっていれば、そのアクセス ポイントで RM を制御できます。RM は、複数のインフラストラクチャ ノードを含むシステム全体にかかわる機能です。アクセス ポイントの RM 機能は、他のネットワーク デバイスからの無線計測要求に応答して動作します。この無線計測要求は、アクセス ポイントやそれにアソシエートされているクライアント アダプタに対して、所定の無線計測を行い、その結果を報告することを指示するものです。 （注）　このパラメータは、Install Wizard バージョン 1.2 以降を 350 シリーズのクライアント アダプタで使用した場合にのみ利用できます。 （注）　アクセス ポイントでは、Cisco IOS リリース 12.2(13)JA 以降を使用して RM を有効化している必要があります。この機能を有効にする手順は、アクセス ポイントの資料を参照してください。 **値の範囲：**有効または無効 **デフォルト：**無効

表 4-5　Infrastructure タブのパラメータ（続き）

パラメータ	説明
RTS Threshold	低レベルの RF プロトコルが request-to-send（RTS; 送信要求）パケットを発行する際のデータ パケットのサイズを指定します。 このパラメータを小さい値に設定すると、RTS パケットが頻繁に送信されるようになります。このような場合は、使用可能な帯域幅の消費量が増え、他のネットワーク パケットのスループットが低下します。ただし、障害物や金属面の多い高マルチパス環境で発生する妨害や衝突に対しては、システムは素早く復旧できます。 **値の範囲**：0 ～ 2312 **デフォルト**：2312 （注）　RTS および CTS のメカニズムの詳細は、IEEE 802.11 規格を参照してください。
RTS Retry Limit	クライアント アダプタが、前回送信した RTS パケットに対する clear-to-send（CTS; 送信クリア）パケットを受信しなかった場合に、RTS パケットを再送信する回数を指定します。 このパラメータを大きな値に設定すると、妨害が生じたときに使用可能な帯域幅が減少します。ただし、障害物や金属面の多い高マルチパス環境で発生する妨害や衝突に対しては、システムは強くなります。 **値の範囲**：1 ～ 128 **デフォルト**：16（2.4GHz クライアント アダプタの場合）または 32（5GHz クライアント アダプタの場合） （注）　RTS および CTS のメカニズムの詳細は、IEEE 802.11 規格を参照してください。

Ad Hoc タブ

Ad Hoc タブ ウィンドウ（図 4-11 を参照）では、アドホック ネットワークでのクライアント アダプタの動作を制御するパラメータを設定できます。

（注）　アドホック パラメータを設定できるのは、クライアント アダプタをアドホック ネットワークで動作するように設定している場合のみです。表 4-1 の Network Type パラメータを参照してください。

図 4-11　Ad Hoc タブ ウィンドウ

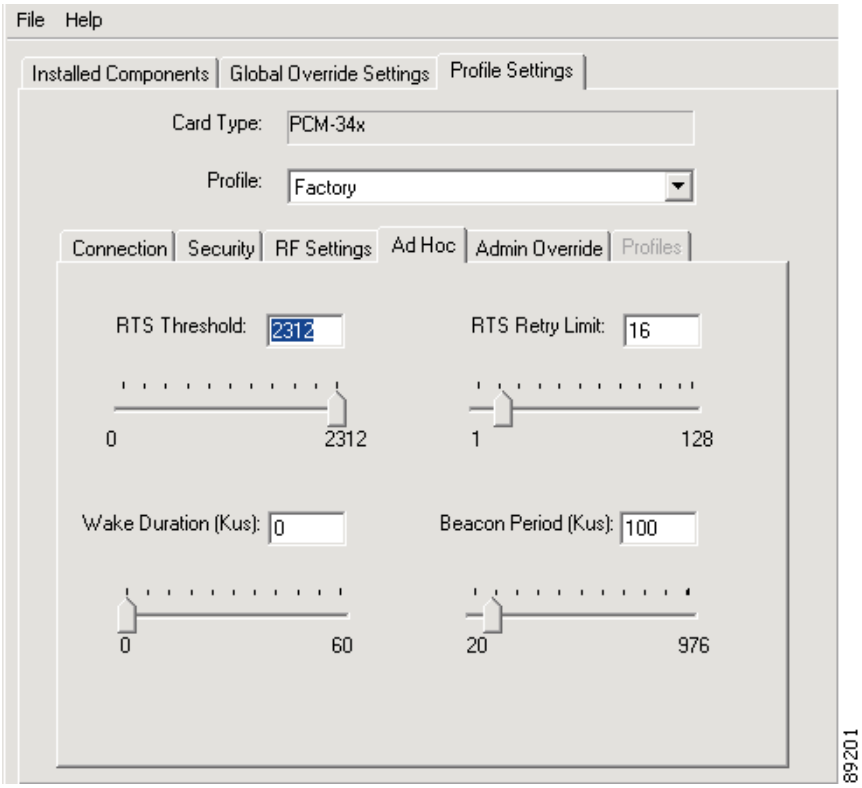


表 4-6 は、クライアント アダプタの拡張アドホック パラメータとその説明を示しています。パラメータを変更する場合は、この表の指示に従ってください。

表 4-6　Ad Hoc タブのパラメータ

パラメータ	説明
RTS Threshold	低レベルの RF プロトコルが request-to-send（RTS; 送信要求）パケットを発行する際のデータ パケットのサイズを指定します。 このパラメータを小さい値に設定すると、RTS パケットが頻繁に送信されるようになります。このような場合は、使用可能な帯域幅の消費量が増え、他のネットワーク パケットのスループットが低下します。ただし、障害物や金属面の多い高マルチパス環境で発生する妨害や衝突に対しては、システムは素早く復旧できます。 **値の範囲**：0 ～ 2312 **デフォルト**：2312 （注）　RTS および CTS のメカニズムの詳細は、IEEE 802.11 規格を参照してください。
RTS Retry Limit	クライアント アダプタが、前回送信した RTS パケットに対する clear-to-send（CTS; 送信クリア）パケットを受信しなかった場合に、RTS パケットを再送信する回数を指定します。 このパラメータを大きな値に設定すると、妨害が生じたときに使用可能な帯域幅が減少します。ただし、障害物や金属面の多い高マルチパス環境で発生する妨害や衝突に対しては、システムは強くなります。 **値の範囲**：1 ～ 128 **デフォルト**：16（2.4GHz クライアント アダプタの場合）または 32（5GHz クライアント アダプタの場合） （注）　RTS および CTS のメカニズムの詳細は、IEEE 802.11 規格を参照してください。

表 4-6　Ad Hoc タブのパラメータ（続き）

パラメータ	説明
Wake Duration (Kms)	ビーコンの後、クライアント アダプタが Announcement Traffic Indication Message（ATIM）パケットを受信するためにアクティブ状態を保持する時間を指定します。ATIM パケットは、アダプタを次のビーコンまでアクティブにしておくために送信されるメッセージです。 表 4-1 の Power Save Mode パラメータを参照してください。 **値の範囲：** 0Kμs（CAM モード時）、5 ～ 60Kμs（Max PSP または Fast PSP モード時） **デフォルト：**0Kμs （注）　クライアント アダプタが CAM モードに設定されている場合は、Wake Duration を 0Kμs に設定する必要があります。クライアント アダプタが Max PSP または Fast PSP モードの場合は、Wake Duration を最低 5Kμs に設定する必要があります。 （注）　Kms は単位を表すソフトウェア用語です。K = 1024、μ = 10^{-6}、s = 秒を表します。したがって、Kμs は 0.001024 秒、1.024 ミリ秒、または 1024 マイクロ秒に相当します。
Beacon Period (Kms)	ビーコン パケットの間隔を指定します。ビーコン パケットは、アドホック モードでクライアントがお互いを検索する場合に便利です。 **値の範囲：**20 ～ 976Kμs **デフォルト：**100Kμs

Admin Override タブ

Admin Override タブ ウィンドウ（図 4-12 を参照）では、個々のプロファイルの設定を管理者が上書きできるように指定できます。各プロファイルを異なる設定にすることができます。

（注）　Global Override Settings タブの設定がすべてのプロファイルに適用され、これらの個々のプロファイルの設定が上書きされます。

図 4-12　Admin Override タブ ウィンドウ

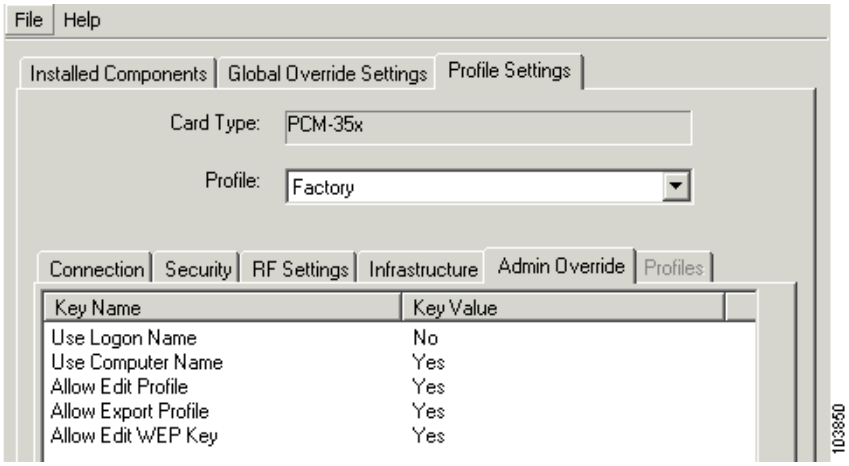


表 4-7 は、Admin Override タブのパラメータとその説明を示しています。パラメータを変更する場合は、この表の指示に従ってください。

表 4-7　Admin Override タブのパラメータ

パラメータ	説明
Use Logon Name	Windows のログイン名をクライアントのログイン名として使用するかどうかを指定します。 **値の範囲**：Yes または No **デフォルト**：No （注）　*Use Logon Name* を選択すると、Use Computer Name パラメータは自動的に選択解除されます。
Use Computer Name	コンピュータの名前をクライアントのログイン名として使用するかどうかを指定します。 **値の範囲**：Yes または No **デフォルト**：No （注）　*Use Computer Name* を選択すると、Use Logon Name パラメータは自動的に選択解除されます。

表 4-7　Admin Override タブのパラメータ

パラメータ	説明
Allow Edit Profile	ACU を使用してクライアント アダプタの設定プロファイルを編集できるかどうかを指定します。 **値の範囲**：Yes または No **デフォルト**：Yes
Allow Export Profile	ACU を使用してクライアント アダプタの設定プロファイルをディスク ファイルにエクスポートできるかどうかを指定します。 **値の範囲**：Yes または No **デフォルト**：Yes
Allow Edit WEP	ACU を使用して、クライアント アダプタの設定プロファイルにある WEP セキュリティ オプションを編集できるかどうかを指定します。 **値の範囲**：Yes または No **デフォルト**：Yes

Auto Profile Selection

Profile フィールドで Auto Profile Selection を選択すると、クライアント アダプタ用の最大 16 個のプロファイル（または保存された設定）を管理できます。これらのプロファイルを使用すると、異なる設定情報が必要なさまざまな場所でクライアント アダプタを使用できます。たとえば、クライアント アダプタを会社、自宅、および空港などの公共エリアで使用するためにプロファイルを設定できます。プロファイルを作成しておけば、クライアント アダプタを新しい場所に移動するたびに再設定しなくても、プロファイルが自動的に切り替わります。

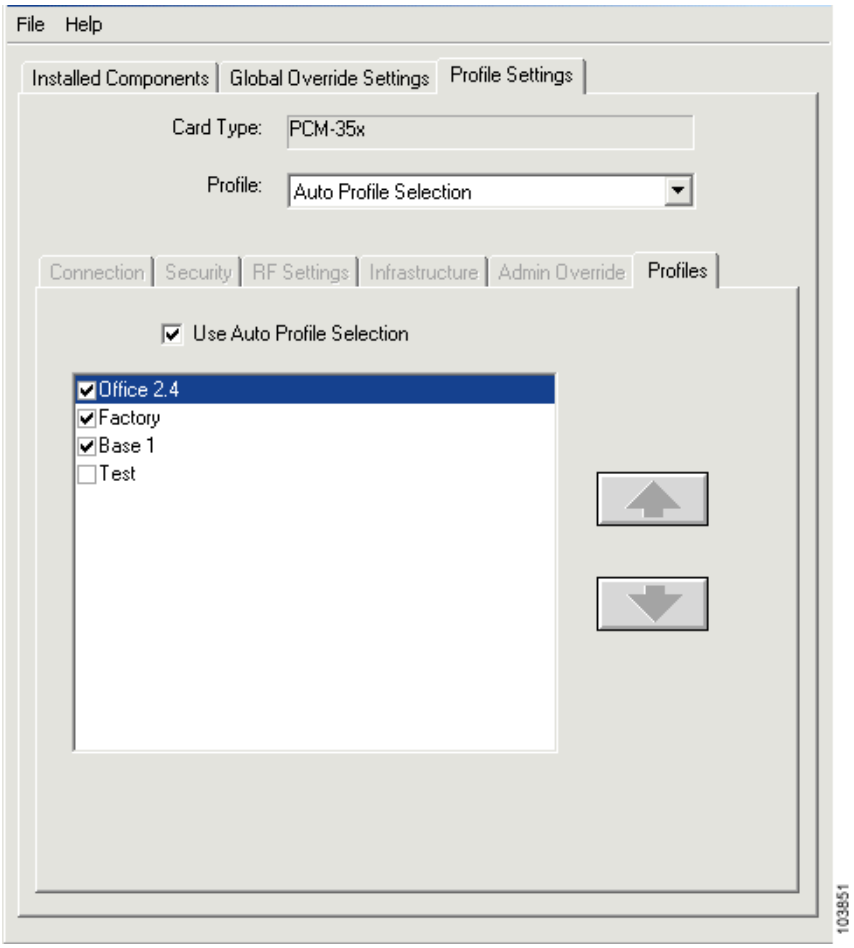
（注）　自動プロファイル選択では、複数の SSID、ヌルの（値が指定されていない）SSID、または同じ SSID を持つプロファイルはサポートされません。

Profiles タブ

Profile ドロップダウン メニューから Auto Profile Selection を選択すると、Profiles タブ ウィンドウが表示されます（図 4-13 を参照）。ウィンドウには使用可能なプロファイルがすべて表示されるので、そこから自動切り替えの対象となるプロファイルを選択して優先順位を付けることができます。あるエリアから別のエリアへローミングすると、アクセス ポイントへの接続が確立されるまで、プロファイルの SSID が優先順位に基づいてスキャンされます。クライアント アダプタからアクセス ポイントへのアソシエーションが失われると、リスト内で優先順位が最も高いプロファイルから SSID のスキャンが再開されます。

（注）　自動プロファイル選択では、ヌルの（値が指定されていない）SSID、重複する SSID、または複数の SSID を持つプロファイルは表示されません。これらのタイプのプロファイルは、プロファイルの自動切り替えでは使用できません。

図 4-13　Profiles タブ ウィンドウ



優先順位の設定と自動プロファイル選択の有効化

クライアント アダプタでプロファイルを設定して自動プロファイル選択を有効にする手順は、次のとおりです。

ステップ 1　自動プロファイル選択の対象とするプロファイルのチェック ボックスをオンにします。

ステップ 2　各プロファイルをクリックし、上矢印と下矢印を使用して、プロファイルを希望どおりの優先順位に並べます。リストの先頭は優先順位が最も高く、末尾は優先順位が最も低くなります。

ステップ 3　**Use Auto Profile Selection** チェックボックスをオンにします。