CHAPTER 4

ネットワーク アクセス マネージャの設定

この章では、ネットワーク アクセス マネージャ設定の概要について、ならびにユーザ ポリシーおよびネットワーク プロファイルの追加と設定の手順について説明します。この章で説明する内容は、次のとおりです。

概要

ネットワーク アクセス マネージャは、企業ネットワーク管理者によって定められたポリシーに従って、セキュアなレイヤ 2 ネットワークを提供するクライアント ソフトウェアです。ネットワーク アクセス マネージャは、最適なレイヤ 2 アクセス ネットワークを検出して選択し、有線およびワイヤレス ネットワークの両方へのアクセスに対するデバイス認証を実行します。ネットワーク アクセス マネージャは、セキュアなアクセスに必要なユーザおよびデバイス アイデンティティならびにネットワーク アクセス プロトコルを管理します。管理者定義のポリシーに違反する接続をエンド ユーザが確立しないように、インテリジェントに動作します。

AnyConnect Secure Mobility Client のネットワーク アクセス マネージャ コンポーネントは、次の主な機能をサポートします。

- 有線（IEEE 802.3）およびワイヤレス（IEEE 802.11）ネットワーク アダプタ
- Windows マシン クレデンシャルを使用する Pre-login 認証

- Windows ログイン クレデンシャルを使用するシングル サインオン ユーザ認証
- 簡略で使いやすい IEEE 802.1X 設定
- IEEE MACsec 有線暗号化および企業ポリシー制御
- EAP 方式：
  - EAP-FAST、PEAP、EAP-TTLS、EAP-TLS、および LEAP（IEEE 802.3 有線のみの EAP-MD5、EAP-GTC、および EAP-MSCHAPv2）
- 内部 EAP 方式：
  - PEAP：EAP-GTC、EAP-MSCHAPv2、および EAP-TLS
  - EAP-TTLS：EAP-MD5 および EAP-MSCHAPv2 およびレガシー方式（PAP、CHAP、MSCHAP、および MSCHAPv2）
  - EAP-FAST：GTC、EAP-MSCHAPv2、および EAP-TLS
- 暗号化モード：
  - スタティック WEP（オープンまたは共有）、ダイナミック WEP、TKIP、および AES
- キー確立プロトコル：
  - WPA、WPA2/802.11i、および CCKM（IEEE 802.11 NIC カードに応じて選択）

（注） CCKM でサポートされるアダプタは、Windows XP 上の Cisco CB21AG のみです

- スマート カードが提供するクレデンシャル。AnyConnect は、次の環境のスマート カードをサポートします。
  - Windows XP、7、および Vista 上の Microsoft CAPI 1.0 および CAPI 2.0
  - Mac OS X（10.4 以降）でトークンされたキーチェーン

（注） AnyConnect は、Linux または PKCS #11 デバイス上のスマート カードをサポートしません。

ネットワーク アクセス マネージャのシステム要件

ネットワーク アクセス マネージャ モジュールには、次が必要です。

- ASDM バージョン 6.4(0)104 以降

（注） スタンドアロン ネットワーク アクセス マネージャ エディタは、ネットワーク アクセス マネージャ プロファイル設定の代替としてサポートされています。セキュリティ上の理由から、AnyConnect は、標準エディタで編集されたネットワーク アクセス マネージャ プロファイルは受け入れません。

- 次のオペレーティング システムがネットワーク アクセス マネージャをサポートしています。
  - Windows 7（x86（32 ビット）および x64（64 ビット））
  - Windows Vista SP2（x86（32 ビット）および x64（64 ビット））
  - Windows XP SP3（x86（32 ビット））

– Windows Server 2003 SP2（x86（32 ビット））

ライセンスとアップグレード要件

AnyConnect ネットワーク アクセス マネージャは、無償でシスコの無線アクセス ポイント、ワイヤレス LAN コントローラ、スイッチ、および RADIUS サーバで使用できるようにライセンスされています。AnyConnect Essentials ライセンスまたは Premium ライセンスは必要ありません。関連するシスコの装置では、現在の SmartNet 契約が必要です。

ネットワーク アクセス マネージャの事前展開

ネットワーク アクセス マネージャを事前展開する場合、AnyConnect クライアントが ASA への初期接続を確立する前に、ネットワーク アクセス マネージャをエンドポイントにインストールします。ネットワーク アクセス マネージャ モジュールをインストールする前に、AnyConnect Secure Mobility Client をエンドポイントにインストールする必要があります。AnyConnect Secure Mobility Client のインストール手順については、「AnyConnect Secure Mobility Client の展開」（P.2-1）を参照してください。

ネットワーク アクセス マネージャの停止と起動

ローカル管理者特権を持つユーザが、ネットワーク アクセス マネージャを起動および停止できます。ローカル管理者特権を持たないユーザは、プロファイル エディタの [認証（Authentication）] パネルで定義されるサービス パスワードを使用しないと、ネットワーク アクセス マネージャを起動および停止できません。

プロファイル エディタ

ネットワーク アクセス マネージャ プロファイル エディタは、設定プロファイルの作成と事前設定クライアント プロファイルの作成のために設計されました。この設定がエンドポイントで展開されると、ネットワーク アクセス マネージャが管理面で定義されているエンド ユーザおよび認証ポリシーを適用できるようになり、事前設定ネットワーク プロファイルをエンド ユーザが使用できるようになります。プロファイル エディタを使用するには、プロファイルの設定を作成して保存し、設定をクライアントに配置します。AnyConnect には、ASDM 内にプロファイル エディタが含まれていますが、スタンドアロン バージョンも使用できます。プロファイル エディタの要件と展開手順については、第 2 章「AnyConnect Secure Mobility Client の展開」を参照してください。

新しいプロファイルの追加

ネットワーク アクセス マネージャに新しいプロファイルを追加するには、次の手順を実行します。

ステップ 1　ASDM ツールバーの [設定（Configuration）] をクリックします。

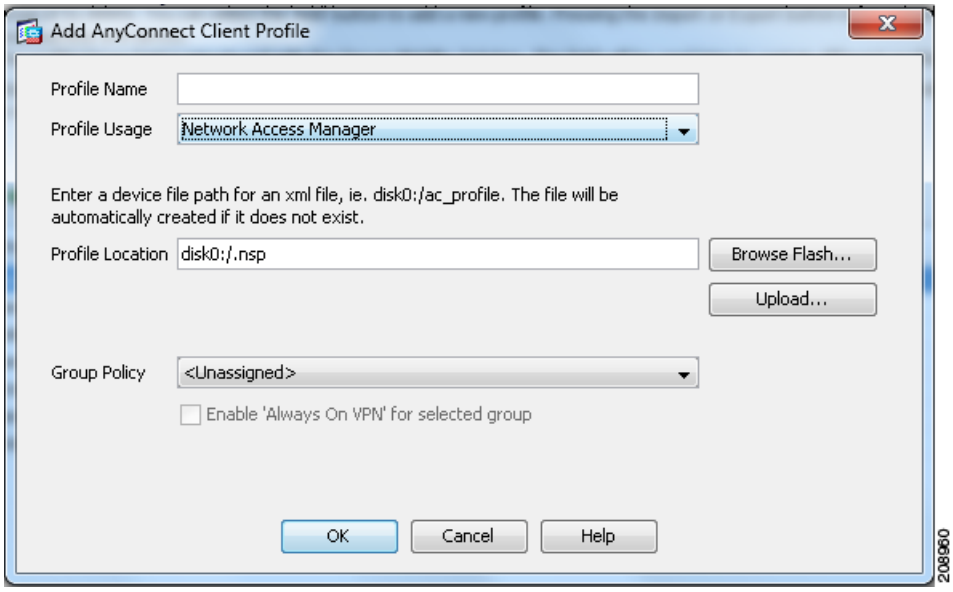
ステップ 2　ナビゲーション領域の左端にある [リモート アクセス VPN（Remote Access VPN）] をクリックします。

ステップ 3　[ネットワーク クライアント アクセス（Network Client Access）] をクリックします。

ステップ 4　[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] をクリックします。[プロファイル（profile）] ウィンドウが表示されます。

ステップ 5　[追加（Add）] をクリックします。[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profile）] ウィンドウが表示されます（図 4-1 を参照）。

図 4-1　[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profile）] ウィンドウ



ステップ 6　プロファイル名を入力します。

（注）　ネットワーク アクセス マネージャ プロファイルの作成にスタンドアロン プロファイル エディタを使用している場合は、[プロファイル名（Profile Name）] フィールドのエントリとして **configuration.xml** を使用する必要があります。プロファイル エディタは、このファイルを newConfigFiles ディレクトリにコピーします。このプロセスを開始するには、ユーザがネットワーク アクセス マネージャを修復する必要があります。ネットワーク アクセス マネージャが再起動されると、新しい設定ファイルが検証されてネットワーク アクセス マネージャ /system ディレクトリに移動されます。

ステップ 7　[プロファイルの使用（Profile Usage）] ドロップダウン リストから [ネットワーク アクセス マネージャ（Network Access Manager）] を選択して、[OK] をクリックします。

ステップ 8　（任意）[プロファイル ロケーション（Profile Location）] パラメータに、XML ファイルのデバイス ファイル パスを確立します。

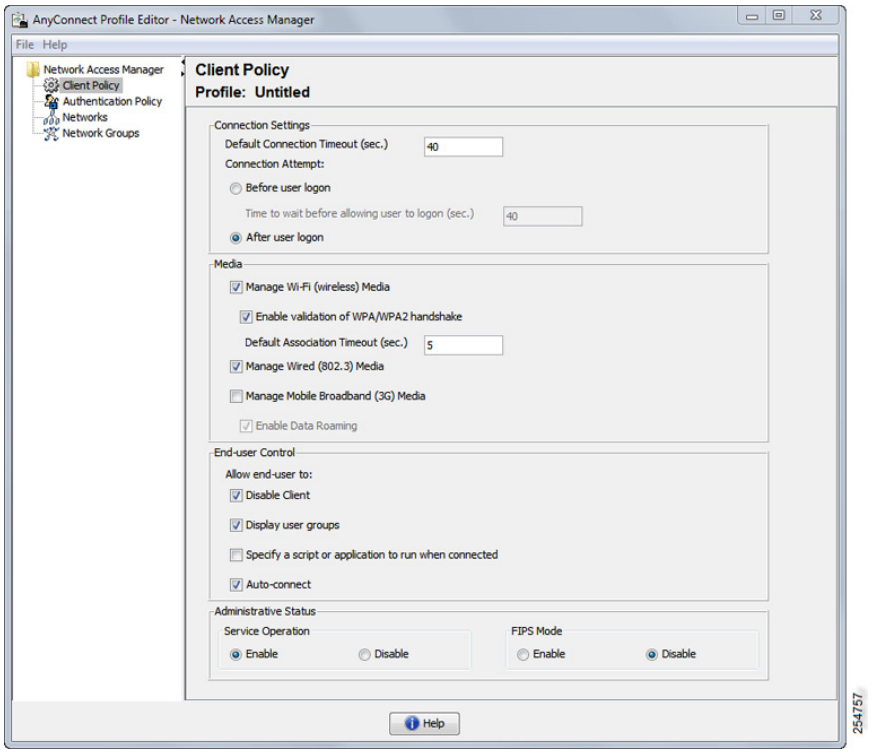
ステップ 9　（任意）ドロップダウン リストから AnyConnect グループ ポリシーを選択します。

ステップ 10　[OK] をクリックします。

クライアント ポリシーの設定

[クライアント ポリシー（Client Policy）] ウィンドウでは、クライアント ポリシー オプションを設定できます（図 4-2 を参照）。

図 4-2　[クライアント ポリシー（Client Policy）] ウィンドウ



次の 4 つのセクションで構成されます。

- 管理ステータス（Administrative Status）
  - [サービス オペレーション（Service Operation）] パラメータを使用すると、ネットワーク アクセス マネージャ機能をオンまたはオフに切り替えられます。サービスをディセーブルにすることを選択した場合、ネットワーク アクセス マネージャは、クライアント上のネットワーク接続を管理できません。
  - FIPS モードをオンまたはオフに切り替えられます。連邦情報処理標準（FIPS 104-2）は、米国 政府の標準で、暗号化モジュールのセキュリティ要件について定めています。FIPS モードをイネーブルにすると、ネットワーク アクセス マネージャは、政府の要件を満たす方法で暗号化の処理を実行します。処理の通常の FIPS モードはディセーブルです。詳細については、「FIPS と追加セキュリティのイネーブル化」（P.8-1）を参照してください。
- [接続の設定（Connection Settings）]：ユーザ ログインの前または後にユーザ接続コンポーネントを使用したネットワークの試行をするかどうかを定義できます。

- [デフォルトの接続タイムアウト（Default Connection Timeout）]：ユーザが作成したネットワークの接続タイムアウト パラメータとして使用する秒数を指定します。デフォルト値は、40 秒です。
- [ユーザ ログインの前（Before User Logon）]：Windows ユーザ ログイン手順が実行される前に、ネットワーク アクセス マネージャがユーザ接続をすぐに試行するように指定します。Windows ログイン手順には、ユーザ アカウント（Kerberos）認証、ユーザ GPO のロード、および GPO ベースのログイン スクリプトの実行が含まれます。
- [ユーザ ログインまでの待機時間（Time to Wait Before Allowing User to Logon）]：ネットワーク アクセス マネージャが完全なネットワーク接続を確立するまでに待機する最大秒数（最悪のケース）を指定します。ネットワーク接続がこの時間内に確立できない場合、Windows ログイン プロセスでユーザ ログインが続行されます。デフォルトは 5 秒です。

（注）　ネットワーク アクセス マネージャがワイヤレス接続を管理するように設定されている場合、ワイヤレス接続の確立には時間が余計に必要なため、30 秒以上を使用することを推奨します。DHCP 経由で IP アドレスを取得するために必要な時間も考慮する必要があります。2 つ以上のネットワーク プロファイルが設定されている場合、2 つ以上の接続試行に対応するように値を大きくできます。

- [ユーザ ログイン後（After User Logon）]：Windows ユーザ ログイン手順後に、ネットワーク アクセス マネージャがユーザ接続を試行することを指定します。

- [メディア（Media）]：ネットワーク アクセス マネージャ クライアントによって制御されるメディア タイプが選択できます。
  - [Wi-Fi（ワイヤレス）メディアの管理（Manage Wi-Fi (wireless) Media）]：WiFi メディアの管理をイネーブルにします。任意で WPA/WPA2 ハンドシェイク検証もイネーブルにできます。

    IEEE 802.11i ワイヤレス ネットワーキング標準には、キー導出中に EAPOL キー データの送信されたアクセス ポイントの RSN IE がビーコン/プローブ応答フレームにあるアクセス ポイントの RSN IE と一致することをサプリカントが検証する必要があることが定められています。WPA/WPA2 ハンドシェイクの検証をイネーブルにする場合は、デフォルト アソシエーション タイムアウトを指定する必要があります。WPA/WPA2 ハンドシェイク設定の検証のイネーブル化をオフにすると、この検証手順は省略されます。

    （注）　ただし、一部のアダプタでは、アクセス ポイントの RSN IE を常に提供するわけではないため、認証試行に失敗し、クライアントが接続されません。

  - [有線（IEEE 802.3）メディアの管理（Manage Wired (IEEE 802.3) Media）]：ネットワーク アクセス マネージャの有線メディアの管理をイネーブルにします。

- [エンドユーザの制御（End-user Control）]：ユーザの次の制御を決定できます。
  - [クライアントの無効化（Disable Client）]：AnyConnect UI を使用した有線およびワイヤレス メディアのネットワーク アクセス マネージャによる管理をユーザがディセーブルまたはイネーブルにできます。
  - [ユーザ グループの表示（Display User Groups）]：管理者定義のグループに対応しない場合でも、ユーザが作成したグループ（CSSC 5.x から作成）を表示して、接続できるようにします。
  - [接続時に実行するスクリプトまたはアプリケーションの指定（Specify a Script or Application To Run When Connected）]：ネットワークの接続時に実行するスクリプトまたはアプリケーションをユーザが指定できます。

（注）　スクリプトの設定は、1 つのユーザ設定ネットワークに固有であり、そのネットワークが接続状態になったときに実行するローカル ファイル（.exe、.bat、または .cmd）をユーザが指定できます。競合を避けるために、スクリプト機能では、ユーザはユーザ定義のネットワークのスクリプトまたはアプリケーションの設定のみを実行でき、管理者定義のネットワークは実行できません。スクリプト機能では、スクリプトの実行に関して管理者ネットワークをユーザが変更できません。このため、ユーザは管理者ネットワークのインターフェイスを使用できません。また、ユーザにスクリプトの実行設定を許可しない場合、この機能はネットワーク アクセス マネージャ GUI に表示されません。

- [自動接続（Auto-connect）] : 選択すると、ネットワーク アクセス マネージャは、ユーザが選択する必要なく、自動的にネットワークに接続されます。デフォルトは自動接続です。

認証ポリシーの設定

このウィンドウでは、グローバル アソシエーションおよび認証ネットワーク ポリシーを定義できます。これらのポリシーは、ユーザが作成できるすべてのネットワークに適用されます。ポリシーを使用すると、ユーザが GUI で作成できるネットワークのタイプが制限できます。いずれかのアソシエーションまたは認証モードをオンにしない場合、ユーザはネットワークを作成できません。モードのサブセットを選択すると、ユーザはこれらのタイプのネットワークを作成できますが、オフのタイプは作成できません。目的のアソシエーションまたは認証モードをそれぞれ選択するか、[すべて選択（Select All）] を選択します。

[ネットワーク アクセス マネージャ（Network Access Manager）] メニューから [認証ポリシー（Authentication Policy）] を選択すると、図 4-3 に示されているウィンドウが表示されます。

お客様の要件に応じて、セキュア モビリティ環境で異なる認証メカニズムが使用されますが、すべてのメカニズムが IEEE 802.1X、EAP、および RADIUS をサポートするプロトコルとして使用します。これらのプロトコルでは、ワイヤレス LAN クライアントの認証成功に基づいたアクセス制御ができ、またユーザがワイヤレス LAN ネットワークを認証することもできます。

このシステムでは、AAA のその他の要素（許可およびアカウンティング）も RADIUS および RADIUS アカウンティングを通じて通信するポリシーを通じて提供されています。

認証プロトコル選択のメカニズムは、現在のクライアント認証データベースと統合されています。セキュアなワイヤレス LAN 展開では、ユーザが新しい認証システムを作成する必要はありません。

EAP

EAP とは、認証プロトコルがそれを伝送するトランスポート プロトコルからデカップリングされていることの要件に対処する IEFT RFC のことです。このデカップリングによって、トランスポート プロトコル（IEEE 802.1X、UDP、または RADIUS など）は、認証プロトコルを変更せずに、EAP プロトコルを伝送できます。

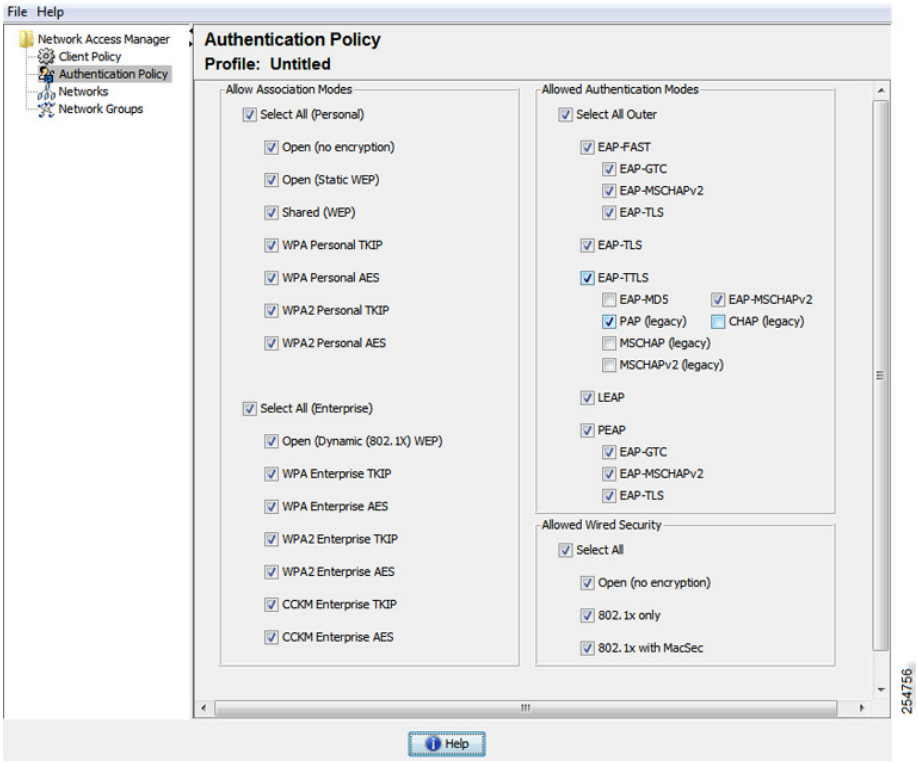
基本的な EAP プロトコルは、比較的単純で次の 4 つのパケット タイプから構成されます。

- EAP 要求：オーセンティケータは、要求パケットをサプリカントに送信します。各要求には type フィールドがあり、要求されている内容を示します。これには、使用するサプリカント アイデンティティや EAP タイプなどが含まれます。シーケンス番号により、オーセンティケータおよびピアは、各 EAP 要求に対応する EAP 応答を一致できます。

- EAP 応答：サプリカントは、オーセンティケータに応答パケットを送信して、EAP 要求開始に一致するシーケンス番号を使用します。EAP 応答のタイプは、通常 EAP 要求と一致しますが、応答が NAK の場合は除きます。
- EAP success：オーセンティケータは、認証に成功すると、成功パケットをサプリカントに送信します。
- EAP failure：オーセンティケータは、認証に失敗すると、失敗パケットをサプリカントに送信します。

EAP を IEEE 802.11X システムで使用している場合、アクセス ポイントは EAP パススルー モードで動作します。このモードでは、アクセス ポイントはコード、識別子、および長さのフィールドを確認して、サプリカントから受信した EAP パケットを AAA サーバに転送します。オーセンティケータで AAA サーバから受信したパケットは、サプリカントに転送されます。

図 4-3　[認証ポリシー（Authentication Policy）] ウィンドウ



このページの各オプションの説明については、次を参照してください。

- 個人または企業アソシエーション モードについて：ネットワーク セキュリティ レベルの定義
- 許可された認証モードについて：ネットワーク マシンまたはユーザ認証の定義
- 許可された有線セキュリティについて：ネットワーク接続タイプの定義

ネットワークの設定

[ネットワーク（Networks）] ウィンドウでは、企業ユーザ向けに事前定義のネットワークを設定できます。すべてのグループで使用できるネットワークを設定する、または特定のネットワークで使用するグループを作成できます。

グループとは、基本的に、設定された接続（ネットワーク）の集合です。各設定された接続は、グループに属するか、すべてのグループのメンバである必要があります。

（注） 下位互換性を確保するため、Cisco Secure Services Client で展開された管理者作成のネットワークは、SSID をブロードキャストしない非表示ネットワークとして扱われます。ユーザ ネットワークは、自身の SSID をブロードキャストするネットワークとして扱われます。

新しいグループを作成できるのは管理者だけです。設定にグループが定義されていない場合、プロファイル エディタによって自動生成グループが作成されます。自動生成グループには、管理者定義のグループに割り当てられていないネットワークが含まれます。クライアントは、アクティブ グループに定義されている接続を使用してネットワーク接続の確立を試みます。[ネットワーク グループ（Network Groups）] ウィンドウの [ネットワークの作成（Create networks）] オプションの設定に応じて、エンド ユーザは、ユーザ ネットワークをアクティブ グループに追加するか、アクティブ グループからユーザ ネットワークを削除できます。

定義されているネットワークは、リストの先頭にあるすべてのグループで使用できます。globalNetworks 内にあるネットワークを制御できるため、エンド ユーザが接続できる企業ネットワークを指定できます。これは、ユーザ定義のネットワーク内にある場合も同様です。管理者設定のネットワークは、エンド ユーザは削除できません。

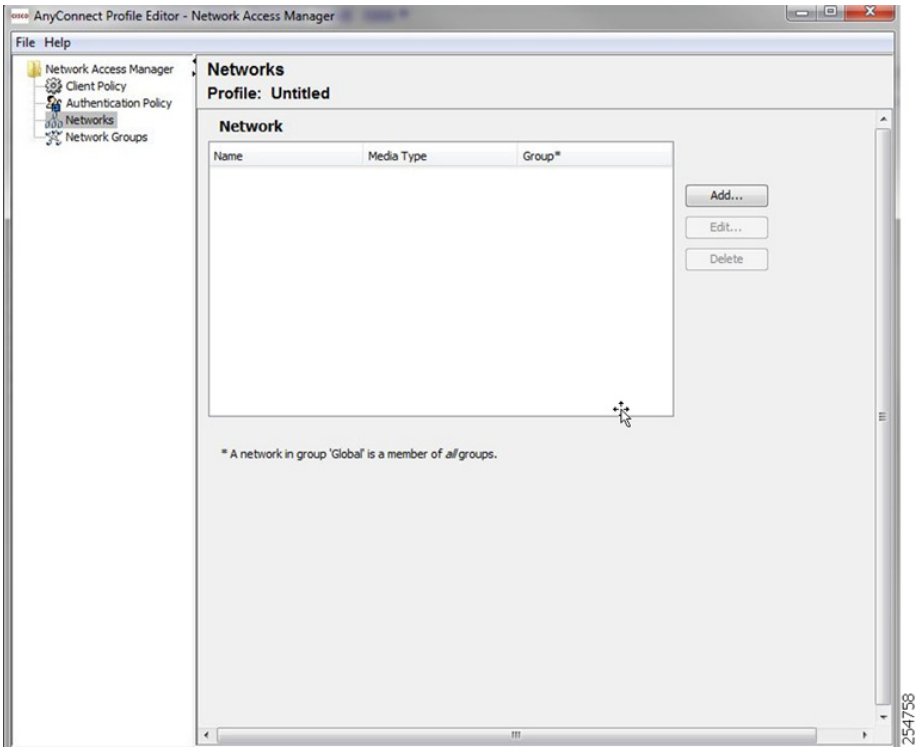
（注） エンド ユーザは、ネットワークをグループに追加できますが、globalNetworks セクションにあるネットワークは除きます。これは、globalNetworks セクションにあるネットワークはすべてのグループに存在するためで、これらはプロファイル エディタを使用してのみ作成できます。

企業ネットワークの一般的なエンド ユーザは、このクライアントを使用するためにグループの知識を必要としないことに注意してください。アクティブ グループは、設定の最初のグループです。ただし、1 つのグループのみが使用できる場合は、クライアントはアクティブ グループを認識せず、アクティブ グループを表示しません。一方で、複数のグループが存在する場合、UI にはアクティブ グループが選択されたことを示すコンボ ボックスが表示されます。これにより、ユーザはアクティブ グループからの選択ができ、設定は再起動後も持続します。[ネットワーク グループ（Network Groups）] ウィンドウの [ネットワークの作成（Create networks）] オプションの設定に応じて、エンド ユーザはグループを使用せずに自身のネットワークを追加または削除できます。

（注） グループ選択は再起動後も持続して、ネットワークは修復されます（トレイ アイコンを右クリックしながら [ネットワーク修復（Network Repair）] を選択して実行することにより）。ネットワーク アクセス マネージャが修復されたか再起動された場合、ネットワーク アクセス マネージャは以前のアクティブ グループを使用して起動します。

[ネットワーク アクセス マネージャ（Network Access Manager）] メニューから [ネットワーク（Networks）] を選択すると、図 4-4 に示されているウィンドウが表示されます。

図 4-4　[ネットワーク（Networks）] ウィンドウ



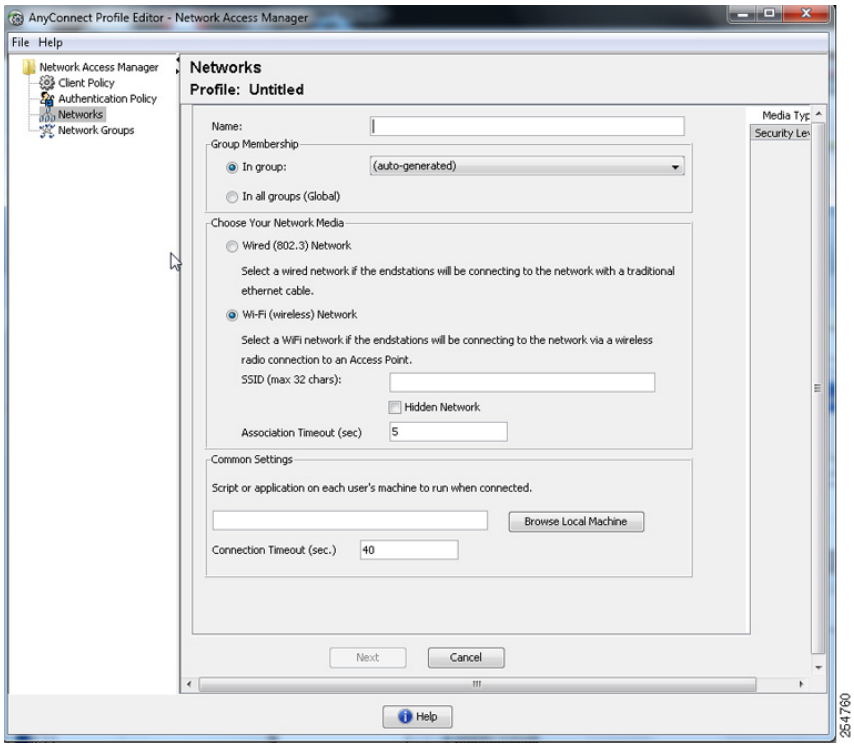
次のいずれかのアクションを選択します。

- [追加（Add）] をクリックし、新しいネットワークを作成します。新しいネットワークの作成を選択する場合は、後のネットワーク メディア タイプの定義の項の手順に従います。
- 変更するネットワークを選択して、[編集（Edit）] をクリックします。
- 削除するネットワークを選択して、[削除（Delete）] をクリックします。

ネットワーク メディア タイプの定義

このウィンドウ パネルでは、有線またはワイヤレス ネットワークを作成または編集できます。設定は、有線またはワイヤレスのいずれを選択するかにより異なります。図 4-5 に、Wi-Fi ネットワークを選択すると表示されるウィンドウを示します。この項では、有線と Wi-Fi オプションの両方について説明します。

図 4-5　[メディア タイプ（Media Type）] パネル



ステップ 1　[名前（Name）] フィールドに、このネットワークに対して表示する名前を入力します。

ステップ 2　（Wi-Fi のみ）[SSID] パラメータに、ワイヤレス ネットワークの SSID を入力します。

ステップ 3　（Wi-Fi のみ）ネットワークが自身の SSID をブロードキャストしていない場合は、[非表示のネットワーク（Hidden Network）] を選択します。

（注）　ネットワーク アクセス マネージャの選択アルゴリズムは、ネットワーク スキャン リストを活用するように最適化されます。自身の SSID をブロードキャストするネットワークの場合、ネットワーク アクセス マネージャは、これらのネットワークがネットワーク スキャン リストに表示されたときに、これらのネットワークとの接続のみを試行します。

ステップ 4　（Wi-Fi のみ）[アソシエーション タイムアウト（Association Timeout）] パラメータに、ネットワーク アクセス マネージャが使用可能なネットワークを再評価する前に特定のワイヤレス ネットワークとのアソシエーションを待機する期間を入力します。デフォルトのアソシエーション タイムアウトは 5 秒です。

ステップ 5　[共通設定（Common Settings）] セクションでは、実行するファイルのパスおよびファイル名を入力するか、場所を参照して実行するファイルを選択します。

スクリプトおよびアプリケーションには、次が適用されます。

- .exe、.bat、または .cmd 拡張子のファイルが受け入れられます。

- ユーザは、管理者作成のネットワーク内で定義されているスクリプトまたはアプリケーションを変更できません。
- プロファイル エディタを使用してパスおよびスクリプトまたはアプリケーションのファイル名の指定のみができます。スクリプトまたはアプリケーションがユーザのマシンに存在しない場合は、エラー メッセージが表示されます。スクリプトまたはアプリケーションがユーザのマシンに存在しないこと、およびシステム管理者に問い合わせが必要なことがユーザに通知されます。
- アプリケーションがユーザのパスに存在する場合を除いて、実行するアプリケーションのフル パスを指定する必要があります。アプリケーションがユーザのパスに存在する場合は、アプリケーション名またはスクリプト名だけを指定できます。

ステップ 6　[接続タイムアウト（Connection Timeout）] パラメータに、ネットワーク アクセス マネージャが別のネットワークへの接続を試行する（接続モードが自動の場合）または別のアダプタを使用する前に、ネットワーク接続の確立を待機する秒数を入力します。

（注）　スマート カード認証システムによっては、認証を完了するまでに 60 秒近くが必要です。スマート カードを使用するときは、[接続タイムアウト（Connection Timeout）] 値を大きくする必要がある場合があります。

ステップ 7　[次へ（Next）] をクリックします。

ネットワーク セキュリティ レベルの定義

有線またはワイヤレス ネットワークのセキュリティ レベル タイプを定義できます。[セキュリティ レベル（Security Level）] 領域で、目的のネットワーク タイプを選択します。

- 認証有線ネットワークの使用：セキュアな企業有線ネットワークで推奨。
- オープン ネットワークの使用：推奨されていないが、有線ネットワーク上のゲスト アクセスで使用可能。
- 共有キーの使用：小規模オフィスやホーム オフィスなどのワイヤレス ネットワークで推奨。
- 認証 WiFi ネットワークの使用：セキュアな企業ワイヤレス ネットワークで推奨。

認証有線ネットワークの使用

セキュリティ レベルに IEEE 802.1X 認証を使用する場合は、次の手順を実行します。

ステップ 1　[ネットワークの認証中（Authenticating Network）] を選択します。

（注）　[ネットワーク メディア タイプ（Network Media Type）] パネルで [有線（802.3）ネットワーク（Wired (802.3) Network）] を必ず選択します（図 4-5 を参照）。

ステップ 2　ネットワーク設定に応じて IEEE 802.1X 設定を調整します。

- [認証期間（秒）（authPeriod(sec.)）]：認証が開始された場合、認証メッセージの間隔がこの時間を超えるとサプリカントはタイムアウトします。認証を再度開始するには、サプリカントでオーセンティケータが必要です。

- [保持期間（秒）（heldPeriod(sec.)）]：認証が失敗した場合、サプリカントはここで定義された時間だけ待機し、この時間を超えると別の認証が試行されます。
- [開始期間（秒）（startPeriod(sec.)）]：EAPoL-Start を送信してオーセンティケータを使用して認証の試行を開始した後、サプリカントはこのタイマーで定義された時間だけオーセンティケータからの応答を待機します。この時間を超えると認証が再度開始されます（次の EAPoL-Start を送信するなど）。
- [最大開始（maxStart）]：EAPoL-Start を送信してオーセンティケータを使用してサプリカントが認証を開始する回数です。この回数を超えるとサプリカントはオーセンティケータが存在しないと見なします。これが発生した場合は、サプリカントはデータ トラフィックを許可します。

ヒント　単一の認証有線接続がオープンおよび認証ネットワークの両方と動作するように設定できます。これは、[開始期間（startPeriod）] および [最大開始（maxStart）] を注意深く設定して、認証開始試行に費やす合計時間がネットワーク接続タイマーよりも小さくなるようにします（[開始期間（startPeriod）] x [最大開始（maxStart）] < ネットワーク接続タイマー）。

（注）このシナリオでは、ネットワーク接続タイマーを（[開始期間（startPeriod）] x [最大開始（maxStart）]）秒だけ大きくして、DHCP アドレスを取得してネットワーク接続を完了するために十分な時間をクライアントに与えます。

逆に、認証が成功した場合のみデータ トラフィックを許可する管理者の場合は、[開始期間（startPeriod）] および [最大開始（maxStart）] を確認して、認証開始試行に費やす合計時間がネットワーク接続タイマーよりも大きくなるようにします（[開始期間（startPeriod）] x [最大開始（maxStart）] > ネットワーク接続タイマー）。

ステップ 3　次のセキュリティ レベルから選択します。

- [キーの管理（Key Management）]：有線ネットワークで使用するキー管理プロトコルを、ドロップダウン リストを使用して決定します。
  - [なし（None）]：キー管理プロトコルを使用しません。また、有線暗号化を実行しません。
  - [MKA]：サプリカントは、MACsec Key Agreement および暗号キーのネゴシエートを試行します。MACsec とは、MAC Layer Security のことで、有線ネットワークを介した MAC レイヤ暗号化を提供します。MACsec プロトコルは、暗号化を使用して MAC レベル フレームを保護する手段であり、MACsec Key Agreement（MKA）エンティティに依存して暗号キーをネゴシエートおよび配布します。

（注）　MACsec Key Agreement の定義の詳細については、IEEE-802.1X-Rev を参照してください。また、MACsec 暗号化プロトコルの定義の詳細については、IEEE 802.1AE-2006 を参照してください。
さらに、利点と制限事項、機能の概要、設計上の考慮事項、展開、およびトラブルシューティングなどを含む MACsec の詳細については、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/deploy_guide_c17-663760.html を参照してください。

- 暗号化
  - [なし（None）]：データ トラフィックの整合性チェックは行われますが、暗号化はされません。
  - [MACsec: AES-GCM-128]：データ トラフィックは、AES-GCM-128 を使用して暗号化されます。

ステップ 4　[ポート認証の例外ポリシー（Port Authentication Exception Policy）] を選択します。[ポート認証の例外ポリシー（Port Authentication Exception Policy）] をイネーブルにすることで、IEEE 802.1X サプリカントの認証プロセス中の動作を調整できます。ポートの例外がイネーブルではない場合、サプリカントは、既存の動作を続けて完全な設定が正常に完了すると（またはこの項で前に説明したように、オーセンティケータからの応答を受信せずに [最大開始（maxStart）] の回数だけ認証が開始された後で）ポートを開くことだけを行います。次のいずれかのオプションを選択します。

- [認証前にデータ トラフィックを許可（Allow data traffic before authentication）]：選択すると、この例外により認証試行の前にデータ トラフィックが許可されます。
- [次の場合でも認証後にデータ トラフィックを許可（Allow data traffic after authentication even if）]
  - [EAP で失敗（EAP Fails）]：選択すると、サプリカントは認証を試行します。しかし、認証に失敗した場合、サプリカントは認証に失敗したにもかかわらず、データ トラフィックを許可します。
  - [EAP では成功したがキー管理で失敗（EAP succeeds but key management fails）]：選択すると、サプリカントはキー サーバとのキーのネゴシエートを試行しますが、何らかの理由によりキー ネゴシエーションに失敗した場合でもデータ トラフィックを許可します。この設定は、キー管理が設定されている場合のみ有効です。キー管理がなしに設定されている場合、このチェックボックスはグレー表示されます。

（注）　MACsec は、ACS バージョン 5.1 以降および MACsec 対応スイッチを必要とします。ACS またはスイッチ設定については、『*Catalyst 3750-X and 3560-X Switch Software Configuration Guide*』を参照してください。

オープン ネットワークの使用

オープン ネットワークは、認証や暗号化を使用しません。オープン（非セキュア）ネットワークを作成するには、次の手順を実行します。

ステップ 1　[セキュリティ レベル（Security Level）] パネルから [ネットワークを開く（Open Network）] を選択します。この選択肢では、最もセキュリティ レベルの低いネットワークが提供されます。これは、ゲスト アクセス ワイヤレス ネットワークに推奨されています。

ステップ 2　[次へ（Next）] をクリックします。

ステップ 3　接続タイプを決定します。「ネットワーク接続タイプの定義」（P.4-17）を参照してください。

共有キーの使用

Wi-Fi ネットワークは、エンド ステーションとネットワーク アクセス ポイント間のデータを暗号化するときに使用するための、暗号キーを導出するために共有キーを使用することがあります。共有キーが WPA または WPA2 Personal とともに使用される場合、この設定では、小規模オフィスやホーム オフィスに適した中 レベルのセキュリティ クラスを提供します。

（注）　この設定は、企業ワイヤレス ネットワークでは推奨されません。

セキュリティレベルに共有キー ネットワークを指定する場合は、次の手順を実行します。

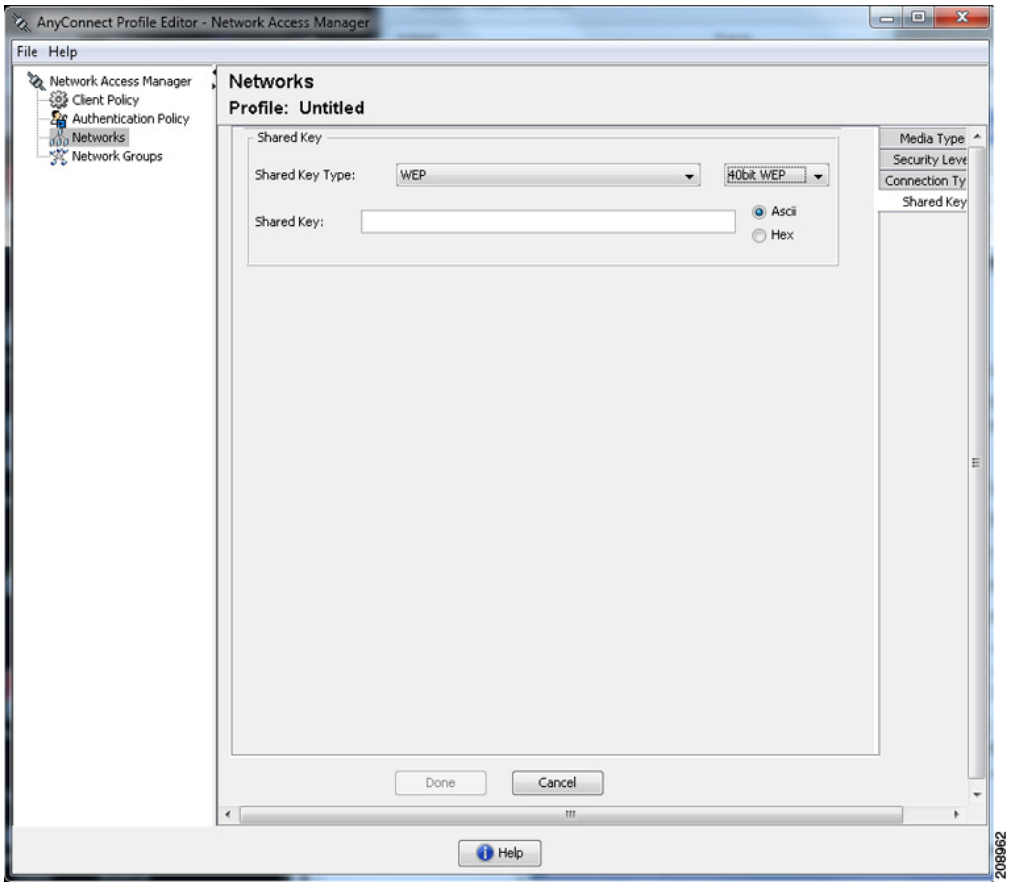
ステップ 1　[共有キー ネットワーク（Shared Key Network）] を選択します。

ステップ 2　[セキュリティ レベル（Security Level）] ウィンドウで [次へ（Next）] をクリックします。

ステップ 3　[ユーザ接続（User Connection）] または [マシン接続（Machine Connection）] を指定します。詳細については、「ネットワーク接続タイプの定義」（P.4-17）を参照してください。

ステップ 4　[次へ（Next）] をクリックします。[共有キー（Shared Key）] パネルが表示されます（図 4-6 を参照）。

図 4-6　[共有キー（Shared Key）] パネル



ステップ 5　[共有キー タイプ（Shared Key Type）]：共有キー タイプを定める共有キー アソシエーション モードを指定します。次の選択肢があります。

- [WEP]：スタティック WEP 暗号化を使用するレガシー IEEE 802.11 オープンシステム アソシエーション。
- [共有（Shared]）]：レガシー IEEE 802.11 共有キー アソシエーション。
- [WPA/WPA2- パーソナル（WPA/WPA2-Personal）]：Wi-Fi セキュリティ プロトコル。パスフレーズ事前共有キー（PSK）から暗号キーを導出します。

ステップ 6　レガシー IEEE 802.11 WEP または共有キーを選択する場合は、40 ビット、64 ビット、104 ビット、または 128 ビットを選択します。40 または 64 ビットの WEP キーは、5 個の ASCII 文字または 10 桁の 16 進数である必要があります。104 または 128 ビットの WEP キーは、13 個の ASCII 文字または 26 桁の 16 進数である必要があります。

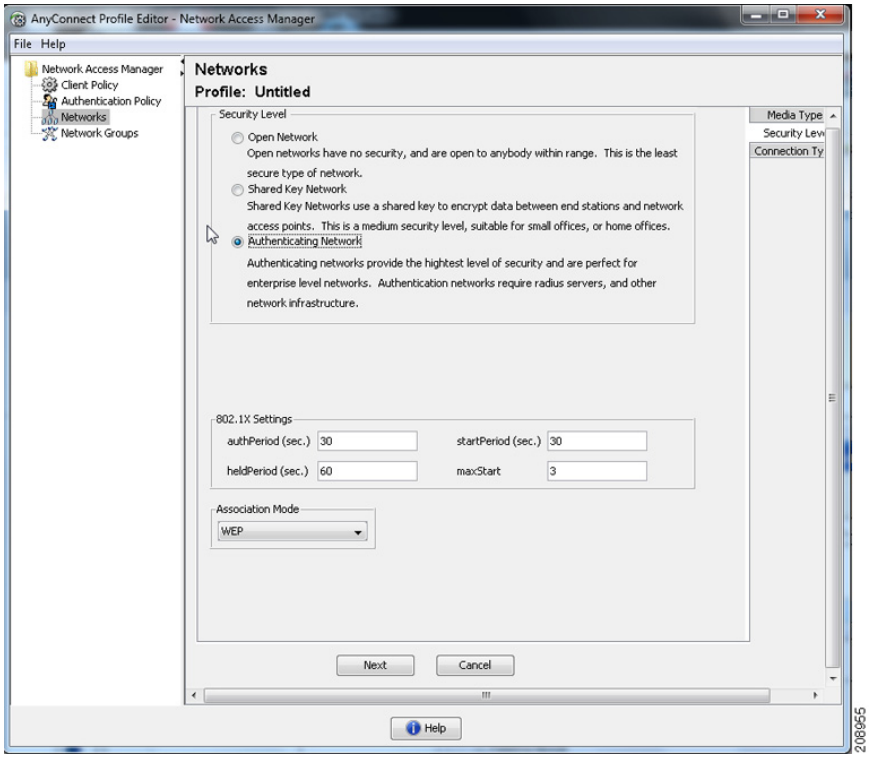
ステップ 7　WPA または WPA2 Personal を選択する場合は、使用する暗号化タイプ（TKIP/AES）を選択してから共有キーを入力します。入力するキーは、8 ～ 63 個の ASCII 文字またはちょうど 64 桁の 16 進数である必要があります。共有キーが ASCII 文字で構成されている場合は、[ASCII] を選択します。共有キーに 64 桁の 16 進数が含まれている場合は、[16 進数（Hexadecimal）] を選択します。

認証 WiFi ネットワークの使用

[ネットワークの認証中（Authenticating Network）] を選択すると、IEEE 802.1X および EAP に基づいたセキュアなワイヤレス ネットワークを作成できます。

セキュリティ レベルに認証ネットワークを指定する場合は、次の手順を実行します（図 4-7 を参照）。

図 4-7　　認証ネットワーク セキュリティ レベル



ステップ 1　[ネットワークの認証中（Authenticating Network）] を選択します。

ステップ 2　大半のネットワークでデフォルト値が機能するはずですが、必要に応じて環境に合わせて IEEE 802.1X 設定を実行することもできます。

- [認証期間（秒）（authPeriod(sec.)）] : 認証が開始された場合、認証メッセージの間隔がこの時間を超えるとサプリカントはタイムアウトします。認証を再度開始するには、サプリカントでオーセンティケータが必要です。デフォルトは 30 秒です。
- [保持期間（秒）（heldPeriod(sec.)）] : 認証が失敗した場合、サプリカントはここで定義された時間だけ待機し、この時間を超えると別の認証が試行されます。デフォルトは 60 秒です。
- [開始期間（秒）（startPeriod(sec.)）] : EAPoL-Start を送信してオーセンティケータを使用して認証の試行を開始した後、サプリカントはこのタイマーで定義された時間だけオーセンティケータからの応答を待機します。この時間を超えると認証が再度開始されます（次の EAPoL-Start を送信するなど）。デフォルトは 30 秒です。
- [最大開始（maxStart）] : EAPoL-Start を送信してオーセンティケータを使用してサプリカントが認証を開始する連続回数です（オーセンティケータからの応答を受信せずに）。この回数を超えるとサプリカントはオーセンティケータが存在しないと見なします。これが発生した場合は、サプリカントはデータ トラフィックを許可します。デフォルトは 3 回です。

（注）　このセクションでは、オーセンティケータがクライアント サプリカントに EAP アイデンティティ要求を送信すると認証が開始します。

ステップ 3　[アソシエーション モード（Association Mode）] には、使用するワイヤレス セキュリティ タイプを指定します。

ネットワーク接続タイプの定義

[接続タイプ（Connection Type）] パネルでは、ネットワーク接続タイプの選択およびこのネットワークを使用した接続試行を許可するときの指定（図 4-8 を参照）ができます。[マシン接続（Machine Connection）] オプションでは、接続にマシン接続タイプを定義します。マシン接続はいつでも使用できますが、通常は接続にユーザ クレデンシャルが不要な場合に常に使用します。[ユーザ接続（User Connection）] オプションでは、接続にユーザ接続タイプを定義します。ユーザは、PC へのログイン試行開始した後にだけ接続を確立できます。必須ではありませんが、ユーザ接続では通常ログイン済みのユーザのクレデンシャルを接続の確立に使用します。

マシンおよびユーザ ネットワークは、マシン部分およびユーザ部分から構成されていますが、マシン部分はユーザが PC にログインしていないときにだけ有効です。設定は 2 つの部分に対して同じですが、マシン接続の認証タイプおよびクレデンシャルは、ユーザ接続の認証タイプおよびクレデンシャルと異なる場合があります。

- [マシン接続（Machine Connection）] : ユーザがログオフしていてユーザ クレデンシャルが使用できないときでも、エンド ステーションがネットワークにログインする必要がある場合は、このオプションを選択します。このオプションは、ユーザがアクセスできるようになる前に、ドメインに接続するため、また GPO および他のアップデートをネットワークから取得するために通常は使用されます。

（注）　VPN Start Before Login（SBL）を期待どおりに機能させるには、ユーザが VPN の開始を試行するときにネットワーク接続が存在する必要があることを考慮する必要があります。ネットワーク アクセス マネージャがインストールされている場合、マシン接続を展開して、適切な接続を確実に使用できるようにする必要があります。

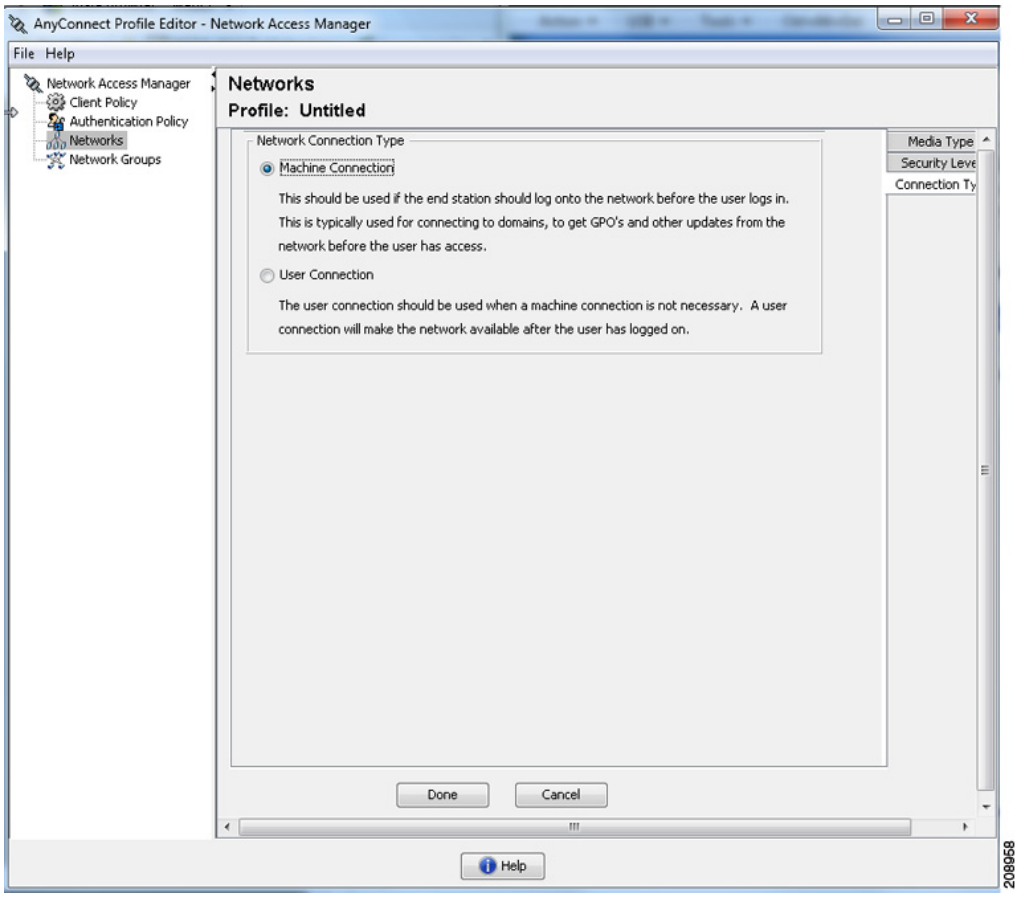
- [ユーザ接続（User Connection）]：マシン接続が不要な場合は、このオプションを選択します。ユーザ接続では、ユーザが PC へのログイン試行を開始した後でネットワークが使用できるようになります。ユーザがその後ログオフすると、ネットワーク接続は終了します。ただし、ユーザ ログオフ後も接続を拡張するように接続が設定されている場合は除きます。

（注）　[クライアント ポリシー接続（Client Policy Connection）] 設定では、ネットワーク アクセス マネージャによってユーザがログインしていると見なすかどうかを決定します（「クライアント ポリシーの設定」（P.4-5）を参照）。[接続の設定（Connection Settings）] が [ユーザ ログインの前に接続を試行（Attempt connection before use logon）] に設定されている場合、ネットワーク アクセス マネージャは、ユーザが入力したクレデンシャルを使用して実際のログイン前にネットワーク接続の確立を試みます。[接続の設定（Connection Settings）] が [ユーザ ログインの後に接続を試行（Attempt connection after use logon）] に設定されている場合、ネットワーク アクセス マネージャは、ユーザが実際にログインするまで待機してからネットワーク接続を確立します。

- [マシンおよびユーザ接続（Machine and User Connection）]：[マシン接続（Machine Connection）] を使用していてユーザがログインしていないとき、および [ユーザ接続（User Connection）] を使用していてユーザがログインしているときにネットワークに PC を常時接続するには、このオプションを選択します。

（注）　オープンおよび共有キー ネットワークの場合は、[マシンおよびユーザ接続（Machine and User Connection）] オプションは使用できません。

図 4-8　[ネットワーク接続タイプ（Network Connection Type）] パネル

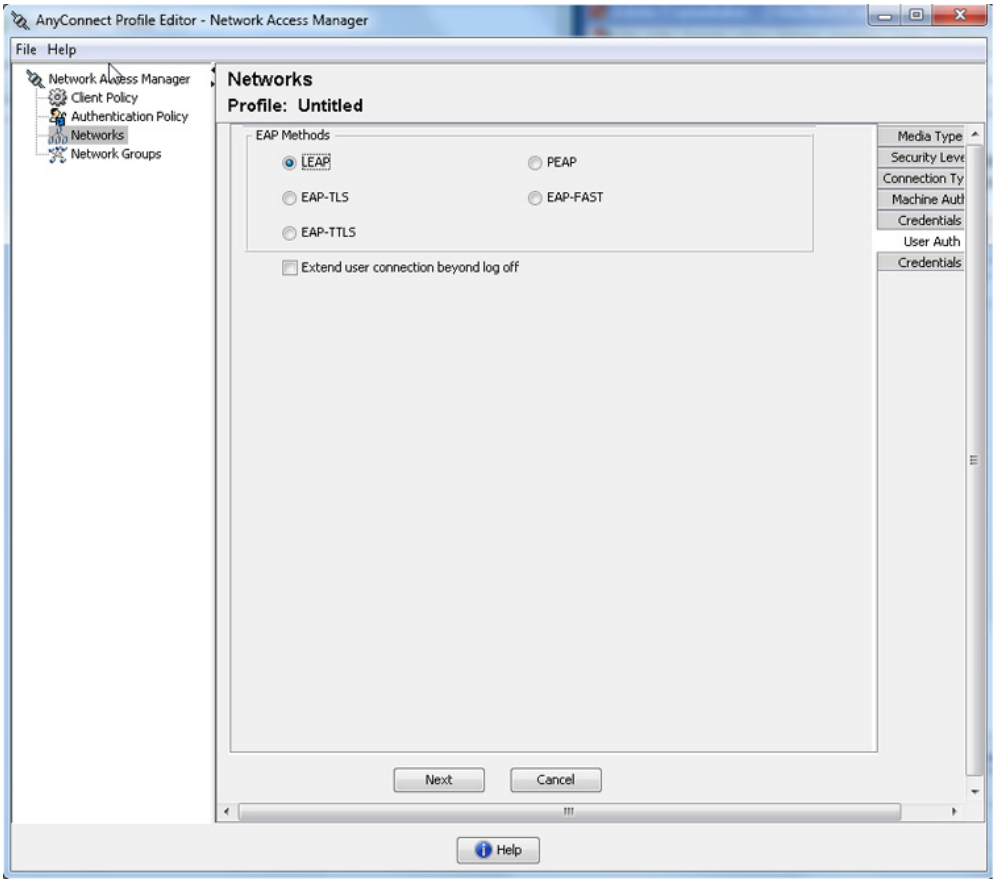


ネットワーク マシンまたはユーザ認証の定義

[マシン認証（Machine Authentication）] または [ユーザ認証（User Authentication）] パネルを使用すると、マシンまたはユーザ（図 4-9 を参照）の認証方式を選択できます。認証方式を指定すると、ウィンドウの中心が選択した方式に適応して、EAP-TLS、EAP-TTLS、EAP-FAST、PEAP、または EAP-GTC に関する詳細を指定するように要求されます。

接続がネットワーク コンピュータのネットワーク アクセス マネージャによって管理されている最中に、ネットワーク コンピュータにリモート アクセスする方法の詳細については、「Windows Remote Desktop の使用」（P.C-7）を参照してください。ここでは、マシン、ユーザ、またはマシンおよびユーザ認証を使用したネットワーク プロファイルについて説明しています。

図 4-9　[マシン認証（Machine Authentication）] または [ユーザ認証（User Authentication）] パネル



（注）　MACsec をイネーブルにした場合は、PEAP、EAP-TLS、または EAP-FAST などの MSK キー導出をサポートする EAP 方式を必ず選択します。

EAP のオプションを選択した場合は、追加設定が必要です。

- EAP-GTC：「EAP-GTC の設定」（P.4-21）を参照してください
- EAP-TLS：「EAP-TLS の設定」（P.4-21）を参照してください。
- EAP-TTLS：「EAP-TTLS の設定」（P.4-22）を参照してください。
- PEAP：「PEAP オプションの設定」（P.4-23）を参照してください。
- EAP-FAST：「EAP-FAST の設定」（P.4-24）を参照してください。

EAP-GTC の設定

EAP-GTC は、単純なユーザ名とパスワード認証に基づく EAP 認証方式です。チャレンジ/レスポンス方式を使用せずに、ユーザ名とパスワードの両方がクリア テキストで渡されます。EAP 方式は、トンネリング EAP 方式の内部で使用（次のトンネリング EAP 方式を参照）、または OTP（トークン）を使用する場合に推奨されます。

EAP-GTC は、相互認証を提供しません。クライアント認証だけを行うため、不正なサーバがユーザのクレデンシャルを取得する可能性があります。相互認証が必要な場合、EAP-GTC は、サーバ認証を提供するトンネリング EAP 方式の内部で使用されます。

キー関連情報は EAP-GTC によって提供されないため、MACsec ではこの方式を使用できません。さらなるトラフィック暗号化のためにキー関連情報が必要な場合、EAP-GTC は、キー関連情報（および必要に応じて内部および外部の EAP 方式の暗号化バインド）を提供するトンネリング EAP 方式の内部で使用されます。

パスワード ソース オプションには、次の 2 つがあります。

- [パスワードを使用した認証（Authenticate using a Password）]：正しく保護されている有線環境にのみ適しています
- [トークンを使用した認証（Authenticate using a Token）]：トークン コードのライフタイムが短い（通常約 10 秒）ため、または OTP であるため、より高いセキュリティを備えています

（注） ネットワーク アクセス マネージャ、オーセンティケータ、または EAP-GTC プロトコルのいずれもパスワードとトークン コード間を区別できません。これらのオプションは、ネットワーク アクセス マネージャ内のクレデンシャルのライフタイムにのみ影響を与えます。パスワードは、ログアウトまでかそれ以降も記憶できますが、トークン コードは記憶できません（認証ごとにユーザがトークン コードの入力を求められるため）。

パスワードが認証に使用される場合、ハッシュ化（または不可逆的に暗号化された）パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。これは、パスワードがオーセンティケータにクリア テキストで渡されるためです。この方式は、データベースがリークしている可能性がある場合に推奨されます。

EAP-TLS の設定

EAP-Transport Layer Security（EAP-TLS）は、TLS プロトコル（RFC 2246）に基づく IEEE 802.1X EAP 認証アルゴリズムです。TLS は、X.509 デジタル証明書に基づく相互認証を使用します。EAP-TLS メッセージ交換は、相互認証、暗号スイート ネゴシエーション、キー交換、クライアントと認証サーバ間の検証、およびトラフィック暗号化に使用できるキー関連情報を提供します。

次のリストに、EAP-TLS クライアント証明書が有線およびワイヤレス接続に強固な認証を提供できる主な理由を示します。

- 通常、ユーザが介入することなく認証が自動で実行される。
- ユーザ パスワードに依存しない。
- デジタル証明書が強固な認証保護を提供する。
- メッセージ交換が公開キー暗号化により保護される。
- ディクショナリ攻撃の被害を受けにくい。
- 認証プロセスにより、データ暗号化および署名のための相互決定されたキーが生成される。

EAP-TLS には、次の 2 つのオプションが含まれています。

- [サーバ証明書の検証（Validate Server Certificate）] : サーバ証明書の検証をイネーブルにします。
- [高速な再接続の有効化（Enable Fast Reconnect）] : TLS セッション再開をイネーブルにします。これにより、TLS セッション データがクライアントとサーバの両方で保持されている限り、短縮化した TLS ハンドシェイクを使用することによってはるかに高速な再認証ができます。

（注）　[スマート カード使用時には無効化（Disable when using a Smart Card）] オプションは、マシン認証では使用できません。

（注）　Windows Vista および Windows 7 では、ユーザがログインするまでスマート カードのサポートは使用できません。

EAP-TTLS の設定

EAP-Tunneled Transport Layer Security（EAP-TTLS）は、EAP-TLS 機能を拡張する 2 フェーズのプロトコルです。フェーズ 1 では、完全な TLS セッションを実行して、フェーズ 2 で使用するセッション キーを導出して、サーバとクライアント間で属性を安全にトンネリングします。フェーズ 2 中には、多数のさまざまなメカニズムを使用する追加認証の実行にトンネリングされた属性を使用できます。

ネットワーク アクセス マネージャは、EAP-TTLS 認証中に使用する内部および外部方式の暗号化バインドをサポートしません。暗号化バインドが必要な場合は、EAP-FAST を使用する必要があります。暗号化バインドは、クレデンシャルを知らなくても攻撃者がユーザの接続をハイジャックできる中間者攻撃の特殊クラスからの保護を提供します。

フェーズ 2 で使用できる認証メカニズムには、次のプロトコルが含まれます。

- PAP（パスワード認証プロトコル）: ピアが双方向ハンドシェイクを使用してそのアイデンティティを証明する単純な方式を提供します。ID/ パスワード ペアは、認証が認められるか失敗するまで、ピアからオーセンティケータに繰り返し送信されます。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証する必要があります。

  パスワードがオーセンティケータに渡されるため、ハッシュ化（または不可逆的に暗号化された）パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。この方式は、データベースがリークしている可能性がある場合に推奨されます。

  （注）　EAP-TTLS PAP は、トークンおよび OTP ベースの認証で使用できます。

- CHAP（チャレンジ ハンドシェイク認証プロトコル）: スリーウェイ ハンドシェイクを使用してピアのアイデンティティを検証します。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証してください。このチャレンジ/ レスポンス方式を使用する場合、オーセンティケータのデータベースにクリア テキスト パスワードを保存する必要があります。
- MS-CHAP（Microsoft CHAP）: スリーウェイ ハンドシェイクを使用してピアのアイデンティティを検証します。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証してください。パスワードの NT-hash に基づいてこのチャレンジ/ レスポンス方式を使用して、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。
- MS-CHAPv2 : 応答パケット内にピア チャレンジおよび成功パケット内にオーセンティケータ応答を含めることによって、ピア間の相互認証を提供します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃を防ぐために）サーバをクライアントの前に認証する必要がある場

合、EAP-TTLS を設定してフェーズ 1 でサーバの証明書を検証する必要があります。パスワードの NT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。

- EAP：次の EAP 方式が使用できます。
  - EAP-MD5（EAP-Message Digest 5）：スリーウェイ ハンドシェイクを使用してピアのアイデンティティを検証します（CHAP と類似）。このチャレンジ/レスポンス方式を使用する場合、オーセンティケータのデータベースにクリア テキスト パスワードを保存する必要があります。
  - EAP-MSCHAPv2：スリーウェイ ハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃の防止のためなどで）サーバをクライアントの前に認証する必要がある場合、EAP-TTLS を設定してフェーズ 1 でサーバの証明書を検証する必要があります。パスワードの NT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。
- EAP-TTLS 設定
  - [サーバ ID の検証（Validate Server Identity）]：サーバ証明書の検証をイネーブルにします。
  - [高速な再接続の有効化（Enable Fast Reconnect）]：内部認証が省略されたかどうか、またはオーセンティケータによって制御されているかどうかに関係なく、外部 TLS セッション再開のみをイネーブルにします。

（注）　[スマート カード使用時には無効化（Disable when using a Smart Card）] オプションは、マシン認証では使用できません。Windows Vista および Windows 7 では、ユーザがログインするまでスマート カードのサポートは使用できません。

- [内部方式（Inner Methods）]：TLS トンネルが作成された後で内部方式の使用を指定します。

PEAP オプションの設定

Protected EAP（PEAP）は、トンネリング TLS ベースの EAP 方式です。PEAP は、内部認証方式の暗号化に対するクライアント認証の前に、サーバ認証に TLS を使用します。内部認証は、信頼される暗号保護されたトンネル内部で実行され、証明書、トークン、およびパスワードを含む、さまざまな内部認証方式をサポートします。ネットワーク アクセス マネージャは、PEAP 認証中に使用する内部および外部方式の暗号化バインドをサポートしません。暗号化バインドが必要な場合は、EAP-FAST を使用する必要があります。暗号化バインドは、クレデンシャルを知らなくても攻撃者がユーザの接続をハイジャックできる中間者攻撃の特殊クラスからの保護を提供します。

PEAP は、次のサービスを提供することによって EAP 方式を保護します。

- EAP パケットに対する TLS トンネル作成
- メッセージ認証
- メッセージの暗号化
- クライアントに対するサーバの認証

次の認証方法を使用できます。

- パスワード
  - EAP-MSCHAPv2：スリーウェイ ハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃の防止のためなどで）サーバをクライアントの前に認証する必要がある場合、PEAP を設定してサーバの証明

書を検証する必要があります。パスワードの NT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。

  - EAP-GTC（EAP Generic Token Card）：ユーザ名とパスワードを伝送するために EAP エンベロープを定義します。相互認証が必要な場合は、PEAP を設定してサーバの証明書を検証する必要があります。パスワードがクリア テキストでオーセンティケータに渡されるため、ハッシュ化（または不可逆的に暗号化された）パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。この方式は、データベースがリークしている可能性がある場合に推奨されます。

- トークン
  - EAP-GTC：トークン コードまたは OTP を伝送するために EAP エンベロープを定義します。
- 証明書
  - EAP-TLS：ユーザ証明書を伝送するために EAP エンベロープを定義します。中間者攻撃（有効なユーザの接続のハイジャック）を避けるため、同じオーセンティケータに対する認証用に PEAP（EAP-TLS）および EAP-TLS プロファイルを混在させないことを推奨します。その設定に応じて、オーセンティケータを設定する必要があります（プレーンおよびトンネリングされた EAP-TLS の両方をイネーブルにしない）。
- PEAP 設定
  - [サーバ ID の検証（Validate Server Identity）] : サーバ証明書の検証をイネーブルにします。
  - [高速な再接続の有効化（Enable Fast Reconnect）] : 外部 TLS セッション再開のみをイネーブルにします。オーセンティケータは、内部オーセンティケータを省略するかどうかを制御します。
- [スマート カード使用時には無効化（Disable when using a Smart Card）] および [トークンと EAP GTC を使用した認証（Authenticate using a Token and EAP GTC）] オプションは、マシン認証では使用できません。
- [クレデンシャル ソースに基づく内部方式（Inner methods based on Credentials Source）] : パスワードまたは証明書を使用する認証が選択できます。
  - [パスワードを使用した認証（Authenticate using a Password）] : [EAP-MSCHAPv2] または [EAP-GTC]
  - [EAP-TLS、証明書を使用（EAP-TLS, using Certificate）]
  - [トークンと EAP GTC を使用した認証（Authenticate using a Token and EAP GTC）]

（注） Windows Vista および Windows 7 では、ユーザがログインするまでスマート カードのサポートは使用できません。

EAP-FAST の設定

EAP-FAST は、IEEE 802.1X 認証タイプで、柔軟性があり、展開や管理も容易です。EAP-FAST は、さまざまなユーザおよびパスワード データベース タイプ、サーバ主導のパスワードの失効と変更、およびデジタル証明書（任意）をサポートします。

EAP-FAST は、証明書を使用せず、ディクショナリ攻撃からの保護を提供する IEEE 802.1X EAP タイプを展開するお客様向けに開発されました。

EAP-FAST は、TLS メッセージを EAP 内にカプセル化します。また、次の 3 つのプロトコル フェーズから構成されます。

1. Authenticated Diffie-Hellman Protocol（ADHP）を使用して Protected Access Credential（PAC）と呼ばれる共有秘密クレデンシャルを持つクライアントをプロビジョニングするプロビジョニング フェーズ。
2. トンネルの確立に PAC を使用するトンネル確立フェーズ。
3. 認証サーバでユーザのクレデンシャル（トークン、ユーザ名 / パスワード、またはデジタル証明書）を認証する認証フェーズ。

他の 2 つのトンネリング EAP 方式とは異なり、EAP-FAST は内部および外部方式間に暗号化バインドを提供して、攻撃者が有効なユーザの接続をハイジャックする特殊な中間者攻撃を防止します。

[EAP-FAST 設定（EAP-FAST Settings）] パネルでは、EAP-FAST 設定ができます。

- EAP-FAST 設定（EAP-FAST Settings）
  - [サーバ ID の検証（Validate Server Identity）] : サーバ証明書の検証をイネーブルにします。これをイネーブルにすると、管理ユーティリティに 2 つの追加のダイアログが導入されて、ネットワーク アクセス マネージャ プロファイル エディタのタスク リストに [証明書（Certificate）] パネルがさらに追加されます。
  - [高速な再接続の有効化（Enable Fast Reconnect）] : セッション再開をイネーブルにします。EAP-FAST で認証セッションをレジュームする 2 つのメカニズムには、内部認証を再開するユーザ認可 PAC、また短縮化した外部 TLS ハンドシェイクができる TLS セッション再開が含まれます。この [高速な再接続の有効化（Enable Fast Reconnect）] パラメータは、両方のメカニズムをイネーブルまたはディセーブルにします。オーセンティケータがいずれを使用するかを決定します。

    （注） マシン PAC は、短縮化した TLS ハンドシェイクを提供し、内部認証を省きます。この制御は、PAC パラメータのイネーブル / ディセーブルによって処理されます。

    （注） Windows Vista および Windows 7 では、ユーザがログインするまでスマート カードのサポートは使用できません。

    （注） [スマート カード使用時には無効化（Disable when using a Smart Card）] オプションは、マシンでは使用できません。

- [クレデンシャル ソースに基づく内部方式（Inner methods based on Credentials Source）] : パスワードまたは証明書を使用する認証ができます。
  - [パスワードを使用した認証（Authenticate using a Password）] : [EAP-MSCHAPv2] または [EAP-GTC] EAP-MSCHAPv2 は、相互認証を提供しますが、サーバを認証する前にクライアントを認証します。サーバを最初に認証する相互認証を使用する場合は、EAP-FAST を認証付きプロビジョニングのみに設定して、サーバの証明書を検証します。パスワードの NT-hash に基づいてこのチャレンジ / レスポンス方式を使用して、EAP-MSCHAPv2 を使用する場合は、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。パスワードが EAP-GTC 内でクリア テキストでオーセンティケータに渡されるため、ハッシュ化（または不可逆的に暗号化された）パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。この方式は、データベースがリークしている可能性がある場合に推奨されます。

パスワード ベースの内部方式を使用している場合、Protected Access Credential（PAC）を使用する追加オプションが適用されます。認証されていない PAC プロビジョニングを許可するか許可しないかを選択します。

- [証明書を使用した認証（Authenticate using a certificate）] : 証明書を使用する認証に対しての基準を、要求された場合にクライアント証明書を暗号化しないで送信、トンネル内でのみクライアント証明書を送信、またはトンネル内で EAP-TLS を使用してクライアント証明書を送信から決定します。
- [トークンと EAP GTC を使用した認証（Authenticate using a Token and EAP GTC）]

- [PAC の使用（Use PACs）] : EAP-FAST 認証での PAC の使用を指定できます。PAC は、ネットワーク認証を最適化するためにクライアントに配布されるクレデンシャルです。

（注）　EAP-FAST では大半の認証サーバが PAC を使用するため、通常は PAC オプションを使用します。このオプションを削除する前に、認証サーバが EAP-FAST で PAC を使用しないことを確認します。使用する場合は、クライアントの認証試行が失敗します。認証サーバが認証された PAC プロビジョニングをサポートする場合は、認証されていないプロビジョニングをディセーブルにすることを推奨します。認証されていないプロビジョニングはサーバの証明書を検証しないため、不正なオーセンティケータがディクショナリ攻撃を開始できます。

1 つ以上の特定の PAC ファイルを配布と認証のために手動で指定するには、[PAC ファイル（PAC Files）] パネルを選択して、[追加（Add）] をクリックします。リストから PAC ファイルを削除するには、PAC ファイルを強調表示して、[削除（Remove）] をクリックします。

[パスワード保護（Password protected）] : PAC がパスワード保護でエクスポートされた場合は、[パスワード保護（Password protected）] チェックボックスをオンにして、PAC が暗号化したファイルのパスワードと一致するパスワードを入力します。

ネットワーク クレデンシャルの定義

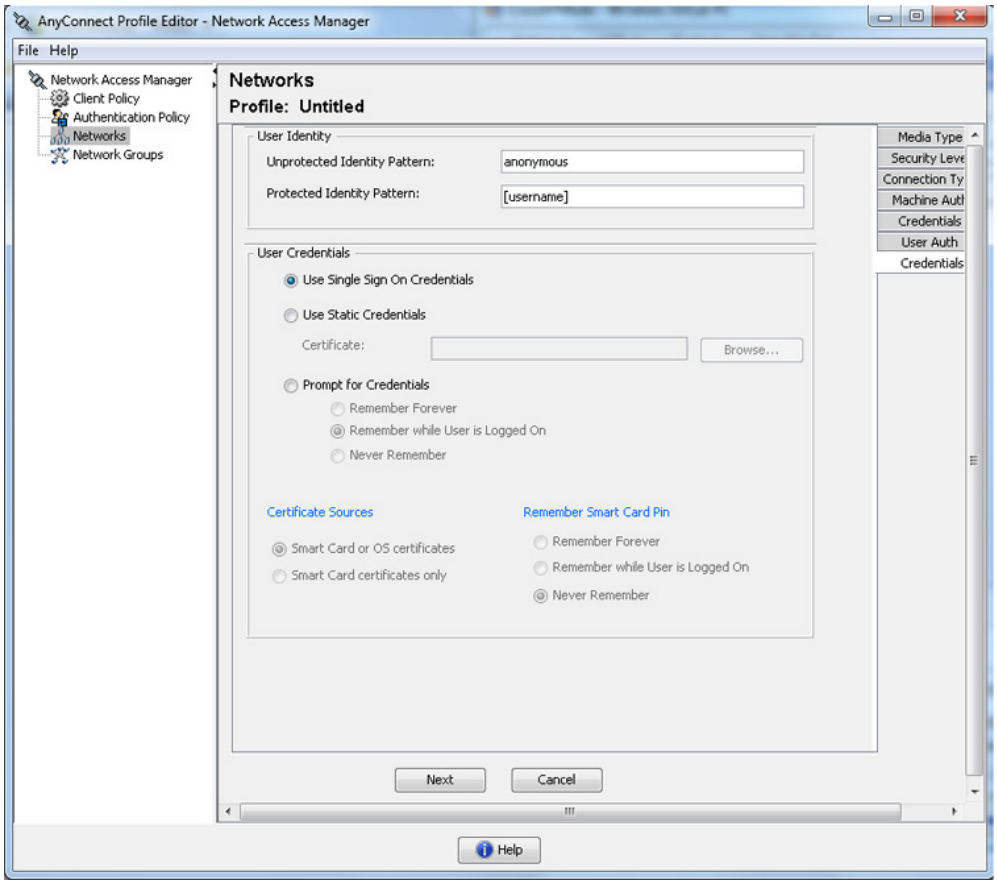
[ネットワーク クレデンシャル（Network Credentials）] では、ユーザまたはマシン クレデンシャルを確立して、信頼サーバの検証規則が確立できます。

- ユーザ クレデンシャルの設定
- マシン クレデンシャルの設定
- 信頼サーバの検証規則の設定

ユーザ クレデンシャルの設定

[クレデンシャル（Credentials）] パネルでは、目的のクレデンシャルを関連付けられたネットワーク（図 4-10 を参照）の認証で使用するために指定できます。

図 4-10　[ユーザ クレデンシャル（User Credentials）] パネル



ステップ 1　[保護されたアイデンティティ パターン（Protected Identity Pattern）] でユーザ アイデンティティを特定する必要があります。ネットワーク アクセス マネージャでは、次のアイデンティティ プレースホルダのパターンがサポートされます。

- [ユーザ名（username）]：ユーザ名を指定します。ユーザが username@domain または domain\username を入力した場合、ドメインの部分は削除されます。
- [未加工（raw）]：ユーザの入力のとおりにユーザ名を指定します。
- [ドメイン（domain）]：ユーザの PC のドメインを指定します。

ユーザ接続の場合に、[ユーザ名（username）] および [ドメイン（domain）] プレースホルダが使用されたときは、常に次の条件が適用されます。

- 認証にクライアント証明書を使用する場合は、[ユーザ名（username）] と [パスワード（password）] のプレースホルダ値はさまざまな X509 証明書プロパティから取得されます。プロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデンティティが userA@cisco.com（ユーザ名 =userA、ドメイン =cisco.com）、マシン認証のアイデンティティが hostA.cisco.com（ユーザ名 =hostA、ドメイン =cisco.com）の場合、次のプロパティが解析さ

れます。

ユーザ証明書に基づいた認証：

- SubjectAlternativeName: UPN = userA@cisco.com
- Subject = .../CN=userA@cisco.com/...
- Subject = userA@cisco.com
- Subject = .../CN=userA/DC=cisco.com/...
- Subject = userA (no domain)

マシン証明書に基づいた認証：

- SubjectAlternativeName: DNS = hostA.cisco.com
- Subject = .../DC=hostA.cisco.com/...
- Subject = .../CN=hostA.cisco.com/...
- Subject = hostA.cisco.com

- クレデンシャル ソースがエンド ユーザの場合、プレースホルダの値はユーザが入力する情報から取得されます。
- クレデンシャルがオペレーティング システムから取得された場合、プレースホルダの値はログイン情報から取得されます。
- クレデンシャルがスタティックの場合は、プレースホルダを使用しないでください。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイデンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の対象になります。典型的な保護されていないアイデンティティのパターンは次のとおりです。

- anonymous@[ドメイン（domain）]：値がクリア テキストで送信されるときに、ユーザ アイデンティティを隠すために、トンネリングされた方式内でよく使用されます。実際のユーザ アイデンティティは、保護されたアイデンティティとして、内部方式で提供されます。
- [ユーザ名（username）]@[ドメイン（domain）]：トンネリングされていない方式の場合

（注） 保護されていないアイデンティティはクリア テキストで送信されます。最初のクリア テキスト アイデンティティ要求または応答が改ざんされた場合は、TLS セッションが確立されるとサーバがアイデンティティを検証できないことを検出することがあります。たとえば、ユーザ ID が無効であるか、または EAP サーバが処理する領域内にない場合があります。

保護されたアイデンティティは、異なる方法でクリア テキスト アイデンティティを表します。userID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正しい領域へのルーティングをイネーブルにするために必要な情報のみを指定する場合があります。典型的な保護されているアイデンティティのパターンは次のとおりです。

- [ユーザ名（username）]@[ドメイン（domain）]
- ユーザのアイデンティティとして使用する実際の文字列（プレースホルダなし）

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデンティティが異なる場合があります（マシン認証の次にユーザ認証が行われるなど）。たとえば、ピアでは最初に nouser@cisco.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシエートされると、そのピアは johndoe@cisco.com のアイデンティティを要求する場合があります。そのため、ユーザのアイデンティティにより保護が提供される場合でも、カンバセーションがローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

ステップ 2　次のユーザ クレデンシャル情報をさらに提供します。

- [シングル サイン オン クレデンシャルの使用（Use Single Sign On Credentials）]：クレデンシャルをオペレーティング システムのログイン情報から取得します。ログイン クレデンシャルが失敗すると、ネットワーク アクセス マネージャは一時的に（次のログインまで）切り替わり、ユーザに GUI でクレデンシャルの入力を求めます。
- [スタティック クレデンシャルの使用（Use Static Credentials）]：ユーザ クレデンシャルをこのプロファイル エディタが提供するネットワーク プロファイルから取得します。スタティック クレデンシャルが失敗すると、ネットワーク アクセス マネージャは、新しい設定がロードされるまでクレデンシャルを再度使用しません。
- [クレデンシャルのプロンプト（Prompt for Credentials）]：クレデンシャルを次に指定されたとおりに AnyConnect GUI を使用してエンド ユーザから取得します。
  - [永久に記憶（Remember Forever）]：クレデンシャルは永久に記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャルの入力を再度求められます。クレデンシャルはファイルに保存され、ローカル マシン パスワードを使用して暗号化されます。
  - [ユーザのログイン中は記憶（Remember while User is Logged On）]：クレデンシャルはユーザがログオフするまで記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャルの入力を再度求められます。
  - [記憶しない（Never Remember）]：クレデンシャルは一切記憶されません。ネットワーク アクセス マネージャは、認証のためにクレデンシャル情報が必要なたびに、ユーザに入力を求めます。

ステップ 3　証明書が要求されたときに、認証のためにいずれの証明書ソースを使用するかを決定します。

- [スマート カードまたは OS の証明書（Smart Card or OS certificates）]：ネットワーク アクセス マネージャは、OS の証明書ストアまたはスマート カードで検出される証明書を使用します。
- [スマート カードの証明書のみ（Smart Card certificates only）]：ネットワーク アクセス マネージャは、スマート カードで検出される証明書のみを使用します。

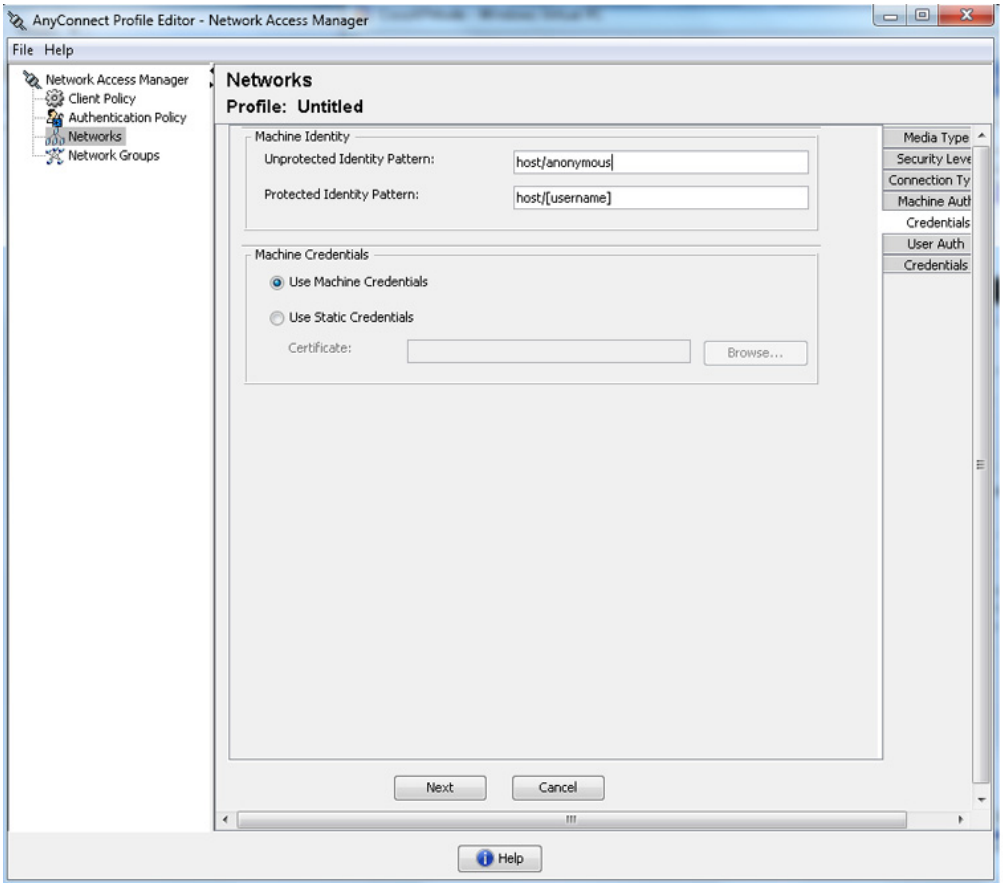
ステップ 4　[スマート カードの PIN の記憶（Remember Smart Card Pin）] パラメータでは、ネットワーク アクセス マネージャがスマート カードから証明書を取得するために使用した PIN を記憶する期間を決定します。使用できるオプションについては、ステップ 2 を参照してください。

（注）　PIN は、証明書自体よりも長く保存されることは決してありません。

マシン クレデンシャルの設定

[クレデンシャル（Credentials）] パネルでは、目的のマシン クレデンシャル（図 4-11 を参照）を指定できます。

図 4-11　　マシン クレデンシャル



ステップ 1　[保護されたアイデンティティ パターン（Protected Identity Pattern）] でマシン アイデンティティを特定する必要があります。ネットワーク アクセス マネージャでは、次のアイデンティティ プレースホルダのパターンがサポートされます。

- [ユーザ名（username）] : ユーザ名を指定します。ユーザが username@domain または domain\username を入力した場合、ドメインの部分は削除されます。
- [未加工（raw）] : ユーザの入力のとおりにユーザ名を指定します。

マシン接続の場合に、[ユーザ名（username）] および [ドメイン（domain）] プレースホルダが使用されたときは、常に次の条件が適用されます。

- 認証にクライアント証明書を使用する場合は、[ユーザ名（username）] と [パスワード（password）] のプレースホルダ値はさまざまな X509 証明書プロパティから取得されます。プロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデンティティが userA@cisco.com（ユーザ名 =userA、ドメイン =cisco.com）、マシン認証のアイデンティティが hostA.cisco.com（ユーザ名 =hostA、ドメイン =cisco.com）の場合、次のプロパティが解析されます。

  ユーザ証明書に基づいた認証：

  - SubjectAlternativeName: UPN = userA@cisco.com
  - Subject = .../CN=userA@cisco.com/...
  - Subject = userA@cisco.com
  - Subject = .../CN=userA/DC=cisco.com/...
  - Subject = userA (no domain)

  マシン証明書に基づいた認証：

  - SubjectAlternativeName: DNS = hostA.cisco.com
  - Subject = .../DC=hostA.cisco.com/...
  - Subject = .../CN=hostA.cisco.com/...
  - Subject = hostA.cisco.com

- クライアント証明書が認証に使用されない場合、クレデンシャルはオペレーティング システムから取得されて、[ユーザ名（username）] プレースホルダは割り当てられたマシン名を表します。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイデンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の対象になります。典型的な保護されていないマシン アイデンティティのパターンは次のとおりです。

- host/anonymous@[ドメイン（domain）]
- マシンのアイデンティティとして送信する実際の文字列（プレースホルダなし）

保護されたアイデンティティは、異なる方法でクリア テキスト アイデンティティを表します。userID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正しい領域へのルーティングをイネーブルにするために必要な情報のみを指定する場合があります。典型的な保護されているマシン アイデンティティのパターンは次のとおりです。

- host/[ユーザ名（username）]@[ドメイン（domain）]
- マシンのアイデンティティとして使用する実際の文字列（プレースホルダなし）

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデンティティが異なる場合があります（マシン認証の次にユーザ認証が行われるなど）。たとえば、ピアでは最初に nouser@cisco.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシエートされると、そのピアは johndoe@cisco.com のアイデンティティを要求する場合があります。そのため、ユーザのアイデンティティにより保護が提供される場合でも、カンバセーションがローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

ステップ 2　次のマシン クレデンシャル情報をさらに提供します。

- [マシン クレデンシャルの使用（Use Machine Credentials）]：クレデンシャルをオペレーティング システムから取得します。

- [スタティック クレデンシャルの使用（Use Static Credentials）]：スタティック クレデンシャルの使用を選択する場合、展開ファイルで送信する実際のスタティック パスワードを指定できます。スタティック クレデンシャルは、証明書ベースの認証には適用されません。

信頼サーバの検証規則の設定

[サーバ ID の検証（Validate Server Identity）] オプションが [EAP] 方式に設定されている場合、[証明書（Certificate）] パネルがイネーブルになって証明書サーバまたは認証局に対する検証規則を設定できます。検証の結果によって、証明書サーバまたは認証局が信頼されるかどうかが決定されます。

証明書サーバの検証規則を定義するには、次の手順を実行します。

ステップ 1　オプション設定が [証明書フィールド（Certificate Field）] および [一致（Match）] カラムに表示されたときに、ドロップダウン矢印をクリックし、目的の設定を強調表示します。

ステップ 2　[値（Value）] フィールドに、値を入力します。

ステップ 3　規則の下で [追加（Add）] をクリックします。

ステップ 4　[信頼された機関の認証（Certificate Trusted Authority）] の部分で、次のいずれかのオプションを選択します。

- [OS にインストールされた任意のルート証明機関を信頼（Trust any Root Certificate Authority (CA) Installed on the OS）]：選択すると、ローカル マシンまたは証明書ストアのみがサーバの証明書チェーン検証の対象になります。
- [ルート証明機関（CA）を含める（Include Root Certificate Authority (CA) Certificates）]

（注）　[ルート証明機関（CA）を含める（Include Root Certificate Authority (CA) Certificates）] を選択した場合は、[追加（Add）] をクリックして CA 証明書を設定にインポートする必要があります。

ネットワーク グループの定義

[ネットワーク グループ（Network Groups）] パネルでは、ネットワーク接続を特定のグループに割り当てられます（図 4-12 を参照）。接続をグループに分類することにより、次の複数の利点がもたらされます。

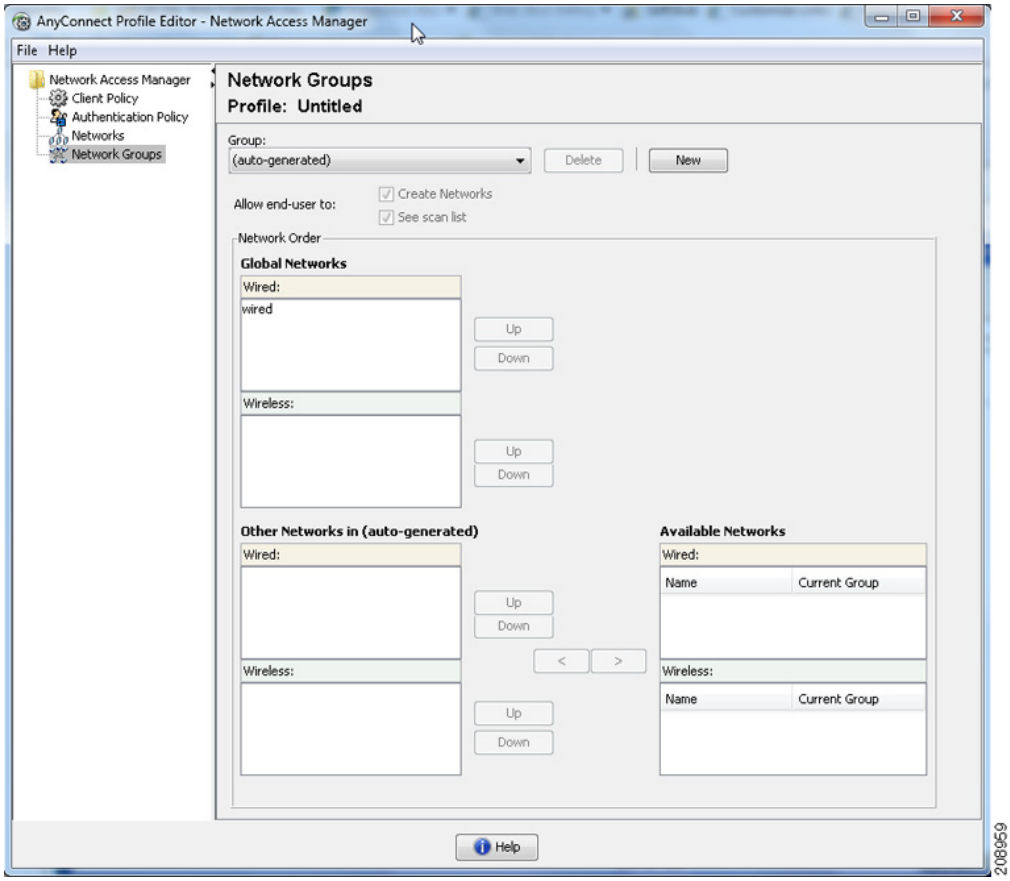
- 接続の確立試行時のユーザ エクスペリエンスの向上。複数の非表示ネットワークが設定された場合、接続が正常に確立するまで、クライアントは非表示ネットワークのリストを定義された順序で順を追って調べます。このような場合に、接続を確立するために必要な時間を大幅に短縮するためにグループが使用されます。
- 設定された接続の管理の簡略化。この利点により、企業内で複数の役割を持つ（または同じ領域に頻繁にアクセスする）ユーザがグループ内のネットワークを調整して選択可能なネットワークのリストを管理しやすくする場合に、管理者ネットワークをユーザ ネットワークから分離できます。

配布パッケージの一部として定義されたネットワークはロックされています。これは、ユーザが設定を編集することや、ネットワーク プロファイルを削除することを防止するためです。

ネットワークをグローバルに定義できます。グローバルに定義すると、ネットワークは [グローバル ネットワーク（Global Networks）] セクションに表示されます。このセクションは、有線とワイヤレス ネットワーク タイプの間で分割されます。このタイプのネットワークに対してのみソート順序編集を実行できます。

すべての非グローバル ネットワークは、グループ内に存在する必要があります。ネットワークが追加されていない場合、事前に定義されているデフォルト グループに追加されます。

図 4-12　[ネットワーク グループ（Network Groups）] ウィンドウ



ステップ 1　ドロップダウン リストから選択して、[グループ（Group）] を選択します。

ステップ 2　[ネットワークの作成（Create networks）] を選択して、エンド ユーザがこのグループ内にネットワークを作成できるようにします。これをオフにした場合、展開されたときにネットワーク アクセス マネージャはこのグループからユーザ作成ネットワークをすべて削除します。これにより、ユーザがネットワーク設定を別のグループに再入力する必要が生じることがあります。

ステップ 3　[スキャン リストの表示（See scan list）] を選択して、AnyConnect GUI を使用してグループがアクティブ グループとして選択されたときに、エンド ユーザがスキャン リストを表示できるようにします。または、このチェックボックスをオフにして、ユーザによるスキャン リストの表示を制限します。たとえば、ユーザが近くのデバイスに誤って接続することを防ぐ必要がある場合に、スキャン リストへのアクセスを制限します。

（注）　これらの設定は、グループごとに適用されます。

ステップ 4　右矢印 [>] および左矢印 [<] を使用して、[グループ（Group）] ドロップダウン リストから選択したグループに対してネットワークを挿入または削除します。ネットワークが現在のグループから移動された場合は、デフォルト グループに配置されます。デフォルト グループを編集する場合、デフォルト グループからネットワークを移動できません（[>] ボタンを使用）。

（注）　指定のネットワーク内で、各ネットワークの表示名は一意である必要があります。このため、1 つのグループには同じ表示名を持つ 2 つ以上のネットワークを含められません。

ステップ 5　[上（Up）] および [下（Down）] 矢印を使用してグループ内のネットワークの優先順位を変更します。