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。

- Windows 7 における有線（IEEE 802.3）、ワイヤレス（IEEE 802.11）、一部のモバイル ブロードバンド（3G）ネットワーク アダプタ。サポート対象アダプタのリスト一式については、『*Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.1*』を参照してください。
- Windows マシン クレデンシャルを使用した事前ログイン認証
- 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 メソッド群：
  - EAP-FAST、PEAP、EAP-TTLS、EAP-TLS、および LEAP（IEEE 802.3 有線のみ EAP-MD5、EAP-GTC、および EAP-MSCHAPv2）
- 内部 EAP メソッド群：
  - 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 メソッド（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 対応の唯一のアダプタは、Cisco CB21AG on Windows XP です。

- スマートカード提供クレデンシャル。AnyConnect は、次の環境でスマート 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（CNG）
  - Windows ログオンは ECDSA 証明書に対応していないため、ネットワーク アクセス マネージャのシングル サインオン（SSO）は ECDSA クライアント証明書に対応していません。

（注）　ネットワーク アクセス マネージャは MAC または Linux には対応していません。

Suite B および FIPS

次の機能は FIPS 認定で、例外を列挙しています。

- ACS および ISE は SuiteB には対応していませんが、FreeRADIUS 2.x + OpenSSL 1.x は対応しています。Microsoft NPS 2008 は Suite-B に一部対応しています（NPS の証明書は RSA でなければなりません）。
- 802.1X/EAP は（RFC5430 で定義されているように）暫定 Suite B プロファイルにのみ対応しています。TLS 1.2 には対応していません。
- MACsec は Windows 7 でのみ FIPS 対応です。
- Windows 7 および XP の Elliptic Curve Diffie-Hellman（ECDH）キー交換
- ECDSA クライアント証明書は Windows 7 および Vista のみに対応しています
- OS ストアの ECDSA CA 証明書は Windows 7 および Vista のみに対応しています。
- PEM エンコードされた）ネットワーク プロファイルの ECDSA CA 証明書は Windows XP/7/Vista に対応しています。
- サーバの ECDSA 証明書チェーン検証は Windows XP/7/Vista に対応しています。

シングル サインオン「シングル ユーザ」の適用

Microsoft Windows XP、Windows 7 および Vista では、複数のユーザが同時にログインできますが、AnyConnect ネットワーク アクセス マネージャはネットワーク認証を 1 人のユーザに制限しています。AnyConnect ネットワーク アクセス マネージャは、ログインしているユーザの数に関係なく、デスクトップまたはサーバ当たり 1 人のユーザにのみアクティブにできます。シングル ユーザ ログインの適用は、いつでもシステムにログインできるユーザは 1 人のみで、管理者は現在ログインしているユーザを強制的にログオフできないことを示しています。

ネットワーク アクセス マネージャ クライアント モジュールが Windows デスクトップにインストールされている場合、デフォルト動作はシングル ユーザ ログインを適用することです。サーバにインストールされている場合、デフォルト動作はシングル ユーザ ログインの適用を緩和することです。 いずれの場合も、レジストリ キーを変更または追加して、デフォルト動作を変更できます。

シングル サインオンのシングル ユーザの適用には、次の機能と制限事項があります。

- Windows 管理者は、現在ログインしているユーザの強制的なログオフが制限されます。
- 接続されたワークステーションへの RDP は同一ユーザにサポートされています。
- 同一ユーザと見なされるためには、クレデンシャルを同じフォーマットにする必要があります。たとえば、me/mydomain は me@mydomain.com と同じではありません。
- また、スマートカード ユーザが同じ PIN を持っている場合、同一ユーザと見なされます。

シングル サインオンのシングル ユーザの適用の設定

Window のワークステーションまたはサーバによる複数ユーザの処理方法を変更したい場合は、レジストリの EnforceSingleLogon の値を変更します。ネットワーク アクセス マネージャはそのキーを Windows XP に追加しませんが、Windows ログイン アクセスを変更する場合は追加できます。レジストリ キーは EnforceSingleLogon で、OverlayIcon レジストリ キーと同じ場所にあります。値 1 は、シングル ユーザ ログインが適用されていることを示し、値 0 は複数ユーザがログインしている可能性があることを示します。

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 6.8

（注） スタンドアロン ネットワーク アクセス マネージャ エディタが、ネットワーク アクセス マネージャ プロファイルを設定する代替方法としてサポートされています。セキュリティ上の理由で、AnyConnect は、AnyConnect プロファイル エディタ外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 マネージャに対応しています。
  - 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）、IPv6 および Suite-B はサポート対象外
  - Windows Server 2008 R2

ライセンスとアップグレード要件

シスコ ワイヤレス アクセス ポイント、ワイヤレス LAN コントローラ、スイッチ、RADIUS サーバで使用する場合は、AnyConnect ネットワーク アクセス マネージャは無償でライセンスが与えられています。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 マネージャの展開

ネットワーク アクセス マネージャは AnyConnect の一部として展開されます。AnyConnect のインストール方法、またネットワーク アクセス マネージャと他のモジュールについては、「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 プロファイルの作成

ネットワーク アクセス マネージャ プロファイルは AnyConnnect の一部としてエンドポイントで展開されているため、ネットワーク アクセス マネージャは管理上定義されたエンド ユーザ要件および認証ポリシーを適用でき、エンド ユーザは事前設定されたネットワーク プロファイルを利用できます。

ネットワーク アクセス マネージャ プロファイル エディタを使用して、1 つ以上のネットワーク アクセス マネージャ プロファイルを作成し、設定します。AnyConnect には ASDM の一部であるプロファイル エディタが、スタンドアロン Windows 版として組み込まれています。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。

（注） クライアント イメージをアップロードするまで、クライアント プロファイルを作成できません。

ASDM からの新しいプロファイルの追加

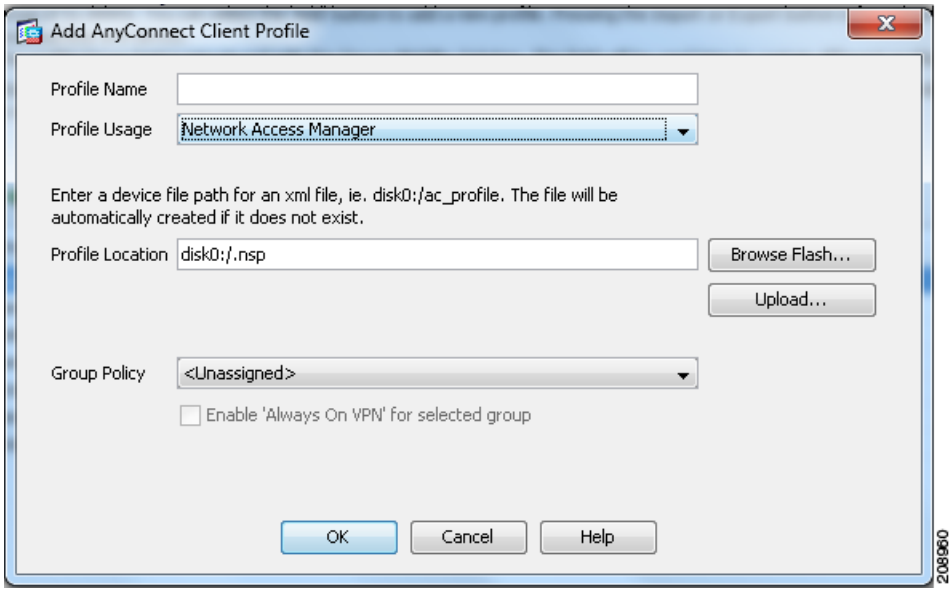
次の手順を実行して、新しいネットワーク アクセス マネージャ クライアント プロファイルを ASDM から ASA に追加します。

ステップ 1　ASDM を開いて [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Client Profile] を選択します。

ステップ 2　[Add] をクリックします。

ステップ 3　[Add AnyConnect Client Profile] ウィンドウが開きます（図 4-1 を参照）。

図 4-1　[Add AnyConnect Client Profile] ウィンドウ



ステップ 4　プロファイル名を入力します。

ステップ 5　[Profile Usage] ドロップダウン リストから、[Network Access Manager] を選択します。

ステップ 6　（任意）[Profile Location] フィールドで [Browse Flash] をクリックし、ASA の XML ファイルのデバイス ファイル パスを選択します。

ステップ 7　（任意）スタンドアロン エディタを使用してネットワーク アクセス マネージャ プロファイルを作成した場合、[Upload] をクリックして、そのプロファイル定義を使用します。

ステップ 8　（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 9　[OK] をクリックします。

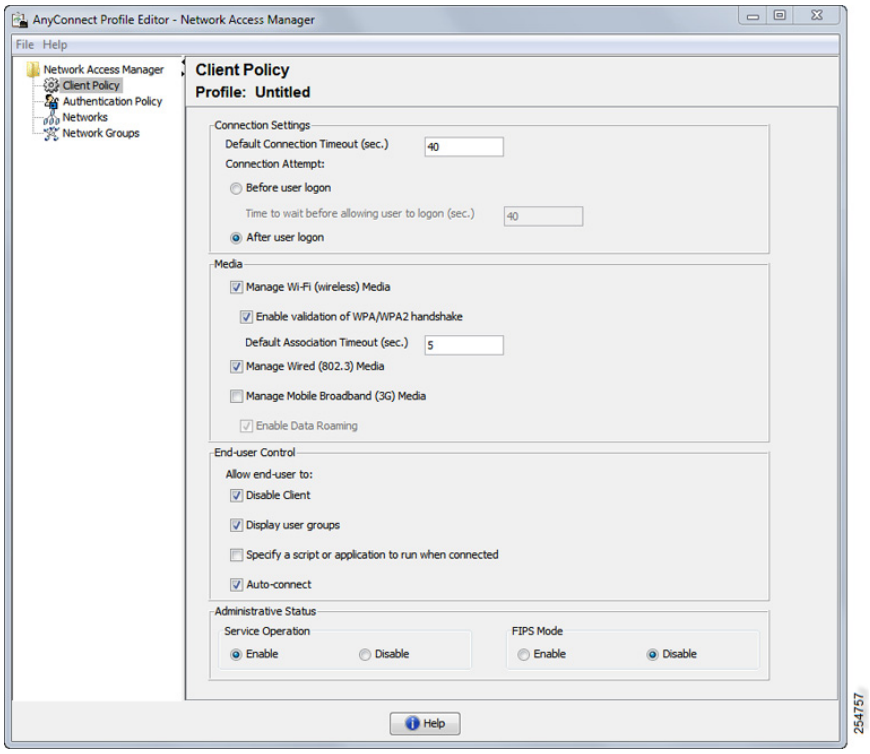
ネットワーク アクセス マネージャ プロファイルの設定

ネットワーク アクセス マネージャ プロファイルは、ネットワーク アクセス マネージャ プロファイル エディタで設定されます。このエディタは ASDM でスタンドアロン Windows アプリケーションとして使用できます。

[Client Policy] ウィンドウ

[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　[Client Policy] ウィンドウ



次の 4 つのセクションで構成されます。

- [Connection Settings]：ユーザ ログインの前または後にネットワーク接続しようとするかどうかを定義できます。
  - [Default Connection Timeout]：ユーザ作成ネットワークの接続タイムアウトとして使用する秒数。デフォルト値は 40 秒です。
  - [Before User Logon]：ユーザがログインする前にネットワークに接続します。サポートされているユーザ ログインの種類として、ユーザ アカウント（Kerberos）認証、ユーザ GPO のロード、GPO ベースのログイン スクリプト実行があります。

    [Before User Logon] を選択した場合、[Time to Wait Before Allowing a User to Logon] も設定することになります。

    [Time to Wait Before Allowing User to Logon]：ネットワーク アクセス マネージャが完全にネットワーク接続するのに待機する最大（最悪のケース）秒数を指定します。この時間内にネットワーク接続が確立できない場合、Windows ログイン プロセスはユーザ ログインにより継続されます。デフォルトは 5 秒です。

（注）　ワイヤレス接続を管理するようネットワーク アクセス マネージャが設定されている場合、[Time to wait before allowing user to logon] を 30 秒以上に設定します。ワイヤレス接続の確立にさらに時間が必要になる可能性があるためです。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。

  - [After User Logon] : ユーザが Windows にログインした後に、ネットワーク アクセス マネージャがネットワーク接続を確立しようとすることを指定します。

- [Media] : ネットワーク アクセス マネージャ クライアントにより制御されるメディアの種類を指定します。
  - [Manage Wi-Fi (wireless) Media] : WiFi メディアの管理、また任意で WPA/WPA2 ハンドシェイクの検証ができるようになります。

    IEEE 802.11i ワイヤレス ネットワーキング規格は、サプリカント（ここではネットワーク アクセス マネージャ）が、キー導出中に IEEE 801.X プロトコル パケットの EAPOL Key データで送信されたアクセス ポイントの RSN IE（Robust Secure Network Information Exchange）がビーコン / プローブ応答フレームで検出されたアクセス ポイントの RSN IE と一致することを検証する必要があることを指定します。WPA/WPA2 ハンドシェイクの検証を有効にする場合、デフォルトのアソシエーション 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有効化をオフにすると、この検証手順は省略されます。

    （注）　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。

  - [Manage Wired (IEEE 802.3) Media] : 有線接続の管理を有効にします。
  - [Manage Mobile Broadband (3G) Media] : Windows 7 モバイル ブロードバンド アダプタの管理を有効にし、データ ローミングを許可するか指定します。この機能はベータ版に入っています。

    （注）　Cisco TAC は、ベータ版には対応していません。

- [End-user Control] : ユーザの次の制御を設定できます。
  - [Disable Client] : ユーザは、AnyConnect UI を使用して、ネットワーク アクセス マネージャによる有線メディアおよびワイヤレス メディアの管理を無効および有効にできます。
  - [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。
  - [Specify a Script or Application To Run When Connected] : ユーザは、ネットワーク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指定できます。

（注）　スクリプト設定は 1 つのユーザ設定ネットワークに固有であり、ユーザはローカル ファイル（.exe、.bat、または .cmd）を指定して、そのネットワークが接続状態になった時に実行できます。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、ユーザが実行中のスクリプトを設定できないようにする場合、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。

  - [Auto-connect]：選択されている場合、ユーザが選択しなくても、ネットワーク アクセス マネージャは自動的にネットワークに接続します。デフォルトは自動接続です。

- Administrative Status
  - [Service Operation]：このサービスを無効にすると、このプロファイルを使用しているクライアントはレイヤ 2 接続を確立するために接続できません。
  - [FIPS Mode]：連邦情報処理標準（FIPS 140-2 Level 1）は米国 政府の規格で、暗号化モジュールのセキュリティ要件を指定します。FIPS モードを有効にすると、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操作を行います。追加情報については、第 9 章「NGE、FIPS、および追加セキュリティ」を参照してください。

    FIPS は、次の表に示すようにソフトウェアとハードウェアの種類に応じて、MACsec または Wifi 向けのネットワーク アクセス マネージャによりサポートされています。

表 4-1　ネットワーク アクセス マネージャによる FIPS サポート

メディア/オペレーティング システム	Windows XP/2003	Windows 7/Vista
MACsec で有線	FIPS に準拠していません。	Intel HW MACsec 対応 NIC の場合、またはハードウェア以外の MACsec を使用している場合に FIPS に準拠しています。
Wifi	3eti ドライバがインストールされている場合に FIPS に準拠しています。	FIPS に準拠していません。

[Authentication Policy] ウィンドウ

[Authentication Policy] ウィンドウでは、すべてのネットワーク接続に適用される、アソシエーションおよび認証ネットワーク フィルタを作成できます。アソシエーション モードまたは認証モードのいずれもオンにしない場合、認証 wi-fi ネットワークに接続できません。モードのサブセットを選択すると、それらのタイプのネットワークにのみ接続できます。目的のアソシエーション モードまたは認証モードをそれぞれ選択するか、[Select All] を選択します。

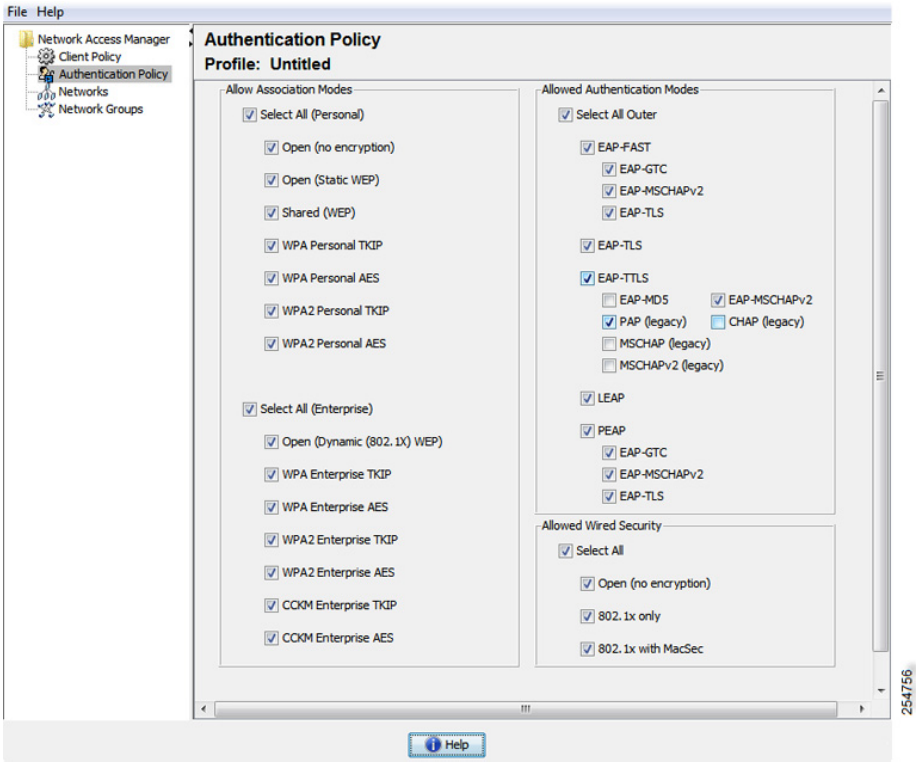
内部方式も特定の認証プロトコルのみに制限される可能性がある点に注意してください。内部方式は、[Allowed Authentication Modes] ペインの外部方式（トンネリング）下にインデントされて表示されます。

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。

内部トンネリングに使用できる EAP 方式は、内部方式のクレデンシャル タイプと外部トンネリング方式に基づいています。次のリストで、外部トンネル方式はそれぞれ、各クレデンシャル タイプに対応した内部方式の種類を一覧表示しています。

- PEAP
  - パスワード クレデンシャル：EAP-MSCHAPv2 または EAP-GTC
  - トークン クレデンシャル：EAP-GTC
  - 証明書クレデンシャル：EAP-TLS
- EAP-FAST
  - パスワード クレデンシャル：EAP-MSCHAPv2 または EAP-GTC
  - トークン クレデンシャル：EAP-GTC
  - 証明書クレデンシャル：EAP-TLS
- EAP-TTLS
  - パスワード クレデンシャル：EAP-MSCHAPv2、EAP-MD5、PAP（L）、CHAP（L）、MSCHAP（L）、MSCHAP-v2（レガシー）
  - トークン クレデンシャル：PAP（レガシー）チャレンジ/レスポンス方式はトークン ベースの認証には適していないため、NAM でサポートされるデフォルト トークン オプションは PAP です。
  - 証明書クレデンシャル：該当なし

図 4-3　[Authentication Policy] ウィンドウ



[Networks] ウィンドウ

[Networks] ウィンドウでは、企業ユーザの事前定義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。[Networks] ウィンドウでは、ウィザードが起動して既存のウィンドウにペインが追加される場合があり、[Next] をクリックして詳細な設定オプションに進みます。

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。[Network Groups] ウィンドウの [*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。グローバル ネットワーク 内にあるネットワークを制御できるため、ユーザ定義のネットワーク内にある場合でも、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。エンド ユーザは管理者が設定したネットワークを変更したり、削除したりできません。

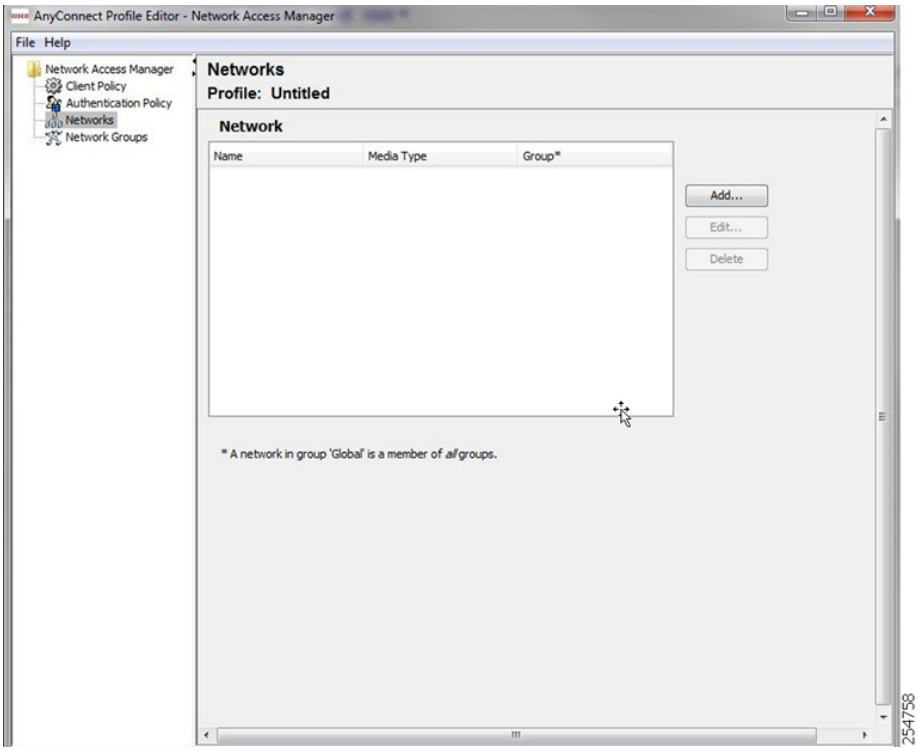
（注） エンド ユーザは、globalNetworks セクションのネットワークを除き、グループにネットワークを追加できます。これらのネットワークはすべてのグループ内に存在し、プロファイル エディタを使用してしか作成できないためです。

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 グループは設定内の最初のグループですが、グループが 1 つしか使用できない場合、アクティブ グループは認識されず、表示されません。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。ユーザはアクティブ グループから選択でき、設定は再起動後も保持されます。[Network Groups] ウィンドウの [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分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 [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。

[Network Access Manager] メニューから [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　[Networks] ウィンドウ



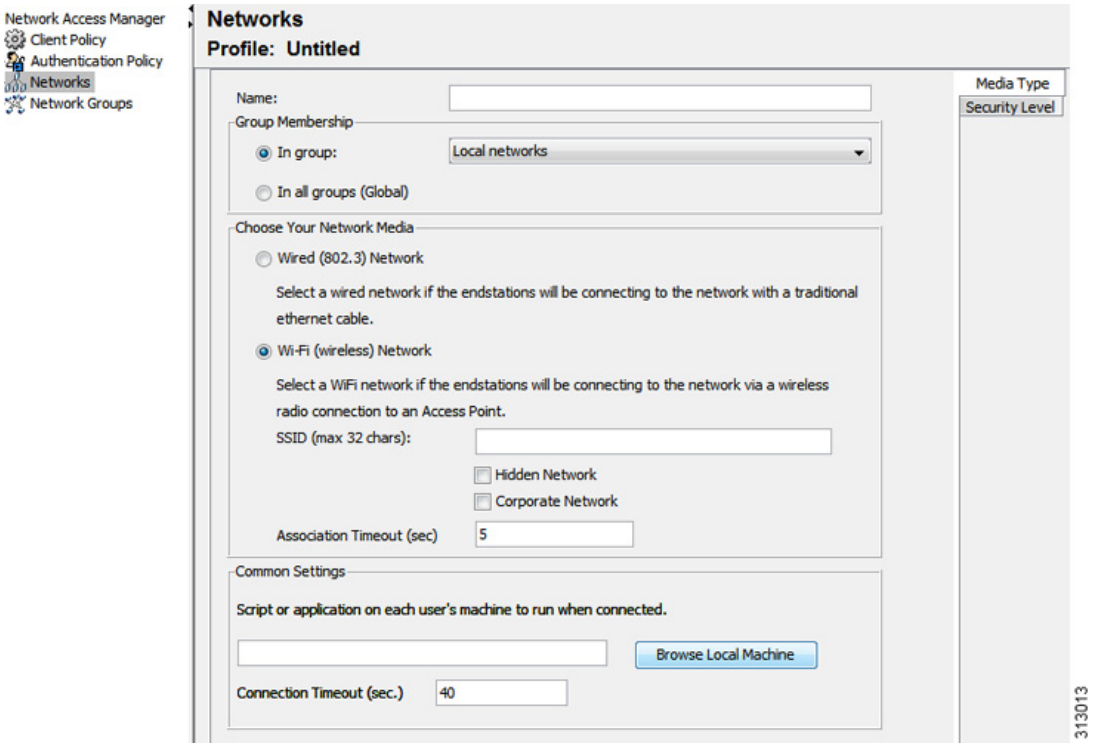
次のいずれかのアクションを選択します。

- 新しいネットワークを作成するには、[Add] をクリックします。新しいネットワークを作成する場合、次の項の情報を使用して、クライアント プロファイルを設定します。まず、次の項 [Networks] - [Media Type] ページから始めます。
- 変更するネットワークを選択して、[Edit] をクリックします。
- 削除するネットワークを選択して、[Delete] をクリックします。

[Networks] - [Media Type] ページ

[Networks] ウィンドウの [Media Type] ページにより、有線ネットワークまたはワイヤレス ネットワークを作成または編集できます。設定は、有線を選択するか、ワイヤレスを選択するかによって異なります。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　[Media Type] ページ



最初のダイアログでは、セクションは 4 つあります。

- [Group Membership]：このプロファイルが使用できるはずであるネットワーク グループ（複数の場合もあり）を選択します。
- [Name]：このネットワークに表示される名前を入力します。
- [Network Media]：[Wired] または [Wi-Fi (wireless)] を選択します。[Wi-Fi] を選択すると、次のパラメータも設定できます。
  - SSID パラメータで、ワイヤレス ネットワークの SSID（Service Set Identifier）を入力します。
  - ネットワークの SSID をブロードキャストしていなくても、ネットワークに接続させる場合は [Hidden Network] を選択します。
  - 企業ネットワークが近くにある場合、最初に Corporate として設定されたネットワークへ強制的に接続する場合は [Corporate Network] を選択します。企業ネットワークが非ブロードキャスト（非表示）SSID を使用し、非表示として設定されている場合、NAM は非表示 SSID をアクティブにプローブし、企業の SSID が圏内にある場合、接続を確立します。
  - [Association Timeout]：ネットワーク アクセス マネージャが、使用できるネットワークを再評価するまで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時間を入力します。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。

- [Common Settings] :
  - [Script or application] : ローカル システムで実行するファイルのパスとファイル名を入力するか、フォルダを参照してファイルを選択します。次のルールは、スクリプトおよびアプリケーションに適用されます。

    .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、管理者が作成したネットワークで定義されたスクリプトまたはアプリケーションは変更できません。

    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、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。
  - [Connection Timeout] : ネットワーク アクセス マネージャが、（接続モードが自動の場合）別のネットワークに接続しようとする、または別のアダプタを使用するまで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） 認証を完了するまでに 60 秒近くかかるスマートカード認証システムもあります。スマートカードを使用している場合、特に、スマートカードが接続に成功するまでにいくつかネットワークに接続しなければならない場合に、[Connection Timeout] 値を増やさなければならない場合があります。

ネットワーク接続に関する注意事項

ネットワーク アクセス マネージャは、エンド ユーザのネットワーク スキャン リストで見つかった設定済みネットワークにのみ接続しようとします。

Windows 7 では、ネットワーク アクセス マネージャは非表示 SSID をプローブします。最初の非表示 SSID が見つかると、検索を中止します。複数の非表示ネットワークが設定されている場合、ネットワーク アクセス マネージャは次のように SSID を選択します。

- 管理者が定義した最初の非表示企業ネットワーク
- 管理者が定義した非表示ネットワーク
- ユーザが定義した最初の非表示ネットワーク

ネットワーク アクセス マネージャは一度に 1 つの非ブロードキャスト SSID しかプローブしないため、サイトの非表示企業ネットワークは 1 つのみにすることをお勧めします。

ネットワークの設定が完了したら、[Next] をクリックして、[Networks] ウィザードの [Security Level] ペインを表示します。

[Networks] - [Security Level] ページ

[Networks] ウィザードの [Security Level] ページで、[Open Network]、[Authentication Network]、または（ワイヤレス ネットワーク メディアにのみ表示された）[Shared Key Network] を選択します。これらのネットワーク タイプの設定フローはそれぞれ異なっており、次の項で説明します。

- [Authenticating Network] の設定：**セキュアな企業**にお勧めします。
- オープン ネットワークの設定：お勧めしませんが、キャプティブ ポータル環境からゲスト アクセスをする場合に使用できます。
- 共有キー ネットワークの設定：**小規模オフィス**または自宅のオフィスなど、ワイヤレス ネットワークにお勧めします。

[Authenticating Network] の設定

[Security Level] セクションで [Authenticating Network] を選択した場合、以下に説明するペインが追加で表示されます。このペインの設定を完了したら、[Next] ボタンをクリックするか、[Connection Type] タブを選択して [Network Connection Type] ダイアログを開きます。

[802.1X Settings] ペイン

ネットワーク設定に応じて IEEE 802.1X 設定を調整します。

- [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。
- [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。
- [startPeriod(sec)]：EAPOL-Start メッセージに対する応答をオーセンティケータから受信しない場合に、EAPOL-Start メッセージを再送信する間隔（秒）です。
- [maxStart]：サプリカントが、オーセンティケータがいないと見なす前に、IEEE 801.X プロトコル パケット、EAPOL Key データ、EAPoL-Start を送信することで、サプリカントがオーセンティケータの認証を開始する回数です。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、[startPeriod] および [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（[startPeriod] x [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（[startPeriod] x [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 トラフィックを行いたい管理者は、認証の開始に費やした総時間がネットワーク接続タイマーより長くなるような startPeriod および maxStart になるようにします（[start Period x maxStart] > [Network Connection Timer]）。

[Security] ペイン

有線ネットワークの場合のみ表示されます。

[Security] ペインで、次のパラメータの値を選択します。

- [Key Management]：ドロップダウン リストを使用して、MACsec 対応有線ネットワークで使用するキー管理プロトコルを決定します。
  - [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 キー管理プロトコル ポリシーと暗号キーをネゴシエートしようとします。MACsec は MAC レイヤ セキュリティで、有線ネットワークで MAC レイヤ暗号化を行います。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。

- Encryption
  - [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]：このオプションは、キー管理に MKA を選択した場合のみ使用できます。ES-GCM-128 を使用して、データ トラフィックが暗号化されます。

[Port Authentication Exception Policy] ペイン

有線ネットワークの場合のみ表示されます。

[Port Authentication Exception Policy] では、認証プロセス中の IEEE 802.1x サプリカントの動作を変更できます。ポート例外が有効でない場合、サプリカントはその既存の動作を続け、設定が完全に成功した場合のみ（または、この項で前述したように、オーセンティケータからの応答がない状態で maxStarts 数の認証が開始された後に）ポートを開きます。次のいずれかのオプションを選択します。

- [Allow data traffic before authentication]：このオプションにより、認証試行の前にデータ トラフィックが許可されます。
- [Allow data traffic after authentication even if]：次の場合でもデータ トラフィックが許可されます。
  - [EAP Fails]：選択すると、EAP が失敗した場合でも、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 succeeds but key management fails]：選択すると、EAP は成功してキー管理が失敗した場合、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 またはスイッチの設定については、『*Catalyst 3750-X and 3560-X Switch Software Configuration Guide*』を参照してください。

アソシエーション モード

ワイヤレス ネットワークの場合のみ表示されます。

アソシエーション モードを選択します。オプションは次のとおりです。

- WEP
- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA 2 Enterprise (TKIP)
- WPA 2 Enterprise (AES)
- [CCKM (TKIP)]：（Cisco CB21AG ワイヤレス NIC が必要）
- [CCKM (AES)]：（Cisco CB21AG ワイヤレス NIC が必要）

オープン ネットワークの設定

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　[Security Level] ページで [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　[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。[Networks] - [Network Connection Type] ペインを参照してください。

[Next] をクリックするか [Connection Type] タブを選択すると、[Network Connection Type] ダイアログが開きます。

共有キー ネットワークの設定

Wi-Fi ネットワークは、エンド ポイントとネットワーク 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、暗号キーを導出する場合に共有キーを使用することがあります。WPA または WPA2 Personal を備えた共有キーを使用すると、小規模オフィスや自宅オフィスに適した Medium レベルのセキュリティ クラスが実現します。

（注）　共有キーによるセキュリティは、企業ワイヤレス ネットワークにはお勧めしません。

セキュリティ レベルを [Shared Key Network] にする場合は、次の手順を実行します。

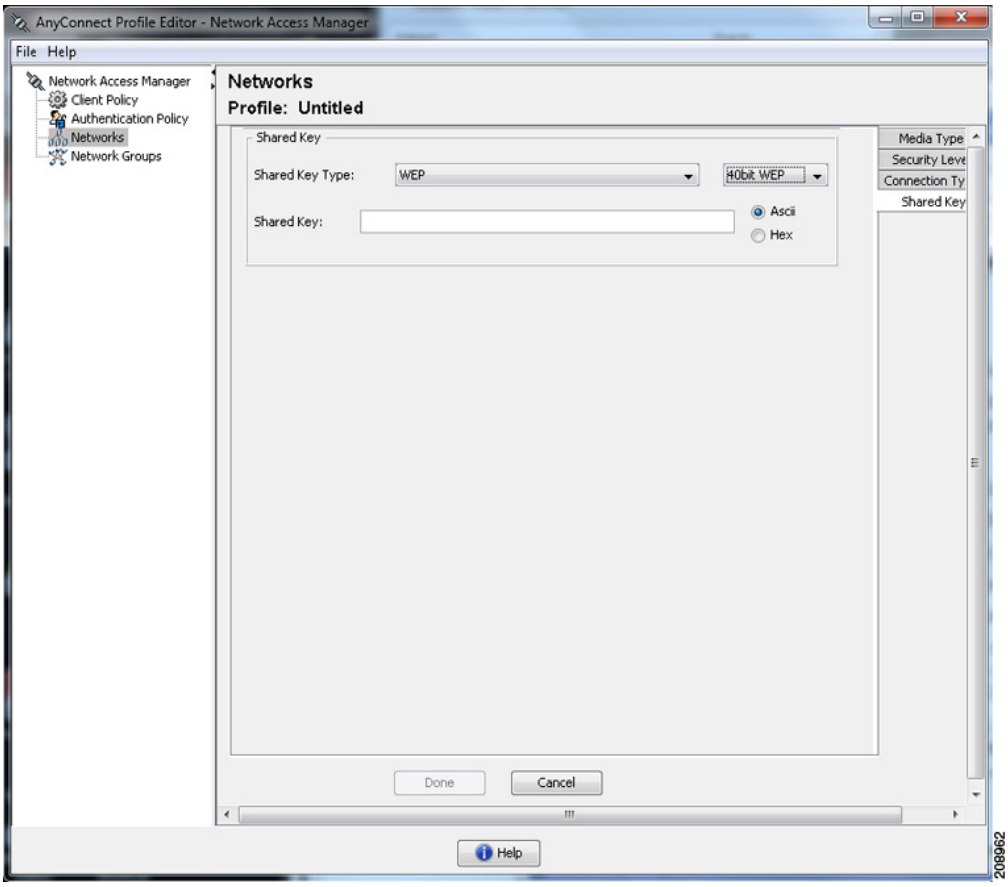
ステップ 1　[Shared Key Network] を選択します。

ステップ 2　[Security Level] ウィンドウで [Next] をクリックします。

ステップ 3　[User Connection] または [Machine Connection] を指定します。詳細については、「[Networks] - [Network Connection Type] ペイン」（P.4-19）を参照してください。

ステップ 4　[Next] をクリックします。[Shared Key] ペインが表示されます（図 4-6 を参照）。

図 4-6　[Shared Key] ペイン



ステップ 5　[Shared Key Type]：共有キーのタイプを決定する共有キー 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 暗号化とのレガシー IEEE 802.11 オープン システム アソシエーション
- [Shared]：スタティック WEP 暗号化とのレガシー IEEE 802.11 共有キー アソシエーション
- [WPA/WPA2-Personal]：パスフレーズ事前共有キー（PSK）から暗号キーを導出する Wi-Fi セキュリティ プロトコル

ステップ 6　レガシー IEEE 802.11 WEP または共有キーを選択した場合は、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 を選択した場合は、（TKIP/AES）を使用する暗号化のタイプを選択し、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、[Hexadecimal] を選択します。

ステップ 8　[Done] をクリックします。[OK] をクリックします。

[Networks] - [Network Connection Type] ペイン

ここでは、ネットワーク アクセス マネージャ プロファイル エディタのセキュリティ レベルに続いて、[Networks] ウィンドウの [Network Connection Type] ペインについて説明します。オープン ネットワークのペインを図 4-7 に示します。次のいずれかの接続タイプを選択します。

- [Machine Connection] : マシンの Windows Active Directory ID を認証に使用します。マシン接続は通常、接続時にユーザ クレデンシャルが必要ない場合に使用します。ユーザがログオフし、ユーザ クレデンシャルが使用できない場合でも、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にこのオプションを選択します。このオプションは通常、ユーザがアクセスする前に、ドメインに接続し、ネットワークから GPO および他のアップデートを取得する場合に使用します。

  （注） 既知のネットワークが使用できない場合、VPN start before login（SBL）は失敗します。しかし、ネットワーク アクセス マネージャを [*Before user logon*] に、またマシン接続認証を設定している場合、ネットワーク アクセス マネージャはユーザにネットワーク情報を要求し、VPN SBL は正常に行われます。

- [User Connection] : ユーザ クレデンシャルを認証に使用します。

  [Client Policy] ペインで [*Before user logon*] が選択された場合、Windows スタート画面でユーザがログオン クレデンシャルを入力した後、ネットワーク アクセス マネージャはユーザのクレデンシャルを収集します。Windows がユーザの Windows セッションを開始している間に、ネットワーク接続が確立されます。

  [Client Policy] ペインで [*After user logon*] が選択された場合、ユーザが Windows にログインしてから、接続が開始されます。

  ユーザがログオフすると、現在のユーザのネットワーク接続は終了します。マシン ネットワーク プロファイルが使用できる場合、NAM はマシン ネットワークに再接続します。

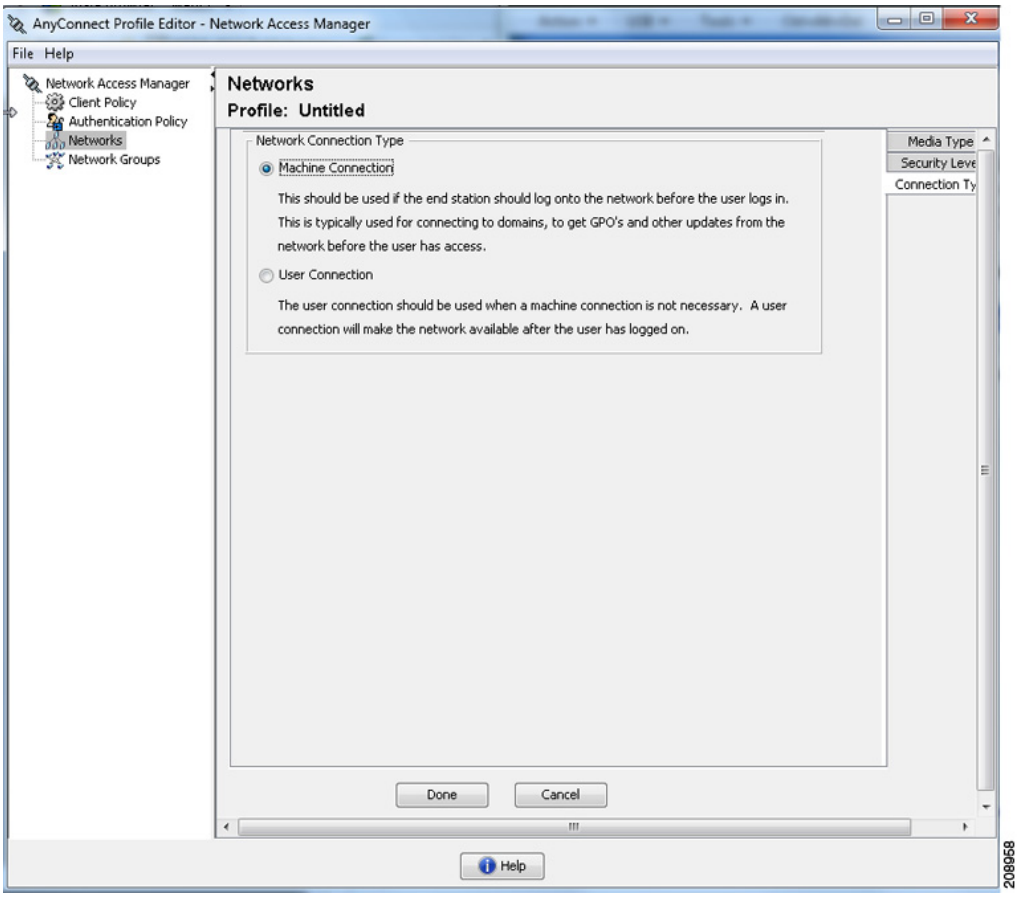
- [Machine and User Connection] : [Security Level] ペインで選択したように、[*Authenticating Network*] を設定している場合のみ指定できます。マシン ID とユーザ クレデンシャルの両方を使用しますが、マシン部分はユーザが PC にログインしていない場合のみ有効です。2 つの部分の設定は同じですが、マシン接続の認証タイプとクレデンシャルは、ユーザ接続の認証タイプとクレデンシャルと異なる場合があります。

  [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 [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。

  EAP-FAST が（次のペインで）EAP 方式として設定されている場合、EAP チェーンがサポートされています。つまりネットワーク アクセス マネージャは、マシンとユーザが既知のエンティティで、企業により管理されていることを検証するということです。これは、Bring Your Own Device（BYOD; 個人所有デバイスの持ち込み）に便利です。

  [Network Connection Type] を選択すると、[Networks] ダイアログにその他のタブが表示されます。これらのタブでは、選択された [Network Connection Type] の EAP 方式とクレデンシャルを設定できます。

図 4-7　オープン ネットワークの [Network Connection Type] ペイン



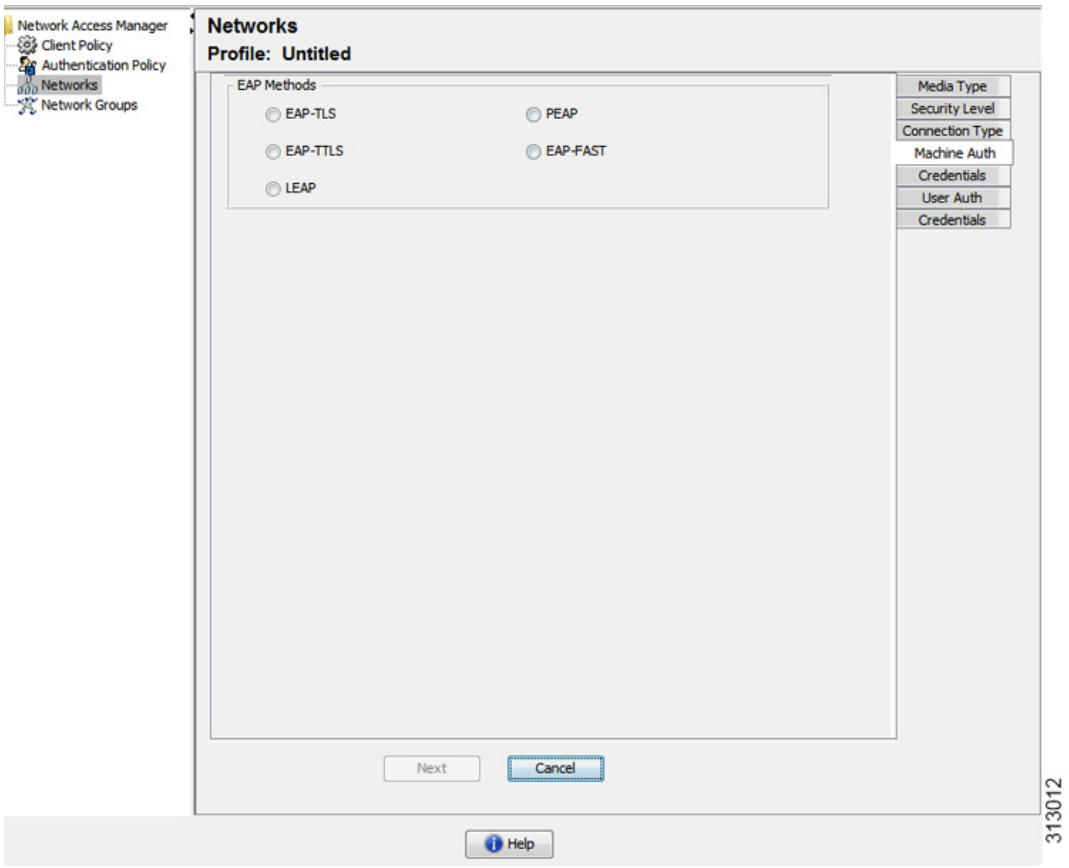
[Networks] - [User Authentication] または [Machine Authentication] ページ

[Network Connection Type] を選択した後、それらの接続タイプの認証方式を選択しました。認証方式を選択したら、ウィンドウの中央に選択した方式が適用され、さらに情報を指定する必要があります。

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、「Using a Windows Remote Desktop」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 4-8 の [EAP Methods] ペインは、ワイヤレス ネットワークのユーザ認証を示しています。

図 4-8　ワイヤレスの [User Authentication] ペイン



（注）　MACsec を有効にした場合は、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。

選択した EAP 方式によって、このペインで設定を追加できます。

- EAP-GTC：「EAP-GTC の設定」（P.4-22）を参照してください。
- EAP-TLS：「EAP-TLS の設定」（P.4-23）を参照してください。
- EAP-TTLS：「EAP-TTLS の設定」（P.4-23）を参照してください。
- PEAP：「PEAP オプションの設定」（P.4-25）を参照してください。
- EAP-FAST：「EAP-FAST の設定」（P.4-26）を参照してください。
- LEAP：「LEAP の設定」（P.4-28）を参照してください。

EAP の概要

EAP は、認証プロトコルを伝送するトランスポート プロトコルから認証プロトコルをデカップリングするための要件に対応する IETF RFC 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：サプリカントは応答パケットをオーセンティケータに送信し、シーケンス番号を使用して開始 EAP 要求と照合します。EAP 応答のタイプは、通常 EAP 要求と一致しますが、応答が負（NAK）の場合は除きます。
- EAP 成功：オーセンティケータは、サプリカントの認証が成功した場合、成功パケットを送信します。
- EAP 失敗：オーセンティケータは、認証が失敗した場合、サプリカントに失敗パケットを送信します。

EAP が IEEE 802.11X システムで使用中の場合、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。

EAP-GTC の設定

EAP-GTC は、単純なユーザ名とパスワードに基づく 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。この方式は、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。クライアントのみ認証するため、不正なサーバがユーザのクレデンシャルを取得するおそれがあります。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。

EAP-GTC によりキー関連情報は提供されないため、MACsec ではこの方式は使用できません。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。

- [Authenticate using a Password]：十分に保護された有線環境にのみ適しています。
- [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。

- [Validate Server Certificate]：サーバ証明書の検証を有効にします。
- [Enable Fast Reconnect]：TLS セッション再開を有効にします。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） [Disable when using a Smart Card] オプションは、マシン接続認証では使用できません。

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-TTLS の設定（SNMP Configuration）

- 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
  - [Validate Server Identity]：サーバ証明書の検証を有効にします。
  - [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有効にします。

    （注）　[Disable when using a Smart Card] は、マシン接続認証では使用できません。

- [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。Wi-Fi メディアタイプにのみ使用できます。

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。

- パスワードを使った認証
  - 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。
- 証明書を使った EAP-TLS
  - 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 の両方を有効にしない）。

PEAP の設定

- PEAP-EAP の設定
  - [Validate Server Identity]：サーバ証明書の検証を有効にします。
  - [Enable Fast Reconnect]：外部 TLS セッション再開のみを有効にします。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。
  - [Disable when using a Smart Card]：スマート カードを使用して認証する場合に高速再接続を使用しません。スマート カードは、ユーザ接続にのみ適用されます。

  - [Authenticate using a Token and EAP GTC]：マシン認証には使用できません。
- クレデンシャル ソースに基づく内部方式
  - [Authenticate using a password]：EAP-MSCHAPv2 または EAP-GTC に対応
  - [Authenticate using a Certificate]：EAP-TLS に対応
  - [Authenticate using a Token and EAP-GTC]：マシン認証には使用できません。

（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-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。

AnyConnect 3.1 の時点では、マシン接続とユーザ接続の両方が設定されている場合、EAP チェーンがサポートされています。つまりネットワーク アクセス マネージャは、マシンとユーザが既知のエンティティで、企業により管理されていることを検証するということです。これは、Bring Your Own Device（BYOD; 個人所有デバイスの持ち込み）に便利です。EAP チェーンの詳細については、RFC 3748 を参照してください。

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 の設定

- EAP-FAST の設定
  - [Validate Server Identity]：サーバ証明書の検証を有効にします。これを有効にすると、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 [Certificate] ペインがさらに追加されます。
  - [Enable Fast Reconnect]：セッション再開を有効にします。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 [Enable Fast Reconnect] パラメータは、両方のメカニズムを有効または無効にします。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 パラメータの有効/無効によって処理されます。

（注）　[Disable when using a Smart Card] オプションは、ユーザ接続認証にのみ使用できます。

- [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。
  - [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。パスワードは 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、ハッシュ化された（または不可逆的に暗号化された）データベースに対する認証でこのプロトコルを使用できます。

    パスワード ベースの内部方式を使用している場合、認証されていない PAC プロビジョニングを許可する追加オプションが使用できます。
  - [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。
  - Authenticate Using a Token and EAP-GTC
- [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無効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 Files] ペインを選択して、[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、[Remove] をクリックします。

  [Password protected]：PAC がパスワード保護でエクスポートされた場合は、[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。

LEAP の設定

LEAP（Lightweight EAP）はワイヤレス ネットワークに対応しています。拡張認証プロトコル（EAP）フレームワークに基づき、WEP よりセキュアなプロトコルを作成するためシスコにより開発されました。

（注）　強力なパスワードおよび定期的に失効するパスワードを使用しない限り、LEAP はディクショナリ攻撃を受ける場合があります。認証方式がディクショナリ攻撃の被害を受けにくい EAP-FAST、PEAP または EAP-TLS を使用することをお勧めします。LEAP セキュリティの詳細については、http://www.cisco.com/en/US/tech/tk722/tk809/technologies_security_notice09186a00801aa80f.html を参照してください。

LEAP 設定はユーザ認証にのみ使用できます。

- [Extend user connection beyond log off]：ユーザ認証のみについて、ユーザがログオフした場合に接続を維持します。同じユーザが再度ネットワークにログインしても、接続はアクティブのままになります。

ネットワーク クレデンシャルの定義

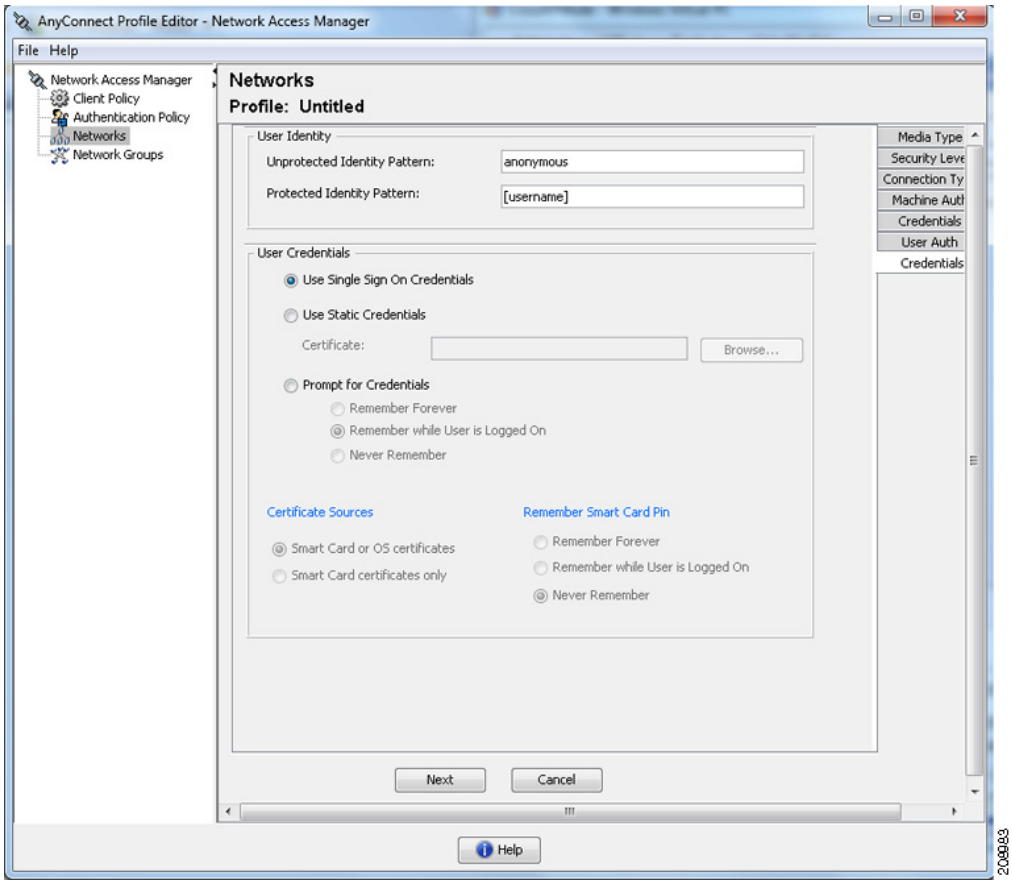
[Networks] > [Credentials] ペインで、ユーザ クレデンシャルまたはマシン クレデンシャルのいずれを使用するか指定し、信頼サーバ検証ルールを設定します。

- 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

[Credentials] ペインでは、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 4-9 を参照）の認証で使用するために指定できます。

図 4-9　EAP-TLS の [User Credentials] ペイン



ステップ 1　[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。

- [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。
- [raw]：ユーザの入力のとおりにユーザ名を指定します。
- [domain]：ユーザの PC のドメインを指定します。

ユーザ接続で、プレースホルダ [username] および [domain] を使用する場合、次の条件が当てはまります。

- 認証にクライアント証明書を使用する場合は、[username] と [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/DC=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@[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。
- [username]@[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有効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。

- [username]@[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。

- [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。

- [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。
- [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。
  - [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。
  - [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。
  - [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。

- [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。
- [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　[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。

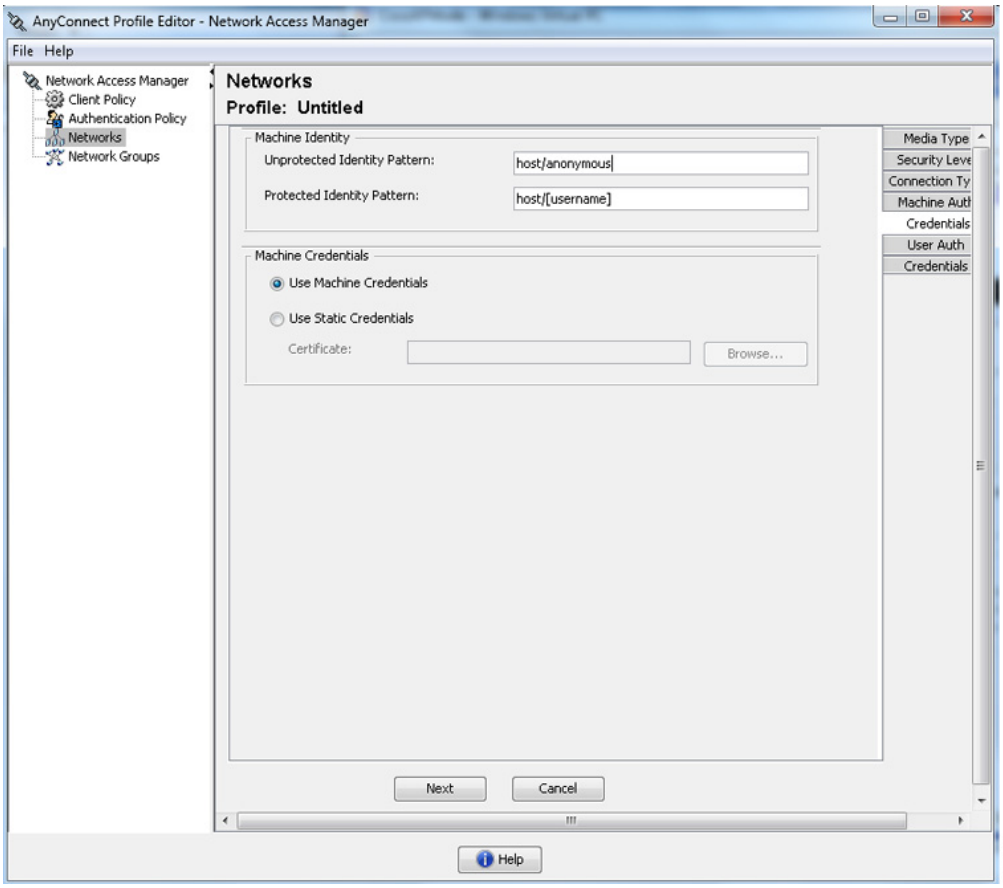
（注）　PIN は、証明書自体よりも長く保存されることは決してありません。

別名 Cryptographic Service Provider（CSP）および Key Storage Provider（KSP）というスマート カードのチップとドライバによっては、他より接続に時間がかかるスマート カードもあります。ネットワークで、スマート カードを使用して認証するのに十分な時間を与えるため、接続タイムアウトを増やさなければならない場合があります。

マシン クレデンシャルの設定

[Credentials] パネルでは、目的のマシン クレデンシャル（図 4-10 を参照）を指定できます。

図 4-10　マシン クレデンシャル



ステップ 1　[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。

- [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。
- [raw]：ユーザの入力のとおりにユーザ名を指定します。
- [domain]：ユーザの PC のドメインを指定します。

マシン接続の場合に、[username] および [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、[username] と [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、[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@[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有効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/[username]@[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。

- [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。
- [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

[Validate Server Identity] オプションが [EAP] 方式に設定されている場合、[Certificate] パネルが有効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 [Certificate Field] および [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　[Value] フィールドに、値を入力します。

ステップ 3　規則の下で [Add] をクリックします。

ステップ 4　[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。

- [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。
- Include Root Certificate Authority (CA) Certificates

（注）　[Include Root Certificate Authority (CA) Certificates] を選択した場合は、[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。

[Network Groups] ウィンドウ

[Network Groups] ウィンドウで、ネットワーク接続を特定のグループに割り当てます（図 4-11 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。

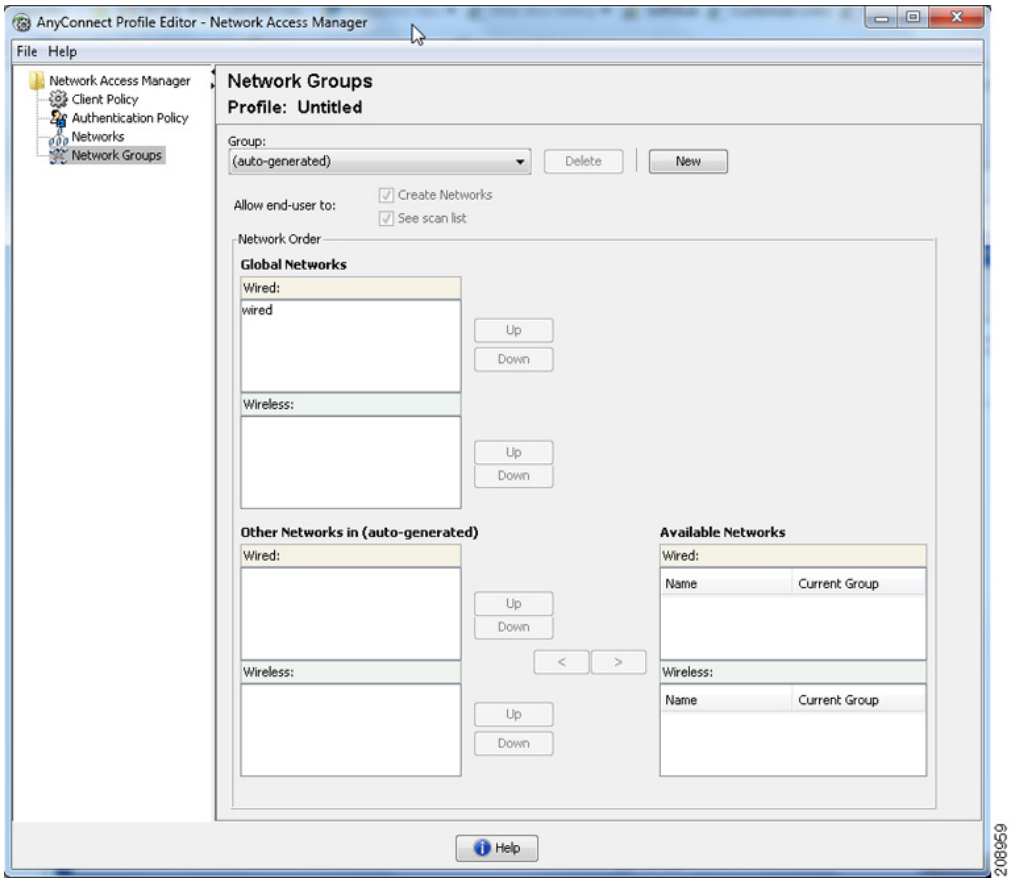
- 接続の確立試行時のユーザ エクスペリエンスの向上。複数の非表示ネットワークが設定された場合、接続が正常に確立するまで、クライアントは非表示ネットワークのリストを定義された順序で順を追って調べます。このような場合に、接続を確立するために必要な時間を大幅に短縮するためにグループが使用されます。
- 設定された接続の管理の簡略化。この利点により、企業内で複数の役割を持つ（または同じ領域に頻繁にアクセスする）ユーザがグループ内のネットワークを調整して選択可能なネットワークのリストを管理しやすくする場合に、管理者ネットワークをユーザ ネットワークから分離できます。

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 [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。あるグループがデフォルトで作成されている場合、すべてのネットワークがグローバルの場合にそのグループを削除できます。

図 4-11　[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、[Group] を選択します。

ステップ 2　[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　[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、[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　[Up] および [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。