CHAPTER 2

Cisco SSC のセットアップ

この章では、Cisco Secure Services Client の概要、およびユーザ プロファイルの追加、設定、およびテスト方法について説明します。この章は、次の項で構成されています。

概要

Cisco Secure Service Client（SSC）は、有線ネットワークと無線ネットワークの両方にデバイスがアクセスするための 802.1X（レイヤ 2）認証機能を提供するクライアント ソフトウェアです。安全なアクセスに必要なユーザとデバイスの ID、およびネットワーク アクセス プロトコルが、SSC によって管理されます。インテリジェントな機能を備えた SSC によって、従業員とゲストは、企業の有線ネットワークまたは無線ネットワークに簡単に接続できます。

SSC は、主に次の機能をサポートしています。

- 有線（802.3）および無線（802.11）ネットワーク アダプタ
- 統合 VPN
- Windows マシンのクレデンシャルを使用した認証
- Windows のログオン クレデンシャルを使用したシングル サインオン ユーザ認証
- 簡略化された使いやすい 802.1X の設定
- EAP 方式：
  - EAP-FAST、EAP-PEAP、EAP-TTLS、EAP-TLS、および LEAP（802.3 有線については EAP-MD5、EAP-GTC、および EAP-MSCHAPv2 のみ）。
- 内部 EAP 方式：
  - PEAP：EAP-GTC、EAP-TLS、および EAP-MSCHAPv2
  - EAP-FAST：EAP-GTC、EAP-TLS、および EAP-MSCHAPv2
  - EAP-TTLS:EAP-MD5 および EAP-MSCHAPv2（また、従来のプロトコル：PAP、CHAP、MSCHAP、MSCHAPv2）
- 暗号化モード：
  - 静的 WEP（オープンまたは共有）、動的 WEP（802.1X で生成）、TKIP、および AES
- キー設定プロトコル：
  - WPA、WPA2/802.11i、および CCKM（802.11 NIC アダプタに応じて選択）
- スマートカード提供のクレデンシャル
- Cisco Trust Agent（CTA）もインストールされている場合は CTA の処理

サポートされるオペレーティング システム

サポートされる 32 ビット オペレーティング システムは、次のとおりです。

- Windows XP Professional（SP2）
- Windows 2000（SP4）
- Windows 2003 Server Enterprise Edition（SP2）

（注） Media Center、Tablet PC、Professional x64 などの、他のバージョンの Windows XP はサポートされません。

SSC ソフトウェアの入手

SSC 5.1.0 ソフトウェアは、Cisco Software Center から入手できます。

- SSCMgmtToolKit_5.1.0.zip：sscManagementUtility およびサポート ファイルが含まれています。
- Cisco_SSC-XP2K_5.1.0.zip：SSC ファイルが含まれています。ライセンスの詳細は、「SSC ライセンスの詳細」の項（P.2-3）を参照してください。
- CiscoClientUtilities_5.1.0.zip：Log Packager が含まれています。

SSC ソフトウェアは、Cisco Software Center から入手できます。URL は次のとおりです。

http://www.cisco.com/public/sw-center/index.shtml

Wireless Software > **Client Adapters and Client Software** > **Cisco Secure Services Client** の順にクリックし、画面の指示に従って Latest Releases の 5.1.0 に進みます。

（注）　ソフトウェアをダウンロードするには、Cisco.com に登録するか、登録済みのユーザである必要があります。

SSC ライセンスの詳細

Cisco.com の Cisco Software Center から入手する SSC ソフトウェアには、2 つの特別なライセンスが付属しており、それぞれに次のような制限があります。

- 有線および無線の両方に対する 90 日間のトライアル ライセンス。これは、90 日の評価期間に限ってすべての機能を使用できる SSC のライセンスです。90 日以降もすべての機能を使用するには、シスコから永続的なライセンスをご購入いただく必要があります。
- 永続的な有線専用ライセンス。すべての機能を使用可能な 90 日間の SSC トライアル ライセンスの、限定されたサブセットが付与されます。すべての機能を使用するには、シスコから永続的なライセンスをご購入いただく必要があります。

これらの特別なライセンスでサポートされている機能に関する追加情報は、Cisco.com の *Cisco Secure Services Client Version 5.1 Bulletin* を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/ps7034/prod_bulletins_list.html

（注）　トライアル　ライセンス期間の期限が切れた後に、ユーザがサポートされていない機能を使用しようとすると、SSC では、システム管理者に連絡するように指示するポップアップ メッセージが表示されます。ライセンスの期限が切れている場合、このメッセージは、ユーザが無期限ライセンスを取得するまでの間、SSC を起動するたびに表示されます。

SSC 5.1 の無期限ライセンスは、次の製品番号を使用してシスコにご注文いただけます。

- AIR-SC5.0-XP2K

ネットワーク管理者とエンドユーザのエクスペリエンス

802.1X 方式や EAP 方式は、一般的なエンタープライズ ユーザには知られていません。ユーザの主な関心は、有線接続や無線接続にマウスをクリックするだけで簡単に接続できるかどうかということにあります。SSC は、複雑な部分をできる限り隠すことで、シンプルなユーザ エクスペリエンスを提供するように設計されています。

ただし、ネットワーク管理者は、エンタープライズ展開の要件に合わせて SSC を設定およびカスタマイズするための柔軟性を必要とします。SSC 管理ユーティリティは、設定に関する管理者のニーズを満たすように設計されています。以降の項では、SSC 管理ユーティリティの使用方法について説明します。

SSC Management Utility

SSC Management Utility は、システム管理者向けのスタンドアロン アプリケーションとして設計されています。このユーティリティを使用することで、システム管理者は SSC 設定プロファイルを作成および編集して、事前設定済みのクライアント パッケージを作成できます。事前設定済みのクライアント パッケージは、エンドユーザの PC に展開されます。

Management Utility には、2 つの操作モードがあります。Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）、およびシステム管理者がコマンド ラインで特定の操作を行うことができる Command Line Interfac（CLI; コマンドライン インターフェイス）です。

コマンドラインでの操作

Management Utility（sscManagementUtility）のコマンドライン バージョンの構文は、次のとおりです。

sscManagementUtility { **validate** | **sign** | **help** | **package** } [*command specific options*]

sscManagementUtility *help*

sscManagementUtility *validate* {***–i*** *input-file* | ***--in***=*input-file*}

sscManagementUtility sign {***–i*** *input-file* | ***--in***=*input-file*} {***–o*** *output-file* | ***--out***=*output-file*}

sscManagementUtility package {**–p** *srcMsi-file* | **--package**=*srcMsi-file*} {**-i** *xml-file* | **--in**=*xml-file*} {**–o** *dstMsi-file* | **--out**=*dstMsi-file*}

表 2-1 は、sscManagementUtility CLI コマンドとコマンドライン オプションの一覧を示しています。

表 2-1　sscManagementUtility コマンドおよびコマンドライン オプション

コマンド エレメント	意味
validate	宛先パッケージ xml ファイルのみを検証します。
sign	宛先パッケージ xml ファイルの後処理（検証、暗号化、および署名）を実行します。
help	ユーティリティのリリースおよびコマンド使用情報の表示
package	クライアント宛先パッケージを作成します。
–i *input-file* ***--in***=*input-file*	処理される宛先パッケージ xml ファイルのパスとファイル名。
–o *output-file* ***--out***=*output-file*	展開の準備が整った処理済み宛先パッケージ xml ファイルのパスとファイル名。

表 2-1　sscManagementUtility コマンドおよびコマンドライン オプション（続き）

コマンド エレメント	意味
–p *srcMsi-file* **--package=***srcMsi-file*	元のクライアント ソース パッケージ .msi ファイルのパスとファイル名。 **（注）** SSC 5.0 の場合は、sscPackageGen ユーティリティを使用して宛先パッケージ ファイルを生成する必要があります。
–i *xml-file* **--in=***xml-file*	処理済みおよび署名済みの設定 .xml ファイルのパスとファイル名。
–o *dstMsi-file* **--out=***dstMsi-file*	宛先パッケージ .msi ファイルのパスとファイル名。

標準エラー出力（stderr）には、次のような戻りコードが送信されます。

- 0：操作に成功。
- 1：引数が不正。
- 2：設定ファイルのバージョンが不明。
- 3：スキーマの検証に失敗。
- 4：ビジネス ルールの検証に失敗。
- 5：参照ファイルが見つからない。
- 1：予期しないエラー（詳細は stderr を参照）。

（注） SSCMgmtTookkit.zip ファイルからファイルを抽出する場合は、元のフォルダ構造とファイルの場所が維持されていることを確認してください。Management Utility では、ユーティリティと同じフォルダのデータ フォルダに配置されているサポート ファイルが使用されます。ファイルやフォルダを最初のインストール場所から移動しないでください。

GUI の操作

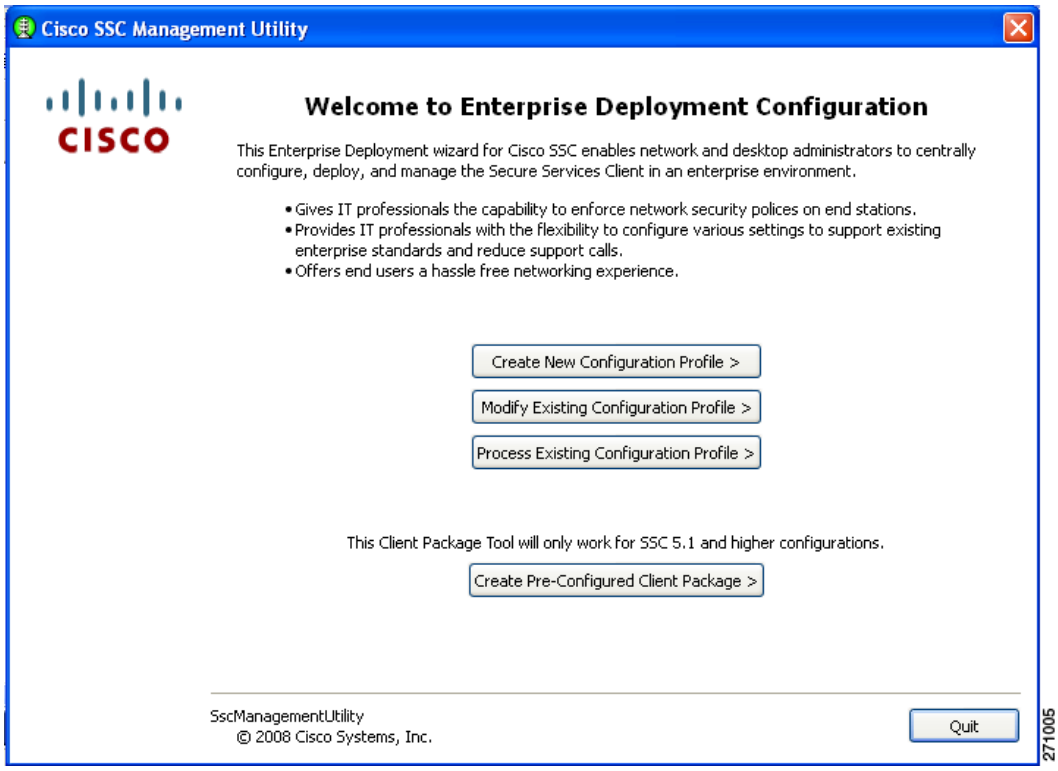
Management Utility の GUI では、管理者が、画面の指示に従い、一連のウィンドウとメニュー オプションを使用して、有線ネットワークや無線ネットワークのセキュリティ プロファイルを指定または設定できます。

Management Utility の GUI を使用するにあたっては、次のことを覚えておいてください。

- 項目の横に？記号が付いている場合は、？をクリックすると、状況依存ヘルプが表示されます。
- **Next** をクリックしたときに表示されるウィンドウは、現在のウィンドウで何が選択されているかによって異なります。

SSC Management Utility の GUI を有効にするには、**sscManagementUtility.exe** をダブルクリックします。Welcome ウィンドウが表示されます（図 2-1 を参照）。

図 2-1　Cisco SSC Management Utility の開始ウィンドウ



このウィンドウには 4 種類のボタンがあります。

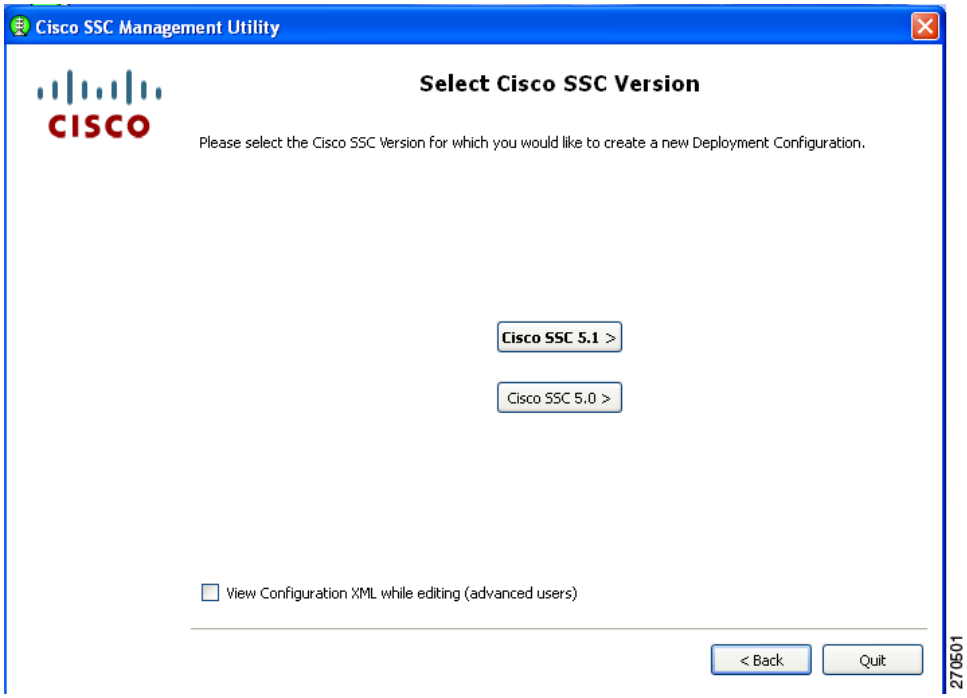
- Create New Configuration Profile：新しい展開プロファイルを作成するために使用します。Management Utility では、システム管理者が、画面の指示に従い、単一のネットワークまたは複数のネットワークに対してクライアント ポリシーとセキュリティ認証ポリシーを指定できます。設定ファイルが、設定スキーマやビジネス ルールに従っているかどうかが検証されます。
- Modify Existing Configuration Profile : 以前に作成した（未処理または処理済みの）設定ファイルのポリシーの設定を修正するために使用します。処理済みのプロファイルは、検証および署名された後、（共有キーとパスワードが）暗号化され、証明書と Proxy Auto-Configuration（PAC; プロキシ自動設定）ファイルが埋め込まれます。
- Process Existing Configuration Profile : 既存の設定プロファイル（処理済みまたは未処理）を設定スキーマやビジネス ルールに従って処理および検証するために使用します。その際、次の処理が実行されます。
  - 作成されたファイルの有効性の検証
  - 参照証明書または PAC ファイルの埋め込み
  - パスワードまたは共有キーの暗号化
  - 管理者によって展開された設定ファイルがエンドユーザによって不正に変更されるのを防ぐための、最終的な設定ファイルへの署名
- Create Pre-Configured Client Package：管理ユーティリティは、クライアント ソース パッケージ ファイルを、処理済みかつ署名済みの設定ファイルと結合し、クライアント宛先パッケージ ファイルを生成します。クライアント宛先パッケージ ファイルは、ユーザの PC を SSC と定義済みプロファイルで設定するために使用されます。

（注）　SSC 5.0 の場合は、sscPackageGen ユーティリティを使用して宛先パッケージ ファイルを生成する必要があります。

新しい設定ファイルの作成

新しい設定ファイルを作成するには、**Create New Configuration Profile** をクリックします。図 2-2 に示すウィンドウが表示されます。

図 2-2　Select Cisco SCS Version ウィンドウ



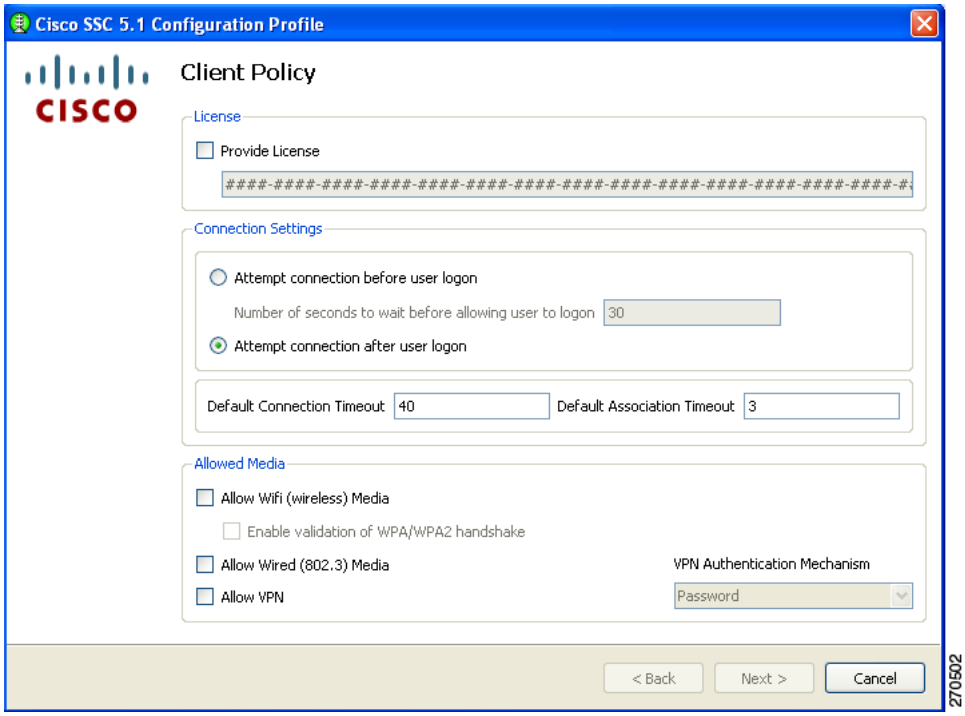
SSC Management Utility を使用すると、SSC 5.1 または 5.0 用の設定ファイルを作成できます。

Cisco SSC 5.1 をクリックすると、Client Policy ウィンドウが表示されます（図 2-3）。

クライアント ポリシーの設定

Client Policy ウィンドウでは、クライアント ポリシーのオプションを設定できます（図 2-3 を参照）。

図 2-3　Client Policy ウィンドウ



（注）　SSC リリース 5.0 以降では、エンドユーザが SSC GUI を使用してライセンス番号を入力することはできません。ネットワーク管理者は、すべてのエンドユーザに適切なライセンスが与えられるように、SSC Management Utility を使用して宛先パッケージに有効なライセンスを入力する責任があります。

このウィンドウには次の 3 つのセクションがあります。

- License section：シスコから購入した制限のない新規 SSC ライセンス キーを指定できます。

（注）　Cisco.com の Download Center からダウンロードする SSC ソフトウェアには、90 日間限定のトライアル ライセンスが付属しています。

- Connection Settings：ユーザのログオン後、または Windows のドメイン認証前（ログオン前）に、802.1X 認証を試みる必要があるかどうかを指定します。ログオン前を選択する場合は、接続までの待機時間を指定することもできます。この時間の間にネットワーク接続を確立できない場合、Windows ログオン プロセスはユーザ ログオンを続行します。
- Allowed Media：SSC クライアントによって制御されるメディアの種類を有効にします。

（注）　SSC リリース 5.0 以降は、シングルホームであるため、同時に動作可能なネットワーク接続は 1 つだけです。また、有線接続は無線接続よりも優先順位が高くなります。

無線接続に対して VPN を有効にする場合は、VPN で使用される認証メカニズムを次から指定できます。

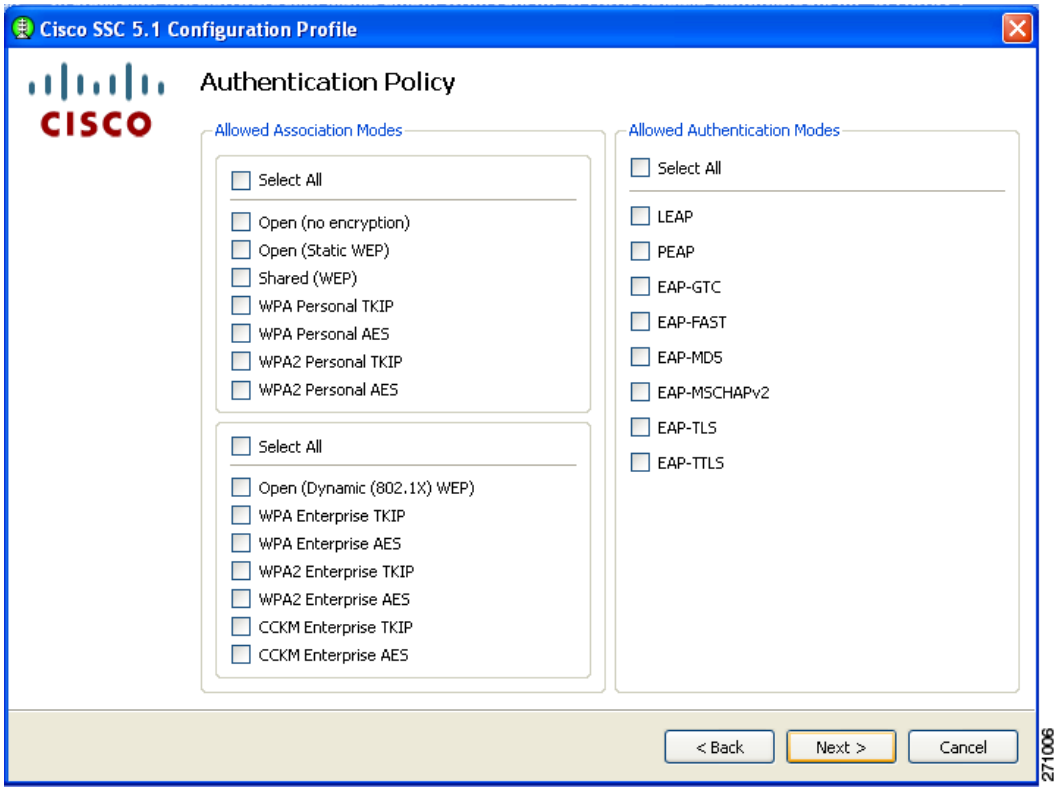
- Soft token authentication：ソフト トークン アカウント用のユーザ名とパスワードの入力が必要です。SSC は自動的に Secure Computing SofToken-II プログラムからソフト トークンを取得して、IPSec VPN クライアントに渡します。
- Password authentication：VPN パスワードの入力が必要です。SSC は自動的に IPSec VPN クライアントを起動して、パスワードを渡します。
- Certificate authentication：何も入力する必要はありません。SSC は自動的に IPSec VPN クライアントを起動し、VPN サーバは証明書を取得します。

選択を完了したら、**Next** をクリックします。Authentication Policy ウィンドウが表示されます（図 2-4）。

認証ポリシーの設定

このウィンドウでは、グローバル アソシエーションと認証ネットワークのポリシーを定義できます。グローバル ポリシーは、管理者またはユーザが作成するすべてのネットワークに適用されます。

図 2-4　Authentication Policy ウィンドウ

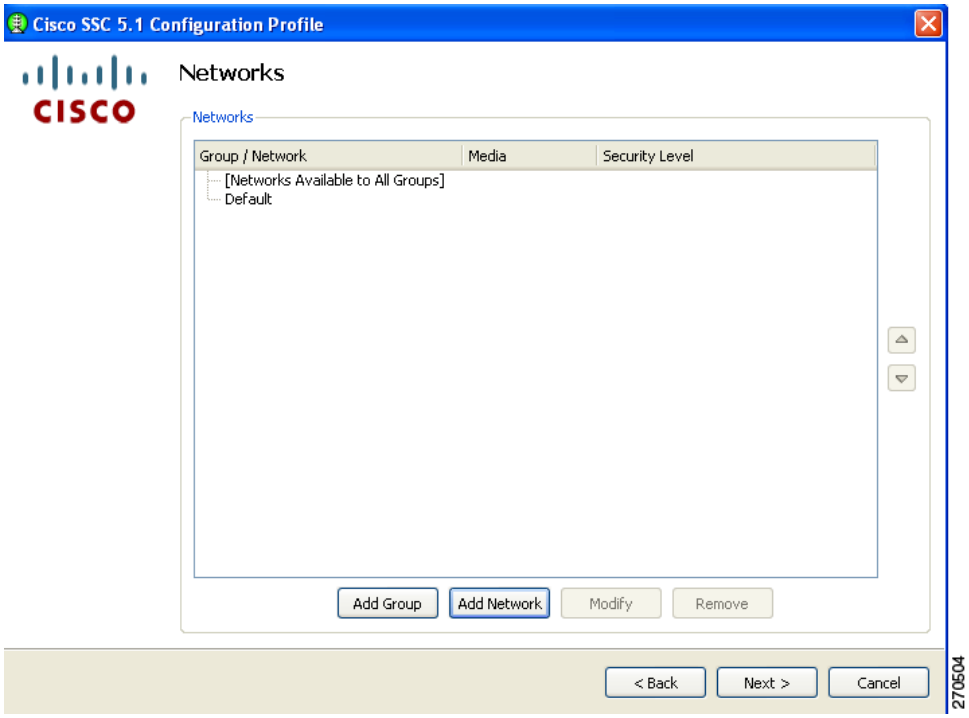


選択を完了したら、**Next** をクリックします。Networks ウィンドウが表示されます（図 2-5）。

ネットワークの設定

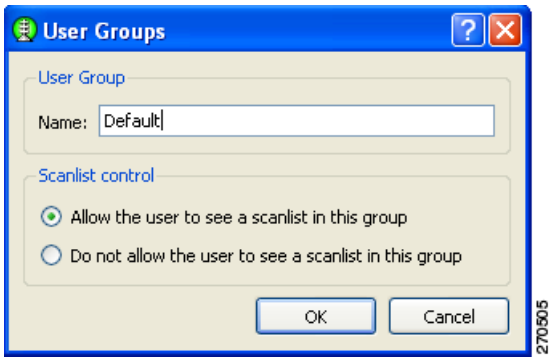
Networks ウィンドウでは、企業ユーザ向けに定義済みのネットワークを設定できます。すべてのグループで使用できるネットワークを設定するか、特定のネットワークのみでグループを作成できます。グループの詳細は、「SSC のグループ」の項（P.2-31）を参照してください。

図 2-5　Networks ウィンドウ



Add Group をクリックすると、User Groups ウィンドウが表示されます（図 2-6）。

図 2-6　User Groups ウィンドウ

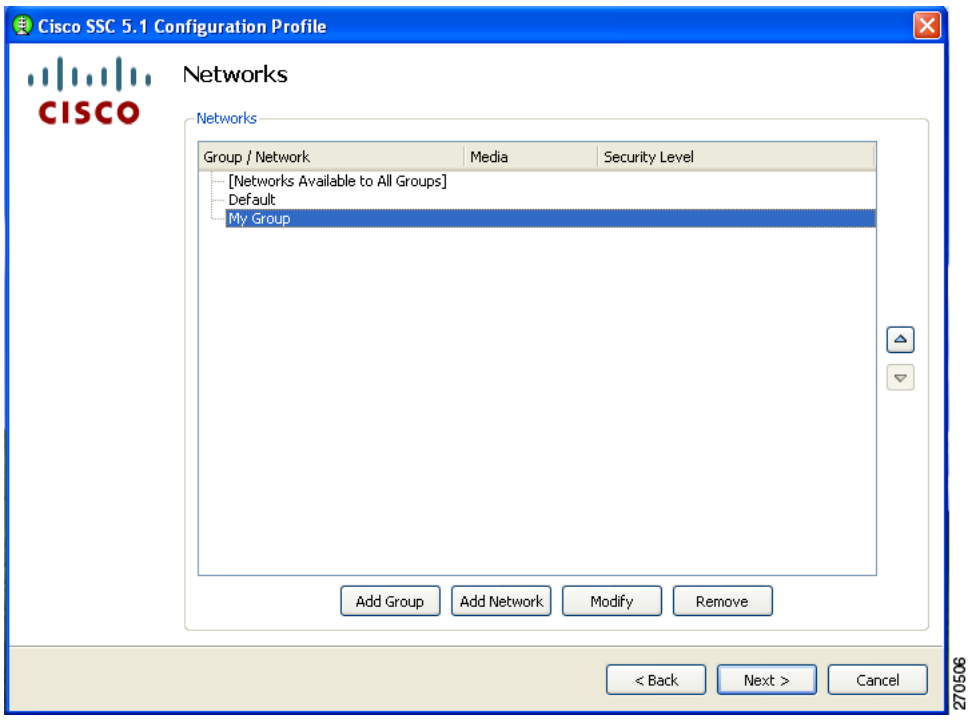


Scanlist control セクションでは、このグループがアクティブな場合に、ユーザにスキャンリストを表示するかどうかを制御できます。たとえば、ユーザが隣接するデバイスに誤って接続することがないようにするため、スキャンリストの表示の制限が必要になる場合もあります。

（注）　これはグループ別の設定です。エンドユーザが SSC GUI を使用して作成したグループについては、スキャンリスト コントロールは、*Allow the user to see a scanlist in this group* に設定されます。

新しいグループを作成し終わったら、**OK** をクリックします。Networks ウィンドウが再び表示されます。今度は、作成した新しいグループ（図 2-7 の *My Group*）が追加されています。

図 2-7　新しいグループが表示されている Network ウィンドウ



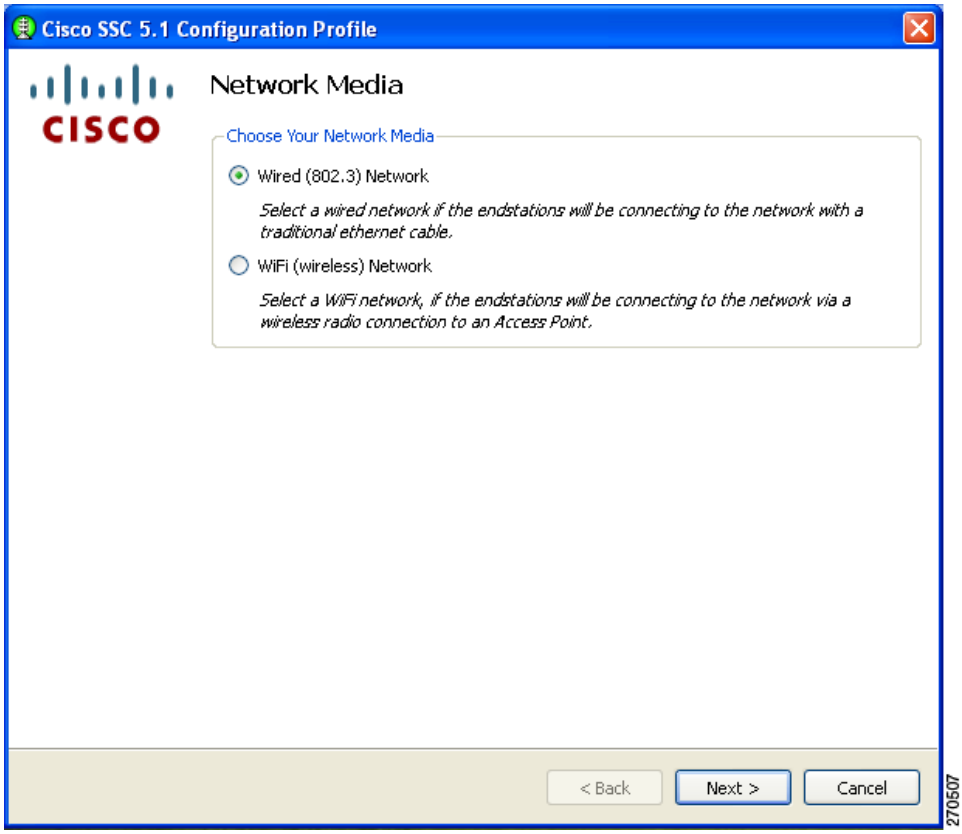
ネットワーク グループには、単一または複数の、ネットワーク プロファイルの説明が含まれます。ネットワーク プロファイルによって、個別のネットワークの特定のプロパティおよび動作が定義されます。ネットワーク プロファイルは、次のような特性を備えています。

- ユーザフレンドリなネットワーク名
- ネットワーク接続に使用されるネットワーク アクセス メディア（有線、Wi-Fi、およびアダプタの詳細
- ネットワークのセキュリティ クラス（オープン、共有キー、認証）の定義
- ネットワークの接続コンテキストの定義（マシンのみ、ユーザのみ、マシンおよびユーザ）
- Wi-Fi アソシエーションおよび暗号化方式（Wi-Fi ネットワーク）
- サポートされる認証方式とプロパティ（認証ネットワーク）
- 状況により、静的キー（認証なしのネットワーク）
- クレデンシャルのタイプとソースの定義（認証ネットワーク）
- 信頼できるサーバ（認証ネットワークの場合）、および認証局（CA）証明書の展開、EAP-FAST Protected Access CredentialPAC の手動プロビジョニングのサポートの定義

配信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ます。このためエンドユーザは設定を編集することも、プロファイルを削除することもできません。

Network ウィンドウ（図 2-7）では、My Group などの新しく作成されたグループを、選択して **Add Network** をクリックすることにより、ネットワークに追加できます。Network Media ウィンドウが表示されます（図 2-8 を参照）。

図 2-8　Network Media ウィンドウ



このウィンドウでは、有線ネットワークまたは無線ネットワークを選択できます。

Wired (803.3) Network を選択して **Next** をクリックすると、Wired Network Setting ウィンドウが表示されます（図 2-9）。

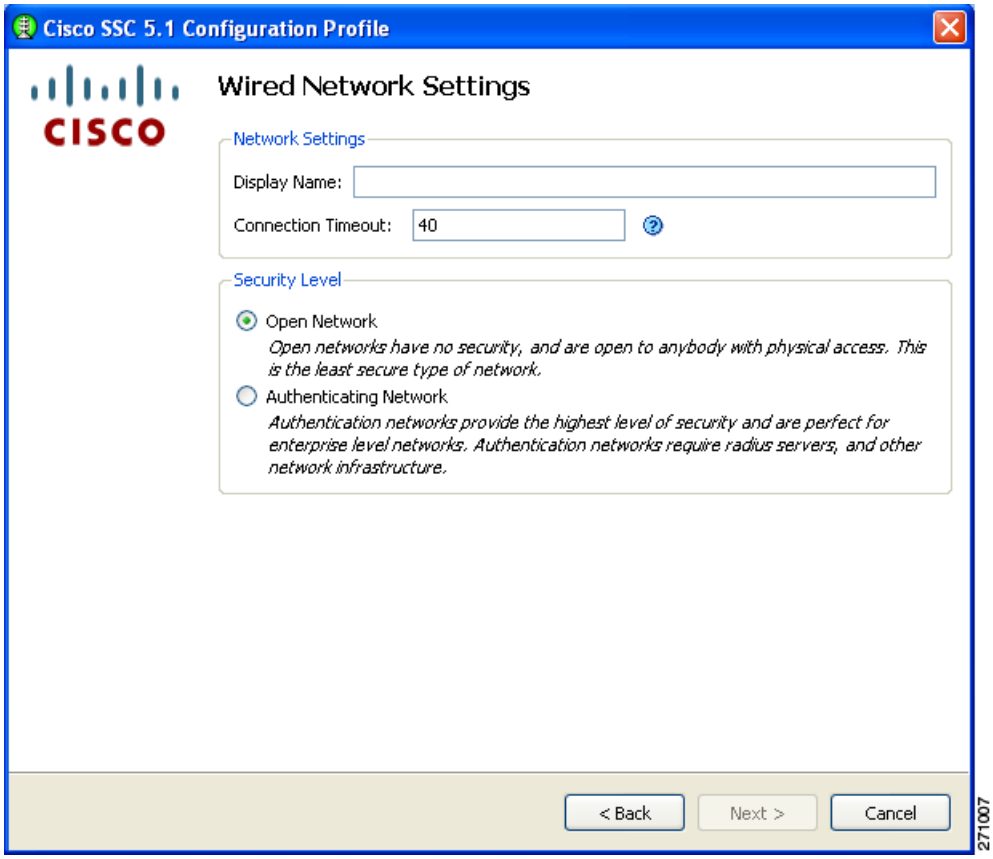
Wifi (wireless) Network を選択して **Next** をクリックすると、WiFi Network Setting ウィンドウが表示されます（図 2-11）。

すべてのグループとネットワークの追加が完了した後、Next ボタンをクリックすると、図 2-24 が表示されます（「設定ファイルの検証」の項（P.2-29）を参照）。

有線ネットワークの設定

Wired Network Settings ウィンドウでは、オープン（セキュリティで保護されていない）ネットワーク、または 802.1X 認証を使用する有線ネットワークを作成できます（図 2-9）。

図 2-9　Wired Network Settings ウィンドウ



Display Name フィールドには、この有線ネットワークに表示される名前を入力できます。

Connection Timeout の値は、SSC クライアントが別のネットワークへの接続を試みる前にネットワーク接続の確立を待機する時間の長さです。

（注）　一部のスマートカード認証システムでは、認証が完了するまでに 60 秒近くかかる場合があります。スマートカードを使用する場合は、Connection Timeout の値を大きくする必要があります。

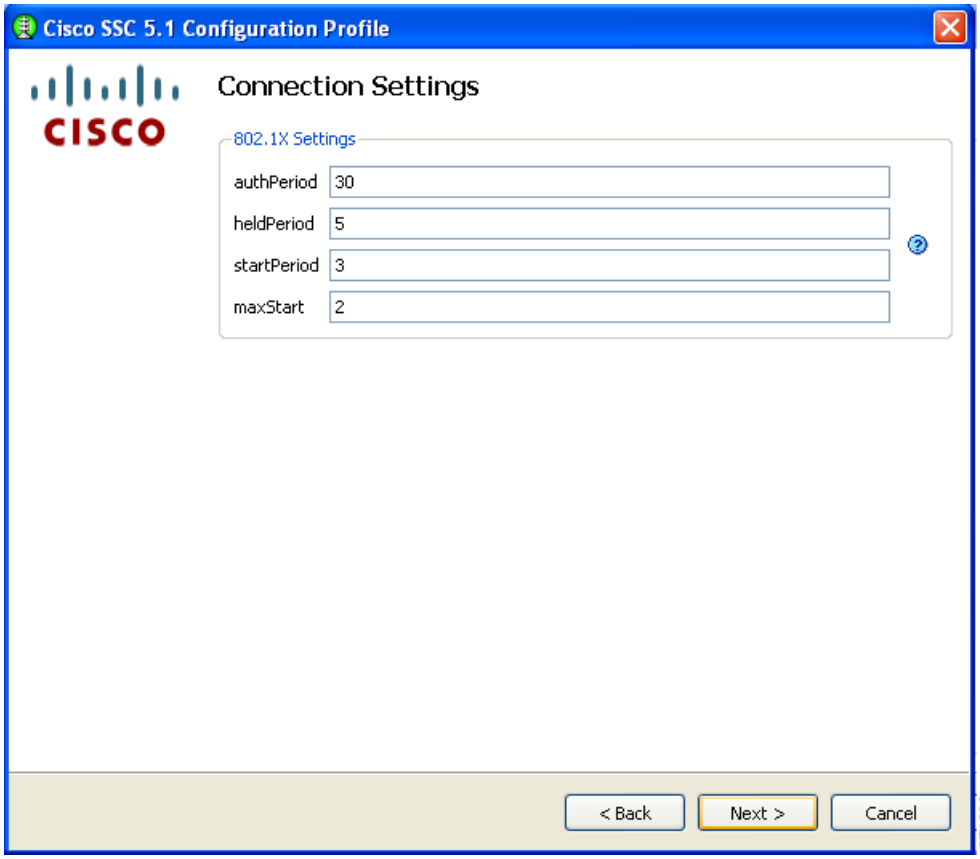
Security Level エリアでは、次のいずれかのネットワークの種類を選択します。

- Open Network：この設定は、有線ネットワークでのゲスト アクセスにお勧めします。
- Authenticating Network：この設定は、安全なエンタープライズ有線ネットワークにお勧めします。

Open Network を選択して **Next** をクリックすると、802.1X Connection Setting ウィンドウが表示されます（図 2-12）。

Authenticating Network を選択して **Next** をクリックすると、802.1X Connection Settings ウィンドウが表示されます（図 2-10）。このウィンドウでは、802.1X タイマの値を入力できます。デフォルトの値は、ほとんどの有線ネットワークに使用できますが、環境に合わせて設定を変更することもできます。

図 2-10　有線ネットワーク用の Connection Settings ウィンドウ

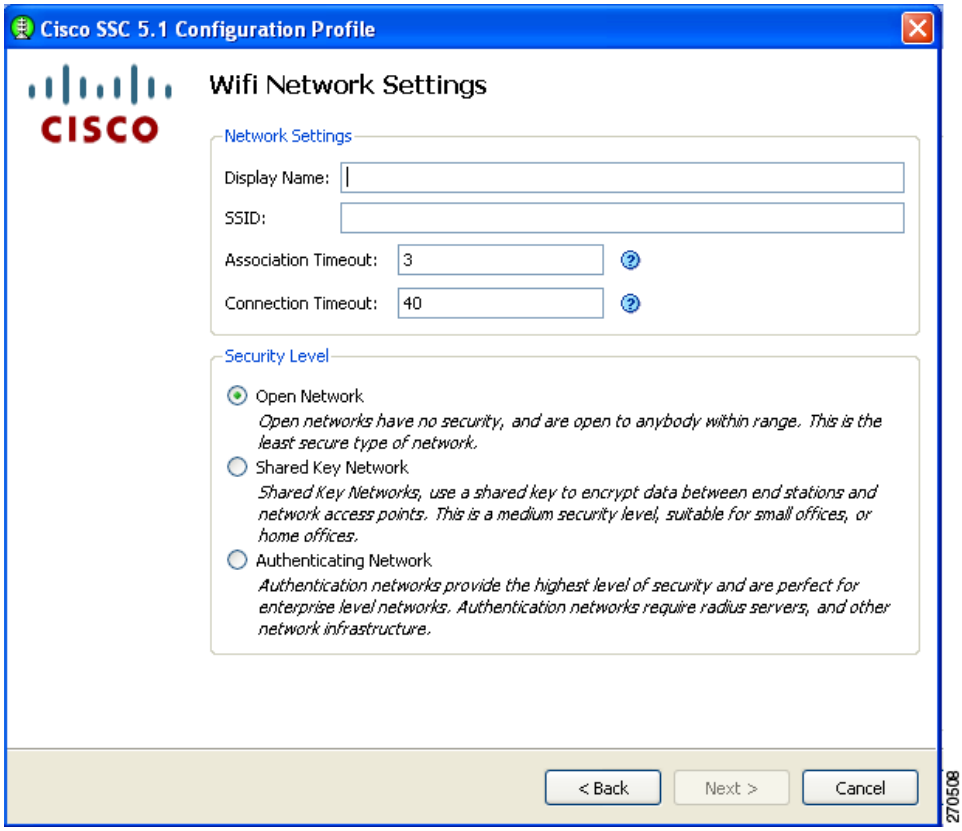


接続の設定が完了したら、**Next** をクリックします。Network Connection Type ウィンドウが表示されます（図 2-13）。

WiFi ネットワークの設定

WiFi Network Settings ウィンドウでは、オープン（セキュリティで保護されていない）ネットワーク、共有キー ネットワーク、または 802.1X 認証を使用する有線ネットワークを作成できます（図 2-11）。

図 2-11　WiFi Network Settings ウィンドウ



Display Name フィールドには、この無線ネットワークに表示される名前を入力できます。

SSID フィールドには、この無線ネットワークの SSID（またはネットワーク名）を入力する必要があります。

Association Timeout の値は、SSC が別のネットワークへのアソシエーションを試みる前に SSID へのアソシエーションを待機する時間の長さです。

Connection Timeout の値は、SSC が別のネットワークへの接続を試みる前にネットワーク接続の確立を待機する時間の長さです。

（注）　一部のスマートカード認証システムでは、認証が完了するまでに 60 秒近くかかる場合があります。スマートカードを使用する場合は、Connection Timeout の値を大きくする必要があります。

Security Level エリアでは、次のいずれかのネットワークの種類を選択します。

- Open Network：この設定は、有線ネットワークのゲスト アクセスにお勧めします。

- Shared Key Network：この設定は、エンタープライズ無線ネットワークにはお勧めしません。
- Authenticating Network：この設定は、安全なエンタープライズ無線ネットワークにお勧めします。

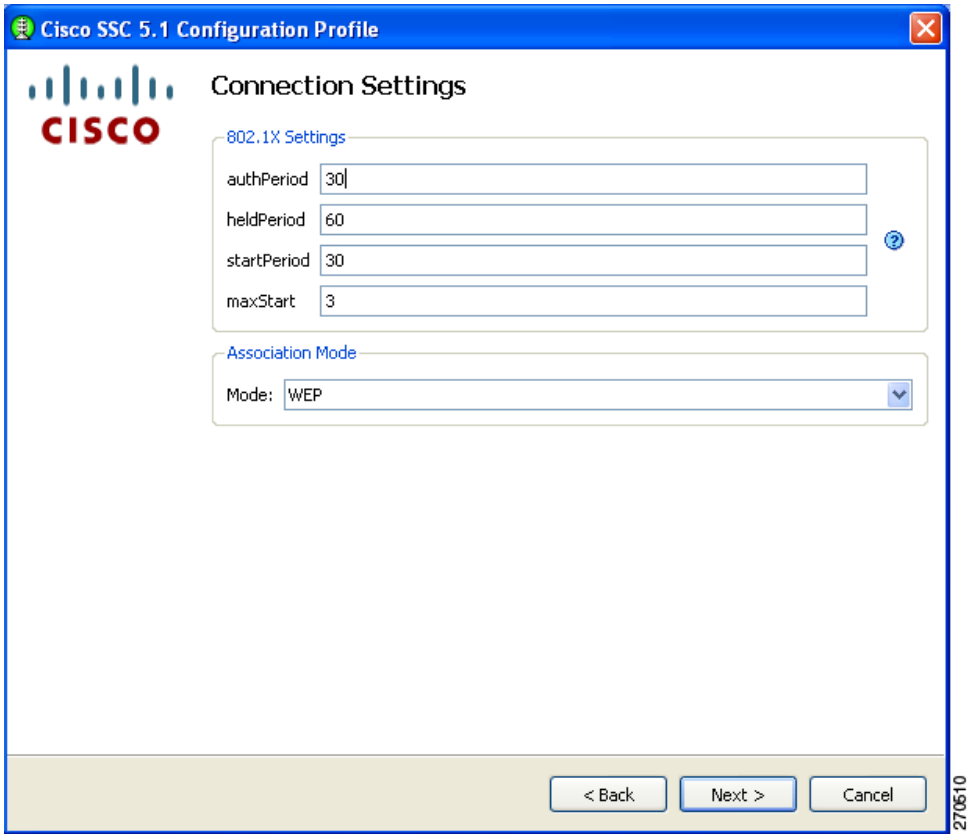
選択を完了したら、**Next** をクリックします。CCX Settings ウィンドウが表示されます。

（注）　CCX の設定は、Windows Vista 環境だけに適用されます。

Windows XP または Windows 2000 を使用している場合は、CCX 設定ウィンドウを無視して **Next** をクリックします。802.1X Connection Settings ウィンドウが表示されます（図 2-12）。

このウィンドウでは、802.1X タイマの値を入力できます。デフォルトの値は、ほとんどのネットワークに使用できますが、環境に合わせて設定を変更することもできます。

図 2-12　無線ネットワーク用の 802.1X Connection Settings ウィンドウ



Association Mode フィールドで、ドロップダウン矢印をクリックして、このネットワークのアソシエーション モードを選択します。

- WEP
- WPA Enterprise（TKIP）
- WPA Enterprise（AES）
- WPA2 Enterprise（TKIP）

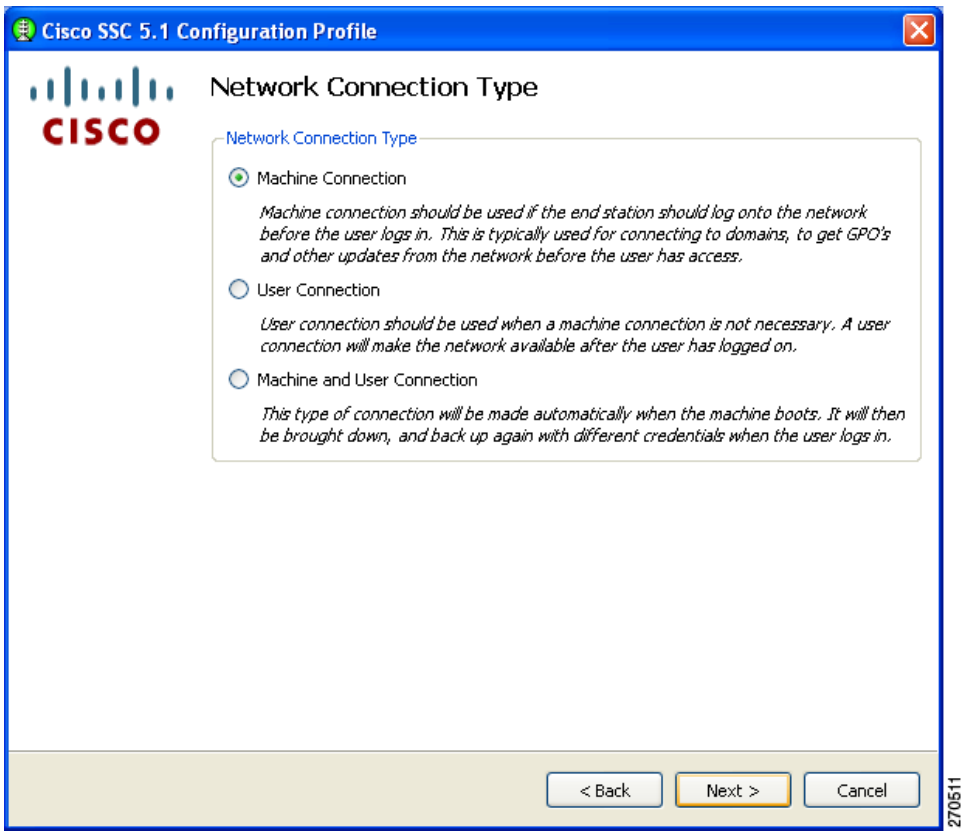
- WPA2 Enterprise（AES）
- CCKM（TKIP）
- CCKM（AES）

（注）　選択したアソシエーション モードは、Authentication Policy ウィンドウから有効にする必要があります（「認証ポリシーの設定」の項（P.2-9）を参照）。

接続の設定が完了したら、**Next** をクリックします。Network Connection Type ウィンドウが表示されます（図 2-13）。

ネットワーク接続の種類の設定

図 2-13　Network Connection Type ウィンドウ



このウィンドウでは、ネットワーク接続の種類を指定できます。SSC でのデフォルトは、Machine Connection です。User Connection オプションでは、接続の種類をユーザ接続として定義します。ユーザが PC にログオンすると、ユーザ接続が試行されます。

Machine and User Connection には、マシンの接続とユーザの接続の両方が含まれます。SSID は、どちらの接続でも同じですが、マシンの接続のクレデンシャルとユーザの接続のクレデンシャルは、種類が異なります。

（注）　オープン ネットワークには、Machine and User Connection オプションを使用できません。

ネットワーク接続の種類の指定が完了したら、**Next** をクリックします。Machine Authentication (EAP) Method ウィンドウが表示されます（図 2-14）。

EAP 認証の設定

Machine Authentication (EAP) Method ウィンドウと User Authentication (EAP) Method ウィンドウでは、マシンとユーザの認証方法をそれぞれ選択できます。両方のウィンドウに、同じ認証方法のオプションがあります。

図 2-14 の画面には、無線ネットワーク接続用の EAP 方式が示されています。

図 2-14　無線ネットワーク接続用の Machine Authentication (EAP) Method ウィンドウ

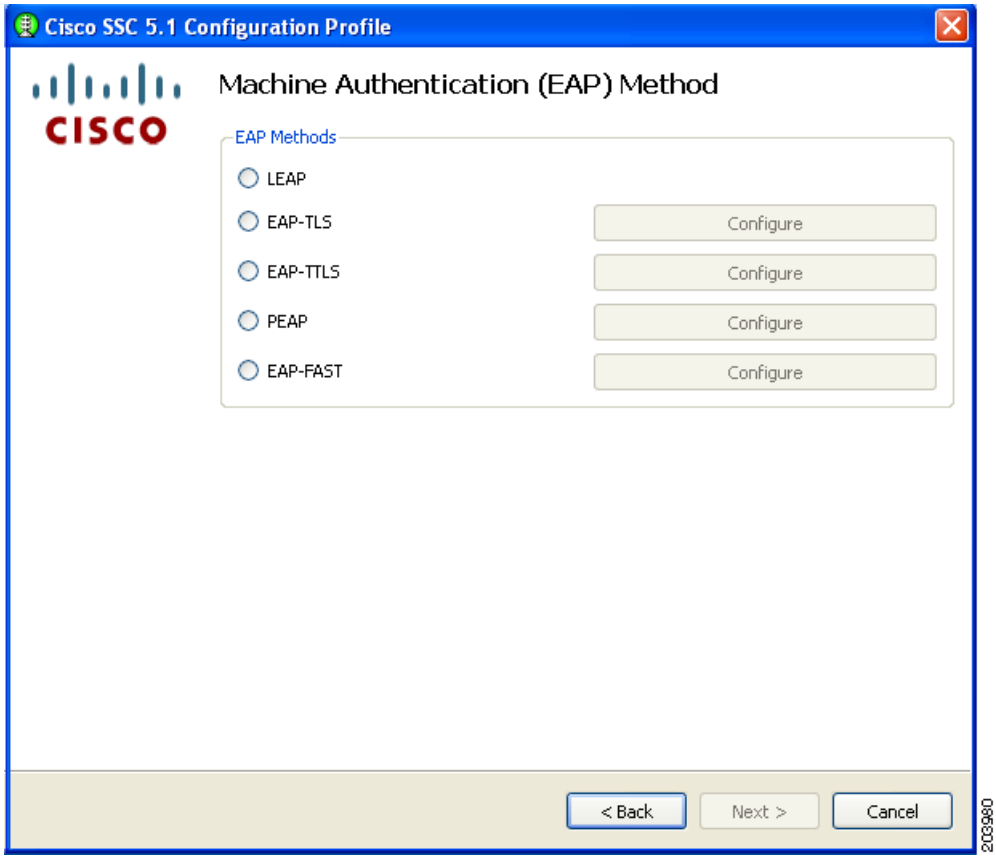
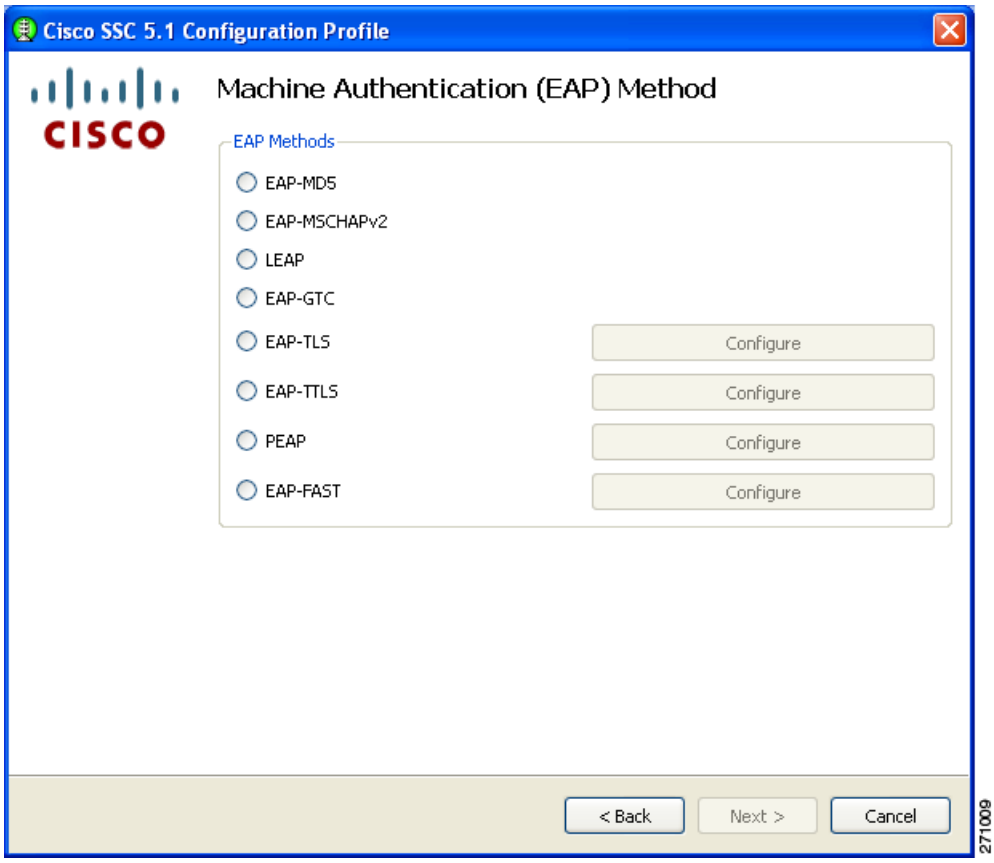


図 2-15 の画面には、有線ネットワーク接続用の EAP 方式が示されています。

図 2-15　有線ネットワーク接続用の Machine Authentication (EAP) Method ウィンドウ



（注）　選択した認証モードは、Authentication Policy ウィンドウから有効にする必要があります（「認証ポリシーの設定」の項（P.2-9）を参照）。

設定ボタンでいずれかの EAP オプションを選択する場合は、該当する Configure ボタンをクリックして EAP メソッドを設定する必要があります。

- EAP TLS：「EAP TLS の設定」の項（P.2-20）を参照してください。
- EAP TTLS：「EAP TTLS の設定」の項（P.2-21）を参照してください。
- PEAP：「PEAP オプションの設定」の項（P.2-22）を参照してください。
- EAP Fast：「EAP Fast の設定」の項（P.2-23）を参照してください。

EAP TLS、EAP TTLS、PEAP、または EAP Fast の設定ウィンドウで、Validate Server Identity オプションを選択する場合は、**Next** をクリックすると、図 2-20 のウィンドウが表示されます（「信頼できるサーバ検証規則の設定」の項（P.2-25）を参照）。

Validate Server Identity オプションを選択しない場合は、**Next** をクリックすると、図 2-22 の画面が表示されます（「信頼できる認証局の設定」の項（P.2-26）を参照）。

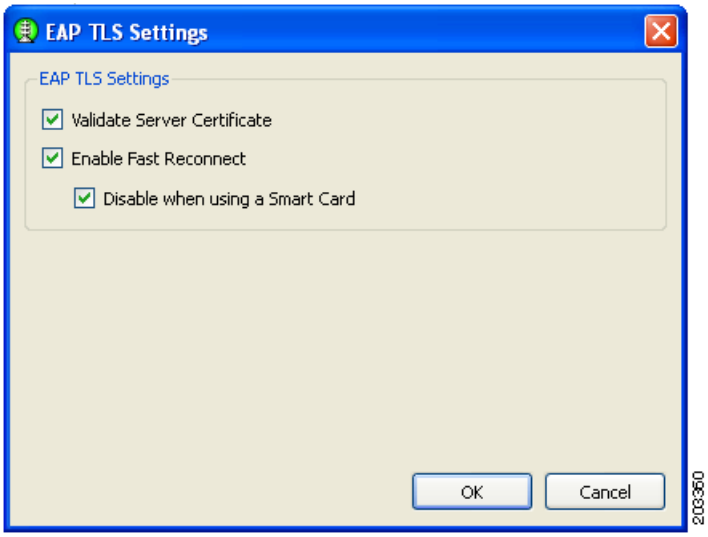
EAP TLS の設定

EAP TLS Settings ウィンドウには、次の 2 つのオプションがあります（図 2-16）。

- Validate Server Certificate：サーバ証明書の検証を有効にします。
- Enable Fast Reconnect：セッションの再開を有効にします。

（注）　*Disable when using a Smart Card* オプションは、マシンの認証には使用できません。

図 2-16　EAP-TLS Settings ウィンドウ

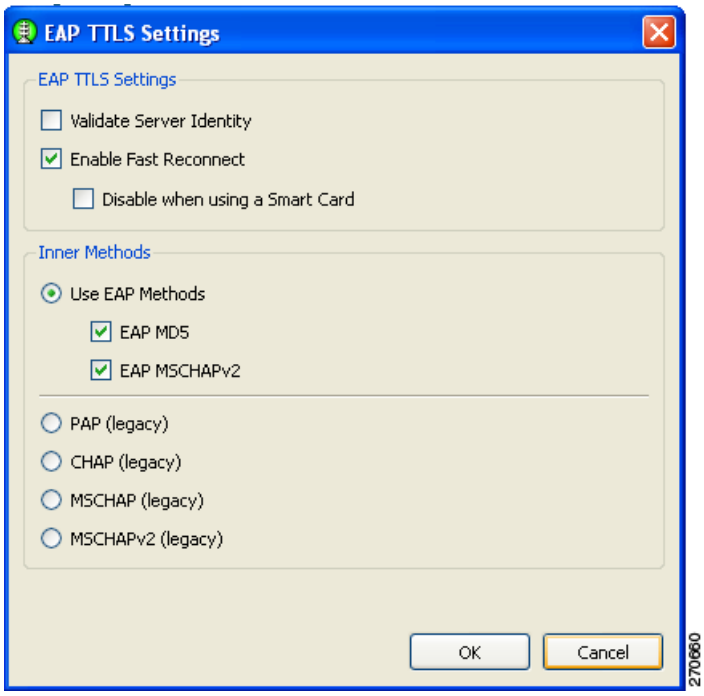


OK をクリックすると、Machine or User Authentication (EAP) Method ウィンドウが再表示されます（「EAP 認証の設定」の項（P.2-18）を参照）。

EAP TTLS の設定

EAP TTLS Settings ウィンドウでは、EAP TTLS を設定できます（図 2-17 を参照）。

図 2-17　EAP TTLS Settings ウィンドウ



EAP TTLS Settings ウィンドウは、次の 2 つのセクションで構成されています。

- EAP TTLS Settings
  - Validate Server Identity：サーバ証明書の確認を有効にします。
  - Enable Fast Reconnect：セッションの再開を有効にします。

（注）　*Disable when using a Smart Card* オプションは、マシン認証 (EAP) 方式の設定ウィンドウでは使用できません。

- Inner Methods：EAP 方式を指定します。

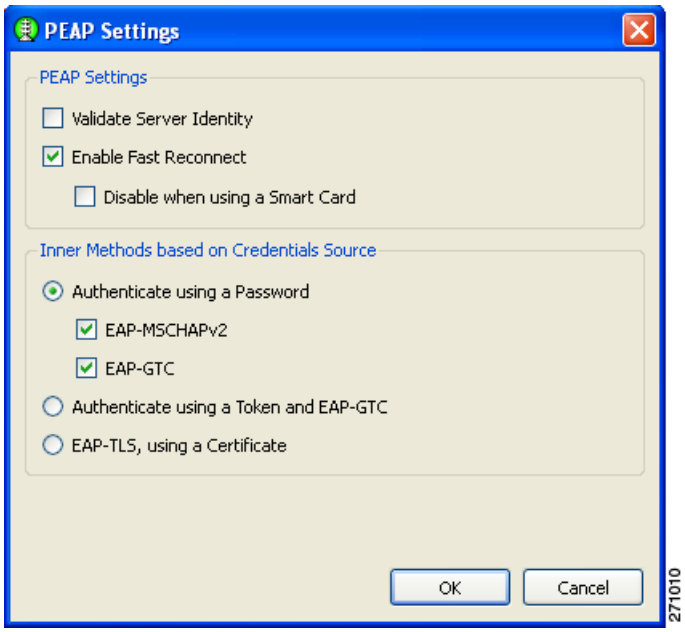
（注）　EAP MD5 または EAP MSCHAPv2 を選択する前に、Authentication Policy ウィンドウでこのオプションを有効にする必要があります（「認証ポリシーの設定」の項（P.2-9）を参照）。

設定が完了したら、**OK** をクリックします。Machine or User Authentication (EAP) Method ウィンドウが再表示されます（「EAP 認証の設定」の項（P.2-18）を参照）。

PEAP オプションの設定

PEAP Settings ウィンドウでは、PEAP を設定できます（図 2-18 を参照）。

図 2-18　PEAP Setting ウィンドウ



このウィンドウには次の 2 つのセクションがあります。

- PEAP Settings
  - Validate Server Identity：サーバ証明書の確認を有効にします。
  - Enable Fast Reconnect：セッションの再開を有効にします。

（注）　*Disable when using a Smart Card* オプションと *Authenticate using a Token and EAP GTC* オプションは、マシンの認証には使用できません。

- Inner methods based on Credentials Source：パスワードまたは証明書を使用した認証を選択できるようにします。

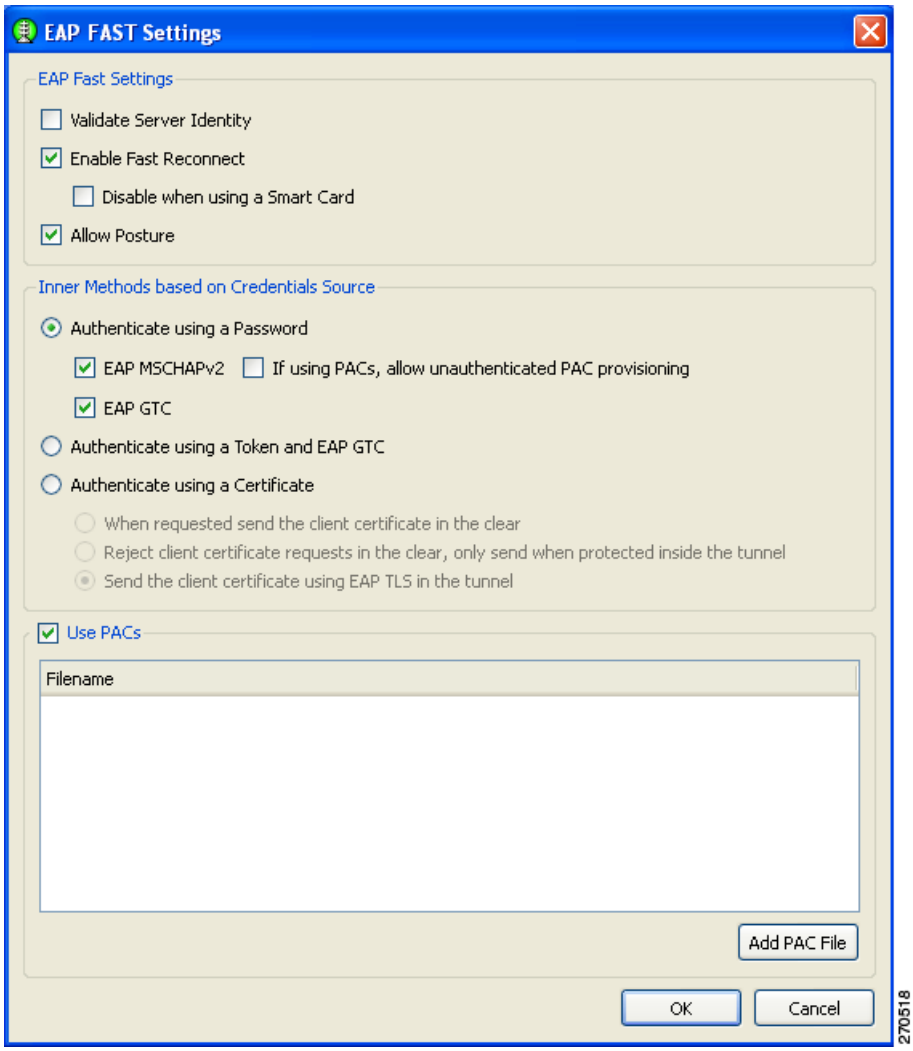
（注）　EAP MSCHAPv2 または EAP GTC を選択する前に、Authentication Policy ウィンドウでこのオプションを有効にする必要があります（「認証ポリシーの設定」の項（P.2-9）を参照）。

選択を完了したら、**OK** をクリックします。Machine or User Authentication Method ウィンドウが再表示されます（「EAP 認証の設定」の項（P.2-18）を参照）。

EAP Fast の設定

EAP FAST Settings ウィンドウでは、EAP Fast を設定できます（図 2-19）。

図 2-19　EAP FASTSettings ウィンドウ



このウィンドウは、次の 3 つのセクションで構成されています。

- EAP Fast Settings
  - Validate Server Identity：サーバ証明書の確認を有効にします。
  - Enable Fast Reconnect：セッションの再開を有効にします。

（注）　*Disable when using a Smart Card* オプションと *Authenticate using a Token and EAP GTC* オプションは、マシンの認証には使用できません。

— Allow Posture：*ポスチャ*という用語は、ネットワークへのアクセスを要求しているエンドポイント デバイスの状況を特定するために使用できる属性の集まりを意味します。これらの属性の中には、エンドポイント デバイスの種類やオペレーティング システムに関連するものもあれば、エンドポイントに存在する可能性のある、ウイルス対策（AV）スキャニング ソフトウェアなどの各種セキュリティ アプリケーションをサポートするものもあります。

検証または評価ポスチャは、ポスチャ データに対する一連の規則に適用され、そのエンドポイントに対する信頼レベルが評価されます。アセスメント、つまり**ポスチャ トークン**は、ネットワーク アクセスの認証の条件の 1 つとして使用できます。ポスチャ検証を従来のユーザ認証と併用することで、エンドポイント デバイスとユーザの完全なセキュリティ アセスメントを実現できます。

（注）　Allow Posture は、Windows XP と Windows 2000 環境に対応した SSC ではサポートされていません。SSC は、このオプションを Windows Vista 環境のみでサポートしています。

- Inner methods based on Credentials Source：パスワード、証明書、トークン、または EAP GTC を使用した認証を可能にします。

（注）　EAP MSCHAPv2 または EAP GTC を選択する前に、Authentication Policy ウィンドウでこのオプションを有効にする必要があります（「認証ポリシーの設定」の項（P.2-9）を参照）。

- Use PACsEAP-FAST 認証で PAC が使用されるように指定します。

（注）　通常、ほとんどの認証サーバでは EAP FAST に PACS を使用するため、Use PACs オプションは、オンにする必要があります。このオプションをオフにする前に、認証サーバが EAP FAST に PACs を使用していないことを確認してください。使用している場合、クライアント認証の試行は失敗します。

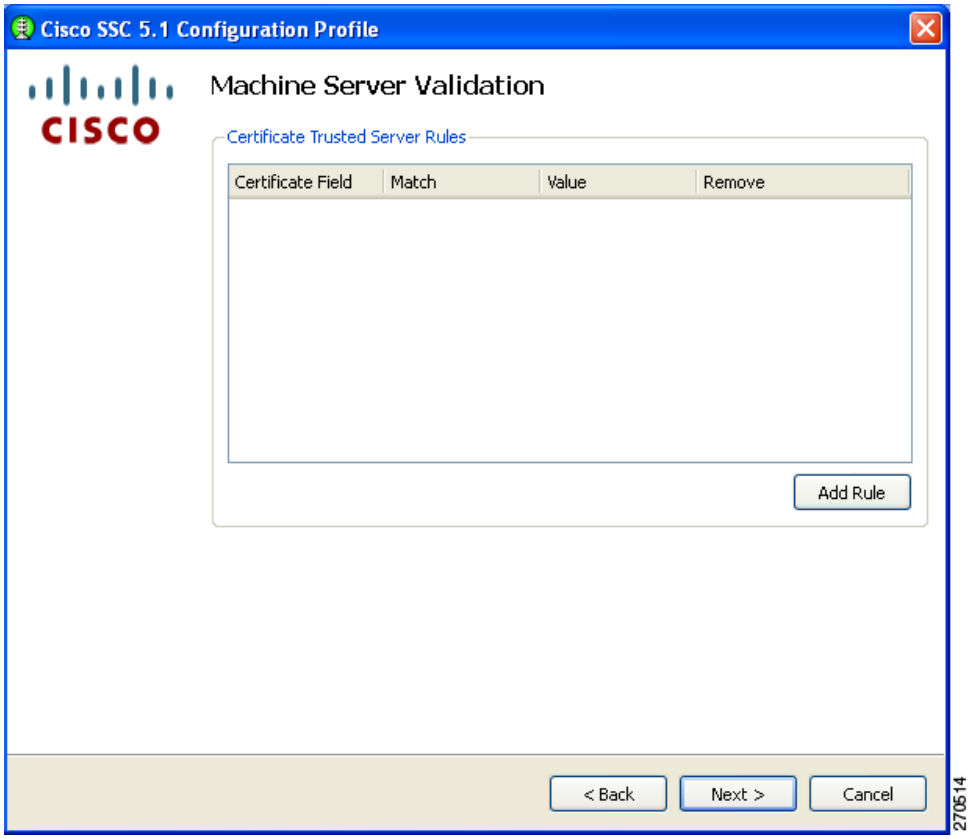
このウィンドウでは、**Add PAC File** をクリックして特定の PAC ファイルまたは認証を 1 つ以上手動で提供できます。

選択を完了したら、**OK** をクリックします。Machine or User Authentication (EAP) Method ウィンドウが再表示されます（「EAP 認証の設定」の項（P.2-18）を参照）。

信頼できるサーバ検証規則の設定

EAP 方式で Validate Server Identity が設定されている場合、証明書で信頼できるサーバ規則の設定を Machine Server Validation ウィンドウで設定できます（図 2-20）。

図 2-20　Certificate Trusted Server Validation Rules ウィンドウ



サーバ検証規則を定義するには、次の手順に従います。

a. **Add Rule** をクリックします。

b. **Certificate Field** 列および **Match** 列にオプションの設定が表示されたら、ドロップダウン矢印をクリックして、必要な設定を選択します。

c. Value フィールドに値を入力します。

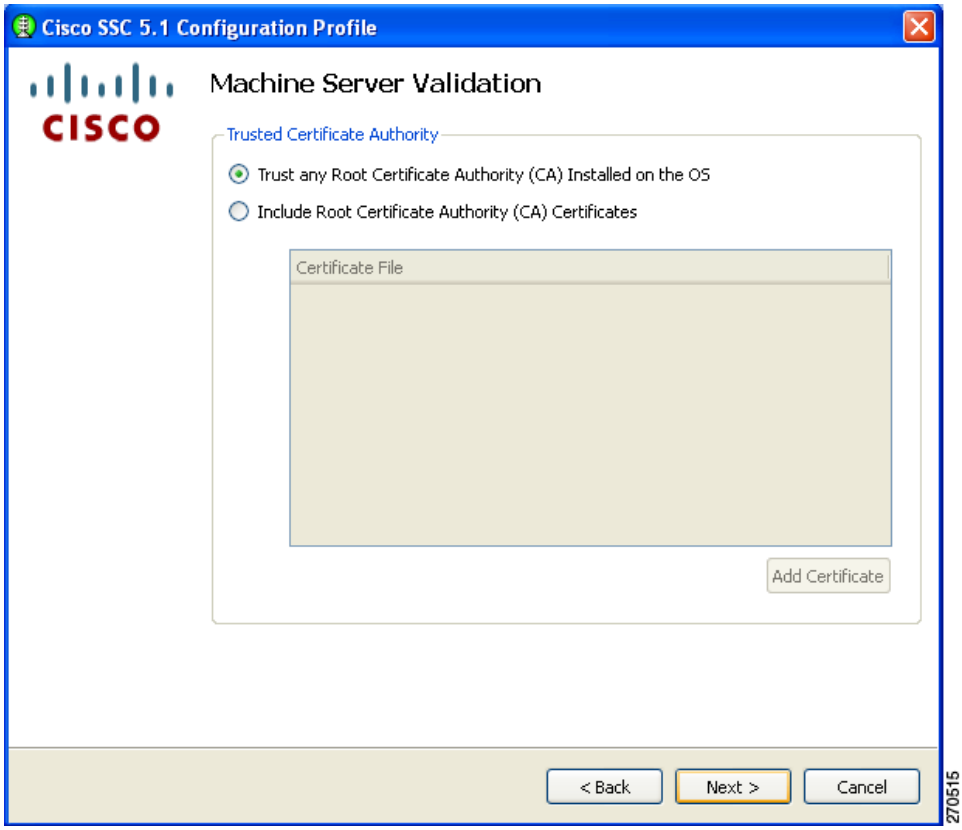
（注）　**Remove** をクリックして規則を削除します。

定義が完了したら、**Next** をクリックします。図 2-21 が表示されます。

信頼できる認証局の設定

Trusted Certificate Authority ウィンドウでは、認証機関のオプションを設定できます。

図 2-21　Trusted Certificate Authority ウィンドウ



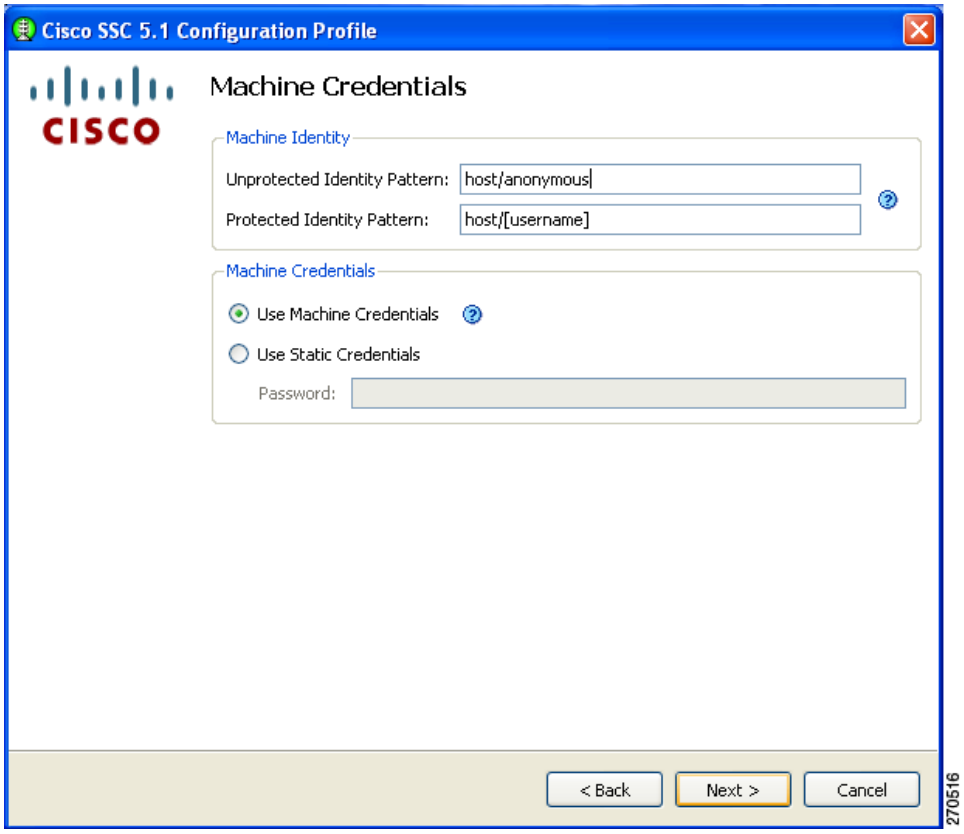
Include Root Certificate Authority (CA) Certificate オプションをオンにした場合は、**Add Certificate** をクリックして証明書ファイルを追加する必要があります。

設定が完了したら、**Next** をクリックします。Machine Credentials ウィンドウが表示されます（図 2-22）。

マシン クレデンシャルの設定

Machine Credentials ウィンドウでは、マシン クレデンシャルを指定できます（図 2-22）。

図 2-22　Machine Credentials ウィンドウ



（注）　EAP-TLS 認証方式が選択されている場合は、Protected Identity Pattern オプションを使用できません。

SSC リリース 5.0 以降では、ID を指定する際に次のプレースホルダ パターンがサポートされています。

- [username] 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。

[username] および [domain] のプレースホルダを使用する場合は、次の条件が適用されます。

- 認証にクライアント証明書が使用される場合、プレースホルダの値は、クライアント証明書の CN フィールドから取得されます。
- それ以外の場合、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、[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。

マシンの保護されていない ID の一般的なパターンは　*host/anonymous.[domain]* です。

　— このプロファイルに対してパスワード ソースが設定されている場合、パターンは実際の文字列となり、プレースホルダなしのユーザ名として送信されます。

マシンの保護された ID の一般的なパターンは *host/[username].[domain]* です。

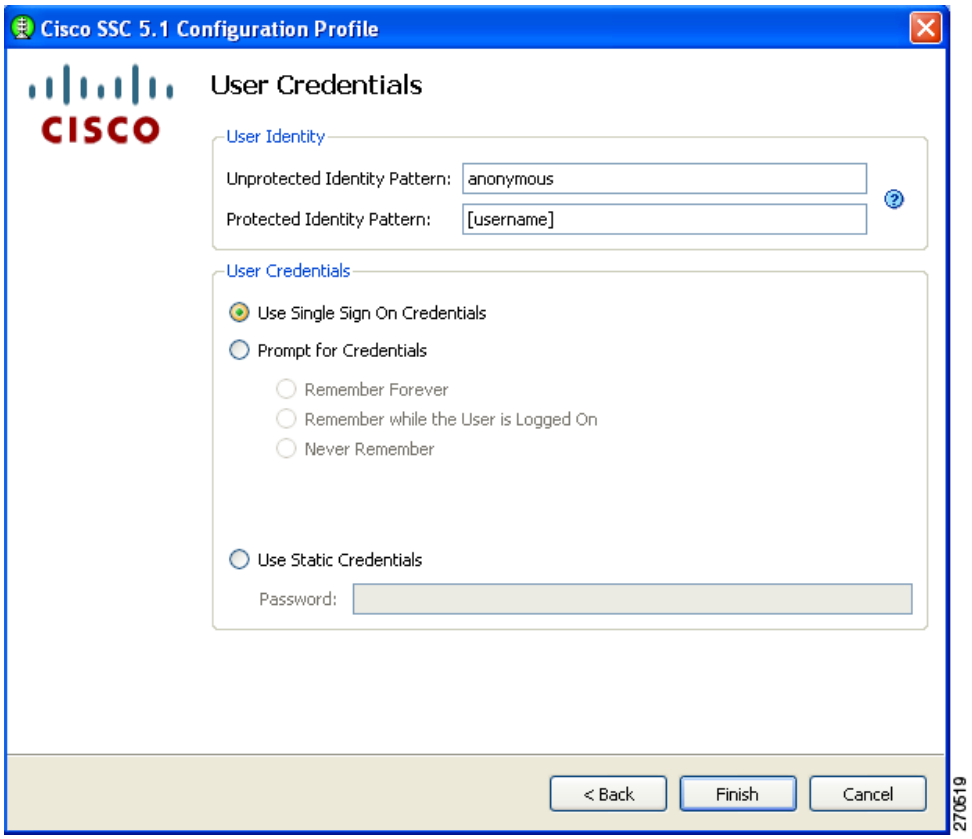
　— このプロファイルに対してパスワード ソースが設定されている場合、パターンは実際の文字列となり、ユーザ名として送信されます。

設定が完了したら **Finish** をクリックします。Networks ウィンドウが再表示されます（図 2-7）。

ユーザ クレデンシャルの設定

ユーザ接続を設定したら、User Credentials ウィンドウを使用してユーザ クレデンシャルを設定できます（図 2-23）。

図 2-23　User Credentials ウィンドウ



（注）　EAP-TLS 認証方式が選択されている場合は、Protected Identity Pattern オプションを使用できません。

SSC リリース 5.0 以降では、ユーザ ID を指定する際に次のプレースホルダ パターンがサポートされています。

- [username] 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。

[username] および [domain] のプレースホルダを使用する場合は、次の条件が適用されます。

- 認証にクライアント証明書が使用される場合、プレースホルダの値は、クライアント証明書の CN フィールドから取得されます。
  - クレデンシャル ソースがエンドユーザである場合、プレースホルダの値は、ユーザが入力した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る場合は、プレースホルダの値はログオン情報から取得されます。

ユーザの保護されていない ID の一般的なパターンは、トンネル方式の場合は *anonymous@[domain]* 、非トンネル方式の場合は *[username]@[domain]* です。

クライアント証明書が使用されていない場合、ユーザ ID パターンは実際の文字列となり、プレースホルダなしのユーザ名として送信されます。ユーザの保護された ID の一般的なパターンは *[username]@[domain]* です。

パスワード ソースがこのプロファイルである場合、パターンは実際の文字列となり、プレースホルダなしのパスワードとして送信されます。

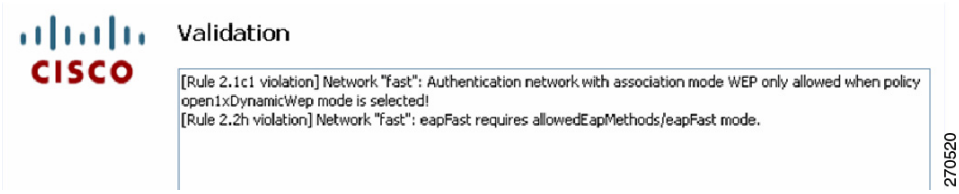
シングル サインオン クレデンシャル（SSC はクレデンシャルをオペレーティング システムから取得します）を使用するか、ユーザにクレデンシャルの入力を求めるか、または、展開ファイルにある実際の固定パスワード クレデンシャルを送信するように指定するかによって、ユーザ クレデンシャルを指定できます。

完了したら **Finish** をクリックします。指定したグループとネットワークの設定を含む、図 2-7 のウィンドウが再表示されます。**Next** をクリックすると、Validation ウィンドウが表示されます。

設定ファイルの検証

この時点で、管理ユーティリティはポリシー設定に対して、定義されたネットワークの検証を行います。なんらかのポリシー違反がある場合、それが表示されます。ファイルを保存する前にエラーを修正する必要があります。たとえば、エラーは Validation ウィンドウに表示されることがあります（図 2-24）。

図 2-24　検証エラーのある Validation ウィンドウ



違反が見つからなかった場合は、展開ファイルを任意の場所またはデフォルトの場所に保存できます。処理されたファイル（クレデンシャル、PAC、および CA 証明書を暗号化し、署名したもの）はデフォルトで次の場所に保存されます。

C:\Documents and Settings\All Users\Application Data\Cisco\Cisco Secure ServicesClient\newConfigFiles\configuration.xml

Cisco SSC クライアントは、新しい宛先パッケージを探す際にこの場所を調べます。システムにクライアントがインストールされている場合は、作成した設定を展開前に自動的にテストし、検証することもできます。

Finish をクリックすると、設定ファイルが保存されます。

作成した展開パッケージを変更する必要がある場合は、管理ユーティリティを再度開き、Welcome ウィンドウ（図 2-1）で **Modify Existing Configuration** をクリックして、保存した設定ファイルを選択します。

事前設定済みのクライアント宛先パッケージ ファイルの作成

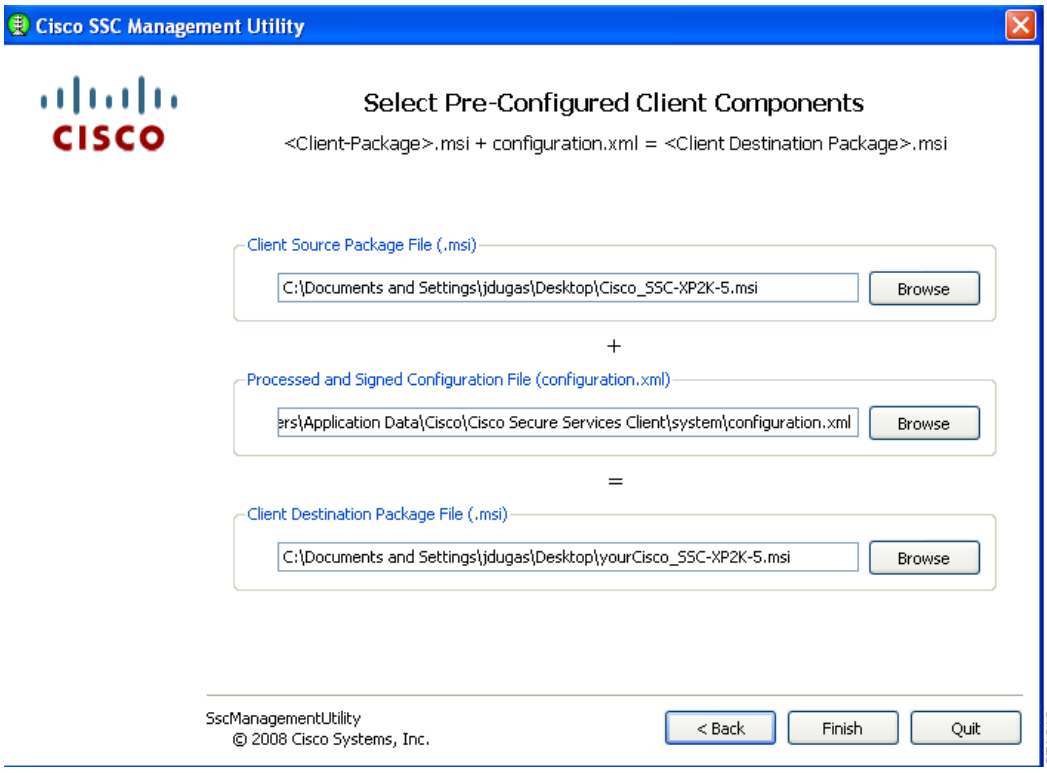
sscManagement Utility を使用すると、ネットワーク管理者によって設定されたプロファイルを使ってクライアント宛先パッケージを作成できます。

（注）　SSC 5.0 については、sscPackageGen ユーティリティを使用して宛先パッケージ ファイルを生成する必要があります。

Management Utility GUI の使用

事前設定済みのクライアント パッケージを作成するには、管理者が Management Utility GUI ウィンドウ上の Create Pre-Configured Client Package ボタンをクリックします（図 2-25）。

図 2-25　Select Pre-Configured Client Components ウィンドウ



管理ユーティリティは、クライアント ソース パッケージ ファイル（Cisco_SSC-SP2K-5.msi）を処理済みで署名済みの設定ファイル（configuration.xml）と結合し、最終的なクライアント宛先パッケージ ファイル（yourCisco_SSC-XP2K-5.msi）を生成します。

デフォルトのファイル場所を選択するか、**Browse** をクリックしてファイルを見つけます。**Finish** をクリックします。

事前設定済みのクライアント宛先ファイル（yourCisco_SSC-SP2K-5.msi）は、好みの配布方法を使用して任意のユーザ PC に配布できます。

SSC のグループ

グループは、基本的には設定された接続（ネットワーク）の集合です。設定された各接続は、いくかのグループに属するか、配信パッケージの *globalNetworks* セクションに含まれている必要があります。

（注） エンドユーザは、グループにのみネットワークを追加でき、*globalNetworks* セクションに追加することはできません（エンドユーザには通常、配信パッケージに署名できる管理ツールへのアクセス権がないため）。

接続をグループに分類することには、いくつかの利点があります。

- 接続する際のユーザエクスペリエンスの向上。この利点を説明するには、クライアントがネットワーク接続を確立するしくみを理解していることが重要です。クライアントは、正常な接続が確立されるまで、使用可能なネットワークのリストを定義された順序で試します。

  たとえば、ビジネス キャンパスの外部へ移動することが多い企業のエンドユーザの場合、WiFi パブリック ネットワークまたはホットスポット用に接続を設定します。グループがない場合は、新しく設定されたホーム ネットワークがこのリストの最後に追加されますが、このリストの数が非常に多い可能性があります。クライアントは、ホーム ネットワークへの接続が確立されるまで、すべてのパブリック ネットワークも含め、リストを最初から順に試します。この方法では、最後に追加されたネットワークへの接続が確立されるまでに時間がかかります。
- 設定された接続を簡単に管理。前の例で、エンドユーザが接続時間を短くするために一部の接続を削除した場合、削除された接続が後で必要になる可能性があります。ただし、接続リストをグループに分ければ、各グループ リストのサイズはずっと小さくなります。グループ間で簡単に切り替えることができ、より高速な接続が可能になります。

グループは、管理者またはエンドユーザが作成します。設定には少なくとも 1 つのグループが定義されている必要があります。複数のグループがある場合、1 つのグループを *アクティブ グループ*として選択する必要があります。クライアントは、アクティブ グループ内に定義された接続を使用してネットワーク接続を試行します。エンドユーザは、アクティブ グループでのみネットワークの追加または削除を行えます。グループを追加または削除するには、クライアント GUI のメイン ウィンドウで Configure Groups ボタンをクリックします。

配信パッケージの *globalNetworks* セクションで定義されているネットワークは、リストの上位に表示され、すべてのグループで利用できます。*globalNetworks* を作成できるのは企業の管理者のみであるため、ユーザ定義のネットワークが混在する場合でも、管理者はエンドユーザが接続できる企業ネットワークを制御できます。エンドユーザは、管理者が設定したネットワークを削除することはできません。

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うえでグループの知識を有する必要はないことに注意してください。作成した配信パッケージにデフォルトのグループを忘れずに指定するのは、管理者の責任です。使用可能なグループが 1 つだけである場合、クライアントはそれをアクティブ グループとして選択します。エンドユーザは、グループを使用しなくても、自分のネットワークを追加または削除できます。

（注） グループの選択は、リブートまたは SSC の修復中には維持されません。SSC を修復したり再起動した場合、SSC は configuration.xml ファイルで最初に設定されたグループに戻ります。

VPN 統合

SSC 5.1 は、自動的な VPN 接続機能が統合されますが、ユーザ PC に Cisco IPSec VPN クライアント（4.8 以降）をインストールする必要があります。SSC では、VPN 接続を確立するときに必要とされるユーザの操作が最小限に抑えられています。SSC IPSec VPN 認証オプションは、次のとおりです。

- Password 単純なパスワード認証を指定します。
- Secure Computing SofToken II 認証のための Secure Computing SofToken II からのソフト トークンを指定します。このオプションを使用するには、Secure Computing SofToken II がユーザの PC にインストールされている必要があります。SSC では、VPN デーモンにクレデンシャルとして自動的に渡されたパスワードを、Secure Computing SofToken II APIs を使用して取得します。
- Certificate 証明書認証を指定し、接続を使用して使用する証明書を指定します。このオプションを使用すると、エンドユーザによる入力は不要になります。

VPN コンセントレータがグループ認証などでユーザ認証を必要としない場合、ユーザは情報を入力する必要がありません。

認証が VPN コンセントレータによって要求されている場合、ユーザは以下の VPN ログオン情報の入力を求められます。

- Softoken authentication ソフト トークン アカウントのユーザ名と PIN のプロンプト。
- Password authentication ユーザ名とパスワードのプロンプト。
- Certificate authentication プロンプトは必要ありません。

VPN 接続に成功すると、SSC はユーザが PC にログオンしている間も将来の VPN 接続試行に備えてユーザが入力した情報を保持します。VPN 接続に失敗した場合、SSC はユーザに VPN ログオン情報の入力を再度要求します。

SSC はユーザがログオフする際、PC をシャットダウンする際、または SSC を修復する際にユーザの VPN 情報を削除します。

サポートされている VPN 機能

SSC は次の VPN 機能をサポートしています。

- VPN アクセスの 1 つのクレデンシャル セットは、すべてのネットワークと VPN 接続にアクセスし、ユーザがログオフするか、サービスが再起動（修復またはリブート）されるまで保持されます。
- 個々のプロファイルはそれぞれ自動的な VPN 接続、および VPN 接続エントリの選択を有効または無効にする設定を持ちます。
- ユーザが自動的な VPN 接続設定を変更できるように、ネットワークを編集するオプションが用意されています。
- SSC は、IPSec VPN と Secure Computing SofToken に対して .dll ファイルをロードします。.dll ファイルをロードできない場合、VPN 機能は無効化されます。
- SSC には VPN 接続の状況を示す新しいアイコンがあります。
  - トレイ アイコンを右クリックすると、Connect VPN または Disconnect VPN へのオプションが表示されます。
- ソフト トークン クレデンシャルのプロンプト。

サポートされていない VPN 機能

SSC は次の VPN 機能はサポートしていません。

- ソフト トークン クレデンシャルとしての、スキーマ内の固定クレデンシャルの使用。
- ソフト トークン クレデンシャルとしての、スキーマ内のシングル サインオン クレデンシャルの使用。
- ハードウィエア トークンの使用。
- Secure Computing SofToken II からのソフト トークンに対するパスワードの変更。