Cisco Secure Services Client
アドミニストレータ ガイド

Release 5.0

Text Part Number: OL-13686-01-J

本書に記載されている製品の仕様と情報は、予告なく変更される場合があります。本書内の記述、情報、および推奨事項は、すべて正確なものと考えられ、提示されていますが、明示か暗黙かを問わず、どのような保証もされていません。製品の使用についてはすべて、ユーザの責任となります。

製品のソフトウェア ライセンスおよび限定保証は、製品に同梱される情報パケットに記録され、この記述の内容が本書に適用されます。ソフトウェア ライセンスもしくは限定保証書が見つからない場合は、シスコの代理店に問い合わせて入手してください。

シスコが導入する TCP ヘッダ圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

本書におけるその他の保証にもかかわらず、シスコの代理店が提供するドキュメント ファイルおよびソフトウェアはすべて、すべての欠陥に対して「無保証」で提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

シスコまたはその代理店は、本書の使用または使用不能から発生する逸失利益、もしくはデータの損失または損傷を含みますが、これらに限定されることなく、すべての間接的、特別、二次的、または偶発的な損害に対して、シスコまたはその代理店がこの損害の可能性を通知されていた場合であっても、責任を負うものではありません。

このドキュメントで使用されているインターネット プロトコル（IP）アドレスは実際のアドレスを示したものではありません。このドキュメントに含まれる例、コマンドの出力表示、および図は説明のみを目的として提供されています。説明中に実際の IP アドレスが含まれていた場合は、意図的ではなく偶然に起因します。

Cisco Secure Services Client アドミニストレータ ガイド

CONTENTS

はじめに

ここでは、『Cisco Secure Services Client アドミニストレータ ガイド リリース 5.0』の概要説明、関連資料の参照情報を紹介し、その他のマニュアルおよびテクニカル サポートの入手方法を説明しています。

ここで取り上げる内容は次のとおりです。

対象読者と範囲

このガイドは、さまざまな企業部門 / 組織で、Cisco Secure Services Client (SSC) の複数のエンドユーザ マシンに対する派生エンドユーザ バージョンの設定および展開を担当する、システム管理者および IT 管理者を対象としています。このガイドに記載された情報は、サポートを担当するエンドユーザ マシンに関する次の定義とカスタマイズの全体に役立ちます。

- ポリシー：展開された SSC の機能とユーザ エクスペリエンスを定義します。
- ネットワーク：管理するすべての企業ネットワーク接続の設定を定義します。

マニュアルの構成

このガイドは、次のように構成されています。

第 1 章「エンタープライズ展開」には、事前設定されたエンドユーザ SSC の展開方法が記載されています。

第 2 章「SSC Management Utility GUI を使用した展開例」では、展開例を示し、Cisco SSC Management Utility を使用して企業固有の配信パッケージを作成する方法について説明します。

第 3 章「トラブルシューティング」では、Cisco SSC リリース 5.0 ログ ファイル、ログ メッセージ形式、ログ パッケージャ ユーティリティ、および SSC クライアントで問題が見つかった場合に行う操作について説明します。

付録 A「Postprocessing 検証エラー」には、postprocessing ユーティリティに関するエラー タイプおよびエラー メッセージのリストがあります。

付録 B「Cisco Secure Client Services リリース 5.0 ログ メッセージ」には、SSC リリース 5.0 クライアントによって生成されるログ メッセージの一覧があります。

表記法

このガイドでは、説明および情報を分かりやすく表示するため、次の表記法を使用しています。

- ユーティリティ コマンド
  - コマンドは、**太字**で示しています。
  - 変数は、*イタリック* 体で示しています。
- スキーマ オブジェクト
  - テキスト内でエレメント名とアトリビュート名を使用するときは*イタリック*体で表示されます。
- 「注」では、次の表記法と記号を使用します。

（注） *注釈*です。「注」には、その項に関連する追加情報や、このマニュアルに記述されていない参考資料が示されています。

ヒント 「ヒント」には役立つ情報が記載されます。

関連資料

Cisco Secure Services Client の詳細は、次の資料を参照してください。

- 『Cisco Secure Services Client リリース ノート』: 新機能および未解決および解決済みの注意事項が SSC のリリース別に記載されています。

これらのシスコ SSC 技術マニュアルは次の URL から入手することができます。

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

技術情報の入手、サポートの依頼、セキュリティ ガイドライン

技術情報の入手、サポートの依頼、マニュアルのフィードバックのご送信、セキュリティ ガイドライン、推奨エイリアス、および一般的なシスコのマニュアルの詳細は、毎月更新されるシスコ製品マニュアルの『What' New』を参照してください。これには新規および改訂があったシスコの技術マニュアルのすべてが掲載され、次の Web サイトにあります。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

エンタープライズ展開

この章は、次の項で構成されています。

概要

Cisco Secure Service Client（SSC）は、セキュリティを確保して有線および無線接続を行うための 802.1X 認証サプリカントです。SSC にはステータスを表示し、ユーザのコマンドを受け入れるユーザ インターフェイスがあります。IEEE 802.1X セキュリティ プロトコルで保護されたネットワークにコンピュータを接続できます。クライアント / サーバ認証が正常完了しないと、802.1.X 対応アクセス デバイス（無線アクセス ポイントまたは有線イーサネット スイッチ）のポート アクセス コントロールによってネットワークに対するエンドユーザの接続が許可されません。

SSC には次の 2 つの基本バージョンがあります。

- アウトオブザボックス バージョン

  cisco.com からダウンロードされた SSC は設定されていません。これは、エンドユーザ バージョンの設定と導出されたバージョンの展開を行う IT 組織向けのバージョンです。この展開バージョンは、サポート対象のさまざまな企業部門および組織での使用に適しています。IT 管理者がユーザ エクスペリエンスおよびエンドユーザが実行可能な選択および設定オプションを管理します。アウトオブザボックス バージョンは、ほとんどの機能へのアクセスを可能にし、初期開始時にネットワークの設定を必要とする完全なオープン ポリシーに基づいています。ただし、IT 管理者が設定およびネットワーク設定のすべてを完全に管理するには、配信パッケージ設定ファイルを展開する必要があります。

- デフォルトのダウンロード パッケージ。これには、無期限の有線のみのライセンスで構成されたデフォルト設定が含まれています。無線トライアル ライセンスは、次の URL にある cisco.com からダウンロードできます。

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

  無線トライアル ライセンスが有効化されると、次の実行が可能になります。

  （1）90 日間の一時的なライセンスによる無線機能の評価

  （2）有線および無線の双方の機能を備えた製品の永続的なライセンス取得

- エンドユーザ展開バージョン

  展開されるエンドユーザ バージョンは、多くの場合 IT/ システム管理者が機能セットの制限などを設定の記述によって事前設定して、展開されます。通常は、企業ネットワークへの即時接続を許可する事前定義の企業ネットワークが 1 つ以上組み込まれます。

（注） アウトオブザボックスのデフォルトの有線 SSC でサポートされるものは次のとおりです。

- 有線（802.3）ネットワーク アダプタ
- EAP 方式：EAP-FAST、EAP-MSCHAPv2、EAP-GTC、EAP-TLS
- 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

トライアル ライセンスでは、以下のサポートも追加されました。

- 無線（802.11）ネットワーク アダプタ
- 他の EAP 方式：LEAP、EAP-PEAP、EAP-TTLS、EAP-MD5

サポートされるオペレーティング システム環境

サポートされるオペレーティング システム環境は次のとおりです。

- Windows XP Professional（SP1、SP2）Windows 2000（SP4）または Windows 2003 サーバ

（注） Home、Media Center、Tablet PC、Professional x64 など、他のエディションの Windows XP はサポートされません。

配信パッケージ

配信パッケージでは、個別のエンドユーザ SSC の動作および接続方法が定義されます。配信パッケージは、次の機能ブロックが含まれた設定ファイルで構成されます。

- ライセンス

  展開されるエンドユーザ SSC にはまず、シスコシステムズから入手した企業ライセンスが必要です。これは、アウトオブザボックス バージョンに付属する有線専用ライセンスに置き換わるものです。

- ポリシー
  - ユーザ管理ポリシー

    ネットワーク メディア サポートを設定します。
  - ネットワーク ポリシー

    サポート対象ネットワークすべてのタイプおよび機能の制限を設定します。
- 接続設定

  ネットワーク接続実行時のグローバルな動作を設定します。
- 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することができ、*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、各リストのサイズはずっと小さくなります。グループを使用すれば、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は、1 つのグループを *アクティブなグループ*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 グループで定義された接続を使用してネットワーク接続を行います。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 のメイン画面で *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することができます。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持ってい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、リブートまたはクライアントを修復した後は維持されません。クライアントを修復したり再起動した場合、クライアントは configuration.xml ファイルで最初に設定されたグループに戻ります。

- ネットワーク

  ネットワークには、単一または一連のネットワーク プロファイルの記述が組み込まれます。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。このプロファイルには次の特性があります。

  - 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 Credential（PAC）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構成設定を編集できません。

SSC を必要な企業環境に合わせて調整する際に必要な主要手順は、次のとおりです。

1. 作成：管理者が配信パッケージ ファイルを作成します。個別の配信パッケージ ファイルには、1 つ以上のネットワークの設定の記述を格納できます。配信パッケージの形式、構造、およびコンテンツの詳細は、「配信パッケージの作成」を参照してください。
2. 展開：管理者はアプリケーションおよび配信パッケージ ファイルをパッケージ化してエンド ステーションに展開します。展開オプションと手順の詳細は、「配信パッケージ」を参照してください。
3. 導入：SSC によって配信パッケージ ファイルが検出され、使用されます。この手順は自動で行われ、管理者の操作は必要ありません。展開の手順の完了後まもなく、新規の配信パッケージ ファイルの存在が検出されます。その後、確認の処理が行われ、有効性が確認されると、SSC の自動再設定が適宜実行されます。

配信パッケージ ユーティリティ

配信パッケージの作成と展開に必要なすべてのユーティリティ ツールおよびサポート ファイルが 1 つのパッケージ化されたファイル、SSCMgmtToolkit_{ リリース }.zip に格納されます。この章の後半部分では、項目のそれぞれを紹介して、説明します。

ユーティリティ パッケージは Cisco SSC ダウンロード ページからオンラインでダウンロードできます。まず、下記の SSC 製品サポートにアクセスしてください。

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

Download Software > **Client Adapters and Client Software** の順にクリックして、プロンプトに従って SSC ダウンロード ページにアクセスします。

配信パッケージの作成

配信パッケージのスキーマ

SSC の配信パッケージ ファイルには、XML 形式が使用されます。特定の .xml 配信パッケージ（設定）ファイルの全体的な構造は、SSC 配信パッケージ スキーマ、configuration.xsd によって定義されます。

SSC 配信パッケージ スキーマは、標準 W3C XML スキーマに準拠したドキュメントで、すべての .xml 設定ファイルのコンテンツの記述および制約に使用されます。このガイドの読者は、W3C XML スキーマ仕様の構文および XML 出力のインスタンス生成に精通しているものと想定されます。

スキーマ のプロパティ

このスキーマには次の特色があります。

- 配信パッケージ インスタンスの XML ファイルはすべて、エンドユーザの設定を十分に理解できるように読み取り可能なテキスト ファイルになっています。ユーザの可読性をサポートするため、スキーマには次の特性があります。
  - 構成設定のそれぞれは、特定のスキーマ エレメントで示されます。
  - 構成設定は、オプション エレメントの存在またはエレメント値によって伝達されます。
  - スキーマ アトリビュートを使用することで、より明確な構成設定が可能になります。
- ネットワークの定義は階層的な決定ツリー構造です。スキーマを使用した設定を進めるに従って、選択に応じたツリーが構造化されます。ツリーを詳細に検討することにより、必要な固有のタイプのネットワークに関係する設定可能パラメータのセットが自動的に絞られます。さらに、これによって、特定の設定パラメータに使用可能な値セットも自動的に絞り込まれます。たとえば、無線ネットワークには接続のアソシエーション モードの設定が必要です。このときに、認証ネットワークを選択した場合と共有ネットワークを選択した場合とでは、使用可能な値セットが異なります。決定は基本的に次の順序で行われます。

  すべてのネットワーク

  1. ネットワークの接続メディア（有線または無線）の選択
  2. 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）の選択
  3. ネットワークの接続コンテキスト（マシンのみ、ユーザのみ、マシンおよびユーザ）の選択

  認証ネットワークの決定ツリーの場合は、次のように続行します。

  4. クレデンシャル タイプと収集方式の選択
  5. 認証方式（複数の場合あり）の選択

スキーマの確認

スキーマには列挙値が含まれますが、使用可能な用途およびエレメントの組み合わせや、非列挙的文字列の要件のすべてを明示的に指定するわけではありません。これらの詳細にはビジネス ルールのセットで対応します。

このため生成される .xml 配信パッケージ ファイルが SSC で受け入れられるようにするには、次の基準を満たす必要があります。

- .xml ファイルは、SSC 配信パッケージ スキーマの構文要件に従い有効であること。
- .xml ファイルは、スキーマのビジネス ルールのエレメント関係要件に従い有効であること。

配信パッケージの作成手順

配信パッケージ xml インスタンス ファイルを作成するには、2 とおりの基本的な方法がサポートされています。

- スキーマの言語に基づく方法：リリース 4.2 より前のリリースでは手動プロセスをサポート
- 記述の英語に基づく方法：ウィザード ユーティリティ

スキーマの言語に基づく方法

次の手順を使用して、配信パッケージ ファイルを作成します。

ステップ 1　SSC スキーマの指定に従って、記述 .xml 配信パッケージ ファイルを生成します。これを実行するその他の方法として、次の方法もあります。

- スキーマから XML インスタンス ファイルを直接作成できる市販の XML エディタを使用します。これらのツールで XML を編集する際は、コンテキスト ヘルプを利用してインスタンス ファイルの確認に利用することができます。この種のアプリケーションの例として、次のアプリケーションが挙げられます。
  - Altova 社製 XMLSpy
  - データディレクト テクノロジーズ社製 Stylus Studio
- 任意のテキスト エディタと、スキーマ構造とエレメントの詳細説明を使用して、最初からまたは記載例をカット アンド ペーストして、XML インスタンス ファイルを作成します。

ヒント　テキスト言語（この場合は XML）の構文を認識するプログラム テキスト エディタを使用することによって、テキストの編集が大幅に簡略化されます。この種のエディタは多数市販されています。終了タグの自動挿入やエレメント インデントのクリーンアップなどの追加機能がサポートされるエディタもあります。

ヒント　XML 構文

XML の構文規則は非常に単純です。ここでは、基本的な概念のいくつかを紹介します。

- .xml ファイルのそれぞれにルート エレメントがありますが、ここでは *configuration* です。これは記述エレメントのコンテナとして機能します。
- すべての XML エレメントに終了タグが必要です。
- XML エレメントが正しくネストされている必要があります。
- XML タグでは大文字と小文字が区別されます。
- エレメントには子エレメント、コンテンツ（テキスト値）、アトリビュートを任意の組み合わせで組み込むことができます。
- アトリビュート値はすべて引用符で囲む必要があります。
- 正しくない XML 文字は、次のエンティティ参照で置き換える必要があります。エンティティ参照は必ず「&」記号で始まり「;」記号で終わります。

  小なり：文字 < には < を使用します。
  大なり：文字 > には > を使用します。
  アンパサンド：文字 & には & を使用します。
  アポストロフィ：文字 ' には ' を使用します。
  引用符：文字 " には " を使用します。
- 空白は保持されます（これは、指定の列挙コンテンツ値の入力時などに重要です。列挙値およびブール値には先行空白と後続空白を使用しないでください）。
- コメントは構文 <!-- コメント --> で囲みます。

個別の .xml 配信パッケージ ファイル（配信パッケージ スキーマのインスタンスとも呼ばれます）は、次のビルディング ブロックから構築されます。

```
<configuration>
  <childElement>with content</childElement>
  <elementWithAttr attr=”{value}”>
    <anotherChild>
      <!-- その他の階層エレメント -->
    </anotherChild>
  </elementWithAttr> <!-- 終了タグを正しくネストします -->
  <emptyElement1></emptyElement1> <!-- 空白エレメントには子やコンテンツはありません -->
  <emptyElement2/> <!-- このマニュアルで使用される空白エレメントの短縮形表記 -->
</configuration>
```

（注）　配信パッケージ ファイル名：
配信パッケージの名前は configuration.xml である必要があります。

ステップ 2　生成されたパッケージ配信 .xml ファイルを SSC postprocess コマンドライン ユーティリティ、sscManagementUtility.exe に転送します。sscManagementUtility では、次の必須動作が実行されます。

- 後処理後の配信パッケージのスキーマとビジネス ルール違反の検証を行います。
- すべてのクレデンシャルとシークレットを元のクリア テキストから暗号化します。

- 入力ファイル（生成された配信 .xml ファイル）で参照されたすべてオプション ファイルを取得しパッケージ化します。オプション ファイルには、PAC や CA 証明書があります。
- 配信パッケージ ファイルにデジタル署名を行い、エンド ステーションに配置された際のコンテンツの不正変更を防止できるようにします。

このユーティリティのコマンドラインの記述については、「Postprocessing ユーティリティ」を参照してください。

記述の英語に基づく方法

配信パッケージ ファイルの作成プロセスを順を追って説明するウィザードが用意されています。sscManagementUtility の GUI を使用することで、以下の操作を行えます。

- 検証および署名済みの配信パッケージを最初から作成する
- 署名されていない既存のファイルをインポートして、それを基に変更する
- 既存の配信パッケージに対して後処理を実行する

sscManagementUtility の GUI バージョンは、SSC リリース 4.1 以降のすべてのバージョンに対して、配信パッケージ xml ファイルの作成および処理をサポートしています。

sscManagementUtility を実行して、ユーティリティを開きます。ユーティリティを呼び出し、GUI を開始します。

Postprocessing ユーティリティ

postprocessing ユーティリティのコマンドライン バージョンの構文を以下に示します。.

sscManagementUtility.com {***help*** | ***validate*** | ***sign***} [command specific arguments]

sscManagementUtility.com *help*

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

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

表 1-1　sscManagementUtility コマンド エレメント

コマンド エレメント	意味
validate	配信パッケージ xml ファイルのみを検証します。
sign	配信パッケージ xml ファイルの後処理（検証、暗号化、署名）を行います。
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
-i *input-file* ***--in***=*input-file*	処理対象の配信パッケージ xml ファイルへの絶対または相対パス
-o *output-file* ***--out***=*output-file*	処理され、展開の準備ができた配信パッケージ xml ファイルへの絶対または相対パス

標準エラー出力（stderr）には、次のようなエラーが送信されます。

- 使用エラー（不適切なコマンド）
- ファイル I/O エラー
- 配信パッケージ XML ファイルの不明なバージョン
- XML スキーマ確認エラー

- XML 暗号化エラー
- XML 署名エラー
- ビジネス ルール違反

後処理で生成されるエラーの概要については、付録 A「Postprocessing 検証エラー」を参照してください。

（注） ユーティリティ（sscManagementUtility.com）には、次のサポート　ファイルが必要です。これらのファイルは、SSC バージョンで構成されたデータ フォルダの SSCAdminUtils_{ リリース }.zip ファイルで提供されます。このフォルダ構造は、zip ファイルの内容を解凍する際、そのまま維持する必要があります。

- configuration.xsd、スキーマ ファイル

  リリースの番号は、スキーマ自身で定義されます。インスタンス化された各配信パッケージ xml ファイルは、ファイルに関連付けられたスキーマ ファイルのリリース番号決定方式を維持します。

- validateRules.xsl、ビジネス ルール ファイル

  リリース番号付けは、次のようにファイルの名前空間によって制御されます。

  xmlns:validateRules="http://www.cisco.com/2007/CSSCValidationRules/A.B.C、ここでは A、B、および C は、それぞれメジャー、マイナー、メンテナンスに対応します。

（注） 管理ユーティリティは、Microsoft msvcp71.dll および msvcr71.dll ファイルを使用します。通常、これらのファイルは、SSC のインストール時にシステムにロードされます。これらの展開ツールを SSC がないマシンで使用可能にするため、これらのファイルは SSCAdminUtils_{ リリース }.zip ファイルで提供され、ユーティリティと同じフォルダに配置されます。

また、ユーティリティの GUI バージョンは、提供されているいくつかの QT dll ファイルを使用します。これらもユーティリティと同じフォルダに配置する必要があります。

配信パッケージ - SSC リリースの互換性

SSC のリリース番号付け

シスコから取得した管理ツールキット パッケージ（.zip）ファイルおよびインストール ファイル（.msi）の前のリリースは、次のような形式になっています。

SSCMgmtToolkit_A.B.C.xxxx.zip または Cisco_SSC-{OS}-A_B_C_xxxx.msi

Windows 2000/XP リリースの SSC の場合は、次のようになります。

SSCMgmtToolkit_A.B.C.xxxx.zip または Cisco_SSC-XP2K-A.msi です。ここで、*A* は、メジャー リリースの変更を示します。

SSCMgmtToolkit と SSC の間の互換性

次の表は、指定の SSC リリースのすべての機能を備えた配信パッケージを生成するために使用する管理ユーティリティ パッケージのリリースの一覧です。

表 1-2　管理ユーティリティと SSC

管理ツールキット パッケージのリリース	サポートされる SSC リリース
SSCMgmtToolkit_5.0.0.xxxx.zip	Cisco_SSC-XP2K-4_1_0_xxxx.msi
	Cisco_SSC-XP2K-4_1_1_xxxx.msi
	Cisco_SSC-XP2K-4_1_2_xxxx.msi
	Cisco_SSC-XP2K-4_2_0_xxxx.msi
	Cisco_SSC-XP2K-5.msi

配信パッケージと SSC の間の互換性

SSC リリース 5.0 は、メジャー ソフトウェア リリースであり、新しいスキーマが使用されています。このスキーマは以前の SSC リリースのスキーマと互換性がありません。古いスキーマから新しいスキーマへの変換を支援するため、スキーマ変換ツールが用意されています。詳細については、「SSC リリース 4.1.x インストールから SSC リリース 5.0 へのアップグレード」の項 (P.1-12) を参照してください。

この変換ツールでは、管理者が作成した SSC リリース 4.1 の配信パッケージ（スキーマ バージョン 4.1.x）を SSC リリース 5.0 スキーマに変換できません。ただし、SSC リリース 4.1 の内部設定ファイル（*Program Files¥Cisco Systems¥Cisco Secure Services Client* にあるファイル）を使用して、管理者が設定したネットワークを SSC リリース 5.0 スキーマに変換します。

配信パッケージの展開

シスコでは、すでに IT 管理者にはエンドユーザ ステーションへのファイルの移動に優先的に使用する方法（Microsoft の SMS 方式など）があると想定しています。

このためシスコでは独立したコマンドライン ユーティリティ sscPackageGen.exe を用意して、次のエンタープライズ展開操作を容易にします。

- Windows インストーラによる事前設定 SSC の 1 ステップ インストール
- Windows インストーラによる初期展開 SSC およびインストール済み SSC の更新

（注） リモート デスクトップによる展開はサポートされていません。

エンタープライズ展開ユーティリティ

エンタープライズ展開ユーティリティ（sscPackageGen）は、アウトオブザボックス インストール ファイル（.msi）、および配信パッケージ ファイル（.xml）を入力として取得し、新たな事前設定済みインストールファイル（.msi）を生成します。ユーティリティの構文は次のとおりです。

sscPackageGen {***insert*** | ***patch***} *source dest file*

表 1-3　sscPackageGen コマンド エレメント

コマンド エレメント	意味
insert	msi ファイル作成コマンド
patch	msp ファイル作成コマンド
source	入力 msi ファイルへの完全絶対パス
dest	出力 msi または msp ファイルへの完全絶対パス
file	入力配信パッケージ xml ファイルへの完全絶対パス

エンドユーザの初期インストール

次の方式のいずれか 1 つを選択して、エンドユーザ SSC の初期インストールを行います。

- エンタープライズ展開インストール方式
- 従来のインストール方式（推奨）

エンタープライズ展開インストール方式

SSC および対応する配信パッケージは、単一のファイルとして展開され、単一操作でインストールされます。必要なサポート ファイル（CA 証明書および PAC）は、すでに配信パッケージ自体に追加されていることを思い出してください。

例 1-1　初期インストール ファイル

シスコから入手したインストール ファイル（Cisco_SSC-XP2K-5）、および各自の検証および後処理済みの配信パッケージファイル（configuration.xml）から *yourSSCInstallPkg.msi* という名前の事前設定済みインストール ファイルを作成します。

```
sscPackageGen insert C:¥Cisco_SSC-XP2K-5.msi C:¥yourSSCInstallPkg.msi
C:¥configuration.xml
```

yourSSCInstallPkg.msi をエンド ステーションに展開して実行すると、SSC が事前定義した配信パッケージ設定でインストールされます。

SSC では、標準の Microsoft インストーラ メカニズムによる 1 ステップのサイレント インストールがサポートされます。この例の場合は、次を実行します。

msiexec /i yourSSCInstallPkg.msi /quiet /norestart

（パラメータ *norestart* は、サイレント インストールでコンピュータが再起動されないようにします）

従来のインストール方式

複数手順の操作（Release 4.1 より前のリリースと同様）も使用できます。

1. シスコから入手したインストール ファイル（Cisco_SSC-XP2K-5）を展開して、インストールします。
2. エンドユーザの設定を次の項の説明に従って更新します。

（注） SSC リリース 5.0 以降では、中間ドライバを使用してネットワーク アダプタを制御します。インストールは停止し、SSC が共存できない別のドライバの存在が検出されたかどうかをユーザに通知します。競合するアプリケーションは無効化するかアンインストールする必要があります。

エンドユーザの設定の更新

エンドユーザの設定の更新には、従来の更新方式が使用されます。

後処理後の配信パッケージ .xml ファイルの展開（SSC リリース 4.1 より前のリリースと同様）を実行できます。

1. SSC インストーラによって作成された次のフォルダに、新規 / 更新の後処理後の配信パッケージ .xml ファイルを展開します。

   C:¥Documents and Settings¥All Users¥Application Data¥Cisco¥
   Cisco Secure Services Client¥newConfigFiles

2. Cisco Secure Services Client サービスを再開するか、Help メニューから **Repair** を選択します。

（注） SSC では、新しい接続を行うときに、新しい設定ファイルを検出し実装することもできます。

SSC リリース 4.1.x インストールから SSC リリース 5.0 へのアップグレード

既存の SSC 4.1.x リリースから SSC リリース 5.0 へアップグレードするコンポーネントには、次の 2 種類があります。

- SSC リリース 4.1.x より前に展開された管理者（ロックされた）ネットワークはすべて、SSC リリース 5.0 にアップグレードする必要があります。
- エンドユーザが作成した SSC リリース 4.1.x のネットワークはすべて、SSC リリース 5.0 にアップグレードする必要があります。

管理者が展開したネットワークの SSC リリース 4.1.x から SSC リリース 5.0 へのアップグレード

管理者のコンピュータには、SSC リリース 5.0 クライアント エレメントがなければなりません。

- SSC リリース 5.0 インストール msi ファイル（Cisco_SSC-XP2K-5.msi）
- 設定管理ユーティリティ（SSCMgmtToolkit_5.0.0.xxxx.zip）
- 設定統合ツール（ConfigCombiner.exe）
- 設定変換ツール（ConfigConverter.exe）
- 管理者 xslt ファイル（configConvert_3_1_admin.xslt）：管理者設定 SSC リリース 5.0 スキーマの変換に使用します。
- カスタム インストール パッケージを生成する sscPackageGen

また、管理者は最新の SSC Release 4.x 展開パッケージを SSC リリース 4.1.2 内部設定に変換する必要があります。これは、*Program Files¥Cisco Systems¥Cisco Secure Services Client* フォルダにある *profiles* フォルダです。

SSC リリース 4.x 配信と同じように設定された SSC リリース 5.0 クライアントを展開するには、次の操作が必要です。

1. 統合ツール（ConfigCombiner.exe）を使用して、SSC リリース 4.1 の設定ファイルを 1 つのファイルにまとめます。

   使用方法：ConfigCombiner.exe [options]

   オプションは次のとおりです。

   --source *directory* or -s *directory*：ソース ディレクトリ パスを指定します。ソース ディレクトリ オプションが指定されていない場合、ソース ディレクトリのデフォルト値は *C:¥Program Files¥Cisco Systems¥Cisco Secure Services Client¥profiles* です。

   --quiet または -q：結果をダンプしません。

   --help：ツールの使用方法を示します。

統合ツールの使用例を以下に示します。

```
ConfigCombiner.exe -q
```

この操作の出力として、*configuration.xml* というファイルが生成されます。このファイルは、ツールを実行したフォルダに配置されます。ファイルには、*c:¥Program Files¥Cisco Systems¥Cisco Secure Client Services¥profiles* にある複数のフォルダの情報が含まれます。

（注） この操作の結果として SSC リリース 4.1.x ファイルが変更されることはありません。

2. 管理者 XSLT ファイル（configConvert_3_1_admin.xslt）に変換ツール ConfigConverter.exe を使用して、統合ツールの出力を単一の SSC リリース 5.0 configuration.xml ファイルに変換します。

   使用方法：ConfigConverter.exe [options]

   オプションには以下の値を使用できます。

   --quiet or -q：結果をダンプしないように指定します。

   --output *filename* or -o *filename*：出力 XML ファイルを指定します。

   --input *filename* or -i *filename*：入力 XML ファイルを指定します。

   --xslt *filename* or -xslt *filename*：XSLT ファイルを指定します。

   管理者が展開したネットワークを ConfigConverter ツールを使用して変換するときは、*--xslt* ファイル オプションを指定し、XSLT ファイル名を **configConvert_3_1_admin.xslt** に設定する必要があります。エンドユーザのシステムでエンドユーザが作成したネットワークを変換するために、さまざまなデフォルト xslt ファイルに対して使用されるツールと同じものです。

   変換ツールの使用例を以下に示します。

   ```
   ConfigConverter.exe -i configuration.xml -o configuration.xml--xslt
   configConvert_3_1_admin.xslt
   ```

   この操作の出力は、SSC リリース 5.0 のスキーマと互換性があり、SSC リリース 4.1.x で展開されたネットワークと同じ構成の配信パッケージです。

3. ここで、以下の操作を実行するために管理ユーティリティを使用できます。
   - SSC リリース 5.0 configuration.xml（管理者が展開した SSC リリース 4.1 ネットワークを含む）を読み込む
   - 必要に応じて、SSC リリース 5.0 configuration.xml ファイルおよびルートを変更する
   - SSC リリース 5.0 configuration.xml ファイルに署名する
4. packageGen ツールを実行して、署名された configuration.xml ファイルを SSC リリース 5.0 の msi ファイルとバンドルし、パッケージを展開します。

エンドユーザが作成した SSC リリース 4.1.x ネットワークの SSC リリース 5.0 へのアップグレード

SSC リリース 5.0 をアップグレードとしてコンピュータにインストールすると、SSC リリース 4.1.x でエンドユーザが作成したネットワークは自動的に SSC リリース 5.0 ネットワークへアップグレードされます。管理者またはエンドユーザは何もする必要がありません。アップグレードの結果は次のようになります。

- SSC リリース 5.0 が、展開された管理者の設定ファイルで実行を開始します。
- SSC リリース 4.1 でエンドユーザが作成したプロファイルはすべて、SSC リリース 5.0 クライアントにインポートされます。
- この変換は、アップグレードの間に 1 回だけ行われます。

- SSC リリース 4.1 では複数のユーザ xml ファイルがエンドステーション上にありますが、SSC リリース 5.0 ではユーザ XML ファイルは 1 つだけです。変換ツールは、SSC リリース 4.1 の複数のユーザプロファイル ファイルの内容を SSC リリース 5.0 の単一のユーザ XML ファイルにまとめます。SSC リリース 4.1 の各ユーザ XML ファイルは、SSC リリース 5.0 のグループに対応します。グループ名は、ユーザ xml ファイル名で、先頭に *CSSC4_* が付いています。*allusers* ファイル内のプロファイルは、*CSSC4_allusers* グループに組み込まれます。エンドユーザは、使用可能なネットワークのリストを GUI を使用して確認し、不要なネットワークはある場合は削除する必要があります。
- SSC リリース 4.1 の 1 つのネットワークに対して、SSC リリース 5.0 では複数のネットワークが作成されることがあります。これは、SSC リリース 4.1 のスキーマでは、各ネットワークで複数の EAP 方式を使用できるのに対し、SSC リリース 5.0 のスキーマでは、各ネットワークで EAP 方式を 1 つしか使用できないためです。つまり、SSC リリース 4.1 のユーザ ネットワークは、SSC リリース 5.0 への変換後は、SSC リリース 4.1 のネットワーク名と EAP 方式の両方が含まれたネットワーク名になるということです。これは、混乱を避けるために行われる処置です。
- SSC リリース 4.1 から SSC リリース 5.0 へのアップグレードのとき、ユーザの静的クレデンシャルはすべて SSC リリース 5.0 にインポートされます。ユーザが入力した WEP および PSK クレデンシャルも SSC リリース 5.0 にインポートされます。ただし、802.1x クレデンシャルはインポートされません。これらは必要に応じて再入力する必要があります。

クライアント証明書の事前インストール

エンドユーザ SSC ファイルでクライアント証明書をベースとする EAP 方式が使用される場合は、ユーザのクレデンシャルの提供に使用されるクライアント証明書を別途展開して、適切な Windows 証明書ストア（ユーザの個人用のストア）に配置する必要があります。配信パッケージ ファイルではクライアント証明書は展開されません。

CHAPTER 2

SSC Management Utility GUI を使用した展開例

この章では、展開例を示し、Cisco SSC Management Utility を使用して企業固有の配信パッケージを作成する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。

SSC Management Utility GUI の展開例

SSC 管理ユーティリティを使い始める前に、次の点に注意してください。

- 項目の横にある？記号をクリックすると、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ページは、現在のページで何を選択するかによって決まります。

次の手順で、GUI を使用して企業固有の配信パッケージを作成する方法を説明します。

ステップ 1　**sscManagementUtility.exe** をクリックすると、最初のページが表示されます（図 2-1 を参照）。

図 2-1　SSC Management Utility Welcome ページ

このページには 3 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最初から作成します。
- Modify Existing Configuration Profile：以前に作成した（未処理の）展開ファイルを修正します。
- Process Existing Configuration Profile : 既存の未処理の展開ファイルを処理します。処理では次の操作が行われます。
  - ファイル内のクレデンシャルとその他のシークレットの暗号化
  - CA 証明書およびファイルで指定されている PAC ファイルの取得
  - 管理者によって展開された設定ファイルの不正変更を防ぐための、生成されたファイルへの署名

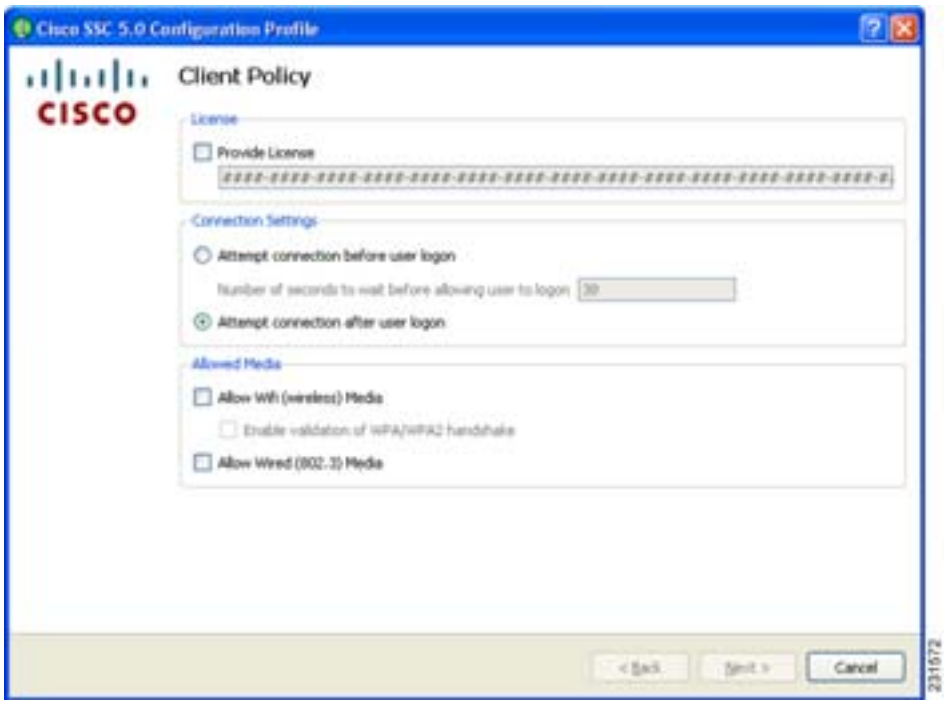
ステップ 2　新しい設定ファイルを最初から作成する場合、**Create New Configuration Profile** をクリックすると、図 2-2 が表示されます。

図 2-2　Select Cisco SCS Version ページ

SSC 管理ユーティリティを使用すると、Cisco SSC リリース 5.0、4.1、および 4.2（この図では SCS 5.0 のみが表示されています）の設定ファイルを作成できます。

ステップ 3　**Cisco SSC 5.0** をクリックすると、Client Policy（図 2-3）が表示されます。

図 2-3　Cisco Policy ページ



（注）　Cisco SSC リリース 5.0 では、エンドユーザが 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。企業の管理者は、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、有効なライセンスが含まれた配信パッケージを作成する責任があります。

このページには 2 つのセクションがあります。

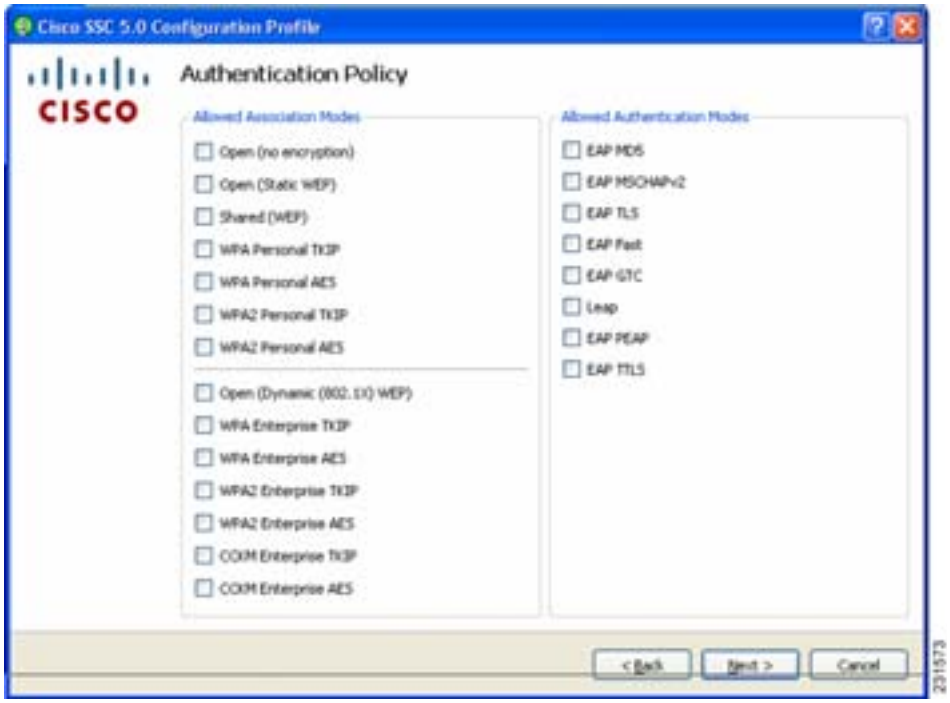
- Connection Settings section：ログオン前など、Windows ドメイン認証の前に 802.1x 認証を試みる必要があるかどうかを指定します。ログオン前の場合は、接続までの待機時間を指定することもできます。この時間の間にネットワーク接続を確立できない場合、Windows ログオン プロセスはユーザ ログオンを続行します。
- Allowed Media section：Cisco SSC クライアントで制御するメディアの種類を指定します。

（注）　Cisco SSC リリース 5.0 は、シングルホームであるため、同時に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。

無線メディアが許可されている場合は、WPA/WPA2 ハンドシェイクの検証を有効または無効にすることができます。

ステップ 4　このページで適切なオプションを選択し、**Next** をクリックすると、図 2-4 が表示されます。

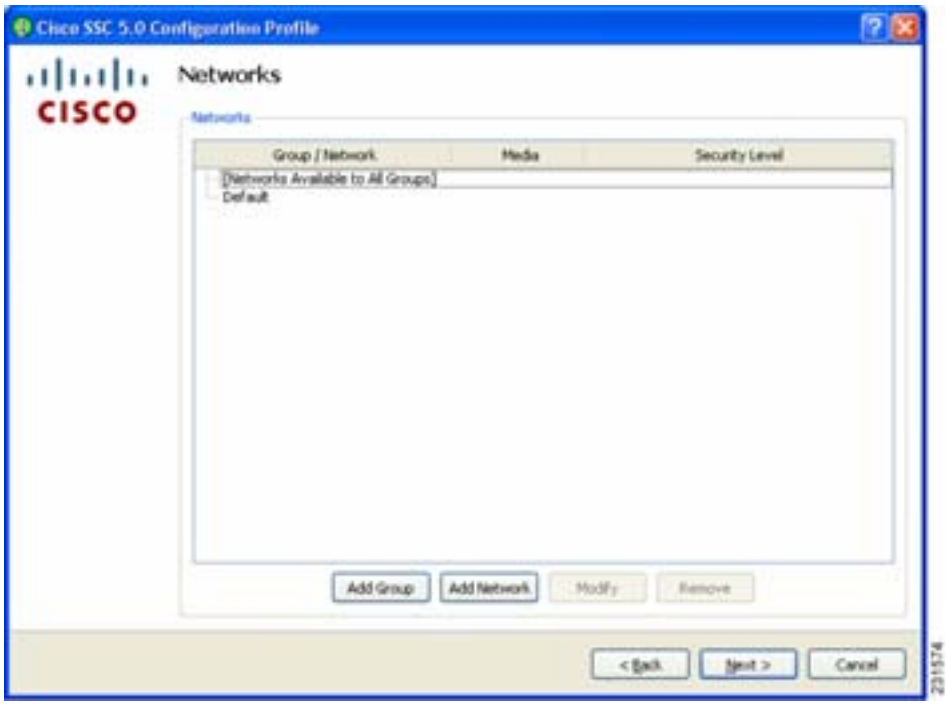
図 2-4　Authentication Policy ページ



この画面では、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グローバルに設定されます。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。

ステップ 5　必要なネットワーク ポリシー オプションを選択し、**Next** をクリックすると、Networks ページ（図 2-5）が表示されます。

図 2-5　Networks ページ



この画面では、企業向けに定義済みのネットワークを構成できます。すべてのグループで利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することができます。グループの詳細については、「配信パッケージ」の項 (P.1-3) を参照してください。

ステップ 6　グループの作成を開始するには、**Add Group** をクリックして、User Group ページ（図 2-6）を表示します。

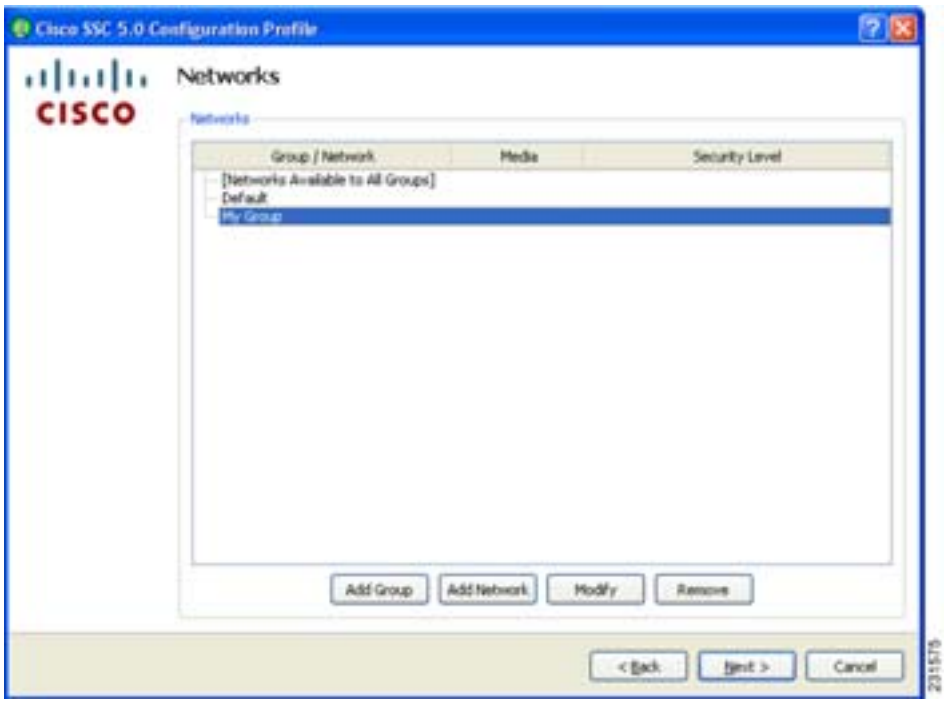
図 2-6　Add Group ページ

Scan list control：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。ユーザがスキャン リストを表示できないようにすることが必要になる場合があります。たとえば、エンドユーザが誤ってネットワークに接続することがないよう、隣接する無線デバイスを排除する必要がある場合などです。

（注） これはグループ別の設定です。エンドユーザが 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 scan list in this group* に設定されます。

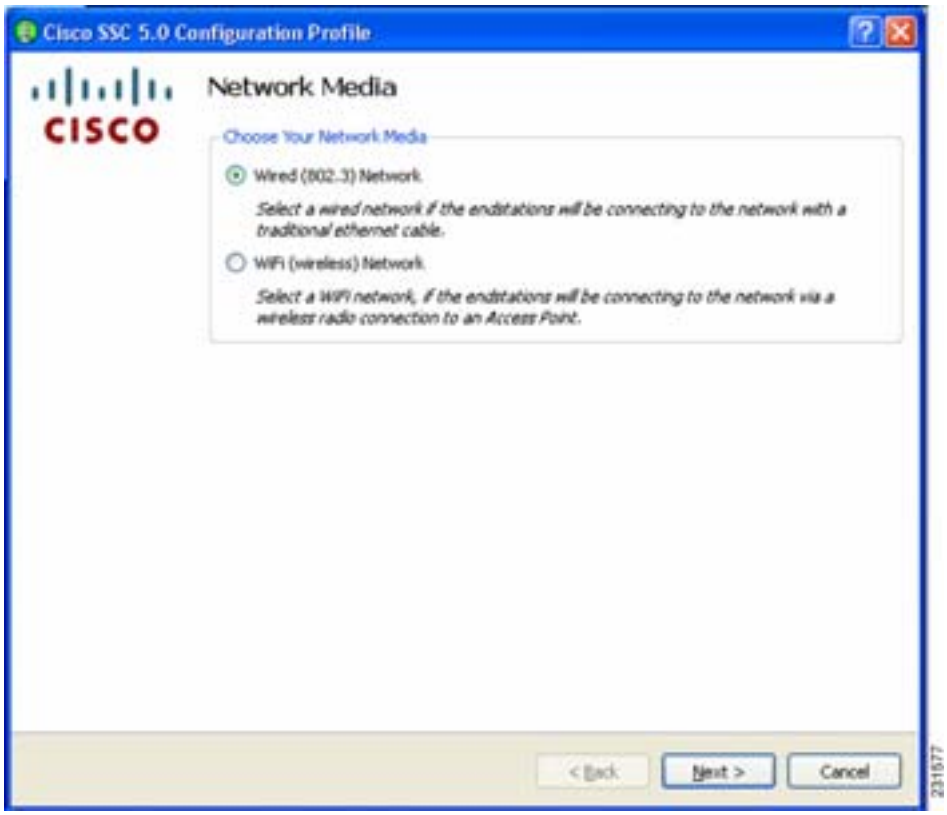
ステップ 7　ユーザグループ名を入力し、必要なスキャン リスト コントロール オプションを選択します。完了したら **OK** をクリックします。Networks ページが再び表示され、作成した新しいグループ（この例では *My Group*）が表示されます。

図 2-7　新しいグループが表示されている Network ページ



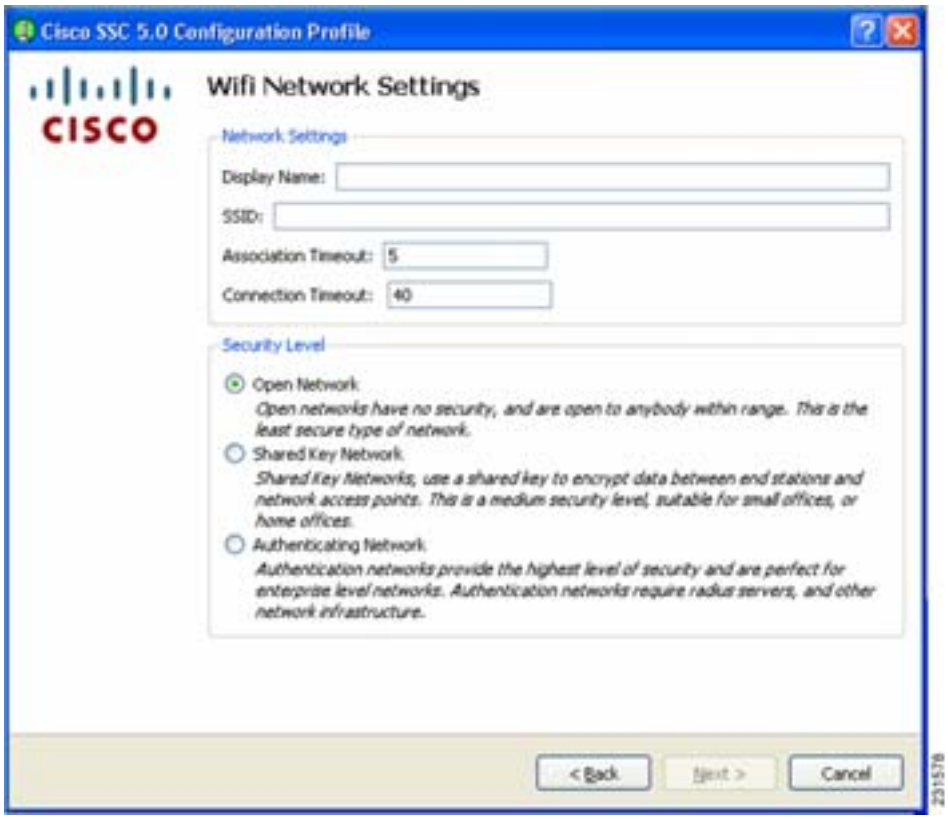
ステップ 8　新しく作成したグループ（この例では、My Group）にネットワークを追加するには、**My Group** をクリックして選択し、**Add Network** をクリックします。Network Media ページ（図 2-8）が表示されます。

図 2-8　Network Media ページ



ステップ 9　このページでは、有線ネットワークまたは無線ネットワークを追加するかどうかを指定できます。この例では、**Wifi (wireless) Network** を選択して無線ネットワークを追加し、**Next** をクリックします。WiFi Network Setting ページ（図 2-9）が表示されます。

図 2-9　WiFi Network Settings ページ



ステップ 10　このページでは、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 認証ネットワークを作成できます。

ステップ 11　Display Name フィールドにネットワーク名を入力します。

ステップ 12　SSID フィールドに、アソシエーション先の SSID を入力します。

ステップ 13　ネットワークの種類を選択します。この例では、**Open Network** をクリックします。

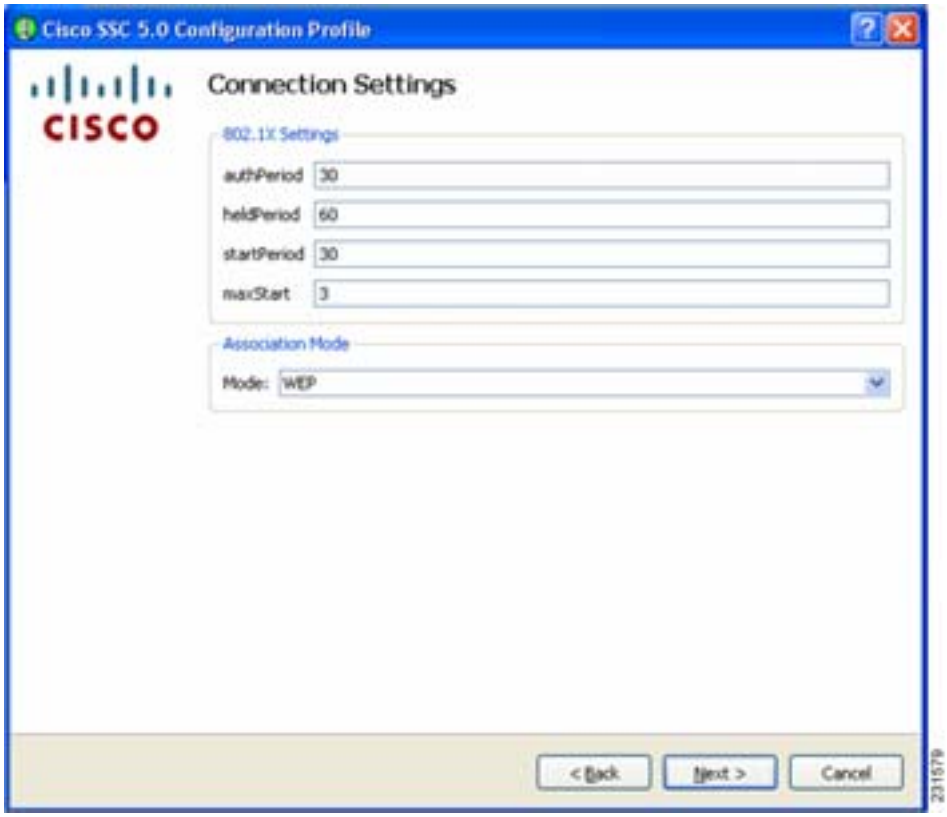
Association Timeout の値は、Cisco SSC クライアントが別のネットワークを試す前に SSID へのアソシエーションを待機する時間です。

Connection Timeout の値は、Cisco SSC クライアントが別のネットワークを試す前にネットワーク接続の確立を待機する時間です。

ネットワーク接続は、Cisco SSC クライアントがそのネットワークの IP アドレスを取得した場合に確立したものとして見なされます。

ステップ 14　**Next** をクリックすると、802.1x の接続設定ページが表示されます。

図 2-10　802.1X Connection Setting ページ



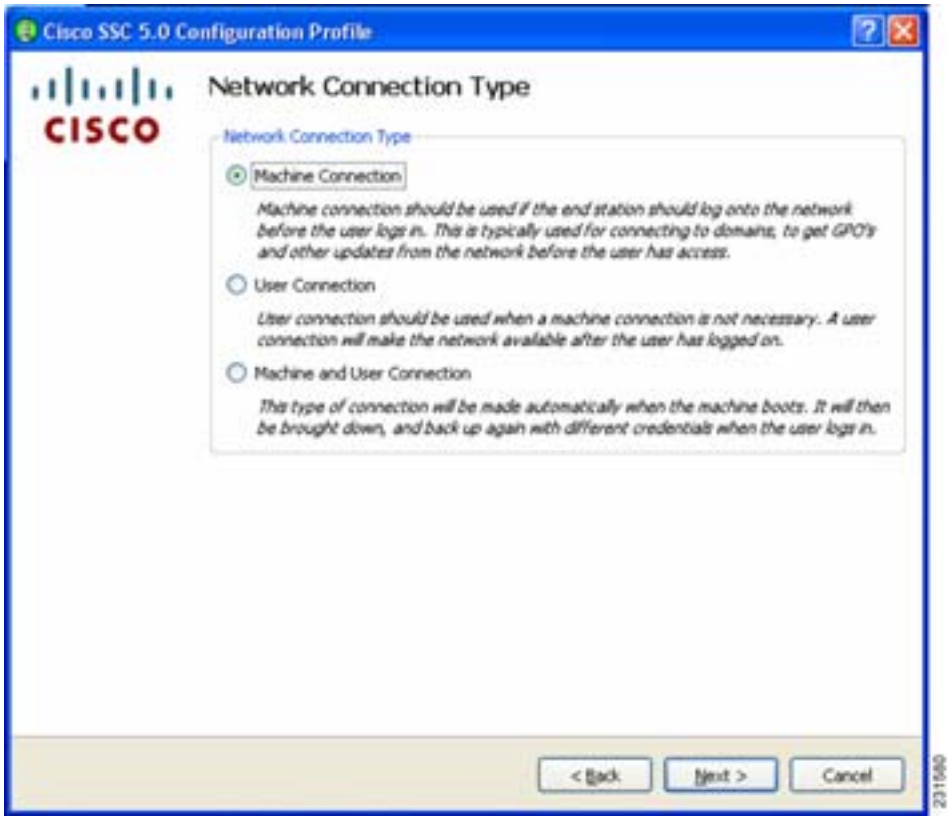
この画面では、802.1x タイマの値を入力します。デフォルトの値は、ほとんどのネットワークに使用できますが、環境に合わせて設定することもできます。

ステップ 15　目的の 802.1x タイマの値を入力します。この例では、デフォルト値を受け入れます。

ステップ 16　このネットワークのアソシエーション モードを、ドロップダウン矢印をクリックして選択します。この例では **WEP** を選択します。

ステップ 17　**Next** をクリックすると、Network Connection Type ページ（図 2-11）が表示されます。

図 2-11　Network Connection Type ページ



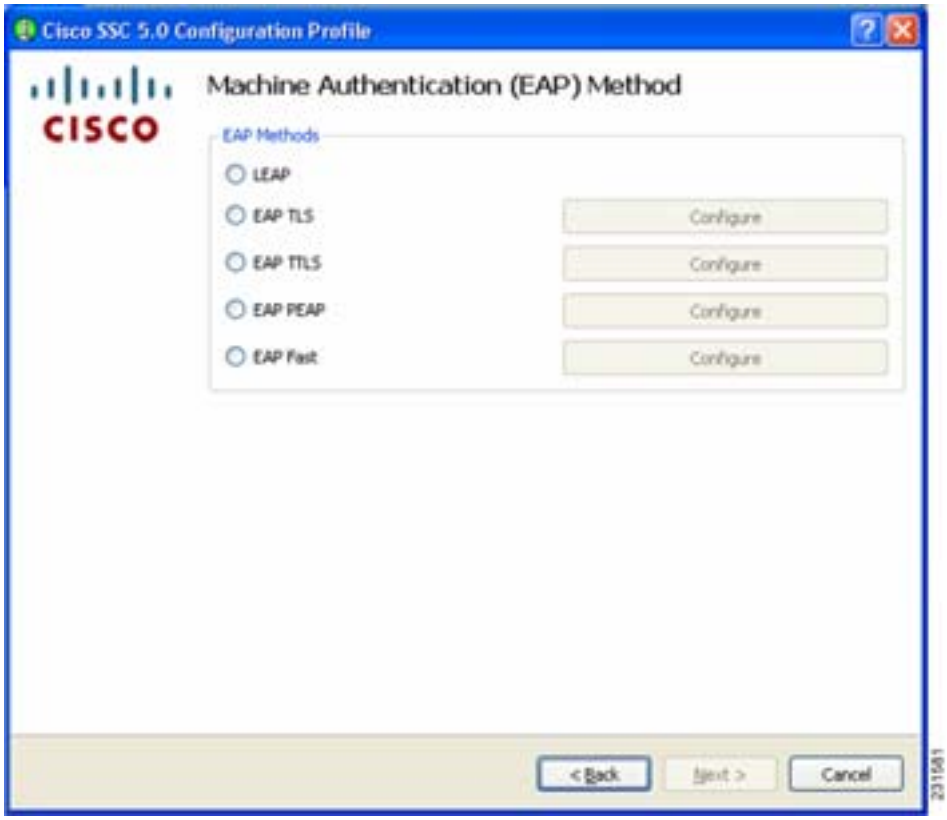
このページでは、ネットワーク接続の種類を指定します。SSC クライアントでは Machine Connection がデフォルトです。User Connections は、ユーザ セッションのときにのみ試されます。

マシンとユーザのネットワーク設定には、マシン部分とユーザ部分が含まれています。SSID は、どちらでも同じですが、マシン接続のクレデンシャルは、ユーザ接続のクレデンシャル タイプと異なります。

ステップ 18　この例では **Machine and User Connection** を選択します。

ステップ 19　**Next** をクリックすると、Machine Authentication Method ページ（図 2-12）が表示されます。

図 2-12　Machine Authentication Method ページ



このページでは、マシンの認証方法を指定します。

ステップ 20　この例では、Peap-MSChapv2 ネットワークを作成するために、**EAP PEAP** を選択します。

ステップ 21　PEAP 設定を構成するには、EAP PEAP の横にある **Configure** をクリックします。EAP Peap Setting ページ（図 2-13）が表示されます。

図 2-13　EAP PEAP Setting ページ

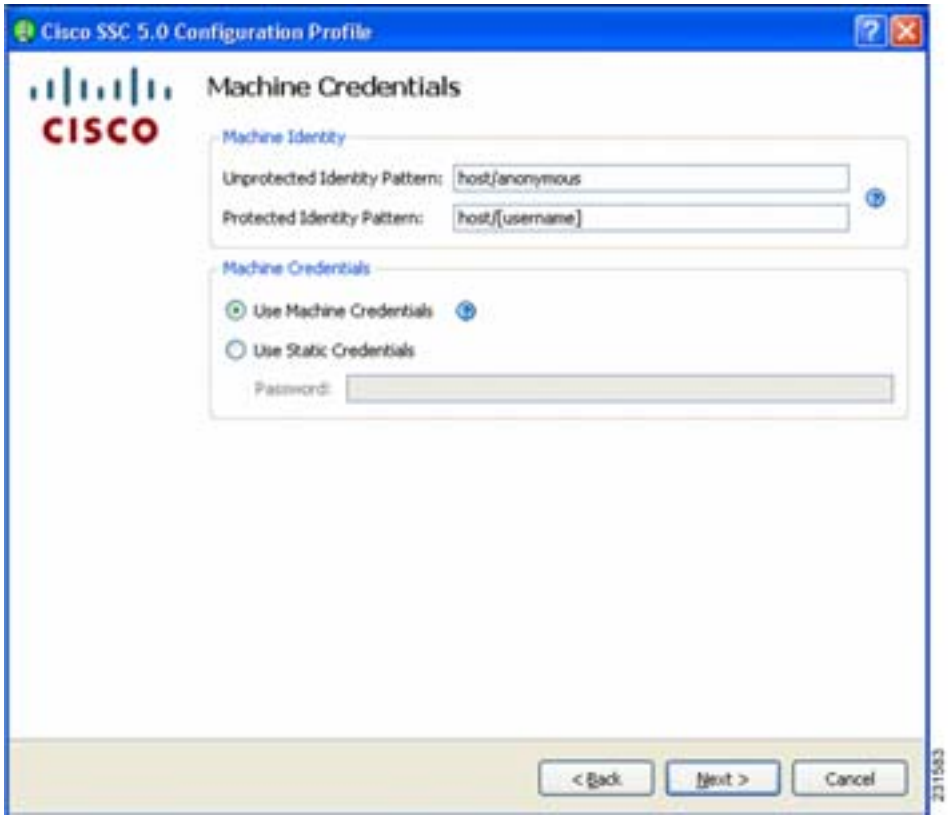
このページでは、次のオプションを指定します。

- 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。
- 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。

ステップ 22　必要なオプションを選択して **OK** をクリックし、Machine Authentication Method （図 2-12）ページに戻ります。

ステップ 23　**Next** をクリックすると、Machine Credentials ページ（図 2-14）ページが表示されます。

図 2-14　Machine Credentials ページ



このページでは、このネットワークの確立に使用するクレデンシャルを指定できます。

Cisco SSC リリース 5.0 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]
- [domain]

[username] や [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。

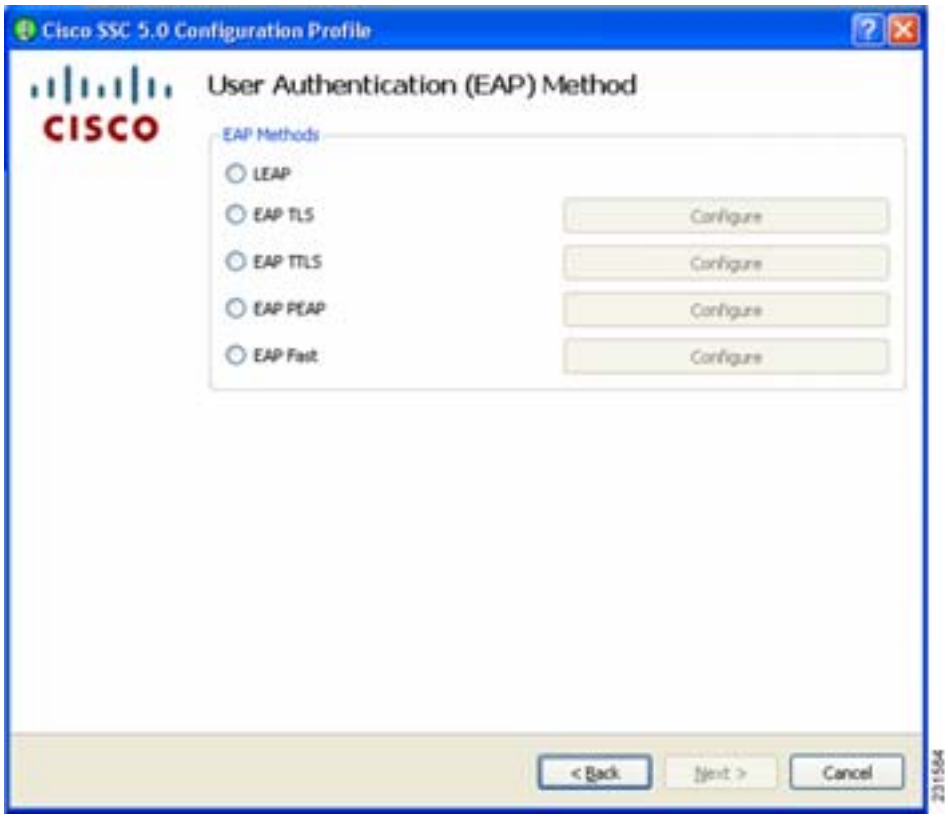
　— このプロファイルに対してパスワード ソースが設定されている場合、パターンは実際の文字列となり、プレースホルダなしのユーザ名として送信されます。

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。

ステップ 24 マシン接続に必要な設定を入力し、**Next** をクリックします。User Authentication Method ページ（図 2-15）が再び表示されます。

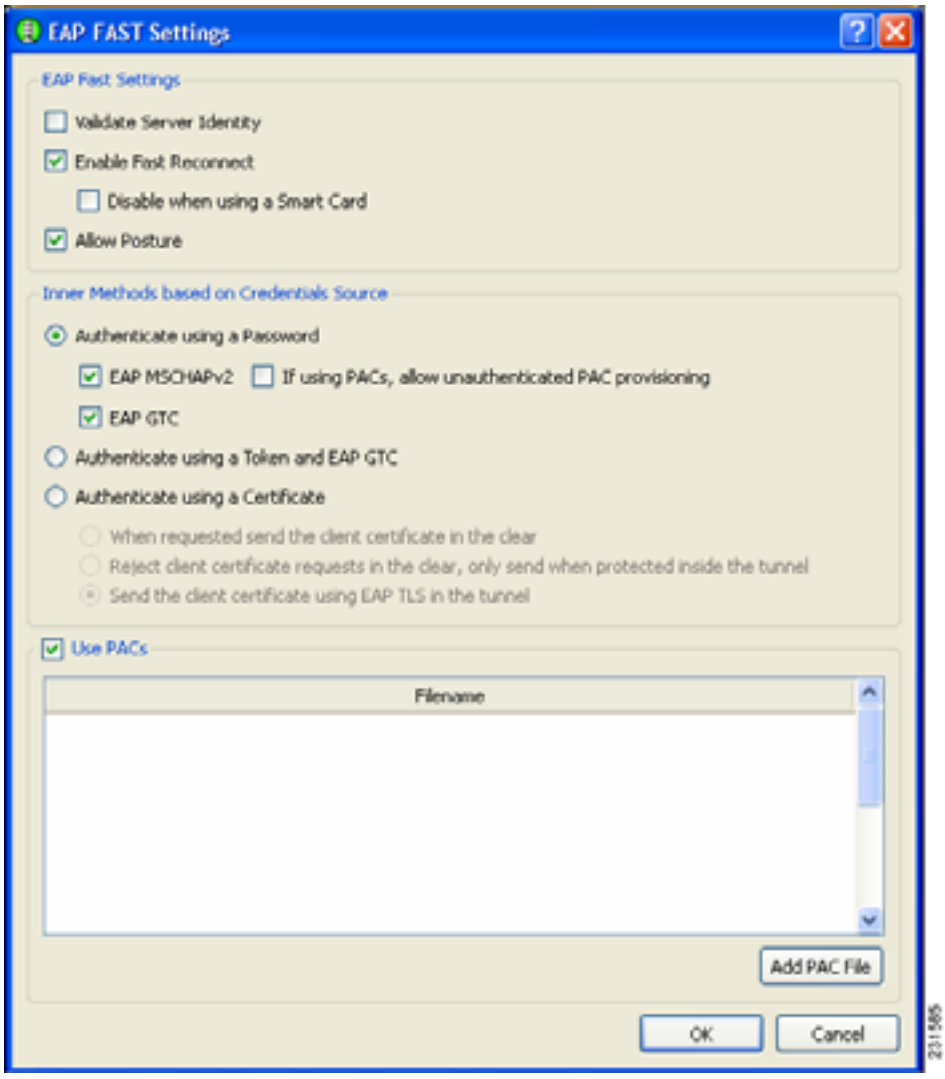
図 2-15　User Authentication Method ページ



ここで、マシン接続のためのクレデンシャルを指定する必要があります。

ステップ 25　このユーザ認証の例では、**EAP Fast** をクリックし、EAP-Fast の横にある **Configure** をクリックします。EAP Fast Settings ページ（図 2-16）が表示されます。

図 2-16　EAP Fast Settings ページ

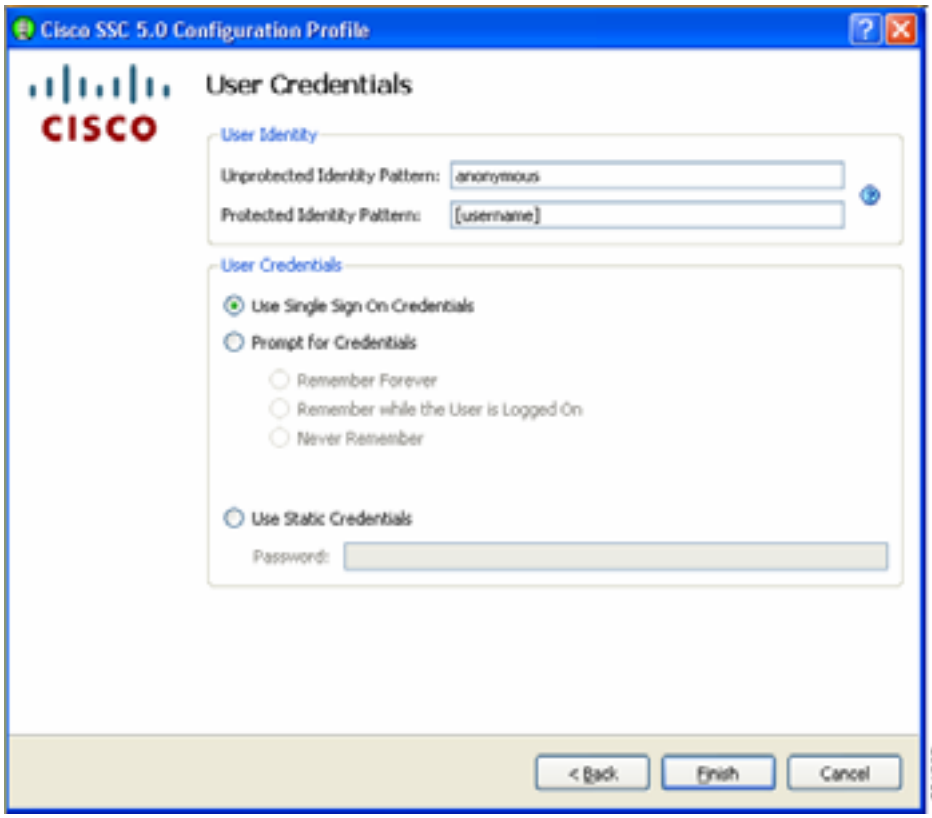


このページには、Add PAC File をクリックして、手動でプロビジョニングされた PAC を含めるオプションがあります。PAC ファイルの内容が配信パッケージに追加され、1 つの展開ファイルが生成されます。

ステップ 26　この例では、図 2-16 に示されている EAP Fast オプションを選択し、**OK** をクリックします。User Authentication Method ページ（図 2-15）が再び表示されます。

ステップ 27　**Next** をクリックして、ユーザ クレデンシャルを設定します。User Credentials ページ（図 2-17）が表示されます。

図 2-17　User Credentials ページ



このページでは、このネットワークの確立に使用するクレデンシャルを指定できます。

Cisco SSC リリース 5.0 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]
- [domain]

[username] や [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。

クレデンシャル 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ユーザ名として送信されます。

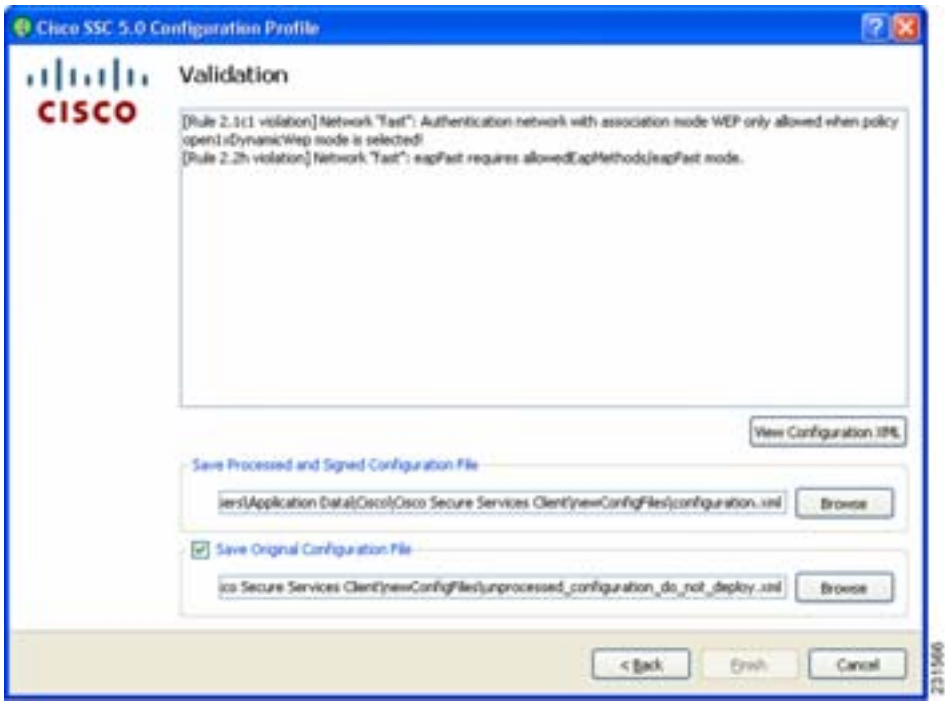
ID パターンを指定した場合は、クレデンシャル ソースを指定できます。クレデンシャルの入力を求める画面を表示するか、シングル サインオン クレデンシャル（SSC クライアントはオペレーティング システムからこれらを取得します）を使用するか、または展開ファイルにある実際のクレデンシャルを送信するように指定できます。

選択が完了したら、Finish をクリックします。これでネットワークの作成は完了です。

これで必要な数だけネットワークを追加できるようになりました。追加し終わったら、*Next* をクリックします。

この時点で、管理ツール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。作成したネットワークでポリシー違反が見つかった場合は、違反が表示されます。エラーが示されている場合は、ファイルを保存する前にそれらを修正する必要があります。たとえば、このような Validation ページ（図 2-18）が表示されます。

図 2-18　Validation ページ



違反が見つからなかった場合は、展開ファイルを保存できます。管理ユーティリティによって、指定した場所に 2 種類の形式の展開ファイルが保存されます。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 Services Client¥newConfigFiles¥configuration.xml

Cisco SSC クライアントは、新しい配信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。

未処理の展開ファイルは、次の場所に保存されます。

C:¥Documents and Settings¥All Users¥Application Data¥Cisco¥Cisco Secure Services Client¥newConfigFiles¥unprocessed_configuration_do_not_deploy.xml

注意　このファイルには、プレーンテキスト形式のクレデンシャルが含まれています。

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、最初のページ（図 2-1）で *Modify Existing Configuration* をクリックして、保存した未処理の展開ファイルを選択します。

CHAPTER 3

トラブルシューティング

この章では、Cisco SSC リリース 5.0 ログ ファイル、ログ メッセージ形式、Log Packager ユーティリティ、SSC クライアントで問題が見つかった場合に行う操作、およびよく寄せられる質問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 SSC リリース 5.0 では、クライアントの問題のトラブルシューティングに役立つクライアント アクション シーケンスが含まれたログ ファイルが生成されます。このログ ファイルは *CurrentLog.txt* という名前で、*Documents And Settings/All Users/Application Data/Cisco/Cisco Secure Services Client/logs* フォルダにあります。同じフォルダに *PreviousLog.txt* という名前のファイルがある場合もありますが、これは以前のログ ファイルです。CurrentLog.txt ファイルのサイズが 2Mb を超えるか、クライアントが再起動されると、既存のログ ファイルの名前は PreviousLog.txt に変更され、新しいログ ファイルが作成されます。

これらのファイルには、さまざまなレベルのログ メッセージが次のような形式で含まれています。

- %CSSC-3-ERROR_MSG：通常の処理の妨げとなる例外を示すために使用されるエラー　ログ メッセージ。
- %CSSC-4-WARNING_MSG：クライアントがセキュリティで保護されていない状態であること、または、予期しない問題が発生したが処理は続行できる状態であることを示すために使用される警告ログ メッセージ。
- %CSSC-6-INFO_MSG：クライアントが通常の処理中の状態にあることを示す情報目的のログ メッセージ。
- %CSSC-7-DEBUG_MSG：サポート チームに役立つデバッグ ログ メッセージ。

特定のエラー、警告、または情報メッセージを識別するには、一般的に使用されるスクリプト記述ツールを使用するか、またはログ ファイルを解析します。SSC リリース 5.0 で提供されるエラー メッセージ、警告メッセージ、および情報メッセージの詳細については、付録 B「Cisco Secure Client Services リリース 5.0 ログ メッセージ」を参照してください。

Log Packager

SSC リリース 5.0 には *Log Packager* という名前のツールが付属しています。このツールは、クライアント情報を含む、すべての関連システム情報を収集し、サポート チームがクライアントの問題を解決できるようにします。レポートの情報には、クライアント ログ、クライアント構成、ライセンス情報、アダプタ情報などが含まれます。

このツールは、Cisco.com の Cisco SSC 製品ソフトウェア ダウンロード ページで、*Cisco_Client_Utilities_2KXP-1_0_0_0.msi* という名前の .msi ファイルとして入手できます。

（注） 製品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。

.msi ファイルを取得するには、次の指示に従います。

ステップ 1　Web ブラウザを使用して次の URL を表示します。

http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=280753707

ステップ 2　**Client Adapters and Client Software** > **Cisco Secure Services Client v5.0** の順にクリックして、Cisco.com にログインするか、登録します。

ステップ 3　**Windows XP** または **Windows 2000** をクリックすると、Select a Release ページが表示されます。

ステップ 4　Latest Releases で **5.0.0** をクリックします。

ステップ 5　**Cisco_Client_Utilities_2KXP-1_0_0_0.msi** をクリックすると、Downloads ページが表示されます。

ステップ 6　**Download** をクリックして、ソフトウェア ライセンス契約に同意します。

ステップ 7　ログオン プロンプトでユーザ名およびパスワードを入力します。

ステップ 8　プロンプトに従ってソフトウェアをお使いのコンピュータにダウンロードします。

このパッケージを企業のエンドシステムにインストールするには、任意の展開方法を使用できます。

Cisco SSC クライアント リリース 5.0 で解決できない問題が発生した場合は、シスコのサポートに問い合わせる前に、次の操作を実行してください。

1. 問題が発生したシステムに Log Packager ツールをインストールします。インストールすると、**Start** > **All Programs** > **Cisco** からツールを利用できるようになります。
2. Log Packager ツールを起動し、Collect Data ボタンをクリックします。
3. Log Packager によるデータの収集が完了すると、デスクトップに *CiscoSupportReport.zip* という名前の新しい ZIP ファイルが生成されます。または、ツールの起動後に *Locate Report file* ボタンをクリックして、直接 ZIP ファイルのある場所に移動することもできます。このファイルは、シスコのサポートへ問い合わせる際に必要となります。

シスコのサポートへの問い合わせ手順については、「技術情報の入手、サポートの依頼、セキュリティ ガイドライン」の項 (P.-vi) を参照してください。

よく寄せられる質問

Q. 802.1x ネットワークはどのように設定するのですか。

A. 推奨：管理ユーティリティをダウンロードし（「配信パッケージ ユーティリティ」の項 (P.1-5)を参照）、ファイルを解凍し、パッケージに含まれている *sscManagementUtility.exe* を実行します。

Q. 接続するボタンをクリックしても、指定したネットワークに接続できません。

A. CSSC は常に指定されたネットワークに接続しようとします。接続が失敗した場合は、リスト内の次のネットワークに進みます。これが、接続が確立されるまで続けられます。特定のネットワークに接続する必要がある場合は、ネットワークを右クリックして、**Connect exclusively** を選択します。

APPENDIX A

Postprocessing 検証エラー

コマンド使用エラー

(注) sscManagementUtility ユーティリティを実行すると、次のいずれかの結果が発生します。

- 成功：確認メッセージが返されます。署名オプションの場合は、処理された内容で出力ファイルが作成されます。
- 失敗：エラー メッセージが返されます。出力ファイルは作成されますが、空白です。

- 入力ファイルのファイル拡張子を .xml にする必要がある場合

  コマンド構文の例

  ```
  sscManagementUtility validate -i distPkg
  ```

  エラー メッセージ

  ```
  Input file "distPkg" should have the ".xml" extension!
  ```

- 入力ファイルのファイル拡張子が不適切な場合

  コマンド構文の例

  ```
  sscManagementUtility validate -i distPkg.txt
  ```

  エラー メッセージ

  ```
  Input file "distPkg.txt" should have the ".xml" extension!
  ```

- コマンド ラインの構文エラー

  コマンド構文の例

  ```
  sscManagementUtility distPkg.xml distPkgSigned.xml
  ```

  エラー メッセージ

  ```
  Usage:
    sscManagementUtility [command] [command specific options]
  Command:
    help - print usage
    validate - validate configuration Xml file
    sign - validate and sign configuration Xml file
  validate options:
    sscManagementUtility validate [-i <input file>]
    -i --in
       path to the original distribution package xml file
  sign options:
    sscManagementUtility sign [-i <input file>] [-o <output file]
    -i --in
  ```

```
   path to the original distribution package xml file
-o --out
   path to the processed and ready to deploy xml file
```

コマンド構文エラーのほとんどには、この例のようにコマンド ヘルプ情報が表示されます。

XML スキーマ確認エラー

（注） ユーティリティに組み込みの XLM スキーマ確認処理で検出されたエラーは、次のタイプのいずれかとして表示されます。

パーサー エラー

スキーマ確認エラー

スキーマ確認エラーの例の一部を次に紹介します。

- 入力ファイル distPkg.xml が空白の場合

  エラー メッセージ

  distPkg.xml:1:parser error :Document is empty

  distPkg.xml:1:parser error :Start tag expected, '<' not found

  failed to parse distPkg.xml

- 基本エレメントのバージョン アトリビュートが欠落している場合

  エラーが含まれる XML 入力テキスト

  <configuration>

  エラー メッセージ

  Loaded version: ..

  Unknown configuration version.

- エレメント終了タグ（<collectionBehavior）が欠落している場合

ヒント 解析エラーの構造は階層的です。常にトップダウンで解決します。実際のエラーでは、ほとんどの場合連鎖的にエラーが生成され、このようなエラーがファイルの後方に表示されます。

この場合は、line 49 のエラー 1 つを修正すると、それ以降に表示され、報告された解析エラーのすべてが解消します。

エラーが含まれる XML 入力テキスト

```
(line 48)   <userAuthentication>
(line 49)     <collectionBehavior
(line 50)       <withPassword>
(line 51)         <cachePasswordFromUser>
(line 52)           <forever/>
(line 53)         </cachePasswordFromUser>
(line 54)       </withPassword>
(line 55)     </collectionBehavior>
```

エラー メッセージ

Entity:line 50:parser error :error parsing attribute name <withPassword>

Entity:line 50:parser error :attributes construct error <withPassword>

Entity:line 50:parser error :Couldn't find end of Start Tag collectionBehavior line 49 <withPassword>

Entity:line 55:parser error :Opening and ending tag mismatch:userAuthentication line 48 and collectionBehavior </collectionBehavior>^

Entity:line 84:parser error :Opening and ending tag mismatch:authenticationNetwork line 47 and userAuthentication </userAuthentication>

Entity:line 96:parser error :Opening and ending tag mismatch:wifiNetwork line 39 and authenticationNetwork </authenticationNetwork>

Entity:line 97:parser error :Opening and ending tag mismatch:globalNetworks line 30 and wifiNetwork </wifiNetwork>

Entity:line 98:parser error :Opening and ending tag mismatch:networks line 29 and globalNetworks </globalNetworks>

Entity:line 102:parser error :Opening and ending tag mismatch:configuration line 2 and networks </networks>

Entity:line 104:parser error :Extra content at the end of the document <connectionSettings>

Document not loaded.

- エレメントのアトリビュートが欠落している場合

  エラーが含まれる XML 入力テキスト

  ```
  <unprotectedIdentityPattern>anonymous</unprotectedIdentityPattern>
  ```

  エラー メッセージ

  element unprotectedIdentityPattern:Schemas validity error :Element 'unprotectedIdentityPattern':The attribute 'encryptContent' is required but missing.

  Schema validation failed (1868)

- Elements out-of-order as required by schema

  エラーが含まれる XML 入力テキスト

  ```
  <wifiNetwork>
    <connectionTimeout>30</connectionTimeout>
    <displayName>My Corporate Wi-Fi Network</displayName>
  ```

  エラー メッセージ

  element connectionTimeout:Schemas validity error :Element 'connectionTimeout':This element is not expected.Expected is (displayName).

  Schema validation failed (1871)

- 必要なエレメントが欠落している場合

  エラーが含まれる XML 入力テキスト

  ```
  <wifiNetwork>
    <connectionTimeout>30</connectionTimeout>
    <doNotAllowEapOverUdp/>
  ```

  エラー メッセージ

  element connectionTimeout:Schemas validity error :Element 'connectionTimeout':This element is not expected.Expected is (displayName).

  Schema validation failed (1871)

- 必要なエレメント値が欠落している場合

  エラーが含まれる XML 入力テキスト

  ```
  <wifiNetwork>
    <displayName></displayName>
    <connectionTimeout>30</connectionTimeout>
  ```

  エラー メッセージ

  element displayName:Schemas validity error :Element 'displayName':[facet 'minLength'] The value has a length of '0'; this underruns the allowed minimum length of '1'.

element displayName:Schemas validity error :Element 'displayName':" is not a valid value of the atomic type 'NonEmptyString'.

Schema validation failed (1824)

- エレメント値のデータ型のエラー

  エラーが含まれる XML 入力テキスト

  ```
  <wifiNetwork>
    ....
    <associationTimeout>0</associationTimeout>
  ```

  エラー メッセージ

  element associationTimeout:Schemas validity error :Element 'associationTimeout ':'0' is not a valid value of the atomic type 'xs:positiveInteger'.

  Schema validation failed (1824)

- 列挙値に余分な空白スペースが含まれる場合

  エラーが含まれる XML 入力テキスト

  ```
  <associationMode>
    <wpa>
    <encryption>TKIP </encryption>
    </wpa>
  </associationMode>
  ```

  エラー メッセージ

  element encryption:Schemas validity error :Element 'encryption':[facet 'enumeration'] The value 'TKIP ' is not an element of the set{'AES', 'TKIP'}.

  element encryption:Schemas validity error :Element 'encryption':'TKIP ' is not a valid value of the atomic type 'WpaEncryption'.

  Schema validation failed (1824)

ファイル参照エラー

配信パッケージ スキーマには、XML インスタンス ファイルへの包含が指定された外部ファイルの参照として機能するエレメントが複数組み込まれます。

ファイル参照エラーの例の一部を次に紹介します。

CA 証明書ファイル

- ファイルへのパスに誤りがある（指定されたファイルが存在しない）場合

  XML 入力テキスト

  ```
  <caReference>E:¥path¥CaCertFile.pem</caReference>
  ```

  エラー メッセージ

  CA certificate file:"E:¥path¥CaCertFile.pem" doesn't exist

- ファイル タイプに誤りがある場合

  XML 入力テキスト

  ```
  <caReference>CaCertFile</caReference>
  ```

  エラー メッセージ

  CA certificate file:"CaCertFile" should be in .pem format

PAC ファイル

- ファイルへのパスに誤りがある（指定されたファイルが存在しない）場合

  XML 入力テキスト

  ```
  <aIdReference>E:¥path¥pacRefFile</aIdReference>
  ```

エラー メッセージ

Pac file "E:¥path¥pacRefFile" processing error:can not open pac file E:¥path¥pacRefFile

- PAC パスワードが入力されないか無効の場合

  XML 入力テキスト：オプション エレメント secretKey が設定されていない場合

```
<reference>
  <aIdReference>pacRefFile</aIdReference>
</reference>
```

  XML 入力テキスト：パスワード値が正しくない場合

```
<reference>
  <aIdReference>pacRefFile</aIdReference>
  <secretKey>1234</secretKey>
</reference>
```

  エラー メッセージ

  Pac file "pacRefFile" processing error:Invalid password to access pac file

ビジネス ルール検証エラー

次に、ビジネス ルール検証エラーのリストを例とともに紹介します。

詳細は、使用されているエレメントの注釈の説明を参照してください。

- ルール 1.1 トンネル認証方式を使用する認証無線ネットワークには、1 つ以上の対応する内部方式の指定が必要です。これは、EAP FAST、EAP PEAP、および EAP TLS に適用されます。

  エラーが含まれる XML 入力テキスト

```
<wifiNetwork>
  <displayName>Test 1.1.1</displayName>
  ....
        <eapFast>
        ....
              <methods></methods>
```

  エラー メッセージ

  [Rule 1.1.1 violation] Network Test 1.1.1 EapFast authentication settings should use at least one of the following methods as inner method:eapMschapv2 or eapGtc.

  エレメント *methods* または *eapMethods* の説明を参照してください。

- ルール 1.2.1 ログオン前のネットワーク接続に対してユーザ接続コンテキストが設定されている場合、クレデンシャルのソースは制限されます。OS から取得したスマートカードを使用したクライアント証明書のみがサポートされます。Windows 証明書ストアのクライアント証明書はサポートされません。ユーザからパスワードを取得することはできません。

  ケース 1：OS のスマートカード証明書（ルール 1.2.1a）。

  エラーが含まれる XML 入力テキスト

```
<displayName>Test 1.2.1a</displayName>
...
  <userAuthentication>
    ...
    <certificateSource>
      <certificateFromUser> {Must be from logon.}
...
<connectionSettings>
  <connectionBehaviorAtLogon>
    <attemptConnectionBeforeUserLogon>
```

  エラー メッセージ

  [Rule 1.2.1a violation] Network Test 1.2.1a Certificate source for user authentication must be certificateFromLogon!

ケース 2：OS またはプロファイルのパスワード（ルール 1.2.1b）。

エラーが含まれる XML 入力テキスト

```
<displayName>Test 1.2.1b</displayName>
...
  <userAuthentication>
    ...
    <passwordSource>
      <passwordFromUser> {Must be from logon or profile.}
...
<connectionSettings>
  <connectionBehaviorAtLogon>
    <attemptConnectionBeforeUserLogon>
```

エラー メッセージ

[Rule 1.2.1b violationPassword source for user authentication must not be passwordFromUser] Network Test 1.2.1b Collection behavior for user authentication must be smartCardOnlyCertificate!

エレメント *attemptConnectionBeforeUserLogon* の説明を参照してください。

- ルール 1.2.2a-c ユーザ クレデンシャルの収集方法は、指定されたクレデンシャルの種類によって異なります。

ケース 1：パスワード ベースのクレデンシャル。

エラーが含まれる XML 入力テキスト

```
<displayName>Test 1.2.2a</displayName>
...
  <authenticationNetwork>
    ...
    <collectionBehavior>
      <withCertificate> {not consistent with source, withPassword required}
    ...
    <authenticationMethod>
    ...
      <passwordSource>
        <passwordFromUser/>
```

エラー メッセージ

[Rule 1.2.2a violation] Network Test 1.2.2a Collection behavior for user authentication with passwordFromUser must be authenticateWithPassword!

ケース 2：証明書ベースのクレデンシャル。

エラーが含まれる XML 入力テキスト

```
<displayName>Test 1.2.2b</displayName>
...
  <authenticationNetwork>
    ...
    <collectionBehavior>
      <withPassword> {not consistent with source, withCertificate required}
    ...
    <authenticationMethod>
    ...
      <certificateSource>
        <certificateFromUser/>
```

エラー メッセージ

[Rule 1.2.2b violation] Network Test 1.2.2b Collection behavior for user authentication with certificateFromUser must be authenticateWithCertificate!

ケース 3：トークン ベースのクレデンシャル。

エラーが含まれる XML 入力テキスト

```
<displayName>Test 1.2.2c</displayName>
...
  <authenticationNetwork>
    ...
    <collectionBehavior>
      <withCertificate> {not consistent with source, withToken required}
    ...
    <authenticationMethod>
    ...
      <tokenSource>
```

エラー メッセージ

[Rule 1.2.2c violation] Network Test 1.2.2c Collection behavior for user authentication with tokens must be authenticateWithToken!

エレメント *collectionBehavior* の説明を参照してください。

- ルール 2.1 Wi-Fi アソシエーションに関するネットワーク ポリシーに、少なくとも 1 つのアソシエーション モードを組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedAssociationModes></allowedAssociationModes> {no child element specified}
  ```

  エラー メッセージ

  [Rule 2.1 violation] At least one association mode must be specified for networkPolicy/allowedAssociationModes!

  エレメント *allowedAssociationModes* の説明を参照してください。

- ルール 2.1a 認証または共有秘密情報がないネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *openNoEncryptionfd* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedAssociationModes>
      <wpaEnterpriseTkip/> {No open networks configured.}
    </allowedAssociationModes>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 2.1a</displayName>
      <openNetwork/> {Not allowed}
    </wiredNetwork>
    <wifiNetwork>
      <displayName>Test 2.1a</displayName>
      ...
      <openNetwork> {Not allowed}
      ...
    </wifiNetwork>
  ```

  エラー メッセージ

  [Rule 2.1a violation] Network "Test 2.1a" :openNetwork only allowed when openNoEncryption mode is selected!

  エレメント *openNetwork* の説明を参照してください。

- ルール 2.1b WEP 静的キー ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *openStaticWep* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

```
<networkPolicy>
  <allowedAssociationModes>
    <wpaEnterpriseTkip/> {No open WEP configured.}
  </allowedAssociationModes>
....
<networks>
  <wifiNetwork>
    <displayName>Test 2.1b</displayName>
    ...
    <sharedKeyNetwork>
      ...
      <wep>
        ...
        <ieee80211Authentication>open</ieee80211Authentication> {Not allowed}
```

  エラー メッセージ

  [Rule 2.1b violation] Networks "Test2.1b":wep with ieee80211Authentication/open only allowed when policy openStaticWep mode is selected!

  エレメント *ieee80211Authentication.* の説明を参照してください。

- ルール 2.1c WEP 静的キー ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *openStaticWep* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

```
<networkPolicy>
  <allowedAssociationModes>
    <wpaEnterpriseTkip/> {No shared WEP configured.}
  </allowedAssociationModes>
....
<networks>
  <wifiNetwork>
    <displayName>Test 2.1b</displayName>
    ...
    <sharedKeyNetwork>
      ...
      <wep>
        ...
        <ieee80211Authentication>shared</ieee80211Authentication> {Not allowed}
```

  エラー メッセージ

  [Rule 2.1c violation] Networks "Test2.1c":wep with ieee80211Authentication/shared only allowed when policy sharedStaticWep mode is selected!

  エレメント *ieee80211Authentication.* の説明を参照してください。

- ルール 2.1c1 任意の動的 WEP 認証ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *open1xDynamicWep* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedAssociationModes>
      <wpaEnterpriseTkip/> {No WEP configured.}
    </allowedAssociationModes>
  ....
  <networks>
    <wifiNetwork>
      <displayName>Test 2.1c1</displayName>
      ...
      <authenticationNetwork>
        ...
        <associationMode>
          <wep> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.1c1 violation] Network "Test 2.1c1":Authentication network with association mode WEP only allowed when policy open1xDynamicWep mode is selected!

  エレメント *associationMode* の説明を参照してください。

- ルール 2.1d TKIP 暗号化を使用する WPA-Personal 共有キー ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *wpaPersonalTkip* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedAssociationModes>
      <wpaEnterpriseTkip/> {No wpaPersonalTkip configured.}
    </allowedAssociationModes>
  ....
  <networks>
    <wifiNetwork>
      <displayName>Test 2.1d</displayName>
      ...
      <sharedKeyNetwork>
        ...
        <wpa>
          ...
          <encryption>TKIP</encryption> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.1d violation] Network "Test 2.1d":wpa with encryption/TKIP only allowed when policy wpaPersonalTkip mode is selected!

  エレメント *encryption* の説明を参照してください。

- ルール 2.1e AES 暗号化を使用する WPA-Personal 共有キー ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *wpaPersonalAes* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

```
<networkPolicy>
  <allowedAssociationModes>
    <wpaEnterpriseTkip/> {No wpaPersonalAes configured.}
  </allowedAssociationModes>
....
<networks>
  <wifiNetwork>
    <displayName>Test 2.1e</displayName>
    ...
    <sharedKeyNetwork>
      ...
      <wpa>
        ...
        <encryption>AES</encryption> {Not allowed}
```

  エラー メッセージ

  [Rule 2.1e violation] Network "Test 2.1e":wpa with encryption/AES only allowed when policy wpaPersonalAes mode is selected!

  エレメント *wpa/encryption* の説明を参照してください。

- ルール 2.1 f　TKIP 暗号化を使用する WPA2-Personal 共有キー ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *wpa2PersonalTkip* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

```
<networkPolicy>
  <allowedAssociationModes>
    <wpaEnterpriseTkip/> {No wpa2PersonalTkip configured.}
  </allowedAssociationModes>
....
<networks>
  <wifiNetwork>
    <displayName>Test 2.1f</displayName>
    ...
    <sharedKeyNetwork>
      ...
      <wpa2>
        ...
        <encryption>TKIP</encryption> {Not allowed}
```

  エラー メッセージ

  [Rule 2.1f violation] Networks "Test 2.1f":wpa2 with encryption/TKIP only allowed when policy wpa2PersonalTkip mode is selected!

  エレメント *wpa2/encryption* の説明を参照してください。

- ルール 2.1g AES 暗号化を使用する WPA2-Personal 共有キー ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *wpa2PersonalAes* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

```
<networkPolicy>
  <allowedAssociationModes>
    <wpaEnterpriseTkip/> {No wpa2PersonalAes configured.}
  </allowedAssociationModes>
....
<networks>
  <wifiNetwork>
    <displayName>Test 2.1g</displayName>
    ...
    <sharedKeyNetwork>
      ...
      <wpa2>
        ...
        <encryption>AES</encryption> {Not allowed}
```

  エラー メッセージ

  [Rule 2.1g violation] Networks "Test 2.1g":wpa2 with encryption/AES only allowed when policy wpa2PersonalAes mode is selected!

  エレメント *wpa2/encryption* の説明を参照してください。

- ルール 2.1h TKIP 暗号化を使用する WPA-Enterprise ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *wpaEnterpriseTkip* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

```
<networkPolicy>
  <allowedAssociationModes>
    <wpaEnterpriseAes/> {No wpaEnterpriseTkip configured.}
  </allowedAssociationModes>
....
<networks>
  <wifiNetwork>
    <displayName>Test 2.1h</displayName>
    ...
    <authenticationNetwork>
      ...
      <associationMode>
        <wpa>
          <encryption>TKIP</encryption> {Not allowed}
```

  エラー メッセージ

  [Rule 2.1h violation] Network "Test 2.1h":wpa with encryption/TKIP only allowed when policy wpaEnterpriseTkip mode is selected!

  エレメント *associationMode* の説明を参照してください。

- ルール 2.1i AES 暗号化を使用する WPA-Enterprise ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *wpaEnterpriseAes* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedAssociationModes>
      <wpaEnterpriseTkip/> {No wpaEnterpriseAes configured.}
    </allowedAssociationModes>
  ....
  <networks>
    <wifiNetwork>
      <displayName>Test 2.1i</displayName>
      ...
      <authenticationNetwork>
        ...
        <associationMode>
          <wpa>
            <encryption>AES</encryption> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.1i violation] Network "Test 2.1i":wpa with encryption/AES only allowed when policy wpaEnterpriseAes mode is selected!

  エレメント *associationMode* の説明を参照してください。

- ルール 2.1j TKIP 暗号化を使用する WPA2-Enterprise ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *wpa2EnterpriseTkip* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedAssociationModes>
      <wpaEnterpriseAes/> {No wpa2EnterpriseTkip configured.}
    </allowedAssociationModes>
  ....
  <networks>
    <wifiNetwork>
      <displayName>Test 2.1j</displayName>
      ...
      <authenticationNetwork>
        ...
        <associationMode>
          <wpa2>
            <encryption>TKIP</encryption> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.1j violation] Network "Test2.1j":wpa2 with encryption/TKIP only allowed when policy wpa2EnterpriseTkip mode is selected!

  エレメント *associationMode* の説明を参照してください。

- ルール 2.1k AES 暗号化を使用する WPA2-Enterprise ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *wpa2EnterpriseAes* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

```
<networkPolicy>
  <allowedAssociationModes>
    <wpaEnterpriseTkip/> {No wpa2EnterpriseAes configured.}
  </allowedAssociationModes>
....
<networks>
  <wifiNetwork>
    <displayName>Test 2.1k</displayName>
    ...
    <authenticationNetwork>
      ...
      <associationMode>
        <wpa2>
          <encryption>AES</encryption> {Not allowed}
```

  エラー メッセージ

  [Rule 2.1k violation] Network "Test2.1k":wpa2 with encryption/AES only allowed when policy wpa2EnterpriseAes mode is selected!

  エレメント *associationMode* の説明を参照してください。

- ルール 2.1l CCKM キー管理および TKIP 暗号化を使用する WPA/WPA2-Enterprise ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *cckmEnterpriseTkip* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

```
<networkPolicy>
  <allowedAssociationModes>
    <wpaEnterpriseTkip/> {No cckmEnterpriseTkip configured.}
  </allowedAssociationModes>
....
<networks>
  <wifiNetwork>
    <displayName>Test 2.1l</displayName>
    ...
    <authenticationNetwork>
      ...
      <associationMode>
        <cckm>
          <encryption>TKIP</encryption> {Not allowed}
```

  エラー メッセージ

  [Rule 2.1l violation] Network "Test2.1l":cckm with encryption/TKIP only allowed when policy cckmEnterpriseTkip mode is selected!

  エレメント *associationMode* の説明を参照してください。

- ルール 2.1m CCKM キー管理および AES 暗号化を使用する WPA/WPA2-Enterprise ネットワークをサポートするには、アソシエーション モードに関するネットワーク ポリシーに *cckmEnterpriseAes* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedAssociationModes>
      <wpaEnterpriseAes/> {No cckmEnterpriseAes configured.}
    </allowedAssociationModes>
  ....
  <networks>
    <wifiNetwork>
      <displayName>Test 2.1m</displayName>
      ...
      <authenticationNetwork>
        ...
        <associationMode>
          <cckm>
            <encryption>AES</encryption> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.1m violation] Network "Test2.1m":wpa2 with encryption/AES only allowed when policy wpa2EnterpriseAes mode is selected!

  エレメント *associationMode* の説明を参照してください。

- ルール 2.2 EAP に関するネットワーク ポリシーに、少なくとも 1 つのメソッドを組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedEapMethods></allowedEapMethods> {no child element specified}
  ```

  エラー メッセージ

  [Rule 2.2 violation] At least one eapMethod must be specified for networkPolicy/allowedEapMethods!

  エレメント *allowedEapMethods* の説明を参照してください。

- ルール 2.2a EAP-MD5 の設定がある認証有線ネットワークをサポートするには、EAP 方式に関するネットワーク ポリシーに *eapMd5* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-MD5 configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 2.2a</displayName>
      ...
      <authenticationNetwork>
        ...
        <authenticationMethod>
          <eapMd5> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.2a violation] Network "Test 2.2a" :eapMethod/eapMd5 requires allowedEapMethods/eapMd5.

  エレメント *authenticationMethod* 、*machineAuthentication*、または *machine* の説明を参照してください。

- ルール 2.2b EAP-MSCHAPv2 の設定がある認証有線ネットワークをサポートするには、EAP 方式に関するネットワーク ポリシーに *eapMschapv2* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-MSCHAPv2 configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 2.2b</displayName>
      ...
      <authenticationNetwork>
        ...
        <authenticationMethod>
          <eapMschapv2> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.2b violation] Network "Test 2.2b" :eapMschapv2 requires allowedEapMethods/eapMschapv2 mode.

  エレメント *authenticationMethod* 、*machineAuthentication*、または *machine* の説明を参照してください。

- ルール 2.2c EAP-GTC の設定がある認証有線ネットワークをサポートするには、EAP 方式に関するネットワーク ポリシーに *eapGtc* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-GTC configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 2.2c</displayName>
      ...
      <authenticationNetwork>
        ...
        <authenticationMethod>
          <eapGtc> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.2c violation] Network "Test 2.2c" :eapMethod/eapGtc requires allowedEapMethods/eapGtc mode.

  エレメント *authenticationMethod* 、*machineAuthentication*、または *machine* の説明を参照してください。

- ルール 2.2d EAP-LEAP の設定がある認証有線または無線ネットワークをサポートするには、EAP 方式に関するネットワーク ポリシーに *leap* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-LEAP configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 2.2d</displayName>
      ...
      <authenticationNetwork>
        ...
        <authenticationMethod>
          <leap> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.2d violation] Network "Test 2.2d" :eapMethod/leap requires allowedEapMethods/leap mode.

  エレメント *authenticationMethod* 、*machineAuthentication*、または *machine* の説明を参照してください。

- ルール 2.2e 外部トンネルで EAP-TLS の設定がある認証有線または無線ネットワークをサポートするには、EAP 方式に関するネットワーク ポリシーに *eapTls* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-TLS configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 2.2e</displayName>
      ...
      <authenticationNetwork>
        ...
        <authenticationMethod>
          <eapTls> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.2e violation] Network "Test 2.2e" :eapMethod/eapTls requires allowedEapMethods/eapTls mode.

  エレメント *authenticationMethod* 、*machineAuthentication*、または *machine* の説明を参照してください。

- ルール　2.2f　EAP-TTLS　の設定がある認証有線または無線ネットワークをサポートするには、EAP 方式に関するネットワーク ポリシーに *eapTtls* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-TTLS configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 2.2f</displayName>
      ...
      <authenticationNetwork>
        ...
        <authenticationMethod>
          <eapTtls> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.2f violation] Network "Test 2.2f" :eapMethod/eapTtls requires allowedEapMethods/eapTtls mode.

  エレメント *authenticationMethod* 、*machineAuthentication*、または *machine* の説明を参照してください。

- ルール　2.2g　EAP-PEAP　の設定がある認証有線または無線ネットワークをサポートするには、EAP 方式に関するネットワーク ポリシーに *eapPeap* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-PEAP configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 2.2g</displayName>
      ...
      <authenticationNetwork>
        ...
        <authenticationMethod>
          <eapPeap> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.2g violation] Network "Test 2.2g" :eapMethod/eapPeap requires allowedEapMethods/eapPeap mode.

  エレメント *authenticationMethod* 、*machineAuthentication*、または *machine* の説明を参照してください。

- ルール 2.2h EAP-FAST の設定がある認証有線または無線ネットワークをサポートするには、EAP 方式に関するネットワーク ポリシーに *eapFast* を組み込む必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapPeap/> {No EAP-FAST configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 2.2h</displayName>
      ...
      <authenticationNetwork>
        ...
        <authenticationMethod>
          <eapFast> {Not allowed}
  ```

  エラー メッセージ

  [Rule 2.2h violation] Network "Test 2.2h" :eapMethod/eapFast requires allowedEapMethods/eapFast mode.

  エレメント *authenticationMethod* 、*machineAuthentication*、または *machine* の説明を参照してください。

- ルール 3a SSC では 1 つ以上のメディア タイプを設定する必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <userControlPolicy>
    ...
    <allowedMedia></allowedMedia> {Missing a child element.}
  ```

  エラー メッセージ

  [Rule 3a violation] At least one media type must be specified for userControlPolicy/allowedMedia!

  エレメント *allowedMedia* の説明を参照してください。

- ルール 3b 有線ネットワークの設定をサポートするには、一般ポリシーで有線メディアを使用できるように設定する必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networks>
    <wiredNetwork> {Not allowed.}
      <displayName>Test 3b</displayName>
  ...
  <userControlPolicy>
    ...
    <allowedMedia>
      <wifi/> {Wired not configured.}
    </allowedMedia>
  ```

  エラー メッセージ

  [Rule 3b violation] Network "Test 3b":wiredNetwork may not be present unless userControlPolicy/allowedMedia/wired is present.

  エレメント *wiredNetwork* の説明を参照してください。

- ルール 3c Wi-Fi ネットワークの設定をサポートするには、一般ポリシーで無線メディアを使用できるように設定する必要があります。

  エラーが含まれる XML 入力テキスト

  ```
  <networks>
    <wifiNetwork> {Not allowed.}
      <displayName>Test 3c</displayName>
  ...
  <userControlPolicy>
    ...
    <allowedMedia>
      <wired/> {Wireless not configured.}
    </allowedMedia>
  ```

  エラー メッセージ

  [Rule 3c violation] Network "Test 3c":wifiNetwork may not be present unless userControlPolicy/allowedMedia/wifi is present.

  エレメント *wifiNetwork* の説明を参照してください。

スクリプト エラー

処理の各フェーズの障害を識別できるように戻りコードが実装されています。すべてのアプリケーション戻りコードを次に紹介します。

- 0　成功
- 1　正しくない引数
- 2　不明な設定ファイル バージョン
- 3　スキーマ検証に失敗
- 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）

APPENDIX **B**

Cisco Secure Client Services リリース 5.0 ログ メッセージ

この付録では、Cisco Secure Cilent Services リリース 5.0 で生成されるログ メッセージの一覧を示します。

- **Starting Cisco_SSCservice.exe:** *version number*：SSC サービスが開始していることを示します。
- **Cisco Trust Agent successfully loaded**
- **Failed to load Cisco Trust Agent**
- **Password sent**
- **Certificate sent**
- **Manual user** *logon type* **logon processing initiated by user** *user id*.
- **Normal Shutdown** *version number*：通常のシャットダウンを示します。
- **Fatal Shutdown** *version number*：致命的なシャットダウンを示します。
- **Machine startup**：クライアントがブート時の処理を開始していることを示します。
- **Account logon**：クライアントがユーザ ログオンを検出したことを示します。
- **SSO credentials (Microsoft)**：クライアントが Microsoft GINA（ネットワーク認証で使用されるかどうかに関係なく）からクレデンシャルを収集するときを示します。
- **Account logoff**：クライアントがユーザ ログオフを検出したことを示します。
- **Adapter detected** *Adapter Id* ：システムで新しいアダプタが検出されたことを示します。*Adapter Id* はアダプタの Globally Unique Identifier（GUID; グローバル一意識別子）を表しています。
- **Adapter removed** *Adapter Id*：前に報告されたアダプタが失われた（または取り外された）ことを示します。
- **Adapter controlled** *Adapter Id*：特定のアダプタの制御が開始されることを示します（SSC 中間ドライバがネットワーク フレームへの応答を開始し、アダプタの機能を設定し始めています）。
- *Adapter Id* **Adapter control failed** *error code*：SSC クライアントがアダプタの制御を試みたものの、失敗したことを示します。*error code* は内部エラー コードです。
- **{WPA | WPA2} unsupported.** *Adapter Id*：アダプタが制御されるときおよびアダプタが WPA または WPA2 をサポートしているかどうかを示します。
- **Wireless Zero Config deactivated** *Adapter Id*：Wireless Zero Config が検出されたアダプタの制御が開始され、そのアダプタが自動的に無効にされたことを示します。
- **Adapter control released** *Adapter Id*:特定のアダプタに対する制御が解放されたことを示します。

- **Connection Association Started** (*WiFi Association /Encryption Mode*) : WiFi アダプタで接続を要求する場合、アソシエーションを行う必要があります。このログ メッセージは、SSC クライアントが SSID へのアソシエーションを試行していることを示します。*WiFi Association/Encryption mode* の値は次のいずれかです。
  - Open
  - Shared 40 bit key
  - Shared 128 bit key
  - Static WEP 40 bit key
  - Static WEP 128 bit key
  - Dynamic WEP 40 bit key
  - Dynamic WEP 128 bit key
  - WPA-Personal TKIP encryption
  - WPA-Personal AES encryption
  - WPA-Enterprise TKIP encryption
  - WPA-Enterprise AES encryption
  - WPA2-Personal TKIP encryption
  - WPA2-Personal AES encryption
  - WPA2-Enterprise TKIP encryption
  - WPA2-Enterprise AES encryption
- **Starting wired connection, skipping association**
- *Adapter Id* **Connection Association Success (link up)**：アソシエーションが正常に
- 完了したことを示します。
- **Connection Association Failed.(Failure:***error number*)：アソシエーションが正常に完了しなかったことを示します。*error number* は内部エラー コードです。
- *Adapter Id* **Connection Authentication Started**：認証の試みが開始されたことを示します。
- *Adapter Id* **Identity requested**：AP から ID 要求がきたことを示します。
- *Adapter Id* **Identity sent**：ID が送信されたかどうかを示します。
- *Adapter Id* **EAP suggested by server:***Authentication Method name*：サーバによって EAP 認証方式が推奨されたことを示します。*Authentication Method name* の値は次のいずれかです。
  - EAP-PEAP
  - EAP-TTLS
  - EAP-TLS
  - EAP-LEAP
  - EAP-MD5
  - EAP-GTC
  - EAP-FAST
  - EAP-MSCHAPv2
  - MSCHAPv2
  - MSCHAP
  - CHAP
  - PAP

- *Adapter Id* **EAP requested by client:(***Authentication Method name, , Authentication Method name*)：クライアントによって EAP 認証方式が要求されたことを示します。*Authentication Method name* の値は次のいずれかです。
  - EAP-PEAP
  - EAP-TTLS
  - EAP-TLS
  - EAP-LEAP
  - EAP-MD5
  - EAP-GTC
  - EAP-FAST
  - EAP-MSCHAPv2
  - MSCHAPv2
  - MSCHAP
  - CHAP
  - PAP
- *Adapter Id* **Port State** *Port State* and **Status** *Port status*：アダプタのポートの状態およびステータスを示します。

  Port State の値は次のいずれかです。
  - AC_PORT_STATE_STOPPED：ポートが停止されていることを示します。
  - AC_PORT_STATE_CONNECTING：認証の開始を待機していることを示します。
  - AC_PORT_STATE_AUTHENTICATING：最初の 802.1x 認証をアクティブに実行していることを示します。
  - AC_PORT_STATE_AUTHENTICATED：認証が正常に完了したことを示します。
  - AC_PORT_STATE_REAUTHENTICATING：802.1x 再認証をアクティブに実行していることを示します。
  - AC_PORT_STATE_UNAUTHENTICATED：ポートが認証を求めているが、リンクがダウンしているか、クレデンシャルが正しくないなど、その他の状態が原因で認証できないことを示します。
  - AC_PORT_STATE_AUTH_NOT_REQUIRED：802.1x 認証が必要ないことを示します。この状態になるのは、有線アダプタまたは WEP モードの無線アダプタの場合のみです。

  Port status は、Port State の値によって異なります。これはポートの状態のサブ状態を示します。
- *Adapter Id* **FAST:unauthenticated provisioning supported**：FAST の認証なしのプロビジョニングがアダプタでサポートされていることを示します。
- *Adapter Id* **FAST:phase 1 tunnel for unauthenticated provisioning**
- *Adapter Id* **Allowing session resumption**：SSC クライアントが TLS ベース認証（PEAP、TTLS、FAST、または TLS）を開始し、前のセッション ID でのセッション再開を試みていることを示します。
- *Adapter Id* **Authentication Success**：認証が正常に完了したことを示します。
- *Adapter Id* **Authentication Failed**：認証が正常に完了しなかったことを示します。
- *Adapter Id* **IP Address Received:***IP Address*：接続が IP アドレスを受け取ったことを示します。
- *Adapter Id* **DHCP:Sending DHCP request.**
- *Adapter Id* **DHCP:Request failed**.
- *Adapter Id* **Wireless Zero Config reactivated for adapter**
- *Access Id* **WiFi access device has invalid channel number:***SSID, channel*
- *Adapter Id* **Couldn't find pre-shared key in profile**
- *Adapter Id***:EAP-TTLS method requested by client:***method name*
- **Starting wifi connection, trying ssid** *ssid name*

- **Licensing:No license found**.
- **Licensing:License read:***License string.*
- *License string***:(do not translate) is the license string read from the license file**.
- **Licensing:License invalid (trial period expired** *License string, trial period*).
- **Licensing:License invalid (termination date reached:***License string, termination date*). *termination date* is the date in format yyyy-mm-dd that the license expired.
- **Licensing:License invalid because product id does not match:***License string, licensed product id*
- **Licensing:License invalid (OEM id does not match:***License string, licensed OEM id*)
- **Licensing:License invalid (maintenance date reached:***License string, maintenance date*).*maintenance date* の値は、ライセンスのメンテナンスの期限を yyyy-mm-dd 形式で表した日付です。
- **Licensing:License invalid (unknown problem:***License string*)
- **Licensing:License is valid and accepted:***License string.*
- **Licensing:Ignoring trial license.Tampering detected:***License string* : ライセンスの履歴ファイルの復号化に失敗すると、すべての新しいトライアル ライセンスに対してこのメッセージが出力されます。
- **Licensing:License invalid, can not decode license:***License string*
- **The configuration is invalid and will be ignored.Error:***error string*
- **Trusted Server list empty, server can not be validated**
- **Validating the server:** *Authentication Server Id*
- **Server certificate validated:** *Authentication Server Id*
- *Authentication Session Id* **Server certificate invalid (unknown CA)**
- **Server certificate invalid (name mismatch:** *CN/DC/Alt name from server cert*)
- **Invalid key type in distribution package**
- *Outer method***:invalid/unsupported inner authentication method:***inner method*
- **Invalid outer EAP method:***method name*
- *Outer method***:No inner authentication methods configured**
- **Disallowed element in configuration:wireless adapters unlicensed**
- **Disallowed element in configuration:wired adapters unlicensed**
- **Disallowed element in configuration:EAP method:***method name*
- **Disallowed element in configuration:Association mode:***association mode*
- **Symbolic name:** *GUID of adapter***, MacAddr:(***MAC addrress of adapter***), Mtu:(***MTU size***), Media:(***percentage***), Encryption:(***encryption modes***), Auth:(***auth modes***)**
- **Server certificate chain invalid**
- **Server certificate chain is not trusted**
- **Invalid wep key length:** *key length***, should be %d or %d**
- **The wildcard (***pattern string***) in the pattern is unknown and will be removed**
- **Internal error** *error number***, contact software manufacturer** : シスコのサポートまで問い合わせる必要があることを示します。