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。