



Cisco SSC の使用方法

この章では、SSC の概要、およびユーザが使用可能な、SSC GUI の主要機能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 \(P. 4-1\)](#)
- [メイン SSC GUI ウィンドウの使用方法 \(P. 4-2\)](#)
- [SSC トレイ アイコンの使用方法 \(P. 4-17\)](#)

概要

SSC は 2 つの論理インターフェイスから実行されます。

- **SSC トレイ アイコン** : SSC の主な機能や情報に迅速にアクセスできるように設計された、最小限のユーザインターフェイスです。
- **メイン SSC GUI ウィンドウ** : すべての SSC 機能を提供する、主要なユーザインターフェイスです。

SSC トレイ アイコンインターフェイスは、Windows の有線接続アイコンと同様のユーザインターフェイスを簡素化したものです。SSC トレイ アイコンを使用すると、数回クリックするだけで無線接続を管理できます。

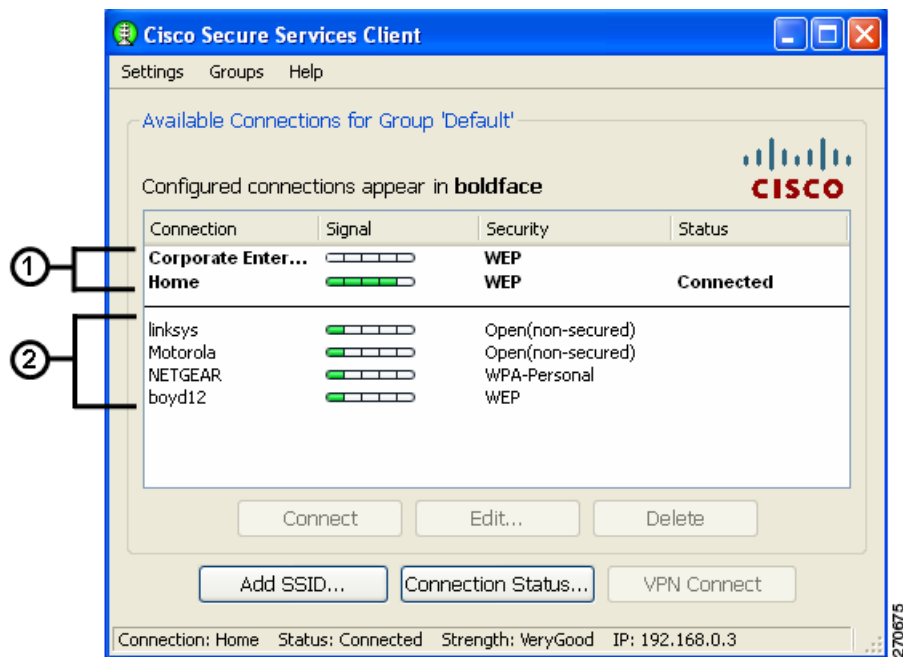
メイン SSC GUI インターフェイスには、ネットワークの設定、クライアントの有効化または無効化、VPN の設定、および信号の強さや詳細なネットワーク スキャン リストなどのネットワーク情報の表示の機能が追加されています。

メイン SSC GUI ウィンドウの使用方法

メイン SSC GUI ウィンドウには3つの領域があり、ユーザによるネットワークの設定、制御、および管理を支援します。

- メニュー領域：SSC および Wi-Fi 無線の有効化 / 無効化、グループの表示と設定、およびヘルプ情報の取得を行うための領域です。
- グラフィカル領域：設定済みのネットワーク接続のリスト、および検出された隣接ネットワークのリストが表示されます。
- ボタン領域：ネットワーク接続の追加、編集、削除、およびネットワークへの接続を行うための領域です。また、接続状態に関する情報の表示や、VPN トンネルを使用した接続も可能です。

図 4-1 メイン SSC GUI ウィンドウ



<p>1 設定済みの接続が次の順序で表示されます。</p> <p>最初に優先される基準：管理者が作成した接続が展開された順に表示されます。</p> <p>次に優先される基準：ユーザが作成した接続が作成された順に表示されます。</p>	<p>2 検出されたスキャン リストの接続は、隣接ネットワークであり、ユーザ接続に使用できる場合があります。これらの接続は、無線アクセスポイントの SSID で識別され、セキュリティ レベル グループ別に表示されます。</p>
---	--

表 4-1 には、メイン SSC GUI ウィンドウのコンポーネントについての説明をまとめてあります。

表 4-1 メイン SSC GUI ウィンドウのコンポーネント


コンポーネント	説明
列	Connection 設定済みのネットワーク接続のリスト、および検出された隣接ネットワークのスキャン リストが示されます。
	Signal 接続が無線の場合、受信信号の相対的な強さがバーで表示されます。無線接続が検出されない場合や非表示の場合（非ビーコンの場合）には、バーで強度が示されません。接続が有線の場合は、静的なブレースホルダアイコンが表示されます。
	Security セキュリティ レベルを示します。 Open (non-secured) : 認証も暗号化も実行されないことを示しています。 WEP : 静的な WEP 暗号化による従来のオープン アソシエーション、または WEP 共有キーによる共有アソシエーション。 WPA/WPA2-Personal : パスフレーズ事前共有キー (PSK) を使用する Wi-Fi 規格。WPA2 は、802.11i 規格に完全に準拠するように改善された、WPA の最新規格です。 WPA/WPA2-Enterprise : 認証サーバを使用する Wi-Fi 規格。WPA2 は、802.11i 規格に完全に準拠するように改善された、WPA の最新規格です。 CCKM-Enterprise : Cisco Central Key Management (CCKM) セキュリティ プロトコルを使用すると、802.11 ステーションが、クライアントと新しい親アクセス ポイントとの間で迅速に再認証を行って新規セッションを確立できます。  (注) 設定済みのネットワークの場合、表示されるセキュリティ レベルは、管理者およびユーザによって設定されたものです。検出されたネットワークのスキャン リストの場合、複数のセキュリティ レベルが使用可能であれば、最も安全なレベルが表示されます。
	Status 現在の接続の状態を表示します。 Searching for adapter : アダプタが使用可能でないか無効であることを示しています。 Associating : 現在、802.11 アソシエーション プロトコルを使用して接続をアソシエート中であることを示しています。 Authenticating : 現在、802.1X 認証プロトコルを使用して接続を認証中であることを示しています。 Acquiring IP address : 接続の IP アドレスを取得中であることを示しています。 Connected : 接続が確立されたことを示しています。

表 4-1 メイン SSC GUI ウィンドウのコンポーネント (続き)

コンポーネント	説明	
ボタン	Connect	選択された設定済みの接続、またはスキャンリスト内の隣接ネットワークに接続します。
	Edit	選択された、ユーザが設定した接続を編集します。 ユーザは、事前設定済みのネットワーク接続やスキャンリスト内の隣接ネットワークを編集できません。
	Delete	選択された、ユーザが設定した接続を削除します。 ユーザは、事前設定済みのネットワーク接続やスキャンリスト内の隣接ネットワークを削除できません。
	Add SSID	新規接続を追加して設定します。
	Connection Status	現在使用中の接続の状態に関する情報を表示します。
	VPN Connect	VPN 接続を有効化します。 configuration.xml ファイル内の、管理者によるクライアント ポリシーの設定で、VPN が指定されている必要があります。
	メニュー	Settings
Groups		設定済みのグループのリスト、およびグループ設定オプションが表示されます。 Configure Groups : 設定済みの接続の新規グループを設定できます。
Help		ヘルプ情報を参照できます。 Help : SSC ヘルプ情報を提供します。 Repair : SSC を修復できます。 About : SSC のバージョン情報を提供します。

設定済みの接続への接続

メイン SSC GUI ウィンドウには、ネットワーク管理者が展開した、事前設定済みの接続プロファイルのリストと、ユーザが作成した、設定済み接続プロファイルのリストが表示されます。SSC では、2つのモードで接続を作成できます。

- 自動接続モード
- 排他接続モード

自動接続

通常よく使用される自動接続モードでは、使用可能な設定済みの接続から、SSC が自動的に最適なものを選択します。グループに有線接続と無線接続の両方が含まれる場合は、有線接続が優先されます。接続に失敗した場合や接続が切断された場合、SSC は設定済み接続リストの次のエントリに対して接続を試行します。



(注) SSC では、一度に1つの接続だけ許可されます。

SSC が設定済み接続リストの最初から接続を再開する条件は、次のとおりです。

- ユーザまたは停電によって PC が再起動された。
- ユーザが別の接続グループに切り替えた。
- ユーザが Repair オプションを使用して SSC を再起動した。

自動接続モードでは、以下のいずれかの操作を行うことによって、ユーザが SSC の接続基準を上書きできます。

- 設定済みの接続を選択し、Connect ボタンをクリックする。
- 設定済みの接続を右クリックし、Connect オプションを選択する。
- 設定済みの接続をダブルクリックする。

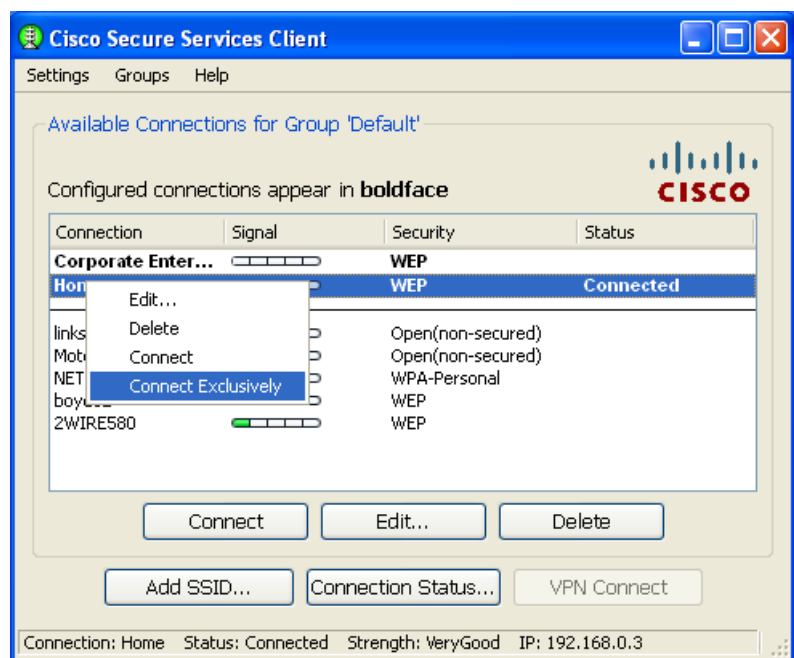
ユーザがこれらの操作を行うと、SSC は現在の接続を中断し、選択された設定済み接続プロファイルを使用して接続を開始しようとします。SSC は自動接続モードのままです。

接続の試行に失敗すると、SSC は、リスト内の最初の設定済み接続への接続を試行します。

排他接続モード

SSC では、ユーザが排他接続を指定できます (図 4-2 を参照)。これによって、SSC は既存の接続を切断し、新たに指定された接続に排他的に接続しようとします。接続に失敗した場合や接続が切断された場合、SSC は別の接続への切り替えを試行しません。

図 4-2 Connect Exclusively オプション



自動接続モードの場合、次の操作を行うことによって排他接続オプションを有効にできます。設定済みの接続を右クリックし、Connect Exclusively オプションを選択します。

排他接続モードを終了して自動接続モードに戻るには、接続を右クリックして Connect Exclusively オプションをもう一度選択します。

通常、排他接続モードを使用するのは、SSC が既存の有線接続を切断して、指定された無線接続だけに接続するようにする場合です。

新規接続の作成

ユーザは、次のようないくつかの方法で、手動で新規接続を設定できます。

- スキャンリスト内の検出されたネットワークをダブルクリックする。
- スキャンリスト内の検出されたネットワークを右クリックし、Connect オプションを選択する。
- スキャンリスト内の検出されたネットワークを選択し、Connect ボタンをクリックする。
- Add SSID ボタンをクリックする。Add SSID ボタンは、無線が次のような状況にある場合に使用します。
 - スキャン可能なアクセス ポイント：ビーコンまたは応答をアクティブなプローブに送信することによって検出されるが、使用不可能であると見なされている（物理的に検出範囲にない）。
 - スキャン不可能なアクセス ポイント：無線スキャンにおいて検出可能と設定されておらず（非ビーコンまたは非表示）、物理的に検出範囲にない場合がある。

SSC のセキュリティ オプション

SSC GUI では、以下のセキュリティ オプションを使用して新規接続プロファイルを作成できます。

- Open(non-secured)
- WEP
- Shared WEP
- WPA Personal AES
- WPA Personal TKIP
- WPA2 Personal AES
- WPA2 Personal TKIP
- WPA Enterprise AES
- WPA Enterprise TKIP
- WPA2 Enterprise AES
- WPA2 Enterprise TKIP
- CCKM Enterprise AES
- CCKM Enterprise TKIP



(注)

ユーザが使用可能なセキュリティ オプションは、展開された SSC 設定ファイルで管理者がどのオプションを有効にしたかによって異なります。

VPN 接続オプションの設定

いずれの接続セキュリティ設定ウィンドウでも、一番下の部分で VPN 接続オプションを設定できます。VPN オプションを設定する手順は、次のとおりです。

- Automatically connect to VPN オプションをオンにします。
- ドロップダウン矢印をクリックして VPN 認証オプションのいずれか 1 つを選択します。



(注)

VPN 接続オプションは、Cisco IPsec VPN (4.8 以降) がユーザの PC にインストールされている場合にだけ使用できます。



(注) VPN で SofToken-II を使用する場合は、SSC でユーザ名および PIN の入力を求められるので、SofToken アプリケーション用に通常使用する PIN を入力します。SofToken - II アプリケーションによって生成されるワンタイム パスワードは入力しないでください。



(注) SSC でユーザの VPN クレデンシャルが保持されるのは、ユーザがログオフするか SSC がシャットダウンするまでです。

オープンな安全でないネットワーク接続の使用

スキャンリストから Open(non-secured) のネットワークを選択すると、SSC はその接続を自動的に設定済みの接続として再割り当てし、設定済み接続リストの一番下に移動してから、接続を開始します（より優先順位の高い有線接続が使用可能でない場合）。

WEP または Shared WEP 接続の設定

スキャンリストから WEP または Shared WEP ネットワークを選択すると、Enter Connection Info ウィンドウが表示されます（図 4-3）。キーを入力するか、パスフレーズを使用して WEP キーを生成してください。

図 4-3 WEP または Shared WEP の情報

Enter Connection Info

Connect

Descriptive Name:

SSID Name:

Security:

Key:

Show key

A 40/64 bit WEP keys must be 5 ASCII characters or 10 hex digits. A 104/128 bit WEP keys must be 13 ASCII characters or 26 hex digits.

VPN Settings

Automatically connect to VPN

270677

一部のルータでは、パスフレーズを使用して一意の WEP キーを作成します。Generate Router WEP key ボタンを使用すると、SSC で WEP キーの作成に使用される 64 ビット（16 進数 10 桁）または 126 ビット（16 進数 26 桁）のルータ パスフレーズを入力できます。

WPA Personal または WPA2 Personal Connection の設定

WPA Personal または WPA2-Personal のいずれかのセキュリティ オプションが設定されたネットワークを選択する場合は、パーソナル キーを入力する必要があります。SSC でサポートされる WPA Personal および WPA2 Personal のセキュリティ タイプは次のとおりです。

- WPA Personal AES
- WPA Personal TKIP
- WPA2 Personal AES
- WPA2 Personal TKIP

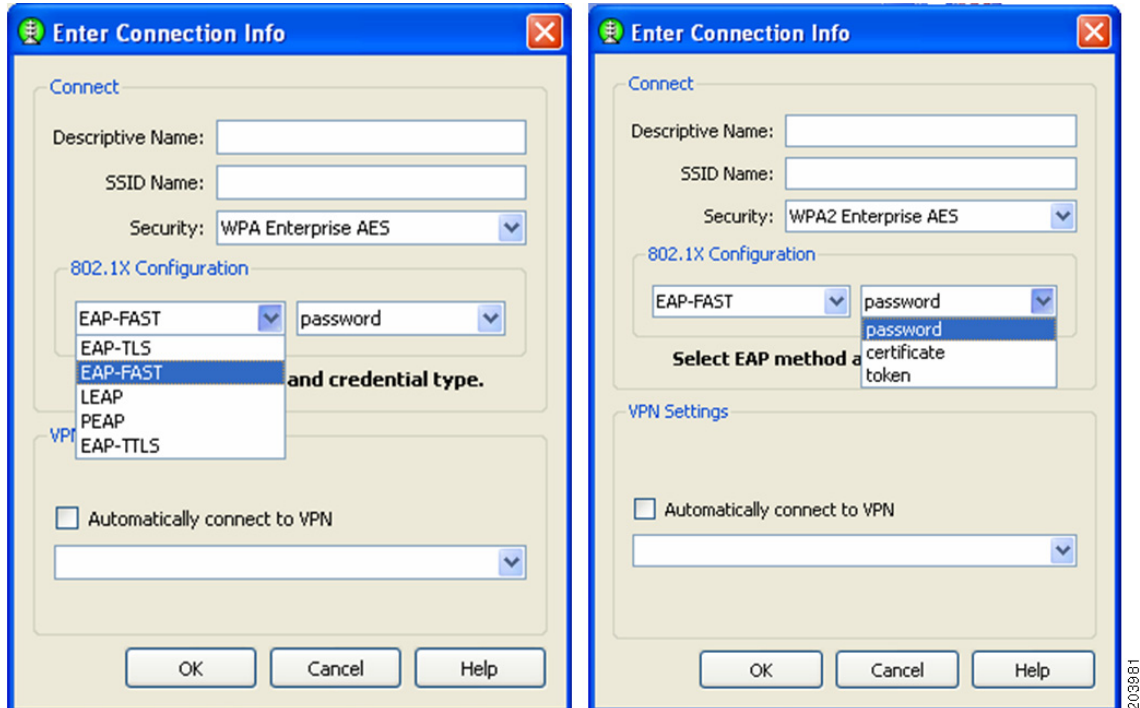
Enter Connection Info ウィンドウでは、WPA Personal または WPA2 Personal のセキュリティ設定を行います (図 4-4)。

- WPA Personal または WPA2 Personal の情報

802.1X 接続の設定

スキャン リストから 802.1X のセキュリティが設定されたネットワークを選択する場合は、使用する EAP 方式およびクレデンシャルを選択する必要があります（図 4-4 を参照）。

図 4-4 802.1X のセキュリティ情報



(注)

SSC GUI では、いくつかの限られた 802.1X オプションを使用できます。802.1X プロファイルは、ネットワーク管理者が、展開を目的として SSC 管理ユーティリティを使用して作成します。

SSC では、次の種類の 802.1X セキュリティがサポートされています。

- WPA Enterprise AES
- WPA Enterprise TKIP
- WPA2 Enterprise AES
- WPA2 Enterprise TKIP
- CCKM Enterprise AES
- CCKM Enterprise TKIP



(注)

ユーザが使用可能なオプションは、展開された SSC 設定ファイルで管理者がどのオプションオプションを有効にしたかによって異なります。

EAP 方式ドロップダウン矢印をクリックして、SSC でサポートされている EAP 方式のいずれか 1 つを選択します。

- LEAP
- PEAP
- EAP-TLS
- EAP-TTLS
- EAP-FAST

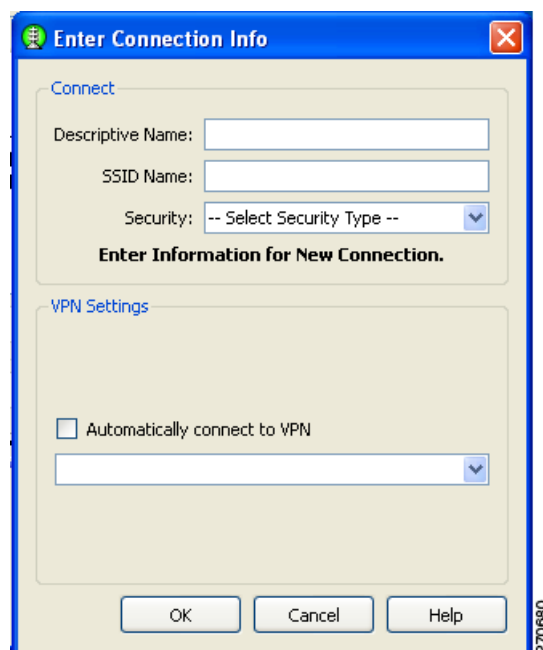
証明書の種類のドロップダウン矢印をクリックして、SSC でサポートされている証明書の種類のいずれか 1 つを選択します。

- Static password
- Certificate
- Token

Add SSID ボタンを使用した新規接続の設定

Add SSID ボタンをクリックすると、[図 4-5](#) のウィンドウが表示されます。

図 4-5 新規接続情報



次のセキュリティ オプションを設定する必要があります。

1. Descriptive Name : 接続を識別するために表示される名前。
2. SSID Name : 接続を確立するために使用されるネットワーク名です。アクセス ポイントは、ビーコンでこの SSID をブロードキャストします。
3. Security : 接続に使用するセキュリティ認証の種類を指定します (「[SSC のセキュリティ オプション](#)」の項 (P.4-6) を参照)。
4. VPN : VPN 接続オプションを指定します (「[VPN 接続オプションの設定](#)」の項 (P.4-6) を参照)。

設定済みの接続の管理

メイン SSC GUI ウィンドウで、ユーザが作成した設定済みの接続を編集または削除できます。



(注)

ユーザは、管理者が展開した事前設定済みの接続を編集または削除することはできませんが、それらの設定を表示することはできます。

ユーザが作成した設定済みの接続を削除するには、削除する設定済みの接続を右クリックして Delete オプションを選択します。

ユーザが作成した設定済みの接続の編集

メイン SSC GUI ウィンドウには、ユーザが作成した設定済みの接続を編集するためのオプションがあります。

- 設定済みの接続を右クリックして Edit オプションを選択すると、[図 4-6](#) が表示されます。
- 設定済みの接続を選択して Edit ボタンをクリックすると、[図 4-6](#) が表示されます。

図 4-6 設定済みの接続のプロファイル フィールド

ユーザは、次の接続プロファイル フィールドを編集できます。

- Descriptive Name
- Key (該当する場合)



(注)

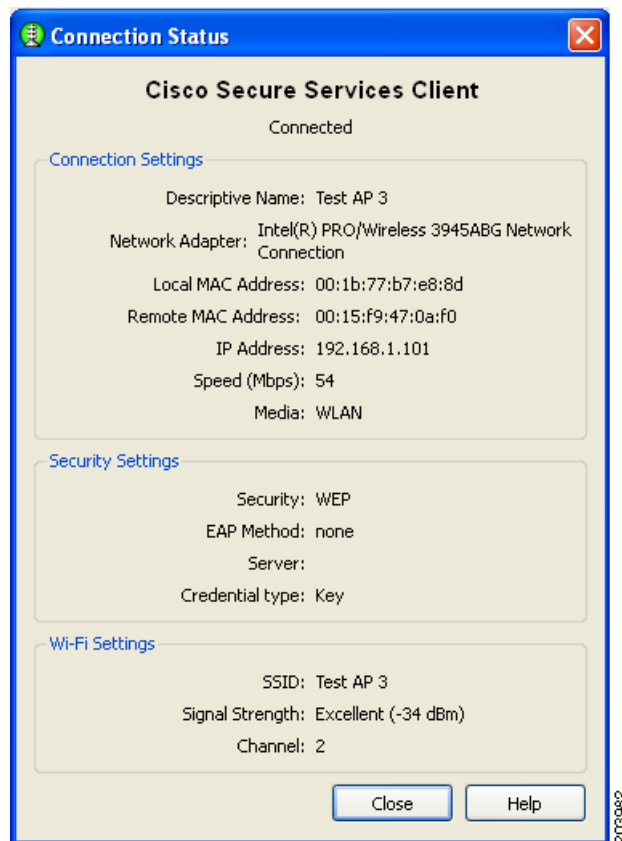
接続のセキュリティ モードを変更するには、接続を削除してから、セキュリティ オプションを新たに設定して接続を作成し直す必要があります。

接続状態の情報の取得

次のいずれかの操作を行うことによって、現在の接続状態に関する情報を取得できます。

- SSC GUI ウィンドウで **Connection Status** をクリックすると、[図 4-7](#) が表示されます。
- SSC トレイ アイコンを右クリックして **Connection Status** を選択すると、[図 4-7](#) が表示されます。

図 4-7 SSC の Connection Status ウィンドウ

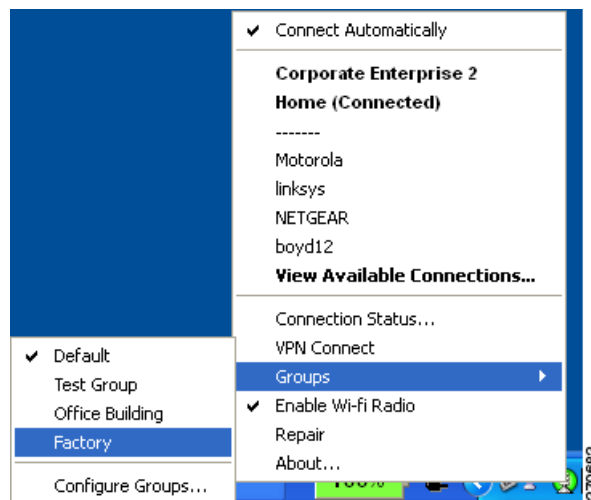


ネットワーク グループの選択

SSC にはグループ機能があり、ネットワーク接続を便宜上いくつかのグループに分類できます。SSC では、2 とおりの方法で、設定済みの接続グループを選択して有効にできます。

- SSC トレイ アイコンを使用 (図 4-8 を参照)
 - SSC トレイ アイコンを右クリックし、Groups までスクロールして、リストから対象のグループを選択します。
- メイン SSC GUI ウィンドウの Group メニューを使用 (図 4-9 を参照)
 - メイン SSC GUI ウィンドウで、Groups をクリックして対象のグループを選択します。

図 4-8 SSC トレイ アイコンのショートカット メニュー



アクティブなグループを変更すると、SSC では次の処理が実行されます。

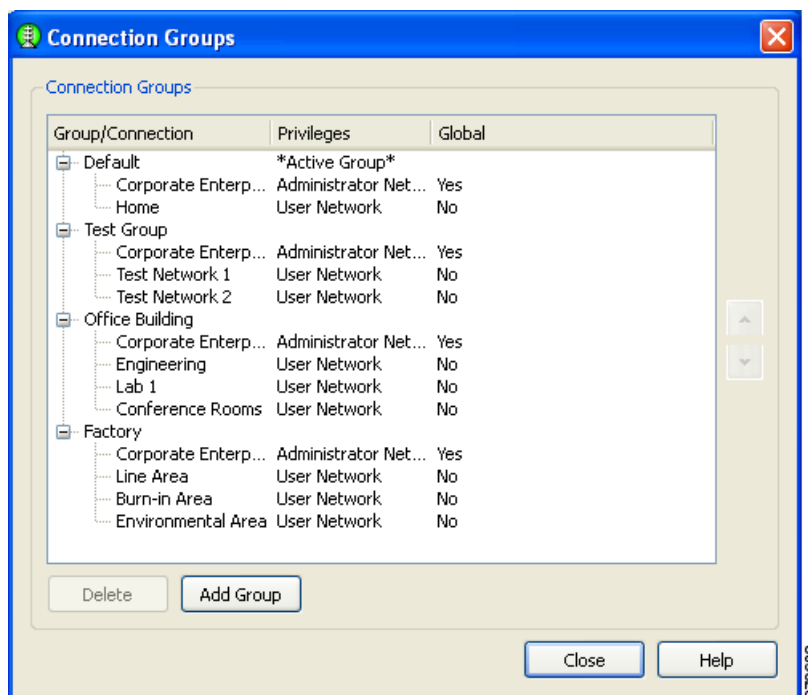
- 現在のグループからのアクティブな接続があれば切断します。
- 排他接続モードが有効であれば、それを取り消します。
- 新規グループの接続リストの一番上から、自動接続プロセスを開始します。

ネットワーク接続グループの管理

Connection Groups ウィンドウでは、ネットワーク接続グループを管理できます。Connection Groups ウィンドウを開くには、次のいずれかの操作を行います。

- メイン SSC GUI ウィンドウで **Groups > Configure Groups** をクリックすると、[図 4-9](#) が表示されます。
- SSC トレイ アイコンを右クリックし、Groups までスクロールして **Configure Groups** を選択すると、[図 4-9](#) が表示されます。

図 4-9 Connection Groups ウィンドウ



Connection Groups ウィンドウでは、新規グループを追加したり、ユーザが作成したネットワーク接続やグループを削除したりできます。



(注) 事前設定済みの接続をユーザが削除することはできません。

メニューコントロール

メイン SSC GUI メニューには3つの選択項目があります。

- **Settings** : SSC または無線を、有効または無効にします。
- **Group** : グループを選択、追加、または削除します。
- **Help** : ヘルプ情報の参照、SSC の修復、パケット キャプチャの有効化、SSC バージョン情報の参照に使用します。

Settings メニュー

Settings をクリックすると、ドロップダウンリストが表示されます (図 4-10 参照)。

図 4-10 Settings のメニュー オプション



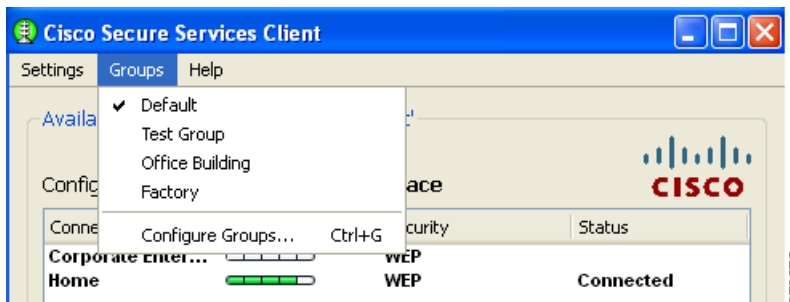
Settings メニューには次のオプションがあります。

- **Enable Client** : SSC でネットワーク アダプタを管理するかどうかを制御します。
 - オンの場合、SSC により、すべての有線アダプタおよび無線アダプタが、展開された設定ファイルの使用可能なメディア ポリシーの設定に従って管理されます。
 - オフの場合、SSC は無効になっており、ネットワーク アダプタが SSC によって制御されることは一切ありません。
- **Enable Wi-Fi Radio** : 管理対象のすべての無線アダプタの無線の状態が制御されます。
 - オンの場合、すべての無線アダプタの無線は有効であり、アクティブです。
 - オフの場合、すべての無線アダプタの無線は無効であり、オフになっています。

Groups メニュー

Groups をクリックすると、ドロップダウンリストが表示されます (図 4-11 参照)。

図 4-11 メイン SSC GUI の Groups



Groups メニューには次の機能があります。

- 設定済みのグループのリストを表示します。
 - チェックマークが付いているグループは、アクティブです。
 - リストに示されたグループをクリックして選択すると、そのグループを有効にできます。
- **Configure Groups** : 新規グループを作成したり、ユーザが作成したグループや設定済みの接続を削除したりできます。詳細は、「[ネットワーク接続グループの管理](#)」の項 (P.4-14) を参照してください。

Help メニュー

Help をクリックすると、ドロップダウン メニューに次のオプションが表示されます。

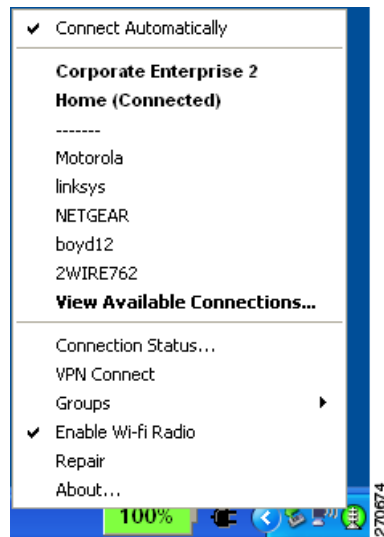
- **Help** : ヘルプ インターフェイスを開き、ヘルプ情報を提供します。
- **Repair** : SSC サービスを強制的に再起動します。次の処理が実行されます。
 - SSC サービスの再起動中、SSC トレイ アイコンには赤いバツ印が表示されます。
 - SSC により、新規設定が検出および処理されます。
 - SSC が自動接続モードで再起動し、以前にアクティブであったグループの接続リストの一番上から接続が開始されます。
- **About** : 製品名とバージョン番号を表示します。

SSC トレイ アイコンの使用法

SSC トレイ アイコンでは、次の2とおりの簡単な方法で、接続を有効または無効にできます。

- SSC トレイ アイコンをダブルクリックして、メイン SSC GUI ウィンドウを有効にします。
- SSC トレイ アイコンを右クリックして、アイコンメニューを有効にします (図 4-12 を参照)。

図 4-12 SSC アイコンのショートカット メニュー



SSC アイコンのショートカット メニューには、メイン SSC GUI ウィンドウで使用可能な多くのコントロールへのショートカットがあります。

- **Connect Automatically** : SSC の動作モードを示します。
 - オンの場合、使用可能な設定済みの接続のうちで最適なものが、SSC によって自動的に選択されます。
 - オフの場合、SSC は、下のリストでチェックマークが付いている設定済みの接続だけに接続します。
- 設定済みの接続は、太字で示されます。
 - このリストの接続にチェックマークが付いていて、SSC 自動接続機能がオフの場合は、その接続に対して排他接続が試行されます。
 - このリストの接続に (connected) と表示されている場合、SSC は現在その設定済みの接続に接続されています。
 - このリストの接続をクリックすると、SSC は、指定された設定済みの接続への接続を試行します。接続に失敗すると、SSC は、設定済みの接続のリストから、次に最適な接続を検索します。
- 検出されたスキャンリスト ネットワークは、点線の下に表示されます。
 - スキャンリストのネットワークをクリックすると、SSC は、指定されたネットワークへの接続を試行します。ネットワークでセキュリティが有効になっている場合、SSC は、必要なキー情報の入力を要求します。

必要なセキュリティ情報の入力後に接続に失敗すると、SSC は、設定済みの接続のリストから次に最適な接続を検索します。新規ネットワーク接続は、設定済みの接続のリストに含まれたままになります。

- Connection Status : 役に立つ接続情報を提供します。
 - Connection Status をクリックすると、Connection Status ウィンドウが表示され、接続、セキュリティ、および Wi-Fi 設定情報が表示されます。Connection Status ウィンドウの Help ボタンをクリックすると、ウィンドウの要素および値に関する情報を参照できます。
- Connect VPN : 自動 VPN 接続を有効にできます。
 - Connect VPN をクリックすると、VPN Settings ウィンドウが表示され、現在アクティブな接続で自動 VPN 接続を有効にしたり、VPN 接続エントリを選択したりできます。
- Groups : 設定済み接続グループのリストが表示され、接続グループを追加または削除できます。
 - Configure Groups : Configure Groups をクリックすると、Connection Groups ウィンドウが表示され、設定済みの接続グループのリストが表示されます。Connection Groups ウィンドウの Help ボタンをクリックすると、ウィンドウの要素および値に関する情報を参照できます。
- Enable Wi-Fi Radio : 無線のオンとオフを切り替えられます。
- Repair : SSC を再起動して修復手順を有効にできます。
- About : 製品名とバージョン情報を表示します。