CHAPTER 4

Using Cisco SSC

This chapter provides an overview of SSC and the main SSC GUI features. The chapter contains these sections:

Overview

SSC runs from two logical interfaces:

- SSC tray icon—A minimal user interface designed for quick access to primary SSC functions and information.
- Main SSC GUI window—The primary user interface designed to provide complete SSC functionality.

The SSC tray icon interface simplifies the user interface similarly to a Windows wired connection icon. The SSC tray icon allows the user to manage wireless connections using a few simple clicks.

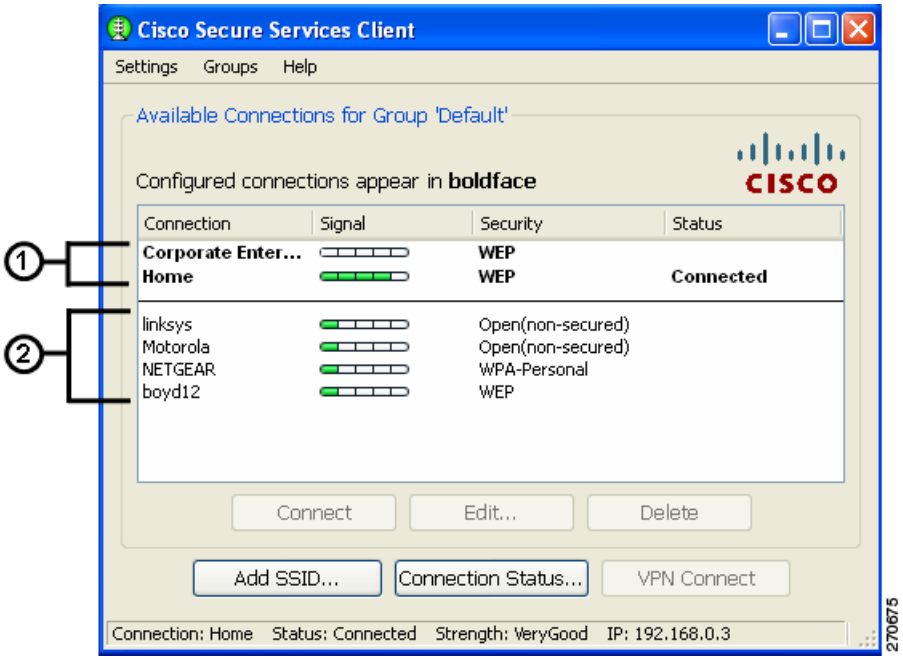
The main SSC GUI interface adds functionality for configuring networks, enabling or disabling the client, configuring VPN, and viewing network information such as signal strength and the complete network scan list.

Using the Main SSC GUI Window

The main SSC GUI window contains three main areas to help the user configure, control, and manage networks:

- Menu area—Enables and disables SSC and the Wi-Fi radio, views and configures groups, and obtains helpful information.
- Graphical area—Displays a listing of configured network connections and a list of detected neighboring networks.
- Button area—Allows the user to add, edit, delete, and connect to network connections. The user can also view connection status information and connect using a VPN tunnel.

Figure 4-1 Main SSC GUI Window



1	Configured connections are listed in the following order: First—By administrator-created connections in the order they were deployed. Second—By user-created connections in the order they were created.	**2**	Discovered scan-list connections are neighboring networks that might be available for user connections. They are identified by the SSID of the wireless access point. These connections are listed by security level groupings.

Table 4-1 describes the main SSC GUI window components.

Table 4-1 Main SSC GUI Window Components

Component		Description
Column	Connection	Identifies a list of configured network connections and a scan-list of detected neighboring networks.
	Signal	When the connection is wireless, this column displays a relative signal strength bar of the received radio signal. If the wireless connection is not detected or hidden (non-beaconing), then an empty bar is displayed. If the connection is wired, a static placeholder icon is displayed.
	Security	Identifies the security level: Open (non-secured)—Specifies no authentication and no encryption. WEP—Legacy open association with static WEP encryption or shared association with WEP-shared keys. WPA/WPA2-Personal—A Wi-Fi standard that uses a pass-phase pre-shared key (PSK). WPA2 is a recent upgrade to WPA based on the full 802.11i standard. WPA/WPA2-Enterprise—A Wi-Fi standard that uses an authentication server. WPA2 is a recent upgrade to WPA based on the full 802.11i standard. CCKM-Enterprise—Cisco Central Key Management (CCKM) security protocol enables an 802.11 station to quickly re-authenticate and establish a new session between a client and a new parent access point. **Note** For the configured networks, the security level displayed is the setting configured by the administrator and the user. For the scan-list detected networks, the security level is the most secure level when multiple security levels are available.
	Status	Displays the current connection status: Searching for adapter—Specifies an adapter is not available or the adapter is disabled. Associating—Indicates that the connection is currently associating using the 802.11 association protocol. Authenticating—Indicates that the connection is currently authenticating using the 802.1X authentication protocol. Acquiring IP address: Indicates that the connection is obtaining an IP address. Connected—Indicates that a connection has been established.

Table 4-1 Main SSC GUI Window Components

Component		Description
Button	Connect	Used to connect to a highlighted configured connection or a neighboring network from the scan list.
	Edit	Used to edit the highlighted user-configured connection. The user cannot edit a pre-configured network connection or neighboring networks in the scan list.
	Delete	Used to delete the highlighted user-configured connection. The user cannot delete a pre-configured network connection or a neighboring network in the scan list.
	Add SSID	Used to add and configure a new connection.
	Connection Status	Displays status information for the current connection being used.
	VPN Connect	Used to activate a VPN connection. VPN must be specified in the administrator's client policy settings in the configuration.xml file.
Menu	Settings	Enable Client—Allows the user to enable or disable SSC. Enable Wi-Fi Radio—Allows the user to enable or disable the radio. A checkmark indicates that the option is enabled.
	Groups	Contains a lists the configured groups and a group configuration option. Configure Groups—Allows the user to configure a new group of configured connections.
	Help	Allows the user to obtain helpful information. Help—Provides SSC help information. Repair—Allows the user to repair the SSC. About—Provides SSC version information.

Connecting Configured Connections

The main SSC GUI window contains a list of network administrator-deployed pre-configured connection profiles and a list of user-created configured connection profiles. SSC supports two modes for making connections:

- Automatic connection mode
- Exclusive connection mode

Automatic Connections

In the normally preferred automatic connection mode, SSC automatically chooses the best available configured connection. If the group contains both wired and wireless connections, the wired connection has higher priority. When a connection is unsuccessful or broken, SSC attempts a connection with the next entry in the configured connections list.

Note SSC allows only one connection at a time.

The SSC criteria for restarting at the top of the configured connection list include:

- The user restarting the PC by the user or a power interruption.
- The user switching to another connection group.
- The user using the Repair option to restart SSC.

In automatic connection mode, the user can override the SSC connection criteria by performing one of these operations:

- Highlighting a configured connection and clicking the Connect button.
- Right-clicking a configured connection and choosing the Connect option.
- Double-clicking a configured connection.

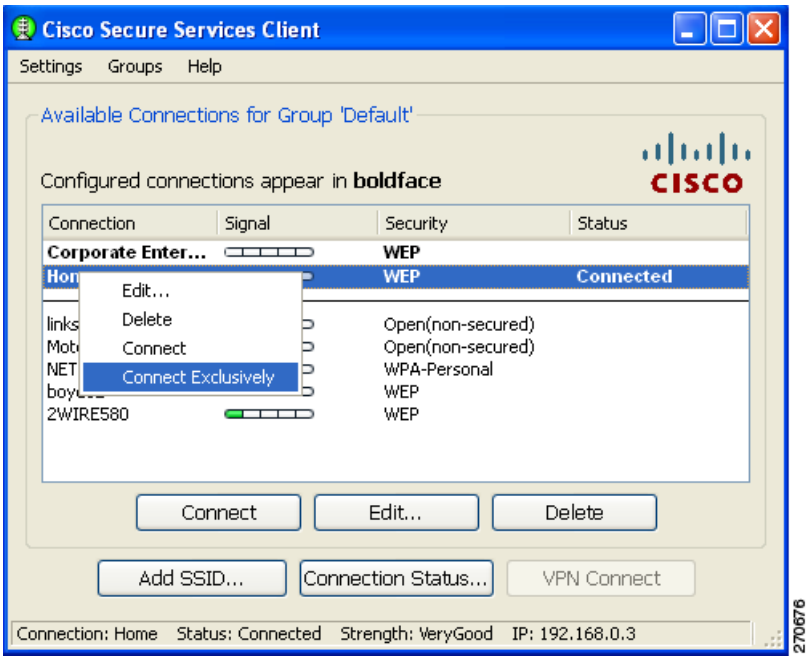
These operations cause SSC to break the current connection and attempt to initiate a connection with the selected configured connection profile. SSC remains in the automatic connection mode.

If the connection attempt is unsuccessful, SSC attempts to connect to the first configured connection in the list.

Exclusive Connection Mode

SSC allows the user to specify an exclusive connection (see Figure 4-2). This causes SSC to break an existing connection and forces SSC to exclusively attempt to connect to the new specified selection. If the connection fails or is broken, SSC does not attempt to switch to an alternate connection.

Figure 4-2 Connect Exclusively Option



The user can activate the exclusive connection option by right-clicking a configured connection and choosing the Connect Exclusively option.

To exit the exclusive connection mode and revert to automatic connection mode, the user must right-click the connection and choose the Connect Exclusively option again.

The typical reason for using the exclusive connection mode is to force SSC to drop an existing wired connection and to connect only to the specified wireless connection.

Creating New Connections

The user can manually configure a new connection several ways:

- Double-clicking a detected network from the scan-list.
- Right-clicking a detected network from the scan-list and choose the Connect option.
- Highlighting a detected network from the scan-list and click the Connect button.
- Clicking the Add SSID button. The Add SSID button should be used in these wireless situations:
  - Scanable access point—Transmits beacons or responses to active probes to allow detection but is known not to be available (not physically within detection range).
  - Non Scanable access point—Not configured to be detectable in a wireless scan (not-beaconing or hidden) and might not be physically within detection range.

SSC Security Options

Using the SSC GUI, the user can create new connection profiles using these security options:

- 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

Note The security options that are available to a user depend upon the administrator-enabled options in the deployed SSC configuration file.

Configuring VPN Connection Options

The bottom section of all the connection security configuration windows allows the user to configure VPN connection options. To configure the VPN options, the user performs these operations:

- Checks the Automatically connect to VPN option.
- Clicks the drop-down arrow and chooses one of the VPN authentication options.

Note The VPN connection option is only available when Cisco IPSec VPN (4.8 or later) is installed on the user's PC.

Note When using VPN with SofToken-II and the SSC prompts for the username and PIN, the user must provide to SSC the PIN normally intended for the SofToken application. The user must not enter the one-time password that is generated by the SofToken-II application.

Note SSC maintains the user VPN credentials only until the user logs off or the SSC shuts down.

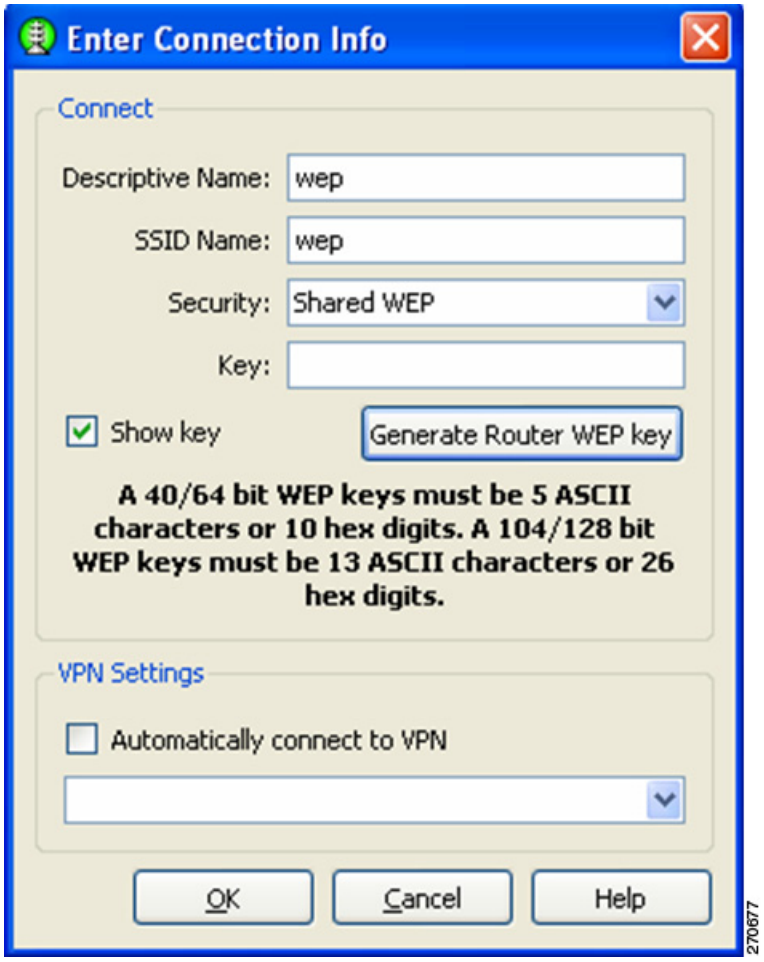
Using an Open Non-Secured Network Connection

When the user selects an Open(non-secured) network from the scan-list, SSC automatically reassigns the connection as a configured connection, moves the connection to the bottom of the configured connections list, and initiates the connection (unless a higher priority wired connection is available).

Configuring a WEP or Shared WEP Connection

When a user selects a WEP or Shared-WEP network from the scan-list, the Enter Connection Info window appears (Figure 4-3). The user needs to provide the key or generate a pass-phrase-based WEP key.

Figure 4-3 WEP or Shared WEP Information



Some routers use a pass-phrase to create a unique WEP key. The Generate Router WEP key button can be used to enter a router pass-phrase of 64 bits (10 hexadecimal digits) or 126 bits (26 hexadecimal digits) that SSC uses to create a WEP key.

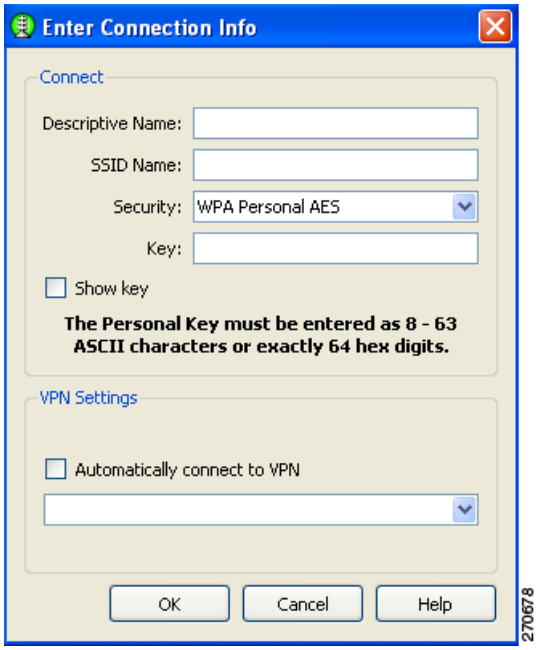
Configuring a WPA Personal or a WPA2 Personal Connection

When the user selects a network with WPA Personal or WPA2-Personal security options, the user needs to provide the personal key. SSC supports these WPA Personal and WPA2 Personal security types:

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

The Enter Connection Info window allows the user to configure WPA Personal or WPA2 Personal security settings. (Figure 4-4)

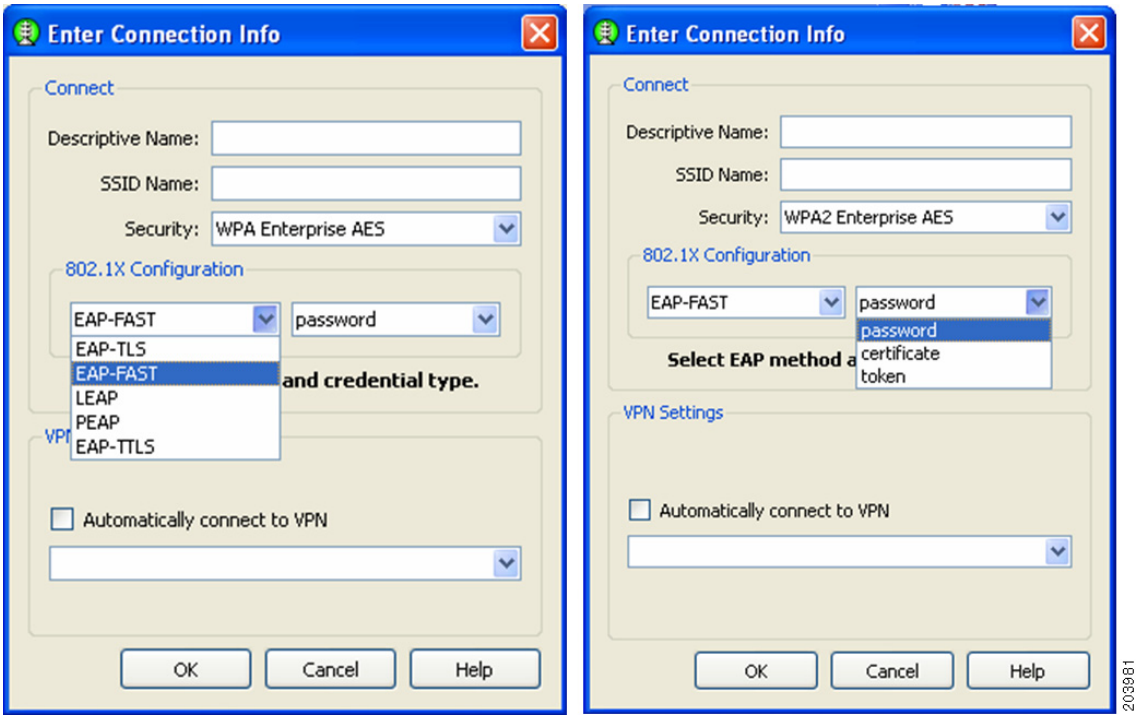
- WPA Personal or WPA2 Personal Information



Configuring an 802.1X Connection

When the user selects a network with 802.1X security from the scan list, the user needs to choose the EAP method and the type of credentials that are used (see Figure 4-4).

Figure 4-4 802.1X Security Information



Note The SSC GUI provides a limited subset of 802.1X options. For deployment purposes, 802.1X profiles should be created by the network administrator using the SSC management utility.

SSC supports these 802.1X security types:

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

Note The specific options available to a user depends upon the administrator-enabled options in the deployed SSC configuration file.

Click the EAP method drop-down arrow and choose one of these SSC supported EAP methods:

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

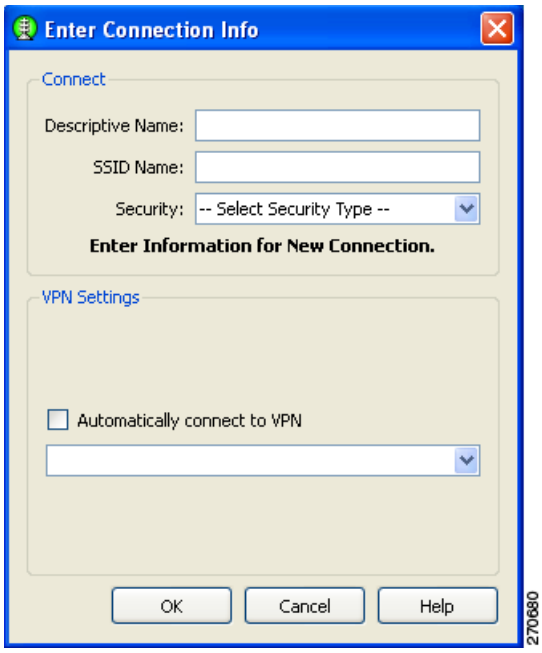
Click the certificate type drop-down arrow and choose one of these SSC supported certificate types:

- Static password
- Certificate
- Token

Configuring a New Connection Using the Add SSID Button

When the user clicks the Add SSID button, the window shown in Figure 4-5 appears.

Figure 4-5 New Connection Information



The user needs to configure these Security options:

1. Descriptive Name—A name that is displayed to identify the connection.
2. SSID Name—The network name that is used to establish the connection and is broadcast by the access point in its beacon.
3. Security—Specifies the type of security authentication used by the connection (see the "SSC Security Options" section on page 4-7).
4. VPN—Specifies the VPN connection options (see the "Configuring VPN Connection Options" section on page 4-7).

Managing Configured Connections

From the main SSC GUI window, the user can edit or delete user-created configured connections.

Note Administrator-deployed pre-configured connections cannot be edited or deleted by the user, but the settings can be viewed.

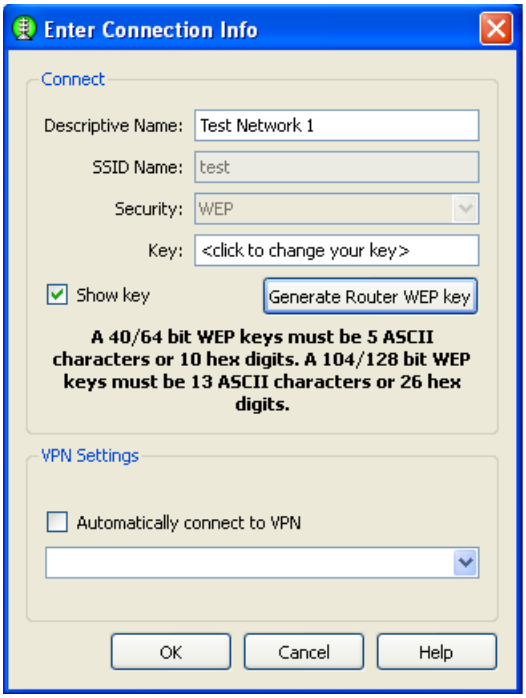
To delete a user-created configuration connection, the user needs to right-click the desired configuration connection and choose the Delete option.

Editing a User-Created Configured Connection

The main SSC GUI window provides these edit options for user-created configured connections:

- Right-click the desired configured connection and choose the Edit option. Figure 4-6 appears.
- Highlight the desired configured connection and click the Edit button. Figure 4-6 appears.

Figure 4-6 Configured Connection Profile Fields



The user can edit these connection profile fields:

- Descriptive Name
- Key (when applicable)

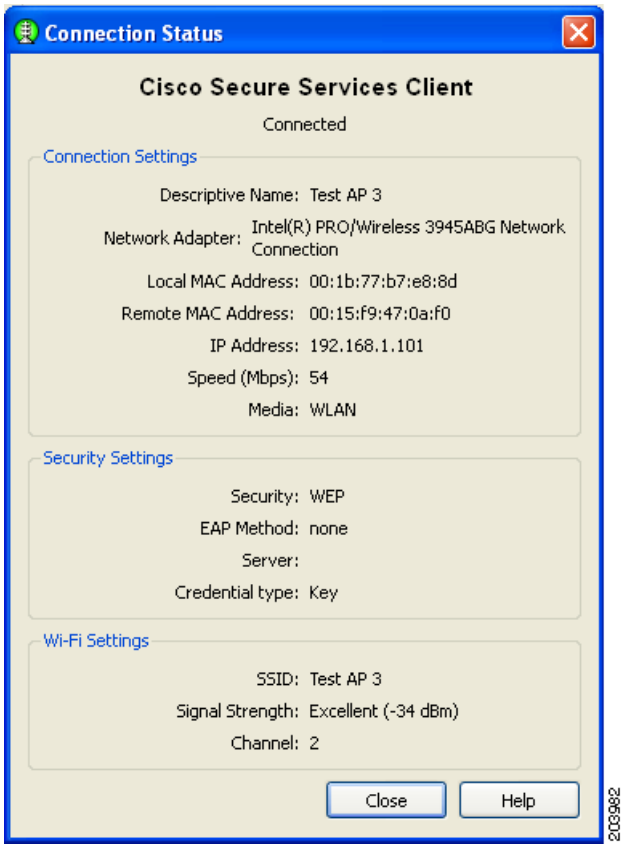
Note To change the security mode of the connection, the user must first delete the connection and then recreate the connection using a new security option.

Obtaining Connection Status Information

The user can obtain current connection status information by performing one of these operations:

- On the SSC GUI window, click **Connection Status** and Figure 4-7 appears.
- Right-click the SSC tray icon and choose **Connection Status**. Figure 4-7 appears.

Figure 4-7 SSC Connection Status Window

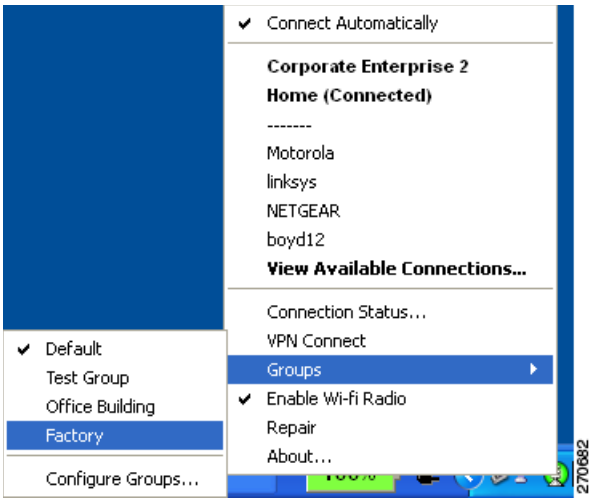


Selecting Network Groups

SSC supports a group feature that allows the user to partition network connections into convenient groups. SSC provides two ways for the user to select and activate a configured connection group:

- Use the SSC tray icon (see Figure 4-8).
  - Right-click the SSC tray icon, scroll to Groups, and choose the desired group from the list.
- Use the Group menu on the main SSC GUI window (see Figure 4-9).
  - On the main SSC GUI window, click Groups and choose the desired group.

Figure 4-8 SSC Tray Icon Right-Click Menu



Changing the active group causes SSC to perform these operations:

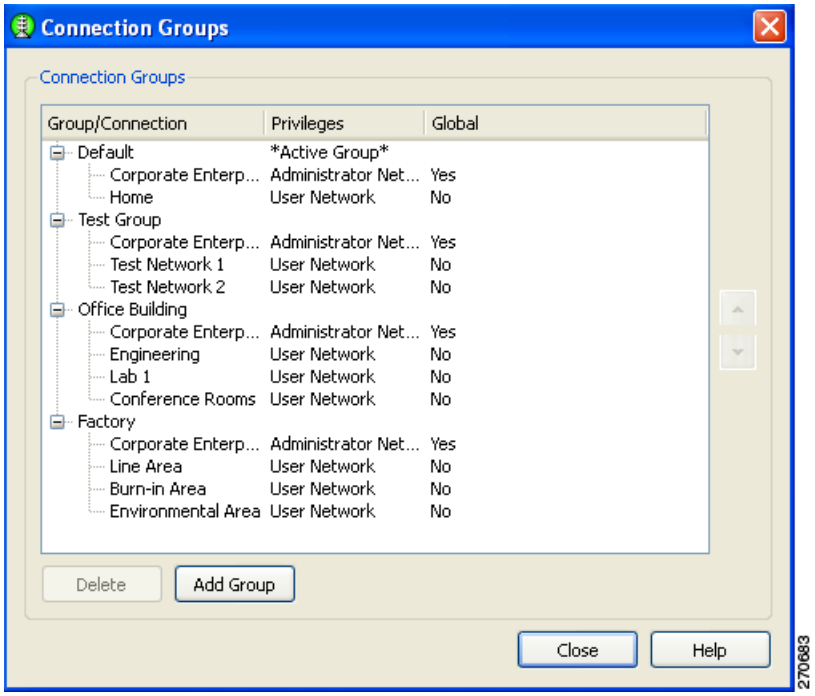
- Drops any active connection from the current group.
- Cancels exclusive connect mode if active.
- Starts the automatic connection process from the top of new group's connection list.

Managing Network Connection Groups

The user can manage network connection groups by using the Connection Groups window. To open the Connection Groups window, the user can perform one of these operations:

- From the main SSC GUI window, click ***Groups*** > **Configure Groups** and Figure 4-9 appears.
- Right-click the SSC tray icon, scroll to Groups, and choose **Configure Groups**. Figure 4-9 appears.

Figure 4-9 Connection Groups Window



From the Connection Groups window, the user can add new groups or delete user-created network connections or groups.

Note Pre-configured connections cannot be deleted by the user.

Menu Controls

The main SSC GUI menu contains three menu selections:

- Settings—Used to enable or disable SSC or the radio.
- Group—Used to select, add, or delete groups.
- Help—Used to obtain helpful information, repair SSC, enable packet capture, or obtain SSC version information.

Settings Menu

When the user clicks **Setting**s, a drop-down list appears (see Figure 4-10).

Figure 4-10 Settings Menu Options

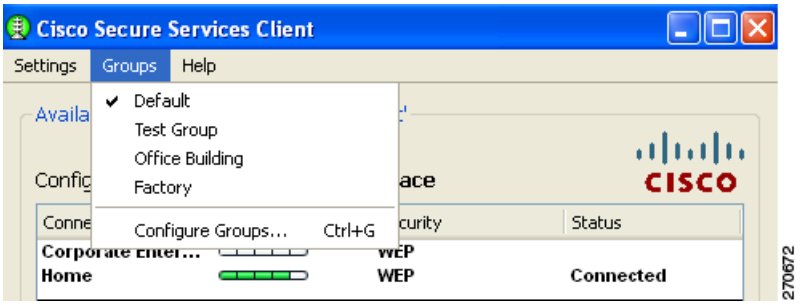
The Settings menu contains these options:

- Enable Client—Controls whether SSC is managing the network adapters.
  - When checked, the SSC is managing all wired and wireless adapters according to the allowed media policy setting of the deployed configuration file.
  - When unchecked, SSC is disabled and has relinquished control of all network adapters.
- Enable Wi-Fi Radio—Controls the state of the radio in all managed wireless adapters.
  - When checked, all wireless adapters radios are enabled and active.
  - When unchecked, all wireless adapter radios are disable and turned off.

Groups Menu

When the user clicks **Groups**, a drop-down list appears (see Figure 4-11).

Figure 4-11 Main SSC GUI Groups



The Groups menu provides these features:

- Displays a list of configured groups.
  - A checkmark indicates the active group.
  - The user can click on a listed group to activate the selected group.
- Configure Groups—Allows the user to create new groups and to delete user-created groups and configured connections. For additional information, see the "Managing Network Connection Groups" section on page 4-15.

Help Menu

When the user clicks **Help**, a drop-down menu appears with these options:

- Help—Opens the Help interface and provides helpful information.
- Repair—Forces a restart of the SSC service and causes the following actions:
  - The SSC tray icon displays a red x while the SSC service is restarting.
  - SSC detects and processes any new configuration settings.
  - SSC restarts in automatic connection mode from the top of the connection list for the previously active group.
- About—Displays the product name and version number.

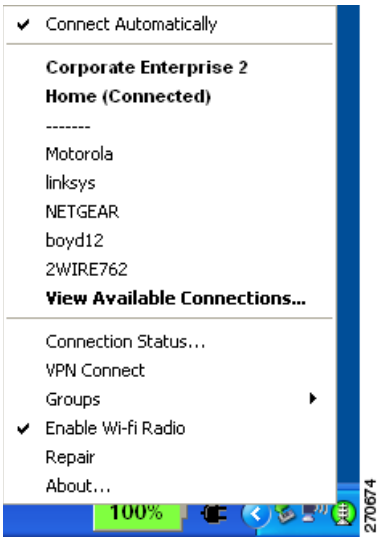
Using the SSC Tray Icon

The SSC tray icon provides two convenient ways for the user to activate a desired connection:

- Double-click the SSC tray icon to activate the main SSC GUI window.
- Right-click the SSC tray icon to activate the icon menu (see Figure 4-12).

Note If the SSC tray icon is not visible, you can access SSC by navigating to Start Menu > All Programs > Cisco > Cisco Secure Services Client and clicking **Cisco Secure Services Client Open**.

Figure 4-12 SSC Icon Right-Click Menu



The SSC icon right-click menu provides shortcuts to many of the controls available on the main SSC GUI window:

- Connect Automatically—Indicates the operating mode of SSC.
  - When checked, SSC automatically chooses the best available configured connection.
  - When unchecked, SSC will only connect to the checked configured connection in the list below.
- Configured connections are indicated in bold.
  - When a connection in this list is checked, the SSC Connect Automatically feature is turned off and an exclusive connection is being attempted on this connection.
  - When a connection in this list is followed by (connected), SSC is currently connected to the indicated configured connection.
  - When the user clicks a connection in this list, SSC attempts to connect to the specified configured connection. If the connection fails, SSC continues to search for the next best connection from the configured connections list.
- Detected scan-list networks are listed directly below the dotted line.
  - When the user clicks a network in the scan-list, SSC attempts to connect to the specified network. If the network has security enabled, SSC prompts the user to enter the needed Key information.

    After the user enters the needed security information, if the connection attempt fails, SSC continues to search for the next best connection from the configured connection list. The new network connection remains in the configured connection list.
- Connection Status—Provides the user with valuable connection information.
  - When Connection Status is clicked, the Connection Status window appears and provides connection, security, and Wi-Fi setting information.The user can click the Help button on the Connection Status window to obtain information about the window elements and values.
- Connect VPN—Allows the user to enable an automatic VPN connection.
  - When Connect VPN is clicked, the VPN Settings window appears and allows the user to enable automatic VPN connection on the currently active connection and to select a VPN connection entry.

- Groups—Displays a list of configured connection groups and allows the user to add or delete connection groups.
  - Configure Groups—When Configure Groups is clicked, the Connection Groups window appears to display a list of configured connection groups. The user can click the Help button on the Connection Groups window to obtain information about the window elements and values
- Enable Wi-Fi Radio—Allows the user to turn the radio on and off.
- Repair—Allows the user to restart SSC and enable its repair procedure.
- About—Displays the product name and version information.