Cisco Secure Services Client Users Guide

Software Release 5.1.0
December 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: 78-18640-01

Cisco Secure Services Client User Guide

CHAPTER 1

Cisco Secure Services Client Introduction

Overview

The Cisco Secure Services Client (SSC) is client software that provides 802.1X (Layer 2) and device authentication for access to both wired and wireless networks. SSC manages user and device identity and the network access protocols required for secure access. It works intelligently to make it simple for employees and guests to connect to an enterprise wired or wireless network.

SSC supports these main features:

- Wired (802.3) and wireless (802.11) network adapters
- Integrated VPN support
- Pre-logon authentication using windows machine credentials
- Single sign-on user authentication using windows logon credentials
- Simplified and easy to use 802.1X configuration
- EAP methods:
  - EAP-FAST, EAP-PEAP, EAP-TTLS, EAP-TLS, and LEAP (EAP-MD5, EAP-GTC and EAP-MSCHAPv2 for 802.3 wired only).
- Inner EAP methods:
  - PEAP—EAP-GTC, EAP-MSCHAPv2, and EAP-TLS.
  - EAP-TTLS—EAP-MD5 and EAP-MSCHAPv2 (also legacy protocols—PAP, CHAP, MSCHAP, and MSCHAPv2).
  - EAP-FAST—EAP-GTC, EAP-MSCHAPv2, and EAP-TLS.
- Encryption modes:
  - Static WEP (Open or Shared), dynamic WEP (generated with 802.1X), TKIP and AES
- Key establishment protocols:
  - WPA, WPA2/802.11i and CCKM (selectively, depending on the 802.11 NIC card)
- Smartcard provided credentials
- Cisco Trust Agent (CTA) processing when CTA is also installed

Supported Operating System Environments

The supported 32-bit operating system environments are:

- Windows XP Professional (SP2)
- Windows XP Home Edition (SP2)
- Windows 2000 (SP4)
- Windows 2003 Server Enterprise Edition (SP2)
- Other Windows XP versions, such as Media Center, Tablet PC, and Professional x64 are not supported.

Obtaining SSC Software

SSC Release 5.1.0 software is available from the Cisco Software Center:

- Cisco_SSC-XP2K_5.1.0.zip—Contains the SSC files.
- CiscoClientUtilities_5.1.0.zip—Contains the Log Packager.

The SSC software can be obtained from the Cisco Software Center at this URL

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

Click **Wireless Software > Client Adapters and Client Software > Cisco Secure Services Client** and follow the prompts to 5.1.0 under Latest Releases.

Note You must register with Cisco.com or be a registered user to download software.

SSC License Information

You have a wired, EAP-FAST only license. See your adminstrator for more licensed features.

Cisco SSC Installation Information

The installation and set-up process is completed for you:

- Your system administrator typically sends the Cisco SSC client software to your computer.
- The Cisco SSC is automatically installed on your computer.
- Your administrator pre-configures your enterprise network connections. No additional set-up should be required.

CHAPTER 2

Using Cisco SSC

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

Overview

SSC is designed to be run from two logical interfaces:

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

The SSC tray icon interface is designed to simplify the user interface similar to a Windows wired connection icon. The SSC tray icon allows the user to manage wireless connections using a few simple clicks.

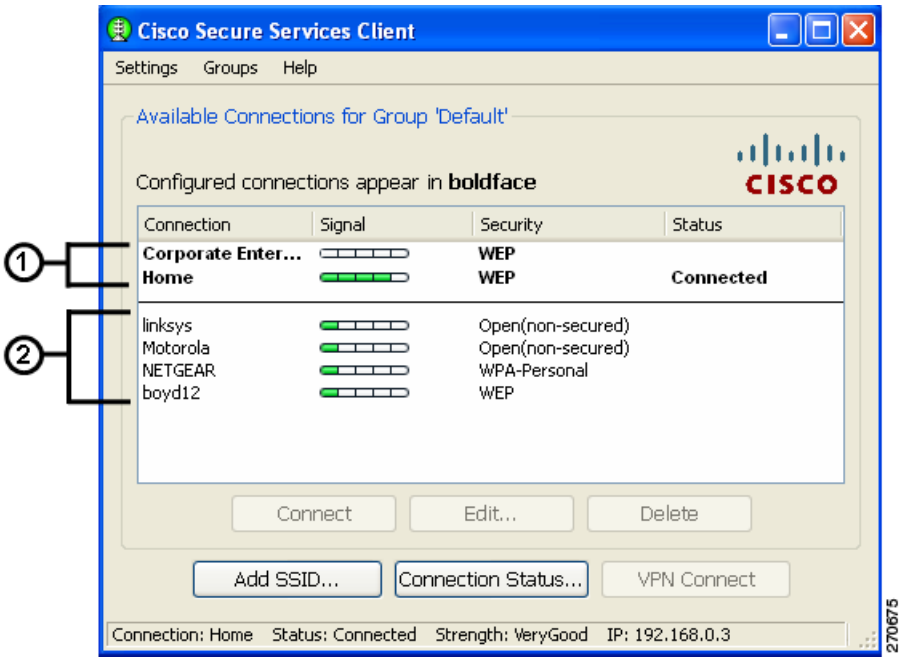
The main SSC GUI interface is designed to provide additional functionality that allows configuration of the networks, enabling or disabling of the client, VPN configuration, and to view network information such as signal strength and the complete network scan list.

Using the Main SSC GUI Page

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

- Menu area—Enables and disables SSC and the WiFi radio, view and configure groups, and obtain 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 2-1 Main SSC GUI Page



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**	Scan-list connections are discovered 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 2-1 describes the main SSC GUI page components.

Table 2-1 Main SSC GUI Page Components

Components		Description
Columns	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, 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-phrase 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.
	Status	Displays the current connection status: Searching for adapter—Specifies an adapter is not available or the adapter is disabled. Associating—Indicates the connection is currently associating using the 802.11 association protocol. Authenticating—Indicates the connection is currently authenticating using the 802.1X authentication protocol. Acquiring IP address: Indicates the connection is obtaining an IP address. Connected—Indicates a connection has been established.
Buttons	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. **Note** 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. **Note** 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. **Note** VPN must be specified in the connection profile.

Table 2-1 Main SSC GUI Page Components

Components		Description
Menus	Settings	Enable Client—Allows the user to enable or disable SSC. Enable Wi-Fi Radio—Allows the user to enable or disable the radio. **Note** A checkmark indicates 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 With Configured Connections

The main SSC GUI page 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 only allows one connection at a time.

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

- 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:

- Highlight a configured connection and click the Connect button.
- Right-click a configured connection and choose the Connect option
- Double-click 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.

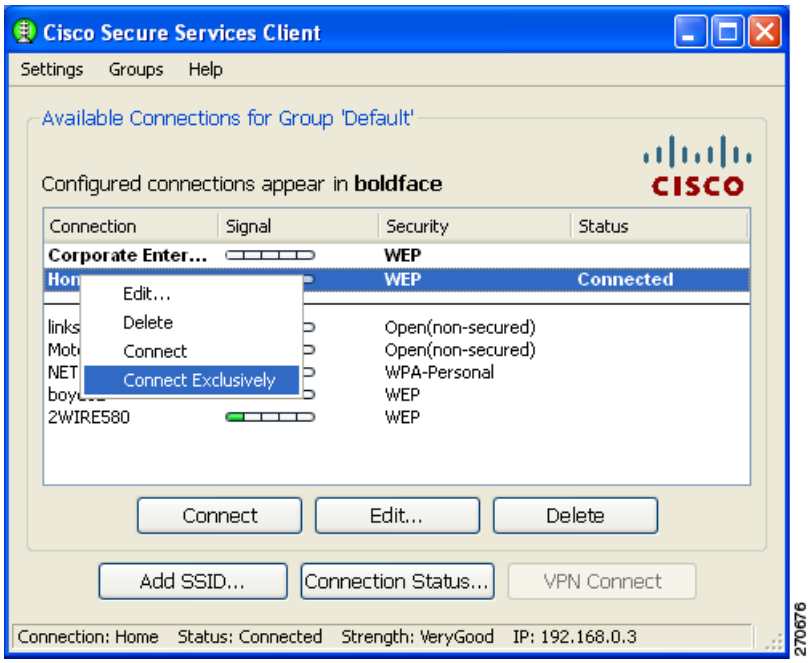
If the connection attempt is unsuccessful, SSC attempts to connect to the first configured connection in the list.

Note If you try to connect to a wireless network while the PC is connected via a wired connection, the PC reconnects to the wired connection rather than connecting to the wireless network.

Exclusive Connections Mode

SSC allows the user to specify an exclusive connection (see Figure 2-2). 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 2-2 Connect Exclusively Option



While in either automatic connection mode, the user can activate the exclusive connection option by performing this operation:

- Right-click a configured connection and choose the Connect Exclusively option

To exit the exclusive connection mode and revert back to automatic connection mode, the user must perform this operation:

- 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

SSC supports several methods that the user can use to manually create a new configured connection:

- Double-click a detected network from the scan-list.
- Right-click a detected network from the scan-list and choose the Connect option.
- Highlight a detected network from the scan-list and click the Connect button.
- Click the Add SSID button. The Add SSID button should be used in these wireless situations:
  - scanable access points—Transmits beacons or responses to active probes to allow detection, but is known not to be available (that is, 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 Supported Security Options

SSC supports 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

Configuring VPN Connection Options

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

- Check the Automatically connect to VPN option.
- Click the drop-down arrow and choose one of the VPN authentication options.

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

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

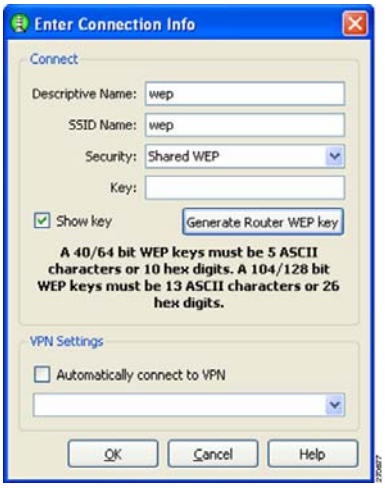
Using an Open Non-Secured Network Connection

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

Configuring a WEP or Shared WEP Connection

When a user selects a WEP or Shared-WEP network from the scan-list, Figure 2-3 appears.

Figure 2-3 WEP or Shared WEP Information



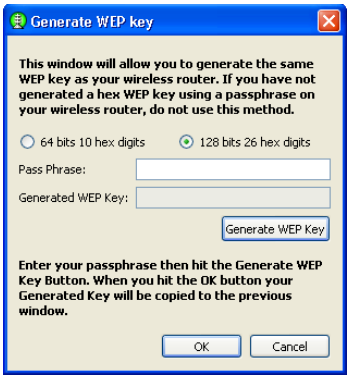
The user must provide the key in the **Key** text box or generate a pass-phrase based WEP key.

To generate a pass-phrase based WEP key, follow these steps:

Step 1 Click **Generate Router WEP key**. The Generate WEP key window allows you to generate the same WEP key as your wireless router.

Note If you have not generated a hex WEP key using a pass-phrase on your wireless router, do not use this method.

Figure 2-4 Generate WEP Key Window



Step 2 Enter the pass-phrase that you used to generate the WEP key on your router.

Step 3 Click **Generate WEP Key**.

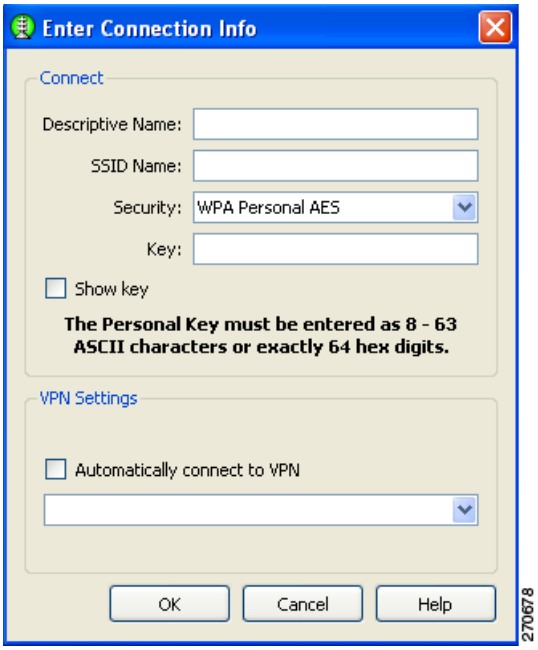
Step 4 Click **OK**. Your generated key is copied to the Enter Connection Info window **Key** text box.

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. The WPA Personal and WPA2 Personal security types supported by SSC are listed below:

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

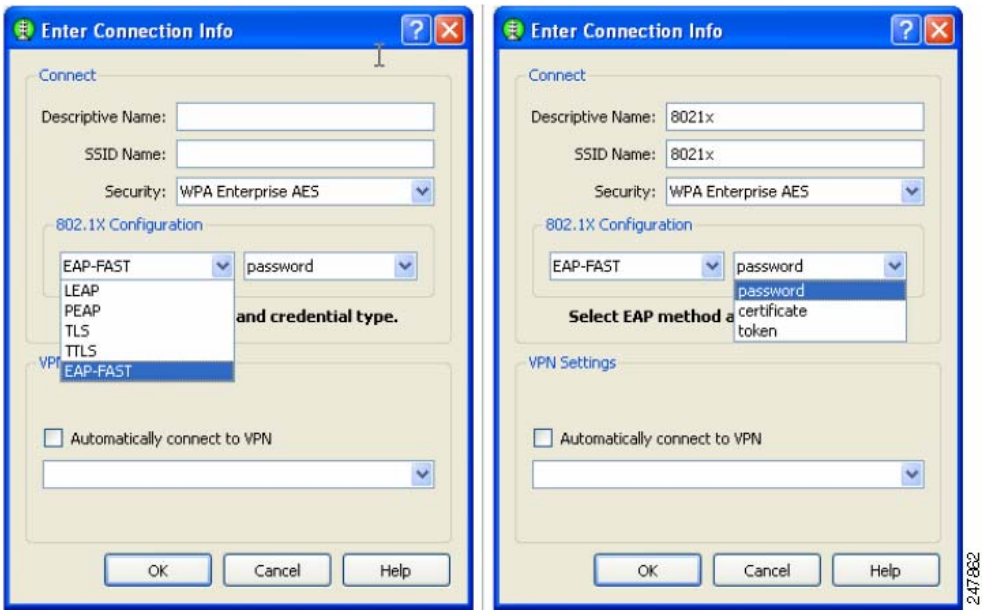
Figure 2-5 WPA Personal or WPA2 Personal Information



Configuring an 802.1X Connection

When the user selects a network with 802.1X security from the scan list, the user needs to select the EAP method and the type of credentials that is used (see Figure 2-6).

Figure 2-6 802.1X Security Information



SSC supports these 802.1X security types:

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

The user needs to click the EAP method drop-down arrow and choose one of these SSC supported EAP methods:

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

The user needs to click the credential type drop-down arrow and choose one of these SSC supported credential types:

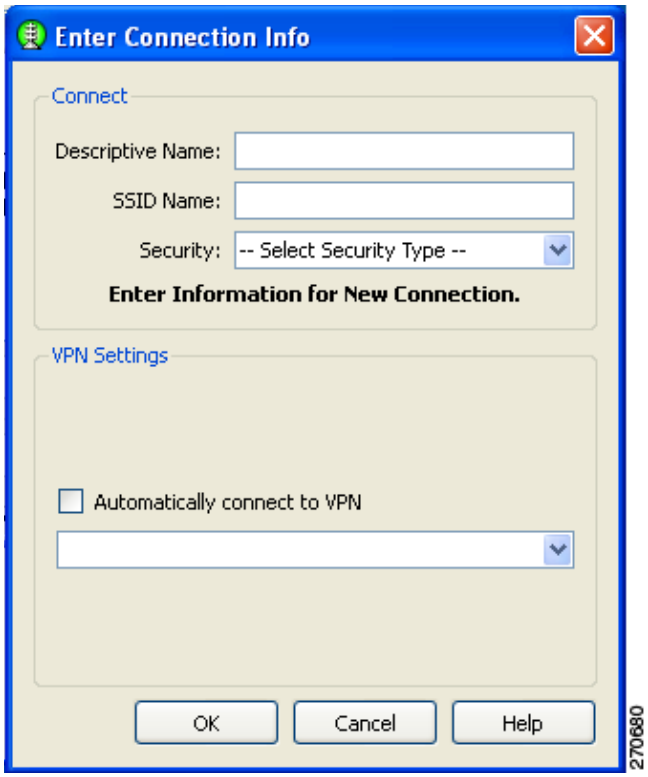
- Static password
- Certificate
- Token

Note SSC provides minimal configurability options for 802.1X connections. For deployment purposes, profiles should be created using the SSC management Utility.

Configuring a New Connection Using the Add SSID Button

When the user clicks the Add SSID button, Figure 2-7 appears.

Figure 2-7 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 it's beacon.
3. Security—Specifies the type of security authentication used by the connection (see the "SSC Supported Security Options" section on page 2-6.
4. VPN—Specifies the VPN connection options (see the "Configuring VPN Connection Options" section on page 2-7).

Managing Configured Connections

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

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

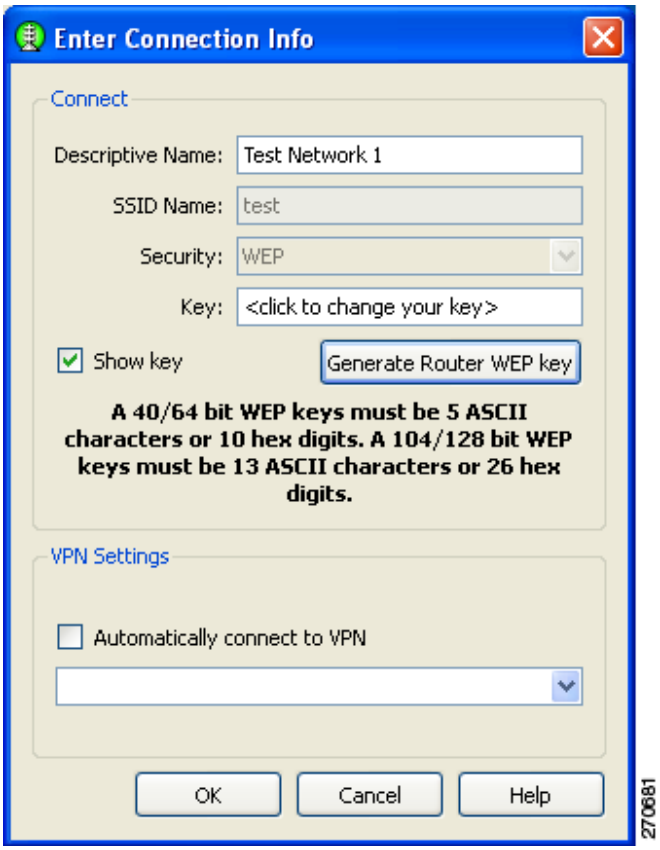
To delete a user created configuration connection, the user needs to right-click the desired configuration connection and choose the Delete option.

Editing a User-Created Configured Connection

The main SSCGUI page provides these edit options for user created configured connections:

- Right-click the desired configured connection and choose the Edit option. Figure 2-8 appears.
- Highlight the desired configured connection and click the Edit button. Figure 2-8 appears.

Figure 2-8 Configured Connection Profile Fields



The user can edit these connection profile fields:

- Descriptive Name
- Key (when applicable)

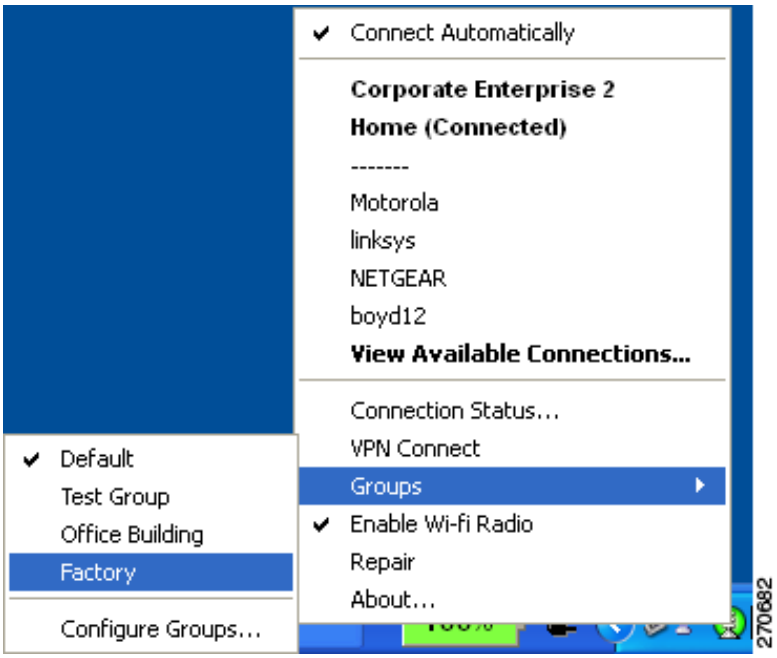
Note To change the security mode of the connection, the user must first delete the connection and then recreate the connection using a new security option.

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 2-8).
  - 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 page (see Figure 2-10).
  - On the main SSC GUI page, click Groups and choose the desired group.

Figure 2-9 SSC Tray Icon Right- Click Menu



Changing the active group causes SSC to perform these operations:

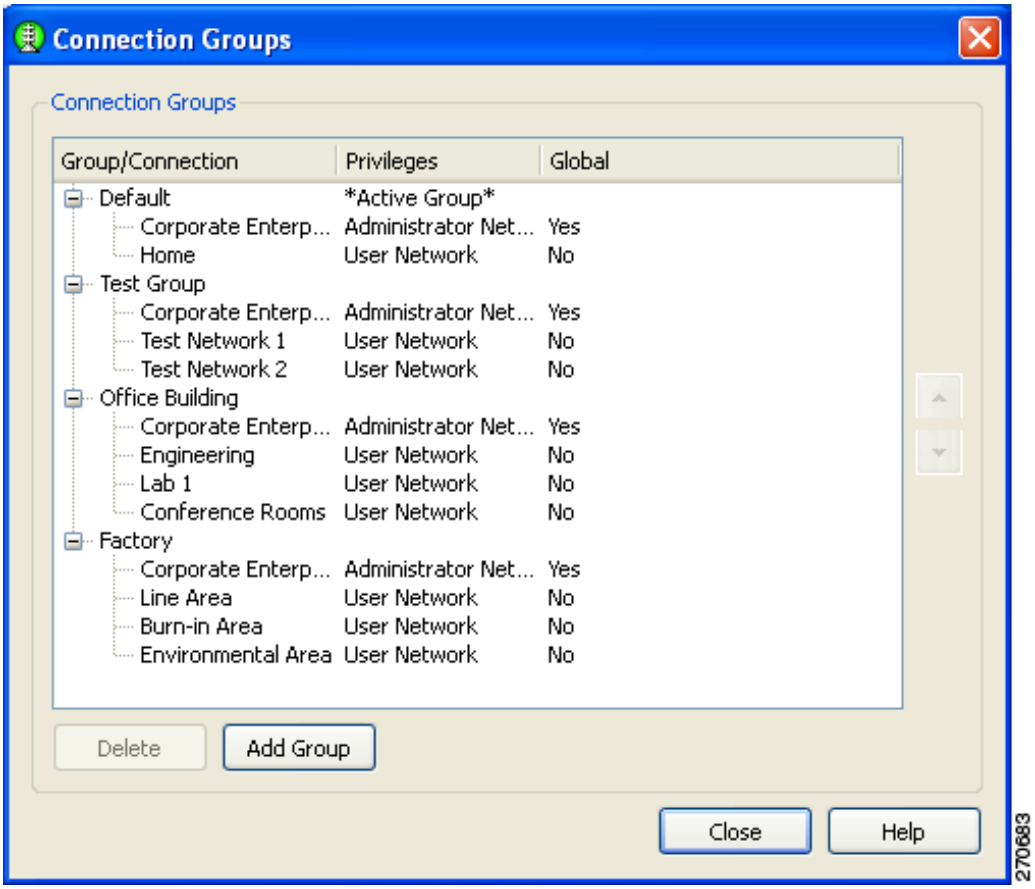
- Drops any active connection from the current group.
- Cancels exclusive connect mode if active.
- Starts the automatic connection process from the top of new group's connection list.

Managing Network Connection Groups

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

- From the main SSC GUI page, click ***Groups*** > **Configure Groups** and Figure 2-10 appears.
- Right-click the SSC tray icon, scroll to Groups and choose Configure Groups. Figure 2-10 appears.

Figure 2-10 Connection Groups Page



From the Connection Groups page, 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, or to obtain SSC version information.

Settings Menu

When the user clicks **Setting**s, a drop-down list appears (see Figure 2-11).

Figure 2-11 Settings Menu Options

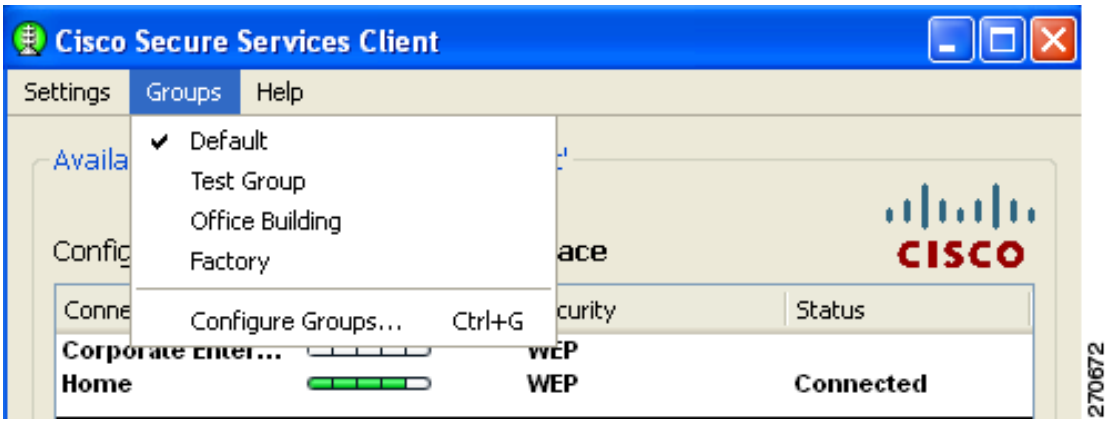
The Settings menu contains these options:

- 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 WiFi 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 2-12).

Figure 2-12 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 2-14.

Help Menu

When the user clicks **Help**, a drop-down menu appears (see Figure 2-13).

Figure 2-13 Help Menu Options

The Help menu provides 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 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 system notification tray icons are explained in the following table (Table 2-2):

Table 2-2 System Notification Tray Icons

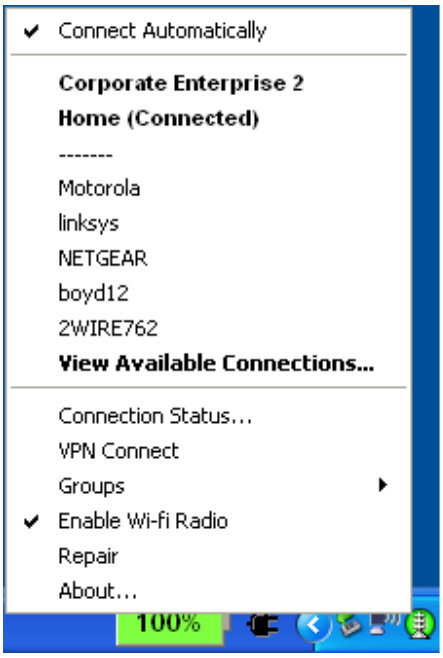
Tray Icon	Description
	Wireless—Secured connection.
	Wireless—Secured, VPN connected state.
	Wireless—Unsecured, open connection.
	Wireless—Unsecured, VPN connected state.
	Wired—Secured connection.
	Wired—Secured, VPN connected state.
	Wired—Unsecured, open connection.
	Wired—Unsecured, VPN connected state.
	Serious client error.

Note A blue background with a dashed line indicates an unsecured, open connection. A green background with a solid border indicates a secured connection. The lock indicates a VPN connected state. An animated state (pulsing lines radiating out from center) indicates the client is trying to make a connection.

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 page.
- Right-click the SSC tray icon to activate the icon menu (see Figure 2-14).

Figure 2-14 SSC Icon Right-Click Menu



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

- Connect Automatically—Indicates the operating mode of SSC.
  - When checked, this indicates SSC automatically chooses the best available configured connection.
  - When unchecked, this indicates 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, this indicates 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), this indicates 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 entering 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 clicked, the Connection Status page appears and provides connection, security, and Wi-Fi setting information.The user can click the Help button on the Connection Status page to obtain information about the page elements and values.
- Connect VPN—Allows the user to enable an automatic VPN connection.
  - When clicked, the VPN Settings page appears to allow 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 clicked, the Connection Groups page appears to display a list of configured connection groups. The user can click the Help button on the Connection Groups page to obtain information about the page elements and values
- Enable Wifi 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.