Cisco Secure Services Client: Manage your Mobile Devices Security

With an exploding number of Wi-Fi mobile devices to manage, businesses are facing multiple challenges that range from device provisioning to access security, while at the same time having to ensure a consistent and simple user experience.

Management remains a key element of cost of ownership, and IT organizations are now looking for solutions that will help them centrally and easily provision mobile devices with user access profiles.

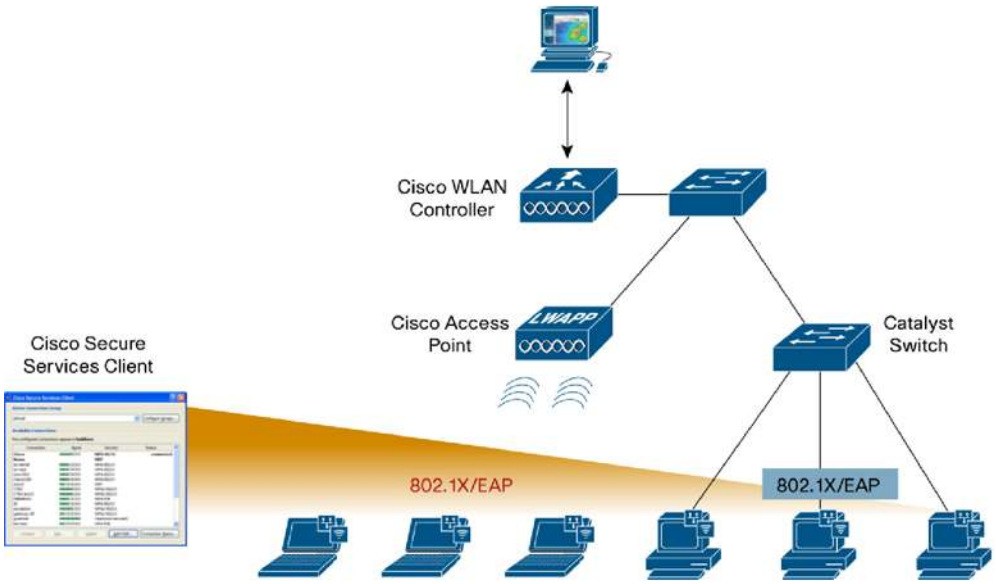
Just as important, the number of noncorporate networks made available to mobile device users, (such as home networks, hotspots, or any neighboring wireless networks that the Wi-Fi device may decide to associate with) calls for specific solutions capable of automatically ensuring secured access in all situations in which mobile devices are used in the day of a mobile worker.

Solution Overview

With Cisco® Secure Services Client Version 5.1, companies can now have a flexible, secure solution that will ease the burden of logging into wired and wireless networks and will improve employee productivity, whether they are in the office, at home, or at a local hotspot.

The Cisco Secure Services Client is a software supplicant that enables businesses to deploy a single authentication framework to access both wired and wireless networks. The software client manages the user and device identity and the network access protocols required for secure access. The client optimizes the user experience when connecting to a Cisco Unified Wired and Wireless Network. The sample customer topology in Figure 1 shows how the Cisco Secure Services Client is used across the Cisco Unified Wireless Network.

Figure 1. Cisco Secure Services Network Topology



New Features

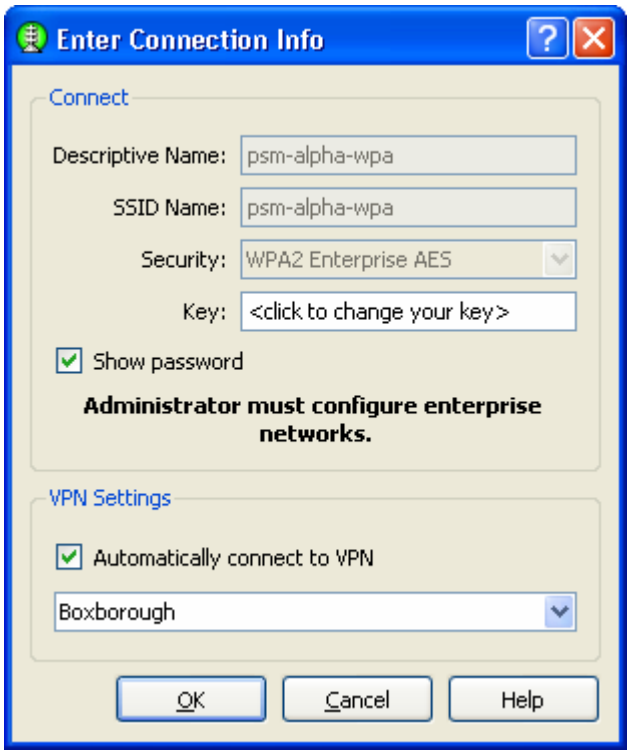
Cisco has added the following new features to enhance both the end user and IT administrator's experience.

Integrated Cisco IPSec VPN

The SSC can now be configured to automatically start the Cisco IPSec VPN. This improves the end user experience by initiating the VPN application automatically upon establishment of a successful network connection without additional user intervention. The feature is accessible by the end user via the GUI (Figure 2), or the IT administrator can select this option in the XML file for enterprisewide deployment. In addition, SSC on Windows 2000 and XP can also automatically initiate the Secure Computing SofToken II application without additional user intervention to obtain the user's one-time password.

Using the integrated Cisco IPSec VPN on Windows XP requires that the end station have version 4.8 of the IPSec VPN preinstalled. Using the integrated Cisco IPSec VPN on Windows Vista requires that the end station have version 5.0.03.0560 of the IPSec VPN preinstalled.

Figure 2. The Cisco SSC Automatic VPN Connection Setting



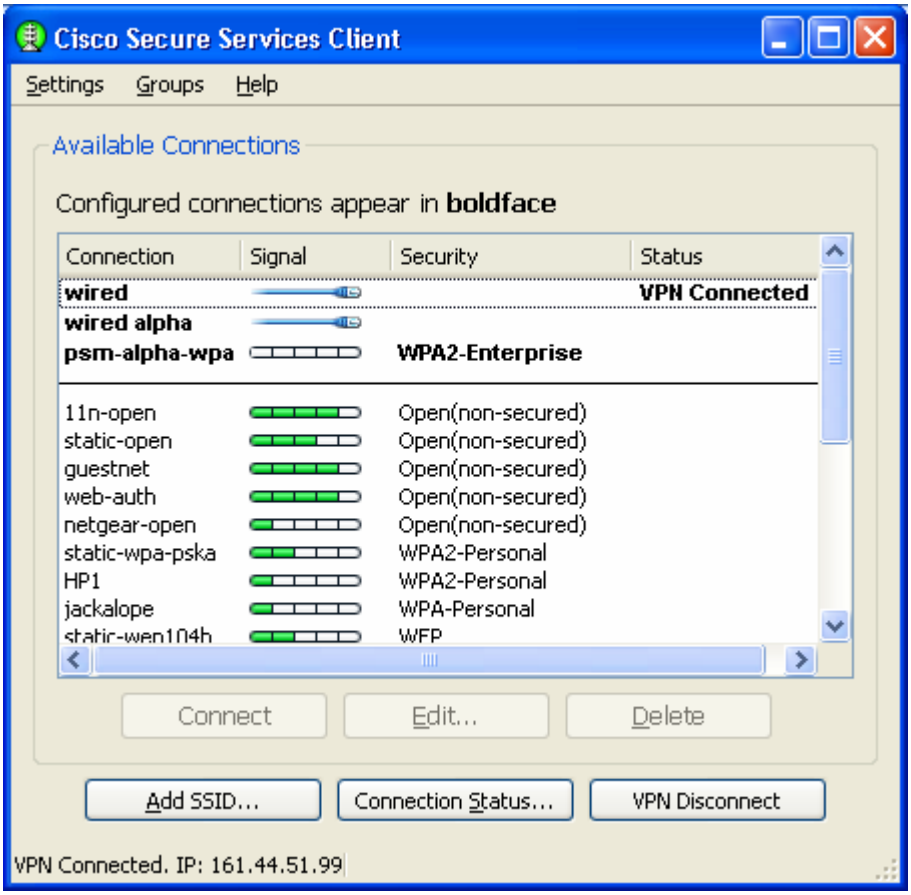
Support for FIPS 140-2 Level 1

The SSC on Windows XP has been certified by NIST for Federal Information Processing Standards (FIPS) 140-2 Level 1. When ordered with the FIPS drivers (AIR-SSCFIPS-DRV), the Windows XP version of the SSC and the drivers combine to create the SSC FIPS solution. The FIPS drivers run on most major Wi-Fi chipset manufacturers.

Simple User Interface

The new graphical user interface provides a convenient “two-click connect” to office, home, and public wired and wireless networks. This allows end users to connect to the network more easily and eliminates the security concerns of connecting to any open SSID. The user interface provides a comprehensive range of features and is accessible by right-clicking the taskbar icon or using the desktop icon. End users can view the connection status indicator for network name, strength, connection status, and IP address (Figure 3).

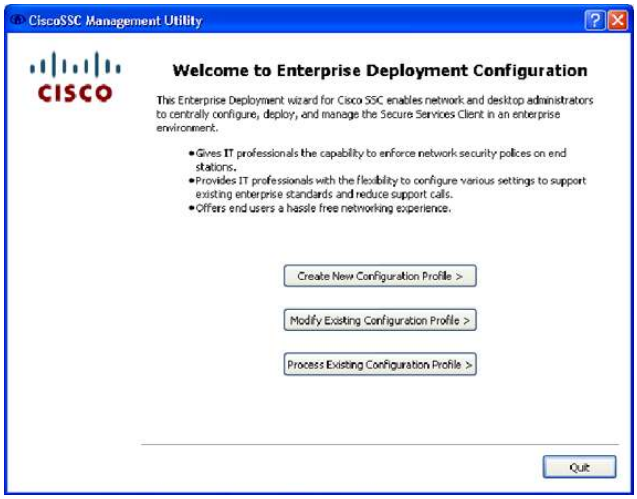
Figure 3. The Cisco SSC Interface: Viewing Connection Status Information



Enterprise Deployment

The Enterprise Deployment feature allows IT administrators to configure, automate, and deploy user profiles through a single XML file or the management utility supplied by Cisco. The management utility (Figure 4) steps the IT administrator through the policy and configuration settings for users, devices, and networks. This reduces the time and cost associated with deploying the clients to end users.

Figure 4. The Cisco SSC Management Utility



Filtering Unwanted Service Set Identifiers

The ability to filter unwanted Service Set Identifier (SSID) networks also gives IT administrators more control. This feature is useful in an environment where there are multiple wireless networks. For example, an IT administrator may want to prevent employees from receiving wireless signals from public or residential networks in an apartment building that is adjacent to the office. In this scenario, the IT administrator can configure separate SSID groups for the office and home. This is advantageous for the end user as well, who will benefit from viewing fewer networks.

Enforcing Wired Access

During the configuration process, IT administrators can also enforce wired access when the software client is configured in automatic mode. This eliminates bridging or packet data storms between wired and wireless networks. In the event that an end user desires wireless access, they can override this setting by using the manual mode.

Business Benefits

The latest Cisco Secure Services Client enhancements provide the following critical benefits for end users and IT administrators:

- **Improved user experience**
  - Allows employees to connect to office, home, and public networks more easily
  - Improves employee productivity
  - Reduces operating expenses of the IT help desk with a lower number of support calls
- **Enhanced security**
  - Enforces corporate compliance across all wired and wireless endpoint devices
  - Prevents users from changing corporate configurations and minimizes the number or support calls for restoring access
- **Centralized management**
  - Provides a consistent administrator experience with centralized management
  - Automates management with an editable XML file for scripting

Summary

The Cisco Secure Services Client delivers a unified, end-to-end security framework across the Cisco Unified Wired and Wireless Network and supports new features that benefit both IT administrators and end users. The client now provides an improved user experience, enhanced security, integrated VPN, FIPS support, and support for centralized management.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C02-423166-01 10/08