CHAPTER 5

Troubleshooting End User Wireless Networks

This chapter provides troubleshooting suggestions for typical user problems and contains these sections:

Using the Cisco SSC Simplified User Interface

SSC is designed to eliminate the chances of an end user corrupting the 802.1X configurations that have been deployed by an administrator. Users cannot edit the deployed configuration profiles. Also, the 802.1X wireless configurations are validated and tested prior to deployment mis-configured 802.1X settings are unlikely.

The SSC GUI also helps to minimize the possibility of end user errors with manual entries. Home networks can be created by simply double-clicking the detected home SSID (network name) or by selecting it from the SSC tray icon. Where the user is required to provide a WEP key for home networks, the key entry can be unmasked to allow easy visual verification.

By minimizing the user interface and hiding unneeded 802.1X information from the end user, SSC helps the user to easily diagnose wireless connection settings:

- The signal strength can quickly indicate if the user's PC is located within range of the wireless network (if the SSID is not hidden).
- The user can quickly connect to a specific network profile by right-clicking the profile and choosing **Connect Exclusively**.
- The user can determine if the error is caused by incorrect credentials.
- If authentication fails, the user can right-click on the SSC system tray icon and choose **Connection Status** to view connection information to verify the settings.
- To fix a wireless association that was previously working, the user can right-click the SSC system tray icon and choose **Repair**.
- The user can click the Microsoft wireless network connection icon in the system tray, then right-click the desired wireless network connection, and choose **Repair** to have Windows attempt to fix a wireless association that was previously working.

- The user can turn the Wi-Fi radio off and on by right-clicking the SSC system tray icon and choosing **Enable Wi-Fi Radio**. The check mark indicates the radio is turned on.
- The user can use the SSC Help menu to obtain usage information.
- The user should ensure that the latest wireless NIC (radio) driver for the operating system is loaded on the PC.

When the user is unable to resolve the network problem after following the self-help options listed above, it might be necessary to contact the support help desk to resolve the problem.

When a help desk call is generated the user might report one of the following problems:

- Association Failure—See the "Association Failure" section on page 5-2.
- Authentication Failure—See the "Authentication Failure" section on page 5-4.
- IP Connectivity Failure—See the "IP Connectivity Failure" section on page 5-5.

Association Failure

This section describes two association problems that might be experienced by a typical user.

Example 1 - Unable to Connect to the Home Access Point

The user cannot configure SSC to use his home access point. In a home environment, the user might be using one of these association modes:

- Open with no security
- Open with static WEP key
- Shared with static WEP key
- WPA Personal (PSK) with TKIP (passphrase based)
- WPA Personal (PSK) with AES (passphrase based)
- WPA2 Personal (PSK) with TKIP (passphrase based)
- WPA2 Personal (PSK) with AES (passphrase based)

The support help desk should be able to assist in correcting the problem and might ask the user to follow these operations:

1. Power off all wireless network components and wait for 3 minutes. Power up each network component in the sequence shown below but wait for the component to completely power up before powering up the next component:
   a. Modem (cable, DSL, or satellite)
   b. Router
   c. Access point
   d. PC

Note The user's home network might contain a wireless router instead of a separate access point. The wireless router is a router with an integrated access point.

2. Verify that the wireless connection can be established.

3. If the wireless connection is unsuccessful and the user knows the access point IP address, verify that the client profile settings match the access point's settings. This might be accomplished by one of these methods:
   a. Directly connect to the Ethernet port of the access point and browse to the access point's GUI.
   b. If the user has a wired or wireless router with Ethernet ports, connect to an Ethernet port and browse to the access point's web window to verify the access point's settings.
4. If the wireless connection is unsuccessful and the user doesn't know the access point IP address, verify that the client profile's settings match the access point's settings using this method:
   a. Disable the SSC by clicking **Settings > Enable Client**. A check mark indicates that SSC is enabled.
   b. Use the previously configured client (in most cases it is the Windows native client).
   c. If the access point connection is successful, the user can access the access point's web window to verify the access point's settings.
5. If the user has documented the access point configuration, the user might be experiencing one of these common problems:
   - Open or Shared mode of 802.11 authentication with WEP keys.

     The user might have mis-configured the client using *Open WEP* instead of *Shared WEP* or vice versa. The user can toggle the settings using SSC to try the other mode.
   - Incorrect WEP key generation or incorrect manual input.

     Some access points use a passphrase to generate a WEP key. The user should highlight the connection and click **Edit > Generate Router WEP key** and provide the passphrase to generate the correct WEP key.

     If a passphrase is not used, the user should highlight the connection in the SSC GUI, click **Edit,** and check **Show password** to visually verify the password entered.
   - Incorrect WPA/WPA2 passphrase manual input.

     The user might have forgotten the password because the previously used client application was caching the credentials. The user might need to reconfigure the access point's settings with a new password (see Steps 3 and 4 above).
   - Mismatching WEP key index.

     Some access points provide multiple key indices in which the WEP key can be configured. Cisco recommends that the first key index be configured with the static WEP key. The user might need to reconfigure the access point's WEP key setting (see Steps 3 and 4 above).
   - MAC filtering enabled on access point.

     If the user's PC has multiple wireless network adapters installed and enabled, SSC might be using a wireless network adapter that is being blocked by the MAC filter settings on the access point. The user might need to reconfigure the access point's settings (see Steps 3 and 4 above).

If the user is still unable to successfully connect to the access point, the user should reset the access point to factory defaults and then re-configure the access point's settings.

Example 2 - Unable to Connect to the Enterprise Network

The user cannot connect to the enterprise network using a wireless connection in a cube, conference room, or office building.

The network administrator deploys pre-configured configuration profiles within an enterprise. There are two main reasons for an 802.11 association failure in an enterprise environment:

1. Lack of wireless coverage or excessive wireless noise.

   This may happen when the wireless deployment is not well designed or because of noisy spectrum due to other devices in the environment that may even include microwave ovens.

2. Use of obsolete wireless NIC drivers.

   Wireless networks have been around for a long time and it is very likely that the user's PC has an old version of the wireless NIC driver. It is recommended that the network administrator redistribute known good NIC drivers for the NIC driver chipsets within his enterprise environment to all users.

Authentication Failure

In an enterprise environment in which the 802.1X configuration is correctly deployed with SSC and the network infrastructure components (including the access points, controllers, and the RADIUS server) are correctly configured, these problems might cause an authentication failure:

- The user provided incorrect credentials.
- The user unknowingly provided incorrect credentials a set number of times, locking his account and making it unable to work with the correct credentials.
- The user credentials have expired.
- The network infrastructure, public key infrastructure (PKI), or the user database has a problem: an access point cannot communicate to the authentication server, the authentication server is not functioning, or its configuration has changed.
- The device involved in the authentication process is not functioning properly, such as the smart card, smart card reader, or token, etc.
- The user's PC does not have Windows Internet Explorer 5.0 or later installed.

If the problem continues, the support help desk should request that the user provide a Cisco Support Report with packet capturing enabled. For instructions on creating the support report, see the "Gathering Logs and Packet Traces" section on page 5-8.

IP Connectivity Failure

When the 802.1X authentication is successful, SSC tries to get a valid IP address. In some networks, it might take up to 40 seconds to renew the IP address. If the wireless LAN adapter fails to receive a valid IP address, these actions might help to resolve the problem or identify the cause:

- Disable and then enable the wireless NIC adapter.
- Repair the connection by right-clicking the SSC system tray icon and choosing **Repair**.
- Right-click the network connection in the SSC GUI and choose **Connect Exclusively**.
- Use network tools, such as ARP, ping, and ipconfig to check Layer 2 or Layer 3 connection status, and availability of an IP address.

The root cause of the problem might be as simple as a DHCP server running out of available IP addresses.

Integrated VPN Connection Failure

SSC allows the user to automatically establish a VPN connection after connecting to a wireless profile, if the profile is configured to do so.

The end user might be unable to establish a VPN tunnel to his enterprise network using SSC. VPN problems might be indicated as follows:

- The SSC VPN Connect button is not visible on the SSC main window.

  This might happen if the administrator did not deploy a profile with the *Allow VPN* option checked to the user.

- The SSC VPN Connect button is visible but dimmed.

  This might happen if the Cisco VPN client version is older than 4.8. The user must upgrade the VPN client on his PC.

- The user cannot access the VPN service.

  This may happen if the user is using the stand-alone Cisco VPN client interface to establish VPN connections. If the Cisco VPN client interface is being used to connect and disconnect VPN connections, SSC gives up control over VPN functionality.

  To resolve this problem, the user should not use the standalone Cisco VPN client interface to establish a connection. He should allow SSC to establish the VPN connection. However, if desired, he can use the Cisco VPN client interface to see the connection status.

- SSC displays a VPN connection failed error.

  This might happen when the user credentials provided to SSC are incorrect. When using SSC with the Soft Token option, the user credentials to be provided to SSC must be the username and the user PIN that were previously provided to the SofToken-II application.

Note For Windows 2000 and Windows XP, the unique soft-token password generated by the SofToken II application must NOT be provided to SSC when prompted for the VPN username and PIN.

Note For Windows Vista, Secure Computing SofToken II is not supported. When SofToken II authentication is specified in the network configuration and SSC prompts for the username and password, the username and the unique one-time password must be entered. This is different from Windows 2000 and Windows XP where the SoftToken II application password is entered.

If the VPN problem continues, a Cisco support report should be provided to the support help desk to analyze the problem and determine the root cause of the problem (see the "Gathering Logs and Packet Traces" section on page 5-8).

Co-Existence with Other Wireless Client Managers

To enable the Cisco Aironet Client Utility (ACU) to coexist with SSC, the user must configure the wireless network adapter to allow Windows to configure the adapter. The user must follow these steps to configure the wireless network adapter:

Step 1 Right-click **My Networks** on the desktop.

Step 2 Right-click the wireless network adapter and choose **Properties**.

Step 3 Click **Wireless Networks** and check **Use Windows to configure my wireless network settings**.

Step 4 Click **OK** and close the Network Connections window.

To enable the Cisco Aironet Desktop Utility (ADU) to coexist with SSC, the user must configure the ADU to allow SSC to control the adapter.

Note It might be necessary for the user to download the latest ADU version from the Cisco Software Center at this URL: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875243

The user must click **Client Adapters and Client Software** and follow the prompts. The user must register or be a registered user of Cisco.com to download software.

The user must follow these steps to configure the ADU:

Step 1 Open the ADU by double-clicking the ADU task bar icon.

Step 2 Click **Options > Select Client Software** and the Select Client Software pop-up window appears.

Step 3 Check **Third-Party Tool** and click **OK** on the pop-up window.

Step 4 When the Client Software selection pop-up indicates successful, click **OK**.

Step 5 Close the ADU.

When SSC is active, it takes control from the Microsoft Windows native wireless client. In other words, the Windows native client can display SSID's but cannot configure or set wireless connection settings. To stop SSC from controlling the wireless adapter, the user must disable SSC by clicking **Settings** and choosing **Enable Client** (a check indicates SSC is enabled). Disabling SSC gives control of the wireless adapter to any other wireless client management application that can manage the wireless connections.

Note SSC and the Odyssey Access Client Manager application must not be installed at the same time on a user's PC.

The iPassConnect client software and SSC can co-exist if the following instructions are carried out when the user is using a public Wi-Fi hotspot (such as an airport).

Step 1 Right-click the SSC tray icon and choose the name of the Wi-Fi connection.

Step 2 When the SSC icon turns blue and is no longer animated, you need to activate the iPassConnect application and use it to authenticate yourself and to successfully establish a VPN connection.

Step 3 In iPassConnect choose **Available Connections** and then choose the name of the connection that you are already connected to with SSC.

Step 4 iPassConnect prompts you for your username and password. Enter your corporate network username and then use your soft token application to generate the password.

Step 5 iPassConnect finishes authenticating and launches the Cisco VPN application. At this point you should exit the Cisco VPN application, right-click the SSC icon, and choose **Connect VPN**.

Note Typically the webauth systems available at most hot spots keep you authenticated for over an hour. If you lose your connection, you must connect again. Right-click the SSC icon and choose **Connect VPN** when available. If you don't succeed the first time, try choosing **Connect VPN** again another couple of times. If that doesn't work, launch a web window and see if you have connectivity to the internet or if the web window requests that you authenticate yourself. If the web window is asking for authentication information, you need to repeat the iPassConnect steps starting with Step 4.

Gathering Logs and Packet Traces

SSC provides a diagnostic utility called the *Log Packager,* which is part of the Cisco Client Utilities. Installed separately, this utility is available from the Windows Start > Programs menu. The utility provides SSC's current status, interface and driver details, FIPS status, and wireless LAN information (SSIDs detected, association status, etc.). This information can be useful in diagnosing connectivity problems when using SSC and the NIC adapter.

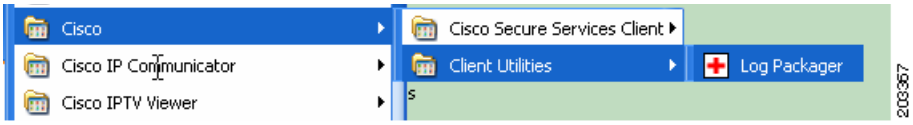
Note When using Windows Vista, the Log Packager does not include a scan list in the report.

Creating the Cisco Support Report for SSC

To create the Cisco support report, follow these steps:

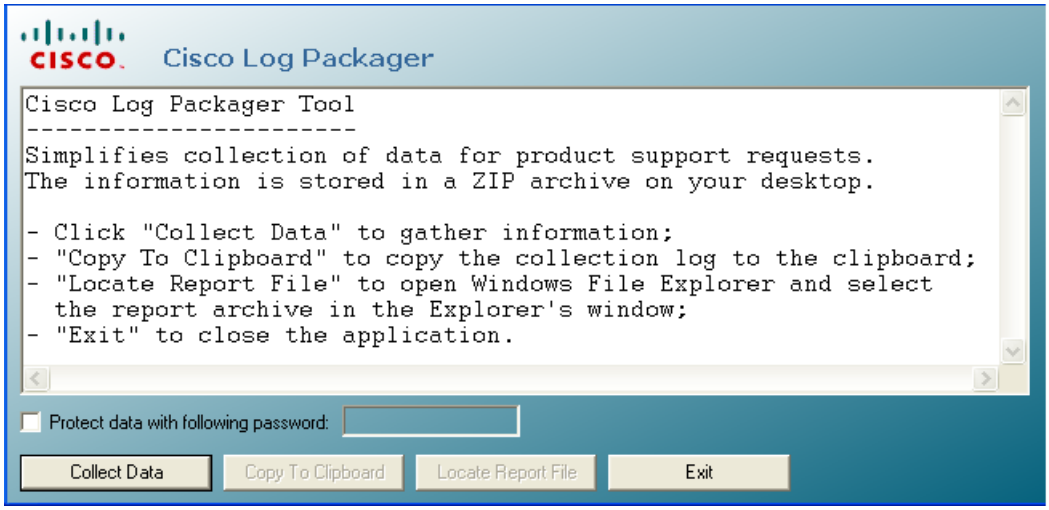
Step 1 Click **Start > All Programs > Cisco > Client Utilities > Log Packager** (see Figure 5-1).

Figure 5-1 Accessing the Client Utility Using Windows Program Menu



When the Log Packager program opens, Figure 5-2 appears.

Figure 5-2 Log Packager Window



Step 2 Click **Collect Data**.

Step 3 When the buttons are visible again, click **Locate Report File**. A Microsoft Explorer window opens in the directory with the zipped report file. The filename is CiscoSupportReport.zip and is located on your PC desktop. The zip file contains a number of log files, capture files, several .xslt files, and several configuration .xml files.

If you click **Copy to Clipboard**, the contents of the CiscoSupportReportLog.txt file is copied to the Windows clipboard.

Step 4 Close Windows Explorer and the Cisco Log Packager.