LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product. The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC website. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an “Active” SMC product. A product is considered to be “Active” while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an “Active” SMC product. A list of discontinued products with their respective dates of discontinuance can be found at: http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product. Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer’s expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER’S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC’S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER’S OR ANY THIRD PERSON’S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL,
CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.
Compliances

Federal Communication Commission Interference Statement
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
• Reorient or relocate the receiving antenna.
• Increase the distance between the equipment and receiver.
• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
• Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Mark Declaration of Conformance for EMI and Safety (EEC)
This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following references have been applied in order to prove presumption of compliance with the R&TTE Directive 1999/5/EC:
• EN 300 328
• EN 301 489-1
• EN 301 489-17
• EN 60950-1

A copy of the CE Declaration of Conformity is available for download at: http://www.smc.com

Intended for indoor use in the following countries:

AT, BE, CZ, CY, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LT, LU, MT, NL, NO, PL, PT, SI, SK, ES, SE, CH, UK.
Table of Contents

Chapter 1 – Wireless LAN Networking
  Transmission Rate 5
  Type of Wireless Networks 5
    Ad-Hoc (IBSS) Network 5
    Infrastructure (BSS) Network 6
  Wireless LAN Security 9
  Data Encryption with WEP 10

Chapter 2 - Getting Started
  About Your Draft 11n Wireless USB2.0 Adapter 11
  Package Content 11
  System Requirement 12
  LED Definition 12
  Wireless Utility and Adapter Hardware Installation 12
  Using the Utility to Configure Your Network 16
    Link Information 16
    Site Survey 18
    Profile 19
    WPS 23

Chapter 3 – Maintenance
  Uninstalling the Driver 28
  Uninstall the Client Utility 28
  Upgrading the Wireless Utility 28

Glossary 29
Chapter 1- Wireless LAN Networking

This section provides background information on wireless LAN networking technology.

---

**CAUTION**

THE INFORMATION IN THIS SECTION IS FOR YOUR REFERENCE. CHANGING NETWORK SETTINGS AND PARTICULARLY SECURITY SETTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

---

Transmission Rate (Transfer Rate)

The adapter provides various transmission (data) rate options for you to select. In most networking scenarios, the factory default Fully Auto setting proves the most efficient. This setting allows your adapter to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the adapter automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the adapter gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

Types of Wireless Networks

Wireless LAN networking works in either of the two modes: ad-hoc and infrastructure. In infrastructure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSSs in the same subnet. In ad hoc mode (also known as peer-to-peer mode), wireless devices communicate with each other directly and do not use an access point. This is an Independent BSS (IBSS).

To connect to a wired network within a coverage area using access points, set the adapter operation mode to Infrastructure (BSS). To set up an independent wireless workgroup without an access point, use Ad-hoc (IBSS) mode.

**Ad-Hoc (IBSS) Network**

Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

To set up an ad-hoc network, configure all the stations in ad-hoc mode. Use the same SSID and channel for each.
When a number of wireless stations are connected using a single access point, you have a Basic Service Set (BSS).
In the ESS diagram below, communication is done through the access points, which relay data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resources, such as a printer, on the wired network.
In an ESS environment, users are able to move from one access point to another without losing the connection. In the diagram below, when the user moves from BSS (1) to BSS (2) the adapter automatically switches to the channel used in BSS (2).
**WIRELESS LAN SECURITY**

Because wireless networks are not as secure as wired networks, it’s vital that security settings are clearly understood and applied.

The list below shows the possible wireless security levels on your adapter starting with the most secure. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. EAP requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or the LAN to provide authentication service for wireless stations.

1. Wi-Fi Protected Access (WPA)
2. IEEE802.1X EAP with RADIUS Server authentication
3. WEP Encryption
4. Unique ESSID
DATA

CAUTION

DO NOT ATTEMPT TO CONFIGURE OR CHANGE SECURITY SETTINGS FOR A NETWORK WITHOUT AUTHORIZATION AND WITHOUT CLEARLY UNDERSTANDING THE SETTINGS YOU ARE APPLYING. WITH POOR SECURITY SETTINGS, SENSITIVE DATA YOU SEND CAN BE SEEN BY OTHERS.

ENCRYPTION WITH WEP

The WEP (Wired Equivalent Privacy) security protocol is an encryption method designed to try to make wireless networks as secure as wired networks. WEP encryption scrambles all data packets transmitted between the adapter and the access point or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your adapter.

- Automatic WEP key generation based on a password phrase called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.

- For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the Security Settings screen of the wireless utility and entering them manually as the WEP keys in the other WLAN adapter(s).

The adapter allows you to configure up to four WEP keys and only one key is used as the default transmit key at any one time.

THE ADAPTER SUPPORTS UP TO FOUR 64-BIT OR 128-BIT WEP KEYS.
Chapter 2 - Getting Started

2.1 About Your Draft 11n Wireless USB2.0 Adapter

The EZ Connect™ N Draft 11n Wireless USB2.0 Adapter (SMCWUSB-N) is another cutting edge introduction in 2.4GHz wireless communication for desktop and notebook computers. Designed for both the home and office, this wireless USB2.0 adapter provides the speed, coverage and security expected by today's wireless users. The SMCWUSB-N is 802.11n draft v2.0 compliant while maintaining full backwards compatibility with the Wireless-G (802.11g) and Wireless-B (802.11b) standards. This next generation standard utilizes advanced MIMO (Multiple-In, Multiple-Out) technology to deliver incredible speed and range. With wireless speeds up to 300Mbps and extended coverage, there is enough bandwidth to simultaneously stream video and audio, play online games, transfer large files, make VoIP calls and surf the Internet. With security being a key consideration, SMCWUSB-N supports the latest WPA and WPA2 wireless encryption standards, which prevent unauthorized access to wireless networks and ensure data is secure. Wireless security can also be set up easily using Wi-Fi Protected Setup™ (WPS) that enables push button or PIN configuration. The SMCWUSB-N includes an easy installation wizard which guides you step-by-step through the process. Once installed the WLAN utility allows you to scan for available wireless networks and manage multiple network profiles so connecting becomes instantaneous.

The following lists the main features:

- IEEE802.11n draft v2.0 compliant
- Wireless speeds up to 300Mbps
- Increased speeds & coverage - up to 5x the speed of 802.11g
- Fully backwards compatible with 802.11b/g wireless networks
- Stream HD video, Listen to digital music, Play online games, Transfer large files, Make VoIP calls & Surf the Internet simultaneously
- WEP 64-/128-Bit, WPA & WPA2 wireless encryption
- EZ Installation Wizard for easy installation
- Supports Windows 2000/XP/Vista
- WLAN management utility

2.2 Package Contents

- EZ Connect™ N Wireless USB 2.0 Adapter (SMCWUSB-N)
- EZ Installation Wizard & Documentation CD
2.3 System Requirements

- 2.4 GHz 802.11n draft wireless network or 2.4 GHz 802.11b/g wireless network
- Microsoft Windows 2000, XP or Vista
- A Notebook or Desktop computer with:
  - 300MHz CPU or above
  - Available USB2.0 port
  - 20MB of available hard disk space
- CD-ROM drive

2.4 LED Definition

The following table describes the LED on behavior:

<table>
<thead>
<tr>
<th>COLOR</th>
<th>STATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>OFF</td>
<td>No power</td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>Wireless connected without data traffic</td>
</tr>
<tr>
<td></td>
<td>Slow Blinking</td>
<td>Power on without wireless connection</td>
</tr>
<tr>
<td></td>
<td>Normal Blinking</td>
<td>Wireless connected with data traffic</td>
</tr>
</tbody>
</table>

2.5 Wireless Utility & Adapter Hardware Installation

**IMPORTANT: Do not plug in the EZ Connect™ N Wireless USB2.0 Adapter until instructed.**

Follow the instructions below to install the USB Adapter and Utility.

**STEP 1**
Put the EZ Installation & Documentation CD in to your CD-ROM drive. The CD will auto run.

**STEP 2**
Click [Install Driver/Utility] and follow the on-screen instructions. **Note:** During installation a “Software Installation” warning may appear, click [Continue Anyway].
**STEP 3**
The InstallShield Wizard prompts you for confirmation. Click **Next** on the following screen.

**STEP 4**
In the destination Folder screen you are asked to confirm the Destination Folder for the application software. If you would like, you may change the destination folder to another location. Click **Next**
**STEP 5**
The wizard is ready to begin installation. Click **Install** on it.

![Image of the wizard ready to install](image)

**STEP 6**
Click **Finish** to complete the client utility installation.

![Image of the wizard finishing installation](image)

**STEP 7**
After clicking [Finish] the Wizard will exit. Plug in the EZ Connect™ N Wireless USB2.0 Adapter to an available USB port. The “Found New Hardware Wizard” will appear. Click [No, not this time], then [Next].

![Image of the EZ Connect™ N Wireless USB2.0 Adapter](image)
**STEP 8**  
Click [Install the software automatically (Recommended)], then click [Next]. A “Hardware Installation” warning may appear, click [Continue Anyway].

**STEP 9**  
Click [Finish] to complete the Driver/Utility installation.
2.6 Using the Utility to Configure Your Network

The following are explanations on how to configure and use the Utility program. After completing the installation procedure, a new icon as shown below will automatically appear in the lower right tray bar.

![Wireless Client Utility Icon]

Hold your mouse pointer over the icon, and press the right mouse button to open the Wireless Client Utility.

The Wireless Client Utility window as shown below will appear.

![Wireless Client Utility Window]

The user can now use any of the management functions available in the IEEE 802.11 Wireless Client Utility.

2.6.1 Link Information

Click the Link Information tab to see general information about the program and its operations. The Link Information tab does not require any configuration.
The following table describes the items found on the Link Information screen.

<table>
<thead>
<tr>
<th>Wireless Network Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile Name</strong></td>
<td>The name of the current selected configuration profile. Set up the configuration name on the <strong>Profile tab</strong>.</td>
</tr>
<tr>
<td><strong>SSID</strong></td>
<td>Displays the wireless network name.</td>
</tr>
<tr>
<td><strong>Link Status</strong></td>
<td>Shows whether the station is associated to the wireless network.</td>
</tr>
<tr>
<td><strong>Network Type</strong></td>
<td>The type of network the station is connected to. The options include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Infrastructure (access point)</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Ad Hoc</strong></td>
</tr>
<tr>
<td><strong>Wireless Mode</strong></td>
<td>Displays the wireless mode: 802.11n, 11g or 11b.</td>
</tr>
<tr>
<td><strong>Channel</strong></td>
<td>Shows the currently connected channel.</td>
</tr>
<tr>
<td><strong>Transmit Rate</strong></td>
<td>Displays the current transmit rate in Mbps.</td>
</tr>
<tr>
<td><strong>AP MAC Address</strong></td>
<td>Displays the MAC address of the access point the wireless adapter is associated to.</td>
</tr>
<tr>
<td><strong>Signal Strength</strong></td>
<td>Shows the strength of the signal.</td>
</tr>
<tr>
<td><strong>Security Status</strong></td>
<td>Shows the security type – Disable, WEP, WPA/WPA2, WAP-PSK/WAP2-PSK or 802.1X</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Displays the authentication mode.</td>
</tr>
<tr>
<td><strong>TCP/IP Status</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Displays the computer's IP address.</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Displays subnet mask</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td>Displays gateway address</td>
</tr>
</tbody>
</table>
2.6.2 Site Survey

Click the Site Survey tab to see available infrastructure and ad hoc networks. On this screen, click Refresh to refresh the list at any time.

Connecting to a different network

Hold your mouse pointer over the network icon, and click the right mouse button to select the network.

Click the Connect button to connect the available network. If no configuration profile exists for that network, the Profile Settings window opens to ask to create a profile for the network. Follow the procedures to create profile for that network.
2.6.3 Profile

To add a new configuration profile, click **Add** on the Profile tab.

To modify a configuration profile, select the configuration from the Profile list and click the **Edit** button.

**Scan Available Networks**

Click the **Browse** button on the Profile Settings screen to scan for available infrastructure and ad hoc networks. On this list, click **Refresh** to refresh the list at any time.
To configure a profile for Ad-Hoc or Infrastructure mode, select the Network Type field on the Profile Settings.

Click **Next** to continue the profile setting.

To define the security mode, select the security button of the desired security mode. And then click **Next** to continue. Please see following table for details of security modes.

<table>
<thead>
<tr>
<th>WPA/WPA2</th>
<th>Enables the use of Wi-Fi Protected Access (WPA). Choosing WPA/WPA2 opens the WPA/WPA2 <strong>Security Settings</strong> screen. The options include:</th>
</tr>
</thead>
</table>
**TLS (Transport Layer Security)** is a Point-to-Point Protocol (PPP) extension supporting additional authentication methods within PPP. Transport Layer Security (TLS) provides for mutual authentication, integrity-protected cipher suite negotiation, and key exchange between two endpoints.

**PEAP (EAP-GTC) (Protected Extensible Authentication Protocol)** authenticates wireless LAN clients using only server-side digital certificates by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The tunnel then protects the subsequent user authentication exchange.

**PEAP (EAP-MSCHAP V2) (Protected Extensible Authentication Protocol)** To use PEAP (EAP-MSCHAP V2) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.

**TTLS (Tunneled Transport Layer Security)** An EAP variant that provides mutual authentication using a certificate for server authentication, and via a secure TLS tunnel for the client.

**LEAP (Lightweight and Efficient Application Protocol)** is the general framework for a set of high-performance, efficient protocols which are ideal for mobile and wireless applications. LEAP is designed to address all the technical requirements of the wireless data communications industry, and is oriented towards providing the greatest benefit to the industry and the consumer.

<table>
<thead>
<tr>
<th>WPA-PSK/WPA2-PSK</th>
<th>Enables WPA/WPA2 Passphrase security. Fill in the WPA/WPA2 Passphrase on <strong>Security Settings</strong> screen.</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x</td>
<td>Enables 802.1x security. This option requires IT administration. Choosing 802.1x opens the 802.1x <strong>Security Settings</strong> screen. The options include:</td>
</tr>
<tr>
<td></td>
<td><strong>TLS</strong></td>
</tr>
<tr>
<td></td>
<td><strong>PEAP</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TTLS</strong></td>
</tr>
<tr>
<td></td>
<td><strong>LEAP</strong></td>
</tr>
</tbody>
</table>

**Advanced Settings**

After Security Settings finished, the **Advanced Settings** screen will be shown as following.
The following table describes the items found on the Advanced Settings screen.

<table>
<thead>
<tr>
<th>Power Save Mode</th>
<th>Shows the power save mode. Power management is disabled in ad hoc mode. The options include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <strong>Continuous Access Mode</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Maximum Power Saving</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Fast Power Saving</strong></td>
</tr>
<tr>
<td>802.11b Preamble</td>
<td>Displays the 802.11b preamble format.</td>
</tr>
<tr>
<td></td>
<td>The options include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Long</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Short</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Auto</strong></td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>Value from 0 ~ 2347</td>
</tr>
<tr>
<td>FRAG Threshold</td>
<td>Value from 256 ~ 2346</td>
</tr>
<tr>
<td>Wireless Mode</td>
<td>Include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>802.11b</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>802.11g</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>802.11n</strong></td>
</tr>
</tbody>
</table>

After advance settings are finished, the following screen showed as below. You can activate the profile now or later.
2.6.4 WPS Setting

The user obtains a device password (PIN Code) from the STA and enters the password into the Registrar. Both the Enrollee and the Registrar use PIN Config method for the configuration setup. The detail indicates as follows.
1. Go to the WPS setting page, click "Refresh" button to update available WPS APs.

2. Select an AP (SSID/BSSID) that STA want join to.

3. Click "PIN" button to start PIN connection.
4. Enter PIN Code of STA into the Registrar when prompted by the Registrar.

5. The result will look like the below figure.
6. Then connect successfully. The result will look like the below figure.

![Wireless Client Utility WPS Settings](image)

**WPS Status Bar Description:**

1. A successful PIN configuration:

   Start PIN connection - SSID ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive EAP-Req (Start) ~> Sending M1 ~> Received M2 ~> (Received M2D ~> Sending EAP-Rsp (ACK)) ~> Sending M3 ~> Received M4 ~> Sending M5 ~> Received M6 ~> Sending M7 ~> Received M8 ~> Sending EAP-Rsp(Done) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

2. WPS configuration doesn't complete after two-minute connection:

   WPS Eap process failed.

3. When Errors occur within two-minute connection, the WPS status bar might report on "WPS Eap process failed".

   Error messages might be:

   1. Receive EAP with wrong NONCE.
2. Receive EAP without integrity.


4. An inappropriate EAP-FAIL received.

Chapter 3 – Maintenance

This chapter describes how to uninstall or upgrade the Wireless Utility.

3.1 Uninstall the Driver
Follow the steps below to remove (or uninstall) the USB Adapter driver from your computer.

Step 1. To remove the driver from the OS, go to Start -> Control Panel
Step 2. Double-click System
Step 3. Under Hardware tab, click Device Manager.
Step 4. Double-click Network Adapter
Step 5. Right-click mouse button on “802.11n USB Wireless Network Adapter”, and choose Uninstall
Step 6. Click OK to confirm that you are going to uninstall the driver

3.2 Uninstall the Client Utility
Follow the steps below to remove the Client Utility from your computer.

Step 1. To remove the utility from the OS, go to Start -> Control Panel
Step 2. Double-click Add-Remove Programs
Step 3. Select 802.11n Wireless Client Utility, and click the Remove button

3.3 Upgrading the Wireless Utility
To perform the upgrade, follow the steps below.

Step 1. Download the latest version of the utility from the web site and save the file on your computer.
Step 2. Follow the steps in Section 2.2 to remove the current Wireless Utility from your computer.
Step 3. Restart your computer if prompted.
Step 4. After restarting, refer to the procedure in the Chapter 2 to install the new utility.
Glossary

For unfamiliar terms used below, look for entries elsewhere in the glossary.

AD-HOC (IBSS)
Ad-hoc mode does not require an AP or a wired network. A network that transmits wireless from computer to computer without the use of a base station (access point).

Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

CHANNEL
A radio frequency used by a wireless device is called a channel.

EAP AUTHENTICATION
EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1X transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

ENCRYPTION
The reversible transformation of data from the original to a difficult-to-interpret format. Encryption is a mechanism for protecting confidentiality, integrity, and authenticity of data. It uses an encryption algorithm and one or more encryption keys.

FRAGMENTATION THRESHOLD
This is the maximum data fragment size that can be sent before the packet is fragmented into smaller packets.

IEEE 802.1X
The IEEE 802.1X standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

INFRASTRUCTURE (BSS)
When a number of wireless stations are connected using a single AP, you have a Basic Service Set (BSS).
ROAMING
In an infrastructure network, wireless stations are able to switch from one BSS to another as they move between the coverage areas. During this period, the wireless stations maintain uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate AP depending on the signal strength, network utilization among other factors.

SSID
The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)
Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server.

USER AUTHENTICATION
WPA applies IEEE 802.1X and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. If you do not have an external RADIUS server, use WPA-PSK/WPA2-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, clients will be granted access to a WLAN.

WEP
WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the WCB-321A and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

WPA/WPA2
Wi-Fi Protected Access (WPA) and WPA2 (future upgrade) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption. WPA2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
FOR TECHNICAL SUPPORT, CALL:
1300 725 323

INTERNET
E-mail addresses:  support@smc-australia.com.au

ENGLISH
Technical Support Information available at www.smc.com

FRENCH
Informations Support Technique sur www.smc.com

DEUTSCH
Technischer Support und weitere Information unter www.smc.com

SPANISH
En www.smc.com Ud. podrá encontrar la información relativa a servicios de soporte técnico

DUTCH
Technische ondersteuningsinformatie beschikbaar op www.smc.com

PORTUGUES
Informações sobre Suporte Técnico em www.smc.com

SWEDISH
Information om Teknisk Support finns tillgängligt på www.smc.com

Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:
http://www.smc-australia.com.au