SMC® Networks

USER GUIDE

EZ Connect™ N
Draft 11n Wireless USB2.0 Adapter

SMCWUSBS-N

Wireless USB Adapter User Guide

The easy way to make all your network connections

SMC®
Networks
20 Mason
Irvine, CA 92618
Phone: (949) 679-8000

October 2007
Pub. # 149100040600E
E102007-EK-R01

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

SMC Networks, Inc.
20 Mason
Irvine, CA 92618

Trademarks:

SMC is a registered trademark; and EZ Switch, TigerStack and TigerSwitch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

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 Web site. 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.

SMC Networks, Inc.
20 Mason
Irvine, CA 92618

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 of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation 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

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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Canada RSS Statement

This Class B digital apparatus complies with Canada RSS-210.

Cet appareil numérique de la classe B est conforme à la norme CNR-210 du Canada.

Canada IC Statement

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Australia/New Zealand AS/NZS 4771

N11846

Japan VCCI Class B

　この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると受信障害を引き起こすことがあります。

　取り扱い説明書に従って正しい取り扱いをして下さい。

Taiwan DGT (NCC)

根據交通部低功率管理辦法規定：

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

EC Conformance Declaration CE0682(!)

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950-1 (IEC 60950-1) - Product Safety
- EN 300 328 - Technical requirements for 2.4 GHz radio equipment
- EN 301 489-1, EN 301 489-17 - EMC requirements for radio equipment

This device is intended for use in the following European Community and EFTA countries:

- Austria
- Belgium
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United Kingdom

Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below:

- In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

Council recommendation 1999/519/EC of 12 July 1999, limitations of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)

Czech	SMC Networks tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Danish	Undertegnede *SMC Networks* erklærer herved, at følgende udstyr *Radio LAN device* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	Hiermit erklärt SMC Networks, dass sich dieses Wireless LAN Gerat in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet. Die offizielle EC-Declaration of Conformity finden Sie im Internet unter http://www.smc.com unter der entsprechenden Produktkategorie.
Estonian	Käesolevaga kinnitab SMC Networks seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, SMC Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. The official EC-Declaration of Conformity can be found under the corresponding product section on the web http://www.smc.com.
Spanish	Por medio de la presente SMC Networks declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE. The official EC-Declaration of Conformity can be found under the corresponding product section on the web http://www.smc.com.
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *SMC Networks* ΔΗΛΩΝΕΙ ΟΤΙ *Radio LAN device* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
French	Par la présente SMC Networks déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. La declaration de conformité officielle peut être trouvée sur notre site internet http://www.smc.com dans la rubrique Produits.
Italian	Con la presente SMC Networks dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian	Ar šo *SMC Networks* deklarē, ka *Radio LAN device* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian	Šiuo *SMC Networks* deklaruoja, kad šis *Radio LAN device* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Dutch	Hierbij verklaart SMC Networks dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Het officiële EC- gelijkvormigheidattest kan men vinden op de internetsite http://www.smc.com onder de betrokken productcategorie.
Maltese	Hawnhekk, SMC Networks, jiddikjara li dan Radio LAN device jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Hungarian	Alulírott, SMC Networks nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polish	Niniejszym SMC Networks oświadcza, że *Radio LAN device* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Portuguese	SMC Networks declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovak	SMC Networks týmto vyhlasuje, že *Radio LAN device* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Finnish	SMC Networks vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
Swedish	Härmed intygar SMC Networks att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG

Icelandic	Hér með lýsir *SMC Networks* yfir því að *Radio LAN device* er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norwegian	*SMC Networks* erklærer herved at utstyret *Radio LAN device* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Countries of Operation & Conditions of Use in EC / EFTA member states

English	This device is a 2.4 GHz wireless LAN transceiver, intended for indoor home and office use in all notified EC and EFTA member states. In accordance with article 6.4 of the R&TTE Directive 1999/5/EC the following EC/ EFTA member states have been notified: Austria, Belgium, Denmark, Finland, France, Germany, Italy, Luxembourg, Netherlands, Norway, Spain, Sweden, Switzerland, United Kingdom, Portugal, Greece, Ireland, Iceland. Requirements for outdoor operation, like license requirements and allowed channels of operation apply in some countries. Please contact your local regulation authority or SMC Networks for details on current restrictions for outdoor use.
French	Ce produit est un appareil radio LAN transceiver de 2.4 GHz destiné aux PME et a l'utilisation domestique dans tous les pays certifiés conformes aux conditions de l'EU et de l'EFTA. En accord avec l'article 6.4 de la R&TTE directive 1999/5/EC, the membres de la EU et de l'EFTA sont les suivants: Autriche, Belgique, Danemark, finalnde, France, Allemagne, Italie, Luxembourg, Pays-Bas, Norvège, Espagne, Suède, Suisse, Royaume-Uni, Portugal, Grèce, Irelande, Icelande. Des conditions sont appliquées à certains pays pour l'utilisation en extérieur, tels que des licences spécifiques et des canaux d'opération. Veuillez contacter votre autorité locale ou SMC Networks pour plus de détails quant aux restrictions actuelles concernant l'utilisation en extérieur.
Dutch	Dit toestel is een 2.4 Ghz draadloze Lan transceiver, bestemd voor gebruik binnen huis en kantoor in alle geïnformeerde lidstaten van de EC en de EFTA. In overeenstemming met artikel 6.4 van de R&T TE Directive 1999/5/EC zijn de volgende EC/ EFTA lidstaten verwittigd: België, Denemarken, Duitsland, Finland, Frankrijk,Griekenland, Ierland, IJsland, Italië, Luxemburg, Nederland, Noorwegen,Oostenrijk, Portugal, Spanje , Verenigd Koninkrijk, Zweden, Zwitserland. Benodigdheden voor gebruik buiten, zoals gebruiksvergunningen en toegelaten werkkanalen zijn van toepassing in sommige landen. Gelieve uw lokale instantie of SMC Networks te contacteren voor details op huidige beperkingen voor gebruik in buitenlucht.
Spanish	Este aparato es un transmisor inalambrico de 2.4 GHz, previsto para el uso interior en domicilios y Pymes en todos los Estados de la CE y la EFTA notificados. De acuerdo con el artículo 6.4 de la Directiva R&TTE 1999/5/EC los siguientes estados de la CE y de la EFTA han sido notificados: Austria, Bélgica, Dinamarca, Finlandia, Francia, Alemania, Italia, Luxemburgo, Países Bajos, Noruega, Espana, Suecia, Suiza, Reino Unido, Portugal, Grecia, Irlanda, Islandia. Los requisitos para su uso exterior, como requerimiento de licencia y canales de operación permitidos se aplican en algunos paises. Por favor contacte la autoridad reguladora local o SMC Networks para más detalles en relacion con las restricciones actuales para uso exterior.
German	Dieses Wireless LAN Gerat arbeitet im 2.4 GHz Frequenzband und ist fur den Einsatz im Innenbereich in den benachrichtigten EC/ EFTA Mitgliedstaaten geeignet. In Übereinstimmung mit Artikel 6.4 der R&TTE Direktive 1999/5/EC wurden folgende Mitgliedstaaten benachrichtigt: Österreich, Belgien, Dänemark, Finland, Frankreich, Deutschland, Italien, Luxemburg, Niederlande, Norwegen, Spanien, Schweden, Schweiz, Großbritannien, Portugal, Griechenland, Irland, Island. Für den Einsatz im Aussenbereich sind in einigen Ländern Lizenzen erforderlich oder die Anzahl der Kanäle ist eingeschränkt. Bitte kontaktieren Sie Ihre Regulierungsbehörde oder SMC Networks für die aktuellen Einschrankungen beim Einsatz im Aussenbereich.

SMC Contact for this device in Europe is:

SMC Networks Europe,
Edificio Conata II,
Calle Fructuos Gelabert 6-8, 2, 4a,
08970 - Sant Joan Despi,
Barcelona, Spain

About This Guide

Purpose

This guide details the hardware features of the wireless USB adapter, including its physical and performance-related characteristics, and how to install the device and use its configuration software.

Audience

This guide is for PC users with a working knowledge of computers. You should be familiar with Windows operating system concepts.

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Related Publications

The following publication gives basic information on how to install and use the wireless USB adapter.

Quick Installation Guide

Also, as part of the the wireless USB adapter’s software, there is online help that describes all configuration related features.

Revision History

This section summarizes the changes in each revision of this guide.

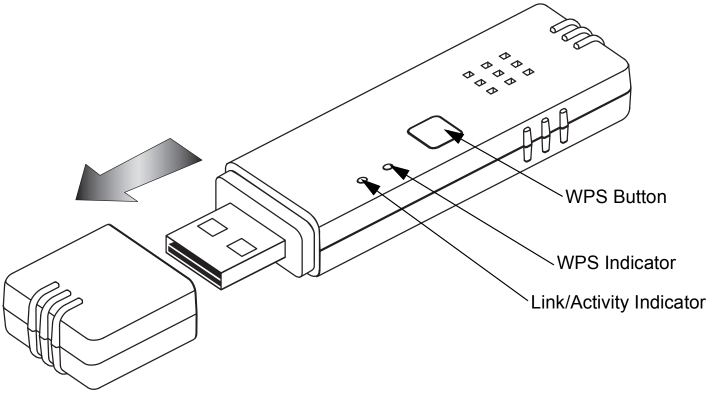
October 2007 Revision

This is the first revision of this guide.

Contents

Chapter 1: Introduction

The SMCWUSBS-N is a Wi-Fi (IEEE 802.11b/g/n) Wireless USB Adapter that enables wireless connectivity for your PC. The device provides a Wi-Fi client solution for PCs using a USB 2.0 interface. The USB adapter also includes a comprehensive configuration, site survey, and profile management utility that can be installed on a Windows 2000, Windows XP or Windows Vista system.



Features

- Wi-Fi compliant with IEEE 802.11n (draft 2.0) and IEEEE 802.11b/g standards
- High-speed connection up to 300 Mbps in 802.11n mode
- Dynamic data rate scaling from 1 to 300 Mbps
- Low interference and high susceptibility to guarantee reliable performance
- Support WEP, WPA-PSK, WPA2-PSK security
- Wi-Fi Protected Setup (WPS), including push button and PIN methods
- WMM (Wi-Fi Multimedia)
- Windows 2000, XP and Vista drivers
- WHQL certified
- WLAN site survey and profile management utility
- Infrastructure and Ad-hoc operating modes

System Requirements

Before you install the EZ Connect Wireless USB Adapter, check your system meets the following requirements:

- 2.4 GHz 802.11n (draft 2.0) or 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

Package Checklist

The Wireless USB Adapter package includes these items:

- EZ Connect N Wireless USB 2.0 Adapter (SMCWUSBS-N)
- EZ Installation Wizard & Documentation CD
- Quick Installation Guide.
- Warranty Information Card

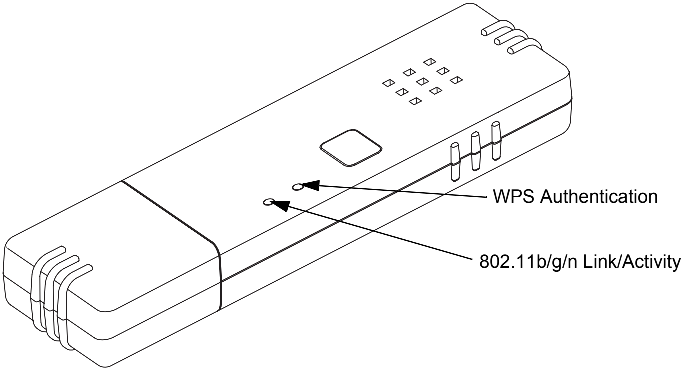
Inform your dealer if there are any incorrect, missing or damaged items. If possible, retain the carton, including the original packing materials. Use them to repack the product in case there is a need to return it.

Hardware Description

SMC’s EZ Connect Wireless USB Adapter supports wireless communications at up to 300 Mbps. This adapter operates in the 2.4 GHz band and is fully compliant with IEEE 802.11b/g and 802.11n (draft 2.0). It can be installed in a notebook or desktop PC with a USB port. Support is provided for Windows 2000, Windows XP, and Windows Vista.

LED Indicators

The Wireless USB Adapter includes two status LED indicators, as described in the following figure and table.



LED	Status	Description
WPS	On/Flashing Green	Indicates the WPS button is pressed, and WPS authentication is in progress.
	Off	Indicates WPS authentication is not in progress.
Link/Activity	On/Flashing Green	Indicates the power is on, and the 802.11b/g/n radio is enabled. Flashing indicates wireless network activity.
	Off	Indicates the power is off, or the 802.11b/g/n radio is disabled.

WPS Button

Use the WPS button on the Wireless USB Adapter to automatically connect multiple devices to the network. Within two minutes, press the physical or virtual button on wireless client devices to enable them to join the WLAN.

The WPS configuration process may be initiated on any device and there is no restriction to the order in which buttons are pressed.

Any WPS-compatible devices could unintentionally join the WLAN if they are within range during the two-minute set up period after the WPS button is pressed.

For more details about Wi-Fi Protected Setup, please refer to “WPS” on page 3-14.

Chapter 2: Driver and Utility Installation

The CD-ROM that comes with the package contains the USB driver and software utility for the Wireless USB Adapter. New or updated drivers can be downloaded from SMC's web site at http://www.smc.com.

The installation screens are similar for all Microsoft Windows systems. The installation interface for only Windows XP is shown in this user guide.

To install the Wireless USB Adapter's driver and utilities for Windows 2000, Windows XP or Windows Vista, follow these steps:

Important: Do not plug in the EZ Connect N Wireless USB2.0 Adapter until instructed. Put the EZ Installation & Documentation CD into your CD-ROM drive. The CD will auto run.

1. Turn on your PC and wait until the Windows system has completely started.
2. Load the driver and utility CD that comes with the package. The install program should start automatically.

   Click Install Driver and Utility to continue the installation.

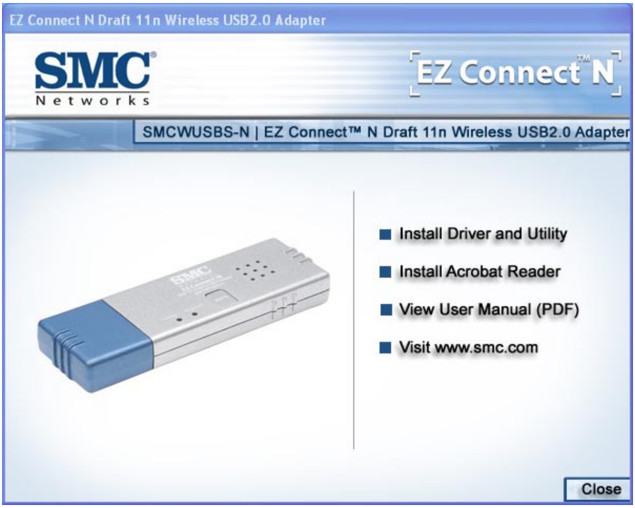
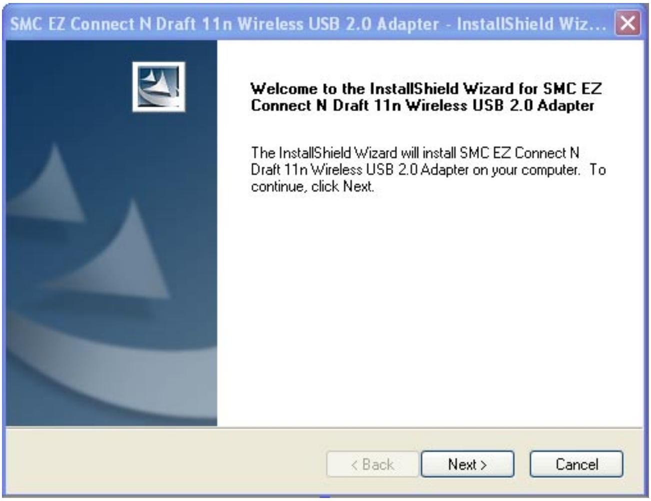

EZ Connect N Draft 11n Wireless USB2.0 Adapter
SMC Networks
EZ Connect™ N
SMCWUSBS-N | EZ Connect™ N Draft 11n Wireless USB2.0 Adapter
Install Driver and Utility
Install Acrobat Reader
View User Manual (PDF)
Visit www.smc.com
Close

Figure 2-1. EZ Connect N CD - Homepage

Note: If the install program does not start automatically, open the folder that displays the CD's contents and find the file "SMCWUSBS_N.exe" in the root directory. Double click the file to start the install program.

3. Click Next to continue the installation.



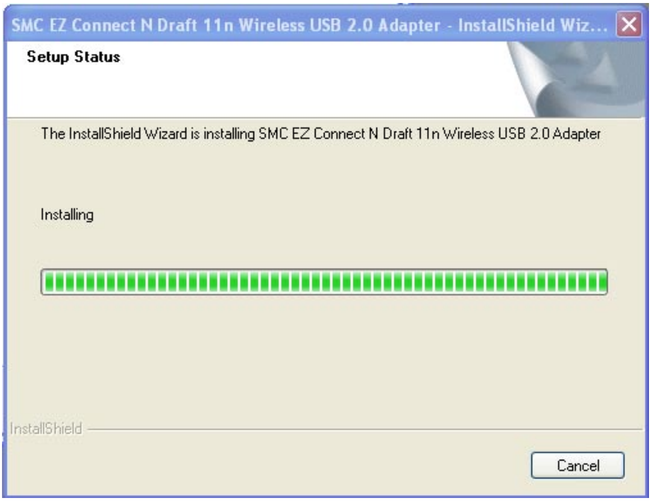
SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter - InstallShield Wiz...

Welcome to the InstallShield Wizard for SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter

The InstallShield Wizard will install SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter on your computer. To continue, click Next.

Figure 2-2. EZ Connect N CD - Driver and Utility Installation

4. Wait for the software installation procedure to complete.



SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter - InstallShield Wiz...

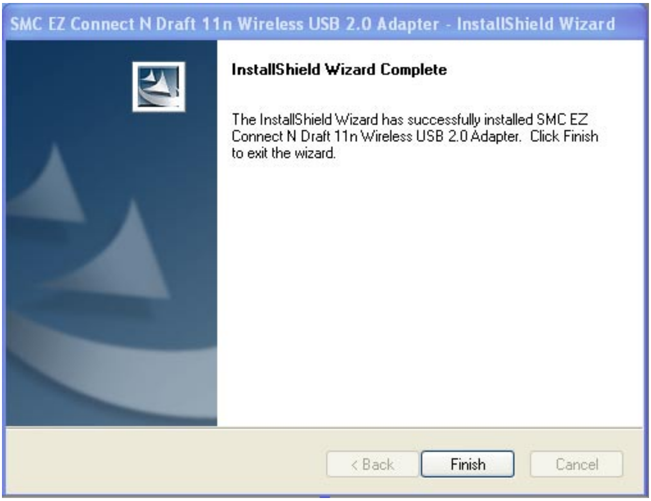
Setup Status

The InstallShield Wizard is installing SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter

Installing

Figure 2-3. EZ Connect N CD - Installation in Progress

5. When the “Installation Complete” message displays, click Finish.



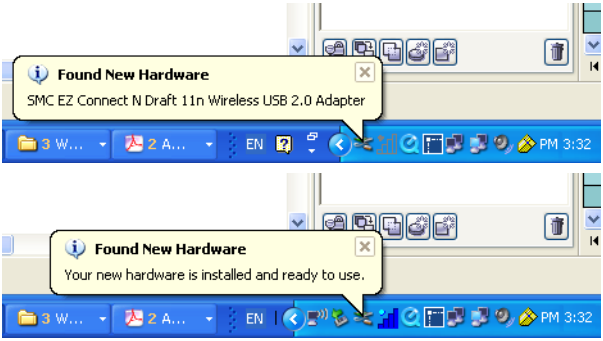
SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter. Click Finish to exit the wizard.

Figure 2-4. EZ Connect N CD - Installation Finished

6. Insert the Wireless USB Apapter in an available USB slot. The new hardware is detected and automatically installed. Now the device is ready to use.



Found New Hardware

SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter

Found New Hardware

Your new hardware is installed and ready to use.

Figure 2-5. Found New Hardware

Chapter 3: Configuration

Accessing the EZ Connect Wireless Utility

Once the the SMC EZ Connect Wireless utility installation is complete, the configuration utility can be accessed by selecting the “SMC EZ Connect N Wireless Utility” icon from the “SMC EZ Connect N Wireless Utility” folder.

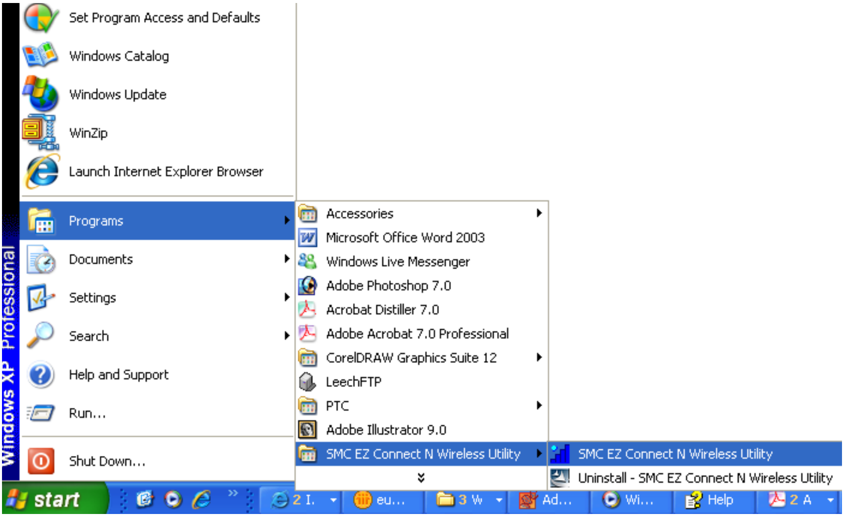


Figure 3-1. Accessing EZ Connect N Wireless Utility

A quick launch icon will appear in the lower right-hand corner of the task bar. When the icon is blue, it indicates that the wireless connection is in progress. When the icon is grey, it indicates no connection.

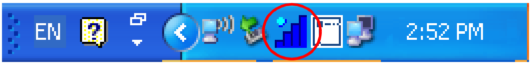


Figure 3-2. EZ Connect N Wireless Utility Icon

Note: When the utility icon is displayed, it indicates that the Wireless USB Adapter driver is installed properly.

Double-click the icon to open the SMC EZ Connect N Wireless Utility program, providing quick access to the adapter settings.

The utility screens are similar in all Microsoft Windows systems. The interface for Windows XP is described in this user guide.

Wireless Utility Configuration

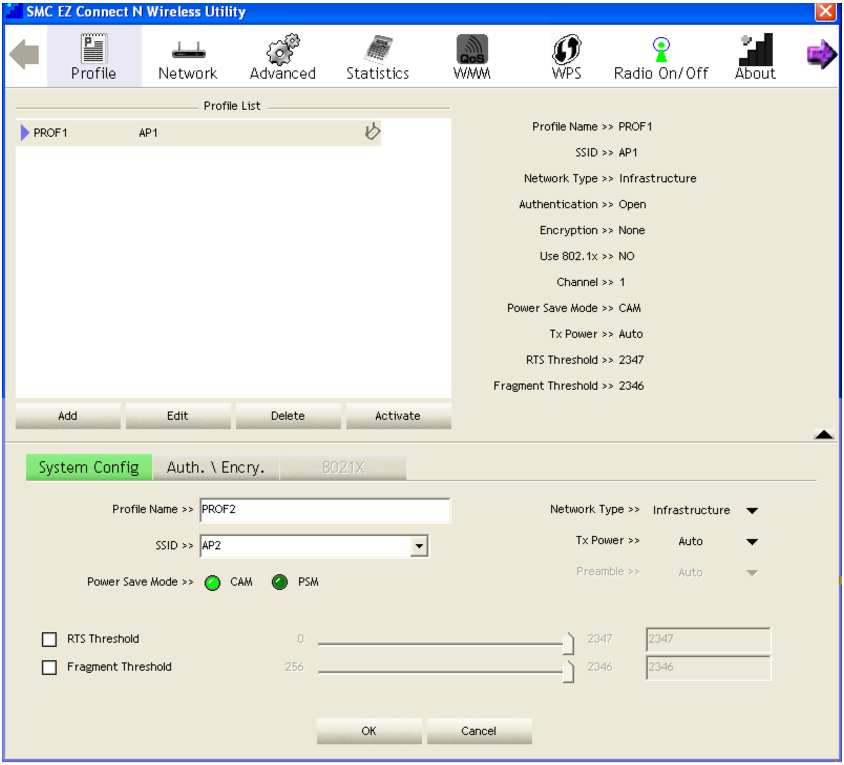
The SMC EZ Connect Wireless utility screen includes the options in the table below. For details on the configuration for each feature, see the corresponding page number.

Table 3-1. Utility Configuration Options

Tools	Description	Page
Profile	Configures the basic wireless settings for multiple profiles	3-3
Network	Displays available wireless networks	3-9
Advanced	Configures the advanced wireless settings	3-11
Statisics	Displays the detail counter information	3-12
WMM	Enables Wi-Fi Multimedia (WMM) features	3-13
WPS	Configures Wi-Fi Protected Setup (WPS) settings	3-14
Radio On/Off	Switches the radio signal on or off	3-16
About	Displays software information	3-16
Help	Launches EZ Connect wireless utility help	3-17

Profile

The profile settings page allows you to set and save different wireless settings. You can activate the suitable profile according to the environment where the wireless connection is used.



Profile List

PROF1	AP1

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 1
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

Profile Name >> PROF2
SSID >> AP2
Power Save Mode >> ● CAM ● PSM
Network Type >> Infrastructure
Tx Power >> Auto
Preamble >> Auto

□ RTS Threshold 0 2347 2347
□ Fragment Threshold 256 2346 2346

Figure 3-3. Profile - System Configuration

To Add a profile, click the Add button and configure the following displayed items:

System Configure — Configure the wireless network.

- **Profile Name** – The name of the profile. (0-32 ASCII characters and symbols are allowed; no spaces can be used)
- **SSID** – Select the SSID (Service Set Identity) name of the wireless network to which the client will connect.
- **Network Type** – The type of wireless network. (Default: Infrasturcture)
  - **Ad hoc** – An ad hoc wireless LAN is a group of computers each with wireless adapters, connected as an independent wireless LAN. Select Ad hoc to associate to a peer computer.

  - **Infrastructure** – An integrated wireless and wired LAN is called an Infrastructure configuration. Select Infrastructure to associate to an AP.

- **Power Save Mode** (available when “Infrastucture” is selected as the network type) – Enable or disable the power save operation. (Default: CAM)
  - **CAM** – Constantly awake mode, which always keeps the radio on.
  - **PSM** – Power save mode, which turns the radio off when no data is being transferred.
- **TX Power** – The amount of power transmitted by the radio when sending a signal. (Default: Auto)
- **Preamble** (availabe when “Ad hoc” is selected as the network type) – Select “Auto” to have the Wireless USB Adapter automatically use short preamble if the clients and access points in your wireless network support this feature, otherwise select “Long”. (Default: Auto)
- **Channel** (only availabe when “Ad hoc” is selected as the network type) – The radio channel used to communicate with wireless clients. The channel has to be the same as the peer computer. (Default: 1)
- **RTS Threshold** – Adjust the RTS threshold value by sliding the bar or key in the value directly when the feature is enabled. (Default: Disabled)

  Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The Wireless USB Adapter sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

  If the RTS threshold is set to 0, the Wireless USB Adapter always sends RTS signals. If set to 2347, the Wireless USB Adapter never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

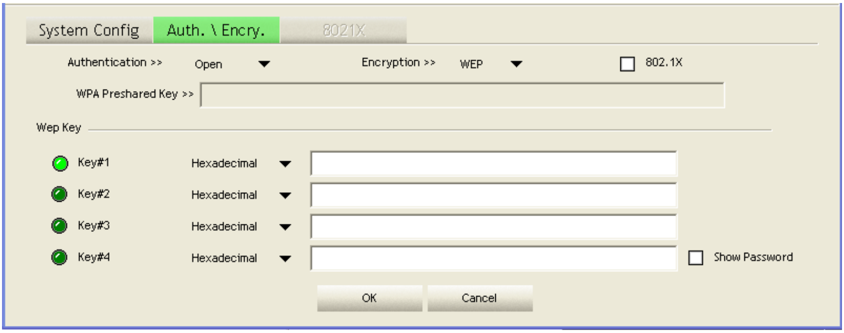
  Wireless devices contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 0-2347 bytes: Default: 2347 bytes)

- **Fragment Threshold** – Adjust the Fragment threshold value by sliding the bar or key in the value directly when the feature is enabled. (Default: Disabled)

  The fragmentation threshold is the minimum packet size that can be fragmented when passing through the adapter. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. (Range: 256-2346 bytes; Default: 2346 bytes)

Click Ok to confirm the configuration or click Cancel to cancel the settings.

- **Authentication / Encryption** — Configure authentication and encryption to match the security of the wireless network.



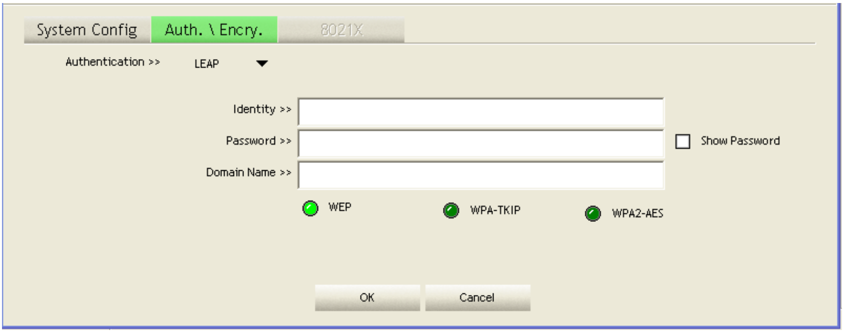
Authentication >> Open
Encryption >> WEP
☐ 802.1X
WPA Preshared Key >>
Wep Key
● Key#1 Hexadecimal
● Key#2 Hexadecimal
● Key#3 Hexadecimal
● Key#4 Hexadecimal
☐ Show Password

Figure 3-4. Profile - Authentication\Encryption

The displayed items on this page can be described as follows:

- **Authentication** – Select the authentication mode. For an infruastructure network, seven modes are supported by the Wireless USB Adapter, including Open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK. For an ad hoc network, Open, Shared and WPA-None modes are supported.
  - **Open** – Open-system authentication accepts any client attempting to connect to the access point without verifying its identity.
  - **Shared** – The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to clients before attempting authentication.
  - **LEAP** – The Lightweight Extensible Authentication Protocol (LEAP) is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
    When LEAP is select, input LEAP identity, password, domain name, and select encryption type. Check the Show Password box to display password characters as you type instead of asterisks.

  Click OK to confirm the configuration or click Cancel to cancel the settings.



Authentication >> LEAP

Identity >>

Password >> □ Show Password

Domain Name >>

● WEP ● WPA-TKIP ● WPA2-AES

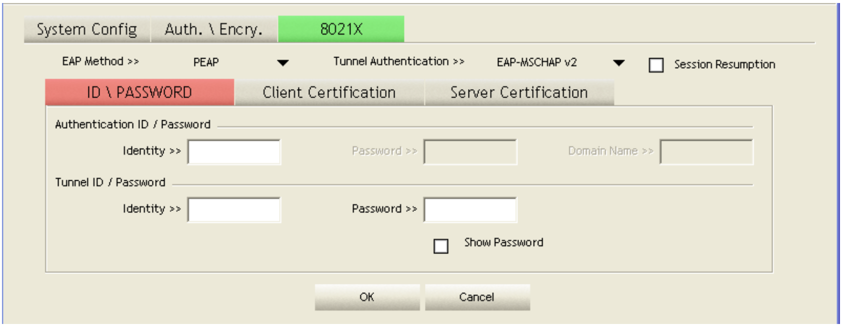
Figure 3-5. Authentication - LEAP

- **WPA / WPA-PSK** – Wi-Fi Protected Access (WPA) employs a combination of technologies to provide an enhanced security solution for wireless networks. The WPA Pre-shared Key (WPA-PSK) mode for small networks uses a common password phrase that must be manually distributed to all clients that want to connect to the netwok.
- **WPA2 / WPA2-PSK** – WPA2 is a futher security enhancement that includes the now ratified IEEE 802.11i wireless security standard.

- **Encryption** – Configure the encryption. For open and shared authentication mode, the selection options are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
  - **None** – No encryption is used.
  - **WEP** – Enables the Wireless USB Adapter to use WEP shared keys. If enabled, you must configure at least one key. Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.
  - **TKIP** – Use Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.
  - **AES** – Use Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

  Click OK to confirm the configuration or click Cancel to cancel the settings.

- **802.1X** — Use IEEE 802.1X (802.1X) for user authentication and distributing dynamically generated encryption keys. IEEE 802.1X is a standard framework for network access control that uses a RADIUS server on the local network for user authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, usernames and passwords, or other) from the client to the RADIUS server.



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Session Resumption

Authentication ID / Password

Identity >>

Password >>

Domain Name >>

Tunnel ID / Password

Identity >>

Password >>

□ Show Password

Figure 3-6. Profile - 802.1X

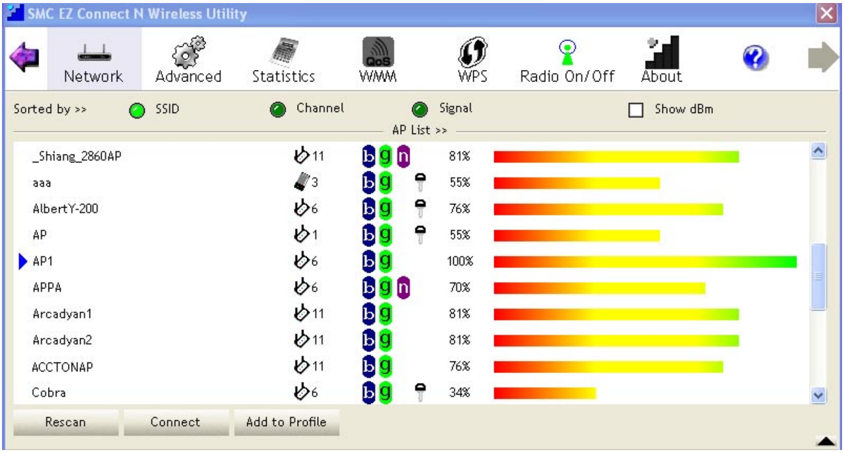
- **EAP Method** – Select an 802.1X authentication method.
  - **PEAP** – Protected Extensible Authentication Protocol. PEAP transport securely sends authentication data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
  - **TLS / Smart Card** – Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
  - **TTLS** – Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
  - **EAP-Fast** – Flexible Authentication via Secure Tunneling. An authentication method developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution. For tunnel authentication, only "Generic Token Card" authentication is supported currently.
  - **MD5-Challenge** – Message Digest Challenge. MD5 is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.

- **Tunnel Authentication** – Selects the tunnel authentication protocol. This pull-down menu is only available when the authentication type is PEAP or TTLS. When EAP-FAST is used, the protocol setting is always Generic Token Card and cannot be changed.
  - **EAP-MSCHAP v2** – This authentication uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.
  - **EAP-TLS / SmartCard** – This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It uses a client certificate for authentication.
  - **Generic Token Card** – This authentication uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.
  - **CHAP** – This authentication uses an MD5 one-way encryption scheme to hash the response to a challenge issued by the authenticator. It requires passwords to be stored in a reversibly encrypted form.
  - **MS-CHAP** – This authentication is similar to CHAP, the main difference is that with MS-CHAP the password only needs to be stored as a MD4 hash instead of a reversibly encrypted form.
  - **MS-CHAP-V2** – MS-CHAP v2 is similar to MS-CHAP with the difference that the server also authenticates itself with the client.
  - **PAP** – PAP provides a simple method for a remote node to establish its identity using a two-way handshake. A username and password pair is repeatedly sent by the remote node across the link until authentication is acknowledged.
- **ID / Password** – Configures the identity an password for authentication.
  - **Authentication ID / Password** – Identity, password and domain name of the server. Only "EAP-FAST" and "LEAP" authentication require a domain name.
  - **Tunnel ID / Password** – Identity and Password of the authentication server.
- **Client Certification** – Enable client certification.
  - **Use Client Certification** – If PEAP or TTLS is selected as the authentication method, you can use a certificate stored in the local computer. If TLS/Smart Card is used, this box is always checked.
- **Server Certification** – Enable server certification.
  - **User Cerificate Chain** – Enable the use of certificate chain and select a certification authority (CA) server.
  - **Allow Intermediate certificates** – Enable the use of intermediate certificates.
  - **Sever Name** – Input the server name of CA server here.
  - **Server Name must match exactly** – Enable the wireless configuration utility to check that the CA server name setting matches with the connected CA server. If not, the connection is dropped.
  - **Domain Name must end in specified name** – Enable the wireless configuration utility to check the end of domain name. If defects are found, the connection is dropped.

  Click OK to confirm the configuration or click Cancel to cancel the settings.

Network

The network setting page allows you to set and save different wireless settings. You can activate the suitable profile according to the environment where the wireless connection is used.



_Shiang_2860AP	11	b g n		81%
aaa	3	b g	🔑	55%
AlbertY-200	6	b g	🔑	76%
AP	1	b g	🔑	55%
▶ AP1	6	b g		100%
APPA	6	b g n		70%
Arcadyan1	11	b g		81%
Arcadyan2	11	b g		81%
ACCTONAP	11	b g		76%
Cobra	6	b g	🔑	34%

Figure 3-7. Network

The displayed items on this page can be described as follows:

Sort by — Indicate that the AP list is sorted by SSID, Channel or Signal.

Show dBm — Show the dBm strength of the received signal.

Rescan — Click the button to scan all channels for nearby wireless networks.

Connect — Click the button to connect the selected network.

Add to Profile — Click the button to add the selected network to the profile setting. The Profile page is displayed for configuration.

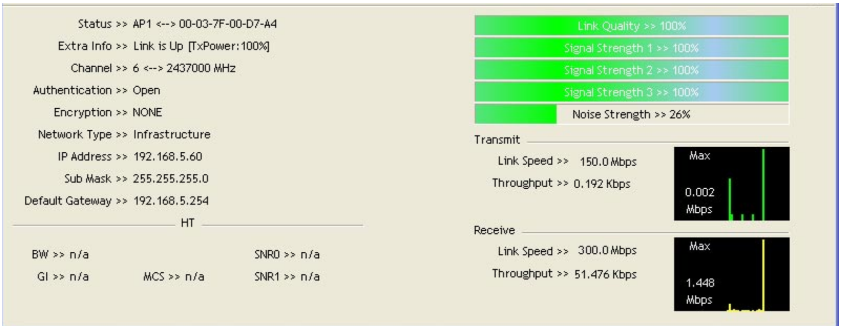
Table 3-2. Icon Indications

Icons	Description
▶	Connection is successful
	Network type is infrastructure mode
	Network type is ad-hoc mode
🔑	Wireless network is security-enabled
b	The network supports 802.11b connections

Table 3-2. Icon Indications	
Icons	**Description**
g	The network supports 802.11g connections
n	The network supports 802.11n connections

You can press the ▼ button on the buttom right corner to display the network status, as shown below.

Note: The maximum transmit link speed of this wireless USB adpater is 150 Mbps and the maximum receive link speed is 300 Mbps.



Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 192.168.5.60
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT

BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

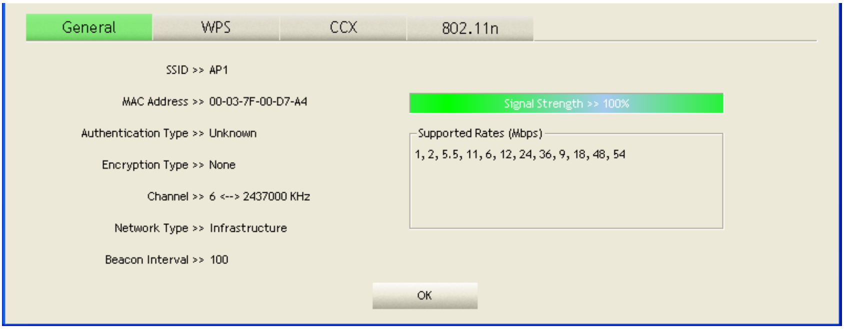
Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%
Noise Strength >> 26%

Transmit
Link Speed >> 150.0 Mbps
Throughput >> 0.192 Kbps

Receive
Link Speed >> 300.0 Mbps
Throughput >> 51.476 Kbps

Figure 3-8. Network Status

You can also double-click one of the access points on the list to display its general, WPS, CCX and 802.11n information, as shown below.



SSID >> AP1
MAC Address >> 00-03-7F-00-D7-A4
Authentication Type >> Unknown
Encryption Type >> None
Channel >> 6 <--> 2437000 KHz
Network Type >> Infrastructure
Beacon Interval >> 100

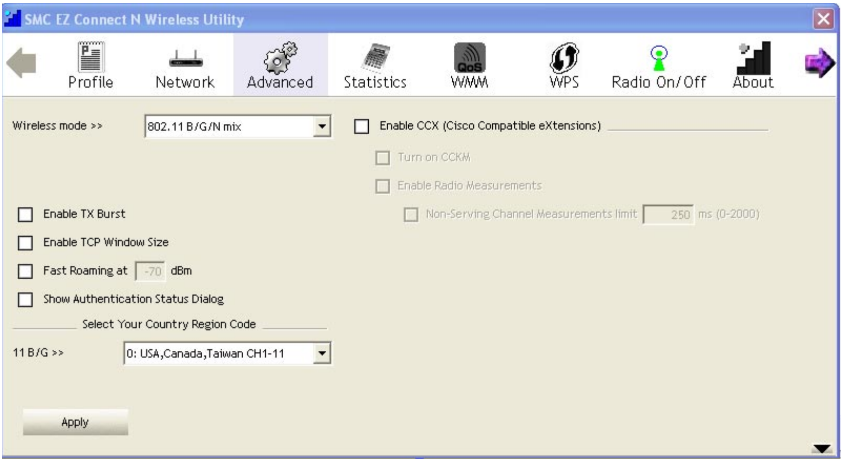
Signal Strength >> 100%

Supported Rates (Mbps)
1, 2, 5.5, 11, 6, 12, 24, 36, 9, 18, 48, 54

Figure 3-9. Access Point Status

Advanced

The Advanced page allows you to configure extended features for the wireless network.



Wireless mode >> 802.11 B/G/N mix

□ Enable CCX (Cisco Compatible eXtensions)

□ Turn on CCKM

□ Enable Radio Measurements

□ Non-Serving Channel Measurements limit 250 ms (0-2000)

□ Enable TX Burst

□ Enable TCP Window Size

□ Fast Roaming at -70 dBm

□ Show Authentication Status Dialog

Select Your Country Region Code

11 B/G >> 0: USA,Canada,Taiwan CH1-11

Figure 3-10. Advanced

The displayed items on this page can be described as follows:

Wireless Mode — Select 802.11 B/G/N mix or 802.11 B/G mix as the wireless mode.

Enable TX Burst — Enable the option to accelerate the data transmit rate.

Enable TCP Window Size — Adjust TCP window size automatically for better performance.

Fast Roaming — Enable fast roaming at the specified receive power threshold.

Show Authentication Status Dialog — Display the status of 802.1X authentication.

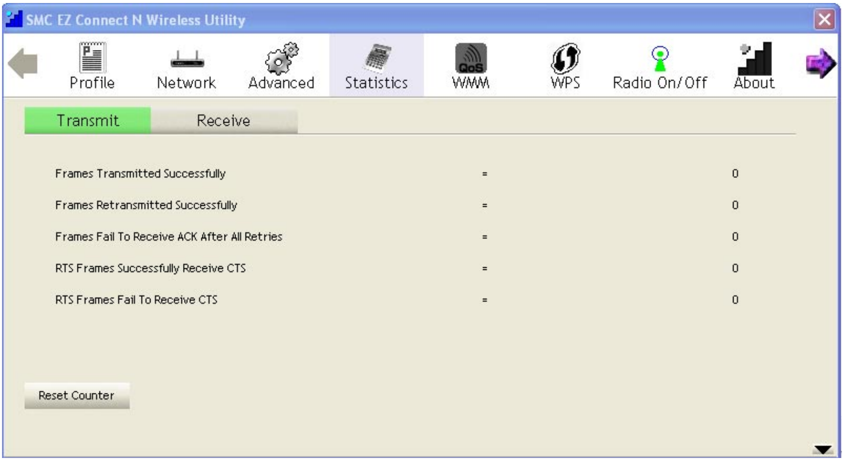
Enable CCX — Enable Cisco Compatible Extensions function.

- **Turn On CCKM** – Enable Cisco Centralized Key Management to allow fast roaming between CCKM-enable access points .
- **Enable Radio Measurements** – Improve wireless connectivity when connecting to CCX-compatible access point.
  - **Non-Serving Channel Measurements limit** – Check the option to enable measurement on unused radio channels and set the time limit for the measurement. (Default: 250ms)

Country Region Code — Select the country in which the device is being used. Setting the country code restricts operation of the device to radio channels and transmit power levels permitted for wireless networks as specified by the local regulatory authority

Statistics

The statistics page displays the connected-related statistics with detail counter information. Click Reset Counter to reset all the items back to 0

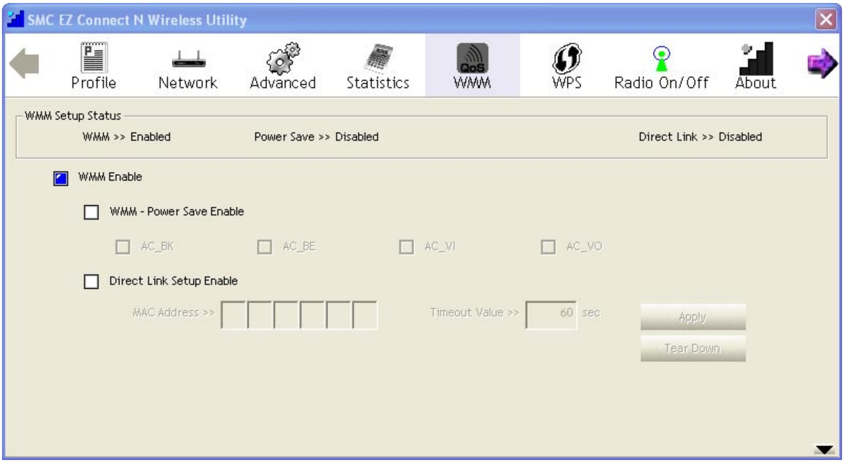


```
Frames Transmitted Successfully                 =        0
Frames Retransmitted Successfully               =        0
Frames Fail To Receive ACK After All Retries    =        0
RTS Frames Successfully Receive CTS             =        0
RTS Frames Fail To Receive CTS                  =        0
```

Figure 3-11. Statistics

WMM

Wi-Fi Multimedia (WMM), also known as Wireless Multimedia Extensions (WME), is a Wi-Fi Alliance interoperability certification. It provides basic Quality of Service (QoS) features for IEEE 802.11 wireless networks.



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Link >> Disabled

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

□ Direct Link Setup Enable

MAC Address >>   Timeout Value >> 60 sec

Figure 3-12. WMM

The displayed items on this page can be described as follows:

WMM Enable — Enable WMM function.

- **WMM - Power Save Enable** – Enable the power save mode.
  - **AC_BK** – Background / low priority
  - **AC_BE** – Best effort
  - **AC_VI** – Video first
  - **AC_VO** – Voice first
- **Direct Link Setup Enable** – Enable DLS (Direct Link Setup) function.
  - **MAC Address** – MAC address of another WMM-enabled wireless device that has a direct link to this Wireless USB Adapter.
  - **Timeout Value** – Set the time period before automatically disconnecting the WMM-enabled wireless device. If the value is zero, the link is always connected. (Default: 60 seconds; Range: 0-65535)
  - **Tear Down** – Select the device that you want to remove from DLS table and click this button.

WPS

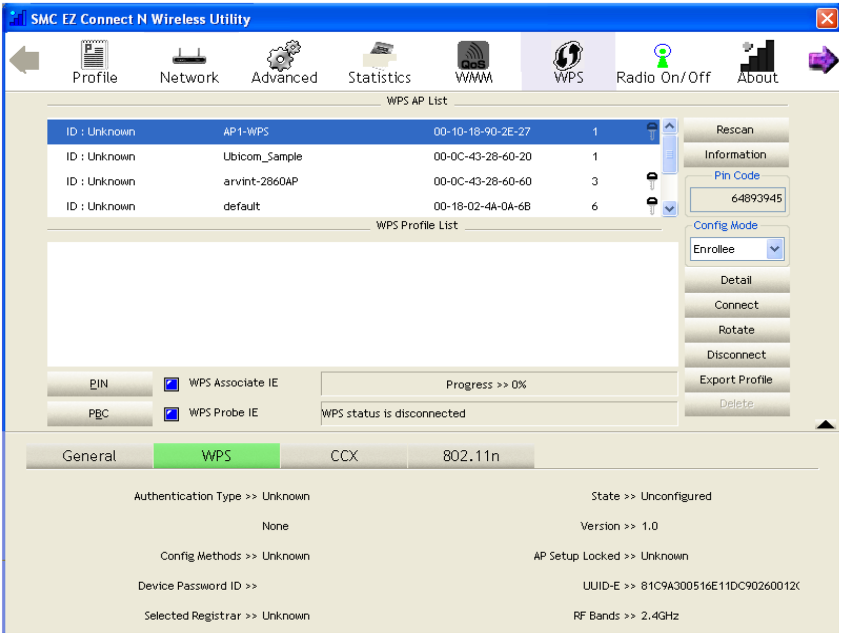
Wi-Fi Protected Setup (WPS) is based on push-button or PIN (Personal Identification Number) entry authentication to provide strong WPA/WPA2 encryption keys to client devices. Users can push a button on the access point and the client device to exchange the encryption key. With a PIN, users can enter a code generated by the client device to connect to the network.

WPS Setup - PBC (Push-button Configuration)

1. Push the WPS button on your wireless access point or start WPS standby mode as instructed by the wireless access point's user manual.

2. Before you start to establish the wireless connection using WPS, define the Wireless USB Adpater as a WPS "Enrollee" or a "Registrar" by selecting the Config Mode options.

   - **Enrollee** – An enrollee is the device being added to the network.
     If the Wireless USB Adapter is set as an enrollee, click the Rescan button on the utility WPS setup page to search for WPS-enabled access points near you. All access points found will be displayed in the WPS AP List. Select an access point on the list and click the Connect button to activate the connection. You can also click the Information button to see the detailed information about the selected access point.



ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 0%

WPS status is disconnected

Authentication Type >> Unknown
None
Config Methods >> Unknown
Device Password ID >>
Selected Registrar >> Unknown

State >> Unconfigured
Version >> 1.0
AP Setup Locked >> Unknown
UUID-E >> 81C9A300516E11DC90260012(
RF Bands >> 2.4GHz

Figure 3-13. WPS Setting - Enrollee Mode

- **Registrar** – A registrar is the network enrollment center.
  If the Wireless USB Adapter is set as a registrar, click the Rescan button on the utility WPS setup page to search for WPS-enabled wireless devices near you. All enrollees found will be displayed in the WPS Profile List. Select an enrollee on the list and click the Connect button to activate the connection.

3. Press the physical button on the Wireless USB Adapter or click PBC button on this utility page to start to establish a wireless connection (this may require several seconds to one minute to complete).

Notes: **1.** If WPS fails, click the PBC button few more times to try again.

2. When an access point or a WPS enrollee is connected, you can click Disconnect to disconnect from the connected device, or select another WPS-enabled wireless access point or enrollee, then click Connect to establish connection.

3. You can also click the Rotate button to select the next access point or enrollee in the list and establish a connection.

4. To delete an access point from the list, click Delete.

WPS Setup - PIN Configuration

The WPS PIN (Personal Identification Number) setup is optional to the WPS button setup. It is more secure than using the WPS button. All WPS-compatible devices have their own PIN number.

1. When the Wireless USB Adapter is set as an enrollee, the PIN number of your Wireless USB Adapter is an eight-digit number located at the upper-right position of configuration utility. Remember this number and input it to your wireless access point as the WPS PIN code. Please also refer to the user manual of your wireless access point for instructions about WPS setup.

   Click PIN button and wait for few seconds to one minute. If a wireless access point with correct PIN code is found, you will be connected to that access point.

Note: You may have to click PIN for few more times to try again. If you still cannot connect to an access point this way, please make sure the PIN code you provided to access point is correct.

2. When the Wireless USB Adapter is set as a registrar, input the enrollee’s PIN number to the Pin Code box located in the upper-right position of configuration utility.

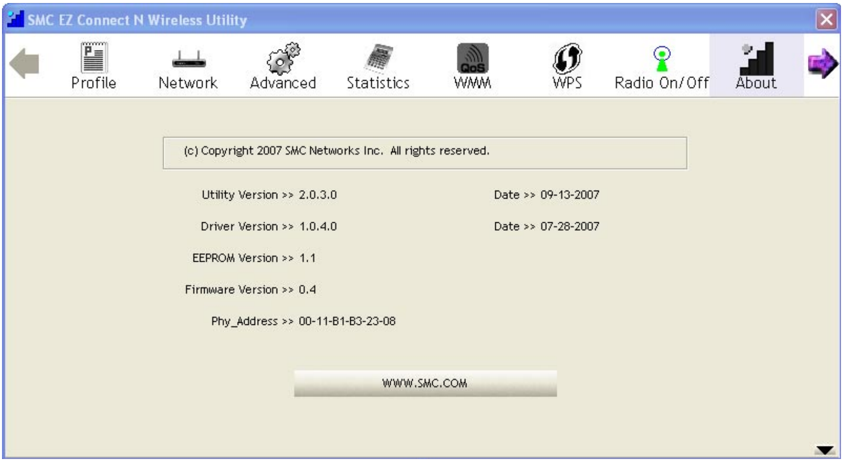
   Click PIN button and wait for few seconds to one minute. If a WPS enrollee with correct PIN code is found, it will be connected to the Wireless USB Adapter.

Radio Setting

Press the Radio On/Off icon to disable or enable the radio signal connection.

About

The about page displays the information about version numbers of the configuration utility, firmware and other information of the device. Click the WWW.SMC.COM button to visit the SMC website for other information.



(c) Copyright 2007 SMC Networks Inc. All rights reserved.

Utility Version >> 2.0.3.0 Date >> 09-13-2007

Driver Version >> 1.0.4.0 Date >> 07-28-2007

EEPROM Version >> 1.1

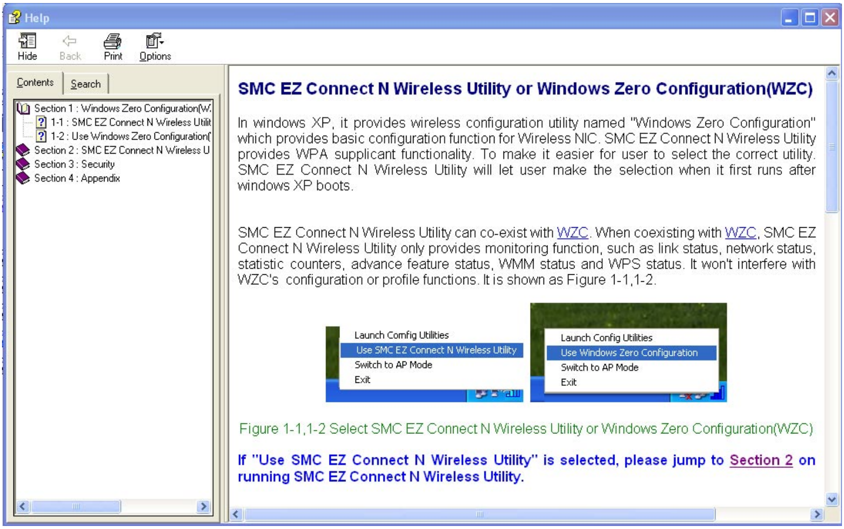
Firmware Version >> 0.4

Phy_Address >> 00-11-B1-B3-23-08

Figure 3-14. About Information Display

Help

The help page provides detailed information about each setting of the EZ Connect utility. Click the contents on the left screen and view the information on the right screen.


Help
Hide
Back
Print
Options
Contents
Search
Section 1 : Windows Zero Configuration(W
1-1 : SMC EZ Connect N Wireless Utilit
1-2 : Use Windows Zero Configuration(
Section 2 : SMC EZ Connect N Wireless U
Section 3 : Security
Section 4 : Appendix
Launch Comfig Utilities
Use SMC EZ Connect N Wireless Utility
Switch to AP Mode
Exit
Launch Config Utilities
Use Windows Zero Configuration
Switch to AP Mode
Exit

SMC EZ Connect N Wireless Utility or Windows Zero Configuration(WZC)

In windows XP, it provides wireless configuration utility named "Windows Zero Configuration" which provides basic configuration function for Wireless NIC. SMC EZ Connect N Wireless Utility provides WPA supplicant functionality. To make it easier for user to select the correct utility. SMC EZ Connect N Wireless Utility will let user make the selection when it first runs after windows XP boots.

SMC EZ Connect N Wireless Utility can co-exist with WZC. When coexisting with WZC, SMC EZ Connect N Wireless Utility only provides monitoring function, such as link status, network status, statistic counters, advance feature status, WMM status and WPS status. It won't interfere with WZC's configuration or profile functions. It is shown as Figure 1-1,1-2.

Figure 1-1,1-2 Select SMC EZ Connect N Wireless Utility or Windows Zero Configuration(WZC)

If "Use SMC EZ Connect N Wireless Utility" is selected, please jump to Section 2 on running SMC EZ Connect N Wireless Utility.

Figure 3-1. Help Screen Display

Chapter 4: Network Planning

SMC's EZ Connect Wireless Solution supports a stand-alone wireless network configuration, as well as an integrated configuration with Ethernet LANs.

The SMCWUSBS-N wireless USB adapter can be configured as:

- **Ad hoc** - for small peer-to-peer networks with other wireless devices
- **Infrastructure** - for a wireless extension to an existing wired LAN through an access point

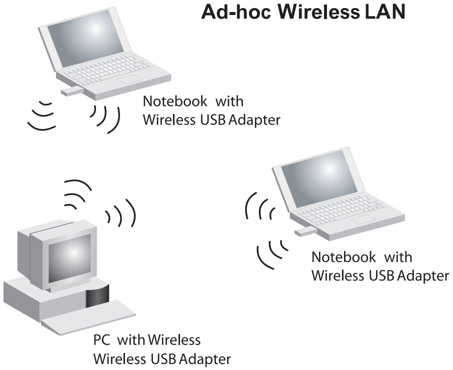
Network Topologies

Ad Hoc Wireless LAN

An ad hoc wireless LAN consists of a group of computers, each equipped with a wireless adapter, connected via radio signals as an independent wireless LAN.

Computers in a specific ad hoc wireless LAN must be configured to the same radio channel.

An ad hoc wireless LAN can be used for a small branch office or SOHO operation.

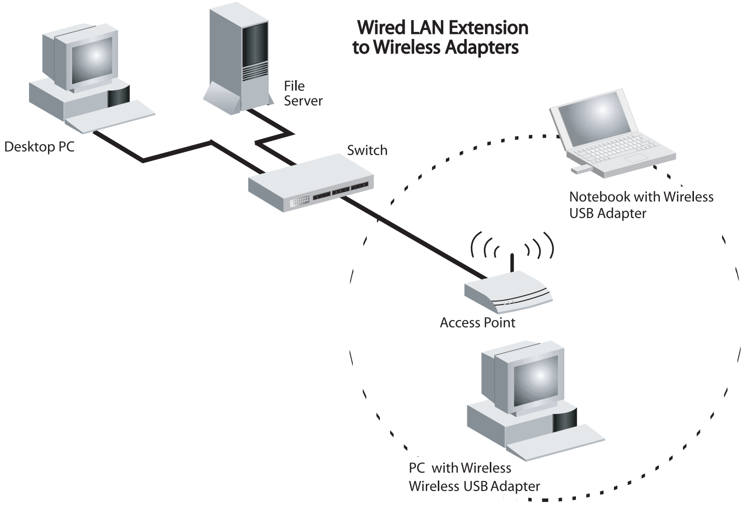

Ad-hoc Wireless LAN
Notebook with Wireless USB Adapter
Notebook with Wireless USB Adapter
PC with Wireless Wireless USB Adapter

Infrastructure Wireless LAN

The SMCWUSBS-N can also provide access to a wired LAN for wireless workstations. An integrated wired and wireless LAN is called an Infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users, and an access point that is directly connected to the wired LAN. Each wireless PC in this BSS can communicate with to any computer in its wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure via an access point.

The infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also increases the effective wireless transmission range for wireless PCs by passing their signal through one or more access points.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure.



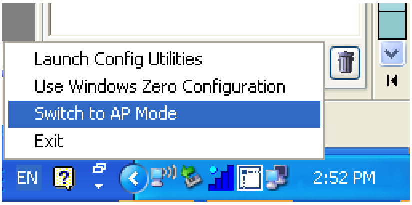
Chapter 5: AP Mode Configuration

The USB Adapter's utility can extend the functionality of the device by adding an Access Point (AP) mode to its normal client capabilities.

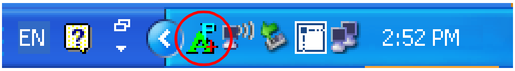
In AP mode, the USB Adapter operates as a "Soft AP." The Soft AP feature creates a Wireless LAN to Ethernet bridge using the host PC's existing Ethernet port. When the host PC is connected to an Internet connection, the Soft AP uses Windows Internet Connection Sharing (ICS) so that all associated wireless clients can share that connection.

Switching to AP Mode

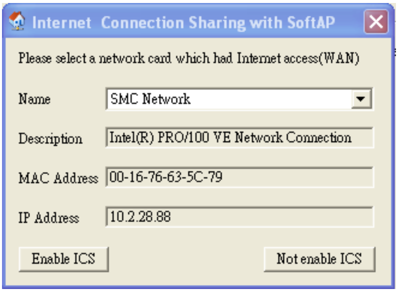
Click the SMC EZ Connect Wireless utility icon with the right mouse button and then select “Switch to AP Mode.”



A quick launch icon will appear in the lower right-hand corner of the task bar.



An Internet connection screen appears after switching to AP mode. Select a network and click the Enable ICS button to use Windows Internet Connection Sharing (ICS) and start the the Soft AP utility configuration.



Internet Connection Sharing with SoftAP

Please select a network card which had Internet access(WAN)

Name: SMC Network

Description: Intel(R) PRO/100 VE Network Connection

MAC Address: 00-16-76-63-5C-79

IP Address: 10.2.28.88

Double-click the quick launch icon to open the Soft AP utility configuration for the next time.

The utility screens are similar in all Microsoft Windows systems. The interface for Windows XP is described in this user guide.

AP Mode Utility Configuration

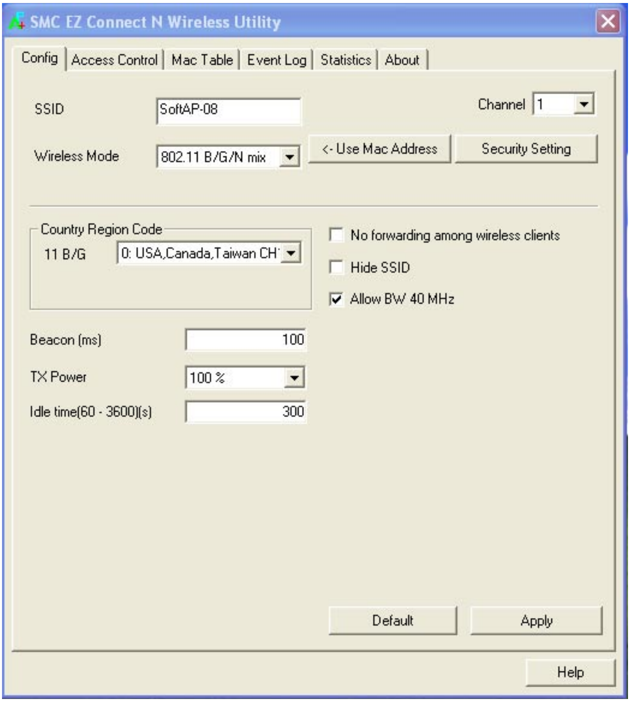
The Soft AP utility screen includes the options in the table below. For details on the configuration for each feature, see the corresponding page number.

Table 5-1. Utility Configuration Options

Tools	Description	Page
Config	Configures the basic wireless settings for multiple profiles	5-3
Access Control	Controls the MAC address connected to the AP	5-6
Mac Table	Displays current link information	5-7
Event Log	Displays the messages generated during the operation	5-8
Statistics	Displays the detail counter information	5-9
About	Displays software information	5-10
Help	Launches Soft AP utility help	5-11

Configuration

The configuration page allows you to set parameters for the wireless network.



SSID: SoftAP-08

Channel: 1

Wireless Mode: 802.11 B/G/N mix

Country Region Code
11 B/G: 0: USA,Canada,Taiwan CH

□ No forwarding among wireless clients

□ Hide SSID

☑ Allow BW 40 MHz

Beacon (ms): 100

TX Power: 100 %

Idle time(60 - 3600)(s): 300

Figure 5-1. Configuration

The displayed items on this page can be described as follows:

SSID — The service set identifier for this access point.

Wireless Mode — Selects the wireless mode.

- **802.11 B/G Mixed** – Clients can transfer data at both 802.11b and 802.11g standard rates to communicate with the access point.
- **802.11 B Only** – Clients can only transfer data at 802.11b standard rates to communicate with the access point.
- **802.11 G Only** – Clients can only transfer data at 802.11g standard rates to communicate with the access point
- **802.11 B/G/N mix** – Clients can transfer data at 802.11b, 802.11g and 802.11n standard rates to communicate with the access point

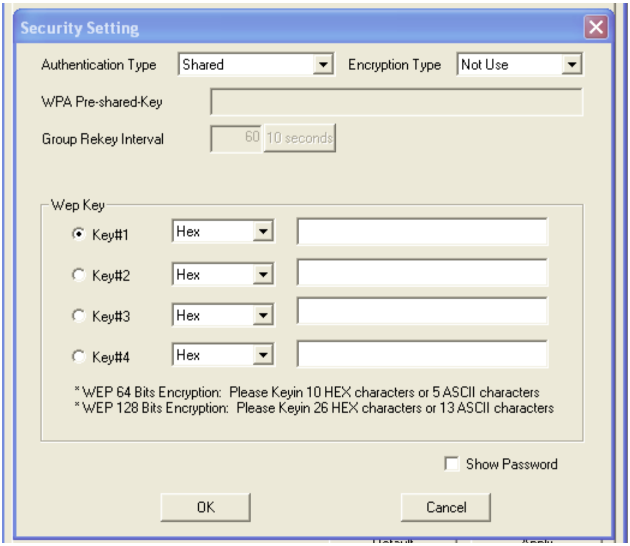
Channel — The radio channel used to communicate with wireless clients.

Use Mac Address — Click the button to display the physical layer address of the access point.

Security Setting — Configure the authentication and encryption.

- **Authentication Type** – Selects the wireless security mechanism for the network.
  - **Open** – Accepts any client attempting to connect to the access point without verifying its identity.
  - **Shared** – Uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to clients.
  - **WPA-PSK** – Use pre-shared key authentication for WPA-compliant clients.
  - **WPA2-PSK** – Use pre-shared key authentication for WPA2-compliant clients.
  - **WPA-PSK / WPA2-PSK** – Use pre-shared key authentication for WPA- and WPA2-compliant clients when they coexist in the same network.
- **Encryption Type** – Selects the encryption cipher to use for multicast and unicast data traffic.
  - **Not Use** – No encryption is used.
  - **WEP** – Uses WEP shared keys.
  - **TKIP** – Uses TKIP keys for both multicast and unicast encryption..
  - **AES** – Uses AES keys for both multicast and unicast encryption.
  - **Both** – Uses TKIP for the multicast cipher and TKIP or AES for the unicast cipher depending on the capability of associated clients.
- **Pre-shared Key** – Enter a key as an easy-to-remember form of letters and numbers. The key must be from 8 to 32 characters, which can include spaces. All wireless clients must be configured with the same key to communicate with the access point.
- **Group Rekey Interval** – Enter the group key renewal time. This feature is only avaliable when WPA-PSK encryption is used.
- **WEP Key** – Only avaliable when WEP encryption is selected. Standard keys are either 5 or 13 alpanumeric characters; or 10 or 32 hexadecimal digits. Check the Show Password box to display password characters as you type instead of asterisks.

Click OK to confirm the configuration or click Cancel to cancel the settings.



Security Setting

Authentication Type: Shared

Encryption Type: Not Use

WPA Pre-shared-Key:

Group Rekey Interval: 60 10 seconds

Wep Key

- ● Key#1 Hex
- ○ Key#2 Hex
- ○ Key#3 Hex
- ○ Key#4 Hex

*WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters
*WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters

□ Show Password

Figure 5-2. Configuration - Security Setting

Country Region Code — Select the country region where the access point is in operation.

Table 5-2. Country Channel List	
Classification	**Range**
0: USA, Canada, Taiwan	CH 1 ~ CH 11
1: Europe	CH 1 ~ CH 13
2: Spain	CH 10 ~ CH 11
3: France	CH 10 ~ CH 13
4: Japan (MKK)	CH 14
5: Japan (TELEC)	CH 1 ~ CH 14
6: ISRAEL	CH 3 ~ CH 9
7: ISRAEL	CH 5 ~ CH 13

Beacon (ms) — Set the time invterval between two beacons. (Default: 100ms)

TX Power — Set the access point transmit power. (Default: 100%)

Idle time — Set the idle time. (Default: 300s)

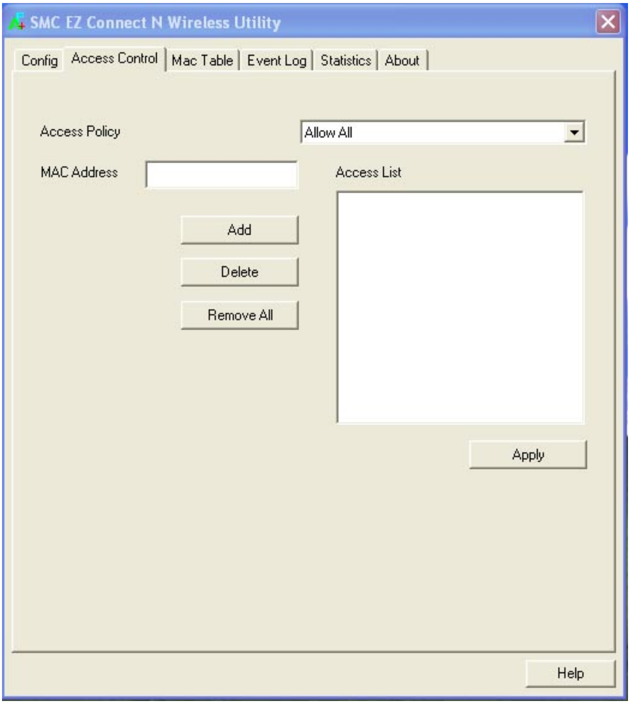
No forwarding among wireless clients — Check the box to prevent traffic being forwarded among the wireless clients.

Hide SSID — Check the box to hide the access point SSID.

Allow BW 40 MHz — Enable double-width 40 MHz channels for extra throughput.

Access Control

The access control page allows you to restrict the MAC address connected to this AP.



Access Policy: Allow All

MAC Address:

Access List

Figure 5-3. Access Control

The displayed items on this page can be described as follows:

Access Policy — Select a policy for access control. (Default: Disable)

- **Disable** – Disable the feature.
- **Allow All** – Allow the access for the listed MAC addresses.
- **Reject All** – Deny the access for the listed MAC addresses.

Mac Address — Input the MAC address applied this feature.

Add — Click Add to add the MAC adress to the Access List.

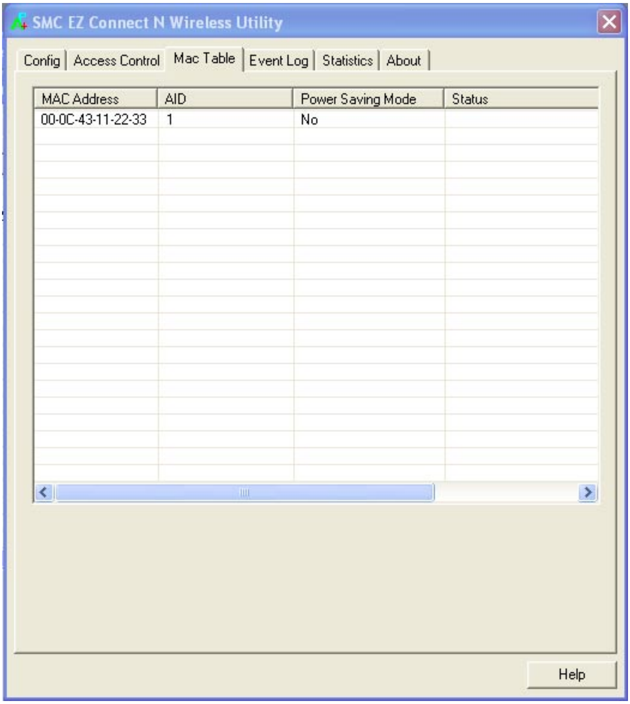
Delete — To delete a MAC address from the list, click Delete.

Remove All — Click Remove All to delete all the MAC addresses from the list.

Apply — Click Apply to apply the above changes.

MAC Table

The MAC table page displays the current station link information.



MAC Address	AID	Power Saving Mode	Status
00-0C-43-11-22-33	1	No	

Figure 5-4. MAC Table

The displayed items on this page can be described as follows:

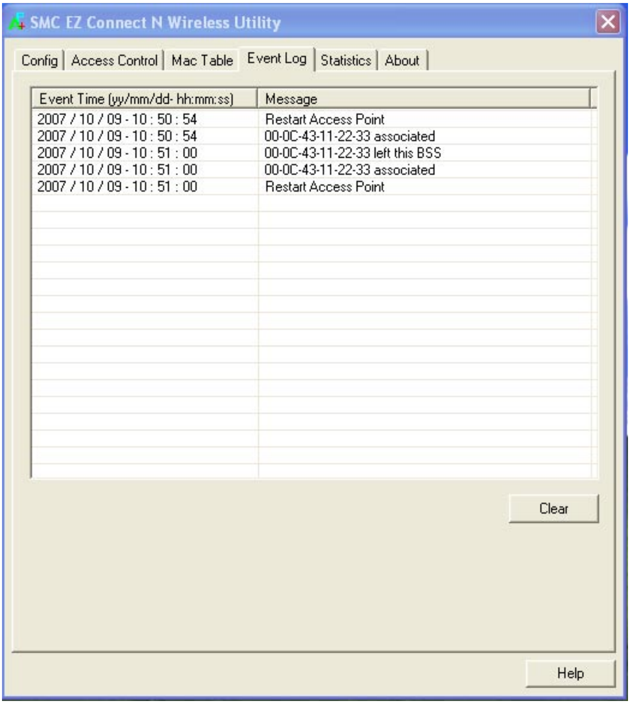
MAC Address — The MAC addresses of the connected stations.

AID — Raise value by the current wireless connection.

Power Saving Mode — The power saving status of the connected station.

Event Log

The event log page displays system messages generated during system operation. The logged messages can serve as a valuable tool for isolating Wireless USB Adapter and network problems.

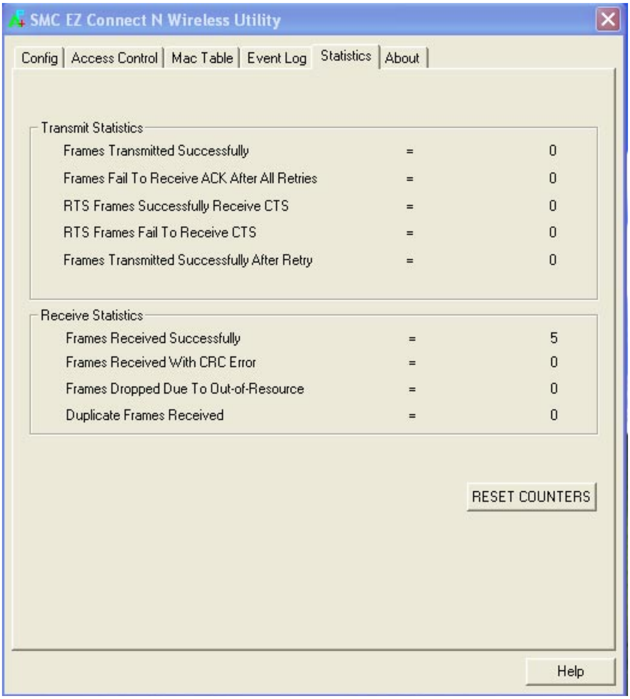


Event Time (yy/mm/dd- hh:mm:ss)	Message
2007 / 10 / 09 - 10 : 50 : 54	Restart Access Point
2007 / 10 / 09 - 10 : 50 : 54	00-0C-43-11-22-33 associated
2007 / 10 / 09 - 10 : 51 : 00	00-0C-43-11-22-33 left this BSS
2007 / 10 / 09 - 10 : 51 : 00	00-0C-43-11-22-33 associated
2007 / 10 / 09 - 10 : 51 : 00	Restart Access Point

Figure 5-5. Event Log

Statistics

The statistics page displays the connected-related statistics with detail counter information. Click Reset Counters to reset all the items back to 0.



Transmit Statistics

Frames Transmitted Successfully	=	0
Frames Fail To Receive ACK After All Retries	=	0
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0
Frames Transmitted Successfully After Retry	=	0

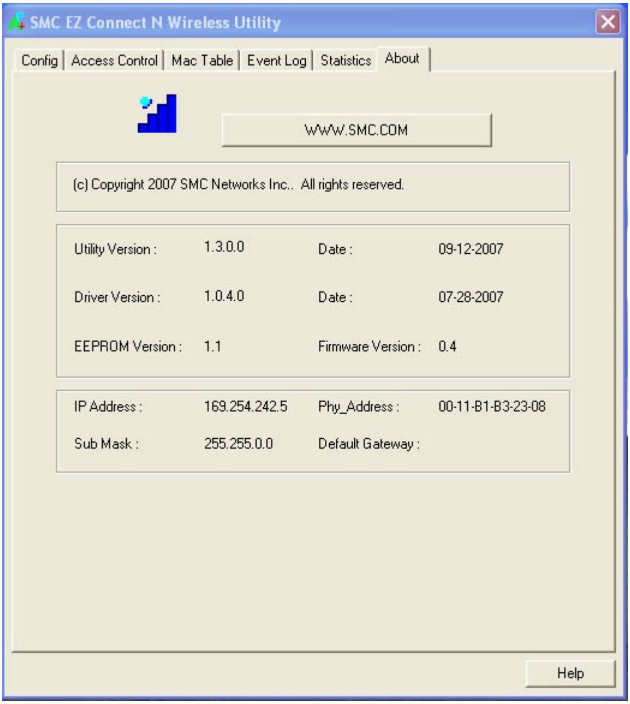
Receive Statistics

Frames Received Successfully	=	5
Frames Received With CRC Error	=	0
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0

Figure 5-6. Statistics

About

The about page displays the information about version numbers of the configuration utility, firmware and other information of the device. Click the WWW.SMC.COM button to visit the SMC website for other information.



(c) Copyright 2007 SMC Networks Inc.. All rights reserved.

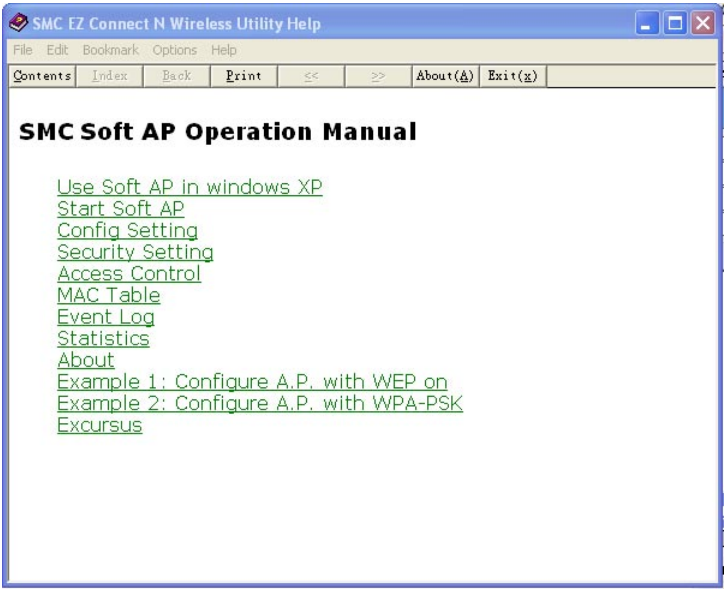
Utility Version :	1.3.0.0	Date :	09-12-2007
Driver Version :	1.0.4.0	Date :	07-28-2007
EEPROM Version :	1.1	Firmware Version :	0.4

IP Address :	169.254.242.5	Phy_Address :	00-11-B1-B3-23-08
Sub Mask :	255.255.0.0	Default Gateway :	

Figure 5-7. About Information Display

Help

The help page provides detailed information about each setting of the Soft AP utility. Click one of the headings to view the information.

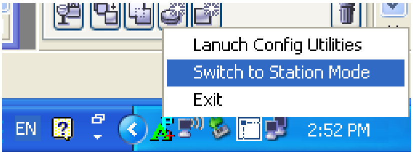

SMC EZ Connect N Wireless Utility Help
File Edit Bookmark Options Help
Contents Index Back Print << >> About(A) Exit(x)

SMC Soft AP Operation Manual

Use Soft AP in windows XP
Start Soft AP
Config Setting
Security Setting
Access Control
MAC Table
Event Log
Statistics
About
Example 1: Configure A.P. with WEP on
Example 2: Configure A.P. with WPA-PSK
Excursus

Figure 5-8. Help Screen Display

If you want to switch the device back to the station mode, click the Soft AP utility icon with the right button of the mouse and then select Switch to Station Mode.



Appendix A: Troubleshooting

USB Adapter Installation Problems

If your computer cannot find the EZ Connect Wireless USB Adapter or the network driver does not install correctly, check the following items:

- Make sure the adapter is connected to the USB port. Check for any hardware problems, such as physical damage to the adapter’s connector.
- Try the adapter in another USB port. If this also fails, try using another SMCWUSBS-N wireless adapter that is known to operate correctly.
- Check for a defective computer or USB port by trying the adapter in another computer that is known to operate correctly.

Network Connection Problems

If the Link/Activity LED on the USB adapter is not lit, or if you cannot access network resources from the computer, check the following:

- Make sure the correct software driver is installed. Try reinstalling the driver.
- Make sure the computer and other network devices are receiving power.
- The access point you want to connect to may not be functioning correctly. Try using another access point.
- If you cannot access a Windows service on the network, check that you have enabled and configured the service correctly. If you cannot connect to a particular server, be sure that you have access rights and a valid ID and password.
- If you cannot access the Internet, be sure you have currently configured your system for TCP/IP.

If your wireless station cannot communicate with a computer on the Ethernet LAN when configured for Infrastructure mode, check the following:

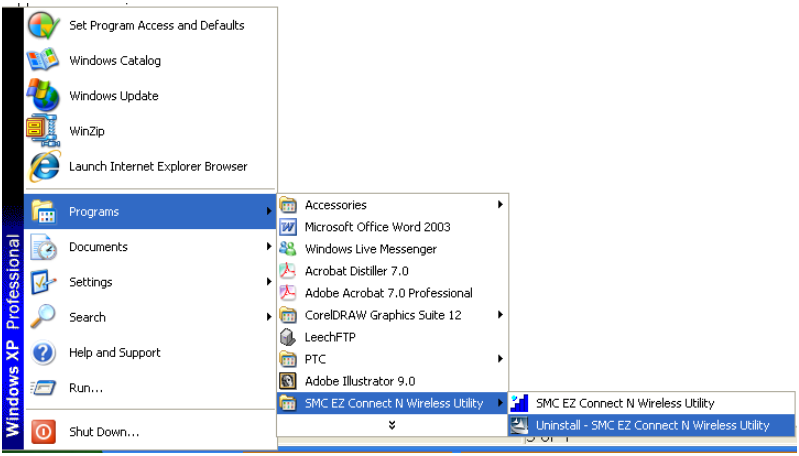
- Make sure the access point that the station is associated with is powered on.
- Check that the wireless settings (i.e., security, SSID, Channel) match the access point or other stations to which you are attempting to connect.
- If you still cannot connect, change the access point and all the stations within the BSS to another radio channel.

Uninstalling the Utility

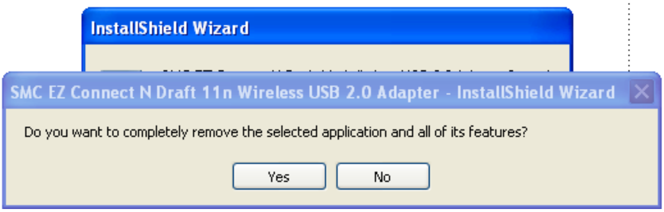
If you are having problems with the utility, you may need to uninstall the software from the system.

Follow these steps:

1. From the Windows Start menu, find the SMC EZ Connect N Utility uninstall option. Click to start the uninstall process.


Set Program Access and Defaults
Windows Catalog
Windows Update
WinZip
Launch Internet Explorer Browser
Programs
Documents
Settings
Search
Help and Support
Run...
Shut Down...
Windows XP Professional
Accessories
Microsoft Office Word 2003
Windows Live Messenger
Acrobat Distiller 7.0
Adobe Acrobat 7.0 Professional
CorelDRAW Graphics Suite 12
LeechFTP
PTC
Adobe Illustrator 9.0
SMC EZ Connect N Wireless Utility
SMC EZ Connect N Wireless Utility
Uninstall - SMC EZ Connect N Wireless Utility

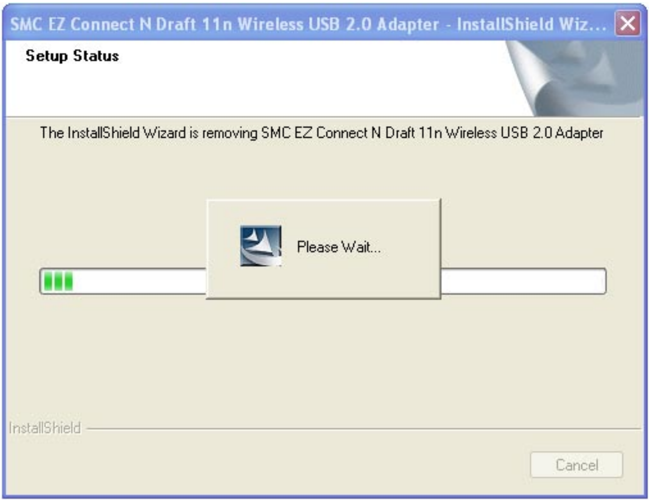
2. Click Yes to uninstall the utility.


InstallShield Wizard

SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter - InstallShield Wizard

Do you want to completely remove the selected application and all of its features?

3. Uninstallation begins.



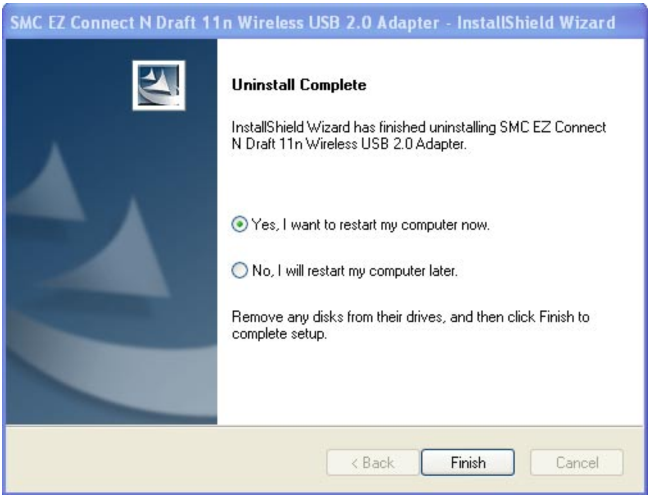
SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter - InstallShield Wiz...

Setup Status

The InstallShield Wizard is removing SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter

Please Wait...

4. When the uninstall is complete, click Finish to exit.



SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter - InstallShield Wizard

Uninstall Complete

InstallShield Wizard has finished uninstalling SMC EZ Connect N Draft 11n Wireless USB 2.0 Adapter.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Appendix B: Specifications

Interface
USB version 2.0 compliant

Power
+5V DC, 0.5A over USB connection

Radio Specifications
IEEE 802.11n (draft 2.0)
IEEE 802.11b/g

Frequency
North America: 2.412 - 2.462 GHz
Japan: 2.412 - 2.472 GHz
Europe: 2.412 - 2.472 GHz

Operating Channels
North America
  Certification: FCC; Channel: 11
Japan
  Certification: JTAC; Channel: 14
Europe
  Certification: ETSI; Channel: 13

Data Rate Shifting
1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
802.11n (draft 2.0) offering up to 300 Mbps

Antennas
Two internal 2 dBi antennas
Frequency Range: 2.4 - 2.5 GHz
Gain: 0 - 1 dBi
VSWR: 2.0 Max
Polarization: Linear
Impedance: 50 Ohm

LED Indicators
Link/Activity, WPS

TX Output Power (Typical)
11b 17.5 +/- 1 dBm
11g 14.5 +/- 1 dBm@54Mbps
11n 14.5 +/- 1 dBm

Rx Sensitivity (Typical)
-86 dBm @ 11 Mbps
-72 dBm @ 54 Mbps
-70 dBm @ 64-QAM, 20MHz channel spacing
-65 dBm @ 64-QAM, 40MHz channel spacing

Physical Size
82 x 26 x 11 mm (3.23 x 1.02 x 0.43 in.)

Weight
16 g (0.56 oz)

Temperature
Operating: -10 to 50 °C (14 to 122 °F)

Humidity
5% to 90%

EMC
FCC: Part15 subpart C
IC: RSS-210
CE: EN300328
NCC: LP0002
C-Tick

Radio
FCC: Part15 subpart B
IC: CES-003
CE: EN301489-1/-17

Safety
CE: EN60950-1

SMC®
Networks

TECHNICAL SUPPORT

From U.S.A. and Canada (24 hours a day, 7 days a week)
Phn: (800)SMC-4-YOU / (949)679-8000
Fax: (949)502-3400

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 "nns tillgängligt på www.smc.com

INTERNET
E-mail address: techsupport@smc.com

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

World Wide Web
http://www.smc.com/

SMCWUSBS-N

20 Mason • Irvine, CA 92618 • Phn: (949)679-8000 • www.smc.com