User Manual
EPSON

DNUB-E1

Revision: 1
Issue Date: 2012/09/10

Revision History

Edition #		Reason for revision	Issue date	Author
1.0	●	Initial Draft Document	2012/09/10	Lydia Tsai
	●			
	●			
	●			
	●			

1. General Description

DNUB-E1 is a 802.11n sign-chip solutions for USB dongle. It's very small and cost-effective modules which can bundle with TVs, set-top boxes, personal video recorders and other devices to a WiFi network.

2. Usage

Thank you for purchasing the WLAN a/b/g/n USB2.0 Adapter that provides the easiest way to wireless networking. This User Manual contains detailed instructions in the operation of this product. Please keep this manual for future reference.
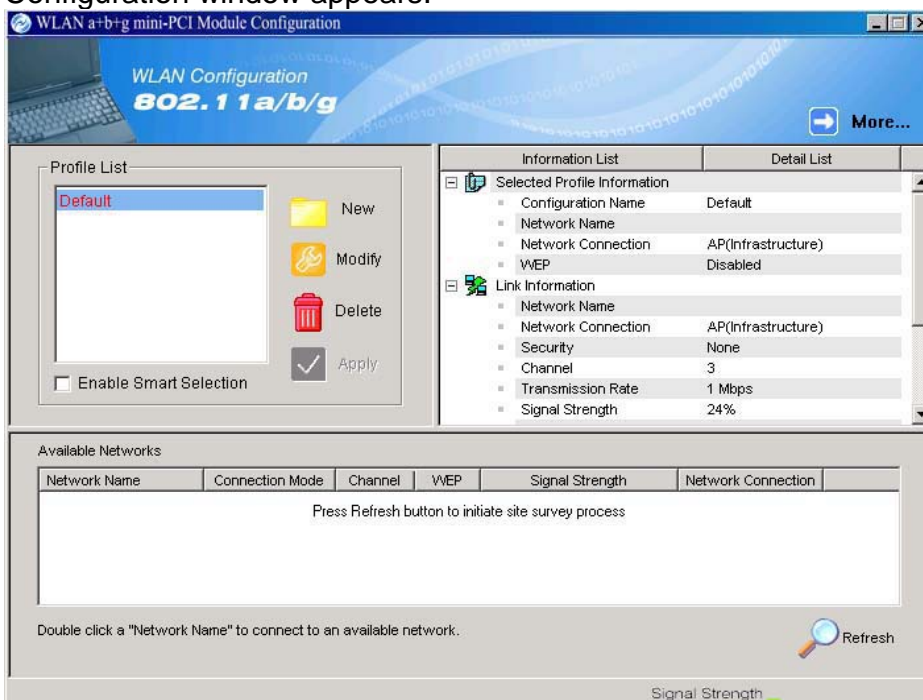
System Requirements
- A laptop PC contains:
  - 32 MB memory or greater
  - 300 MHz processor or higher
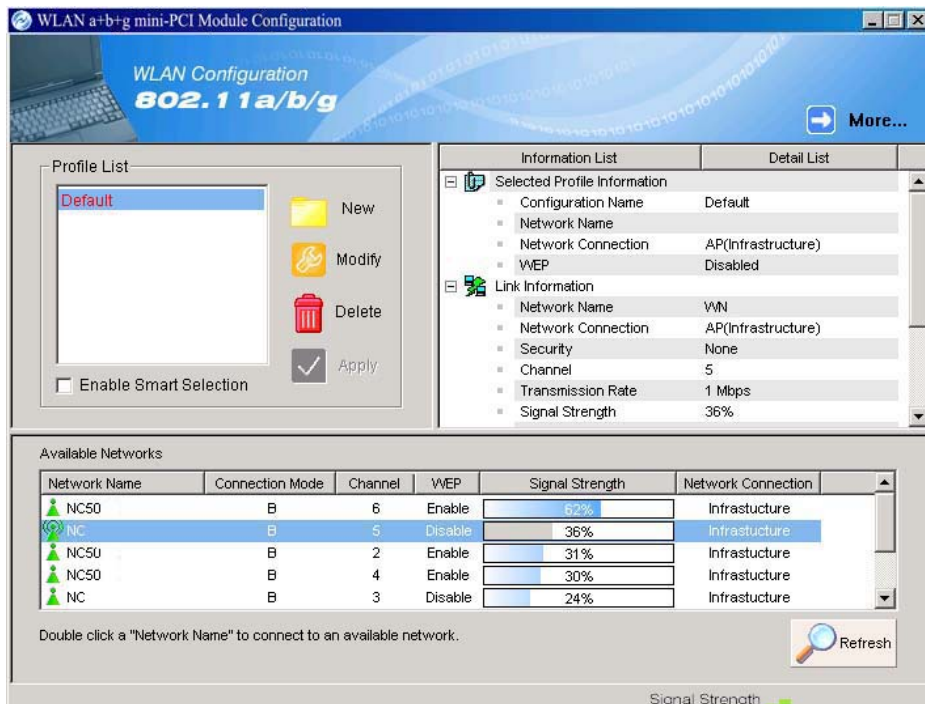- Microsoft® Win™ 2000/ME/98 Second Edition/XP

3. Driver/Utility Installation / Uninstallation

3. Connecting to an Existing Network

1. Double click the shortcut icon of WLAN a+b+g USB2.0 Adapter on the desktop, and the Configuration window appears.
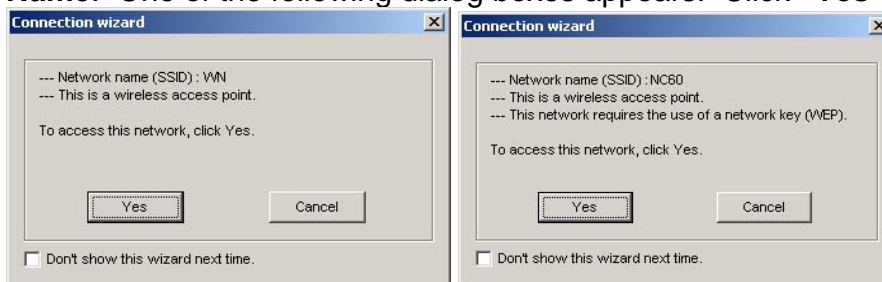

2. Click on the **Refresh** button to list all available networks.

Note! To automatically connect to the network with the strongest signal, select **Enable Smart Selection**. **Any** displays in Profile List.

3. From the list of "Available Networks", choose one network by double clicking the **Network Name**. One of the following dialog boxes appears. Click **"Yes"** to continue.


4. If the chosen network has security enabled, the **Security** tab displays. Select the security option used by the network. Contact the network administrator for the correct settings.
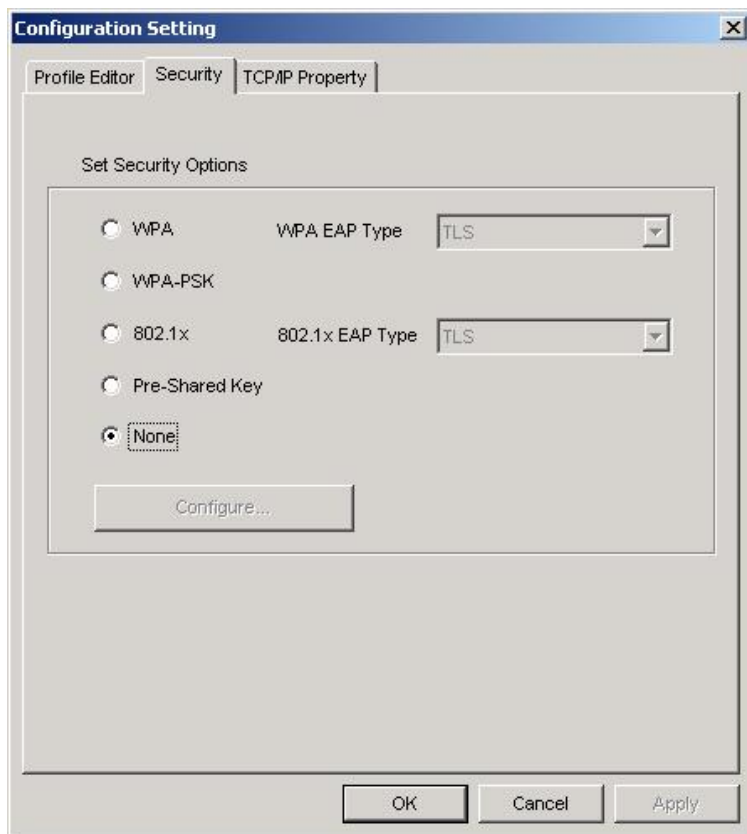
5. If selecting **WPA** or **802.1X**, select the EAP type, then click on the **Configure** button to select the certificate.
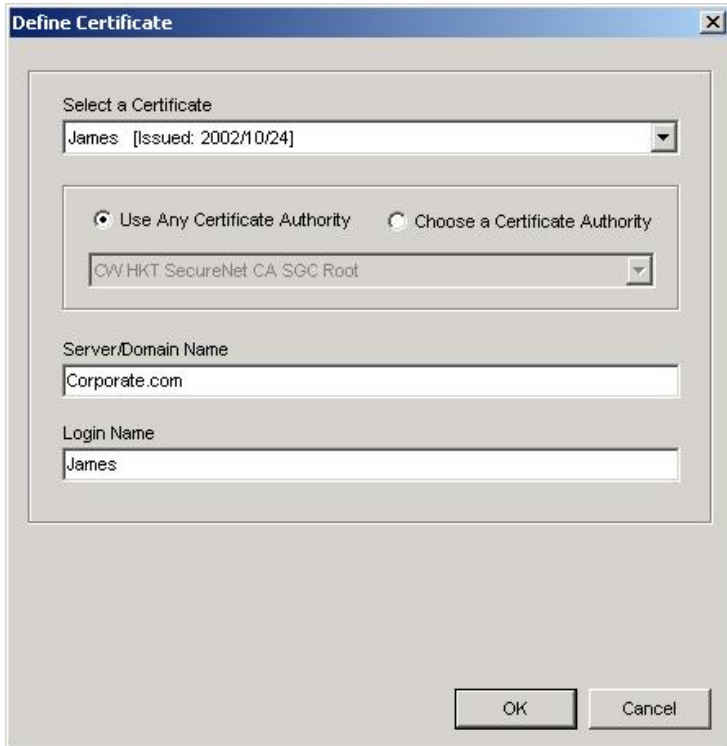
6. If selecting **WPA-PSK**, click on the **Configure** button to enter the PassPhrase.
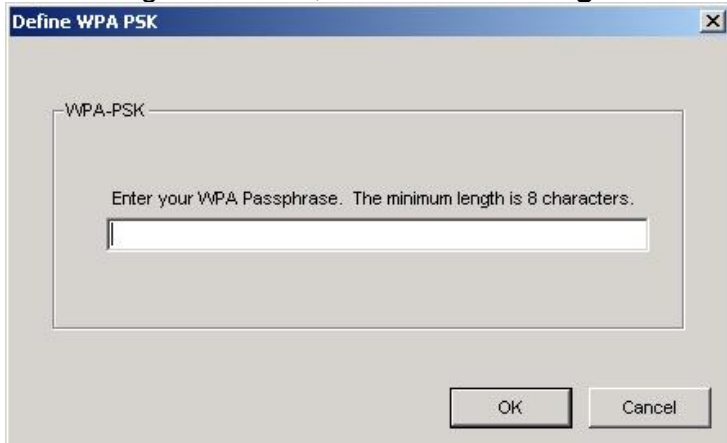
7. If selecting **Pre-Shared Key**, click on the **Configure** button to enter the correct Encryption Keys**.**
   Key entry method:
   a.10hex digits: User must enter 10 hexadecimal digits.
      The hexadecimal define is "0-9" and "A-F".
      ex: 123456abc
   b.5 chars: User must enter 5 characters. ex: ab3#@
   c.13 chars: User must enter 13 characters.
      ex: ab3#@kf08&kdk
   d.16 chars: User must enter 16 characters.
         ex: ab3#@kf08&kdk456
   For WEP key, please contact with MIS administrator.

8. Click on **OK** (or **Apply** if using the other tabs) when done to save the settings.

9. Once connected (the icon or in front of the name of the Connected Network), you can check the signal strength from the icon in the Windows System Tray.

8

Additional Note for Windows XP

In Windows XP, it is recommended that you use the WLAN a+b+g USB2.0 Adapter Configuration Utility. Before using the Utility, please follow the steps below to disable the Windows XP Zero Configuration:

Option 1:

1. Double click the shortcut icon to open the Utility.
2. From the Windows System Tray, you should see the signal icon. Right-click it and select "Disable Zero-Configuration".
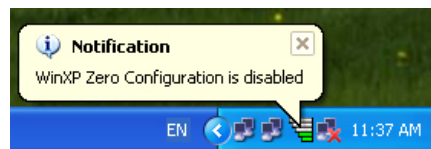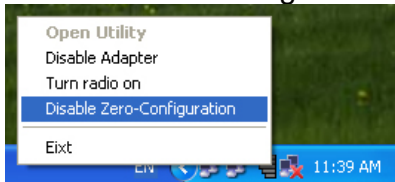
Option 2:

Go to "Control Panel" and double click "Network Connections".

Right-click "Wireless Network Connection" of "WLAN a+b+g USB2.0 Adapter", and select "Properties".
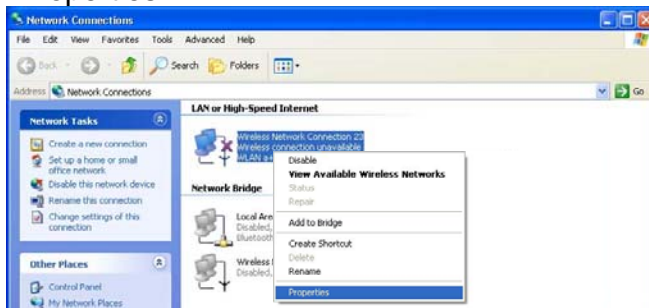
Select "Wireless Networks" tab, and uncheck the check box of "Use Windows to configure my wireless network settings", and then click "OK".
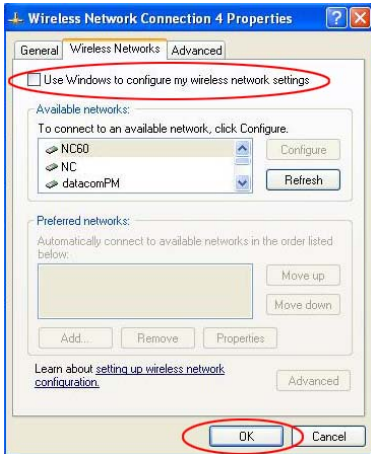
4. Creating an Ad Hoc New Network

NOTE! Ad-hoc mode is available only for 802.11b/g. It is not available for 802.11a. This is a client product and do not have radar detection function specified by FCC. The software will not let you to use ad-hoc under 802.11a.

1. In the Configuration window, click **Ne** [New]
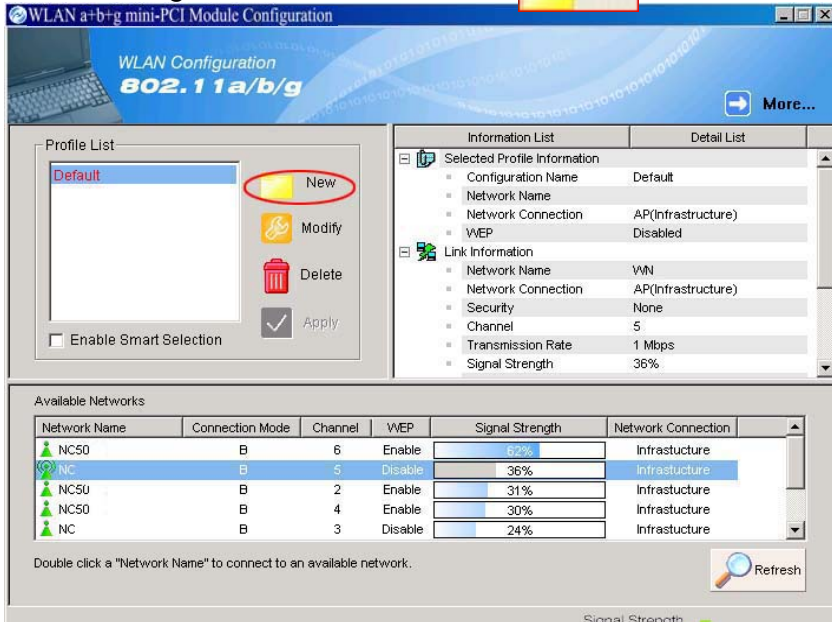
2. Select the "Profile Editor" tab.
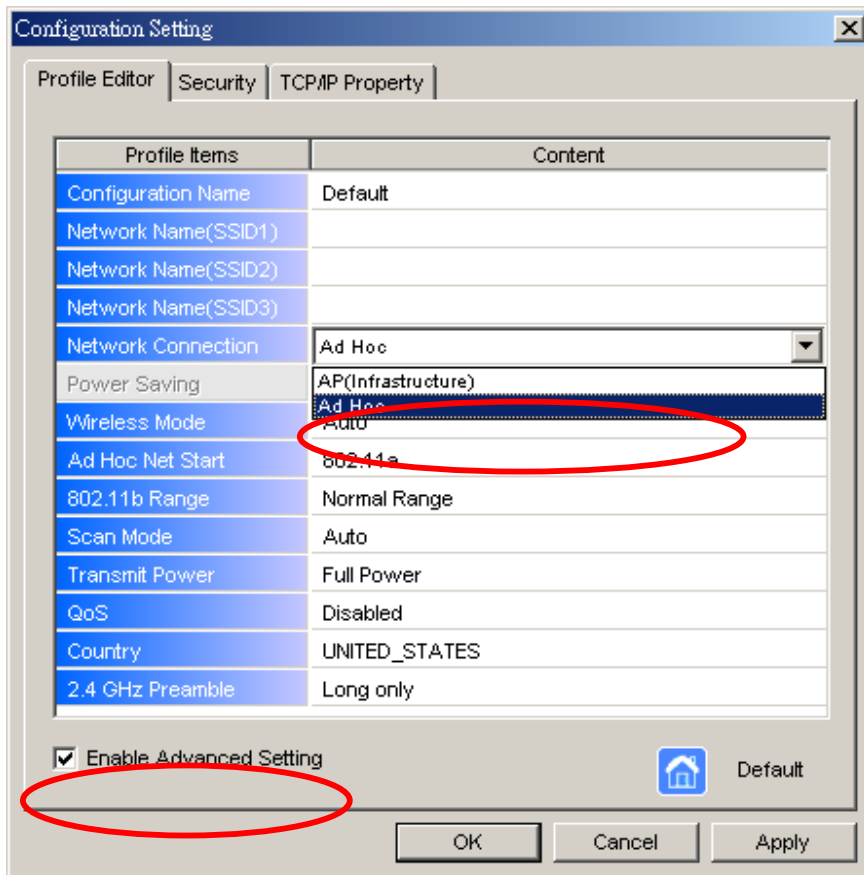
3. Choose the check box of **Enable Advanced Setting** to edit all settings.
4. If joining or creating an Ad-Hoc network, choose **Ad Hoc**.
5. Click **OK** (or **Apply** if using the other tabs) to save the settings.
   For details of each setting, refer to **Modifying a Wireless Network on page 20**.
6. Click the **Security** tab. If not using security, select **None**.

7. If security is used, select **Pre-Shared Key** and click on the **Configure** button.

8. Enter an encryption key in the **Shared: First** field.

9. Click **OK** (or **Apply** if using the other tabs) to save the settings. The new **Network Name** is listed in the **Profile List**.
   The driver does not allow channel selection in Ad-Hoc mode. Instead, the driver starts with an initial channel then checks channel status. If the channel is busy, the driver automatically uses a different channel.

For details of each setting, please see chapter 5.

5. Modifying a Wireless Network

5.1 Infrastructure Mode and Ad Hoc Mode
You can set the Wireless Network Adapter to work in either **Infrastructure mode** or
**Ad Hoc mode**.

NOTE! Ad-hoc mode is available only for 802.11b/g. It is not available for 802.11a. This is
a client product and do not have radar detection function specified by FCC. The software will
not let you to use ad-hoc under 802.11a.

Infrastructure Mode
In infrastructure mode, devices communicate with each other by first going through an Access
Point (AP). Wireless devices can communicate with each other or can communicate with a
wired network. When one AP is connected to wired network and a set of wireless stations, it
is referred to as a BSS (Basic Service Set).
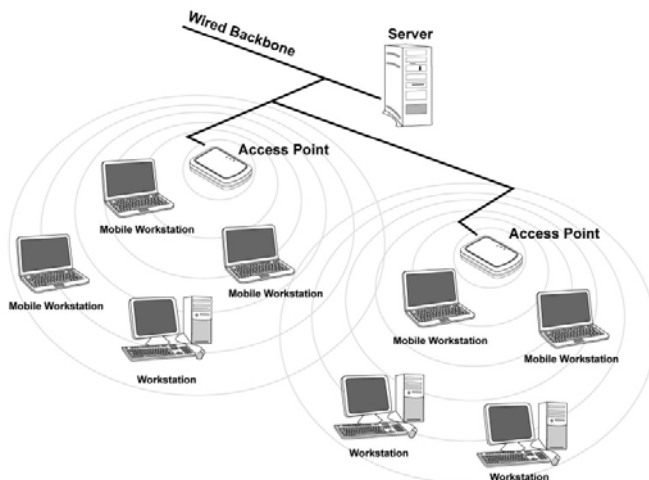
Ad Hoc Mode
Ad-hoc mode is also called "peer-to-peer mode" or "Independent Basic Service Set (IBSS)".
In ad hoc mode, devices communicate directly with each other without using an Access Point
(AP).

NOTE! Ad-hoc mode is available only for 802.11b/g. It is not available for 802.11a. This is
a client product and do not have radar detection function specified by FCC. The software will
not let you to use ad-hoc under 802.11a.
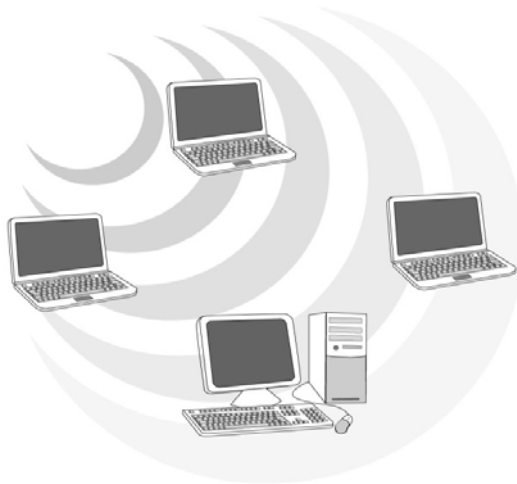
5.2 Modifying a Wireless Network

1. Open "WLAN a+b+g USB2.0 Adapter Configuration" by double clicking the shortcut icon on the desktop.

   Note! If there's no network name listed in the "Profile List", click **Refresh** button and double click a Network Name from **Available Networks**. The chosen Network Name is listed in the Profile List.

2. From the Profile List, select one Profile and click **Modify** button .

3. Select **Profile Editor** tab and edit the settings. Click **OK** to save the modifications.

- ■ **Configuration Name:** This name identifies the configuration. This name should be unique.
- ■ **Network Name (SSID1) (SSID2) (SSID3):** The name of the wireless network. This name cannot be longer than 32 characters. If the field is set to be "ANY" or is left blank, your computer will connect to an AP with the best signal strength.
- ■ **Network Connection:** Specifies the mode of the network. Two options are "Infrastructure" and "Ad Hoc".
- ■ **Power Saving:** Minimizes power consumption while maintaining network connectivity and high data transfer performance. In **Ad Hoc** mode, **Power Savings** function cannot be enabled. The power management options are:
  - • **Off**: PC Card is powered up at all times.
  - • **Normal**: PC Card sleeps less often and stays asleep for a shorter period.
  - • **Maximum**: PC Card sleeps more frequently and stays asleep as much as possible.
- ■ **Wireless Mode:** Three options are "802.11b", "802.11a", "802.11g", "Super A", "Super G" or "Auto". "Auto" allows the use of either 802.11a, 802.11g or 802.11b mode.

NOTE! Ad-hoc mode is available only for 802.11b/g. It is not available for 802.11a. This is a client product and do not have rador detection function specified by FCC. The software will not let you to use ad-hoc under 802.11a.

- **Ad Hoc Net Start:** Specifies a band to establish an Ad Hoc network if no matching SSID is found. Options available are the following: 802.11b and 802.11g.
  NOTE! Ad-hoc mode is available only for 802.11b/g. It is not available for 802.11a. This is a client product and do not have radar detection function specified by FCC. The software will not let you to use ad-hoc under 802.11a.
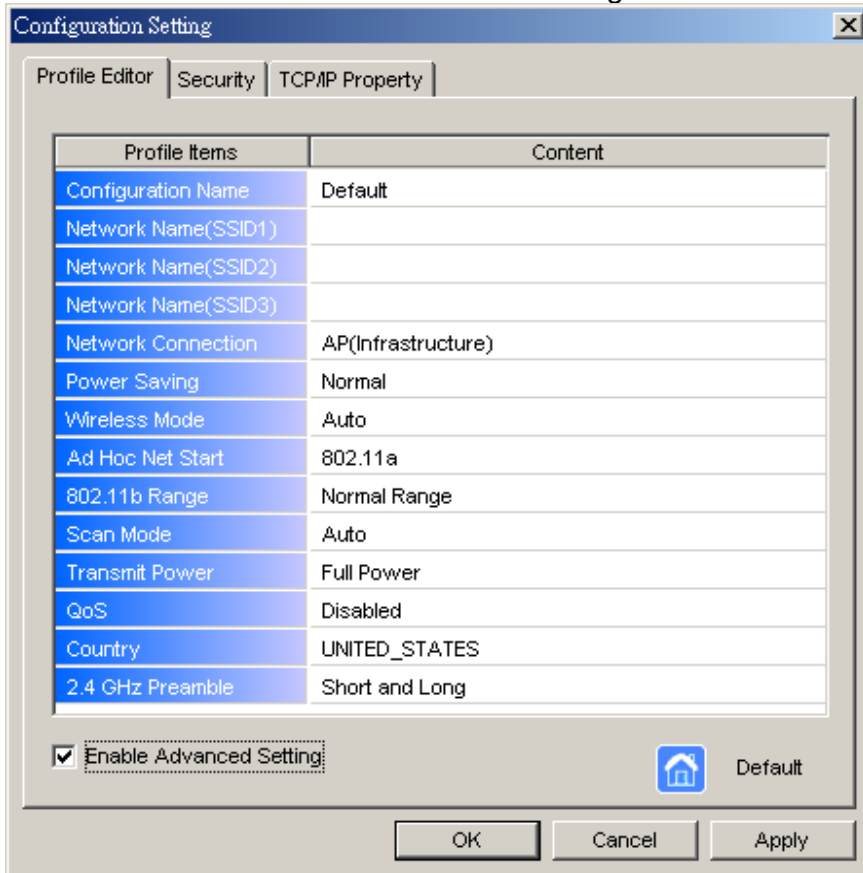- **802.11b Range:** Options are **Normal Range** and **Extended Range**. This function can let user to determine the transfer range in 802.11b mode. Extended Range can prolong the transfer range with a lower data transmitting rate.
- **Scan Mode:** Options are **Active Scan**, **Passive Scan** and **Auto**. In Active Scan, the driver sends out the probe request frames from each channel and collects the response frames from the responding. In Passive Scan, the driver scan each requested channel, listening the beacons on each channel.
- **Transmit Power:** This setting allows you to change the output power of the PC Card to increase or decrease the coverage area.
- **QoS:** Disables or enables the PC Card to cooperate in a network using QoS (Quality of Service).
- **2.4 GHz Preamble:** Allows Ad-Hoc compatibility with other 2.4 GHz devices. Two options are **Short and Long** and **Long only**. Use **Long Only** when configuring the client for an 802.11b RoamAbout AP wireless network.

4. Select **Security** tab and choose the security mode.
   Note! *Check with your Network Administrator for the security features supported by your AP.*

- ■ **WPA:** Enables the use of WiFi protected Access (WPA). This option requires IT administration.
   a) Select **WPA** to open the WPA EAP drop-down menu. The options includes TLS and PEAP.
   b) Click on the **Configure** button and complete the configuration information in the Define Certificate dialog.
- ■ **WPA-PSK:** Enables the WPA-Pre Shared Key (PSK). Click on the **Configure** button and complete the configuration information in the WPA Passphrase dialog.
- ■ **802.1x:** Enables 802.1x security. This option requires IT administration.
   a) Select **802.1x** to open the 802.1x EAP drop-down menu. The options include TLS and PEAP.
   b) Click on the **Configure** button and complete the configuration information in the Define Certificate dialog.

- **Pre-Shared Key:** Enables the use of pre-shared keys that are defined on the AP and the station.
  a) Select the **Pre-Shared Key** radio button.
  b) Click on the **Configure** button and complete the configuration information in the Define Certificate dialog.
- **None:** No security.

5.   Define the Certificate.
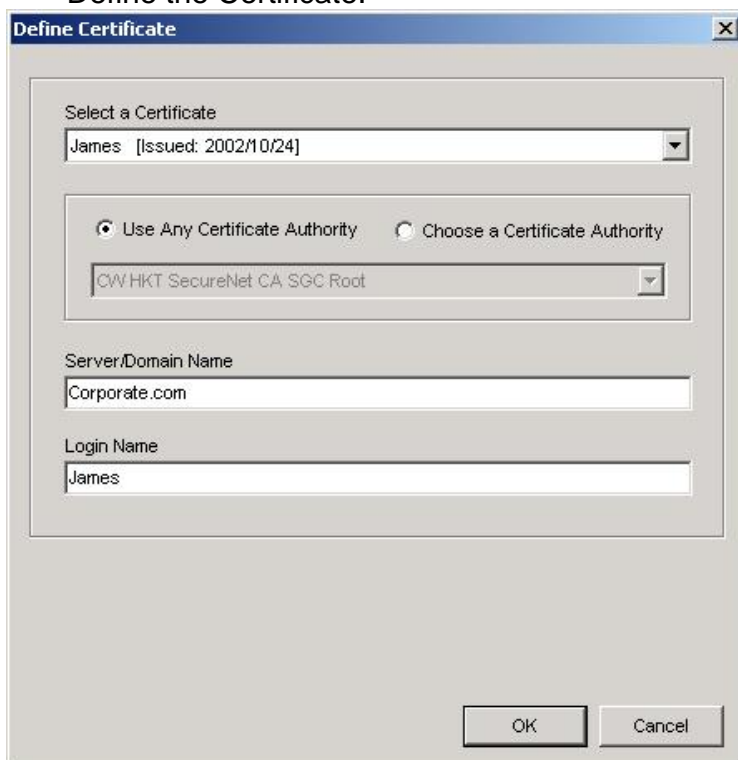
- **Select a Certificate:** Select the Certificate to Authenticate to the RADIUS server from the drop-down menu.
- **Use any Certificate Authority:** The Default Setting. Select this radio button to use any Certificate Authority (CA) for authentication.
- **Choose a Certificate Authority:** Select this radio button to choose the desired Certificate Authority for authentication from the drop-down menu.
- **Server/Domain Name:** The the RADIUS server name or the domain name used for the network access.
- **Login Name:** The username used to log into the server or domain.
- **Define User Information (PEAP)**: Click on the **Define User Information** button and complete the configuration information in the Define User Information dialog.

6. If selecting **WPA-PSK**, click on the **Configure** button to enter the PassPhrase. The PassPhrase must be a minimum of 8 printable ASCII characters. The PassPhrase

should be at least 20 characters to make it more difficult for an attacker to decipher the key.

7. If selecting **Pre-Shared Key**, click on the **Configure** button to enter the Encryption Keys.When finished, click **OK**. For WEP key, please contact with MIS administrator.

■ **Key Entry Method:** Determines the entry method for the key. Hexadecimal (0-9, A-F) or ASCII text (all keyboard characters).

■ **Default Encryption Key:** Allows you to choose one encryption key (First, Second, Third, or Fourth) as the transmit key, which encrypts transmissions from the PC Card.

■ **Unique Key:** Defines the per-session encryption key for the current network configuration. Not used in Ad-Hoc mode.

■ **Shared Keys:** Use these fields to enter the wireless network's encryption keys. The keys must be in the correct position (First, Second, Third, or Fourth).

■ **Key Length:** Defines the length of each encryption key.
   o For 40/64 bit (enter 10 digits for hexadecimal or 5 characters for ASCII)
   o For 104/128 bit (Enter 26 digits for hexadecimal or 13 characters for ASCII)

When the length is changed, the number of available characters in the field automatically changes. If a previously entered key is too long, the key is

automatically truncated to fit. If the key length is increased again, the key does not update to the previous value.

8. Click **OK** to save the settings.

9. Select "TCP/IP Property" tab. Enter the settings and click "OK" to save the settings.
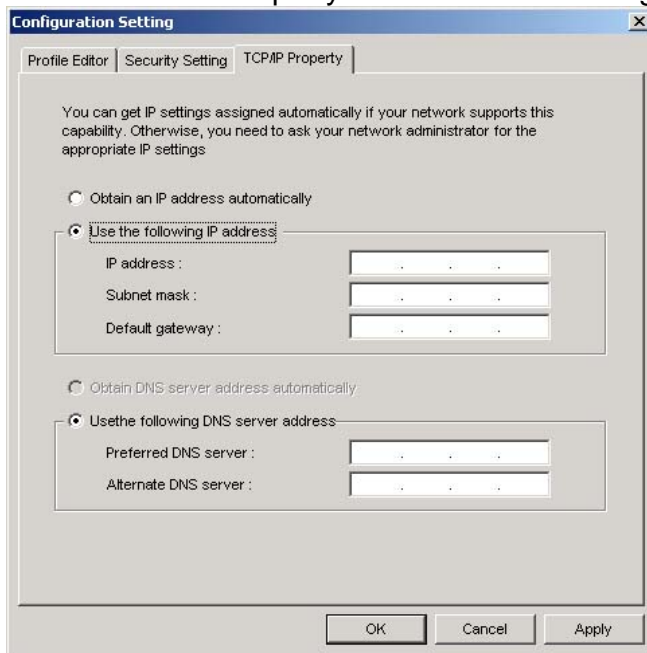
■ If the network uses DHCP server, choose **Obtain an IP address automatically**.
■ If the network does not use DHCP server, choose **Use the following IP address** to set the relative settings. For the IP configuration information, please contact the network administrator.

FCC Statement:

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.

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.

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.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

This device is restricted for indoor use.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

IC Statement:

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause
undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures.
Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

Dynamic Frequency Selection (DFS) for devices operating in the bands 5250- 5350 MHz, 5470-5600 MHz and 5650-5725 MHz
Sélection dynamique de fréquences (DFS) pour les dispositifs fonctionnant dans les bandes 5250-5350 MHz, 5470-5600 MHz et 5650-5725 MHz

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une
utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Users should also be advised that high-power radars are allocated as primary users (i.e. priority
users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.
De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.
For indoor use only.

Pour une utilisation en intérieur uniquement.

IMPORTANT NOTE:
IC Radiation Exposure Statement:
This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.
Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.