Wistron NeWeb Corporation
20 Park Avenue II, Hsinchu Science Park, Hsinchu 308, Taiwan, R.O.C.
Phone: 886-3-666-7799 Fax: 886-3-666-7711
Website: www.wneweb.com

User Manual

Model Name: DNUB-F1

Wistron NeWeb

Wistron NeWeb Corporation
20 Park Avenue II, Hsinchu Science Park, Hsinchu 308, Taiwan, R.O.C.
Phone: 886-3-666-7799 Fax: 886-3-666-7711
Website: www.wneweb.com

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

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

IMPORTANT NOTE:

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

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 20cm between the radiator & your body.

This device is intended only for OEM integrators under the following conditions:

The antenna must be installed such that 20 cm is maintained between the antenna and users, and
The transmitter module may not be co-located with any other transmitter or antenna.
As long as 2 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed

IMPORTANT NOTE:

In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: “Contains FCC ID: NKR-F1”. The grantee's FCC ID can be used only when all FCC compliance requirements are met.

Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user’s manual of the end product which integrates this module.
The end user manual shall include all required regulatory information/warning as show in this manual.

IC Statement

This device complies with RSS-210 of the Industry Canada 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.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution :

(i) 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;

(ii) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the e.i.r.p. limit; and

(iii) the maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.

(iv) 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.

Wistron NeWeb

Wistron NeWeb Corporation
20 Park Avenue II, Hsinchu Science Park, Hsinchu 308, Taiwan, R.O.C.
Phone: 886-3-666-7799 Fax: 886-3-666-7711
Website: www.wneweb.com

Avertissement:

Le guide d'utilisation des dispositifs pour réseaux locaux doit inclure des instructions précises sur les restrictions susmentionnées, notamment :

(i) les dispositifs fonctionnant dans la bande 5 150-5 250 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;

(ii) le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5 250-5 350 MHz et 5 470-5 725 MHz doit se conformer à la limite de p.i.r.e.;

(iii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5 725-5 825 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

(iv) 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 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

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 20cm de distance entre la source de rayonnement et votre corps.

This device is intended only for OEM integrators under the following conditions: (For module device use)
1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
2) The transmitter module may not be co-located with any other transmitter or antenna.

As long as 2 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed.

Cet appareil est conçu uniquement pour les intégrateurs OEM dans les conditions suivantes: (Pour utilisation de dispositif module)
L'antenne doit être installée de telle sorte qu'une distance de 20 cm est respectée entre l'antenne et les utilisateurs, et
Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

Tant que les 2 conditions ci-dessus sont remplies, des essais supplémentaires sur l'émetteur ne seront pas nécessaires. Toutefois, l'intégrateur OEM est toujours responsable des essais sur son produit final pour toutes exigences de conformité supplémentaires requis pour ce module installé.

IMPORTANT NOTE:
In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the Canada authorization is no longer considered valid and the IC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate Canada authorization.

NOTE IMPORTANTE:
Dans le cas où ces conditions ne peuvent être satisfaites (par exemple pour certaines configurations d'ordinateur portable ou de certaines co-localisation avec un autre émetteur), l'autorisation du Canada n'est plus considéré comme valide et l'ID IC ne peut pas être utilisé sur le produit final. Dans ces circonstances, l'intégrateur OEM sera chargé de réévaluer le produit final (y compris l'émetteur) et l'obtention d'une autorisation distincte au Canada.

End Product Labeling
This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: “Contains IC: 4441A-F1”.

Plaque signalétique du produit final
Ce module émetteur est autorisé uniquement pour une utilisation dans un dispositif où l'antenne peut être installée de telle sorte qu'une distance de 20cm peut être maintenue entre l'antenne et les utilisateurs. Le produit final doit être étiqueté dans un endroit visible avec l'inscription suivante: "Contient des IC: 4441A-F1".

Manual Information To the End User
The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user’s manual of the end product which integrates this module.
The end user manual shall include all required regulatory information/warning as show in this manual.

Manuel d'information à l'utilisateur final
L'intégrateur OEM doit être conscient de ne pas fournir des informations à l'utilisateur final quant à la façon d'installer ou de supprimer ce module RF dans le manuel de l'utilisateur du produit final qui intègre ce module.
Le manuel de l'utilisateur final doit inclure toutes les informations réglementaires requises et avertissements comme indiqué dans ce manuel.

Wistron NeWeb

Wistron NeWeb Corporation
20 Park Avenue II, Hsinchu Science Park, Hsinchu 308, Taiwan, R.O.C.
Phone: 886-3-666-7799 Fax: 886-3-666-7711
Website: www.wneweb.com

1. General Description

The DNUB-O1 module is 802.11n sign-chip solutions for USB dongle. It's very small and cost-effective modules which can bundle with PCs, 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

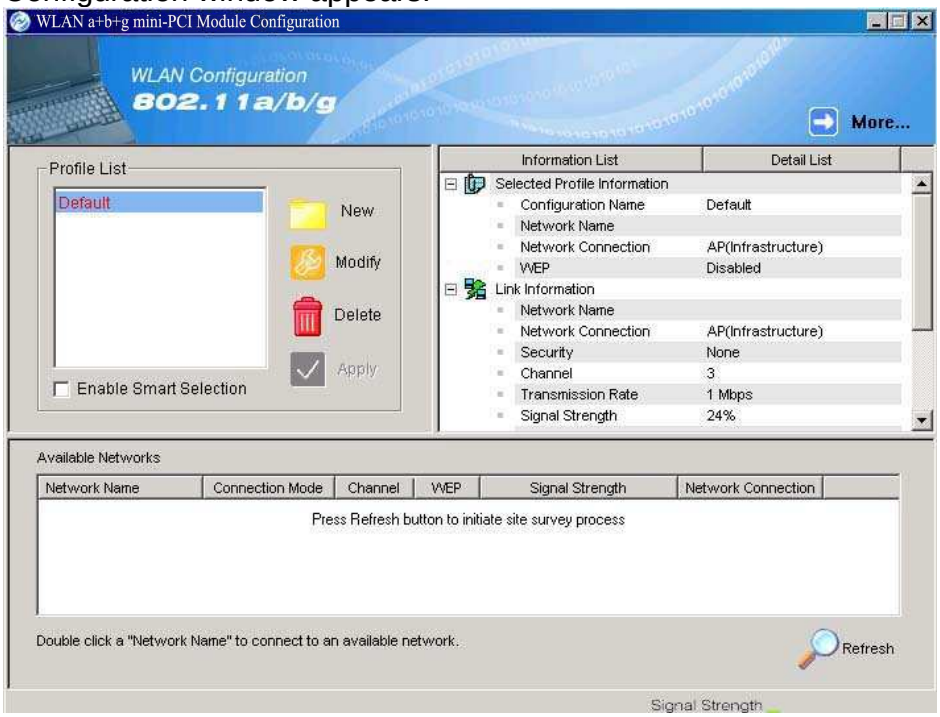
- A laptop PC contains:
  - 32 MB memory or greater
  - 300 MHz processor or higher
- Microsoft® Win™2000/ME/98 Second Edition/XP

Wistron NeWeb Corporation
20 Park Avenue II, Hsinchu Science Park, Hsinchu 308, Taiwan, R.O.C.
Phone: 886-3-666-7799 Fax: 886-3-666-7711
Website: www.wneweb.com

3. Driver/Utility Installation / Uninstallation

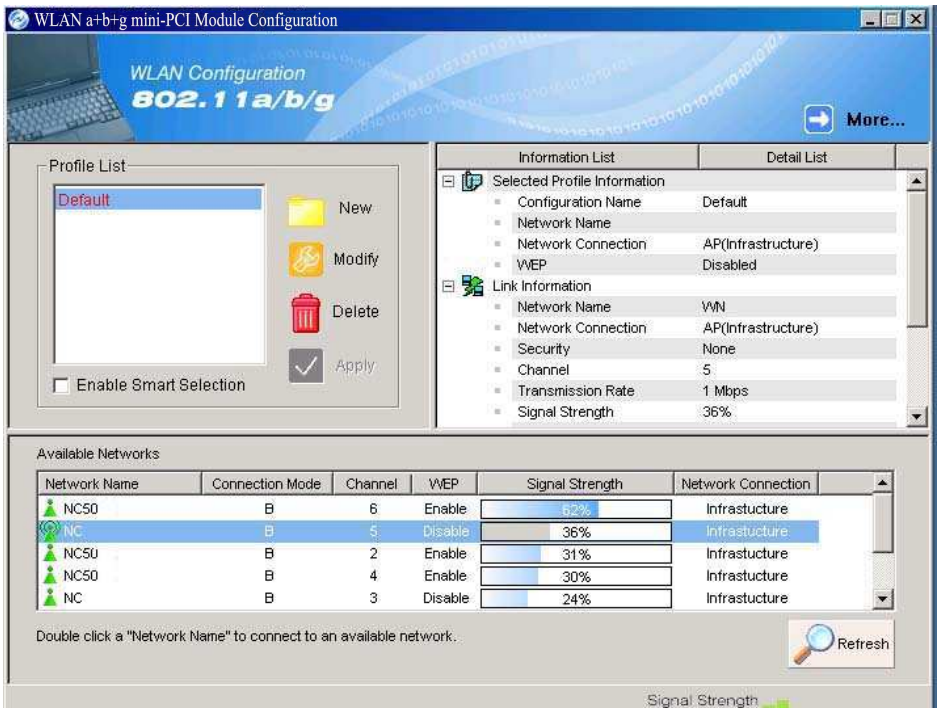
3. Connecting to an Existing Network

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** butto 

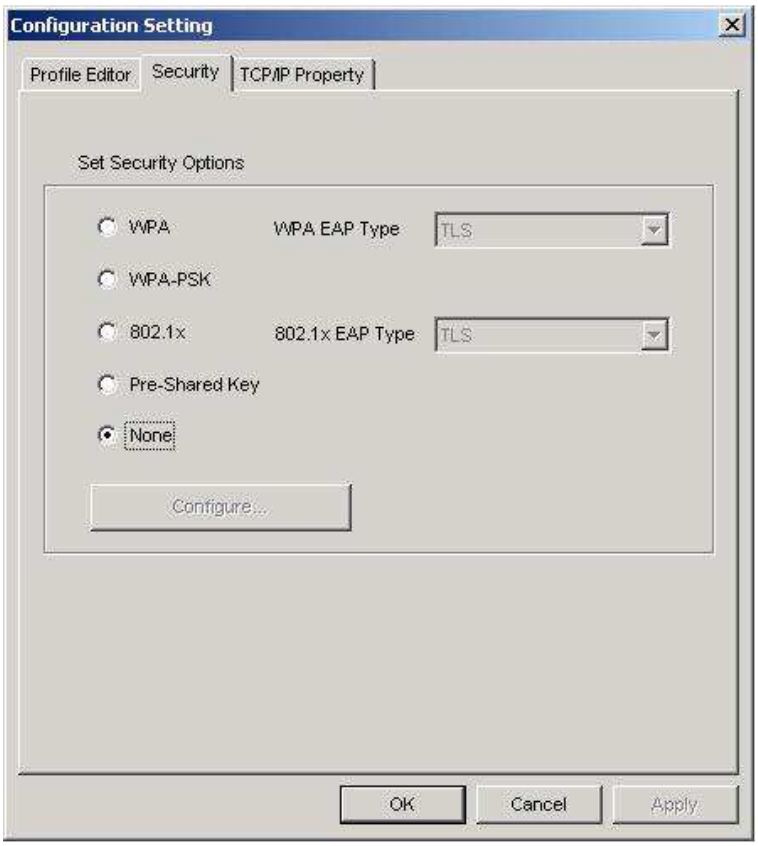
o list all available networks.



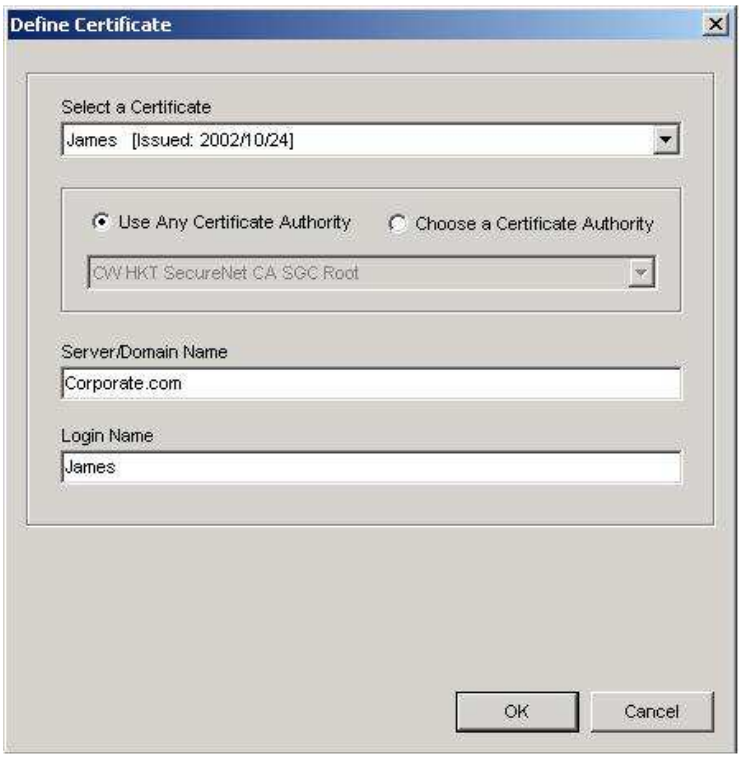
Note! To automatically connect to the network with the strongest signal, select **Enable Smart Selection**. **Any** displays in Profile List.

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.

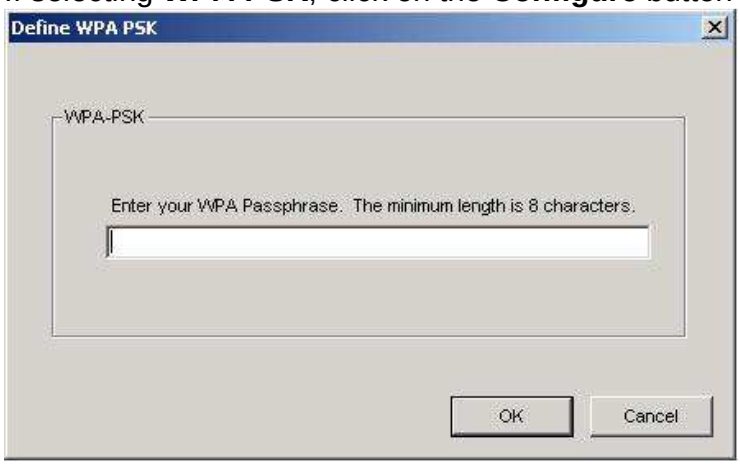
4. If the chosen network has security enabled, the **Security** tab displays. Select the security option used by the network. Contact the network administrator for the correct settings.



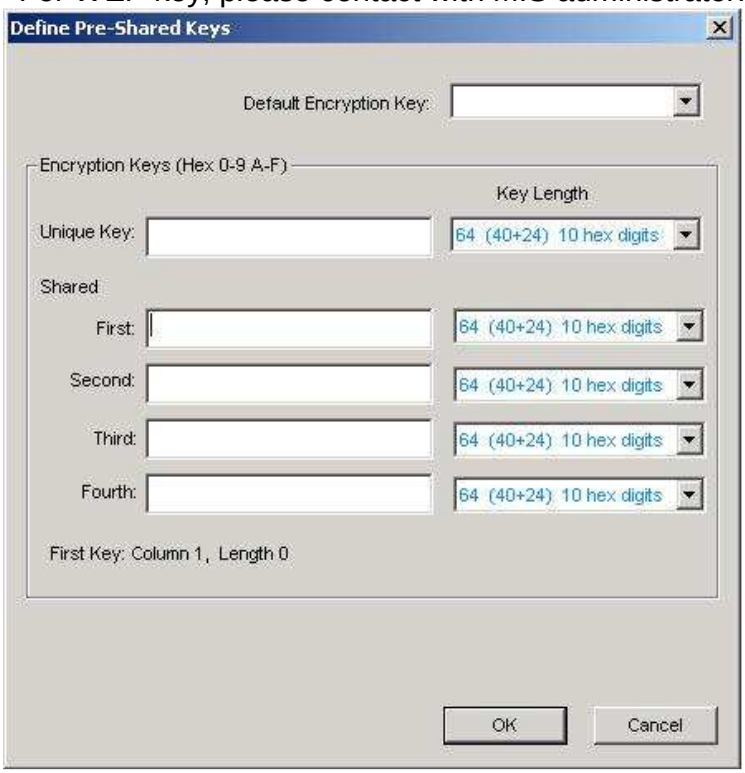
5. If selecting **WPA** or **802.1X**, select the EAP type, then click on the **Configure** button to select the certificate.



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.

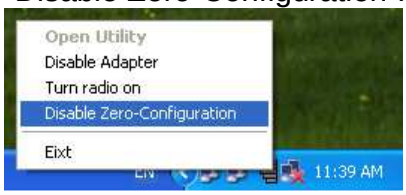
Wistron NeWeb Corporation
20 Park Avenue II, Hsinchu Science Park, Hsinchu 308, Taiwan, R.O.C.
Phone: 886-3-666-7799 Fax: 886-3-666-7711
Website: www.wneweb.com

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:

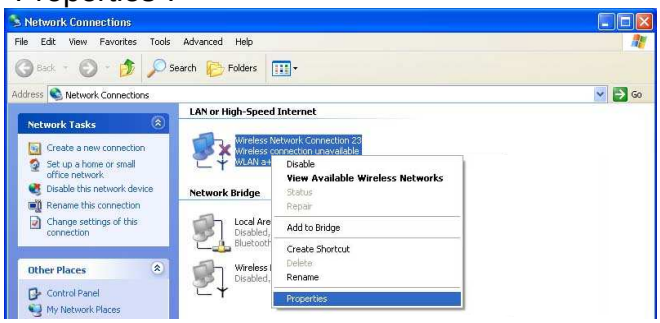
1. Double click the shortcut icon to open the Utility.
2. From the Windows System Tray, you should see the signal icon. Right-click it and select "Disable Zero-Configuration".



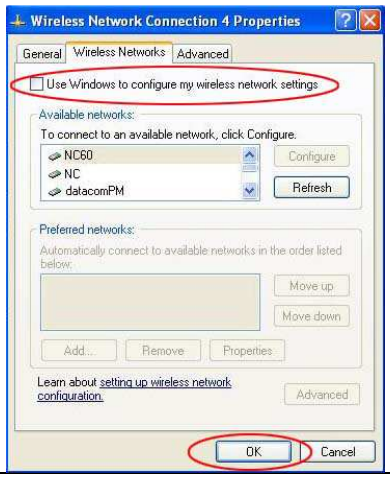
Option 2:

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".



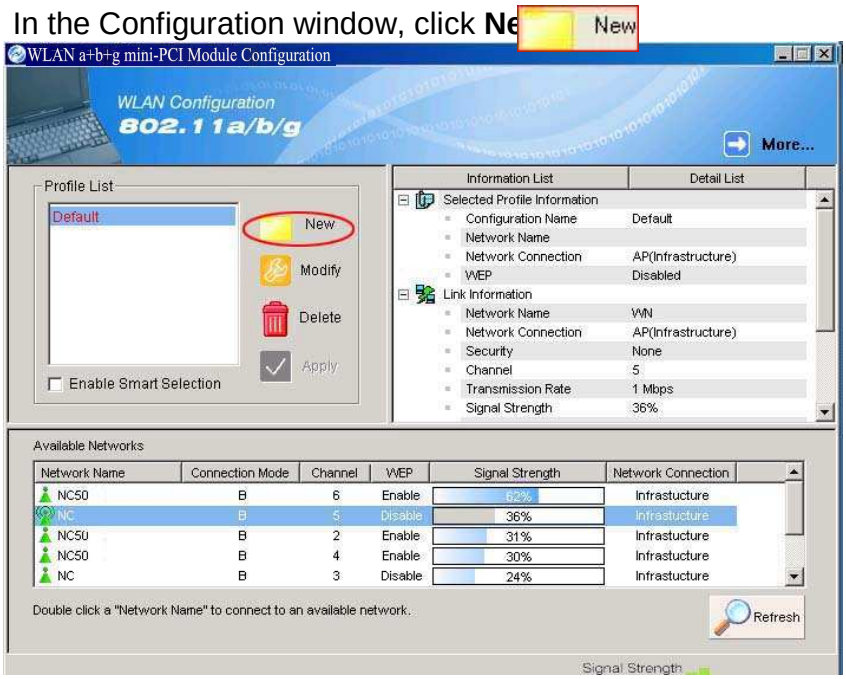
Select "Wireless Networks" tab, and uncheck the check box of "Use Windows to configure my wireless network settings", and then click "OK".



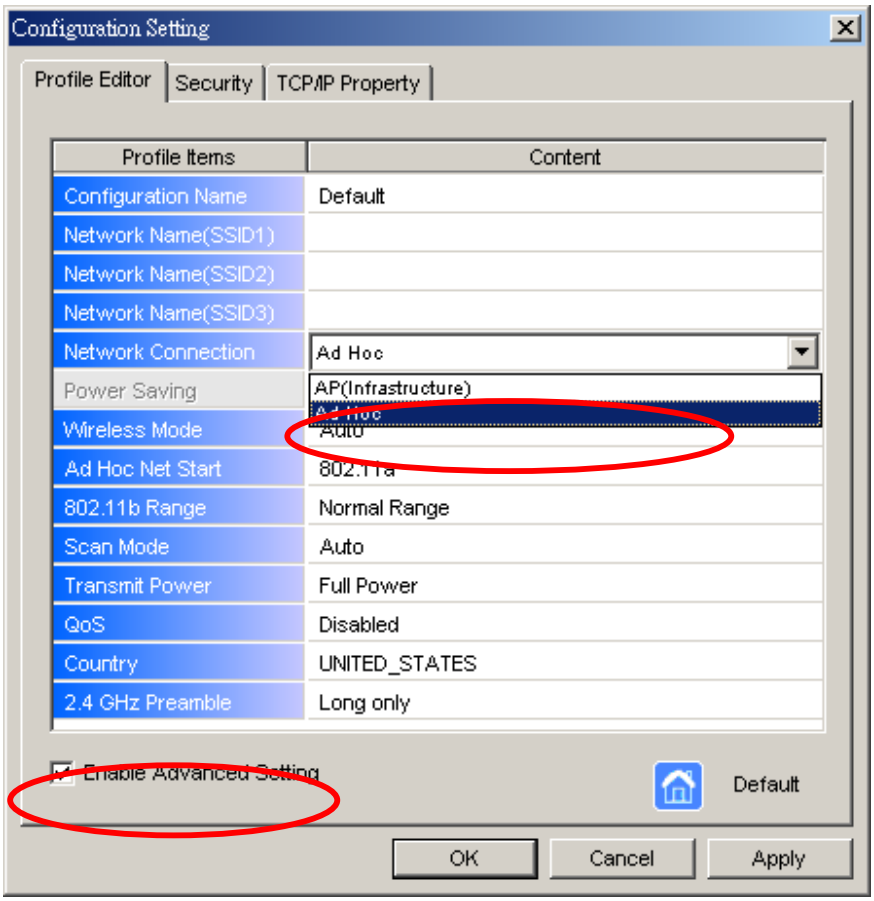
4. Creating an Ad Hoc New Network

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.

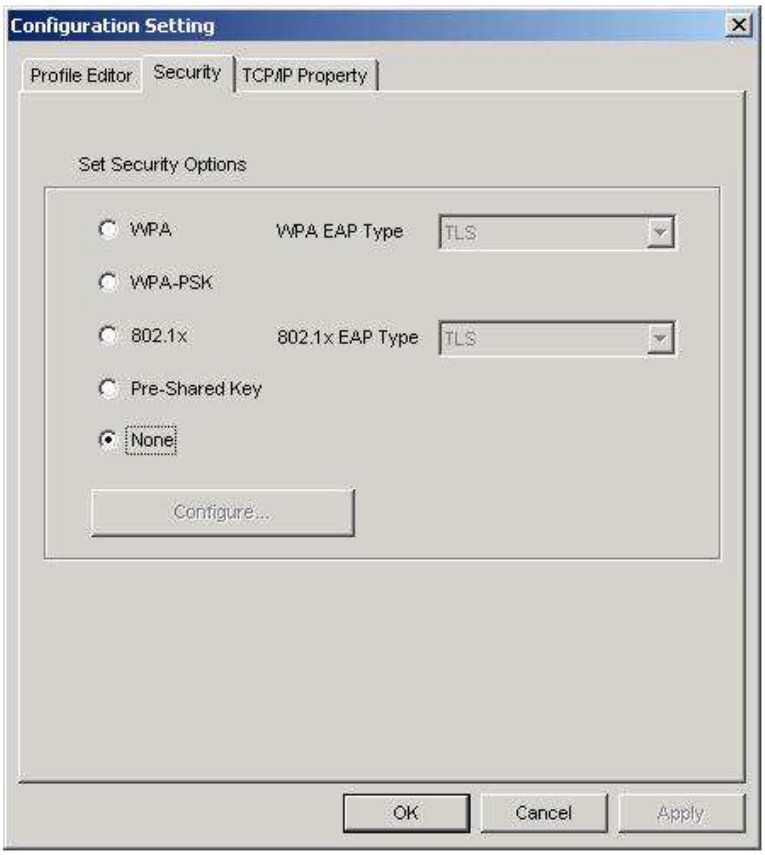
1. In the Configuration window, click **Ne**



2. Select the “Profile Editor” tab.

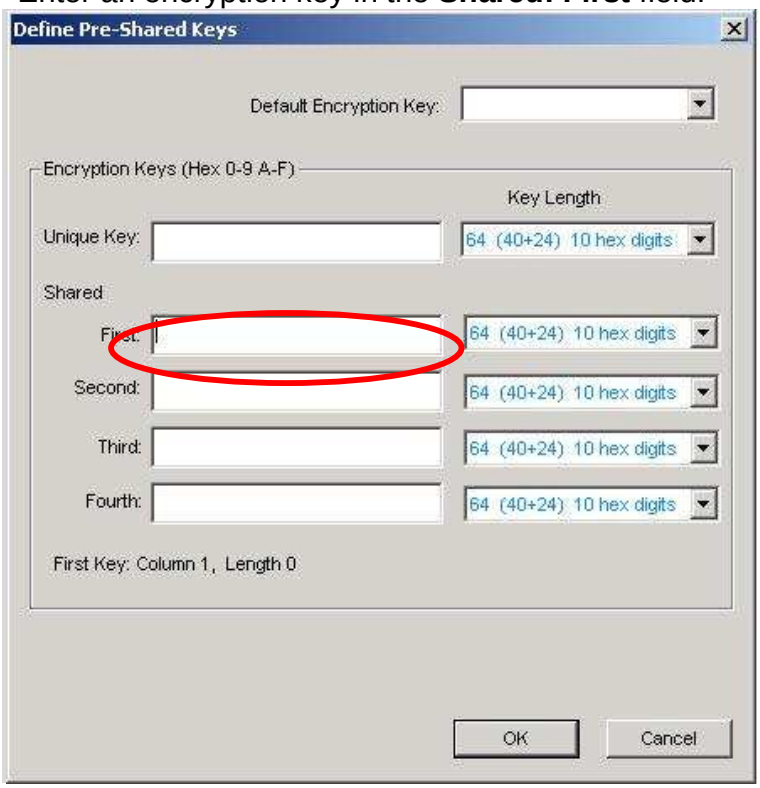


3. Choose the check box of **Enable Advanced Setting** to edit all settings.
4. If joining or creating an Ad-Hoc network, choose **Ad Hoc**.
5. Click **OK** (or **Apply** if using the other tabs) to save the settings.
   For details of each setting, refer to **Modifying a Wireless Network on page 20**.
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.

Wistron NeWeb Corporation
20 Park Avenue II, Hsinchu Science Park, Hsinchu 308, Taiwan, R.O.C.
Phone: 886-3-666-7799 Fax: 886-3-666-7711
Website: www.wneweb.com

5. Modifying a Wireless Network

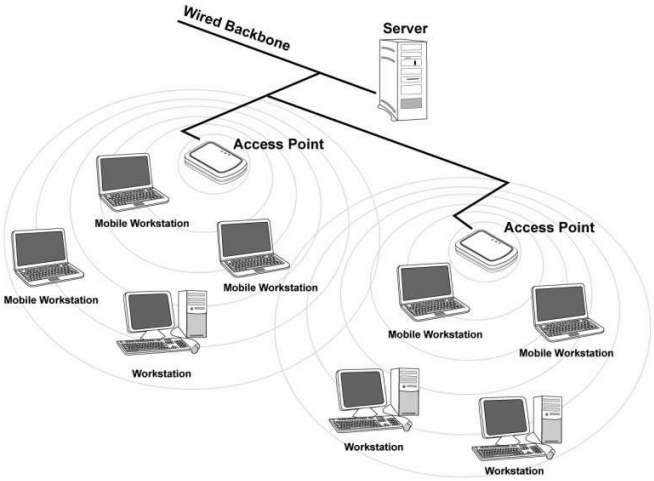
5.1 Infrastructure Mode and Ad Hoc Mode

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.

Wistron NeWeb

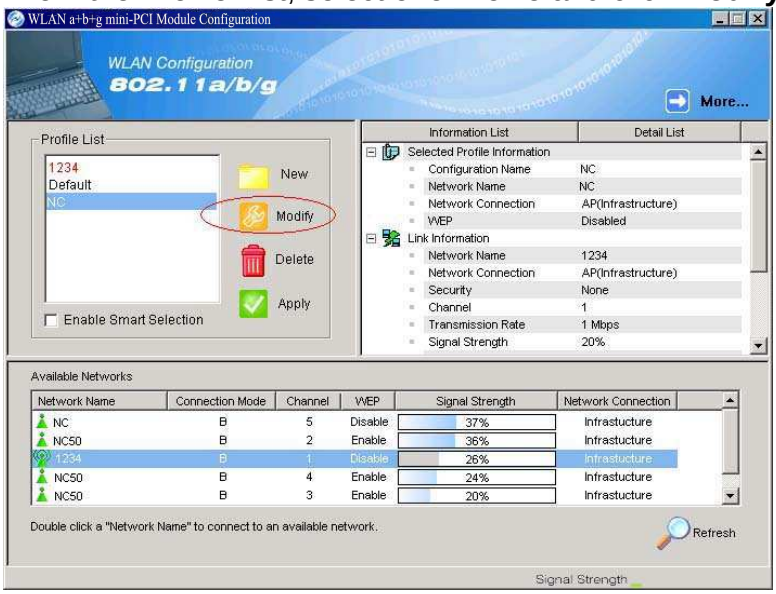
Wistron NeWeb Corporation
20 Park Avenue II, Hsinchu Science Park, Hsinchu 308, Taiwan, R.O.C.
Phone: 886-3-666-7799 Fax: 886-3-666-7711
Website: www.wneweb.com

5.2 Modifying a Wireless Network

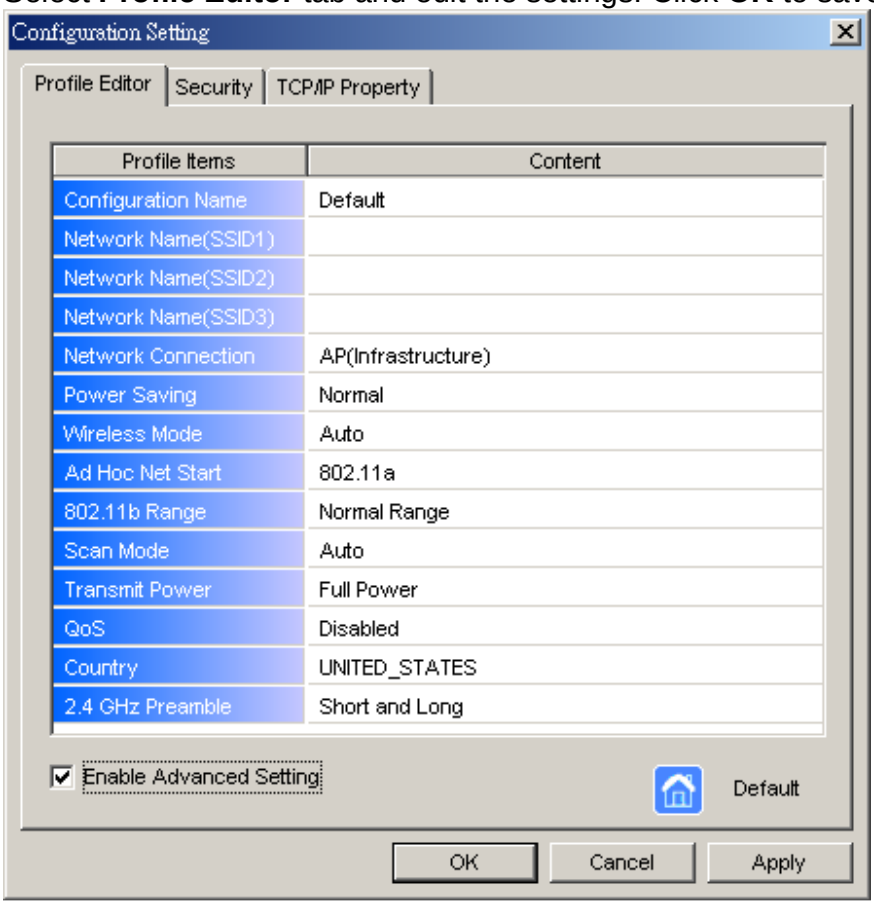
1. Open "WLAN a+b+g USB2.0 Adapter Configuration" by double clicking the shortcut icon on the desktop.

   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.

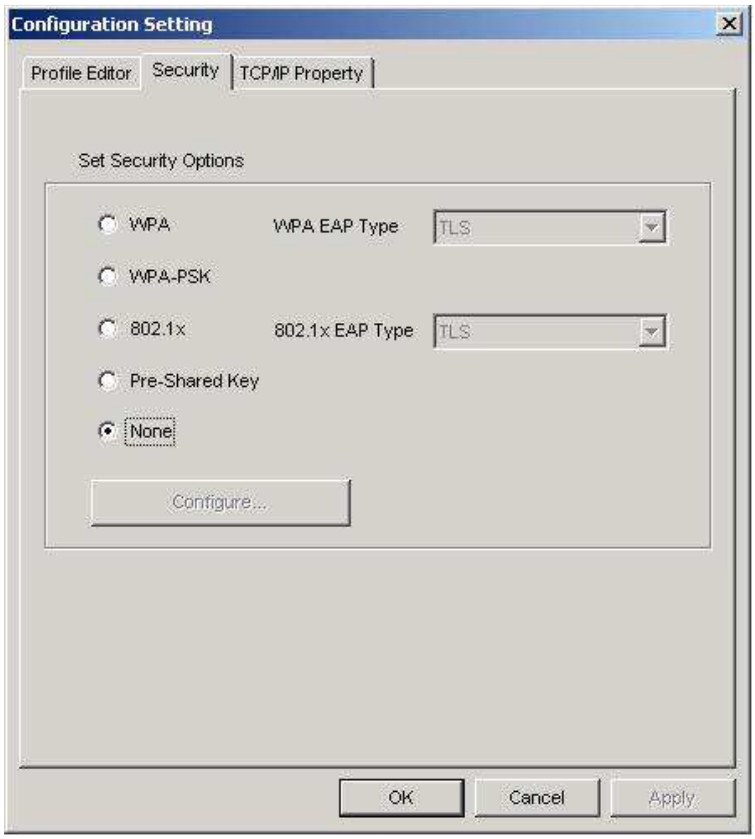


- **Configuration Name:** This name identifies the configuration. This name should be unique.
- **Network Name (SSID1) (SSID2) (SSID3):** The name of the wireless network. This name cannot be longer than 32 characters. If the field is set to be “ANY” or is left blank, your computer will connect to an 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.

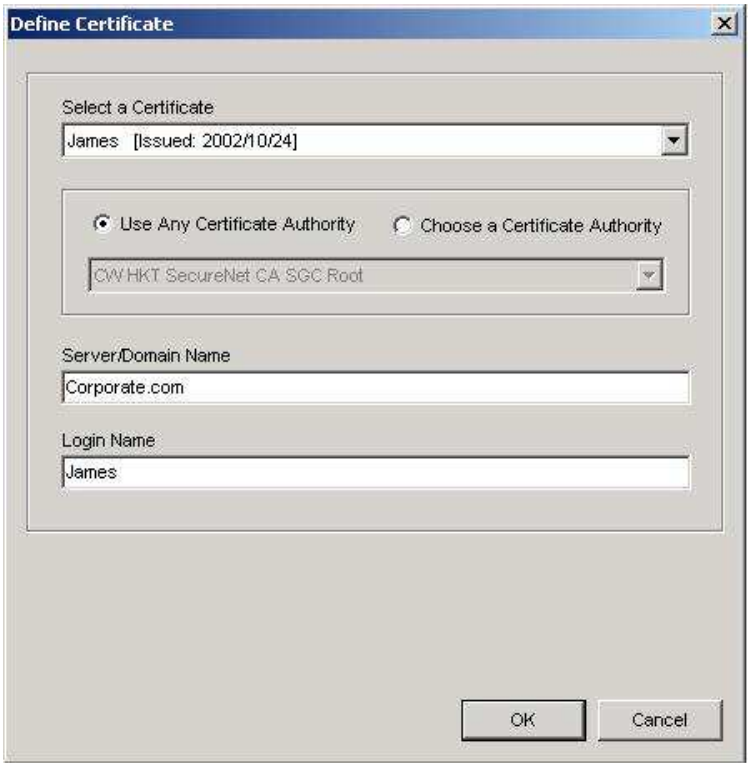
4. Select **Security** tab and choose the security mode.
   Note! *Check with your Network Administrator for the security features supported by your AP.*



- **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.

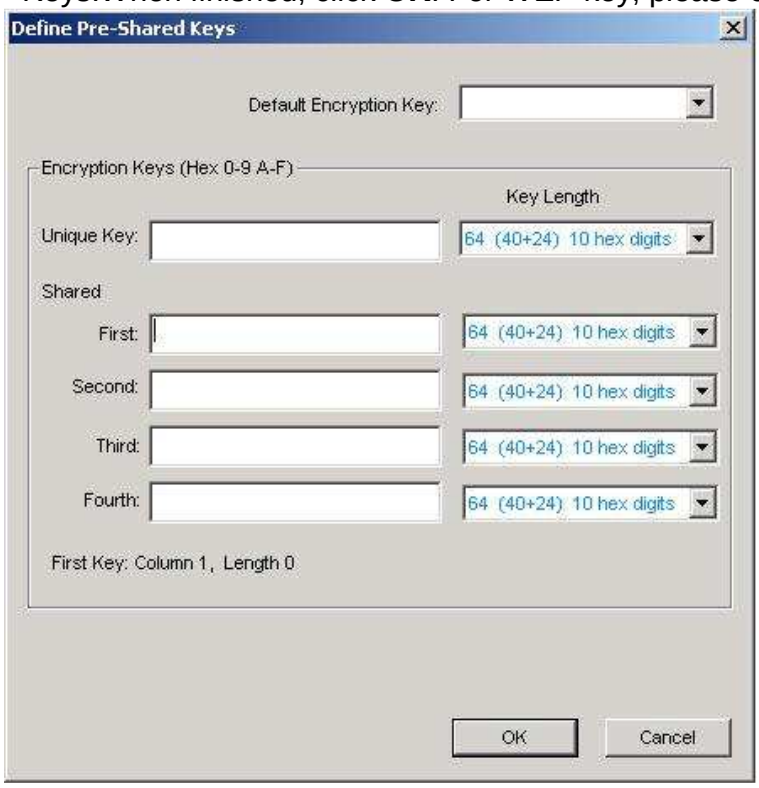


- **Select a Certificate:** Select the Certificate to Authenticate to the RADIUS server from the drop-down menu.
- **Use any Certificate Authority:** The Default Setting. Select this radio button to use any Certificate Authority (CA) for authentication.
- **Choose a Certificate Authority:** Select this 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.



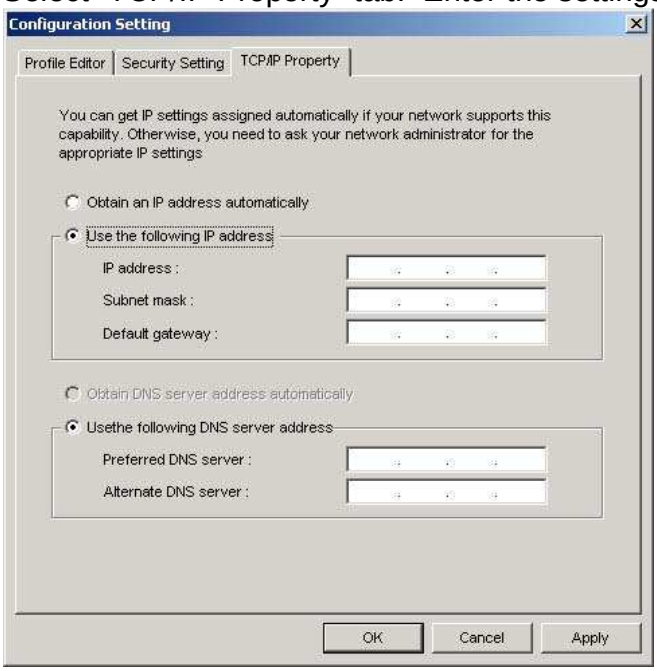
- **Key Entry Method:** Determines the entry method for the key. Hexadecimal (0-9, A-F) or ASCII text (all keyboard characters).
- **Default Encryption Key:** Allows you to choose one encryption key (First, Second, Third, or Fourth) as the transmit key, which encrypts transmissions from the PC Card.
- **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.