KEEBOX

User's Guide

Wireless 150 N USB Adapter

W150NU

V1

Table of Contents

Product Overview **1**
Package Contents 1
System Requirements 1
Introduction 2
Wireless Tips 3
Features 5
Hardware Overview 6
Installation Procedure **7**
System Preparation 7
Removing Existing Wireless Adapter Installation *7*
Disabling Other Wireless Adapters *8*
Installing the Wireless Adapter 11
Adapter Configuration 16
KEEBOX 150N Wireless Utility *16*
Available Network *17*
Profile Management *18*
Creating a Wireless Profile *19*
Creating a Basic Security Wireless Profile 20
Creating a Basic Security Wireless Profile- Open \ WEP 21
Creating a Basic Security Wireless Profile- Shared \ WEP 22
Creating a Basic Security Wireless Profile- WPA-PSK \ TKIP 23
Creating a Basic Security Wireless Profile- WPA-PSK \ AES 24
Creating a Basic Security Wireless Profile- WPA2-PSK \ TKIP 25
Creating a Basic Security Wireless Profile- WPA2-PSK \ AES 26
Creating an Advanced Security Wireless Profile 27
Creating an Advanced Security Wireless Profile-Open Authentication 29
Creating an Advanced Security Wireless Profile-Shared Authentication 30
Creating an Advanced Security Wireless Profile-WPA-EAP (Enterprise) Authentication 31
Creating an Advanced Security Wireless Profile-WPA-PSK (Personal) Authentication 33
Creating an Advanced Security Wireless Profile-WPA2-EAP (Enterprise) Authentication 34
Creating an Advanced Security Wireless Profile-WPA2-PSK (Personal) Authentication 36
Enabling and Configuring 802.1x Parameter for a Wireless Profile 37
Configuring 802.1x Validate Server Certificate Settings 38

Editing a Wireless Profile *39*
WPS Push Button Configuration (PBC) *40*
WPS PIN Code *42*
About *43*
Technical Specifications **44**

Product Overview

Package Contents

- W150NU
- CD-ROM with Utility & Driver
- Multi-Language Quick Installation Guide

System Requirements

Computer

- CD-ROM Drive
- Available USB 2.0 port
- Windows 2000 (Service Pack 4), Windows XP (Service Pack 2), Windows Vista, or Windows 7

Introduction

- A convenient method for connecting a PC or notebook to a wireless network.
- High speed wireless n adapter in an ultra compact housing
- Plug into any USB port on a laptop or desktop computer to upgrade to wireless n connectivity
- Surf the Web, stream music, play online games, and make Internet calls
- Features Wi-Fi Protected Setup (WPS): For initial wireless connection, press the WPS button on your wireless n router then press the WPS button on the adapter and they exchange encryption keys and connect automatically
- Works with Window 7 (32/64bit), Vista (32/64bit), and XP (32/64bit)

Wireless Tips

The following are some general wireless tips to help minimize the impact of interference within an environment.

Assign your network a unique SSID. Do not use anything that would be identifying like “Smith Family Network”. Choose something that you would easily identify when searching for available wireless networks.

Do **not** turn off the SSID broadcast. The SSID broadcast is intended to be on and turning it off can cause connectivity issues. The preferred method of securing a wireless network is to choose a strong form of encryption with a strong and varied encryption key.

Note: after setting up the SSID, encryption type and encryption key/passphrase, please make a note of them for future reference. You will need this information to connect your wireless computers to the wireless router/access point.

Change the channel. Most wireless access points and routers are defaulted to channel 6. If you have a site survey tool that will display the channels you can plan your channel selection around neighboring access points to minimize interference from them. If your site survey tool does not display the channel try using channels 1 or 11.

If using 802.11n you should be securing the network with WPA2 security.

Note: Due to Wi-Fi certification considerations if you choose WEP, WPA or WPA2-TKIP encryption this device may operate in legacy wireless mode (802.11b/g). You may not get 802.11n performance as these forms of encryption are not supported by the 802.11n specification.

Please also make sure that the wireless hardware is not placed in any type of shelving or enclosures.

Avoid stacking hardware on top of each other to prevent overheating issues. Maintain enough free space around the hardware for good ventilation and airflow. There should also be plenty of free space around the antennas to allow the wireless signal to propagate.

There are a number of other environmental factors that can impact the range of wireless devices.

1. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose.

2. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.

3. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.

4. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.

5. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, HAM radios, Walkie-Talkies and baby monitors.

6. Any device operating on the 2.4GHz frequency will cause interference. Devices such as 2.4GHz cordless phones or other wireless remotes operating on the 2.4GHz frequency can potentially drop the wireless signal. Although the phone may not be in use, the base can still transmit wireless signal. Move the phone's base station as far away as possible from your wireless devices.

If you are still experiencing low or no signal consider repositioning the wireless devices or installing additional access points. The use of higher gain antennas may also provide the necessary coverage depending on the environment.

Features

Features

- Based on IEEE 802.11n (draft 2.0) technology
- Backward compatible with IEEE 802.11b/g standards
- Supports Ad-Hoc (Peer-to-Peer b/g only) or Infrastructure (AP-Client) mode
- Maximum reliability, throughput, and connectivity with Automatic Data Rate Switching
- Seamless roaming among 802.11b/g/n networks
- Supports 64/128-bit WEP, WPA/WPA2-RADIUS, and WPA /WPA2-PSK
- One-step network connection with Wi-Fi Protected Setup (WPS) button
- Easy user setup
- Coverage of up to 100 meters (330 ft.) indoor and 300 (980 ft.) meters outdoor * depending on the environment
- 1-year limited warranty

Hardware Overview

WPS Button
Press the WPS button to automatically establish a connection to an access point or wireless router that has WPS-enabled. Refer to WPS Push Button Configuration (PBC) 40 for

USB Connection
Take of the adapter's lid and connect the USB connection to an available USB port on your computer.

Activity LED
This LED flashes when there is network activity.

Installation Procedure

System Preparation

Ensure that you carry out the following on your computer before installing the Wireless N 150 USB Adapter:

- Remove existing wireless adapter installations
- Disable any wireless adapters that are built-in to your computer
- Ensure that you have the correct wireless settings, such as the SSID and security settings, for the wireless network that you want to connect to.

Removing Existing Wireless Adapter Installation

If you currently have a wireless adapter installed in your computer, ensure you uninstall the wireless adapter software before installing the software for the Wireless N 150 USB Adapter as this may cause a conflict with the new software. If you want to use multiple wireless adapters on your computer at different times, configure the utilities so that they do not load when the computer boots up. If you are running Windows XP or a later Windows version, the built-in wireless utility can be used to manage all adapters.

To remove the existing wireless utility on a PC running Windows XP/Vista/7:

- Click **Start** > **Control Panel** > **Add or Remove Programs**
- Select the wireless utility that you want to remove.
- Click the **Remove** button and follow the steps in the wizard to remove the utility.

To remove the existing wireless utility on a PC running Windows 2000:

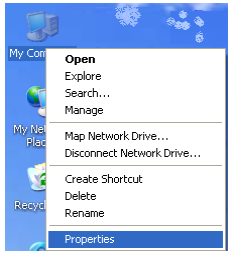
- Click **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**
- Select the wireless utility that you want to remove.
- Click the **Remove** button and follow the steps in the wizard to remove the utility.

Disabling Other Wireless Adapters

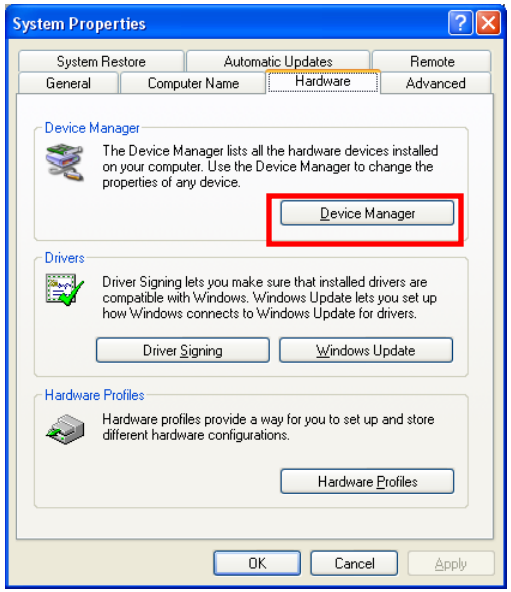
A built-in wireless adapter is included in most new laptops. In order to prevent any potential conflicts, it is recommended to disable the built-in wireless adapter before installing the Wireless N 150 USB Adapter.

Carry out the following to disable a network adapter:

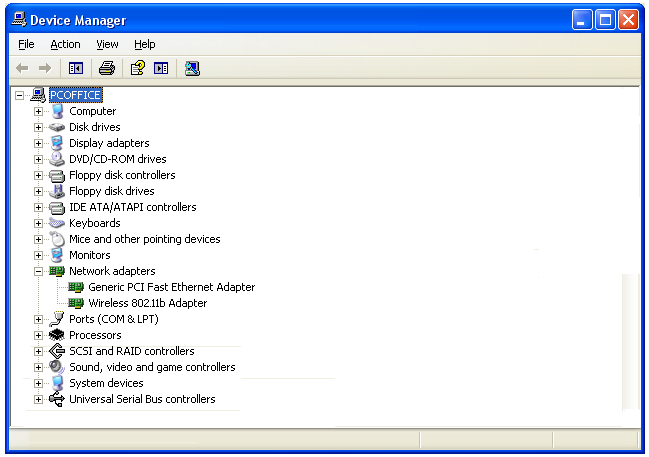
1. On your computer's desktop, right-click the **My Computer** icon and select **Properties**.



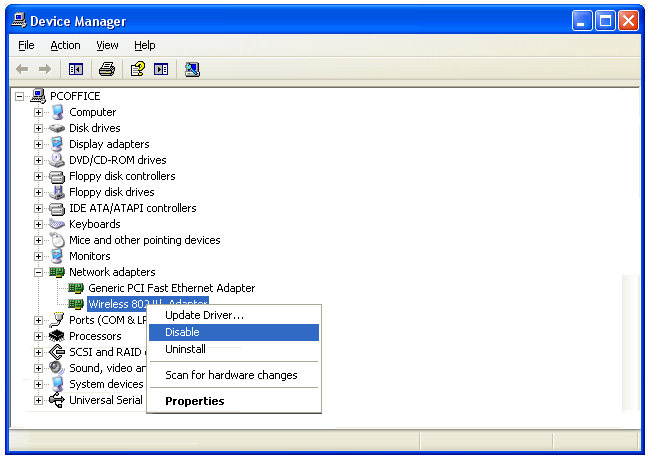
2. Click the **Hardware** tab and then click the **Device Manager** button.



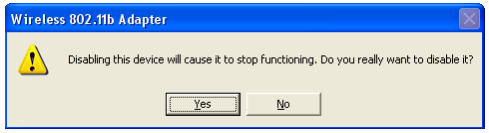
3. In the **Device Manager** window, scroll down the list and click the **+** icon next to **Network Adapters**.



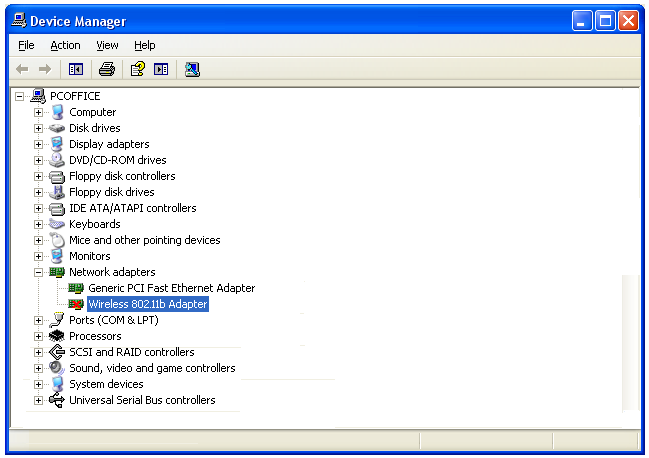
4. Right-click the adapter that you would like to disable and select the **Disable** option.



5. Click the **Yes** button to confirm that you want to disable the adapter.



6. The adapter's icon will now be crossed out with a red X, which indicates that the adapter is disabled. If you would like to re-enable the adapter in the future, right-click it and select the **Enable** option.



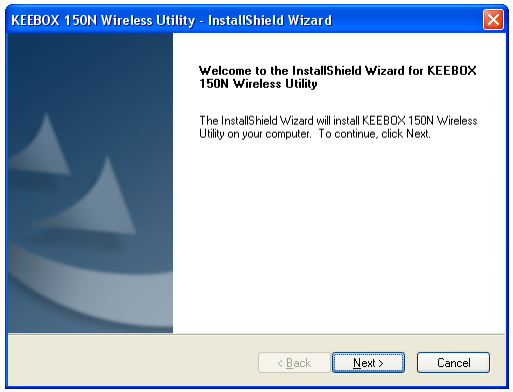
Installing the Wireless Adapter

Carry out the following to install the Wireless N 150 USB Adapter:

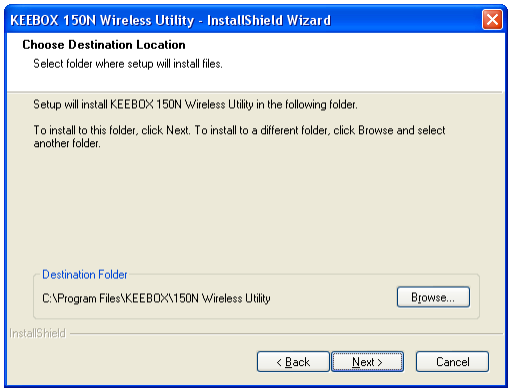
Caution: Ensure that you install the driver software on the included CD before connecting the Wireless N 150 USB Adapter to your computer.

1. Insert the included CD-ROM into your computer and click **Install Driver & Utility**.

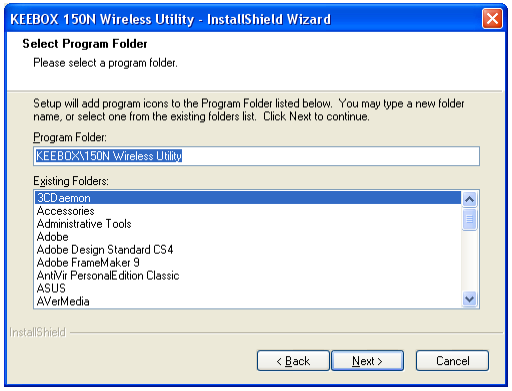
2. The InstallShield Wizard will appear. Click the **Next** button to proceed to the next window.



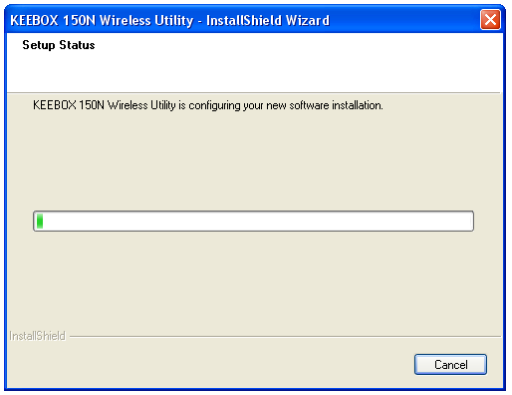
3. Specify the location that you want to install the utility files in. By default, the utility application files are installed in the **C:\Program Files\KEEBOX\150N Wireless Utility** folder. If you want to install the files in a different location, click the **Browse** button. When you have selected the utility installation location, click **Next** to continue to the next wizard window.



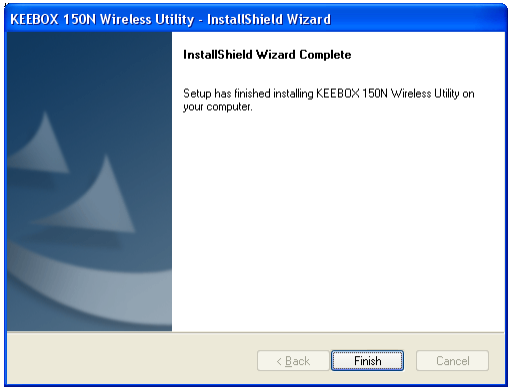
4. Specify the program folder that you want the Wireless N 150 USB Adapter Utility icon to be installed in. By default, the wizard creates a program folder called **KEEBOX\150N Wireless Utility**. If you would like to create a different folder name, enter the name of the new folder in the **Program Folder** field. To use an existing folder, select the folder in the **Existing Folders** section. When you have specified the Program Folder settings, click **Next** to continue to the next wizard window.



5. The following window appears while the installation is being carried out:



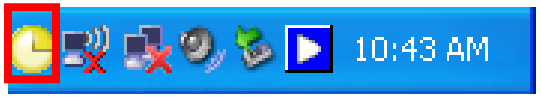
6. Click **Finish** to complete the installation.



7. Insert the Wireless N 150 USB Adapter into an available USB port on your computer.

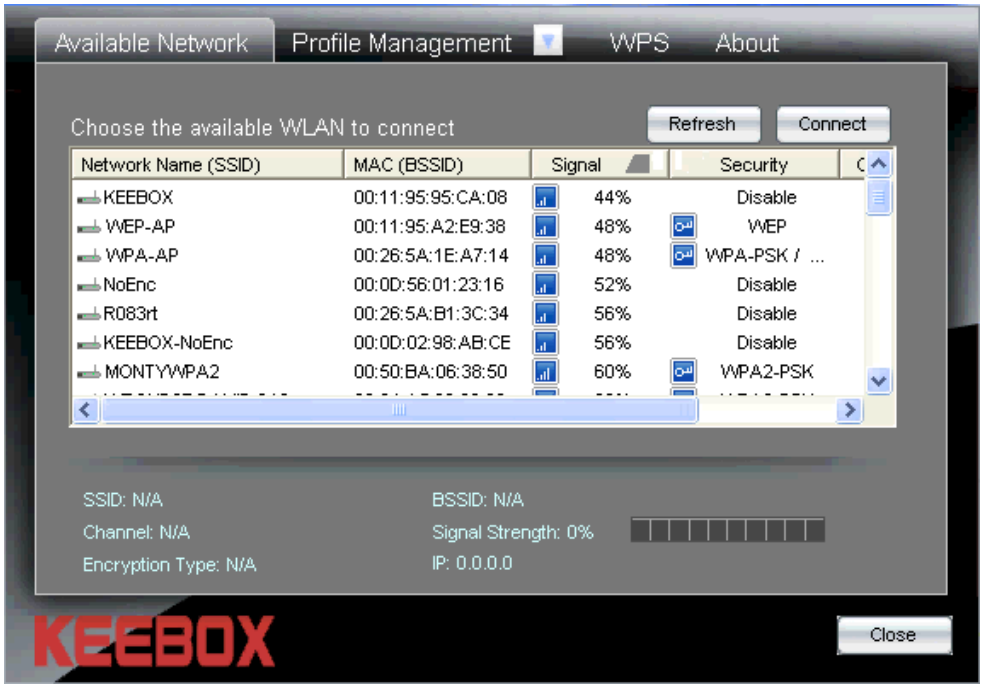
8. The **Found New Hardware** icon will display in the Windows Taskbar. The Found New Hardware Wizard will automatically install the driver for the Wireless N 150 USB adapter.

9. After the driver has been installed, the Wireless N 150 USB Adapter icon will appear in the right corner of the Windows Taskbar.



10. Right-click the Wireless N 150 USB Adapter icon and select the **Available Networks** option.

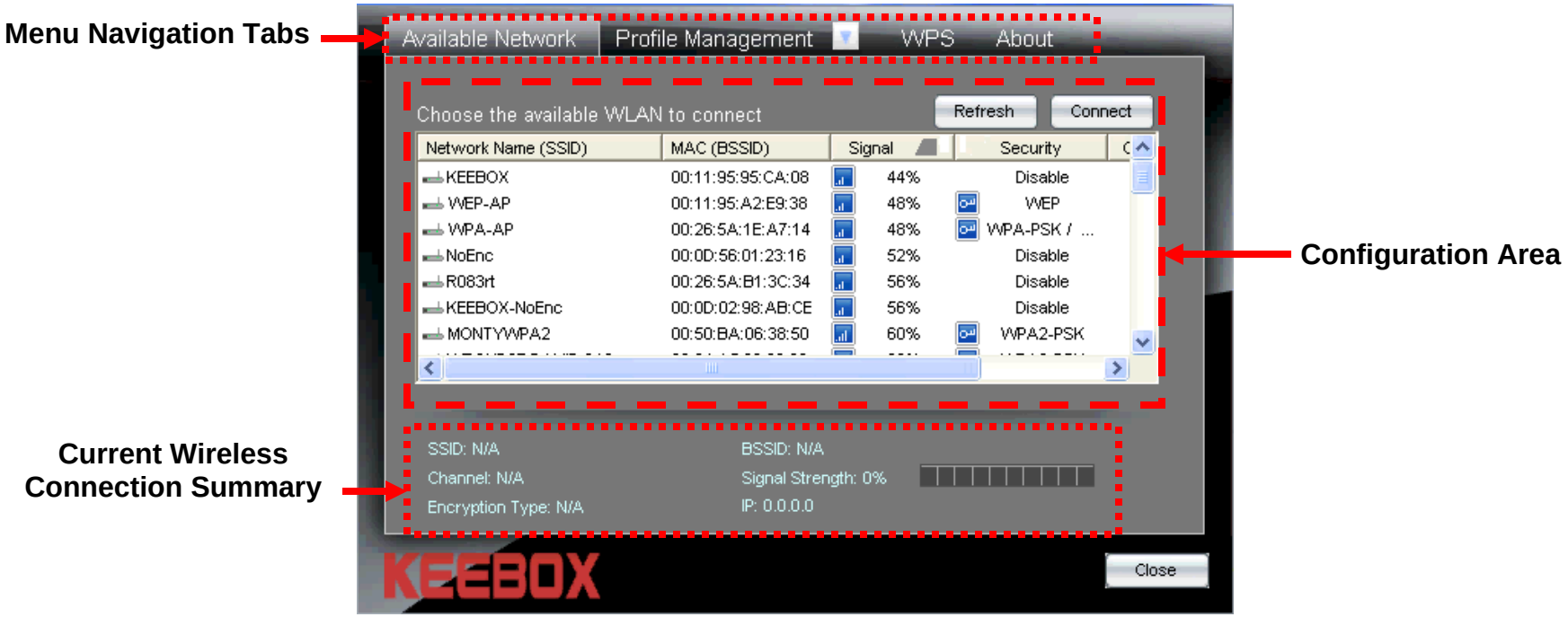
11. This will open the KEEBOX 150 N Wireless Utility, as shown below.



Adapter Configuration

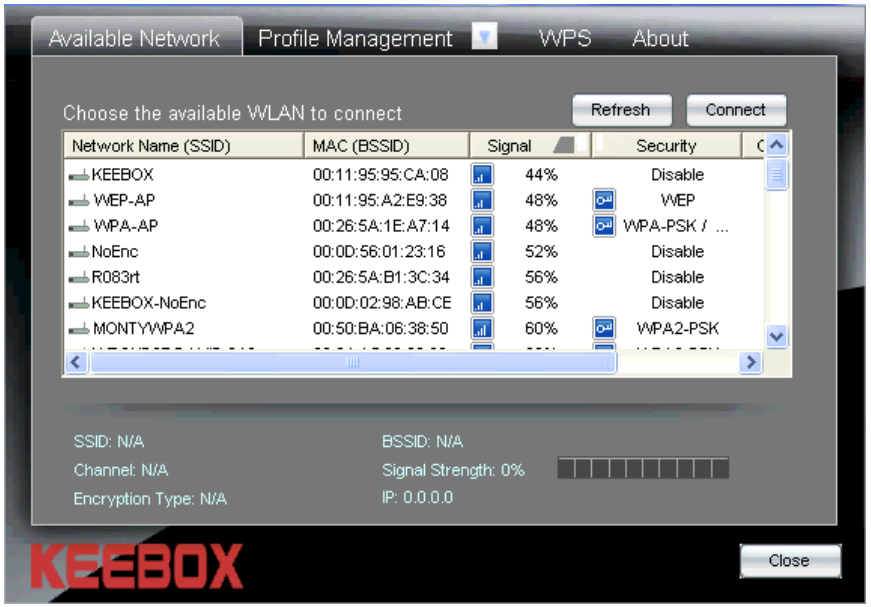
KEEBOX 150N Wireless Utility

The user can use the KEEBOX 150N Wireless Utility to manage the KEEBOX Wireless 150N USB Adapter. The utility provides a user friendly method for configuring the wireless adapter's settings.



Available Network

The Available Network window is used to display all the available wireless networks that are located in your area. You can also use this window to connect to one of the available wireless networks.



Network Name (SSID): This field displays the Service Set Identifier (SSID) of the wireless network. An SSID is used to assign a name to the wireless network.

MAC (BSSID): This field displays the Basic Service Set Identifier (BSSID) of the wireless device. The BSSID is usually the MAC address of the wireless device.

Signal: This field displays the strength of the wireless connection.

Security: This field displays the security method that has been implemented on the wireless network. If a wireless network has no security enabled, this field will display **Disable**.

Channel: This field displays the channel that the wireless network is using.

Connect Button: Use this button to connect to a wireless network. To connect to a wireless network:

1. Click the Network Name (SSID) of the wireless LAN that you want to.
2. Click the **Connect** button.
3. If choosing a secure wireless network, a pop-up window will appear.
4. Enter the required security information to connect to the wireless network.

Refresh Button: Click this button to refresh the list of wireless networks.

Profile Management

The Profile Management window is used to display and manage wireless network profiles. To enable a Profile, click the button next to the Profile Management tab and select the appropriate profile from the list.

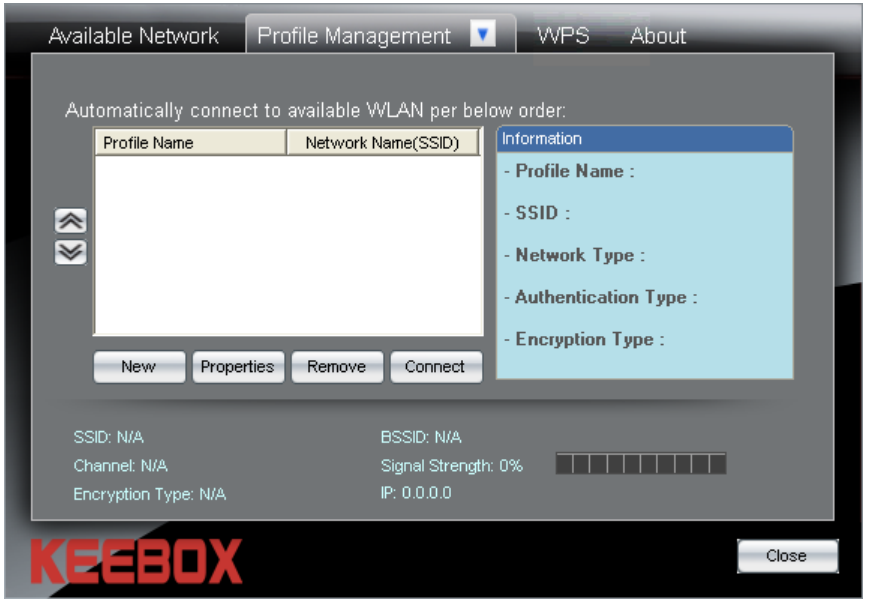
New: Click this button to create a new wireless profile. Refer to page 19 for more information on how to create a new wireless profile.

Properties: Click this button to modify an existing wireless profile. Refer to page 38 for more information on how to modify an existing wireless profile.

Remove: Click this button to delete an existing wireless profile.

Connect: To use an existing wireless profile, select the wireless profile from the list and click **Connect**.

Information: This section displays the *Profile Name*, *SSID*, *Network Type*, *Authentication Type*, and *Encryption Type* of the wireless profile that has been selected in the profile list.



Creating a Wireless Profile

The following window appears after clicking the **New** button in the Profile Management window.

Profile Name: Enter a name to identify the location that the new profile will be used in, (e.g. Lounge, Coffee Shop, Work).

Network Name (SSID): Enter the SSID of the wireless network that you want to use this profile for.

Network Type: Use the drop-down menu to select the wireless network type. If you will be connecting to a wireless router or access point, select the *Infrastructure* mode. Select the *Ad-Hoc* option if you will connect to a peer-to-peer wireless network.

Basic Security for Personal: Click this radio button if you are connecting the Wireless N 150 USB adapter to a home wireless network. Refer to page 20 for more information.

Advanced Security for Enterprise: Click this radio button if you are connecting the Wireless N 150 USB adapter to a company wireless network. Refer to page 27 for more information.

Creating a Basic Security Wireless Profile

Click the **Basic Security for Personal** radio button to create a basic wireless profile. The Basic Security Wireless Profile supports the *Open\Disable*, *Open\WEP*, *Shared\WEP*, *WPA-PSK\TKIP*, *WPA-PSK\AES, WPA2-PSK\TKIP*, and *WPA2-PSK\AES* security types. Use the **Security** drop-down menu to select the security type.

Creating a Basic Security Wireless Profile- Open \ WEP

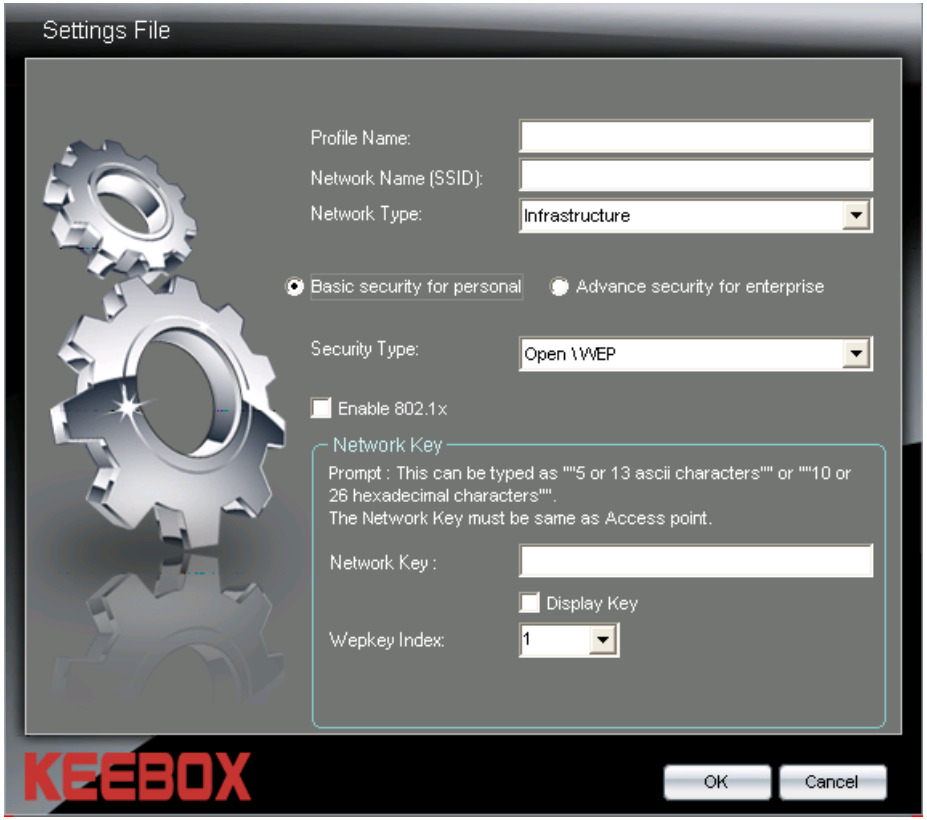
Select the Open \ WEP option from the **Security** drop-down menu to use the Open \ WEP security option.

Enable 802.1x: Check this box to enable 802.1x settings on the Wireless N 150 USB Adapter. If enabling 802.1x, the fields required for configuring the 802.1x parameters appear in the section that is used for Network Key configuration. See page 37 for more information on how to configure the Wireless N 150 USB Adapter to use 802.1x.

Network Key: If not enabling 802.1x, enter the WEP key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

Wepkey Index: Use the drop-down menu to select the *WEP Key Index Number* that is being used on your access point or wireless router.



OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.

Creating a Basic Security Wireless Profile- Shared \ WEP

Select the Shared \ WEP option from the **Security** drop-down menu to use the Shared \ WEP security option.

Network Key: Enter the WEP key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

Wepkey Index : Use the drop-down menu to select the *WEP Key Index Number* that is being used on your access point or wireless router.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.

Creating a Basic Security Wireless Profile- WPA-PSK \ TKIP

Select the WPA-PSK \ TKIP option from the **Security** drop-down menu to use the WPA-PSK \ TKIP security option.

Network Key: Enter the WPA key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.

Creating a Basic Security Wireless Profile- WPA-PSK \ AES

Select the WPA-PSK \ AES option from the **Security** drop-down menu to use the WPA-PSK \ AES security option.

Network Key: Enter the WPA key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.

Creating a Basic Security Wireless Profile- WPA2-PSK \ TKIP

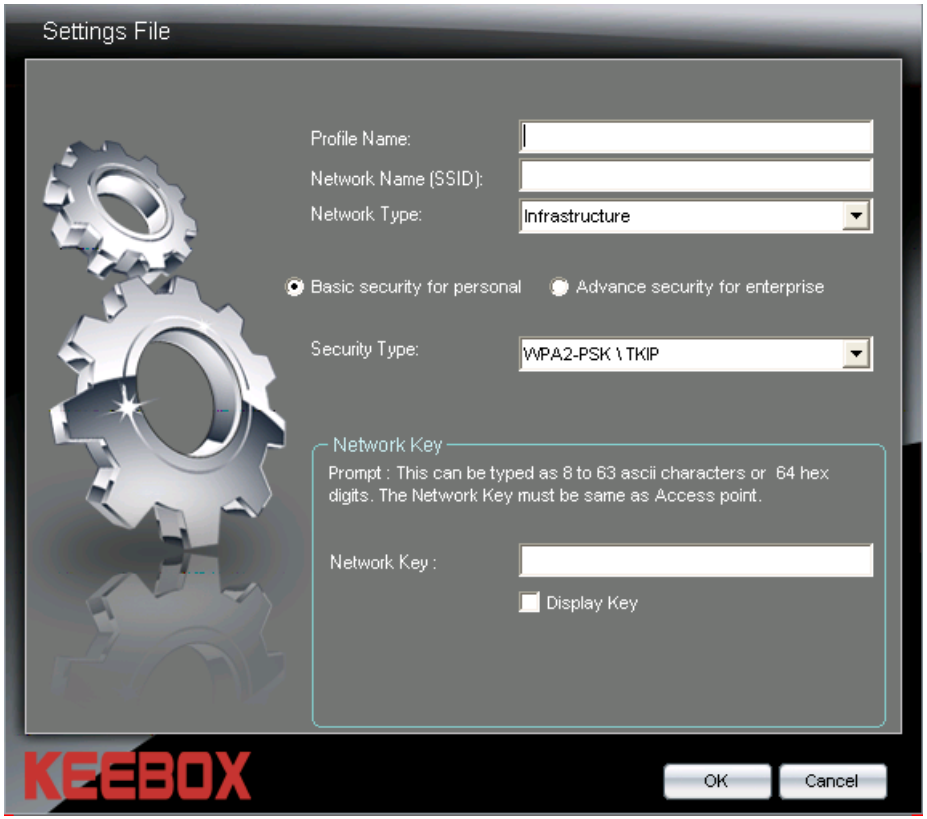
Select the WPA2-PSK \ TKIP option from the **Security** drop-down menu to use the WPA2-PSK \ TKIP security option.

Network Key: Enter the WPA2 key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.



Creating a Basic Security Wireless Profile- WPA2-PSK \ AES

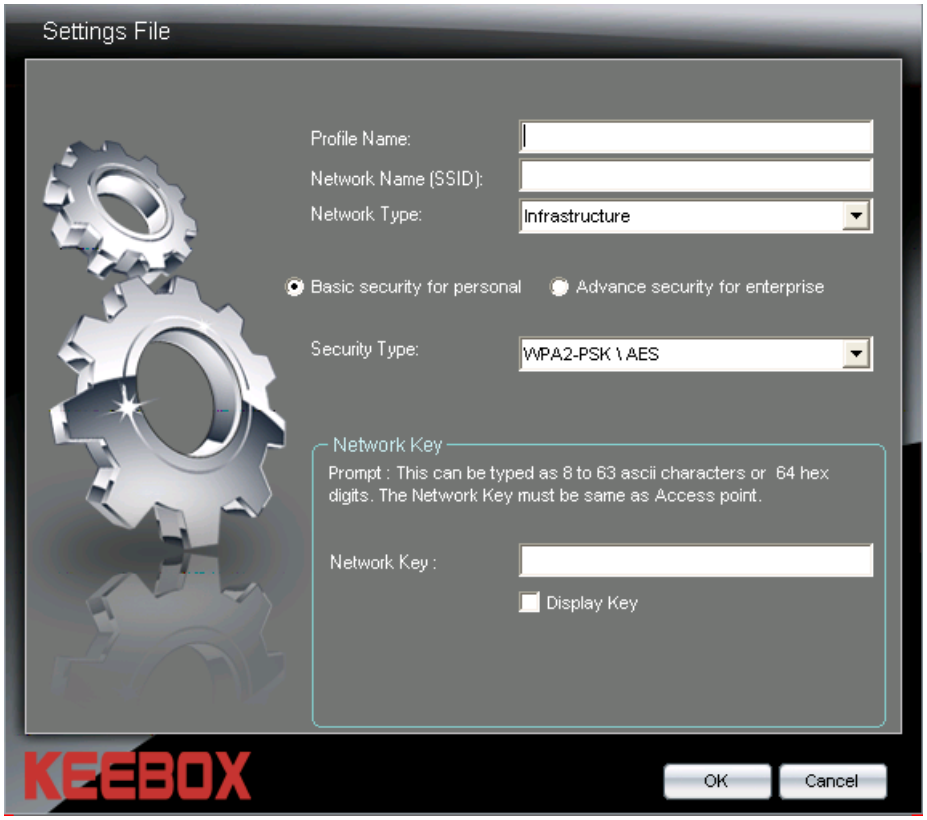
Select the WPA2-PSK \ AES option from the **Security** drop-down menu to use the WPA2-PSK \ AES security option.

Network Key: Enter the WPA2 key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.



Creating an Advanced Security Wireless Profile

Click the **Advanced Security for Enterprise** radio button to create an advanced wireless profile. Use the drop-down menus to select the *Authentication* and *Encryption Type* that is being used on your wireless network.

Authentication Type: Use the drop-down menu to select the Authentication Type that is being used on your wireless network. The available options are:

- *Open*
- *Shared*
- *WPA-EAP (Enterprise)*
- *WPA-PSK (Personal)*
- *WPA2-EAP (Enterprise)*
- *WPA2-PSK (Personal)*

Encryption Type: Use the drop-down menu to select the *Encryption Method* that your wireless network is using with the specified authentication type.

Enable 802.1x: Check this box to enable 802.1x settings on the Wireless N 150 USB Adapter. If enabling 802.1x, the fields required for configuring the 802.1x parameters appear in the section that is used for Network Key configuration. See page 37 for more information on how to configure the Wireless N 150 USB Adapter to use 802.1x.

Network Key: If not enabling 802.1x, enter the WEP key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

Wepkey Index : Use the drop-down menu to select the *WEP Key Index Number* that is being used on your access point or wireless router.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

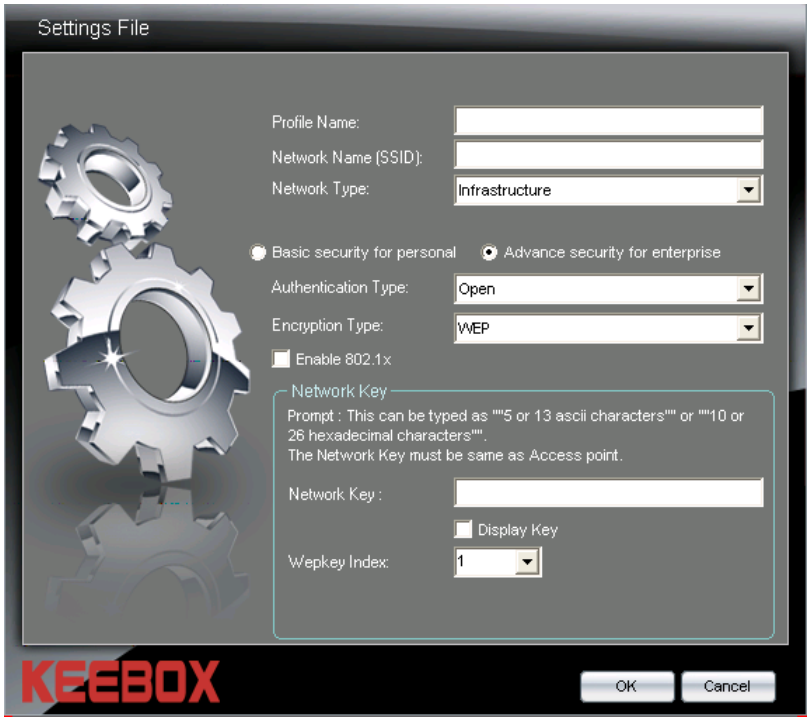
Cancel Button: Click this button to cancel any changes made.

Creating an Advanced Security Wireless Profile-Open Authentication

Authentication Type: Select the *Open* authentication type from the drop-down menu.

Encryption Type: If your network is using encryption with the open authentication method, select W*EP* from the drop-down menu. If no encryption is being used select *Disabled*.

Enable 802.1x: Check this box to enable 802.1x settings on the Wireless N 150 USB Adapter. If enabling 802.1x, the fields required for configuring the 802.1x parameters appear in the section that is used for Network Key configuration. See page 37 for more information on how to configure the Wireless N 150 USB Adapter to use 802.1x.



Network Key: If not enabling 802.1x, enter the WEP key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

Wepkey Index : Use the drop-down menu to select the *WEP Key Index Number* that is being used on your access point or wireless router.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.

Creating an Advanced Security Wireless Profile-Shared Authentication

Authentication Type: Select the *Shared* authentication type from the drop-down menu.

Encryption Type: The Shared authentication option only supports the *WEP* encryption method.

Network Key: Enter the WEP key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

Wepkey Index: Use the drop-down menu to select the *WEP Key Index Number* that is being used on your access point or wireless router.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.

Creating an Advanced Security Wireless Profile-WPA-EAP (Enterprise) Authentication

Authentication Type: Select the *WPA-EAP (Enterprise)* authentication type from the drop-down menu.

Encryption Type: Use the drop-down menu to select whether the *TKIP or AES* encryption method is being used on your network.

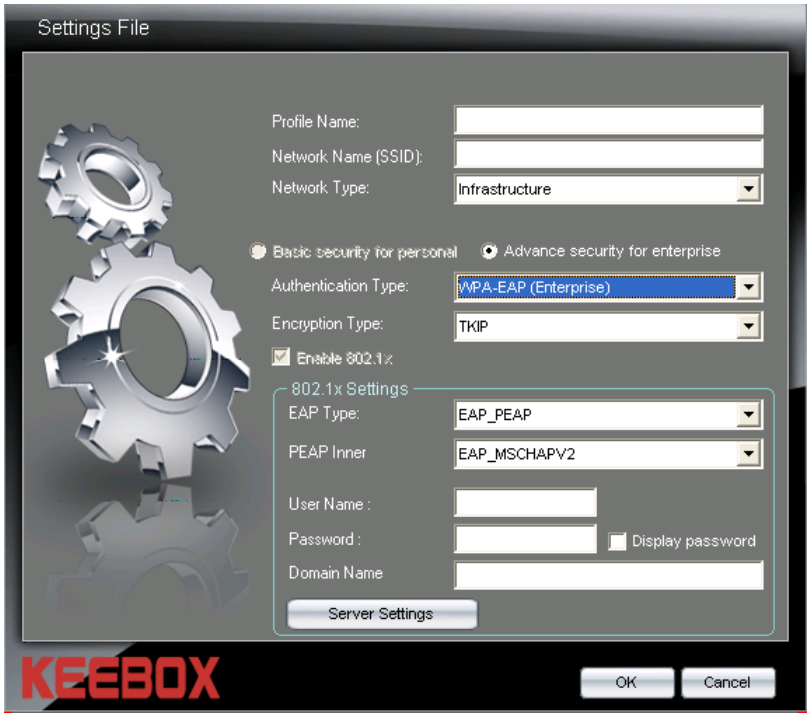
Enable 802.1x: The *WPA-EAP (Enterprise)* authentication method uses 802.1x.

EAP Type: Use the drop-down menu to select the *EAP Type* being used by your network.

If selecting the *EAP_TLS* option, select the *User Certificate* that is being used from the **User Certificate** drop-down menu.

If selecting the *EAP_PEAP* option, select the *PEAP Inner* value that is being used from the **PEAP Inner** drop-down menu.

If selecting the *EAP_TTLS* option, select the *TTLS Inner* value that is being used from the **TTLS Inner** drop-down menu.



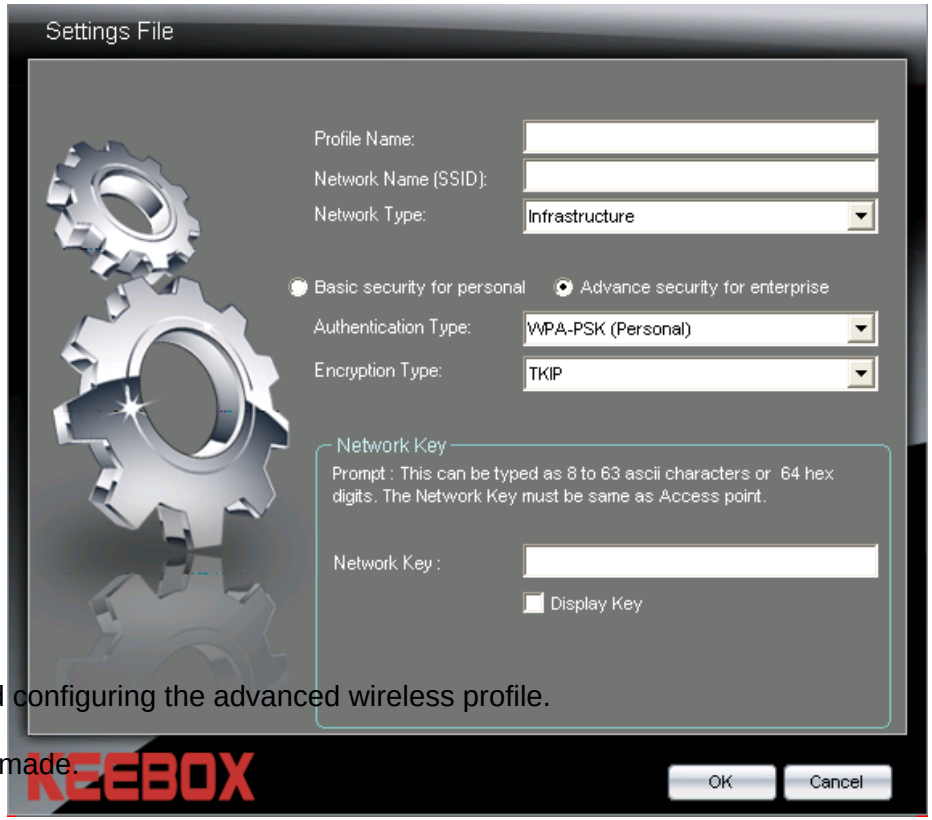
User Name: Enter the user name that is being used for 802.1x in this field.

Password: Enter the password for the 802.1x user name in this field.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.

Creating an Advanced Security Wireless Profile-WPA-PSK (Personal) Authentication



Authentication Type: Use the drop-down menu to select the *WPA-PSK (Personal)* authentication option.

Encryption Type: Use the drop-down menu to select whether the *TKIP* or *AES* encryption type is being used on your wireless network.

Network Key: Enter the WPA key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

OK Button: Click this button when you have finished configuring the advanced wireless profile.
finished configuring the
advanced wireless profile.
Click this button to cancel any changes made.

Cancel Button: Click this button to cancel any changes made.

Creating an Advanced Security Wireless Profile-WPA2-EAP (Enterprise) Authentication

Authentication Type: Select the *WPA2-EAP (Enterprise)* authentication type from the drop-down menu.

Encryption Type: Use the drop-down menu to select whether the *TKIP or AES* encryption method is being used on your network.

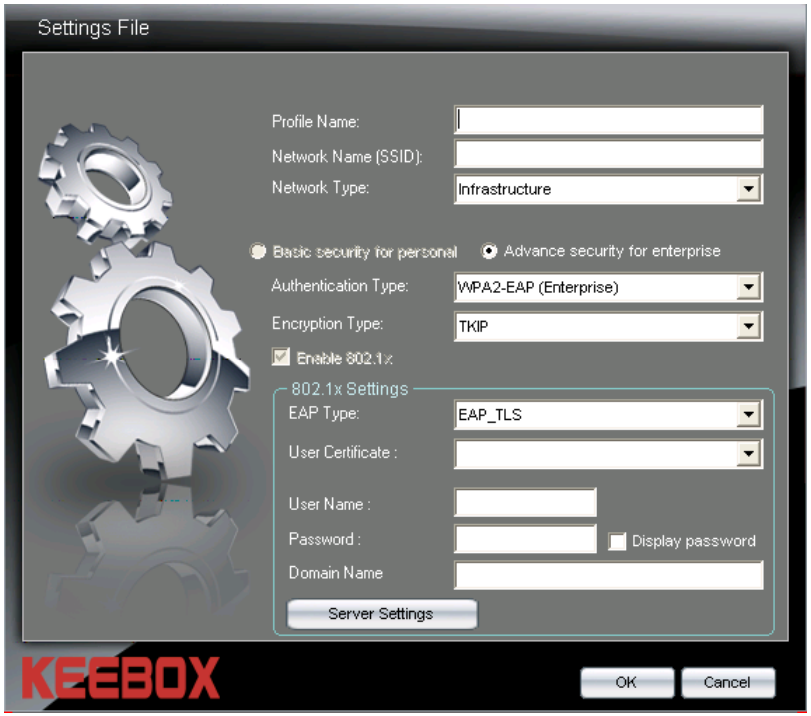
Enable 802.1x: The *WPA-EAP (Enterprise)* authentication method uses 802.1x.

EAP Type: Use the drop-down menu to select the *EAP Type* being used by your network.

If selecting the *EAP_TLS* option, select the *User Certificate* that is being used from the **User Certificate** drop-down menu.

If selecting the *EAP_PEAP* option, select the *PEAP Inner* value that is being used from the **PEAP Inner** drop-down menu.

If selecting the *EAP_TTLS* option, select the *TTLS Inner* value that is being used from the **TTLS Inner** drop-down menu.



User Name: Enter the user name that is being used for 802.1x in this field.

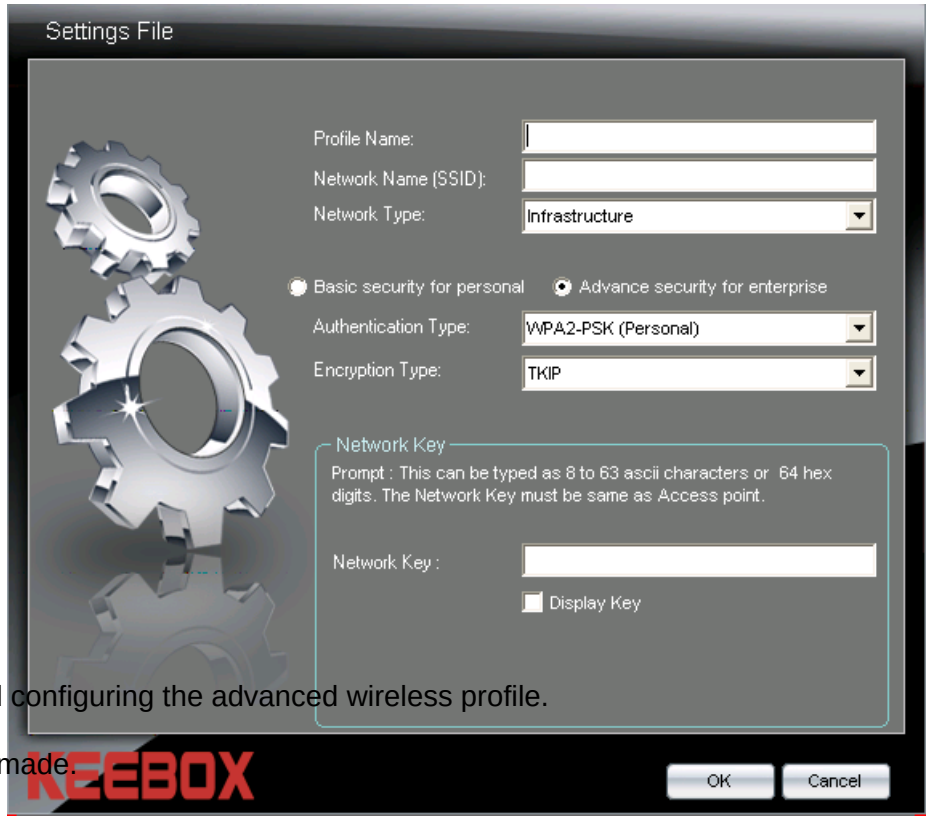
Password: Enter the password for the 802.1x user name in this field.

Server Settings: Click this button to configure the Trusted Root Certification Authorities List. See page 38 for more information.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.

Creating an Advanced Security Wireless Profile-WPA2-PSK (Personal) Authentication



Authentication Type: Use the drop-down menu to select the *WPA2-PSK (Personal)* authentication option.

Encryption Type: Use the drop-down menu to select whether the *TKIP* or *AES* encryption type is being used on your wireless network.

Network Key: Enter the WPA key that is used on your access point or wireless router.

Display Key: Check this box if you would like to view the key that has been entered in the **Network Key** field. If this box is left unchecked, the Network Key will appear as a series of *.

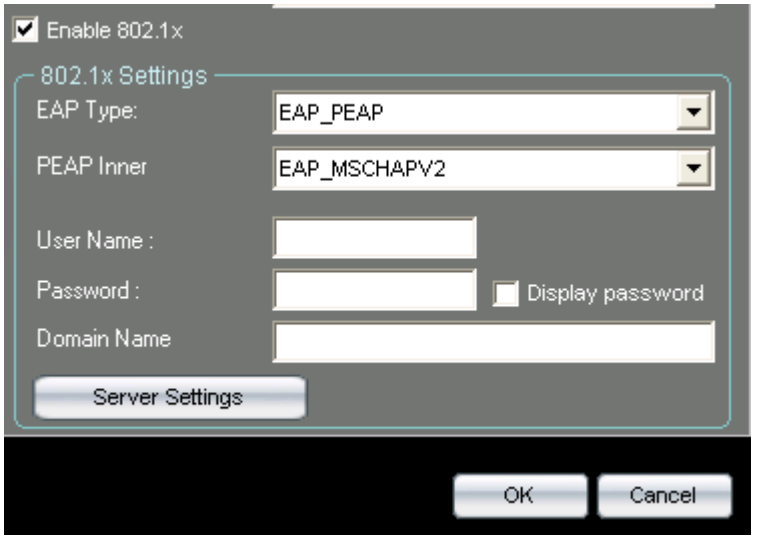
OK Button: Click this button when you have finished configuring the advanced wireless profile.

Click this button when you have finished configuring the advanced wireless profile. any changes made.

Cancel Button: Click this button to cancel any changes made.

Enabling and Configuring 802.1x Parameter for a Wireless Profile

The Open \ WEP Basic and Advanced Security options can be configured to use 802.1x. To use 802.1x with these security options, check the **Enable 802.1x** box and configure the parameters that appear in the 802.1x Settings section as described below:



Enable 802.1x: Check this box to enable 802.1x.

EAP Type: Use the drop-down menu to select the *EAP Type* being used by your network.

If selecting the *EAP_TLS* option, select the *User Certificate* that is being used from the **User Certificate** drop-down menu.

If selecting the *EAP_PEAP* option, select the *PEAP Inner* value that is being used from the **PEAP Inner** drop-down menu.

If selecting the *EAP_TTLS* option, select the *TTLS Inner* value that is being used from the **TTLS Inner** drop-down menu.

User Name: Enter the user name that is being used for 802.1x in this field.

Password: Enter the password for the 802.1x user name in this field. Check the **Display Password** box to display the password in clear text. To display the passwords as a series of ****, uncheck the **Display Password** box.

Server Settings: Click this button to configure the Trusted Root Certification Authorities List. See the following page for more information.

OK Button: Click this button when you have finished configuring the advanced wireless profile.

Cancel Button: Click this button to cancel any changes made.

Configuring 802.1x Validate Server Certificate Settings

Carry out the following to configure the 802.1x Validate Server Certificate Settings.

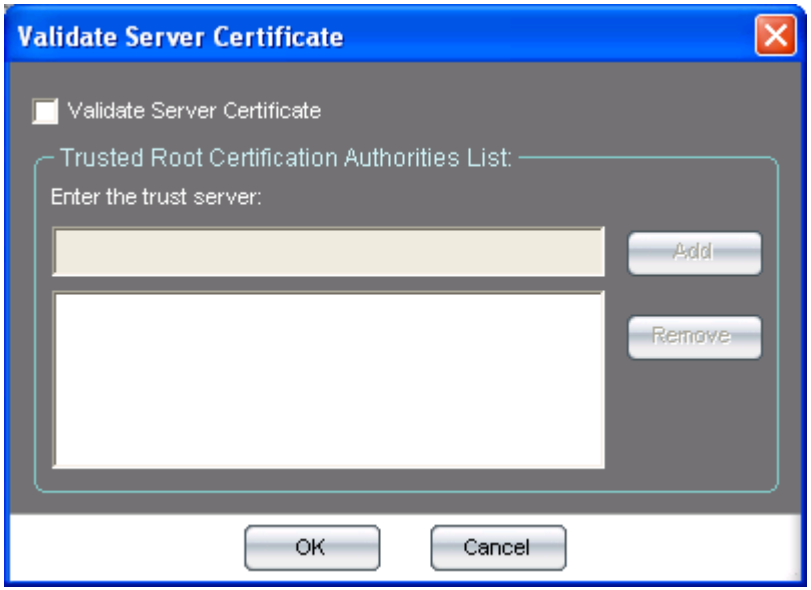
Validate Server Certificate: Check this box to enable the 802.1x Validate Server Certificate option.

Trust Root Certification Authorities List: Carry out the following to add a new Trust Server:

1. Enter the *DNS host name* of the Trust Server in the input field.
2. Click the **Add** button.

Carry out the following to remove a Trust server.

1. Select the Trust Server that you want to remove from the list.
2. Click the **Remove** button.



OK Button: Click this button when you have finished configuring the Validate Server Certificate settings.

Cancel Button: Click this button to cancel any changes made to the Validate Server Certificate settings.

Editing a Wireless Profile

To modify an existing wireless profile, select the profile that you want to modify in the Profile Management list and click the **Properties** button to reveal the following window.

Profile Name: Enter a name to identify the location that the new profile will be used in (e.g. Lounge, Coffee Shop, Work).

Network Name (SSID): Enter the SSID of the wireless network that you want to use this profile for.

Network Type: Use the drop-down menu to select the wireless network type. If you will be connecting to a wireless router or access point, select the *Infrastructure* mode. Select the *Ad-Hoc* option if you will connect to a peer-to-peer wireless network.

Basic Security for Personal: Click this radio button if you are connecting the Wireless N 150 USB adapter to a home wireless network. Refer to page 20 for more information.

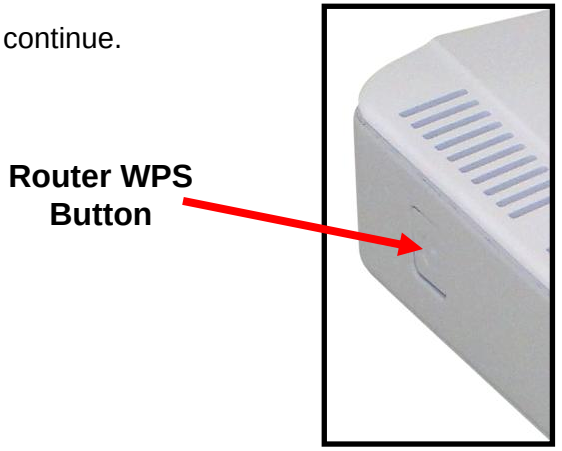
Advanced Security for Enterprise: Click this radio button if you are connecting the Wireless N 150 USB adapter to a company wireless network. Refer to page 27 for more information.

WPS Push Button Configuration (PBC)

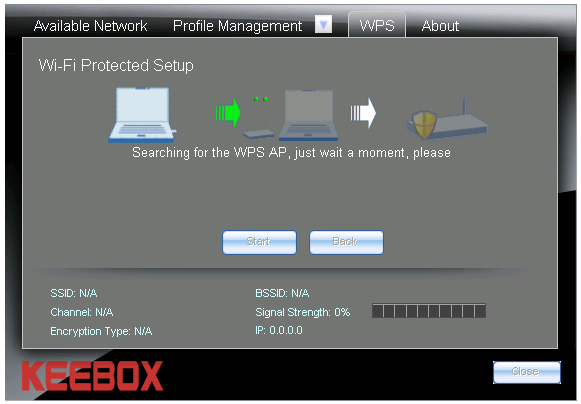
Carry out the following steps to connect to your network using the WPS Push Button Configuration method.

1. Press the WPS button on the adapter and hold for four seconds until the wizard screen appears.

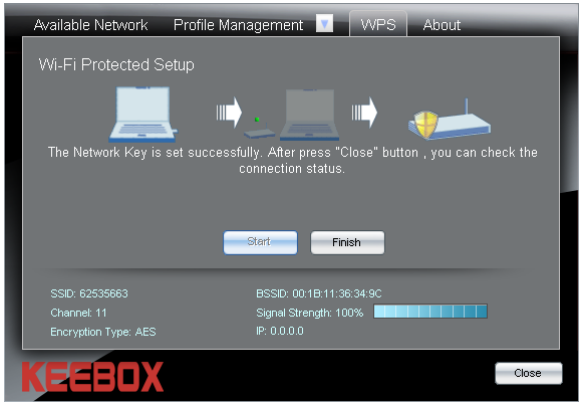
2. Press the WPS button located on your access point or router to continue.



3. The following window appears while the Wireless N 150 USB Adapter attempts to connect to the access point or wireless router.



4. After the adapter has successfully established a network connection, the following screen will appear on your computer. Click **Finish** to complete WPS PBC setup.



WPS PIN Code

Carry out the following steps to connect to your network using the WPS PIN Code method

1. Select PIN (Personal Identification Number) and click **Next**.

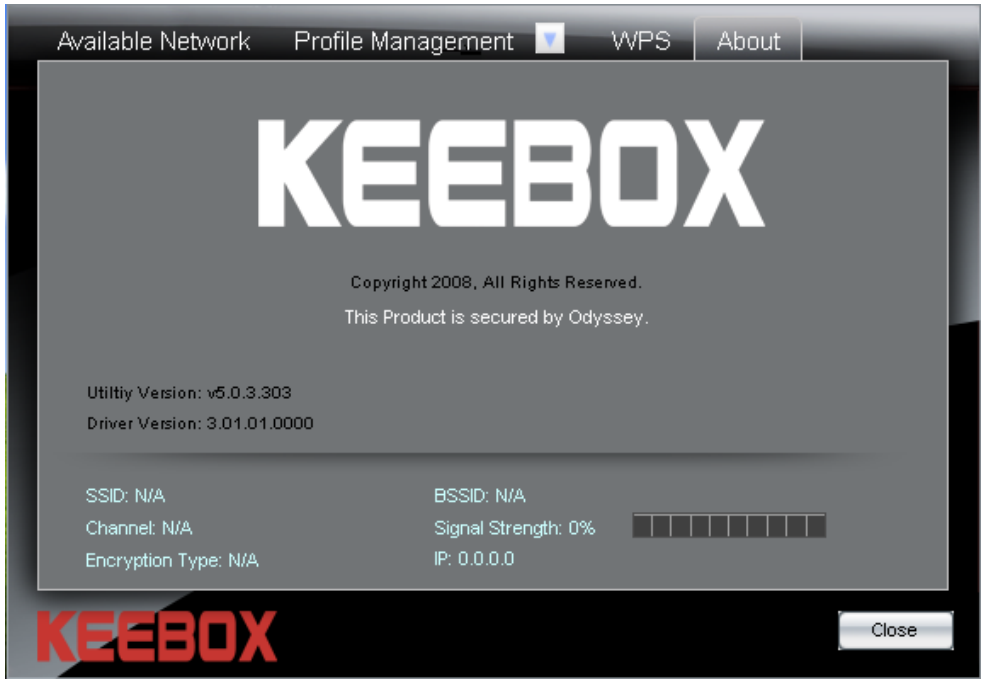
2. Make sure your access point or wireless router is close by. Write down the number on the screen. Enter this number in your access point or wireless router. Please refer to the manufacture's manual for instructions. Once you click Next, you will have 2 minutes to enter this number in your access point or wireless router.

3. The adapter will try to establish connectivity to your access point or wireless router.

4. When this screen appears, you have successfully established connectivity. Click **Finish** to complete your setup.

About

Use the About window to view information about the Firmware and Utility versions of the wireless adapter.



Technical Specifications

Hardware	
Interface	USB 2.0, 1.1 standard
Standards	IEEE 802.11b, IEEE 802.11g, and based on IEEE 802.11n (draft 2.0) technology
WPS Button	Enables WPS connection
Power Consumption	Receive mode: 220mA (max) ; Continuous mode: 550mA (max)
Supported OS	Windows 7 (32/64-bit) / Vista (32/64-bit) / Windows XP(32/64-bit)
Dimensions (LxWxH)	**TBD**
Weight	**TBD**
Temperature	Operating: 0° ~ 45° C (32° ~ 113° F) Storage: -20° ~ 75° C (-4° ~ 167° F)
Humidity	5% ~ 95% max. (non-condensing)
Certifications	CE, FCC
Wireless	
Modulation	802.11b: DSS 802.11g: OFDM 801.11n: OFDM
Frequency	2.412 ~ 2.484 GHz
Media Access Protocol	CSMA/CA with ACK
Data Rate (auto fallback)	802.11b: up to 11Mbps 802.11g: up to 54Mbps 802.11n: up to 150Mbps
Output Power	802.11b: 15dBm (typical) 802.11g: 13dBm (typical) 802.11n : 13dBm (typical)
Receiving Sensitivity	TBD
Encryption	64/128-bit WEP (Hex & ASCII), WPA/WPA2-RADIUS, WPA/WPA2-PSK (AES/TKIP)
Channels	1~11 (FCC), 1~13 (ETSI)

Limited Warranty

KEEBOX warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

W150NU – 1 Year Warranty

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

If a product does not operate as warranted during the applicable warranty period, KEEBOX shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of KEEBOX. Replacement products may be new or reconditioned. KEEBOX does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

KEEBOX shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to KEEBOX pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting KEEBOX within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all KEEBOX products. Products that are sent to KEEBOX for RMA service must have the RMA number marked on the outside of return packages and sent to KEEBOX prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

WARRANTIES EXCLUSIVE: IF THE KEEBOX PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT KEEBOX'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR

A PARTICULAR PURPOSE. KEEBOX NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF KEEBOX'S PRODUCTS.

KEEBOX SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT 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 MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW KEEBOX ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT KEEBOX'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some KEEBOX products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to http://www.KEEBOX.com/gpl or http://www.KEEBOX.com Download section and look for the desired KEEBOX product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. KEEBOX does not provide technical support for these codes. Please go to http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

KEEBOX

Copyright © 2010 KEEBOX. All Rights Reserved.