LevelOne

User Manual

WUA-0600

N_Max Wireless USB Adapter

Ver. 1.0.0-0802

Safety

FCC WARNING

This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1) Reorient or relocate the receiving antenna.
2) Increase the separation between the equipment and receiver.
3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4) Consult the dealer or an experienced radio/TV technician for help.

CE Declaration of conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

CE Marking Warning

Hereby, Digital Data Communications, declares that this (Model-no. WUA-0600) is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The CE-Declaration of Conformity can be downloaded at:

http://www.levelone.eu/support.php

Table of Content

Introduction

Congratulations on your purchase of LevelOne *N_Max* Wireless USB Adapter.

This manual helps to get familiar with the LevelOne *N_Max* Wireless LAN Adapter. This manual contains detailed instructions in operation of this product. Please keep this manual for future reference.

With a Wireless LAN Adapter, a laptop computer or a station can communicate with another computer in a wireless way. Easy-to-use utilities are bundled with Wireless LAN Adapter for configuration, monitoring, and diagnosis purposes.

Wireless LAN Adapter can wirelessly transmit and receive data, with the Wireless LAN Adapter, you can locate your Notebook PC or station wherever you want without wires and cables.

Wireless LAN Adapter provides users with an access to real-time information anywhere in their organization. The mobility provides productivity and service, which are not available under wired networks. The Wireless LAN Adapter configuration is easy to change from peer-to-peer networks, suitable for a small number of users, to full infrastructure networks of thousands of users that allow roaming around a broad area.

User Manual Overview

Introduction	Describes *N_Max* Wireless USB Adapter.
Unpacking and Setup	Helps user to get started with the basic installation of the *N_Max* Wireless USB Adapter.
Hardware Installation	Describes the LED indicators of the *N_Max* Wireless USB Adapter.
Software Installation	Tells how to setup the driver and the utility setting.
Technical Specifications	Lists the technical (general, physical and environmental) specifications of the *N_Max* Wireless USB Adapter.

Unpacking and Setup

This chapter provides the package contents and setup information for the *N_Max* Wireless USB Adapter.

Features

- Extended and high-speed wireless connectivity with wireless *N* technology
- Hardware Push Button for Wi-Fi Protected Setup
- Backward compliant with IEEE802.11g and 11b standards
- Operates on the 2.4GHz frequency band
- Supports 64/128-bit WEP, WPA, WPA2 encryption for high level of security
- USB 2.0/1.1/1.0 Interface
- Supports Windows 2000/XP/Vista
- For Maximum Performance use Wireless *N* Router

Package Contents

Open the box of the *N_Max* Wireless USB Adapter and carefully unpack it. The box should contain the following items:

- WUA-0600 *N_Max* Wireless USB Adapter
- Extension Cable
- Quick Installation Guide
- CD Manual/Driver/Utility

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the Wireless USB Adapter can be performed using the following steps:

- Visually inspect the USB Adapter and make sure that it is fully plugged in to the USB port.
- Make sure that there is a well environment that there is no much intrusion to have a better connection.

Hardware Installation

Installation Procedure for USB Adapter

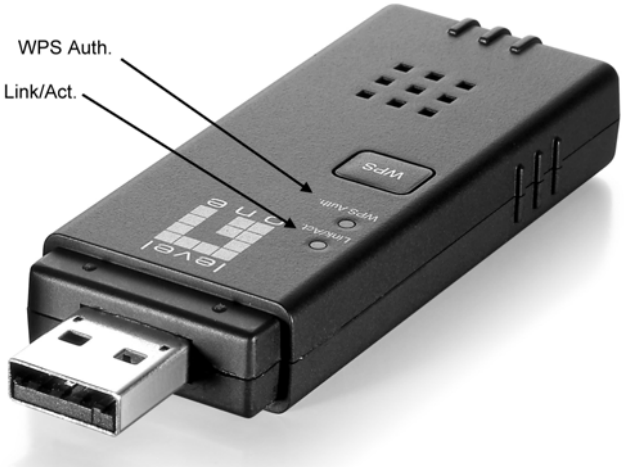
You should install the supplied software BEFORE inserting the Wireless USB Adapter when using Windows 2000, XP or Vista.

Note

The following installation was operated under Windows XP. (Procedures are similar for Windows 2000.)

If you have installed the Wireless Adapter driver & utility before, please uninstall the old version first.

LED Indicator



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

Check the installation

The LEDs of the Wireless USB Adapter are clearly visible and the status of the network link can be seen instantly:

1. Once the device is plugged to the station’s USB port, the Link/Act. LED of the Wireless USB Adapter will light up indicating a normal status with power.
2. While the Wireless USB Adapter linked up and transmitting data to the Access Point or to other Wireless LAN station, the WPS Auth. LED will start alternate blinking.

WPS Button

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

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

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

For more details about Wi-Fi Protected Setup, please refer to —**WPS Button**

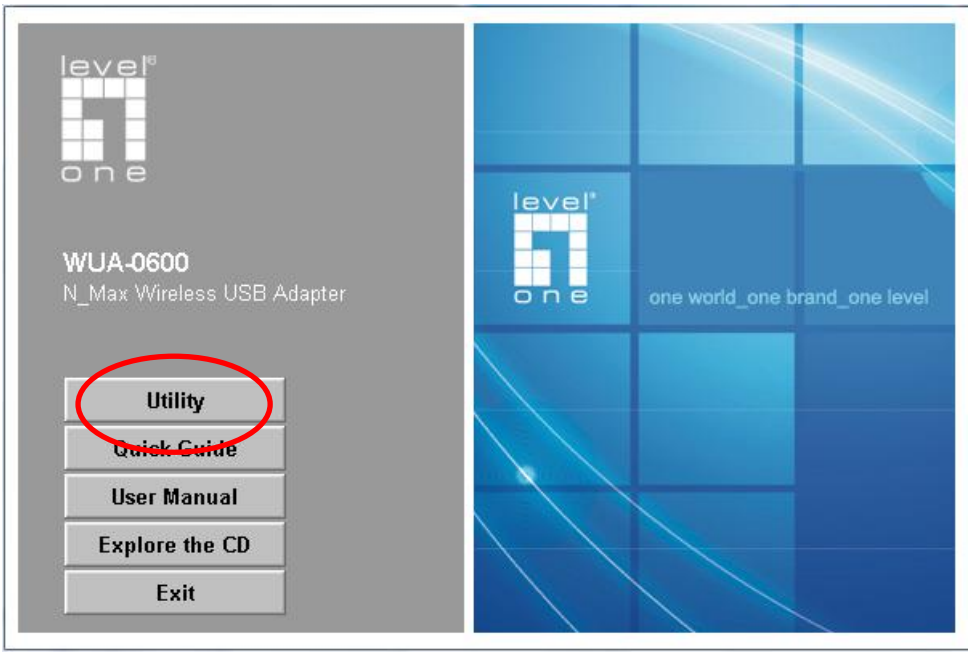
Software Installation

This section will lead you to install the driver and utility of the *N_Max* Wireless USB Adapter.

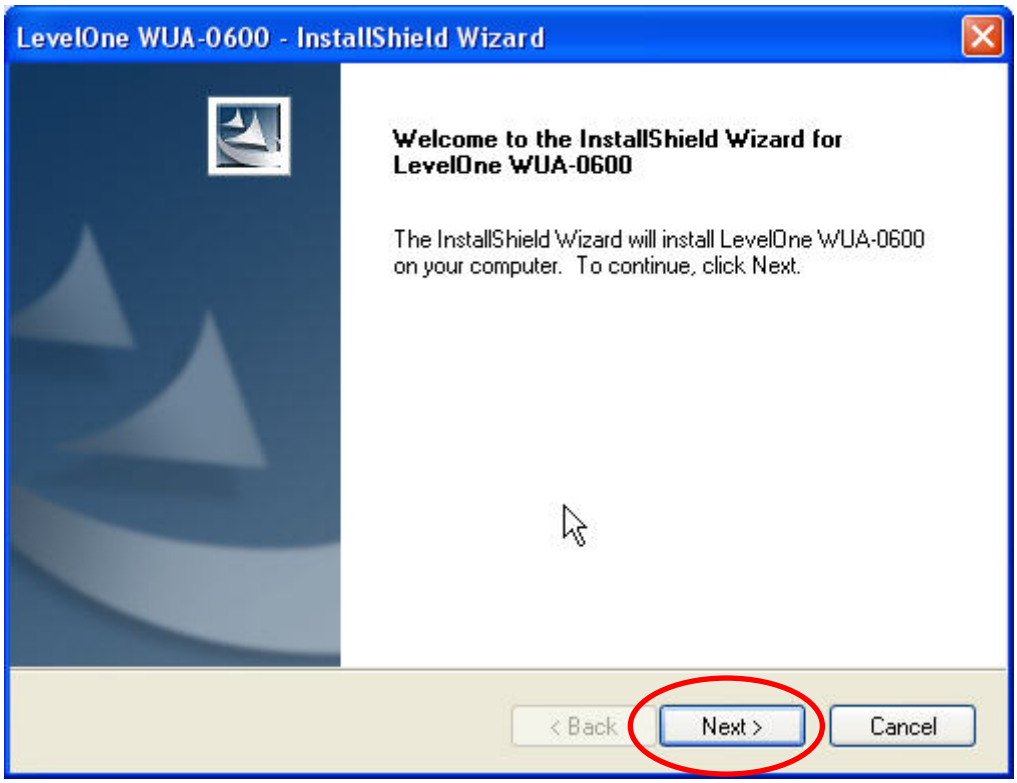
Windows 2000/XP/Vista Utility Installation

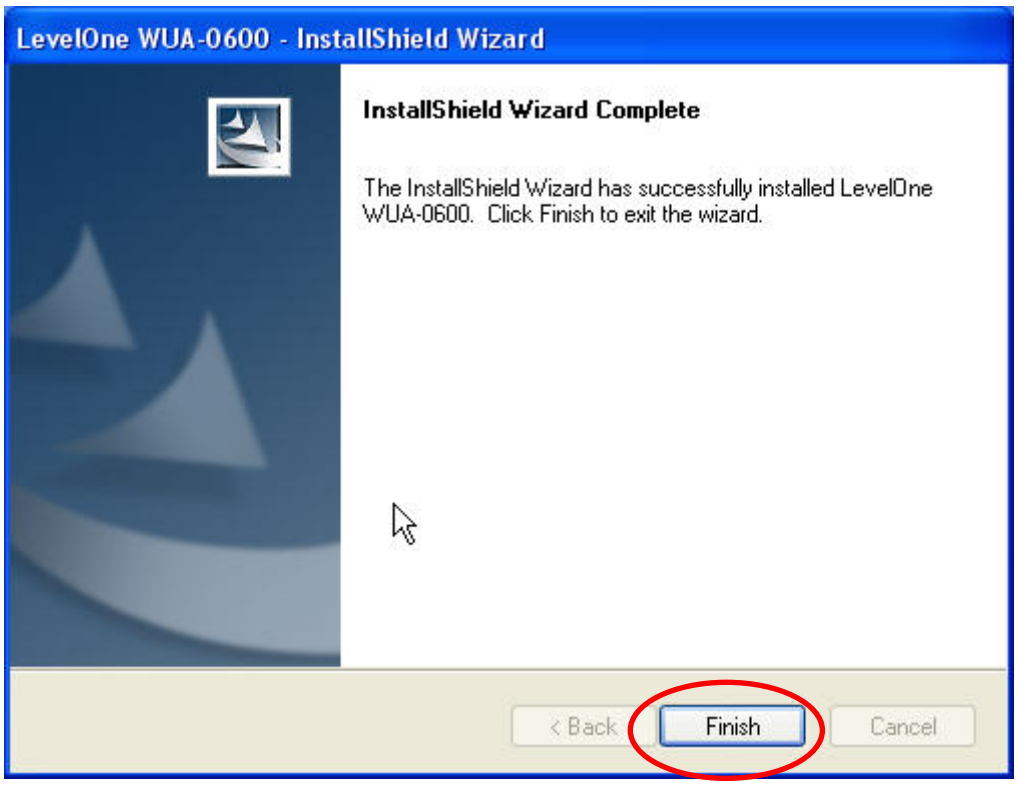
1. Insert the *N_Max* Wireless USB Adapter Utility CD into the computer and then the Auto-run screen will appear. Alternatively, open a file browser and double click on the autorun.exe file located in the CD directory.

2. Click **"Utility**" to install the driver and utility and the install wizard will begin installing the software. Follow the install wizard instructions to complete the installation.

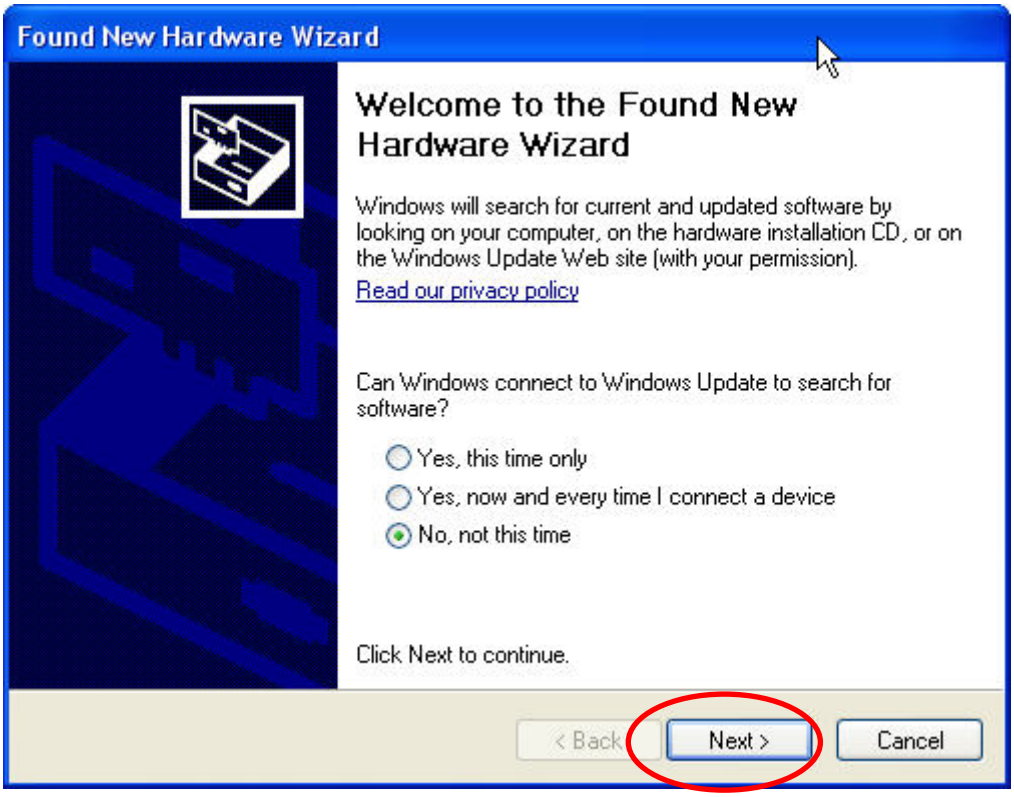


3. Follow the Install Shield Wizard Instructions. Click "**Next**" to continue and follow the on-screen instruction to finish it.

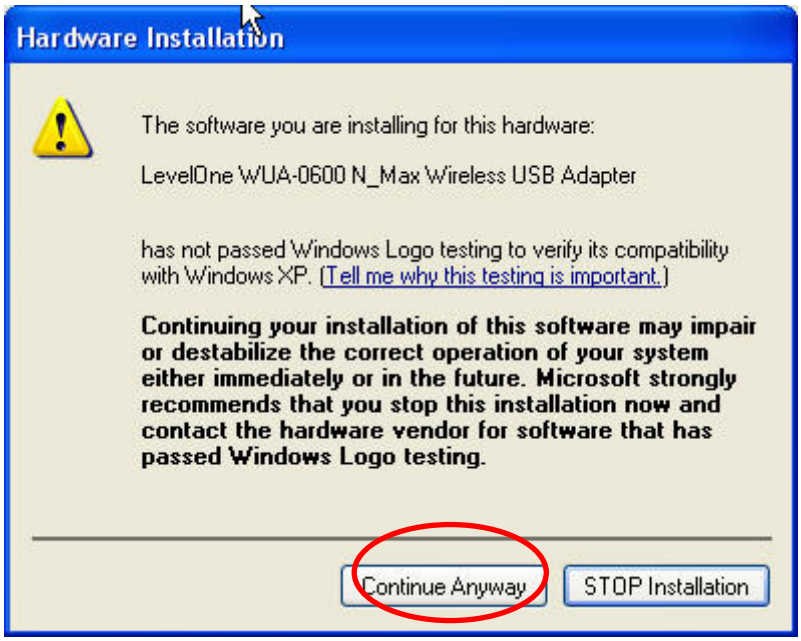

LevelOne WUA-0600 - InstallShield Wizard
Welcome to the InstallShield Wizard for LevelOne WUA-0600
The InstallShield Wizard will install LevelOne WUA-0600 on your computer. To continue, click Next.
< Back
Next >
Cancel


LevelOne WUA-0600 - InstallShield Wizard
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed LevelOne WUA-0600. Click Finish to exit the wizard.
< Back
Finish
Cancel

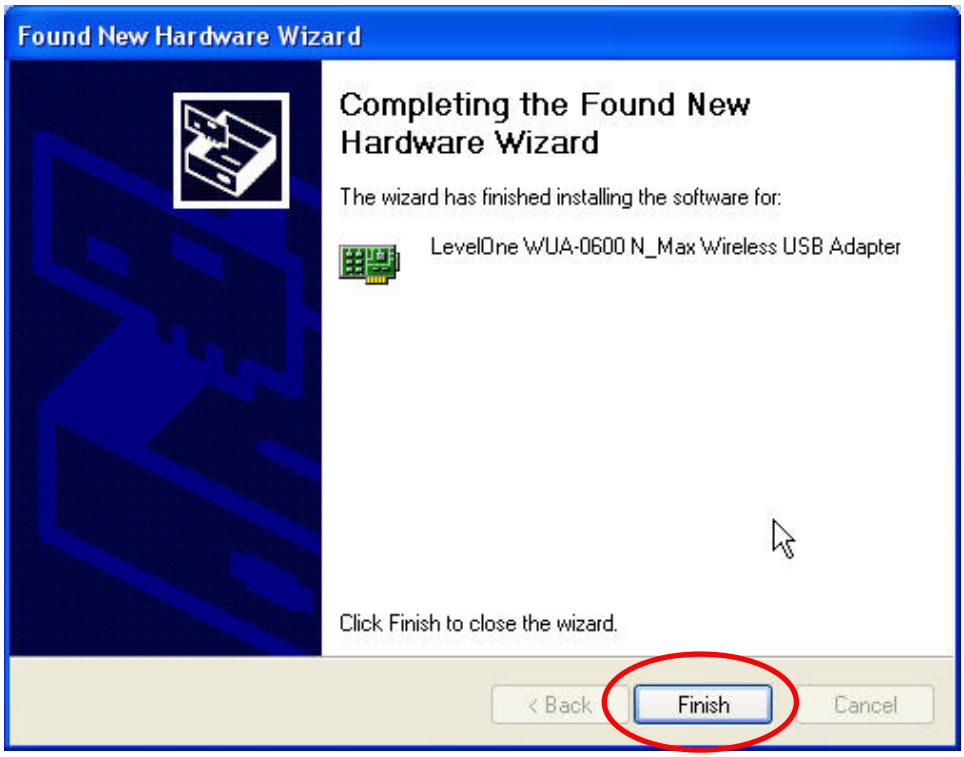
4. Insert the *N_Max* Wireless USB adapter into the USB port, the following screen will prompt, click "**Next**" to continue.



5. Select "**Install the software automatically (Recommended)**" and click "**Next**" to continue.

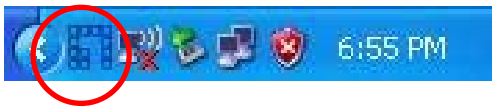


6. The warning message will pop up, please select "**Continue Anyway**"
7. The software installation has now completed.



The installation program will help you to setup the Wireless LAN utility. ***Be noted that the Windows XP and Vista have its own Wireless Utility; you can either use the utility of Windows XP/Vista or the provided utility.***

When the Wireless LAN utility is installed properly, you will see the icon on the Windows task bar. The user can configure the wireless settings using the Wireless USB Adapter Configuration Utility. Double-click the utility icon that appears in the taskbar



When the icon in the toolbar represents in full blue color then the signal strength has an excellent performance with the AP, if it represents in half blue color then the signal strength has a fair performance with the AP, and if the icon represents in low blue, then the signal strength has a worst performance with the wireless station.

 Excellent Wireless Signal Strength

 Adequate Wireless Signal Strength

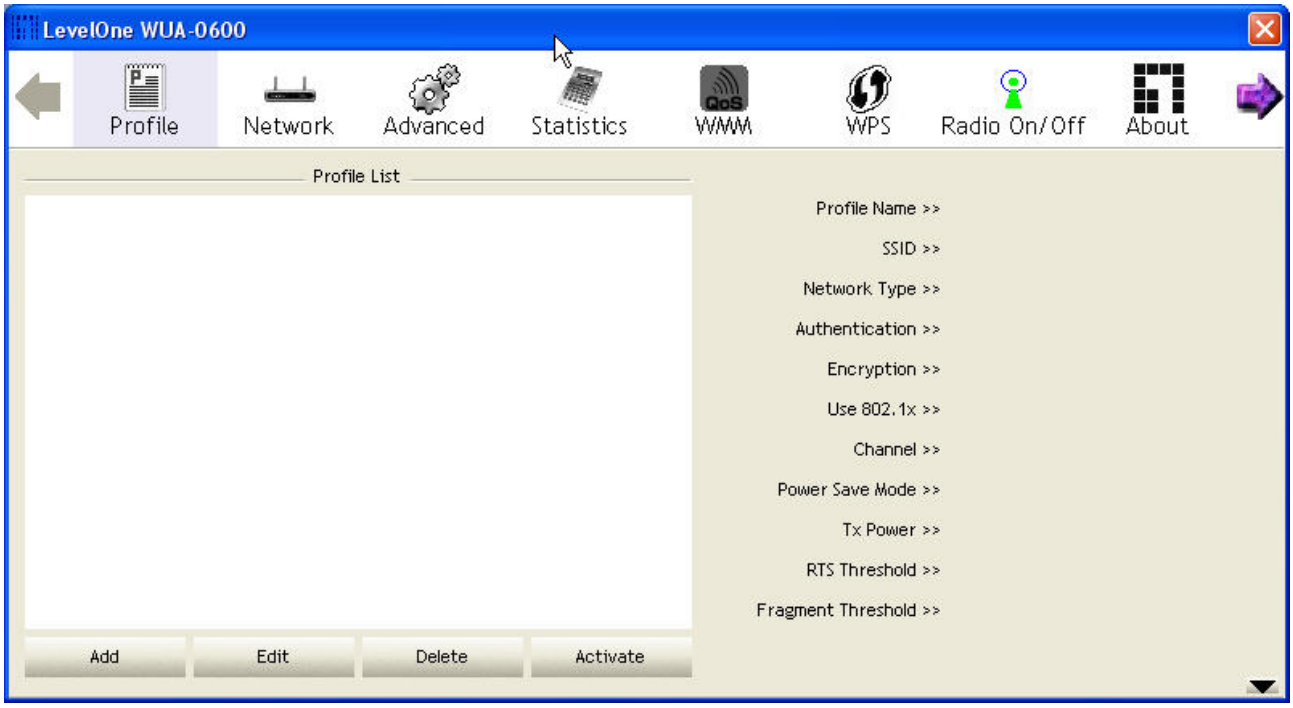
 Low Wireless Signal Strength

 Wireless Card inactive

Wireless Utility Configuration

Profile

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



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

Configure: Configure the wireless network.

Profile Name: The name of the profile; 0-32 ASCII characters and symbols are allowed; no spaces can be used.

SSID: Select the SSID (Service Set Identity) name of the wireless network to which the client will connect.

Network Type: Wireless network type. The default setting is Infrastructure mode.

Ad hoc: An ad hoc wireless LAN is a group of computers each with wireless adapters, connected as an independent wireless LAN. Select Ad hoc to associate to a peer computer.

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

Power Save Mode (available when Infrastructure mode is selected as the network type)
Enable or disable the power save operation. (Default: CAM)

CAM: Constantly awake mode, which always keeps the radio on.

PSM: Power save mode, which turns the radio off when no data is being transferred.

TX Power: The amount of power transmitted by the radio when sending a signal. (Default: Auto)

Preamble (available when Ad hoc is selected as the network type)
Select Auto to have the Wireless USB Adapter automatically use short preamble if the clients and access points in your wireless network support this feature, otherwise select “Long“. (Default: Auto)

Channel (only available when “Ad hoc“ is selected as the network type)
The radio channel used to communicate with wireless clients. The channel has to be the same as the peer computer. (Default: 1)

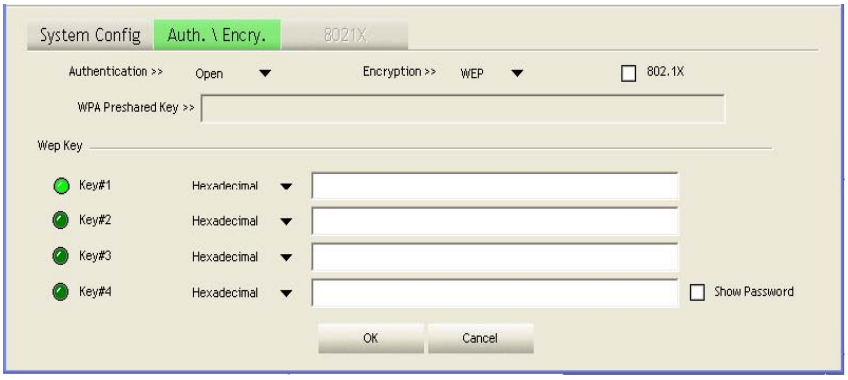
RTS Threshold: Adjust the RTS threshold value by sliding the bar or key in the value directly when the feature is enabled. (Default: Disabled) Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The Wireless USB Adapter sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.
If the RTS threshold is set to 0, the Wireless USB Adapter always sends RTS signals. If set to 2347, the Wireless USB Adapter never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

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

Fragment Threshold: Adjust the Fragment threshold value by sliding the bar or key in the value directly when the feature is enabled. (Default: Disabled) The fragmentation threshold is the minimum packet size that can be fragmented when passing through the adapter. Fragmentation of the PDUs

(Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. (Range: 256-2346 bytes; Default: 2346 bytes)
Click Ok to confirm the configuration or click Cancel to cancel the settings.

Authentication / Encryption: Configure authentication and encryption to match the security of the wireless network.



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

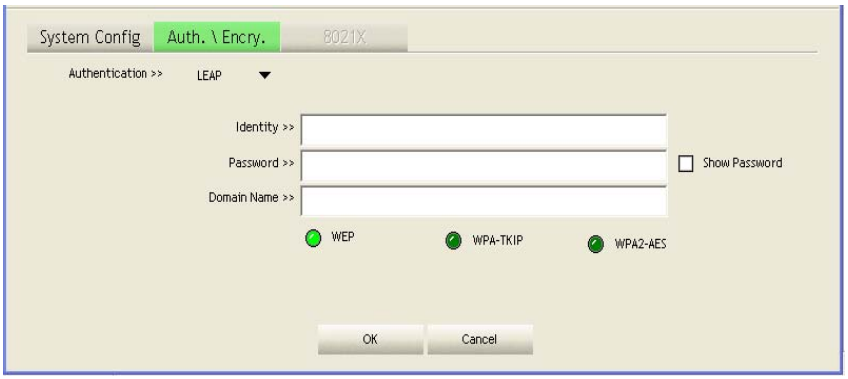
Authentication: Select the authentication mode. For an infrastructure network, seven modes are supported by the Wireless USB Adapter, including Open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK. For an ad hoc network, Open, Shared and WPA-None modes are supported.

Open: Open-system authentication accepts any client attempting to connect to the access point without verifying its identity.

Shared: The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to clients before attempting authentication.

LEAP: The Lightweight Extensible Authentication Protocol (LEAP) is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication. When LEAP is select, input LEAP identity, password, domain name, and select encryption type. Check the Show Password box to display password characters as you type instead of asterisks.

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



WPA / WPA-PSK: Wi-Fi Protected Access (WPA) employs a combination of technologies to provide an enhanced security solution for wireless networks. The WPA Pre-shared Key (WPA-PSK) mode for small networks uses a common password phrase that must be manually distributed to all clients that want to connect to the network.

WPA2 / WPA2-PSK: WPA2 is a further security enhancement that includes the now ratified IEEE 802.11i wireless security standard.

Encryption

Configure the encryption. For open and shared authentication mode, the selection options are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.

None: No encryption is used.

WEP: Enables the Wireless USB Adapter to use WEP shared keys. If enabled, you must configure at least one key. Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

TKIP: Use Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

AES: Use Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

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

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

EAP Method: Select an 802.1X authentication method.

PEAP: Protected Extensible Authentication Protocol. PEAP transport securely sends authentication data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.

TLS / Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

TTLS: Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

EAP-Fast: Flexible Authentication via Secure Tunneling. An authentication method developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution. For tunnel authentication, only "Generic Token Card" authentication is supported currently. –

MD5-Challenge: Message Digest Challenge. MD5 is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.

Tunnel Authentication: Selects the tunnel authentication protocol. This pull-down menu is only available when the authentication type is PEAP or TTLS. When EAP-FAST is used, the protocol setting is always Generic Token Card and cannot be changed.

EAP-MSCHAP v2: This authentication uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

EAP-TLS / SmartCard: This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It uses a client certificate for authentication.

Generic Token Card: This authentication uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

CHAP: This authentication uses an MD5 one-way encryption scheme to hash the response to a challenge issued by the authenticator. It requires passwords to be stored in a reversibly encrypted form.

MS-CHAP: This authentication is similar to CHAP; the main difference is that with MS-CHAP the password only needs to be stored as a MD4 hash instead of a reversibly encrypted form.

MS-CHAP-V2: MS-CHAP v2 is similar to MS-CHAP with the difference that the server also authenticates itself with the client.

PAP: PAP provides a simple method for a remote node to establish its identity using a two-way handshake. A username and password pair is repeatedly sent by the remote node across the link until authentication is acknowledged.

ID / Password: Configures the identity and password for authentication.

Authentication ID / Password: Identity, password and domain name of the server. Only "EAP-FAST" and "LEAP" authentication require a domain name.

Tunnel ID / Password: Identity and Password of the authentication server.

Client Certification: Enable client certification.

Use Client Certification: If PEAP or TTLS is selected as the authentication method, you can use a certificate stored in the local computer. If TLS/Smart Card is used, this box is always checked.

Server Certification: Enable server certification.

User Certificate Chain: Enable the use of certificate chain and select a certification authority (CA) server.

Allow Intermediate certificates: Enable the use of intermediate certificates.

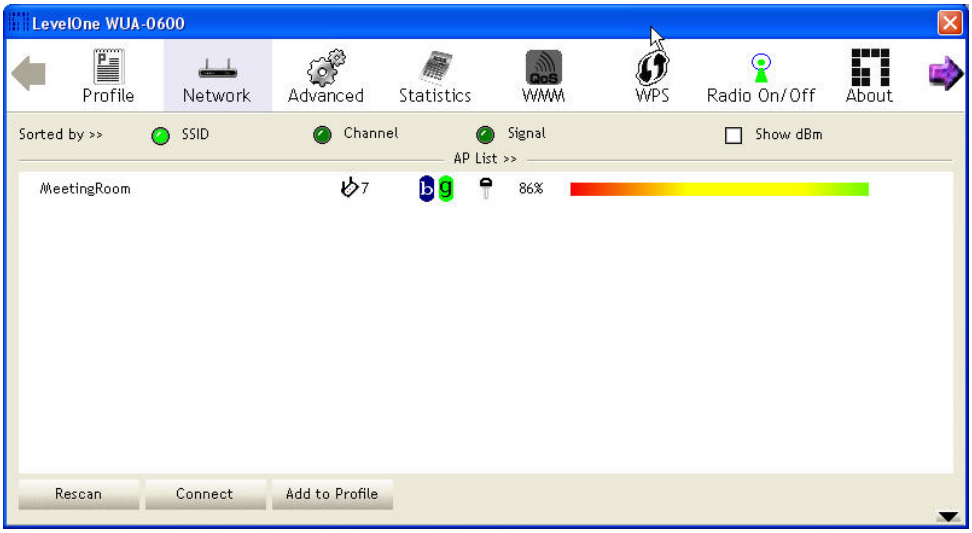
Sever Name: Input the server name of CA server here.

Server Name must match exactly: Enable the wireless configuration utility to check that the CA server name setting matches with the connected CA server. If not, the connection is dropped.

Domain Name must end in specified name: Enable the wireless configuration utility to check the end of domain name. If defects are found, the connection is dropped.
Click OK to confirm the configuration or click Cancel to cancel the settings.

Network

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



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

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

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

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

Connect: Click the button to connect the selected network.

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

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

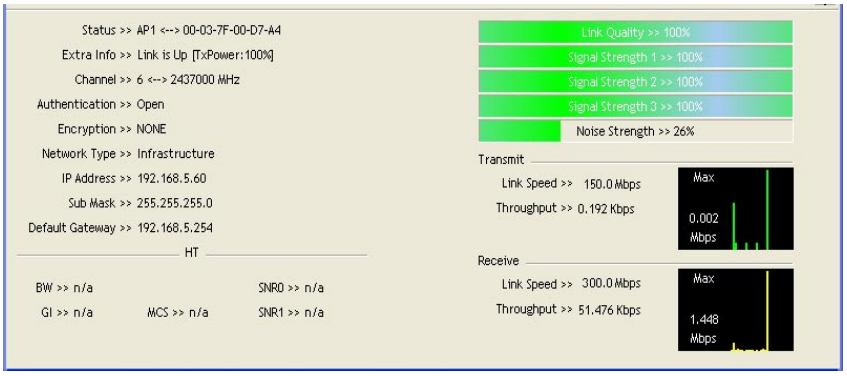
	Icon Indications
Icons	**Description**

g	The network supports 802.11g connections
n	The network supports 802.11n connections

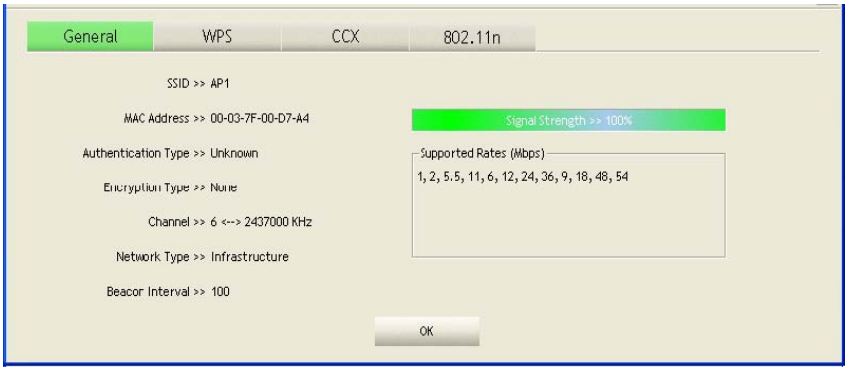
You can press the button on the bottom right corner to display the network status, as shown below.

Note

The maximum transmit link speed of this wireless USB adapter is 150 Mbps and the maximum receive link speed is 270 Mbps.



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



Advanced

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

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

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

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

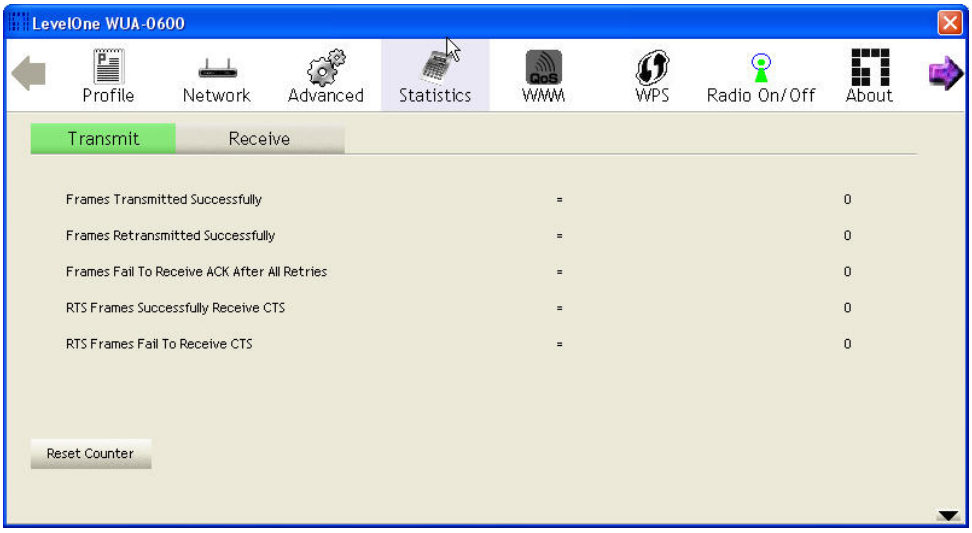
Enable TCP Window Size: Adjust TCP window size automatically for better performance.

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

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

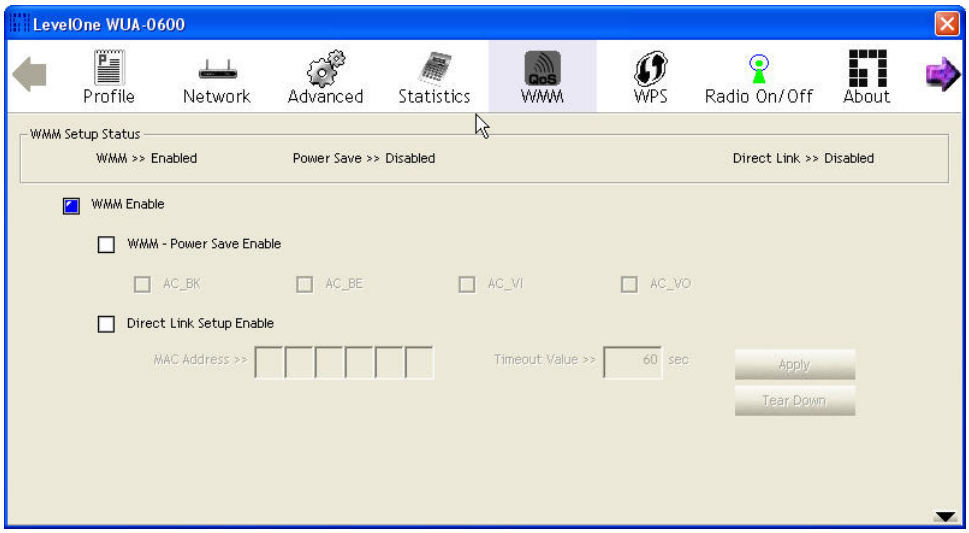
Statistics

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



WMM

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



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

WMM Enable: Enable WMM function.

WMM - Power Save Enable: Enable the power save mode.

- **AC_BK**: Background / low priority
- **AC_BE**: Best effort
- **AC_VI**: Video first
- **AC_VO**: Voice first

Direct Link Setup Enable: Enable DLS (Direct Link Setup) function.

MAC Address: MAC address of another WMM-enabled wireless device that has a direct link to this Wireless USB Adapter.

- **Timeout Value**: Set the time period before automatically disconnecting the WMM-enabled wireless device. If the value is zero, the link is always connected. (Default: 60 seconds; Range: 0-65535)
- **Tear Down:** Select the device that you want to remove from DLS table and click this button.

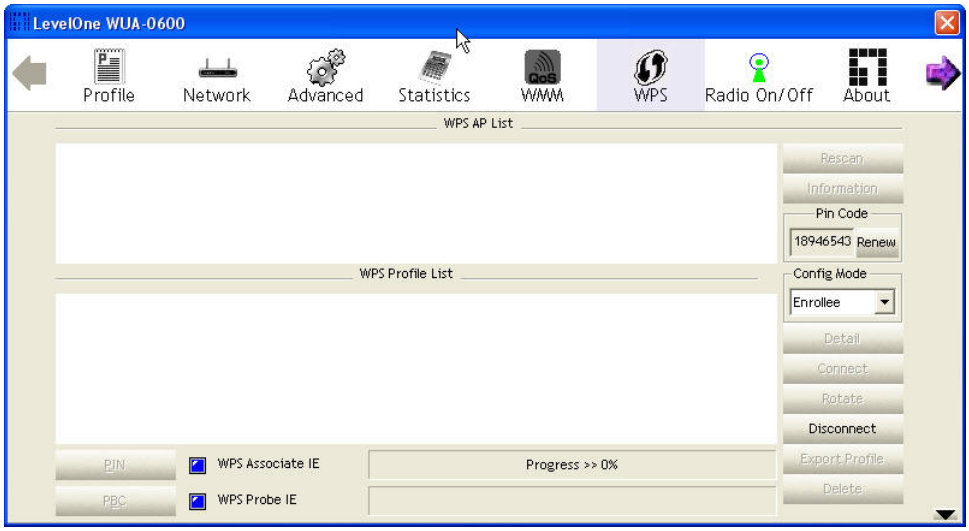
WPS

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

WPS Setup - PBC (Push-button Configuration)

1. Push the WPS button on your wireless access point or start WPS standby mode as instructed by the wireless access point‘s user manual.
2. Before you start to establish the wireless connection using WPS, define the Wireless USB Adapter as a WPS —“Enrollee“ or a —“Registrar“ by selecting the Config Mode options.

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



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

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

Note

If WPS fails, click the PBC button few more times to try again.

4. When an access point or a WPS enrollee is connected, you can click Disconnect to disconnect from the connected device, or select another WPS-enabled wireless access point or enrollee, then click Connect to establish connection.
5. You can also click the “Rotate” button to select the next access point or enrollee in the list and establish a connection.
6. To delete an access point from the list, click Delete.

WPS Setup - PIN Configuration

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

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

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

Note

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

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

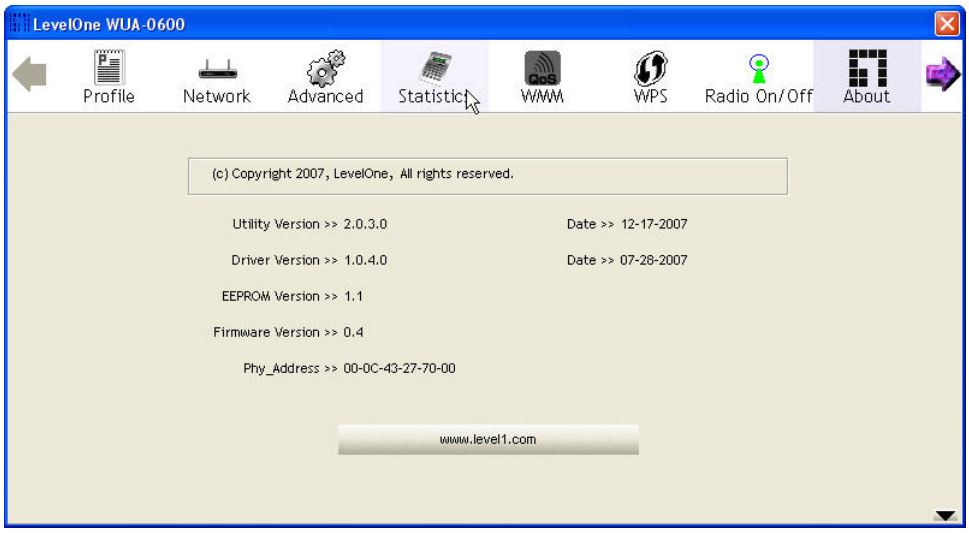
   Click PIN button and wait for few seconds to one minute. If a WPS enrollee with correct PIN code is found, it will be connected to the Wireless USB Adapter.

Radio Setting

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

About

This page displays the information of version numbers, configuration utility, firmware and other information regarding this wireless USB adapter. Click the www.level1.com button to visit the LevelOne website for other information.



Network Planning

LevelOne WUA-0600 *N_Max* Wireless USB Adapter supports a stand-alone wireless network configuration, as well as an integrated configuration with Ethernet LANs.

The wireless USB adapter can be configured as:

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

Network Topologies Ad Hoc Wireless LAN

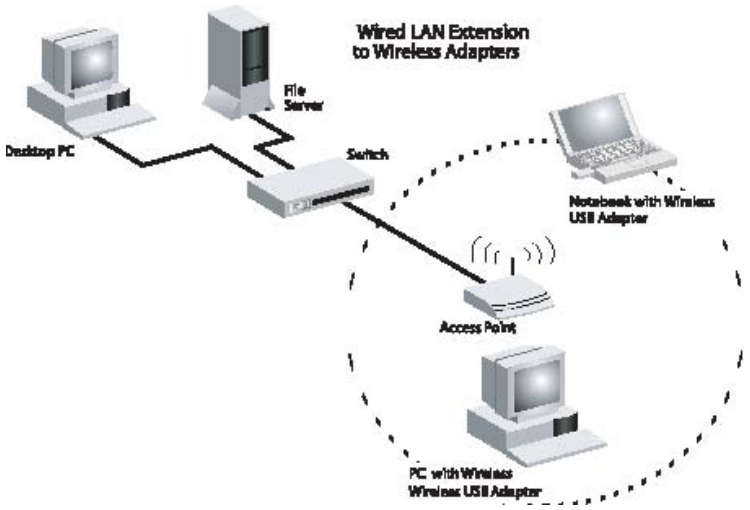
An ad hoc wireless LAN consists of a group of computers, each equipped with a wireless adapter, connected via radio signals as an independent wireless LAN.

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

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

Infrastructure Wireless LAN

LevelOne WUA-0600 can also provide access to a wired LAN for wireless workstations. An integrated wired and wireless LAN is called an Infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users, and an access point that is directly connected to the wired LAN. Each wireless PC in this BSS can communicate with to any computer in its wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure via an access point.



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

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

Technical Specifications

General	
Radio Specification	IEEE 802.11n (draft 2.0), IEEE 802.11b/g
Interface	USB Version 2.0 Compliant
Data Transfer Rate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps 802.11n (draft 2.0) offering up to 270Mbps
Receiver Sensitivity	Draft N 40MHz Channel Spacing -65dBm @ 64-QAM Draft N 20MHz Channel Spacing -70dBm @ 64-QAM 54Mbps: Typical -72dBm @ 10% PER (Packet Error Rate) 11Mbps: Typical -86dBm @ 8% PER (Packet Error Rate)
Transmit Power	Draft N: 14.5 ±1dBm 802.11g: 14.5±1dBm 802.11b: 17.5±1dBm
Frequency Range	2412 ~ 2462 MHz ISM band (channels 1 ~ 11) 2412~2472MHz ISM band (channels 1 ~ 13)
Modulation Schemes	DBPSK/DQPSK/CCK/OFDM
Channels	1~11 channels (FCC), 1~13 channels (ETSI), 1~14 channels (MKK-Japan)
Security	64/128-bits WEP Encryption, WPA-PSK, WPA2-PSK, WPA, WPA2
Diagnostic LED	Link/Act WPS Auth.
Antenna	Two internal 2 dBi antennas Frequency Range: 2.4 ~ 2.5GHz Gain: 0 ~ 1 dBi VSWR: 2.0 Max Polarization Linear Impedance: 50 Ohm
Physical and Environmental	
Driver Support	Windows 2000, Windows XP, Windows Vista
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C

Humidity	10% ~ 95% RH, no condensation
Dimensions	82 x 26 x 11mm
Certifications	EN60960-1, Part 15B, EN301489-1/-17, Part 15C, EN300328