Copyright Statement

Tenda® is the registered trademark of Shenzhen Tenda Technology Co., Ltd. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. Without prior expressed written permission from Shenzhen Tenda Technology Co., Ltd, any individual or party is not allowed to copy, plagiarize, reproduce, or translate it into other languages.

All photos and product specifications mentioned in this manual are for references only. Upgrades of software and hardware may occur; Tenda reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes. If you would like to know more about our product information, please visit our website at www.tendacn.com.

Table of Contents

Chapter 1 Product Overview

W310A is a best–in–class 802.11n indoor access point designed specifically for business–class environments such as hotels, airports, coffee shops, shopping centers, sporting venues, and university campus. With transfer rates of up to 300 Mbps on the 2.4 GHz frequency band, the device provides an adequate level of service to all users who connect with legacy 802.11b/g adapters in addition to the latest 802.11n adapters for faster downloads and instant communication. Versatile and powerful, the W310A offers a built–in USB port that charges mobile devices such as a smart phone or an iPad via a USB cable. Integrated 802.3af Power over Ethernet (PoE) allows installation in areas where power outlets are not readily available. Plus, the provided unified management utility based on X86 allows network administrators to centrally manage IP addresses, SSID and security settings, etc of APs on LAN, thus enabling a highly manageable and extremely robust wireless network.

1.1 Package Contents

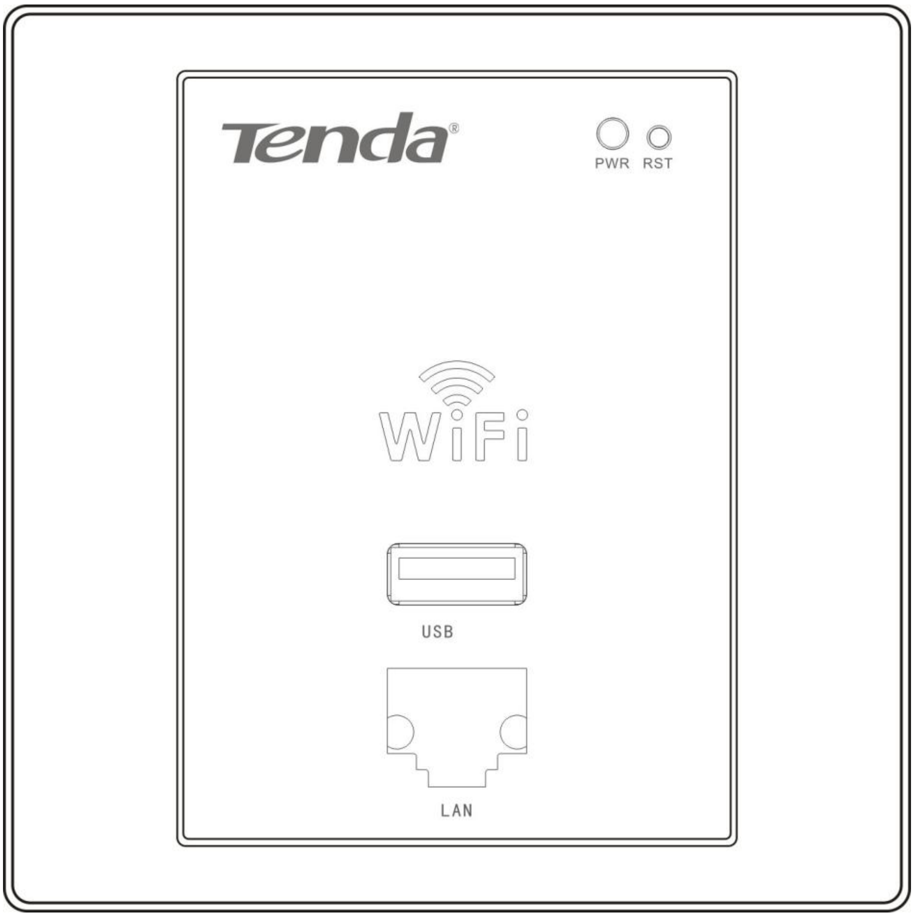
The product package should contain the following items:

- W310A
- 2 Screws
- Quick Install Guide

If any of the above items is incorrect, missing, or damaged, please contact your Tenda reseller for immediate replacement.

1.2 Hardware Description

The wireless access point hardware functions are described below.



The following explains the LED indicators.

PWR: Power Indicator

Solid: Device is receiving electrical power.

Blink: Device is operating properly.

Off: Device is receiving no electrical power or connected to power supply improperly;

RST: Restores the device to the factory default settings when pushed and held for 7 seconds.

The following explains the interfaces:

USB Port: USB port that charges mobile devices such as a smart phone or an iPad via a USB cable.

LAN: 100M Ethernet Port for connecting to an Ethernet LAN device such as a PC or switch, etc.

1.3 Features

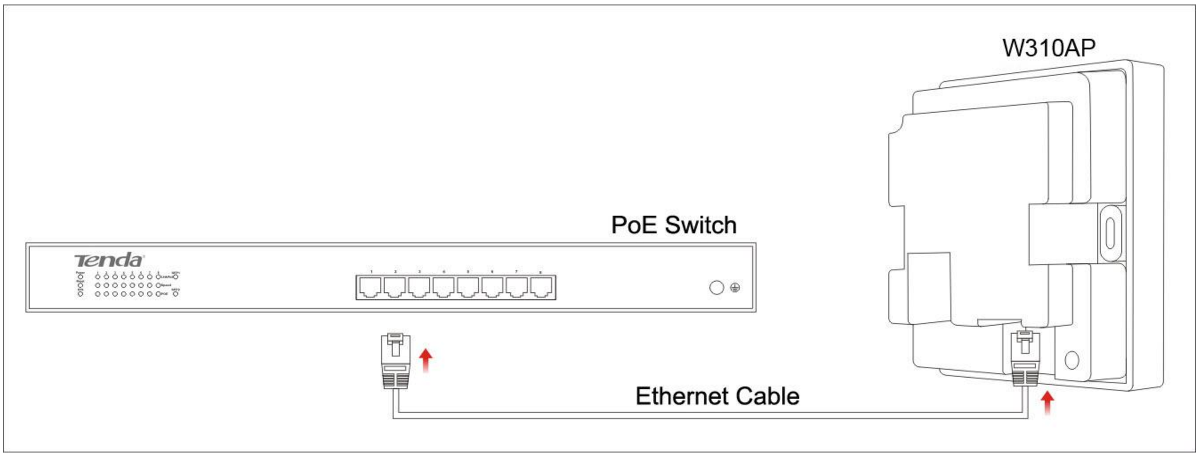
- Compliant with IEEE 802.11n/g/b
- 100M Ethernet port for wired LAN connection
- Wireless rates of up to 300Mbps
- Integrated Power over Ethernet (IEEE802.3af) lowers deployment costs
- Unified Management allows network administrators to centrally manage APs on LAN
- WEP, WPA–PSK, WPA2–PSK and WPA–PSK/WPA2–PSK encryptions secure wireless network against unauthorized accesses
- Can be configured to select an optimum channel for device to operate on
- Provide powered USB for charging mobile devices like smartphones
- Transmit power tunable

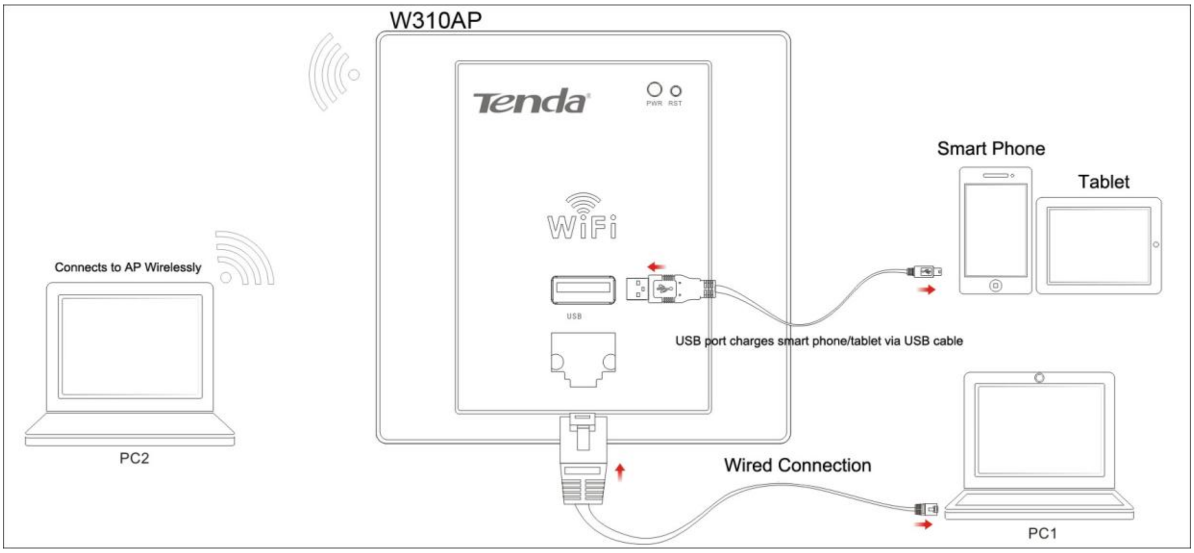
Chapter 2 Installation

1. **Connect one end of one Ethernet cable to a PoE switch** and the other end to the PoE port on the W310A.

2. **Connect one end of another Ethernet cable to the LAN** port on the W310A and the other end to your PC or connect your PC to W310A wirelessly.

The connection diagram is shown below:




W310AP
Tenda
PWR RST
WiFi
USB
Smart Phone
Tablet
Connects to AP Wirelessly
USB port charges smart phone/tablet via USB cable
PC2
Wired Connection
PC1

Chapter 3 Configuration Guide

3.1 Web Login

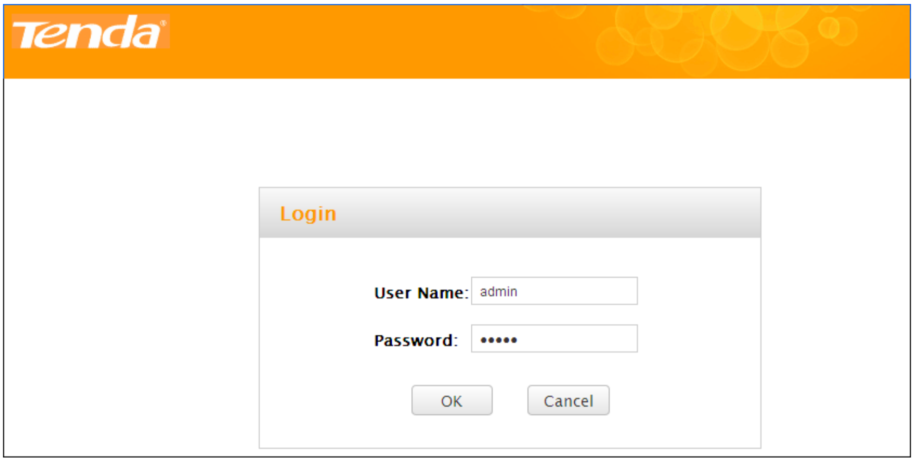
Connect to the W310A via a wired connection (Ethernet cable). The default IP address of your wireless access point is 192.168.0.254. If you are using the default IP subnet, the computer you are using to connect to the device should be configured with an IP address that starts with 192.168.0.x (where x can be any number between 1~253) and a Subnet Mask of 255.255.255.0; if you have changed the subnet of the wireless access point, the computer you are using to connect must be within the same subnet. For TCP/IP settings, see **Appendix 1**.

To connect to the W310A using the defaults IP address:

1. Open a Web browser.

2. Enter 192.168.0.254 into your browser.

3. When prompted enter the default User Name **admin** and default Password **admin** into the login window.

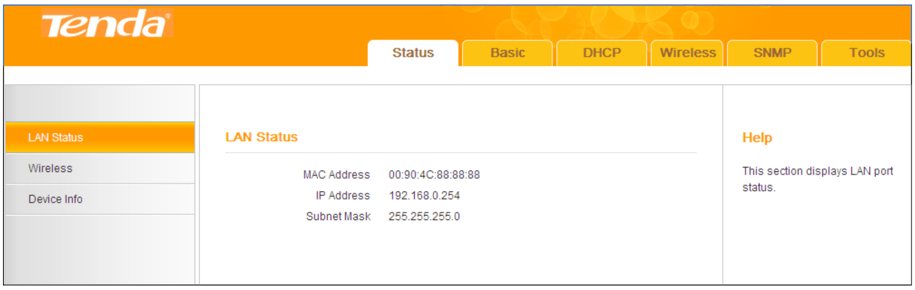


Login

User Name: admin

Password: •••••

4. Click **OK** and your Web browser shall automatically display the home page, as shown below:



LAN Status

MAC Address 00:90:4C:88:88:88
IP Address 192.168.0.254
Subnet Mask 255.255.255.0

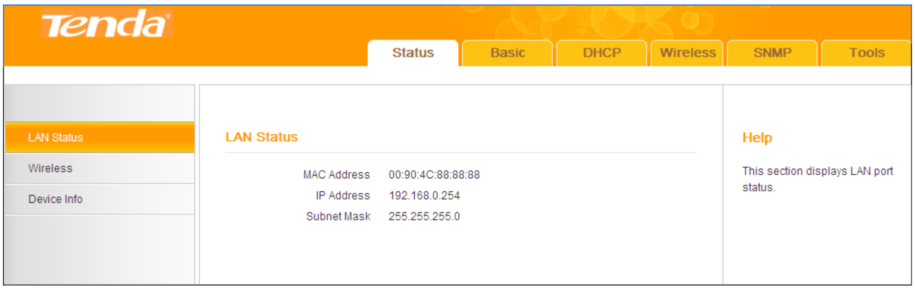
Help

This section displays LAN port status.

3.2 Status

3.2.1 LAN Status

This screen displays the MAC address, IP address and subnet mask of current AP’ s LAN interface.



LAN Status

MAC Address 00:90:4C:88:88:88
IP Address 192.168.0.254
Subnet Mask 255.255.255.0

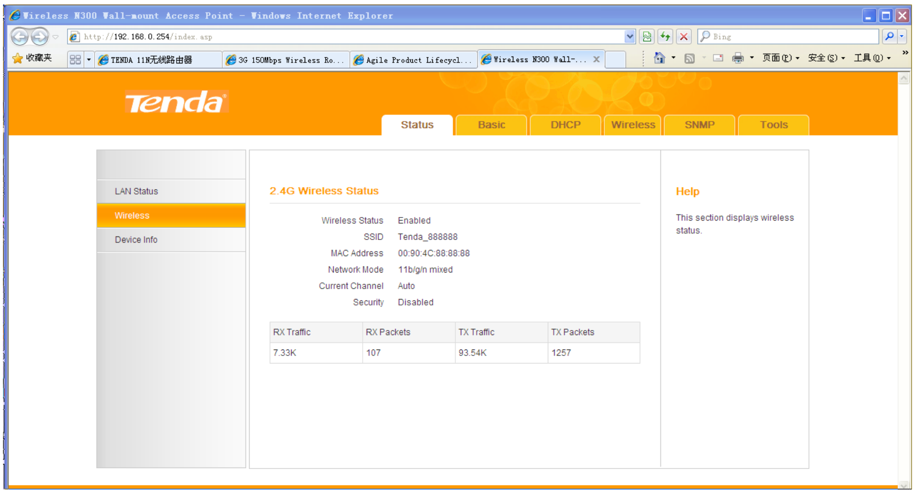
Help

This section displays LAN port status.

- **MAC Address**: Displays current AP’ s LAN MAC address.
- **IP Address**: Displays current AP’ s IP address.
- **Subnet Mask**: Displays current AP’ s subnet mask.

Wireless Status

This section displays wireless status, SSID, MAC address, network mode, current channel, security and traffic statistics.


Wireless N300 Wall-mount Access Point - Windows Internet Explorer
http://192.168.0.254/index.asp
Bing
收藏夹
TENDA 11N无线路由器
3G 150Mbps Wireless Ro...
Agile Product Lifecycl...
Wireless N300 Wall-...
页面(P)
安全(S)
工具(O)
Tenda
Status
Basic
DHCP
Wireless
SNMP
Tools
LAN Status
Wireless
Device Info

2.4G Wireless Status

Wireless Status	Enabled
SSID	Tenda_888888
MAC Address	00:90:4C:88:88:88
Network Mode	11b/g/n mixed
Current Channel	Auto
Security	Disabled

RX Traffic	RX Packets	TX Traffic	TX Packets
7.33K	107	93.54K	1257

Help

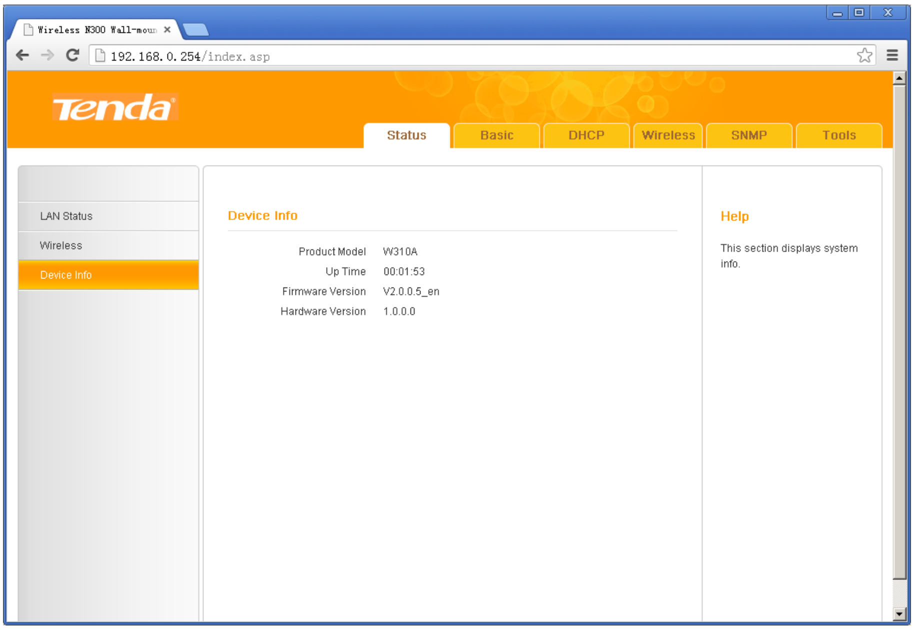
This section displays wireless status.

- Wireless Status: Displays whether wireless is enabled or not.
- SSID: Displays current SSID of the wireless network.
- MAC Address: Displays the MAC address of device’s wireless interface.
- Network Mode: Displays currently operative network mode.
- Current Channel: Displays the channel that device is currently operating on.
- Security: Displays current security Mode.

Wireless traffic statistics info is shown on the table on the bottom of the screen.

Device Info

This screen displays device info including Product Model, Up Time, Firmware Version and Hardware Version.



Device Info

Product Model W310A
Up Time 00:01:53
Firmware Version V2.0.0.5_en
Hardware Version 1.0.0.0

Help

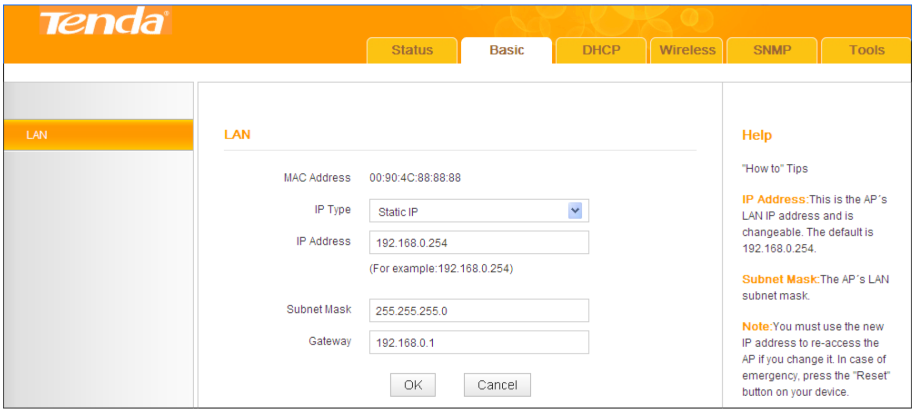
This section displays system info.

- Product Model：Displays device's model number.
- Up Time: Displays device's uptime.
- Firmware Version: Displays Device’s current firmware version.
- Hardware Version: Displays Device’s current hardware version.

3.3 Basic

3.3.1 LAN

The basic LAN settings for your access point are configured on this screen. Most of the default settings work in most cases. However, if your access point is part of a more complex LAN network, then modify the settings to meet the requirements of your network based on the explanation of the various fields.



LAN

MAC Address 00:90:4C:88:88:88

IP Type: Static IP

IP Address: 192.168.0.254

(For example:192.168.0.254)

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

Help

"How to" Tips

IP Address:This is the AP´s LAN IP address and is changeable. The default is 192.168.0.254.

Subnet Mask:The AP´s LAN subnet mask.

Note:You must use the new IP address to re-access the AP if you change it. In case of emergency, press the "Reset" button on your device.

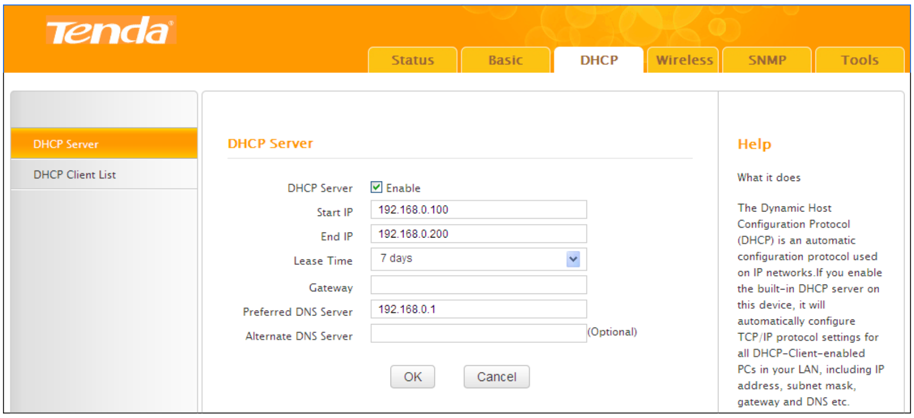
- **Static IP:** Manually specify the Static IP information that corresponds with your existing networking equipment. The default LAN IP is 192.168.0.254. You change the default LAN IP address, gateway address and subnet mask.
- **Dynamic IP:** Select it if you have a DHCP server on your LAN and you enable DHCP. The wireless access point gets its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the access point to your LAN.

  ⚠ **Note:** You must log on to device web utility using the new IP address once you changed it.

3.4 DHCP

3.4.1 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built–in DHCP server on the device, it will automatically configure the TCP/IP settings for all your LAN computers (including IP address, subnet mask, gateway and DNS etc), eliminating the need of manual intervention. Just be sure to set all computers on your LAN to be DHCP clients by selecting "**Obtain an IP Address Automatically**" respectively on each such PC. When turned on, these PCs will automatically load IP information from the DHCP server. (This feature is enabled by default. Do NOT disable it unless necessary).



DHCP Server

DHCP Server ☑ Enable
Start IP 192.168.0.100
End IP 192.168.0.200
Lease Time 7 days
Gateway
Preferred DNS Server 192.168.0.1
Alternate DNS Server (Optional)

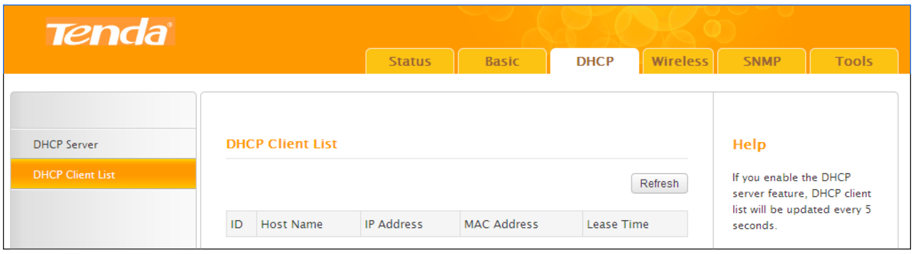
Help

What it does

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks.If you enable the built-in DHCP server on this device, it will automatically configure TCP/IP protocol settings for all DHCP-Client-enabled PCs in your LAN, including IP address, subnet mask, gateway and DNS etc.

3.4.2 DHCP Client List

DHCP Client List displays information of devices that have obtained IP addresses from the device' s DHCP Server including MAC address and lease time, etc.



DHCP Client List

ID	Host Name	IP Address	MAC Address	Lease Time

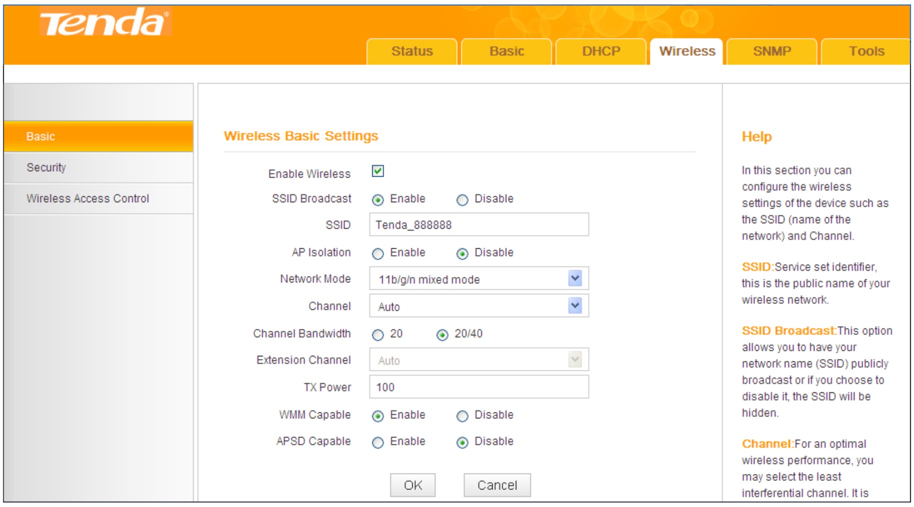
Help

If you enable the DHCP server feature, DHCP client list will be updated every 5 seconds.

3.5 Wireless

3.5.1 Basic

This section describes how to configure the available wireless settings.



Wireless Basic Settings

Enable Wireless ☑

SSID Broadcast ● Enable ○ Disable

SSID Tenda_888888

AP Isolation ○ Enable ● Disable

Network Mode 11b/g/n mixed mode

Channel Auto

Channel Bandwidth ○ 20 ● 20/40

Extension Channel Auto

TX Power 100

WMM Capable ● Enable ○ Disable

APSD Capable ○ Enable ● Disable

Help

In this section you can configure the wireless settings of the device such as the SSID (name of the network) and Channel.

SSID:Service set identifier, this is the public name of your wireless network.

SSID Broadcast:This option allows you to have your network name (SSID) publicly broadcast or if you choose to disable it, the SSID will be hidden.

Channel:For an optimal wireless performance, you may select the least interferential channel. It is

- **Enable Wireless:** Check/uncheck to enable/disable the wireless feature.
- **Broadcast (SSID):** Select **Enable/Disable** to make your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan they perform a scan to see what's available. When disabled, such wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID. By default, it is enabled.
- **SSID:** This is the public name of your wireless network.
- **AP Isolation:** When enabled, devices wirelessly connected to the same SSID will be unable to intercommunicate. This will further improve wireless network security.
- **Network Mode:** Select a right mode according to your wireless client. The default mode is 11b/g/n mixed.

  11b mode: Select it if you have only 11b wireless devices in your wireless network. Up to 11Mbps wireless rate is supported on this mode.

  11g mode: Select it if you have only 11g wireless devices in your wireless network. Up to 54Mbps wireless rate is supported on this mode.

11b/g mixed mode: Select it if you have 11b and 11g wireless devices in your wireless network.

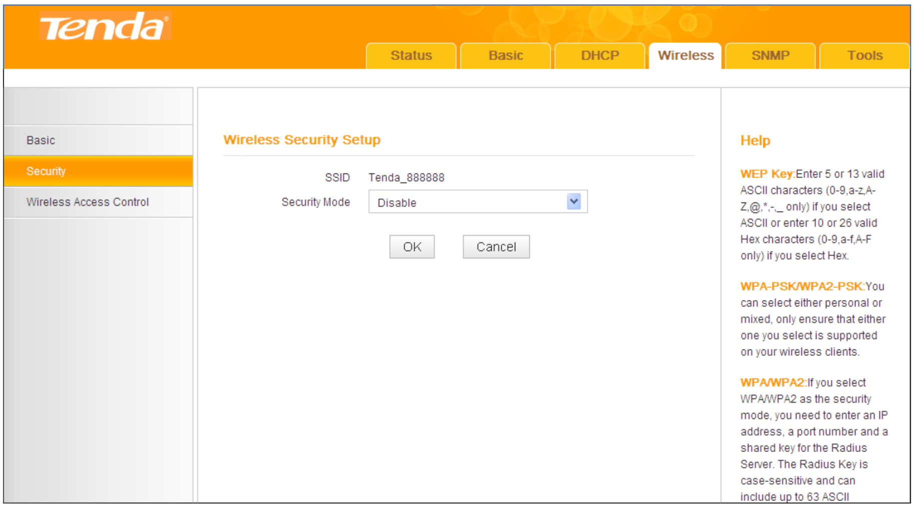
11b/g/n mixed mode: Select it if you have 11b, 11g and 11n wireless devices in your wireless network. In this mode wireless connection rate is negotiated.

- **Channel:** Select from 1~13 channels or Auto. The best selection is a channel that is the least used by neighboring networks.
- **Extension Channel:** This is used to ensure N speeds for 802.11n devices on the network.
- **Channel Bandwidth:** Select a proper channel bandwidth to enhance wireless performance. Select 20/40M frequency width when device is operating in 11n, select 20M frequency width when device is operating in non-11n mode.
- **WMM-Capable:** WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data such as video or audio (recommended).
- **ASPD Capable:** Select to enable/disable the auto power saving mode. By default, this option is disabled.
- **TX Power:** Configure a proper power level for optimal performance. The default is 100.

3.5.2 Security

Use the security features appropriate to your needs to protect your wireless network from unauthorized accesses.

3 encryptions types are provided: WEP, WPA-PSK and WPA2-PSK.



Wireless Security Setup

SSID Tenda_888888

Security Mode Disable

Help

WEP Key:Enter 5 or 13 valid ASCII characters (0-9,a-z,A-Z,@,*,-,_ only) if you select ASCII or enter 10 or 26 valid Hex characters (0-9,a-f,A-F only) if you select Hex.

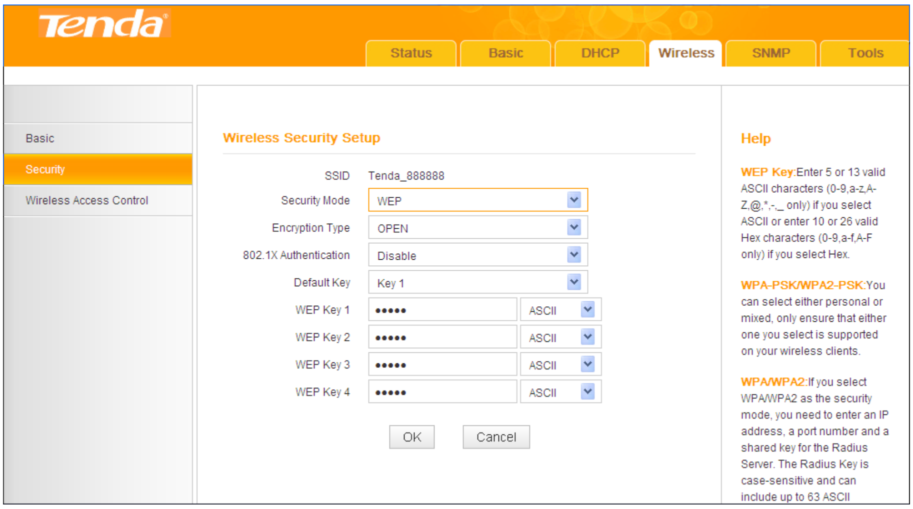
WPA-PSK/WPA2-PSK:You can select either personal or mixed, only ensure that either one you select is supported on your wireless clients.

WPA/WPA2:If you select WPA/WPA2 as the security mode, you need to enter an IP address, a port number and a shared key for the Radius Server. The Radius Key is case-sensitive and can include up to 63 ASCII

- **WEP**

Wired Equivalent Privacy (WEP) data encryption is intended to provide data confidentiality comparable to that of a traditional wired network. WEP is a legacy security setting. We recommend that you use WPA2 or WPA for stronger wireless security.

Select WEP from the Security screen and you can configure fields on the screen below:



Wireless Security Setup

SSID Tenda_888888

Security Mode WEP

Encryption Type OPEN

802.1X Authentication Disable

Default Key Key 1

WEP Key 1 ••••• ASCII

WEP Key 2 ••••• ASCII

WEP Key 3 ••••• ASCII

WEP Key 4 ••••• ASCII

Help

WEP Key:Enter 5 or 13 valid ASCII characters (0-9,a-z,A-Z,@,*,-,_ only) if you select ASCII or enter 10 or 26 valid Hex characters (0-9,a-f,A-F only) if you select Hex.

WPA-PSK/WPA2-PSK:You can select either personal or mixed, only ensure that either one you select is supported on your wireless clients.

WPA/WPA2:If you select WPA/WPA2 as the security mode, you need to enter an IP address, a port number and a shared key for the Radius Server. The Radius Key is case-sensitive and can include up to 63 ASCII

- **Security Mode:** Select a proper WEP from the drop–down list.
- **Encryption Type:** Select OPEN or Shared from the drop–down list.

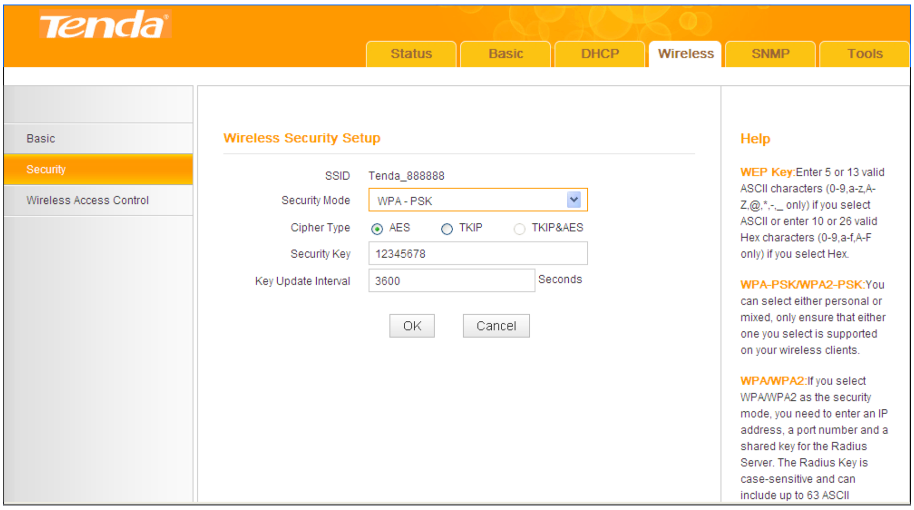
- **Default Key:** Select a key from the preset keys 1–4 for current use.
- **WEP Key**: Select ASCII or Hex for a WEP key. The ASCII supports 5 or 13 ASCII characters. The Hex supports 10 or 26 Hex characters.

- **WPA–PSK**

WPA–PSK

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128–bit per–packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only authorized network users can access the wireless network. WPA adopts enhanced encryption algorithm over WEP.

Select WPA–PSK from the Security screen and you can configure fields on the screen below:



Wireless Security Setup

SSID Tenda_888888

Security Mode WPA - PSK

Cipher Type ● AES ○ TKIP ○ TKIP&AES

Security Key 12345678

Key Update Interval 3600 Seconds

OK Cancel

Help

WEP Key:Enter 5 or 13 valid ASCII characters (0-9,a-z,A-Z,@,*,-,_ only) if you select ASCII or enter 10 or 26 valid Hex characters (0-9,a-f,A-F only) if you select Hex.

WPA-PSK/WPA2-PSK:You can select either personal or mixed, only ensure that either one you select is supported on your wireless clients.

WPA/WPA2:If you select WPA/WPA2 as the security mode, you need to enter an IP address, a port number and a shared key for the Radius Server. The Radius Key is case-sensitive and can include up to 63 ASCII

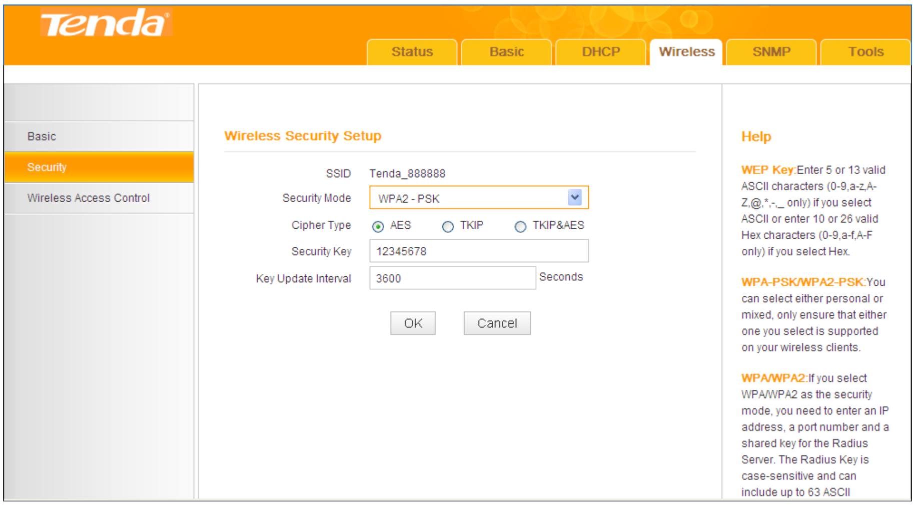
- **Cipher Type:** Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol). The default is AES.
- **Security Key:** Enter a security key, which must be between 8–63

ASCII characters (0~9,a~z,A~Z,@ ,*, – ,_).

- **Key Update Interval:** Specify a valid time interval for the key to be updated.

- **WPA2–PSK**

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.



Wireless Security Setup

SSID Tenda_888888

Security Mode WPA2 - PSK

Cipher Type ● AES ○ TKIP ○ TKIP&AES

Security Key 12345678

Key Update Interval 3600 Seconds

Help

WEP Key:Enter 5 or 13 valid ASCII characters (0-9,a-z,A-Z,@,*,-,_ only) if you select ASCII or enter 10 or 26 valid Hex characters (0-9,a-f,A-F only) if you select Hex.

WPA-PSK/WPA2-PSK:You can select either personal or mixed, only ensure that either one you select is supported on your wireless clients.

WPA/WPA2:If you select WPA/WPA2 as the security mode, you need to enter an IP address, a port number and a shared key for the Radius Server. The Radius Key is case-sensitive and can include up to 63 ASCII

- **Cipher Type:** Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol). The default is AES.
- **Security Key:** Enter a security key, which must be between 8–63 ASCII characters (0~9,a~z,A~Z,@ ,*, – ,_).
- **Key Update Interval:** Specify a valid time interval for the key to be updated.

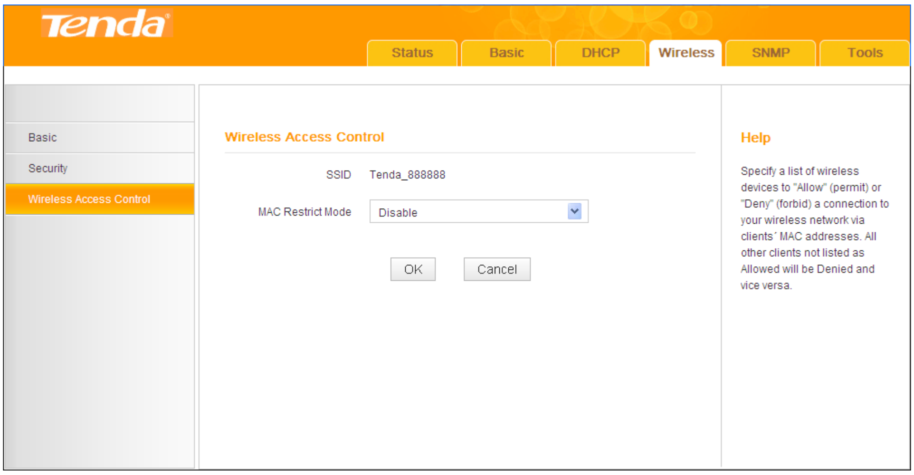
3.5.3 Wireless Access Control

Specify a list of devices to “Allow” or “Deny” a connection to your wireless network via the devices' MAC Addresses. All other devices not listed as Permitted will be Forbidden and vice versa.

MAC Restrict Mode: Select **Allow** or **Deny** from the drop–down list.

① To permit a wireless device to connect to your wireless network, select **Allow**, enter its MAC address, click **Add** and then **OK**. Then only this device listed as "Allowed" will be able to connect to your wireless network; all other wireless devices will be forbidden.

② To disallow a wireless device to connect to your wireless network, select **Deny**, enter its MAC address, click **Add** and then **OK**. Then this device listed as "Denied" will be unable to connect to your wireless network.



Wireless Access Control

SSID Tenda_888888

MAC Restrict Mode Disable

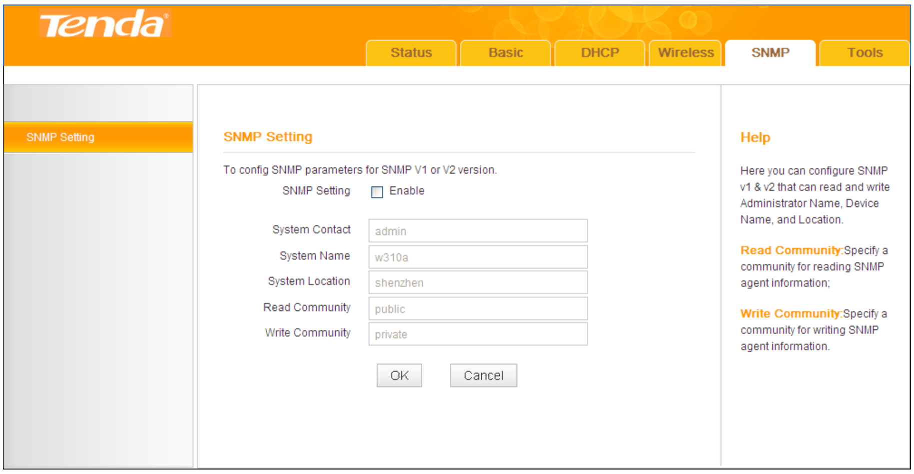
Help

Specify a list of wireless devices to "Allow" (permit) or "Deny" (forbid) a connection to your wireless network via clients' MAC addresses. All other clients not listed as Allowed will be Denied and vice versa.

3.6 SNMP

The Simple Network Management Protocol (SNMP) is widely used in local area networks (LANs) for collecting information, managing, and monitoring network devices, such as servers, printers, hubs, switches, and routers. Specialized software in each SNMP capable device, known as an Agent, continuously monitors the status of the device and reports the results to the SNMP Manager software, which can then act on the report.

This device supports both SNMP v1 and SNMP v2.



SNMP Setting

To config SNMP parameters for SNMP V1 or V2 version.

SNMP Setting ☐ Enable

System Contact	admin
System Name	w310a
System Location	shenzhen
Read Community	public
Write Community	private

OK Cancel

Help

Here you can configure SNMP v1 & v2 that can read and write Administrator Name, Device Name, and Location.

Read Community:Specify a community for reading SNMP agent information;

Write Community:Specify a community for writing SNMP agent information.

Click **Enable** to enable the SNMP feature.

- ***System Contact:*** Input the administrator’s name.
- ***System Name:*** Input the name of the AP, e.g., W310A.
- ***System Location:*** Input the AP’s location.
- ***Read Community:*** Indicates the community read access string to permit reading this AP’s SNMP information. The default is Public.
- ***Write Community:*** Indicates the community read/write access string to permit reading and re–writing this AP’s SNMP information. The default is Private.

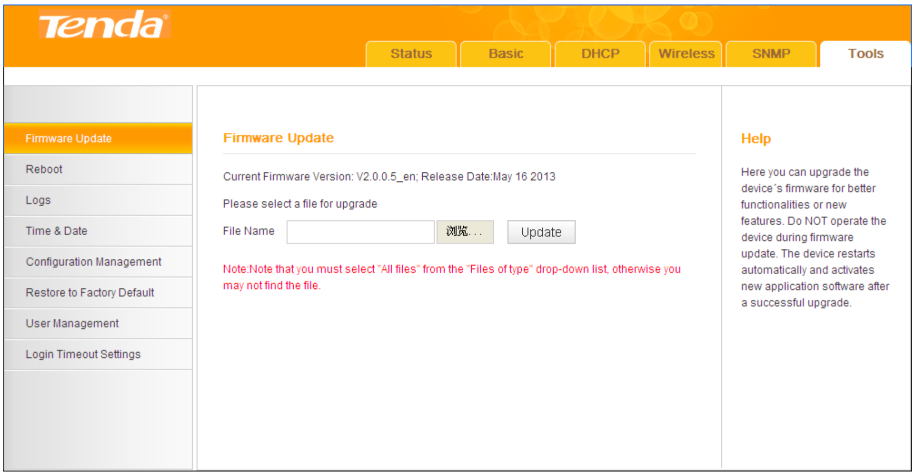
3.7 Tools

This chapter describes how to maintain the device.

3.7.1 Upgrading Software

Firmware upgrade is released periodically to improve the functionality of your device or to add new features. If you run into a problem with a specific feature of the device, log on to our website (www.tendacn.com) to download the latest firmware to update your device.

Click **Tools** –> **Firmware Update** to enter the screen below:



Firmware Update

Current Firmware Version: V2.0.0.5_en; Release Date:May 16 2013

Please select a file for upgrade

File Name

Note:Note that you must select "All files" from the "Files of type" drop-down list, otherwise you may not find the file.

Help

Here you can upgrade the device's firmware for better functionalities or new features. Do NOT operate the device during firmware update. The device restarts automatically and activates new application software after a successful upgrade.

To upgrade device software:

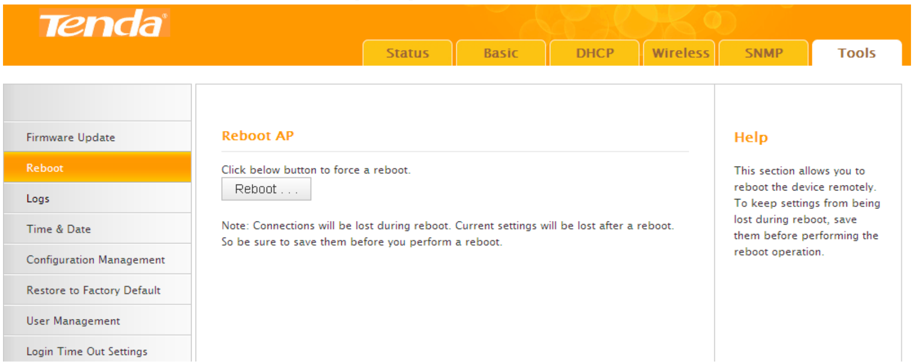
1. Open a web browser and go to www.tendacn.com to download latest firmware.
2. Unzip the compressed upgrade file (.ZIP file).
3. Click **Browse** to locate and select upgrade file on your hard disk.
4. Click **Update** to upgrade device firmware.
5. When the firmware upgrade completes, your wireless access point will automatically restart.
6. Restore the AP back to factory default settings after reboot.

⚠ **Warning:** When uploading software to the Wireless AP, it is important not to disconnect the device from power supply. If the power supply is interrupted, the upload may fail, corrupt the software, and render the device inoperable. When the upload completes, your wireless access point will automatically restart. The upgrade process typically takes about several minutes.

3.7.2 Rebooting Device

The Reboot option restarts the wireless access point using its current settings. Connections will be lost during reboot.

Click Tools –> Reboot to display screen below:



Reboot AP

Click below button to force a reboot.

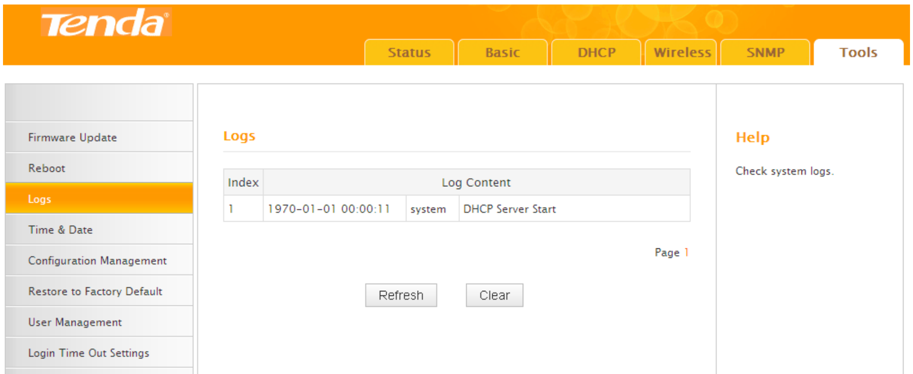
Note: Connections will be lost during reboot. Current settings will be lost after a reboot. So be sure to save them before you perform a reboot.

Help

This section allows you to reboot the device remotely. To keep settings from being lost during reboot, save them before performing the reboot operation.

3.7.3 Logs

Here you can view the history of the device’ s actions. Up to 150 entries are logged. Click **Refresh** to update current log info or click **Clear** to clear all logs.



Logs

Index	Log Content		
1	1970-01-01 00:00:11	system	DHCP Server Start

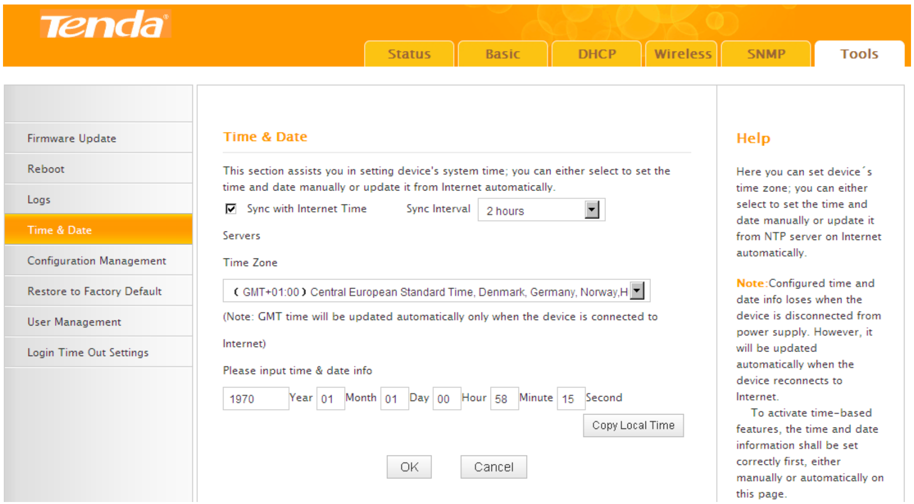
Page 1

Help

Check system logs.

3.7.4 Time & Date

This page is used to set the router’ s system time. You can choose to set the time manually or get the GMT time from the Internet and the system will automatically connect to NTP server to synchronize the time.



Time & Date

This section assists you in setting device's system time; you can either select to set the time and date manually or update it from Internet automatically.

☑ Sync with Internet Time Sync Interval 2 hours

Servers

Time Zone

（GMT+01:00）Central European Standard Time, Denmark, Germany, Norway,H

(Note: GMT time will be updated automatically only when the device is connected to Internet)

Please input time & date info

1970 Year 01 Month 01 Day 00 Hour 58 Minute 15 Second

Help

Here you can set device´s time zone; you can either select to set the time and date manually or update it from NTP server on Internet automatically.

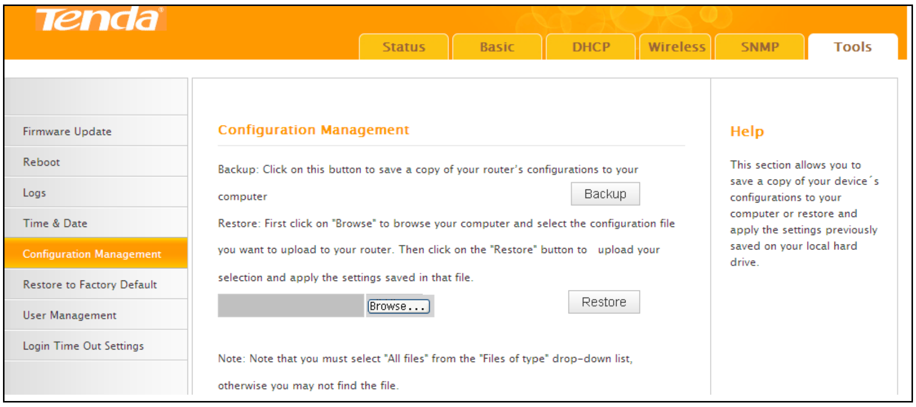
Note:Configured time and date info loses when the device is disconnected from power supply. However, it will be updated automatically when the device reconnects to Internet.

To activate time-based features, the time and date information shall be set correctly first, either manually or automatically on this page.

3.7.5 Configuration Management

This section allows you to save a copy of the device configurations on your local hard drive or to restore the previous configurations back to the device.

1. **Backup:** Once you have configured the device the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your device in case that the device is restored to factory default settings. To do so, click the “Backup” button and specify a directory to save settings on your local hardware.
2. **Restore:** Click the "Browse" button to locate and select a configuration file that is saved previously on your local hard drive and then click **Restore** to restore it. Configurations will be restored after device reboot.



Configuration Management

Backup: Click on this button to save a copy of your router's configurations to your computer

Restore: First click on "Browse" to browse your computer and select the configuration file you want to upload to your router. Then click on the "Restore" button to upload your selection and apply the settings saved in that file.

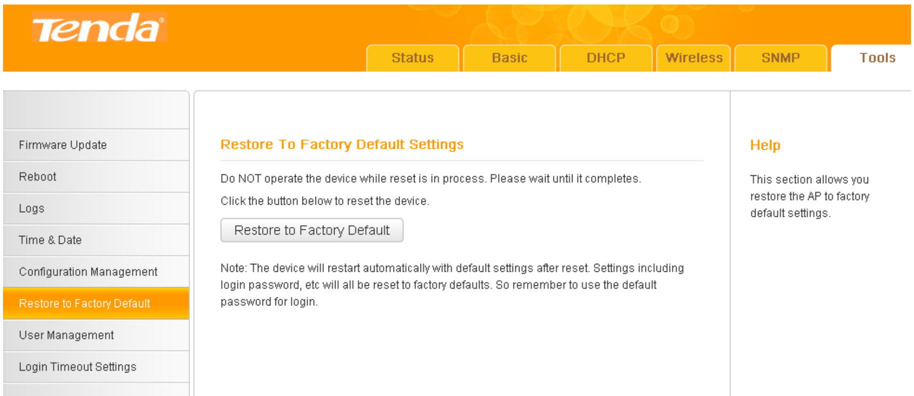
Note: Note that you must select "All files" from the "Files of type" drop-down list, otherwise you may not find the file.

Help

This section allows you to save a copy of your device´s configurations to your computer or restore and apply the settings previously saved on your local hard drive.

3.7.6 Restore to Factory Default Settings

Click the **Restore to Factory Default** button to reset Device to factory default settings.



Restore To Factory Default Settings

Do NOT operate the device while reset is in process. Please wait until it completes.

Click the button below to reset the device.

Note: The device will restart automatically with default settings after reset. Settings including login password, etc will all be reset to factory defaults. So remember to use the default password for login.

Help

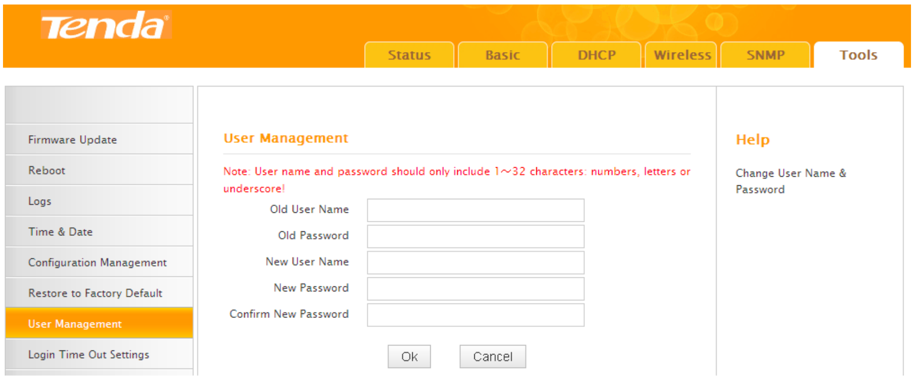
This section allows you restore the AP to factory default settings.

Factory Default Settings:

- **User Name:** admin
- **Password:** admin.
- **IP Address:** 192.168.0. 254
- **Subnet mask:** 255.255.255.0.

3.7.7 User Management

Here you can change the user name and password for web login. The default password is **admin**. We suggest that you change this password to a more secure password.



User Management

Note: User name and password should only include 1～32 characters: numbers, letters or underscore!

Old User Name

Old Password

New User Name

New Password

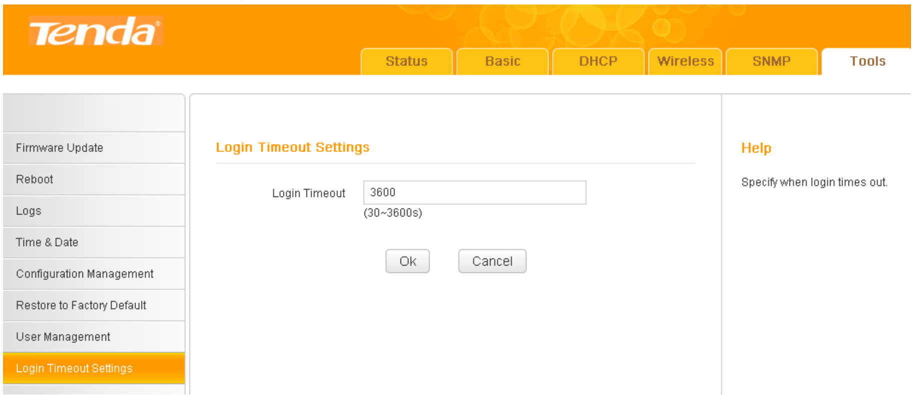
Confirm New Password

Help

Change User Name & Password

3.7.8 Login Timeout Setup

Here you can set up the Login Timeout. Device returns to login window automatically depending on the specified login timeout and user name/password will be required.



Login Timeout Settings

Login Timeout 3600

(30~3600s)

Help

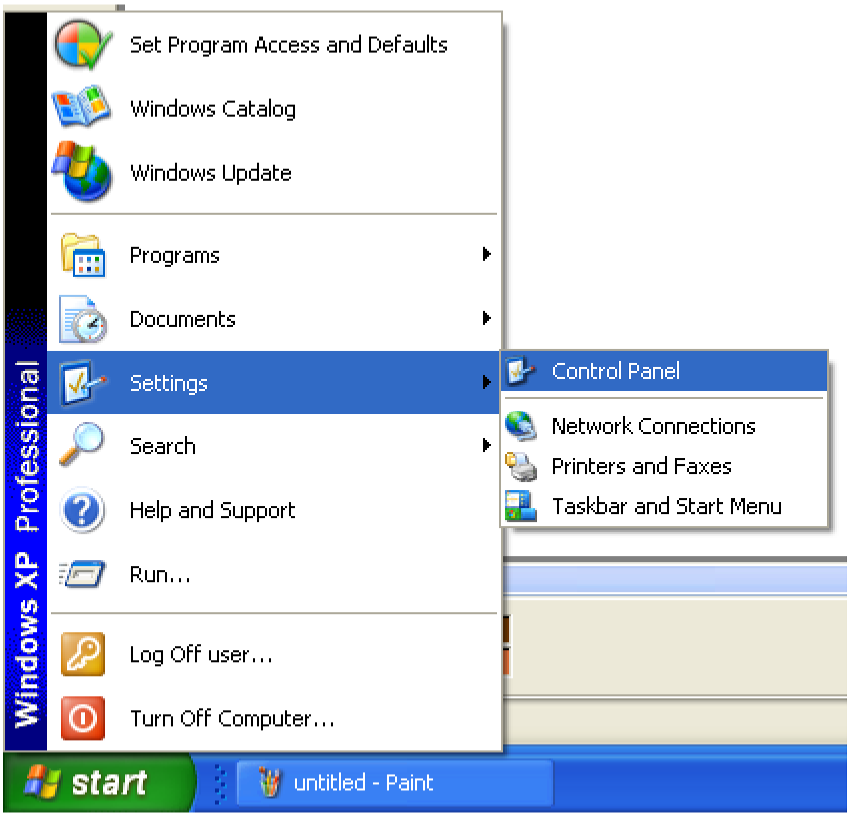
Specify when login times out.

Appendix 1 TCP/IP Setup

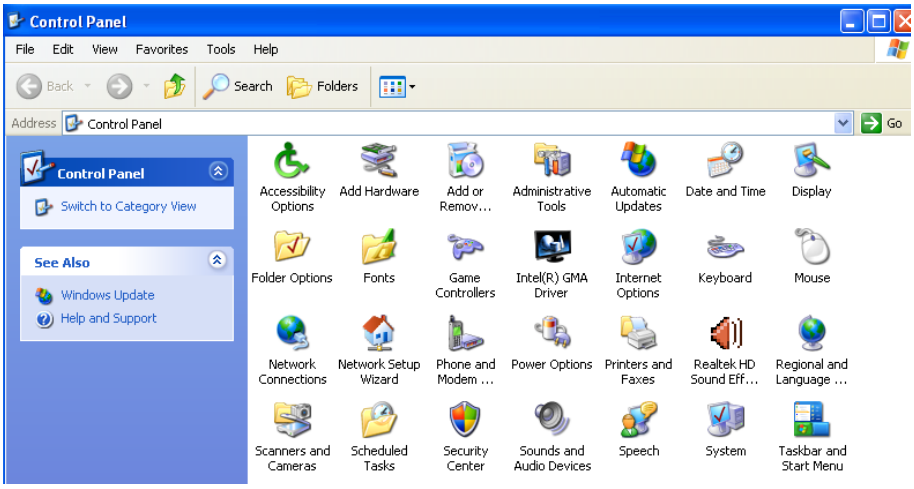
This section presents you how to config your PC’ s TCP/IP settings in **Windows XP**. Before you start, make sure your PC has an installed NIC. If not, please install one first.

Follow steps below:

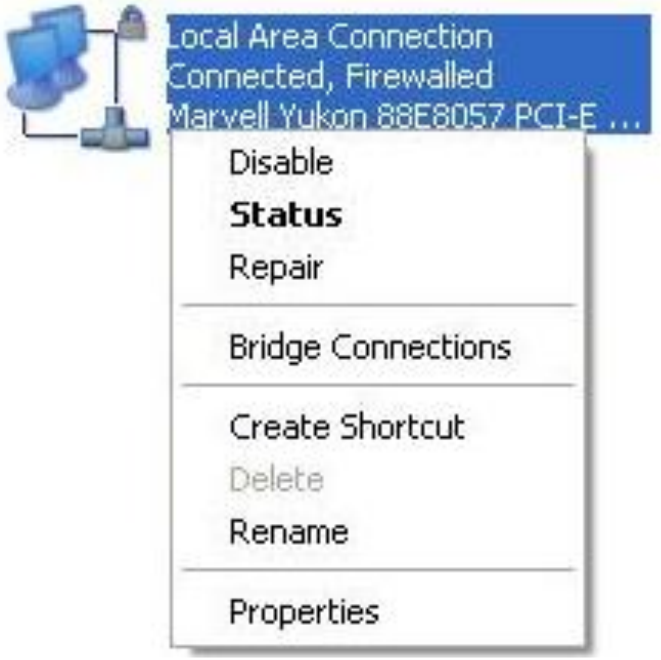
1. Click **Start –> Settings –> Control Panel.**

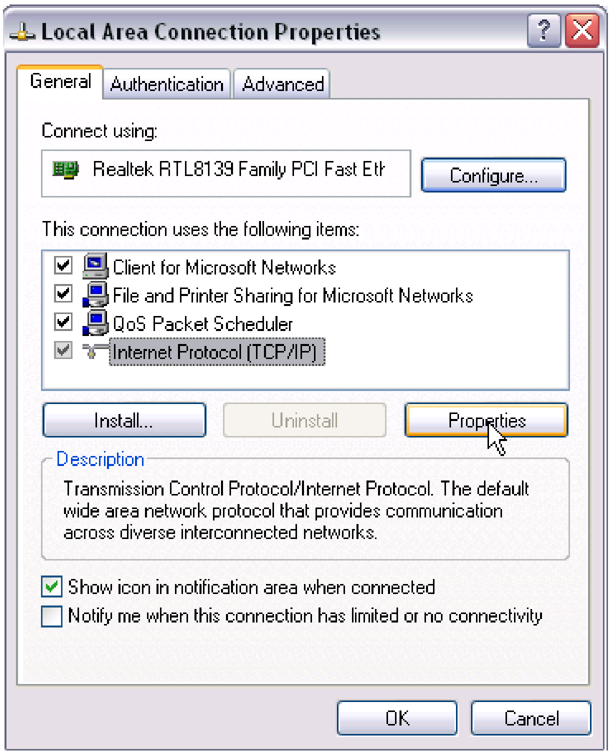


2.Click **Network Connections.**



3.Right click **Local Area Connection**, click **Properties**, select **Internet Protocol (TCP/IP)** on the appearing window and then click **Properties**.





Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

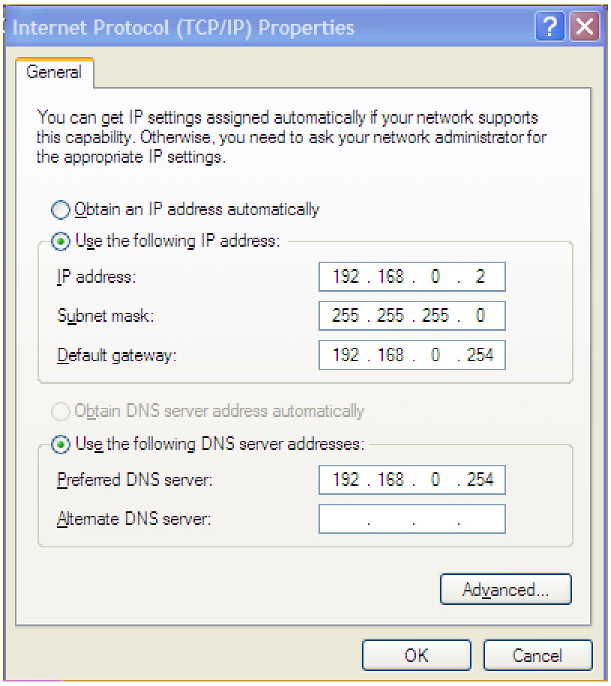
☑ Show icon in notification area when connected

☐ Notify me when this connection has limited or no connectivity

4. Select **Use the following IP address** and configure as below:

IP address: 192.168.0.x (where x can be any number between 2~253)

Subnet Mask: 255.255.255.0.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 254

Alternate DNS server: . . .

5. Click **OK** twice to exit.

Appendix 2: Notification of Compliance

CE Mark Warning

This is a Class B product In a domestic environment,this product may cause radio interference,in which case the user may be required to take adequate measures.This device complies with EU 1999/5/EC.

NOTE:(1)The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.(2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable

FCC Statement

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.

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

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

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

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

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

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.

NOTE:(1)The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.(2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable