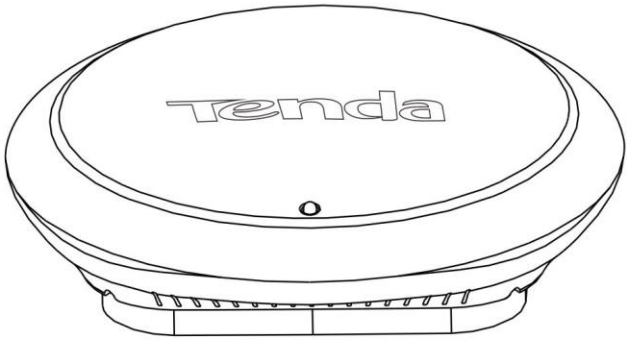
Tenda

User Guide



W301A

Wireless N300 Ceiling Access Point

WH302A

Wireless N300 High Power Access Point

Copyright Statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda! Please read this user guide before you start! This user guide instructs you to install and configure the device.

Convention

Icon	Description
Note	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
Tip	This format is used to highlight a procedure that will save time or resources.

Technical Support:

Website: http://www.tendacn.com

Telephone: (86 755) 2765 7180

Email: support@tenda.com.cn

Contents

Chapter 1 Product Overview

The wireless AP, mini and exquisite, is a best-in-class 802.11n indoor access point designed specifically for wireless projects. With existing structure, the device saves time and costs and provides an adequate level of service for 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 wireless AP offers multiple security modes, which makes your data transmission safe.

1.1 Package Contents

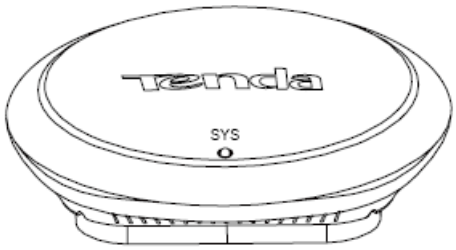
Please verify that the package contains the following items:

- Wireless AP
- Power Adapter
- Screws
- Ethernet Cable
- Bracket
- Install Guide

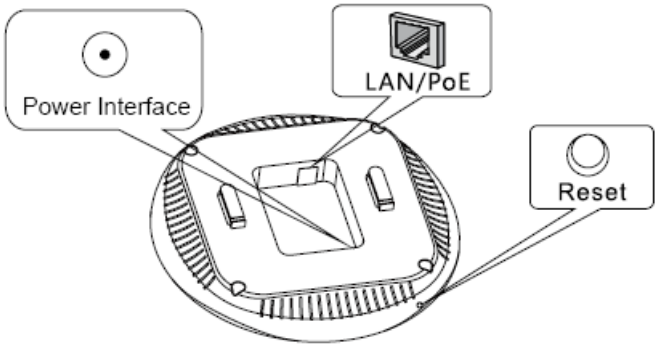
If any of the above items are incorrect, missing, or damaged, please contact your reseller for immediate replacement.

1.2 Hardware Description

LEDs, Interfaces and Buttons



LED	Status	Description
SYS	Blinking	The device is functioning properly.
	Off	The device is receiving no electrical power or the LED is disabled manually via Web interface.
	Solid	The device is functioning improperly.



- **Reset:** Press it for over 7 seconds with a needle to restore factory default settings (see Appendix---3. Default Settings.
- **Power Interface:** Used for connecting the included power adapter.
- **LAN / PoE:** PoE port for connecting to power supply or an IEEE 802.3at compliant PoE switch; 1000M Ethernet port for connecting to an Ethernet device such as a PC or switch, etc.

1.3 Installation Considerations

For better performance, it is advisable to place the device:

- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, etc.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs.
- Away from large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

Chapter 2 Installation

2.1 Physical Installation

Tip----------

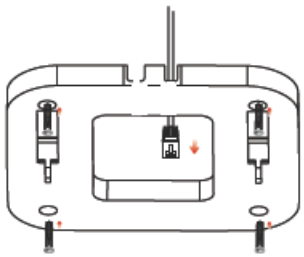
1. The PoE switch should be IEEE 802.3at compliant.

2. With a PoE device, it is advisable to connect to the PoE device for power supply; Without a PoE device, please use the included power adapter for power supply.

Connect to a PoE Device

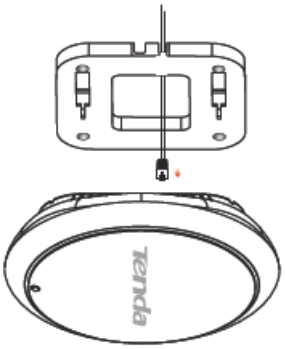
Step 1: Insert the Ethernet cable into the bracket (Recommended: Cat5, Cat5e or higher);

Step 2: Install the bracket onto the ceiling (Drill 4 holes on the ceiling, maneuver the bracket until it fits in the holes on the ceiling and then fix the bracket onto the ceiling with the included screws.);

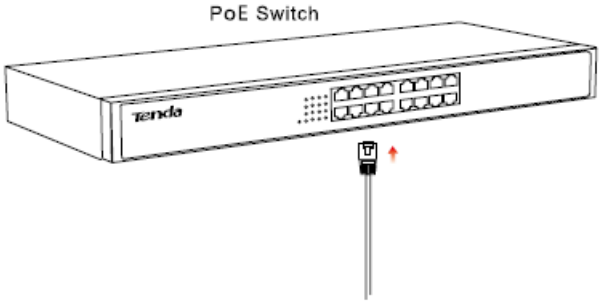


Step 3: Connect the Ethernet cable to the LAN port of the device;

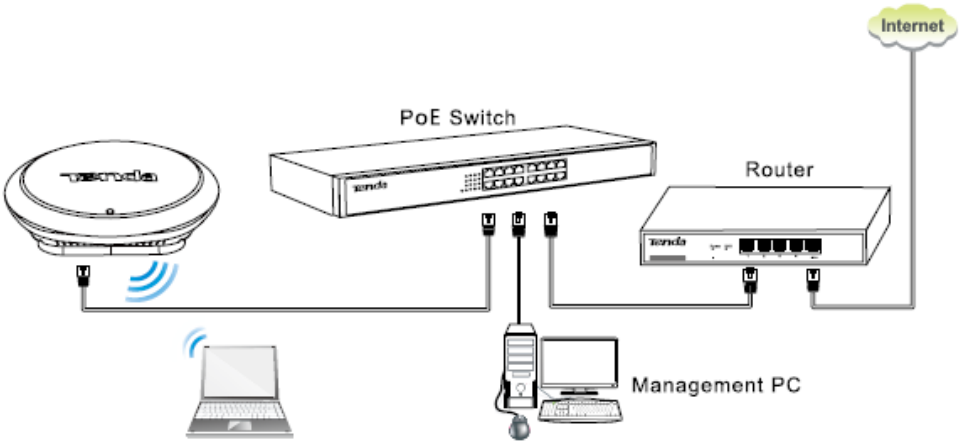
Step 4: Fix the device onto the bracket;



Step 5: Connect the other end of the Ethernet cable to a PoE port on an IEEE 802.3at-compliant switch;



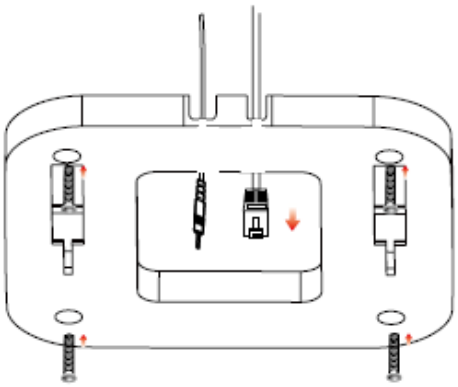
Step 6: Check the network topology as shown below:



Connect to a Power Outlet with the Included Power Adapter

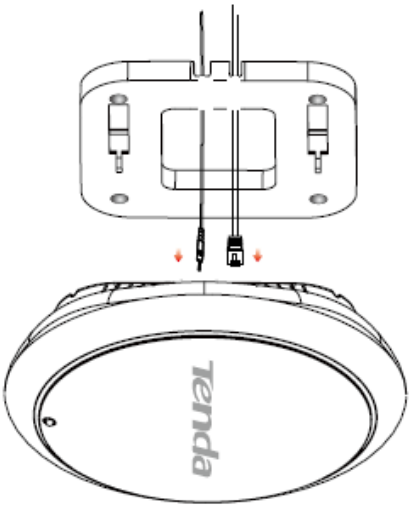
Step 1: Insert the Ethernet cable and power cord into the bracket;

Step 2: Install the bracket onto the ceiling (Drill 4 holes on the ceiling, maneuver the bracket until it fits in the holes on the ceiling and then fix the bracket onto the ceiling with the included screws.);

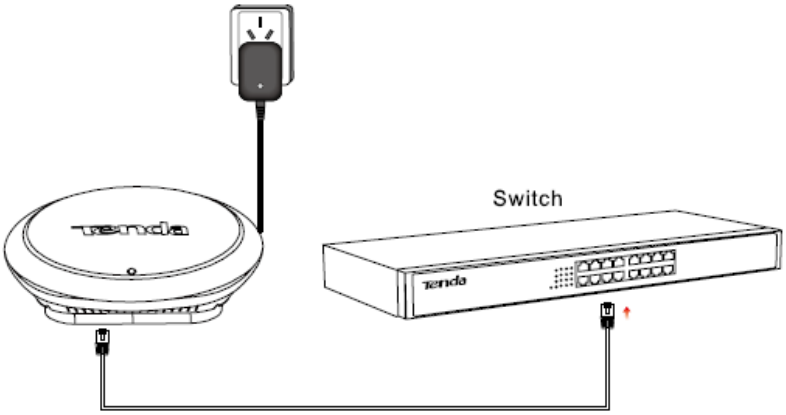


Step 3: Connect the Ethernet cable and power cord to the device;

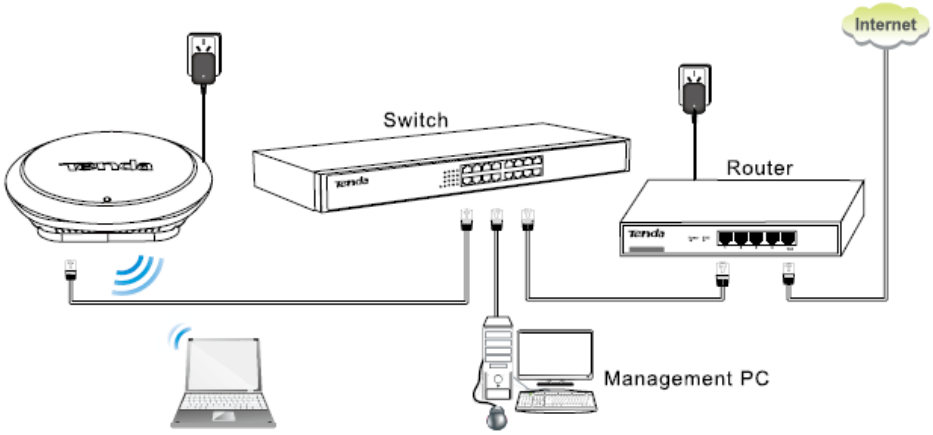
Step 4: Fix the device onto the bracket;



Step 5: Connect the other end of the Ethernet cable to a switch and plug the included power adapter into a power outlet;



Step 6: Check the network topology as shown below:



2.2 Configure Your PC

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 (2~253) 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. If you are not clear about this configuration, please refer to Appendix ---1. Configure PC TCP/IP Settings.

2.3 Connect to Your Device Wirelessly

Having finished above settings, you can search for the device's default wireless network (SSID) from your wireless devices (notebook, iPad, iPhone, etc) and enter a security key to connect to it wirelessly.

Tip ----------

1. The device's SSID is Tenda_XXXXXX by default and XXXXXX is the last six characters of the MAC address which you can find on this device's label.
2. To join your wireless network, the PC you use must have an installed wireless network adapter. If not, install one.

Windows 7

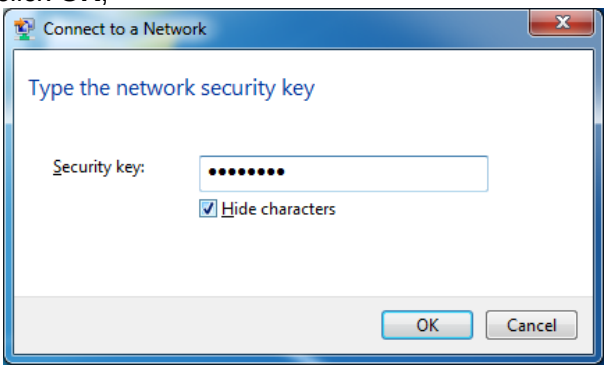
1. Click the icon  at the bottom right corner on your desktop;

Tip ----------

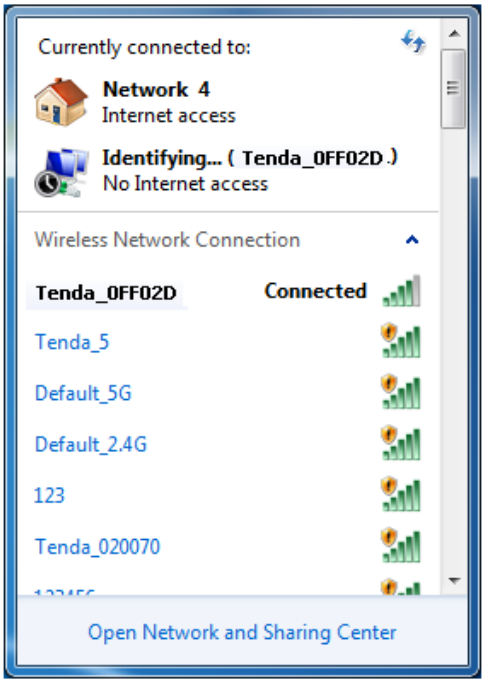
If you cannot find the icon  , try disabling the wired network adapter or unplug the Ethernet cable from the wired network adapter of your PC and refresh your desktop. If the problem remains unsolved, click **Start > Control Panel > Network and Internet > Network and Sharing Center**, right click **Wireless Network Connection** and click **Connect/Disconnect**. Steps for this are similar to the following.

2. Select the wireless network you wish to connect and click **Connect**;

3. Enter the security key and click **OK**;



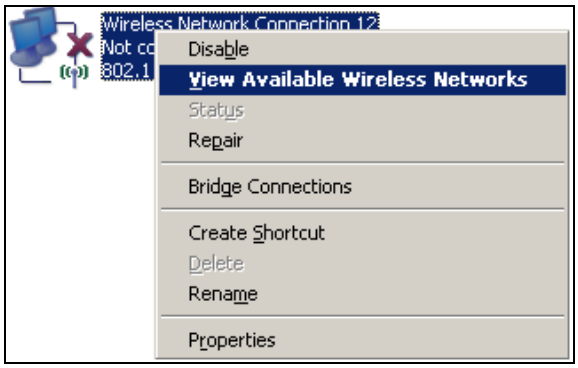
4. When you see **Connected** displayed next to the wireless network you've selected, you have connected to the wireless network successfully.



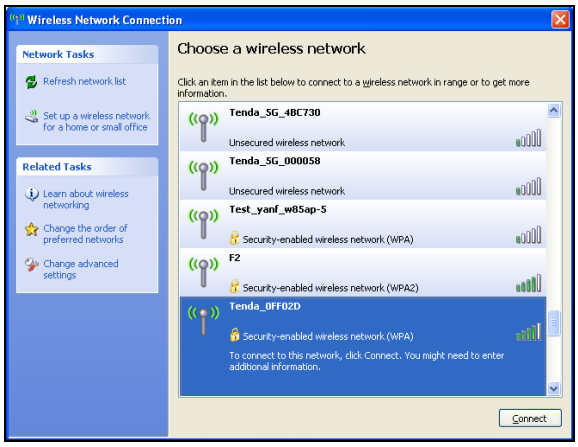
Windows XP

1. Right click **My Network Places** from your PC's desktop and click **Properties**;

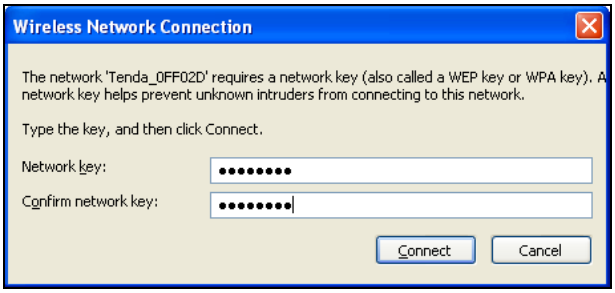
2. Right click **Wireless Network Connection** and select **View Available Wireless Networks**;



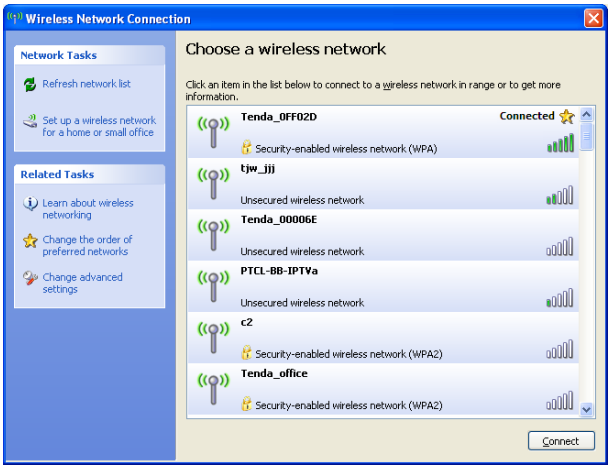
3. Double click the wireless network you wish to connect;



4. Enter the security key and click **Connect**;



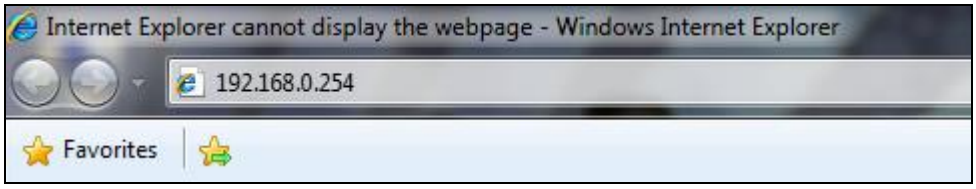
5. When you see **Connected** displayed next to the wireless network you've selected, you have connected to the wireless network successfully.



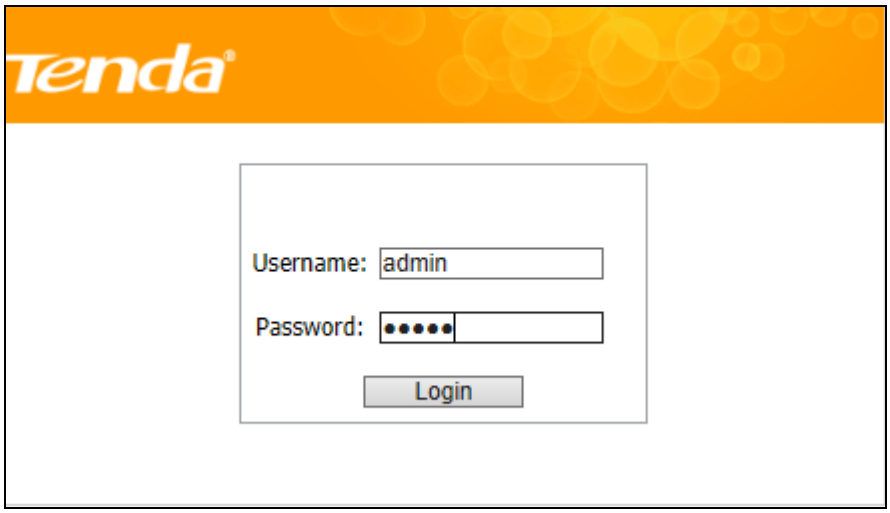
Chapter 3 Advanced Settings

3.1 Web Login

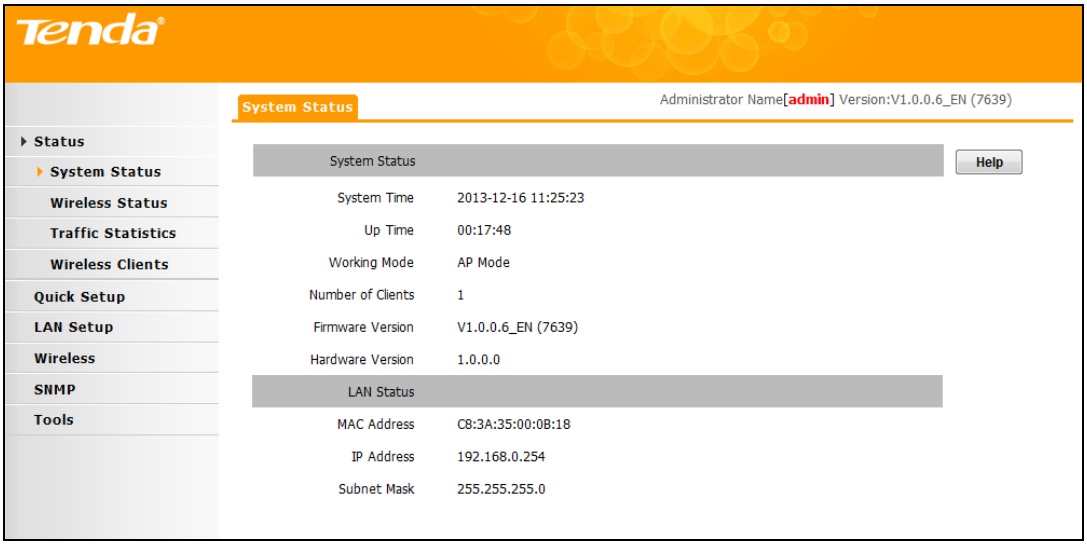
1. Launch a web browser, input **192.168.0.254** in the address bar and press **Enter**.



2. Enter the default Username (admin) and default Password (admin) into the login window.



3. Click **Login** and your Web browser shall automatically display the home page.



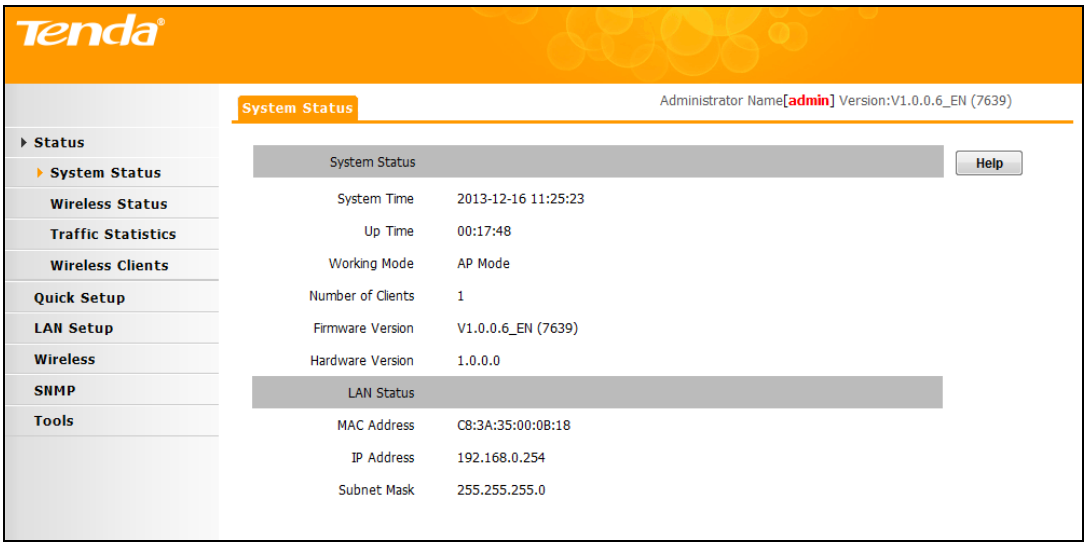
Tip----------

In order to access the Internet and log in to this device's Web interface at the same time, it is advisable to set this device's LAN IP address to be different but on the same network segment as the remote device(such as a router), and then set your PC to **Obtain an IP address automatically**.

3.2 Status

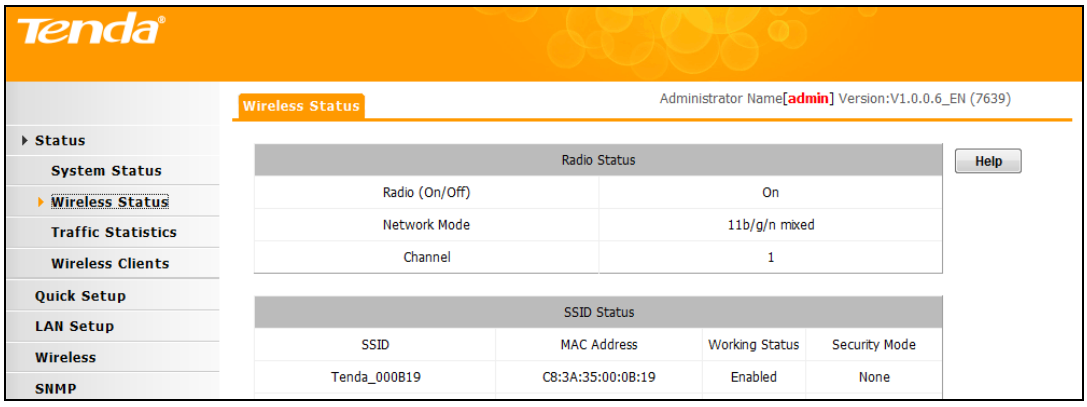
3.2.1 System Status

Click **Status** to enter screen below. This screen displays this device's current system status and LAN status.



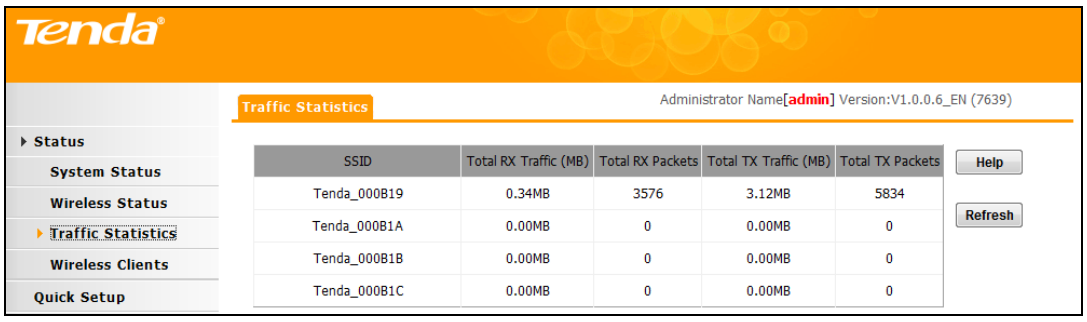
3.2.2 Wireless Status

Click **Status > Wireless Status** to enter screen below. This section displays this device's Radio status and SSID status.



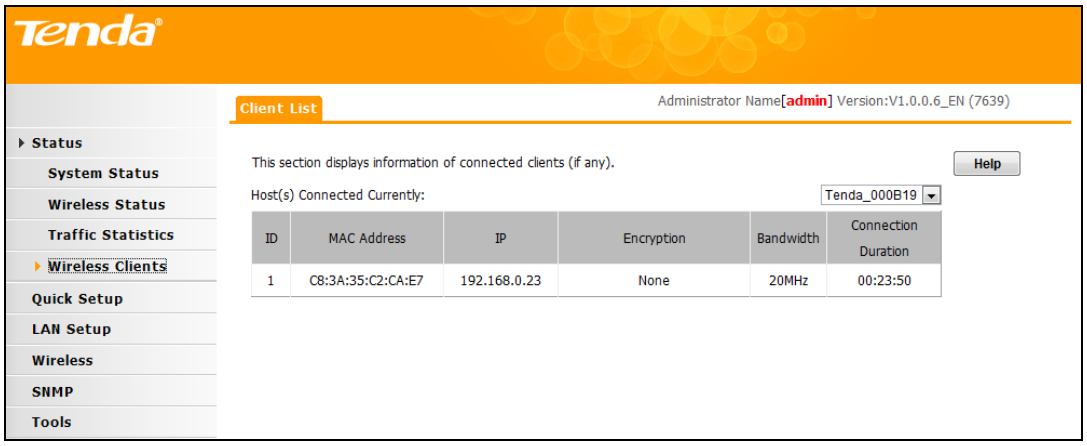
3.2.3 Traffic Statistics

Click **Status > Traffic Statistics** to enter screen below. This section displays current traffic statistics of the device's SSIDs.



3.2.4 Wireless Clients

Click **Status > Wireless Clients** to enter screen below. This section displays information of connected clients (if any).



3.3 Quick Setup

This device supports 3 working modes for expanding wireless network coverage. You can select one as you need.

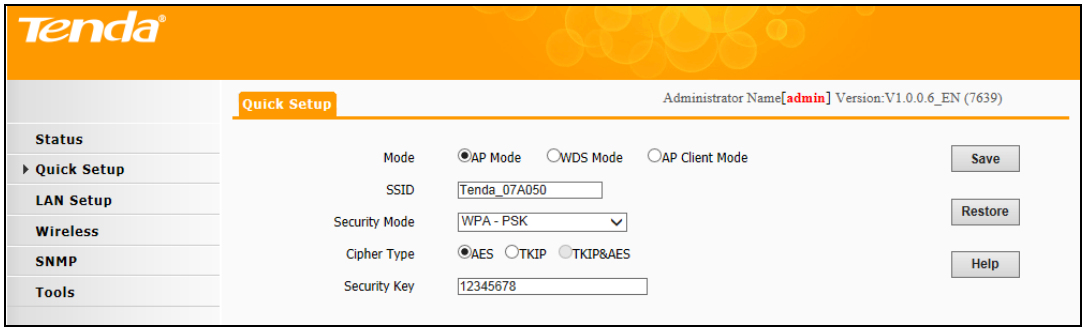
AP Mode: In this mode, the AP connects to the remote device via an Ethernet cable and then clients can connect to the AP wirelessly, thus achieving the conversion between wired networks and wireless networks. And without any configuration, you can achieve network sharing among multiple clients.

WDS Mode: In the WDS mode, the AP and the remote device should support WDS feature. By scanning each other and keeping their SSIDs, channels, security modes and keys the same, they can bridge successfully. Then clients can connect to the AP wirelessly for Internet access.

AP Client Mode: In this mode, what you need to do is to scan the remote device's signal and bridge it successfully without any configuration on the remote device. Then clients can connect to the AP wirelessly for Internet access.

3.3.1 AP Mode

Click **Quick Setup** to enter screen below:



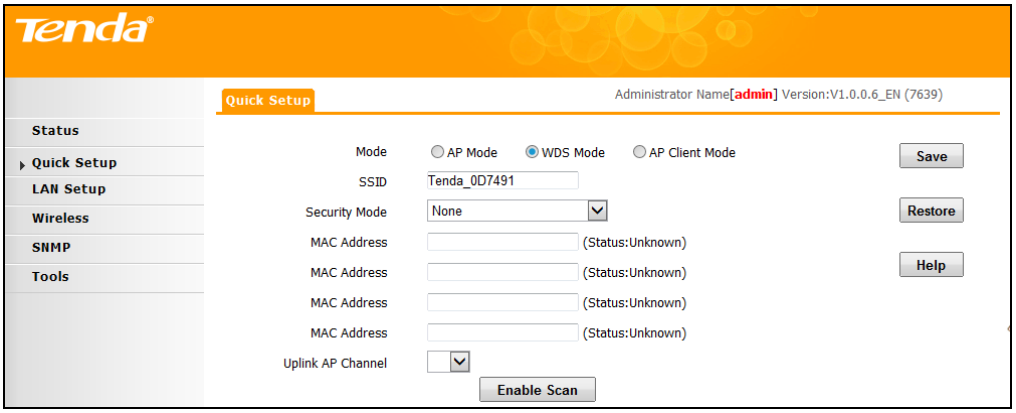
Configuration Procedures:

1. **SSID:** This field is optional. You can change your SSID here if you want to;

2. **Security Mode:** Configure the security mode (WPA-PSK is recommended);
3. **Cipher Type:** Select a cipher type according to your need (AES is recommended);
4. **Security Key:** Configure a security key;
5. Click **Save**.

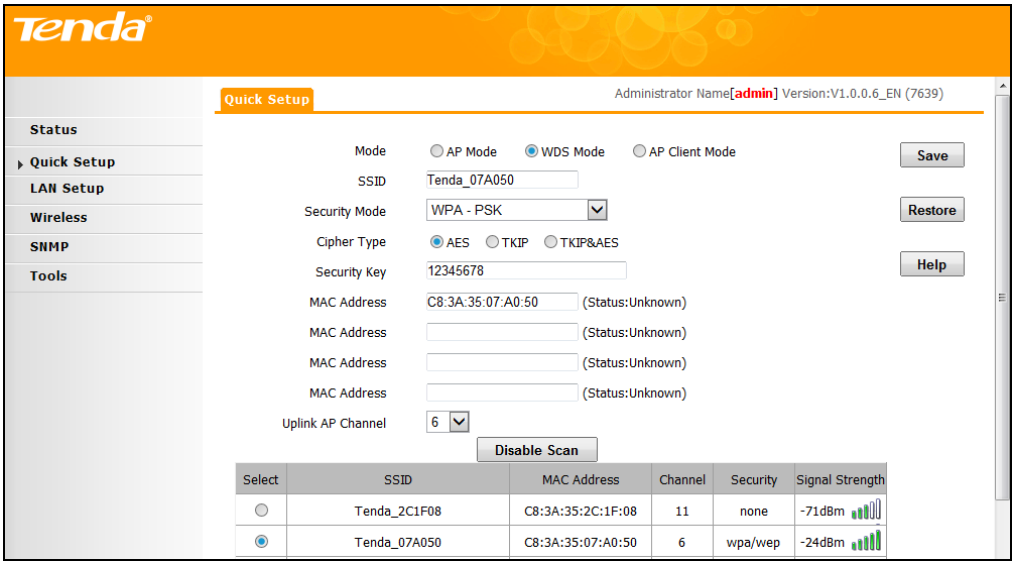
3.3.2 WDS Mode

In this mode, this device can provide access to at most 4 APs. Click **Quick Setup** and select **WDS Mode** to enter screen below:



Configuration Procedures:

1. Click **Enable Scan**;
2. Select the remote SSID you wish to connect;
3. Configure the security settings, including security mode, cipher type and security key. These settings should be kept the same as the remote device's;
4. Click **Save**.



5. Log in to the remote device's Web interface and follow steps 1-4 as shown above to configure the same settings on it.

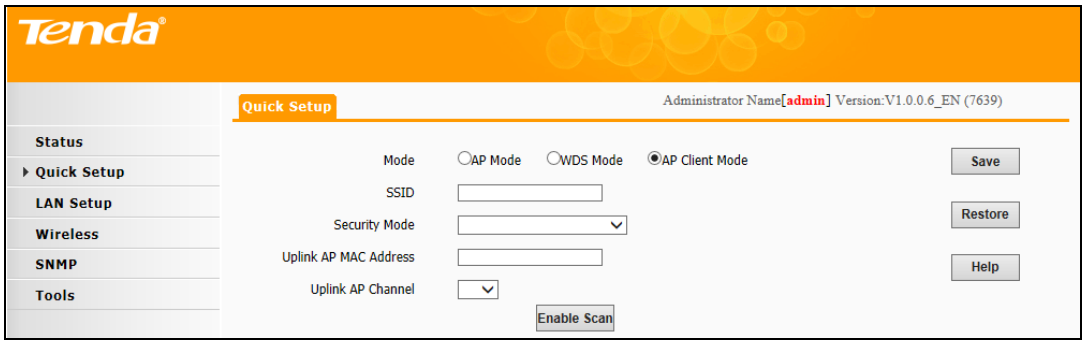
When bridged successfully, **Status** displays **"Connected"** next to the corresponding **MAC Address** field.

Note

In WDS mode, both the AP and the remote device should support WDS feature and you should keep their SSIDs, channels, security modes and keys the same. As for IP addresses, they should not be the same but on the same network segment.

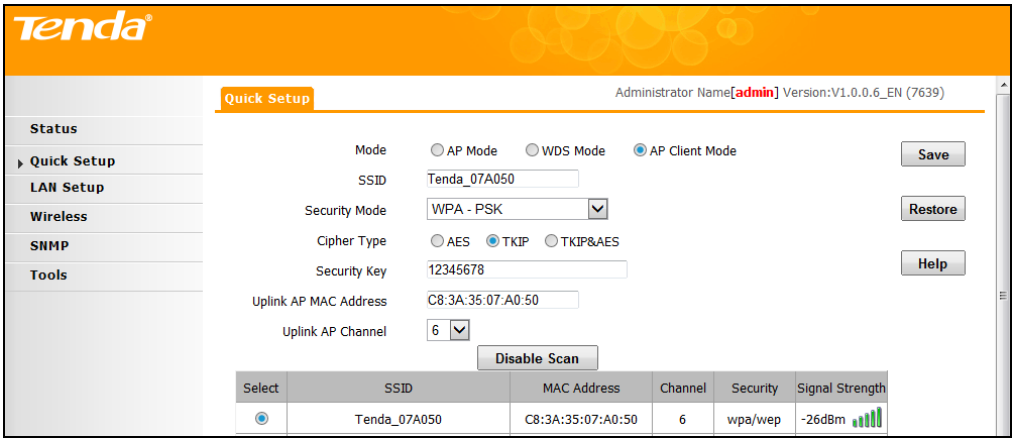
3.3.3 AP Client Mode

In this mode, the AP negotiates with the remote device successfully and also provides access to clients. The device's SSID won't be changed. Click **Quick Setup** and select **AP Client Mode** to enter screen below:



Configuration Procedures:

1. Click **Enable Scan**;
2. Select the remote SSID you wish to connect;
3. Configure the security settings, including security mode, cipher type and security key. These settings should be kept the same as the remote device's;
4. Click **Save**.

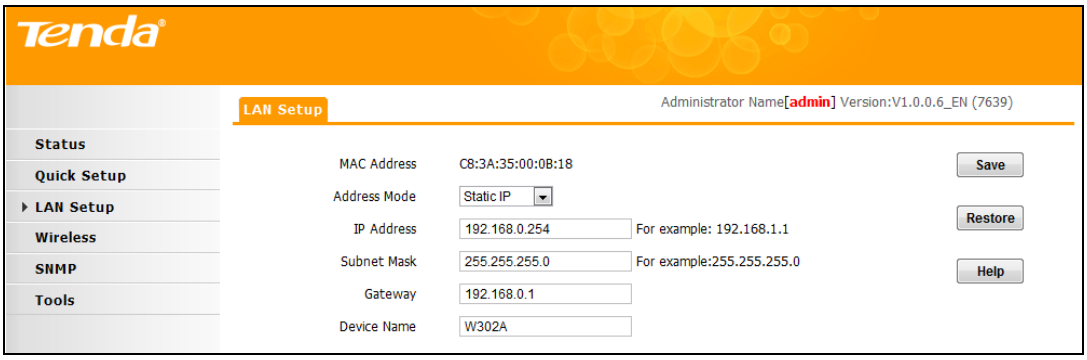


Note

After finishing settings on **Quick Setup** interface, please refer to Appendix---1. Configure PC TCP/IP Settings to set your PC to **Obtain an IP address automatically**, and then you can surf the Internet.

3.4 LAN Setup

Click **LAN Setup** and here you can configure address mode, the LAN IP address and subnet mask.



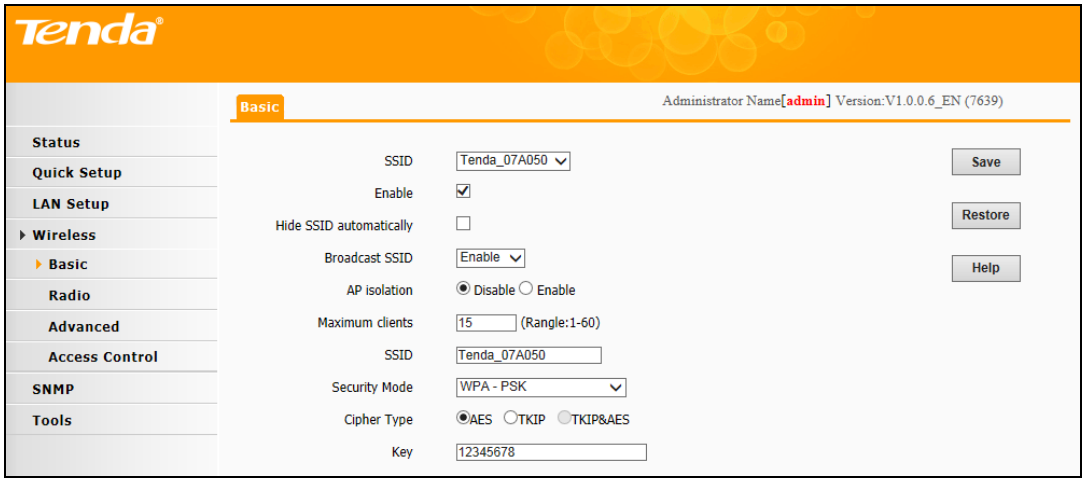
Note

1. The default LAN IP address is 192.168.0.254 and subnet mask is 255.255.255.0.
2. In order to log in to the Web interface, make sure LAN IP address and IP of your PC are on the same network segment.
3. If you change this IP address, you must use the new one to re-log in to the device.
4. If in the WDS mode or AP Client mode, address mode of the LAN IP address should not be **Dynamic IP**.

3.5 Wireless

3.5.1 Basic

Click **Wireless > Basic** to configure the available wireless settings.



1. SSID: Select a SSID from the drop-down list. It supports 4 SSIDs at most.

2. Enable: Once checked, the wireless feature will be enabled.

3. Hide SSID Automatically: When number of clients outnumbers the maximum value, SSID will be hidden automatically.

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

5. AP Isolation: Isolates clients connecting to the same SSID.

6. Maximum Clients: Here you can configure the number of clients (1~60) that can connect the current SSID.

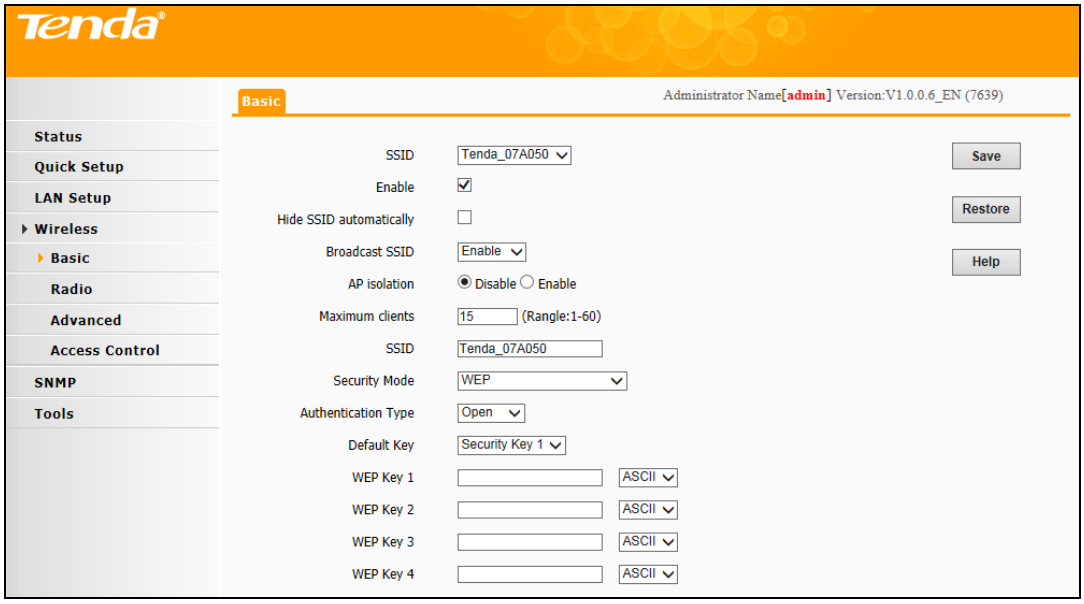
7. SSID: Displays the SSID name and you can change the name here.

8. Security Mode: Configure security settings for the current SSID. This device supports WEP, WPA-PSK,

WPA2-PSK and Mixed WPA/WPA2-PSK (To learn more, read the following).

(1) WEP

WEP (Wired Equivalent Privacy): WEP is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard, its intention is to provide data confidentiality comparable to that of a traditional wired network. Wireless speed can reach up to 54Mbps if WEP is used.



1. Open: Uses "no authentication" + WEP Encryption. Wireless clients can associate with the device without going through authentication. Only data in transmission is encrypted with WEP encryption.

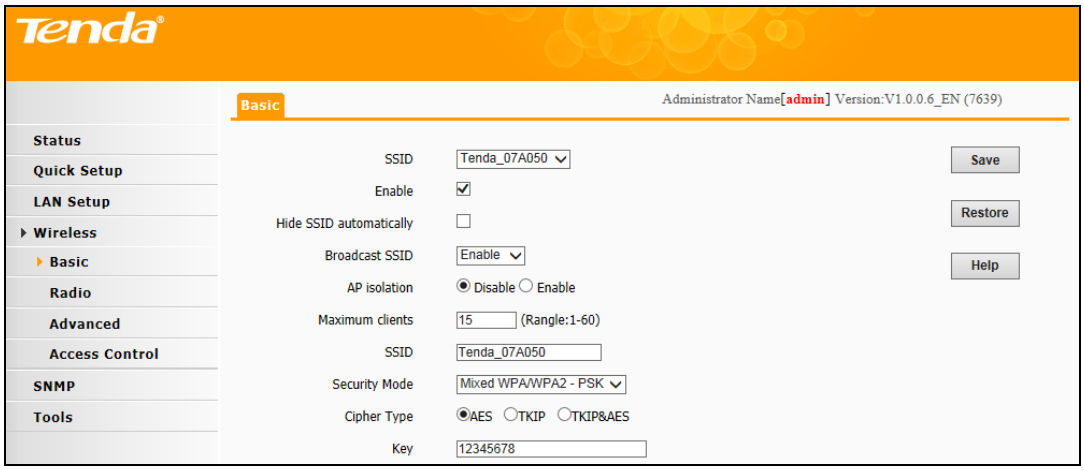
2. Shared: Uses shared key authentication + WEP Encryption. A WEP key that is mutually agreed in advance is required from both sides while wireless clients try to associate with the device. Association is established only if the two sides provide the same WEP key.

3. Default Key: Specify a WEP key from the preset keys for current use. For example, if you select Key 2, wireless clients must join your wireless network using this Key 2.

(2) WPA-PSK, WPA2-PSK

WPA: 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 tampered with. Only authorized network users can access the wireless network. WPA adopts enhanced encryption algorithm over WEP.

WPA2: WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP. It is more secure than WPA and WEP.



1. Security Mode: Supports WPA-PSK, WPA2-PSK and WPA/WPA2-PSK Mixed.

WPA-PSK: Supports AES and TKIP cipher types.

WPA2-PSK: Supports AES, TKIP and TKIP+AES cipher types.

WPA/WPA2-PSK mixed: If selected, both WPA-PSK and WPA2-PSK secured wireless clients can join your wireless network.

2. Cipher Type: Includes AES, TKIP and TKIP&AES.

AES: If selected, wireless speed can reach up to 300Mbps.

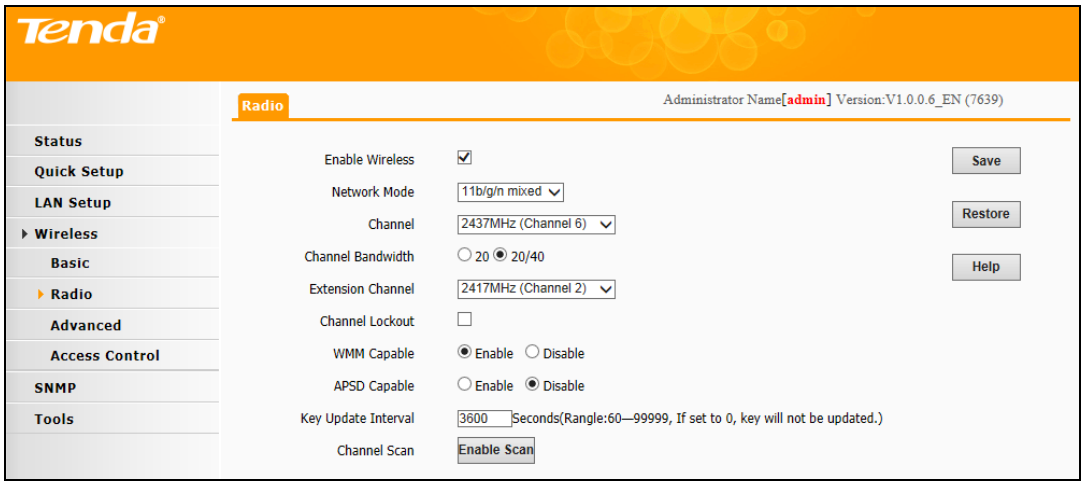
TKIP: If selected, wireless speed can reach up to 54Mbps.

TKIP+AES: If selected, both AES and TKIP enabled wireless clients can join your wireless network.

3. Key: Specify the security key.

3.5.2 Radio

Click **Wireless > Radio** to enter screen below. Here you can configure basic wireless settings including network mode, channel, extension channel, channel bandwidth, etc.



1. Enable Wireless: Check/uncheck to enable/disable the wireless feature.

2. 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 in this mode.

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

11b/g mixed mode: Select it if you have 11b and 11g wireless devices in your wireless network. Up to 54Mbps wireless rate is supported in this mode.

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. Up to 300Mbps wireless rate is supported in this mode.

3. Channel: Select from 1~13 channels or Auto. It is recommended to select a channel that is the least used by neighboring networks.

4. Channel Bandwidth: Select a proper channel bandwidth to enhance wireless performance. This option is available only in 802.11b/g/n. Wireless speed in the channel bandwidth of 20/40 is 2 times in 20.

5. Extension Channel: This is used to ensure N speeds for 802.11n devices on the network. This option is available in 11b/g/n mixed mode with channel bandwidth of 20/40.

6. WMM-Capable: WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data such as video or audio (recommended).

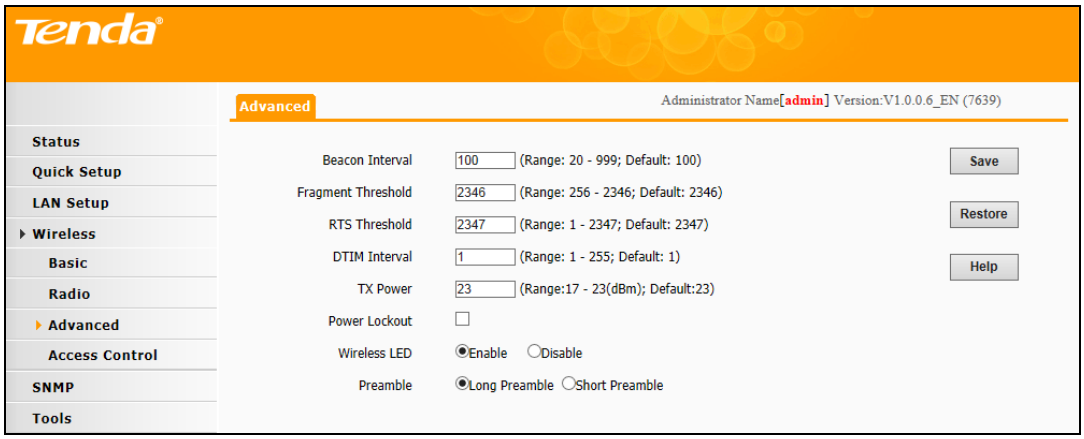
7. ASPD Capable: Select to enable/disable the auto power saving mode. By default, this option is disabled.

8. Key Update Interval: You can configure security key's update cycle (60—99999 seconds) here. If it's set to 0, key will not be updated.

9. Channel Scan: You can click **Enable Scan** to scan wireless networks.

3.5.3 Advanced

Click **Wireless > Advanced** and here you can configure advanced wireless settings. If you are new to networking and have never configured these settings before, we recommend you to leave the default settings unchanged.



1. Beacon Interval: This is a time interval between any two consecutive Beacon packets sent by an Access Point to synchronize a wireless network. Specify a valid value between 20 and 999. The default setting is 100.

2. Fragment Threshold: Specify a valid Fragment Threshold value between 255 and 2346. The default is 2346. Any wireless packet exceeding the preset value will be divided into several fragments before transmission.

3. RTS Threshold: Specify a valid value between 1 and 2347. The default is 2347. If a packet exceeds the preset value, RTS/CTS scheme will be used to reduce collisions. Set it to a smaller value provided that there are distant clients and interference.

4. DTIM Interval: A DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of

the next window for listening to broadcast and multicast messages. When such packets arrive in the router's buffer, the router will send DTIM (delivery traffic indication message) and DTIM interval to alert clients of the receiving packets. Specify a valid value between 1-255. The default is 1.

5. TX Power: Control TX power. Specify a valid value between 17 and 23. The default is 23.

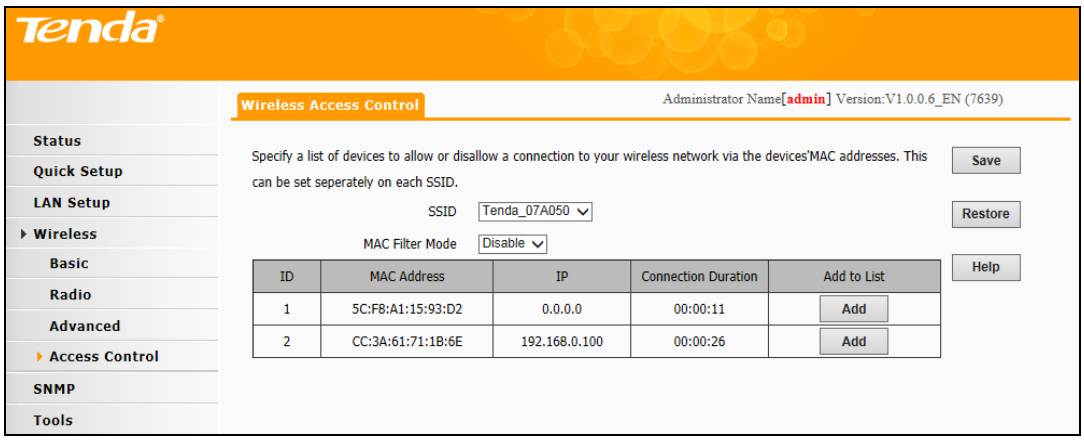
6. Power Lockout: Once enabled, you cannot change power manually.

7. Wireless LED: You can enable or disable wireless LED manually.

8. Preamble: The 8 bytes of the preamble and the Start of Frame create a pattern of 64 bits. 7 bytes of the preamble are for synchronization and 1 byte is for SFD, which basically says here comes a new frame, being a "get ready" notification. There are two types of preambles: long preamble and short preamble. By default, the device transmits data using the long preamble.

3.5.4 Access Control

Click **Wireless > Access Control** to enter screen below. Specify a list of devices to allow or disallow a connection to your wireless network via the device's MAC addresses. To deactivate this feature, select "Disable"; to activate it, select "Allow" or "Deny".



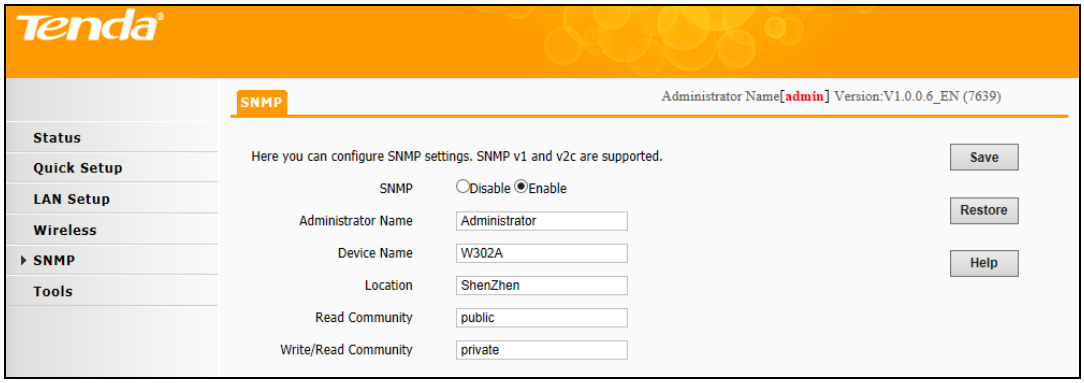
MAC Filter Mode: Select Allow or Deny from the drop-down list.

1. To permit a wireless device to connect to your wireless network, select **Allow**, enter its MAC address, click **Add** and then **Save**. Then only devices listed as “Allowed” will be able to connect to your wireless network.

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

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 v2C. Click **SNMP** to enter screen below:



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

1. Administrator Name: Input the administrator's name.

2. Device Name: Input the name of the AP, e.g., WIRELESS AP.

3. Location: Input the AP's location.

4. Read Community: Indicates the community read access string to permit reading this AP's SNMP information. The default is Public.

5. Write/Read Community: Indicates the community write/read access string to permit reading and re-writing this AP's SNMP information. The default is Private.

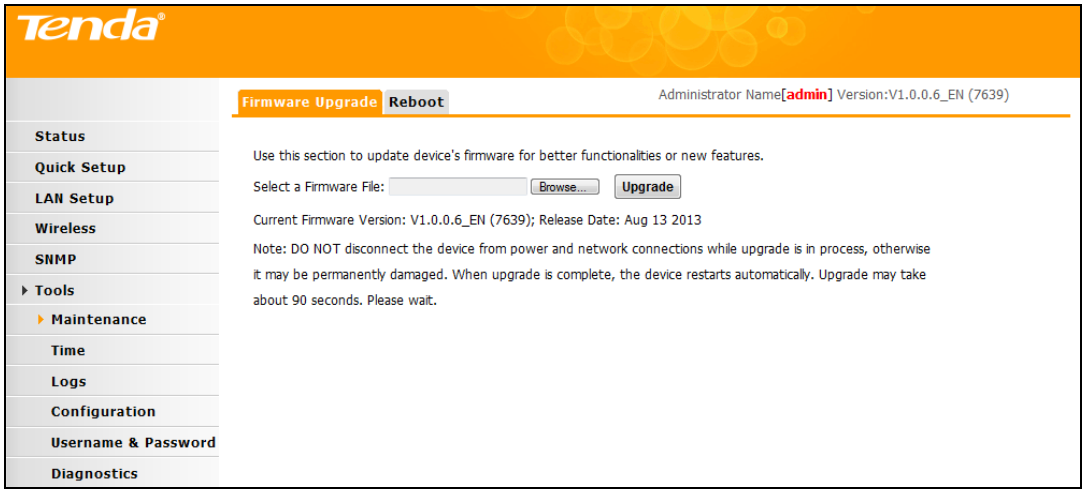
3.7 Tools

3.7.1 Maintenance

Firmware Upgrade

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 (http://www.tendacn.com) to download the latest firmware to update your device.

Click **Tools > Maintenance > Firmware Upgrade** to enter screen below:



To upgrade device software:

1. Launch a web browser and go to **http://www.tendacn.com** to download the latest firmware.
2. Unzip the compressed upgrade file (.ZIP file).
3. Click **Browse** to locate and select the upgrade file on your hard disk.
4. Click **Upgrade** to upgrade device firmware.

5. When the firmware upgrade completes, the device will automatically restart.
6. Restore the AP to factory default settings after reboot.

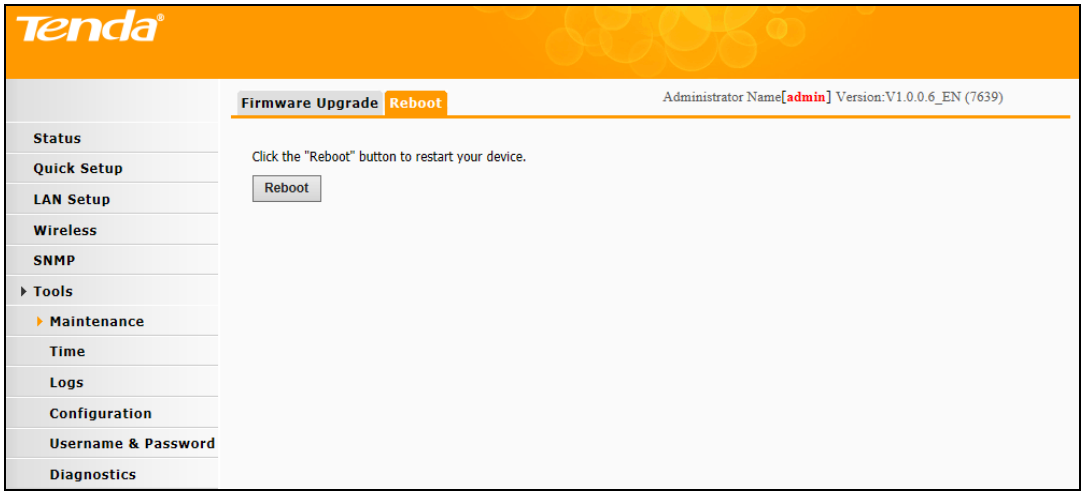
Note

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, the device will automatically restart. The upgrade process typically takes about several minutes.

Reboot

The Reboot option restarts the device. All connections will be lost while rebooting.

Click **Tools > Maintenance > Reboot** to enter screen below:



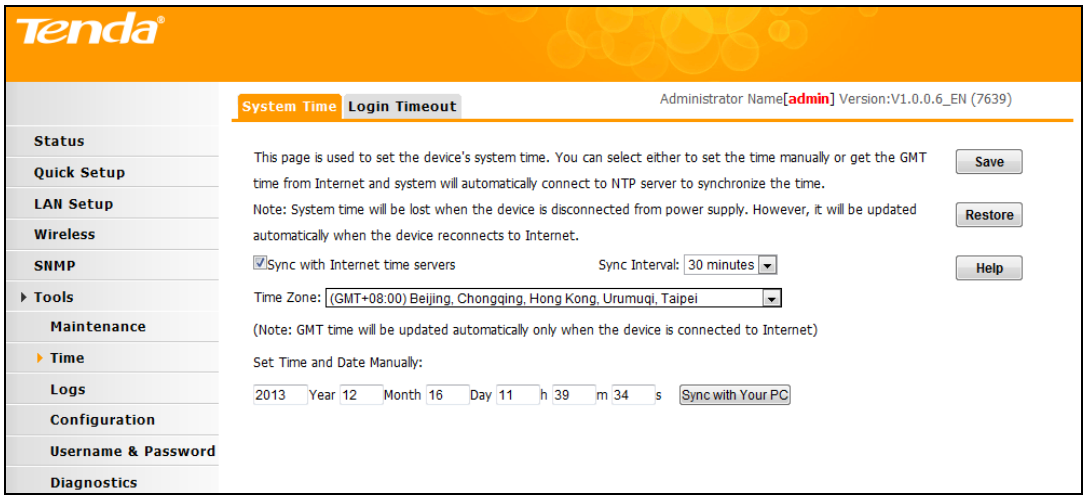
3.7.2 Time

System Time

Click **Tools > Time > System Time** to enter the system time screen. This page is used to set the device's system time. System time can be configured using the following 2 methods:

Sync with Internet time servers: If enabled, system automatically connects to NTP server on the Internet to synchronize the time.

Set Time and Date Manually/Sync with Your PC: Specify the time and date manually or click **Sync with Your PC** to automatically copy your current PC's time to the device.



To Sync with Internet time servers:

1. Check **Sync with Internet time servers** to enable it.
2. Select a Sync Interval from the drop-down list.
3. Select your time zone.

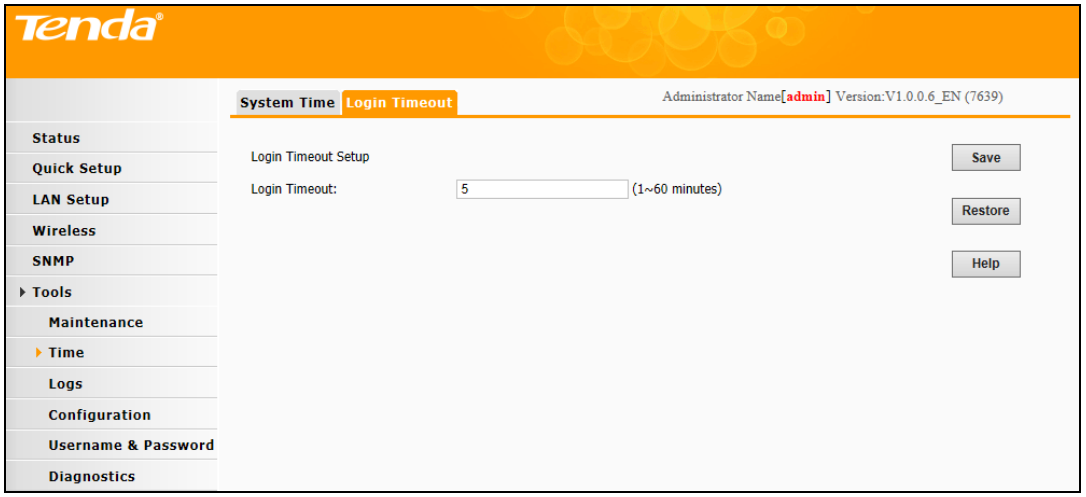
To set time and date manually:

1. Uncheck **Sync with Internet time servers** to disable it.
2. Specify the time and date manually or click **Sync with Your PC** to automatically copy your PC's time to the device.

And then go to **Status** to make sure the system time is correctly updated.

Login Timeout

Click **Tools > Time > Login Timeout** and here you can configure the web login timeout (1-60 minutes). The default is 5 minutes. Device returns to login window automatically depending on the specified login timeout and user name/password will be required.

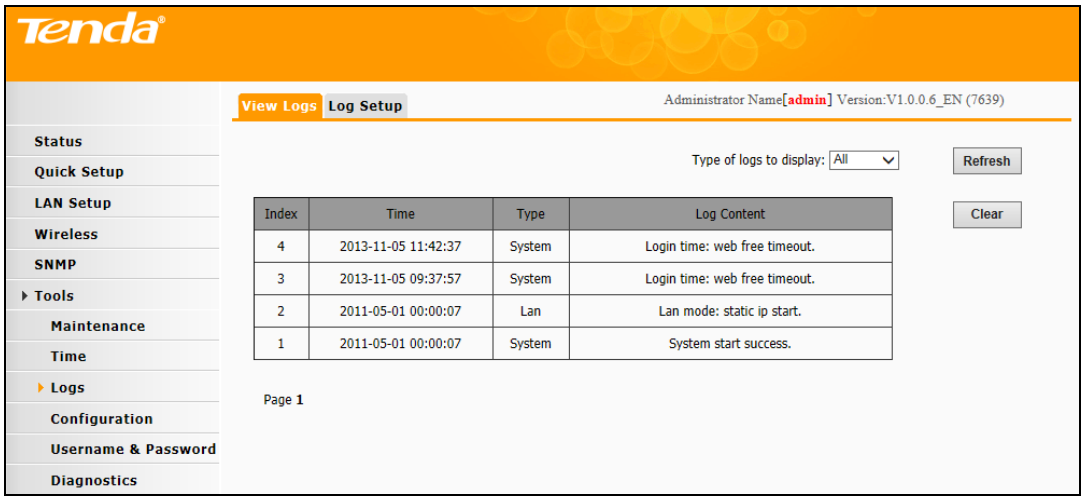


3.7.3 Logs

View Logs

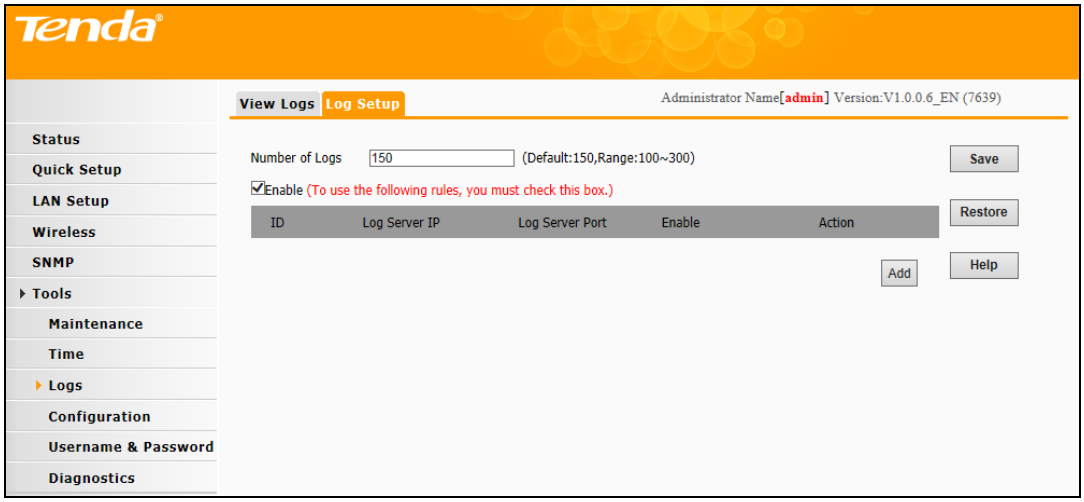
Click **Tools > Logs > View Logs** to enter screen below. Here you can view the history of the device's actions.

Click **Refresh** to update current log info or click **Clear** to clear all logs.



Log Setup

Click **Tools > Logs > Log Setup** to configure system logs. Here you can set up number of logs and rules of log settings. Up to 300 entries can be logged. The default is 150.



To configure the log server:

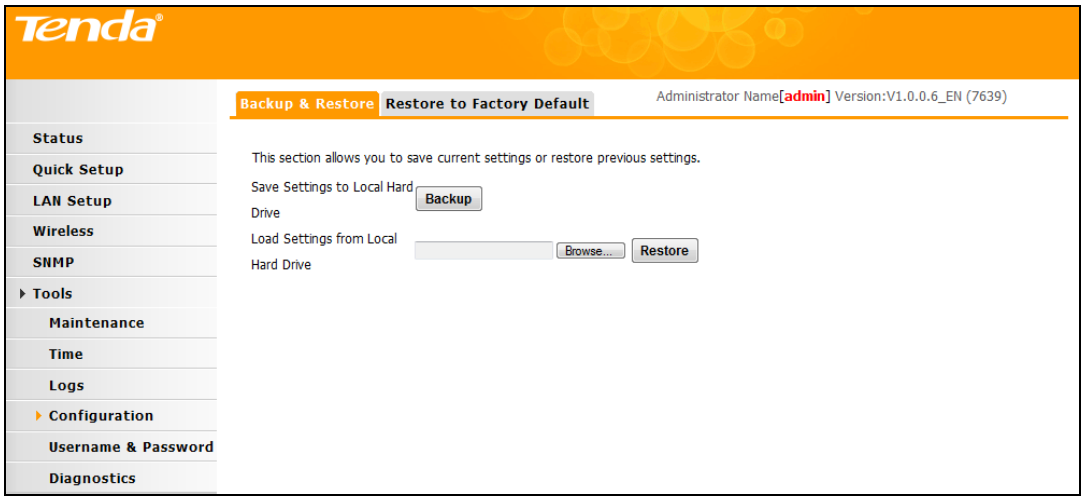
1. Click **Add** to add a log server.
2. Specify the IP address and port of the syslog server on your LAN and enable the log server.
3. Check the "To use the following rules, you must check this checkbox." option.

If configured successfully, the system will begin to log events and simultaneously send them to the specified log server on your LAN. You can view all logs there.

3.7.4 Configuration

Backup & Restore

Click **Tools > Configuration > Backup & Restore** to enter screen below. 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.

Tip----------

The default backup configuration file name is APcfgfile.cfg. It is advisable to keep the filename extension(.cfg) unchanged.

Restore to Factory Default

If the device or clients connected to the device fail to access Internet due to incorrect configurations and you cannot solve the problem, click **Tools > Configuration > Restore to Factory Default** to reset the device and then reconfigure it.

To restore to factory default settings, two methods are available:

Method 1: Using UI

Click the **Restore to Factory Default** button and wait until the progress indicator displays 100% completed.

Method 2: Pressing the hardware reset button

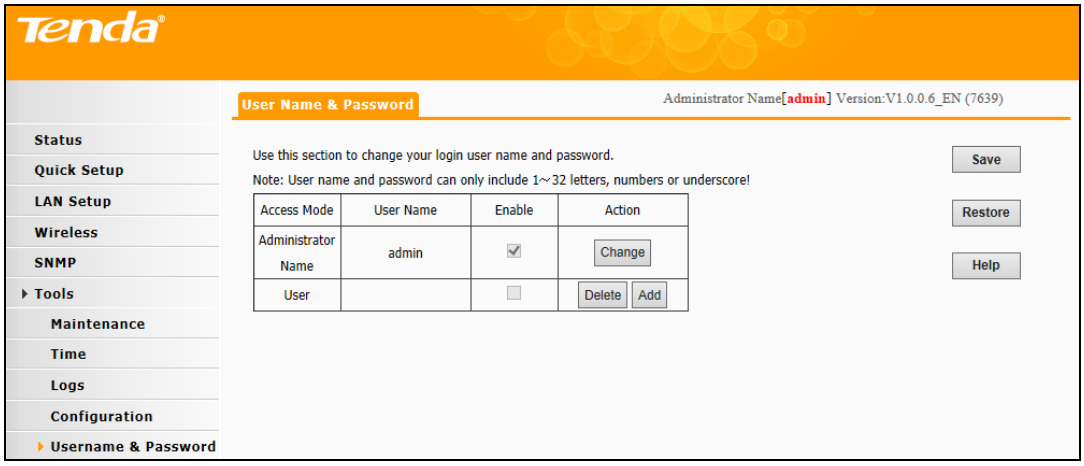
Press the **Reset** button on this device with a needle for about 7 seconds.

Factory Default Settings:

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

3.7.5 Username & Password

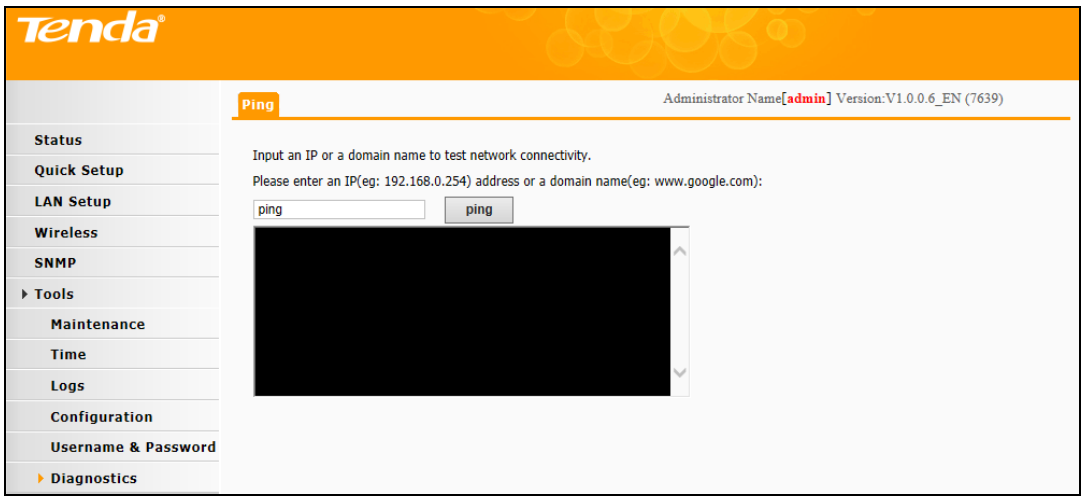
Click **Tools > Username & Password** to enter screen below. Here you can change the user name and password for web login. The default password is **admin**. We suggest that you change this password to a more secure password.



- **Administrator:** If you log in to the device as an administrator, you have all available rights to access the device.
- **User:** If you log in to the device as a user, you can only view configurations instead of configuring or changing any existing configurations.

3.7.6 Diagnostics

This page allows you to test your network connection. If your network is malfunctioning, click **Tools > Diagnostics** to use the ping utility to test your network and find out where the problem is.

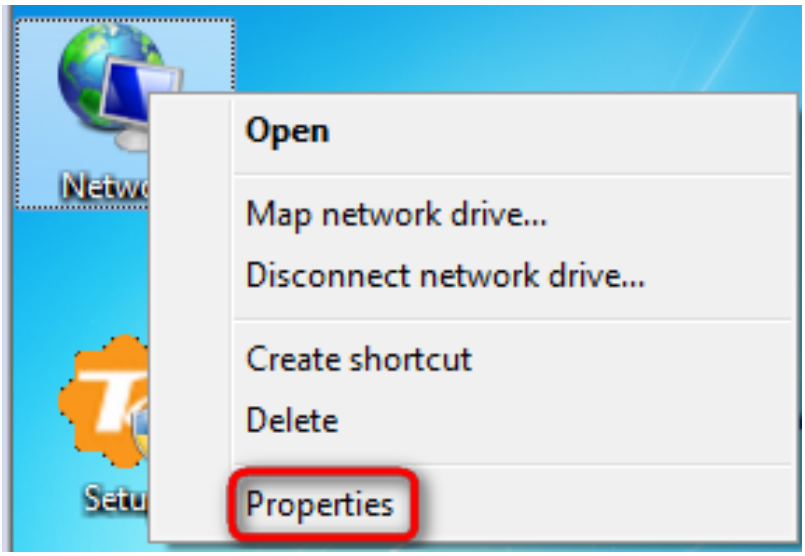


Appendix

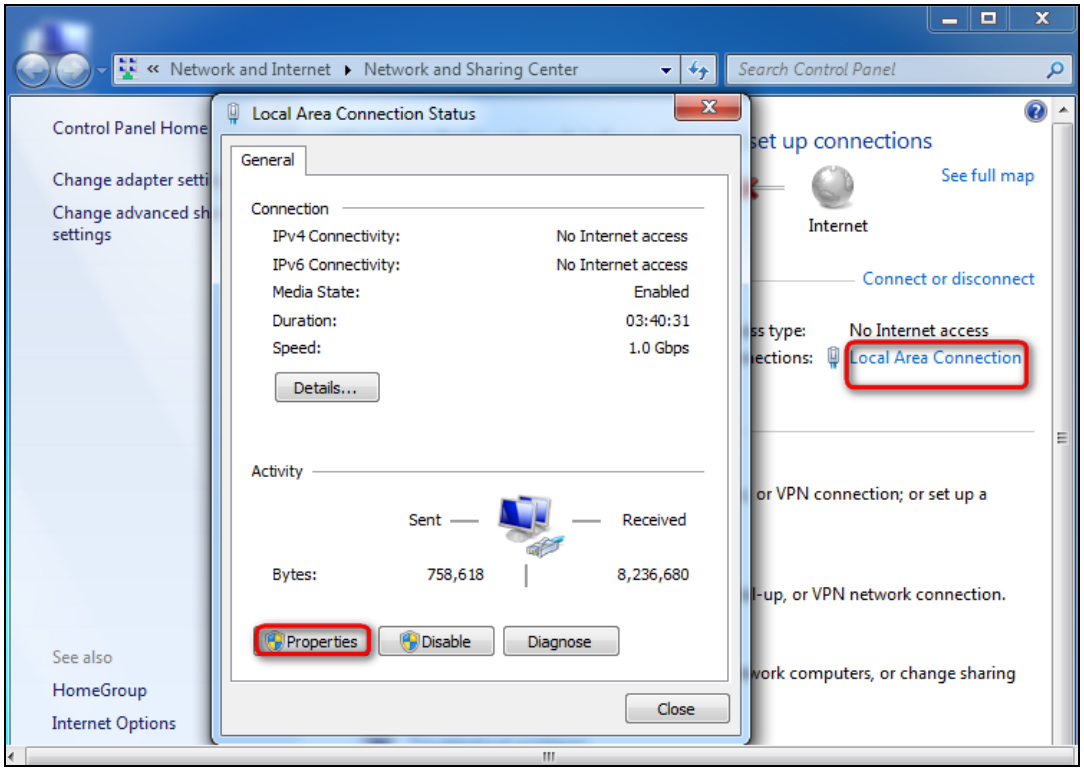
1.Configure PC TCP/IP Settings

Win7 OS Configuration

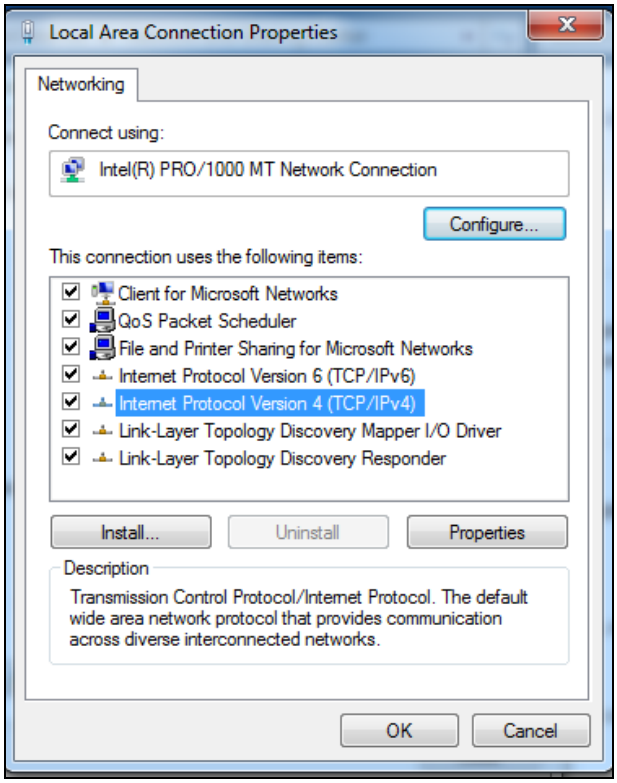
1. Right click **Network** on your desktop and select **Properties**;



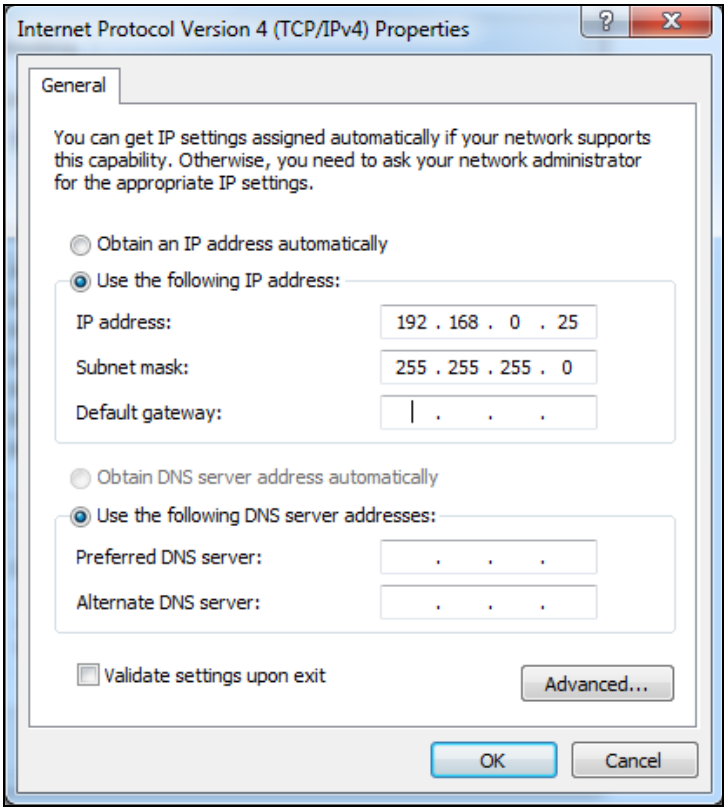
2. Click **Local Area Connection > Properties**;



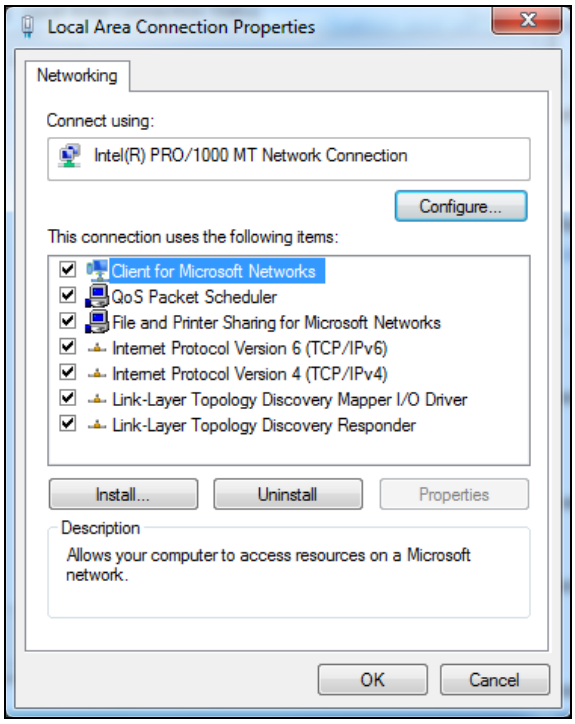
3. Double click **Internet Protocol Version 4 (TCP/IPv4)**;



4. Select **Use the following IP address**, enter 192.168.0.X (2~253) in the **IP address** field and 255.255.255.0 in the **Subnet mask** field and then click **OK** to save your configurations.

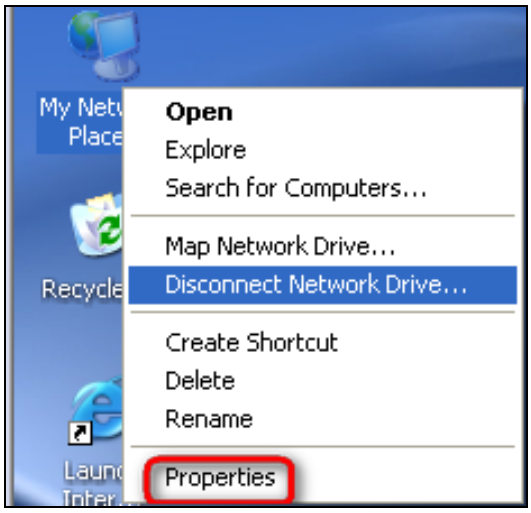


5. Click **OK**.

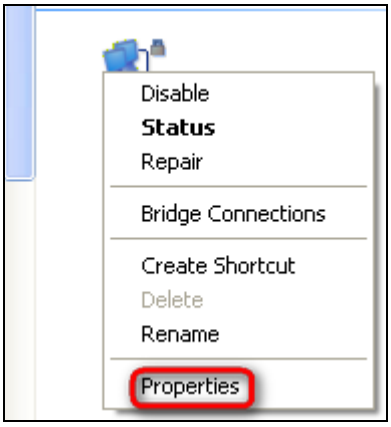


Windows XP OS Configuration

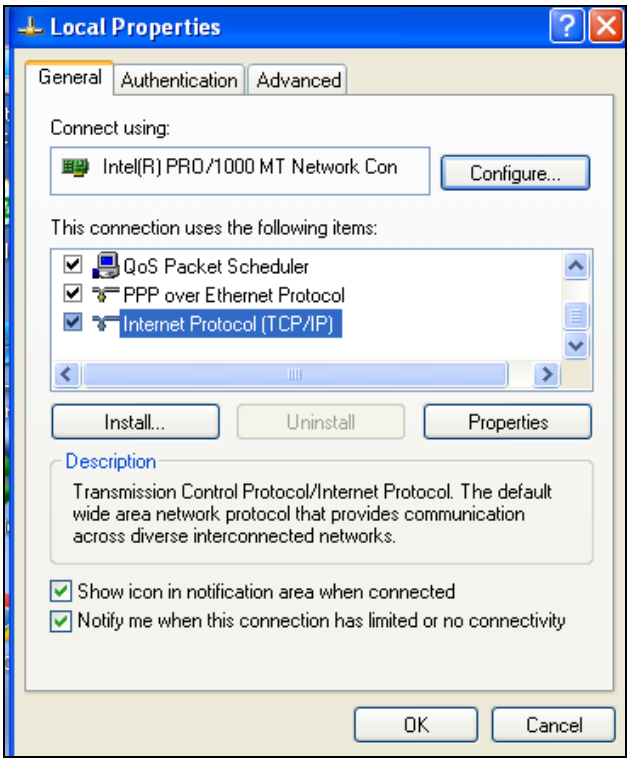
1. Right click **My Network Places** and click **Properties**;



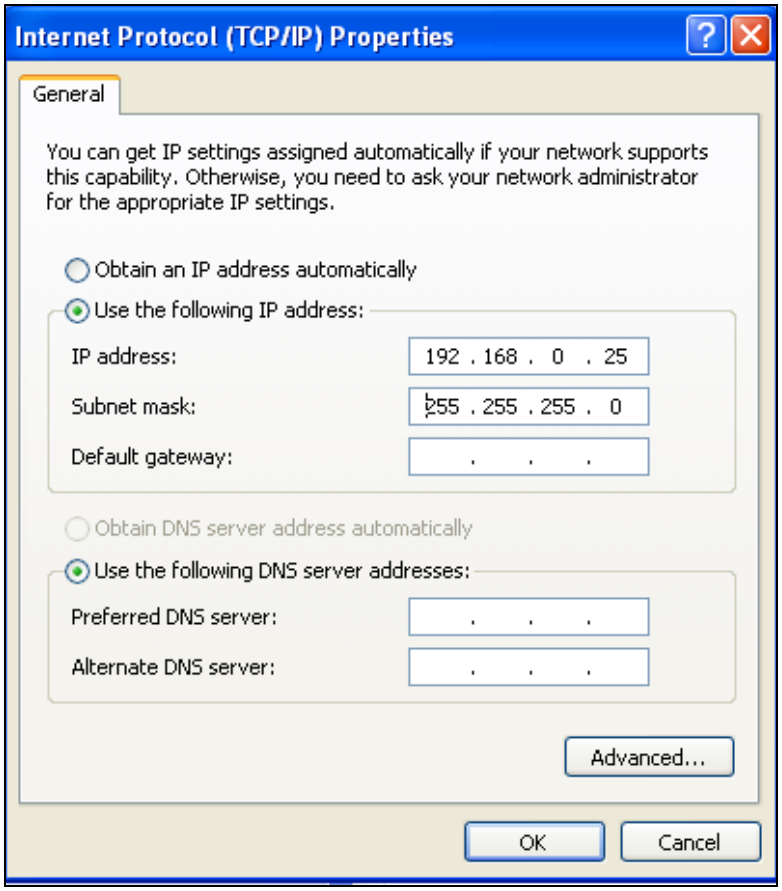
2. Right click **Local** and click **Properties**;



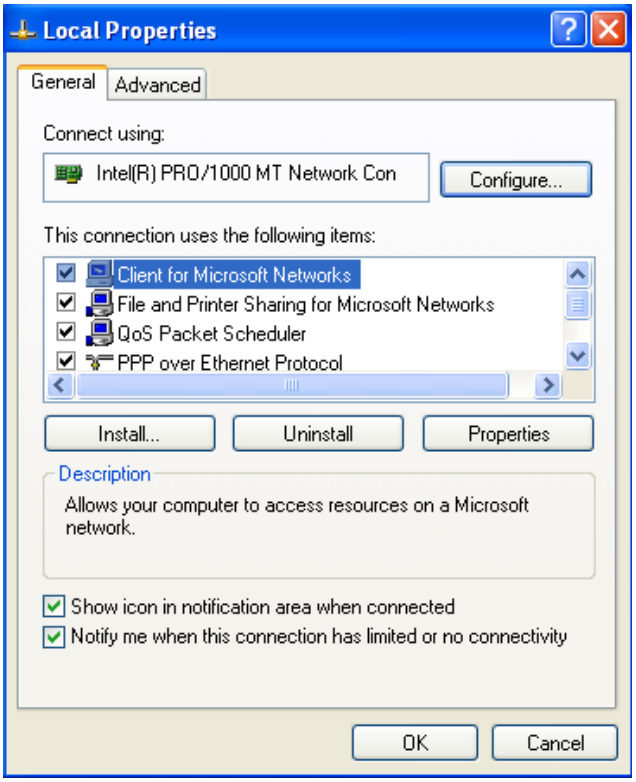
3. Find and double click **Internet Protocol (TCP/IP)**;



4. Select **Use the following IP address**, enter 192.168.0.X (2~253) in the **IP address** field and 255.255.255.0 in the **Subnet mask** field and then click **OK** to save the configurations;



5. Click **OK**.


Local Properties
General
Advanced
Connect using:
Intel(R) PRO/1000 MT Network Con
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
PPP over Ethernet Protocol
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel

2. FAQs

This section provides solutions to problems that may occur during installation and operation of the device. Read the following if you are running into problems. If your problem is not covered here, please feel free to go to www.tendacn.com to find a solution or email your problems to: support@tenda.com.cn. We will be more than happy to help you out as soon as possible.

Q: I enter the device's LAN IP address in the web browser but cannot access the utility. What should I do?

a. Check whether device is functioning correctly. The SYS LED should blink a few seconds after device is powered up.

b. Verify physical connectivity by checking whether a corresponding port's link LED lights up. If not, try a different cable.

c. Press and hold the Reset button on your device for over 7 seconds to restore factory default settings, and then re-log in to the device.

d. Check the TCP/IP settings on your PC and verify that the IP address, 192.168.0.X (2-253), is not used by other network devices.

e. Clear the browser cache or try another web browser.

f. Contact our technical support for help if the problem still exists after you tried all the above.

Q: What should I do if I forget the login username and password to my device?

a. Try the default username and password admin/admin.

b. Reset your device by pressing the Reset button for over 7 seconds.

Q: My computer shows an IP address conflict error after having connected to the device. What should I do?

a. Check if there are other DHCP servers present in your LAN. If there are other DHCP servers except your router, disable them immediately.

b. The default IP address of the device is 192.168.0.254; make sure this address is not used by another PC or device. In case that two computers or devices share the same IP addresses, change either to a different address.

Q: After joining your wireless connection, I can access the Internet but unable to log in to this device's Web interface. What should I do?

Please set your PC's IP to 192.168.0.X (2~253), log in to this device's Web interface to modify LAN IP address, which should be different but on the same network segment as the remote device, and then set your PC to **Obtain an IP address automatically**.

3. Default Settings

Parameters		Default Settings
AP Web Login	Login IP	192.168.0.254
	Username	admin
	Password	admin
Quick Setup	Working Mode	AP Mode
LAN Setup	Address Mode	Static IP
	IP Address	192.168.0.254
	Subnet Mask	255.255.255.0
	Gateway	192.168.0.1
Wireless	Wireless Setup	Enabled
	Primary SSID	Tenda_XXXXXX
	Network Mode	11/b/g/n mixed
	SSID Broadcast	Enabled
	AP Isolation	Disabled
	Channel	Auto
	Channel Bandwidth	20/40
	Channel Extension	Auto
	WMM Capable	Enabled
	APSD Capable	Disabled
	Security Mode	None
	Access Control	Disabled
SNMP	SNMP	Disabled
Tools	Time	Sync with Internet time servers

4. Safety and Emission Statement

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.

NCC Notice

第十二條

經形式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方的繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。