



**802.11 Mode:** Select a correct network mode according to your wireless clients.

- **11b mode:** This network mode delivers wireless speed up to 11Mbps and is only compatible with 11b wireless clients.
- **11g mode:** This network mode delivers wireless speed up to 54Mbps and is only compatible with 11g wireless clients.
- **11b/g mixed mode:** This network mode delivers wireless speed up to 54Mbps and is compatible with 11b/g wireless clients.
- **11b/g/n mixed mode:** This network mode delivers wireless speed up to 300Mbps and is compatible with 11b/g/n wireless clients.

**BSSID:** This is the MAC address of the device's wireless interface.

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

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

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

---

---

## 3.2 Security

Click **Wireless -> Security** to enter the configuration screen. Here you can define a security key to secure your wireless network against unauthorized accesses.

### Configuration Procedures:

- ① Configure **Security Mode**, **Cipher Type** and **Security Key**.
- ② Click **Save** to save your settings.



### Knowledge Center

**WEP:** WEP is intended to provide data confidentiality comparable to that of a traditional wired network.

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

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

**Default Key:** Select a key to be effective for the current WEP encryption. For example, if you select **Key 2**, wireless clients must join your wireless network using this **Key 2**.

**WPA-PSK:** WPA personal supports AES and TKIP cipher types.

**WPA2-PSK:** WPA2 personal supports AES, TKIP and TKIP+AES cipher types.

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

**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 secured wireless clients can join your wireless network.

**Key Renewal Interval:** Enter a valid time period for the key to be changed.

---

## WPS

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings. Simply enter a PIN code or press the hardware WPS button and a secure wireless connection is established.

The screenshot shows the Tenda router's configuration interface. The top navigation bar includes tabs for Wizard, Status, Basic, Wireless, Advanced, and Tools. The left sidebar has options for Basic, Security (selected), Access Control, and Connection Status. The main content area is titled 'Wireless Security' and contains the following settings:

- SSID: Tenda\_38DDC9
- Security Mode: Disable (dropdown menu)
- WPS Settings:
  - WPS:  Disable  Enable
  - Device Pin: 69790980
  - WPS Type:  PBC  PIN

Buttons for 'Start PIN', 'Reset OOB', 'Save', and 'Cancel' are located at the bottom of the settings area. A 'Help' section on the right provides additional information:

**Help**  
WEP Key: Select Open, Shared or Mixed WEP from the corresponding drop-down list. ASCII: Enter 5 or 13 ASCII characters. Hex: Enter 10 or 16 Hex characters.  
WPA/WPA2: You can select either personal or mixed, only ensure that either one you select is supported on your wireless clients.  
Important: If you are an advanced user and have configured security mode before, you can select any mode you like, only to assure that the one you choose is also supported by your wireless clients; if you are new to networking and have never configured this parameter before, we suggest that you select "WPA-PSK" or WPA2-PSK.



## Knowledge Center

**WPS:** Select **Enable/Disable** to enable/disable the WPS encryption.

**WPS Type:** Select PBC (Push-Button Configuration) or PIN.

**Reset OOB:** If clicked, the WPS LED will turn off and the security function will be disabled automatically. The WPS server on the router enters idle mode and will not respond to any client's WPS connection request.

---

**Device PIN:** Displays the device's PIN code.

**Start PIN:** If you enter the client's PIN code on the router, clicking this button starts the PIN connection.

---

---

### **Operation Instructions:**

**PBC:** If you press the hardware WPS button on the device for 1 second, the WPS LED will blink for about 2 minutes, indicating that the PBC encryption method is successfully enabled. During this time, an authentication routine can be performed between your device and a WPS/PBC capable wireless client. Simply enable the WPS/PBC on the client wireless device. If it passes the authentication, the wireless client device connects to your device and the WPS LED turns off. Repeat the steps above if you want to add more wireless client devices to your device.

**PIN:** To use this option, you must know the PIN code from the wireless client and enter it in the corresponding field on your device while using the same PIN code on the client side for this connection.

---

---

### **Note**

- ① To use the WPS encryption, the wireless client device must also be WPS-capable.
  - ② The **WPS** becomes unavailable if you select any of the following option: **Open**, **Shared**, **WPA2-PSK** plus **TKIP**, and **Mixed WPA/WPA2-PSK** plus **TKIP**.
- 
- 

## **3.3 Access Control**

Specify a list of devices to "Allow" or "Deny" a connection to your wireless network via the devices' MAC Addresses.

Click **Wireless -> Access Control** to enter the configuration screen. Three options are available: **Disable**, **Deny** and **Allow**.

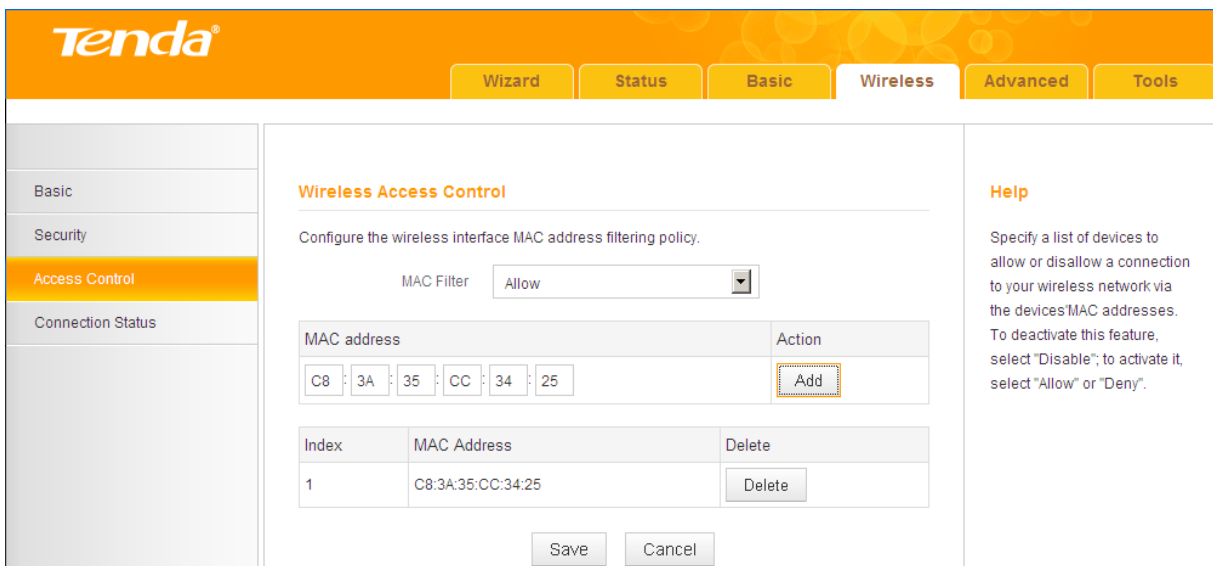
- A.** If you want to allow all wireless clients to join your wireless network, select **Disable**.

- B.** If you want to allow ONLY the specified wireless clients to join your wireless network, select **Allow**.
- C.** If you want to disallow ONLY the specified wireless clients to join your wireless network, select **Deny**.

**Wireless Access Control Application Example:**

To only allow your own notebook at the MAC address of C8:3A:35:CC:34:25 to join your wireless network:

- ① Select **Allow**.
- ② Enter **C8:3A:35:CC:34:25**.
- ③ Click **Add** to add the MAC address to the MAC address list.
- ④ Click **Save** to save your settings.



 **Tip**

If you don't want to configure the complex wireless security settings and want to disallow others to join your wireless network, you can configure a wireless access control rule to allow only your own wireless device.

### 3.4 Connection Status

Click **Wireless -> Connection Status**. Here you can see a list of wireless

devices (if any) connected to the device.

**Wireless Connection Status**

This section displays info of connected wireless clients.

Currently Connected Clients:

NO.	MAC address	Bandwidth
1	70:72:3C:30:4B:D7	58.0 Mbps

**Help**

This section displays info of connected wireless clients.  
MAC: Wireless MAC address of a current host.



### Tip

- ① The **Bandwidth** here refers to the channel bandwidth instead of wireless connection rate.
- ② You can know whether there are unauthorized accesses to your wireless network by viewing this connection status list.

## 4 Advanced Applications

This section includes the following:

- To remotely access the device via a domain name or access a server on a LAN PC, see [\*\*4.1 DDNS Settings\*\*](#).
- To let an Internet user access your LAN PC without any restriction, see [\*\*4.2 DMZ Host\*\*](#).
- To automatically map the ports between WAN and LAN, see [\*\*4.3 UPNP\*\*](#).
- To enable the remote Web management feature, see [\*\*4.4 Remote Web Management\*\*](#).
- To regulate bandwidth, see [\*\*4.5 Bandwidth Control \(Available only in 4G600\)\*\*](#).
- To restrict your LAN PCs to access certain services on the Internet via their IP addresses, see [\*\*4.6 Client Filter \(Available only in 4G600\)\*\*](#).

### 4.1 DDNS Settings

Dynamic DNS or DDNS is a term used for the updating in real time of Internet Domain Name System (DNS) name servers. We use a numeric IP address allocated by Internet Service Provider (ISP) to connect to the Internet; the address may either be stable ("static"), or may change from one session on the Internet to the next ("dynamic"). However, a numeric address is inconvenient to remember; an address which changes unpredictably makes connection impossible. The DDNS provider allocates a static host name to the user; whenever the user is allocated a new IP address this is communicated to the DDNS provider by software running on a computer or network device at that address; the provider distributes the association between the host name and the address to the Internet's DNS servers so that they may resolve DNS queries. Thus, uninterrupted access to devices and services whose numeric IP address may change is maintained.

Click **Advanced -> DDNS Settings** to enter the screen below.



### Tip

To use the DDNS feature, you need to have an account with one of the **DDNS Service Providers** in the drop-down list first.

### DDNS Application Example:

If your ISP gives you a dynamic (changing) public IP address, you want to access your router remotely (see [4.4 Remote Web Management](#)) but you cannot predict what your router's WAN IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. It lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If your DDNS service provider provides you with a DDNS account (**User Name:** tenda, **Password:** 123456, **Domain Name:** tenda.dyndns.org) and you want to use the PC at the IP address of 218.88.93.33 to remotely access this device on the port number of 8090. Then follow the steps below:

- ① **DDNS Settings:** Check the **Enable DDNS** box.
- ② **DDNS Service Provider:** Select your DDNS service provider from the drop-down list. Here in this example, select **dyndns.org**.
- ③ **User Name:** Enter the DDNS user name you have registered with your



DDNS service provider. Here in this example, enter tenda.

④ **Password:** Enter the DDNS Password you have registered with your DDNS service provider. Here in this example, enter 123456.

⑤ **Domain Name:** Enter the DDNS domain name you have registered with your DDNS service provider. Here in this example, enter tenda.dyndns.org.

⑥ Click **Save** to save your settings.

The screenshot shows the Tenda router's web interface. At the top, there's a navigation bar with tabs: Wizard, Status, Basic, Wireless, Advanced (selected), and Tools. On the left, a sidebar lists settings: DDNS Settings (selected), DMZ Host, UPnP, and Remote Web Management. The main content area is titled 'DDNS Settings' and includes a 'DNS Settings' section with a checked 'Enable DDNS' option. Below this, there are fields for 'DNS Service Provider' (a dropdown menu showing 'dyndns.org' with a 'Register Now' link), 'User Name' (text box with 'tenda'), 'Password' (text box with masked characters), and 'Domain Name' (text box with 'tenda.dyndns.org'). At the bottom of this section are 'Save' and 'Cancel' buttons. To the right, a 'Help' section provides instructions on how to use DDNS, including a link to 'Register Now' and details about selecting a service provider and entering credentials.

⑦ Click **Remote Web Management**, enable the **Remote Web Management** feature, enter **8090** in the **Port** field, **218.88.93.33** in the **IP Address** field and then click **Save** to save your settings.

The screenshot shows the Tenda router's web interface. At the top, there's a navigation bar with tabs: Wizard, Status, Basic, Wireless, Advanced (selected), and Tools. On the left, a sidebar lists settings: DDNS Settings, DMZ Host, UPnP, and Remote Web Management (selected). The main content area is titled 'Remote WEB Management' and includes an 'Enable' checkbox which is checked. Below this, there are fields for 'Port' (text box with '8090') and 'IP Address' (text box with '218.88.93.33'). At the bottom of this section are 'Save' and 'Cancel' buttons. To the right, a 'Help' section explains the Remote Web Management feature, stating it allows the router to be managed from the Internet via a web browser and provides instructions on enabling the feature and specifying the port and IP address.

Now, you can access your device from the Internet by typing your device's domain name into your browser's address or location field on your PC

(218.88.93.33) followed by a colon (:) and the remote management port number. Here in this example, enter **http://tenda.dyndns.org:8090**.

## 4.2 DMZ Host

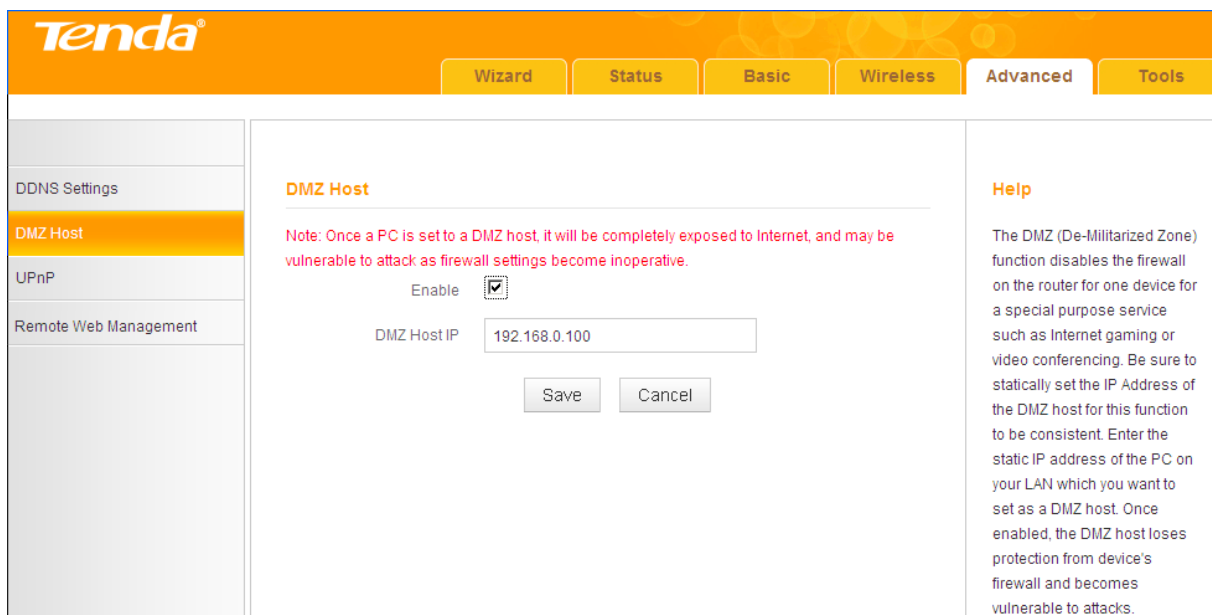
The DMZ (De-Militarized Zone) function disables the firewall on the router for one device for a special purpose service such as Internet gaming or video conferencing applications that are not compatible with NAT (Network Address Translation).

Click **Advanced -> DMZ Host** to enter the screen below.

---

### Note

- ① DMZ host poses a security risk. A computer configured as the DMZ host loses much of the protection of the firewall and becomes vulnerable to attacks from external networks.
  - ② Hackers may use the DMZ host computer to attack other computers on your network.
- 



The screenshot shows the Tenda router's web interface. The top navigation bar includes 'Wizard', 'Status', 'Basic', 'Wireless', 'Advanced', and 'Tools'. The 'Advanced' tab is selected, and the 'DMZ Host' sub-tab is active. On the left sidebar, 'DMZ Host' is highlighted. The main content area displays the 'DMZ Host' configuration. A red note reads: 'Note: Once a PC is set to a DMZ host, it will be completely exposed to Internet, and may be vulnerable to attack as firewall settings become inoperative.' Below this, the 'Enable' checkbox is checked. The 'DMZ Host IP' field contains the value '192.168.0.100'. At the bottom of the configuration area are 'Save' and 'Cancel' buttons. On the right side, a 'Help' section provides a detailed explanation of the DMZ function, stating that it disables the firewall for a specific device, making it vulnerable to attacks.

### Configuration Procedures:

- ① **DMZ Host IP:** The IP address of the device for which the router's firewall

will be disabled. Be sure to statically set the IP address of the device that serves as a DMZ host for this function to be consistent.

- ② **Enable:** Check to enable the DMZ host functionality.
- ③ Click **Save** to save your settings.



Security softwares such as anti-virus softwares and OS built-in firewall, etc. may affect the DMZ host feature. Disable them if the DMZ host fails.

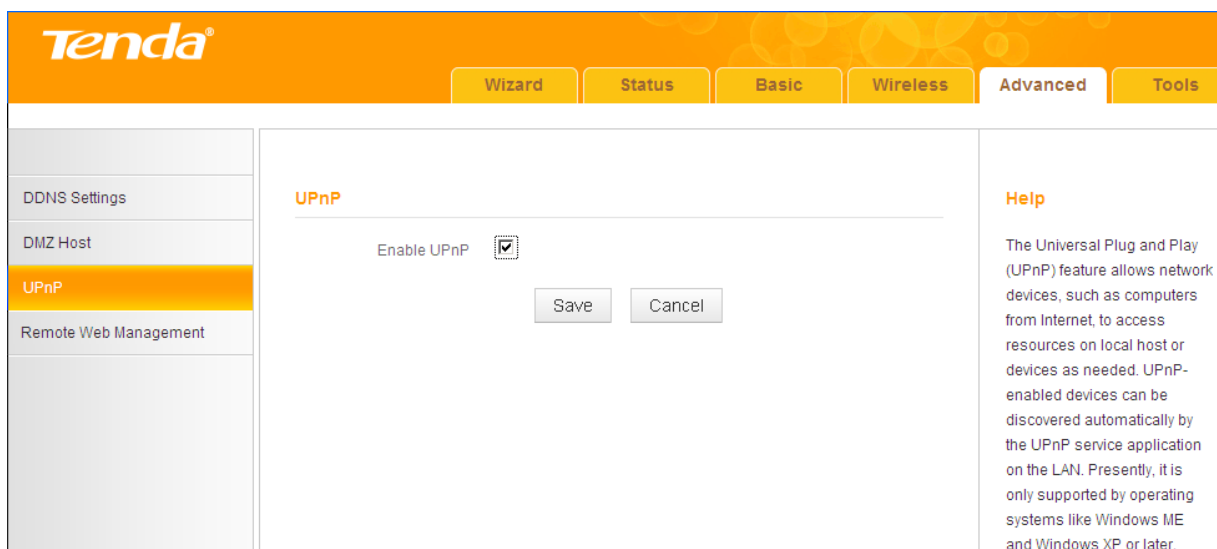
---

---

## 4.3 UPnP

The Universal Plug and Play (UPnP) feature allows network devices, such as computers from the Internet, to access resources on local host or devices as needed. UPnP-enabled devices can be discovered automatically by the UPnP service application on the LAN. If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you may need to enable Universal Plug and Play (UPnP) for better experience.

Click **Advanced -> UPnP** to enter the configuration screen. The UPnP feature is enabled by default.

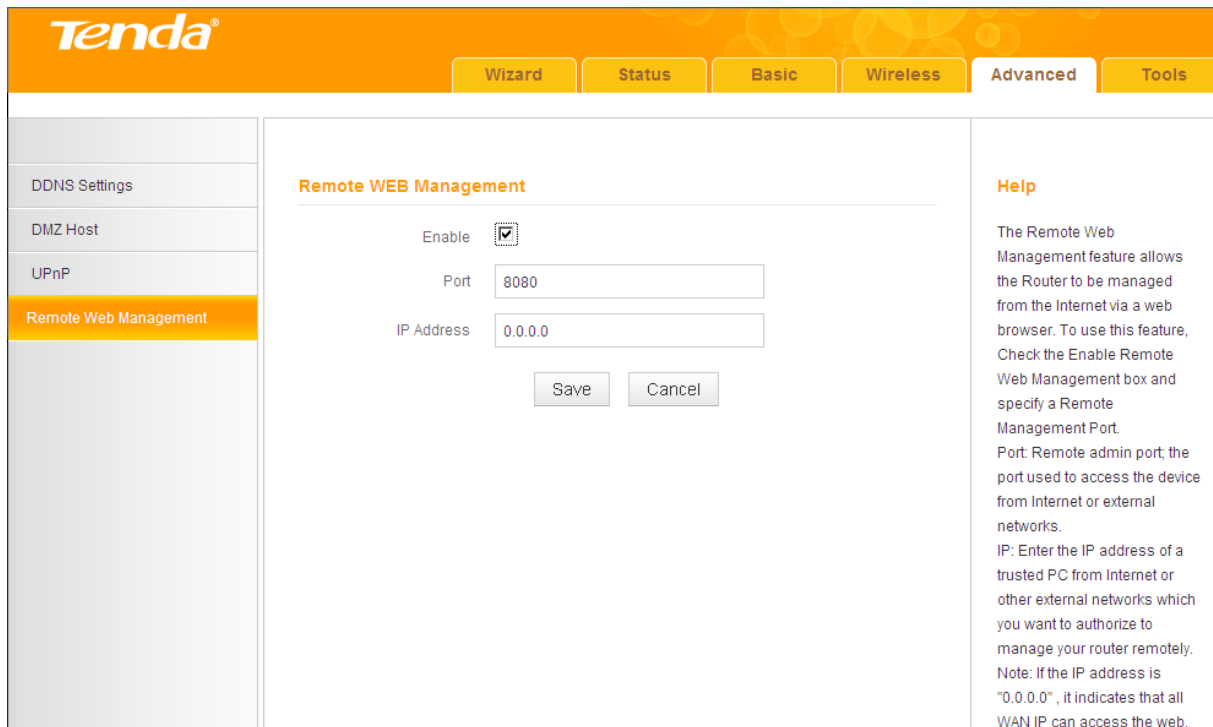


The screenshot shows the Tenda web interface. At the top, there's a navigation bar with tabs: Wizard, Status, Basic, Wireless, Advanced, and Tools. The 'Advanced' tab is selected. On the left, there's a sidebar menu with options: DDNS Settings, DMZ Host, UPnP (highlighted), and Remote Web Management. The main content area is titled 'UPnP' and contains a checkbox labeled 'Enable UPnP' which is checked. Below the checkbox are 'Save' and 'Cancel' buttons. On the right side of the main content area, there's a 'Help' section with text explaining the UPnP feature: 'The Universal Plug and Play (UPnP) feature allows network devices, such as computers from Internet, to access resources on local host or devices as needed. UPnP-enabled devices can be discovered automatically by the UPnP service application on the LAN. Presently, it is only supported by operating systems like Windows ME and Windows XP or later.'

## 4.4 Remote Web Management

The Remote Web Management allows the device to be configured and managed remotely from the Internet via a Web browser.

Click **Advanced** -> **Remote Web Management** to enter the configuration screen.



### Tip

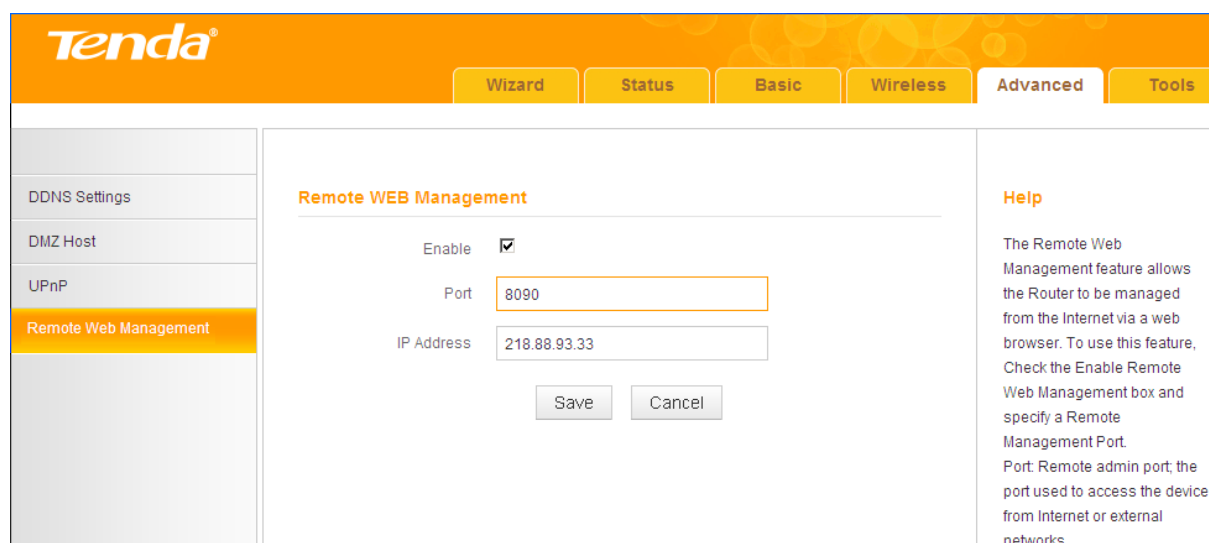
- ① For better security, configure a port number (between 1025 and 65535) as the remote Web management interface, do not use the number of any common service port (1~1024).
- ② Make sure your WAN IP address (Internet IP address) is a public IP address. Private IP addresses are not routed on the Internet.
- ③ It is unsafe to make your router remotely accessible to all PCs on external network. For the purpose of security, we suggest that you only enter the IP address of the PC that is to be used to remotely manage your device.

### Remote Web Management Application Example:

To access your device (WAN IP address: 102.33.66.88) at your home from the

PC (218.88.93.33) at your office via the port number of 8090, follow the steps below:

- ① **Enable:** Check to enable the remote Web management feature.
- ② **Port:** Enter 8090.
- ③ **IP Address:** Specify the IP address for remote management. Here in this example, enter 218.88.93.33.
- ④ Click **Save** to save your settings.



Type "http://102.33.66.88:8090" into your browser's address or location field and you can remotely access the router from your home.



### Knowledge Center

**IP Address:** Here you can specify the IP address for remote management (If set to "0.0.0.0", the device becomes remotely accessible to all the PCs on the Internet or other external networks).

**Port:** This is the management port to be open to outside access. The default setting is 8080. This can be changed.

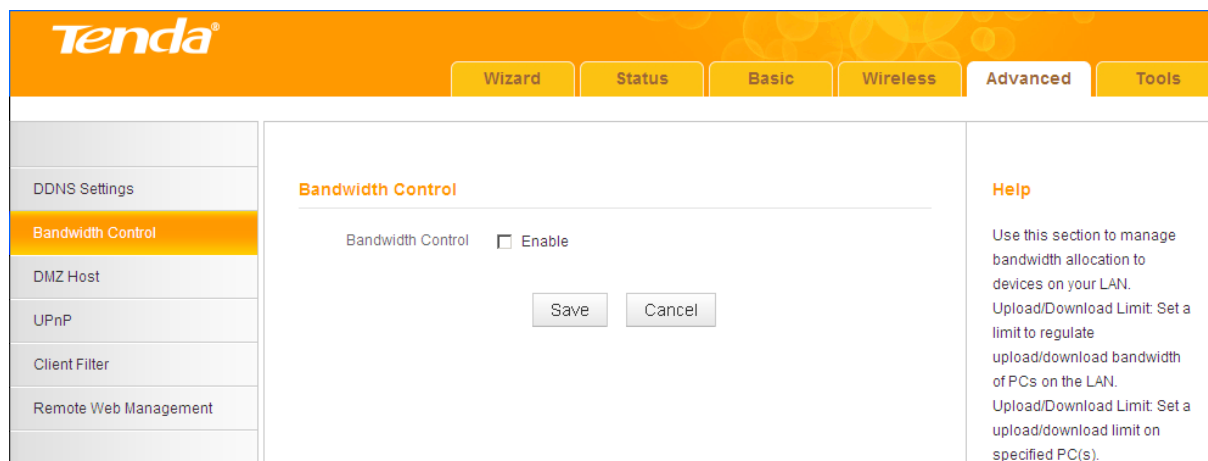
---

---

## 4.5 Bandwidth Control (Available only in 4G600)

If there are multiple PCs behind your device competing for limited bandwidth resource, then you can use this feature to specify a reasonable amount of

bandwidth for each such PC, so that no one will be over stuffed or starved to death. Note that this feature is unavailable in **3G/4G Router Mode**.



### Bandwidth Control Application Example:

You share a 4M-broadband service with your neighbor (at the IP address of 192.168.0.125). He always downloads a large volume of data from the Internet, which sharply frustrates your Internet surfing experience; you can use this feature to set limits for the volume of Internet traffic he can get. For example, you can equally split the bandwidth, so your neighbor can only use up to 2M Internet traffic and you can smoothly enjoy 2M.

### Configuration Procedures:

- ① **Bandwidth Control:** Check the **Enable** box to enable the feature.
- ② **IP Address:** Enter the last number of the IP address. Here in this example, enter 125 in both boxes.
- ③ **Upload Limit:** Set a limit to regulate the uplink bandwidth of PC(s) on the LAN. Here in this example, enter 32 in both boxes.
- ④ **Download Limit:** Set a limit to regulate the downlink bandwidth of PC(s) on the LAN. Here in this example, enter 256 in both boxes.
- ⑤ **Enable:** Check to enable the current rule.
- ⑥ **Add to List:** Click to add the current rule to the rule list.
- ⑦ Click **Save** to save your settings.

**Tenda**

Wizard Status Basic Wireless **Advanced** Tools

DDNS Settings

**Bandwidth Control**

DMZ Host

UPnP

Client Filter

Remote Web Management

**Bandwidth Control**

Bandwidth Control  Enable

IP Address 192.168.0.  ~

Upload Limit  KB/s(Max Traffic)

Download Limit  KB/s(Max Traffic)

Enable

ID	IP Range	Uplink	Downlink	Enable	Edit	Delete
1	192.168.0.125~125	32	256	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

**Help**

Use this section to manage bandwidth allocation to devices on your LAN. Upload/Download Limit: Set a limit to regulate upload/download bandwidth of PCs on the LAN. Upload/Download Limit: Set a upload/download limit on specified PC(s).



### Tip

- ① 1M=128KByte/s.
- ② The volume of uplink traffic/downlink traffic should not be larger than that allowed on your device's WAN (Internet) port. Consult your ISP, if you are not sure of the total volume of Internet traffic that you can have.
- ③ The bandwidth for ADSL/DSL line usually refers to the download bandwidth.

## 4.6 Client Filter (Available only in 4G600)

This section allows you to set the times specific clients can or cannot access the Internet via the devices' IP addresses and service port. Note that this feature is unavailable in **3G/4G Router Mode**.



## Knowledge Center

**Default:** The default policy for the client filter. For the packets that do not match the set rule, the default rule is applied.

**Filter Mode:** Specify a filter mode for the rule.

- ✓ **Deny:** Disallow the packets that match the set rule to pass the router. For other packets that do not match the set rule, the default policy is applied.
- ✓ **Allow:** Allow the packets that match the set rule to pass the router. For other packets that do not match the set rule, the default policy is applied.

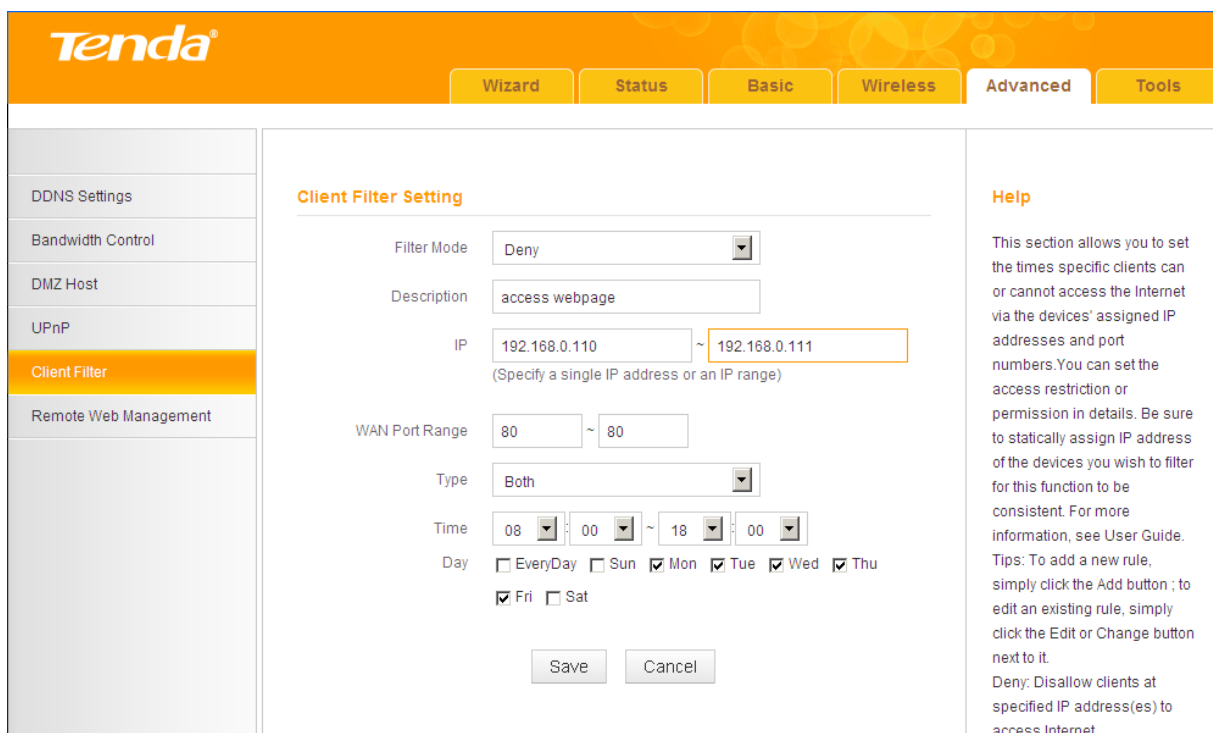
### Client Filter Application Example:

To prohibit PCs within the IP address range of 192.168.0.110--192.168.0.111 from accessing Web pages during the time period of 8:00~18:00 from Monday to Friday, follow the steps below:

- ① Click **Add** to add a filter rule.
- ② **Filter Mode:** Select **Deny**.
- ③ **Description:** Briefly describe the current rule. This field is optional.
- ④ **IP:** Enter 192.168.0.110 as the starting IP address and 192.168.0.111 as the ending IP address.



- ⑤ **WAN Port Range:** Enter a service port number. Here in this example, enter 80 in both boxes. HTTP port 80 is the standard protocol for Web servers.
- ⑥ **Type:** Select a protocol for the traffic. If you are unsure, select **Both**.
- ⑦ **Time:** Specify a time period for the current rule to take effect. Here in this example, select 8:00~18:00.  
**Day:** Select a day, or several days of the week for the current rule to take effect. Here in this example, select **Mon, Tue, Wed, Thur** and **Fri**.
- ⑧ Click **Save** to save your settings.



- ⑨ **Enable Client Filter:** Check to enable the client filter feature.
- ⑩ Select **Allow** from the **Default** drop-down list and then click **Save**.

**Tenda**

Wizard   Status   Basic   Wireless   **Advanced**   Tools

DDNS Settings  
Bandwidth Control  
DMZ Host  
UPnP  
**Client Filter**  
Remote Web Management

### Client Filter

Enable Client Filter

Default Allow Access from clients NOT included in below list to Internet

Mode	IP	Port	Type	Time	Day							Action
					S	M	T	W	T	F	S	
Deny	192.168.0.110-192.168.0.111	80-80	Both	08:00-18:00	x	√	√	√	√	√	x	Edit Del

Delete All   Add

Save   Cancel

### Help

This section allows you to set the times specific clients can or cannot access the Internet via the devices' assigned IP addresses and port numbers. You can set the access restriction or permission in details. Be sure to statically assign IP address of the devices you wish to filter for this function to be consistent. For more information, see User Guide.

Tips: To add a new rule, simply click the Add button ; to edit an existing rule, simply click the Edit or Change button next to it.

Deny: Disallow clients at specified IP address(es) to access Internet.



### Tip

- ① The valid service port number range is 1 ~ 65535.
- ② If you have not set up the system time for this device, click **Tools -> Time & Date** to configure correct time and date settings for the rule(s) to be effective.

## 5 Tools

- To configure system time, see [5.1 Time & Date](#).
- To upgrade firmware, see [5.2 Firmware Upgrade](#).
- To backup or restore configurations, see [5.3 Backup & Restore](#).
- To restore factory default settings, see [5.4 Restore to Factory Default](#).
- To change login password, see [5.5 Change Password](#).
- To view logs, see [5.6 Logs](#).
- To restart device, see [5.7 Reboot](#).

### 5.1 Time & Date

Click **Tools** -> **Time & Date** to enter the configuration screen.



Configured time and date settings will be lost if the device gets disconnected from power supply. However, it will be updated automatically when the device reconnects to the Internet. To activate time-based features (e.g. **Client Filter**), the time and date settings should be set correctly first, either manually or automatically.

---

---

#### **A. To synchronize with Internet time servers:**

- ① **Internet Time Server:** Check to enable the feature (If enabled, time and date will be updated automatically from the Internet).
- ② **Sync Interval:** Specify a time interval for periodic update of time and date information from the Internet.
- ③ **Time Zone:** Select your current time zone.
- ④ Click **Save** to save your settings.
- ⑤ Go to the **Status** screen to make sure the system time is correctly updated.

**Tenda**

Wizard Status Basic Wireless Advanced Tools

**Time & Date**

Internet Time Server  Enable

Sync Interval 2 hours

Time Zone ( GMT+08:00 )Beijing,China, Hong

Input Time And Date 2013 - 12 - 16 18 : 43 : 11

Copy Local Time

Save Cancel

**Help**

This page is used to set the device'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. Note: System time will be lost 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 (e.g. firewall), the time and date info shall be set correctly first, either manually or automatically.

### Note

In the **Universal Repeater Mode**, the **Internet Time Server - Enable** feature is not available, so you can only set the time and date manually.

### **B. To set time and date manually/synchronize with your PC:**

- ① **Internet Time Server:** Uncheck to disable the feature.
- ② Specify the time and date manually or click **Copy Local Time** to automatically copy your PC's time to the device.
- ③ Click **Save** to save your settings.

The screenshot shows the Tenda web interface. At the top, there is a navigation bar with tabs: Wizard, Status, Basic, Wireless, Advanced, and Tools. The 'Tools' tab is active. On the left, a sidebar menu lists various tools: Time & Date (highlighted), Firmware Upgrade, Backup & Restore, Restore to Factory Default, Change Password, Logs, and Reboot. The main content area is titled 'Time & Date' and contains the following settings:

- Internet Time Server:  Enable
- Sync Interval: 2 hours (dropdown menu)
- Time Zone: ( GMT+08:00 )Beijing,China, Hong (dropdown menu)
- Input Time And Date: 2013 - 12 - 16 18 : 43 : 11

Below the settings are three buttons: 'Copy Local Time', 'Save', and 'Cancel'. On the right side of the main content area, there is a 'Help' section with the following text:

**Help**  
This page is used to set the device'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.  
Note: System time will be lost 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 (e.g. firewall), the time and date info shall be set correctly first, either manually or automatically.

- ④ Go to the **Status** screen to make sure the system time is correctly updated.

## 5.2 Firmware Upgrade

Click **Tools -> Firmware Upgrade** to enter the configuration screen. Firmware upgrade is released periodically to improve the functionality of your device and also 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.

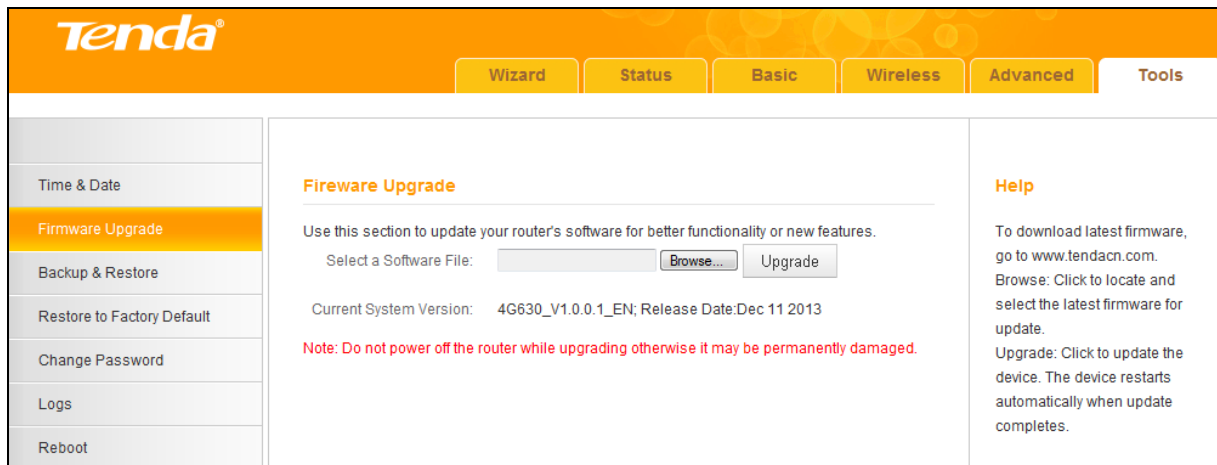
---

### Note

- ① Before you upgrade the firmware, make sure you are having a correct firmware. A wrong firmware may damage the device.
  - ② It is advisable that you upgrade the device's firmware over a wired connection. DO NOT disconnect the power connection to the device when the upgrade is in process otherwise the router may be permanently damaged.
- 

### Configuration Procedures:

- 1 Click **Browse**.



- 2 Select the firmware file you want to use and click **Open**.
- 3 Click **Upgrade**.
- 4 Click **OK** on the appearing screen and wait for it to complete.

When upgrade is completed, check the **Current System Version** field. It should display the firmware you load.

### 5.3 Backup & Restore

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. Click **Tools -> Backup & Restore** to enter the configuration screen.



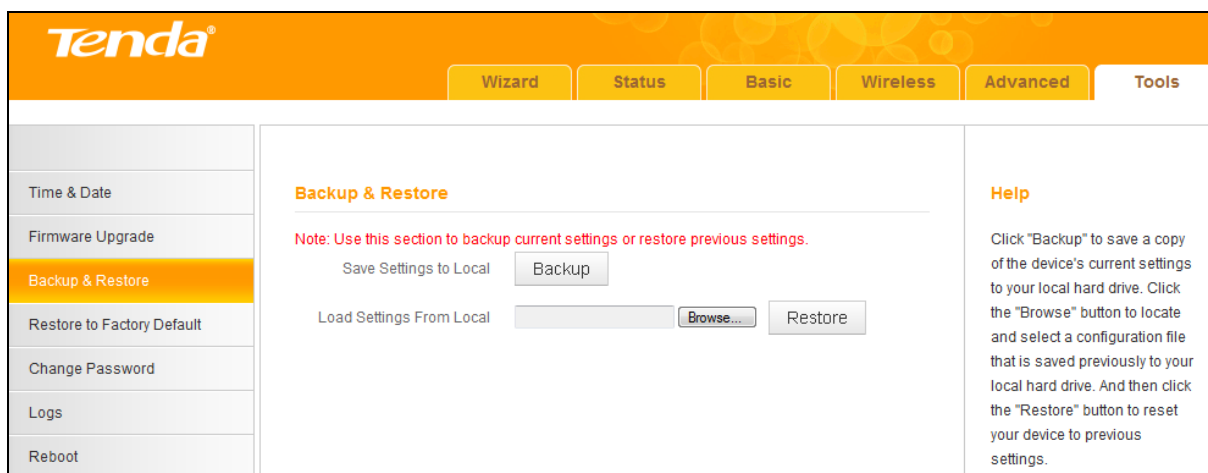
**Tip**  
It is advisable to include the file name suffix of ".cfg" to avoid problems when renaming the file name.

---

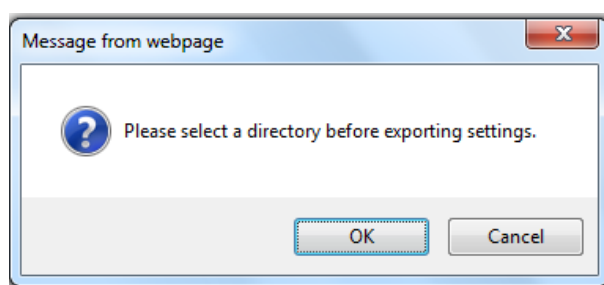
---

**To backup configurations:**

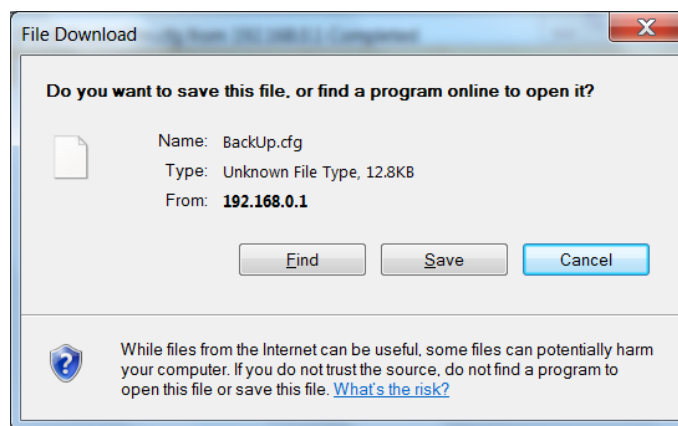
- 1 Click **Backup**.



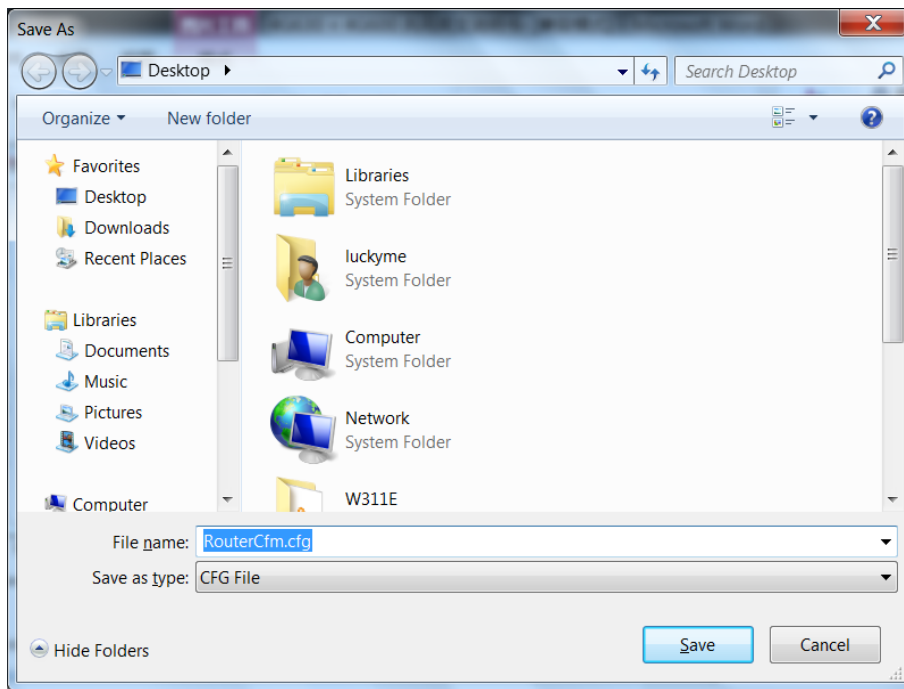
② Click **OK** on the appearing window.



③ Click **Save** on the **File Download** window.

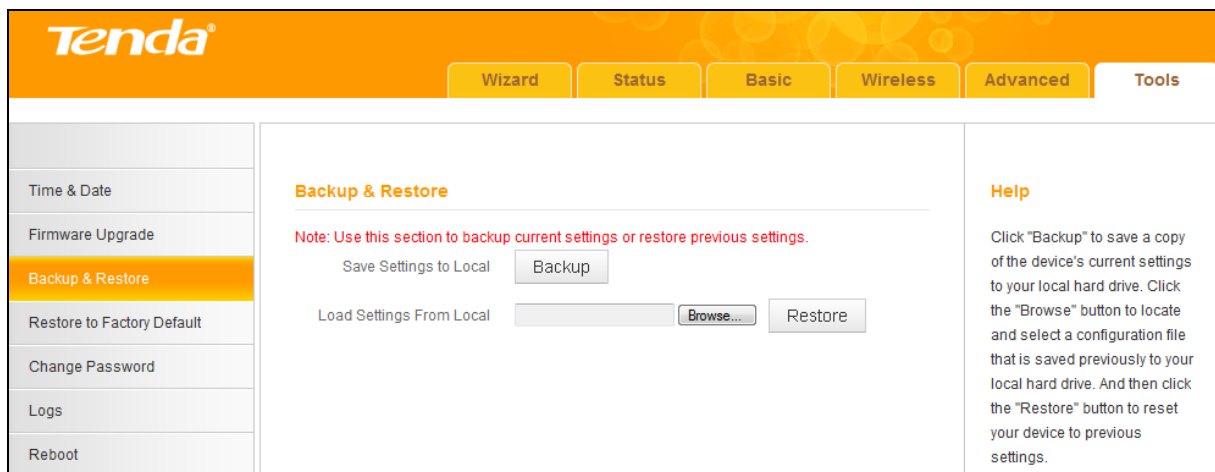


④ Select a local hard drive to save the file and click **Save**.



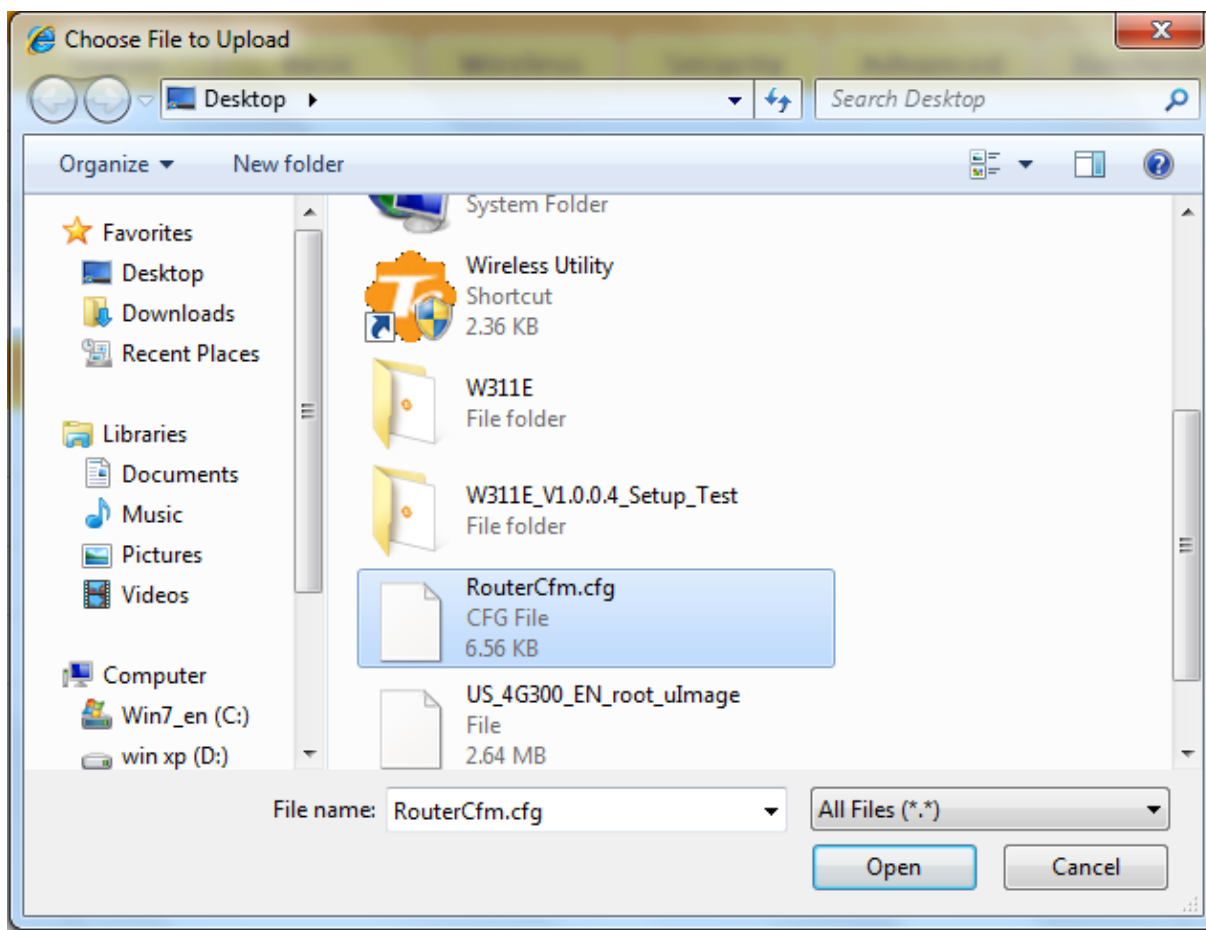
### To restore configurations:

- 1 Click **Browse**.



- 2 Select the configuration file that is saved previously to your local hard drive and click **Open**.





- ③ Click the **Restore** button to reset your device to previous settings.

## 5.4 Restore to Factory Default

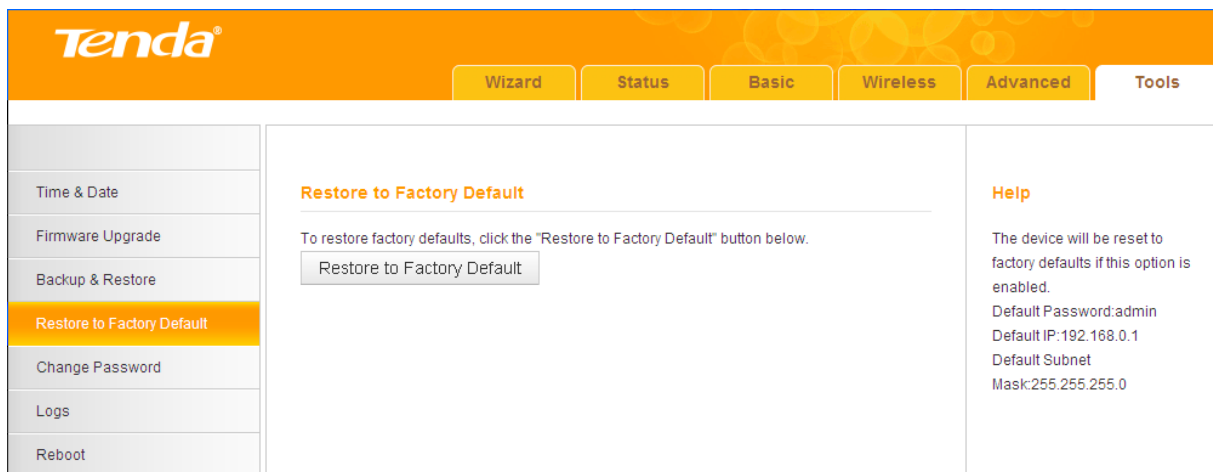
Click **Tools -> Restore to Factory Default** to enter the configuration screen. Here you can reset the device to factory default settings.

---

### Note

- ① If you enable this option, the device will be restored to factory default values. You will have to reconfigure Internet connection settings and wireless settings.
- ② Do not restore factory default settings unless the following happens:
  - ✓ You need to join a different network or unfortunately forget the login password.
  - ✓ You cannot access the Internet and your ISP or our technical support asks

you to reset the device.



The factory default settings are listed below:

- **IP Address:** 192.168.0.1
- **Subnet Mask:** Enter 255.255.255.0.
- **Password:** admin

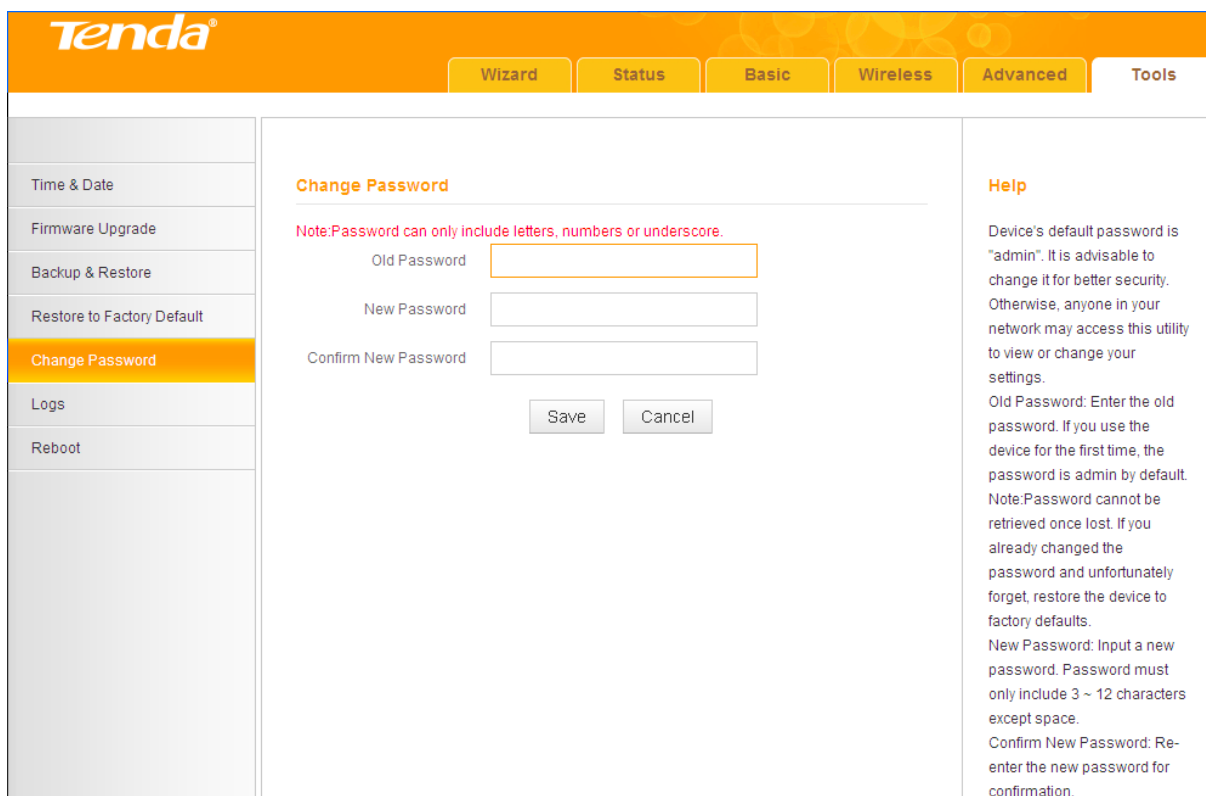
## 5.5 Change Password

Click **Tools** -> **Change Password** to enter the configuration screen. It is strongly recommended that you change the factory default login password. Otherwise, anyone in your network can access this utility to change your settings.



**Tip**

- ① The default login password is "admin".
- ② A valid password must only include letters, numbers or underscore.

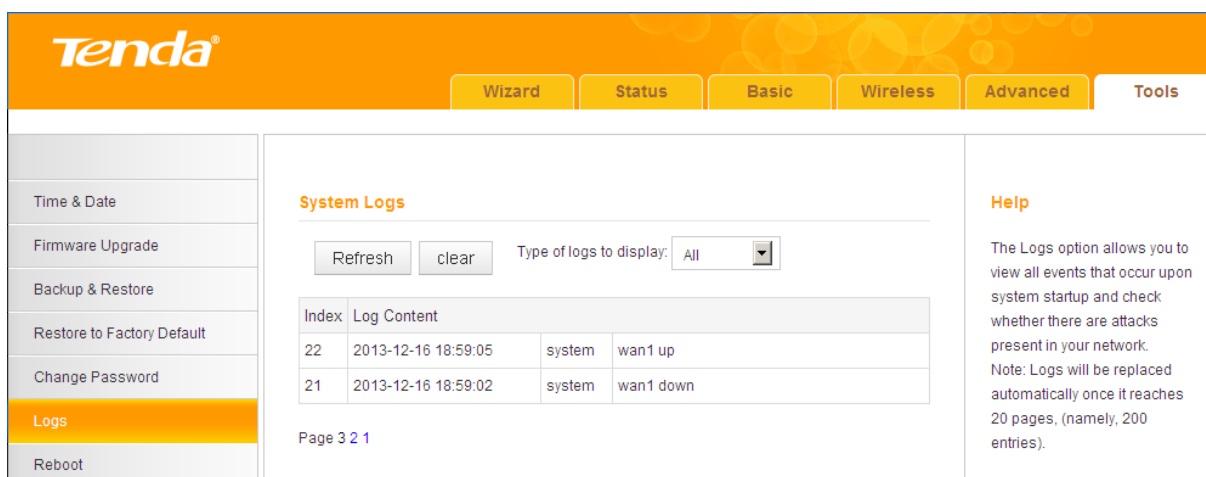


### Configuration Procedures:

- ① **Old Password:** Enter the current login password.
- ② **New Password:** Input a new password.
- ③ **Confirm New Password:** Re-enter the new password for confirmation.
- ④ Click **Save** to save your settings.

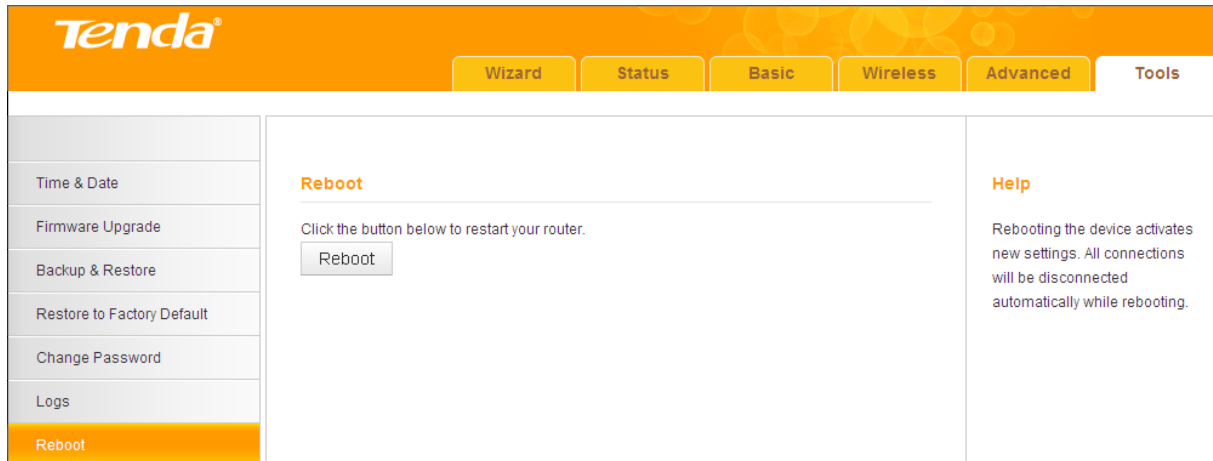
## 5.6 Logs

Click **Tools -> Logs** to enter the configuration screen. Here you can view the history of the device's actions upon system startup.



## 5.7 Reboot


When a certain feature does not take effect or the device is malfunctioning, try rebooting the device.



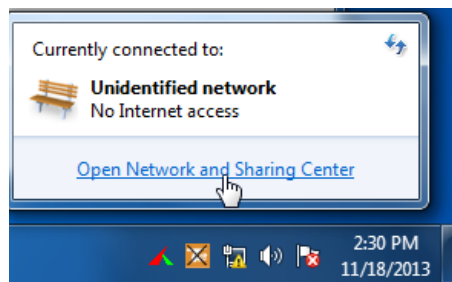
# IV Appendix


## 1 Configure Your PC

### Windows 7

**Step 1:** Click the icon  on the right bottom corner of your desktop.

**Step 2:** Click **Open Network and Sharing Center**.

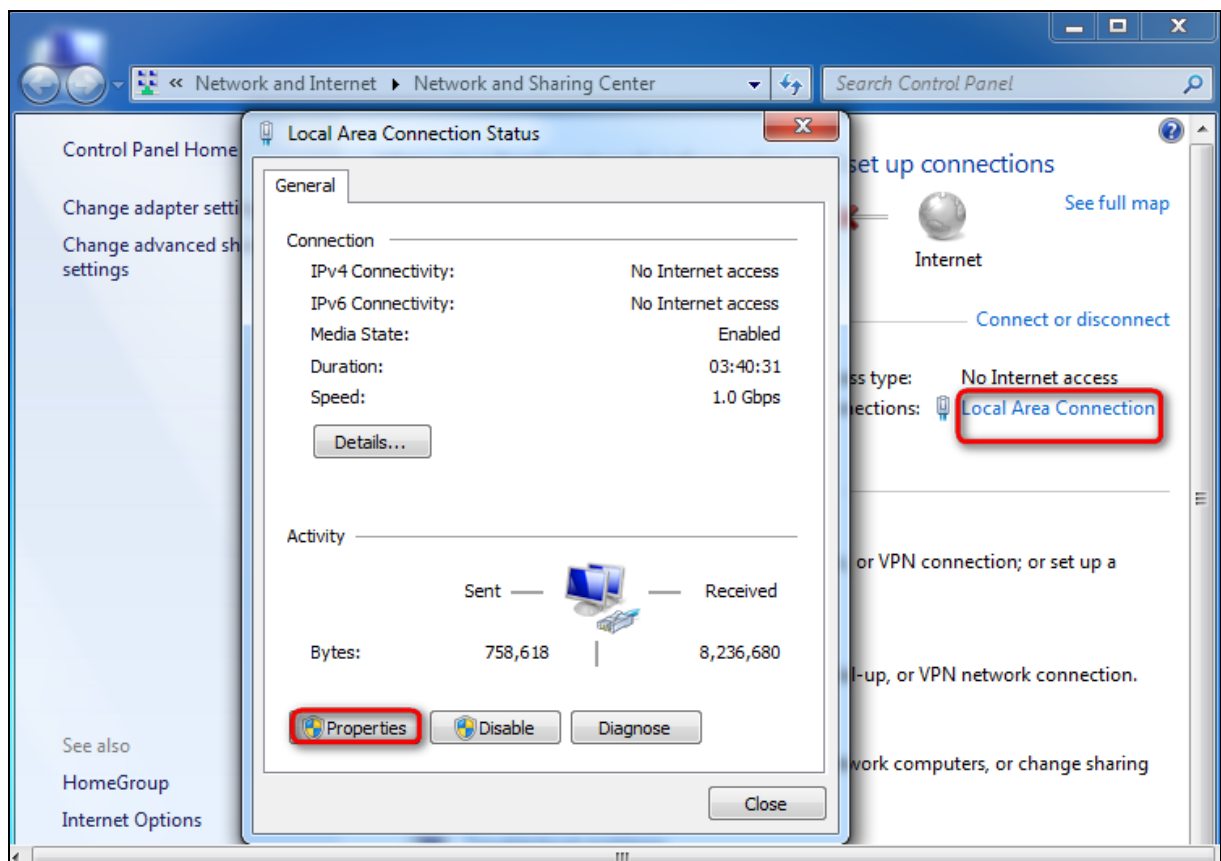


If you cannot find the icon  on the right bottom corner of your desktop, follow steps below: Click **Start -> Control Panel -> Network and Internet -> Network and Sharing Center**.

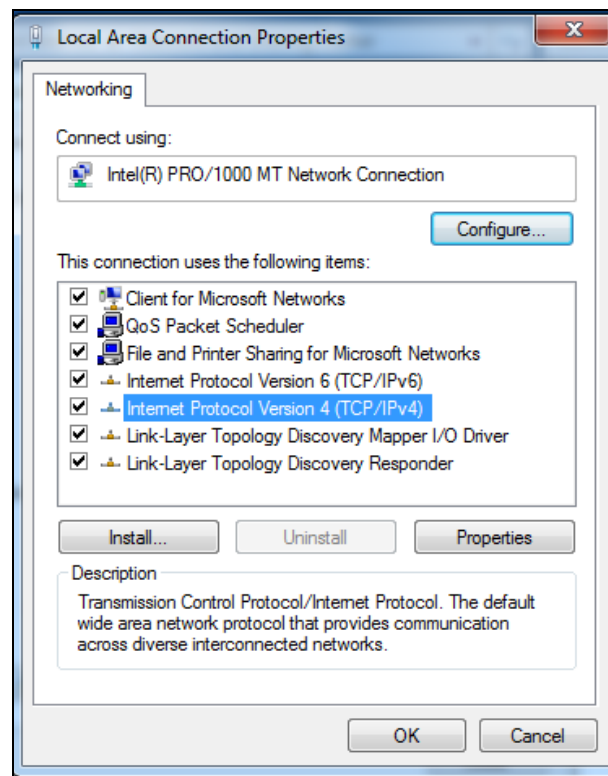
---

---

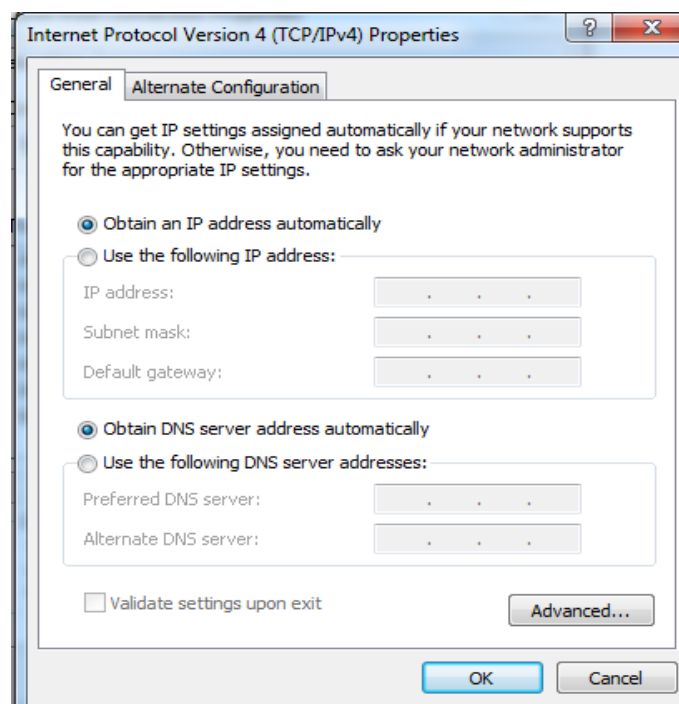
**Step 3: Click Local Area Connection -> Properties.**



**Step 4: Find and double click Internet Protocol Version 4(TCP/IPv4).**



**Step 5:** Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.



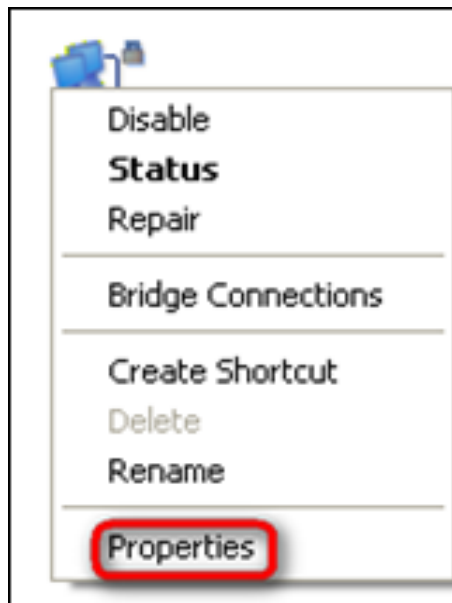
**Step 6:** Click **OK** on the **Local Area Connection Properties** window (see **Step 4** for the screenshot).

## Windows XP

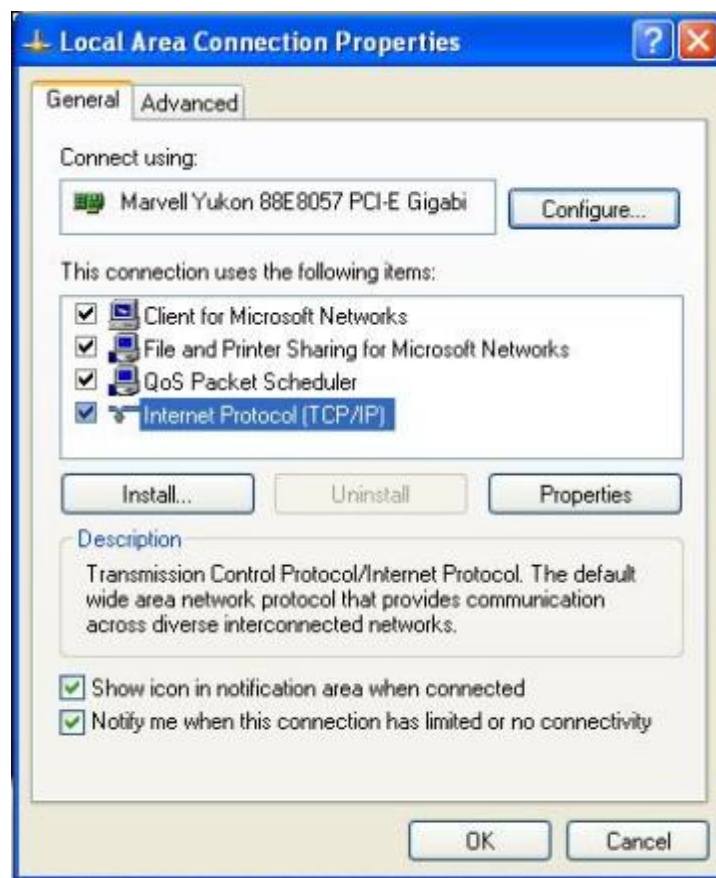
**Step 1:** Right click **My Network Places** on your desktop and select **Properties**.



**Step 2:** Right click **Local Area Connection** and select **Properties**.

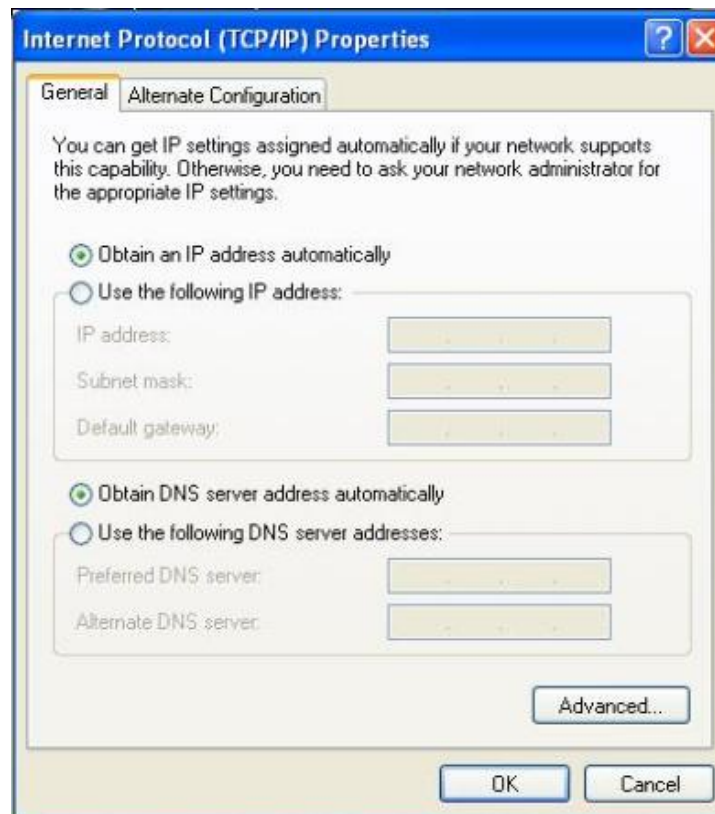


**Step 3:** Scroll down to find and double click **Internet Protocol (TCP/IP)**.





**Step 4:** Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.



**Step 5:** Click **OK** on the **Local Area Connection Properties** window (see **Step 3** for the screenshot).



## 2 Join Your Wireless Network



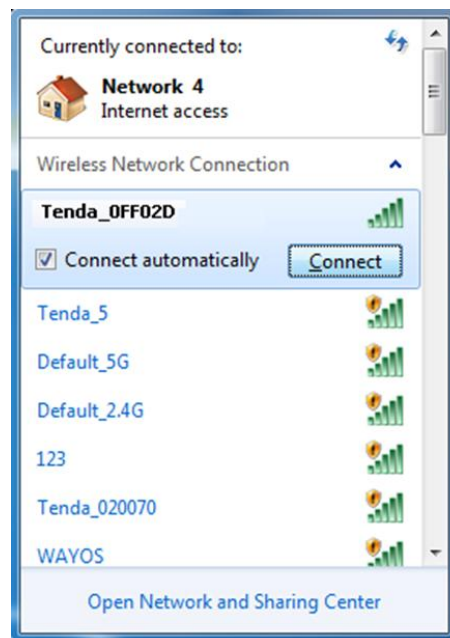
### Tip

- ① To join your wireless network, the PC you use must have an installed wireless network adapter. If not, install one.
  - ② The device's SSID is "Tenda\_XXXXXX" by default (where "XXXXXX" is the last six characters of its MAC address). You can find the MAC address and/or SSID on the label attached to the device's bottom).
- 

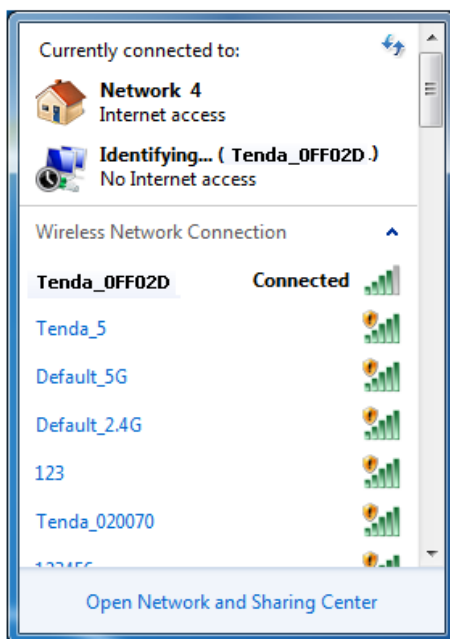
### Windows 7

**Step 1:** Click  or  from the right bottom of your desktop.

**Step 2:** Double click the name of the wireless network (SSID) you wish to join and then follow onscreen instructions.



When **Connected** appears next to the selected wireless network (SSID), you have successfully connected to it.

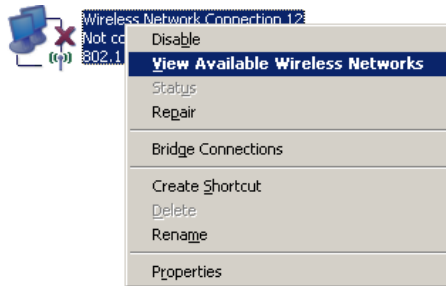


## Windows XP

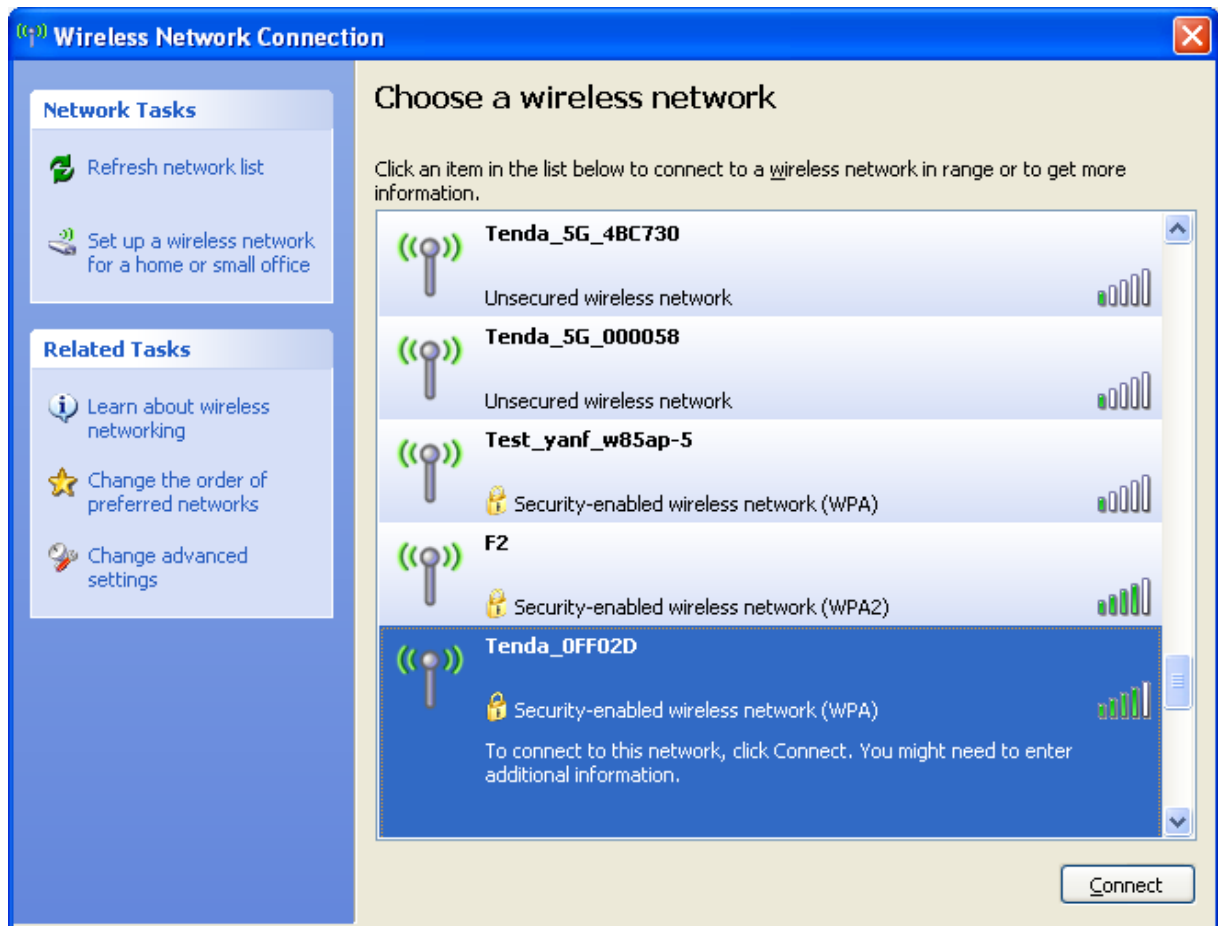
**Step 1:** Right click **My Network Places** and select **Properties**.



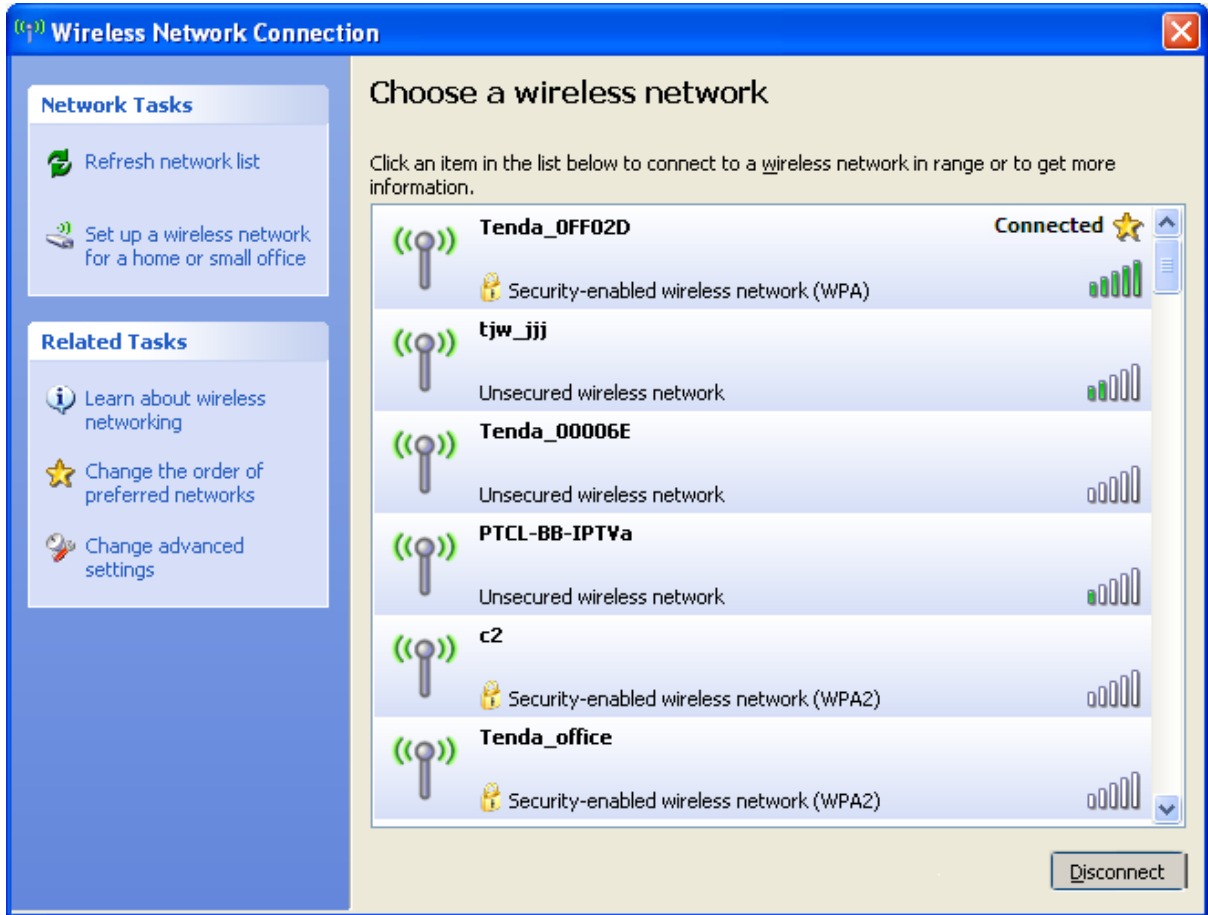
**Step 2:** Right click **Wireless Network Connection** and select **View Available Wireless Networks**.



**Step 3:** Double click the name of the wireless network (SSID) you wish to join and then follow onscreen instructions.



When **Connected** appears next to the selected wireless network (SSID), you have successfully connected to it.



## 3 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](http://www.tendacn.com) to find a solution or email your problems to: [support@tenda.com.cn](mailto:support@tenda.com.cn) or [support02@tenda.com.cn](mailto:support02@tenda.com.cn). We will be more than happy to help you out as soon as possible.

### 1. Q: I cannot access the device's management interface. What should I do?

- Make sure the **PWR** (power) LED on the device is on and the **SYS** LED blinks normally.
- Make sure all cables are correctly connected and the corresponding **LAN** LED on the device is on.
- Verify that your PC's TCP/IP settings are configured correctly. If you select the "Use the following IP address" option, set your PC's IP address to any IP address between 192.168.0.2~192.168.0.254. Or you can select the "Obtain an IP address automatically" option.
- Delete your browser cache and cookies or use a new browser. Make sure you enter 192.168.0.1 in your browser's address bar.
- Open your browser and click **Tools -> Internet Options -> Connections -> LAN Settings**, uncheck the **Use a proxy server for your LAN** option.
- Press the **WPS/Reset** button for over 6 seconds to restore your device to factory default settings. Then log in to your device again.

### 2. Q: I changed the login password and unfortunately forget it. What should I do?

Press the **WPS/Reset** button for over 6 seconds to restore your device to factory default settings.

### 3. Q: My computer shows an IP address conflict error when it connects to the

**device. What should I do?**

- Make sure there are no other DHCP servers on your LAN or other DHCP servers are disabled.
- Make sure the device's LAN IP is not used by other devices on your LAN. The device's default LAN IP address is 192.168.0.1.
- Make sure the statically assigned IP addresses to the PC(s) on LAN are not used by others device(s).

**4. Q: I cannot access email and the Internet/Some Websites do not open. What should I do?**

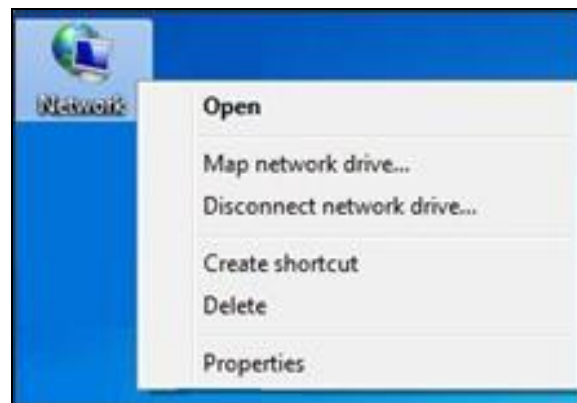
This problem mainly happens to users who use the PPPoE or Dynamic IP Internet connection type. You need to change the MTU size. Try changing the MTU to 1450 or 1400. If this does not help, gradually reduce the MTU from the maximum value until the problem disappears. For details, see [\*\*WAN MTU Setup\*\*](#).

## 4 Remove Wireless Network from Your PC

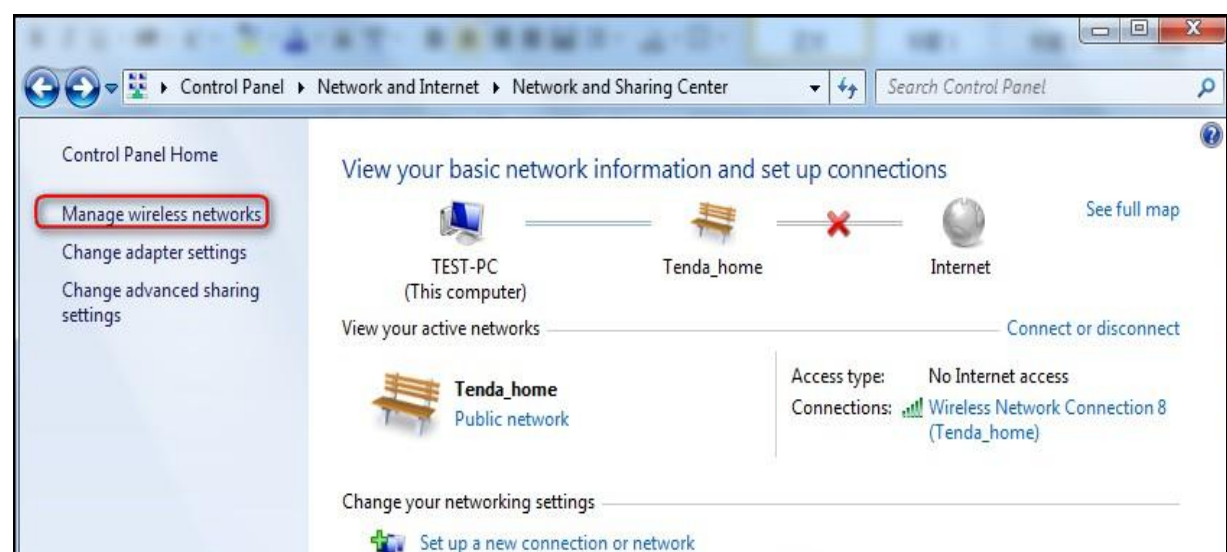
When you change your wireless network (For example, change your device's SSID or security key), the old wireless settings on your PC will not be updated accordingly, you must manually remove them from your PC; otherwise, you may not be able to wirelessly connect to the device. This section explains how to remove a wireless network from your PC.

### Windows 7

- 1 Right-click the **Network** icon and select **Properties**.

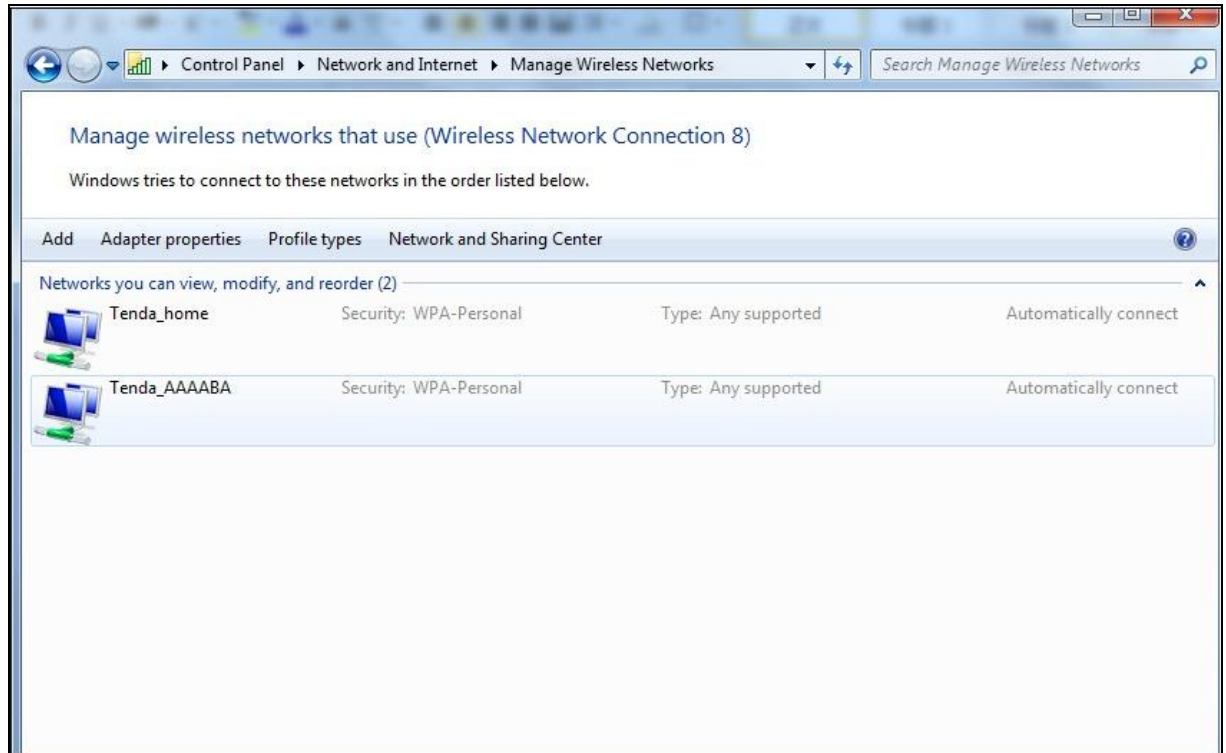


- 2 Select **Manage Wireless Networks**.



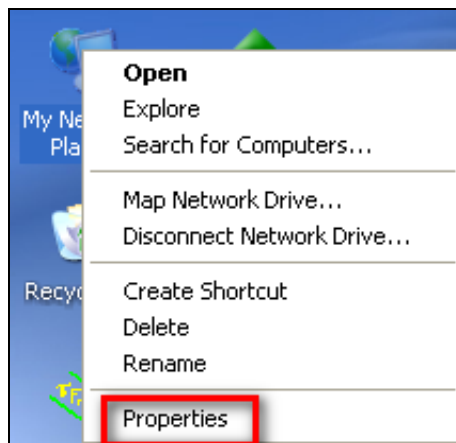
- 3 Select the wireless network and click **Remove network**.



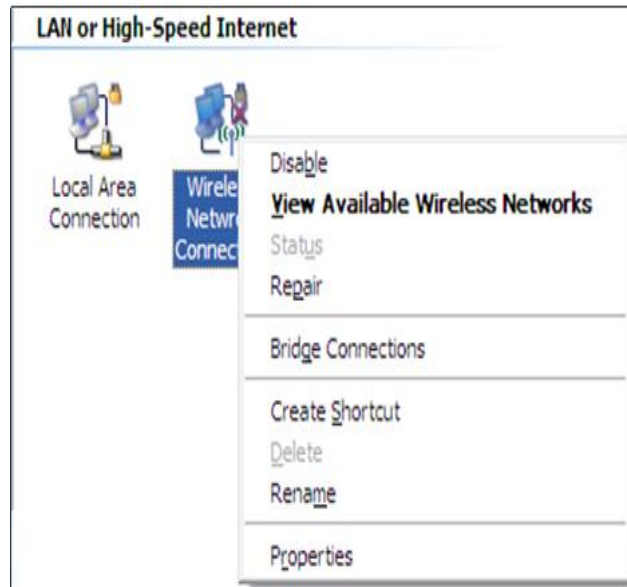


## Windows XP

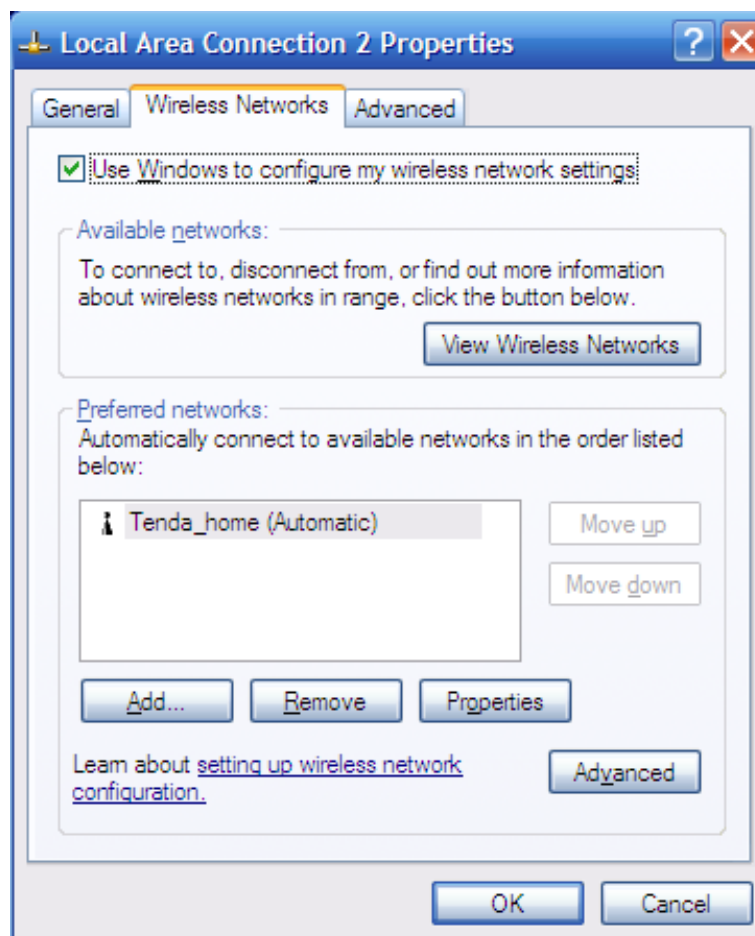
- 1 Right-click **My Network Places** and select **Properties**.



- 2 Right click **Wireless Network Connection** and then select **Properties**.



- Click **Wireless Networks**, select the wireless network name under **Preferred networks** and then click the **Remove** button.



## 5 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 RJ-45 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 RJ-45 cable.

### **NCC Notice**

經型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、加大功率或變更設計之特性及功能。

低功率射頻電機之作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得繼續使用。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。