Tenda

W6-S Wireless In-Wall Access Point

User Guide

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 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 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 a warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda! Please read this user guide before you start with W6-S.

Conventions

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	**System** > **Live Users**
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX:XX:XX:XX:XX:XX*
UI control	Bold	On the **Policy** page, click the **OK** button.
Message	“ ”	The “Success” message appears.

The symbols that may be found in this document are defined as follows.

Symbol	Meaning
NOTE	This symbol 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 symbol is used to highlight a procedure that will save time or resources.

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
AP	Access Point
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMZ	Demilitarized Zone
DNS	Domain Name System
IPTV	Internet Protocol Television
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
MPPE	Microsoft Point-to-Point Encryption
PPP	Point To Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet

Acronym or Abbreviation	Full Spelling
PPTP	Point to Point Tunneling Protocol
SSID	Service Set Identifier
STB	Set Top Box
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WISP	Wireless Internet Service Provider
WPS	WiFi Protected Setup

Additional Information

For more information, search this product model on our website at http://www.tendacn.com.

Technical Support

If you need more help, contact us by any of the following means. We will be glad to assist you as soon as possible.

Hotline	Global: (86) 755-27657180	Email	support@tenda.cn
	United States: 1-800-570-5892		
	Canada: 1-888-998-8966		
	Hong Kong: 00852-81931998		
	Australia: 1300787922		
	New Zealand: 800787922		
Website	http://www.tendacn.com	Skype	tendasz

Contents

1 Get to Know Your Device

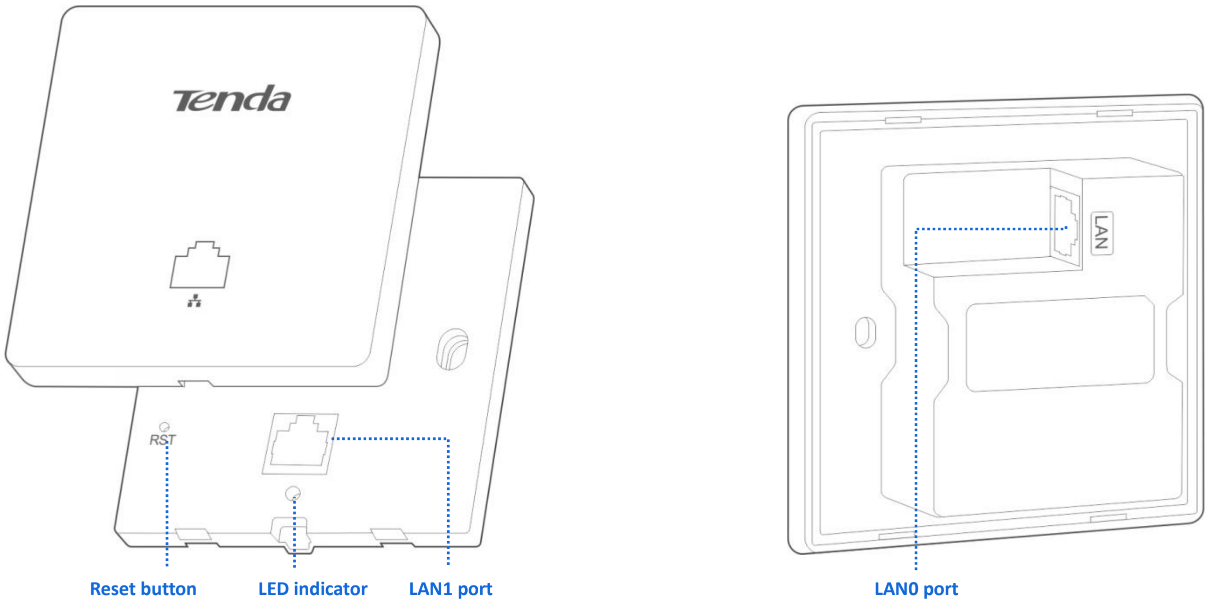
1.1 Overview

Tenda wireless in-wall access point offers a wireless transmission rate of up to 300 Mbps. It can be powered by an 802.3af PoE switch. Adopting a design adaptable to an 86 type wall mount junction box, it can blend into the interiors of villas, large apartments and hotels and provide perfect wireless connection.

1.2 Appearance

This section describes the button, LED indicator, ports, and label of the AP.

1.2.1 Button, LED Indicator, and Ports



Reset Button

It is visible after the front cover of the AP is removed. After the AP is powered on, you can use a paper clip to hold down this button for 8 seconds to restore the factory settings.

LED Indicator

LED Indicator	Blinking: The AP is working properly.
	Off: The AP is not powered on, the indicator has been turned off, or the AP is faulty.

LAN1 Port

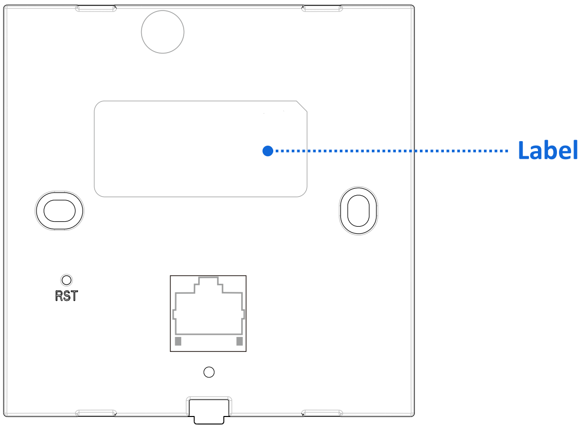
Located on the front of the AP, this port is connected to a computer or switch for exchanging data in 10/100 Mbps auto-negotiation mode.

LAN0 Port

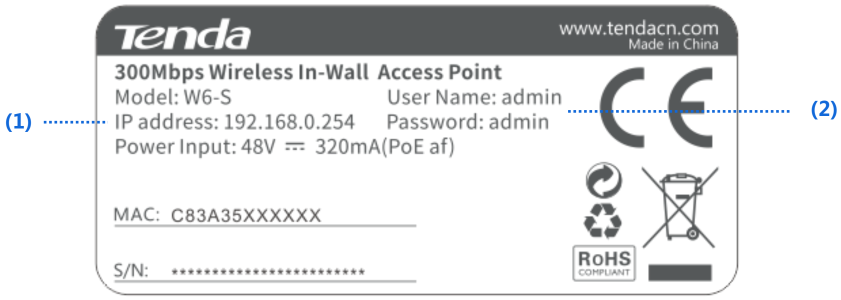
It is located on the back of the AP for supplying power to the AP through PoE and exchanging data in 10/100 Mbps auto-negotiation mode. Connect this port using an Ethernet cable to an IEEE 802.3af PoE switch or PoE power supply equipment to supply power to the AP.

1.2.2 Label

It is visible after the front cover of the AP is removed. The following figure shows its position.



The label is described as follows:



Tenda www.tendacn.com
Made in China

300Mbps Wireless In-Wall Access Point
Model: W6-S User Name: admin
IP address: 192.168.0.254 Password: admin
Power Input: 48V ⎓ 320mA(PoE af)

MAC: C83A35XXXXXX

S/N: ************************

RoHS COMPLIANT

- (1): Default IP address of the AP. You can use this IP address to log in to the web UI of the AP.
- (2): Default user name and password of the web UI of the AP.

2 Application Scenarios

2.1 Large Apartment or Villa

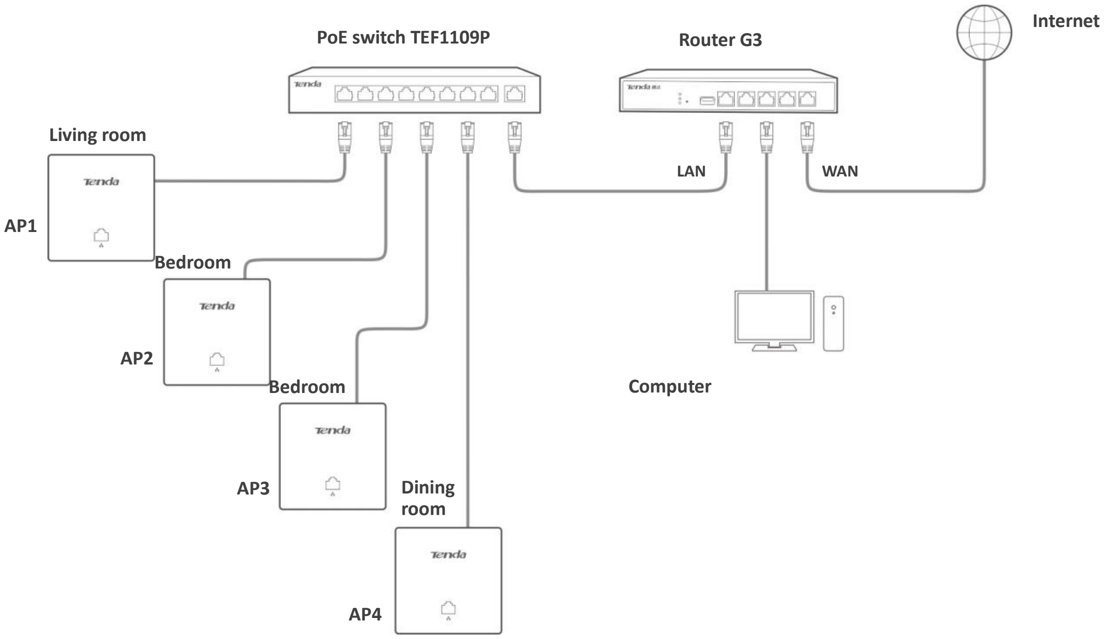
2.1.1 Deploying the AP with a Tenda Router That Includes the AP Controller Functionality

For a large apartment or villa, you are recommended to adopt the Tenda wireless product suite, which includes a wired router (such as G3), a PoE switch (such as TEF1109P), and 4 to 8 W6-S. Deploy one W6-S in each room and place the router and switch in an electronic junction box.

Perform the following procedure:

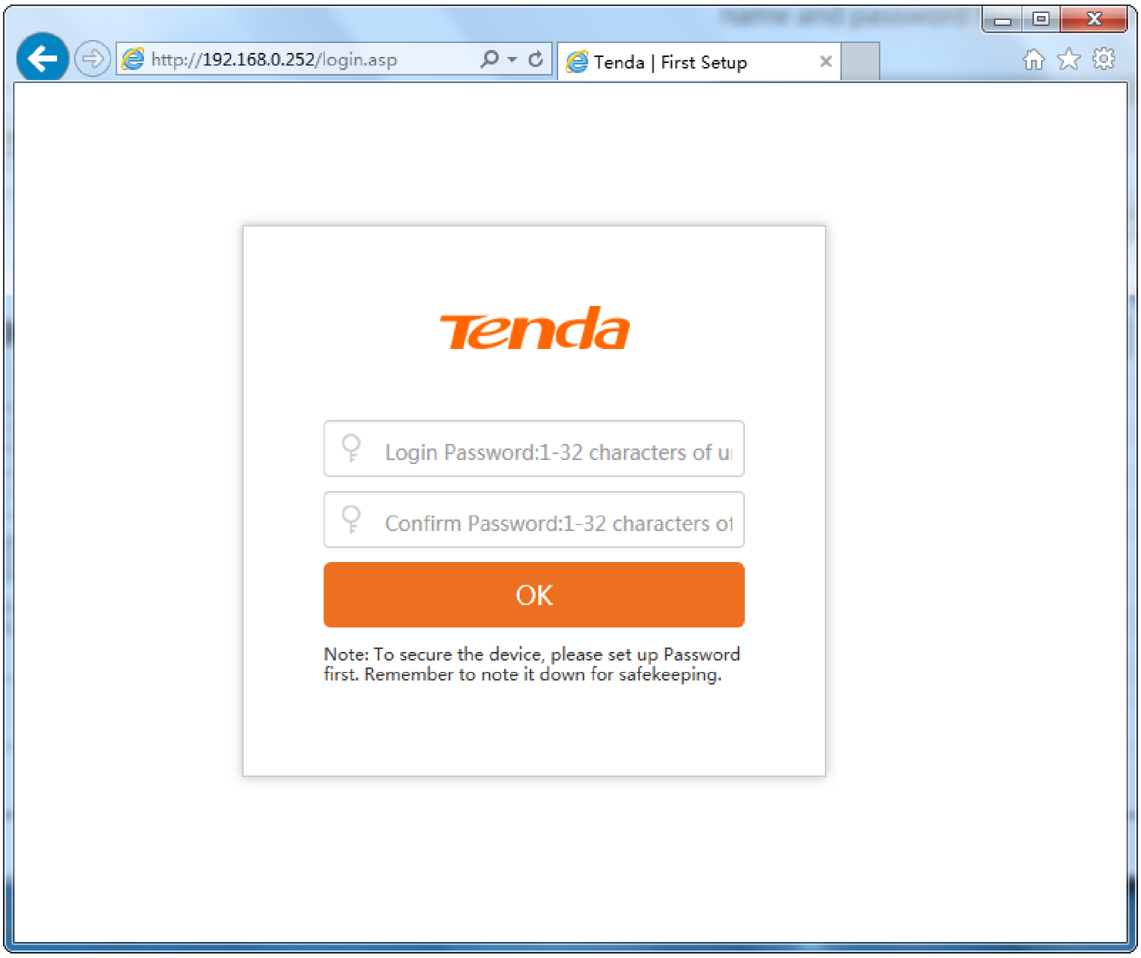
Step 1 Connect the devices.

Connect the WAN port of the router to the ADSL or optical modem. Connect a LAN port of the router to the Uplink port of the PoE switch. Connect the LAN0 port of each AP to a PoE port of the switch using the in-wall Category 5 UTP cable led into each 86 type wall mount junction box used to mount the APs. Connect a computer for configuring the AP to the LAN port of the router. See the following figure.



Step 2 Log in to the web UI of the router.

Start a web browser, enter the management IP address of the router (default: 192.168.0.252), and press **Enter**. Set your password on the page that appears, and click **OK** to access the home page of the web UI.



http://192.168.0.252/login.asp

Tenda | First Setup

Login Password:1-32 characters of u

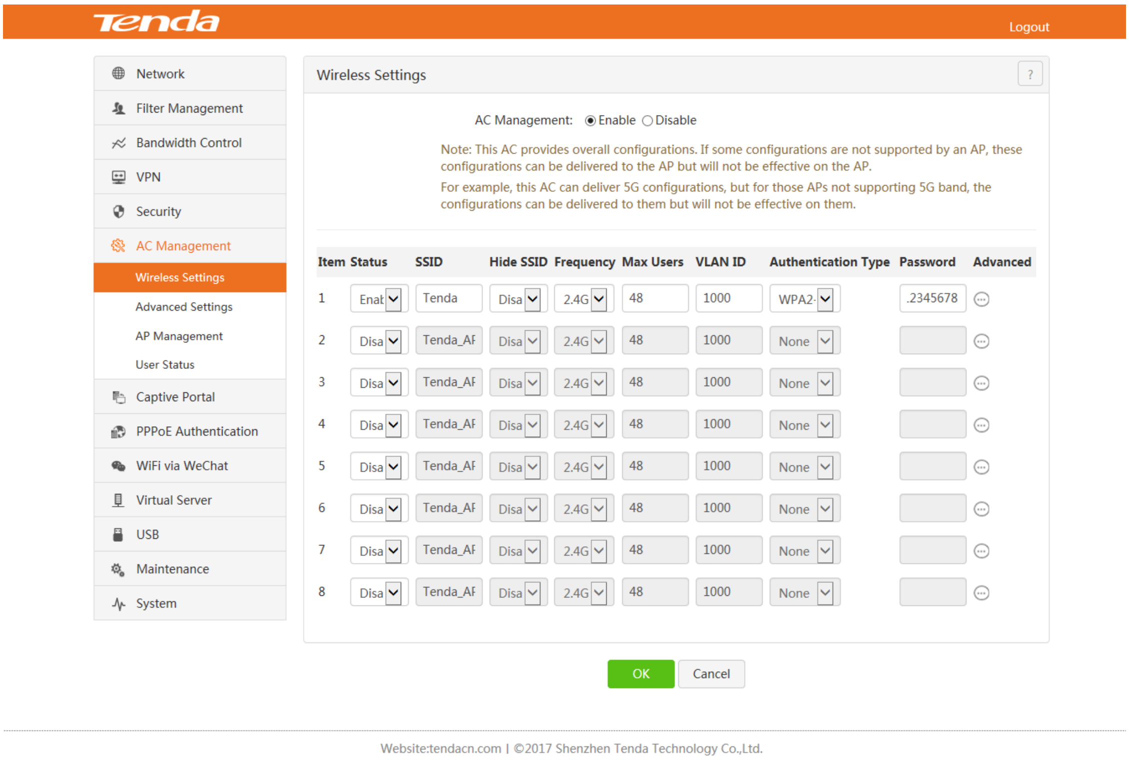
Confirm Password:1-32 characters o

OK

Note: To secure the device, please set up Password first. Remember to note it down for safekeeping.

Step 3 Configure the APs.

Choose **AC Management** > **Wireless Settings**, select **Enable** to enable the AP management function. In the first rule, change the **SSID** value to your network wireless name (such as **Tenda**), select an authentication type (such as **WPA2-PSK**), and set a wireless network password (such as **12345678**). Click **OK** to save the settings. For details about how to configure the AP on the router web UI, refer to the user guide for the router. The user guide is available at http://www.tendacn.com.



Wireless Settings

AC Management: ● Enable ○ Disable

Note: This AC provides overall configurations. If some configurations are not supported by an AP, these configurations can be delivered to the AP but will not be effective on the AP.

For example, this AC can deliver 5G configurations, but for those APs not supporting 5G band, the configurations can be delivered to them but will not be effective on them.

Item	Status	SSID	Hide SSID	Frequency	Max Users	VLAN ID	Authentication Type	Password	Advanced
1	Enat	Tenda	Disa	2.4G	48	1000	WPA2-	.2345678	⋯
2	Disa	Tenda_AF	Disa	2.4G	48	1000	None		⋯
3	Disa	Tenda_AF	Disa	2.4G	48	1000	None		⋯
4	Disa	Tenda_AF	Disa	2.4G	48	1000	None		⋯
5	Disa	Tenda_AF	Disa	2.4G	48	1000	None		⋯
6	Disa	Tenda_AF	Disa	2.4G	48	1000	None		⋯
7	Disa	Tenda_AF	Disa	2.4G	48	1000	None		⋯
8	Disa	Tenda_AF	Disa	2.4G	48	1000	None		⋯

Website:tendacn.com I ©2017 Shenzhen Tenda Technology Co.,Ltd.

---End

2.1.2 Deploying the AP with Another Brand's Router

This section describes how to deploy the AP with another brand's router.

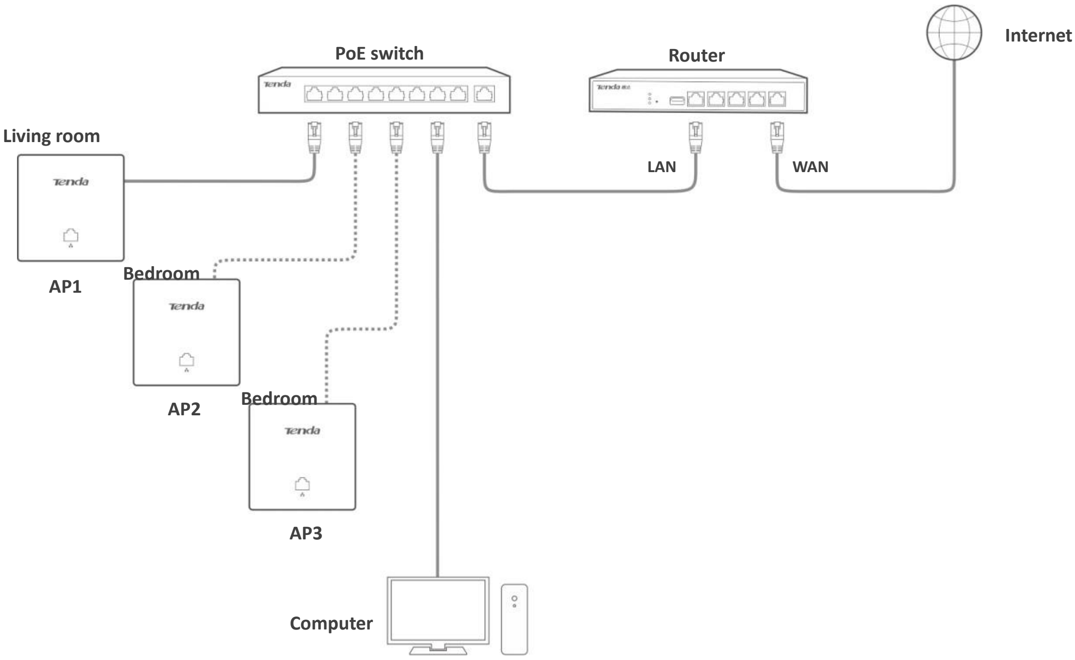
Perform the following procedure:

Step 1 Connect the devices.

See the following figure.

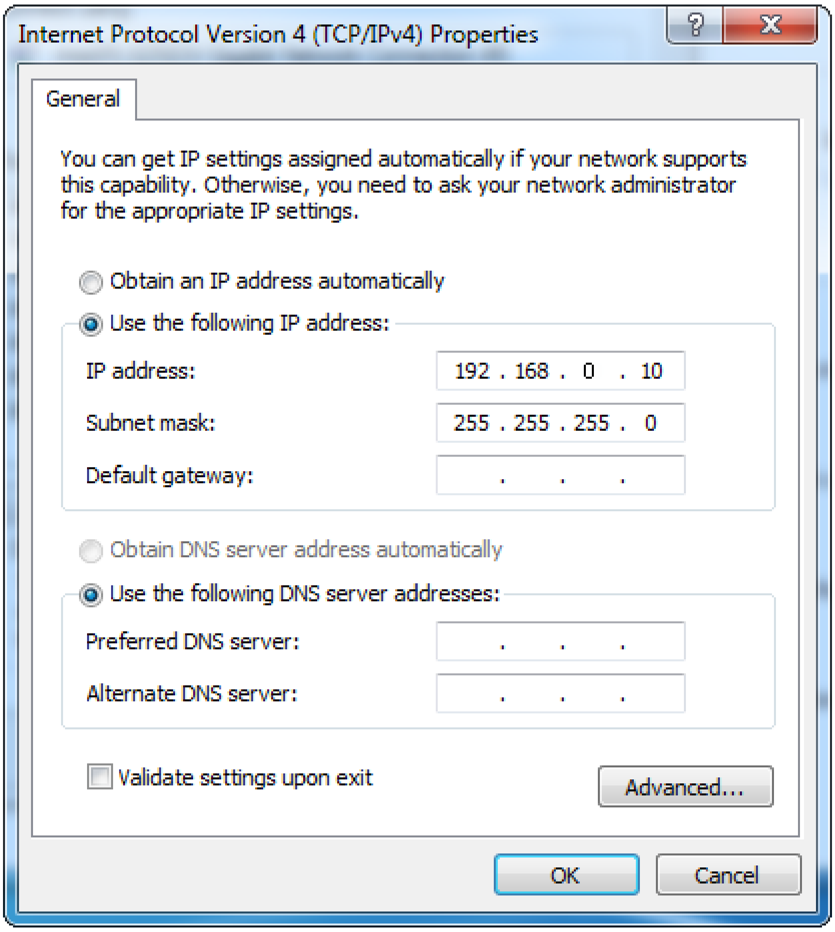
NOTE

Connect one AP to the PoE switch, change the IP address of the AP to prevent IP address conflicts, and configure the AP. Then, repeat this procedure to configure the other APs.



Step 2 Set the IP address of your computer. (Windows 7 is taken as an example to describe the procedure.)

Use an Ethernet cable to connect the computer to the PoE switch. Right-click the network icon in the lower-right corner of the desktop of the computer, and click **Open Network and Sharing Center**, **Local Area Connection**, and then **Properties**. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, select **Use the following IP address**, set **IP address** to **192.168.10.*X*** (*X*: 2 - 253) and **Subnet mask** to **255.255.255.0**, and click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

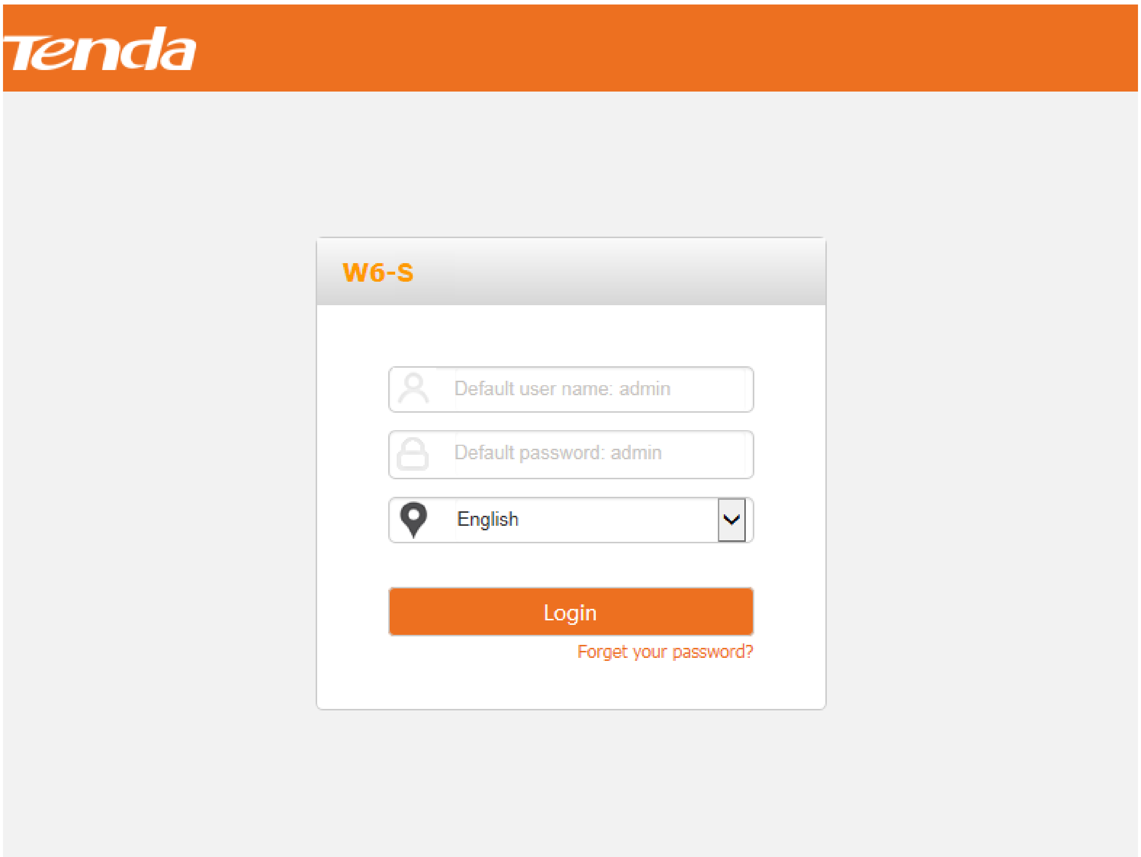
Alternate DNS server: . . .

□ Validate settings upon exit

Step 3 Log in to the web UI of the AP.

Start a web browser, enter the management IP address of the AP (default: 192.168.0.254), and press

Enter. Enter the user name and password of the AP (default user name and password: **admin**) and click **Login**.



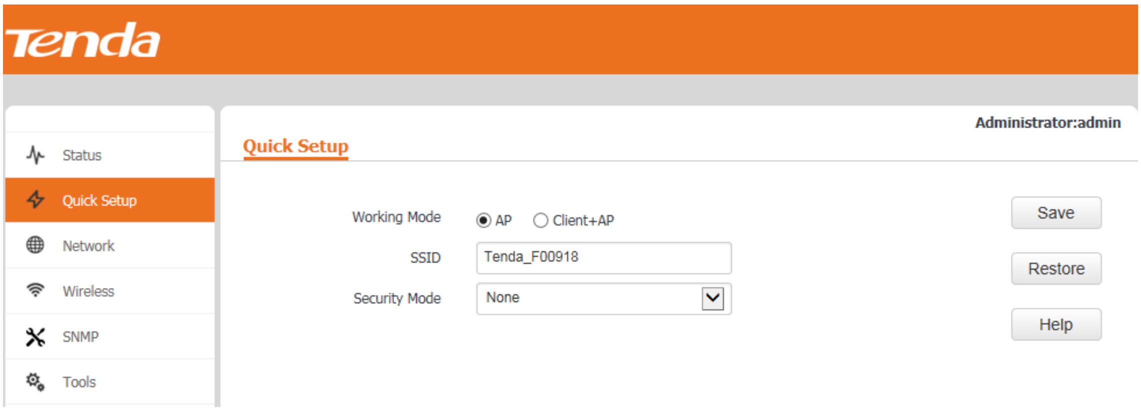
W6-S

Default user name: admin

Default password: admin

English

Step 4 Configure the AP.
Configure the AP on the web UI. For details, refer to section 4 and the sections that follow.



Administrator:admin

Quick Setup

Working Mode ● AP ○ Client+AP

SSID Tenda_F00918

Security Mode None

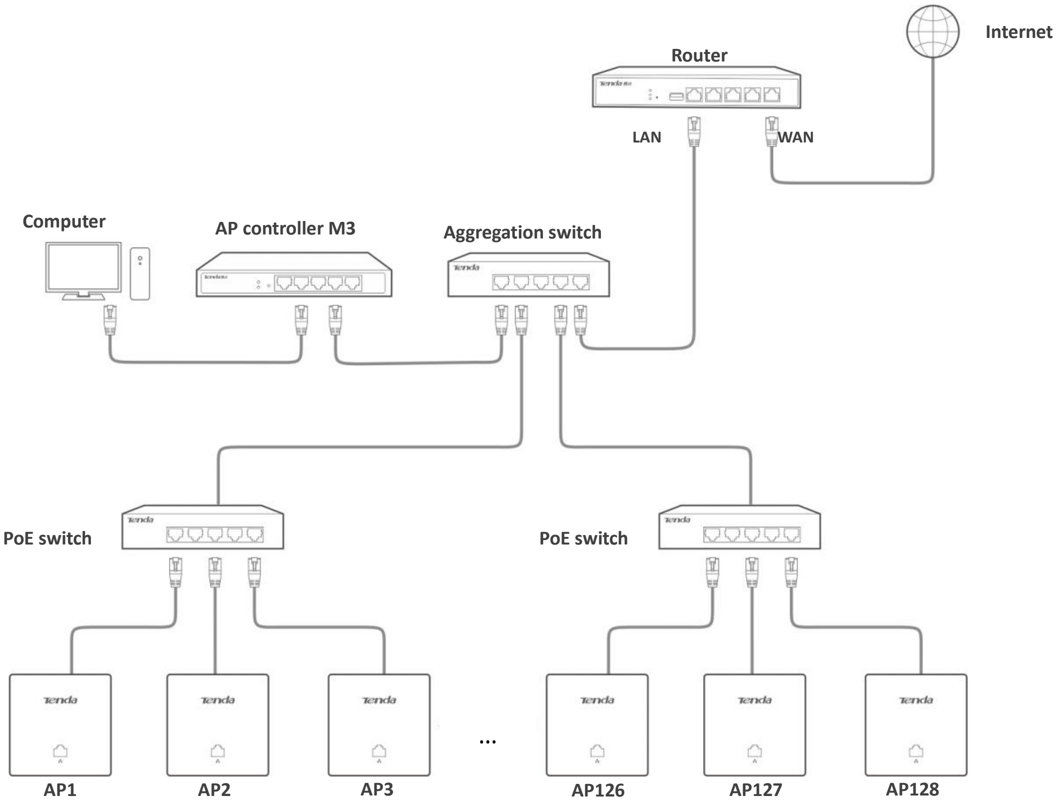
---End

2.2 Hotel

A hotel may be deployed with a large number of APs. You can use Tenda wireless AP controller (such as M3) to configure and manage them centrally and efficiently.

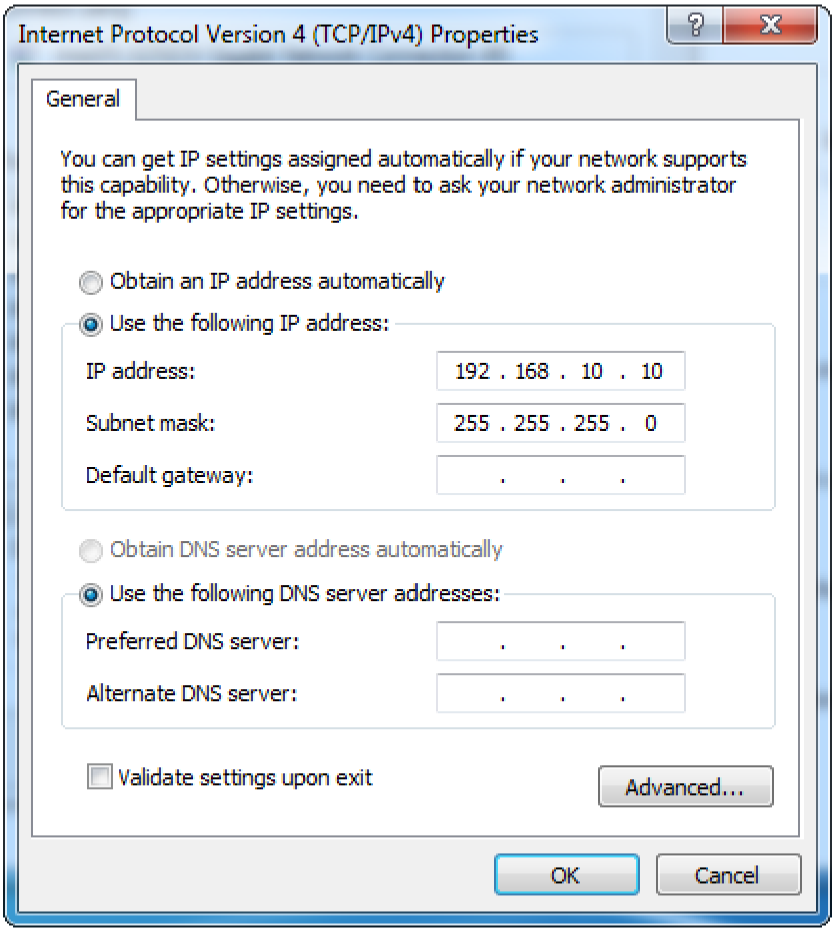
Perform the following procedure:

Step 1 Connect the devices.
See the following figure.



Step 2 Set the IP address of your computer. (Windows 7 is taken as an example to describe the procedure.)

Use an Ethernet cable to connect the computer to the AP controller. Right-click the network icon in the lower-right corner of the desktop of the computer, and click **Open Network and Sharing Center**, **Local Area Connection**, and then **Properties**. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, select **Use the following IP address**, set **IP address** to **192.168.10.*X*** (*X*: 2 - 253) and **Subnet mask** to **255.255.255.0**, and click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 10 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

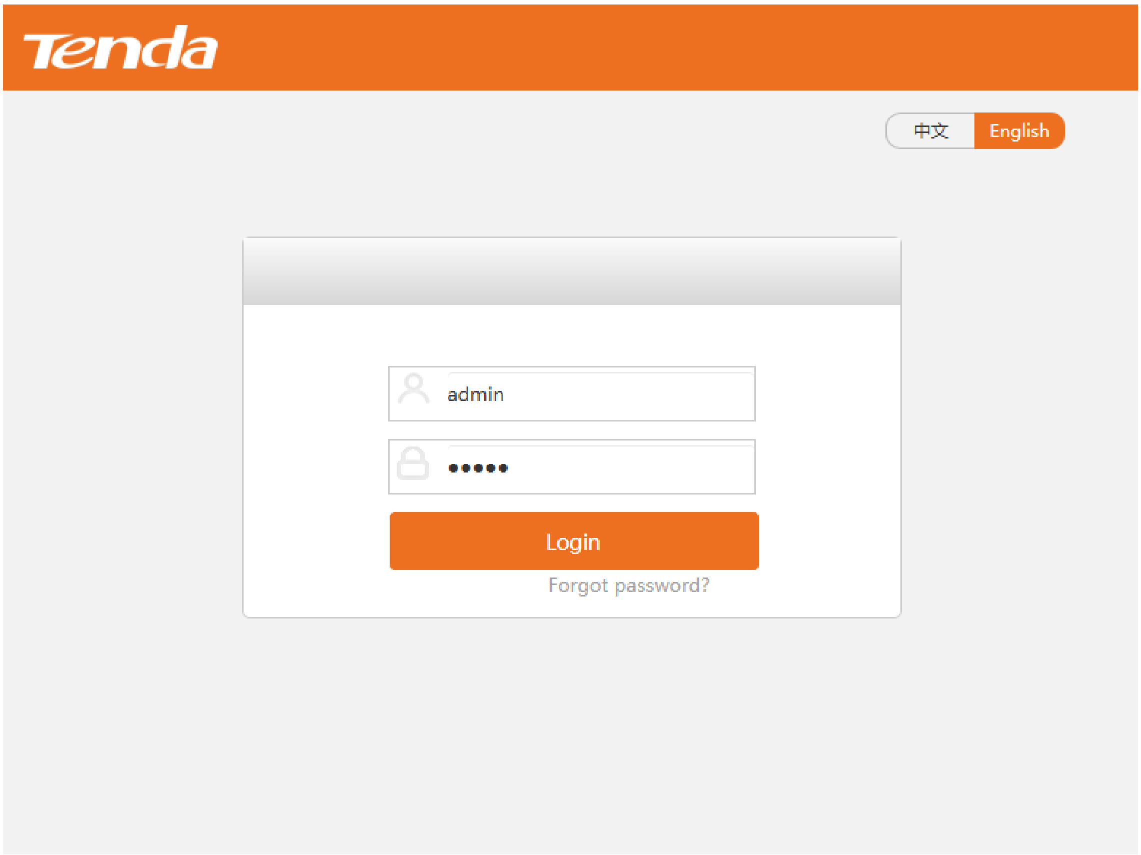
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

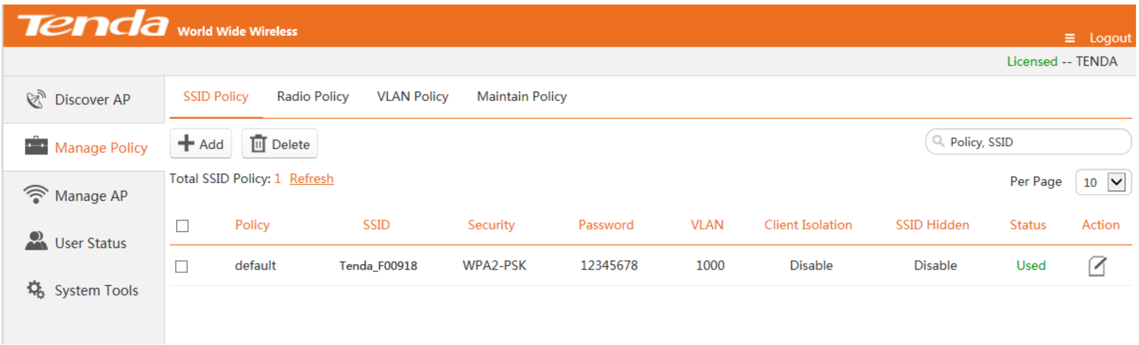
Step 3 Log in to the web UI of the AP controller.

Start a web browser, enter the management IP address of the AP controller (default: 192.168.10.1), and press **Enter**. Enter the user name and password of the AP controller (default user name and password: **admin**) and click **Login**.



Step 4 Configure the APs.

Configure the APs on the web UI of the AP controller. For details about how to configure the AP on the web UI of the AP controller, refer to the user guide for the AP controller. The user guide is available at http://www.tendacn.com.



Total SSID Policy: 1 Refresh

□	Policy	SSID	Security	Password	VLAN	Client Isolation	SSID Hidden	Status	Action
□	default	Tenda_F00918	WPA2-PSK	12345678	1000	Disable	Disable	Used	✎

---End

The following chapters describe how to configure the AP on the web UI of the AP.

3 Login

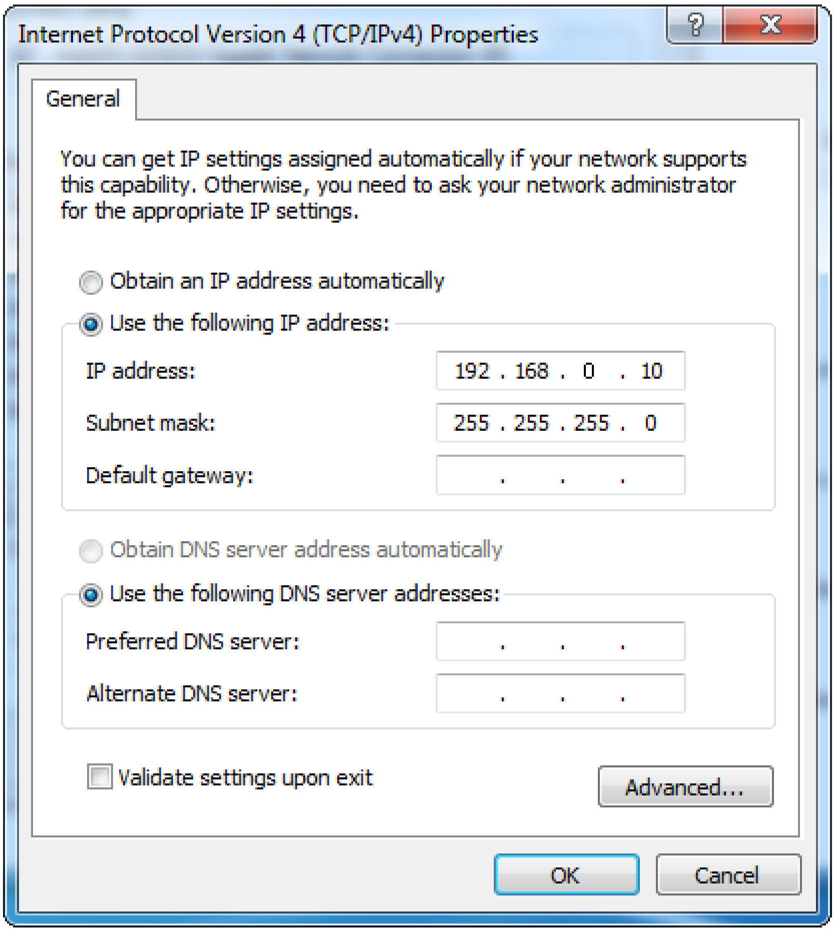
3.1 Logging In to the Web UI of the AP

You can log in to the web UI of the AP using a web browser.

Perform the following procedure:

Step 1 Use an Ethernet cable to connect the management computer to the AP or the switch connected to the AP.

Step 2 Set **IP address** of your local area connection to **192.168.0.*X*** (*X*: 2 - 253) and **Subnet mask** to **255.255.255.0**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

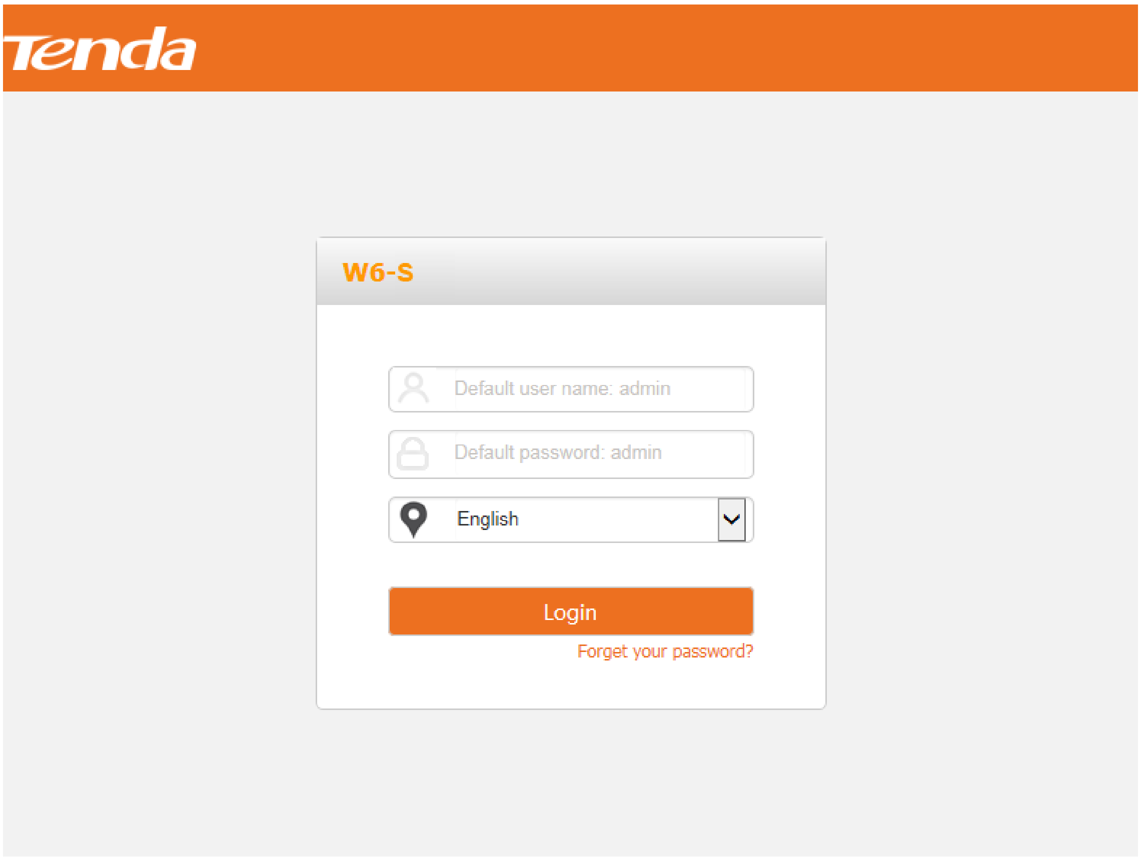
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Step 3 Start a web browser on the computer, enter the management IP address of the AP (default: 192.168.0.254) in the address bar, and press **Enter**.

Step 4 Enter the user name and password of the AP (default user name and password: **admin**) and press **Login**.

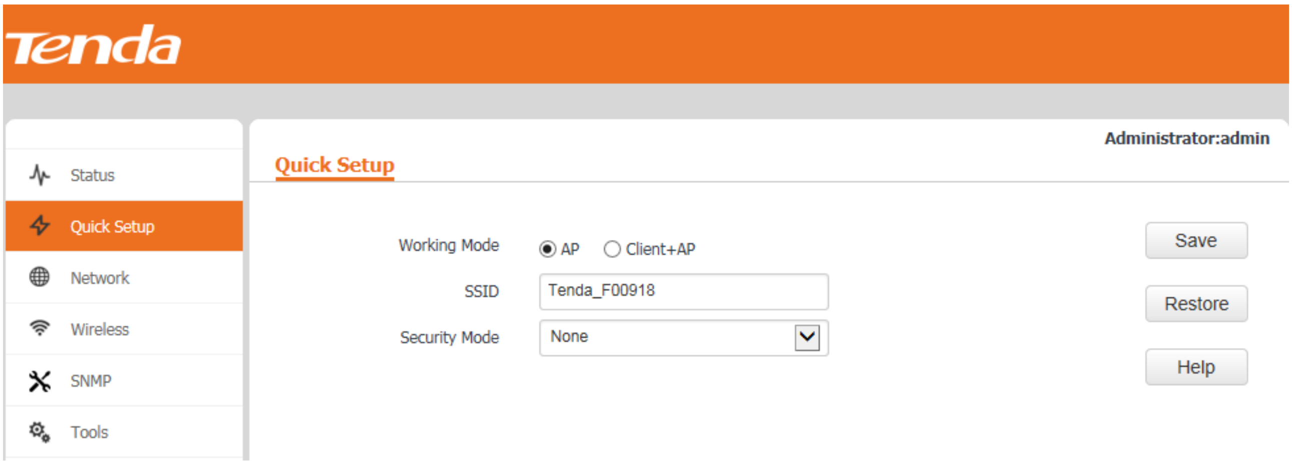


NOTE

If this page is not displayed, refer to Q1 in **FAQ**.

---End

You can now start configuring the AP.



Quick Setup

Working Mode: ● AP ○ Client+AP

SSID: Tenda_F00918

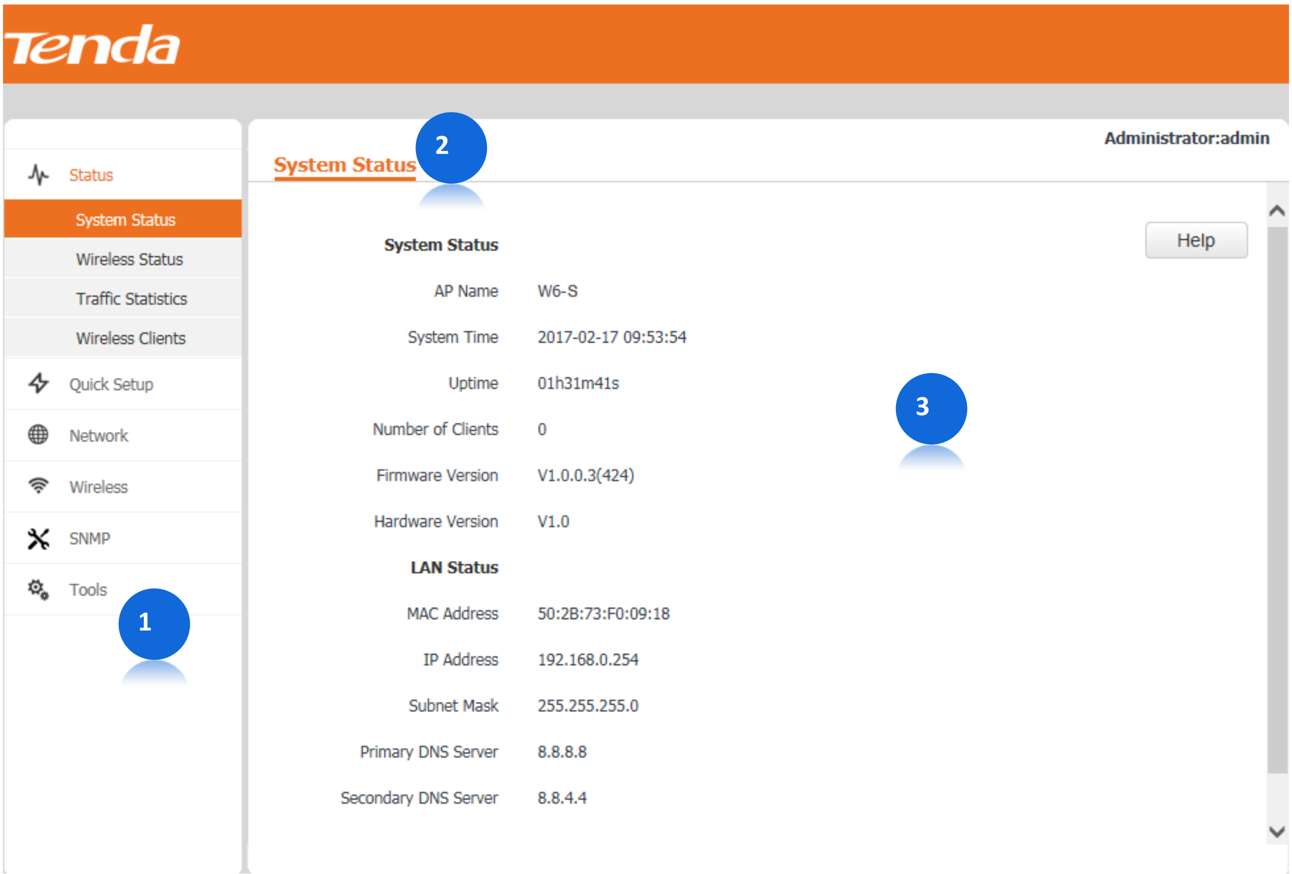
Security Mode: None

3.2 Logging Out of the Web UI of the AP

If you log in to the web UI of the AP and perform no operation within the login timeout interval, the AP logs you out. When you close the web browser, the system logs you out as well.

3.3 Management UI Layout

The web UI of the AP is composed of three parts, including the 2-level navigation tree, tab page area, and configuration area. See the following figure.



System Status

AP Name W6-S

System Time 2017-02-17 09:53:54

Uptime 01h31m41s

Number of Clients 0

Firmware Version V1.0.0.3(424)

Hardware Version V1.0

LAN Status

MAC Address 50:2B:73:F0:09:18

IP Address 192.168.0.254

Subnet Mask 255.255.255.0

Primary DNS Server 8.8.8.8

Secondary DNS Server 8.8.4.4

NOTE

The functions and parameters dimmed on the web UI indicates that they are not supported by the AP or cannot be changed in the current configuration.

Part	Name	Description
①	2-level navigation tree	The navigation tree and tab page area enable you to access functions of the AP.
②	Tab page area	
③	Configuration area	It enables you to view and modify configuration.

3.4 Common Buttons

The following table describes the common buttons available on the web UI of the AP.

Button	Description
Refresh	It is used to update the content of the current page.

Button	Description
Save	It is used to save the configuration on the current page and enable the configuration to take effect.
Restore	It is used to change the current configuration on the current page back to the original configuration.
Help	It is used to view help information corresponding to the settings on the current page.

4 Quick Setup

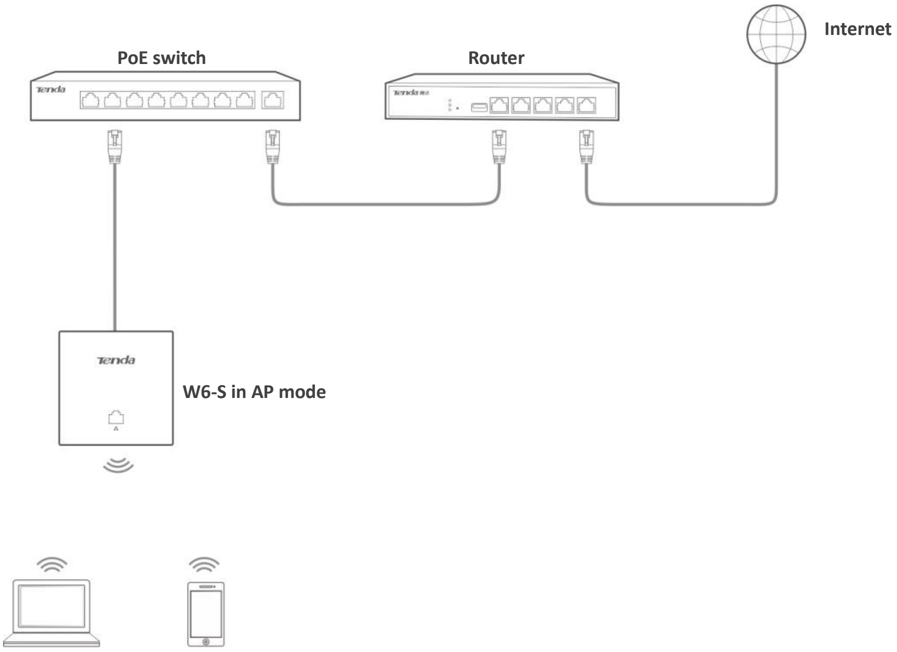
4.1 Overview

This module enables you to quickly configure the AP so that wireless devices such as smart phones and pads can access the internet through the wireless network of the AP.

This AP can work in AP or Client+AP mode.

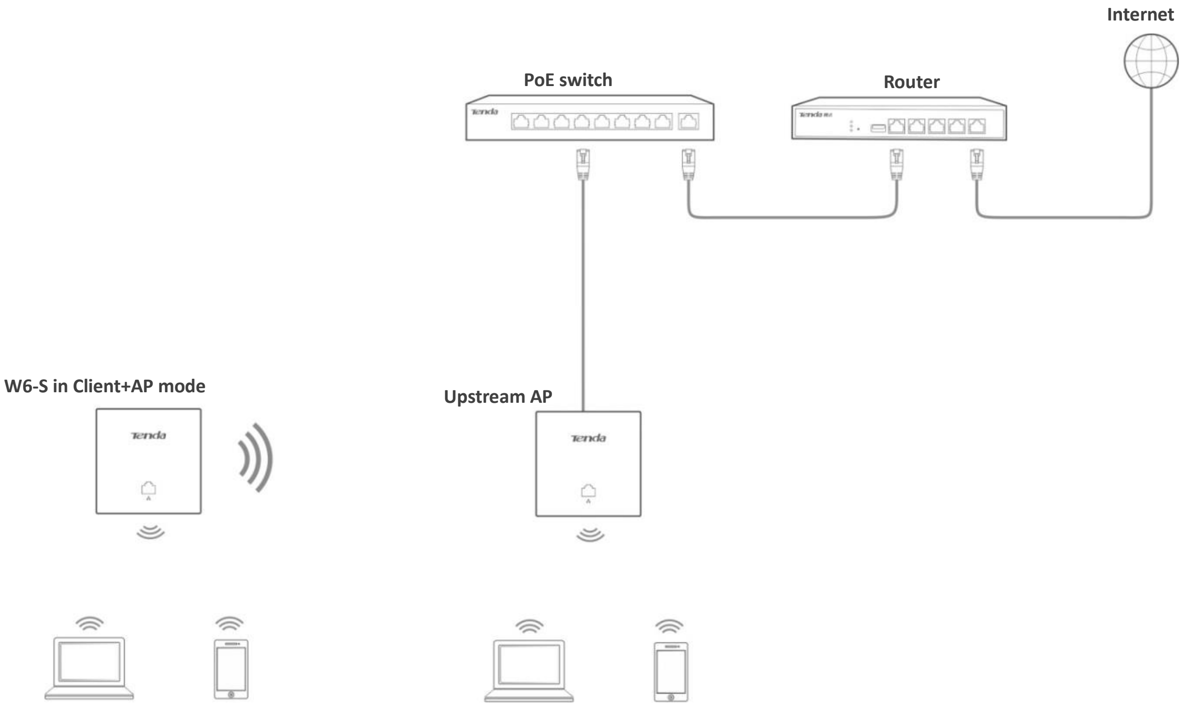
AP Mode

By default, the AP works in this mode. In this mode, the AP connects to the internet using an Ethernet cable and converts wired signals into wireless signals to provide wireless network coverage. See the following topology.



Client+AP Mode

In this mode, the AP is wirelessly bridged to an upstream device (such as a wireless router or AP) to extend the wireless network coverage of the upstream device. See the following topology.



4.2 Setup Procedures

4.2.1 AP Mode

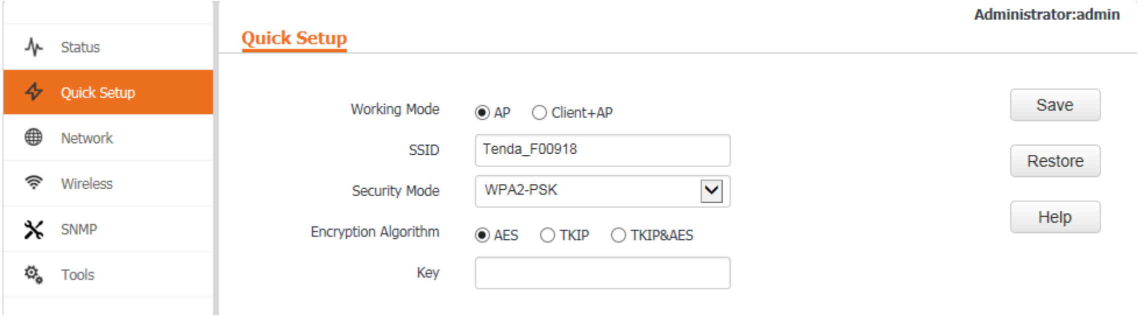
Step 1 Choose **Quick Setup**.

Step 2 Set **Working Mode** to **AP**.

Step 3 (Optional) Change the value of **SSID**, which indicates the primary SSID of the AP, to your wireless network name.

Step 4 Select a security mode from the **Security Mode** drop-down list box and set the corresponding parameters. (You are recommended to set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.)

Step 5 Click **Save**.



Quick Setup

Working Mode ● AP ○ Client+AP

SSID Tenda_F00918

Security Mode WPA2-PSK

Encryption Algorithm ● AES ○ TKIP ○ TKIP&AES

Key

---End

Parameter description

Parameter	Description
Working Mode	It specifies the working mode of the AP.
SSID	It specifies the primary SSID (wireless network name) of the AP.

Parameter	Description
Security Mode	It specifies the security mode of the wireless network of the AP. The options include: None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2.

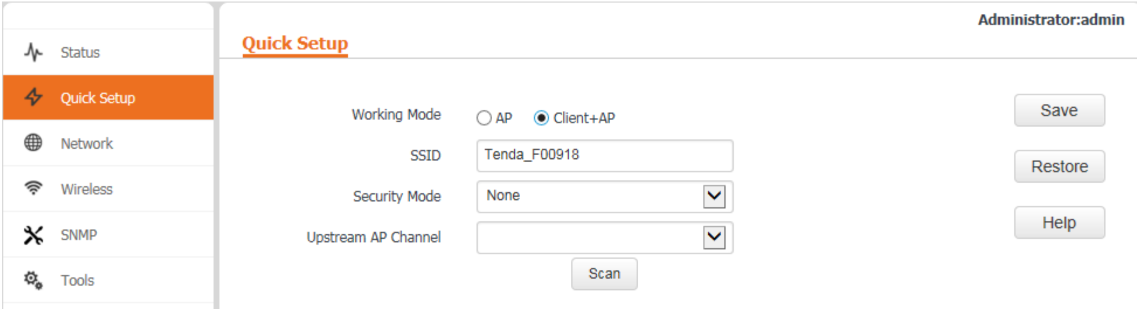
After the configuration, you can select the SSID on your wireless devices such as smart phones and enter your wireless network password to connect to the wireless network of the AP and access the internet through the AP.

4.2.2 Client+AP Mode

Step 1 Choose **Quick Setup**.

Step 2 Set **Working Mode** to **Client+AP**.

Step 3 Click **Scan**.



Working Mode ○ AP ● Client+AP

SSID: Tenda_F00918

Security Mode: None

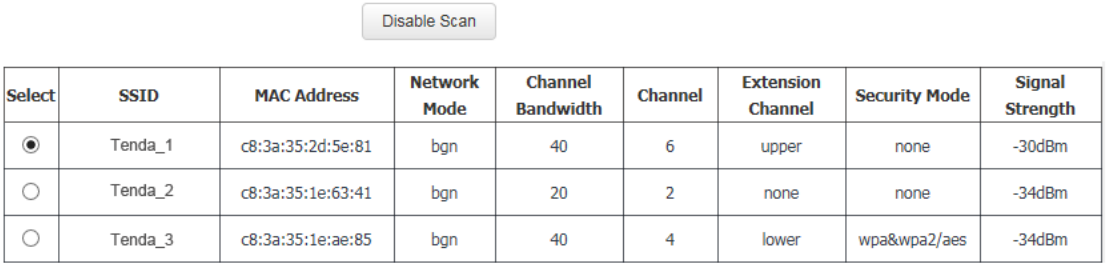
Upstream AP Channel:

Step 4 Select the wireless network to be extended from the wireless network list that appears.

NOTE

- If no wireless network is found, choose **Wireless** > **RF**, ensure that **Enable RF** is selected, and try scanning wireless network again.
- After a wireless network to be extended is selected, the AP identifies the SSID, security mode, and channel of the wireless network and enters them on the page. The other parameters including **Key**, **RADIUS Server IP**, **RADIUS Port**, and **RADIUS Password** must be entered manually.

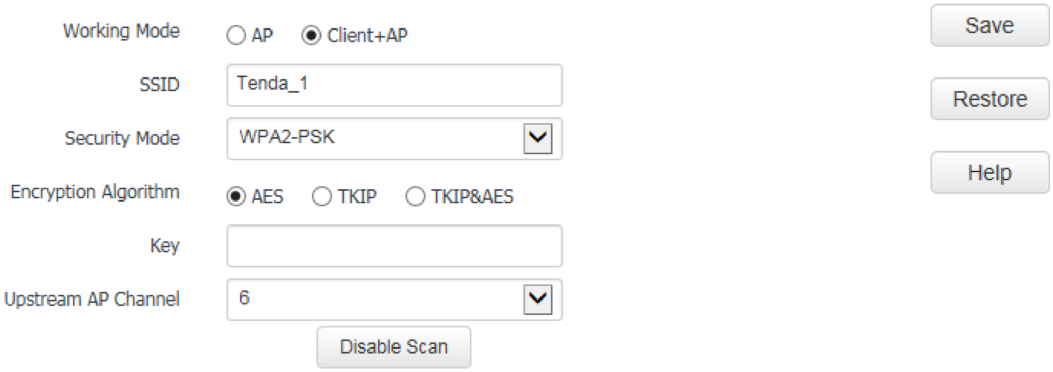
Step 5 Click **Disable Scan**.



Select	SSID	MAC Address	Network Mode	Channel Bandwidth	Channel	Extension Channel	Security Mode	Signal Strength
●	Tenda_1	c8:3a:35:2d:5e:81	bgn	40	6	upper	none	-30dBm
○	Tenda_2	c8:3a:35:1e:63:41	bgn	20	2	none	none	-34dBm
○	Tenda_3	c8:3a:35:1e:ae:85	bgn	40	4	lower	wpa&wpa2/aes	-34dBm

Step 6 If the wireless network of the upstream device is encrypted, set **Key** to the wireless network password of the device or set **RADIUS Server IP**, **RADIUS Port**, and **RADIUS Password** to the IP address, port number, and password of the RADIUS server.

Step 7 Click **Save**.



Working Mode ○ AP ● Client+AP

SSID Tenda_1

Security Mode WPA2-PSK

Encryption Algorithm ● AES ○ TKIP ○ TKIP&AES

Key

Upstream AP Channel 6

---End

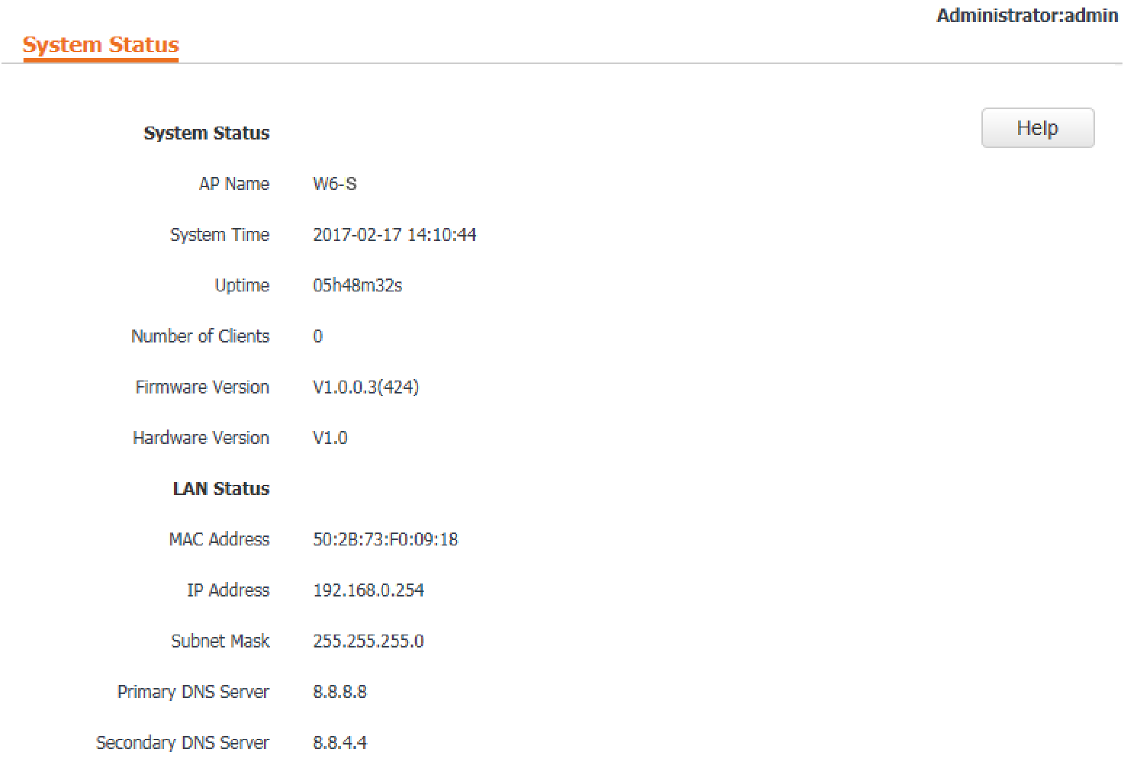
After the configuration, you can select the SSID on your wireless devices such as smart phones and enter your wireless network password to connect to the wireless network of the AP and access the internet through the AP. If you do not know the SSID of the AP, go to the **Wireless** > **Basic** page.

5 Status

5.1 System Status

To access the page, choose **Status** > **System Status**.

The page displays the system and LAN port status of the AP.



System Status

AP Name	W6-S
System Time	2017-02-17 14:10:44
Uptime	05h48m32s
Number of Clients	0
Firmware Version	V1.0.0.3(424)
Hardware Version	V1.0

LAN Status

MAC Address	50:2B:73:F0:09:18
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4

Parameter description

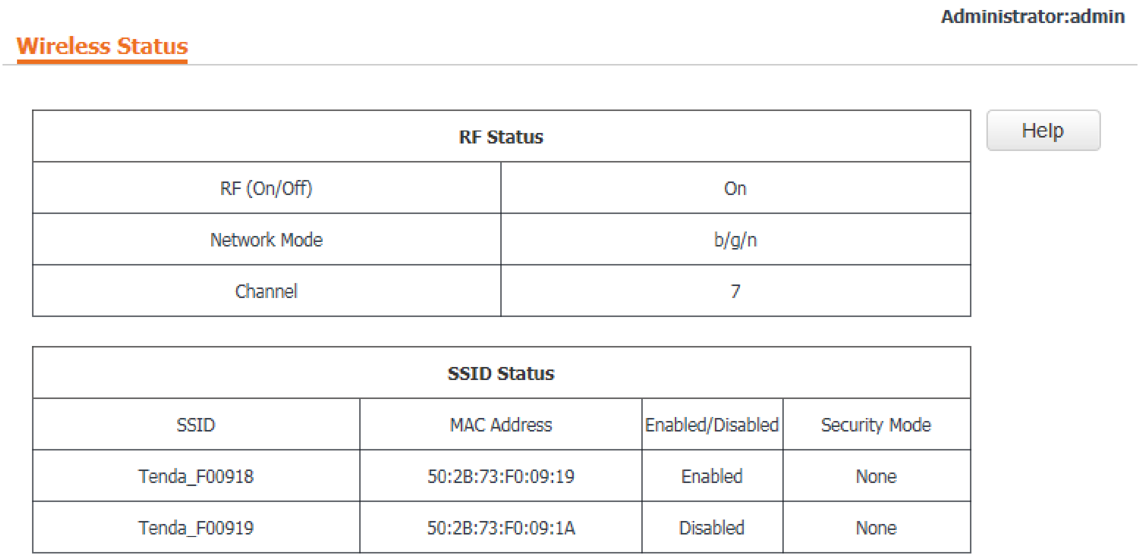
Parameter	Description
AP Name	It specifies the name of the AP. A unique AP name helps quickly identify the AP. You can change the AP name on the **Network** > **LAN Setup** page.
System Time	It specifies the current system time of the AP.
Uptime	It specifies the time that has elapsed since the AP was started last time.
Number of Clients	It specifies the number of wireless clients currently connected to the AP.
Firmware Version	It specifies the firmware version number of the AP.
Hardware Version	It specifies the hardware version number of the AP.
MAC Address	It specifies the physical address of the LAN port of the AP. If you connect the AP to other devices using Ethernet cables, the AP uses this MAC address to communicate with those

Parameter	Description
	devices.
IP Address	It specifies the IP address of the AP. The web UI of the AP is accessible at this IP address. You can change the IP address on the **Network** > **LAN Setup** page.
Subnet Mask	It specifies the subnet mask of the IP address of the AP.
Primary DNS Server and Secondary DNS Server	- **Primary DNS Server**: It specifies the IP address of the primary DNS server of the AP. - **Secondary DNS Server**: It specifies the IP address of the secondary DNS server of the AP.

5.2 Wireless Status

To access the page, choose **Status** > **Wireless Status**.

This page displays general RF settings and SSID status of the AP.



RF Status	
RF (On/Off)	On
Network Mode	b/g/n
Channel	7

SSID Status			
SSID	MAC Address	Enabled/Disabled	Security Mode
Tenda_F00918	50:2B:73:F0:09:19	Enabled	None
Tenda_F00919	50:2B:73:F0:09:1A	Disabled	None

Parameter description

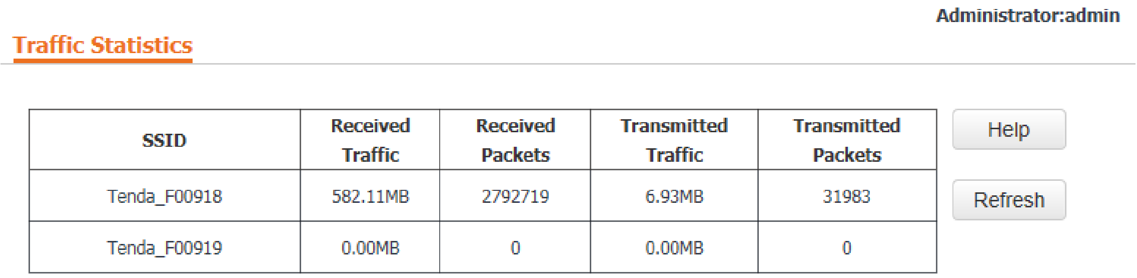
Parameter		Description
RF Status	RF (On/Off)	It specifies whether the wireless function of the AP is enabled.
	Network Mode	It specifies the current network mode of the AP.
	Channel	It specifies the current working channel of the AP.
SSID Status	SSID	It specifies the names of all the wireless networks of the AP.
	MAC Address	It specifies the physical addresses corresponding to the SSIDs of the AP.
	Enabled/Disabled	It specifies the status of the wireless networks corresponding to the SSIDs of the AP.

Parameter		Description
	Security Mode	It specifies the security modes of the wireless networks corresponding to the SSIDs of the AP.

5.3 Traffic Statistics

To access the page, choose **Status** > **Traffic Statistics**.

This page displays the statistics about historical traffic of the wireless networks of the AP. To view the latest statistics, click **Refresh**.



Administrator:admin

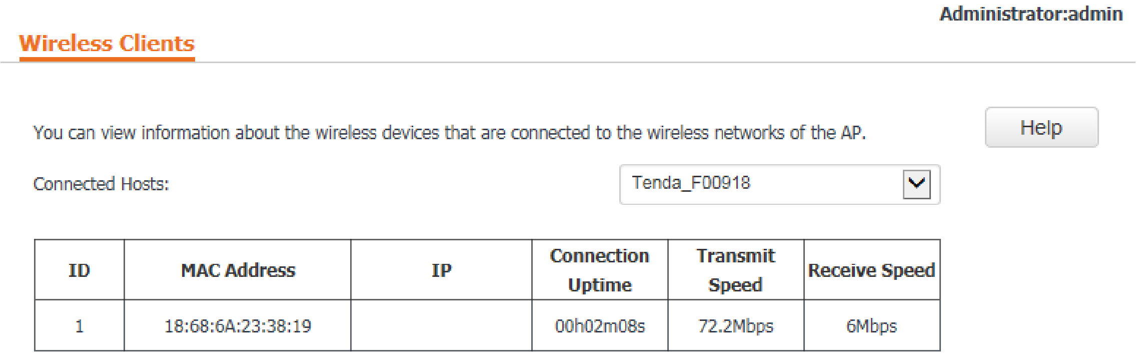
Traffic Statistics

SSID	Received Traffic	Received Packets	Transmitted Traffic	Transmitted Packets
Tenda_F00918	582.11MB	2792719	6.93MB	31983
Tenda_F00919	0.00MB	0	0.00MB	0

5.4 Wireless Clients

To access the page, choose **Status** > **Wireless Clients**.

On this page, you can view information about the wireless clients connected to the wireless networks corresponding to the SSIDs of the AP.



Administrator:admin

Wireless Clients

You can view information about the wireless devices that are connected to the wireless networks of the AP.

Connected Hosts: Tenda_F00918

ID	MAC Address	IP	Connection Uptime	Transmit Speed	Receive Speed
1	18:68:6A:23:38:19		00h02m08s	72.2Mbps	6Mbps

By default, the page displays information about the wireless clients connected to the wireless network corresponding to the primary SSID (first SSID) of the AP. To view information about the wireless clients connected to the wireless network corresponding to the other SSID, select the SSID from the drop-down list box in the upper-right corner.

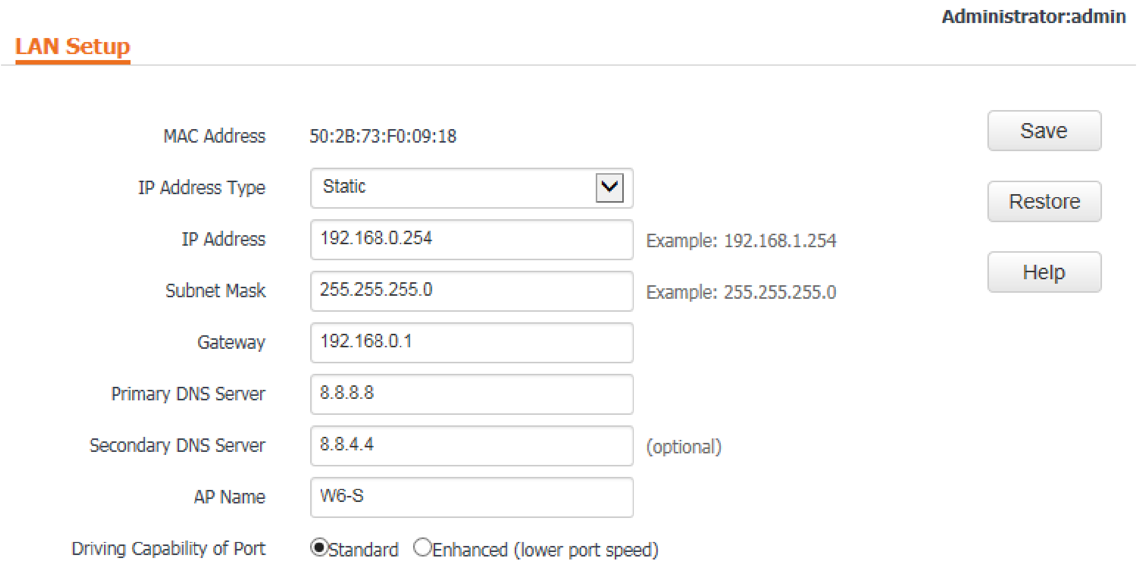
6 Network Settings

6.1 LAN Setup

6.1.1 Overview

To access the page, choose **Network** > **LAN Setup**.

This page enables you to view the MAC address of the LAN port of the AP and set the name, port driving capability, IP obtaining method, and other related parameters of the AP.



MAC Address	50:2B:73:F0:09:18	
IP Address Type	Static	
IP Address	192.168.0.254	Example: 192.168.1.254
Subnet Mask	255.255.255.0	Example: 255.255.255.0
Gateway	192.168.0.1	
Primary DNS Server	8.8.8.8	
Secondary DNS Server	8.8.4.4	(optional)
AP Name	W6-S	
Driving Capability of Port	● Standard ○ Enhanced (lower port speed)	

Parameter description

Parameter	Description
MAC Address	It specifies the MAC address of the LAN port of the AP. The default primary SSID of the AP is Tenda_*XXXXXX*, where *XXXXXX* indicates the last 6 characters of this MAC address.
IP Address Type	It specifies the IP address obtaining mode of the AP. The default option is **Static**. • **Static**: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is set manually. • **Dynamic**: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is obtained from a DHCP server on your LAN. NOTE If **IP Address Type** is set to **Dynamic**, you can log in to the web UI of the AP only with the IP address assigned to the AP by the DHCP server. The IP address is specified on the client list of the DHCP server.
IP Address	It specifies the IP address of the AP. The web UI of the AP is accessible at this IP address.

Parameter	Description
	The default IP address is 192.168.0.254. Generally, ensure that this IP address is in the same network segment as the LAN IP address of your LAN router connected to the internet, so that the AP can access the internet.
Subnet Mask	It specifies the subnet mask of the IP address of the AP. The default subnet mask is 255.255.255.0.
Gateway	It specifies the gateway IP address of the AP. Generally, set the gateway IP address to the LAN IP address of your LAN router connected to the internet, so that the AP can access the internet.
Primary DNS Server	It specifies the primary DNS server of the AP. If your LAN router connected to the internet provides the DNS proxy function, this IP address can be the LAN IP address of the router. Otherwise, enter a correct DNS server IP address.
Secondary DNS Server	It specifies the IP address of the secondary DNS server of the AP. This parameter is optional. If a DNS server IP address in addition to the IP address of the primary DNS server is available, enter the additional IP address in this field.
AP Name	It specifies the name of the AP. By default, the name is the model of the AP, such as W6-S. You are recommended to change the name of the AP to indicate the location of the AP, such as Bedroom, so that you can easily identify the AP when managing many APs.
Driving Capability of Port	It specifies the driving capability of the LAN0 port of the AP. • **Standard**: This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended. • **Enhanced**: This mode features a long transmission distance but relatively low transmission rate (usually 10 Mbps). This mode is recommended only if the Ethernet cable that connects the LAN0 port of the AP to a peer device exceeds 100 meters. In this case, the connected LAN port of the peer device must work in auto-negotiation mode. Otherwise, the LAN0 port of the AP may not be able to properly transmit or receive data.

6.1.2 Changing the LAN IP Address of the AP

Manually Setting the IP Address

In Static mode, you must manually set the IP address, subnet mask, gateway IP address, and DNS server IP addresses of the AP. Therefore, this mode is recommended if you need to deploy only a few APs.

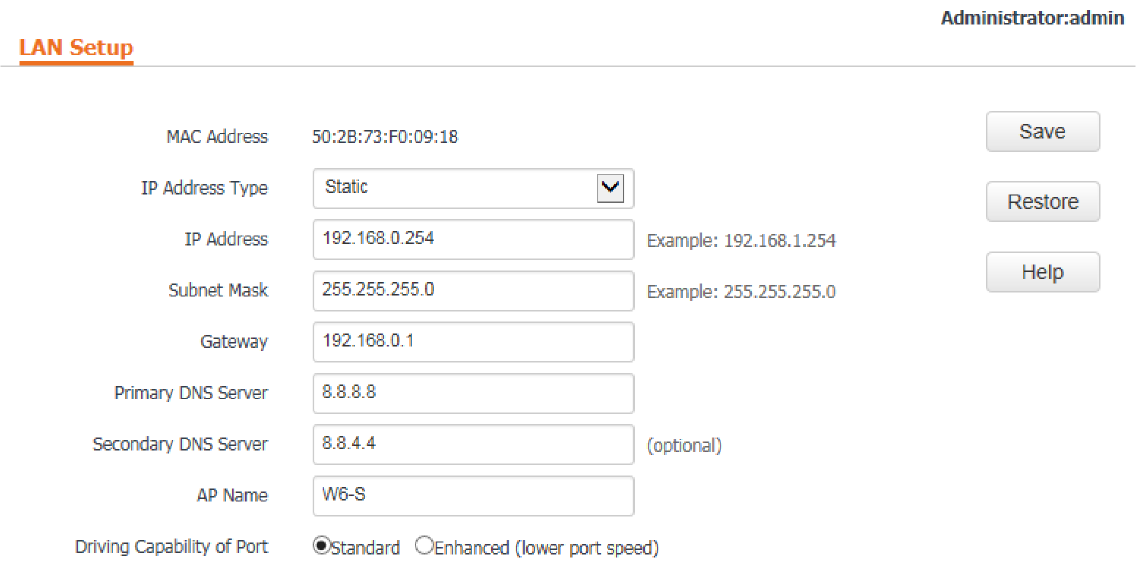
Perform the following procedure:

Step 1 Choose **Network** > **LAN Setup**.

Step 2 Set **IP Address Type** to **Static**.

Step 3 Set **IP Address**, **Subnet Mask**, **Gateway**, and **Primary DNS Server**. If another DNS server is available, set **Secondary DNS Server** to the IP address of the additional DNS server.

Step 4 Click **Save**.


Administrator:admin

LAN Setup

MAC Address	50:2B:73:F0:09:18	
IP Address Type	Static	
IP Address	192.168.0.254	Example: 192.168.1.254
Subnet Mask	255.255.255.0	Example: 255.255.255.0
Gateway	192.168.0.1	
Primary DNS Server	8.8.8.8	
Secondary DNS Server	8.8.4.4	(optional)
AP Name	W6-S	
Driving Capability of Port	● Standard ○ Enhanced (lower port speed)	

---End

After the configuration, if the new and original IP addresses belong to the same network segment, you can log in to the web UI of the AP by accessing the new IP address. Otherwise, assign your management computer an IP address that belongs to the same network segment as the new IP address of the AP before login.

Automatically Obtaining an IP Address

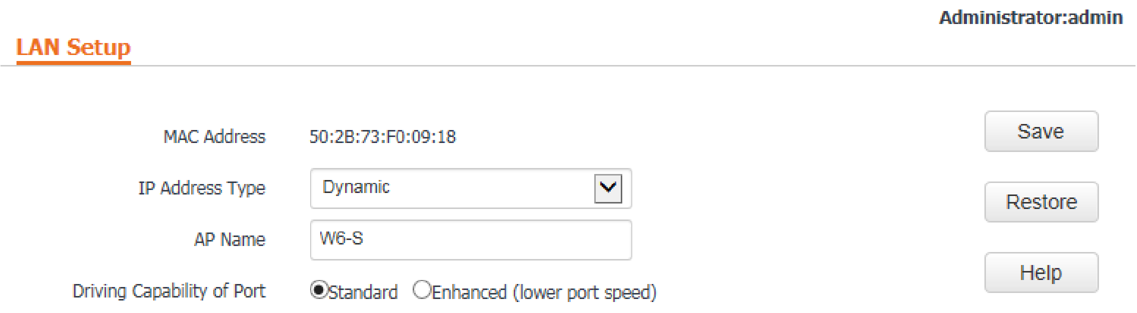
This mode enables the AP to automatically obtain an IP address, a subnet mask, a gateway IP address, DNS server IP addresses from a DHCP server on your LAN. If a large number of APs are deployed, you can adopt this mode to prevent IP address conflicts and effectively reduce your workload.

Perform the following procedure:

Step 1 Choose **Network** > **LAN Setup**.

Step 2 Set **IP Address Type** to **Dynamic**.

Step 3 Click **Save**.


Administrator:admin

LAN Setup

MAC Address	50:2B:73:F0:09:18
IP Address Type	Dynamic
AP Name	W6-S
Driving Capability of Port	● Standard ○ Enhanced (lower port speed)

---End

After the configuration, if you want to relog in to the web UI of the AP, check the client list of the DHCP server for the IP address assigned to the AP, ensure that the IP address of the management computer and the IP address of the AP belong to the same network segment, and access the IP address of the AP.

6.2 DHCP Server

6.2.1 Overview

The AP provides a DHCP server function to assign IP addresses to clients on the LAN. By default, the DHCP server function is disabled.

NOTE

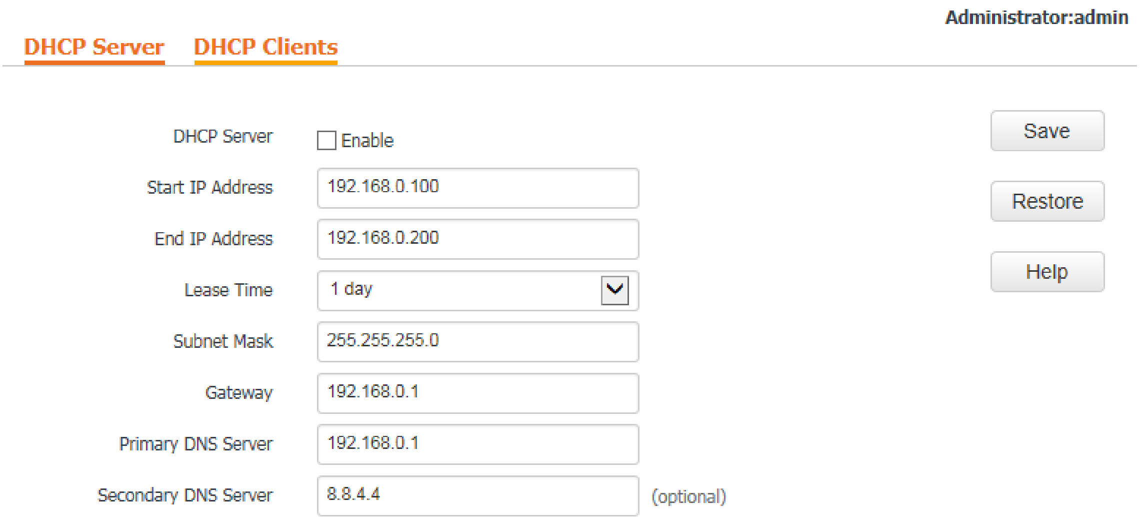
If the new and original IP addresses of the LAN port belong to different network segment, the system changes the IP address pool of the DHCP server function of the AP so that the IP address pool and the new IP address of the LAN port belong to the same network segment.

6.2.2 Configuring the DHCP Server

Step 1 Choose **Network** > **DHCP Server**.

Step 2 Set the parameters. Generally, you need to set only **DHCP Server**, **Gateway**, and **Primary DNS Server**.

Step 3 Click **Save**.



DHCP Server	□ Enable
Start IP Address	192.168.0.100
End IP Address	192.168.0.200
Lease Time	1 day
Subnet Mask	255.255.255.0
Gateway	192.168.0.1
Primary DNS Server	192.168.0.1
Secondary DNS Server	8.8.4.4 (optional)

---End

Parameter description

Parameter	Description
DHCP Server	It specifies whether to enable the DHCP server function of the AP. By default, it is disabled.
Start IP Address	It specifies the start IP address of the IP address pool of the DHCP server. The default value is **192.168.0.100**.
End IP Address	It specifies the end IP address of the IP address pool of the DHCP server. The default value is **192.168.0.200**. NOTE The start and end IP addresses must belong to the same network segment as the IP address of the LAN port of the AP.
Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a client.

Parameter	Description
	When half of the lease time has elapsed, the client sends a DHCP Request to the DHCP server to renew the lease time. If the request succeeds, the lease time is extended according to the request. Otherwise, the client sends the request again when 7/8 of the lease time has elapsed. If the request succeeds, the lease time is extended according to the request. Otherwise, the client must request an IP address from the DHCP server after the lease time expires. It is recommended that you retain the default value **1 day**.
Subnet Mask	It specifies the subnet mask assigned by the DHCP server to clients. The default value is **255.255.255.0**.
Gateway	It specifies the default IP address gateway assigned by the DHCP server to clients. Generally, it is the IP address of the LAN port of a router on the LAN. The default value is **192.168.0.254**. NOTE A client can access a server or host not in the local network segment only through a gateway.
Primary DNS Server	It specifies the primary DNS server IP address assigned by the DHCP server to clients. The default value is **192.168.0.254**. NOTE To enable clients to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS Server	It specifies the secondary DNS server IP address assigned by the DHCP server to clients. This parameter is optional.

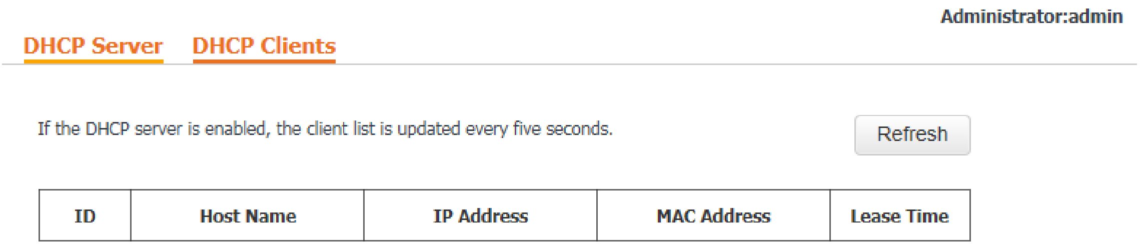
NOTE

If another DHCP server is available on your LAN, ensure that the IP address pool of the AP does not overlap the IP address pool of that DHCP server. Otherwise, IP address conflicts may occur.

6.2.3 Viewing the DHCP Client List

If the AP functions as a DHCP server, you can view the DHCP client list to understand the details about the clients that obtain IP addresses from the DHCP server. The details include host names, IP addresses, MAC addresses, and lease times.

To access the page, choose **Network** > **DHCP Server** and click **DHCP Clients**.



If the DHCP server is enabled, the client list is updated every five seconds.

ID	Host Name	IP Address	MAC Address	Lease Time

To view the latest DHCP client list, click **Refresh**.

7 Wireless Settings

7.1 Basic Settings

7.1.1 Overview

This module enables you to set SSID-related parameters of the AP.

Broadcast SSID

When the AP broadcasts an SSID, nearby wireless clients can detect the SSID. When this parameter is set to **Disable**, the AP does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. This to some extent enhances the security of the wireless network.

NOTE

After **Broadcast SSID** is set to **Disable**, a hacker can still connect to the corresponding wireless network if he/she manages to obtain the SSID by other means.

Isolate Client

This parameter implements a function similar to the VLAN function for wired networks. It isolates the wireless clients connected to the same wireless network corresponding to an SSID, so that the wireless clients can access only the wired network connected to the AP. Applying this function to hotspot setup at public places such as hotels and airports helps increase network security.

WMF

The number of wireless clients keeps increasing currently, but wired and wireless bandwidth resources are limited. Therefore, the multicast technology, which enables single-point data transmission and multi-point data reception, has been widely used in networks to effectively reduce bandwidth requirements and prevent network congestion.

Nevertheless, if a large number of clients are connected to a wireless interface of a wireless network and multicast data is intended for only one of the clients, the data is still sent to all the clients, which unnecessarily increases wireless resource usage and may lead to wireless channel congestion. In addition, multicast stream forwarding over an 802.11 network is not secure.

The WMF function of the AP converts multicast traffic into unicast traffic and forwards the traffic to the multicast traffic destination in the wireless network. This helps save wireless resources, ensure reliable transmission, and reduce delays.

Max. Number of Clients

This parameter specifies the maximum number of clients that can connect to the wireless network corresponding to an SSID. If the number is reached, the wireless network rejects new connection requests from clients. This limit helps balance load among APs.

Security Mode

A wireless network uses radio, which is open to the public, as its data transmission medium. If the wireless network is not protected by necessary measures, any client can connect to the network to use the resources of the network or access unprotected data over the network. To ensure communication security, transmission links of wireless networks must be encrypted for protection.

The AP supports various security modes for network encryption, including **None**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **Mixed WPA/WPA2-PSK**, **WPA**, and **WPA2**.

- None

  It indicates that any wireless client can connect to the wireless network. This option is not recommended because it affects network security.

- WEP

  It uses a static key to encrypt all exchanged data, and ensures that a wireless LAN has the same level of security as a wired LAN. Data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum wireless network throughput of only 54 Mbps. Therefore, this security mode is not recommended.

- WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK

  Mixed WPA/WPA2-PSK indicates that wireless clients can connect to a wireless network using either WPA-PSK or WPA2-PSK.

  In these security modes, an AP adopts a preshared key for authentication, and generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the security modes suitable for ensuring security of home wireless networks. Nevertheless, because the initial preshared key for authentication is manually set and all clients use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.

- WPA and WPA2

  To address the key management weakness of WPA-PSK and WPA2-PSK, the WiFi Alliance puts forward WPA and WPA2, which use 802.1x to authenticate clients and generate data encryption–oriented root keys. WPA and WPA2 use the root keys to replace the preshared keys that set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK.

  WPA and WPA2 uses 802.1x to authenticate clients and the login information of a client is managed by the client. This effectively reduces the probability of information leakage. In addition, each time a client connects to an AP that adopts the WPA or WPA2 security mode, the RADIUS server generates a data encryption key and assigns it to the client. This makes it difficult for attackers to obtain the key. These features of WPA and WPA2 help significantly increase network security, making WPA and WPA2 the preferred security modes of wireless networks that require high security.

7.1.2 Changing the Basic Settings

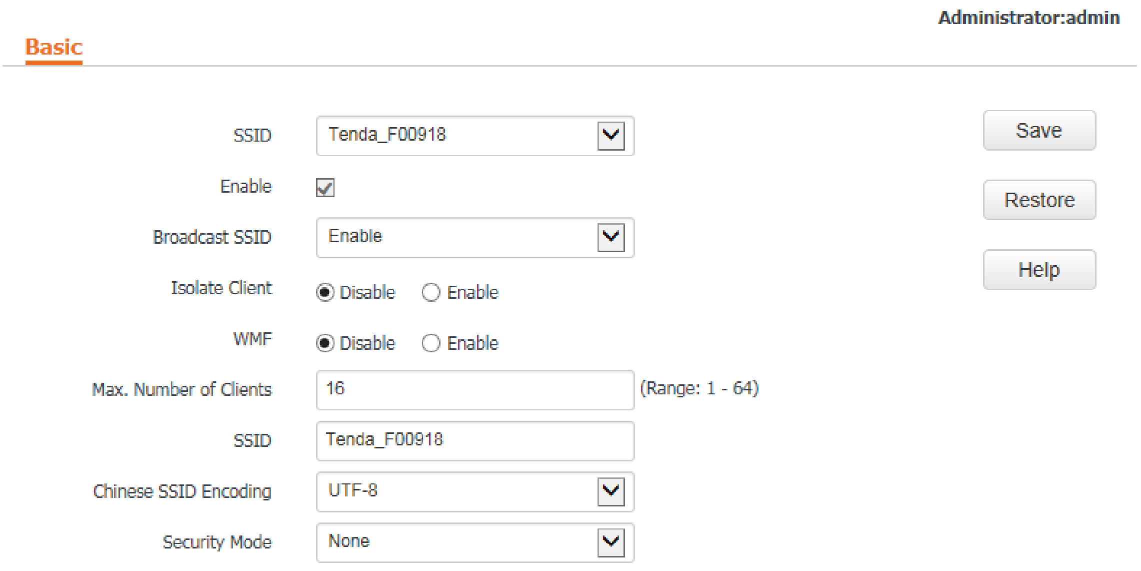
To change the basic settings of an SSID, perform the following procedure:

Step 1 Choose **Wireless** > **Basic**.

Step 2 Select the SSID from the **SSID** drop-down list box.

Step 3 Change the parameters as required. Generally, you only need to change the **Enable**, **SSID**, and **Security Mode** settings.

Step 4 Click **Save**.



SSID	Tenda_F00918
Enable	☑
Broadcast SSID	Enable
Isolate Client	● Disable ○ Enable
WMF	● Disable ○ Enable
Max. Number of Clients	16 (Range: 1 - 64)
SSID	Tenda_F00918
Chinese SSID Encoding	UTF-8
Security Mode	None

---End

Parameter description

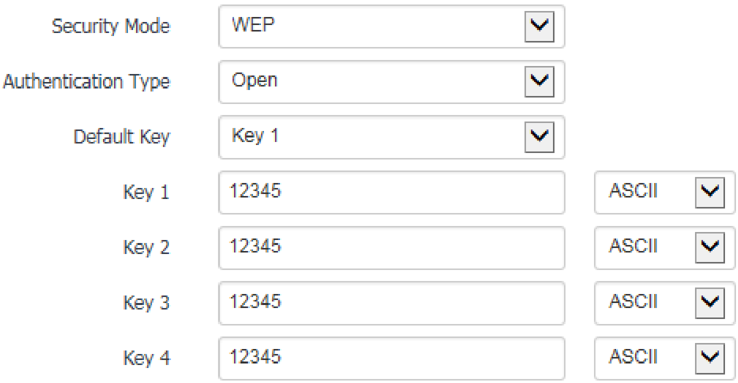
Parameter	Description
SSID	It specifies the SSID to be configured. The AP supports 2 SSIDs and the first SSID displayed is the primary SSID.
Enable	It specifies whether to enable the selected SSID. By default, the primary SSID is enabled and the other SSIDs are disabled. You can enable them as required.
Broadcast SSID	It specifies whether to broadcast the selected SSID. • **Enable**: It indicates that the AP broadcasts the selected SSID. In this case, nearby wireless clients can detect the SSID. • **Disable**: It indicates that the AP does not broadcast the selected SSID. In this case, if you want to connect a wireless client to the wireless network corresponding to the SSID, you must manually enter the SSID on the client. NOTE This AP can automatically hide its SSID. When the number of clients connected to the AP with an SSID of the AP reaches the upper limit, the AP stops broadcasting the SSID.
Isolate Client	• **Enable**: It indicates that the wireless clients connected to the AP with the selected SSID cannot communicate with each other. This improves wireless network security. • **Disable**: It indicates that the wireless clients connected to the AP with the selected SSID can communicate with each other. By default, it is disabled.
WMF	• **Enable**: It indicates that the WMF function is enabled. • **Disable**: It indicates that the WMF function is disabled.
Max. Number of Clients	It specifies the maximum number of clients that can be concurrently connected to the wireless network corresponding to an SSID. After this upper limit is reached, the AP rejects new requests from clients for connecting to the wireless network.

Parameter	Description
	A total of 128 wireless clients are allowed for all the enabled SSIDs of the AP.
SSID	It enables you to change the selected SSID. Chinese characters are allowed in an SSID.
Chinese SSID Encoding	It specifies the encoding format of Chinese characters in an SSID. This parameter takes effect only if the SSID contains Chinese characters. The default value is **UTF-8**. If both SSIDs of the AP are enabled and contain Chinese characters, you are recommended to set this parameter to **UTF-8** for one SSID and to **GB2312** for the other, so that any wireless client can identify one or both SSIDs.
Security Mode	It specifies the security mode of the selected SSID. The options include: None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2.

None

It allows any wireless client to connect to a wireless network. This option is not recommended because it affects network security.

WEP



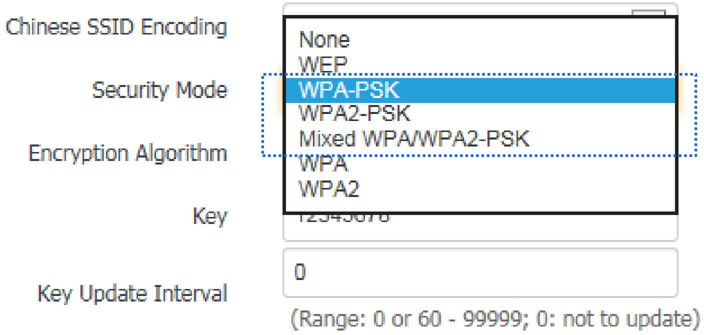
Security Mode	WEP	
Authentication Type	Open	
Default Key	Key 1	
Key 1	12345	ASCII
Key 2	12345	ASCII
Key 3	12345	ASCII
Key 4	12345	ASCII

Parameter description

Parameter	Description
Authentication Type	It specifies the authentication type for the WEP security mode. The options include **Open**, **Shared**, and **802.1x**.The options share the same encryption process. • **Open**: It specifies that authentication is not required and data exchanged is encrypted using WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. • **Shared**: It specifies that a shared key is used for authentication and data exchanged is encrypted using WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key. • **802.1x** specifies that 802.1x authentication is required and data exchanged is encrypted using WEP. In this case, ports are enabled for user authentication when valid clients connect to the wireless network corresponding to the selected SSID, and disabled when

Parameter	Description
	invalid users connect to the wireless network.
Default Key	It specifies the WEP key for the Open or Shared authentication type. For example, if **Default Key** is set to **Key 2**, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by **Key 2**.
ASCII	It indicates that a key selected for the Open or Shared authentication type contains hexadecimal characters. 5 or 13 ASCII characters are allowed in the key.
Hex	It indicates that a key selected for the Open or Shared authentication type contains hexadecimal characters. 10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key.
RADIUS Server IP	These parameters are dedicated to the 802.1x authentication type to specify the IP address, port number, and password of the RADIUS server for client authentication.
RADIUS Port	
RADIUS Password	

WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK


Chinese SSID Encoding

Security Mode: WPA-PSK

Encryption Algorithm

Key: 12345678

Key Update Interval: 0

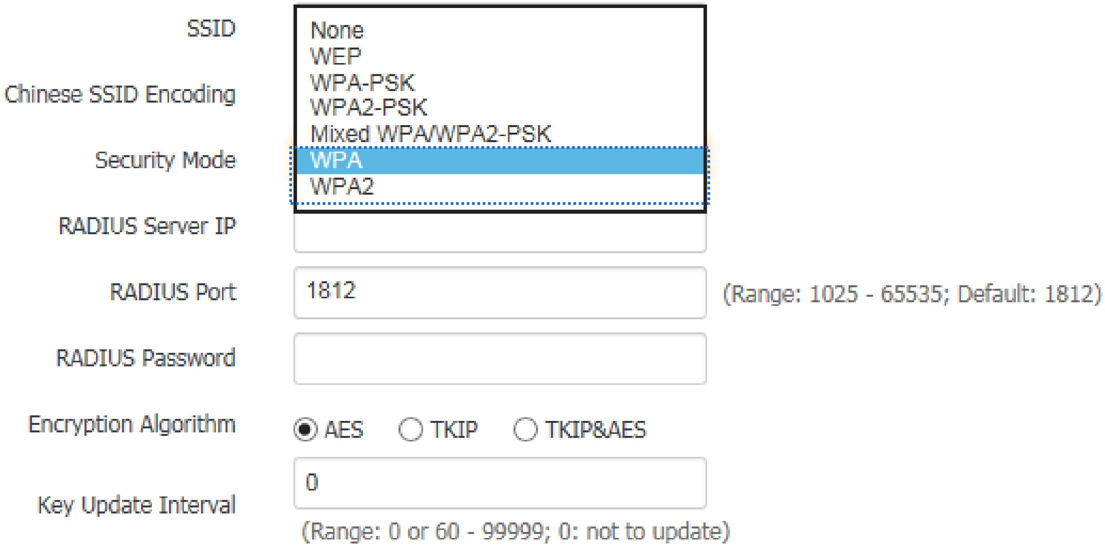
(Range: 0 or 60 - 99999; 0: not to update)

Parameter description

Parameter	Description
Security Mode	The **WPA-PSK**, **WPA2-PSK**, and **Mixed WPA/WPA2-PSK** options are available for network protection with a preshared key. • **WPA-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA-PSK. • **WPA2-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2-PSK. • **Mixed WPA/WPA2-PSK**: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. If **Security Mode** is set to **WPA-PSK**, this parameter has the **AES** and **TKIP** values. If **Security Mode** is set to **WPA2-PSK** or **Mixed WPA/WPA2-PSK**, this parameter has the **AES**, **TKIP**, and **TKIP&AES** values.

Parameter	Description
	- **AES**: It indicates the Advanced Encryption Standard. - **TKIP**: It indicates the Temporal Key Integrity Protocol. If **TKIP** is used, the maximum wireless throughput of the AP is limited to 54 Mbps. - **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a preshared WPA key. A WPA key can contain 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value **0** indicates that a WAP key is not updated.

WPA and WPA2



SSID

Chinese SSID Encoding

Security Mode: None / WEP / WPA-PSK / WPA2-PSK / Mixed WPA/WPA2-PSK / WPA / WPA2 (WPA selected)

RADIUS Server IP

RADIUS Port: 1812 (Range: 1025 - 65535; Default: 1812)

RADIUS Password

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key Update Interval: 0 (Range: 0 or 60 - 99999; 0: not to update)

Parameter description

Parameter	Description
Security Mode	The **WPA** and **WPA2** options are available for network protection with a RADIUS server. - **WPA**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA. - **WPA2**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2.
RADIUS Server IP	It specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	It specifies the port number of the RADIUS server for client authentication.
RADIUS Password	It specifies the shared password of the RADIUS server.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. The available options include **AES**, **TKIP**, and **TKIP&AES**.

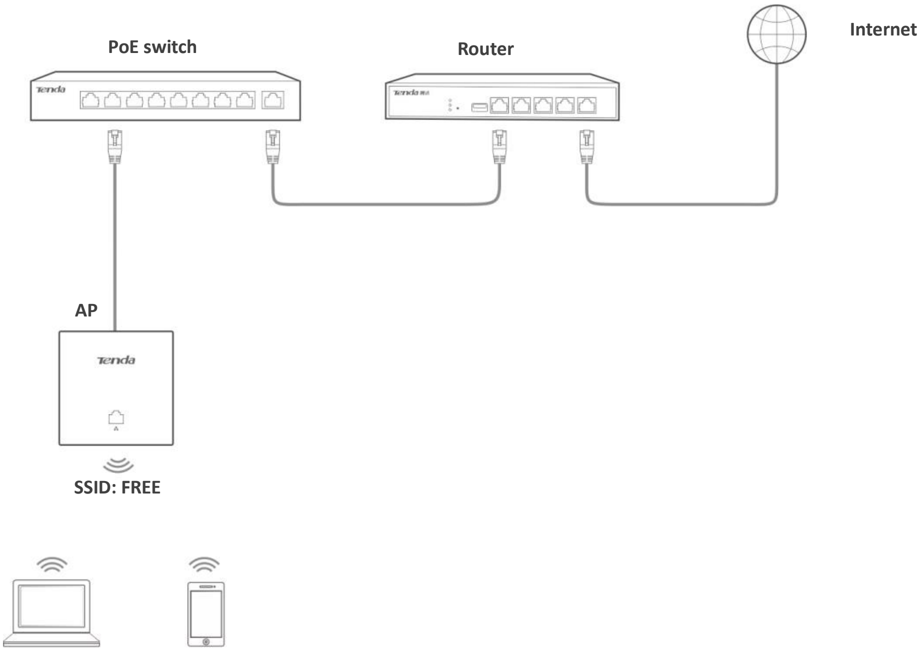
Parameter	Description
	• **AES**: It indicates the Advanced Encryption Standard. • **TKIP**: It indicates the Temporal Key Integrity Protocol. • **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value **0** indicates that a WAP key is not updated.

7.1.3 Examples of Configuring Basic Settings

Setting Up a Non-encrypted Wireless Network

- Networking requirement

  In a hotel lounge, guests can connect to the wireless network without a password and access the internet through the wireless network. See the following figure.



- Configuration procedure

  Assume that the second SSID of the AP is used.

Step 1 Choose **Wireless** > **Basic**.

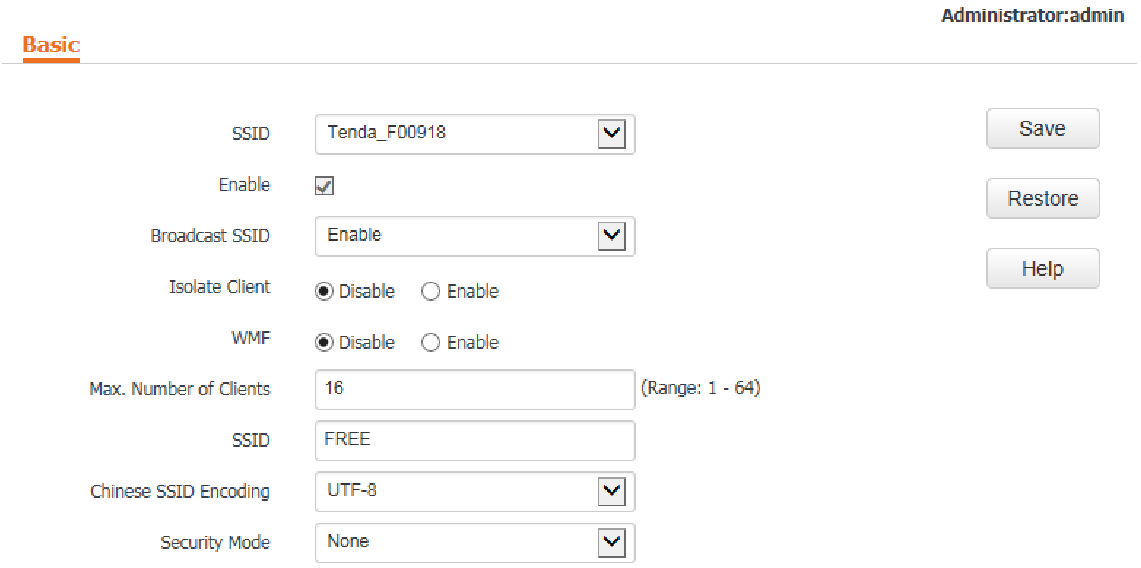
Step 2 Select the second SSID from the **SSID** drop-down list box.

Step 3 Select the **Enable** check box.

Step 4 Change the value of the **SSID** text box to **FREE**.

Step 5 Set **Security Mode** to **None**.

Step 6 Click **Save**.



Administrator:admin

Basic

SSID: Tenda_F00918

Enable: ☑

Broadcast SSID: Enable

Isolate Client: ● Disable ○ Enable

WMF: ● Disable ○ Enable

Max. Number of Clients: 16 (Range: 1 - 64)

SSID: FREE

Chinese SSID Encoding: UTF-8

Security Mode: None

---End

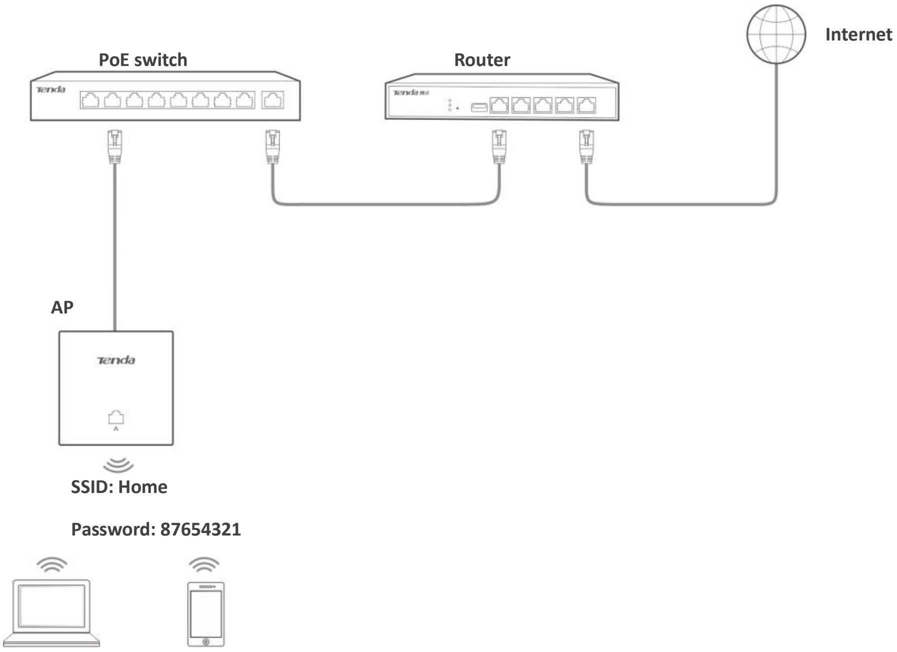
- Verification

  Verify that wireless devices can connect to the **FREE** wireless network without a password.

Setting Up a Wireless Network Encrypted Using WPA-PSK, WPA2-PSK, or Mixed WPA/WPA2-PSK

- Networking requirement

  A home wireless network with a certain level of security must be set up through a simply procedure. See the following figure.



- Configuration procedure

  Assume that the second SSID of the AP, the WPA2-PSK security mode, and AES encryption algorithm are used.

Step 1 Choose **Wireless** > **Basic**.

Step 2 Select the second SSID from the **SSID** drop-down list box.

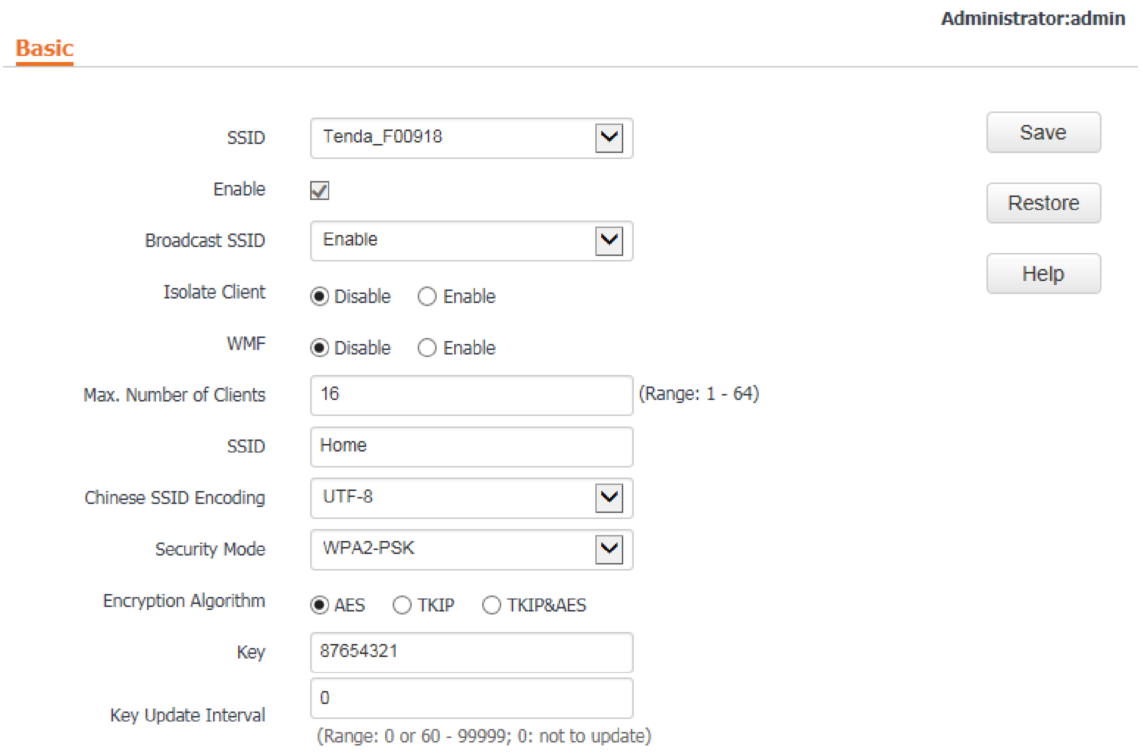
Step 3 Select the **Enable** check box.

Step 4 Change the value of the **SSID** text box to **Home**.

Step 5 Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.

Step 6 Set **Key** to **87654321**.

Step 7 Click **Save**.



Administrator:admin

Basic

SSID	Tenda_F00918
Enable	☑
Broadcast SSID	Enable
Isolate Client	● Disable ○ Enable
WMF	● Disable ○ Enable
Max. Number of Clients	16 (Range: 1 - 64)
SSID	Home
Chinese SSID Encoding	UTF-8
Security Mode	WPA2-PSK
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Key	87654321
Key Update Interval	0 (Range: 0 or 60 - 99999; 0: not to update)

---End

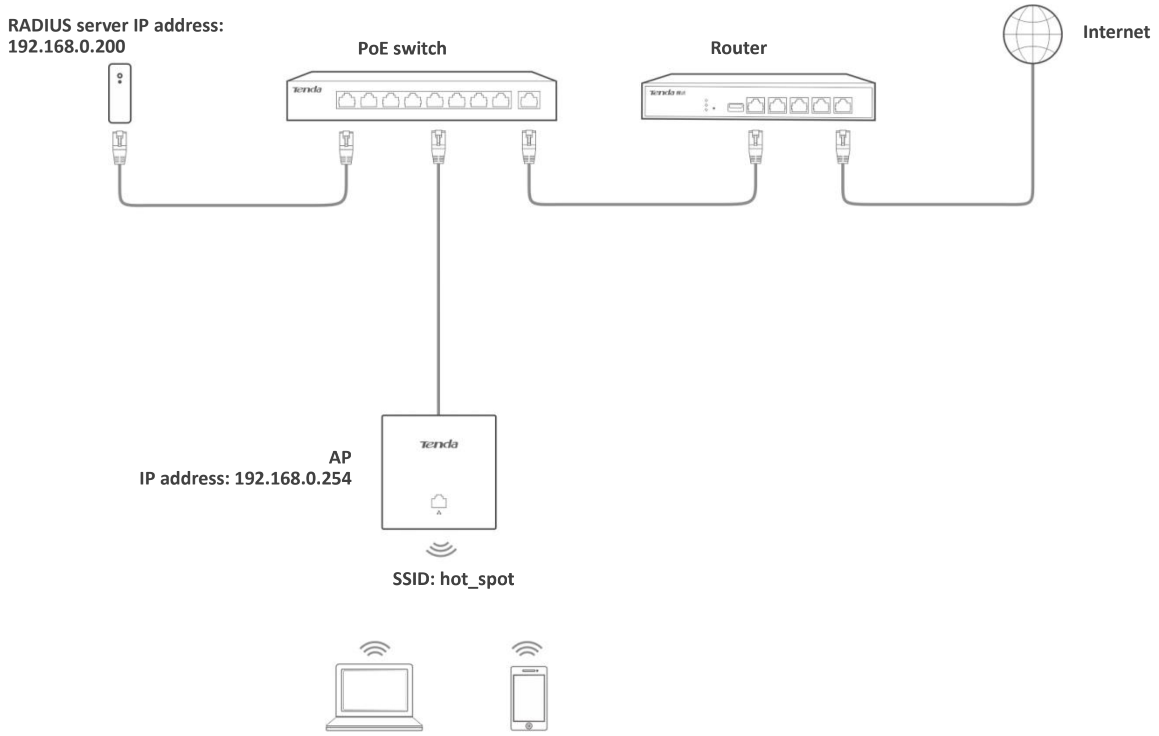
- Verification

Verify that wireless devices can connect to the **Home** wireless network with the password **87654321**.

Setting Up a Wireless Network Encrypted Using WPA or WPA2

- Networking requirement

A highly secure wireless network is required and a RADIUS server is available. See the following figure.

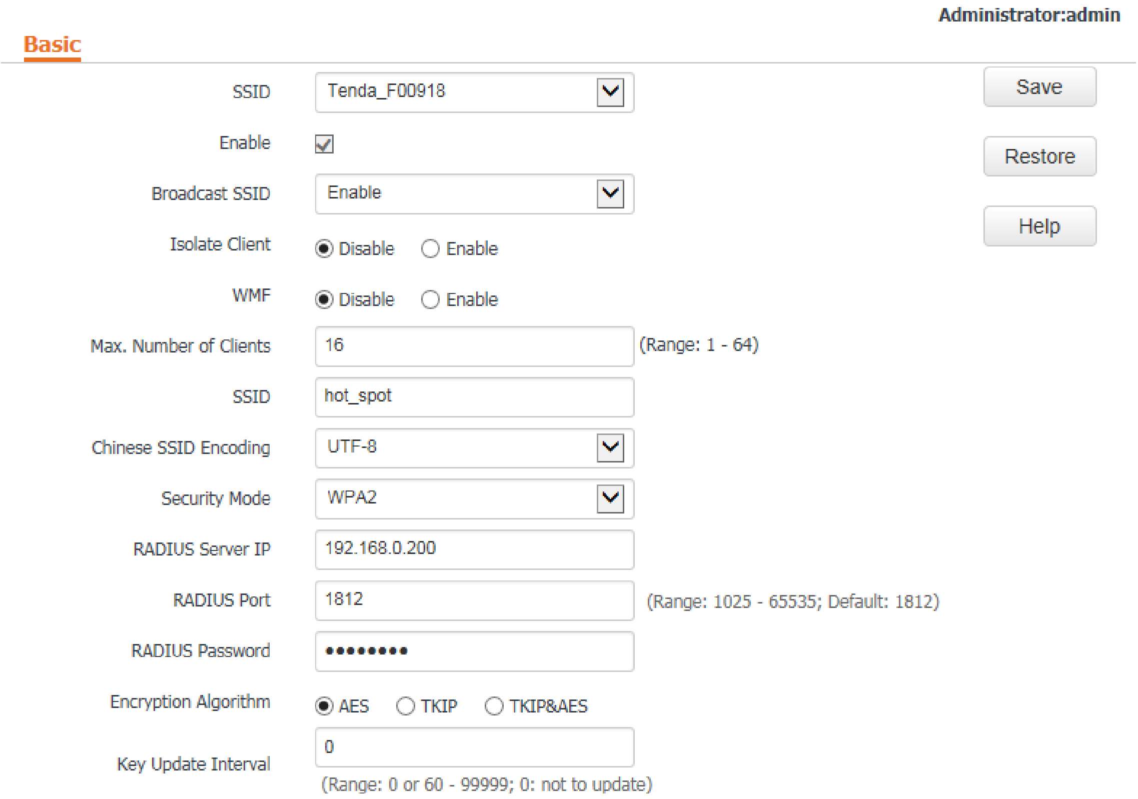


- Configuration procedure

Step 1 Configure the AP.

Assume that the IP address, port number, and password of the RADIUS server are 192.168.0.200, 1812, and 12345678 respectively, and that the second SSID of the AP and the WPA2 security mode are used.

1. Choose **Wireless** > **Basic**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Select the **Enable** check box.
4. Change the value of the **SSID** text box to **hot_spot**.
5. Set **Security Mode** to **WPA2**.
6. Set **RADIUS Server IP**, **RADIUS Port**, and **RADIUS Password** to **192.168.0.200**, **1812**, and **12345678** respectively.
7. Set **Encryption Algorithm** to **AES**.
8. Click **Save**.



Administrator:admin

Basic

SSID	Tenda_F00918	
Enable	☑	
Broadcast SSID	Enable	
Isolate Client	● Disable ○ Enable	
WMF	● Disable ○ Enable	
Max. Number of Clients	16	(Range: 1 - 64)
SSID	hot_spot	
Chinese SSID Encoding	UTF-8	
Security Mode	WPA2	
RADIUS Server IP	192.168.0.200	
RADIUS Port	1812	(Range: 1025 - 65535; Default: 1812)
RADIUS Password	••••••••	
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES	
Key Update Interval	0	(Range: 0 or 60 - 99999; 0: not to update)

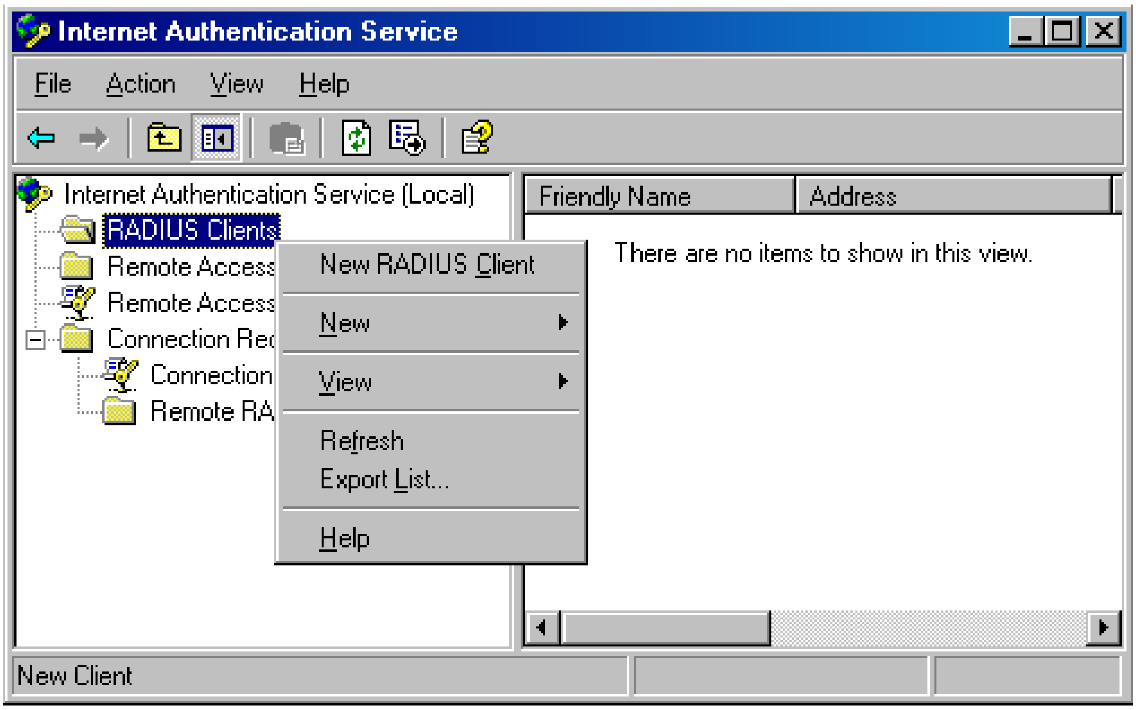
Step 2 Configure the RADIUS server.

NOTE

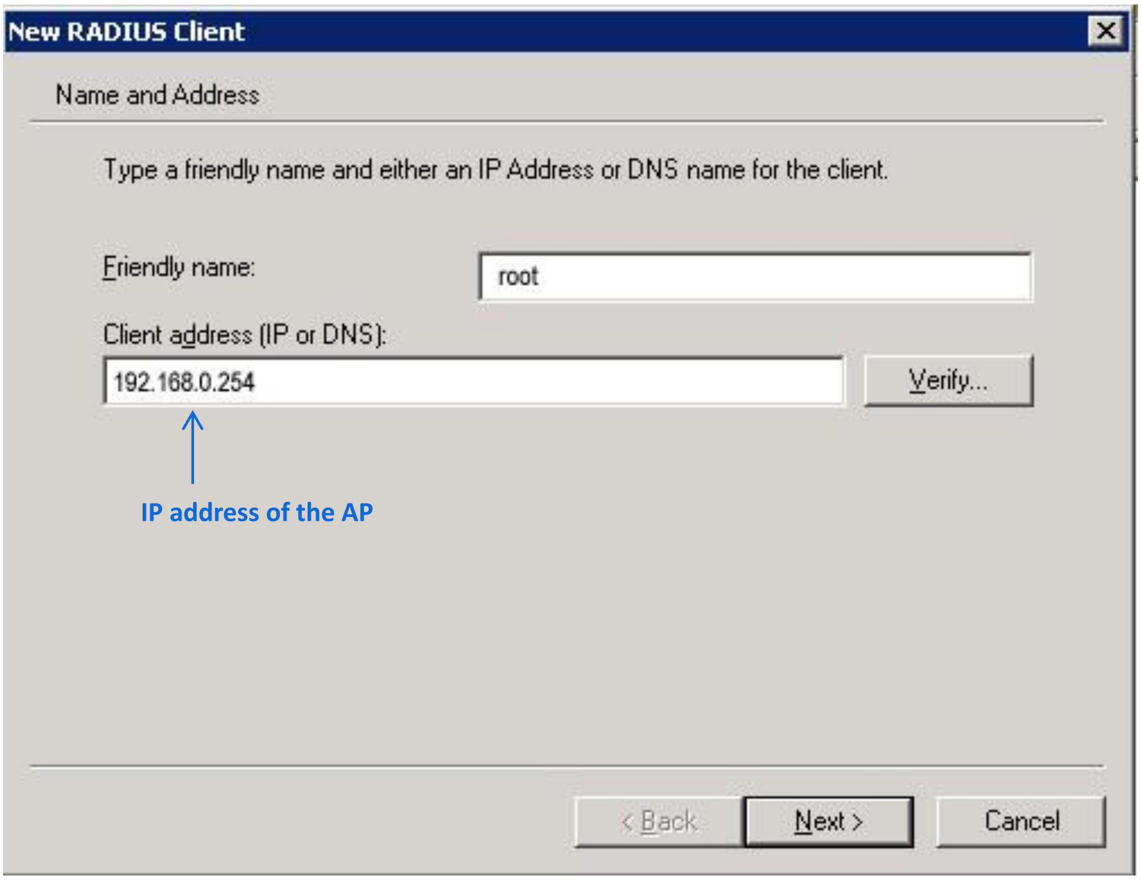
Windows 2003 is used as an example to describe how to configure the RADIUS server.

1. Configure a RADIUS client.

(1) In the **Computer Management** dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.



(2) Enter a RADIUS client name (which can be the name of the AP) and the IP address of the AP, and click **Next**.

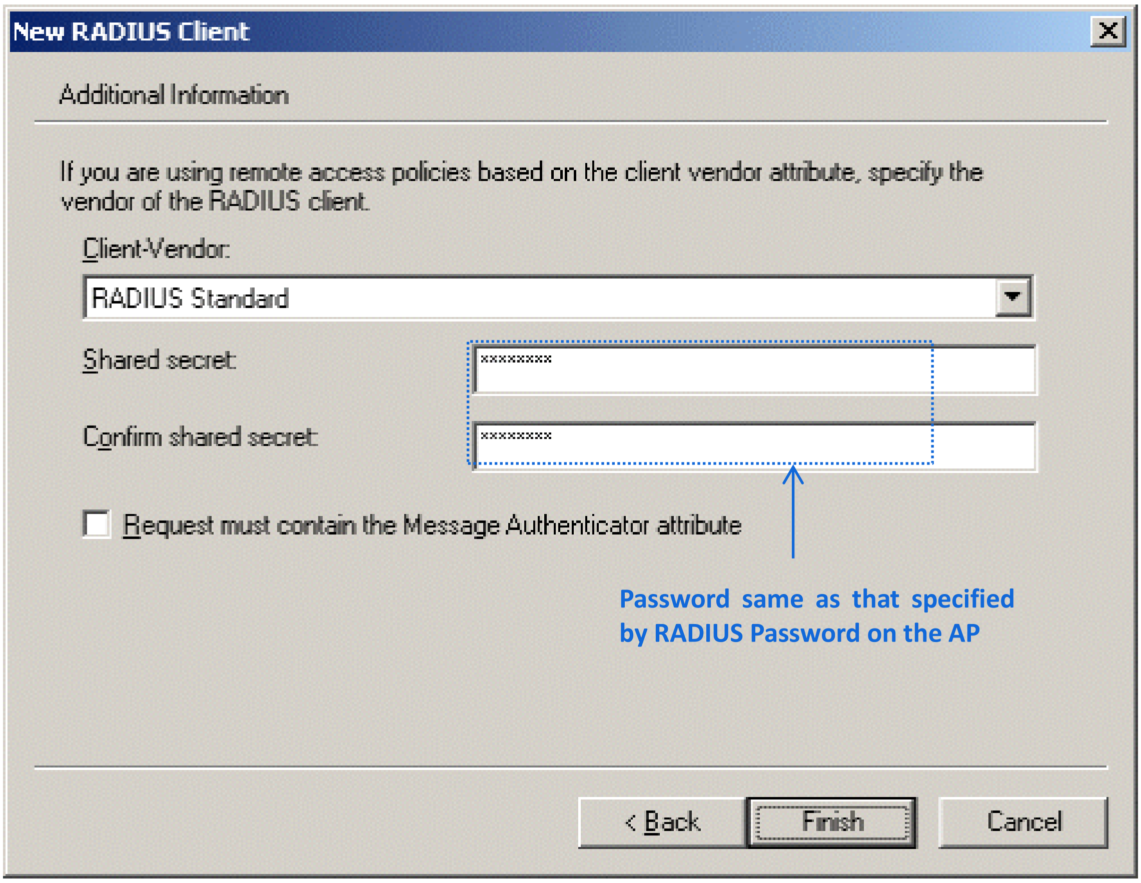


Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: root

Client address (IP or DNS): 192.168.0.254

(3) Enter **12345678** in the **Shared secret** and **Confirm shared secret** text boxes, and click **Finish**.



New RADIUS Client
Additional Information
< Back
Finish
Cancel
Password same as that specified by RADIUS Password on the AP

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

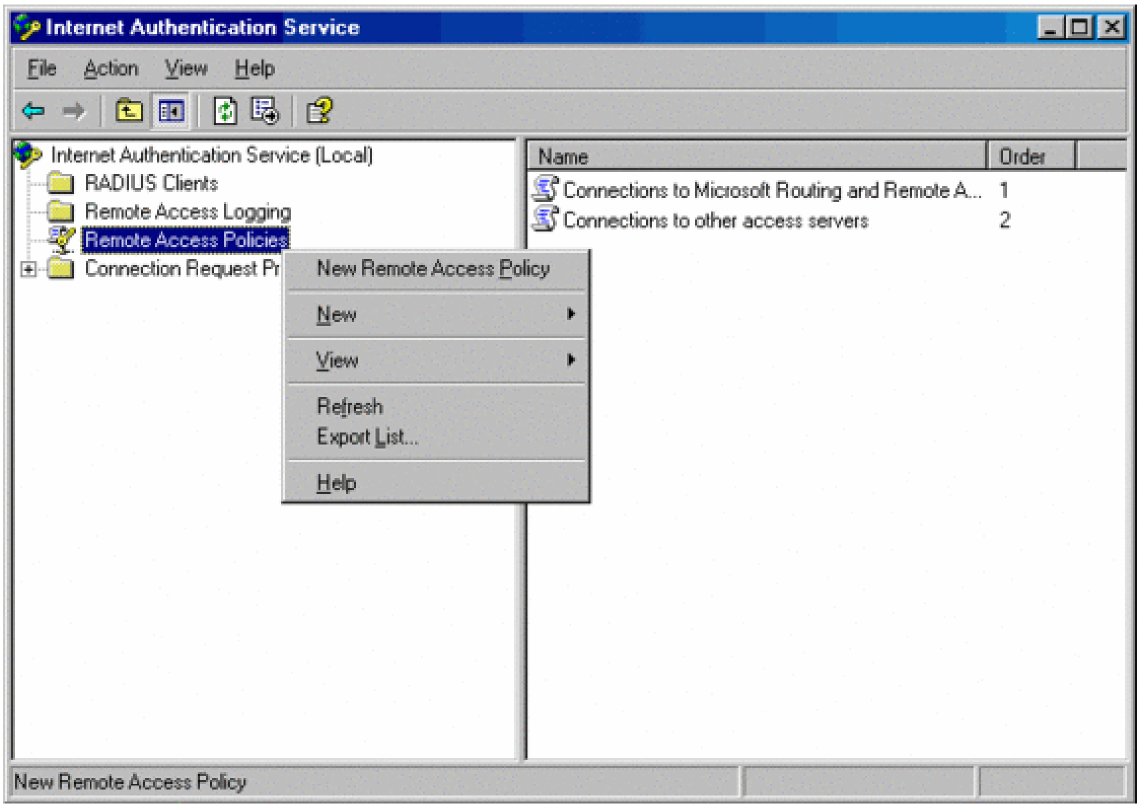
Shared secret: ********

Confirm shared secret: ********

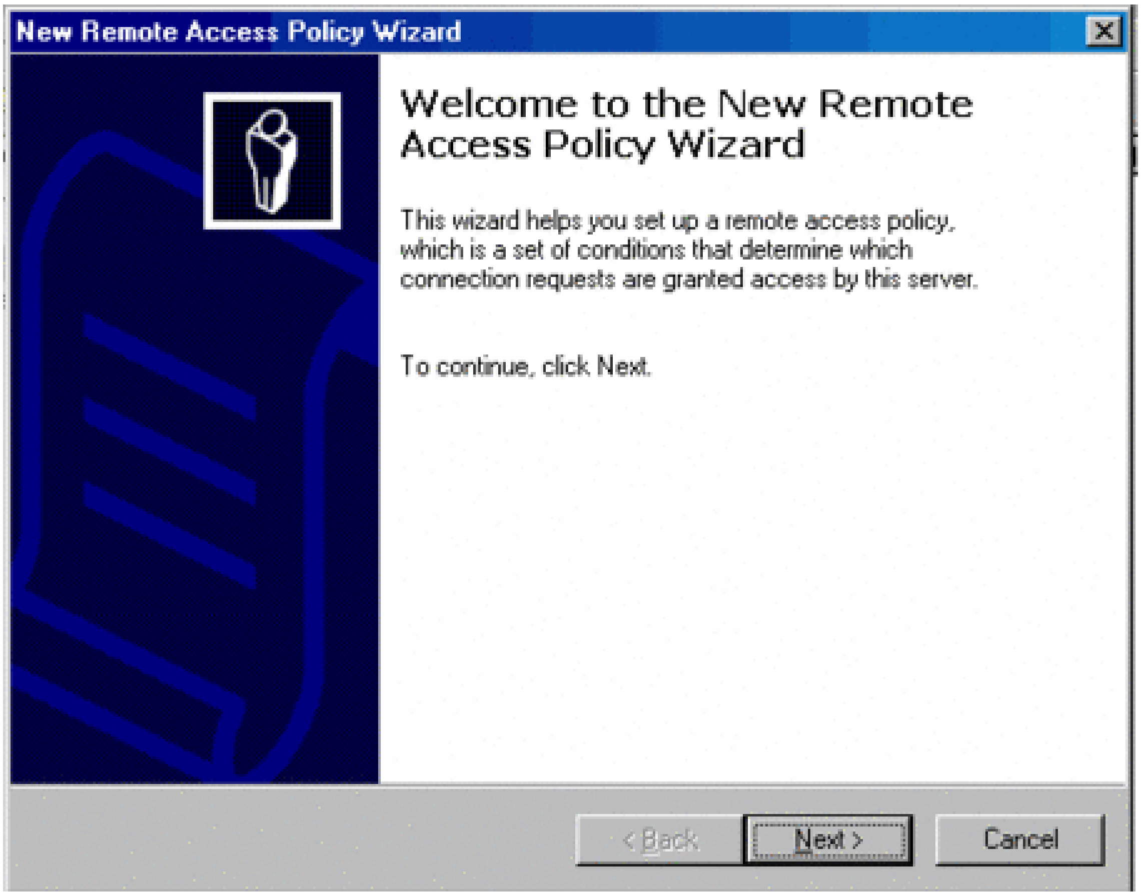
□ Request must contain the Message Authenticator attribute

2. Configure a remote access policy.

(1) Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



(2) In the **New Remote Access Policy Wizard** dialog box that appears, click **Next**.

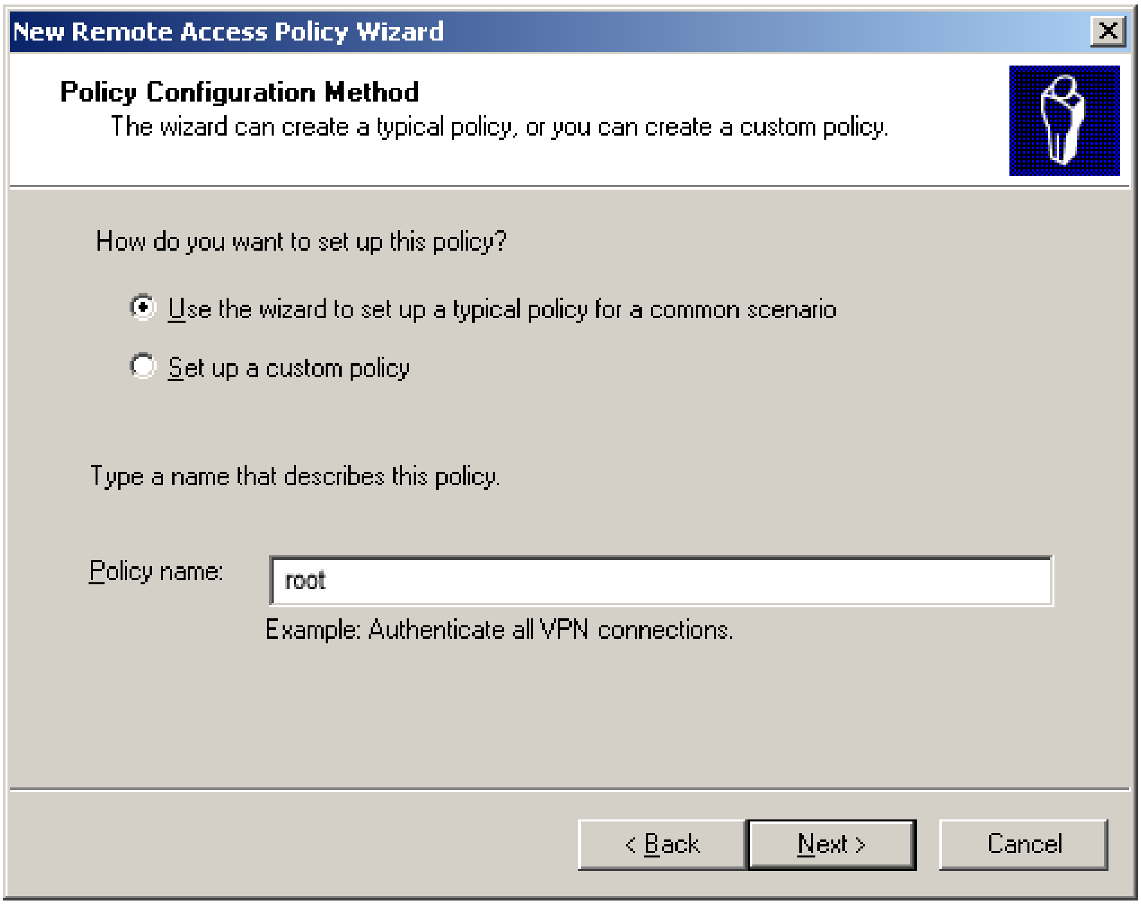

New Remote Access Policy Wizard

Welcome to the New Remote Access Policy Wizard

This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.

To continue, click Next.

(3) Enter a policy name and click **Next**.



Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

● Use the wizard to set up a typical policy for a common scenario

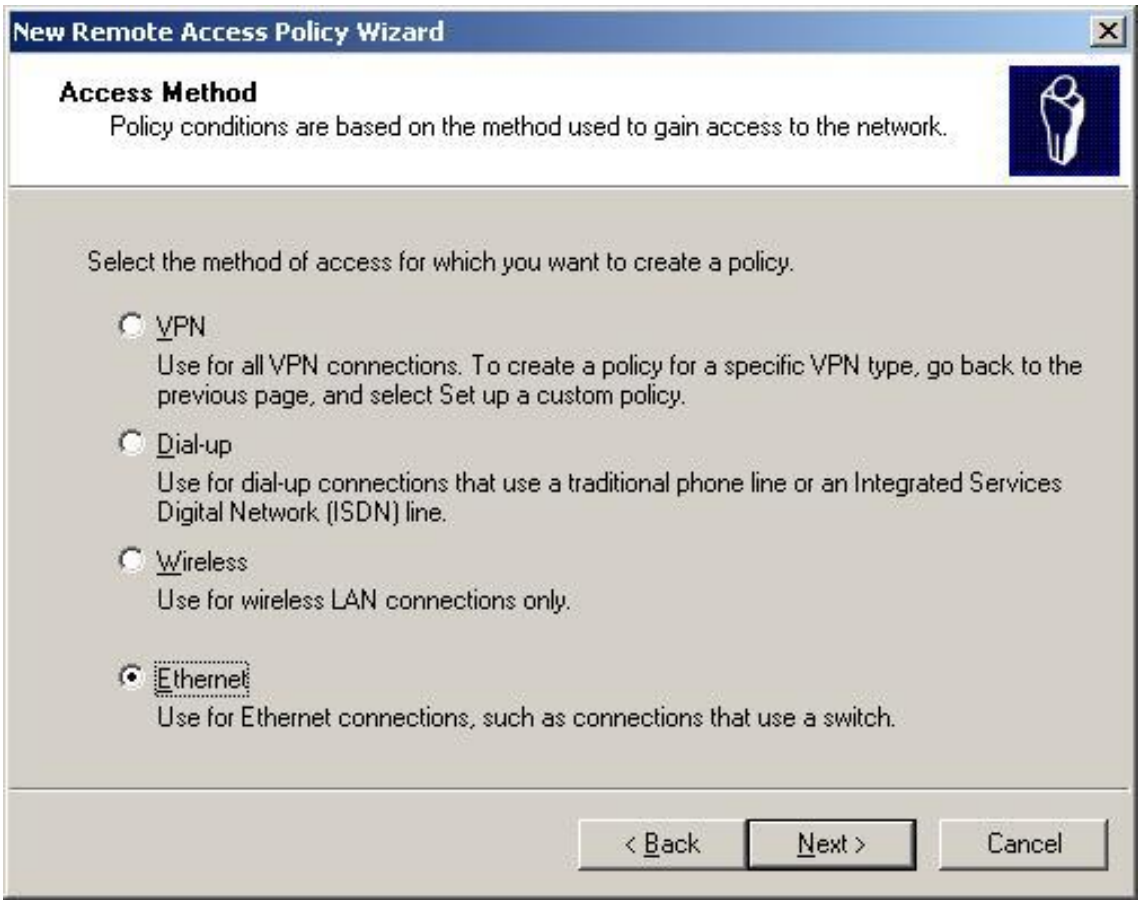
○ Set up a custom policy

Type a name that describes this policy.

Policy name: root

Example: Authenticate all VPN connections.

(4) Select **Ethernet** and click **Next**.



New Remote Access Policy Wizard

Access Method

Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

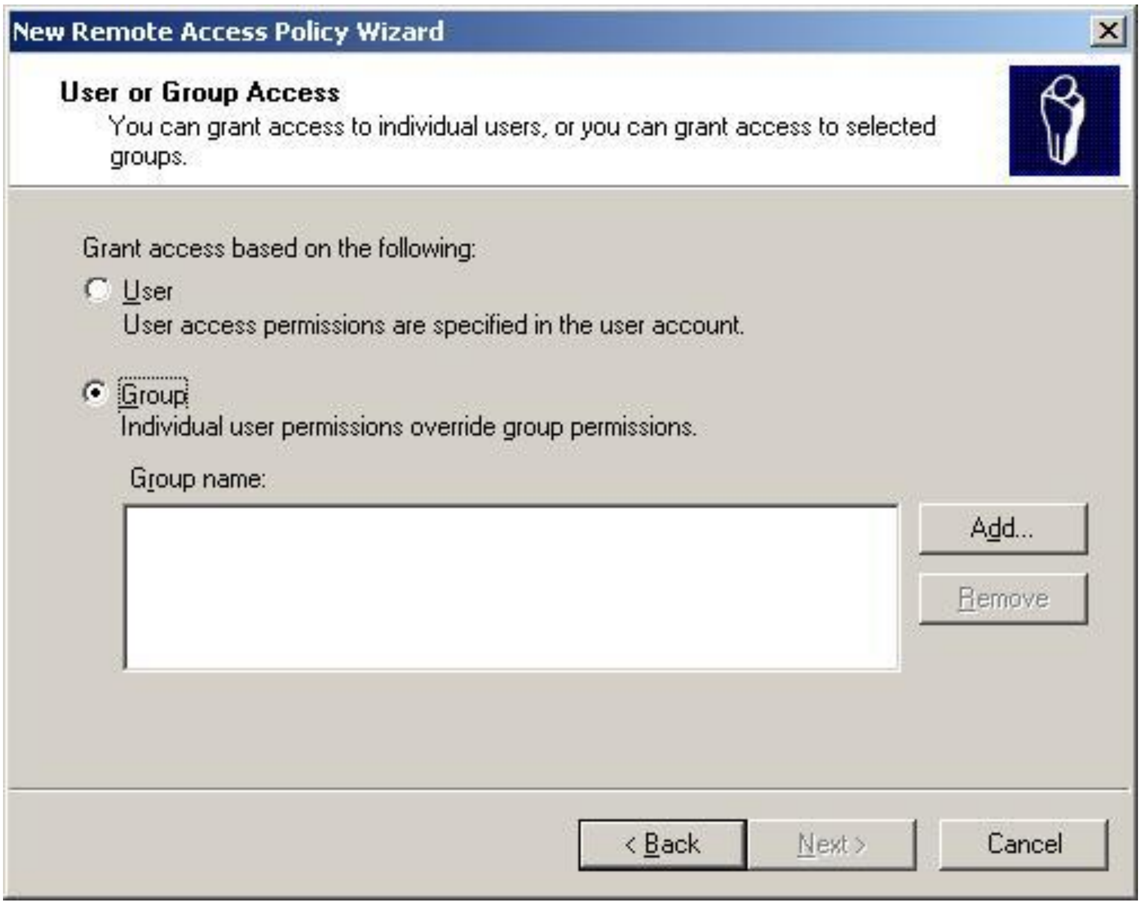
○ VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

○ Dial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.

○ Wireless
Use for wireless LAN connections only.

● Ethernet
Use for Ethernet connections, such as connections that use a switch.

(5) Select **Group** and click **Add**.



New Remote Access Policy Wizard

User or Group Access

You can grant access to individual users, or you can grant access to selected groups.

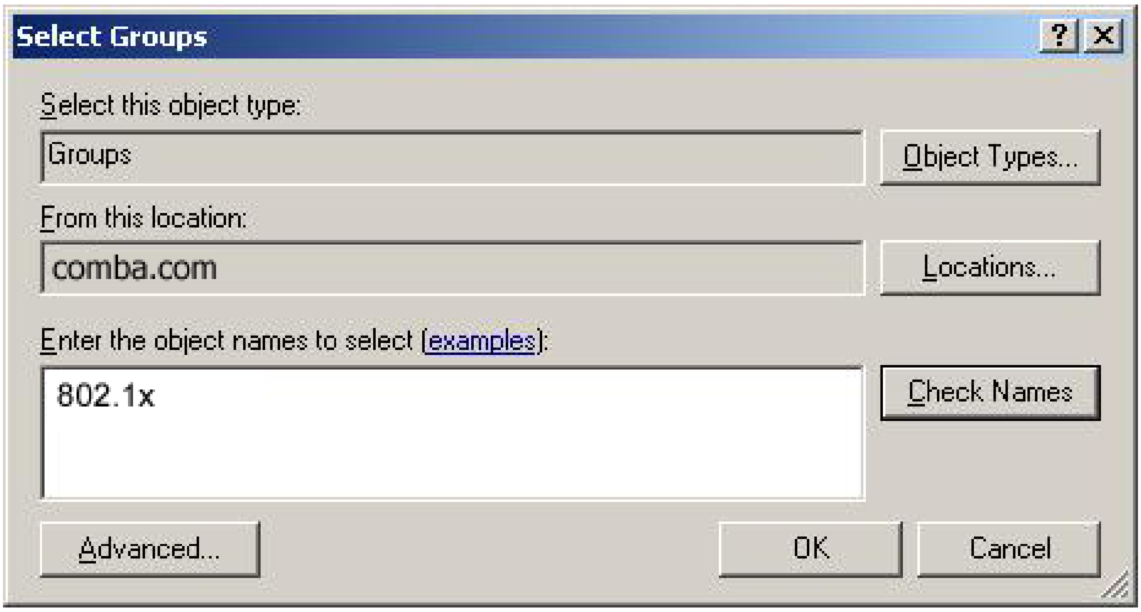
Grant access based on the following:

○ User
User access permissions are specified in the user account.

● Group
Individual user permissions override group permissions.

Group name:

(6) Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



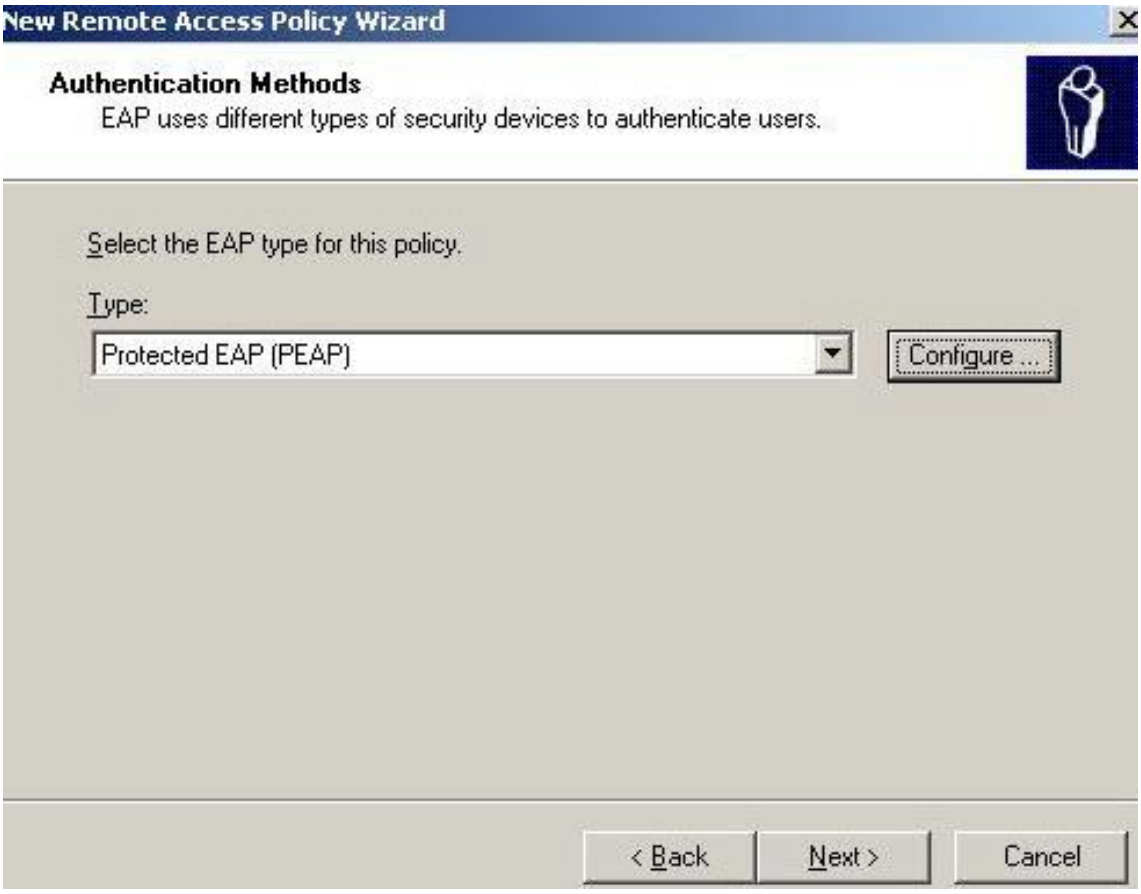
Select Groups

Select this object type: Groups

From this location: comba.com

Enter the object names to select (examples): 802.1x

(7) Select **Protected EAP (PEAP)** and click **Next**.



New Remote Access Policy Wizard

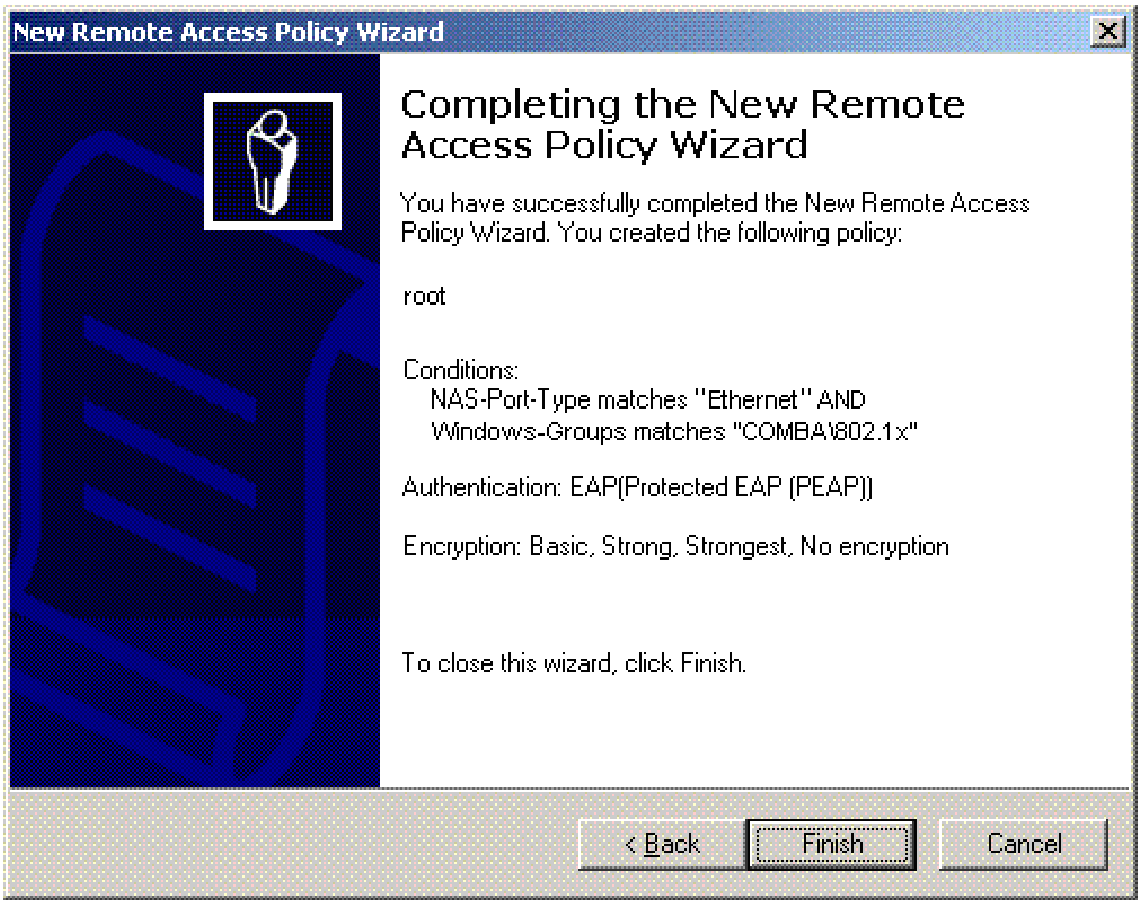
Authentication Methods

EAP uses different types of security devices to authenticate users.

Select the EAP type for this policy.

Type: Protected EAP (PEAP)

(8) Click **Finish**. The remote access policy is created.



Completing the New Remote Access Policy Wizard

You have successfully completed the New Remote Access Policy Wizard. You created the following policy:

root

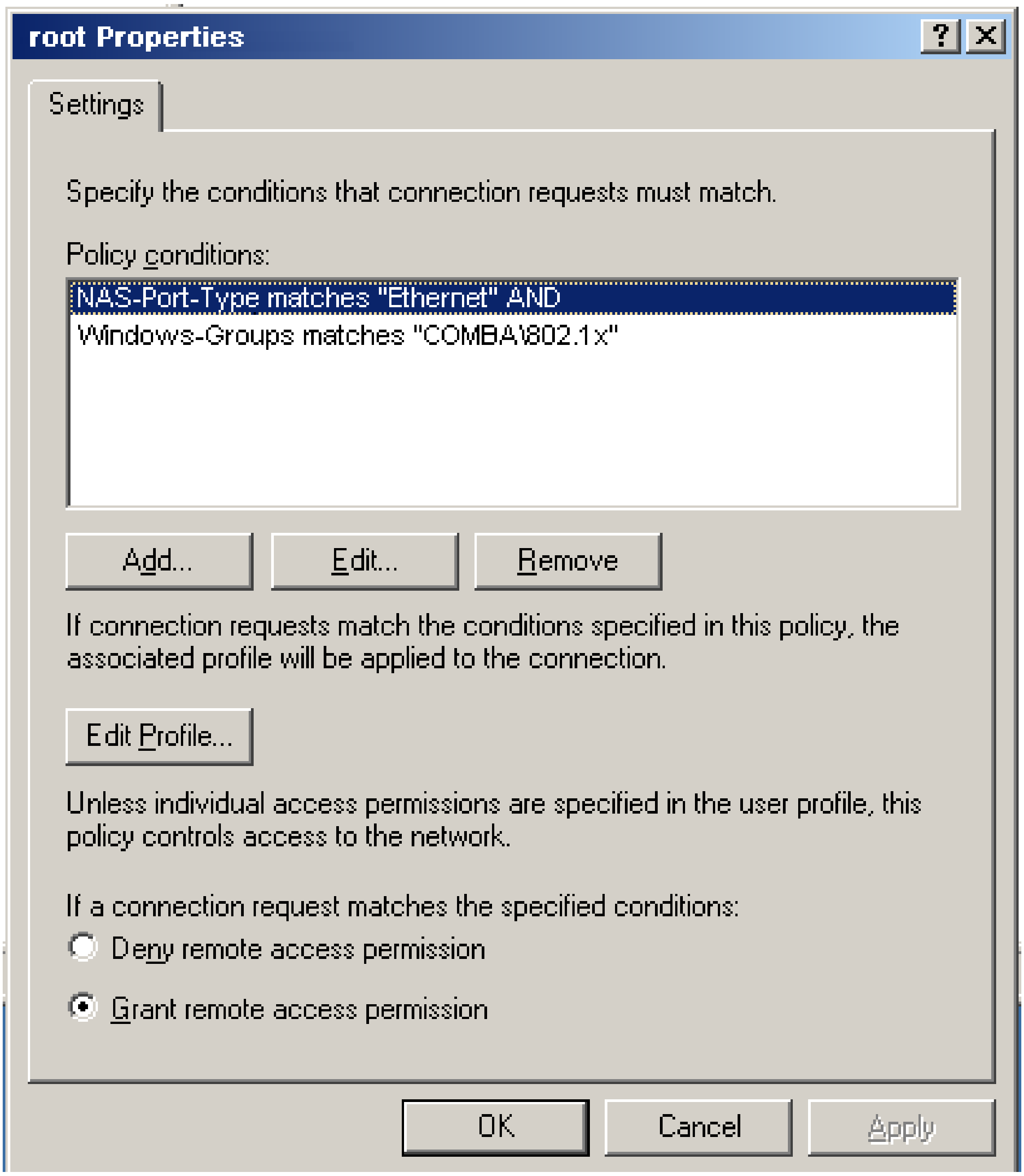
Conditions:
NAS-Port-Type matches "Ethernet" AND
Windows-Groups matches "COMBA\802.1x"

Authentication: EAP(Protected EAP (PEAP))

Encryption: Basic, Strong, Strongest, No encryption

To close this wizard, click Finish.

(9) Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



Specify the conditions that connection requests must match.

Policy conditions:

NAS-Port-Type matches "Ethernet" AND
Windows-Groups matches "COMBA\802.1x"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

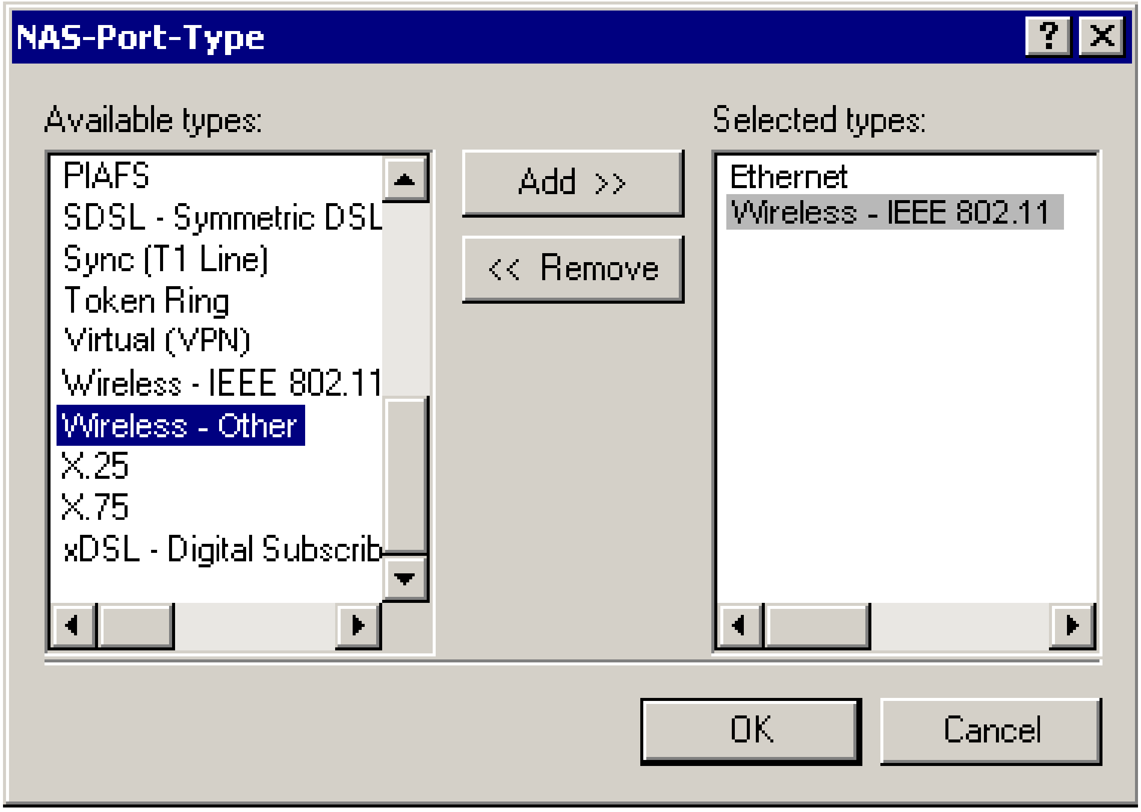
Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

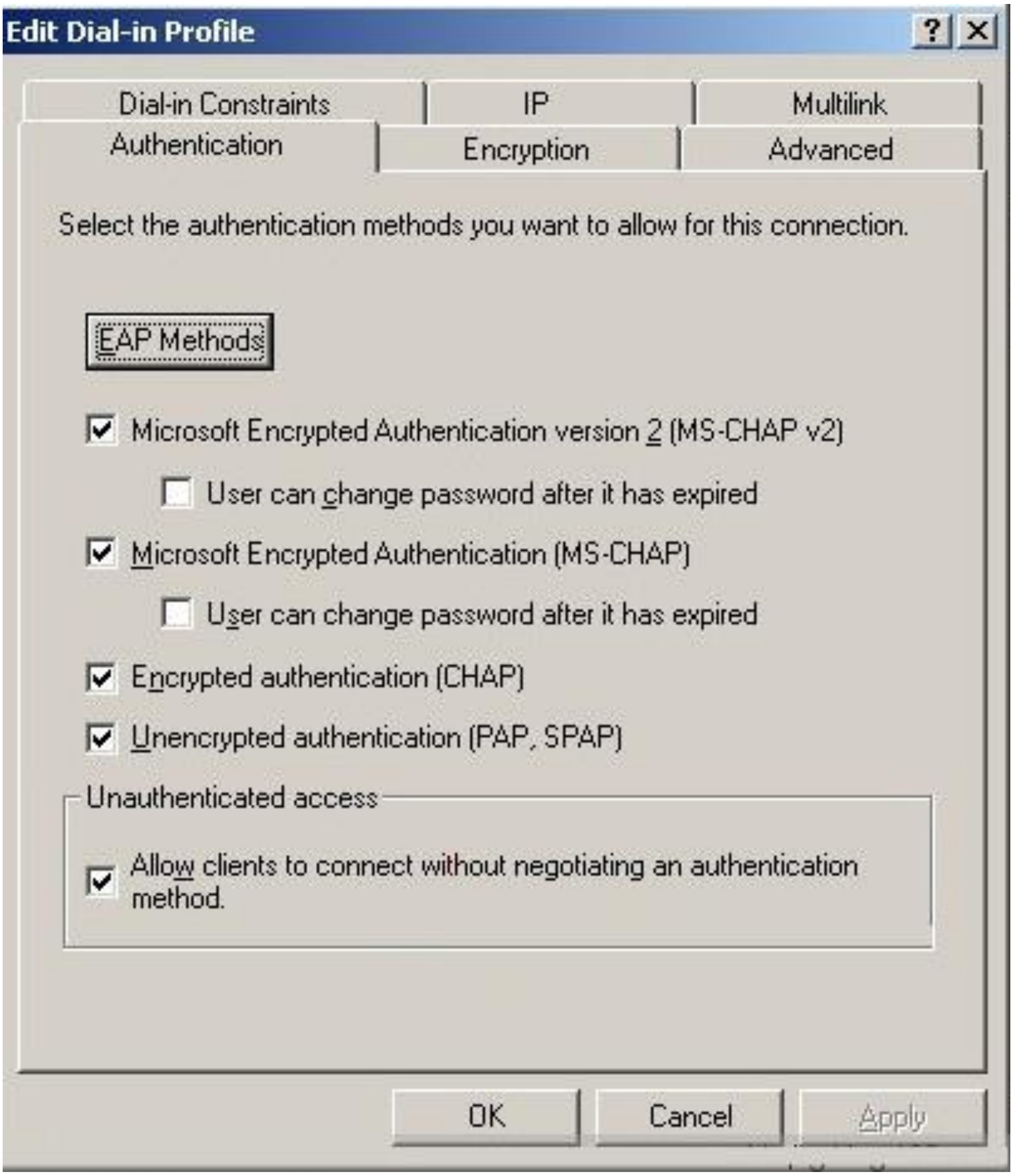
○ Deny remote access permission

● Grant remote access permission

(10) Select **Wireless – Other**, click **Add**, and click **OK**.



(11) Click **Edit Profile**, click the **Authentication** tab, configure settings as shown in the following figure, and click **OK**.



Select the authentication methods you want to allow for this connection.

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☐ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

☑ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☑ Allow clients to connect without negotiating an authentication method.

(12) When a message appears, click **No**.

3. Configure user information.

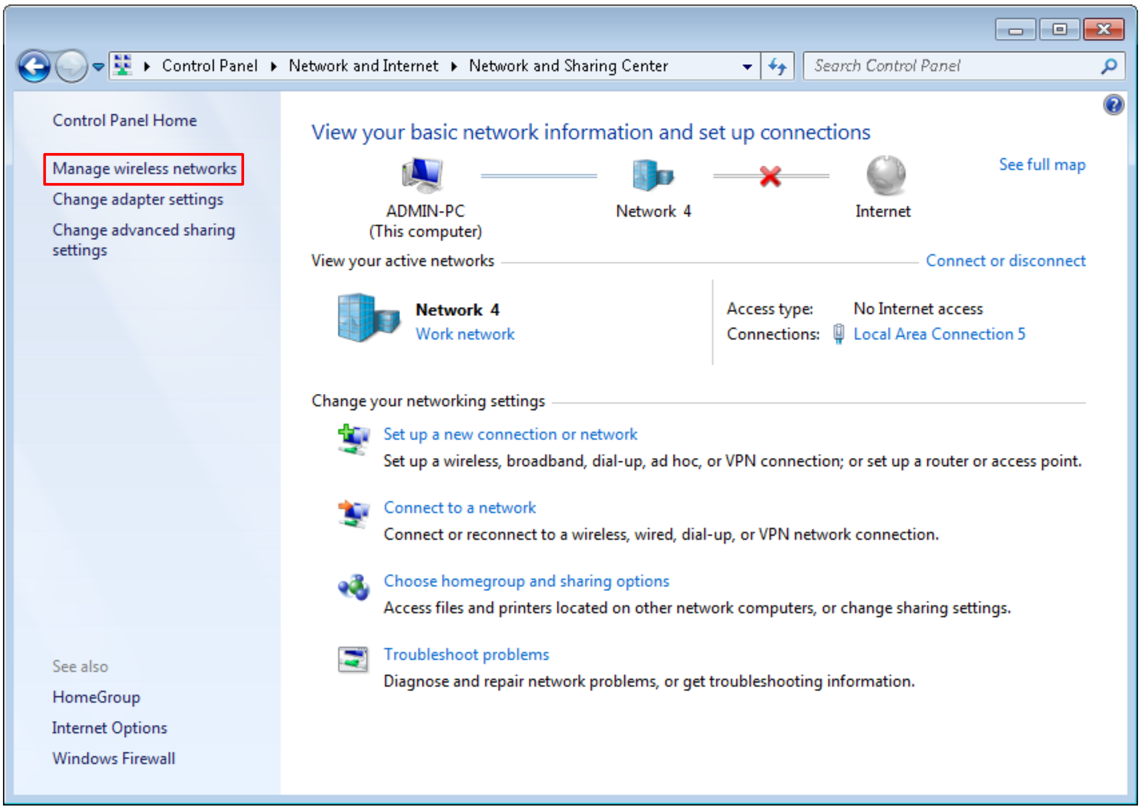
Create a user and add the user to group **802.1x**.

Step 3 Configure your wireless device.

NOTE

Windows 7 is taken as an example to describe the procedure.

(1) Choose **Start** > **Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



View your basic network information and set up connections

View your active networks

Network 4
Work network

Access type: No Internet access
Connections: Local Area Connection 5

Change your networking settings

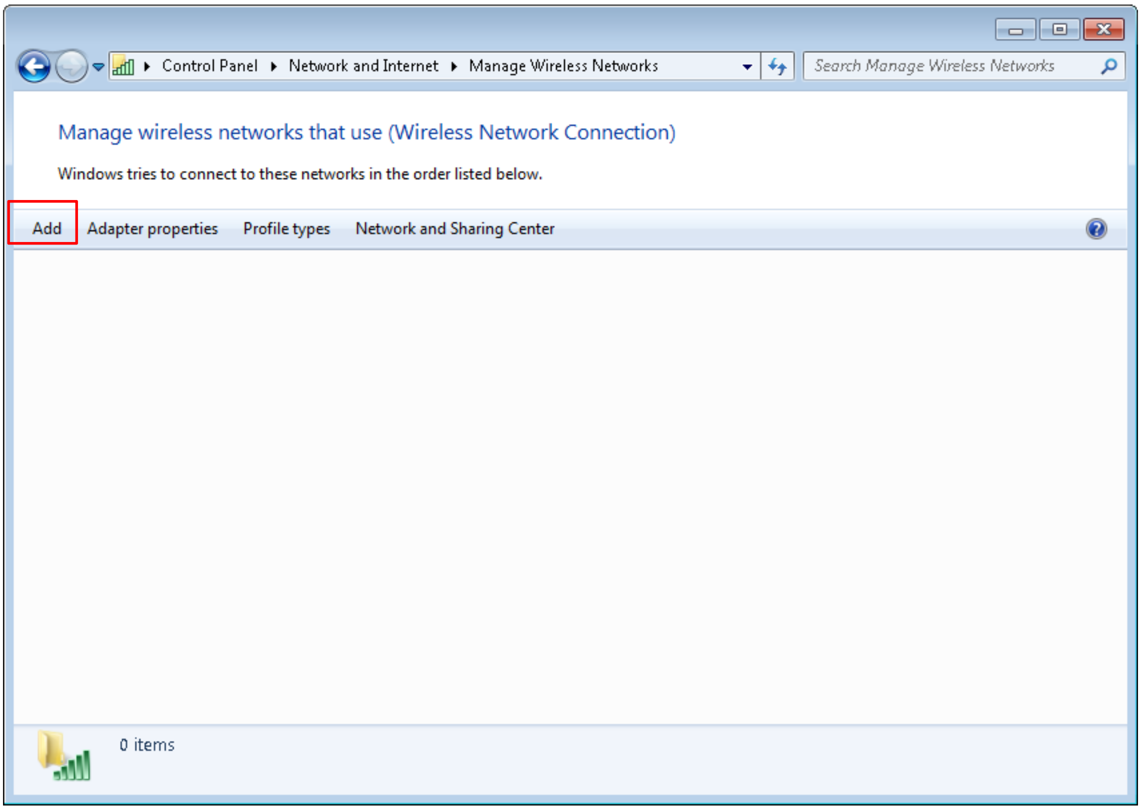
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

(2) Click **Add**.

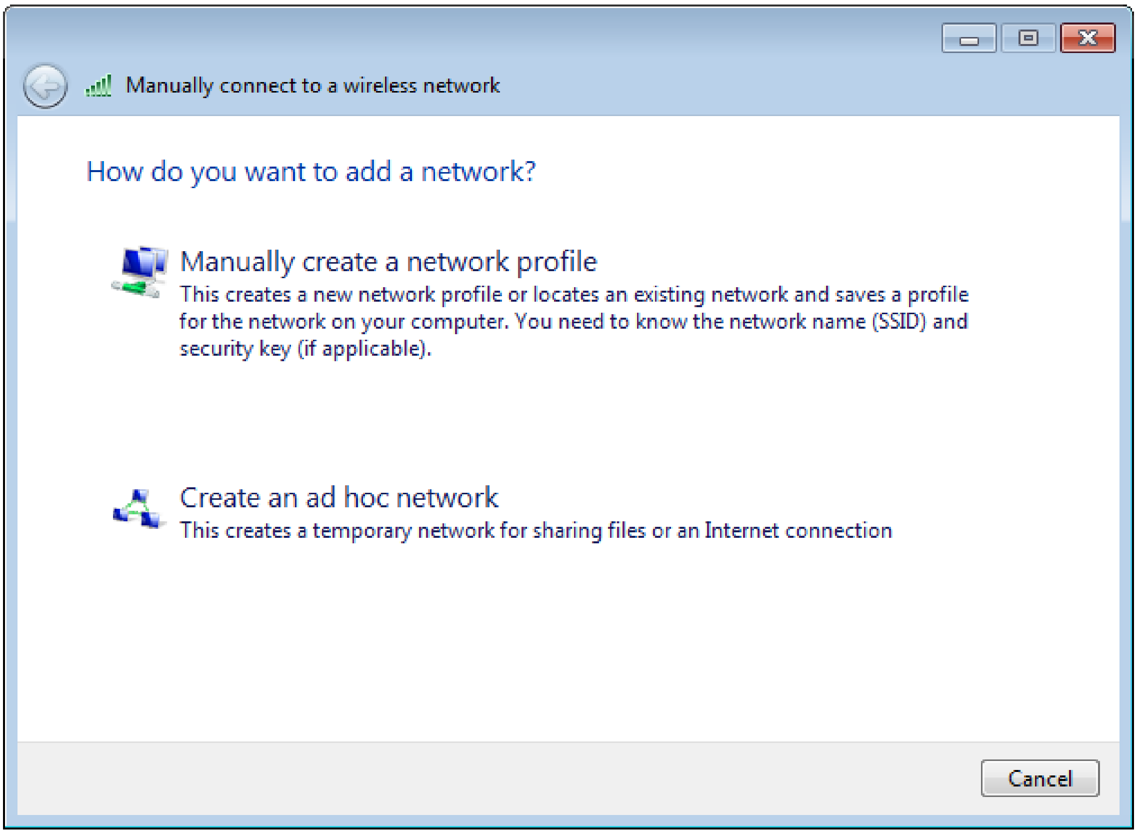

Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Networks
Add
Adapter properties
Profile types
Network and Sharing Center

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

0 items

(3) Click **Manually create a network profile**.



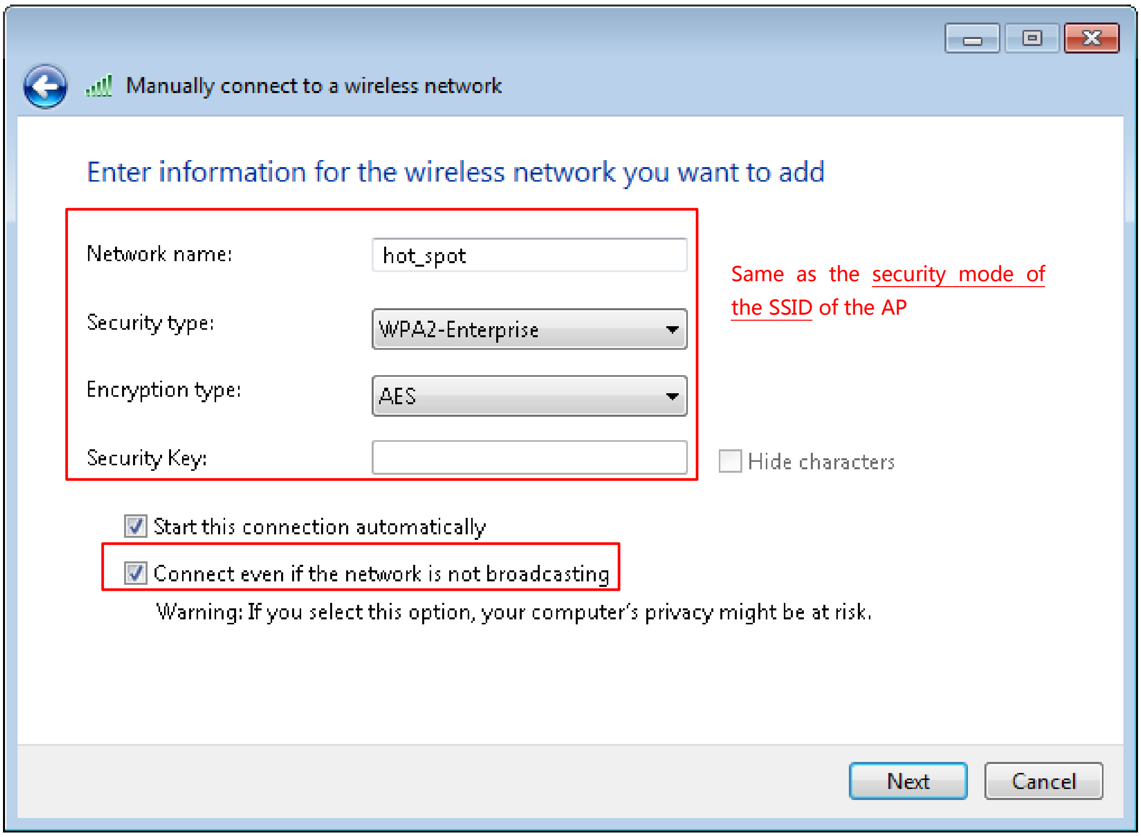
Manually connect to a wireless network

How do you want to add a network?

Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

(4) Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: hot_spot

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

□ Hide characters

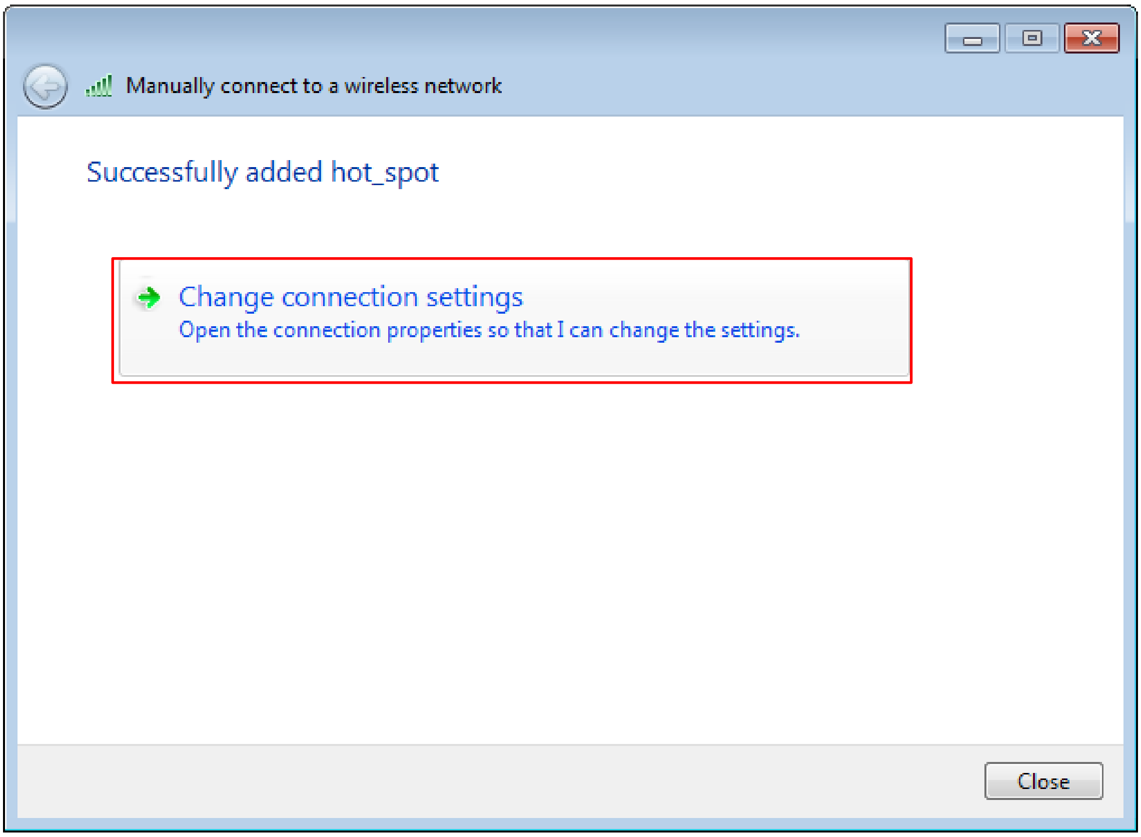
☑ Start this connection automatically

☑ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Same as the security mode of the SSID of the AP

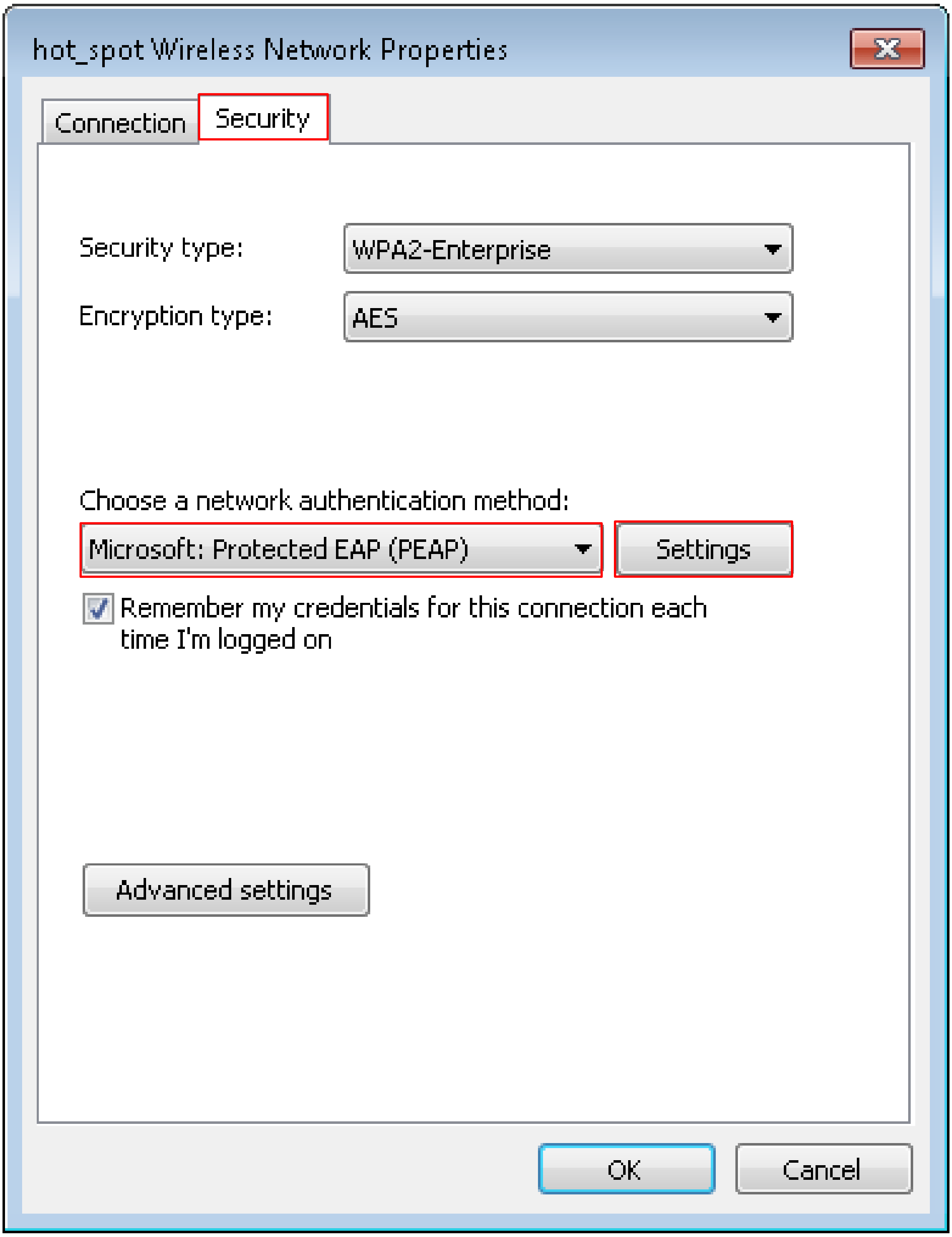
(5) Click **Change connection settings**.



Successfully added hot_spot

Change connection settings
Open the connection properties so that I can change the settings.

(6) Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



Security type: WPA2-Enterprise

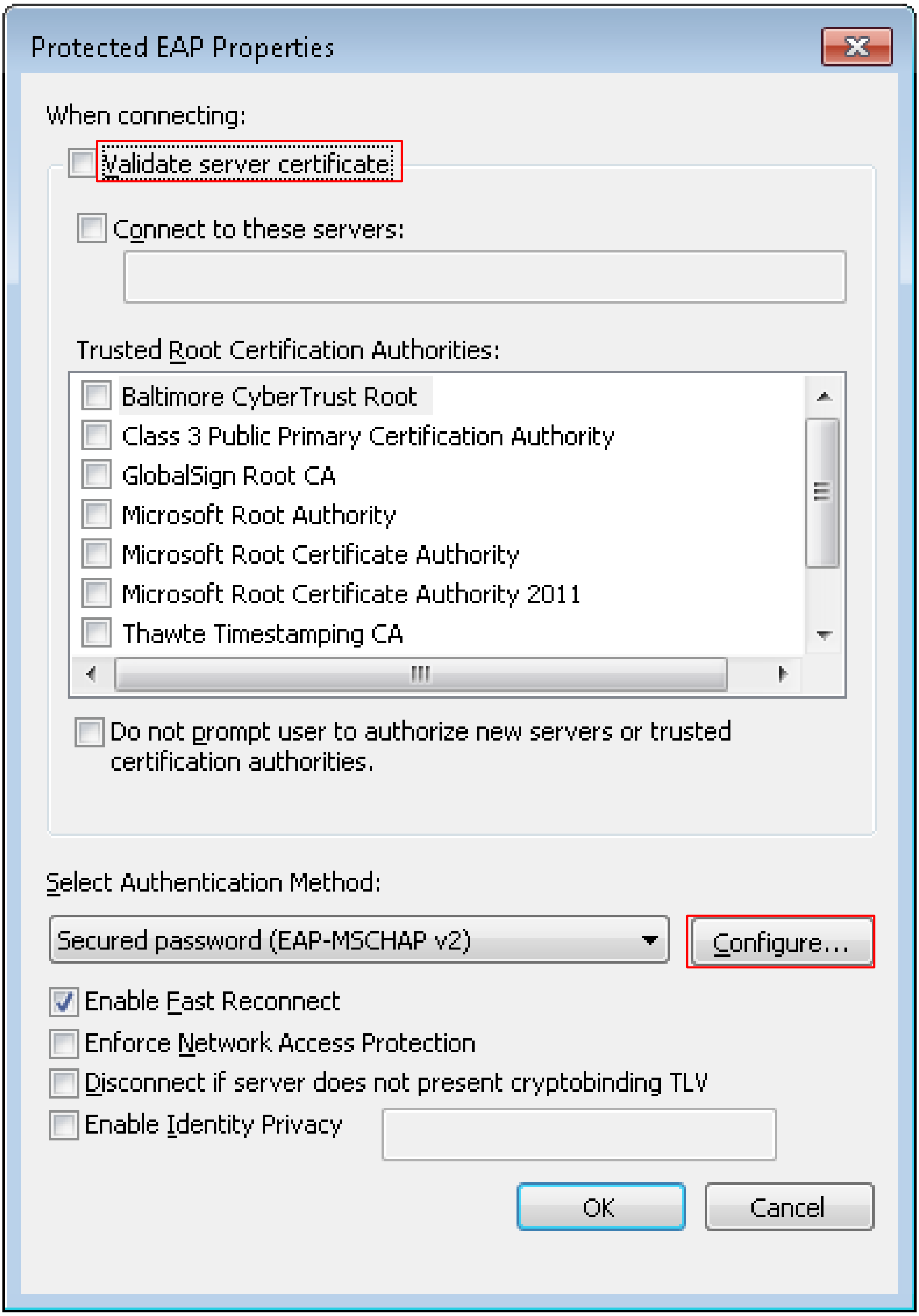
Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

(7) Deselect **Validate server certificate** and click **Configure**.



Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

- □ Baltimore CyberTrust Root
- □ Class 3 Public Primary Certification Authority
- □ GlobalSign Root CA
- □ Microsoft Root Authority
- □ Microsoft Root Certificate Authority
- □ Microsoft Root Certificate Authority 2011
- □ Thawte Timestamping CA

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

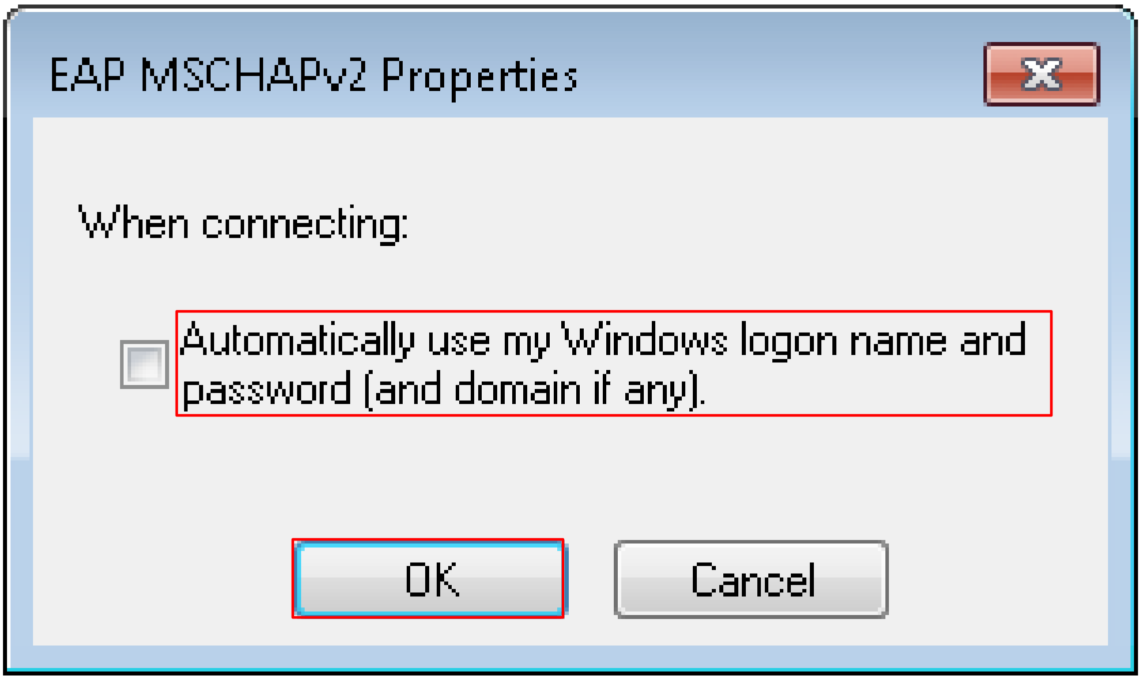
☑ Enable Fast Reconnect

□ Enforce Network Access Protection

□ Disconnect if server does not present cryptobinding TLV

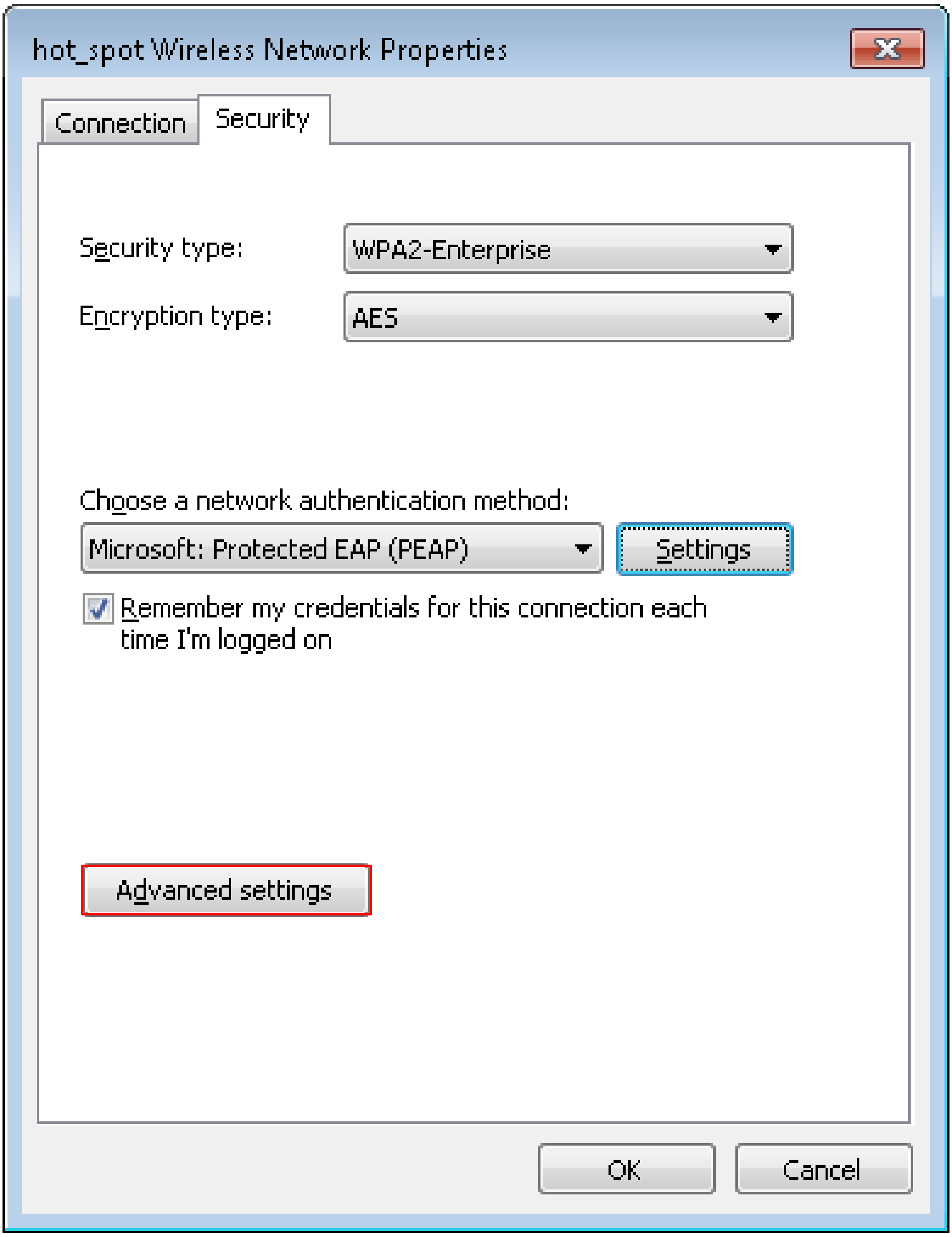
□ Enable Identity Privacy

(8) Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



EAP MSCHAPv2 Properties
When connecting:
□ Automatically use my Windows logon name and password (and domain if any).
OK
Cancel

(9) Click **Advanced settings**.



hot_spot Wireless Network Properties

Security type: WPA2-Enterprise

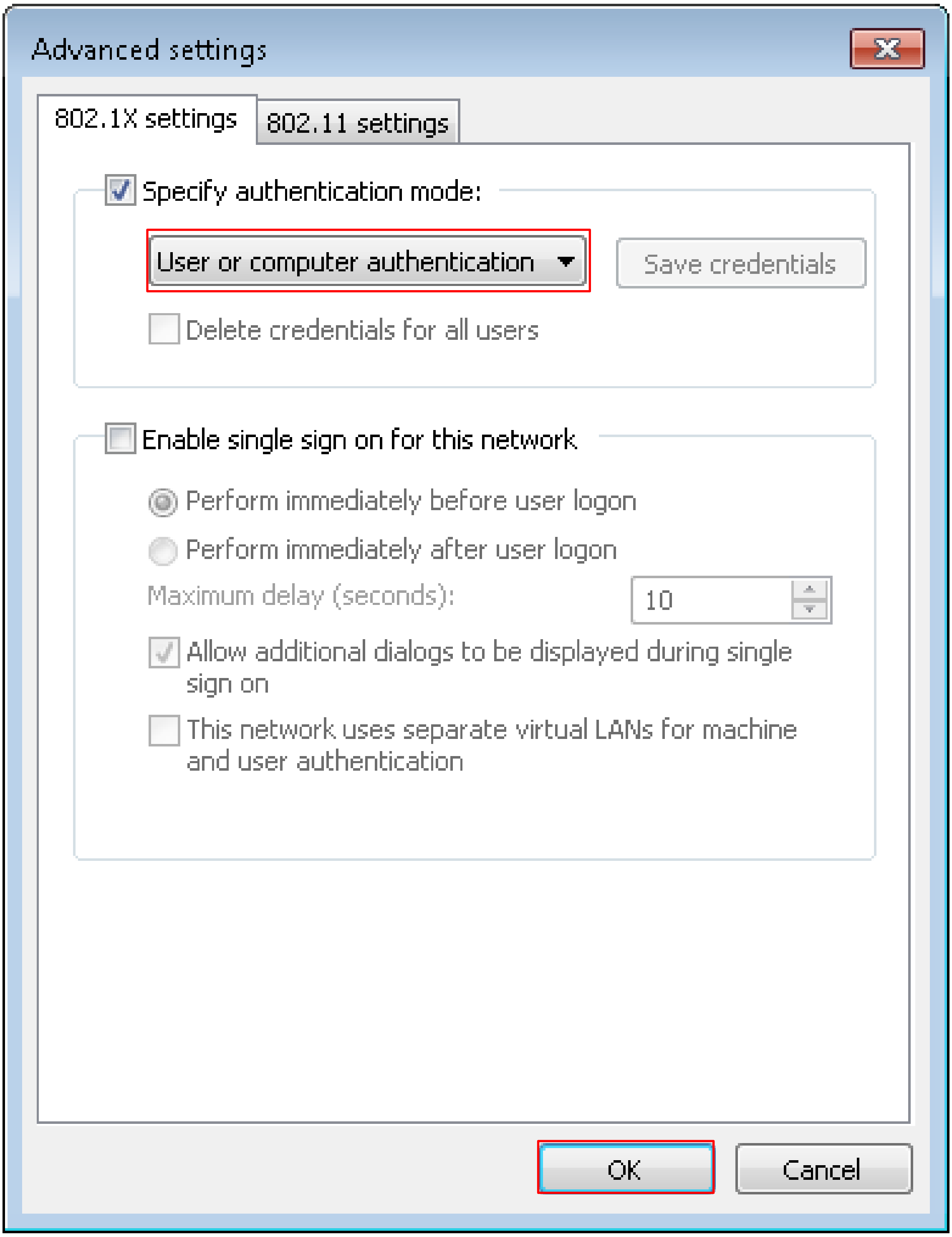
Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

(10) Select **User or computer authentication** and click **OK**.



Advanced settings

802.1X settings | 802.11 settings

☑ Specify authentication mode:

User or computer authentication ▾ | Save credentials

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

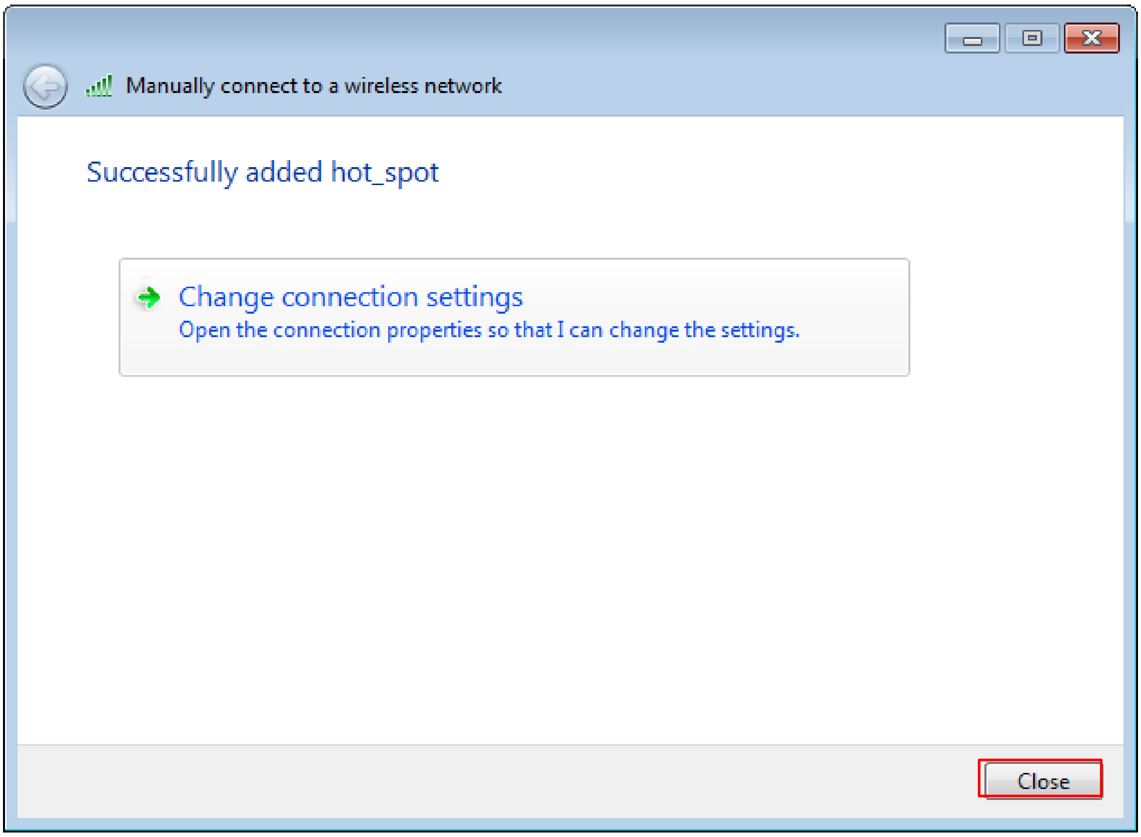
○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

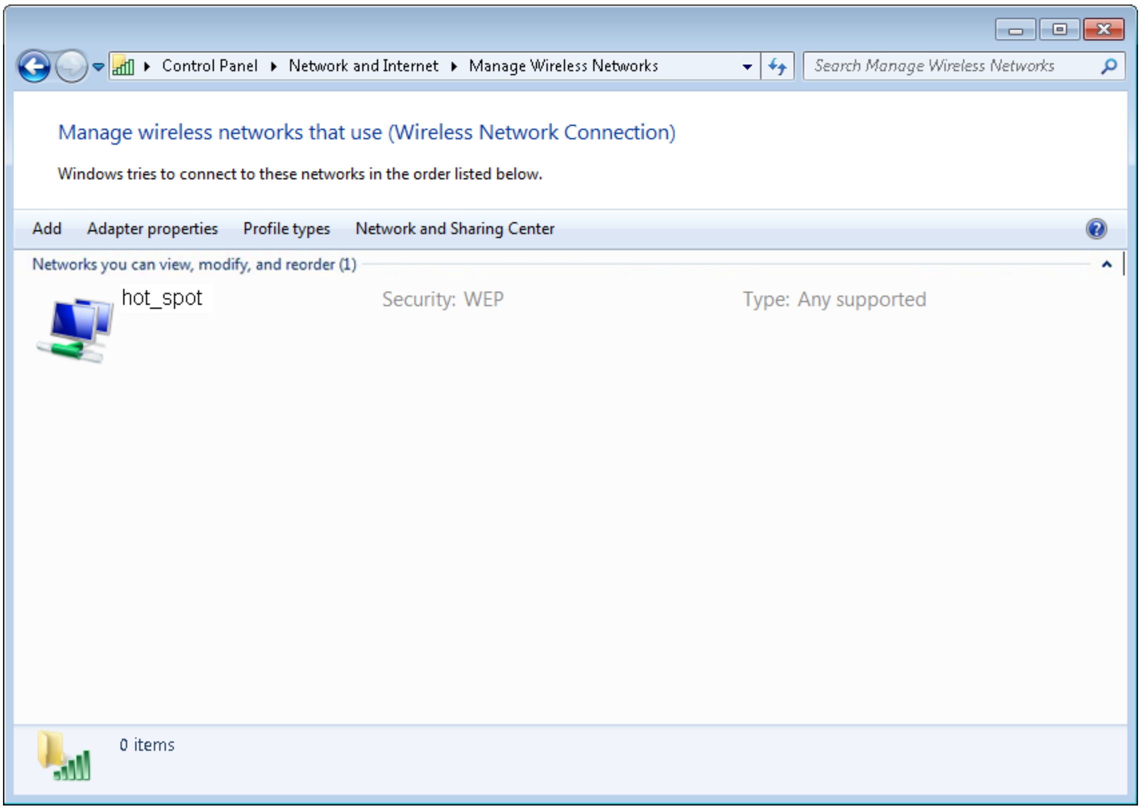
(11) Click **Close**.



Successfully added hot_spot

Change connection settings

Open the connection properties so that I can change the settings.



Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Networks

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

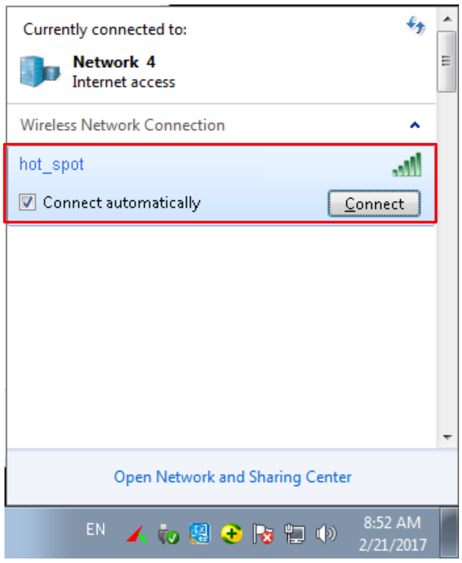
Add
Adapter properties
Profile types
Network and Sharing Center

Networks you can view, modify, and reorder (1)

hot_spot Security: WEP Type: Any supported

0 items

(12) Click the network icon in the lower-right corner of the desktop, select the wireless network of the AP, such as **hot_spot** in this example, and click **Connect**.



Currently connected to:

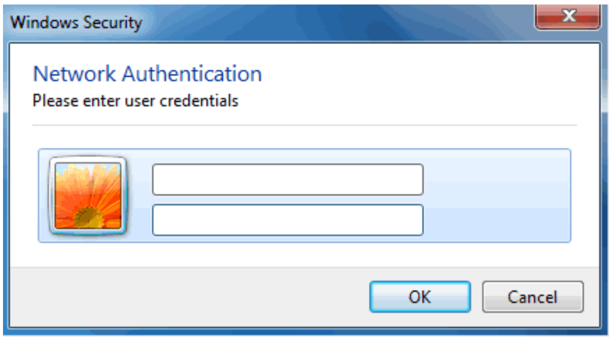
Network 4
Internet access

Wireless Network Connection

hot_spot

☑ Connect automatically

(13) In the **Windows Security** dialog box that appears, enter the user name and password set on the RADIUS server and click **OK**.



Windows Security

Network Authentication

Please enter user credentials

---End

- Verification

Wireless devices can connect to the wireless network hot_spot.

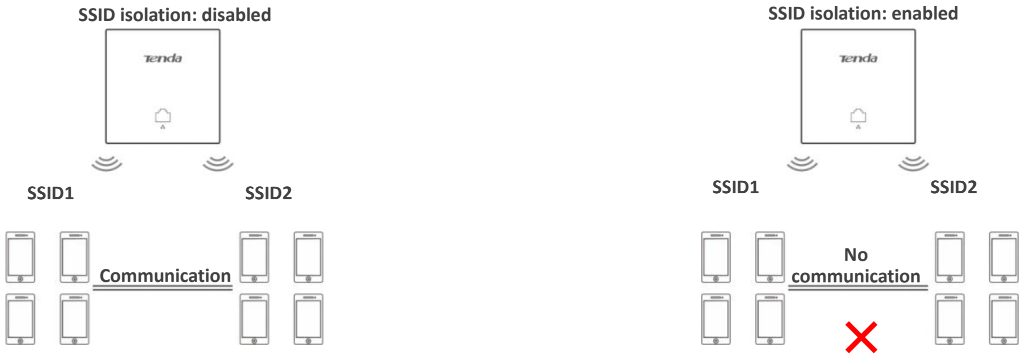
7.2 RF Settings

7.2.1 Overview

The RF module is used to set RF parameters of the AP. This section describes some functions of the module.

SSID Isolation

This function isolates the wireless clients connected to different wireless networks of the AP. For example, if user 1 connects to the wireless network corresponding to SSID1, whereas user 2 connects to the wireless network corresponding to SSID2, the two users cannot communicate with each other after SSID isolation is implemented.



WMM

802.11 networks offer wireless access services based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) channel competition mechanism, which allows all wireless clients to fairly compete for channels. All the services implemented over wireless networks share the same channel competition parameters. Nevertheless, different services usually have different requirements for bandwidth, delay, and jitter. This requires wireless networks to offer accessibility based on the services implemented over the networks.

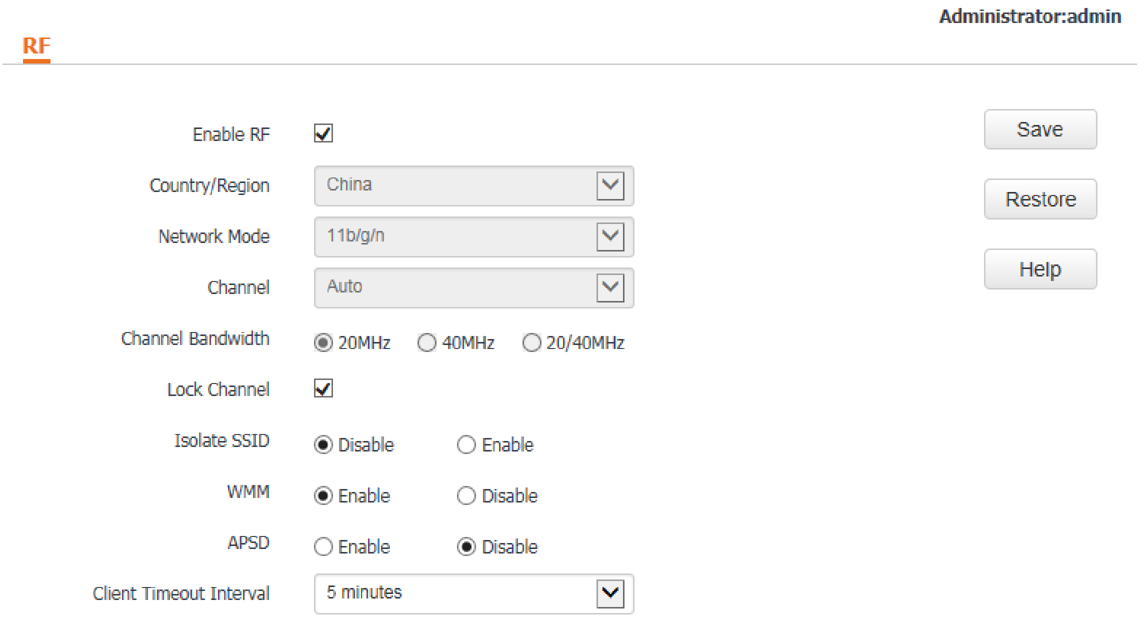
WMM is a wireless QoS protocol used to ensure that packets with high priorities are transmitted first. This ensures better voice and video service experience over wireless networks.

7.2.2 Changing the RF Settings

Step 1 Choose **Wireless** > **RF**.

Step 2 Change the parameters as required. Generally, you only need to change the **Enable RF**, **Channel**, and **Lock Channel** settings.

Step 3 Click **Save**.



Enable RF ☑

Country/Region China

Network Mode 11b/g/n

Channel Auto

Channel Bandwidth ● 20MHz ○ 40MHz ○ 20/40MHz

Lock Channel ☑

Isolate SSID ● Disable ○ Enable

WMM ● Enable ○ Disable

APSD ○ Enable ● Disable

Client Timeout Interval 5 minutes

---End

Parameter description

Parameter	Description
Enable RF	It specifies whether to enable the wireless function of the AP.

Parameter	Description
Country/Region	It specifies the country or region where the AP is used. This parameter helps comply with channel regulations of the country or region. The default value is **China**.
Network Mode	It specifies the wireless network mode of the AP. The available options include **11b**, **11g**, **11b/g**, and **11b/g/n**. This parameter can be set if **Lock Channel** is not selected. - **11b**: The AP works in 802.11b mode and only wireless devices compliant with 802.11b can connect to the wireless networks of the AP. - **11g**: The AP works in 802.11g mode and only wireless devices compliant with 802.11g can connect to the wireless networks of the AP. - **11b/g**: The AP works in 802.11b/g mode and only wireless devices compliant with 802.11b or 802.11g can connect to the wireless networks of the AP. - **11b/g/n**: The AP works in 802.11b/g/n mode. Wireless devices compliant with 802.11b or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n can connect to the wireless networks of the AP.
Channel	It specifies the operating channel of the AP. This parameter can be set if Lock Channel is not selected. **Auto**: It indicates that the AP automatically adjusts its operating channel according to the ambient environment.
Channel Bandwidth	It specifies the wireless channel bandwidth of the AP. This parameter can be set if the AP works in 802.11 b/g/n mode and Lock Channel is not selected. - **20MHz**: It indicates that the AP can use only 20MHz channel bandwidth. - **40MHz**: It indicates that the AP uses 40MHz channel bandwidth first, and changes to 20HMz channel bandwidth if severe channel competition occurs in the ambient environment. - **20/40MHz**: It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment.
Expansion Channel	It specifies the wireless expansion channel of the AP. This parameter can be set if the channel bandwidth of the AP is set to **40MHz** or **20/40MHz** and Lock Channel is not selected.
Lock Channel	It is used to lock the channel settings of the AP. If this parameter is selected, channel settings including **Country/Region**, **Network Mode**, **Channel**, **Channel Bandwidth**, and **Expansion Channel** cannot be changed.
Isolate SSID	It specifies whether to isolate the wireless clients connected to the AP with different SSIDs. - **Disable**: It indicates that the wireless clients connected to the AP with different SSIDs can communicate with each other. - **Enable**: It indicates that the wireless clients connected to the AP with different SSID cannot communicate with each other. This improves wireless network security.
WMM	It specified whether to enable the Wi-Fi Multimedia (WMM) function. If the function is enabled, the AP forwards video and audio data with top priority. To improve multimedia data (such as data of online videos) transmission performance of the AP, enable this function.

Parameter	Description
APSD	It specifies whether to enable the Automatic Power Save Delivery (APSD) function. It helps reduce power consumption of the AP. By default, it is disabled.
Client Timeout Interval	It specifies the timeout interval of clients. After a wireless client connects to the AP, the AP disconnects from the wireless client if no data is exchanged between them within the interval.

7.3 Channel Scan

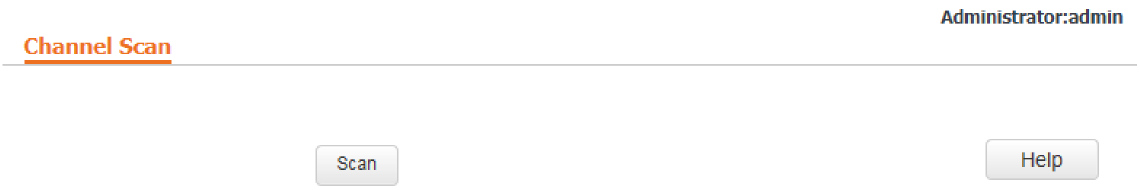
7.3.1 Overview

This function enables you to learn about the wireless signals near the AP, including information about SSID, MAC address, channel, and signal strength. The information helps you choose a relatively idle channel for the AP to improve wireless transmission efficiency.

7.3.2 Scanning Channels

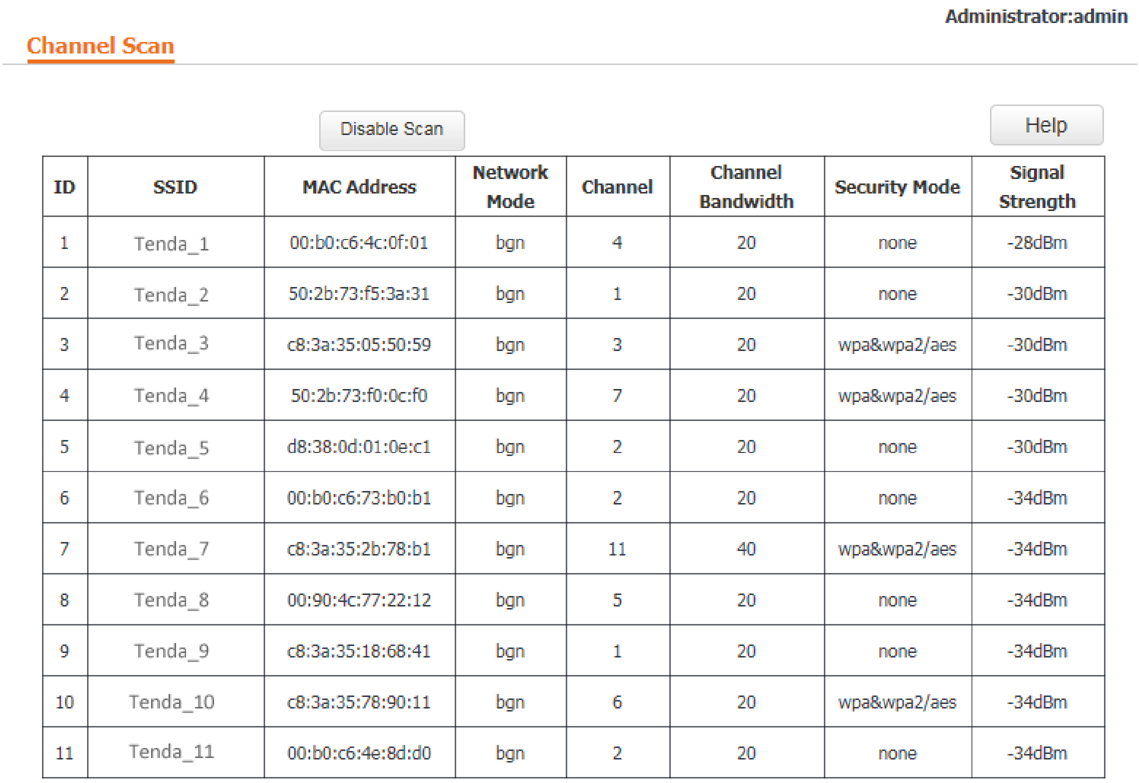
Step 1 Choose **Wireless** > **Channel Scan**.

Step 2 Click **Scan**.



---End

The following figure shows the scan result.



ID	SSID	MAC Address	Network Mode	Channel	Channel Bandwidth	Security Mode	Signal Strength
1	Tenda_1	00:b0:c6:4c:0f:01	bgn	4	20	none	-28dBm
2	Tenda_2	50:2b:73:f5:3a:31	bgn	1	20	none	-30dBm
3	Tenda_3	c8:3a:35:05:50:59	bgn	3	20	wpa&wpa2/aes	-30dBm
4	Tenda_4	50:2b:73:f0:0c:f0	bgn	7	20	wpa&wpa2/aes	-30dBm
5	Tenda_5	d8:38:0d:01:0e:c1	bgn	2	20	none	-30dBm
6	Tenda_6	00:b0:c6:73:b0:b1	bgn	2	20	none	-34dBm
7	Tenda_7	c8:3a:35:2b:78:b1	bgn	11	40	wpa&wpa2/aes	-34dBm
8	Tenda_8	00:90:4c:77:22:12	bgn	5	20	none	-34dBm
9	Tenda_9	c8:3a:35:18:68:41	bgn	1	20	none	-34dBm
10	Tenda_10	c8:3a:35:78:90:11	bgn	6	20	wpa&wpa2/aes	-34dBm
11	Tenda_11	00:b0:c6:4e:8d:d0	bgn	2	20	none	-34dBm

7.4 Advanced Settings

7.4.1 Overview

This module is used to set the RF performance optimization parameters of the AP.

7.4.2 Changing the Advanced Settings

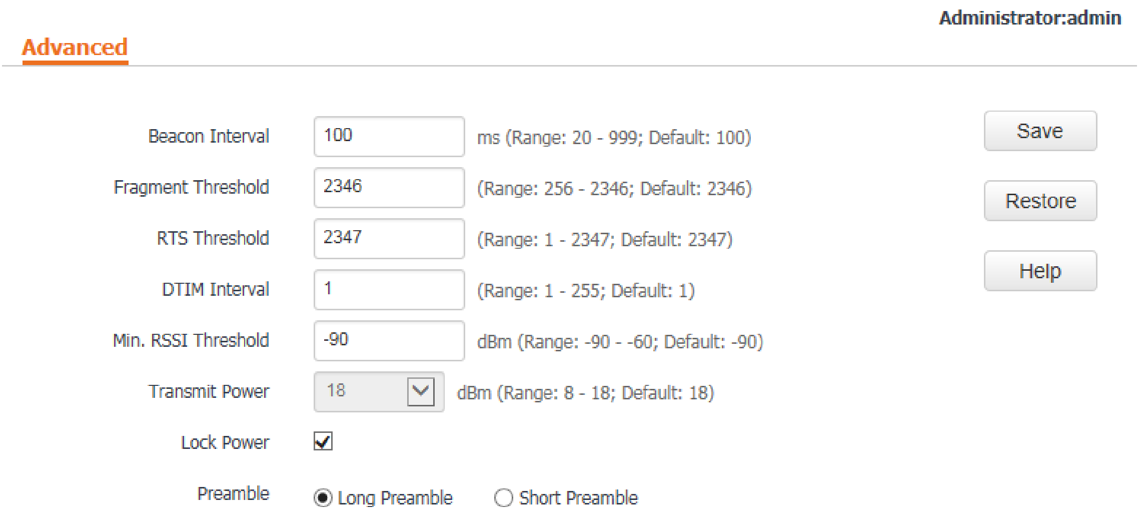
NOTE

It is recommended that you change the settings only under the instruction of professional personnel, so as to prevent decreasing the wireless performance of the AP.

Step 1 Choose **Wireless** > **Advanced**.

Step 2 Change the parameter settings as required.

Step 3 Click **Save**.


Administrator:admin

Advanced

Beacon Interval	100	ms (Range: 20 - 999; Default: 100)
Fragment Threshold	2346	(Range: 256 - 2346; Default: 2346)
RTS Threshold	2347	(Range: 1 - 2347; Default: 2347)
DTIM Interval	1	(Range: 1 - 255; Default: 1)
Min. RSSI Threshold	-90	dBm (Range: -90 - -60; Default: -90)
Transmit Power	18	dBm (Range: 8 - 18; Default: 18)
Lock Power	☑	
Preamble	● Long Preamble	○ Short Preamble

---End

Parameter description

Parameter	Description
Beacon Interval	It specifies the interval for transmitting the Beacon frame. The value range is 20 to 999. The unit is millisecond. The Beacon frame is transmitted at the specified interval to announce the presence of a wireless network. Generally, a smaller interval enables wireless clients to connect to the AP more quickly, while a larger interval ensures higher data transmission efficiency.
Fragment Threshold	It specifies the threshold of a fragment. The value range is 256 to 2346. The default value is **2346**. The unit is byte. Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented. In case of a high error rate, you can reduce the threshold to enable the AP to resend only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment without interference, you can increase the threshold to reduce the number of acknowledgement times, so as to increase the frame throughput.
RTS Threshold	It specifies the frame length threshold for triggering the RTS/CTS mechanism. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The value range is 1 to 2347. The unit is byte. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	It specifies the interval for transmitting the Delivery Traffic Indication Message (DTIM) frame. The value range is 1 to 255. The unit is Beacon. A countdown starts from this value. The AP transmits broadcast and multicast frames in its cache only when the countdown reaches zero. For example, if **DTIM Interval** is set to **1**, the AP transmits all cached frames after each

Parameter	Description
	beacon frame is transmitted.
Min. RSSI Threshold	It specifies the minimum strength of received signals acceptable to the AP. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to the AP. If there are multiple APs, an appropriate value of this parameter ensures that wireless clients connect to the APs with strong signals.
Transmit Power	It specifies the transmit power of the AP. This parameter can be set if Lock Power is not selected. A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the wireless network performance and security.
Lock Power	It specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.
Preamble	It specifies whether to use long preamble or short preamble. A preamble is a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. By default, the **Long Preamble** option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the **Short Preamble** option.

7.5 Access Control

7.5.1 Overview

It specifies, based on MAC address filter rules, the wireless devices that can or cannot access the wireless networks of the AP.

The AP supports the following MAC address filter rules:

- **Disable**: It indicates that access control is disabled. In this case, all wireless devices can access the wireless networks of the AP.
- **Allow**: It indicates that only the wireless devices with the specified MAC addresses can access the wireless networks of the AP.
- **Disallow**: It indicates that only the wireless devices with the specified MAC addresses cannot access the wireless networks of the AP.

7.5.2 Configuring Access Control

Step 1 Choose **Wireless** > **Access Control**.

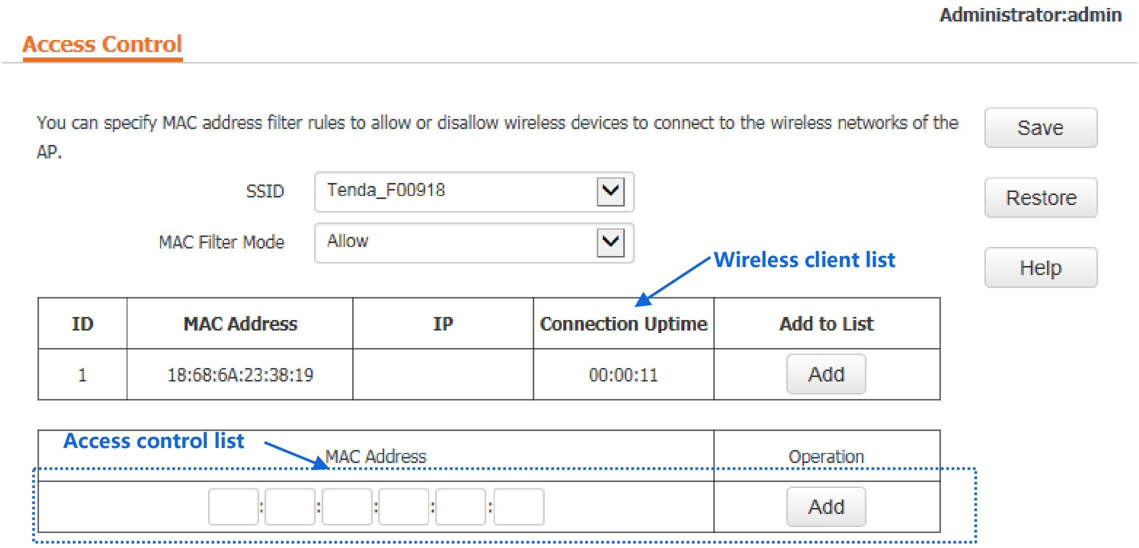
Step 2 From the **SSID** drop-down list box, select the SSID of the wireless network on which access control must be implemented.

Step 3 Select an access control mode from the **MAC Filter Mode** drop-down list box.

Step 4 If you select **Allow** or **Disallow**, enter the MAC addresses to control in the access control list and click **Add**.
If a wireless device to be controlled has been connected to the AP, you can click **Add** corresponding to

the device in the wireless client list to directly add it to the access control list.

Step 5 Click **Save**.



Administrator:admin

Access Control

You can specify MAC address filter rules to allow or disallow wireless devices to connect to the wireless networks of the AP.

SSID: Tenda_F00918

MAC Filter Mode: Allow

ID	MAC Address	IP	Connection Uptime	Add to List
1	18:68:6A:23:38:19		00:00:11	Add

MAC Address	Operation
: : : : :	Add

---End

Parameter description

Parameter	Description
SSID	It specifies the SSID that requires wireless client access control.
MAC Filter Mode	It specifies the mode for filtering MAC addresses. • **Disable**: It indicates that access control is disabled. • **Allow**: It indicates that only the wireless clients on the access control list can connect to the AP with the selected SSID. • **Disallow**: It indicates that only the wireless clients on the access control list cannot connect to the AP with the selected SSID.

7.5.3 Example of Configuring Access Control

- Networking requirement

A wireless network whose SSID is Home has been set up in a large apartment. Only family members are allowed to connect to the wireless network.

The family members have three wireless devices whose MAC addresses are C8:3A:35:00:00:01, C8:3A:35:00:00:02, and C8:3A:35:00:00:03.

- Configuration procedure

Step 1 Choose **Wireless** > **Access Control**.

Step 2 Select **Home** from the **SSID** drop-down list box.

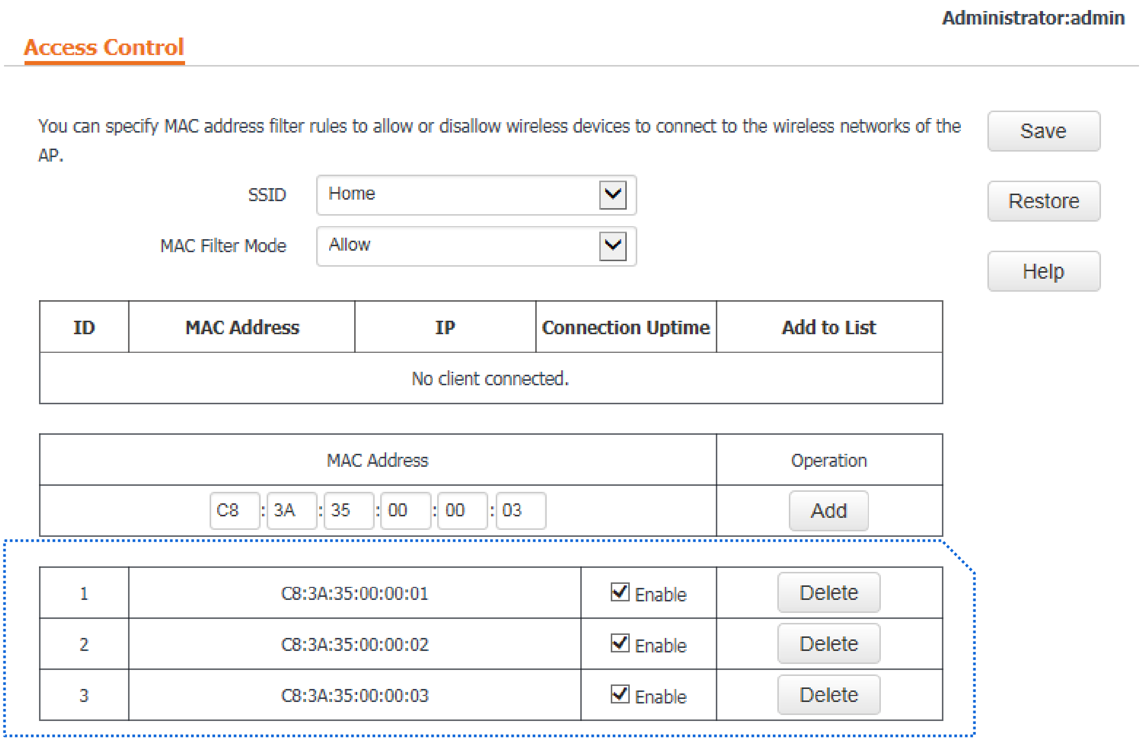
Step 3 Select **Allow** from the **MAC Filter Mode** drop-down list box.

Step 4 Enter **C8:3A:35:00:00:01** in the **MAC Address** text box and click **Add**. Repeat this step to add **C8:3A:35:00:00:02** and **C8:3A:35:00:00:03** as well.

Step 5 Click **Save**.

---End

The following figure shows the configuration.



Administrator:admin

Access Control

You can specify MAC address filter rules to allow or disallow wireless devices to connect to the wireless networks of the AP.

SSID: Home

MAC Filter Mode: Allow

ID	MAC Address	IP	Connection Uptime	Add to List
No client connected.				

MAC Address	Operation
C8 : 3A : 35 : 00 : 00 : 03	Add

1	C8:3A:35:00:00:01	☑ Enable	Delete
2	C8:3A:35:00:00:02	☑ Enable	Delete
3	C8:3A:35:00:00:03	☑ Enable	Delete

- Verification

  Only the specified wireless devices can connect to the **Home** wireless network.

7.6 QVLAN Settings

7.6.1 Overview

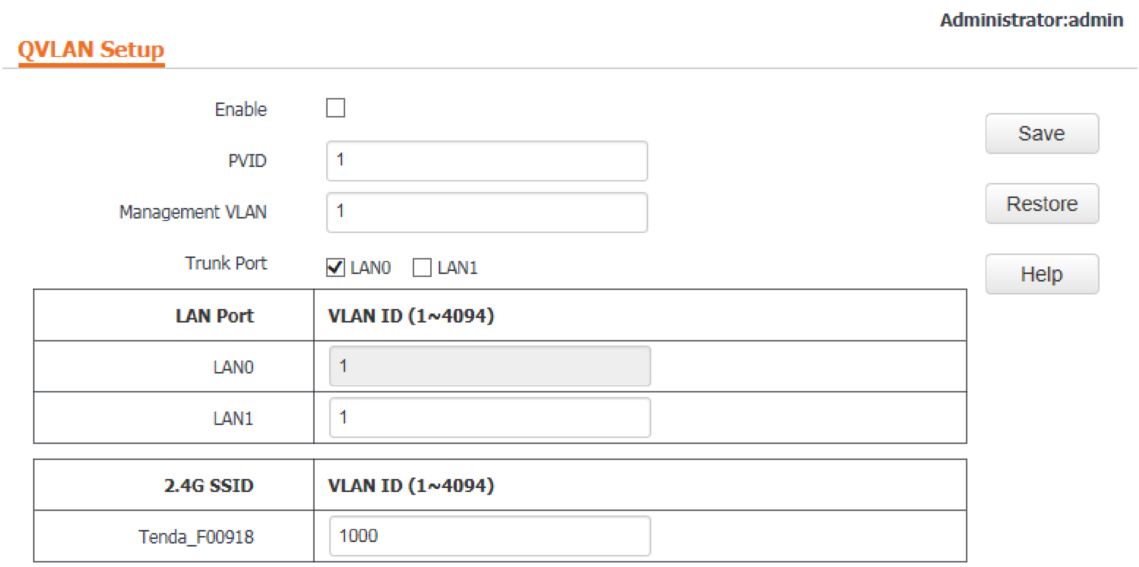
The AP supports 802.1Q VLANs and is applicable in a network environment where 802.1Q VLANs have been defined. By default, the QVLAN function is disabled.

7.6.2 Configuring the QVLAN Function

Step 1 Choose **Wireless** > **QVLAN Setup**.

Step 2 Change the parameters as required. Generally, you only need to change the **Enable** and **2.4G SSID VLAN ID** settings.

Step 3 Click **Save**.



Administrator:admin

QVLAN Setup

Enable	□
PVID	1
Management VLAN	1
Trunk Port	☑ LAN0 □ LAN1

LAN Port	VLAN ID (1~4094)
LAN0	1
LAN1	1

2.4G SSID	VLAN ID (1~4094)
Tenda_F00918	1000

---End

Parameter description

Parameter	Description
Enable	It specifies whether to enable the QVLAN function of the AP. By default, it is disabled.
PVID	It specifies the ID of the default native VLAN of the trunk port of the AP. The default value is **1**.
Management VLAN	It specifies the ID of the AP management VLAN. The default value is **1**. After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
Trunk Port	It specifies the LAN port used as a trunk port of the AP. The default value is **LAN0**. Traffic of all VLANs can pass through a trunk port. NOTE If the QVLAN function is enabled, set at least one LAN port as a trunk port. **LAN0** indicates the LAN port at the rear of the AP, whereas **LAN1** indicates the LAN port at the front of the AP.
LAN Port	It specifies the LAN ports of the AP, including LAN0 and LAN1.
VLAN ID	It specifies the VLAN ID corresponding to a LAN port used as an access port.
2.4G SSID	It specifies the currently enabled SSIDs of the AP.
VLAN ID	It specifies VLAN IDs corresponding to SSIDs. The default value is **1000**. The value range is 1 to 4094. After the QVLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID and VLAN ID of an access port are the same.

If the QVLAN function is enabled, tagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the VID in the data, whereas untagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the PVID of the port that receives the data.

The following table describes how ports of different link types process transmitted and received data.

Port	Method to Process Received Data		Method to Process Transmitted Data
	Tagged Data	Untagged Data	
Access	Forward the data to other ports of the VLAN corresponding to the VID in the data.	Forward the data to the other ports of the VLAN corresponding to the PVID of the port that receives the data	Transmit data after removing tags from the data.
Trunk			If the VID and PVID of a port are the same, transmit data after removing tags from the data. If the VID and PVID of a port are different, transmit data without removing tags from the data.

7.6.3 Example of Configuring QVLAN Settings

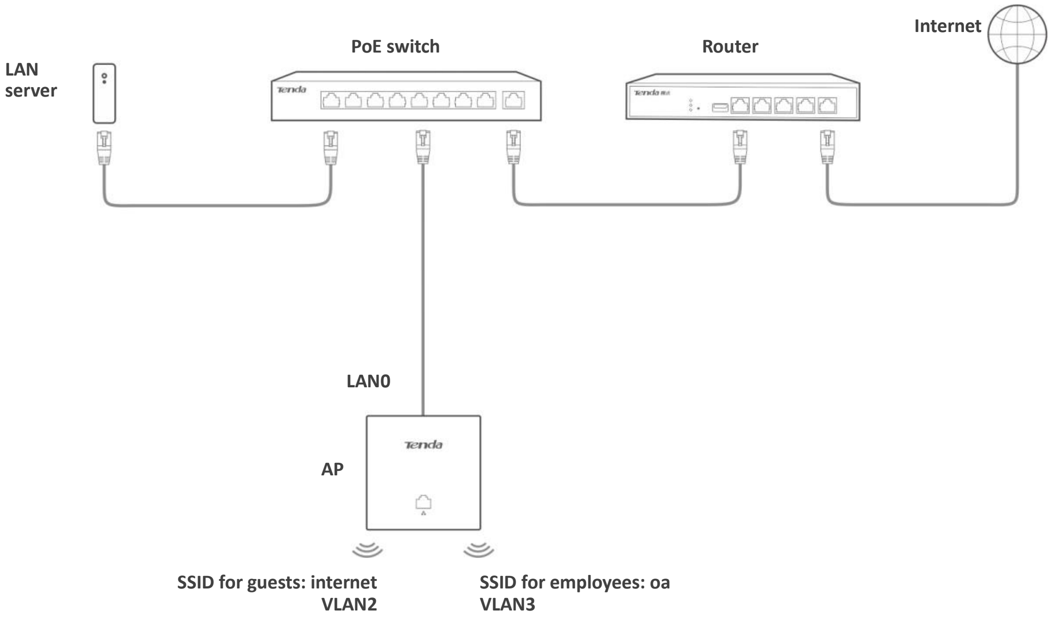
- Networking requirement

  A hotel has the following wireless network coverage requirements:

  - Guests are connected to VLAN 2 and can access only the internet.
  - Employees are connected to VLAN 3 and can access only the LAN.

  Assume that the SSID of the wireless network for guests is **internet** and the SSID of the wireless network for employees is **oa**.

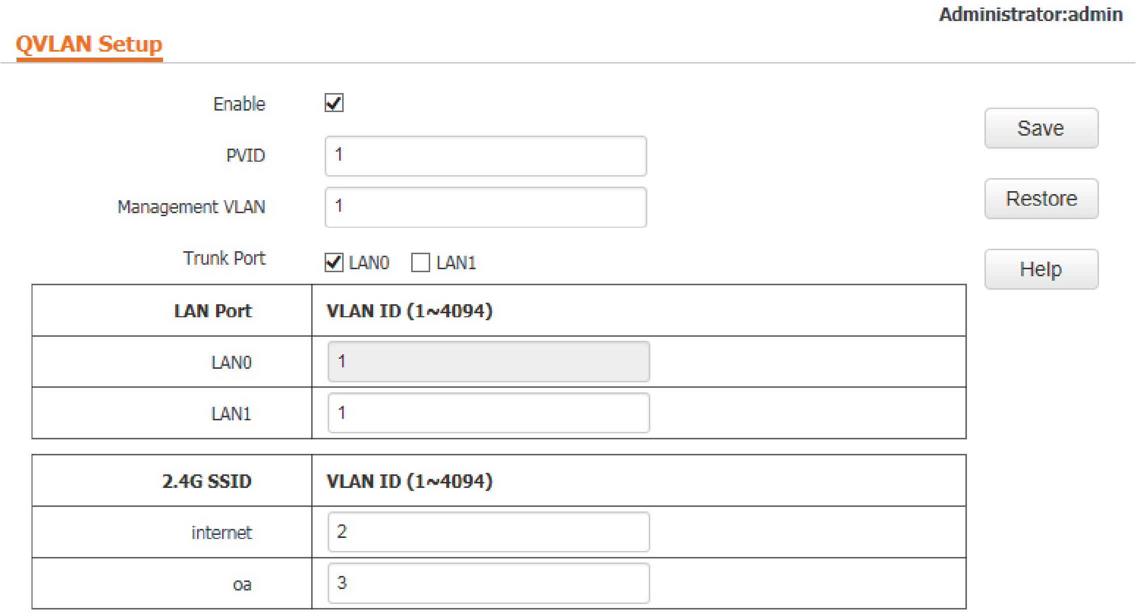
- Network topology



- Configuration procedure

Step 1 Configure the AP.

1. Log in to the web UI of the AP and choose **Wireless** > **QVLAN Setup**.
2. Select the **Enable** check box.
3. Change the VLAN ID of the SSID **internet** to **2** and the VLAN ID of the SSID **oa** to **3**.
4. Click **Save**.



QVLAN Setup

Enable ☑

PVID 1

Management VLAN 1

Trunk Port ☑ LAN0 □ LAN1

LAN Port	VLAN ID (1~4094)
LAN0	1
LAN1	1

2.4G SSID	VLAN ID (1~4094)
internet	2
oa	3

5. Wait until the AP reboots.

Step 2 Configure the switch.

1. Create IEEE 802.1Q VLANs described in the following table on the switch.

Port Connected To	Accessible VLAN ID	Port Type	PVID
AP	1, 2, and 3	Trunk	1
LAN server	3	Access	3
Router	2	Access	2

2. Retain the default settings of other ports. For details, refer to the user guide for the switch.

---End

- Verification

Wireless clients connected to the **internet** wireless network can access only the internet, whereas the wireless clients connected to the **oa** wireless network can access only the LAN.

8 SNMP

8.1 Overview

The Simple Network Management Protocol (SNMP) is the most widely used network management protocol in TCP/IP networks. SNMP enables you to remotely manage all your network devices compliant with this protocol, such as monitoring the network status, changing network device settings, and receive network event alarms.

SNMP allows automatic management of devices from various vendors regardless of physical differences among the devices.

8.1.1 SNMP Management Framework

The SNMP management framework consists of SNMP manager, SNMP agent, and Management Information Base (MIB).

- SNMP manager: It is a system that controls and monitors network nodes using the SNMP protocol. The SNMP manager most widely used in network environments is Network Management System (NMS). An NMS can be a dedicated network management server, or an application that implements management functions in a network device.
- SNMP agent: It is a software module in a managed device. The module is used to manage data about the device and report the management data to an SNMP manager.
- MIB: It is a collection of managed objects. It defines a series of attributes of managed objects, including names, access permissions, and data types of objects. Each SNMP agent has its MIB. An SNMP manager can read and/or write objects in the MIB based on the permissions assigned to the SNMP manager.

An SNMP manager manages SNMP agents in an SNMP network. The SNMP manager exchanges management information with the SNMP agents using the SNMP protocol.

8.1.2 Basic SNMP Operations

The AP allows the following basic SNMP operations:

- Get: An SNMP manager performs this operation to query the SNMP agent of the AP for values of one or more objects.
- Set: An SNMP manager performs this operation to set values of one or more objects in the MIB of the SNMP agent of the AP.

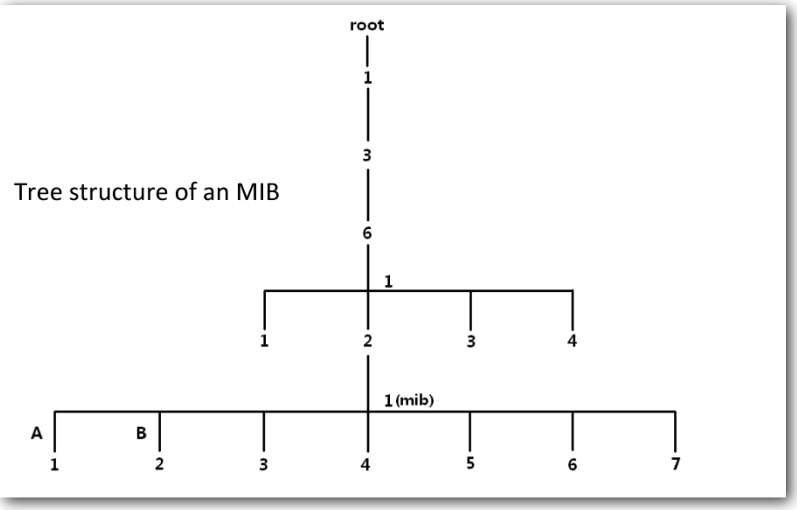
8.1.3 SNMP Protocol Version

The AP is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism. Community name is used to define the relationship between an SNMP agent and an SNMP manager. If the community name contained in an SNMP packet is rejected by a device, the packet is discarded. A community name functions as a password to control SNMP agent access attempts of SNMP managers.

SNMP V2C is compatible with SNMP V1 and provides more functions than SNMP V1. Compared with SNMP V1, SNMP V2C supports more operations (GetBulk and InformRequest) and data types (such as Counter64), and provides more error codes for better distinguishing errors.

8.1.4 MIB Introduction

An MIB adopts a tree structure. The nodes of the tree indicate managed objects. A path consisting of digits and starting from the root can be used to uniquely identify a node. This path is called an object identifier (OID). The following figure shows the structure of an MIB. In the figure, the OID of A is 1.3.6.1.2.1.1, whereas the OID of B is 1.3.6.1.2.1.2.

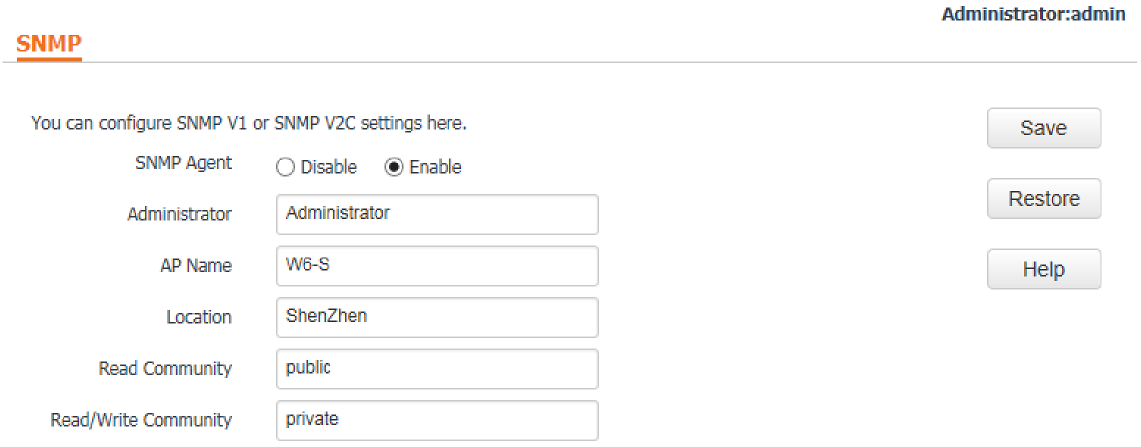


8.2 Configuring the SNMP Function

Step 1 Choose **SNMP** and set **SNMP Agent** to **Enable**.

Step 2 Set related SNMP parameters.

Step 3 Click **Save**.



You can configure SNMP V1 or SNMP V2C settings here.

SNMP Agent	○ Disable ● Enable
Administrator	Administrator
AP Name	W6-S
Location	ShenZhen
Read Community	public
Read/Write Community	private

---End

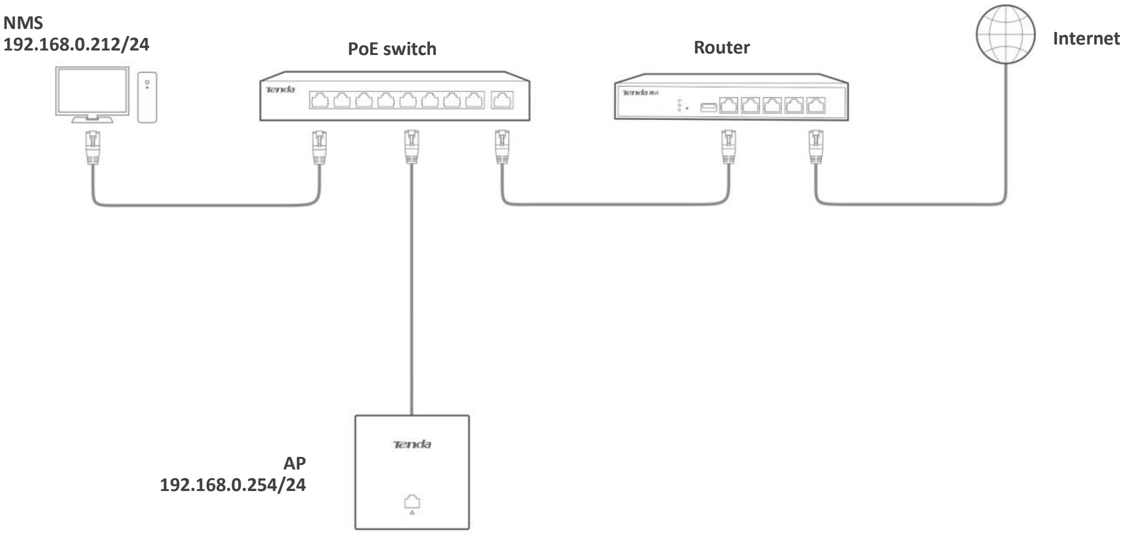
Parameter description

Parameter	Description
SNMP	It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled. An SNMP manager and the SNMP agent can communicate with each other only if their

Parameter	Description
	SNMP versions are the same. Currently, the SNMP agent function of the AP supports SNMP V1 and SNMP V2C.
Administrator	It specifies the name of the administrator of the AP. The default name is **Administrator**. You can change the name as required.
AP Name	It specifies the device name of the AP. The default device name is the model of the AP. NOTE It is recommended that you change the AP name so that you can easily identify the AP when managing the AP using SNMP.
Location	It specifies the location where the AP is used. You can change the location as required.
Read Community	It specifies the read password shared between SNMP managers and this SNMP agent. The default password is **public**. The SNMP agent function of the AP allows an SNMP manager to use the password to read variables in the MIB of the AP.
Read/Write Community	It specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is **private**. The SNMP agent function of the AP allows an SNMP manager to use the password to read/write variables in the MIB of the AP.

8.3 Example of Configuring the SNMP Function

- Networking requirement
  - The AP connects to an NMS over an LAN. This IP address of the AP is 192.168.0.254/24 and the IP address of the NMS is 192.168.0.212/24.
  - The NMS uses SNMP V1 or SNMP V2C to monitor and manage the AP.



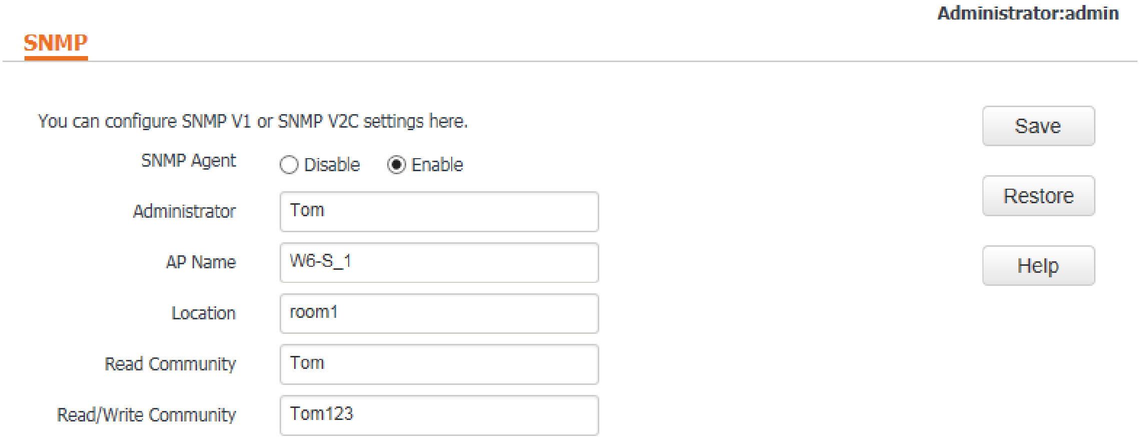
- Configuration procedure

Step 1 Configure the AP.

NOTE

Assume that the administrator name is **Tom**, read community is **Tom**, and read/write community is **Tom123**.

1. Log in to the web UI of the AP and choose **SNMP**.
2. Set **SNMP Agent** to **Enable**.
3. Set the SNMP parameters.
4. Click **Save**.



Administrator:admin

SNMP

You can configure SNMP V1 or SNMP V2C settings here.

SNMP Agent	○ Disable ● Enable
Administrator	Tom
AP Name	W6-S_1
Location	room1
Read Community	Tom
Read/Write Community	Tom123

Step 2 Configure the NMS.

On an NMS that uses SNMP V1 or SNMP V2C, set the read community to **Tom** and read/write community to **Tom123**. For details about how to configure the NMS, refer to the configuration guide for the NMS.

---End

- Verification

After the configuration, the NMS can connect to the SNMP agent of the AP and can query and set some parameters on the SNMP agent through the MIB.

9 Tools

9.1 Firmware Upgrade

This function upgrades the firmware of the AP for more functions and higher stability.

NOTE

To prevent damaging the AP, verify that the new firmware version is applicable to the AP before upgrading the firmware and keep the power supply of the AP connected during an upgrade.

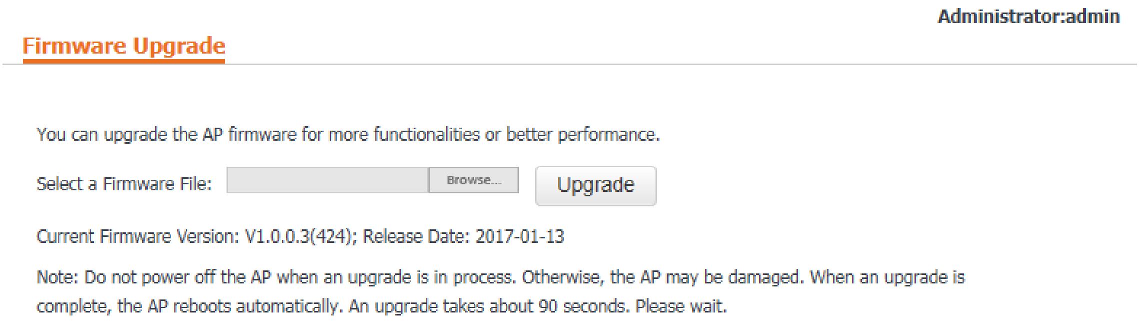
Perform the following procedure:

Step 1 Download the package of a later firmware version for the AP from http://www.tendacn.com to your local computer, and decompress the package.

Step 2 Log in to the web UI of the AP and choose **Tools** > **Firmware Upgrade**.

Step 3 Click **Browse** and select the file for upgrading the firmware.

Step 4 Click **Upgrade**.



You can upgrade the AP firmware for more functionalities or better performance.

Select a Firmware File:

Current Firmware Version: V1.0.0.3(424); Release Date: 2017-01-13

Note: Do not power off the AP when an upgrade is in process. Otherwise, the AP may be damaged. When an upgrade is complete, the AP reboots automatically. An upgrade takes about 90 seconds. Please wait.

---End

Wait until the progress bar is complete. Log in to the web UI of the AP again. Choose **Status** > **System Status** and check whether the upgrade is successful based on **Firmware Version**.

NOTE

After the firmware is upgraded, you are recommended to restore the factory settings of the AP and configure the AP again, so as to ensure stability of the AP and proper operation of new functions.

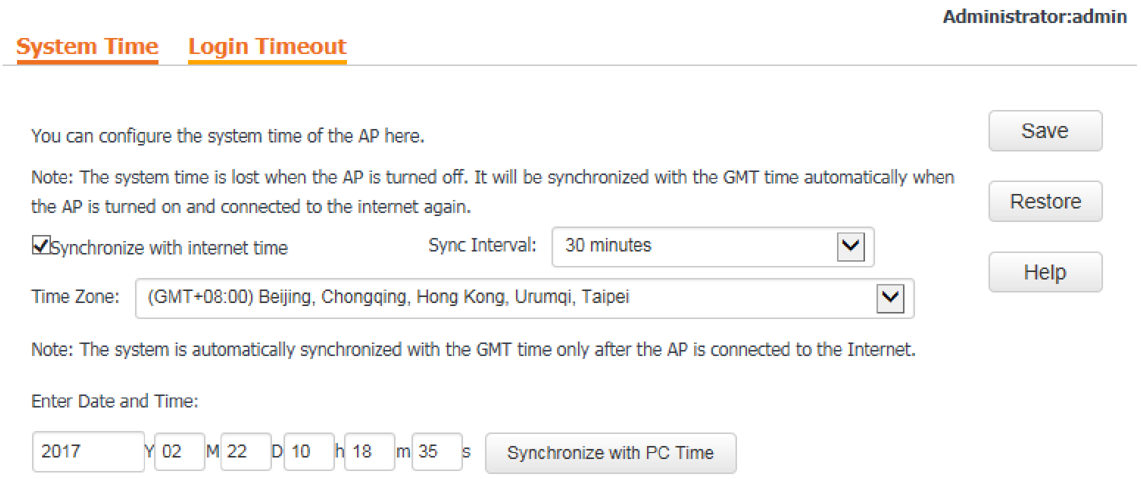
9.2 Date & Time

This module enables you to set the system time and login timeout interval of the AP.

9.2.1 System Time

Ensure that the system time of the AP is correct, so that logs can be recorded correctly and the reboot schedule can be executed correctly.

To access the page, choose **Tools** > **Date & Time**.



You can configure the system time of the AP here.

Note: The system time is lost when the AP is turned off. It will be synchronized with the GMT time automatically when the AP is turned on and connected to the internet again.

☑Synchronize with internet time Sync Interval: 30 minutes

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei

Note: The system is automatically synchronized with the GMT time only after the AP is connected to the Internet.

Enter Date and Time:

2017 Y 02 M 22 D 10 h 18 m 35 s

The AP allows you to set the system time by synchronizing the time with the internet or manually setting the time. By default, it is configured to synchronize the system time with the internet.

Synchronizing the System Time with the Internet

The AP automatically synchronizes its system time with a time server of the internet. This enables the AP to automatically correct its system time after being connected to the internet.

For details about how to connect the AP to the internet, refer to LAN Setup.

Perform the following procedure:

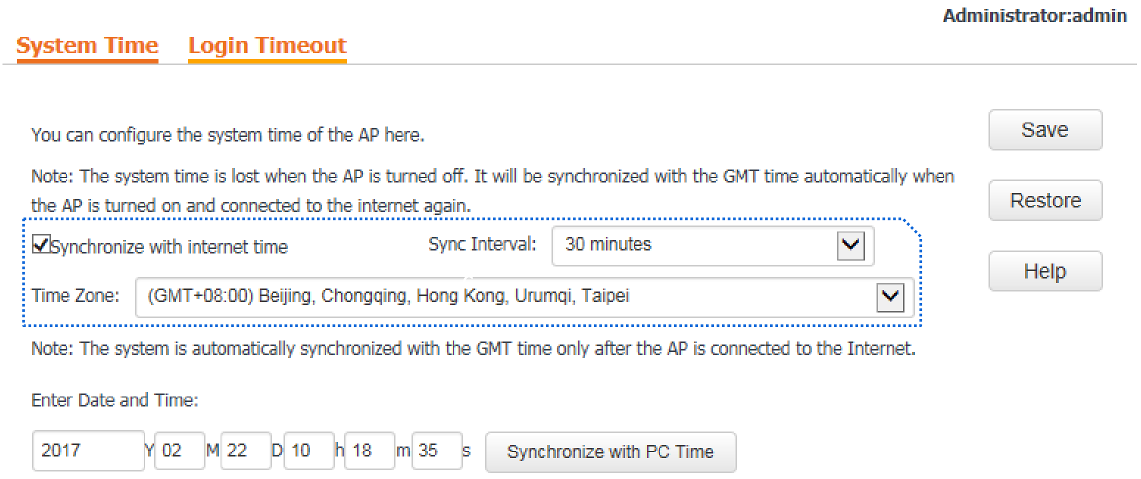
Step 1 Choose **Tools** > **Date & Time**.

Step 2 Select **Synchronize with internet time**.

Step 3 Set **Sync Interval** to the interval at which the AP synchronizes its system time with a time server of the internet. The default value **30 minutes** is recommended.

Step 4 Set **Time Zone** to your time zone.

Step 5 Click **Save**.



You can configure the system time of the AP here.

Note: The system time is lost when the AP is turned off. It will be synchronized with the GMT time automatically when the AP is turned on and connected to the internet again.

☑Synchronize with internet time Sync Interval: 30 minutes

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei

Note: The system is automatically synchronized with the GMT time only after the AP is connected to the Internet.

Enter Date and Time:

2017 Y 02 M 22 D 10 h 18 m 35 s

---End

Manually Setting the System Time

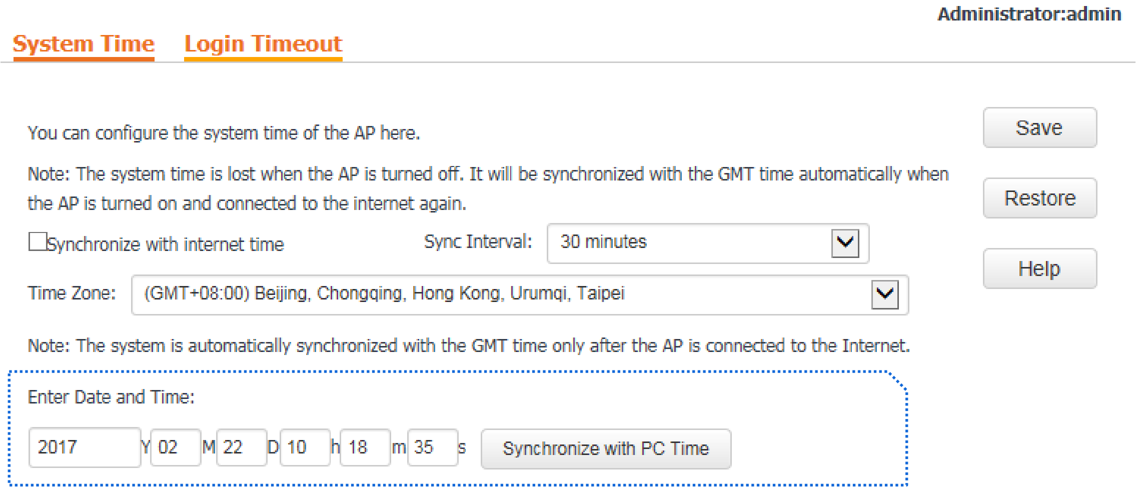
You can manually set the system time of the AP. If you choose this option, you need to set the system time each time after the AP reboots.

Perform the following procedure:

Step 1 Choose **Tools** > **Date & Time**.

Step 2 Enter a correct date and time, or click **Synchronize with PC Time** to synchronize the system time of the AP with the system time (ensure that it is correct) of the computer being used to manage the AP.

Step 3 Click **Save**.



You can configure the system time of the AP here.

Note: The system time is lost when the AP is turned off. It will be synchronized with the GMT time automatically when the AP is turned on and connected to the internet again.

□Synchronize with internet time Sync Interval: 30 minutes

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei

Note: The system is automatically synchronized with the GMT time only after the AP is connected to the Internet.

Enter Date and Time:

2017 Y 02 M 22 D 10 h 18 m 35 s Synchronize with PC Time

---End

9.2.2 Login Timeout

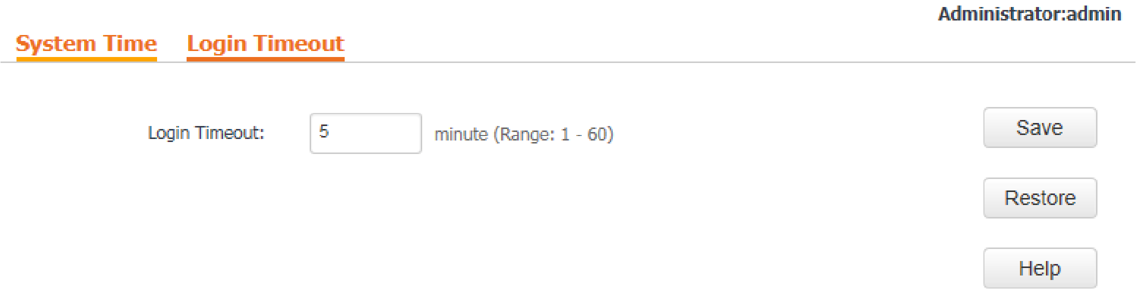
If you log in to the web UI of the AP and perform no operation within the login timeout interval, the AP logs you out for network security. The default login timeout interval is 5 minutes.

Perform the following procedure:

Step 1 Choose **Tools** > **Date & Time** and click the **Login Timeout** tab.

Step 2 Change the login timeout interval as required.

Step 3 Click **Save**.



Login Timeout: 5 minute (Range: 1 - 60)

---End

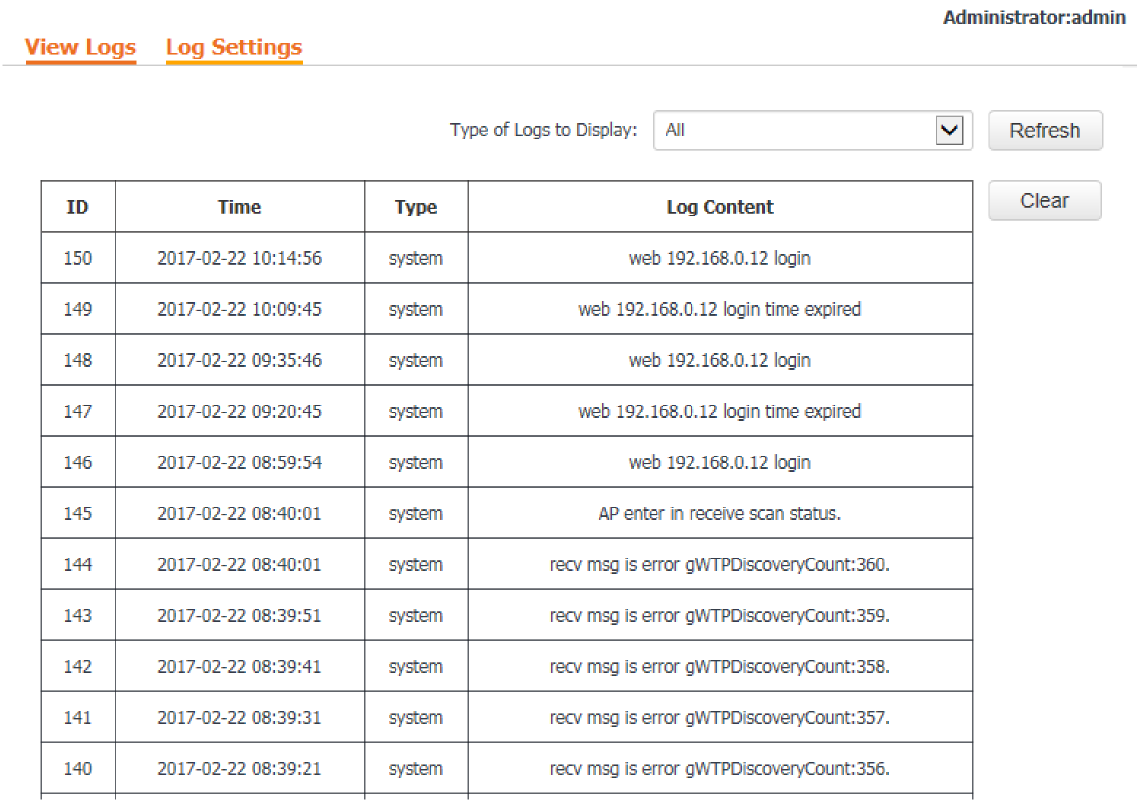
9.3 Logs

This module enables you to view logs and configure log settings.

9.3.1 Viewing Logs

The logs of the AP record various events that occur and the operations that users perform after the AP starts. In case of a system fault, you can refer to the logs during troubleshooting.

To access the page, choose **Tools** > **Logs**.



Type of Logs to Display: All

ID	Time	Type	Log Content
150	2017-02-22 10:14:56	system	web 192.168.0.12 login
149	2017-02-22 10:09:45	system	web 192.168.0.12 login time expired
148	2017-02-22 09:35:46	system	web 192.168.0.12 login
147	2017-02-22 09:20:45	system	web 192.168.0.12 login time expired
146	2017-02-22 08:59:54	system	web 192.168.0.12 login
145	2017-02-22 08:40:01	system	AP enter in receive scan status.
144	2017-02-22 08:40:01	system	recv msg is error gWTPDiscoveryCount:360.
143	2017-02-22 08:39:51	system	recv msg is error gWTPDiscoveryCount:359.
142	2017-02-22 08:39:41	system	recv msg is error gWTPDiscoveryCount:358.
141	2017-02-22 08:39:31	system	recv msg is error gWTPDiscoveryCount:357.
140	2017-02-22 08:39:21	system	recv msg is error gWTPDiscoveryCount:356.

To ensure that the logs are recorded correctly, verify the system time of the AP on the **System Time** tab page at **Tools** > **Date & Time**.

To view the latest logs of the AP, click **Refresh**. To clear the existing logs of the AP, click **Clear**.

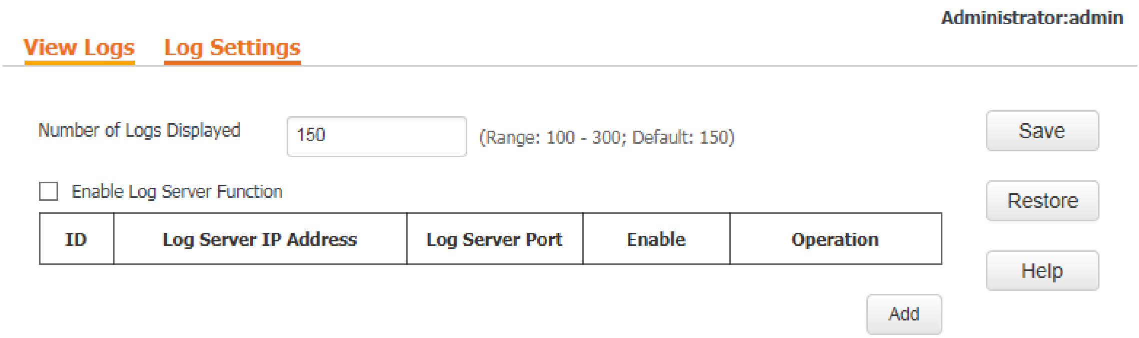
NOTE

- When the AP reboots, the previous logs are lost.
- The AP reboots when the AP is powered on after a power failure, the QVLAN function is configured, the firmware is upgraded, an AP configuration is restored, or the factory settings are restored.

9.3.2 Configuring Log Settings

To access the page, choose **Tools** > **Logs** and click **Log Settings**.

On this page, you can set the number of logs to be displayed and configure log servers.



Number of Logs Displayed 150 (Range: 100 - 300; Default: 150)

□ Enable Log Server Function

ID	Log Server IP Address	Log Server Port	Enable	Operation

Setting the Number of Logs to Be Displayed

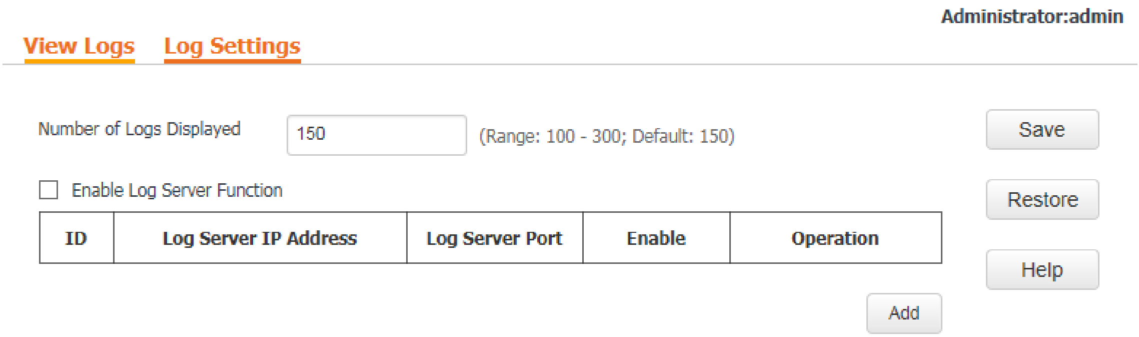
By default, the AP can display a maximum of 150 logs on the **View Logs** page. You can change the number as required.

Perform the following procedure:

Step 1 Choose **Tools** > **Logs** and click **Log Settings**.

Step 2 Change the number of logs as required within the range of 100 to 300.

Step 3 Click **Save**.



Number of Logs Displayed 150 (Range: 100 - 300; Default: 150)

□ Enable Log Server Function

ID	Log Server IP Address	Log Server Port	Enable	Operation

---End

Configuring Log Server Settings

After you specify a log server, the AP sends its logs to the log server. You can view all the historical logs of the AP on the log server.

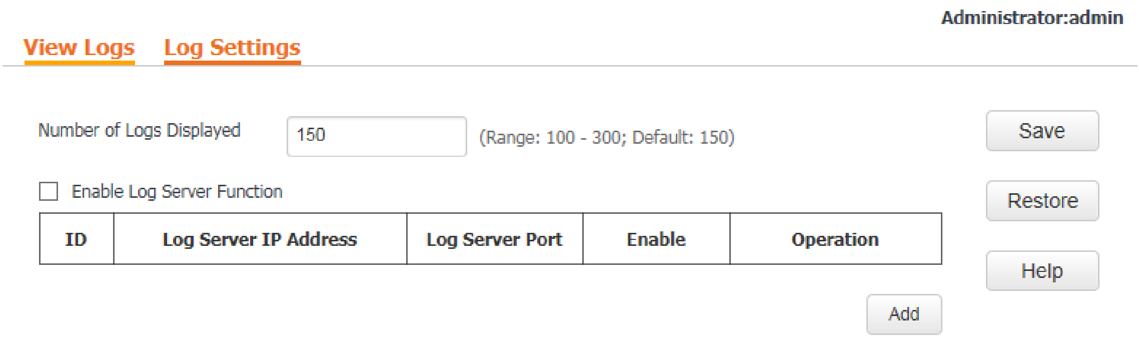
NOTE

To ensure that system logs can be sent to a log server, choose **Network** > **LAN Setup** and set the IP address, subnet mask, and gateway of the AP for communicating with the log server.

- Procedure for adding a log server

Step 1 Choose **Tools** > **Logs** and click **Log Settings**.

Step 2 Click **Add**.



Number of Logs Displayed: 150 (Range: 100 - 300; Default: 150)

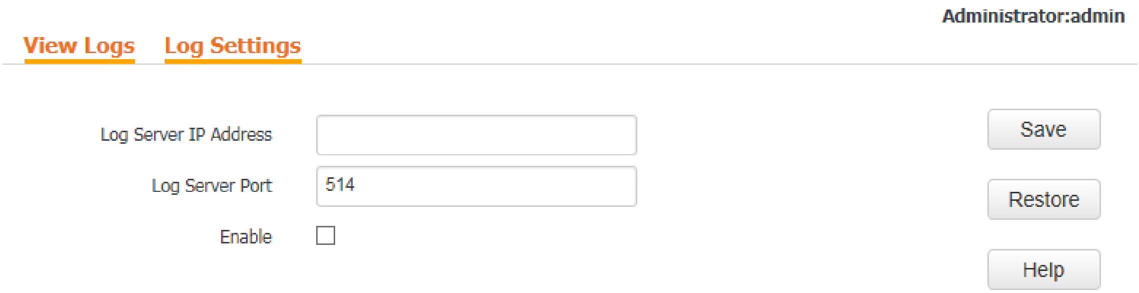
□ Enable Log Server Function

ID	Log Server IP Address	Log Server Port	Enable	Operation

Step 3 Set parameters as follows:

1. Set **Log Server IP Address** to the IP address of the log server.
2. Set **Log Server Port** to the UDP port number used to send and receive system logs. The default port number 514 is recommended.
3. Select **Enable** to enable the log server.

Step 4 Click **Save**.



Log Server IP Address:

Log Server Port: 514

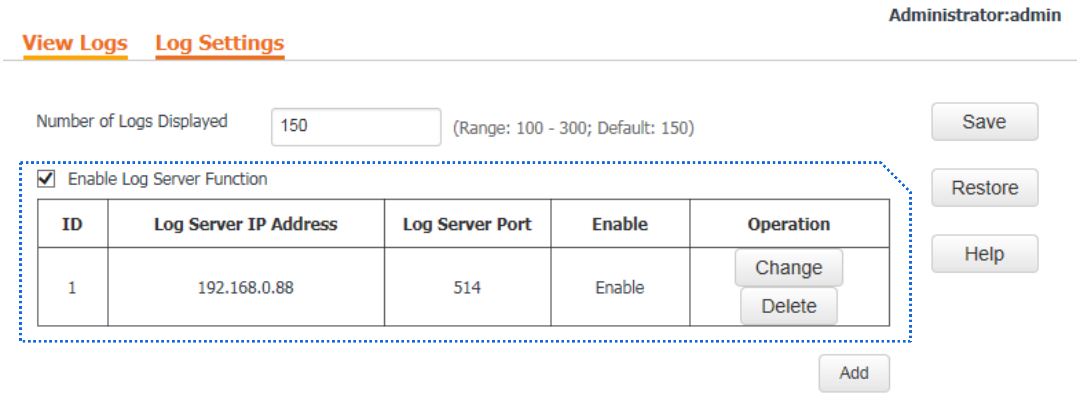
Enable □

Step 5 Select **Enable Log Server Function**.

Step 6 Click **Save**.

---End

The following figure shows an example of log server settings.



Number of Logs Displayed: 150 (Range: 100 - 300; Default: 150)

☑ Enable Log Server Function

ID	Log Server IP Address	Log Server Port	Enable	Operation
1	192.168.0.88	514	Enable	Change Delete

- Procedure for changing log server settings

Step 1 Choose **Tools** > **Logs** and click **Log Settings**.

Step 2 Click **Change** corresponding to the log server settings to be changed.

Step 3 Change the parameter settings as required.

Step 4 Click **Save**.

---End

- Procedure for deleting log server settings

Step 1 Choose **Tools** > **Logs** and click **Log Settings**.

Step 2 Click **Delete** corresponding to the log server settings to be deleted.

---End

9.4 Configuration Management

This module enables you to back up the current configuration of the AP, restore a configuration of the AP, and restore the factory settings of the AP.

9.4.1 Backing Up and Restoring Configurations

The backup function enables you to back up the current configuration of the AP to a local computer. The restoration function enables you to restore the AP to a previous configuration.

If the AP enters the optimum condition after you greatly change the configuration of the AP, you are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the AP.

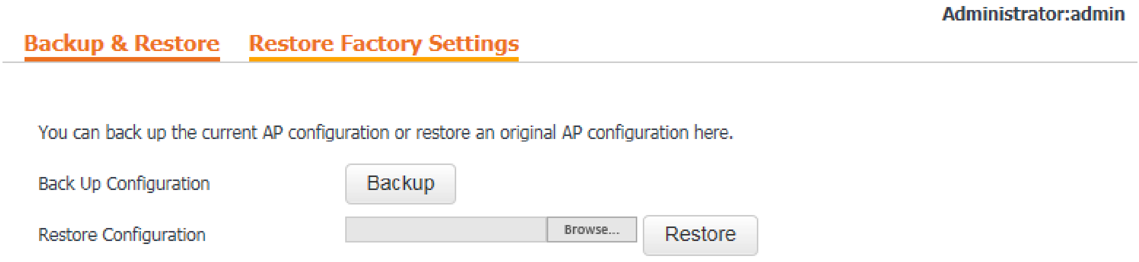
TIP

If you need to apply same or similar configurations to many APs, you can configure one of the APs, back up the configuration of the AP, and use the backup to restore the configuration on the other APs. This improves configuration efficiency.

Backing Up the Current Configuration

Step 1 Choose **Tools** > **Configuration**.

Step 2 Click **Backup** and follow the on-screen instructions to perform operations.



You can back up the current AP configuration or restore an original AP configuration here.

Back Up Configuration Backup

Restore Configuration Browse... Restore

---End

Restoring a Configuration

Step 1 Choose **Tools** > **Configuration**.

Step 2 Click **Browse** and select the file of the configuration to be restored.

Step 3 Click **Restore** and follow the on-screen instructions to perform operations.

---End

9.4.2 Restoring the Factory Settings

If you cannot locate a fault of the AP or forget the password of the web UI of the AP, you can reset the AP to restore its factory settings and then configure it again. The AP can be reset using software or hardware.

After the factory settings are restored, the login IP address of the AP is changed to **192.168.0.254**, and the user name and password of the AP are changed to **admin**.

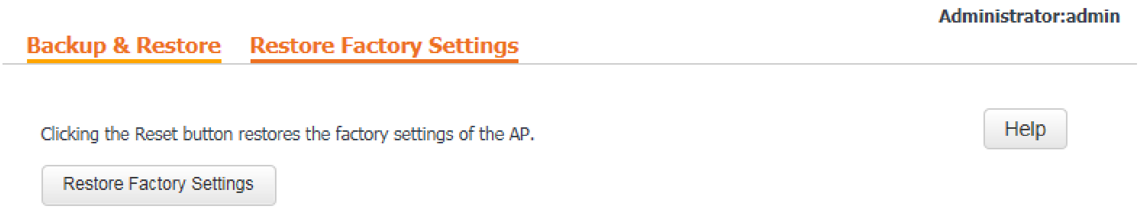
NOTE

- When the factory settings are restored, your configuration is lost. Therefore, you need to reconfigure the AP to connect to the internet. Restore the factory settings of the AP only when necessary.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.

Restoring the Factory Settings Using Software

Step 1 Choose **Tools** > **Configuration** and click the **Restore Factory Settings** tab.

Step 2 Click the **Restore Factory Settings** button.



Clicking the Reset button restores the factory settings of the AP.

---End

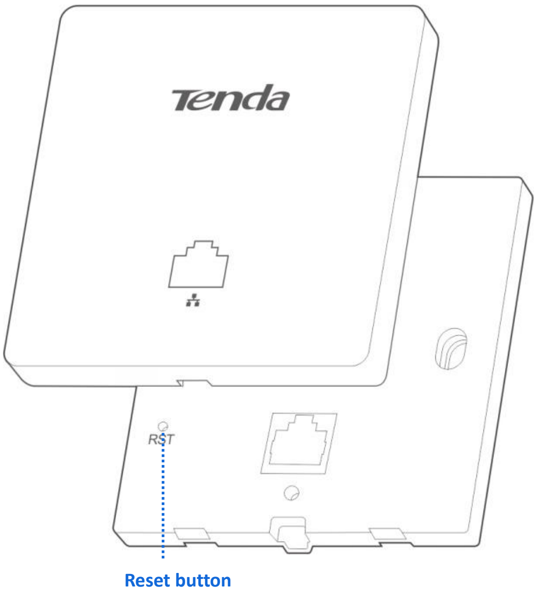
Restoring the Factory Settings Using Hardware

This method enables you to restore the factory settings without logging in to the web UI of the AP.

Perform the following procedure:

Step 1 After the AP is powered on, use a paper clip to hold down the reset button for 8 seconds.

Step 2 Wait about 1 second.

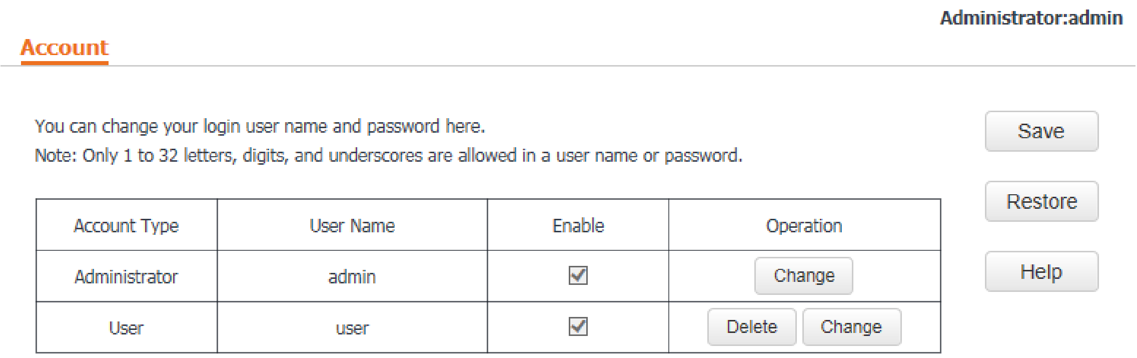


---End

9.5 Account Management

To access the page, choose **Tools** > **Account**.

On this page, you can change the login account information of the AP to prevent unauthorized login.



You can change your login user name and password here.

Note: Only 1 to 32 letters, digits, and underscores are allowed in a user name or password.

Account Type	User Name	Enable	Operation
Administrator	admin	☑	Change
User	user	☑	Delete Change

Parameter description

Parameter	Description
Account Type	- **Administrator**: An account of this type enables you to view and modify settings of the AP. - **User**: An account of this type enables you to view settings of the AP.
User Name	It specifies the user name of an account. By default, the AP has one administrator account and one user account. Both the user name and password of the administrator account are **admin**. Both the user name and password of the user account are **user**.
Enable	It specifies whether an account is enabled. The administrator account is always enabled. The user account is enabled by default and can be disabled.
Operation	- **Change**: This button is used to change the user name and password of the account corresponding to the button. - **Delete**: This button is used to delete the user account. - **Add**: This button is used to add the user account after the account is deleted. NOTE After changing, deleting, or adding an account, click **Save**.

9.6 Diagnostics Tool

If the network connection fails, you can use the diagnostics tool included with the AP to locate the faulty node.

Perform the following procedure:

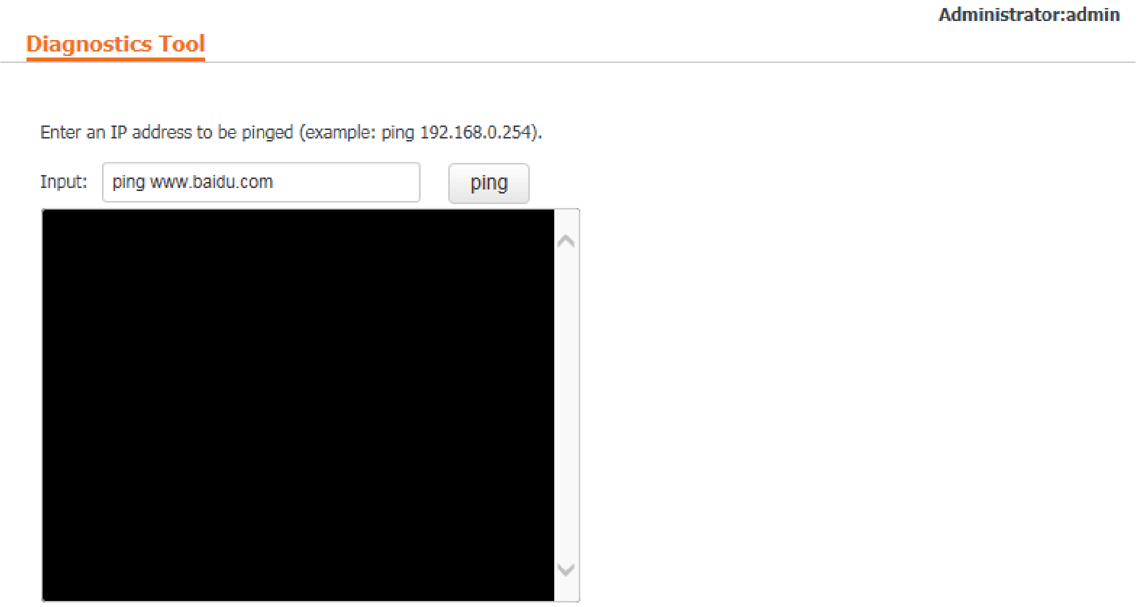
NOTE

The link to www.baidu.com is used as an example.

Step 1 Choose **Tools** > **Diagnostics Tool**.

Step 2 Enter the IP address or domain name to be pinged in the **Input** text box. In this example, enter **ping www.baidu.com**.

Step 3 Click **Ping**.



Administrator:admin

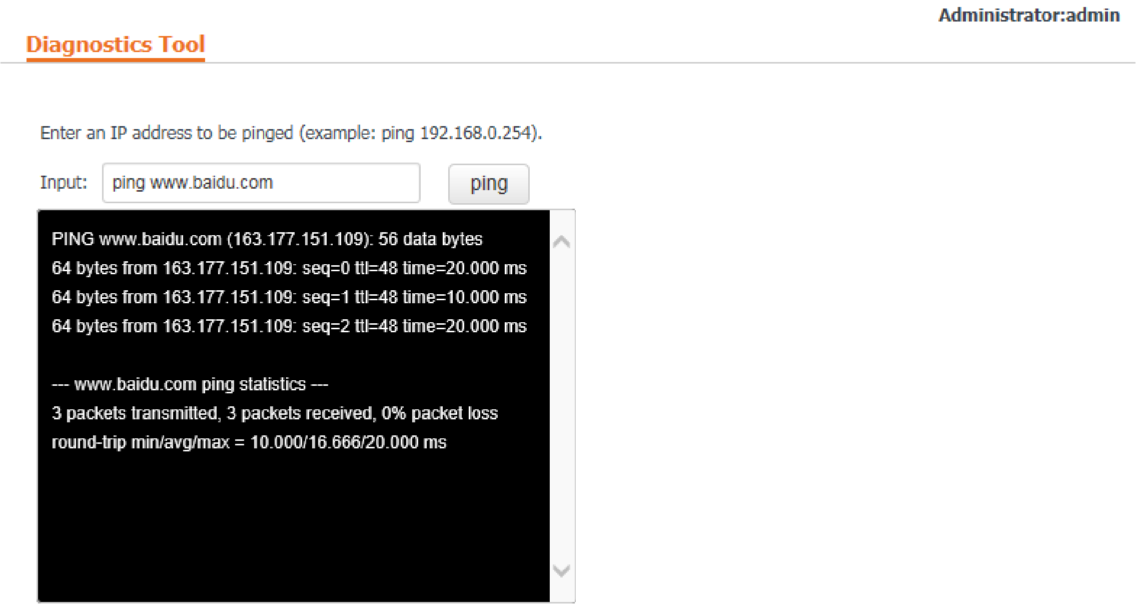
Diagnostics Tool

Enter an IP address to be pinged (example: ping 192.168.0.254).

Input: ping www.baidu.com

---End

The diagnosis result will be displayed in a few seconds in the black text box below the **Input** text box. See the following figure.



Administrator:admin

Diagnostics Tool

Enter an IP address to be pinged (example: ping 192.168.0.254).

Input: ping www.baidu.com

```
PING www.baidu.com (163.177.151.109): 56 data bytes
64 bytes from 163.177.151.109: seq=0 ttl=48 time=20.000 ms
64 bytes from 163.177.151.109: seq=1 ttl=48 time=10.000 ms
64 bytes from 163.177.151.109: seq=2 ttl=48 time=20.000 ms

--- www.baidu.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 10.000/16.666/20.000 ms
```

9.7 Device Reboot

This module enables you to manually reboot the AP or configure the AP to automatically reboot.

NOTE

When the AP reboots, all connections are released. You are recommended to reboot the AP at an idle hour.

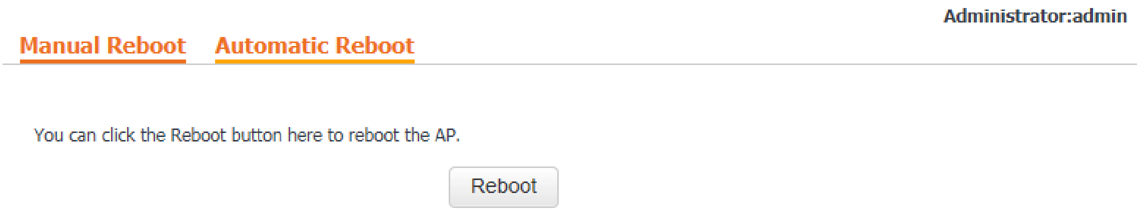
9.7.1 Manually Rebooting the AP

If a setting does not take effect, you can try rebooting the AP to resolve the problem.

Perform the following procedure:

Step 1 Choose **Tools** > **Device Reboot**.

Step 2 Click **Reboot**.



You can click the Reboot button here to reboot the AP.

---End

9.7.2 Configuring the AP to Automatically Reboot

This function enables the AP to automatically reboot as scheduled. You can use this function to prevent wireless performance degradation or network instability that occurs after a long AP uptime. The AP can reboot:

- **At intervals**: In this mode, the AP reboots at the interval that you specify.
- **At specified time**: In this mode, the AP reboots weekly at the time that you specify.

Configuring the AP to Reboot at an Interval

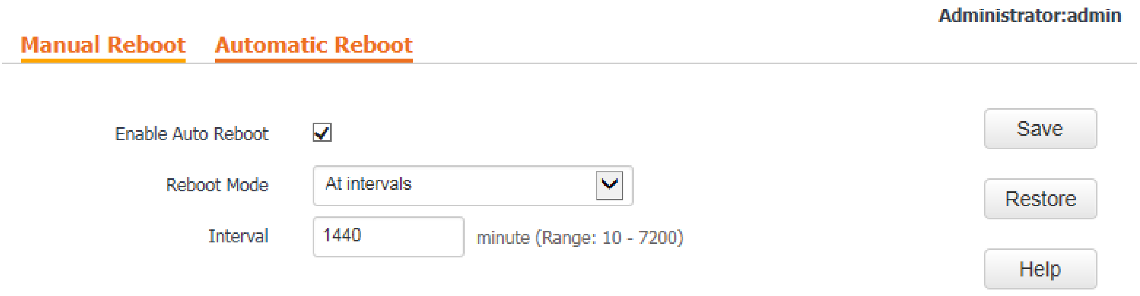
Step 1 Choose **Tools** > **Device Reboot** and click the **Automatic Reboot** tab.

Step 2 Select the **Enable Auto Reboot** check box.

Step 3 Set **Reboot Mode** to **At intervals**.

Step 4 Set **Interval** to a value in minutes, such as **1440**.

Step 5 Click **Save**.



Enable Auto Reboot ☑

Reboot Mode: At intervals

Interval: 1440 minute (Range: 10 - 7200)

---End

Configuring the AP to Reboot at Specified Time

Step 1 Choose **Tools** > **Device Reboot** and click the **Automatic Reboot** tab.

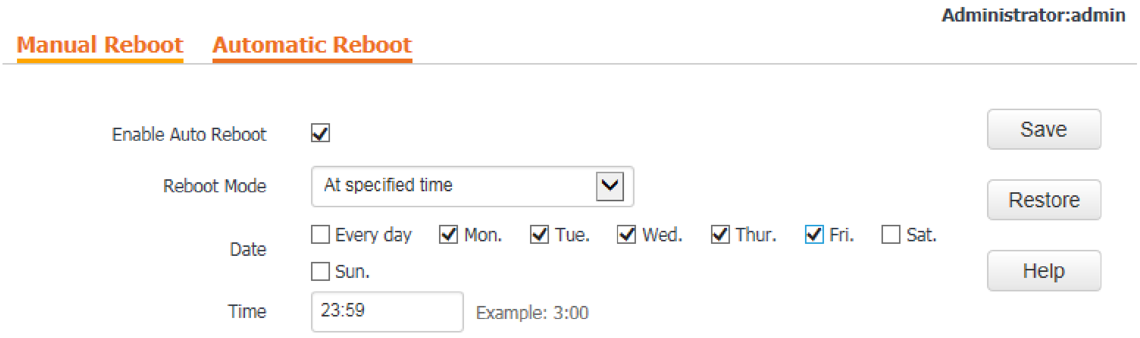
Step 2 Select the **Enable Auto Reboot** check box.

Step 3 Set **Reboot Mode** to **At specified time**.

Step 4 Select the day or days when the AP reboots.

Step 5 Set the time when the AP reboots, such as **23:59**.

Step 6 Click **Save**.


Enable Auto Reboot ☑

Reboot Mode: At specified time

Date: □ Every day ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thur. ☑ Fri. □ Sat. □ Sun.

Time: 23:59 Example: 3:00

---End

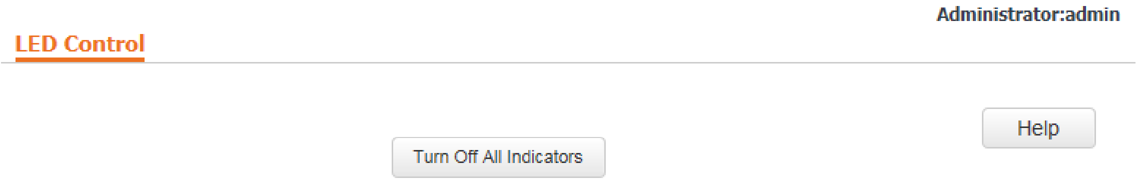
9.8 LED Control

This function enables you to turn on/off the LED indicator of the AP. By default, the LED indicator is turned on.

- Procedure for turning off the LED indicator

Step 1 Choose **Tools** > **LED Control**.

Step 2 Click **Turn Off All Indicators**.



---End

- Procedure for turning on the LED indicator

Step 1 Choose **Tools** > **LED Control**.

Step 2 Click **Turn On All Indicators**.

---End

9.9 Uplink Detection

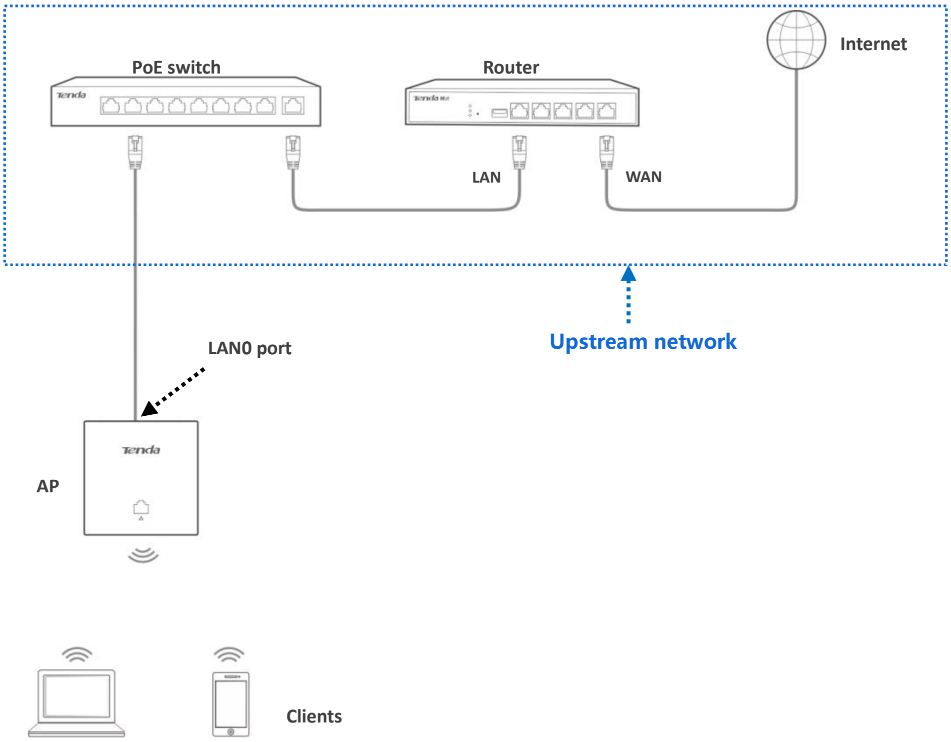
9.9.1 Overview

In AP mode, the AP connects to its upstream network using the LAN0 port. If a critical node between the LAN0 port and the upstream network fails, the AP as well as the wireless clients connected to the AP cannot access the upstream network. If uplink detection is enabled, the AP regularly pings specified hosts through the LAN0 port. If all the hosts are not reachable, the AP stops its wireless service and wireless clients cannot find the SSIDs of the

AP. The client can reconnect to the AP only after the connection between the AP and the upstream networks is recovered.

If the uplink of the AP with uplink detection enabled is faulty, wireless clients can connect to the upstream network through another nearby AP that works properly.

The following figure shows the upstream network of the AP.



9.9.2 Configuring Uplink Detection

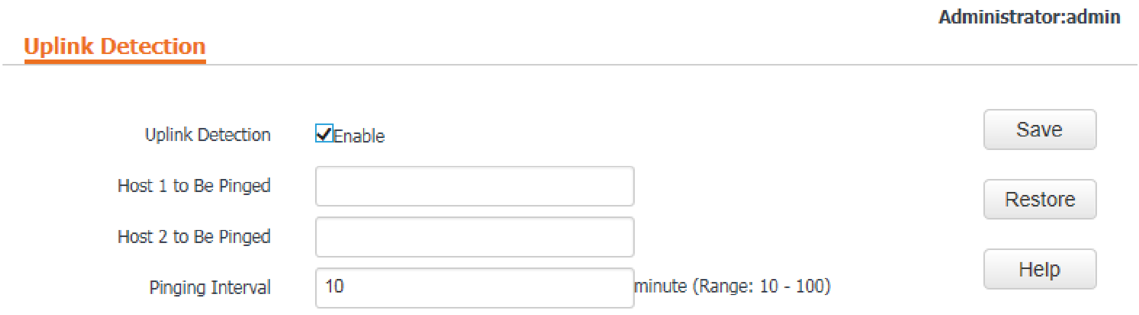
Step 1 Choose **Tools** > **Uplink Detection**.

Step 2 Select the **Enable** check box of **Uplink Detection**.

Step 3 Set **Host a to Be Pinged** or **Host 2 to Be Pinged** to the IP address of the host to be pinged through the LAN0 port of the AP, such as the IP address of the switch or router directly connected to the AP.

Step 4 Set **Pinging Interval** to the interval at which the AP detects its uplink.

Step 5 Click **Save**.


Administrator:admin

Uplink Detection

Uplink Detection ☑Enable

Host 1 to Be Pinged

Host 2 to Be Pinged

Pinging Interval 10 minute (Range: 10 - 100)

---End

Appendixes

A. FAQ

Q1. I cannot access the web UI of the AP after entering 192.168.0.254. What should I do?

A1. Check the following items:

- Verify that the IP address of your computer is 192.168.0.*X* (*X*: 2~253).
- Clear the cache of your web browser or replace the web browser, and try login again.
- Disable the firewall of your computer or replace the computer, and try login again.
- If two or more APs are connected to your network without an AP controller or a router equipped with the AP controller functionality, connect one of the APs to your PoE switch and change the IP address of the AP. Repeat this procedure to connect the other APs to the PoE switch and change the IP addresses of the APs.
- The AP may be being managed by an AP controller and therefore its IP address is no longer 192.168.0.254. In that case, log in to the web UI of the AP controller to view the new IP address of the AP, and log in to the AP using the new IP address.
- If the problem persists, restore the factory settings of the AP and try login again.

Q2. My wireless AP controller cannot find the AP. What should I do?

A2. Check the following items:

- Verify that the devices are connected properly and the AP has started.
- If VLANs have been defined on your network, verify that the corresponding VLAN has been added to your AP controller.
- Restart the AP or restore the factory settings of the AP, and try scanning the AP again.

Q3. I forget the login user name and password of the AP. What should I do to log in to the web UI of the AP?

A3. Try login with the default IP address **192.168.0.254** and default user name and password **admin**. If login fails, restore the factory settings and use the default login information to try login again.

Q4. I cannot access the web UI of the AP. What should I do to restore the factory settings?

A4. After the AP is powered on, use a paper clip to hold down the reset button for 8 seconds and then wait about 1 second. After the factory settings are restored, configure the AP again.

Q5. What should I do if a computer connected to the AP displays an IP address conflict message?

A5. Check the following items:

- Verify that the IP address of the computer is not used by another device on your LAN. The default IP address of the AP is 192.168.0.254.
- Verify that the static IP addresses assigned to computers on your LAN are not used by other devices.

For more technical assistance, visit our website at http://www.tendacn.com or send your question to support@tenda.cn. We will help you resolve your problem as soon as possible.

B. Default Parameter Values

The following table lists the default parameter values of the AP.

Parameter			Default Value
Login	Management IP address		192.168.0.254
	User Name/Password	Administrator	admin/admin
		User	user/user
Quick Setup	Working Mode		AP
LAN Setup	IP Address Type		Static
	IP Address		192.168.0.254
	Subnet Mask		255.255.255.0
	Gateway		192.168.0.1
	Primary DNS Server		8.8.8.8
	Secondary DNS Server		8.8.4.4
	AP Name		W6-S
DHCP Server	DHCP Server		Disable
	Start IP Address		192.168.0.100
	End IP Address		192.168.0.200
	Lease Time		1 day
	Subnet Mask		255.255.255.0
	Gateway		192.168.0.1
	Primary DNS Server		8.8.8.8
	Secondary DNS Server		8.8.4.4
Basic	SSID		The AP allows 2 SSIDs. The default primary SSID of the AP is Tenda_*XXXXXX*, where *XXXXXX* indicates the last 6 characters of the MAC address of the LAN ports of the AP. The default seconds SSID of the AP is Tenda_*XXXXXX*, where *XXXXXX* indicates the last 6 characters of the MAC address of the LAN ports of the AP plus 1. By default, the primary SSID (first SSID) is enabled, and the secondary SSID is disabled.
	Broadcast SSID		Enable
	Isolate Client		Disable

Parameter		Default Value
	WMF	Disable
	Max. Number of Clients	16
	Chinese SSID Encoding	UTF-8
	Security Mode	None
RF	Enable RF	Enable
	Country/Region	China
	Network Mode	11b/g/n
	Channel	Auto
	Channel Bandwidth	20MHz
	Lock Channel	Enable
	Isolate SSID	Disable
	WMM	Enable
	APSD	Disable
	Client Timeout Interval	5 minutes
Advanced	Beacon Interval	100ms
	Fragment Threshold	2346
	RTS Threshold	2347
	DTIM Interval	1
	Min. RSSI Threshold	-90dBm
	Transmit Power	18dBm
	APSD	Disable
	Lock Power	Enable
	Preamble	Long Preamble
Access Control		Disable
QVLAN Setup	Enabled	Disable
	PVID	1
	Management VLAN	1
	Trunk Port	LAN0
	LAN Port VLAN ID	1
	2.4G SSID VLAN ID	1000

Parameter			Default Value
SNMP	SNMP Agent		Disable
	Administrator		Administrator
	AP Name		W6-S
	Location		ShenZhen
	Read Community		public
	Read/Write Community		private
Tools	Date & Time	System Time	If **Synchronize with internet time** is selected: Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei
		Login Timeout	5 minutes
	Number of Logs Displayed		150
	Log server settings		None
	Enable Auto Reboot		Disable
	LED Control		Turn On All Indicators
	Uplink Detection		Disable

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 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.

Declaration of Conformity

Hereby, SHENZHEN TENDA TECHNOLOGY CO., LTD. declares that the radio equipment type W6-S is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address:
http://www.tendacn.com/en/service/page/ce.html

Operate Frequency: 2412-2472 MHz EIRP Power (Max.): 19.8 dBm Software Version: V1.0.3

RECYCLING

This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment.

User has the choice to give his product to a competent recycling organization or to the retailer when he buys new electrical or electronic equipment.