11AC 1200Mbps 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 the warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda! Please read this user guide before you start with W9

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.

Symbols in this User Guide:

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

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
AP	Access Point
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
SSID	Service Set Identifier
VLAN	Virtual Local Area Network
PoE	Power Over Ethernet
WEP	Wired Equivalent Privacy
AES	Advanced Encryption Standard
TKIP	Temporal Key Integrity Protocol

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	Canada: 1-888-998-8966 Hong Kong: 00852-81931998	Email	support@Tenda.cn
Website	http://www.Tendacn.com	Skype	Tendasz

Contents

1 Product Overview 1
1.1 Overview 1
1.2 Appearance 1
1.2.1 Button, LED Indicator, and Ports 1
1.2.2 Label 2
2 Application Scenarios 4
2.1 Large Apartment or Villa 4
2.1.1 Deploying the AP with a Tenda Router with the AP Controller Functionality 4
2.1.2 Deploying the AP with a Router of Another Brand 5
2.2 Hotel 9
3 Login 10
3.1 Logging in to the Web UI of the AP 10
3.2 Logging out of the Web UI of the AP 12
3.3 Web UI Layout 12
3.4 Common Buttons 14
4 Quick Setup 15
4.1 Overview 15
4.2 Quick Setup 17
4.2.1 AP Mode 17
4.2.2 Client+AP Mode 18
5 Status 21
5.1 System Status 21
5.2 Wireless Status 23
5.3 Traffic Statistics 24
5.4 Wireless Clients 25
6 Network Settings 26
6.1 LAN Setup 26
6.1.1 Modifying the LAN IP Address of the AP 27
6.2 DHCP Server 30
6.2.1 Overview 30
6.2.2 Configuring the DHCP Server 30
6.2.3 Viewing the DHCP Client List 32

7 Wireless Settings 33
7.1 Basic Settings 33
7.1.1 Overview 33
7.1.2 Modifying SSID Settings 35
7.1.3 Examples of Configuring SSID Settings 40
7.2 Radio Settings 60
7.2.1 Overview 60
7.2.2 Modifying Radio Settings 60
7.3 Radio Optimization 63
7.3.1 Overview 63
7.3.2 Optimizing Radio 64
7.4 WMM Settings 67
7.4.1 Overview 67
7.4.2 Modidying WMM Settings 68
7.5 Access Control 70
7.5.1 Overview 70
7.5.2 Configuring Access Control 70
7.5.3 Example of Configuring Access Control 72
7.6 Advanced Settings 73
7.6.1 Overview 73
7.6.2 Changing the Advanced Settings 73
7.7 QVLAN Settings 75
7.7.1 Overview 75
7.7.2 Configuring the QVLAN Function 75
7.7.3 Example of Configuring QVLAN Settings 76
8 SNMP 79
8.1 Overview 79
8.1.1 SNMP Management Framework 79
8.1.2 Basic SNMP Operations 79
8.1.3 SNMP Protocol Version 80
8.1.4 MIB Introduction 80
8.2 Configuring the SNMP Function 81
8.3 Example of Configuring the SNMP Function 82
9 Tools 84
9.1 Firmware Upgrade 84
9.2 Date & Time 86
9.2.1 System Time 86

9.2.2 Login Timeout Interval 88
9.3 Logs 89
9.3.1 Viewing Logs 89
9.3.2 Configuring Log Settings 89
9.4 Configuration 93
9.4.1 Backing Up and Restoring Configurations 93
9.4.2 Restoring the Factory Settings 95
9.5 Account 97
9.6 Diagnostics Tool 98
9.7 Reboot Device 100
9.7.1 Manual Reboot 100
9.7.2 Reboot Schedule 101
9.8 LED Control 103
9.9 Uplink Check 104
9.9.1 Overview 104
9.9.2 Configuring Uplink Check 104
Appendixes 106
A.1 FAQ 106
A.2 Default Parameter Values 107

1 Product Overview

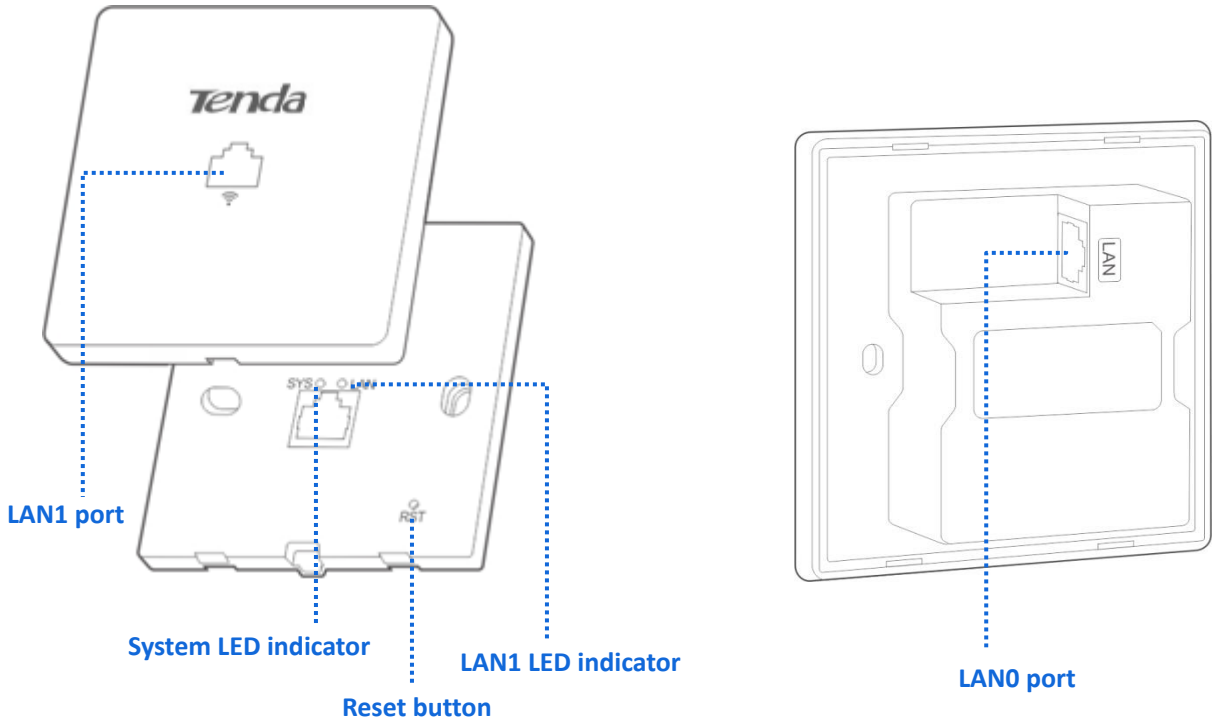
1.1 Overview

Tenda 11AC 1200Mbps Wireless In-Wall Access Point operates both on 2.4 GHz and 5 GHz, and offers a wireless transmission rate of as high as 1200 Mbps. It can be powered by IEEE 802.3af standard PoE switch and managed using its web UI or a Tenda wireless AP controller (or a Tenda router that supports the AP controller functionality). The in-wall design makes W9 perfect for providing WiFi coverage in villas, medium to large apartments, and hotels.

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 about 8 seconds to restore the factory settings.

- LED Indicator

LED	Status	Description
SYS	Blinking green	The AP works properly.
	Off	The AP is not powered on.
LAN	Solid blue	The rear (LAN0) port is connected.
	Blinking blue	Data is being transmitted over the rear (LAN0) port.
	Off	The rear (LAN0) port is not connected.

- LAN1 Port

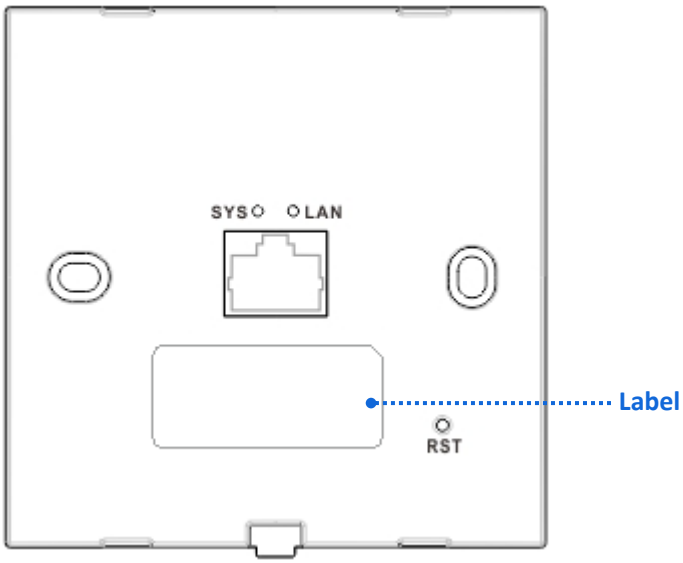
This port is located on the front panel of the AP and transmits data in 10/100 Mbps auto-negotiation mode. It is used to connect to a computer, a switch and so on.

- LAN0 Port

It is located on the rear of the AP for supplying PoE power to the AP and exchanging data in 10/100 Mbps auto-negotiation mode. Connect this port using an Ethernet cable to an IEEE 802.3af PoE device 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:

(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

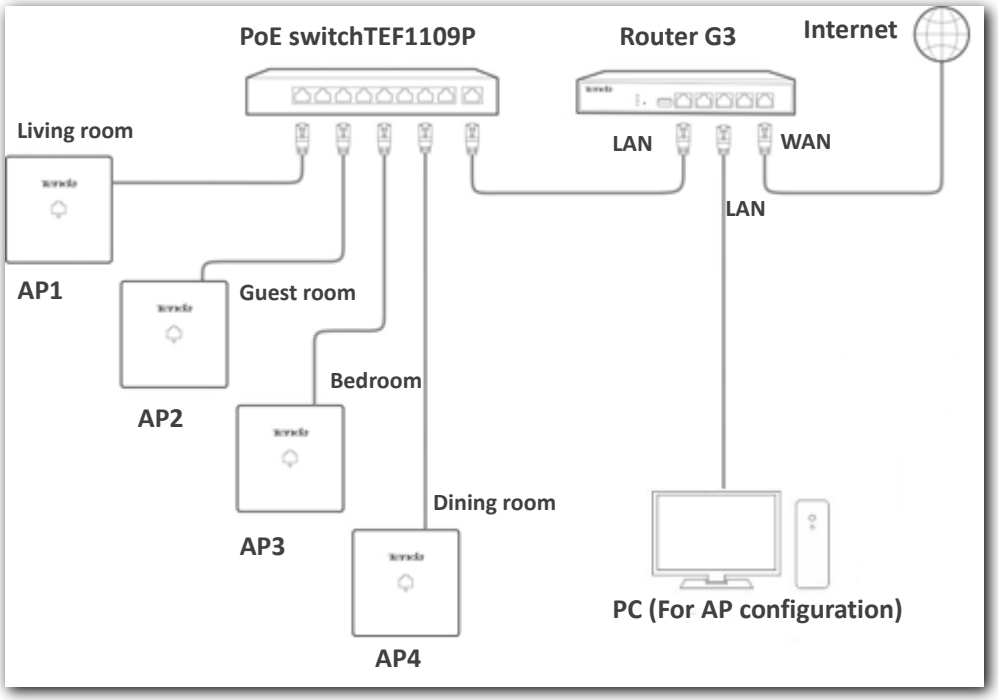
2.1 Large Apartment or Villa

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

For a large apartment or villa, you are recommended to adopt the Tenda wireless product solution, which includes a wired router (such as G3), a PoE switch (such as TEF1109P), and 4 to 8 W9. Deploy one W9 in each room and place the router and switch in an electronic junction box. The following describes the procedure.

Step 1 Connect the devices.

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



Step 2 Configure the AP.

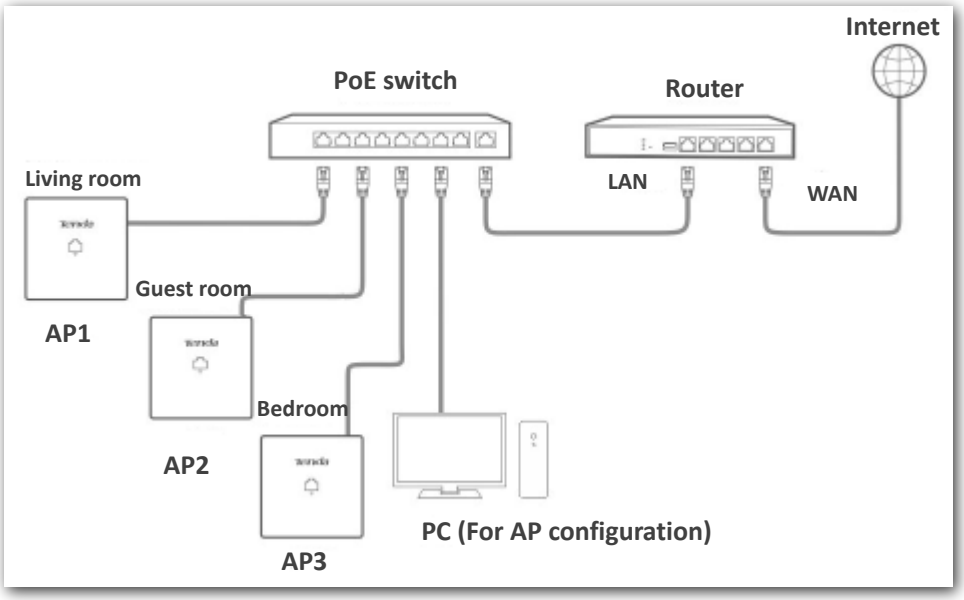
1. Start a web browser, enter the management IP address of the router to log in to the web UI of the router, and configure the APs. For details about how to configure the AP on the router web UI, refer to the user guide of the router. The user guide is available at http://www.Tenda.com.cn.

2.1.2 Deploying the AP with a Router of Another Brand

The following describes the procedure.

Step 1 Connect the devices.

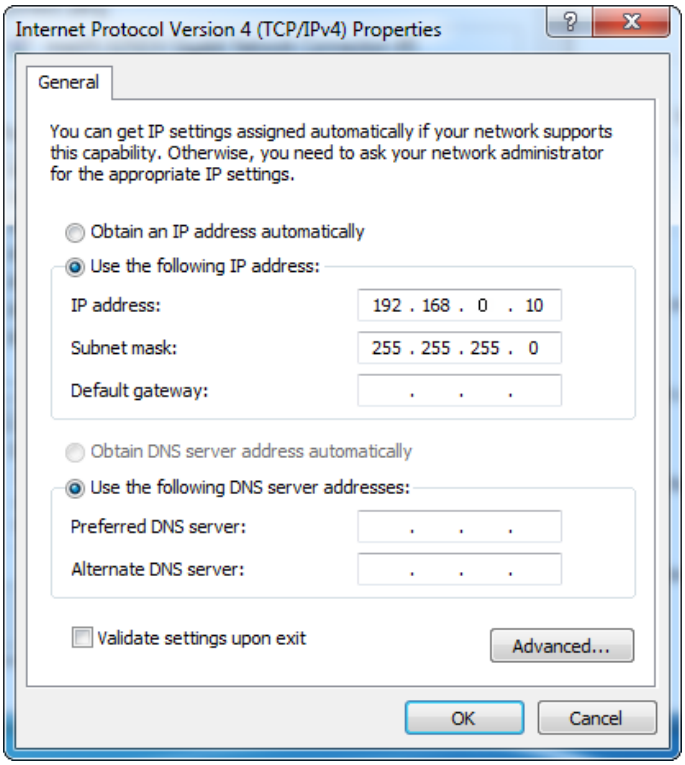
1. Use an Ethernet cable to connect the computer to the PoE switch.
2. Connect one AP (such as AP1) to the PoE switch, as shown in the following topology. Change the IP address of the AP to avoid IP address conflicts. Repeat this procedure to configure the other APs.



Step 2 Set the IP Address of Your Computer (Example: Windows 7).

1. 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**.

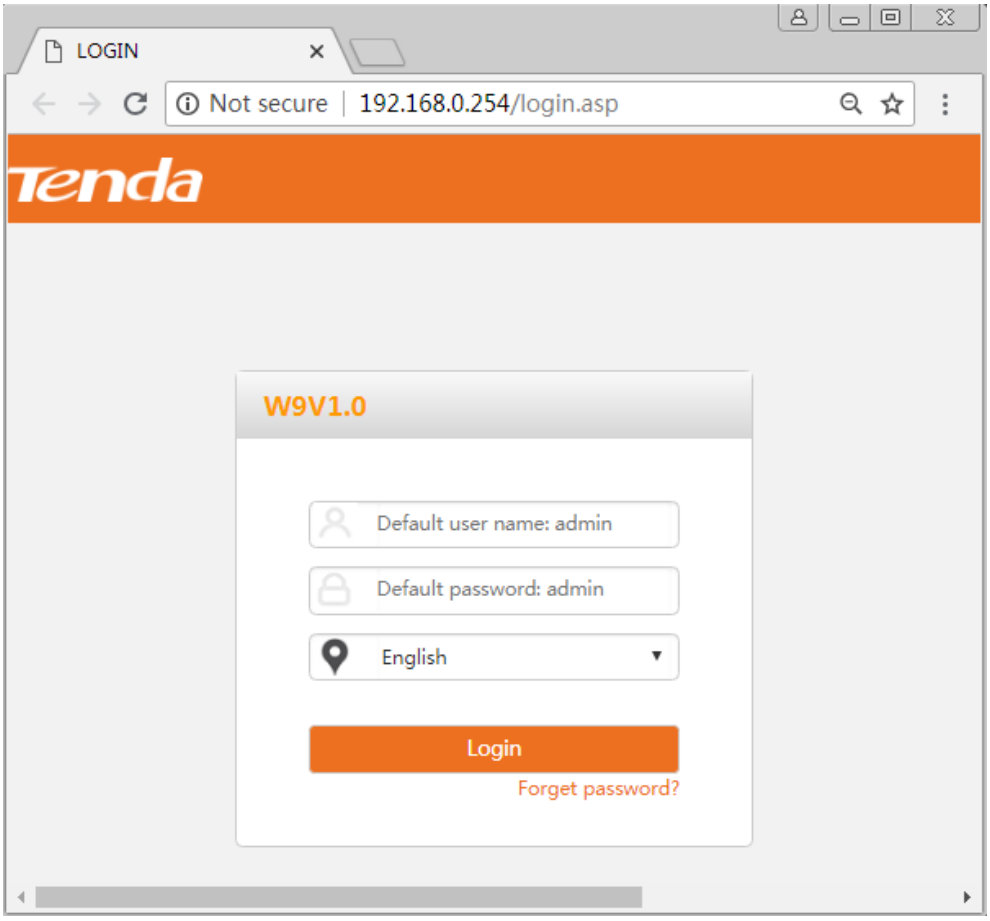
2. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, select **Use the following IP address**, set **IP address** to **192.168.0.*X*** (*X*: 2 - 253) and **Subnet mask** to **255.255.255.0**, and click **OK**.



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

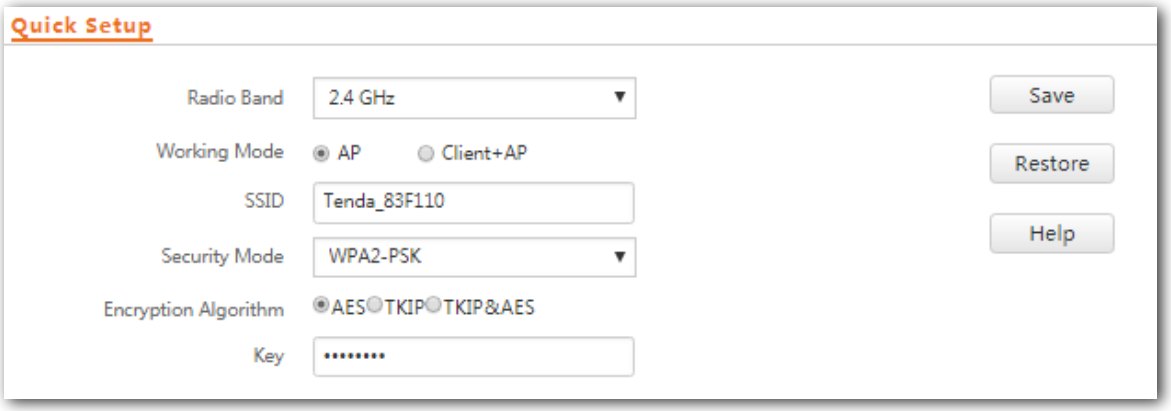
1. Start a web browser, enter the management IP address of the AP (default: **192.168.0.254**), and press **Enter**.

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

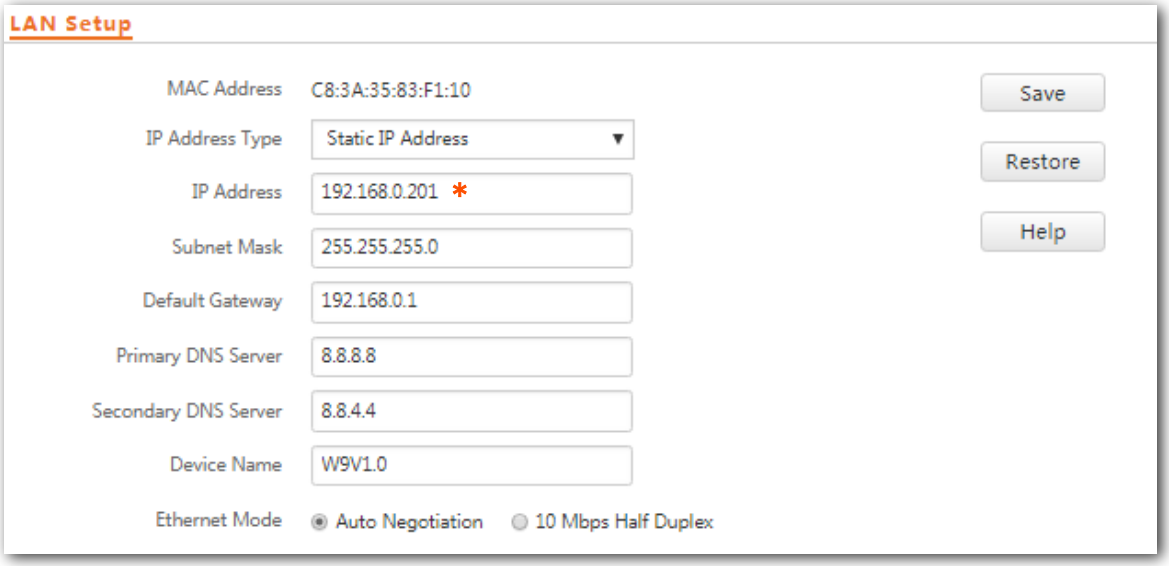


Step 4 Set AP1.

1. To access the page, click **Quick Setup**. Select the check box of **AP Mode**, enter an SSID (wireless network name), select **WPA2-PSK** from the dropdown list box of **Security Mode**, select the check box of **AES** as the **Cipher Type**, enter a security key (wireless network password, such as 12345678), and click **Save**.



2. Choose **Network Settings > LAN Setup,** change the IP address to an unused IP address that in the same network segment as those of the later connected APs, such as 192.168.0.201, and click **Save**.



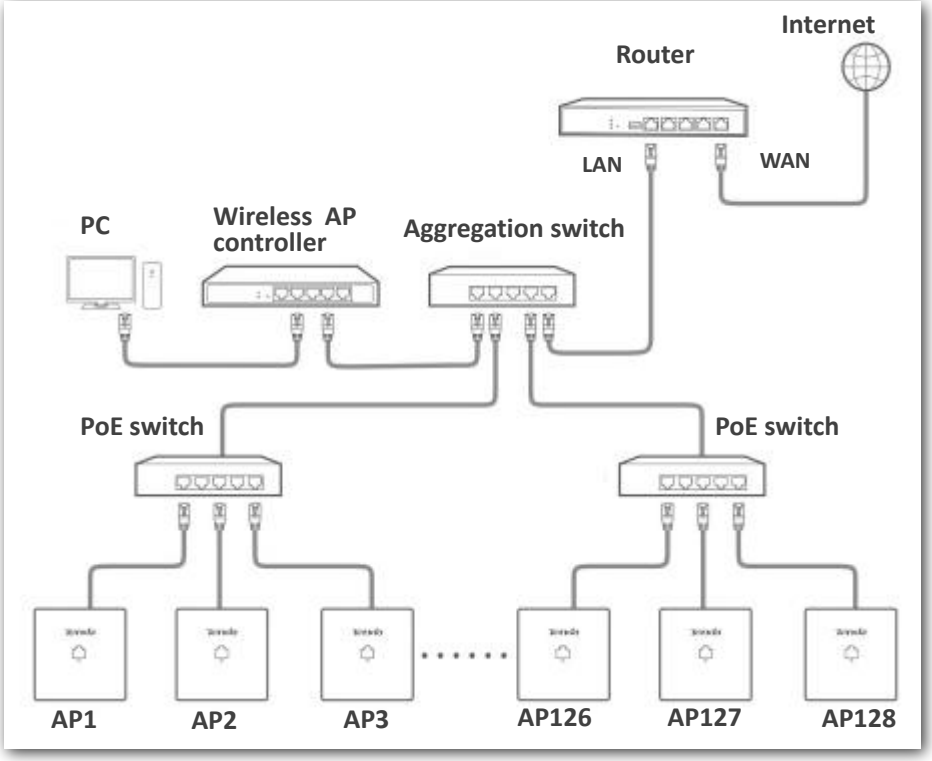
Step 5 Set the other APs. Perform step 3 and step 4 to connect the other APs to the PoE switch one by one and configure them.

For more description of settings, please see contents of Chapter 4.

2.2 Hotel

A large number of APs need to be deployed in a hotel. You can use a Tenda wireless AP controller (such as M3) to configure and manage them centrally and efficiently. The following describes the procedure.

Step 1 Connect the devices.
See the following figure.



Step 2 Configure the APs.
Log in to the web UI of the AP controller on the computer connected to the AP controller. For details about how to configure the AP on the web UI of the AP controller, visit http://www.Tenda.com.cn to download the user guide.

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

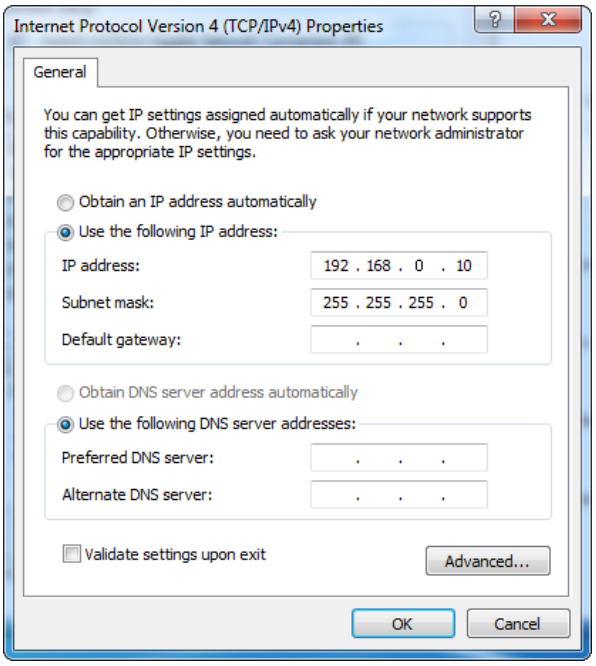
3 Login

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. The procedure is as follows:

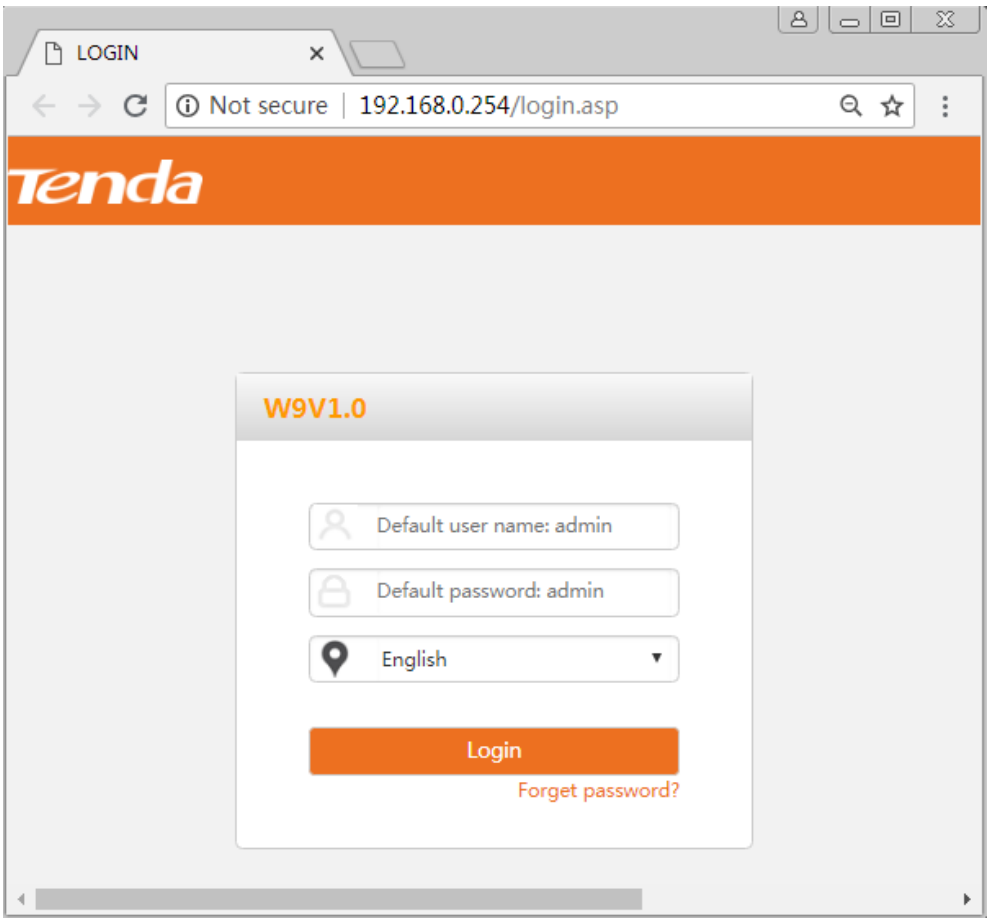
Step 1 Use an Ethernet cable to connect the management computer to the AP or the switch connected to the AP.

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**.



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/admin**) and click **Login**.

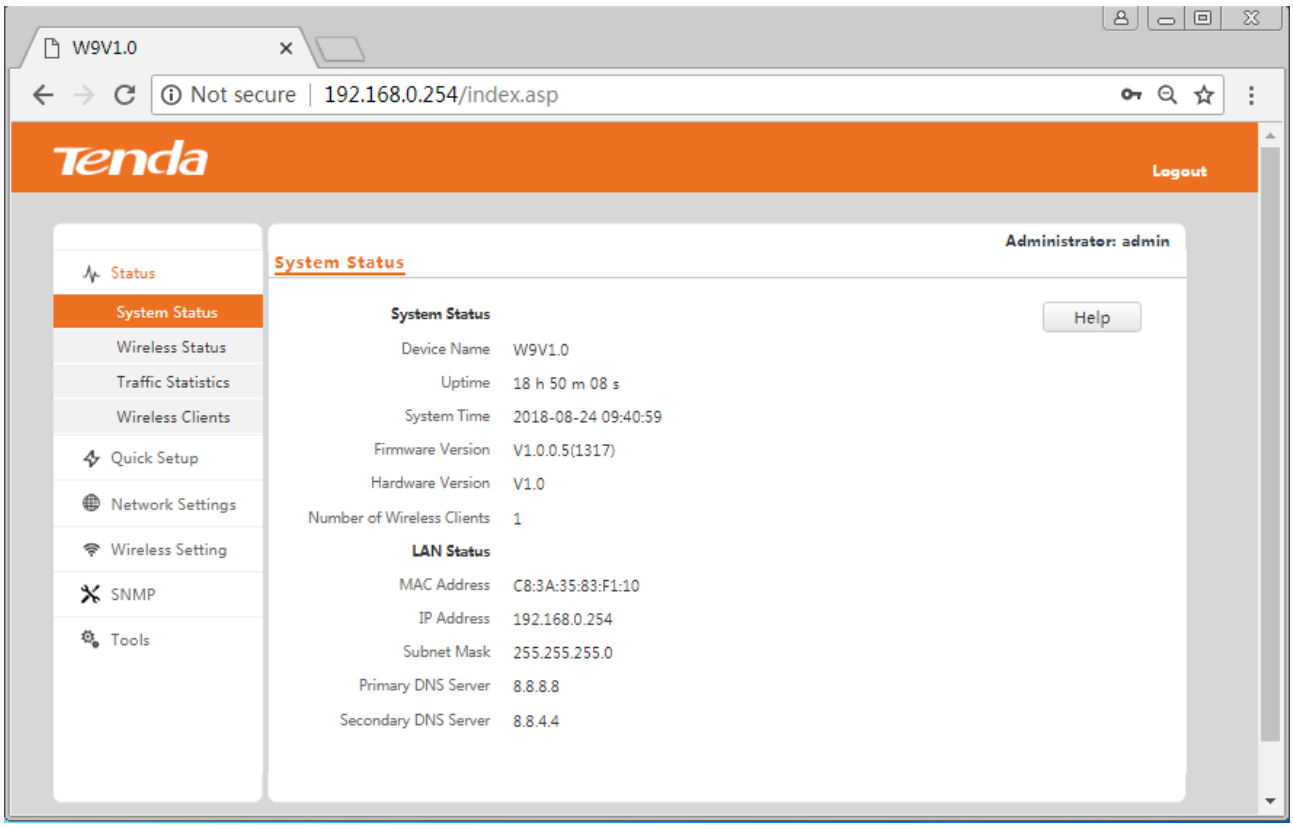


NOTE

If the login page is not displayed, refer to Q2 in **FAQ**.

---End

You can now start configuring the AP.

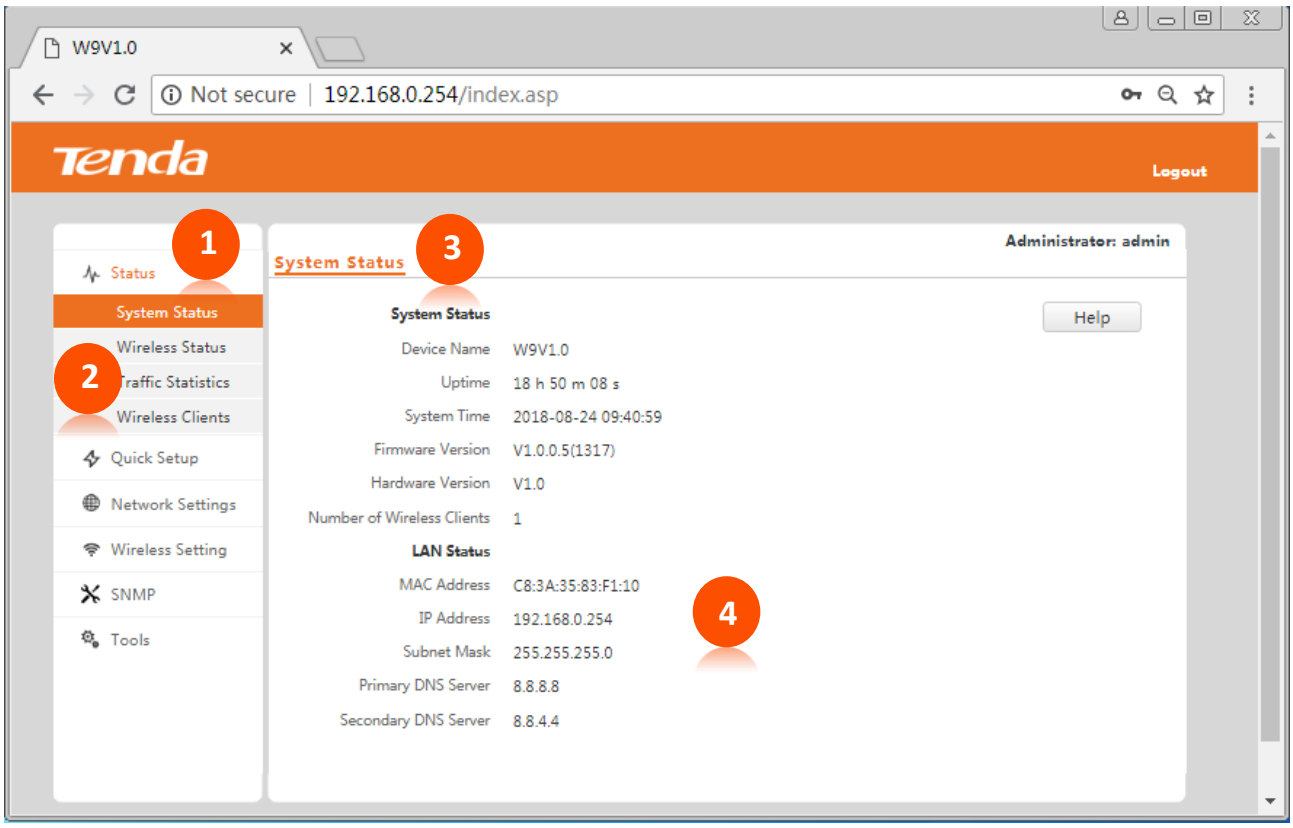


3.2 Logging out of the Web UI of the AP

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. You can log out by clicking Logout in the upper-right corner.

3.3 Web UI Layout

The web UI of the AP is composed of four parts, including the 1-level navigation tree, 2-level navigation tree, tab page area, and configuration area. See the following figure.



TIP

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.

No.	Name	Description
1	1-level navigation bar	The navigation bars and tab pages display the function menu of the AP. When you select a function in navigation bar, the configuration of the function appears in the configuration area.
2	2-level navigation bar	
3	Tab page area	
4	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 refresh the current page.
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

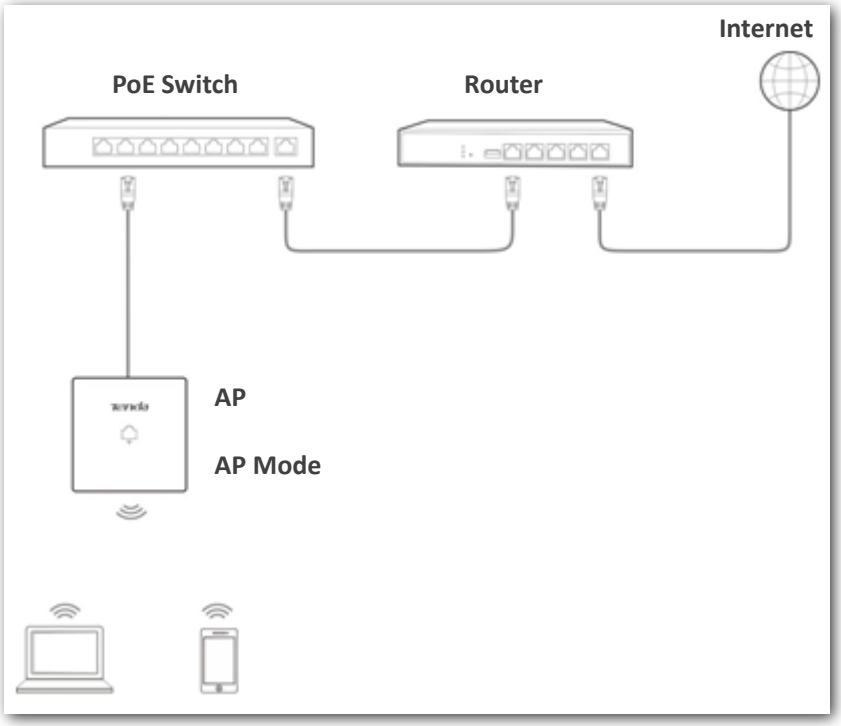
4.1 Overview

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

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

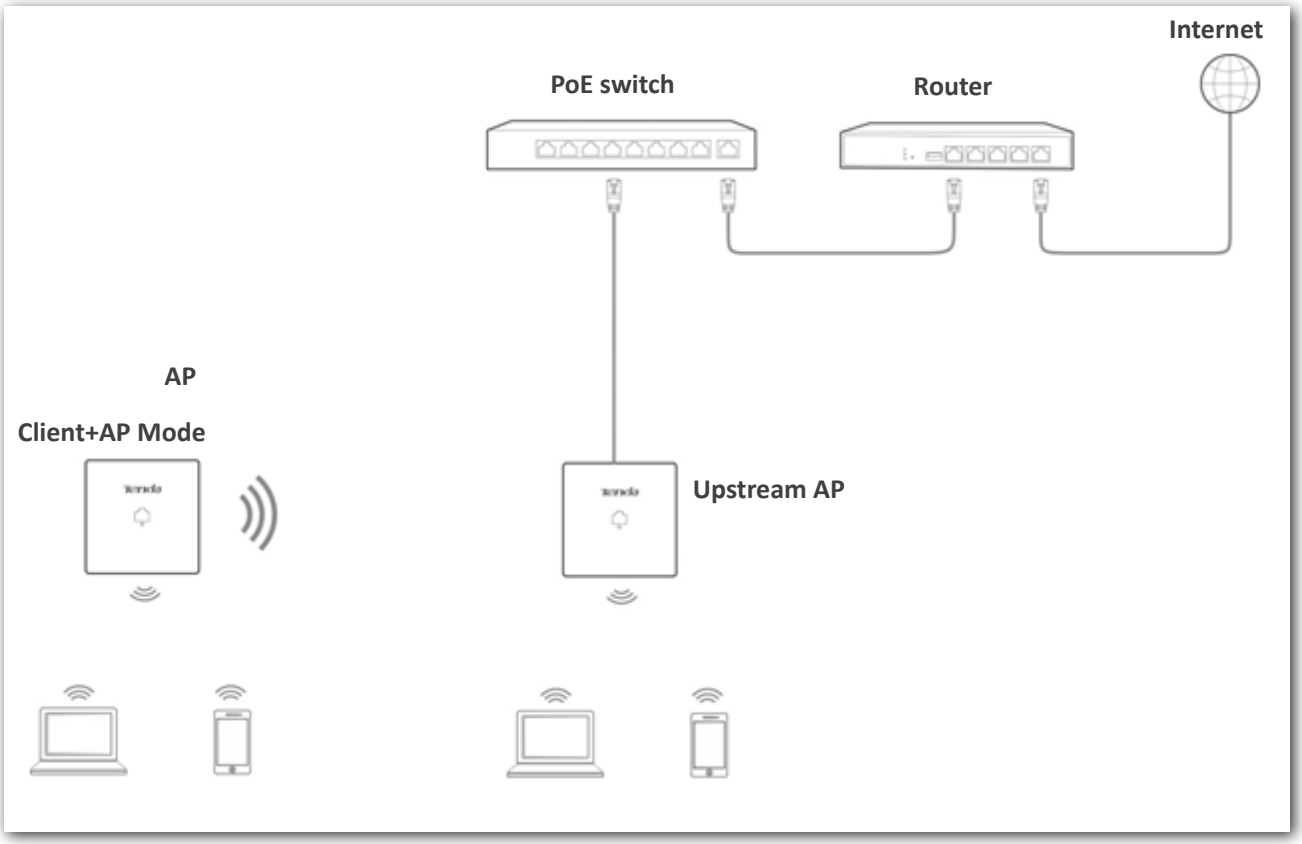
- AP Mode

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 Quick Setup

4.2.1 AP Mode

TIP

Before configuration, ensure that the upstream device has been connected to the internet.

Step 1 Choose **Quick Setup**.

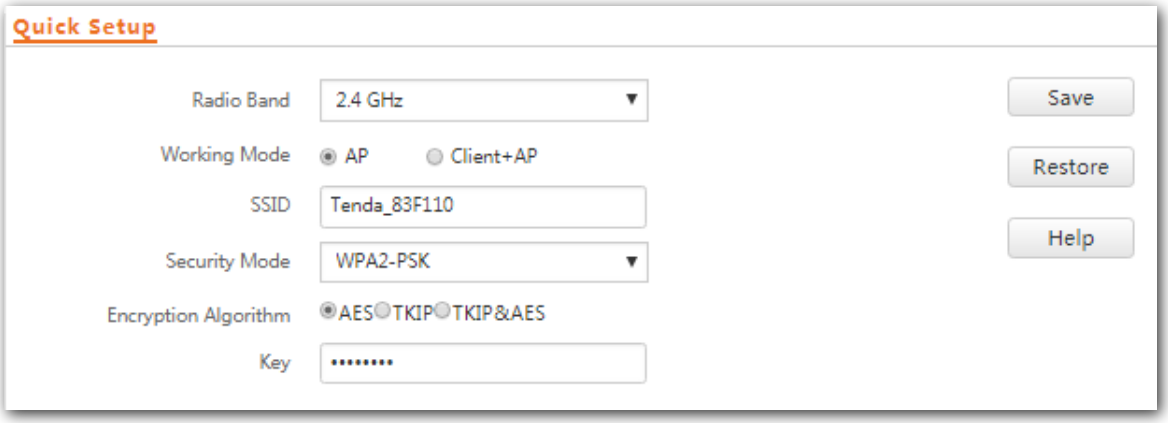
Step 2 Select a radio band from the drop-down list box to be configured, which is **2.4 GHz** in this example.

Step 3 Keep the default configuration of working mode.

Step 4 (Optional) Change the value of **SSID**, which indicates the primary SSID of the AP, to your wireless network name.

Step 5 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 6 Click **Save**.



Step 7 To configure the WIFi network of another radio band, select the radio band, and repeat **steps 3**-**6**.

---End

Parameter description

Parameter	Description
Radio Band	It specifies the radio band of the WiFi network to be configured.
Working Mode	It specifies the working mode of the AP, including AP mode and Client+AP mode.
SSID	It specifies the primary SSID (wireless network name) of the AP.
Security Mode	It specifies the security mode of the wireless network of the AP. Options include: None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.
Encryption Algorithm	It specifies the WPA encryption algorithm of the repeated WiFi network. After you select the upstream WiFi network from the scanned wireless network list, this parameter will be populated automatically.
Key	Manually enter the WiFi password of the repeated WiFi network.

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

TIP

Before configuration, ensure that the upstream AP has been connected to the internet.

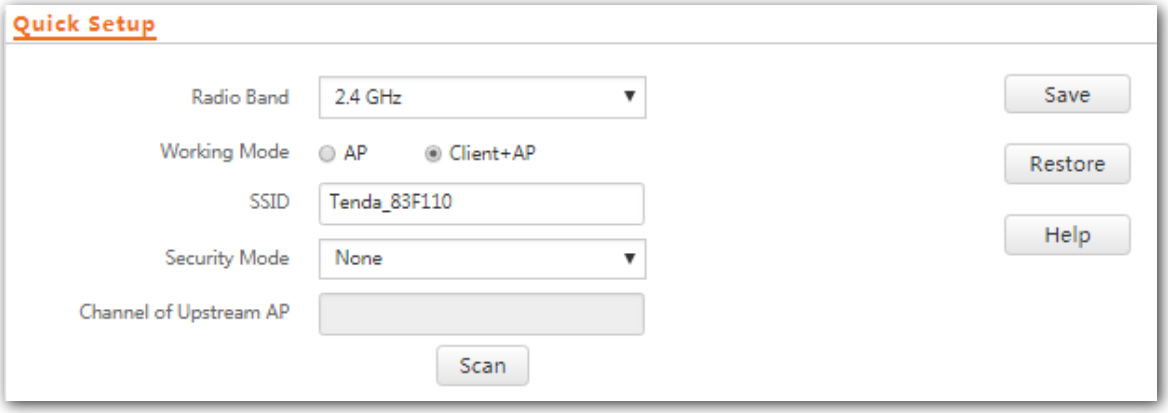
For two bands bridging scenario, please ensure that you choose the same upstream AP for both the 2.4 GHz and 5 GHz WiFi networks.

Step 1 Choose **Quick Setup**.

Step 2 Select the radio band from the drop-down list box to be configured, which is **2.4 GHz** in this example.

Step 3 Set **Working Mode** to **Client+AP**.

Step 4 Click **Scan**.



Step 5 Select the wireless network to be extended from the wireless network list that appears.

NOTE

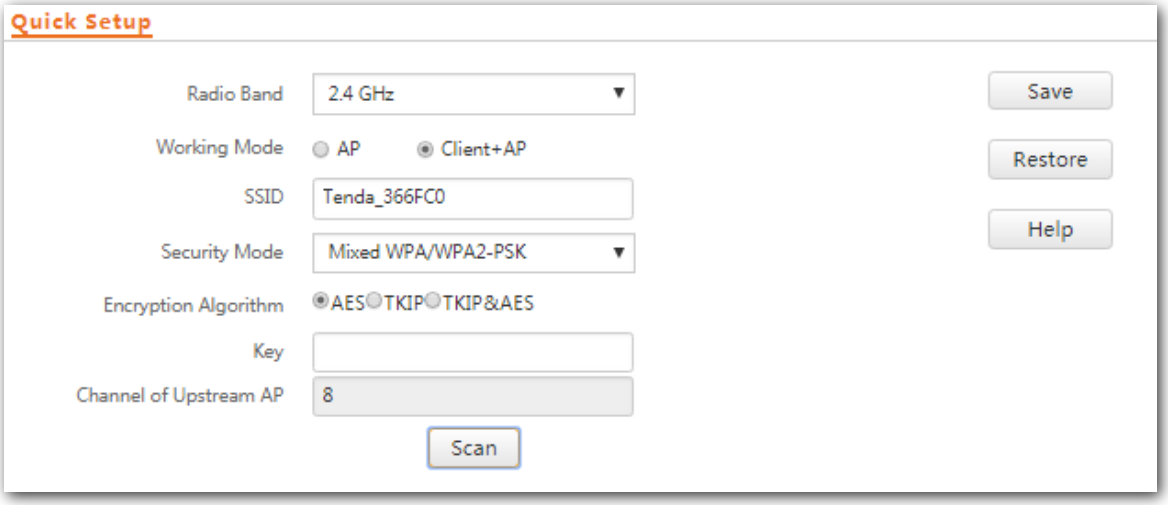
- If no wireless network is found, choose **Wireless Settings** > **Radio Settings**, ensure that **Enable Wireless** is selected, and try scanning wireless network again.
- After a wireless network to be extended is selected, the SSID, security mode, and channel of the wireless network are populated automatically. The **Key** (if any) should be entered manually.

Step 6 Click **Disable Scan**.

Select	SSID	MAC Address	Network Mode	Channel Bandwidth	Channel	Extension Channel	Security Mode	Signal Strength
○	Tenda_843F00	c8:3a:35:84:3f:01	bgn	20MHz	7	none	none	-14dBm
○	Tenda_366FC0	c8:3a:35:36:6f:c1	bgn	20MHz	8	none	wpa&wpa2/aes	-34dBm

Step 7 If the wireless network of the upstream device is encrypted, set **Key** to the wireless network password of the device.

Step 8 Click **Save**.



Step 9 To extend the WiFi network at 5 GHz radio band, select the radio band, and repeat **steps 3**-**8**.

---End

After the configuration, you can select the SSID (click **Status** > **Wireless Status** to view the SSID of this AP) 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 Settings** > **SSID Settings** page.

Parameter Description

Parameter	Description
Radio Band	It specifies the radio band of the WiFi network to be configured.
Working Mode	It specifies the working mode of the AP, including AP mode and Client+AP mode. • **AP mode**: In this mode, wireless clients can connect to this device, but this device cannot connect to peers. • **Client+AP mode**: In this mode, this device is bridged wirelessly to an upstream device and provides the wireless access service to clients.
SSID	It specifies the WiFi network name (SSID) of the WiFi network to be repeated. After you select the upstream WiFi network from the scanned wireless network list, this parameter will be populated automatically.
Security Mode	It specifies the security mode of which the upstream WiFi network adopted. After you select the upstream WiFi network from the scanned wireless network list, this parameter will be populated automatically. The AP can repeat WiFi network encrypted with None or WEP (Open or Shared), WPA-PSK, WPA2-PSK and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode. NOTE The AP can scan the WiFi network with WPA (WPA2) Enterprise encryption, but cannot identify its security mode.
Authentication Type	Manually select the authentication type of the upstream device if the security mode of the upstream device is WEP.
Default Key	Manually choose the default key number of the upstream device if the security mode of the upstream device is WEP.
Key 1/2/3/4	WiFi password of the upstream device if the security mode of the upstream device is WEP.
Encryption Algorithm	It specifies the WPA encryption algorithm of the repeated WiFi network. After you select the upstream WiFi network from the scanned wireless network list, this parameter will be populated automatically.
Key	Manually enter the WiFi password of the upstream device if the security mode of the upstream device is WPA.
Channel of Upstream AP	It specifies the channel of the upstream AP. After you select the upstream WiFi network from the scanned wireless network list, this parameter will be populated automatically.

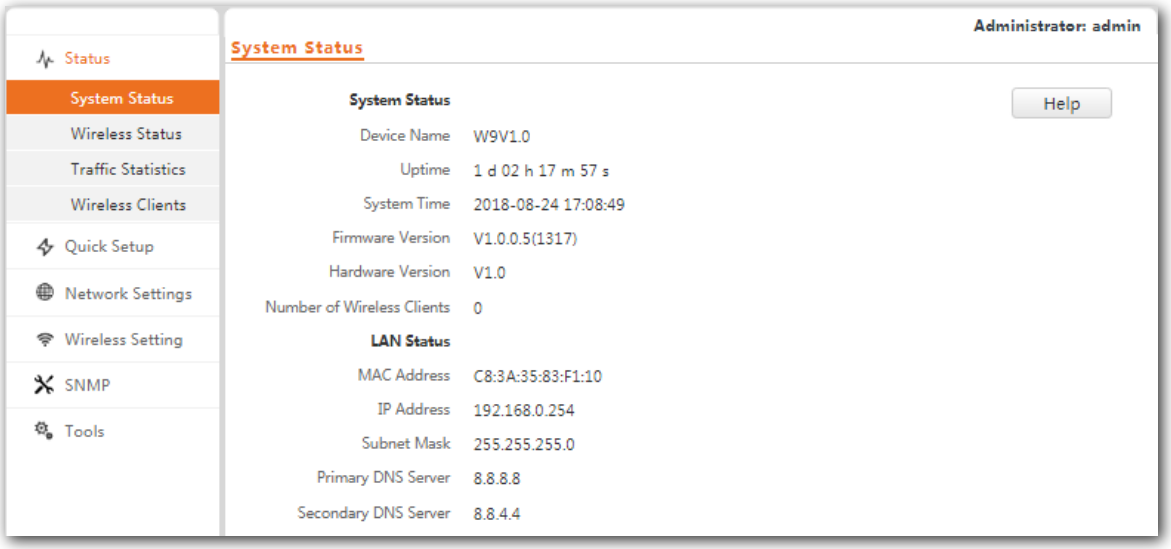
5 Status

This module allows you to view system status, wireless status, traffic statistics and wireless clients.

5.1 System Status

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

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



Parameter description

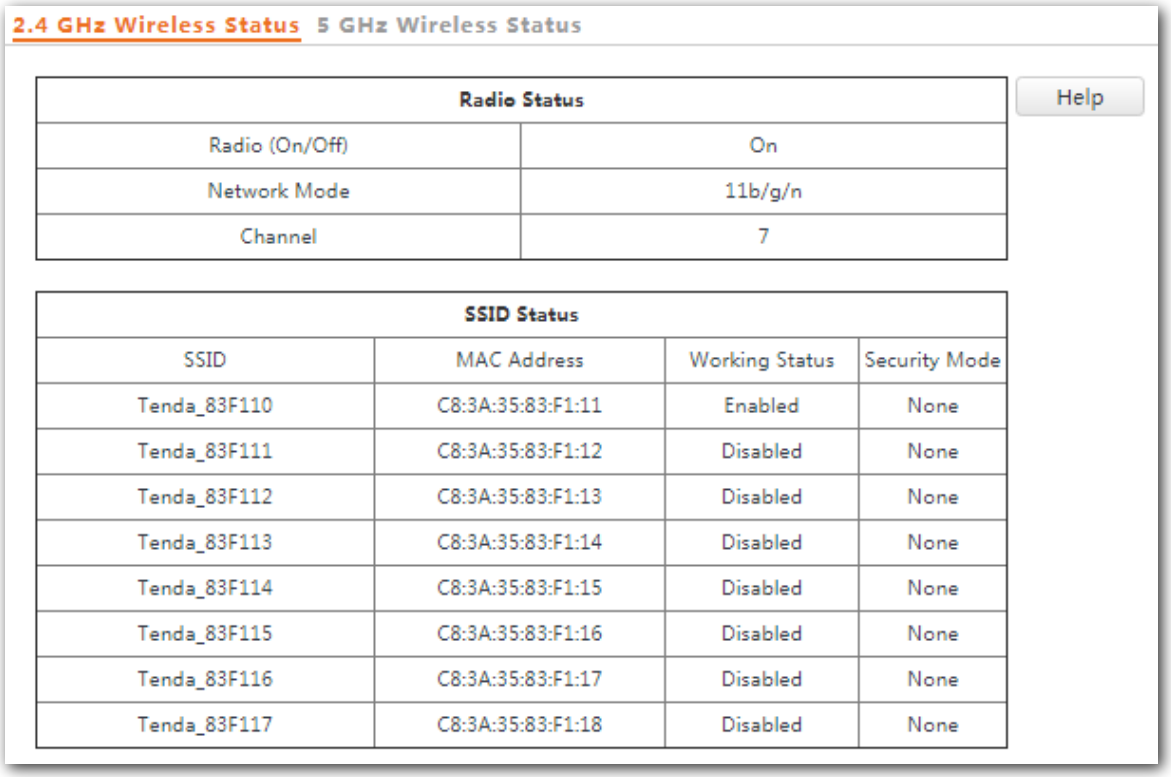
Parameter	Description
Device Name	It specifies the name of the AP. A unique AP name helps quickly identify the AP. You can change the AP name on the **Network Settings** > **LAN Setup** page.
Uptime	It specifies the time that has elapsed since the AP was started last time.
System Time	It specifies the current system time of the AP.
Number of Wireless 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.

Parameter	Description
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 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 Settings** > **LAN Setup** page.
Subnet Mask	It specifies the subnet mask of the IP address of the AP.
Primary DNS Server	It specifies the primary DNS server of the AP.
Secondary DNS Server	It specifies the secondary DNS server of the AP.

5.2 Wireless Status

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

This page displays general radio status and SSID status of the AP. By default, the page displays the information of 2.4 GHz wireless status. To view the wireless status of 5 GHz, click **5 GHz Wireless Status.**



Parameter description

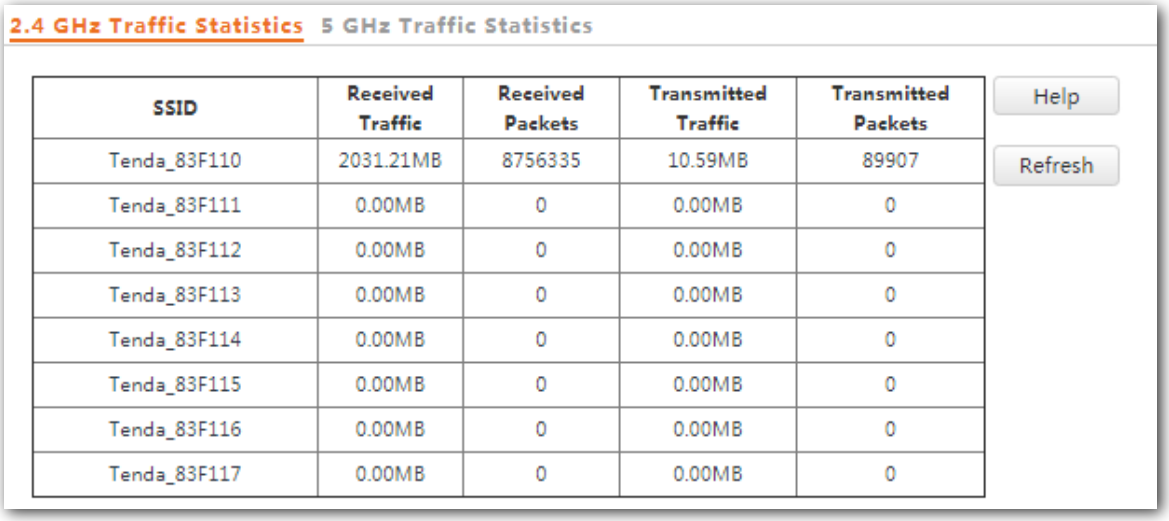
Parameter		Description
Radio Status	Radio (On/Off)	It specifies whether the wireless function of the AP is enabled.
	Network Mode	It specifies the current network mode of the AP.
	Channel	It specifies the current working channel of the AP.
SSID Status	SSID	It specifies the names of all the wireless networks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

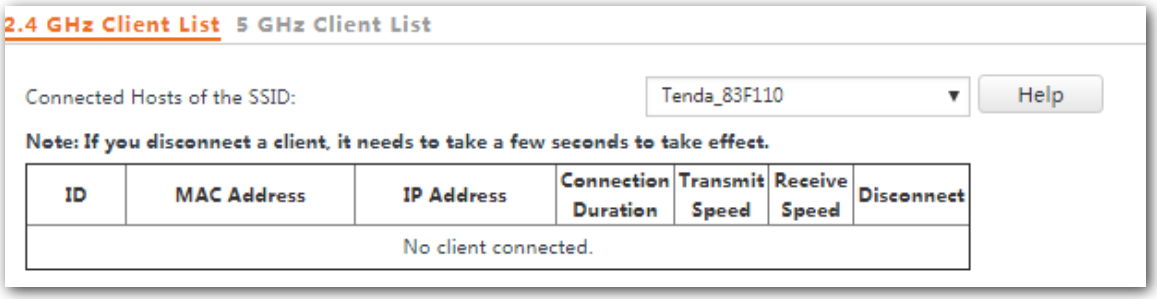
By default the page displays the traffic statistics information of 2.4 GHz. To view information about 5 GHz, click **5 GHz Traffic Statistics.** To view the latest statistics, click **Refresh**.



5.4 Wireless Clients

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

This page displays information about the wireless clients connected to the wireless networks corresponding to the SSIDs of the AP.



By default, the page displays information about the wireless clients connected to the 2.4 GHz wireless network corresponding to the primary SSID of the AP. To view information about the wireless clients connected to the 5 GHz wireless network corresponding to the other SSID, click the **5 GHz Client List** tab, and select the SSID from the drop-down list box in the upper-right corner.

Parameter description

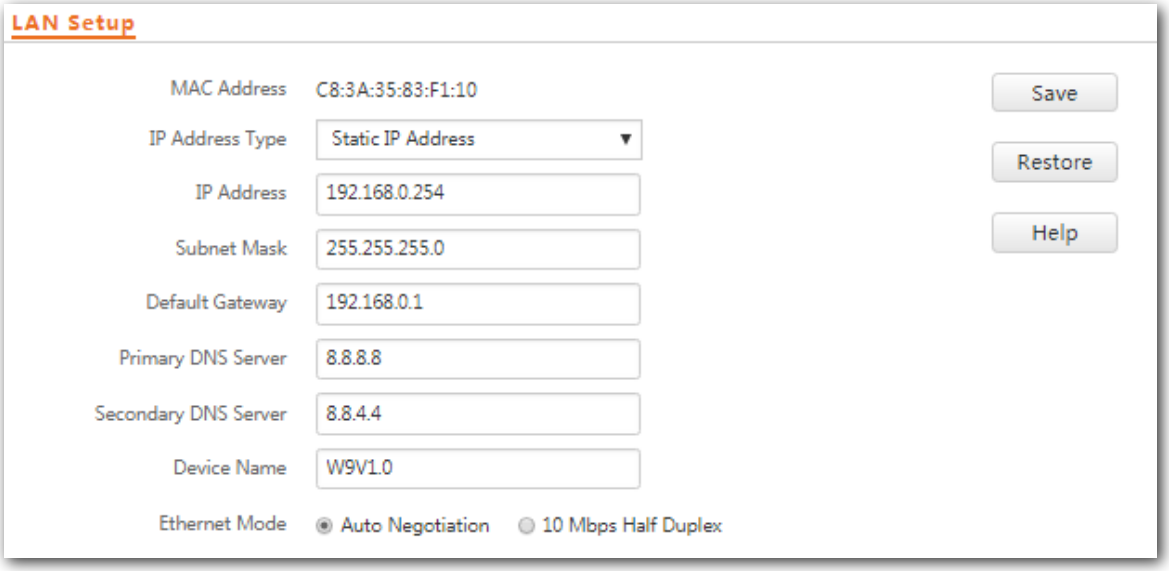
Parameter	Description
MAC Address	It specifies the MAC address of the wireless client.
IP Address	It specifies the IP address of the wireless client.
Connection Duration	It specifies the online time of the wireless client.
Transmit Speed	It specifies the current transmit speed of the wireless client.
Receive Speed	It specifies the current receive speed of the wireless client.
Disconnect	Clicking disconnects the corresponding client. To view the disconnected client, choose **Wireless Setting** > **Access Control**.

6 Network Settings

6.1 LAN Setup

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

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



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 IP Address**. • **Static IP Address**: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is set manually. • **DHCP**: 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. TIP If **Address Mode** is set to **DHCP**, 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

Parameter	Description
	server.
IP Address	It specifies the IP address of the AP. The web UI of the AP is accessible at this IP address. 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.
Device Name	It specifies the name of the AP. By default, the name is the model of the AP, such as W9V1.0. 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.
Ethernet Mode	It specifies the Ethernet mode of LAN0 of this AP. • **Auto Negotiation**: This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended. • **10 Mbps Half Duplex**: 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.

6.1.1 Modifying the LAN IP Address of the AP

Manually Setting the IP Address

In this 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.

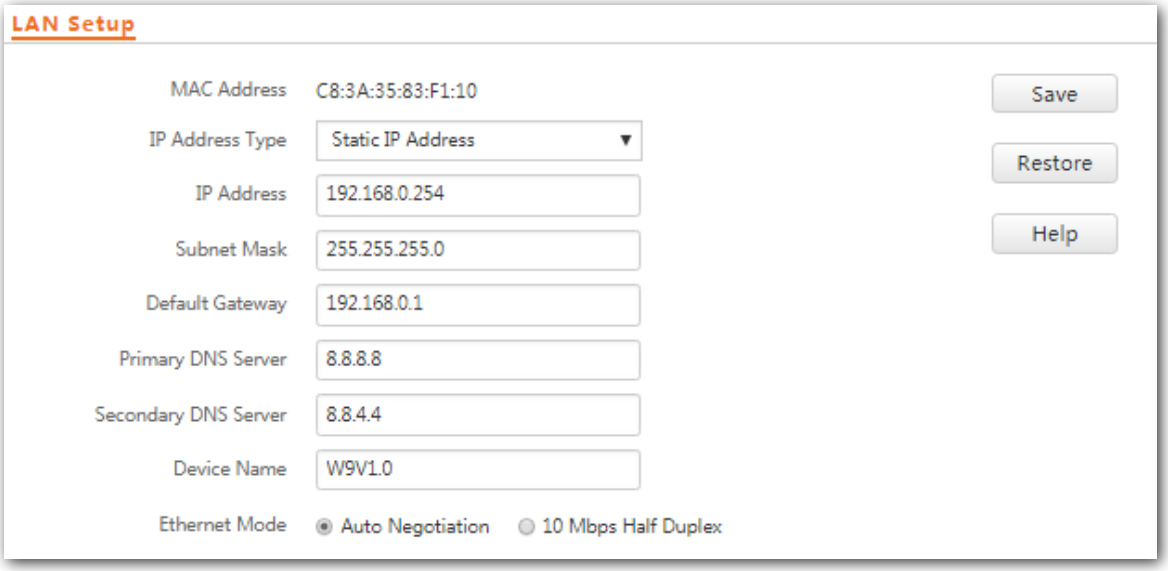
Configuration procedure:

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

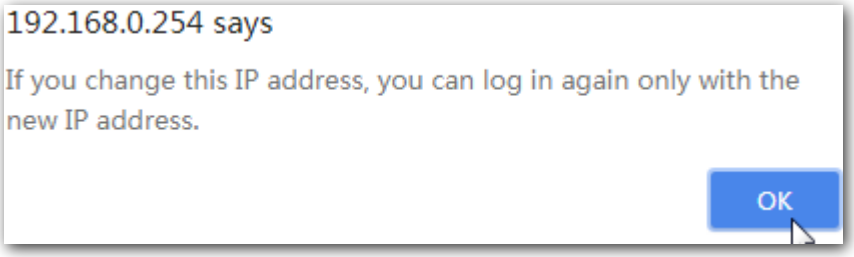
Step 2 Set **IP Address Type** to **Static IP Address**.

Step 3 Set **IP Address**, **Subnet Mask**, **Default 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**.



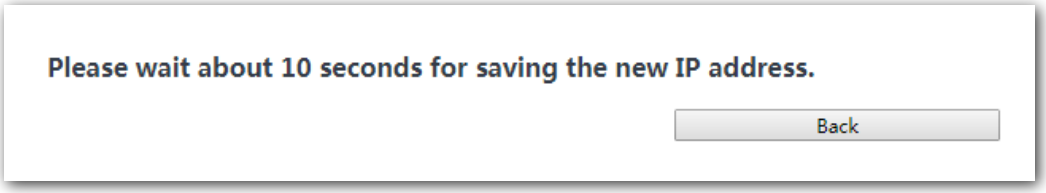
Step 5 Click **OK**.



---End

The following page is displayed. To continue to configure the AP, please do as follows:

- If the new and original IP addresses belong to the same network segment, click **Back** to log in to the web UI of AP again.
- Otherwise, assign your 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

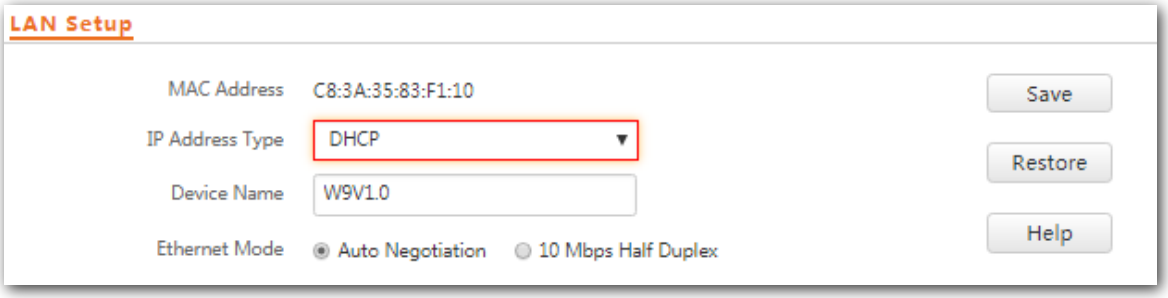
This mode enables the AP to automatically obtain an IP address, a subnet mask, a gateway IP address, DNS server IP addresses from a DHCP server on your LAN. If a large number of APs are deployed, you can adopt this mode to avoid IP address conflicts and effectively reduce your workload.

Configuration procedure:

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

Step 2 Set **Address Mode** to **DHCP**.

Step 3 Click **Save**.



---End

After the configuration, if you want to log in to the web UI of the AP again, 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

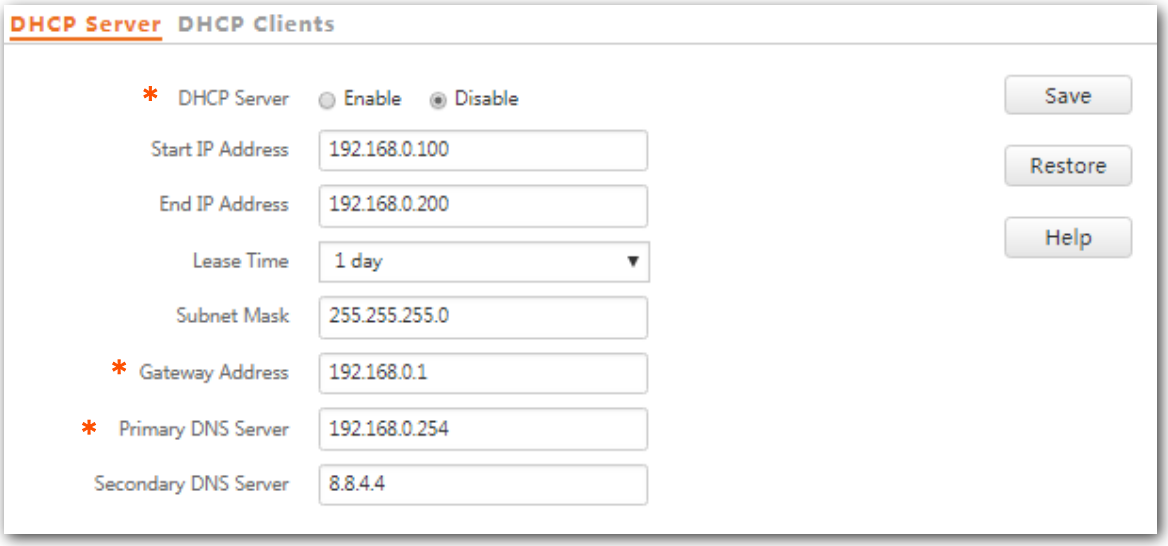
If the new and original IP addresses of the LAN port belong to different network segment, the system changes the IP address pool of the DHCP server function of the AP so that the IP address pool and the new IP address of the LAN port belong to the same network segment.

6.2.2 Configuring the DHCP Server

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

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

Step 3 Click **Save**.



---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**. TIP 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. 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 Address	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**. TIP 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**. TIP 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.

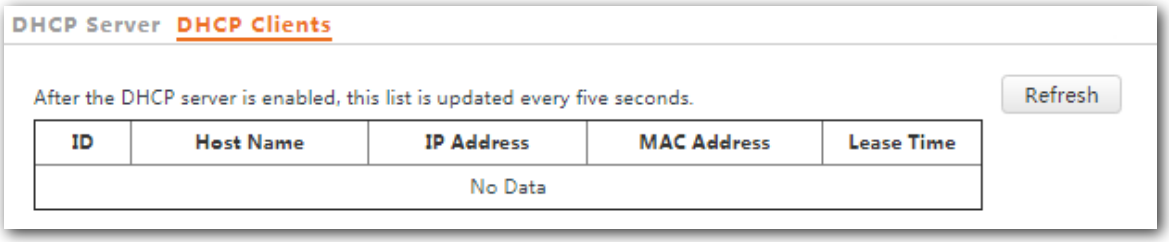
NOTE

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 Settings** > **DHCP Server** and click **DHCP Client** tab.



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. It enhances the security of the wireless network.

It is worth noting that 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

They belong to pre-shared key or personal key modes, where Mixed WPA/WPA2-PSK supports both WPA-PSK and WPA2-PSK.

WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK adopt a pre-shared key for authentication, while the AP generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home wireless networks. Nevertheless, because the initial pre-shared 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 pre-shared 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 Modifying SSID Settings

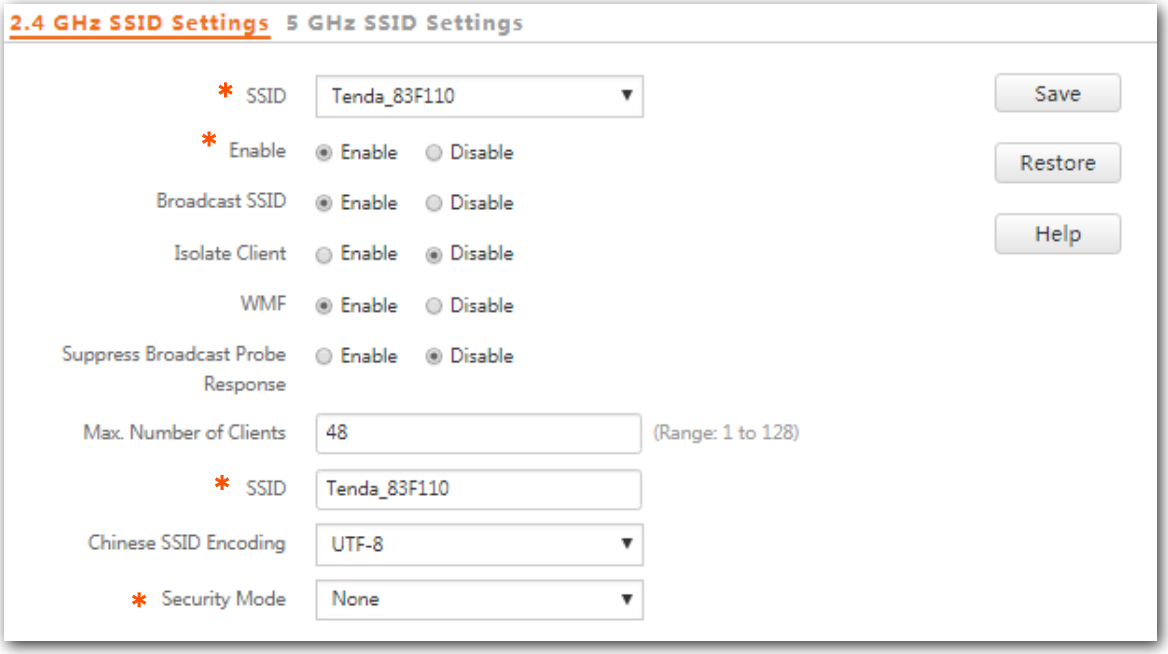
To change the related settings of an SSID, perform the following procedure:

Step 1 Choose **Wireless Setting**> **SSID Settings**.

Step 2 Click the tab to choose the radio band to be set.

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

Step 4 Click **Save**.



---End

Parameter description

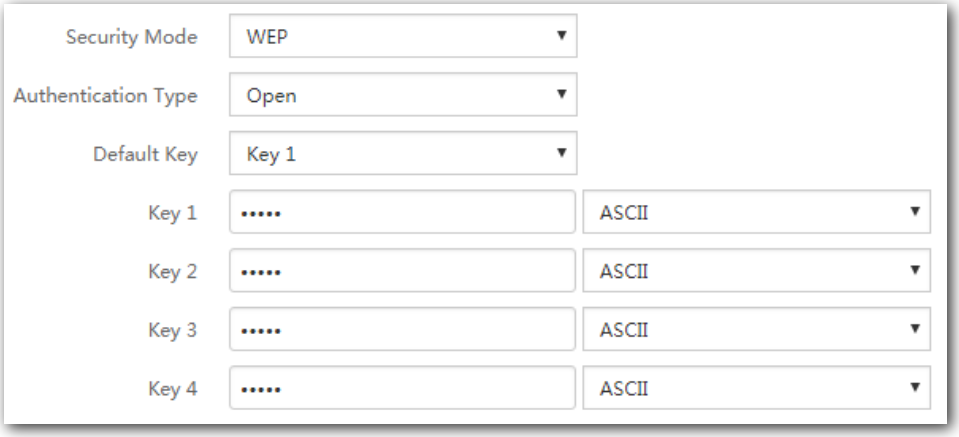
Parameter	Description
SSID	It specifies the SSID to be configured. The AP supports 8 SSIDs for the 2.4 GHz and 4 SSIDs for the 5 GHz, and the first SSID displayed is the primary SSID.
Enable	It specifies whether to enable the selected SSID. By default, the primary SSID is enabled. While the other SSIDs are disabled. Users can enable them if needed.
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

Parameter	Description
	enter the SSID on the client. TIP 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.
Suppress Broadcast Probe Response	By default, wireless devices keep sending Probe Request packets that include the SSID field to scan their nearby wireless networks. After receiving such packets, this device determines whether the wireless devices are allowed to access its wireless networks based on the packets and responds using the Probe Response packets (including all Beacon frame parameters), which consumes a lot of wireless resources. After this function is enabled, this device does not respond to the requests without an SSID, saving wireless resources.
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. 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.Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.

- None

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

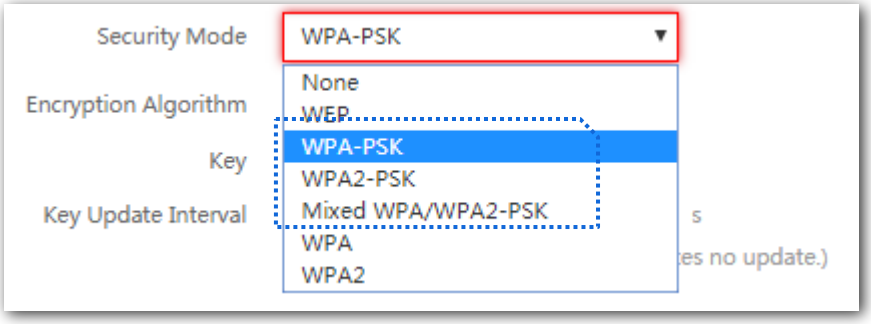
- WEP



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 invalid users connect to the wireless network.
Default Key	It specifies the WEP key for the Open or Shared encryption type. For example, if **Default Key** is set to **Security Key 2**, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by **Security 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	These parameters are dedicated to the 802.1x authentication type. It specifies the IP address/port number/shared key of the RADIUS server for authentication.
RADIUS Port	
RADIUS Password	

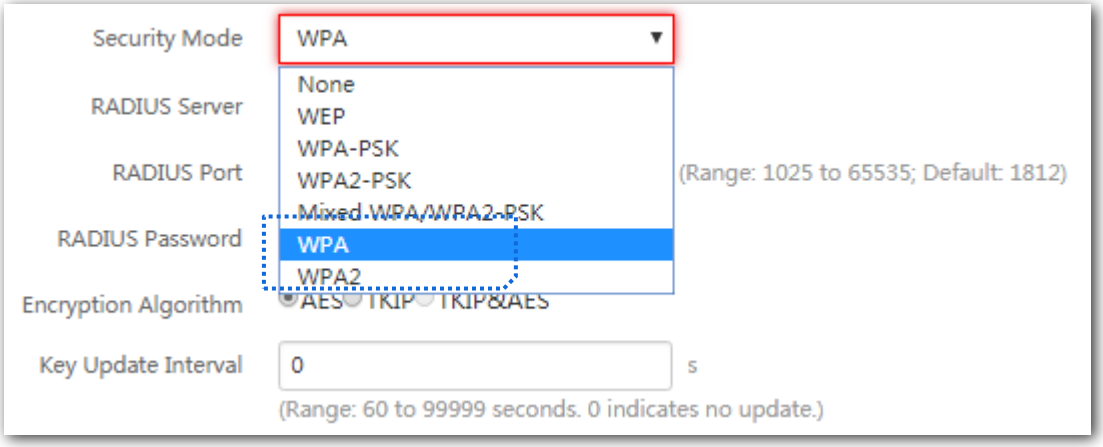
- WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK



Parameter description

Parameter	Description
Security Mode	It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. • **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. • **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 pre-shared 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



Parameter description

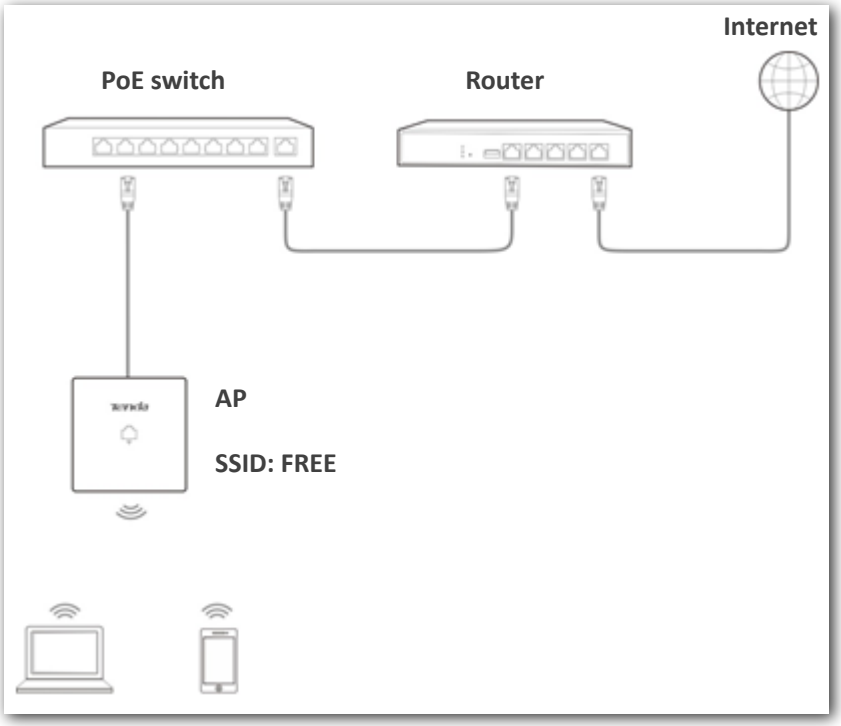
Parameter	Description
Security Mode	The **WPA** and **WPA2** options are available for network protection with a RADIUS server. • **WPA**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA. • **WPA**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA.
RADIUS Server	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**. • **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 SSID 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 WiFi network.



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 Setting** > **SSID Settings**.

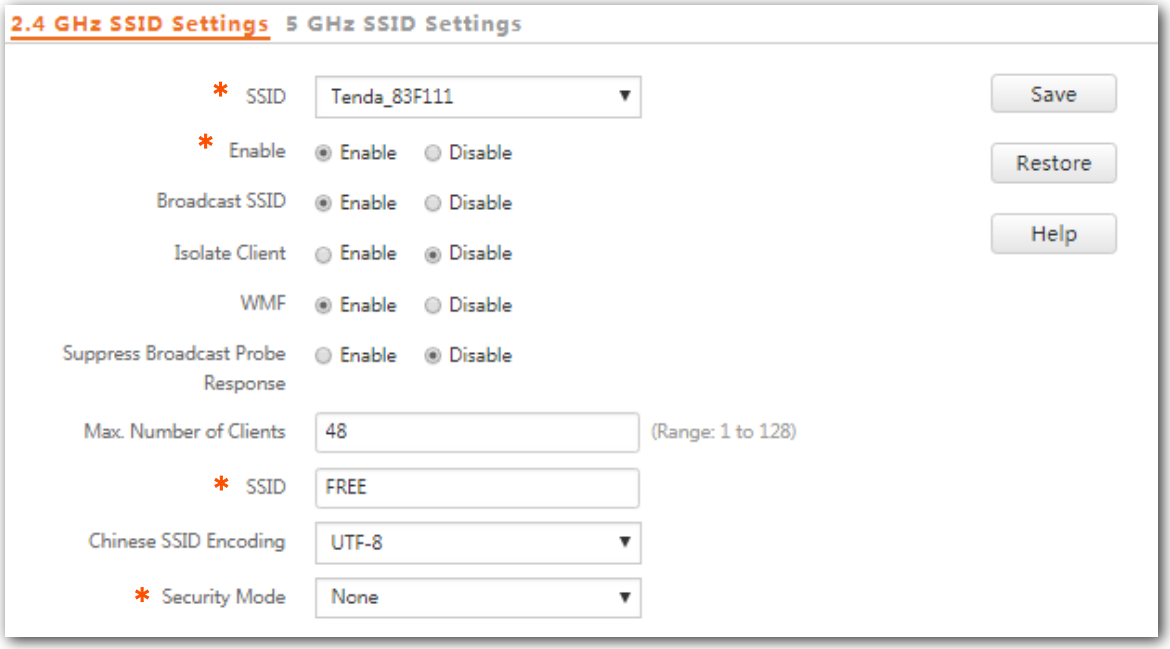
Step 2 Select the second SSID from the **SSID** drop-down list box.

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**.



---End

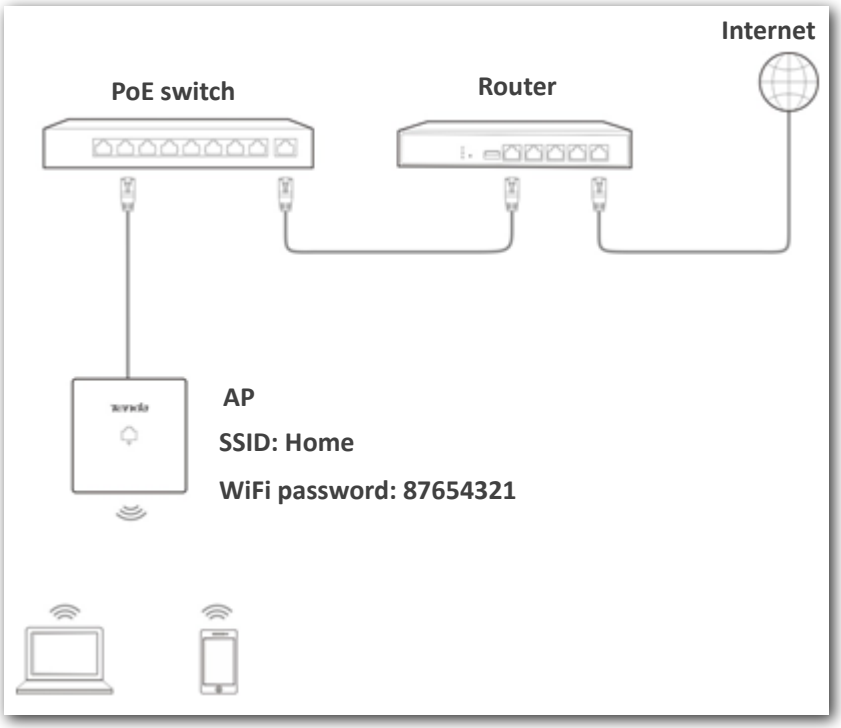
Verification

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

Setting up a Wireless Network Encrypted Using WPA/WPA2-PSK

Networking requirement

A home wireless network with a certain level of security must be set up through a simply procedure. In this case, WPA/WPA2 pre-shared key mode is recommended. 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 Setting** > **SSID Settings**.

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

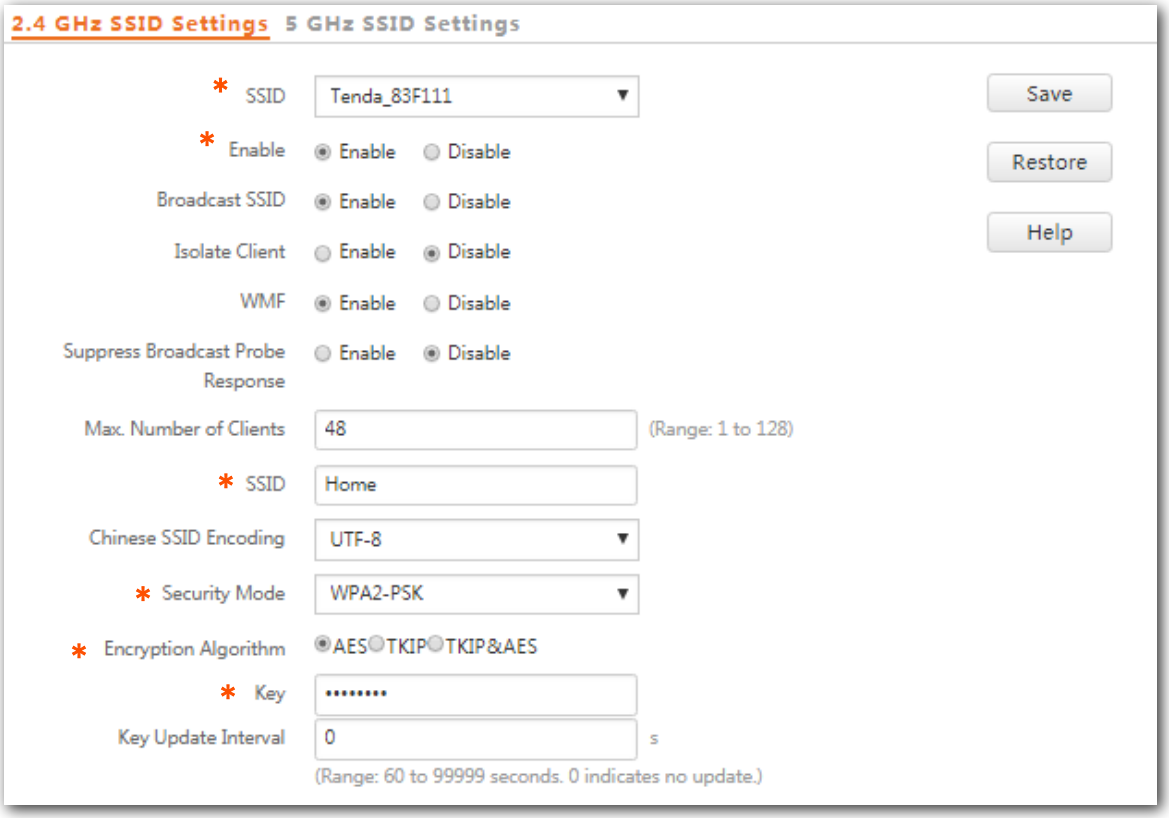
Step 3 Select the **Enable** check box.

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**.



---End

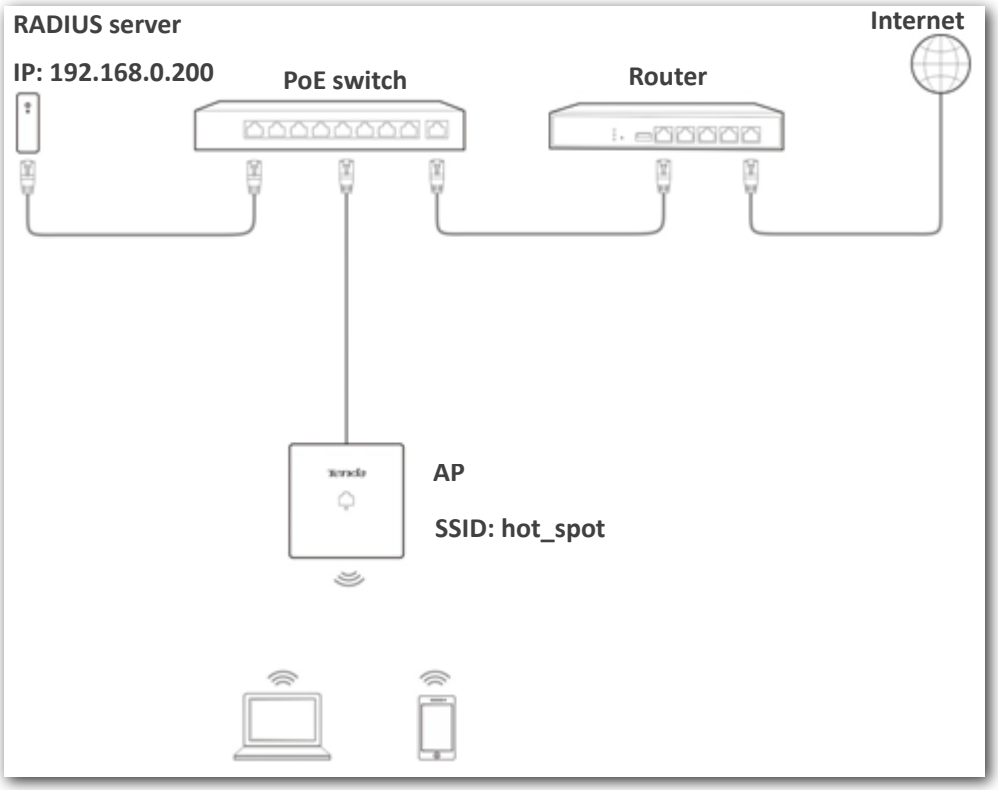
Verification

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. In this case, WPA or WPA2 pre-shared key mode is recommended. See the following figure.



Configuration procedure

Configure the AP

Assume that the IP address of the RADIUS server is 192.168.0.200, the Key is 12345678, and the port number for authentication is 1812.

Assume that the second SSID of the AP is used.

Step 1 Choose **Wireless Setting** > **SSID Settings**.

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

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

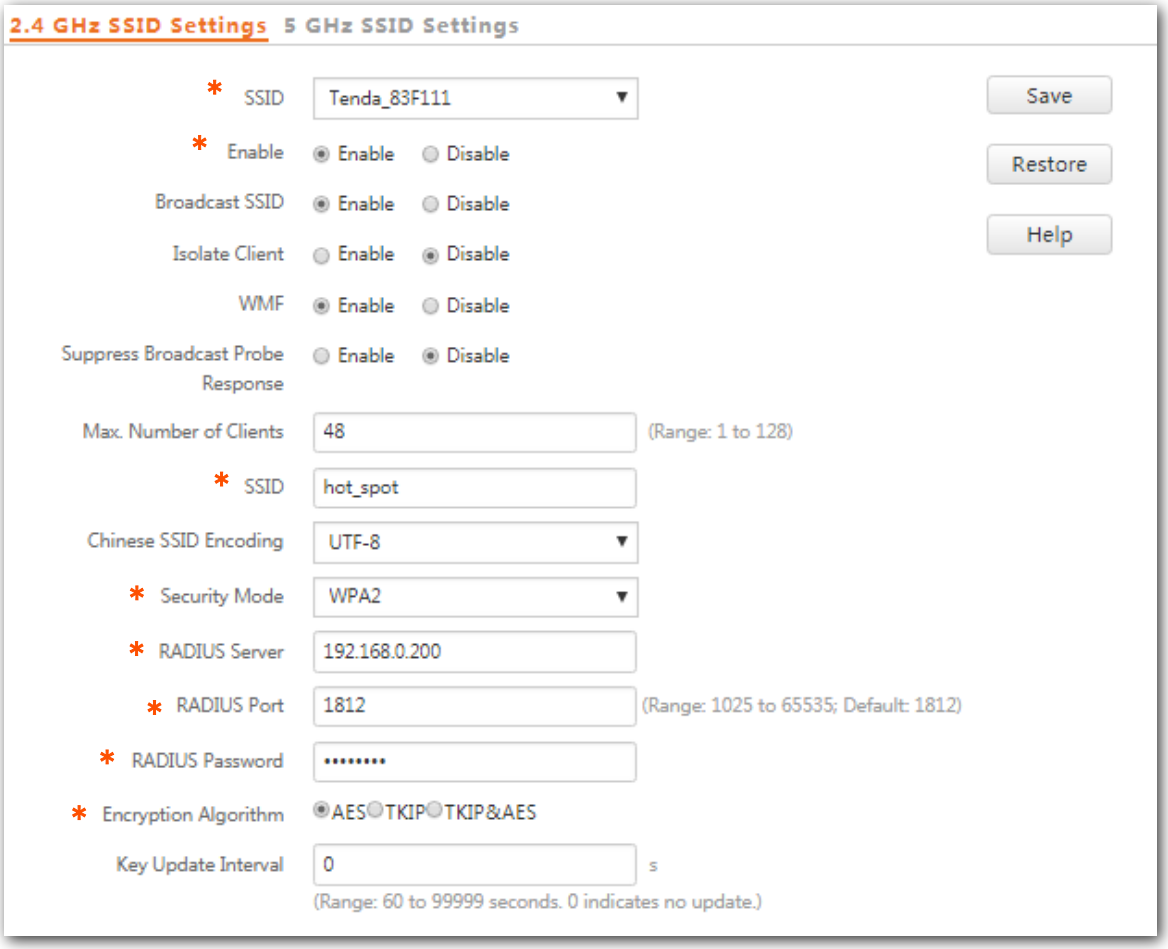
Step 4 Change the value of the **SSID** text box to **hot_spot**.

Step 5 Set **Security Mode** to **WPA2**.

Step 6 Set **RADIUS Server IP**, **RADIUS Port**, and **RADIUS Password** to **192.168.0.200, 1812**, and **12345678** respectively.

Step 7 Set **Encryption Algorithm** to **AES**.

Step 8 Click **Save**.



---End

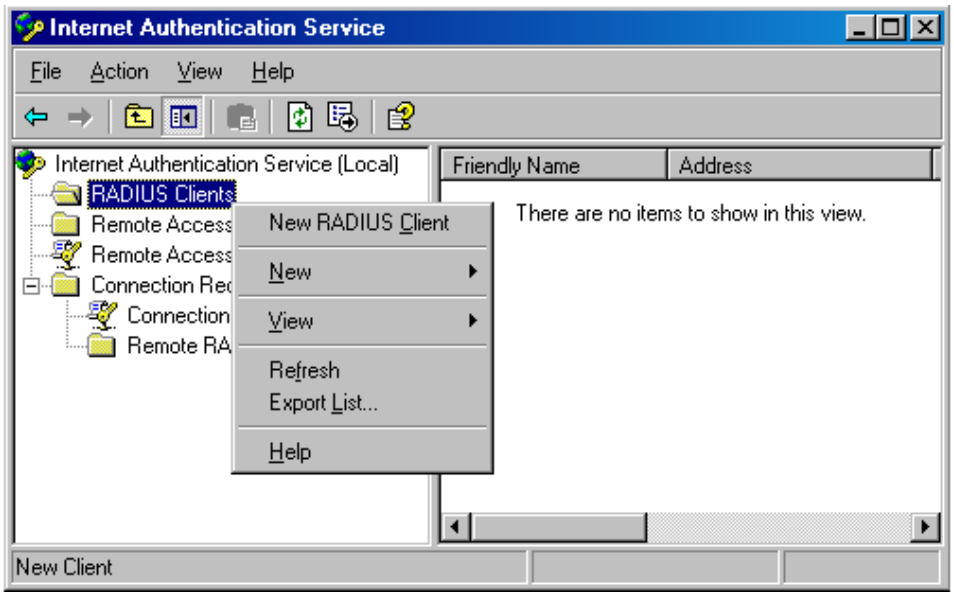
Configure the RADIUS server

NOTE

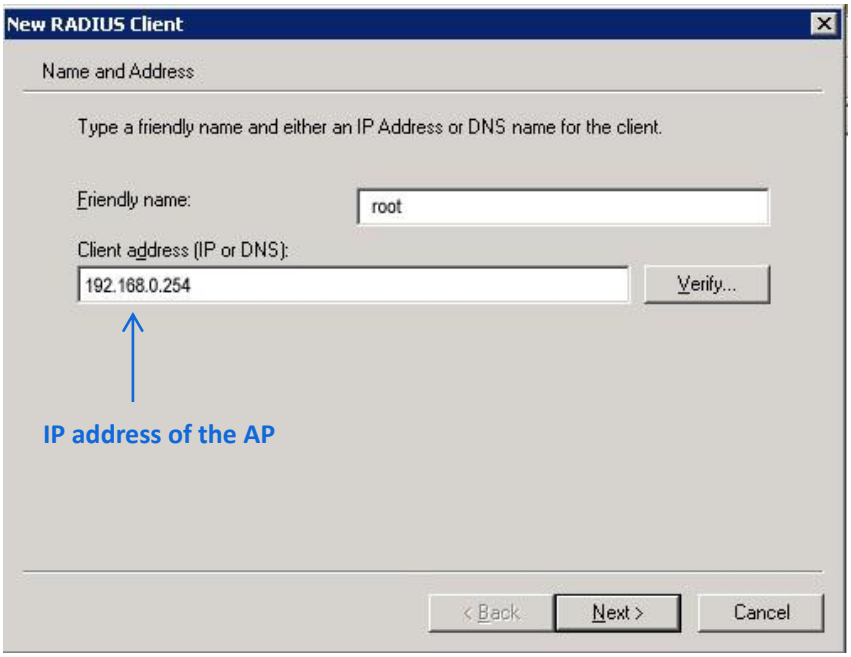
Windows 2003 is used as an example to describe how to configure the RADIUS server.

Step 1 Configure a RADIUS client.

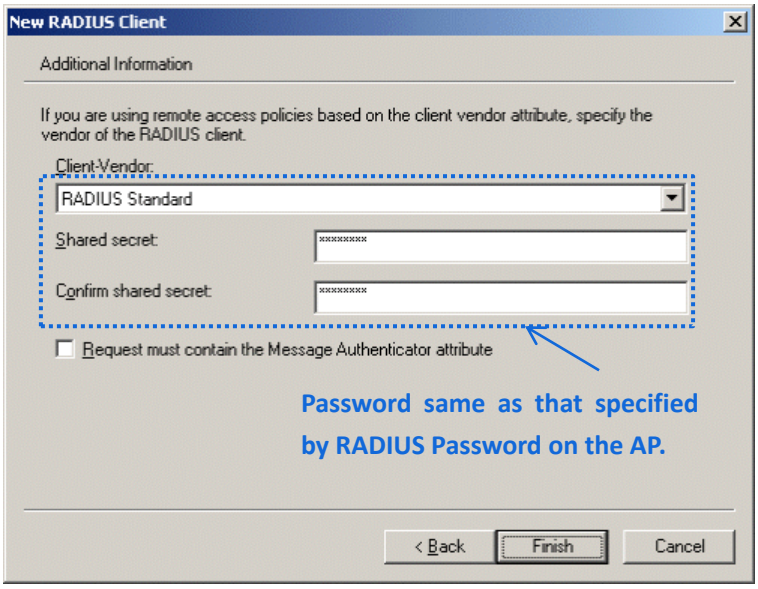
1. In the **Computer Management** dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.



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

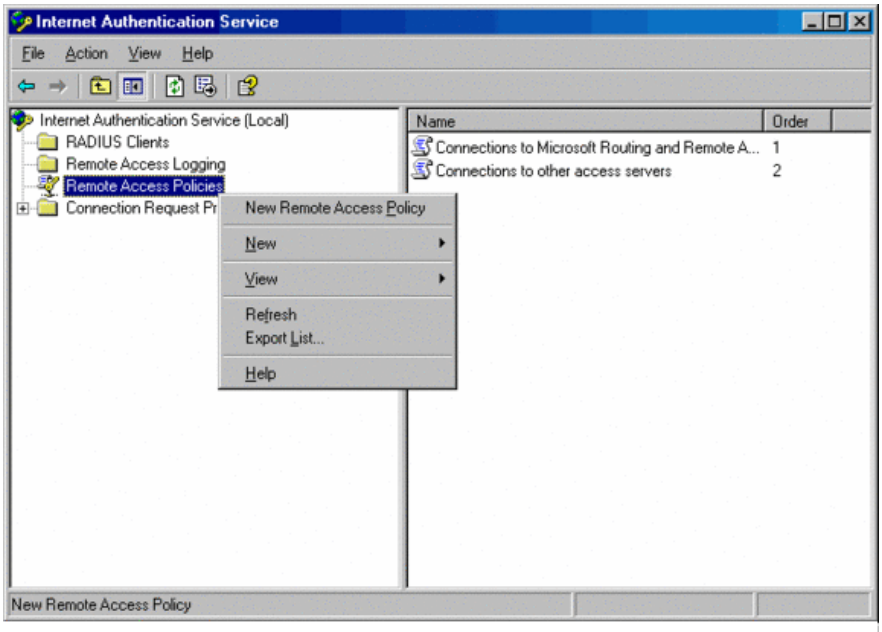


3. Enter **12345678** in the **Shared secret** and **Confirm shared secret** text boxes, and click **Finish**.

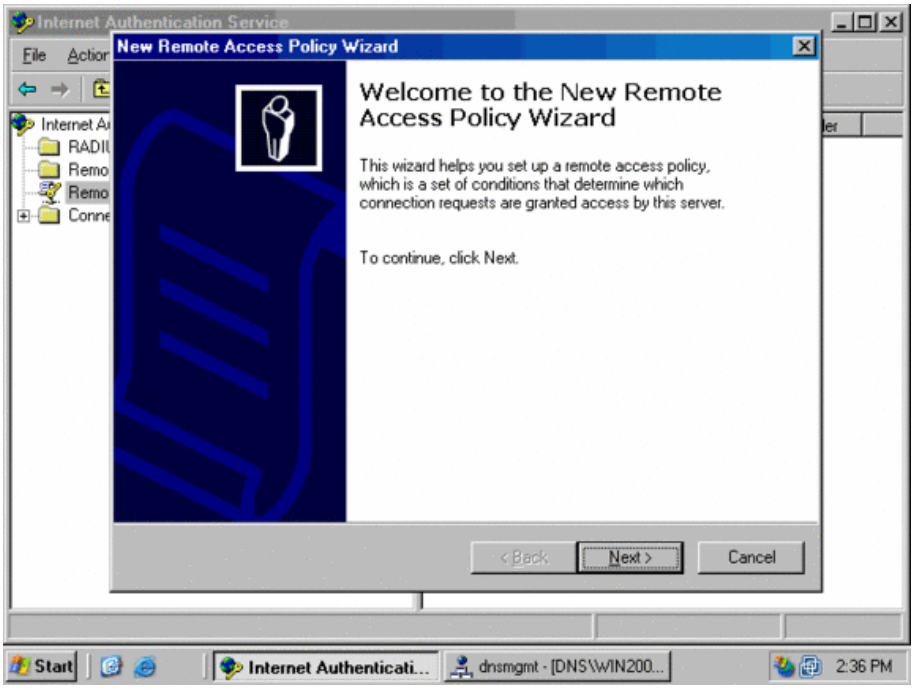


Step 2 Configure a remote access policy.

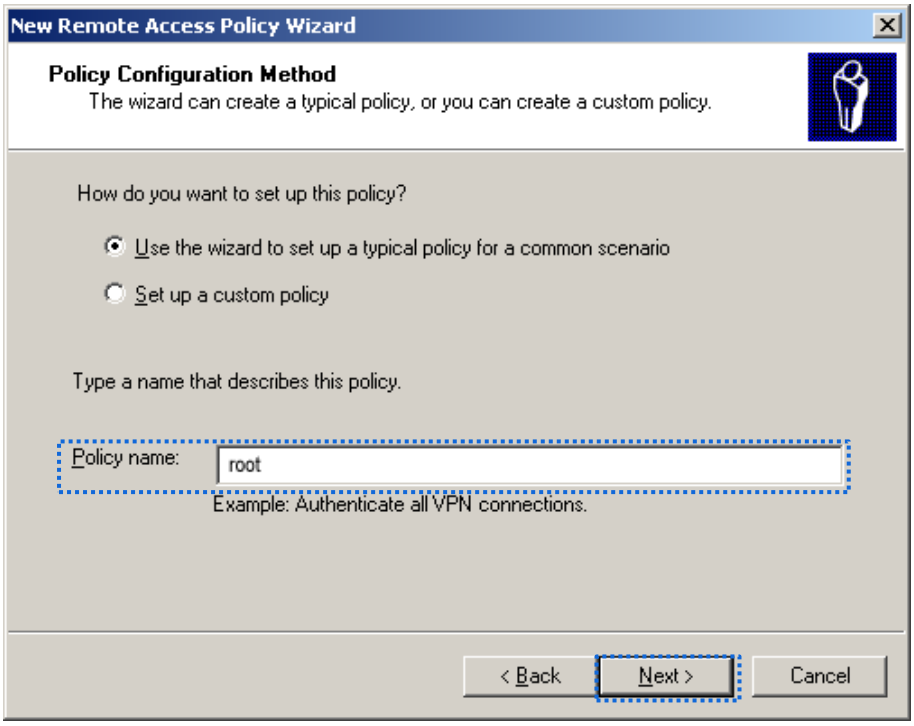
1. Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



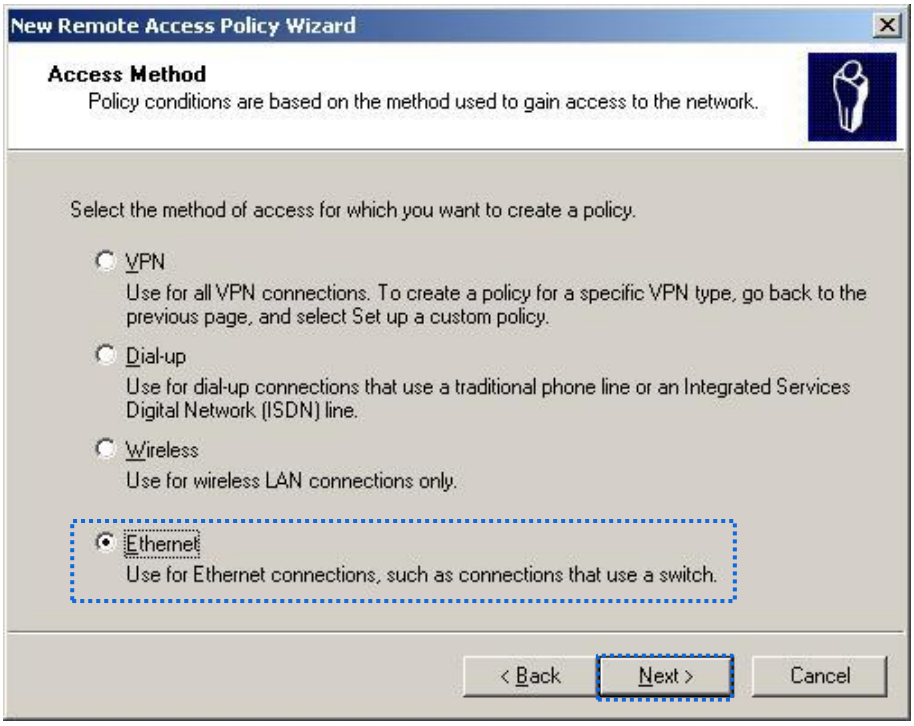
2. In the **New Remote Access Policy Wizard** dialog box that appears, click **Next**.



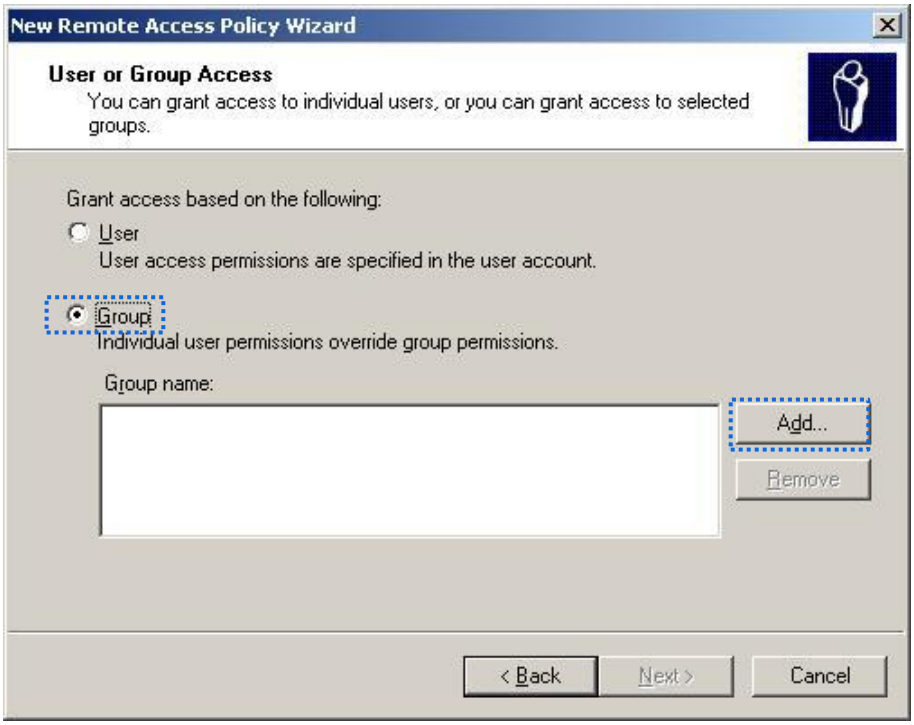
3. Enter a policy name and click **Next**.



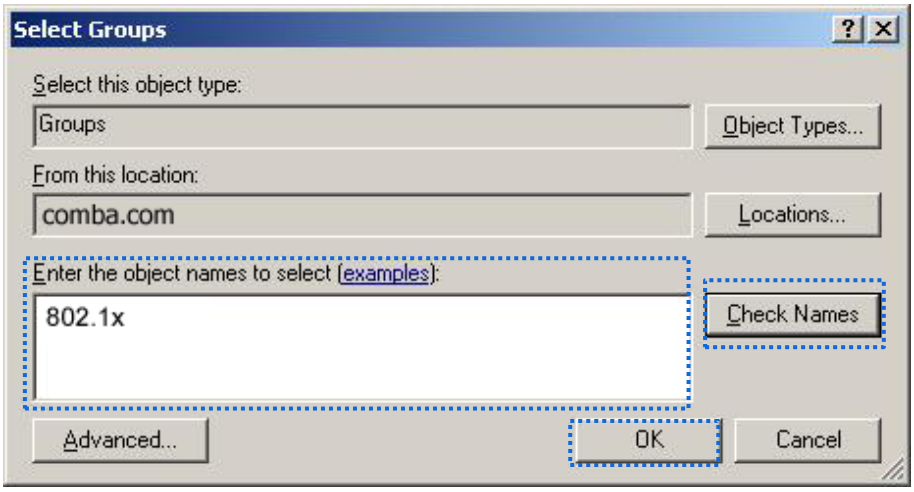
4. Select **Ethernet** and click **Next**.



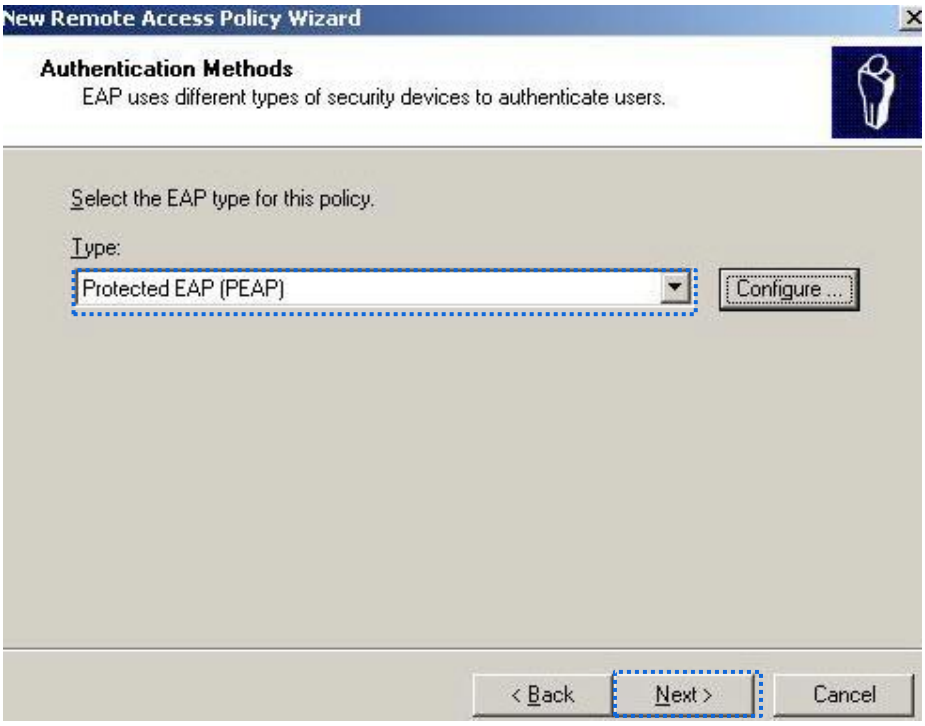
5. Select **Group** and click **Add**.



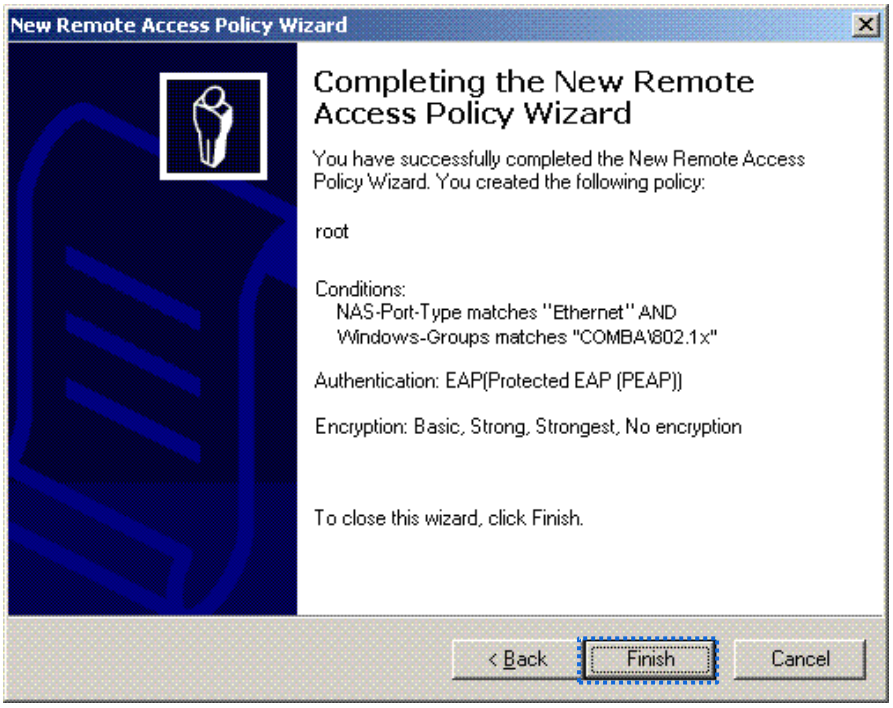
6. Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



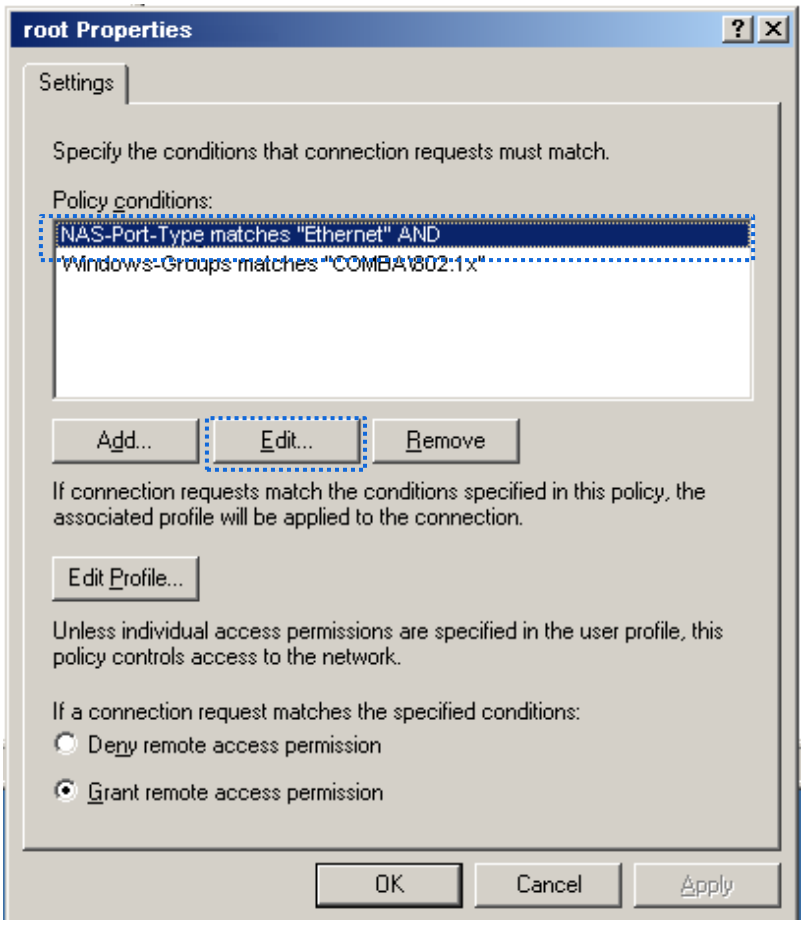
7. Select **Protected EAP (PEAP)** and click **Next**.



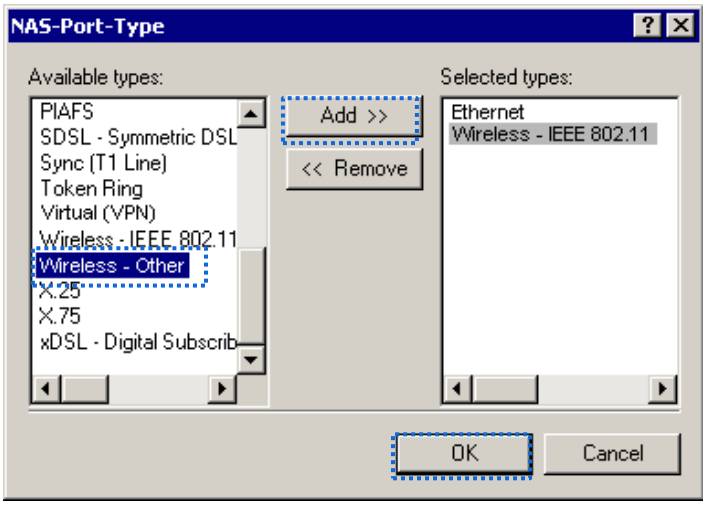
8. Click **Finish**. The remote access policy is created.



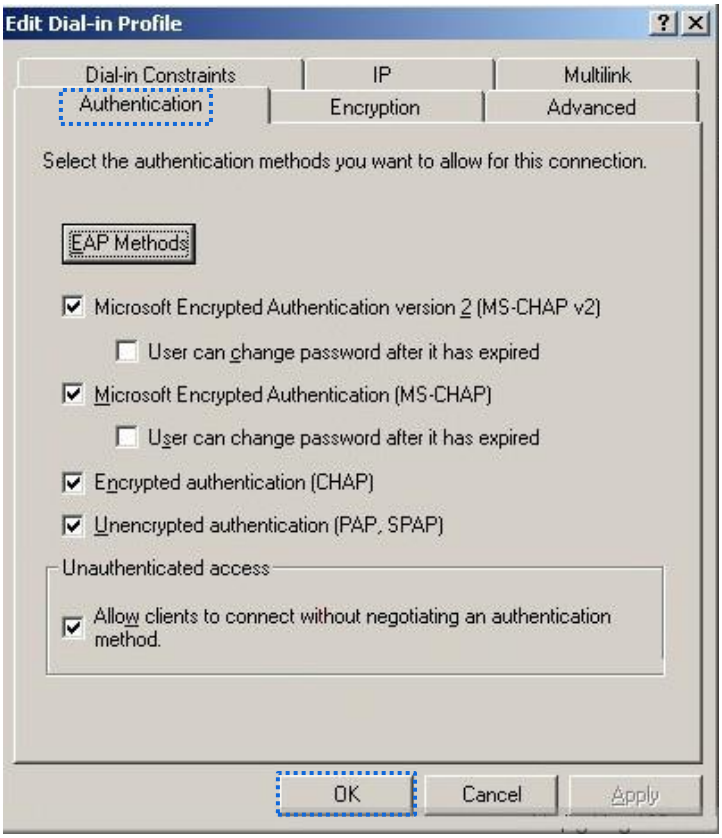
9. Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



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**.



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

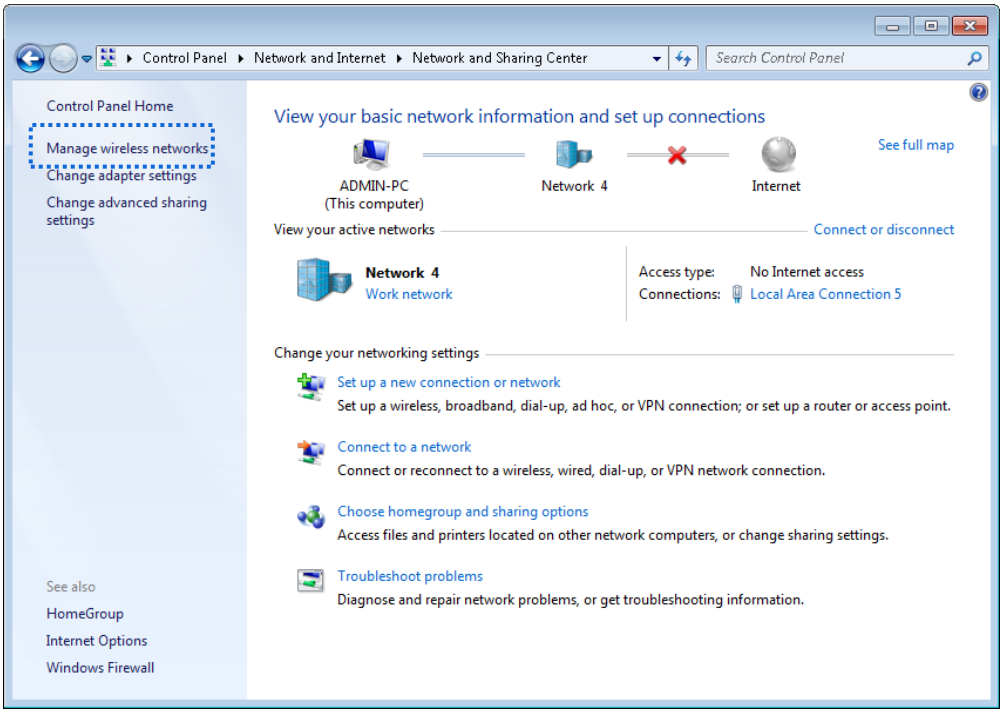
Step 3 Configure user information.
Create a user and add the user to group **802.1x**.

---End

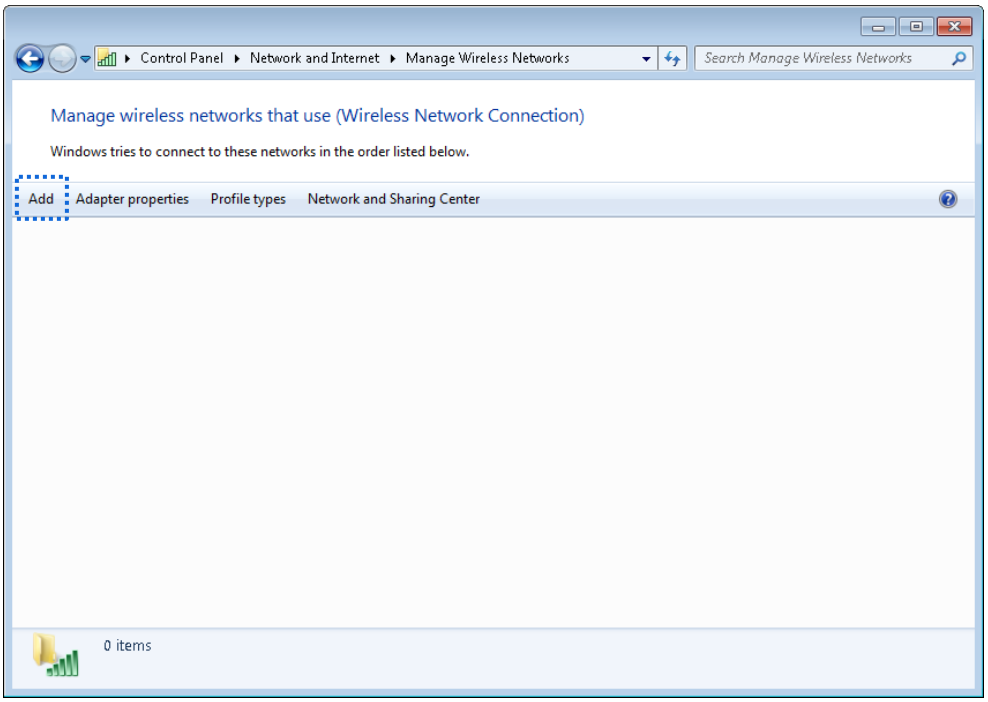
TIP

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

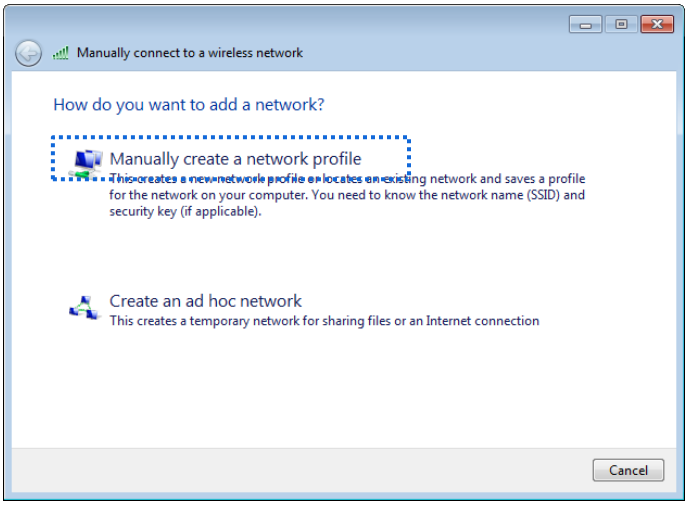
Step 1 Choose **Start** > **Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



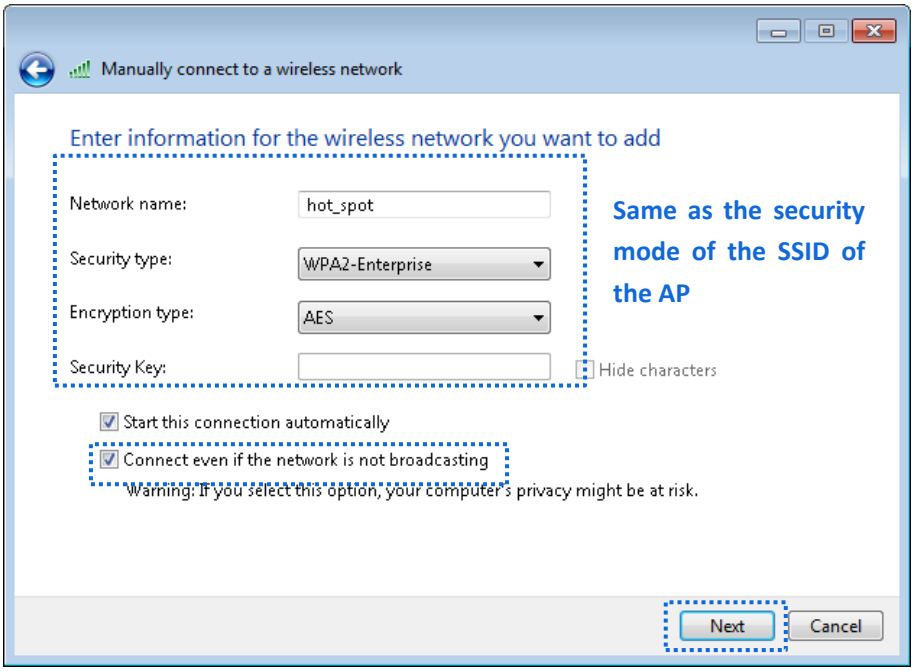
Step 2 Click **Add**.



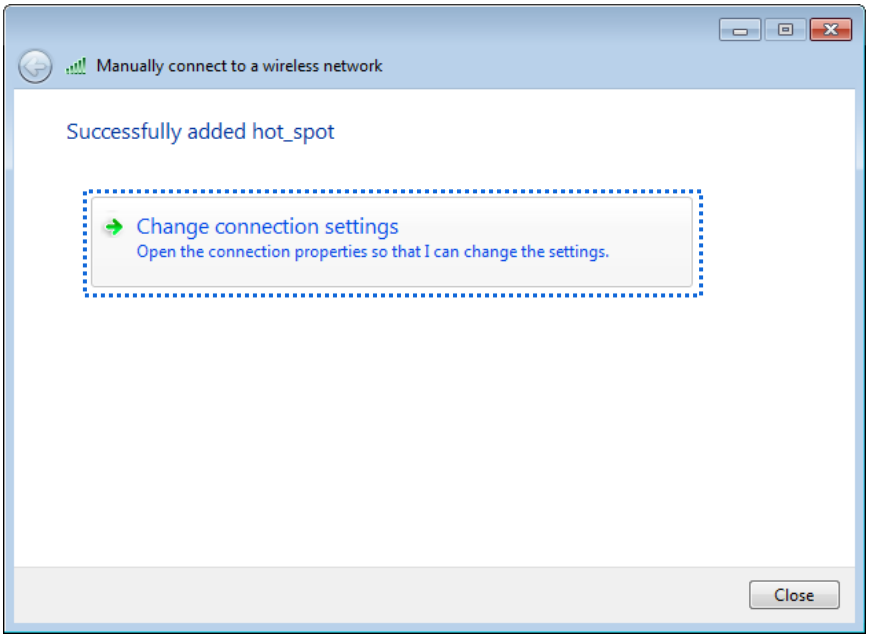
Step 3 Click **Manually create a network profile**.



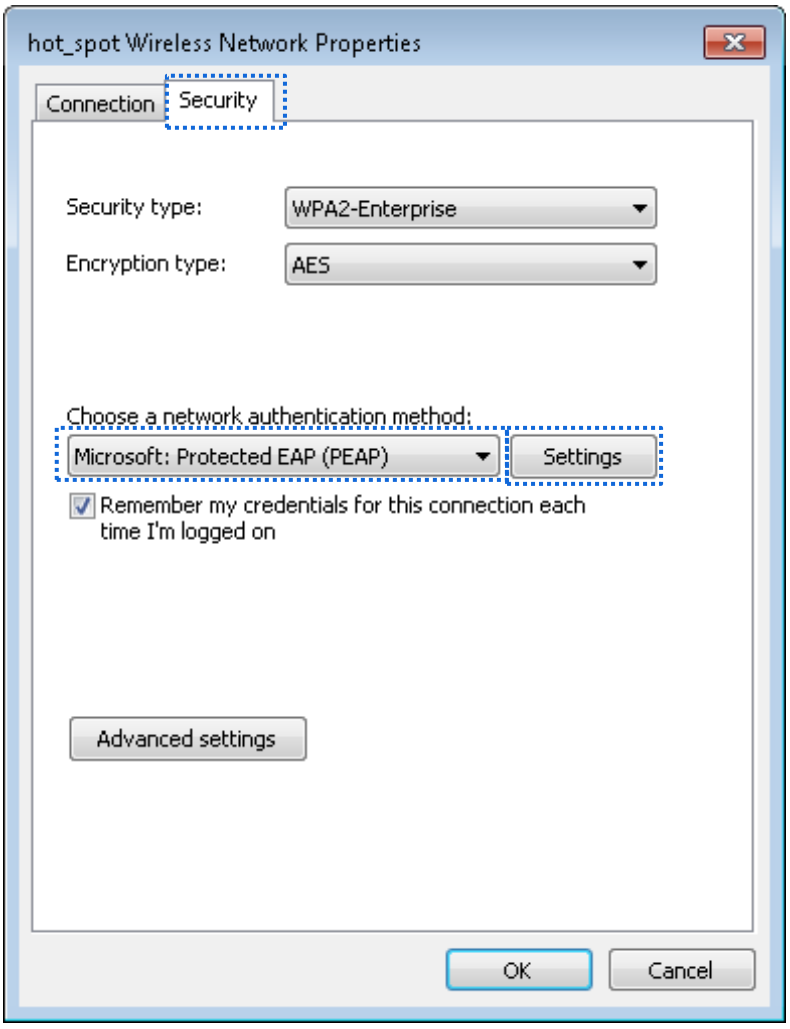
Step 4 Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.



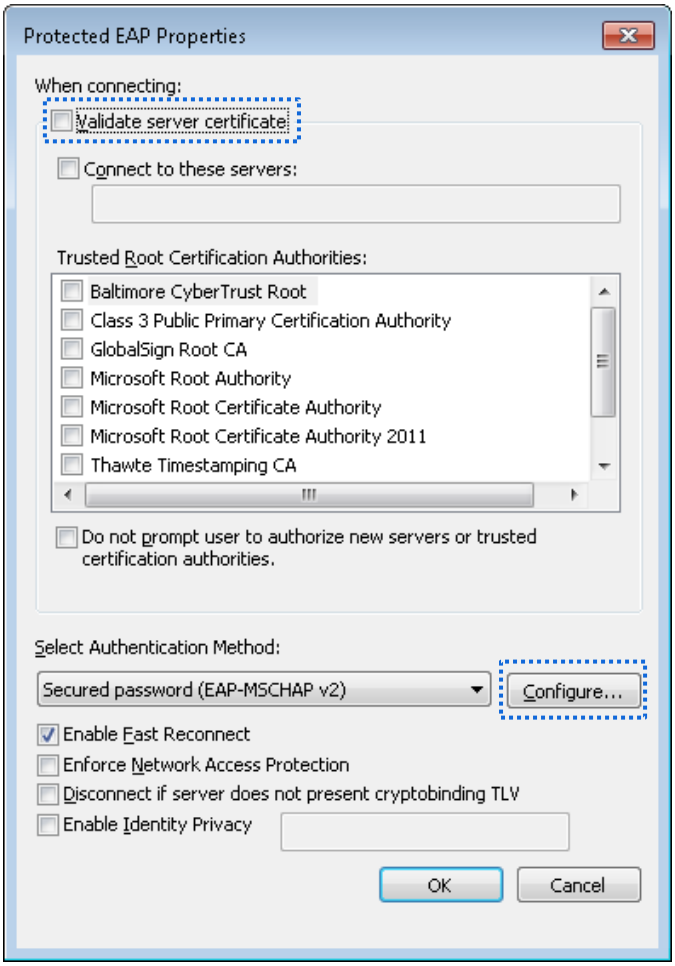
Step 5 Click **Change connection settings**.



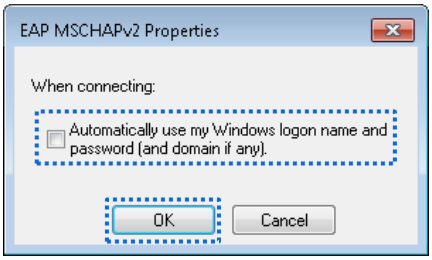
Step 6 Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



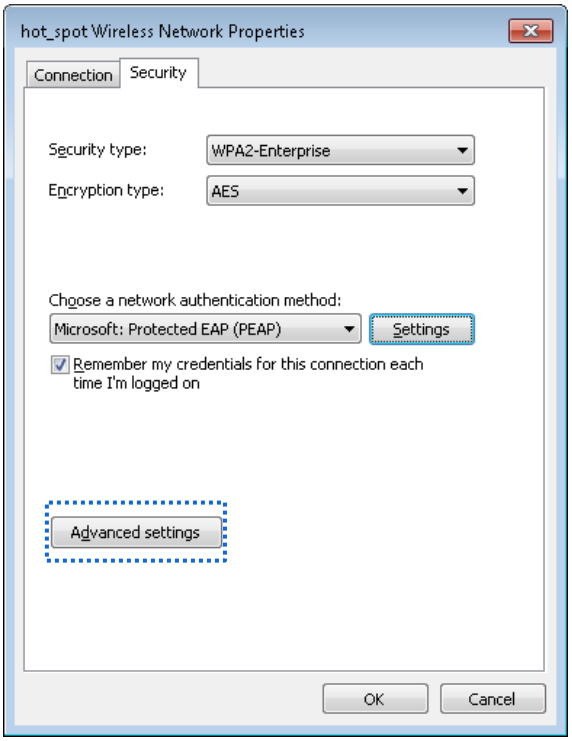
Step 7 Deselect **Validate server certificate** and click **Configure**.



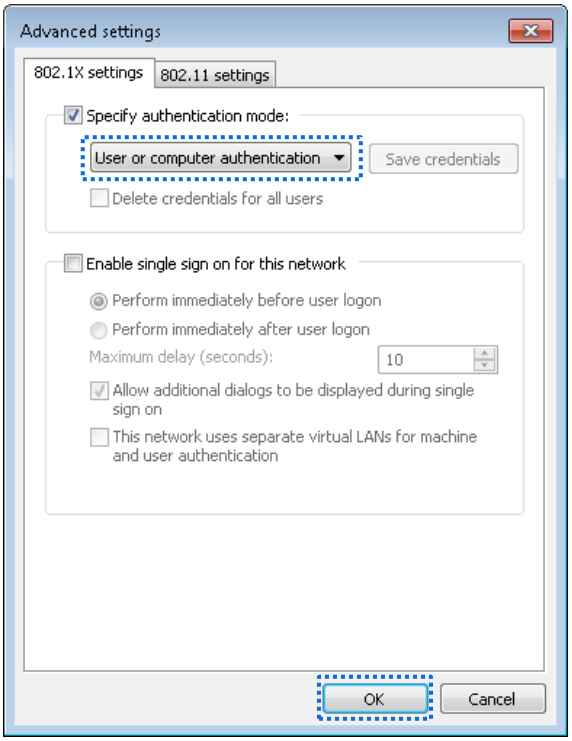
Step 8 Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



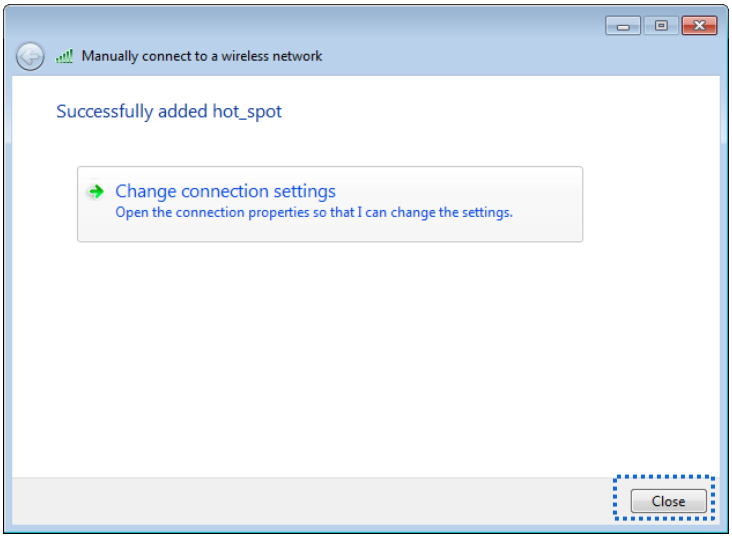
Step 9 Click **Advanced settings**.

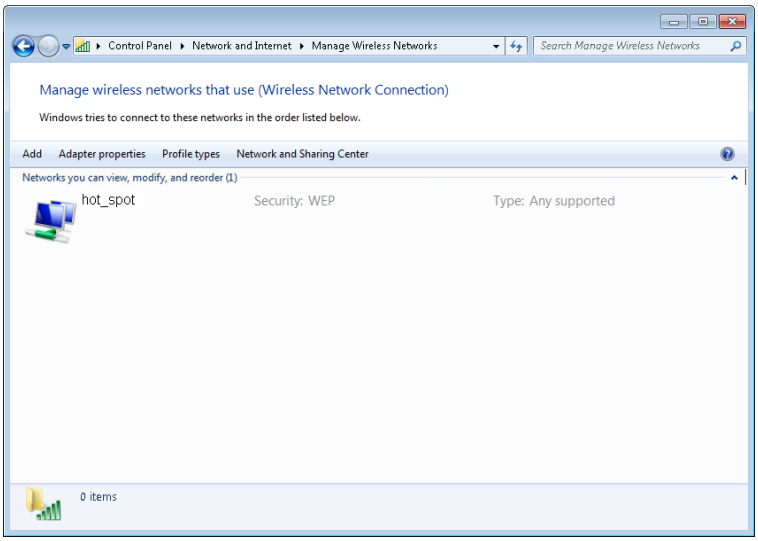


Step 10 Select **User or computer authentication** and click **OK**.

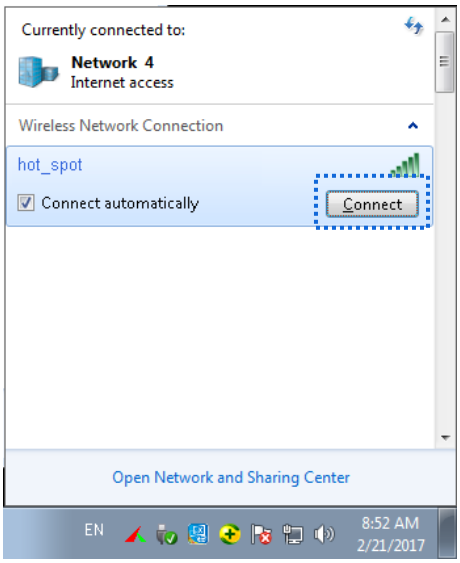


Step 11 Click **Close**.

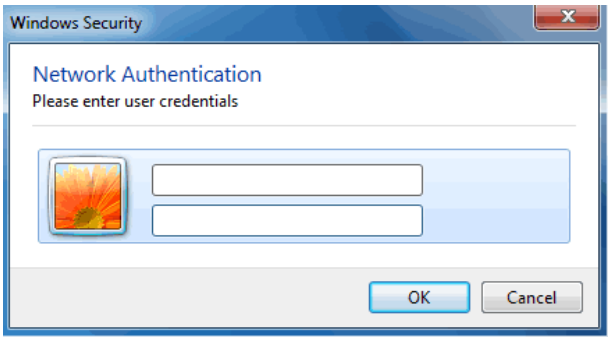




Step 12 Click the network icon in the lower-right corner of the desktop and choose the wireless network of the AP, such as **hot_spot** in this example.



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



---End

Verification

Wireless devices can connect to the wireless network named **hot_spot**.

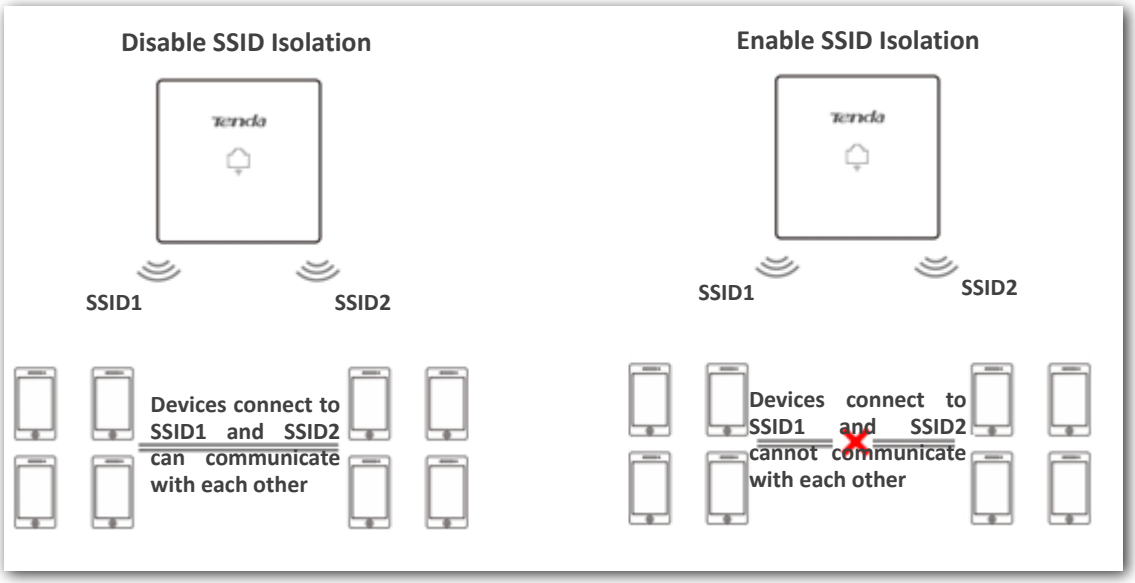
7.2 Radio Settings

7.2.1 Overview

This module is used to set Radio parameters of the AP. The following briefly describes the SSID isolation function.

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.



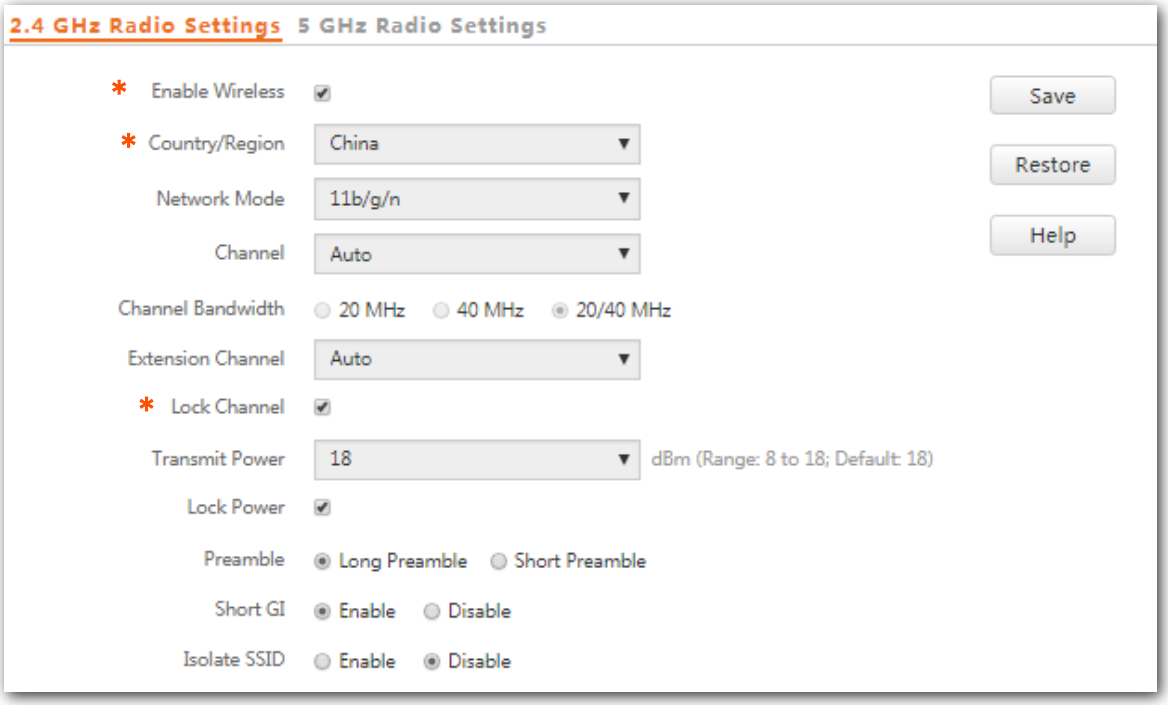
7.2.2 Modifying Radio Settings

Step 1 Choose **Wireless Setting** > **Radio Settings**.

Step 2 Choose the radio band to be configured, which is **2.4 GHz Radio Band Settings** in this example.

Step 3 Change the parameters as required. To change the **Country/Region** parameter, please unselect the **Channel Lockout** at first.

Step 4 Click **Save**.



---End

Parameter description

Parameter	Description
Enable Wireless	It specifies whether to enable the wireless function of the AP.
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. Available options include 11b/g/n mixed, 11b, 11g, 11b/g/n mixed. This parameter can be set if **Channel Lockout** is not selected. • **11b**: The AP works in 802.11b mode and only wireless devices compliant with 802.11b can connect to the 2.4 GHz 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 2.4 GHz 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 2.4 GHz 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 2.4 GHz wireless networks of the AP. • **11a**: The AP works in 802.11a mode and only wireless devices compliant with 802.11a can connect to the 5 GHz wireless networks of the AP. • **11ac:** The AP works in 802.11ac mode and only wireless devices compliant with 802.11ac can connect to the 5 GHz wireless networks of the AP. • **11a/n**: The AP works in 802.11a/n mode and only wireless devices compliant with 802.11a or 802.11n can connect to the 5 GHz wireless networks of the AP.

Parameter	Description
Channel	It specifies the operating channel of the AP. This parameter can be set if **Channel Lockout** 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, 802.11ac, 802.11a/n mode and **Channel Lockout** is not selected. • **20 MHz**: It indicates that the AP can use only 20 MHz channel bandwidth. • **40 MHz**: It indicates that the AP uses 40 MHz channel bandwidth first, and changes to 20 MHz channel bandwidth if severe channel competition occurs in the ambient environment. • **20/40 MHz**: It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment.
Extension 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 **40** or **20/40** and **Channel Lockout** 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.
Transmit Power	It specifies the transmit power of the AP. 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	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.
Short GI	Short Guard Interval. There is a delay on the receiving side due to multipath and other factors during the wireless signal transmission in space. If the subsequent data block is transmitted too quickly, it will interfere with the previous data block, and the short guard interval can be used to circumvent this interference. Short GI helps to increase the wireless throughput by 10%.
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.

7.3 Radio Optimization

7.3.1 Overview

Application Scenarios

Generally, wireless networks are widely applied to the following two scenarios:

- Ordinary scenario

For areas that demand wide WiFi coverage, such as offices, public buildings, schools, warehouses and hospitals.

- High density scenario

For large crowded areas, such as:

  - Conference halls, theaters, exhibition and banquet halls
  - Indoor and open stadiums
  - Classrooms at colleges and universities
  - Airports and railway stations

Radio Optimization Parameters

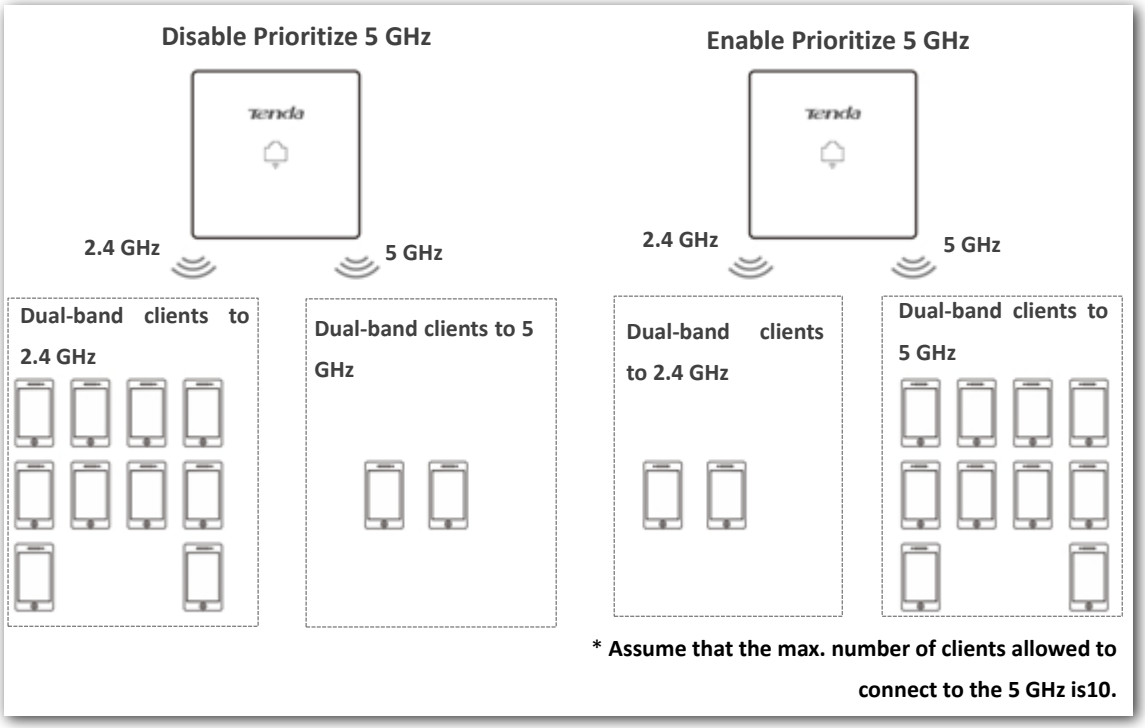
To address the demands of both coverage-oriented and high-density scenarios, the AP provides a series of parameters for radio optimization, facilitating our customers to create qualified wireless network service.

- Prioritize 5 GHz

Although the 2.4 GHz band is more widely used than the 5 GHz band in actual wireless networks application, channels and signals on 2.4 GHz suffer more serious congestion and interference since there are only 3 non-overlapped communication channels on this band. The 5 GHz band could provide more non-overlapped communication channels. The quantity could reach more than 20 in some countries.

With the evolvement of the wireless networks, wireless clients that support both the 2.4 GHz and 5 GHz are more popular. However, by default, such dual-band wireless clients choose the 2.4 GHz to connect, resulting in even worse congestion of the 2.4 GHz band and the waste of the 5 GHz band.

The prioritize 5 GHz functions enables such dual-band wireless clients to connect the 5 GHz band on network initialization if the 5 GHz signal strength the AP received reaches or exceeds the 5 GHz threshold so as to improve the utilization of the 5 GHz band, reduce the load and interference on the 2.4 GHz band, thus bettering user experience.



NOTE

The prioritize 5 GHz function takes effect only on the condition that the wireless both of the 2.4 GHz and 5 GHz are enabled, and the two bands share the same SSID, security mode and password.

- Air Interface Scheduling

In mixed wireless rates environment, the traditional FIFO (First-in First-out) allocates more air interface time to clients with low transmission capacity and low spectrum efficiency, reducing the system throughput of each AP then the system utilization.

The air interface scheduling function evenly allocates downlink transmission time to clients so that clients with high transmission rate could transmit more data, improving the throughput of each AP and quantity of clients allowed to be connected.

7.3.2 Optimizing Radio

NOTE

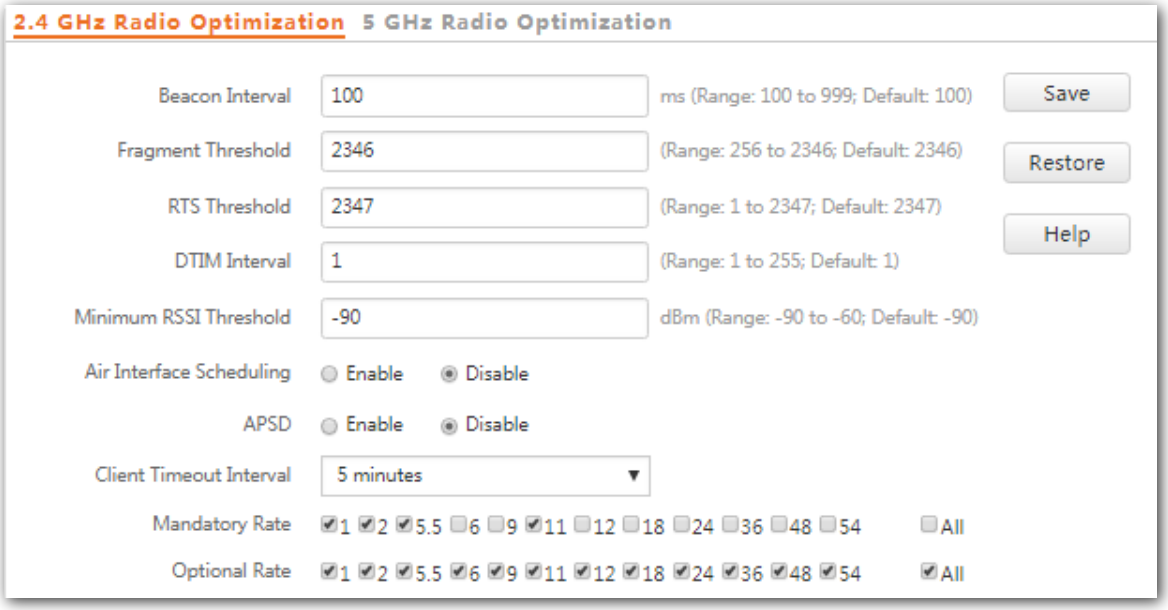
You are recommended to retain the default settings if without the professional guidance.

Step 1 Choose **Wireless Setting** > **Radio Optimization**.

Step 2 Click the tab to choose the radio band to be configured.

Step 3 Change parameters as needed.

Step 4 Click **Save**.



---End

Parameter description

Parameter	Description
Beacon Interval	Used to set the interval at which this device sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.
Fragment Threshold	Threshold of a fragment. 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 this device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput.
RTS Threshold	Frame length threshold for triggering the RTS/CTS mechanism. The unit is byte. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. 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 reduce conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	Countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval. For example, if DTIM Interval is set to 1, this device transmits all cached frames at one Beacon

Parameter	Description
	interval.
Minimum RSSI Threshold	Minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device. A proper value facilitates wireless devices to connect to the AP with stronger signal in case of multiple APs exist.
Prioritize 5 GHz	• **Enable**: Dual band wireless devices prefer the 5 GHz WiFi network of the AP to connect. • **Disable**: Dual band wireless devices connect to either 2.4 GHz or 5 GHz WiFi network of the AP at random.
5 GHz Threshold	With this function enabled, if the strength of the signals transmitted by a wireless device is stronger than this threshold, the wireless device connects to the 5 GHz WiFi network. Otherwise, it connects to the 2.4 GHz WiFi network.
Air Interface Scheduling	Used to enable or disable the air interface scheduling function of the AP. This enables the users experiencing high download rates to download more data, so that this device can achieve higher system throughput and connect to a greater number of clients.
APSD	APSD: Automatic Power Save Delivery. If it is enabled, the power consumption of this device is reduced after a specified period during which no traffic is transmitted or received. By default, it is disabled.
Client Timeout Interval	Used to set the wireless client disconnection interval of this device. The device disconnects from a wireless client if no traffic is transmitted or received by the wireless client within the interval.
Mandatory Rate	It specifies rates that wireless clients must support in order to connect to the wireless networks of this device.
Optional Rate	It specifies the additional rates that the AP supports, which are optional to wireless clients.

7.4 WMM Settings

7.4.1 Overview

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.

WMM involves the following terms:

- Enhanced Distributed Channel Access (EDCA): It is a channel competition mechanism to ensure that packets with higher priorities are assigned more bandwidth and transmitted earlier.

- Access Category (AC): The WMM mechanism divides WLAN traffic by priority in descending order into the AC-VO (voice stream), AC-VI (video stream), AC-BE (best effort), and AC-BK (background) access categories. The access categories use queues with different priorities to send packets. The WMM mechanism ensures that packets in queues with higher priorities have more opportunities to access channels.

According to the 802.11 protocol family, all devices listen on a channel before using the channel to send data. If the channel stays idle for or longer than a specified period, the devices wait a random backoff period within the contention window. The device whose backoff period expires first can use the channel. The 802.11 protocol family applies the same backoff period and contention window to all devices across a network to ensure that the devices have the same channel contention opportunity.

- EDCA Parameters

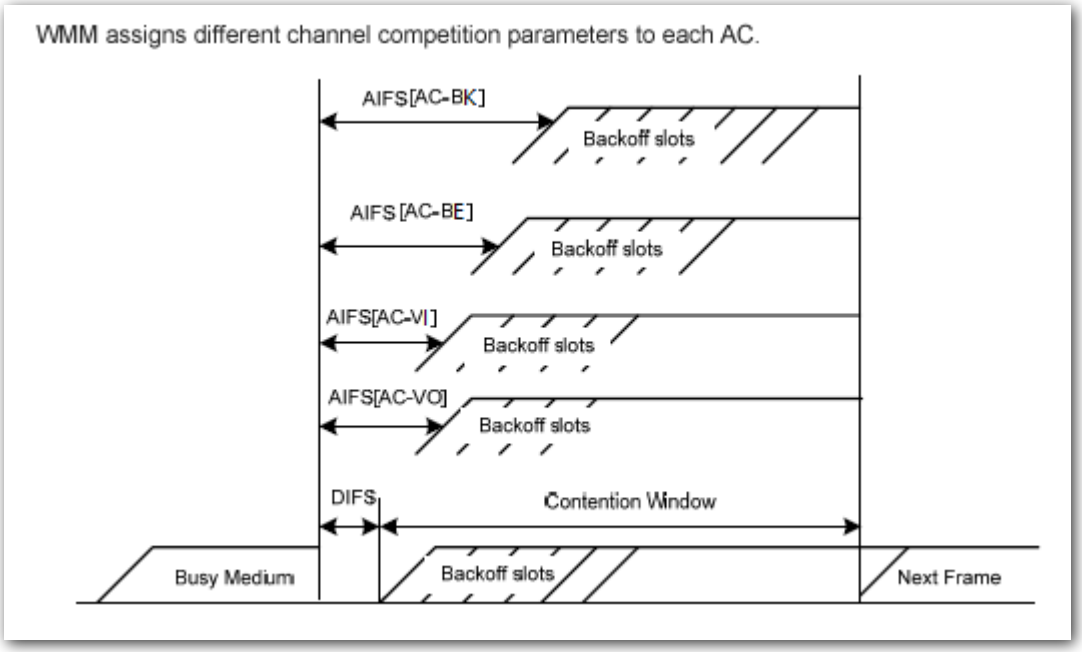
WMM changes the contention mechanism of 802.11 networks by dividing packets into four ACs, among which the ACs with higher priorities have more opportunities to access channels. The ACs help achieve different service levels.

WMM assigns each AC a set of EDCA parameters for channel contention, including:

- Arbitration Inter Frame Spacing Number (AIFSN): Different from the fixed distributed inter-frame spacing (DIFS) specified in the 802.11 protocol family, AIFSN varies across ACs. A greater AIFSN indicates a longer backoff period. See AIFS in the following figure.

- Contention window minimum (CWmin) and contention window maximum (CWmax) specify the average backoff period. The period increases along with these two values. See the backoff slots in the following figure.

- Transmission Opportunity (TXOP): It specifies the maximum channel use duration after successful channel contention. The duration increases along with this value. The value **0** indicates that a device can send only one packet through a channel after winning contention for the channel.



- ACK Policies

WMM specifies the Normal ACK and No ACK policies.

- According to the No ACK policy, no ACK packet is used during wireless packet transmission to acknowledge packet reception. This policy is applicable to scenarios where interference is mild and can effectively improve transmission efficiency. In case of strong interference, lost packets will not be resent if this policy is adopted. This leads to a higher packet loss rate and reduces the overall performance.

- According to the Normal ACK policy, each time a receiver receives a packet, it sends back an ACK packet to acknowledge packet reception.

7.4.2 Modidying WMM Settings

By default, the WMM function of the AP is enabled and the **Optimized For Capacity** mode is adopted. Procedure for changing the WMM settings:

Step 1 Choose **Wireless Setting** > **WMM Settings**.

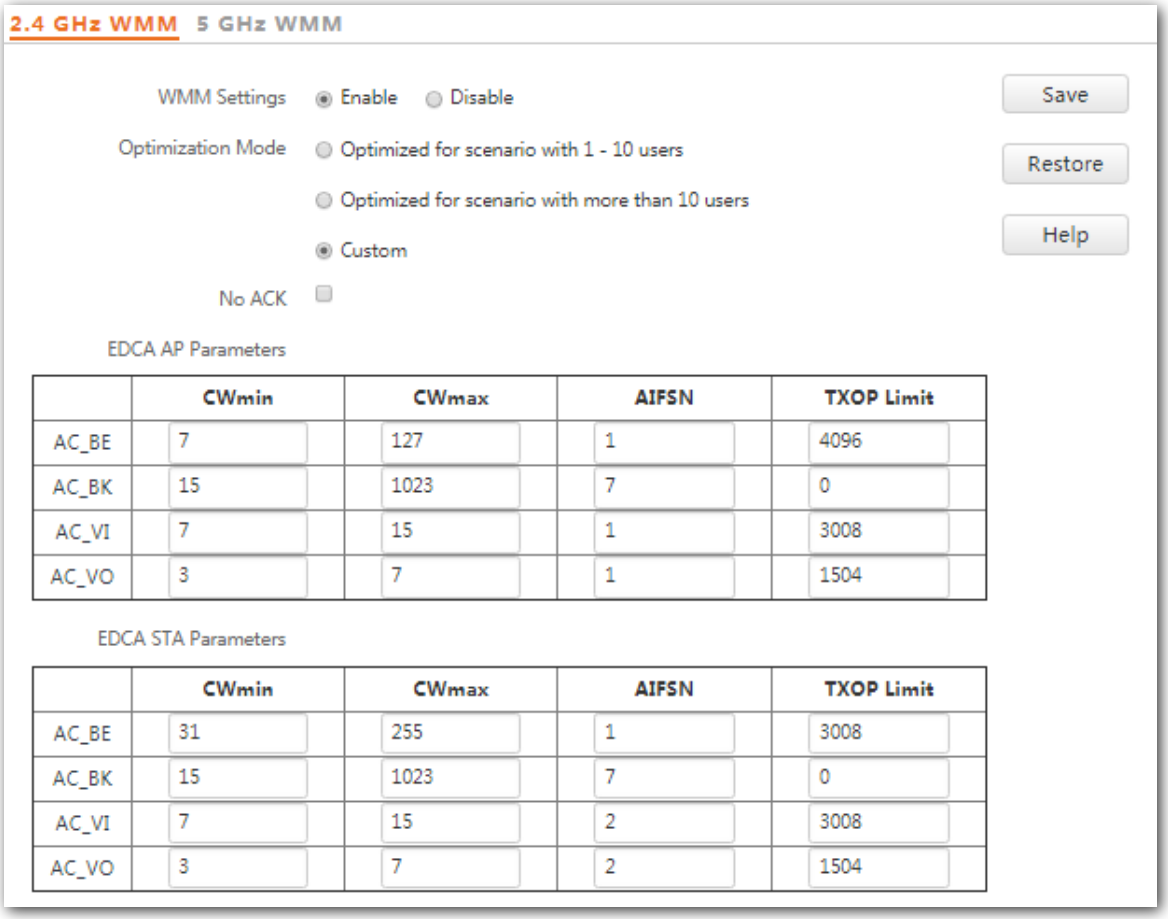
Step 2 Click the tab to choose the radio band to set.

Step 3 Set **WMM** to **Enable**.

Step 4 Select the required WMM optimization mode.

Step 5 If you select **Custom**, set the WMM parameters as required.

Step 6 Click **Save**.



---End

Parameter description

Parameter	Description
WMM Settings	• **Enable**: It is used to enable the WMM function. • **Disable**: It is used to disable the WMM function.
WMM Optimization Mode	It specifies the WMM optimization modes supported by the AP: • **Optimized For scenario with 1 - 10 users**: If 10 or less clients are connected to the AP, you are recommended to select this mode to obtain higher client throughput. • **Optimized For scenario with more than 10 users**: If more than 10 clients are connected to the AP, you are recommended to select this mode to ensure client connectivity. • **Custom**: This mode enables you to set the WMM EDCA parameters for manual optimization.
No ACK	If the check box is selected, the No ACK policy is adopted. If the check box is deselected, the Normal ACK policy is adopted.
EDCA Parameters	For details, refer to section 7.4.1 Overview.

7.5 Access Control

7.5.1 Overview

The access control function enables you to allow or disallow the wireless devices to access the wireless network of the AP based on their MAC addresses.

The AP supports the following 3 filter modes:

- **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 Setting** > **Access Control**.

Step 2 Select a wireless network radio band on which access control must be implemented.

Step 3 From the **SSID** drop-down list box, select an SSID of the wireless network to which the rule applies.

Step 4 Select a filter mode from the **MAC Address Filter Mode** drop-down list.

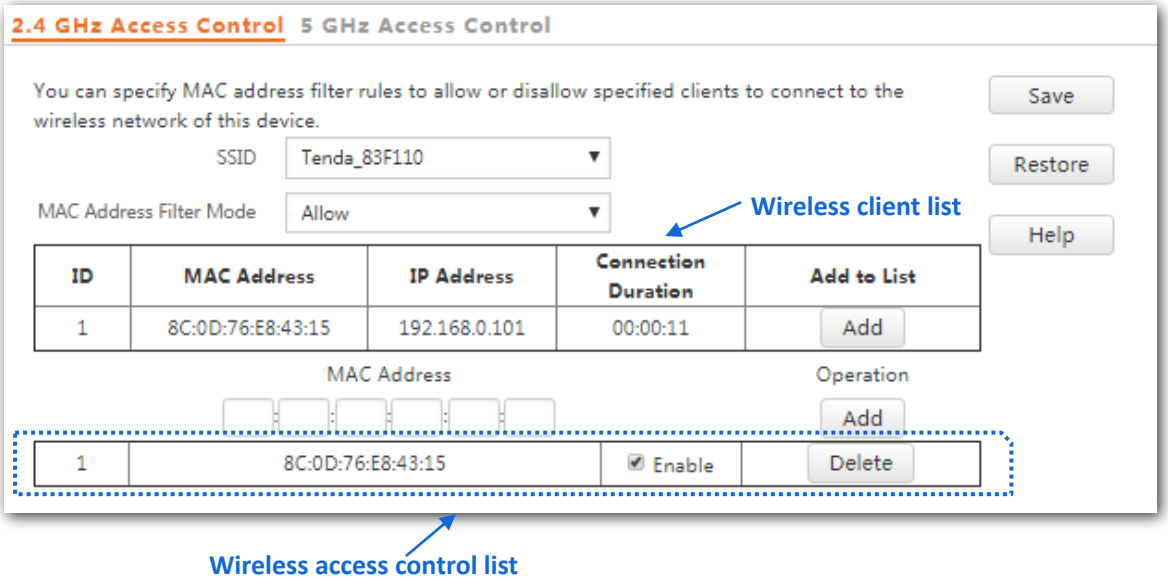
Step 5 Enter the MAC addresses of the wireless devices to which the rule applies.

Step 6 Click **Add**.

TIP

If you want to control the devices in the wireless client list, directly click the Add button corresponding to the device.

Step 7 Click **Save**.



Parameter description

Parameter	Description
SSID	It specifies the wireless network to which the rule applies.
MAC Filter Mode	It specifies the filter mode of the rule. • **Disable**: It indicates that the access control function 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 Access Control function of the AP is recommended. 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 Setting** > **Access Control** > **5 GHz Access Control**.

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

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

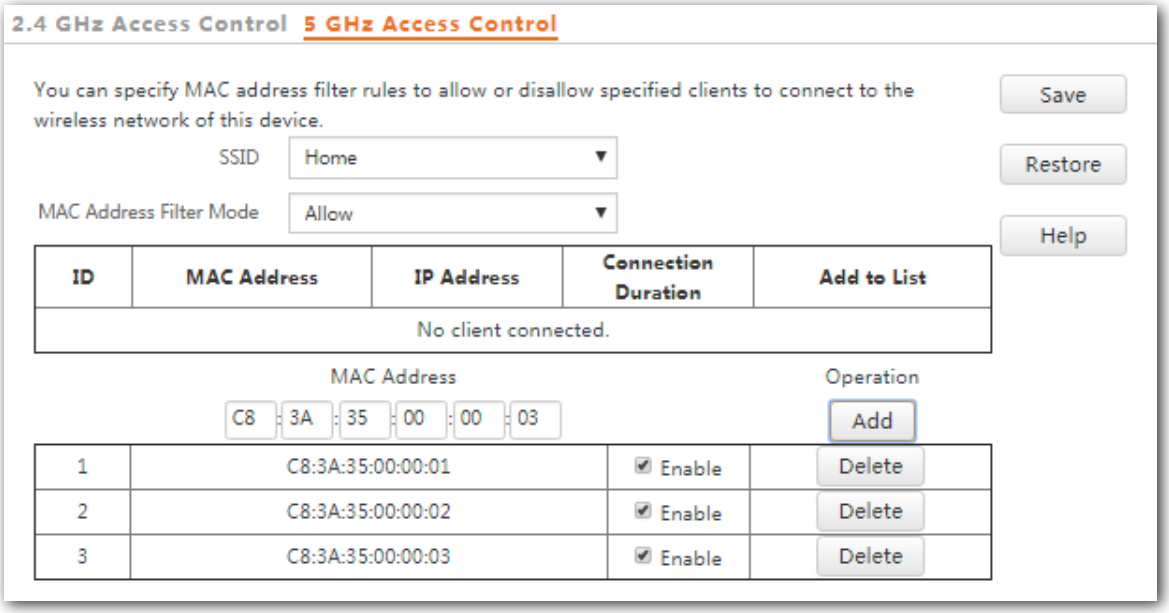
Step 4 Enter **C8:3A:35:00:00:01** in the **MAC Address** text box and click **Add**.

Step 5 Repeat step 4 to add **C8:3A:35:00:00:02** and **C8:3A:35:00:00:03** as well.

Step 6 Click **Save**.

---End

The following figure shows the configuration.



Verification

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

7.6 Advanced Settings

7.6.1 Overview

This module is used to set the Identify Client Type and Broadcast Packet Filter of the AP.

- Identify Client Type

It specifies whether to identify operating system types of wireless clients connected to this device. Terminal types that the AP can identify include: Android, iOS, WPhone, Windows, Mac OS, and so on.

- Broadcast Packet Filter

By default, this device forwards lots of invalid broadcast packets from wired networks, which may affect business data transfer. The broadcast packet filter function allows you to filter broadcast packets by types so that invalid packets are not forwarded. This reduces air interface resources usage and ensures more bandwidth for business data transfer.

7.6.2 Changing the Advanced Settings

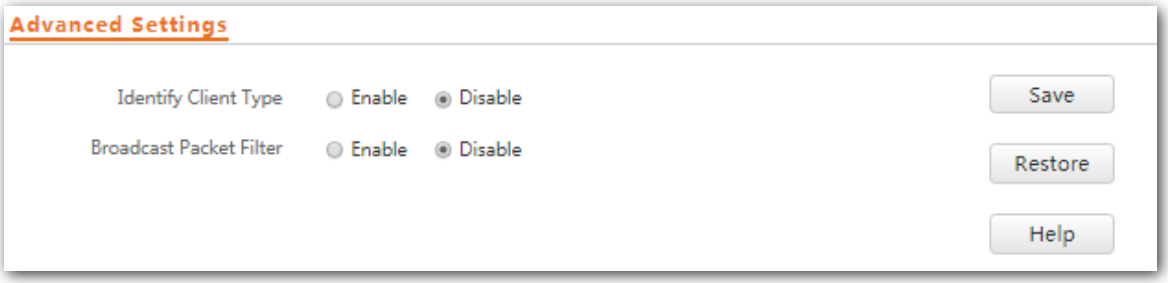
NOTE

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 Setting** > **Advanced Settings**.

Step 2 Change the parameter settings as required.

Step 3 Click **Save**.



---End

Parameter description

Parameter	Description
Identify Client Type	• **Enable**: It specifies whether to enable the function. The operating system type of wireless devices connected to the AP's WiFi network can be viewed by choosing **Status** > **Wireless Clients**. • **Disable**: It specifies whether to disable the function.
Broadcast Packet Filter	• **Enable**: It specifies whether to enable the function. With the function enabled, the AP can reduce air interface resources usage and ensure the bandwidth for business data transfer.

Parameter	Description
	• **Disable**: It specifies whether to disable the function.
Filter Mode	Select a mode after you enable the broadcast packet filter function. • **Accept only DHCP and ARP packets**: Filter out all broadcast or multicast data except DHCP and ARP packets. • **Accept only ARP packets**: Filter out all broadcast or multicast data except ARP packets.

7.7 QVLAN Settings

7.7.1 Overview

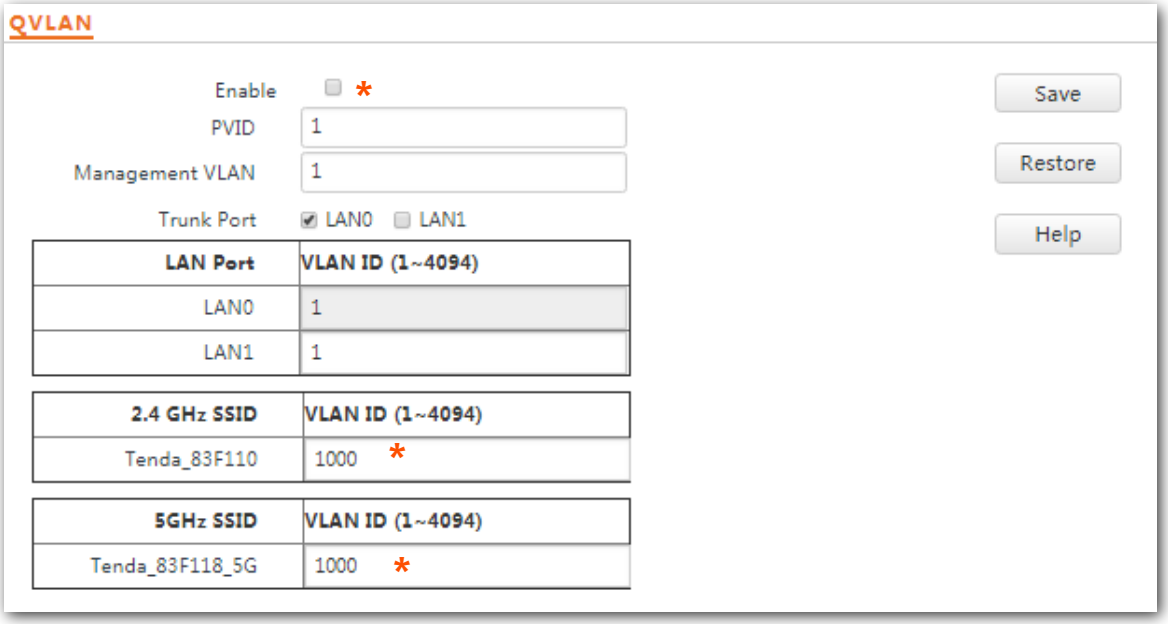
The AP supports 802.1Q VLANs and is applicable in a network environment where 802.1Q VLANs have been defined. By default, the QVLAN function is disabled.

7.7.2 Configuring the QVLAN Function

Step 1 Choose **Wireless Setting** > **QVLAN Settings**.

Step 2 Change the parameters as required. Generally, you only need to change the **Enable, LAN Port**, **2.4 GHz SSID VLAN ID** and **5 GHz SSID VLAN ID** settings.

Step 3 Click **Save**.



---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.

Parameter	Description
	NOTE If the QVLAN function is enabled, at least one LAN port needs to be set as a trunk port. LAN0 indicates the LAN port at the rear of the AP (PoE power supply, data transmission multiplexing port), whereas LAN1 indicates the LAN port (data transmission 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. The default value is 1.
2.4 GHz SSID	It specifies the currently enabled SSIDs of the AP at 2.4 GHz band.
5 GHz SSID	It specifies the currently enabled SSIDs of the AP at 5 GHz band.
VLAN ID	It specifies VLAN IDs corresponding to SSIDs. The default value is **1000**. 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.

7.7.3 Example of Configuring QVLAN Settings

Networking requirement

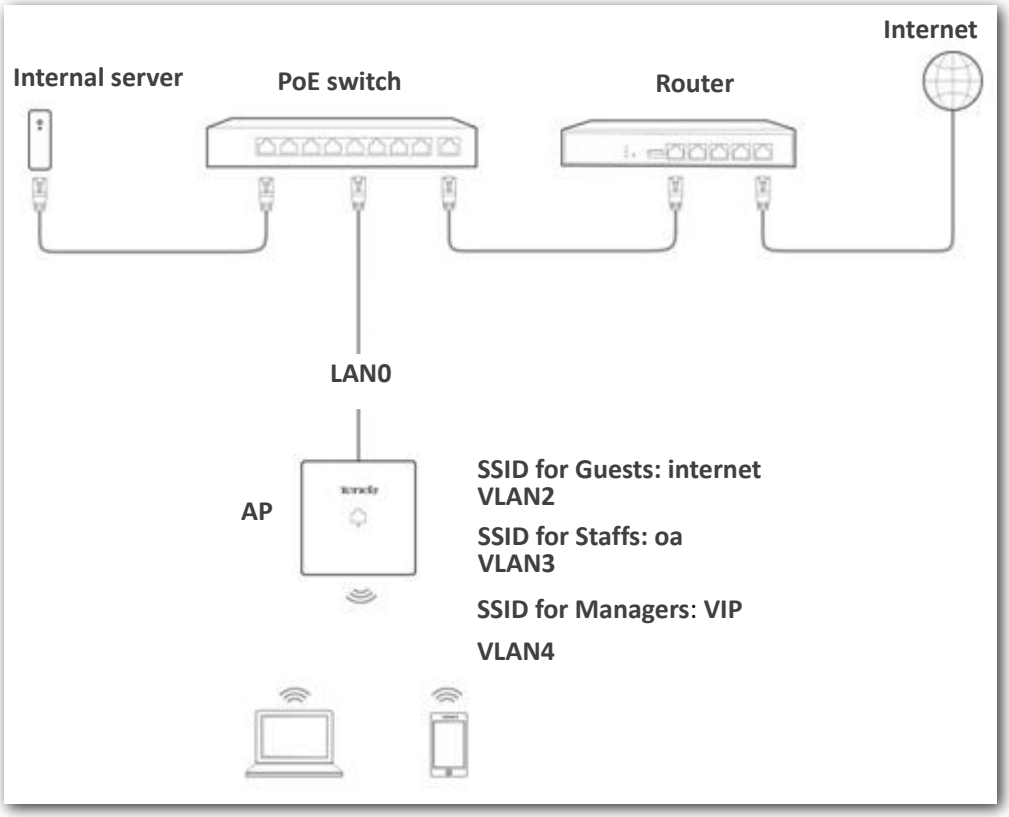
A hotel has the following wireless network coverage requirements:

- Guests are connected to VLAN 2 and can access only the internet. Staffs are connected to VLAN 3 and can access only the LAN.
- Managers are connected to VLAN4 and can access both the LAN and the internet.

Networking assumption

- Set the SSID to **internet** for guests, **oa** for staffs, and **VIP** for managers for 2.4 GHz network.
- The wireless networks with the aforementioned SSIDs are enabled and set on the AP.

Network topology



Configuration procedure

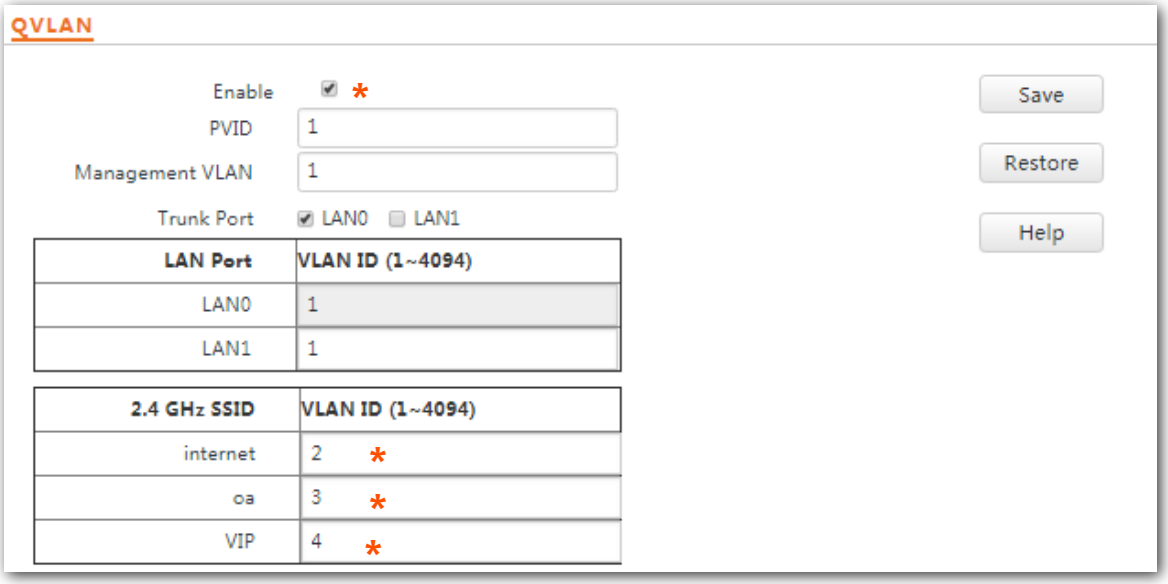
Configure the AP

Step 1 Log in to the web UI of the AP and choose **Wireless Setting** > **QVLAN Settings**.

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

Step 3 Modify the VLAN ID of the SSIDs at 2.4 GHz band. Set the VLAN of internet to **2**, oa to **3**, and VIP to **4** respectively.

Step 4 Click **Save**.



---End

Wait for the automatic reboot of the AP.

Configure the switch

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

Port Connected To	Accessible VLAN ID	Port Type	PVID
AP	1,2,3,4	Trunk	1
LAN server	3,4	Trunk	1
Router	2,4	Trunk	1

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

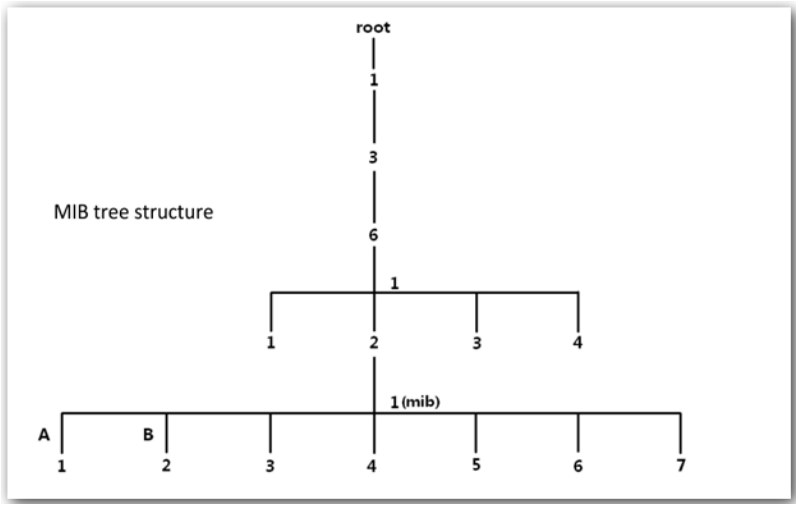
8.1.3 SNMP Protocol Version

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 calling 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.

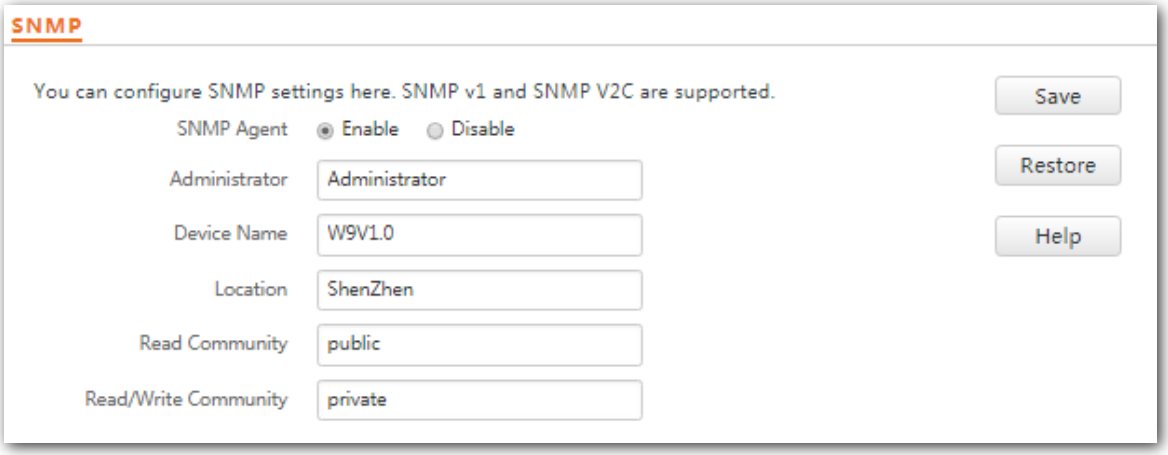


8.2 Configuring the SNMP Function

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

Step 2 Set related SNMP parameters.

Step 3 Click **Save**.



---End

Parameter description

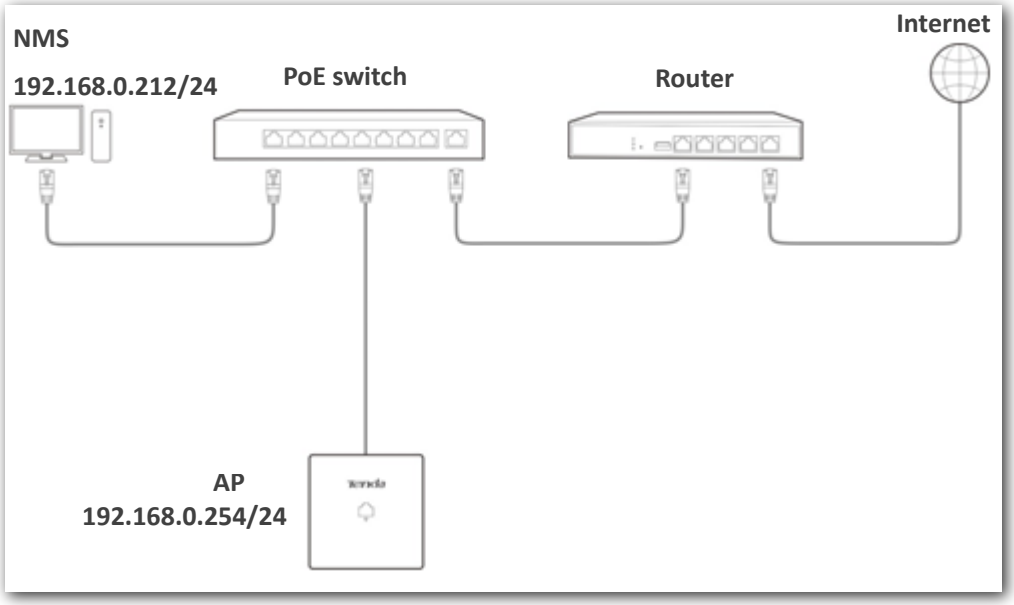
Parameter	Description
SNMP Agent	It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled. An SNMP manager and the SNMP agent can communicate with each other only if their SNMP versions are the same. Currently, the SNMP agent function of the AP supports SNMP V1 and 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.
Device Name	It specifies the device name of the AP. The default device name is the model of the AP. TIP 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. The default location is ShenZhen. 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**.

Parameter	Description
	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 use SNMP V1 or SNMP V2C to monitor and manage the AP.



Configuration procedure

Configuring the AP

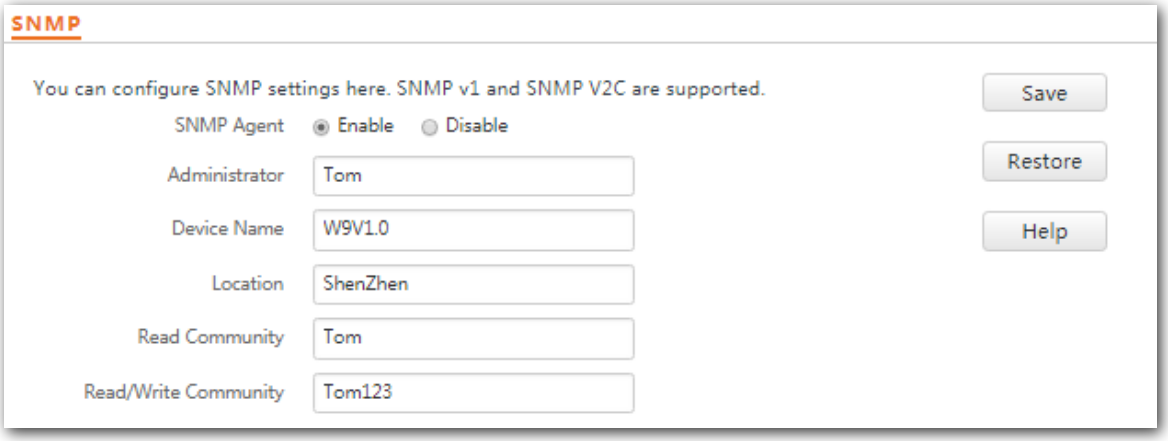
Assume that the administrator name is **Tom**, read community is **Tom**, and read/write community is **Tom123**.

Step 1 Log in to the web UI of the AP and choose **SNMP**.

Step 2 Set **SNMP Agent** to **Enable**.

Step 3 Set the SNMP parameters, Administrator, Device Name, Location, Read Community and Read/Write Community

Step 4 Click **Save**.



---End

Configuring the NMS

On an NMS that uses SNMP V1 or SNMP V2C, set the read community to **Tom** and read/write community to **Tom 123**. For details about how to configure the NMS, refer to the configuration guide for the NMS.

Verification

After the configuration, the NMS can connect to the SNMP agent of the AP and 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.

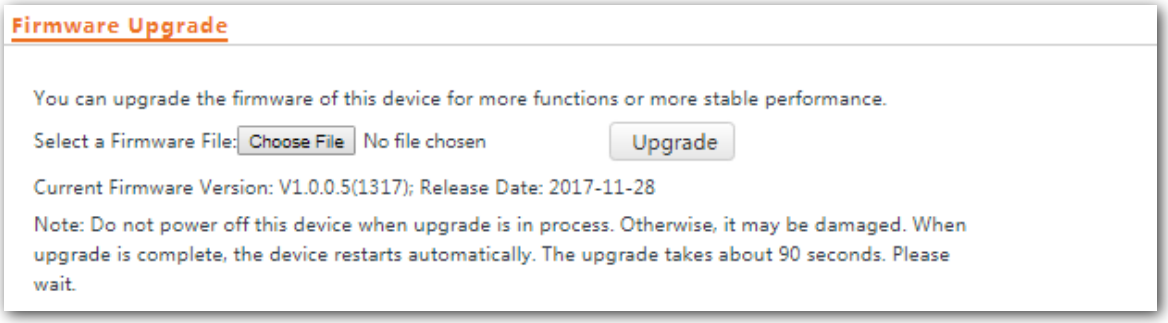
Configuration procedure:

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

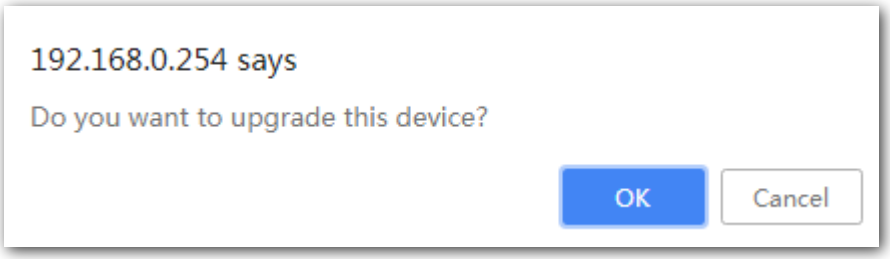
Step 2 Log in to the web UI of the AP and choose **Tools** > **Firmware Upgrade**.

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

Step 4 Click **Upgrade**.

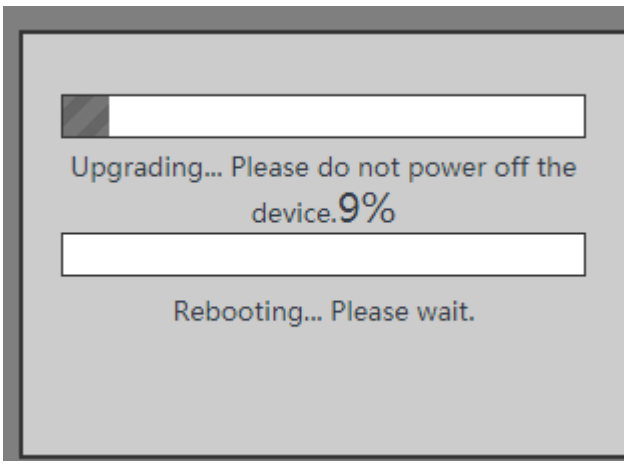


Step 5 Click **OK**.



---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.

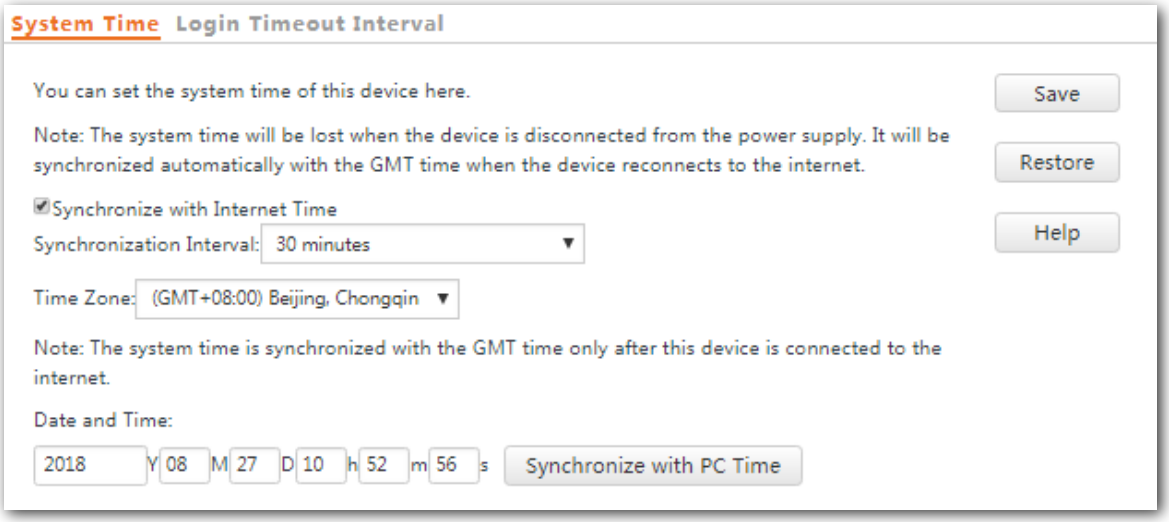
9.2 Date & Time

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.

Log in to the web UI of the AP, choose **Tools > Date & Time > System Time**.



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.

TIP

No matter which method you use to configure system time, when you log into the web UI of the AP, AP will automatically synchronize the time of the current management host.

Synchronizing with Internet Time

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.

Procedure for configuring the AP to synchronize its system time with the internet:

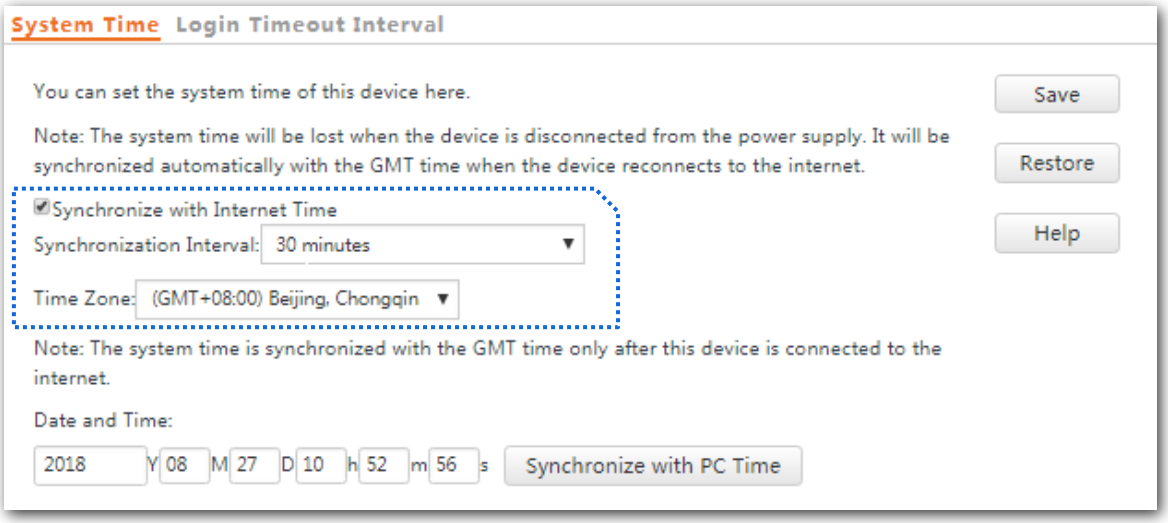
Step 1 Choose **Tools** > **Date & Time** > **System Time**.

Step 2 Select **Synchronize with Internet Time**.

Step 3 Set **Synchronization 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 the GMT standard time zone for the area where the AP is currently located.

Step 5 Click **Save**.



---End

Setting Time and Date Manually

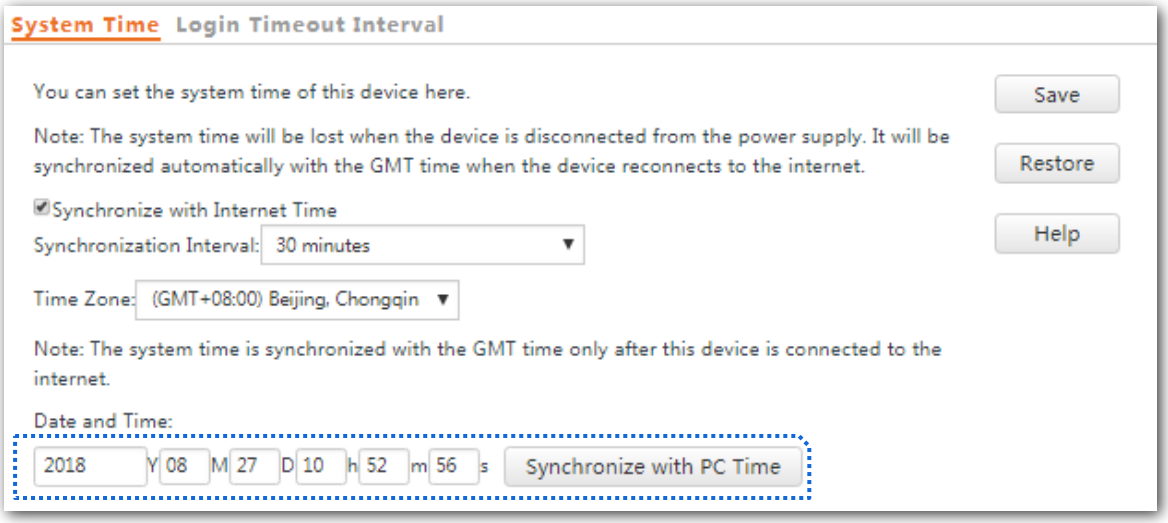
You can manually set the system time of the AP. If you choose this option, you need to set the system time each time after the AP reboots.

Configuration procedure:

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



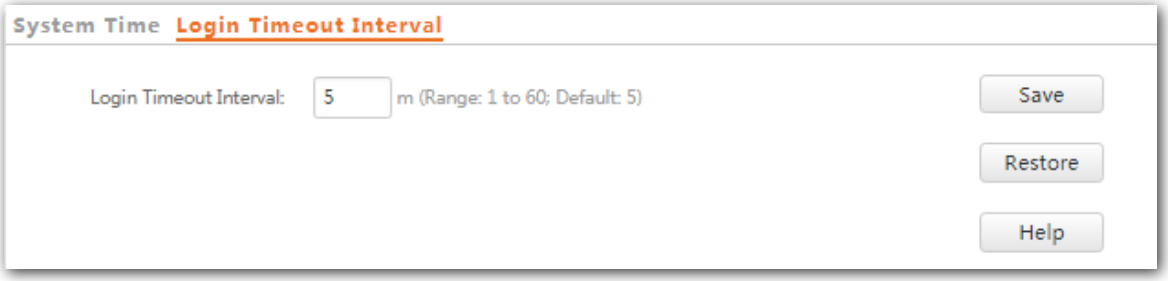
---End

9.2.2 Login Timeout Interval

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.

Procedure for setting the login timeout interval:

1. Choose **Tools** > **Date & Time,** and click **Login Timeout Interval**.
2. Change the login timeout interval as required.
3. Click **Save**.



---End

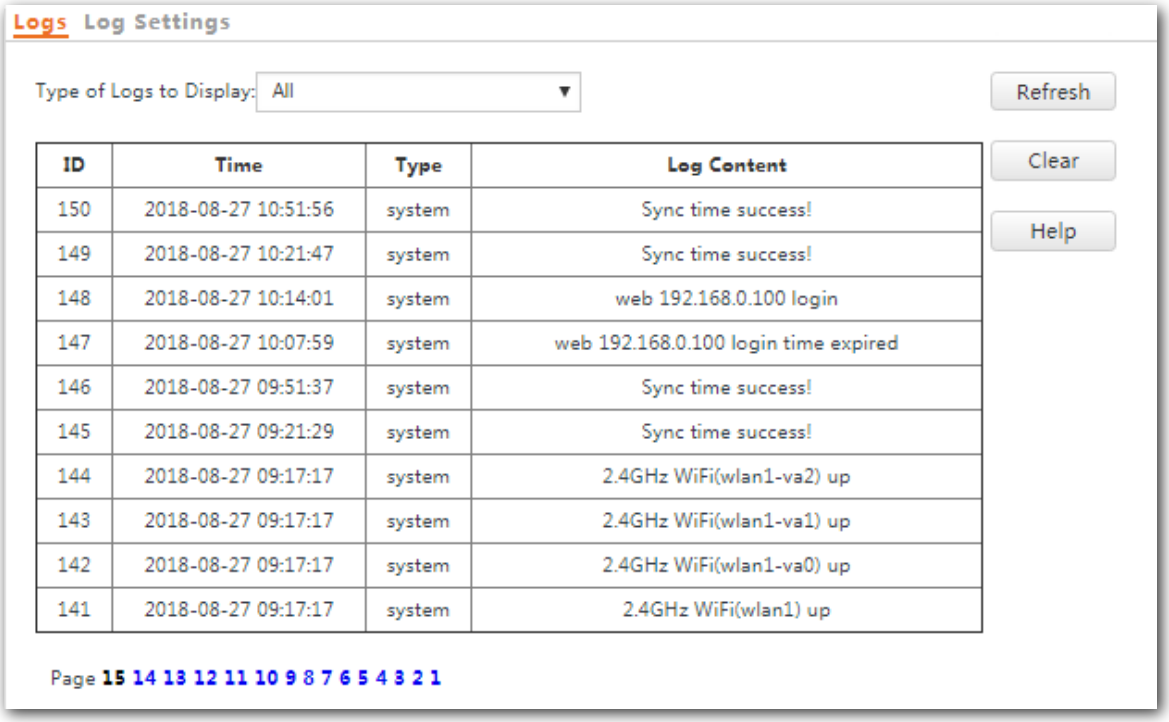
9.3 Logs

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**.



To ensure that the logs are recorded correctly, verify the system time of the AP. You can correct the system time of the AP by choosing **Tools** > **Time & Date** > **System Time**.

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

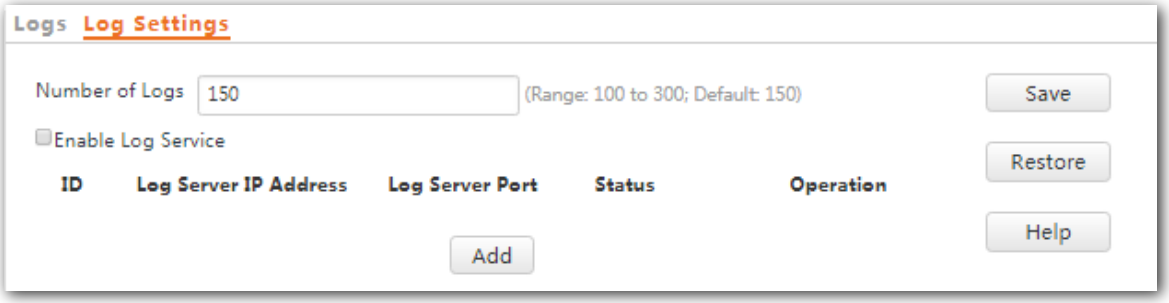
NOTE

- 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 backed up or 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.



Setting the Number of Logs to Be Displayed

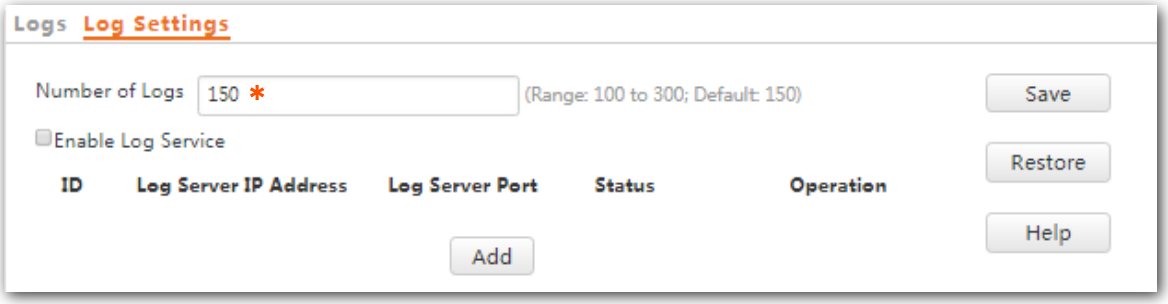
By default, the AP can display a maximum of 150 logs on the **View Logs** page. You can change the number as required.

Configuration procedure:

Step 1 To access the page, 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**.



---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.

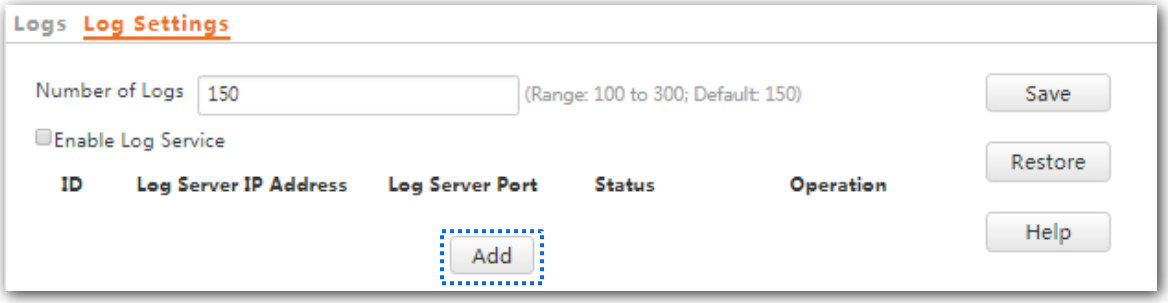
NOTE

To ensure that system logs can be sent to a log server, choose **Network Settings** > **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 To access the page, choose **Tools** > **Logs** and click **Log Settings**.

Step 2 Click **Add**.



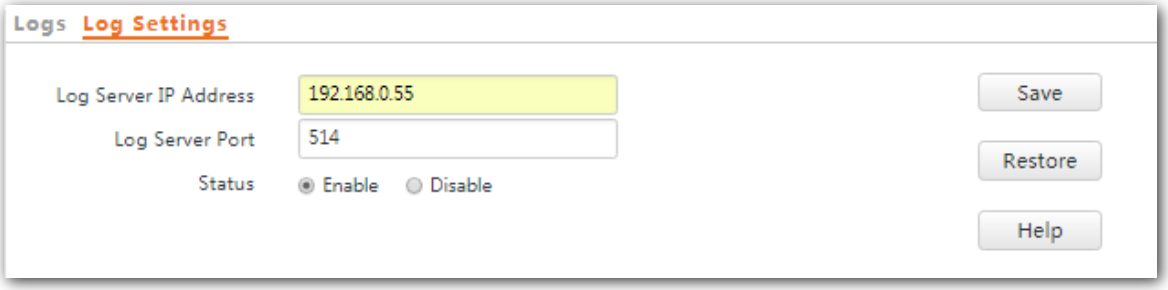
Step 3 Set parameters as follows:

Set **Log Server IP Address** to the IP address of the log server.

Set **Log Server Port** to the UDP port number used to send and receive system logs. The default port number 514 is recommended.

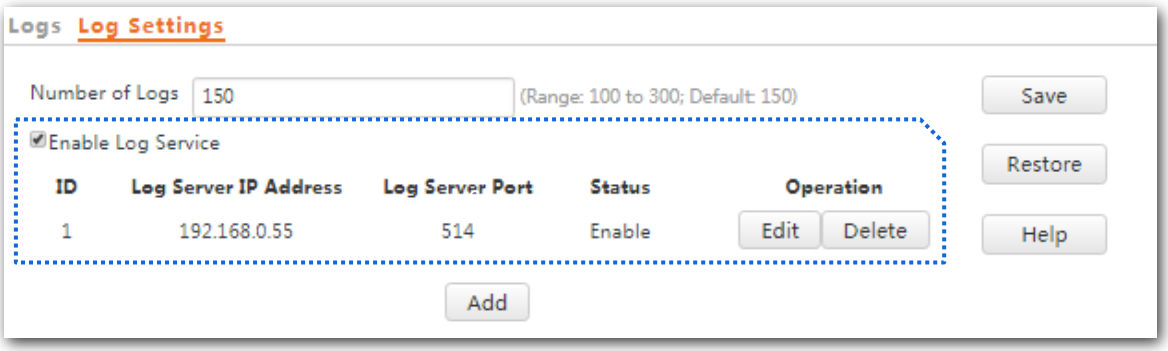
Select **Enable** to enable the log server.

Step 4 Click **Save**.



---End

The following figure shows the configuration.



Procedure for changing log server settings

Step 1 To access the page, choose **Tools** > **Logs** and click **Log Settings**.

Step 2 Click **Edit** 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 To access the page, choose **Tools** > **Logs** and click **Log Settings**.

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

Step 3 Click **OK**.

---End

9.4 Configuration

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.

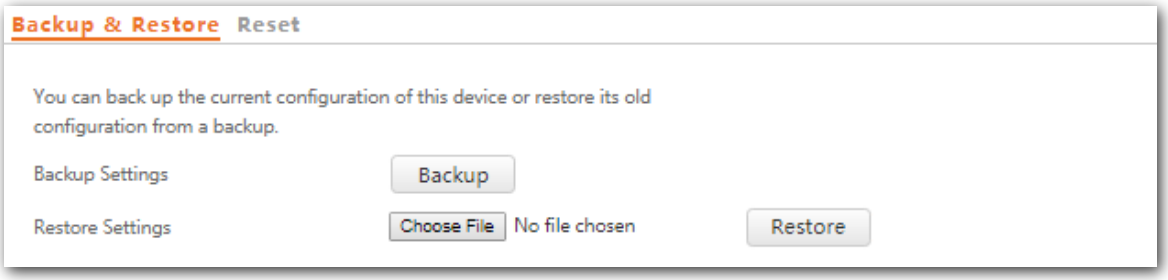
NOTE

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.

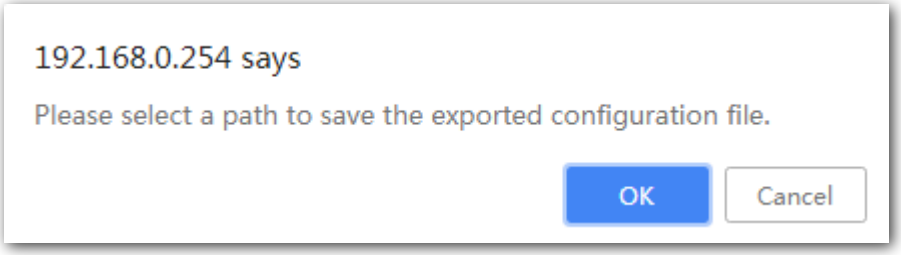
Backing Up the Current Configuration

Step 1 Choose **Tools** > **Configuration** > **Backup & Restore**.

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



Step 3 Click **OK**.



---End

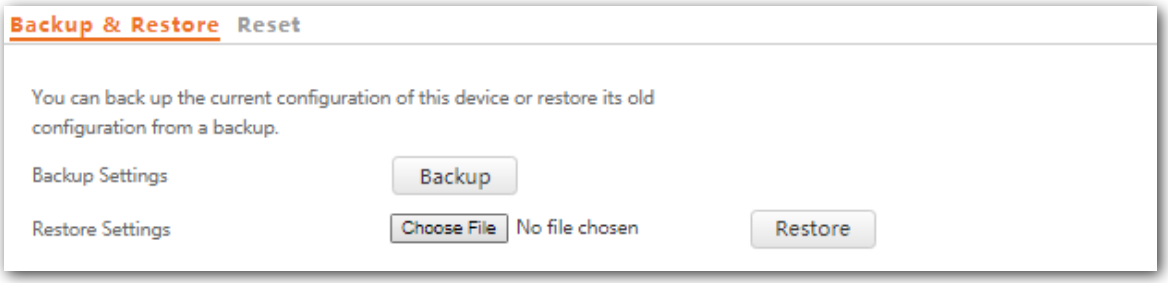
A configuration file named APCfm.cfg is downloaded.

Restoring a Configuration

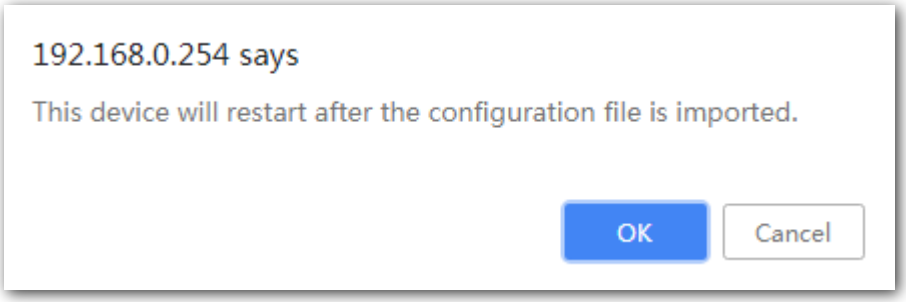
Step 1 Choose **Tools** > **Configuration** > **Backup & Restore**.

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

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

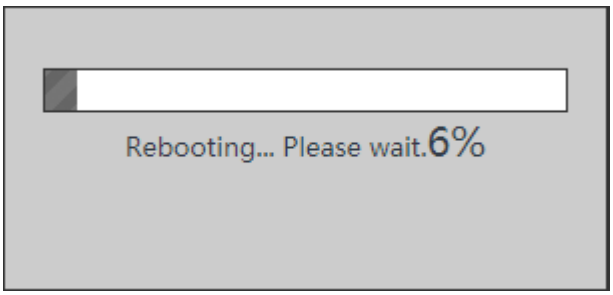


Step 4 Click **OK**.



---End

The AP restores the configurations successfully when the progress bar is done.



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.

NOTE

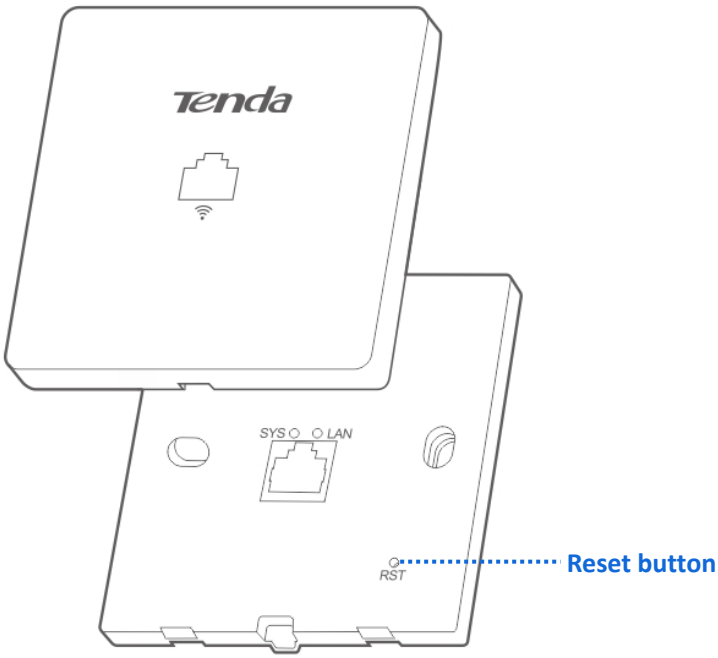
- When the factory settings are restored, your configuration is lost. Therefore, you need to reconfigure the AP to reconnect to the internet. Restore the factory settings of the AP only when necessary.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.
- After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

Method 1:

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

Procedure: After the AP is powered on, use a pin to hold down the reset button for 8 seconds and release it until the green LED indicator turns solid on.

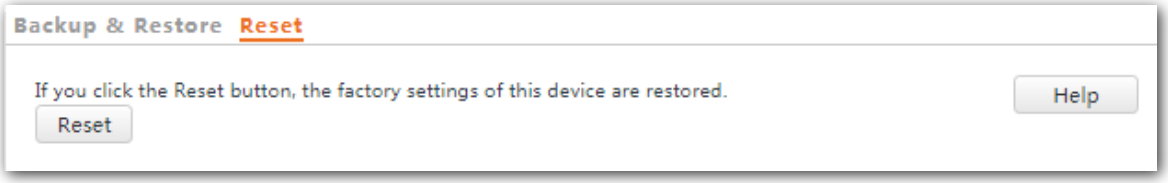
The AP is restored to factory settings when the green LED indicator (SYS indicator) blinks again.



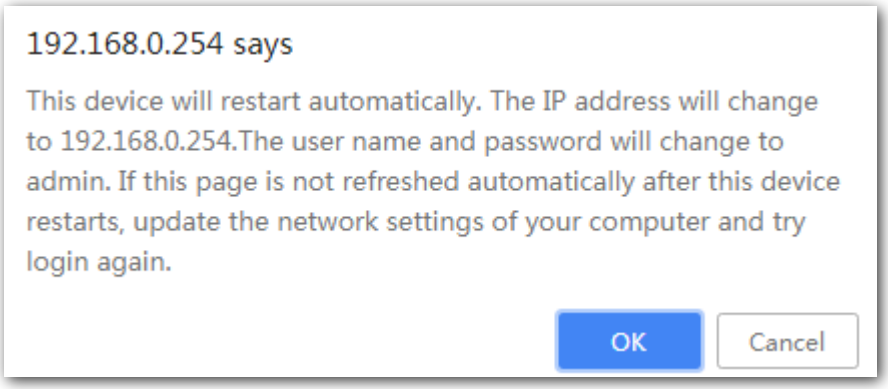
Method 2:

Step 1 Log in to the web UI of the AP, choose **Tools** > **Configuration** and click the **Reset** tab.

Step 2 Click the **Reset** button.

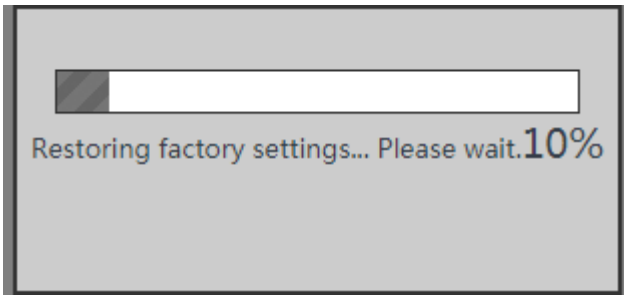


Step 3 Click **OK**.



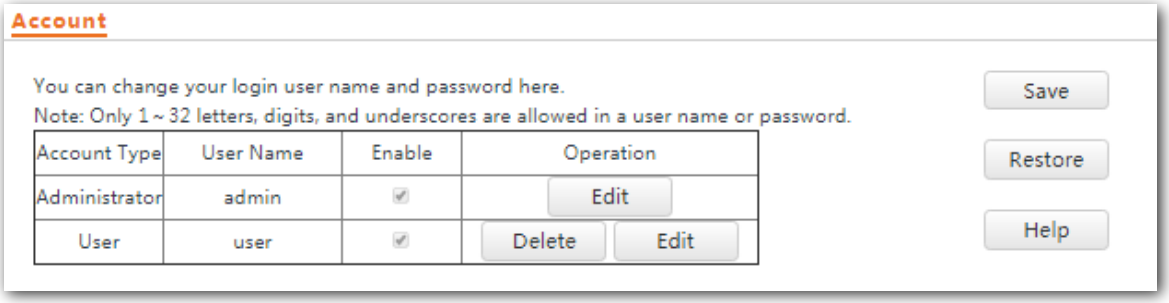
---End

Wait until the progress bar is done.



9.5 Account

To access page for changing user names and passwords, choose **Tools** > **Account**.
On this page, you can change the login account information of the AP to prevent unauthorized login.



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 only.
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	• **Edit**: This button is used to modify 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 a user account after the account is deleted. NOTE After editing, deleting, or adding an account, click **Save** to apply the settings.

9.6 Diagnostics Tool

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

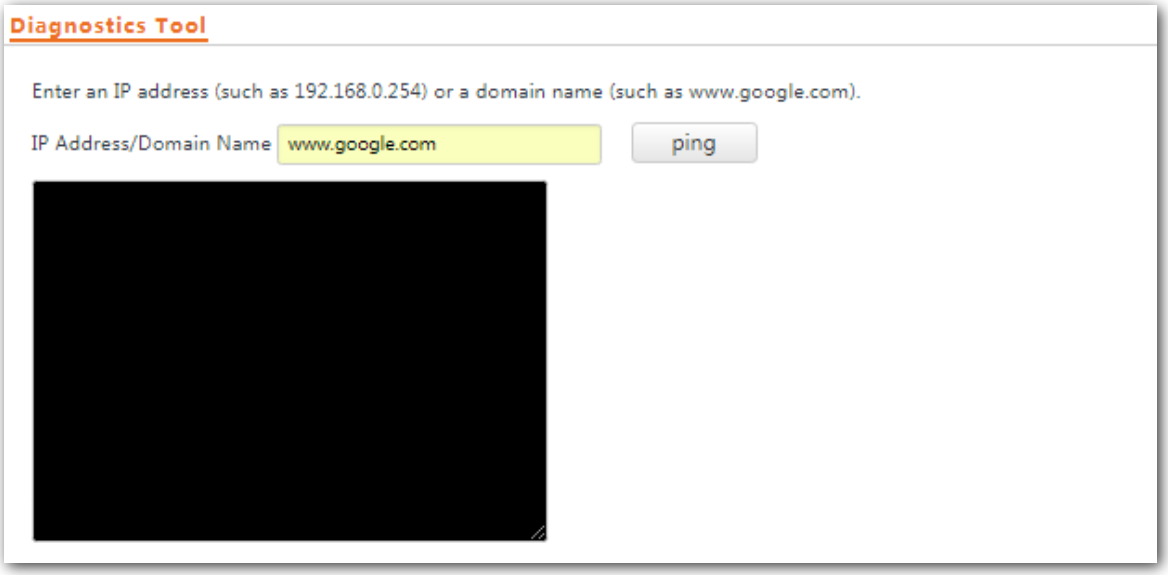
Procedure:

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

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

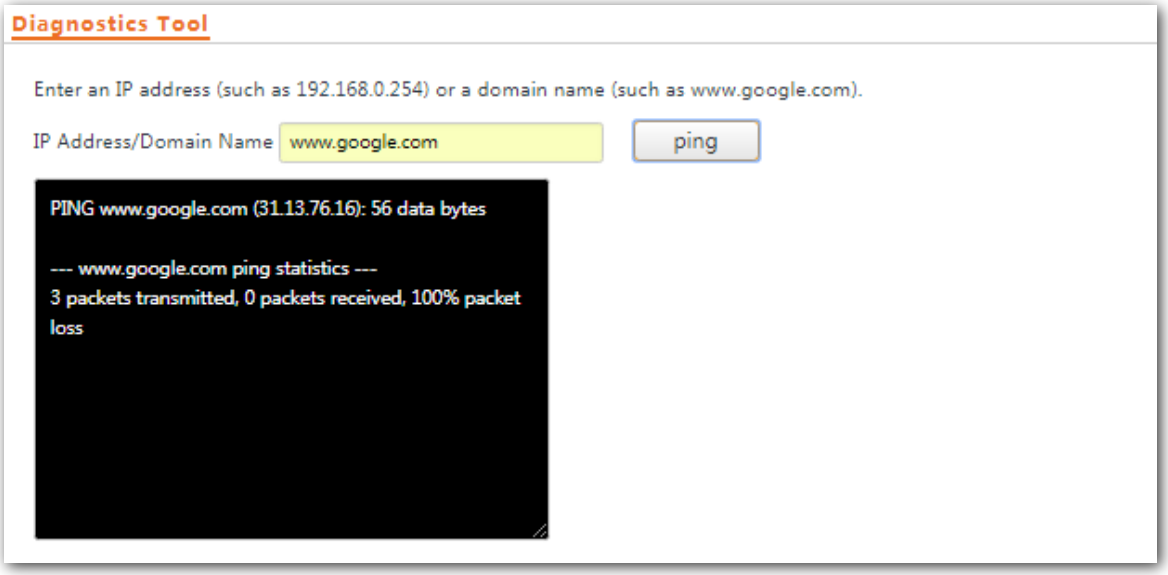
Step 2 Enter the IP address or domain name to be pinged in the **IP Address/Domain Name** text box. In this example, enter **www.google.com**.

Step 3 Click **Ping**.



---End

The diagnosis result will be displayed in a few seconds in the black text box below the **IP Address/Domain Name** text box. See the following figure.


Diagnostics Tool
Enter an IP address (such as 192.168.0.254) or a domain name (such as www.google.com).
IP Address/Domain Name
www.google.com
ping
PING www.google.com (31.13.76.16): 56 data bytes
--- www.google.com ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss

9.7 Reboot Device

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.

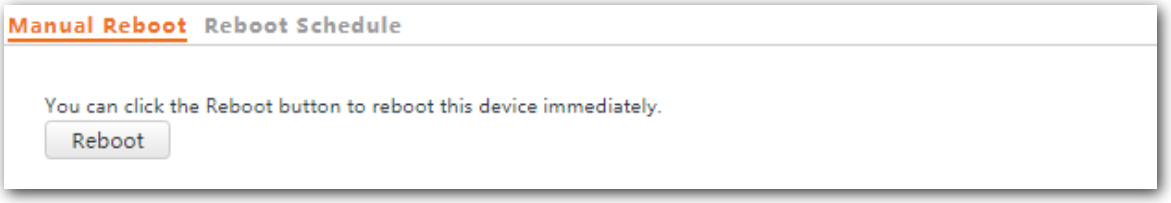
9.7.1 Manual Reboot

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

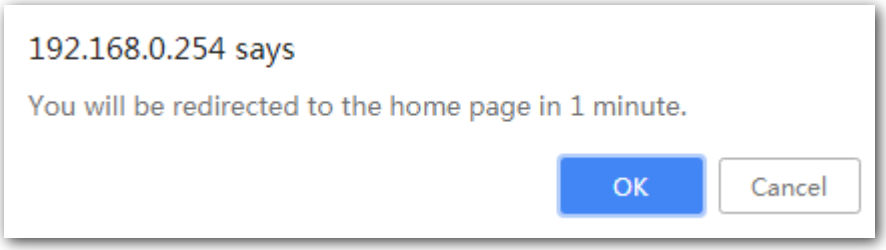
Procedure:

Step 1 To access the page, choose **Tools** > **Reboot Device** > **Manual Reboot**.

Step 2 Click **Reboot**.

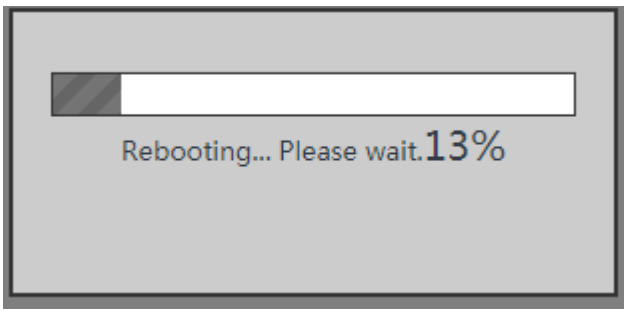


Step 3 Click **OK**.



---End

Wait until the progress bar is done.



9.7.2 Reboot Schedule

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 Intervals

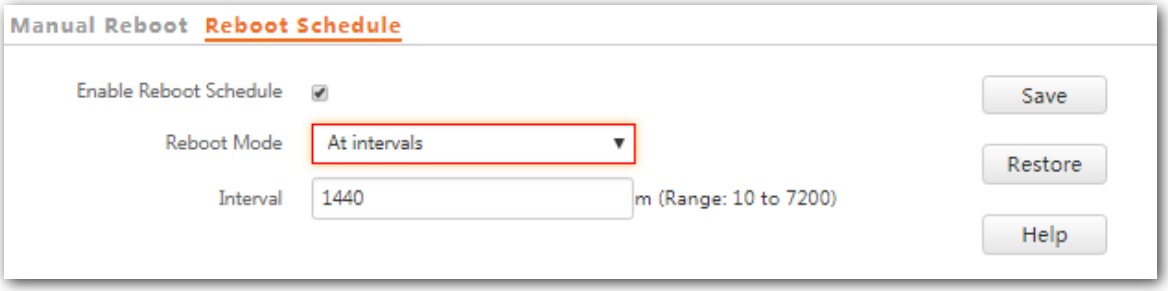
Step 1 Choose **Tools** > **Reboot Device** and click the **Reboot Schedule** tab.

Step 2 Select the **Enable Reboot Schedule** 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**.



---End

Configuring the AP to Reboot at Specified Time

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

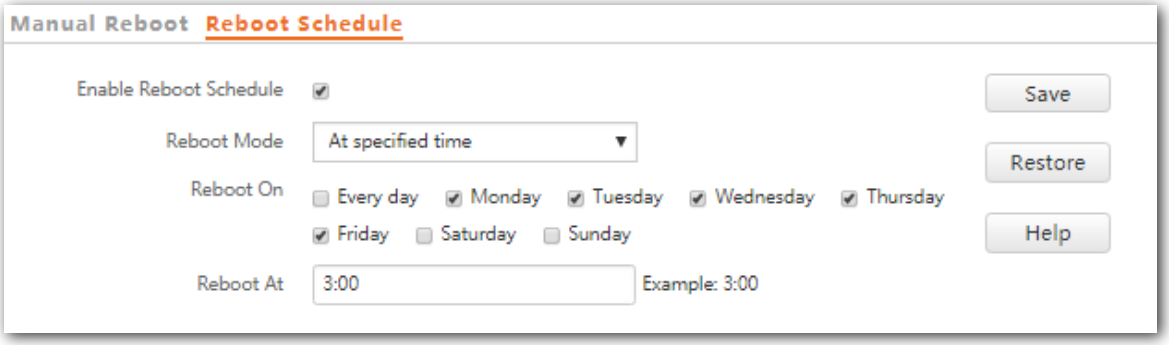
Step 2 Select the **Enable Reboot Schedule** check box.

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

Step 4 Select the day or days when the AP reboots, such as **Monday** - **Friday**

Step 5 Set the time when the AP reboots, such as **3:00**.

Step 6 Click **Save**.


Manual Reboot
Reboot Schedule
Enable Reboot Schedule
Reboot Mode
At specified time
Reboot On
Every day
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Reboot At
3:00
Example: 3:00
Save
Restore
Help

---End

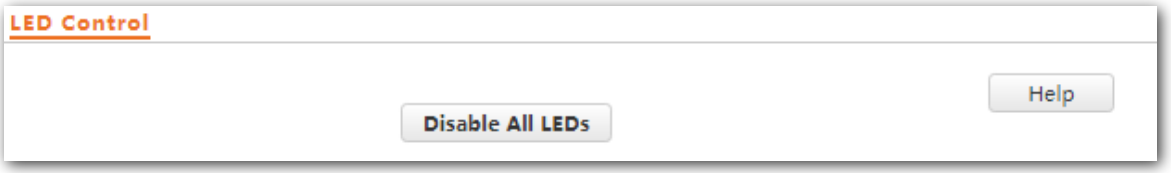
9.8 LED Control

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 **Disable all LEDs**.

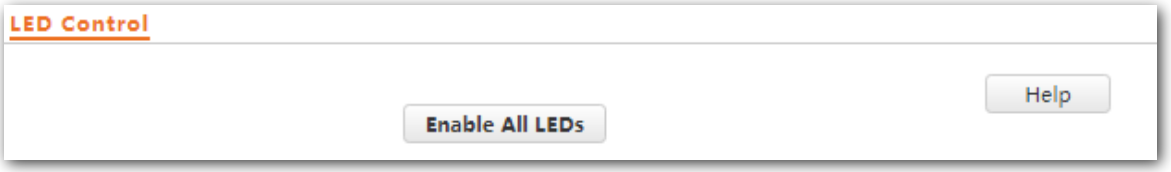


---End

Procedure for turning on the LED indicator:

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

Step 2 Click **Enable All LEDs**.



---End

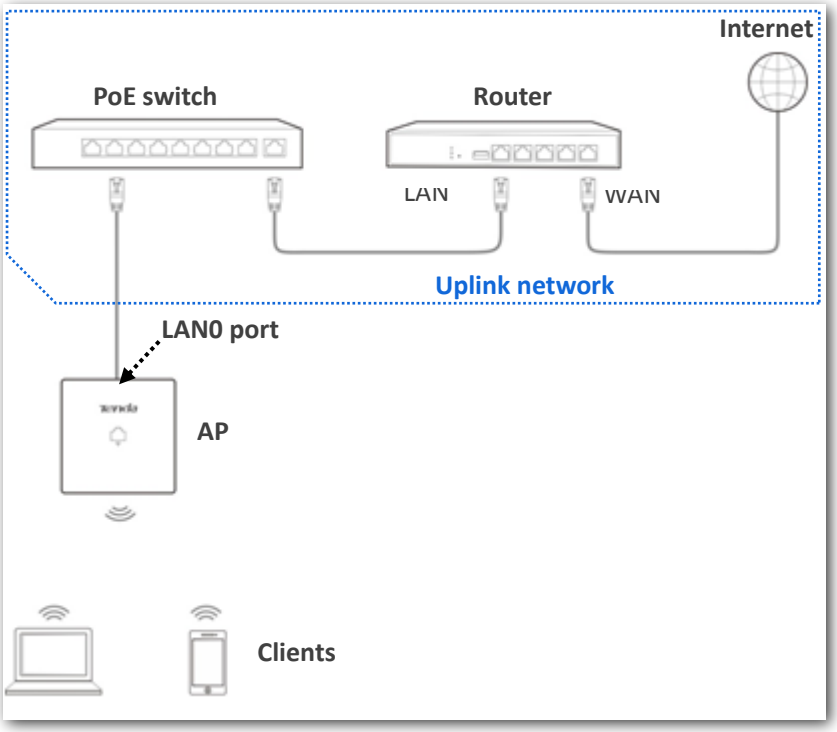
9.9 Uplink Check

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 check 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 check enabled is faulty, wireless clients can connect to the upstream network through another nearby AP that works properly.

See the following topology (The LAN0 port serves as the uplink port).



9.9.2 Configuring Uplink Check

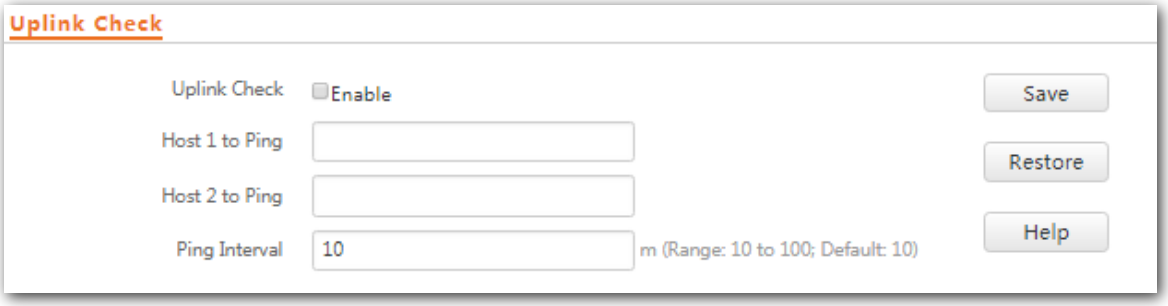
Step 1 Choose **Tools** > **Uplink Check**.

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

Step 3 Set **Host1 to Ping** or **Host2 to Ping** 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 **Ping Interval** to the interval at which the AP checks its uplink.

Step 5 Click **Save**.


Uplink Check
Uplink Check
Enable
Host 1 to Ping
Host 2 to Ping
Ping Interval
10
m (Range: 10 to 100; Default: 10)
Save
Restore
Help

---End

Appendixes

A.1 FAQ

Q1: The LED indicators are off, what should I do?

A1. Try the following solutions:

- Verify the AP's rear port is connected to a PoE port (compliant with IEEE 802.3af) of the PoE switch properly.
- Ensure the Ethernet cable used to connect the AP and PoE switch is an eight-core Ethernet cable.

Q2: I cannot access the web UI of the AP. What should I do?

A2. Check the following items:

- Verify that the IP address of your computer is in the same segment as the AP's IP address. If the IP address of the AP is 192.168.0.254, the IP address of the computer should be set as 192.168.0.*X* (*X*: 2-253).Ensure the IP address of the AP (it is 192.168.0.254 by default) is entered in the browser address bar (not search bar).
- If two or more APs are connected to your network without a Tenda AP controller (including a router equipped with the AP controller functionality). Change the IP address of each AP during configuration to avoid IP conflict. Otherwise, you can't access to the web UI of other 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.

Q3：How to reset the AP?

A3. After the AP is powered on, use a pin to hold down the reset button for 8 seconds and release it until the green LED indicator turns solid on.

The AP is restored to factory settings when the green LED indicator (SYS indicator) blinks again.

Q4: My wireless devices, such as smart phones, cannot access the internet via the AP after configuration. What should I do?

A4. Try the following solutions:

- Ensure that your wireless devices connect to the wireless network of the AP.
- Verify the router connected to the AP can access to the internet successfully.

A.2 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 Mode
LAN Setup	IP Address Type		Static IP Address
	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
	Device Name		The model of the AP. For example, the default name of W9 V1.0 is W9V1.0.
DHCP Server	DHCP Server		Disable
	Start IP		192.168.0.100
	End IP		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
SSID Settings	SSID	2.4 GHz	The AP allows 8 SSIDs. The SSID displayed is Tenda_*XXXXXX*. Where *XXXXXX* indicates the range from the last 6 characters to the last 6 characters + 7 of the MAC address of the LAN ports of the AP. By default, the primary SSID is enabled, and the other SSIDs are disabled.

Parameter			Default Value
		5 GHz	The AP allows 4 SSIDs. The SSID displayed is Tenda_*XXXXXX*_*5G*. Where *XXXXXX* indicates the range from the last 6 characters + 8 to the last 6 characters +11 of the MAC address of the LAN ports of the AP. By default, the primary SSID is enabled, and the other SSIDs are disabled.
	Broadcast SSID		Enable
	Isolate Client		Disable
	WMF		Enable
	Suppress Broadcast Probe Response		Disable
	Max. Number of Clients		48
	Chinese SSID Encoding		UTF-8
	Security Mode		None
Radio Settings	Enable wireless		Enable
	Country/Region		China
	Network Mode	2.4GHz	11b/g/n
		5GHz	11ac
	Channel		Auto
	Channel Bandwidth	2.4GHz	20/40 MHz
		5GHz	80 MHz
	Lock Channel		Enable
	Lock Power		Enable
	Preamble		Long Preamble
	Short GI		Enable
	Isolate SSID		Disable
Radio Optimization	Beacon Interval		100 ms
	Fragment Threshold		2346
	RTS Threshold		2347

Parameter			Default Value
	DTIM Interval		1
	Minimum RSSI Threshold		-90 dBm
	Prioritize 5GHz		Disable
	Air Interface Scheduling		Disable
	APSD		Disable
	Client Timeout Interval		5 minutes
	Mandatory Rate	2.4 GHz	1, 2, 5.5, 11
		5 GHz	6, 12, 24
	Optional Rate	2.4 GHz	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
		5 GHz	6, 9, 12, 18, 24, 36, 48, 54
WMM Settings	WMM		Enable
	WMM Optimization Mode		Optimized for scenario with more than 10 users
Access Control			Disable
Advanced Settings	Identify Client Type		Disable
	Broadcast Packet Filter		Disable
QVLAN	Enabled		Disable
	PVID		1
	Management VLAN		1
	Trunk Port		LAN0
	LAN Port VLAN ID		1
	2.4 GHz SSID VLAN ID		1000
	5 GHz SSID VLAN ID		1000
SNMP	SNMP Agent		Disable
	Administrator		Administrator
	Device Name		The model of the AP. For example, the default name of W9 V1.0 is W9V1.0.
	Location		ShenZhen
	Read Community		public

Parameter			Default Value
	Read/Write Community		private
Tools	Time & Date	System Time	If **Synchronize with Internet time** is selected: Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei
		Login Timeout Interval	5 minutes
	Number of Logs Displayed		150
	Log server settings		None
	Reboot Schedule		Disable
	LED Control		Enable all LEDs
	Uplink Check		Disable