# AC1200 Wave2 Celling Access Point

# User Guide

V1.0

## Copyright Statement

© 2022 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Tenda is a registered trademark legally held by Shenzhen Tenda Technology Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Shenzhen Tenda Technology Co., Ltd.

## Disclaimer

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

# Preface

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

This user guide walks you through all functions on the AC1200 Wave2 Celling Access Point. All the screenshots and product figures herein, unless otherwise specified, are taken from i24.

## Conventions

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

| Item | Presentation | Example |
|---|---|---|
| Cascading menus | > | Internet Settings > LAN Setup |
| Parameter and value | Bold | Set **SSID** to **Tom**. |
| Variable | Italic | Format: *XX:XX:XX:XX:XX:XX* |
| UI control | Bold | On the **Quick Setup** page, click the **Save** button. |

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

| Symbol | 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. |

## For more documents

APs of this series support central management either by Tenda Access Point Controller (AC) or Tenda router that supports AP management. For detailed information, refer to user guides of target ACs or routers.

Search target product models on our official website www.tendacn.com to obtain the latest product documents.

Product document overview

| Document | Description |
|---|---|
| Data Sheet | It introduces the basic information of the device, including product overview, selling points, and specifications. |
| Quick Installation Guide | It introduces how to set up the device quickly for internet access, the descriptions of LED indicators, ports, and buttons, FAQ, statement information, and so on. |
| User Guide | Walks you through detailed functions and configurations of APs, including all the functions on the web UI. |

## Technical Support

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

| | | | |
|---|---|---|---|
| ☎ Hotline | Global: (86) 755-27657180<br>(China Time Zone) | ✉ Email | support@tenda.com.cn |
| | United States: 1-800-570-5892<br>(Toll Free: 7 x 24 hours) | | |
| | Canada: 1-888-998-8966<br>(Toll Free: Mon - Fri 9 am - 6 pm PST) | | |
| | Hong Kong: 00852-81931998 | | |
| Website | https://www.tendacn.com/ | | |

## Revision History

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the i24 was introduced.

| Version | Date | Description |
|---|---|---|
| v1.0 | 2022-03-17 | Original publication. |

# Contents

# 1 Get to know your device

## 1.1 Product overview

Tenda AC1200 Wave2 Celling Access Point supports ceiling installation and wall-mounting installation, which is suitable for indoor wireless coverage in hotels, enterprises, KTV and other public places. The AP supports IEEE 802.3at standard PoE power supply and power adapter power supply. Users can choose flexibly according to actual needs. Users can manage the AP through the web UI of the AP, or through a Tenda access point controller or Tenda router that supports AP management.

## 1.2 Application scenarios

### 1.2.1 Small-scale wireless network networking

If you need to network a small-scale wireless network with several APs, you can use the following solution: 1 wired router + 1 PoE switch + n ceiling APs.

TIP

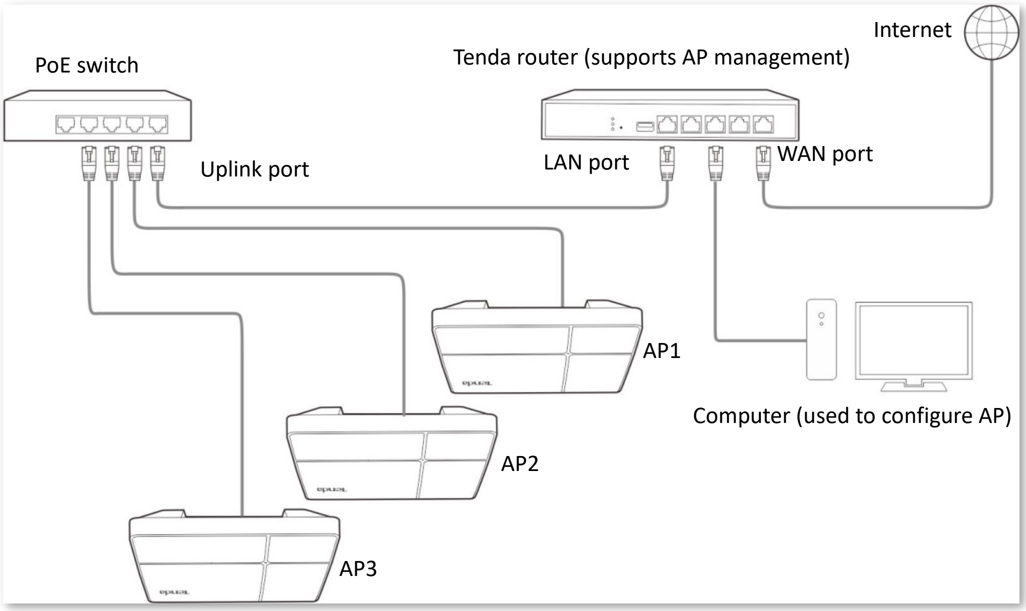
PoE power supply is used as an example in this section.

## With a Tenda router that supports AP management

Using a Tenda router that supports AP management, APs can be configured in batches through the router.

### Network topology

Connect all APs to the PoE ports of the PoE switches with Ethernet cables, as shown in the figure below.


Internet
PoE switch
Tenda router (supports AP management)
Uplink port
LAN port
WAN port
AP1
Computer (used to configure AP)
AP2
AP3

### Setting APs

Connect the management computer to the router with an Ethernet cable. Then log in to the web UI of the router to set APs in batches. For details, please refer to the user guide of the corresponding router model.

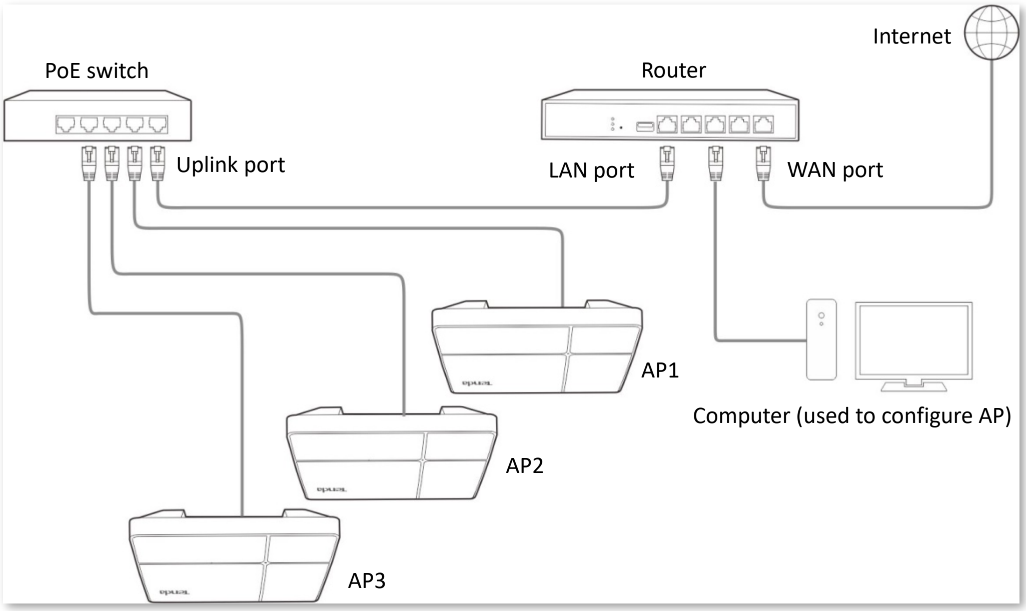
## With other routers

The router does not support configure APs in batches in the following situations.

- The router is not a Tenda router.
- The router is a Tenda router that does not support AP management.

### Network topology

Connect all APs to the PoE ports of the PoE switches with Ethernet cables, as shown in the figure below.



### Setting APs

Connect the management computer to the router with an Ethernet cable. Then log in to the web UI of the AP to set the AP separately. For details, please refer to Logging in to the web UI of the AP and the following sections.

NOTE

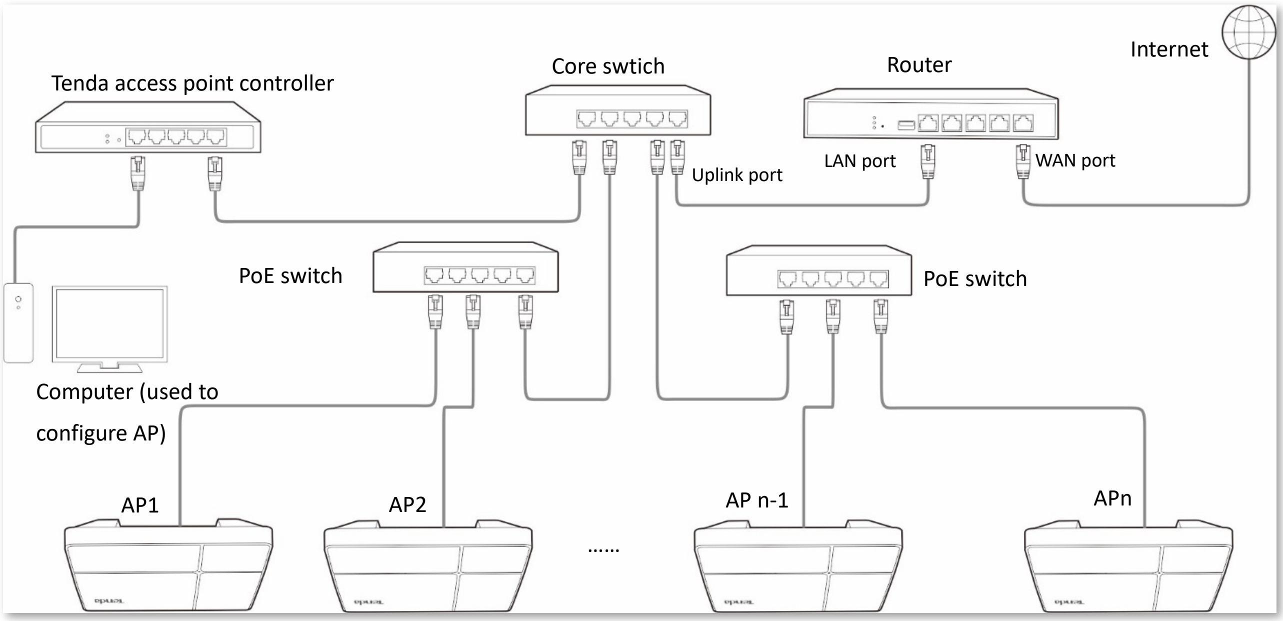
If multiple APs are connected to the network at the same time, to avoid network failure caused by IP address conflict, you need to modify the IP address of the AP when setting the AP. For details, see Modify LAN IP.

## 1.2.2 Large-scale wireless network networking

If you need to network a large-scale wireless network, such as hotels, enterprises, stations, the management is more complicated due to the large number of installed APs. It is recommended to deploy Tenda access point controllers in the network to centrally manage all APs.

- **Network topology**

Connect all APs to the PoE ports of the PoE switches with Ethernet cables, as shown in the figure below.



- **Set APs**

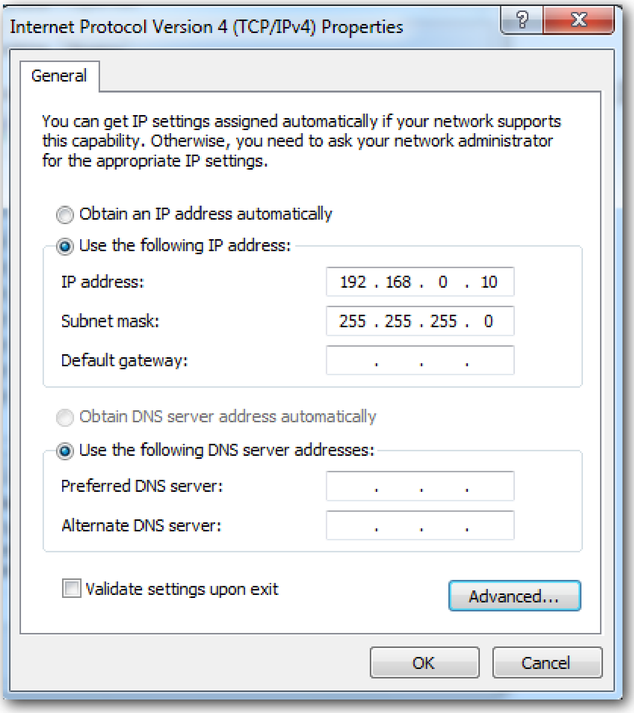
Connect the computer to the access point controller with an Ethernet cable. Then log in to the web UI of the access point controller to set APs in batches. For details, please refer to the user guide of the corresponding access point controller model.

# 2 Web UI operations

## 2.1 Logging in to the web UI of the AP

**Step 1** Connect your computer to the AP or the switch connected to the AP with an Ethernet cable.

**Step 2** Ensure that the IP address of the management computer is in the same network segment of the AP. For example, if the IP address of the AP is **192.168.0.254**, the management computer should be configured with an IP address of **192.168.0.*X*** (*X*: 2~253).



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

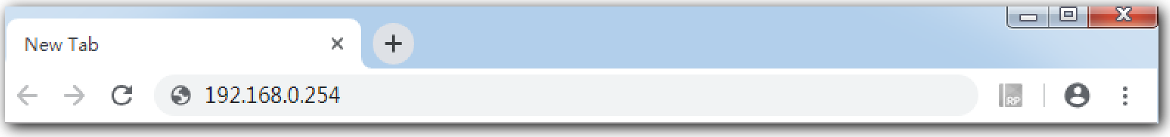
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

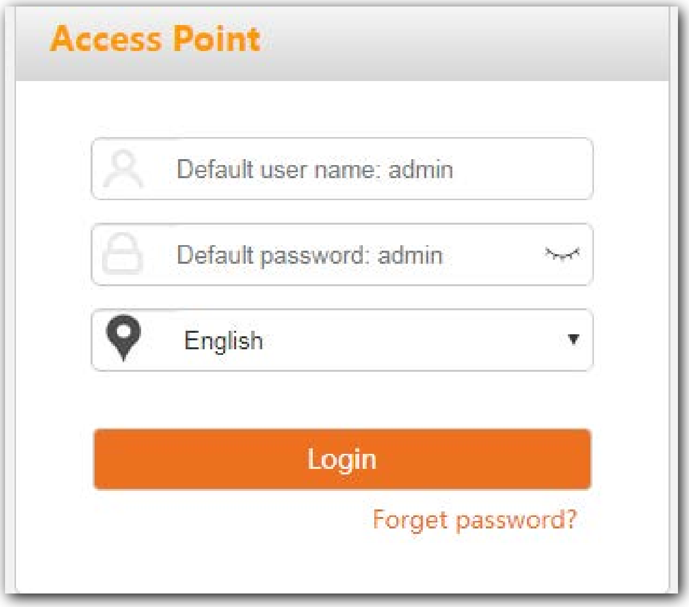
□ Validate settings upon exit

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



192.168.0.254

Step 4 Enter the login user name and password (default: **admin/admin**), and click **Login**.

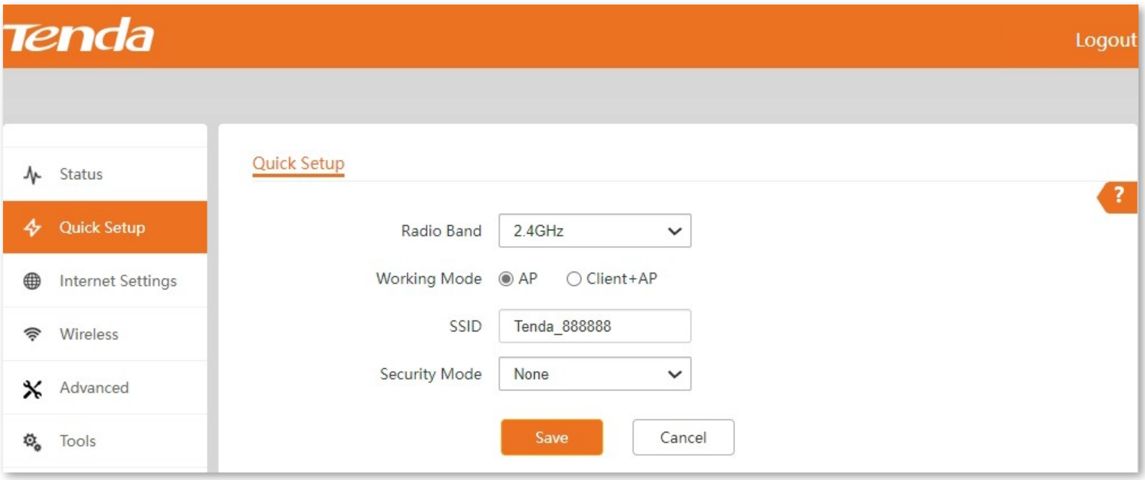


NOTE

If the login page does not appear, refer to Q1 in A.2 FAQ.

---- End

Log in to the web UI of the AP. You can configure the AP now.



Radio Band: 2.4GHz

Working Mode: ● AP ○ Client+AP

SSID: Tenda_888888

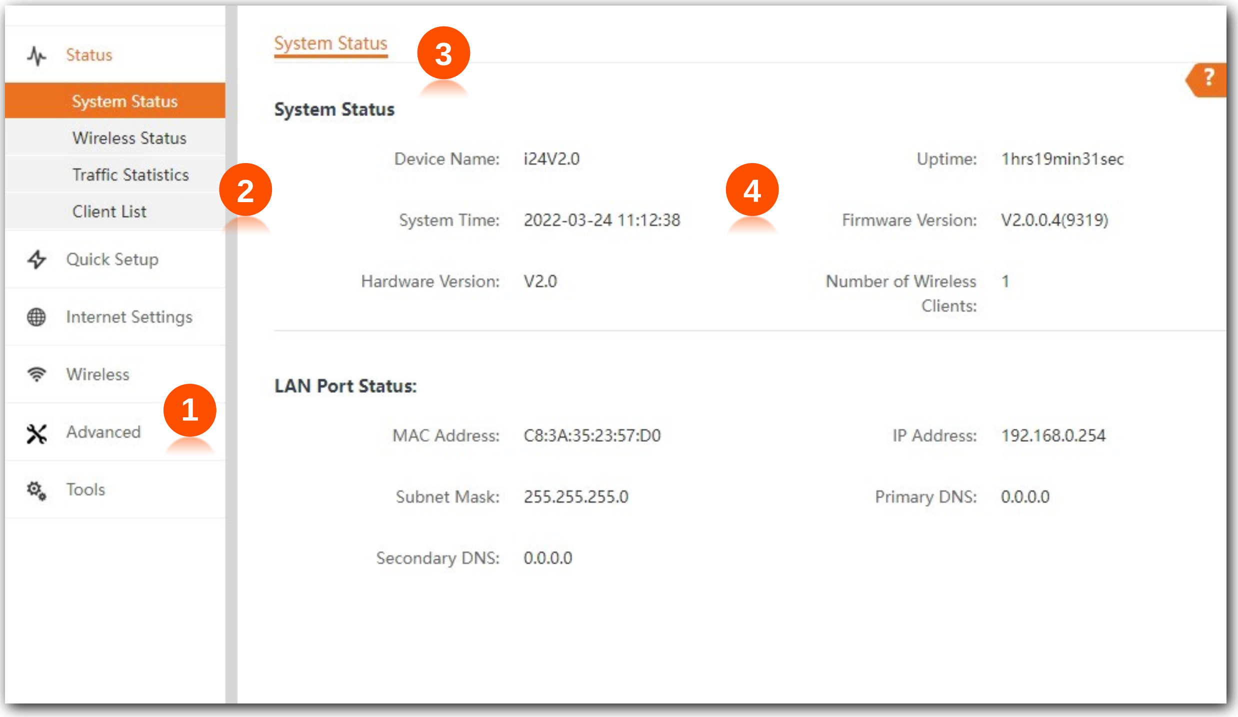
Security Mode: None

## 2.2 Logging out

After logging in to the web UI of the AP, if no operations are performed during the Login Timeout Interval, the system will log out automatically. In addition, you can click **Logout** on the upper right corner to safely exit from the web UI.

## 2.3 Web UI layout

The web UI of the AP consists of four sections, including the level-1, and level-2 navigation bars, tab page area, and the configuration area. See the following figure.



**System Status**

Device Name: i24V2.0

Uptime: 1hrs19min31sec

System Time: 2022-03-24 11:12:38

Firmware Version: V2.0.0.4(9319)

Hardware Version: V2.0

Number of Wireless Clients: 1

**LAN Port Status:**

MAC Address: C8:3A:35:23:57:D0

IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

TIP

Functions or parameters displayed in gray on the web UI are not supported yet or cannot be modified under the current configurations.

| No. | Name | Description |
|---|---|---|
| 1 | Level-1 navigation bar | Used to display the function menu of the AP. Users can select functions in the navigation bars and the configuration appears in the configuration area. |
| 2 | Level-2 navigation bar | |
| 3 | Tab page area | |
| 4 | Configuration area | Used to modify or view your configuration. |

## 2.4 Frequently-used buttons

The following table describes the frequently-used buttons available on the web UI of the AP.

| Button | Description |
|---|---|
| Refresh | Used to refresh the current page. |
| Save | Used to save the configuration on the current page and enable the configuration to take effect. |
| Cancel | Used to modify the current configuration on the current page back to the original configuration. |
| ? | Used to get the online help. |

# 3 Quick setup

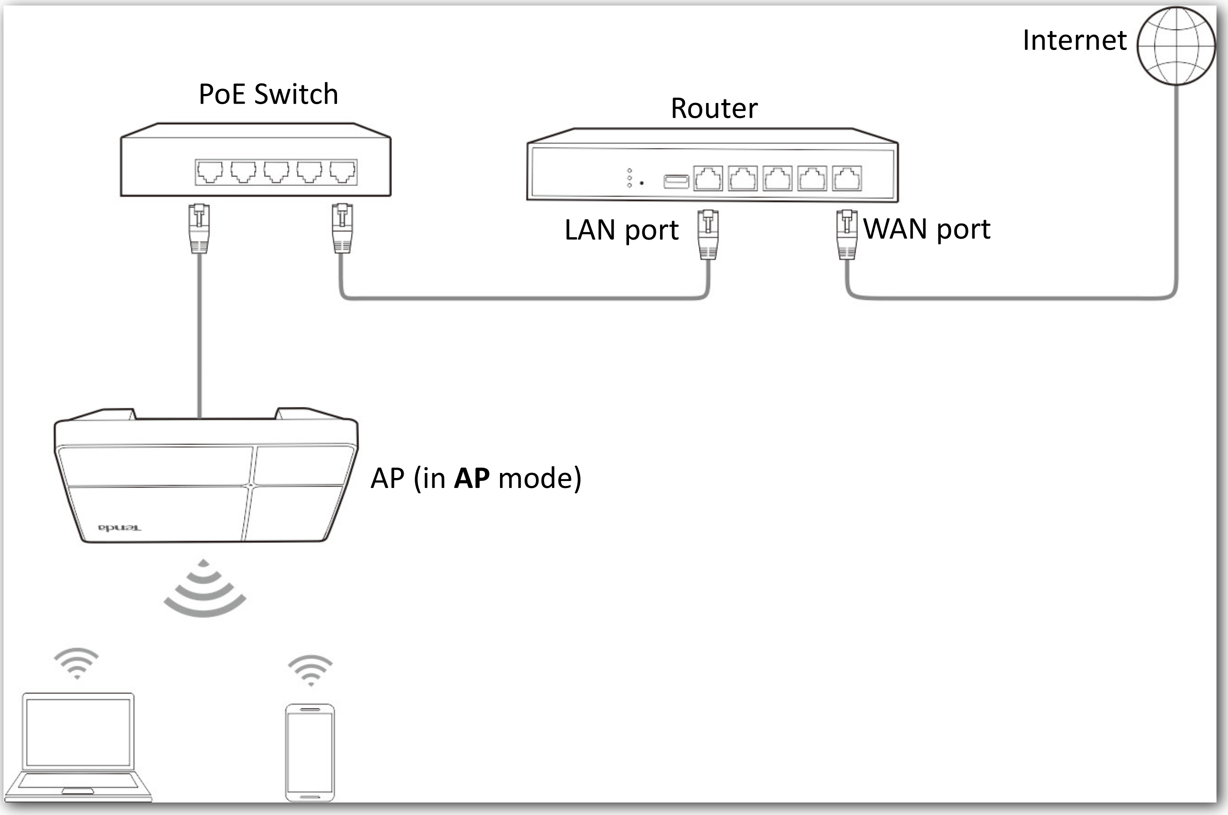
In the **Quick Setup** module, you can set up the AP in a quick way to enable internet access for your wireless devices such as smart phones and tablets.

The AP supports two working modes: AP mode and Client+AP mode.

## 3.1 AP mode

### 3.1.1 Overview

The AP works in this mode by default. In this mode, AP connects to the internet using Ethernet cables and transforms wired signals to wireless signals for wireless coverage. See the following topology.



## 3.1.2 Configuring AP mode

TIP

Before you start, ensure that the upstream router has connected to the internet successfully.

**Step 1** Choose **Quick Setup**.

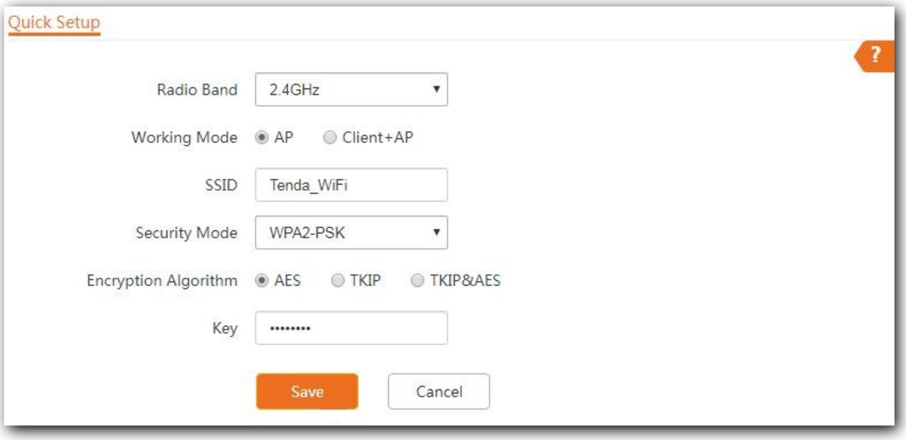
**Step 2** Select **2.4 GHz** from the **Radio Band** drop-down list menu.

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

**Step 4** Customize an **SSID** (wireless network name) in the **SSID** box, which is **Tenda_WiFi** in this example. This SSID is also your primary SSID on 2.4 GHz band.

**Step 5** Select the security mode from the **Security Mode** drop-down list menu, which is **WPA2-PSK** in this example.

**Step 6** Click **Save**.



Quick Setup

Radio Band: 2.4GHz

Working Mode: ● AP ○ Client+AP

SSID: Tenda_WiFi

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

**Step 7** If you need to set other wireless networks in another radio band, please select another wireless radio band and perform step 3 - 6 again.

**---- End**

After configuration, you can connect wireless devices such as smartphones to the WiFi network of your AP using the SSID and WiFi password you set.

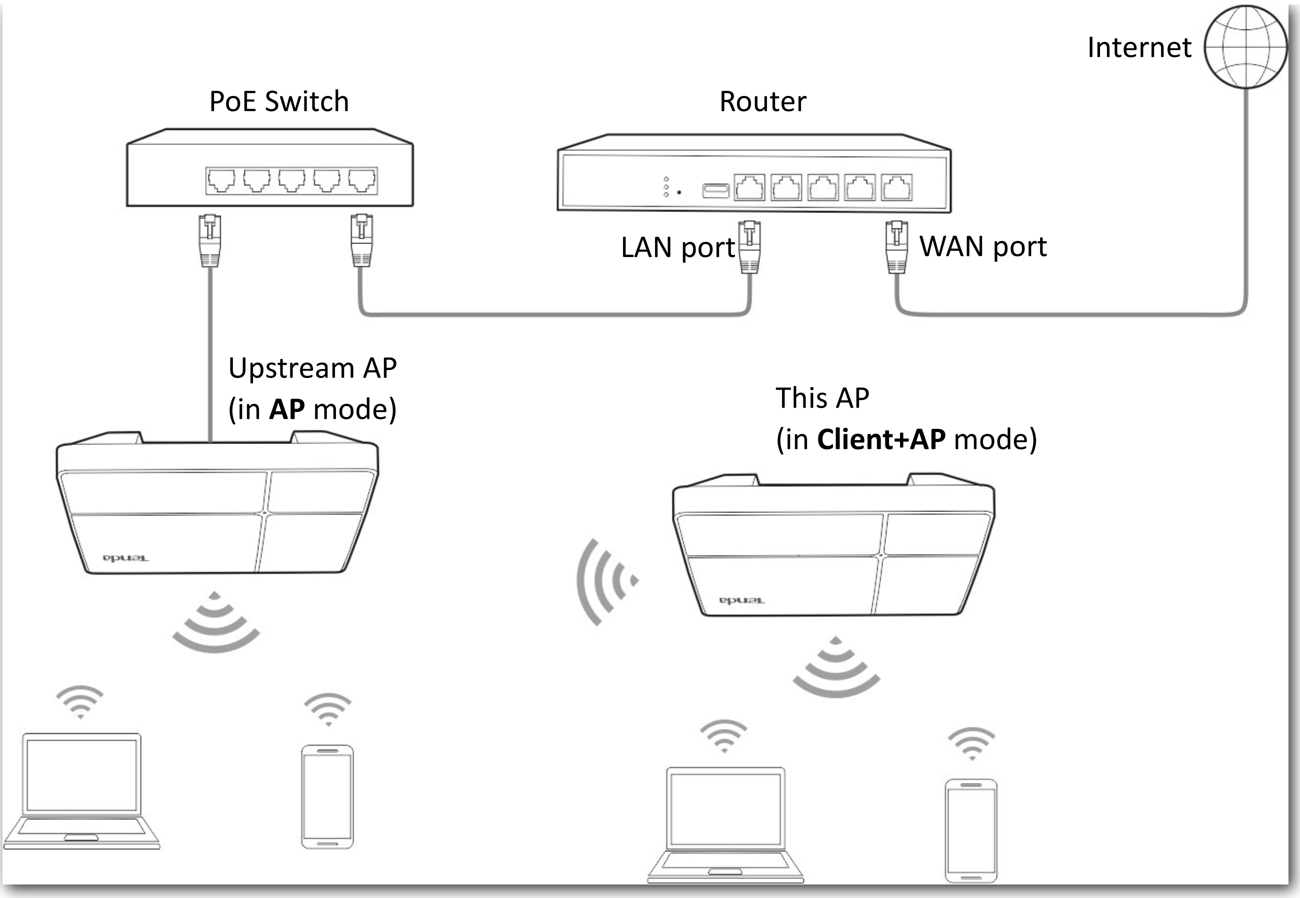
### Parameter description

| Parameter | Description |
|---|---|
| Radio Band | It is used to select the radio band for configurations. |
| Working Mode | Choose the AP mode to transform the wireless network to wireless network. |
| SSID | Click to modify the WiFi name of the primary network under the selected radio band. |
| Security Mode | Select the security modes for target wireless networks, including None, WEP, WPA-PSK, WPA2-PSK, WPA-PSK & WPA2-PSK, WPA and WPA2. |

## 3.2 Client+AP mode

### 3.2.1 Overview

In this mode, the AP extends the existing wireless network by bridging the upstream wireless signals (such as wireless router, AP). See the following topology.



## 3.2.2 Configuring Client+AP mode

TIP

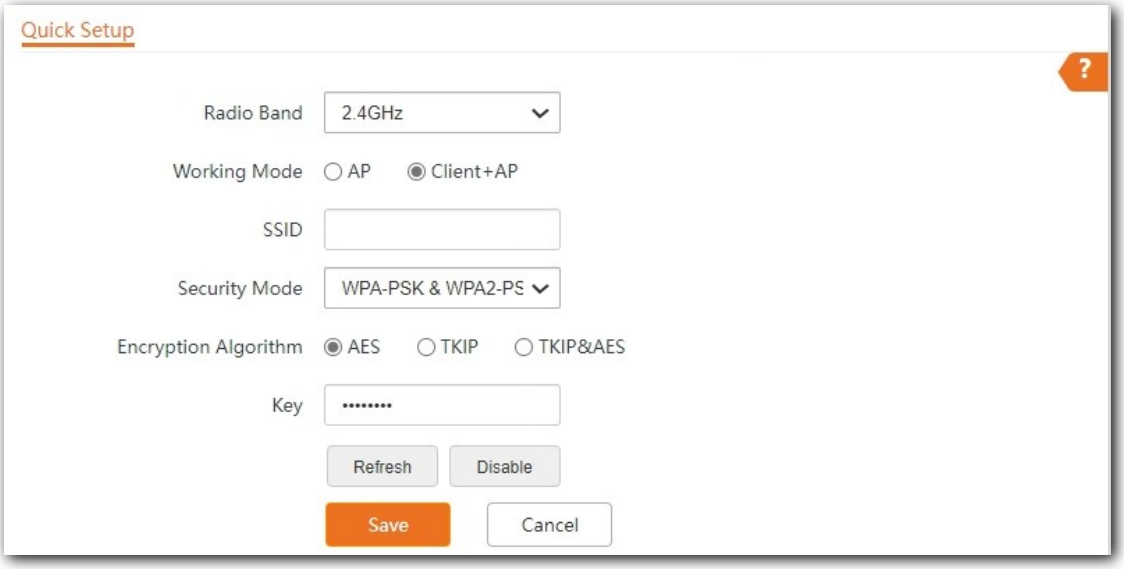
Before you start, ensure that the upstream AP has connected to the internet successfully.

**Step 1** Choose **Quick Setup**.

**Step 2** Select **2.4 GHz** from the **Radio Band** drop-down list menu.

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

**Step 4** Click **Scan**.



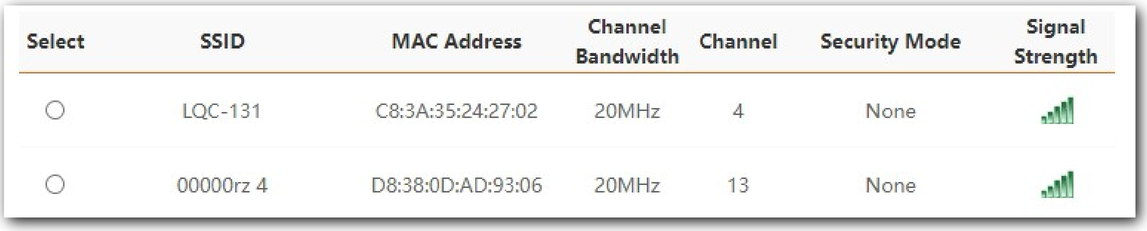
Quick Setup

| | |
|---|---|
| Radio Band | 2.4GHz |
| Working Mode | ○ AP ● Client+AP |
| SSID | |
| Security Mode | WPA-PSK & WPA2-PS |
| Encryption Algorithm | ● AES ○ TKIP ○ TKIP&AES |
| Key | •••••••• |

**Step 5** Select the WiFi network to extend.

TIP

- If the SSID is not displayed, choose **Wireless** > **RF Settings**, ensure that your upstream wireless network is enabled. If not, enable it. Then refresh the scan result.
- The device detects and auto-fills **SSID, Security Mode**.



| Select | SSID | MAC Address | Channel Bandwidth | Channel | Security Mode | Signal Strength |
|---|---|---|---|---|---|---|
| ○ | LQC-131 | C8:3A:35:24:27:02 | 20MHz | 4 | None | |
| ○ | 00000rz 4 | D8:38:0D:AD:93:06 | 20MHz | 13 | None | |

**Step 6** Click **Disable**.

**Step 7** Click **Save**.

---- End

After the configuration, devices connected to the AP can access the upstream wireless network after entering the wireless password (Key).

TIP

If you do not know the SSID and key of the AP, go to **Wireless Setting** > **SSID Settings** page.

### Parameter description

| Parameter | Description |
|---|---|
| Radio Band | It is used to select the radio band for configurations. |
| Working Mode | Choose the **Client+AP** mode to bridge the upstream WiFi network. |
| SSID | It specifies the WiFi network name (SSID) of the WiFi network to be bridged. 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.<br>The AP can support WiFi network encrypted with None or WEP (Open or Shared), WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK.<br>• If the wireless network to be bridged adopts the **WEP** security mode, **Authentication Type**, **Default Key**, and **Key x** (*x* ranges from 1 to 4) need to be entered manually.<br>• If the wireless network to be bridged adopts the **WPA-PSK**, **WPA2-PSK** or **WPA-PSK & WPA2-PSK** security mode, **Encryption Algorithm** will be populated automatically and you only need to enter the **Key**. |
| Refresh | Used to refresh the scan results. |
| Scan/Disable | • **Scan**: Used to scan nearby available wireless networks. The scan results are displayed on the lower page.<br>• **Disable**: The button only appears after you clicked **Scan**. It is used to end the scan operation and collapse the scan result. |

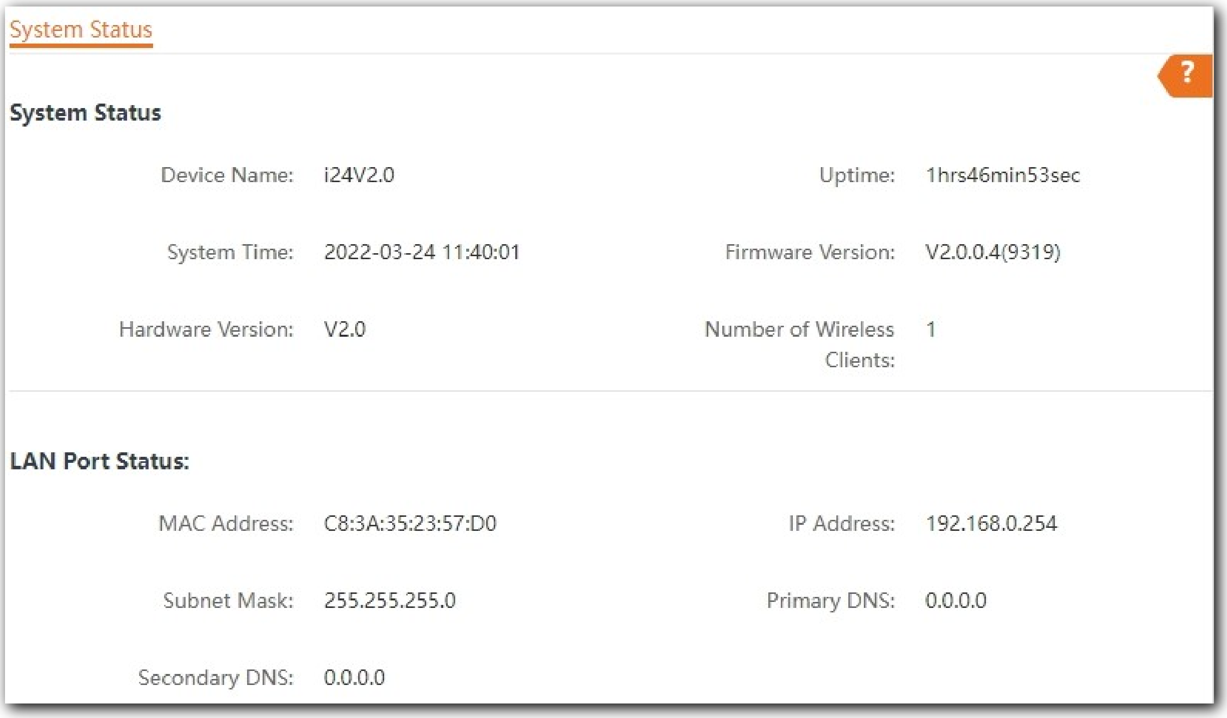
# 4 Status

This module presents you with the system information of the AP and wireless network status, including system status, wireless status, traffic statistics, and client list (information of wireless clients connected to the AP).

## 4.1 System status

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

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



System Status

Device Name: i24V2.0

Uptime: 1hrs46min53sec

System Time: 2022-03-24 11:40:01

Firmware Version: V2.0.0.4(9319)

Hardware Version: V2.0

Number of Wireless Clients: 1

LAN Port Status:

MAC Address: C8:3A:35:23:57:D0

IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

### Parameter description

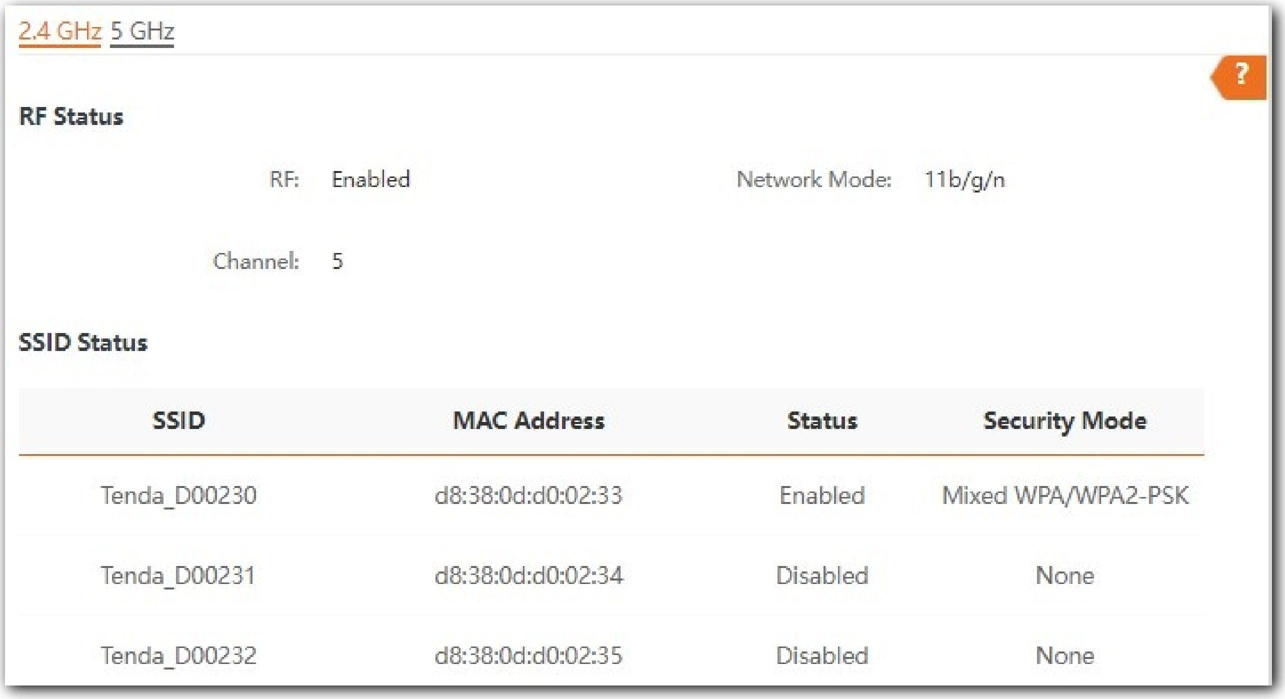
| Parameter | Description |
|---|---|
| Device Name | It specifies the name of the AP.<br>You can modify it on **LAN Setup** page. |
| Uptime | It specifies the time that has elapsed since the AP starts up last time. |
| System Time | It specifies the current system time of the AP. |
| Firmware Version | It specifies the current firmware version number of the AP. |

| Parameter | Description |
|---|---|
| Hardware Version | It specifies the current hardware version number of the AP. |
| Number of Wireless Clients | It specifies the quantity of wireless devices currently connected to the AP. |
| MAC Address | It specifies the physical address of the AP's LAN port. |
| IP Address | It specifies the IP address of the AP's LAN port, which can be used to log in to the web UI.<br>You can modify it on **LAN Setup** page. |
| Subnet Mask | It specifies the subnet mask of the AP. |
| Primary DNS | It specifies the primary DNS server of the AP. |
| Secondary DNS | It specifies the secondary DNS server of the AP. |

## 4.2 Wireless status

This page displays radio information and SSID information of the AP.

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



RF Status

RF: Enabled

Network Mode: 11b/g/n

Channel: 5

SSID Status

| SSID | MAC Address | Status | Security Mode |
|---|---|---|---|
| Tenda_D00230 | d8:38:0d:d0:02:33 | Enabled | Mixed WPA/WPA2-PSK |
| Tenda_D00231 | d8:38:0d:d0:02:34 | Disabled | None |
| Tenda_D00232 | d8:38:0d:d0:02:35 | Disabled | None |

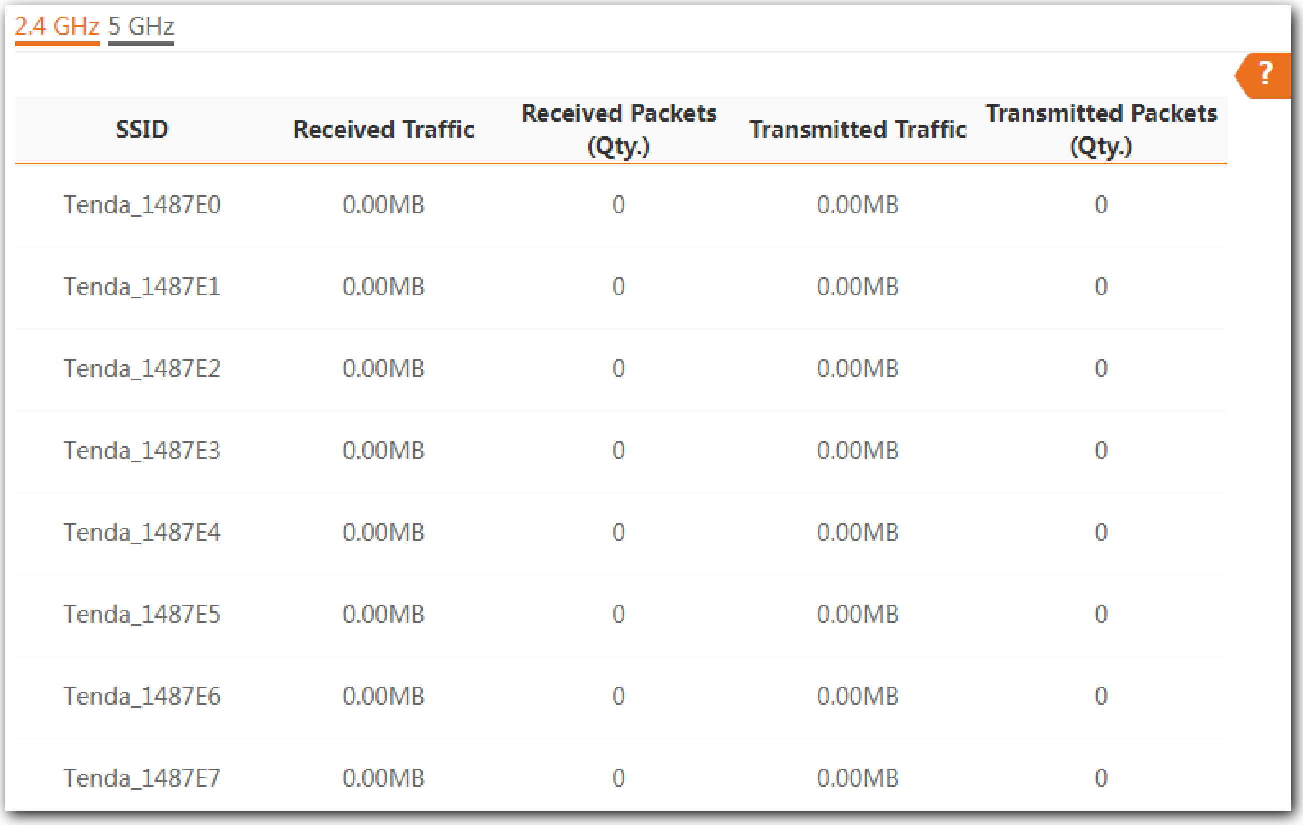
### Parameter description

| Parameter | | Description |
|---|---|---|
| RF Status | RF | It specifies whether the wireless function of the AP is enabled. |
| | Network Mode | It specifies the network mode currently enabled by the AP on each radio band. |
| | 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 address of the corresponding wireless network. |
| | Status | It specifies whether or not the corresponding WiFi network is enabled. |
| | Security Mode | It specifies the security modes of the wireless networks corresponding to the SSIDs of the AP. |

## 4.3 Traffic statistics

This page allows you to view statistical information about traffic based on SSIDs.

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

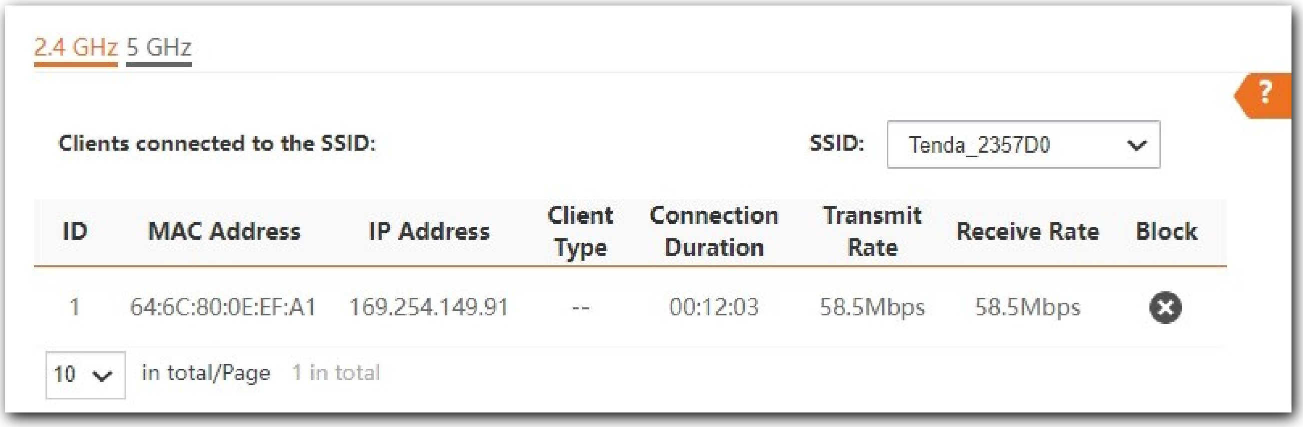


| SSID | Received Traffic | Received Packets (Qty.) | Transmitted Traffic | Transmitted Packets (Qty.) |
|---|---|---|---|---|
| Tenda_1487E0 | 0.00MB | 0 | 0.00MB | 0 |
| Tenda_1487E1 | 0.00MB | 0 | 0.00MB | 0 |
| Tenda_1487E2 | 0.00MB | 0 | 0.00MB | 0 |
| Tenda_1487E3 | 0.00MB | 0 | 0.00MB | 0 |
| Tenda_1487E4 | 0.00MB | 0 | 0.00MB | 0 |
| Tenda_1487E5 | 0.00MB | 0 | 0.00MB | 0 |
| Tenda_1487E6 | 0.00MB | 0 | 0.00MB | 0 |
| Tenda_1487E7 | 0.00MB | 0 | 0.00MB | 0 |

## 4.4 Client list

This page allows you to view wireless clients connected to each SSID of the AP and their basic information, and to block unknown wireless clients.

To access the page, choose **Status** > **Client List**.



Clients connected to the SSID: SSID: Tenda_2357D0

| ID | MAC Address | IP Address | Client Type | Connection Duration | Transmit Rate | Receive Rate | Block |
|---|---|---|---|---|---|---|---|
| 1 | 64:6C:80:0E:EF:A1 | 169.254.149.91 | -- | 00:12:03 | 58.5Mbps | 58.5Mbps | ⊗ |

10 in total/Page 1 in total

### Parameter description

| Parameter | Description |
|---|---|
| SSID | Select the SSID from the drop-down list menu to view client information connected to it. |
| MAC Address | It specifies the physical address of the wireless client. |
| IP Address | It specifies the IP address of the wireless client. |
| Client Type | It specifies the operating system of the wireless client. |
| Connection Duration | It specifies the online time of the wireless client. |
| Transmit Rate | It specifies the real time traffic the client has transmitted. |
| Receive Rate | It specifies the real time traffic the client has received. |
| Block | Click ⊗ to block the client from accessing the AP's wireless network.<br>To unblock a client, navigate to **Wireless** > Access Control. |

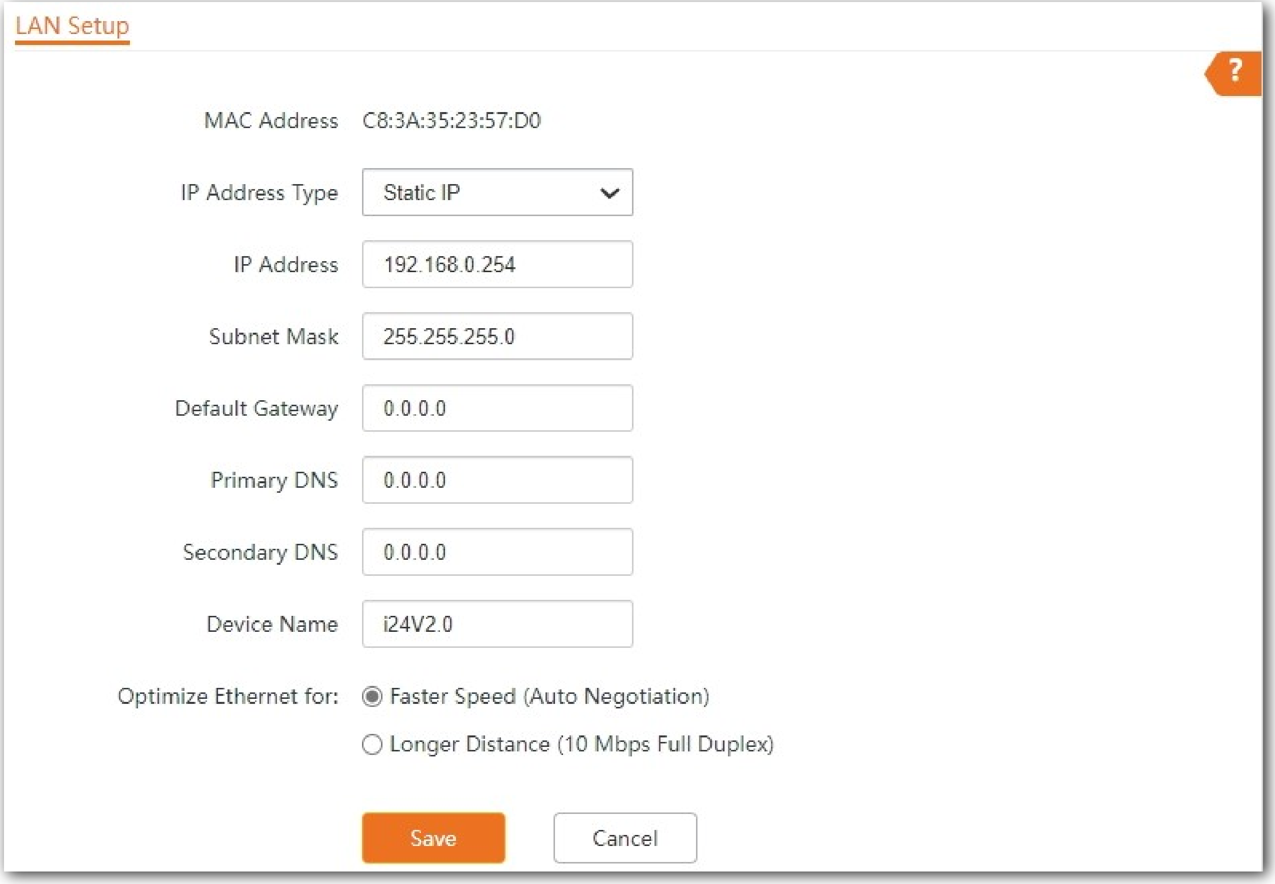
# 5 Internet settings

## 5.1 LAN setup

### 5.1.1 Overview

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

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



LAN Setup

| | |
|---|---|
| MAC Address | C8:3A:35:23:57:D0 |
| IP Address Type | Static IP |
| IP Address | 192.168.0.254 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 0.0.0.0 |
| Primary DNS | 0.0.0.0 |
| Secondary DNS | 0.0.0.0 |
| Device Name | i24V2.0 |
| Optimize Ethernet for: | ● Faster Speed (Auto Negotiation)<br>○ Longer Distance (10 Mbps Full Duplex) |

### Parameter description

| Parameter | Description |
|---|---|
| MAC Address | It specifies the MAC address of the AP's LAN port. |
| IP Address Type | It specifies IP address obtaining method of the AP.<br>• **Static IP (default)**: You are required to set related parameters manually.<br>• **DHCP (Dynamic IP Address)**: The AP automatically obtains related parameters from a DHCP server on your LAN network.<br>TIP<br>After setting the IP address obtaining method to **DHCP (Dynamic IP Address)**, before logging in to the web UI of the AP next time, check the IP address obtained by the AP in the client list of the DHCP server in the network first, then use the IP address to log in. |
| IP Address | It specifies the LAN IP address (also the login IP address) of the AP. Default: **192.168.0.254**. |
| Subnet Mask | It specifies the subnet mask of the AP. Default: **255.255.255.0**. |
| Default Gateway | It specifies the gateway IP address of the AP.<br>Generally, enter the LAN IP address of the router which has internet accessibility into this box. |
| Primary DNS | It specifies the IP address of the primary DNS server of the AP.<br>If DNS proxy function is supported on your router connected to the internet, you can set the IP address of the primary DNS server to the LAN IP address of your router. Otherwise, enter a correct DNS server IP address. |
| Secondary DNS | It specifies the IP address of the secondary DNS server of the AP. This parameter is optional. |
| Device Name | It specifies the name of the AP.<br>You are recommended to change the name of the AP to indicate the location of the AP (such as Living Room), so that you can easily identify the AP when managing many APs. |
| Optimize Ethernet for | It specifies the Ethernet mode of the PoE Ethernet port of the AP.<br>• **Faster Speed (Auto Negotiation)**: This option features a high data rate but short transmission distance. Generally, we recommend you select this option.<br>• **Longer Distance (10 Mbps Half Duplex)**: This option features long transmission distance but low data rate. Generally, the negotiated speed is 10 Mbps.<br>If the Ethernet cable connecting the Ethernet port of the AP to the peer device is longer than 100 meters, the **Longer Distance (10 Mbps Half Duplex)** mode is recommended. In this case, ensure that the peer device adopts auto negotiation option. |

## 5.1.2 Modify LAN IP

### Static IP address

The IP address, subnet mask, default gateway, and primary/secondary DNS server of the AP are manually specified by the network administrator, which is suitable for the occasions where only one or few APs are deployed in the network.

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

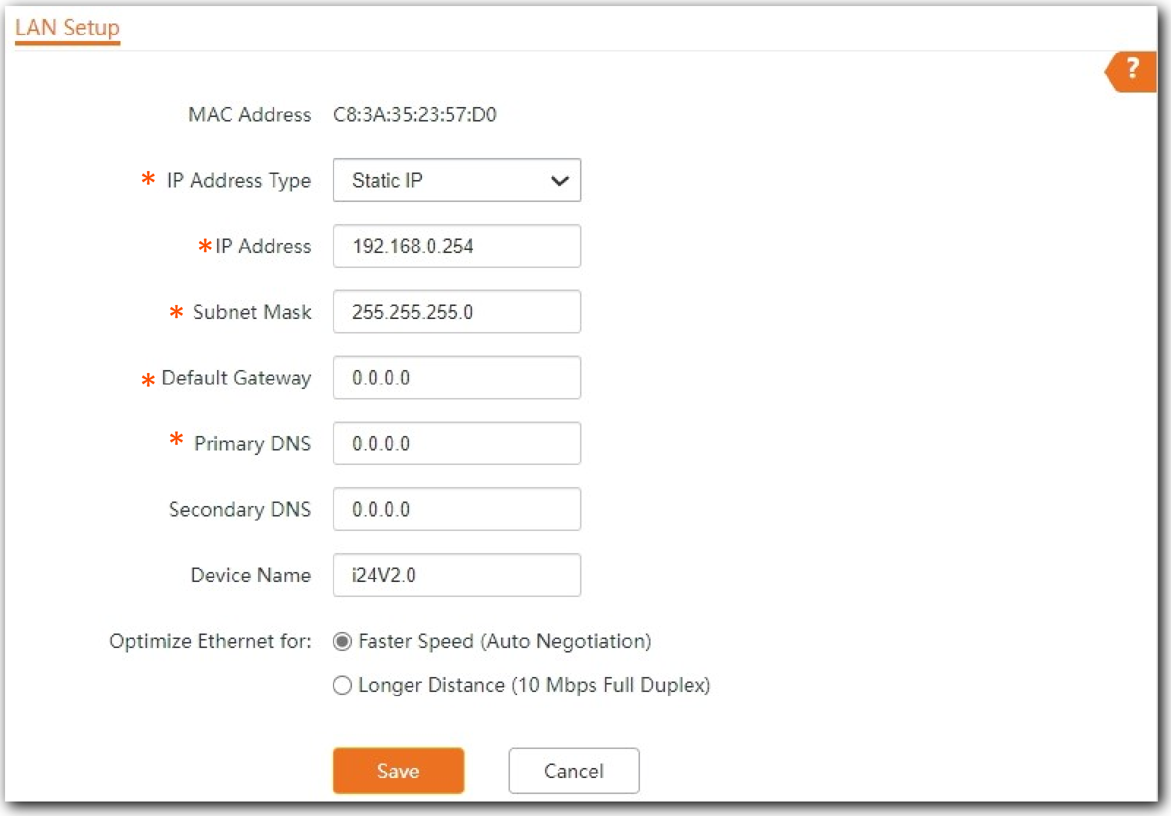
**Step 2** Select **Static IP** from the **IP Address Type** drop-down list menu.

**Step 3** Set **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS** and **Secondary DNS**.

NOTE

Ensure that the modified IP address is not occupied by other devices in the LAN.

**Step 4** Click **Save** to apply your settings.



LAN Setup

| | |
|---|---|
| MAC Address | C8:3A:35:23:57:D0 |
| * IP Address Type | Static IP |
| *IP Address | 192.168.0.254 |
| * Subnet Mask | 255.255.255.0 |
| * Default Gateway | 0.0.0.0 |
| * Primary DNS | 0.0.0.0 |
| Secondary DNS | 0.0.0.0 |
| Device Name | i24V2.0 |
| Optimize Ethernet for: | ● Faster Speed (Auto Negotiation)<br>○ Longer Distance (10 Mbps Full Duplex) |

---- End

If you want to continue setting up the AP, please follow the instructions below:

- After the configuration, if the new IP address of the AP belongs to the same network segment as the IP address of your management computer, you can log in to the web UI of the AP directly using the new IP address.
- Otherwise, before logging in to the AP's web UI using the new IP address, assign your computer an IP address that belongs to the same network segment as the new IP address.

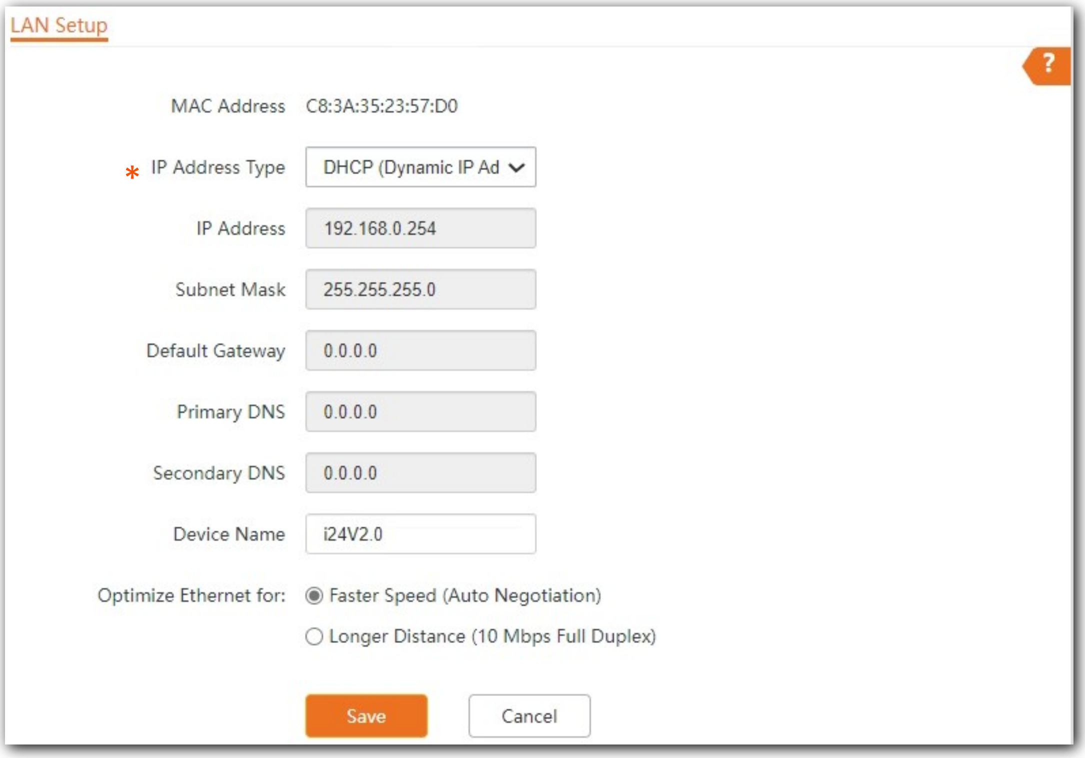
## Obtain IP address automatically

The AP automatically obtains the IP address, subnet mask, default gateway, primary/secondary DNS from the DHCP server in the network. If multiple APs need to be deployed in the network, this method can avoid IP address conflicts and effectively reduce the workload of network administrators.

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

**Step 2** Select **DHCP (Dynamic IP Address)** from the **IP Address Type** drop-down list menu.

**Step 3** Click **Save** to apply your settings.



LAN Setup

| | |
|---|---|
| MAC Address | C8:3A:35:23:57:D0 |
| * IP Address Type | DHCP (Dynamic IP Ad |
| IP Address | 192.168.0.254 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 0.0.0.0 |
| Primary DNS | 0.0.0.0 |
| Secondary DNS | 0.0.0.0 |
| Device Name | i24V2.0 |
| Optimize Ethernet for: | ● Faster Speed (Auto Negotiation)<br>○ Longer Distance (10 Mbps Full Duplex) |

**---- End**

To view the new IP address of the AP, go to the upstream DHCP client list. Modify the IP address of the management computer so that it is in the same network segment as the new IP address of the AP. Then access the new IP address of the AP to log in.

# 5.2 DHCP server

## 5.2.1 Overview

The AP supports the DHCP server function to assign IP addresses to devices connected to it. By default, this function is disabled.

TIP

If the new and original IP addresses of the LAN port belong to different network segments, 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.

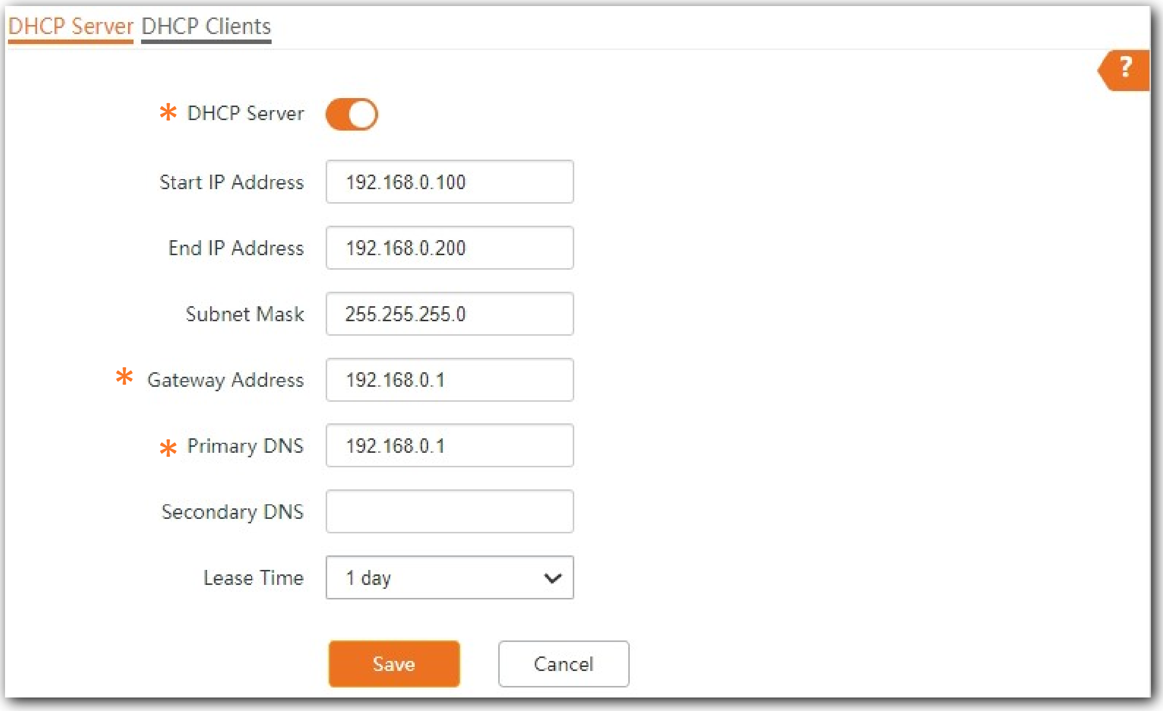
## 5.2.2 Configuring DHCP server of the AP

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

**Step 2** Enable **DHCP Server** function.

**Step 3** Customize required parameters. (Generally, you only need to modify **Gateway Address**, **Primary DNS**)

**Step 4** Click **Save**.



|  |  |
|---|---|
| * DHCP Server | ● |
| Start IP Address | 192.168.0.100 |
| End IP Address | 192.168.0.200 |
| Subnet Mask | 255.255.255.0 |
| * Gateway Address | 192.168.0.1 |
| * Primary DNS | 192.168.0.1 |
| Secondary DNS |  |
| Lease Time | 1 day |

---- End

NOTE

If another DHCP server is available in 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.

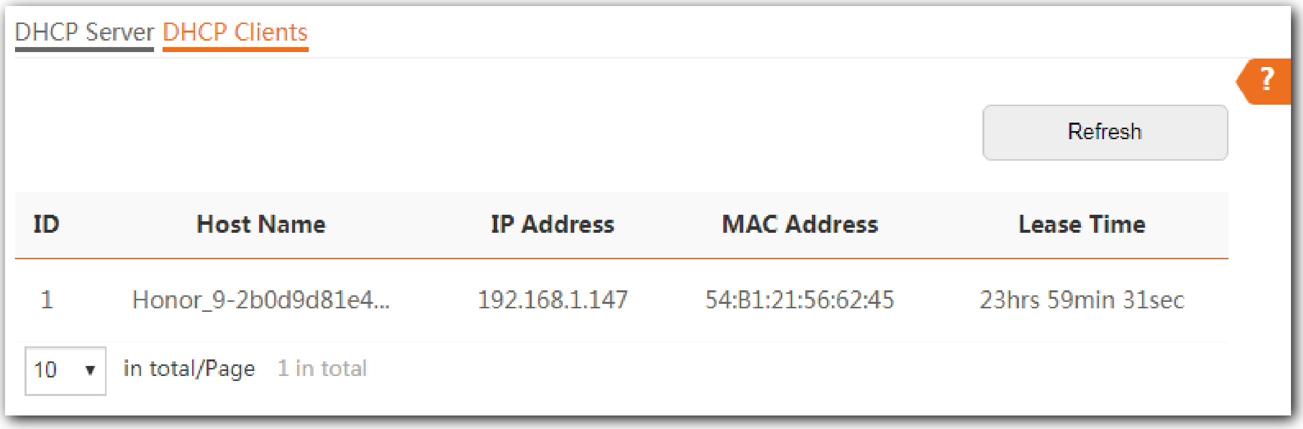
### Parameter description

| 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 DHCP server's IP address pool. The default value is **192.168.0.100**. |
| End IP Address | It specifies the end IP address of the DHCP server's IP address pool. The default value is **192.168.0.200**.<br>TIP<br>The **Start IP address** and **End IP address** must be in the same network segment as the AP's IP address. |
| Subnet Mask | It specifies the subnet mask assigned by the DHCP server to devices. The default value is **255.255.255.0**. |
| Gateway Address | It specifies the gateway IP address assigned by the DHCP server to devices. Generally, it is the LAN IP address of the router connected to the internet. The default value is **192.168.0.1**.<br>TIP<br>When clients access servers or hosts beyond the current network segment, the data must be forwarded by the gateway. |
| Primary DNS | It specifies the IP address of the primary DNS server assigned by the DHCP server to devices.<br>TIP<br>To enable devices to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address. |
| Secondary DNS | It specifies the IP address of the secondary DNS server assigned by the DHCP server to devices. This parameter is optional, which indicates you can leave it blank if your ISP does not provide this parameter. |
| Lease Time | It specifies the validity period of an IP address assigned by the DHCP server to a device.<br>When half of the lease time has elapsed, the device sends a DHCP request to the DHCP server to renew the lease time. If the request succeeds, the lease time is extended based on the request. Otherwise, the device sends a request again when 7/8 of the lease time has elapsed. If the request succeeds, the lease time is extended based on the request. Otherwise, the device must request a new IP address from the DHCP server after the lease time expires.<br>It is recommended to retain the default value (**1 day**). |

### 5.2.3 Viewing DHCP clients

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, and so on.

To access the page, choose **Internet Settings** > **DHCP Server** and click **DHCP Clients** tab.



| ID | Host Name | IP Address | MAC Address | Lease Time |
|---|---|---|---|---|
| 1 | Honor_9-2b0d9d81e4... | 192.168.1.147 | 54:B1:21:56:62:45 | 23hrs 59min 31sec |

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

# 6 Wireless

## 6.1 SSID

### 6.1.1 Overview

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

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

#### Broadcast SSID

After enabling broadcast SSID, nearby wireless clients can detect the corresponding SSID. After disabling the broadcast SSID, the AP cannot broadcast the SSID, and the nearby wireless clients cannot detect the corresponding SSID. At this time, if you want to access the wireless network of the SSID, you need to enter the SSID manually on the wireless client, which enhances the security of the wireless network to a certain extent.

It should be noted that after disabling broadcast SSID, if hackers obtain the SSID by other means, they can still access the target network.

#### Isolate Client

This parameter implements a function similar to the VLAN function for wired networks. It isolates the wireless devices connected to the same WiFi network, so that the wireless devices can access only the wired network connected to the AP. You can apply this function to hotspot setup in public spaces, such as hotels and airports to keep wireless users isolated and improve network security.

#### Isolate SSID

After enabling, wireless clients connected to different SSIDs cannot communicate with each other, which can enhance the security of the wireless network.

#### Max. Number of Clients

This parameter specifies the maximum number of devices that can connect to the WiFi network corresponding to an SSID. If the number is reached, the WiFi network rejects new connection requests from devices.

Setting the maximum number of clients can avoid the situation that some SSIDs on the AP are overloaded and cause poor user experience, while other SSIDs have idle bandwidth.

## Security Mode

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

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 device can connect to the WiFi network. This option is not recommended because it leads to network insecurity.

- **WEP**

It uses a static key to encrypt all exchanged data, and ensures that a WLAN has the same level of security as a wired LAN. However, data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum WiFi 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 WPA-PSK & WPA2-PSK supports both WPA-PSK and WPA2-PSK.

WPA-PSK, WPA2-PSK, and WPA-PSK & 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 WiFi networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all devices 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 devices 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 devices and the login information of a device is managed by the device. This effectively reduces the probability of information leakage. In addition, each time a device 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 device, which makes it difficult for attackers to obtain the key. These features of WPA and WPA2 security modes help increase network security significantly, making WPA and WPA2 the preferred security modes of WiFi networks that require high security.

## 6.1.2 Modifying SSID-related parameters

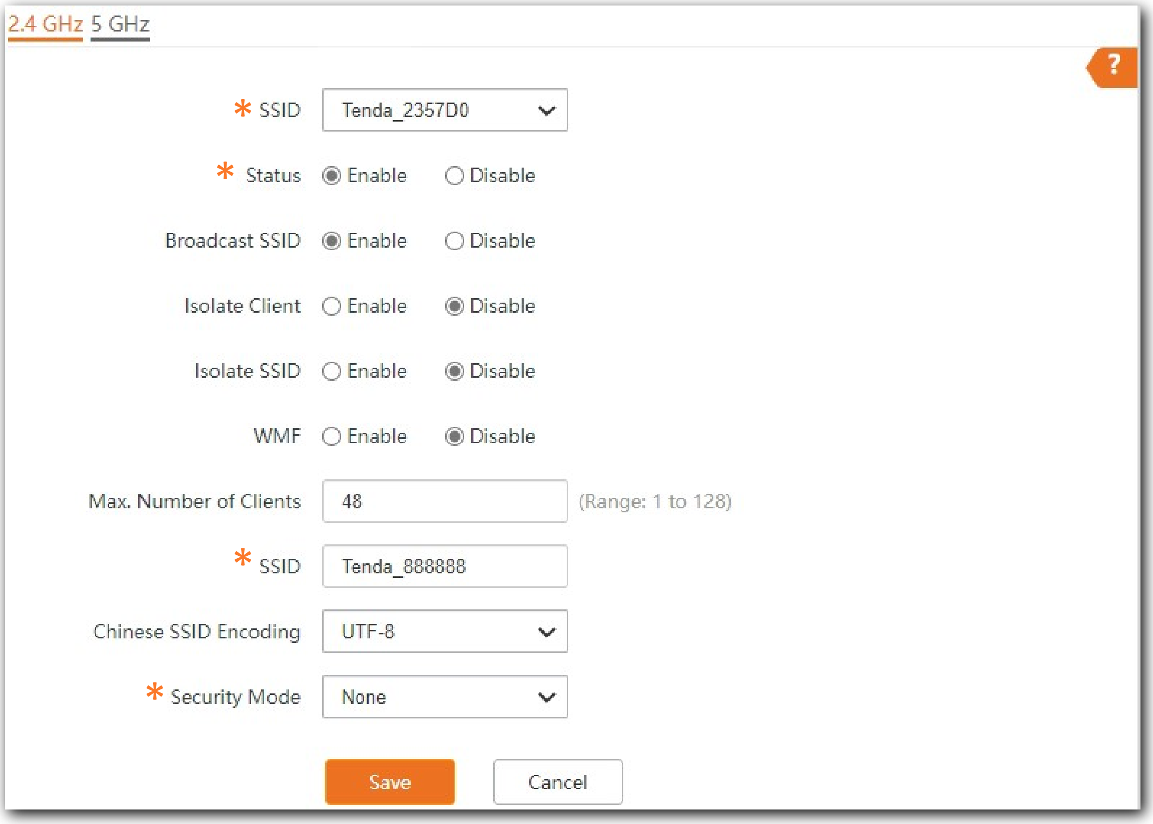
**Step 1** Choose **Wireless** > **SSID**.

**Step 2** Click the tab of the radio band where the SSID to be modified is located.

**Step 3** Select the SSID from the **SSID** drop-down list menu.

**Step 4** Customize the parameters as required (Generally you only need to modify **Status**, **SSID** and security-related parameters).

**Step 5** Click **Save** to apply your settings.



| | | |
|---|---|---|
| * SSID | Tenda_2357D0 | |
| * Status | ● Enable | ○ Disable |
| Broadcast SSID | ● Enable | ○ Disable |
| Isolate Client | ○ Enable | ● Disable |
| Isolate SSID | ○ Enable | ● Disable |
| WMF | ○ Enable | ● Disable |
| Max. Number of Clients | 48 | (Range: 1 to 128) |
| * SSID | Tenda_888888 | |
| Chinese SSID Encoding | UTF-8 | |
| * Security Mode | None | |

---- End

**Parameter description**

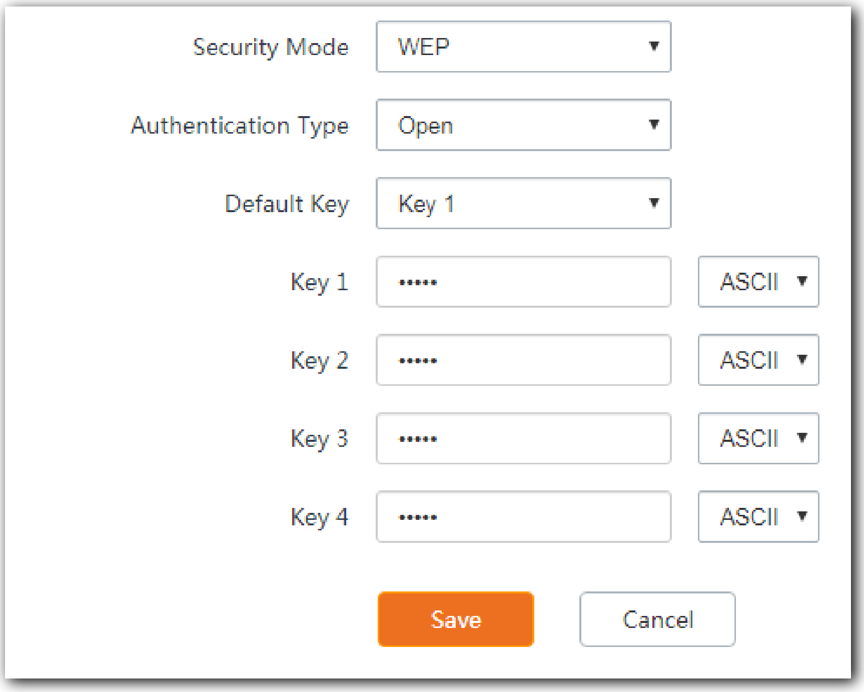
| Parameter | Description |
|---|---|
| SSID | It specifies the SSID to be configured.<br>The AP supports 8 SSIDs for the 2.4 GHz radio band and 4 SSIDs for the 5 GHz radio band. On each band, the first displayed SSID is the primary SSID. |
| Status | It specifies the status of the selected SSID.<br>The primary SSID is enabled by default and you can enable other SSIDs manually. |

| Parameter | Description |
|---|---|
| Broadcast SSID | The broadcast status of the SSID you selected.<br>- **Enable**: AP is broadcasting SSID. Nearby wireless clients can detect the SSID. By default, this function is **Enable**.<br>- **Disable**: AP stops broadcasting SSID. Nearby wireless clients cannot detect the SSID, and you need to enter the SSID manually on the wireless client to access the wireless network. |
| Isolate Client | - **Enable**: The devices connected under the selected SSID cannot communicate with each other, which can enhance the security of the wireless network.<br>- **Disable**: The devices connected under the selected SSID can communicate with each other. By default, this function is **Disable**. |
| Isolate SSID | - **Enable**: Devices under different SSIDs cannot communicate with each other.<br>- **Disable**: Devices under different SSIDs can communicate with each other. By default, this function is **Disable**. |
| WMF | - **Enable**: Converts multicast traffic into unicast traffic and forwards the traffic to the multicast traffic destination in the WiFi network, helping save wireless resources, ensuring reliable transmission, and reducing delays.<br>- **Disable**: Converts multicast traffic into unicast traffic and forwards the traffic to all the users. By default, this function is **Disable.** |
| Max. Number of Clients | This parameter specifies the maximum number of devices that can connect to the WiFi network corresponding to an SSID.<br>If the number is reached, the WiFi network rejects new connection requests from devices. This limit helps balance load among SSIDs. |
| SSID | Click this field to modify the selected SSID (the name of the wireless network). |
| Chinese SSID Encoding | It specifies the character encoding format. The default value is **UTF-8**.<br>If you want to configure multiple Chinese SSIDs for the AP, you are recommended to select the UTF-8 encoding format for some SSIDs and the GB2312 encoding format for other SSIDs so as to ensure compatibility for different wireless clients. |
| Security Mode | It specifies the security modes supported by the AP, including: NONE, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA and WPA2. |

### ■ None

It indicates that any wireless device can connect to the WiFi network. This option is not recommended because it leads to network insecurity.

## WEP



Security Mode: WEP

Authentication Type: Open

Default Key: Key 1

Key 1: ••••• ASCII

Key 2: ••••• ASCII

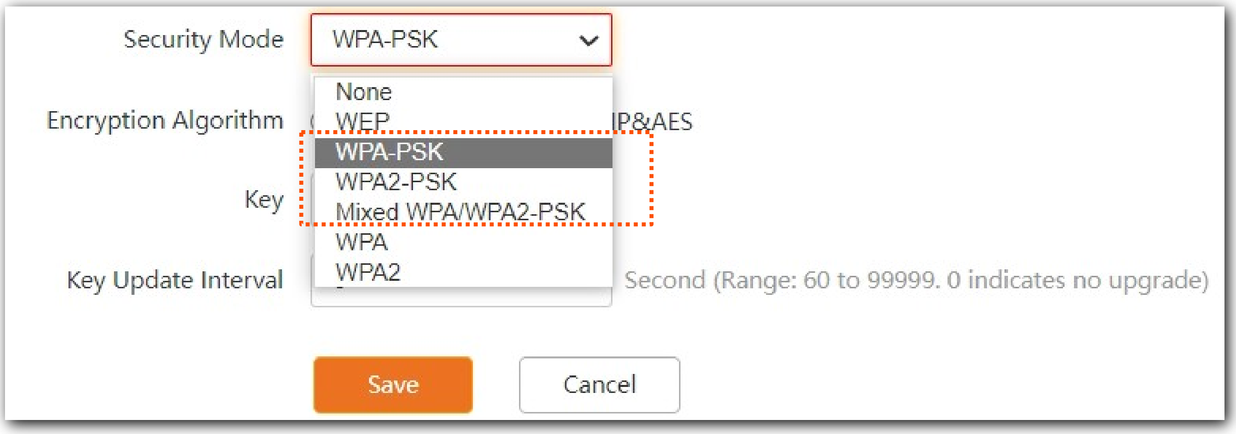
Key 3: ••••• ASCII

Key 4: ••••• ASCII

### Parameter description

| Parameter | Description |
|---|---|
| Authentication Type | It specifies the authentication type for the WEP security mode. The options include **Open** and **Shared**. The options share the same encryption process.<br>- **Open**: It specifies that authentication is not required and data exchanged is encrypted with 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.<br>- **Shared**: It specifies that a shared key is used for authentication and data exchanged is encrypted with 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. |
| Default Key | It specifies the WEP key for the **Open** or **Shared** encryption type.<br>For example, if **Default Key** is set to **Key 2**, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Key 2. |
| Key 1/2/3/4 | Enter one to four WEP keys. Only the key that is designated as the **Default Key** is effective. The character of the key consists of two types.<br>- ASCII: Enter 5 or 13 ASCII printable characters.<br>- Hex: Enter 10 or 26 hexadecimal characters (0-9, a-f, A-F). |

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



Security Mode: WPA-PSK

Encryption Algorithm: IP&AES

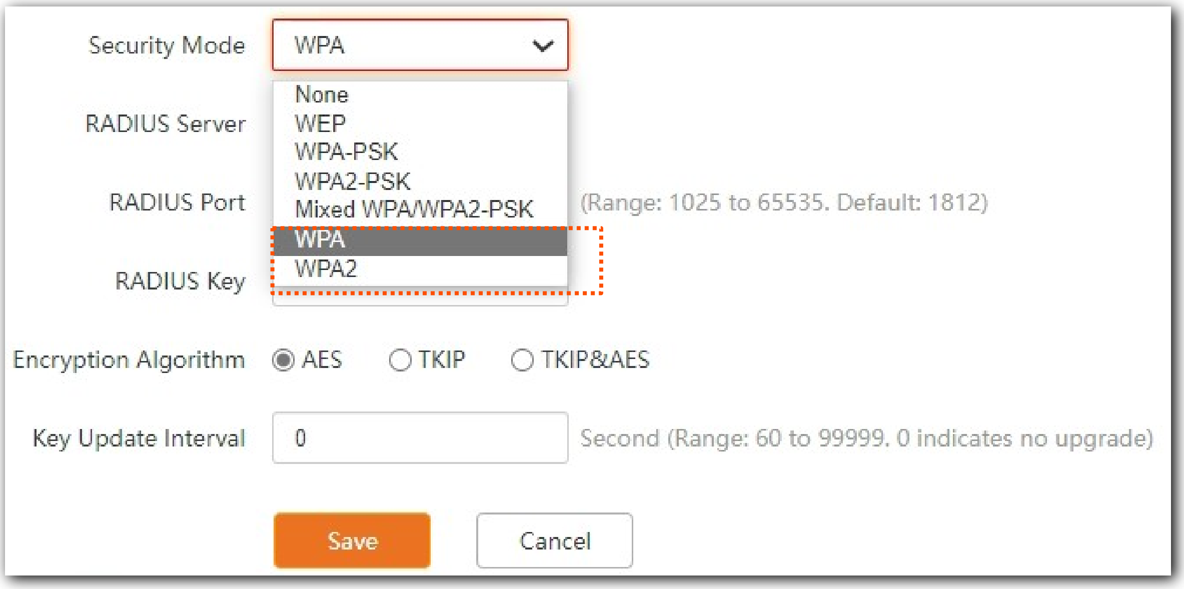
Key

Key Update Interval: Second (Range: 60 to 99999. 0 indicates no upgrade)

## Parameter description

| Parameter | Description |
|---|---|
| Security Mode | Select security mode.<br>• WPA-PSK: The wireless network adopts the WPA-PSK security mode, which has better compatibility.<br>• WPA2-PSK: The wireless network adopts the WPA2-PSK security mode, which has a higher security level.<br>• Mixed WPA/WPA2-PSK: Compatible with WPA-PSK and WPA2-PSK. At this time, wireless devices can connect to the corresponding wireless network using both WPA-PSK and 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.<br>• **AES**: It indicates the Advanced Encryption Standard.<br>• **TKIP**: It indicates the Temporal Key Integrity Protocol. If **TKIP** is used, the maximum wireless throughput of the AP is limited to 54 Mbps.<br>• **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, that is, the password clients use to connect to the wireless network. |
| Key Update Interval | It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.<br>The value **0** indicates that a WPA key is not updated. |

### WPA and WPA2



Security Mode: WPA

None
WEP
WPA-PSK
WPA2-PSK
Mixed WPA/WPA2-PSK
WPA
WPA2

RADIUS Server

RADIUS Port (Range: 1025 to 65535. Default: 1812)

RADIUS Key

Encryption Algorithm ● AES ○ TKIP ○ TKIP&AES

Key Update Interval: 0 Second (Range: 60 to 99999. 0 indicates no upgrade)

## Parameter description

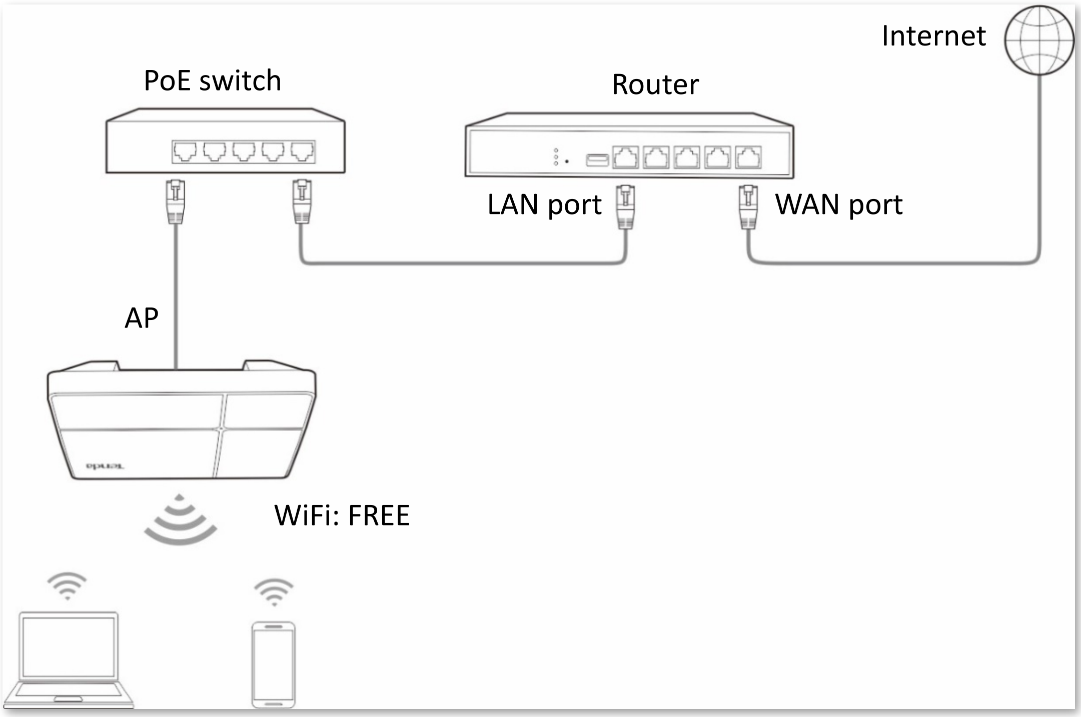
| Parameter | Description |
|---|---|
| Security Mode | Select security mode.<br>• WPA: The wireless network adopts the WPA enterprise security mode.<br>• WPA2: The wireless network adopts the WPA2 enterprise security mode. |
| RADIUS Server | It specifies the IP address of the RADIUS server for client authentication. |
| RADIUS Port | It specifies the port number of the RADIUS server for client authentication. |
| RADIUS Key | It specifies the shared key of the RADIUS server. |
| Encryption Algorithm | It specifies the encryption algorithm corresponding to the selected security mode.<br>• **AES**: It indicates the Advanced Encryption Standard.<br>• **TKIP**: It indicates the Temporal Key Integrity Protocol.<br>• **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.<br>The value **0** indicates that a WPA key is not updated. |

### 6.1.3 Example of SSID configurations

#### Example of setting up an open 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 2.4 GHz radio band of the AP is to be configured.

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

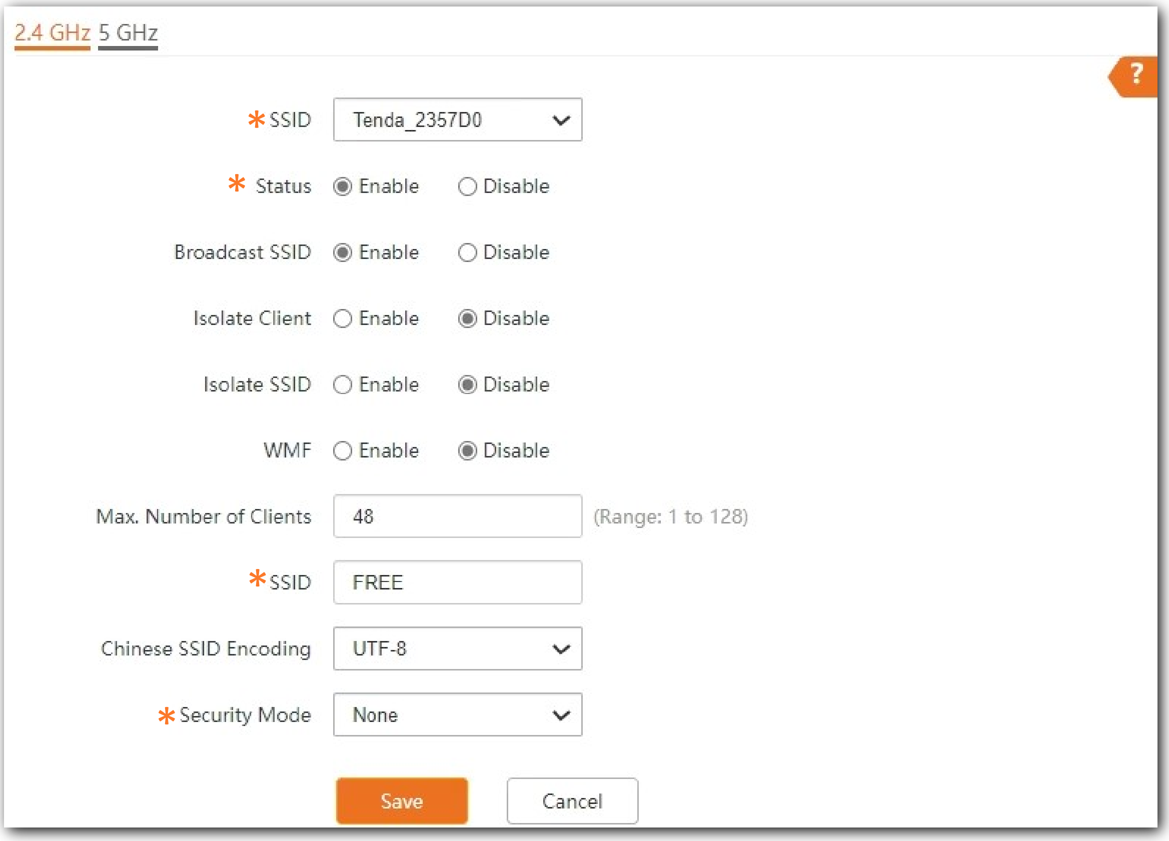
Step 2 Select the second SSID from the **SSID** drop-down list menu.

Step 3 Set **Status** to **Enable**.

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

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

Step 6 Click **Save**.



| | |
|---|---|
| *SSID | Tenda_2357D0 |
| * Status | ● Enable ○ Disable |
| Broadcast SSID | ● Enable ○ Disable |
| Isolate Client | ○ Enable ● Disable |
| Isolate SSID | ○ Enable ● Disable |
| WMF | ○ Enable ● Disable |
| Max. Number of Clients | 48 (Range: 1 to 128) |
| *SSID | FREE |
| Chinese SSID Encoding | UTF-8 |
| *Security Mode | None |

---- End

## Verification

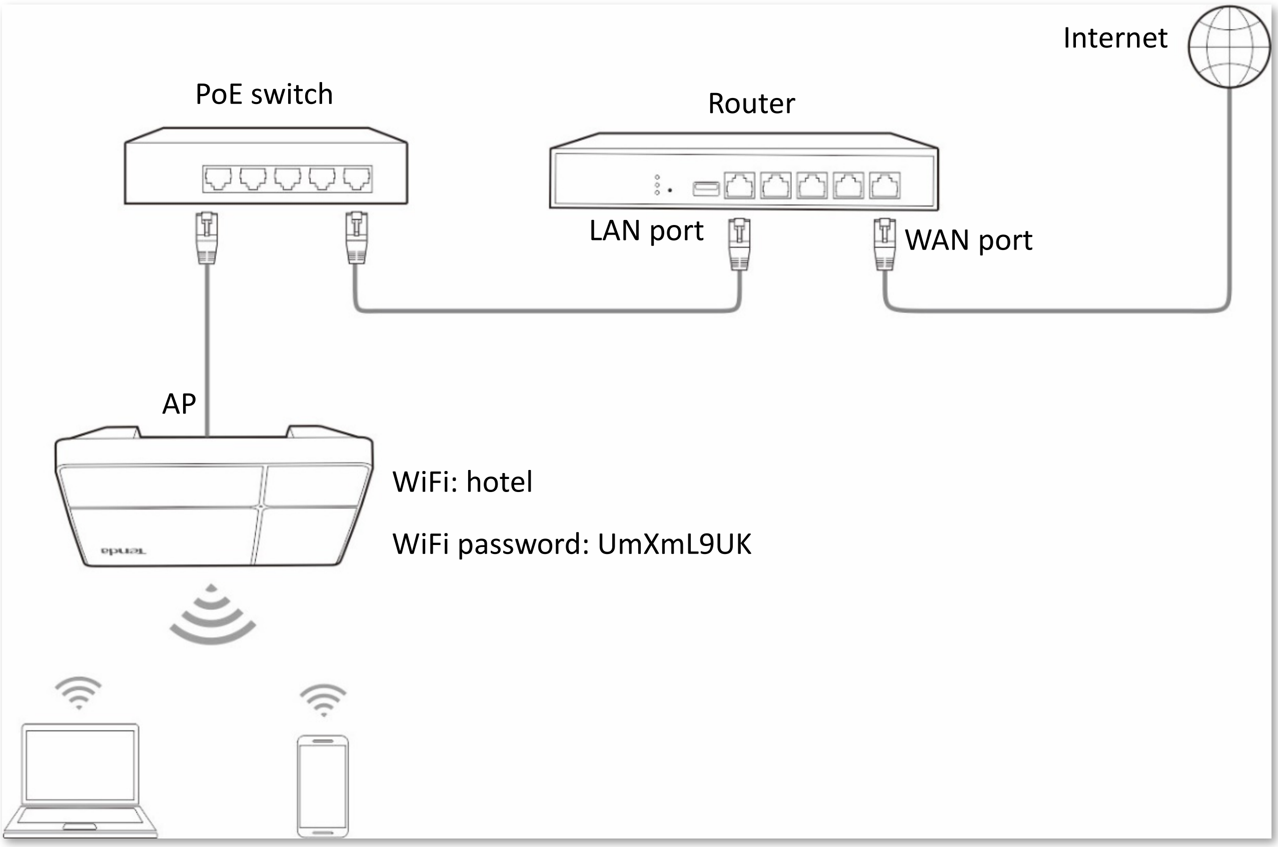
Wireless devices can connect to the **FREE** wireless network without a password.

## Example of setting up a wireless network encrypted with PSK

### Networking requirement

A hotel wireless network with a certain level of security must be set up through a simply procedure. In this case, WPA, WPA2-PSK or WPA-PSK & WPA2-PSK security mode is recommended.

Assume that the SSID is **hotel**, the Wifi password is **UmXmL9UK**. See the following figure.



## Configuration procedure

Assume that the second SSID of the 2.4 GHz radio band of the AP is to be configured.

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

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

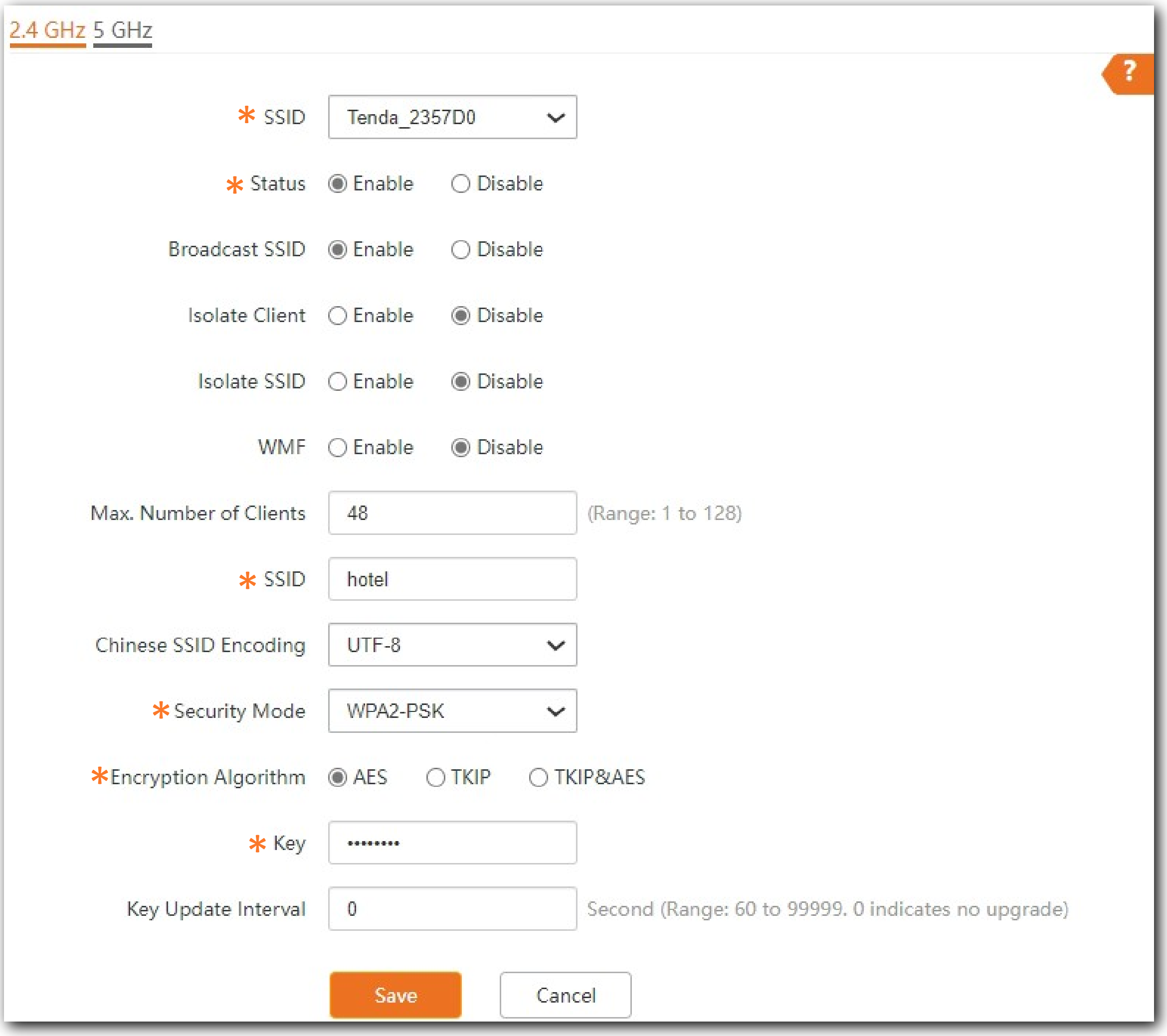
**Step 3** Set **Status** to **Enable**.

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

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

**Step 6** Set **Key** to **UmXmL9UK**.

**Step 7** Click **Save**.



| | |
|---|---|
| * SSID | Tenda_2357D0 |
| * Status | ● Enable ○ Disable |
| Broadcast SSID | ● Enable ○ Disable |
| Isolate Client | ○ Enable ● Disable |
| Isolate SSID | ○ Enable ● Disable |
| WMF | ○ Enable ● Disable |
| Max. Number of Clients | 48 (Range: 1 to 128) |
| * SSID | hotel |
| Chinese SSID Encoding | UTF-8 |
| * Security Mode | WPA2-PSK |
| *Encryption Algorithm | ● AES ○ TKIP ○ TKIP&AES |
| * Key | •••••••• |
| Key Update Interval | 0 Second (Range: 60 to 99999. 0 indicates no upgrade) |

---- End

## Verification

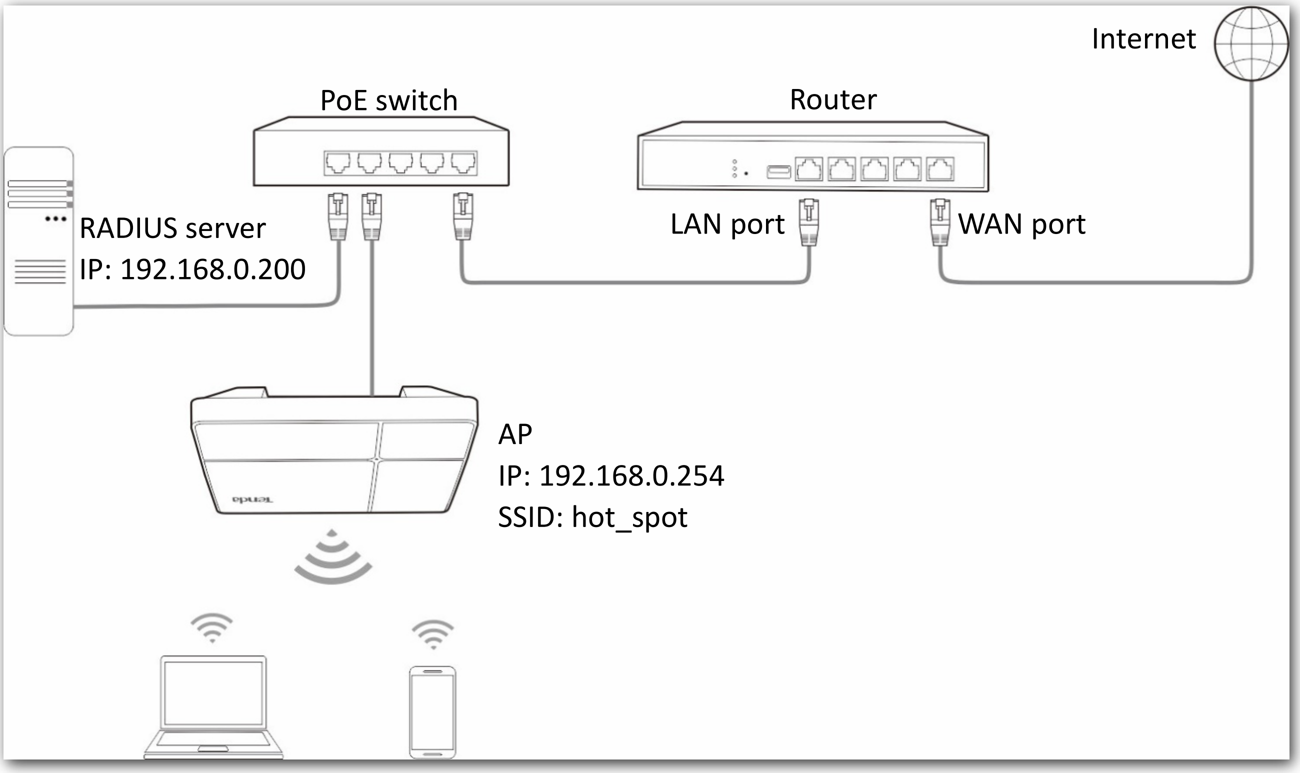
Wireless devices can connect to the **hotel** wireless network with the password **UmXmL9UK**.

## Example of setting up a wireless network encrypted with WPA or WPA2

### Networking requirement

A highly secure wireless network is required and a RADIUS server is available. In this case, WPA or WPA2 mode is recommended.

Assume that the IP address of the RADIUS server is **192.168.0.200**, the RADIUS password is **12345678**, the port number for authentication is **1812**, and the SSID is **hot_spot**. See the following figure.



### Configuration procedure

**Configure the AP.**

Assume that the second SSID of the 2.4 GHz radio band of the AP is to be configured.

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

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

Step 3 Set **Status** to **Enable**.

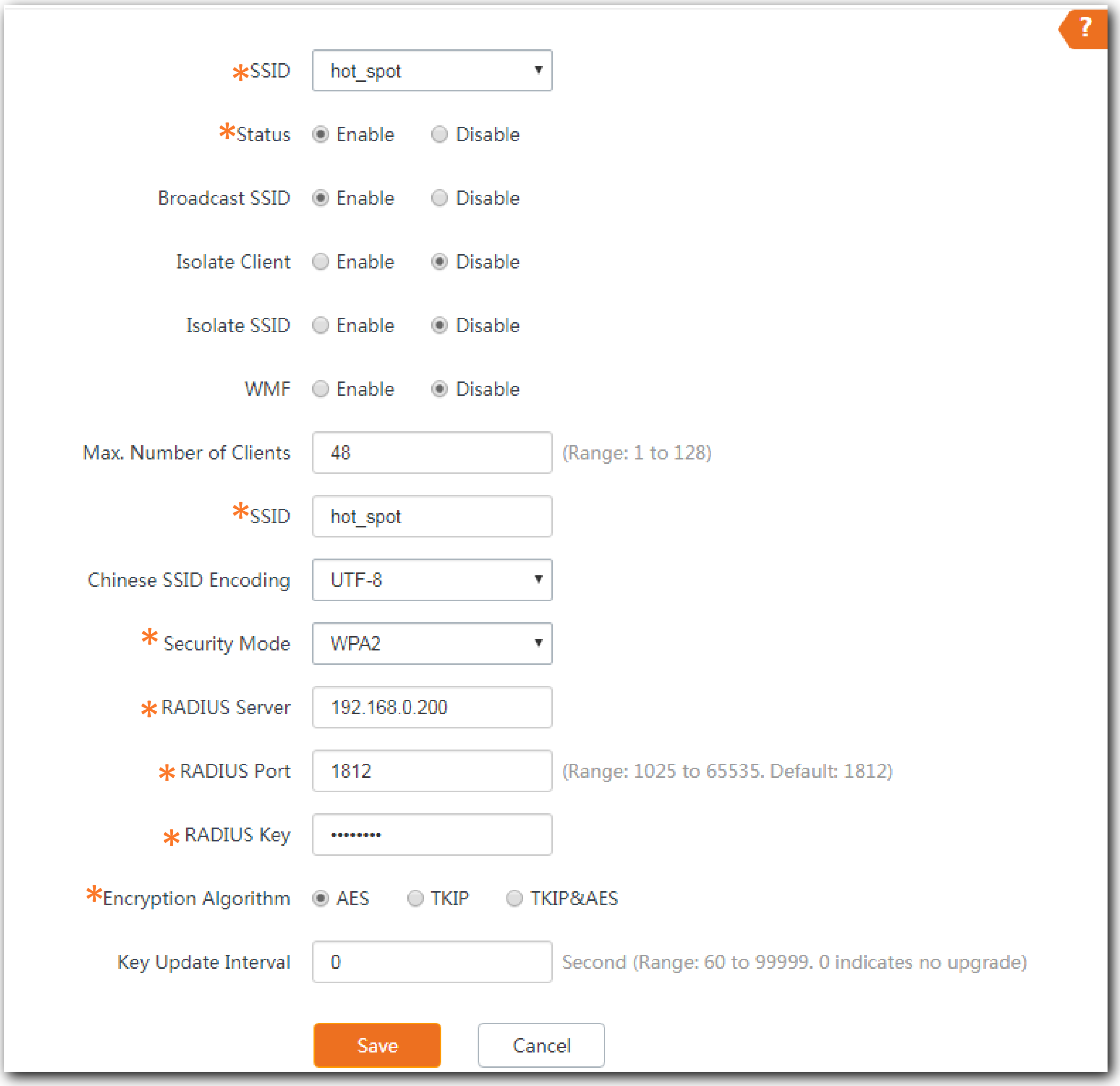
Step 4 Change the value of the SSID text box to **hot_spot**.

Step 5 Set **Security Mode** to **WPA2**. The RADIUS-related parameters appear.

**Step 6** Enter your **RADIUS Server**, **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** to apply your settings.



*SSID: hot_spot

*Status: ● Enable ○ Disable

Broadcast SSID: ● Enable ○ Disable

Isolate Client: ○ Enable ● Disable

Isolate SSID: ○ Enable ● Disable

WMF: ○ Enable ● Disable

Max. Number of Clients: 48 (Range: 1 to 128)

*SSID: hot_spot

Chinese SSID Encoding: UTF-8

* Security Mode: WPA2

* RADIUS Server: 192.168.0.200

* RADIUS Port: 1812 (Range: 1025 to 65535. Default: 1812)

* RADIUS Key: ••••••••

*Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key Update Interval: 0 Second (Range: 60 to 99999. 0 indicates no upgrade)

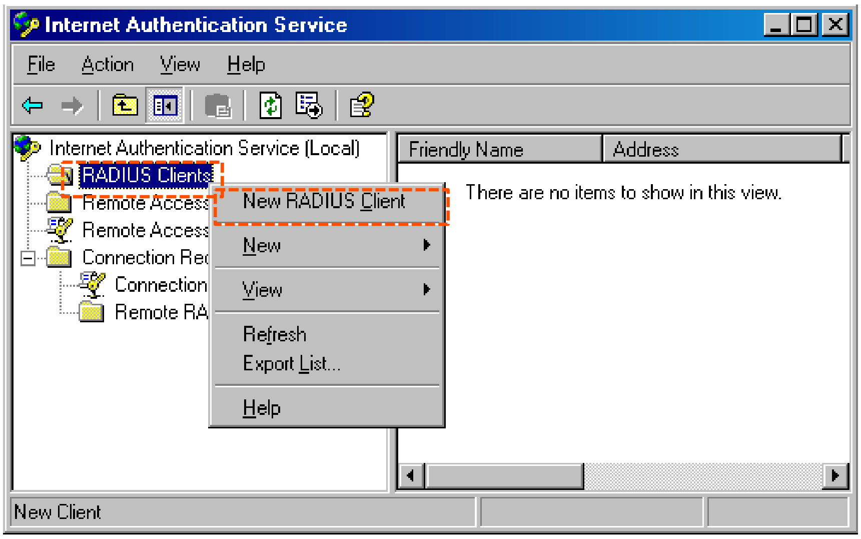
### Configure the RADIUS client.

TIP

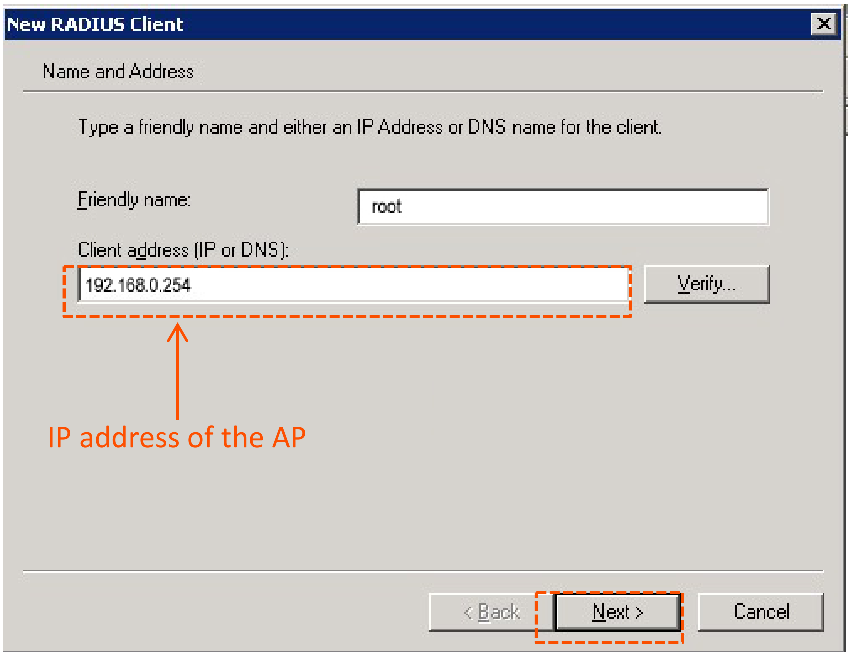
Windows 2003 is used as an example to describe how to configure the RADIUS client.

**Step 1** Configure 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 (device name of the AP is recommended) and the IP address of the AP, and click **Next**.


New RADIUS Client

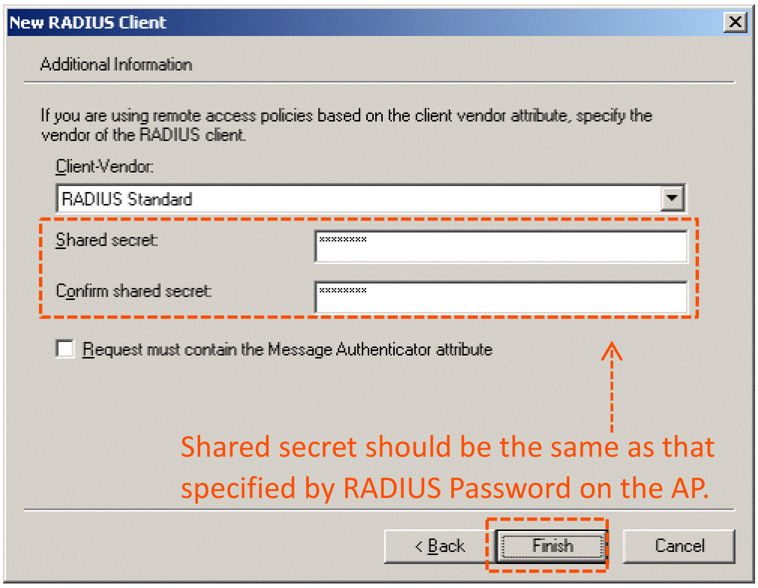
Name and Address

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

Friendly name: root

Client address (IP or DNS): 192.168.0.254

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



New RADIUS Client

Additional Information

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

Client-Vendor: RADIUS Standard

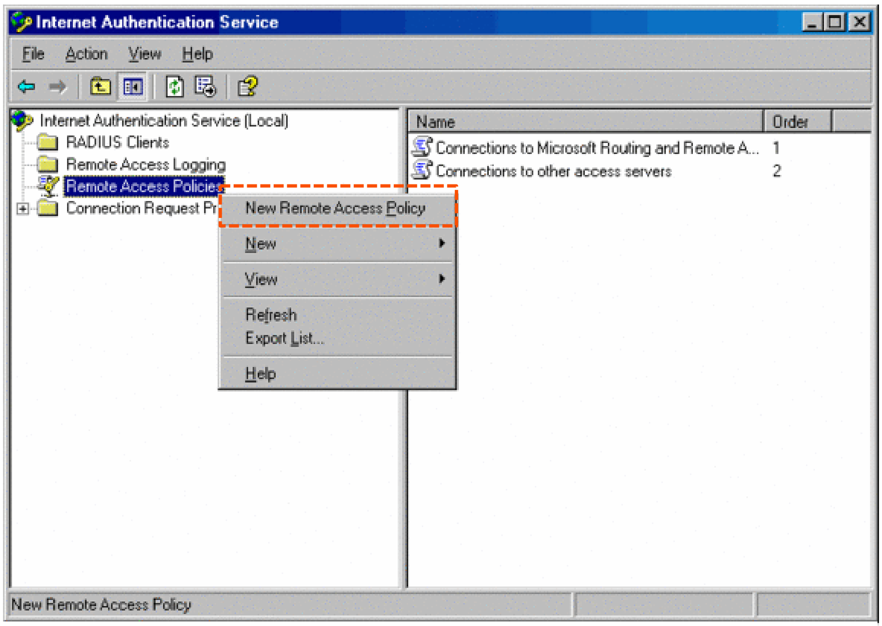
Shared secret: ********

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

Shared secret should be the same as that specified by RADIUS Password on the AP.

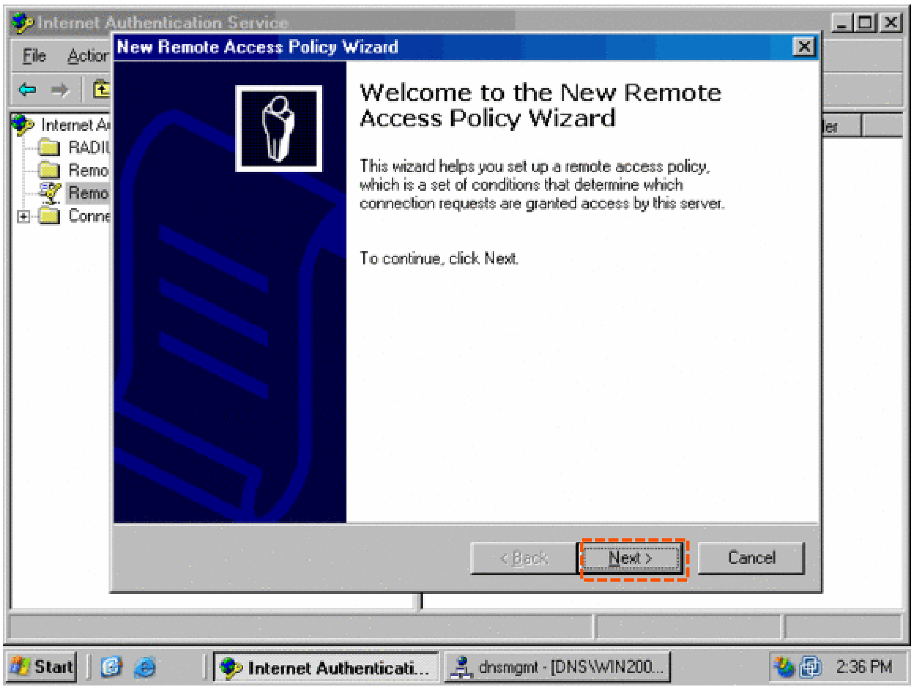
**Step 2** Configure a remote access policy.

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



| Name | Order |
|---|---|
| Connections to Microsoft Routing and Remote A... | 1 |
| Connections to other access servers | 2 |

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

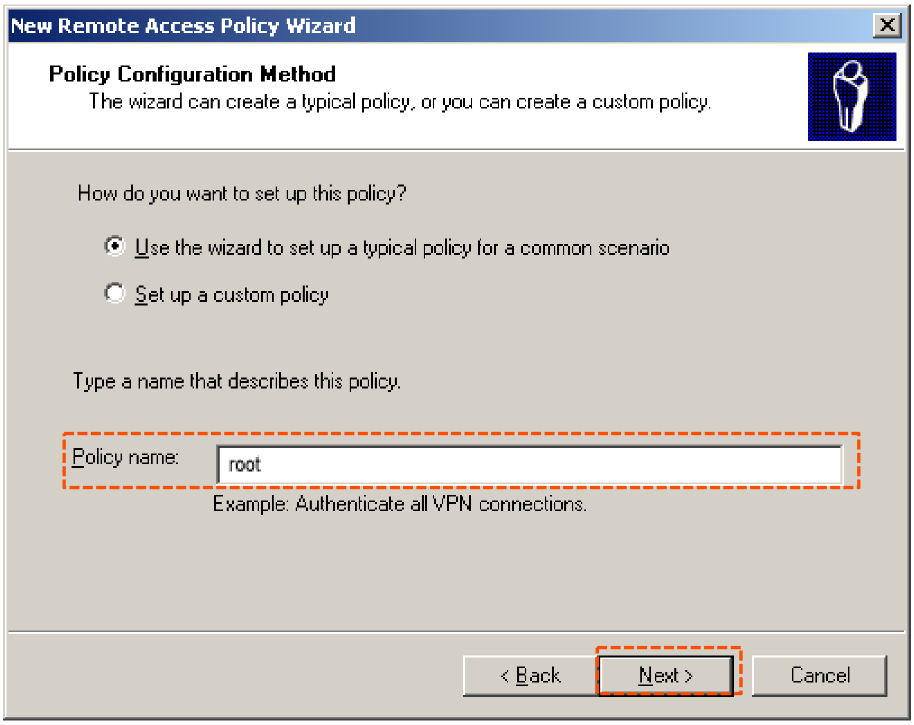


Welcome to the New Remote Access Policy Wizard

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

To continue, click Next.

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



Policy Configuration Method

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

How do you want to set up this policy?

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

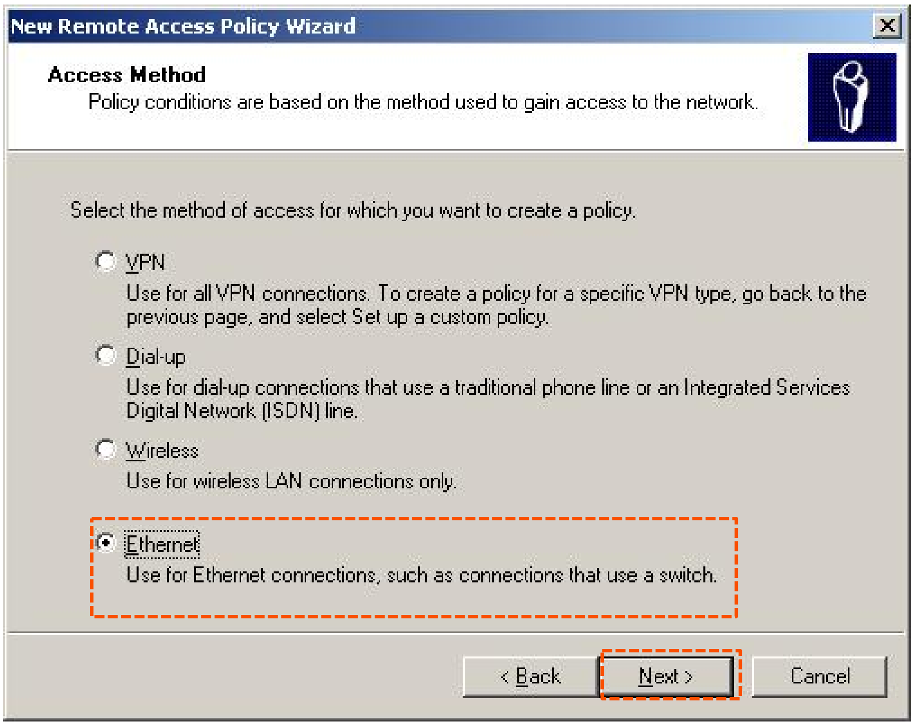
○ Set up a custom policy

Type a name that describes this policy.

Policy name: root

Example: Authenticate all VPN connections.

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



New Remote Access Policy Wizard

**Access Method**

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

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

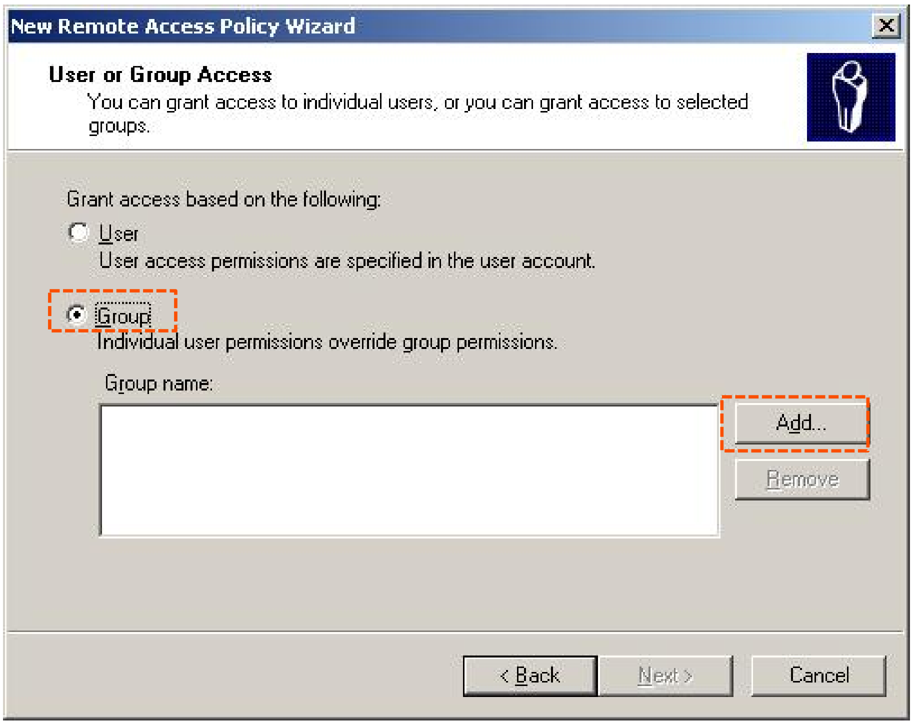
○ VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

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

○ Wireless
Use for wireless LAN connections only.

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

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



New Remote Access Policy Wizard

**User or Group Access**

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

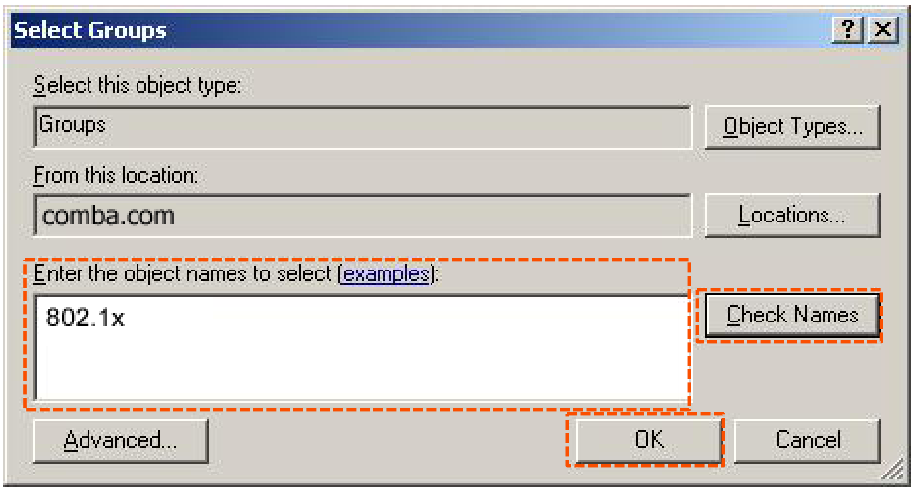
Grant access based on the following:

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

● Group
Individual user permissions override group permissions.

Group name:

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



Select Groups

Select this object type:

Groups

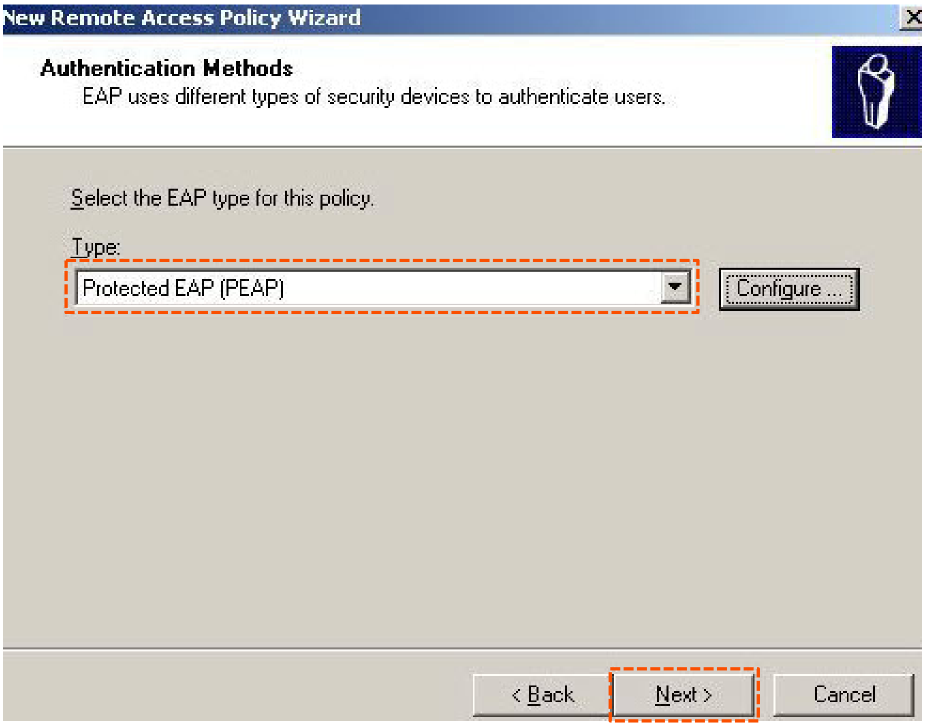
From this location:

comba.com

Enter the object names to select (examples):

802.1x

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



New Remote Access Policy Wizard

**Authentication Methods**

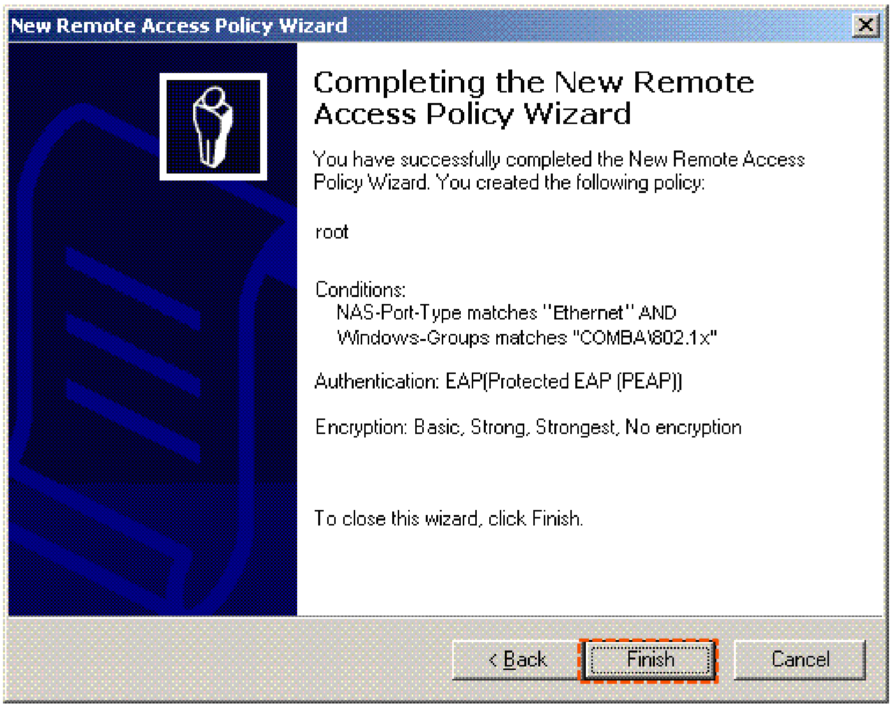
EAP uses different types of security devices to authenticate users.

Select the EAP type for this policy.

Type:

Protected EAP (PEAP)

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



Completing the New Remote Access Policy Wizard

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

root

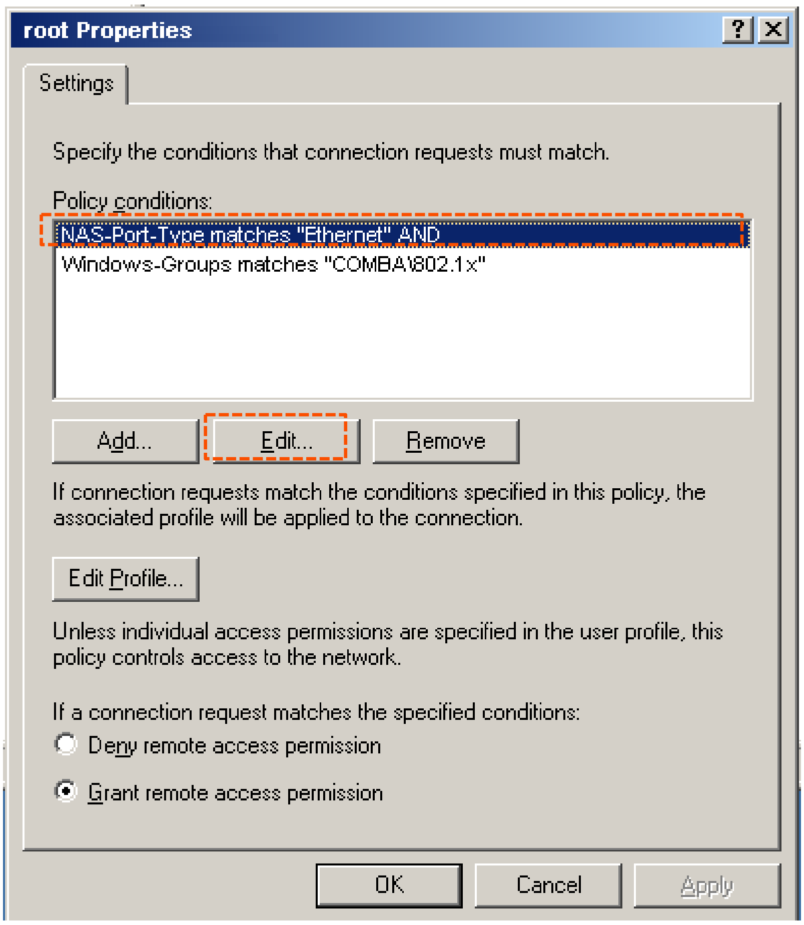
Conditions:
NAS-Port-Type matches "Ethernet" AND
Windows-Groups matches "COMBA\802.1x"

Authentication: EAP(Protected EAP (PEAP))

Encryption: Basic, Strong, Strongest, No encryption

To close this wizard, click Finish.

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



Specify the conditions that connection requests must match.

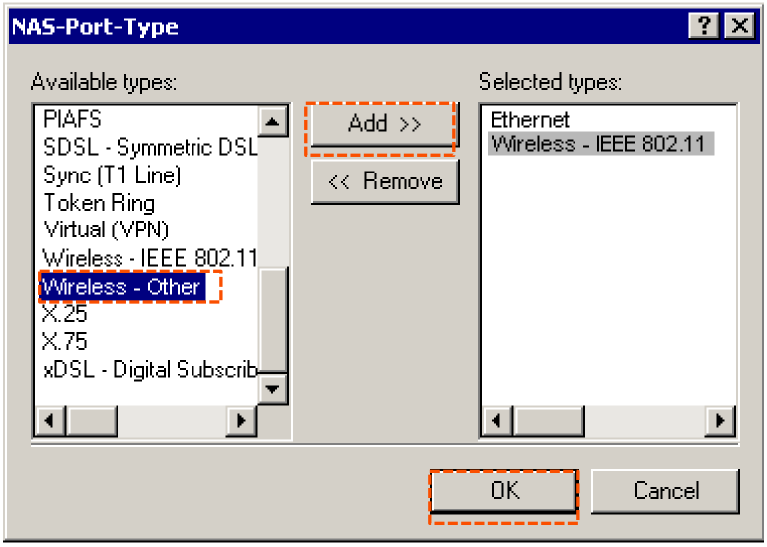
Policy conditions:
NAS-Port-Type matches "Ethernet" AND
Windows-Groups matches "COMBA\802.1x"

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

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

If a connection request matches the specified conditions:
○ Deny remote access permission
● Grant remote access permission

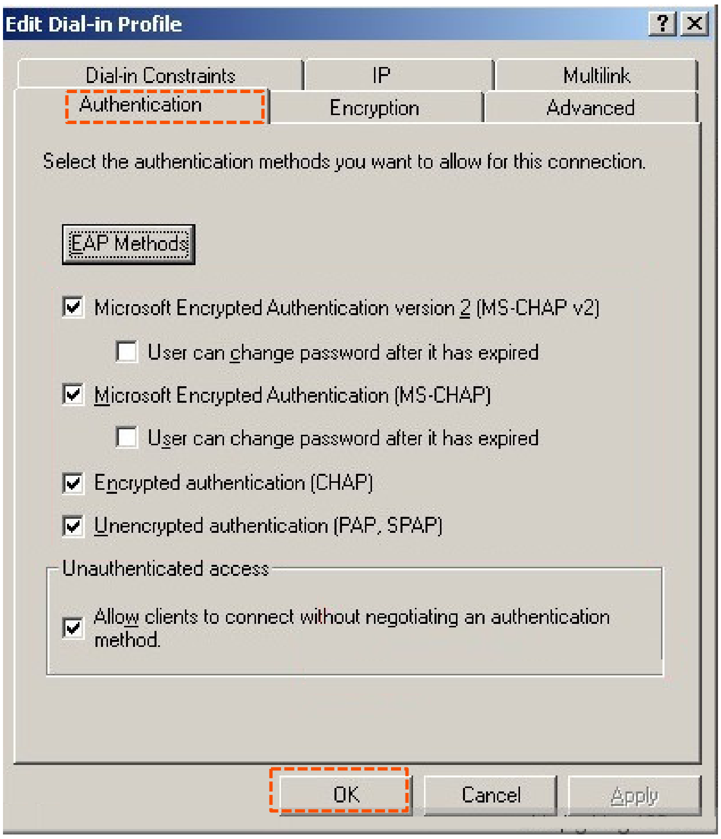
10. Select **Wireless – Other**, click **Add**, and click **OK**.



Selected types:

Ethernet
Wireless - IEEE 802.11

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



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

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

□ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

☑ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☑ Allow clients to connect without negotiating an authentication method.

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

**Step 3** Configure user information.

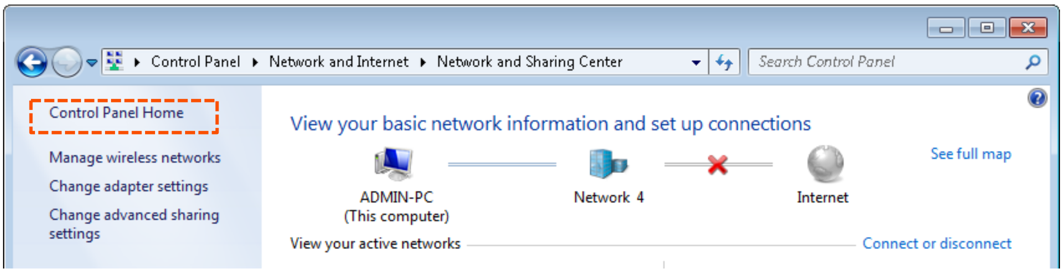
Create a user and add the user to group **802.1x**.

### Configure your wireless device

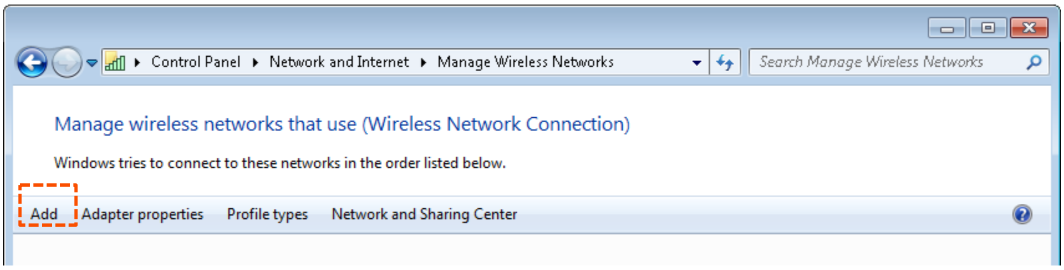
TIP

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**.


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
ADMIN-PC
(This computer)
Network 4
Internet
View your active networks
Connect or disconnect

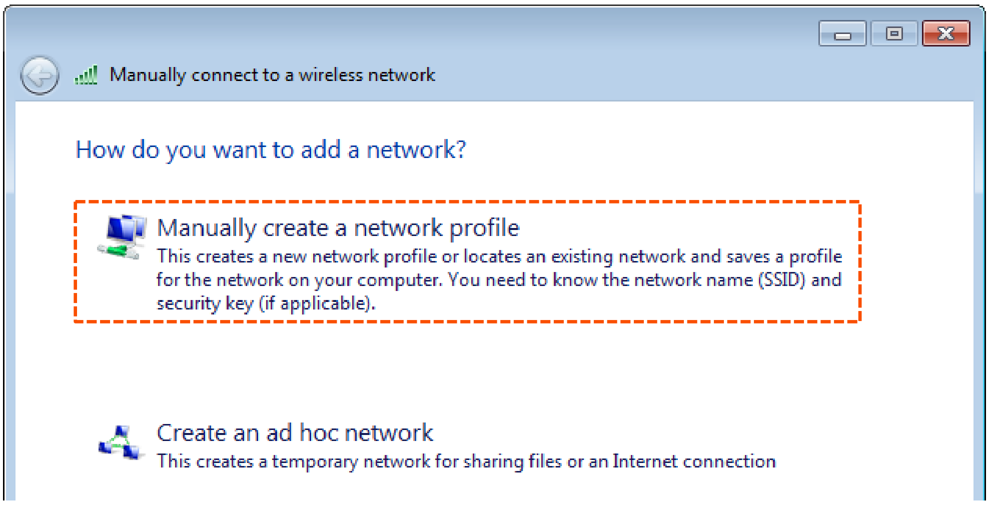
**Step 2** Click **Add**.


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

Manage wireless networks that use (Wireless Network Connection)

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

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

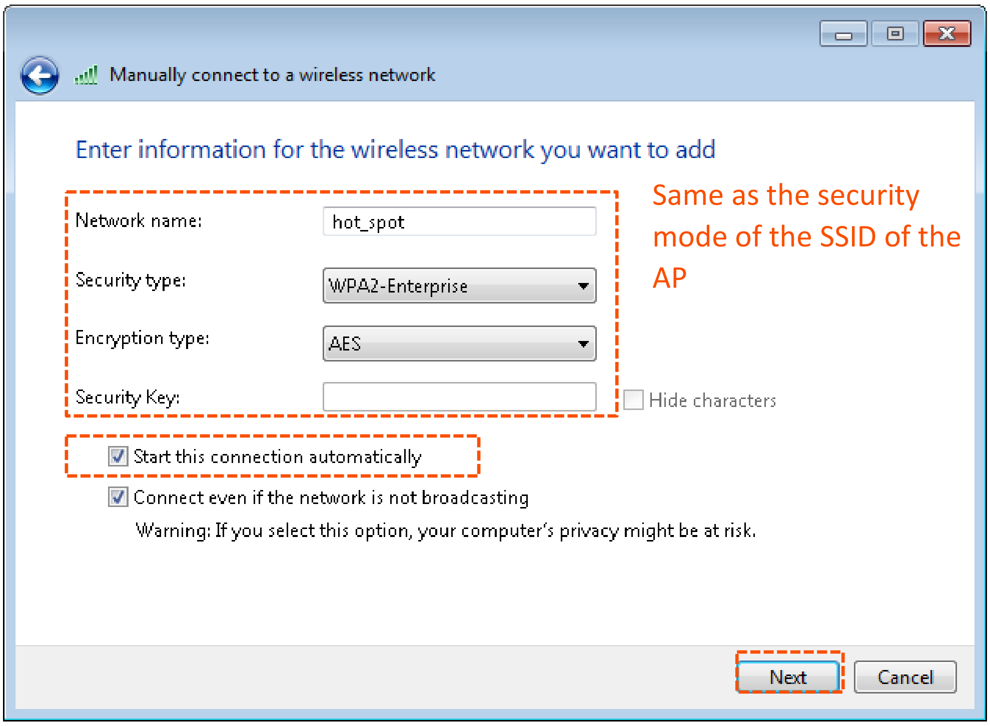


How do you want to add a network?

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

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

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



Enter information for the wireless network you want to add

Network name: hot_spot

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

□ Hide characters

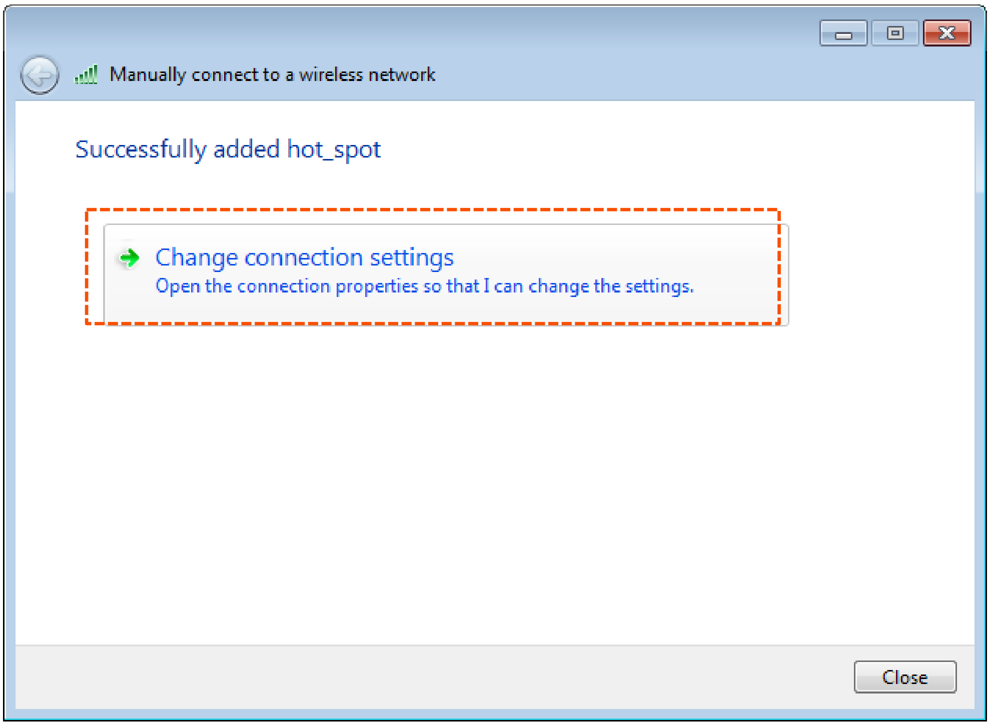
☑ Start this connection automatically

☑ Connect even if the network is not broadcasting

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

Same as the security mode of the SSID of the AP

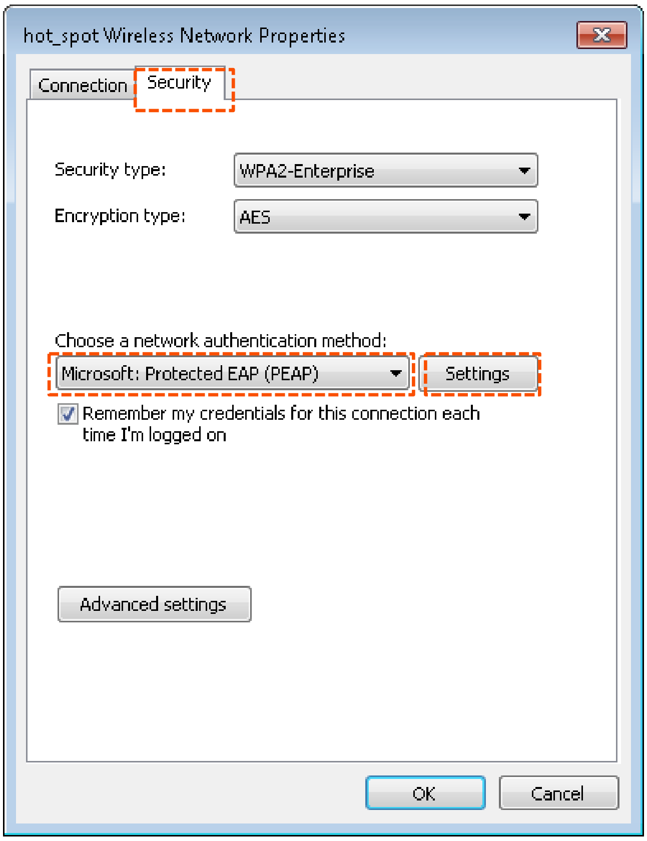
**Step 5** Click **Change connection settings**.



Successfully added hot_spot

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

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



hot_spot Wireless Network Properties

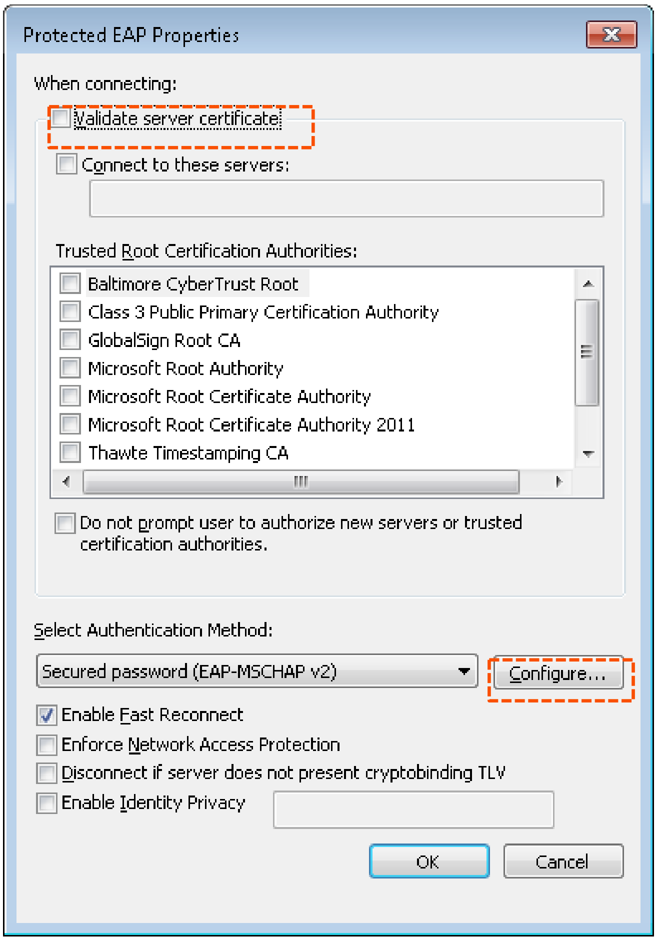
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: Microsoft: Protected EAP (PEAP)

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

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



Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

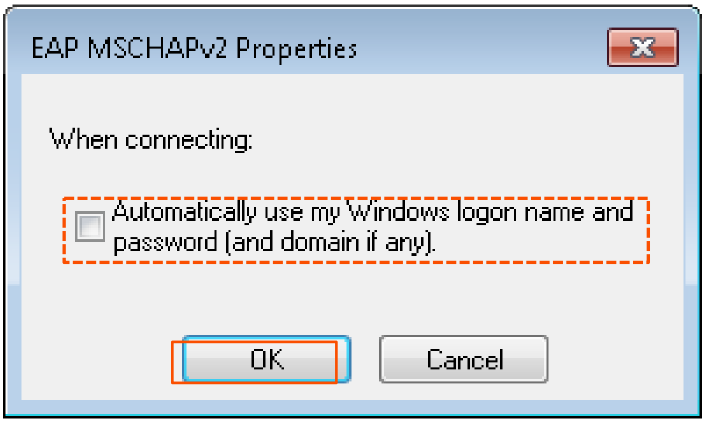
□ Baltimore CyberTrust Root
□ Class 3 Public Primary Certification Authority
□ GlobalSign Root CA
□ Microsoft Root Authority
□ Microsoft Root Certificate Authority
□ Microsoft Root Certificate Authority 2011
□ Thawte Timestamping CA

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

Select Authentication Method: Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

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

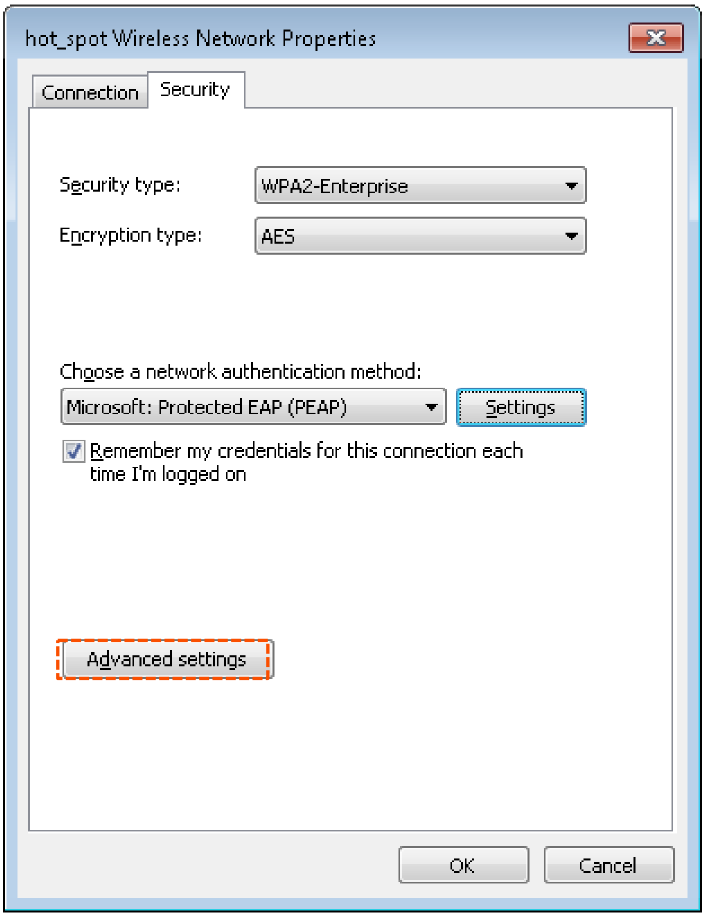


EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

**Step 9** Click **Advanced settings**.



hot_spot Wireless Network Properties

Security type: WPA2-Enterprise

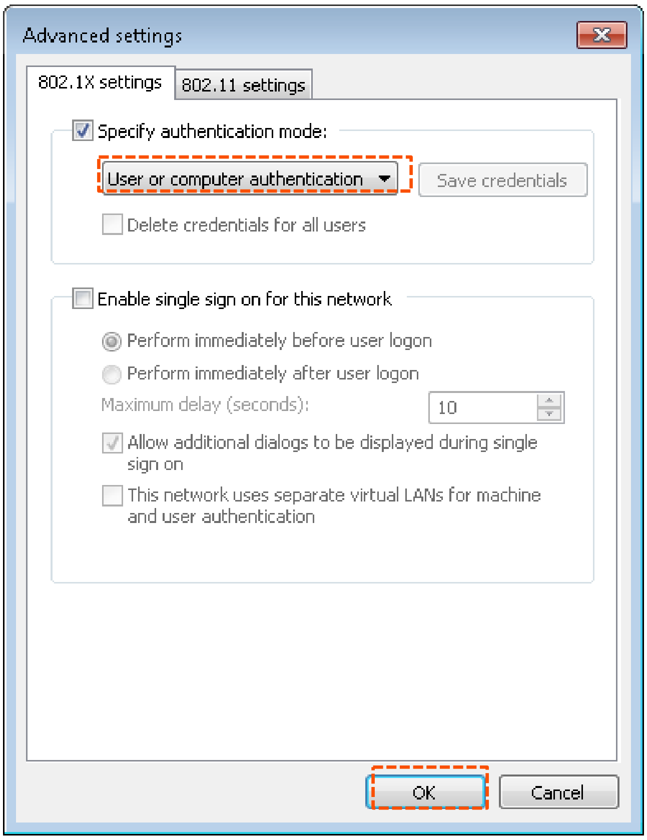
Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

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

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



Advanced settings

802.1X settings | 802.11 settings

☑ Specify authentication mode:

User or computer authentication ▼ | Save credentials

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

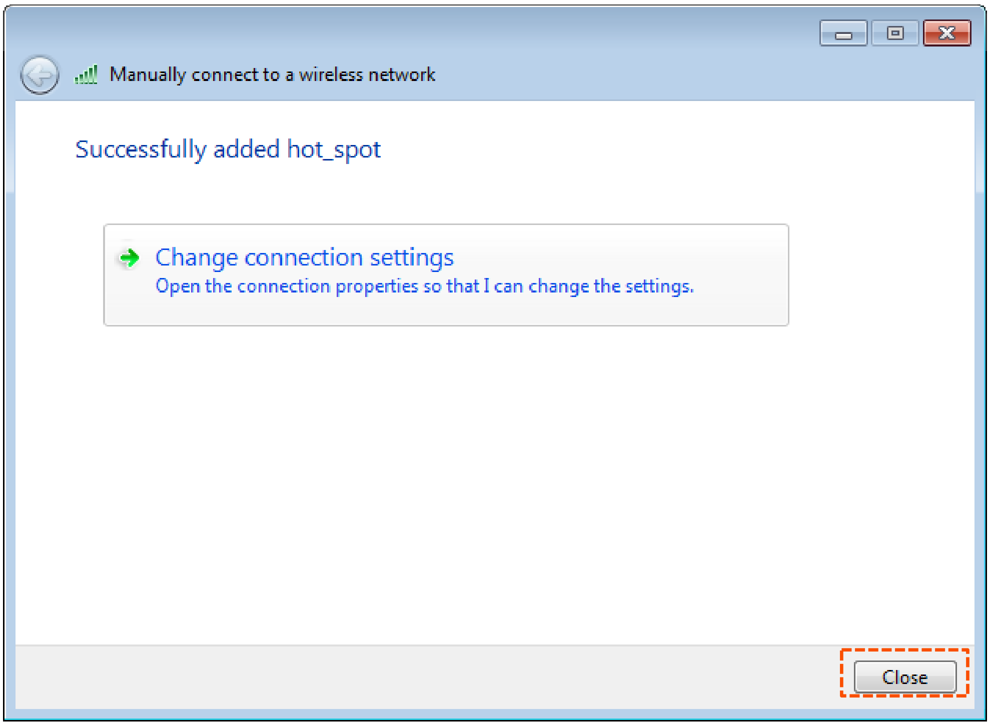
○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

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

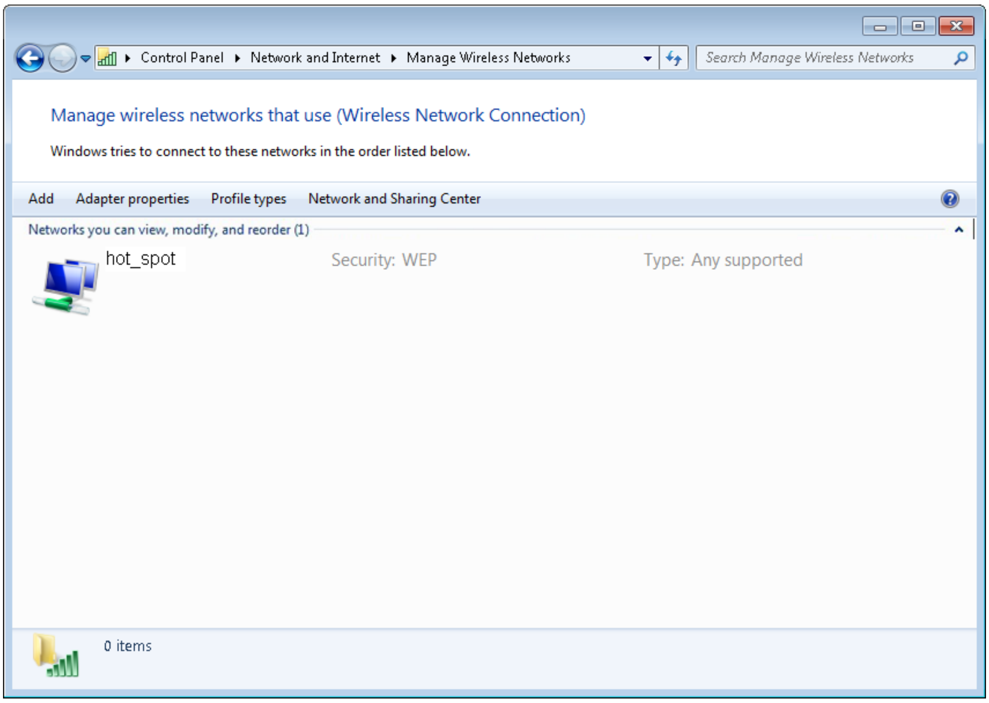
**Step 11** Click **Close**.



Manually connect to a wireless network

Successfully added hot_spot

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



Control Panel ▸ Network and Internet ▸ Manage Wireless Networks

Search Manage Wireless Networks

Manage wireless networks that use (Wireless Network Connection)

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

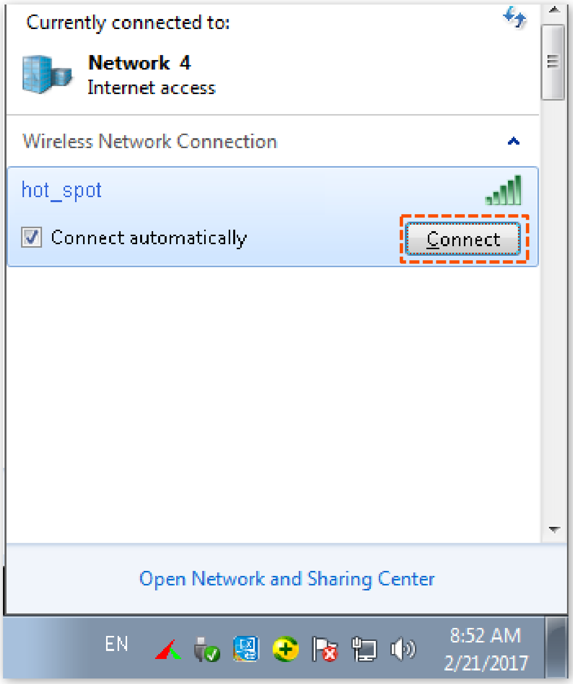
Add   Adapter properties   Profile types   Network and Sharing Center

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

hot_spot   Security: WEP   Type: Any supported

0 items

**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.



Currently connected to:

**Network 4**
Internet access

Wireless Network Connection

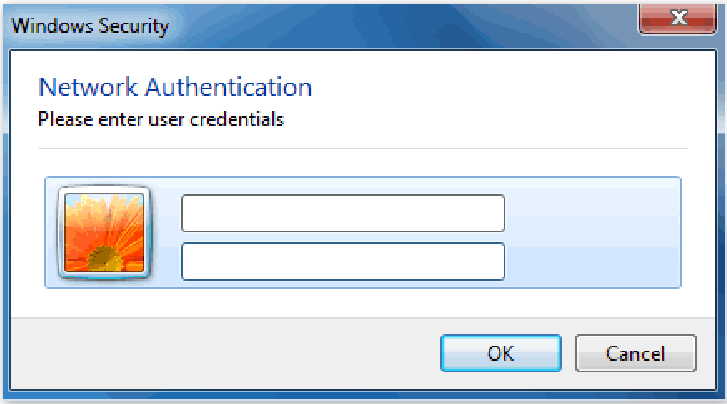
hot_spot

☑ Connect automatically   Connect

Open Network and Sharing Center

EN   8:52 AM 2/21/2017

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



Windows Security

Network Authentication

Please enter user credentials

---- End

- **Verification**

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

# 6.2 RF settings

## 6.2.1 Overview

RF (Radio Frequency) settings allow you to configure advanced settings about the AP, such as country/region, network mode, channel, power.

To access the page, choose **Wireless** > **RF settings**

## 6.2.2 Configuring RF settings

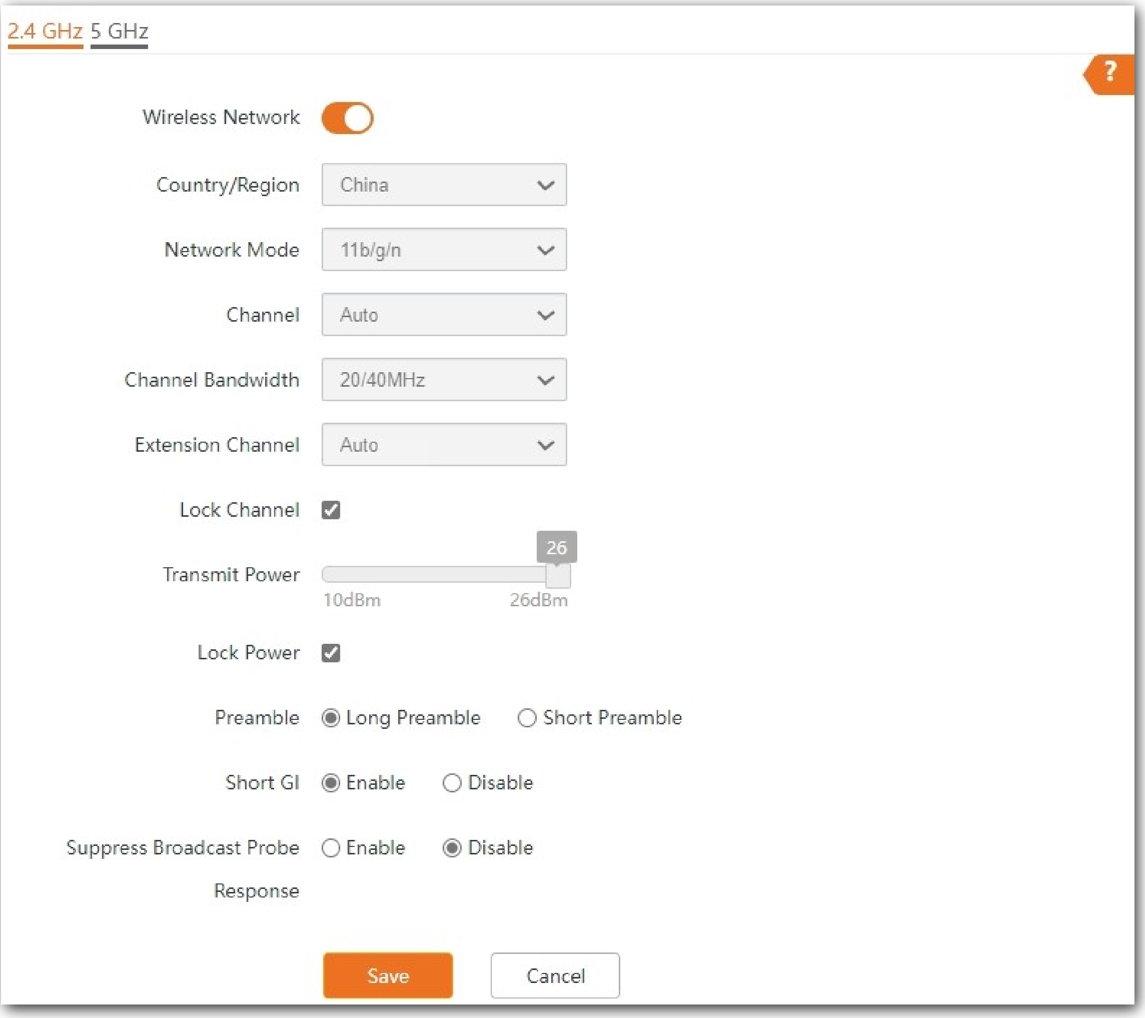
**Step 1** Choose **Wireless** > **RF Settings**.

**Step 2** Click the tab of the radio band to be modified.

**Step 3** Enable **Wireless Network**.

**Step 4** Modify the parameters as required (generally you only need to adjust **Channel**, **Lock Channel**, **Transmit Power**, and **Lock Power**).

**Step 5** Click **Save**.



Wireless Network: On

Country/Region: China

Network Mode: 11b/g/n

Channel: Auto

Channel Bandwidth: 20/40MHz

Extension Channel: Auto

Lock Channel: ☑

Transmit Power: 26 (10dBm – 26dBm)

Lock Power: ☑

Preamble: ● Long Preamble ○ Short Preamble

Short GI: ● Enable ○ Disable

Suppress Broadcast Probe Response: ○ Enable ● Disable

**---- End**

### Parameter description

| Parameter | Description |
|---|---|
| Wireless Network | It specifies whether to enable the radio 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**. This parameter can be set if Lock Channel is not selected. |
| Network Mode | It specifies the wireless network mode of the AP. This parameter can be set if Lock Channel is not selected.<br>Available options for 2.4 GHz are **11b**, **11g**, **11b/g**, **11b/g/n**.<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>Available options for 5 GHz are **11a**, **11ac**, and **11a/n**.<br>• 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.<br>• 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.<br>• 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. |
| Channel | It specifies the operating channel of the AP. This parameter can be set if Lock Channel is not selected.<br>**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 11b/g/n, 11ac, or 11a/n mode and Lock Channel is not selected.<br>• 20 MHz: It indicates that the AP can use only 20 MHz channel bandwidth.<br>• 40 MHz: It indicates that the AP can use only 40 MHz channel bandwidth.<br>• 20/40 MHz: Only available for 2.4 GHz. It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment.<br>• 80MHz: Only available for 5 GHz. It indicates that the AP can use only 80 MHz channel bandwidth. |

| Parameter | Description |
|---|---|
| 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. This parameter can be set if **Lock Power** is not selected.<br>A higher value leads to wider WiFi coverage. However, decreasing the value properly increases performance and security of the wireless network. |
| Lock Power | It is used to lock the current transmit power of the radio band. If selected, the settings cannot be adjusted. |
| Preamble | It specifies a group of bits located at the beginning of a packet, according to which the receiver of the packet can perform synchronization and prepare for receiving data.<br>By default, the **Long Preamble** option is selected for compatibility with old network adopters installed on wireless devices. To achieve better synchronization performance of networks, you can select the **Short Preamble** option. |
| Short GI | Short guard interval for preventing data block interference.<br>Propagation delays may occur on the receiver side due to factors such as multipath wireless signal transmission. If a data block is transmitted at an overly high speed, it may interfere with the previous data block. The short GI helps prevent such interference. Enabling the short GI can yield a 10% improvement in wireless data throughput. |
| 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.<br>After this function is enabled, this device does not respond to the requests without an SSID, saving wireless resources. |

# 6.3 RF optimization

## 6.3.1 Overview

### Wireless network application secenarios

- **Common scenario**

Generally used in offices, public buildings, schools, warehouses and hospitals where a large area of wireless network coverage is required.

- **High-density scenario**

A large number of people and terminal devices are concentrated in a large but highly concentrated area, which requires high-density deployment of APs. Common high-density scenarios include:

- Conference rooms, theaters, exhibition halls, banquet halls
- Indoor/outdoor stadiums
- College classrooms
- Airports, railway stations

### Optimizaiton parameters

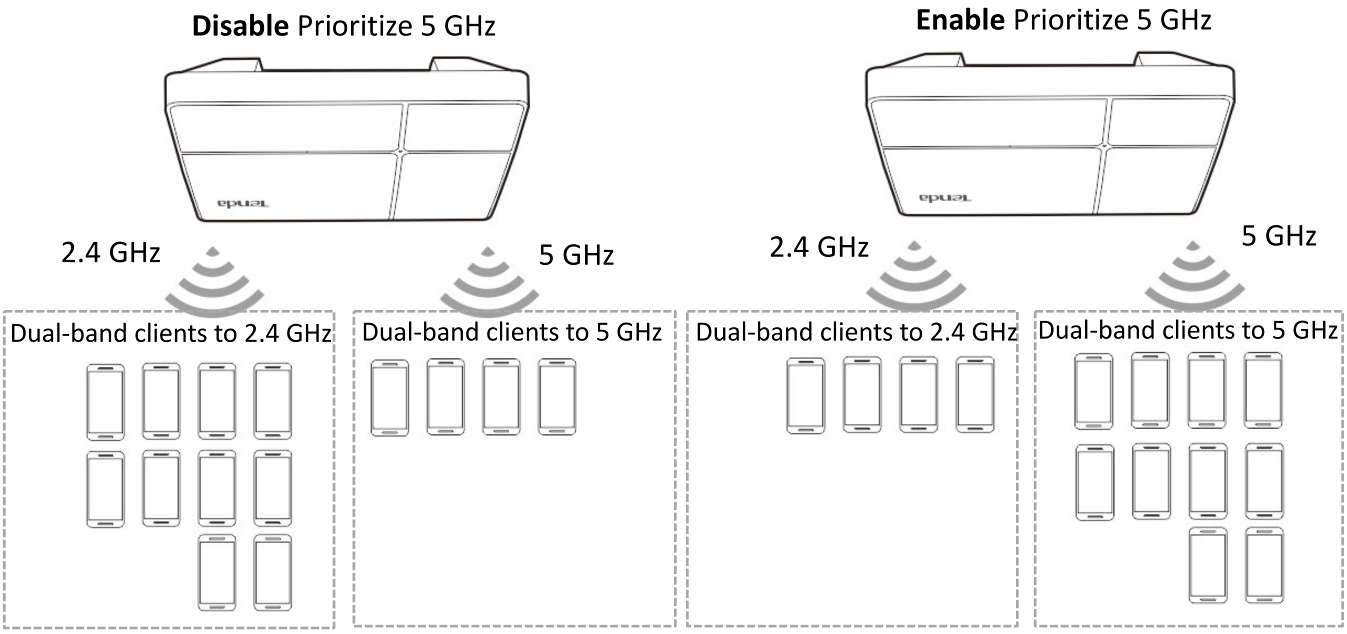
The AP provides a series of optimization parameters to meet different requirements for wireless access in common scenarios (mainly coverage) and high-density scenarios (requiring higher capacity), and to provide customers with high-quality wireless network services.

- **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 function 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.


Disable Prioritize 5 GHz
Enable Prioritize 5 GHz
2.4 GHz
5 GHz
2.4 GHz
5 GHz
Dual-band clients to 2.4 GHz
Dual-band clients to 5 GHz
Dual-band clients to 2.4 GHz
Dual-band clients to 5 GHz

* Assume that the max. number of clients allowed to connect to the 5 GHz is 10.

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 number of clients allowed to be connected.

## 6.3.2 Modifying radio optimization settings

NOTE

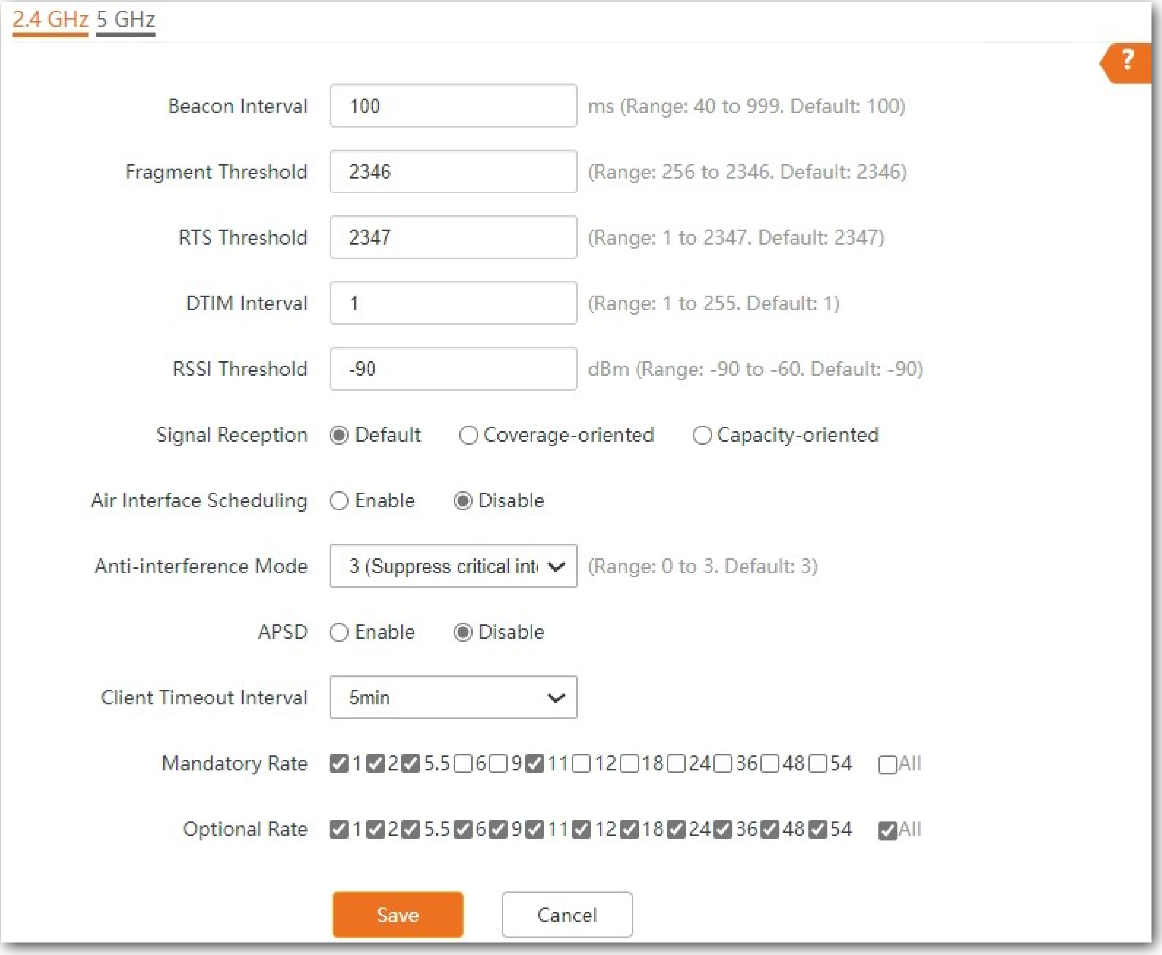
You are strongly recommended to modify the settings only with professional guidance to prevent degrading wireless performance.

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

**Step 2** Click the radio band tab of the radio to be optimized.

**Step 3** Modify the parameters as required.

**Step 4** Click **Save** to apply your settings.



| | | |
|---|---|---|
| Beacon Interval | 100 | ms (Range: 40 to 999. Default: 100) |
| Fragment Threshold | 2346 | (Range: 256 to 2346. Default: 2346) |
| RTS Threshold | 2347 | (Range: 1 to 2347. Default: 2347) |
| DTIM Interval | 1 | (Range: 1 to 255. Default: 1) |
| RSSI Threshold | -90 | dBm (Range: -90 to -60. Default: -90) |
| Signal Reception | ● Default ○ Coverage-oriented ○ Capacity-oriented | |
| Air Interface Scheduling | ○ Enable ● Disable | |
| Anti-interference Mode | 3 (Suppress critical int | (Range: 0 to 3. Default: 3) |
| APSD | ○ Enable ● Disable | |
| Client Timeout Interval | 5min | |
| Mandatory Rate | ☑1 ☑2 ☑5.5 □6 □9 ☑11 □12 □18 □24 □36 □48 □54 □All | |
| Optional Rate | ☑1 ☑2 ☑5.5 ☑6 ☑9 ☑11 ☑12 ☑18 ☑24 ☑36 ☑48 ☑54 ☑All | |

**---- End**

### Parameter description

| Parameter | Description |
|---|---|
| Beacon Interval | It specifies the interval for transmitting the Beacon frame.<br>The Beacon frame is transmitted at the specified interval to announce the presence of a wireless network. Generally, a smaller interval enables wireless devices to connect to the AP more quickly, while a larger interval ensures higher data transmission speed for the AP. |
| Fragment Threshold | It specifies the threshold of a fragment.<br>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.<br>In an environment of high error rate, you can reduce the threshold to enable the AP to resend only the fragments that have not been sent successfully, so as to increase the frame throughput.<br>In an environment without interference, you can increase the threshold to reduce the number of acknowledgement times, so as to increase the frame throughput. |
| RTS Threshold | It specifies the frame length threshold for triggering the RTS/CTS mechanism. Unit: **byte**. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts.<br>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 WiFi network to recover from conflicts quicker. For a WiFi network with high user density, you can reduce this threshold for reducing conflicts.<br>The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold. |
| DTIM Interval | It specifies the interval for transmitting the Delivery Traffic Indication Message (DTIM) frame. Unit: **Beacon**.<br>A countdown starts from this value. The AP transmits broadcast and multicast frames in its cache only when the countdown reaches zero.<br>For example, if **DTIM Interval** is set to **1**, the AP transmits all cached frames after each beacon frame is transmitted. |
| Deployment Mode | • **Default**: This mode is applicable to most application scenarios.<br>• **Coverage-oriented**: This mode broadens WiFi coverage of APs but also increases the interference to APs. It is applicable to such scenarios with low AP deployment density as warehouses and hotel corridors.<br>• **Capacity-oriented**: This mode reduces WiFi coverage of APs but also decreases the interference to APs. It is applicable to such scenarios with high AP deployment density as conference rooms, classrooms, exhibition halls, and banquet halls. |

| Parameter | Description |
|---|---|
| Prioritize 5 GHz | If enabled, devices that support 5 GHz band choose to connect the AP's 5 GHz WiFi network first.<br>Otherwise, they randomly connect to 2.4GHz or 5 GHz WiFi network.<br>This option is available on the **5 GHz** configuration page. |
| Prioritize 5 GHz Threshold | With Prioritize 5 GHz 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 | It specifies whether to enable the air interface scheduling function of the AP.<br>If this function is enabled, the same download time is assigned to users experiencing different download rates, ensuring a better experience for high-rate users. |
| Anti-interference Mode | It specifies the anti-interference modes you can select for your AP.<br>• **0 (Disable)**: Interference suppression measures are disabled.<br>• **1 (Suppress weak interference)**: Suppress mild interference for weak radio environment.<br>• **2 (Suppress moderate interference)**: Suppress moderate interference for bad radio environment.<br>• **3 (Suppress critical interference)**: Suppress critical interference for heavy loading radio environment. |
| APSD | Automatic Power Save Delivery.<br>APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled. |
| MU-MIMO | Multi-User Multiple-Input Multiple-Output.<br>If enabled, AP can communicate with multiple users concurrently, avoiding WiFi network congestion and improving communication. This option is available on the **5 GHz** configuration page. |
| 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. The clients meeting the basic requirement can connect to the AP with higher rate. |

# 6.4 WMM

## 6.4.1 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 experience of voice and video service over WiFi 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 voice stream (AC-VO), video stream (AC-VI), best effort (AC-BE), and background (AC-BK) 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.

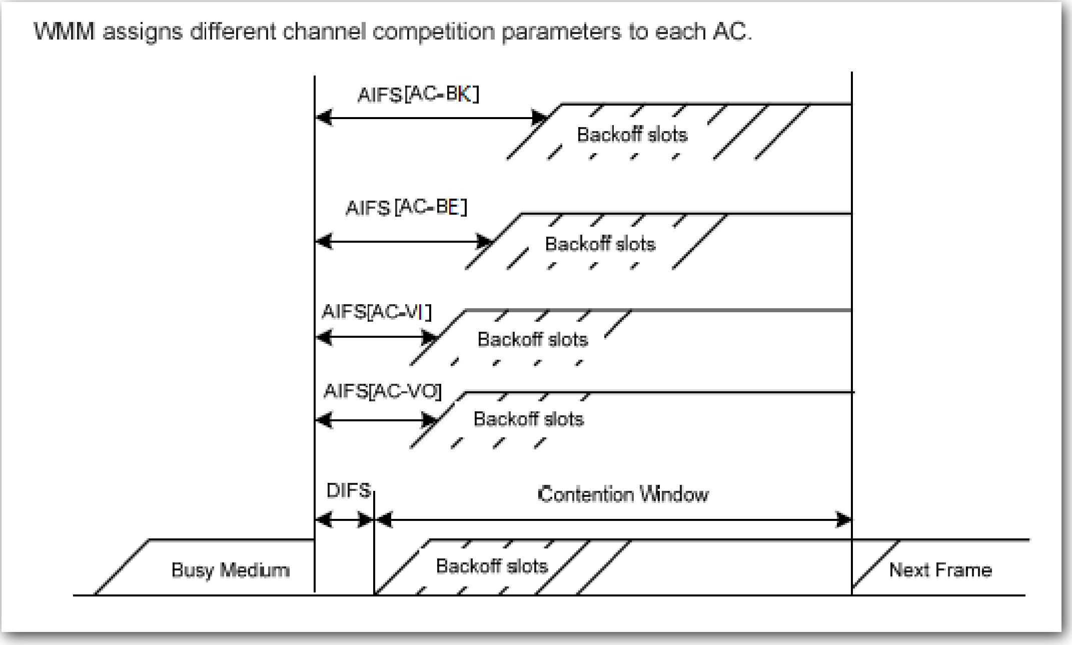
- **EDCA Parameters**

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 are not sent again if this policy is adopted. This leads 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.

## 6.4.2 Configuring WMM settings

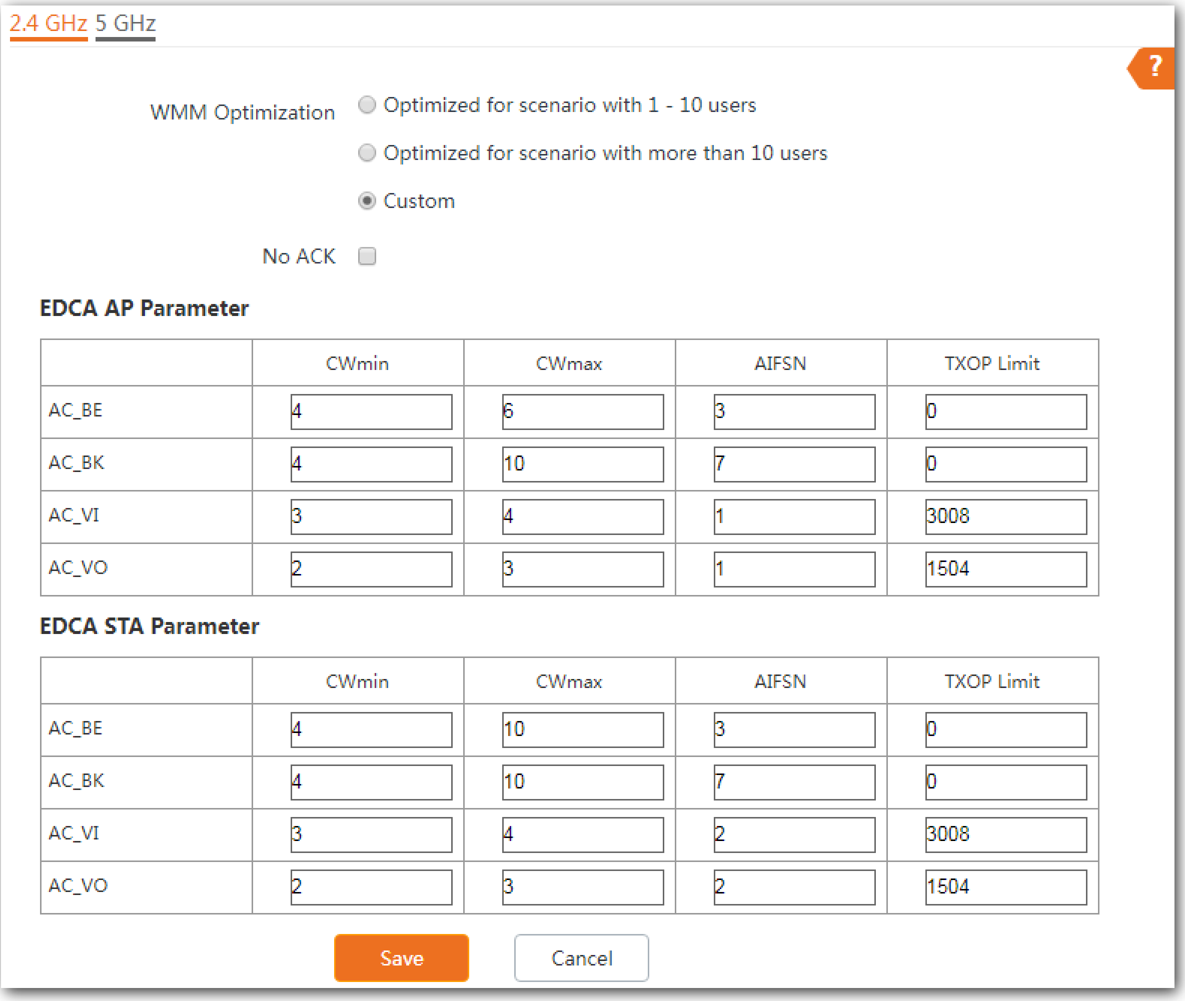
Step 1 Choose **Wireless** > **WMM.**

Step 2 Click the tab of the radio band whose WMM settings are to be modified.

Step 3 Select WMM optimization according to your actual situations.

Step 4 If you select **Custom** for **WMM Optimization**, customize the related parameters as required.

Step 5 Click **Save**.



WMM Optimization ○ Optimized for scenario with 1 - 10 users

○ Optimized for scenario with more than 10 users

● Custom

No ACK □

**EDCA AP Parameter**

| | CWmin | CWmax | AIFSN | TXOP Limit |
|---|---|---|---|---|
| AC_BE | 4 | 6 | 3 | 0 |
| AC_BK | 4 | 10 | 7 | 0 |
| AC_VI | 3 | 4 | 1 | 3008 |
| AC_VO | 2 | 3 | 1 | 1504 |

**EDCA STA Parameter**

| | CWmin | CWmax | AIFSN | TXOP Limit |
|---|---|---|---|---|
| AC_BE | 4 | 10 | 3 | 0 |
| AC_BK | 4 | 10 | 7 | 0 |
| AC_VI | 3 | 4 | 2 | 3008 |
| AC_VO | 2 | 3 | 2 | 1504 |

**---- End**

## Parameter description

| Parameter | Description |
|---|---|
| WMM Optimization | It specifies the WMM optimization modes supported by the AP:<br>• **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.<br>• **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.<br>• **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.<br>If the check box is deselected, the Normal ACK policy is adopted. |
| EDCA AP Parameter | See EDCA Parameters. |
| EDCA STA Parameter | |

# 6.5 Access control

## 6.5.1 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 2 filter modes:

- **Whitelist**: It indicates that only the wireless devices with the specified MAC addresses can access the wireless networks of the AP.

- **Blacklist**: It indicates that only the wireless devices with the specified MAC addresses cannot access the wireless networks of the AP.

## 6.5.2 Configuring access control

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

**Step 2** Choose a wireless network radio band on which access control is to be configured.

**Step 3** Select the SSID to which the access control is applied from the **SSID** drop-down list menu.

**Step 4** Enable **Access Control**.

**Step 5** Set **Mode** to **Blacklist** or **Whitelist**.

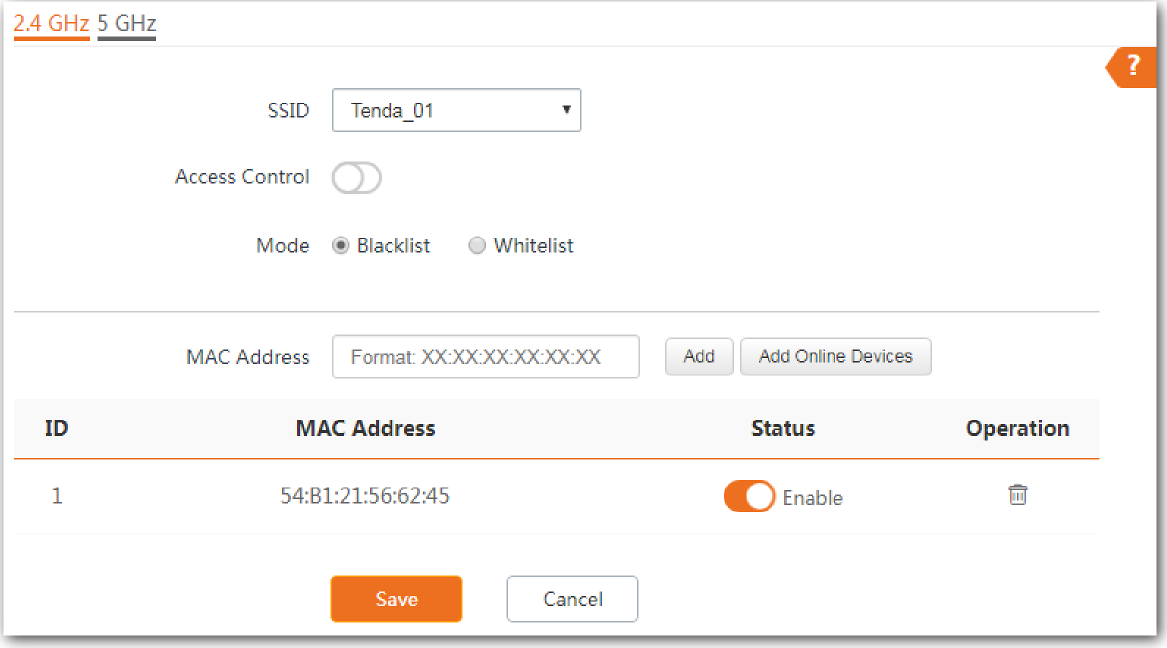
**Step 6** Enter the MAC address of the wireless device to which the rule applies.

**Step 7** Click **Add**.

TIP

If the wireless device to be controlled has connected to the AP, click Add Online Devices to quickly add the MAC address of the device to the access control client list.

**Step 8** Click **Save**.



SSID: Tenda_01

Access Control ○

Mode: ● Blacklist ○ Whitelist

MAC Address: Format: XX:XX:XX:XX:XX:XX

| ID | MAC Address | Status | Operation |
|---|---|---|---|
| 1 | 54:B1:21:56:62:45 | Enable | 🗑 |

---- End

**Parameter description**

| Parameter | Description |
|---|---|
| SSID | It specifies the wireless network to which the rule applies. |
| Access Control | It specifies whether or not to enable this function. |
| Mode | Set access control mode.<br>• **Whitelist**: It indicates that only the wireless clients on the wireless access control list can connect to the AP with the selected SSID.<br>• **Blacklist**: It indicates that only the wireless clients on the wireless access control list cannot connect to the AP with the selected SSID. |

## 6.5.3 Example of configuring access control

### Networking requirement

A wireless network whose SSID is **VIP** under the 5 GHz radio band has been set up in a company. Only a few members are allowed to connect to the wireless network.

The Access Control function of the AP is recommended. The members have three wireless devices whose MAC addresses are **C8:3A:35:00:00:01**, **C8:3A:35:00:00:02**, and **C8:3A:35:00:00:03**.

### Configuration procedure

Step 1 Choose **Wireless** > **Access Control** > **5 GHz**.

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

Step 3 Enable **Access Control** function.

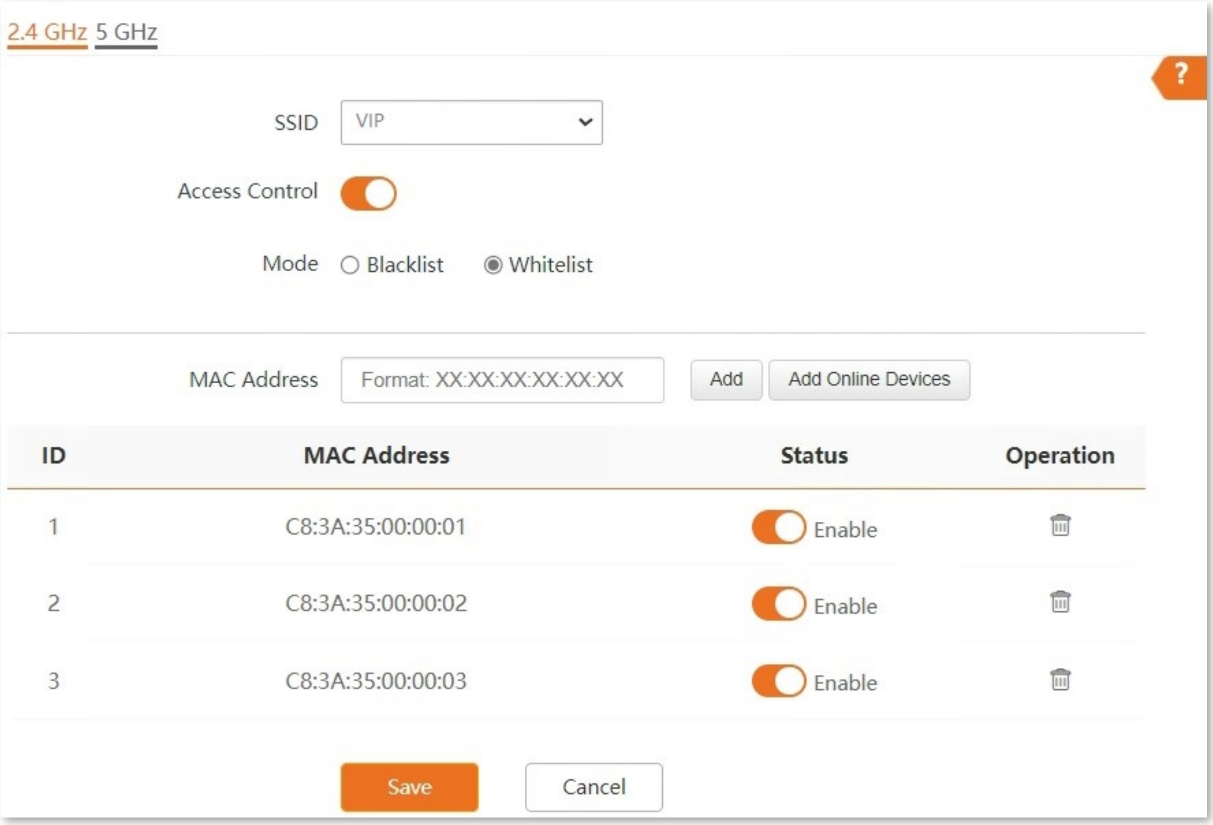
Step 4 Set **Mode** to **Whitelist**.

Step 5 Enter **C8:3A:35:00:00:01** in the **MAC Address** text box and click **Add**. Repeat this step to add **C8:3A:35:00:00:02** and **C8:3A:35:00:00:03** as well.

Step 6 Click **Save**.

---End

The following figure shows the configuration.



SSID: VIP

Access Control: enabled

Mode: ○ Blacklist ● Whitelist

MAC Address: Format: XX:XX:XX:XX:XX:XX

| ID | MAC Address | Status | Operation |
|---|---|---|---|
| 1 | C8:3A:35:00:00:01 | Enable | 🗑 |
| 2 | C8:3A:35:00:00:02 | Enable | 🗑 |
| 3 | C8:3A:35:00:00:03 | Enable | 🗑 |

## Verification

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

# 6.6 Advanced settings

## 6.6.1 Overview

This page enables you to set the **Identify Client Type** and **Broadcast Packet Filter** of the AP.

To access the page, choose **Wireless** > **Advanced Settings**.

- **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.

- **Broadcast Packet Filter**

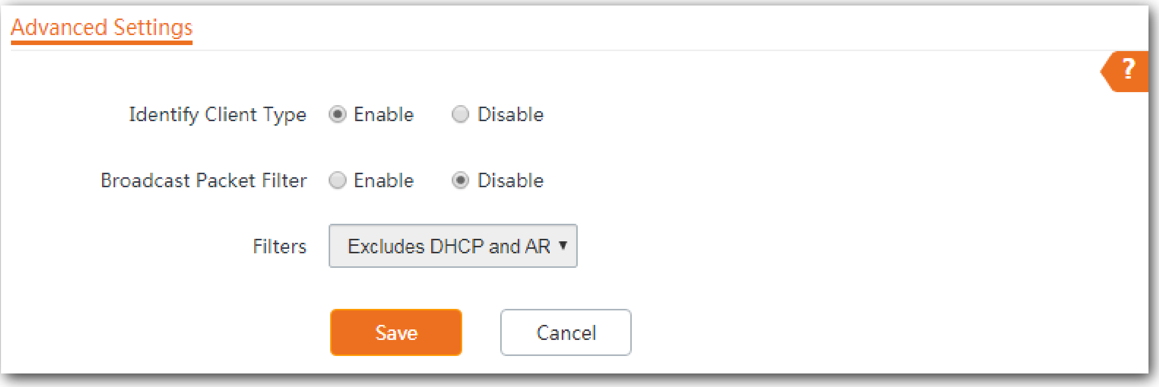
By default, this device forwards lots of invalid broadcast packets from wired networks, which may affect business data transfer. The broadcast packet filter function allows you to filter broadcast packets by types so that invalid packets are not forwarded. This reduces air interface resources usage and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

## 6.6.2 Modify adcanced settings

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

**Step 2** Modify the parameters as required.

**Step 3** Click **Save**.



Advanced Settings

Identify Client Type ● Enable ○ Disable

Broadcast Packet Filter ○ Enable ● Disable

Filters: Excludes DHCP and AR

**---End**

### Parameter description

| Parameter | Description |
|---|---|
| Identify Client Type | - **Enable**: Enable the identify client type function. With the function enabled, the operating system type of wireless devices connected to the AP’s WiFi network can be viewed by choosing Status > Wireless Clients.<br>- **Disable**: Disable the identify client type function. |
| Broadcast Packet Filter | - **Enable**: With the function enabled, the AP can reduce air interface resources usage and ensure the bandwidth for business data transfer.<br>- **Disable**: Disable the broadcast packet filter function. |
| Filter Mode | Select a mode after you enable the broadcast packet filter function.<br>- **Excludes DHCP and ARP**: Filter out all broadcast or multicast data except DHCP and ARP packets.<br>- **Excludes ARP**: Filter out all broadcast or multicast data except ARP packets. |

# 6.7 QVLAN settings

## 6.7.1 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.

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 | | | Transmit data without removing tags from the data. |

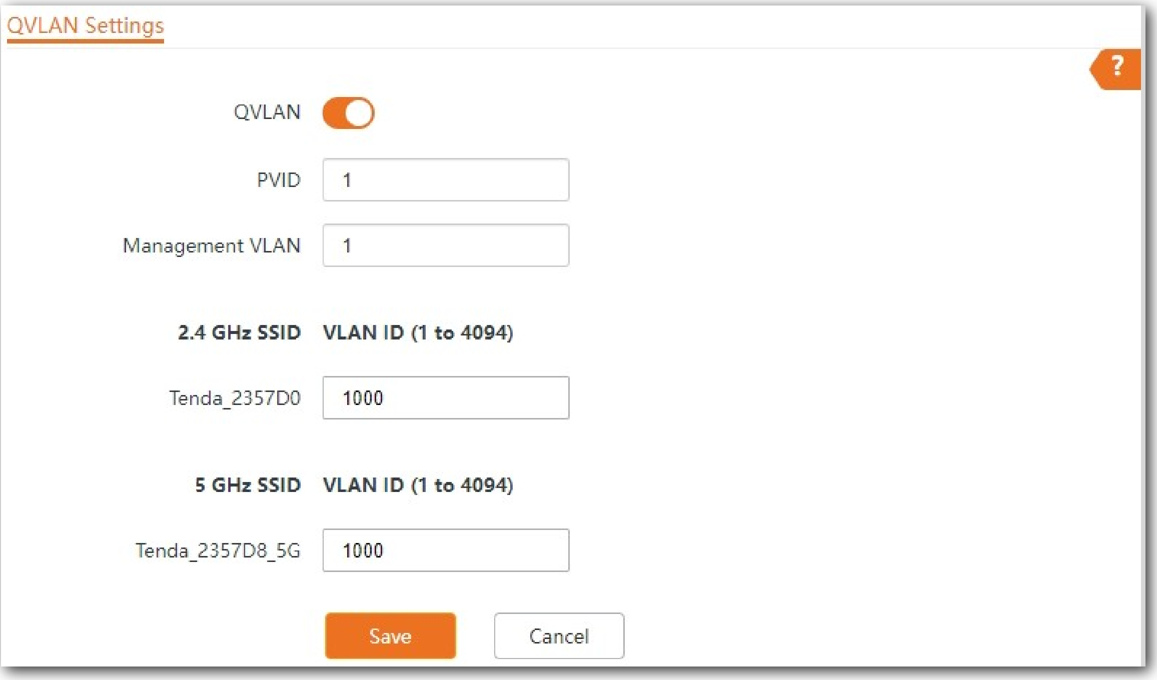
## 6.7.2 Configure the QVLAN function

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

**Step 2** Enable **QVLAN** function.

**Step 3** Change the parameters as required. Generally, you only need to change the **2.4 GHz SSID VLAN ID** and **5 GHz SSID VLAN ID** settings.

**Step 4** Click **Save**.



QVLAN Settings

QVLAN: ●

PVID: 1

Management VLAN: 1

2.4 GHz SSID — VLAN ID (1 to 4094)

Tenda_2357D0: 1000

5 GHz SSID — VLAN ID (1 to 4094)

Tenda_2357D8_5G: 1000

---End

**Parameter description**

| Parameter | Description |
|---|---|
| QVLAN | 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**. After the QVLAN function is enabled, the LAN port is the trunk port. Traffic of all VLANs can pass through a trunk port. |
| Management VLAN | It specifies the ID of the AP management VLAN. The default value is **1**.<br>After changing the management VLAN, you can manage the AP only after connecting your computer or access point controller to the new management VLAN. |
| 2.4 GHz SSID | It specifies the currently enabled SSID(s) over the 2.4 GHz band of the AP. |
| 5 GHz SSID | It specifies the currently enabled SSID(s) over the 5 GHz band of the AP. |
| VLAN ID | It specifies the VLAN IDs corresponding to SSIDs. By default, this value is **1000**.<br>After the QVLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID of an access port is the same as its VLAN ID. |

## 6.7.3 Example of configuring QVLAN

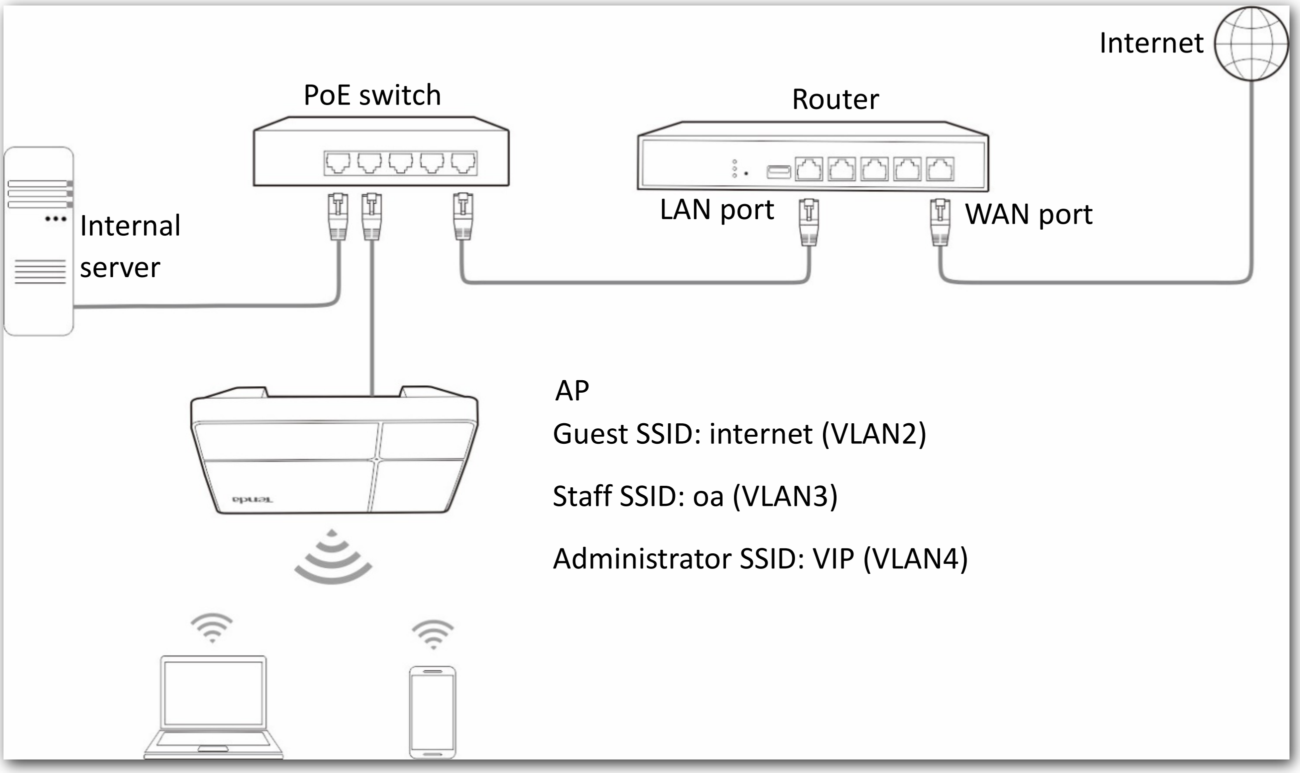
### Networking requirement

A hotel has the following WiFi network coverage requirements:

- Guests are allowed to connect to VLAN2 and only able to access the internet.
- Hotel staffs are allowed to connect to VLAN3 and only able to access the intranet.
- Hotel administrators are allowed to connect to VLAN4, able to access both the intranet and the internet.

Assume that the SSID for guests is **internet**, the SSID for staffs is **oa** and the SSID for administrators is **VIP**. The SSIDs are enabled and configured successfully on the AP.

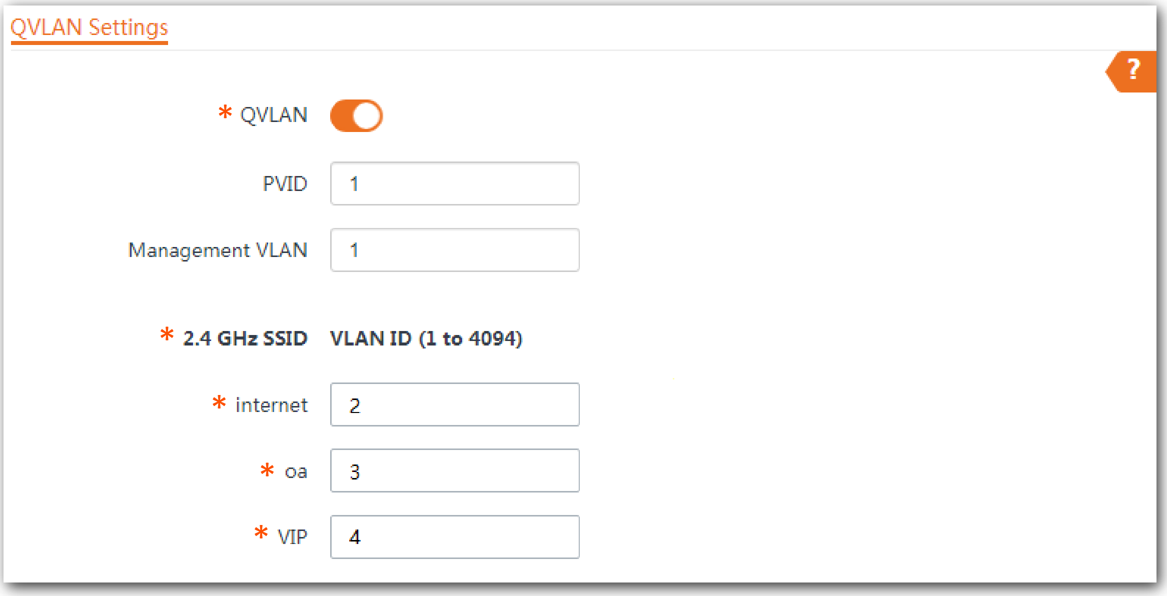
### Network topology



## Configuration procedure

**Step 1** Configure the AP.

1. Log in to the web UI of the AP and choose **Wireless** > **QVLAN Settings**.
2. Enable **QVLAN**.
3. Modify the VLAN IDs as shows in the following figure.



* QVLAN: enabled

PVID: 1

Management VLAN: 1

| * 2.4 GHz SSID | VLAN ID (1 to 4094) |
|---|---|
| * internet | 2 |
| * oa | 3 |
| * VIP | 4 |

4. Click **Save** to apply your settings.
5. Click **OK**. And wait for the AP completes rebooting.

**Step 2** Configure the switch.

Create IEEE 802.1q VLANs described in the following table on the switch. Retain the default settings of other ports. For details, refer to the user guide of the switch.

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

**Step 3** Configure the router and the internal server.

To ensure your wireless devices connected to the AP can access the internet, you should configure QVLAN function on your router and internal server which support QVLAN function. Detailed VLAN parameters are listed as follows:

VLAN parameters configured on your router:

| Port Connected To | Accessible VLAN ID | Port Type | PVID |
|---|---|---|---|
| Switch | 2, 4 | Trunk | 1 |

VLAN parameters configured on your internal server:

| Port Connected To | Accessible VLAN ID | Port Type | PVID |
|---|---|---|---|
| Switch | 3, 4 | Trunk | 1 |

For configuration details, refer to the user guides of your router and internal server.

**---- End**

## Verification

Wireless devices connected to the SSID **internet** can access only the internet. Wireless devices connected to the SSID **oa** can access only the intranet. Wireless devices connected to the SSID **VIP** can access both the internet and the intranet.

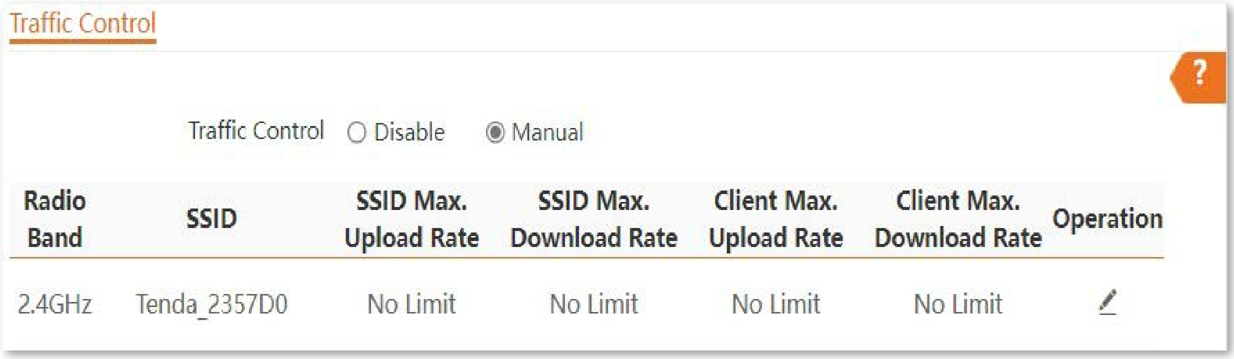
# 7 Advanced

## 7.1 Traffic control

### 7.1.1 Overview

The Traffic Control page allows you to set limits on the internet speed of clients to guarantee a proper allocation of limited broadband resources.

By default, the Traffic Control function is disabled. If you want to use this function, configure it on the **Advanced** > **Traffic Control** page. The following figure displays the page when Traffic Control is enabled.



Traffic Control ○ Disable ● Manual

| Radio Band | SSID | SSID Max. Upload Rate | SSID Max. Download Rate | Client Max. Upload Rate | Client Max. Download Rate | Operation |
|---|---|---|---|---|---|---|
| 2.4GHz | Tenda_2357D0 | No Limit | No Limit | No Limit | No Limit | ✎ |

**Parameter description**

| Parameter | Description |
|---|---|
| Traffic Control | - **Disable**: The Traffic Control function is disabled.<br>- **Manual**: The Traffic Control function is enabled. The network administrator manually set SSID and the maximum upload/download speed of user devices to limit the total bandwidth of SSID and evenly allocate bandwidth to users. In this way, if multiple SSIDs are enabled, and a user network with a lower priority (such as guest network) occupies an excessively high internet speed or a user occupies too much bandwidth, such circumstances as excessively low internet speed or even internet unavailability for other users will not occur. |
| Radio Band | It specifies the radio band of the WiFi network on which you want to set a traffic control rule. |
| SSID | It specifies the name of the WiFi network on which you want to set a traffic control rule. |

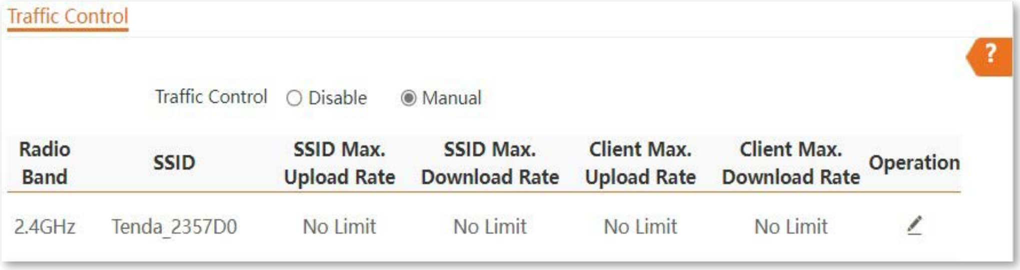
| Parameter | Description |
|---|---|
| SSID Max. Upload Rate<br>SSID Max. Download Rate | It specifies the maximum upload/download rate allowed for a WiFi network. If you leave it blank, the maximum upload/download rate of the target WiFi network are not limited. |
| Client Max. Upload Rate<br>Client Max. Download Rate | It specifies the maximum upload/download rate allowed for every user device connected to the target WiFi network. If you leave it blank, the maximum upload/download rate of every user device connected to the target WiFi network are not limited. |
| Operation | Click ✎ to set the maximum upload/download rate allowed for the target WiFi network and the maximum upload/download rate allowed for every user device connected to the target WiFi network. |

## 7.1.2 Configure traffic control

**Step 1** Click **Advanced** > **Traffic Control**.

**Step 2** Set **Traffic Control** to **Manual**.

**Step 3** On the **Traffic Control** list, click ✎ on the row where the WiFi network to be controlled resides.



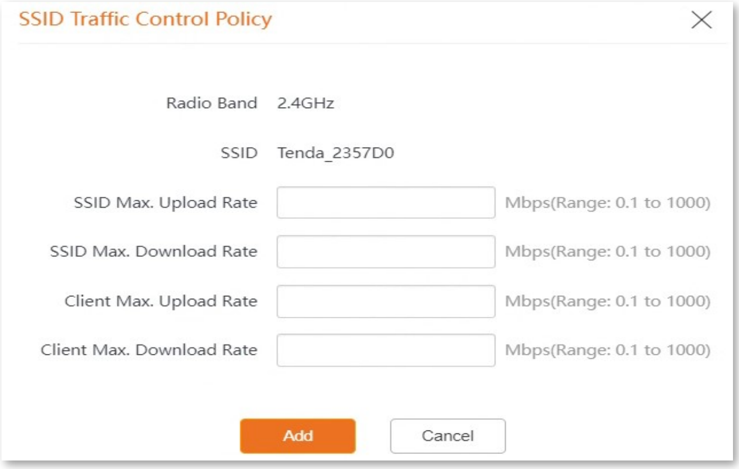
Traffic Control

Traffic Control ○ Disable ● Manual

| Radio Band | SSID | SSID Max. Upload Rate | SSID Max. Download Rate | Client Max. Upload Rate | Client Max. Download Rate | Operation |
|---|---|---|---|---|---|---|
| 2.4GHz | Tenda_2357D0 | No Limit | No Limit | No Limit | No Limit | ✎ |

**Step 4** Set the maximum upload/download rate allowed for the WiFi network and the maximum upload/download rate allowed for every user device connected to the WiFi network.

**Step 5** Click **Add**.



SSID Traffic Control Policy

Radio Band 2.4GHz

SSID Tenda_2357D0

SSID Max. Upload Rate Mbps(Range: 0.1 to 1000)

SSID Max. Download Rate Mbps(Range: 0.1 to 1000)

Client Max. Upload Rate Mbps(Range: 0.1 to 1000)

Client Max. Download Rate Mbps(Range: 0.1 to 1000)

**---- End**

# 7.2 SNMP

## 7.2.1 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 receiving network event alarms.

SNMP supports managing devices bought from various vendors automatically, regardless of physical differences among the devices.

### 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. Network Management System (NMS) is the most widely used SNMP manager in network environments. 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. This 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, defining a series of attributes of managed objects, including names, access permissions, and data types of objects. Each SNMP agent has its own MIB. An SNMP manager can read/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.

### Basic SNMP operations

The AP supports 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.

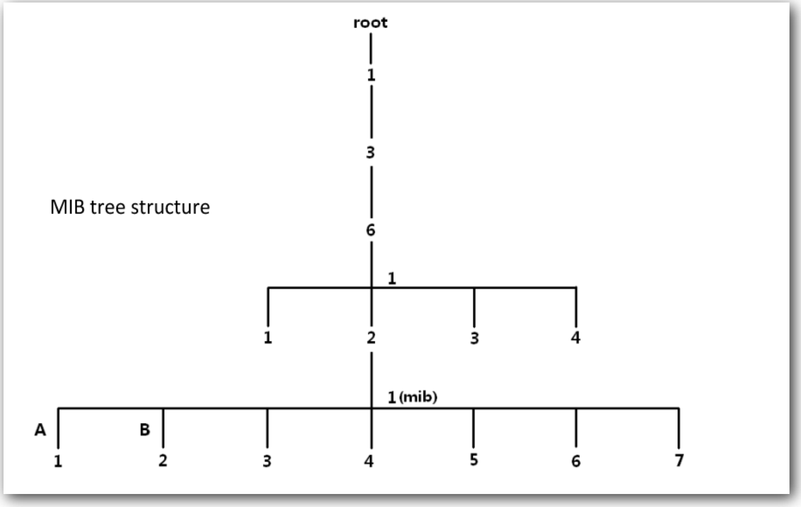
### SNMP protocol version

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.

### 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.



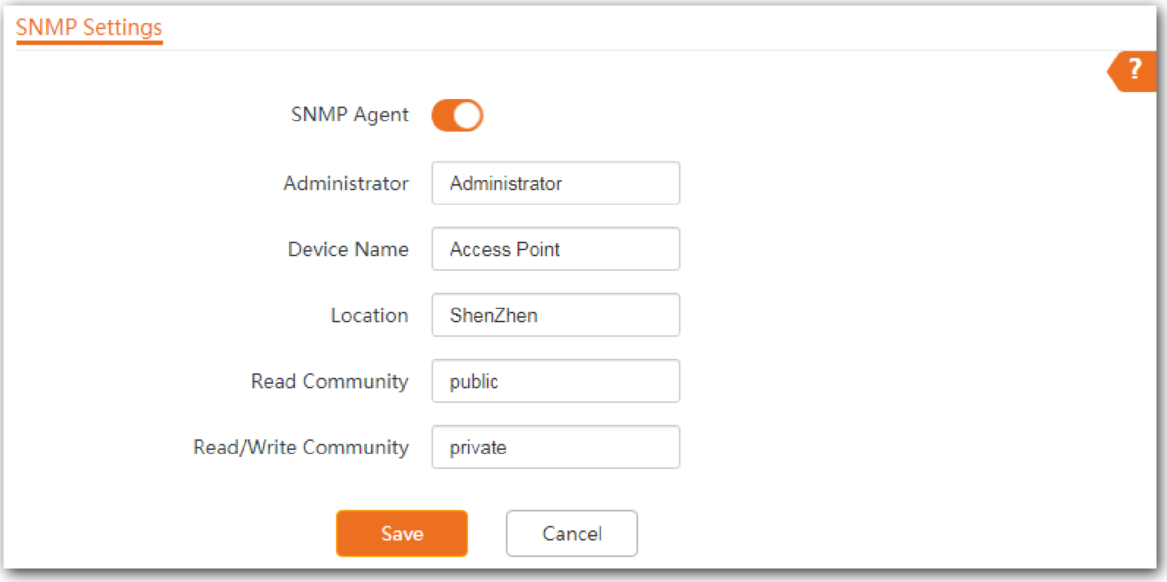
## 7.2.2 Configuring the SNMP function

**Step 1** Choose **Advanced** > **SNMP**.

**Step 2** Enable **SNMP Agent**.

**Step 3** Set related parameters.

**Step 4** Click **Save** to apply your settings.



SNMP Settings

SNMP Agent: ●

Administrator: Administrator

Device Name: Access Point

Location: ShenZhen

Read Community: public

Read/Write Community: private

---- End

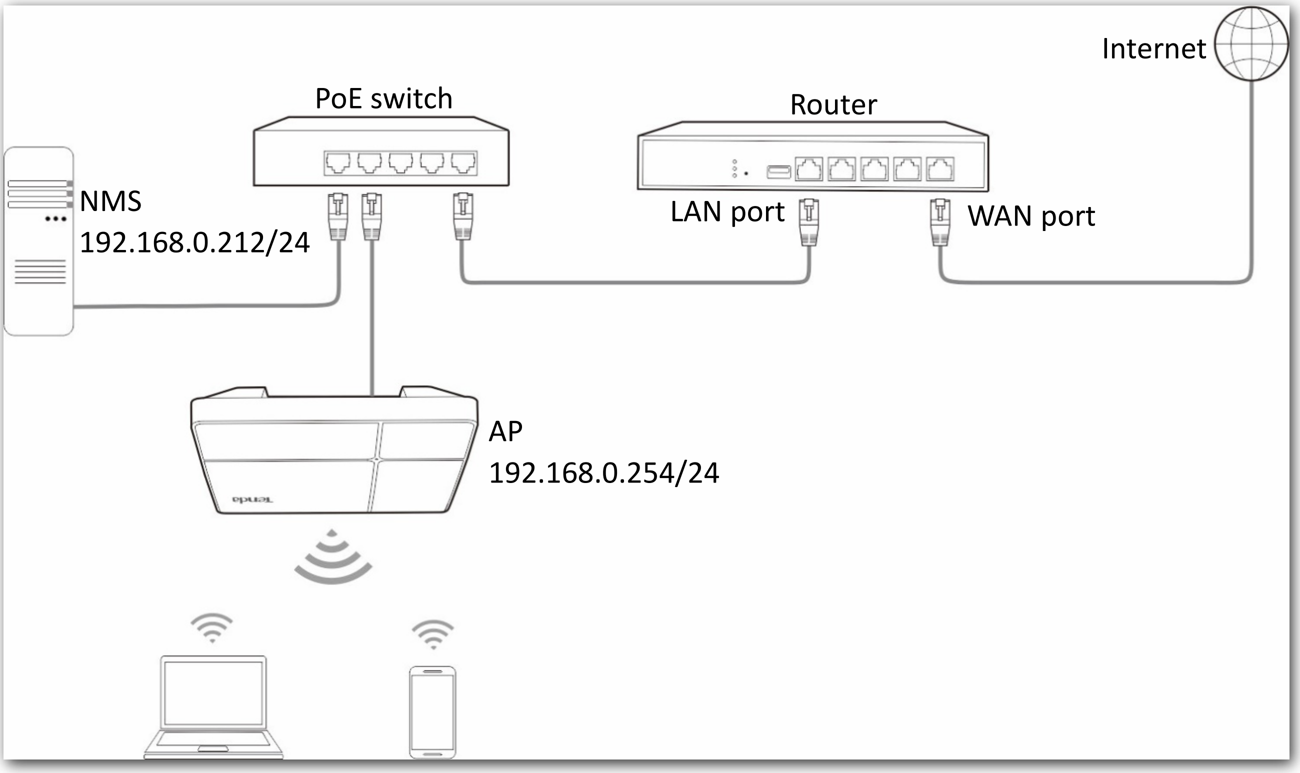
## Parameter description

| Parameter | Description |
|---|---|
| SNMP Agent | It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled.<br>An SNMP manager and the SNMP agent can communicate with each other only when their SNMP versions are the same. Currently, the SNMP agent function of the AP supports SNMP V1 and SNMP V2C. |
| Administrator | It specifies the administrator's name of the AP. The default name is **Administrator**. You can modify the administrator's name if required. |
| Device Name | It specifies the device name of the AP. By default, the device name is **Access Point**. You can modify it if required.<br>TIP<br>You are recommended to modify the AP name so that you can identify your AP easily when managing the AP using SNMP. |
| Location | It specifies the location where the AP is used. The default location is **ShenZhen**. You can modify the location according to your actual situation. |
| Read Community | It specifies the read password shared between SNMP managers and the SNMP agent. The default password is **public**.<br>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 the SNMP agent. The default password is **private**.<br>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. |

## 7.2.3 Example of configuring SNMP settings

### Networking requirement

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

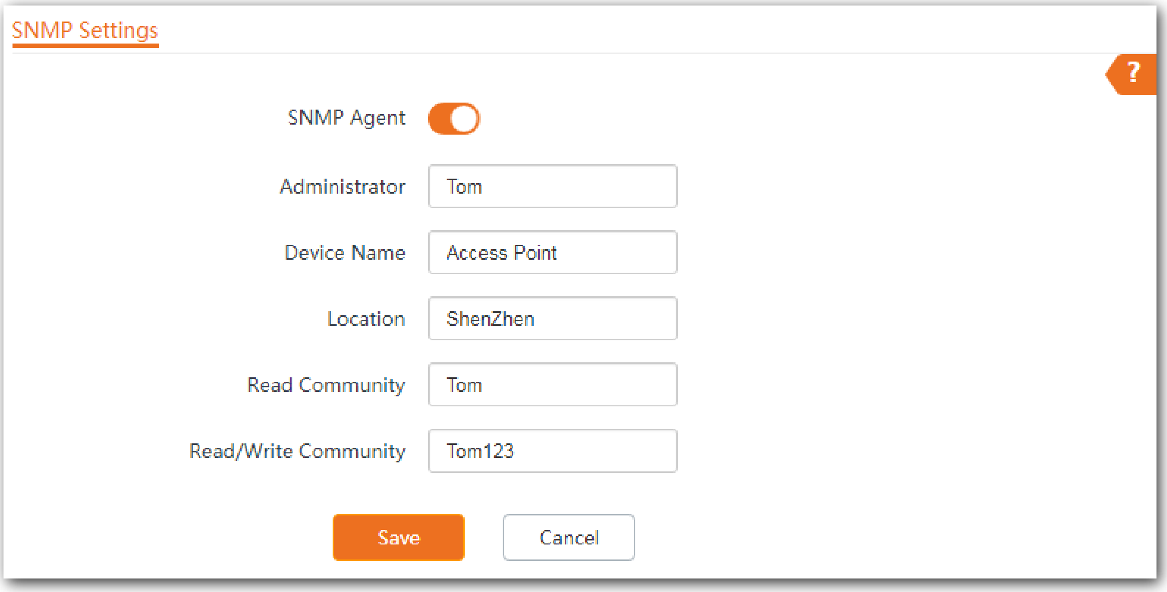


## Configuration procedure

**Step 1** Configure the AP.

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

1. Log in to the web UI of the AP and choose **Advanced** > **SNMP**.
2. Set **SNMP Agent** to **Enable**.
3. Set the SNMP parameters: **Administrator**, **Device Name**, **Location**, **Read Community**, **Read/Write Community**.
4. Click **Save** to apply your settings.



SNMP Settings

SNMP Agent: ●

|  |  |
|---|---|
| Administrator | Tom |
| Device Name | Access Point |
| Location | ShenZhen |
| Read Community | Tom |
| Read/Write Community | Tom123 |

**Step 2** Configure the NMS.

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

**---- End**

## Verification

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

# 8 Tools

## 8.1 Date & time

This section allows you to set the system time and login timeout interval of your AP.

### 8.1.1 System time

This function is used to set the system time. To make the time-related functions effective, ensure that the system time of the AP is set correctly. The AP supports **Sync with Internet Time** and **Manual** to correct the system time.

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

#### Configuring AP to 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. The AP can also self-calibrate after restarting, without the need for network administrators to reset.

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

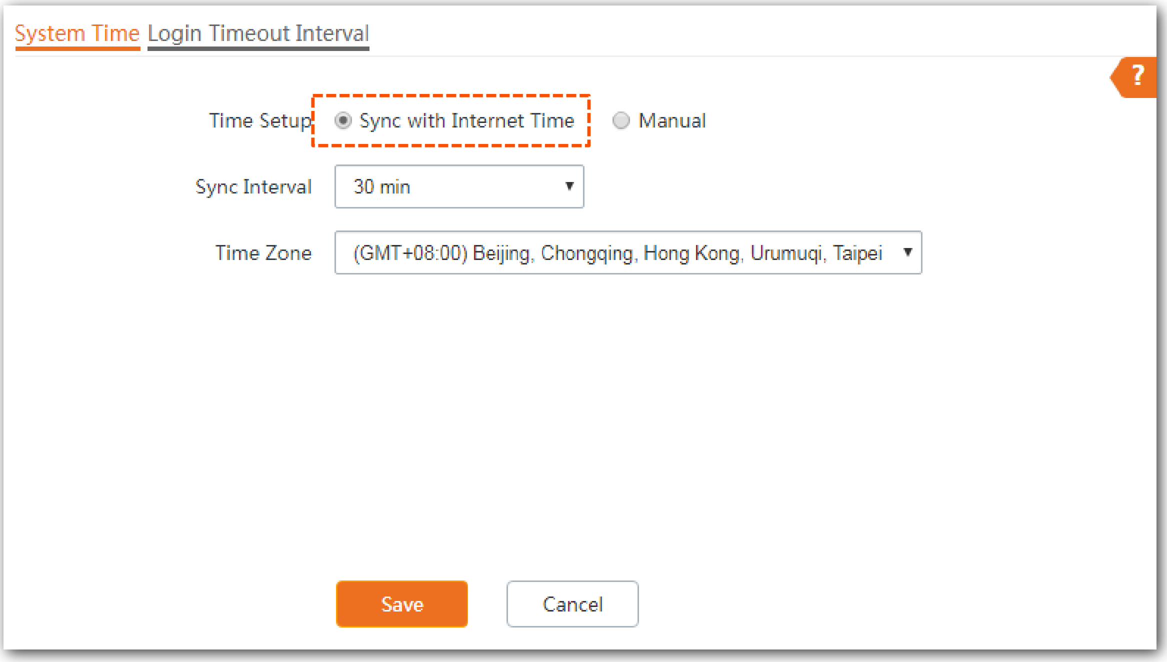
**Step 1** Choose **Tools** > **Date & Time** > **System Time**.

**Step 2** Tick the **Sync with Internet Time** box.

**Step 3** Select a value from the **Sync Interval** drop-down list menu as required, which is **30 min** in this example.

**Step 4** Choose the **Time Zone** where the AP locates.

**Step 5** Click **Save** to apply your settings.



Time Setup ● Sync with Internet Time ○ Manual

Sync Interval 30 min

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

---- End

The AP synchronizes with the internet time every 30 minutes.

## Configuring date and time manually

The network administrator manually sets the system time of the AP. With this method, you need to manually reconfigure the system time each time the AP reboots.

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

Step 2 For manual setup, you can:

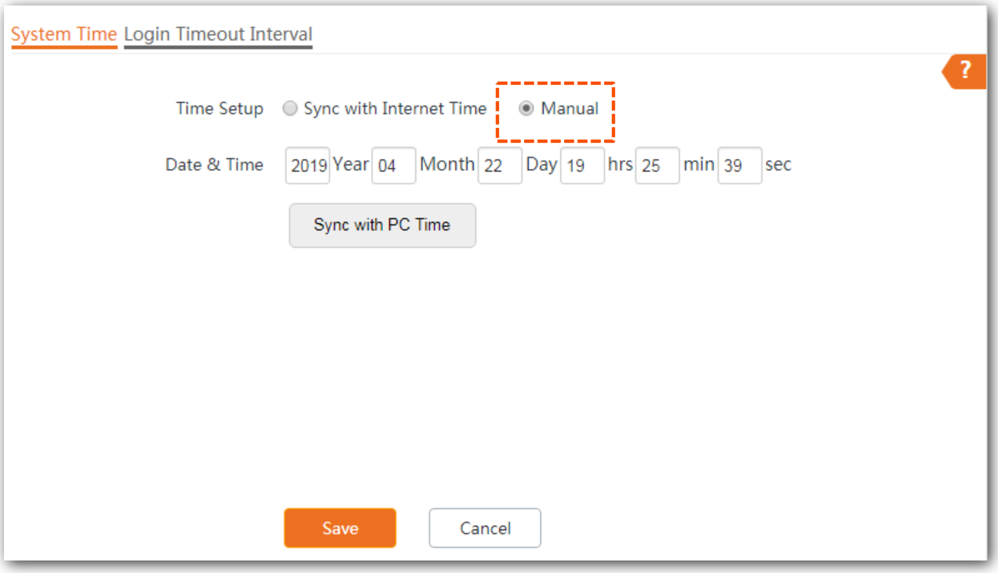
Option one: Enter a correct date and time manually.

Option two: Click **Sync with PC Time**, the AP auto-fills the system time of your management computer in the **Date & Time** fields.

TIP

Make sure that the system time of your management computer is correct.

Step 3 Click **Save** to apply your settings.



System Time | Login Timeout Interval

Time Setup ○ Sync with Internet Time ● Manual

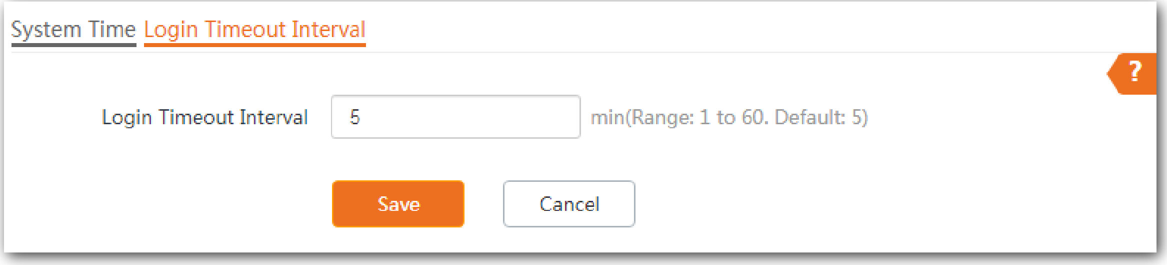
Date & Time 2019 Year 04 Month 22 Day 19 hrs 25 min 39 sec

**---- End**

## 8.1.2 Configuring 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 automatically for network security.

The default login timeout interval is **5** minutes. The Login Timeout Interval page allows you to modify the login timeout interval. To access the page, choose **Tools** > **Date & Time** > **Login Timeout Interval**.



System Time | Login Timeout Interval

Login Timeout Interval 5 min(Range: 1 to 60. Default: 5)

## 8.2 Maintenance

The Maintenance page allows you to reboot and reset AP, upgrade firmware, back up or restore settings, and control LED indicator.

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

### 8.2.1 Reboot

If a parameter does not take effect or the AP does not work properly, you can try rebooting the AP to resolve the problem.

The AP supports two rebooting methods:

- Manual Reboot: Reboot the AP by clicking the Reboot button.
- Reboot Schedule: Let the AP reboot at the specified time or interval you set.

TIP

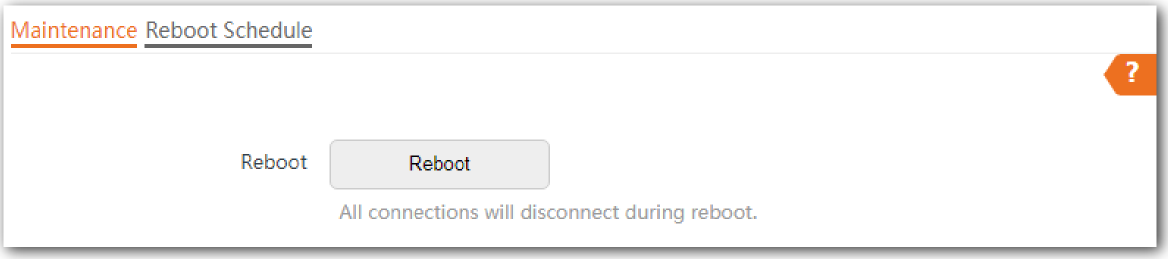
Rebooting the AP disconnects all connections. You are recommended to reboot the AP in spare time.

#### Manual reboot

Step 1 Choose **Tools** > **Maintenance**.

Step 2 Click **Reboot**.

Step 3 Click **OK** on the pop-up window.



All connections will disconnect during reboot.

---- End

Wait for the AP completes rebooting.

#### Reboot schedule

You can let the AP reboot:

- At interval: The AP reboots at the interval you set.
- At specified time: The AP reboots regularly at the time you set.

## ■ Configuring the AP to reboot at an interval

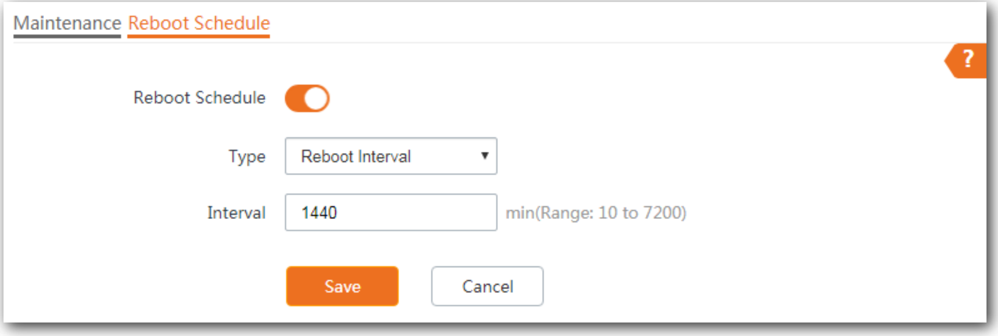
**Step 1** Click **Tools** > **Maintenance**, and click the **Reboot Schedule** tab.

**Step 2** Enable **Reboot Schedule**.

**Step 3** Select **Reboot Interval** from the **Type** drop-down list menu.

**Step 4** Set **Interval** as required, which is **1440** minutes in this example.

**Step 5** Click **Save** to apply your settings.



Maintenance Reboot Schedule

Reboot Schedule: ●

Type: Reboot Interval ▾

Interval: 1440 min(Range: 10 to 7200)

**---- End**

After the configurations, the AP will automatically reboot in a day.

## ■ Configuring the AP to reboot at specified time

**Step 1** Click **Tools** > **Maintenance**, and click the **Reboot Schedule** tab.

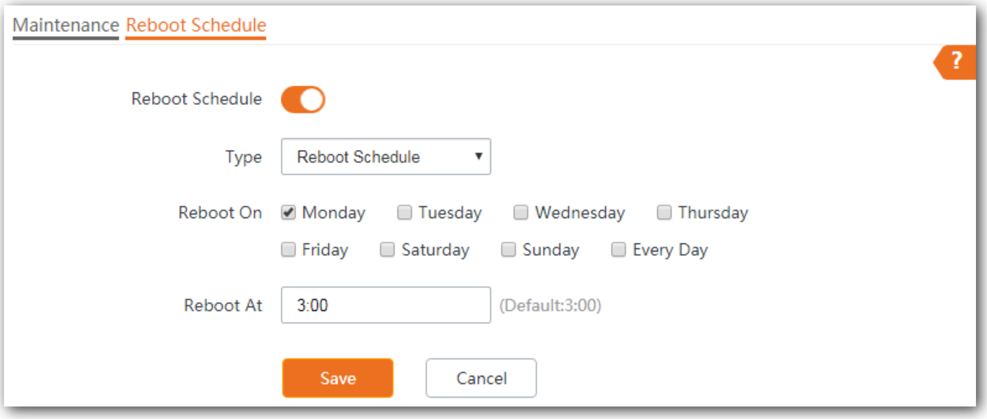
**Step 2** Enable **Reboot Schedule**.

**Step 3** Select **Reboot Schedule** from the **Type** drop-down list menu.

**Step 4** Select the required day(s) when the AP reboots, which is **Monday** in this example.

**Step 5** Set the time when the AP reboots, which is **3:00** in this example.

**Step 6** Click **Save** to apply your settings.



Maintenance Reboot Schedule

Reboot Schedule: ●

Type: Reboot Schedule ▾

Reboot On: ☑ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday □ Every Day

Reboot At: 3:00 (Default:3:00)

**---- End**

The AP reboots at 3:00 every Monday.

## 8.2.2 Reset

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**.

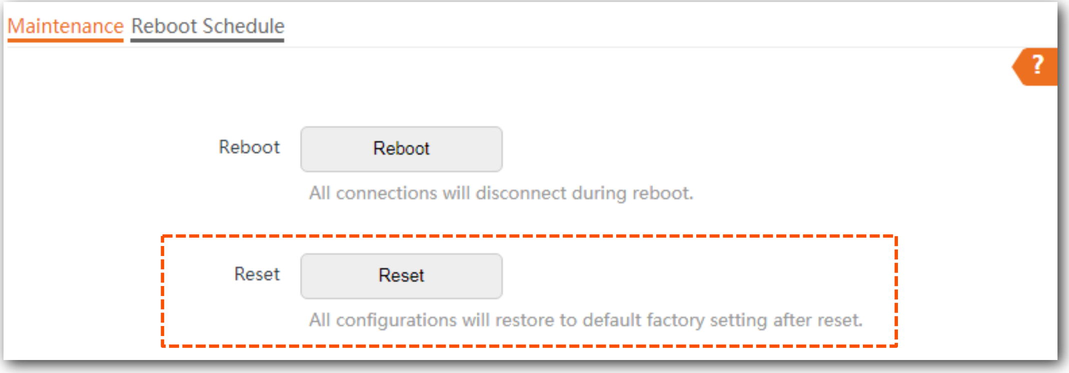
**Method 1:**

After AP completes startup, hold down the reset button (**RESET** or **Reset**) for about 8 seconds. When the indicator of the AP blinks again, the AP completes resetting.

**Method 2:**

Step 1 Click **Tools** > **Maintenance**.

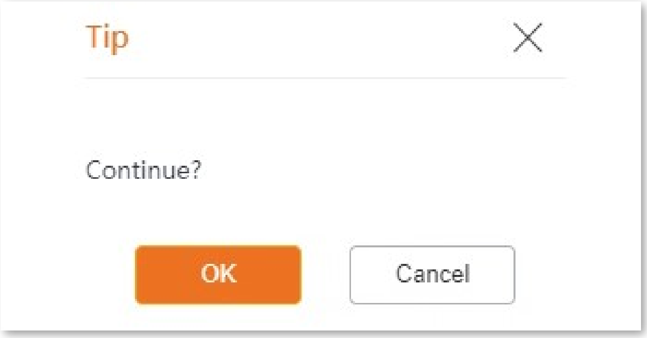
Step 2 Click the **Reset** button.



All connections will disconnect during reboot.

All configurations will restore to default factory setting after reset.

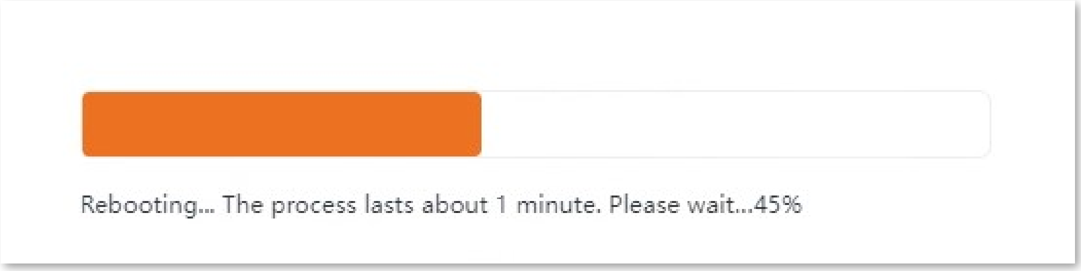
Step 3 Click **OK** on the pop-up window.



Continue?

---- End

Wait until the progress bar completes.



Rebooting... The process lasts about 1 minute. Please wait...45%

### 8.2.3 Upgrade firmware

This function enables you to upgrade the AP's firmware to get more functions and higher stability.

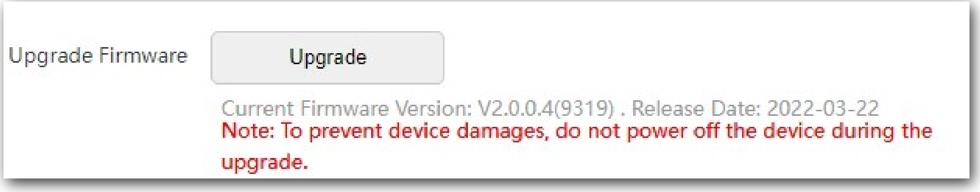
NOTE

To enable your AP to work properly after an upgrade, ensure that the firmware used to upgrade complies with your product model. When upgrading, do not power off the AP.

**Step 1** Download the latest firmware version for the AP from http://www.tendacn.com to your local computer and decompress the package.

**Step 2** Log in to the web UI of the AP, navigate to **Tools** > **Maintenance** > **Maintenance**.

**Step 3** Click **Upgrade**.

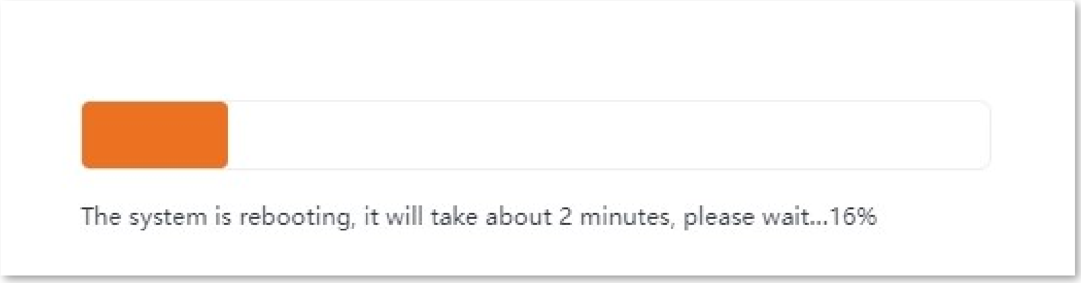


Current Firmware Version: V2.0.0.4(9319) . Release Date: 2022-03-22
Note: To prevent device damages, do not power off the device during the upgrade.

**Step 4** Select and upload the firmware that has been downloaded to your computer.

---- End

Wait until the progress bar completes. Then log in to the web UI of the AP again. Click **Status** > **System Status** and check whether the upgrade is successful according to the **Firmware Version** parameter.



The system is rebooting, it will take about 2 minutes, please wait...16%

TIP

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.

## 8.2.4 Backup and restoring configurations

The backup function is used to export the current configuration of the AP to your computer. The restore function is used to import a configuration file to the AP.

You are recommended to back up the configuration after it is significantly changed. When the performance of your AP decreases because of an improper configuration, or after you restore the AP to factory settings, you can use this function to restore a configuration that has been backed up.

TIP

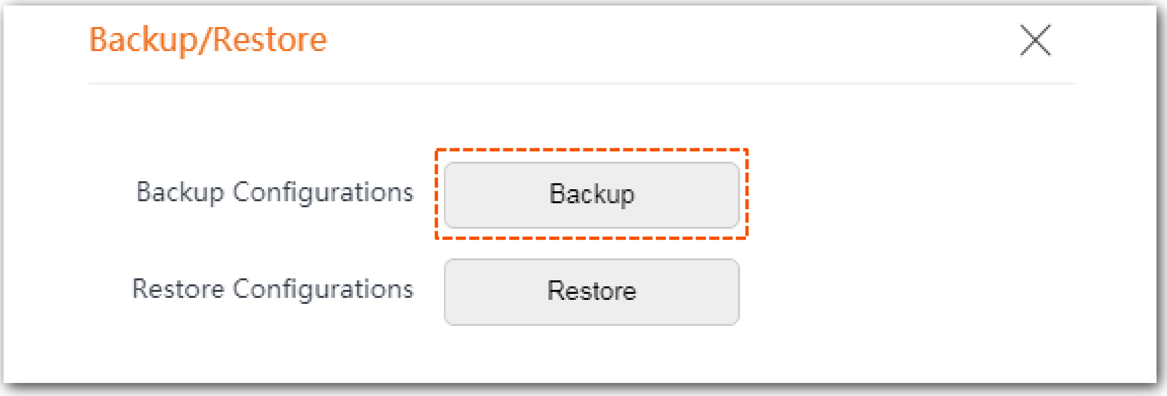
If you need to apply same or similar configuration to many APs, you can configure one of the APs, back up its configuration, and use the backup configuration file to restore the configuration of other APs.

### Backup the current configuration

**Step 1** Click **Tools** > **Maintenance** > **Maintenance**.

**Step 2** Click **Backup/Restore**.

**Step 3** Click **Backup** on the pop-up window.



---- End

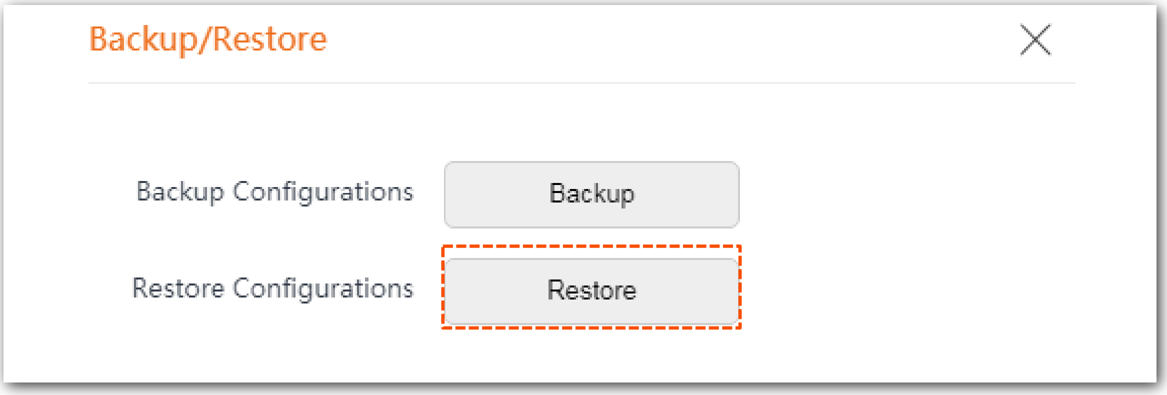
A configuration file indicated with **APCfm.cfg** will be downloaded.

## Restoring previous configuration

**Step 1** Click **Tools** > **Maintenance** > **Maintenance**.

**Step 2** Click **Backup/Restore**.

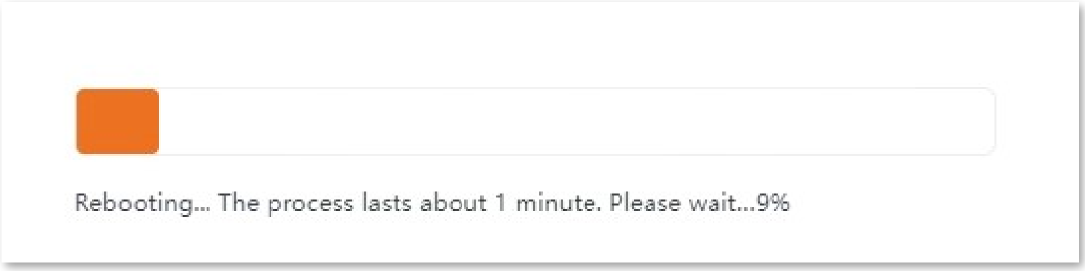
**Step 3** Click **Restore** on the pop-up window.



**Step 4** Choose the configuration file you backed up.

**---- End**

Wait until the progress bar completes.



Rebooting... The process lasts about 1 minute. Please wait...9%

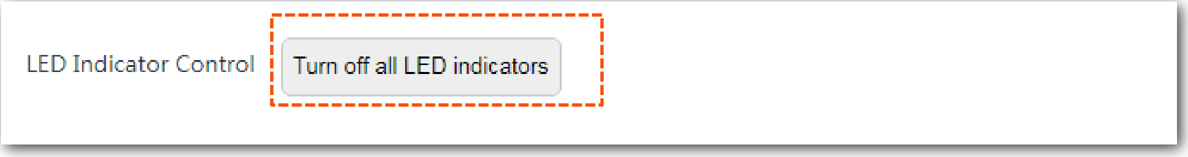
## 8.2.5 LED indicator control

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

### Turn off the LED indicator

**Step 1** Click **Tools** > **Maintenance** > **Maintenance**.

**Step 2** Click **Turn off all LED indicators**.



**---- End**

After the configurations, the LED indicator is turned off and no longer displays the working status of the AP.

### Turn on the LED indicator

**Step 1** Click **Tools** > **Maintenance** > **Maintenance**.

**Step 2** Click **Turn on all LED indicators**.

**---- End**

After the configurations, the LED indicator lights up again and you can judge the working status of the AP.

# 8.3 Account

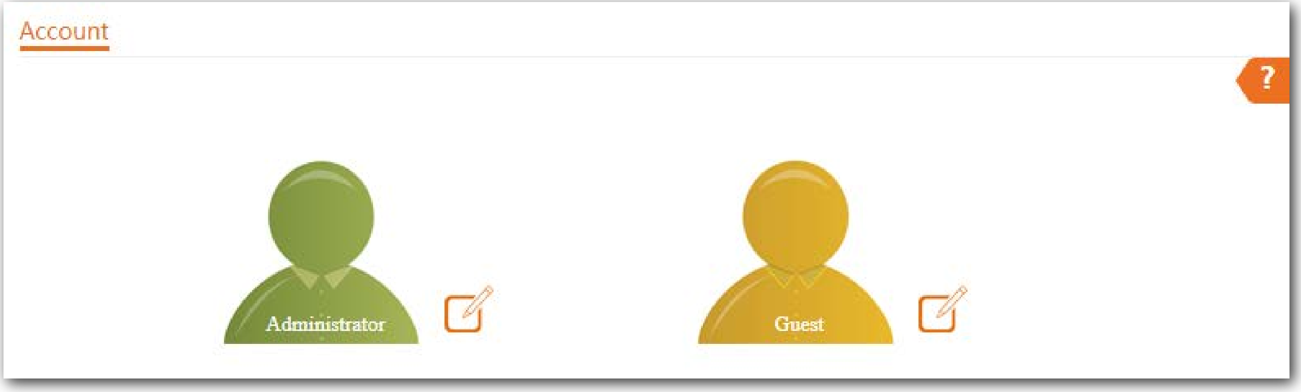
## 8.3.1 Overview

The Account page allows you to modify the information of the login account to keep unauthorized users from entering the web UI and modifying configurations, thus protecting the wireless network.

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

The router supports two account types: **Administrator** and **Guest**. The difference between them is their permission.

- The **Administrator** account has permission to view and modify the settings. The default username and password for this account are **admin/admin** (both are case-sensitive). You can view and modify it here.
- The **Guest** account can only view other than modifying the settings. The default username and password for this account are **user/user** (both are case-sensitive). You can view it here.



### 8.3.2 Modifying the password and user name of login account

**Step 1** Click **Tools** > **Account** to enter the configuration page.

**Step 2** Click ✎ beside the account to be modified.

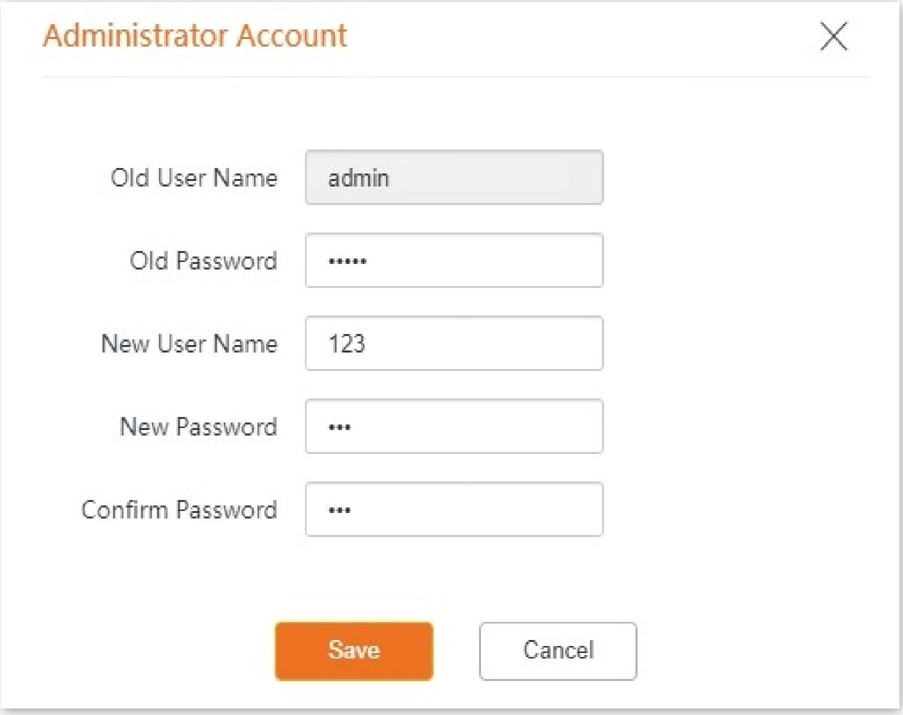
**Step 3** Enter the current password in **Old Password**.

**Step 4** Enter the new account name, for example, **123**, in **New User Name**.

**Step 5** Enter the new password in **New Password**.

**Step 6** Enter again the new password in **Confirm Password**.

**Step 7** Click **Save**.



Administrator Account

| | |
|---|---|
| Old User Name | admin |
| Old Password | ••••• |
| New User Name | 123 |
| New Password | ••• |
| Confirm Password | ••• |

**---- End**

# 8.4 System Log

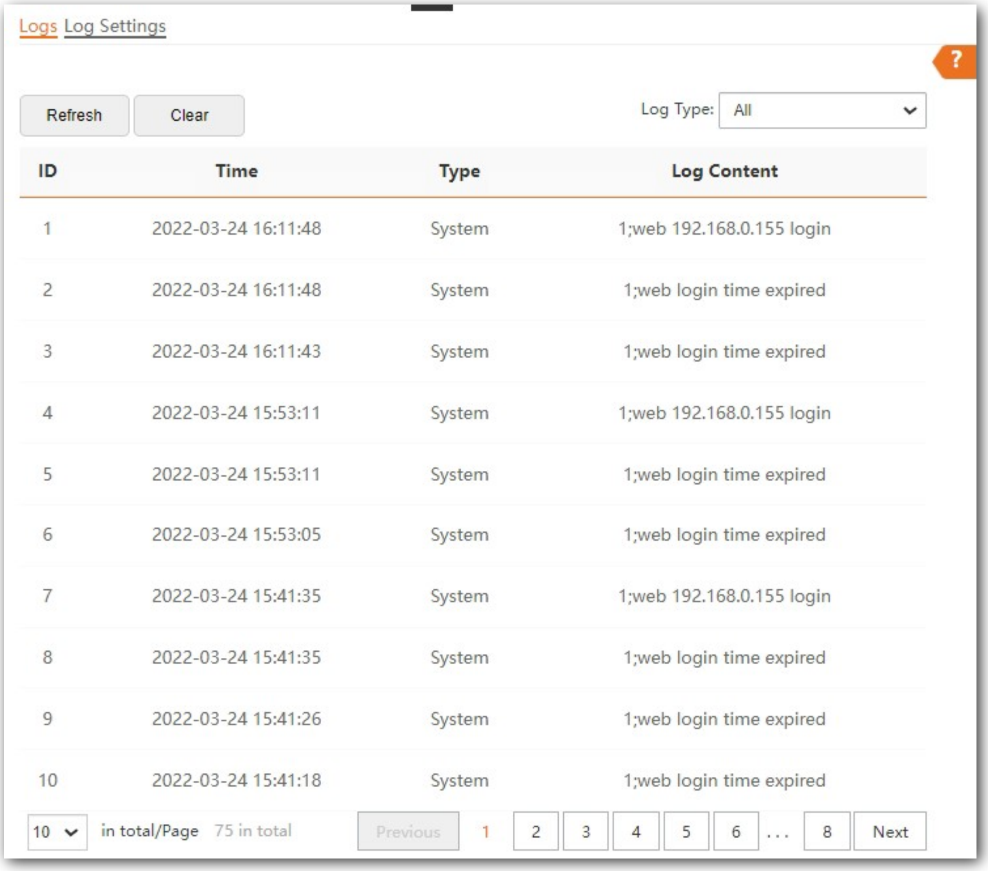
This section allows you to view system logs and configure log servers.

## 8.4.1 Viewing system logs

System logs record information about system running status and the operation you performed on it. When system malfunctions occur, you can use system log for troubleshooting.

The Logs page allows you to view system logs.

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



| ID | Time | Type | Log Content |
|---|---|---|---|
| 1 | 2022-03-24 16:11:48 | System | 1;web 192.168.0.155 login |
| 2 | 2022-03-24 16:11:48 | System | 1;web login time expired |
| 3 | 2022-03-24 16:11:43 | System | 1;web login time expired |
| 4 | 2022-03-24 15:53:11 | System | 1;web 192.168.0.155 login |
| 5 | 2022-03-24 15:53:11 | System | 1;web login time expired |
| 6 | 2022-03-24 15:53:05 | System | 1;web login time expired |
| 7 | 2022-03-24 15:41:35 | System | 1;web 192.168.0.155 login |
| 8 | 2022-03-24 15:41:35 | System | 1;web login time expired |
| 9 | 2022-03-24 15:41:26 | System | 1;web login time expired |
| 10 | 2022-03-24 15:41:18 | System | 1;web login time expired |

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

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

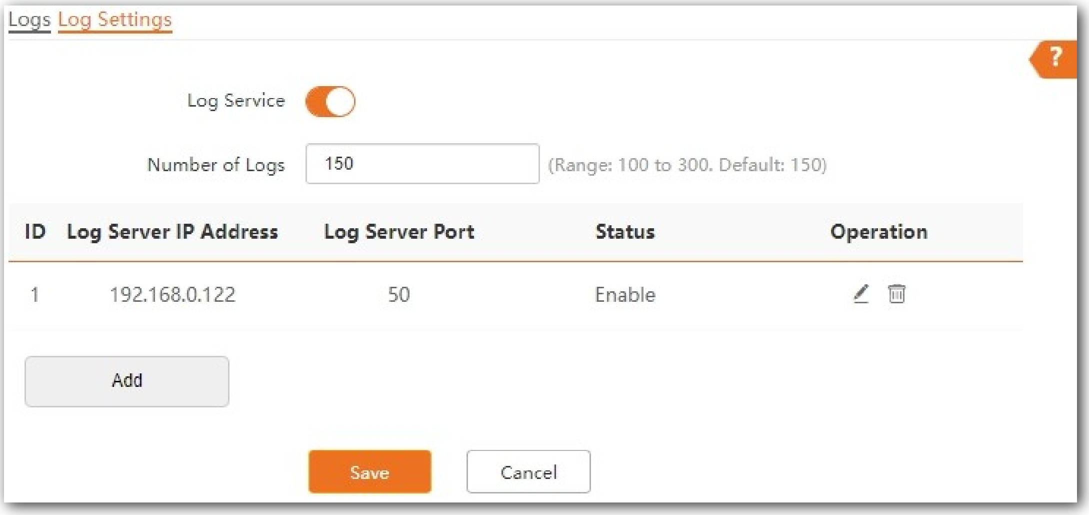
NOTE

- 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 restored, or the factory settings are restored.

## 8.4.2 Log settings

The Log Settings page allows you to set the number of logs to be displayed and configure log servers.

To access the page, choose **Tools** > **System Log** > **Log Settings**.



Logs Log Settings

Log Service

Number of Logs 150 (Range: 100 to 300. Default: 150)

| ID | Log Server IP Address | Log Server Port | Status | Operation |
|---|---|---|---|---|
| 1 | 192.168.0.122 | 50 | Enable | ✎ 🗑 |

Add

Save Cancel

### Parameter description

| Parameter | Description |
|---|---|
| Log Service | It specifies whether to enable the log service function. This function is disabled by default.<br>You can modify the number of logs to be displayed and configure log server only if the Log Service function is enabled. |
| Number of Logs | It specifies the largest number of logs that can be displayed on the web UI. |
| Log Server IP Address | It specifies the IP address of the log server.<br>To ensure that system logs can be sent to the log server, set the **IP Address**, **Subnet Mask** and **Default Gateway** of the AP on the **Internet Settings** > **LAN Setup** page to enable the AP to access the log server. |
| Log Server Port | It specifies the port (514 by default) used by the log service. It should be the same port with the port configured by the log server. |
| Status | It specifies the status of the log server rule. |
| Operation | It specifies the operations you can perform on the log server:<br>- Click ✎ to modify the IP address, port, or status of the log server.<br>- Click 🗑 to delete the target log server. |
| Add | Click it to add a log server. |

## Modifying number of logs to be displayed on Web UI

The web UI of the AP can display up to 150 logs by default, and you can modify them as required.

Step 1 Choose **Tools** > **System Log > Log Settings**.

Step 2 Enable **Log Service**.

Step 3 Modify the **Number of Logs** as required.

Step 4 Click **Save**.

**---- End**

## Log settings

After you configure a log server, AP automatically synchronizes system logs to the log server you configured. You can view all the logs on the log server.

NOTE

To ensure that system logs can be sent to the log server, set the **IP Address**, **Subnet Mask** and **Default Gateway** of the AP on the **Internet Settings** > **LAN Setup** page to enable the AP to access the log server.

- Add a Log Server

Step 1 Choose **Tools** > **System Log > Log Settings**.

Step 2 Enable **Log Service**.

Step 3 Click **Add**.

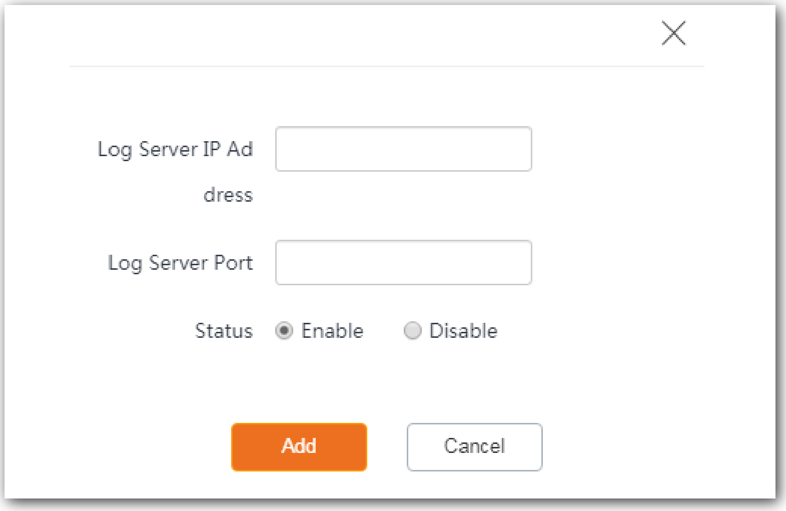
Step 4 Perform the following procedures:

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

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

(3) Set **Status** to **Enable**.

(4) Click **Add**.



Log Server IP Ad dress

Log Server Port

Status ● Enable ○ Disable

**Step 5** Click **Save**.

**---- End**

- Modify a Log Server

**Step 1** Choose **Tools** > **System Log > Log Settings**.

**Step 2** Enable **Log Service**.

**Step 3** Click ✎ to modify the target log server in the operation column of the log server list.

**Step 4** Modify the parameters as required in the pop-up page. Then click **Add**.

**Step 5** Click **Save**.

**---- End**

- Delete a Log Server

**Step 1** Choose **Tools** > **System Log > Log Settings**.

**Step 2** Enable **Log Service**.

**Step 3** Click 🗑 to delete the target log server in the operation column of the log server list.

**Step 4** Click **Save**.

**---- End**

## 8.5 Diagnostic tool

The AP supports Ping command, which is used to check whether or not the connection between the AP and a specified host is correct and the connection quality when facing network reachability issues.

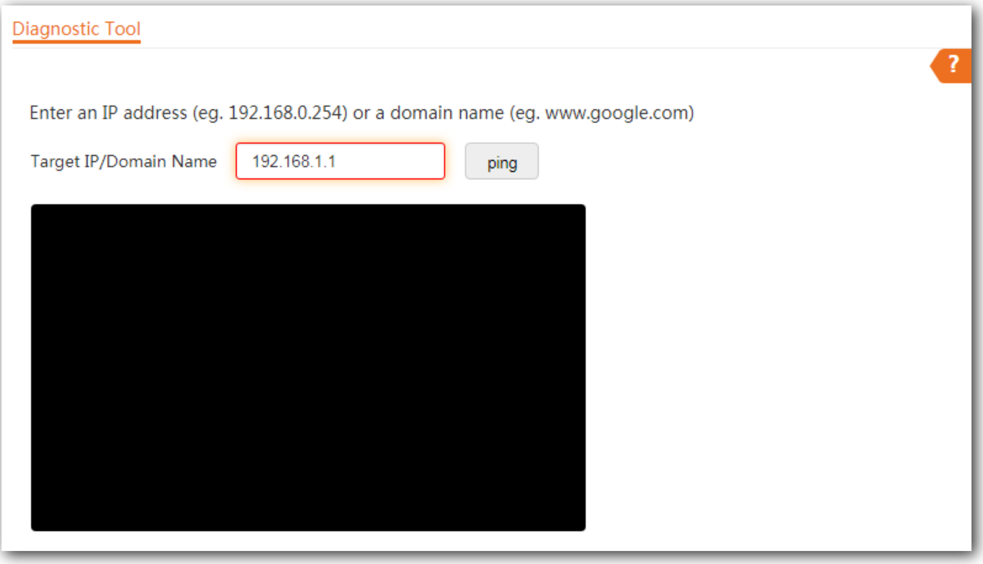
**Executing Ping command**

Assume that you need to check the connection quality between the AP and its upstream router:

Step 1 Choose **Tools** > **Diagnostic Tool** to enter the configuration page.

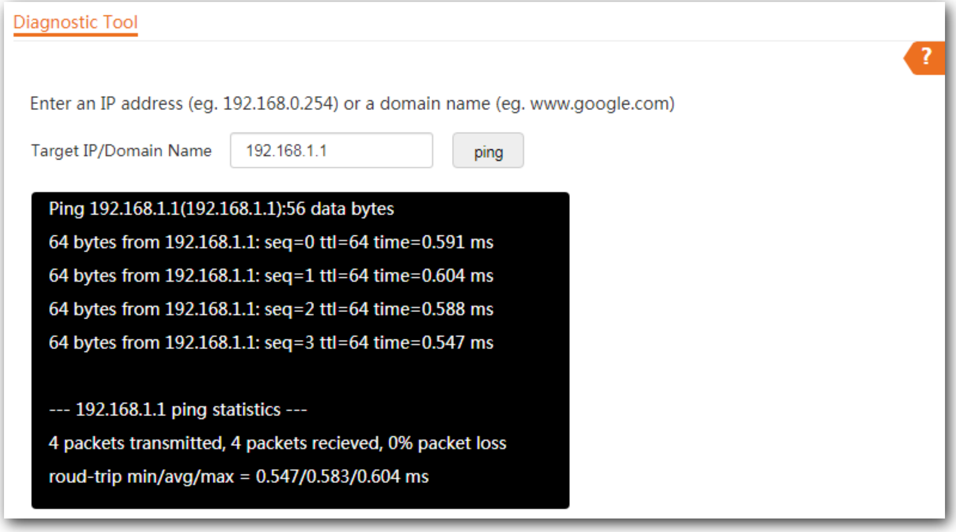
Step 2 Enter the IP address of its upstream router in the **Target IP/Domain Name** box, which is **192.168.1.1** in this example.

Step 3 Click **ping**.


Diagnostic Tool
?
Enter an IP address (eg. 192.168.0.254) or a domain name (eg. www.google.com)
Target IP/Domain Name
192.168.1.1
ping

---- End

Wait a moment. The Ping result is displayed in the black square. See the following figure:


Diagnostic Tool
?
Enter an IP address (eg. 192.168.0.254) or a domain name (eg. www.google.com)
Target IP/Domain Name
192.168.1.1
ping

```
Ping 192.168.1.1(192.168.1.1):56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.591 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.604 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.588 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.547 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets recieved, 0% packet loss
roud-trip min/avg/max = 0.547/0.583/0.604 ms
```

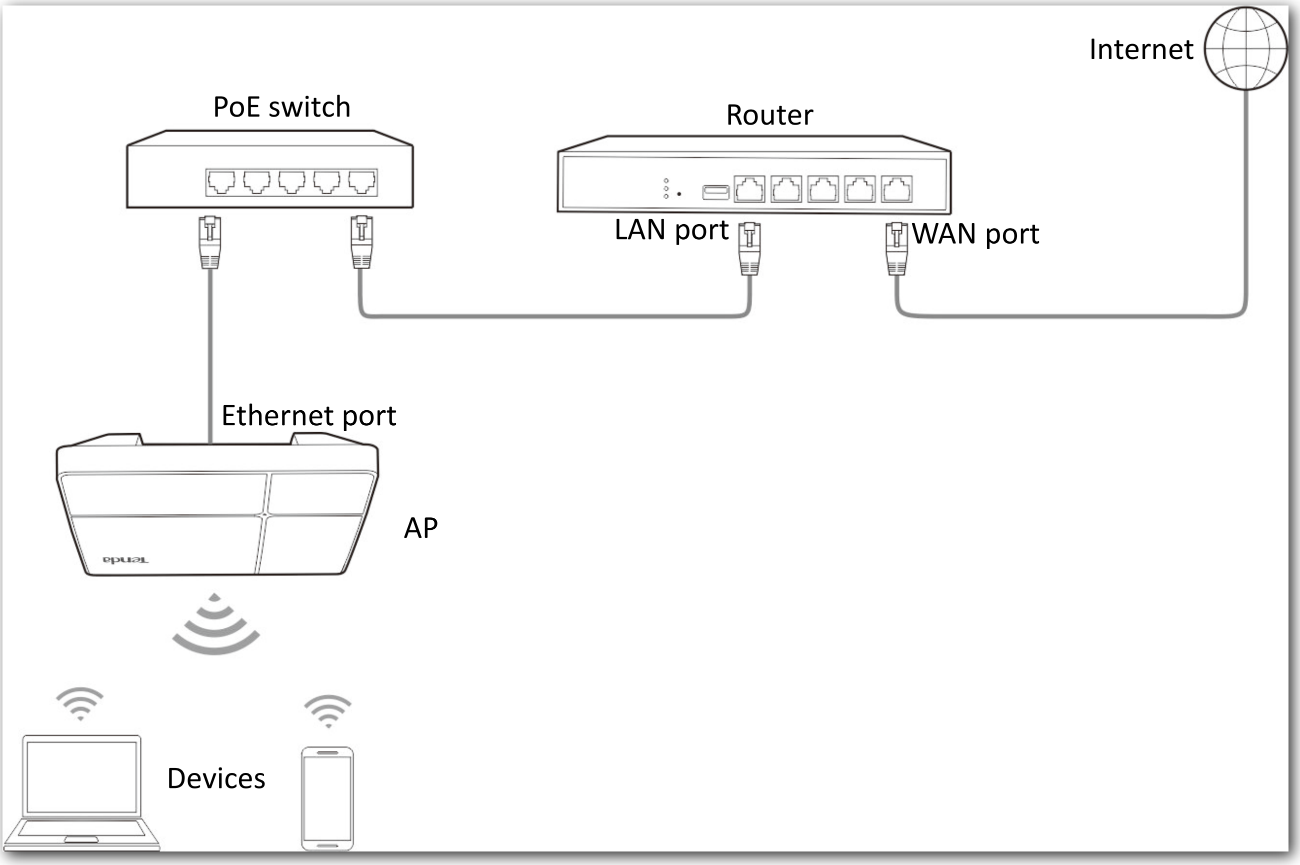
# 8.6 Uplink check

## 8.6.1 Overview

In AP mode, the AP connects to its upstream network using the LAN port. If a critical node between the LAN port and the upstream network fails, the AP as well as the wireless devices connected to the AP cannot access the upstream network. If uplink detection is enabled, the AP regularly pings specified hosts through the LAN port. If all the hosts are not reachable, the AP stops its wireless service and wireless devices cannot find the SSIDs of the AP. The device 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 devices can connect to the upstream network through another nearby AP that works properly.

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



## 8.6.2 Configuring uplink detection

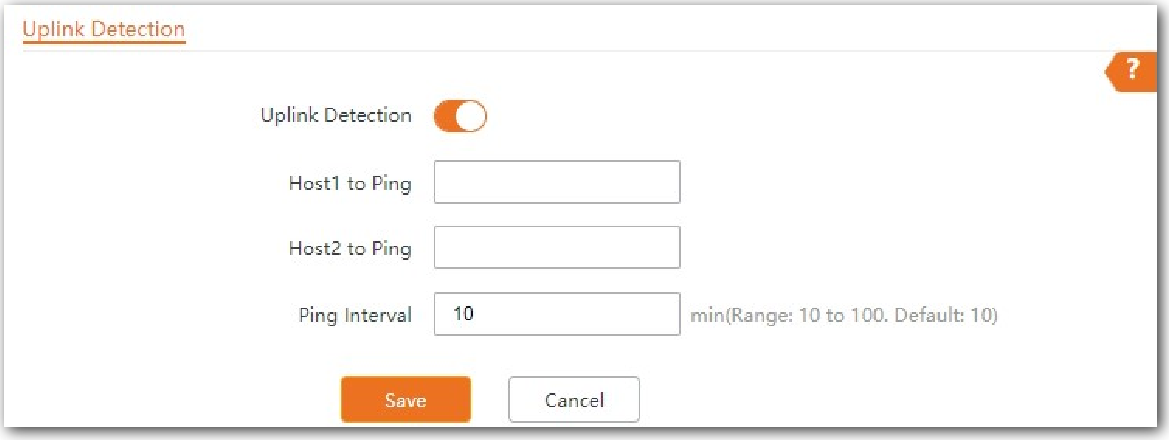
**Step 1** Choose **Tools** > **Uplink Detection**.

**Step 2** Enable **Uplink Detection**.

**Step 3** Enter the IP address of the host to be pinged in **Host1 to Ping** or **Host2 to Ping**, such as the IP address of the switch or router directly connected to the Ethernet port of the AP.

**Step 4** Enter the interval at which the AP detects its uplink in **Ping Interval** box.

**Step 5** Click **Save** to apply your settings.


Uplink Detection

Uplink Detection: ●

Host1 to Ping:

Host2 to Ping:

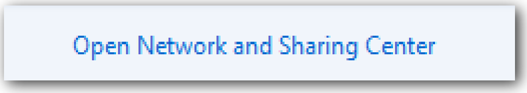
Ping Interval: 10 min(Range: 10 to 100. Default: 10)

---- End

# Appendix

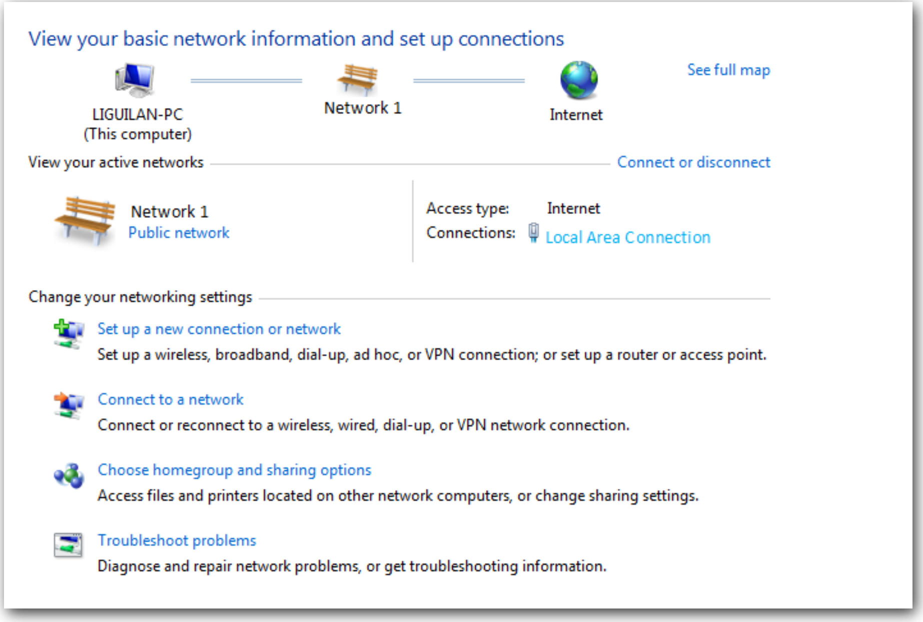
## A.1 Configuring a static IP address for your computer (Example: Windows 7)

**Step 1** Right-click 🖧 in the lower-right corner of the desktop and choose **Open Network and Sharing Center**.



Open Network and Sharing Center

**Step 2** Click **Local Area Connection**.



View your basic network information and set up connections

See full map

LIGUILAN-PC
(This computer)

Network 1

Internet

View your active networks

Connect or disconnect

Network 1
Public network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

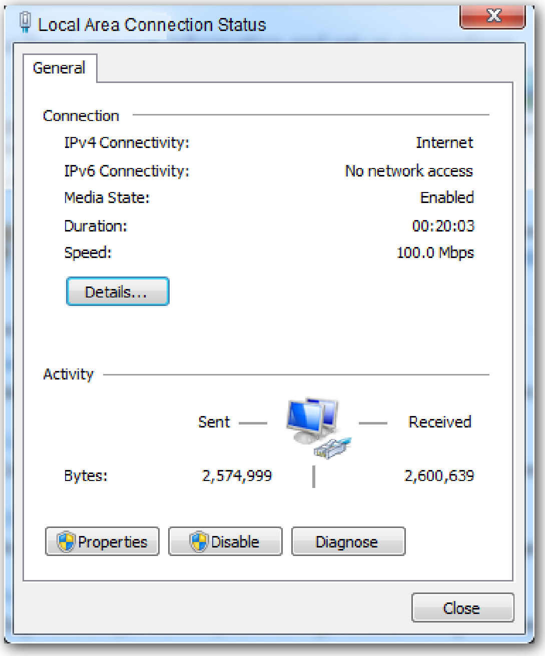
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

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

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

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

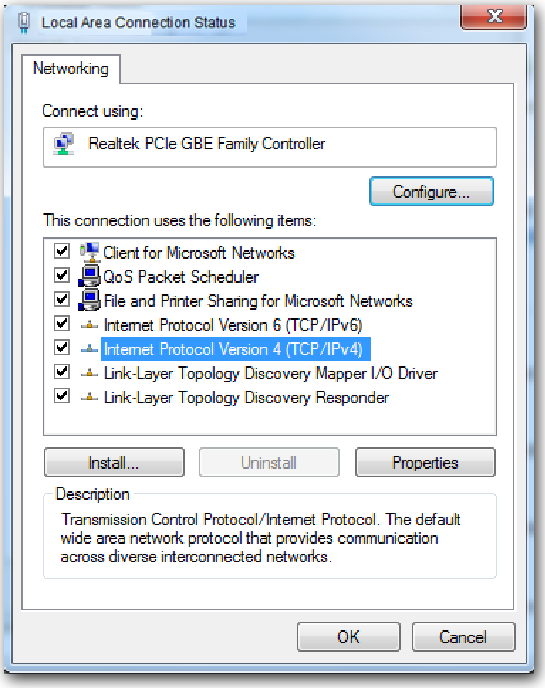
**Step 3** Click **Properties**.



IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:20:03
Speed: 100.0 Mbps

Bytes: 2,574,999 2,600,639

**Step 4** Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



Connect using:

Realtek PCIe GBE Family Controller

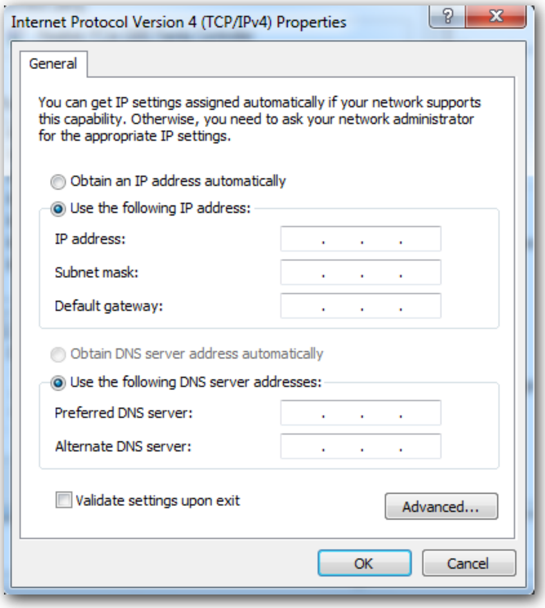
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

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

**Step 5** Select **Use the following IP address** and **Use the following DNS server address**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

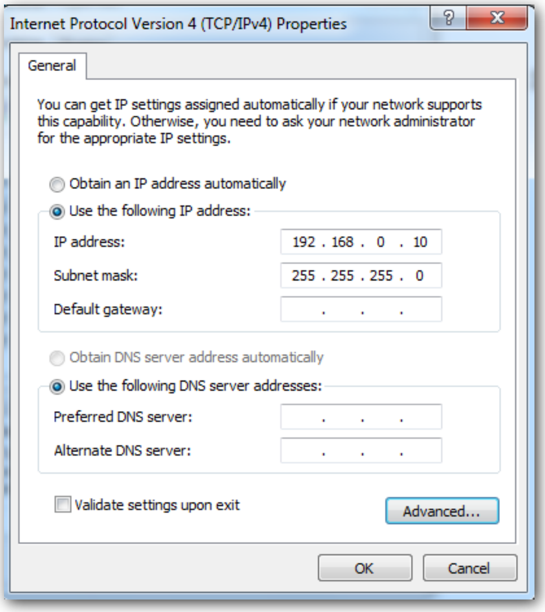
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

**Step 6** **IP address**, **Subnet mask**: Set a static IP address, subnet mask for your computer, which is **192.168.0.10** and **255.255.255.0** in this example, and click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

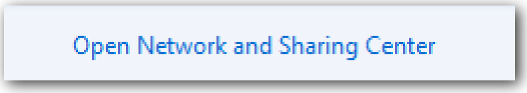
Alternate DNS server: . . .

□ Validate settings upon exit

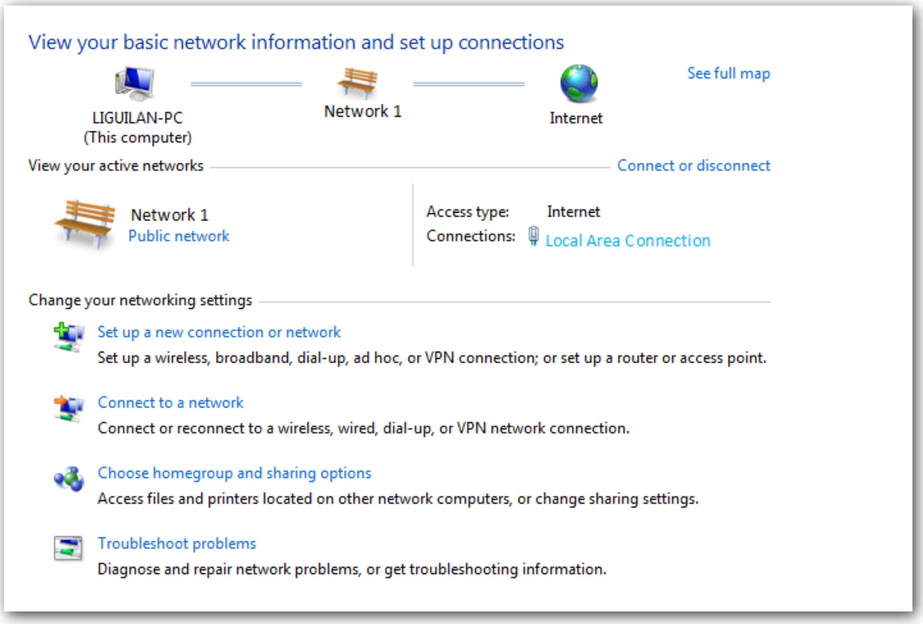
**---- End**

Configuration succeeds. You can check whether your configuration is successful on the **Network Connection Details** page. Procedure is as follows:

**Step 1** Right-click in the lower-right corner of the desktop and choose **Open Network and Sharing Center**.



**Step 2** Click **Local Area Connection**.



View your basic network information and set up connections

View your active networks

Network 1
Public network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

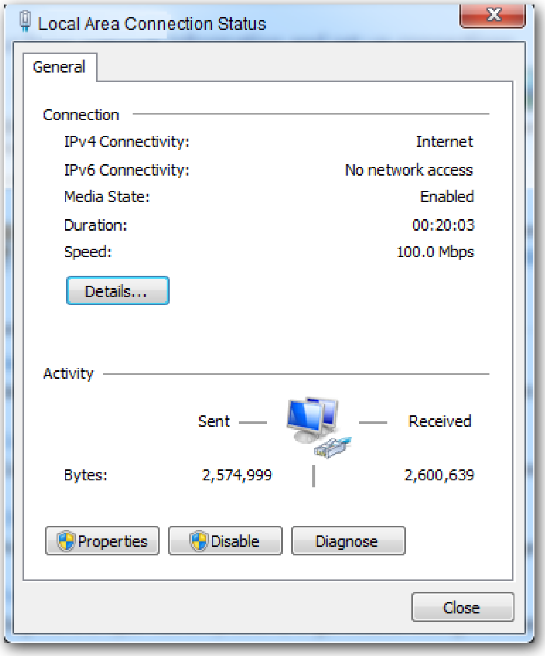
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

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

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

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

**Step 3** Click **Details**.



Local Area Connection Status

Connection

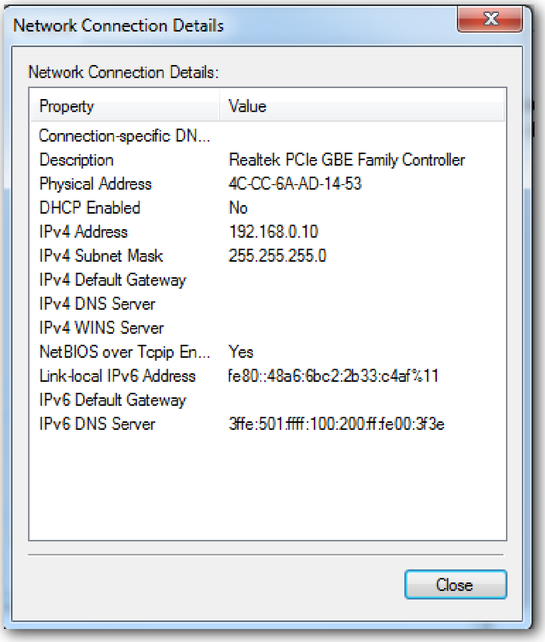
IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:20:03
Speed: 100.0 Mbps

Activity

Sent — Received

Bytes: 2,574,999 2,600,639

**Step 4** Check whether your configuration is successful on the **Network Connection Details** page. Parameters in **IPv4 Address**, **IPv4 Subnet Mask** represent the IP address, subnet mask of your computer.



Network Connection Details:

| Property | Value |
|---|---|
| Connection-specific DN... | |
| Description | Realtek PCIe GBE Family Controller |
| Physical Address | 4C-CC-6A-AD-14-53 |
| DHCP Enabled | No |
| IPv4 Address | 192.168.0.10 |
| IPv4 Subnet Mask | 255.255.255.0 |
| IPv4 Default Gateway | |
| IPv4 DNS Server | |
| IPv4 WINS Server | |
| NetBIOS over Tcpip En... | Yes |
| Link-local IPv6 Address | fe80::48a6:6bc2:2b33:c4af%11 |
| IPv6 Default Gateway | |
| IPv6 DNS Server | 3ffe:501:ffff:100:200:ff:fe00:3f3e |

## A.2 FAQ

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

**A1**: Try the following solutions:

- Ensure that all your Ethernet cables are properly connected.
- If there is no Tenda AC or Tenda router that supports AP management in the network, ensure that the IP address of your computer has been set to 192.168.0.*X* (*X*: 2 to 253), and the IP address is not used by any other devices in the same network.
- Clear the cache of your web browser, or replace the web browser.
- Disable the firewall of your computer.
- Replace your computer.
- If two or more APs are connected in the network without an Tenda AC or Tenda router that supports AP management, an IP address conflict may happen. You should leave only one AP in the network first and set a new IP address 192.168.0.*X* (*X*: 2 to 253) for the AP. Then repeat this procedure to modify the IP addresses of the other APs. Meanwhile, make sure that the IP address of your computer is in the same network segment with your APs' new IP addresses. Then try logging in to the web UI of your APs using their new IP addresses.
- If the AP has been managed by an Tenda AC or Tenda router that supports AP management, the AP's IP address may be no longer 192.168.0.254. In that case, go to the web UI of the **AC/router** to view the new IP address of the AP, and then log in to the AP's web UI using the new IP address.
- If the problem persists, reset the AP, and then try logging in again.

**Q2**: My access point controller (AC) cannot find my AP. What should I do?

**A2**: Try the following solutions:

- Ensure that all the devices in the network are connected properly and the LED of the AP blinks.
- If VLANs have been defined in your network, verify that the corresponding VLAN has been added to your AP controller.
- Reboot your AP.
- Upgrade firmware your AP to the latest version.
- Reset your AP.

## A.3 Default parameter values

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

| Parameter | | | Default Value |
|---|---|---|---|
| Login | Login IP address | | 192.168.0.254 |
| | User Name\|Password | Administrator | admin\|admin |
| | | User | user\|user |
| Quick Setup | Working Mode | | AP |
| LAN Setup | IP Address Type | | The default IP address type of the LAN port is static IP address.<br>If the LAN where the AP is located has a Tenda access point controller (including a Tenda router that supports AP management), the AP may automatically obtain a new IP address from the DHCP server of the access point controller. In this case, go to the client list of the DHCP server of the access point controller to check the IP address obtained by the AP. |
| | IP Address | | 192.168.0.254 |
| | Subnet Mask | | 255.255.255.0 |
| DHCP Server | | | Disable |
| SSID | SSID | 2.4 GHz | The AP allows 8 SSIDs.<br>SSID is Tenda_*XXXXXX*. *XXXXXX* indicates the last 6 digits of the AP's LAN MAC address with a range of *XXXXXX~XXXXXX+7.*<br>By default, the primary SSID is enabled, and the other SSIDs are disabled. |
| | | 5 GHz | The AP allows 4 SSIDs.<br>SSID is Tenda_*XXXXXX*_5G. *XXXXXX* indicates the last 6 digits of the AP's LAN MAC address with a range of *XXXXXX*+8~*XXXXXX*+11.<br>By default, the primary SSID is enabled, and the other SSIDs are disabled. |
| RF Settings | Wireless Network | | Enable |
| | Network Mode | 2.4GHz | 11b/g/n |
| | | 5GHz | 11ac |

| Parameter | | | Default Value |
|---|---|---|---|
| | Channel Bandwidth | 2.4GHz | 20 MHz |
| | | 5GHz | 80 MHz |

## A.4 Acronyms and Abbreviations

| Acronym or Abbreviation | Full Spelling |
|---|---|
| AC | Access Point Controller (Network Equipment) |
| AC | Access Category (WMM settings) |
| ACK | Acknowledge |
| AES | Advanced Encryption Standard |
| AIFSN | Arbitration Inter Frame Spacing Number |
| AP | Access Point |
| APSD | Automatic Power Save Delivery |
| ARP | Address Resolution Protocol |
| BE | Best Effort |
| BK | Background |
| CAT5e | Category 5 Ethernet |
| CSMA/CA | Carrier Sense Multiple Access with Collision Avoidance |
| CTS | Clear To Send |
| Cwmax | Contention Window Maximum |
| Cwmin | Contention Window Minimum |
| DHCP | Dynamic Host Configuration Protocol |
| DIFS | Distributed Inter-Frame Spacing |
| DNS | Domain Name Server |
| DTIM | Delivery Traffic Indication Message |
| EDCA | Enhanced Distributed Channel Access |
| GI | Guard Interval |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| LAN | Local Area Network |
| MAC | Medium Access Control |

| Acronym or Abbreviation | Full Spelling |
|---|---|
| MIB | Management Information Base |
| MU-MIMO | Multi-User Multiple-Input Multiple-Output |
| NMS | Network Management System |
| NTS | Network Time Server |
| OID | Object Identifier |
| PoE | Power-over-Ethernet |
| PPP | Point to Point Protocol |
| PVID | Port-based VLAN ID |
| QVLAN | IEEE 802.11q VLAN |
| RADIUS | Remote Authentication Dial-In User Service |
| RF | Radio Frequency |
| RSSI | Received Signal Strength Indicator |
| RTS | Request To Send |
| SNMP | Simple Network Management Protocol |
| SSID | Service Set Identifier |
| STA | Station |
| SYS | System |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TKIP | Temporal Key Integrity Protocol |
| TXOP | Transmission Opportunity |
| UI | User Interface |
| UTF-8 | 8-bit Unicode Transformation Format |
| VI | Video Stream |
| VID | Virtual ID |
| VLAN | Virtual Local Area Network |
| VO | Voice Stream |
| WAN | Wide Area Network |

| Acronym or Abbreviation | Full Spelling |
|---|---|
| WEP | Wired Equivalent Privacy |
| WMF | Wireless Multicast Forwarding |
| WMM | Wi-Fi Multimedia |
| WPA | Wi-Fi Protected Access |
| WPA-PSK | Wi-Fi Protected Access-Pre-shared Key |