

User Guide

AX3000 Wi-Fi 6 Ceiling Access Point

i27



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 of AX3000 Wi-Fi 6 Ceiling Access Point i27.

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	<i>Italic</i>	Format: <i>XX:XX:XX:XX:XX:XX</i>
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 supplement or explain relevant operations.

For more documents

The AP can be centrally managed either by Tenda AP controllers (AC) or Tenda routers that support 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

Document	Description
Datasheet	Walks you through basic parameters of AP, including product overview, product features, product specifications and so on.
User Manual	Walks you through quick setup of AP, safety precautions and statement.
Quick Installation Guide	Walks you through a rapid AP network establishment, including AP installation, network configuration, LED/Port/Button description, FAQ, and so on.
User Guide	Walks you through detailed functions and configurations of APs, including all the functions on the web UI.

Technical Support

Contact us if you need more help. We will be glad to assist you as soon as possible.

Email: support@tenda.com.cn

Website: 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 user guide was released.

Version	Date	Description
V1.0	2022-11-29	Original publication.

Contents

1	Log in to the web UI	1
	1.1 Login.....	1
	1.2 Logout	3
2	Web UI	4
	2.1 Layout.....	4
	2.2 Frequently-used buttons	5
3	Quick setup	6
	3.1 AP mode.....	6
	3.1.1 Overview	6
	3.1.2 Quick setup	6
	3.2 Client+AP working mode	8
	3.2.1 Overview	8
	3.2.2 Quick setup	9
4	Status	12
	4.1 System status	12
	4.2 Wireless status	14
	4.3 Traffic statistics	15
	4.4 Client list	16
5	Internet settings.....	18
6	Wireless	20
	6.1 SSID	20
	6.1.1 Overview	20
	6.1.2 Example of SSID configurations	27
	6.2 RF settings.....	47
	6.3 RF optimization	51
	6.4 Frequency analysis	55

6.4.1	Overview	55
6.4.2	View frequency analysis	55
6.4.3	Execute channel scan	56
6.5	WMM	57
6.5.1	Overview	57
6.5.2	Configure WMM settings.....	59
6.6	Access control	61
6.6.1	Overview	61
6.6.2	Configure access control.....	62
6.6.3	Example of configuring access control.....	63
6.7	Advanced settings	65
6.8	QVLAN settings.....	66
6.8.1	Overview	66
6.8.2	Configure the QVLAN function	68
6.8.3	Example of configuring QVLAN.....	69
7	Advanced	72
7.1	Overview	72
7.2	Configure traffic control	74
8	Tools.....	75
8.1	Date & time	75
8.1.1	System time	75
8.1.2	Login timeout interval	76
8.2	Maintenance	78
8.2.1	Reboot.....	78
8.2.2	Reset.....	80
8.2.3	Upgrade firmware	81
8.2.4	Backup/restore	81
8.2.5	LED indicator control	84
8.3	Account	86

8.3.1 Overview	86
8.3.2 Modifying the password and user name of login account	87
8.4 System Log	88
8.5 Diagnostic tool	89
8.6 Uplink check	90
8.6.1 Overview	90
8.6.2 Configure uplink detection	91
Appendix	92
A.1 Default parameter values	92
A.2 Acronyms and abbreviations	93

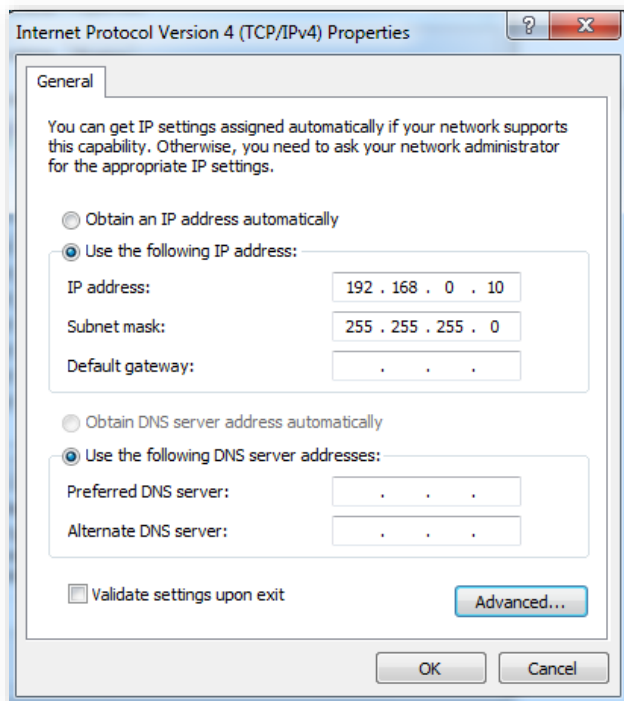
1

Log in to the web UI

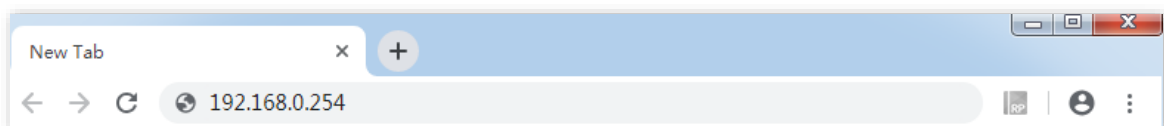
1.1 Login

- 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).



- 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.



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

----End



If the login page does not appear, please try the following solutions:

- Check that the Ethernet cable is connected properly.
- Ensure that the IP address of the computer is set to the same network segment as that of the AP. If the AP's IP address is still 192.168.0.254, you can set the IP address of your computer to **192.168.0.X** (X ranges from 2 to 253 and is not occupied by other devices).
- If the AP is managed by a controller, the AP may obtain an IP address from a DHCP server in the LAN. You can check the new IP address from the client list of the DHCP server, and use this IP address to log in.
- Reset the AP and try logging in using the default IP address. How to reset: After the AP is started, hold down the **RESET** button for about 8 seconds and release it. Wait about 8 seconds, AP is restored to factory settings and restarted.

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

1.2 Logout

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 Web UI

2.1 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.

The screenshot displays the web UI of an Access Point (AP). On the left is a navigation sidebar with a level-1 bar (Wireless) and a level-2 bar (Client List). The main content area is titled 'System Status' and contains configuration details for the device, such as Device Name, System Time, Hardware Version, Uptime, Firmware Version, and LAN Port Status. A help icon (?) is visible in the top right corner of the main content area.

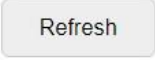

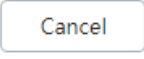



Functions or parameters displayed in gray on the web UI are not supported yet or cannot be modified under the current configurations.

No.	Name	Description
1	Level-1 navigation bar	
2	Level-2 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.
3	Tab page area	
4	Configuration area	Used to modify or view your configuration.

2.2 Frequently-used buttons

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

Button	Description
	Used to refresh the current page.
	Used to save the configuration on the current page and enable the configuration to take effect.
	Used to modify the current configuration on the current page back to the original configuration.
	Used to get the online help.

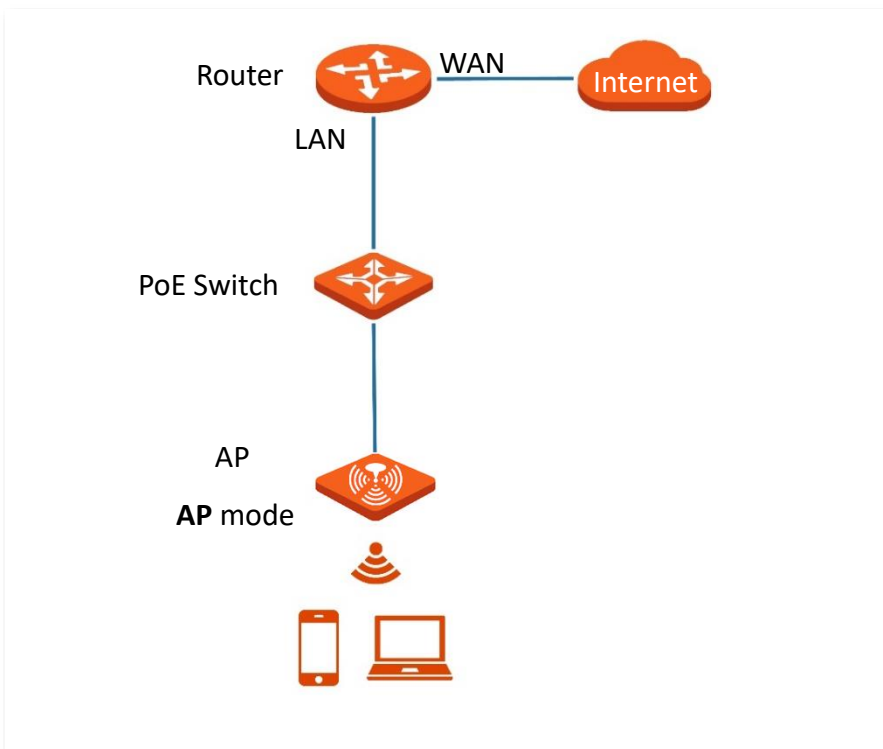
3 Quick setup

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.

3.1 AP mode

3.1.1 Overview

In this mode, the AP connects to the internet in a wired manner, and converts wired network into wireless network. AP works in this mode by default. See the following topology.



3.1.2 Quick setup



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

Step 1 Choose **Quick Setup**.

Step 2 Choose the **Radio Band** you wish to configure, for example, **2.4 GHz**.

Step 3 Set a wireless network name ([primary SSID](#)) in the **SSID** box.

Step 4 Select a **Security Mode** and configure the incurred parameters.

Step 5 Click **Save**.

The screenshot shows a 'Quick Setup' window with the following settings:

- Radio Band: 2.4GHz
- Working Mode: AP, Client+AP
- SSID: Tenda_1DA278
- Security Mode: WPA-PSK & WPA2-PSK
- Encryption Algorithm: AES, TKIP, TKIP&AES
- Key: [Masked]

Buttons: Save, Cancel

Step 6 If you need to set other wireless networks in another radio band, please select another wireless radio band and perform step [2](#) to [5](#) again.

---- End

Search and connect your wireless devices such as smart phones to the **SSID** you set. Enter the wireless password (the **Key** you set) and you will be able to access the internet.

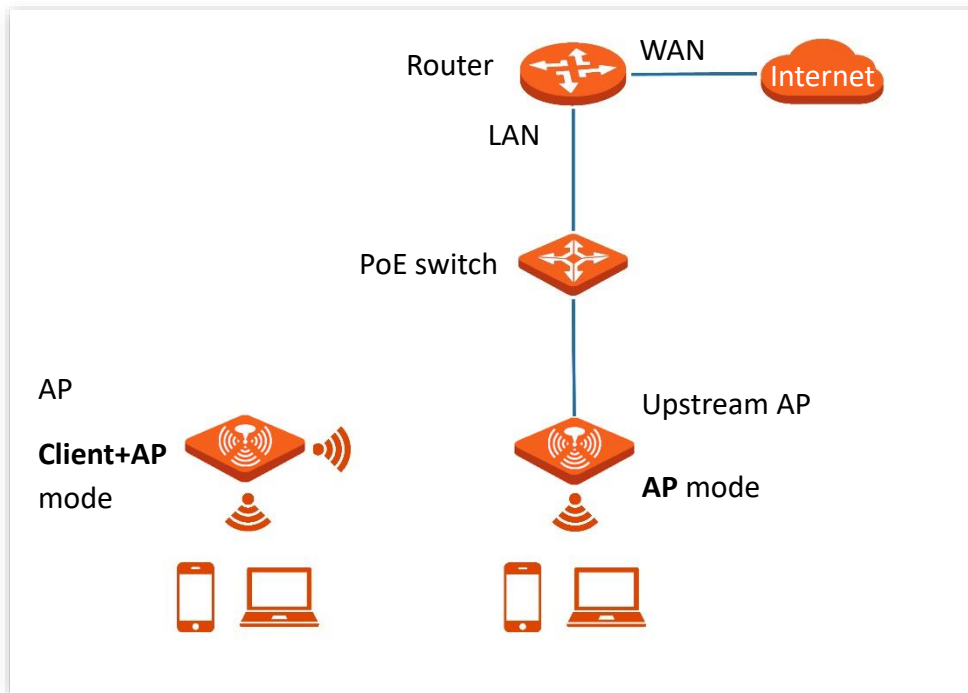
Parameter description

Parameter	Description
Radio Band	It is used to select the radio band for configurations.
Working Mode	It specifies the working modes supported by the device. <ul style="list-style-type: none"> AP mode (default mode): This mode is used to convert wired networks into wireless networks. Client+AP mode: This mode is used to bridge the upstream WiFi 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 , WPA3-SAE , WPA2-PSK&WPA3-SAE , Mixed WPA/WPA2-PSK , WPA and WPA2 .

3.2 Client+AP working mode

3.2.1 Overview

In this mode, the AP extends the existing wireless network by bridging the upstream wireless signals. See the following typical network topology.



3.2.2 Quick setup



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

Step 1 Choose **Quick Setup**.

Step 2 Choose the **Radio Band** you wish to configure, for example, **2.4GHz**.

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

Step 4 Click **Scan**.

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



- If no wireless network is found, choose **Wireless > RF Settings**, ensure that **Wireless Network** is selected, and try scanning wireless network again.
- After a wireless network to be extended is selected, the SSID, security mode, and channel of the wireless network are populated automatically.

Select	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
<input checked="" type="radio"/>	EW15D	[blurred]	20	5	WPA2-PSK/AES	[signal strength icon]
<input type="radio"/>	0101wkd_v33v1.0	[blurred]	20	2	WPA2-PSK/AES	[signal strength icon]
<input type="radio"/>	333	[blurred]	20	2	Mixed WPA/WPA2-PSK...	[signal strength icon]

Step 6 If the wireless network of the upstream device is encrypted, enter the wireless network password of the device in the **Key** column.

Step 7 Click **Save**.

Quick Setup

Radio Band: 2.4GHz

Working Mode: AP Client+AP

SSID: EW15D

Security Mode: WPA2-PSK

Encryption Algorithm: AES TKIP TKIP&AES

Key:

Refresh Scan

Save Cancel

---End


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



TIP
If you do not know the SSID and key of the AP, you can check the SSID and key of the AP on the **Wireless > SSID** page.

Parameter description

Parameter	Description
Radio Band	Select the radio band you wish to configure.
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.

Parameter	Description
Security Mode	<p>It specifies the security mode which the upstream WiFi network adopts.</p> <p>See Security Mode for details.</p> <p> TIP</p> <ul style="list-style-type: none"> • 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. • If the wireless network to be bridged adopts the WPA-PSK, WPA2-PSK, WPA-PSK&WPA2-PSK, WPA3-SAE, or WPA2-PSK&WPA3-SAE 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	<ul style="list-style-type: none"> • Scan: Used to scan nearby available wireless networks. The scan results are displayed on the lower page. • Disable: The button only appears after you clicked Scan. It is used to end the scan operation and collapse the scan result.

4 Status

4.1 System status

The **System Status** page allows you to check the **System Status** and **LAN Port Status** of the AP.

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

The screenshot shows the 'System Status' page with a help icon (question mark) in the top right corner. The page is divided into two main sections: 'System Status' and 'LAN Port Status'.

System Status:

- Device Name: Access Point
- Uptime: 35min5sec
- System Time: 2022-11-14 16:47:07
- Firmware Version: V1.0.0.1(601)
- Hardware Version: V1.0
- Number of Wireless Clients: 0

LAN Port Status:

- MAC Address: [REDACTED]
- 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	
System Status	Device Name	It specifies the name of the AP. 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.
	Hardware Version	It specifies the current hardware version number of the AP.
	Number of	It specifies the quantity of wireless devices currently connected to the

Parameter	Description
Wireless Clients	AP.
MAC Address	It specifies the physical address of the AP's LAN port.
LAN Port Status	IP Address It specifies the IP address of the AP and it is also the management IP address of the AP, which can be used to log in to the web UI. 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

The **Wireless Status** page allows you to check **RF Status** and **SSID Status** of the AP.

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

[2.4 GHz](#) [5 GHz](#)
?

RF Status

RF: Enabled Network Mode: 11b/g/n/ax

Channel: 7

SSID Status

SSID	MAC Address	Status	Security Mode
Tenda_1DA278	C8:3A:35:1D:A2:7A	Enabled	None
Tenda_1DA27B	C8:3A:35:1D:A2:7B	Disabled	None
Tenda_1DA27C	C8:3A:35:1D:A2:7C	Disabled	None
Tenda_1DA27D	C8:3A:35:1D:A2:7D	Disabled	None

Parameter description

Parameter	Description
RF Status	<p>RF: It specifies whether the wireless function of the AP is enabled.</p> <p>Network Mode: It specifies the network mode currently enabled by the AP on each radio band.</p> <p>Channel: It specifies the current working channel of the AP.</p>
SSID Status	<p>SSID: It specifies the names of all the wireless networks of the AP.</p> <p>MAC Address: It specifies the physical address of the corresponding wireless network.</p> <p>Status: It specifies whether or not the corresponding WiFi network is enabled.</p> <p>Security Mode: It specifies the security modes of the wireless networks corresponding to the SSIDs of the AP.</p>

4.3 Traffic statistics

The **Traffic Statistics** page allows you to check statistical information about traffic based on SSIDs.

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

[2.4 GHz](#) [5 GHz](#)

SSID	Received Traffic	Received Packets (Qty.)	Transmitted Traffic	Transmitted Packets (Qty.)
Tenda_1DA278	0.00MB	0	0.09MB	602
Tenda_1DA27B	0.00MB	0	0.00MB	0
Tenda_1DA27C	0.00MB	0	0.00MB	0
Tenda_1DA27D	0.00MB	0	0.00MB	0
Tenda_1DA27E	0.00MB	0	0.00MB	0
Tenda_1DA27F	0.00MB	0	0.00MB	0
Tenda_1DA270	0.00MB	0	0.00MB	0

Parameter description

Parameter	Description
SSID	It specifies the wireless network name.
Received Traffic	It specifies the total number of bytes received by a wireless network.
Received Packets (Qty.)	It specifies the total number of packets received by a wireless network.
Transmitted Traffic	It specifies the total number of bytes transmitted by a wireless network.
Transmitted Packets (Qty.)	It specifies the total number of packets transmitted by a wireless network.



All the statistics are cleared when the wireless function is disabled or this device is rebooted. All the wireless network statistics of an SSID are cleared when the SSID is disabled.


4.4 Client list


The **Client List** page allows you to view wireless clients connected to each SSID of the AP and their basic information.

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

The screenshot shows the 'Client List' page for the SSID 'Tenda_1DA278'. At the top, there are tabs for '2.4 GHz' and '5 GHz'. Below the tabs, the text 'Clients connected to the SSID:' is followed by a dropdown menu showing 'Tenda_1DA278'. A table with 8 columns is displayed: ID, MAC Address, IP Address, Client Type, Connection Duration, Transmit Rate, Receive Rate, and Block. The table contains one row with the following data: ID 1, MAC Address [blurred], IP Address 192.168.0.108, Client Type --, Connection Duration 00:04:11, Transmit Rate 137Mbps, Receive Rate 68Mbps, and a Block button with an 'x' icon. Below the table, there is a pagination control showing '10' in a dropdown, 'in total/Page', and '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	<p>It specifies the operating system of the client.</p> <p> TIP</p> <p>The AP identifies the client type only when both the two conditions are met:</p> <ul style="list-style-type: none"> The Identify Client Type function is enabled (To enable it, navigate to Wireless > Advanced Settings). The client connected to the AP has accessed an http:// URL. <p>Otherwise, -- is displayed.</p>
Connection Duration	It specifies the duration of a connection between a wireless client and a wireless network with a specified SSID.
Transmit Rate	It specifies the real time traffic the client has transmitted.

Parameter	Description
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. To unblock a client, navigate to Wireless > Access Control .

5 Internet settings

The **LAN Setup** page allows you to check the MAC address of the LAN port of AP, modify the IP address obtaining method of the AP, modify device name, and modify Ethernet mode.

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

LAN Setup

MAC Address

IP Address Type

IP Address

Subnet Mask

Default Gateway


Primary DNS

Secondary DNS

Device Name

Optimize Ethernet for: Faster Speed (Auto Negotiation)
 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	<p>It specifies IP address obtaining method of the AP.</p> <ul style="list-style-type: none"> • Static IP: You are required to set related parameters manually. This method is suitable for scenarios where only one or several APs are deployed. • DHCP (Dynamic IP Address): The AP automatically obtains related parameters from a DHCP server on your LAN network. This method is suitable for scenarios where a great number of APs are deployed. <p> TIP</p> <p>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.</p>
IP Address	It specifies the LAN IP address (also the login IP address) of the AP. The web UI of the AP is accessible at this IP address.
Subnet Mask	It specifies the subnet mask of the AP. Default: 255.255.255.0 .
Default Gateway	<p>It specifies the gateway IP address of the AP.</p> <p>Generally, enter the LAN IP address of the router connected to the internet.</p>
Primary DNS	<p>It specifies the IP address of the primary DNS server of the AP.</p> <p>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.</p>
Secondary DNS	<p>It specifies the IP address of the secondary DNS server of the AP. This parameter is optional.</p> <p>If you have two DNS server IP addresses, you can enter the other one here.</p>
Device Name	<p>It specifies the name of the AP.</p> <p>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.</p>
Optimize Ethernet for	<p>It specifies the Ethernet mode of the PoE power-supply port of the AP.</p> <ul style="list-style-type: none"> • Faster Speed (Auto Negotiation): This option features a high data rate but short transmission distance. Generally, you are advised to select this option. • Longer Distance (10 Mbps Full Duplex): This option features long transmission distance but low data rate. Generally, the negotiated speed is 10 Mbps. <p>If the Ethernet cable connecting the PoE Ethernet port of the AP to the peer device is longer than 100 meters, the Longer Distance (10 Mbps Full Duplex) mode is recommended. In this case, ensure that the peer device adopts auto negotiation option.</p>

6 Wireless

6.1 SSID

6.1.1 Overview

The **SSID** page allows you to set SSID-related parameters of the AP.

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

The screenshot shows the SSID configuration interface. At the top, there are tabs for '2.4 GHz' and '5 GHz'. A help icon (?) is in the top right corner. The main configuration area includes:

- SSID:** A dropdown menu showing 'Tenda_1DA278'.
- Status:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Broadcast SSID:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Guest:** Radio buttons for 'Enable' and 'Disable' (selected).
- Isolate Client:** Radio buttons for 'Enable' and 'Disable' (selected).
- Isolate SSID:** Radio buttons for 'Enable' and 'Disable' (selected).
- WMF:** Radio buttons for 'Enable' and 'Disable' (selected).
- Max. Number of Clients:** A text input field containing '48', with '(Range: 1 to 128)' to its right.
- SSID:** A text input field containing 'Tenda_1DA278'.
- Security Mode:** A dropdown menu showing 'None'.

At the bottom, there are two buttons: 'Save' (orange) and 'Cancel' (white).

Parameter description

Parameter	Description
SSID	It specifies the SSID to be configured. On each band, the first displayed SSID is the primary SSID.

Parameter	Description
Status	It specifies the status of the selected SSID. The primary SSID is enabled by default and you can enable other SSIDs manually.
Broadcast SSID	After this function is disabled, AP stops broadcasting SSID and nearby wireless clients cannot detect the SSID. Users need to enter the SSID manually on the wireless client to access the wireless network, enhancing the security of the wireless network.
Guest	After this function is enabled, the connected wireless clients can only access the internet and other wireless clients under the guest network, but cannot access the web UI of router and the main LAN network.
Isolate Client	It isolates the wireless clients connected to the same wireless network corresponding to an SSID, so that the wireless clients can only access the internet and other wired clients (such as a computer) connected to the AP. Applying this function to hotspot setup at public places such as hotels and airports helps increase network security.
Isolate SSID	After this function is enabled, wireless devices connected to different SSIDs of the AP cannot communicate with each other, enhancing the security of the wireless network.
WMF	The WMF function of the AP converts multicast traffic into unicast traffic and forwards the traffic to the multicast traffic destination in the wireless network. This helps save wireless resources, ensure reliable transmission, and reduce delays.
Max. Number of Clients	It specifies the maximum number of devices that can connect to the WiFi network corresponding to an SSID. If the number is reached, new devices cannot connect to the SSID unless some devices cut off their connections.
SSID	Click this field to modify the selected SSID (the name of the wireless network).
Security Mode	It specifies the security modes supported by the AP, including: None , WEP , WPA-PSK , WPA2-PSK , WPA3-SAE , WPA2-PSK&WPA3-SAE , Mixed WPA/WPA2-PSK , WPA and WPA2 .

Security Mode

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

The AP supports various security modes for network encryption, including [None](#), [WEP](#), [WPA-PSK](#), [WPA2-PSK](#), [WPA3-SAE](#), [WPA2-PSK&WPA3-SAE](#), [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 is abbreviated for Wired Equivalent Privacy. 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.

The image shows a configuration window for WEP security. It contains the following elements:

- Security Mode:** A dropdown menu set to 'WEP'.
- Authentication Type:** A dropdown menu set to 'Open'.
- Default Key:** A dropdown menu set to 'Key 1'.
- Key 1:** A text input field containing five dots, with an 'ASCII' dropdown menu to its right.
- Key 2:** A text input field containing five dots, with an 'ASCII' dropdown menu to its right.
- Key 3:** A text input field containing five dots, with an 'ASCII' dropdown menu to its right.
- Key 4:** A text input field containing five dots, with an 'ASCII' dropdown menu to its right.

Parameter description

Parameter	Description
Authentication Type	<p>It specifies the authentication type for the WEP security mode. The options include Open and Shared. The options share the same encryption process.</p> <ul style="list-style-type: none"> • 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. • 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	<p>It specifies the WEP key for the current SSID.</p> <p>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.</p>

Parameter	Description
Key 1/2/3/4	<p>4 WEP keys are allowed at the same time, but only the one specified by the Default Key is valid. The key type includes ASCII and Hex.</p> <ul style="list-style-type: none"> • ASCII: 5 or 13 ASCII characters are allowed in the key. • Hex: 10 or 26 hexadecimal characters are allowed in the key (0-9, a-f, A-F).

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

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

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

The screenshot shows a configuration window with the following settings:

- Security Mode:** Mixed WPA/WPA2-PSK
- Encryption Algorithm:** WPA2-PSK
- Key:** Mixed WPA/WPA2-PSK
- Key Update Interval:** Second (Range: 60 to 99999. 0 indicates no upgrade)

Buttons: Save, Cancel

WPA3-SAE

It is an upgraded version of WPA2-PSK. With Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF), this security mode provides protection against dictionary attacks and information disclosure, saving you the trouble to set a complicated password.



If your wireless clients do not support WPA3-SAE or the WiFi experience is unsatisfying, you are recommended to set the security mode to WPA2-PSK.

Security Mode: Mixed WPA/WPA2-PSK

Encryption Algorithm: WPA2-PSK

Key: Mixed WPA/WPA2-PSK

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

Buttons: Save, Cancel

WPA2-PSK&WPA3-SAE

It indicates that the wireless network adopts the mixed encryption mode of WPA2-PSK/AES and WPA3-SAE/AES to ensure safety.

Security Mode: Mixed WPA/WPA2-PSK


Encryption Algorithm: WPA2-PSK

Key: Mixed WPA/WPA2-PSK

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

Buttons: Save, Cancel

Parameter description

Parameter	Description
Security Mode	<p>It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA3-SAE, and WPA2-PSK&WPA3-SAE.</p> <ul style="list-style-type: none"> • WPA-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA-PSK. • WPA2-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA2-PSK. • WPA3-SAE: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA3-SAE. • WPA2-PSK&WPA3-SAE: The wireless network adopts the mixed encryption mode of WPA2-PSK/AES and WPA3-SAE/AES to ensure safety. • Mixed WPA/WPA2-PSK: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK. <p> TIP</p> <p>WPA3-SAE is an upgraded version of WPA2-PSK. If your wireless clients do not support WPA3-SAE or the WiFi experience is unsatisfying, you are recommended to set the security mode to WPA/WPA2-PSK (recommended).</p>
Encryption Algorithm	<p>It specifies the encryption algorithm corresponding to the selected security mode.</p> <ul style="list-style-type: none"> • AES: It indicates the Advanced Encryption Standard. • TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. • TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	<p>It specifies a pre-shared WPA key, that is, the password clients use to connect to the wireless network.</p>
Key Update Interval	<p>It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.</p> <p>The value 0 indicates that a WPA key is not updated.</p>

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.

Parameter description

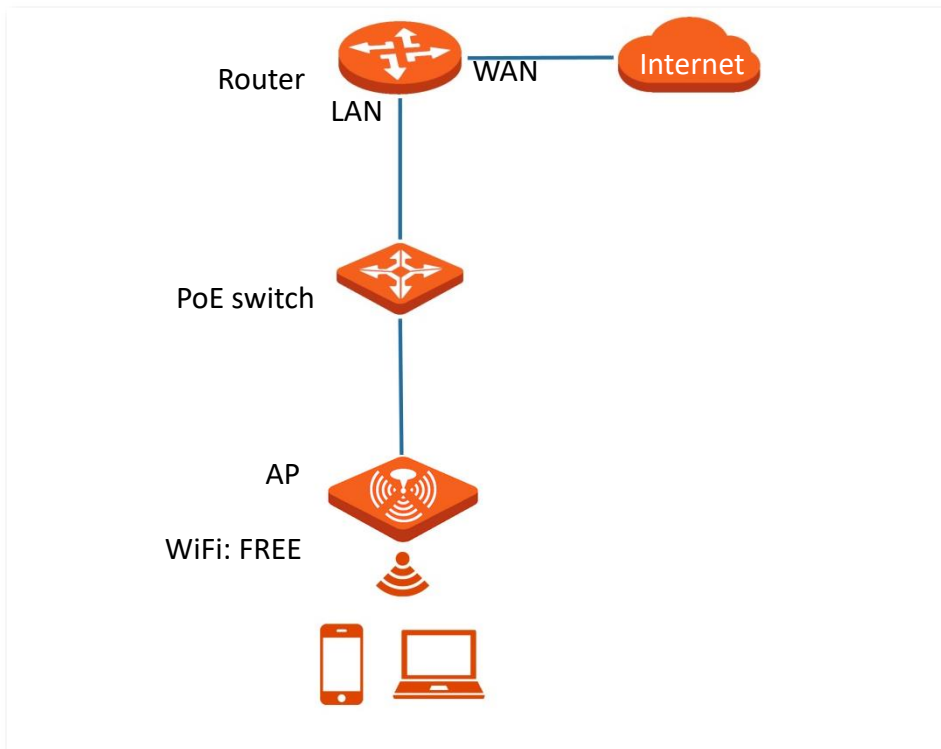
Parameter	Description
Security Mode	Select security mode. <ul style="list-style-type: none"> • WPA: The wireless network adopts the WPA enterprise security mode. • WPA2: The wireless network adopts the WPA2 enterprise security mode.
RADIUS Server	It specifies the IP address of the RADIUS server for client 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. <ul style="list-style-type: none"> • AES: It indicates the Advanced Encryption Standard. • TKIP: It indicates the Temporal Key Integrity Protocol. • TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value 0 indicates that a WPA key is not updated.

6.1.2 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 first SSID of the 2.4 GHz radio band of the AP is to be configured.

- Step 1** Choose **Wireless > SSID**.
- Step 2** Select the first 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**.

2.4 GHz 5 GHz ?

* SSID

* Status Enable Disable

Broadcast SSID Enable Disable

Guest Enable Disable

Isolate Client Enable Disable

Isolate SSID Enable Disable

WMF Enable Disable

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

* SSID

* Security Mode

----End

Verification

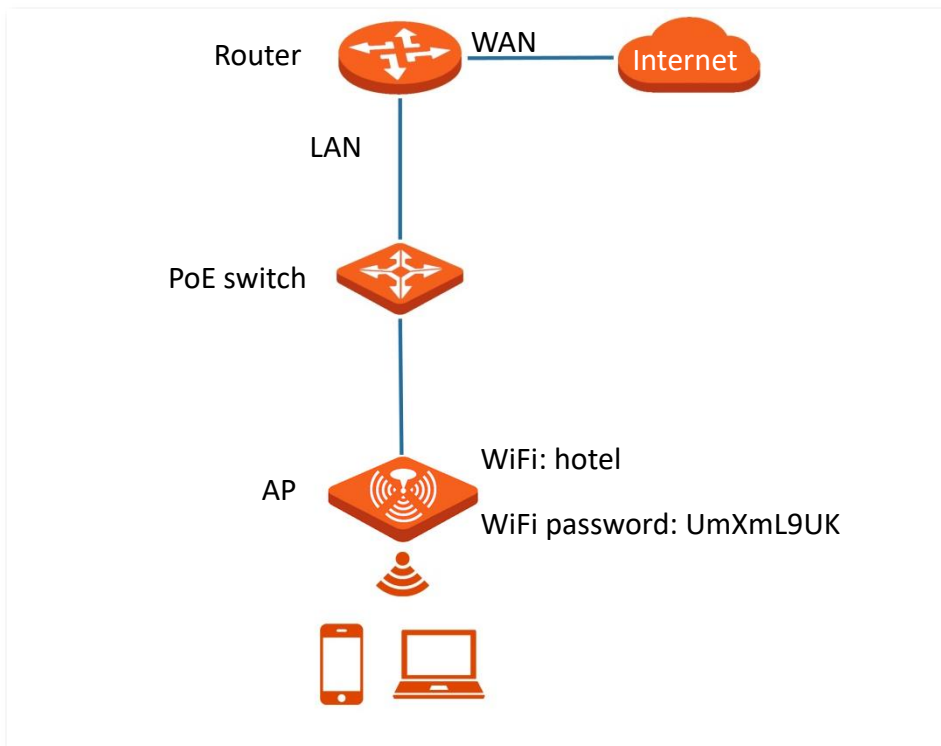
Wireless devices can connect to the **FREE** wireless network without a password.

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-PSK, WPA2-PSK or Mixed WPA/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 first SSID of the 2.4 GHz radio band of the AP is to be configured. WPA2-PSK and AES are used here for illustration.

- Step 1** Choose **Wireless > SSID**.
- Step 2** Select the first 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**.

2.4 GHz 5 GHz

* SSID

* Status Enable Disable

Broadcast SSID Enable Disable

Guest Enable Disable

Isolate Client Enable Disable

Isolate SSID Enable Disable

WMF Enable Disable

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

* SSID

* Security Mode

* Encryption Algorithm AES TKIP TKIP&AES

* Key

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

---- End

Verification

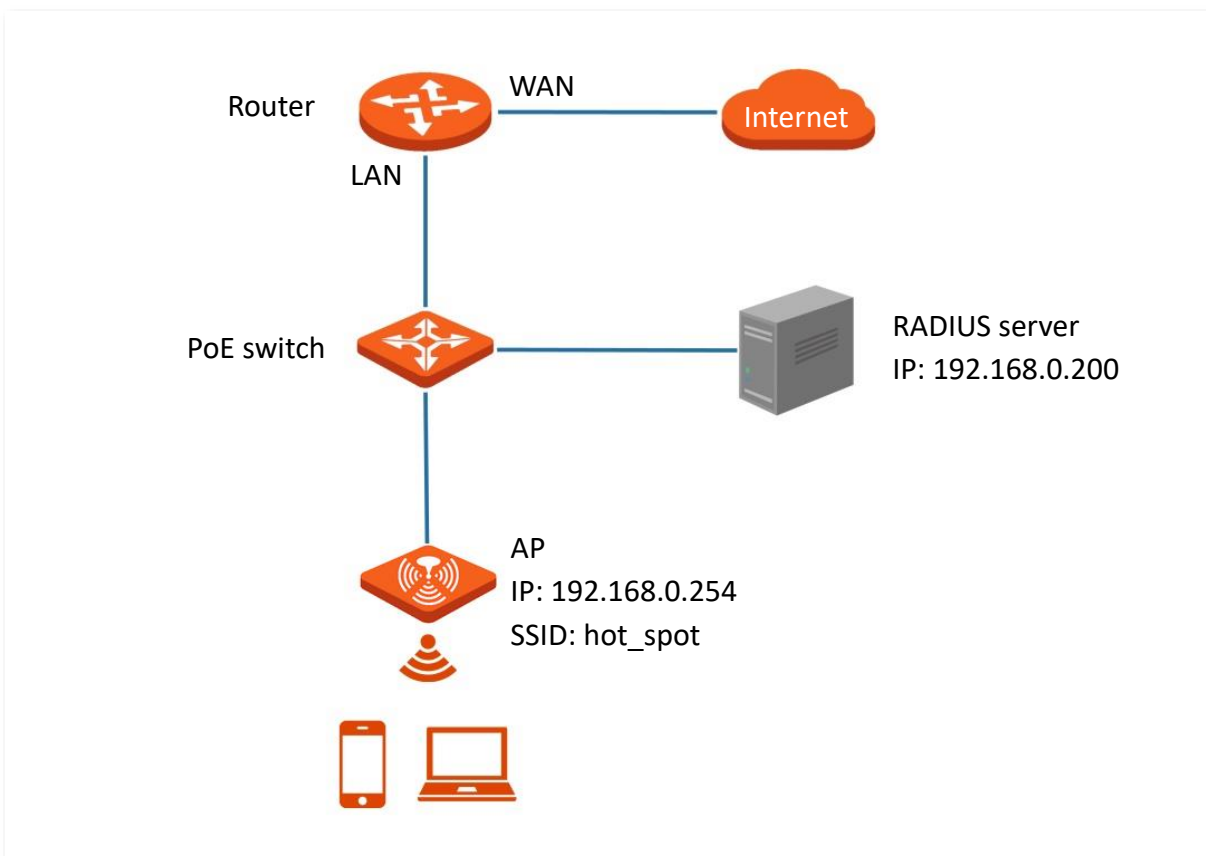
Wireless devices can connect to the **hotel** wireless network with the password **UmXmL9UK**.

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 **UmXmL9UK**, 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 first SSID of the 2.4 GHz radio band of the AP is to be configured. WPA2 and AES are used here for illustration.

- Step 1** Choose **Wireless > SSID**.
- Step 2** Select the first 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**.
- Step 6** Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Key** to **192.168.0.200**, **1812**, and **UmXmL9UK** respectively.
- Step 7** Set **Encryption Algorithm** to **AES**.
- Step 8** Click **Save** to apply your settings.

2.4 GHz 5 GHz
?

* SSID

* Status Enable Disable

Broadcast SSID Enable Disable

Guest Enable Disable

Isolate Client Enable Disable

Isolate SSID Enable Disable

WMF Enable Disable

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

* SSID

* Security Mode

* RADIUS Server

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

* RADIUS Key

* Encryption Algorithm AES TKIP TKIP&AES

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

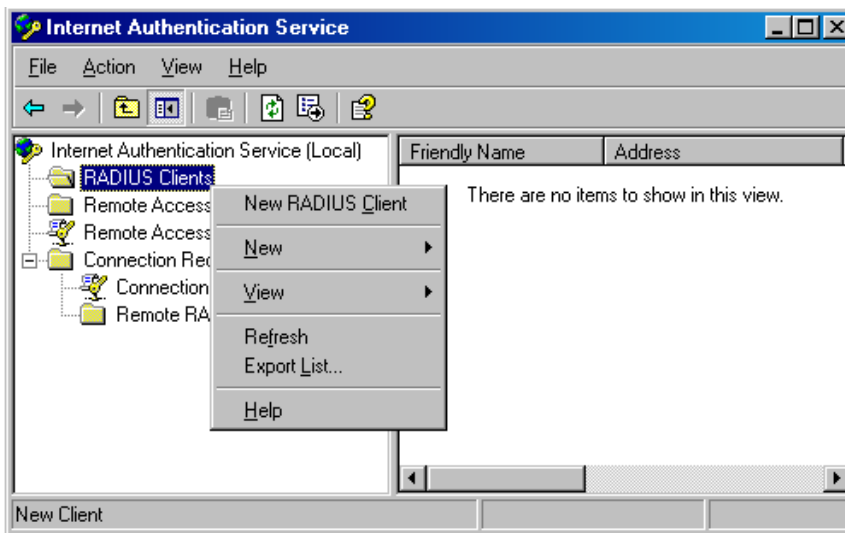
Configure the RADIUS server.



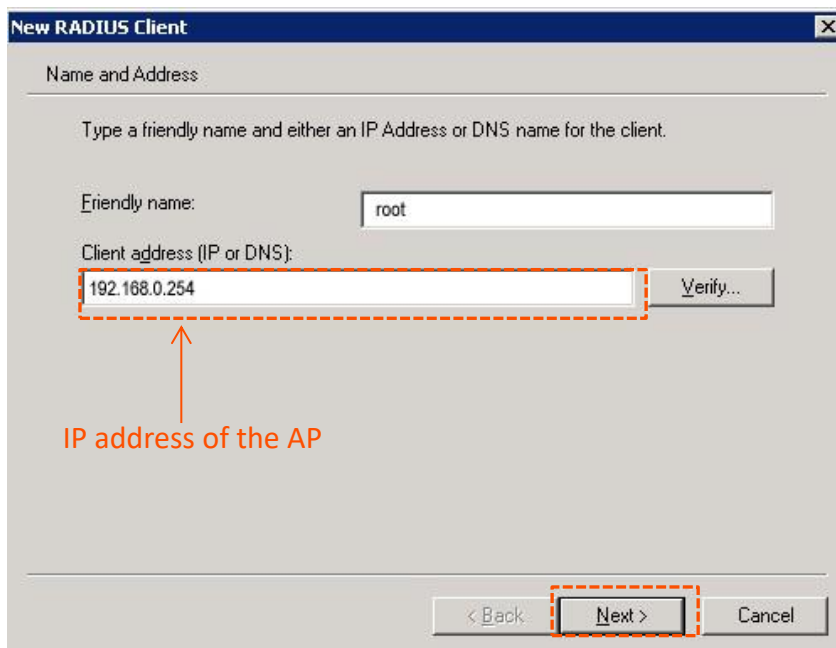
Windows 2003 is used as an example to describe how to configure the RADIUS server.

Step 1 Configure RADIUS client.

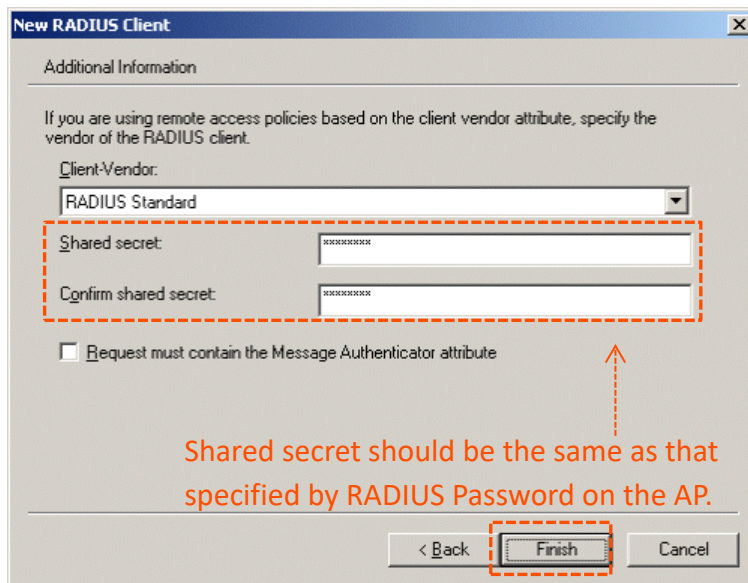
1. In the **Computer Management** dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.



2. Enter a RADIUS client name (device name of the AP is recommended) and the IP address of the AP, and click **Next**.

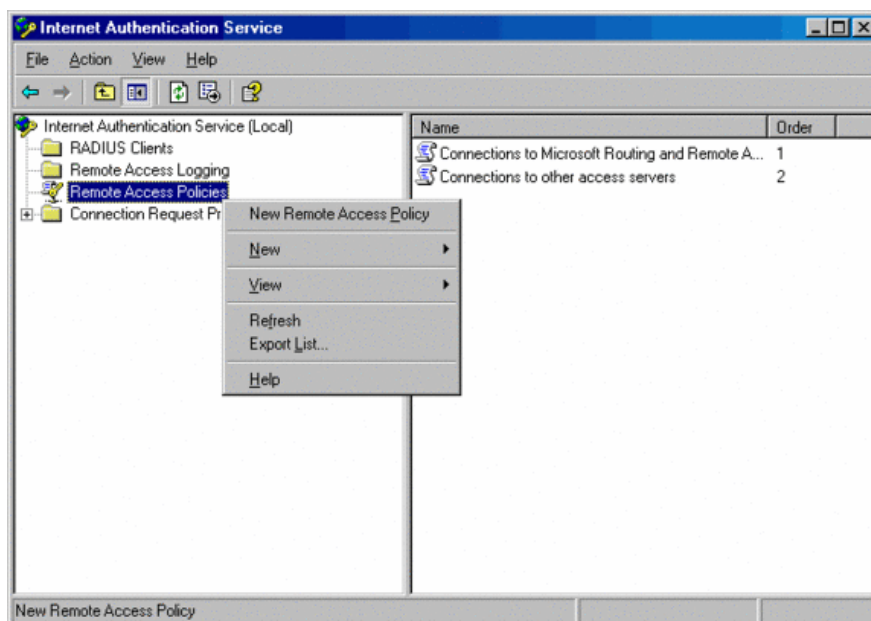


3. Enter **UmXmL9UK** in the **Shared secret** and **Confirm shared secret** text boxes, and click **Finish**.

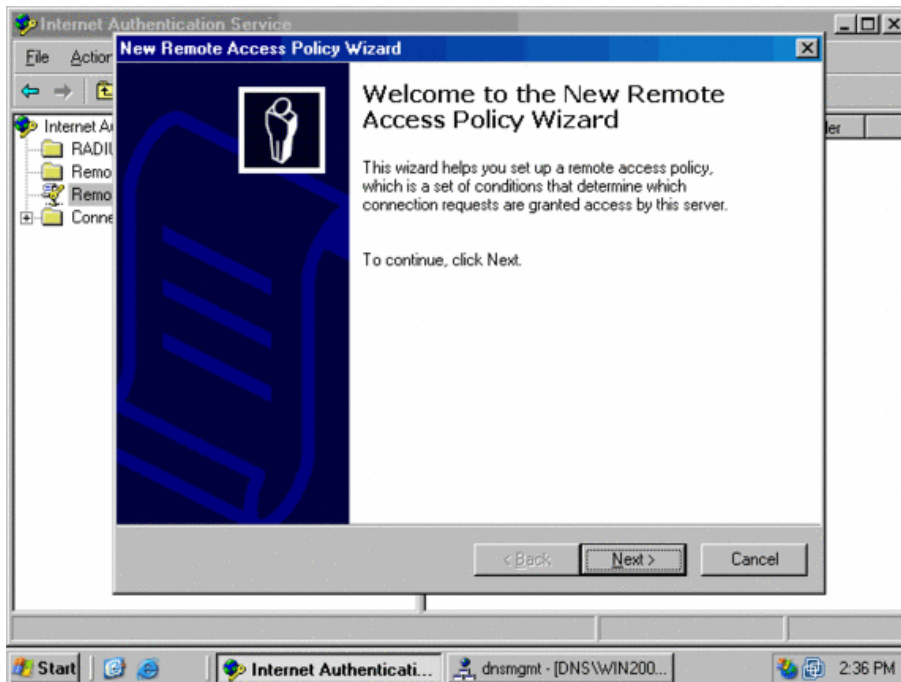


Step 2 Configure a remote access policy.

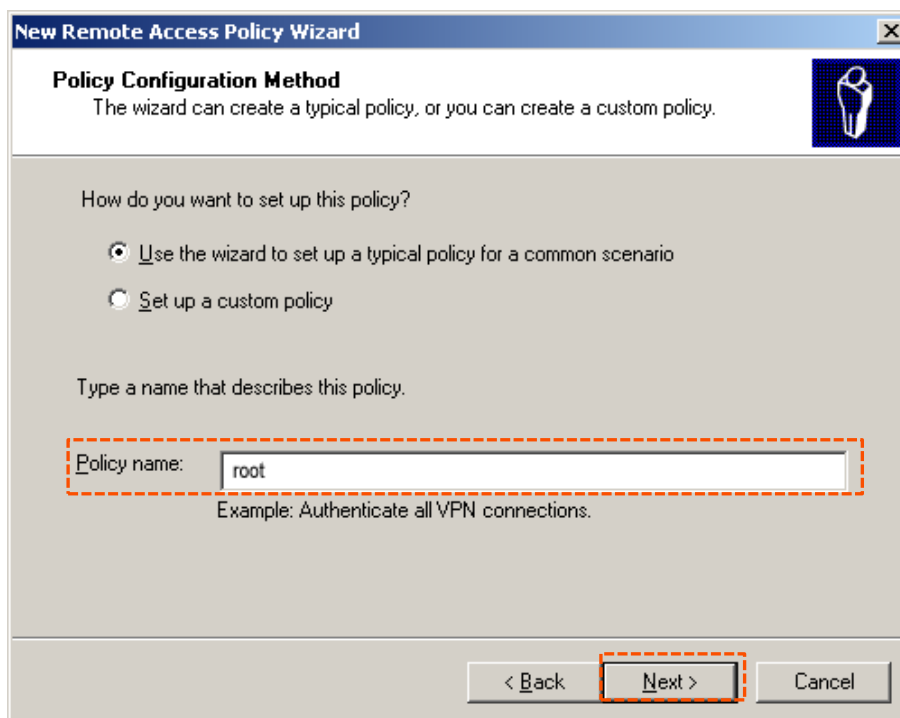
1. Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



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



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



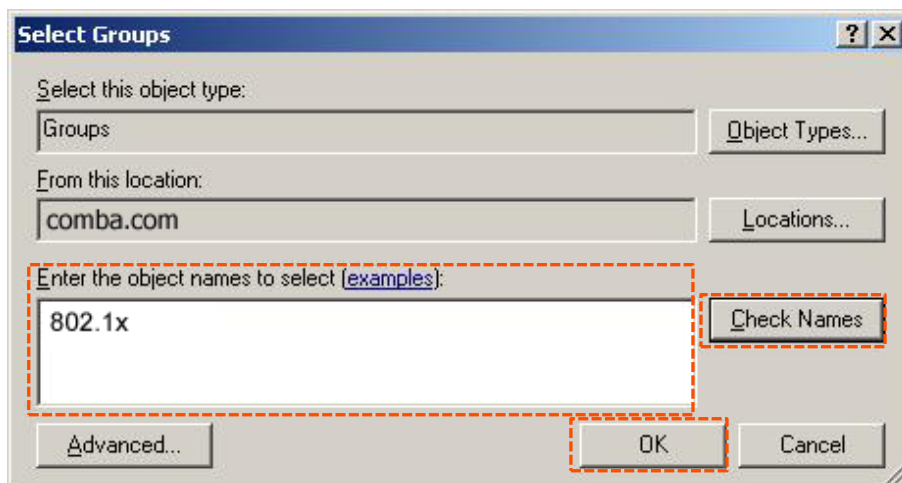
4. Select **Ethernet** and click **Next**.

The screenshot shows the 'New Remote Access Policy Wizard' dialog box. The title bar reads 'New Remote Access Policy Wizard'. The main heading is 'Access Method' with a sub-heading 'Policy conditions are based on the method used to gain access to the network.' Below this, there is a text prompt: 'Select the method of access for which you want to create a policy.' There are three radio button options: 'VPN' (with sub-text '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' (with sub-text 'Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.'), and 'Wireless' (with sub-text 'Use for wireless LAN connections only.'). The 'Ethernet' option is selected and highlighted with a dashed orange box; its sub-text is 'Use for Ethernet connections, such as connections that use a switch.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is also highlighted with a dashed orange box.

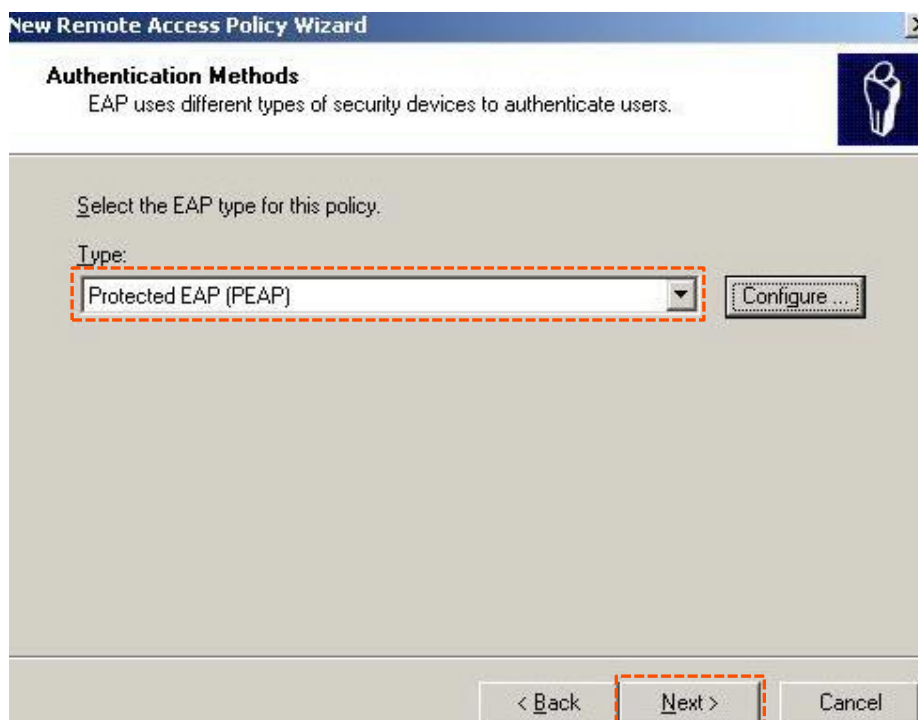
5. Select **Group** and click **Add**.

The screenshot shows the 'New Remote Access Policy Wizard' dialog box. The title bar reads 'New Remote Access Policy Wizard'. The main heading is 'User or Group Access' with a sub-heading 'You can grant access to individual users, or you can grant access to selected groups.' Below this, there is a text prompt: 'Grant access based on the following:'. There are two radio button options: 'User' (with sub-text 'User access permissions are specified in the user account.') and 'Group' (with sub-text 'Individual user permissions override group permissions.'). The 'Group' option is selected and highlighted with a dashed orange box. Below the 'Group' option is a text field labeled 'Group name:' which is currently empty. To the right of the text field are two buttons: 'Add...' and 'Remove'. The 'Add...' button is highlighted with a dashed orange box. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

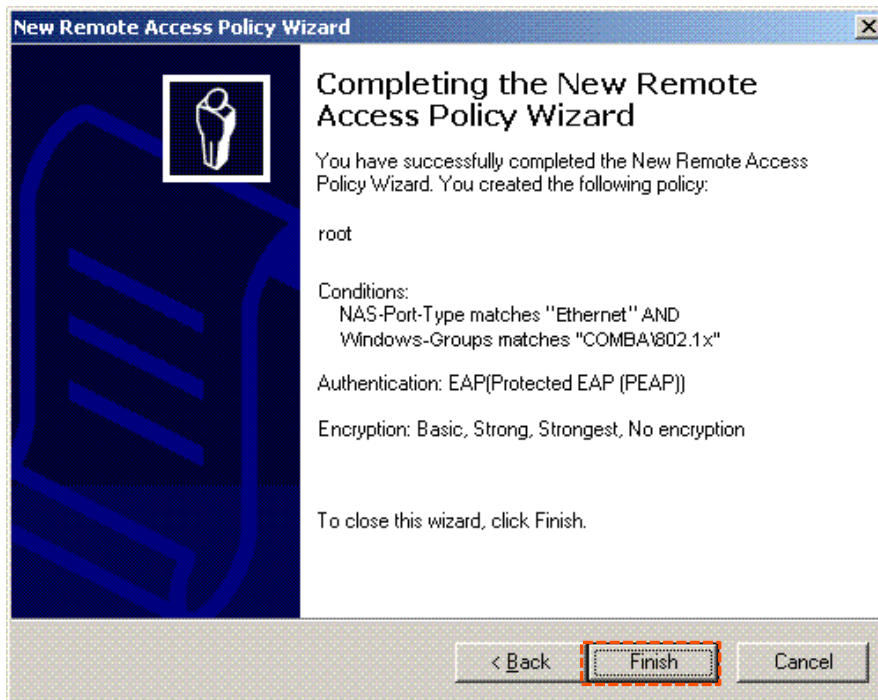
- Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



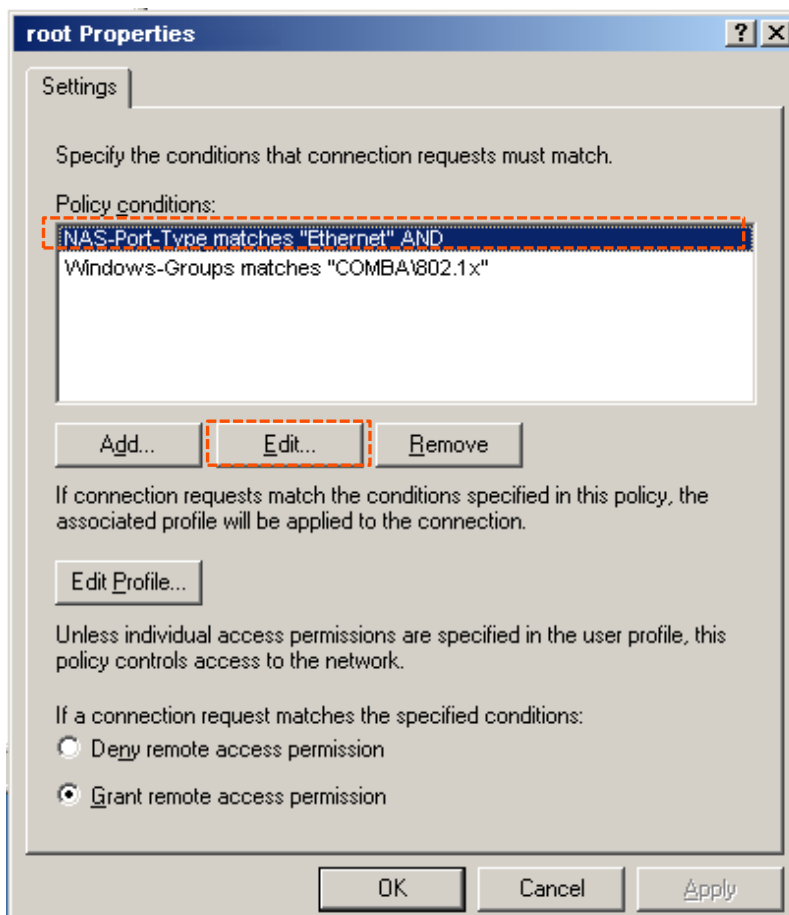
- Select **Protected EAP (PEAP)** and click **Next**.



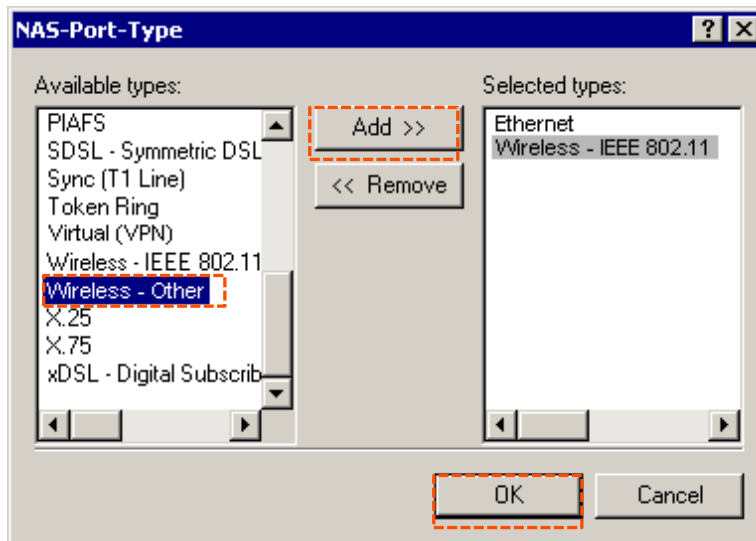
- Click **Finish**. The remote access policy is created.



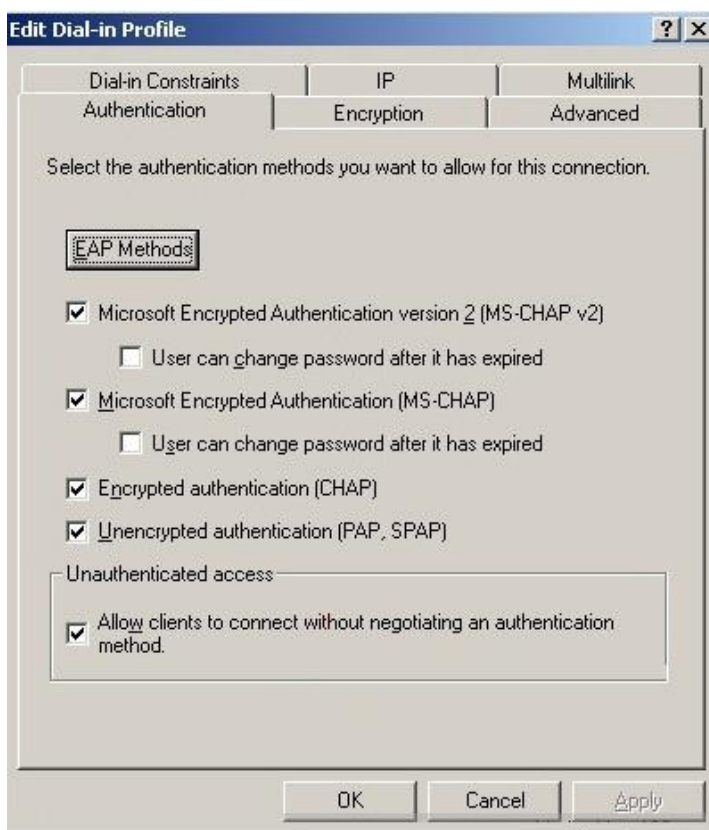
- Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



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



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



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

Step 3 Configure user information.

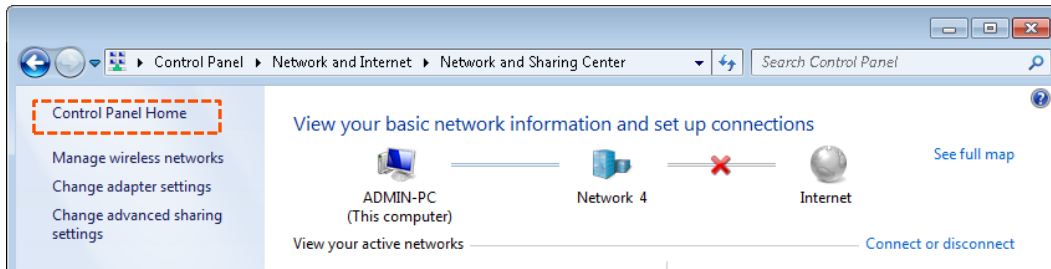
Create a user and add the user to group **802.1x**.

Configure your wireless device.

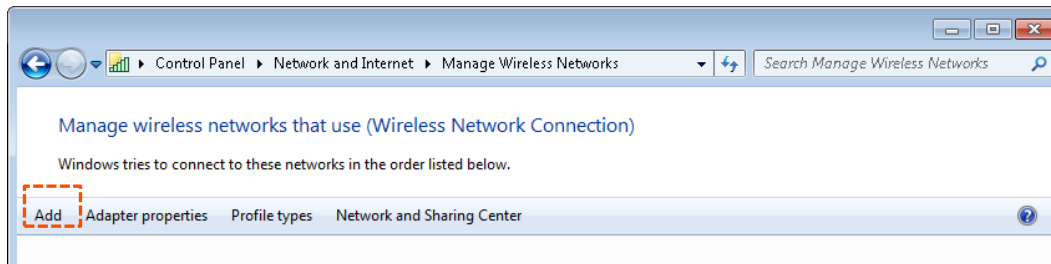


Windows 7 is taken as an example to describe the procedure.

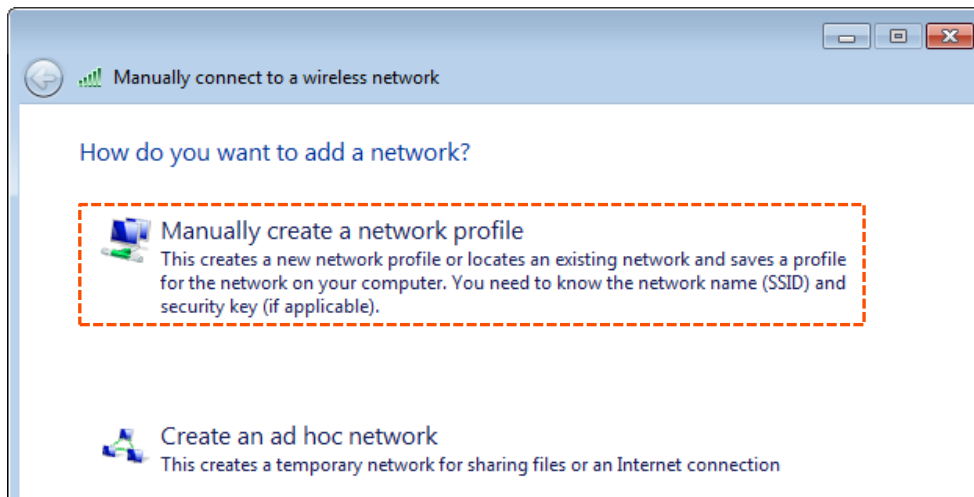
- Step 1** Choose **Start > Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



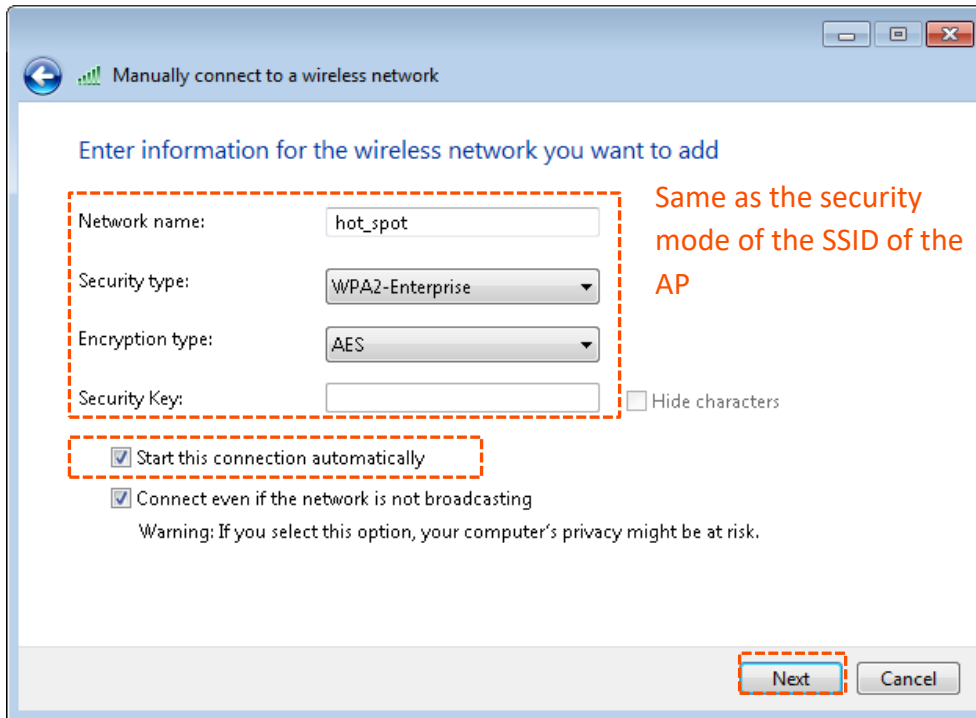
- Step 2** Click **Add**.



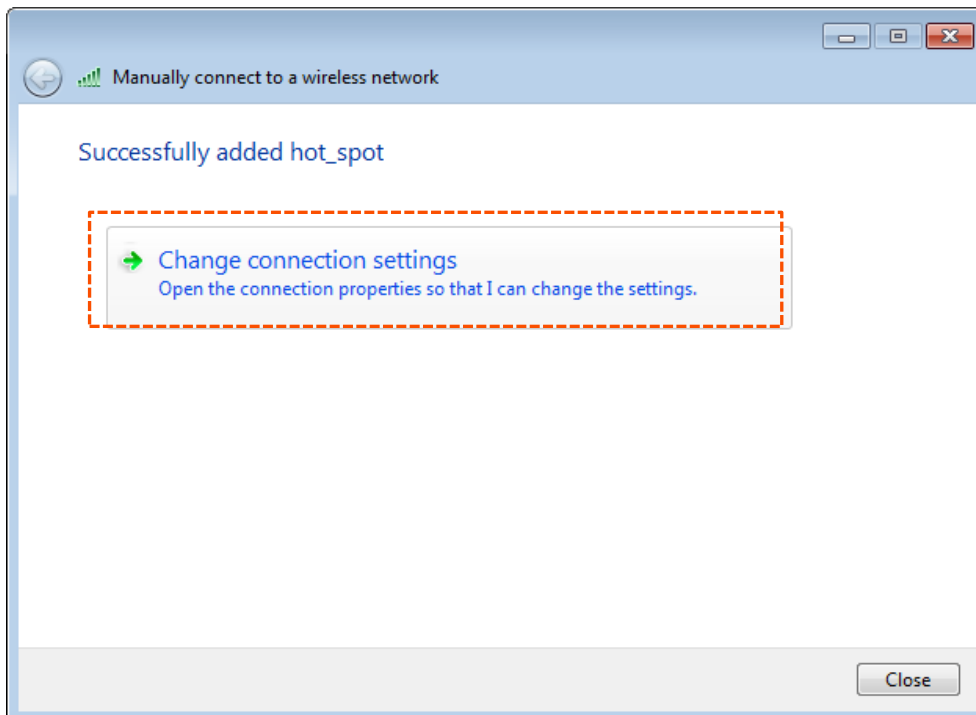
- Step 3** Click **Manually create a network profile**.



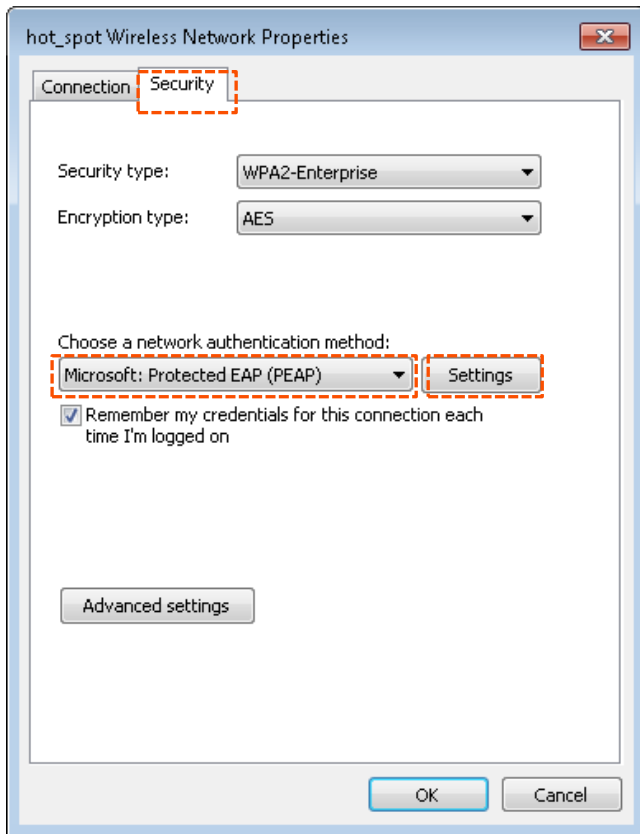
Step 4 Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.



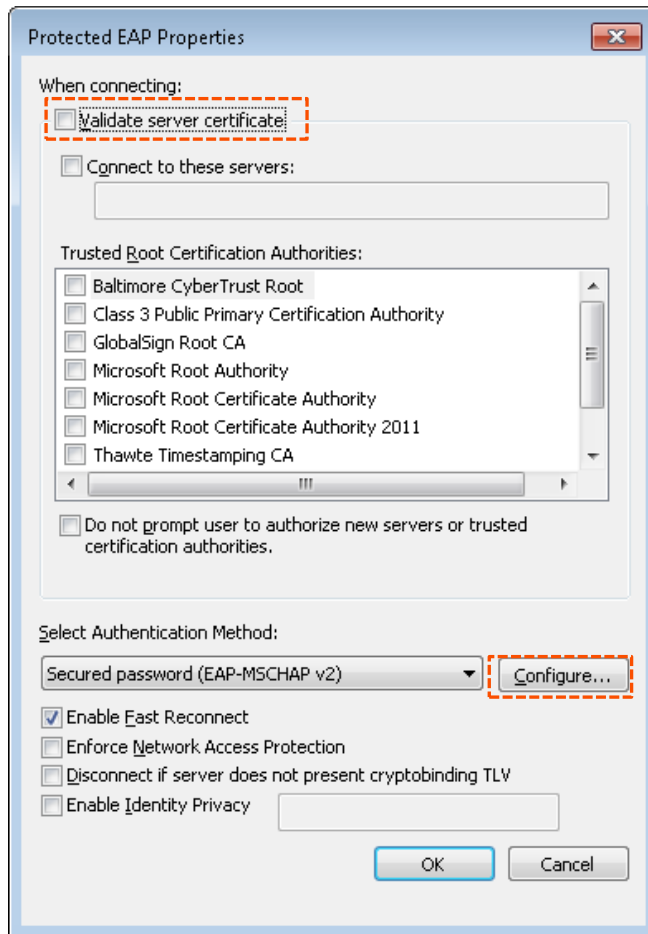
Step 5 Click **Change connection settings**.



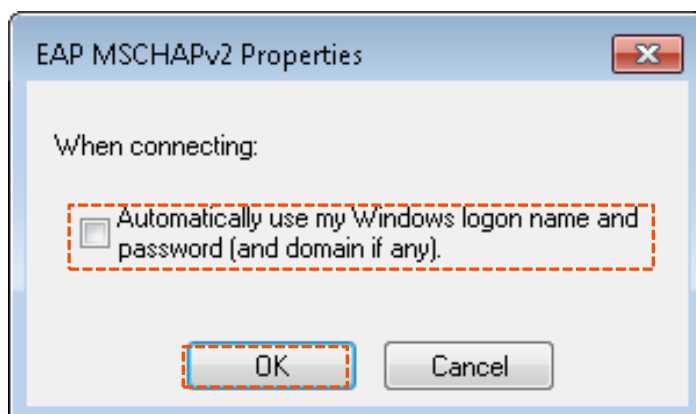
Step 6 Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



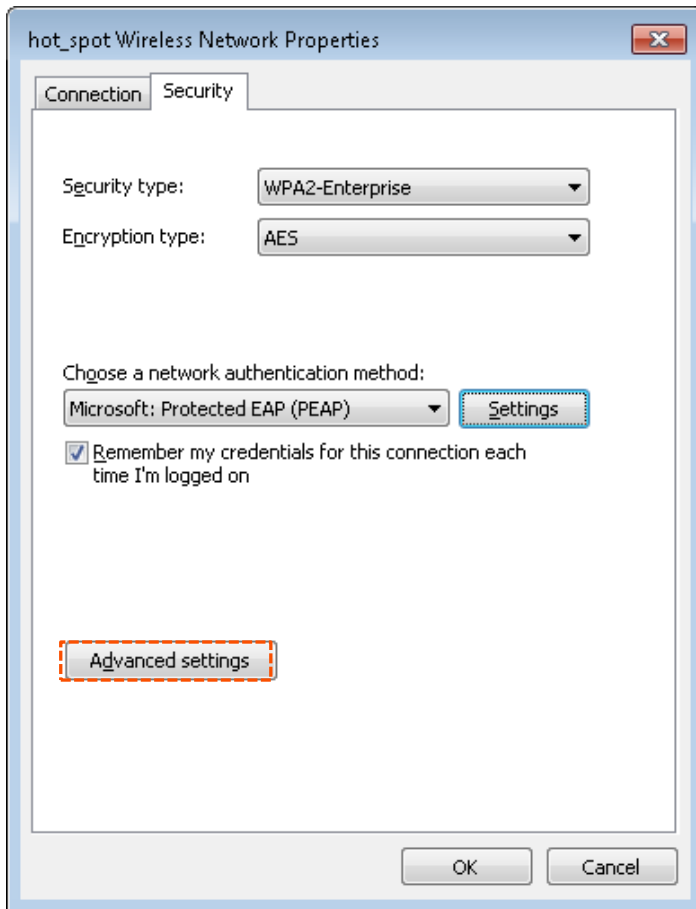
Step 7 Deselect **Validate server certificate** and click **Configure**.



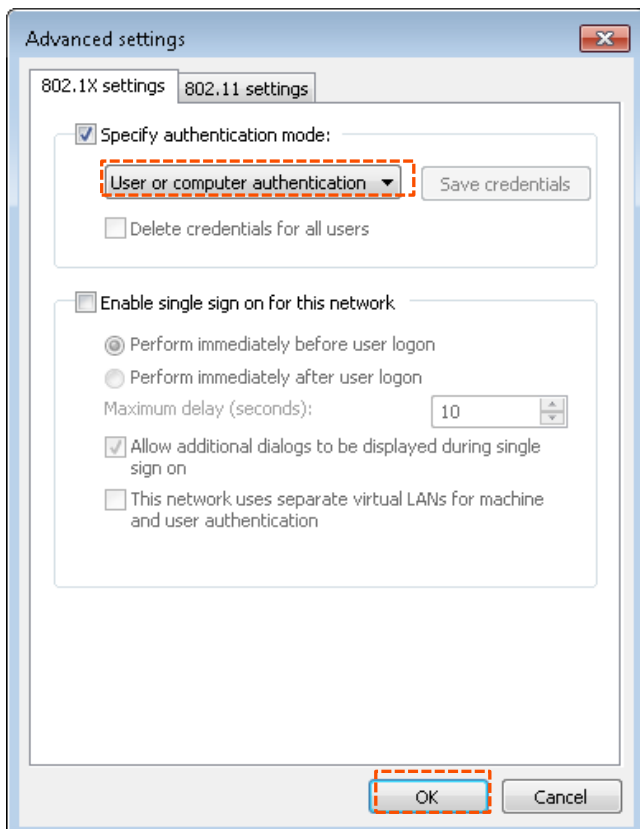
Step 8 Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



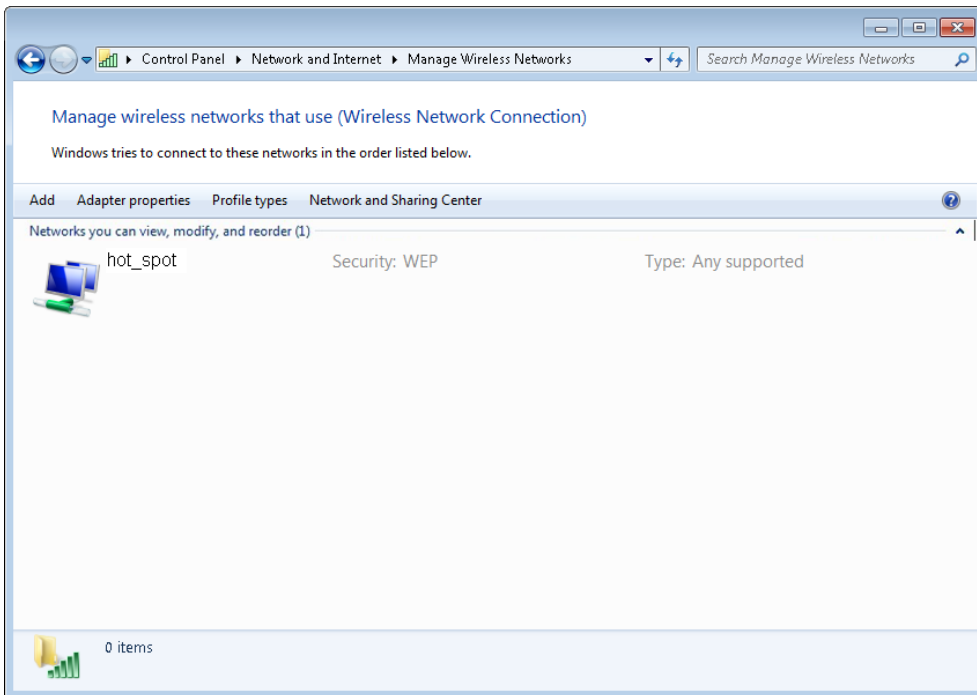
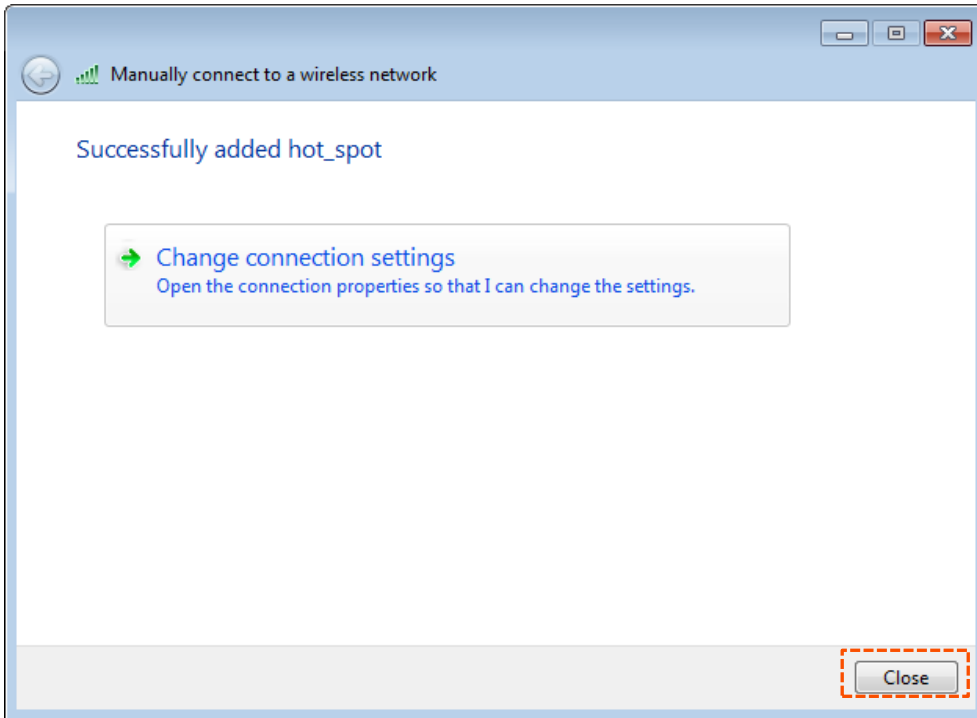
Step 9 Click **Advanced settings**.



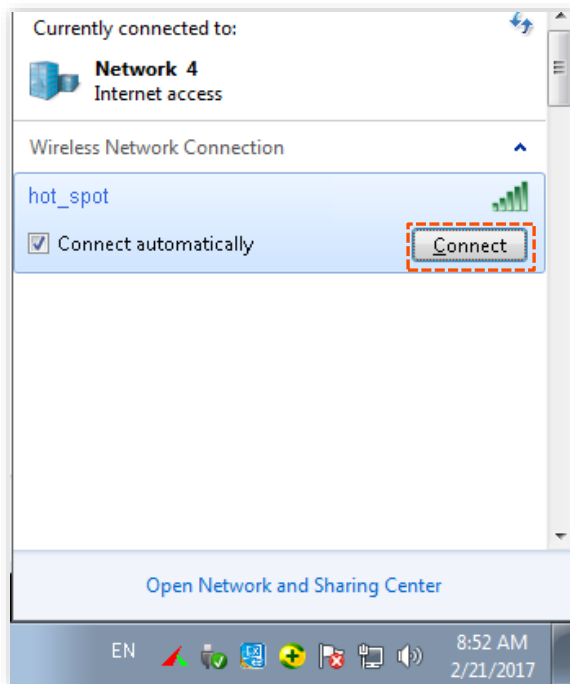
Step 10 Select **User or computer authentication** and click **OK**.



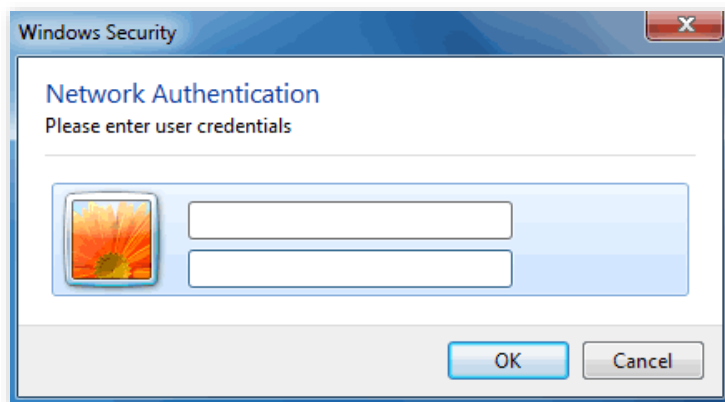
Step 11 Click **Close**.



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



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



---- End

Verification

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

6.2 RF settings

The **RF Settings** page allows you to configure advanced settings about the AP.

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

The screenshot shows the RF Settings interface. At the top, there are tabs for '2.4 GHz' and '5 GHz'. A red question mark icon is in the top right corner. The 'Wireless Network' toggle is turned on. Below it are several configuration options:

- Country/Region:** A dropdown menu set to 'China'.
- Network Mode:** A dropdown menu set to '11b/g/n/ax'.
- Channel:** A dropdown menu set to 'Auto'.
- Channel Bandwidth:** A dropdown menu set to '20/40MHz'.
- Extension Channel:** A dropdown menu set to 'Auto'.
- Lock Channel:** An unchecked checkbox.
- Transmit Power:** A slider ranging from 10dBm to 15dBm, with the current value set to 15.

Parameter description

Parameter	Description
Wireless Network	It specifies whether to enable the wireless function of the AP.
Country/Region	It specifies the country or region where the AP is used. This parameter helps comply with channel regulations of the country or region. The default value is China . This parameter can be set if Lock Channel is not selected.

Parameter	Description
Network Mode	<p>It specifies the wireless network mode of the AP. This parameter can be set if Lock Channel is not selected.</p> <p>Available options for 2.4 GHz are 11b, 11g, 11b/g, 11b/g/n, 11b/g/n/ax.</p> <ul style="list-style-type: none"> • 11b: The AP works in 802.11b mode and only wireless devices compliant with 802.11b can connect to the 2.4 GHz wireless networks of the AP. • 11g: The AP works in 802.11g mode and only wireless devices compliant with 802.11g can connect to the 2.4 GHz wireless networks of the AP. • 11b/g: The AP works in 802.11b/g mode and only wireless devices compliant with 802.11b or 802.11g can connect to the 2.4 GHz wireless networks of the AP. • 11b/g/n: The AP works in 802.11b/g/n mode. Wireless devices compliant with 802.11b or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n can connect to the 2.4 GHz wireless networks of the AP. • 11b/g/n/ax: The AP works in 11b/g/n/ax mode. Wireless devices compliant with 802.11b, or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n or 802.11ax can connect to the 2.4 GHz wireless networks of the AP. <p>Available options for 5 GHz are 11a, 11ac, 11a/n, and 11a/n/ac/ax.</p> <ul style="list-style-type: none"> • 11a: The AP works in 802.11a mode and only wireless devices compliant with 802.11a can connect to the 5 GHz wireless networks of the AP. • 11ac: The AP works in 802.11ac mode and only wireless devices compliant with 802.11ac can connect to the 5 GHz wireless networks of the AP. • 11a/n: The AP works in 802.11a/n mode and only wireless devices compliant with 802.11a or 802.11n can connect to the 5 GHz wireless networks of the AP. • 11a/n/ac/ax: The AP works in 11a/n/ac/ax mode. Wireless devices compliant with 802.11a, or 802.11ac and wireless devices working at 5 GHz and compliant with 802.11n or 802.11ax can connect to the 5 GHz wireless networks of the AP.
Channel	<p>It specifies the operating channel of the AP. This parameter can be set if Lock Channel is not selected.</p> <p>Auto: It indicates that the AP automatically adjusts its operating channel according to the ambient environment.</p>

Parameter	Description
Channel Bandwidth	<p>It specifies the wireless channel bandwidth of the AP. This parameter can be set if the AP works in 802.11 b/g/n, 802.11b/g/n/ax, 802.11ac, 802.11a/n, or 11a/n/ac/ax mode and Lock Channel is not selected.</p> <ul style="list-style-type: none"> • 20 MHz: It indicates that the AP can use only 20 MHz channel bandwidth. • 40 MHz: It indicates that the AP can use only 40 MHz channel bandwidth. • 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. • 80 MHz: Only available for 5 GHz. It indicates that the AP can use only 80 MHz channel bandwidth. • 160 MHz: Only available for 5 GHz. It indicates that the AP can use only 160 MHz channel bandwidth. • 20/40/80/160 MHz: Only available for 5 GHz. It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz, 40 MHz, 80 MHz, or 160 MHz according to the ambient environment.
Extension Channel	It is used to determine the operating frequency band of this device when the device uses the 40 MHz channel bandwidth in 11n mode for 2.4 GHz.
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	<p>It specifies the transmit power of the AP.</p> <p>A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the wireless network performance and security.</p>
Lock Power	It specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.
Preamble	<p>A preamble is a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data.</p> <p>By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the Short Preamble option.</p>
Short GI	<p>Short Guard Interval.</p> <p>There is a delay on the receiving side due to multipath and other factors during the wireless signal transmission in space. If the subsequent data block is transmitted too quickly, it will interfere with the previous data block, and the short guard interval can be used to circumvent this interference. Short GI helps to increase the wireless throughput by 10%.</p>

Parameter	Description
Suppress Broadcast Probe Response	<p>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.</p> <p>After this function is enabled, this device does not respond to the requests without an SSID, saving wireless resources.</p>

6.3 RF optimization

The **RF Optimization** page allows you to modify the radio parameters to optimize performance.

To access the page, choose **Wireless > RF Optimization**.



You are recommended to retain the default settings if without the professional guidance to prevent degrading wireless performance of the AP.

2.4 GHz 5 GHz
?

Beacon Interval ms (Range: 20 to 999. Default: 100)

Fragment Threshold (Range: 256 to 2346. Default: 2346)

RTS Threshold (Range: 1 to 2347. Default: 2347)

DTIM Interval (Range: 1 to 255. Default: 1)

RSSI Threshold dBm (Range: -90 to -60. Default: -90)

Signal Transmission Coverage-oriented Capacity-oriented

Air Interface Scheduling Enable Disable

Anti-interference Mode (Range: 0 to 3. Default: 3)

Parameter description

Parameter	Description
Beacon Interval	Used to set the interval at which this device sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.

Parameter	Description
Fragment Threshold	<p>It specifies the threshold of a fragment.</p> <p>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.</p> <p>In case of a high error rate, you can reduce the threshold to enable this device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput.</p> <p>In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput.</p>
RTS Threshold	<p>It specifies the frame length threshold for triggering the RTS/CTS mechanism. The unit is byte.</p> <p>If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts.</p> <p>Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold to reduce conflicts.</p> <p>The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.</p>
DTIM Interval	<p>It specifies the countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval.</p> <p>For example, if DTIM Interval is set to 1, this device transmits all cached frames at one Beacon interval.</p>
RSSI Threshold	<p>It specifies the minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device.</p> <p>A proper value facilitates wireless devices to connect to the AP with stronger signal in case of multiple APs exist.</p>
Signal Transmission	<ul style="list-style-type: none"> • Coverage-oriented: This mode broadens WiFi coverage of APs, and is usually used in scenarios deployed with fewer APs, such as offices, warehouses, and hospitals. • Capacity-oriented: This mode effectively decreases mutual interference among APs, and is usually used in scenarios deployed with massive APs, such as conferences, exhibition halls, banquet halls, stadiums, classrooms of higher-education institutes, airports and so on.
Prioritize 5 GHz	<p>If this function is enabled, dual band wireless devices prefer the 5 GHz WiFi network of the AP to connect when the 5 GHz signal strength transmitted by devices is equal to or stronger than the Prioritize 5 GHz Threshold.</p>
Prioritize 5 GHz Threshold	<p>With Prioritize 5 GHz function enabled, if the strength of the signals transmitted by a wireless device is equal to or stronger than this threshold, the wireless device connects to the 5 GHz WiFi network. Otherwise, it connects to the 2.4 GHz WiFi network.</p>

Parameter	Description
Air Interface Scheduling	<p>Used to enable or disable the air interface scheduling function of the AP.</p> <p>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.</p>
Anti-interference Mode	<p>It specifies the anti-interference modes you can select for your AP.</p> <ul style="list-style-type: none"> • 0 (Disable): Interference suppression measures are disabled. • 1 (Suppress weak interference): Suppress mild interference for weak radio environment. • 2 (Suppress moderate interference): Suppress moderate interference for bad radio environment. • 3 (Suppress critical interference): Suppress critical interference for heavy loading radio environment.
APSD	<p>Automatic Power Save Delivery.</p> <p>APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.</p>
MU-MIMO	<p>Multi-User Multiple-Input Multiple-Output.</p> <p>If this function is enabled, AP can communicate with multiple users concurrently, avoiding WiFi network congestion and improving communication.</p>
OFDMA	<p>Orthogonal Frequency Division Multiple Access.</p> <p>If this function is enabled, multiple clients can transmit data at the same time, so that the transmission efficiency is improved, delay is reduced, and user experience is enhanced.</p> <p>However, this function may cause compatibility issues; therefore, you are recommended to disable this function to avoid compatibility issues.</p>
Client Timeout Interval	<p>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.</p>
Mandatory Rate	<p>It specifies rates that wireless clients must support in order to connect to the wireless networks of this device.</p>
Optional Rate	<p>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.</p>

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 evolution 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.



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.

6.4 Frequency analysis

6.4.1 Overview

The **Frequency Analysis** page allows you to analyze frequency and the **Channel Scan** page allows you to scan channels.

To access the pages, choose **Wireless > Frequency Analysis**.

■ Frequency Analysis

From the intuitive result, you can check how many wireless networks (total SSIDs) use the same channel and choose a channel with low usage as the operating channel of the device for better wireless transmission efficiency.

■ Channel Scan

The scan result list presents you with information about nearby wireless network, including SSID, MAC address, channel, channel bandwidth, and signal strength.

6.4.2 View frequency analysis

Step 1 Choose **Wireless > Frequency Analysis**.

Step 2 Click **2.4 GHz Frequency Analysis** or **5 GHz Frequency Analysis** tab to select the wireless network radio band for frequency analysis. **2.4 GHz Frequency Analysis** is taken as an example here.

Step 3 Enable **Scan**.

The screenshot shows the '2.4 GHz Frequency Analysis' tab selected. At the top, there are tabs for '2.4 GHz Frequency Analysis', '5 GHz Frequency Analysis', '2.4 GHz Channel Scan', and '5 GHz Channel Scan'. Below the tabs, there is a 'Scan' toggle switch (currently turned on) and a 'Rescan' button. A table displays the results for 13 channels. The 'Channel Usage (%)' row is color-coded: red for high usage (96%), yellow for moderate usage (74%), and green for low usage (all other channels).

Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
Total SSID:	27	4	8	5	3	18	6	5	5	6	25	0	3
Channel Usage (%)	96	25	44	28	20	74	35	30	30	35	96	5	19

---End

After scanning, you can select a channel with low usage as the AP operating channel.

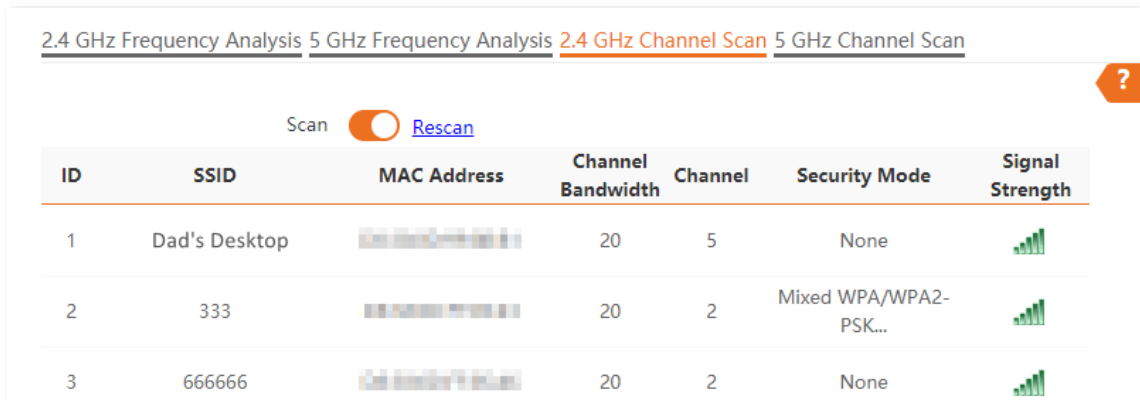
- ■: High channel usage. The channel is not recommended.
- ■: Moderate channel usage.
- ■: Low channel usage. The channel is recommended.

6.4.3 Execute channel scan

Step 1 Choose **Wireless > Frequency Analysis**.

Step 2 Click **2.4 GHz Channel Scan** or **5 GHz Channel Scan** tab to select the wireless network radio band for channel scan. **2.4 GHz Channel Scan** is taken as an example here.

Step 3 Enable **Scan**.



The screenshot shows the '2.4 GHz Channel Scan' interface. At the top, there are four tabs: '2.4 GHz Frequency Analysis', '5 GHz Frequency Analysis', '2.4 GHz Channel Scan' (which is selected and highlighted in orange), and '5 GHz Channel Scan'. Below the tabs, there is a 'Scan' toggle switch that is turned on, and a 'Rescan' button. A help icon (?) is visible in the top right corner. The main content is a table with the following columns: ID, SSID, MAC Address, Channel Bandwidth, Channel, Security Mode, and Signal Strength. The table contains three rows of data.

ID	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
1	Dad's Desktop	[blurred]	20	5	None	[signal strength icon]
2	333	[blurred]	20	2	Mixed WPA/WPA2-PSK...	[signal strength icon]
3	666666	[blurred]	20	2	None	[signal strength icon]

---End

6.5 WMM

6.5.1 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.

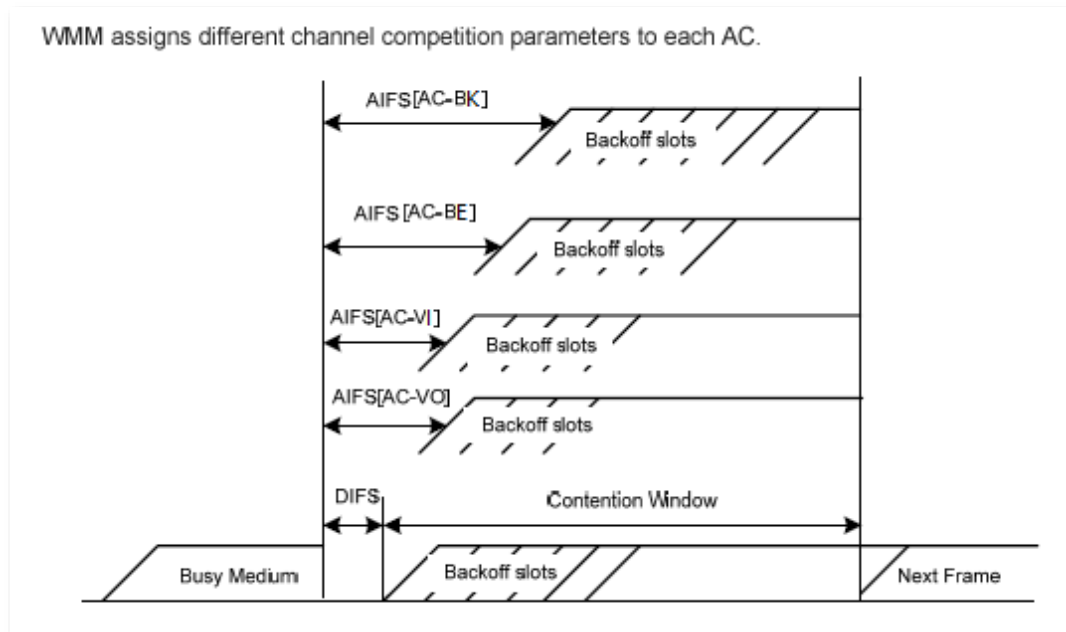
EDCA Parameters

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.

6.5.2 Configure WMM settings



The WMM function of the corresponding radio band cannot be set to **Disable** in the following cases:

- The network mode of the AP at 2.4 GHz is **11b/g/n** or **11b/g/n/ax**
- The network mode of the AP at 5 GHz is **11a/n**, **11ac** or **11a/n/ac/ax**.

The **WMM** page allows you to enable or disable the WMM function of the corresponding radio band of the AP. This function is enabled by default.

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

2.4 GHz 5 GHz
?

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	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="3"/>	<input type="text" value="0"/>
AC_BK	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="1"/>	<input type="text" value="94"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="1"/>	<input type="text" value="47"/>

EDCA STA Parameter

	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="3"/>	<input type="text" value="0"/>
AC_BK	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="94"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="47"/>

Save
Cancel

Parameter description

Parameter	Description
WMM Optimization	<p>It specifies the WMM optimization modes supported by the AP:</p> <ul style="list-style-type: none"> • Optimized for scenario with 1 - 10 users: If 10 or less clients are connected to the AP, you are recommended to select this mode to obtain higher client throughput. • Optimized for scenario with more than 10 users: If more than 10 clients are connected to the AP, you are recommended to select this mode to ensure client connectivity. • Custom: This mode enables you to set the WMM EDCA parameters for manual optimization.
No ACK	<p>Available when WMM Optimization is set to Custom.</p> <p>No Acknowledgement (No ACK): When this policy is used, the recipient will not acknowledge received packets during wireless packet exchange. It is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.</p> <ul style="list-style-type: none"> • If the check box is selected, the No ACK policy is adopted. • If the check box is deselected, the Normal ACK policy is adopted.
EDCA Parameters	<p>Available when WMM Optimization is set to Custom.</p> <p>For details, refer to EDCA Parameters.</p>

6.6 Access control

6.6.1 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.

To access the page, choose **Wireless > Access Control**.

The AP supports the following 2 filter modes:

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

Access Control is disabled by default.

2.4 GHz 5 GHz
?

SSID


Access Control

Mode Blacklist Whitelist

MAC Address

ID	MAC Address	Status	Operation
No data			

Parameter description

Parameter	Description
SSID	It specifies the wireless network to which the rule applies.
Access Control	It specifies whether to enable this function.
Mode	Set access control mode. <ul style="list-style-type: none"> • Blacklist: It indicates that only the wireless clients on the wireless access control list cannot connect to the AP with the selected SSID. • Whitelist: It indicates that only the wireless clients on the wireless access control list can connect to the AP with the selected SSID.
MAC Address	It specifies the MAC address of client.
Add	Manually add the device with the MAC address you specified to the access control list.
Add Online Devices	Add the online wireless clients to the access control list conveniently.
Status	It specifies the status of the rule. You can enable or disable it as required.
Operation	Click  to delete the rule.

6.6.2 Configure access control

- Step 1** Choose **Wireless > Access Control**. Choose a wireless network radio band on which access control is to be configured.
- Step 2** Select the SSID to which the access control is applied from the **SSID** drop-down list menu.
- Step 3** Enable **Access Control**.
- Step 4** Set **Mode** to **Blacklist** or **Whitelist**.
- Step 5** Enter the MAC address of the wireless device to which the rule applies. Then 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 6** Click **Save**.

----End

6.6.3 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 **D8:38:0D:00:00:01**, **D8:38:0D:00:00:02**, and **D8:38:0D: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 **D8:38:0D:00:00:01** in the **MAC Address** text box and click **Add**. Repeat this step to add **D8:38:0D:00:00:02** and **D8:38:0D:00:00:03** as well.
 - Step 6** Click **Save**.
- End

The following figure shows the configuration.

The screenshot shows the configuration page for the 5 GHz radio band. The SSID is set to 'VIP'. The 'Access Control' toggle is turned on. The 'Mode' is set to 'Whitelist'. Below this, there is a 'MAC Address' input field with a format hint 'Format: XX:XX:XX:XX:XX:XX' and two buttons: 'Add' and 'Add Online Devices'. A table below lists the configured MAC addresses and their status.

ID	MAC Address	Status	Operation
1	D8:38:0D:00:00:01	Enable	🗑️
2	D8:38:0D:00:00:02	Enable	🗑️
3	D8:38:0D:00:00:03	Enable	🗑️

At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons.

Verification

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

6.7 Advanced settings

The **Advanced Settings** 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.

The screenshot shows the 'Advanced Settings' page with the following configuration:

- Identify Client Type:** Enable, Disable
- Broadcast Packet Filter:** Enable, Disable
- Filters:** A dropdown menu currently set to 'Excludes ARP'.
- Buttons:** 'Save' (orange) and 'Cancel' (white).

Parameter description

Parameter	Description
Identify Client Type	If this function is enabled and the client connected to the AP has accessed an http://URL , the operating system type of the client can be viewed when you choose Status > Client List .
Broadcast Packet Filter	If this function is enabled, the AP can reduce air interface resources usage and ensure the bandwidth for business data transfer.
Filters	Select a mode after you enable the Broadcast Packet Filter function. <ul style="list-style-type: none"> • Excludes DHCP and ARP: Filter out all broadcast or multicast data except DHCP and ARP packets. • Excludes ARP: Filter out all broadcast or multicast data except ARP packets.

6.8 QVLAN settings

6.8.1 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.

The **QVLAN Settings** page allows you to set VLAN IDs of all wireless networks.

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

QVLAN Settings ?

QVLAN

PVID

Management VLAN


2.4 GHz SSID VLAN ID (1 to 4094)

Tenda_1DA278

5 GHz SSID VLAN ID (1 to 4094)

Tenda_1DA278_5G

Parameter description

Parameter	Description
QVLAN	It specifies whether to enable the QVLAN function of the AP.
PVID	It specifies the ID of the default native VLAN of the trunk port of the AP.
Management VLAN	It specifies the ID of the AP management VLAN. After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
2.4 GHz SSID	It specifies the currently enabled SSID(s) over the 2.4 GHz/5 GHz band of the AP, and the VLAN IDs corresponding to SSIDs.
5 GHz SSID	 TIP
VLAN ID	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.

6.8.2 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

Management VLAN

2.4 GHz SSID VLAN ID (1 to 4094)

* Tenda_1DA278

5 GHz SSID VLAN ID (1 to 4094)

* Tenda_1DA278_5G

---End

6.8.3 Example of configuring QVLAN

Networking requirement

A hotel has the following wireless network coverage requirements:

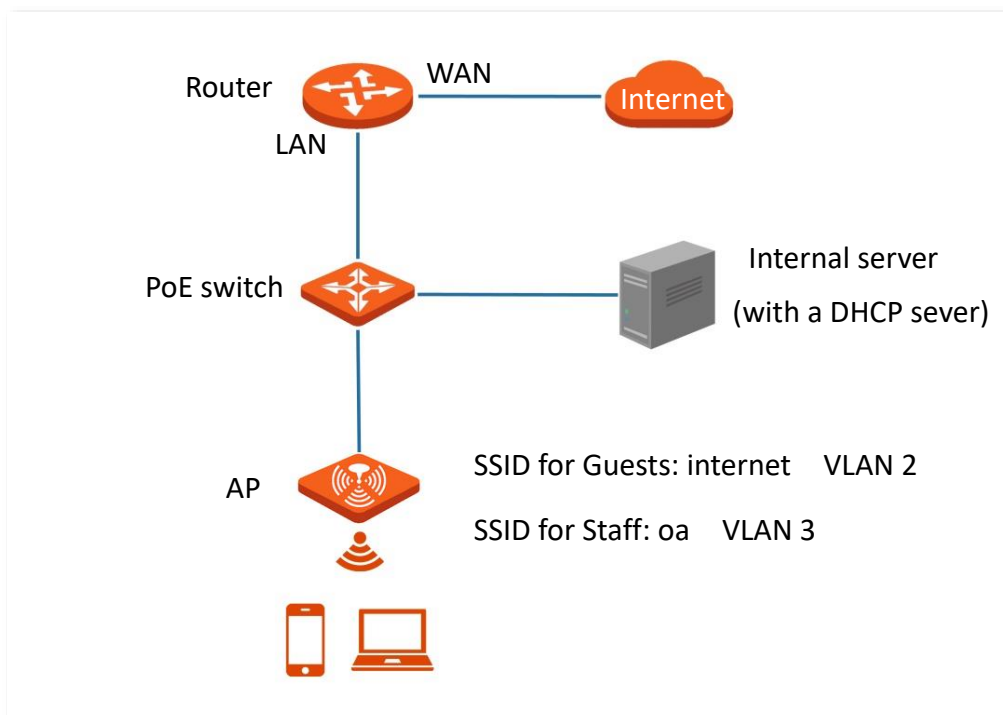
- Guests are connected to VLAN 2 and can only access the internet.
- Staff are connected to VLAN 3 and can only access the internal server.

Solution

- Set the SSID to **internet** for guests, **oa** for staff on the 2.4 GHz network.
- Configure VLANs for the above SSIDs on the AP.
- Configure VLAN forwarding rules on the switch.



The internal server must be deployed with a DHCP server in the LAN to assign IP addresses to downlink devices.



Configuration procedure

I. Configure the AP

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

Step 2 Enable QVLAN Settings.

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

Step 4 Click **Save**.

QVLAN Settings

* QVLAN

PVID

Management VLAN

2.4 GHz SSID VLAN ID (1 to 4094)

* internet

* oa

5 GHz SSID VLAN ID (1 to 4094)

Tenda_1DA278_5G

Step 5 Click **OK** after confirming the prompted message.

Wait for the automatic reboot of the AP.

II. Configure the switch

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

Port Connected To	Accessible VLAN ID	Port Type	PVID
AP	1,2,3	Trunk	1
Router	2	Access	2
Internal Server	3	Access	3

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

---End

Verification

Wireless clients connected to the **internet** wireless network can only access the internet, and wireless clients connected to the **oa** wireless network can only access the internal server.

7 Advanced

7.1 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.


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_1DA278	No Limit	No Limit	No Limit	No Limit	✎
5GHz	Tenda_1DA278_5G	No Limit	No Limit	No Limit	No Limit	✎

Parameter description


Parameter	Description
Traffic Control	<ul style="list-style-type: none"> • Disable: The Traffic Control function is disabled. • Manual: The Traffic Control function is enabled. The network administrator manually sets SSID and the maximum upload/download rate 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.

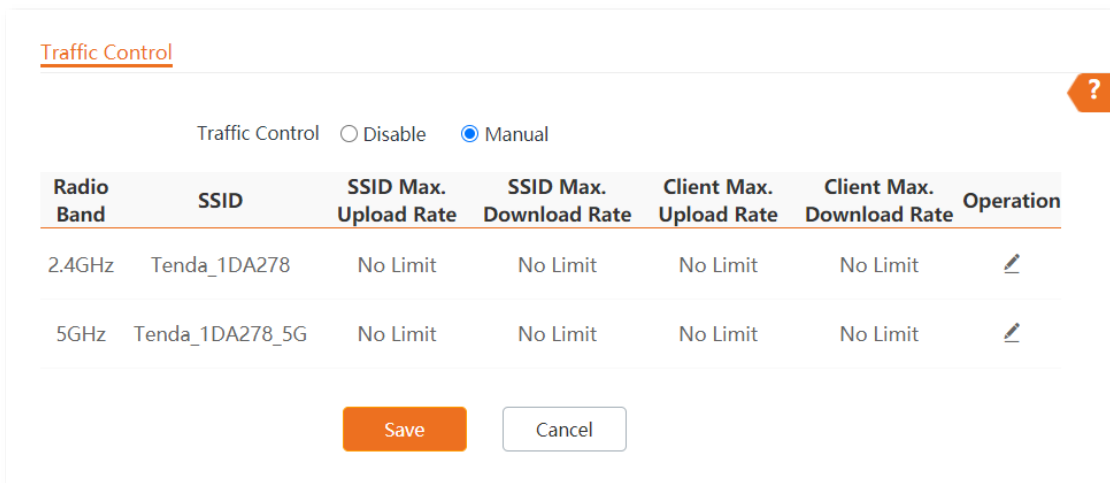
Parameter	Description
SSID Max. Upload Rate	They specify the maximum upload/download rate allowed for a WiFi network. If you leave them blank, the maximum upload/download rate of the target WiFi network are not limited.
SSID Max. Download Rate	
Client Max. Upload Rate	They specify the maximum upload/download rate allowed for every user device connected to the target WiFi network. If you leave them blank, the maximum upload/download rate of every user device connected to the target WiFi network are not limited.
Client Max. Download Rate	
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.

7.2 Configure traffic control



Step 1 Choose **Advanced**.

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.



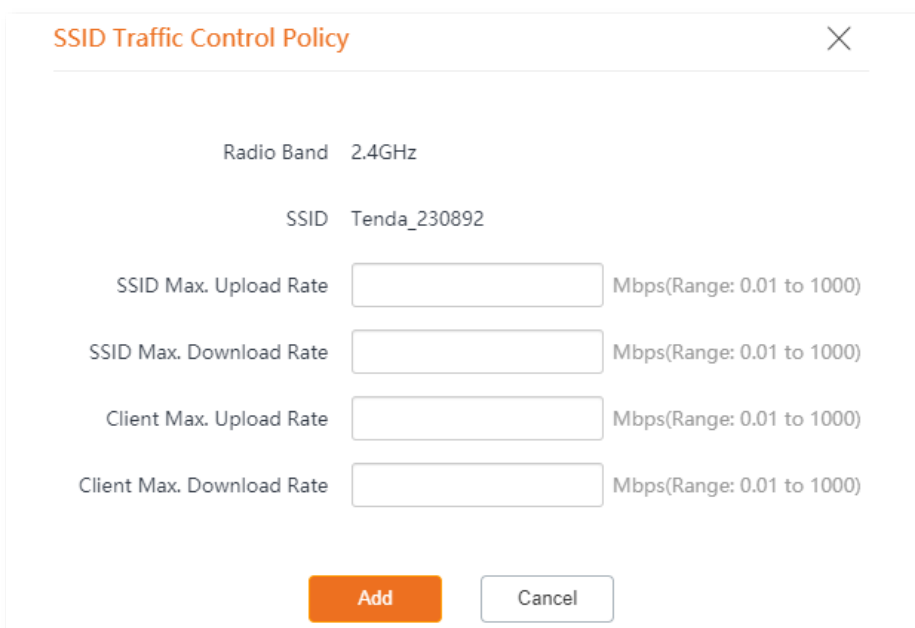
Traffic Control Disable Manual

Radio Band	SSID	SSID Max. Upload Rate	SSID Max. Download Rate	Client Max. Upload Rate	Client Max. Download Rate	Operation
2.4GHz	Tenda_1DA278	No Limit	No Limit	No Limit	No Limit	
5GHz	Tenda_1DA278_5G	No Limit	No Limit	No Limit	No Limit	

Save Cancel

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_230892

SSID Max. Upload Rate Mbps(Range: 0.01 to 1000)

SSID Max. Download Rate Mbps(Range: 0.01 to 1000)

Client Max. Upload Rate Mbps(Range: 0.01 to 1000)

Client Max. Download Rate Mbps(Range: 0.01 to 1000)

Add Cancel

---End

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

The **System Time** page allows you to set the system time.

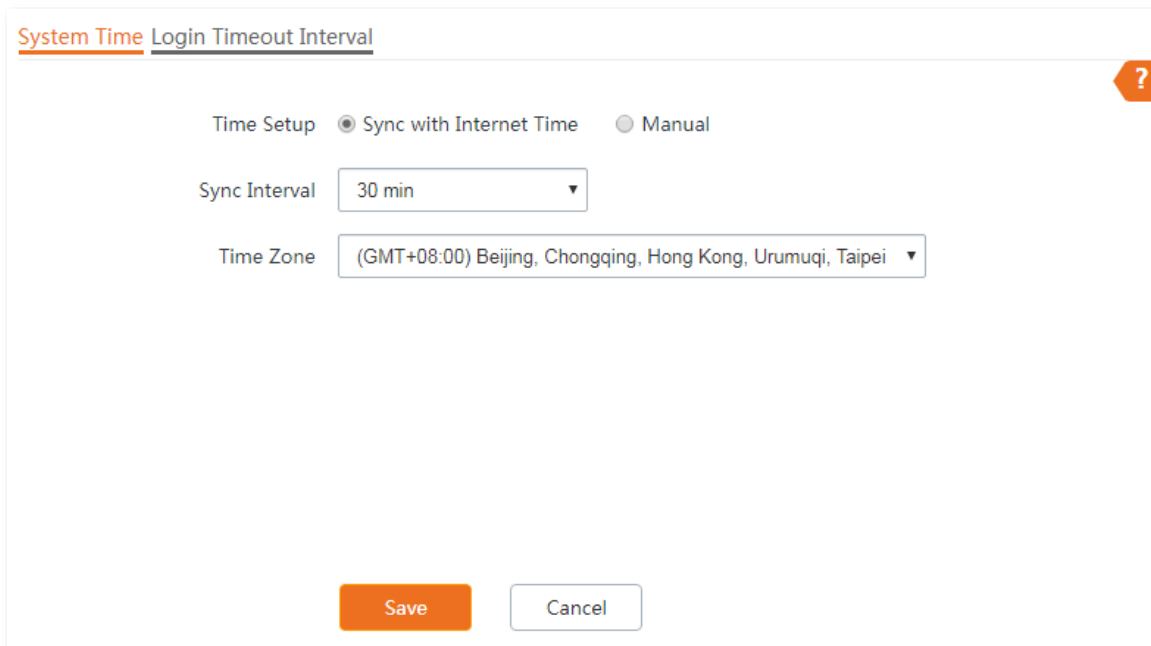
To access the page, choose **Tools > Date & Time > System Time**.

Ensure that the system time of the AP is correct, so that time-based functions can take effect properly. The AP supports [Sync with Internet Time](#) and [Manual](#) to correct the system time.

Sync 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 setting again.

For details about how to connect the AP to the internet, refer to [LAN Setup](#).



The screenshot shows a web interface for configuring system time. At the top, there are two tabs: "System Time" (selected) and "Login Timeout Interval". A question mark icon is in the top right corner. The "Time Setup" section has two radio buttons: "Sync with Internet Time" (selected) and "Manual". Below this, the "Sync Interval" is set to "30 min" in a dropdown menu. The "Time Zone" is set to "(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei" in a dropdown menu. At the bottom, there are two buttons: "Save" (orange) and "Cancel" (white with orange border).

Parameter description

Parameter	Description
Time Setup	It specifies the modes to set the system time.
Sync Interval	It is valid only when Sync with Internet Time is selected. It specifies the interval at which the AP will automatically synchronize with a time server of the internet.
Time Zone	It specifies the standard time zone of the region in which the AP locates.

Manual

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

Enter a correct date and time, or click **Sync with PC Time** to synchronize the system time of the AP with the system time (ensure that it is correct) of the management computer.

8.1.2 Login timeout interval

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

The **Login Timeout Interval** page allows you to modify the login timeout interval. The default login timeout interval is **5** minutes.

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

System Time Login Timeout Interval

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

?

Save Cancel

8.2 Maintenance

The **Maintenance** page allows you to [reboot](#) and [reset AP](#), [upgrade firmware](#), [back up or restore settings](#), and [control LED indicator](#).

8.2.1 Reboot

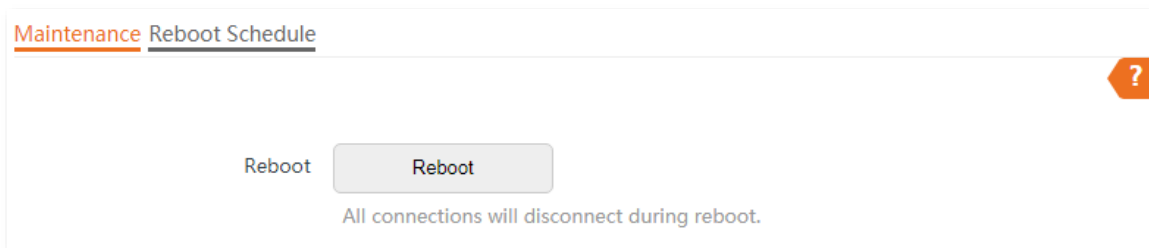


Rebooting the AP disconnects all connections. You are recommended to reboot the AP in spare time.

Manual reboot

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

Method: on the **Tools > Maintenance > Maintenance** page, click **Reboot**.



Reboot schedule

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

- [Reboot Interval](#): The AP reboots at the interval you set.
- [Reboot Schedule](#): The AP reboots regularly at the time you set.

Configuring the AP to reboot at an interval



Rebooting at intervals is based on the system time. To avoid reboot time error, ensure that the [system time](#) is correct.

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

Step 2 Enable **Reboot Schedule**.

Step 3 Set **Type** to **Reboot Interval**.

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

Step 5 Click **Save**.

Maintenance Reboot Schedule ?

Reboot Schedule

Type

Interval 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 > Reboot Schedule**.

Step 2 Enable **Reboot Schedule**.

Step 3 Set **Type** to **Reboot Schedule**.

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

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

Step 6 Click **Save**.

Maintenance Reboot Schedule ?

Reboot Schedule

Type

Reboot On Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday Every Day

Reboot At (Default:3:00)

----End

After the configurations, the AP will automatically reboot at 3 a.m. every Monday to Friday.

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

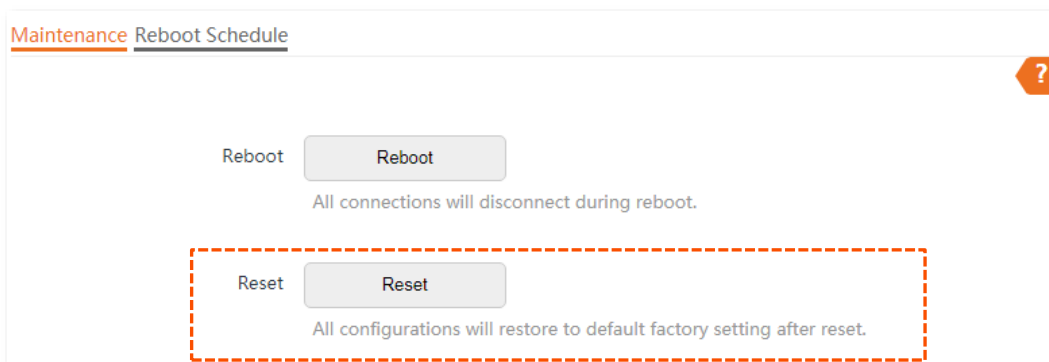
- When the factory settings are restored, your configuration is lost. Therefore, you need to reconfigure the AP to reconnect to the internet. Restore the factory settings of the AP only when necessary.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.
- After 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 for about 8 seconds.

Method 2:

Log in to the web UI of the AP, on the **Tools > Maintenance > Maintenance** page, click **Reset**.



8.2.3 Upgrade firmware

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



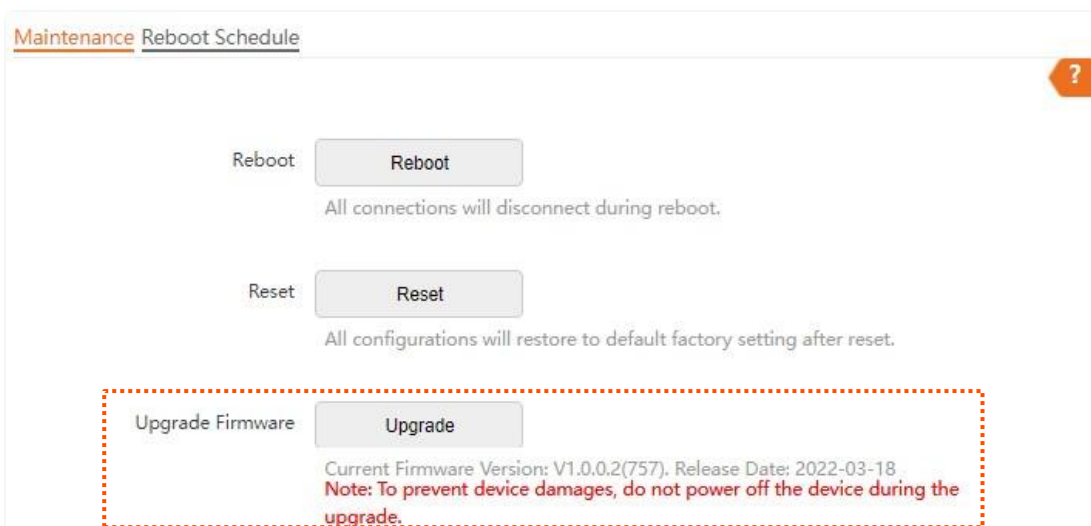
To ensure a correct upgrade and avoid damage:

- Make sure the new firmware is applicable to the AP.
- Keep a proper power supply to the AP during the upgrade.

Step 1 Download the latest firmware version for the AP from www.tendacn.com to your local computer and decompress the package. Generally, the package is in the format of **.bin**.

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

Step 3 Click **Upgrade**.



Step 4 Choose and upload the upgrade file in the popped window.

----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.



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/restore

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

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

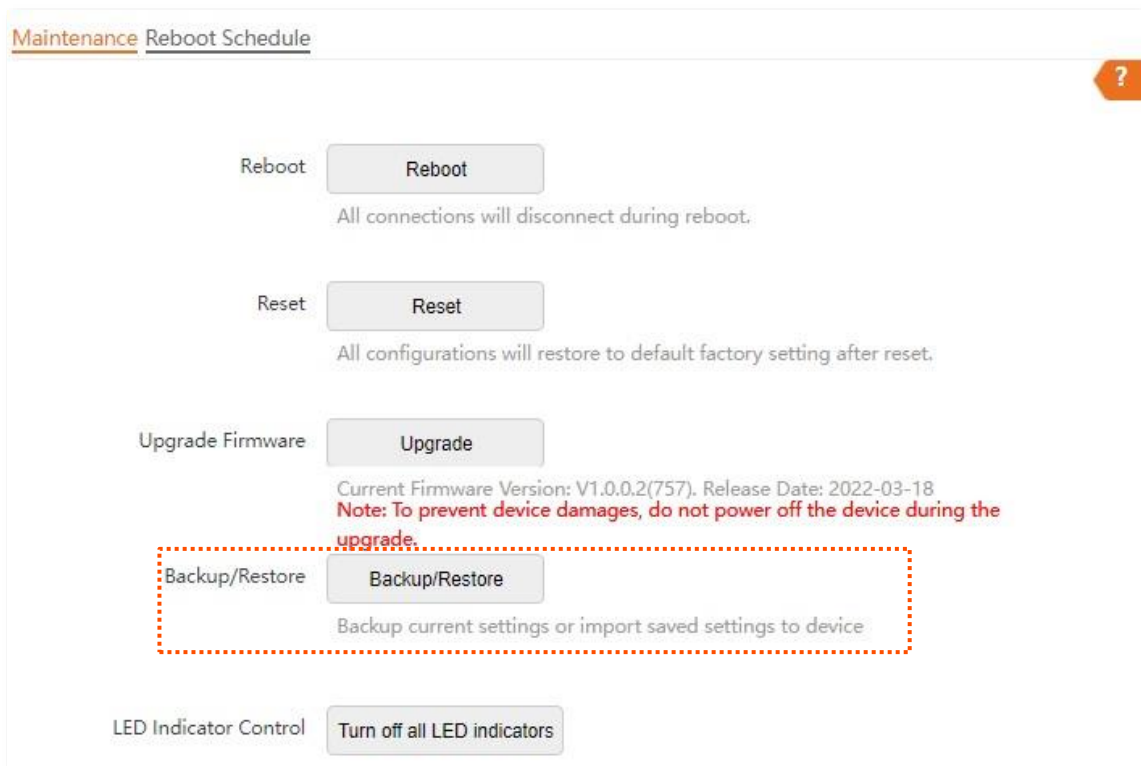


If you need to apply same or similar configurations to many APs, you can configure one of the APs, back up the configuration of the AP, and use the backup to restore the configuration on the other APs. This improves configuration efficiency.

Backup the current configuration

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

Step 2 Click **Backup/Restore**.



Step 3 Click **Backup**.



----End

A configuration file named **APCfm.cfg** will be downloaded.

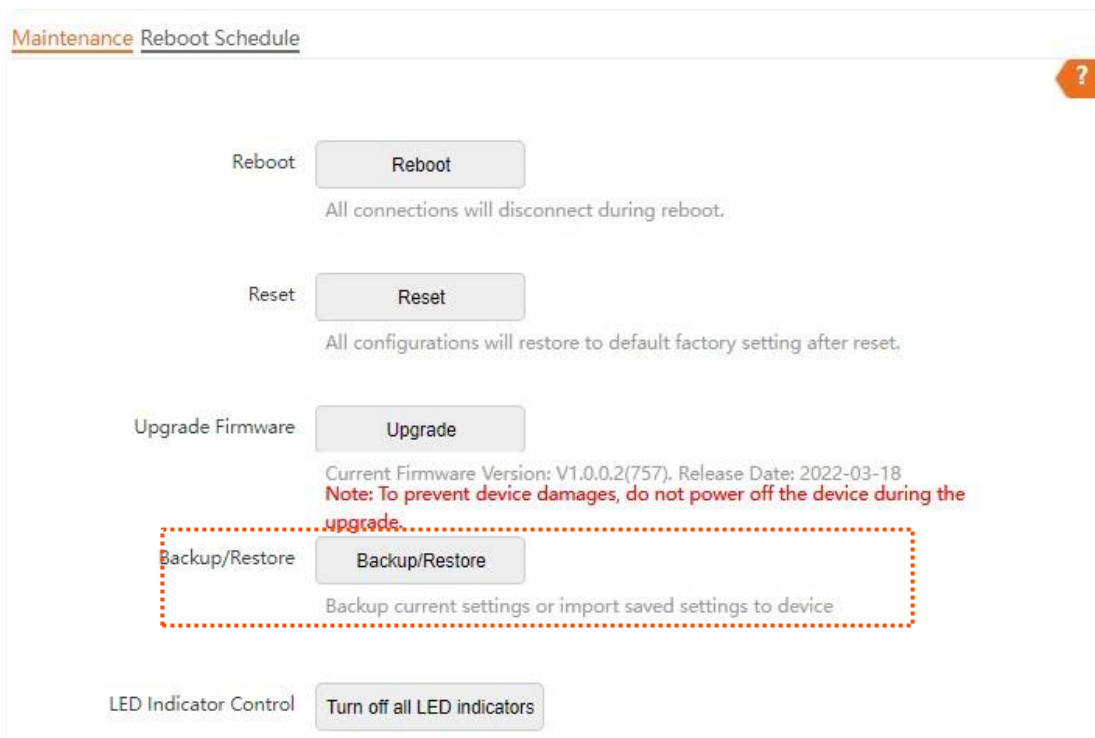


If the prompt “This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?” appears, click “Keep”.

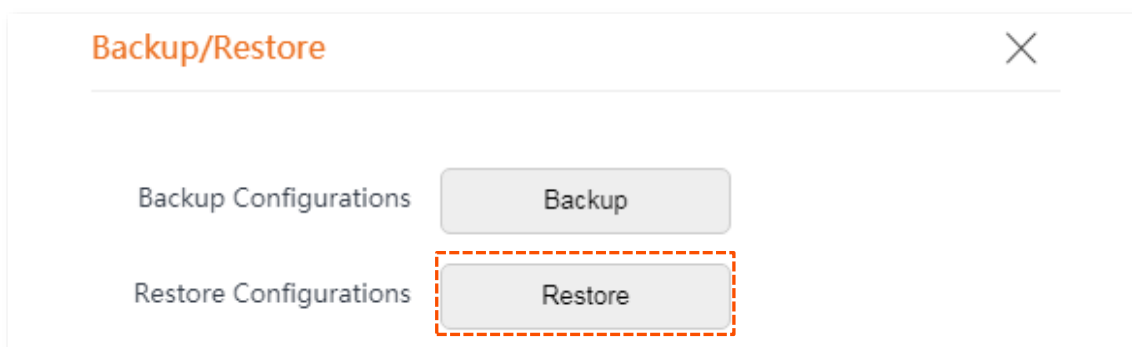
Restore a configuration

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

Step 2 Click **Backup/Restore**.



Step 3 Click **Restore**.



Step 4 Choose the configuration file you backed up.

----End

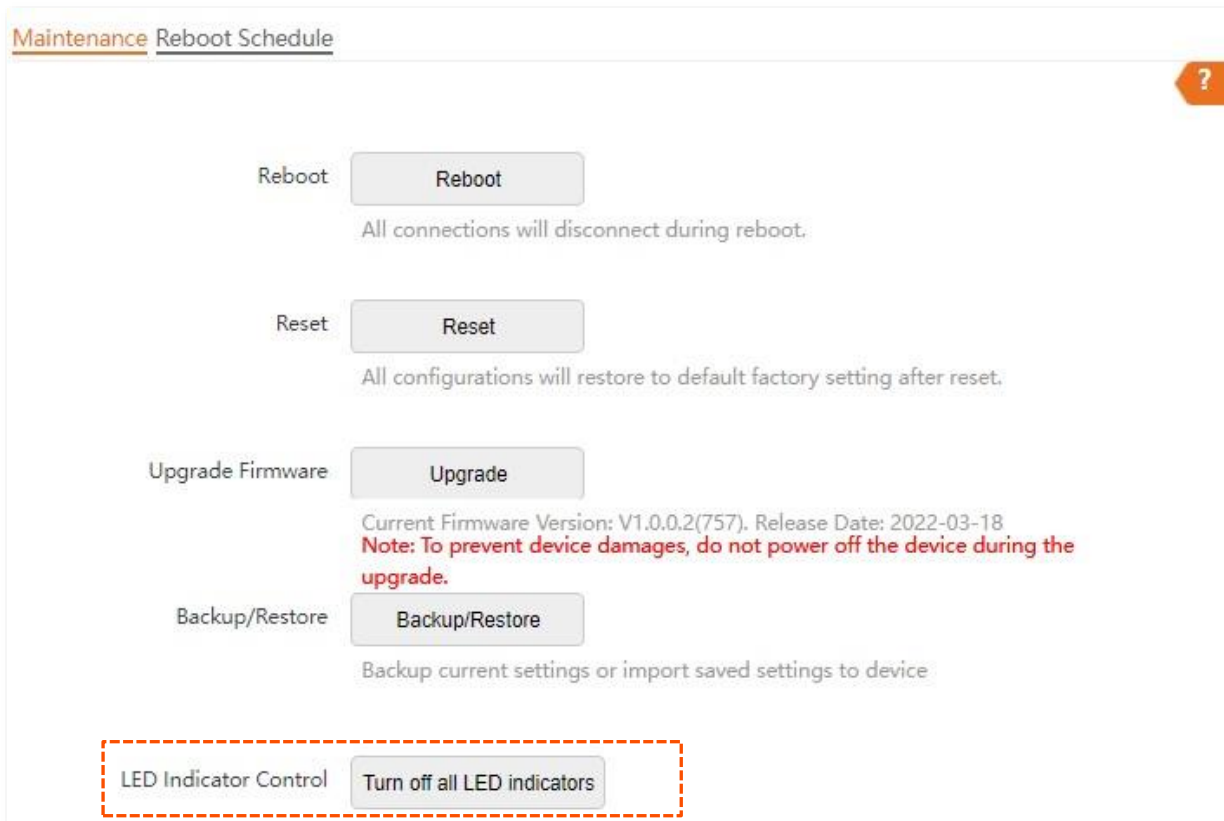
The AP restores the configurations successfully when the progress bar is done.

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

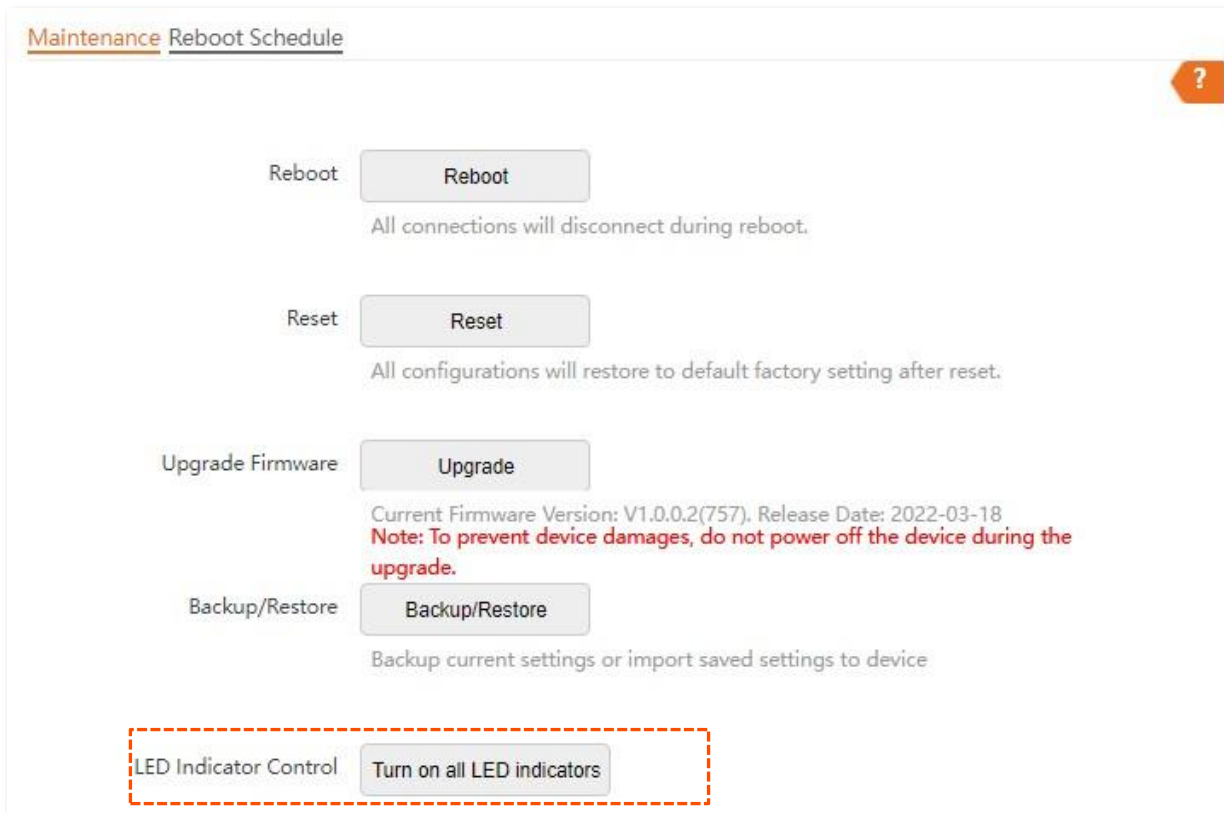
On the **Tools > Maintenance > Maintenance** page, click **Turn off all LED indicators**.



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

Turn on the LED indicator

On the **Tools > Maintenance > Maintenance** page, click **Turn on all LED indicators**.



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

8.3 Account

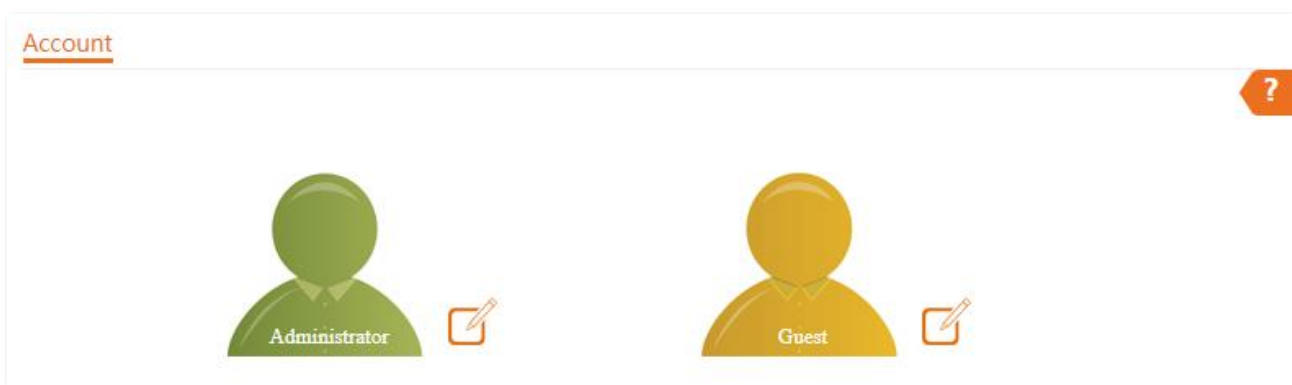
8.3.1 Overview

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**.


AP supports two account types: **Administrator** and **Guest**.

- **Administrator:** This account type has permission to view and modify the settings. The default username and password for this account are **admin/admin** (both are case-sensitive).
- **Guest:** This account type can only view other than modifying the settings. The default username and password for this account are **user/user** (both are case-sensitive). This account type is disabled by default.



8.3.2 Modifying the password and user name of login account

Step 1 Click **Tools > Account**.

Step 2 Click  beside the account to be modified.

Step 3 If the account to be modified is a Guest, enable the **Guest Account** first. Otherwise, go to the next step.

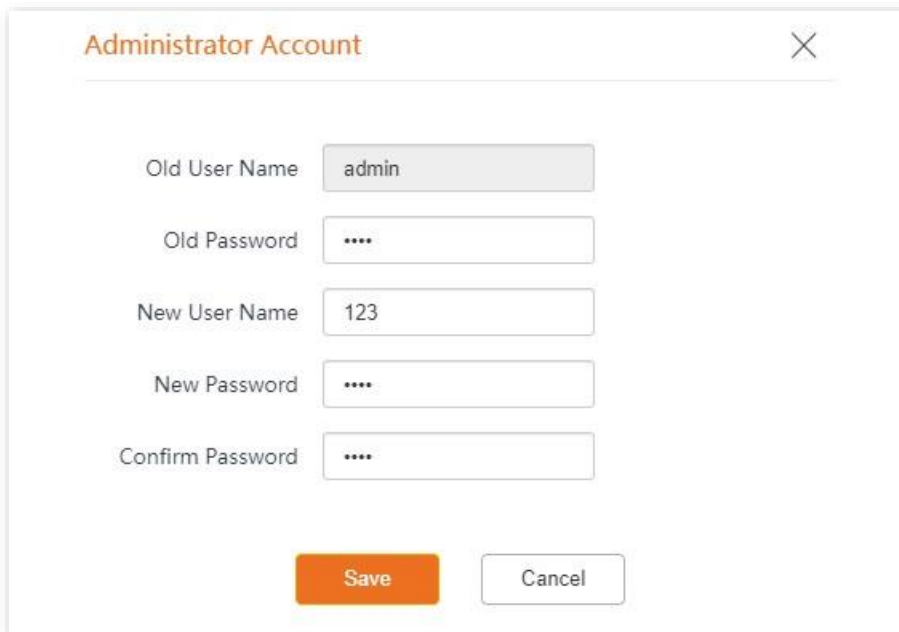
Step 4 Enter the current password in **Old Password**.

Step 5 Enter the new account name, for example, **123**, in **New User Name**.

Step 6 Enter the new password in **New Password**.

Step 7 Enter again the new password in **Confirm Password**.

Step 8 Click **Save**.



The image shows a dialog box titled "Administrator Account" with a close button (X) in the top right corner. The dialog contains five input fields and two buttons at the bottom. The fields are labeled as follows:

- Old User Name: admin
- Old Password: ****
- New User Name: 123
- New Password: ****
- Confirm Password: ****

At the bottom of the dialog, there are two buttons: "Save" (orange) and "Cancel" (white with grey border).

----End

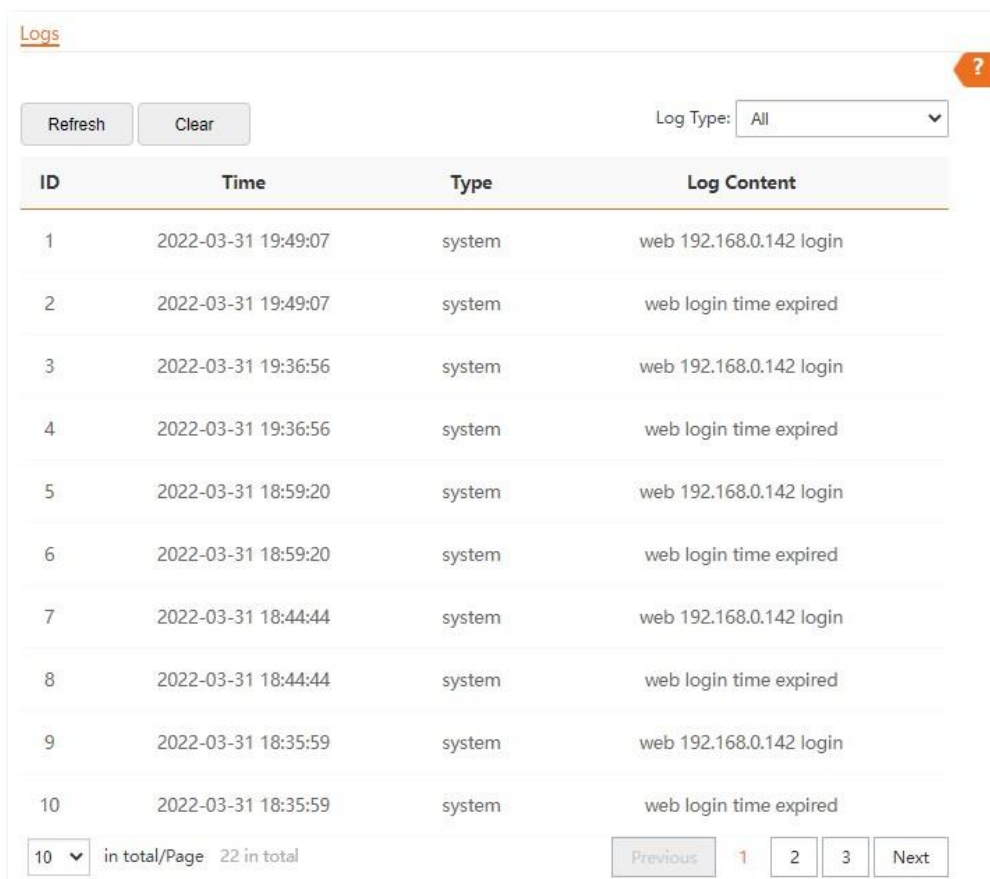
Then you will be redirected to the login page. Enter the new password and click **Login** to log in to the AP.

8.4 System Log

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

The **Logs** page allows you to view system logs.

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



ID	Time	Type	Log Content
1	2022-03-31 19:49:07	system	web 192.168.0.142 login
2	2022-03-31 19:49:07	system	web login time expired
3	2022-03-31 19:36:56	system	web 192.168.0.142 login
4	2022-03-31 19:36:56	system	web login time expired
5	2022-03-31 18:59:20	system	web 192.168.0.142 login
6	2022-03-31 18:59:20	system	web login time expired
7	2022-03-31 18:44:44	system	web 192.168.0.142 login
8	2022-03-31 18:44:44	system	web login time expired
9	2022-03-31 18:35:59	system	web 192.168.0.142 login
10	2022-03-31 18:35:59	system	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**.

By default, AP saves the latest 150 logs. The earlier logs will be automatically deleted if more than 150 logs are generated. 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.

8.5 Diagnostic tool

With the diagnostic tool, you can detect the connection status and connection quality of a network.

Assume that you need to check the connection quality between the AP and its upstream router (IP address: **192.168.1.1**).

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

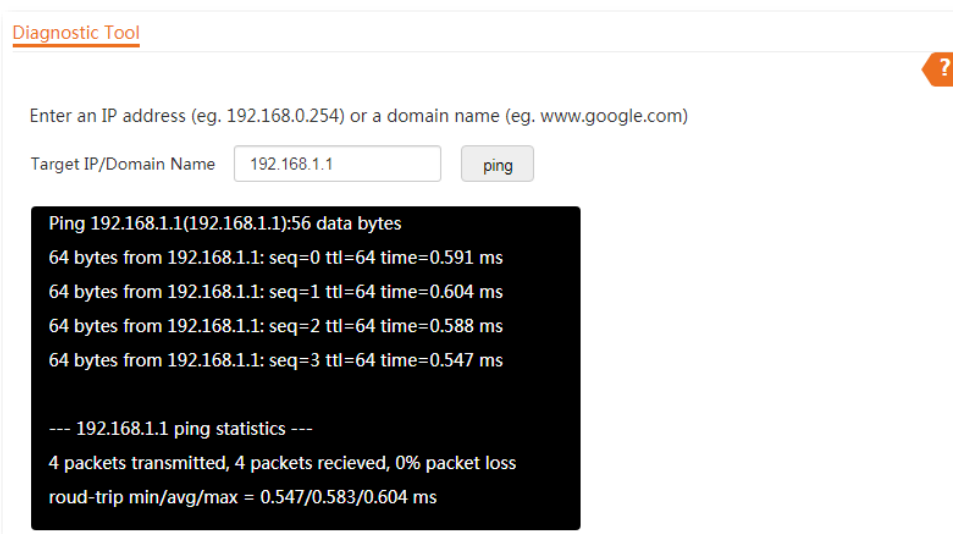
Enter an IP address (eg. 192.168.0.254) or a domain name (eg. www.google.com)

Target IP/Domain Name

[Black square]

----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

```
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
```

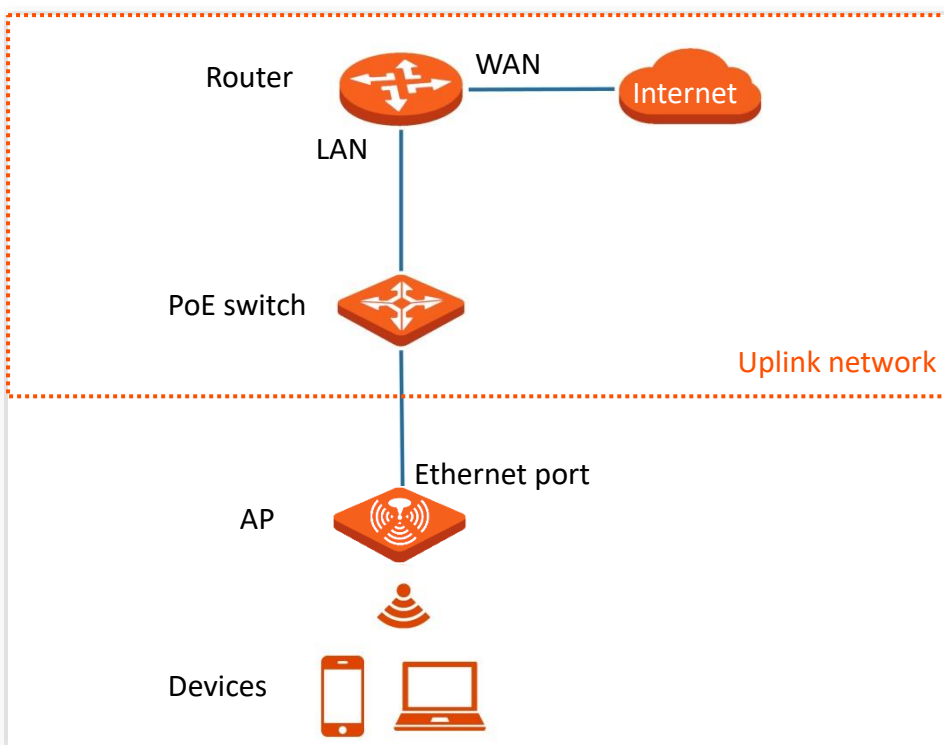

8.6 Uplink check

8.6.1 Overview

In AP mode, the AP connects to its upstream network using the Ethernet port (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 clients cannot find the SSIDs of the AP. The client can reconnect to the AP only after the connection between the AP and the upstream networks is recovered.

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

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



8.6.2 Configure 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. If there is only one host IP address, enter this IP address in both **Host1 to Ping** and **Host2 to Ping**.

Step 4 Set **Ping Interval** to the interval at which the AP detects its uplink. The default value is **10** minutes.

Step 5 Click **Save**.

The screenshot shows the 'Uplink Detection' configuration window. At the top left, the title 'Uplink Detection' is underlined. To the right is a help icon (a question mark in an orange circle). Below the title, there is a toggle switch for 'Uplink Detection' which is currently turned on. Underneath, there are three input fields: 'Host1 to Ping', 'Host2 to Ping', and 'Ping Interval'. The 'Ping Interval' field contains the number '10' and has a tooltip that says 'min(Range: 10 to 100. Default: 10)'. At the bottom of the window, there are two buttons: 'Save' (in orange) and 'Cancel' (in white with a grey border).

----End


Parameter description

Parameter	Description
Uplink Detection	It specifies whether to enable the Uplink Detection function of the AP.
Host1 to Ping	Enter the IP address of the host to be pinged. This parameter can be set if Uplink Detection is enabled.
Host2 to Ping	
Ping Interval	Set the interval at which this device detects the uplink. This parameter can be set if Uplink Detection is enabled.

Appendix

A.1 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
Quick Setup	Working Mode	AP
LAN Setup	IP Address Type	Static IP  TIP If there is a DHCP server in the LAN, the AP's LAN IP address type will be changed to DHCP automatically. In this case, you need to check the new IP address of the AP on the client list of the DHCP server.
		192.168.0.254
		255.255.255.0
SSID	SSID	2.4 GHz The AP allows 8 SSIDs. SSID is Tenda_XXXXXX. XXXXXX indicates the last 6 digits of the AP's LAN MAC address with a range of XXXXXX~XXXXXX+7. By default, the primary SSID is enabled, and the other SSIDs are disabled.
		5 GHz The AP allows 8 SSIDs. 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+15. By default, the primary SSID is enabled, and the other SSIDs are disabled.
RF Settings	Wireless Network	Enable

A.2 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
Short GI	Short Guard Interval
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

Acronym or Abbreviation	Full Spelling
WAN	Wide Area Network
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