In-wall Wireless Access Point

User Guide

Copyright Statement

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!

This user guide walks you through all functions on the in-wall wireless access point (AP) products. All the screenshots herein, unless otherwise specified, are taken from W12.

> TIP
>
> Web UI of different models may differ. The Web UI actually displayed shall prevail.

Conventions

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

Item	Presentation	Example
Cascading menus	>	System > Live Users
Button	Bold	Click the **OK** button.
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX:XX:XX:XX:XX:XX*

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 the device.
TIP	This format is used to highlight a procedure that will save time or resources.

For More Documents

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

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

Product document overview

Document	Overview
Datasheet	Walks you through basic parameters such as product overview, product features, and specifications of APs.
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

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

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

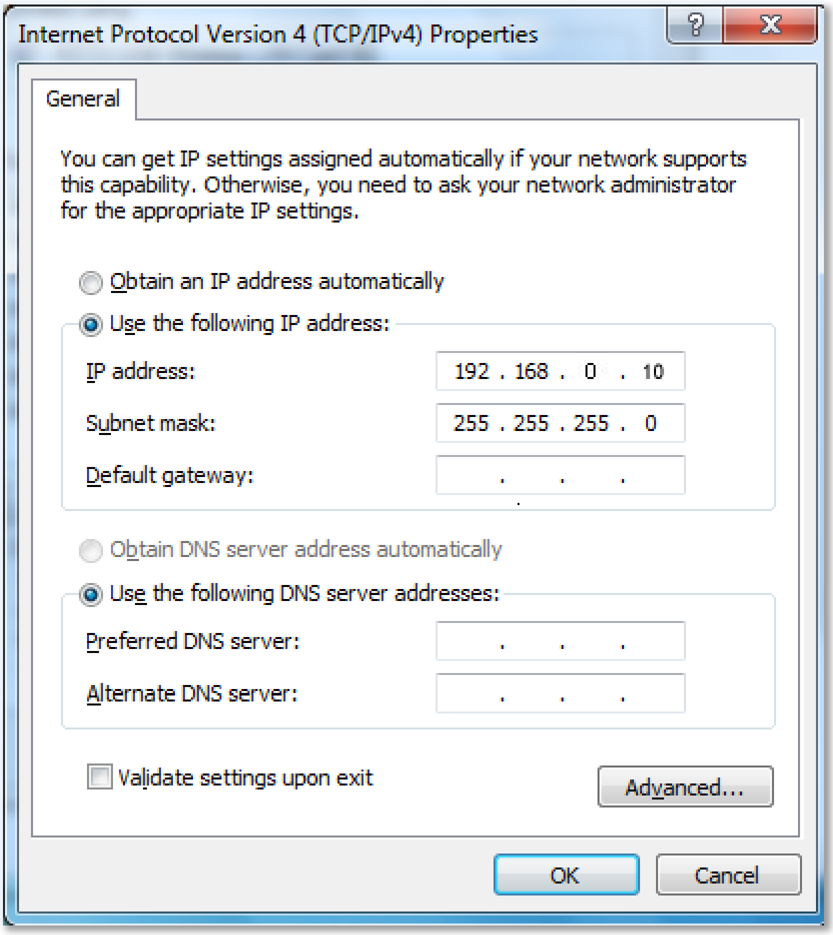
Contents

1 Log in to the Web UI

1.1 Login

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

Step 2 Configure the IP address of the computer to one in a same network segment with the AP. For example, if IP address of the AP is **192.168.0.254**, then the IP address of the computer can be configured to **192.168.0.*X*** (*X* ranges from 2 to 253 and is not occupied by other devices) and subnet mask is **255.255.255.0**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

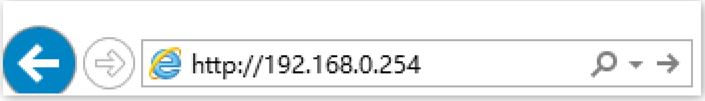
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

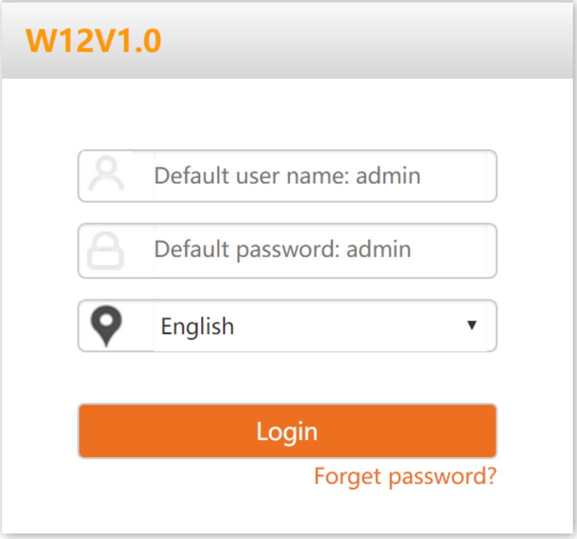
□ Validate settings upon exit

Step 3 Start a browser on the computer and visit the IP address of AP (**192.168.0.254** by default).



http://192.168.0.254

Step 4 Enter the login user name and password, and click **Login**.



W12V1.0

Default user name: admin

Default password: admin

English

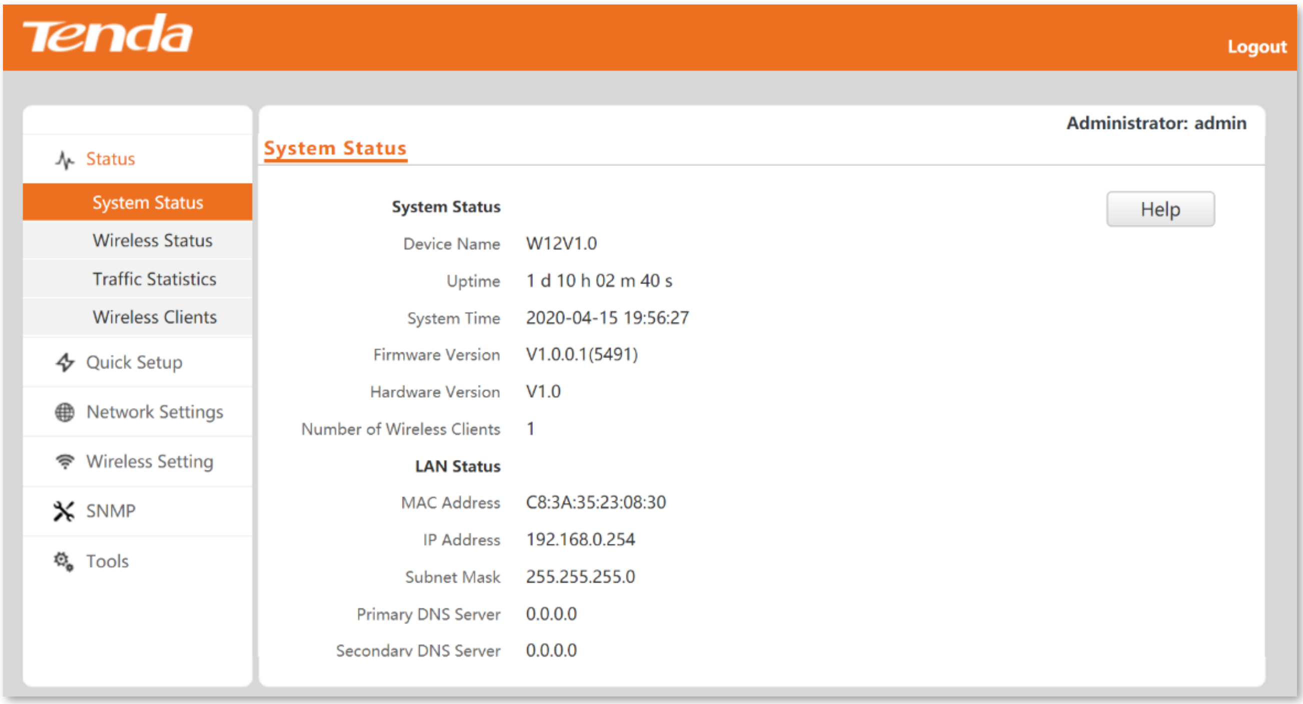
---End

TIP

If the above page does not appear, try the following solutions:

- If an Tenda AP (including Tenda router with AC functionality) has already been deployed in the network, AP may have been managed by the AC and its IP address has changed. Please log in to the Web UI of the AC and check the new IP address of the AP, and log in again using the new IP address.
- If more than one AP are deployed in the network, IP address conflicts may occur, causing web UI login errors. Verify that the IP address of the AP is not occupied before being integrated into the network.
- Reset the AP and log in using the default IP address. How to reset: When the **SYS** LED indicator blinks green, remove the front cover, hold down the reset button for about 8 seconds, and release when the green LED indicator turns solid on. When the **SYS** LED indicator blinks again, the AP is reset.

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



System Status

System Status	
Device Name	W12V1.0
Uptime	1 d 10 h 02 m 40 s
System Time	2020-04-15 19:56:27
Firmware Version	V1.0.0.1(5491)
Hardware Version	V1.0
Number of Wireless Clients	1
LAN Status	
MAC Address	C8:3A:35:23:08:30
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Primary DNS Server	0.0.0.0
Secondarv DNS Server	0.0.0.0

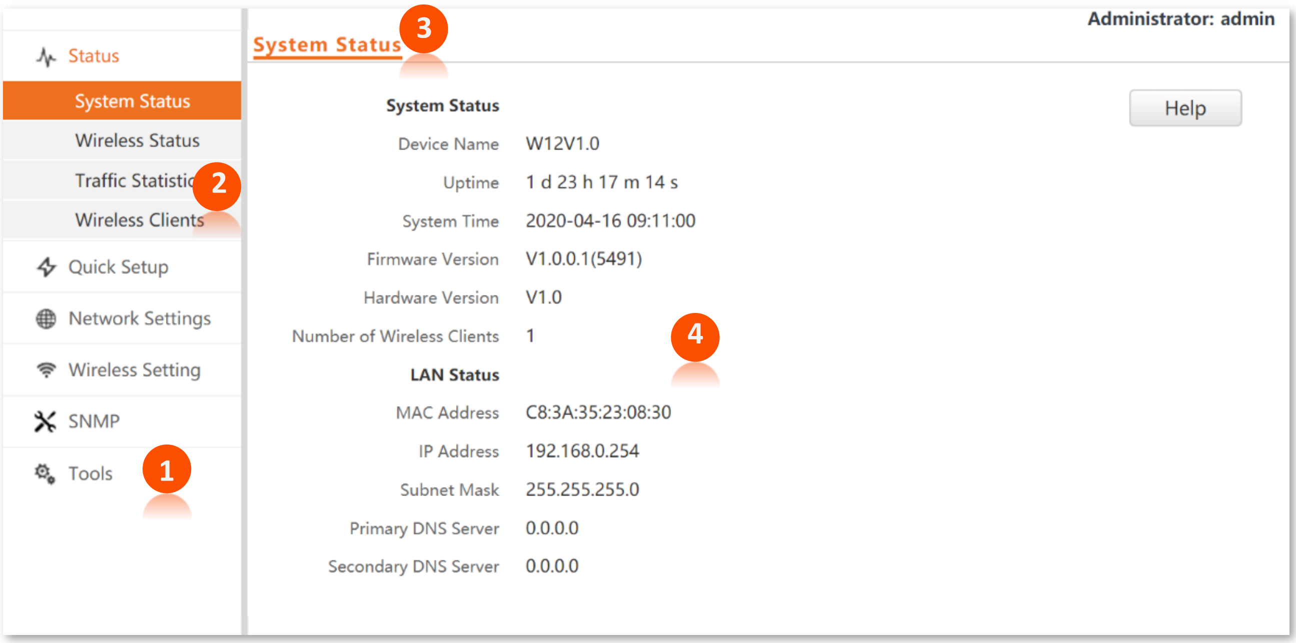
1.2 Logout

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 is composed of four parts: first-level navigation bar, second-level navigation bar, tab, and the configuration area, as shown below.



System Status

Device Name W12V1.0

Uptime 1 d 23 h 17 m 14 s

System Time 2020-04-16 09:11:00

Firmware Version V1.0.0.1(5491)

Hardware Version V1.0

Number of Wireless Clients 1

LAN Status

MAC Address C8:3A:35:23:08:30

IP Address 192.168.0.254

Subnet Mask 255.255.255.0

Primary DNS Server 0.0.0.0

Secondary DNS Server 0.0.0.0

TIP

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

No.	Name	Description
1	First-level navigation bar	Function menu that organizes AP by navigation tree and tab. You can choose function menu as needed and the result appears on the configuration area.
2	Second-level navigation bar	
3	Tab	
4	Configuration area	Area where you perform or check configurations.

2.2 Common Buttons

Buttons commonly used on the web UI are illustrated as below.

Common button	Description
Refresh	Refresh the current page.
Save	Save configurations on the current page and make the configurations take effect.
Restore	Cancel the unsaved configurations on the current page and restore to previous configurations.
Help	Check the help information of the current page.

3 Quick Setup

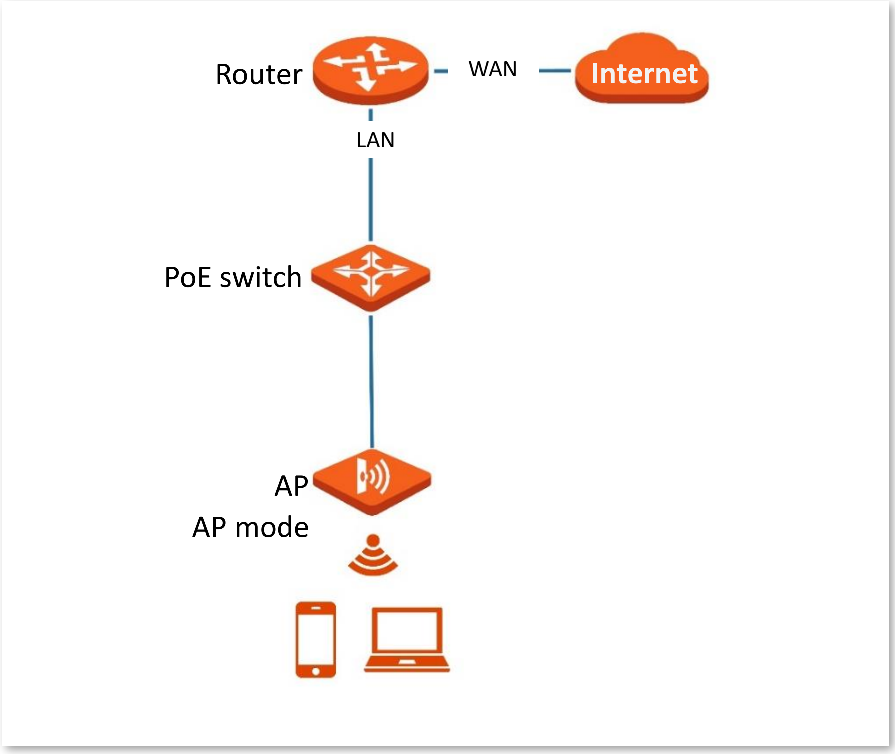
In the **Quick Setup** module, you can set up the AP in a quick way to enable internet access for your wireless devices such as smart phones and tablets.

The AP supports working modes of AP and Client+AP.

3.1 AP Working Mode

3.1.1 Overview

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



3.1.2 Quick Setup

TIP

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

Step 1 Click **Quick Setup**.

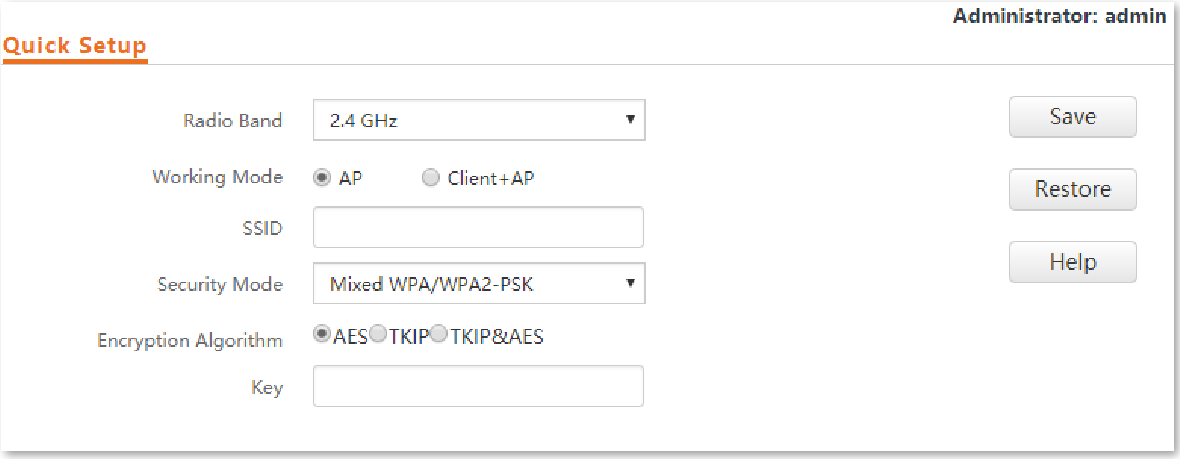
Step 2 Choose the **Radio Band** you wish to configure, for example, **2.4GHz**.

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

Step 4 Set an **SSID** (Primary SSID).

Step 5 Select a **Security Mode** and configure the incurred parameters.

Step 6 Click **Save**.



Administrator: admin

Quick Setup

Radio Band: 2.4 GHz

Working Mode: ● AP ○ Client+AP

SSID:

Security Mode: Mixed WPA/WPA2-PSK

Encryption Algorithm: ●AES ○TKIP ○TKIP&AES

Key:

Step 7 If you need to configure the other radio band, repeat **steps** 2 to 6.

---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

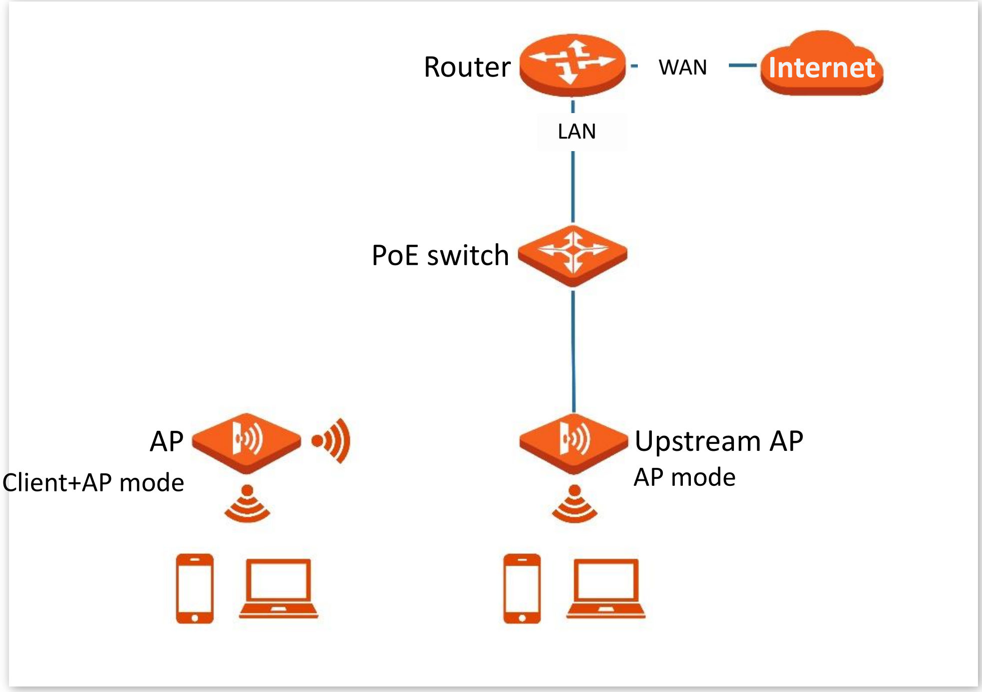
Parameter	Description
Radio Band	Select the radio band you wish to configure.
Working Mode	Choose the AP mode to transform the wireless network to wireless network.
SSID	Click to modify the WiFi name of the primary network under the selected radio band.

Parameter	Description
Security Mode	Select the security modes for target wireless networks. Supported security modes are as follows: • **None**: No password for the wireless network and any wireless clients can access the network. To ensure network security, this mode is not recommended. • **WEP**: It uses a static key to encrypt all exchanged data, and ensures that a wireless LAN has the same level of security as a wired LAN. Data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum wireless network throughput of only 54 Mbps. Therefore, this security mode is not recommended. • **WPA-PSK**, **WPA2-PSK**, **Mixed WPA/WPA2-PSK**: WPA pre-shared key authentication. The key you set is only used for identity verification while data encryption key is automatically generated by AP based on encryption rule TKIP or AES, solving the vulnerability of WEP static key and therefore, is proper for personal or home networks. Mixed WPA/WPA2-PSK indicates that AP is compatible with both WPA-PSK and WPA2-PSK security modes. • **WPA**, **WPA2**: 802.1x is used to authenticate users and generate root key for encrypting data instead of using pre-shared key you set manually. Data encryption key is automatically generated by AP based on encryption rule TKIP or AES, which is proper for wireless networks with high security requirements such as enterprises.

3.2 Client+AP Mode

3.2.1 Overview

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



3.2.2 Quick Setup

TIP

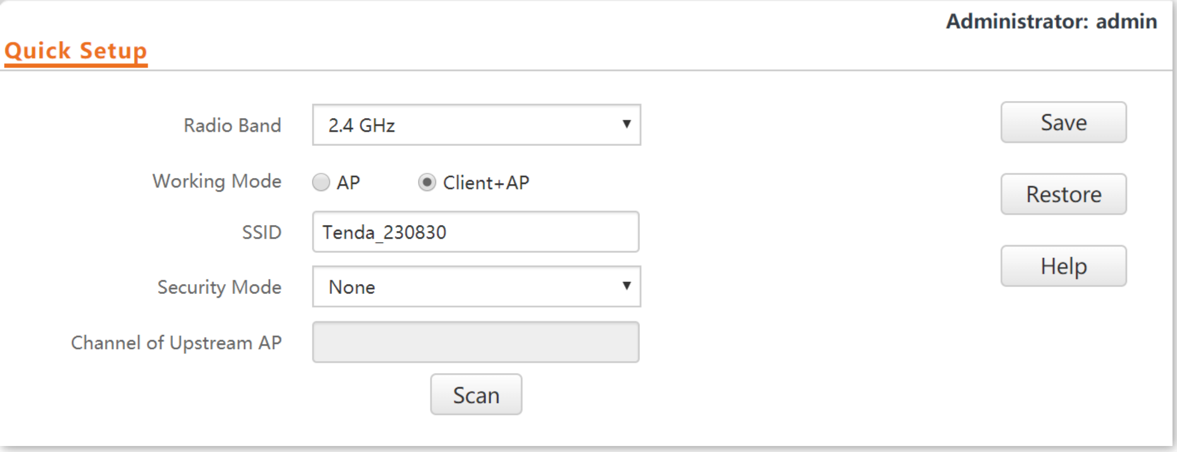
Before configuration, ensure that the upstream AP has been connected to the internet.

Step 1 Choose **Quick Setup**.

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

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

Step 4 Click **Scan** .



Radio Band: 2.4 GHz

Working Mode: ○ AP ● Client+AP

SSID: Tenda_230830

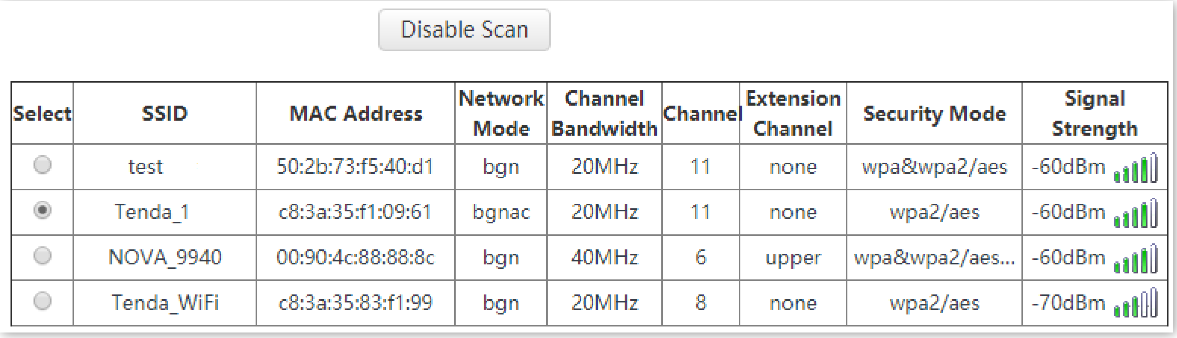
Security Mode: None

Channel of Upstream AP:

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

TIP

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

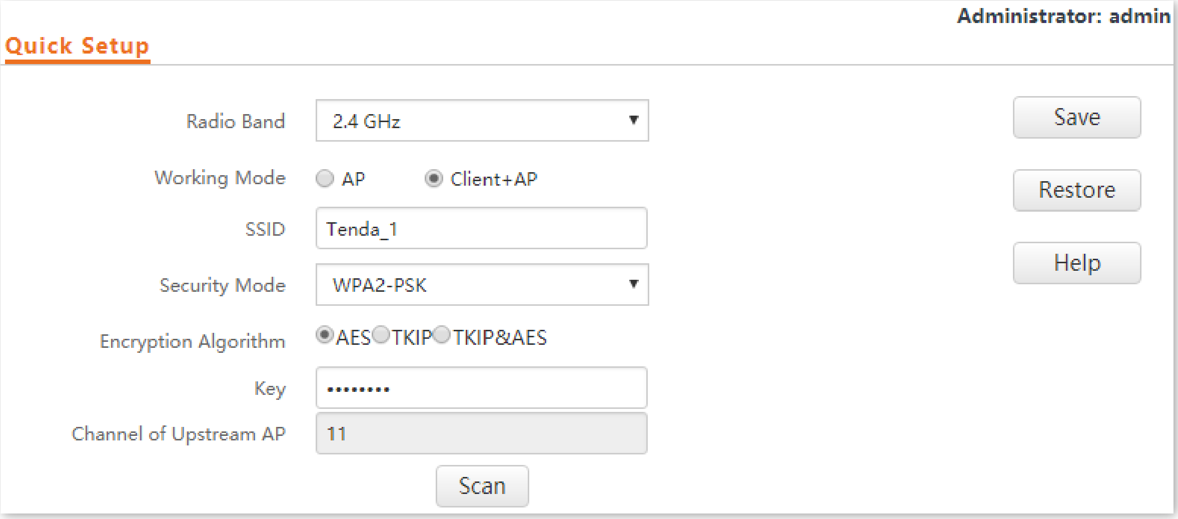


Select	SSID	MAC Address	Network Mode	Channel Bandwidth	Channel	Extension Channel	Security Mode	Signal Strength
○	test	50:2b:73:f5:40:d1	bgn	20MHz	11	none	wpa&wpa2/aes	-60dBm
●	Tenda_1	c8:3a:35:f1:09:61	bgnac	20MHz	11	none	wpa2/aes	-60dBm
○	NOVA_9940	00:90:4c:88:88:8c	bgn	40MHz	6	upper	wpa&wpa2/aes...	-60dBm
○	Tenda_WiFi	c8:3a:35:83:f1:99	bgn	20MHz	8	none	wpa2/aes	-70dBm

Step 6 Click **Disable Scan**.

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

Step 8 Click **Save**.



Administrator: admin

Quick Setup

Radio Band: 2.4 GHz

Working Mode: ○ AP ● Client+AP

SSID: Tenda_1

Security Mode: WPA2-PSK

Encryption Algorithm: ●AES○TKIP○TKIP&AES

Key: ••••••••

Channel of Upstream AP: 11

---End

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

TIP

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

Parameter description

Parameter	Description
Radio Band	It specifies the radio band of the WiFi network to be configured.
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.

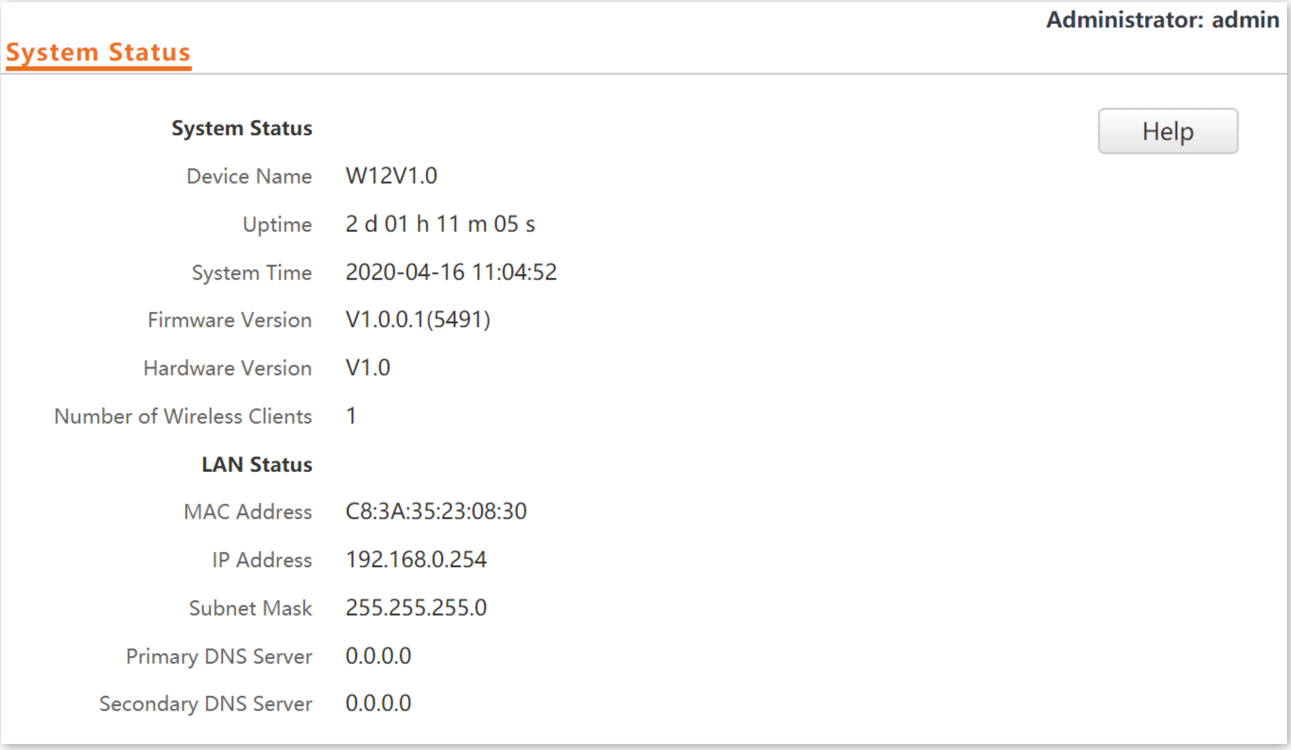
Parameter	Description
Security Mode	It specifies the security mode of which the upstream WiFi network adopted. After you select the upstream WiFi network from the scanned wireless network list, this parameter will be populated automatically. The AP can support WiFi network encrypted with **None** or **WEP** (Open or Shared), **WPA-PSK**, **WPA2-PSK** and **Mixed WPA/WPA2-PSK**. • **None**: No password for the wireless network and any wireless clients can access the network. To ensure network security, this mode is not recommended. • **WEP**: It uses a static key to encrypt all exchanged data, and ensures that a wireless LAN has the same level of security as a wired LAN. Data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum wireless network throughput of only 54 Mbps. Therefore, this security mode is not recommended. • **WPA-PSK**, **WPA2-PSK**, **Mixed WPA/WPA2-PSK**: WPA pre-shared key authentication. The key you set is only used for identity verification while data encryption key is automatically generated by AP based on encryption rule TKIP or AES, solving the vulnerability of WEP static key and therefore, is proper for personal or home networks. Mixed WPA/WPA2-PSK indicates that AP is compatible with both WPA-PSK and WPA2-PSK security modes. NOTE • 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 or Mixed WPA/WPA2-PSK security mode, **Encryption Algorithm** will be populated automatically and you only need to enter the **Key**.

4 Status

4.1 System Status

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

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



System Status

Device Name	W12V1.0
Uptime	2 d 01 h 11 m 05 s
System Time	2020-04-16 11:04:52
Firmware Version	V1.0.0.1(5491)
Hardware Version	V1.0
Number of Wireless Clients	1

LAN Status

MAC Address	C8:3A:35:23:08:30
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

Parameter description

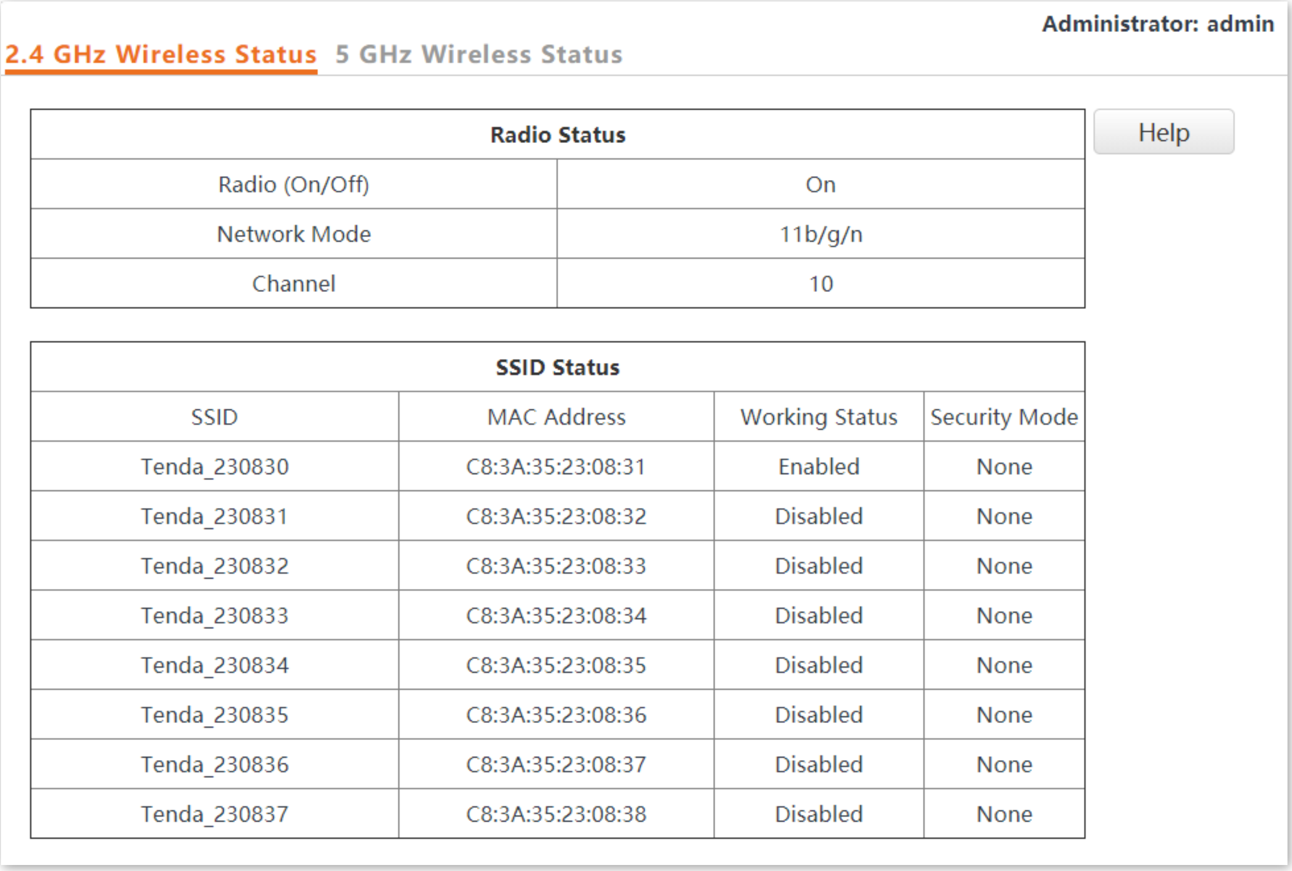
Parameter	Description
Device Name	It specifies the name of the AP. A unique AP name helps quickly identify the AP. You can change the AP name on the **Network Settings** > **LAN Setup** page.
Uptime	It specifies the time that has elapsed since the AP was started last time.
System Time	It specifies the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

Parameter	Description
Hardware Version	It specifies the hardware version of the AP.
Number of Wireless Clients	It specifies the number of wireless clients currently connected to the AP.
MAC Address	It specifies the physical address of the LAN port of the AP. If you connect the AP to other devices using Ethernet cables, the AP uses this MAC address to communicate with those devices.
IP Address	It specifies the IP address of the AP and it is also the management IP address of the AP. The web UI of the AP is accessible by visiting this IP address. You can change the IP address on the **Network Settings** > **LAN Setup** page.
Subnet Mask	It specifies the subnet mask of the IP address of the AP.
Primary DNS Server	It specifies the primary DNS server of the AP.
Secondary DNS Server	It specifies the secondary DNS server of the AP.

4.2 Wireless Status

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

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



Radio Status	
Radio (On/Off)	On
Network Mode	11b/g/n
Channel	10

SSID Status

SSID	MAC Address	Working Status	Security Mode
Tenda_230830	C8:3A:35:23:08:31	Enabled	None
Tenda_230831	C8:3A:35:23:08:32	Disabled	None
Tenda_230832	C8:3A:35:23:08:33	Disabled	None
Tenda_230833	C8:3A:35:23:08:34	Disabled	None
Tenda_230834	C8:3A:35:23:08:35	Disabled	None
Tenda_230835	C8:3A:35:23:08:36	Disabled	None
Tenda_230836	C8:3A:35:23:08:37	Disabled	None
Tenda_230837	C8:3A:35:23:08:38	Disabled	None

Parameter description

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

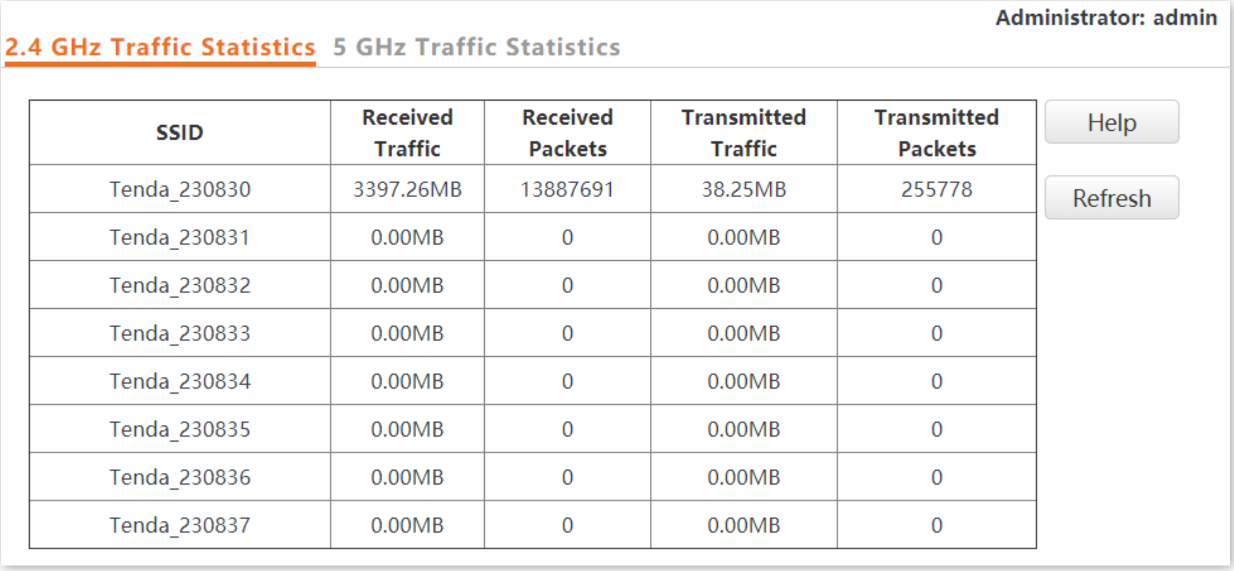
Parameter		Description
	Security Mode	It specifies the security modes of the wireless networks corresponding to the SSIDs of the AP.

4.3 Traffic Statistics

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

This page displays the statistics about historical packets of the wireless networks of the AP.

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

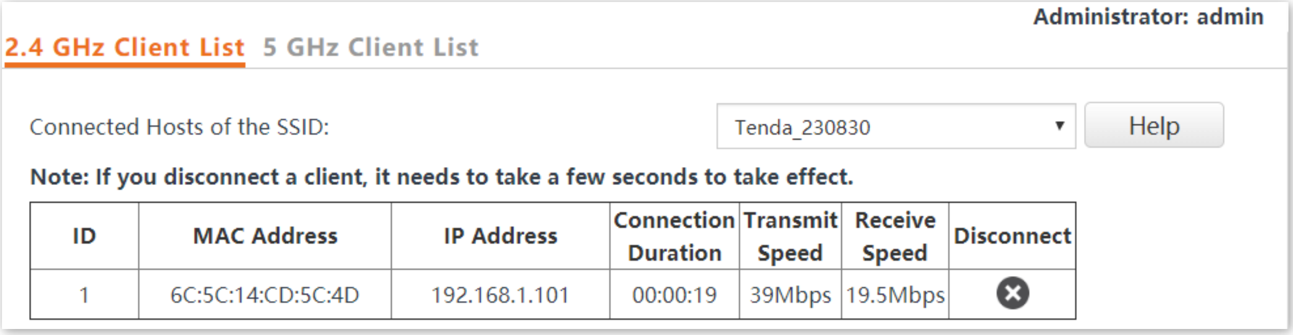


SSID	Received Traffic	Received Packets	Transmitted Traffic	Transmitted Packets
Tenda_230830	3397.26MB	13887691	38.25MB	255778
Tenda_230831	0.00MB	0	0.00MB	0
Tenda_230832	0.00MB	0	0.00MB	0
Tenda_230833	0.00MB	0	0.00MB	0
Tenda_230834	0.00MB	0	0.00MB	0
Tenda_230835	0.00MB	0	0.00MB	0
Tenda_230836	0.00MB	0	0.00MB	0
Tenda_230837	0.00MB	0	0.00MB	0

4.4 Wireless Clients

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

This page displays information about the wireless clients connected to the wireless networks corresponding to the SSIDs of the AP. You can also disconnect certain connected clients.



Connected Hosts of the SSID: Tenda_230830

Note: If you disconnect a client, it needs to take a few seconds to take effect.

ID	MAC Address	IP Address	Connection Duration	Transmit Speed	Receive Speed	Disconnect
1	6C:5C:14:CD:5C:4D	192.168.1.101	00:00:19	39Mbps	19.5Mbps	⊗

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

Parameter description

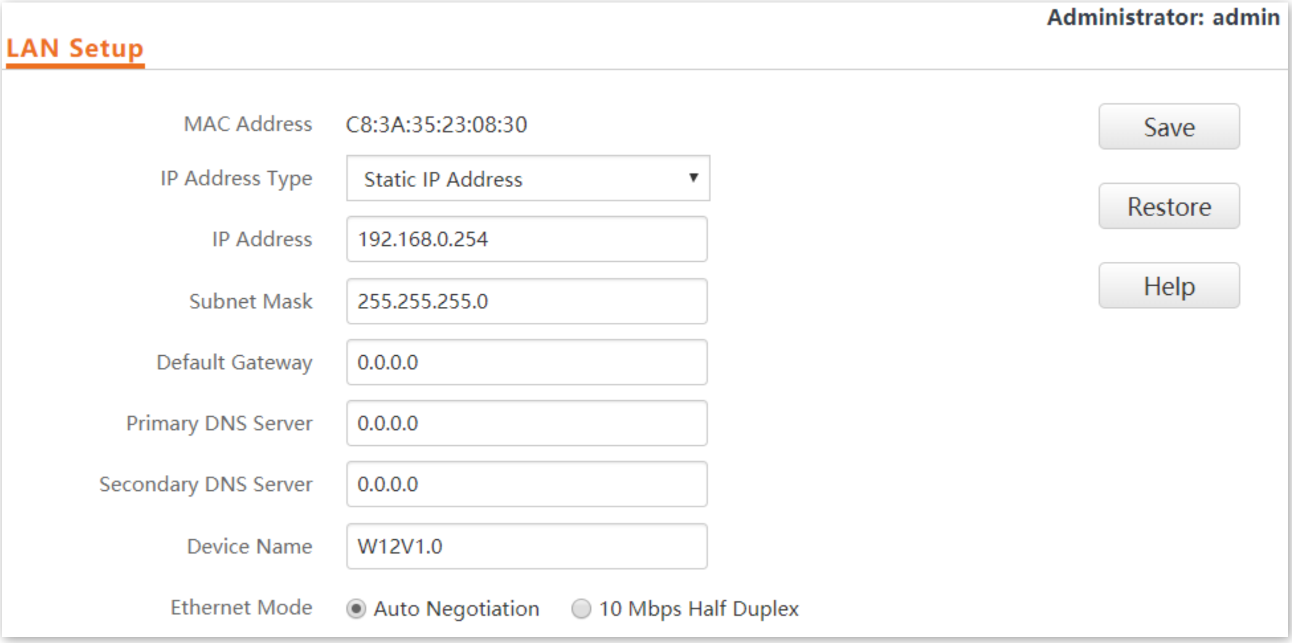
Parameter	Description
SSID	It specifies the wireless network to be checked.
MAC Address	It specifies the MAC address of the wireless client.
IP Address	It specifies the IP address of the wireless client.
Client Type	It specifies the OS type of the wireless client. TIP Only when AP is enabled **Identify Client Type** and the client visited a HTTP website, the OS type of the client can be identified.
Connection Duration	It specifies the online duration of the wireless client.
Transmit Speed	It specifies the current transmit speed of the wireless client.
Receive Speed	It specifies the current receive speed of the wireless client.
Disconnect	Clicking ⊗ disconnects the corresponding client. To view the disconnected client, choose **Wireless Setting** > **Access Control**.

5 Network Settings

5.1 LAN Setup

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

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



Administrator: admin

LAN Setup

MAC Address: C8:3A:35:23:08:30

IP Address Type: Static IP Address ▾

IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Device Name: W12V1.0

Ethernet Mode: ● Auto Negotiation ○ 10 Mbps Half Duplex

Parameter description

Parameter	Description
MAC Address	It specifies the MAC address of the LAN port of the AP.

Parameter	Description
IP Address Type	It specifies the IP address obtaining mode of the AP. The default option is **Static IP Address**. ● **Static IP Address**: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is set manually. It is proper for the scenarios where only one or several APs are required in the network. ● **DHCP**: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is obtained from a DHCP server on your LAN. It is proper for the scenarios where a large group of APs are required in the network. TIP If **Address Type** is set to **DHCP**, you can log in to the web UI of the AP only with the IP address assigned to the AP by the DHCP server. The IP address is specified on the client list of the DHCP server.
IP Address	It specifies the IP address of the AP. The web UI of the AP is accessible at this IP address. The default IP address is **192.168.0.254**.
Subnet Mask	It specifies the subnet mask of the IP address of the AP. The default subnet mask is **255.255.255.0**.
Default Gateway	It specifies the gateway IP address of the AP. Generally, set the gateway IP address to the LAN IP address of your LAN router connected to the internet, so that the AP can access the internet.
Primary DNS Server	It specifies the primary DNS server of the AP. If your LAN router connected to the internet provides the DNS proxy function, this IP address can be the LAN IP address of the router. Otherwise, enter a correct DNS server IP address.
Secondary DNS Server	It specifies the IP address of the secondary DNS server of the AP. This parameter is optional. If a DNS server IP address in addition to the IP address of the primary DNS server is available, enter the additional IP address in this field.
Device Name	It specifies the name of the AP. By default, the name is the model of the AP, such as W12V1.0. You are recommended to change the name of the AP to indicate the location of the AP (such as Bedroom), so that you can easily identify the AP when managing many APs.

Parameter	Description
Ethernet Mode	It specifies the Ethernet mode of the PoE power-supply port (the rear port of W36AP) of this AP. • **Auto Negotiation**: This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended. • **10 Mbps Half Duplex**: This mode features a long transmission distance but relatively low transmission rate (usually 10 Mbps). TIP • The 10 Mbps Half Duplex mode is recommended only if the Ethernet cable that connects the PoE power-supply port of the AP to a peer device exceeds 100 meters. In this case, the connected LAN port of the peer device must work in auto-negotiation mode. Otherwise, the PoE power-supply port of the AP may not be able to properly transmit or receive data. • Modifications to **Ethernet Mode** take effect after you reset the AP or unplug from and plug into the port again.

5.2 DHCP Server

5.2.1 Overview

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

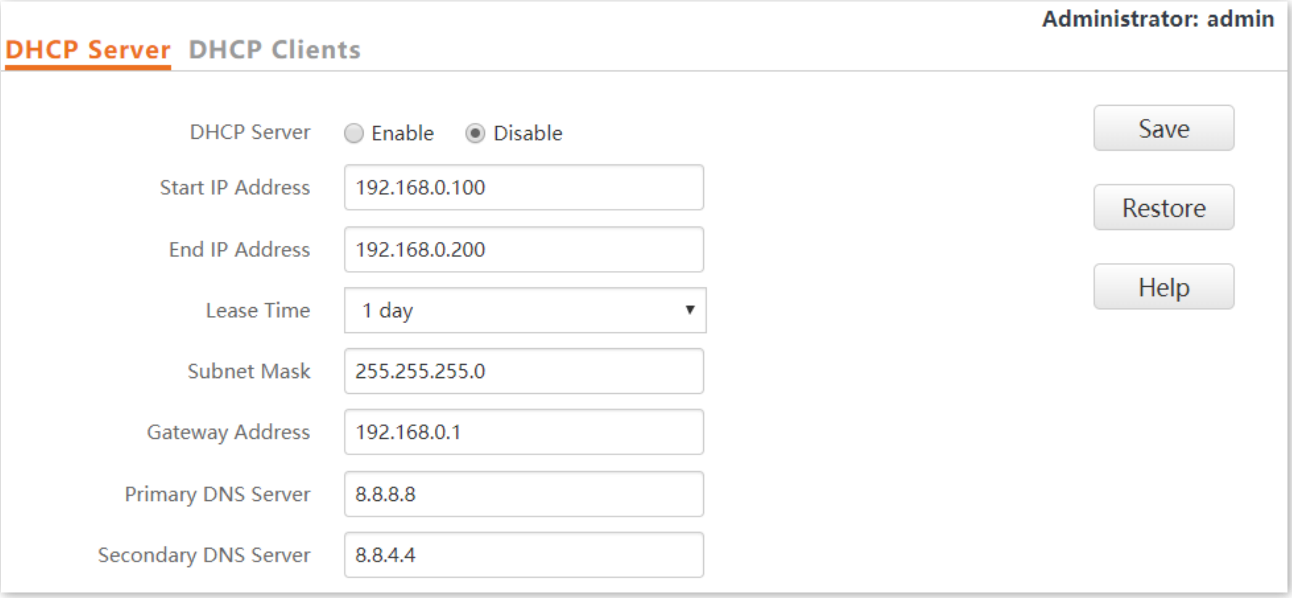
TIP

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

5.2.2 Configure the DHCP Server

To access the page, choose **Network Settings** > **DHCP Server**.

This page enables you to set parameters related to the DHCP server.



DHCP Server ○ Enable ● Disable

Start IP Address 192.168.0.100

End IP Address 192.168.0.200

Lease Time 1 day

Subnet Mask 255.255.255.0

Gateway Address 192.168.0.1

Primary DNS Server 8.8.8.8

Secondary DNS Server 8.8.4.4

NOTE

If there are other DHCP servers in the network, ensure that the DHCP address pool of the AP does not overlap with those of other DHCP servers so as to avoid address conflicts.

Parameter description

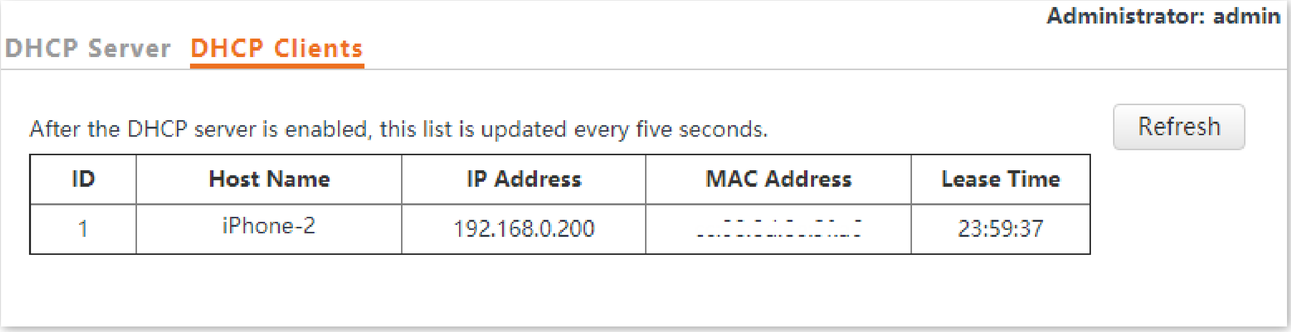
Parameter	Description
DHCP Server	It specifies whether to enable the DHCP server function of the AP. By default, it is disabled.

Parameter	Description
Start IP Address	It specifies the start IP address of the IP address pool of the DHCP server. The default value is **192.168.0.100**.
End IP Address	It specifies the end IP address of the IP address pool of the DHCP server. The default value is **192.168.0.200**.
Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a client. When half of the lease time has elapsed, the client sends a DHCP Request to the DHCP server to renew the lease time. If the request succeeds, the lease time is extended according to the request. Otherwise, the client sends the request again when 7/8 of the lease time has elapsed. If the request succeeds, the lease time is extended according to the request. Otherwise, the client must request an IP address from the DHCP server after the lease time expires. If the number of clients is greater than that of the DHCP address pools and clients change frequently, modify the value to a shorter period of time. Otherwise, it is recommended that you retain the default value **1 day**.
Subnet Mask	It specifies the subnet mask assigned by the DHCP server to clients.
Gateway Address	It specifies the default IP address of the gateway assigned by the DHCP server to clients, which is generally the IP address of the LAN port of the router. TIP When clients access servers or hosts beyond the current network segment, the data must be forwarded by the gateway.
Primary DNS Server	It specifies the primary DNS server IP address assigned by the DHCP server to clients. TIP To enable clients to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS Server	It specifies the secondary DNS server IP address assigned by the DHCP server to clients. This parameter is optional.

5.2.3 View the DHCP Client List

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

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



After the DHCP server is enabled, this list is updated every five seconds.

ID	Host Name	IP Address	MAC Address	Lease Time
1	iPhone-2	192.168.0.200	[illegible]	23:59:37

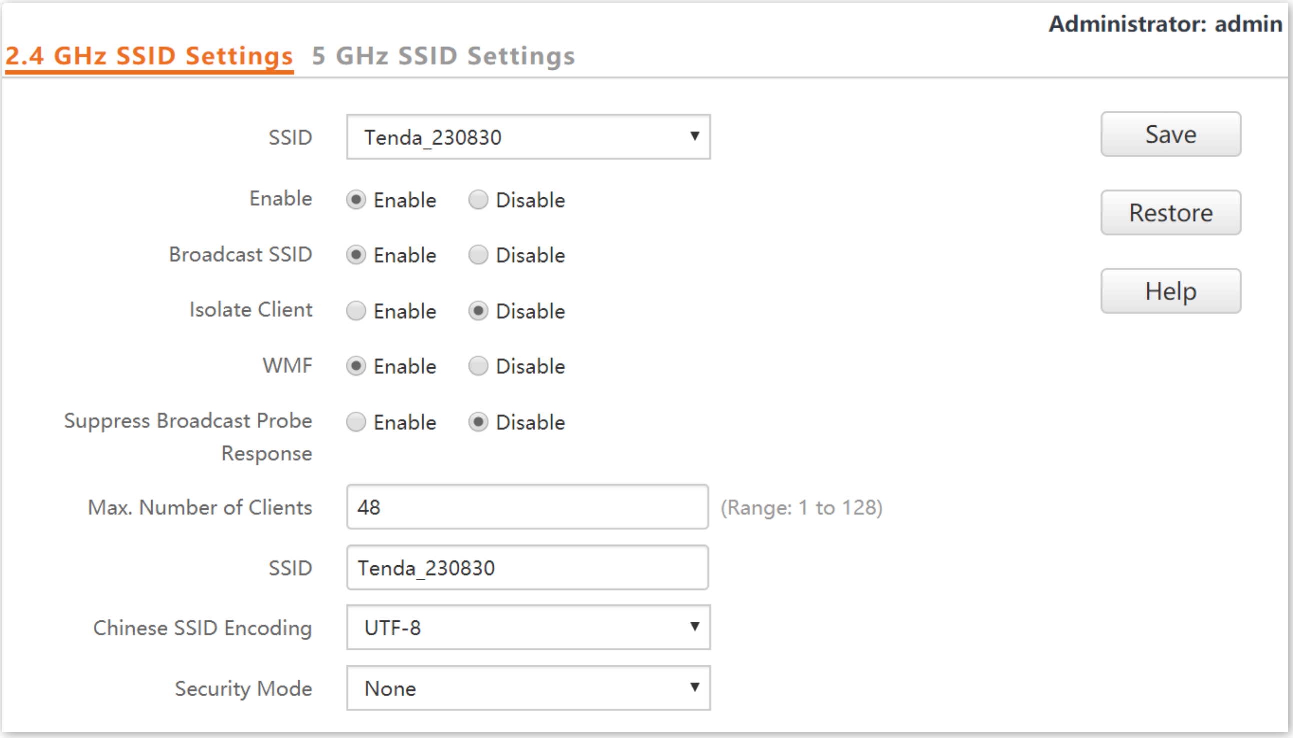
To view the latest DHCP client list, click **Refresh**.

6 Wireless Setting

6.1 SSID Settings

6.1.1 Overview

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



Administrator: admin

2.4 GHz SSID Settings 5 GHz SSID Settings

SSID	Tenda_230830 ▾
Enable	● Enable ○ Disable
Broadcast SSID	● Enable ○ Disable
Isolate Client	○ Enable ● Disable
WMF	● Enable ○ Disable
Suppress Broadcast Probe Response	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)
SSID	Tenda_230830
Chinese SSID Encoding	UTF-8 ▾
Security Mode	None ▾

Parameter description

Parameter	Description
SSID	It specifies the SSID to be configured. APs of this series support 8 SSIDs for the 2.4 GHz radio band and 4 SSIDs for the 5 GHz radio band. The first SSID displayed on the page under the radio band tab is the primary SSID of the radio band.
Enable	It specifies the status of the selected SSID. Primary SSID is enabled by default while other SSIDs are disabled by default. You can enable them as needed.

Parameter	Description
Broadcast SSID	When this parameter is set to Disable, the AP does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. It enhances the security of the wireless network.
Isolate Client	It isolates the wireless clients connected to the same wireless network corresponding to an SSID, so that the wireless clients can access only the wired network connected to the AP. Applying this function to hotspot setup at public places such as hotels and airports helps increase network security.
WMF	The 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.
Suppress Broadcast Probe Response	By default, wireless devices keep sending Probe Request packets that include the SSID field to scan their nearby wireless networks. After receiving such packets, this device determines whether the wireless devices are allowed to access its wireless networks based on the packets and responds using the Probe Response packets (including all Beacon frame parameters), which consumes a lot of wireless resources. After this function is enabled, this device does not respond to the requests without an SSID, saving wireless resources.
Max. Number of Clients	It specifies the maximum number of clients that can be concurrently connected to the wireless network corresponding to an SSID. After this upper limit is reached, the AP rejects new requests from clients for connecting to the wireless network.
SSID	It enables you to change the selected SSID. Chinese characters are allowed in an SSID.
Chinese SSID Encoding	It specifies the encoding format of Chinese characters in an SSID. The default value is **UTF-8**. If multiple SSIDs of the AP are enabled and contain Chinese characters, you are recommended to set this parameter to **UTF-8** for some SSIDs and to **GB2312** for others, so that any wireless clients can identify these SSIDs.
Security Mode	It specifies the security mode of the selected SSID. The options include: None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2.Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.

Security Mode

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

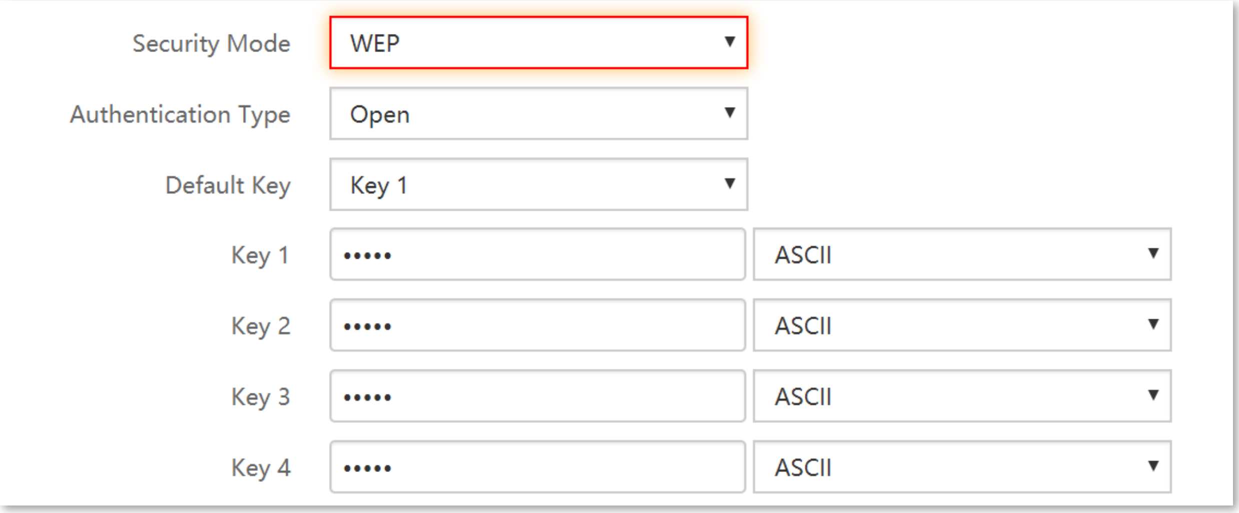
The AP supports various security modes for network encryption, including **None**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **Mixed WPA/WPA2-PSK**, **WPA**, and **WPA2**.

- **None**

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

- **WEP**

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



Security Mode: WEP

Authentication Type: Open

Default Key: Key 1

Key 1: ••••• ASCII

Key 2: ••••• ASCII

Key 3: ••••• ASCII

Key 4: ••••• ASCII

Parameter description

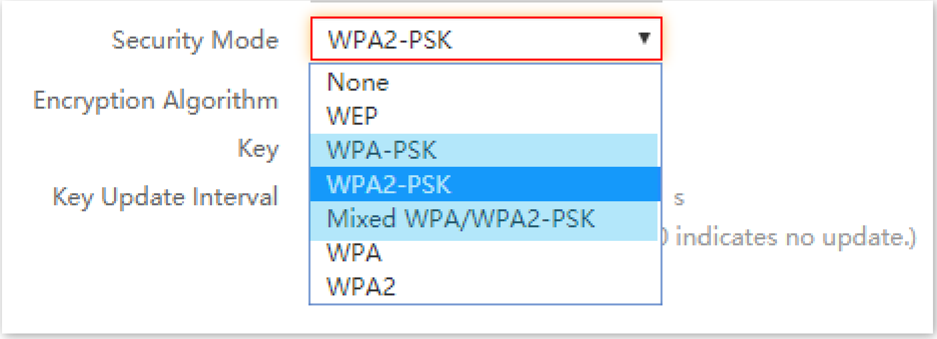
Parameter	Description
Authentication Type	It specifies the authentication type for the WEP security mode. The options include **Open**, **Shared**, and **802.1x**. The options share the same encryption process. • **Open**: It specifies that authentication is not required and data exchanged is encrypted 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. • **802.1x**: It specifies that 802.1x authentication is required and data exchanged is encrypted with WEP. In this case, ports are enabled for user authentication when valid clients connect to the wireless network corresponding to the selected SSID, and disabled when invalid users connect to the wireless network.

Parameter	Description
Default Key	It specifies the WEP key for the **Open** or **Shared** encryption type. For example, if **Default Key** is set to **Key 2**, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Key 2.
Key 1/2/3/4	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 Hexadecimal. • **ASCII**: 5 or 13 ASCII characters are allowed in the key. • -**Hex**: 10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key.
RADIUS Server	These parameters are dedicated to the 802.1x authentication type. It specifies the IP address/port number/shared key of the RADIUS server for authentication.
RADIUS Port	
RADIUS Password	

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

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

WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK adopt a pre-shared key for authentication, while the AP generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home wireless networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all clients use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.


Security Mode WPA2-PSK

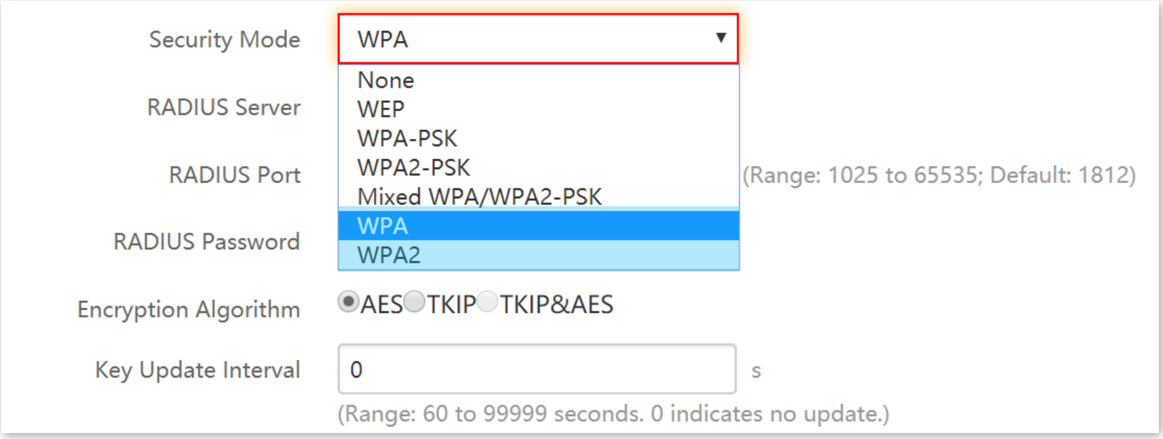
Parameter description

Parameter	Description
Security Mode	It indicates the personal or pre-shared key security mode, including **WPA-PSK**, **WPA2-PSK**, and **Mixed WPA/WPA2-PSK**. • **WPA-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA-PSK. • **WPA2-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA2-PSK. • **Mixed WPA/WPA2-PSK**: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. If **Security Mode** is set to **WPA-PSK**, this parameter has the **AES** and **TKIP** values. If **Security Mode** is set to **WPA2-PSK** or **Mixed WPA/WPA2-PSK**, this parameter has the **AES**, **TKIP**, and **TKIP&AES** values. • **AES**: It indicates the Advanced Encryption Standard. • **TKIP**: It indicates the Temporal Key Integrity Protocol. If **TKIP** is used, the maximum wireless throughput of the AP is limited to 54 Mbps. • **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a pre-shared WPA key, that is, the password clients use to connect to the wireless network.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value **0** indicates that a WAP key is not updated.

WPA and WPA2

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

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



Security Mode	WPA
RADIUS Server	
RADIUS Port	(Range: 1025 to 65535; Default: 1812)
RADIUS Password	
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Key Update Interval	0 s (Range: 60 to 99999 seconds. 0 indicates no update.)

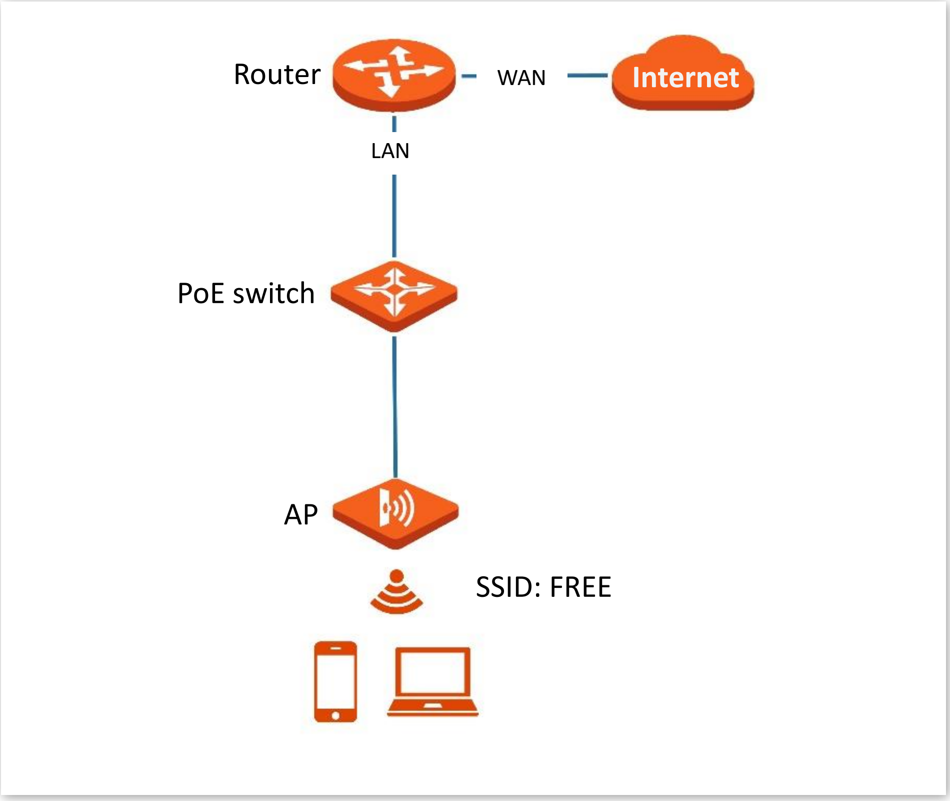
Parameter description

Parameter	Description
Security Mode	The **WPA** and **WPA2** options are available for network protection with a RADIUS server. • **WPA**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA. • **WPA2**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA2.
RADIUS Server	It specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	It specifies the port number of the RADIUS server for client authentication.
RADIUS Password	It specifies the shared password of the RADIUS server.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. The available options include **AES**, **TKIP**, and **TKIP&AES**. • **AES**: It indicates the Advanced Encryption Standard. • **TKIP**: It indicates the Temporal Key Integrity Protocol. 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 Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value **0** indicates that a WAP key is not updated.

6.1.2 Example of Setting up an Open Wireless Network

Networking requirement

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



Configuration procedure

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

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

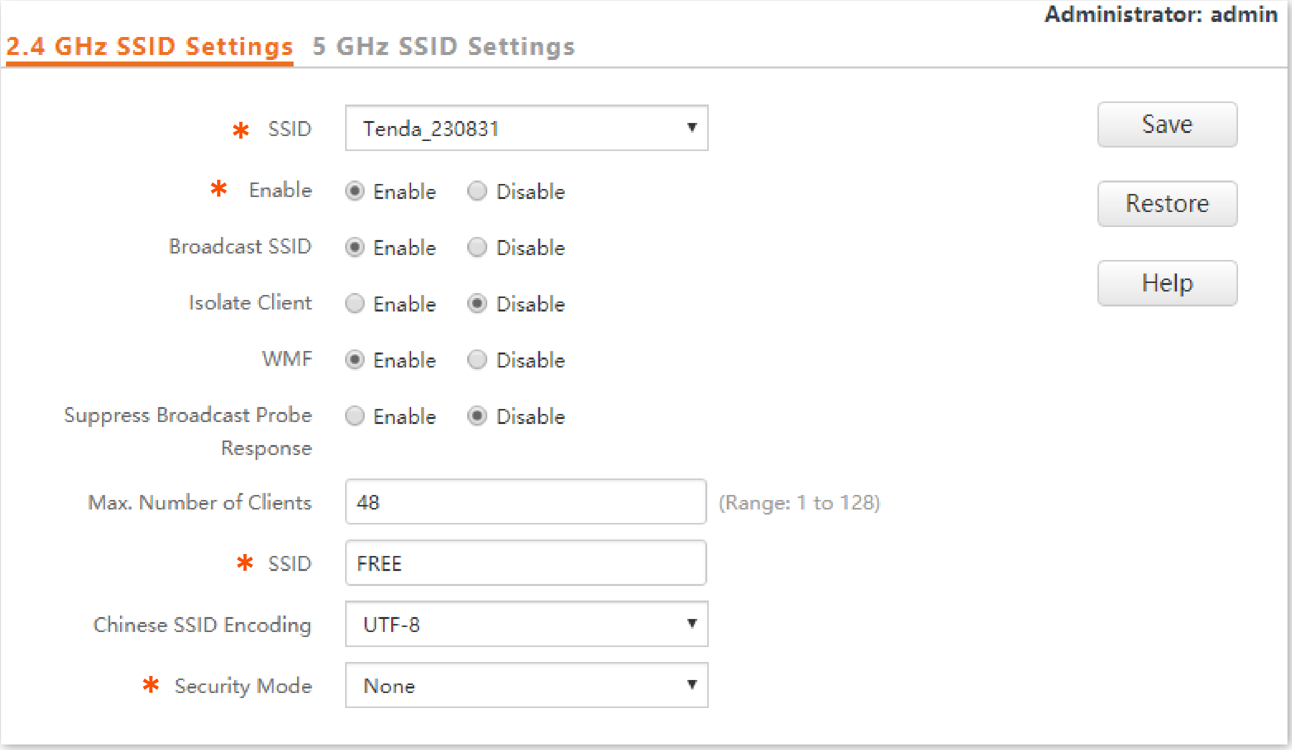
Step 2 Select the second SSID from the **SSID** drop-down list box.

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

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

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

Step 6 Click **Save**.



* SSID: Tenda_230831

* Enable: ● Enable ○ Disable

Broadcast SSID: ● Enable ○ Disable

Isolate Client: ○ Enable ● Disable

WMF: ● Enable ○ Disable

Suppress Broadcast Probe Response: ○ Enable ● Disable

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

* SSID: FREE

Chinese SSID Encoding: UTF-8

* Security Mode: None

---End

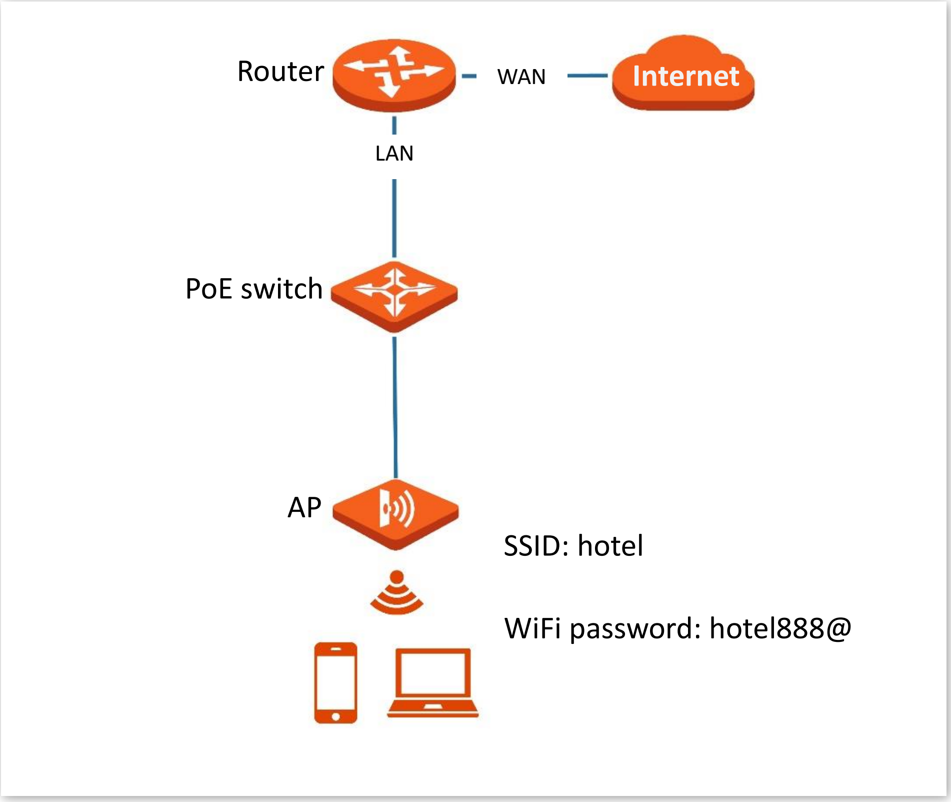
Verification

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

6.1.3 Example of Setting up a Wireless Network Encrypted with PSK

Networking requirement

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



Configuration procedure

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

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

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

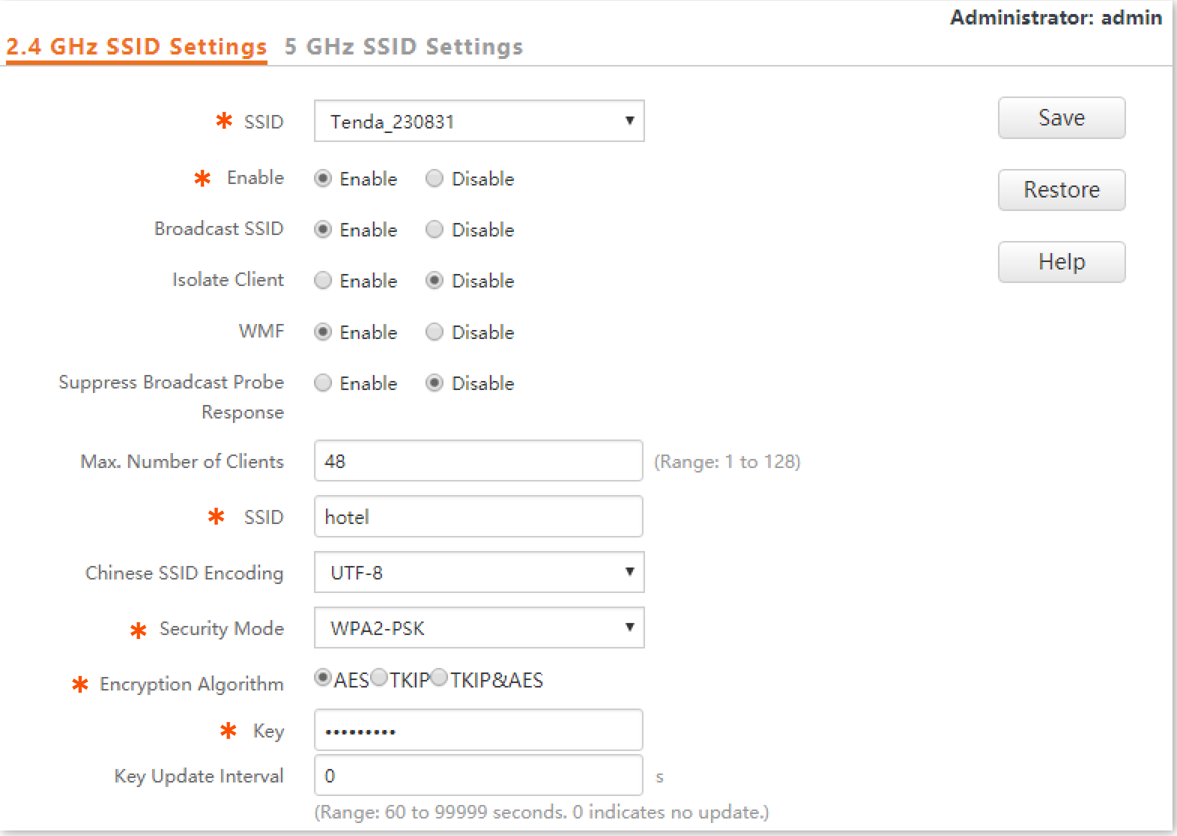
Step 3 Select the **Enable** check box.

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

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

Step 6 Set **Key** to **hotel888@**.

Step 7 Click **Save**.



* SSID	Tenda_230831 ▾
* Enable	● Enable ○ Disable
Broadcast SSID	● Enable ○ Disable
Isolate Client	○ Enable ● Disable
WMF	● Enable ○ Disable
Suppress Broadcast Probe Response	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)
* SSID	hotel
Chinese SSID Encoding	UTF-8 ▾
* Security Mode	WPA2-PSK ▾
* Encryption Algorithm	●AES○TKIP○TKIP&AES
* Key	•••••••••
Key Update Interval	0 s (Range: 60 to 99999 seconds. 0 indicates no update.)

---End

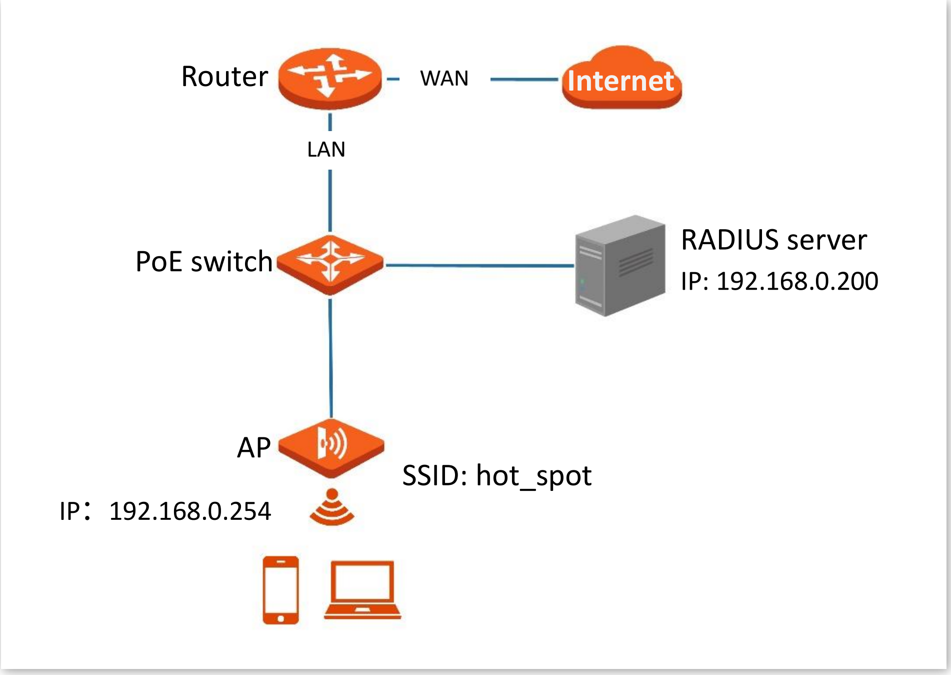
Verification

Wireless devices can connect to the **hotel** wireless network with the password **hotel888@**.

6.1.4 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. See the following figure.



Configuration procedure

- **Configure the AP**

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

Assume that the second SSID of the AP is used.

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

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

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

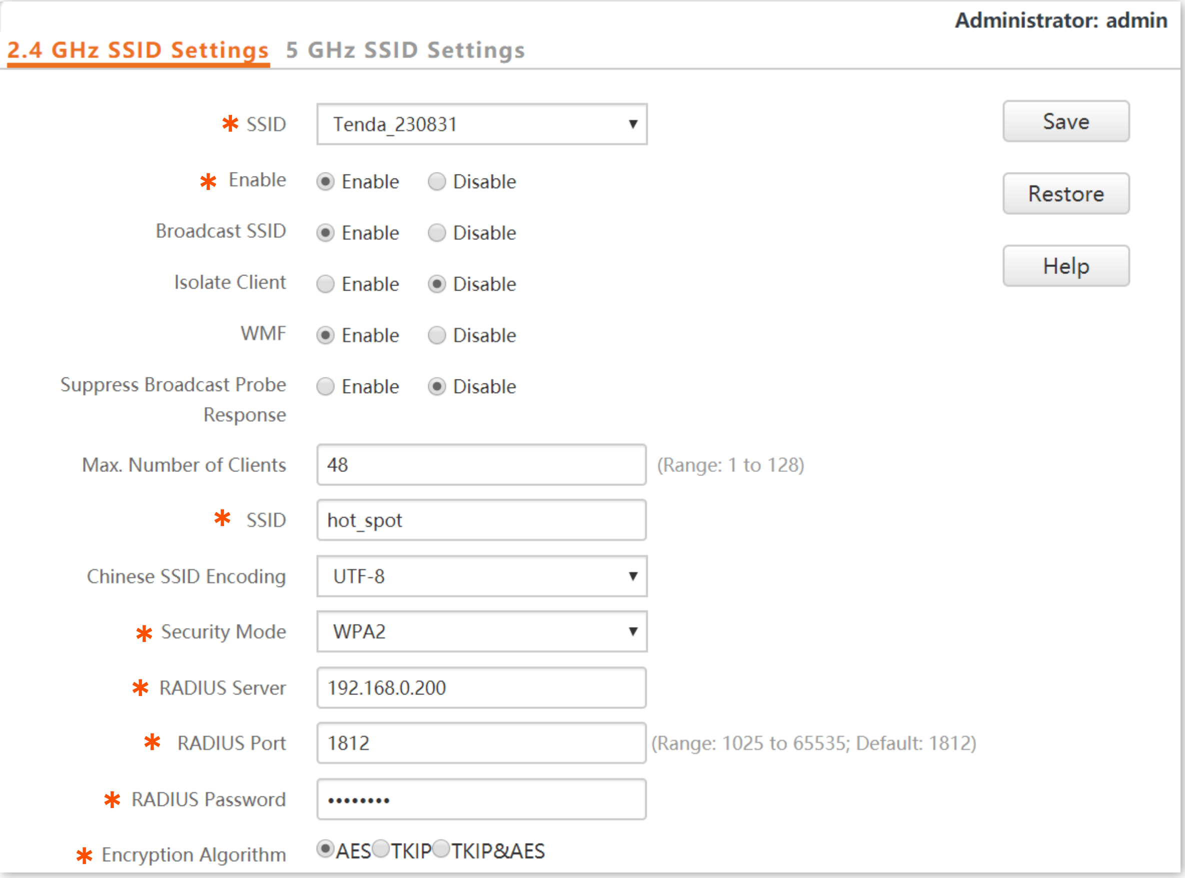
Step 4 Change the value of the **SSID** text box to **hot_spot**.

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

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

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

Step 8 Click **Save**.



Administrator: admin

2.4 GHz SSID Settings 5 GHz SSID Settings

Save

Restore

Help

* SSID	Tenda_230831 ▾
* Enable	● Enable ○ Disable
Broadcast SSID	● Enable ○ Disable
Isolate Client	○ Enable ● Disable
WMF	● Enable ○ Disable
Suppress Broadcast Probe Response	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)
* SSID	hot_spot
Chinese SSID Encoding	UTF-8 ▾
* Security Mode	WPA2 ▾
* RADIUS Server	192.168.0.200
* RADIUS Port	1812 (Range: 1025 to 65535; Default: 1812)
* RADIUS Password	••••••••
* Encryption Algorithm	●AES○TKIP○TKIP&AES

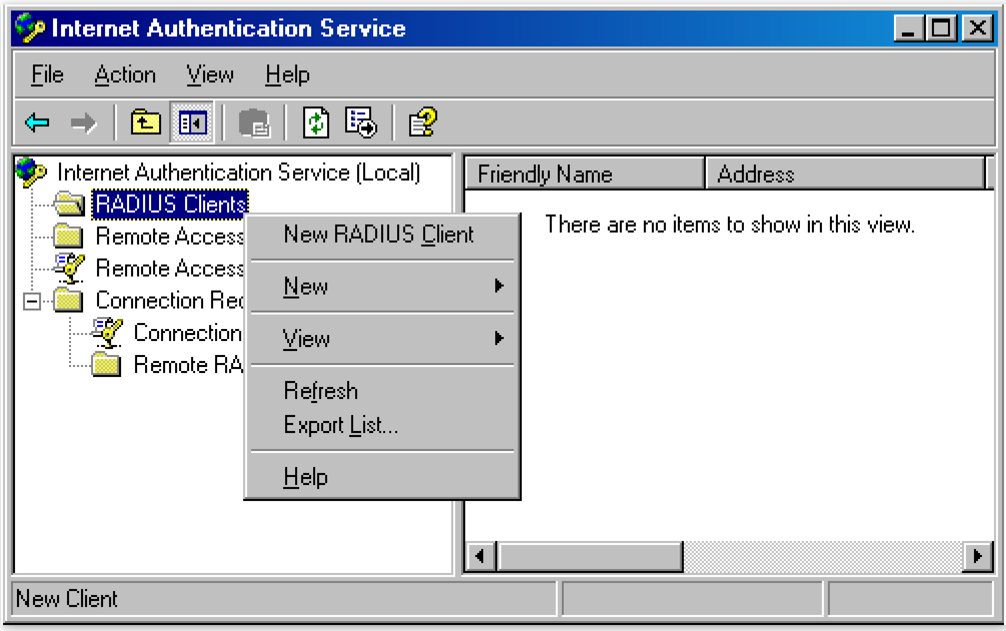
■ Configure the RADIUS server

TIP

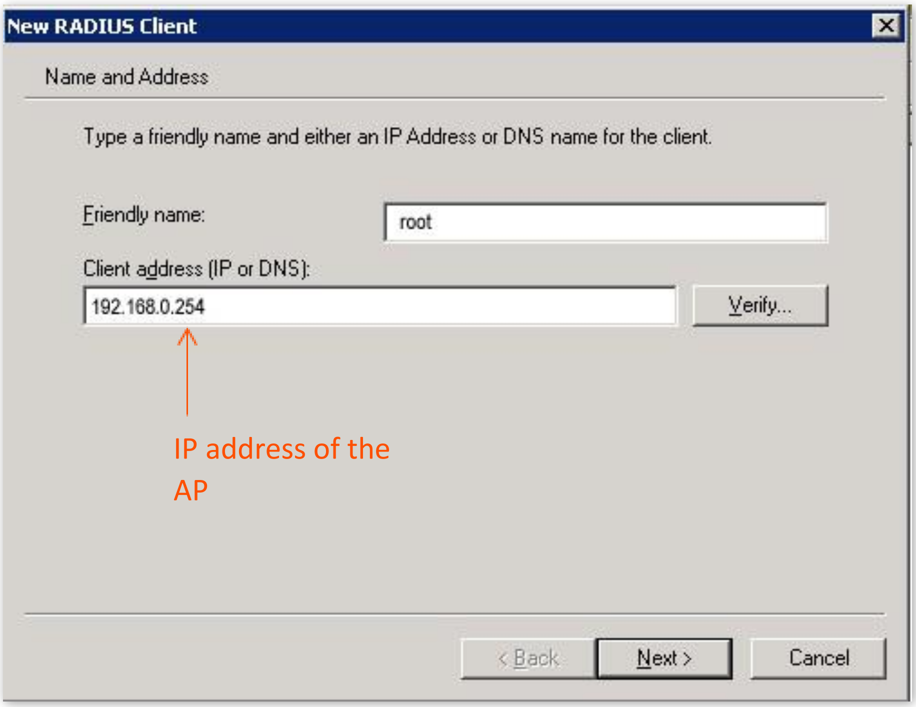
Windows 2003 is used as an example to describe how to configure the RADIUS server.

Step 1 Configure a RADIUS client.

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



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


New RADIUS Client

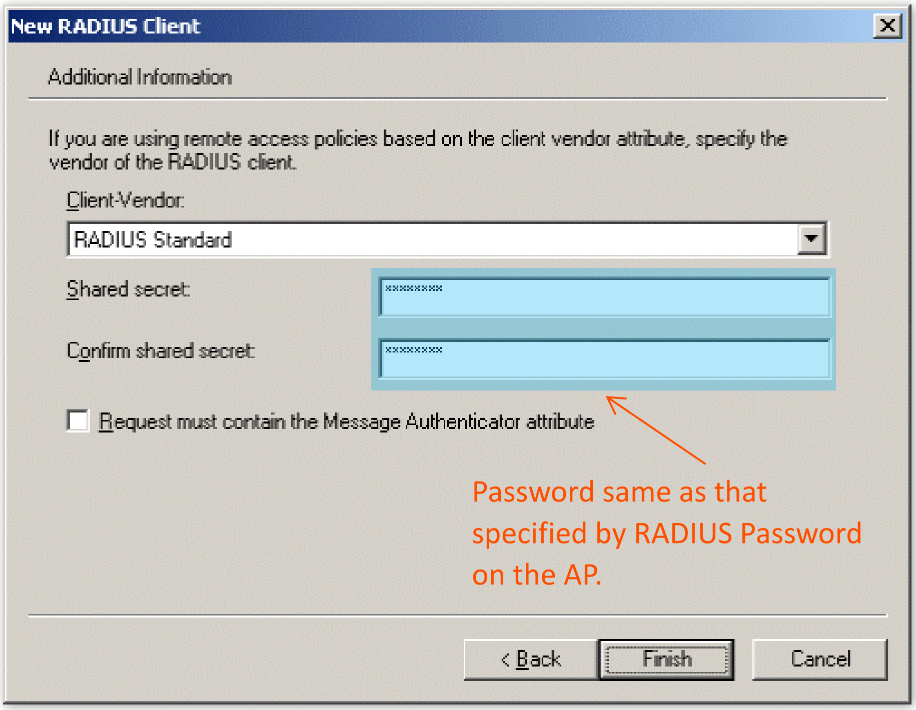
Name and Address

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

Friendly name: root

Client address (IP or DNS): 192.168.0.254

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



New RADIUS Client

Additional Information

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

Client-Vendor: RADIUS Standard

Shared secret: ********

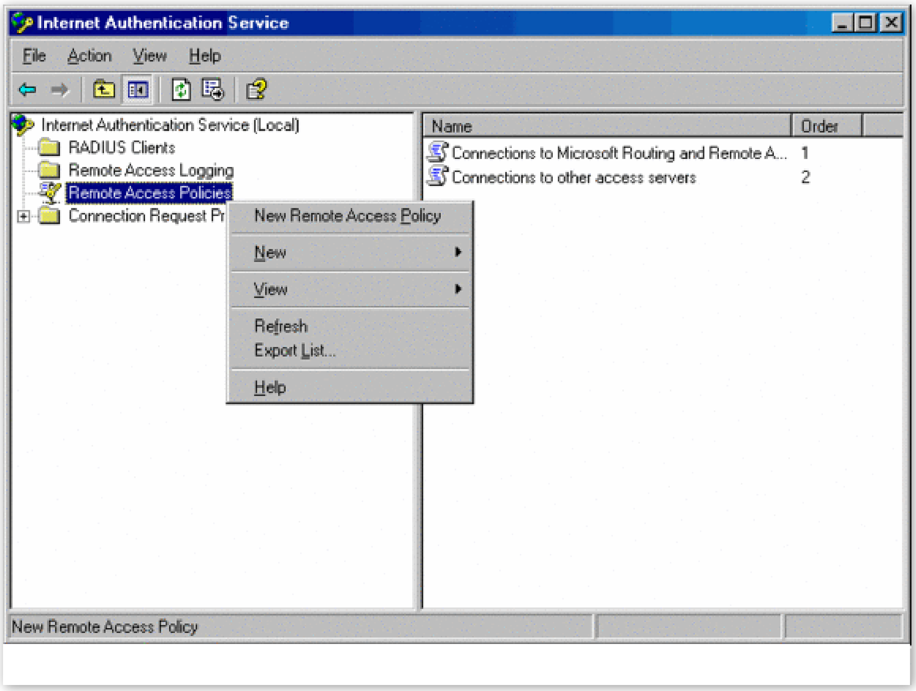
Confirm shared secret: ********

□ Request must contain the Message Authenticator attribute

Password same as that specified by RADIUS Password on the AP.

Step 2 Configure a remote access policy.

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



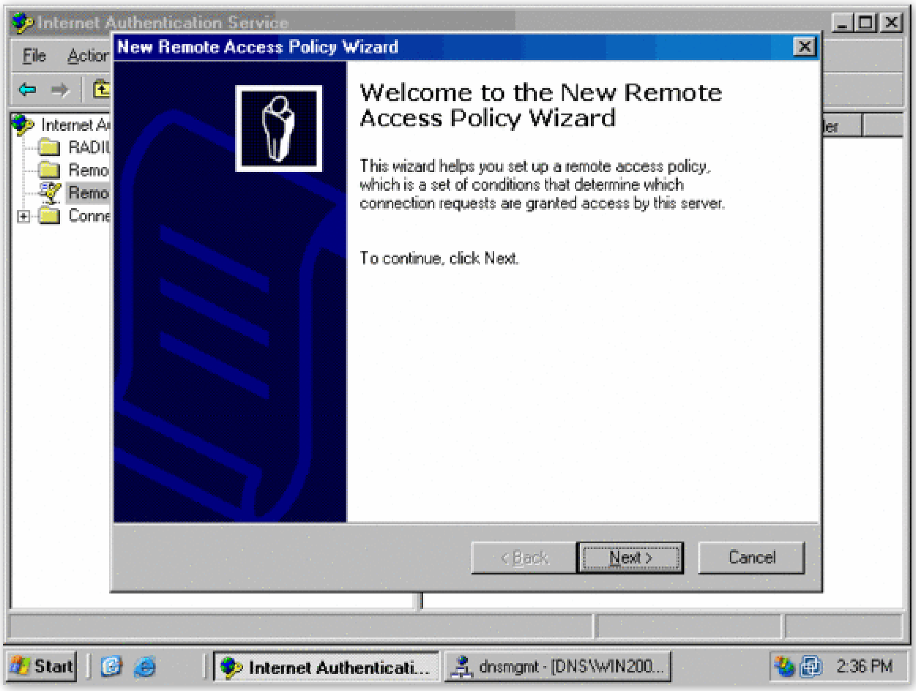
Internet Authentication Service

Internet Authentication Service (Local)
- RADIUS Clients
- Remote Access Logging
- Remote Access Policies
- Connection Request Pr

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

New Remote Access Policy

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

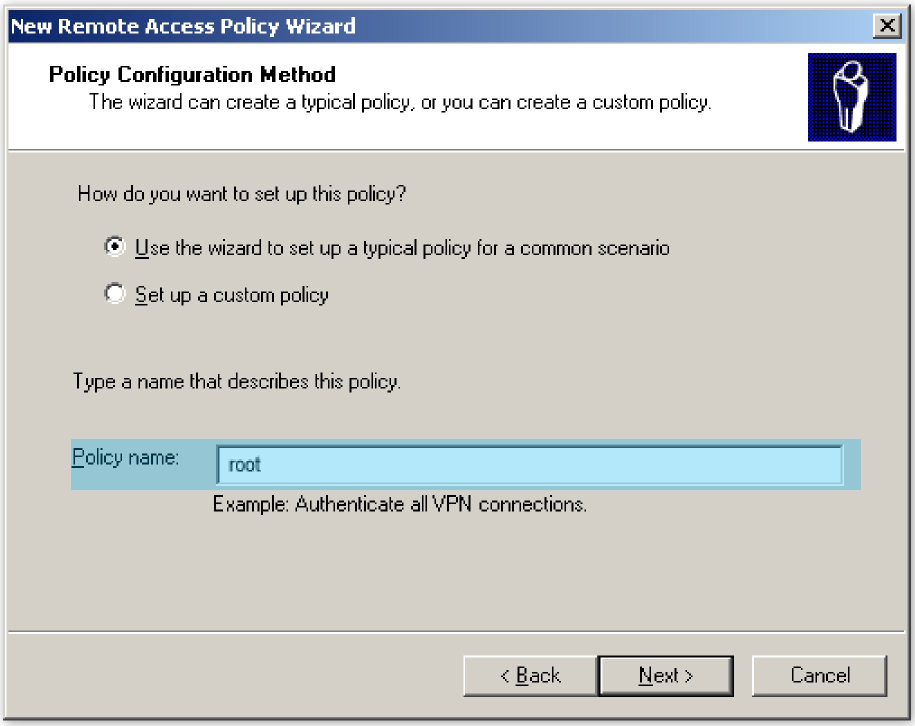


Welcome to the New Remote Access Policy Wizard

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

To continue, click Next.

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



Policy Configuration Method

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

How do you want to set up this policy?

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

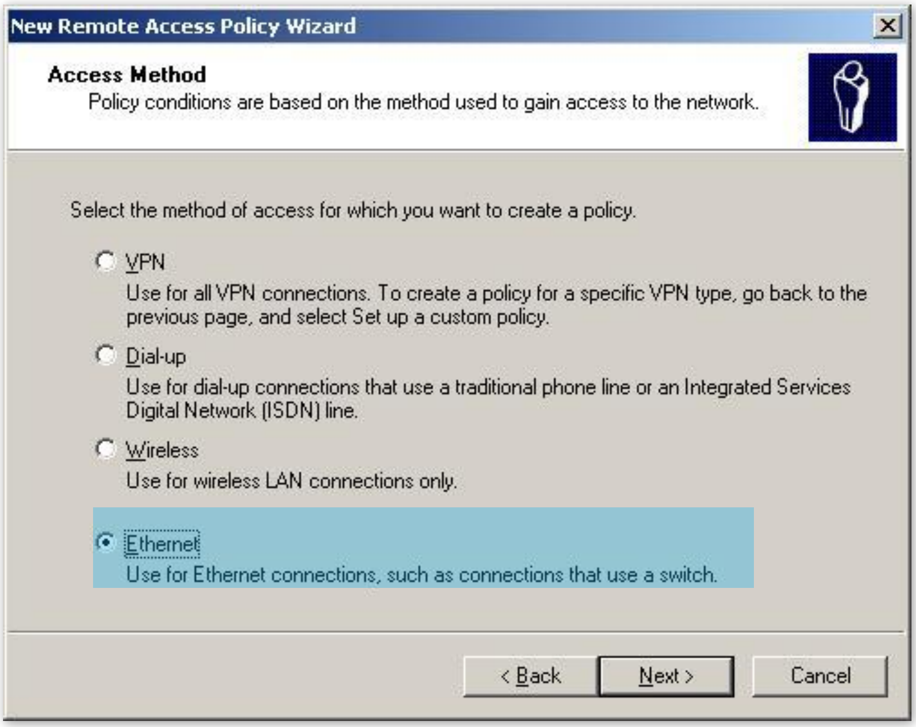
○ Set up a custom policy

Type a name that describes this policy.

Policy name: root

Example: Authenticate all VPN connections.

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



New Remote Access Policy Wizard

Access Method

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

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

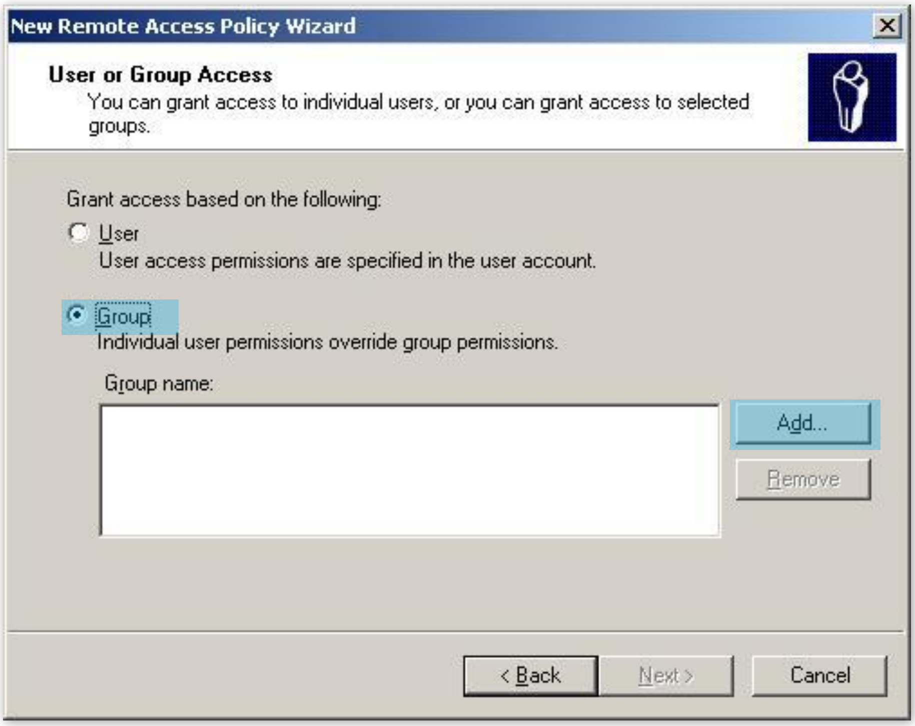
○ VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

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

○ Wireless
Use for wireless LAN connections only.

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

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



New Remote Access Policy Wizard

User or Group Access

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

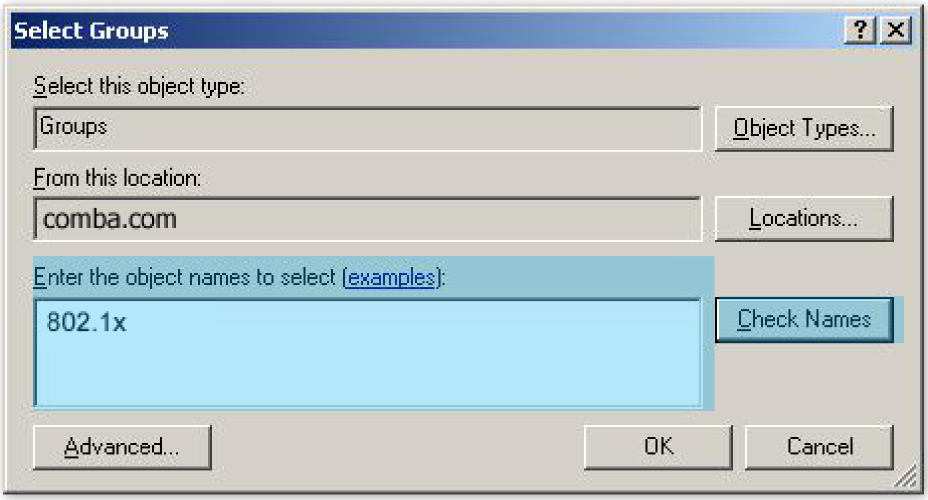
Grant access based on the following:

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

● Group
Individual user permissions override group permissions.

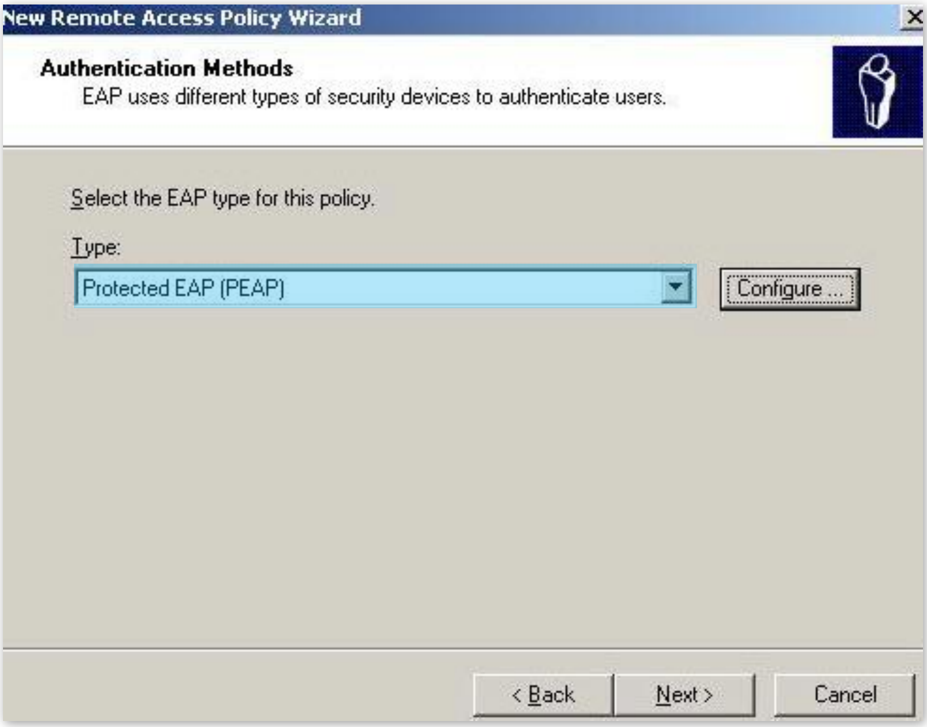
Group name:

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



Select this object type:
Groups
From this location:
comba.com
Enter the object names to select (examples):
802.1x

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

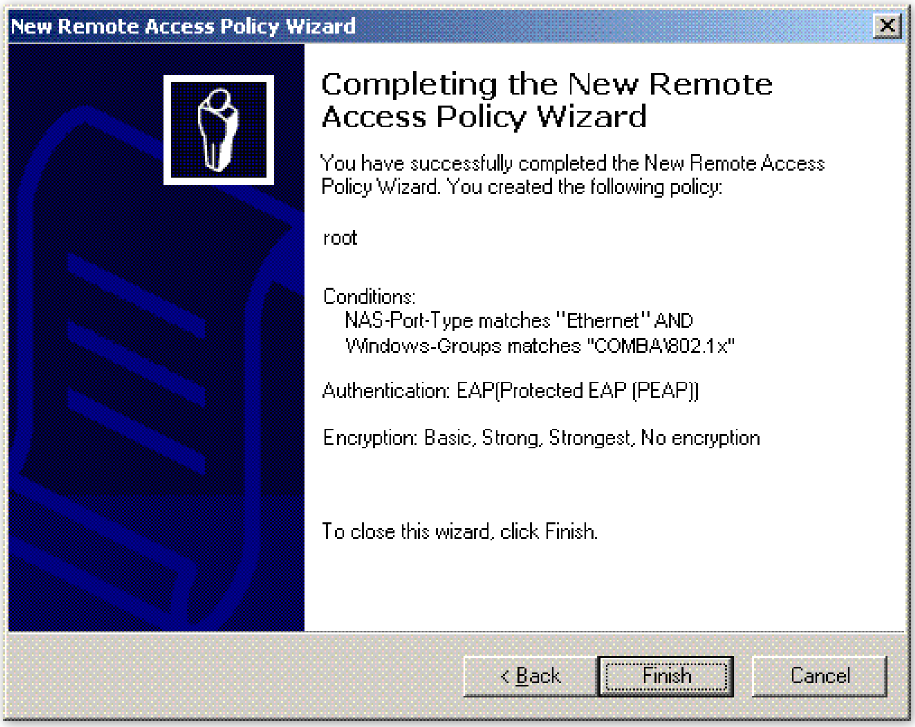


Authentication Methods
EAP uses different types of security devices to authenticate users.

Select the EAP type for this policy.

Type:
Protected EAP (PEAP)

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



New Remote Access Policy Wizard

Completing the New Remote Access Policy Wizard

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

root

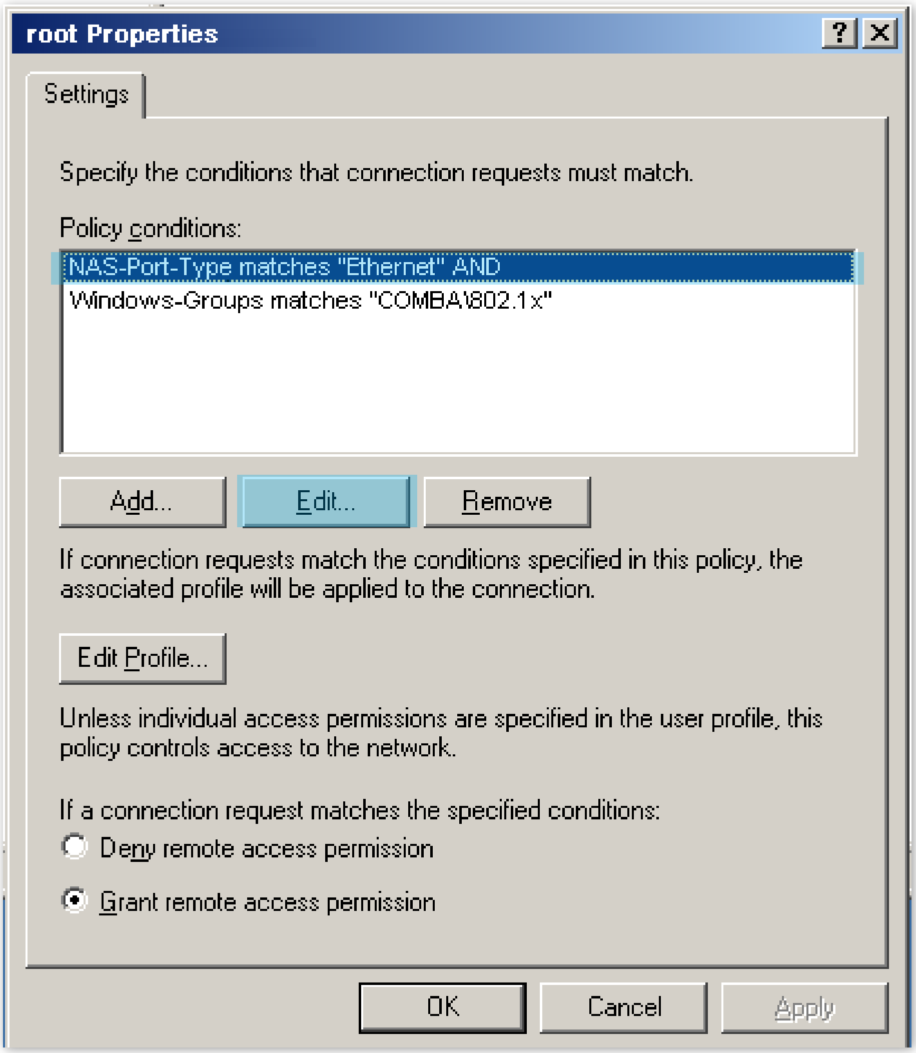
Conditions:
NAS-Port-Type matches "Ethernet" AND
Windows-Groups matches "COMBA\802.1x"

Authentication: EAP(Protected EAP (PEAP))

Encryption: Basic, Strong, Strongest, No encryption

To close this wizard, click Finish.

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



Specify the conditions that connection requests must match.

Policy conditions:

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

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

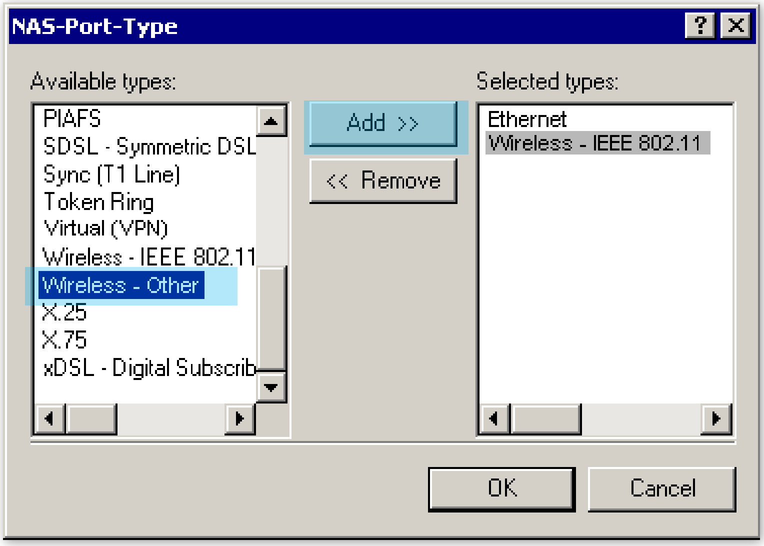
Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

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



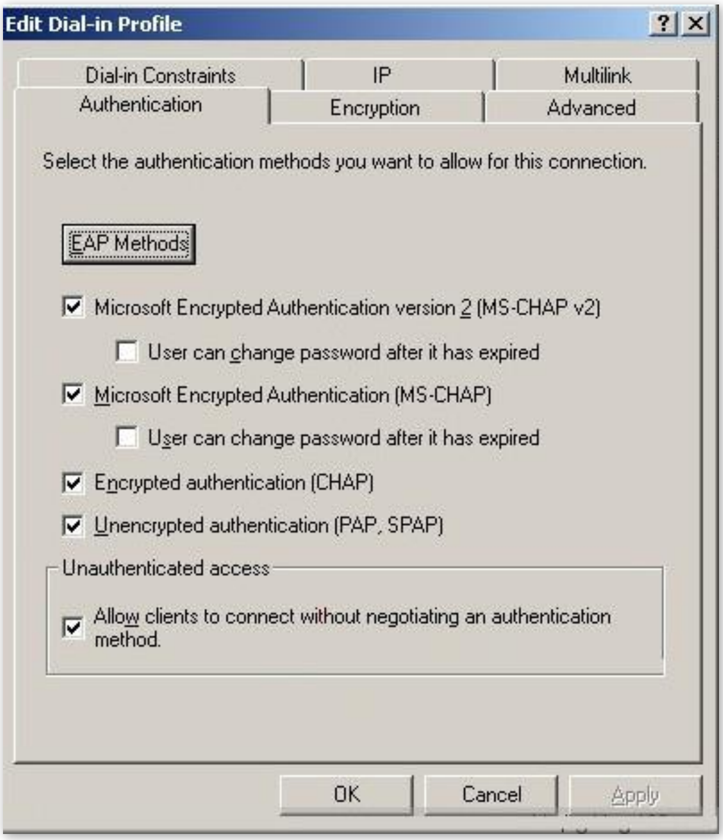
Available types:

PIAFS
SDSL - Symmetric DSL
Sync (T1 Line)
Token Ring
Virtual (VPN)
Wireless - IEEE 802.11
Wireless - Other
X.25
X.75
xDSL - Digital Subscrib

Selected types:

Ethernet
Wireless - IEEE 802.11

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



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

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

□ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

☑ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☑ Allow clients to connect without negotiating an authentication method.

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

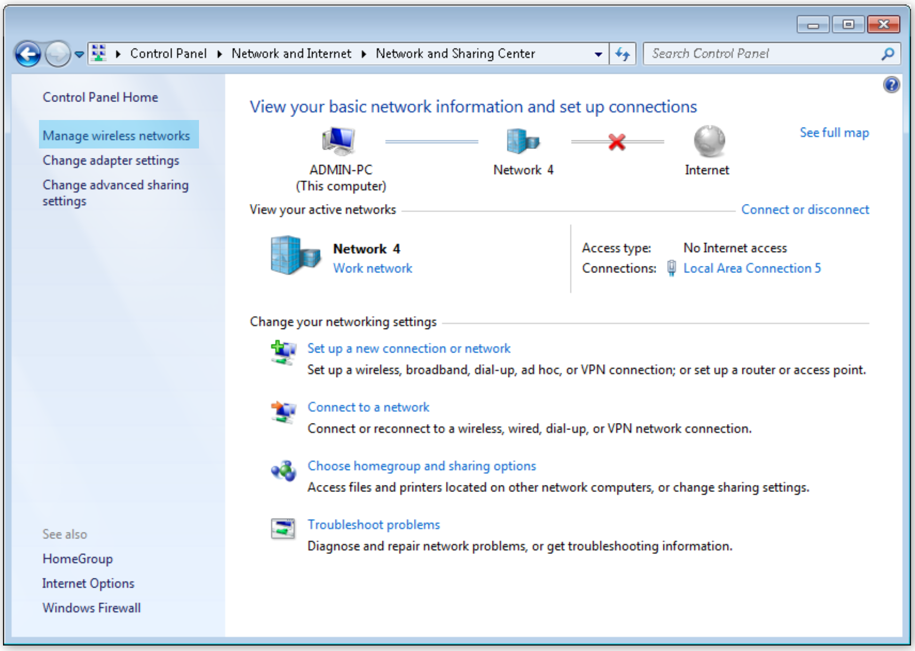
Step 3 Configure user information.
Create a user and add the user to group **802.1x**.

Step 4 Configure your wireless device.

TIP

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

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



View your basic network information and set up connections

View your active networks

Network 4
Work network

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

Change your networking settings

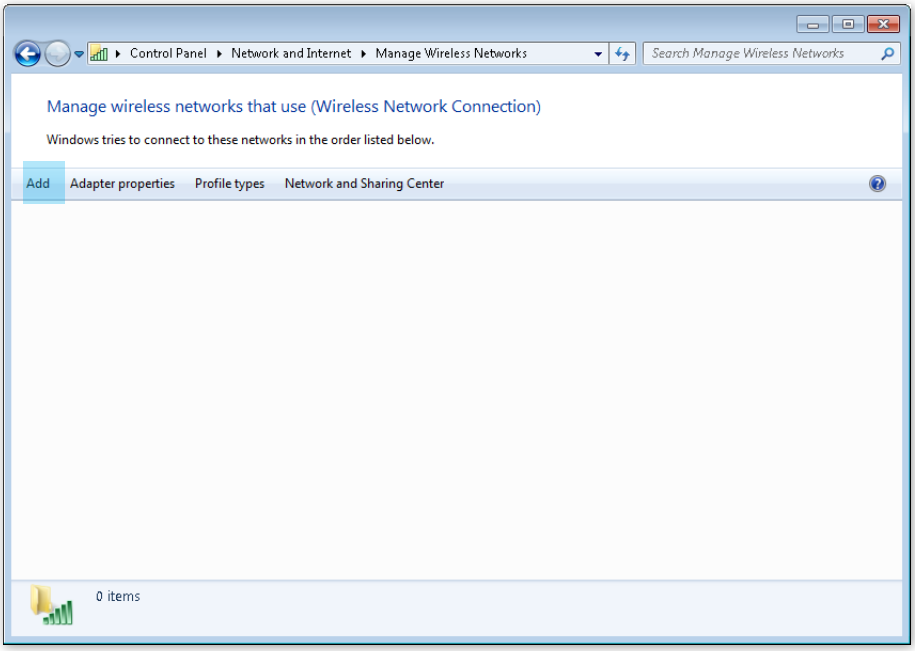
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

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

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

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

2. Click **Add**.

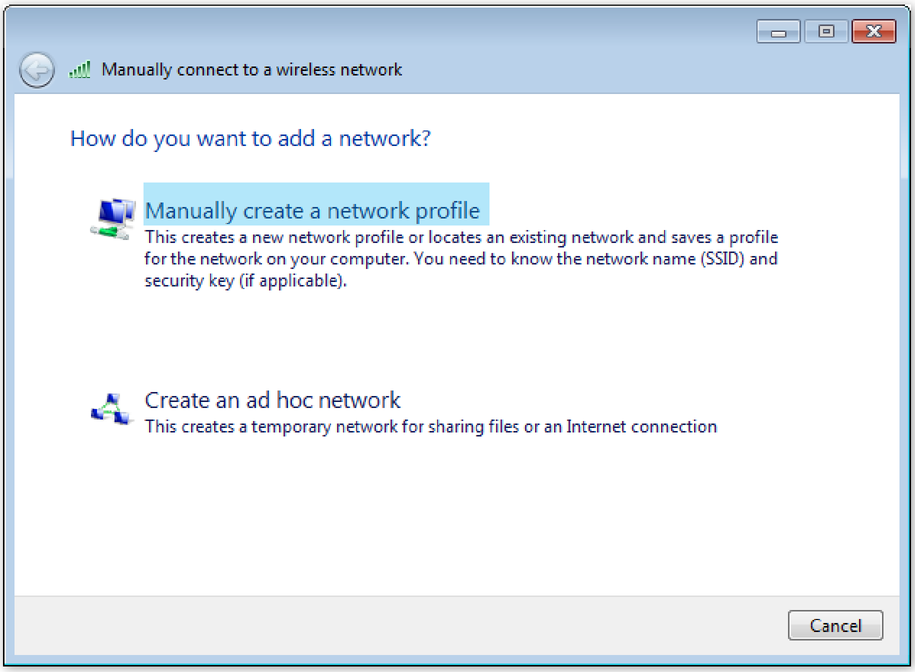

Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Networks
Add
Adapter properties
Profile types
Network and Sharing Center

Manage wireless networks that use (Wireless Network Connection)

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

0 items

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



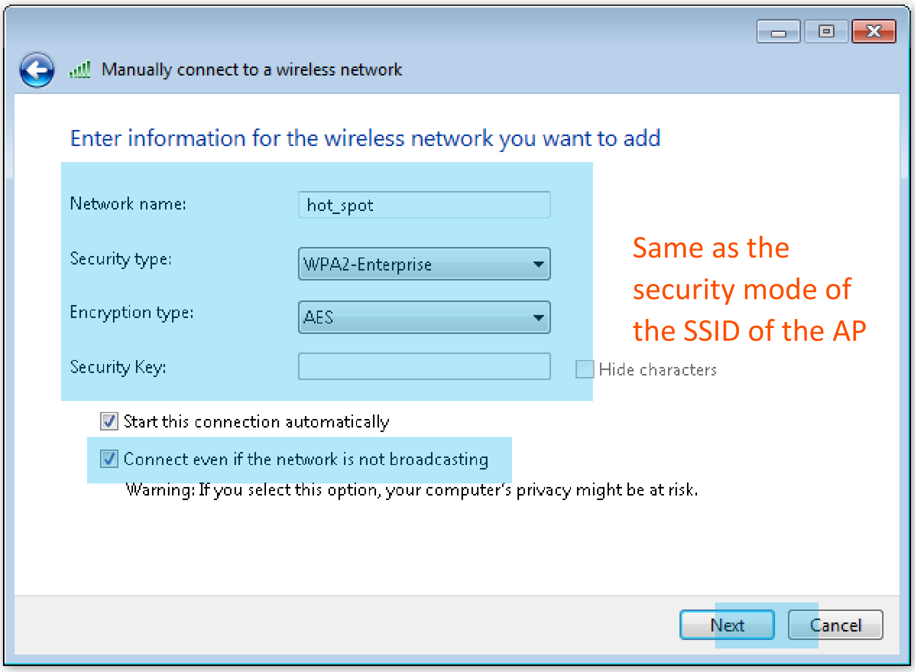
Manually connect to a wireless network

How do you want to add a network?

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

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

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



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:	hot_spot
Security type:	WPA2-Enterprise
Encryption type:	AES
Security Key:	

□ Hide characters

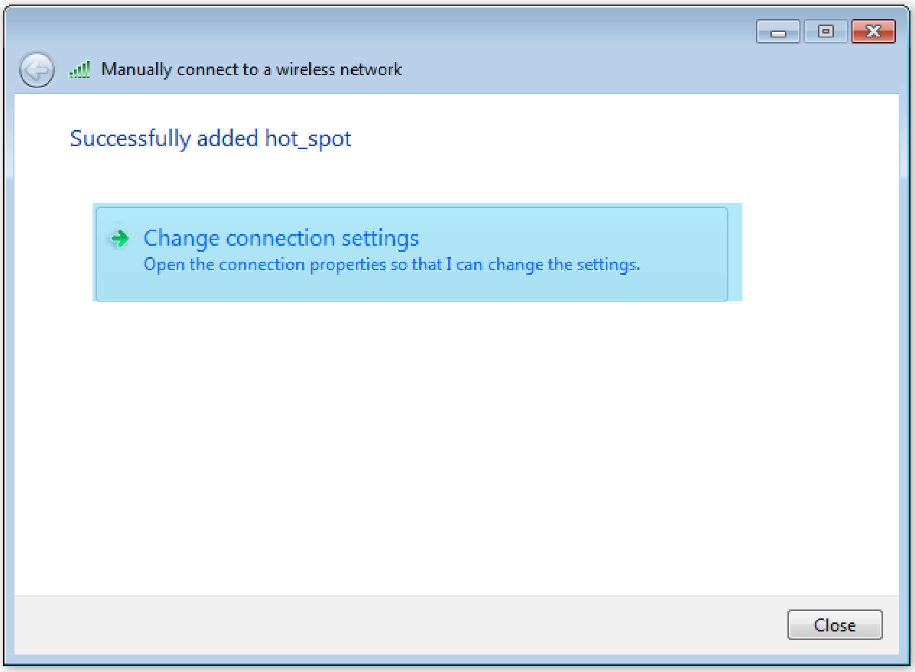
Same as the security mode of the SSID of the AP

☑ Start this connection automatically

☑ Connect even if the network is not broadcasting

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

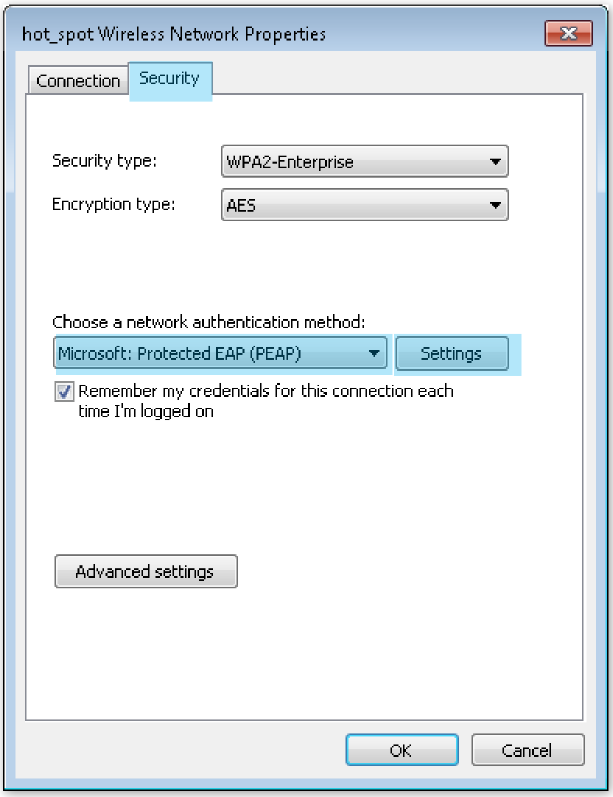
5. Click **Change connection settings**.



Successfully added hot_spot

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

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



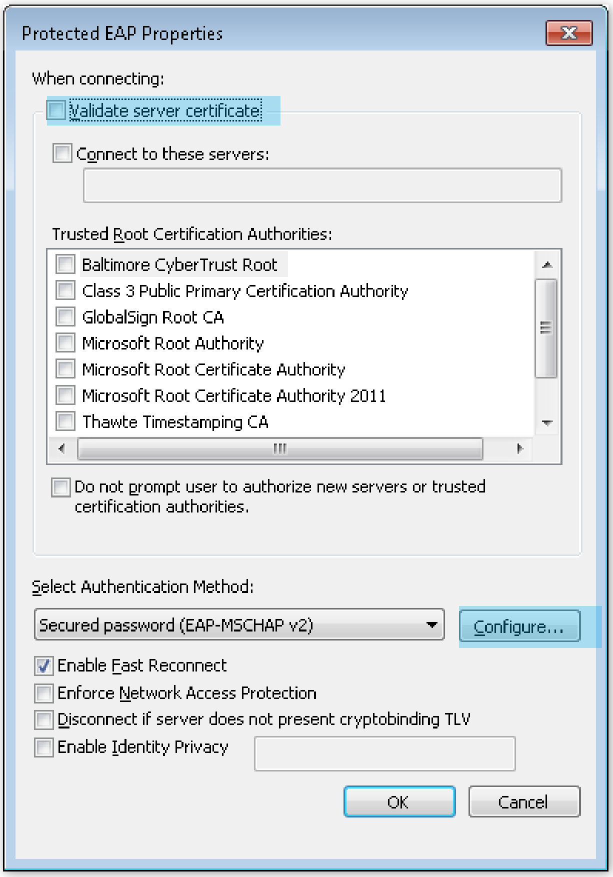
Security type: WPA2-Enterprise

Encryption type: AES

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

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

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



Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

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

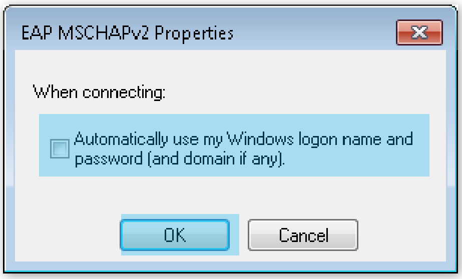
□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

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

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

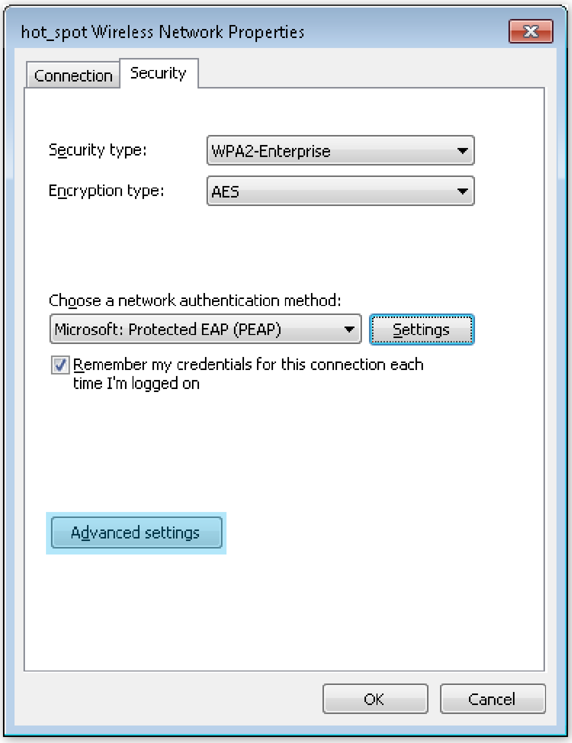


EAP MSCHAPv2 Properties

When connecting:

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

9. Click **Advanced settings**.



hot_spot Wireless Network Properties

Security type: WPA2-Enterprise

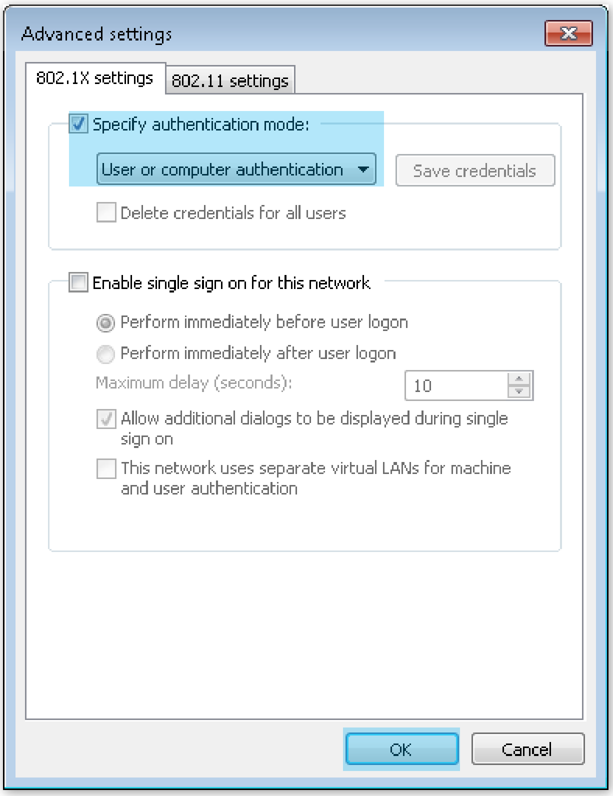
Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

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

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



Advanced settings

☑ Specify authentication mode:

User or computer authentication

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

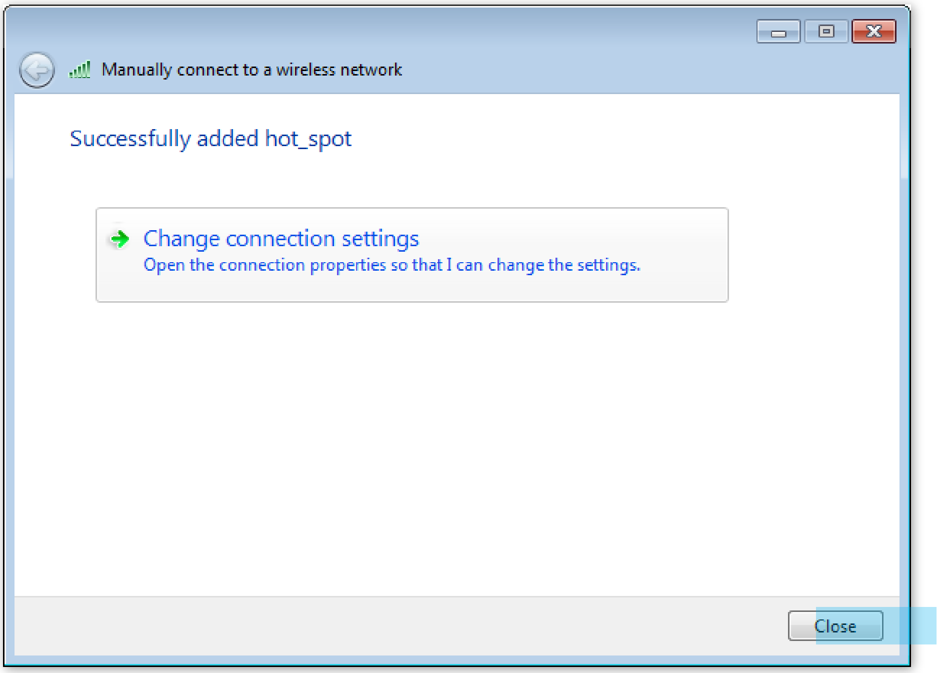
○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

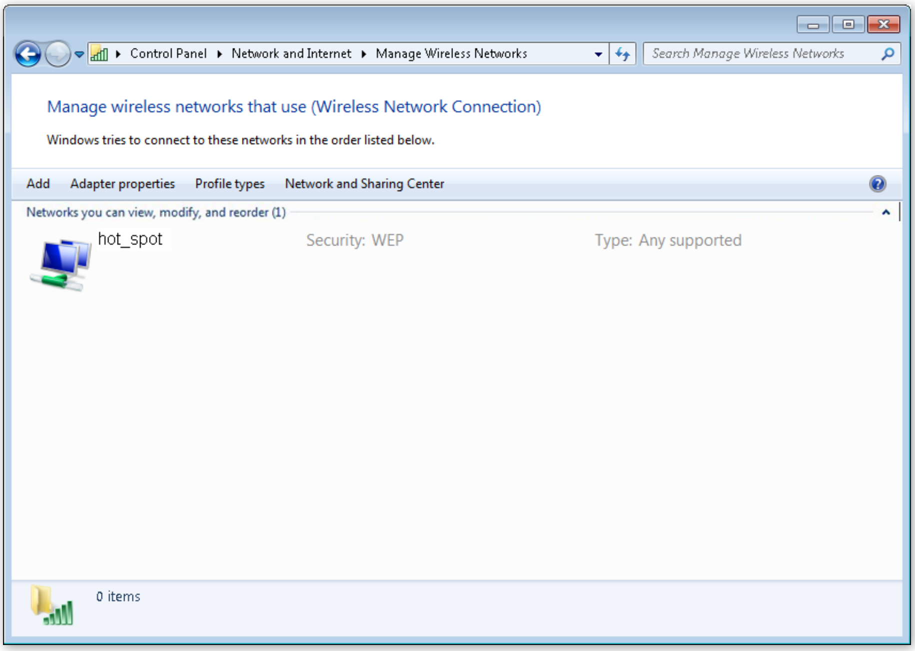
□ This network uses separate virtual LANs for machine and user authentication

11. Click **Close**.



Successfully added hot_spot

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


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

Manage wireless networks that use (Wireless Network Connection)

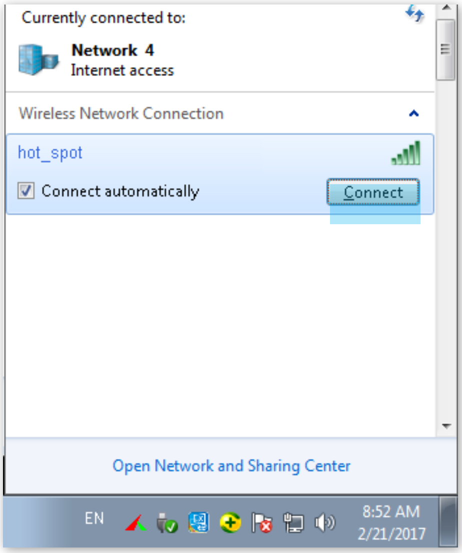
Windows tries to connect to these networks in the order listed below.

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

hot_spot Security: WEP Type: Any supported

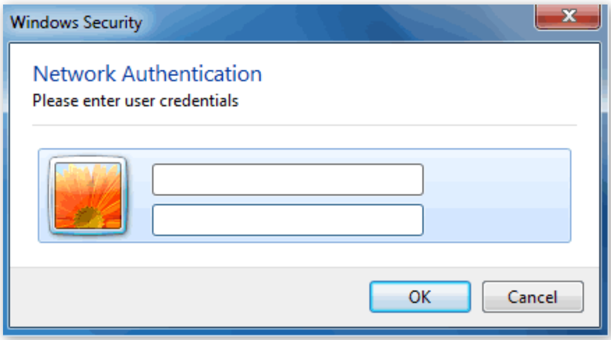
0 items

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



☑ Connect automatically

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



Network Authentication

Please enter user credentials

---End

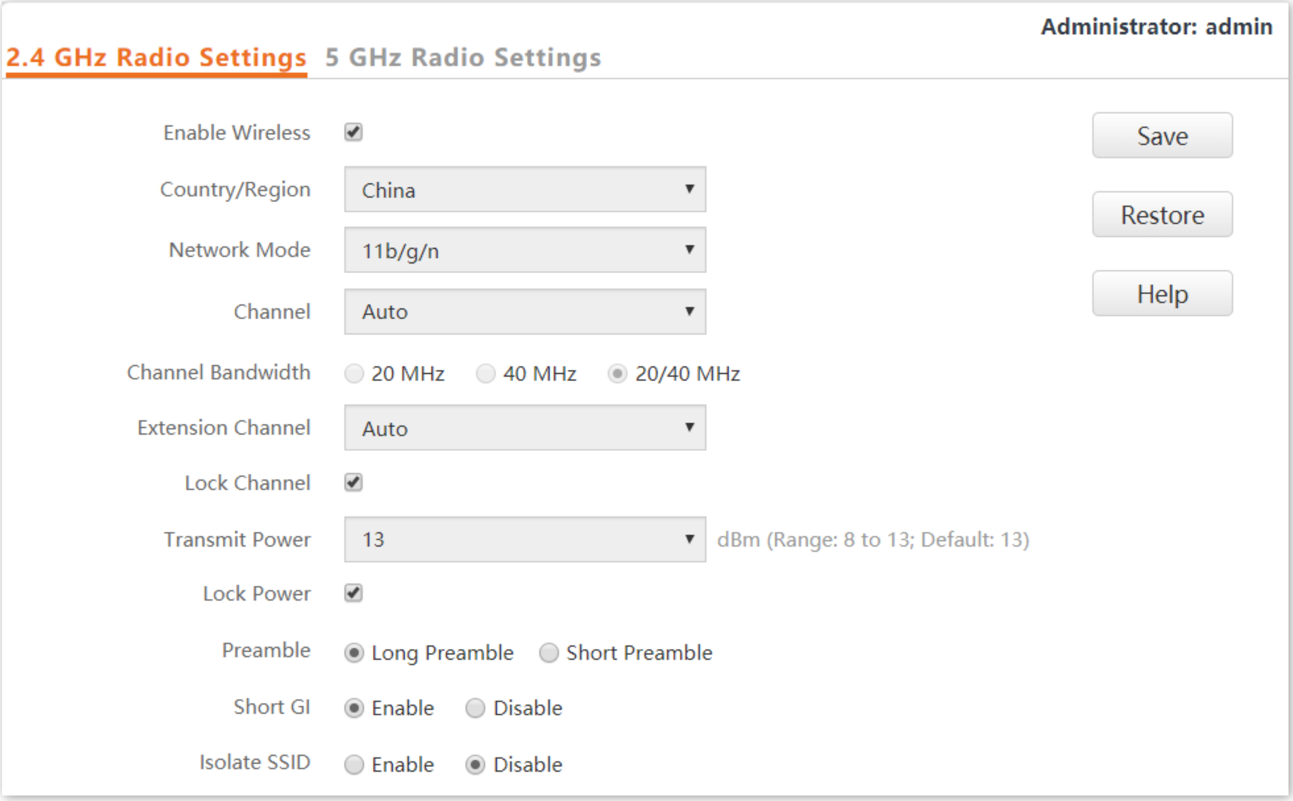
Verification

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

6.2 Radio Settings

To access the page, choose **Wireless Setting** > **Radio Settings**.

This page enables you to modify the basic radio parameters.



Administrator: admin

2.4 GHz Radio Settings 5 GHz Radio Settings

Enable Wireless	☑
Country/Region	China ▾
Network Mode	11b/g/n ▾
Channel	Auto ▾
Channel Bandwidth	○ 20 MHz ○ 40 MHz ● 20/40 MHz
Extension Channel	Auto ▾
Lock Channel	☑
Transmit Power	13 ▾ dBm (Range: 8 to 13; Default: 13)
Lock Power	☑
Preamble	● Long Preamble ○ Short Preamble
Short GI	● Enable ○ Disable
Isolate SSID	○ Enable ● Disable

Parameter description

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

Parameter	Description
Network Mode	It specifies the wireless network mode of the AP. This parameter can be set if **Lock Channel** is not selected. Available options for 2.4 GHz are **11b**, **11g**, **11b/g**, and **11b/g/n** and available options for 5 GHz are **11a**, **11ac**, and **11a/n**. - **11b**: The AP works in 802.11b mode and only wireless devices compliant with 802.11b can connect to the 2.4 GHz wireless networks of the AP. - **11g**: The AP works in 802.11g mode and only wireless devices compliant with 802.11g can connect to the 2.4 GHz wireless networks of the AP. - **11b/g**: The AP works in 802.11b/g mode and only wireless devices compliant with 802.11b or 802.11g can connect to the 2.4 GHz wireless networks of the AP. - **11b/g/n**: The AP works in 802.11b/g/n mode. Wireless devices compliant with 802.11b or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n can connect to the 2.4 GHz wireless networks of the AP. - **11a**: The AP works in 802.11a mode and only wireless devices compliant with 802.11a can connect to the 5 GHz wireless networks of the AP. - **11ac:** The AP works in 802.11ac mode and only wireless devices compliant with 802.11ac can connect to the 5 GHz wireless networks of the AP. - **11a/n**: The AP works in 802.11a/n mode and only wireless devices compliant with 802.11a or 802.11n can connect to the 5 GHz wireless networks of the AP.
Channel	It specifies the operating channel of the AP. This parameter can be set if **Lock Channel** is not selected. **Auto**: It indicates that the AP automatically adjusts its operating channel according to the ambient environment.
Channel Bandwidth	It specifies the wireless channel bandwidth of the AP. This parameter can be set if the AP works in 802.11 b/g/n, 802.11ac, 802.11a/n mode and **Lock Channel** is not selected. - **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**: It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment. - **80 MHz**: It indicates that the AP can use only 80 MHz channel bandwidth.
Lock Channel	It is used to lock the channel settings of the AP. If this parameter is selected, channel settings including **Country/Region**, **Network Mode**, **Channel**, **Channel Bandwidth**, and **Expansion Channel** cannot be changed.
Transmit Power	It specifies the transmit power of the AP. A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the wireless network performance and security.
Lock Power	It specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.

Parameter	Description
Preamble	A preamble is a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. By default, the **Long Preamble** option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the **Short Preamble** option.
Short GI	Short Guard Interval. There is a delay on the receiving side due to multipath and other factors during the wireless signal transmission in space. If the subsequent data block is transmitted too quickly, it will interfere with the previous data block, and the short guard interval can be used to circumvent this interference. Short GI helps to increase the wireless throughput by 10%.
Isolate SSID	With the function enabled, the wireless clients connected to the AP with different SSID cannot communicate with each other. This improves wireless network security.

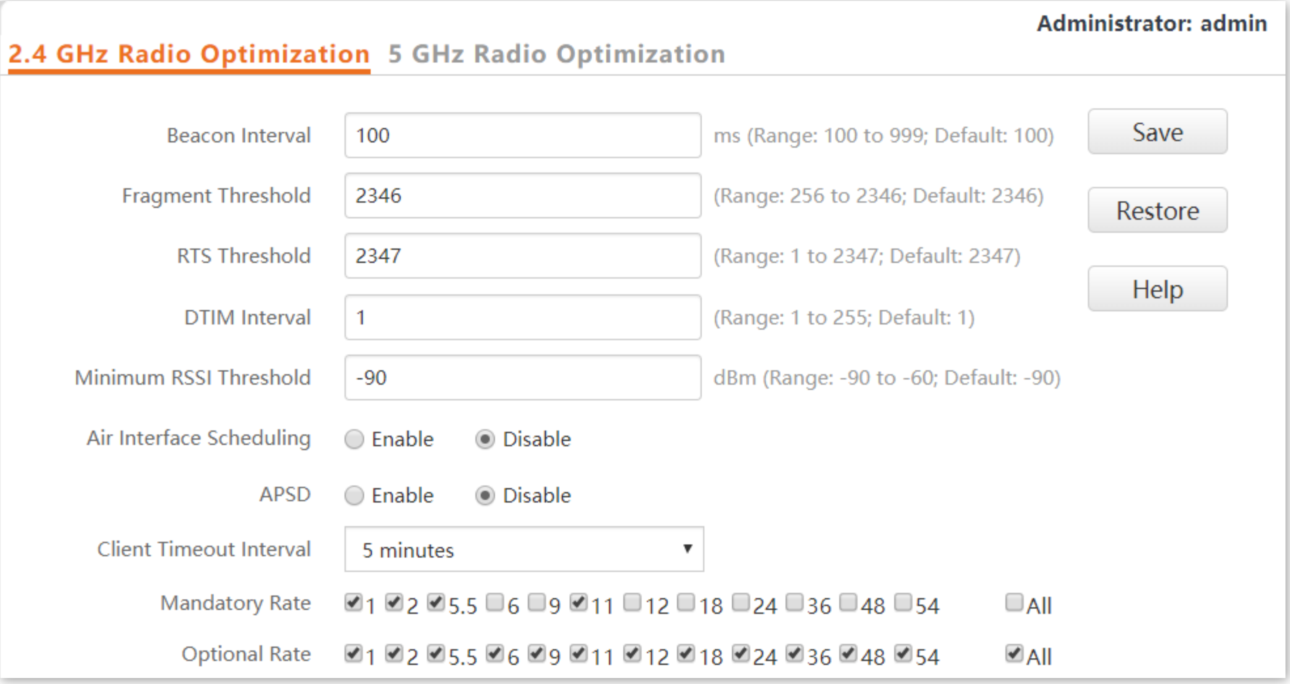
6.3 Radio Optimization

To access the page, choose **Wireless Setting** > **Radio Optimization**.

This page enables you to modify the radio parameters to optimize performance.

NOTE

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



Administrator: admin

2.4 GHz Radio Optimization   5 GHz Radio Optimization

Beacon Interval: 100 ms (Range: 100 to 999; Default: 100)

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

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

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

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

Air Interface Scheduling: ○ Enable ● Disable

APSD: ○ Enable ● Disable

Client Timeout Interval: 5 minutes ▾

Mandatory Rate: ☑1 ☑2 ☑5.5 □6 □9 ☑11 □12 □18 □24 □36 □48 □54 □All

Optional Rate: ☑1 ☑2 ☑5.5 ☑6 ☑9 ☑11 ☑12 ☑18 ☑24 ☑36 ☑48 ☑54 ☑All

Parameter description

Parameter	Description
Beacon Interval	Used to set the interval at which this device sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.
Fragment Threshold	Threshold of a fragment. Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented. In case of a high error rate, you can reduce the threshold to enable this device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput.

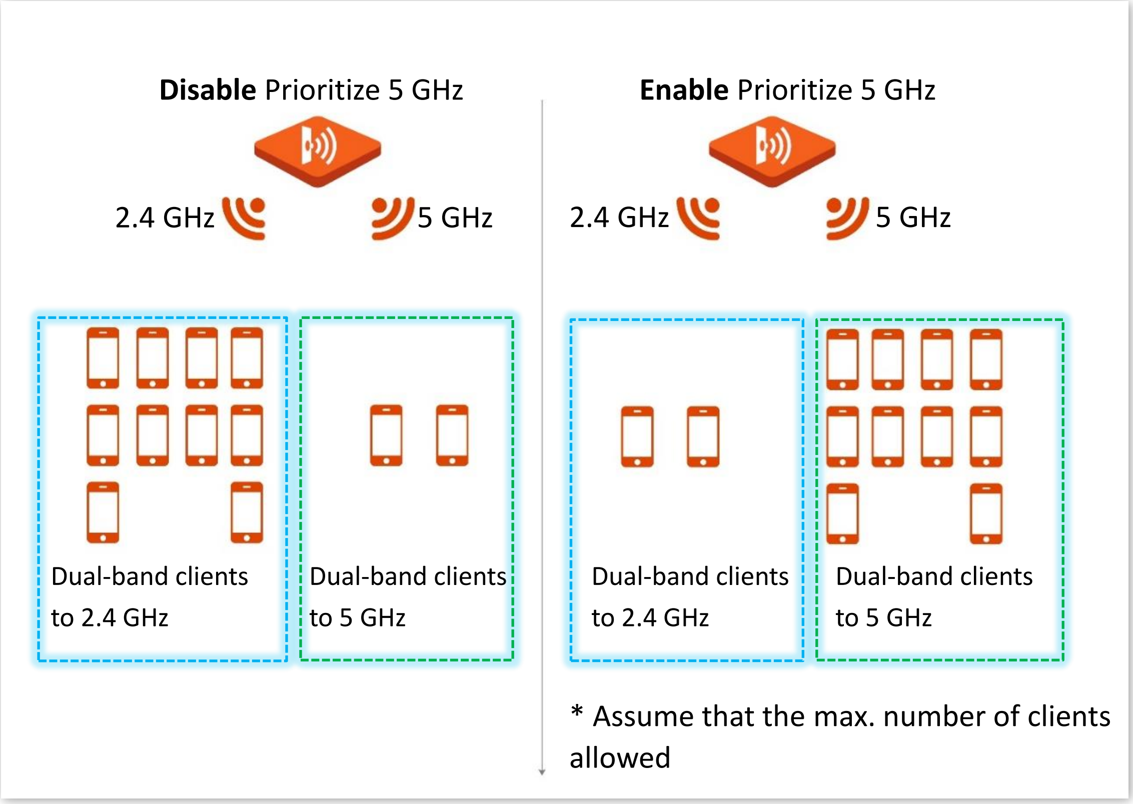
Parameter	Description
RTS Threshold	Frame length threshold for triggering the RTS/CTS mechanism. The unit is byte. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold to reduce conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	Countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval. For example, if **DTIM Interval** is set to **1**, this device transmits all cached frames at one Beacon interval.
Minimum RSSI Threshold	Minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device. A proper value facilitates wireless devices to connect to the AP with stronger signal in case of multiple APs exist.
Prioritize 5 GHz	It specifies that dual band wireless devices prefer the 5 GHz WiFi network of the AP to connect.
5 GHz Threshold	With this function enabled, if the strength of the signals transmitted by a wireless device is stronger than this threshold, the wireless device connects to the 5 GHz WiFi network. Otherwise, it connects to the 2.4 GHz WiFi network.
Air Interface Scheduling	Used to enable or disable the air interface scheduling function of the AP. This enables the users experiencing high download rates to download more data, so that this device can achieve higher system throughput and connect to a greater number of clients.
APSD	Automatic Power Save Delivery.If it is enabled, the power consumption of this device is reduced after a specified period during which no traffic is transmitted or received. By default, it is disabled.
Client Timeout Interval	Used to set the wireless client disconnection interval of this device. The device disconnects from a wireless client if no traffic is transmitted or received by the wireless client within the interval.
Mandatory Rate	It specifies rates that wireless clients must support in order to connect to the wireless networks of this device.
Optional Rate	It specifies the additional rates that the AP supports, which are optional to wireless clients.

Prioritize 5 GHz

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

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

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


Disable Prioritize 5 GHz
2.4 GHz
5 GHz
Dual-band clients to 2.4 GHz
Dual-band clients to 5 GHz
Enable Prioritize 5 GHz
2.4 GHz
5 GHz
Dual-band clients to 2.4 GHz
Dual-band clients to 5 GHz
* Assume that the max. number of clients allowed

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 WMM Settings

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

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

WMM involves the following terms:

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

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

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

EDCA Parameters

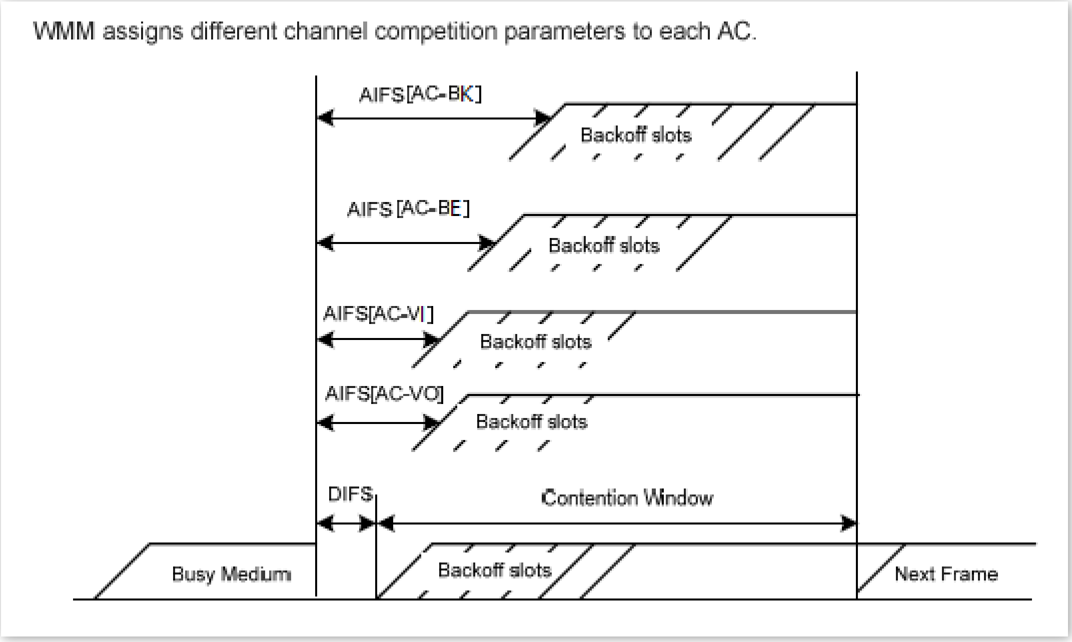
WMM changes the contention mechanism of 802.11 networks by dividing packets into four ACs, among which the ACs with higher priorities have more opportunities to access channels. The ACs help achieve different service levels.

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

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

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

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



WMM assigns different channel competition parameters to each AC.

ACK Policies

WMM specifies the Normal ACK and No ACK policies.

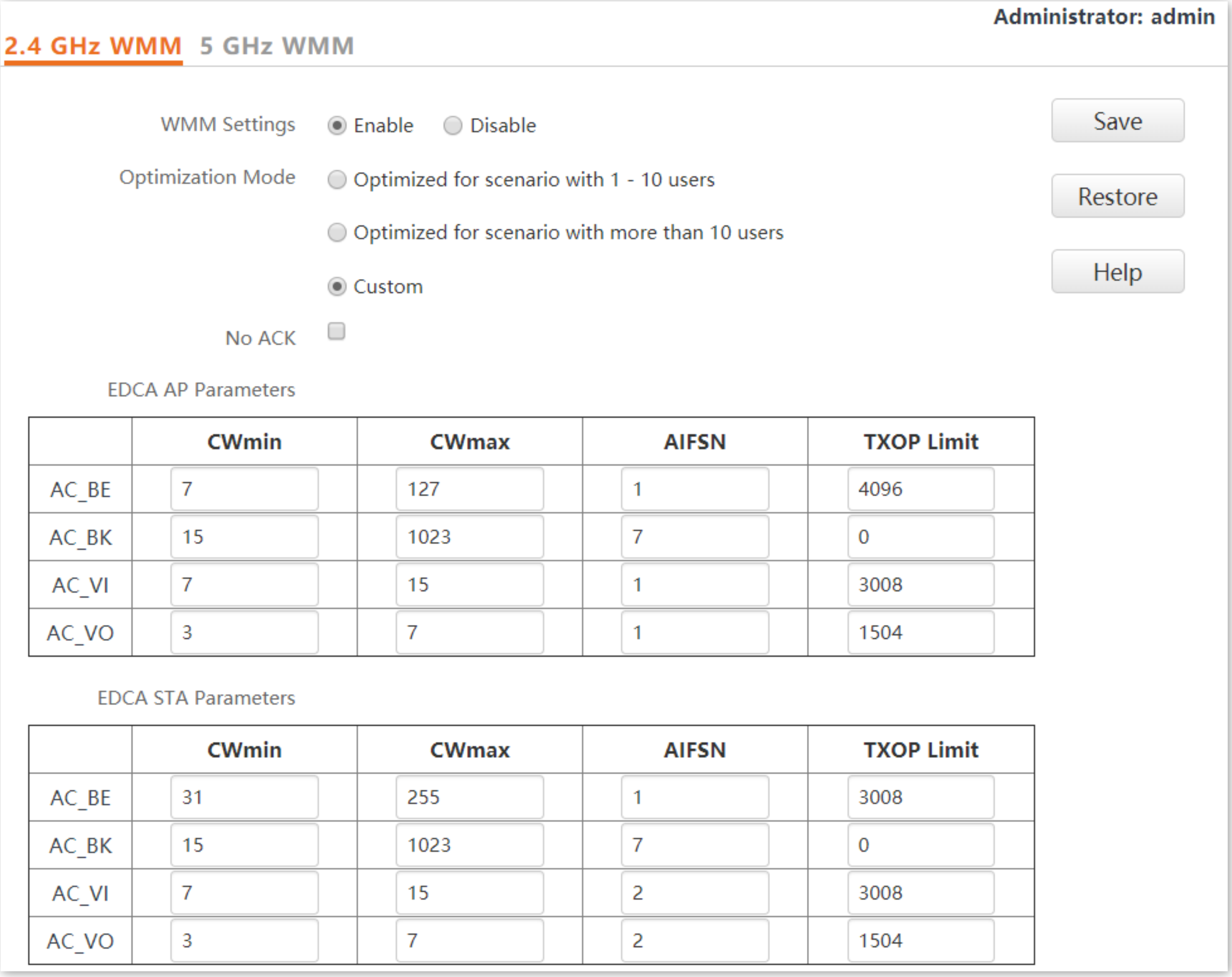
- According to the No ACK policy, no ACK packet is used during wireless packet transmission to acknowledge packet reception. This policy is applicable to scenarios where interference is mild and can effectively improve transmission efficiency. In case of strong interference, lost packets will not be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

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

Configure the WMM function

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

This page enables you to configure related WMM parameters.



WMM Settings ● Enable ○ Disable

Optimization Mode ○ Optimized for scenario with 1 - 10 users

○ Optimized for scenario with more than 10 users

● Custom

No ACK □

EDCA AP Parameters

	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	7	127	1	4096
AC_BK	15	1023	7	0
AC_VI	7	15	1	3008
AC_VO	3	7	1	1504

EDCA STA Parameters

	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	31	255	1	3008
AC_BK	15	1023	7	0
AC_VI	7	15	2	3008
AC_VO	3	7	2	1504

Parameter description

Parameter	Description
WMM Settings	• **Enable**: It specifies that the WMM function is enabled. • **Disable**: It specifies that the WMM function is disabled.

Parameter	Description
Optimization Mode	It specifies the WMM optimization modes supported by the AP: - **Optimized For scenario with 1 - 10 users**: If 10 or less clients are connected to the AP, you are recommended to select this mode to obtain higher client throughput. - **Optimized For scenario with more than 10 users**: If more than 10 clients are connected to the AP, you are recommended to select this mode to ensure client connectivity. - **Custom**: This mode enables you to set the WMM EDCA parameters for manual optimization.
No ACK	If the check box is selected, the No ACK policy is adopted. If the check box is deselected, the Normal ACK policy is adopted.
EDCA Parameters	For details, refer to section 6.4 WMM Settings.

6.5 Access Control

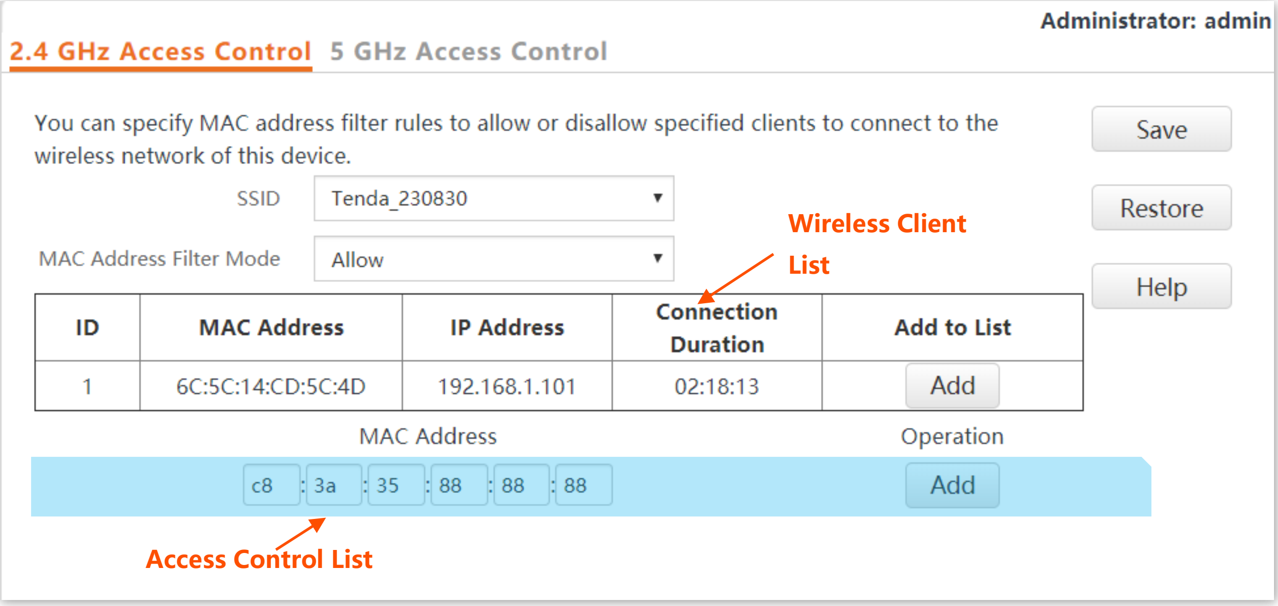
6.5.1 Overview

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

The AP supports the following 2 filter modes:

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

Access Control is disabled by default. The following figure displays the page when Access Control is enabled (**Allow** is taken as an example).



You can specify MAC address filter rules to allow or disallow specified clients to connect to the wireless network of this device.

SSID: Tenda_230830

MAC Address Filter Mode: Allow

ID	MAC Address	IP Address	Connection Duration	Add to List
1	6C:5C:14:CD:5C:4D	192.168.1.101	02:18:13	Add

MAC Address	Operation
c8 : 3a : 35 : 88 : 88 : 88	Add

Parameter description

Parameter	Description
SSID	It specifies the wireless network to which the rule applies.

Parameter	Description
MAC Filter Mode	It specifies the filter mode of the rule. • **Disable**: It indicates that the access control function is disabled. • **Allow**: It indicates that only the wireless clients on the wireless access control list can connect to the AP with the selected SSID. • **Disallow**: It indicates that only the wireless clients on the wireless access control list cannot connect to the AP with the selected SSID.

6.5.2 Configure Access Control

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

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

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

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

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

Step 6 Click **Add**.

TIP

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

Step 7 Click **Save**.

---End

6.5.3 Example of Configuring Access Control

Networking requirement

A wireless network whose SSID is **Tenda_230838_5G** under the 5 GHz radio band has been set up in a company. Only a few members are allowed to connect to the wireless network.

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

Configuration procedure

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

Step 2 Select **Tenda_230838_5G** from the **SSID** drop-down list.

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

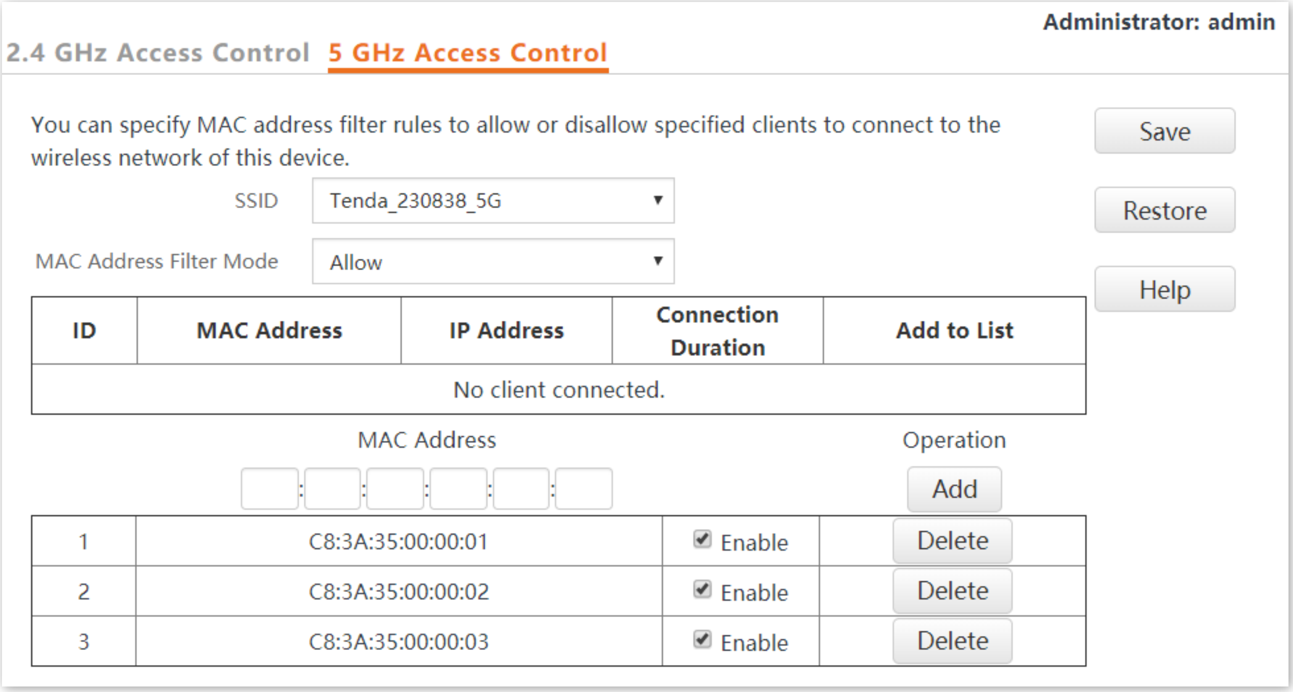
Step 4 Enter **C8:3A:35:00:00:01** in the **MAC Address** text box and click **Add**.

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

Step 6 Click **Save**.

---End

The following figure shows the configuration.



Administrator: admin

2.4 GHz Access Control 5 GHz Access Control

You can specify MAC address filter rules to allow or disallow specified clients to connect to the wireless network of this device.

SSID: Tenda_230838_5G

MAC Address Filter Mode: Allow

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

MAC Address: □:□:□:□:□:□ Operation: Add

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

Verification

Only the specified wireless devices can connect to the **Tenda_230838_5G** wireless network.

6.6 Advanced Settings

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

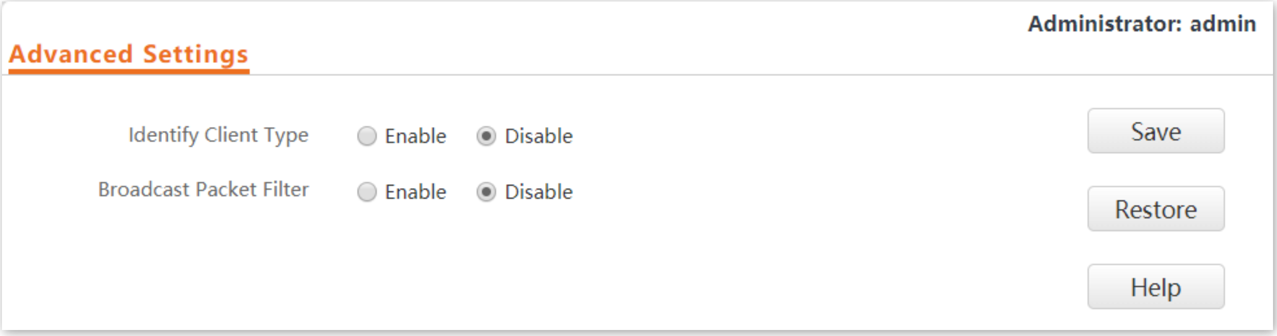
This page enables you to set the **Identify Client Type** and **Broadcast Packet Filter** of the AP.

Identify Client Type

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

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.



Administrator: admin

Advanced Settings

Identify Client Type ○ Enable ● Disable

Broadcast Packet Filter ○ Enable ● Disable

Parameter description

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

6.7 QVLAN Settings

6.7.1 Overview

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

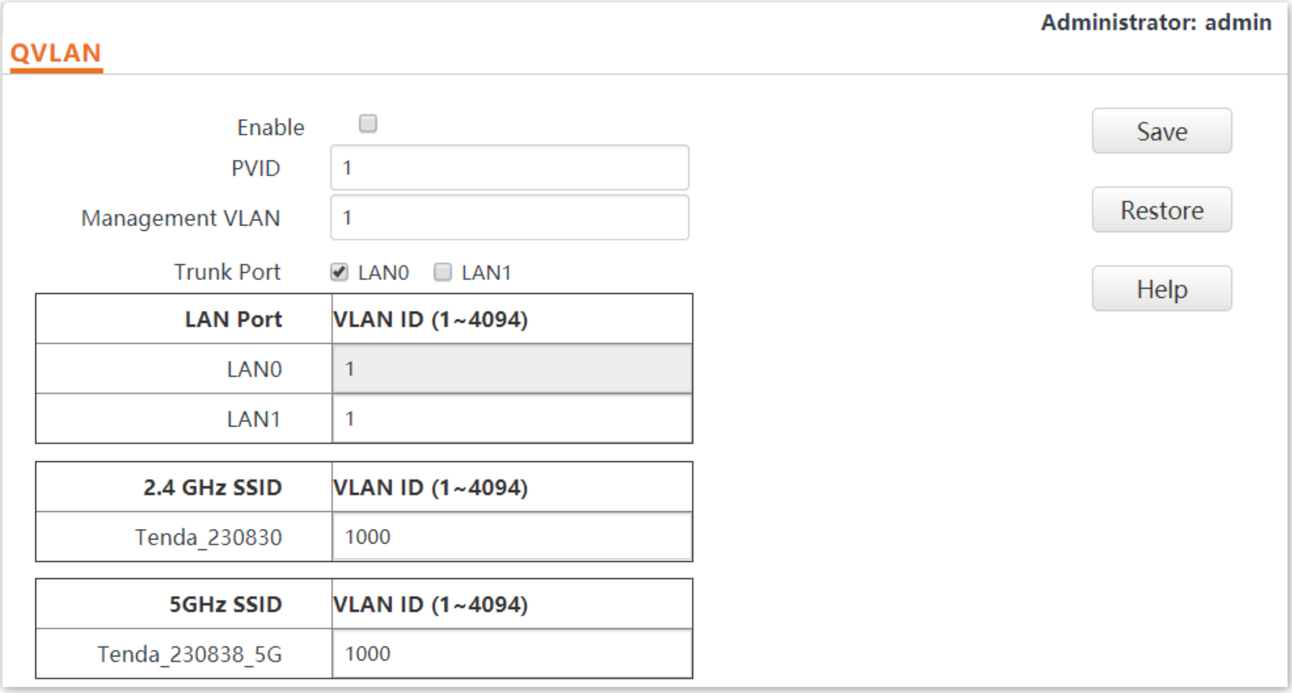
If the QVLAN function is enabled, tagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the VID in the data, whereas untagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the PVID of the port that receives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

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

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

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

This page enables you to set VLAN IDs of all wireless networks.



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

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

2.4 GHz SSID	VLAN ID (1~4094)
Tenda_230830	1000

5GHz SSID	VLAN ID (1~4094)
Tenda_230838_5G	1000

Parameter description

Parameter	Description
Enable	It specifies whether to enable the QVLAN function of the AP. By default, it is disabled.
PVID	It specifies the ID of the default native VLAN of the trunk port of the AP. After the QVLAN function is enabled, the LAN port is the trunk port. Traffic of all VLANs can pass through a trunk port. Its default value is **1**.
Management VLAN	It specifies the ID of the AP management VLAN. The default value is **1**. After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
Trunk Port	It specifies the LAN port used as a trunk port of the AP. The default value is **LAN0**. Traffic of all VLANs can pass through a trunk port. NOTE If the QVLAN function is enabled, at least one LAN port needs to be set as a trunk port.

Parameter	Description
LAN Port	It specifies the LAN ports of the AP, including LAN0 and LAN1. LAN0 indicates the LAN port at the rear of the AP (PoE power supply, data transmission multiplexing port), whereas LAN1 indicates the LAN port (data transmission port) at the front of the AP TIP LAN ports not set as a trunk port can be seen as an access port. You can set a VLAN ID for it.
2.4 GHz SSID	It specifies the currently enabled SSIDs of the AP at 2.4 GHz band.
5 GHz SSID	It specifies the currently enabled SSIDs of the AP at 5 GHz band.
VLAN ID	It specifies VLAN IDs corresponding to SSIDs. The default value is **1000**. After the QVLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID and VLAN ID of an access port are the same.

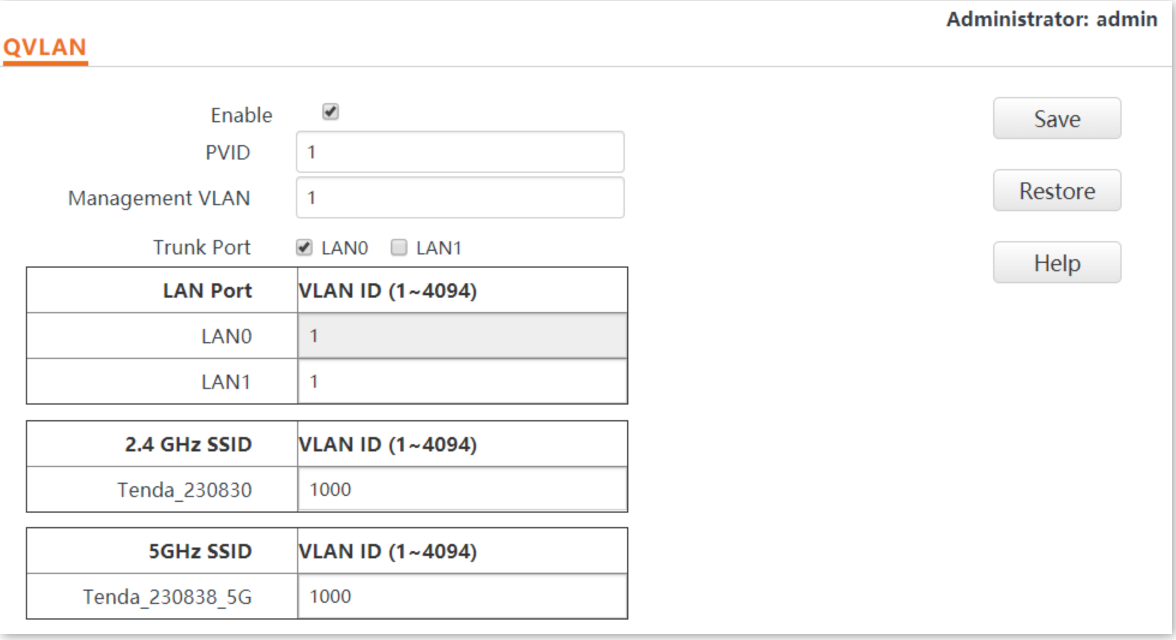
6.7.2 Configure the QVLAN Function

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

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

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

Step 4 Click **Save**.



Enable ☑

PVID 1

Management VLAN 1

Trunk Port ☑ LAN0 □ LAN1

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

2.4 GHz SSID	VLAN ID (1~4094)
Tenda_230830	1000

5GHz SSID	VLAN ID (1~4094)
Tenda_230838_5G	1000

---End

6.7.3 Example of Configuring QVLAN Settings

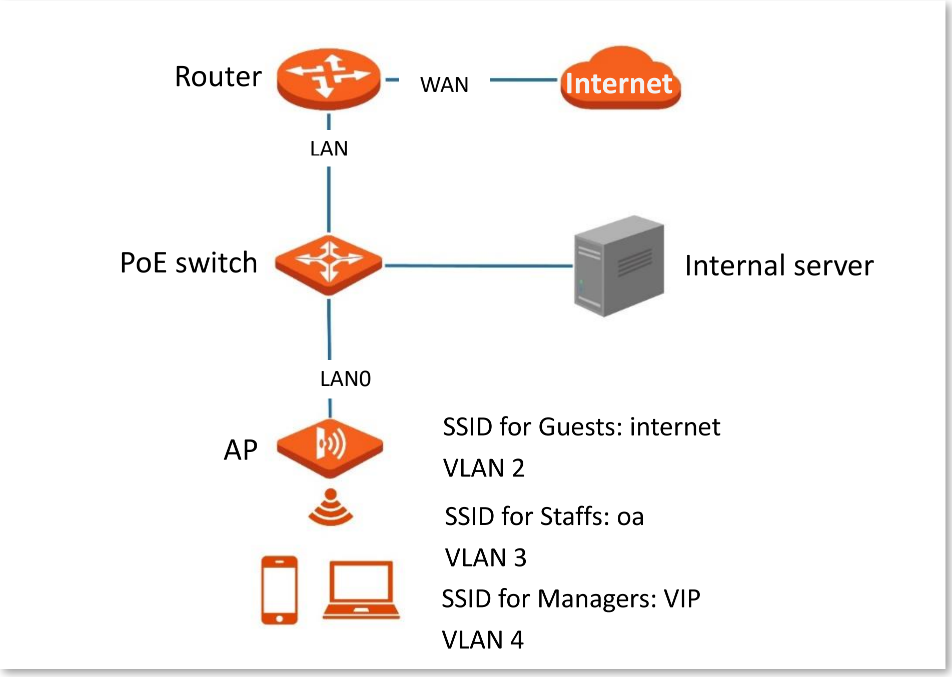
Networking requirement

A hotel has the following wireless network coverage requirements:

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

Networking assumption

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



Configuration procedure

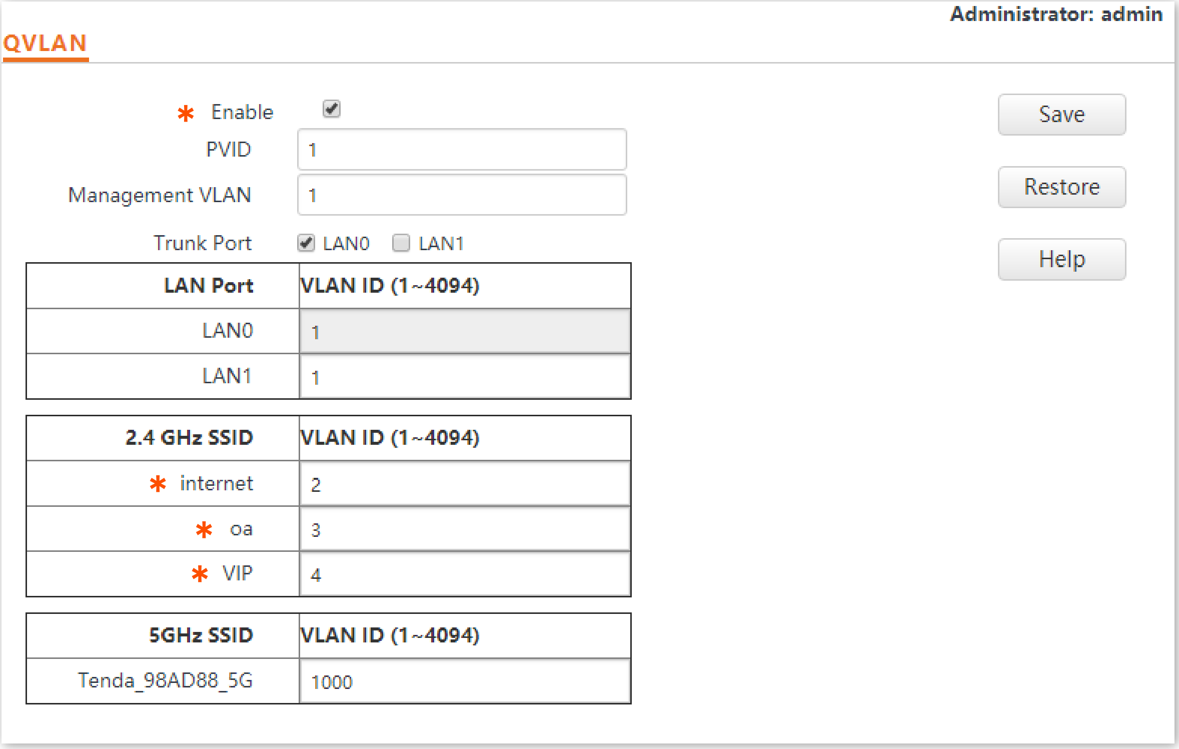
- **Configure the AP**

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

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

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

Step 4 Click **Save**.



* Enable ☑

PVID: 1

Management VLAN: 1

Trunk Port: ☑ LAN0 □ LAN1

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

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

5GHz SSID	VLAN ID (1~4094)
Tenda_98AD88_5G	1000

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

Wait for the automatic reboot of the AP.

■ Configure the switch

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

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

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

■ Configure the router and internal server

To ensure a normal internet access for wireless clients connected to the AP, the router and internal server must support the QVLAN function and need to be configured. See the following table.

Router:

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

Internal server:

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

For details, refer to the user guides for the corresponding devices.

---End

Verification

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

7 SNMP

7.1 Overview

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

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

SNMP Management Framework

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

- SNMP manager: It is a system that controls and monitors network nodes using the SNMP protocol. The SNMP manager most widely used in network environments is Network Management System (NMS). An NMS can be a dedicated network management server, or an application that implements management functions in a network device.

- SNMP agent: It is a software module in a managed device. The module is used to manage data about the device and report the management data to an SNMP manager.

- MIB: It is a collection of managed objects. It defines a series of attributes of managed objects, including names, access permissions, and data types of objects. Each SNMP agent has its MIB. An SNMP manager can read and/or write objects in the MIB based on the permissions assigned to the SNMP manager.

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

Basic SNMP Operations

The AP allows the following basic SNMP operations:

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

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

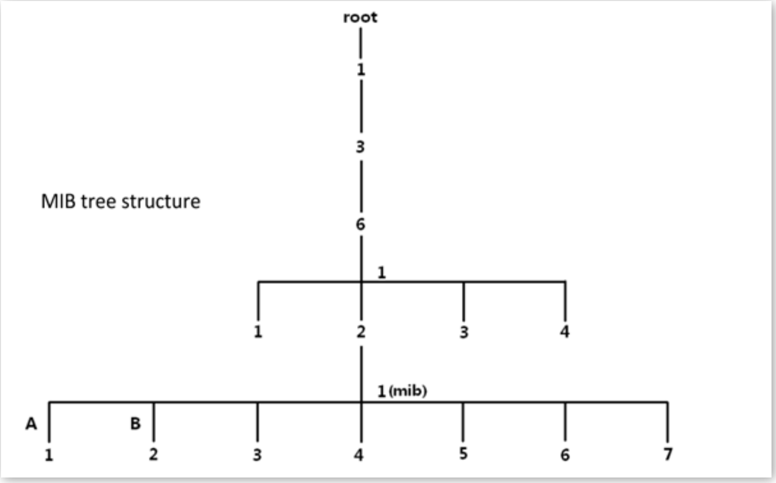
SNMP Protocol Version

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

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

MIB Introduction

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

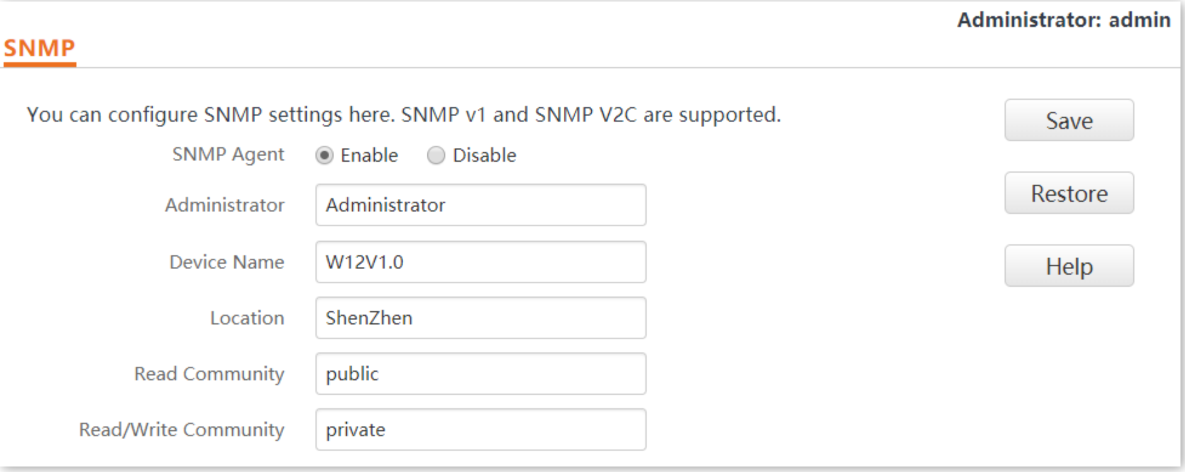


Configure the SNMP Function

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

Step 2 Set related SNMP parameters.

Step 3 Click **Save**.



You can configure SNMP settings here. SNMP v1 and SNMP V2C are supported.

SNMP Agent ● Enable ○ Disable

Administrator: Administrator

Device Name: W12V1.0

Location: ShenZhen

Read Community: public

Read/Write Community: private

---End

Parameter description

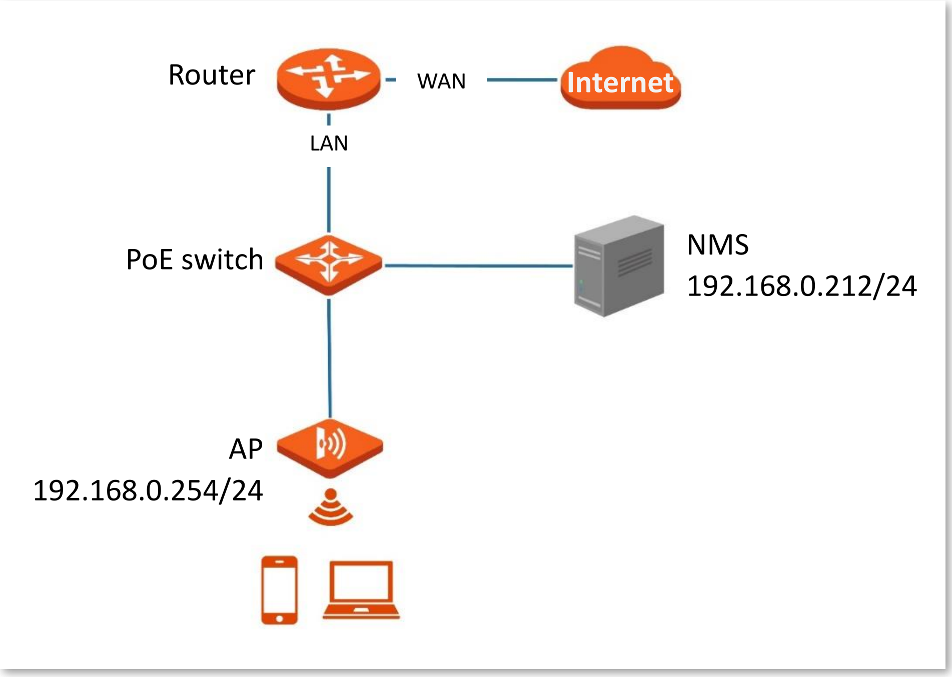
Parameter	Description
SNMP Agent	It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled. An SNMP manager and the SNMP agent can communicate with each other only if their SNMP versions are the same. Currently, the SNMP agent function of the AP supports SNMP V1 and SNMP V2C.
Administrator	It specifies the name of the administrator of the AP. The default name is **Administrator**. You can change the name as required.
Device Name	It specifies the device name of the AP. The default device name is the model of the AP. TIP It is recommended that you change the AP name so that you can easily identify the AP when managing the AP using SNMP.
Location	It specifies the location where the AP is used. The default location is **ShenZhen**. You can change the location as required.
Read Community	It specifies the read password shared between SNMP managers and this SNMP agent. The default password is **public**. The SNMP agent function of the AP allows an SNMP manager to use the password to read variables in the MIB of the AP.

Parameter	Description
Read/Write Community	It specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is **private**. The SNMP agent function of the AP allows an SNMP manager to use the password to read/write variables in the MIB of the AP.

7.2 Example of Configuring the SNMP Function

Networking requirement

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



Configuration procedure

Configure the AP

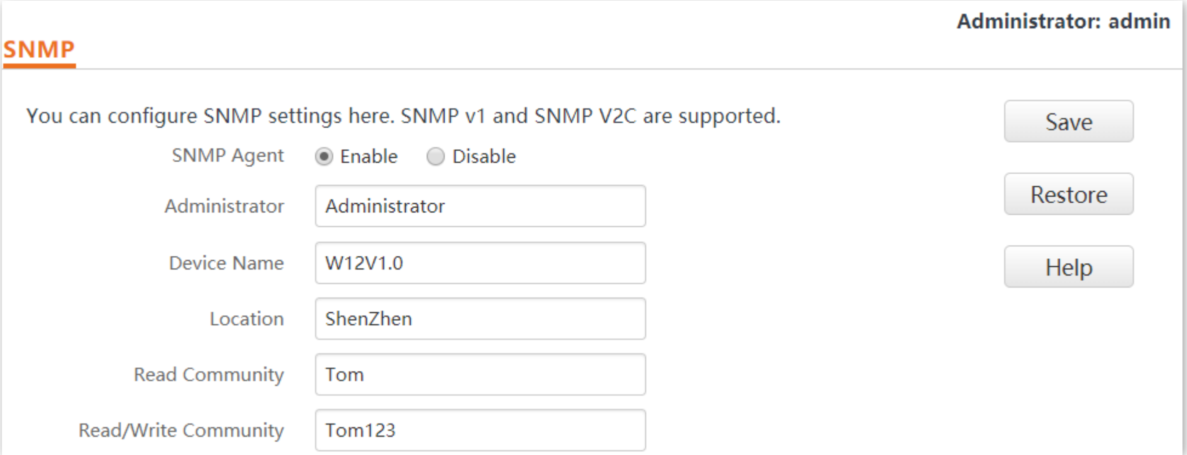
Assume that the administrator name is **Tom**, read community is **Tom**, and read/write community is **Tom123**.

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

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

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

Step 4 Click **Save**.


Administrator: admin

SNMP

You can configure SNMP settings here. SNMP v1 and SNMP V2C are supported.

SNMP Agent	● Enable ○ Disable
Administrator	Administrator
Device Name	W12V1.0
Location	ShenZhen
Read Community	Tom
Read/Write Community	Tom123

- **Configure the NMS**

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

---End

Verification

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

8 Tools

8.1 Firmware Upgrade

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

NOTE

To ensure a correct upgrade and avoid damage, please:

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

Configuration procedure:

Step 1 Download the package of a later 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.

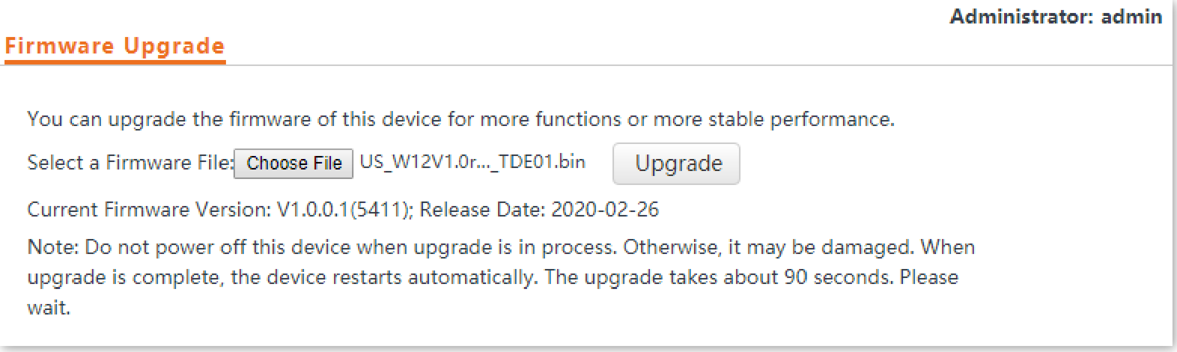
Step 2 Log in to the web UI of the AP and choose **Tools** > **Firmware Upgrade**.

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

TIP

File uploading button of different web browsers may differ. The actual web browser shall prevail. IE Explorer is taken as an example here.

Step 4 Click **Upgrade**.



Administrator: admin

Firmware Upgrade

You can upgrade the firmware of this device for more functions or more stable performance.

Select a Firmware File: Choose File US_W12V1.0r..._TDE01.bin Upgrade

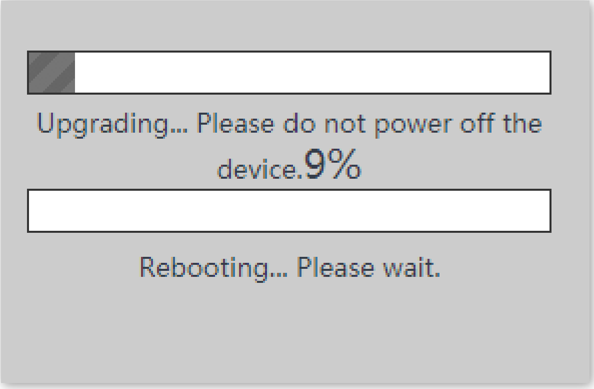
Current Firmware Version: V1.0.0.1(5411); Release Date: 2020-02-26

Note: Do not power off this device when upgrade is in process. Otherwise, it may be damaged. When upgrade is complete, the device restarts automatically. The upgrade takes about 90 seconds. Please wait.

Step 5 Click **OK**.

---End

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



Upgrading... Please do not power off the device.9%

Rebooting... Please wait.

TIP

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

8.2 Date & Time

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

8.2.1 System Time

Ensure that the system time of the AP is correct, so that time-based functions can take effect properly.

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

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

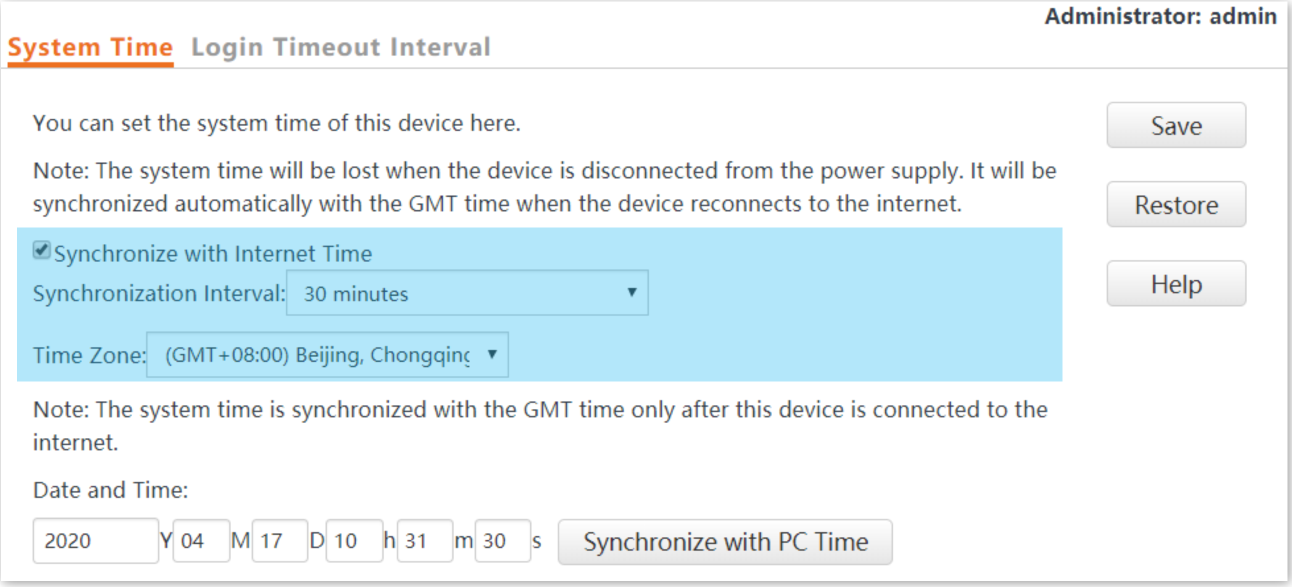
TIP

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

Synchronize with Internet Time

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

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



You can set the system time of this device here.

Note: The system time will be lost when the device is disconnected from the power supply. It will be synchronized automatically with the GMT time when the device reconnects to the internet.

☑ Synchronize with Internet Time

Synchronization Interval: 30 minutes

Time Zone: (GMT+08:00) Beijing, Chongqinç

Note: The system time is synchronized with the GMT time only after this device is connected to the internet.

Date and Time:

2020 Y 04 M 17 D 10 h 31 m 30 s Synchronize with PC Time

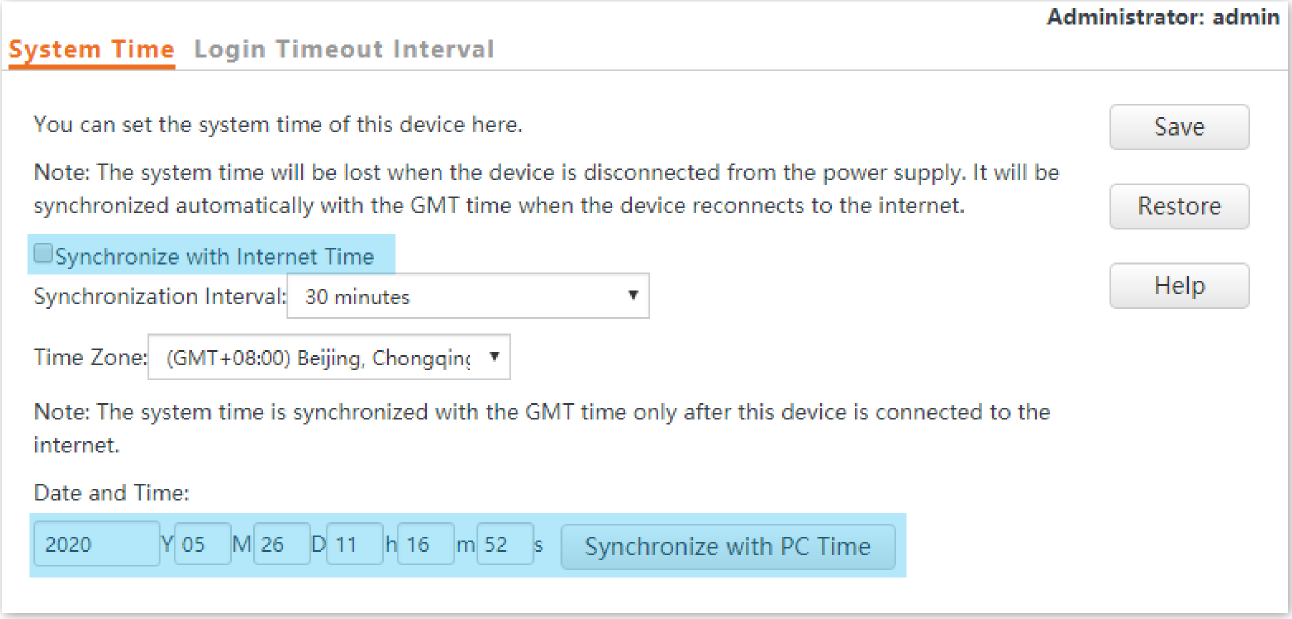
Parameter description

Parameter	Description
Synchronize with Internet Time	It specifies whether to enable synchronization with the internet time.
Synchronization Interval	It is valid only when **Synchronize with Internet Time** is enabled. It specifies the interval at which the AP will automatically synchronize with a time server of the internet.
Time Zone	It is valid only when **Synchronize with Internet Time** is enabled. It specifies the standard time zone of the region in which the AP locates.

Manually Set the Time

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

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



You can set the system time of this device here.

Note: The system time will be lost when the device is disconnected from the power supply. It will be synchronized automatically with the GMT time when the device reconnects to the internet.

□Synchronize with Internet Time

Synchronization Interval: 30 minutes

Time Zone: (GMT+08:00) Beijing, Chongqing

Note: The system time is synchronized with the GMT time only after this device is connected to the internet.

Date and Time:

2020 Y 05 M 26 D 11 h 16 m 52 s

8.2.2 Login Timeout Interval

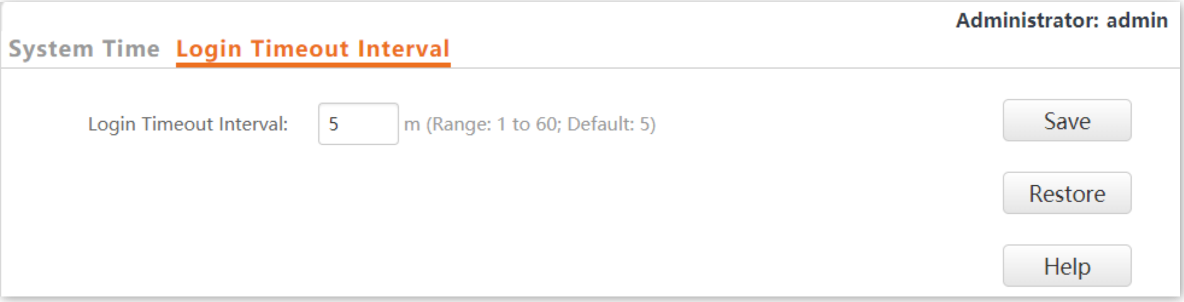
If you log in to the web UI of the AP and perform no operation within the login timeout interval, the AP logs you out for network security. The default login timeout interval is 5 minutes.

Procedure for setting the login timeout interval:

Step 1 Choose **Tools** > **Date & Time**, and click **Login Timeout Interval**.

Step 2 Change the login timeout interval as required.

Step 3 Click **Save**.



Administrator: admin

System Time Login Timeout Interval

Login Timeout Interval: 5 m (Range: 1 to 60; Default: 5)

---End

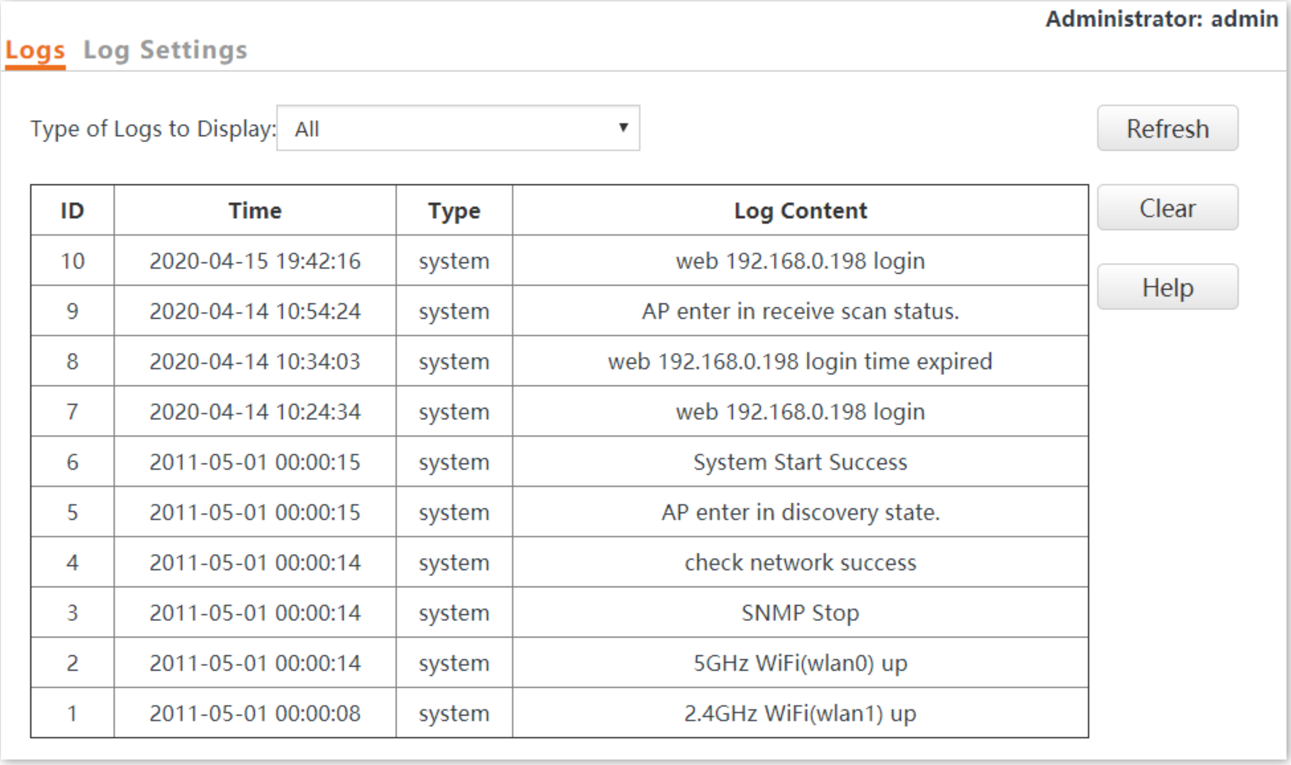
8.3 Logs

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

8.3.1 View Logs

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

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



Type of Logs to Display: All

ID	Time	Type	Log Content
10	2020-04-15 19:42:16	system	web 192.168.0.198 login
9	2020-04-14 10:54:24	system	AP enter in receive scan status.
8	2020-04-14 10:34:03	system	web 192.168.0.198 login time expired
7	2020-04-14 10:24:34	system	web 192.168.0.198 login
6	2011-05-01 00:00:15	system	System Start Success
5	2011-05-01 00:00:15	system	AP enter in discovery state.
4	2011-05-01 00:00:14	system	check network success
3	2011-05-01 00:00:14	system	SNMP Stop
2	2011-05-01 00:00:14	system	5GHz WiFi(wlan0) up
1	2011-05-01 00:00:08	system	2.4GHz WiFi(wlan1) up

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

By default, the latest 150 logs are saved. To view the latest logs of the AP, click **Refresh**. To clear the existing logs of the AP, click **Clear**.

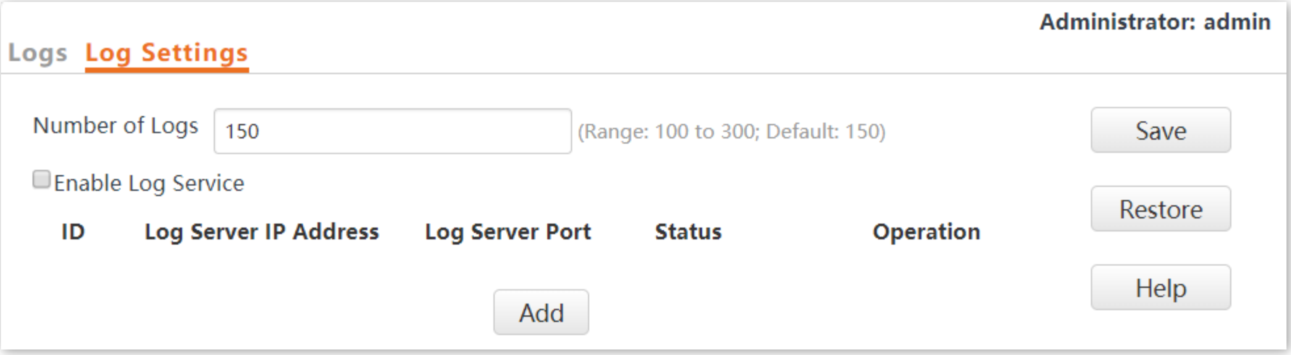
NOTE

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

8.3.2 Configure Log Settings

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

This page enables you to set the number of logs to be displayed and configure log servers.



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

□ Enable Log Service

ID	Log Server IP Address	Log Server Port	Status	Operation

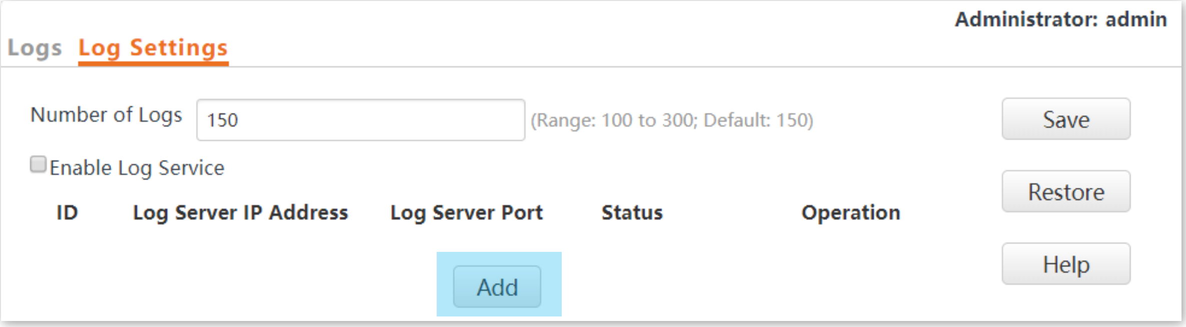
Parameter description

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

Procedure for adding a log server

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

Step 2 Click **Add**.



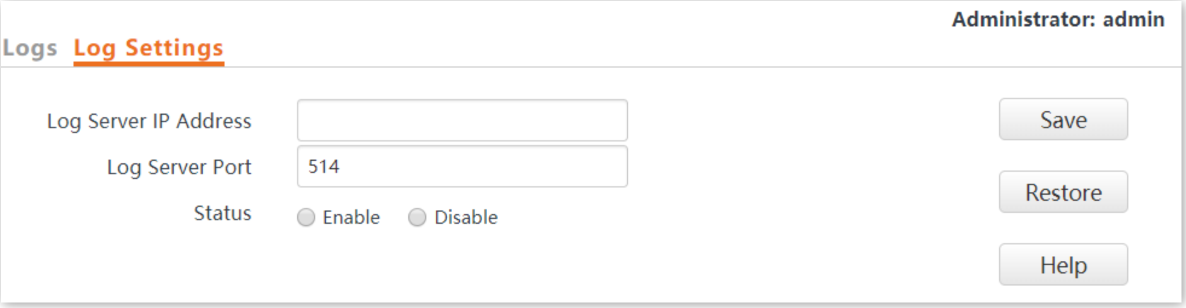
Number of Logs 150 (Range: 100 to 300; Default: 150)

□ Enable Log Service

ID	Log Server IP Address	Log Server Port	Status	Operation

Step 3 Set parameters as follows, and click Save.

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



Log Server IP Address

Log Server Port 514

Status ○ Enable ○ Disable

Step 4 Check **Enable Log Service**.

Step 5 Click **Save**.

---End

8.4 Configuration

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

8.4.1 Back Up and Restore Configurations

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

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

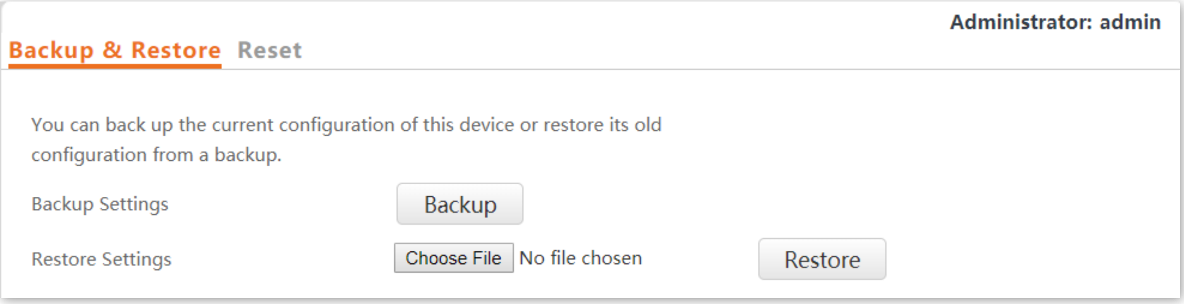
TIP

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

Back Up the Current Configuration

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

Step 2 Click **Backup**.

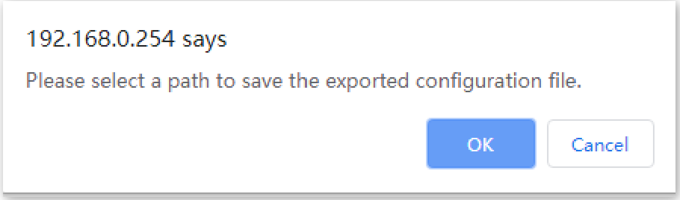


You can back up the current configuration of this device or restore its old configuration from a backup.

Backup Settings Backup

Restore Settings Choose File No file chosen Restore

Step 3 Click **OK**.



192.168.0.254 says

Please select a path to save the exported configuration file.

---End

A configuration file named **APCfm.cfg** is downloaded.

TIP

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

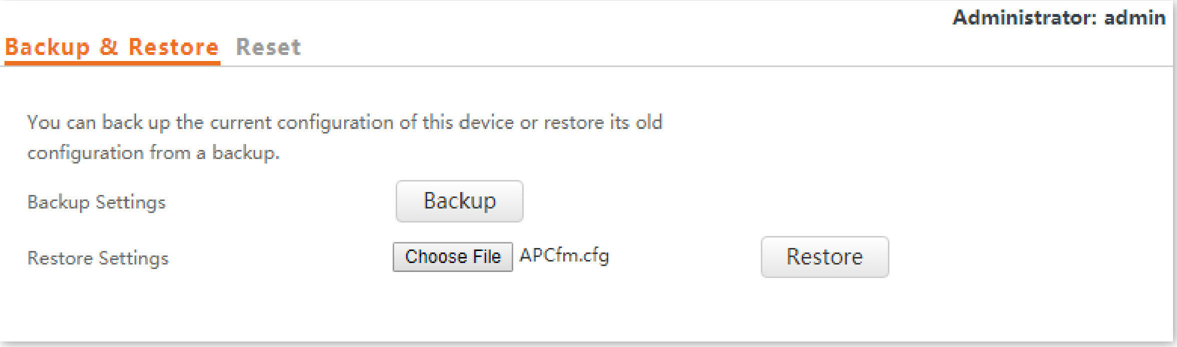
Step 1 Choose **Tools** > **Configuration** > **Backup & Restore**.

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

TIP

File uploading button of different web browsers may differ. The actual web browser shall prevail. IE Explorer is taken as an example here.

Step 3 Click **Restore**.



You can back up the current configuration of this device or restore its old configuration from a backup.

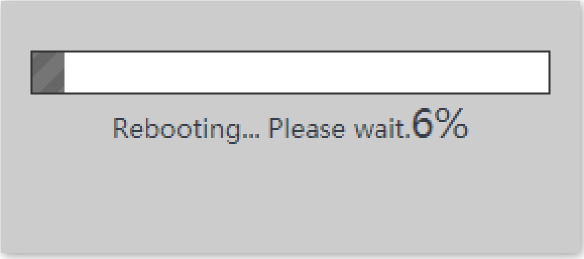
Backup Settings

Restore Settings

Step 4 Click **OK**.

---End

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



Rebooting... Please wait.6%

8.4.2 Restore the Factory Settings

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

NOTE

- When the factory settings are restored, your configuration is lost. Therefore, you need to reconfigure the AP to reconnect to the internet. Restore the factory settings of the AP only when necessary.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.
- After the factory settings are restored, the login IP address of the AP is changed to **192.168.0.254**, and the user name and password of the AP are changed to **admin**.

Method 1:

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

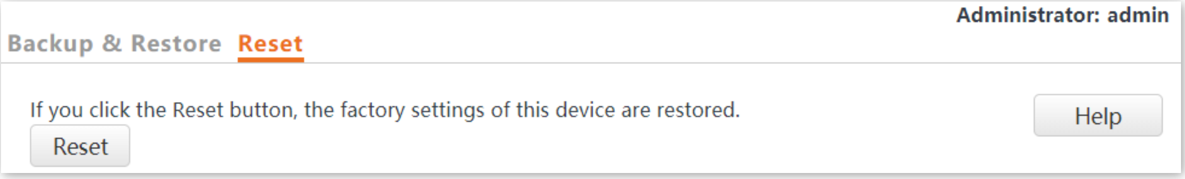
Procedure: When the **SYS** LED indicator blinks green, uncover the AP, use a pin to press the reset button (RST) for 8 seconds and release it until the green LED indicator turns solid on.

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

Method 2:

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

Step 2 Click the **Reset** button.



Administrator: admin

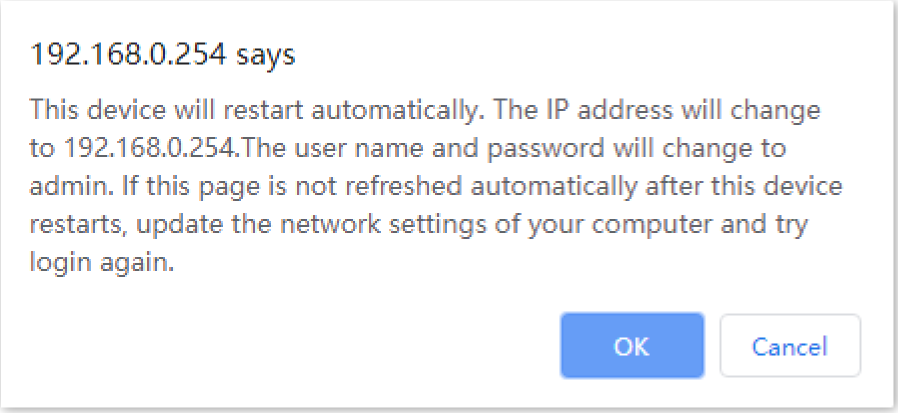
Backup & Restore Reset

If you click the Reset button, the factory settings of this device are restored.

Reset

Help

Step 3 Click **OK**.



192.168.0.254 says

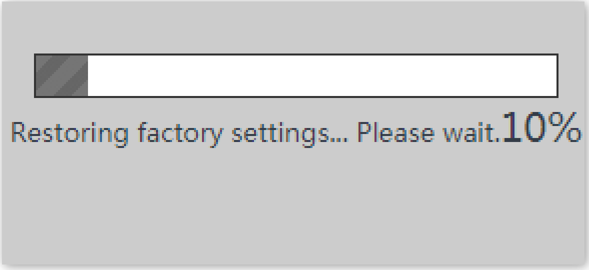
This device will restart automatically. The IP address will change to 192.168.0.254.The user name and password will change to admin. If this page is not refreshed automatically after this device restarts, update the network settings of your computer and try login again.

OK

Cancel

---End

Wait until the progress bar is done.

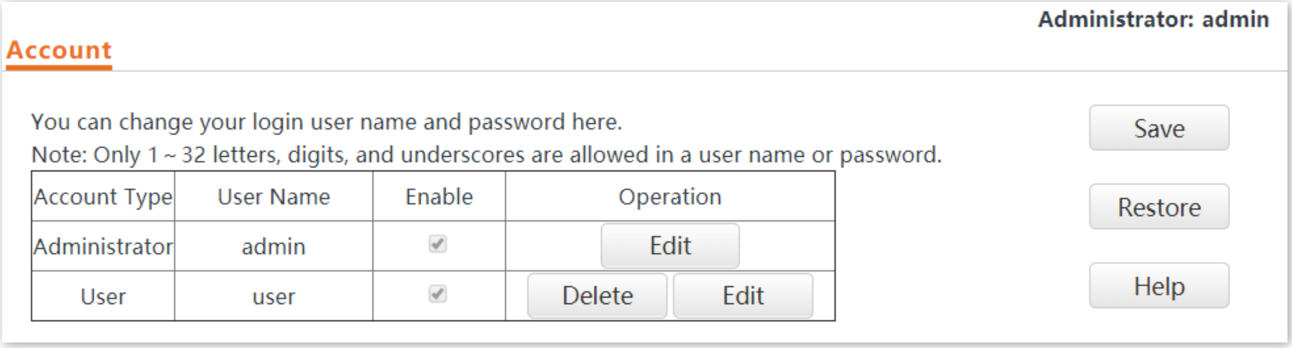


Restoring factory settings... Please wait.10%

8.5 Account

To access page for changing user names and passwords, choose **Tools** > **Account**.

This page enables you to change the login account information of the AP to prevent unauthorized login.



You can change your login user name and password here.
Note: Only 1 ~ 32 letters, digits, and underscores are allowed in a user name or password.

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

Parameter description

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

8.6 Diagnostics Tool

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

Procedure:

The link to **192.168.10.1** is used as an example.

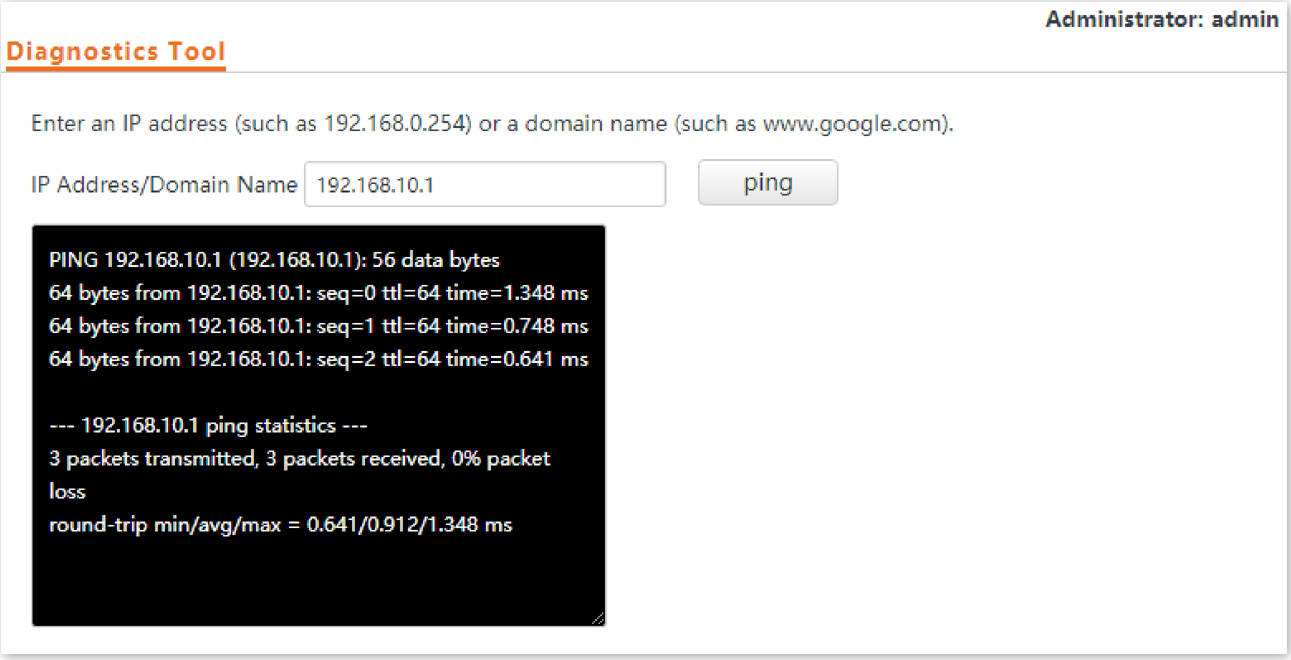
Step 1 Choose **Tools** > **Diagnostics Tool**.

Step 2 Enter the IP address or domain name to be pinged in the **IP Address/Domain Name** text box. In this example, enter **192.168.10.1**.

Step 3 Click **ping**.

---End

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



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

IP Address/Domain Name: 192.168.10.1

```
PING 192.168.10.1 (192.168.10.1): 56 data bytes
64 bytes from 192.168.10.1: seq=0 ttl=64 time=1.348 ms
64 bytes from 192.168.10.1: seq=1 ttl=64 time=0.748 ms
64 bytes from 192.168.10.1: seq=2 ttl=64 time=0.641 ms

--- 192.168.10.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet
loss
round-trip min/avg/max = 0.641/0.912/1.348 ms
```

8.7 Reboot Device

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

TIP

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

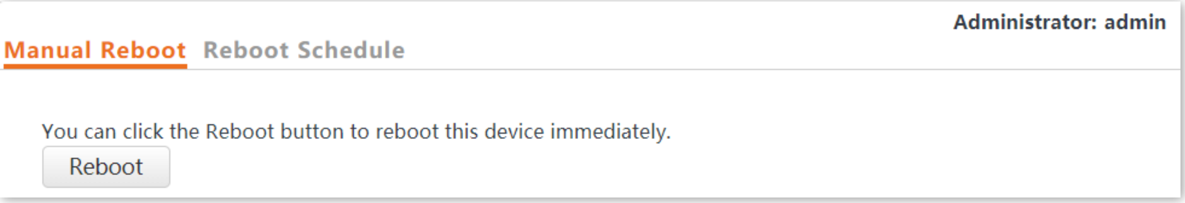
8.7.1 Manual Reboot

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

Procedure:

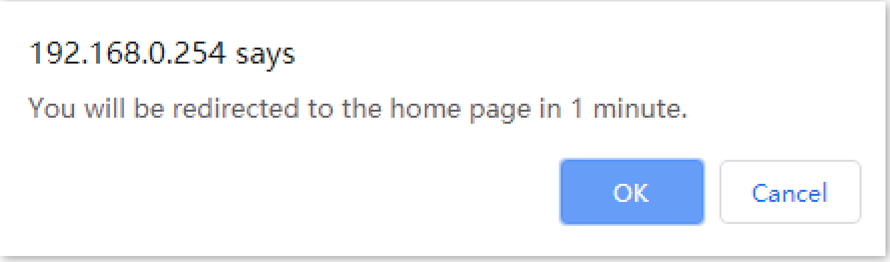
Step 1 To access the page, choose **Tools** > **Reboot Device** > **Manual Reboot**.

Step 2 Click **Reboot**.



You can click the Reboot button to reboot this device immediately.

Step 3 Click **OK**.

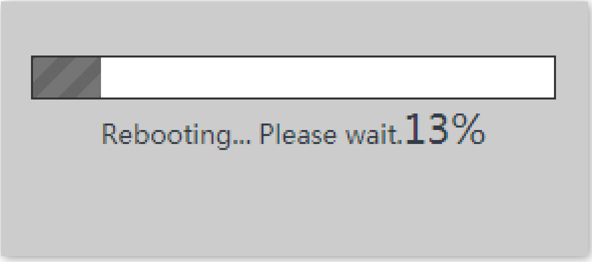


192.168.0.254 says

You will be redirected to the home page in 1 minute.

---End

Wait until the progress bar is done.



Rebooting... Please wait.13%

8.7.2 Reboot Schedule

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

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

Configure the AP to Reboot at Intervals

TIP

Rebooting at intervals is based on the system time. To avoid reboot time error, ensure that the system time is correct.

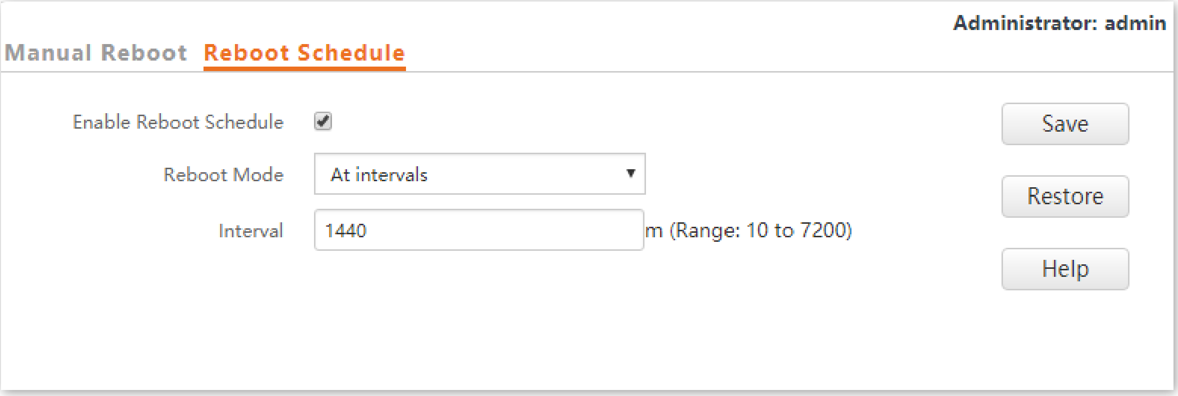
Step 1 Choose **Tools** > **Reboot Device** and click the **Reboot Schedule** tab.

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

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

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

Step 5 Click **Save**.



Enable Reboot Schedule ☑

Reboot Mode: At intervals

Interval: 1440 m (Range: 10 to 7200)

---End

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

Configure the AP to Reboot at Specified Time

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

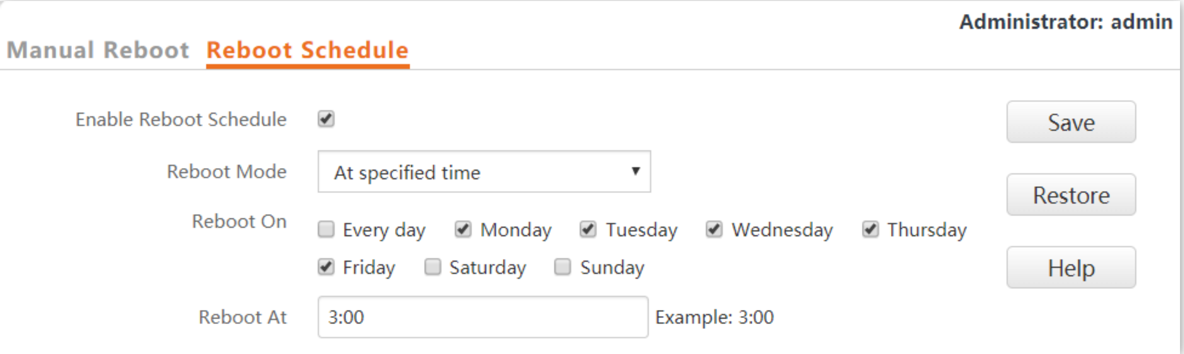
Step 2 Select the **Enable Reboot Schedule** check box.

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

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

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

Step 6 Click **Save**.



Enable Reboot Schedule ☑

Reboot Mode: At specified time ▾

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

Reboot At: 3:00 Example: 3:00

---End

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

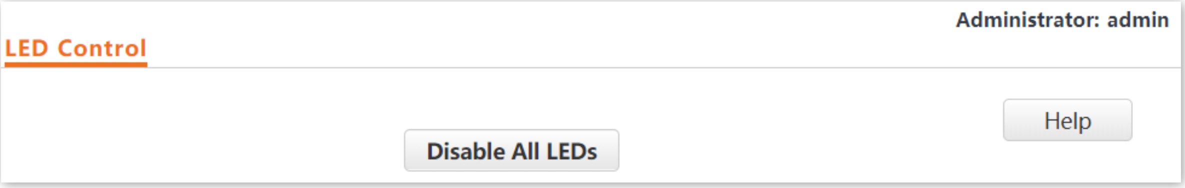
8.8 LED Control

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

Procedure for turning off the LED indicator:

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

Step 2 Click **Disable All LEDs**.



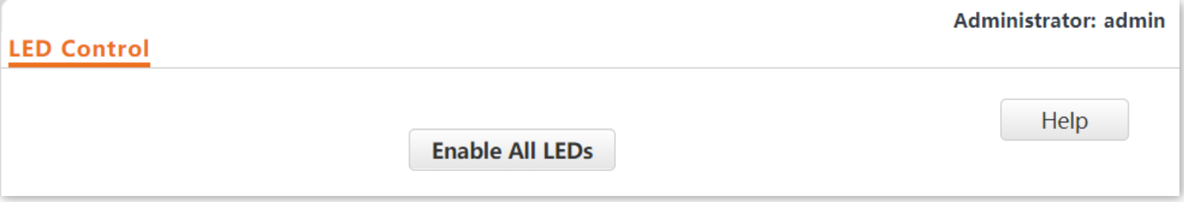
---End

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

Procedure for turning on the LED indicator:

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

Step 2 Click **Enable All LEDs**.



---End

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

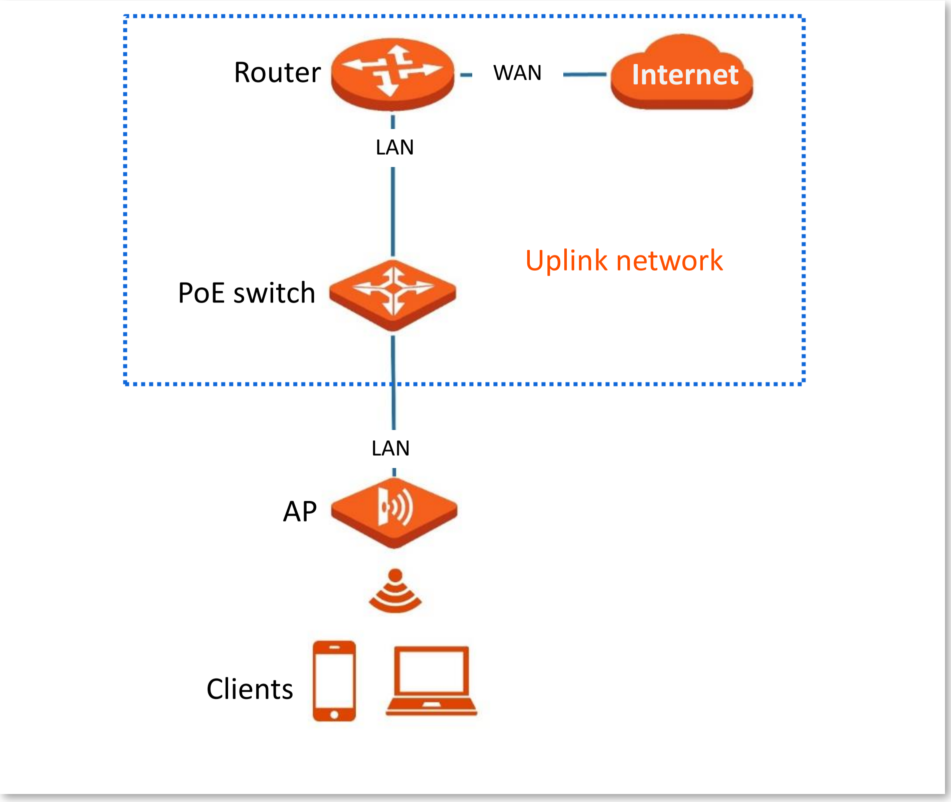
8.9 Uplink Check

8.9.1 Overview

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

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

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



8.9.2 Configure Uplink Check

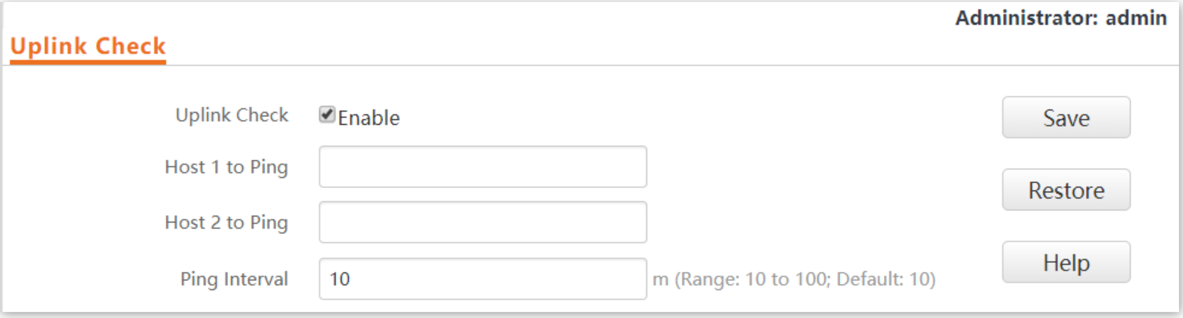
Step 1 Choose **Tools** > **Uplink Check**.

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

Step 3 Set **Host 1 to Ping** or **Host 2 to Ping** to the IP address of the host to be pinged through the LAN0 port of the AP, such as the IP address of the switch or router directly connected to the AP.

Step 4 Set **Ping Interval** to the interval at which the AP checks its uplink.

Step 5 Click **Save**.



Uplink Check

Uplink Check ☑ Enable

Host 1 to Ping

Host 2 to Ping

Ping Interval 10 m (Range: 10 to 100; Default: 10)

---End

Appendixes

A.1 Factory default settings

The following table lists the default values of major parameters of the AP.

Parameter			Default Value
Login	Management IP address		192.168.0.254
	User Name/Password	Administrator	admin|admin
		User	user|user
Quick Setup	Working Mode		AP Mode
LAN Setup	IP Address Type		Static IP Address
	IP Address		192.168.0.254
	Subnet Mask		255.255.255.0
DHCP Server			Disable
SSID Settings	SSID	2.4 GHz	The AP allows 8 SSIDs. The SSID displayed is Tenda_XXXXXX. Where XXXXXX indicates the range from the last 6 characters to the last 6 characters + 7 of the MAC address of the LAN ports of the AP. By default, the primary SSID is enabled, and the other SSIDs are disabled.
		5 GHz	The AP allows 4 SSIDs. The SSID displayed is Tenda_XXXXXX_5G. Where XXXXXX indicates the range from the last 6 characters + 8 to the last 6 characters +11 of the MAC address of the LAN ports of the AP. By default, the primary SSID is enabled, and the other SSIDs are disabled.

Parameter			Default Value
Radio Settings	Enable wireless		Enable
	Network Mode	2.4GHz	11b/g/n
		5GHz	11ac
	Channel Bandwidth	2.4GHz	20 MHz
		5GHz	80 MHz
SNMP Agent			Disable

A.2 Acronyms & Abbreviations

Acronyms & Abbreviations	Full Name
AC	Access Category
AC	Access Point Controller
AES	Advanced Encryption Standard
AIFSN	Arbitration Inter Frame Spacing Number
AP	Access Point
APSD	Automatic Power Save Delivery
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EDCA	Enhanced Distributed Channel Access
LAN	Local Area Network
MIB	Management Information Base
MU-MIMO	Multi-User Multiple-Input Multiple-Output
PoE	Power over Ethernet
PSK	Pre-shared Key
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TXOP	Transmission Opportunity
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access