

User Guide

802.11AC Indoor/Outdoor Wi-Fi Access Point

OAP1200



Copyright Statement

© 2023 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

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

Disclaimer

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

Preface

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



This user guide walks you through all functions on the web UI of 802.11AC Indoor/Outdoor Wi-Fi Access Point. All the screenshots herein are only for illustration. Refer to the actual conditions.

Conventions

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

Item	Presentation	Example
Cascading Menus	>	Click Status > Device Status
Parameter and value	Bold	Set User Name to Tom .
UI control	Bold	On the Policy page, click the OK button.
Variable	Italic	Format: <i>XX:XX:XX:XX:XX:XX</i>
Message	“ ”	The “Success” message appears.

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

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

For more documents

If you want to get more documents of the device, visit www.tendacn.com and search for the corresponding product model.

Technical support

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

Email address: support@tenda.cn

Website: www.tendacn.com

Revision history

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since this guide was first published.

Version	Date	Description
V1.0	2023-11-15	Original publication.

Contents

1	Login and logout	8
1.1	Login	8
1.2	Logout	10
2	Quick setup	11
2.1	AP mode	11
2.1.1	Overview	11
2.1.2	Configure AP mode	12
2.2	Client+AP mode	14
2.2.1	Overview	14
2.2.2	Configure Client+AP mode	15
3	Status	18
3.1	View system status	18
3.2	View wireless status	20
3.3	View traffic statistics	21
3.4	View client list	22
4	Internet settings	23
4.1	Configure LAN setup	23
4.2	Configure DHCP server	26
4.2.1	Overview	26
4.2.2	Set DHCP server	26
4.2.3	View DHCP clients	28
5	Wireless settings	29
5.1	SSID settings	29
5.1.1	Overview	29
5.1.2	Example of setting up an open wireless network	36
5.1.3	Example of setting up a wireless network encrypted with PSK	38

5.1.4 Example of setting up a wireless network encrypted with WPA or WPA2	40
5.2 RF settings	56
5.3 RF optimization	59
5.4 Load balancing	63
5.4.1 Load balancing between APs.....	63
5.4.2 Load balancing between bands.....	64
5.5 Frequency analysis	66
5.5.1 Overview	66
5.5.2 View frequency analysis	66
5.5.3 Execute channel scan	67
5.6 WMM	68
5.6.1 Overview	68
5.6.2 Configure WMM Settings	69
5.7 Access control	72
5.7.1 Overview	72
5.7.2 Configure access control	72
5.7.3 Example of configuring access control	74
5.8 Advanced settings	76
5.8.1 Overview	76
5.8.2 Configure advanced settings	76
5.9 QVLAN settings	77
5.9.1 Overview	77
5.9.2 Configure QVLAN.....	77
5.9.3 Example of configuring QVLAN settings.....	79
6 Advanced	82
6.1 Deployment mode	82
6.1.1 Overview	82
6.1.2 Configure deployment mode	84
6.2 Traffic control	85

6.2.1 Overview	85
6.2.2 Configure traffic control	86
6.3 SNMP.....	88
6.3.1 Overview	88
6.3.2 Configure SNMP agent	90
6.3.3 Example of configuring the SNMP function	92
6.4 Cloud maintenance	94
6.4.1 Overview	94
6.4.2 Example of configuring cloud maintenance.....	95
7 Tools	98
7.1 Date & Time	98
7.1.1 Configure system time.....	98
7.1.2 Login timeout interval	99
7.2 Maintenance	100
7.2.1 Reboot	100
7.2.2 Reset.....	102
7.2.3 Upgrade firmware	103
7.2.4 Backup/Restore	104
7.2.5 LED indicator control	106
7.3 Account	108
7.3.1 Overview	108
7.3.2 Modify the password and user name of login account.....	109
7.4 System log	110
7.4.1 View system logs	110
7.4.2 Log settings.....	111
7.5 Diagnostic tool	114
7.6 Uplink detection.....	116
7.6.1 Overview	116
7.6.2 Configure uplink detection.....	117

Appendix 118

A.1 Factory default settings 118

A.2 Acronyms & Abbreviations 119

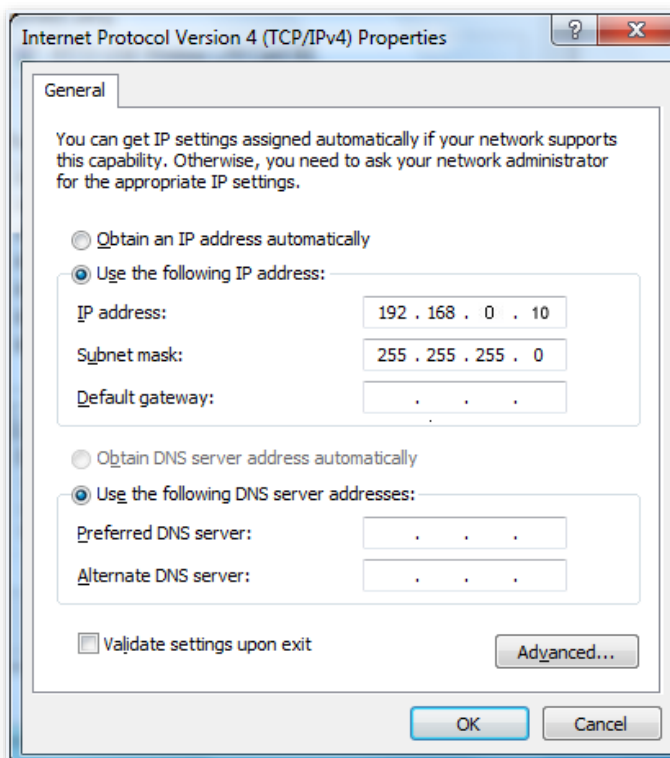
1 Login and logout

1.1 Login

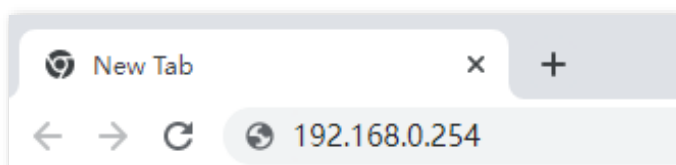
Step 1 Use an Ethernet cable to connect the management computer to Access Point (AP) or the switch connected to the AP.

Step 2 Configure the IP address of the computer to one in a same network segment with the AP.

For example, if the default IP address of the AP is **192.168.0.254**, then you can set the IP address of the computer to **192.168.0.X** (X ranges from 2 to 253 and is not occupied by other devices), and subnet mask to **255.255.255.0**.



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



Step 4 Enter the user name and password (both are **admin** by default), and click **Login**.

OAP1200V2.0

Default user name: admin

Default password: admin

English

Login

Forget password?

---End



TIP

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

- Ensure that all your Ethernet cables are properly connected.
- Ensure that the IP address of the computer is in a same network segment with the AP.
- If two or more APs are connected in a network without a controller, connect one AP to the network first, change its IP address to a different IP address on the same network segment, and then connect to the next AP and proceed the same modifications.
- The AP may obtain an IP address from a DHCP server in the LAN. You can check the new IP address from the client list of the DHCP server and use this new IP address to log in.
- If the problem persists, [reset the AP](#), and then try logging in again.

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

Quick Setup

Radio Band: 2.4GHz

Working Mode: AP Client+AP

SSID: [Empty Field]

Security Mode: None

Save Cancel

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 exit from the web UI.

2 Quick setup

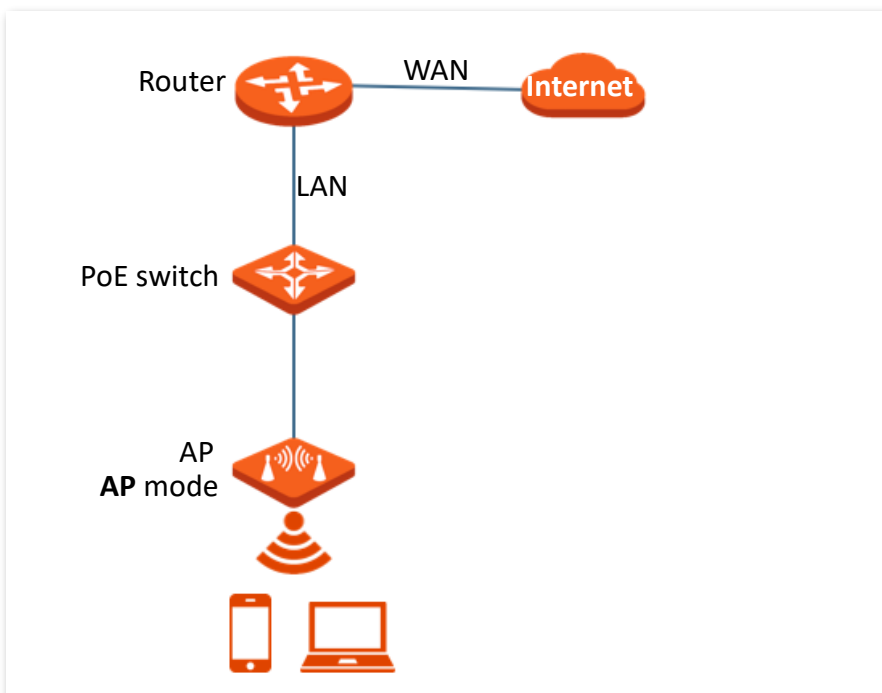
In the **Quick Setup** module, you can set up the AP in a quick way to enable internet access for your wireless devices such as smartphones and tablets.

AP supports two working modes: [AP mode](#) and [Client+AP mode](#).

2.1 AP mode

2.1.1 Overview

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



2.1.2 Configure AP mode



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

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Quick Setup**.
- Step 3** Set **Radio Band** you want to configure, which is **2.4GHz** in this example.
- Step 4** Set **Working Mode** to **AP**.
- Step 5** Set SSID ([primary SSID](#)).
- Step 6** Select **Security Mode**, which is **WPA2-PSK** in this example.
- Step 7** Set **Encryption Algorithm** and **Key** as required.
- Step 8** Click **Save**.

The screenshot shows the 'Quick Setup' configuration page. It features a lightbulb icon in the top right corner. The configuration options are as follows:

- Radio Band:** 2.4GHz (dropdown menu)
- Working Mode:** AP (radio button selected), Client+AP (radio button unselected)
- SSID:** [Empty text input field]
- Security Mode:** WPA-PSK (dropdown menu)
- Encryption Algorithm:** AES (radio button selected), TKIP (radio button unselected), TKIP&AES (radio button unselected)
- Key:** [Text input field with 7 dots]

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

- Step 9** If you need to configure the **5GHz** radio band as well, repeat steps [3](#) to [7](#).

---End

Search and connect your wireless devices such as smartphones to the **SSID** you set. Enter the wireless password (the **Key** you set) and you can access the internet.

Parameter description

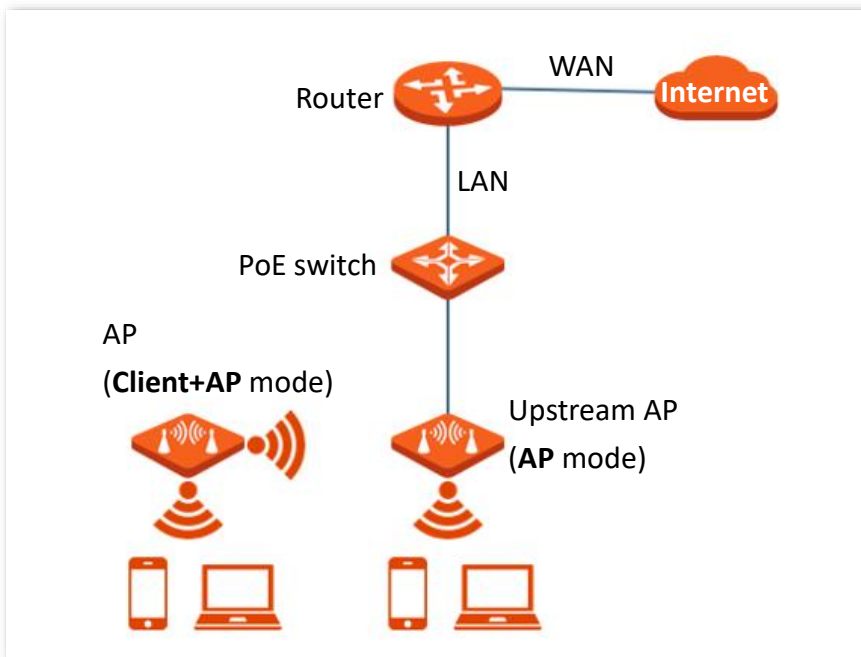
Parameter	Description
Radio Band	Used to select the radio band for configurations.

Parameter	Description
Working Mode	<p>Specifies the working mode of the AP.</p> <ul style="list-style-type: none">- AP: Choose the AP mode to convert wired networks into wireless networks.- Client+AP: Choose the Client+AP mode to bridge the upstream wireless network.
SSID	<p>Specifies the primary network name of the selected radio band. You can click it to modify the SSID.</p>
Security Mode	<p>Specifies the security mode you set for your AP's wireless network, including None, WEP, WPA-PSK, WPA2-PSK, WPA-PSK & WPA2-PSK, WPA and WPA2.</p>

2.2 Client+AP mode

2.2.1 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 typical network topology.



2.2.2 Configure Client+AP mode



TIP

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

Step 1 [Log in to the web UI of the AP.](#)

Step 2 Navigate to **Quick Setup**.

Step 3 Set **Radio Band** you want to configure, which is **2.4GHz** in this example.

Step 4 Set **Working Mode** to **Client+AP**.

Step 5 Click **Scan**.

Quick Setup

Radio Band: 2.4GHz

Working Mode: AP Client+AP

SSID:

Security Mode: None

Refresh Scan

Save Cancel

Step 6 Select the wireless network to be extended from the wireless network list that appears.



TIP

- If no wireless network is found, navigate to **Wireless > RF Settings**, ensure that **Wireless Network** is enabled, and try scanning wireless network again.
- The device detects and auto-fills **SSID**, **Security Mode** of the upstream wireless network for you.
- If the upstream network is encrypted, enter the wireless network password of the device in the **Key** column.

Select	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
<input type="radio"/>			20MHz		None	
<input checked="" type="radio"/>			20MHz		WPA2-PSK/AES	

Buttons: Refresh, Disable, Save, Cancel

Step 7 Click **Save**.

Quick Setup

Radio Band: 2.4GHz

Working Mode: AP Client+AP

SSID: []

Security Mode: WPA2-PSK

Encryption Algorithm: AES TKIP TKIP&AES

Key: []

Buttons: Refresh, Disable, Save, Cancel

---End


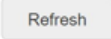
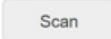
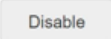

Search and connect your wireless devices such as smartphones to the **SSID** of the AP. Enter the wireless password (the **Key** you set) and you can access the internet.



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

Parameter description

Parameter	Description
Radio Band	Used to select the radio band for configurations.

Parameter	Description
Working Mode	<p>Specifies the working mode of the AP.</p> <ul style="list-style-type: none"> – AP: Choose the AP mode to convert wired networks into wireless networks. – Client+AP: Choose the Client+AP mode to bridge the upstream wireless network.
SSID	<p>Specifies the WiFi name (SSID) of the wireless network to be bridged. After you select the upstream wireless network from the scanned wireless network list, this parameter will be populated automatically.</p>
Security Mode	<p>Specifies the security mode of which the upstream wireless network adopted.</p> <p>The AP can support wireless network encrypted with None, WEP, WPA-PSK, WPA2-PSK and WPA-PSK & WPA2-PSK.</p> <p> NOTE</p> <ul style="list-style-type: none"> – If the wireless network to be bridged adopts the WEP security mode, Authentication Type, Default Key, and Key X (<i>X</i> ranges from 1 to 4) need to be entered manually. – If the wireless network to be bridged adopts the WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK security mode, Encryption Algorithm will be populated automatically and you only need to enter the Key.
	Used to refresh the scan results.
	Used to scan nearby available wireless networks. The scan results are displayed below.
	Used to end the scan operation and collapse the scan result.
	<p> TIP</p> <p>The button only appears after you clicked Scan.</p>

3 Status

3.1 View system status

[Log in to the web UI of the AP](#), and navigate to **Status > System Status**, you can check the system and LAN port status of the AP.

System Status

System Status

Device Name: OAP1200V2.0 Management Status: Disconnected

Uptime: 2hrs48min21sec System Time: 2023-10-30 17:05:24

Firmware Version: V2.0.0.1(10553) Hardware Version: V2.0

Number of Wireless Clients: 0

LAN Port Status

MAC Address: [redacted] IP Address: 192.168.0.127

Subnet Mask: 255.255.255.0 Primary DNS: 192.168.0.1

Secondary DNS: [redacted]

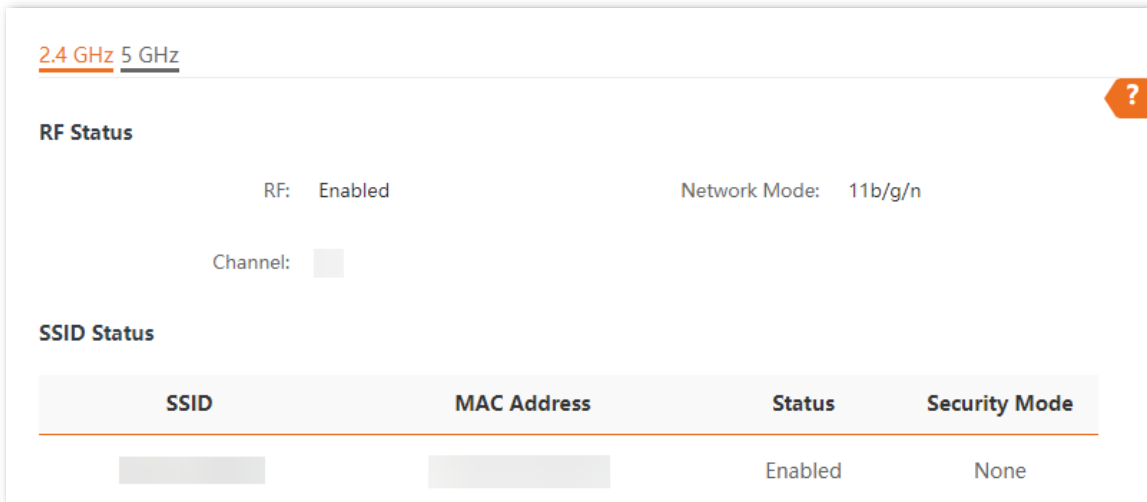
Parameter description

Parameter	Description
Device Name	Specifies the name of the AP. You can modify it on the LAN Setup page.
System Status	
Management Status	Specifies the connection between the AP and Tenda cloud platform.
Uptime	Specifies the time that has elapsed since the AP starts up last time.

Parameter	Description
System Time	Specifies the current system time of the AP.
Firmware Version	Specifies the current firmware version number of the AP.
Hardware Version	Specifies the current hardware version number of the AP.
Number of Wireless Clients	Specifies the quantity of wireless devices currently connected to the AP.
MAC Address	Specifies the physical address of the LAN port of the AP.
IP Address	Specifies the IP address of the LAN port of the AP, which can be used to log in to the web UI. You can modify it on the LAN Setup page.
Subnet Mask	Specifies the subnet mask of the AP.
Primary DNS	Specifies the primary DNS server of the AP.
Secondary DNS	Specifies the secondary DNS server of the AP.

3.2 View wireless status

[Log in to the web UI of the AP](#), and navigate to **Status > Wireless Status**, you can check general radio status and SSID status of the AP.



Parameter description

Parameter	Description	
RF	Specifies whether the wireless function of the AP is enabled.	
RF Status	Network Mode	Specifies the current network mode of the AP.
	Channel	Specifies the current working channel of the AP.
SSID Status	SSID	Specifies the names of all the wireless networks of the AP.
	MAC Address	Specifies the physical addresses corresponding to the SSIDs of the AP.
	Status	Specifies whether the wireless networks corresponding to the SSIDs of the AP are enabled.
	Security Mode	Specifies the security modes of the wireless networks corresponding to the SSIDs of the AP.

3.3 View traffic statistics

[Log in to the web UI of the AP](#), and navigate to **Status > Traffic Statistics**, you can check the statistics about historical packets of the wireless networks of the AP.



All the statistics are cleared when the wireless function is disabled or this device is rebooted.

2.4 GHz		5 GHz		
SSID	Received Traffic	Received Packets (Qty.)	Transmitted Traffic	Transmitted Packets (Qty.)
	199.58MB	738050	4.90MB	27282

Parameter description

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

3.4 View client list

[Log in to the web UI of the AP](#), and navigate to **Status > Client List**, you can check the information about the wireless clients connected to the wireless networks of the AP. You can also block certain connected clients.


2.4 GHz 5 GHz

Clients connected to the SSID: SSID: Tenda_23E9D0

ID	MAC Address	IP Address	Connection Duration	Transmit Rate	Receive Rate	Block
1		192.168.0.110	00:01:31	39Mbps	6Mbps	⊗

10 in total/Page 1 in total

Parameter description

Parameter	Description
SSID	Used to select the SSID from the drop-down list menu to view client information connected to it.
ID	Specifies the ID number of the clients connected to the SSID.
MAC Address	Specifies the physical address of the client.
IP Address	Specifies the IP address of the client.
Connection Duration	Specifies the online duration of the wireless client.
Transmit Rate	Specifies the current transmission rate of the client.
Receive Rate	Specifies the current receiving rate of the client.
Block	Used to click  to block the client from accessing the AP's wireless network. To unblock a client, navigate to Wireless > Access Control .

4 Internet settings

4.1 Configure LAN setup

[Log in to the web UI of the AP](#), and navigate to **Internet Settings > LAN Setup**, you can 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.

LAN Setup ?

MAC Address

IP Address Type

IP Address

Subnet Mask

Default Gateway

Primary DNS


Secondary DNS

Device Name

Optimize Ethernet for: Faster Speed (Auto Negotiation)
 Longer Distance (10 Mbps Full Duplex)

Parameter description

Parameter	Description
MAC Address	Specifies the MAC address of the LAN port of the AP.

Parameter	Description
IP Address Type	<p>Specifies the IP address obtaining mode of the AP.</p> <ul style="list-style-type: none"> – Static IP: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP are set manually. It is proper for the scenarios where only one or several APs are deployed in the network. – DHCP (Dynamic IP Address): It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP are obtained from a DHCP server on your LAN. It is proper for the scenarios where a large group of APs are deployed in the network. <p> TIP</p> <p>If IP Address Type is set to DHCP (Dynamic IP Address), 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.</p>
IP Address	Specifies the IP address of the AP. The web UI of the AP is accessible at this IP address.
Subnet Mask	Specifies the subnet mask of the IP address of the AP.
Default Gateway	<p>Specifies the gateway IP address of the AP.</p> <p>Generally, set the gateway IP address to the LAN IP address of your egress router connected to the internet, so that the AP can access the internet.</p>
Primary DNS	<p>Specifies the primary DNS server of the AP.</p> <p>If your egress 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.</p>
Secondary DNS	<p>Specifies the secondary DNS server address of the AP. This parameter is optional.</p> <p>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.</p>
Device Name	<p>Specifies the name of the AP.</p> <p>You are recommended to change the name of the AP to indicate the location of the AP (such as Bedroom), so that you can easily identify the AP when managing many APs.</p>

Parameter	Description
Optimize Ethernet for	<p>Specifies the Ethernet mode of the PoE/LAN port of this AP.</p> <ul style="list-style-type: none">- Faster Speed (Auto Negotiation): This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended.- Longer Distance (10 Mbps Full Duplex): This mode features a long transmission distance but relatively low transmission rate (usually 10 Mbps). <p>The 10 Mbps Full Duplex mode is recommended only when the Ethernet cable that connects the PoE/LAN 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/LAN port of the AP may not be able to properly transmit or receive data.</p>

4.2 Configure DHCP server

4.2.1 Overview

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



If the modified IP address of the LAN port is not in the same network segment with the original one, the system automatically modifies the DHCP address pool so that the pool is in the same network segment with the new IP address of the LAN port.

4.2.2 Set DHCP server

Step 1 [Log in to the web UI of the AP.](#)

Step 2 Navigate to **Internet Settings > DHCP Server > DHCP Server.**

Step 3 Enable the **DHCP Server** function.

Step 4 Set parameters as required. Generally, you only need to modify **Gateway Address** and **Primary DNS**.

Step 5 Click **Save**.

DHCP Server DHCP Clients

* DHCP Server

Start IP Address

End IP Address

Subnet Mask

* Gateway Address

* Primary DNS

Secondary DNS

Lease Time

---End



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

Parameter description

Parameter	Description
DHCP Server	Specifies whether to enable the DHCP Server function of the AP. By default, it is disabled.
Start IP Address	Specify the start or end IP address of the DHCP server's IP address pool. The default value of start or end IP address is 192.168.0.100/192.168.0.200 .
End IP Address	
Subnet Mask	Specifies the subnet mask assigned by the DHCP server to devices.
Gateway Address	<p>Specifies the gateway IP address assigned by the DHCP server to devices. Generally, it is the LAN IP address of the router connected to the internet.</p> <p> Only through a gateway can a LAN device access a server or host which is not in the local network segment.</p>
Primary DNS	<p>Specifies the IP address of the primary DNS server assigned by the DHCP server to devices.</p> <p> To enable devices to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.</p>
Secondary DNS	Specifies the IP address of the secondary DNS server assigned by the DHCP server to devices. This parameter is optional, which indicates you can leave it blank if the DHCP server does not assign this parameter.
Lease Time	<p>Specifies the validity period of an IP address assigned by the DHCP server to a device. When the lease time expires:</p> <ul style="list-style-type: none"> - If the client is still connected to the AP, the client will renew the lease and continue to keep the IP address. - If the client is no longer connected to the AP, the AP will release the IP address. If another client sends a request to apply for an IP address, the AP can assign the IP address to such client. <p>It is recommended to set to 1 day if there is no other special requirement.</p>

4.2.3 View DHCP clients

After enabling the DHCP server, [log in to the web UI of the AP](#), and navigate to **Internet Settings > DHCP Server > DHCP Clients**, you can view DHCP clients and the connection information.

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

ID	Host Name	IP Address	MAC Address	Lease Time
1		192.168.0.129		23hrs 41min 21sec
2		192.168.0.110		23hrs 41min 25sec

10 in total/Page 2 in total

Parameter description

Parameter	Description
ID	Specifies the ID number of the DHCP client.
Host Name	Specifies the host name of the DHCP client.
IP Address	Specifies the IP address of the DHCP client.
MAC Address	Specifies the physical address of the DHCP client.
Lease Time	Specifies the validity period of an IP address assigned by the DHCP server to a device.
Refresh	Used to refresh the current results.

5 Wireless settings

5.1 SSID settings

5.1.1 Overview

[Log in to the web UI of the AP](#), and navigate to **Wireless > SSID**, you can set the SSID-related parameters of the AP.

2.4 GHz 5 GHz

SSID

Status Enable Disable

Broadcast SSID Enable Disable

Guest Enable Disable

Isolate Client Enable Disable

Isolate SSID Enable Disable

WMF Enable Disable



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

SSID

Chinese SSID Encoding

Security Mode

Parameter description

Parameter	Description
SSID	<p>Specifies the SSID to be configured.</p> <p>The AP allows you to enable 8 SSIDs on 2.4 GHz band, and 8 SSIDs on 5 GHz band. On each band, the first displayed SSID is the primary SSID.</p>
Status	<p>Specifies the status of the selected SSID.</p> <p>The primary SSID is enabled by default and you can enable other SSIDs manually.</p>
Broadcast SSID	<p>Specifies whether to enable the Broadcast SSID function.</p> <p>After this function is disabled, AP stops broadcasting SSID and nearby wireless clients cannot detect the SSID. Users need to enter the SSID manually on the wireless client to access the wireless network, enhancing the security of the wireless network.</p>
Guest	<p>Specifies whether to enable the Guest function.</p> <p>After this function is enabled, guests can connect to the internet and only access the internet.</p>
Isolate Client	<p>Specifies whether to enable the Isolate Client function.</p> <p>After this function is enabled, 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.</p> <p> TIP</p> <p>It is available only when the Guest function is disabled.</p>
Isolate SSID	<p>Specifies whether to enable the Isolate SSID function.</p> <p>After this function is enabled, wireless devices connected to different SSIDs of the AP cannot communicate with each other, enhancing the security of the wireless network.</p> <p> TIP</p> <p>It is available only when the Guest function is disabled.</p>
WMF	<p>Specifies whether to enable the WMF function.</p> <p>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.</p>

Parameter	Description
Max. Number of Clients	Specifies the maximum number of devices that can connect to the wireless network corresponding to an SSID. If the number is reached, new devices cannot connect to the SSID unless some devices cut off their connections.
SSID	Used to click it to modify the selected SSID (name of the wireless network).
Chinese SSID Encoding	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	Specifies the security modes supported by the AP, including: None , WEP , WPA-PSK , WPA2-PSK , Mixed WPA/WPA2-PSK , WPA and WPA2 .

Security mode

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

The AP supports various security modes for network encryption, including [None](#), [WEP](#), [WPA-PSK](#), [WPA2-PSK](#), [WPA-PSK & WPA2-PSK \(Mixed WPA/WPA2-PSK\)](#), [WPA and WPA2](#).

■ None

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

■ WEP

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

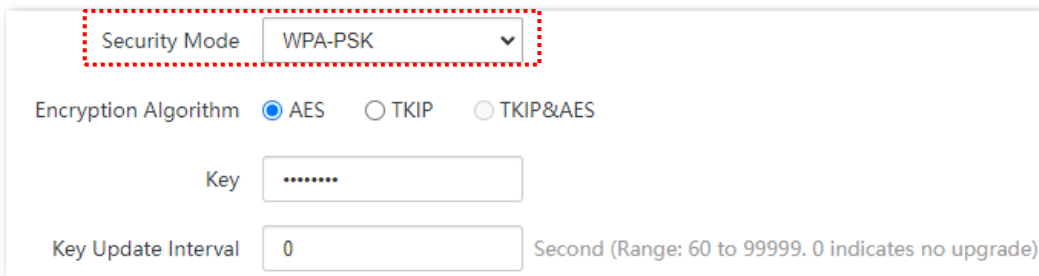
Parameter description

Parameter	Description
Authentication Type	<p>Specifies the authentication type for the WEP security mode. The options include Open and Shared. The options share the same encryption process.</p> <ul style="list-style-type: none"> - Open: It specifies that authentication is not required and data exchanged is encrypted with WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. - Shared: It specifies that a shared key is used for authentication and data exchanged is encrypted with WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key.
Default Key	<p>Specifies the WEP key for the current SSID.</p> <p>For example, if Default Key is set to Key 2, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Key 2.</p>
Key 1/2/3/4	<p>Specifies 4 WEP keys which are allowed at the same time, but only the one specified by the Default Key is valid. The key type includes ASCII and Hexadecimal.</p> <ul style="list-style-type: none"> - 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.

■ WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK (Mixed WPA/WPA2-PSK)

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

WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK (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 devices use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.



The image shows a configuration panel for wireless security. At the top, the 'Security Mode' is set to 'WPA-PSK' in a dropdown menu, which is highlighted with a red dashed border. Below this, the 'Encryption Algorithm' is set to 'AES' with a selected radio button, while 'TKIP' and 'TKIP&AES' are unselected. A 'Key' field contains a masked password represented by seven dots. At the bottom, the 'Key Update Interval' is set to '0' seconds, with a note indicating that 0 means no upgrade and the range is from 60 to 99999 seconds.

Parameter description

Parameter	Description
Security Mode	<p>Specifies the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK (Mixed WPA/WPA2-PSK).</p> <ul style="list-style-type: none"> – WPA-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA-PSK. – WPA2-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA2-PSK. – WPA-PSK & 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	<p>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 WPA-PSK & WPA2-PSK (Mixed WPA/WPA2-PSK), this parameter has the AES, TKIP, and TKIP&AES values.</p> <ul style="list-style-type: none"> – AES: It indicates the Advanced Encryption Standard. – TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. – TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	Specifies a pre-shared WPA key, that is, the password clients use to connect to the wireless network.
Key Update Interval	<p>Specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.</p> <p>The value 0 indicates that a WPA key is not updated.</p>

■ WPA and WPA2

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

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

Security Mode: WPA

RADIUS Server: []

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

RADIUS Key: [.....]

Encryption Algorithm: AES TKIP TKIP&AES

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

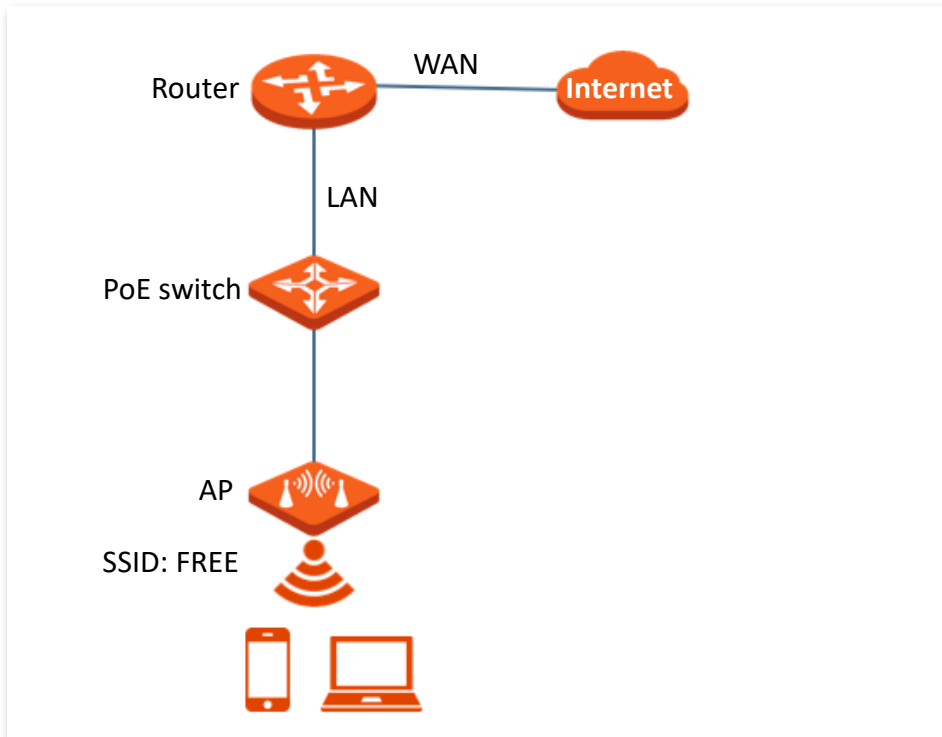
Parameter description

Parameter	Description
Security Mode	<p>The WPA and WPA2 options are available for network protection with a RADIUS server.</p> <ul style="list-style-type: none"> - 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	
RADIUS Port	Specify the IP address/port number/shared password of the RADIUS server.
RADIUS Key	
Encryption Algorithm	<p>Specifies the encryption algorithm corresponding to the selected security mode. The available options include AES, TKIP, and TKIP&AES.</p> <ul style="list-style-type: none"> - AES: It indicates the Advanced Encryption Standard. - TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. - TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key Update Interval	<p>Specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.</p> <p>The value 0 indicates that a WPA key is not updated.</p>

5.1.2 Example of setting up an open wireless network

Networking requirements

In an industrial park, guests can connect to the wireless network without a password and access the internet through the wireless network.



Procedures

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

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Wireless > SSID**.
- Step 3** Select the second SSID from the **SSID** drop-down list box.
- Step 4** Set **Status** to **Enable**.
- Step 5** Change the value of the **SSID** text box to **FREE**.
- Step 6** Set **Security Mode** to **None**.
- Step 7** Click **Save**.

The screenshot shows the configuration page for a 2.4 GHz SSID. The page has a header with '2.4 GHz' and '5 GHz' tabs, and a help icon in the top right. The configuration options are as follows:

- * SSID**: A dropdown menu.
- * Status**: Enable, Disable
- Broadcast SSID**: Enable, Disable
- Guest**: Enable, Disable
- Isolate Client**: Enable, Disable
- Isolate SSID**: Enable, Disable
- WMF**: Enable, Disable
- Max. Number of Clients**: (Range: 1 to 128)
- * SSID**:
- Chinese SSID Encoding**:
- * Security Mode**:

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

---End

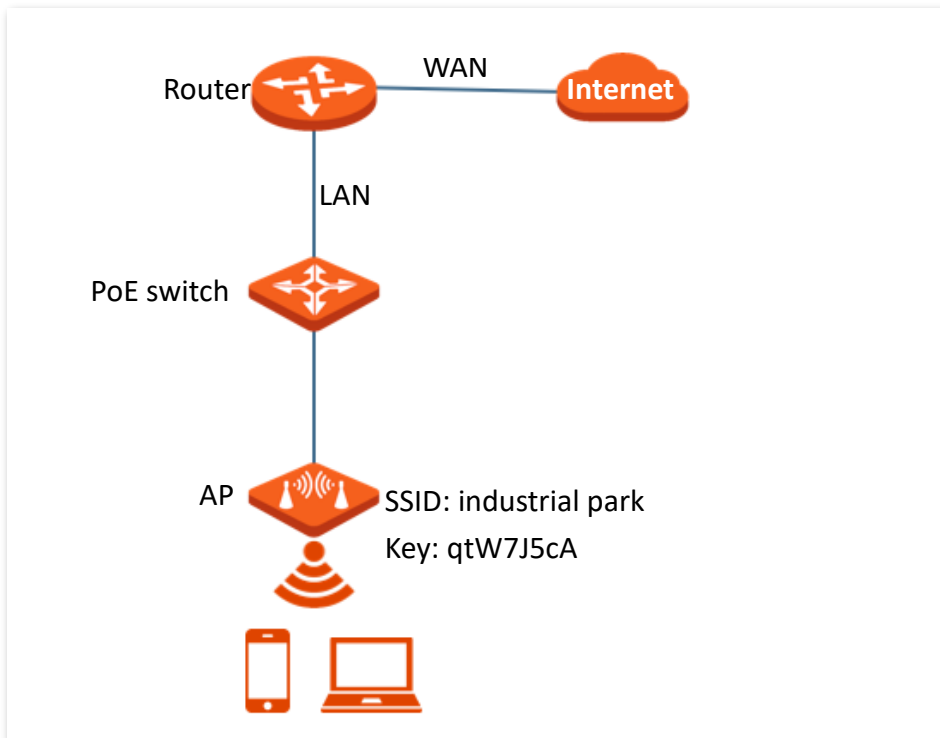
Verification

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

5.1.3 Example of setting up a wireless network encrypted with PSK

Networking requirements

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



Procedures

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

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Wireless > SSID**.
- Step 3** Select the second SSID from the **SSID** drop-down list box.
- Step 4** Set **Status** to **Enable**.
- Step 5** Change the value of the **SSID** text box to **industrial park**.
- Step 6** Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.
- Step 7** Set **Key** to **qtW7J5cA**.
- Step 8** Click **Save**.

2.4 GHz 5 GHz

* SSID

* Status Enable Disable

Broadcast SSID Enable Disable

Guest Enable Disable

Isolate Client Enable Disable

Isolate SSID Enable Disable

WMF Enable Disable

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

* SSID

Chinese SSID Encoding

* Security Mode

* Encryption Algorithm AES TKIP TKIP&AES

* Key

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

---End

Verification

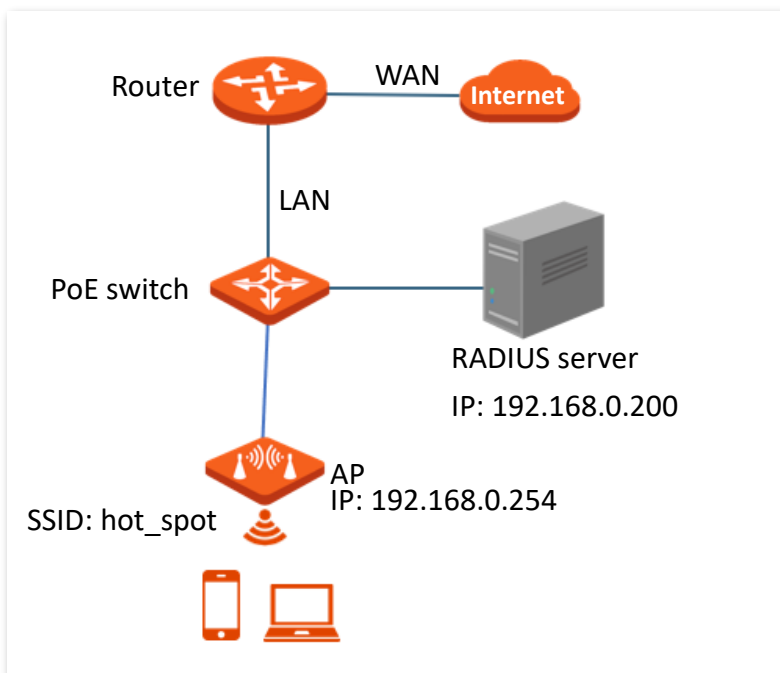
Wireless devices can connect to the **industrial park** wireless network with the password **qtW7J5cA**.

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

Networking requirements

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.

Assume that the IP address of the RADIUS server is **192.168.0.200**, the Key is **qtW7J5cA**, and the port number for authentication is **1812**.



Procedures

I. Configure the AP

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

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Wireless > SSID**.
- Step 3** Select the second SSID from the **SSID** drop-down list box.
- Step 4** Set **Status** to **Enable**.
- Step 5** Change the value of the **SSID** text box to **hot_spot**.
- Step 6** Set **Security Mode** to **WPA2**.

Step 7 Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Password** to **192.168.0.200**, **1812**, and **qtW7J5cA** respectively.

Step 8 Set **Encryption Algorithm** to **AES**, and click **Save**.

The screenshot shows a configuration window for a wireless network. At the top, there are tabs for "2.4 GHz" and "5 GHz". A red asterisk indicates a required field. The settings are as follows:

- SSID:** [Empty text box]
- Status:** Enable Disable
- Broadcast SSID:** Enable Disable
- Guest:** Enable Disable
- Isolate Client:** Enable Disable
- Isolate SSID:** Enable Disable
- WMF:** Enable Disable
- Max. Number of Clients:** (Range: 1 to 128)
- SSID:**
- Chinese SSID Encoding:**
- Security Mode:**
- RADIUS Server:**
- RADIUS Port:** (Range: 1025 to 65535. Default: 1812)
- RADIUS Key:**
- Encryption Algorithm:** AES TKIP TKIP&AES
- Key Update Interval:** Second (Range: 60 to 99999. 0 indicates no upgrade)

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

---End

II. Configure the RADIUS server

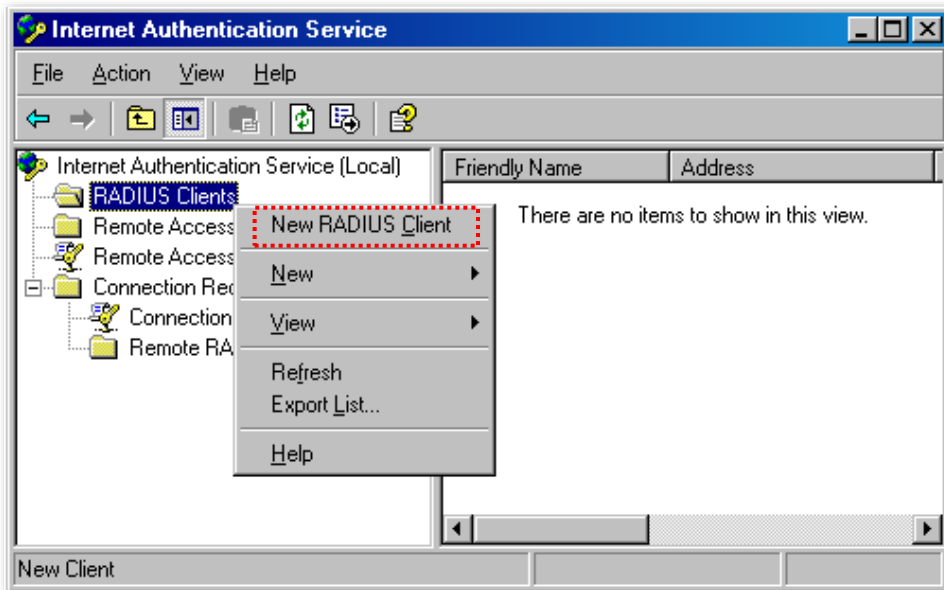


TIP

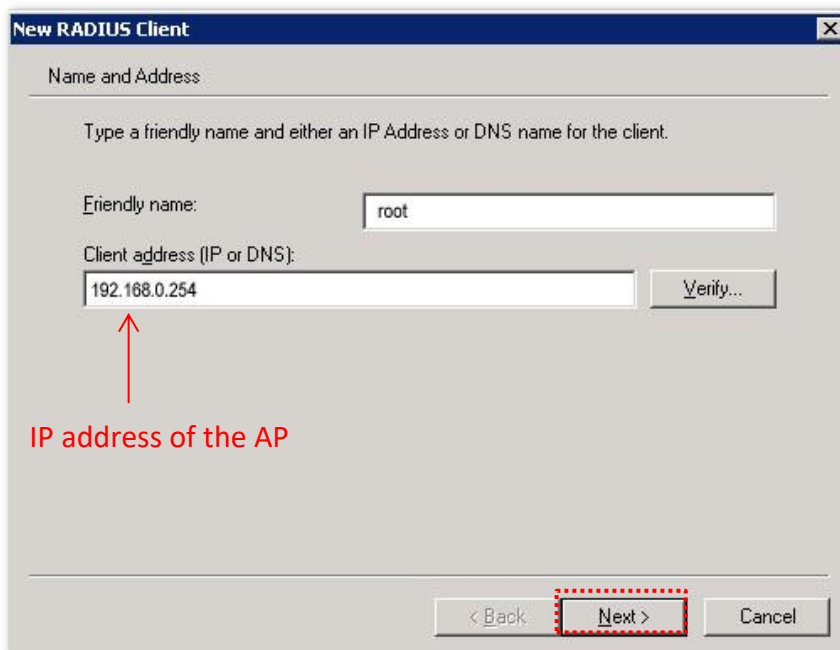
Windows 2003 is used as an example to describe how to configure the RADIUS server.

Step 1 Configure a RADIUS client.

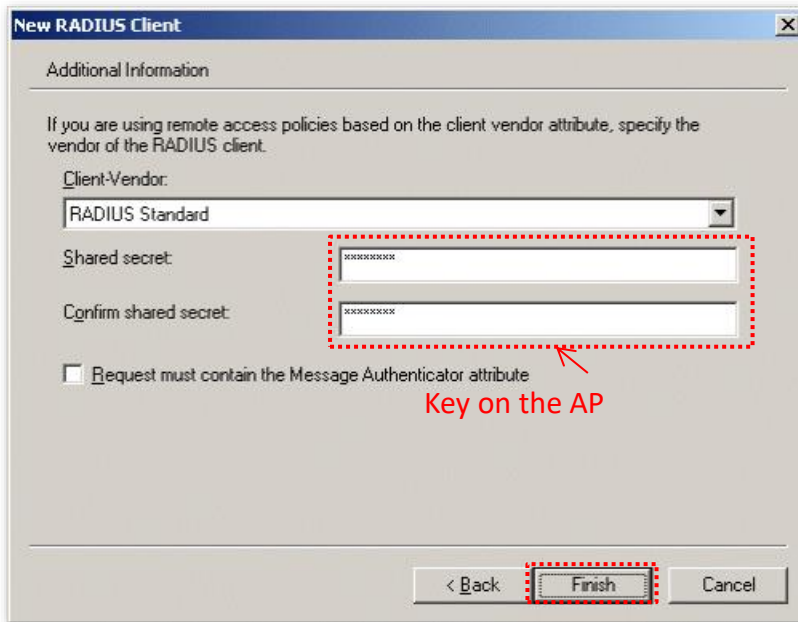
1. In the **Computer Management** dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.



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



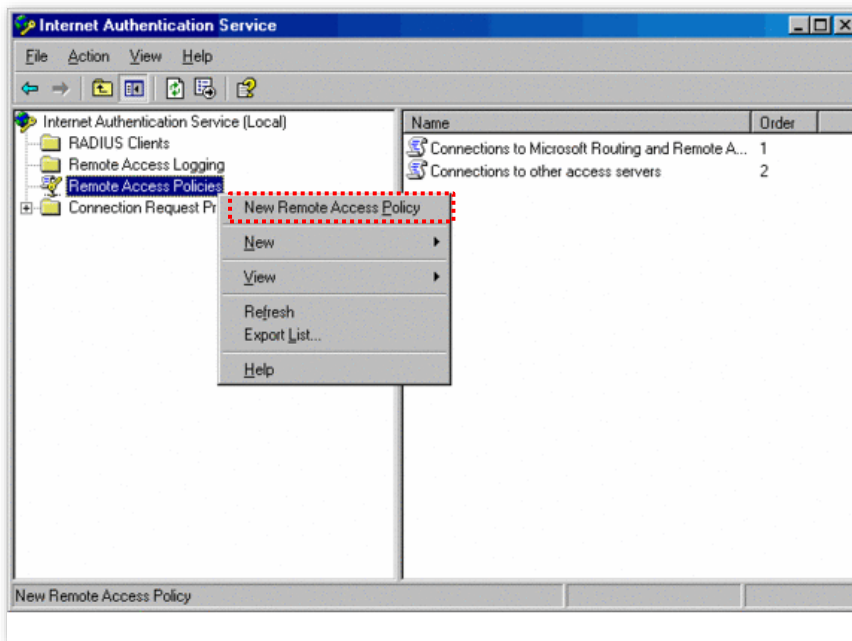
3. Enter **qtW7J5cA** in the **Shared secret** and **Confirm shared secret** text boxes, and click **Finish**.

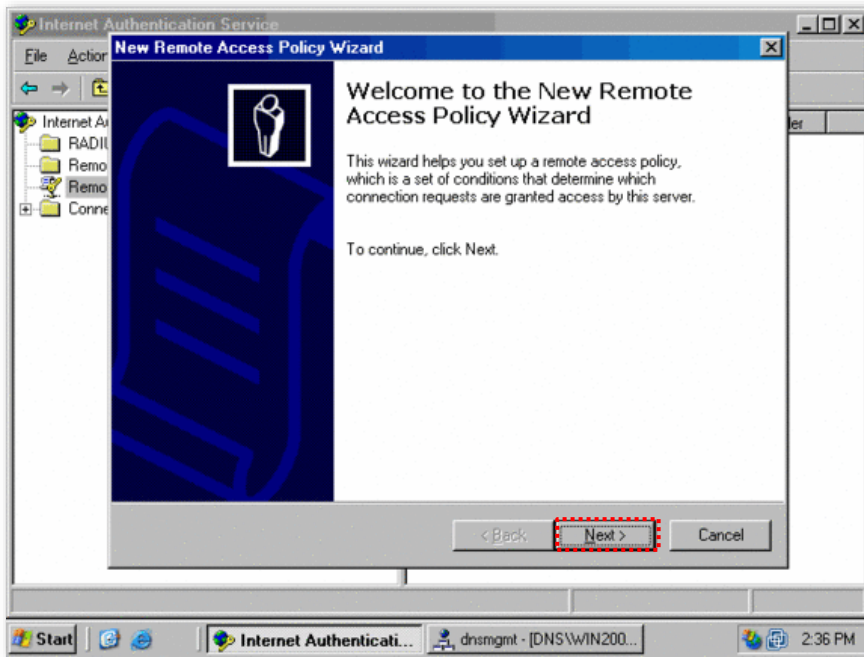


Step 2 Configure a remote access policy.

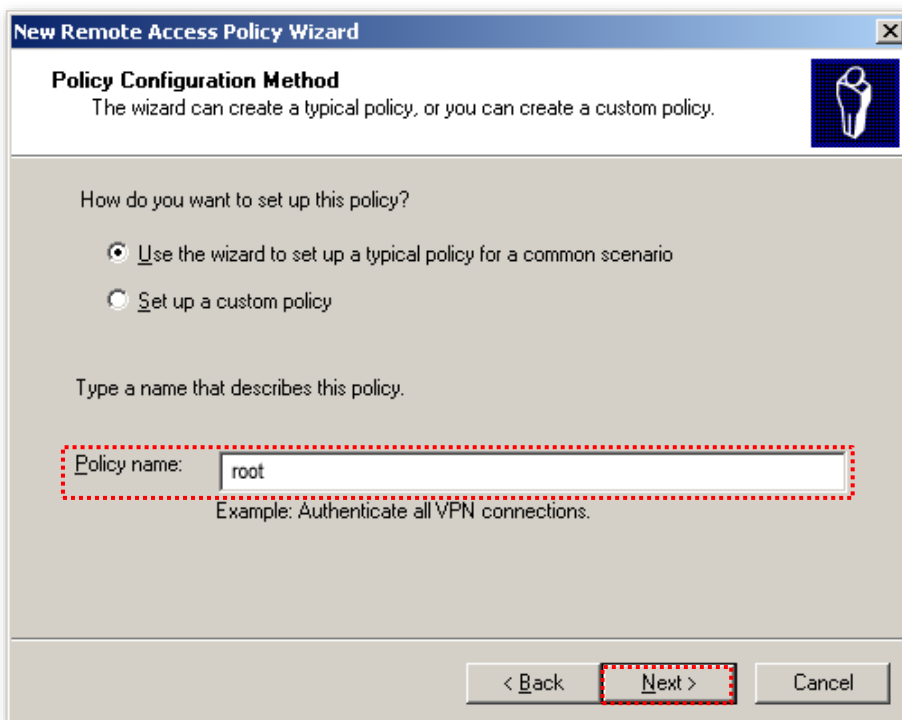
1. Right-click **Remote Access Policies** and choose **New Remote Access Policy**.

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

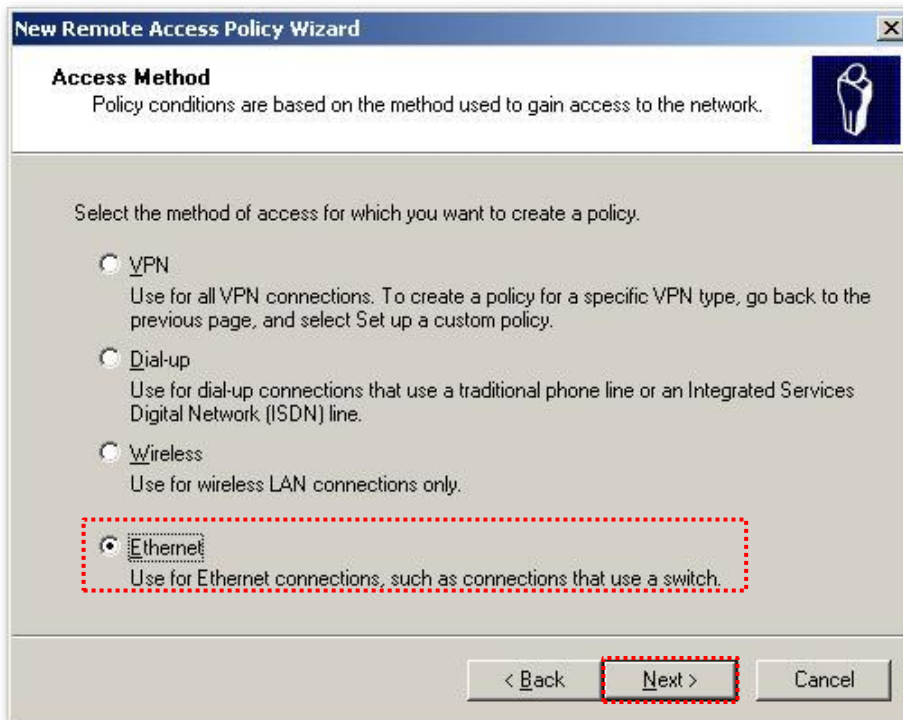




2. Enter a policy name and click **Next**.



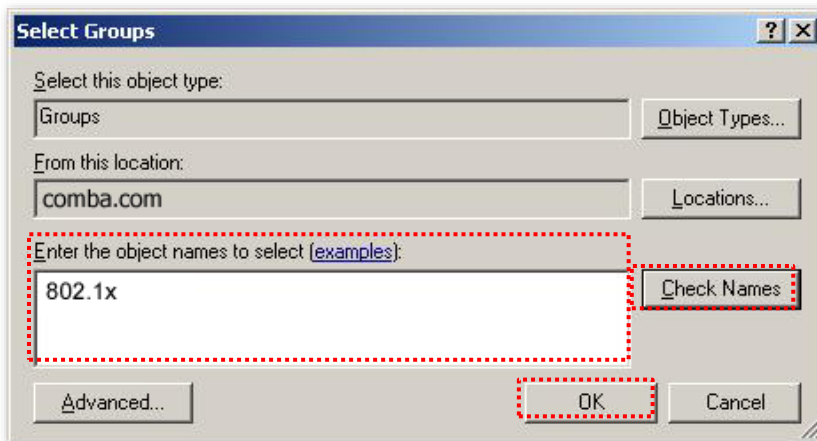
3. Select **Ethernet** and click **Next**.



4. Select **Group** and click **Add**.



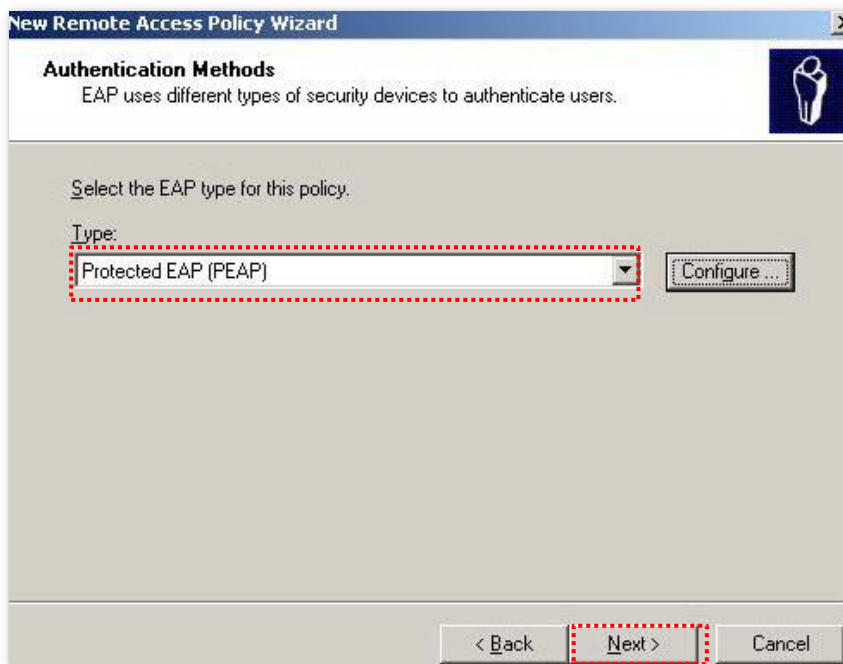
5. Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.

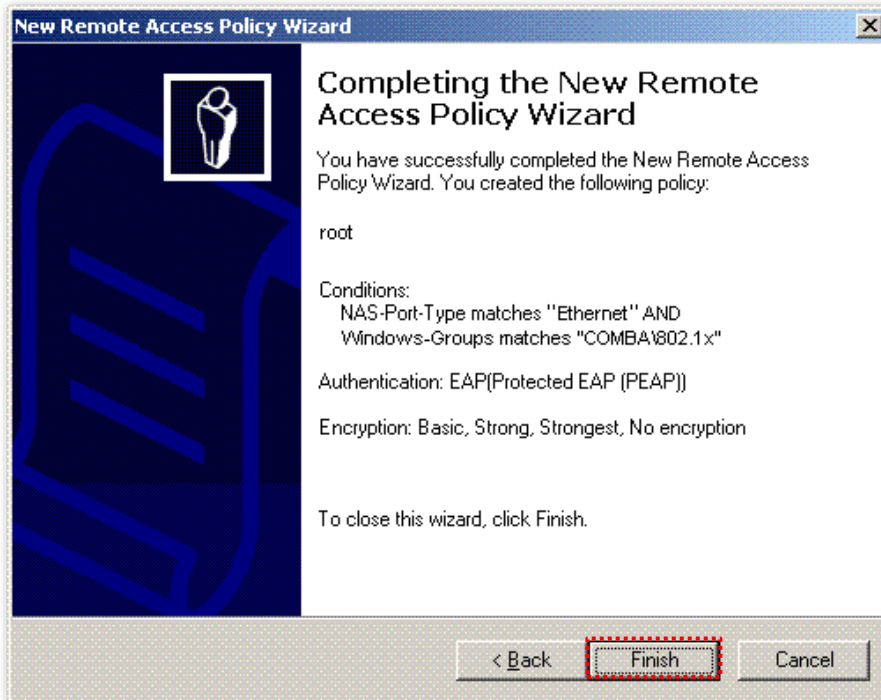


6. Select **Protected EAP (PEAP)** and click **Next**.

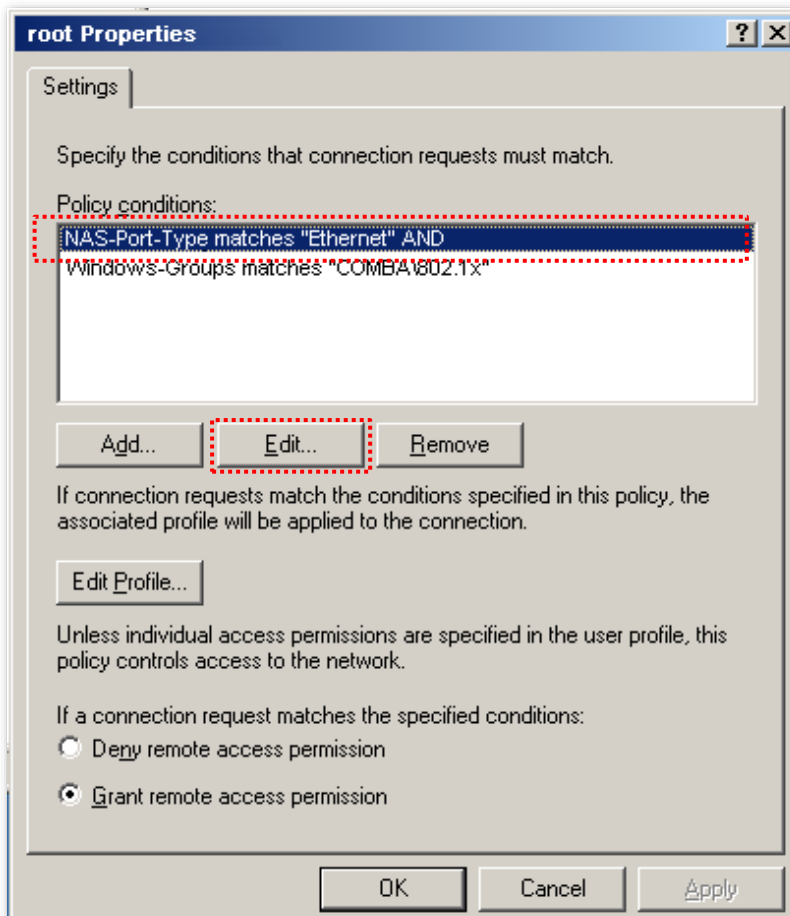
In the **New Remote Access Policy Wizard** dialog box that appears, click **Finish**.

The remote access policy is created.

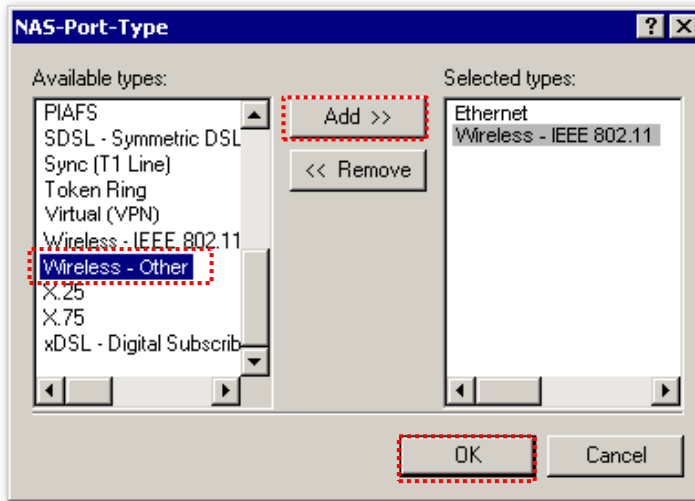




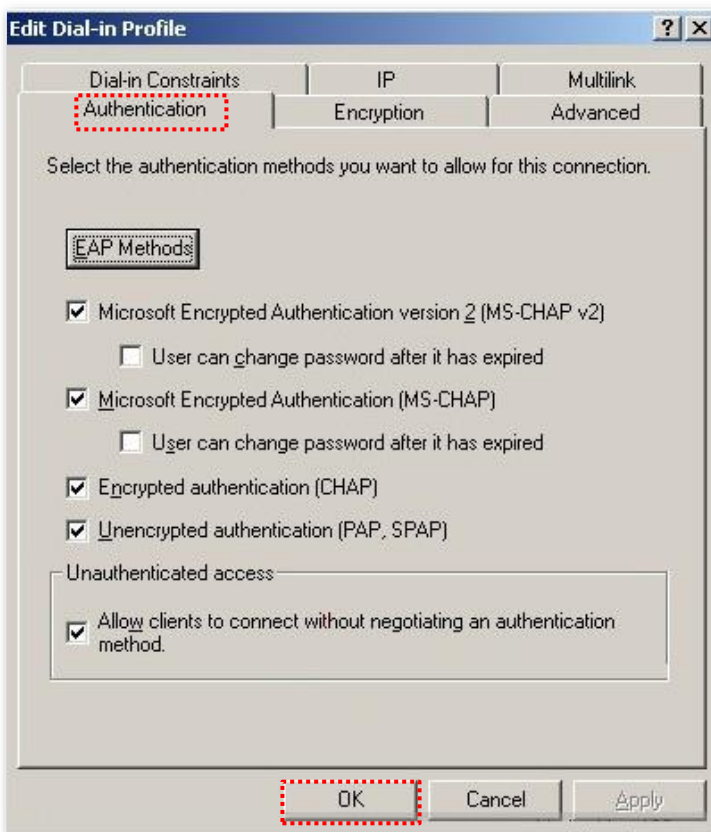
7. Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



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



9. Click **Edit Profile**, click the **Authentication** tab, configure settings as shown in the following figure, and click **OK**. When a message appears, click **No**.



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

---End

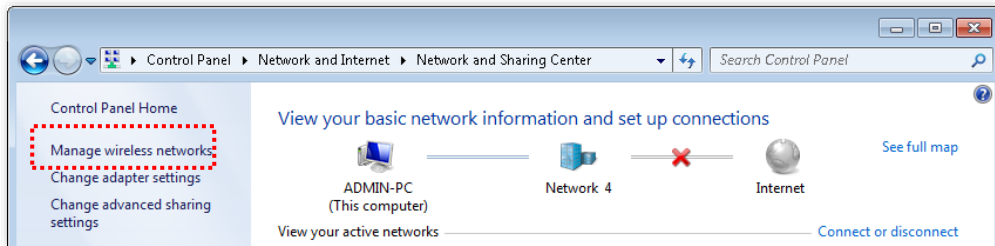
III. Configure your wireless device



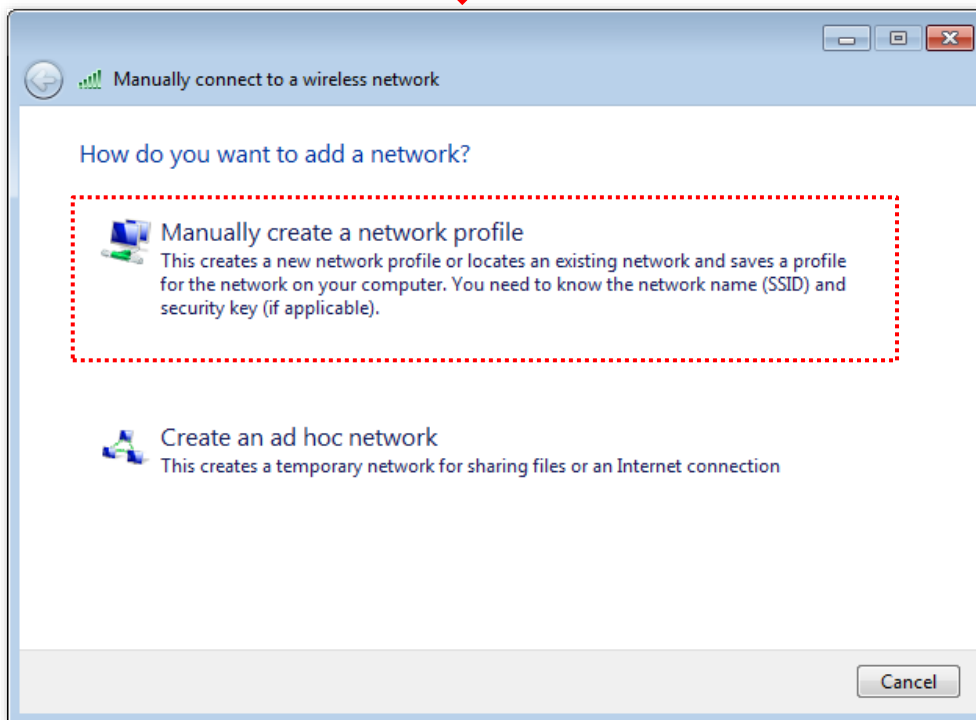
TIP

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

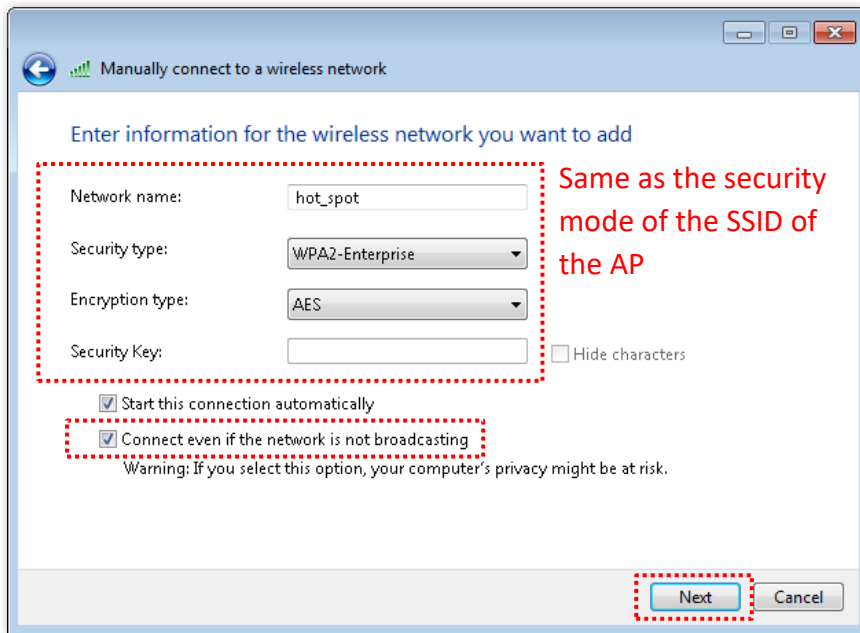
- Step 1** Navigate to **Start > Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



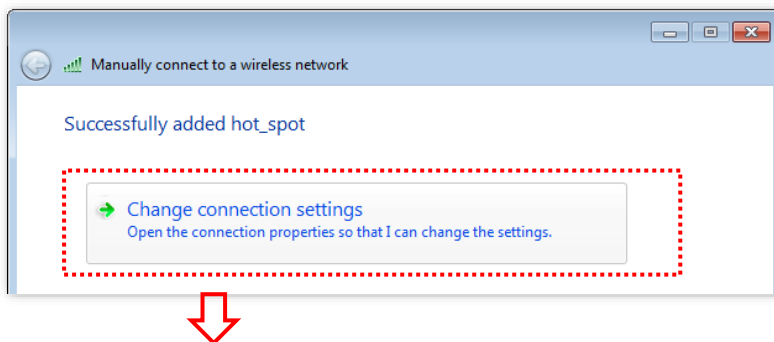
- Step 2** Click **Add**, and click **Manually create a network profile**.

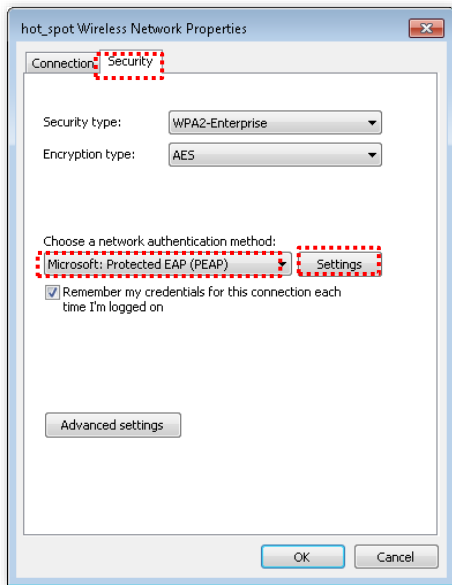


Step 3 Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.

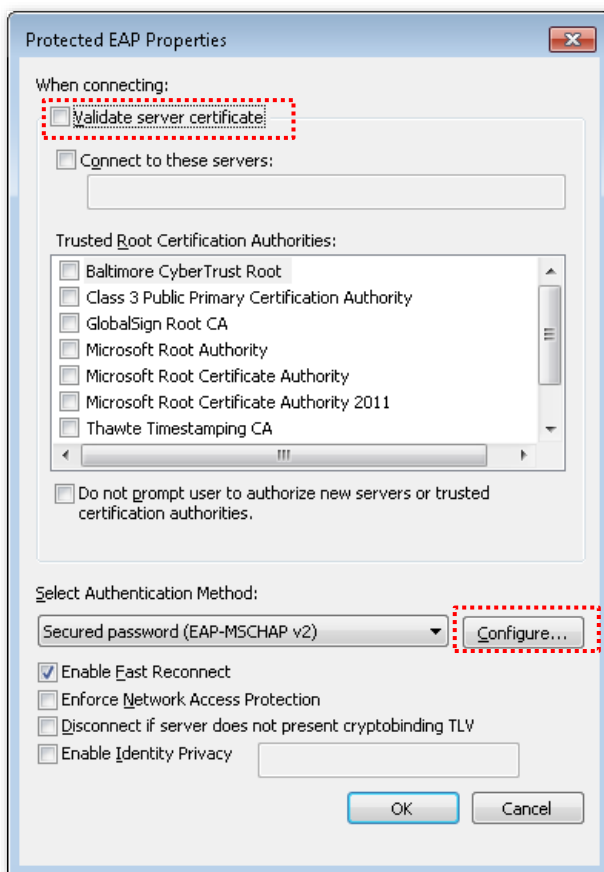


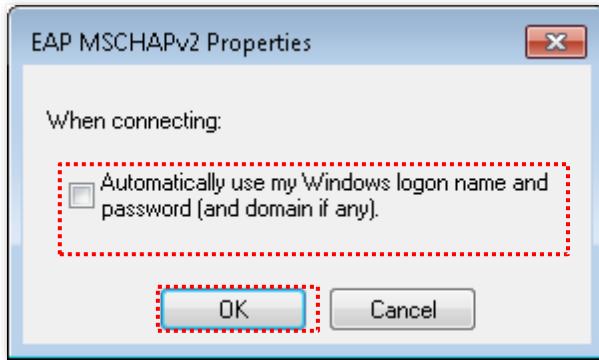
Step 4 Click **Change connection settings**. Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



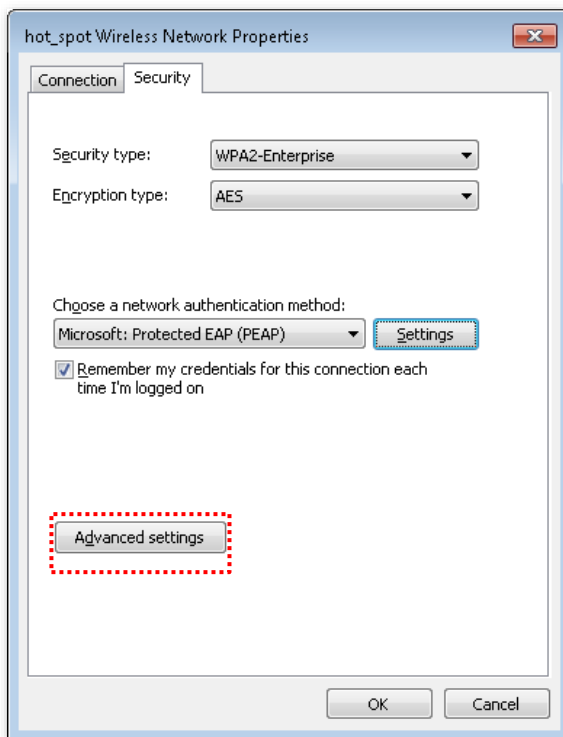


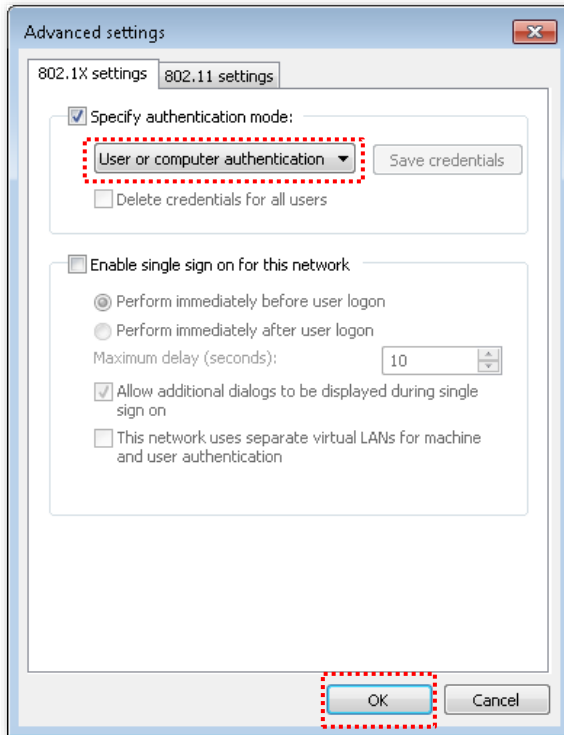
Step 5 Deselect **Validate server certificate** and click **Configure**. Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



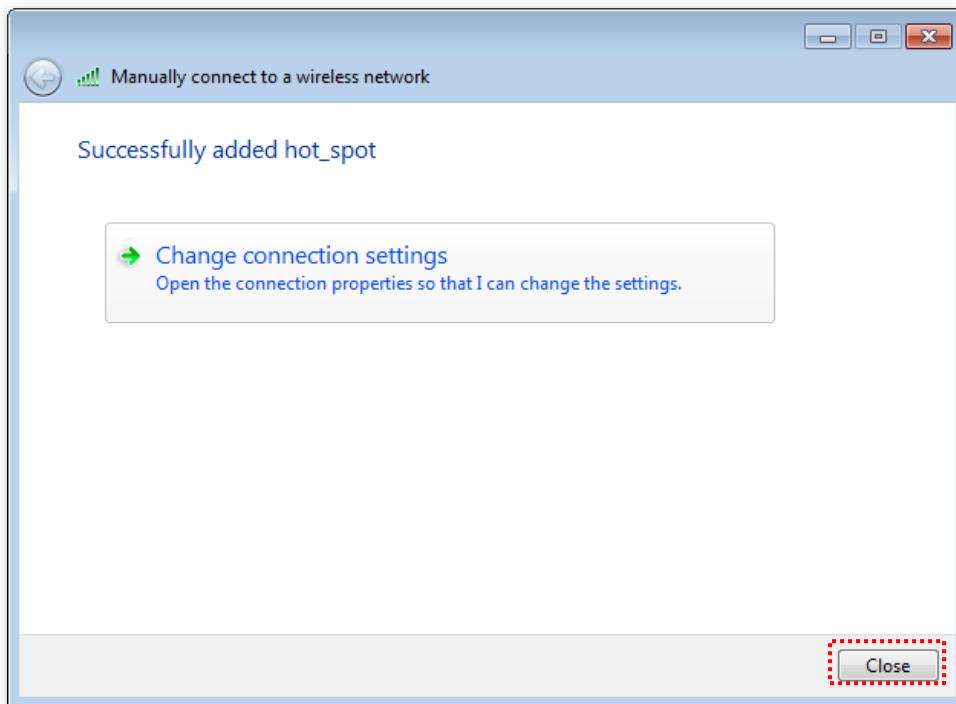


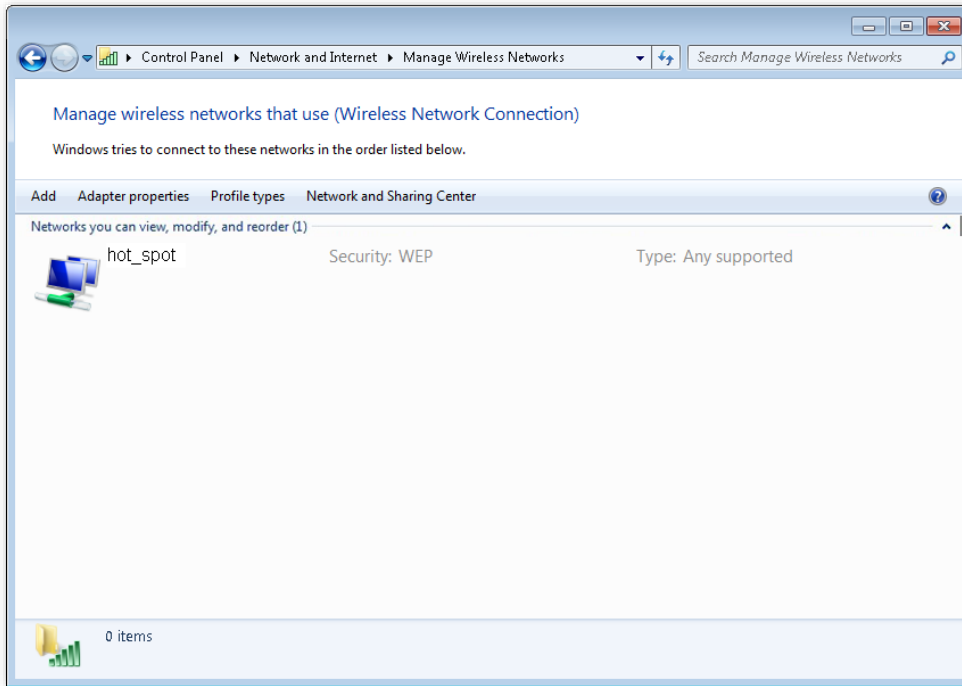
Step 6 Click **Advanced settings**. Select **User or computer authentication** and click **OK**.



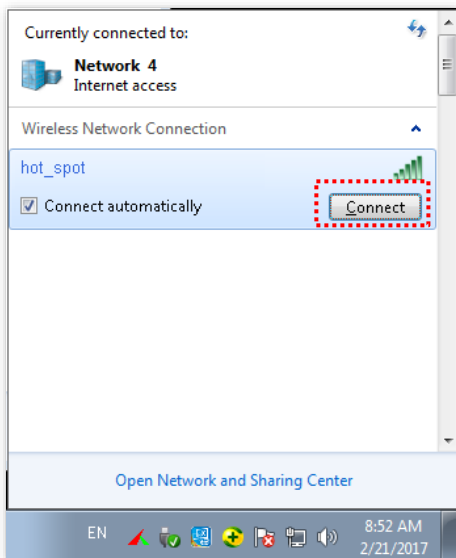


Step 7 Click **Close**.

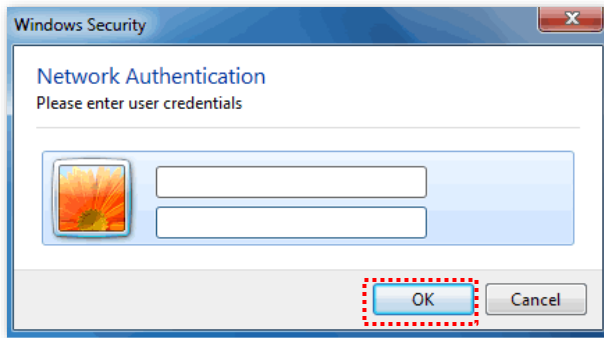




Step 8 Click the network icon in the lower-right corner of the desktop and choose the wireless network of the AP, which is **hot_spot** in this example. And click **Connect**.



Step 9 In the **Windows Security** dialog box that appears, enter the [user name and password](#) set on the RADIUS server and click **OK**.



---End

Verification

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

5.2 RF settings

[Log in to the web UI of the AP](#), and navigate to **Wireless > RF Settings**, you can configure advanced settings about the AP, such as channel, power, and short GI.

2.4 GHz 5 GHz

Wireless Network

Country/Region ALL

Network Mode 11b/g/n

Channel Auto

Channel Bandwidth 20/40MHz

Extension Channel Auto

Lock Channel

Transmit Power 10dBm 26dBm

Lock Power

Preamble Long Preamble Short Preamble

Short GI Enable Disable

Suppress Broadcast Probe Response Enable Disable

Save Cancel

Parameter description

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

Parameter	Description
Network Mode	<p>Specifies the wireless network mode of the AP. This parameter can be set if Lock Channel is not selected.</p> <p>Available options for 2.4 GHz are 11b, 11g, 11b/g, and 11b/g/n.</p> <ul style="list-style-type: none"> - 11b: The AP works in 802.11b mode and only wireless devices compliant with 802.11b can connect to the 2.4 GHz wireless networks of the AP. - 11g: The AP works in 802.11g mode and only wireless devices compliant with 802.11g can connect to the 2.4 GHz wireless networks of the AP. - 11b/g: The AP works in 802.11b/g mode and only wireless devices compliant with 802.11b or 802.11g can connect to the 2.4 GHz wireless networks of the AP. - 11b/g/n: The AP works in 802.11b/g/n mode. Wireless devices compliant with 802.11b or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n can connect to the 2.4 GHz wireless networks of the AP. <p>Available options for 5 GHz are 11a, 11ac, and 11a/n.</p> <ul style="list-style-type: none"> - 11a: The AP works in 802.11a mode and only wireless devices compliant with 802.11a can connect to the 5 GHz wireless networks of the AP. - 11ac: The AP works in 802.11ac mode and only wireless devices compliant with 802.11ac can connect to the 5 GHz wireless networks of the AP. - 11a/n: The AP works in 802.11a/n mode and only wireless devices compliant with 802.11a or 802.11n can connect to the 5 GHz wireless networks of the AP.
Channel	<p>Specifies the operating channel of the AP. This parameter can be set if Lock Channel is not selected.</p> <p>Auto: It indicates that the AP automatically adjusts its operating channel according to the ambient environment.</p>
Channel Bandwidth	<p>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.</p> <ul style="list-style-type: none"> - 20 MHz: It indicates that the AP can use only 20 MHz channel bandwidth. - 40 MHz: It indicates that the AP can use only 40 MHz channel bandwidth. - 20/40 MHz: It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment. - 80MHz: It indicates that the AP can use only 80 MHz channel bandwidth.
Extension Channel	Used to determine the operating frequency band of this device when it uses the 40 MHz channel bandwidth in 11n mode.
Lock Channel	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.

Parameter	Description
Transmit Power	<p>Specifies the transmit power of the AP.</p> <p>A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the wireless network performance and security.</p>
Lock Power	<p>Specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.</p>
Preamble	<p>Specifies a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data.</p> <p>By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the Short Preamble option.</p>
Short GI	<p>Specifies whether to enable the Short Guard Interval function.</p> <p>There is a delay on the receiving side due to multipath and other factors during the wireless signal transmission in space. If the subsequent data block is transmitted too quickly, it will interfere with the previous data block, and the short guard interval can be used to circumvent this interference. Short GI helps to increase the wireless throughput by 10%.</p>
Suppress Broadcast Probe Response	<p>Specifies whether to enable the Suppress Broadcast Probe Response function.</p> <p>By default, wireless devices keep sending Probe Request packets that include the SSID field to scan their nearby wireless networks. After receiving such packets, this device determines whether the wireless devices are allowed to access its wireless networks based on the packets and responds using the Probe Response packets (including all Beacon frame parameters), which consumes a lot of wireless resources.</p> <p>After this function is enabled, this device does not respond to the requests without an SSID, saving wireless resources.</p>

5.3 RF optimization

[Log in to the web UI of the AP](#), and navigate to **Wireless > RF Optimization**, you can modify the radio parameters to optimize performance.



It is recommended to modify the settings only with the professional guidance to prevent degrading wireless performance.

2.4 GHz 5 GHz
?

Beacon Interval ms (Range: 40 to 999. Default: 100)

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

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

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

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

Signal Reception Default Coverage-oriented Capacity-oriented

Air Interface Scheduling Enable Disable

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

APSD Enable Disable

Client Timeout Interval

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

Save
Cancel

Parameter description

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

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

Parameter	Description
Prioritize 5 GHz	Specifies whether to enable the Prioritize 5 GHz function. If this function is enabled, dual band wireless devices prefer the 5 GHz wireless network of the AP to connect when the 5 GHz signal strength transmitted by devices is stronger than the Prioritize 5 GHz Threshold .
Prioritize 5 GHz Threshold	With the Prioritize 5 GHz function enabled, if the strength of the signals transmitted by a wireless device is stronger than this threshold, the wireless device connects to the 5 GHz wireless network. Otherwise, it connects to the 2.4 GHz wireless network.
Air Interface Scheduling	Specifies whether to enable the Air Interface Scheduling function. If this function is enabled, the same download time is assigned to users experiencing different download rates, ensuring a better experience for high-rate users.
Anti-interference Mode	Specifies the anti-interference modes you can select for your AP. The default option is 3 (Suppress critical interference) . <ul style="list-style-type: none"> - 0 (Disable): Interference suppression measures are disabled. - 1 (Suppress weak interference): Suppress mild interference for weak radio environment. - 2 (Suppress moderate interference): Suppress moderate interference for bad radio environment. - 3 (Suppress critical interference): Suppress critical interference for heavy loading radio environment.
APSD	Specifies whether to enable the Automatic Power Save Delivery function. APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
MU-MIMO	Specifies whether to enable the Multi-User Multiple-Input Multiple-Output function. If this function is enabled, AP can communicate with multiple users concurrently, avoiding wireless network congestion and improving communication. This option is available on the 5 GHz configuration page.
Client Timeout Interval	Used to set the wireless client disconnection interval of this device. The device disconnects from a wireless client if no traffic is transmitted or received by the wireless client within the interval.
Mandatory Rate	Specifies rates that wireless clients must support in order to connect to the wireless networks of this device.
Optional Rate	Specifies the additional rates that the AP supports, which are optional to wireless clients. The clients meeting the basic requirement can connect to the AP with higher rate.

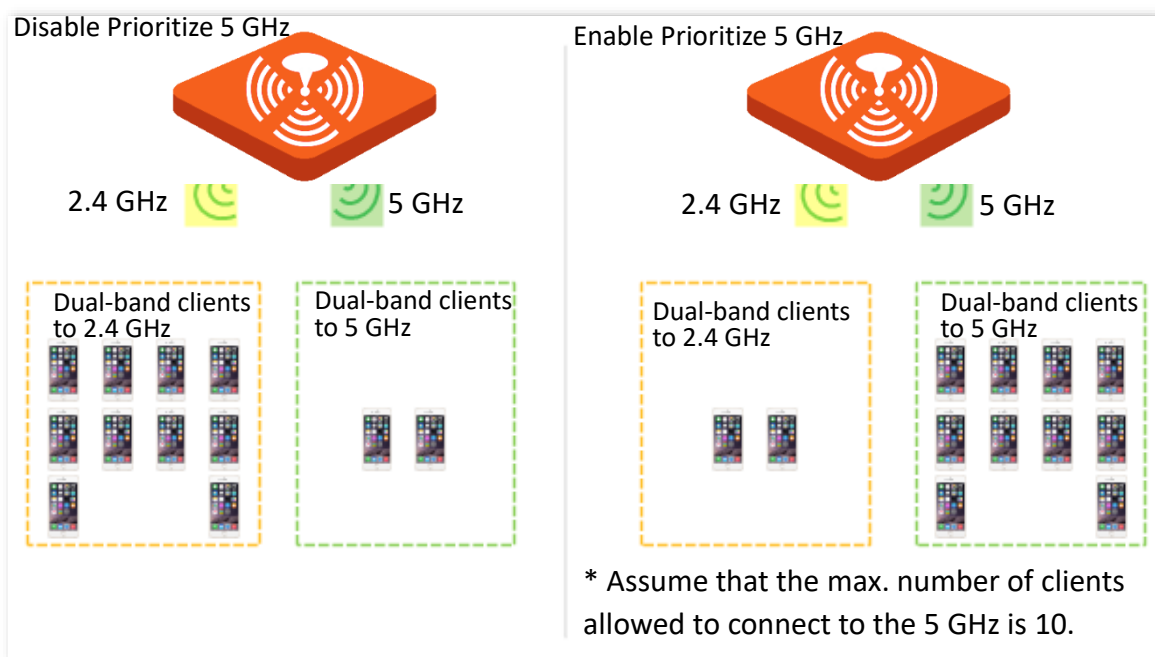
■ Prioritize 5 GHz

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.



NOTE

The prioritize 5 GHz function takes effect only on the condition that 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 First-in First-out (FIFO) 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.

5.4 Load balancing

5.4.1 Load balancing between APs

In an actual wireless network environment, especially in high-density scenarios, it often happens that too many users connect to a certain AP. As a result, some APs are overloaded while others are idle. For APs that apply the same load balancing policy between APs, the load balancing between APs function can accurately balance the load among these APs. In this way, the utilization of network resources can be maximized and the utilization rate of system resources can be effectively improved.

[Log in to the web UI of the AP](#), and navigate to **Wireless > Load Balancing > Between APs**, you can view or configure the parameters of load balancing between APs.

However, disabling/enabling the load balancing between APs and load balancing policy delivery functions can only be configured by the controller (a device with AP management and load balancing between APs function), and cannot be configured on the AP. For details, refer to the AP management function in user guides for the corresponding controllers.



You can modify the load balancing between APs parameters on the web UI of the AP only after the controller (a device with AP management and the load balancing between APs functions) delivers a load balancing policy to the AP for the first time.

Between APs Between Bands

Between APs Disable Enable

Load Balancing Policy

Trigger User Threshold

Deviation

Decision-making Time s

Reconnection Times

Parameter description

Parameter	Description
Between APs	Specifies whether to enable the load balancing between APs function. This function is enabled by a controller (a device with AP management and load balancing between APs function). By default, this function is disabled.
Load Balancing Policy	Specifies the load balancing policy between APs applied by AP. The load balancing policy is delivered by a controller (a device with AP management and load balancing between APs function). It supports load balancing based on user number.
Trigger User Threshold	Specifies the threshold to trigger load balancing between APs. When users connected to an AP reaches the threshold, load balancing between APs is triggered.
Deviation	Specifies the deviation between the number of users of two APs. If deviation between the user numbers of two APs applying the same load balancing policy exceeds this value, new users are directed to the AP with fewer users first.
Decision-making Time	<p>Specifies the time period in which AP refuses user connection request. It is recommended to keep the default settings.</p> <p>If within this time period, the number of AP refusals has reached the Reconnection Times, AP allows access from this user.</p> <p>If within this time period, the number of AP refusals does not reach Reconnection Times, the number of refusals is erased.</p>
Reconnection Times	Specifies the largest number of user connection attempts. If the number of AP refusals has reached this value in Decision-making Time , AP allows access from this user. It is recommended to keep the default settings.

5.4.2 Load balancing between bands

The AP supports wireless networks with two frequency bands, 2.4 GHz and 5 GHz. Some clients in the network only support the 2.4 GHz radio band while some support dual-band. And generally, when dual-band clients access the wireless network, the 2.4 GHz radio band is selected by default. Therefore, the 2.4 GHz radio band may be overloaded while the 5GHz radio band may be relatively idle. To prevent the above situation, it is recommended to enable the load balancing between bands function to balance the load between the radio bands of the AP and improve user's internet experience.

[Log in to the web UI of the AP](#), and navigate to **Wireless > Load Balancing > Between Bands**, you can view or configure the parameters of load balancing between bands.

This function is disabled by default. The following figure displays the page when **Between Bands** is enabled.

Between APs Between Bands ?

Between Bands Disable Enable

Trigger User Threshold

Deviation

Decision-making Time s

Reconnection Times

Parameter description

Parameter	Description
Between Bands	Specifies whether to enable the load balancing between bands function.
Trigger User Threshold	Specifies the threshold to trigger load balancing between bands. When users connected to the AP reach the threshold, load balancing between bands is triggered.
Deviation	Specifies the deviation between the number of users connected to two bands. If the deviation exceeds this value, new users are directed to the band with fewer users first.
Decision-making Time	Specifies the time period in which AP refuses user connection request. It is recommended to keep the default settings. If within this time period, the number of AP refusals has reached the Reconnection Times , AP allows access from this user. If within this time period, the number of AP refusals does not reach Reconnection Times , the number of refusals is erased.
Reconnection Times	Specifies the largest number of user connection attempts. If the number of AP refusals has reached this value in Decision-making Time , AP allows access from this user. It is recommended to keep the default settings.

5.5 Frequency analysis

5.5.1 Overview

[Log in to the web UI of the AP](#), and navigate to **Wireless > Frequency Analysis**, you can analyze frequency and scan channels.

Frequency analysis

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

Channel scan

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

5.5.2 View frequency analysis

Step 1 [Log in to the web UI of the AP](#).

Step 2 Navigate to **Wireless > Frequency Analysis**.

Step 3 Click **2.4 GHz Frequency Analysis** or **5 GHz Frequency Analysis** tab to select the wireless network radio band for frequency analysis, which is **2.4 GHz Frequency Analysis** in this example.

Step 4 Enable **Scan**.

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

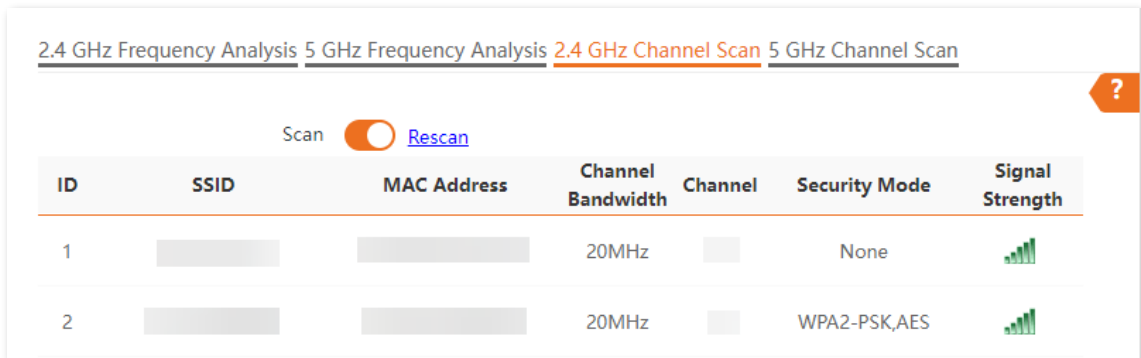
---End

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

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



5.5.3 Execute channel scan

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Wireless > Frequency Analysis**.
- Step 3** Click **2.4 GHz Channel Scan** or **5 GHz Channel Scan** tab to select the wireless network radio band for channel scan, which is **2.4 GHz Frequency Analysis** in this example.
- Step 4** Enable **Scan**.



2.4 GHz Frequency Analysis 5 GHz Frequency Analysis 2.4 GHz Channel Scan 5 GHz Channel Scan

Scan Rescan

ID	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
1			20MHz		None	
2			20MHz		WPA2-PSK,AES	

---End

5.6 WMM

5.6.1 Overview

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

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

WMM involves the following terms:

- Enhanced Distributed Channel Access (EDCA): It is a channel competition mechanism to ensure that packets with higher priorities are assigned more bandwidth and transmitted earlier.
- Access Category (AC): The WMM mechanism divides WLAN traffic by priority in descending order into the AC-VO (voice stream), AC-VI (video stream), AC-BE (best effort), and AC-BK (background) access categories. The access categories use queues with different priorities to send packets. The WMM mechanism ensures that packets in queues with higher priorities have more opportunities to access channels.

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

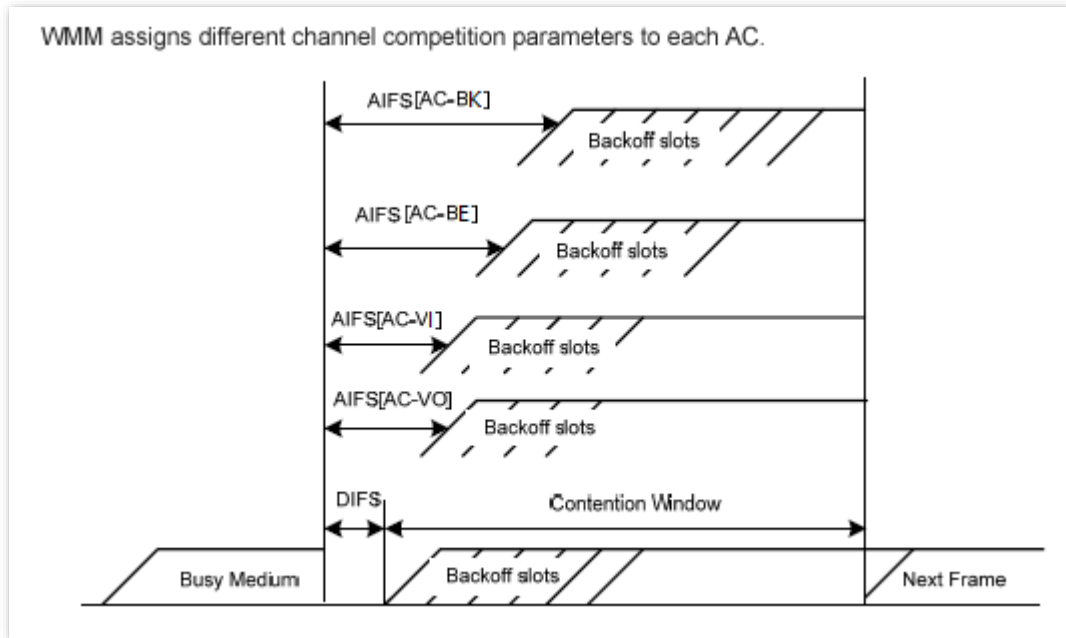
■ EDCA parameters

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

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

- Arbitration Inter Frame Spacing Number (AIFSN): Different from the fixed distributed inter-frame spacing (DIFS) specified in the 802.11 protocol family, AIFSN varies across ACs. A greater AIFSN indicates a longer backoff period. See AIFS in the following figure.
- Contention window minimum (CWmin) and contention window maximum (CWmax) specify the average backoff period. The period increases along with these two values. See the backoff slots in the following figure.

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



■ ACK policies

WMM specifies the Normal ACK and No ACK policies.

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

5.6.2 Configure WMM Settings

Step 1 [Log in to the web UI of the AP.](#)

Step 2 Navigate to **Wireless > WMM**.

Step 3 Select a wireless network radio band on which WMM is to be implemented.

Step 4 Select a WMM optimization mode as required.

Step 5 Change the parameters as required when the optimization mode is set to **Custom**.

Step 6 Click **Save**.

2.4 GHz 5 GHz

WMM Optimization Optimized for scenario with 1 - 10 users
 Optimized for scenario with more than 10 users
 Custom

No ACK

EDCA AP Parameter

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

EDCA STA Parameter

	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

Save Cancel

---End

Parameter description

Parameter	Description
WMM Optimization	<p>Specifies the WMM optimization modes supported by the AP:</p> <ul style="list-style-type: none"> - Optimized for scenario with 1 - 10 users: If 10 or less clients are connected to the AP, you are recommended to select this mode to obtain higher client throughput. - Optimized for scenario with more than 10 users: If more than 10 clients are connected to the AP, you are recommended to select this mode to ensure client connectivity. - Custom: This mode enables you to set the WMM EDCA parameters for manual optimization.

Parameter	Description
No ACK	<p>Available when WMM Optimization is set to Custom.</p> <p>No Acknowledgement (No ACK): When this policy is used, the recipient will not acknowledge received packets during wireless packet exchange. It is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.</p> <ul style="list-style-type: none">- If the check box is selected, the No ACK policy is adopted.- If the check box is deselected, the Normal ACK policy is adopted.
EDCA Parameters	For details, refer to EDCA parameters .

5.7 Access control

5.7.1 Overview

[Log in to the web UI of the AP](#), and navigate to **Wireless > Access Control**, you can 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:

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

5.7.2 Configure access control

Step 1 [Log in to the web UI of the AP](#).

Step 2 Navigate to **Wireless > Access Control**. Choose a wireless network radio band on which access control is to be implemented.

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

Step 4 Enable the **Access Control** function.

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

Step 6 Enter the MAC addresses of the wireless devices to which the rule applies. Then click **Add**.



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

Step 7 Click **Save**.

2.4 GHz 5 GHz

SSID

Access Control


Mode Blacklist Whitelist

MAC Address

ID	MAC Address	Status	Operation
No data			

---End

Parameter description

Parameter	Description
SSID	Specifies the SSID on which the MAC address access control is implemented.
Access Control	Specifies whether to enable the Access Control function.
Mode	<ul style="list-style-type: none"> - Blacklist: Clients with MAC addresses on the access control list cannot access the wireless network of AP. - Whitelist: Client with MAC addresses on the access control list can access the wireless network of AP.
MAC Address	Specifies the MAC address of client.
Add	Used to manually add the device with the MAC address you specified to the access control list.
Add Online Devices	Used to add the online wireless clients to the access control list conveniently.
Status	Specifies the status of the rule. You can enable or disable it as required.
Operation	Used to click  to delete the rule.

5.7.3 Example of configuring access control

Networking requirements

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

The Access Control function of the AP is recommended. The members have three wireless devices whose MAC addresses are **D8:38:0D:00:00:01**, **D8:38:0D:00:00:02**, and **D8:38:0D:00:00:03**.

Procedures

Step 1 [Log in to the web UI of the AP.](#)

Step 2 Navigate to **Wireless > Access Control > 5 GHz**.

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

Step 4 Enable **Access Control** function.

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

Step 6 Enter **D8:38:0D:00:00:01** in the **MAC Address** text box and click **Add**. Repeat the step to add **D8:38:0D:00:00:02** and **D8:38:0D:00:00:03** as well.

Step 7 Click **Save**.

2.4 GHz 5 GHz

SSID: VIP

Access Control:

Mode: Blacklist Whitelist

MAC Address:

ID	MAC Address	Status	Operation
1	D8:38:0D:00:00:01	<input checked="" type="checkbox"/> Enable	<input type="button" value="Delete"/>
2	D8:38:0D:00:00:02	<input checked="" type="checkbox"/> Enable	<input type="button" value="Delete"/>
3	D8:38:0D:00:00:03	<input checked="" type="checkbox"/> Enable	<input type="button" value="Delete"/>

---End

Verification

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

5.8 Advanced settings

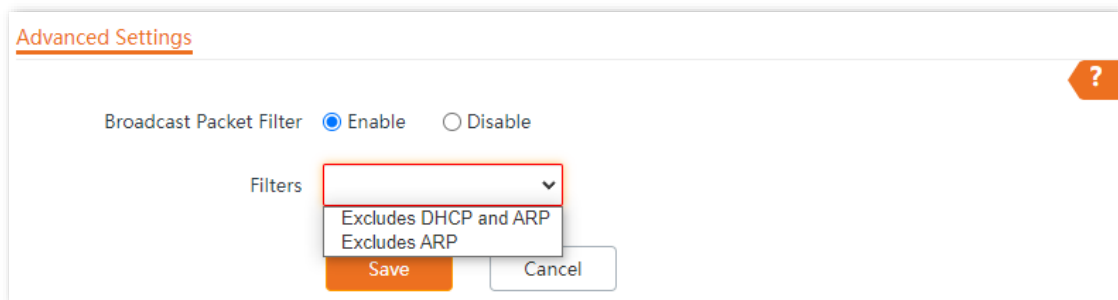
5.8.1 Overview

[Log in to the web UI of the AP](#), and navigate to **Wireless > Advanced Settings**, you can set the broadcast packet filter function of the AP.

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.

5.8.2 Configure advanced settings

- Step 1** [Log in to the web UI of the AP](#).
- Step 2** Navigate to **Wireless > Advanced Settings**.
- Step 3** Change the parameters as required.
- Step 4** Click **Save**.



---End

Parameter description

Parameter	Description
Broadcast Packet Filter	Specifies whether to enable the Broadcast Packet Filter function. If this function is enabled, the AP can reduce air interface resources usage and ensure the bandwidth for business data transfer.
Filters	Used to select a mode after you enable the Broadcast Packet Filter function. <ul style="list-style-type: none"> - Excludes DHCP and ARP: Filter out all broadcast or multicast data except DHCP and ARP packets. - Excludes ARP: Filter out all broadcast or multicast data except ARP packets.

5.9 QVLAN settings

5.9.1 Overview

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

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

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

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

5.9.2 Configure QVLAN

Step 1 [Log in to the web UI of the AP.](#)

Step 2 Navigate to **Wireless > QVLAN Settings**.

Step 3 Enable the **QVLAN** function.

Step 4 Change the parameters as required. Generally, you only need to change the **2.4 GHz SSID VLAN ID** and **5 GHz SSID VLAN ID** settings.

Step 5 Click **Save**.

QVLAN Settings ?

*** QVLAN**

PVID


Management VLAN

2.4 GHz SSID VLAN ID (1 to 4094)

5 GHz SSID VLAN ID (1 to 4094)

---End

Parameter description

Parameter	Description
QVLAN	Specifies whether to enable the QVLAN function of the AP. By default, it is disabled.
PVID	Specifies the default VLAN ID of the AP's trunk port.
Management VLAN	Specifies the ID of the AP management VLAN. After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
2.4 GHz SSID	Specify the currently enabled SSID(s) over the 2.4 GHz/5 GHz band of the AP, and the VLAN IDs corresponding to SSIDs.
5 GHz SSID	
VLAN ID	 TIP After the QVLAN function is enabled, the wireless ports corresponding to SSIDs function as access ports. The PVID of an access port is the same as its VLAN ID.

5.9.3 Example of configuring QVLAN settings

Networking requirements

An industrial park has the following wireless network coverage requirements:

- Guests are connected to VLAN2 and can access only the internet.
- Staffs are connected to VLAN3 and can access only the internal server.

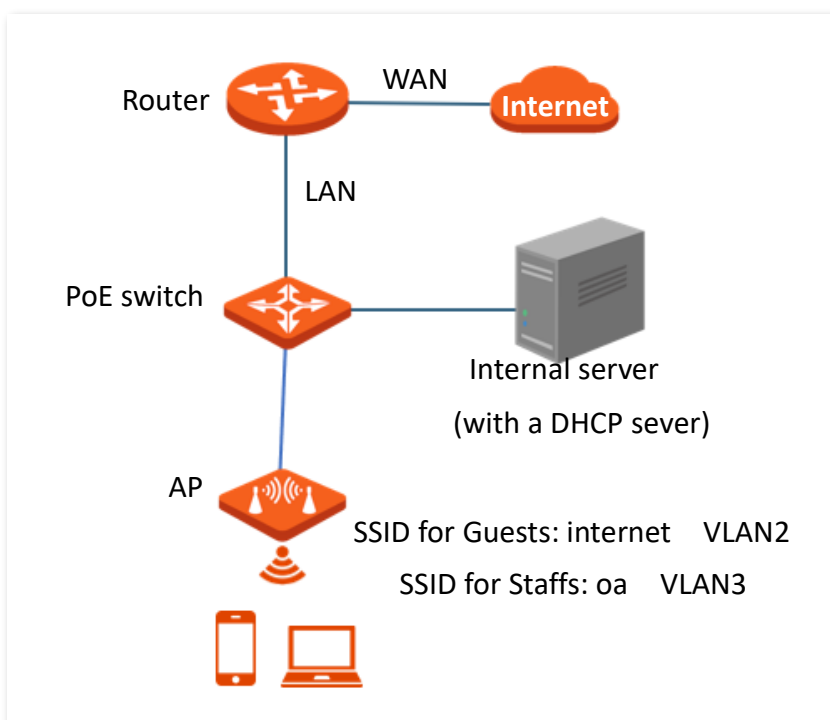
Solution

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



TIP

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



Procedures

I. Configure the AP

Step 1 [Log in to the web UI of the AP.](#)

Step 2 Navigate to **Wireless > QVLAN Settings**.

- Step 3** Enable the **QVLAN** function.
- Step 4** Modify the VLAN ID of the SSIDs at 2.4 GHz band. Set the VLAN ID of **internet** to **2** and the VLAN of **oa** to **3**.
- Step 5** Click **Save**.

QVLAN Settings

* QVLAN

PVID

Management VLAN

2.4 GHz SSID VLAN ID (1 to 4094)

* oa

* internet

5 GHz SSID VLAN ID (1 to 4094)

- Step 6** Click **OK** after confirming the prompted message.
Wait for the automatic reboot of the AP.

---End

II. Configure the PoE switch

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

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

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

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 internal server.

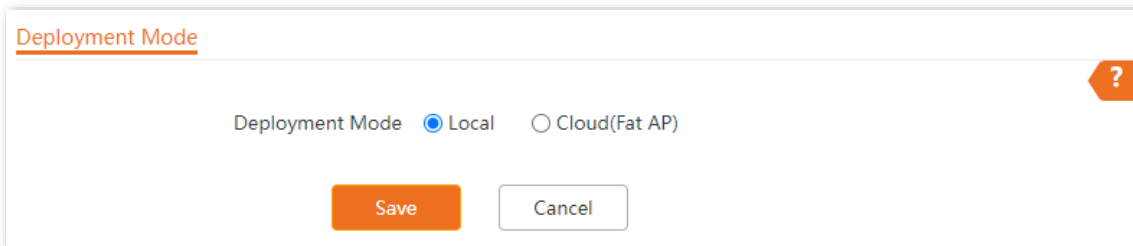
6 Advanced

6.1 Deployment mode

6.1.1 Overview

If a large number of APs are to be deployed in a network, it is recommended that you integrate a Tenda AC in order to achieve a unified AP management.

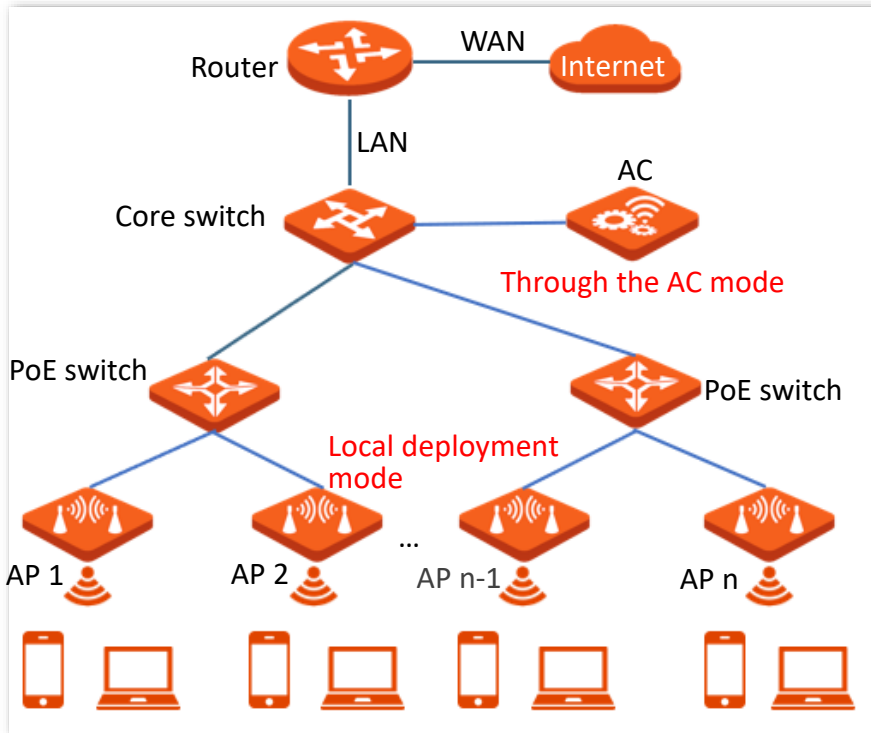
Unified AP management includes local deployment and cloud deployment. The default mode is local deployment mode.



The screenshot shows a dialog box titled "Deployment Mode" with a question mark icon in the top right corner. Inside the dialog, the text "Deployment Mode" is followed by two radio button options: "Local" (which is selected) and "Cloud(Fat AP)". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

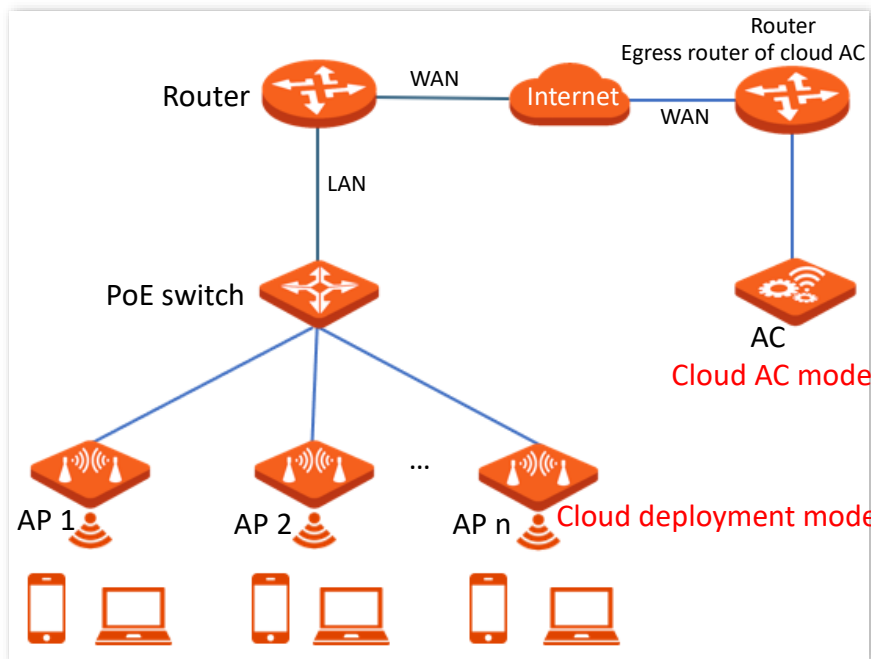
Local deployment

If the network is concentrated and involves a large number of APs, it is recommended that you adopt the local deployment mode to enable unified management by AC through the AC mode. See the following figure.



■ **Cloud deployment**

If the wireless network is dispersed and involves a large number of APs in total but these APs are scattered in small numbers, it is recommended that you adopt the cloud deployment mode in which ACs on the internet manage the scattered cloud APs in a unified manner through the cloud AC mode. See the following figure.



6.1.2 Configure deployment mode

[Log in to the web UI of the AP](#), and navigate to **Advanced > Deployment Mode**, you can change the deployment mode of AP.

Deployment Mode ?

Deployment Mode Local Cloud(Fat AP)

Device Name

Cloud AC Address

Cloud AC Management Port (Range: 1024 to 65535)

Cloud AC Upgrade Port (Range: 1024 to 65535)

Parameter description

Parameter	Description
Deployment Mode	<p>Specifies the deployment mode of AP. Local is selected by default.</p> <ul style="list-style-type: none"> - Local: AP can be managed only by AC on the LAN. - Cloud(Fat AP): AP can be managed only by the remote AC with the specified IP address on the internet or in other networks.
Device Name	<p>Specifies the name of the AP.</p> <p>When multiple APs with the same model exist in the network, different device names can help you differentiate them.</p>
Cloud AC Address	<p>Specifies the WAN IP address (must be a public IP address) of the egress router of the remote AC or the domain name bound by the IP address.</p>
Cloud AC Management Port	<p>Specifies the available port of the egress router of the remote AC, which is used to manage the AP.</p>
Cloud AC Upgrade Port	<p>Specifies the available port of the egress router of the remote AC, which is used to upgrade the AP.</p>

6.2 Traffic control


6.2.1 Overview

The traffic control function allows you to set limits on the internet speed of clients to guarantee a proper allocation of limited broadband resources.

By default, the traffic control function is disabled. If you want to use this function, [log in to the web UI of the AP](#) and configure it on the **Advanced > Traffic Control** page.

Parameter description

Parameter	Description
Traffic Control	<p>Specifies whether to enable the Traffic Control function.</p> <ul style="list-style-type: none"> - Disable: The Traffic Control function is disabled. - Manual: The Traffic Control function is enabled. The network administrator manually sets SSID and the maximum upload/download rate of user devices to limit the total bandwidth of SSID and evenly allocate bandwidth to users. In this way, if multiple SSIDs are enabled, and a user network with a lower priority (such as guest network) occupies an excessively high internet speed or a user occupies too much bandwidth, such circumstances as excessively low internet speed or even internet unavailability for other users will not occur.
Radio Band	Specifies the radio band of the wireless network on which you manually set a traffic control rule.
SSID	Specifies the name of the wireless network on which you manually set a traffic control rule.
SSID Max. Upload Rate	Specify the maximum upload or download rate allowed for a wireless network.
SSID Max. Download Rate	<p>If you leave it blank, the maximum upload or download rate of the target wireless network are not limited.</p> <p>It is available only when you manually set a traffic control rule.</p>

Parameter	Description
Client Max. Upload Rate	Specify the maximum upload or download rate allowed for every user device connected to the target wireless network.
Client Max. Download Rate	If you leave it blank, the maximum upload or download rate of every user device connected to the target wireless network are not limited. It is available only when you manually set a traffic control rule.
Operation	Used to click  to set the maximum upload or download rate allowed for the target wireless network and the maximum upload or download rate allowed for every user device connected to the target wireless network. It is available only when you manually set a traffic control rule.

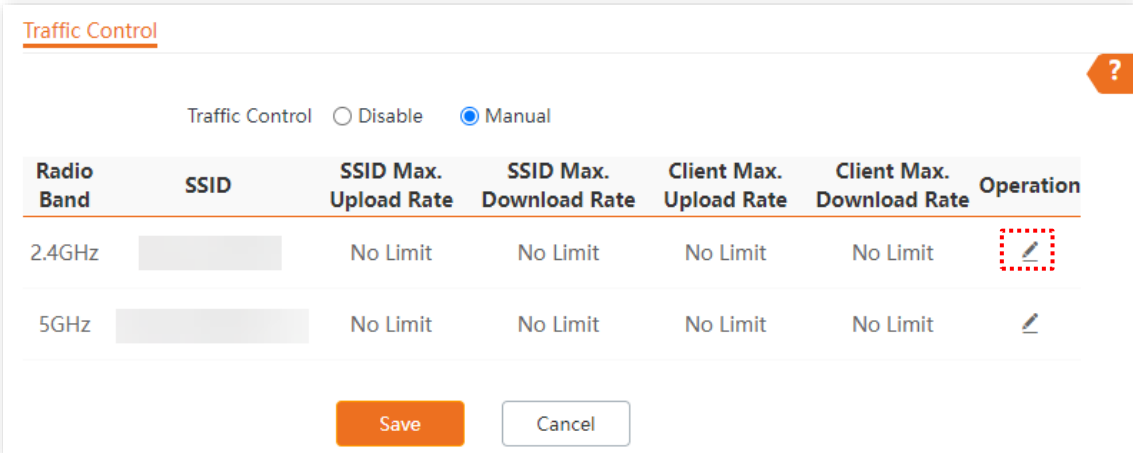
6.2.2 Configure traffic control

Step 1 [Log in to the web UI of the AP.](#)



Step 2 Navigate to **Advanced > Traffic Control.**

Step 3 Set **Traffic Control** to **Manual.**

Step 4 Click  on the row where the wireless network to be controlled resides.



Traffic Control Disable Manual

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

Save Cancel

Step 5 Set the maximum upload or download rate allowed for the wireless network and the maximum upload or download rate allowed for every user device connected to the wireless network.



Blank spaces indicate that the maximum upload or download rate allowed for the wireless network or the maximum upload or download rate allowed for every user device connected to the wireless network is not limited.

Step 6 Click **Add**.

SSID Traffic Control Policy

Radio Band 2.4GHz

SSID

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

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

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

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

Add Cancel

---End

6.3 SNMP

6.3.1 Overview

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

SNMP 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

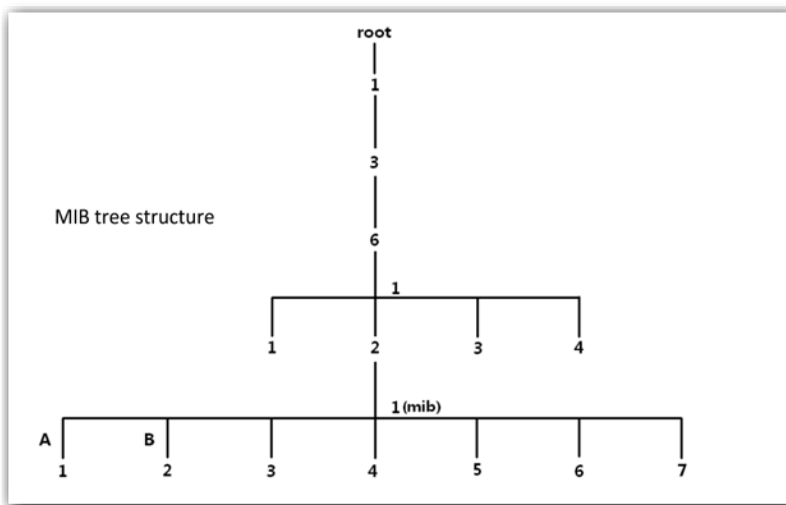
The AP is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism. Community name is used to define the relationship between an SNMP agent and an SNMP manager. If the community name contained in an SNMP packet is rejected by a device, the

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.



6.3.2 Configure SNMP agent

[Log in to the web UI of the AP](#), and navigate to **Advanced > SNMP**, you can configure the SNMP agent function of the AP.

Parameter description

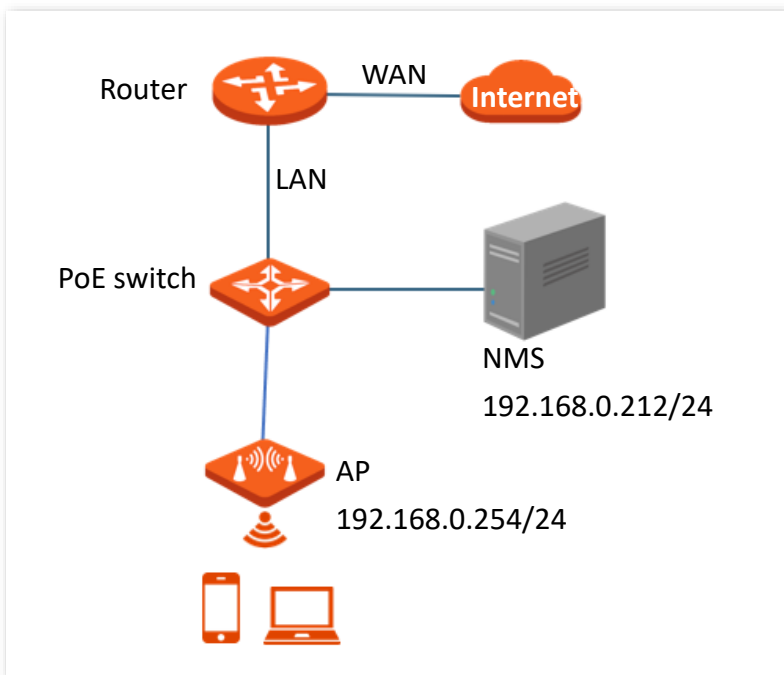
Parameter	Description
SNMP Agent	Specifies whether to enable the SNMP Agent function of the AP. By default, it is disabled. An SNMP manager and the SNMP agent can communicate with each other only when their SNMP versions are the same. Currently, the SNMP agent function of the AP supports SNMP V1 and SNMP V2C.
Administrator	Specifies the name of the administrator of the AP. You can modify the administrator's name as required.
Device Name	Specifies the device name of the AP. You can modify it as required.  TIP It is recommended to modify the device name so that you can identify your AP easily when managing the AP using SNMP.
Location	Specifies the location where the AP is used. You can modify the location as required.
Read Community	Specifies the read password shared between SNMP managers and the SNMP agent. 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	Specifies the read/write password shared between SNMP managers and the SNMP agent. 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.

6.3.3 Example of configuring the SNMP function

Networking requirements

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



Procedures

I. Configure the AP

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

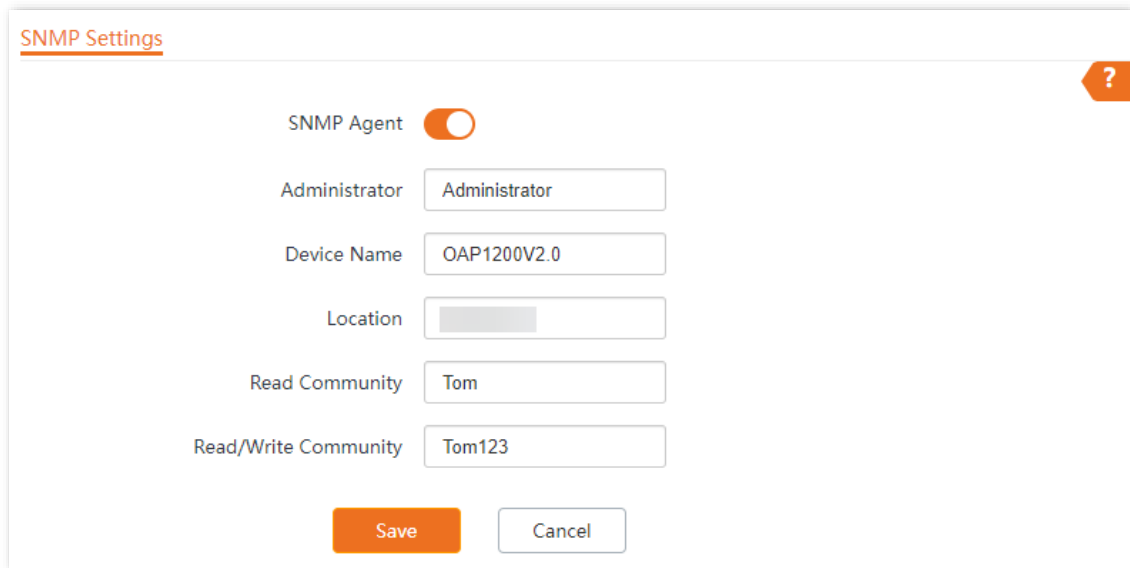
Step 1 [Log in to the web UI of the AP.](#)

Step 2 Navigate to **Advanced > SNMP**.

Step 3 Enable the **SNMP Agent** function.

Step 4 Set the SNMP parameters of **Administrator**, **Device Name**, **Location**, **Read Community** and **Read/Write Community**.

Step 5 Click **Save**.



The image shows a configuration window titled "SNMP Settings" with a question mark icon in the top right corner. The settings are as follows:

SNMP Agent	<input checked="" type="checkbox"/>
Administrator	Administrator
Device Name	OAP1200V2.0
Location	
Read Community	Tom
Read/Write Community	Tom123

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

II. 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

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

6.4 Cloud maintenance

6.4.1 Overview

CloudFi is a cloud platform provided by Tenda, which can uniformly manage Tenda devices that support Tenda ClouFi cloud management.

After an AP is added to the Tenda ClouFi cloud platform, you can view and configure the relevant parameters of the AP on the Tenda ClouFi cloud platform, or locally log in to the web UI of the AP to view and configure it.

[Log in to the web UI of the AP](#), and navigate to **Advanced > Cloud Maintenance**, you can add the AP to the Tenda ClouFi cloud platform.

The cloud maintenance function is disabled by default.

Parameter description

Parameter	Description
Cloud Maintenance	Specifies whether to enable the Cloud Maintenance function of the AP.
Management Mode	<p>Specifies the two modes under which your AP is managed.</p> <ul style="list-style-type: none"> - Cloud Configuration: Applicable to scenarios that require unified configuration and maintenance through the Tenda ClouFi cloud platform. In this mode, all configuration information of the device is delivered by the Tenda ClouFi cloud platform. - Local Device Configuration: Applicable to scenarios that require unified status monitoring through the Tenda ClouFi cloud platform. In this mode, all configurations of the device are completed on its own web UI, and the information is reported to the Tenda ClouFi cloud platform.

Parameter	Description
Unique Cloud Code	Specifies the Tenda ClouFi cloud platform account associated with the device. You can obtain this code on the web UI of the Tenda ClouFi cloud platform https://cloudfi.tendacn.com . Click Add in the upper right corner and obtain it from the drop-down menu.
Report	Specifies whether to enable the Report function. If this function is enabled, parameter information of your APs is reported to the Tenda ClouFi cloud platform and you can manage and maintain your APs on the platform. This function is disabled by default.

6.4.2 Example of configuring cloud maintenance

Manage AP through the web UI of Tenda ClouFi cloud platform

Networking requirements

The AP can be managed through the Tenda ClouFi cloud platform, and all its configuration information is delivered by the Tenda ClouFi cloud platform

Procedures



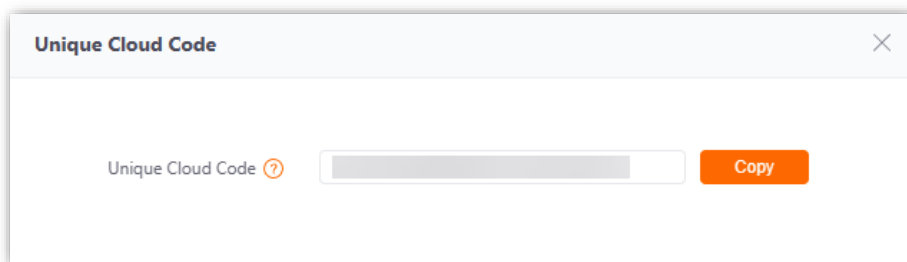
TIP Before configuring the cloud maintenance function of the AP, make sure that the AP is successfully connected to the internet.

I. Log in to Tenda ClouFi cloud platform and obtain unique cloud code

Step 1 On a computer that has connected to the internet, start a web browser, visit <https://cloudfi.tendacn.com>, and log in to Tenda ClouFi cloud platform.

Step 2 Click **Add** at the upper right corner and select **Unique Cloud Code**.

Step 3 Click **Copy** to copy the **Unique Cloud Code**.



---End

II. Enable and configure the cloud maintenance function of the AP

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Advanced > Cloud Maintenance**.
- Step 3** Enable the **Cloud Maintenance** function.
- Step 4** Set the parameters of the cloud maintenance function.
1. Set **Management Mode** to **Cloud Configuration**.
 2. Paste the **Unique Cloud Code** copied in [I-3](#) in the input box.
 3. Enable the **Report** function.
- Step 5** Click **Save**.

Cloud Maintenance

Cloud Maintenance

Cloud Management Type

Unique Cloud Code

Unique Cloud Code is used to associate the device to your Tenda cloud platform account. You can obtain this code on Tenda CloudFi web UI (<https://cloudfi.tendacn.com>)

Report Enable

If disabled, the device cannot be managed and maintained over the cloud server.

---End

III. Log in to Tenda ClouFi cloud platform and add AP to the project

- Step 1** On a computer that has connected to the internet, start a web browser, visit <https://cloudfi.tendacn.com>, and log in to Tenda ClouFi cloud platform.
- Step 2** Click **Add** at the upper right corner and select **Device-joining Alert** from the drop-down list menu.
- Step 3** Locate this AP and add it to your project.

---End

Verification

After the configuration is completed, the AP can be managed through the web UI of the Tenda ClouFi cloud platform, and all its configuration information is delivered by the Tenda ClouFi cloud platform.

7 Tools

7.1 Date & Time

[Log in to the web UI of the AP](#), and navigate to **Tools > Date & Time**, you can set the [system time](#) and [login timeout interval](#) of your AP.

7.1.1 Configure system time

[Log in to the web UI of the AP](#), and navigate to **Tools > Date & Time > System Time**, you can set the system time of your AP.

To make the time-related functions effective, ensure that the system time of the AP is set correctly. The AP supports [Sync with Internet Time](#) and [Manual](#) to correct the system time. The default value is **Manual**.



Sync with internet time

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

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

Parameter description

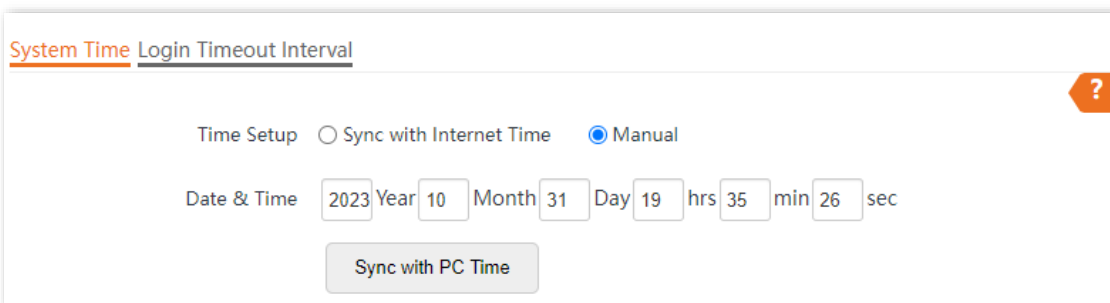
Parameter	Description
Time Setup	Specifies the modes to set the system time.

Parameter	Description
Sync Interval	<p>Specifies the interval at which the AP will automatically synchronize with a time server of the internet.</p> <p> TIP</p> <p>It is available only when Sync with Internet Time is chosen.</p>
Time Zone	<p>Specifies the standard time zone of the region in which the AP locates.</p> <p> TIP</p> <p>It is available only when Sync with Internet Time is chosen.</p>

Manual

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

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



System Time Login Timeout Interval

Time Setup Sync with Internet Time Manual

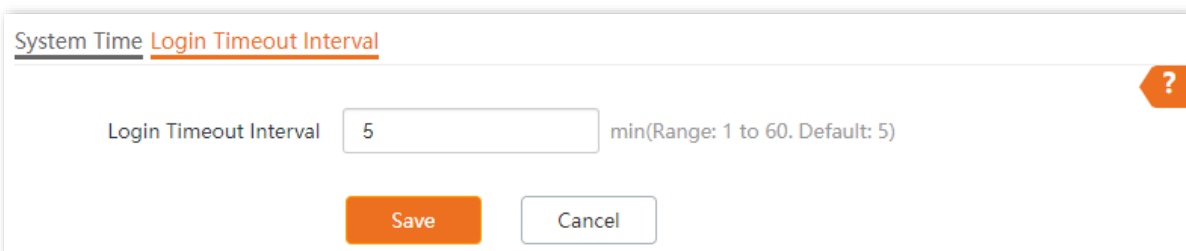
Date & Time 2023 Year 10 Month 31 Day 19 hrs 35 min 26 sec

Sync with PC Time

7.1.2 Login timeout interval

[Log in to the web UI of the AP](#), and navigate to **Tools > Date & Time > Login Timeout Interval**, you can modify the login timeout interval. The default login timeout interval is **5** minutes.

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.



System Time Login Timeout Interval

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

Save Cancel

7.2 Maintenance

[Log in to the web UI of the AP](#), and navigate to **Tools > Maintenance > Maintenance**, you can [reboot](#) and [reset](#) AP, [upgrade firmware](#), [back up or restore settings](#), and [control LED indicator](#).

7.2.1 Reboot

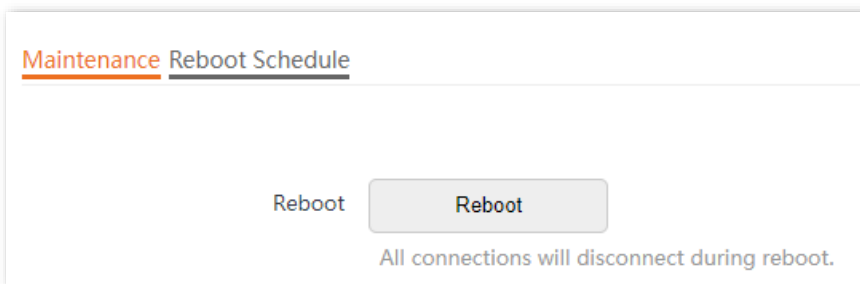


Rebooting the AP disconnects all connections. You are recommended to reboot the AP in spare time.

Manual reboot

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

Navigate to **Tools > Maintenance > Maintenance** and click **Reboot**.



Reboot schedule

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

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

Configure the AP to reboot at an Interval



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

Step 1 [Log in to the web UI of the AP](#).

Step 2 Navigate to **Tools > Maintenance > Reboot Schedule**.

- Step 3** Enable the **Reboot Schedule** function.
- Step 4** Set **Type** to **Reboot Interval**.
- Step 5** Set **Interval** to a value in minutes, which is **1440** in this example.
- Step 6** Click **Save**.

Maintenance Reboot Schedule

Reboot Schedule

Type

Interval min(Range: 10 to 7200)

---End

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

Configure the AP to reboot at a specified time

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Tools > Maintenance > Reboot Schedule**.
- Step 3** Enable the **Reboot Schedule** function.
- Step 4** Set **Type** to **Reboot Schedule**.
- Step 5** Select the day or days when the AP reboots, which is **Monday to Friday** in this example.
- Step 6** Set the time when the AP reboots, which is **3:00** in this example.
- Step 7** Click **Save**.

Maintenance Reboot Schedule

Reboot Schedule

Type

Reboot On Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday Every Day

Reboot At (Default:3:00)

---End

After the configurations, the AP will automatically reboot at **3:00** every Monday to Friday.

7.2.2 Reset

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



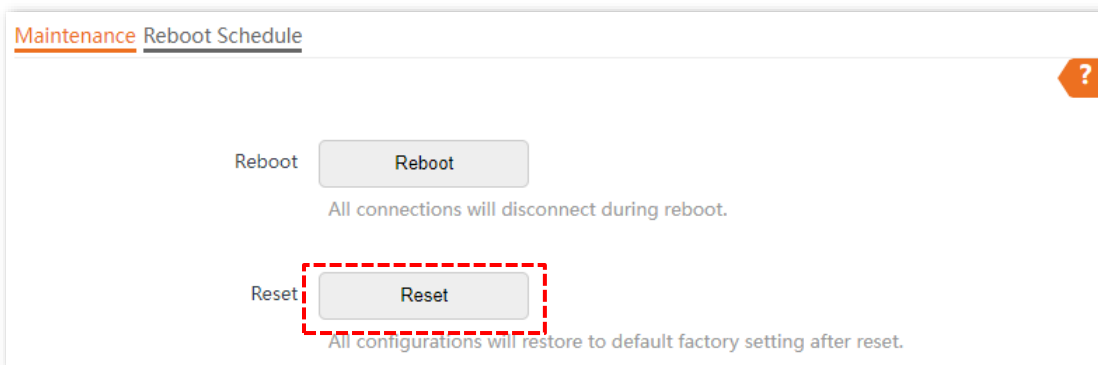
- When the factory settings are restored, your configuration is lost. Therefore, you need to reconfigure the AP to reconnect to the internet. Restore the factory settings of the AP only when necessary.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.
- After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

When the AP is idle, hold down the **Reset** button for about 8 seconds, and release it when the LED indicator turns off. The AP is reset successfully when the LED indicator starts to blink white.

Method 2

[Log in to the web UI of the AP](#), navigate to **Tools > Maintenance > Maintenance** and click **Reset**.



7.2.3 Upgrade firmware

This function allows you to upgrade the firmware of the AP for more functions and higher stability.



To ensure a correct upgrade and avoid damage:

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

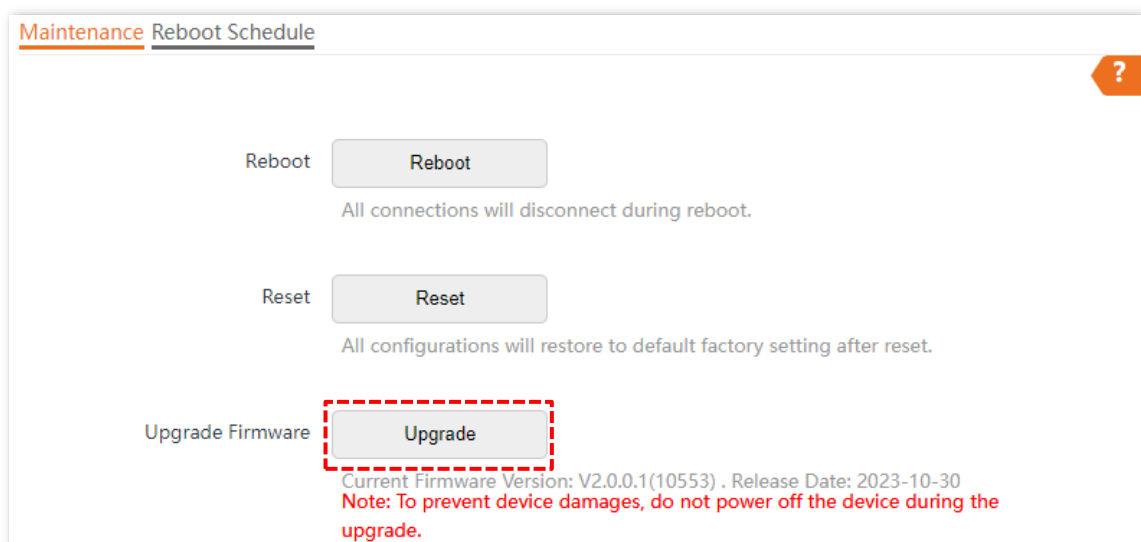
Procedures

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

Step 2 [Log in to the web UI of the AP.](#)

Step 3 Navigate to **Tools > Maintenance > Maintenance**.

Step 4 Click **Upgrade**.



Step 5 Choose the upgrade file in the pop-up window.

---End

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



After the firmware is upgraded, it is 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.

7.2.4 Backup/Restore

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

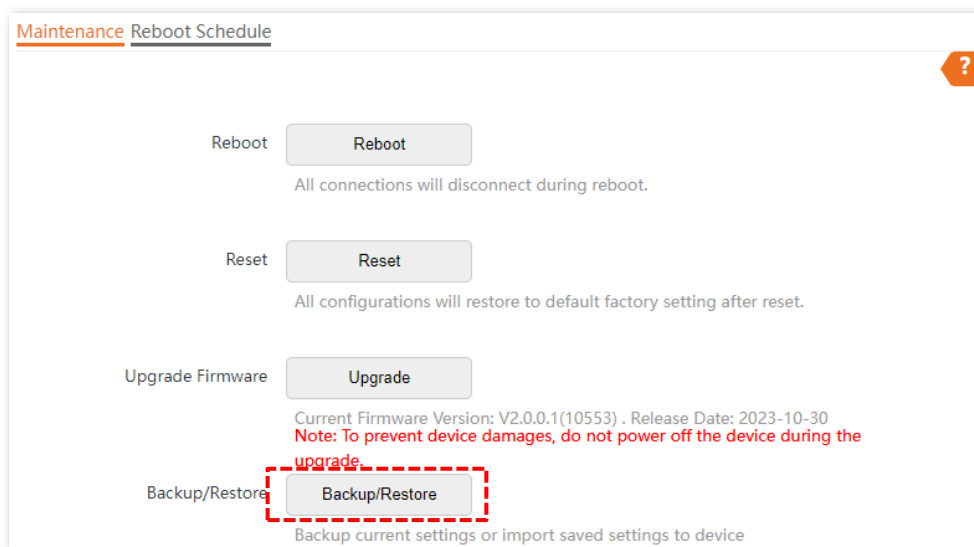
If the AP enters the optimum condition after you greatly change the configuration of the AP, you are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the AP.



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

Back up the current configuration

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Tools > Maintenance > Maintenance.**
- Step 3** Click **Backup/Restore.**



- Step 4** Click **Backup.**



---End

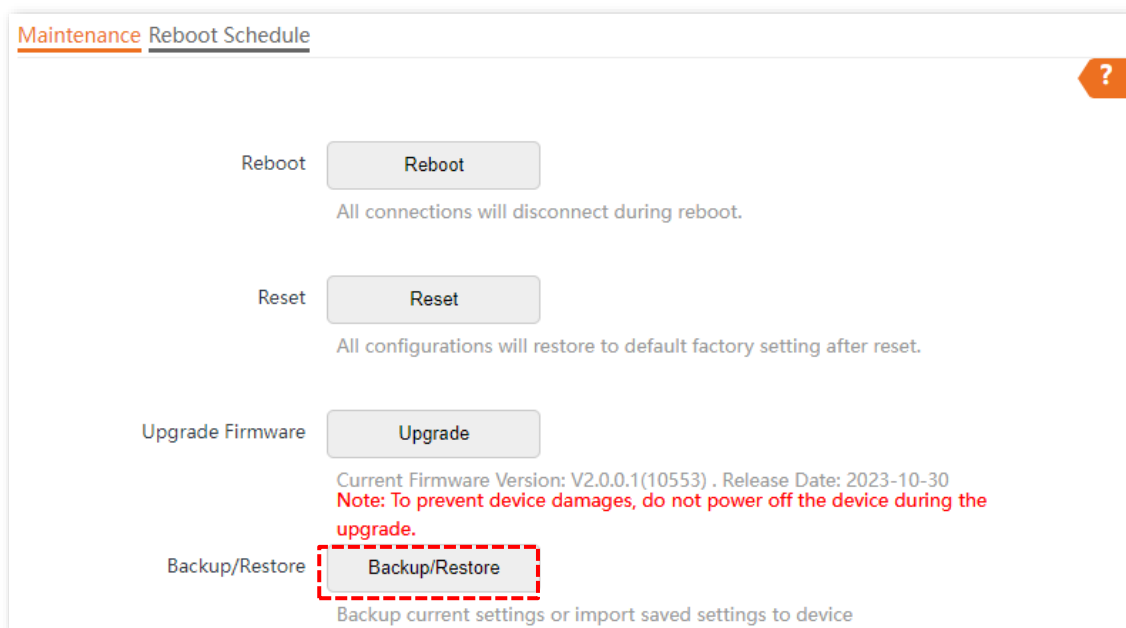
A configuration file named **APCfm.cfg** will be downloaded.



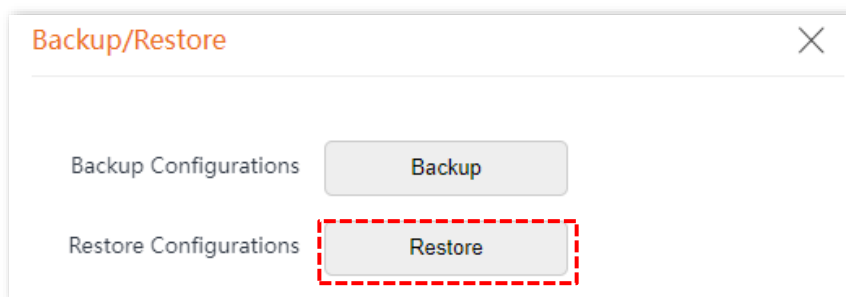
If the prompt “This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?” appears, click **Keep**.

Restore the configuration

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Tools > Maintenance > Maintenance**.
- Step 3** Click **Backup/Restore**.



- Step 4** Click **Restore**.



- Step 5** Choose the configuration file you backed up.

---End

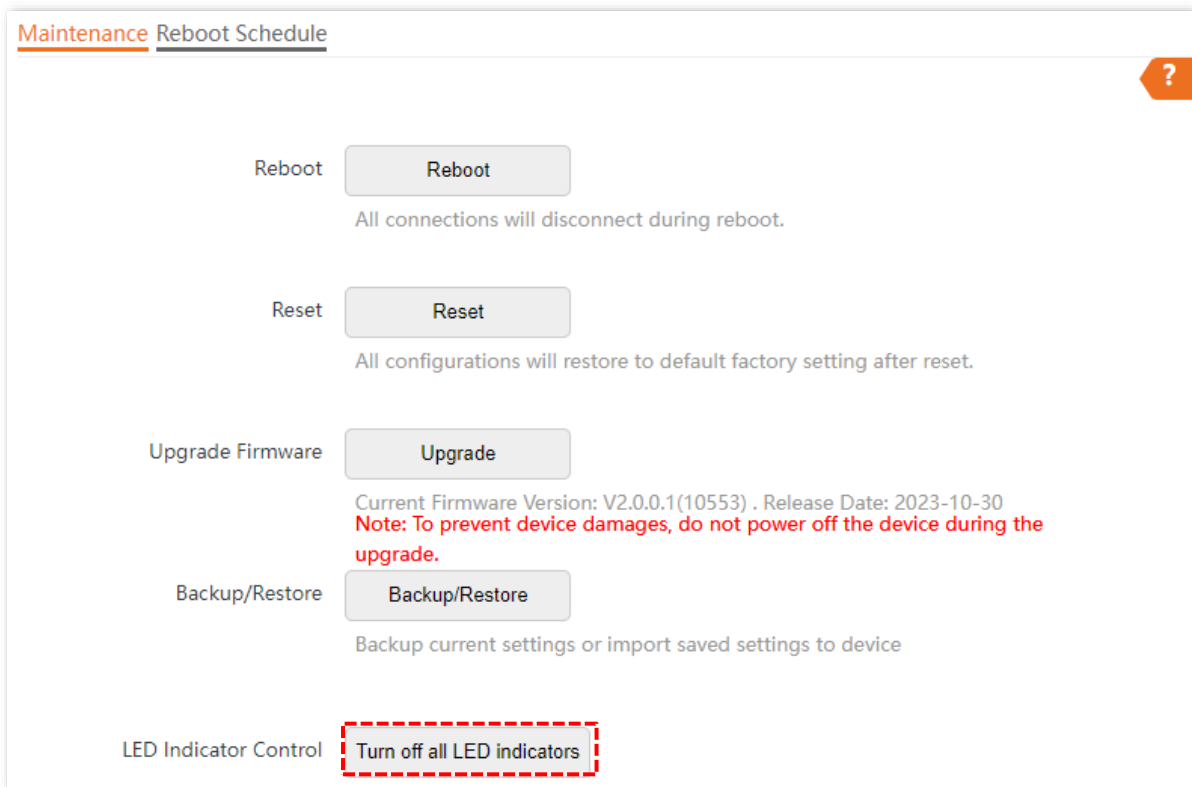
The AP restores the configurations successfully when the progress bar is done.

7.2.5 LED indicator control

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

Turn off the LED indicator

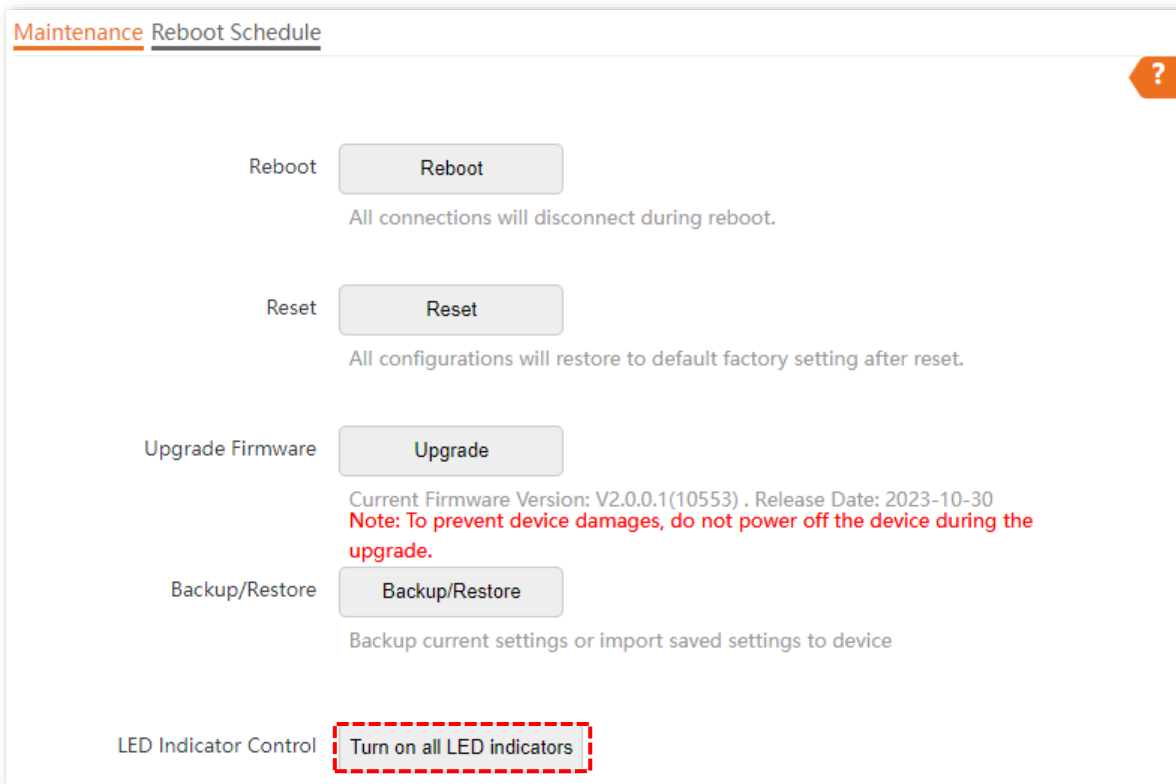
[Log in to the web UI of the AP](#), and navigate to **Tools > Maintenance > Maintenance** and click **Turn off all LED indicators**.



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

Turn on the LED indicator

[Log in to the web UI of the AP](#), and navigate to **Tools > Maintenance > Maintenance**, and click **Turn on all LED indicators**.



After the configuration is completed, the LED indicator is turned on and you can judge the working status of the AP.

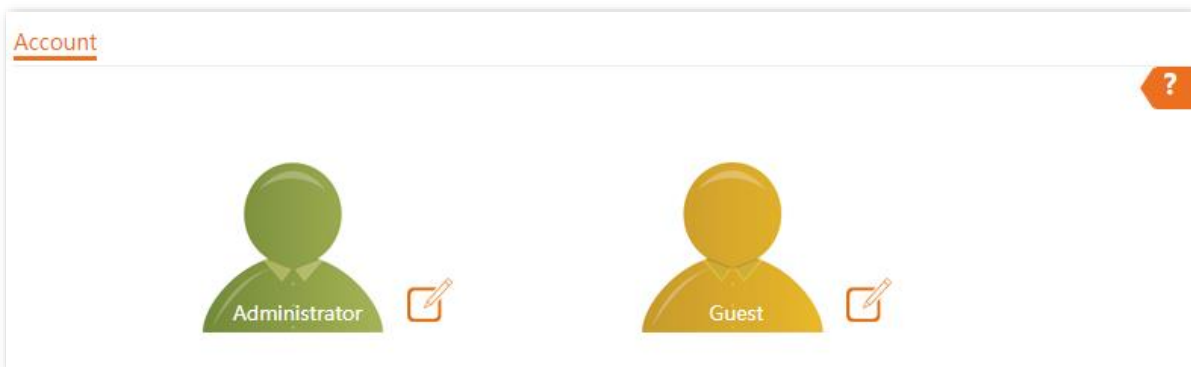
7.3 Account

7.3.1 Overview


[Log in to the web UI of the AP](#), and navigate to **Tools > Account**, you can modify the information of the login account to keep unauthorized users from entering the web UI and modifying configurations, thus protecting the wireless network.

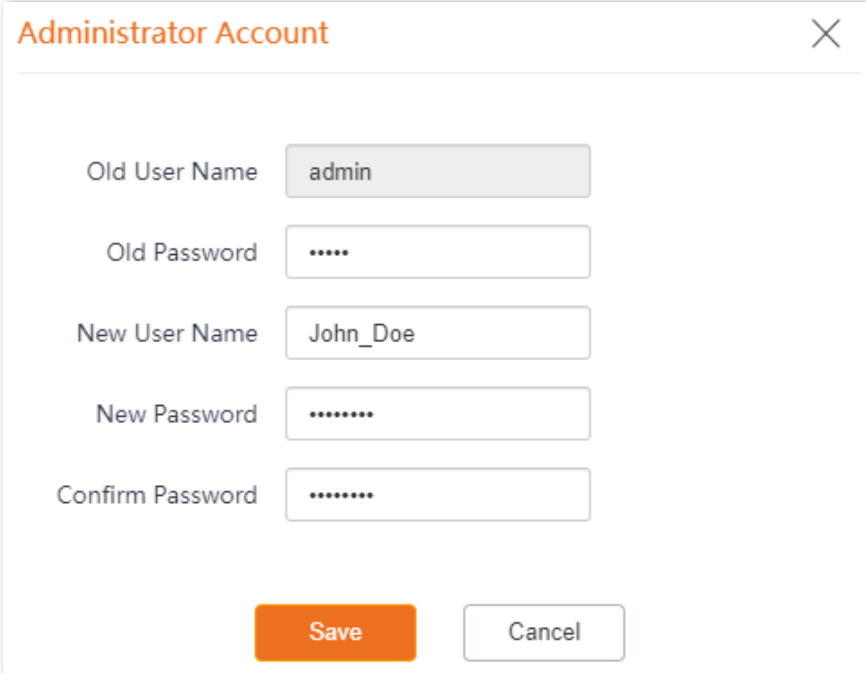
AP supports two account types: **Administrator** and **Guest**. The difference between them lies in their permissions.

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



7.3.2 Modify the password and user name of login account

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Tools > Account**.
- Step 3** Click  beside the account to be modified.
- Step 4** Enable the **Guest Account** first. It is available only when the account to be modified is a **Guest**. Otherwise, go to the next step.
- Step 5** Enter the current password in **Old Password**.
- Step 6** Enter the new account name in **New User Name**, which is **John_Doe** in this example.
- Step 7** Enter the new password in **New Password**.
- Step 8** Enter again the new password in **Confirm Password**.
- Step 9** Click **Save**.



The image shows a dialog box titled "Administrator Account" with a close button (X) in the top right corner. The dialog contains five input fields and two buttons at the bottom. The fields are: "Old User Name" with the value "admin", "Old Password" with five asterisks, "New User Name" with the value "John_Doe", "New Password" with seven asterisks, and "Confirm Password" with seven asterisks. The "Save" button is orange, and the "Cancel" button is white with a grey border.

---End

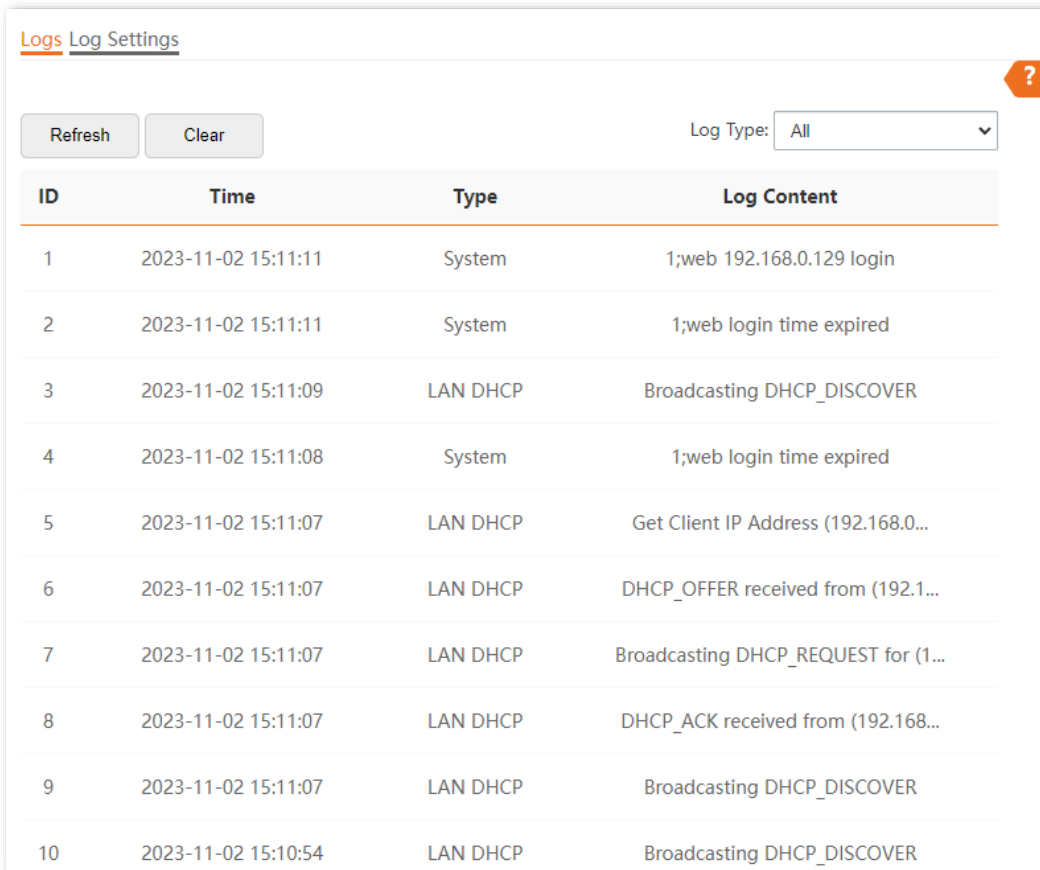
Then you will be redirected to the login page. Enter the new password and click **Login** to log in to the AP.

7.4 System log

7.4.1 View system logs

[Log in to the web UI of the AP](#), and navigate to **Tools > System Log > Logs**, you can view system 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.



The screenshot shows the 'Logs' page in the web UI. At the top, there are tabs for 'Logs' and 'Log Settings'. Below the tabs are 'Refresh' and 'Clear' buttons, and a 'Log Type' dropdown menu set to 'All'. The main content is a table with the following data:

ID	Time	Type	Log Content
1	2023-11-02 15:11:11	System	1;web 192.168.0.129 login
2	2023-11-02 15:11:11	System	1;web login time expired
3	2023-11-02 15:11:09	LAN DHCP	Broadcasting DHCP_DISCOVER
4	2023-11-02 15:11:08	System	1;web login time expired
5	2023-11-02 15:11:07	LAN DHCP	Get Client IP Address (192.168.0...
6	2023-11-02 15:11:07	LAN DHCP	DHCP_OFFER received from (192.1...
7	2023-11-02 15:11:07	LAN DHCP	Broadcasting DHCP_REQUEST for (1...
8	2023-11-02 15:11:07	LAN DHCP	DHCP_ACK received from (192.168...
9	2023-11-02 15:11:07	LAN DHCP	Broadcasting DHCP_DISCOVER
10	2023-11-02 15:10:54	LAN DHCP	Broadcasting DHCP_DISCOVER

To ensure that the logs are recorded correctly, verify that the system time of the AP is correct. You can [correct the system time of the AP](#) on the **Tools > Date & Time > System Time** page.

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 restored, or the factory settings are restored.

7.4.2 Log settings

[Log in to the web UI of the AP](#), and navigate to **Tools > System Log > Logs Settings**, you can set the number of logs to be displayed and configure log servers.

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

Logs [Log Settings](#)



Log Service

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

ID	Log Server IP Address	Log Server Port	Status	Operation
No data				

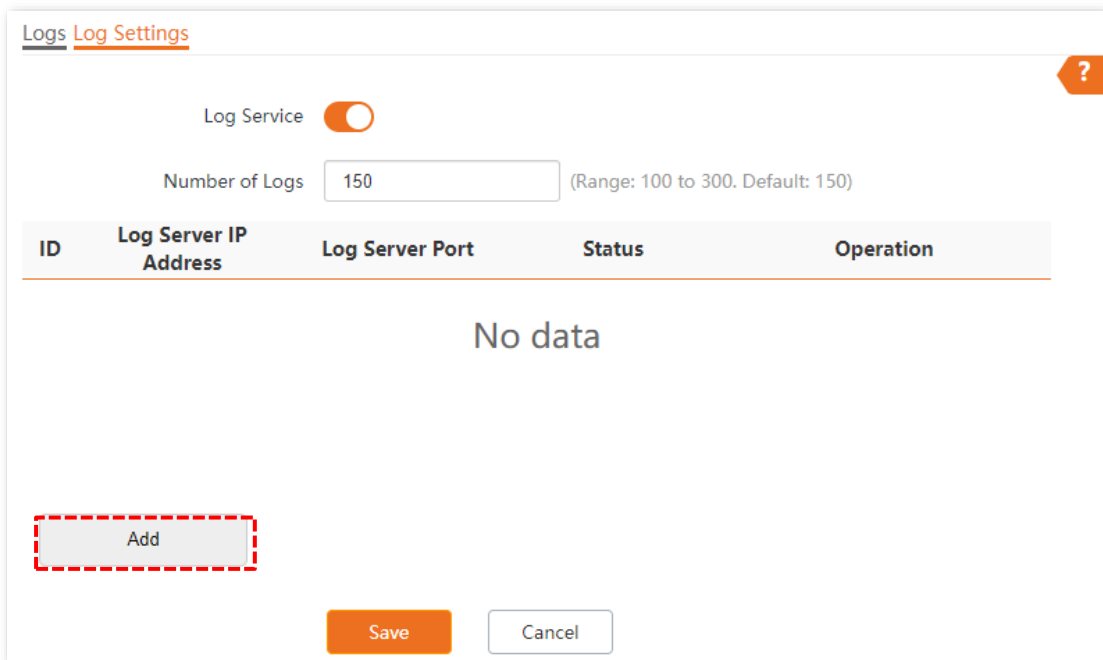
Parameter description

Parameter	Description
Log Service	Specifies whether to enable the Log Service function. This function is disabled by default. You can modify the number of logs to be displayed and configure log server only if the Log Service function is enabled.
Number of Logs	Specifies the largest number of logs that can be displayed on the web UI.
ID	Specifies the ID number of logs.
Log Server IP Address	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 Default Gateway of the AP on the Internet Settings > LAN Setup page to enable the AP to access the log server.

Parameter	Description
Log Server Port	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	Specifies the status of the log server rule.
Operation	Specifies the operations you can perform on the log server: <ul style="list-style-type: none"> - Click  to modify the IP address, port, or status of the log server. - Click  to delete the target log server.
<input type="button" value="Add"/>	Used to click it to add a log server.

Add the log server

- Step 1** [Log in to the web UI of the AP.](#)
- Step 2** Navigate to **Tools > System Log > Log Settings.**
- Step 3** Enable the **Log Service** function.
- Step 4** Click **Add.**



Logs [Log Settings](#)

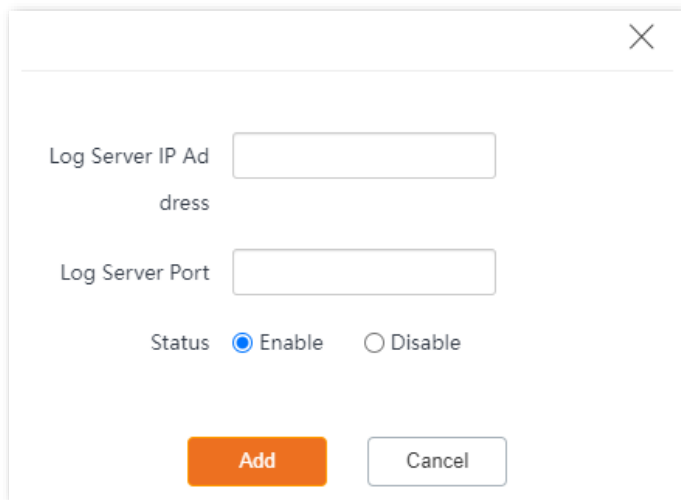
Log Service

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

ID	Log Server IP Address	Log Server Port	Status	Operation
No data				

- Step 5** Perform the following procedures:
1. Set **Log Server IP Address** to the IP address of the log server.
 2. Set **Log Server Port** to the UDP port number used to send and receive system logs. The default port number **514** is recommended.
 3. Set **Status** to **Enable**.

4. Click **Add**.



A screenshot of a dialog box with a close button (X) in the top right corner. The dialog contains two text input fields: "Log Server IP Address" and "Log Server Port". Below the input fields, there is a "Status" section with two radio buttons: "Enable" (which is selected) and "Disable". At the bottom of the dialog, there are two buttons: "Add" (highlighted in orange) and "Cancel".

Step 6 Click **Save**.

---End

7.5 Diagnostic tool

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

Procedures

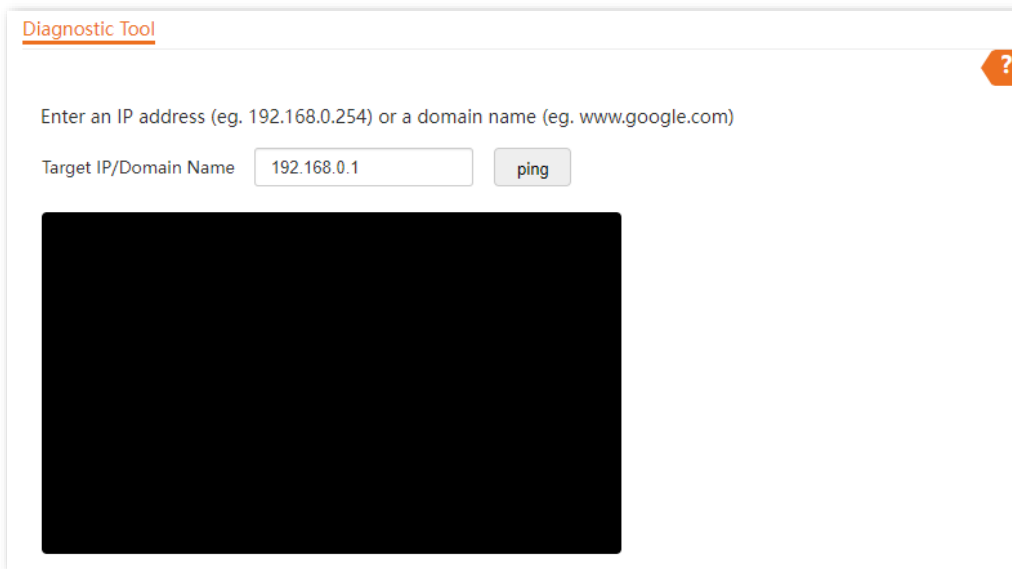
The link to **192.168.0.1** is used as an example.

Step 1 [Log in to the web UI of the AP.](#)

Step 2 Navigate to **Tools > Diagnostic Tool**.

Step 3 Enter the IP address or domain name to be pinged in the **Target IP/Domain Name** text box, which is **192.168.0.1** in this example.

Step 4 Click **ping**.



Diagnostic Tool

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

Target IP/Domain Name

[Large black rectangular box for results]

---End

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

Diagnostic Tool



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

Target IP/Domain Name

```
Ping 192.168.0.1(192.168.0.1):56 data bytes
64 bytes from 192.168.0.1: seq=0 ttl=64 time=0.719 ms
64 bytes from 192.168.0.1: seq=1 ttl=64 time=0.651 ms
64 bytes from 192.168.0.1: seq=2 ttl=64 time=0.751 ms
64 bytes from 192.168.0.1: seq=3 ttl=64 time=0.613 ms

--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 packets recieved, 0% packet loss
roud-trip min/avg/max = 0.613/0.683/0.751 ms
```

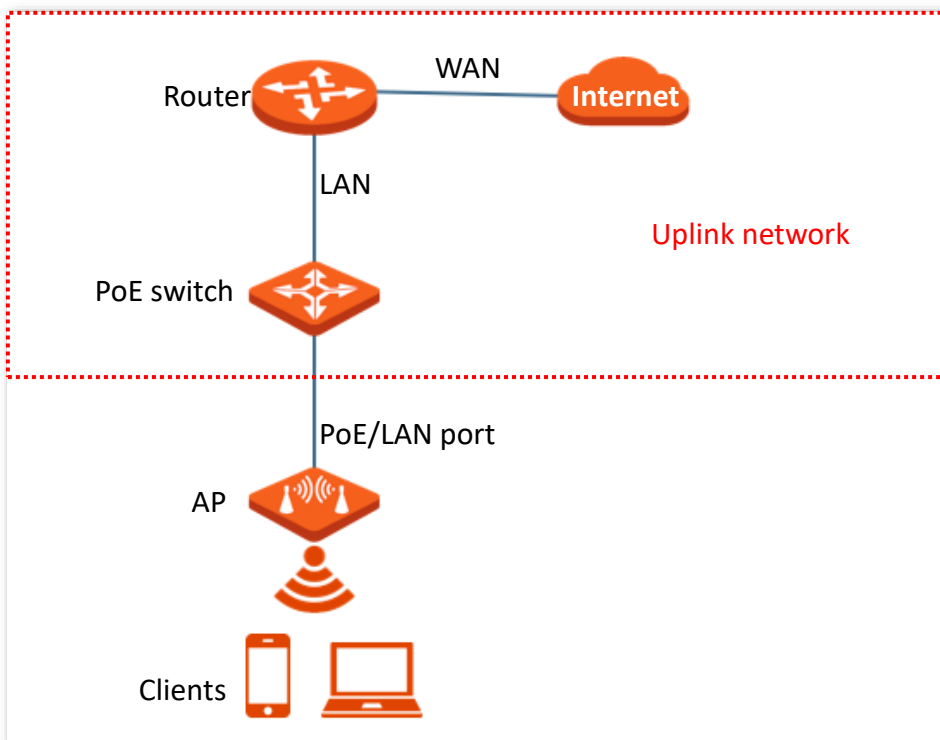
7.6 Uplink detection

7.6.1 Overview

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

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

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



7.6.2 Configure uplink detection

Step 1 [Log in to the web UI of the AP.](#)

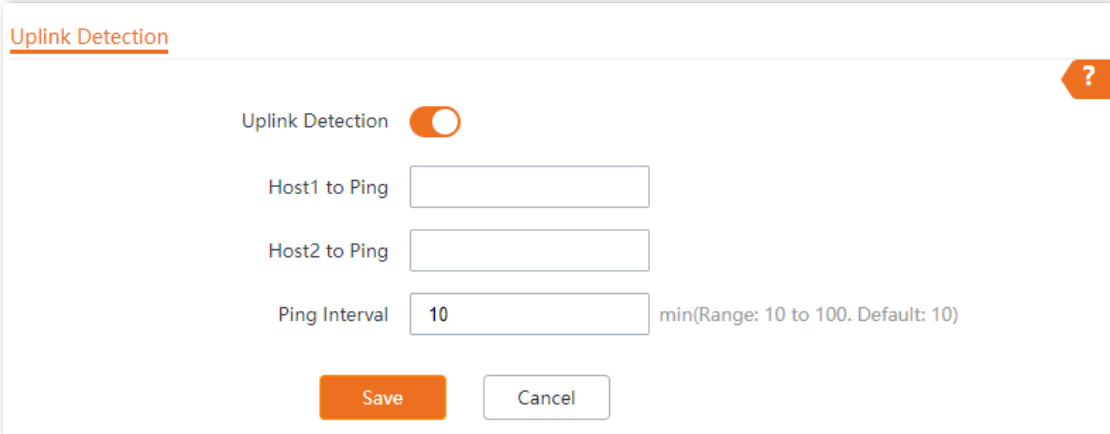
Step 2 Navigate to **Tools > Uplink Detection**.

Step 3 Enable the **Uplink Detection** function.

Step 4 Enter the IP address of the host to be pinged in **Host1 to Ping** or **Host2 to Ping**, such as the IP address of the switch or router directly connected to the Ethernet port of the AP. If there is only one host IP address, enter this IP address in both **Host1 to Ping** and **Host2 to Ping**.

Step 5 Set **Ping Interval** to the interval at which the AP detects its uplink. The default value is **10** minutes.

Step 6 Click **Save**.



Uplink Detection

Uplink Detection

Host1 to Ping

Host2 to Ping

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

Save Cancel

---End

Appendix

A.1 Factory default settings

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

Parameter		Default Value
	Management IP address	192.168.0.254
Login	User Name/Password	Administrator admin admin
		Guest user user
Quick Setup	Working Mode	AP
LAN Setup	IP Address Type	Static IP If there is a DHCP server on the LAN where the AP is deployed, the IP Address Type of the AP LAN port will be automatically changed to DHCP (Dynamic IP Address) , and the AP will automatically obtain an IP address from the DHCP server. Check the IP address obtained by the AP in the client list of the DHCP server.
	IP Address	192.168.0.254
	Subnet Mask	255.255.255.0
DHCP Server		Disable
SSID	SSID	2.4 GHz The AP allows 8 SSIDs. By default, the primary SSID is enabled, and the other SSIDs are disabled.
		5 GHz The AP allows 8 SSIDs. By default, the primary SSID is enabled, and the other SSIDs are disabled.
RF Settings	Wireless Network	Enable

A.2 Acronyms & Abbreviations

Acronyms & Abbreviations	Full Name
AC	Access Point Controller
ACK	Acknowledge character
AES	Advanced Encryption Standard
AIFSN	Arbitration Inter Frame Spacing Number
AP	Access Point
APSD	Automatic Power Save Delivery
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DTIM	Delivery Traffic Indication Map
DNS	Domain Name System
EDCA	Enhanced Distributed Channel Access
FIFO	First-in First-out
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NMS	Network Management System
OID	Object Identifier
PoE	Power over Ethernet
PSK	Pre-shared Key
PVID	Port-base VLAN ID
RF	Radio Frequency
RSSI	Received Signal Strength Indication
RTS	Request to Send
Short GI	Short Guard Interval
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TXOP	Transmission Opportunity
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy

Acronyms & Abbreviations	Full Name
WLAN	Wireless Local Area Network
WMF	Wireless Multicast Forwarding
WMM	WiFi Multimedia
WPA	Wi-Fi Protected Access