

User Guide

AC1200 Wave2 Ceiling Access Point

i23



Copyright statement

©2024 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

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

Disclaimer

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

Preface

Thank you for choosing Tenda! This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick internet setup, while this guide contains details of each function and demonstrates how to configure them.

This user guide walks you through all functions on the web UI of i23.

Conventions

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

The product figures and screenshots in this guide are for examples only. They may be different from the actual products you purchased, but do not affect the normal use.



In this guide, unless otherwise specified:

- The "AP" and "product" mentioned in this guide refer to Tenda ceiling AP.
- The firmware version uses V1.0.0.2(2661) of i23 as an example.
- The screenshots use the AP mode as an example. For other working modes, the actual web UI prevails.

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

Item	Presentation	Example
Cascading menus	>	Navigate to System > Live Users .
UI control	Bold	On the Policy page, click the OK button.
Parameter and value	Bold	Set User Name to Tom .
Variable	<i>Italic</i>	Format: <i>XX:XX:XX:XX:XX:XX</i>

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

Symbol	Meaning
 NOTE	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
 TIP	This format is used to supplement or explain the description of relevant operations.

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 the user guide was first published.

Version	Date	Description
V1.0	2024-08-28	Original publication.

Contents

1	Login and logout	1
1.1	Login	1
1.2	Logout	3
2	Web UI	4
2.1	Layout	4
2.2	Common buttons	5
3	Quick setup	6
3.1	AP mode	6
3.1.1	Overview	6
3.1.2	Configure AP mode	7
3.2	Client+AP mode	8
3.2.1	Overview	8
3.2.2	Configure client+AP mode	8
4	Status	11
4.1	View system status	11
4.2	View wireless status	13
4.3	View traffic statistics	14
4.4	View client list	15
5	Internet settings	16
6	Wireless settings	19
6.1	SSID settings	19
6.1.1	Overview	19
6.1.2	Example of setting up an open wireless network	24
6.1.3	Example of setting up a wireless network encrypted with PSK	26
6.1.4	Example of setting up a wireless network encrypted with WPA or WPA2	28
6.2	RF settings	39

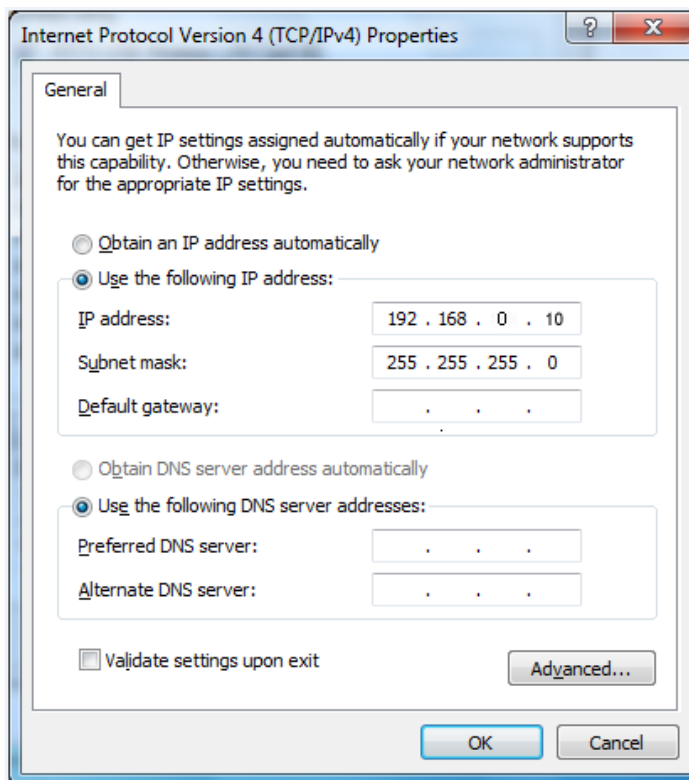
6.3 RF optimization	42
6.4 Frequency analysis	46
6.4.1 Overview	46
6.4.2 View frequency analysis	46
6.4.3 Execute channel scan	47
6.5 WMM settings	48
6.5.1 Overview	48
6.5.2 Configure WMM	50
6.6 Access control	52
6.6.1 Overview	52
6.6.2 Configure access control	53
6.6.3 Example of configuring access control	54
6.7 Advanced settings	55
6.8 QVLAN settings	56
6.8.1 Overview	56
6.8.2 Example of configuring QVLAN settings	57
6.9 WiFi schedule	60
7 Advanced settings	61
7.1 Traffic control	61
7.1.1 Overview	61
7.1.2 Configure traffic control	62
7.2 Cloud maintenance	64
7.2.1 Overview	64
7.2.2 Example of configuring cloud maintenance on web UI	65
7.2.3 Example of configuring cloud maintenance on App	69
8 Tools	72
8.1 Date & Time	72
8.1.1 System time	72
8.1.2 Login timeout interval	73
8.2 Maintenance	74
8.2.1 Reboot	74

8.2.2 Reset	76
8.2.3 Firmware upgrade	77
8.2.4 Backup/Restore	78
8.2.5 LED indicator control	81
8.3 Account	83
8.3.1 Overview	83
8.3.2 Change the password and user name of login account	83
8.4 System log	85
8.5 Diagnostic tool	86
8.6 Uplink detection	87
8.6.1 Overview	87
8.6.2 Configure uplink detection	87
Appendixes	89
A.1 Factory default settings	89
A.2 Acronyms & Abbreviations	90

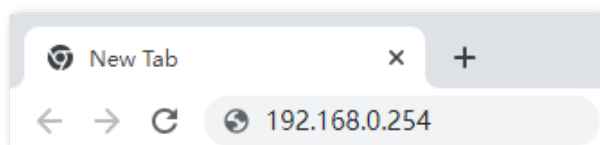
1 Login and logout

1.1 Login

- Step 1** Use an Ethernet cable to connect the management computer to the AP or the switch connected to the AP.
- Step 2** Configure the IP address of the computer to one in a same network segment as the AP. For example, if IP address of the AP is **192.168.0.254**, then the IP address of the computer can be configured to **192.168.0.X** (X ranges from 2 to 253 and is unused) and subnet mask is **255.255.255.0**.



- Step 3** Start a web browser (such as Chrome) on your computer and visit the IP address (**192.168.0.254** by default) of the AP.



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



When logging in to the web UI of the AP for the first time, you need to set your user name and password. If the user name and password cannot be customized for the first login, it is possible that you have not upgraded the AP firmware to the latest version. In this case, it is recommended to [upgrade the firmware](#).

i23V1.0

Enter the user name

Enter the login password

English

Login

[Forget password?](#)

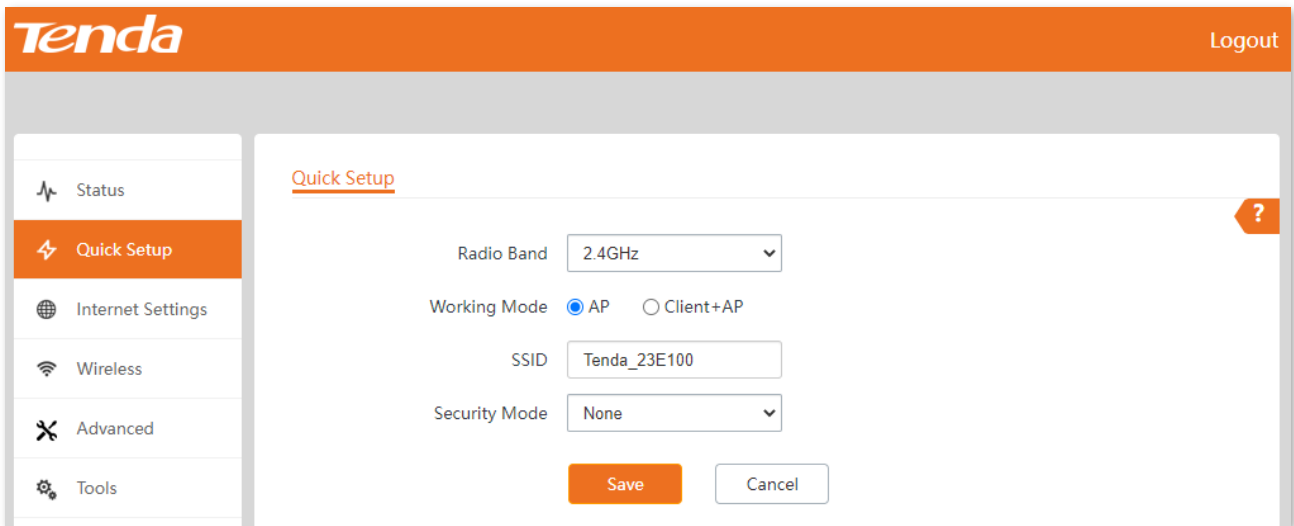
---End



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

- Ensure that the Ethernet cable is properly connected and not loose.
 - If multiple APs are deployed in the network without the DHCP server, IP address conflicts may occur, causing web UI login errors. Connect the APs to the network one by one and [modify the IP addresses of the APs](#).
 - If the LAN where the AP is deployed with DHCP server, AP may automatically obtain the new IP address from the DHCP server. In this case, you can first check the IP address obtained by the AP in the client list of the DHCP server, and then log in to the web UI of the AP using the new IP address. The computer can be set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
 - [Reset the AP](#) and try logging in again.
-

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



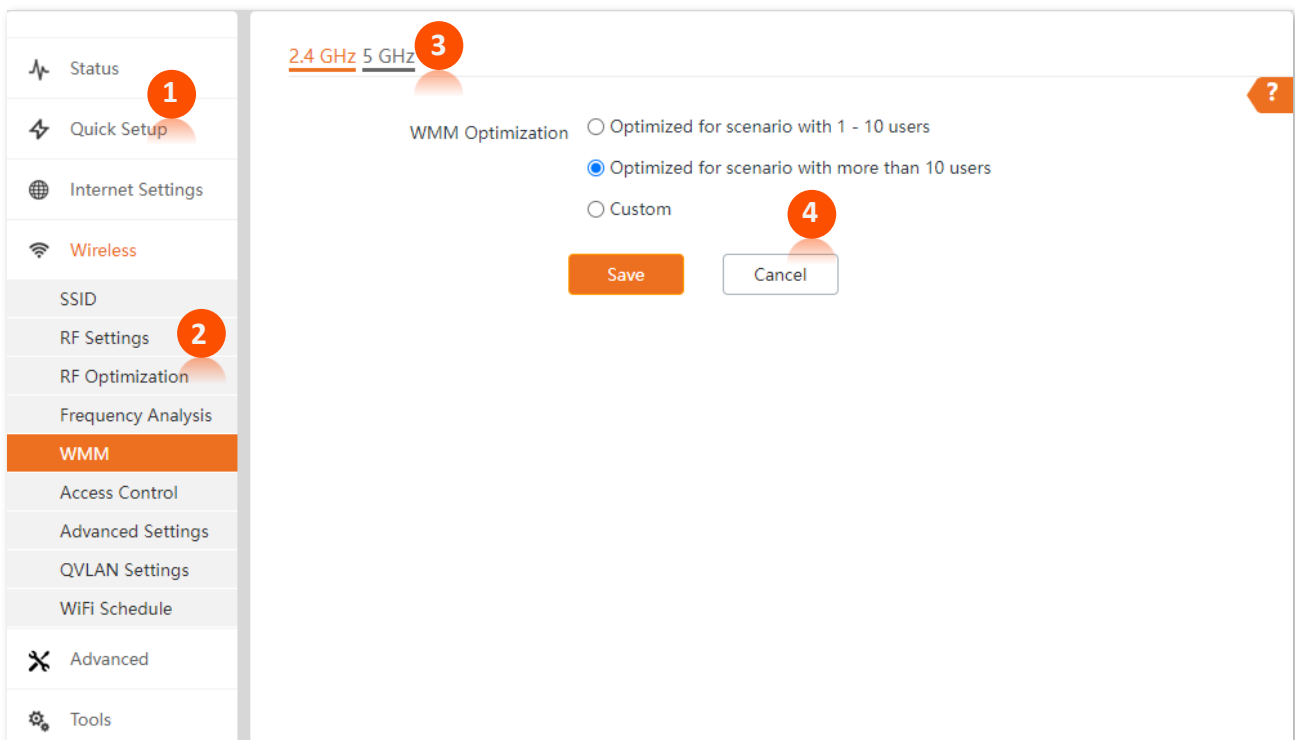
1.2 Logout

After logging in to the web UI of the AP, if no operations are performed during the [login timeout interval](#), the system will log out automatically. In addition, you can click **Logout** in the upper right corner to safely exit from the web UI.

2 Web UI

2.1 Layout

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

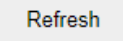

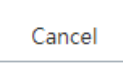



Functions or parameters displayed in gray on the web UI are not supported yet or cannot be modified under the current configurations.

No.	Name	Description
1	Level-1 navigation bar	
2	Level-2 navigation bar	Used to display the function menu of the AP. You can select functions in the navigation bars and the configuration appears in the configuration area.
3	Tab page area	
4	Configuration area	Area where you perform or check configurations.

2.2 Common buttons

Buttons commonly used on the web UI are illustrated below.

Common button	Description
	Used to refresh the current page.
	Used to save configurations on the current page and make the configurations take effect.
	Used to cancel the unsaved configurations on the current page and restore to previous configurations.
	Used to check the help information of the current page.

3 Quick setup

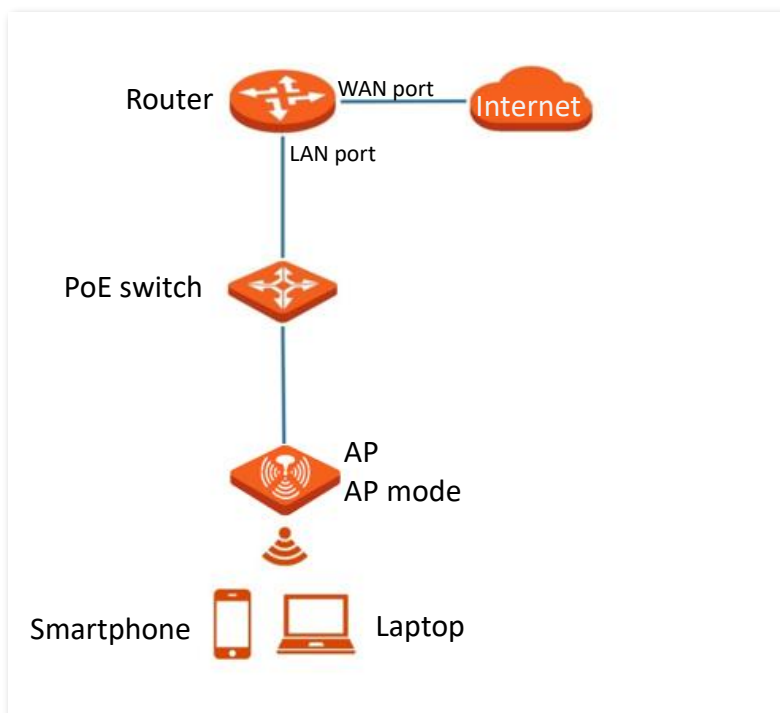
To access the page, [log in to the web UI of the AP](#), and navigate to **Quick Setup**.

On this page, you can set up the AP in a quick way to enable internet access for your WiFi-enabled devices (such as smartphones and laptops).

3.1 AP mode

3.1.1 Overview

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



3.1.2 Configure AP mode



Ensure that the upstream router has been connected to the internet before configuration.

- Step 1** [Log in to the web UI of the AP](#), and navigate to **Quick Setup**.
- Step 2** Select the **Radio Band** to be configured, which is **2.4GHz** in this example.
- Step 3** Set **Working Mode** to **AP**.
- Step 4** Set the **SSID** ([the first SSID](#)).
- Step 5** Select a **Security Mode** and configure the incurred parameters.
- Step 6** Click **Save**.

The screenshot shows the 'Quick Setup' configuration page. It features a title bar with a question mark icon. The main content area contains several configuration options: 'Radio Band' is a dropdown menu set to '2.4GHz'; 'Working Mode' has two radio buttons, with 'AP' selected and 'Client+AP' unselected; 'SSID' is a text input field containing 'Tenda_23E100'; 'Security Mode' is a dropdown menu set to 'WPA-PSK & WPA2-PSK'; and 'Key' is a text input field with masked characters. At the bottom, there are two buttons: 'Save' (orange) and 'Cancel' (white).

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

---End

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

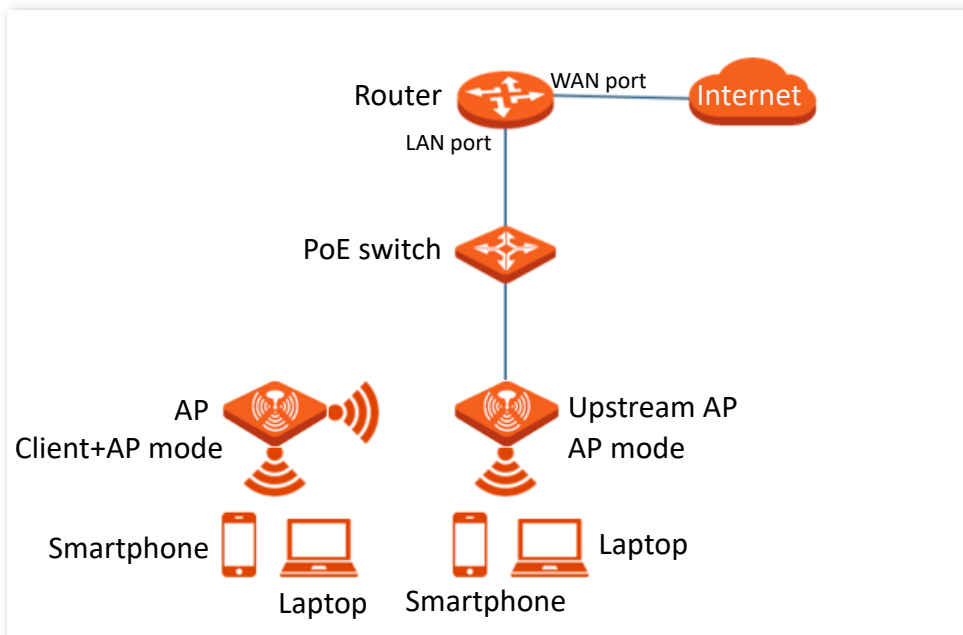
Parameter description

Parameter	Description
Radio Band	Used to select the radio band to configure.
Working Mode	Specifies the working mode of the AP. Select the AP mode to transform the wired network to wireless network.
SSID	Click to modify the wireless name of the first network under the selected radio band.
Security Mode	Select the security modes for target wireless networks. Supported security modes are as follows: None , WEP , WPA-PSK , WPA2-PSK , WPA-PSK&WPA2-PSK , WPA and WPA2 .

3.2 Client+AP mode

3.2.1 Overview

In this mode, the AP 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 figure.



3.2.2 Configure client+AP mode



Ensure that the upstream AP has been connected to the internet before configuration.

- Step 1** [Log in to the web UI of the AP](#), and navigate to **Quick Setup**.
- Step 2** Select the **Radio Band** to be configured, which is **2.4GHz** in this example.
- Step 3** Set **Working Mode** to **Client+AP**.
- Step 4** Click **Scan**.

Quick Setup ?

Radio Band

Working Mode AP Client+AP

SSID

Security Mode

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



- If no wireless network is found, navigate to **Wireless > RF Settings**, ensure that **Wireless Network** for the corresponding frequency band is enabled, and try again.
- After a wireless network to be extended is selected, the SSID and security mode of the wireless network are populated automatically.

Select	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
<input type="radio"/>	Tenda_085DE0		20		WPA2-PSK/AES	
<input checked="" type="radio"/>	Tenda_083980		40		WPA2-PSK/AES	

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

Step 7 Click **Save**.

Quick Setup ?

Radio Band

Working Mode AP Client+AP

SSID

Security Mode

Key


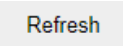

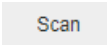
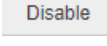
---End

After the configuration is completed, you can select the SSID on your WiFi-enabled devices (such as smartphones) and enter your wireless password to connect to the wireless network of the AP and access the internet through the AP.



Navigate to **Wireless > SSID**, on this page, you can view the SSID and key of the AP.

Parameter description

Parameter	Description
Radio Band	Specifies the radio band of the wireless network to be configured.
Working Mode	Specifies the working mode of the AP. Select the Client+AP mode to bridge the upstream wireless network.
SSID	Specifies the wireless 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.
Security Mode	<p>Specifies the security mode of which the upstream wireless network adopted. After you select the upstream wireless network from the scanned wireless network list, this parameter will be populated automatically.</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 (X ranges from 1 to 4) need to be entered manually. - If the wireless network to be bridged adopts the WPA-PSK, WPA2-PSK or WPA-PSK&WPA2-PSK security mode, you need to enter the Key.
	Used to refresh the scan results.
	<p> : Used to scan for available wireless networks nearby. The scan results are displayed at the bottom of the page.</p> <p> : Used to stop scanning and collapse the scan results. This button only appears after you click Scan.</p>

4 Status

4.1 View system status

To access the page, [log in to the web UI of the AP](#), and navigate to **Status > System Status**.

On this page, you can view the system and LAN port status of the AP.

System Status ?

System Status

Device Name: i23V1.0	Cloud Management: Disconnected
Uptime: 17min2sec	System Time: 2024-08-20 19:42:36
Firmware Version: V1.0.0.2(2661)	Hardware Version: V1.0
Number of Wireless Clients: 0	Working mode: AP
Bridging state: Unbridged	SN:

LAN Port Status:

MAC Address: 	IP Address: 192.168.0.254
Subnet Mask: 255.255.255.0	Primary DNS:
Secondary DNS: 	

Parameter description

Parameter	Description	
System Status	Device Name	Specifies the name of the AP. You can change the AP name on the Internet settings module.
	Cloud Management	Specifies the connection status between the AP and the Tenda CloudFi cloud platform.
	Uptime	Specifies the time that has elapsed since the AP was started last time.
	System Time	Specifies the system time of the AP.
	Firmware Version	Specifies the firmware version of the AP.
	Hardware Version	Specifies the hardware version of the AP.
	Number of Wireless Clients	Specifies the number of wireless clients connected to the AP.
	Working mode	Specifies the working mode of the AP.
	Bridging state	Specifies the bridging status of the AP.
	SN	Specifies the serial number of the AP.
LAN Port Status	MAC Address	Specifies the physical address of the LAN port of the AP.
	IP Address	Specifies the IP address of the AP and it is also the management IP address of the AP. The web UI of the AP is accessible by visiting this IP address. You can change the IP address on the Internet settings module.
	Subnet Mask	Specifies the subnet mask of the AP.
	Primary DNS	Specifies the IP address of the primary DNS server of the AP.
	Secondary DNS	Specifies the IP address of the secondary DNS server of the AP.

4.2 View wireless status

To access the page, [log in to the web UI of the AP](#), and navigate to **Status > Wireless Status**.

On this page, you can view the RF status and SSID status of the AP. By default, the page displays the information of 2.4 GHz wireless status. To view the wireless status of 5 GHz, click **5 GHz**.

The screenshot shows the 'Wireless Status' page with two tabs: '2.4 GHz' (selected) and '5 GHz'. A help icon (?) is in the top right. Under 'RF Status', 'RF' is 'Enabled', 'Network Mode' is '11b/g/n', and 'Channel' is a dropdown menu. Under 'SSID Status', there is a table with the following data:

SSID	MAC Address	Status	Security Mode
Tenda_23E100	[Redacted]	Enabled	None

Parameter description

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

4.3 View traffic statistics

To access the page, [log in to the web UI of the AP](#), and navigate to **Status > Traffic Statistics**.

On this page, you can view the packet statistics for the wireless network of the AP.

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

<u>2.4 GHz</u> <u>5 GHz</u>				
SSID	Received Traffic	Received Packets (Qty.)	Transmitted Traffic	Transmitted Packets (Qty.)
Tenda_23E100	0.00MB	0	0.00MB	0

Parameter description

Parameter	Description
SSID	Specifies the name of the wireless network.
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.

NOTE

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

4.4 View client list



To access the page, [log in to the web UI of the AP](#), and navigate to **Status > Client List**.

On this page, you can view the information about the wireless clients connected to the wireless networks corresponding to the SSIDs of the AP. You can also disconnect certain connected clients.

ID	MAC Address	IP Address	Client Type	Connection Duration	Transmit Rate	Receive Rate	Block
1		192.168.0.107	ios	0h 2m 55s	1Mbps	58Mbps	

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

Parameter description

Parameter	Description
SSID	Used to select a wireless name from the drop-down menu to view wireless clients connected to the wireless network.
MAC Address	Specifies the MAC address of the wireless client.
IP Address	Specifies the IP address of the wireless client.
Client Type	Specifies the operating system type of the wireless client.  TIP It is available only when the identify client type function of the AP is enabled and the client has visited an HTTP website.
Connection Duration	Specifies the online duration of the wireless client.
Transmit Rate	Specifies the transmit rate of the wireless client.
Receive Rate	Specifies the receive rate of the wireless client.
Block	Click  to disconnect the corresponding wireless client, and the client is added to the blocklist of the Access Control . The client cannot connect to the AP again by reconnecting to the wireless network. To unblock a client, navigate to Access Control .

5 Internet settings

To access the page, [log in to the web UI of the AP](#), and navigate to **Internet Settings**.

On this page, you can view the MAC address of the LAN port of the AP and set the IP address, device name, 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 of the AP are set manually. It is proper for the scenarios where only one or several APs are required 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 required 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. The default IP address is 192.168.0.254 .
Subnet Mask	Specifies the subnet mask of the IP address of the AP. The default subnet mask is 255.255.255.0 .
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 LAN 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 LAN router connected to the internet provides the DNS proxy function, this IP address can be the LAN IP address of the router. Otherwise, enter a correct DNS server IP address.</p>
Secondary DNS	<p>Specifies the IP address of the secondary DNS server 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 data-bbox="384 241 1174 271">Specifies the Ethernet mode of the PoE power-supply port of this AP.</p> <ul data-bbox="440 300 1414 450" style="list-style-type: none"> <li data-bbox="440 300 1414 360">– Fast Speed (Auto Negotiation): This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended. <li data-bbox="440 389 1414 450">– Longer Distance (10 Mbps Full Duplex): This mode features a long transmission distance but relatively low transmission rate (usually 10 Mbps). <p data-bbox="384 479 1414 640">The Longer Distance (10 Mbps Full Duplex) mode is recommended only if the Ethernet cable that connects the PoE power-supply port of the AP to a peer device exceeds 100 meters. In this case, the connected LAN port of the peer device must work in auto-negotiation mode. Otherwise, the PoE power-supply port of the AP may not be able to properly transmit or receive data.</p>

6 Wireless settings

6.1 SSID settings

6.1.1 Overview

To access the page, [log in to the web UI of the AP](#), and navigate to **Wireless > SSID**.

On this page, you can set 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


Security Mode

Key

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

Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	

Parameter	Description
SSID	<p>Specifies the SSID to be configured.</p> <p>The first SSID displayed on the page under the radio band tab is the primary SSID of the radio band by default.</p>
Status	<p>Specifies the status of the selected SSID.</p> <p>The first SSID is enabled by default while other SSIDs are disabled by default. You can enable them as required.</p>
Broadcast SSID	<p>Specifies whether to enable the broadcast SSID function.</p> <p>After this function is disabled, the AP does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. It enhances the security of the wireless network.</p>
Guest	<p>Specifies whether to enable the guest function.</p> <p>After this function is enabled, wireless clients connected to the wireless network can only access the internet and cannot access LAN resources (including the web UI of the AP).</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>
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>
Max. Number of Clients	<p>Specifies the maximum number of clients that can be concurrently connected to the wireless network corresponding to an SSID.</p> <p>After this upper limit is reached, new clients cannot connect to the SSID unless some clients cut off their connections.</p>
SSID	Used to change the selected SSID.
Security Mode	Specifies the security mode of the selected SSID. The options include: 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 client can connect to the wireless network. This option is not recommended because it affects network security.

■ WEP

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

Security Mode	WEP	▼
Authentication Type	Open	▼
Default Key	Key 1	▼
Key 1	ASCII ▼
Key 2	ASCII ▼
Key 3	ASCII ▼
Key 4	ASCII ▼

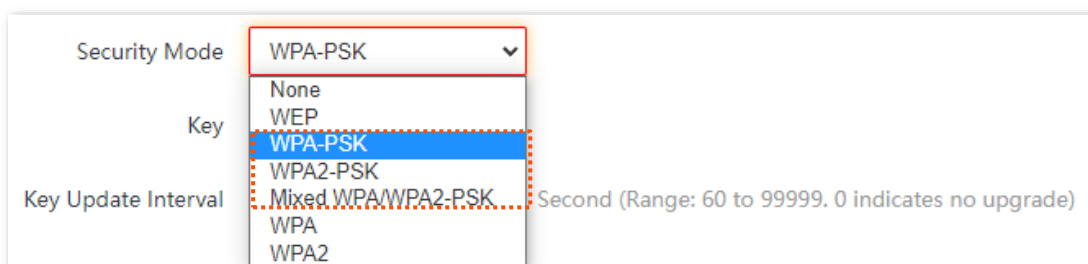
Parameter description

Parameter	Description
Authentication Type	<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 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 clients use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.



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.
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 WAP 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 clients and generate data encryption-oriented root keys. WPA and WPA2 use the root keys to replace the pre-shared keys that set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK.

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

The screenshot shows a configuration window with the following fields and values:

- Security Mode**: A dropdown menu is open, showing options: None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2. The WPA and WPA2 options are highlighted with a blue bar.
- RADIUS Server**: (Empty field)
- RADIUS Port**: (Empty field) (Range: 1025 to 65535. Default: 1812)
- RADIUS Key**: (Empty field)
- Key Update Interval**: (Second (Range: 60 to 99999. 0 indicates no upgrade))

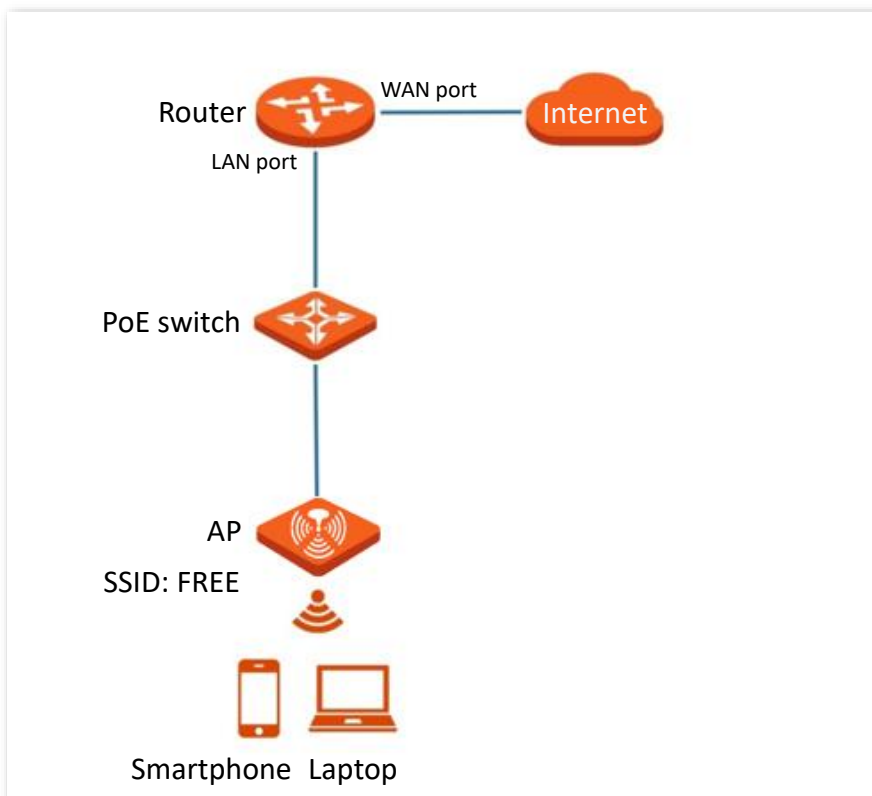
Parameter description

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	Specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	Specifies the port number of the RADIUS server for client authentication.
RADIUS Key	Specifies the shared password of the RADIUS server.
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 WAP key is not updated.</p>

6.1.2 Example of setting up an open wireless network

Networking requirements

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



Configuration procedure

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

Step 1 [Log in to the web UI of the AP](#), and navigate to **Wireless > SSID**.

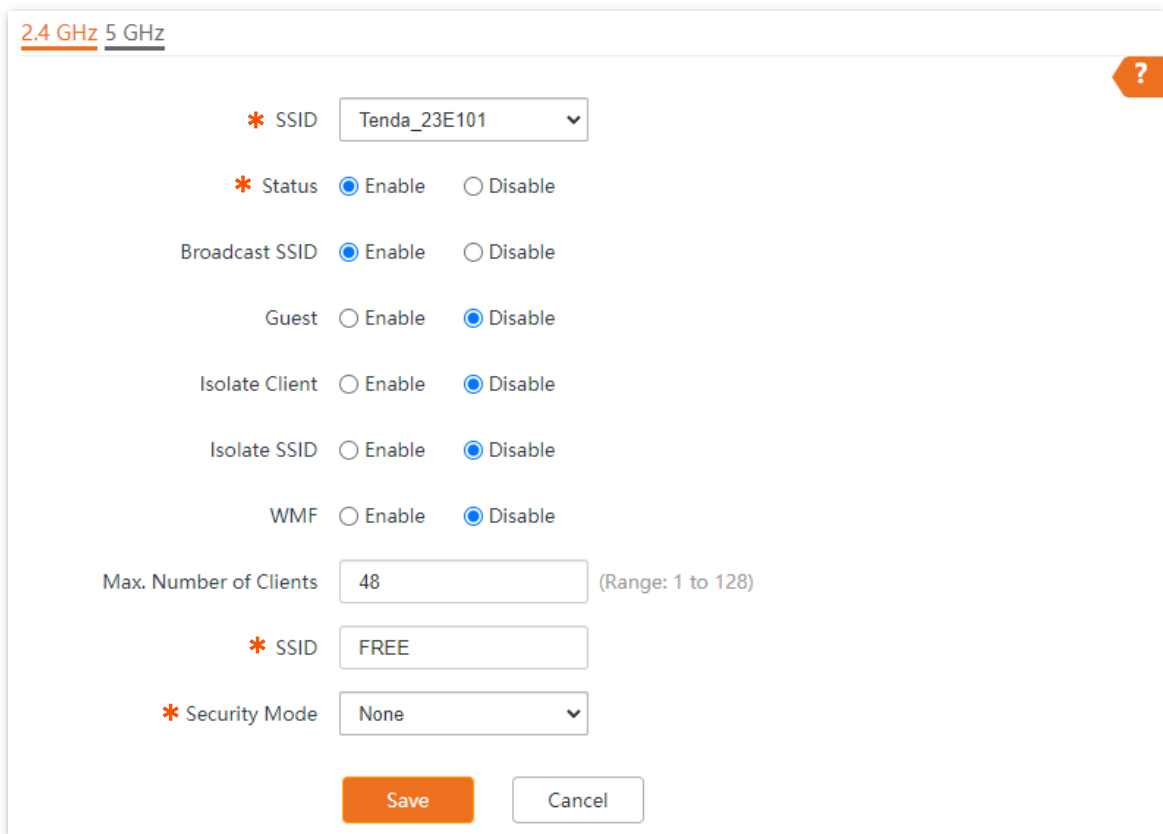
Step 2 Select the second SSID from the **SSID** drop-down list box.

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

Step 4 Set **SSID** to **FREE**.

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

Step 6 Click **Save**.



2.4 GHz 5 GHz

* SSID Tenda_23E101

* 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 48 (Range: 1 to 128)

* SSID FREE

* Security Mode None

Save Cancel

---End

Verification

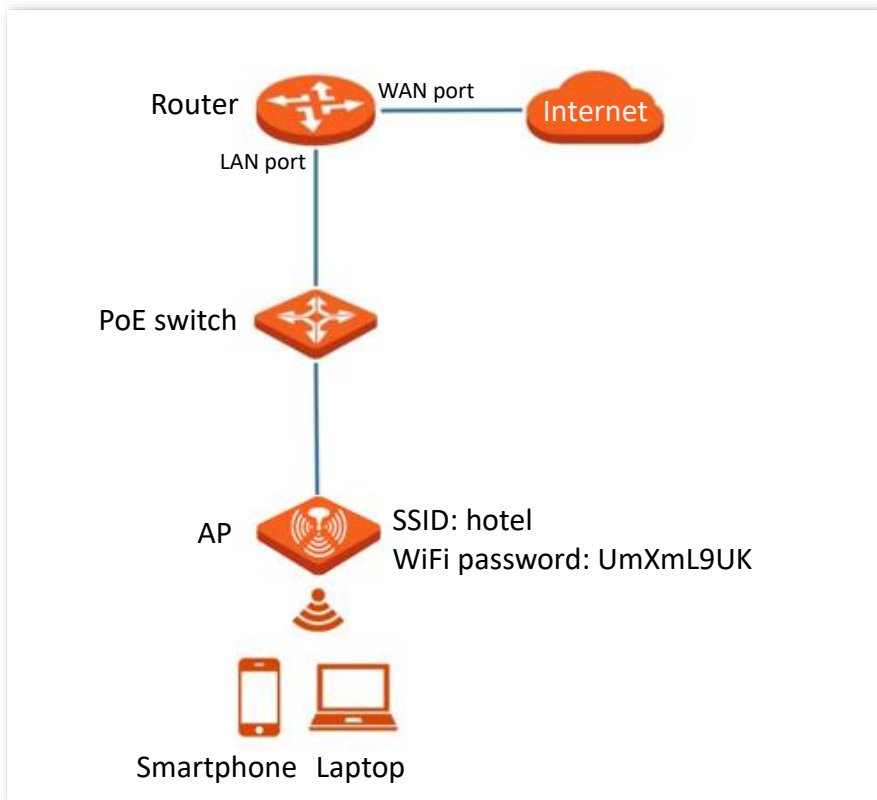
Verify that WiFi-enabled devices can connect to the **FREE** wireless network without a password.

6.1.3 Example of setting up a wireless network encrypted with PSK

Networking requirements

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

Assume that the SSID is **hotel** and the WiFi password is **UmXmL9UK**. See the following figure.



Configuration procedure

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

- Step 1** [Log in to the web UI of the AP](#), and navigate to **Wireless > SSID**.
- Step 2** Select the second SSID from the **SSID** drop-down list box.
- Step 3** Set **Status** to **Enable**.
- Step 4** Set **SSID** to **hotel**.
- Step 5** Set **Security Mode**, which is **WPA2-PSK** in this example.
- Step 6** Set **Key** to **UmXmL9UK**.
- Step 7** Click **Save**.

2.4 GHz 5 GHz

* SSID Tenda_23E101

* 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 48 (Range: 1 to 128)

* SSID hotel

* Security Mode WPA2-PSK

* Key

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

Save Cancel

---End

Verification

Verify that WiFi-enabled devices can connect to the wireless network named **hotel** with the password **UmXmL9UK**.

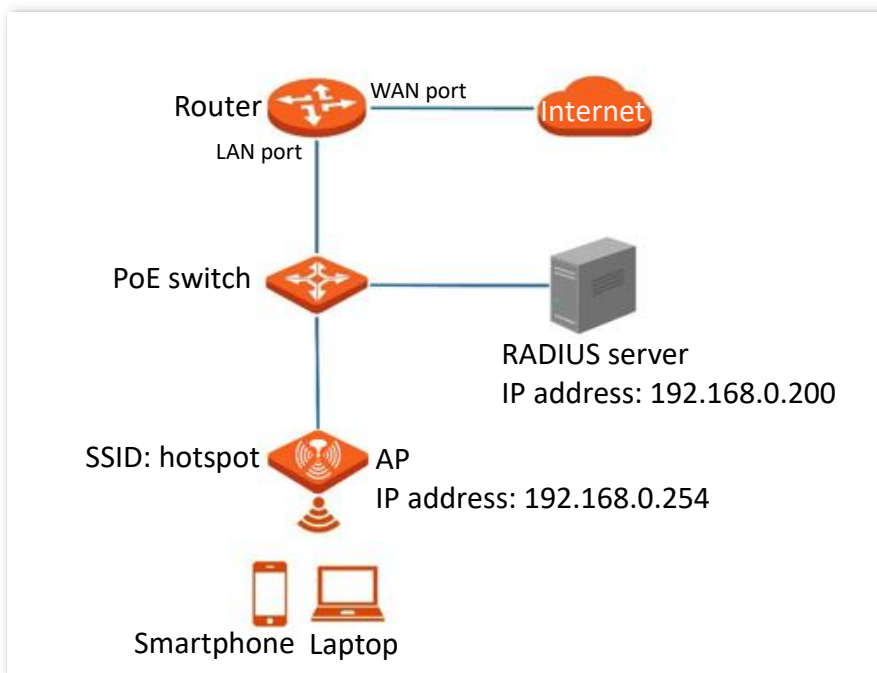
6.1.4 Example of setting up a wireless network encrypted with WPA or WPA2

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

- IP address of the RADIUS server: **192.168.0.200**
- RADIUS port: **1812**
- RADIUS key: **UmXmL9UK**



Configuration procedure

I. Configure the AP

- Step 1** [Log in to the web UI of the AP](#), and navigate to **Wireless > SSID**.
- Step 2** Select the second SSID from the **SSID** drop-down list box.
- Step 3** Set **Status** to **Enable**.
- Step 4** Set **SSID** to **hotspot**.
- Step 5** Set **Security Mode** to **WPA2**.
- Step 6** Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Key** to **192.168.0.200**, **1812**, and **UmXmL9UK** respectively.
- Step 7** Click **Save**.

2.4 GHz 5 GHz

* SSID

* Status Enable Disable

Broadcast SSID Enable Disable

Guest Enable Disable

Isolate Client Enable Disable

Isolate SSID Enable Disable

WMF Enable Disable

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

* SSID

* Security Mode

* RADIUS Server

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

* RADIUS Key

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


----End

II. Configure the RADIUS server

Windows 2016 is used as an example to describe how to configure the RADIUS server.

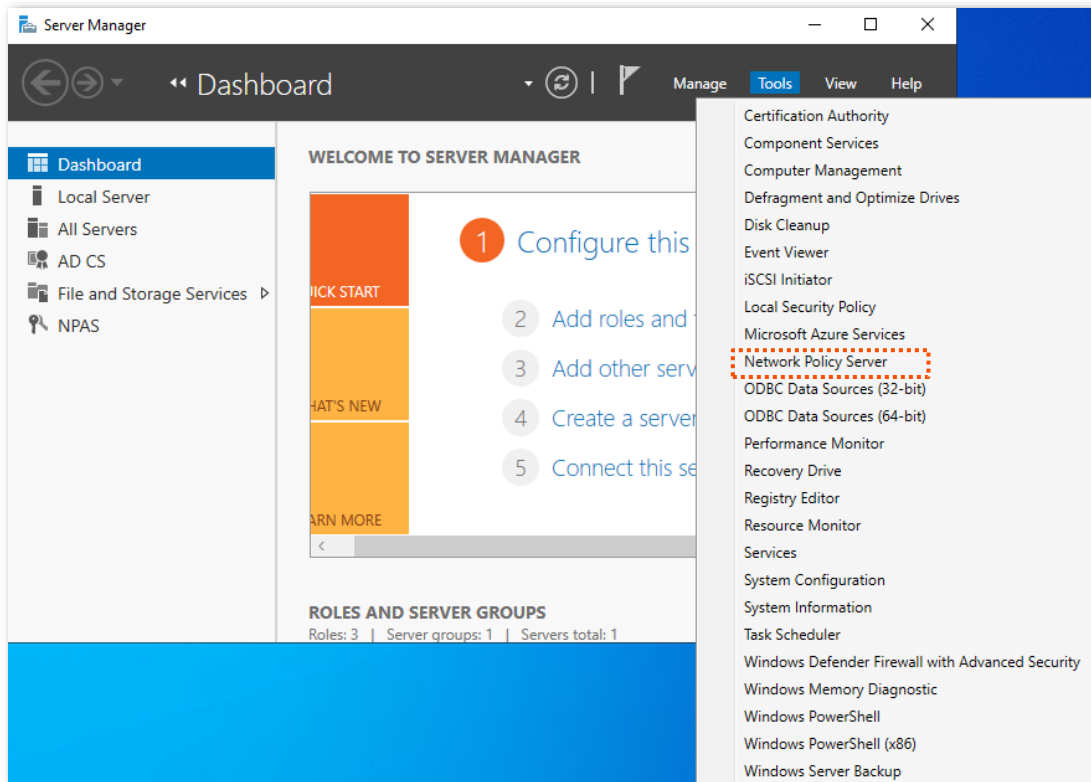
Step 1 Install **Active Directory Certificate Services** and **Network Policy and Access Services**, and deploy the certificate.

On the **Start > Server Manager > Dashboard** page, navigate to **Add roles and features > Server Selection > Server Roles**, and tick the **Active Directory Certificate Services**. According to the operation wizard, install the **Certification Authority of Active Directory Certificate Services** and **Network Policy and Access Services**.

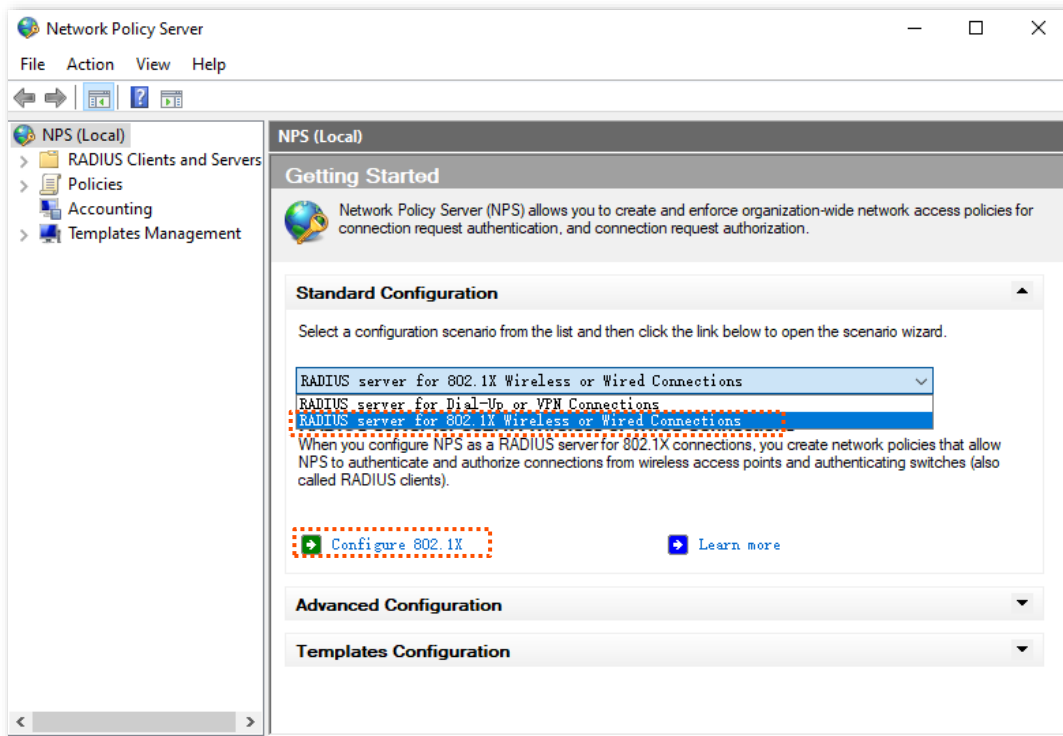
After the service installation is completed, click  in the upper right corner and follow the prompts to deploy the certificate.

Step 2 Configure 802.1X.

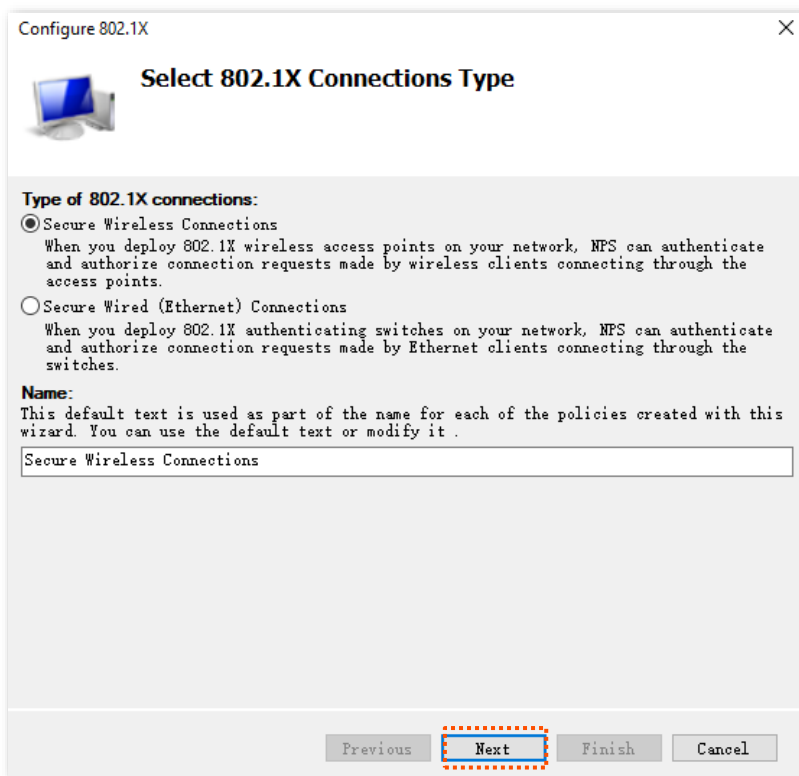
1. Navigate to **Start > Server Manager > Dashboard**, click **Tools** in the upper right corner, and click **Network Policy Server**.



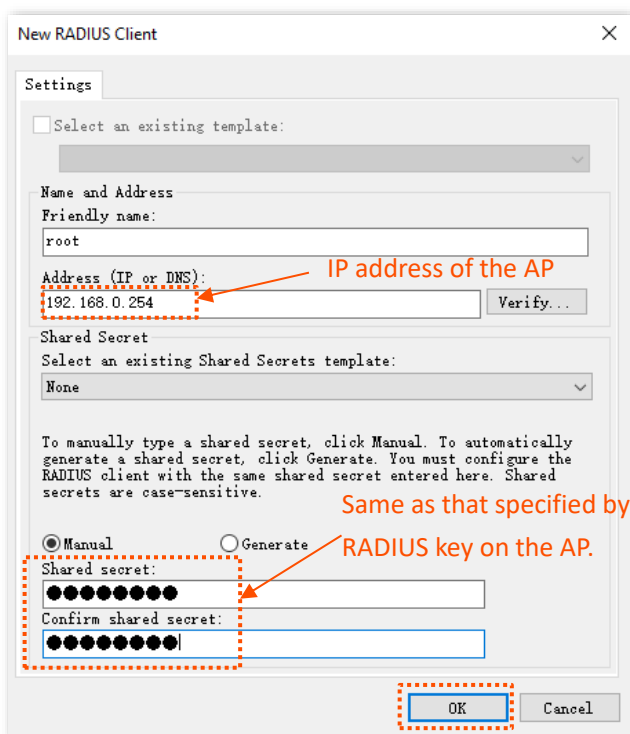
2. Select **RADIUS server for 802.1X Wireless or Wired Connection from Standard Configuration** and click **Configure 802.1X**.



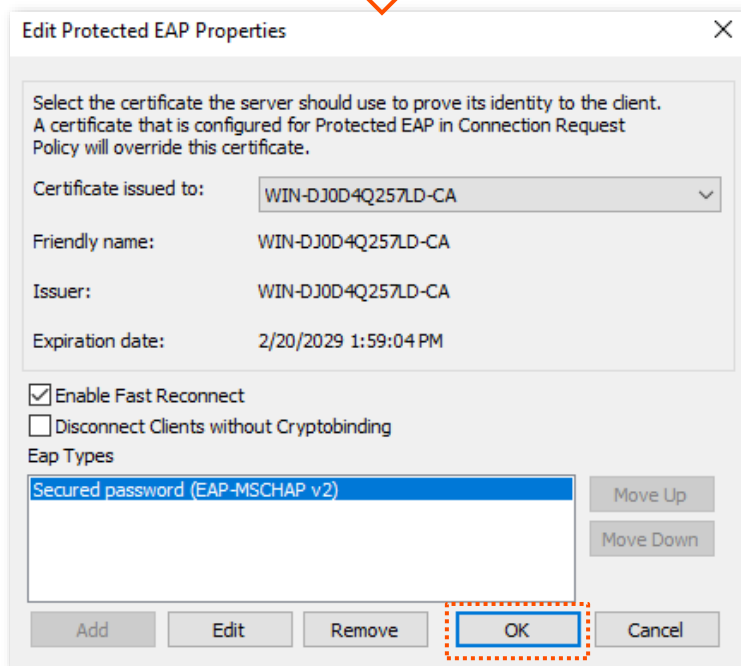
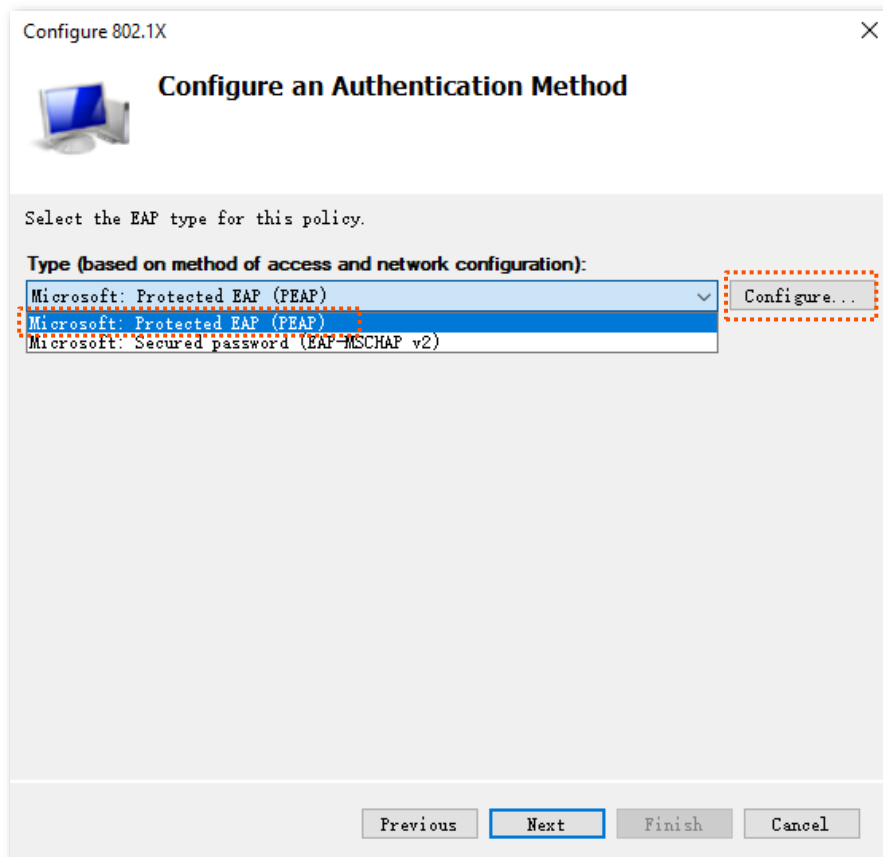
3. Select **Secure Wireless Connections** for **Type of 802.1X connections**. Modify the name as required, which is **Secure Wireless Connections** in this example, and click **Next**.



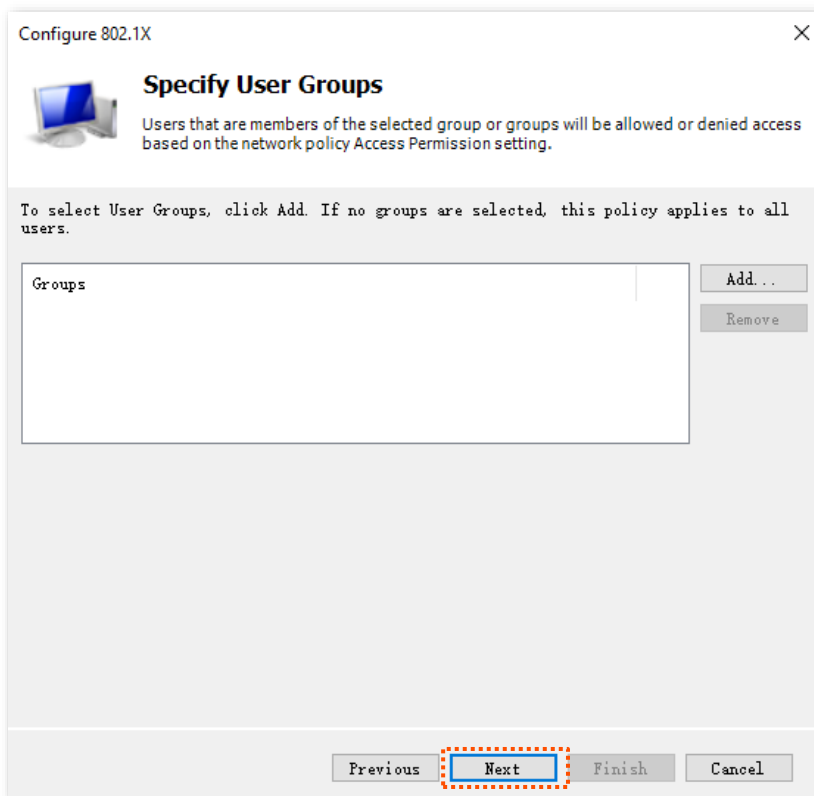
4. On the **Specify 802.1X Switches** page, click **Add**.
5. Set a **RADIUS** client name (which can be the name of the AP) and the IP address of the AP. Enter **UmXmL9UK** in the **Shared secret** and **Confirm shared secret** text boxes, and click **OK**.



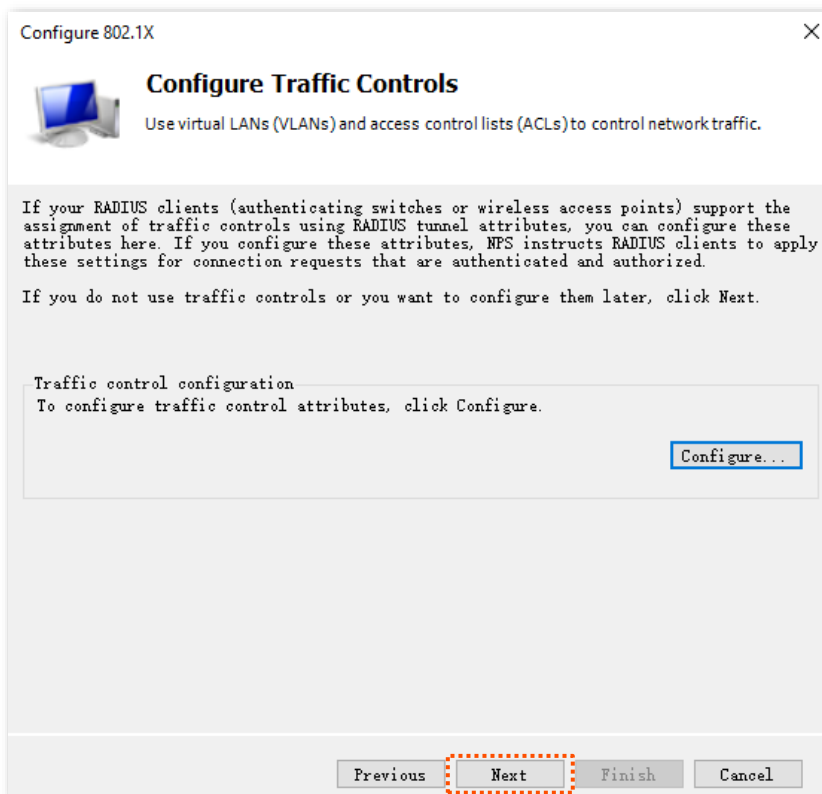
6. Select **Microsoft: Protected EAP (PEAP)** from **Type**, and click **Configure**. Select the certificate deployed in the certificate authority in the previous step, click **OK**, and click **Next** after the configuration is completed.

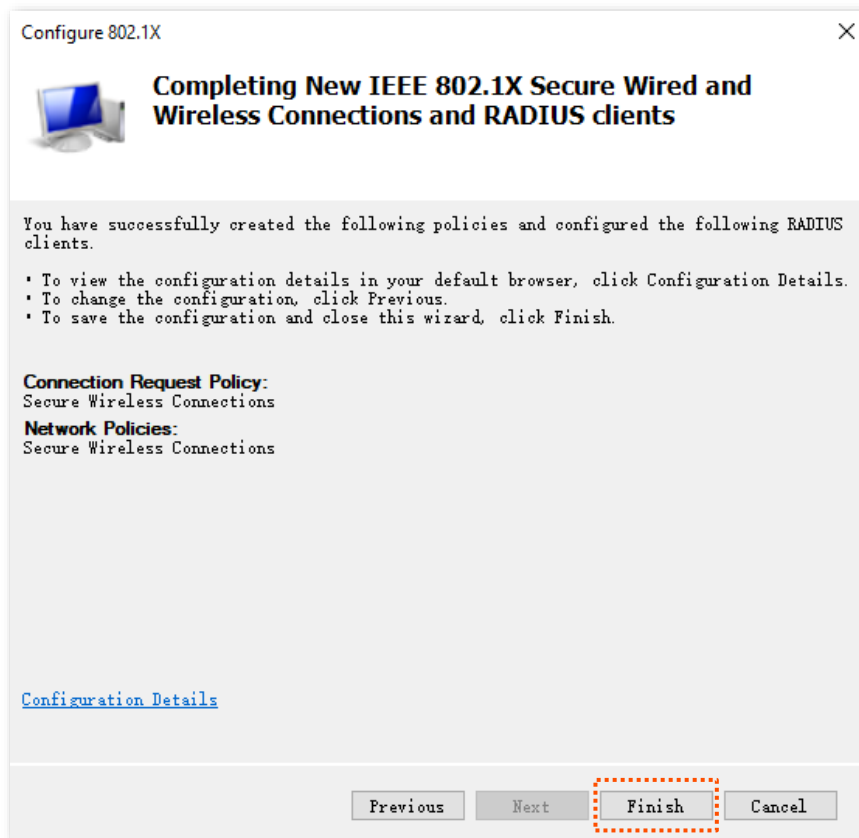


- 7. Click **Next** on the **Specify User Groups** page.



- 8. On the **Configure Traffic Controls** page, configure the parameters as required, click **Next**, and click **Finish**.



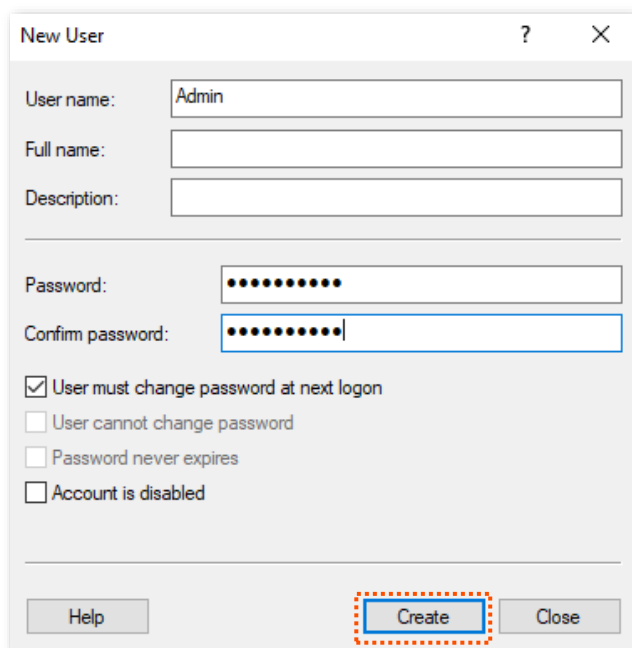


Step 3 Configure the user and user group.

1. Create a user.

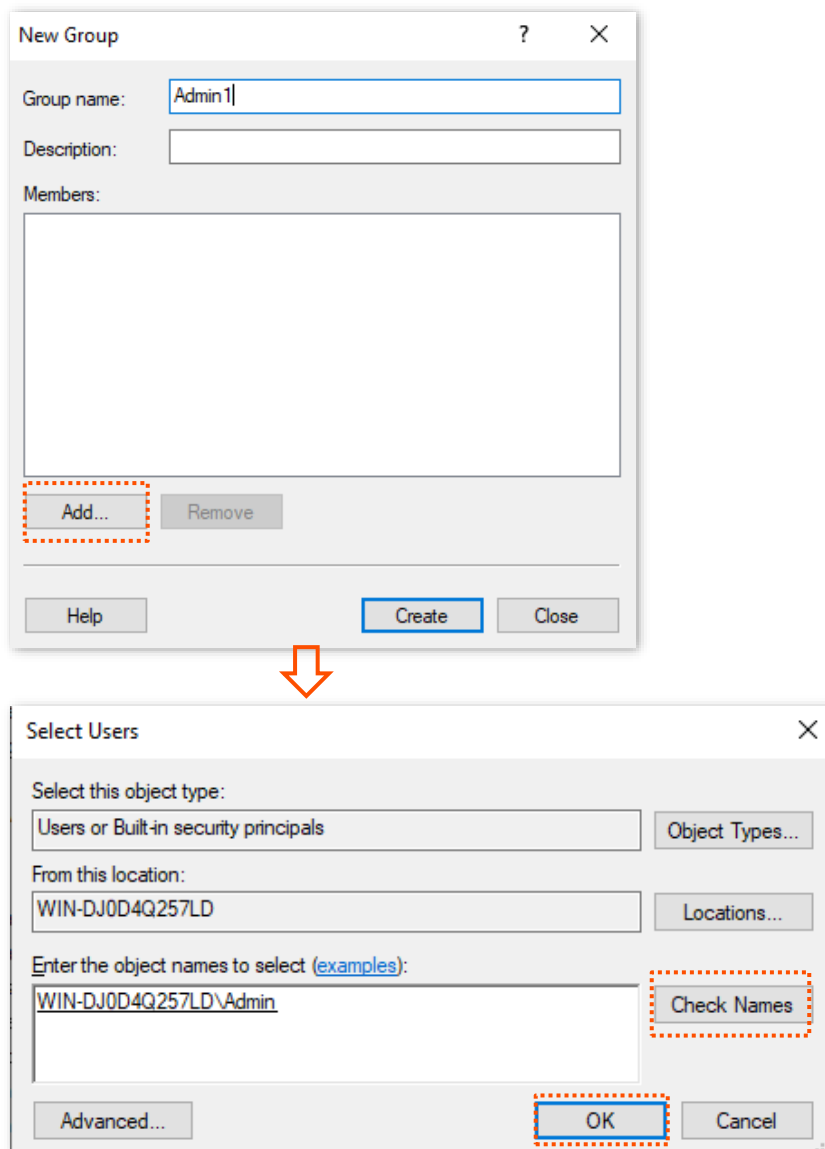
Navigate to **Start > Server Manager > Dashboard**, click **Tools** in the upper right corner, click **Computer Management**, and double-click **Local Users and Groups**.

Right-click **Users**, and select **New User**. Enter the user name and password, which are **Admin** (user name) and **JohnDoe123** (password) in this example. And click **Create**.



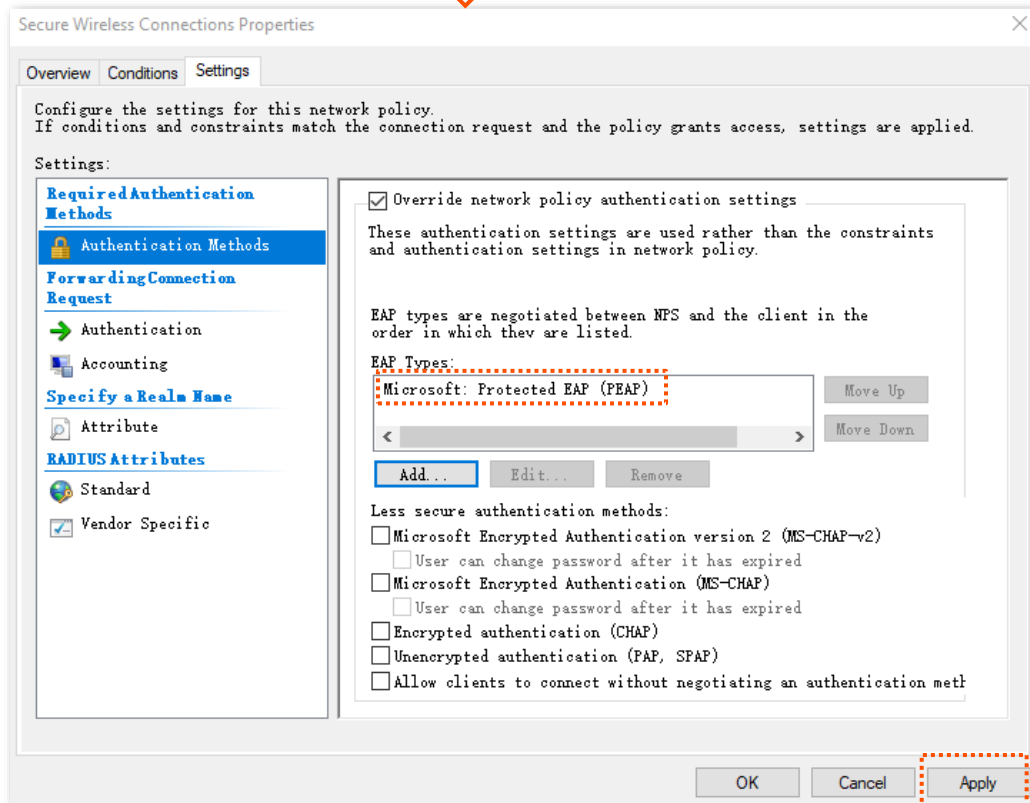
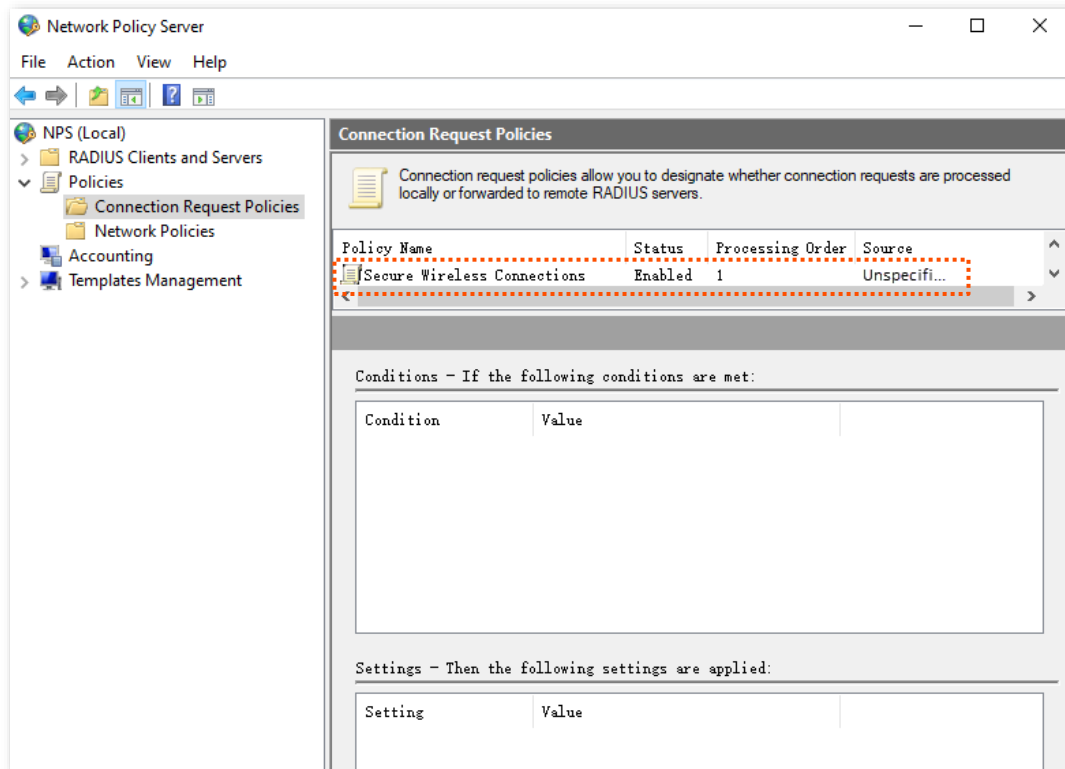
2. Create a user group.

Right-click **Groups**, and select **New Group**. Set **Group name**, which is **Admin1** in this example, and click **Add**. In the **Enter the object names to select** column, enter the created [user name](#), click **Check Names**, and click **OK**. In the **New Group** window, click **Create**.



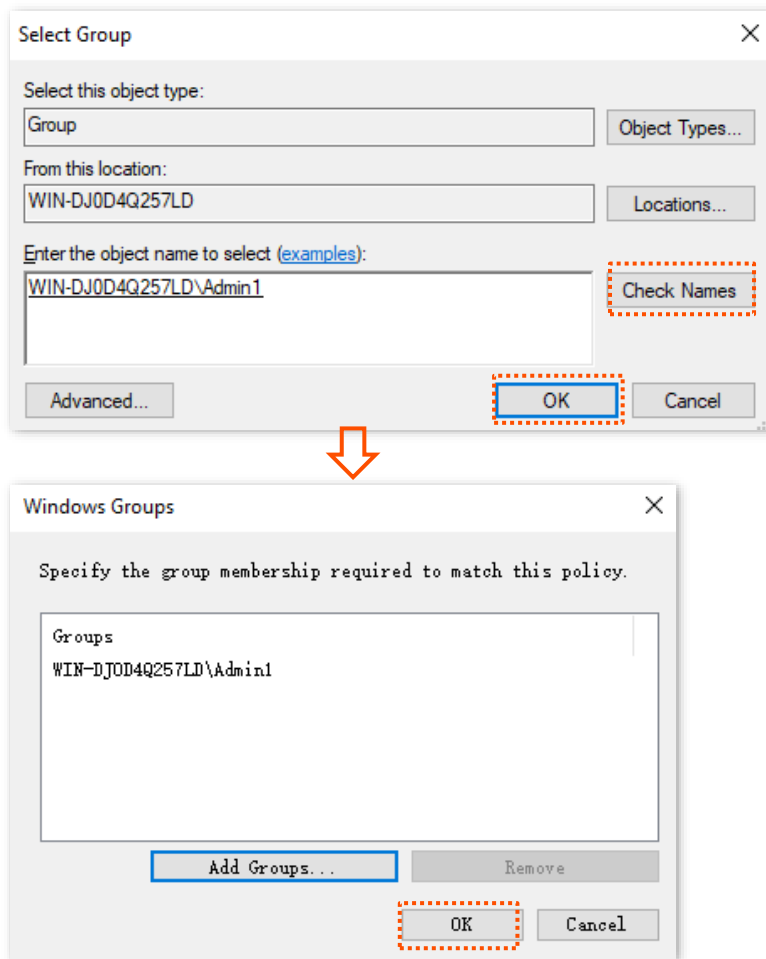
Step 4 Configure the policies.

1. Navigate to **Start > Server Manager > Dashboard**, click **Tools** in the upper right corner, click **Network Policy Server**, and double-click **Policies**.
2. Click **Connection Request Policies** and double-click **Secure Wireless Connections**. On the **Secure Wireless Connections Properties** window, click **Settings** and tick **Override network policy authentication settings**. Click **Add**, add **Microsoft: Protected EAP (PEAP)** as **EAP Types**, and click **Apply**.



3. Click **Network Policies** and double-click **Secure Wireless Connections**. On the **Secure Wireless Connections Properties** window, click **Conditions**, and click **Add**.


Add the **Windows Groups**, enter the created [user group](#), click **Check Names**, click **OK**, then click **OK**, and click **Apply**.



----End

III. Configure the WiFi-enabled device

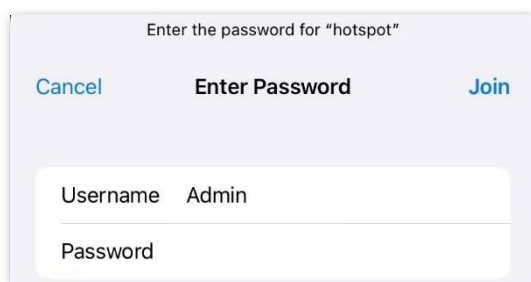
Smartphone (iOS system) is used as an example.

Step 1 Tap the  (Settings) on the smartphone, tap **WLAN**, and connect the smartphone to the AP's wireless network, which is **hotspot** in this example.

Step 2 Enter the [username and password](#), and tap **Join**.



If a pop-up window appears asking whether to trust the certificate, tap **Trust**.



---End

Verification

The WiFi-enabled devices can connect to the wireless network named **hotspot**.



TIP

If the connection fails, please:

- Ensure that the radius server and AP can communicate normally (Ping each other).
 - Try to modify the firewall settings of the radius server: add inbound and outbound rules to allow TCP and UDP specific local port "1812, 1813, 1645, 1646" to connect.
-

6.2 RF settings

To access the page, [log in to the web UI of the AP](#), and navigate to **Wireless > RF Settings**.

On this page, you can modify the basic radio parameters.

Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	
Wireless Network	Specifies whether to enable the wireless network function of the AP.

Parameter	Description
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.
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 and available options for 5 GHz are 11a, 11ac, and 11a/n.</p> <ul style="list-style-type: none"> - 11b: The AP works in 802.11b mode and only WiFi-enabled 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 WiFi-enabled 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 WiFi-enabled 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. WiFi-enabled devices compliant with 802.11b or 802.11g and WiFi-enabled devices working at 2.4 GHz and compliant with 802.11n can connect to the 2.4 GHz wireless networks of the AP. - 11a: The AP works in 802.11a mode and only WiFi-enabled 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 WiFi-enabled 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 WiFi-enabled 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. - 80 MHz: 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. This parameter can be set if Lock Channel is not selected.

Parameter	Description
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.
Transmit Power	Specifies the transmit power of the AP. This parameter can be set if Lock Power is not selected. A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the wireless network performance and security.
Lock Power	Specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.
Preamble	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. By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the Short Preamble option.
Short GI	Specifies whether to enable the short guard interval function. 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%.
Suppress Broadcast Probe Response	Specifies whether to enable the suppress broadcast probe response function. By default, WiFi-enabled devices keep sending Probe Request packets that include the SSID field to scan their nearby wireless networks. After receiving such packets, AP determines whether the WiFi-enabled devices are allowed to access its wireless networks based on the packets and responds using the Probe Response packets (including all Beacon frame parameters), which consumes a lot of wireless resources. After this function is enabled, this device does not respond to the requests without an SSID, saving wireless resources.

6.3 RF optimization

To access the page, [log in to the web UI of the AP](#), and navigate to **Wireless > RF Optimization**.

On this page, you can modify the radio parameters to optimize performance.



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

2.4 GHz
5 GHz

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

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

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

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

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

Signal Transmission Coverage-oriented Capacity-oriented

Air Interface Scheduling Enable Disable

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

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

Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	

Parameter	Description
Beacon Interval	<p>Used to set the interval at which this device sends Beacon frames.</p> <p>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.</p>
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>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 WiFi-enabled device is weaker than this threshold, the WiFi-enabled device cannot connect to this device.</p> <p>A proper value facilitates WiFi-enabled devices to connect to the AP with stronger signal in case of multiple APs exist.</p>

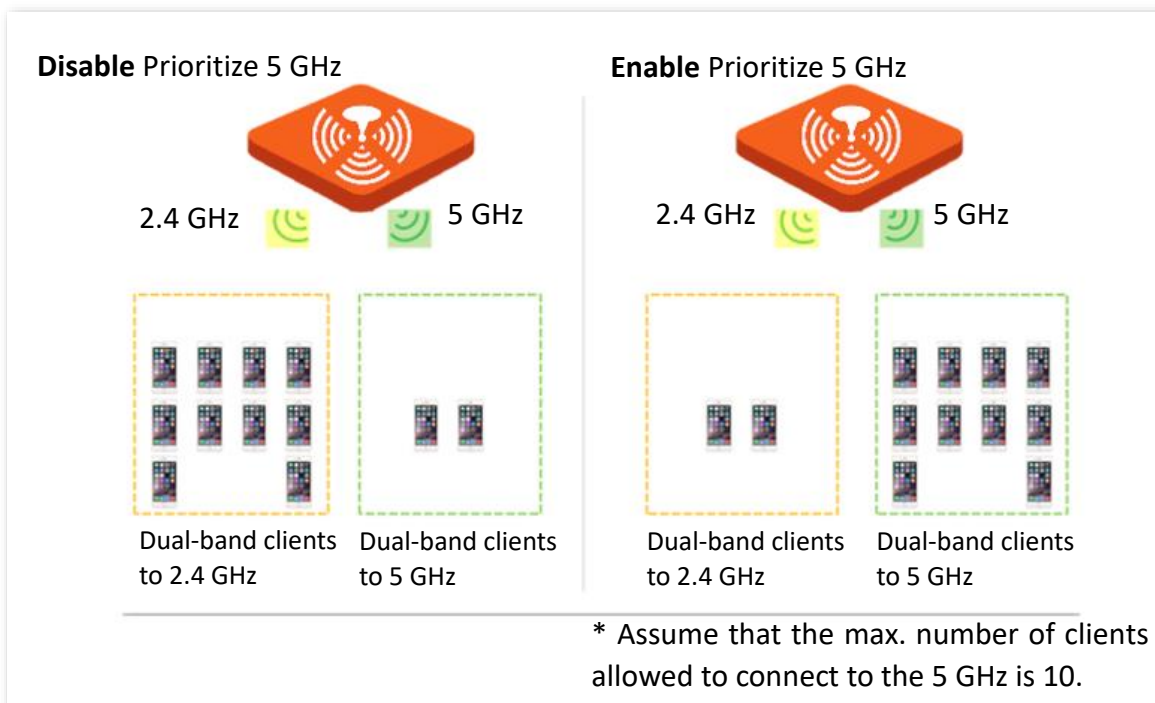
Parameter	Description
Signal Transmission	<p>Select the option based on your actual situation.</p> <ul style="list-style-type: none"> - Coverage-oriented: This mode broadens WiFi coverage of APs, and is usually used in scenarios deployed with fewer APs, such as offices, warehouses, and hospitals. - Capacity-oriented: This mode effectively decreases mutual interference among APs, and is usually used in scenarios deployed with massive APs, such as conferences, exhibition halls, banquet halls, stadiums, classrooms of higher-education institutes and airports.
Air Interface Scheduling	<p>Specifies whether to enable the air interface scheduling function of the AP.</p> <p>This enables the users experiencing high download rates to download more data, so that this device can achieve higher system throughput and connect to a greater number of clients.</p>
Anti-interference Mode	<p>Specifies the anti-interference modes you can select for your AP.</p> <ul style="list-style-type: none"> - 0 (Disable): Interference suppression measures are disabled. - 1 (Suppress weak interference): Suppress mild interference for weak radio environment. - 2 (Suppress moderate interference): Suppress moderate interference for bad radio environment. - 3 (Suppress critical interference): Suppress critical interference for heavy loading radio environment.
APSD	<p>Specifies whether to enable the automatic power save delivery function.</p> <p>APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, it is disabled.</p>
Client Timeout Interval	<p>Used to set the wireless client disconnection interval of this device. The device disconnects from a wireless client if no traffic is transmitted or received by the wireless client within the interval.</p>
Mandatory Rate	<p>Specifies rates that wireless clients must support in order to connect to the wireless networks of this device.</p>
Optional Rate	<p>Specifies the additional rates that the AP supports, which are optional to wireless clients. The clients meeting the mandatory rate can connect to the AP with higher rate.</p>
Prioritize 5 GHz	<p>Specifies whether to enable the prioritize 5 GHz function.</p> <p>If this function is enabled, dual band WiFi-enabled devices prefer the 5 GHz wireless network of the AP to connect when the 5 GHz signal strength transmitted by devices is greater than or equal to the Prioritize 5 GHz Threshold.</p>
Prioritize 5 GHz Threshold	<p>With this function enabled, if the strength of the signals transmitted by a WiFi-enabled device is greater than or equal to this threshold, the WiFi-enabled device connects to the 5 GHz wireless network. Otherwise, it connects to the 2.4 GHz wireless network.</p>

■ Prioritize 5 GHz

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

With the 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 the wireless both of the 2.4 GHz and 5 GHz are enabled, and the two bands share the same SSID, security mode and password.

■ Air interface scheduling

In mixed wireless rates environment, the traditional 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.

6.4 Frequency analysis

6.4.1 Overview

To access the page, [log in to the web UI of the AP](#), and navigate to **Wireless > Frequency Analysis**.

On this page, 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

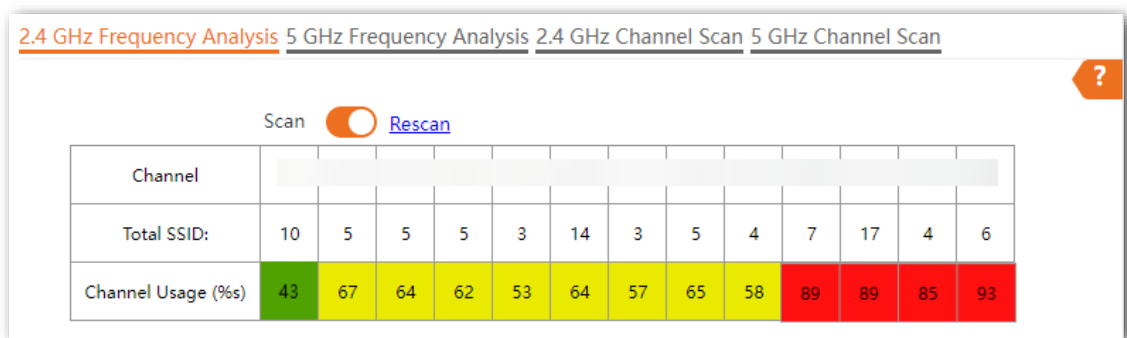
The scan result list presents you with information about nearby wireless network, including SSID, MAC address, channel, channel bandwidth, and signal strength.

6.4.2 View frequency analysis

Step 1 [Log in to the web UI of the AP](#), and navigate to **Wireless > Frequency Analysis**.

Step 2 Click **2.4 GHz Frequency Analysis** or **5 GHz Frequency Analysis** tab to select the wireless network radio band for frequency analysis, which is **2.4 GHz Frequency Analysis** in this example.

Step 3 Enable **Scan**.



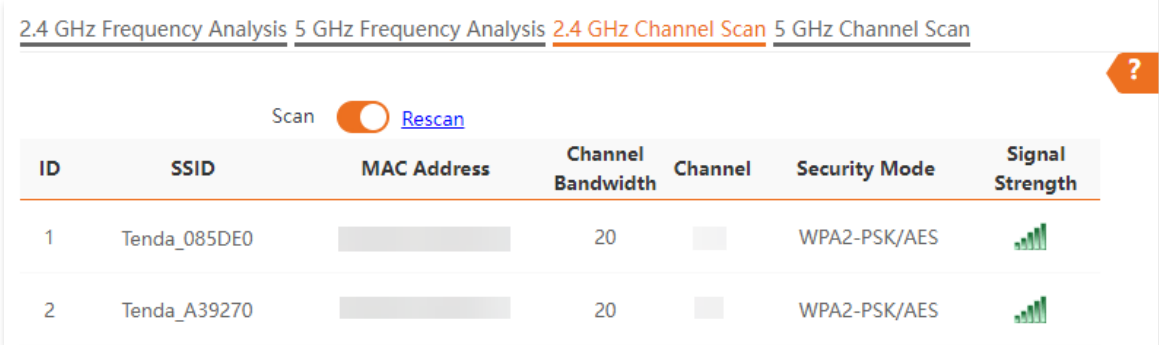
---End

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

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

6.4.3 Execute channel scan

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



The screenshot shows the '2.4 GHz Channel Scan' interface. At the top, there are four tabs: '2.4 GHz Frequency Analysis', '5 GHz Frequency Analysis', '2.4 GHz Channel Scan' (which is selected and highlighted in orange), and '5 GHz Channel Scan'. Below the tabs, there is a 'Scan' toggle switch that is turned on, and a 'Rescan' button. A question mark icon is visible in the top right corner. Below the controls is a table with the following data:

ID	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
1	Tenda_085DE0	[Redacted]	20	[Redacted]	WPA2-PSK/AES	[Signal Strength Icon]
2	Tenda_A39270	[Redacted]	20	[Redacted]	WPA2-PSK/AES	[Signal Strength Icon]

---End

6.5 WMM settings

6.5.1 Overview

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

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

WMM involves the following terms:

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

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

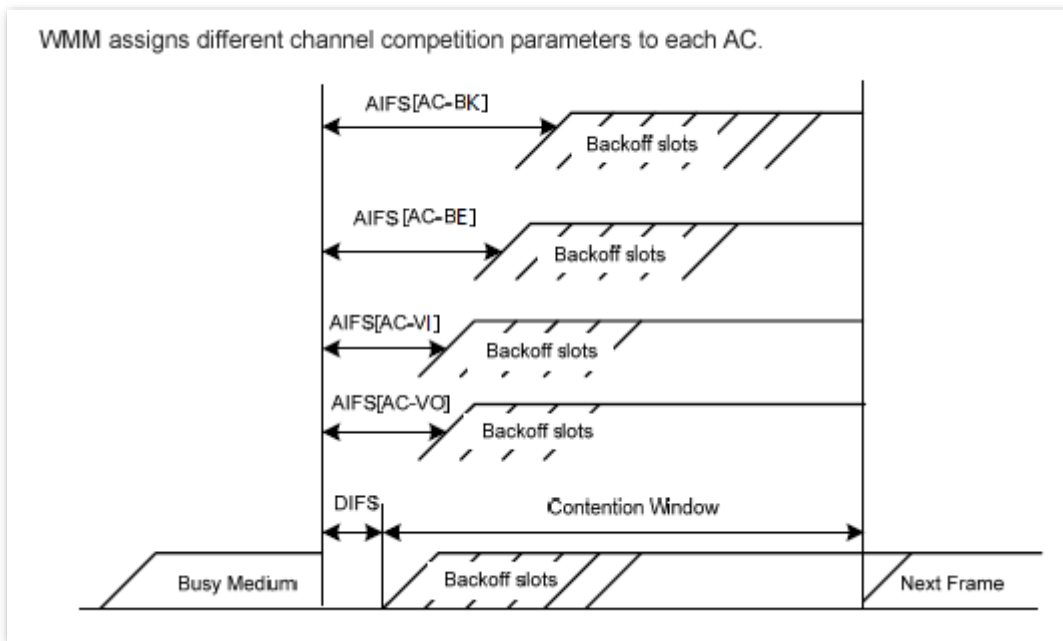
■ EDCA parameters

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

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

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

0 indicates that a device can send only one packet through a channel after winning contention for the channel.



ACK policies

WMM specifies the Normal ACK and No ACK policies.

- According to the No Acknowledgment (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.

6.5.2 Configure WMM

To access the page, [log in to the web UI of the AP](#), and navigate to **Wireless > WMM**.

On this page, you can configure related WMM parameters.

2.4 GHz 5 GHz
?

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

No ACK

EDCA AP Parameter

	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="1"/>	<input type="text" value="4096"/>
AC_BK	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="1"/>	<input type="text" value="3008"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="1"/>	<input type="text" value="1504"/>

EDCA STA Parameter

	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="3"/>	<input type="text" value="0"/>
AC_BK	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="3008"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="1504"/>

Save
Cancel

Parameter description

Parameter	Description
-----------	-------------

2.4 GHz

Used to select the radio band of the AP to be configured.

5 GHz

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.
No ACK	<p>Available only 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 improves 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 AP Parameter	
EDCA STA Parameter	<p>For details, refer to the overview of the WMM settings.</p>

6.6 Access control

6.6.1 Overview

To access the page, [log in to the web UI of the AP](#), and navigate to **Wireless > Access Control**.

On this page, you can configure the access control function to allow or disallow the devices to access the wireless network of the AP based on their MAC addresses.

The AP supports the following 2 filter modes:


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

The access control function is disabled by default. The following figure displays the page when access control is enabled.

The screenshot shows the configuration page for the AP's Access Control. At the top, there are radio buttons for '2.4 GHz' and '5 GHz'. Below that is a dropdown menu for 'SSID' set to 'Tenda_23E101'. The 'Access Control' toggle switch is turned on. Under 'Mode', the 'Blacklist' radio button is selected. A 'MAC Address' input field shows the format 'XX:XX:XX:XX:XX:XX', with 'Add' and 'Add Online Devices' buttons next to it. Below the input is a table with columns 'ID', 'MAC Address', 'Status', and 'Operation'. The table is empty, showing 'No data'. At the bottom are 'Save' and 'Cancel' buttons.

Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	

Parameter	Description
SSID	Specifies the wireless network to which the policy applies.
Access Control	Specifies whether to enable the access control function.
Mode	<p>Specifies the mode of the access control.</p> <ul style="list-style-type: none"> - Blacklist: Wireless clients with MAC addresses on the access control list cannot access the wireless network of AP. - Whitelist: Wireless clients 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 policy. You can enable or disable it as required.
Operation	Click  to delete the policy.

6.6.2 Configure access control

- Step 1** [Log in to the web UI of the AP](#), and navigate to **Wireless > Access Control**.
- Step 2** Select a wireless network radio band on which access control must be implemented.
- Step 3** Select the SSID to which the access control is applied from the **SSID** drop-down list.
- Step 4** Enable the **Access Control** function.
- Step 5** Set **Mode** to **Blacklist** or **Whitelist** as required.
- Step 6** Enter MAC addresses of the WiFi-enabled devices to which the policy applies, and click **Add**.



If the WiFi-enabled 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**.

---End

6.6.3 Example of configuring access control

Networking requirements

A wireless network whose SSID is **VIP** under the 2.4 GHz radio band has been set up in an Enterprise. 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 WiFi-enabled devices whose MAC addresses are **D8:38:0D:00:00:01**, **D8:38:0D:00:00:02**, **D8:38:0D:00:00:03**.

Configuration procedure

- Step 1** [Log in to the web UI of the AP](#), and navigate to **Wireless > Access Control**.
 - Step 2** Select **VIP** from the **SSID** drop-down list.
 - Step 3** Enable the **Access Control** function.
 - Step 4** Set **Mode** to **Whitelist**.
 - Step 5** Enter **D8:38:0D:00:00:01** in the **MAC Address** text box and click **Add**. Repeat this step to add **D8:38:0D:00:00:02** and **D8:38:0D:00:00:03**.
 - Step 6** Click **Save**.
- End

After the configuration is completed, see the following figure.

The screenshot shows the configuration page for the wireless network. At the top, there are tabs for '2.4 GHz' and '5 GHz'. The SSID is set to 'VIP'. The 'Access Control' toggle is turned on. The 'Mode' is set to 'Whitelist' (selected with a radio button). Below this, there is a 'MAC Address' input field with a format hint 'Format: XX:XX:XX:XX:XX:XX' and two buttons: 'Add' and 'Add Online Devices'. A table below lists the configured MAC addresses:

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

At the bottom of the page, there are two buttons: 'Save' (highlighted in orange) and 'Cancel'.

Verification

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

6.7 Advanced settings

To access the page, [log in to the web UI of the AP](#), and navigate to **Wireless > Advanced Settings**.

On this page, you can set the client type identification, broadcast packet filter and fast roaming of the AP.

■ Identify client type

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

■ Broadcast packet filter

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

Parameter description

Parameter	Description
Identify Client Type	Specifies whether to enable the identify client type function. With the function enabled and the client accesses the http URL, the operating system type of WiFi-enabled devices connected to the AP's wireless network can be viewed by navigating to Status > Client List .
Broadcast Packet Filter	Specifies whether to enable the broadcast packet filter function. With the function enabled, the AP can reduce air interface resources usage and ensure the bandwidth for business data transfer.

6.8 QVLAN settings

6.8.1 Overview

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

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

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

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

To access the page, [log in to the web UI of the AP](#), and navigate to **Wireless > QVLAN Settings**.

On this page, you can set VLAN IDs of all wireless networks.

QVLAN Settings ?

QVLAN

Set the VLAN of AP, the management host must belong to the same VLAN as the AP to access the management page of AP;

PVID

Management VLAN


2.4 GHz SSID VLAN ID (1 to 4094)

Tenda_23E101

5 GHz SSID VLAN ID (1 to 4094)

Tenda_23E108_5G

Parameter description

Parameter	Description
QVLAN	Specifies whether to enable the 802.1Q QVLAN function of the AP. By default, it is disabled.
PVID	Specifies the ID of the default native VLAN of the trunk port of the AP. The default value is 1.
Management VLAN	Specifies the ID of the AP management VLAN. The default value is 1. After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
2.4 GHz SSID	Specify the currently enabled SSIDs of the AP at 2.4 GHz or 5 GHz band, and VLAN IDs corresponding to SSIDs.
5 GHz SSID	 TIP
VLAN ID	After the VLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID and VLAN ID of an access port are the same.

6.8.2 Example of configuring QVLAN settings

Networking requirements

A hotel has the following wireless network coverage requirements:

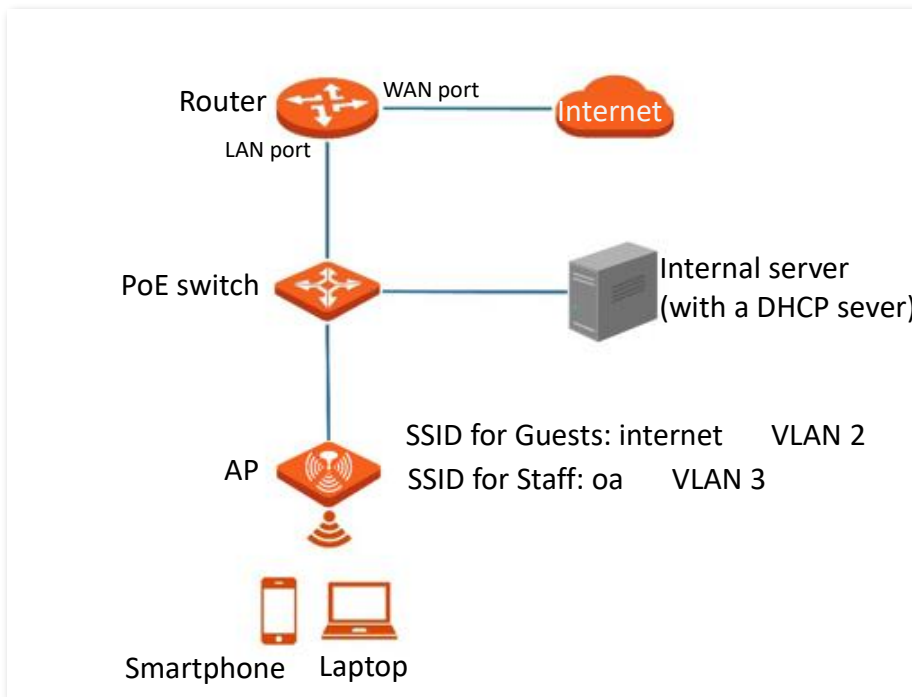
- Guests are connected to VLAN 2 and can access only the internet.
- Staff are connected to VLAN 3 and can access only the intranet.

Solution

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



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



Configuration procedure

I. Configure the AP

- Step 1** [Log in to the web UI of the AP](#) and navigate to **Wireless > QVLAN Settings**.
- Step 2** Enable the **QVLAN** function.
- Step 3** Modify the VLAN ID of the SSIDs at 2.4 GHz band. Set the VLAN ID of **internet** to **2** and **oa** to **3** respectively.
- Step 4** Click **Save**.

QVLAN Settings ?

*** QVLAN**

Set the VLAN of AP, the management host must belong to the same VLAN as the AP to access the management page of AP;

PVID

Management VLAN

2.4 GHz SSID VLAN ID (1 to 4094)

*** internet**

*** oa**

5 GHz SSID VLAN ID (1 to 4094)

Tenda_23E108_5G

II. Configure the switch

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

Port connected to	Accessible VLAN ID	Port type	PVID
AP	1,2,3	Trunk	1
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.

---End





Verification

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


6.9 WiFi schedule

To access the page, [log in to the web UI of the AP](#), and navigate to **Wireless > WiFi Schedule**.

On this page, you can disable the WiFi network of the AP during a specified period. During the scheduled disable period, WiFi-enabled devices such as smartphones cannot search for the WiFi networks.

2.4 GHz		5 GHz		
SSID	Status	Schedule	WiFi Disable Period	Operation
Tenda_23E100	Enabled	Disabled	-	
Tenda_23E101	Enabled	Disabled	-	
Tenda_23E102	Disabled	Disabled	-	
Tenda_23E103	Disabled	Disabled	-	

Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	
SSID	Specifies the name of the wireless network.
Status	Specifies the status of the wireless network, including Enabled or Disabled .
Schedule	Specifies the status of the WiFi schedule of the wireless network.
WiFi Disable Period	Specifies the period when the wireless network automatically disables.
Operation	Click  to set the WiFi schedule function of the wireless network, including enabling or disabling the WiFi schedule function and setting the period for the wireless network to automatically disable.

7 Advanced settings

7.1 Traffic control

7.1.1 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.


To access the page, [log in to the web UI of the AP](#), and navigate to **Advanced > Traffic Control**.

By default, the traffic control function is disabled. The following figure displays the page when traffic control is enabled.

Radio Band	SSID	SSID Max. Upload Rate	SSID Max. Download Rate	Client Max. Upload Rate	Client Max. Download Rate	Operation
2.4GHz	Tenda_23E100	No Limit	No Limit	No Limit	No Limit	

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 the maximum upload or download rate of SSIDs and 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.

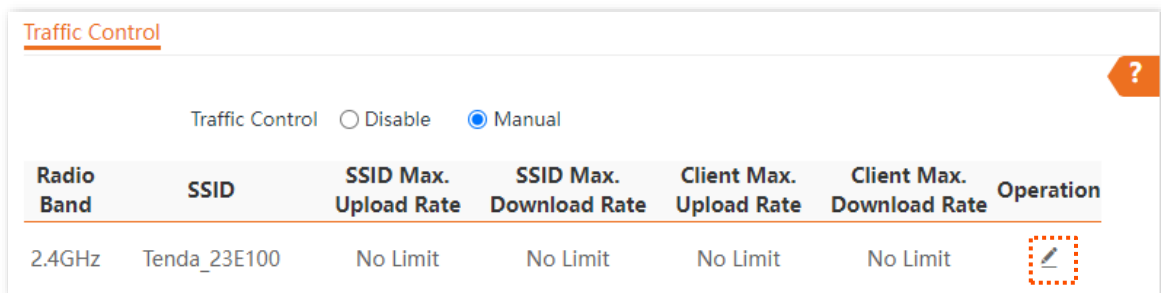
Parameter	Description
SSID	Specifies the name of the wireless network on which you manually set a traffic control rule.
SSID Max. Upload Rate	Specify the maximum upload or download rate allowed for a wireless network. If you leave it blank, the maximum upload or download rate of the target wireless network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

7.1.2 Configure traffic control

Step 1 [Log in to the web UI of the AP](#), and navigate to **Advanced > Traffic Control**.

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

Step 3 Click  on the row where the wireless network to be controlled resides.



Step 4 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.

Step 5 Click **Add**.

SSID Traffic Control Policy ✕

Radio Band 2.4GHz

SSID Tenda_23E100

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

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

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

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

---End

7.2 Cloud maintenance

7.2.1 Overview

The Tenda CloudFi cloud management system is a cloud platform established by Tenda, providing central management for Tenda devices that support cloud management.

The AP can be managed by the Tenda CloudFi cloud platform. You can configure and check the parameters of the router on the web UI of the Tenda CloudFi cloud platform (<https://cloudfi.tendacn.com>) or Tenda CloudFi App.

To access the page, [log in to the web UI of the AP](#), and navigate to **Advanced > Cloud Maintenance**.

On this page, you can add the AP to the Tenda CloudFi cloud platform.

The cloud maintenance function is disabled by default. The following figure displays the page when cloud maintenance is enabled.

Cloud Maintenance

Cloud Maintenance

Management Mode

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.

Parameter description

Parameter	Description
Cloud Maintenance	Specifies whether to enable the cloud maintenance function of the AP.

Parameter	Description
Management Mode	<p>Specifies the mode under which your AP is managed.</p> <ul style="list-style-type: none"> - Cloud Management: Applicable to scenarios that require unified configuration and maintenance through the Tenda CloudFi cloud platform. In this mode, the AP can be managed by the Tenda CloudFi cloud platform and the configuration of relevant functions is delivered by the CloudFi cloud platform. - Local Management: Applicable to scenarios that require unified status monitoring through the Tenda CloudFi cloud platform. In this mode, the AP can be managed on the Tenda CloudFi cloud platform, but all configurations of the AP are completed on its own web UI, and the information is reported to the Tenda CloudFi cloud platform.
Unique Cloud Code	<p>Specifies the Tenda CloudFi cloud platform account associated with the device. You can obtain this code from the web UI of the Tenda CloudFi cloud platform (https://cloudfi.tendacn.com) or Tenda CloudFi App.</p>
Report	<p>Specifies whether to enable the report function. This function is disabled by default.</p> <p>If this function is enabled, parameter information of your APs is reported to the Tenda CloudFi cloud platform and you can manage and maintain your APs on the platform.</p>

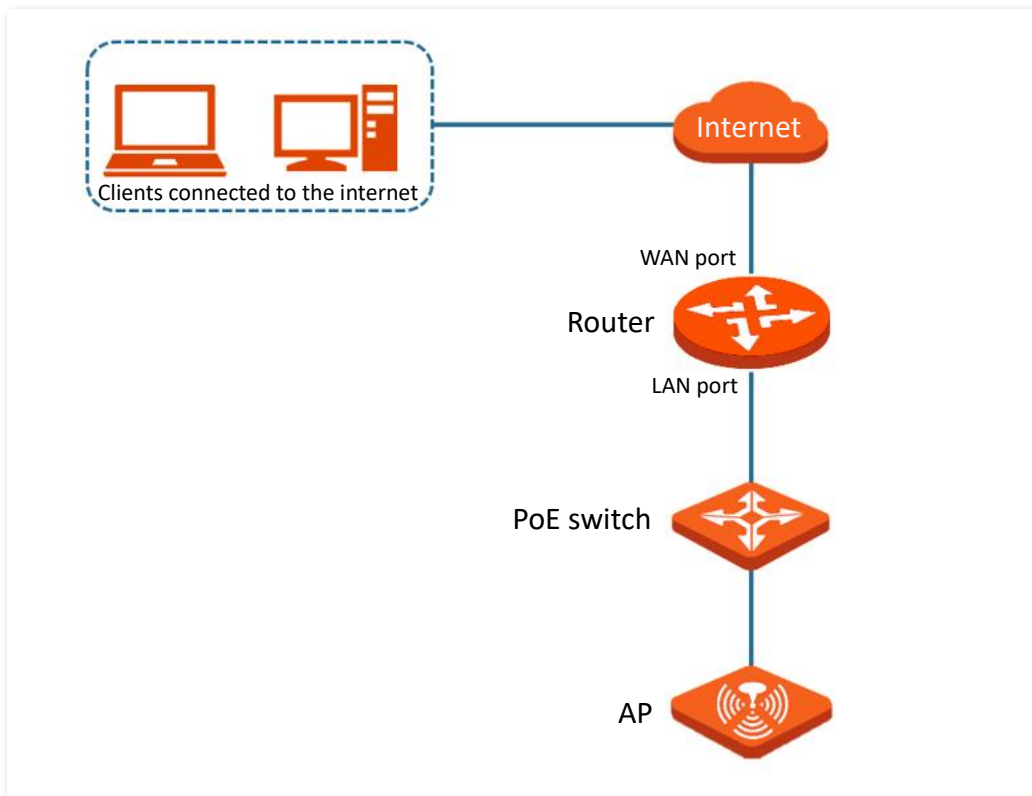
7.2.2 Example of configuring cloud maintenance on web UI

Networking requirements

An enterprise uses the AP to set up a network and has connected to the internet. The requirements are managing the AP remotely and delivering related configurations.

Solution

You can use the cloud management function of the AP and Tenda CloudFi cloud platform web UI (<https://cloudfi.tendacn.com>) to meet the requirements.



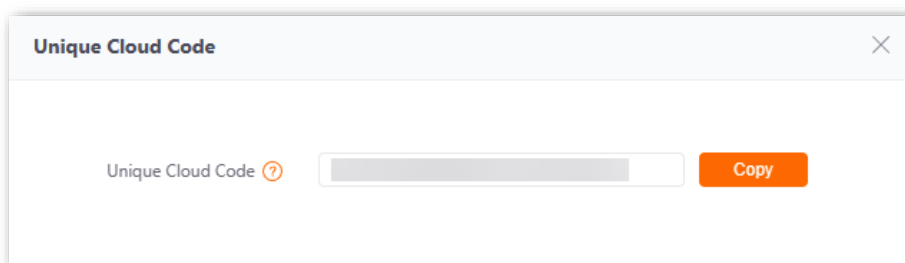
Configuration procedure



Before configuring the cloud maintenance function of the AP, ensure that the internet where the AP is deployed is connected.

I. Log in to Tenda CloudFi 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 CloudFi cloud platform.
- Step 2** Click **Add** in the upper right corner and select **Unique Cloud Code**.
- Step 3** Click **Copy** to copy the **Unique Cloud Code**.



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 Management**.
 2. Paste the **Unique Cloud Code** in the input box.
 3. Enable the **Report** function.
- Step 5** Click **Save**.

Cloud Maintenance

Cloud Maintenance

Management Mode Cloud Management

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.

Save **Cancel**

III. Log in to Tenda CloudFi 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 CloudFi cloud platform.
- Step 2** Click **Add** in the upper right corner and select **Device-joining Alert** from the drop-down list menu.
- Step 3** Select the AP to be added to the project and click **Add Device to Project**. The following figure is for reference only.

Device-joining Alert

Add Device to Project

<input checked="" type="checkbox"/>	Device Type	Model	MAC Address	Public IP Address	Request Time ↑
<input checked="" type="checkbox"/>	AP	i23V1.0			2024-08-21 02:25:10 (GMT)

- Step 4** Select the project to which you want to add the router. The following figure is for reference only.
- If the project has already been created, select **Existing Project** and select the corresponding project in the **Project Name** drop-down menu, and then click **Confirm**.

Add Device to Project [Close]

Add Device to Existing Project
 Add Project

Project Name

Project Scenario

Project Location

Time Zone

[Cancel] [Confirm]

- If you want to create a new project, select **Add Project**, set the **Project Name**, **Project Scenario**, **Project Location** and **Time Zone**, and then click **Confirm**.

Add Device to Project [Close]

Add Device to Existing Project
 Add Project

Project Name

Project Scenario

Project Location

Time Zone

[Cancel] [Confirm]

---End

Added successfully. You can enter the management page of the project to view details. The following figure is for reference only.

Project

Overview | Project

All (1) [Add Project] Search

No.	Status	Project Name	Project Property	Project Scenario	Project Location	Online Devices	Offline Devices	Unread Alarms	Operation
1	Online	XX Enterprise Network	By Creation	Office	American Samoa-Swains	1	-	-	[Edit] [Delete] [Share]

Verification

After the configuration is completed, the AP can be managed through the web UI of the Tenda CloudFi cloud platform (<https://cloudfi.tendacn.com>), and all its configuration is delivered by the Tenda CloudFi cloud platform.

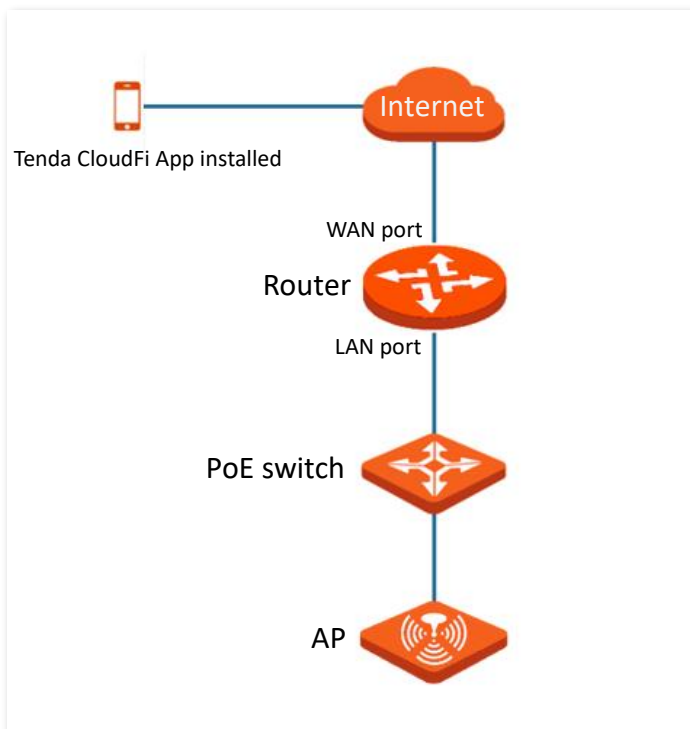
7.2.3 Example of configuring cloud maintenance on App

Networking requirements

An enterprise uses the AP to set up a network and has connected to the internet. The requirements are managing the AP remotely and delivering related configurations.

Solution

You can use the cloud management function of the AP and Tenda CloudFi App to meet the requirements.



Configuration procedure (method 1)



TIP

Before configuring the cloud maintenance function of the AP, ensure that the internet where the AP is deployed is connected.

- Step 1** Download the CloudFi App to your mobile device by scanning the QR code or searching for **Tenda CloudFi** in **Google Play** or **App Store**.



Step 2 Connect a WiFi-enabled device such as a smartphone to the AP's wireless network.

Step 3 Log in to the Tenda CloudFi App, and add the AP to the Tenda CloudFi App.

1. Add a project on the CloudFi App. (Skip if performed)
2. Enter the project where the AP is to be added, tap the pop-up window that shows the AP is detected, and then follow the prompts to add the AP to the project.

---End

You can view the help documentation of the CloudFi App on the **Help Center** page of the CloudFi App for specific methods.

Configuration procedure (method 2)



Before configuring the cloud maintenance function of the AP, ensure that the internet where the AP is deployed is connected.

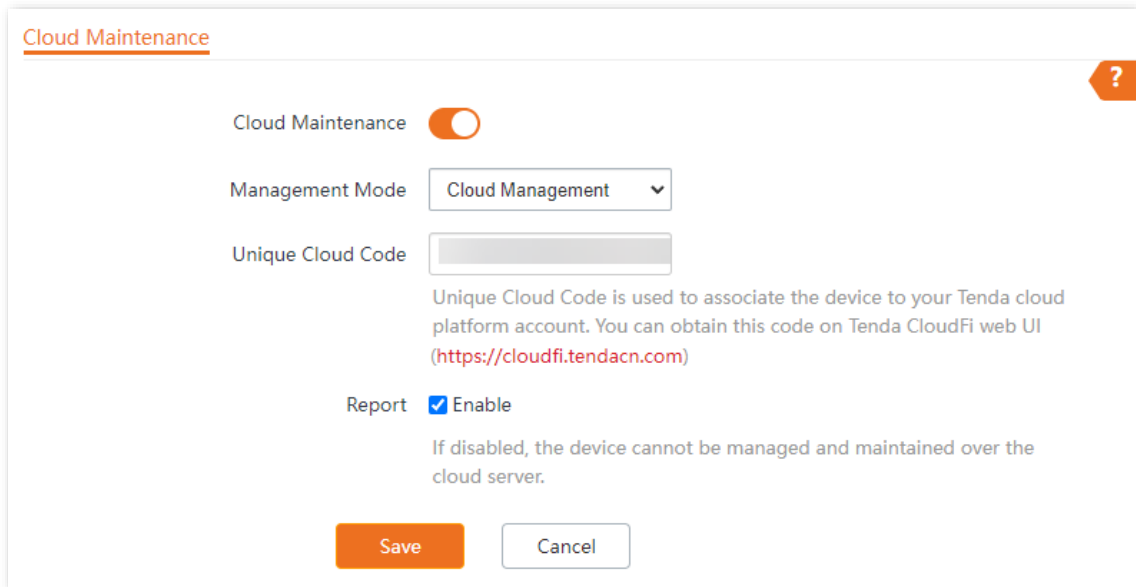
Step 1 Download the CloudFi App to your mobile device by scanning the QR code or searching for **Tenda CloudFi** in **Google Play** or **App Store**.



Step 2 Enable the cloud maintenance function for the AP.

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

- Click **Save**.



Cloud Maintenance ?

Cloud Maintenance

Management Mode Cloud Management ▼

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.

Save Cancel

- Step 3** Log in to the Tenda CloudFi App, and add the AP to the Tenda CloudFi App.
1. Add a project on the CloudFi App. (Skip if performed)
 2. Follow the prompts to add the AP to the project on the **Device-joining Alert** page.
- End

You can view the help documentation of the CloudFi App on the **Help Center** page of the CloudFi App for specific methods.

Verification

After the configuration is completed, the AP can be managed through the Tenda CloudFi cloud management system, and all its configuration is delivered by the CloudFi cloud platform.

8 Tools

8.1 Date & Time

To access the page, [log in to the web UI of the AP](#), and navigate to **Tools > Date & Time**.

On this page, you can set the [system time](#) and [login timeout interval](#) of the AP.

8.1.1 System time

To access the page, [log in to the web UI of the AP](#), and navigate to **Tools > Date & Time > System Time**.

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

The AP allows you to set the system time by [synchronizing the time with the internet](#) or [manually setting the time](#).

Synchronize with internet time

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

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



System Time Login Timeout Interval

Time Setup Sync with Internet Time Manual

Sync Interval 30 min

Time Zone (GMT) Greenwich Mean Time

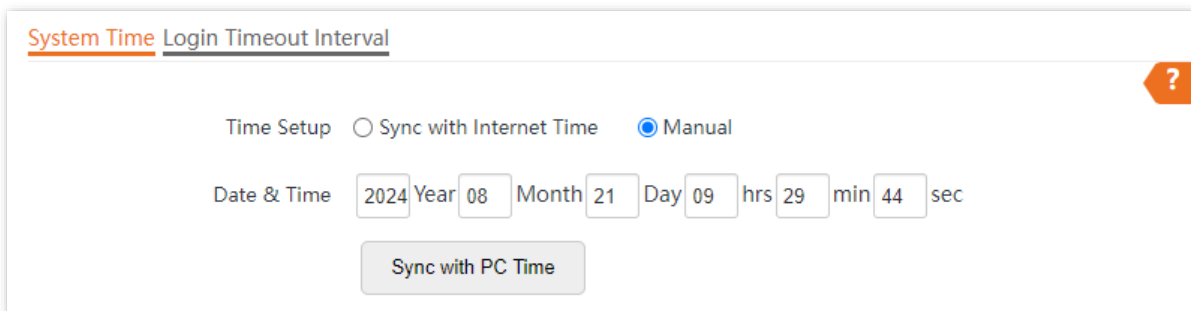
Parameter description

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

Manually set the time

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

Enter a correct date and time, or click **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 2024 Year 08 Month 21 Day 09 hrs 29 min 44 sec

Sync with PC Time

8.1.2 Login timeout interval

To access the page, [log in to the web UI of the AP](#), and navigate to **Tools > Date & Time > Login Timeout Interval**.

On this page, you can set the login timeout interval.

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

8.2 Maintenance

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

8.2.1 Reboot

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



Rebooting the AP will disconnect all connections. You are recommended to reboot the AP at an idle hour.

Manual reboot

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

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

Reboot schedule

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

The AP can reboot:

- [Reboot interval](#): The AP reboots at the interval that you specify.
- [Reboot schedule](#): The AP automatically reboots at the specified date and time.

Configure the AP to reboot at an interval

- Step 1** [Log in to the web UI of the AP](#), and navigate to **Tools > Maintenance > Reboot Schedule**.
- Step 2** Enable the **Reboot Schedule** function.
- Step 3** Set **Type** to **Reboot Interval**.
- Step 4** Set **Interval** to a value in minutes, which is **1440** in this example.
- Step 5** Click **Save**.

Maintenance **Reboot Schedule**

Reboot Schedule

Type

Interval min(Range: 10 to 7200)

---End

After the configuration is completed, the AP will automatically reboot in a day.

Configure the AP to reboot at specified time



TIP

Rebooting at specified time 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](#), and navigate to **Tools > Maintenance > Reboot Schedule**.
- Step 2** Enable the **Reboot Schedule** function.
- Step 3** Set **Type** to **Reboot Schedule**.
- Step 4** Select the date when the AP reboots, which is **Monday to Friday** in this example.
- Step 5** Set the time when the AP reboots, which is **3:00** in this example.
- Step 6** Click **Save**.

Maintenance **Reboot Schedule**

Reboot Schedule

Type

Reboot On Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday Every Day

Reboot At (Default:3:00)

---End

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

8.2.2 Reset

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

NOTE

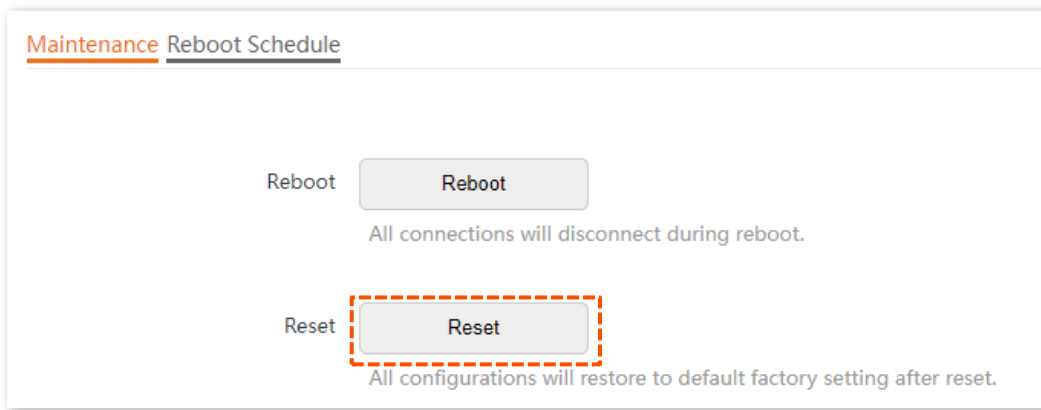
- When the factory settings are restored, your configuration will be cleared. Therefore, you need to reconfigure the AP to reconnect to the internet. Restore the factory settings of the AP only when necessary.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.
- After the factory settings are restored, the login IP address of the AP is changed to **192.168.0.254** by default, and you need to configure the username and password to log in to the web UI of the AP.

Method 1

When the AP is idle, hold the reset button (**Reset**) down with a needle-like object for about 8 seconds, and release it when the indicator lights solid green. When the indicator blinks green again, the AP is reset successfully.

Method 2

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



8.2.3 Firmware upgrade

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

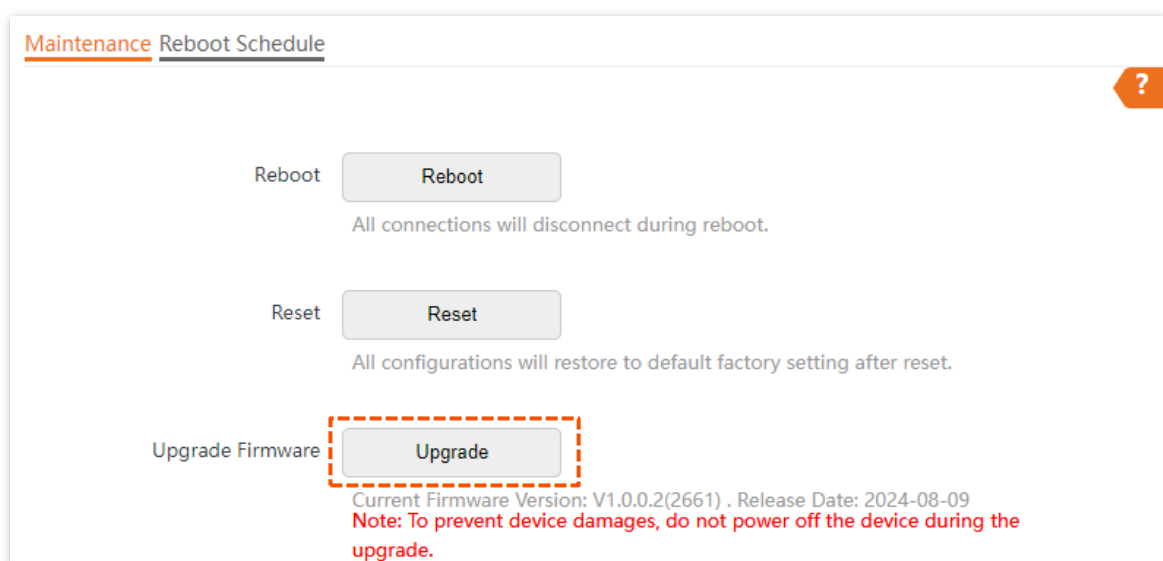


To ensure a correct upgrade and avoid damage, please:

- Ensure that the new firmware is applicable to the AP. Generally, the format of the decompressed file is suffixed with **.bin**.
- Keep a proper power supply to the AP during the upgrade.

Configuration procedure

- Step 1** Download the package of a later firmware version for the AP from www.tendacn.com to your local computer, and decompress the package. Generally, the package is in the format of **.bin**.
- Step 2** [Log in to the web UI of the AP](#), and navigate to **Tools > Maintenance > Maintenance**.
- Step 3** Click **Upgrade**.



- Step 4** Select 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, you are recommended to restore the factory settings of the AP and configure the AP again, so as to ensure stability of the AP and proper operation of new functions.

8.2.4 Backup/Restore

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

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

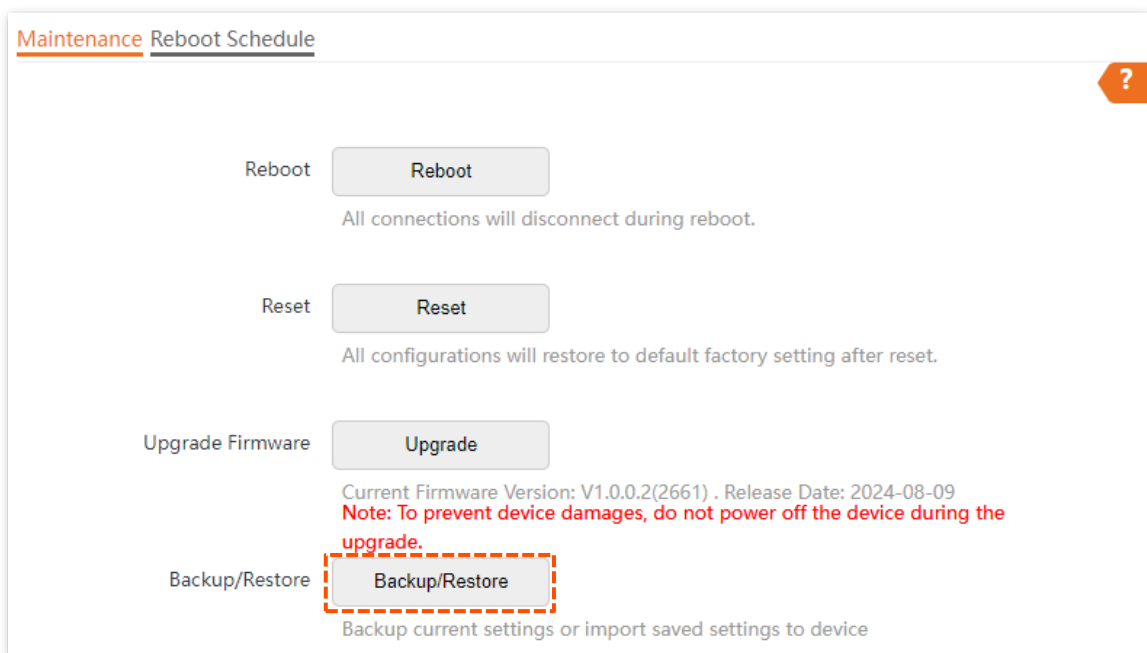


If you need to apply same or similar configurations to many APs, you can configure one of the APs, back up the configuration of the AP, and use the backup to restore the configuration on the other APs. This improves configuration efficiency.

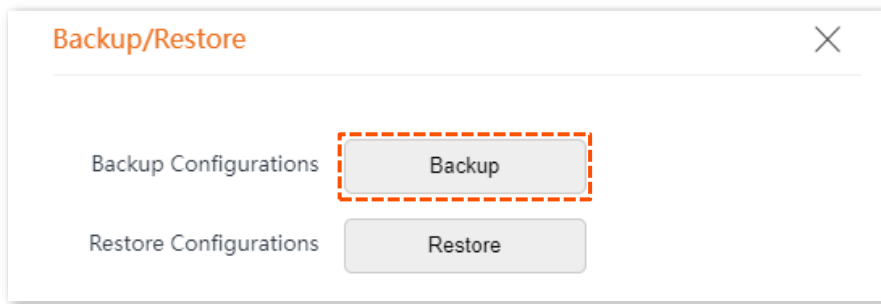
Back up the current configuration

Step 1 [Log in to the web UI of the AP](#), and navigate to **Tools > Maintenance > Maintenance**.

Step 2 Click **Backup/Restore**.



Step 3 Click **Backup**.



---End

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

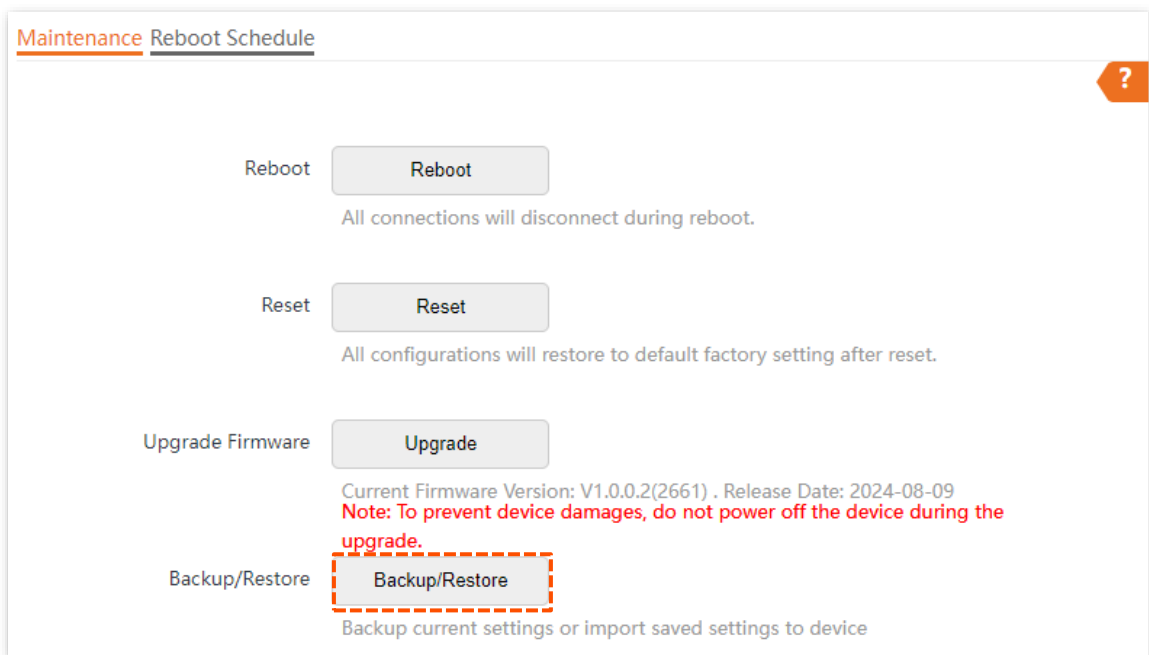


If the prompt "This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?" appears, click "Keep".

Restore a configuration

Step 1 [Log in to the web UI of the AP](#), and navigate to **Tools > Maintenance > Maintenance**.

Step 2 Click **Backup/Restore**.



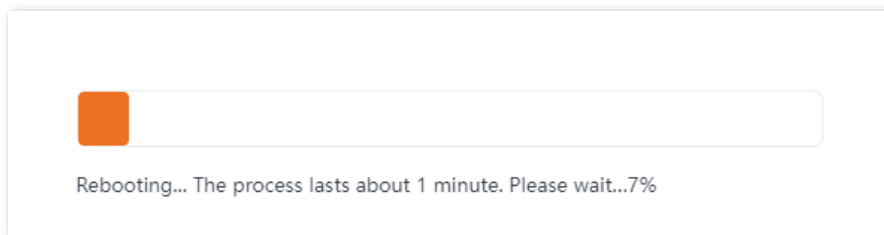
Step 3 Click **Restore**.



Step 4 Select the file of the configuration to be restored.

---End

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



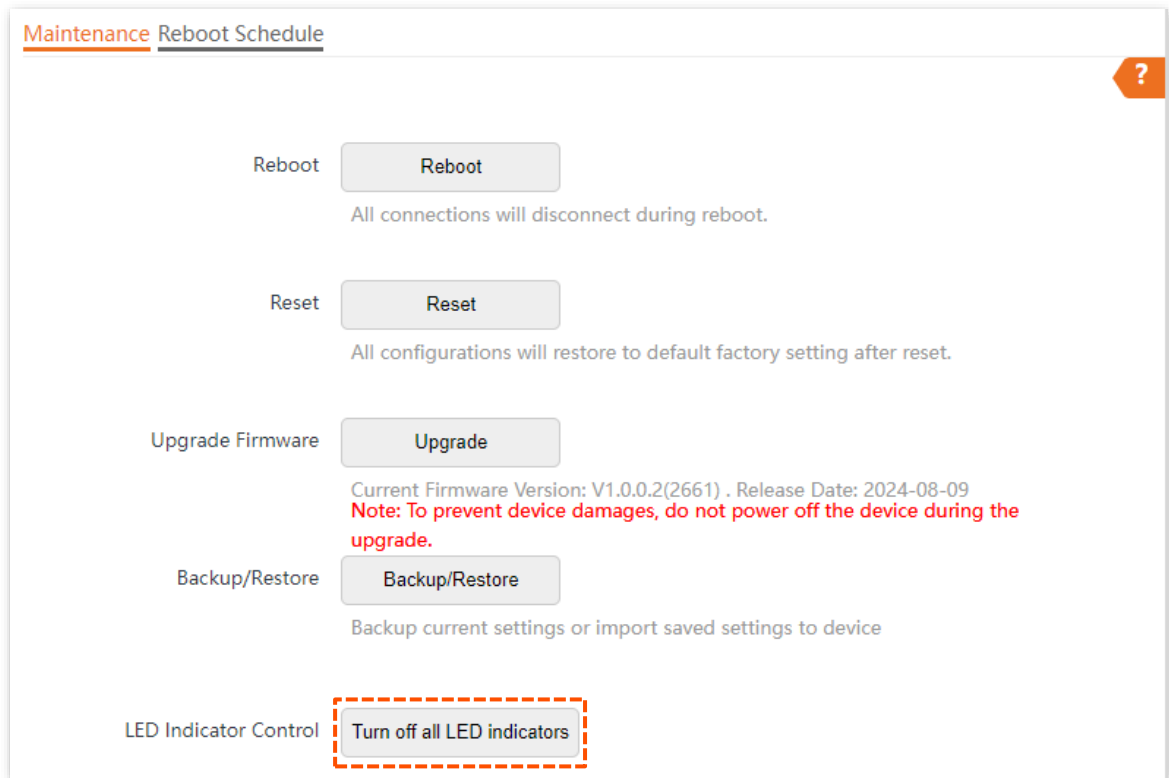
8.2.5 LED indicator control

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

Turn off the LED indicator

Step 1 [Log in to the web UI of the AP](#), and navigate to **Tools > Maintenance > Maintenance**.

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



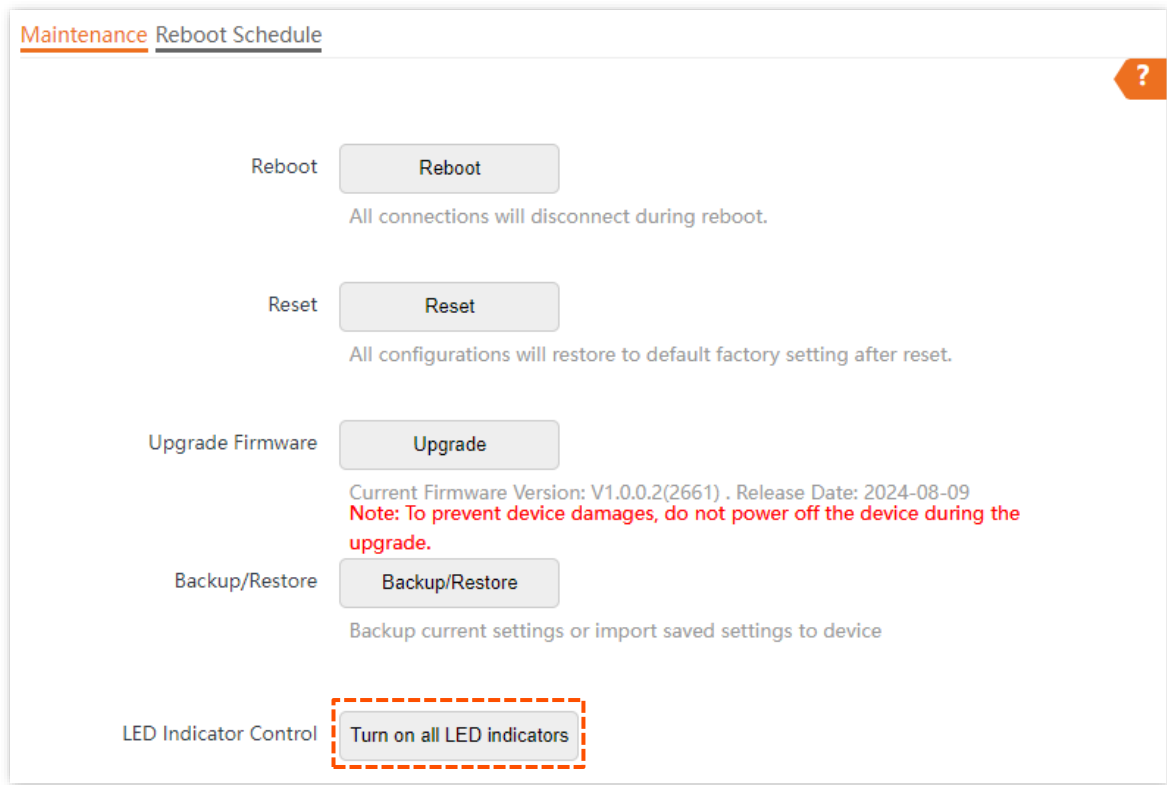
---End

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

Step 1 [Log in to the web UI of the AP](#), and navigate to **Tools > Maintenance > Maintenance**.

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



---End

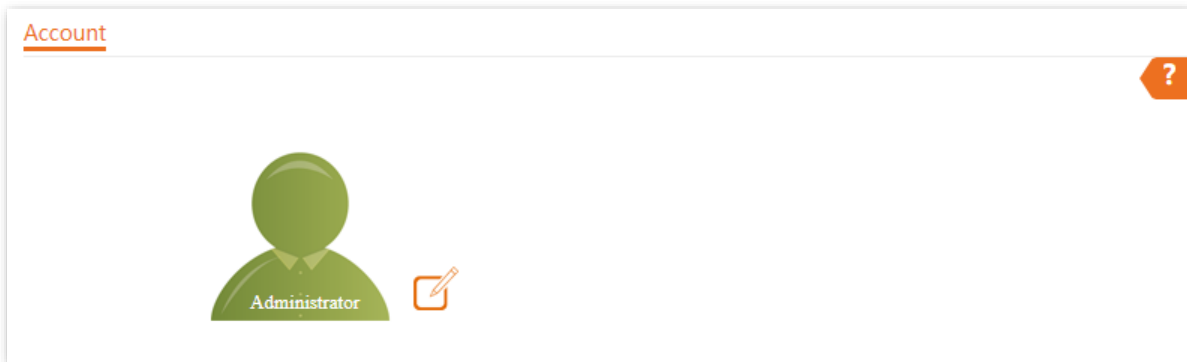
After the configuration is completed, the LED indicator lights up again and you can judge the working status of the AP.

8.3 Account

8.3.1 Overview


To access the page, [log in to the web UI of the AP](#), and navigate to **Tools > Account**.

On this page, you can modify the information of the account to keep unauthorized users from entering the web UI and modifying configurations, thus protecting the wireless network.



8.3.2 Change the password and user name of login account

Step 1 [Log in to the web UI of the AP](#), and navigate to **Tools > Account**.

Step 2 Click  beside the account to be modified.

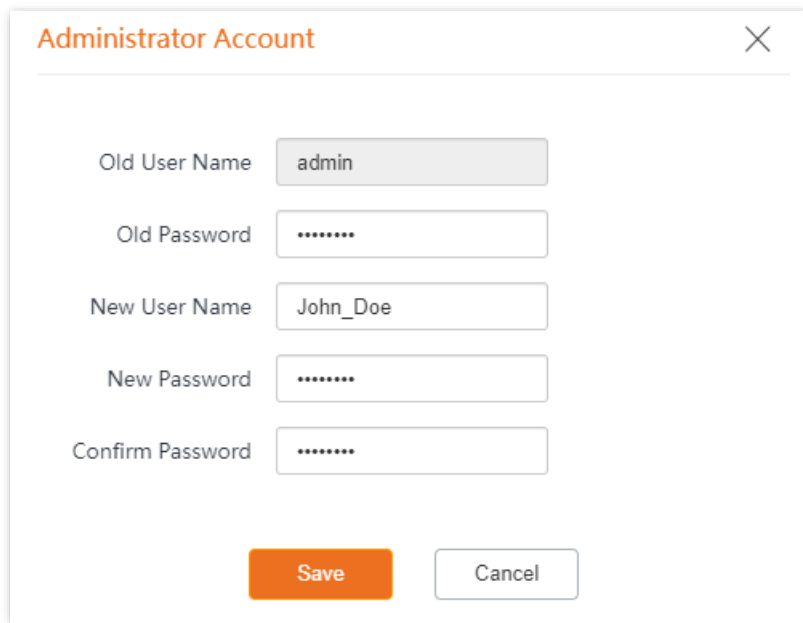
Step 3 Enter the current password in **Old Password**.

Step 4 Enter the new user name in **New User Name**, which is **John_Doe** in this example.

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

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

Step 7 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. The "Old User Name" field is pre-filled with "admin". The "Old Password" field contains seven dots. The "New User Name" field is pre-filled with "John_Doe". The "New Password" field contains seven dots. The "Confirm Password" field contains seven dots. At the bottom, there is an orange "Save" button and a white "Cancel" button with a grey border.

Old User Name	<input type="text" value="admin"/>
Old Password	<input type="password" value="....."/>
New User Name	<input type="text" value="John_Doe"/>
New Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>

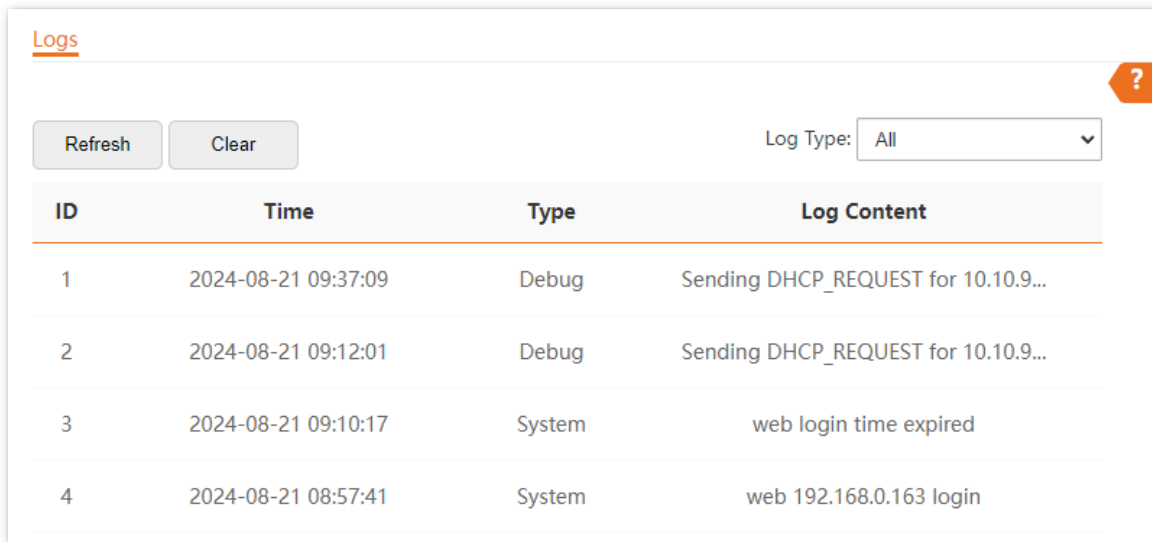
---End

Then you will be redirected to the login page. Enter the new user name and password, and click **Login** to log in to the web UI of the AP.

8.4 System log

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

To access the page, [log in to the web UI of the AP](#), and navigate to **Tools > System Log**.



ID	Time	Type	Log Content
1	2024-08-21 09:37:09	Debug	Sending DHCP_REQUEST for 10.10.9...
2	2024-08-21 09:12:01	Debug	Sending DHCP_REQUEST for 10.10.9...
3	2024-08-21 09:10:17	System	web login time expired
4	2024-08-21 08:57:41	System	web 192.168.0.163 login

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

By default, the latest 300 logs are saved. To view the latest logs of the AP, click **Refresh**. To clear the existing logs of the AP, click **Clear**. Select only **Debug** or **System** log type from the **Log Type** drop-down list box.

NOTE

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

8.5 Diagnostic tool

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

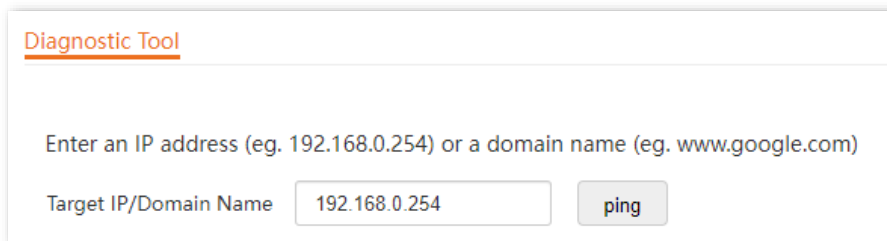
Configuration procedure

The link to **192.168.0.254** is used as an example.

Step 1 [Log in to the web UI of the AP](#), and navigate to **Tools > Diagnostic Tool**.

Step 2 Enter the IP address or domain name to be pinged in the **Target IP/Domain Name** text box, which is **192.168.0.254** in this example.

Step 3 Click **ping**.



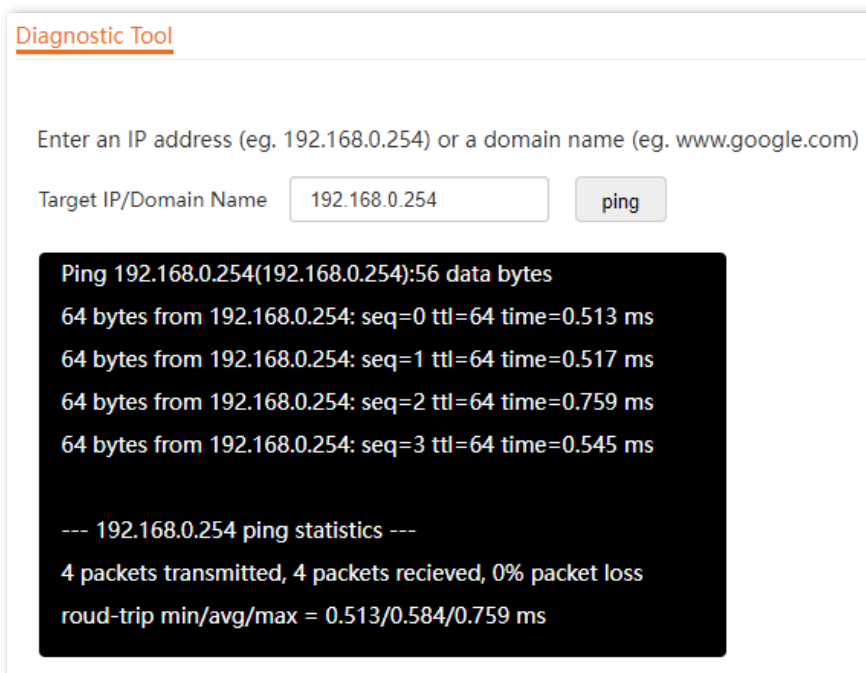
Diagnostic Tool

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

Target IP/Domain Name

---End

The diagnosis result will be displayed in a few seconds in the black text box below the **Target IP/Domain Name** text box. 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 192.168.0.254(192.168.0.254):56 data bytes
64 bytes from 192.168.0.254: seq=0 ttl=64 time=0.513 ms
64 bytes from 192.168.0.254: seq=1 ttl=64 time=0.517 ms
64 bytes from 192.168.0.254: seq=2 ttl=64 time=0.759 ms
64 bytes from 192.168.0.254: seq=3 ttl=64 time=0.545 ms

--- 192.168.0.254 ping statistics ---
4 packets transmitted, 4 packets recieved, 0% packet loss
roud-trip min/avg/max = 0.513/0.584/0.759 ms
```

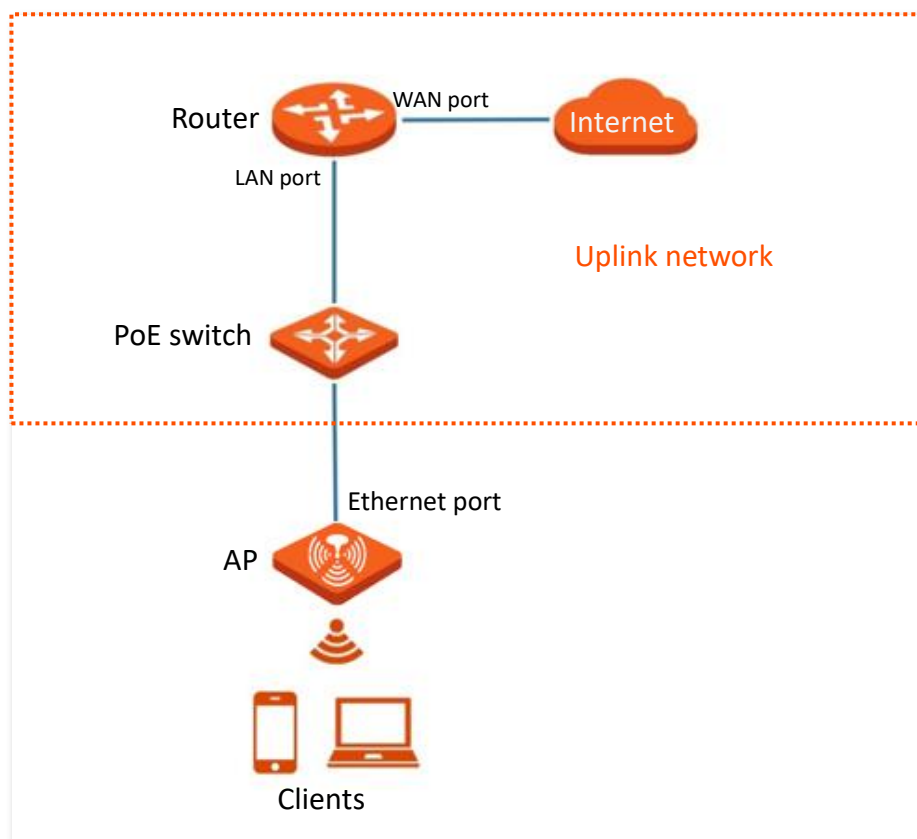
8.6 Uplink detection

8.6.1 Overview

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

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

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



8.6.2 Configure uplink detection

Step 1 [Log in to the web UI of the AP](#), and navigate to **Tools > Uplink Detection**.

Step 2 Enable the **Uplink Detection** function.

- Step 3** Set **Host 1 to Ping** or **Host 2 to Ping** to the IP address of the host to be pinged through the LAN port of the AP, such as the IP address of the switch or router directly connected to the AP.
- Step 4** Set **Ping Interval** to the interval at which the AP checks its uplink.
- Step 5** Click **Save**.

---End


Parameter description

Parameter	Description
Uplink Detection	Specifies whether to enable the uplink detection function of the AP.
Host1 to Ping	Specify the IP address of the host to be pinged through the LAN port of the AP. It is available only when the uplink detection function is enabled.
Host2 to Ping	
Ping Interval	Specifies the interval at which the AP detects the uplink. It is available only when the uplink detection function is enabled. The default value is 10 .

Appendixes

A.1 Factory default settings

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

Parameter		Default Value
Login	Management IP address	192.168.0.254
Quick Setup	Working Mode	AP Mode
Internet Settings	IP Address	Static IP Address
		 TIP With the DHCP server in the LAN, the AP may obtain an IP address from a DHCP server and you can check the new IP address from the client list of the DHCP server. It is available only when the AP is in factory settings.
		192.168.0.254
	Subnet Mask	255.255.255.0
SSID Settings	SSID	2.4 GHz The AP allows X SSIDs. For details, you can log in to the web UI of the AP and view the related parameters on the Wireless > SSID page. The SSID displayed is Tenda_XXXXXX. Where XXXXXX indicates the range from the last 6 characters to the last 6 characters + X-1 of the MAC address of the LAN ports of the AP. By default, the first SSID is enabled, and the other SSIDs are disabled.
		5 GHz The AP allows Y SSIDs. For details, you can log in to the web UI of the AP and view the related parameters on the Wireless > SSID page. The SSID displayed is Tenda_XXXXXX_5G. Where XXXXXX indicates the range from the last 6 characters + X to the last 6 characters + X + Y-1 of the MAC address of the LAN ports of the AP. By default, the first SSID is enabled, and the other SSIDs are disabled.
RF Settings	Wireless Network	Enable

A.2 Acronyms & Abbreviations

Acronym or Abbreviation	Full Spelling
AC	Access Category
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
ASCII	American Standard Code for Information Interchange
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EDCA	Enhanced Distributed Channel Access
GI	Guard Interval
ID	Identity Document
IP	Internet Protocol
IPTV	Internet Protocol Television
LAN	Local Area Network
MAC	Media Access Control
MU-MIMO	Multi-User Multiple-Input Multiple-Output
OFDMA	Orthogonal Frequency Division Multiple Access

Acronym or Abbreviation	Full Spelling
PoE	Power over Ethernet
PSK	Pre-shared Key
PVID	Port-base VLAN ID
RTS	Request To Send
SAE	Simultaneous Authentication of Equals
Short GI	Short Guard Interval
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TXOP	Transmission Opportunity
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WMM	Wi-Fi multi-media
WPA	Wi-Fi Protected Access