User Guide

Ceiling AP Series

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

Copyright statement

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

This guide describes how to configure each feature of the following Tenda ceiling APs.

- i23
- i24
- i26
- i27
- i29
- i33
- i36

NOTE

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

In this guide, unless otherwise specified, all screenshots are taken from i36 V1.0.

Conventions

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	Italic	Format: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*

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

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

More information and support

Visit www.tendacn.com and search for the product model to get your questions answered and get the latest documents.

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
V2.0	2026.01.10	Adjusted the document structure and optimized sentence expression.
V1.0 – V1.3	2024.04 – 2025.05	Historical versions.

Contents

1 Getting started with AP

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

If you are using the AP for the first time or have restored it to factory settings, and the AP is not managed by any network device or cloud platform, refer to the following instructions to use the AP web quick setup wizard to quickly access the internet via Wi-Fi.

For more configuration options through the AP web UI, refer to other chapters of this guide.

1.1 Perform quick setup wizard

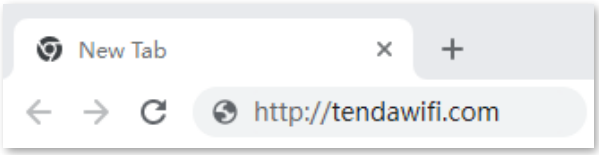
1. Log in to the quick setup page of the AP.

   1) Connect a Wi-Fi-enabled device (such as a smartphone and a laptop) to the AP's Wi-Fi network.

   TIP

   – Ensure that the internet where the AP is deployed is connected.
   – If the AP is not managed by any network device or cloud platform, the AP's Wi-Fi network only has default Wi-Fi names **Tenda_*XXXXXX*** and **Tenda_*XXXXXX*_5G** (***XXXXXX*** is the last six digits of the MAC address on the bottom label of the AP).
   – If **Unsecured Network** prompts on the page, ignore it.

   2) After a successful connection, the Wi-Fi-enabled device will automatically open a browser and be redirected to the **Quick Setup** page. If it does not redirect automatically, start a browser manually and enter **http://tendawifi.com** in the address bar to log in. (Example: laptop)



2. Set the working mode of the AP.

---End

TIP

If the quick setup page does not appear, try the following solutions:

- Ensure that the AP is working properly and the Wi-Fi-enabled device is connected to the correct Wi-Fi network.
- When logging in using your smartphone, ensure that the cellular network (mobile data) of the device is disabled.
- Try to use the IP address to log in to the web UI of the AP.
  - Log in with a new IP address: If the AP obtains an IP address from the DHCP server, you can first check the new IP address from the DHCP server, and then use it to log in. If not, use **192.168.0.254** to log in to the web UI of the AP.
  - Log in with **10.16.16.169**: Set the IP address (10.16.16.*X*, *X* ranges from 1 to 254 and is unused) of the Wi-Fi-enabled devices to the IP address within the same network segment as the AP.
- When logging in using the IP address, if there are at least two APs on the network, it is recommended to connect each AP to the network one by one and change its IP address to ensure that each AP has a unique IP address.
- Clear your browser's cache or use a different browser, and try logging in again.
- Reset the AP and try again.

1.2 Set the working mode of the AP

After logging in to the AP's quick setup page, you can set the working mode and wireless parameters.

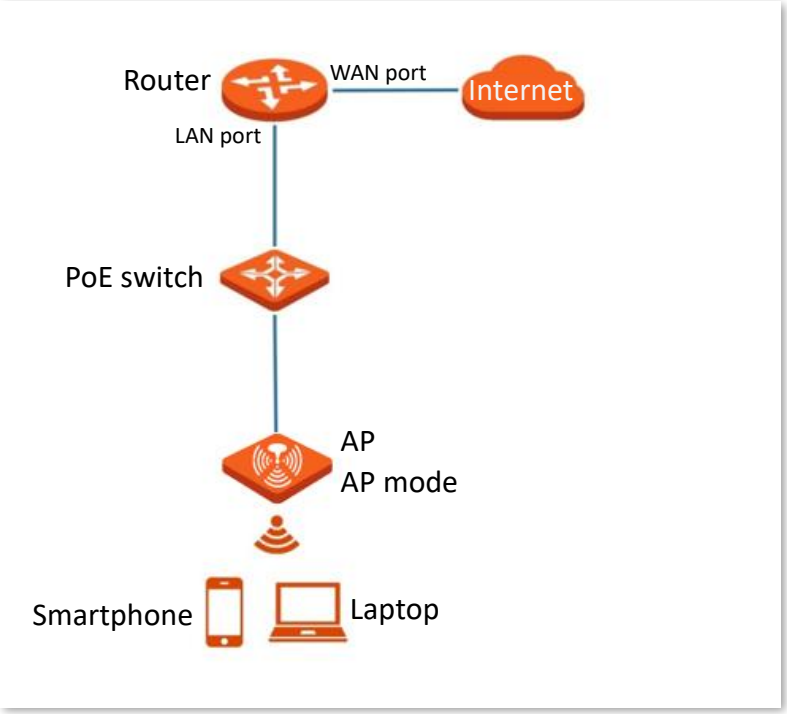
TIP

After logging in to the web UI of the AP:

- You can navigate to **Quick Setup** to modify the AP's working mode.
- If you cannot detect the upstream device's Wi-Fi network when the AP's working mode is set to bridge mode, navigate to **Wireless** > **RF Settings**, ensure that **Wireless Network** for the corresponding frequency band is enabled, and try again.

1.2.1 Configure AP mode

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

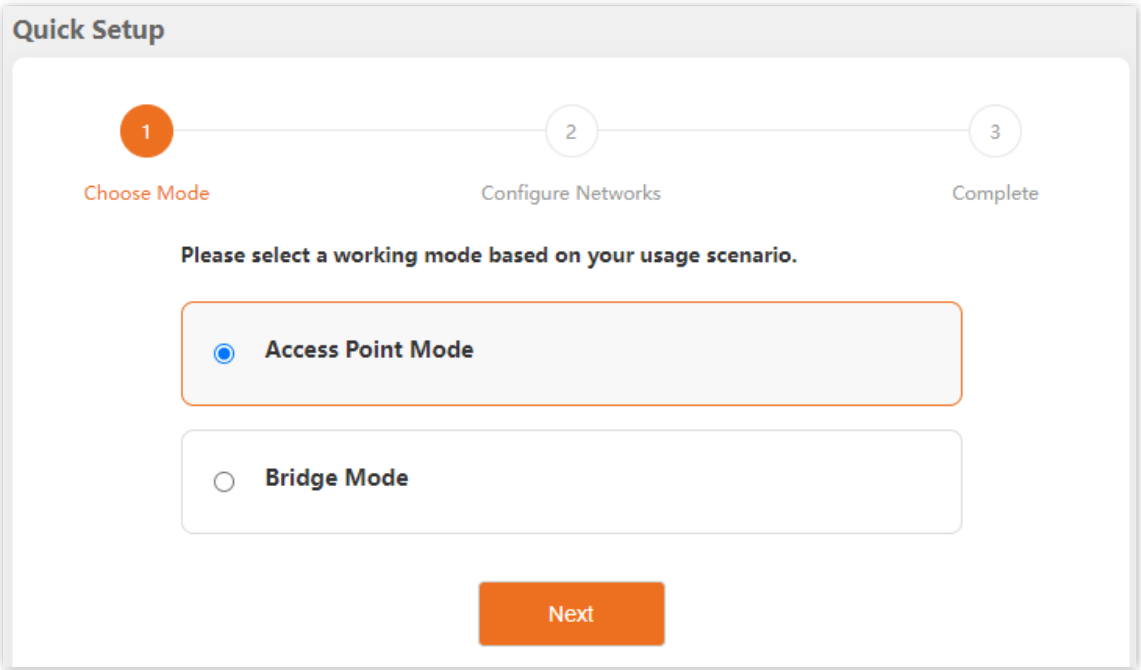


Procedure for configuring AP mode

TIP

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

1. Set the working mode of the AP to **Access Point Mode**, and click **Next**.



2. Enable or disable the **Dual-band same SSID** function as required. The following figure shows an example of enabling the **Dual-band same SSID**.

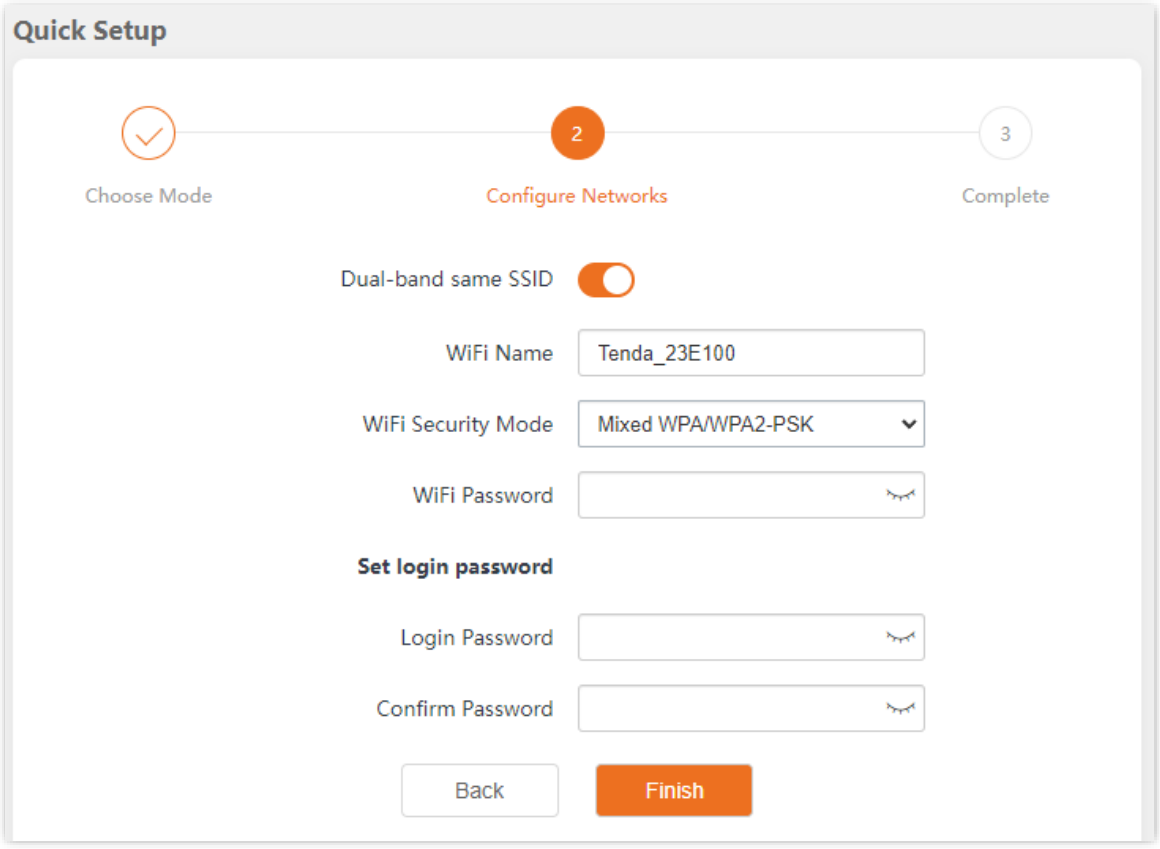
- Enable **Dual-band same SSID**: The Wi-Fi name and password for the 2.4 GHz and 5 GHz networks of the primary Wi-Fi are the same, and only one name is displayed. When you connect to your AP's primary Wi-Fi, you will automatically switch to the best quality Wi-Fi between them.
- Disable **Dual-band same SSID**: The 2.4 GHz and 5 GHz networks for the primary Wi-Fi are displayed separately. You can access the internet through either Wi-Fi network.

3. For the AP's primary Wi-Fi, customize the **WiFi Name**, **WiFi Security Mode** and specific parameters as required.
4. Set the login password for the AP.

NOTE

- Set the Wi-Fi name and password for Wi-Fi access, and the login password for web UI.
- For initial setup or after a reset, set new login and Wi-Fi passwords for privacy and security (The longer the password, the stronger the protection). The character limit and composition rules for passwords are subject to software user interface prompts.

5. Click **Finish**.

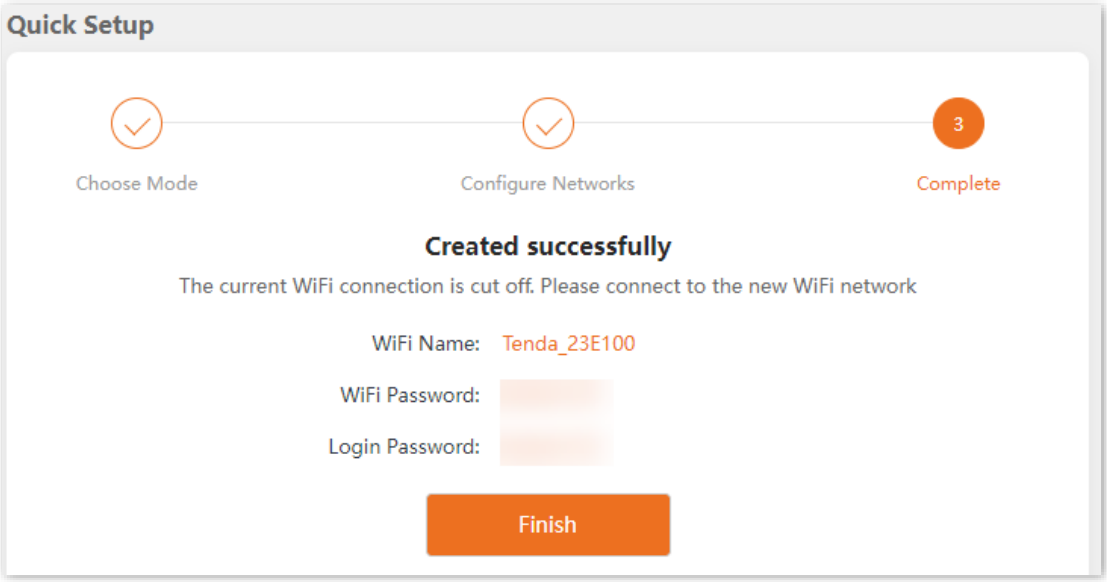


---End

After the configuration is completed, you can use Wi-Fi-enabled devices (such as smartphones) to reconnect to the AP Wi-Fi you configured to access the internet.

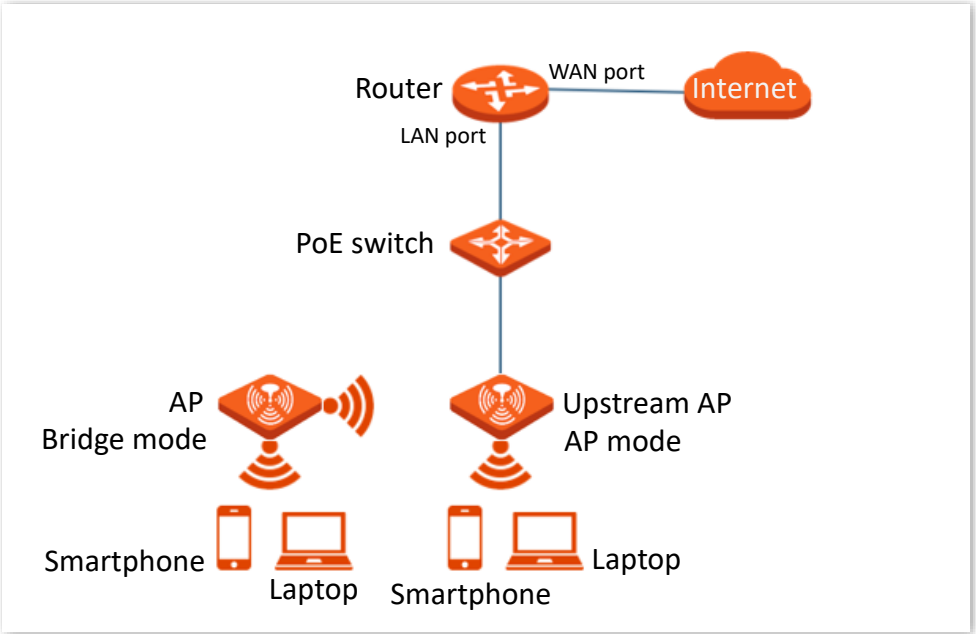
TIP

Log in to the web UI of the AP, and navigate to **Wireless** > **SSID** to enter the page, you can view the Wi-Fi name (SSID) and Wi-Fi password (key) of the AP.



1.2.2 Configure bridge mode

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

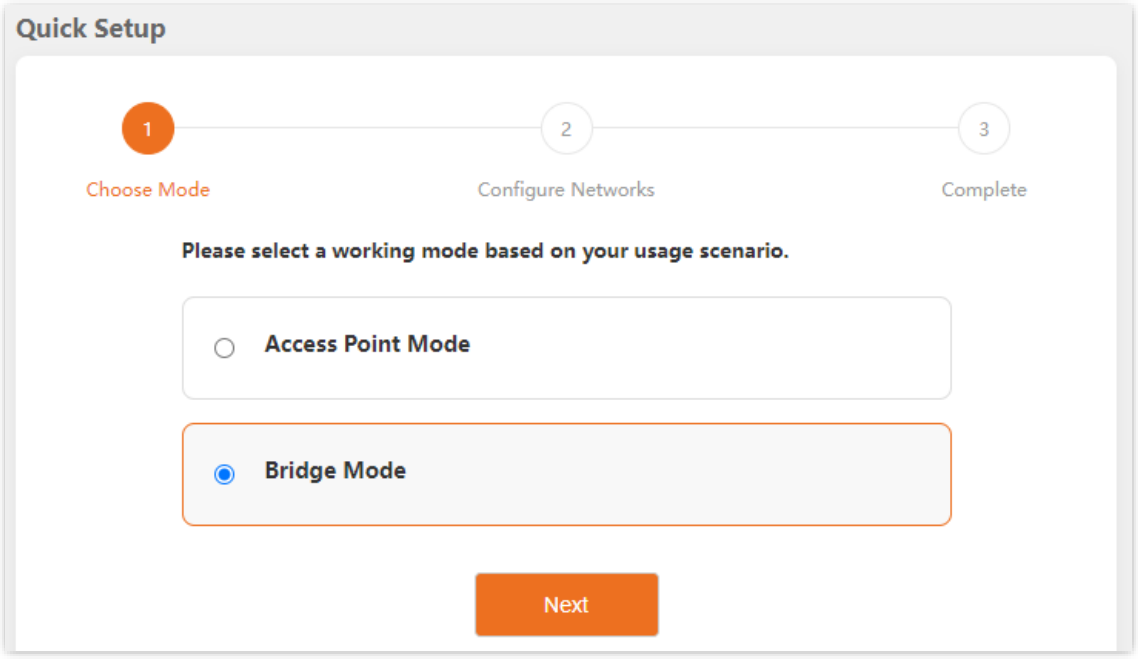


Procedure for configuring bridge mode

TIP

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

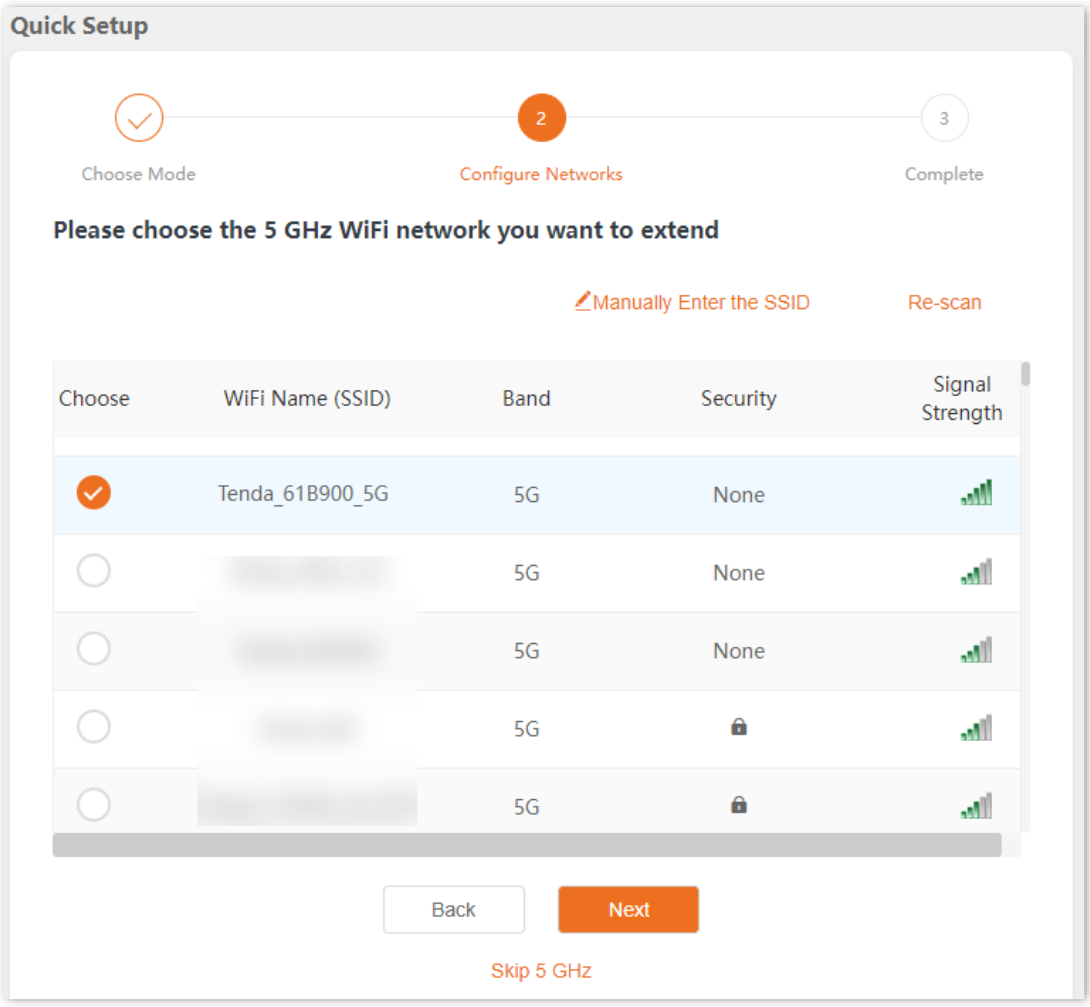
1. Set the working mode of the AP to **Bridge Mode**, and click **Next**.



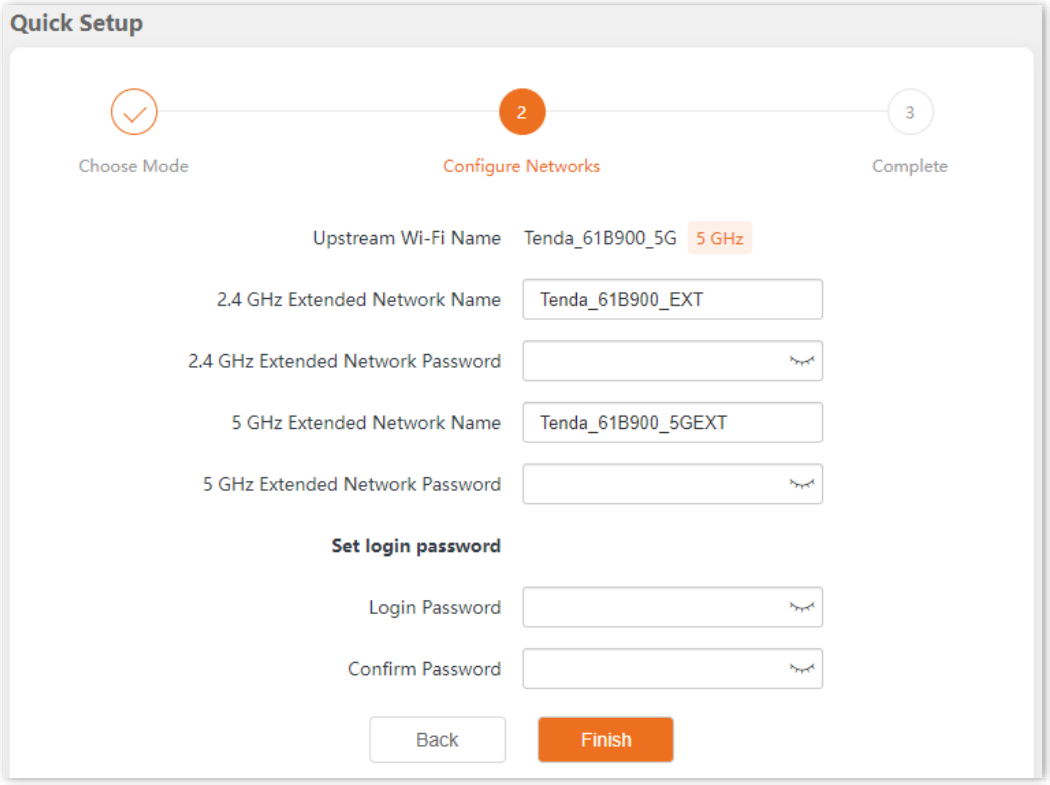
2. Select the upstream device's Wi-Fi to extend the network. If it has a password, enter its password below **Security**. Then click **Next**. The following figure is for reference only.

TIP

If you need to extend the 2.4 GHz Wi-Fi or if the upstream device's Wi-Fi only supports the 2.4 GHz frequency band, click **Skip 5 GHz** at the bottom of the page to extend the 2.4 GHz Wi-Fi.



3. Confirm the name and password of the extended Wi-Fi and modify them as required.
4. Set the login password for the AP.
5. Click **Finish**.

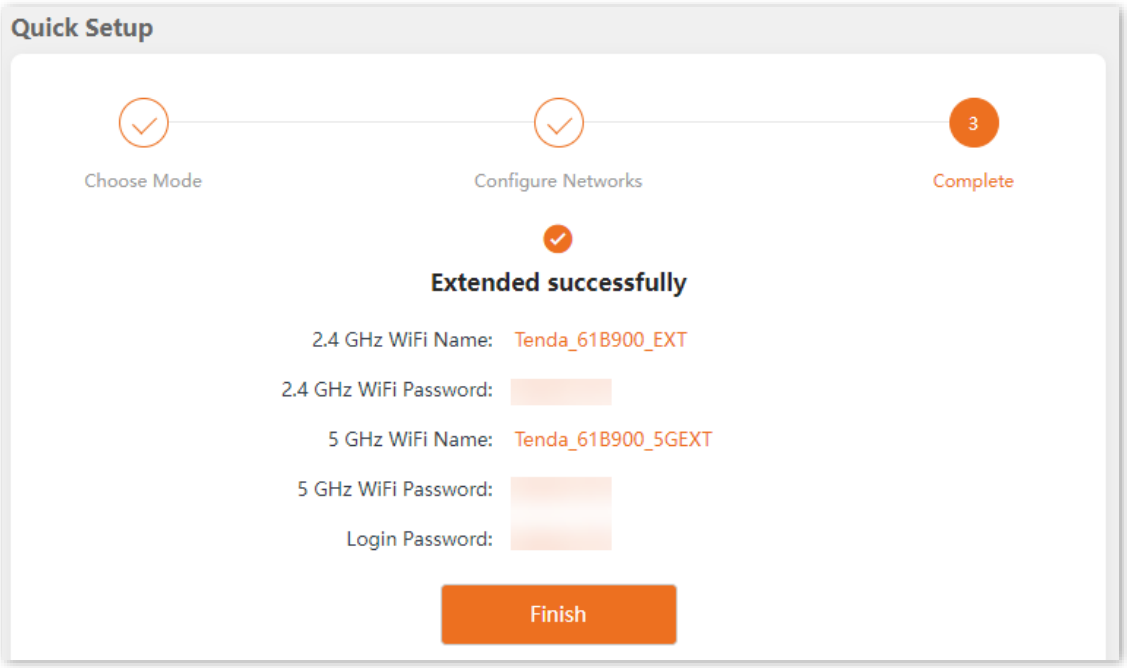


---End

After the configuration is completed, you can use Wi-Fi-enabled devices (such as smartphones) to reconnect to the extended Wi-Fi you set up to access the internet.

TIP

Log in to the web UI of the AP, and navigate to **Wireless** > **SSID** to enter the page, you can view the Wi-Fi name (SSID) and Wi-Fi password (key) of the AP.



2 Login and logout

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

2.1 Log in to the web UI

If you are using the AP for the first time or have restored it to factory settings, and the AP is not managed by any network device or cloud platform, refer to the Getting started with AP section to log in to the web UI of the AP.

For other situations, refer to the following instructions to log in.

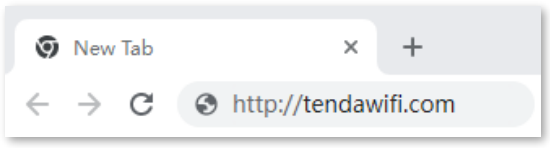
Procedure for logging in to the web UI of the AP

1. Connect a Wi-Fi-enabled device (such as a smartphone and a laptop) to the AP's Wi-Fi network.

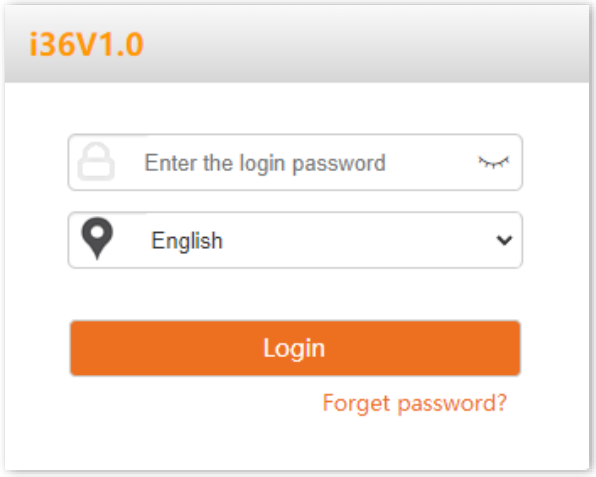
   TIP

   - Ensure that the internet where the AP is deployed is connected.
   - If you have configured the AP's Wi-Fi network through the AP web UI, the Wi-Fi name (SSID) and password are the ones you set.
   - If the AP is managed by a controller (including a router with AP management functions) or a cloud platform, log in to the controller's web UI or the cloud platform to check the AP's Wi-Fi name and password.

2. Start a browser and visit **http://tendawifi.com** in the address bar to log in to the web UI of the AP. (Example: laptop)



3. Enter the login password, and click **Login**.



---End

TIP

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

- Ensure that the AP is working properly and the Wi-Fi-enabled device is connected to the correct Wi-Fi network.
- When logging in using your smartphone, ensure that the cellular network (mobile data) of the device is disabled.
- Try to use the IP address to log in to the web UI of the AP.
  - Log in with a new IP address: If the AP obtains an IP address from the DHCP server, you can first check the new IP address from the DHCP server, and then use it to log in. If not, use **192.168.0.254** to log in to the web UI of the AP.
  - Log in with **10.16.16.169**: Set the IP address (10.16.16.*X*, *X* ranges from 1 to 254 and is unused) of the Wi-Fi-enabled devices to the IP address within the same network segment as the AP.
- When logging in using the IP address, if there are at least two APs on the network, it is recommended to connect each AP to the network one by one and change its IP address to ensure that each AP has a unique IP address.
- If the QVLAN function is enabled, ensure that the VLAN ID of the connected Wi-Fi matches the AP's management VLAN ID.
- Clear your browser's cache or use a different browser, and try logging in again.
- Reset the AP and try again.

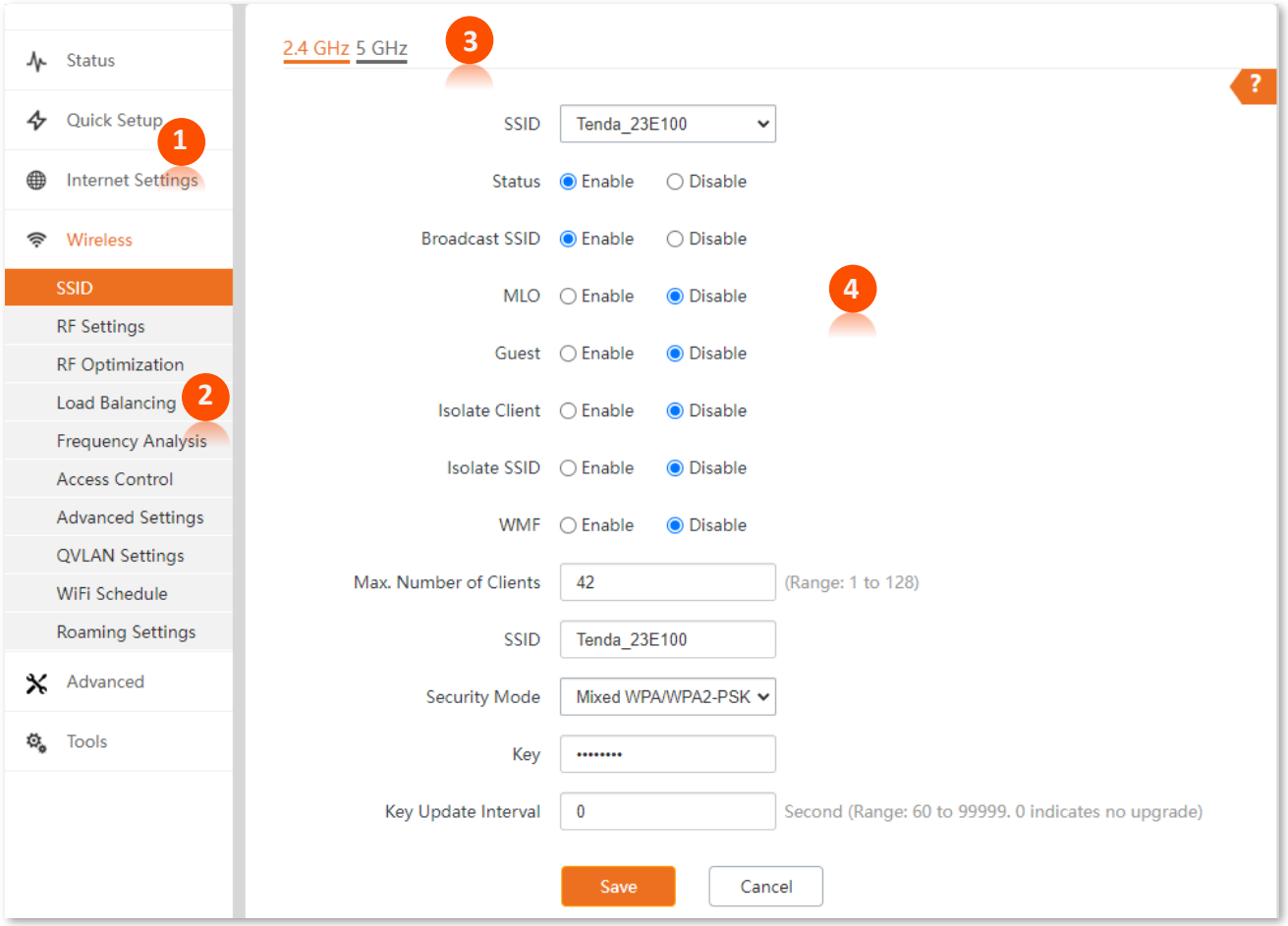
After logging in to the web UI of the AP, you can now configure the AP.

2.2 Log out of the web UI

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.

2.3 View the layout of the web UI

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



TIP

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

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

2.4 Use common buttons

Buttons commonly used on the web UI are illustrated below.

Common button	Description
Refresh	Used to refresh the current page.
Save	Used to save configurations on the current page and make the configurations take effect.
Cancel	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 Manage internet settings

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

3.1 Configure LAN settings

By default, the AP's internet IP address (LAN IP address) is 192.168.0.254. If there is a DHCP server in the LAN where the AP is located, the AP automatically obtains an internet IP address from the DHCP server to connect to the internet.

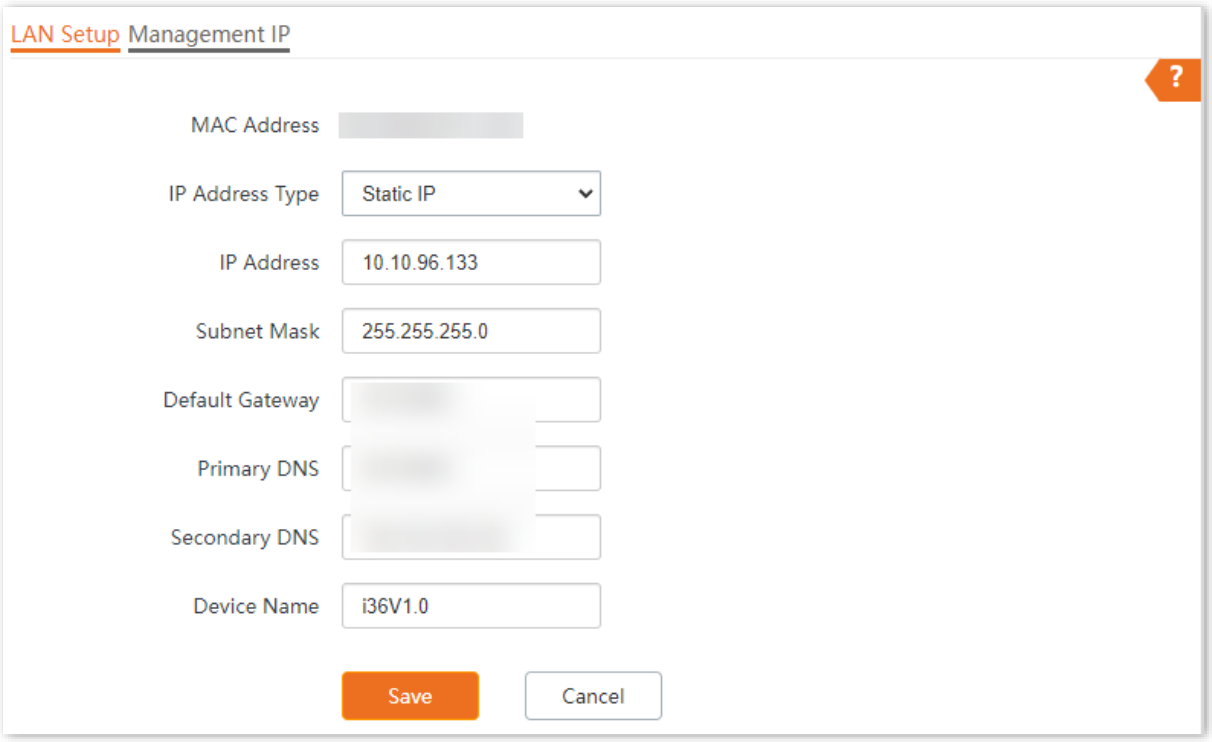
You can view the MAC address of the AP's LAN port and configure the IP address, device name, and other related parameters.

Procedure for configuring LAN settings

1. Log in to the web UI of the AP.
2. Navigate to **Internet Settings** > **LAN Setup** > **LAN Setup**.
3. Set the **IP Address Type** to specify how the AP obtains its internet IP address.

   TIP

   If **Static IP** is selected, manually specify the AP's IP address, subnet mask, default gateway, and DNS server.
4. Click **Save**. The following figure is for reference only.



---End

TIP

If you have changed the AP's internet IP address, you need to use the new IP address to log in to the web UI of the AP.

Parameter description

Parameter	Description
MAC Address	Specifies the MAC address of the LAN port of the AP.
IP Address Type	Specifies the IP address obtaining mode of the AP. - **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. TIP When **DHCP (Dynamic IP Address)** is selected as the IP address type, the AP's IP address may change. Before logging in to the web UI of the AP, check the client list on the DHCP server in the network to find the IP address assigned to the AP, and then use that IP address to log in.

Parameter	Description
IP Address	Specifies the internet IP address (LAN IP address) of the AP. The web UI of the AP is accessible at this IP address. TIP - Before using this IP address to log in to the web UI of the AP, ensure that the IP address of the LAN user is in the same subnet as the AP's IP address. - If the QVLAN function is enabled, only users connected to the AP's management VLAN member ports can use this IP address to log in to the web UI of the AP.
Subnet Mask	Specifies the subnet mask corresponding to the AP's LAN port IP address. It is used to define the address range of the device's network segment.
Default Gateway	Specifies the default gateway corresponding to the AP's LAN port IP address. It is generally set to the LAN port IP address of the egress router.
Primary DNS	Specifies the primary DNS server of the AP. If the egress router has a DNS proxy function, you can enter the LAN port IP address of the egress router here. Otherwise, enter the correct IP address of the DNS server.
Secondary DNS	Specifies the IP address of the secondary DNS server of the AP. This parameter is optional. If there are two DNS server IP addresses, you can enter the secondary IP address in this field.
Device Name	Specifies the name of the AP. You are recommended to change the name of the AP to indicate the location of the AP (such as Hall), so that you can easily identify the AP when managing many APs.
AC Management IP	The AP that is configured with this option will be used as a lighthouse AP. The AP will discover the AC based on the AC address filled in. At the same time, it will guide other APs in the local area network to discover AC. If the current AP is offline, other APs that have been managed by AC in the same local area network will replace it and guide other APs in the LAN to add AC. There is only one lighthouse AP in a local area network. TIP This function is available on some APs. The actual product prevails.

Parameter	Description
Optimize Ethernet for	Specifies the Ethernet mode of the PoE power-supply port of this AP. - **Fast Speed (Auto Negotiation)**: This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended. - **Longer Distance (10 Mbps Full Duplex)**: This mode features a long transmission distance but relatively low transmission rate (usually 10 Mbps). 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. TIP This function is available on some APs. The actual product prevails.

3.2 Configure management IP

Users within the LAN can access the AP's management IP address to log in to its web UI. The default management IP address of the AP is 10.16.16.169.

TIP

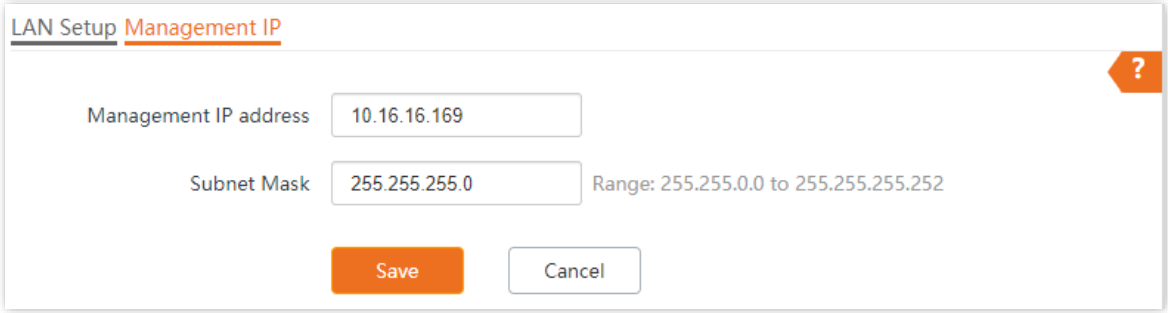
Before using this IP address to log in to the web UI of the AP:

– Ensure that the IP address of the LAN user is in the same subnet as the AP's IP address.

– If the QVLAN function is enabled, ensure that the VLAN ID of the user-connected AP Wi-Fi (or port) matches the AP's management VLAN ID.

Procedure for configuring management IP

1. Log in to the web UI of the AP.
2. Navigate to **Internet Settings** > **LAN Setup** > **Management IP**.
3. Modify the **Management IP address** and **Subnet Mask** as required.
4. Click **Save**.



---End

After the configuration is completed, you need to use the new management IP address to log in to the web UI of the AP.

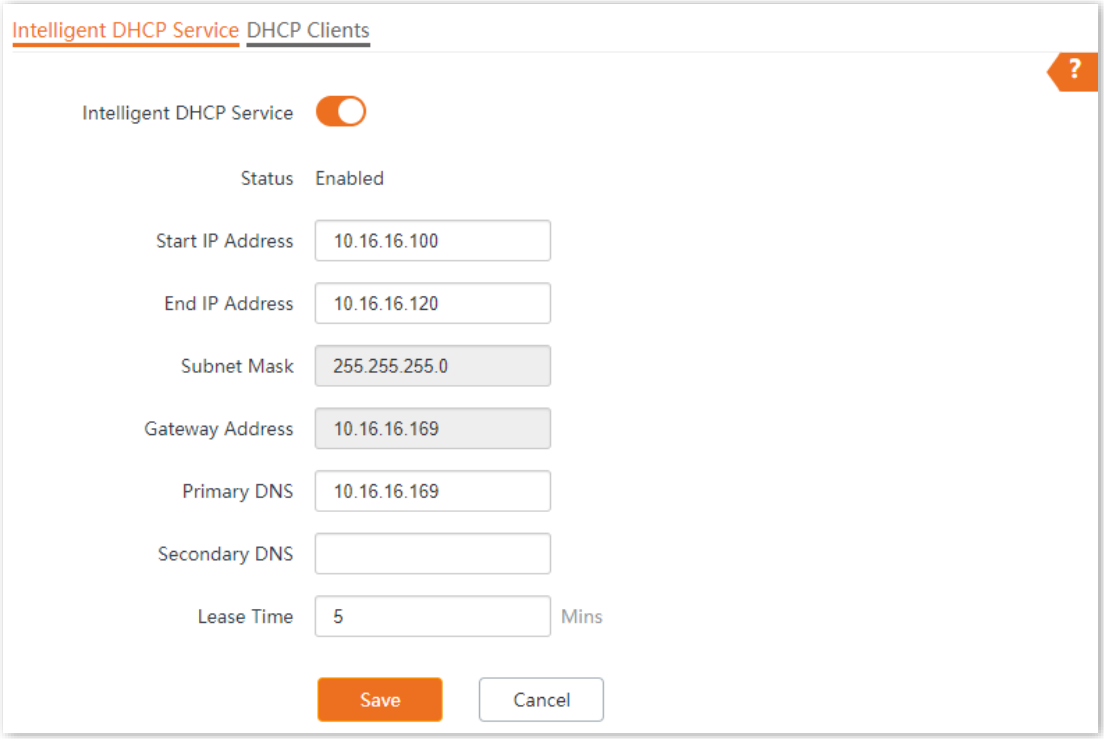
3.3 Use the AP as a DHCP server

The DHCP service is used when there is no other DHCP server in the LAN where the AP is located. In this case, the AP acts as a DHCP server and automatically assigns IP address to devices in the LAN.

The intelligent DHCP service function is enabled by default. When there are other DHCP servers in the LAN where the AP is located, or when the AP is managed by an AC (Tenda wireless controller or a Tenda router that supports AP management), this function will be automatically disabled. If there are no other DHCP servers in the LAN and the AP is not managed by an AC, the AP must be restored to its factory settings to re-enable this function.

3.3.1 Configure DHCP server settings

1. Log in to the web UI of the AP.
2. Navigate to **Internet Settings** > **Intelligent DHCP Service** > **Intelligent DHCP Service**.
3. Enable the **Intelligent DHCP Service** function.
4. Modify the AP's DHCP server parameters as required.
5. Click **Save**.



---End

Parameter description

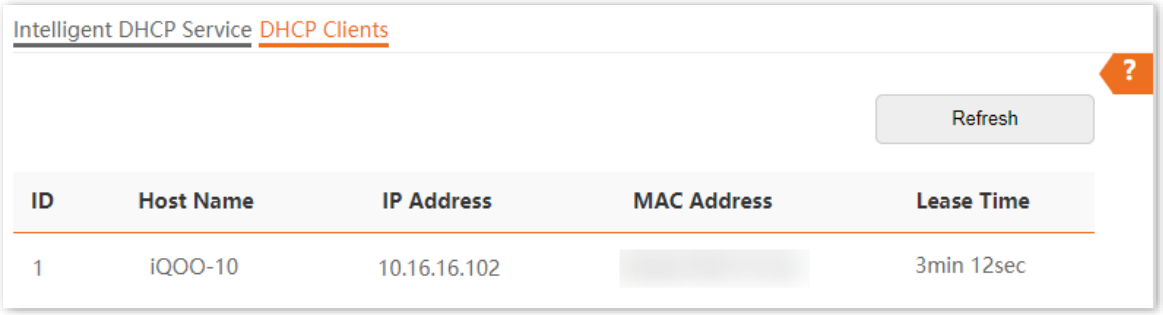
Parameter	Description
Intelligent DHCP Service	Specifies whether to enable the intelligent DHCP service function of the AP.
Status	Specifies the status of the intelligent DHCP service function of the AP.
Start IP Address	Specify the DHCP address pool of the AP refers to the range of IP addresses that can be assigned to clients by the AP's intelligent DHCP server. TIP After changing the AP's management IP address, if the new management IP address is not in the same subnet as the original IP address, the system will automatically adjust the AP's DHCP address pool to match the subnet of the new management IP address.
End IP Address	
Subnet Mask	Specifies the subnet mask assigned by the AP's DHCP server to clients. By default, it is the subnet mask corresponding to the AP's management IP address.
Gateway Address	Specifies the gateway IP address assigned by the AP's DHCP server to clients. By default, it is the management IP address of the AP.
Primary DNS	Specifies the IP address of the primary DNS server assigned by the AP's DHCP server to clients.
Secondary DNS	Specifies the IP address of the secondary DNS server assigned by the AP's DHCP server to clients. This parameter is optional, which indicates you can leave it blank if the DHCP server does not assign this parameter.
Lease Time	Specifies the validity period of an IP address assigned by the AP's DHCP server to clients. When the lease time expires: - If a LAN client is still connected to the AP, the LAN client will renew the lease and continue to keep the IP address. - If a LAN client is no longer connected to the AP, the AP will release its IP address. If another LAN client requests an IP address, the AP can assign the released IP address to the new client.

3.3.2 View DHCP clients

When the AP is acting as a DHCP server, you can view information such as the host name and IP address of devices that obtained an IP address from the AP.

Procedure for viewing DHCP clients

1. Log in to the web UI of the AP.
2. Navigate to **Internet Settings** > **Intelligent DHCP Service** > **DHCP Clients**.
3. (Optional) Click **Refresh** to view the latest DHCP client list.


Intelligent DHCP Service
DHCP Clients
Refresh
ID
Host Name
IP Address
MAC Address
Lease Time
1
iQOO-10
10.16.16.102
3min 12sec

---End

4 Manage wireless settings

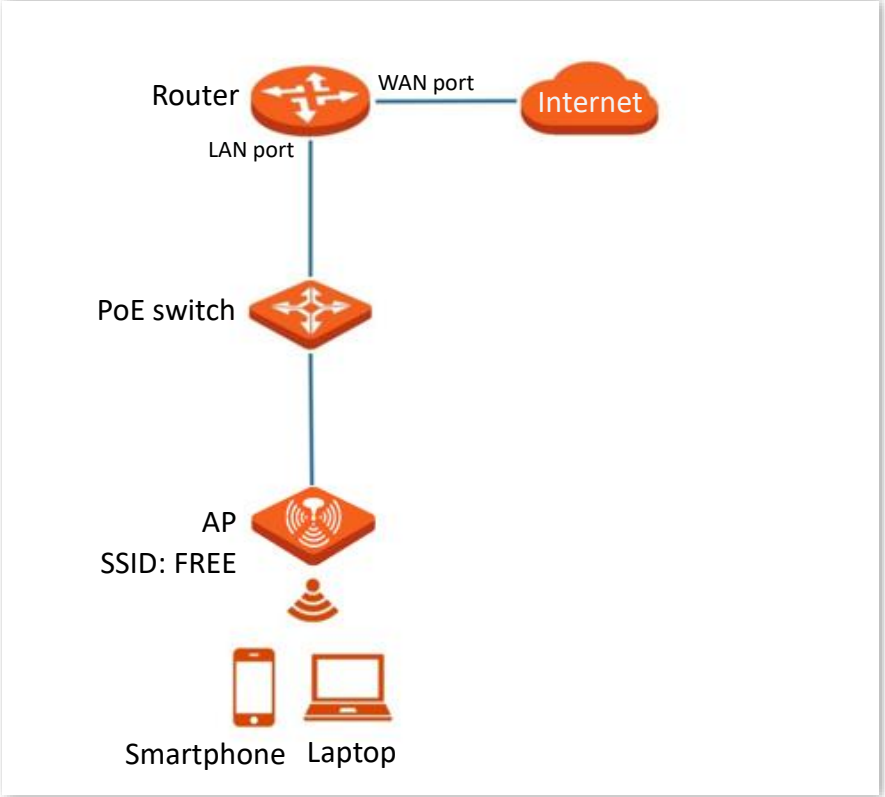
Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

4.1 Configure SSID settings

4.1.1 Example of setting up an open Wi-Fi network

Networking requirements

In a hotel lounge, guests can connect to the Wi-Fi network without a password and access the internet through the Wi-Fi network.

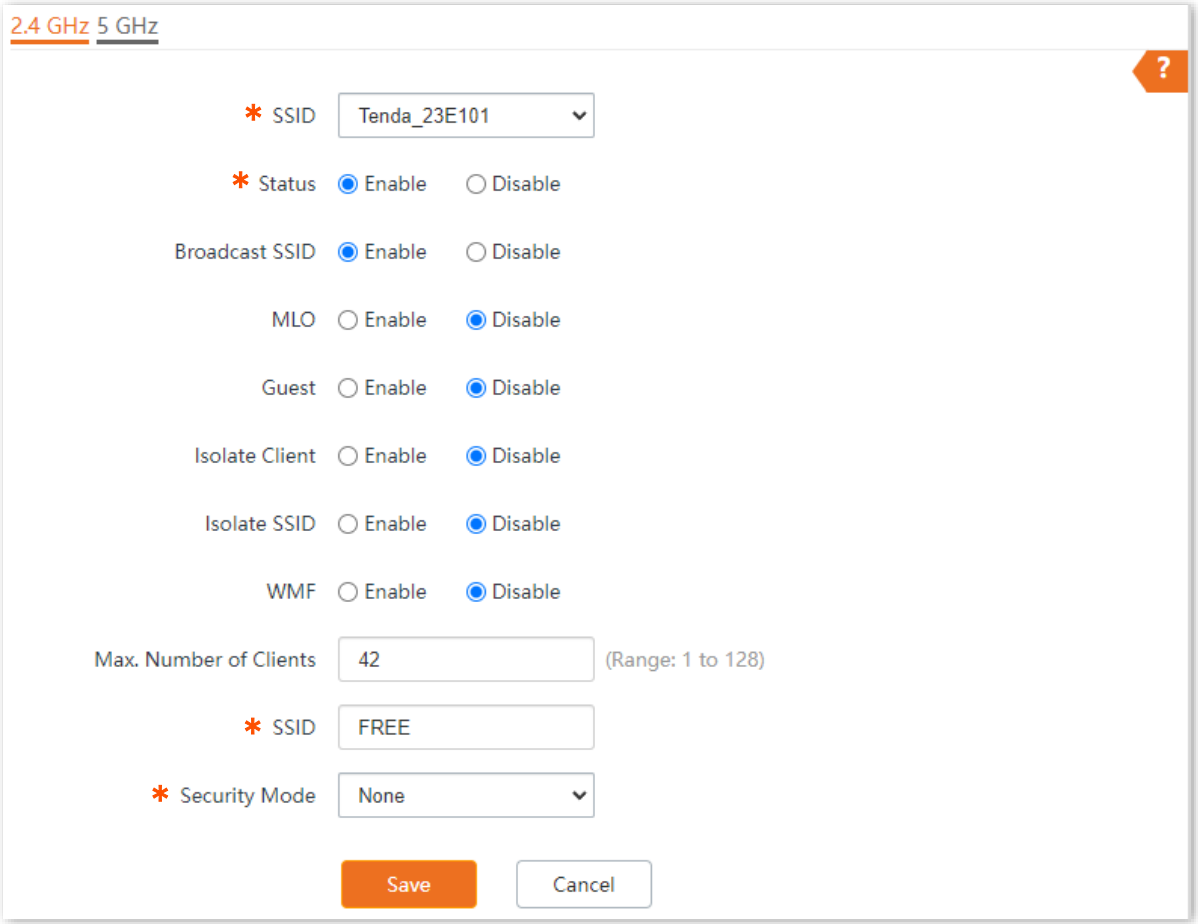


Procedure for setting up an open Wi-Fi network

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

1. Log in to the web UI of the AP.

2. Navigate to **Wireless** > **SSID**.
3. Select the second SSID from the **SSID** drop-down list box.
4. Set **Status** to **Enable**.
5. Set **SSID** to **FREE**.
6. Set **Security Mode** to **None**.
7. Click **Save**.



---End

Verification

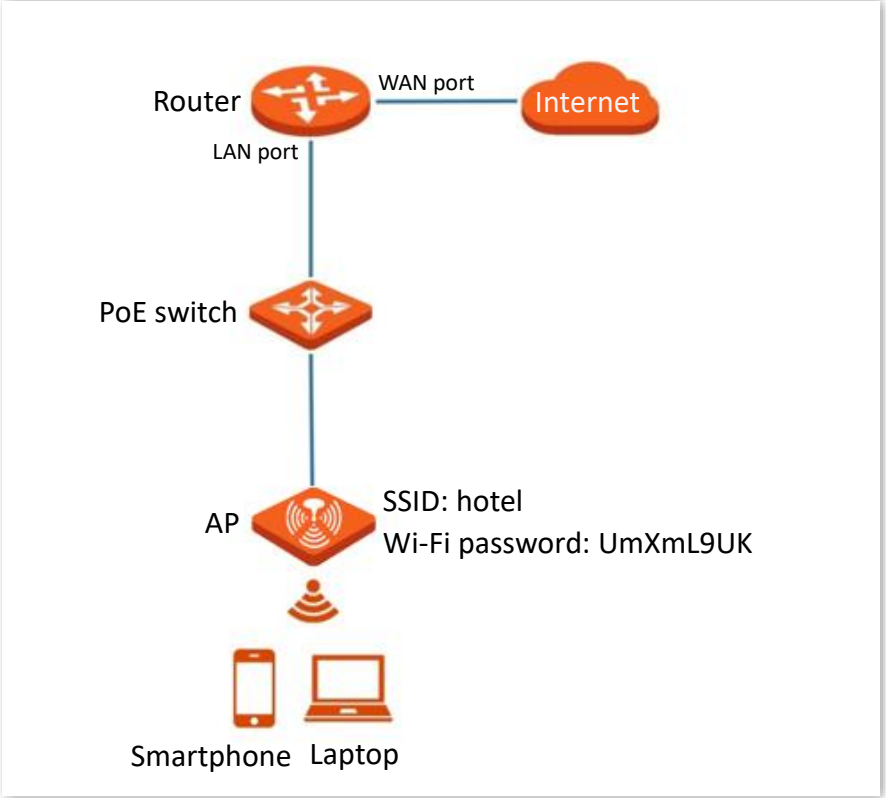
Verify that Wi-Fi-enabled devices can connect to the **FREE** Wi-Fi network without a password.

4.1.2 Example of setting up a Wi-Fi network encrypted with PSK

Networking requirements

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

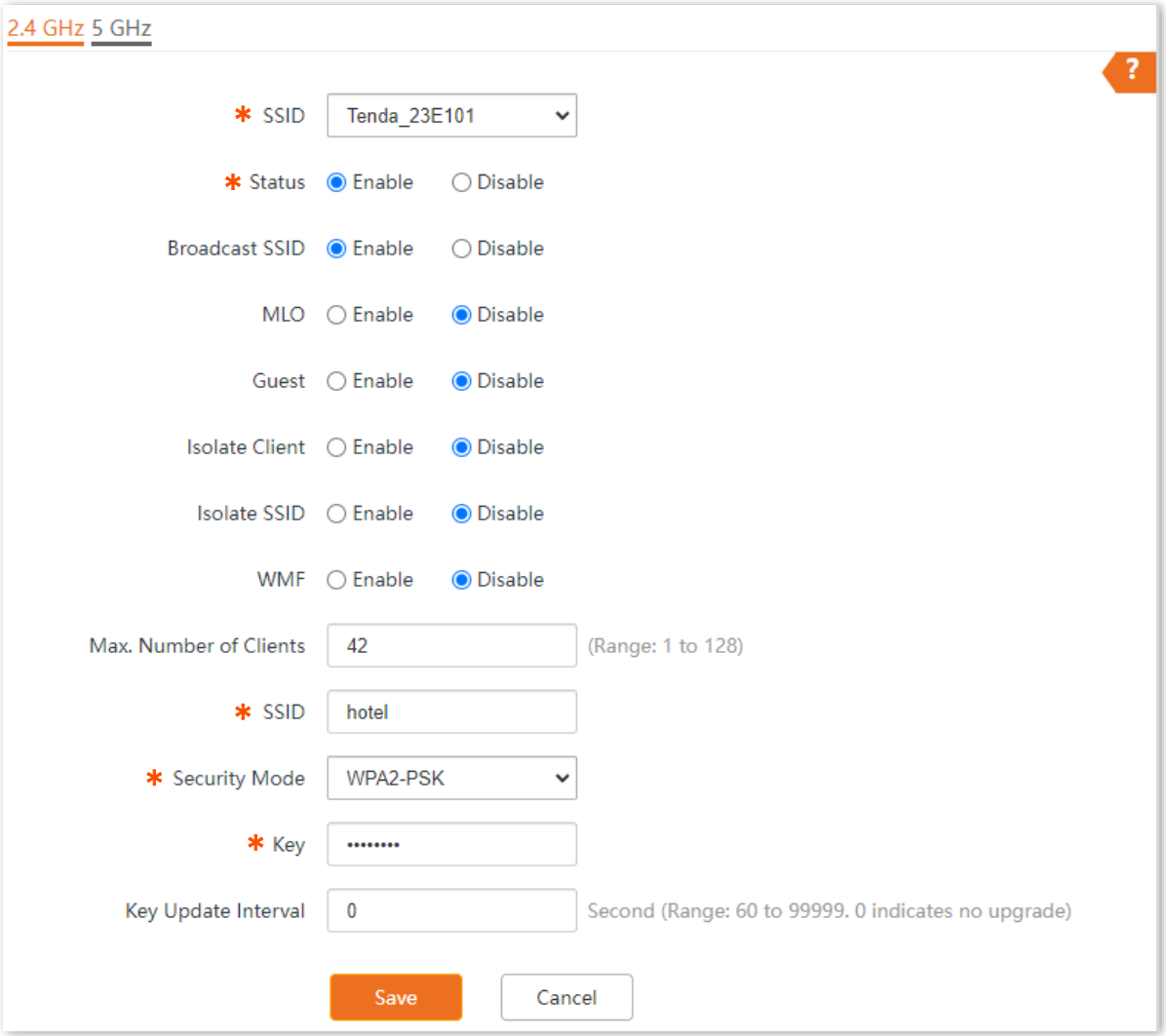
Assume that the SSID is **hotel** and the Wi-Fi password is **UmXmL9UK**. See the following topology.



Procedure for setting up a Wi-Fi network encrypted with PSK

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

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



---End

Verification

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

4.1.3 Example of setting up a Wi-Fi network encrypted with WPA or WPA2

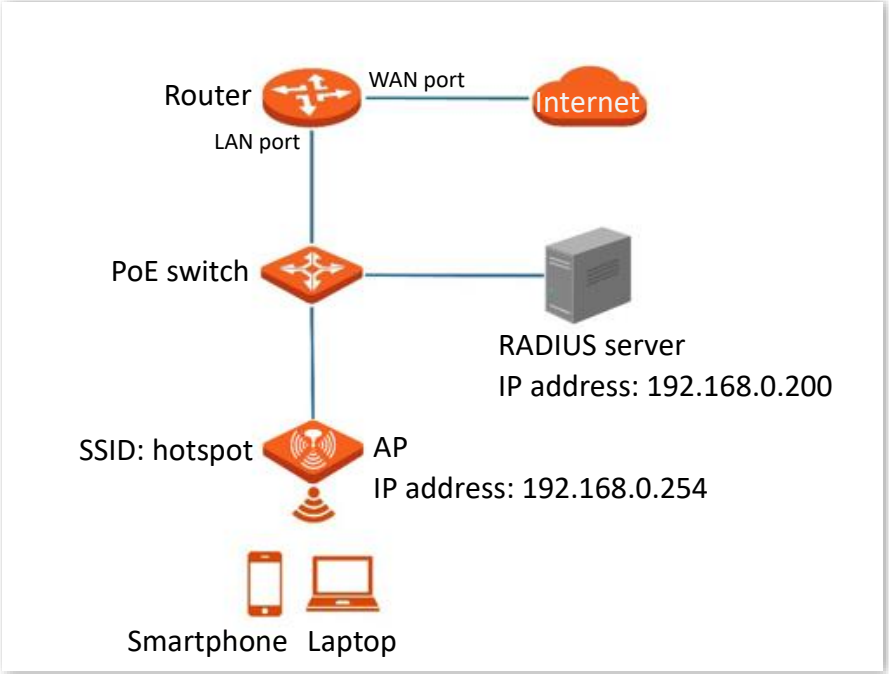
Networking requirements

A highly secure Wi-Fi network is required and a RADIUS server is available. In this case, WPA or WPA2 mode is recommended. See the following topology.

Assume that:

- SSID: **hotspot**
- IP address of the RADIUS server: **192.168.0.200**

- RADIUS port: **1812**
- RADIUS key: **UmXmL9UK**

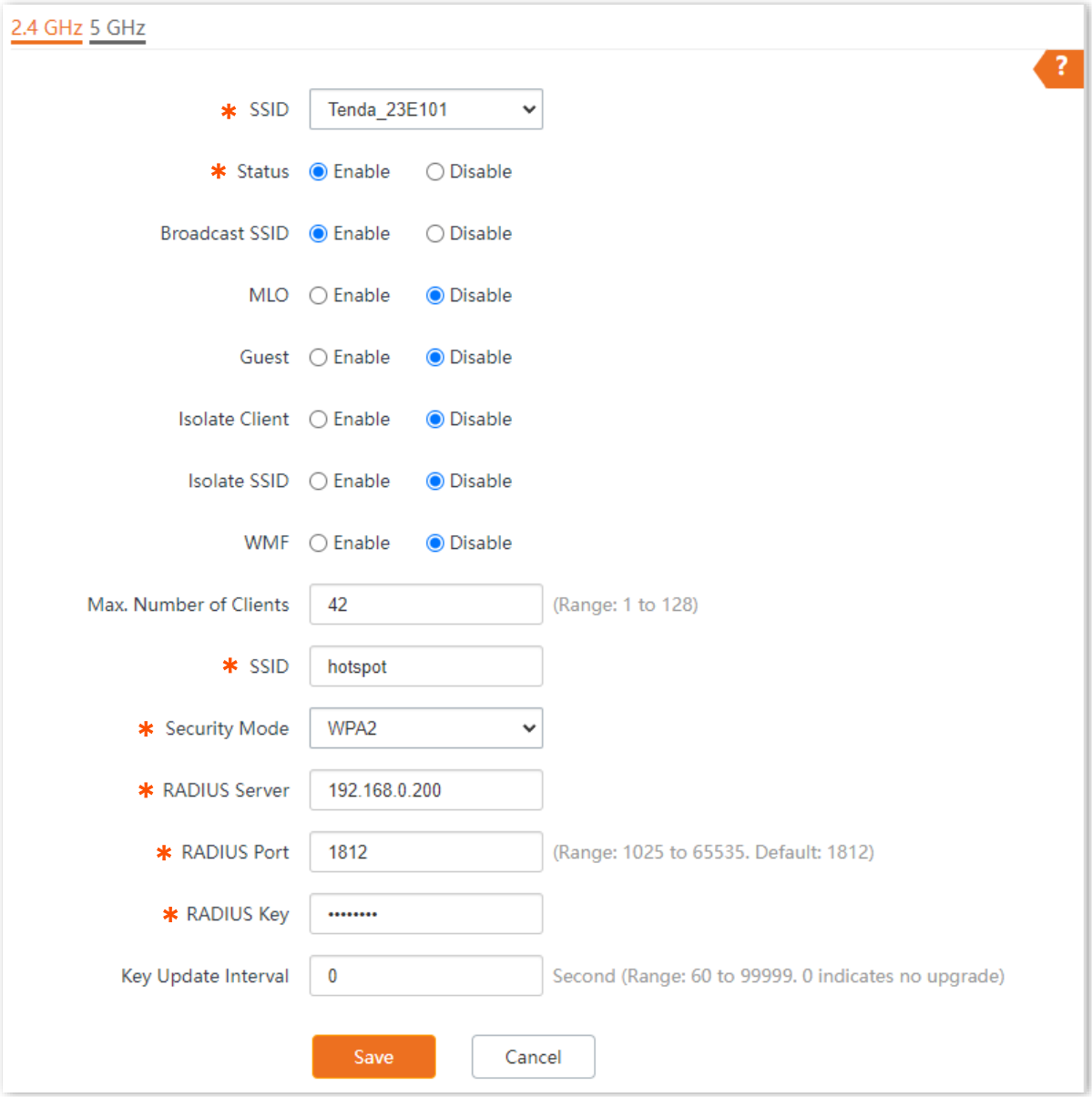


Procedure for setting up a Wi-Fi network encrypted with WPA or WPA2

I. Configure the AP

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

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **SSID**.
3. Select the second SSID from the **SSID** drop-down list box.
4. Set **Status** to **Enable**.
5. Set **SSID** to **hotspot**.
6. Set **Security Mode**, which is **WPA2** in this example.
7. Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Key** to **192.168.0.200**, **1812**, and **UmXmL9UK** respectively.
8. Click **Save**.



II. Configure the RADIUS server

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

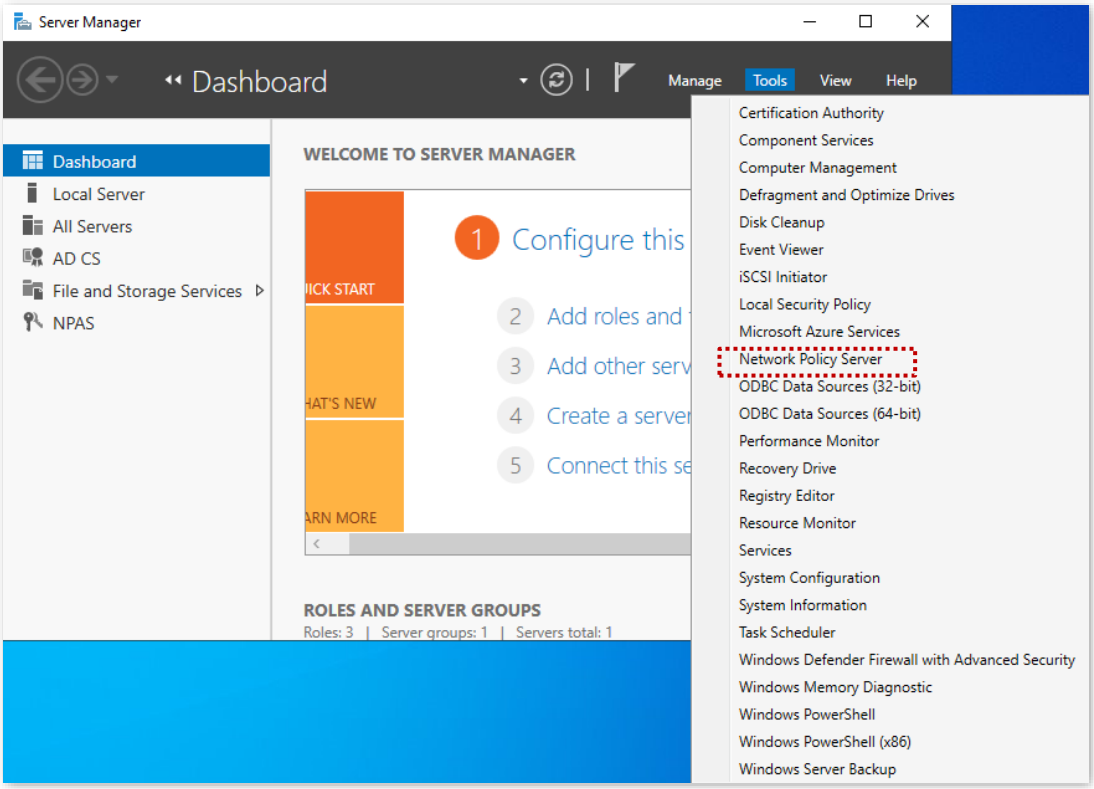
1. Install **Active Directory Certificate Services** and **Network Policy and Access Services**, and deploy the certificate.

   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**.

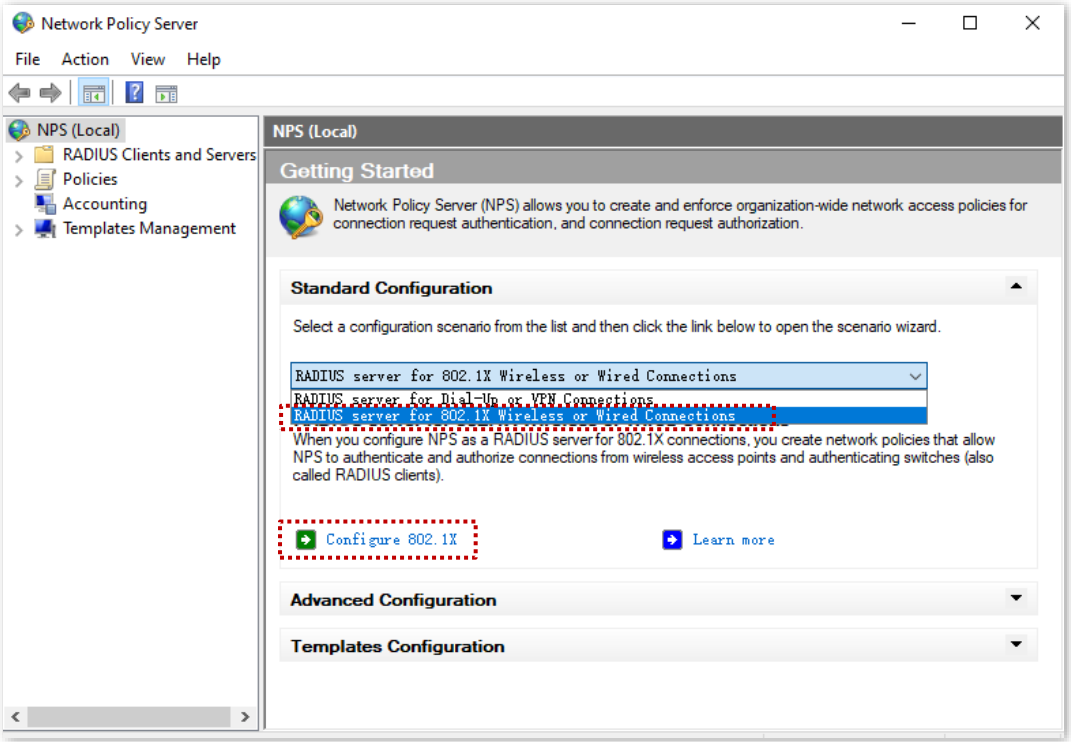
   After the service installation is completed, click in the upper right corner and follow the prompts to deploy the certificate.

2. Configure 802.1X.

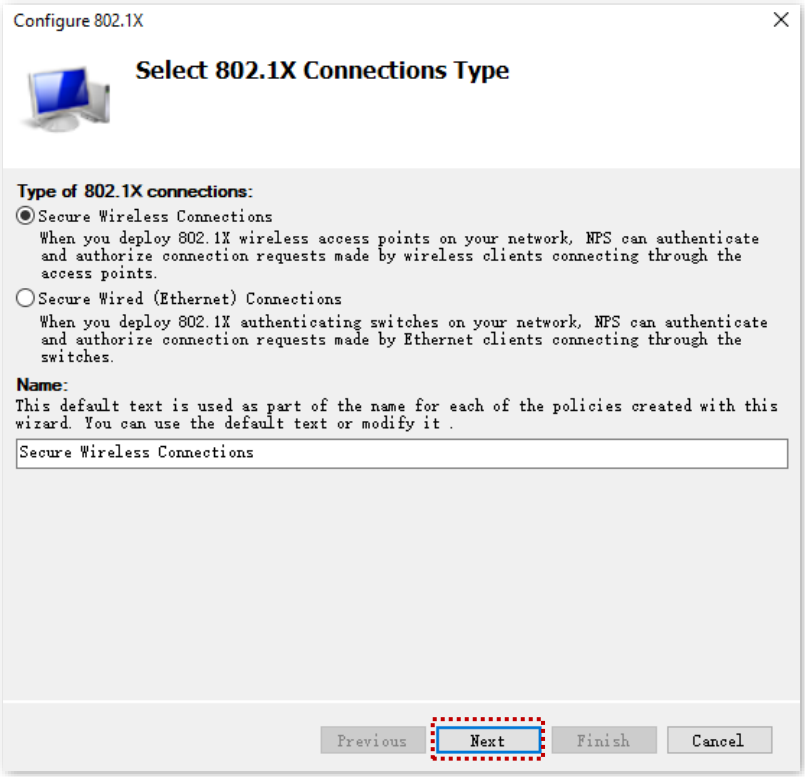
1) Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, and click **Network Policy Server**.



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

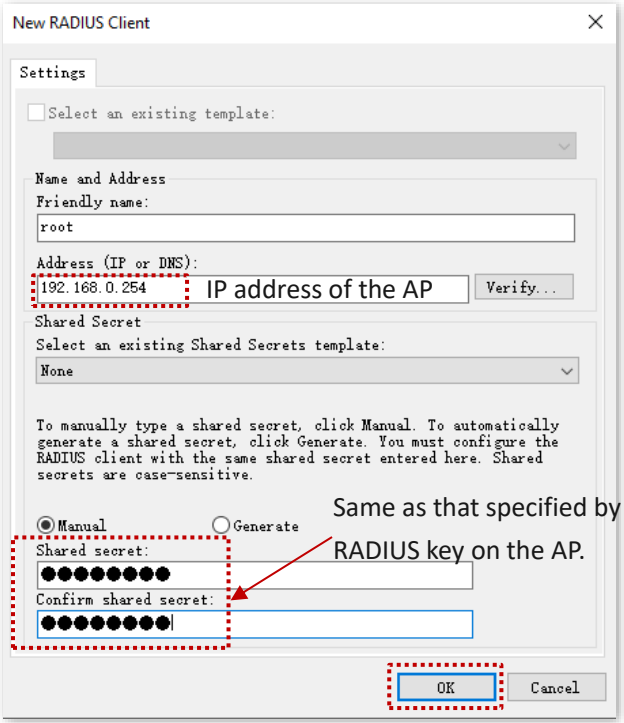


3) Select **Secure Wireless Connections** for **Type of 802.1X connections**. Modify the name as required, which is **Secure Wireless Connections** in this example, and click **Next**.

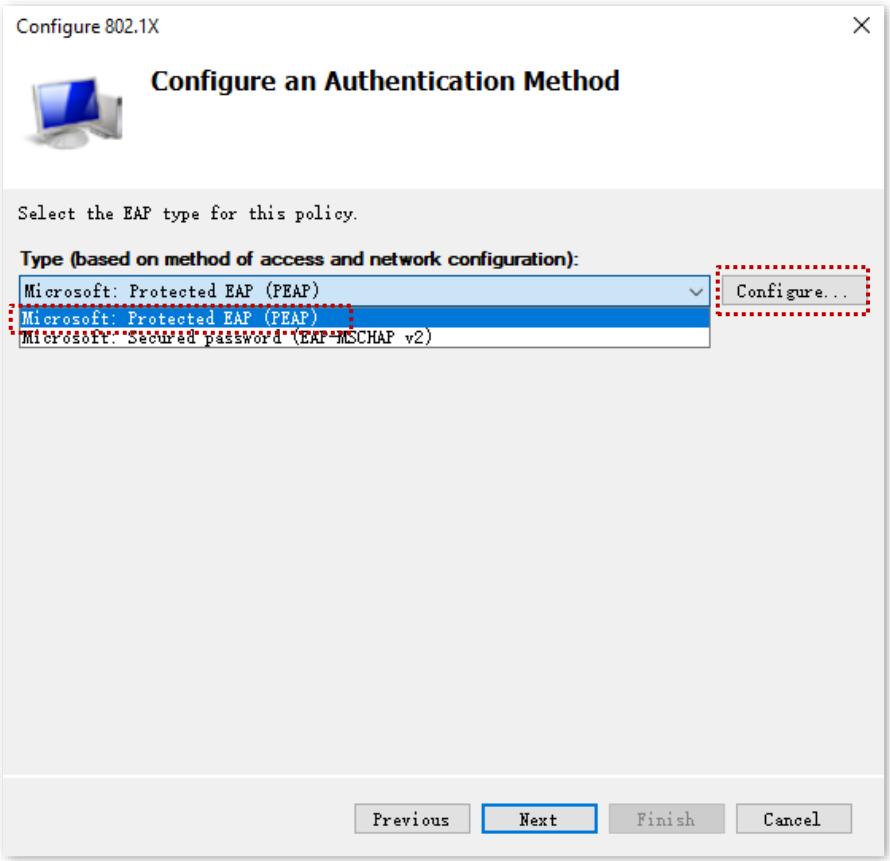


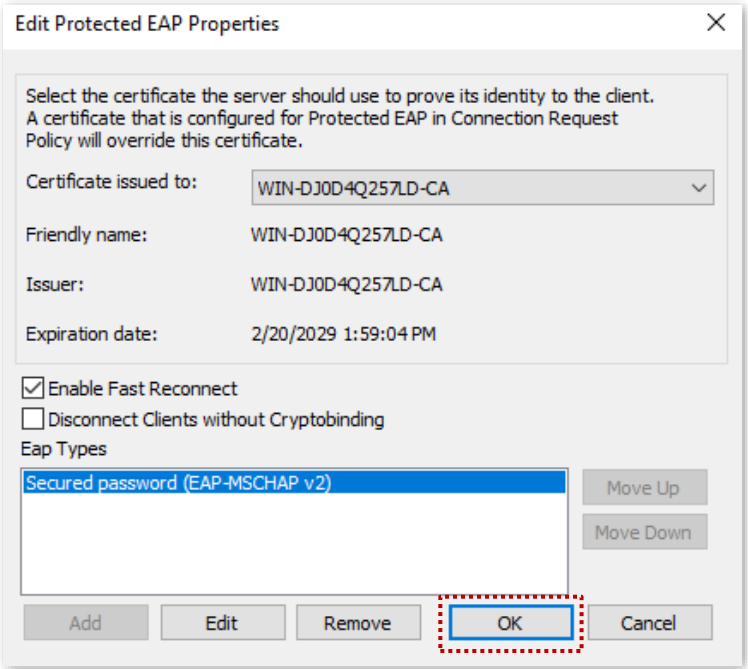
4) On the **Specify 802.1X Switches** page, click **Add**.

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**.

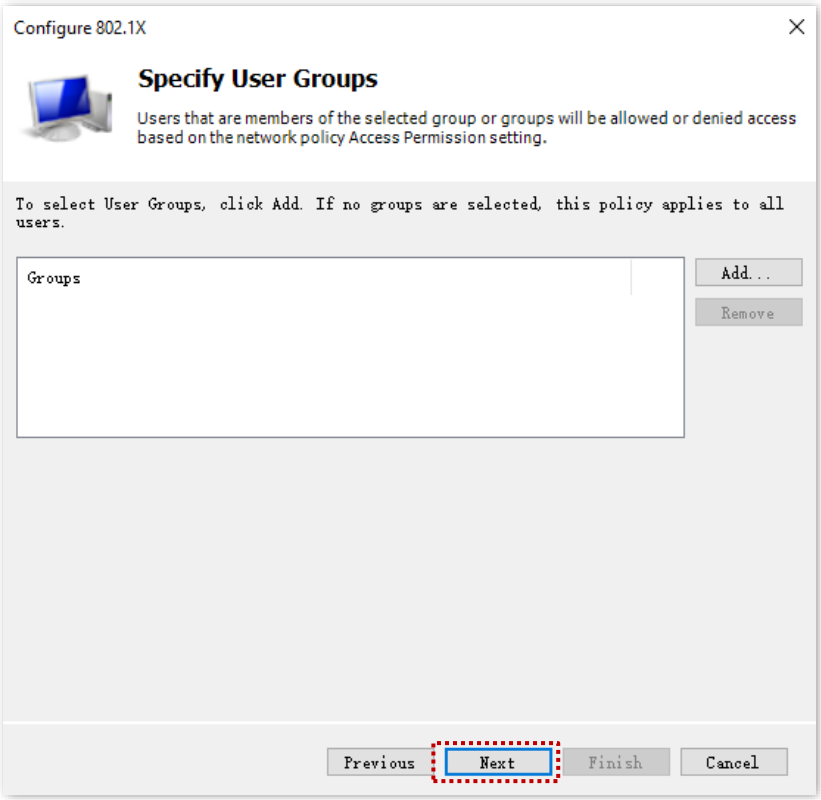


6) Select **Microsoft: Protected EAP (PEAP)** from **Type**, and click **Configure**. Select the certificate deployed in the certificate authority in the previous step, click **OK**, and click **Next** after the configuration is completed.

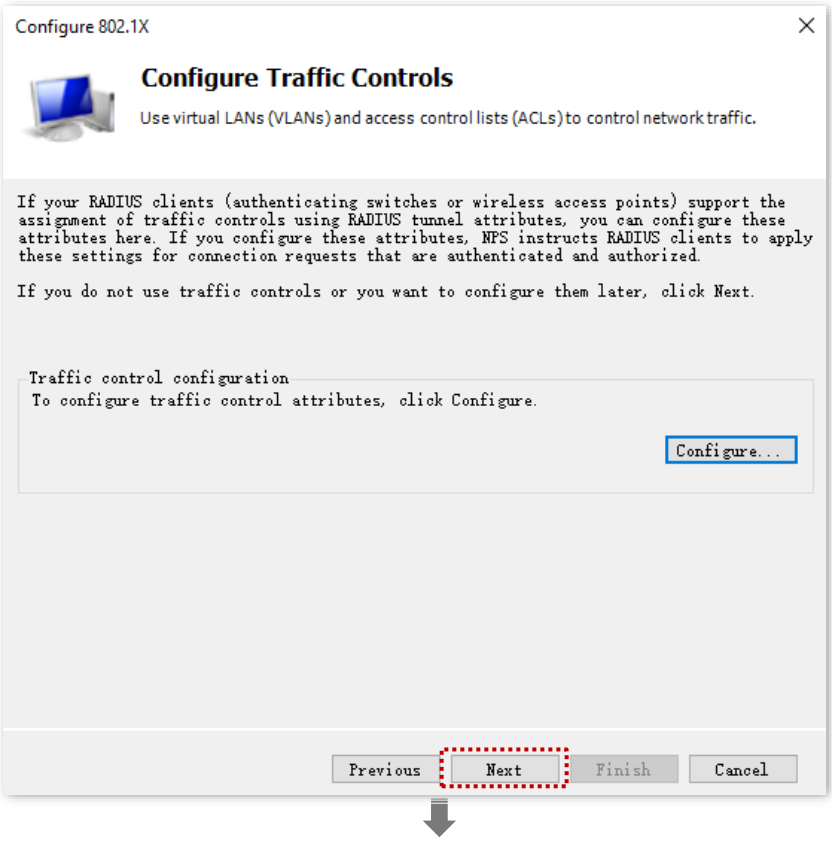


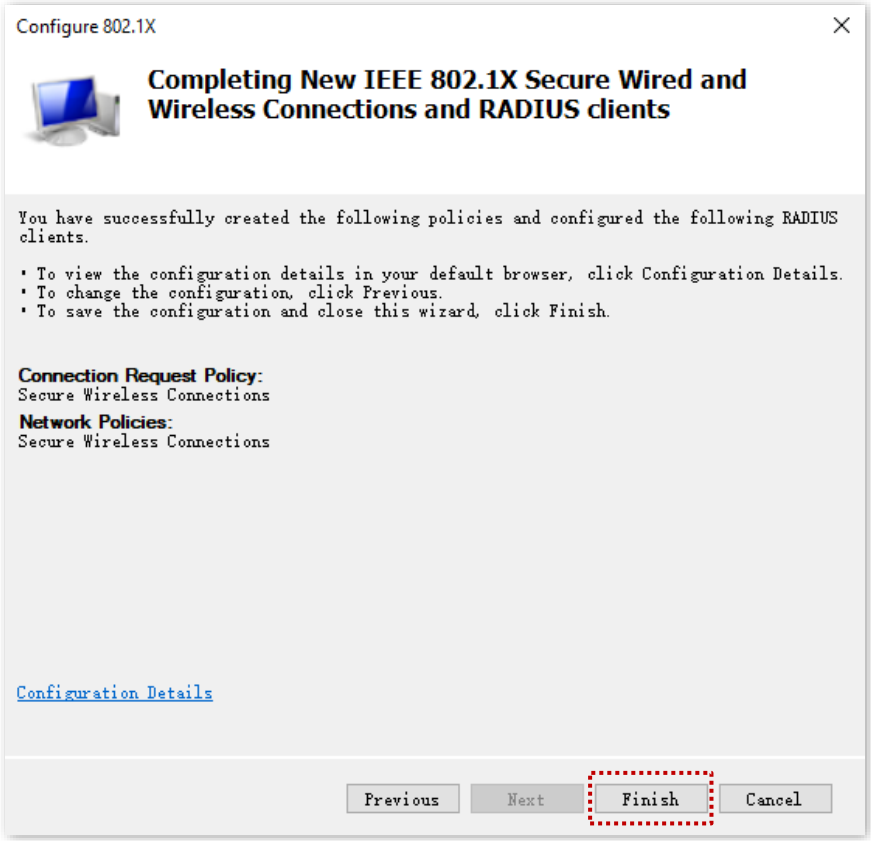


7) Click **Next** on the **Specify User Groups** page.



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



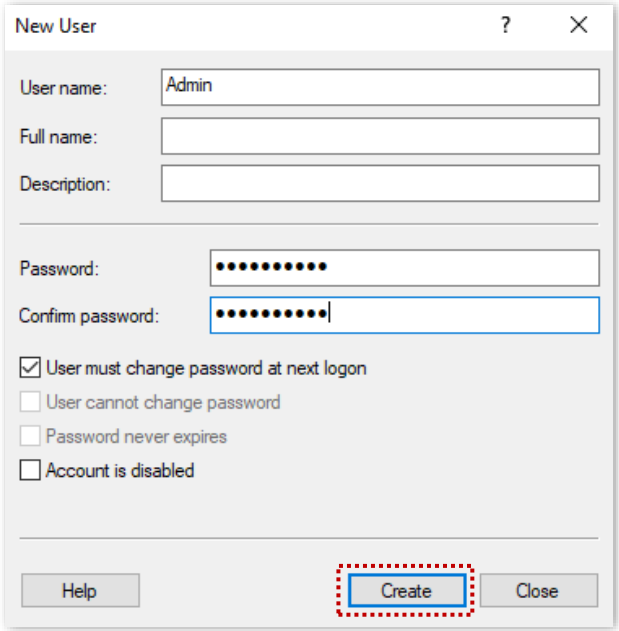


3. Configure the user and user group.

   1) Create a user.

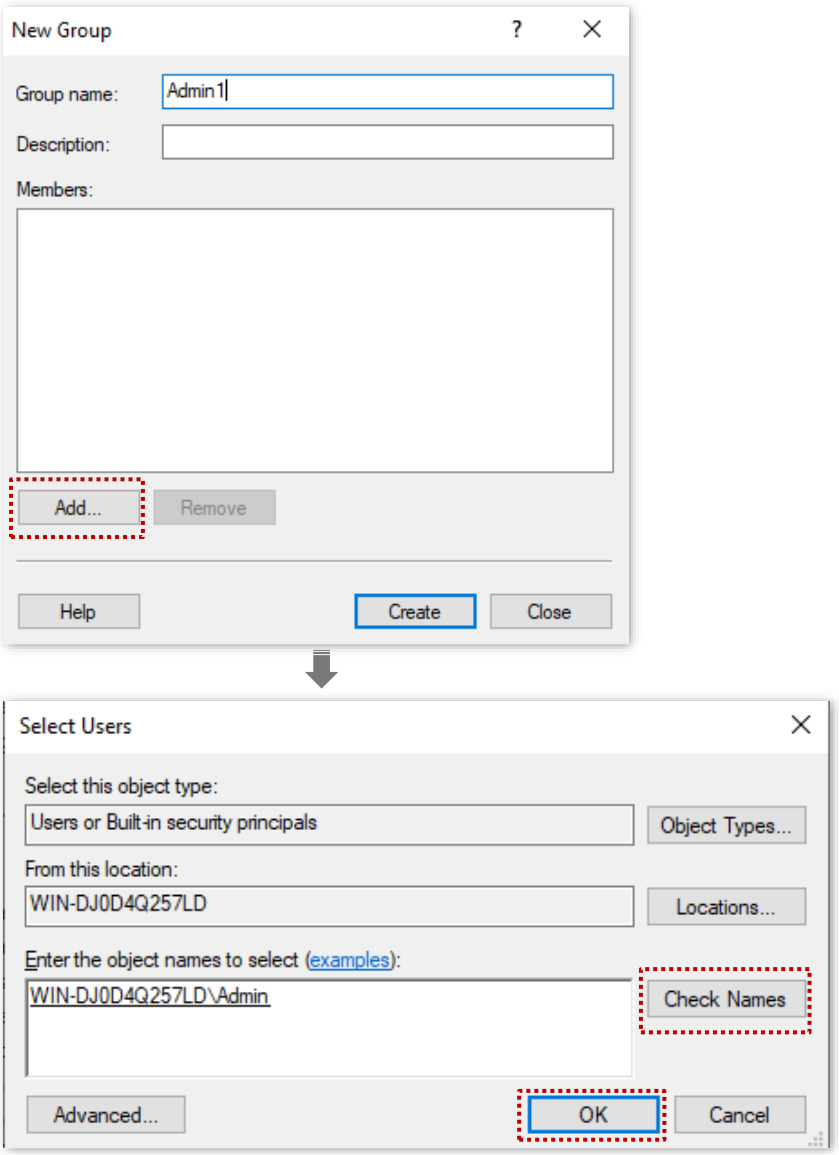
      Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, click **Computer Management**, and double-click **Local Users and Groups**.

      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.

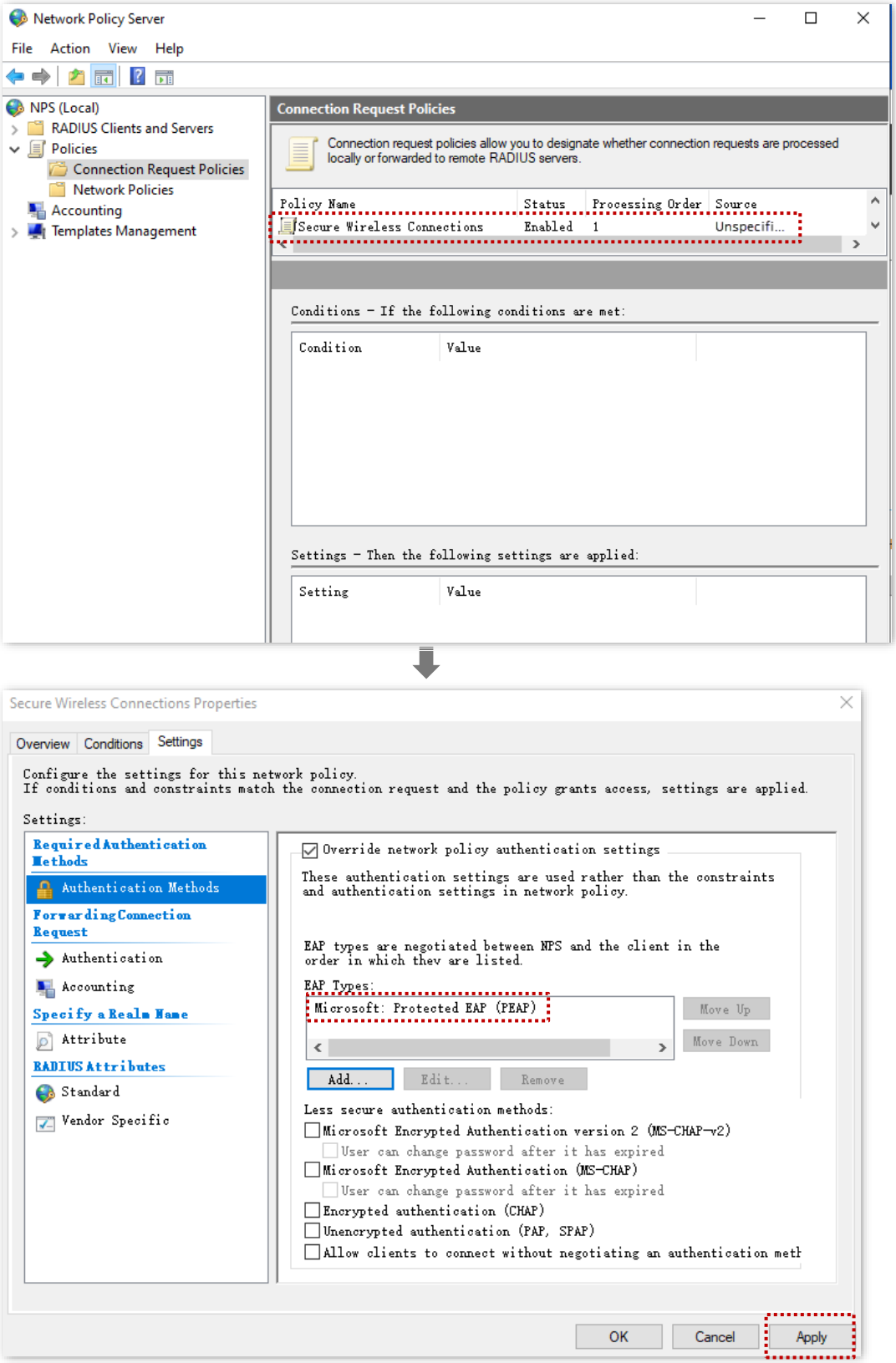
Right-click **Groups**, and select **New Group**. Set **Group name**, which is **Admin1** in this example, and click **Add**. In the **Enter the object names to select** column, enter the created user name, click **Check Names**, and click **OK**. In the **New Group** window, click **Create**.



4. Configure the policies.

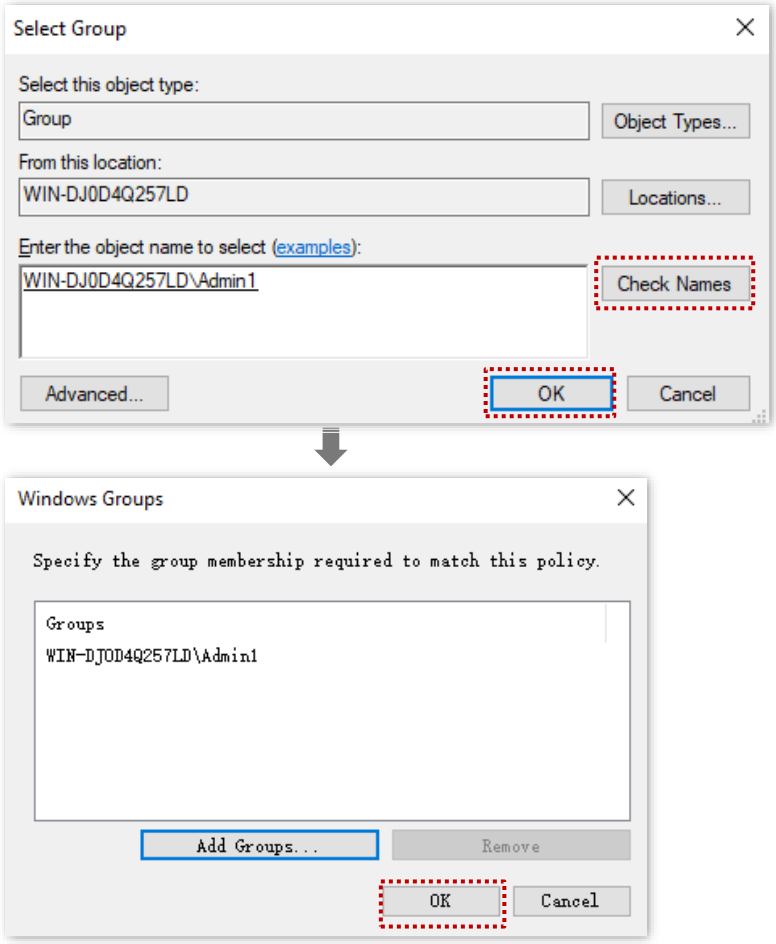
1) Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, click **Network Policy Server**, and double-click **Policies**.

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**.



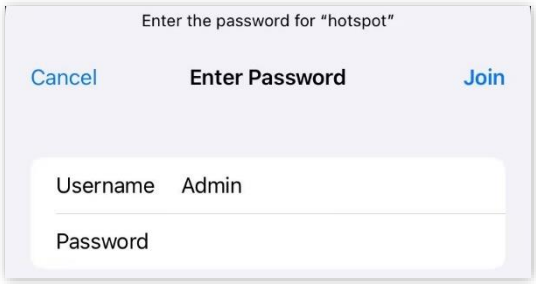
III. Configure the Wi-Fi-enabled device

Smartphone (iOS system) is used as an example.

1. Tap the (Settings) on the smartphone, tap **WLAN**, and connect the smartphone to the AP's Wi-Fi network, which is **hotspot** in this example.
2. Enter the username and password, and tap **Join**.

TIP

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



---End

Verification

The Wi-Fi-enabled devices can connect to the Wi-Fi network named **hotspot**.

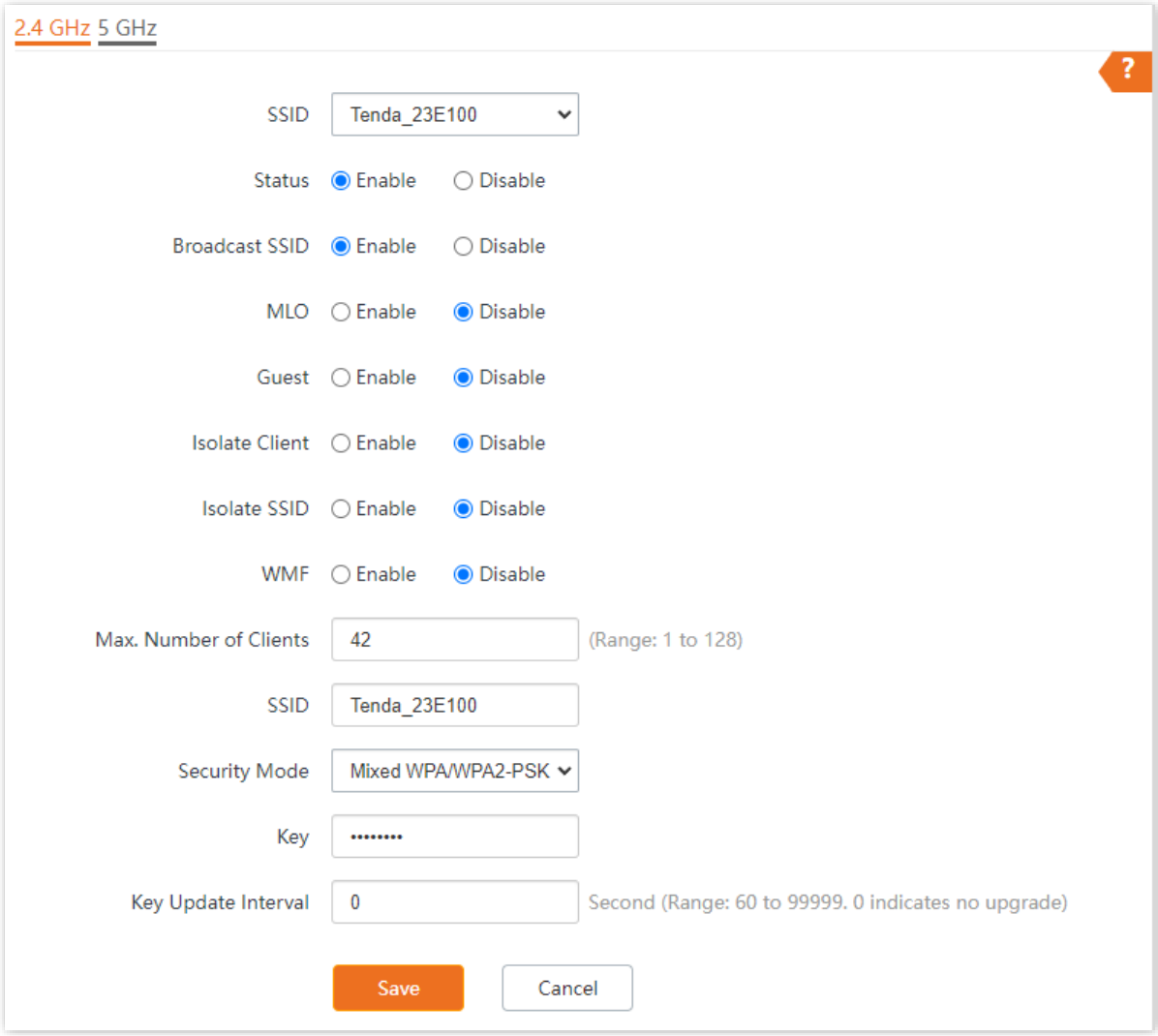
TIP

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.

4.1.4 Parameter description

You can set SSID-related parameters of the AP.



Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	
SSID	Specifies the SSID to be configured. The first SSID displayed on the page under the radio band tab is the primary SSID of the radio band.
Status	Specifies the status of the selected SSID. The first SSID is enabled by default while other SSIDs are disabled by default. You can enable them as required.

Parameter	Description
Broadcast SSID	Specifies whether to enable the broadcast SSID function. 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 Wi-Fi network corresponding to the SSID. It enhances the security of the Wi-Fi network.
MLO	Specifies whether to enable the MLO function. After this function is enabled, coordinate multiple links in different frequency bands for communication to realize multi-band connection with the client, achieving higher bandwidth and lower latency. TIP It is available only when the wireless client supports the Wi-Fi 7 (IEEE 802.11be) protocol.
Guest	Specifies whether to enable the guest function. After this function is enabled, wireless clients connected to the Wi-Fi network can only access the internet and cannot access LAN resources (including the web UI of the AP). Setting up a guest network can meet the internet access needs of guests while ensuring the security of the primary network.
Isolate Client	Specifies whether to enable the isolate client function. After this function is enabled, it isolates the wireless clients connected to the same Wi-Fi 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.
Isolate SSID	Specifies whether to enable the isolate SSID function. After this function is enabled, wireless clients connected to different SSIDs of the AP cannot communicate with each other, enhancing the security of the Wi-Fi network.
WMF	Specifies whether to enable the WMF function. The WMF function of the AP converts multicast traffic into unicast traffic and forwards the traffic to the multicast traffic destination in the Wi-Fi network. This helps save wireless resources, ensure reliable transmission, and reduce delays.
Max. Number of Clients	Specifies the maximum number of clients that can be concurrently connected to the Wi-Fi network corresponding to an SSID. After this upper limit is reached, new clients cannot connect to the SSID unless some clients cut off their connections.
SSID	Used to change the selected SSID.
Security Mode	Specifies the security mode of the selected SSID. The options include: None, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK,WPA, WPA2, WPA3-SAE and WPA2-PSK&WPA3-SAE. TIP The security modes may differ with different models and radio bands of APs. The actual product prevails.

Security mode

A Wi-Fi network uses radio, which is open to the public, as its data transmission medium. If the Wi-Fi 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 Wi-Fi networks must be encrypted for protection.

The AP supports various security modes for network encryption, including None, WPA-PSK, WPA2-PSK, WPA-PSK&WPA2-PSK (Mixed WPA/WPA2-PSK), WPA, WPA2, WPA3-SAE and WPA2-PSK&WPA3-SAE. The security modes may differ with different models and radio bands of APs. The actual product prevails.

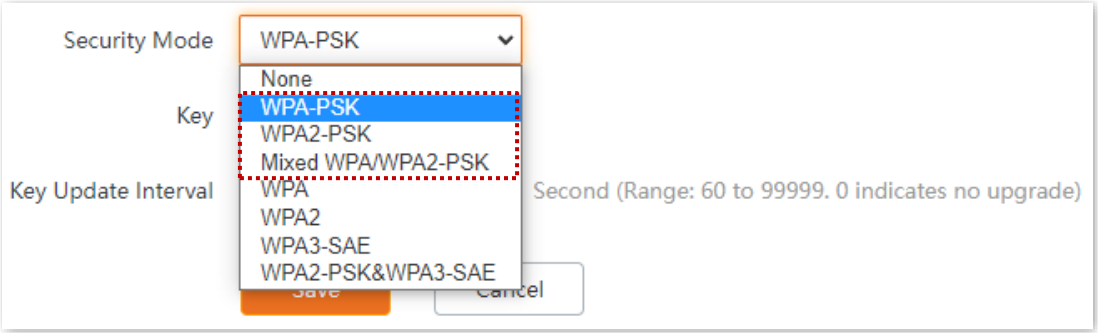
- **None**

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

- **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 Wi-Fi 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.

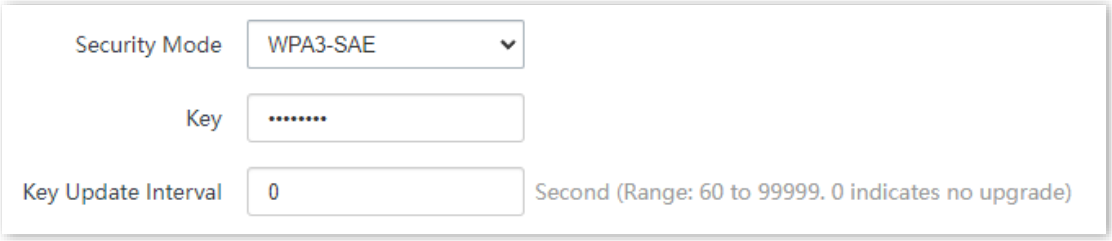


- **WPA3-SAE**

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

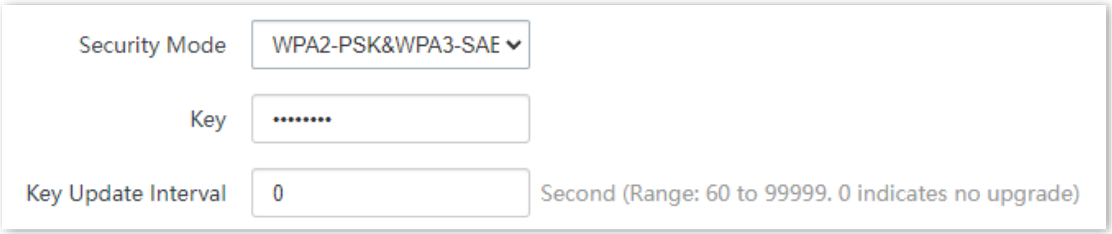
TIP

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



- **WPA2-PSK&WPA3-SAE**

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



Parameter description

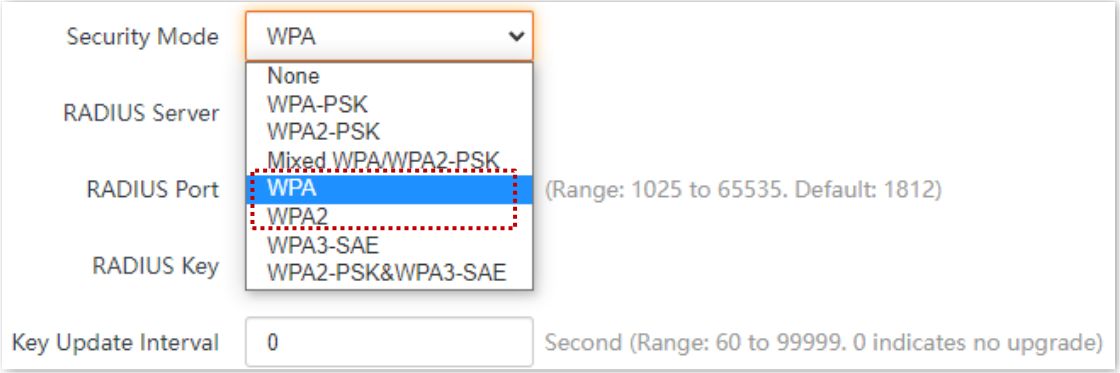
Parameter	Description
Security Mode	Specifies the personal or pre-shared key security mode, including **WPA-PSK**, **WPA2-PSK**, **WPA-PSK&WPA2-PSK (Mixed WPA/WPA2-PSK)**, **WPA3-SAE** and **WPA2-PSK&WPA3-SAE**. – **WPA-PSK**: It indicates that the Wi-Fi network corresponding to the selected SSID is encrypted with WPA-PSK. – **WPA2-PSK**: It indicates that the Wi-Fi 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 Wi-Fi network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK. – **WPA3-SAE**: It indicates that the Wi-Fi network corresponding to the selected SSID is encrypted with WPA3-SAE. – **WPA2-PSK&WPA3-SAE**: The Wi-Fi network adopts the mixed encryption mode of WPA2-PSK/AES and WPA3-SAE/AES to ensure safety.
Key	Specifies a pre-shared WPA key, that is, the password clients use to connect to the Wi-Fi network.
Key Update Interval	Specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value **0** indicates that a WPA key is not updated.

- **WPA and WPA2**

To address the key management weakness of WPA-PSK and WPA2-PSK, the Wi-Fi 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 Wi-Fi networks that require high security.



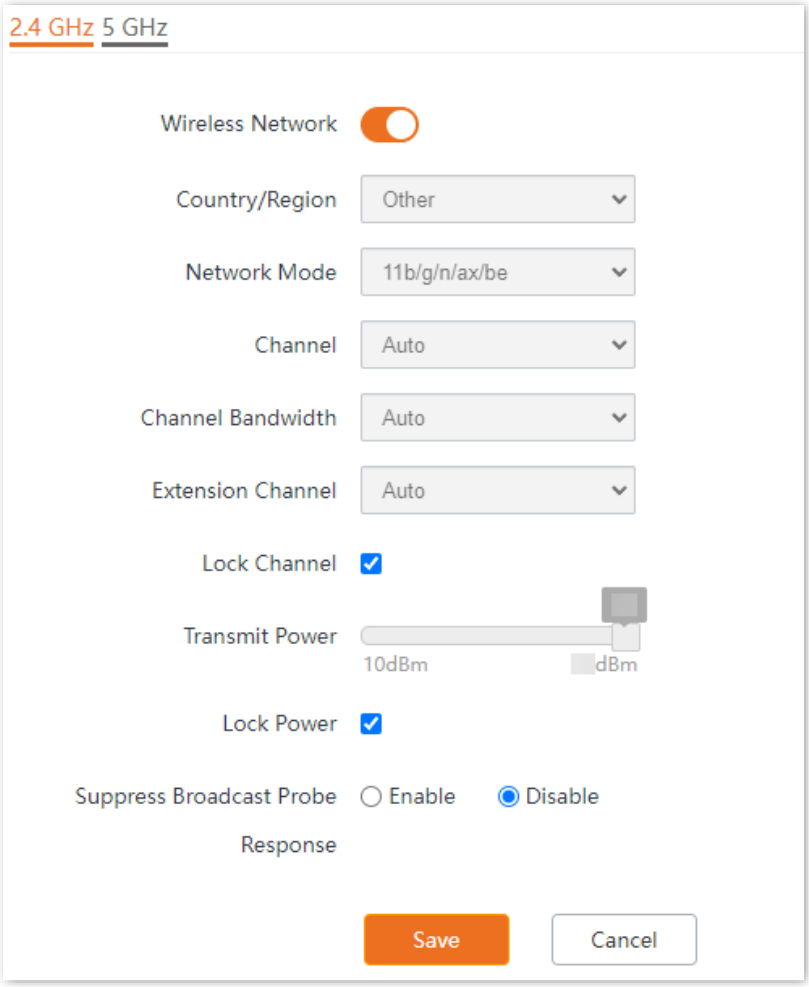
Parameter description

Parameter	Description
Security Mode	The **WPA** and **WPA2** options are available for network protection with a RADIUS server. - **WPA**: It indicates that the Wi-Fi network corresponding to the selected SSID is encrypted with WPA. - **WPA2**: It indicates that the Wi-Fi 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	Specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value **0** indicates that a WPA key is not updated.

4.2 Configure radio frequency

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

You can modify the basic radio parameters.



Parameter description

Parameter	Description
2.4 GHz 5 GHz	Used to select the radio band of the AP to be configured.
Wireless Network	Specifies whether to enable the Wi-Fi network function of the AP.
Country/Region	Specifies the country or region where the AP is used. This parameter helps comply with channel regulations of the country or region. This parameter can be set if Lock Channel is not selected.

Parameter	Description
Network Mode	Specifies the Wi-Fi network mode of the AP. This parameter can be set if Lock Channel is not selected. Available options for 2.4 GHz are **11b**, **11g**, **11b/g**, **11b/g/n**, **11b/g/n/ax** and **11b/g/n/ax/be**, and available options for 5 GHz are **11a**, **11ac**, **11a/n**, **11a/n/ac/ax** and **11a/n/ac/ax/be**. - **11b**: The AP works in 802.11b mode. - **11g**: The AP works in 802.11g mode. - **11b/g**: The AP works in 802.11b/g mode. - **11b/g/n**: The AP works in 802.11b/g/n mode. - **11b/g/n/ax**: The AP works in 11b/g/n/ax mode. - **11b/g/n/ax/be**: The AP works in 11b/g/n/ax/be mode. - **11a**: The AP works in 802.11a mode. - **11ac**: The AP works in 802.11ac mode. - **11a/n**: The AP works in 802.11a/n mode. - **11a/n/ac/ax**: The AP works in 11a/n/ac/ax mode. - **11a/n/ac/ax/be**: The AP works in 11a/n/ac/ax/be mode. TIP The Wi-Fi network modes of the AP may differ with different models of APs. The actual product prevails.
Channel	Specifies the operating channel of the AP. This parameter can be set if Lock Channel is not selected. **Auto**: It indicates that the AP automatically adjusts its operating channel according to the ambient environment. If you frequently experience disconnections, lag, or slow internet speeds when connecting to the AP's Wi-Fi network, try changing the AP's channel. You can use the frequency analysis function to detect channels that are less used and have less interference in the surrounding area.

Parameter	Description
Channel Bandwidth	Specifies the wireless channel bandwidth of the AP. This parameter can be set if Lock Channel is not selected. - **20 MHz**: It indicates that the AP can use only 20 MHz channel bandwidth. - **40 MHz**: It indicates that the AP can use only 40 MHz channel bandwidth. - **80 MHz**: It indicates that the AP can use only 80 MHz channel bandwidth. - **160 MHz**: It indicates that the AP can use only 160 MHz channel bandwidth. - **Auto**: The AP automatically adjusts its channel bandwidth according to the surrounding environment. TIP The wireless channel bandwidths of the AP may differ with different models of APs. The actual product prevails.
Extension Channel	Used to determine the operating frequency band of the AP when it uses the 40 MHz channel bandwidth in 11n mode. This parameter can be set if Lock Channel is not selected.
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 Wi-Fi 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** 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**. TIP This function is available on some APs. The actual product prevails.

Parameter	Description
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%. TIP This function is available on some APs. The actual product prevails.
Suppress Broadcast Probe Response	Specifies whether to enable the suppress broadcast probe response function. By default, Wi-Fi-enabled devices keep sending Probe Request packets that include the SSID field to scan their nearby Wi-Fi networks. After receiving such packets, AP determines whether the Wi-Fi-enabled devices are allowed to access its Wi-Fi 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, the AP does not respond to the requests without an SSID, saving wireless resources.

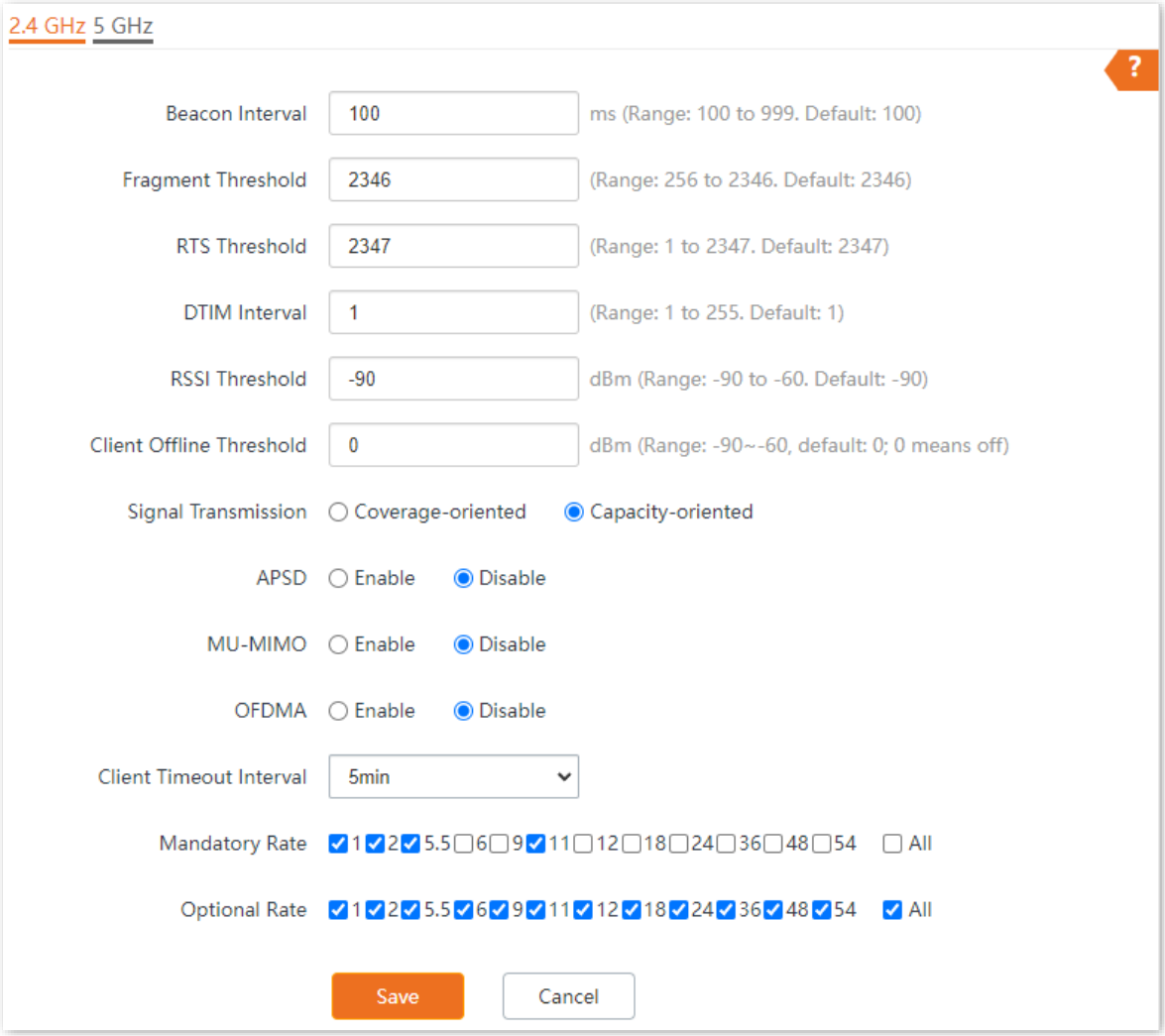
4.3 Optimize radio frequency

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

You can modify the radio parameters to optimize performance.

NOTE

It is recommended to retain the default settings without professional guidance to avoid reducing the AP's wireless performance.



Parameter description

Parameter	Description
2.4 GHz 5 GHz	Used to select the radio band of the AP to be configured.
Beacon Interval	Used to set the interval at which the AP sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a Wi-Fi network. Generally, a smaller interval allows wireless clients to connect to the AP sooner, while a larger interval allows the Wi-Fi network to transmit data quicker.

Parameter	Description
Fragment Threshold	Specifies the threshold of a fragment. Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented. In case of a high error rate, you can reduce the threshold to enable this device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput.
RTS Threshold	Specifies the frame length threshold for triggering the RTS/CTS mechanism. The unit is byte. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a Wi-Fi network to recover from conflicts quicker. For a Wi-Fi network with high user density, you can reduce this threshold to reduce conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	Specifies the countdown before the AP transmits broadcast and multicast frames in its cache. The unit is Beacon interval. For example, if **DTIM Interval** is set to **1**, the AP transmits all cached frames at one Beacon interval.
RSSI Threshold	Used to set the minimum strength of received signals acceptable to the AP. If the strength of the signals transmitted by a Wi-Fi-enabled device is weaker than this threshold, the Wi-Fi-enabled device cannot connect to the AP. A proper value facilitates Wi-Fi-enabled devices to connect to the AP with stronger signal in case of multiple APs exist.
Client Offline Threshold	Used to set the minimum signal strength required for a client to maintain connection to the AP. If a client's access signal strength falls below the configured threshold, the AP will disconnect it.
Signal Transmission	Select the option based on your actual situation. - **Coverage-oriented**: This mode broadens wireless coverage of APs, and is usually used in scenarios deployed with fewer APs, such as offices, warehouses, and hospitals. - **Capacity-oriented**: This mode effectively decreases mutual interference among APs, and is usually used in scenarios deployed with massive APs, such as conferences, exhibition halls, banquet halls, stadiums, classrooms of higher-education institutes and airports.

Parameter	Description
Air Interface Scheduling	Specifies whether to enable the air interface scheduling function of the AP. This enables the users experiencing high download rates to download more data, so that this device can achieve higher system throughput and connect to a greater number of clients. TIP This function is available on some APs. The actual product prevails.
Anti-interference Mode	Specifies the anti-interference modes you can select for your AP. - **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. TIP This function is available on some APs. The actual product prevails.
APSD	Specifies whether to enable the automatic power save delivery function. Enabling APSD helps reduce power consumption.
MU-MIMO	Multi-User Multiple-Input Multiple-Output. If this function is enabled, AP can communicate with multiple users concurrently, avoiding Wi-Fi network congestion and improving communication.
OFDMA	Orthogonal Frequency Division Multiple Access. If this function is enabled, multiple clients can transmit data at the same time, so that the transmission efficiency is improved, delay is reduced, and user experience is enhanced. However, this function may cause compatibility issues. Therefore, you are recommended to disable this function to avoid compatibility issues.
Client Timeout Interval	Used to set the wireless client disconnection interval of the AP. The AP disconnects from a wireless client if no traffic is transmitted or received by the wireless client within the interval.
Mandatory Rate	Specifies rates that wireless clients must support in order to connect to the Wi-Fi networks of the AP.
Optional Rate	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.

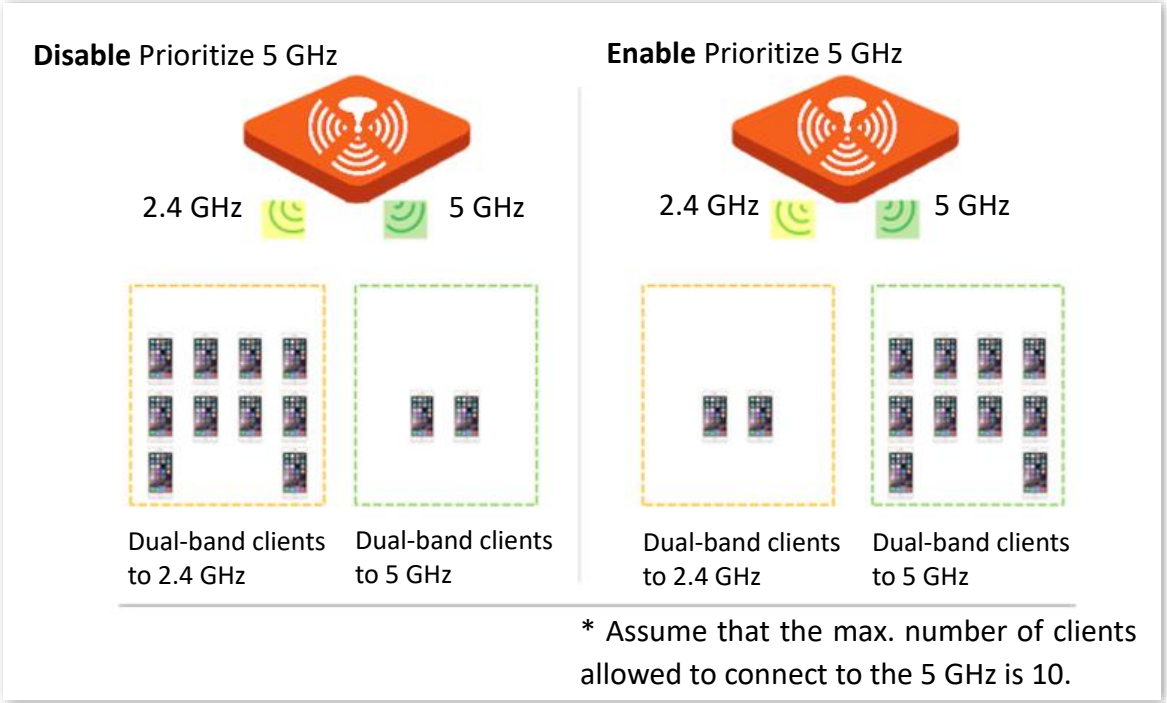
Parameter	Description
Prioritize 5 GHz	Specifies whether to enable the prioritize 5 GHz function. If this function is enabled, dual band Wi-Fi-enabled devices prefer the 5 GHz Wi-Fi network of the AP to connect when the 5 GHz signal strength transmitted by devices is greater than or equal to the **Prioritize 5 GHz Threshold**.
Prioritize 5 GHz Threshold	With this function enabled, if the strength of the signals transmitted by a Wi-Fi-enabled device is greater than or equal to this threshold, the Wi-Fi-enabled device connects to the 5 GHz Wi-Fi network. Otherwise, it connects to the 2.4 GHz Wi-Fi network.

- **Prioritize 5 GHz**

Although the 2.4 GHz band is more widely used than the 5 GHz band in actual Wi-Fi 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 Wi-Fi 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.

4.4 Configure load balancing

4.4.1 Configure load balancing between APs

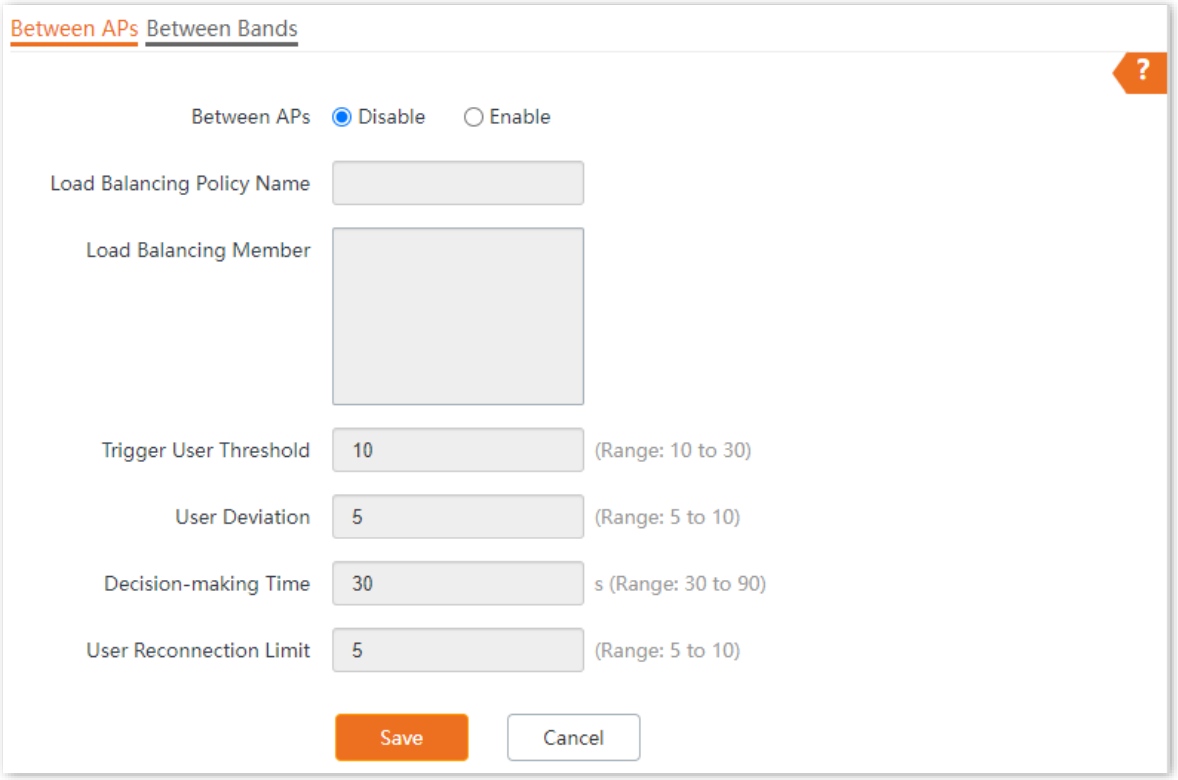
In an actual Wi-Fi network environment, especially in high-density scenarios, it often happens that too many users connect to a certain AP. As a result, some APs are overloaded while others are idle. The load balancing between APs function can accurately balance the load among these APs. In this way,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

TIP

The load balancing policy takes effect only when APs use the same load balancing policy name and have identical SSIDs and Wi-Fi passwords.

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Load Balancing** > **Between APs**.

You can view or configure the parameters of load balancing between APs. The following figure is for reference only.



Parameter description

Parameter	Description
Between APs	Specifies whether to enable the load balancing between APs function.
Load Balancing Policy Name	Specifies the load balancing policy between APs applied by AP. It supports load balancing based on user number. This policy can be delivered to the AP via the controller (a device with AP management and AP load balancing functions) or configured directly through the AP's web UI. TIP If there is no controller in the LAN where the APs are located, APs with the same load balancing policy name will automatically form a load balancing group.
Load Balancing Member	Specifies the APs added in the load balancing policy. The MAC addresses of APs with the same load balancing policy name enabled in the network will be automatically filled in here.
Trigger User Threshold	Specifies the threshold to trigger load balancing between APs. When users connected to an AP reaches the threshold, load balancing between APs is triggered.
User Deviation	Specifies the deviation between the number of users of two APs. If deviation between the user numbers of two APs applying the same load balancing policy exceeds this value, new users are directed to the AP with fewer users first.

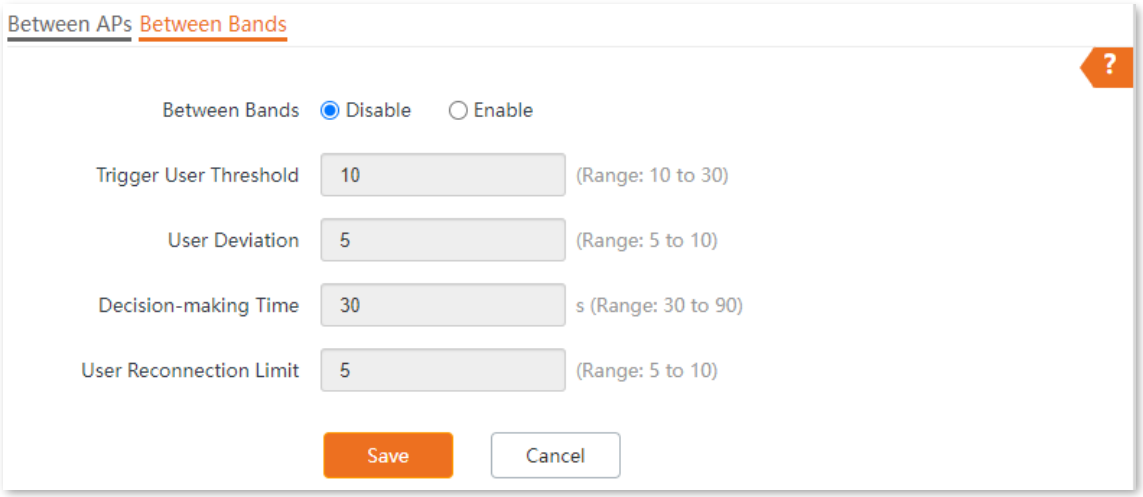
Parameter	Description
Decision-making Time	Specifies the period in which AP refuses user connection request. It is recommended to keep the default settings. If within this period, the number of AP refusals has reached the **User Reconnection Limit**, AP allows access from this user. If within this period, the number of AP refusals does not reach **User Reconnection Limit**, the number of refusals is erased.
User Reconnection Limit	Specifies the largest number of user connection attempts. If the number of AP refusals has reached this value in **Decision-making Time**, AP allows access from this user. It is recommended to keep the default settings.

4.4.2 Configure load balancing between bands

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

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Load Balancing** > **Between Bands**.

You can view or configure the parameters of load balancing between bands. The following figure is for reference only.



Parameter description

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

4.5 Configure frequency analysis

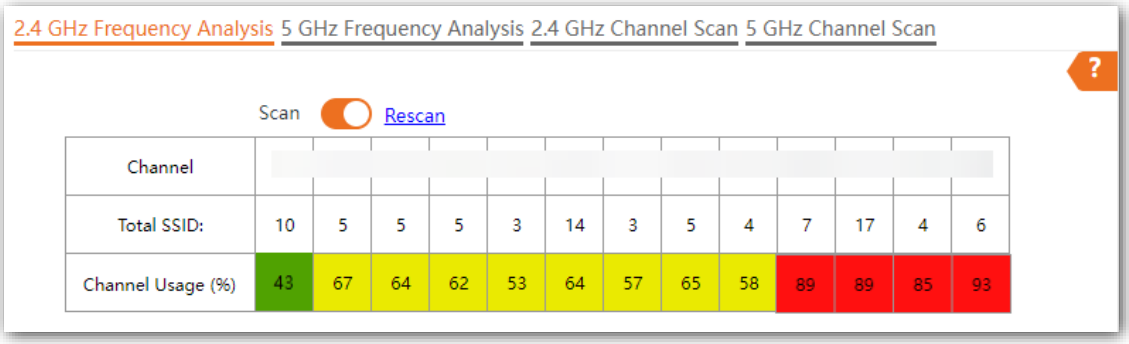
4.5.1 View frequency analysis

You can view the number of signals and channel utilization of each channel, and then select a channel with lower utilization as the working channel of the AP to improve wireless transmission efficiency.

Procedure for viewing frequency analysis

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Frequency Analysis**.
3. Click **2.4 GHz Frequency Analysis** or **5 GHz Frequency Analysis** tab to select the Wi-Fi network radio band for frequency analysis, which is **2.4 GHz Frequency Analysis** in this example.
4. Enable **Scan**.

---End



After scanning, you can select a channel with lower utilization as the AP working channel.

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

4.5.2 Perform channel scan

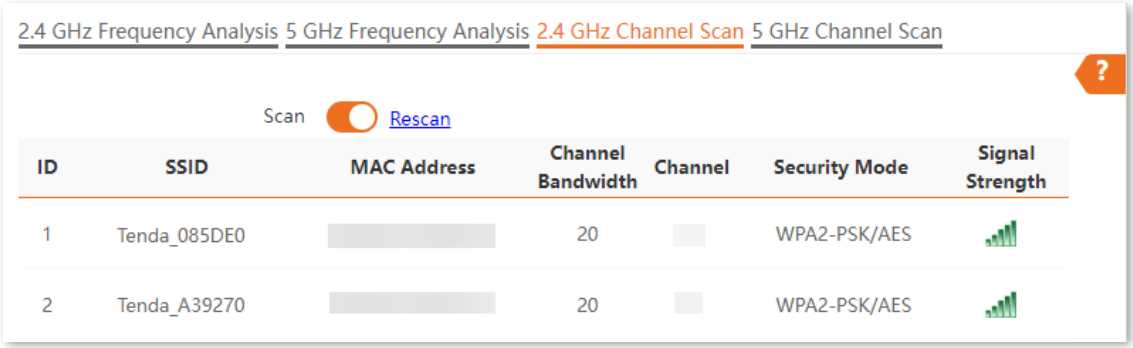
The scan result list presents you with information about nearby Wi-Fi network, including SSID, MAC address, channel, channel bandwidth, and signal strength.

Procedure for performing channel scan

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

---End

Scan results are as shown in the figure below.



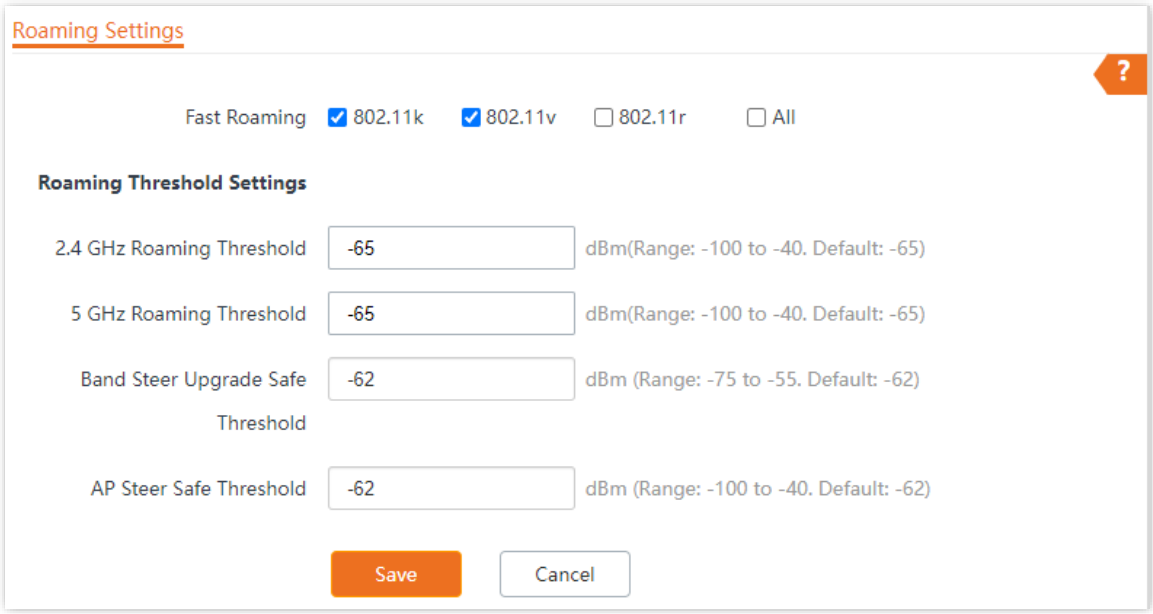
4.6 Configure roaming settings

Wireless roaming means that a client automatically connects to the AP with better signal and disconnects from the original AP when it moves to a critical area covered by two or more APs. The premise is that the SSID, security mode and key of these APs are the same.

The IEEE 802.11k/v/r fast roaming protocol can effectively solve the following problems.

- The packet loss is serious in the traditional roaming process.
- The roaming trigger is not timely.
- The roaming target is not the most suitable AP.

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Roaming Settings**. You can set the roaming parameters of the AP.



Parameter description

Parameter	Description
Fast Roaming	Specifies whether to enable the fast roaming function. - **802.11k:** Wireless spectrum resource measurement protocol. With the protocol enabled, the client will be assisted in scanning roamable target APs, solving the problem of whether you should roam and when you need to roam. - **802.11v:** Wi-Fi network management protocol. With the protocol enabled, the client will be assisted in selecting roamable target APs, solving the problem of which AP to roam to. - **802.11r:** Specifies the fast BSS conversion protocol. With the protocol enabled, it will reduce roaming time without the handshake metric during wireless reconnection, solving the problem of how to roam quickly.

Parameter	Description
2.4 GHz Roaming Threshold	Used to set 2.4 GHz or 5 GHz roaming threshold, which means setting the sensitivity of the client to roaming. When the signal strength received by the client from the AP falls below the roaming threshold, the roaming is triggered and the AP with better link quality is switched over.
5 GHz Roaming Threshold	TIP The larger the roaming threshold, the higher the roaming sensitivity. The smaller the roaming threshold, the lower the roaming sensitivity.
Band Steer Upgrade Safe Threshold	Used to set band steer upgrade safe threshold. When a client is connected to either the 2.4 GHz or 5 GHz band of an AP, it will automatically connect to another frequency band if the received signal strength from the current band falls below the configured threshold.
AP Steer Safe Threshold	Used to set AP steer upgrade safe threshold. When connected to an AP, the client will automatically switch to the other AP with better signal if the client moves and the received signal strength falls below the configured threshold.

4.7 Enable client type identification function

After enabling this function, the AP can identify the operating system types of Wi-Fi-enabled devices connected to its Wi-Fi network, making Wi-Fi network management more effective. The client types that the AP can identify include: Android, iOS, WPhone, Windows, MacOS, and so on.

Procedure for enabling client type identification function

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Advanced Settings**.
3. Enable the **Identify Client Type** function.
4. Click **Save**.

---End

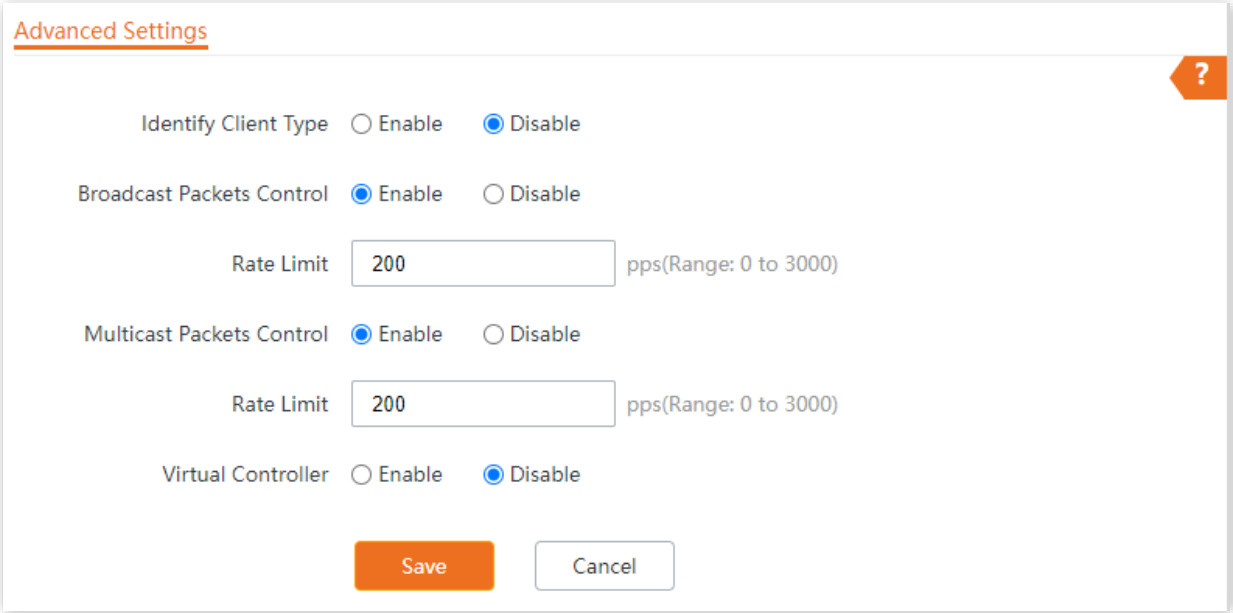
After the configuration is completed, if the client connects to the AP Wi-Fi and has accessed HTTP websites, you can view the client's operating system type on the **Status** > **Client List** page.

4.8 Configure broadcast and multicast packet control

Limiting the transmission rate of broadcast or multicast packets can prevent the channel from being occupied by such invalid traffic, reducing air interface resource waste, lowering interference, improving transmission efficiency, and enhancing user experience.

Procedure for configuring broadcast and multicast packet control

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Advanced Settings**.
3. Enable the **Broadcast Packets Control** function.
4. Set the **Rate Limit** for broadcast packets. It is 200 pps by default.
5. Enable the **Multicast Packets Control** function. It is recommended to enable the WMF function simultaneously.
6. Set the **Rate Limit** for multicast packets. It is 200 pps by default.
7. Click **Save**.



---End

4.9 Use the AP as a virtual controller

When there is no AC controller or router supporting AP management in the network, you can configure one AP as a virtual wireless controller to automatically discover and manage other APs with the same SSID, ensuring seamless roaming stability. Only one virtual controller can be configured within the same local area network.

TIP

This function can only be used in a network environment with no less than 2 APs. The primary AP information is displayed in the virtual controller list.

Procedure for enabling the virtual controller function

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Advanced Settings**.
3. Enable the **Virtual Controller** function.
4. Click **Save**.

---End

5 Control internet access

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

5.1 Add devices to the blocklist

Devices on the blocklist cannot access the corresponding AP's Wi-Fi network for internet access.

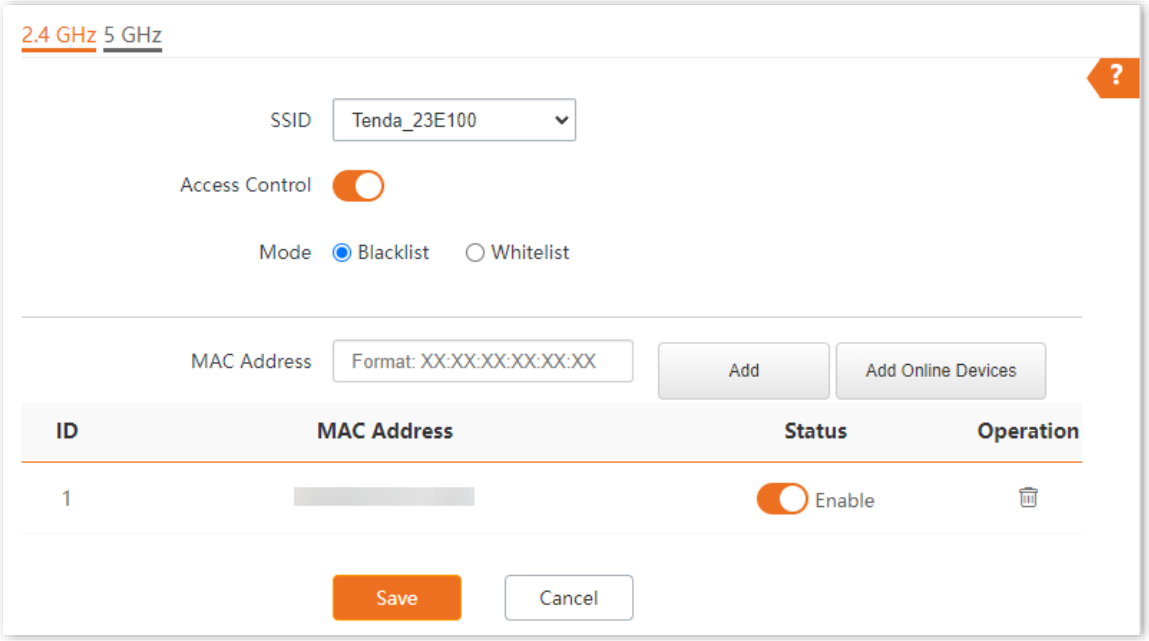
5.1.1 Through the access control function

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Access Control**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Select the **SSID** from the drop-down list.
5. Enable the **Access Control** function, and set **Mode** to **Blacklist**.
6. Enter MAC addresses of the Wi-Fi-enabled devices to which the policy applies, and click **Add**.

   TIP

   If the Wi-Fi-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.

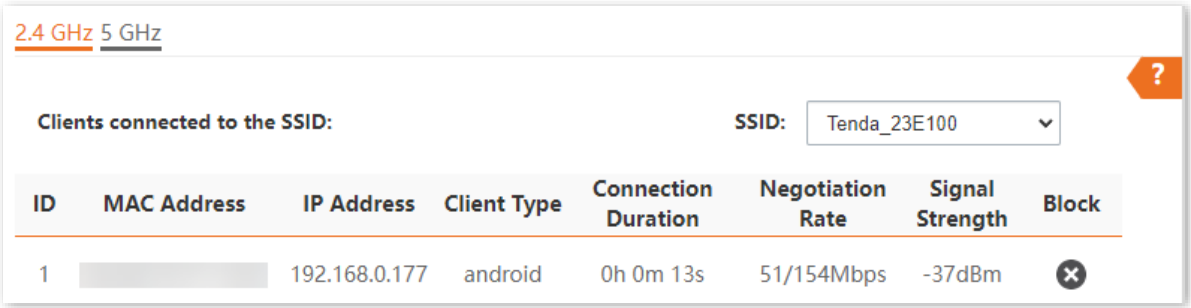
7. Click **Save**.



---End

5.1.2 Through the client list

1. Log in to the web UI of the AP.
2. Navigate to **Status** > **Client List**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Find the device to add to the blocklist, and click ⊗ to disconnect the corresponding device.



---End

After the configuration is completed, the device is added to the access control blocklist. The device cannot connect to the AP again by reconnecting to the Wi-Fi network. To unblock a device, you can remove it from the blocklist.

5.2 Add devices to the whitelist

Devices on the whitelist can connect to the AP's Wi-Fi network to access the internet, while other devices cannot connect to this Wi-Fi network.

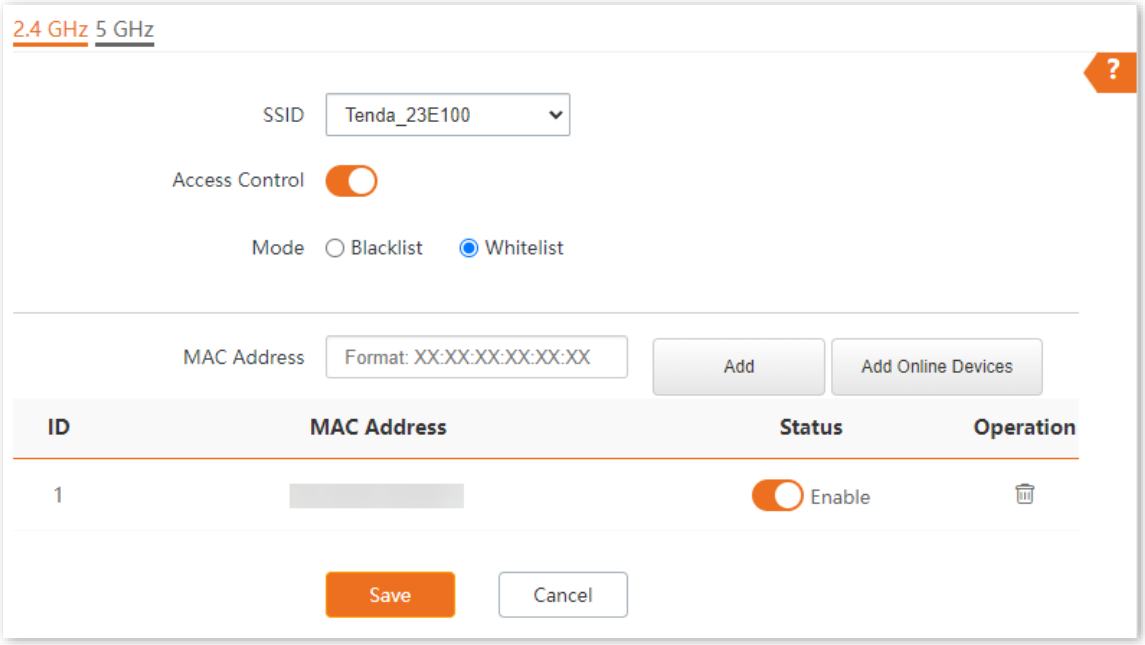
Procedure for adding devices to the whitelist

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Access Control**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Select the **SSID** from the drop-down list.
5. Enable the **Access Control** function, and set **Mode** to **Whitelist**.
6. Enter MAC addresses of the Wi-Fi-enabled devices to which the policy applies, and click **Add**.

TIP

If the Wi-Fi-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.

7. Click **Save**.



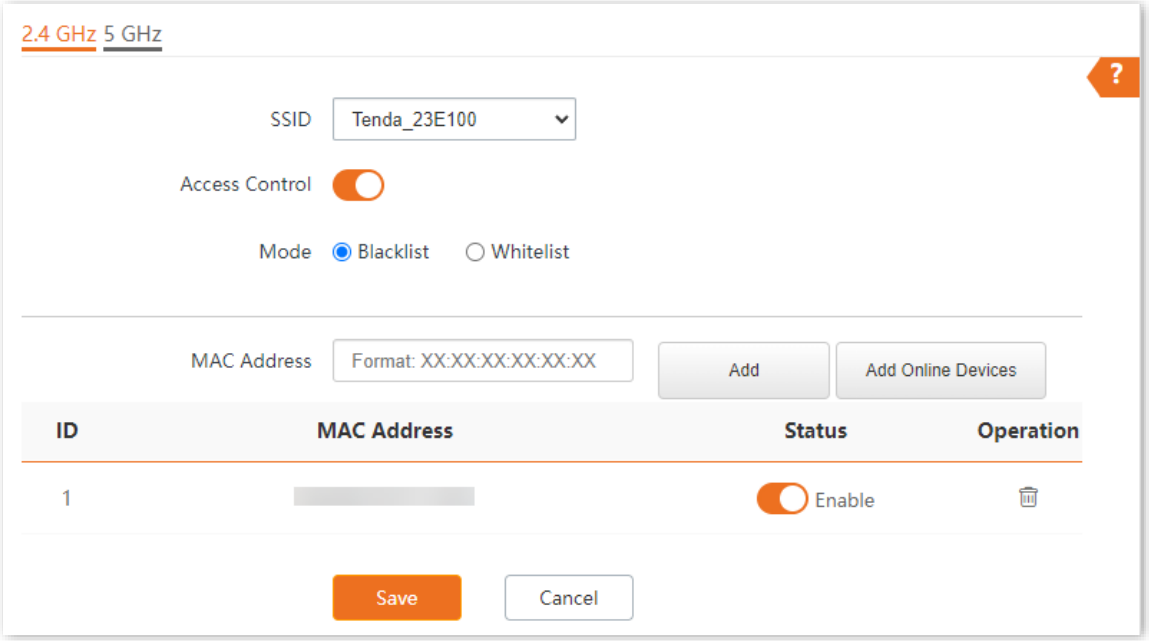
---End

5.3 Remove devices from the blocklist/whitelist

The steps to remove from the blocklist and whitelist are similar. Take removing from the blocklist as an example.

Procedure for removing devices from the blocklist

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Access Control**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Select the **SSID** from the drop-down list.
5. In the access control list, find the device to be removed from the blocklist, then disable the **Enable** toggle or click .
6. Click **Save**.



---End

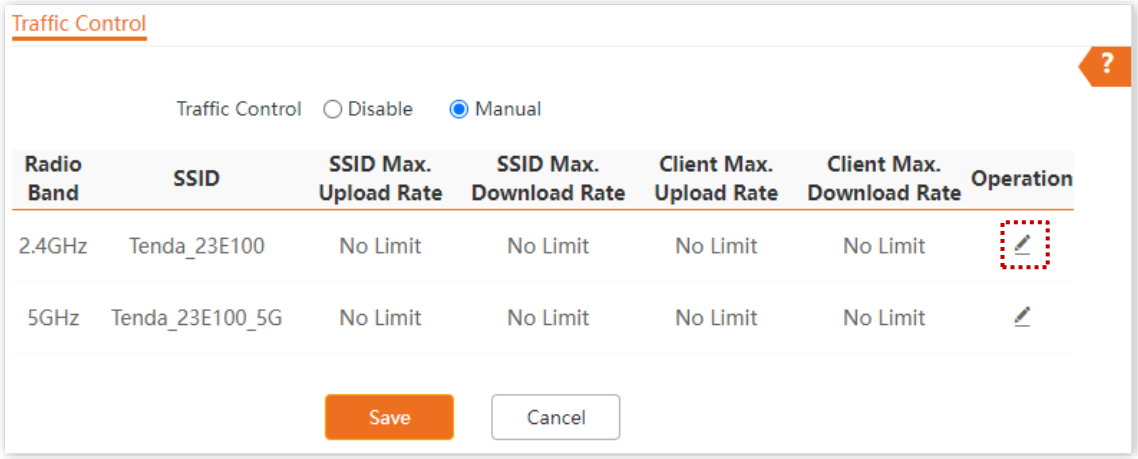
5.4 Control internet access speed

Through the traffic control function, you can set 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.

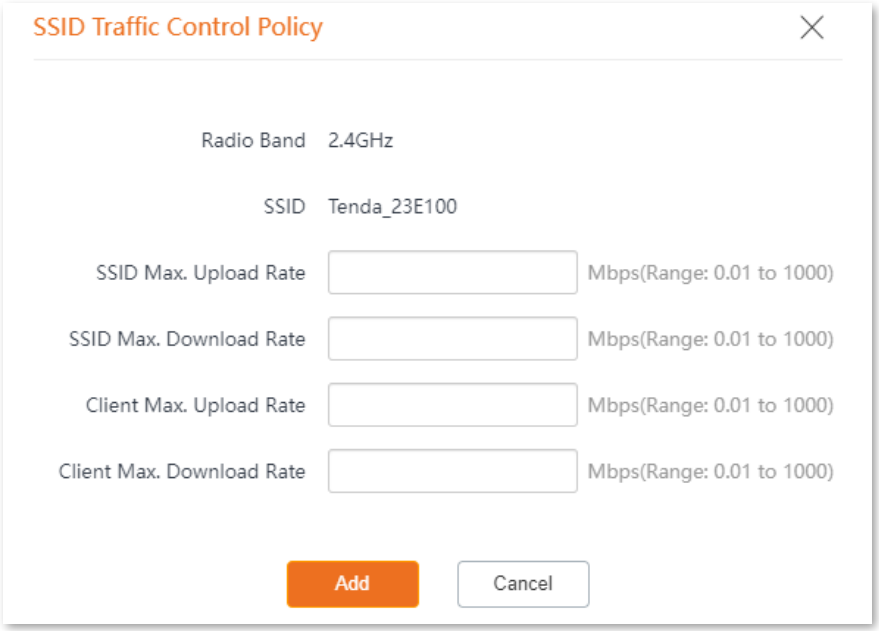
By default, the traffic control function is disabled.

Procedure for controlling internet access speed

1. Log in to the web UI of the AP.
2. Navigate to **Advanced** > **Traffic Control**.
3. Set **Traffic Control** to **Manual**.
4. Click ✎ on the row where the Wi-Fi network to be controlled resides.



5. Set the maximum upload or download rate allowed for the Wi-Fi network and the maximum upload or download rate allowed for every user device connected to the Wi-Fi network.
6. Click **Add**.



---End

Parameter description

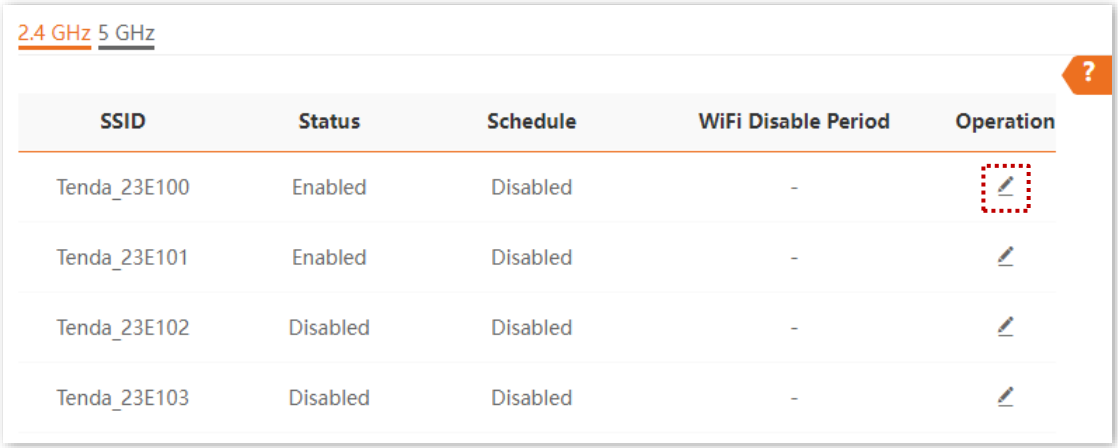
Parameter	Description
Traffic Control	Specifies whether to enable the traffic control function.
Radio Band	Specifies the radio band of the Wi-Fi network on which you manually set a traffic control rule.
SSID	Specifies the name of the Wi-Fi network on which you manually set a traffic control rule.
SSID Max. Upload Rate	Specify the maximum upload or download rate allowed for a Wi-Fi network. If you leave it blank, the maximum upload or download rate of the target Wi-Fi network are not limited. It is available only when you manually set a traffic control rule.
SSID Max. Download Rate	
Client Max. Upload Rate	Specify the maximum upload or download rate allowed for every user device connected to the target Wi-Fi network. If you leave it blank, the maximum upload or download rate of every user device connected to the target Wi-Fi network are not limited. It is available only when you manually set a traffic control rule.
Client Max. Download Rate	
Operation	Click to set the maximum upload or download rate allowed for the target Wi-Fi network and the maximum upload or download rate allowed for every user device connected to the target Wi-Fi network. It is available only when you manually set a traffic control rule.

5.5 Control internet usage time

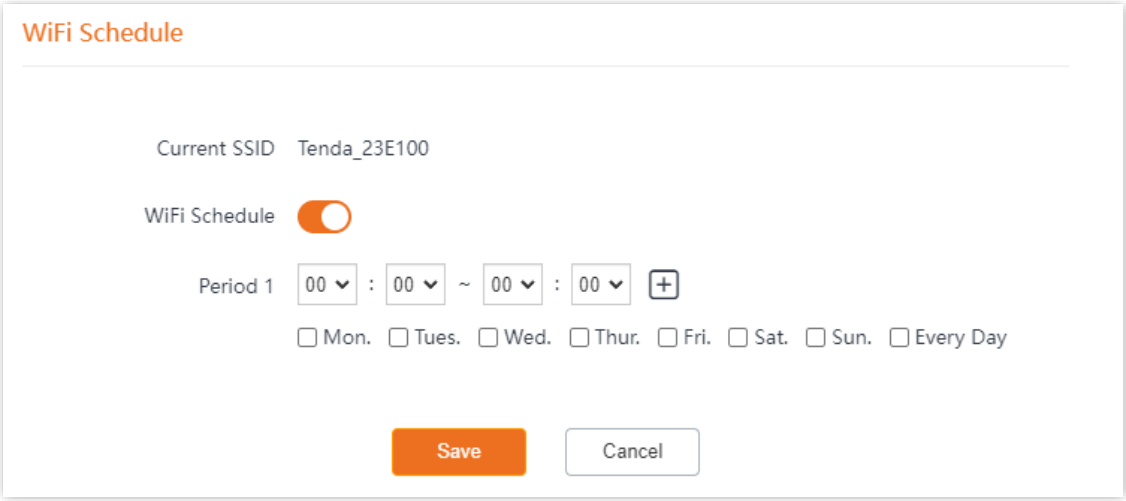
You can disable the Wi-Fi network of the AP during a specified period. During the scheduled disable period, Wi-Fi-enabled devices such as smartphones cannot search for the Wi-Fi networks.

Procedure for controlling internet usage time

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **WiFi Schedule**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Click on the row where the Wi-Fi network to be controlled resides.



5. Enable the **WiFi Schedule** function, and set the period for the Wi-Fi network to automatically disable.



6. Click **Save**.

---End

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 Wi-Fi network.
Status	Specifies the status of the Wi-Fi network, including **Enabled** or **Disabled**.
Schedule	Specifies the status of the WiFi schedule of the Wi-Fi network.
WiFi Disable Period	Specifies the period when the Wi-Fi network automatically disables.
Operation	Click to set the WiFi schedule function of the Wi-Fi network, including enabling or disabling the WiFi schedule function and setting the period for the Wi-Fi network to automatically disable.

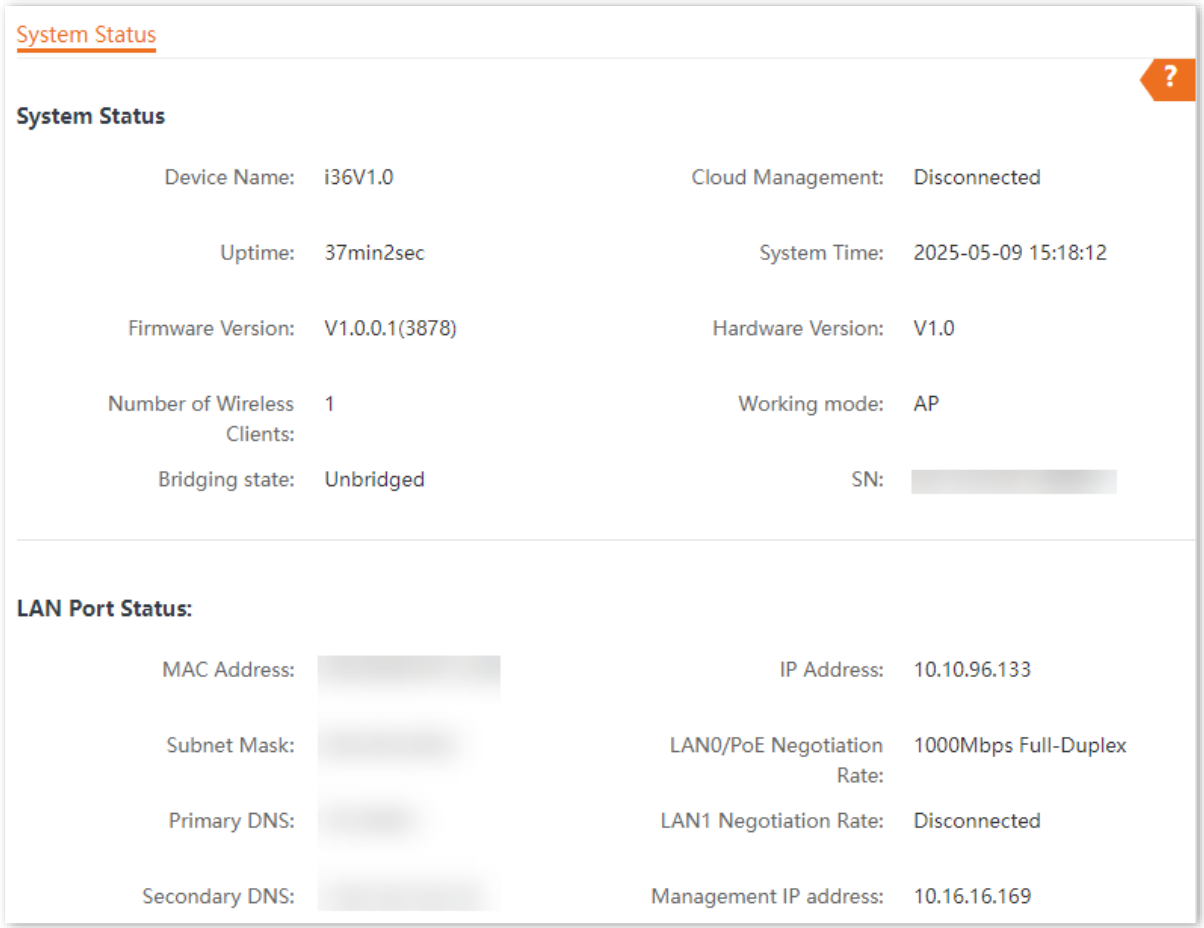
6 Maintain and monitor network

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

6.1 View system status

To access the page, log in to the web UI of the AP, and navigate to **Status** > **System Status**.

You can view the system and LAN port status of the AP. The following figure is for reference only.



Parameter description

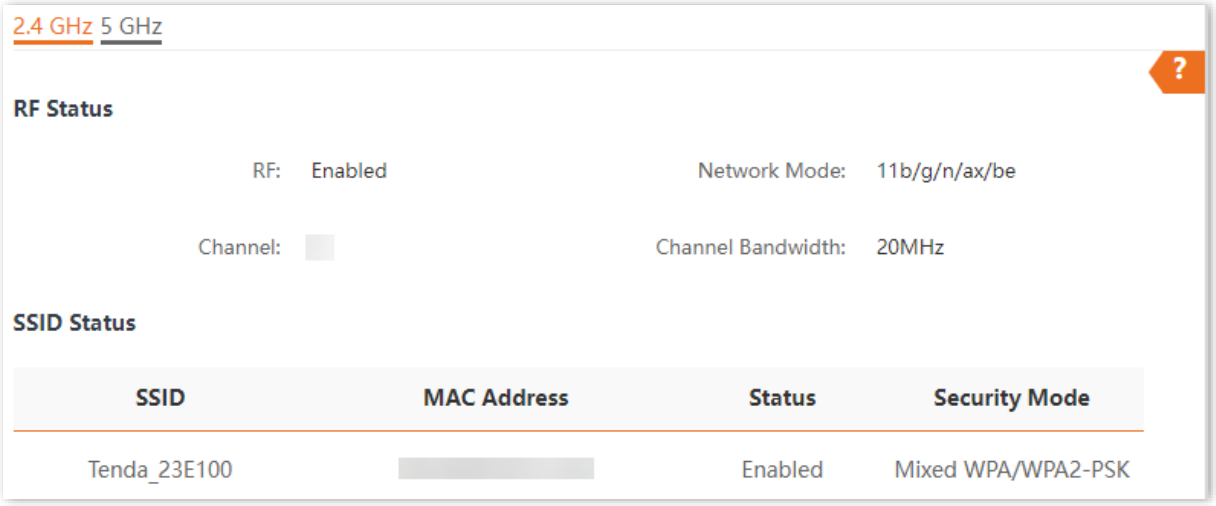
Parameter		Description
System Status	Device Name	Specifies the name of the AP. You can change the AP name on the LAN setup module. You are recommended to change the name of the AP to indicate the location of the AP (such as Hall), so that you can easily identify the AP when managing many APs.
	Cloud 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.
	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.
	Bridging SSID	Specifies the SSID of the upstream device for AP bridging. TIP This function is available on some APs. The actual product prevails.
	SN	Specifies the serial number of the AP.
LAN Port Status	MAC Address	Specifies the physical address of the LAN port of the AP.

Parameter		Description
	IP Address	Specifies the LAN IP address (internet IP address) of the AP. Users within the LAN can log in to the web UI of the AP using this IP address. This IP address is obtained from the LAN's DHCP server by default. If there is no DHCP server in the LAN where the AP is located, the default IP address will be 192.168.0.254. You can change the IP address on the LAN setup module. TIP - Before using this IP address to log in to the web UI of the AP, ensure that the IP address of the LAN user is in the same subnet as the AP's IP address. - If the QVLAN function is enabled, only users connected to the AP's management VLAN member ports can use this IP address to log in to the web UI of the AP.
	Subnet Mask	Specifies the subnet mask corresponding to the LAN port IP address 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.
	LAN0/PoE Negotiation Rate	Specifies the network rate negotiated with the peer device by the AP's PoE power input and data transmission multiplexing interface.
	LAN1 Negotiation Rate	Specifies the network rate negotiated between the AP's intranet network interface and the peer device.
	Management IP address	Specifies the management IP address of the AP. Users within the LAN can log in to the web UI of the AP using this IP address. The default IP address is 10.16.16.169. You can change the IP address on the management IP module. TIP - Before using this IP address to log in to the web UI of the AP, ensure that the IP address of the LAN user is in the same subnet as the AP's IP address. - If the QVLAN function is enabled, only users connected to the AP's management VLAN member ports can use this IP address to log in to the web UI of the AP.

6.2 View wireless status

To access the page, log in to the web UI of the AP, and navigate to **Status** > **Wireless Status**.

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.**



Parameter description

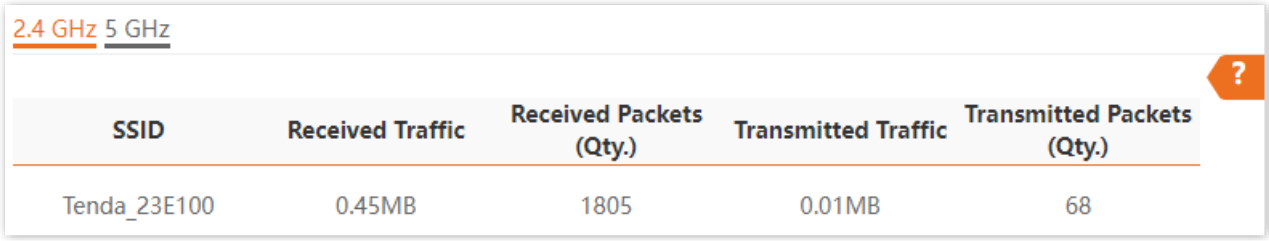
Parameter		Description
RF Status	RF	Specifies the status of the wireless function of the AP.
	Network Mode	Specifies the Wi-Fi network mode of the AP.
	Channel	Specifies the working channel of the AP.
	Channel Bandwidth	Specifies the channel bandwidth of the AP.
SSID Status	SSID	Specifies the names of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

6.3 View traffic statistics

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

You can view the packet statistics for the Wi-Fi 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**.



Parameter description

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

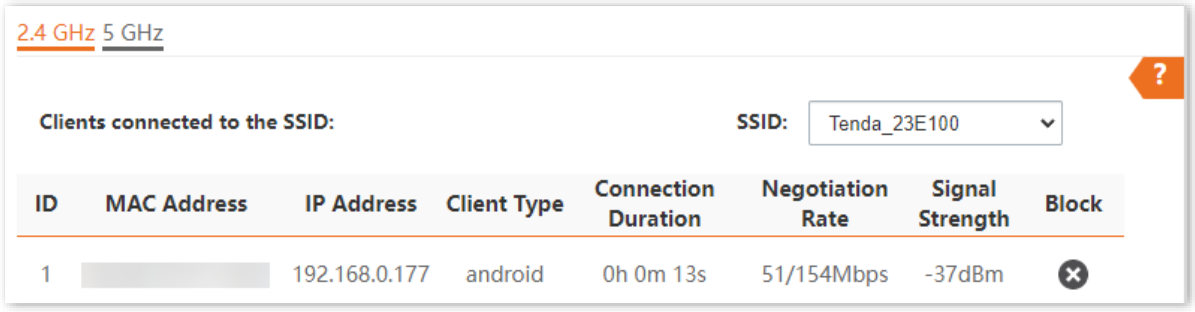
NOTE

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

6.4 View client list

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

You can view the information about the wireless clients connected to the Wi-Fi networks corresponding to the SSIDs of the AP.



By default, the page displays information about the wireless clients connected to the 2.4 GHz Wi-Fi 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 Wi-Fi network corresponding to the SSID, click the **5 GHz** tab.

Parameter description

Parameter	Description
SSID	Used to select a Wi-Fi name (SSID) from the drop-down menu to view wireless clients connected to the Wi-Fi 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 The AP can correctly identify the client's operating system type only when the AP has enabled identify client type function and the client has accessed an HTTP website.
Connection Duration	Specifies the online duration of the wireless client.
Negotiation Rate	Specifies the transmit rate and receive rate of the wireless client.
Signal Strength	Specifies the Wi-Fi signal strength of the client.

6.5 View system log

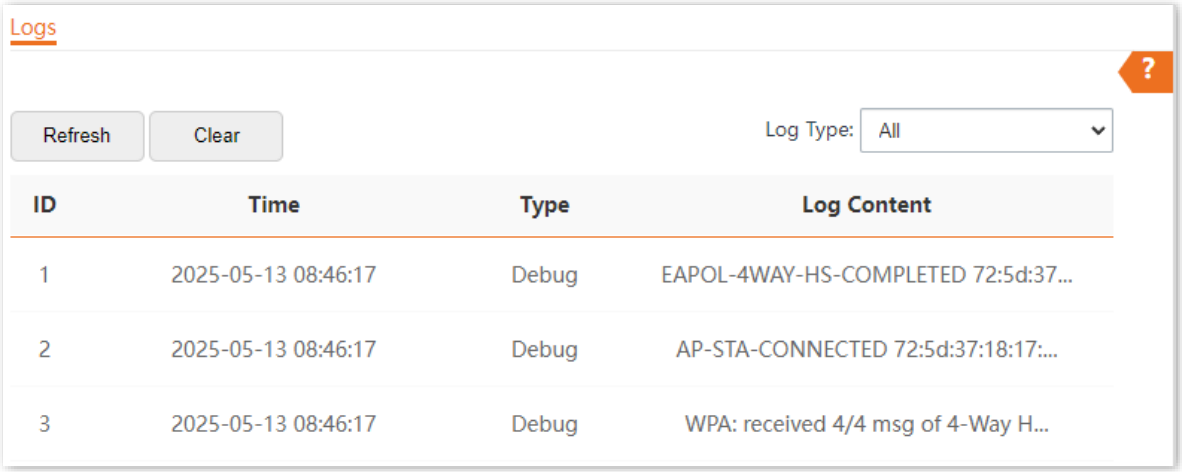
The logs of the AP record various events that occur and the operations that users perform after the AP starts. In case of a system fault, you can refer to the logs during troubleshooting.

NOTE

- 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**.
- 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 restored, or the factory settings are restored.

Procedure for viewing system log

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **System Log**.
3. (Optional) Click **Refresh** to view the latest logs of the AP, or click **Clear** to clear the existing logs of the AP.



---End

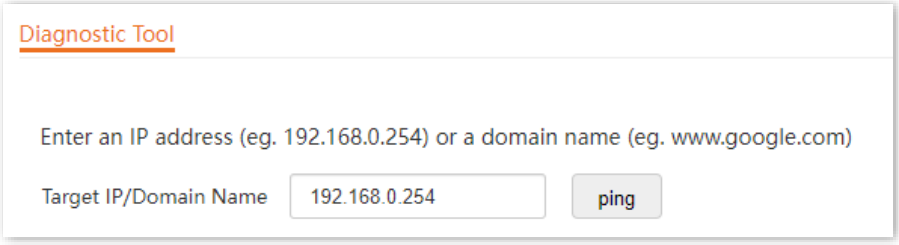
6.6 Diagnose the network

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

Procedure for diagnosing the network

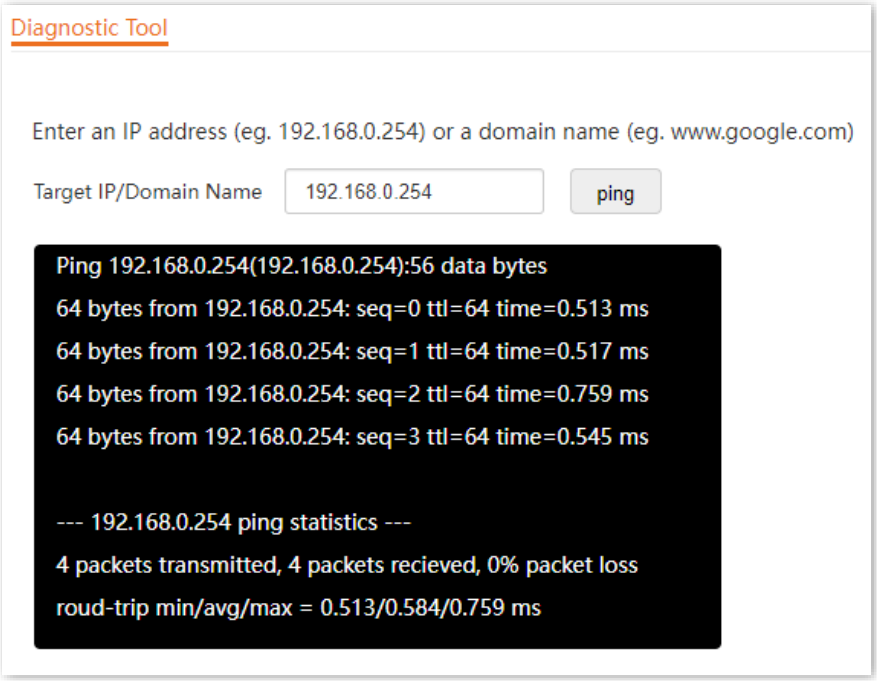
The link to **192.168.0.254** is used as an example.

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Diagnostic Tool**.
3. 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.
4. Click **ping**.



---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.

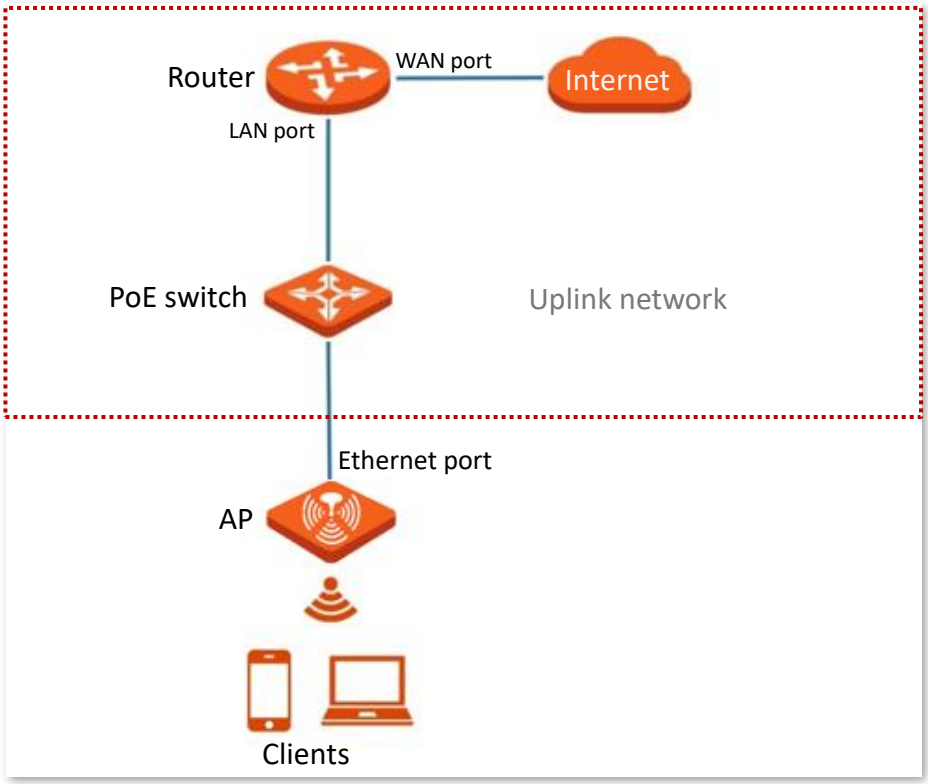


6.7 Configure uplink detection

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 Ethernet port serves as the uplink port).

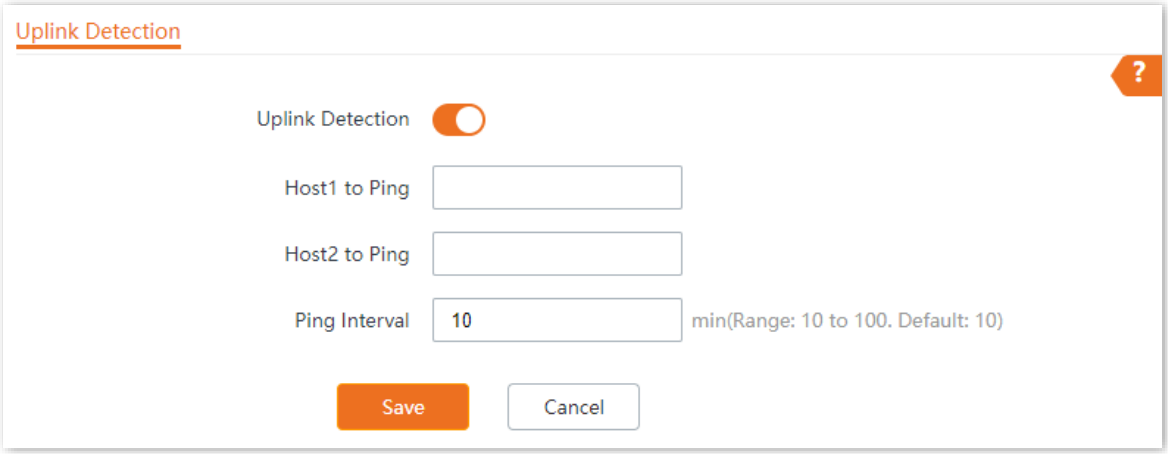


Procedure for configuring uplink detection

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Uplink Detection**.
3. Enable the **Uplink Detection** function.
4. Set **Host1 to Ping** or **Host2 to Ping** to the IP address of the host to be pinged through the Ethernet port of the AP, such as the IP address of the switch or router directly connected to the AP.

   TIP

   If there is only one destination host address, enter that address for both **Host1 to Ping** and **Host2 to Ping**.
5. Set **Ping Interval** to the interval at which the AP detects its uplink.
6. Click **Save**.



---End

Parameter description

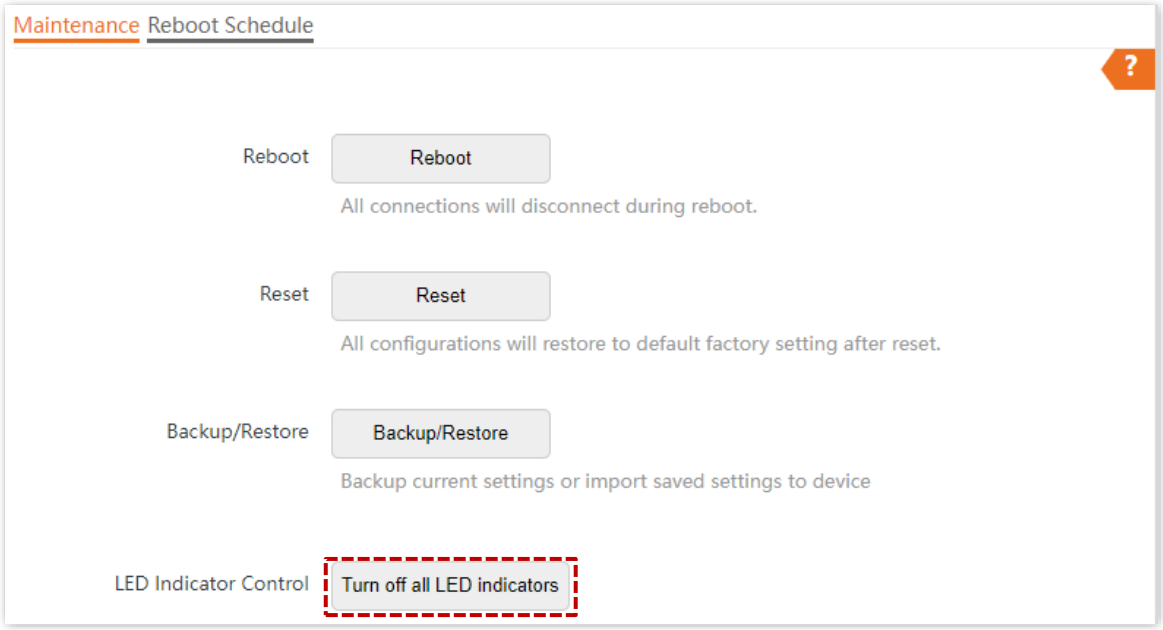
Parameter	Description
Uplink Detection	Specifies whether to enable the uplink detection function of the AP.
Host1 to Ping	Specify the IP address of the host to be pinged through the Ethernet port of the AP. It is available only when the uplink detection function is enabled.
Host2 to Ping	
Ping Interval	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**.

6.8 Control LED indicator

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

6.8.1 Turn off the LED indicator

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.
3. Click **Turn off all LED indicators**.

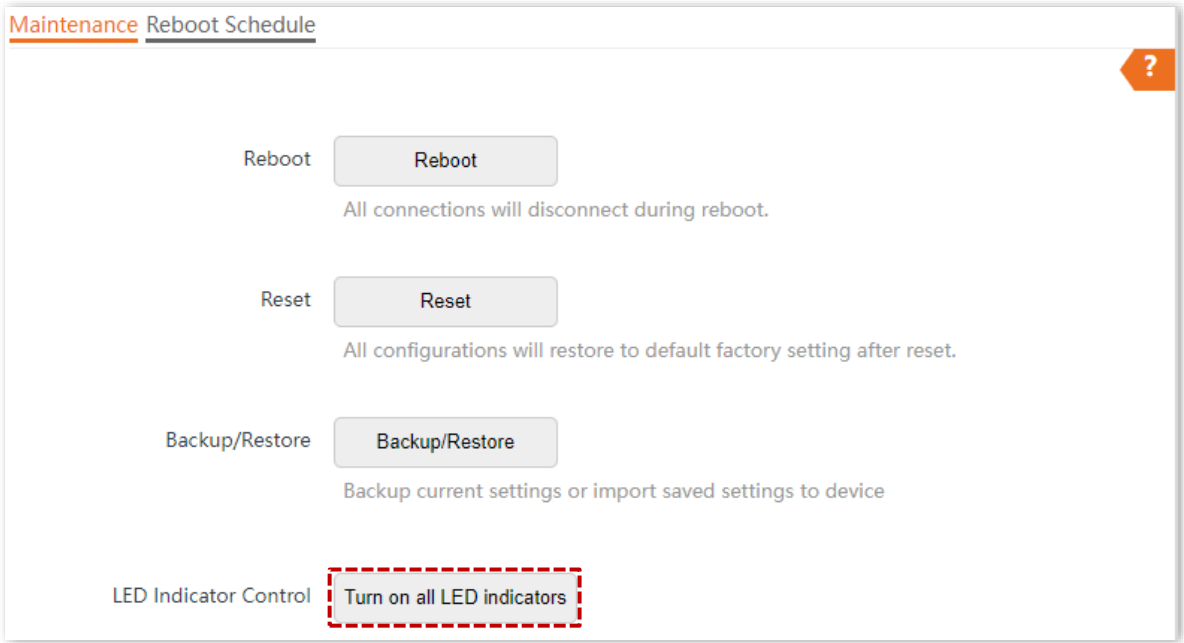


---End

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

6.8.2 Turn on the LED indicator

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.
3. 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.

6.9 Configure system time

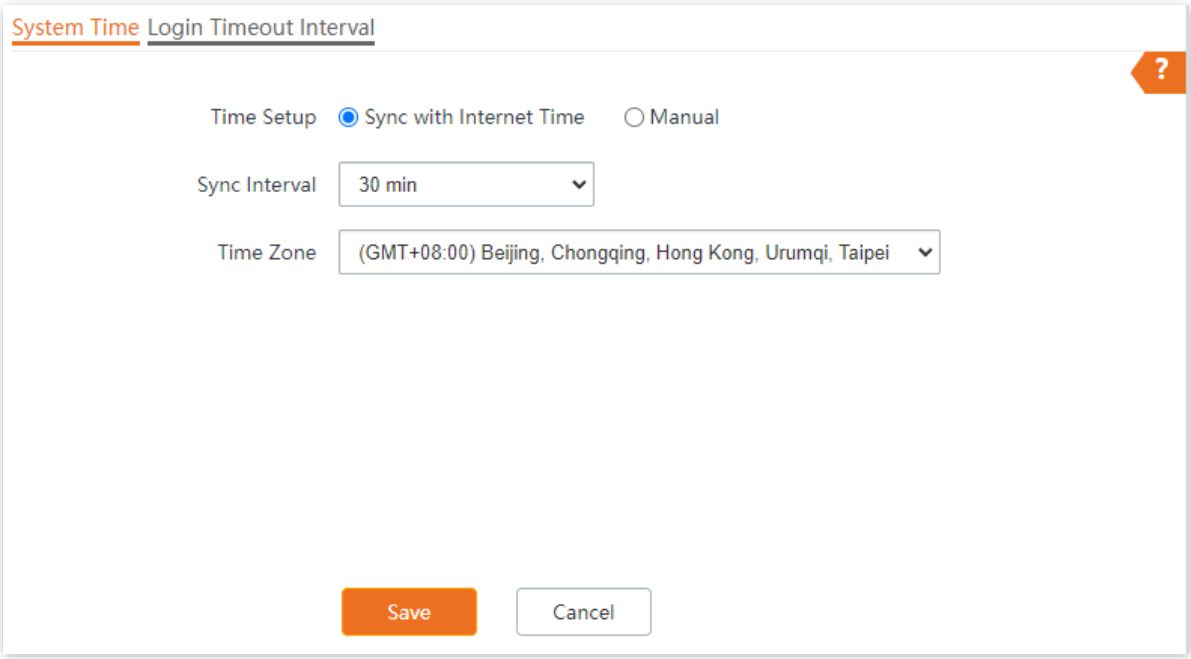
Ensure that the system time of the AP is correct, so that time-based functions can take effect properly. The AP allows you to set the system time by synchronizing the time with the internet or manually setting the time.

6.9.1 Sync the time with the internet

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.

Procedure for synchronizing the time with the internet

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Date & Time** > **System Time**.
3. Set **Time Setup** to **Sync with Internet Time**.
4. Set the interval at which the AP will automatically synchronize with a time server of the internet, which is **30 min** in this example.
5. Set the standard time zone of the region in which the AP locates.
6. Click **Save**.



---End

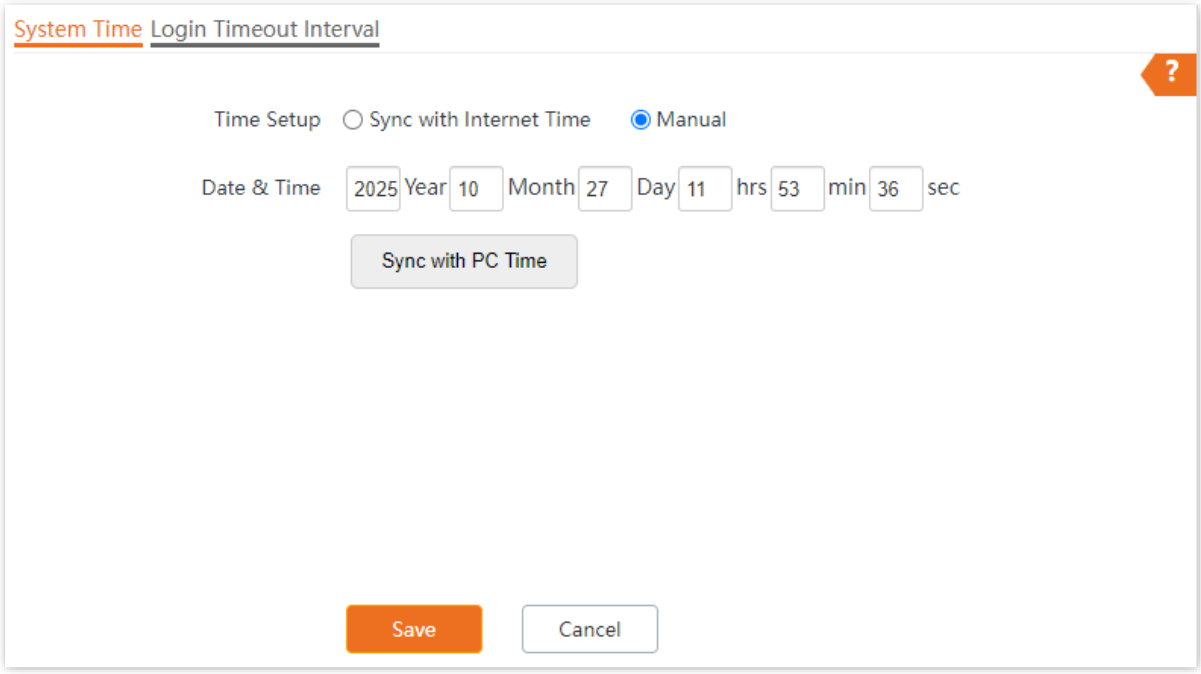
After the configuration is completed, the AP automatically synchronizes with the internet time every 30 minutes.

6.9.2 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.

Procedure for manually setting the time

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Date & Time** > **System Time**.
3. Set **Time Setup** to **Manual**.
4. Manually enter the date and time, or click **Sync with PC Time** to synchronize the system time of the AP with the system time of the management computer.
5. Click **Save**.



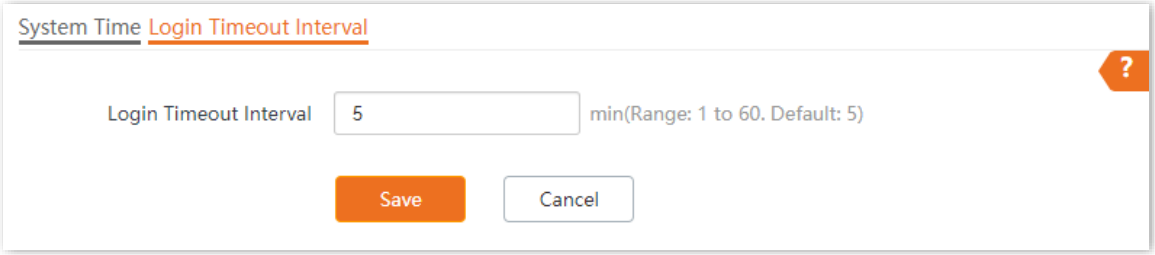
---End

6.10 Configure login timeout interval

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. The default login timeout interval is 5 minutes.

Procedure for configuring login timeout interval

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Date & Time** > **Login Timeout Interval**.
3. Set the **Login Timeout Interval** as required.
4. Click **Save**.



---End

6.11 Change login password

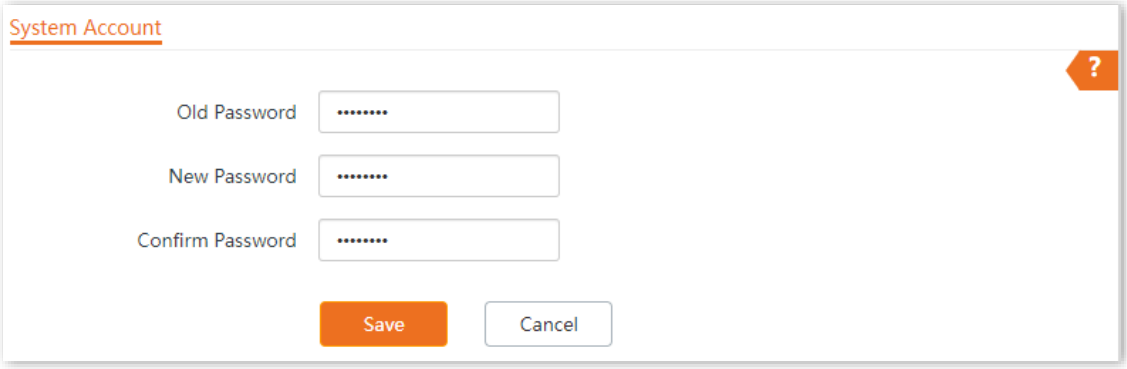
When logging in to the AP's web UI for the first time, set a login password as required to ensure security. Additionally, during AP usage, regularly change the web UI password to maintain ongoing security.

Procedure for changing login password

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **System Account**.
3. Enter the current password in **Old Password**.
4. Enter the new password in **New Password**.

   NOTE

   For initial setup or after a reset, set the new login password to ensure privacy and security. The longer the password, the higher the security. The character limit and composition rules for passwords are subject to software user interface prompts.
5. Enter again the new password in **Confirm Password**.
6. Click **Save**.



---End

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

6.12 Reboot the AP

TIP

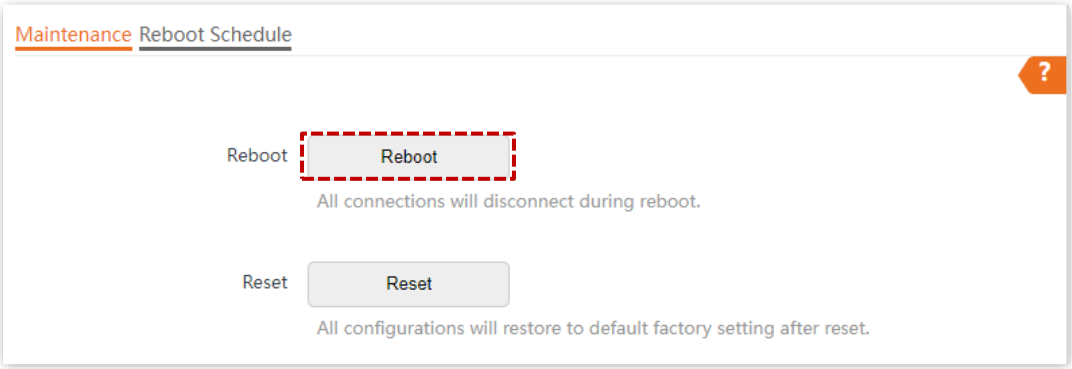
Rebooting the AP will disconnect all connections. You are recommended to reboot the AP at an idle hour.

6.12.1 Manual reboot

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

Procedure for rebooting the AP

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.
3. Click **Reboot**.



4. Confirm the prompt information, and click **OK**.

---End

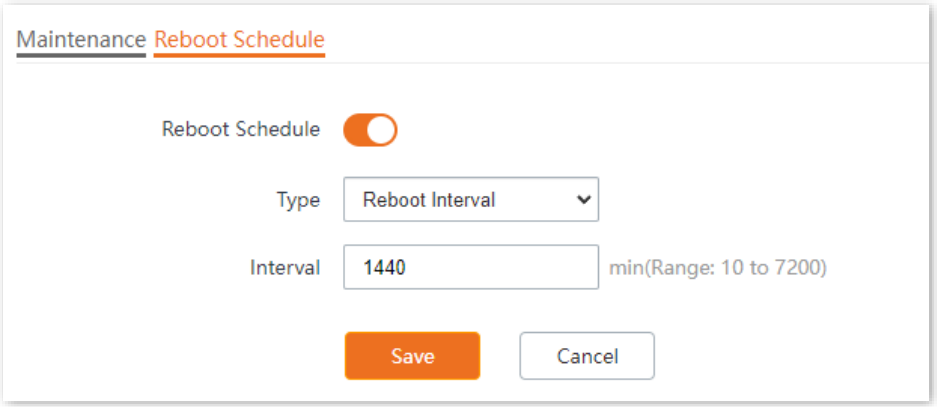
6.12.2 Reboot schedule

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

- 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

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Reboot Schedule**.
3. Enable the **Reboot Schedule** function.
4. Set **Type** to **Reboot Interval**.
5. Set **Interval** to a value in minutes, which is **1440** in this example.
6. Click **Save**.



---End

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

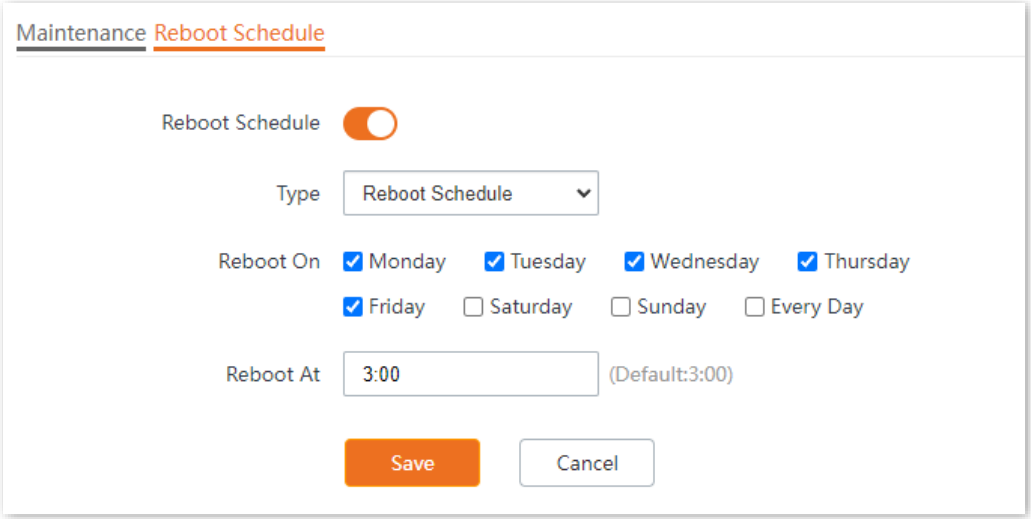
Configure the AP to reboot at specified time

TIP

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

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Reboot Schedule**.
3. Enable the **Reboot Schedule** function.

4. Set **Type** to **Reboot Schedule**.
5. Select the date when the AP reboots, which is **Monday** to **Friday** in this example.
6. Set the time when the AP reboots, which is **3:00** in this example.
7. Click **Save**.



---End

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

6.13 Backup and 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.

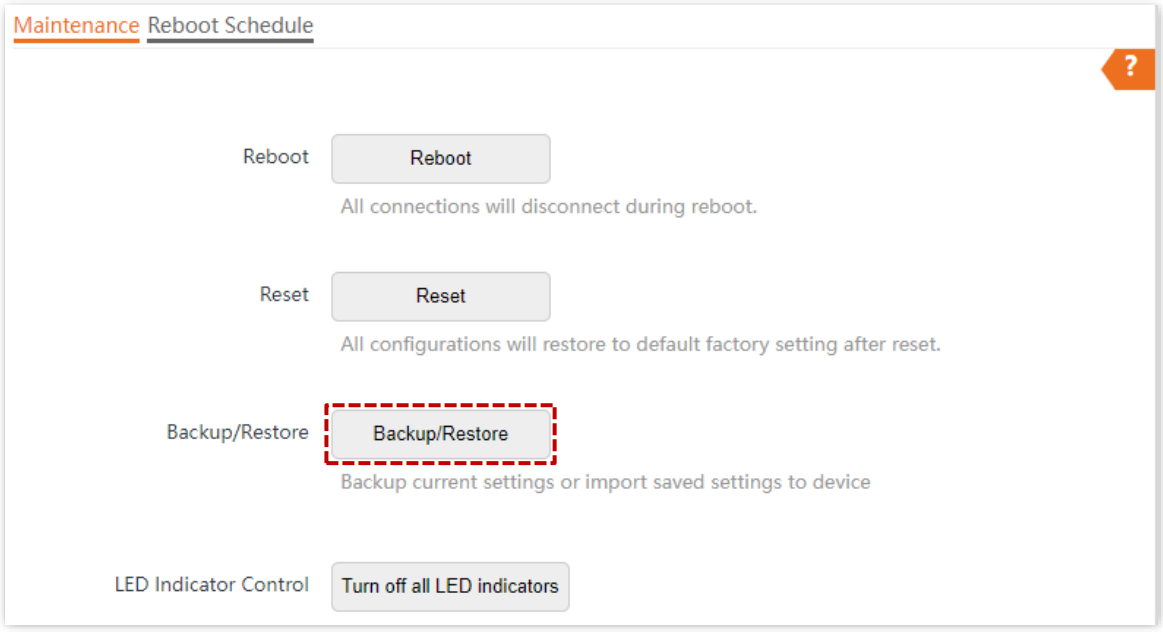
TIP

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

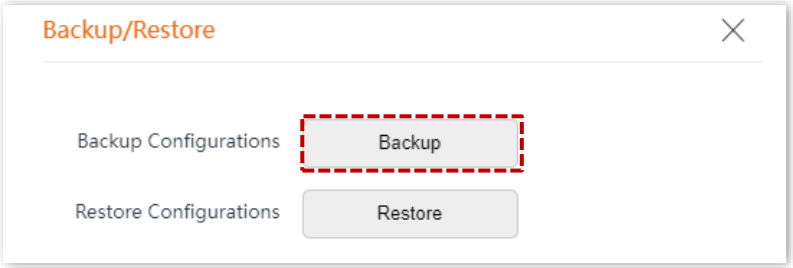
6.13.1 Back up the current configuration

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.

3. Click **Backup/Restore**.



4. Click **Backup**.



---End

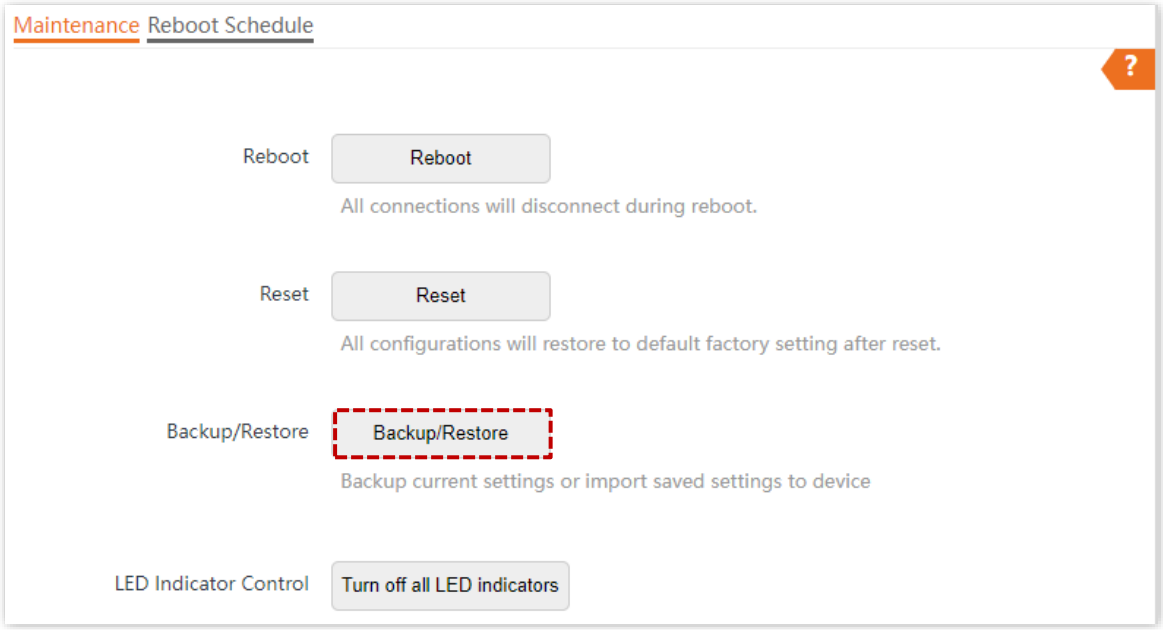
A configuration file named **APCfm.cfg** is downloaded.

TIP

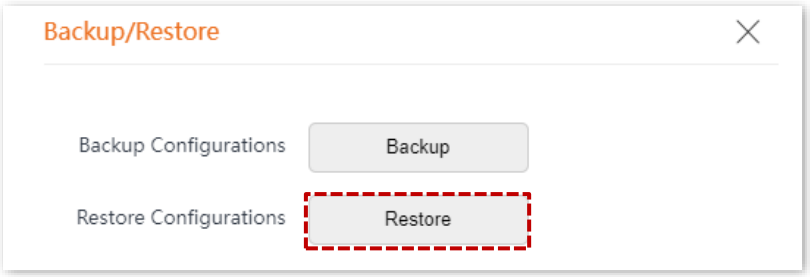
If the prompt “This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?” appears, click “Keep”.

6.13.2 Restore a configuration

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.
3. Click **Backup/Restore**.



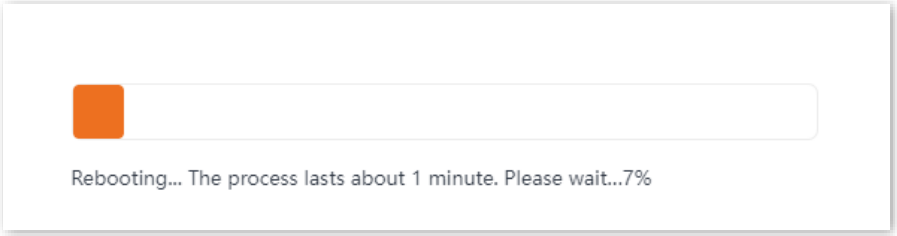
4. Click **Restore**.



5. Select and upload the configuration file (suffixed with **.cfg**) to be restored.

---End

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



6.14 Reset the AP

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

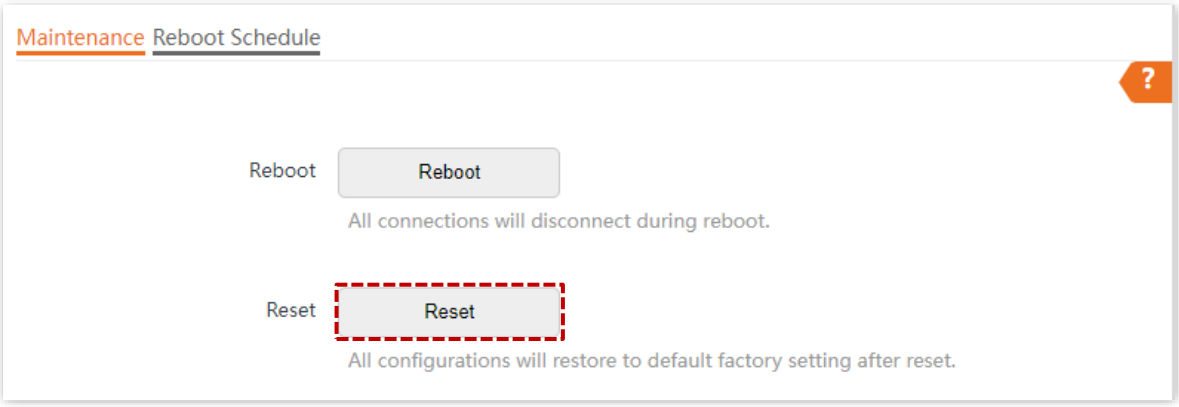
- When the factory settings are restored, your configuration will be cleared. Therefore, you need to reconfigure the AP to reconnect to the internet. Restore the factory settings of the AP only when necessary.
- You are recommended to back up the configuration before restoring the factory settings.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.

Method 1: Reset the AP using the reset button

When the AP is idle, hold the reset button (**RST, RESET**) down with a needle-like object for about 8 seconds. Wait for about 1 minute until the AP is reset successfully.

Method 2: Reset the AP on the web UI

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.
3. Click **Reset**.



4. Confirm the prompt information, and click **OK**.

---End

6.15 Upgrade system software

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

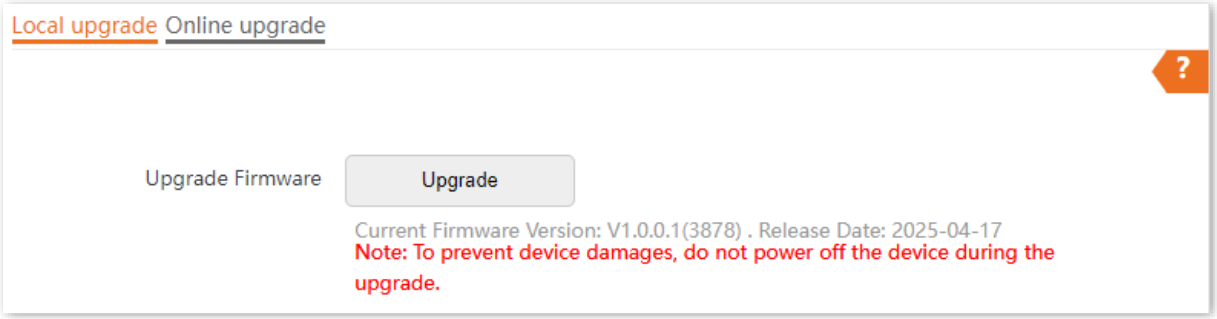
NOTE

To ensure a correct upgrade and avoid damage:

- 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.

6.15.1 Local upgrade

1. Download the package of the latest firmware version for the AP from www.tendacn.com to your local computer, and decompress the package. Generally, the package is in the format of **.bin**.
2. Log in to the web UI of the AP.
3. Navigate to **Tools** > **System Software Upgrade** > **Local upgrade**.
4. Click **Upgrade**. The following figure is for reference only.



5. Select and upload the upgrade file in the pop-up window.

---End

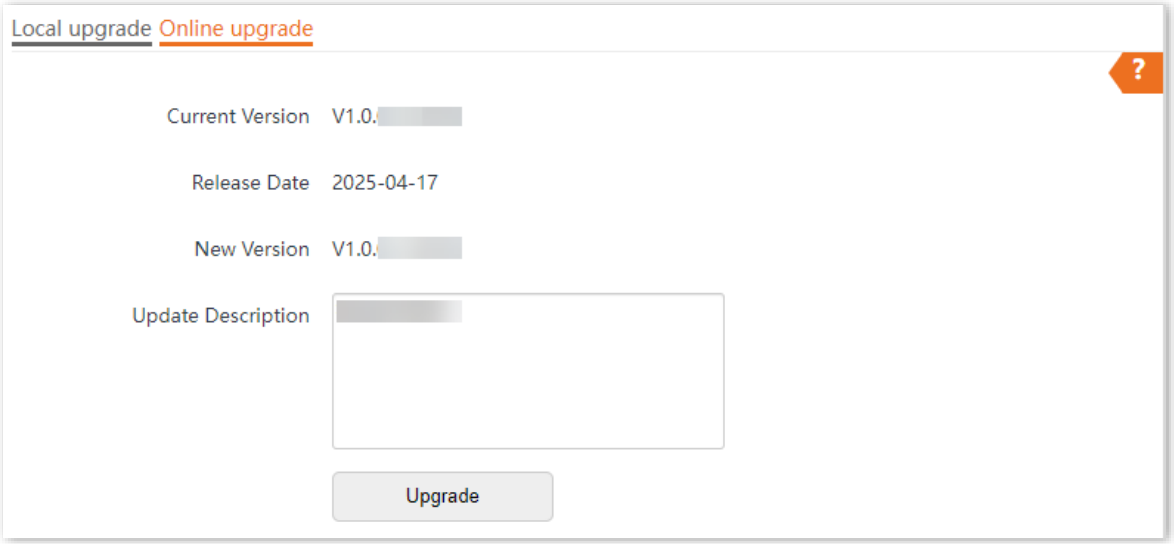
Wait until the progress bar is complete. Log in to the web UI of the AP again, navigate to **Status** > **System Status** and check whether the upgrade is successful based on **Firmware Version**.

6.15.2 Online upgrade

After the AP is connected to the internet, the system automatically detects whether there is a new upgrade firmware and displays the relevant information of the detected upgrade firmware. When a new upgrade firmware is displayed on the page, you can upgrade the AP as required.

Procedure for performing online upgrade

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **System Software Upgrade** > **Online upgrade**.
3. Wait until a new firmware version is detected. The following figure is for reference only.



4. Click **Upgrade**.

---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**.

6.16 Configure remote web management

Generally, the web UI of the AP can only be accessed on clients that are connected to the AP by a LAN port or wirelessly. The remote web management function enables access to the web UI remotely through the domain name in special cases (like when you need remote technical support).

The remote web management function is disabled by default.

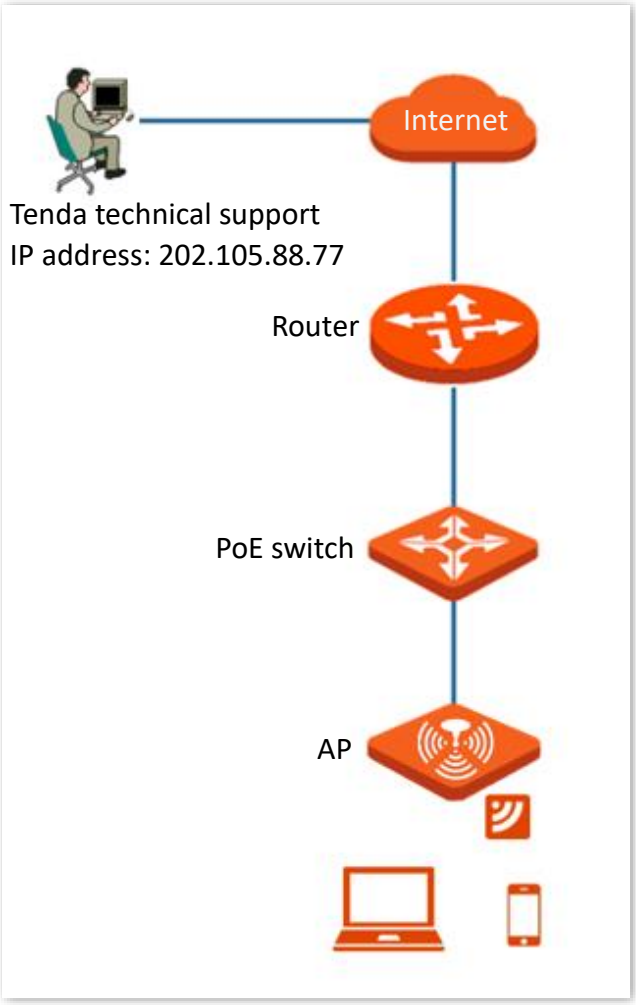
Example of configuring remote management

Networking requirements

An enterprise uses the AP to set up a network and has connected to the internet. The network administrator encountered a problem during configurations and needs the Tenda technical support to remotely log in to the web UI of the AP to perform analysis and troubleshooting.

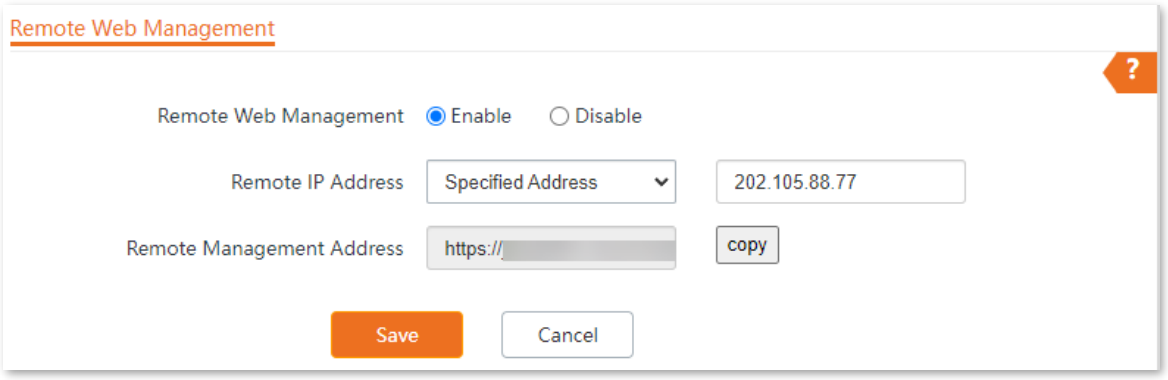
Solution

You can use the remote web management function to meet the requirements.



Procedure for configuring remote management

1. Log in to the web UI of the AP.
2. Navigate to **Advanced** > **Remote Management**.
3. Enable the **Remote Web Management** function.
4. Set **Remote IP Address** to **Specified Address.** And enter the IP address of the computer supported by Tenda technician, which is **202.105.88.77** in this example.
   - **All Addresses**: Devices with any IP address on the internet can access the web UI of the AP. For network security, this option is not recommended.
   - **Specified Address**: Only devices with specified IP addresses can access the web UI of the AP. If the device is in the local area network, the IP address (public IP address) of the gateway of the device should be filled in.
5. Click **Save**.



---End

Verification

The Tenda technical support can log in to the web UI of the AP by visiting the remote management address on the computer (IP address: 202.105.88.77).

6.17 Configure cloud maintenance

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 AP on the web UI of the Tenda CloudFi cloud platform (https://cloudfi.tendacn.com) or the Tenda CloudFi App.

Example of configuring cloud maintenance

Networking requirements

The AP can be managed through the web UI of the Tenda CloudFi cloud platform or the Tenda CloudFi App, and all of its configuration is delivered by the Tenda CloudFi cloud platform.

Procedure for configuring cloud maintenance

TIP

- Before configuring the cloud maintenance function of the AP, ensure that the internet where the AP is deployed is connected.
- Before managing the AP on the cloud, add the AP to the Tenda CloudFi App or the Tenda CloudFi Cloud (https://cloudfi.tendacn.com) first. For more details, see help document in **Help Center** of Tenda CloudFi App or Tenda CloudFi Cloud.

- **Method 1: Add the AP over Wi-Fi**

1. Get the **Tenda CloudFi** from **Google Play**, **App Store**, or via QR code.

Tenda CloudFi

2. Connect your mobile device to the Wi-Fi of the AP.

TIP

- If you have configured the AP's Wi-Fi network through the AP's web UI, the AP's Wi-Fi name and password are those you set.
- If the AP is managed by a Tenda wireless controller or router, log in to the controller or router's management page to view the AP's Wi-Fi name and password.
- If the AP is not managed by any network device, the AP's Wi-Fi network only has default Wi-Fi names **Tenda_*XXXXXX*** and **Tenda_*XXXXXX*_5G** (***XXXXXX*** is the last six digits of the MAC address on the bottom label of the AP).

3. Open the App, and tap an existing project or create a new one.
4. Tap the pop-up window that shows the AP is detected, and add it to the project.

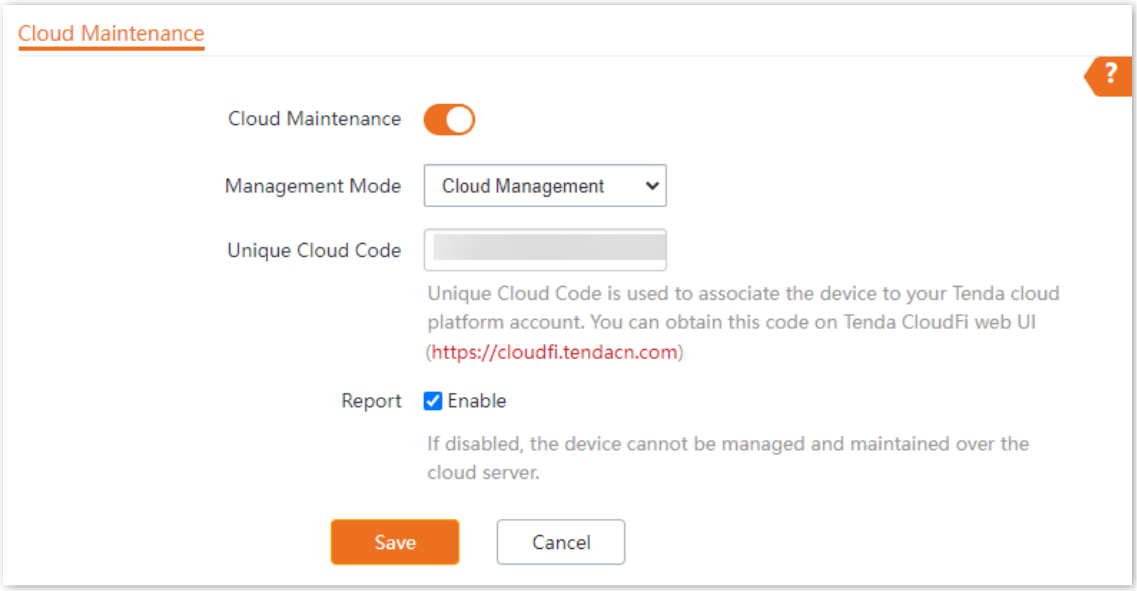
   If the pop-up window does not appear, tap + and follow the on-screen instructions.

---End

- **Method 2: Add the AP with Unique Cloud Code**

1. Get the **Unique Cloud Code** from Tenda CloudFi App or Tenda CloudFi Cloud.
2. Enable and configure the cloud maintenance function of 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** as required.
      - Paste the **Unique Cloud Code** in the input box.
      - Enable the **Report** function.
   5) Click **Save**.



3. Add the AP to the project through **Device-joining Alert** on Tenda CloudFi App or Tenda CloudFi Cloud.

---End

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) or the Tenda CloudFi App, and all of its configuration is delivered by the Tenda CloudFi cloud platform.

Parameter description

Parameter	Description
Cloud Maintenance	Specifies whether to enable the cloud maintenance function of the AP.
Management Mode	Specifies the mode under which your AP is managed. - **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 Tenda 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	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 the Tenda CloudFi App.

Parameter	Description
Report	Specifies whether to enable the report function. This function is disabled by default. 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.

7 Configure QVLAN

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

The AP supports IEEE 802.1Q VLANs and is applicable in a network environment where IEEE 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.

Example of configuring QVLAN settings

Networking requirements

A hotel has the following Wi-Fi network coverage requirements:

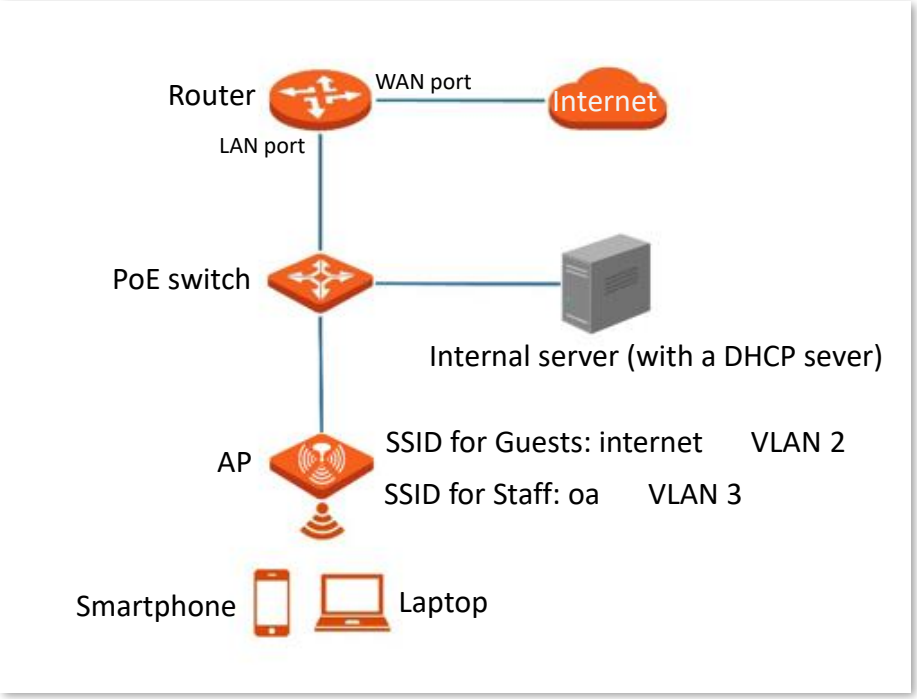
- Guests are connected to VLAN 2 and can access only the internet.
- Staff are connected to VLAN 3 and can access only the intranet.

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.

TIP

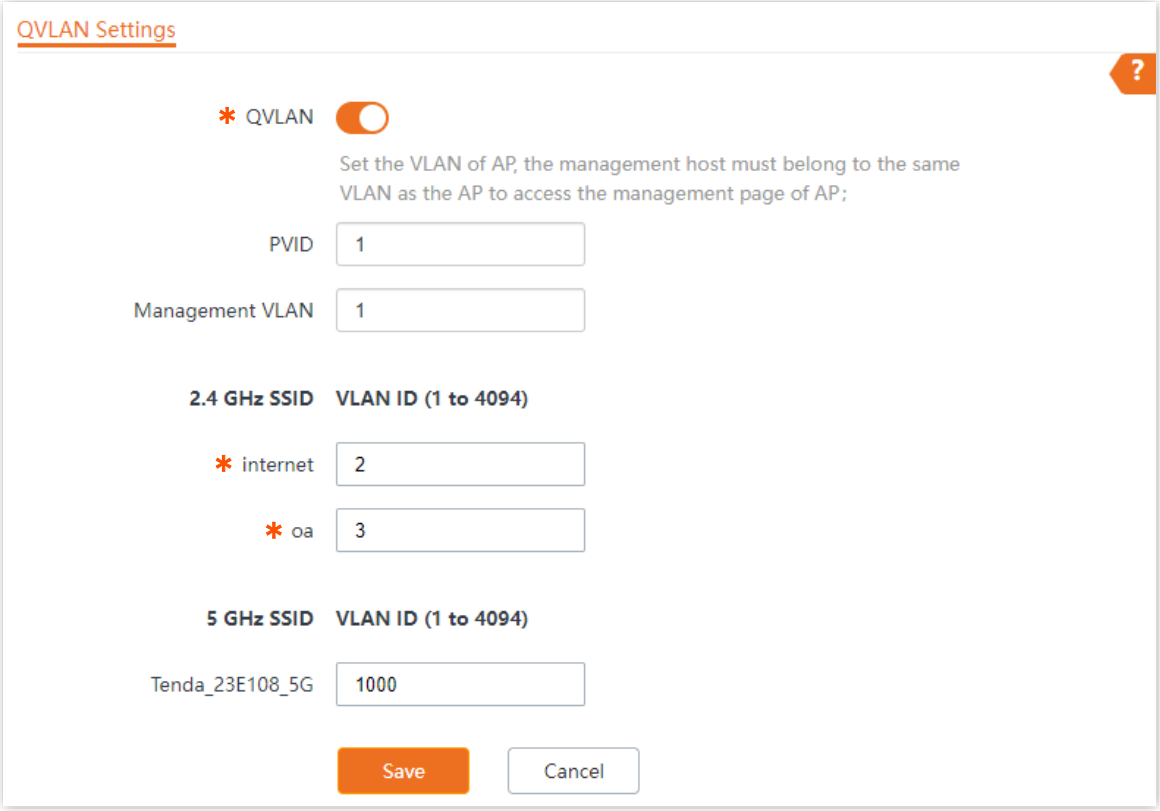
The internal server must be deployed with a DHCP server in the LAN to assign IP addresses to downlink devices.



Procedure for configuring QVLAN settings

I. Configure the AP (Example: i26 V1.0)

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **QVLAN Settings**.
3. Enable the **QVLAN** function.
4. 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.
5. Click **Save**.



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

Parameter description

Parameter	Description
QVLAN	Specifies whether to enable the 802.1Q VLAN function of the AP. By default, it is disabled.

Parameter	Description
PVID	Specifies the ID of the default native VLAN of the trunk port of the AP.
Management VLAN	Specifies the ID of the AP management VLAN. After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
Trunk Port	Used to choose the port which to be set as the trunk mode. Trunk port allows data of all VLANs to pass. NOTE When you enable the 802.1Q VLAN function, choose at least one LAN port as the trunk port. If the AP has only one Ethernet port, this port serves as the trunk port by default.
Wired LAN Port	Specifies the Ethernet port of the AP and the ID of the VLAN to which a LAN port belongs. - **LAN0**: The PoE power and data transmission multi-functional port of the AP. - **LAN1**: The data transmission port of the AP. TIP Ethernet port not set as the trunk port is seen as the access port and you can set its VLAN ID.
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 QVLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID and VLAN ID of an access port are the same.

Appendixes

A.1 Factory default settings

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

Parameter			Default Value
Login	LAN IP address		192.168.0.254 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.
	Management IP address		10.16.16.169
Quick Setup	Working Mode		AP Mode
SSID Settings	SSID	2.4 GHz	The AP allows *X* SSIDs. X may vary with APs of different models. 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. Y may vary with APs of different models. 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 Point Controller
ACK	Acknowledge Character
AES	Advanced Encryption Standard
AP	Access Point
APSD	Automatic Power Save Delivery
CTS	Clear To Send
DHCP	Dynamic Host Configuration Protocol
DTIM	Delivery Traffic Indication Map
DNS	Domain Name System
FIFO	First-in First-out
GI	Guard Interval
ID	Identity Document
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MU-MIMO	Multi-User Multiple-Input Multiple-Output
OFDMA	Orthogonal Frequency Division Multiple Access
PoE	Power over Ethernet
PSK	Pre-shared Key
PVID	Port-base VLAN ID
RF	Radio Frequency
RTS	Request To Send

Acronym or Abbreviation	Full Spelling
SAE	Simultaneous Authentication of Equals
Short GI	Short Guard Interval
SSID	Service Set Identifier
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WMF	Wireless Multicast Forwarding
WPA	Wi-Fi Protected Access