

User Guide

IP-COM WiFi App for AC1200 Enterprise Mesh WiFi System

Copyright Statement

©2018 IP-COM Networks Co., Ltd. All rights reserved.

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

Disclaimer

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

Preface

Thank you for choosing IP-COM! Please read this user guide before you start with AC1200 Enterprise Mesh WiFi System.

Conventions

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

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

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

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

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
ISP	Internet Service Provider
Mesh node(s)	AC1200 Enterprise Mesh WiFi System node(s)

Additional Information

For more information, search this product model on our website at <http://www.ip-com.com.cn>

Technical Support

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



+86-755-27653089



info@ip-com.com.cn



<http://www.ip-com.com.cn>

Contents

1 Registering and Binding	1
2 Management Type.....	6
Local Management	6
Remote Management.....	6
3 My WiFi	7
4 My Profile.....	12
5 Wireless Settings	13
6 Guest Network	14
7 Access Control	15
8 Internet Settings.....	18
Setting up PPPoE.....	19
Setting up DHCP.....	21
Setting up Static IP Address	22
Setting up Bridge	23
Setting up PPPoE Russia	24
Setting up PPTP/PPTP Russia	26
Setting up L2TP/L2TP Russia	28
9 QoS.....	30
10 Add Mesh Device.....	31
11 Fast Roaming	33
12 Capacity-oriented Mode	34

13 Captive Portal	35
Adding authentication-free clients.....	36
Setting up the account authentication rule.....	37
Setting up the one-key authentication rule.....	46
Setting up the SMS authentication rule	49
14 Smart Assistant.....	57
15 Port Forwarding.....	58
16 UPnP	60
17 DHCP Server	61
18 DNS	62
19 Static Route	63
20 Firmware Upgrade	67
21 Maintenance Schedule	69
22 Account Authorization	70

1 Registering and Binding

Binding an IP-COM account to your mesh network helps you secure your mesh network and manage it remotely.

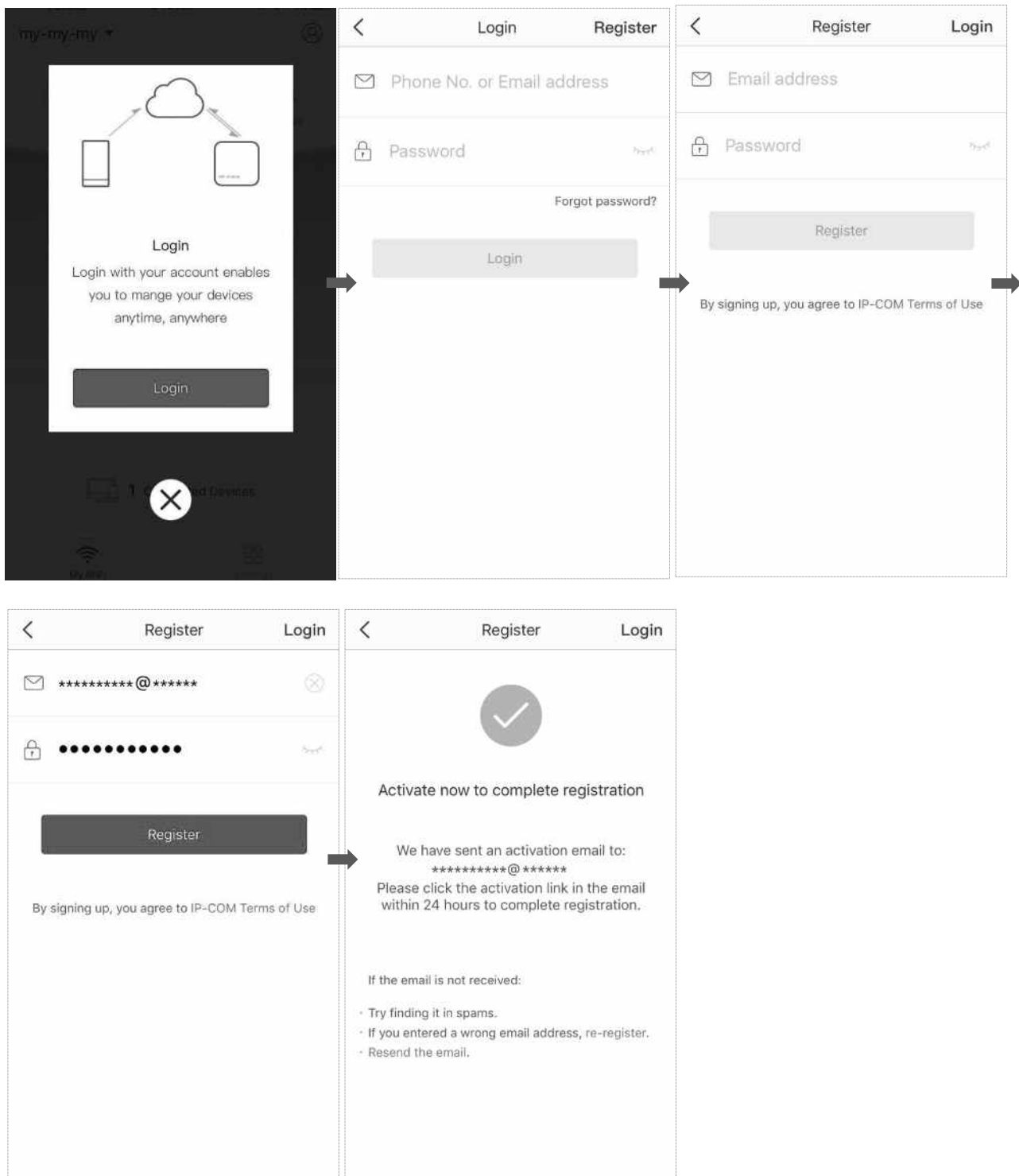
To Register an IP-COM account

Option 1

After you complete installation and setup using the IP-COM WiFi App at the first time, a login prompt page appears.

1. Tap **Login** to enter the login page.
2. Tap **Register** on the upper-right corner.
3. Enter a valid email address.
4. Customize a password for your IP-COM account.
5. Tap **Register**.

A confirmation email will be sent to your email inbox. Check your email and follow the instruction to activate your account. After successful activation, your IP-COM account is registered successfully.



Option 2

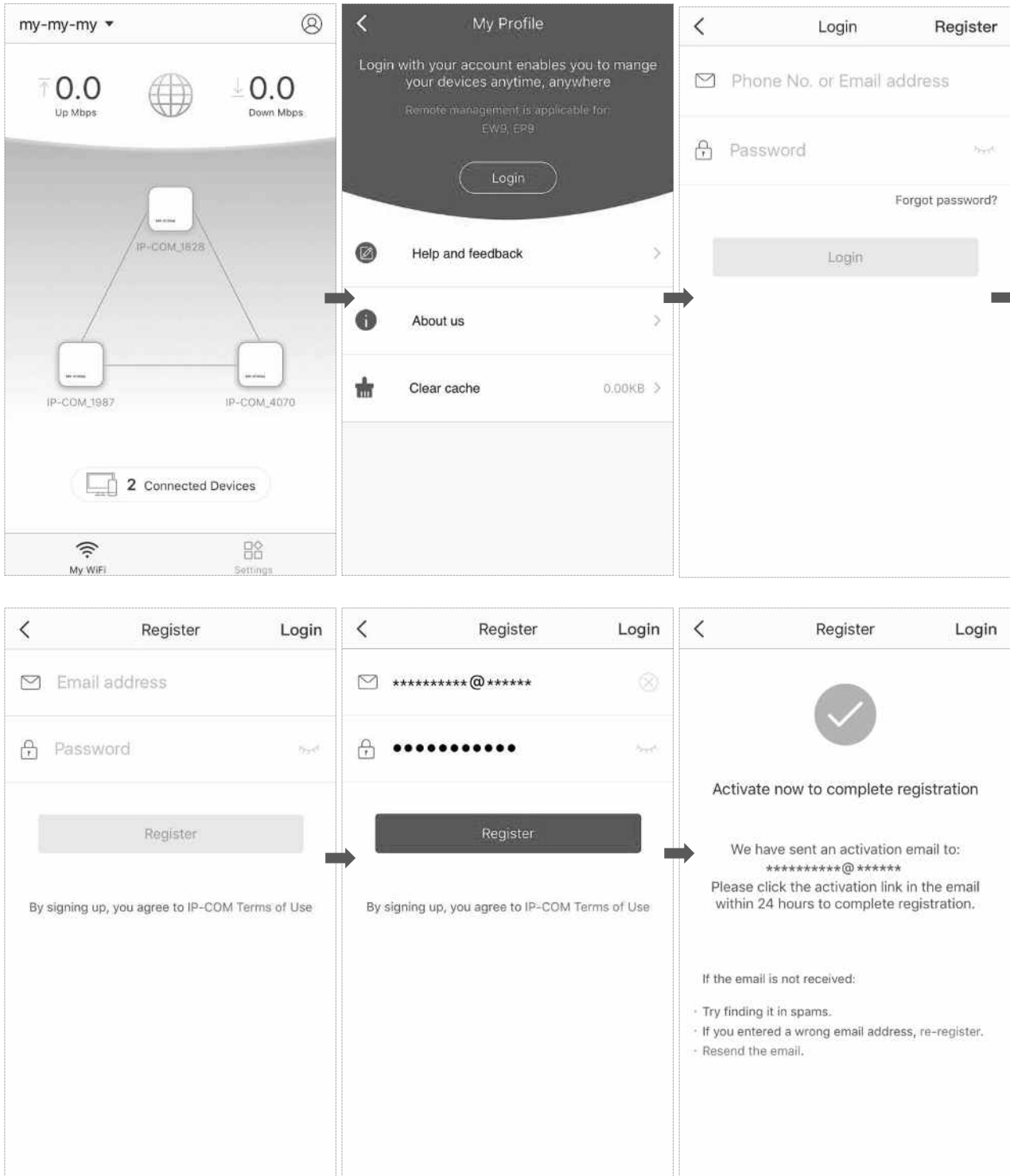
If you miss the Login prompt page, follow the steps below:

1. Run the IP-COM WiFi App, and tap  on the upper-right corner.
2. Tap **Login**.
3. Tap **Register** on the upper-right corner.
4. Enter a valid email address.

5. Customize a password for your IP-COM account.

6. Tap **Register**.

A confirmation email will be sent to your email inbox. Check your email and follow the instruction to activate your account. After successful activation, your IP-COM account is registered successfully.

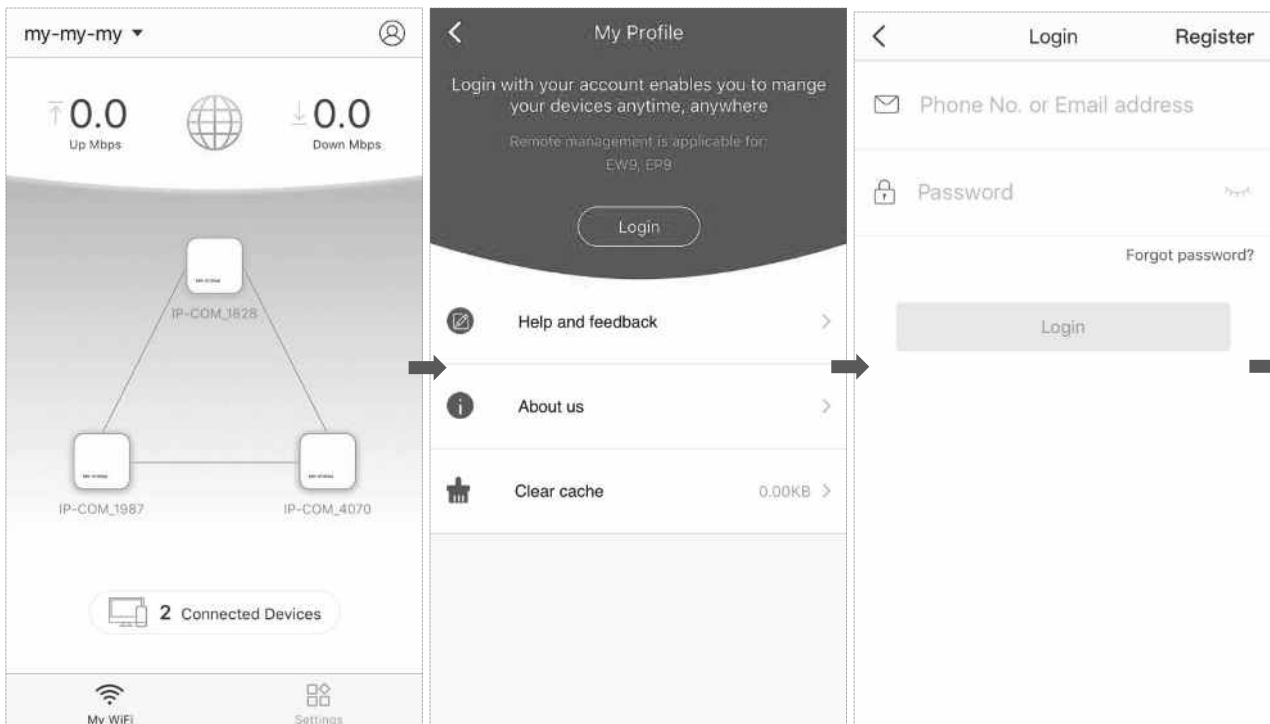


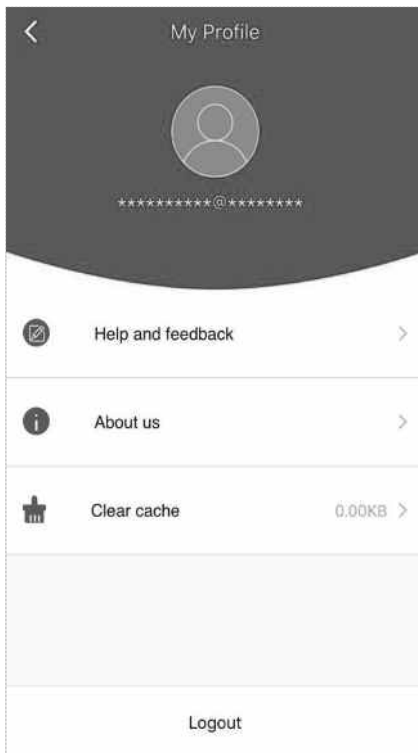
To log in to the IP-COM WiFi App



The account you use to log in to the IP-COM WiFi App at the first time is bound to your mesh network automatically, and it is your administrator account.

1. Connect your smart phone to your mesh WiFi network, and run the IP-COM WiFi App.
2. Tap  on the upper-right corner.
3. Tap **Login**.
4. Enter your registered IP-COM account.
5. Enter the password.
6. Tap **Login**.





Note

After your mesh network is bound to an account, login with the account or authorized accounts is required for network management.

2 Management Type

All IP-COM AC1200 Enterprise Mesh WiFi Systems support the IP-COM WiFi App for local and remote management. You can choose either of them as needed.

Local Management

Local management indicates that you can use the IP-COM WiFi App to manage your mesh network after connecting your smart phone to the mesh network.

Configure procedure:

1. Connect your smart phone to the WiFi network of your mesh nodes.
2. Run the IP-COM WiFi App on the smart phone, and then you can use the App to manage your mesh network.



If your mesh nodes are bound to an IP-COM account, you can manage them only after login with the bound account or other accounts authorized by the account.

Remote Management

Remote management indicates that you can use the IP-COM WiFi App to manage your mesh network anytime, anywhere.

Prerequisites:

Your mesh nodes have connected to the internet successfully.

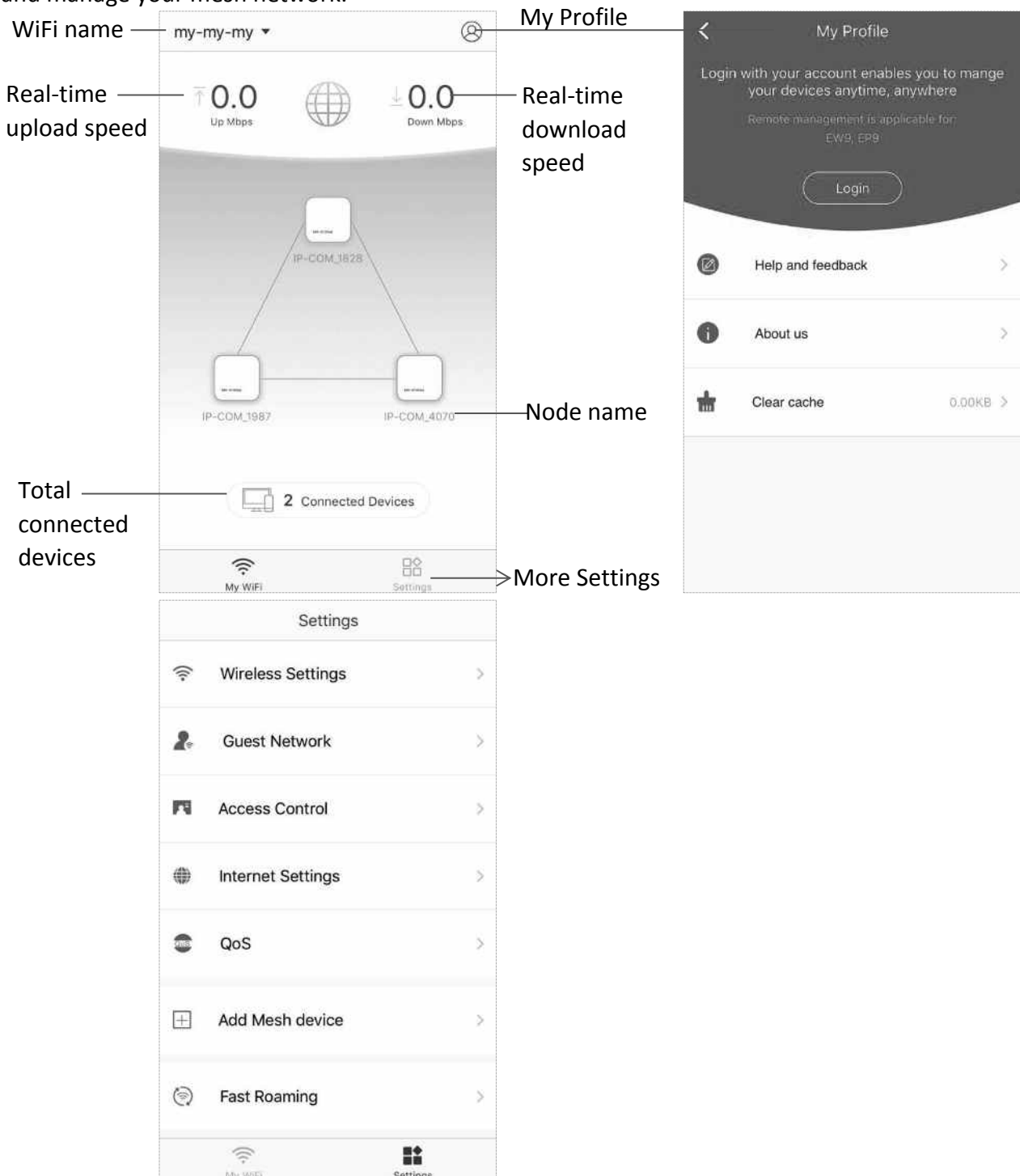
Log in with the bound or authorized account.



- A mesh network can only be bound to an account.
 - If you want to use other accounts to manage your mesh network, you can authorize these accounts after login with the administrator account.
 - Only the administrator account can authorize other accounts to manage the mesh network.
-

3 My WiFi

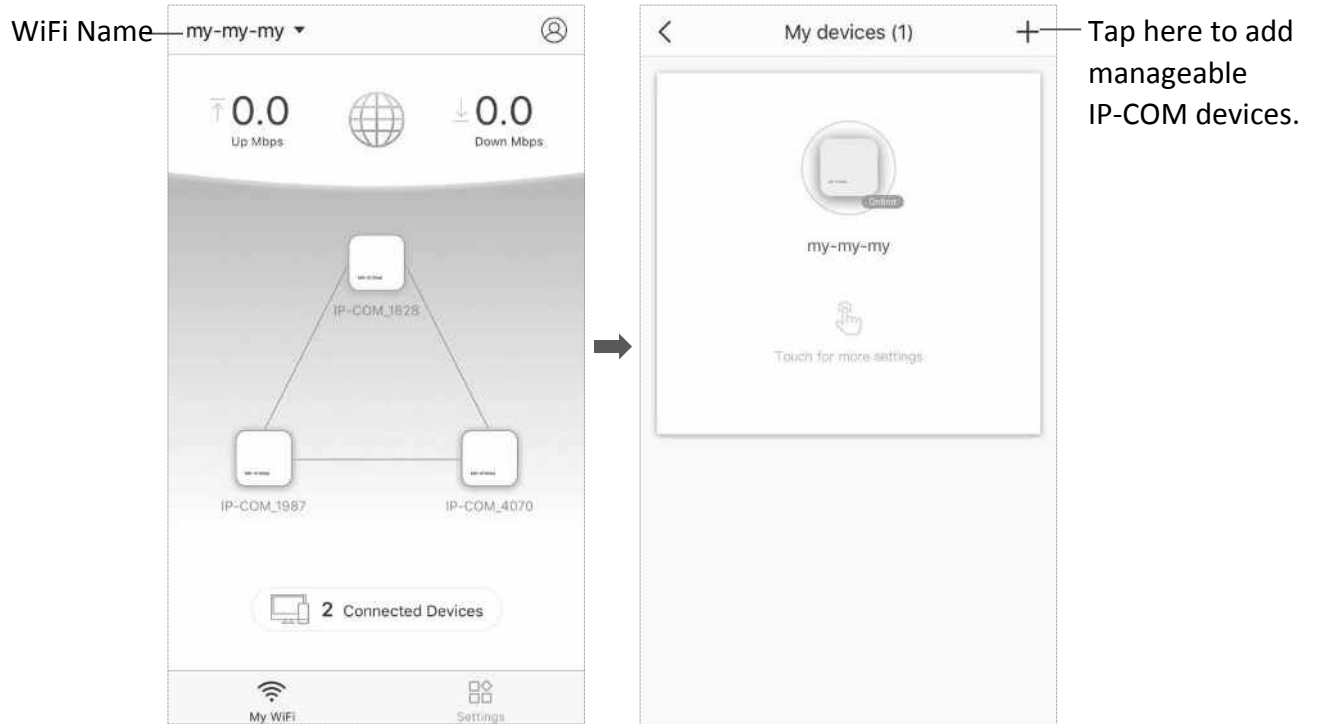
After completing the internet settings, the IP-COM WiFi App shows you the following page. You can view the status of your mesh nodes, real-time upload/download speed and connected devices, and manage your mesh network.



To check or manage your mesh nodes

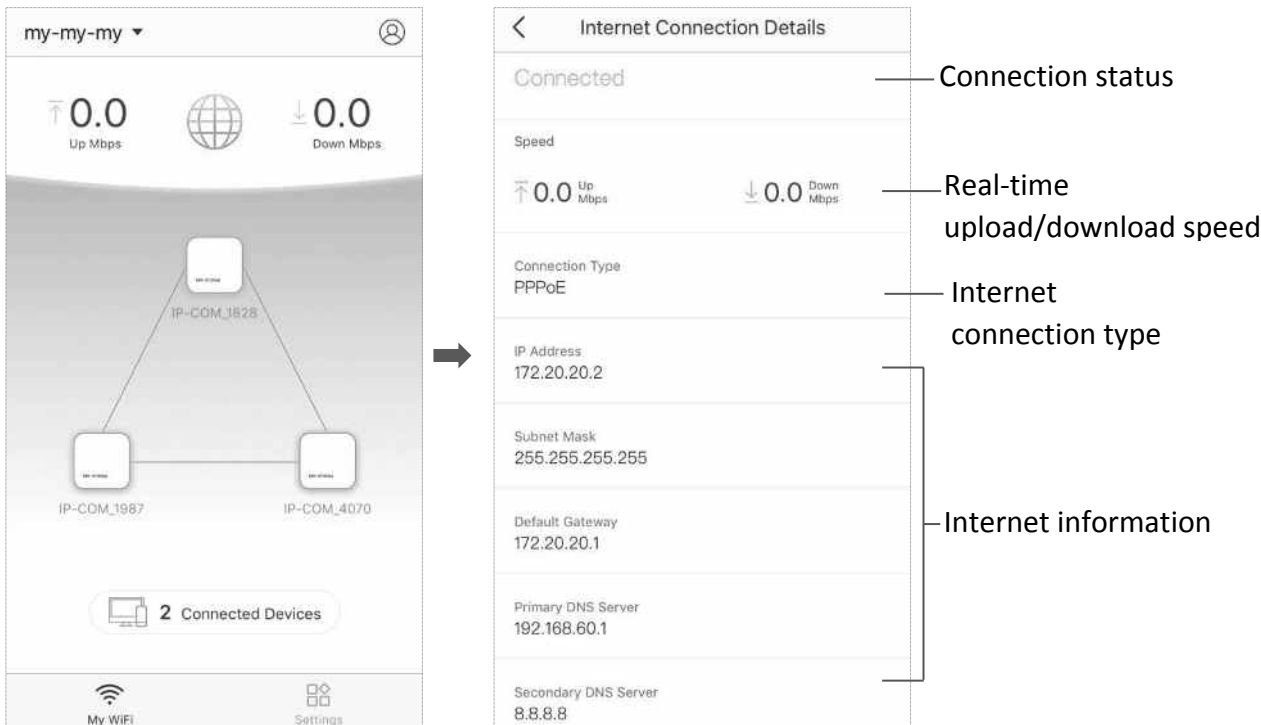
Tap the WiFi name, which is **my-my-my** in the following picture, on the **upper-left** corner of the **My WiFi** page to enter the following page.

All mesh nodes in a network share the same WiFi name.



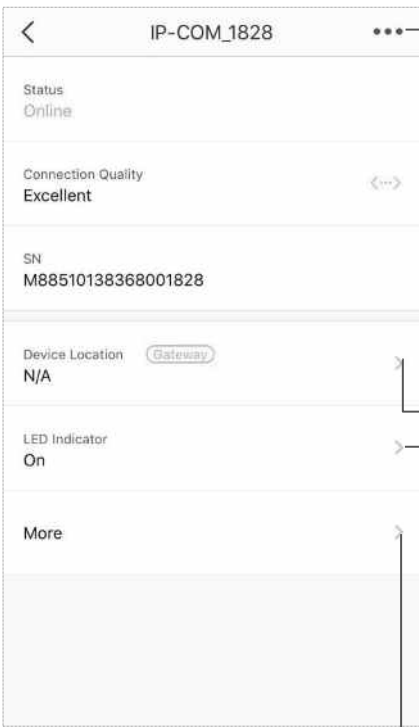
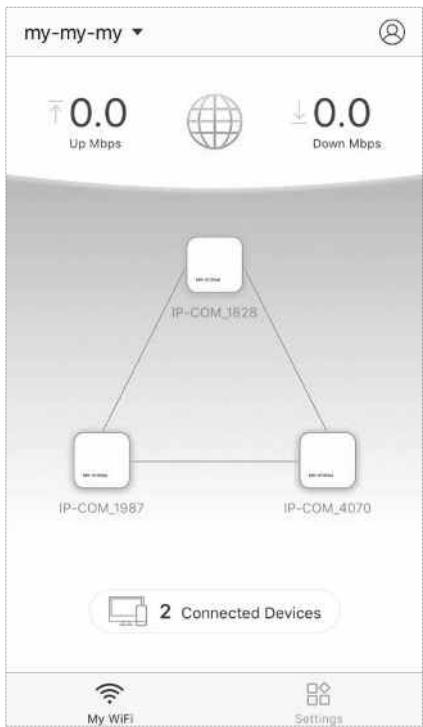
To view details of the internet settings

Tap the  icon on the home page (**My WiFi**) of the App.



To view details of the nodes

Tap the  icon on the home page (**My WiFi**) of the App to see details of the corresponding mesh node.



Choose this to delete the node from your WiFi network.

Choose this to change the location information of the node for convenient management.

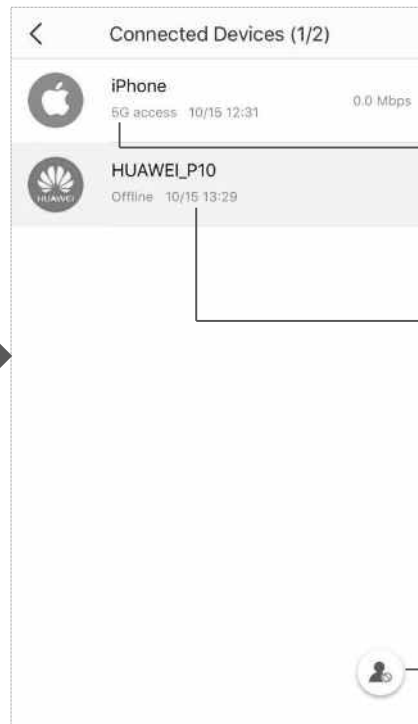
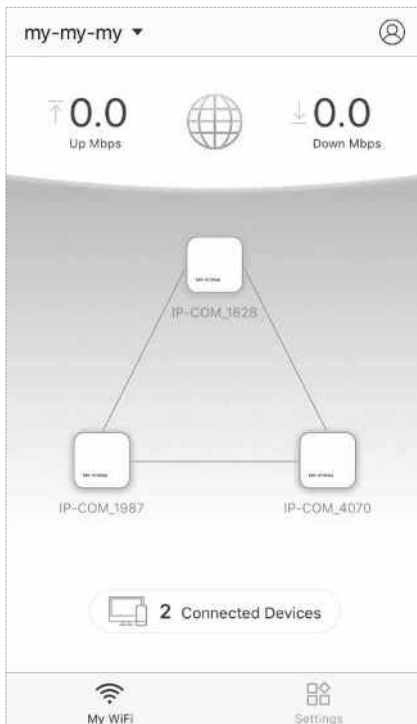
Choose this to enable/disable the LED indicator of the node.



Choose this to see more information about the mesh node.

To view the connected devices

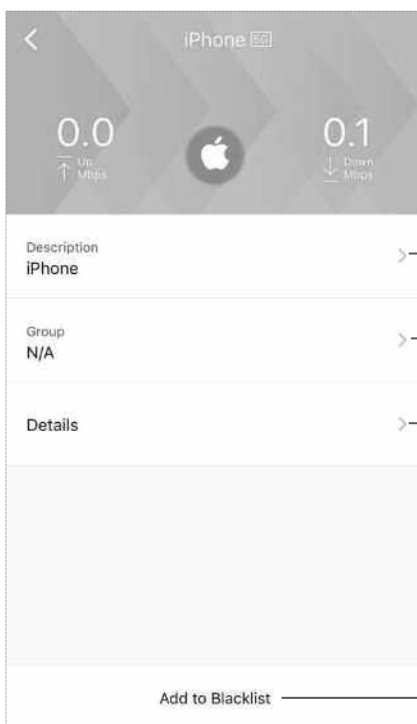
Tap the  icon on the home page (**My WiFi**) of the App. If you want to check the details of a device or manage more closely, choose the device.



This indicates the frequency band of the WiFi network the device connects.

This indicates the time the device connects to the WiFi network.

Tap this to remove connected devices from the blacklist.



Choose this to rename the device, such as Jack's iPhone.

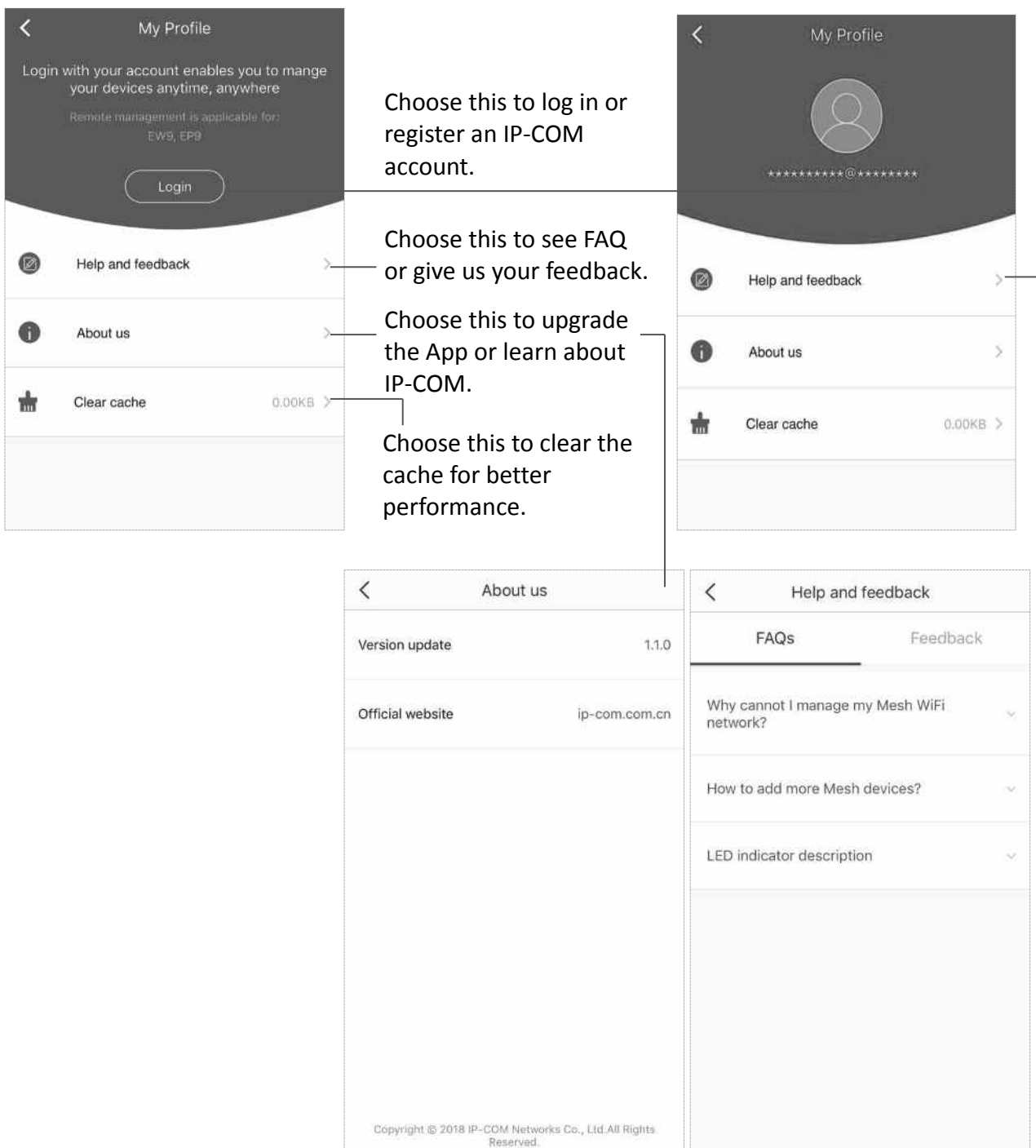
Choose this to create a group or add the connected device to a group for the access control function.

Choose this to check the details of the connected device.

Choose this to block the device. The devices in the blacklist cannot access the internet via the mesh network.

4 My Profile

Tap the  icon in the upper-right corner of the home page (**My WiFi**) for logging in or registering.



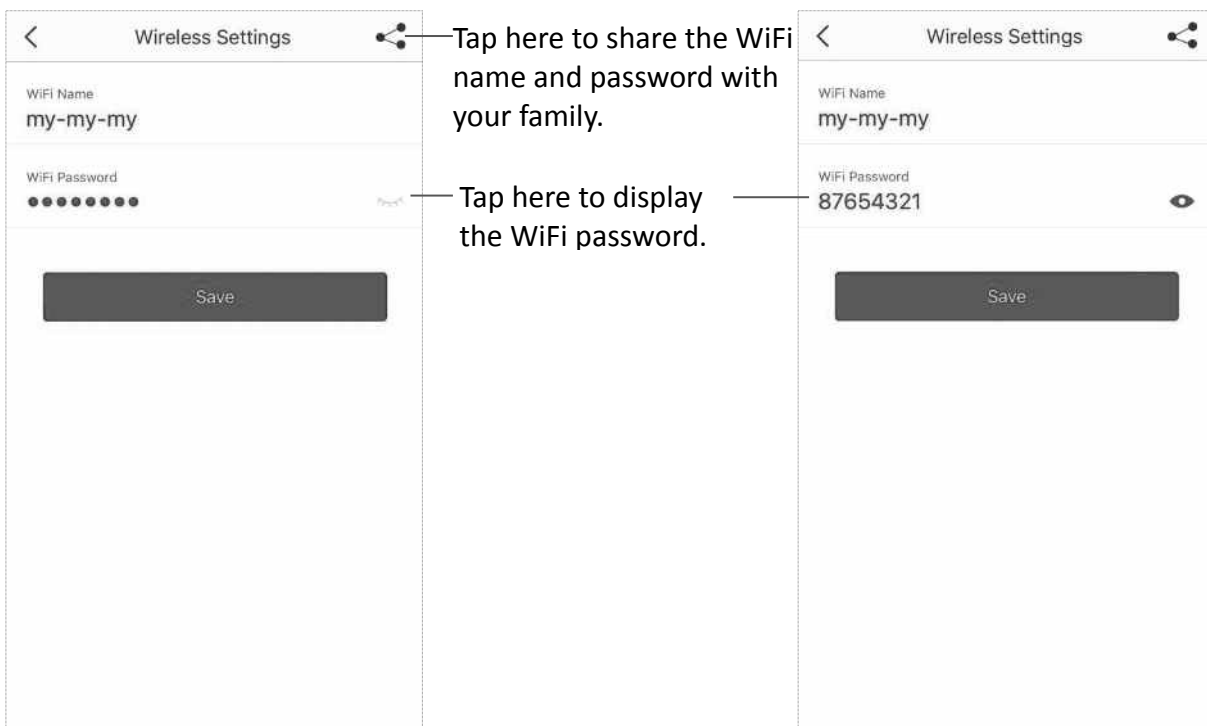
5 Wireless Settings



In this section, you can change the WiFi name and password of your mesh WiFi network.

Perform the following procedure to change your WiFi name and password:

1. Choose **Settings** > **Wireless Settings** to enter the configuration page.
2. Change the WiFi name and password as required.
3. Tap **Save**.



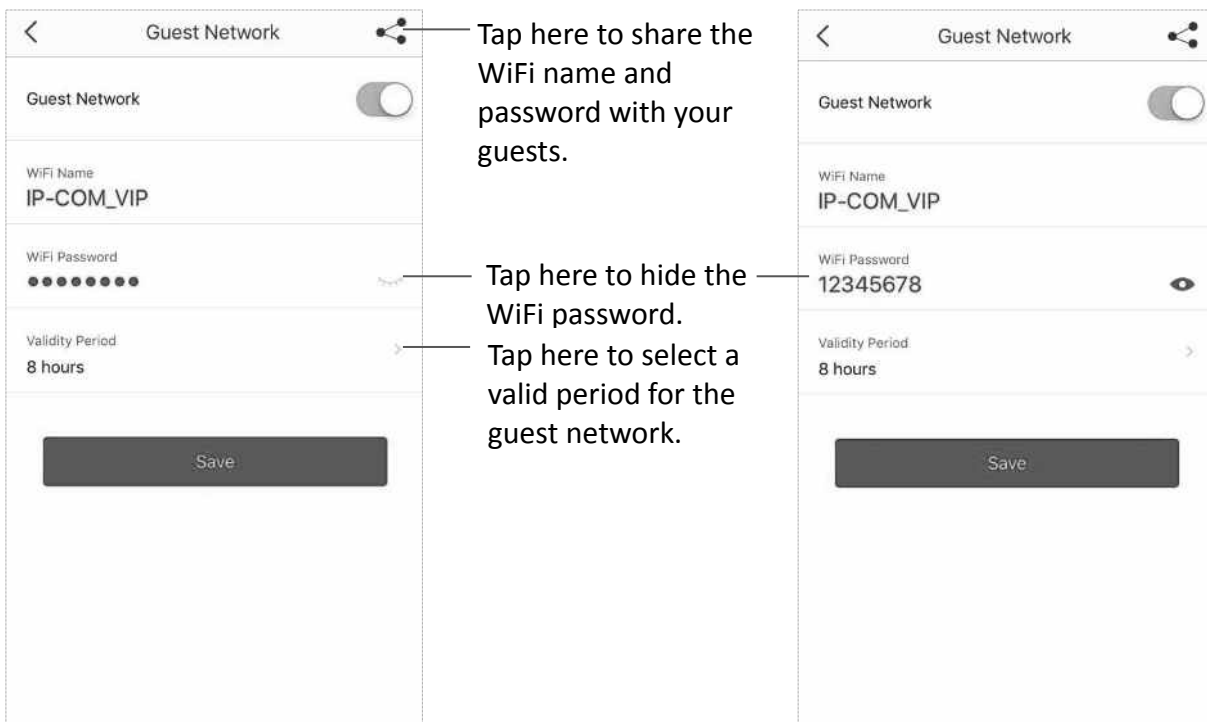
6 Guest Network



The Guest Network function allows you to create a separate network for your guests to secure the main network.

Perform the following procedure to enable the Guest Network:

1. Choose **Settings > Guest Network** to enter the configuration page.
2. Set the button  to the enabled state .
3. Change the WiFi name, password and validity period as required.
4. Tap **Save**.



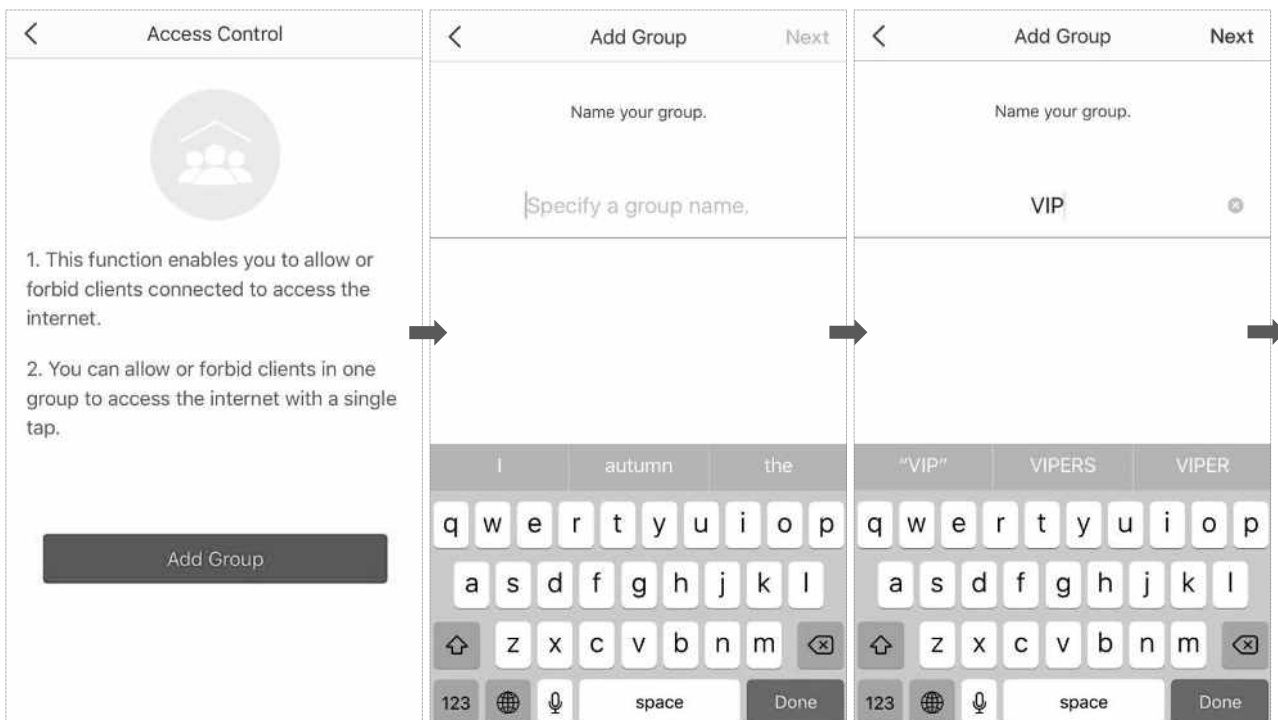
7 Access Control



The Access Control function allows you to create different department-based groups and control their internet time.

Perform the following procedure to set up the Access Control function:

1. Choose **Settings > Access Control** to enter the configuration page.
2. Create a group.
 - (1) Tap **Add Group**.
 - (2) Enter a group name, which is **VIP** in this example, and tap **Next**.
 - (3) Select the devices to be added into the group.
 - (4) Tap **Complete**.





(5) Tap  or  to change the rules.

 indicates that the devices in the group are allowed to access the internet.

 indicates that the devices in the group are not allowed to access the internet.

3. Specify a period for the rule.

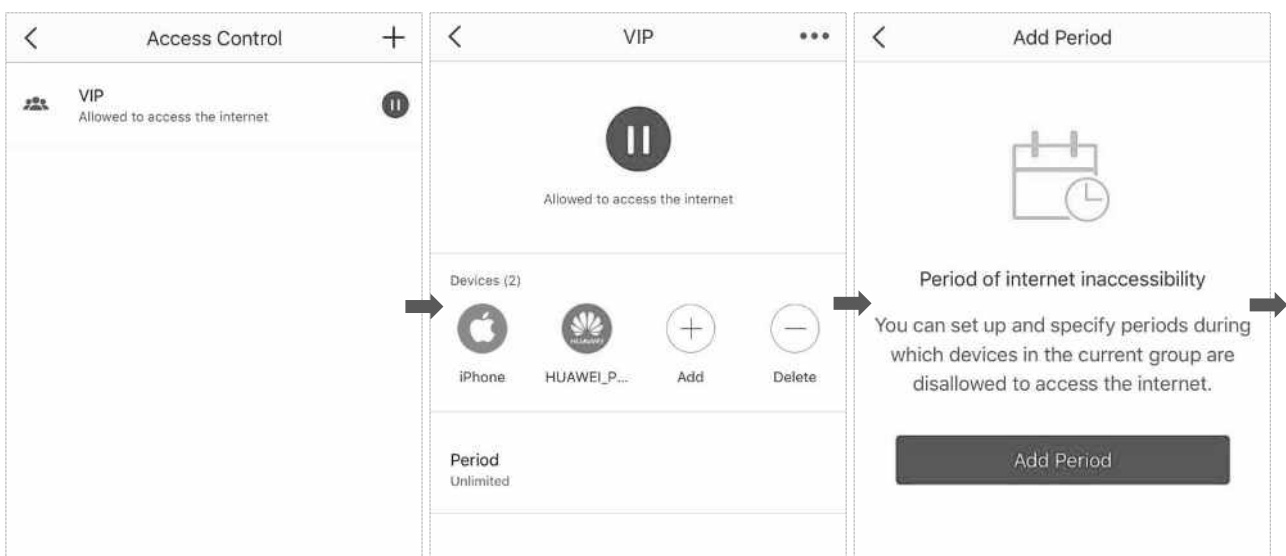
(1) Choose the group.

(2) Tap **Period**.

(3) Tap **Add Period**.

(4) Specify a **Period Name**, **Start Time**, **End Time**, and the dates from when the rule takes effect.

(5) Tap **Save**.



Add Period

Enable

Period Name

Bedtime

Start Time

22:00

End Time

06:00

Effective On

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Save

8 Internet Settings



This section describes how to change your connection type, and set the number of WAN ports.

- **PPPoE:** If this type is selected, you need to enter the PPPoE user name and password provided by your ISP for internet access.
- **DHCP:** If this type is selected, no parameter is required to enter. The mesh node obtains the dynamic IP address and other related parameters automatically from the upstream device.
- **Static IP Address:** If this type is selected, you need to enter the static IP address and other related parameters provided by your ISP for internet access.
- **Bridge:** If this type is selected, the mesh node can access the internet only after being connected to another router with internet accessibility in wired manner.

The following three connection types are available only when the language of your smart phone is set to **Russian** or **Ukraine**.

- **PPPoE Russia:** If this type is selected, you need to enter the PPPoE user name, PPPoE password, service name, server name, MTU value, and IP address information (if any) provided by your ISP for internet access.
- **PPTP/PPTP Russia:** If this type is selected, you need to enter the IP address, user name and password of the PPTP server, MTU value, and IP address information (if any) provided by your ISP for internet access.
- **L2TP/L2TP Russia:** If this type is selected, you need to enter the IP address, user name and password of the L2TP server, MTU value, and IP address information (if any) provided by your ISP for internet access.



If you set the **Connection Type** to **Bridge**, the Guest Network, Access Control, Port Forwarding, UPnP, DNS, QoS, DHCP server, and Double-line Connection functions become unavailable.

Setting up PPPoE

1. Choose **Settings** > **Internet Settings** to enter the configuration page.

2. Tap **Connection Type**.

3. Select **PPPoE**.

4. Enter the PPPoE user name and password provided by your ISP.

If a service name and a server name are provided, tap **advanced** and enter them.

5. Tap **Save**.

Internet Settings Save

WAN1 port

Connection Type
PPPoE

PPPoE User Name
789

PPPoE Password
...

advanced

Double-line Connection
Set WAN2/LAN to the WAN port

Tap here to select a connection type.

Tap here to see the PPPoE password.

Tap here to set the advanced settings.

Tap here to set the internet settings for the second WAN port.

Internet Settings Save

WAN1 port

Connection Type
PPPoE

PPPoE User Name
789

PPPoE Password
789

advanced

MTU
1480

Service Name
Optional

Server Name
Optional

The configuration for WAN2 port is similar.

Internet Settings

Save

WAN1 port

Connection Type

PPPoE

PPPoE User Name

789

PPPoE Password

●●●

advanced

Double-line Connection

Set WAN2/LAN to the WAN port

WAN2 port

Connection Type

PPPoE

Internet Settings

Save

WAN2 port

Connection Type

PPPoE

PPPoE User Name

PPPoE User Name

PPPoE Password

PPPoE Password

advanced

MTU

1480

Service Name

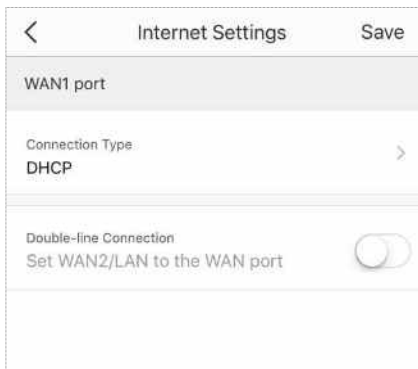
Optional

Server Name

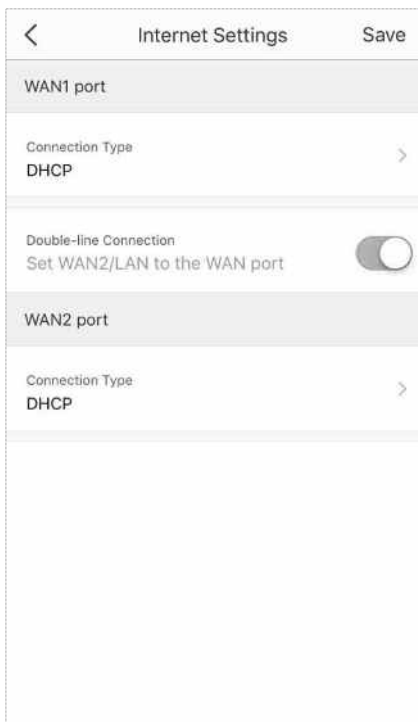
Optional

Setting up DHCP

1. Choose **Settings > Internet Settings** to enter the configuration page.
2. Tap **Connection Type**.
3. Select **DHCP**.
4. Tap **Save**.



The configuration for WAN2 port is similar.



Tap here to set the internet settings for the second WAN port.

Setting up Static IP Address

1. Choose **Settings > Internet Settings** to enter the configuration page.
2. Tap **Connection Type**.
3. Select **Static IP Address**.
4. Enter **IP Address, Subnet Mask, Default Gateway** and **Primary DNS Server**.

If a secondary DNS server is provided, enter it as well.

5. Tap **Save**.

Internet Settings Save

WAN1 port

Connection Type
Static IP Address

IP Address
0.0.0.0

Subnet Mask
0.0.0.0

Default Gateway
0.0.0.0

Primary DNS Server
0.0.0.0

Secondary DNS Server (optional)
0.0.0.0

Double-line Connection
Set WAN2/LAN to the WAN port

Tap here to set the internet settings for the second WAN port.

The configuration for WAN2 port is similar.

Internet Settings Save

WAN1 port

Connection Type
Static IP Address

IP Address
0.0.0.0

Subnet Mask
0.0.0.0

Default Gateway
0.0.0.0

Primary DNS Server
0.0.0.0

Secondary DNS Server (optional)
0.0.0.0

Double-line Connection
Set WAN2/LAN to the WAN port

Internet Settings Save

Double-line Connection
Set WAN2/LAN to the WAN port

WAN2 port

Connection Type
Static IP Address

IP Address
0.0.0.0

Subnet Mask
0.0.0.0

Default Gateway
0.0.0.0

Primary DNS Server
0.0.0.0

Secondary DNS Server (optional)

Setting up Bridge

Ensure that one of the mesh nodes in your mesh network is connected to your router with internet accessibility using an Ethernet cable.

1. Choose **Settings > Internet Settings** to enter the configuration page.
2. Tap **Connection Type**.
3. Select **Bridge**.
4. Tap **Save**.



Tip

If you set the **Connection Type** to **Bridge**, the Guest Network, Access Control, Port Forwarding, UPnP, DNS, QoS, DHCP server, and Double-line Connection functions become unavailable.

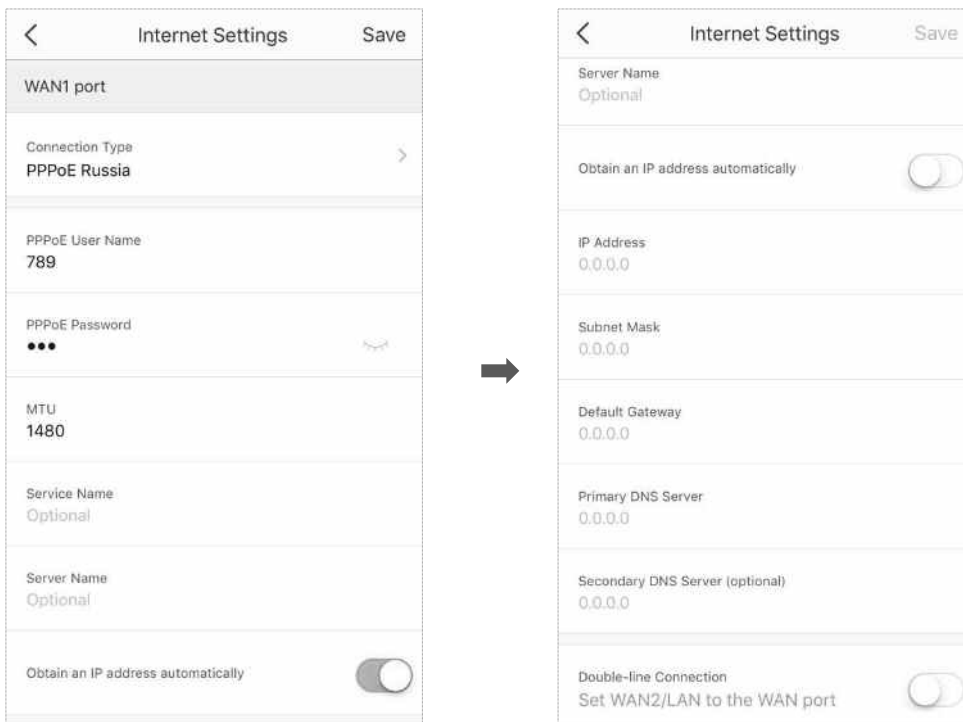
The following three connection types are available only when the language of your smart phone is set to **Russian** or **Ukraine**.

Setting up PPPoE Russia

1. Choose **Settings > Internet Settings** to enter the configuration page.
2. Tap **Connection Type**.
3. Select **PPPoE Russia**.
4. Enter **PPPoE User Name**, **PPPoE Password**, **Service Name** and **Server Name**, and change the **MTU** value as needed.

If a static IP address and related information are provided, set the **Obtain an IP address automatically** button to the  state, and enter them as well.

5. Tap **Save**.



The image displays two screenshots of the 'Internet Settings' application, illustrating the configuration steps for PPPoE Russia. An arrow points from the left screenshot to the right one, indicating a sequence of steps.

Left Screenshot (Initial State):

- WAN1 port
- Connection Type: PPPoE Russia
- PPPoE User Name: 789
- PPPoE Password: [masked]
- MTU: 1480
- Service Name: Optional
- Server Name: Optional
- Obtain an IP address automatically: [off]

Right Screenshot (Final State):

- Server Name: Optional
- Obtain an IP address automatically: [on]
- IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Default Gateway: 0.0.0.0
- Primary DNS Server: 0.0.0.0
- Secondary DNS Server (optional): 0.0.0.0
- Double-line Connection: Set WAN2/LAN to the WAN port [on]

The configuration for WAN2 port is similar.

<

Internet Settings

Save

Server Name

Optional

Obtain an IP address automatically

IP Address

0.0.0.0

Subnet Mask

0.0.0.0

Default Gateway

0.0.0.0

Primary DNS Server

0.0.0.0

Secondary DNS Server (optional)

0.0.0.0

Double-line Connection

Set WAN2/LAN to the WAN port

➔

<

Internet Settings

Save

WAN2 port

Connection Type

PPPoE Russia

>

PPPoE User Name

PPPoE User Name

PPPoE Password

PPPoE Password

MTU

1480

Service Name

Optional

Server Name

Optional

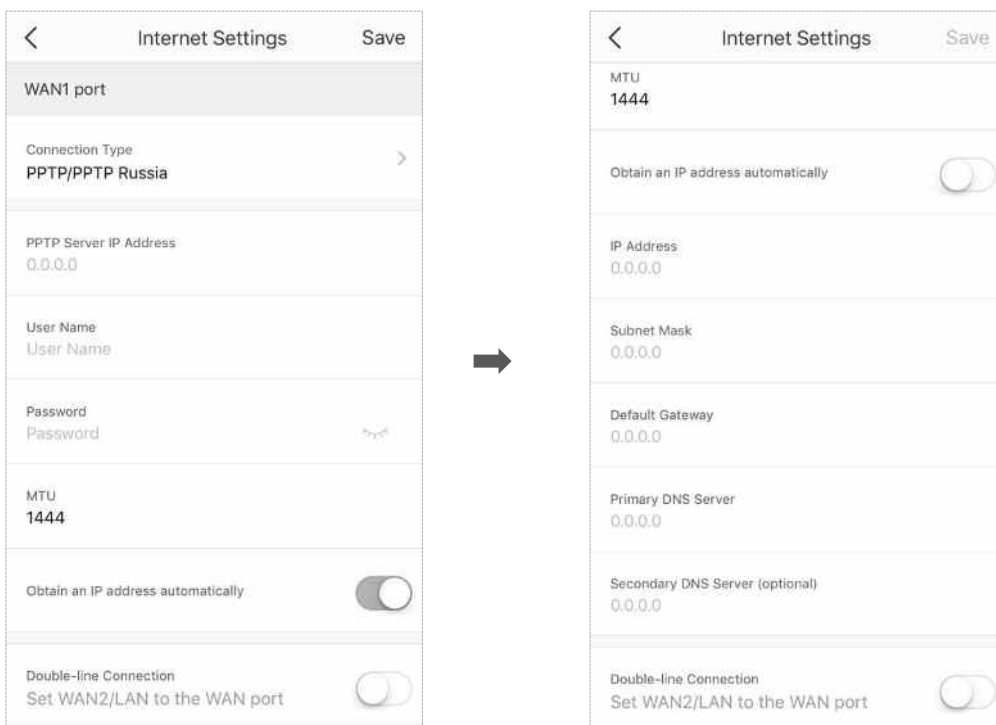
Obtain an IP address automatically

Setting up PPTP/PPTP Russia

1. Choose **Settings > Internet Settings** to enter the configuration page.
2. Tap **Connection Type**.
3. Select **PPTP/PPTP Russia**.
4. Enter **PPTP Server IP Address**, **User Name** and **Password**, and change the **MTU** value as needed.

If a static IP address and related information are provided, set the **Obtain an IP address automatically** button to  state, and enter them as well.

5. Tap **Save**.



The diagram illustrates the configuration process for PPTP/PPTP Russia. It shows two screenshots of the 'Internet Settings' app, connected by a right-pointing arrow. The left screenshot shows the initial configuration screen with fields for WAN1 port, Connection Type (set to PPTP/PPTP Russia), PPTP Server IP Address (0.0.0.0), User Name, Password, MTU (1444), and a toggle for 'Obtain an IP address automatically' (currently off). The right screenshot shows the detailed configuration screen after tapping 'Save', where the 'Obtain an IP address automatically' toggle is now on, and the IP Address, Subnet Mask, Default Gateway, Primary DNS Server, and Secondary DNS Server (optional) fields are all set to 0.0.0.0. The 'Double-line Connection' toggle remains off in both screens.

Field	Initial Value	Final Value
WAN1 port		
Connection Type	PPTP/PPTP Russia	PPTP/PPTP Russia
PPTP Server IP Address	0.0.0.0	
User Name	User Name	
Password	Password	
MTU	1444	
Obtain an IP address automatically	Off	On
IP Address		0.0.0.0
Subnet Mask		0.0.0.0
Default Gateway		0.0.0.0
Primary DNS Server		0.0.0.0
Secondary DNS Server (optional)		0.0.0.0
Double-line Connection	Off	Off

The configuration for WAN2 port is similar.

The figure shows two side-by-side screenshots of the 'Internet Settings' screen, separated by a large black arrow pointing from left to right, indicating a transition or comparison between two states.

Left Screenshot (Original Settings):

- Back arrow and 'Save' button at the top.
- MTU: 1444
- Obtain an IP address automatically: Toggle switch is turned off.
- IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Default Gateway: 0.0.0.0
- Primary DNS Server: 0.0.0.0
- Secondary DNS Server (optional): 0.0.0.0
- Double-line Connection: Set WAN2/LAN to the WAN port. Toggle switch is turned off.

Right Screenshot (Modified Settings):

- Back arrow and 'Save' button at the top.
- Double-line Connection: Set WAN2/LAN to the WAN port. Toggle switch is turned on.
- WAN2 port: Section header.
- Connection Type: PPTP/PPTP Russia (with a right arrow icon).
- PPTP Server IP Address: 0.0.0.0
- User Name: User Name
- Password: Password (with a password icon).
- MTU: 1452
- Obtain an IP address automatically: Toggle switch is turned on.

Setting up L2TP/L2TP Russia

1. Choose **Settings > Internet Settings** to enter the configuration page.
2. Tap **Connection Type**.
3. Select **L2TP/L2TP Russia**.
4. Enter **L2TP Server IP Address**, **User Name** and **Password**, and change the **MTU** value as needed.

If a static IP address and related information are provided, set the **Obtain an IP address automatically** button to ☐ state, and enter them as well.

5. Tap **Save**.

The image displays two sequential screenshots of the 'Internet Settings' application, connected by a right-pointing arrow, illustrating the configuration process for L2TP/L2TP Russia.

Left Screenshot (Initial Setup):

- Header: Internet Settings, Save
- WAN1 port
- Connection Type: L2TP/L2TP Russia
- L2TP Server IP Address: 0.0.0.0
- User Name: User Name
- Password: Password
- MTU: 1460
- Obtain an IP address automatically: ☒
- Double-line Connection: Set WAN2/LAN to the WAN port

Right Screenshot (Configured State):

- Header: Internet Settings, Save
- MTU: 1460
- Obtain an IP address automatically: ☐
- IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Default Gateway: 0.0.0.0
- Primary DNS Server: 0.0.0.0
- Secondary DNS Server (optional): 0.0.0.0
- Double-line Connection: Set WAN2/LAN to the WAN port

The configuration for WAN2 port is similar.

<

Internet Settings

Save

MTU

1460

Obtain an IP address automatically

IP Address

0.0.0.0

Subnet Mask

0.0.0.0

Default Gateway

0.0.0.0

Primary DNS Server

0.0.0.0

Secondary DNS Server (optional)

0.0.0.0

Double-line Connection

Set WAN2/LAN to the WAN port

➔

<

Internet Settings

Save

Double-line Connection

Set WAN2/LAN to the WAN port

WAN2 port

Connection Type

L2TP/L2TP Russia

>

L2TP Server IP Address

0.0.0.0

User Name

User Name

Password

Password

⌨

MTU

1460

Obtain an IP address automatically

9 QoS



The QoS function prioritizes gaming and web browsing activities.

Perform the following procedure to enable the QoS function:

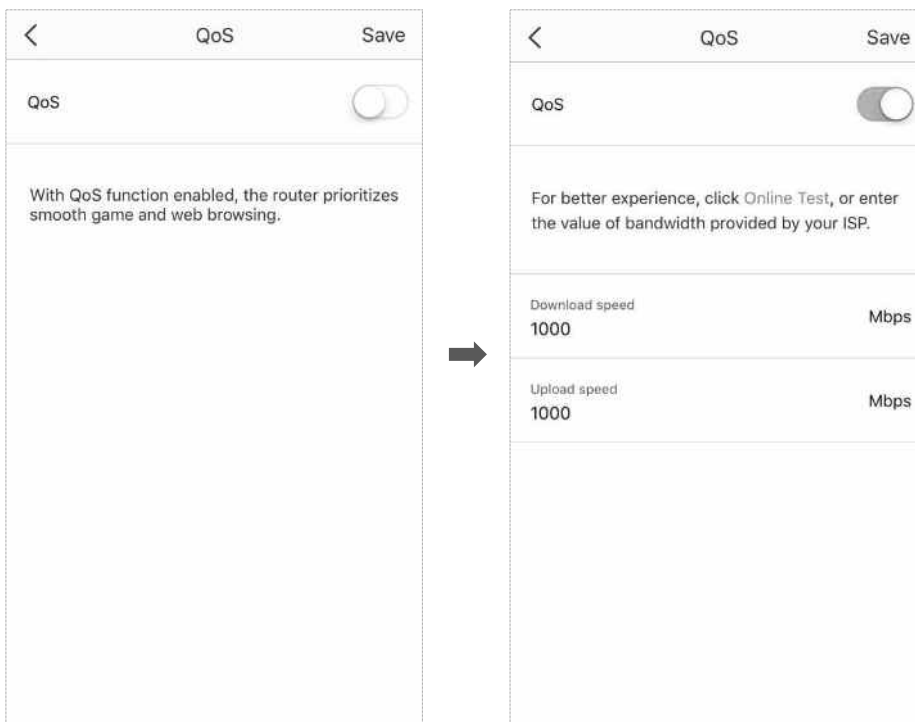
1. Choose **Settings** > **QoS** to enter the configuration page.
2. Set the button  to the enabled state .
3. Enter download and upload speed provided by your ISP, or tap **Online Test**.



Tip

To get an accurate value, ensure that wireless devices connected to your mesh network have no internet activity when testing online.

4. Tap **Save**.



QoS		Save
QoS 		
With QoS function enabled, the router prioritizes smooth game and web browsing.		

QoS		Save
QoS 		
For better experience, click Online Test, or enter the value of bandwidth provided by your ISP.		
Download speed	1000	Mbps
Upload speed	1000	Mbps

10 Add Mesh Device

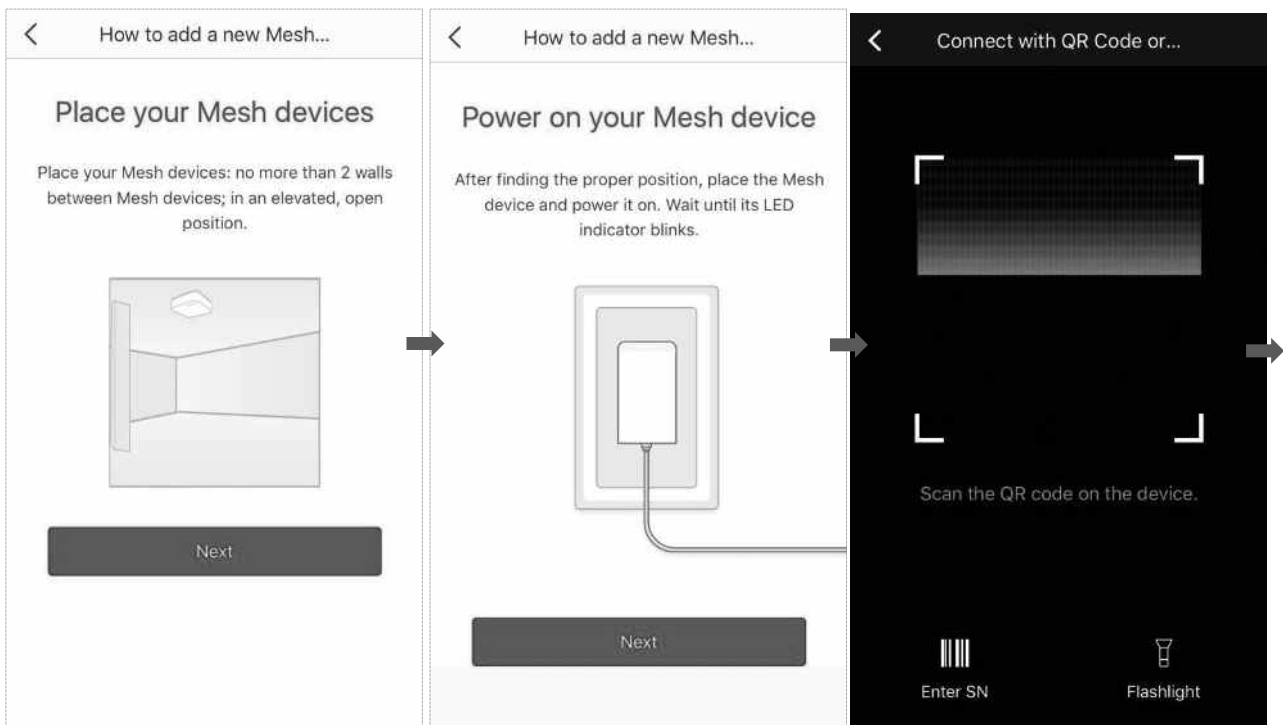


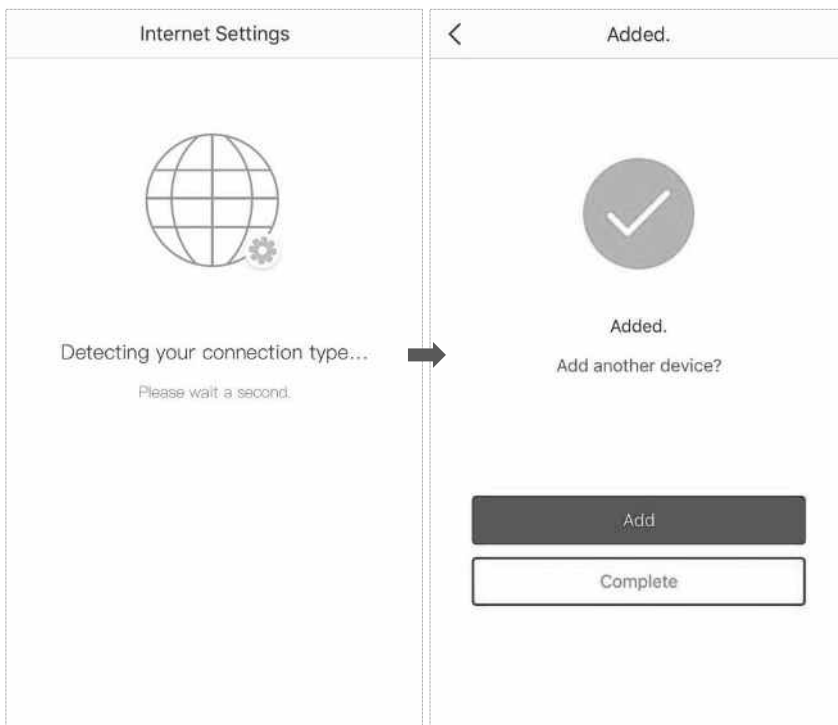
If you want to expand your WiFi coverage, you can add more mesh nodes to your existing mesh network. Use the following table to help you make the best choice.

Scenarios	Solutions
3,500 sq. ft with 60 devices	1 × EW9 + 1 × EP9
5,000 sq. ft with 80 devices	1 × EW9 + 2 × EP9
6,000 sq. ft with 100 devices	1 × EW9 + 3 × EP9

Perform the following procedure to add another mesh node into your existing mesh network:

1. Choose **Settings > Add Mesh device** to enter the configuration page.
2. Follow the on-screen guide to complete the settings.





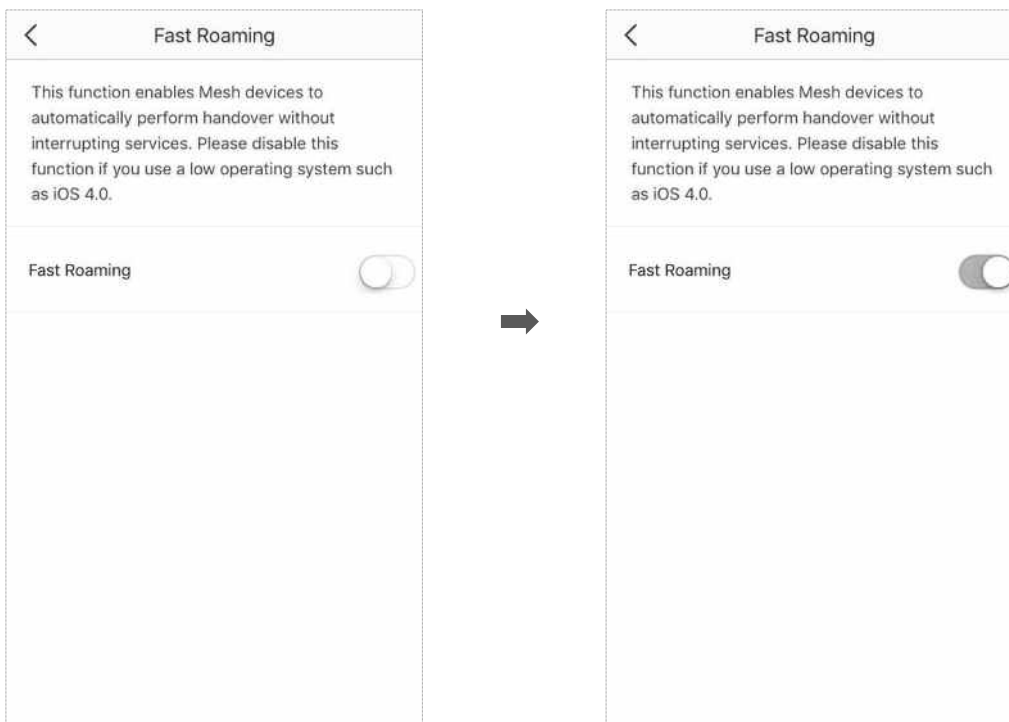
11 Fast Roaming



The Fast Roaming function lets you enjoy uninterrupted internet service when moving around the WiFi-blanketed range.

Perform the following procedure to enable the Fast Roaming function:

1. Choose **Settings > Fast Roaming** to enter the configuration page.
2. Set the button  to the enabled state .



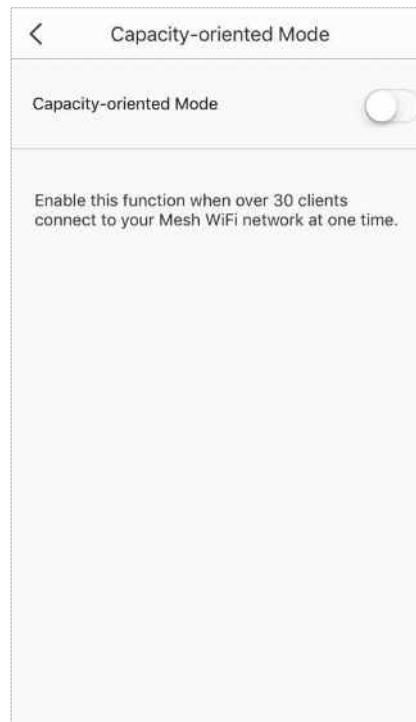
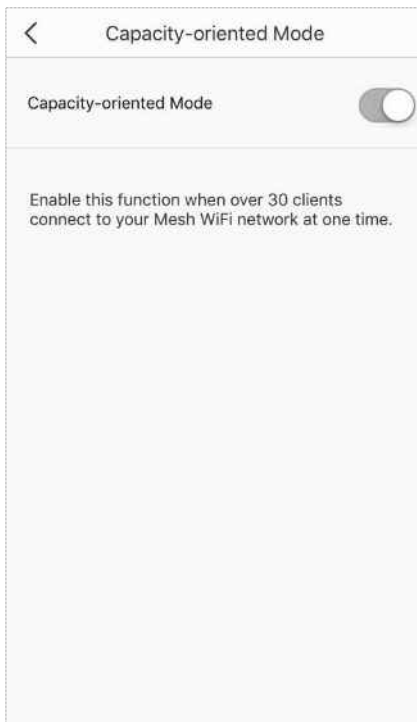
12 Capacity-oriented Mode



The Capacity-oriented mode ensures the internet experience when over 30 clients are connected to your mesh network at one time.

Perform the following procedure to disable/enable the Capacity-oriented Mode:

1. Choose **Settings > Capacity-oriented Mode** to enter the configuration page.
2. Alternate the status between enabled and disabled by tapping icon as required. It is recommended to keep the enabled  state.



13 Captive Portal



A captive portal is an entry to a network that requires users to view a splash page and agree to terms and conditions before using the network. The Mesh WiFi system support three authentication types: account authentication, one-key authentication, and SMS authentication.

- **Account Authentication**

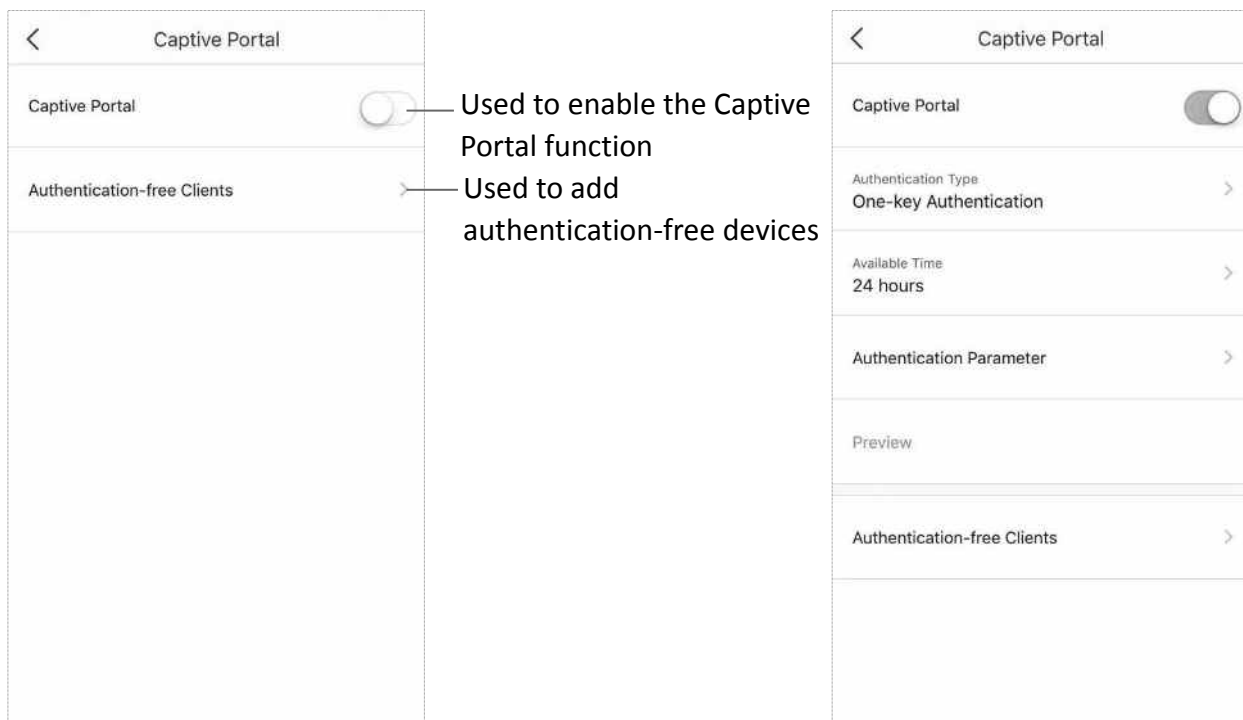
If the Account Authentication is set, Users can access the internet only after being authenticated with the valid user name and password.

- **One-key Authentication**

If the One-key Authentication is set, users can access the internet after tapping the **Connect** button on the authentication page.

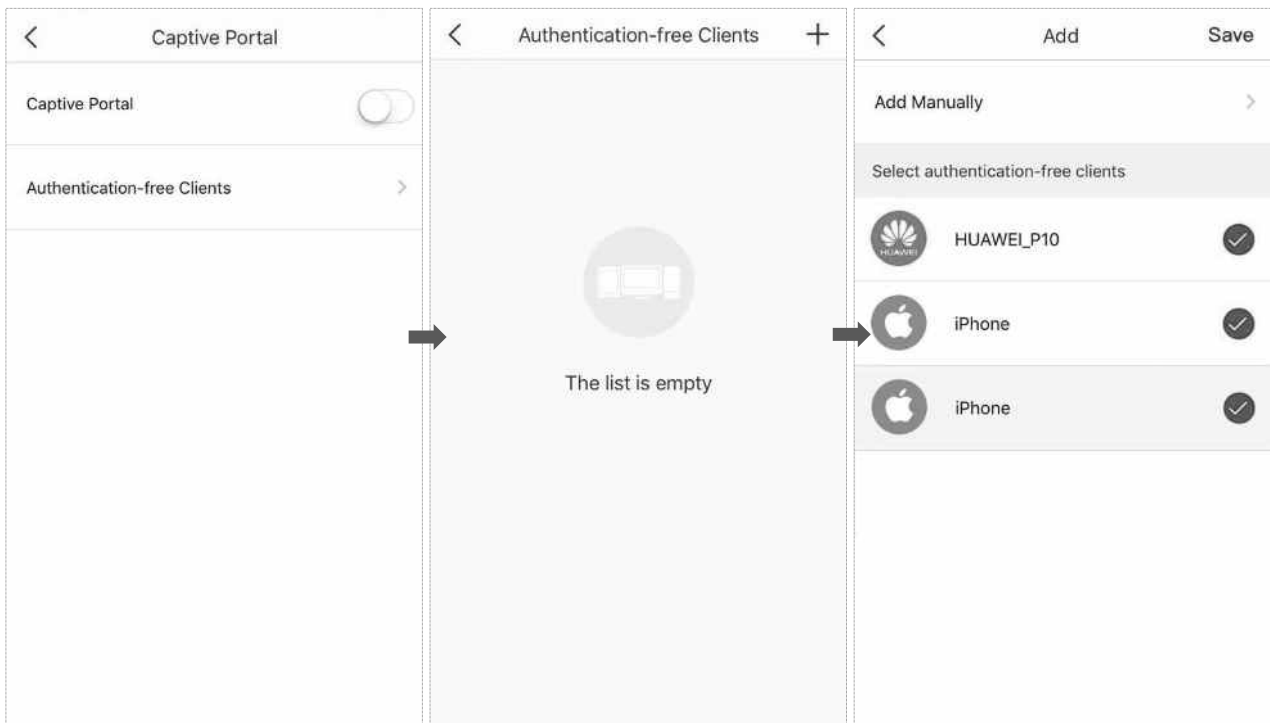
- **SMS Authentication**

If the SMS Authentication is set, users need to enter their phone number on the authentication page to receive a verification code. Then enter the verification code on the authentication page for accessing the internet.

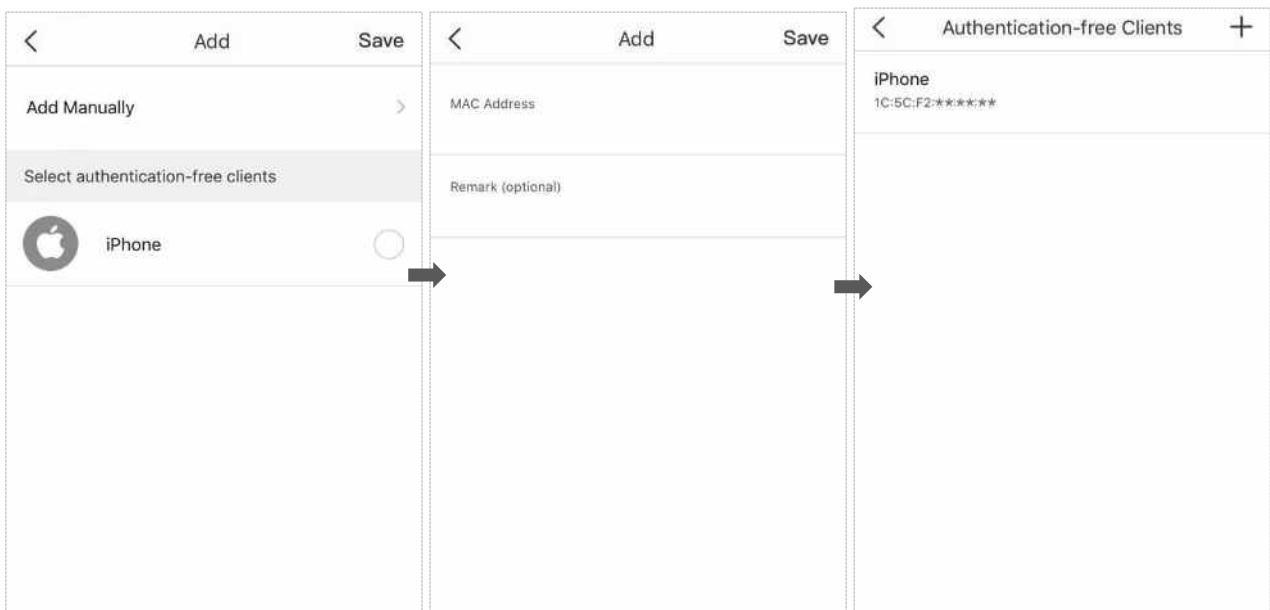


Adding authentication-free clients

1. Choose **Settings > Captive Portal** to enter the configuration page.
2. Tap **Authentication-free Clients**.
3. Tap the **+** icon on the upper-right corner.
4. If the device you want to add has connected to the mesh network, directly select it in the list, and tap **Save**.



If it is not on the list, tap **Add Manually**, enter the MAC address of the device, specify remark, then tap **Save**.



Setting up the account authentication rule

1. Choose **Settings > Captive Portal** to enter the configuration page.
2. Set the button  to the enabled state .
3. Set the Authentication type to **Account Authentication**.

< Captive Portal	< Captive Portal	< Authentication Type
Captive Portal 	Captive Portal 	Account Authentication ☒
Authentication-free Clients >	Authentication Type One-key Authentication >	One-key Authentication ☐
	Available Time 24 hours >	SMS Authentication ☐
	Authentication Parameter >	
	Preview	
	Authentication-free Clients >	

4. Select an available time for the rule, or tap **Custom** to manually specify an available time.
After the available time elapses, the user is required to pass the authentication again.

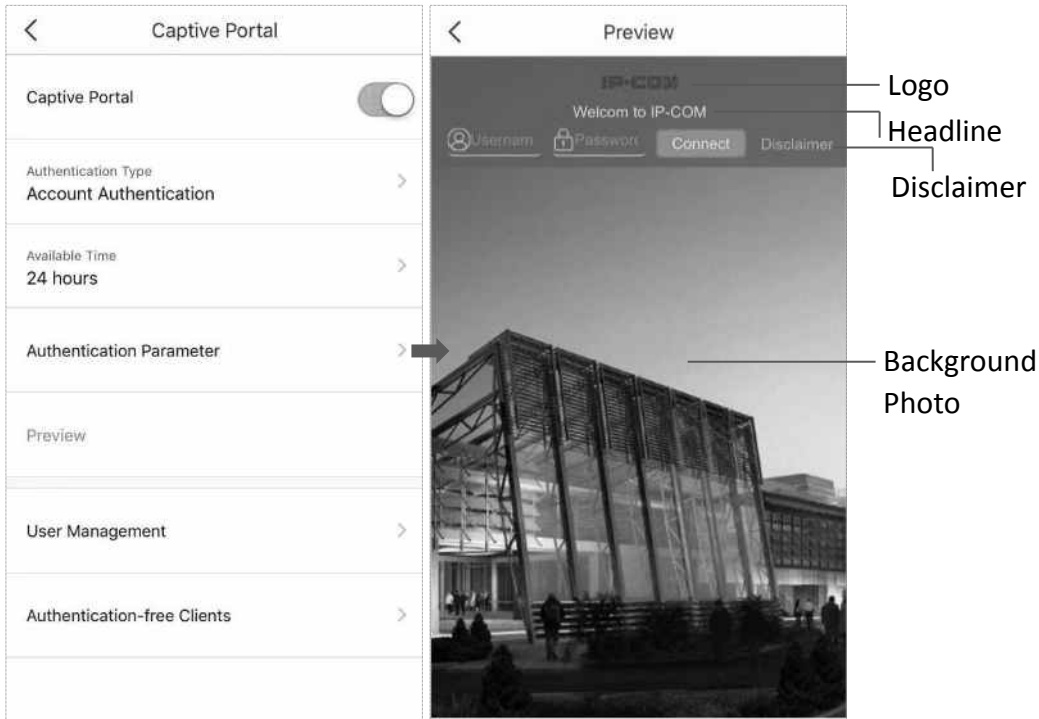
< Captive Portal	< Available Time
Captive Portal 	It is the time period that a user is allowed to stay connected to the internet after being authenticated. After that, the user needs to get authenticated again for internet access.
Authentication Type Account Authentication >	Forever ☐
Available Time 24 hours >	24 hours ☒
Authentication Parameter >	72 hours ☐
Preview	Custom >
User Management >	
Authentication-free Clients >	

5. Tap **Authentication Parameter** to set the parameters on the authentication page.

- (1) Tap **Logo** to upload a logo. This file must be .jpg, .jpeg, or .png file. The file size must be less than 30 KB, and the dimensions in pixels should be 6.5:1.
- (2) Tap **Headline** to enter a headline, and tap **Save**.
- (3) Tap **Background Photo** to upload a background file. This file must be .jpg, .jpeg, or .png file. The file size must be less than 300 KB, and the dimensions in pixels should be 16:9.
- (4) Tap **Disclaimer** to enter the disclaimer content, and tap **Save**.
- (5) Tap **Redirect to** to specify a website that users will visit after passing the authentication, and tap **Save**.
 - **Previous web page:** It specifies that the user will be redirected to the web page he visits before the authentication.
 - **Specified web page:** It specifies that the user will be redirected to the web page you specify here after passing the authentication.
- (6) Tap **Save**.

< Captive Portal	< Authentication Parameter Save	< Redirect Save
Captive Portal 	Logo >	Previous web page 
Authentication Type Account Authentication >	Headline Welcome to IP-COM >	Specified web page 
Available Time 24 hours >	Background Photo >	
Authentication Parameter > →	Disclaimer > →	
Preview	Redirect to Previous web page >	
User Management >		
Authentication-free Clients >		

6. Tap **Preview** to view the authentication page you set.

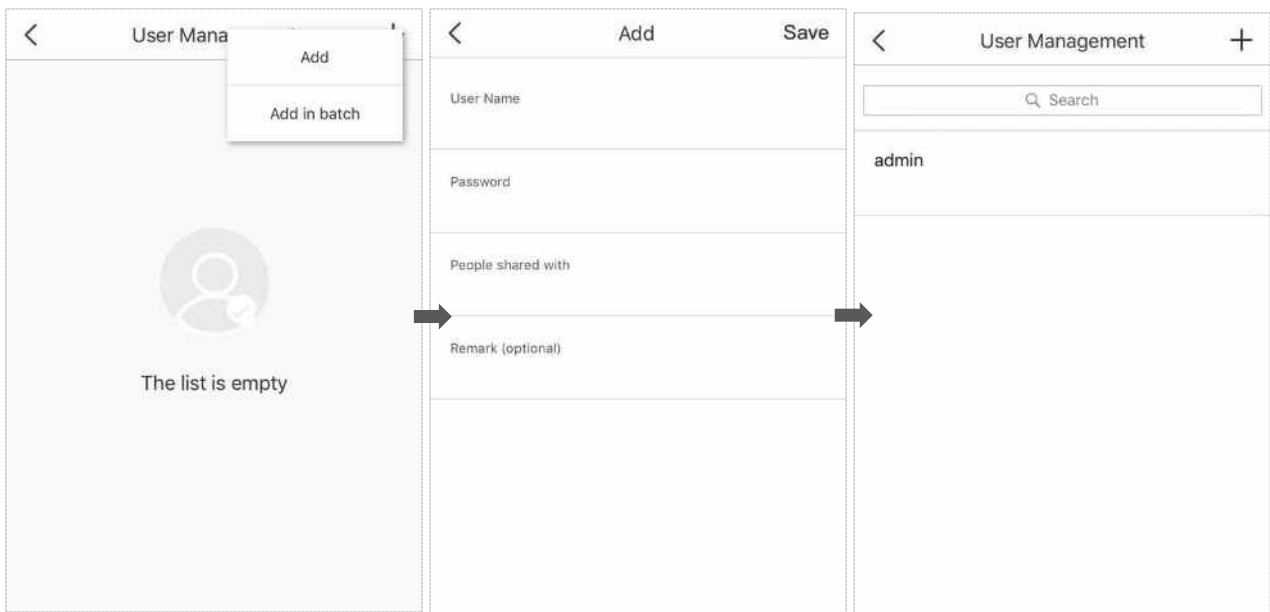


7. Tap **User Management** to add accounts for users.

8. Tap the **+** icon.

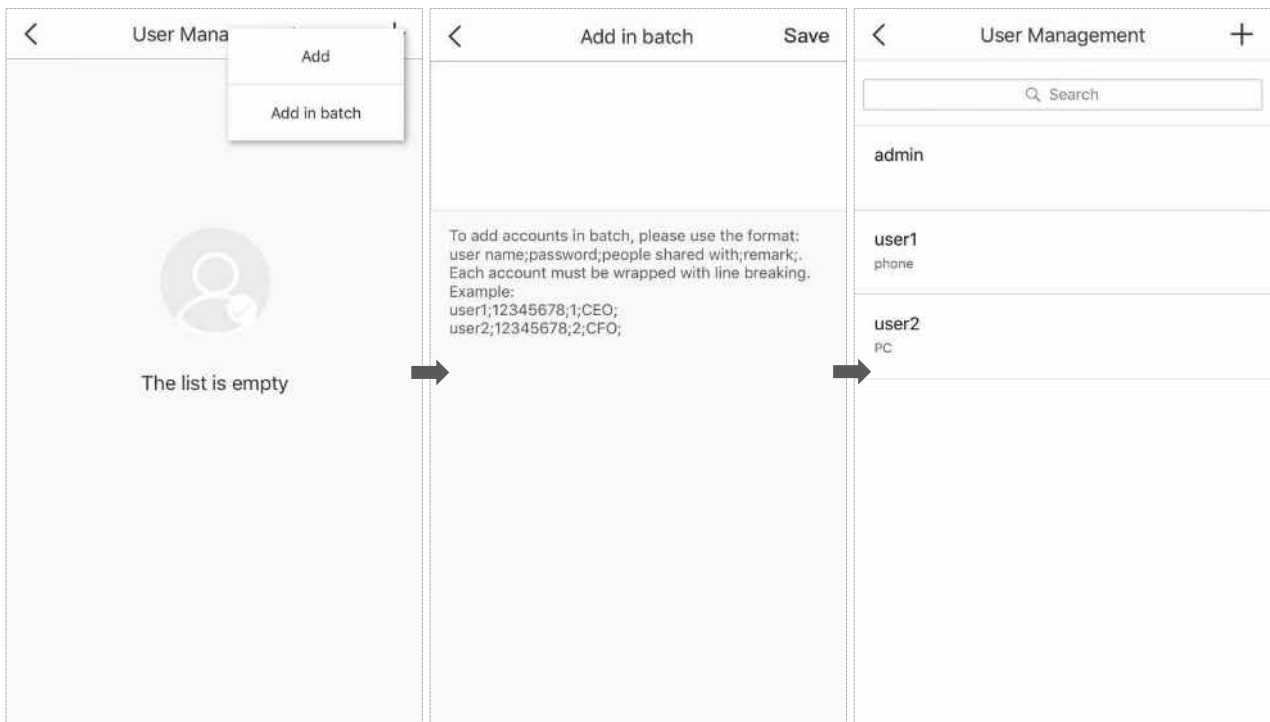
■ **Adding the accounts respectively**

- (1) Tap **Add**.
- (2) Specify a user name.
- (3) Specify a password.
- (4) Specify the number of users that can use this account to login for accessing the internet at the same time.
- (5) Specify a remark.
- (6) Tap **Save**.



■ Adding the accounts in batch

- (1) Tap **Add in batch**.
- (2) Enter the parameters in terms of the onscreen instructions.
- (3) Tap **Save**.



Verification

1. Connect a device to the mesh network in wired or wireless manner, and start a web browser. An authentication page appears.
2. Enter a user name and password for authentication.
3. Tap **Connect**.

You can access the internet after passing the authentication.



Application scenario for account authentication

For example, a large apartment named **Home** uses the Mesh WiFi system to deploy its network. It requires that each room uses an account to pass the authentication for accessing the internet.

Configuration procedure

■ Setting up the account authentication rule

1. Set the button  to the enabled state .
2. Set the Authentication type to **Account Authentication**.

< Captive Portal Captive Portal ☐ Authentication-free Clients >	< Captive Portal Captive Portal ☐ Authentication Type > One-key Authentication > Available Time > 24 hours > Authentication Parameter > Preview Authentication-free Clients >	< Authentication Type Account Authentication ☒ One-key Authentication ☐ SMS Authentication ☐
---	--	--

3. Select or customize an available time for the rule, which is **Forever** in this example.

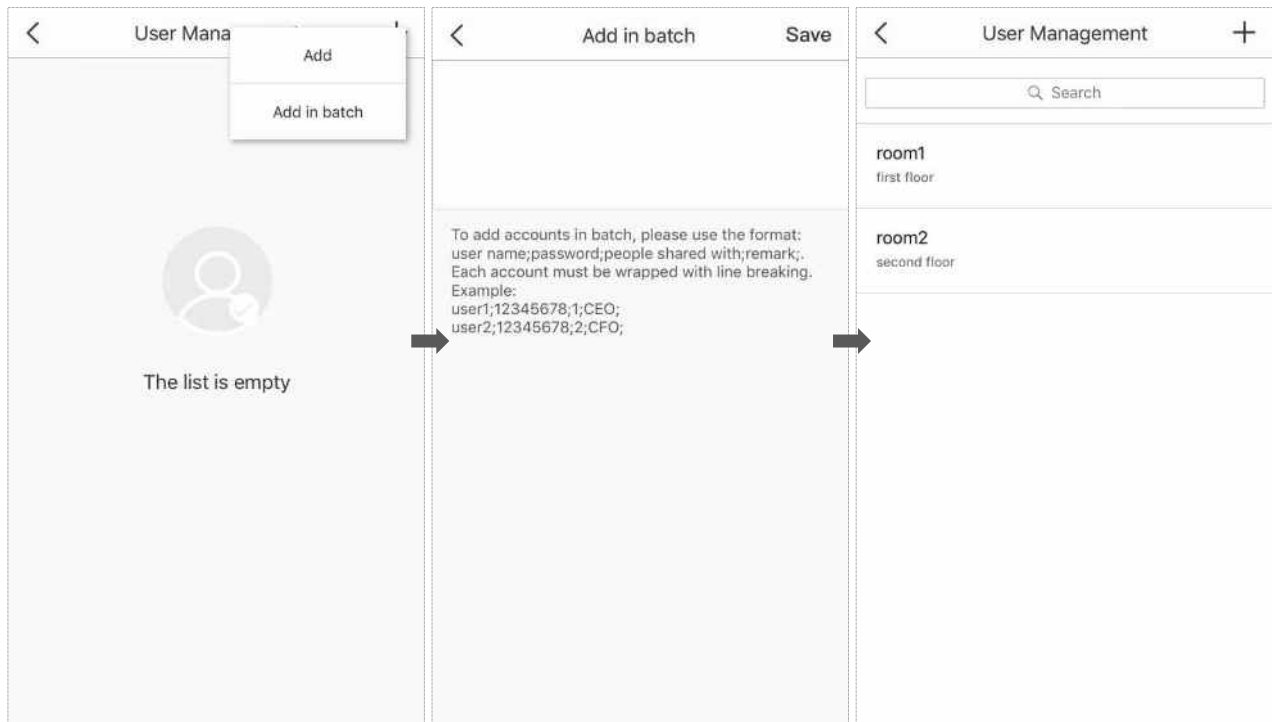
< Captive Portal Captive Portal ☐ Authentication Type > Account Authentication > Available Time > 24 hours > Authentication Parameter > Preview User Management > Authentication-free Clients >	< Available Time It is the time period that a user is allowed to stay connected to the internet after being authenticated. After that, the user needs to get authenticated again for internet access. Forever ☒ 24 hours ☐ 72 hours ☐ Custom >
--	---

4. Tap **Authentication Parameter** to set the parameters on the authentication page.

- (1) Tap **Logo** to upload a logo. This file must be .jpg, .jpeg, or .png file. The file size must be less than 30 KB, and the dimensions in pixels should be 6.5:1.
- (2) Tap **Headline** to enter a headline, which is **Home** in this example, and tap **Save**.
- (3) Tap **Background Photo** to upload a background file. This file must be .jpg, .jpeg, or .png file. The file size must be less than 300 KB, and the dimensions in pixels should be 16:9.

■ Adding accounts for users

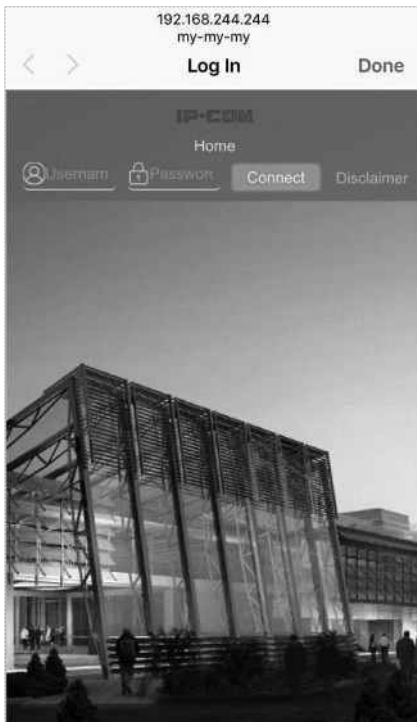
1. Tap **User Management**.
2. Tap the **+** icon.
3. Tap **Add in batch**.
4. Enter the parameters as required, Which are **“room1;good123;1;first floor;”**, and **“room2;good456;1;second floor;”** in this example.
5. Tap **Save**.



■ Verification

1. Connect a device to the mesh network in wired or wireless manner, and start a web browser. An authentication page appears.
2. Enter a user name and password for authentication, which are **room1** and **good123** in this example.
3. Tap **Connect**.

The device can access the internet after passing the authentication.



Setting up the one-key authentication rule

1. Choose **Settings > Captive Portal** to enter the configuration page.

2. Set the button  to the enabled state .

3. Set the **Authentication type** to **One-key Authentication**.

< Captive Portal Captive Portal  Authentication-free Clients >	< Captive Portal Captive Portal  Authentication Type > One-key Authentication > Available Time > 24 hours > Authentication Parameter > Preview Authentication-free Clients >	< Authentication Type Account Authentication ☐ One-key Authentication ☒ SMS Authentication ☐
--	--	---

4. Select an available time for the rule, or tap **Custom** to specify an available time. After the available time elapses, the user is required to pass the authentication again.

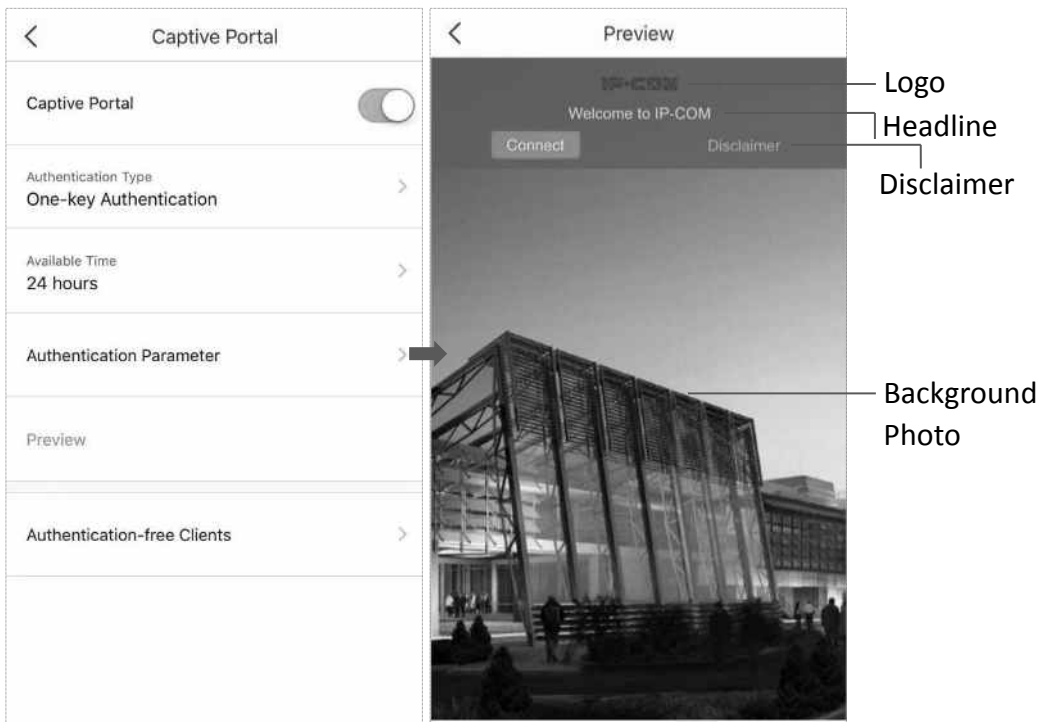
< Captive Portal Captive Portal  Authentication Type > One-key Authentication > Available Time > 24 hours > Authentication Parameter > Preview Authentication-free Clients >	< Available Time It is the time period that a user is allowed to stay connected to the internet after being authenticated. After that, the user needs to get authenticated again for internet access. Forever ☐ 24 hours ☒ 72 hours ☐ Custom >
--	--

5. Tap **Authentication Parameter** to set the parameters on the authentication page.

- (1) Tap **Logo** to upload a logo. This file must be .jpg, .jpeg, or .png file. The file size must be less than 30 KB, and the dimensions in pixels should be 6.5:1.
- (2) Tap **Headline** to enter a headline, and tap **Save**.
- (3) Tap **Background Photo** to upload a background file. This file must be .jpg, .jpeg, or .png file. The file size must be less than 300 KB, and the dimensions in pixels should be 16:9.
- (4) Tap **Disclaimer** to enter the disclaimer content, and tap **Save**.
- (5) Tap **Redirect to** to specify a website that users will visit after passing the authentication, and tap **Save**.
 - **Previous web page**: It specifies that the user will be redirected to the web page he visits before the authentication.
 - **Specified web page**: It specifies that the user will be redirected to the web page you specify here after passing the authentication.
- (6) Tap **Save**.

< Captive Portal	< Authentication Parameter Save	< Redirect Save
Captive Portal 	Logo >	Previous web page 
Authentication Type One-key Authentication >	Headline Welcome to IP-COM >	Specified web page 
Available Time 24 hours >	Background Photo >	
Authentication Parameter > →	Disclaimer > →	
Preview	Redirect to Previous web page >	
Authentication-free Clients >		

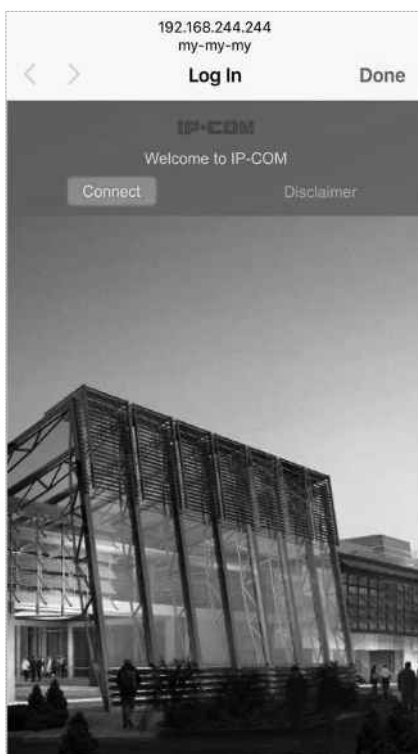
6. Tap **Preview** to view the authentication page you set.



■ Verification

1. Connect a device to the mesh network in wired or wireless manner, and start a web browser. An authentication page appears.
2. Tap **Connect**.

Then you can access the internet.



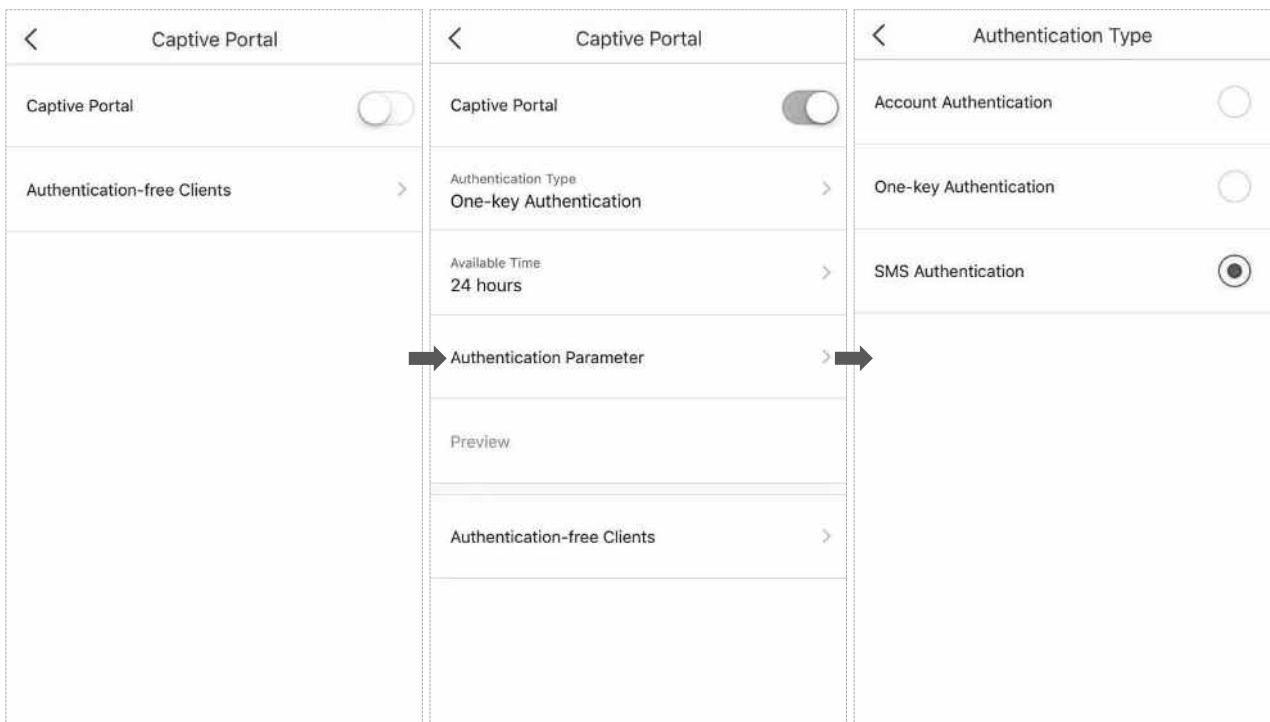
Setting up the SMS authentication rule

Prerequisites

Before you set up the SMS authentication rule, you need to have an NEXMO account and buy NEXMO SMS service.

Configuration procedure

1. Choose **Settings > Captive Portal** to enter the configuration page.
2. Set the button  to the enabled state .
3. Set the **Authentication type** to **SMS Authentication**.



4. Select an available time for the rule, or tap **Custom** to specify an available time. After the available time elapses, the user is required to pass the authentication again.

Captive Portal	Available Time
Captive Portal 	It is the time period that a user is allowed to stay connected to the internet after being authenticated. After that, the user needs to get authenticated again for internet access.
Authentication Type SMS Authentication >	
Available Time 24 hours >	Forever 
SMS Provider Parameter > 	24 hours 
Authentication Parameter >	72 hours 
Preview	Custom >
Authentication-free Clients >	

5. Set up SMS Provider Parameter.

- (1) Tap **SMS Provider Parameter**.
- (2) Enter the API key provided by the NEXMO.
- (3) Enter the API secret provided by the NEXMO.
- (4) Edit a message text for verification of the users who request for accessing the internet.
- (5) Tap **Save**.

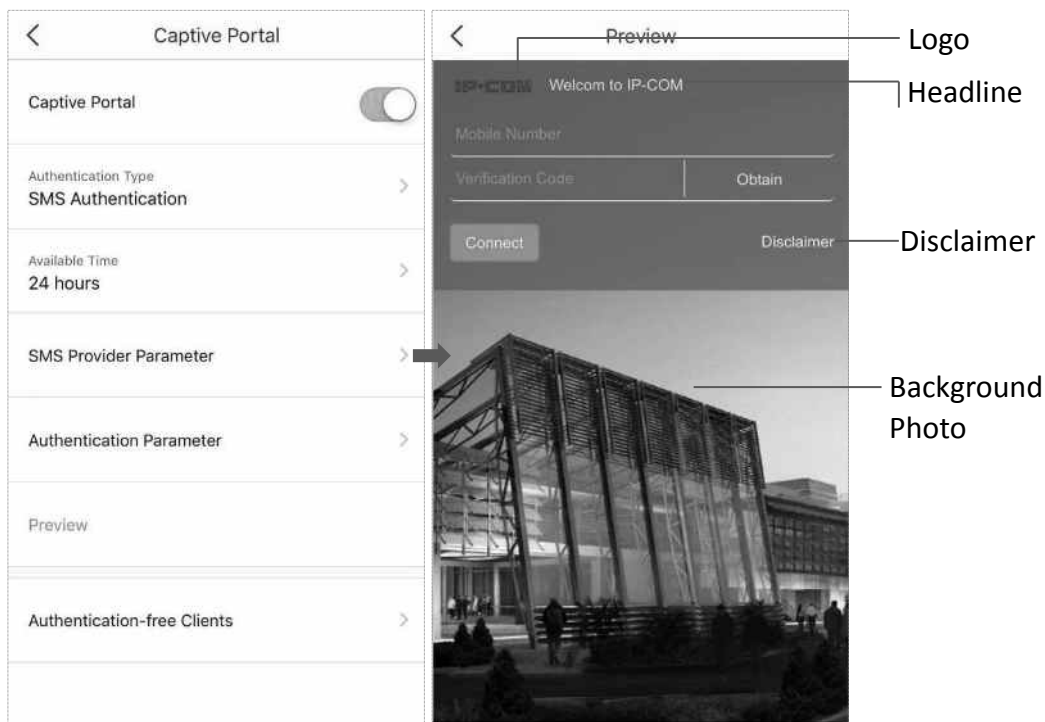
Captive Portal	SMS Provider Parameter	Save
Captive Portal 	Only NEXMO is supported. Please enter the correct account provided by NEXMO.	
Authentication Type SMS Authentication >	api_key	
Available Time 24 hours >	api_secret 	
SMS Provider Parameter > 	Text Message	
Authentication Parameter >	After saving, you are recommended to perform SMS Verification	
Preview		
Authentication-free Clients >		

6. Tap **Authentication Parameter** to set the parameters on the authentication page.

- (1) Tap **Logo** to upload a logo. This file must be .jpg, .jpeg, or .png file. The file size must be less than 30 KB, and the dimensions in pixels should be 6.5:1.
- (2) Tap **Headline** to enter a headline, and tap **Save**.
- (3) Tap **Background Photo** to upload a background file. This file must be .jpg, .jpeg, or .png file. The file size must be less than 300 KB, and the dimensions in pixels should be 16:9.
- (4) Tap **Disclaimer** to enter the disclaimer content, and tap **Save**.
- (5) Tap **Redirect to** to specify a website that users will visit after passing the authentication, and tap **Save**.
 - **Previous web page:** It specifies that the user will be redirected to the web page he visits before after passing the authentication.
 - **Specified web page:** It specifies that the user will be redirected to the web page you specify here after passing the authentication.
- (6) Tap **Save**.

< Captive Portal	< Authentication Parameter Save	< Redirect Save
Captive Portal 	Logo >	Previous web page 
Authentication Type SMS Authentication >	Headline Welcome to IP-COM >	Specified web page 
Available Time 24 hours >	Background Photo >	
SMS Provider Parameter >	Disclaimer >	
Authentication Parameter >	Redirect to Previous web page >	
Preview		
Authentication-free Clients >		

7. Tap **Preview** to view the authentication page you set.



■ Verification

1. Connect a device to the mesh network in wired or wireless manner, and start a web browser. An authentication page appears.
2. Enter your mobile number, and tap **Obtain**.
3. Enter the verification code you received.
4. Tap **Connect**.

You can access the internet after passing the authentication.



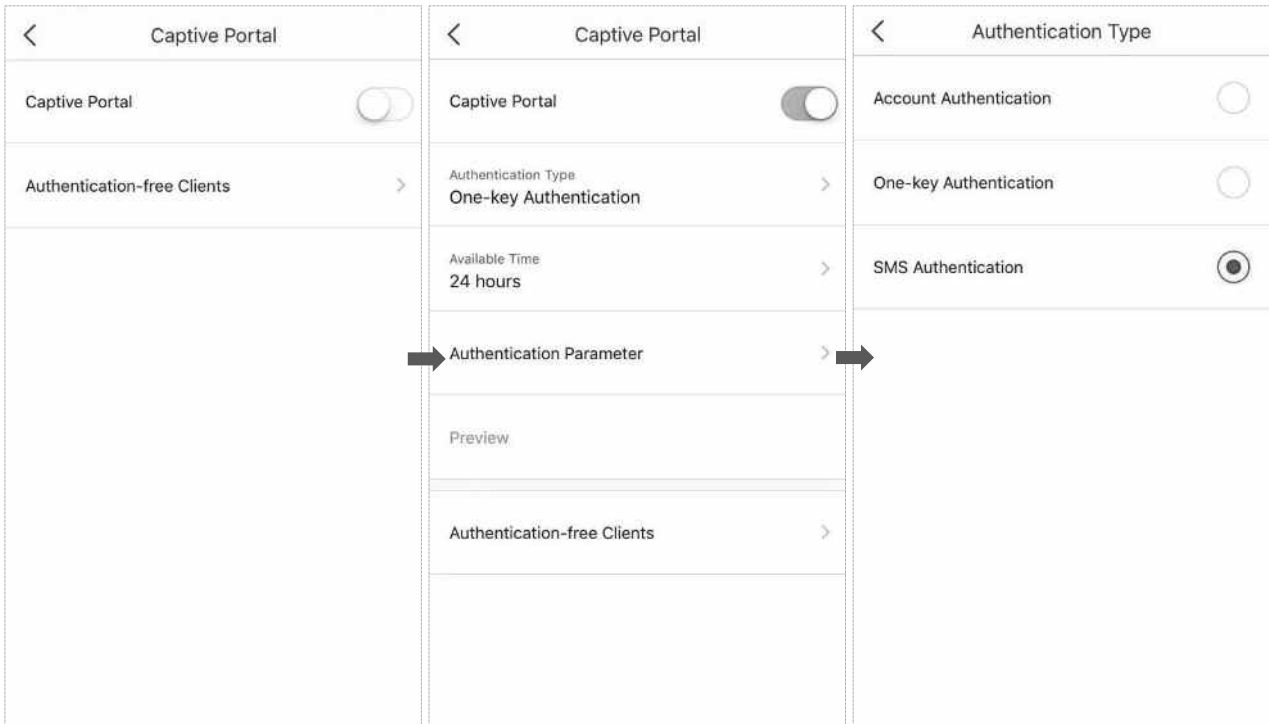
Application scenario for SMS authentication

A coffee bar named **Coffee** uses the Mesh WiFi system to deploy its network. It requires that guests use mobile numbers to pass the authentication for accessing the internet.

Configuration procedure

■ **Setting up the SMS authentication rule**

- 1. Choose **Settings > Captive Portal** to enter the configuration page.
- 2. Set the button  to the enabled state .
- 3. Set the Authentication type to **SMS Authentication**.



4. Select an available time for the rule, which is **24 hours** in this example.

Captive Portal	Available Time
Captive Portal 	It is the time period that a user is allowed to stay connected to the internet after being authenticated. After that, the user needs to get authenticated again for internet access.
Authentication Type SMS Authentication >	
Available Time 24 hours >	Forever ☐
SMS Provider Parameter >	24 hours ☒
Authentication Parameter >	72 hours ☐
Preview	Custom >
Authentication-free Clients >	

5. Set up **SMS Provider Parameter**.

- (1) Tap **SMS Provider Parameter**.
- (2) Enter the API key provided by the NEXMO.
- (3) Enter the API secret provided by the NEXMO.
- (4) Edit a text message sent to the users who request for accessing the internet, which is **"Your verification code is \$\$CODE\$\$."** in this example. **\$\$CODE\$\$** must be included in the text.
- (5) Tap **Save**.

Captive Portal	SMS Provider Parameter
Captive Portal 	Only NEXMO is supported. Please enter the correct account provided by NEXMO.
Authentication Type SMS Authentication >	api_key *****
Available Time 24 hours >	api_secret
SMS Provider Parameter >	Text Message Your verification code is \$\$CODE\$\$. After saving, you are recommended to perform SMS Verification
Authentication Parameter >	
Preview	
Authentication-free Clients >	

6. Tap **Authentication Parameter** to set the parameters on the authentication page.

- (1) Tap **Logo** to upload a logo. This file must be .jpg, .jpeg, or .png file. The file size must be less than 30 KB, and the dimensions in pixels should be 6.5:1.
- (2) Tap **Headline** to enter a headline, which is **Coffee** in this example, and tap **Save**.
- (3) Tap **Background Photo** to upload a background file. This file must be .jpg, .jpeg, or .png file. The file size must be less than 300 KB, and the dimensions in pixels should be 16:9.
- (4) Tap **Disclaimer** to enter the disclaimer content, and tap **Save**.
- (5) Tap **Redirect to**, select **Specified web page**, enter the website, which is **www.coffee.com** in this example, and tap **Save**.
- (6) Tap **Save**.

< Captive Portal	< Authentication Parameter Save	< Redirect Save
Captive Portal 	Logo >	Previous web page ☐
Authentication Type SMS Authentication >	Headline Welcome to IP-COM >	Specified web page ☒
Available Time 24 hours >	Background Photo >	www.coffee.com
SMS Provider Parameter >	Disclaimer >	
Authentication Parameter >	Redirect to Previous web page >	
Preview		
Authentication-free Clients >		

"com"

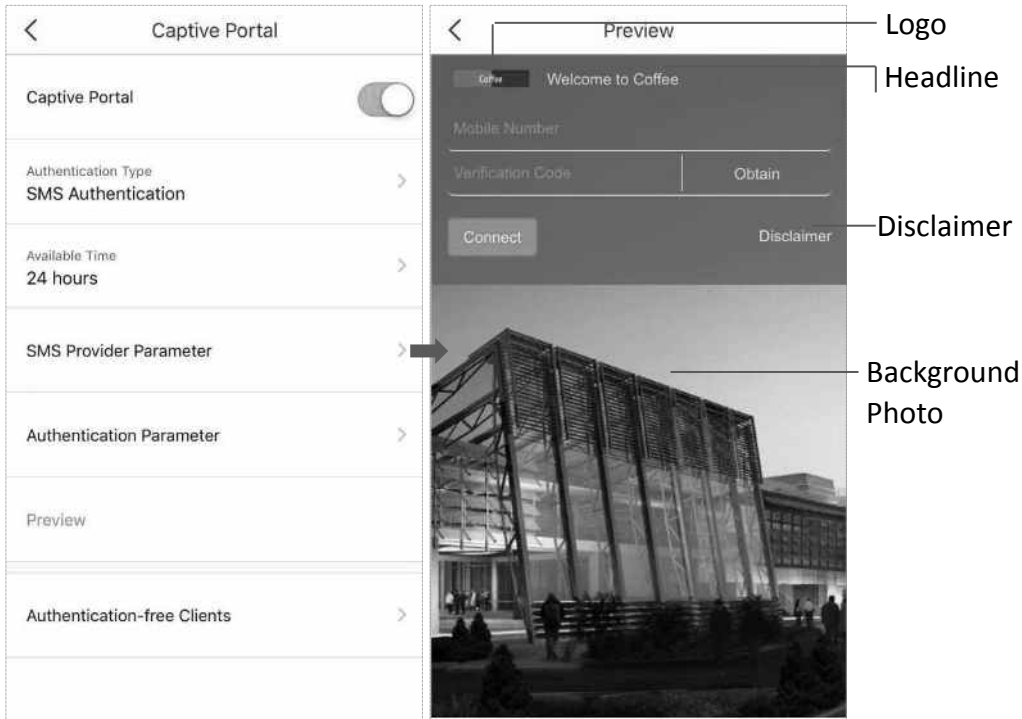
q w e r t y u i o p

a s d f g h j k l

↑ z x c v b n m ↵

123 🌐 🗣️ space return

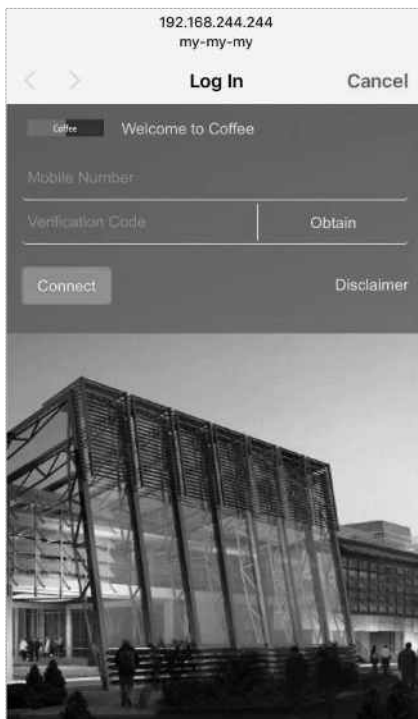
7. Tap **Preview** to view the authentication page you set.



■ Verification

1. Connect a device to the mesh network in wireless manner, and start a web browser. An authentication page appears.
2. Enter your mobile number, and tap **Obtain**.
3. Enter the verification code received on your phone.
4. Tap **Connect**.

The device can access the internet after passing the authentication.



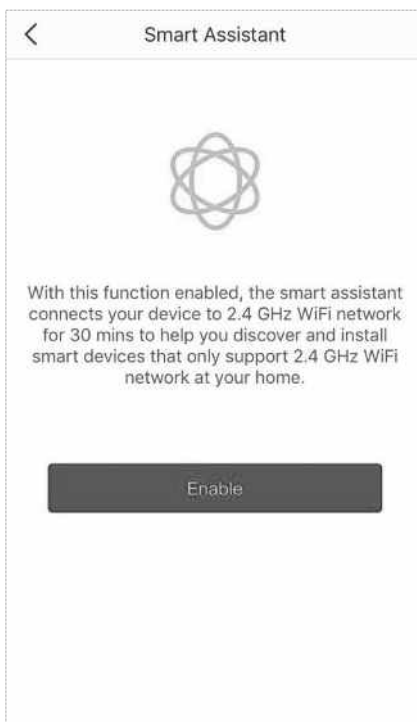
14 Smart Assistant



The mesh WiFi system supports 5 GHz priority. Therefore, dual-band clients, such as smart phones choose the 5 GHz band to connect for faster speed. In this case, to allow your 2.4 GHz WiFi-enabled devices such as printers, or IP cameras to join the mesh WiFi network, you can enable this function to keep your smart phone on 2.4 GHz for 30 minutes.

Perform the following procedure to enable the Smart Assistant function:

1. Choose **Settings > Smart Assistant** to enter the configuration page.
2. Tap **Enable**.



15 Port Forwarding



The Port Forwarding function enables internet users to access your LAN resources, such as resources on the web server or FTP server.

Perform the following procedure to set up the Port Forwarding function:

1. Choose **Settings > Port Forwarding** to enter the configuration page.
2. Tap **Add Rule**.
3. Select the device to which the rule applies.
4. Tap **Next**.
5. Set up a port forwarding rule.
 - (1) **Common Protocol/Port**: optional. The App presets some common protocols and their port numbers, such as FTP, TELNET, and so on. Make your selection as required, the **Internal Port Number** and **External Port Number** are auto-filled. If the port numbers you want to set are not included, you can set them manually in the **Internal Port Number** and **External Port Number** boxes.
 - (2) **Internal Port Number**: Enter the service port of the corresponding server on the LAN device.
 - (3) **External Port Number**: Enter the port which is enabled for the internet users.
 - (4) **Protocol**: Select the protocol of the service. If you are uncertain about it, select **TCP&UDP**.
6. Tap **Save**.

Port Forwarding



The port forwarding function enables users to access your LAN resources through the internet. For example, if a web server or an FTP server is set up on a LAN host, users can access the server through the internet after the port forwarding function is configured. Port forwarding is usually used for some proxies, such as the POP3, SMTP, and TELNET proxies.

Add Rule

Select Device

Next



HUAWEI_P10
192.168.5.129

☒



iPhone
192.168.5.101

☐

Port Forwarding Rule

Save



HUAWEI_P10
192.168.5.129

Common Protocol and Port (Optional) >

Internal Port Number

External Port Number

Protocol

After the settings are saved, the IP address currently assigned to this device is bound to the device.

After completing the settings, internet users can visit **“Protocol name://WAN port IP address of the mesh node:External port”** to access LAN resources.



Note

- Ensure that the WAN IP address of the mesh node is a public IP address, and the internal port you entered is correct.
- Security software, antivirus software, and the built-in OS firewall of the server may cause port forwarding function failures. Disable them when using this function.
- Manually set an IP address for the web server to avoid the service disconnection caused by the dynamic IP address.

16 UPnP



After the UPnP function is enabled, it can automatically enable ports for UPnP-supported programs, such as P2P and gaming software, in the internal network to improve your network experience.

Perform the following procedure to enable/disable the UPnP function:

- 1. Choose **Settings > UPnP** to enter the configuration page.
- 2. Alternate the status between enabled and disabled by tapping icon as required.

< UPnP	< UPnP
UPnP is short for Universal Plug and Play. After the UPnP function of the device is enabled, it can automatically enable ports for UPnP-compliant programs (such as P2P and gaming software) in the internal network for smoother network experience.	UPnP is short for Universal Plug and Play. After the UPnP function of the device is enabled, it can automatically enable ports for UPnP-compliant programs (such as P2P and gaming software) in the internal network for smoother network experience.
UPnP	UPnP

17 DHCP Server



The DHCP Server function allows you to change the IP addresses assigned to all devices that are connected to the mesh network.

Perform the following procedure to change the LAN IP address of the mesh node:

1. Choose **Settings** > **DHCP Server** to enter the configuration page.
2. Select a LAN IP address for the mesh node.
3. Tap **Save**.

<

DHCP Server

Save

Configure the IP addresses assigned to network devices.

Current LAN IP Address: 192.168.5.1/255.255.255.0

10

3

172

4

192 . 168 . 5 . 1

6 2

7 3

255 255

18 DNS



If websites are inaccessible with domain names but accessible with IP addresses, it may be a DNS resolution problem. You can try changing the DNS settings to solve the problem.

Perform the following procedure to change the DNS settings:

1. Choose **Settings** > **DNS** to enter the configuration page.
2. Select **Automatic** or **Manual**.
 - **Automatic:** If you select Automatic, the device obtains the Primary DNS Server and Secondary DNS Server from the upstream device.
 - **Manual:** If you select Manual, enter the correct DNS IP address in the Primary DNS Server box. If you have another DNS server IP address, enter it in the Secondary DNS Server (optional) box.
3. Tap **Save**.

<	DNS	Save	<	DNS	Save
	Obtaining Method Automatic	>		Obtaining Method Manual	>
	Primary DNS Server 192.168.60.1			Primary DNS Server 0.0.0.0	
	Secondary DNS Server (optional) 8.8.8.8			Secondary DNS Server (optional) 0.0.0.0	

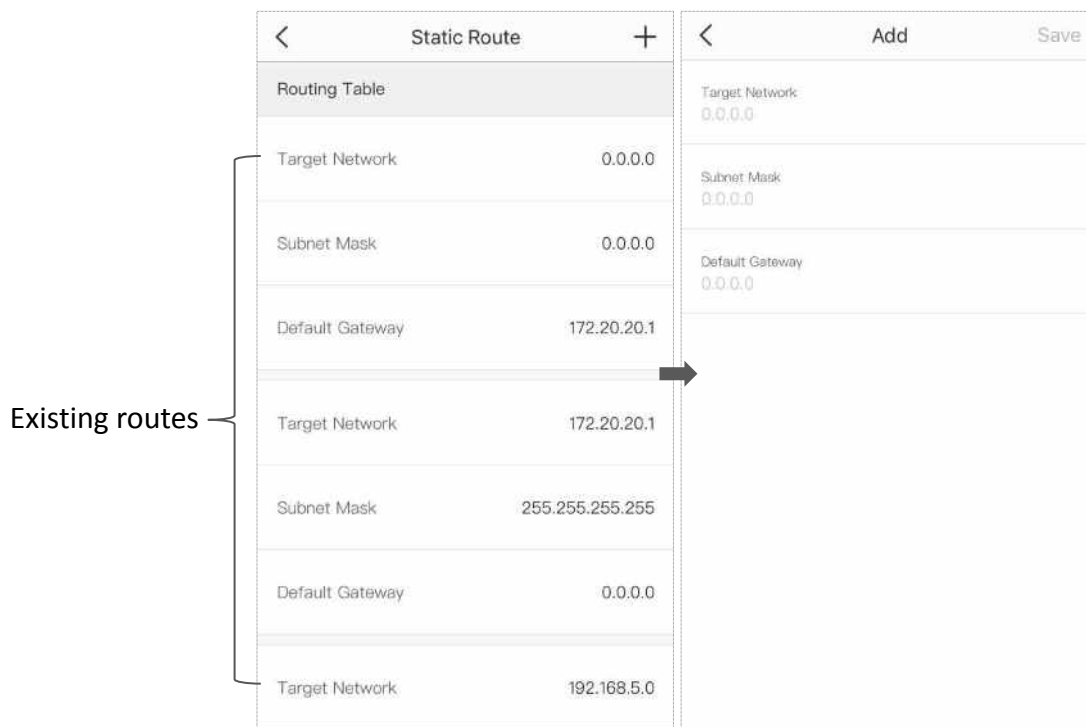
19 Static Route



The Static Route function is performed to select the best route for delivering data from a source address to a destination address. A static route is a manually configured route, which is simple, efficient, and reliable. Appropriate static routes help reduce the number of route selection problems and reduce route selection burden, increasing the packet forwarding speed.

Setting up a static route

1. Choose **Settings > Static Route** to enter the configuration page.
2. Tap the **+** icon.
3. Enter a **Target Network**, a **Subnet Mask**, and a **Default Gateway**.
 - **Target Network:** It specifies the destination IP address.
 - **Subnet Mask:** It specifies the subnet mask of the destination IP address.
 - **Default Gateway:** It specifies the IP address of the gateway. This address must be on the same LAN segment as the router.
4. Tap **Save**.



Application scenario for Static Route

Visiting multiple networks or servers at the same time

A company uses the Mesh system to deploy its networks, and its internal network is isolated from the internet. It requires that devices connected to the mesh network can access the internet and the company's server at the same time.

Solution

- Connect the WAN1 port of EW9 to the internet.
- Connect the WAN2 port of EW9 to the internal network.
- Set static route rules on EW9.

Assume that:

Information of internal network

- IP address: 172.16.0.0
- Subnet mask: 255.255.0.0

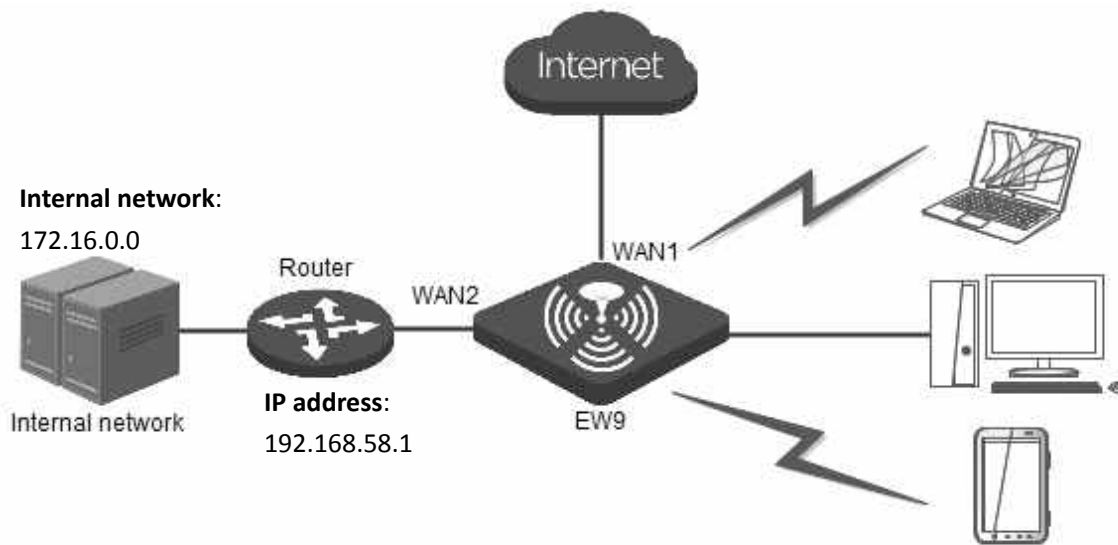
Information for accessing the internal network:

- IP address: 192.168.58.190
- Subnet mask: 255.255.255.0
- Gateway: 192.168.58.1
- Primary DNS: 192.168.58.1

PPPoE user name and password for accessing the internet:

- User name: IP-COM
- Password: IP-COM

The network topology is shown as follows:



Configuration procedure

Step 1 Setting up internet settings



Step 2 Setting up static route rules

■ Setting up the internet settings

1. Choose **Settings > Internet Settings** to enter the configuration page.
2. Tap **Connection Type** of WAN1 port.
3. Select **PPPoE**, and enter the **PPPoE User Name** and **PPPoE Password**, which are **IP-COM** and **IP-COM** in this example.
4. Tap **Save**.
5. Set **Double-line Connection** button to the enabled state .
6. Tap **Connection type** of WAN2.
7. Select **Static IP Address**, and enter the **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary DNS Server**, which are **192.168.58.190**, **255.255.255.0**, **192.168.58.1** and **192.168.58.1** in this example.
8. Tap **Save**.

■ Setting up the static route rules

1. Choose **Settings > Static Route** to enter the configuration page.
2. Tap the **+** icon.
3. Enter the **Target Network**, **Subnet Mask**, and **Default Gateway**, which are **172.16.0.0**, **255.255.0.0**, and **192.168.58.1** in this example.

Static Route

Routing Table

Target Network	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	172.20.20.1

+

Add

Save

Target Network
0.0.0.0

Subnet Mask
0.0.0.0

Default Gateway
0.0.0.0

Static Route

Routing Table

Target Network	172.16.0.0
Subnet Mask	255.255.0.0
Default Gateway	192.168.58.1

+

Edit

Delete

Target Network

Subnet Mask

Default Gateway

172.20.20.1

0.0.0.0

0.0.0.0

192.168.5.0

Click **Edit** to
change the rule.

Click **Delete** to
delete the rule.

Verification

Clients connected to the EW9 can access the internet and the company's server at the same time.

20 Firmware Upgrade



IP-COM is dedicated to improving its products to let users enjoy better performance. Please update the firmware when detecting a new available firmware version.

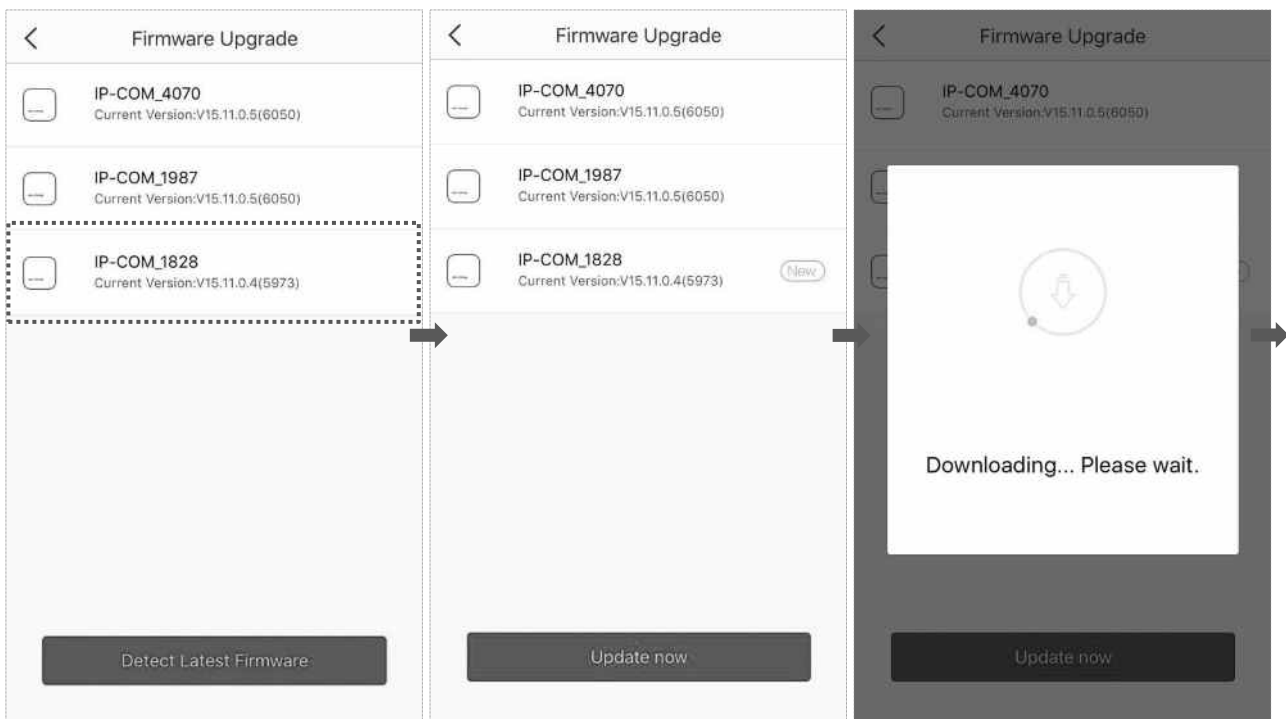
Perform the following procedure to update the firmware:

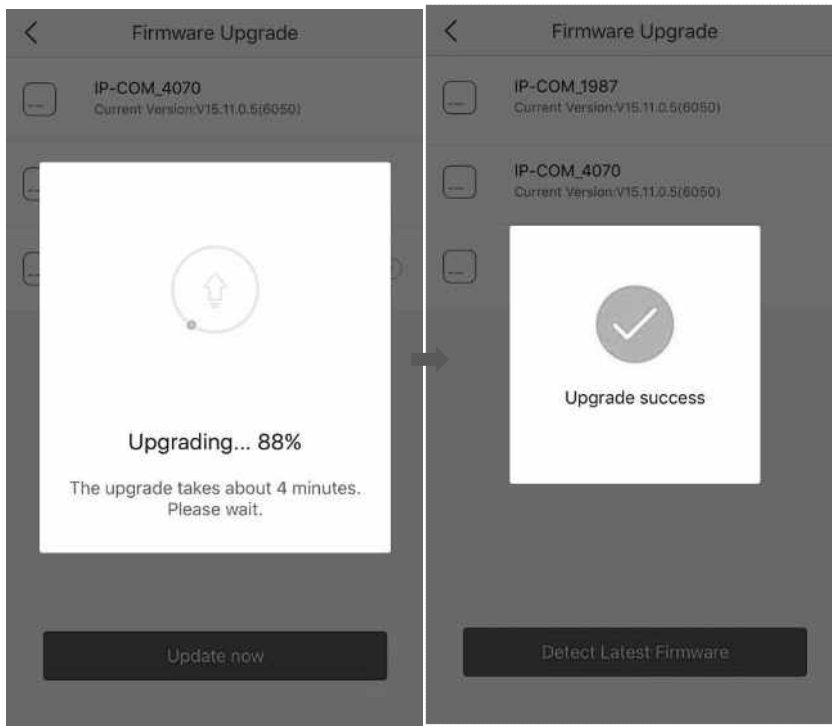


Note

Do not remove the power supply of the mesh nodes when upgrading.

1. Choose **Settings > Firmware Upgrade** to enter the configuration page.
2. Tap **Detect Latest Firmware**.
3. The **New** icon appears if a new firmware version is detected. Tap **Update now** to upgrade these nodes.
4. Wait until all nodes complete the upgrade, and then continue to manage them.





21 Maintenance Schedule



The Maintenance Schedule function makes the mesh nodes reboot at specified time to keep the mesh nodes in good condition.

Perform the following procedure to set up the Maintenance Schedule function:

1. Choose **Settings > Maintenance Schedule** to enter the configuration page.
2. Set the button to the enabled state .
3. Select a **System Reboot Time**. You are recommended to set a time when your network is idle.
4. Select the dates on which the rule takes effect.
5. Enable or disable the **Delay Reboot** function as required.
6. Tap **Save**.



Tip

If the **Delay Reboot** function is enabled, the devices won't reboot at the specified time when the devices are exchanging data and the traffic is greater than 3 KB/s. Within 2 hours after the specified reboot time, the devices keep detecting the traffic, and reboot once when the traffic is lower than 3 KB/s. Otherwise, the devices will reboot the next day at the specified reboot time.

22 Account Authorization



You can authorize other people to manage your mesh network. An authorized account has the same permission as the bound account excluding authorizing other accounts.

Perform the following procedure to authorize another account:

1. Choose **Settings > Account Authorization** to enter the configuration page.
2. Tap **Add an account**.
3. Enter a registered IP-COM account.
4. Tap **OK**.

