tp-link

User Guide

Omada Cloud Controller
OC200

1910012442 REV 1.0.0
September 2018

CONTENTS

1 Quick Start

OC200 is a hardware Omada Cloud Controller, which is running with a built-in software controller. OC200 can manage multiple EAPs centrally just as the software controller does. The difference is that the software controller needs to run in a management host, which is unnecessary for OC200. You just need to pre-configure the OC200, then keep it running in your network.

Follow the steps below to complete the basic settings of OC200.

- *Deploy the OC200*
- *Determine the Management Method*
- *Inform the EAPs of the OC200's Address*
- *Log in to OC200*
- *Create Sites and Adopt EAPs*
- *Monitor and Manage the EAPs*

1.1 Deploy the OC200

There are two kinds of network topologies which are suitable for OC200 deployment:

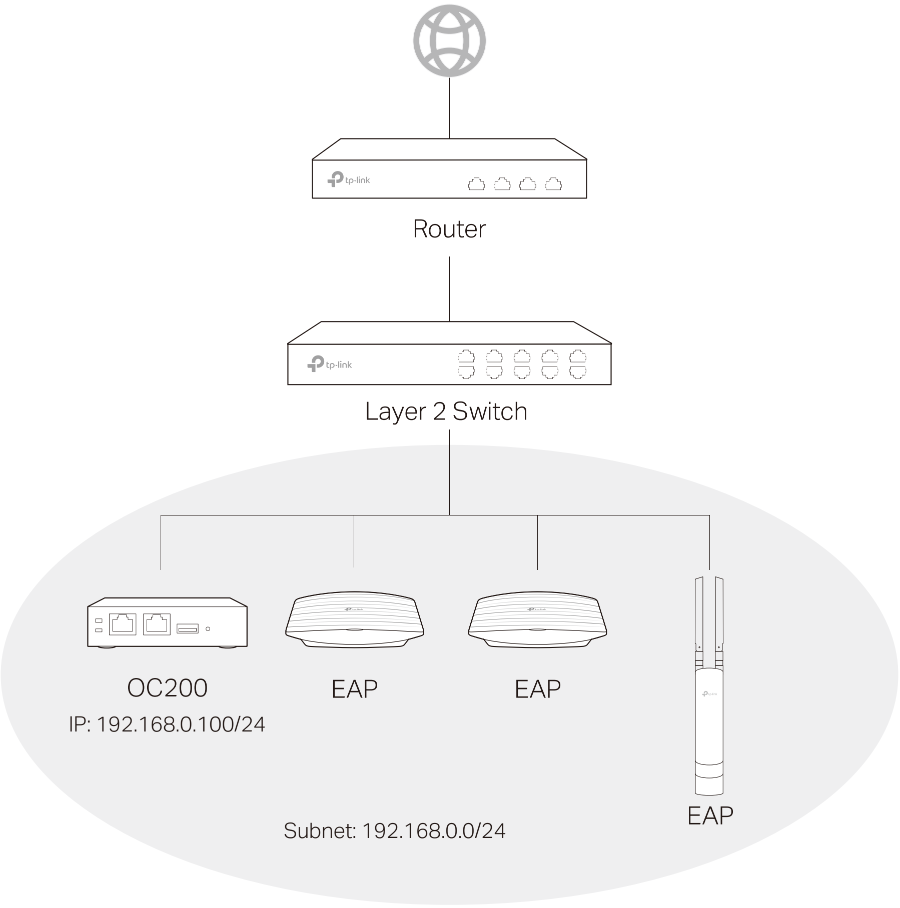
- The OC200 and EAPs are in the same subnet.
- The OC200 and EAPs are in different subnets.

Determine your topology according to your need and refer to the following introductions to build your network topology.

1.1.1 Deploy the OC200 and EAPs in the Same Subnet

If your need to deploy the OC200 and EAPs in the same subnet, refer to the following network topology.

A router acts as a DHCP server to assign IP addresses to EAPs, clients and OC200. The OC200 and the EAPs are in the same subnet.

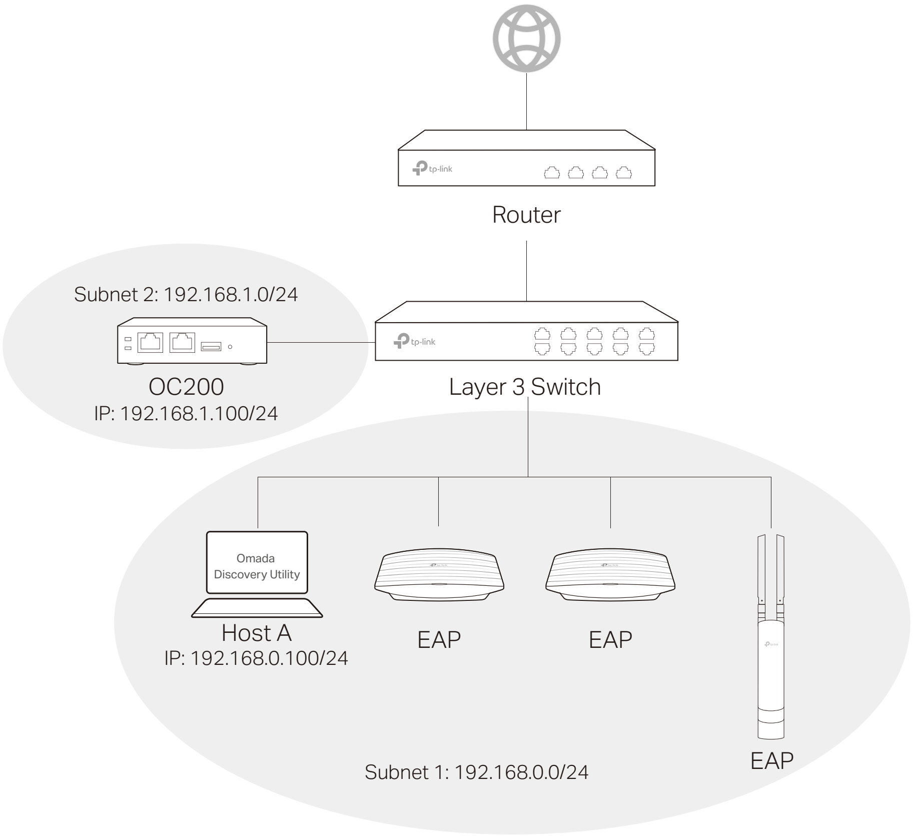


1.1.2 Deploy the OC200 and EAPs in Different Subnets

If your need to deploy the OC200 and EAPs in different subnets, refer to the following network topology.

A router acts as the gateway of the network. A layer 3 switch acts as a DHCP server to assign IP addresses to EAPs, OC200 and clients. The EAPs are in subet 1, of which the IP network segment is 192.168.0.0/24; the OC200 is in subnet 2, of which the IP network segment is 192.168.1.0/24.

For the EAPs and the OC200 are in the different networksegment, the EAPs cannot find the OC200 directly. To help the EAPs find the OC200, you need to install an Omada Discover Utility on a host which is in the same subnet with the EAPs. For how to use Omada Discovery Utility, refer to Inform the EAPs of the OC200's Address.



1.2 Determine the Management Method

OC200 supports two flexible management methods to centrally manage EAPs:

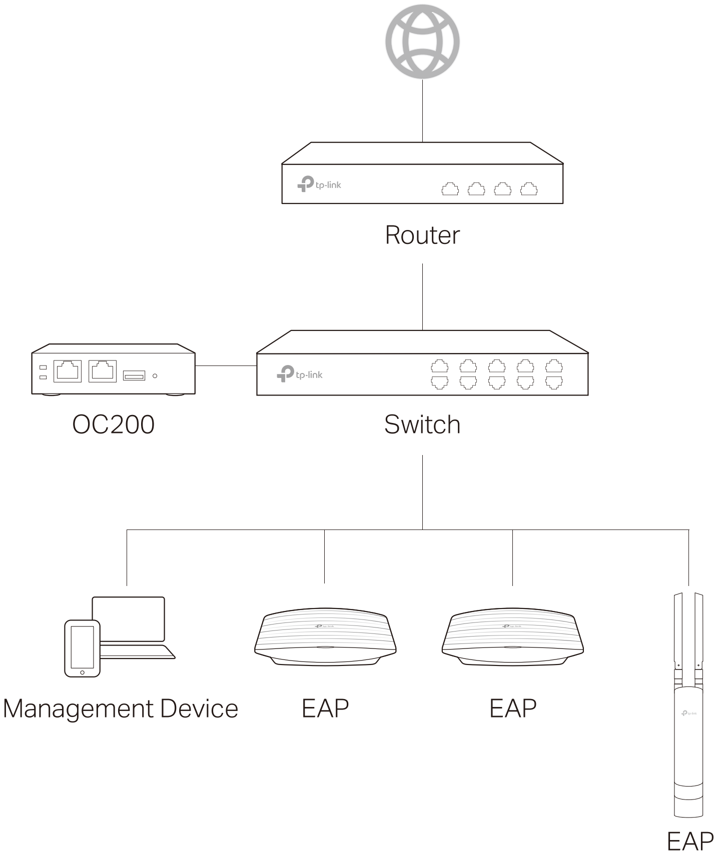
- Management on the local network

- Management via Cloud Access

Determine your management method according to your need and refer to the following introductions to build your network toplogy.

1.2.1 Management on the Local Network

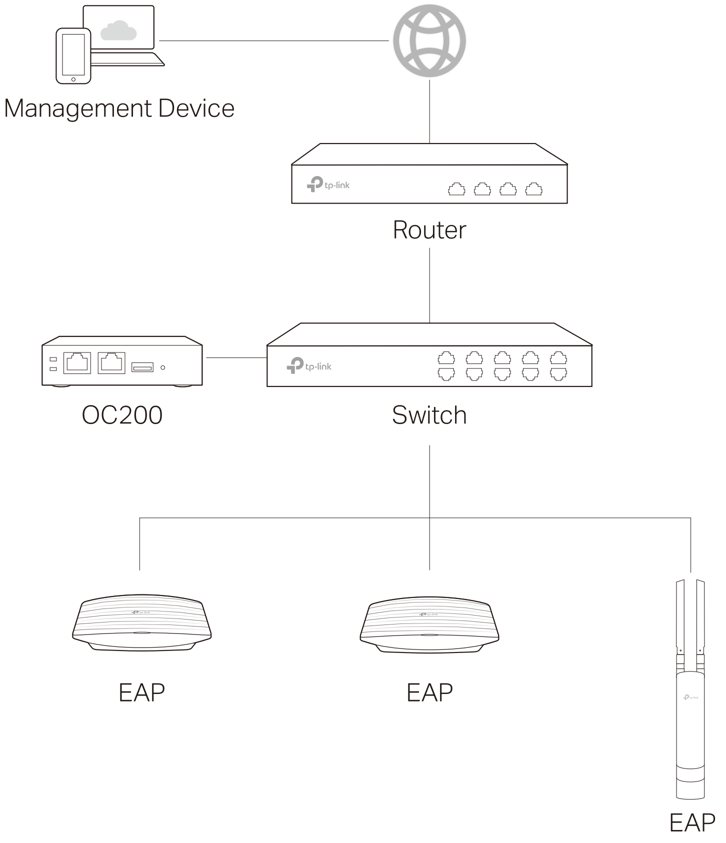
To manage EAPs locally, please deploy your management host on the local network. The following topology is an example for the deployment of the management host. As long as there is a route for the management host to access the OC200, the management host can log in to the OC200 to manage the EAPs. For how to log in to the OC200, please refer to *On the Local Network*.



1.2.2 Management via Cloud Access

If you need to manage EAPs remotely, for example, your EAPs are in your office but you want to manage them at home, you can manage the EAPs via cloud access.

The following topology is a typical example. You just need to deploy your OC200 and EAPs on your local network, and use a management device to control them remotely. On the management device, you can open a web browser to remotely launch the OC200 via Omada Cloud. For more details about Cloud Access, refer to *Omada Cloud Service.*



1.3 Inform the EAPs of the OC200's Address

If your OC200 and EAPs are in the same network subnet, you can skip this section.

If your OC200 and EAPs are in different subnets, you need to install Omada Discovery Utility on a host that is in the same network segment with the EAPs. Omada Discovery Utility can help EAPs find the OC200.

System Requirements

Windows 7/8/10/Server

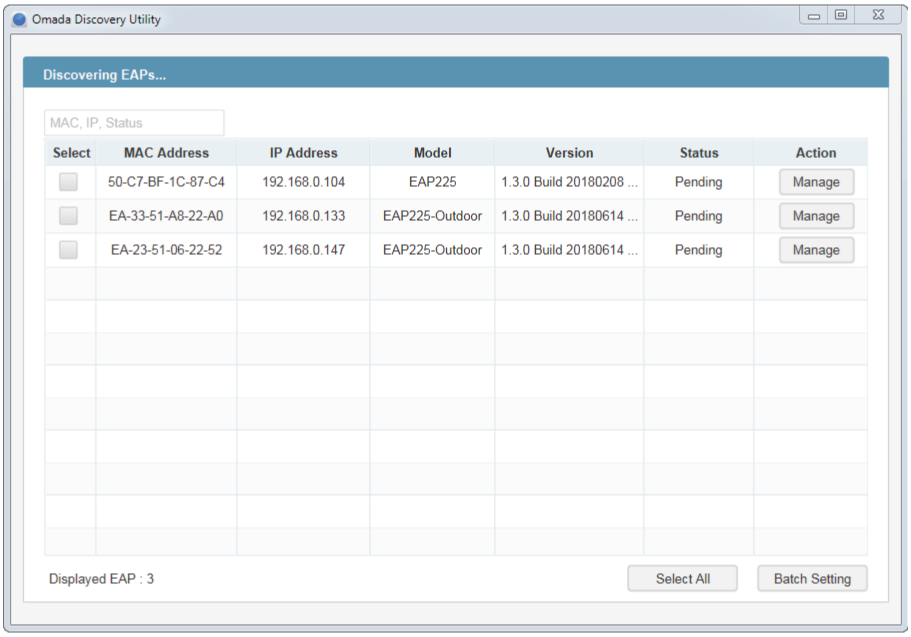
Mac OS X 10.7/10.8/10.9/10.10/10.11

Install and Use Omada Discovery Utility

Follow the steps below to install Omada Discovery Utility and use it to inform the EAPs of the OC200's IP address:

1. Download the installation file from the website *https://www.tp-link.com/en/download/EAP-Controller.html#EAP_Discovery_Tool*. Then follow the instructions to properly install Omada Discovery Utility.

2. Open the Omada Discovery Utility and the following window will pop up. This window shows the information of all EAPs in the same LAN.



Discovering EAPs...

MAC, IP, Status

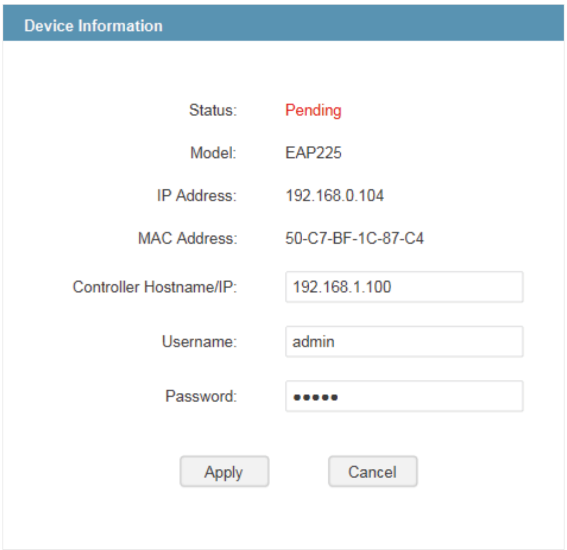
Select	MAC Address	IP Address	Model	Version	Status	Action
□	50-C7-BF-1C-87-C4	192.168.0.104	EAP225	1.3.0 Build 20180208 ...	Pending	Manage
□	EA-33-51-A8-22-A0	192.168.0.133	EAP225-Outdoor	1.3.0 Build 20180614 ...	Pending	Manage
□	EA-23-51-06-22-52	192.168.0.147	EAP225-Outdoor	1.3.0 Build 20180614 ...	Pending	Manage

Displayed EAP : 3

3. Click **Manage** in the **Action** column or select multiple EAPs and click **Batch Setting**.

4. Enter the hostname or IP address of the OC200.

5. Enter the EAP's username and password (both are admin by default).



Device Information

Status: Pending

Model: EAP225

IP Address: 192.168.0.104

MAC Address: 50-C7-BF-1C-87-C4

Controller Hostname/IP: 192.168.1.100

Username: admin

Password: •••••

6. Click **Apply** to inform the EAP of the OC200's hostname or IP address. And then the connection can be established between the EAP and the OC200.

1.4 Log in to OC200

To use OC200 to manage EAPs, you first need to log in to OC200. There are two situations:

- Login in to the OC200 on the local network
- Login in to the OC200 via Omada cloud

1.4.1 On the Local Network

Follow the steps below to enter the management interface of OC200 on the local network:

1. Make sure that your management device has the route to access the OC200.
2. Check the DHCP server (typically a router) for OC200's IP Address. The default fallback IP of address OC 200 is 192.168.0.253.

   Tips: The fallback IP address is used when OC200 fails to get dynamic IP address from the DHCP server
3. Launch a web browser and type OC200's IP address in the address bar, then press **Enter** (Windows) or **Return** (Mac).

1.4.2 Via Omada Cloud

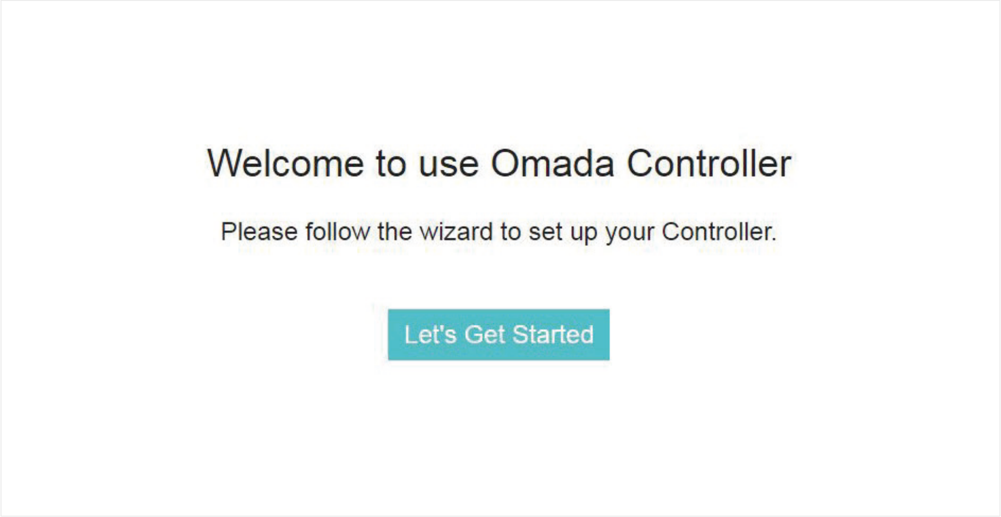
Follow the steps below to log in to OC200 via Omada cloud:

1. Make sure that your management device and OC200 can access the internet.
2. Launch a web browser and visit **https://omada.tplinkcloud.com** in the address bar, then press **Enter** (Windows) or **Return** (Mac).
3. Enter your TP-Link ID and password to log in. Then click **Add Cloud Controller** and follow the instructions to add your OC200.
4. Click **Launch** in the **Action** column to visit the management interface of OC200.

1.4.3 Do the Basic Configurations

In the web browser you can see the configuration page. Follow the setup wizard to complete the basic settings for OC200.

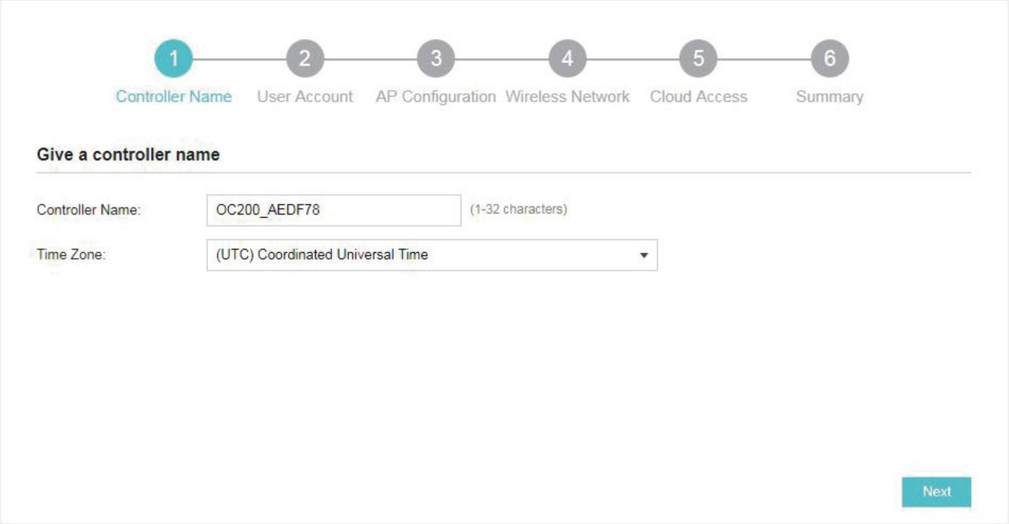
1. Click **Let's Get Started.**



Welcome to use Omada Controller

Please follow the wizard to set up your Controller.

2. Specify a name for OC200 and select the time zone. Click **Next.**

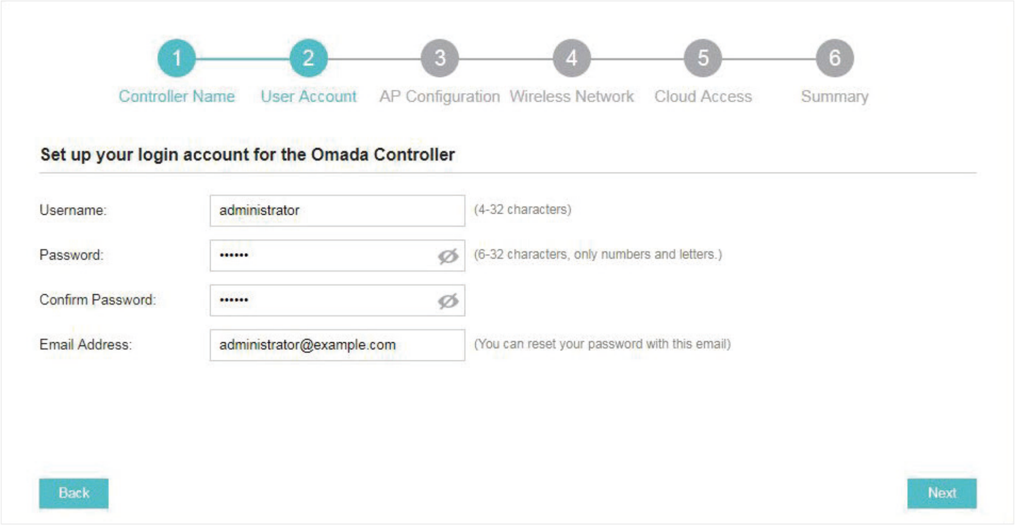


Give a controller name

Controller Name: OC200_AEDF78 (1-32 characters)

Time Zone: (UTC) Coordinated Universal Time

3. Specify a username and password for the login account. Specify the email address to receive the emails and reset your password if necessary. Click **Next.**



Set up your login account for the Omada Controller

Username: administrator (4-32 characters)

Password: •••••• (6-32 characters, only numbers and letters.)

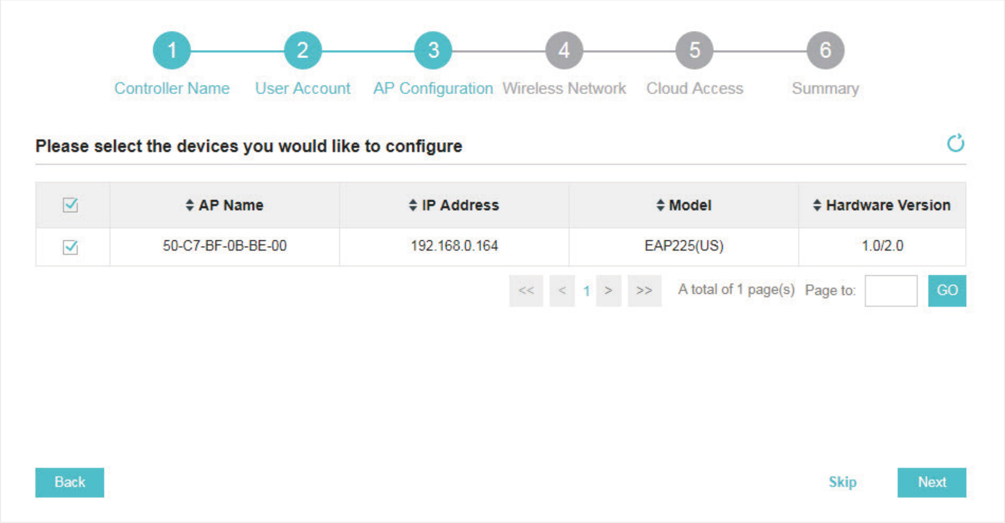
Confirm Password: ••••••

Email Address: administrator@example.com (You can reset your password with this email)

Note:

After logging into OC200, set a mail server so that you can receive emails and reset your password in case that you forget the password. Please refer to Configure Mail Server.

4. The setup page displays all the detected EAPs in the network. Select one or more EAPs to be managed and click **Next**.

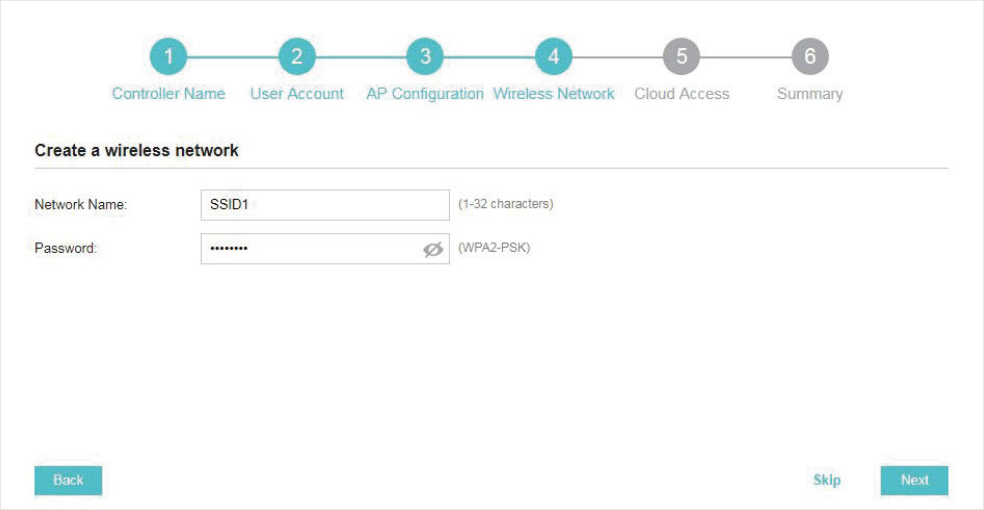


Please select the devices you would like to configure

☑	AP Name	IP Address	Model	Hardware Version
☑	50-C7-BF-0B-BE-00	192.168.0.164	EAP225(US)	1.0/2.0

A total of 1 page(s) Page to:

5. Set an SSID name (wireless network name) and password for the EAPs to be managed. OC200 will create two wireless networks, a 2.4GHz one and a 5GHz one, both encrypted in WPA2-PSK mode. Click **Next**.

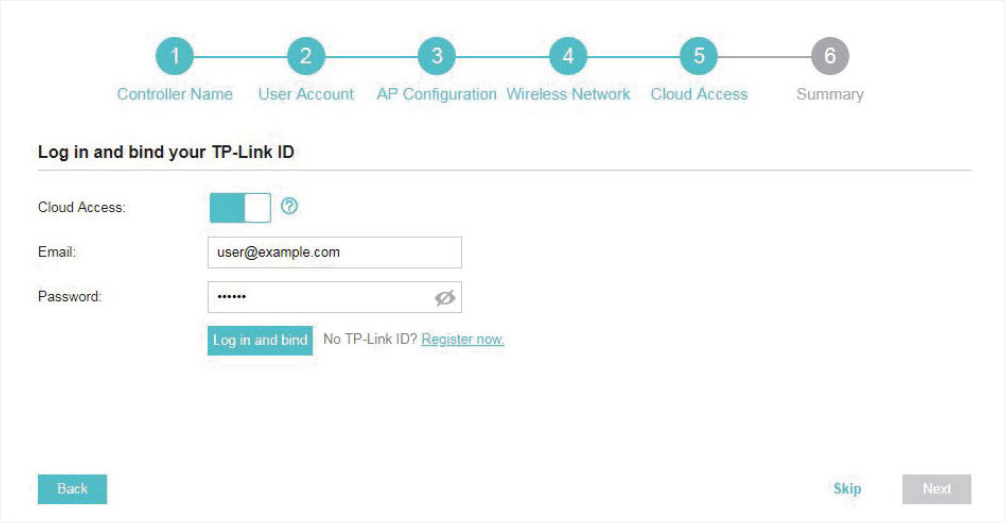


Create a wireless network

Network Name: SSID1 (1-32 characters)

Password: •••••••• (WPA2-PSK)

6. If you want to manage EAPs via Omada cloud, enable the **Cloud Access** button, and bind your TP-Link ID to your OC200, and then click **Next**. If you want to manage EAPs on the local network, you can just click **Skip**. For more details about Omada Cloud, please refer to *Omada Cloud Service.*



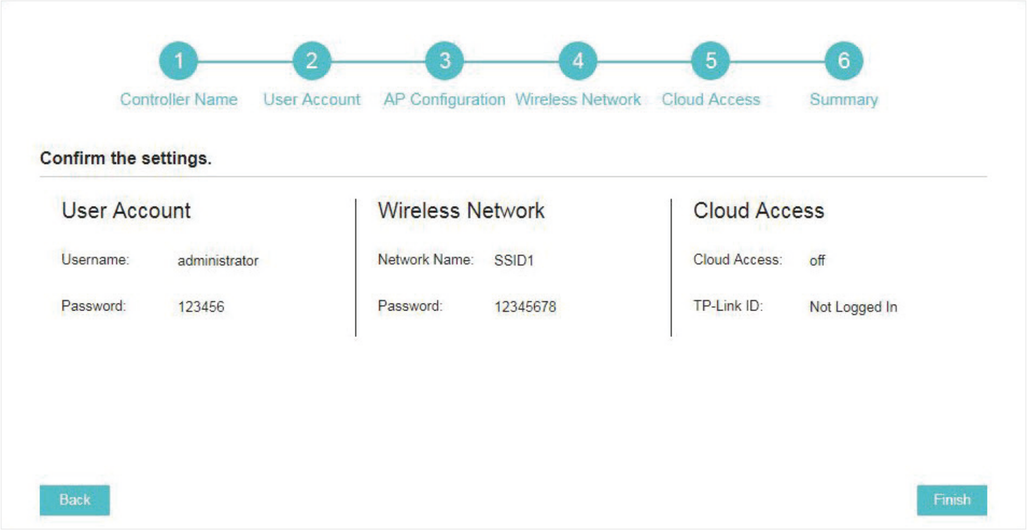
Log in and bind your TP-Link ID

Cloud Access: ON

Email: user@example.com

Password: ••••••

7. Review your settings and click **Finish**.

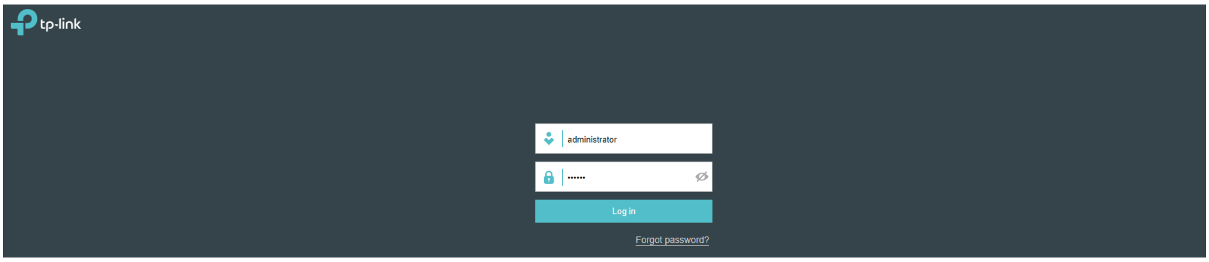


Confirm the settings.

User Account		Wireless Network		Cloud Access	
Username:	administrator	Network Name:	SSID1	Cloud Access:	off
Password:	123456	Password:	12345678	TP-Link ID:	Not Logged In

1.4.4 Log In to the Management Interface

Once the basic configurations are finished, the browser will be redirected to the following page. Log in to the management interface using the username and password you have set in the basic configurations.



administrator

••••••

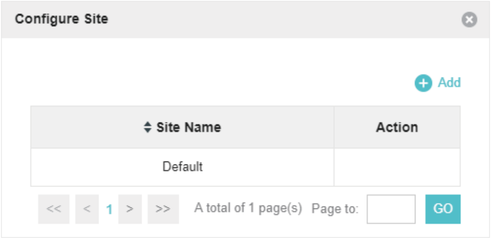
1.5 Create Sites and Adopt EAPs

OC200 can manage multiple EAP networks, which are called sites. Multiple sites are logically separated, and each site has its own configurations. There is an initial site named **Default**. If you have no need to manage EAPs with differnt sites, you can use the default site and skip the **Create Sites** section. However, **Adopt the EAPs** is a necessary step to manage the EAPs.

1.5.1 Create Sites

Follow the steps below to add sites.

1. Click **Sites:** Default ⌄ in the top left corner of the page and select Add/Edit Site, and then the following window will pop up.



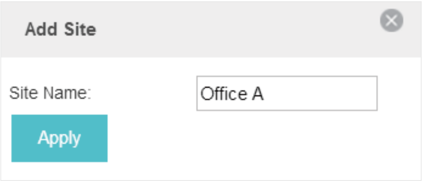
Configure Site ⊗

⊕ Add

⇕ Site Name	Action
Default	

<< < 1 > >> A total of 1 page(s) Page to: GO

2. Click ⊕ Add and set a name for the site.



Add Site ⊗

Site Name: Office A

Apply

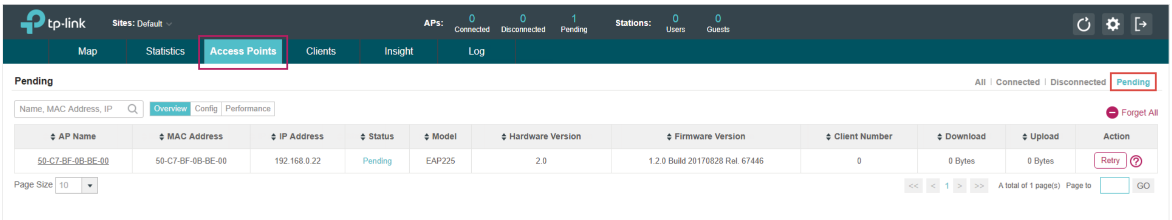
3. Click **Apply** to create the site.

1.5.2 Adopt the EAPs

OC200 can discover all EAP devices currently connected in the network and display their connection status. All EAPs are in **Pending** status when first discovered by OC200. To manage the EAPs, you need to adopt them. In the quick setup process, OC200 will automatically adopt the selected EAPs using the default username and password (both are admin). However, if you have changed the username or password of your EAPs before, OC200 cannot automatically adopt them, and you need to refer to the following steps to adopt them manually.

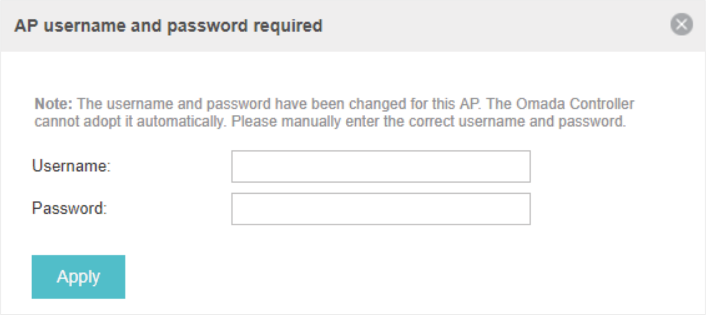
To ensure that all EAPs are adopted, follow the steps below:

1. Select a site and go to **Access Points > Pending**. The table displays all the EAPs that have not been adopted.



AP Name	MAC Address	IP Address	Status	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
50-C7-BF-0B-BE-00	50-C7-BF-0B-BE-00	192.168.0.22	Pending	EAP225	2.0	1.2.0 Build 20170828 Rel. 67446	0	0 Bytes	0 Bytes	Retry

2. Click the **Retry** button in the **Action** column and enter the current username and password of the EAP. Click **Apply**.


AP username and password required

Note: The username and password have been changed for this AP. The Omada Controller cannot adopt it automatically. Please manually enter the correct username and password.

Username:

Password:

Tips:

- If you have a new discovered EAP, you can click the **Adopt** button in the **Action** column to adopt the EAP. OC200 will automatically adopt the EAP using the default username and password (both are admin).
- If you have multiple new discovered EAPs, and all of them have the default username and password (both are admin), you can click the **Batch Adopt** button to adopt them in batch. But if there are any EAPs with the Retry button, it means that the username and password of these EAPs have been changed. You need to first adopt them before batch adopt the rest EAPs.

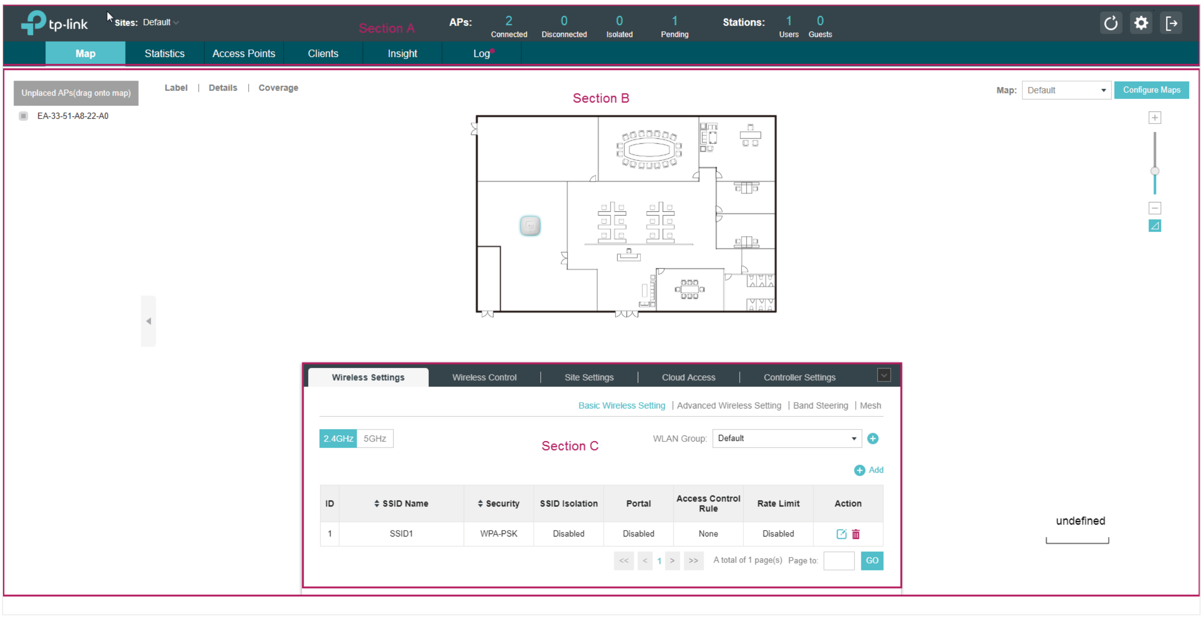
3. After EAPs are adopted, the status will change from **Pending** to **Connected.** All the EAPs' username and password will become the same as those of the OC200's administrator account you created in the Basic Configuration.

Tips:

If you want to change the EAPs' username and password, refer to Device Account.

1.6 Monitor and Manage the EAPs

When all the configurations above are finished, you can centrally monitor and manage the EAPs via the OC200's management interface. The management interface is divided into three sections as the following figure shows.



ID	SSID Name	Security	SSID Isolation	Portal	Access Control Rule	Rate Limit	Action
1	SSID1	WPA-PSK	Disabled	Disabled	None	Disabled	

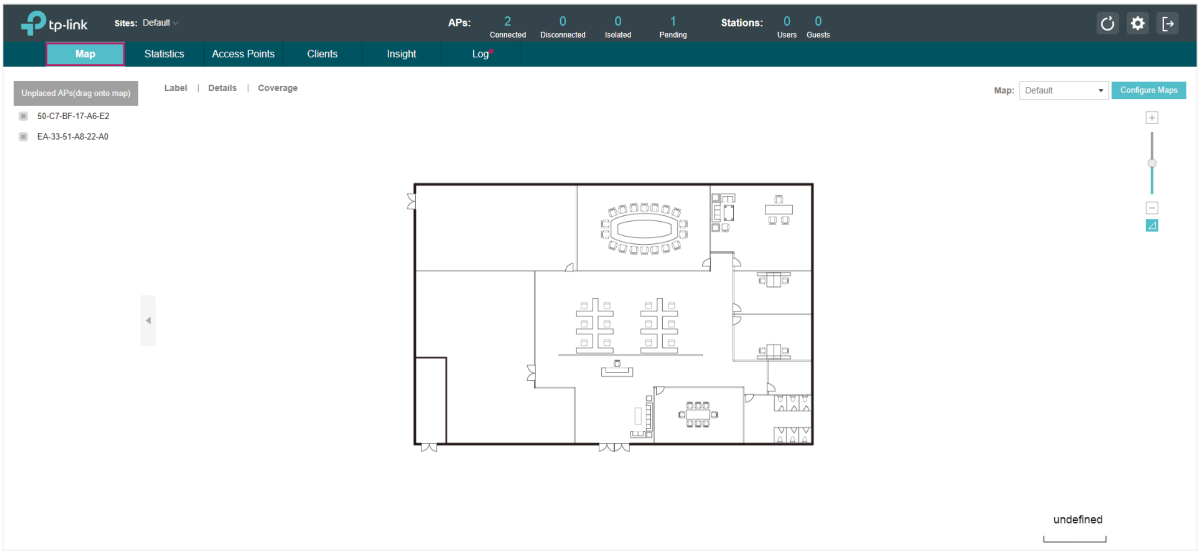
Section A	In Section A, you can check the status of EAPs and clients in the network. Also, you can click ⟳ to refresh the current page, click ⚙ to globally configure the wireless network, and click ⇥ to sign out from the management interface. Furthermore, the **Sites** allows you to group your EAPs and manage them in batches. To configure sites, refer to Create Sites.
Section B	In Section B, you can centrally monitor and manage the EAPs and clients.
Section C	In Section C, you can globally configure the wireless network. The global configurations will take effect on all the adopted EAPs.

2 Monitor and Manage the Network

With OC200 you can monitor the EAP devices and centrally manage your wireless network. This chapter includes the following sections:

2.1 Monitor the Network with the Map

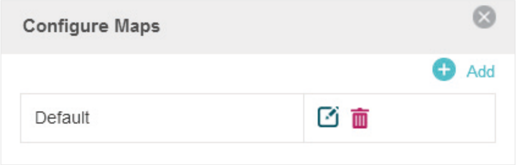
You can upload your local map images and monitor the status and coverage range of each EAP with the map. When you initially launch OC200, a default map is displayed as the following figure shows. Follow the instructions below to add your own map and manage the EAPs via the map.



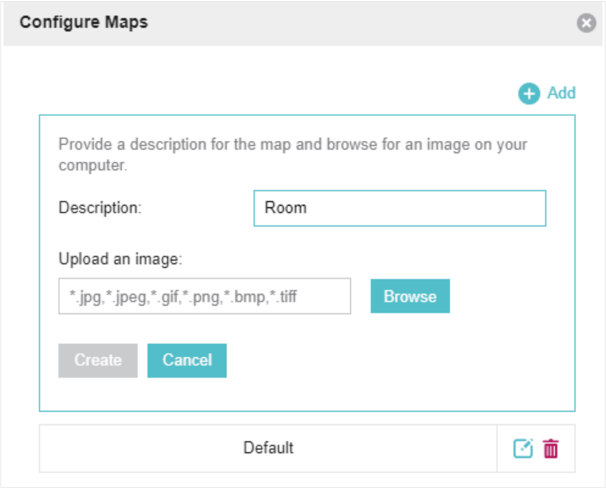
2.1.1 Add a Map

Prepare a map image in .jpg, .jpeg, .gif, .png, .bmp, .tiff format. And then follow the steps below to add the map to the OC200.

1. Click **Configure Maps** on the upper right corner of map and click **Add.**



2. Enter the map description, select your map image, and click **Create.**

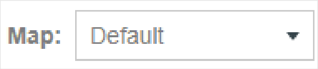


Provide a description for the map and browse for an image on your computer.

Description: Room

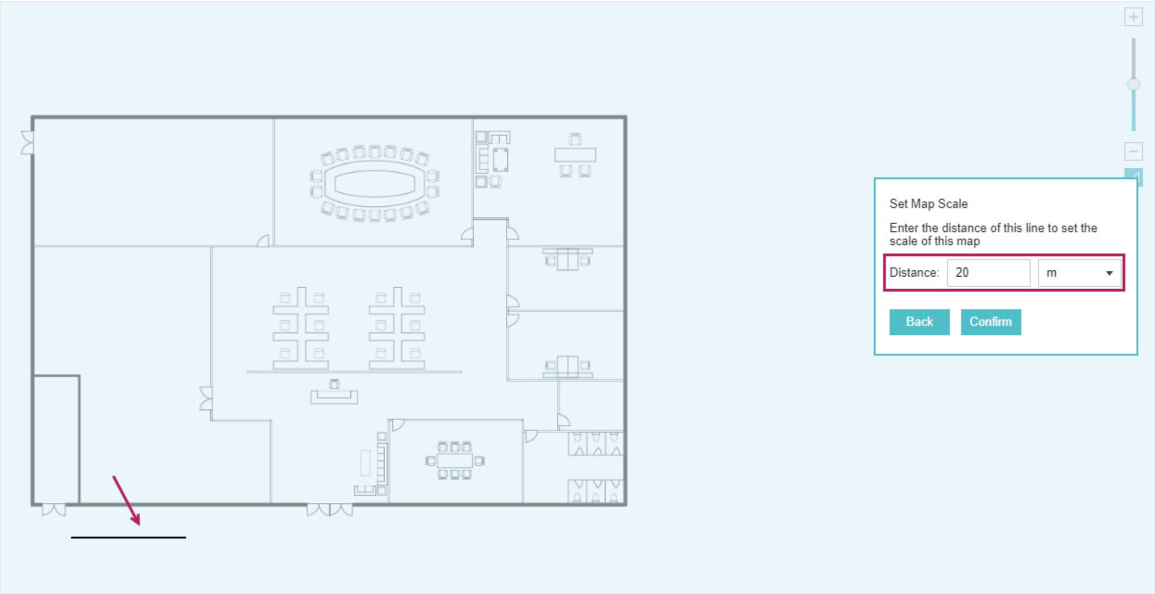
Upload an image: *.jpg,*.jpeg,*.gif,*.png,*.bmp,*.tiff

3. Select your local map from the drop-down list on the upper right corner of map area.



Map: Default ▾

4. Click ◿ . Draw a line on the map and enter the distance the line represents. Then the OC200 will compute and generate the map scale automatically based on your configuration.

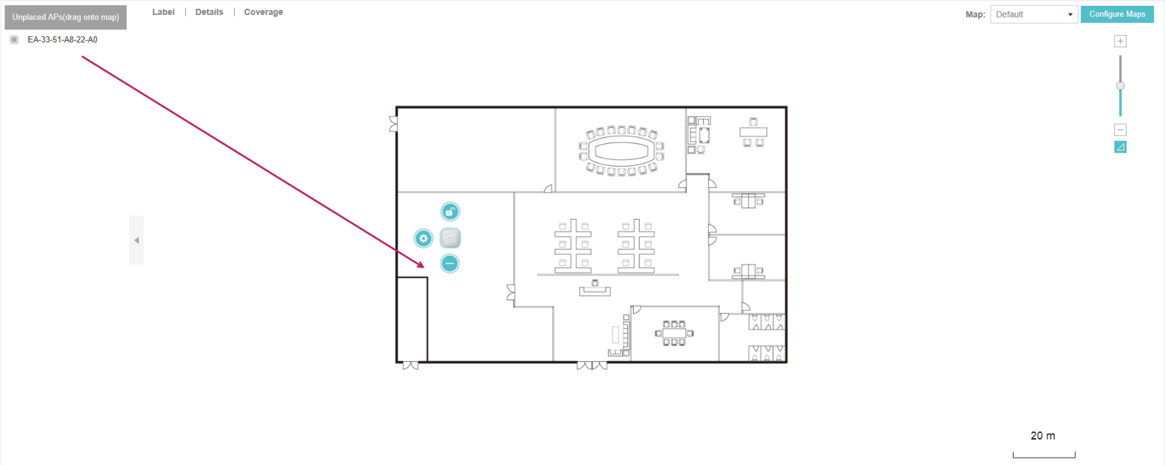


Set Map Scale

Enter the distance of this line to set the scale of this map

Distance: 20 m ▾

5. Drag the EAPs from the **Unplaced APs** list to the appropriate locations on the map according to their actual locations.

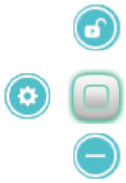


Unplaced APs(drag onto map)

EA-33-51-A8-22-A0

Map: Default ▾

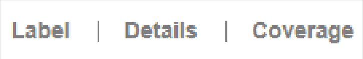
You can click ▢ to reveal additional options:



🔒	Lock the selected EAP in the current location on the map.
🔓	Unlock the selected EAP and you can drag it to another location.
⚙	Display the EAP's details and configure the wireless parameters. Refer to *Configure the EAPs Separately*.
⊖	Remove the selected EAP back into the Unplaced APs list.

2.1.2 Monitor the EAPs on the Map

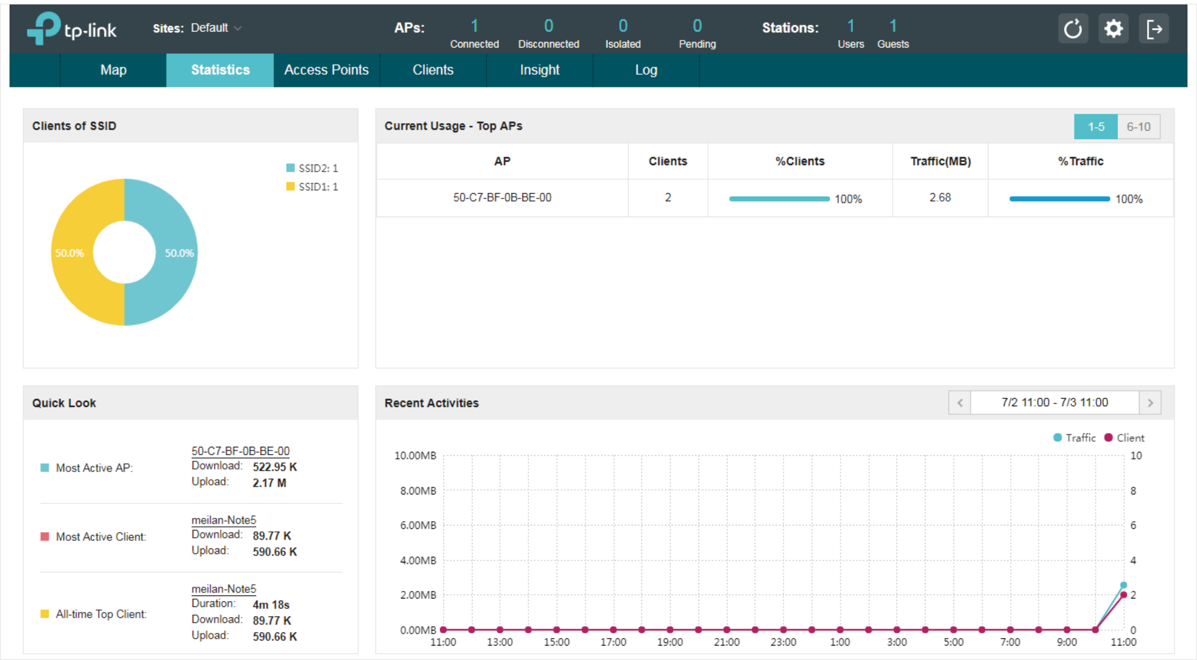
Click any of the following options to display EAP Label, Details, and Coverage on the map.



Label	Display the EAP’s name. The default name is the MAC address of the EAP.
Details	Display the EAP’s name, MAC address, IP address, transmitting/receiving channel, number of connected users, and number of connected guests.
Coverage	Display a visual representation of the wireless range covered by EAPs. The actual signal coverage may be smaller than the visual coverage on the map because the obstacles around the EAPs will weaken the signal.

2.2 View the Statistics of the Network

OC200 collects all statistics of the managed EAPs and displays the statistical information via graphs, pie charts and tables, providing an overview of your wireless network.



AP	Clients	%Clients	Traffic(MB)	%Traffic
50-C7-BF-0B-BE-00	2	100%	2.68	100%

Quick Look

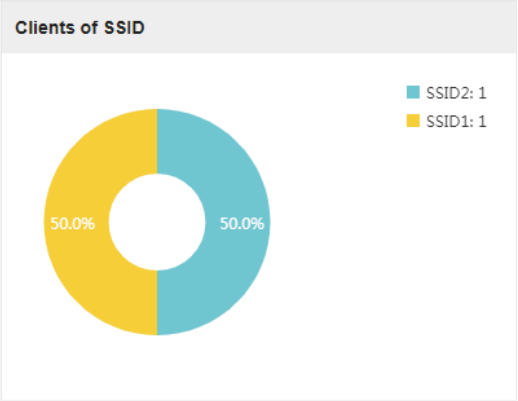
Most Active AP: 50-C7-BF-0B-BE-00
Download: 522.95 K
Upload: 2.17 M

Most Active Client: meilan-Note5
Download: 89.77 K
Upload: 590.66 K

All-time Top Client: meilan-Note5
Duration: 4m 18s
Download: 89.77 K
Upload: 590.66 K

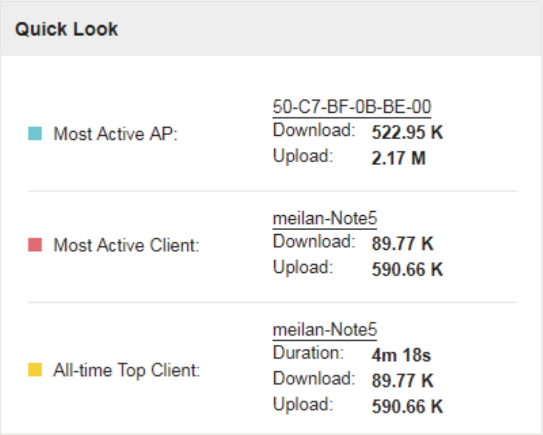
2.2.1 View the Client Distribution on SSID

A visual pie chart shows the client distribution on each SSID. For example, the SSID1 has one client, which occupies 50% of all the clients.



2.2.2 Have a Quick Look at EAPs and Clients

This tab displays the **Most Active AP**, the **Most Active Clients** and the **All-Time Top Client**. You can click the MAC address of the EAP or the client to see more details.



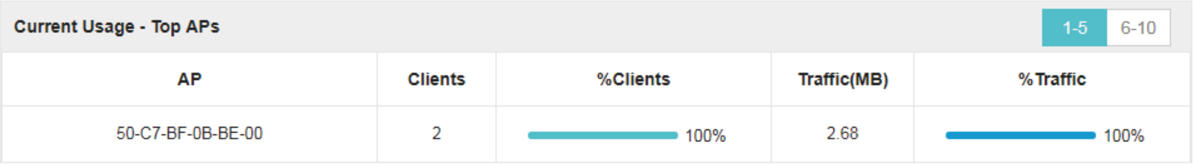
Quick Look

🟦 Most Active AP:	50-C7-BF-0B-BE-00 Download: 522.95 K Upload: 2.17 M
🟥 Most Active Client:	meilan-Note5 Download: 89.77 K Upload: 590.66 K
🟨 All-time Top Client:	meilan-Note5 Duration: 4m 18s Download: 89.77 K Upload: 590.66 K

Most Active AP	The current connected AP with the maximum traffic.
Most Active Client	The current connected client with the maximum traffic.
All-time Top Client	The client with the maximum traffic among all the clients that have ever accessed the EAP network.

2.2.3 View Current Usage-Top EAPs

This tab lists the number of connected clients and the data traffic condition of the ten APs that use the most traffic currently.



Current Usage - Top APs

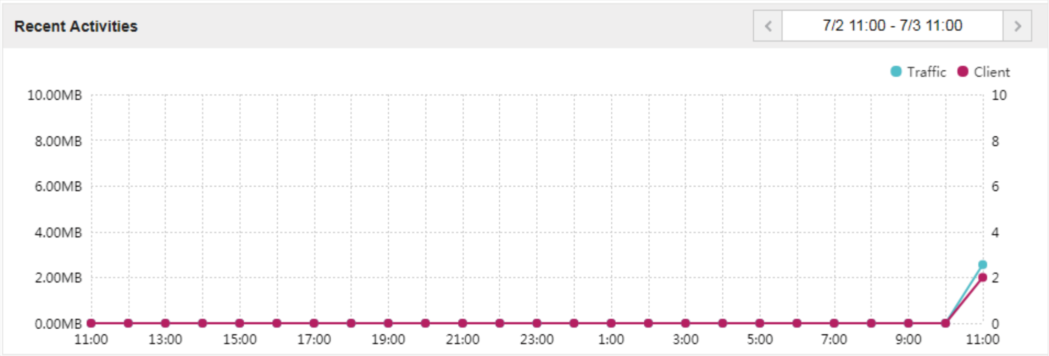
AP	Clients	%Clients	Traffic(MB)	%Traffic
50-C7-BF-0B-BE-00	2	100%	2.68	100%

Clients	The amount of clients connected to this EAP.
%Clients	The proportion of current connected clients to the Top EAPs' total client amount.
Traffic (MB)	The total amount of data transmitted by this EAP, which equals the sum of the transmission traffic of all the current clients that connect to the AP.
%Traffic	The proportion of the EAP's current data transmission amount to the Top EAPs' total transmission amount.

2.2.4 View Recent Activities

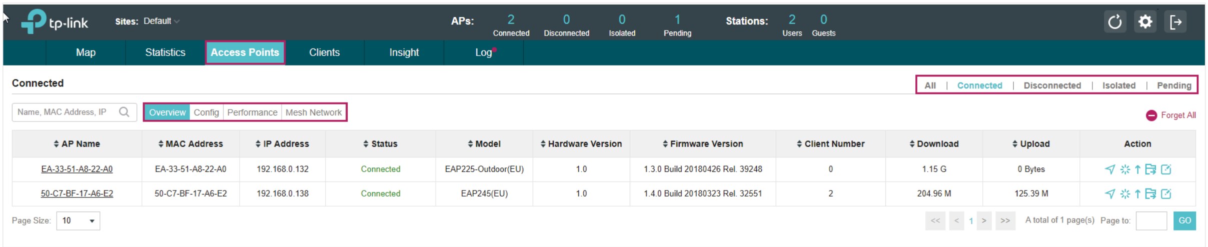
The **Recent Activities** statistics can be toggled between a view for the past specific 24 hours and one for the past specific 30 days.

The left ordinate axis indicates the traffic and the right one represents the number of the clients. The abscissa axis shows the selected time period. **Traffic** indicates a visual graph of the network traffic during the selected time period. **Client** indicates a visual graph of the number of the connected clients during the selected time period. For example, the statistics information at 15:00 indicates the traffic size and client number from 14:00 to 15:00. In the following figure, at 11 o'clock, the traffic is about 3MB and there is 2 clients connected to the AP.



2.3 Monitor and Manage the EAPs

OC200 can discover all the EAP devices currently connected to the network and display the information of them on the **Access Points** page.



AP Name	MAC Address	IP Address	Status	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
EA-33-51-A8-22-A0	EA-33-51-A8-22-A0	192.168.0.132	Connected	EAP225-Outdoor(EU)	1.0	1.3.0 Build 20180426 Rel. 39248	0	1.15 G	0 Bytes	
50-C7-BF-17-A6-E2	50-C7-BF-17-A6-E2	192.168.0.138	Connected	EAP245(EU)	1.0	1.4.0 Build 20180323 Rel. 32551	2	204.96 M	125.39 M	

2.3.1 Manage the EAPs in Different Status

According to their connection status, EAPs are divided into four categories: connected, disconnected, isolated and pending. You can view the EAPs in different status on different pages:

All

Displays the information of all EAPs in different status.

Connected

Displays the connected EAPs.

The status of connected EAPs includes two cases: **Connected** and **Connected (Wireless)**.

Connected: After you adopt a wired EAP in Pending status, its status will become Provisioning, then Configuring and Connected eventually.

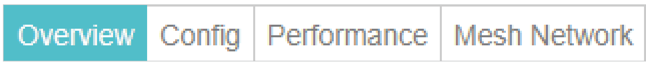
Connected (Wireless): In a mesh network, if an EAP has a successful wireless uplink, its status will become Adopting (Wireless) and then Connected (Wireless).

Only connected EAPs can be managed. A connected EAP will turn into a pending one after you **forget** it. You can refer to *Forget this AP* to forget an EAP or click **Forget All** on the page to forget all the connected EAPs.

Disconnected	Displays the disconnected EAPs. If a connected EAP powers off or disconnects from the OC200, it will be in Disconnected status. When a disconnected EAP is reset to factory defaults or forgot, it will turn into a pending one again. You can refer to *Forget this AP* to forget a EAP or click **Forget All** on the page to forget all the disconnected EAPs.
Isolated	Displays the isolated EAPs. In a mesh network, when the EAP which has been managed before by OC200 connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state. The isolated EAP searches for wireless uplink and the LED on the device turns green and flashes off every 5 seconds. To know more about mesh network, refer to *Configure Mesh*.
Pending	Displays the pending EAPs. The status of pending EAPs includes three cases: **Pending**, **Pending (Wireless)** and **Managed by others**. **Pending:** All the EAPs with wired network connection are in pending status by default when first discovered by OC200. **Pending (Wireless):** The factory default EAP with mesh functions and no wired network connection is in Pending (Wireless) status when first discovered by OC200. **Managed by others:** An EAP is located on the same network as the OC200, but has been already managed by an existing Omada controller before. You can provide the username/password to unbind the EAP from the existing controller and begin adoption in current controller. Only after pending EAPs are adopted and connected, you can manage them. To adopt pending EAPs, refer to *Adopt the EAPs*.

2.3.2 View the Detailed Information of EAPs

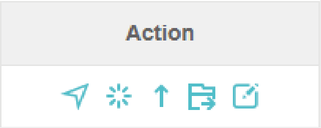
You can click **Overview**, **Config**,**Performance or Mesh Network** tab to view different detailed information of EAPs.



Overview	Displays the EAP's name, MAC address, IP address, status, model, hardware version, firmware version, number of connected clients and download/upload bytes.
Config	Displays the EAP's name, MAC address, IP address, status, model, hardware version, firmware version, WLAN Group bounded with the 2G and 5G of the EAP, and radio of the 2G and 5G.
Performance	Displays the EAP's name, MAC address, IP address, status, model, hardware version, firmware version, number of connected 2G clients and 5G clients, TX(Downloaded Traffic), RX(Uploaded Traffic), TX 2G and TX 5G.
Mesh Network	Displays the EAP's name, MAC address, IP address, status, model, hardware version, firmware version, number of connected clients, hops, uplink APs and downlink APs.

2.3.3 Manage the EAPs in the Action Column

You can execute the corresponding operation to the EAP by clicking an icon in the **Action** column.



Action

➤ ✳ ↑ 🗂 ✎

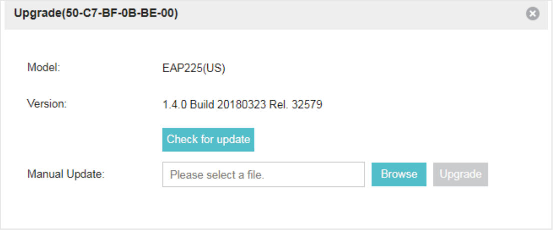
➤ Locate the EAP in the map.

✳ Reboot the EAP.

↑ Upgrade the EAP.

You can click Check for upgrade to detect if the current firmware is the latest version. The latest firmware for the EAP can be detected by the controller automatically. And you can upgrade the EAP online.

Click **Browse** to locate and choose the upgrade file in your computer, then click **Upgrade** to install the latest EAP firmware. The Status will appear as **Upgrading** until the process is complete and the EAP reconnects to the OC200.



Upgrade(50-C7-BF-0B-BE-00)

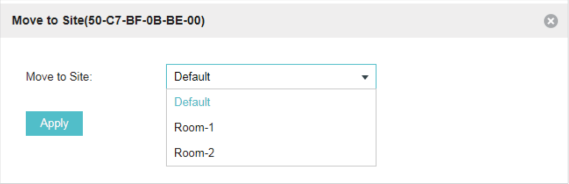
Model: EAP225(US)

Version: 1.4.0 Build 20180323 Rel. 32579

Manual Update: Please select a file.

🗂 Move the EAP to a site.

Select a site that has been created and click **Apply**. You can group all the EAPs by this way and centrally manage them on each site.

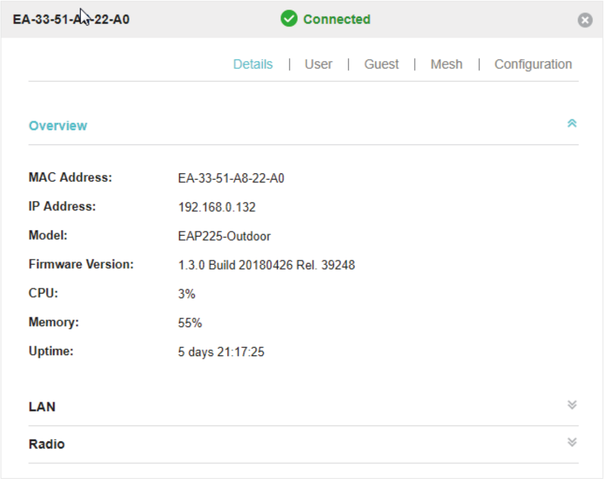


Move to Site(50-C7-BF-0B-BE-00)

Move to Site: Default

Configure the EAP.

For detailed instructions about how to configure the EAP on this window, refer to *Configure the EAPs Separately*.



EA-33-51-A8-22-A0 ✓ Connected

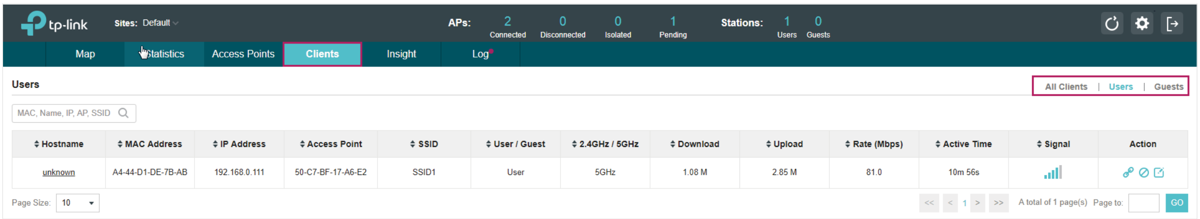
MAC Address:	EA-33-51-A8-22-A0
IP Address:	192.168.0.132
Model:	EAP225-Outdoor
Firmware Version:	1.3.0 Build 20180426 Rel. 39248
CPU:	3%
Memory:	55%
Uptime:	5 days 21:17:25

Note:

- Only managed EAPs can be rebooted or upgraded.
- The EAP which is managed by the OC200 can not be logged in to its own management interface. To log in to the EAP's own management interface, forget the EAP first.

2.4 Monitor and Manage Clients

The **Clients** tab displays the clients connected to the EAP network.



APs: 2 Connected, 0 Disconnected, 0 Isolated, 1 Pending. Stations: 1 Users, 0 Guests

Users

Hostname	MAC Address	IP Address	Access Point	SSID	User / Guest	2.4GHz / 5GHz	Download	Upload	Rate (Mbps)	Active Time	Signal	Action
unknown	A4-44-D1-DE-7B-AB	192.168.0.111	50-C7-BF-17-A6-E2	SSID1	User	5GHz	1.08 M	2.85 M	81.0	10m 56s		

Page Size: 10 &lt;&lt; &lt; 1 &gt; &gt;&gt; A total of 1 page(s) Page to:

2.4.1 View the Current Information of Clients

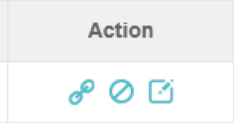
The clients are divided into two types: User and Guest. Users are the clients connected to the EAP wireless network without the Portal Authentication. Guests are the clients connected to the EAP wireless network with the Portal Authentication.

You can click the following tabs to respectively view the detailed information of users and guests.

All Clients	The page displays the information of all clients including users and guests.
Users	The page displays the information of Users.
Guests	The page displays the information of Guests.

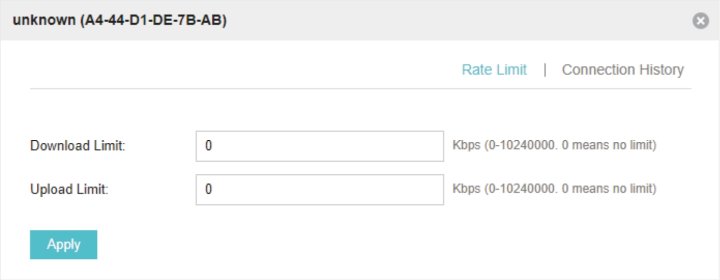
2.4.2 Manage Clients in the Action Column

You can execute the corresponding operation to the EAP by clicking an icon in the **Action** column:



Action
🔗 ⊘ ✎

🔗	Reconnect the client to the network.
⊘	Restrict the client's access to the network.
✎	Configure the rate limit of the client and view the connection history. Enter the download limit and upload limit and click **Apply**.
🛡	If the client is a Guest, you can click this icon to cancel the authorization for it.



unknown (A4-44-D1-DE-7B-AB)

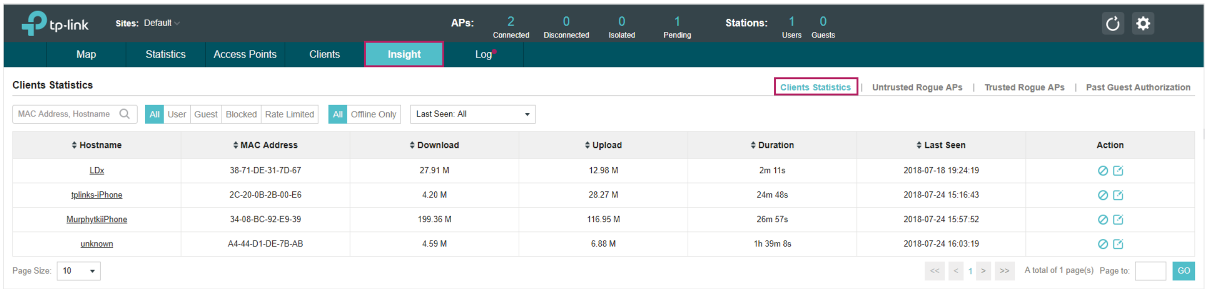
Rate Limit | Connection History

Download Limit: 0 Kbps (0-10240000. 0 means no limit)

Upload Limit: 0 Kbps (0-10240000. 0 means no limit)

2.5 View Clients Statistics During the Specified Period

The **Clients Statistics** page under the **Insight** tab displays the information of clients that have connected to the EAPs network during a specified period.



tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 0 Isolated 1 Pending
Stations: 1 Users 0 Guests
Map
Statistics
Access Points
Clients
Insight
Log
Clients Statistics | Untrusted Rogue APs | Trusted Rogue APs | Past Guest Authorization
MAC Address, Hostname
All
User
Guest
Blocked
Rate Limited
All
Offline Only
Last Seen: All

Clients Statistics

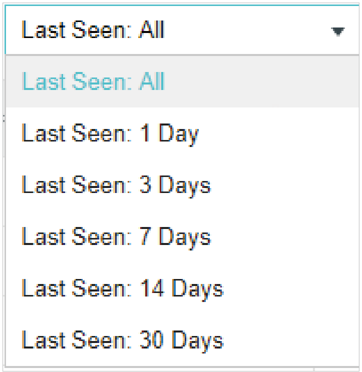
Hostname	MAC Address	Download	Upload	Duration	Last Seen	Action
LDx	38-71-DE-31-7D-67	27.91 M	12.98 M	2m 11s	2018-07-18 19:24:19	⊘ ✎
tplinks-iPhone	2C-20-0B-2B-00-E6	4.20 M	28.27 M	24m 48s	2018-07-24 15:16:43	⊘ ✎
MurphytkiiPhone	34-08-BC-92-E9-39	199.36 M	116.95 M	26m 57s	2018-07-24 15:57:52	⊘ ✎
unknown	A4-44-D1-DE-7B-AB	4.59 M	6.88 M	1h 39m 8s	2018-07-24 16:03:19	⊘ ✎

Page Size: 10

<< < 1 > >>
A total of 1 page(s) Page to:
GO

2.5.1 Select a Specified Period

Select a period from the drop-down menu. Then the page will display clients that have connected to the EAPs network during the period.



2.5.2 View the History Information of Clients

You can click the client's MAC address to get its connection history and configure the Rate Limit feature for this client. In addition, you can click the following tabs to view the information of different types of clients:

All	The page displays the history information of all the clients.
User	The page displays the history information of Users. Users are the clients connected to the EAP wireless network without the Portal Authentication.
Guest	The page displays the history information of Guests. Guests are the clients connected to the EAP wireless network with the Portal Authentication.
Blocked	The page displays the clients that have been blocked.
Rate Limited	The page displays the clients that have been limited upload or download rate.

All	The page displays the history information of all clients.
Offline Only	The page displays the history information of the off-line clients.

2.5.3 Manage Clients in the Action Column

You can execute the corresponding operation to the EAP in the **Action** column:

⊘	Block the client's access to the network.

↻	Resume the client's access.
✎	Configure the rate limit of the client and view the connection history.
⊖	Remove the limit to the client’s upload or download rates.

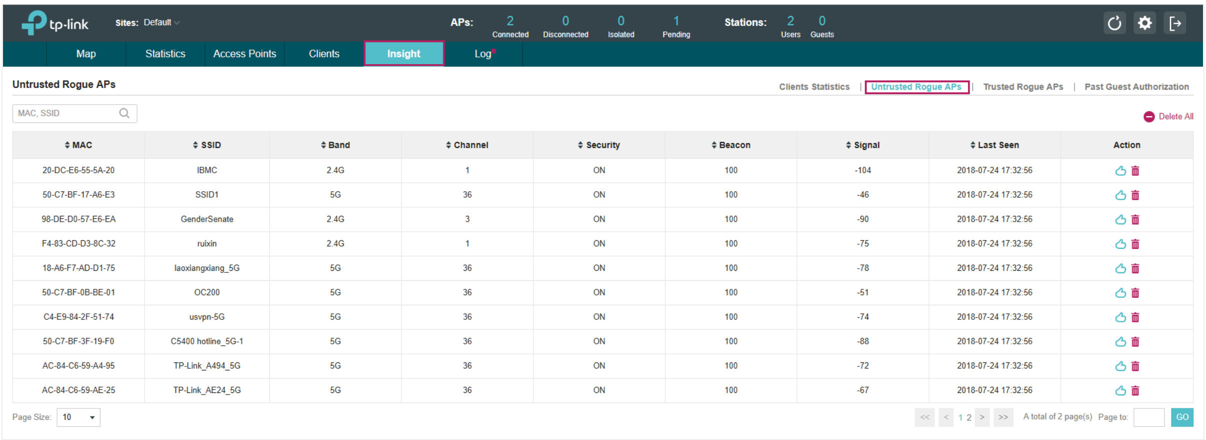
2.6 Manage the Rogue APs List

A Rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator. The OC200 can scan all channels to detect all nearby EAPs. If rogue APs are detected, they will be shown on the **Untrusted Rogue APs** list. Besides, you can move the untrusted rogue APs to the **Trusted Rogue APs** list.

By default, the Rogue AP Detection feature is disabled. To allow your EAP to detect nearby APs, you need to enable this feature for this EAP. You can refer to Rogue AP Detection.

2.6.1 Manage the Untrusted Rogue APs List

The **Untrusted Rogue APs** page displays the detailed information of untrusted rogue APs.


tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 0 Isolated 1 Pending
Stations: 2 Users 0 Guests
Map
Statistics
Access Points
Clients
Insight
Log
Clients Statistics | Untrusted Rogue APs | Trusted Rogue APs | Past Guest Authorization
MAC, SSID
Delete All
Page Size: 10
<< < 1 2 > >>
A total of 2 page(s) Page to:
GO

Untrusted Rogue APs

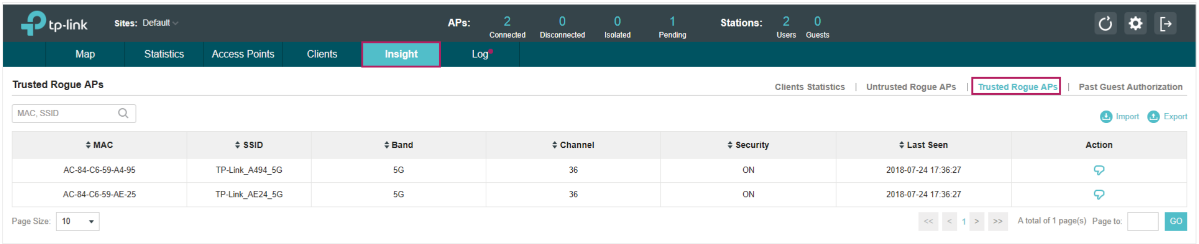
MAC	SSID	Band	Channel	Security	Beacon	Signal	Last Seen	Action
20-DC-E6-55-5A-20	IBMC	2.4G	1	ON	100	-104	2018-07-24 17:32:56	👍 🗑
50-C7-BF-17-A6-E3	SSID1	5G	36	ON	100	-46	2018-07-24 17:32:56	👍 🗑
98-DE-D0-57-E6-EA	GenderSenate	2.4G	3	ON	100	-90	2018-07-24 17:32:56	👍 🗑
F4-83-CD-D3-8C-32	ruixin	2.4G	1	ON	100	-75	2018-07-24 17:32:56	👍 🗑
18-A6-F7-AD-D1-75	laoxiangxiang_5G	5G	36	ON	100	-78	2018-07-24 17:32:56	👍 🗑
50-C7-BF-0B-BE-01	OC200	5G	36	ON	100	-51	2018-07-24 17:32:56	👍 🗑
C4-E9-84-2F-51-74	usvpn-5G	5G	36	ON	100	-74	2018-07-24 17:32:56	👍 🗑
50-C7-BF-3F-19-F0	C5400 hotline_5G-1	5G	36	ON	100	-88	2018-07-24 17:32:56	👍 🗑
AC-84-C6-59-A4-95	TP-Link_A494_5G	5G	36	ON	100	-72	2018-07-24 17:32:56	👍 🗑
AC-84-C6-59-AE-25	TP-Link_AE24_5G	5G	36	ON	100	-67	2018-07-24 17:32:56	👍 🗑

You can execute the corresponding operation to the EAP in the **Action** column:

👍	Move the untrusted rogue AP to the Trusted Rogue APs list.
🗑	Delete this record.
⊖ Delete All	Delete all records.

2.6.2 Manage the Trusted Rogue APs List

The Trusted Rogue APs page displays the detailed information of trusted rogue APs.


tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 0 Isolated 1 Pending
Stations: 2 Users 0 Guests
Map
Statistics
Access Points
Clients
Insight
Log
Clients Statistics | Untrusted Rogue APs | Trusted Rogue APs | Past Guest Authorization
MAC, SSID
Import
Export
Page Size: 10
<< < 1 > >> A total of 1 page(s) Page to: GO

Trusted Rogue APs

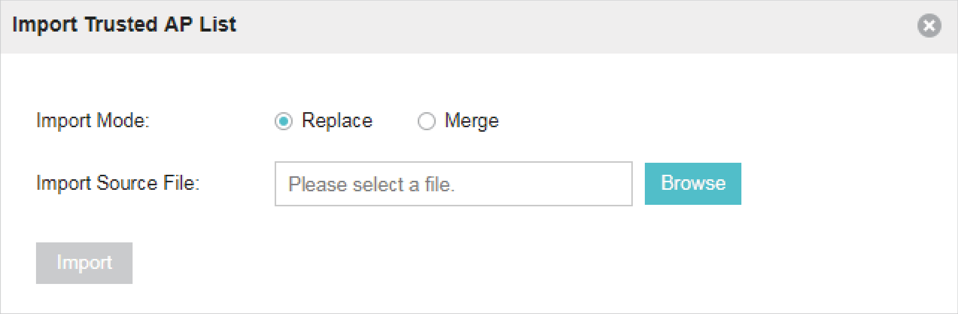
MAC	SSID	Band	Channel	Security	Last Seen	Action
AC-84-C6-59-A4-95	TP-Link_A494_5G	5G	36	ON	2018-07-24 17:36:27	👎
AC-84-C6-59-AE-25	TP-Link_AE24_5G	5G	36	ON	2018-07-24 17:36:27	👎

You can execute the corresponding operation to the EAP by clicking an icon in the **Action** column:

👎 Move the trusted rogue AP to the Untrusted Rogue APs list.

Export — Export and download the current Trusted Rogue APs list and save it on your PC.

Import — Import a saved Trusted Rogue APs list. If the MAC address of an AP appears in list, it will not be detected as a rogue AP.



Import Trusted AP List

Import Mode: ● Replace ○ Merge

Import Source File: Please select a file. Browse

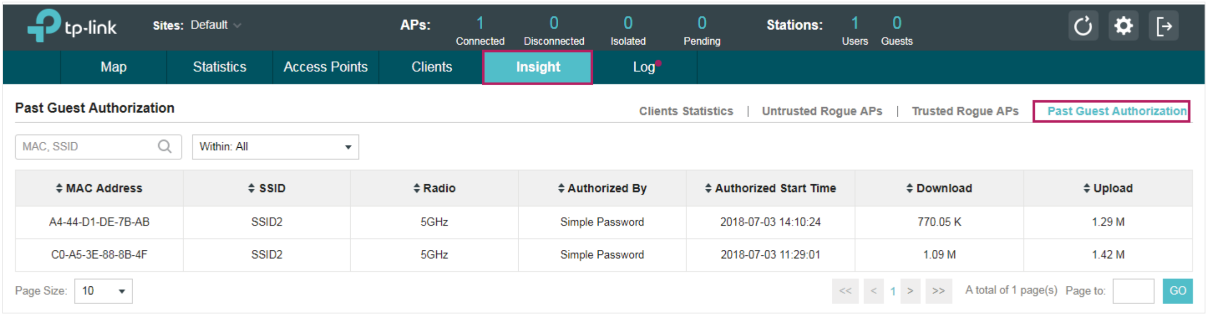
Import

Please follow the steps below:

1. Select **Replace** (replace the current Trusted Rogue APs list with the one you import) or **Merge** (add the APs in the file to the current Trusted Rogue APs list).
2. Click **Browse** to locate the file and choose it.
3. Click **Import** to import the Trusted Rogue APs list.

2.7 View Past Guest Authorization

The Past Guest Authorization page displays the details about all the clients that accessed the network during a certain time period. You can select a period in the drop-down list.


tp-link
Sites: Default
APs: 1 Connected 0 Disconnected 0 Isolated 0 Pending
Stations: 1 Users 0 Guests
Map
Statistics
Access Points
Clients
Insight
Log
Clients Statistics | Untrusted Rogue APs | Trusted Rogue APs | Past Guest Authorization
MAC, SSID
Page Size: 10
<< < 1 > >> A total of 1 page(s) Page to: GO

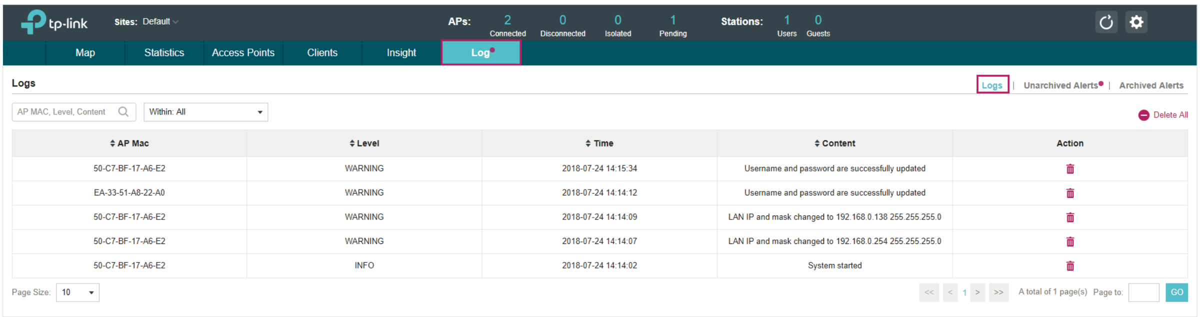
Past Guest Authorization

Within: All

MAC Address	SSID	Radio	Authorized By	Authorized Start Time	Download	Upload
A4-44-D1-DE-7B-AB	SSID2	5GHz	Simple Password	2018-07-03 14:10:24	770.05 K	1.29 M
C0-A5-3E-88-8B-4F	SSID2	5GHz	Simple Password	2018-07-03 11:29:01	1.09 M	1.42 M

2.8 View Logs

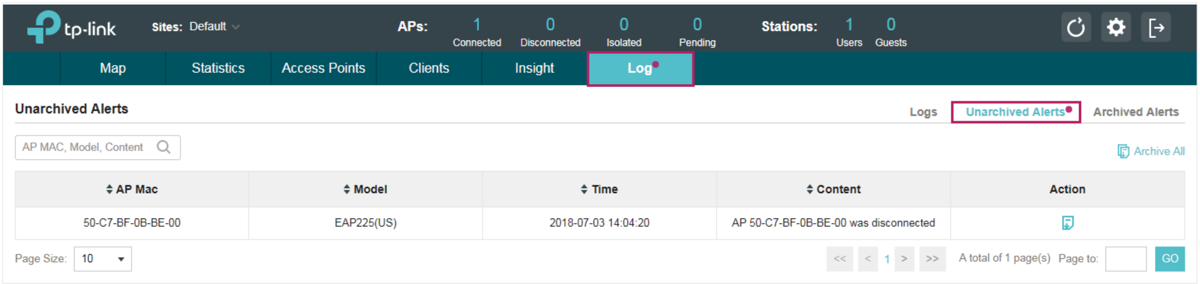
The logs of OC200 can effectively record, classify and manage the system information of the managed EAPs, providing powerful support for you to monitor network operation and diagnose malfunctions. The Logs page displays EAP's MAC address, level, occurred time and content.


tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 0 Isolated 1 Pending
Stations: 1 Users 0 Guests
Map
Statistics
Access Points
Clients
Insight
Log
Logs
Logs | Unarchived Alerts | Archived Alerts
AP MAC, Level, Content
Within: All
Delete All
Page Size: 10
<< < 1 > >> A total of 1 page(s) Page to: GO

AP Mac	Level	Time	Content	Action
50-C7-BF-17-A6-E2	WARNING	2018-07-24 14:15:34	Username and password are successfully updated	🗑
EA-33-51-A8-22-A0	WARNING	2018-07-24 14:14:12	Username and password are successfully updated	🗑
50-C7-BF-17-A6-E2	WARNING	2018-07-24 14:14:09	LAN IP and mask changed to 192.168.0.138 255.255.255.0	🗑
50-C7-BF-17-A6-E2	WARNING	2018-07-24 14:14:07	LAN IP and mask changed to 192.168.0.254 255.255.255.0	🗑
50-C7-BF-17-A6-E2	INFO	2018-07-24 14:14:02	System started	🗑

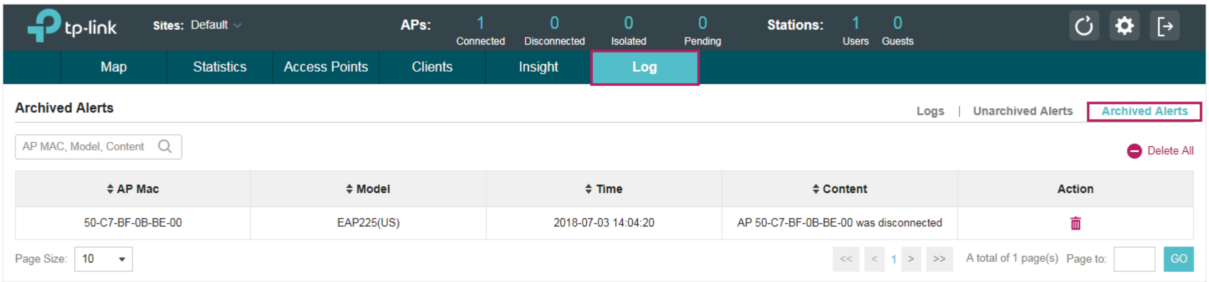
2.9 View Alerts

You can see the status change of your EAPs on the **Unarchived Alerts** page. You can click 🗎 or 🗎 Archive All to move unarchived alerts to the Archived Alerts page.



AP Mac	Model	Time	Content	Action
50-C7-BF-0B-BE-00	EAP225(US)	2018-07-03 14:04:20	AP 50-C7-BF-0B-BE-00 was disconnected	🗎

As follows, the Archived Alerts page displays the alerts archived by you. You can click 🗑 or ⊖ Delete All to delete the records.


tp-link
Sites: Default
APs: 1 Connected 0 Disconnected 0 Isolated 0 Pending
Stations: 1 Users 0 Guests
Map
Statistics
Access Points
Clients
Insight
Log
Archived Alerts
Logs | Unarchived Alerts | Archived Alerts
AP MAC, Model, Content
Delete All
Page Size: 10
<< < 1 > >> A total of 1 page(s) Page to: GO

AP Mac	Model	Time	Content	Action
50-C7-BF-0B-BE-00	EAP225(US)	2018-07-03 14:04:20	AP 50-C7-BF-0B-BE-00 was disconnected	🗑

3 Configure the EAPs Globally

This chapter introduces the global configurations applied to all the managed EAPs. To configure a specific EAP, please refer to Chapter 5 Configure the EAPs Separately.

In global configurations, you can configure the following items:

- *Wireless Network*
- *Access Control*
- *Portal Authentication*
- *Free Authentication Policy*
- *MAC Filter*
- *Scheduler*
- *QoS*
- *Site Settings*

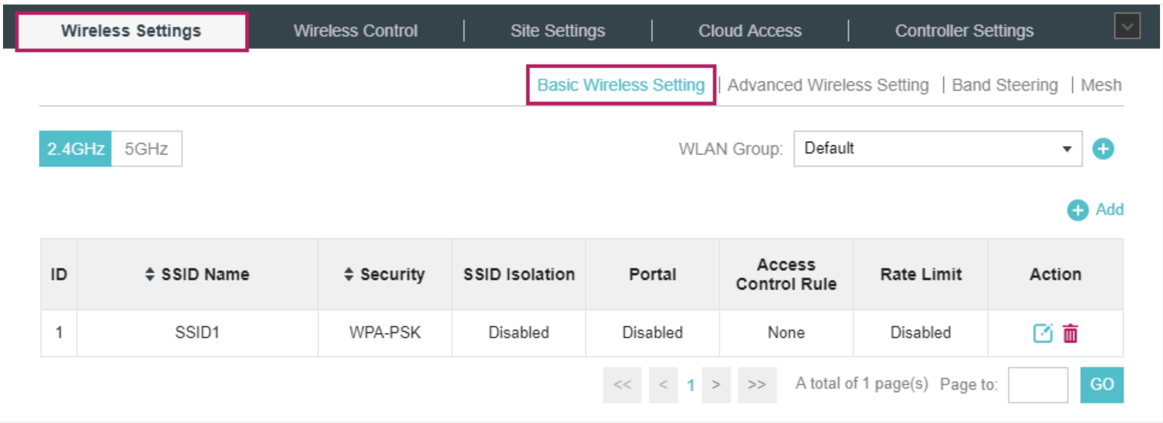
3.1 Wireless Network

In addition to the wireless network you created in Quick Start, you can add more wireless networks and configure the advanced wireless parameters to improve the network quality.

3.1.1 Add Wireless Networks

To add wireless networks, follow the steps below.

1. Go to **Wireless Settings > Basic Wireless Setting**.



Wireless Settings | Wireless Control | Site Settings | Cloud Access | Controller Settings

Basic Wireless Setting | Advanced Wireless Setting | Band Steering | Mesh

2.4GHz 5GHz WLAN Group: Default ⊕

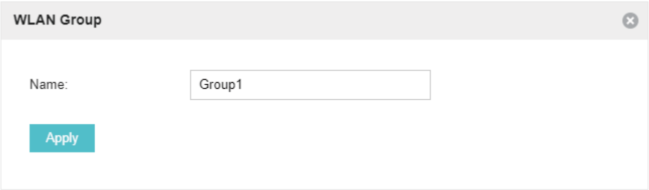
⊕ Add

ID	⇕ SSID Name	⇕ Security	SSID Isolation	Portal	Access Control Rule	Rate Limit	Action
1	SSID1	WPA-PSK	Disabled	Disabled	None	Disabled	✎ 🗑

<< < 1 > >> A total of 1 page(s) Page to: GO

2. Select a band frequency 2.4GHz 5GHz and click ⊕ at the right of WLAN Group: Default to add a WLAN group. WLAN groups are an easy way to quickly deploy EAPs by creating a template-based set of SSIDs with wireless parameters. Different WLAN groups can be applied to different EAPs. If you have no need to group your wireless networks, you can use the default WLAN group and skip this step.

3. Specify a name for the group and click **Apply**.



WLAN Group

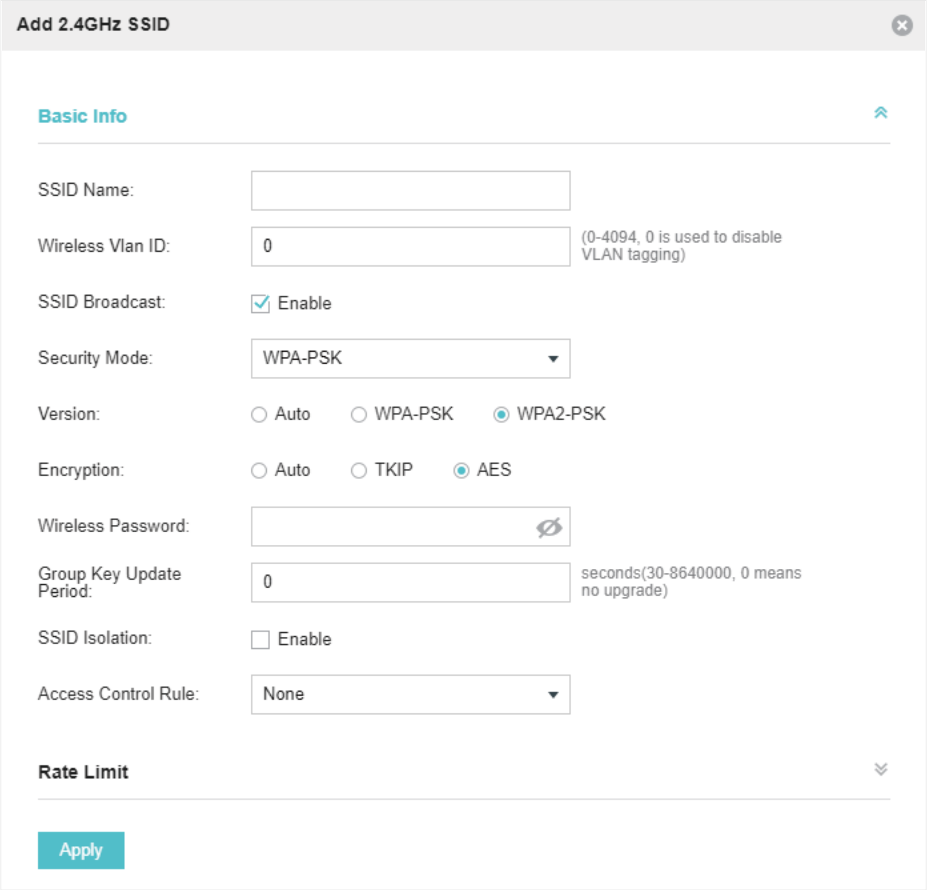
Name: Group1

Apply

4. Select the brand frequency 2.4GHz 5GHz and WLAN group WLAN Group: Default .

5. Click ⊕ Add to add an SSID to the specific WLAN group.

6. Configure the parameters in the following window.



Add 2.4GHz SSID

Basic Info

SSID Name:

Wireless Vlan ID: 0 (0-4094, 0 is used to disable VLAN tagging)

SSID Broadcast: ☑ Enable

Security Mode: WPA-PSK

Version: ○ Auto ○ WPA-PSK ● WPA2-PSK

Encryption: ○ Auto ○ TKIP ● AES

Wireless Password:

Group Key Update Period: 0 seconds(30-8640000, 0 means no upgrade)

SSID Isolation: □ Enable

Access Control Rule: None

Rate Limit

SSID Name	Enter an SSID name contains up to 32 characters.
Wireless Vlan ID	Set a VLAN ID for the wireless network. Wireless networks with the same VLAN ID are grouped to a VLAN. The value ranges from 0 to 4094. 0 means VLAN function is disabled.
SSID Broadcast	With the option enabled, EAPs will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the EAP. Enabled by default.
Security Mode	Select the security mode of the wireless network. **None**: The hosts can access the wireless network without authentication. WEP/WPA-Enterprise/WPA-PSK: The hosts need to get authenticated before accessing the wireless network. For the network security, you are suggested to encrypt your wireless network. Settings vary in different security modes and the details are in the following introduction.
SSID Isolation	With the option enabled, the devices connected in the same SSID of the same AP cannot communicate with each other. Disabled by default.
Access Control Rule	Select an Access Control rule for this SSID. For more information, refer to Access Control.

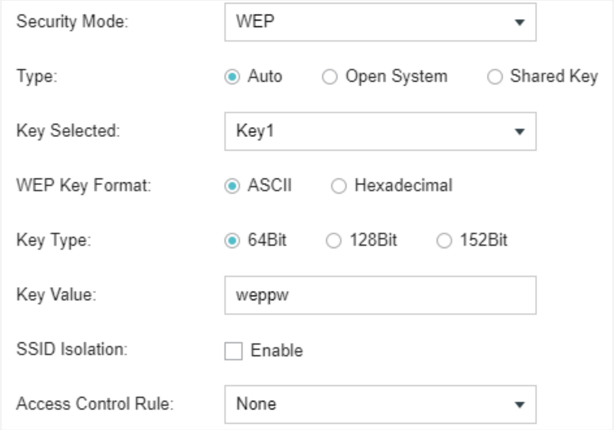
Following is the detailed introduction of **WEP**, **WPA-Enterprise** and **WPA-PSK**.

WEP

WEP is based on the IEEE 802.11 standard and less safe than WPA-Enterprise and WPA-PSK.

Note:

WEP is not supported in 802.11n mode or 802.11ac mode. If WEP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network. If WEP is applied in 11b/g/n mode (2.4GHz) or 11a/n (5GHz), the EAP device may work at a low transmission rate.

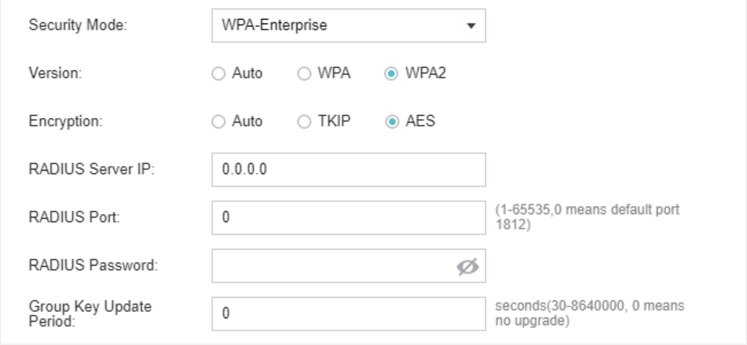


Security Mode:	WEP ▾
Type:	● Auto ○ Open System ○ Shared Key
Key Selected:	Key1 ▾
WEP Key Format:	● ASCII ○ Hexadecimal
Key Type:	● 64Bit ○ 128Bit ○ 152Bit
Key Value:	weppw
SSID Isolation:	□ Enable
Access Control Rule:	None ▾

Type	Select the authentication type for WEP. **Auto**: The OC200 can select Open System or Shared Key automatically based on the wireless station's capability and request. **Open System**: Clients can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission. **Shared Key**: Clients have to input password to pass the authentication, otherwise it cannot associate with the wireless network or transmit data.
Key Selected	Select one key to specify. You can configure four keys at most.
WEP Key Format	Select **ASCII** or **Hexadecima** as the WEP key format. **ASCII**: ASCII format stands for any combination of keyboard characters of the specified length. **Hexadecimal**: Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) with the specified length.
Key Type	Select the WEP key length for encryption. **64Bit**: Enter 10 hexadecimal digits or 5 ASCII characters. **128Bit**: Enter 26 hexadecimal digits or 13 ASCII characters. **152Bit**: Enter 32 hexadecimal digits or 16 ASCII characters.
Key Value	Enter the WEP keys. The length and valid characters are affected by key type.

WPA-Enterprise

The WPA-Enterprise mode requires a RADIUS server to authenticate clients. Since the WPA-Enterprise can generate different passwords for different clients, it is much safer than WPA-PSK. However, it costs much more to maintain and is usually used by enterprise.



Security Mode: WPA-Enterprise

Version: ○ Auto ○ WPA ● WPA2

Encryption: ○ Auto ○ TKIP ● AES

RADIUS Server IP: 0.0.0.0

RADIUS Port: 0 (1-65535,0 means default port 1812)

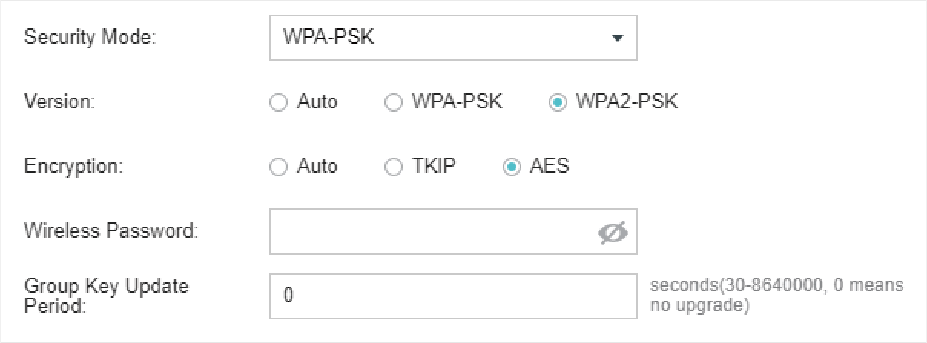
RADIUS Password:

Group Key Update Period: 0 seconds(30-8640000, 0 means no upgrade)

Version	Select the version of WPA-Enterprise. **Auto**: The EAP will automatically choose the version used by each client device. **WPA/WPA2**: Two versions of Wi-Fi Protected Access.
Encryption	Select the Encryption type. **Auto**: The default setting is Auto and the EAP will select TKIP or AES automatically based on the client device's request. **TKIP**: Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network of the EAP. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. **AES**: Advanced Encryption Standard. We recommend you select AES as the encryption type because it is more secure than TKIP.
RADIUS Server IP	Enter the IP address of the RADIUS Server.
RADIUS Port	Enter the port number of the RADIUS Server.
RADIUS Password	Enter the shared secret key of the RADIUS server.
Group Key Update Period	Specify a group key update period, which instructs the EAP how often it should change the encryption keys. The value can be either 0 or 30~8640000 seconds. 0 means no change of the encryption key anytime.

WPA-PSK

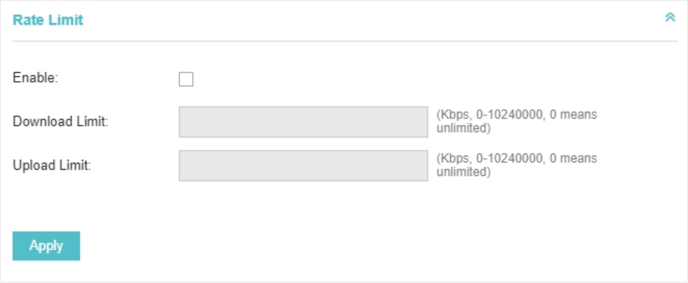
Based on a pre-shared key, WPA-PSK is characterized by high safety and simple settings and is mostly used by common households and small businesses.



Security Mode:	WPA-PSK
Version:	○ Auto ○ WPA-PSK ● WPA2-PSK
Encryption:	○ Auto ○ TKIP ● AES
Wireless Password:	
Group Key Update Period:	0 seconds(30-8640000, 0 means no upgrade)

Version	Select the version of WPA-PSK. **Auto**: The EAP will automatically choose the version for each client device. **WPA-PSK**: Pre-shared key of WPA. **WAP2-PSK**: Pre-shared key of WPA2.
Encryption	Select the Encryption type. **Auto**: The default setting is Auto and the EAP will select TKIP or AES automatically based on the client request. **TKIP**: Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network of the EAP. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. **AES**: Advanced Encryption Standard. We recommend you select AES as the encryption type for it is more secure than TKIP.
Wireless Password	Configure the wireless password with ASCII or Hexadecimal characters. For ASCII, the length should be between 8 and 63 characters with combination of numbers, letters (case-sensitive) and common punctuations. For Hexadecimal, the length should be 64 characters (case-insensitive, 0-9, a-f, A-F).
Group Key Update Period	Specify a group key update period, which instructs the EAP how often it should change the encryption keys. The value can be either 0 or 30~8640000 seconds. 0 means the encryption keys will not be changed all the time.

7. Enable **Rate Limit** for the clients to guarantee the network balance. Enter the value for **Download Limit** and **Upload Limit.** 0 means unlimited. Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.



Rate Limit

Enable: □

Download Limit: (Kbps, 0-10240000, 0 means unlimited)

Upload Limit: (Kbps, 0-10240000, 0 means unlimited)

Apply

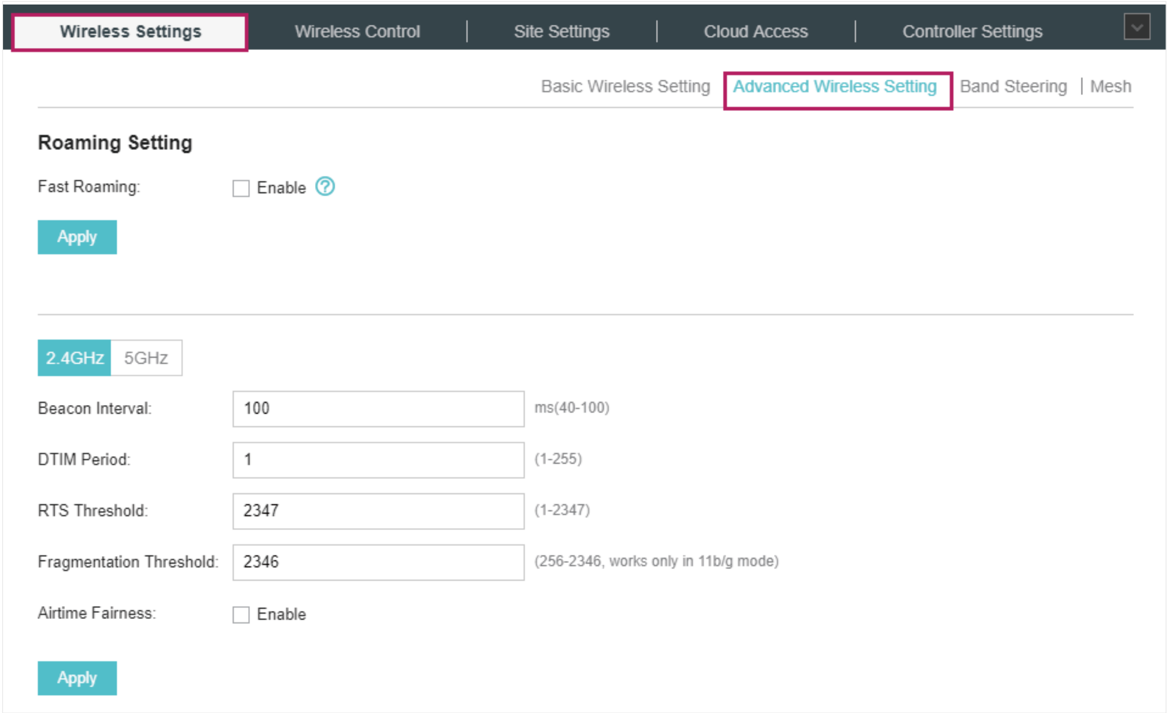
8. Click **Apply**.

3.1.2 Configure Advanced Wireless Parameters

Proper wireless parameters can improve the network's stability, reliability and communication efficiency. The advanced wireless parameters consist of **Fast Roaming**, **Beacon Interval**, **DTIM Period**, **RTS Threshold**, **Fragmentation Threshold** and **Airtime Fairness**.

To configure the advanced wireless parameters, follow the steps below.

1. Go to **Wireless Settings > Advanced Wireless Setting**.



Roaming Setting

Fast Roaming: □ Enable

Apply

2.4GHz | 5GHz

Beacon Interval: 100 ms(40-100)

DTIM Period: 1 (1-255)

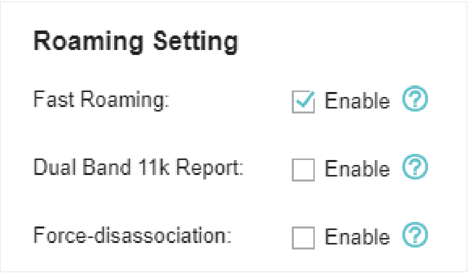
RTS Threshold: 2347 (1-2347)

Fragmentation Threshold: 2346 (256-2346, works only in 11b/g mode)

Airtime Fairness: □ Enable

Apply

2. Enable **Fast Roaming** and configure the corresponding parameters.



Roaming Setting

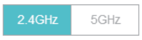
Fast Roaming: ☑ Enable

Dual Band 11k Report: □ Enable

Force-disassociation: □ Enable

Fast Roaming	With this option enabled, 11k/v capable clients can have improved fast roaming experience when moving among different APs.
Dual Band 11k Report	With this feature disabled, the OC200 provides candidate AP report that contains the APs in the same band as the clients. With this feature enabled, the controller provides candidate AP report that contains the APs in both 2.4GHz and 5GHz bands.
Force-disassociation	The OC200 dynamically monitors the link quality of every associated client. When the client's current link quality drops below the predefined threshold and there are some other APs with better signal, the current AP issues an 11v roaming suggestion to the client. With Force-disassociation disabled, the AP only issues a roaming suggestion, but whether to roam or nor is determined by the client. With Force-disassociation enabled, the AP not only issues a roaming suggestion but also disassociates the client after a while. Thus the client is supported to re-associate to a better AP. This function is recommended when there are sticky clients that don't roam.

3. Click **Apply.**

4. Select the band frequency 

.

5. Configure the following parameters.

Beacon Interval	Beacons are transmitted periodically by the EAP device to announce the presence of a wireless network for the clients. **Beacon Interval** value determines the time interval of the beacons sent by the device. You can specify a value between 40 and 100ms. The default is 100ms.
DTIM Period	The DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames. It indicates whether the EAP device has buffered data for client devices. The **DTIM Period** indicates how often the clients served by this EAP device should check for buffered data still on the EAP device awaiting pickup. You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating clients check for buffered data on the EAP device at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend you keep it by default.
RTS Threshold	RTS (Request to Send) can ensure efficient data transmission. When RTS is activated, the client will send a RTS packet to EAP to inform that it will send data before it send packets. After receiving the RTS packet, the EAP notices other clients in the same wireless network to delay their transmitting of data and informs the requesting client to send data, thus avoiding the conflict of packet. If the size of packet is larger than the **RTS Threshold**, the RTS mechanism will be activated. If you specify a low threshold value, RTS packets are sent more frequently and help the network recover from interference or collisions that might occur on a busy network. However, it also consumes more bandwidth and reduces the throughput of the packet. We recommend you keep it by default. The recommended and default value is 2347.

Fragmentation Threshold	The fragmentation function can limit the size of packets transmitted over the network. If a packet exceeds the **Fragmentation Threshold**, the fragmentation function is activated and the packet will be fragmented into several packets. Fragmentation helps improve network performance if properly configured. However, too low fragmentation threshold may result in poor wireless performance caused by the extra work of dividing up and reassembling of frames and increased message traffic. The recommended and default value is 2346 bytes.
Airtime Fairness	With this option enabled, each client connecting to the EAP can get the same amount of time to transmit data, avoiding low-data-rate clients to occupy too much network bandwidth and improving the network throughput. We recommend you enable this function under multi-rate wireless networks.

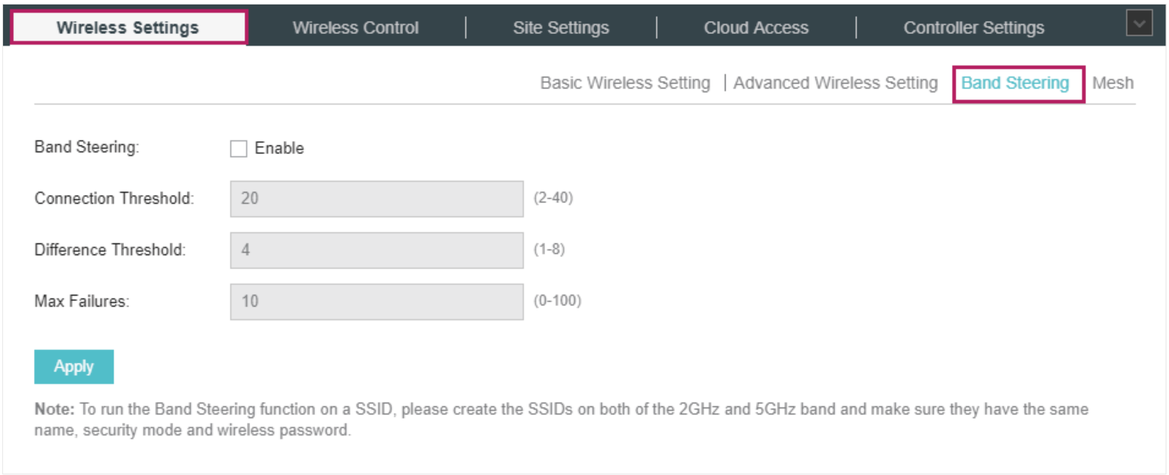
6. Click **Apply**.

3.1.3 Configure Band Steering

A client device that is capable of communicating on both the 2.4GHz and 5GHz frequency bands will typically connect to the 2.4GHz band. However, if too many client devices are connected to an EAP on the 2.4GHz band, the efficiency of communication will be diminished. Band Steering can steer dual-band clients to the 5GHz frequency band which supports higher transmission rates and more client devices, and thus to greatly improve the network quality.

To configure Band Steering, follow the steps below.

1. Go to **Wireless Settings > Band Steering.**



Band Steering: □ Enable

Connection Threshold: 20 (2-40)

Difference Threshold: 4 (1-8)

Max Failures: 10 (0-100)

Note: To run the Band Steering function on a SSID, please create the SSIDs on both of the 2GHz and 5GHz band and make sure they have the same name, security mode and wireless password.

2. Check the box to enable the Band Steering function.

3. Configure the following parameters to balance the clients on both frequency bands:

Connection Threshold/ Difference Threshold	**Connection Threshold** defines the maximum number of clients connected to the 5GHz band. The value of **Connection Threshold** is from 2 to 40, and the default is 20. **Difference Threshold** defines the maximum difference between the number of clients on the 5GHz band and 2.4GHz band. The value of **Difference Threshold** is from 1 to 8, and the default is 4. When the following two conditions are both met, the EAP prefer to refuse the connection request on 5GHz band and no longer steer other clients to the 5GHz band: 1. The number of clients on the 5GHz band reaches the **Connection Threshold** value. 2. The difference between the number of clients on the 2.4GHz band and 5GHz band reaches the **Difference Threshold** value.
Max Failures	If a client repeatedly attempts to associate with the EAP on the 5GHz band and the number of rejections reaches the value of **Max Failures**, the EAP will accept the request. The value is from 0 to 100, and the default is 10.

4. Click **Apply**.

3.1.4 Configure Mesh

Mesh is used to establish a wireless network or expand a wired network through wireless connection on 5GHz radio band. In practical application, it can help users to conveniently deploy APs without requiring Ethernet cable. After mesh network establishes, the EAP devices can be configured and managed within OC200 in the same way as wired EAPs. Meanwhile, because of the ability to self-organize and self-configure, mesh also can efficiently reduce the configuration overhead.

Note:

- Only EAP225-Outdoor with specific firmware (version 1.3 or above) is available for mesh function currently.
- Only the EAPs in the same site can establish a mesh network.

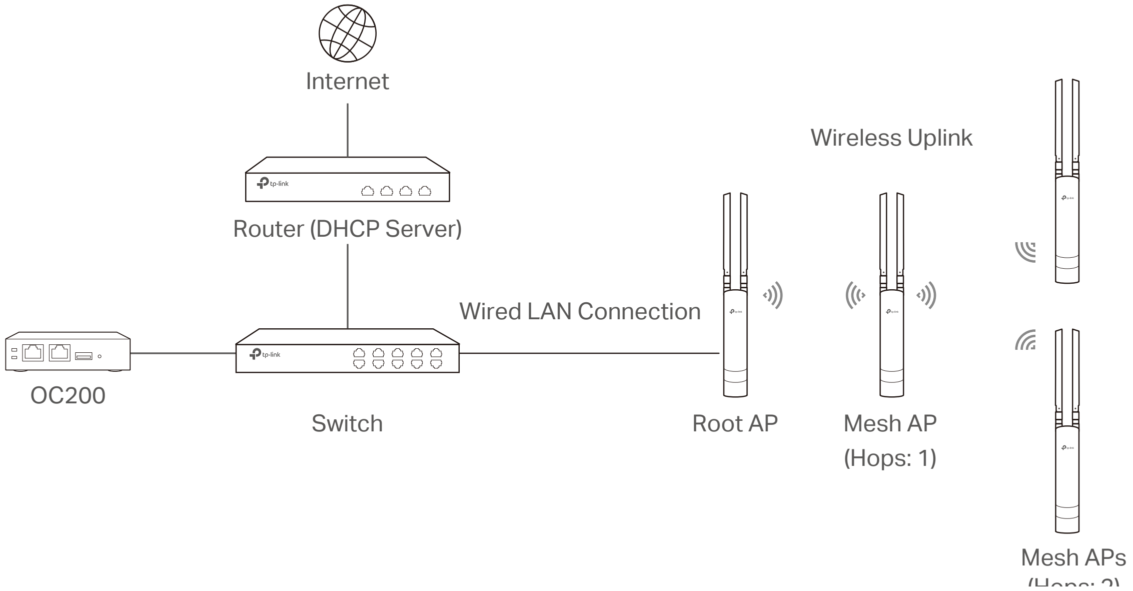
To understand how mesh can be used, the following terms used in OC200 will be introduced:

- Root AP: The AP is managed by OC200 with a wired data connection that can be configured to relay data to and from mesh APs (Downlink AP).
- Isolated AP: When the EAP which has been managed before by OC200 connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state.
- Mesh AP: An isolated AP will be mesh AP after establishing a wireless connection to the AP with network access.
- Uplink AP/Downlink AP: Among mesh APs, the AP that offers the wireless connection for other APs is Uplink AP. A Root AP or an intermediate AP can be the Uplink AP. And the AP that connects

to the Uplink AP is called Downlink AP. An uplink AP can offer direct wireless connection for 4 Downlink APs at most.

- Wireless Uplink: The action that a Downlink AP connects to the uplink AP.
- Hops: In a deployment that uses a root AP and more than one level of wireless uplink with intermediate APs, the uplink tiers can be referred to by root, first hop, second hop and so on. The hops cannot be more than 3.

In a basic mesh network as shown below, there is a root AP that is connected by Ethernet cable, while other isolated APs have no wired data connection. Mesh allows the isolated APs to communicate with pre-configured root AP on the network. Once powered up, factory default or unadopted EAP devices can sense the EAP in range and make itself available for adoption within the OC200.

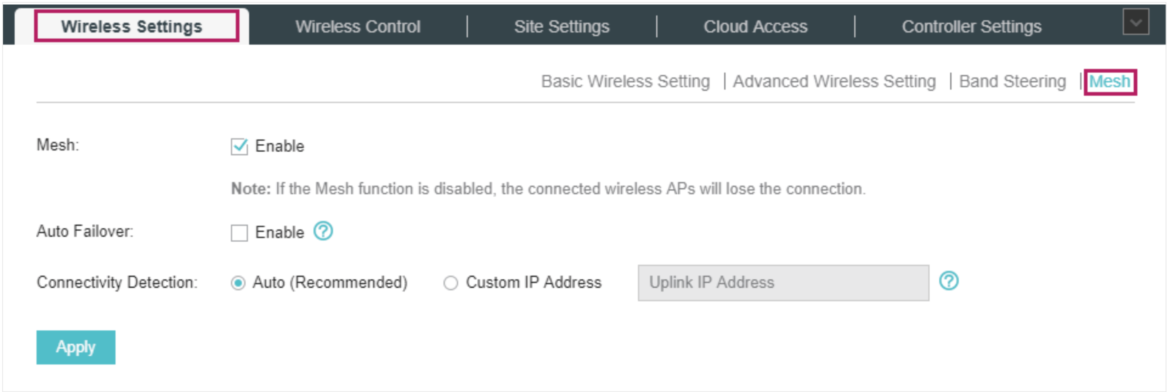


After all the EAPs are adopted, a mesh network is established. Then the EAPs connected to the network wirelessly also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

To establish a mesh network, follow the steps below.

- Enable Mesh Function.
- Adopt the Root AP.
- Set up wireless uplink by adopting APs in Pending (Wireless) or Isolated status.

1. Go to **Wireless Settings > Mesh.**



Mesh: ☑ Enable

Note: If the Mesh function is disabled, the connected wireless APs will lose the connection.

Auto Failover: □ Enable

Connectivity Detection: ● Auto (Recommended) ○ Custom IP Address Uplink IP Address

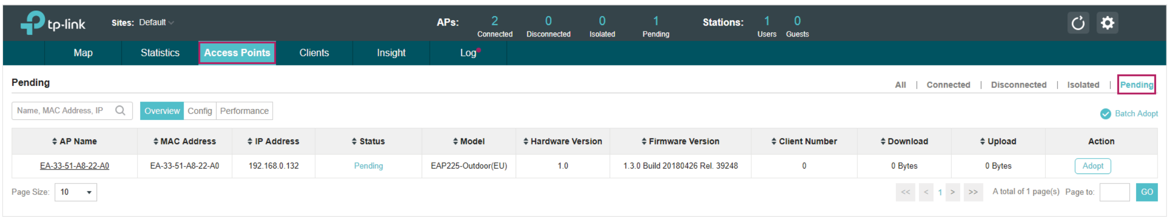
2. Check the box to enable the Mesh function.

3. Configure the following parameters to maintain the mesh network:

Auto Failover	Enable or disable Auto Failover. Auto Failover is used for the OC200 to automatically maintain the mesh network. With this feature enabled, the OC200 can automatically select an uplink AP for the isolated EAP to establish Wireless Uplink. Thus the OC200 will automatically select a new uplink AP for the mesh EAPs to when the original uplink fails.
Connectivity Detection	Specify the method of Connection Detection. In a mesh network, the APs can send ARP request packets to a fixed IP address to test the connectivity. If the link fails, the status of these APs will change to Isolated. **Auto (Recommended):** Select this method and the mesh APs will send ARP request packets to the default gateway for the detection. **Custom IP Address:** Select this method and specify a desired IP address. The mesh APs will send ARP request packets to the custom IP address to test the connectivity. If the IP address of the AP is in different network segments from the custom IP address, the AP will use the default gateway IP address for the detection.

4. Click **Apply**.

5. Go to **Access Points > Pending** and adopt the Root AP. Then the status of the Root AP will change into Connected.


tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 0 Isolated 1 Pending
Stations: 1 Users 0 Guests
Map
Statistics
Access Points
Clients
Insight
Log
All | Connected | Disconnected | Isolated | Pending
Name, MAC Address, IP
Overview
Config
Performance
Batch Adopt

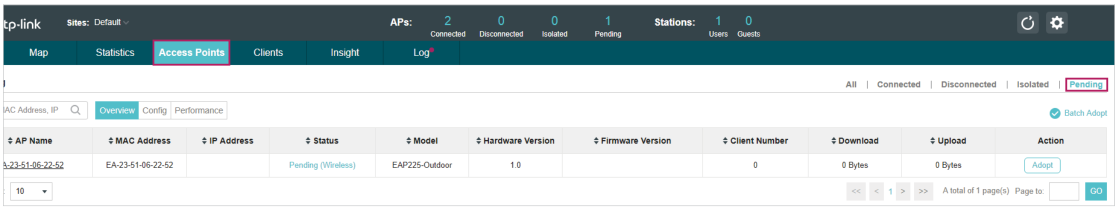
Pending

AP Name	MAC Address	IP Address	Status	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
EA-33-51-A8-22-A0	EA-33-51-A8-22-A0	192.168.0.132	Pending	EAP225-Outdoor(EU)	1.0	1.3.0 Build 20180426 Rel. 39248	0	0 Bytes	0 Bytes	Adopt

Page Size: 10   << < 1 > >> A total of 1 page(s) Page to: GO

6. Install the EAP that will uplink the Root AP wirelessly. Make sure the intended location is within the range of Root AP. The EAPs that is waiting for Wireless Uplink includes two cases: factory default EAPs and EAPs that has been managed by OC200 before.

1) For the factory default EAP, after powering on the device, the EAP will be in Pending (Wireless) status. Go to **Access Points > Pending** and adopt the EAPs in Pending (Wireless) status.

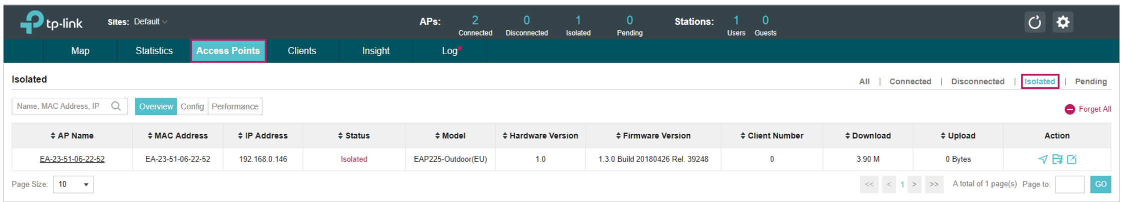

tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 0 Isolated 1 Pending
Stations: 1 Users 0 Guests
Map
Statistics
Access Points
Clients
Insight
Log
All | Connected | Disconnected | Isolated | Pending
AC Address, IP
Overview
Config
Performance
Batch Adopt

AP Name	MAC Address	IP Address	Status	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
A-23-51-06-22-52	EA-23-51-06-22-52		Pending (Wireless)	EAP225-Outdoor	1.0		0	0 Bytes	0 Bytes	Adopt

10
<< < 1 > >>
A total of 1 page(s) Page to:
GO

After adoption begins, the status of Pending (Wireless) EAP will become Adopting (Wireless) and then Connected (Wireless). It should take roughly 2 minutes to show up Connected (Wireless) within your OC200.

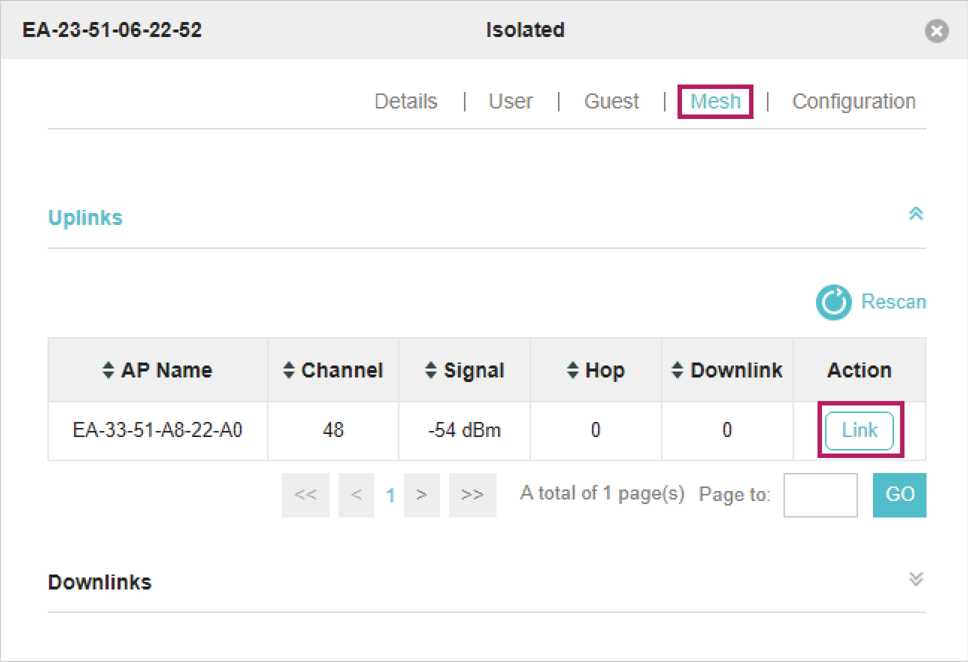
2) For the EAP that has been managed by OC200 before and cannot reach the gateway, it goes into Isolated status when it is discovered again. Go to **Access Points > Isolated**, click ☑.


tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 1 Isolated 0 Pending
Stations: 1 Users 0 Guests
Map
Statistics
Access Points
Clients
Insight
Log
Isolated
All | Connected | Disconnected | Isolated | Pending
Name, MAC Address, IP
Overview
Config
Performance
Forget All

AP Name	MAC Address	IP Address	Status	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
EA-23-51-06-22-52	EA-23-51-06-22-52	192.168.0.146	Isolated	EAP225-Outdoor(EU)	1.0	1.3.0 Build 20180426 Rel. 39248	0	3.90 M	0 Bytes	

Page Size: 10
<< < 1 > >>
A total of 1 page(s) Page to:
GO

The following page will shown, go to **Mesh**, then click Link to connect the Uplink AP.


EA-23-51-06-22-52
Isolated
Details | User | Guest | Mesh | Configuration
Uplinks
Rescan

AP Name	Channel	Signal	Hop	Downlink	Action
EA-33-51-A8-22-A0	48	-54 dBm	0	0	Link

<< < 1 > >>
A total of 1 page(s) Page to:
GO
Downlinks

Once adoption has finished, your device can be managed by the OC200 in the same way as a wired EAP. You can click the EAP's name on the Access Points tab to view and configure the mesh parameters of the EAP on the pop-up window. Please refer to View Mesh Information of the EAP.

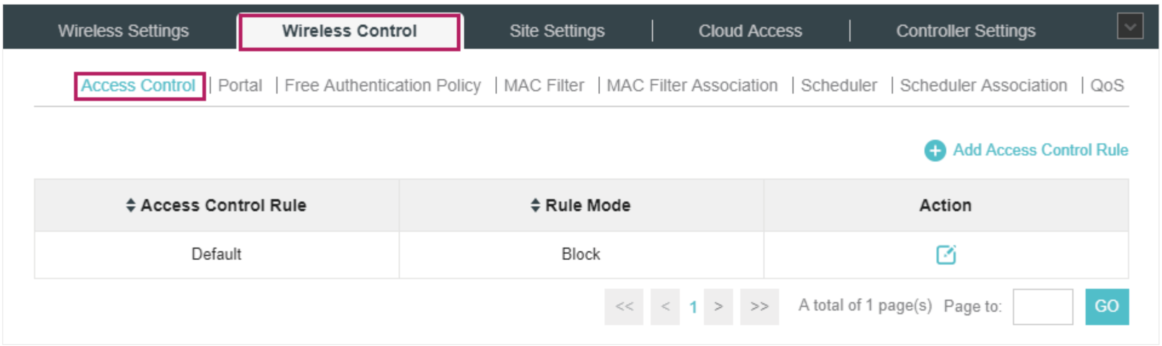
Tips:

- You can manually select the uplink AP that you want to connect in the uplink EAP list. To build a mesh network with better performance, we recommend that you select the Uplink AP with the strongest signal, least hop and least Downlink AP.
- You can enable **Auto Failover** to make the OC200 automatically select an uplink AP for the isolated EAP to establish Wireless Uplink. And the OC200 will automatically select a new uplink AP for the mesh EAPs when the original uplink fails.

3.2 Access Control

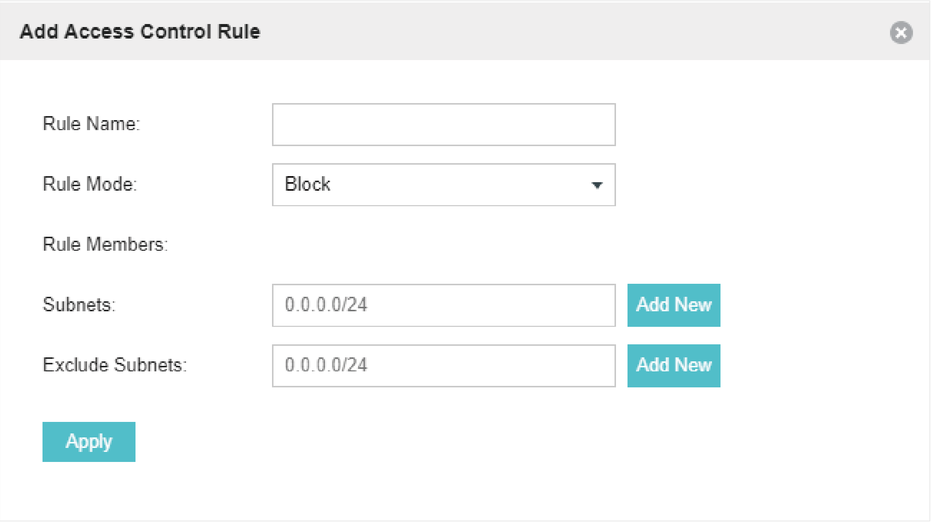
Access Control is used to block or allow the clients to access specific subnets. To configure Access Control rules, follow the steps below.

1. Go to **Wireless Control > Access Control.**



⇕ Access Control Rule	⇕ Rule Mode	Action
Default	Block	✎

2. Click Add Access Control Rule to add a new Access Control rule.



Add Access Control Rule

Rule Name:

Rule Mode: Block

Rule Members:

Subnets: 0.0.0.0/24

Exclude Subnets: 0.0.0.0/24

3. Configure the following parameters.

Rule Name	Specify a name for this rule.
Rule Mode	Select the mode for this rule. **Block**: Select this mode to block clients to access the specific subnets. **Allow**: Select this mode to allow clients to access the specific subnets.
Rule Members	Specify the member subnets for this rule. **Subnets**: Enter the subnet that will follow the rule mode in the format X.X.X.X/X and click Add New . Up to 16 subnets can be added. **Except Subnets**: Enter the excepted subnet in the format X.X.X.X/X and click Add New . Up to 16 subnets can be added. The rule mode will not apply to the subnet that is in both of the Subnets list and Except Subnets list.

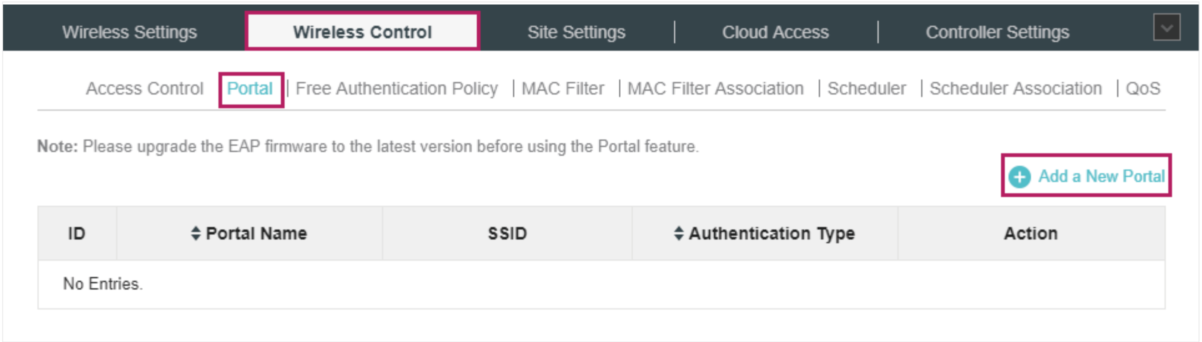
4. Click **Apply**.

5. Go to **Wireless Settings > Basic Wireless Setting** and enable Access Control function of a selected SSID.

3.3 Portal Authentication

Portal authentication enhances the network security by providing authentication service to the clients that just need temporary access to the wireless network. Such clients have to log into a web page to establish verification, after which they will access the network as guests. What's more, you can customize the authentication login page and specify a URL which the newly authenticated clients will be redirected to.

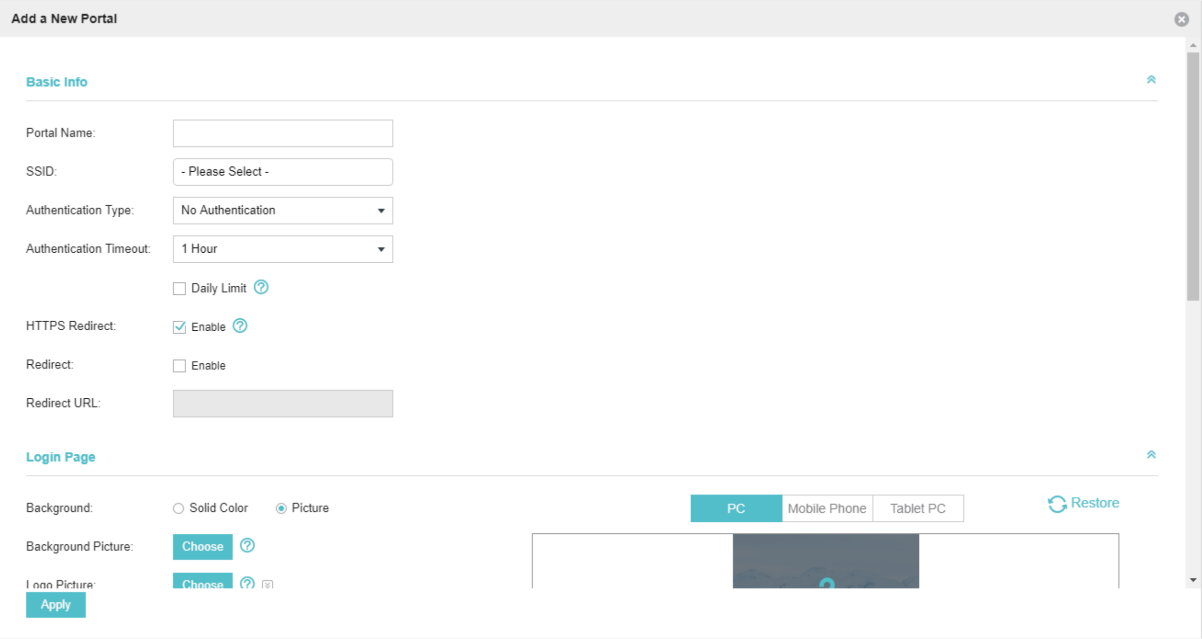
To configure Portal Authentication, go to **Wireless Control > Portal and click** + Add a New Portal **.**



Note: Please upgrade the EAP firmware to the latest version before using the Portal feature.

ID	⬍ Portal Name	SSID	⬍ Authentication Type	Action
No Entries.				

Then the following window will pop up:


Add a New Portal

Basic Info

Portal Name:

SSID: - Please Select -

Authentication Type: No Authentication

Authentication Timeout: 1 Hour

□ Daily Limit

HTTPS Redirect: ☑ Enable

Redirect: □ Enable

Redirect URL:

Login Page

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo Picture: Choose

Apply

These authentication methods are available: *No Authentication*, *Simple Password*, *Local User*, *Voucher*, *SMS*, *Facebook*, *External RADIUS Server* and *External Portal Server*. The following sections introduce how to configure each Portal authentication.

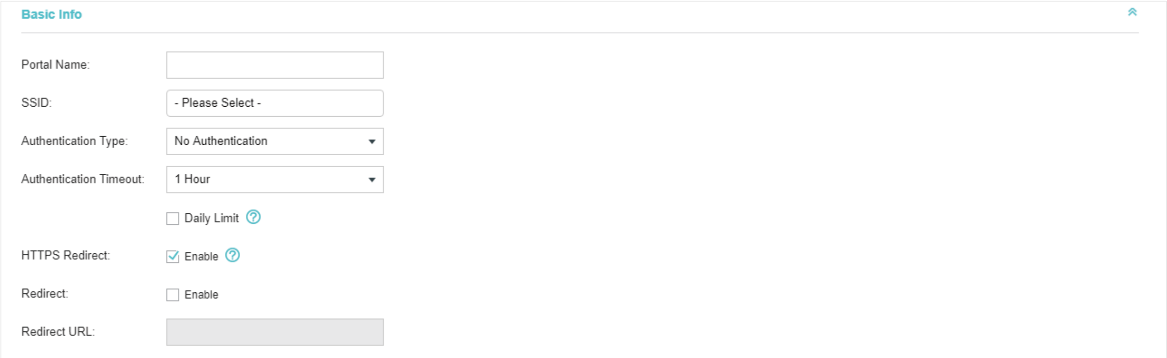
3.3.1 No Authentication

With No Authentication configured, clients can access the network without any authentication.

Follow the steps below to configure No Authentication:

1. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.

2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.


Basic Info

Portal Name:

SSID: - Please Select -

Authentication Type: No Authentication

Authentication Timeout: 1 Hour

□ Daily Limit

HTTPS Redirect: ☑ Enable

Redirect: □ Enable

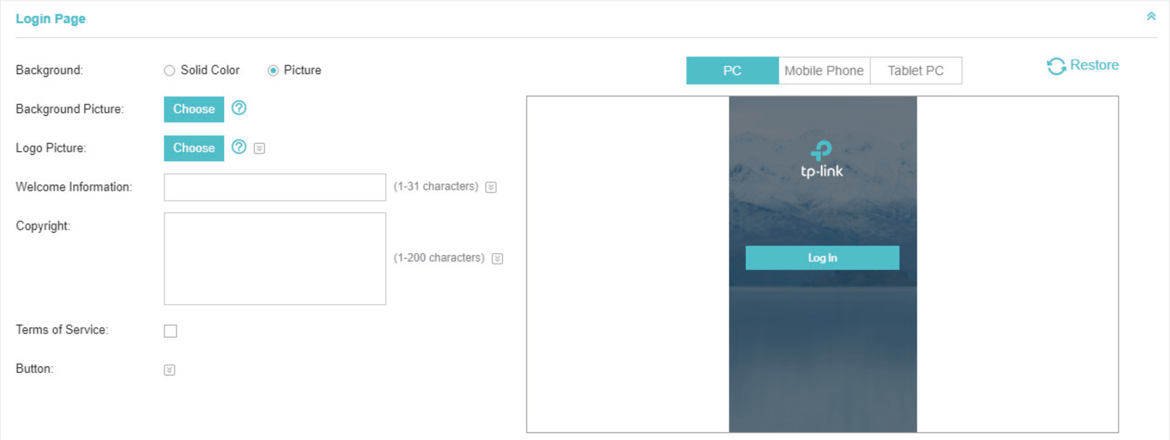
Redirect URL:

Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.

Authentication Type	Select **No Authentication**.
Authentication Timeout	With Daily Limit disabled, the client's authentication will expire after the time period you set and the client needs to log in on the web authentication page again to access the network. Options include **1 Hour, 8 Hours, 24 Hours, 7 Days** and **Custom**. **Custom** allows you to define the time in days, hours and minutes. The default value is one hour. With Daily Limit enabled, the client's authentication will expire after the time period you set and the client cannot log in again in the same day. Options include **30 Minutes, 1 Hour, 2 Hours, 4 Hours** and **8 Hours, Custom. Custom** allows you to define the time in hours and minutes. The default value is 30 minutes.
Daily Limit	With Daily Limit enabled, after authentication times out, the user cannot get authenticated again in the same day.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. In the **Login Page** section, configure the login page for the Portal.



Login Page

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo Picture: Choose

Welcome Information: (1-31 characters)

Copyright: (1-200 characters)

Terms of Service: □

Button:

Configure the following parameters:

Background	Select the background type. Two types are supported: **Solid Color** and **Picture**.
Background Color	If **Solid Color** is selected, configure your desired background color through the color picker or by entering the RGB value manually.

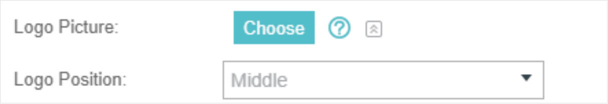
Background Picture

If **Picture** is selected, click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**.

Logo Picture

Click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**.

In addtion, you can click ⌄ and configure the logo position. The options include **Middle, Upper** and **Lower**.



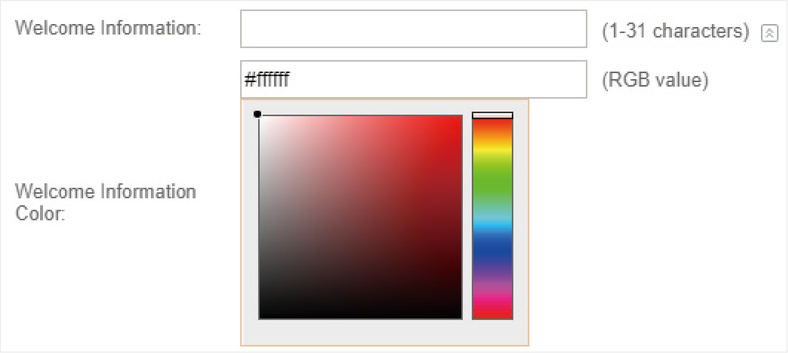
Logo Picture: Choose ? ⌃

Logo Position: Middle ▾

Welcome Information

Specify the welcome information.

In addtion, you can click ⌄ and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



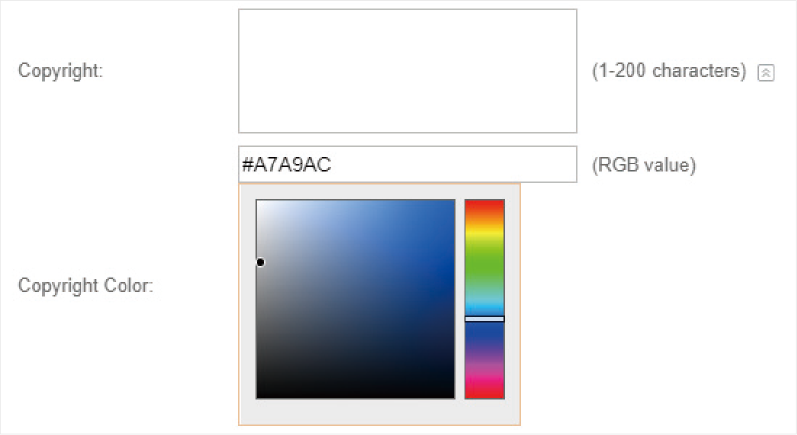
Welcome Information: (1-31 characters) ⌃

Welcome Information Color: #ffffff (RGB value)

Copyright

Specify the copyright information.

In addtion, you can click ⌄ and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.

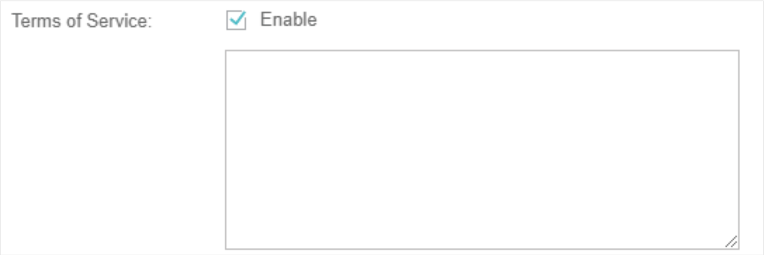


Copyright: (1-200 characters) ⌃

Copyright Color: #A7A9AC (RGB value)

Terms of Service

Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.



Terms of Service: ☑ Enable

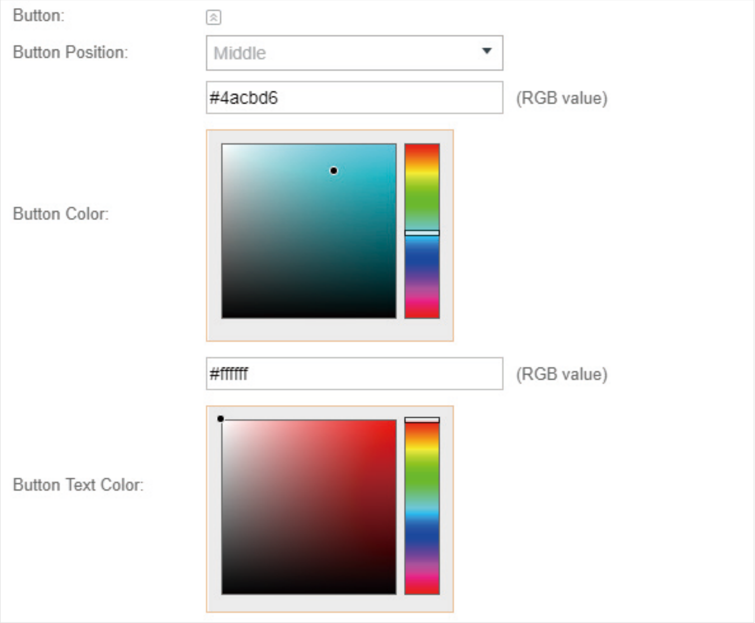
Button

Click ⌄ and configure the button.

Button Position: Set the position of the login button. The options include **Middle, Upper** and **Lower.**

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



Button:

Button Position: Middle

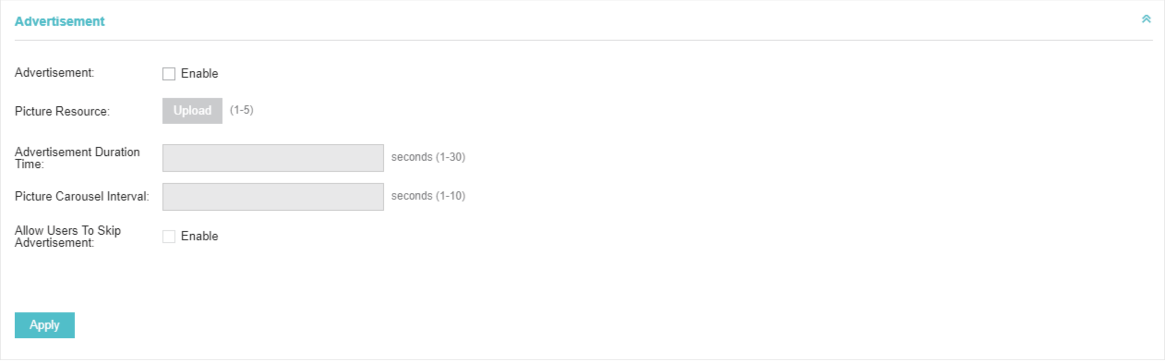
#4acbd6 (RGB value)

Button Color:

#ffffff (RGB value)

Button Text Color:

4. In the **Advertisement** section, select whether display advertisement pictures for users and configure the related parameters.



Advertisement

Advertisement: □ Enable

Picture Resource: Upload (1-5)

Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: □ Enable

Apply

Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow to Skip Advertisement**. The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

5. Click **Apply**.

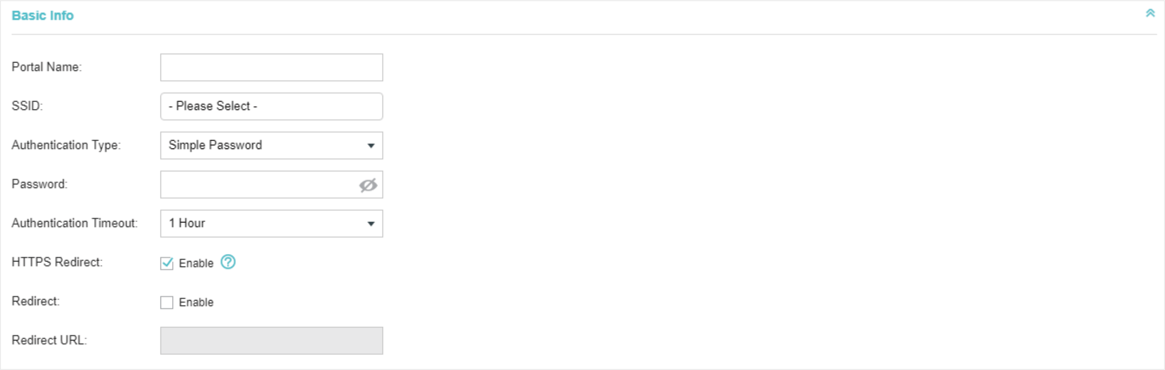
3.3.2 Simple Password

With this Simple Password configured, clients are required to enter the correct password to pass the authentication.

Follow the steps below to configure No Simple Password Portal:

1. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.

2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.



Basic Info

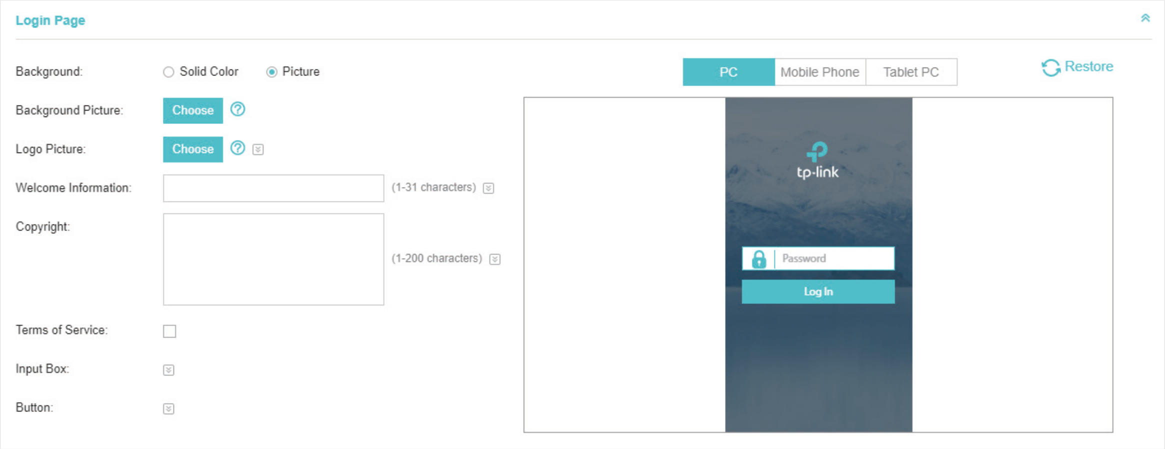
Portal Name:	
SSID:	- Please Select -
Authentication Type:	Simple Password
Password:	
Authentication Timeout:	1 Hour
HTTPS Redirect:	☑ Enable
Redirect:	□ Enable
Redirect URL:	

Configure the following parameters:

Portal Name	Specify a name for the Portal.

SSID	Select an SSID for the Portal.
Authentication Type	Select **Simple Password**.
Password	Set the password for authentication.
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in the web authentication page again to access the network. Options include **1 Hour, 8 Hours, 24 Hours, 7 Days** and **Custom**. **Custom** allows you to define the time in days, hours and minutes. The default value is one hour.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. In the **Login Page** section, configure the login page for the Portal.


Login Page

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo Picture: Choose

Welcome Information: (1-31 characters)

Copyright: (1-200 characters)

Terms of Service: □

Input Box:

Button:

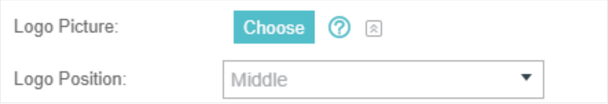
Configure the following parameters:

Background	Select the background type. Two types are supported: **Solid Color** and **Picture**.
Background Color	If **Solid Color** is selected, configure your desired background color through the color picker or by entering the RGB value manually.
Background Picture	If **Picture** is selected, click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**.

Logo Picture

Click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**.

In addtion, you can click ▾ and configure the logo position. The options include **Middle, Upper** and **Lower**.



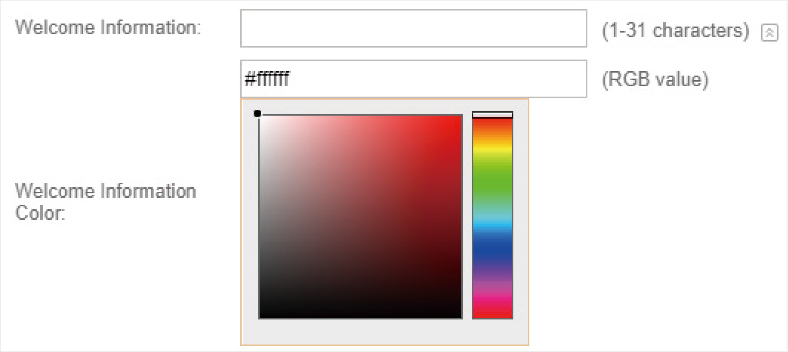
Logo Picture: Choose ? ▴

Logo Position: Middle ▾

Welcome Information

Specify the welcome information.

In addtion, you can click ▾ and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



Welcome Information: (1-31 characters) ▴

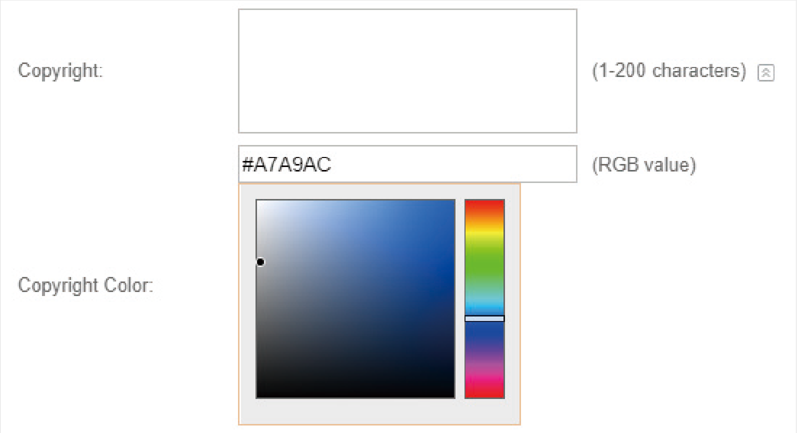
#ffffff (RGB value)

Welcome Information Color:

Copyright

Specify the copyright information.

In addtion, you can click ▾ and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.



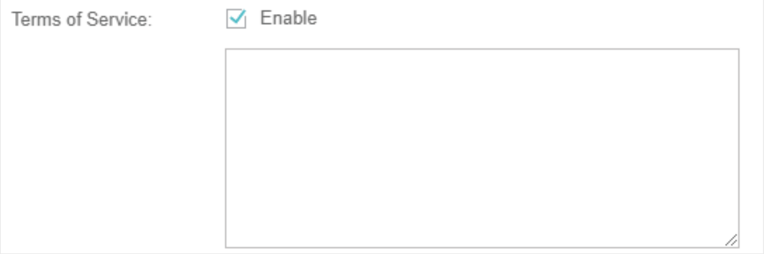
Copyright: (1-200 characters) ▴

#A7A9AC (RGB value)

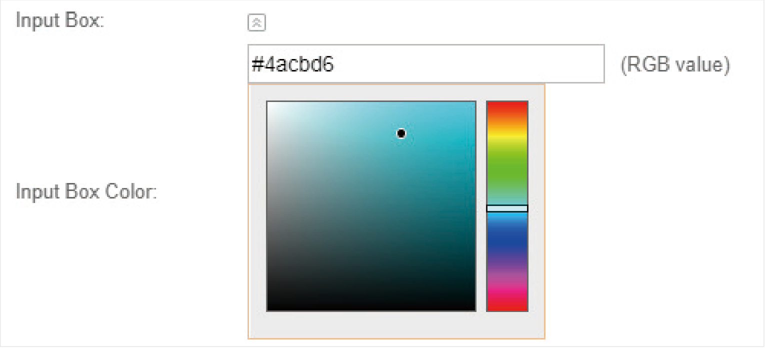
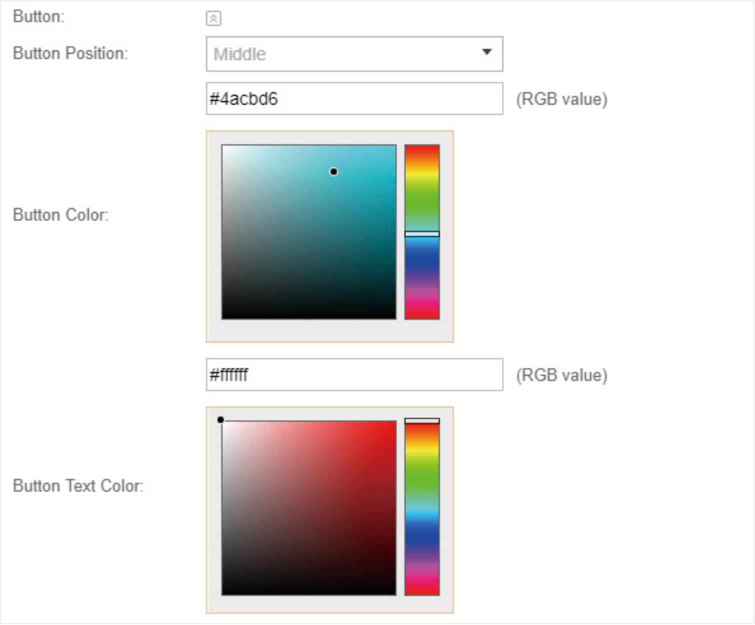
Copyright Color:

Terms of Service

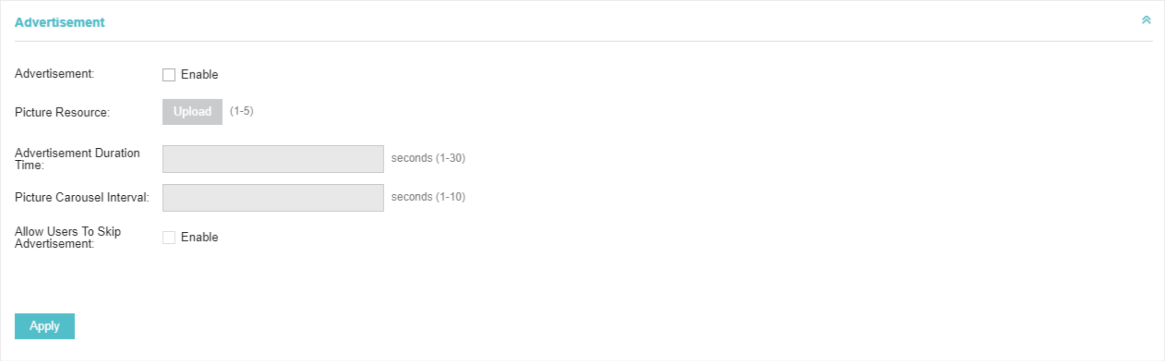
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.



Terms of Service: ☑ Enable

Input Box	Click ⌄ and configure the input box. Select your desired color for the input box through the color picker or by entering the RGB value manually.  Input Box: ⌃ Input Box Color: #4acbd6 (RGB value)
Button	Click ⌄ and configure the button. **Button Position**: Set the position of the login button. The options include **Middle, Upper** and **Lower.** **Button Color**: Select your desired login button color through the color picker or by entering the RGB value manually. **Button Text Color**: Select your desired text color for the button through the color picker or by entering the RGB value manually.  Button: ⌃ Button Position: Middle Button Color: #4acbd6 (RGB value) Button Text Color: #ffffff (RGB value)

4. In the **Advertisement** section, select whether display advertisement pictures for users and configure the related parameters.



Advertisement

Advertisement: □ Enable

Picture Resource: Upload (1-5)

Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: □ Enable

Apply

Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow to Skip Advertisement**. The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

5. Click **Apply**.

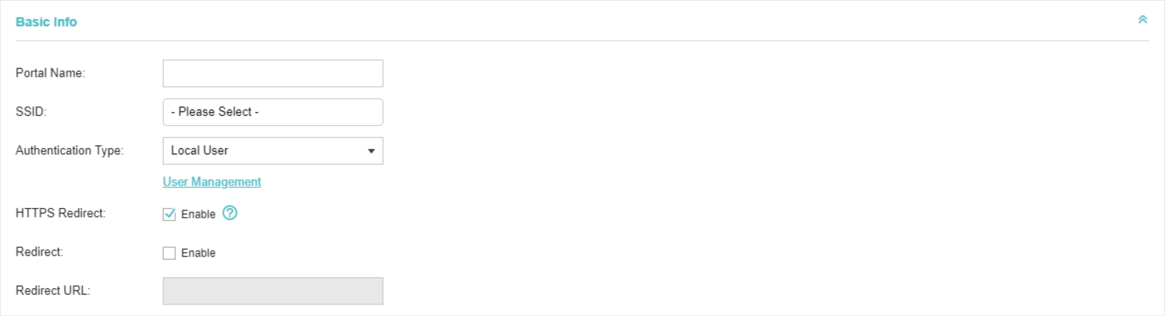
3.3.3 Local User

With this Local User configured, clients are required to enter the correct username and password of the login account to pass the authentication. You can create multiple accounts and assign different accounts for different users.

Configure Local User Portal

Follow the steps below to configure Local User Portal:

1. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.
2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.



Basic Info

Portal Name:

SSID: - Please Select -

Authentication Type: Local User

User Management

HTTPS Redirect: ☑ Enable

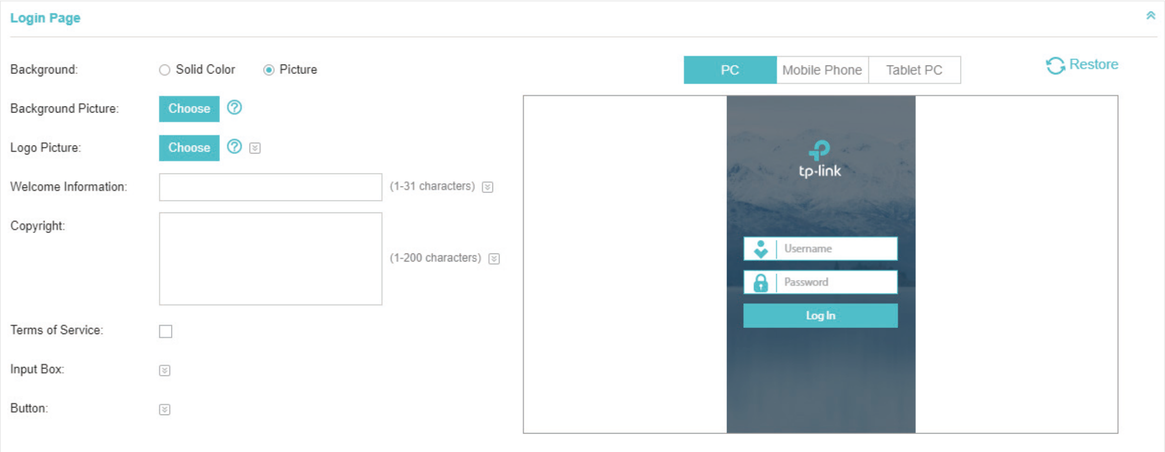
Redirect: □ Enable

Redirect URL:

Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **Local User**.
User Management	You can click this button to configure user accounts for authentication later. Please refer to Create Local User Accounts.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. In the **Login Page** section, configure the login page for the Portal.



Login Page

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo Picture: Choose

Welcome Information: (1-31 characters)

Copyright: (1-200 characters)

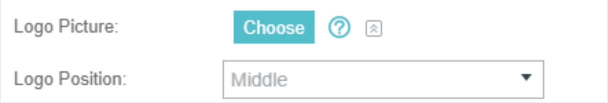
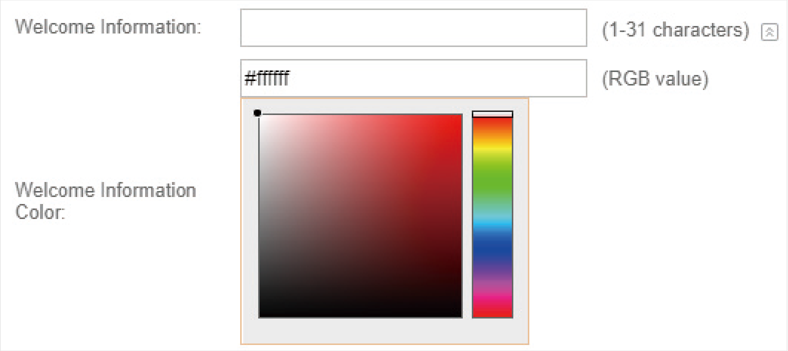
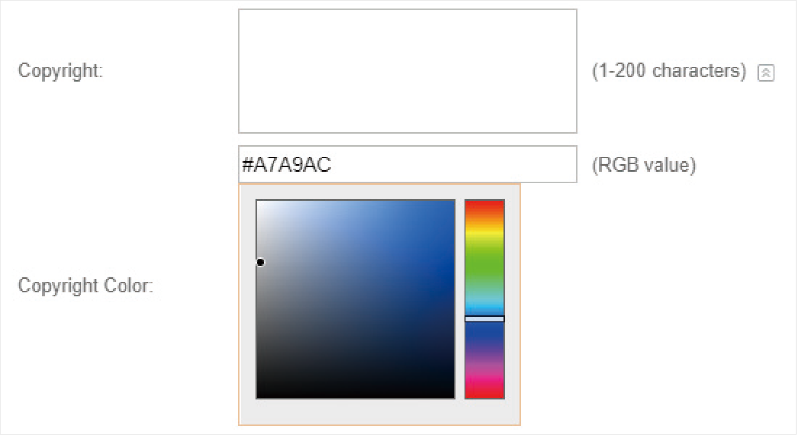
Terms of Service: □

Input Box:

Button:

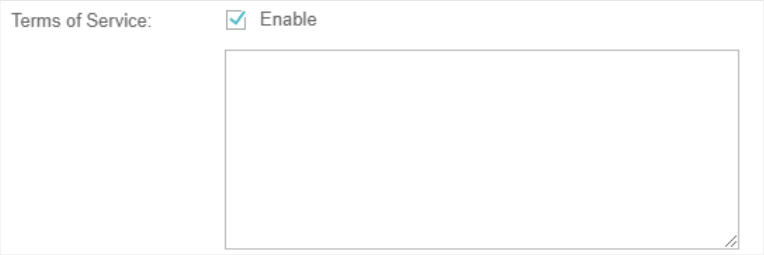
Configure the following parameters:

Background	Select the background type. Two types are supported: **Solid Color** and **Picture**.

Background Color	If **Solid Color** is selected, configure your desired background color through the color picker or by entering the RGB value manually.
Background Picture	If **Picture** is selected, click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**.
Logo Picture	Click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**. In addtion, you can click ⊻ and configure the logo position. The options include **Middle, Upper** and **Lower**.  Logo Picture: Choose Logo Position: Middle
Welcome Information	Specify the welcome information. In addtion, you can click ⊻ and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.  Welcome Information: (1-31 characters) #ffffff (RGB value) Welcome Information Color:
Copyright	Specify the copyright information. In addtion, you can click ⊻ and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.  Copyright: (1-200 characters) #A7A9AC (RGB value) Copyright Color:

Terms of Service

Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

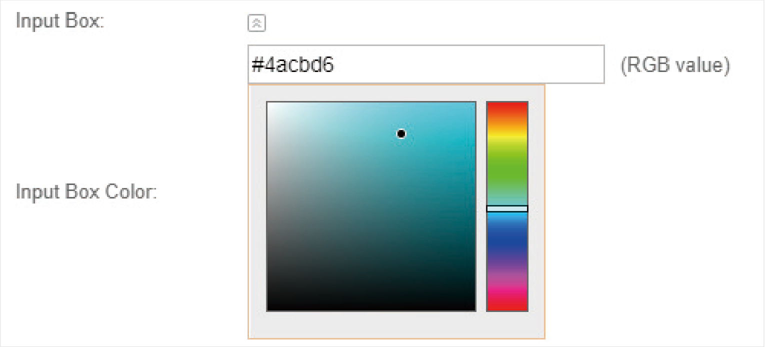


Terms of Service: ☑ Enable

Input Box

Click ⌄ and configure the input box.

Select your desired color for the input box through the color picker or by entering the RGB value manually.



Input Box: ⌃

#4acbd6 (RGB value)

Input Box Color:

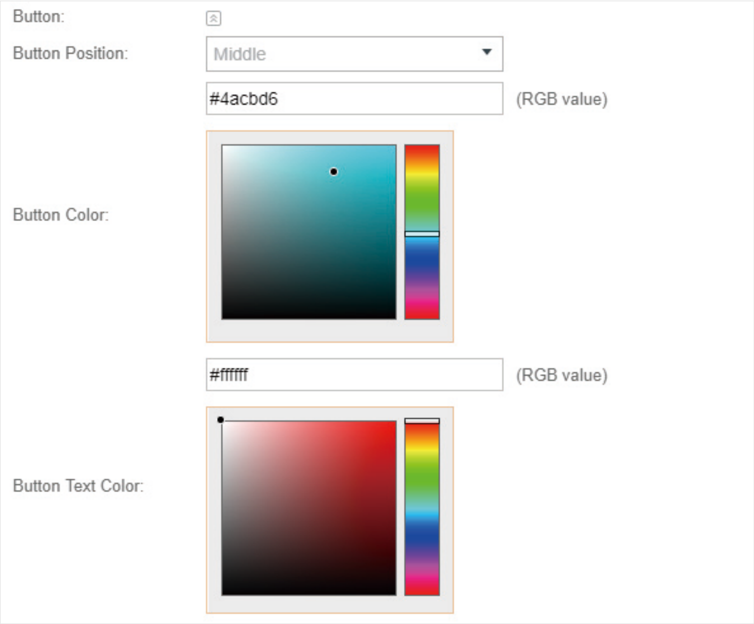
Button

Click ⌄ and configure the button.

Button Position: Set the position of the login button. The options include **Middle, Upper** and **Lower.**

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



Button: ⌃

Button Position: Middle

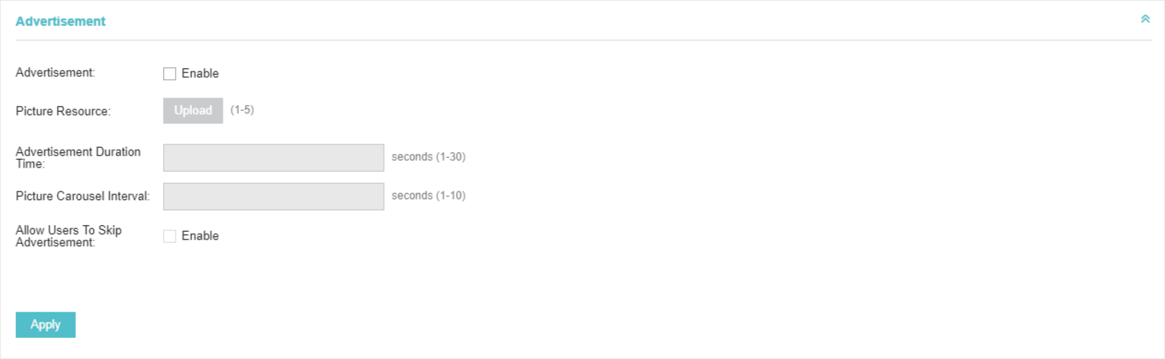
#4acbd6 (RGB value)

Button Color:

#ffffff (RGB value)

Button Text Color:

4. In the **Advertisement** section, select whether display advertisement pictures for users and configure the related parameters.



Advertisement

Advertisement: □ Enable

Picture Resource: Upload (1-5)

Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: □ Enable

Apply

Configure the following parameters:

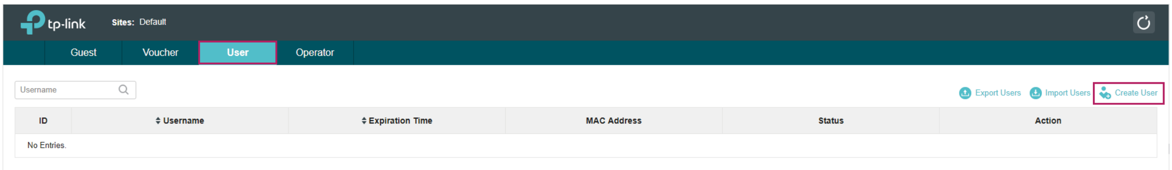
Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow to Skip Advertisement**. The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

5. Click **Apply.**

Create Local User Accounts

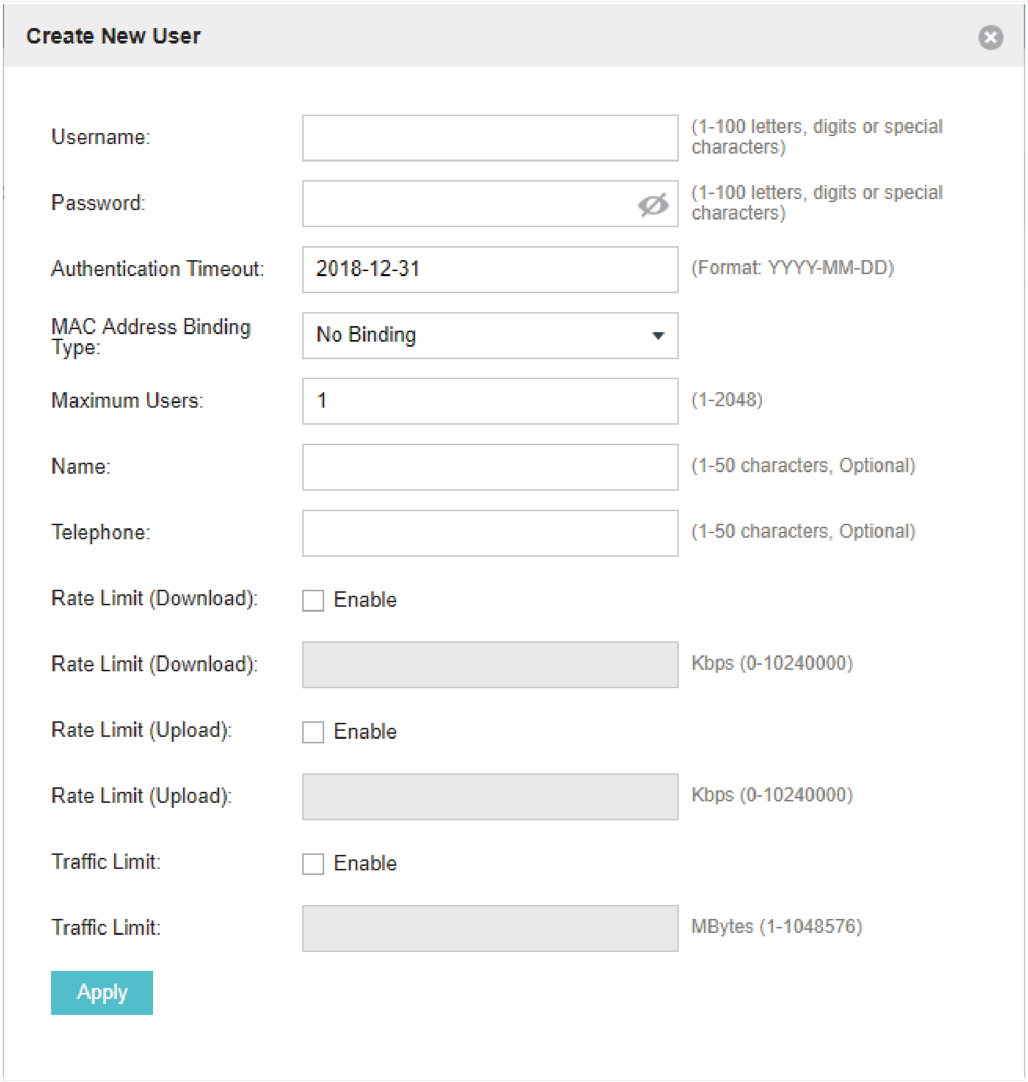
Follow the steps below to create the user accounts for authentication:

1. In the **Basic Info** section on the portal configuration page, click **User Management.** The management page will appear. Go to the **User** page and click Create User .



ID	Username	Expiration Time	MAC Address	Status	Action
No Entries.					

2. The following window will pop up. Configure the required parameters and click **Apply.**



Username:		(1-100 letters, digits or special characters)
Password:		(1-100 letters, digits or special characters)
Authentication Timeout:	2018-12-31	(Format: YYYY-MM-DD)
MAC Address Binding Type:	No Binding	
Maximum Users:	1	(1-2048)
Name:		(1-50 characters, Optional)
Telephone:		(1-50 characters, Optional)
Rate Limit (Download):	□ Enable	
Rate Limit (Download):		Kbps (0-10240000)
Rate Limit (Upload):	□ Enable	
Rate Limit (Upload):		Kbps (0-10240000)
Traffic Limit:	□ Enable	
Traffic Limit:		MBytes (1-1048576)

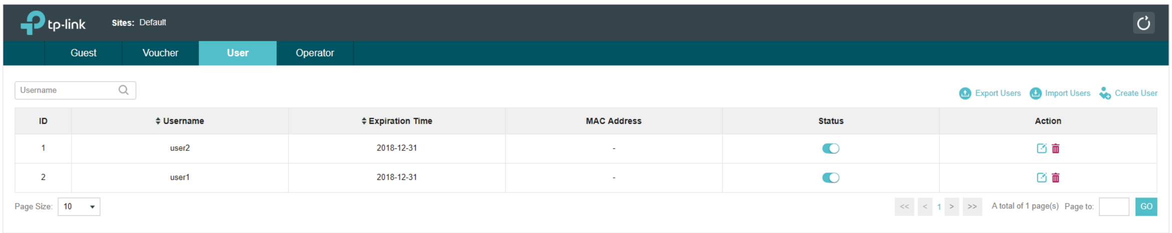
Configure the following parameters:

Username	Specify the username. The username should not be the same as any existing one.
Password	Specify the password. Users will be required to enter the username and password when they attempt to access the network.
Authentication Timeout	Specify the authentication timeout for formal users. After timeout, the users need to log in at the web authentication page again to access the network.
MAC Address Binding Type	There are three types of MAC binding: **No Binding**, **Static Binding** and **Dynamic Binding**. **Static Binding:** Specify a MAC address for this user account. Then only the user with the this MAC address can use the username and password to pass the authentication. **Dynamic Binding:** The MAC address of the first user that passes the authentication will be bound. Then only this user can use the username and password to pass the authentication.

Maximum Users	Specify the maximum number of users able to use this account to pass the authencitation.
Name	Specify a name for identification.
Telephone	Specify a telephone number for identification.
Rate Limit (Download)	Select whether to enable download rate limit. With this option enabled, you can specify the limit of download rate.
Rate Limit (Upload)	Select whether to enable upload rate limit. With this option enabled, you can specify the limit of upload rate.
Traffic Limit	Select whether to enable traffic limit. With this option enabled, you can specify the total traffic limit for the user. Once the limit is reached, the user can no longer use this account to access the network.

3. In the same way, you can add more user accounts. The created user accounts will be displayed in the list. Users can use the username and password of the account to pass the portal authentication.

   By default, the account Status is ●, which means that the user account is enabled and valid. You can also click this button to disable the user account. The icon will be changed to ○, which means that the user account is disabled.



ID	Username	Expiration Time	MAC Address	Status	Action
1	user2	2018-12-31	-	●	✎ 🗑
2	user1	2018-12-31	-	●	✎ 🗑

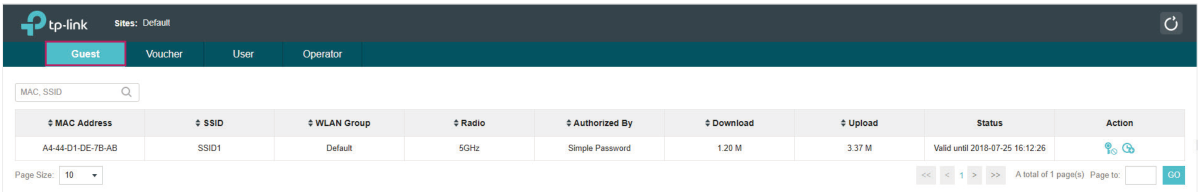
   Additionally, you can click Export Users to backup all the user account information into a CSV file or XLS file and save the file to your PC. If needed, you can click Import Users and select the file to import the account information to the list.

Note:

Using Excel to open the CSV file may cause some numerical format changes, and the number may be displayed incorrectly. If you use Excel to edit the CSV file, please set the cell format as text.

Manage the Guests

On the Guest page, you can view the information of clients that have passed the portal authentication and manage the clients.



MAC Address	SSID	WLAN Group	Radio	Authorized By	Download	Upload	Status	Action
A4-44-D1-DE-7B-AB	SSID1	Default	5GHz	Simple Password	1.20 M	3.37 M	Valid until 2018-07-25 16:12:26	

You can select an icon to execute the corresponding operation:

⊘	Disconnect client.
⊕	Extend the effective time.

Create Operator Accounts

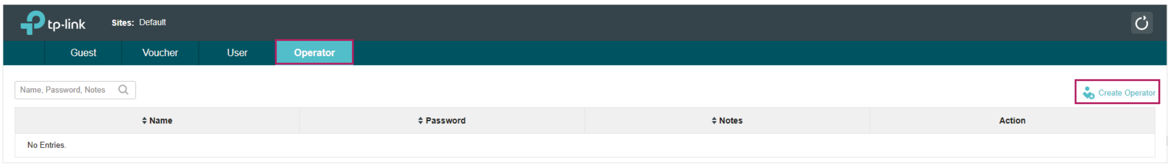
Operator account can be used to remotely manage the Local User Portal and Voucher Portal. Other users can visit the URL **https://OC200 Host's IP Address:8043/hotspot** (For example: https://192.168.0.64:8043/hotspot) and use the Operator account to enter the portal management page.

Note:

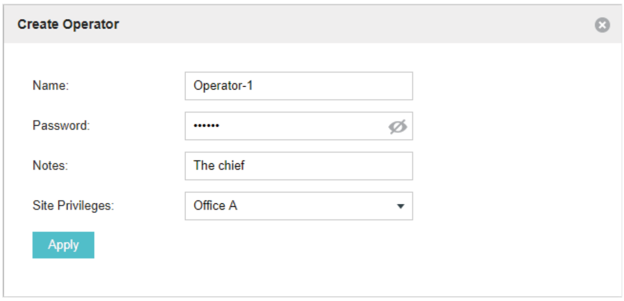
The users who enter the portal management page by Operator account can only create local user accounts and vouchers and manage the clients.

Follow the steps below to create Operator account.

1. Go to the **Operator** page.



2. Click Create Operator and the following window will pop up.


Create Operator

Name: Operator-1

Password: ••••••

Notes: The chief

Site Privileges: Office A

3. Specify the **Name**, **Password** and **Notes** of the Operator account.

4. Select **Site Privileges** from the drop-down list (multiple options available) for the Operator account.

5. Click **Apply** to create an Operator account. Then other users can use this account to enter the hotspot management page.

3.3.4 Voucher

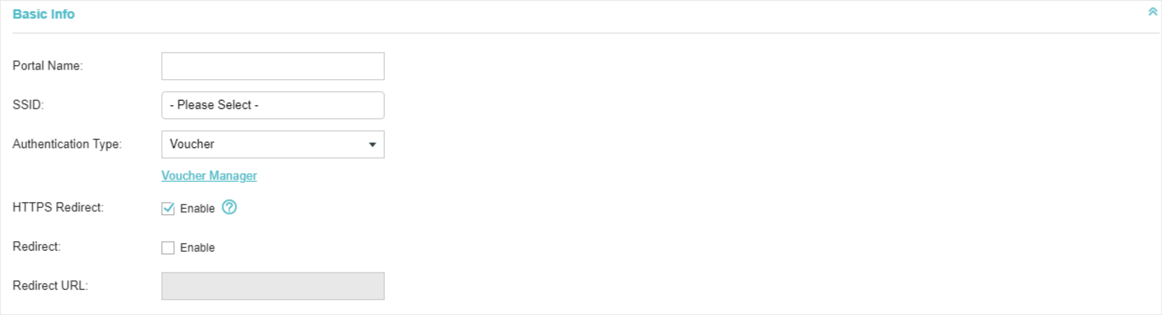
With Voucher configured, you can distribute the vouchers automatically generated by the OC200 to the clients. Clients can use the vouchers to access the network.

Configure Voucher Portal

Follow the steps below to configure Voucher Portal:

1. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.

2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.



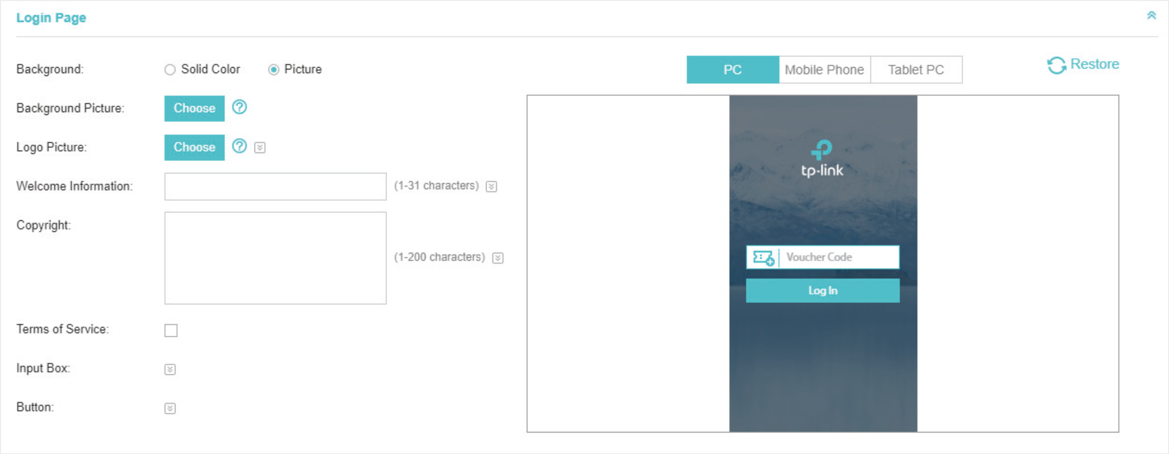
Basic Info

Portal Name:	
SSID:	- Please Select -
Authentication Type:	Voucher Voucher Manager
HTTPS Redirect:	☑ Enable
Redirect:	□ Enable
Redirect URL:	

Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **Voucher**.
User Management	You can click this button to configure vouchers for authentication later. Please refer to Create Vouchers.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. In the **Login Page** section, configure the login page for the Portal.



Login Page

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo Picture: Choose

Welcome Information: (1-31 characters)

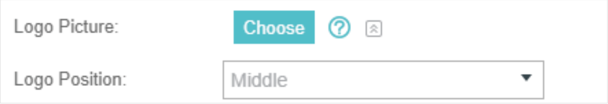
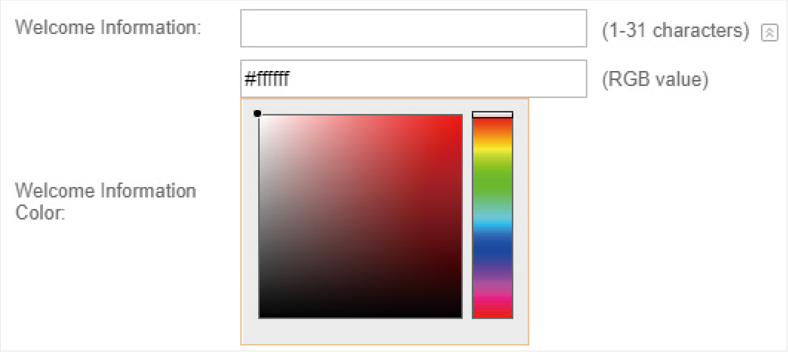
Copyright: (1-200 characters)

Terms of Service: □

Input Box:

Button:

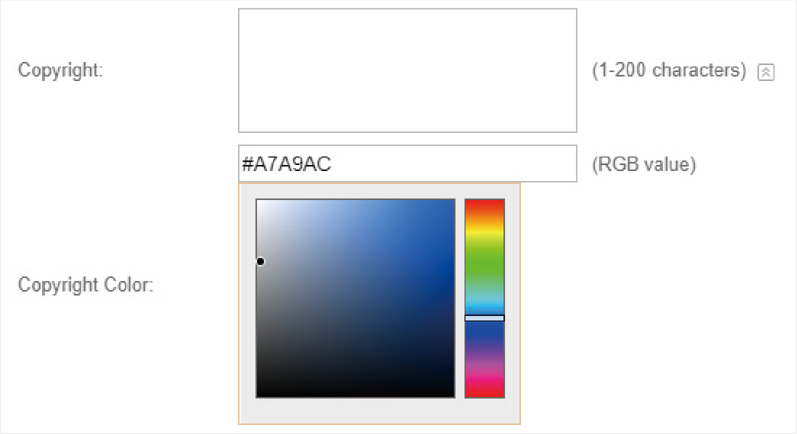
Configure the following parameters:

Background	Select the background type. Two types are supported: **Solid Color** and **Picture**.
Background Color	If **Solid Color** is selected, configure your desired background color through the color picker or by entering the RGB value manually.
Background Picture	If **Picture** is selected, click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**.
Logo Picture	Click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**. In addtion, you can click ⌄ and configure the logo position. The options include **Middle, Upper** and **Lower**.  Logo Picture: Choose Logo Position: Middle
Welcome Information	Specify the welcome information. In addtion, you can click ⌄ and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.  Welcome Information: (1-31 characters) #ffffff (RGB value) Welcome Information Color:

Copyright

Specify the copyright information.

In addtion, you can click ⊻ and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.

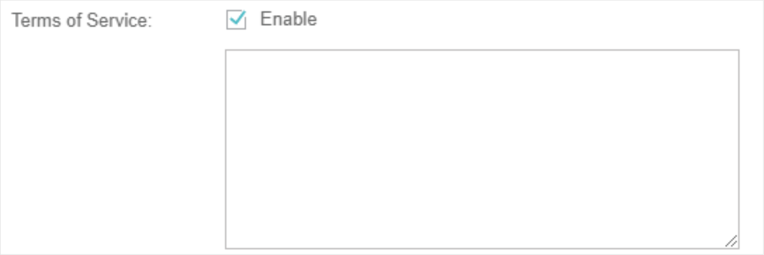


Copyright: (1-200 characters) ⊼

Copyright Color: #A7A9AC (RGB value)

Terms of Service

Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

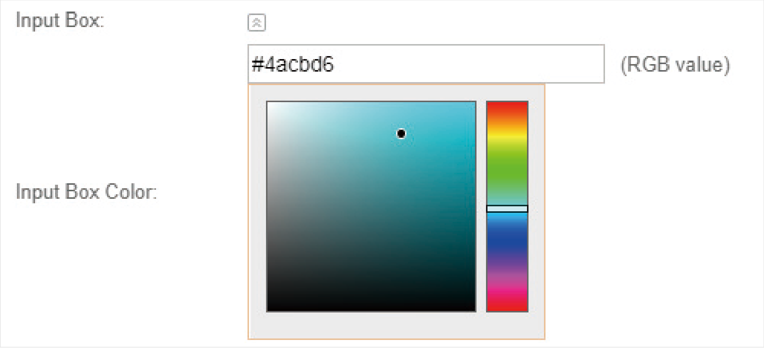


Terms of Service: ☑ Enable

Input Box

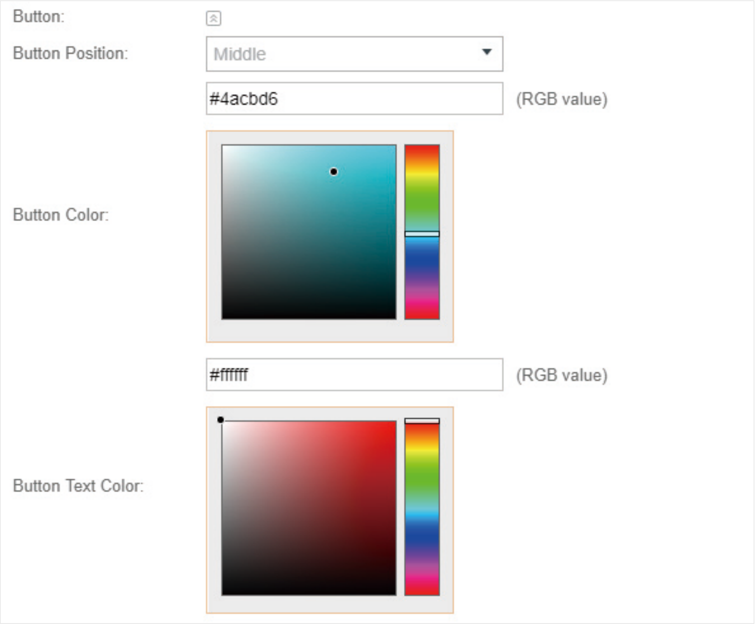
Click ⊻ and configure the input box.

Select your desired color for the input box through the color picker or by entering the RGB value manually.

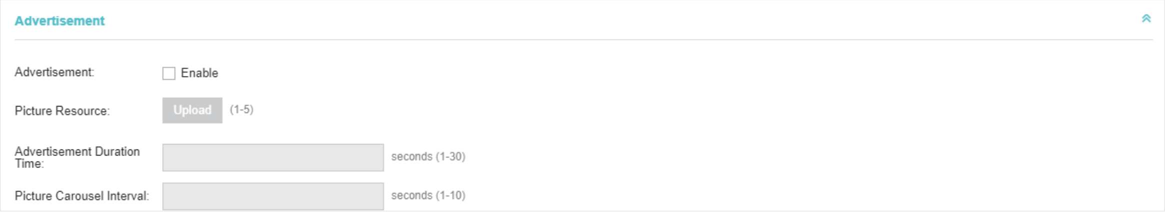


Input Box: ⊼

Input Box Color: #4acbd6 (RGB value)

Button	Click ⊻ and configure the button. **Button Position**: Set the position of the login button. The options include **Middle, Upper** and **Lower.** **Button Color**: Select your desired login button color through the color picker or by entering the RGB value manually. **Button Text Color**: Select your desired text color for the button through the color picker or by entering the RGB value manually.  Button: Button Position: Middle Button Color: #4acbd6 (RGB value) Button Text Color: #ffffff (RGB value)

4. In the **Advertisement** section, select whether display advertisement pictures for users and configure the related parameters.



Advertisement

Advertisement: □ Enable

Picture Resource: Upload (1-5)

Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow to Skip Advertisement**. The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.

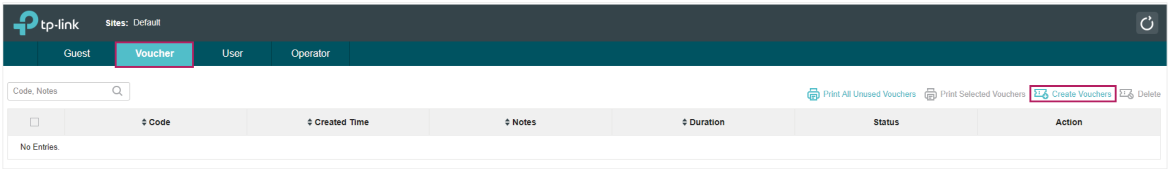
Picture Careusel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

5. Click **Apply**.

Create Vouchers

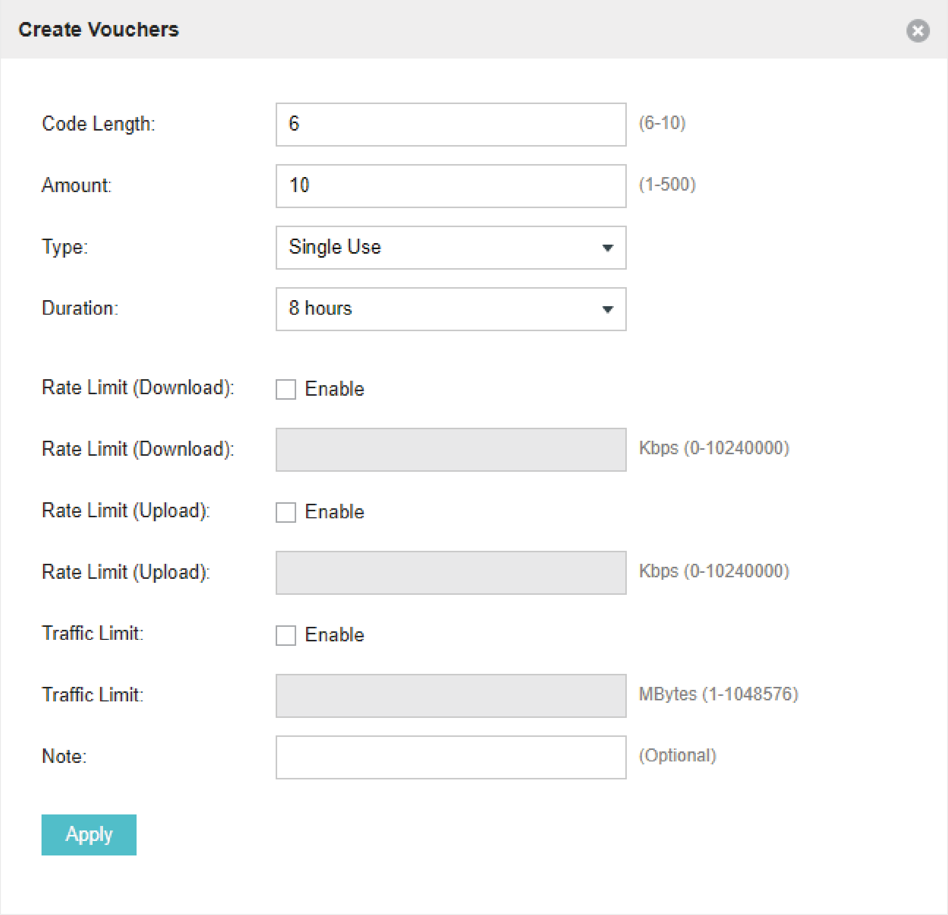
Follow the steps below to create vouchers for authentication:

1. In the **Basic Info** section, click **Voucher Manager.** The voucher management page will appear. Go to the **Voucher** page and click Create Vouchers .



□	♦ Code	♦ Created Time	♦ Notes	♦ Duration	Status	Action
No Entries.						

2. The following window will pop up. Configure the required parameters and click **Apply.**



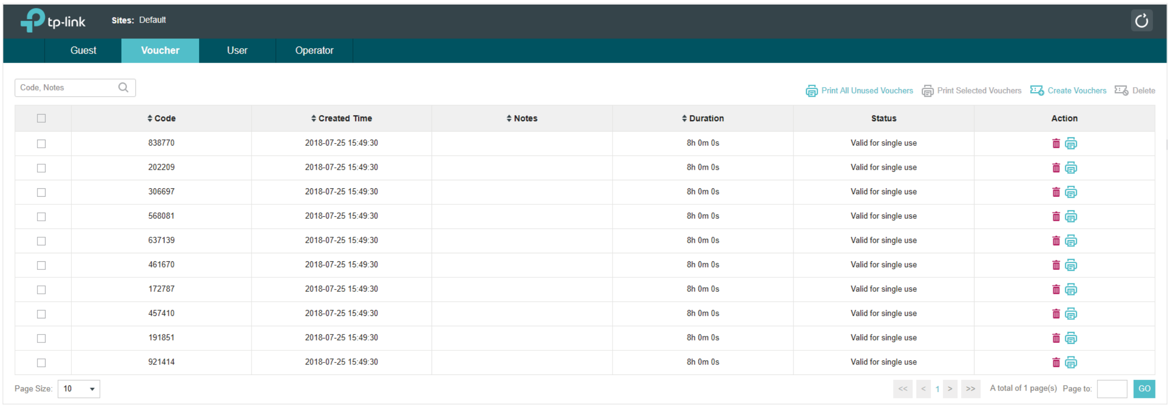
Create Vouchers

Code Length:	6	(6-10)
Amount:	10	(1-500)
Type:	Single Use	
Duration:	8 hours	
Rate Limit (Download):	□ Enable	
Rate Limit (Download):		Kbps (0-10240000)
Rate Limit (Upload):	□ Enable	
Rate Limit (Upload):		Kbps (0-10240000)
Traffic Limit:	□ Enable	
Traffic Limit:		MBytes (1-1048576)
Note:		(Optional)

Configure the following parameters:

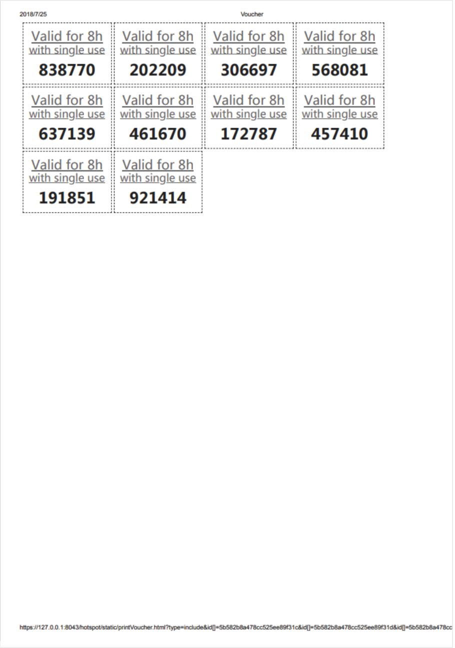
Code Length	Specify the length of the voucher codes to be created.
Amount	Enter the voucher amount to be generated.
Type	Select **Single Use** or **Multi Use**. Single Use means one voucher can only be distributed to one client. Multi Use means one voucher can be distributed to several clients, who can use the same voucher to access the network at the same time. If you select Multi Use, enter the value of **Max Users**. When the number of clients who are connected to the network with the same voucher reaches the value, no more clients can use this voucher to access the network.
Duration	Select the period of validity of the Voucher. The options include **8 hours**, **2 days** and **User-defined**. The period of valid of the voucher is reckoned from the time when it is used for the first time.
Rate Limit (Download)	Select whether to enable download rate limit. With this option enabled, you can specify the limit of download rate.
Rate Limit (Upload)	Select whether to enable upload rate limit. With this option enabled, you can specify the limit of upload rate.
Traffic Limit	Specify the total traffic limit for one voucher. Once the limit is reached, the client can no longer access the network using the voucher.
Notes	Enter a description for the Voucher (optional).

3. The Vouchers will be generated and displayed on the page.



□	Code	Created Time	Notes	Duration	Status	Action
□	838770	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨
□	202209	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨
□	306697	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨
□	568081	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨
□	637139	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨
□	461670	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨
□	172787	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨
□	457410	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨
□	191851	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨
□	921414	2018-07-25 15:49:30		8h 0m 0s	Valid for single use	🗑 🖨

4. Click 🖨 to print a single voucher; click 🖨 Print Selected Vouchers to print your selected vouchers; click 🖨 Print All Unused Vouchers to print all unused vouchers.



2018/7/25 Voucher

Valid for 8h with single use 838770	Valid for 8h with single use 202209	Valid for 8h with single use 306697	Valid for 8h with single use 568081
Valid for 8h with single use 637139	Valid for 8h with single use 461670	Valid for 8h with single use 172787	Valid for 8h with single use 457410
Valid for 8h with single use 191851	Valid for 8h with single use 921414		

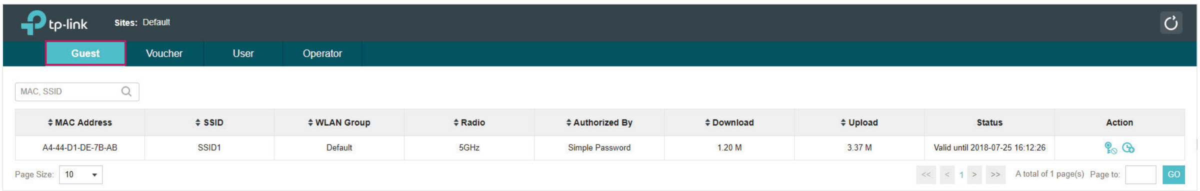
https://127.0.0.1:8043/hotspot/static/printVoucher.html?type=include&id[]=5b582b8a478cc525ee89f31c&id[]=5b582b8a478cc525ee89f31d&id[]=5b582b8a478cc

5. Distribute the vouchers to clients, and then they can use the codes to pass authentication.

6. When the vouchers are invalid, you can click to delete the Voucher or click Delete to delete the selected vouchers.

Manage the Guests

On the Guest page, you can view the information of clients that have passed the portal authentication and manage the clients.



MAC Address	SSID	WLAN Group	Radio	Authorized By	Download	Upload	Status	Action
A4-44-D1-DE-7B-AB	SSID1	Default	5GHz	Simple Password	1.20 M	3.37 M	Valid until 2018-07-25 16:12:26	

You can select an icon to execute the corresponding operation:

	Restrict the client to access the network.
	Extend the effective time.

Create Operator Accounts

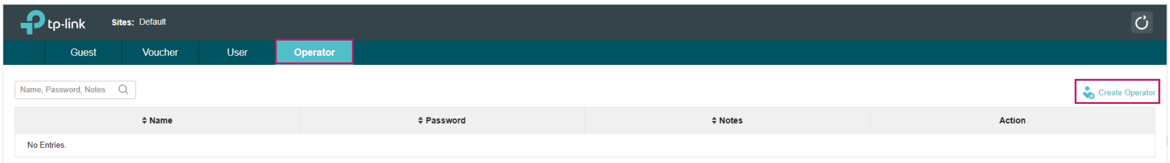
Operator account can be used to remotely manage the Local User Portal and Voucher Portal. Other users can visit the URL **https://OC200 Host's IP Address:8043/hotspot** (For example: https://192.168.0.64:8043/hotspot) and use the Operator account to enter the portal management page.

Note:

The users who enter the portal management page by Operator account can only create local user accounts and vouchers and manage the clients.

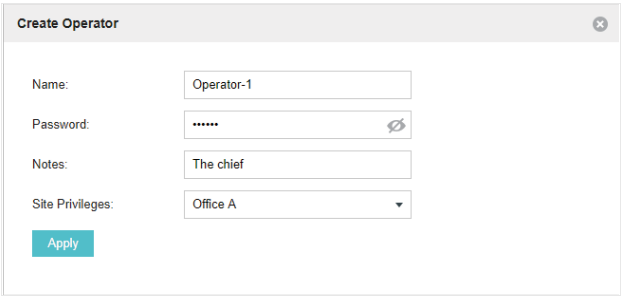
Follow the steps below to create Operator account.

1. Go to the **Operator** page.



Name	Password	Notes	Action
No Entries.			

2. Click Create Operator and the following window will pop up.



Name: Operator-1

Password: ••••••

Notes: The chief

Site Privileges: Office A

3. Specify the **Name**, **Password** and **Notes** of the Operator account.

4. Select **Site Privileges** from the drop-down list (multiple options available) for the Operator account.

5. Click **Apply** to create an Operator account. Then other users can use this account to enter the hotspot administrative system.

3.3.5 SMS

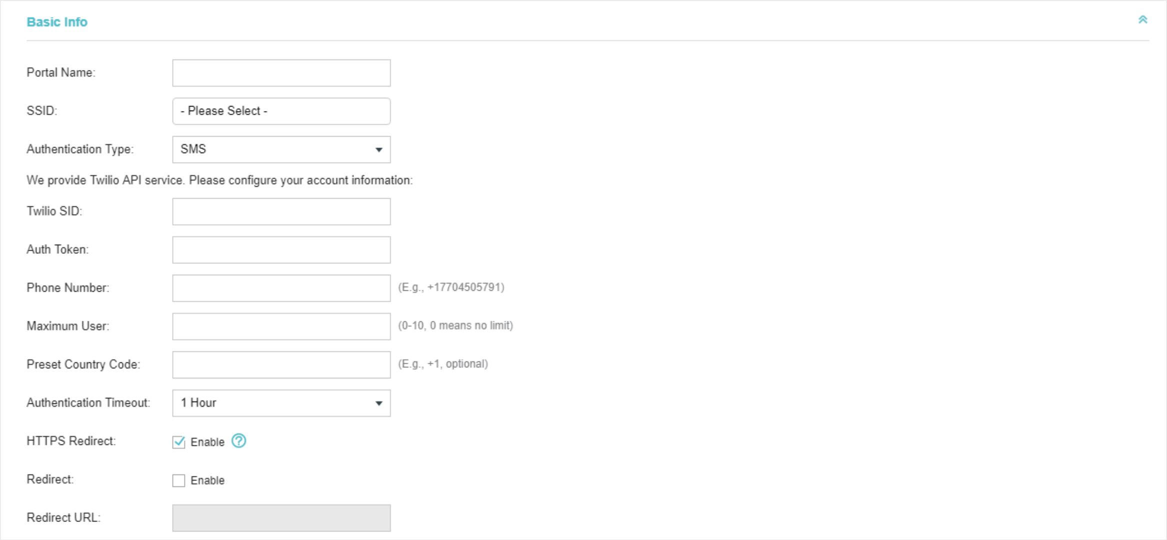
With SMS portal configured, client can get verification codes using their mobile phones and enter the received codes to pass the authentication.

Follow the steps below to configure SMS Portal:

1. Go to www.twilio.com/try-twilio and get a Twilio account. Buy the Twilio service for SMS. Then get the account information, including ACCOUNT SID, AUTH TOKEN and Phone number.

2. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.

3. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.



Basic Info

Portal Name:		
SSID:	- Please Select -	
Authentication Type:	SMS	

We provide Twilio API service. Please configure your account information:

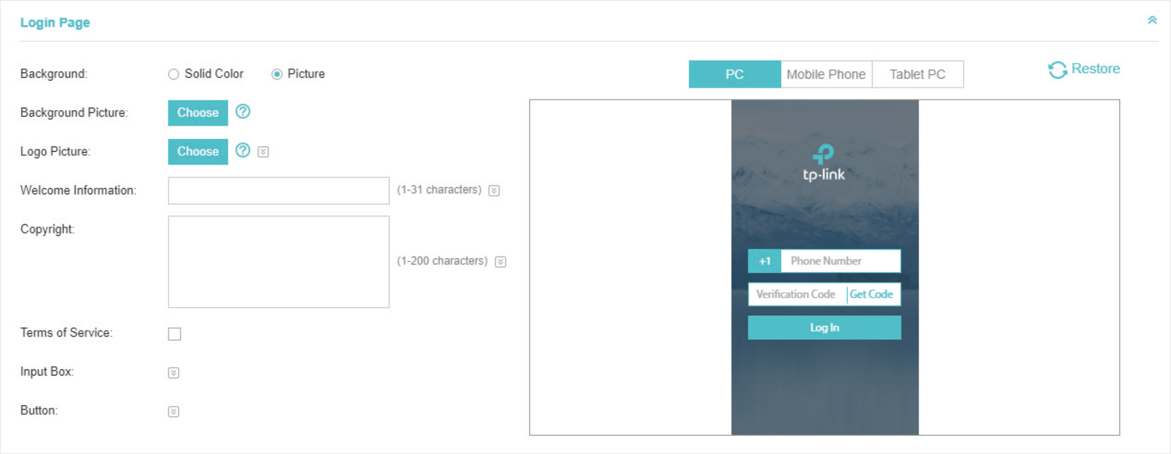
Twilio SID:		
Auth Token:		
Phone Number:		(E.g., +17704505791)
Maximum User:		(0-10, 0 means no limit)
Preset Country Code:		(E.g., +1, optional)
Authentication Timeout:	1 Hour	
HTTPS Redirect:	☑ Enable	
Redirect:	□ Enable	
Redirect URL:		

Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **SMS**.
Twilio SID	Enter the Account SID for Twilio API Credentials.
Auth Token	Enter the Authentication Token for Twilio API Credentials.
Phone Number	Enter the phone number that is used to send verification messages to the clients.
Maximum Users	A telephone can get several codes via messages one by one, and different clients can use different codes to pass the authentication. However, the number of clients that are allowed to be authenticated using the same telephone at the same time has a upper limit. Specify the upper limit in this field.
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in the web authentication page again to access the network. Options include **1 Hour, 8 Hours, 24 Hours, 7 Days** and **Custom**. **Custom** allows you to define the time in days, hours and minutes. The default value is one hour.
Preset Country Code	Set the default country code that will be filled automatically on the authentication page.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.

Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

4. In the **Login Page** section, configure the login page for the Portal.



Login Page

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo Picture: Choose

Welcome Information: (1-31 characters)

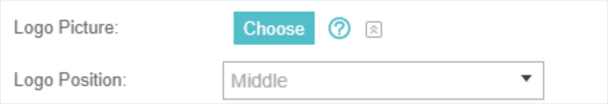
Copyright: (1-200 characters)

Terms of Service: □

Input Box:

Button:

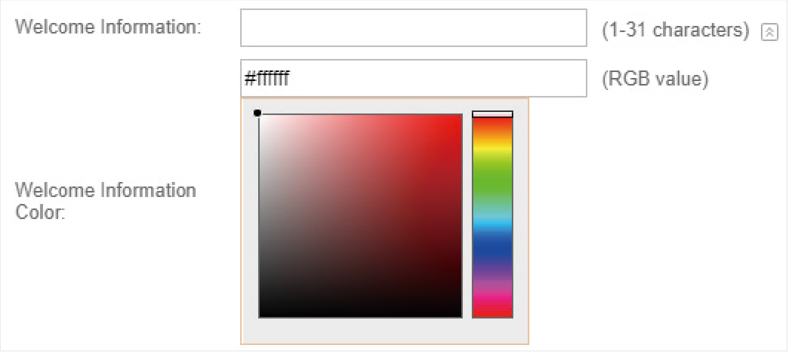
Configure the following parameters:

Background	Select the background type. Two types are supported: **Solid Color** and **Picture**.
Background Color	If **Solid Color** is selected, configure your desired background color through the color picker or by entering the RGB value manually.
Background Picture	If **Picture** is selected, click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**.
Logo Picture	Click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**. In addtion, you can click ⇊ and configure the logo position. The options include **Middle, Upper** and **Lower**.  Logo Picture: Choose Logo Position: Middle

Welcome Information

Specify the welcome information.

In addtion, you can click ▾ and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



Welcome Information: (1-31 characters)

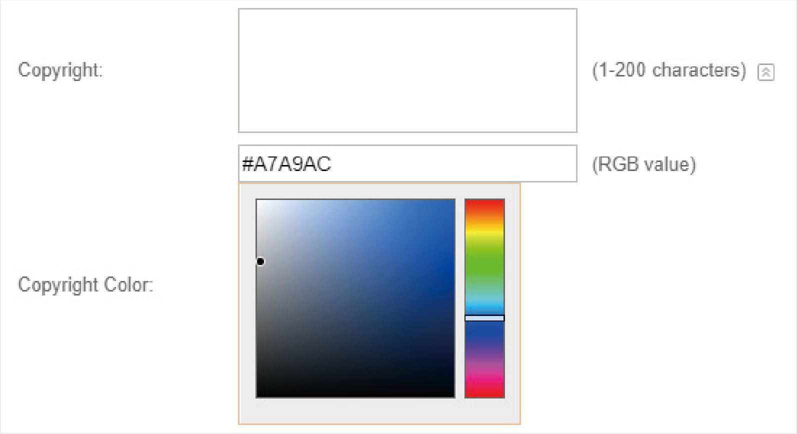
#ffffff (RGB value)

Welcome Information Color:

Copyright

Specify the copyright information.

In addtion, you can click ▾ and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.



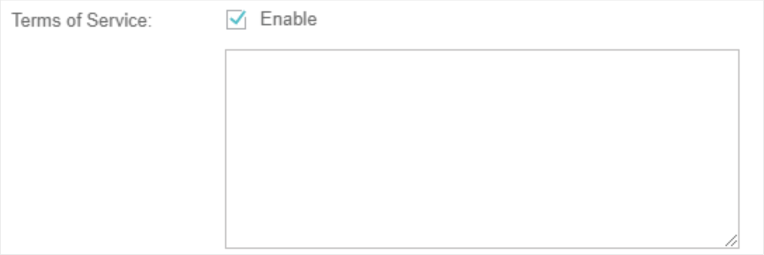
Copyright: (1-200 characters)

#A7A9AC (RGB value)

Copyright Color:

Terms of Service

Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

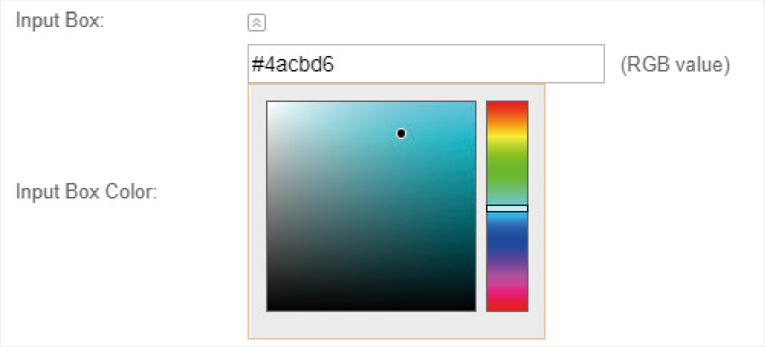


Terms of Service: ☑ Enable

Input Box

Click ⊻ and configure the input box.

Select your desired color for the input box through the color picker or by entering the RGB value manually.



Input Box: ⊼

Input Box Color: #4acbd6 (RGB value)

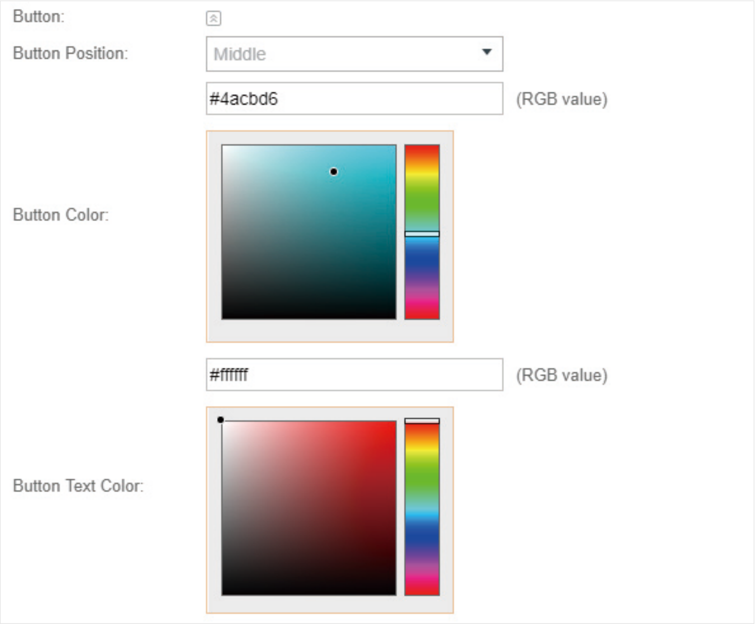
Button

Click ⊻ and configure the button.

Button Position: Set the position of the login button. The options include **Middle, Upper** and **Lower.**

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



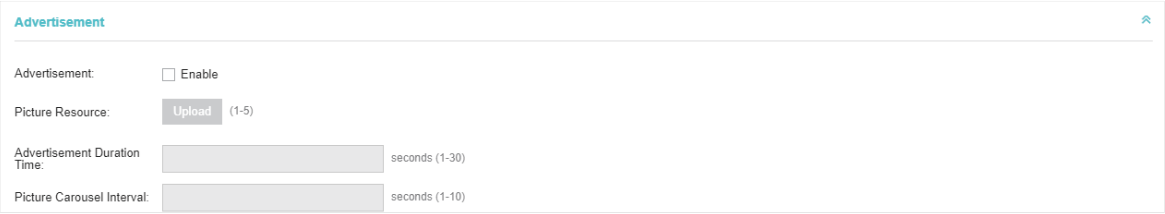
Button: ⊼

Button Position: Middle ▾

Button Color: #4acbd6 (RGB value)

Button Text Color: #ffffff (RGB value)

5. In the **Advertisement** section, select whether display advertisement pictures for users and configure the related parameters.



Advertisement

Advertisement: □ Enable

Picture Resource: Upload (1-5)

Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow to Skip Advertisement**. The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Careusel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

6. Click **Apply**.

For more details about how to configure SMS Portal, you can go to https://www.tp-link.com/en/configuration-guides.html and download the configuration guide for SMS Portal.

3.3.6 Facebook

With Facebook Portal configured, when clients connect to your Wi-Fi, they will be redirected to your Facebook page. To access the internet, clients need to pass the authentication on the page.

Note:

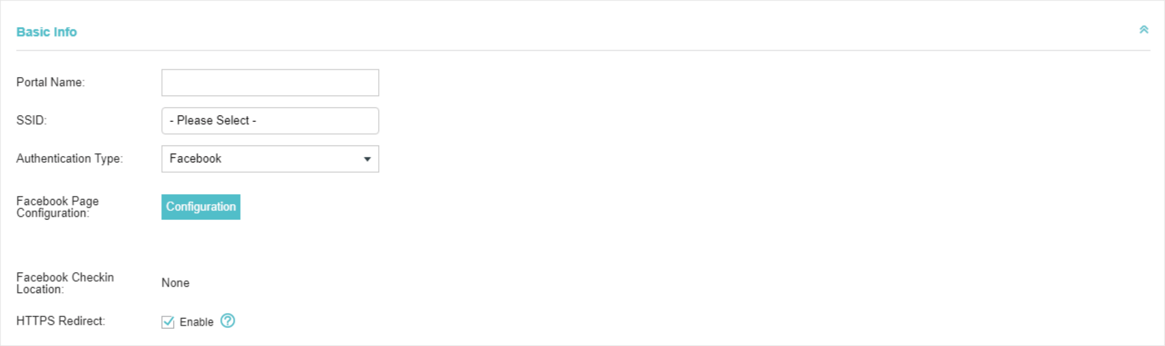
OC200 will automatically create Free Authentication Policy entries for the Facebook Portal. You don't need to create them manually.

Follow the steps below to configure Facebook Portal:

1. Go to www.facebook.com and get a Facebook account. Create your Facebook page according to your needs.

2. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.

3. Go back to the Portal configuration page. In the **Basic Info** section, complete the settings for the portal authentication.



Basic Info

Portal Name:

SSID: - Please Select -

Authentication Type: Facebook

Facebook Page Configuration: Configuration

Facebook Checkin Location: None

HTTPS Redirect: ☑ Enable

Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **Facebook**.
Facebook Page Configuration	Click this button to specify the Facebook Page.
Facebook Checkin Location	If the Facebook page is successfully got by the OC200, the name of the Facebook page will be displayed here.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.

For more details about how to configure Facebook Portal, you can go to https://www.tp-link.com/en/configuration-guides.html and download the configuration guide for Facebook Portal.

3.3.7 External RADIUS Server

If you have a RADIUS server, you can configure External RADIUS Server Portal. With this type of portal, you can get two types of portal customization: Local Web Portal and External Web Portal. The authentication login page of Local Web Portal is provided by the built-in portal server of the OC200. The External Web Portal is provided by external portal server.

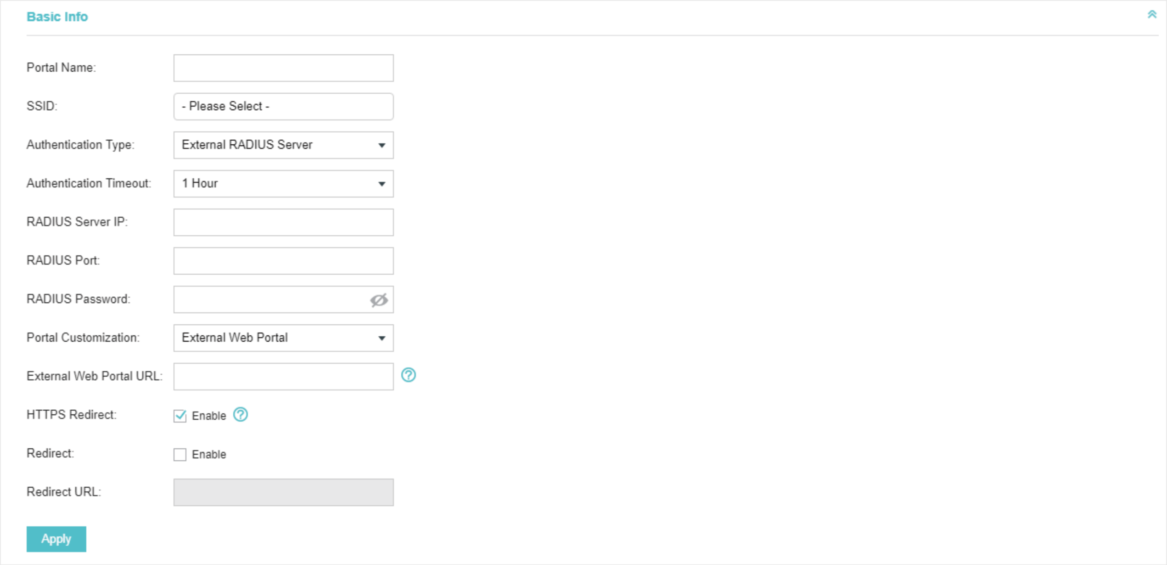
Note:

OC200 will automatically create Free Authentication Policy entries for the External RADIUS Portal.

Follow the steps below to configure External RADIUS Server Portal:

1. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.

2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.



Basic Info

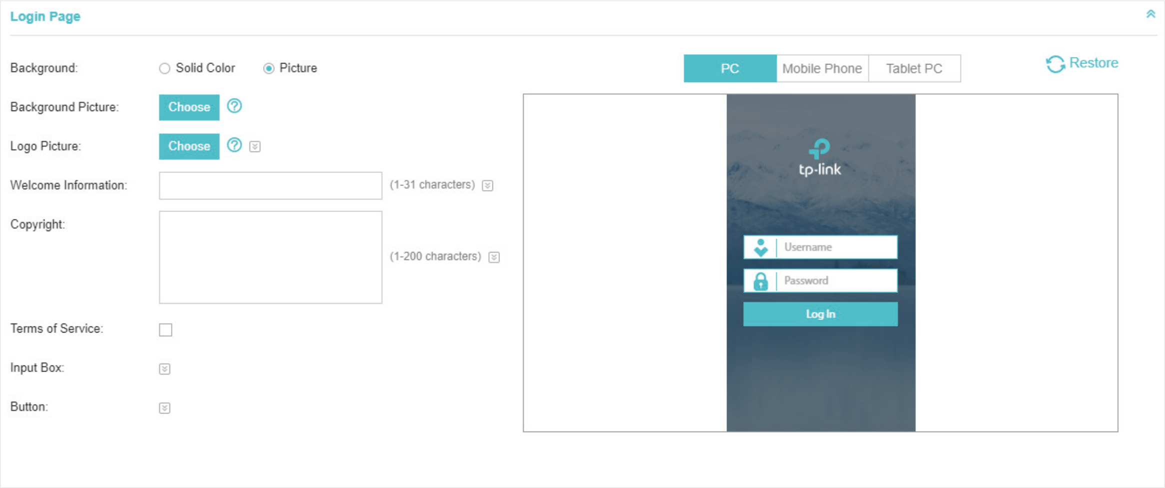
Portal Name:	
SSID:	- Please Select -
Authentication Type:	External RADIUS Server
Authentication Timeout:	1 Hour
RADIUS Server IP:	
RADIUS Port:	
RADIUS Password:	
Portal Customization:	External Web Portal
External Web Portal URL:	
HTTPS Redirect:	☑ Enable
Redirect:	□ Enable
Redirect URL:	

Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **External RADIUS Server**.
RADIUS Server IP	Enter the IP address of the RADIUS server.
RADIUS Port	Enter the port number you have set on the RADIUS server.
RADIUS Password	Enter the password you have set on the RADIUS Server.
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in the web authentication page again to access the network. Options include **1 Hour, 8 Hours, 24 Hours, 7 Days, Custom**. **Custom** allows you to define the time in days, hours, and minutes. The default value is one hour.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL. Disabled by default.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

Portal Customization	Select Local Web Portal or External Web Portal. **Local Web Portal**: If this option is selected, refer to step 4 to configure the login page and step 5 to configure the advertisement. **External Web Portal**: If this option is selected, follow the steps below. 1. Configure the external RADIUS server. 2. Enter the authentication login page's URL provided by the external portal server in the External Web Portal URL field.

3. **Local Web Portal** is configured, configure the login page for the Portal in the **Login Page** section.



Login Page

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo Picture: Choose

Welcome Information: (1-31 characters)

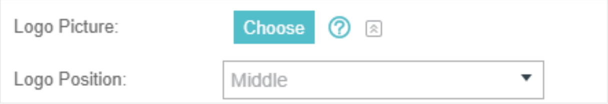
Copyright: (1-200 characters)

Terms of Service: □

Input Box:

Button:

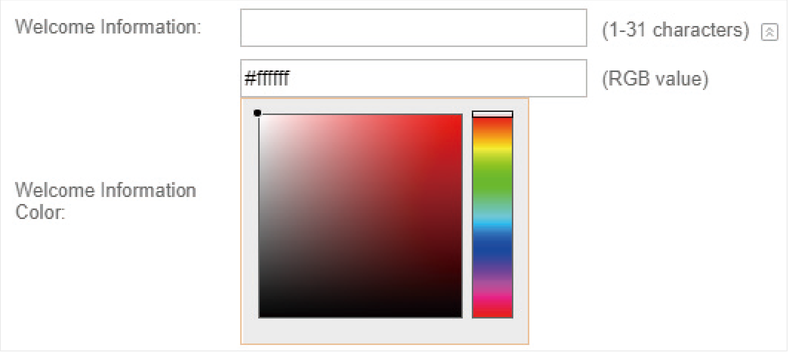
Configure the following parameters:

Background	Select the background type. Two types are supported: **Solid Color** and **Picture**.
Background Color	If **Solid Color** is selected, configure your desired background color through the color picker or by entering the RGB value manually.
Background Picture	If **Picture** is selected, click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**.
Logo Picture	Click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**. In addtion, you can click ⊻ and configure the logo position. The options include **Middle, Upper** and **Lower**.  Logo Picture: Choose Logo Position: Middle

Welcome Information

Specify the welcome information.

In addtion, you can click ⊻ and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



Welcome Information: (1-31 characters)

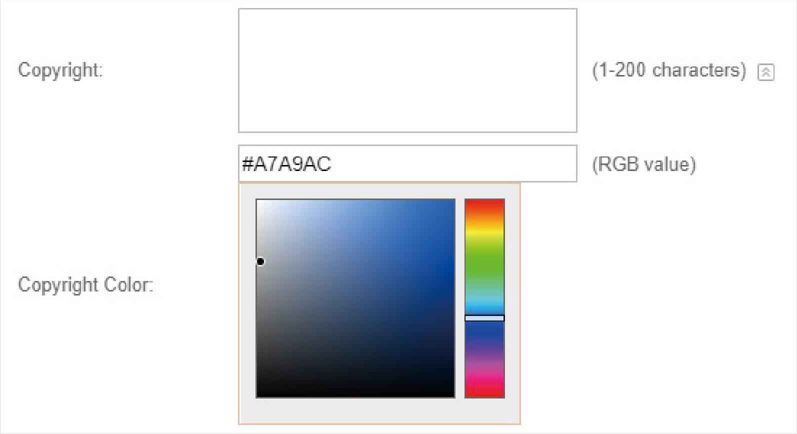
#ffffff (RGB value)

Welcome Information Color:

Copyright

Specify the copyright information.

In addtion, you can click ⊻ and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.



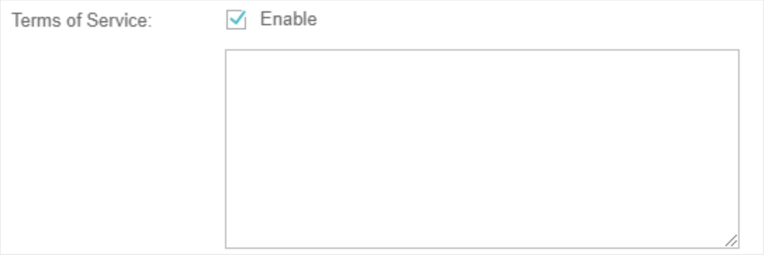
Copyright: (1-200 characters)

#A7A9AC (RGB value)

Copyright Color:

Terms of Service

Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

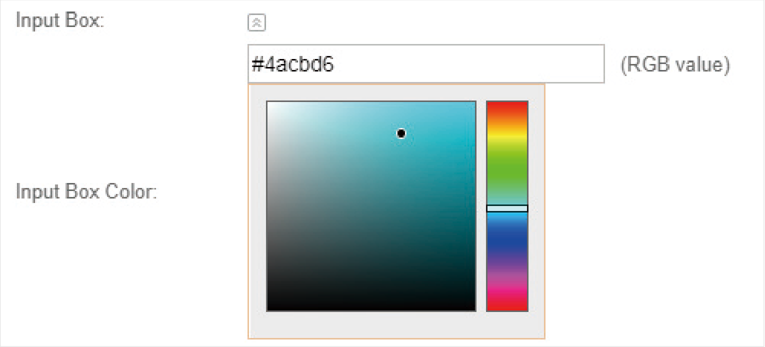


Terms of Service: ☑ Enable

Input Box

Click ⌄ and configure the input box.

Select your desired color for the input box through the color picker or by entering the RGB value manually.



Input Box: ⌃

Input Box Color: #4acbd6 (RGB value)

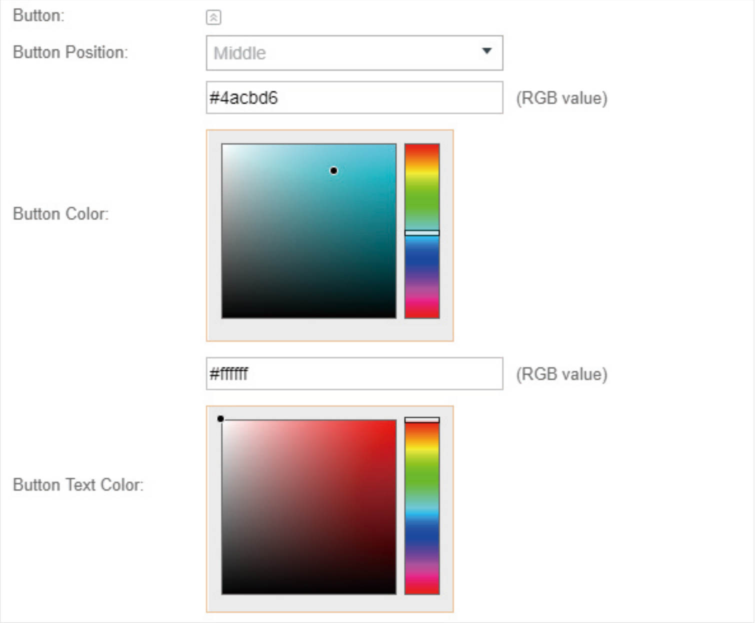
Button

Click ⌄ and configure the button.

Button Position: Set the position of the login button. The options include **Middle, Upper** and **Lower.**

Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.



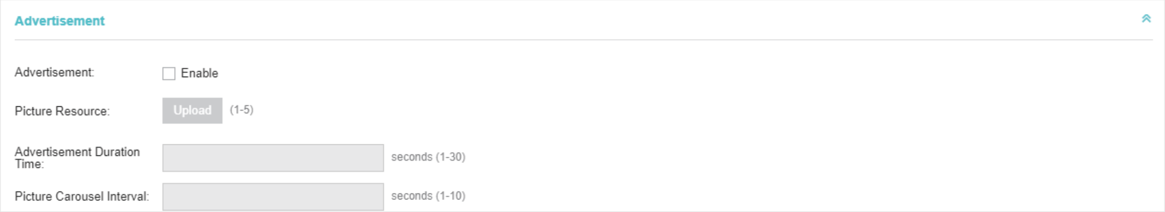
Button: ⌃

Button Position: Middle ▾

Button Color: #4acbd6 (RGB value)

Button Text Color: #ffffff (RGB value)

4. If **Local Web Portal** is configured, select whether display advertisement pictures for users and configure the related parameters in the **Advertisement** section, .



Advertisement

Advertisement: □ Enable

Picture Resource: Upload (1-5)

Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow to Skip Advertisement**.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Careusel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

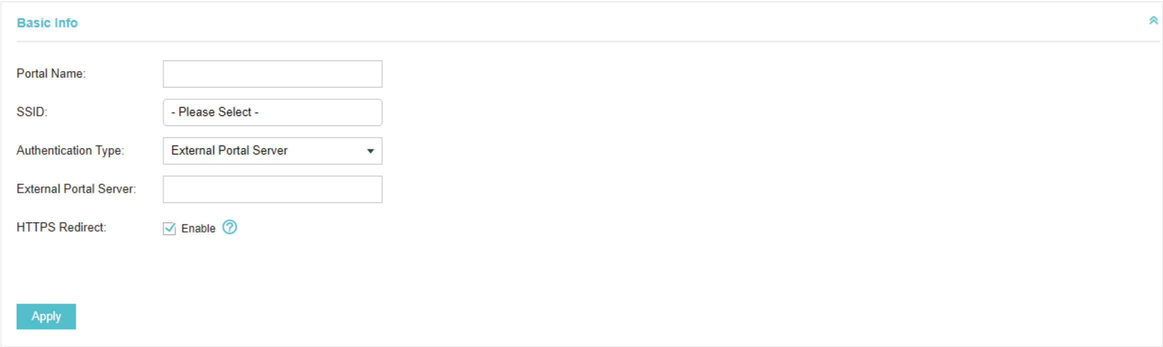
5. Click **Apply**.

3.3.8 External Portal Server

The option of External Portal Server is designed for the developers. They can customized their own authentication type according to the interface provided by OC200, e.g. message authentication and WeChat authentication etc.

1. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.

2. Go back to the Portal configuration page. In the **Basic Info** section, complete the settings for the portal authentication.



Basic Info

Portal Name:

SSID: - Please Select -

Authentication Type: External Portal Server

External Portal Server:

HTTPS Redirect: ☑ Enable

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **External Portal Server**.

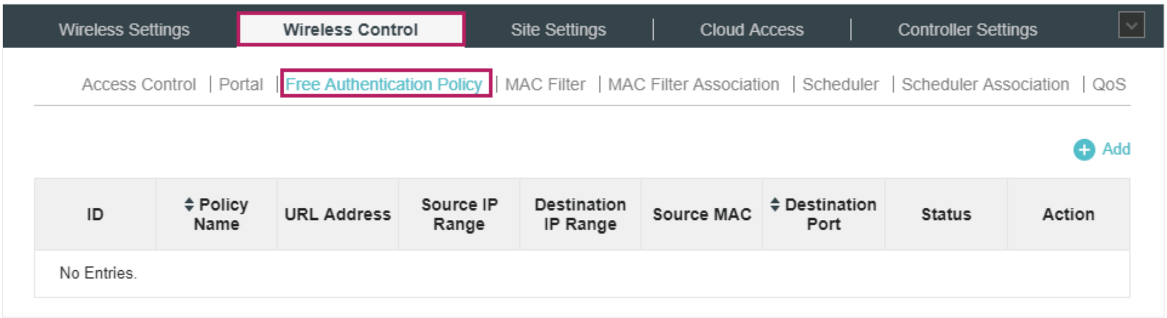
External Portal Server	Enter the complete authentication URL that redirect to an external portal server, for example: http://192.168.0.147:8880/portal/index.php or http://192.168.0.147/portal/index.html
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.

3. Click **Apply**.

3.4 Free Authentication Policy

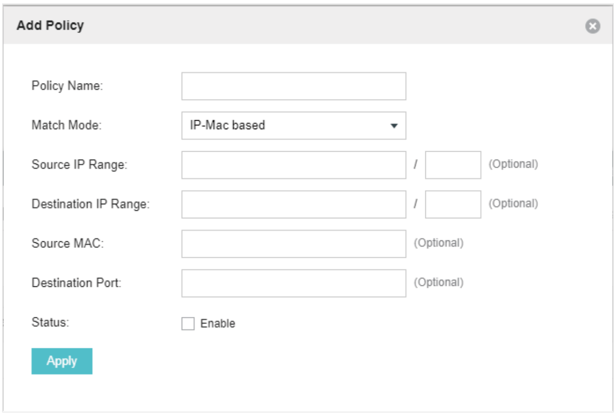
Free Authentication Policy allows some specified clients to access the network resources without authentication. Follow the steps below to add free authentication policy.

1. Go to **Wireless Control > Free Authentication Policy**.



ID	Policy Name	URL Address	Source IP Range	Destination IP Range	Source MAC	Destination Port	Status	Action
No Entries.								

2. Click ⊕ Add and the following window will pop up.



Policy Name:	
Match Mode:	IP-Mac based
Source IP Range:	/ (Optional)
Destination IP Range:	/ (Optional)
Source MAC:	(Optional)
Destination Port:	(Optional)
Status:	□ Enable

3. Configure the following parameters. When all conditions are met, the client can access the network without authentication.

Policy Name	Specify a name for the policy.
Match Mode	Select the match mode for the policy. Two options are provided: **URL**: With this option selected, configure an URL that is allowed to be visited by the clients without authentication. **IP-MAC Based**: With this option selected, configure Source IP Range, Destination IP Range, Source MAC and Destination MAC to specify the specific clients and service that will follow the Free Authentication feature.
URL	Set the URL.
Source IP Range	Set the Source IP Range with the subnet and mask length of the clients.
Destination IP Range	Set the Destination IP Range with the subnet and mask length of the server.
Source MAC	Set the MAC address of client.
Destination Port	Enter the port the service uses.
Status	Check the box to enable the policy.

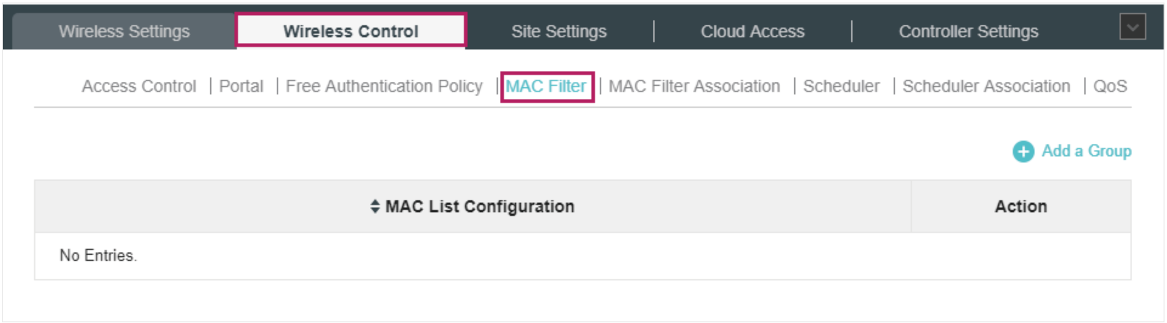
4. Click **Apply** and the policy is successfully added.

3.5 MAC Filter

MAC filter can be used to allow or block the listed clients to access the network. Thereby it can effectively control client's access to the wireless network.

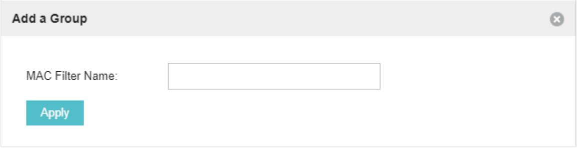
Follow the steps below to configure MAC Filter.

1. Go to **Wireless Control > MAC Filter** to add MAC Filter group and group members.



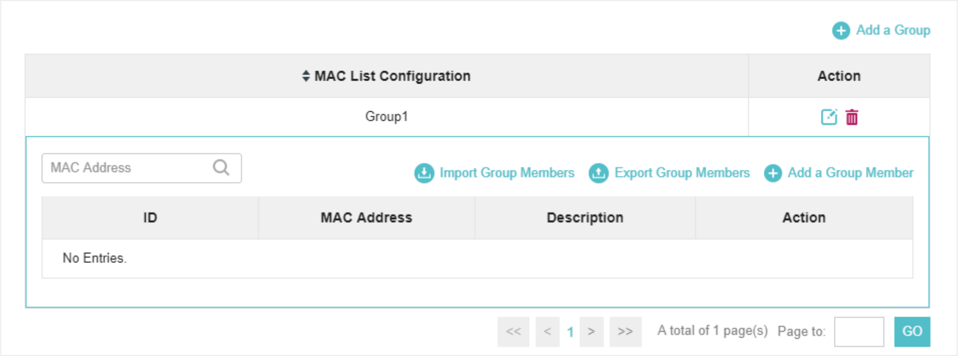
MAC List Configuration	Action
No Entries.	

1) Click ⊕ Add a Group and specify a name for the group.



MAC Filter Name:

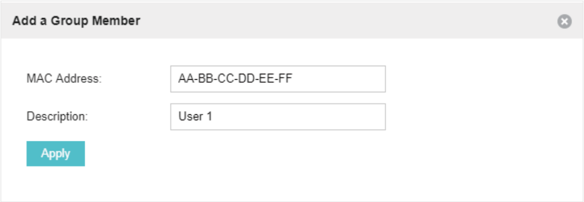
2) Click **Apply** and the group will be successfully added as shown below.



⇕ MAC List Configuration	Action
Group1	✎ 🗑

ID	MAC Address	Description	Action
No Entries.			

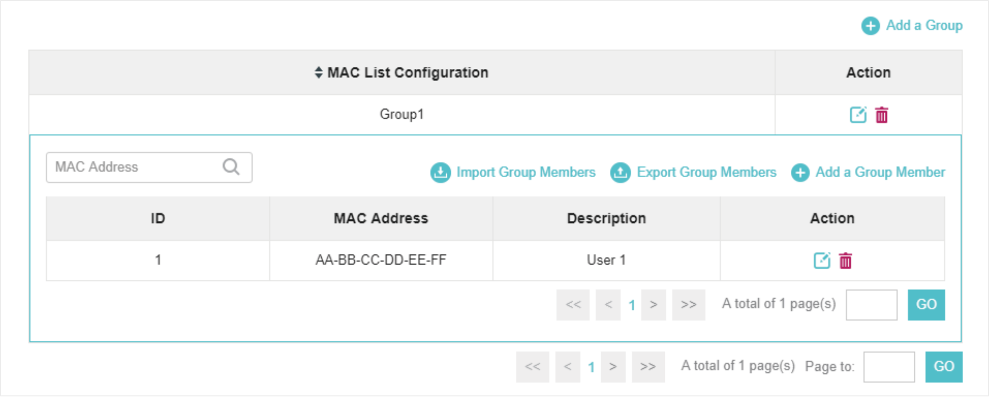
3) Click ⊕ Add a Group Member and enter a MAC address in the format as shown below.



MAC Address: AA-BB-CC-DD-EE-FF

Description: User 1

4) Click **Apply** to add the MAC address into the MAC filter group.



⇕ MAC List Configuration	Action
Group1	✎ 🗑

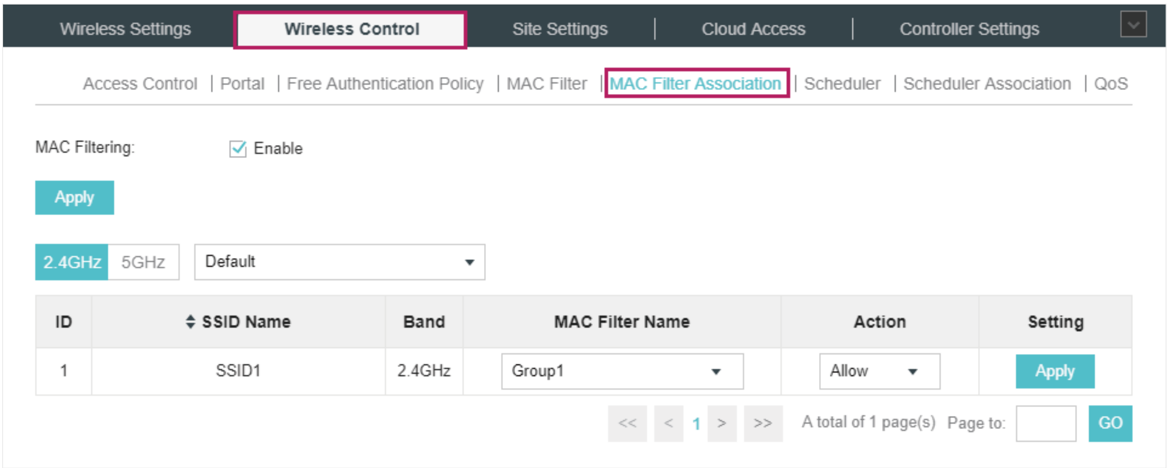
ID	MAC Address	Description	Action
1	AA-BB-CC-DD-EE-FF	User 1	✎ 🗑

2. You can add more groups or members according to your need.

Note:

You can click ⊕ Import Group Members to export the group members to a excel file and save the file on your PC. If needed, you can also click ⊕ Export Group Members to import the group members to the OC200.

3. Go to **Wireless Control > MAC Filter Association** to associate the added MAC Filter group with SSID.


Wireless Settings
Wireless Control
Site Settings
Cloud Access
Controller Settings
Access Control | Portal | Free Authentication Policy | MAC Filter | MAC Filter Association | Scheduler | Scheduler Association | QoS
Apply
2.4GHz
5GHz
<< < 1 > >>
GO

MAC Filtering: ☑ Enable

Default

ID	SSID Name	Band	MAC Filter Name	Action	Setting
1	SSID1	2.4GHz	Group1	Allow	Apply

A total of 1 page(s) Page to:

1) Check the box and click **Apply** to enable MAC Filtering function.

2) Select a band frequency (2.4GHz or 5GHz) and a WLAN group.

3) In the MAC Filter Name column of the specified SSID, select a MAC Filter group in the drop-down list. Then select **Allow/Deny** in the Action column to allow/deny the clients in the MAC Filter group to access the network.

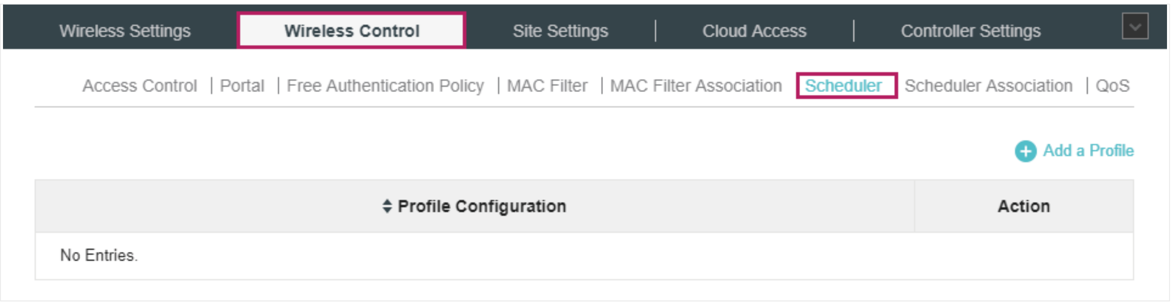
4) Click **Apply** in the Setting column.

3.6 Scheduler

With the Scheduler, the EAPs or its' wireless network can automatically turn on or off at the time you set. For example, you can use this feature to schedule the radio to operate only during the office working time in order to achieve security goals and reduce power consumption. You can also use the Scheduler to make clients can only access the wireless network during the time period you set in the day.

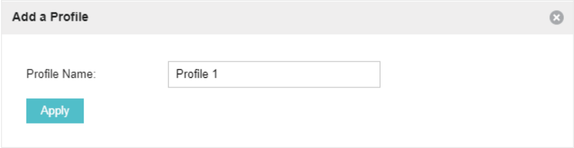
Follow the steps below to configure Scheduler.

1. Go to **Wireless Control > Scheduler**.


Wireless Settings
Wireless Control
Site Settings
Cloud Access
Controller Settings
Access Control | Portal | Free Authentication Policy | MAC Filter | MAC Filter Association | Scheduler | Scheduler Association | QoS
Add a Profile

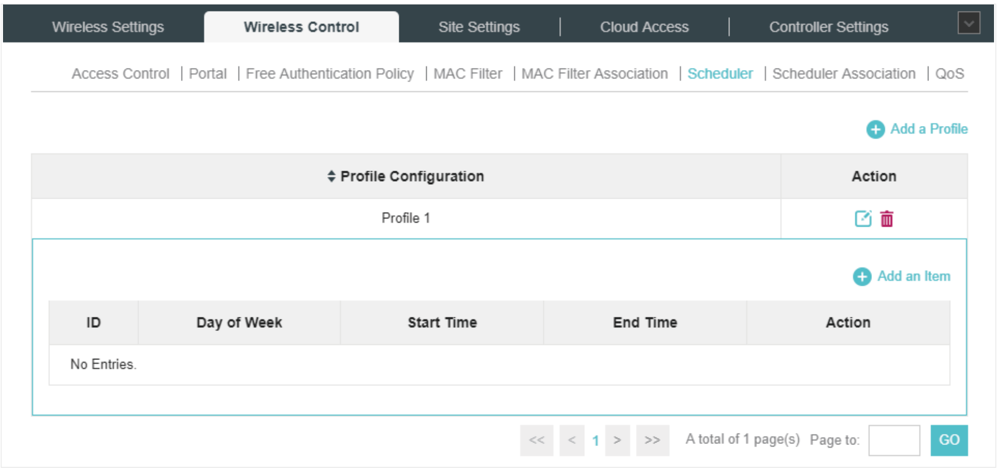
Profile Configuration	Action
No Entries.	

1) Click ⊕ Add a Profile and specify a name for the profile.



Profile Name: Profile 1

2) Click **Apply** and the profile will be added.

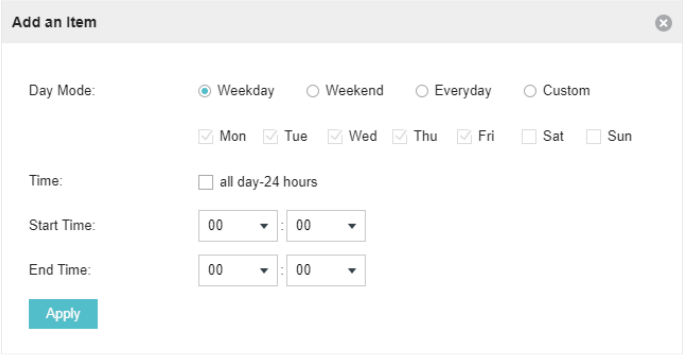


Profile Configuration	Action
Profile 1	

ID	Day of Week	Start Time	End Time	Action
No Entries.				

A total of 1 page(s) Page to:

3) Click ⊕ Add an Item and configure the parameters to specify a period of time.



Day Mode: ● Weekday ○ Weekend ○ Everyday ○ Custom

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

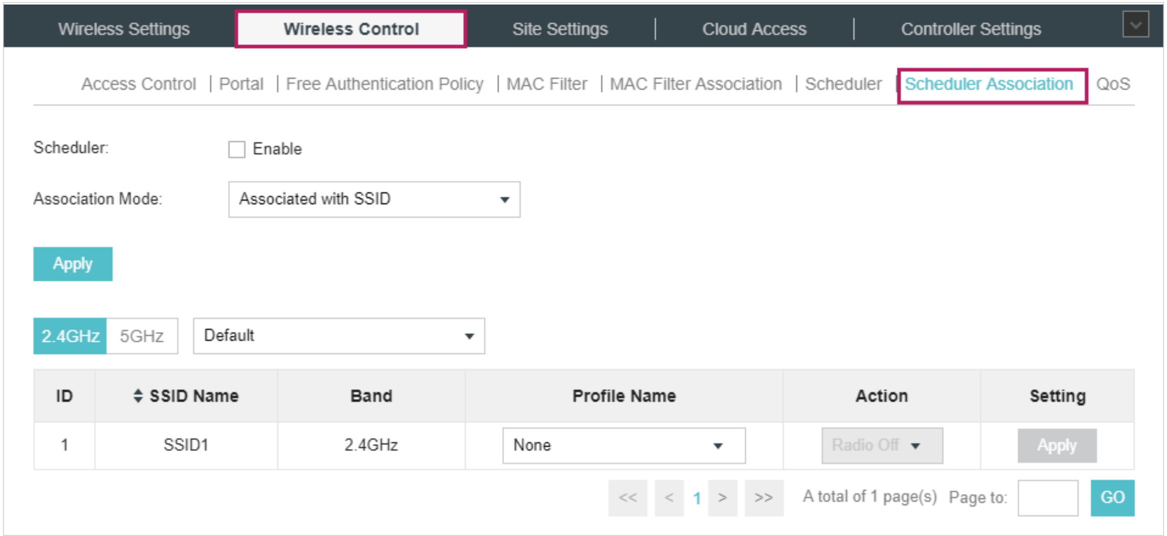
Time: □ all day-24 hours

Start Time: 00 : 00

End Time: 00 : 00

4) Click **Apply** and the profile is successfully added in the list.

2. Go to **Wireless Control > Scheduler Association.**



Scheduler: □ Enable

Association Mode: Associated with SSID

Default

ID	SSID Name	Band	Profile Name	Action	Setting
1	SSID1	2.4GHz	None	Radio Off	Apply

A total of 1 page(s) Page to:

1) Check the box to enable Scheduler function.

2) Select **Associated with SSID** (the profile will be applied to the specific SSID on all the EAPs) or **Associated with AP** (the profile will be applied to all SSIDs on the specific EAP). Then click **Apply**.

3) Select a band frequency (2.GHz or 5GHz) and a WLAN group.

4) In the Profile Name column of the specified SSID or AP, select a profile you added before in the drop-down list. Select **Radio Off/Radio On** to turn on or off the wireless network during the time interval set for the profile.

5) Click **Apply** in the Setting column.

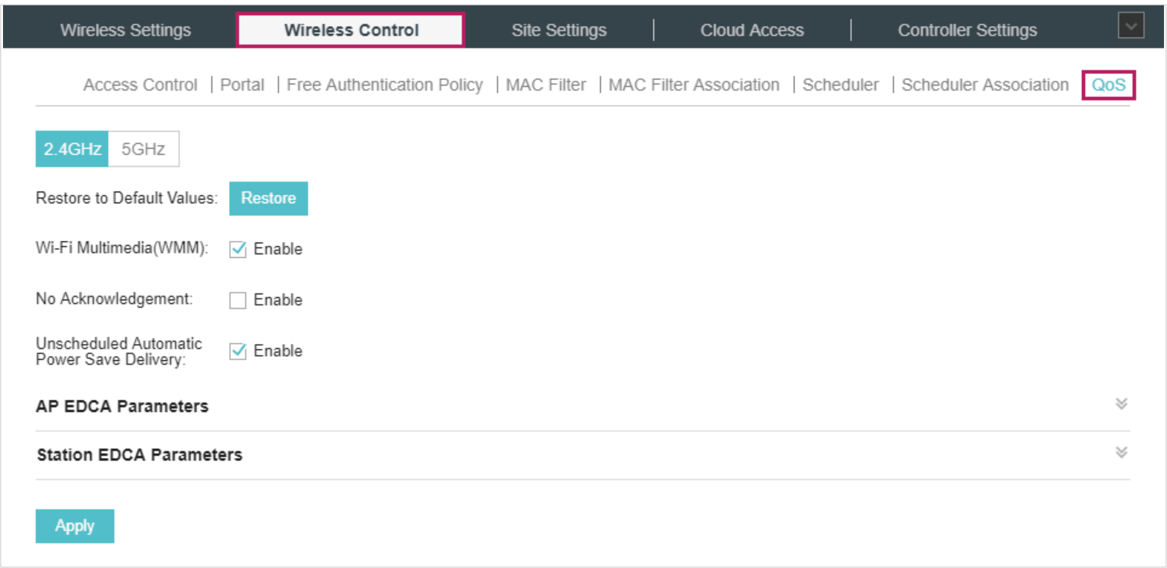
3.7 QoS

The OC200 allows you to configure the quality of service (QoS) on the EAP device for optimal throughput and performance when handling differentiated wireless traffic, such as Voice-over-IP (VoIP), other types of audio, video, streaming media, and traditional IP data.

To configure QoS on the EAP device, you should set parameters on the transmission queues for different types of wireless traffic and specify minimum and maximum wait times (through contention windows) for transmission. In normal use, we recommend you keep the default values for the EAP devices and station EDCA (Enhanced Distributed Channel Access).

Follow the steps below to configure QoS.

1. Go to **Wireless Control > QoS**.



Restore to Default Values: Restore

Wi-Fi Multimedia(WMM): ☑ Enable

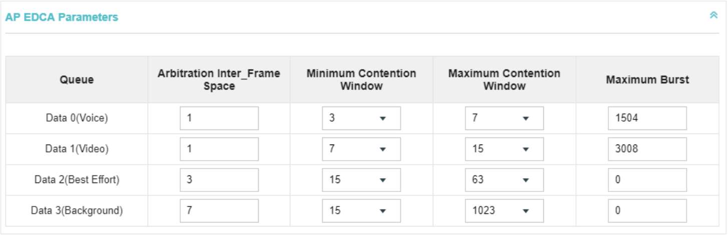
No Acknowledgement: □ Enable

Unscheduled Automatic Power Save Delivery: ☑ Enable

2. Enable or disable the following features.

Wi-Fi Multimedia (WMM)	By default enabled. With WMM enabled, the EAP devices have the QoS function to guarantee the high priority of the transmission of audio and video packets. If 802.11n only mode is selected in 2.4GHz (or 802.11n only, 802.11ac only, or 802.11 n/ac mixed mode in 5GHz), the WMM should be enabled. If WMM is disabled, the 802.11n only mode cannot be selected in 2.4GHz (or 802.11n only, 802.11ac only, or 802.11 n/ac mixed mode in 5GHz).
No Acknowledgment	By default disabled. You can enable this function to specify that the EAP devices should not acknowledge frames with Qos No Ack. Acknowledgeable is recommended if VoIP phones access the network through the EAP device.
Unscheduled Automatic Power Save Delivery	By default enabled. As a power management method, it can greatly improve the energy-saving capacity of clients.

3. Click **AP EDCA Parameters** and the following page will appear. AP EDCA parameters affect traffic flowing from the EAP device to the client station. We recommend you use the defaults.



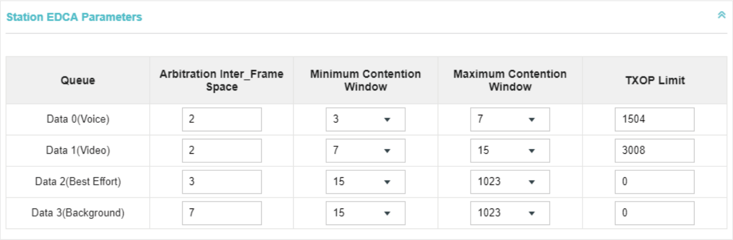
AP EDCA Parameters

Queue	Arbitration Inter_Frame Space	Minimum Contention Window	Maximum Contention Window	Maximum Burst
Data 0(Voice)	1	3	7	1504
Data 1(Video)	1	7	15	3008
Data 2(Best Effort)	3	15	63	0
Data 3(Background)	7	15	1023	0

Queue	**Queue** displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters. **Data 0 (Voice)**—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. **Data 1 (Video)**—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. **Data 2 (Best Effort)**—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. **Data 3 (Background)**—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
Arbitration Inter-Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values for **Arbitration Inter-Frame Space** are from 0 to 15.
Minimum Contention Window	A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. This value can not be higher than the value for the **Maximum Contention Window**.

Maximum Contention Window	The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. This value must be higher than the value for the **Minimum Contention Window**.
Maximum Burst	**Maximum Burst** specifies the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.

4. Click **Station EDCA Parameters** and the following page will appear. Station EDCA parameters affect traffic flowing from the client station to the EAP device. We recommend you use the defaults.



Station EDCA Parameters

Queue	Arbitration Inter_Frame Space	Minimum Contention Window	Maximum Contention Window	TXOP Limit
Data 0(Voice)	2	3	7	1504
Data 1(Video)	2	7	15	3008
Data 2(Best Effort)	3	15	1023	0
Data 3(Background)	7	15	1023	0

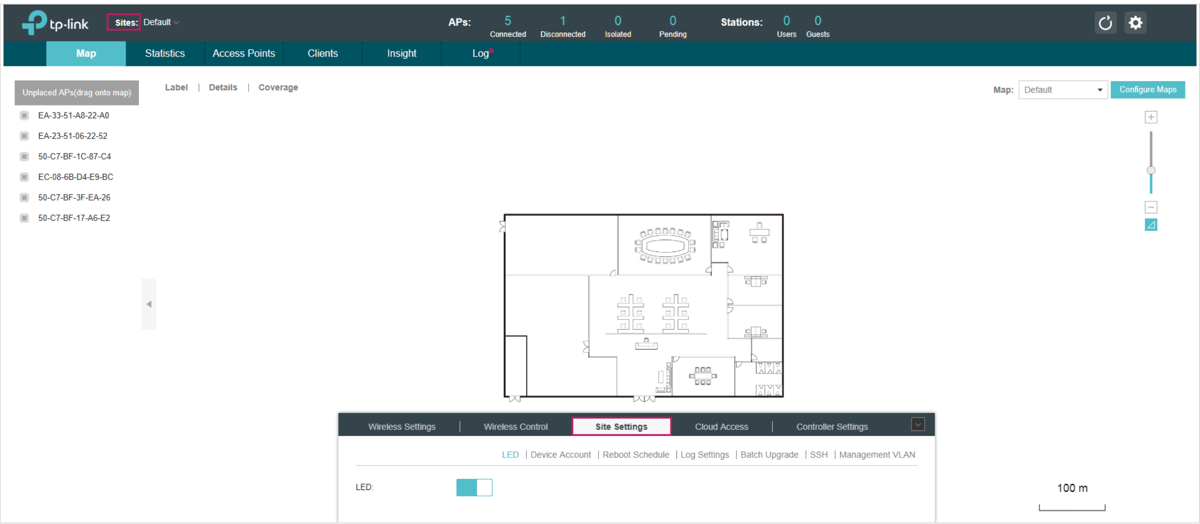
Queue	**Queue** displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters. **Data 0 (Voice)**—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. **Data 1 (Video)**—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. **Data 2 (Best Effort)**—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. **Data 3 (Background)**—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
Arbitration Inter-Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values for **Arbitration Inter-Frame Space** are from 0 to 15.
Minimum Contention Window	A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. This value can not be higher than the value for the **Maximum Contention Window**.
Maximum Contention Window	The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. This value must be higher than the value for the **Minimum Contention Window**.

TXOP Limit	The **TXOP Limit** is a station EDCA parameter and only applies to traffic flowing from the client station to the EAP device. The Transmission Opportunity (TXOP) is an interval of time, in milliseconds, when a WME client station has the right to initiate transmissions onto the wireless medium (WM) towards the EAP device. The valid values are multiples of 32 between 0 and 8192.

5. Click **Apply**.

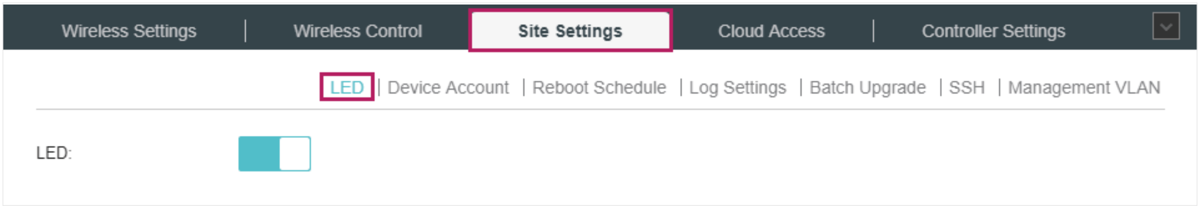
3.8 Site Settings

You can configure the site-specific settings on the **Site Settings** page. To switch sites, select a different site from the **Sites** drop-down menu at the top of any screen.



3.8.1 LED

You can change the LED light status on the EAP devices on the page **Site Settings > LED**.



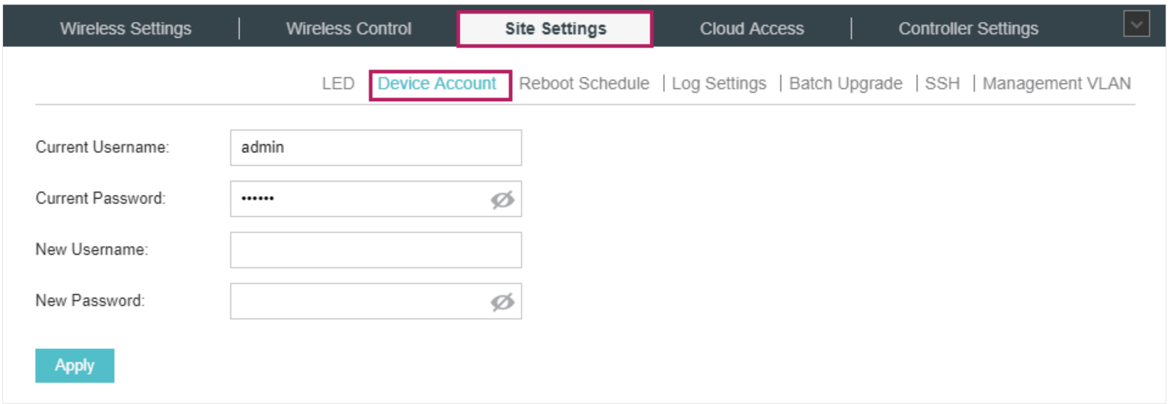
By default, the LED status is ■□, which means that the LED lights of all the EAP devices on the site are on. You can click this button to change the LED light status. The icon will be changed to □■, which means that all the LED lights are off.

3.8.2 Device Account

When the EAP devices are adopted at the first time, their username and password will become the same as those of the OC200 which are specified at Basic Configurations. You can specify a new username and password for the adopted EAPs in batches.

Follow the steps below to change EAP devices' username and password.

1. Go to **Site Settings > Device Account.**



Current Username: admin

Current Password: ••••••

New Username:

New Password:

2. Specify a new username and password for the EAP devices.

3. Click **Apply**.

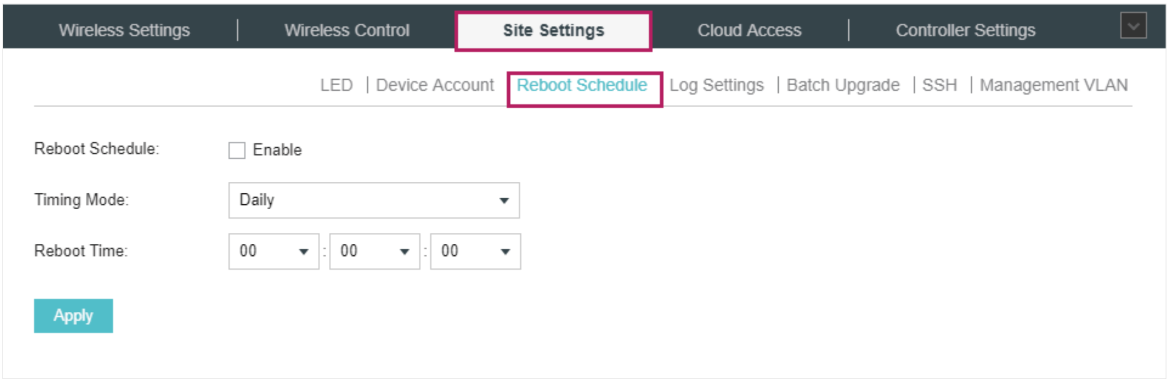
Note:

The new account will be applied to EAP devices but not the OC200. To change the OC200's username and password, please refer to User Account.

3.8.3 Reboot Schedule

You can reboot all the EAPs in the network periodically as needed. Follow the steps below to configure Reboot Schedule.

1. Go to **Site Settings > Reboot Schedule.**



Reboot Schedule: □ Enable

Timing Mode: Daily

Reboot Time: 00 : 00 : 00

2. Check the box to enable the function.

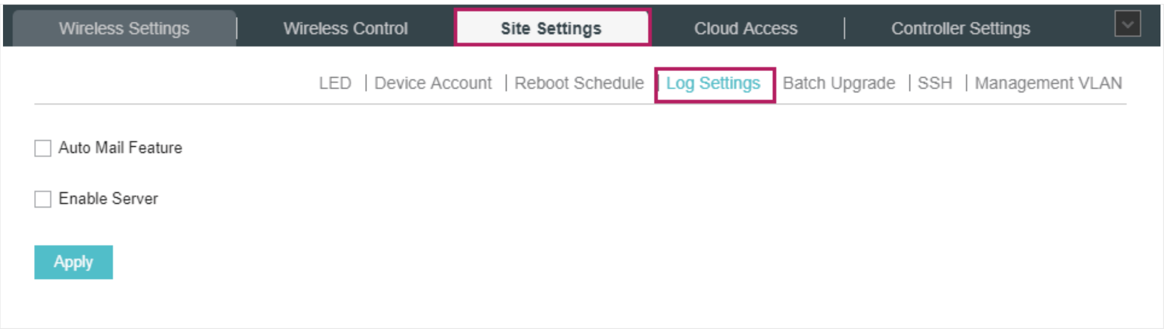
3. Choose **Daily**, **Weekly** or **Monthly** in the **Timing Mode** drop-down list and set a specific time to reboot the EAPs.

4. Click **Apply**.

3.8.4 Log Settings

Follow the steps below to choose the way to receive system logs.

1. Go to **Site Settings > Log Setting.**



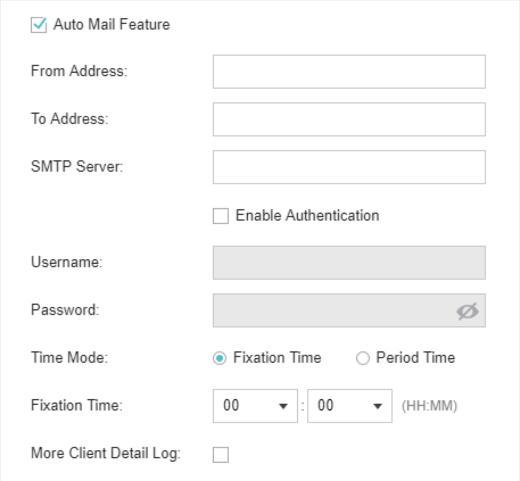
□ Auto Mail Feature

□ Enable Server

2. Check the box to choose the way to receive system logs (you can choose more than one) and click **Apply**. Two ways are available: **Auto Mail Feature** and **Server**.

Auto Mail Feature

If Auto Mail Feature is enabled, system logs will be sent to a specified mailbox. Check the box to enable the feature and configure the parameters.



☑ Auto Mail Feature

From Address:

To Address:

SMTP Server:

□ Enable Authentication

Username:

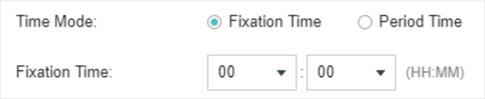
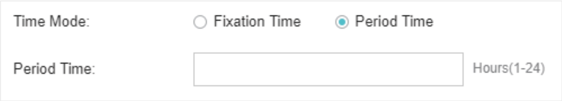
Password:

Time Mode: ● Fixation Time ○ Period Time

Fixation Time: 00 : 00 (HH:MM)

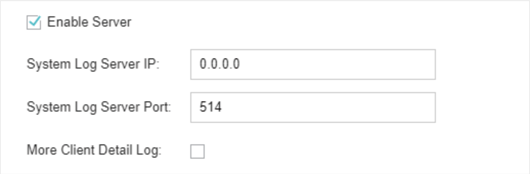
More Client Detail Log: □

From Address	Enter the sender's E-mail address.
To Address	Enter the receiver's E-mail address.
SMTP Server	Enter the IP address of the SMTP server.

Enable Authentication	You can check the box to enable mail server authentication. Enter the sender's mail account name and password.
Time Mode	Select Time Mode. System logs can be sent at specific time or time interval.
Fixation Time	If you select Fixation Time, specify a fixed time to send the system log mails. For example, 08:30 indicates that the mail will be sent at 8:30 am everyday.  Time Mode: ● Fixation Time ○ Period Time Fixation Time: 00 : 00 (HH:MM)
Period Time	If you select Period Time, specify a period time to regularly send the system log mail. For example, 6 indicates that the mail will be sent every six hours.  Time Mode: ○ Fixation Time ● Period Time Period Time: Hours(1-24)
More Client Detail Log	With the option enabled, the logs of clients will be sent to the receiver's E-mail address.

Server

If Server is enabled, system logs will be sent to a server. Check the box to enable the feature and configure the parameters.



☑ Enable Server

System Log Server IP: 0.0.0.0

System Log Server Port: 514

More Client Detail Log: □

System Log Server IP	Enter the IP address of the server.
System Log Server Port	Enter the port of the server.
More Client Detail Log	With the option enabled, the logs of clients will be sent to the server.

3.8.5 Batch Upgrade

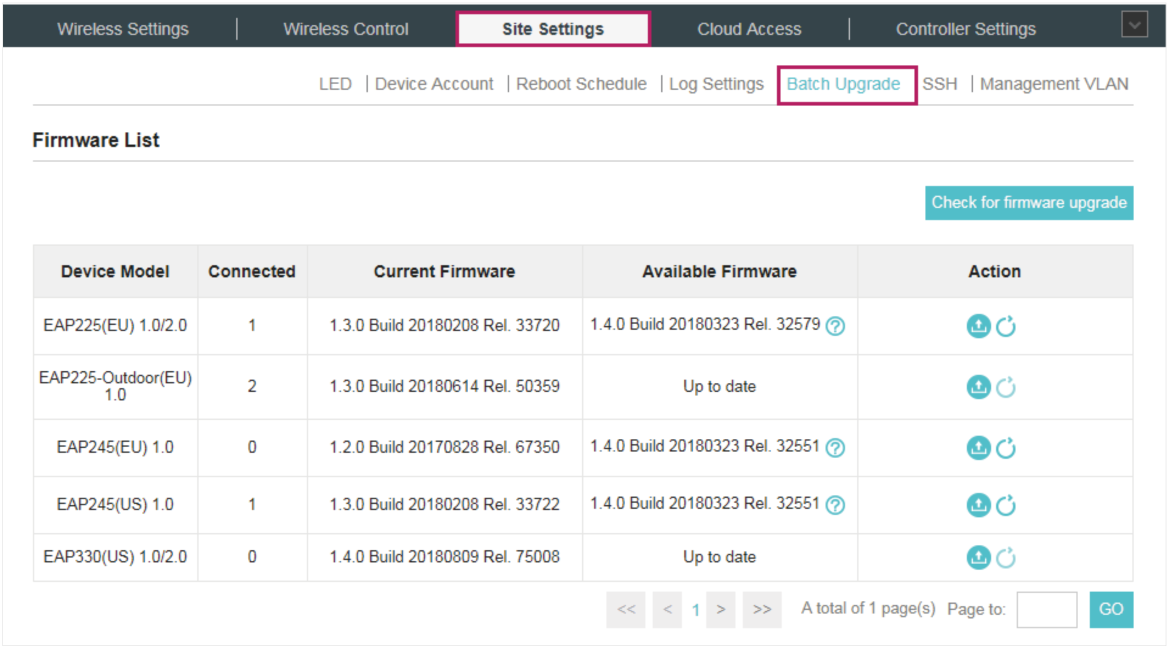
You can upgrade your EAP devices of the same model in batches using Batch Upgrade. Two options are available for upgrading: upgrade online and upgrade manually.

Upgrade Online

The latest firmware for the EAPs can be detected by the OC200 automatically, and you can upgrade the EAPs online. Thus you do not need to save the firmware files locally in advance.

Follow the steps below to upgrade the EAP devices online according to their model.

1. Go to **Site Settings > Batch Upgrade.** The device model, amount, current firmware and available firmware will appear on the **Firmware list.**



Firmware List

Device Model	Connected	Current Firmware	Available Firmware	Action
EAP225(EU) 1.0/2.0	1	1.3.0 Build 20180208 Rel. 33720	1.4.0 Build 20180323 Rel. 32579 ?	⬆ ↻
EAP225-Outdoor(EU) 1.0	2	1.3.0 Build 20180614 Rel. 50359	Up to date	⬆ ↻
EAP245(EU) 1.0	0	1.2.0 Build 20170828 Rel. 67350	1.4.0 Build 20180323 Rel. 32551 ?	⬆ ↻
EAP245(US) 1.0	1	1.3.0 Build 20180208 Rel. 33722	1.4.0 Build 20180323 Rel. 32551 ?	⬆ ↻
EAP330(US) 1.0/2.0	0	1.4.0 Build 20180809 Rel. 75008	Up to date	⬆ ↻

2. Click ↻ in the **Action** column to upgrade the device.

After upgrading, the device will reboot automatically.

Tips:

- You can click Check for firmware upgrade to check if the latest firmware is available.
- You can click ? in the **Available Firmware** column to view the release note of the firmware, which can help you know the new features or improvements of this firmware.

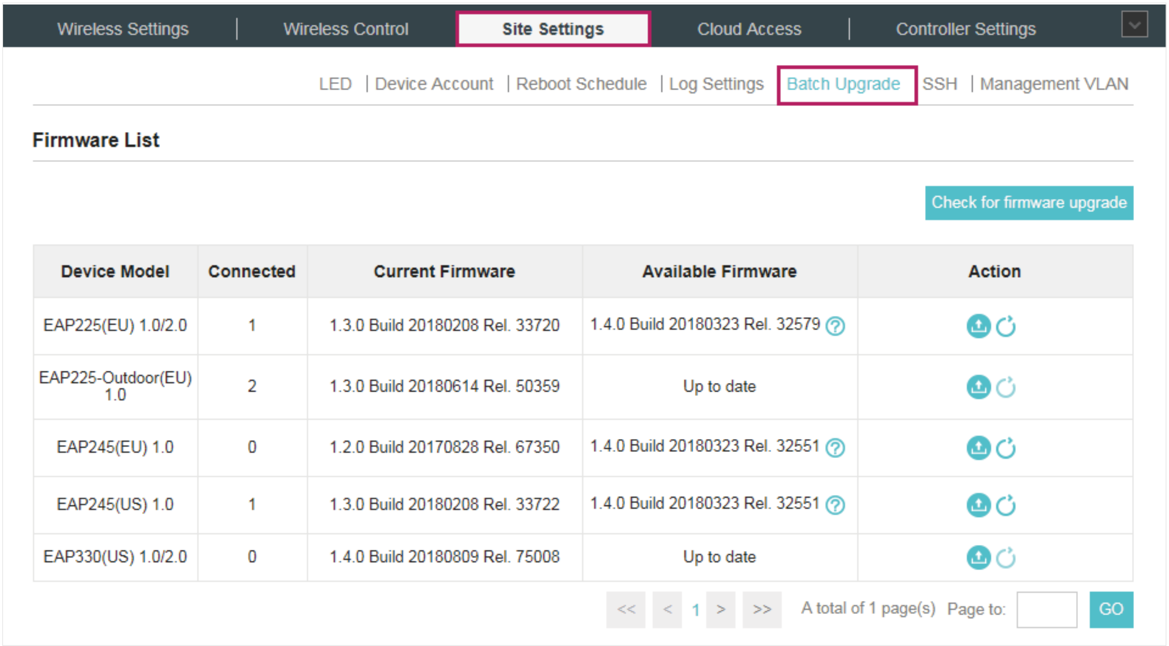
Upgrade Manually

The latest firmware files can be downloaded from the in the download center of TP-Link Website. Then you can upgrade the EAP devices manually.

Follow the steps below to upgrade the EAP devices maually according to their model.

1. Visit http://www.tp-link.com/en/support/download/ to download the latest firmware file of the corresponding model.

2. Go to **Site Settings > Batch Upgrade.**

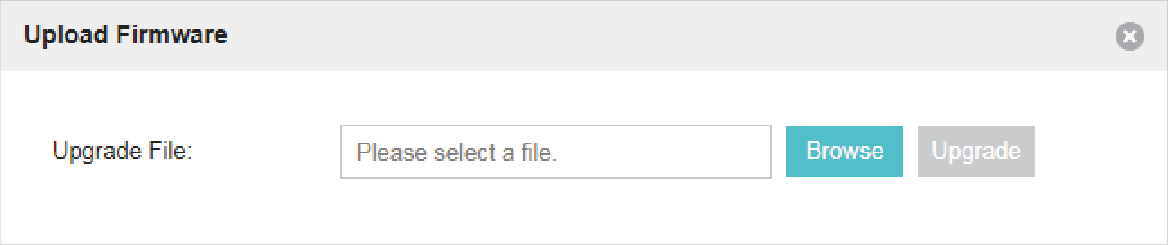


Firmware List

Device Model	Connected	Current Firmware	Available Firmware	Action
EAP225(EU) 1.0/2.0	1	1.3.0 Build 20180208 Rel. 33720	1.4.0 Build 20180323 Rel. 32579 ?	⬆ ↻
EAP225-Outdoor(EU) 1.0	2	1.3.0 Build 20180614 Rel. 50359	Up to date	⬆ ↻
EAP245(EU) 1.0	0	1.2.0 Build 20170828 Rel. 67350	1.4.0 Build 20180323 Rel. 32551 ?	⬆ ↻
EAP245(US) 1.0	1	1.3.0 Build 20180208 Rel. 33722	1.4.0 Build 20180323 Rel. 32551 ?	⬆ ↻
EAP330(US) 1.0/2.0	0	1.4.0 Build 20180809 Rel. 75008	Up to date	⬆ ↻

A total of 1 page(s) Page to:

3. Click ⬆ in the **Action** column to upgrade the device.



Upload Firmware

Upgrade File: Please select a file.

4. Click **Browse** to locate and choose the proper firmware file for the model.

5. Click **Upgrade** to upgrade the device.

After upgrading, the device will reboot automatically.

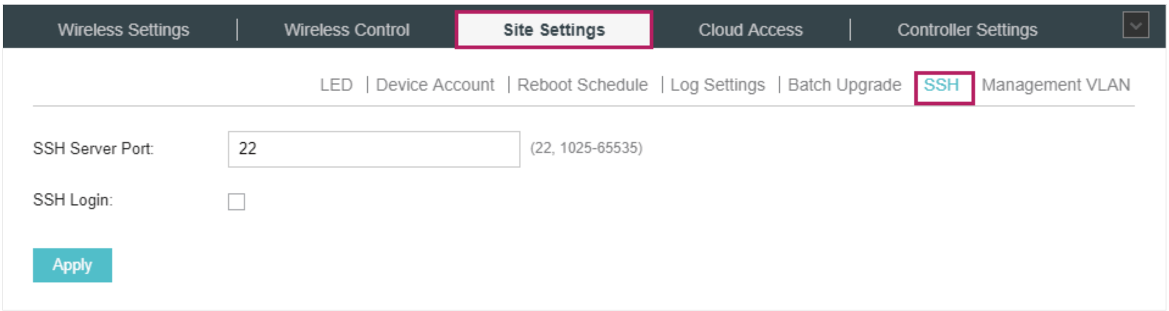
Note:

- The EAP device cannot be upgraded manually when you access the OC200 via Omada Cloud.
- To avoid damage, please do not turn off the device while upgrading.

3.8.6 SSH

SSH is a protocol working in application layer and transport layer. It can provide a secure, remote connection to a device. You can log in to the OC200 via SSH. Follow the steps below to configure SSH on the OC200:

1. Go to **Site Setting > SSH.** Enter the port number of the SSH server.



SSH Server Port: 22 (22, 1025-65535)

SSH Login: □

2. Check the box to enable SSH Login.

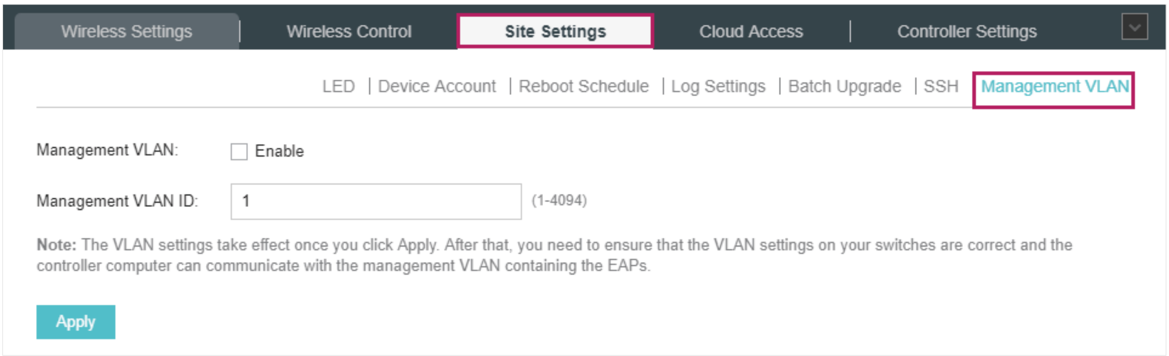
3. Click **Apply**.

3.8.7 Management VLAN

Management VLAN provides a safer way for you to manage the EAP. With Management VLAN enabled, only the hosts in the management VLAN can manage the EAP. Since most hosts cannot process VLAN TAGs, connect the management host to the network via a switch, and set up correct VLAN settings for the switches on the network to ensure the communication between the host and the EAP in the management VLAN.

Follow the steps below to configure Management VLAN.

1. Go to **Site Setting > Management VLAN**. Check the box to enable Management VLAN.



Management VLAN: □ Enable

Management VLAN ID: 1 (1-4094)

Note: The VLAN settings take effect once you click Apply. After that, you need to ensure that the VLAN settings on your switches are correct and the controller computer can communicate with the management VLAN containing the EAPs.

2. Specify the Management VLAN ID. The default VLAN ID is 1.

3. Click **Apply**.

4 Omada Cloud Service

TP-Link Omada Cloud Service provides a better way to realize remote management. With Cloud Access enabled on the OC200 and a TP-Link ID bound with your OC200, you can easily monitor and manage your wireless network. To ensure that your EAPs stay new and get better over time, the Omada Cloud will notify you when a newer firmware upgrade is available. Surely you can also manage multiple OC200s with a single TP-Link ID.

Follow the steps below to configure Cloud Access and access the OC200 via Omada Cloud:

1. Configure the Cloud Access

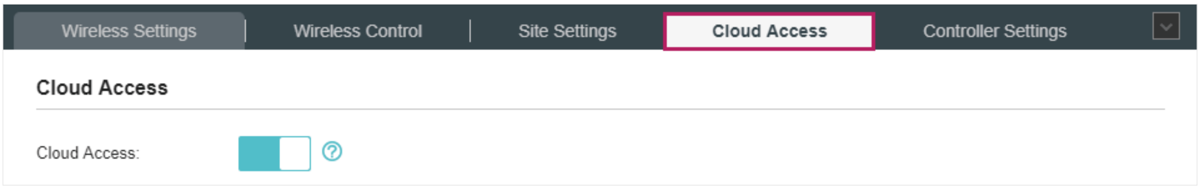
2. Manage the OC200 via Omada Cloud

4.1 Configure the Cloud Access

4.1.1 Enable Cloud Access

You can configure the OC200 via Omada Cloud only when Cloud Access is enabled on the OC200 and you have been added as a Cloud User.

On the page **Cloud Access** you can configure Cloud Access. Click the button to enable the **Cloud Access.** The Cloud Access status is , which means that the Cloud Access is enabled.



Cloud Access

Cloud Access:

4.1.2 Manage the Cloud Users

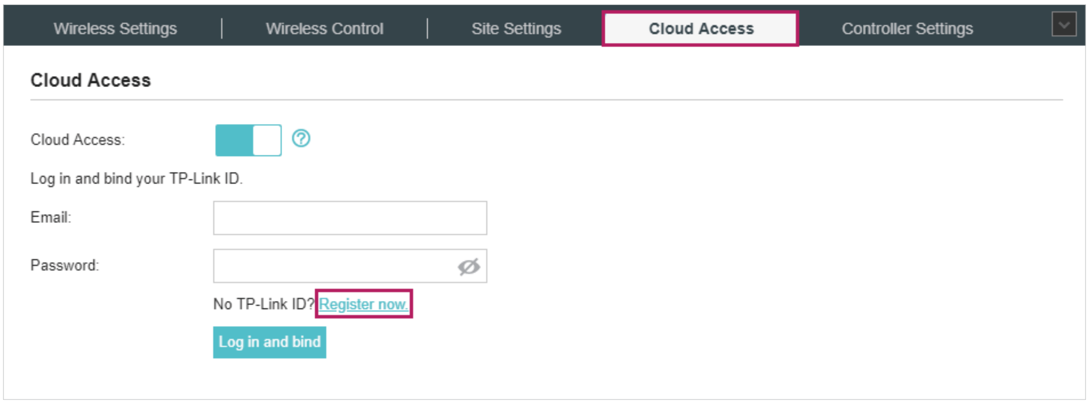
To configure and manage OC200 through Cloud service, you need to have a TP-Link ID, and bind your TP-Link ID to the OC200. Then you can remotely access the OC200 as a Cloud User.

Note:

To register a TP-Link ID and bind it to your OC200, make sure that the management host can access the internet.

Register a TP-Link ID

In the Quick Setup process, you can register a TP-Link ID and bind it to your OC200. If you have skipped the registration during the Quick Setup process, you can go to **Cloud Access**. Click **Register Now** and follow the instructions to register a TP-Link ID.



Cloud Access

Cloud Access:

Log in and bind your TP-Link ID.

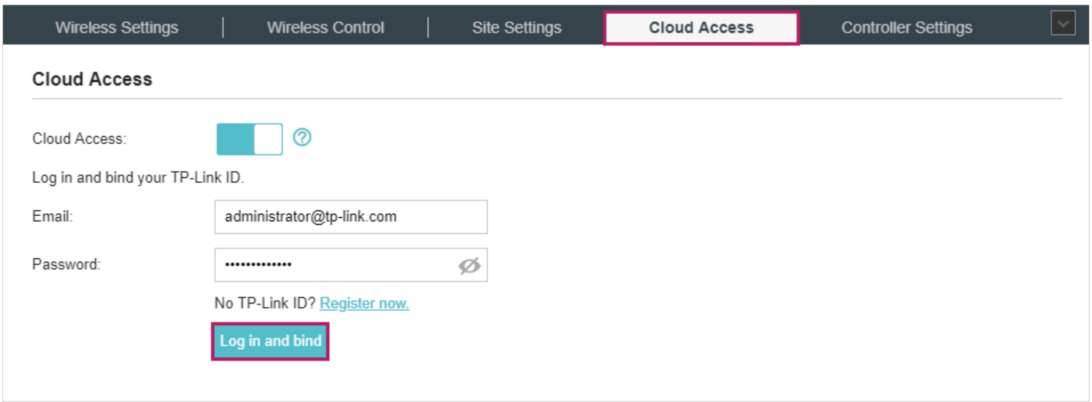
Email:

Password:

No TP-Link ID? Register now

Log in and bind your TP-Link ID

After activating your TP-Link ID, come back to **Cloud Access** page to log in and bind your TP-Link ID to your OC200.



Cloud Access

Cloud Access:

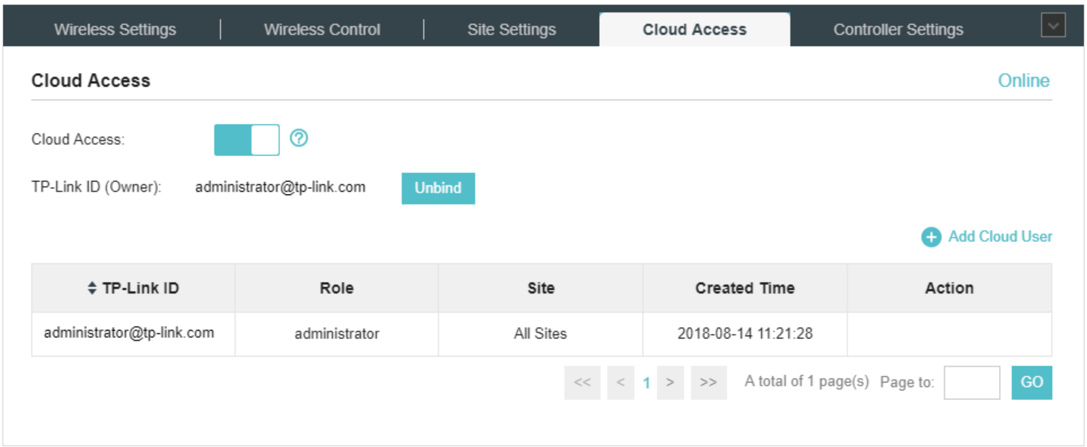
Log in and bind your TP-Link ID.

Email: administrator@tp-link.com

Password: •••••••••••••

No TP-Link ID? Register now.

The TP-Link ID which is bound with the OC200 for the first time will be automatically bound as an administrator. And only one TP-Link ID can be bound with the OC200 as an administrator. An administrator account can add or remove other TP-Link IDs to or from the same OC200 as Cloud Users.



Cloud Access

Online

Cloud Access:

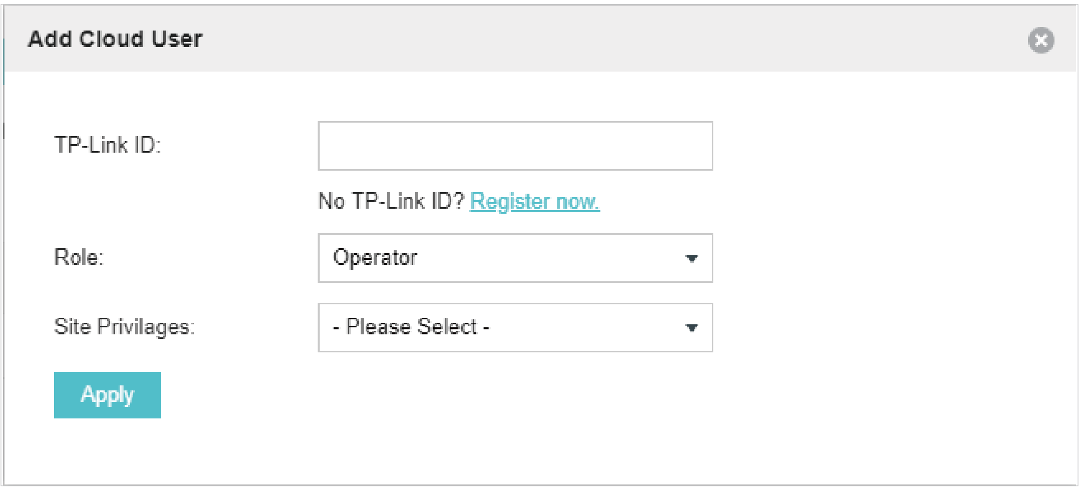
TP-Link ID (Owner): administrator@tp-link.com

TP-Link ID	Role	Site	Created Time	Action
administrator@tp-link.com	administrator	All Sites	2018-08-14 11:21:28	

A total of 1 page(s) Page to:

Add new Cloud Users

After you have an administrator TP-Link ID, you can add new Cloud Users. Click ⊕ Add Cloud User , enter another TP-Link ID as needed and click **Save.**



Add Cloud User

TP-Link ID:

No TP-Link ID? Register now.

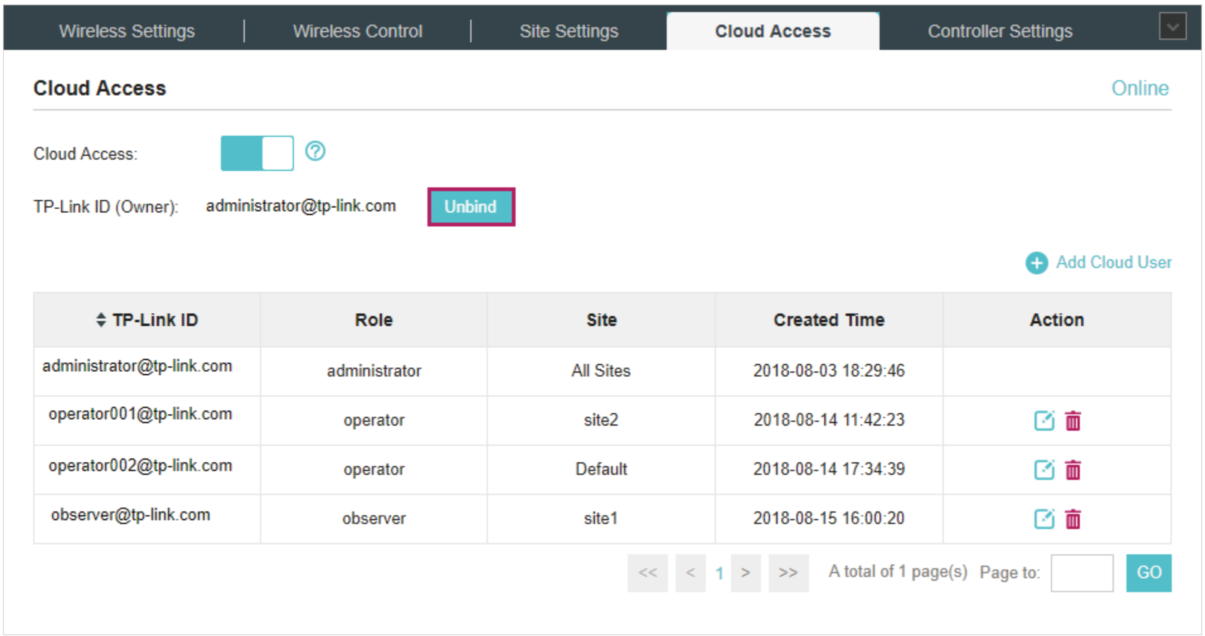
Role: Operator

Site Privilages: - Please Select -

TP-Link ID	Enter the TP-Link ID that you want to add as the new Cloud User. If you do not have another TP-Link ID, you can click **Register Now** and follow the instructions to register a TP-Link ID.
Role	Select the role for the new Cloud User from the drop-down list. Two options are provided: **Operator:** An Operator account can change the settings of the privileged sites that are given by the administrator. And the Operator account cannot manage the cloud users and change settings. **Observer**: An Observer account can only view the status and settings of the privileged sites that are given by the administrator but not change the settings. Both the Operator and Observer accounts cannot manage the cloud users and settings. Thus Operator and Observer accounts can only be created or deleted by the administrator.
Site Privileges	Select the privileged sites (multiple options available) for the Operator or Observer accounts from the drop-down list.

Unbind a TP-Link ID

You can click **Unbind** to unbind your administrator TP-Link ID. Note that Unbind operation cannot be performed when you log in to the OC200 through Omada Cloud service.



Cloud Access — Online

Cloud Access:

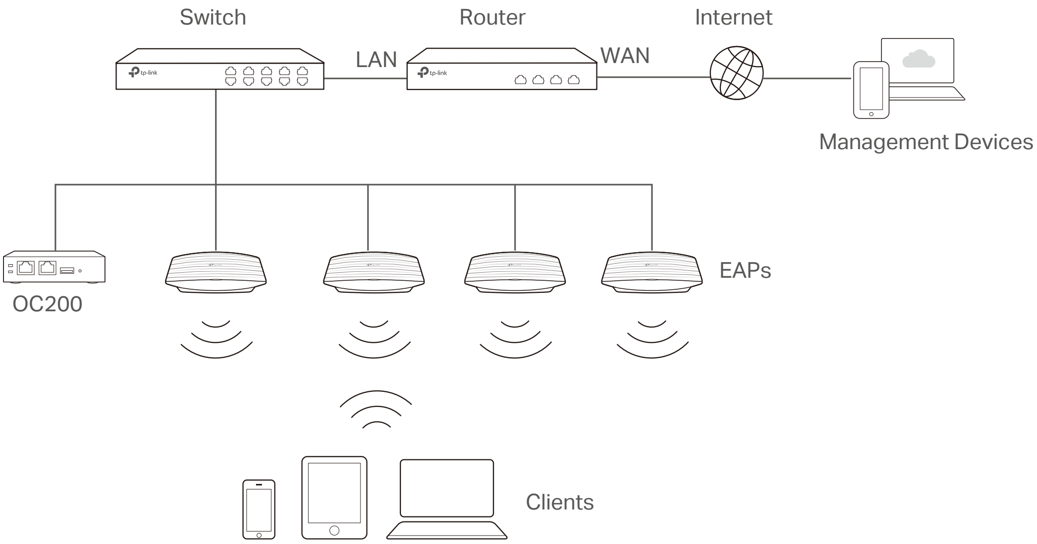
TP-Link ID (Owner): administrator@tp-link.com

TP-Link ID	Role	Site	Created Time	Action
administrator@tp-link.com	administrator	All Sites	2018-08-03 18:29:46	
operator001@tp-link.com	operator	site2	2018-08-14 11:42:23	
operator002@tp-link.com	operator	Default	2018-08-14 17:34:39	
observer@tp-link.com	observer	site1	2018-08-15 16:00:20	

<< < 1 > >> A total of 1 page(s) Page to:

4.2 Manage the OC200 via Omada Cloud

With Cloud Access enabled, you can manage your OC200 remotely using your TP-Link ID. You can refer to the following topology.



Before you remotely access your OC200, make sure that the following requirements have been met:

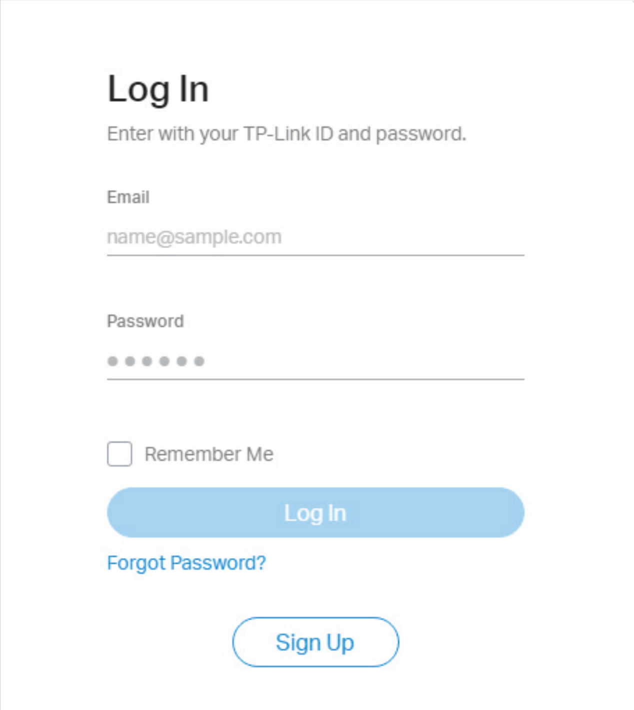
- Cloud Access is enabled on the OC200.
- Your OC200 has been bound with a TP-Link ID. If you don't have a TP-Link ID, refer to Register a TP-Link ID to get one.
- Both your OC200 and management devices have internet access.

4.2.1 Access the OC200 via Omada Cloud

1. Launch a web browser and type **https://omada.tplinkcloud.com** in the address bar, then press **Enter** (Windows) or **Return** (Mac).

https://omada.tplinkcloud.com

2. Enter your TP-Link ID and password and click **Log In**.



Log In

Enter with your TP-Link ID and password.

Email

name@sample.com

Password

●●●●●●

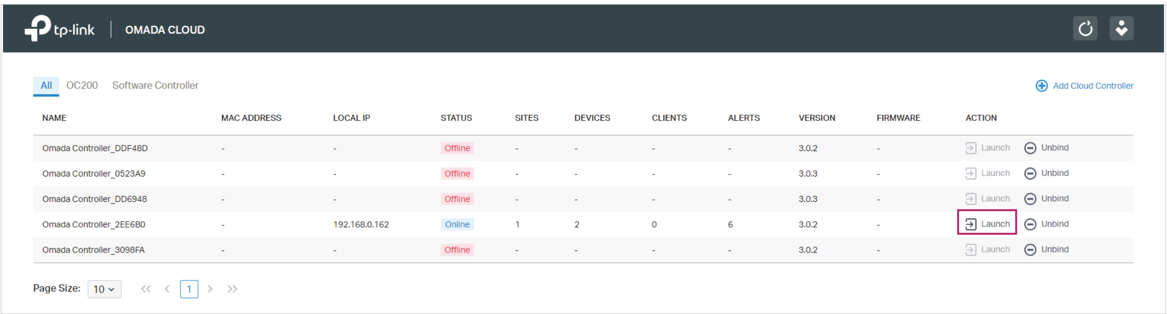
□ Remember Me

Log In

Forgot Password?

Sign Up

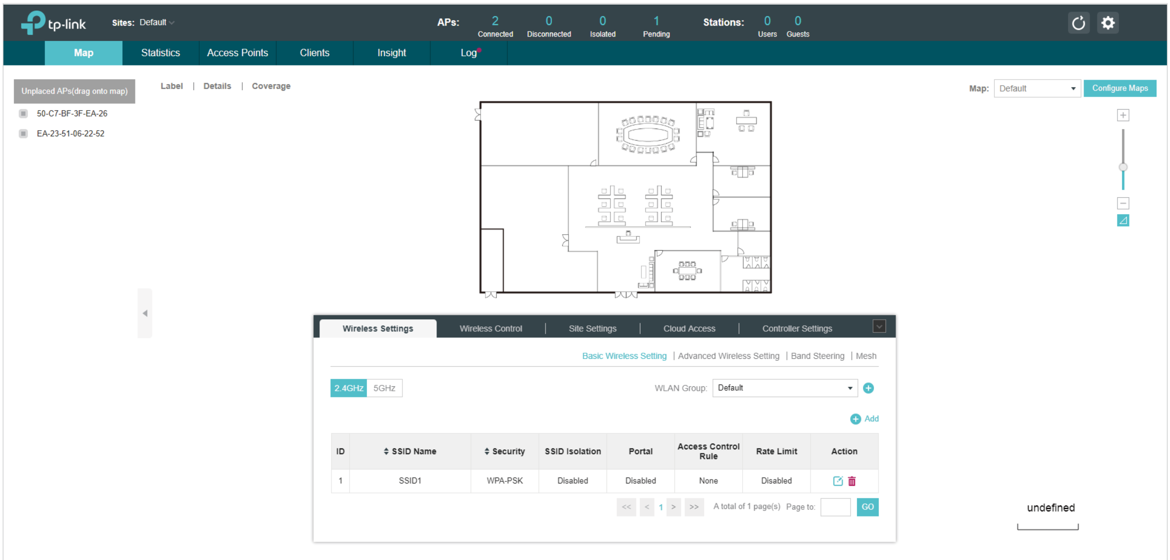
3. After you log in to Omada Cloud, a list of controllers that has been bound with your TP-Link ID will appear. If the OC200 does not appear on the list, you can click ↻ to refresh the current page.



NAME	MAC ADDRESS	LOCAL IP	STATUS	SITES	DEVICES	CLIENTS	ALERTS	VERSION	FIRMWARE	ACTION
Omada Controller_DDF48D	-	-	Offline	-	-	-	-	3.0.2	-	Launch Unbind
Omada Controller_0523A9	-	-	Offline	-	-	-	-	3.0.3	-	Launch Unbind
Omada Controller_DD6948	-	-	Offline	-	-	-	-	3.0.3	-	Launch Unbind
Omada Controller_2EE6B0	-	192.168.0.162	Online	1	2	0	6	3.0.2	-	Launch Unbind
Omada Controller_3098FA	-	-	Offline	-	-	-	-	3.0.2	-	Launch Unbind

Page Size: 10 1

Click **Launch** to access your OC200. Then you can configure and manage your OC200.



ID	SSID Name	Security	SSID Isolation	Portal	Access Control Rule	Rate Limit	Action
1	SSID1	WPA-PSK	Disabled	Disabled	None	Disabled	

<< < 1 > >> A total of 1 page(s) Page to: GO

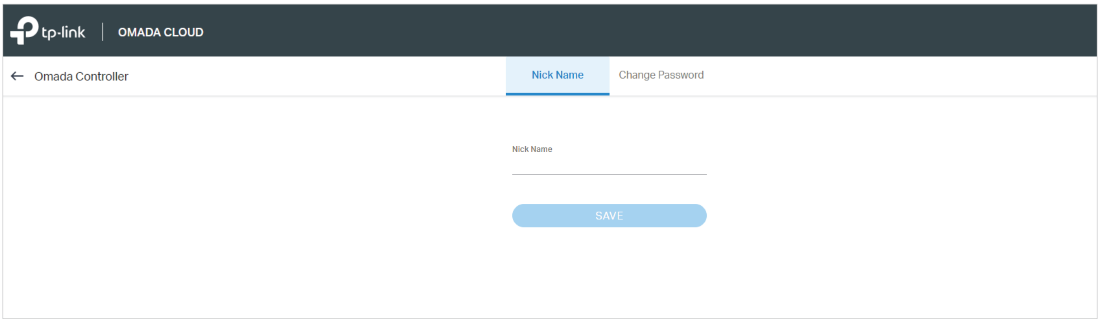
Note:

- To remove the OC200 from your cloud account, you can click ⊖ Unbind .
- To log out Omada Cloud, click and select **Log Out.**

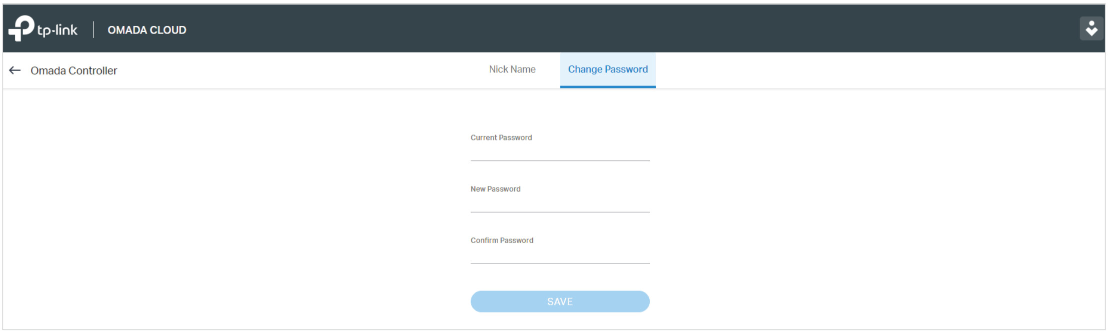
4.2.2 Change your TP-Link ID information

You can change your TP-Link ID information on the Omada Cloud page. Click and select **My TP-Link ID**, the cloud accounting settings will appear.

You can have a nickname for your TP-Link ID. Enter your nick name and click **Save**.



You can also change the password of your TP-Link ID. Enter the current password, then a new password twice and click **Save**.



5 Configure the EAPs Separately

In addition to global configuration, you can configure the EAPs separately and the configuration results will be applied to a specified EAP device.

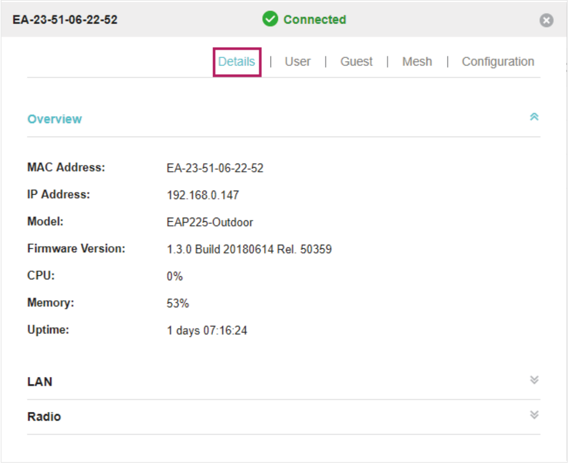
To configure a specified EAP, please click the EAP's name on the **Access Points** tab or click ⚙ of connected EAP on the map. Then you can view the EAP's detailed information and configure the EAP on the pop-up window.

This chapter includes the following contents:

5.1 View the Information of the EAP

5.1.1 Overview

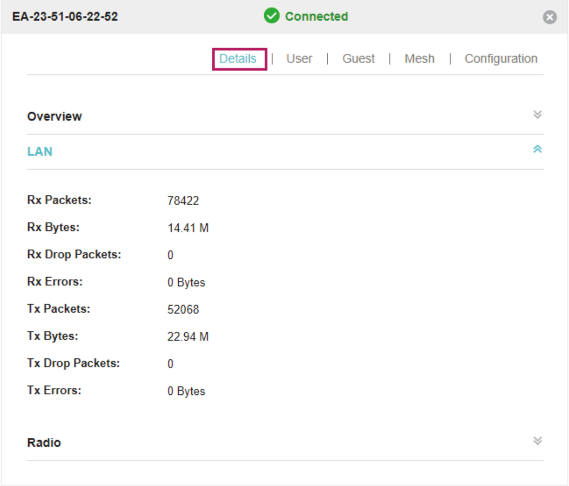
Click **Overview** to view the basic information including EAP's MAC address (or name you set), IP address, model, firmware version, the usage rate of CPU and Memory and uptime (indicates how long the EAP has been running without interruption).



MAC Address:	EA-23-51-06-22-52
IP Address:	192.168.0.147
Model:	EAP225-Outdoor
Firmware Version:	1.3.0 Build 20180614 Rel. 50359
CPU:	0%
Memory:	53%
Uptime:	1 days 07:16:24

5.1.2 LAN

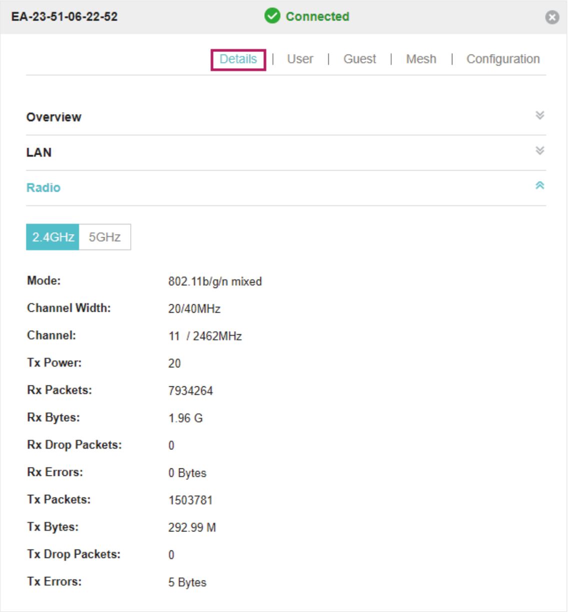
Click **LAN** to view the traffic information of the LAN port, including the total number of packets, the total size of data, the total number of packets loss, and the total size of error data in the process of receiving and transmitting data.



Rx Packets:	78422
Rx Bytes:	14.41 M
Rx Drop Packets:	0
Rx Errors:	0 Bytes
Tx Packets:	52068
Tx Bytes:	22.94 M
Tx Drop Packets:	0
Tx Errors:	0 Bytes

5.1.3 Radio

Click **Radio** to view the radio information including the frequency band, the wireless mode, the channel width, the channel, and the transmitting power. At 2.4GHz, you can also view parameters of receiving/transmitting data.



Mode: 802.11b/g/n mixed

Channel Width: 20/40MHz

Channel: 11 / 2462MHz

Tx Power: 20

Rx Packets: 7934264

Rx Bytes: 1.96 G

Rx Drop Packets: 0

Rx Errors: 0 Bytes

Tx Packets: 1503781

Tx Bytes: 292.99 M

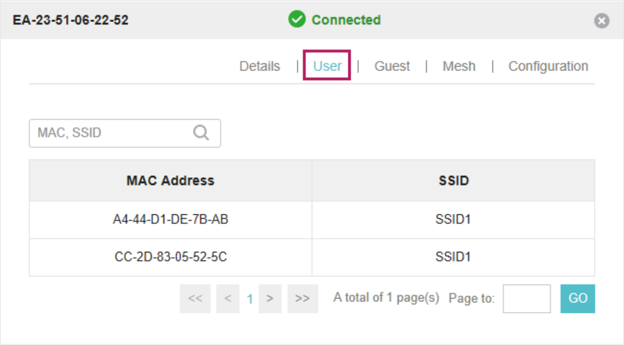
Tx Drop Packets: 0

Tx Errors: 5 Bytes

5.2 View Clients Connecting to the EAP

5.2.1 User

The **User** page displays the information of clients connecting to the SSID with Portal disabled, including their MAC addresses and connected SSIDs. You can click the client's MAC address to get its connection history.

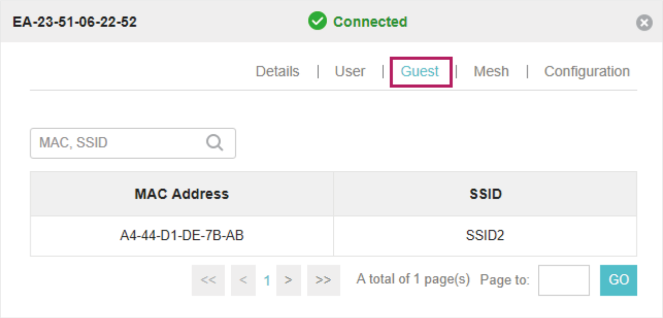

EA-23-51-06-22-52
Connected
Details | User | Guest | Mesh | Configuration
MAC, SSID

MAC Address	SSID
A4-44-D1-DE-7B-AB	SSID1
CC-2D-83-05-52-5C	SSID1

<< < 1 > >>
A total of 1 page(s) Page to:
GO

5.2.2 Guest

The **Guest** page displays the information of clients connecting to the SSID with Portal enabled, including their MAC addresses and connected SSIDs. You can click the client's MAC address to get its connection history.


EA-23-51-06-22-52
Connected
Details | User | Guest | Mesh | Configuration
MAC, SSID
<< < 1 > >> A total of 1 page(s) Page to: GO

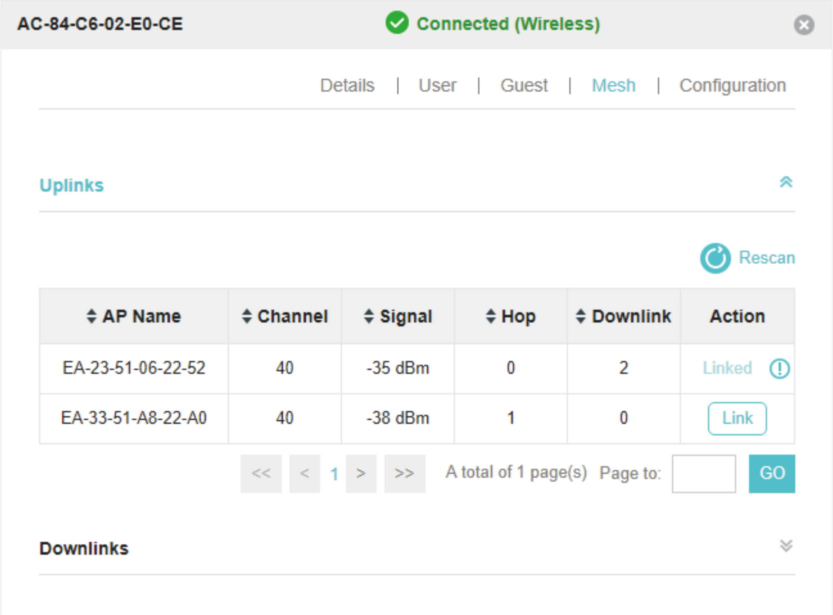
MAC Address	SSID
A4-44-D1-DE-7B-AB	SSID2

5.3 View Mesh Information of the EAP

The **Mesh** page is used to view and configure the mesh parameters of the EAP.

5.3.1 Uplinks

Here you can view the parameters of the uplink APs or click Link to change the uplink AP.


AC-84-C6-02-E0-CE
Connected (Wireless)
Details | User | Guest | Mesh | Configuration
Uplinks
Rescan
<< < 1 > >> A total of 1 page(s) Page to: GO
Downlinks

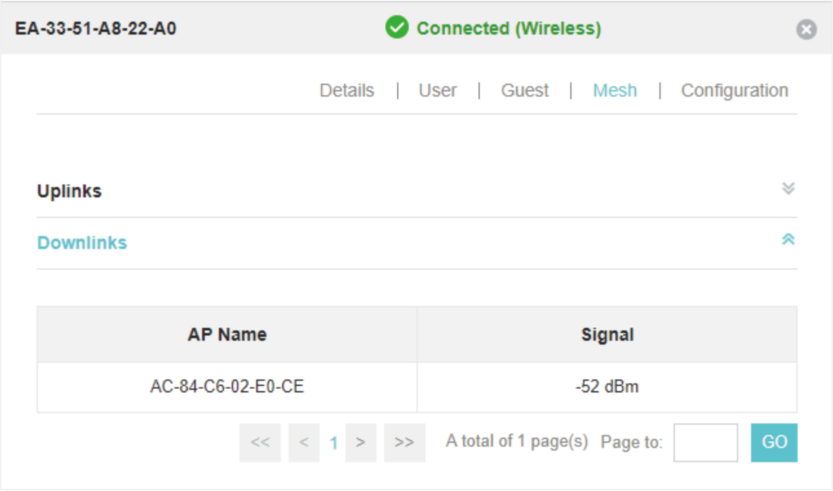
AP Name	Channel	Signal	Hop	Downlink	Action
EA-23-51-06-22-52	40	-35 dBm	0	2	Linked
EA-33-51-A8-22-A0	40	-38 dBm	1	0	Link

Tips:

- You can click Rescan to search the available uplink APs and the Uplink list will refresh.
- To build a mesh network with better performance, we recommend that you select the Uplink AP with the strongest signal, least hop and least Downlink AP.

5.3.2 Downlinks

Here you can view the downlink APs.



EA-33-51-A8-22-A0 ✓ Connected (Wireless)

Details | User | Guest | Mesh | Configuration

Uplinks

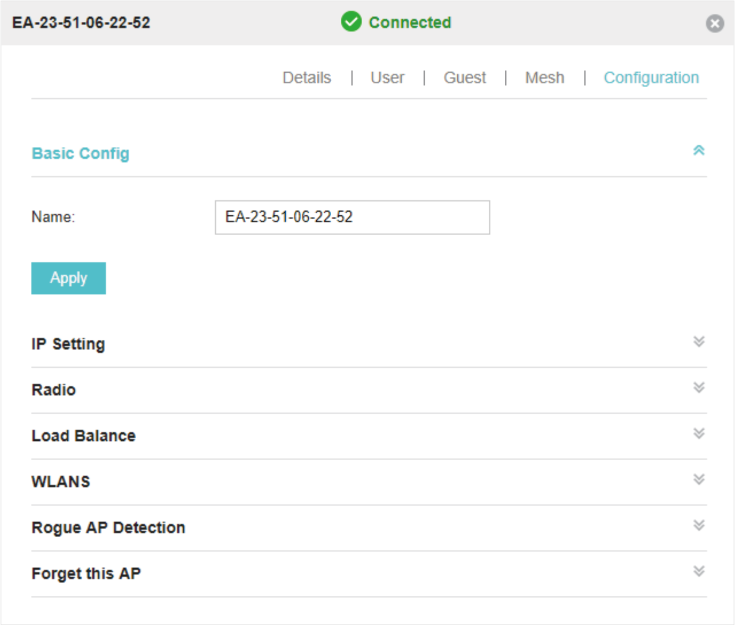
Downlinks

AP Name	Signal
AC-84-C6-02-E0-CE	-52 dBm

<< < 1 > >> A total of 1 page(s) Page to: GO

5.4 Configure the EAP

The **Configuration** page is used to configure the EAP. All the configurations will only take effect on this device.



EA-23-51-06-22-52 ✓ Connected

Details | User | Guest | Mesh | Configuration

Basic Config

Name: EA-23-51-06-22-52

Apply

IP Setting

Radio

Load Balance

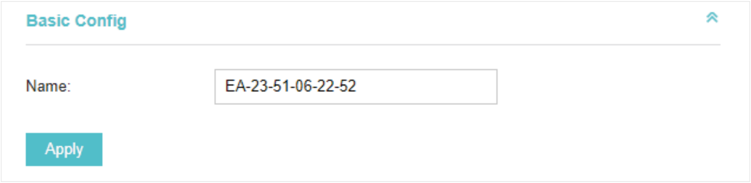
WLANS

Rogue AP Detection

Forget this AP

5.4.1 Basic Config

Here you can change the name of the EAP.



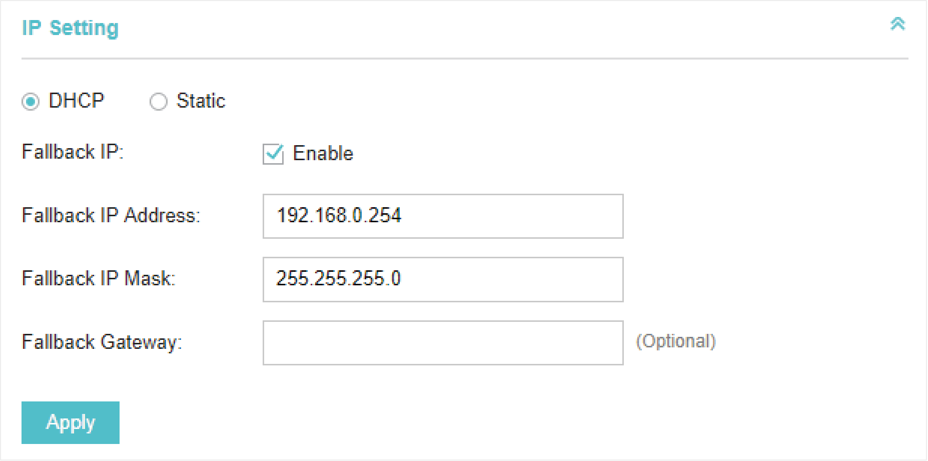
Basic Config

Name: EA-23-51-06-22-52

Apply

5.4.2 IP Setting

You can configure an IP address for this EAP. Two options are provided: DHCP and Static.



IP Setting

● DHCP ○ Static

Fallback IP: ☑ Enable

Fallback IP Address: 192.168.0.254

Fallback IP Mask: 255.255.255.0

Fallback Gateway: (Optional)

Get a Dynamic IP Address From the DHCP Server

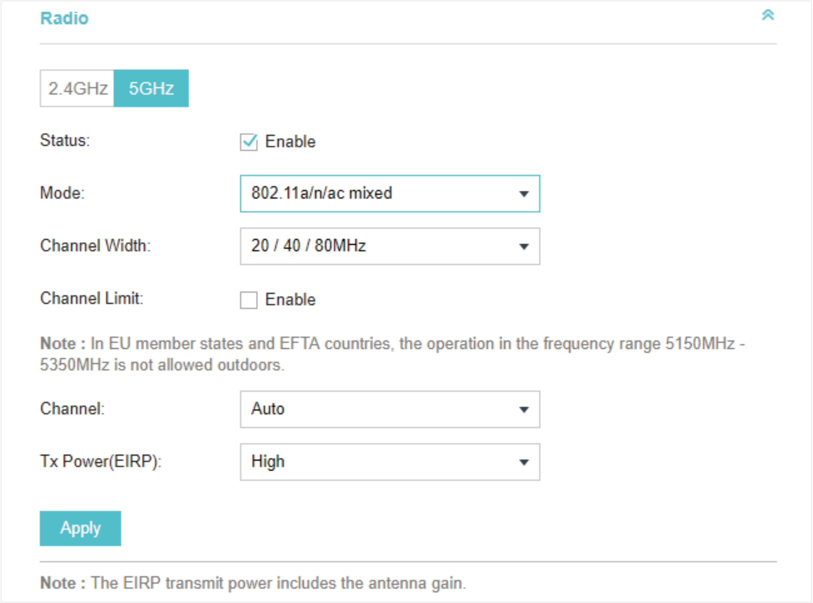
1. Configure your DHCP server.
2. Select **DHCP** on the page above.
3. Enable the Fallback IP feature. When the device cannot get a dynamic IP address, the fallback IP address will be used.
4. Set IP address, IP mask and gateway for the fallback address and click **Apply**.

Manually Set a Static IP Address for the EAP

1. Select **Static**.
2. Set the IP address, IP mask and gateway for the static address and click **Apply**.

5.4.3 Radio

Radio settings directly control the behavior of the radio in the EAP device and its interaction with the physical medium; that is, how and what type of signal the EAP device emits.



Radio

2.4GHz 5GHz

Status: ☑ Enable

Mode: 802.11a/n/ac mixed

Channel Width: 20 / 40 / 80MHz

Channel Limit: □ Enable

Note : In EU member states and EFTA countries, the operation in the frequency range 5150MHz - 5350MHz is not allowed outdoors.

Channel: Auto

Tx Power(EIRP): High

Note : The EIRP transmit power includes the antenna gain.

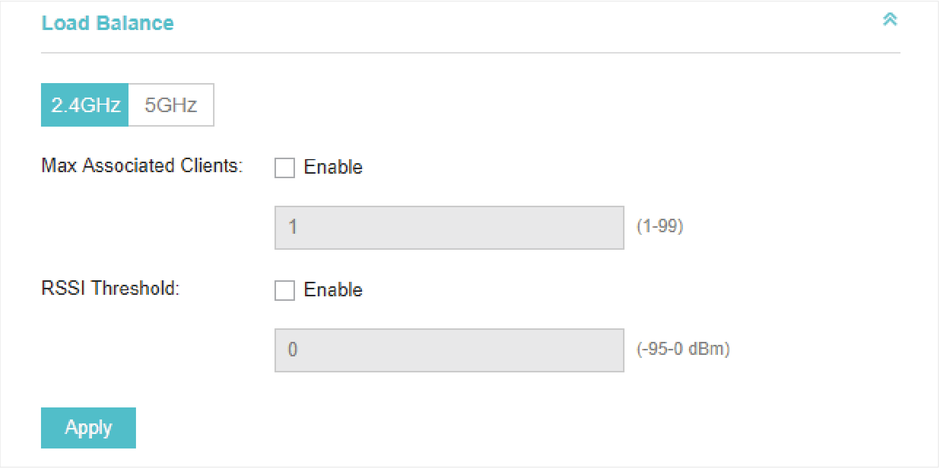
Select the frequency band (2.4GHz/5GHz) and configure the following parameters.

Status	Enabled by default. If you disable the option, the radio on the frequency band will turn off.
Mode	Select the IEEE 802.11 mode the radio uses. When the frequency of 2.4GHz is selected, 802.11b/g/n mixed, 802.11b/g mixed, and 802.11n only modes are available: **802.11b/g/n mixed**: All of 802.11b, 802.11g, and 802.11n clients operating in the 2.4GHz frequency can connect to the EAP device. We recommend you select the 802.11b/g/n mixed mode. **802.11b/g mixed**: Both 802.11b and 802.11g clients can connect to the EAP device. **802.11n only**: Only 802.11n clients can connect to the EAP device. When the frequency of 5GHz is selected, 802.11 n/ac mixed, 802.11a/n mixed, 802.11 ac onl7, 802.11a only, and 802.11n only modes are available: **802.11n/ac mixed**: Both 802.11n clients and 802.11ac clients operating in the 5GHz frequency can connect to the EAP device. **802.11a/n mixed**: Both 802.11a clients and 802.11n clients operating in the 5GHz frequency can connect to the EAP device. **802.11ac only**: Only 802.11ac clients can connect to the EAP device. **802.11a only**: Only 802.11a clients can connect to the EAP device. **802.11n only**: Only 802.11n clients can connect to the EAP device.
Channel Limit	**For the EAPs that support DFS in EU version, there is a Channel Limit option. If you want to use your EAP outdoors, enable this option to comply with the laws in your country.**

Channel Width	Select the channel width of the EAP device. The available options differ among different EAPs. For some EAPs, available options include **20MHz**, **40MHz** and **20/40MHz**. For other EAPs, available options include **20MHz**, **40MHz**, **80MHz** and **20/40/80MHz**. The 20/40 MHz and 20/40/80MHz channels enable higher data rates but leave fewer channels available for use by other 2.4GHz and 5GHz devices. When the radio mode includes 802.11n, we recommend you set the channel bandwidth to 20/40 MHz or 20/40/80MHz to improve the transmission speed.
Channel	Select the channel used by the EAP device to improve wireless performance. The range of available channels is determined by the radio mode and the country setting. If you select Auto for the channel setting, the EAP device scans available channels and selects a channel where the least amount of traffic is detected.
Tx Power (EIRP)	Select the Tx Power (Transmit Power) in the 4 options: **Low, Medium, High** and **Custom**. Low, Medium and High are based on the Min. Txpower (Minimum transmit power) and Max. TxPower (maximum transmit power. It may vary among different countries and regions). **Low**: Min. TxPower + (Max. TxPower-Min. TxPower) * 20% (round off the value) **Medium**: Min. TxPower + (Max. TxPower-Min. TxPower) * 60% (round off the value) **High**: Max. TxPower **Custom**: Enter a value manually.

5.4.4 Load Balance

By setting the maximum number of clients accessing the EAPs, Load Balance helps to achieve rational use of network resources.



Load Balance

Max Associated Clients: □ Enable

1 (1-99)

RSSI Threshold: □ Enable

0 (-95-0 dBm)

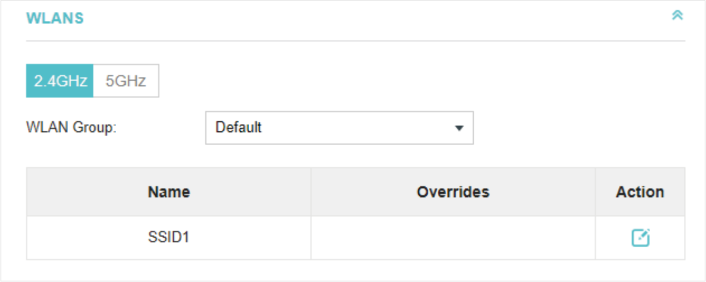
Select the frequency band (2.4GHz/5GHz) and configure the parameters.

Max Associated Clients	Enable this function and specify the maximum number of connected clients. While more clients requesting to connect, the EAP will disconnect those with weaker signals.

RSSI Threshold	Enable this function and enter the threshold of **RSSI** (Received Signal Strength Indication). When the clients' signal is weaker than the **RSSI Threshold** you've set, the clients will be disconnected from the EAP.

5.4.5 WLANs

You can specify a different SSID name and password to override the previous SSID. After that, clients can only see the new SSID and use the new password to access the network. Follow the steps below to override the SSID.

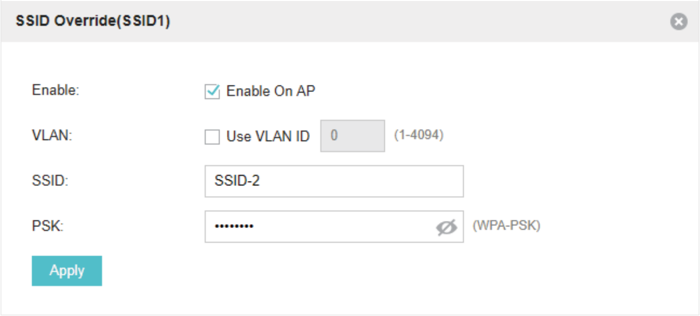


WLAN Group: Default

Name	Overrides	Action
SSID1		✎

1. Select the frequency band and WLAN group.

2. Click ✎ and the following window will pop up.


SSID Override(SSID1)

Enable: ☑ Enable On AP

VLAN: □ Use VLAN ID 0 (1-4094)

SSID: SSID-2

PSK: •••••••• (WPA-PSK)

3. Check the box to enable the feature.

4. You can join the overridden SSID in to a VLAN. Check the **Use VLAN ID** box and specify a VLAN ID.

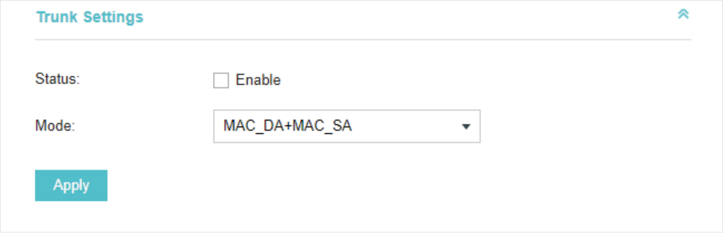
5. Specify a new name and password for the SSID.

6. Click **Apply** to save the configuration.

5.4.6 Trunk Settings

Only EAP330 supports this function.

The trunk function can bundles multiple Ethernet links into a logical link to increase bandwidth and improve network reliability.


Trunk Settings

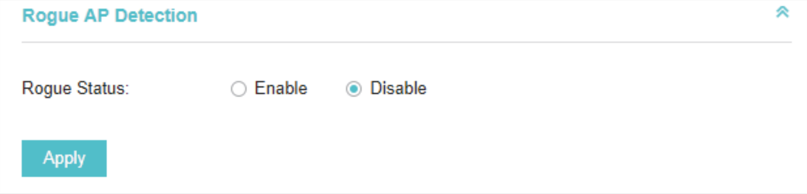
Status: □ Enable

Mode: MAC_DA+MAC_SA

Status	Enable this function. The EAP330 has two 1000Mbps Ethernet ports. If the Trunk function is enabled and the ports are in the speed of 1000Mbps Full Duplex, the whole bandwidth of the trunk link is up to 4Gbps (2000Mbps * 2).
Mode	Select the applied mode of Trunk Arithmetic from the drop-down list. • MAC_DA + MAC_SA: When this option is selected, the arithmetic will be based on the source and destination MAC addresses of the packets. • MAC_DA: When this option is selected, the arithmetic will be based on the destination MAC addresses of the packets. • MAC_SA: When this option is selected, the arithmetic will be based on the source MAC addresses of the packets.

5.4.7 Rogue AP Detection

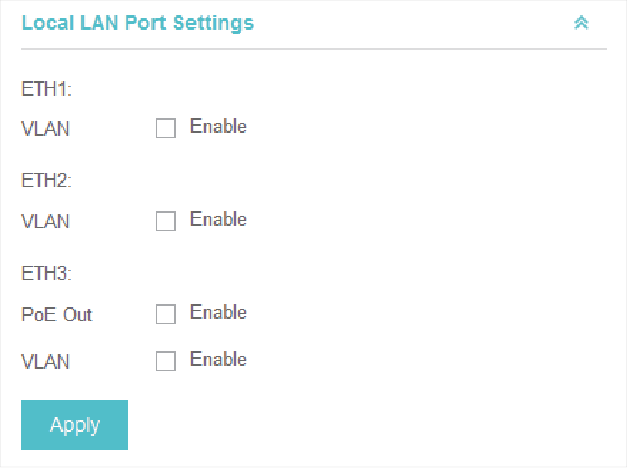
With this option enabled, the EAP device will detect rogue APs in all channels.


Rogue AP Detection

Rogue Status: ○ Enable ● Disable

5.4.8 Local LAN Port Settings (Only for EAP115-Wall and EAP225-Wall)

You can configure the LAN port of the EAP. Here we use EAP225-Wall as an example.


Local LAN Port Settings

ETH1:

VLAN □ Enable

ETH2:

VLAN □ Enable

ETH3:

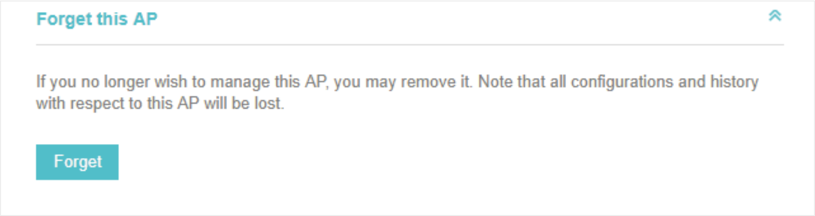
PoE Out □ Enable

VLAN □ Enable

VLAN	Enable this feature and specify the VLAN that the EAP is added to, and then the hosts connected to this EAP can only communicate with the devices in this VLAN. The valid values are from 1 to 4094, and the default is 1.
PoE Out	If your EAP has PoE OUT port, you can enable this option to supply power to the connected device on this port. The EAP that has no PoE OUT port does not support this feature.

5.4.9 Forget this AP

If you no longer want to manage this EAP, you may remove it. All the configurations and history about this EAP will be deleted. It is recommended to back up the configurations of this EAP before you forget it.



Forget this AP

If you no longer wish to manage this AP, you may remove it. Note that all configurations and history with respect to this AP will be lost.

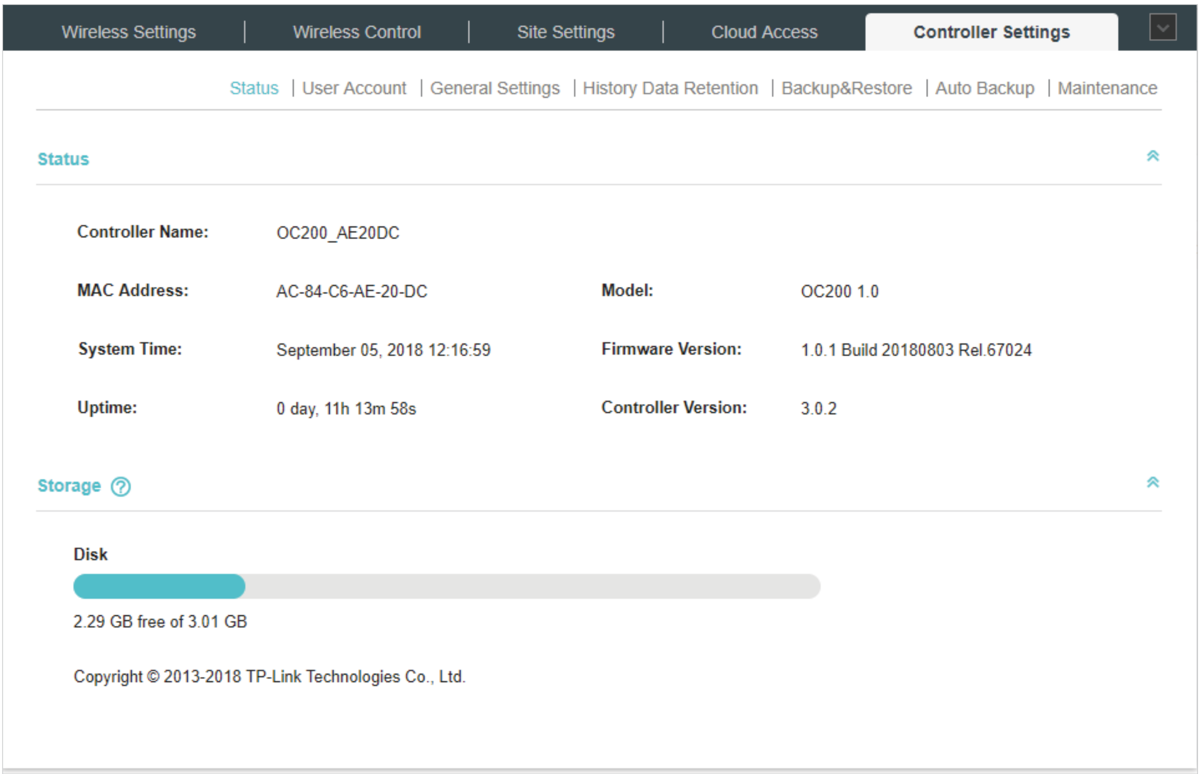
6 Manage the OC200

This chapter mainly introduces how to manage the user account and configure system settings. This chapter includes the following contents.

- *Status*
- *User Account*
- *General Setting*
- *History Data Retention*
- *Backup&Restore*
- *Auto Backup*
- *Maintenance*

6.1 Status

The Status page displays the basic information of the OC200.



Wireless Settings
Wireless Control
Site Settings
Cloud Access
Controller Settings
Status | User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | Maintenance
Status
Storage
Disk

Controller Name: OC200_AE20DC

MAC Address: AC-84-C6-AE-20-DC

Model: OC200 1.0

System Time: September 05, 2018 12:16:59

Firmware Version: 1.0.1 Build 20180803 Rel.67024

Uptime: 0 day, 11h 13m 58s

Controller Version: 3.0.2

2.29 GB free of 3.01 GB

Copyright © 2013-2018 TP-Link Technologies Co., Ltd.

Status	Displays the basic information of the OC200.
Storage	Displays the storage of the OC200 and the external USB storage device. Tips: The external USB storage device will appear here after you have plugged it into the USB port. The USB storage device can be used for backing up data automatically. Note that this function is only available when OC200 is powered by a PoE device.

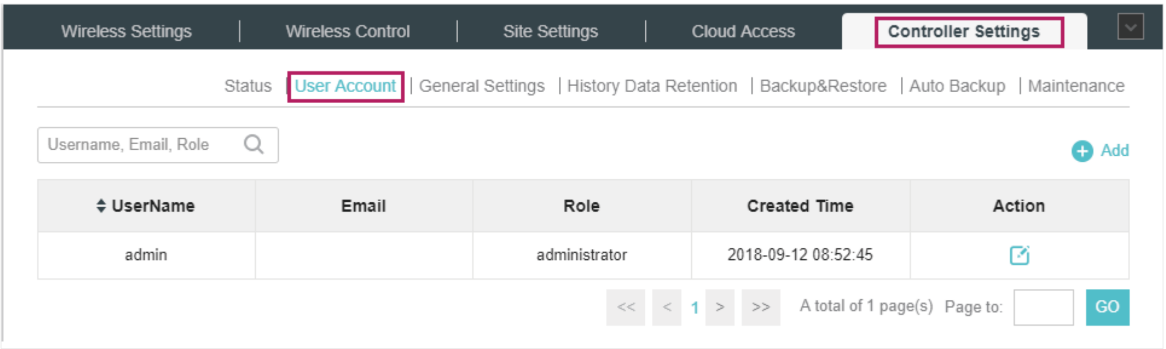
6.2 User Account

You can use different user account to log in to the OC200. User has three roles: administrator, operator and observer. The administration authority varies among different roles.

Administrator	The first administrator account is created in the Basic Configuration process and this account can not be deleted. An administrator can change the settings of the EAP network and create and delete user accounts.
Operator	An operator account can be created or deleted by the administrator. The operator can change the settings of the EAP network.
Observer	An observer account can be created or deleted by the administrator. The observer can only view the status and settings of the EAP network but not change the settings.

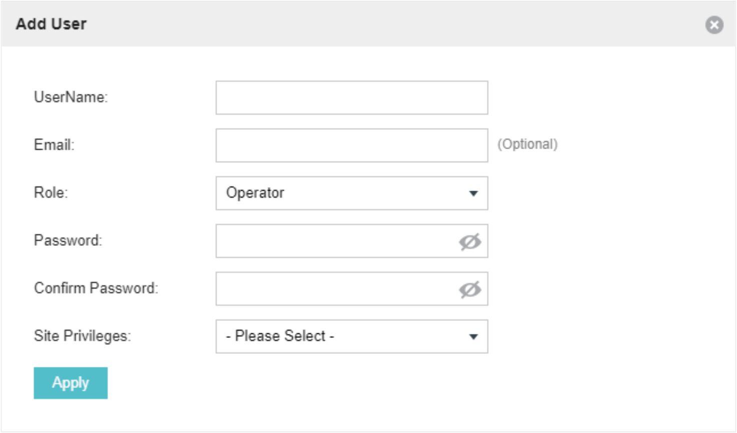
Follow the steps below to add user account.

1. Go to **Controller Settings > User Account.**



UserName	Email	Role	Created Time	Action
admin		administrator	2018-09-12 08:52:45	

2. Click Add and the following window will pop up.



UserName:

Email: (Optional)

Role: Operator

Password:

Confirm Password:

Site Privileges: - Please Select -

3. Specify the username, Email and password of the account.

4. Select the role from the drop-down list.

- If you select **operator** or **observer**, you also need to select the **Site Privileges**.

- If you select **administrator**, the **Site Privileges** option will not appear and all sites are available for the administrator user.

5. Click **Apply** to add the user account.

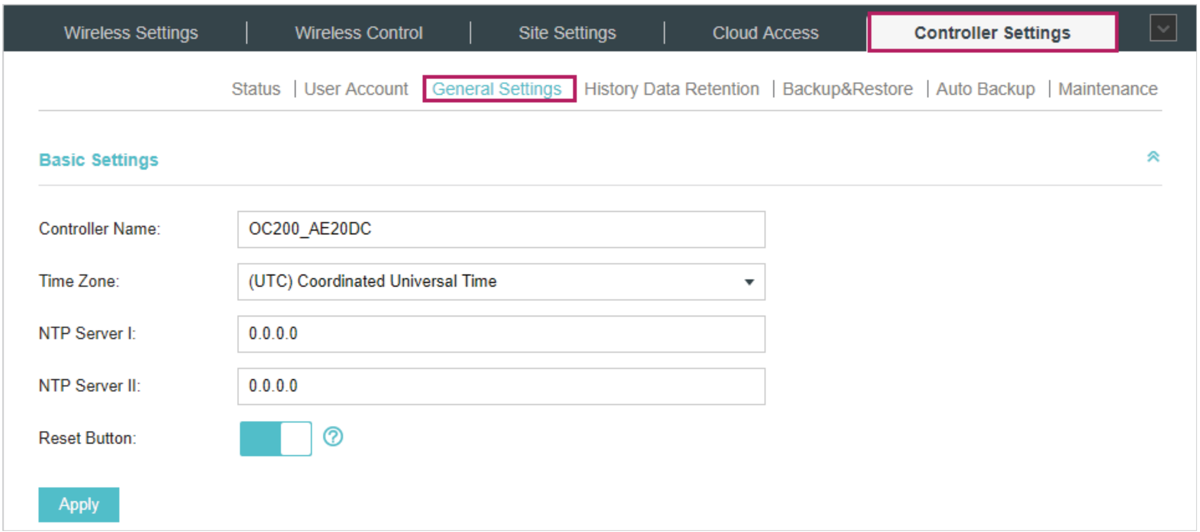
Note:

- You can refer to the **Role** page to view the user role's type, description information, permission scope and created time.
- The user account cannot be used to log in to the OC200 through Omada Cloud Service. To access the OC200 via Cloud Access, you should be a cloud user. To add a cloud user, refer to manage the cloud users.

6.3 General Setting

Go to **Controller Settings** > **General Setting** page and configure the basic settings of OC200.

6.3.1 Configure Basic Settings



Controller Name: OC200_AE20DC

Time Zone: (UTC) Coordinated Universal Time

NTP Server I: 0.0.0.0

NTP Server II: 0.0.0.0

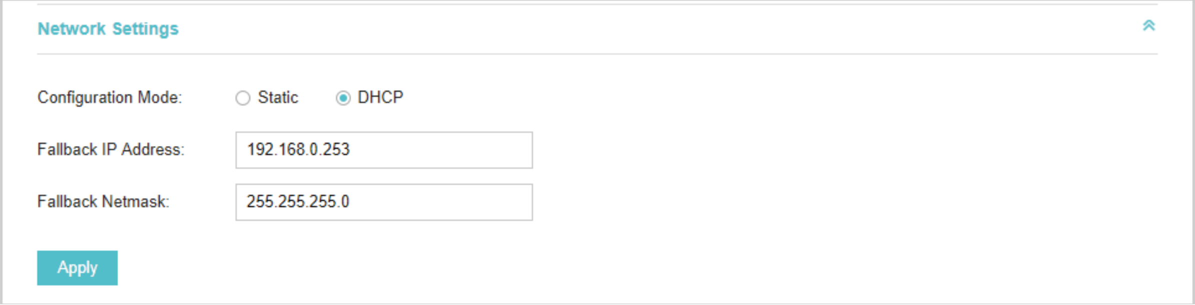
Reset Button:

Controller Name	Specify a name for the OC200.
Time Zone	Specify the time zone for OC200.
NTP Server I	Specify the primary NTP server for the OC200.
NTP Server II	Specify the secondary NTP server for the OC200.
Reset Button	With this option enabled, the OC200 can be reset via its hardware reset button; otherwise can only be reset in the Maintenance page.

6.3.2 Configure Network Settings

Choose the way for the OC200 to get IP settings. By default, it is DHCP.

- **Choose the Configuration Mode as DHCP**



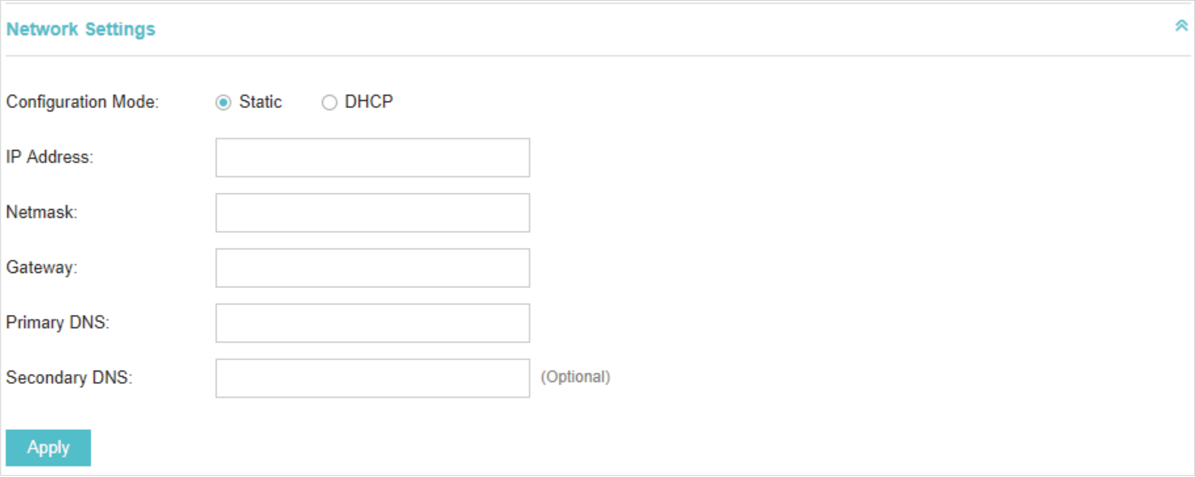
Configuration Mode: ○ Static ● DHCP

Fallback IP Address: 192.168.0.253

Fallback Netmask: 255.255.255.0

Configuration Mode	Choose the configuration mode as DHCP
Fallback IP Address	Specify the fallback IP address for the OC200. The fallback is used when the OC200 failed to get an IP address from the DHCP server.
Fallback Netmask	Specify the mask of the fallback IP address.

- **Choose the Configuration Mode as Static**



Network Settings

Configuration Mode: ● Static ○ DHCP

IP Address:

Netmask:

Gateway:

Primary DNS:

Secondary DNS: (Optional)

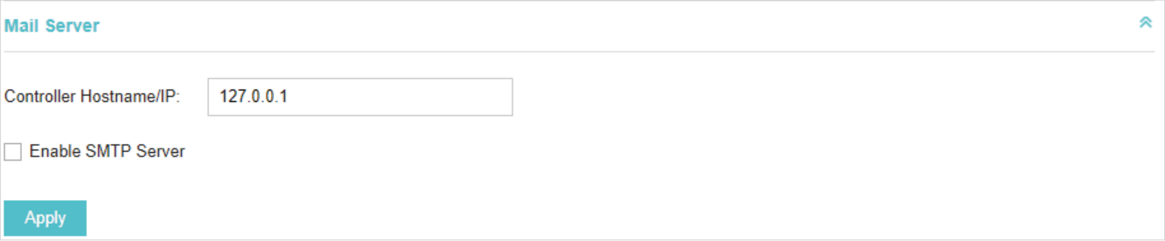
Configuration Mode	Choose the configuration mode as Static.
IP Address	Enter an IP address for the OC200.
Netmask	Enter the mask of the IP address.
Gateway	Enter the IP address of the default gateway for the OC200.
Primary DNS	Enter the IP address of the Primary DNS server.
Secondary DNS	(Optional) Enter the IP address of the Secondary DNS server.

6.3.3 Configure Mail Server

With the Mail Server, you can reset the login password of the user account if necessary. An email with the link of resetting password will be sent from the OC200. It is different from the SMTP Server, which is just for the system log emails sending.

Follow the steps below to configure mail server.

1. Go to **Controller Settings > General Setting** and click **Mail Server**.



Mail Server

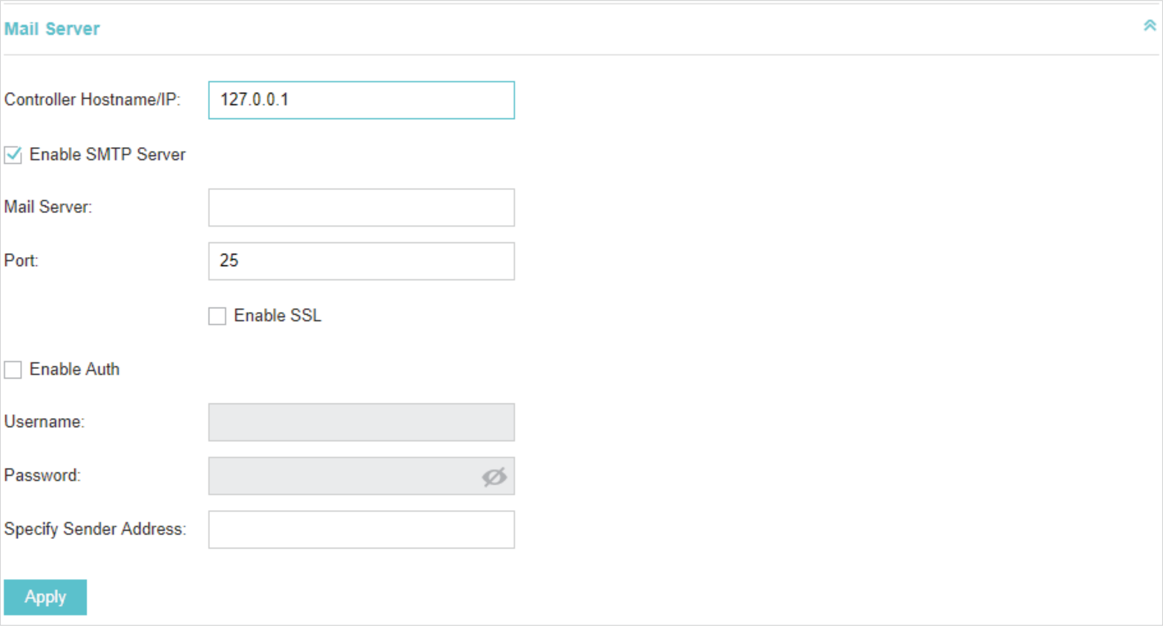
Controller Hostname/IP: 127.0.0.1

□ Enable SMTP Server

2. Enter the hostname or IP address of the OC200. The default IP address of the OC200 is **127.0.0.1**. You can keep it or customize the hostname or IP address which can be visited by the management host.

When the email with the link of resetting password are sent out, the OC200 or IP address will be specified in the Controller URL in every message.

3. Check the box to enable **SMTP Server**, and then the following screen will appear.



Mail Server

Controller Hostname/IP: 127.0.0.1

☑ Enable SMTP Server

Mail Server:

Port: 25

□ Enable SSL

□ Enable Auth

Username:

Password:

Specify Sender Address:

4. Configure the following parameters.

Mail Server	Enter the IP address or domain of SMTP Server.
Port	The SMTP server uses port 25 as default. You can enable SSL (Security Socket Layer) to enhance secure communications over the Internet. If SSL is enabled, the port number will automatically change to 465.
Enable Auth	Check the box to enable authentication (Optional).
Username/Password	If you enable authentication, enter the username and password required by the mail server.
Specify Sender Address	Specify the sender's mail address. Enter the email address that will appear as the sender for resetting password.

5. Click **Apply** to save the configuration.

Note:

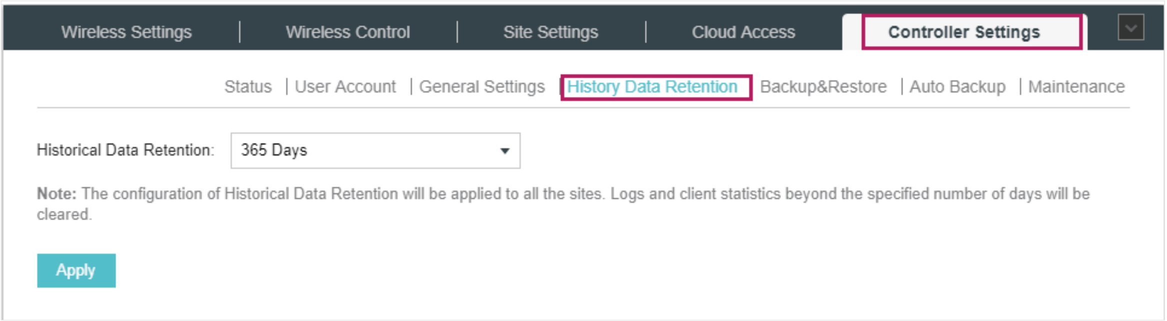
Specify the account email address based on the Mail server to receive the email for resetting password.

6.4 History Data Retention

History Data Retention allows users to determine the retention of logs and client statistics. The logs and client statistics beyond the specified number of days will be cleared. For example, with **7 days** selected, only the logs and client statistics in recent 7 days will be retained, and the data beyond 7 days will be cleared from the OC200.

Follow the steps below to configure Historical Data Retention:

1. Go to **Controller Settings** > **History Data Retention.**



Historical Data Retention: 365 Days

Note: The configuration of Historical Data Retention will be applied to all the sites. Logs and client statistics beyond the specified number of days will be cleared.

2. Select the length of time in days that data will be retained from the drop-down list. Seven options are provided: **7 days**, **30 days**, **60 days**, **90 days**, **180 days**, and **365 days.**

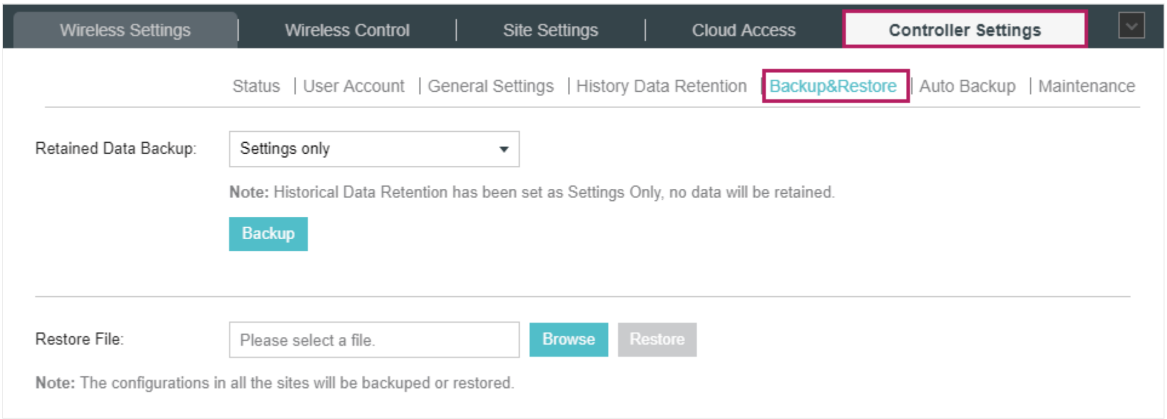
3. Click **Apply.**

6.5 Backup&Restore

You can save the current configuration and data in the OC200 as a backup file and if necessary, restore the configuration using the backup file. We recommend you back up the settings before upgrading the device. This function is available only for local logged-in users.

Follow the steps below to backup and restore the configuration.

1. Go to **Controller Settings > Backup&Restore.**



Retained Data Backup: Settings only

Note: Historical Data Retention has been set as Settings Only, no data will be retained.

Restore File: Please select a file.

Note: The configurations in all the sites will be backuped or restored.

2. Select the length of time in days that data will be backed up in the **Retained Data Backup** drop-down list. For example, with **7days** selected, the data only in recent 7days will be backed up.

3. Click **Backup** to save the backup file.

4. If necessary, click **Browse** to locate and choose the backup file. Then click **Restore** to restore the configuration.

Note:

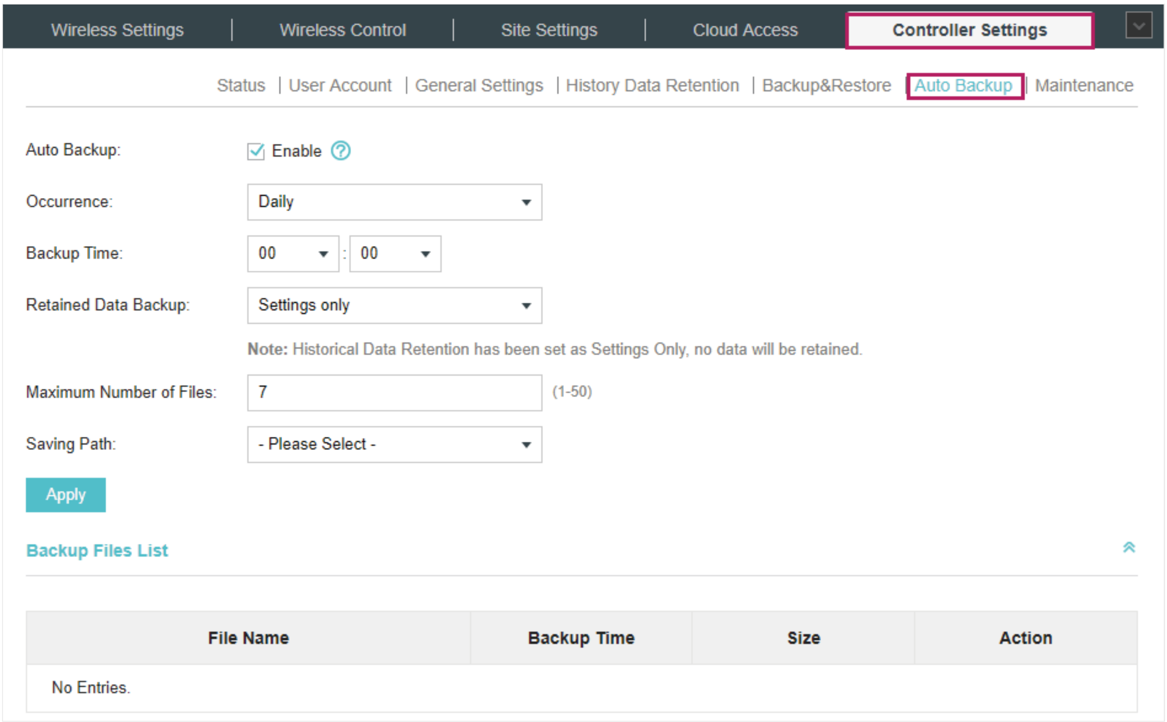
- This function is only for local logged-in users.
- If you do not want to back up historical data, you can select **Settings only** to get only the settings saved in the backup files.
- If you do not want to back up data manually, you can enable the **Auto Backup** function. Please refer to Auto Backup.
- The configuration of the mesh network will not be backed up. Thus the configuration of the mesh network cannot be restored. You should configure the mesh again if necessary. Please refer to Configure Mesh.

6.6 Auto Backup

With Auto Backup enabled, the OC200 settings will be scheduled to back up the configuration and data automatically at the specified time.

Follow the steps below to configure Auto Backup function.

1. Go to **Controller Settings > Auto Backup.**



Auto Backup: ☑ Enable

Occurrence: Daily

Backup Time: 00 : 00

Retained Data Backup: Settings only

Note: Historical Data Retention has been set as Settings Only, no data will be retained.

Maximum Number of Files: 7 (1-50)

Saving Path: - Please Select -

File Name	Backup Time	Size	Action
No Entries.			

2. Check the box to enable Auto Backup function.

3. Select how often to perform Auto Backup in the **Occurrence**. You can choose **Daily**, **Weekly**, **Monthly** or **Yearly** from drop-down list. Then set an appropriate time to back up files in the **Backup Time**.

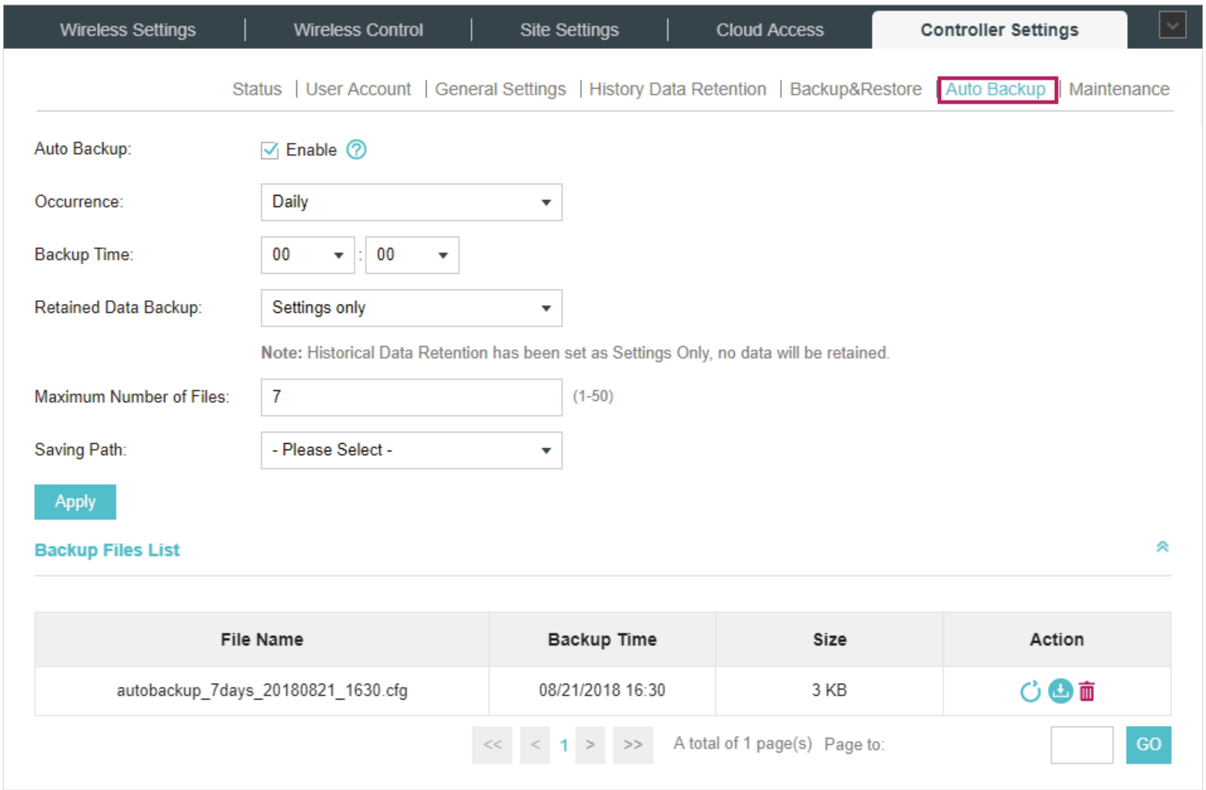
   Note: When you choose the Occurrence as Monthly, please carefully choose the backup date in Backup Time. For example, if you choose to automatically backup the data on the 31th day of every month. When it comes to June, which is only 30 days long, the auto backup will not take effect

4. Select the length of time in days that data will be backed up in the **Retained Data Backup**. For example, with **7days** selected, the data only in recent 7days will be backed up.

5. Specify the maximum number of backup files to save in the **Maximum Number of Files**. The default is 7.

6. Please select the saving path for the data. Please choose the external USB storage device.

You can view the name, backup time and size of the backup files in the **Backup Files List**.



Auto Backup: ☑ Enable

Occurrence: Daily

Backup Time: 00 : 00

Retained Data Backup: Settings only

Note: Historical Data Retention has been set as Settings Only, no data will be retained.

Maximum Number of Files: 7 (1-50)

Saving Path: - Please Select -

Backup Files List

File Name	Backup Time	Size	Action
autobackup_7days_20180821_1630.cfg	08/21/2018 16:30	3 KB	↻ ⬇ 🗑

<< < 1 > >> A total of 1 page(s) Page to:

You can execute the corresponding operation to the backup files by clicking an icon in the Action column.

↻	Restore the data and configurations in the backup file.
⬇	Download the backup file.
🗑	Delete the backup file.

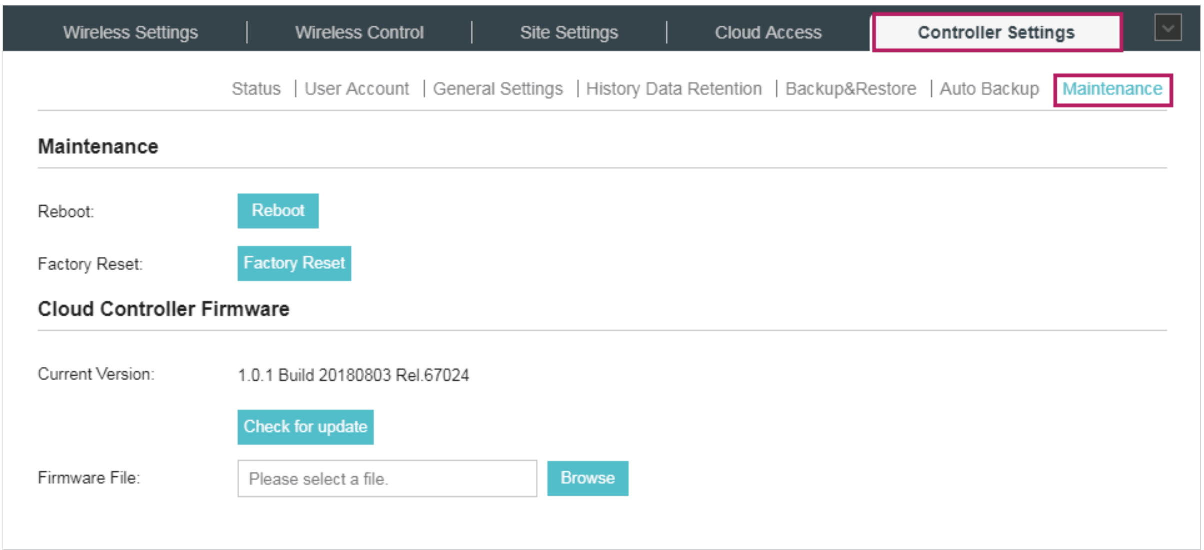
Note:

- To back up data manually and restore the data to the OC200, configure **Backup&Restore** function. Please refer to Backup&Restore.
- If you do not want to back up historical data, you can select **Settings only** to get only the settings saved in the backup files.
- The auto backup files will be stored in the external USB sorage device. This function is only available when OC200 is powered by a PoE device.
- The configuration of the mesh network will not be backed up. Thus the configuration of the mesh network cannot be restored. You should configure the mesh again if necessary. Please refer to Configure Mesh.

6.7 Maintenance

On the **Controller Settings** > **Maintenance** page, you can reboot, rest or upgrade the firmware of OC200.

When you launch theOC200 via Cloud Access, you can check the firmware and upgrade it online. When you launch the OC200 locally, you can upgrade it online, or manually select a firmware to upgrade it.



Maintenance

Reboot:

Factory Reset:

Cloud Controller Firmware

Current Version: 1.0.1 Build 20180803 Rel.67024

Firmware File: Please select a file.

7 Application Example

A factory has a wireless network with three EAPs managed by the OC200. The network administrator wants to :

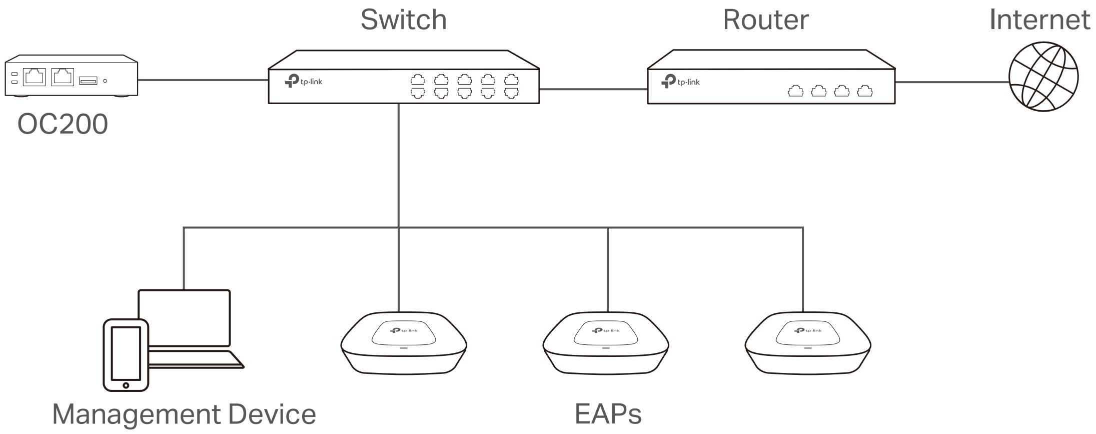
- Monitor the EAPs with the Map.
- Enable Portal function to drive customers' attention to the ads of the supermarket when customers attempt to access the network. The costumers need to use a simple password to pass the authentication.
- Allow the employees of the restaurant to access the network resources without portal authentication.
- Schedule the radio to operate only during the working time (8:00 am to 22:00 pm) in order to reduce power consumption.

Follow the steps below to achieve the requirements above.

7.1 Basic Configuration

Follow the steps below to do the basic configuration.

1. Connect the devices as the following topology shows.



2. Launch the OC200 and follow the instructions to complete some initial configurations.

3. Log into the management interface of OC200.

4. Adopt the pending EAP devices.

7.2 Advanced Settings

After the basic configuration, refer to the following content to meet the network administrator's requirements.

7.2.1 Monitor the EAPs with Map

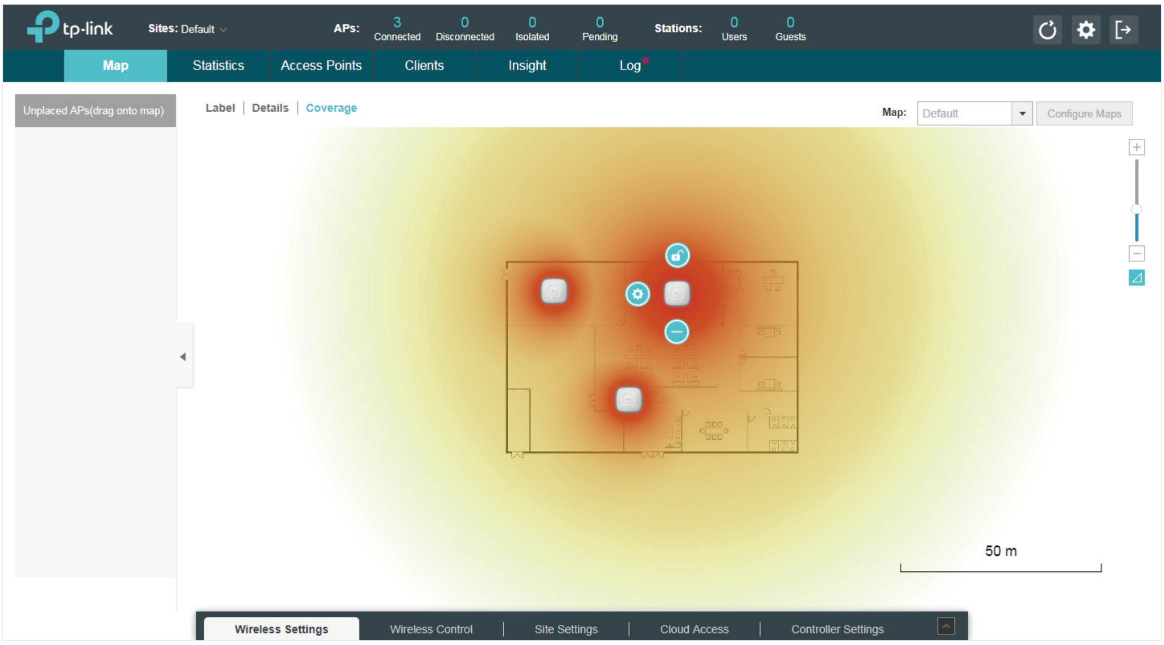
Follow the steps below to create a map and monitor the EAPs with the map.

1. Go to the **Map**.

2. Import a local map and set the map scale.

3. Drag the EAPs to the appropriate locations on the map.

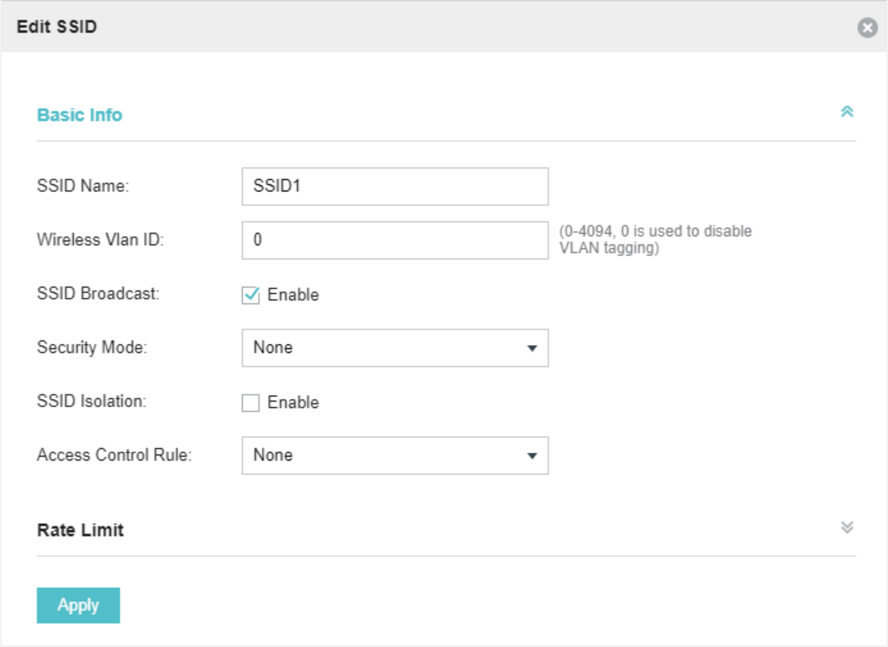
4. Click **Coverage** and you can see the representation of the EAPs' wireless coverage.



7.2.2 Configure Portal Authentication

Follow the steps below to configure Portal function.

1. Go to **Wireless Settings** > **Basic Wireless Settings** and edit the SSID we created in the basic configuration.



Edit SSID

Basic Info

SSID Name: SSID1

Wireless Vlan ID: 0 (0-4094, 0 is used to disable VLAN tagging)

SSID Broadcast: ☑ Enable

Security Mode: None

SSID Isolation: □ Enable

Access Control Rule: None

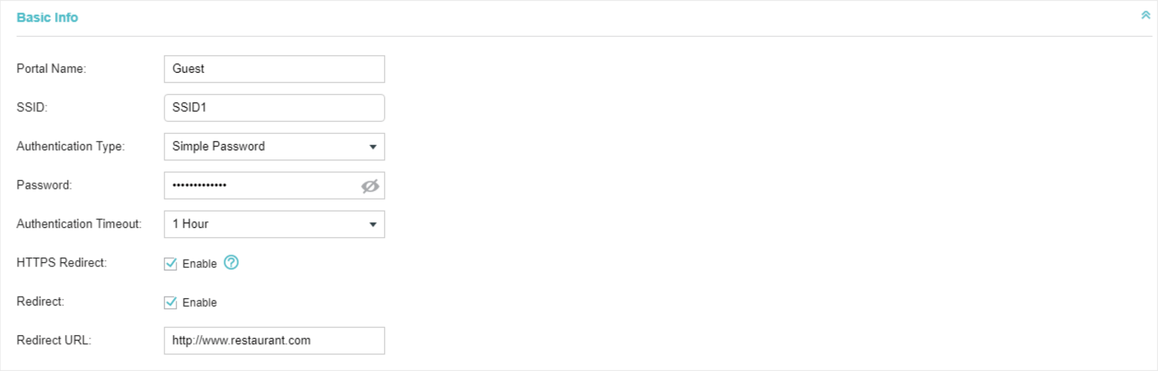
Rate Limit

Apply

To make it easier for customers to connect, change the Security Mode from WPA-PSK to None. Customers can connect to the EAPs without password and be redirected to the Portal Authentication where the correct password will be required.

2. Open the global configuration window and go to **Wireless Control** > **Portal.** Click ⊕ Add a New Portal The configuration window will pop up.

3. In the **Basic Info** section, complete the basic settings for the portal.



Basic Info

Portal Name:	Guest
SSID:	SSID1
Authentication Type:	Simple Password
Password:	•••••••••••••
Authentication Timeout:	1 Hour
HTTPS Redirect:	☑ Enable
Redirect:	☑ Enable
Redirect URL:	http://www.restaurant.com

1) Specify a name for the portal.

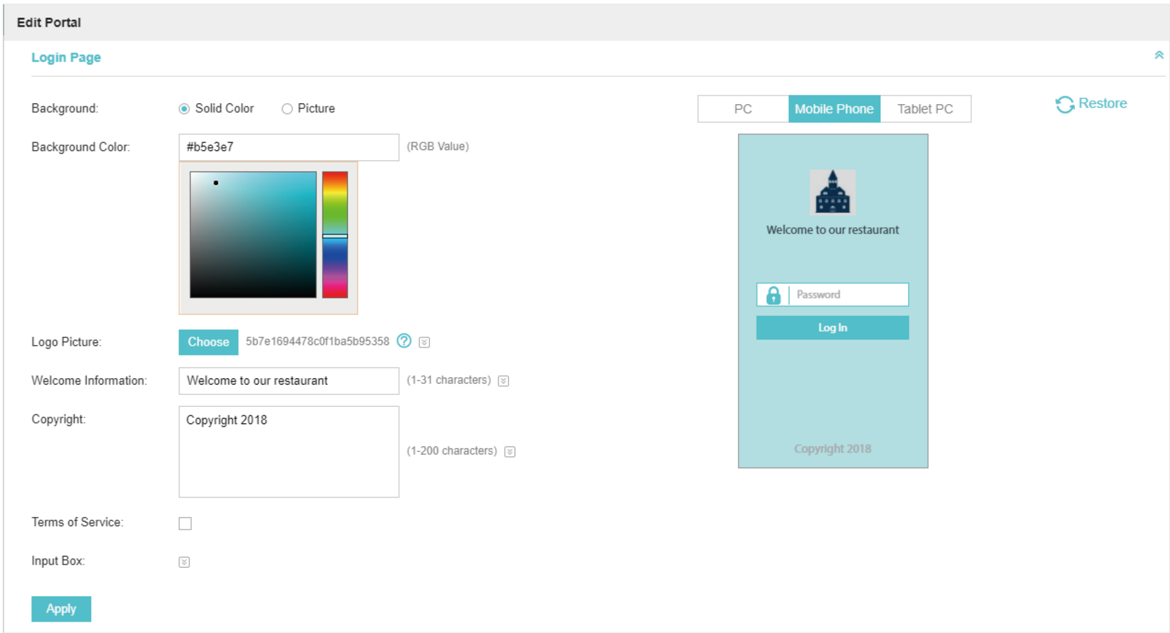
2) Select an SSID for the portal.

3) Select the Authentication Type as Simple Password. Specify a simple password for the guests.

4) Select the **Authentication Timeout.** For example, 1 Hour is suitable for the customers at the restaurant.

5) Enable the **Redirect** to drive the costumers to the restaurant's homepage after successful login. We can put some promotion information on the page.

4. In the **Login Page** section, configure the login page.

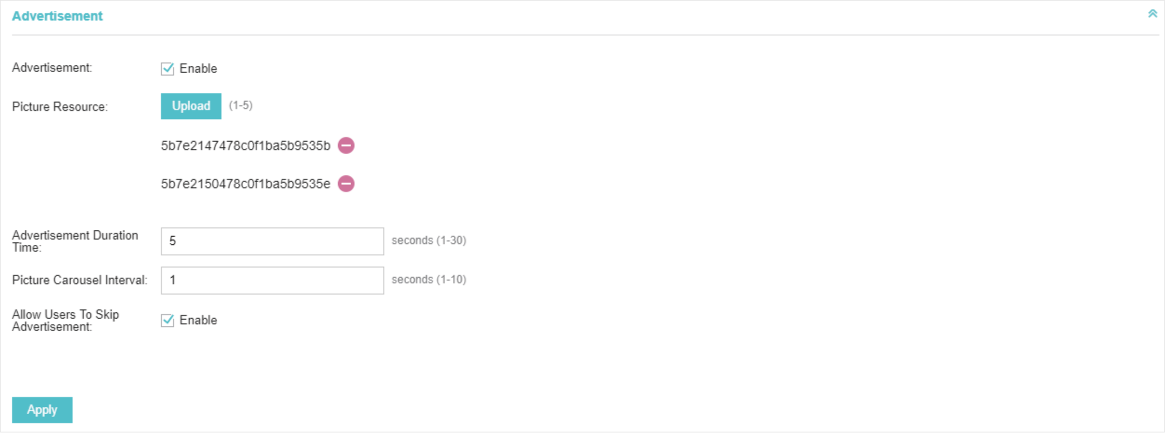


Edit Portal

Login Page

Background:	● Solid Color ○ Picture	
Background Color:	#b5e3e7	(RGB Value)
Logo Picture:	Choose 5b7e1694478c0f1ba5b95358	
Welcome Information:	Welcome to our restaurant	(1-31 characters)
Copyright:	Copyright 2018	(1-200 characters)
Terms of Service:	□	
Input Box:		

5. In the Advertisement section, upload two pictures of the restaurant and set the related parameters.



Advertisement

Advertisement: ☑ Enable

Picture Resource: Upload (1-5)

5b7e2147478c0f1ba5b9535b

5b7e2150478c0f1ba5b9535e

Advertisement Duration Time: 5 seconds (1-30)

Picture Carousel Interval: 1 seconds (1-10)

Allow Users To Skip Advertisement: ☑ Enable

Apply

6. Click **Apply**.

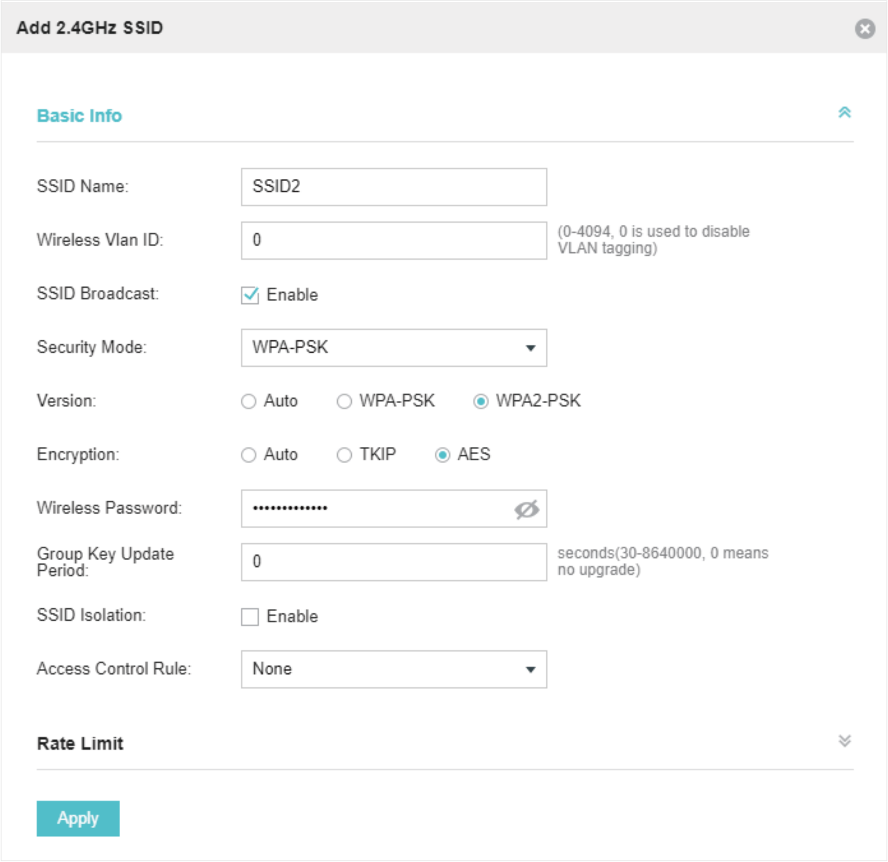
7.2.3 Create a SSID for the Employees

We have created a SSID in the basic configuration for the customers. Here we need to create another SSID for the employees to allow them to access the network without portal authentication. In addition, the new SSID should be invisible for the customers.

Follow the steps below to create a SSID for the employees.

1. Open the global configuration window and go to **Wireless Settings** > **Basic Wireless Settings.**

2. Click **Add** to add a new SSID.



Add 2.4GHz SSID

Basic Info

SSID Name: SSID2

Wireless Vlan ID: 0 (0-4094, 0 is used to disable VLAN tagging)

SSID Broadcast: ☑ Enable

Security Mode: WPA-PSK

Version: ○ Auto ○ WPA-PSK ● WPA2-PSK

Encryption: ○ Auto ○ TKIP ● AES

Wireless Password: ••••••••••••••

Group Key Update Period: 0 seconds(30-8640000, 0 means no upgrade)

SSID Isolation: □ Enable

Access Control Rule: None

Rate Limit

Apply

Configure the parameters.

1) Disable the **SSID Broadcast** to hide this SSID from the customers.

2) Specify the **SSID Name**, **Security Mode** and **Wireless Password**. Let the employees manually enter the SSID name and password, and choose the security mode you set to access the network.

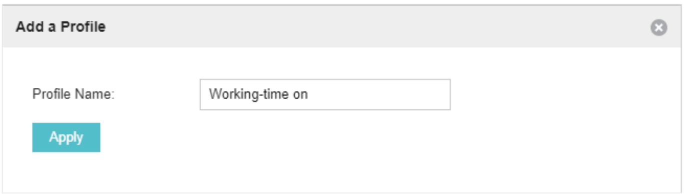
3) Click **Apply** to save the configuration.

7.2.4 Configure Scheduler

Follow the steps below to schedule the radio to operate only during the working time (from 8:00 to 22:00).

1. Open the global configuration window and go to **Wireless Control** > **Scheduler**.

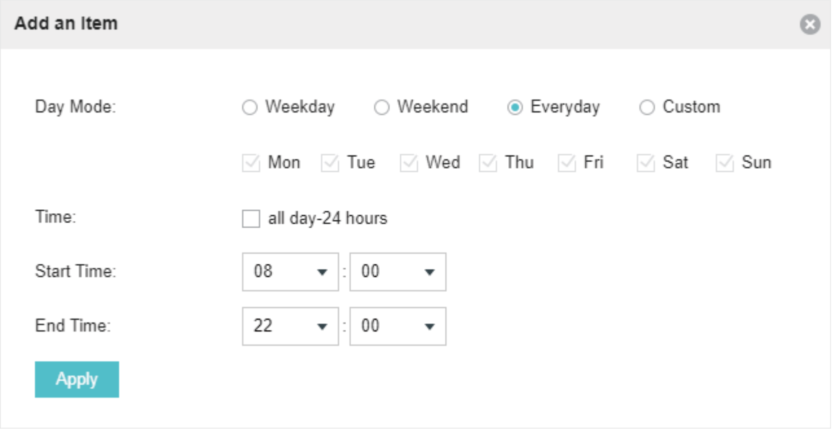
1) Add a profile.



Add a Profile

Profile Name: Working-time on

2) Add an item for the profile. The parameters are set as shown on the following screen.



Add an Item

Day Mode: ○ Weekday ○ Weekend ● Everyday ○ Custom

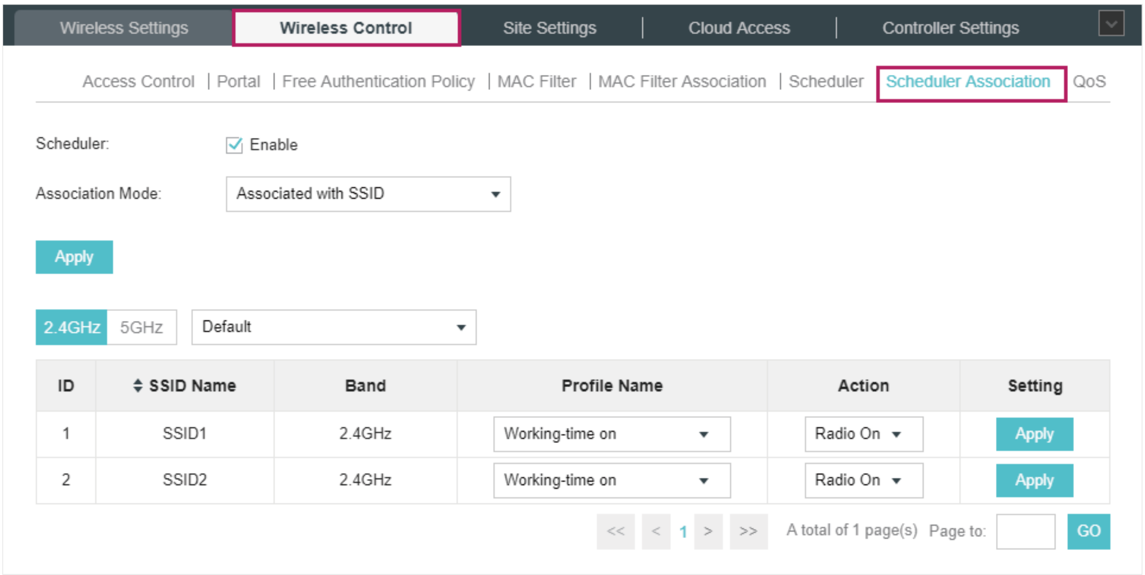
☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Time: □ all day-24 hours

Start Time: 08 : 00

End Time: 22 : 00

2. Go to **Scheduler Association** tab.


Wireless Settings
Wireless Control
Site Settings
Cloud Access
Controller Settings
Access Control | Portal | Free Authentication Policy | MAC Filter | MAC Filter Association | Scheduler
Scheduler Association
QoS
Apply
2.4GHz
5GHz
<< < 1 > >>
A total of 1 page(s) Page to:
GO

Scheduler: ☑ Enable

Association Mode: Associated with SSID

Default

ID	SSID Name	Band	Profile Name	Action	Setting
1	SSID1	2.4GHz	Working-time on	Radio On	Apply
2	SSID2	2.4GHz	Working-time on	Radio On	Apply

1) Enable the function and select **Associated with SSID**. Click **Apply**.

2) In the **Profile Name** column of both SSIDs, select the profile we just created.

3) In the **Action** column of both SSIDs, select **Radio On.**

4) Click **Apply** in the **Setting** column of both SSIDs.

5) Select **5GHz** and do the same configurations as above.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. tp-link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2018 TP-Link Technologies Co., Ltd.. All rights reserved.

FCC STATEMENT

Product Name：Omada Cloud Controller

Model Number: OC200

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: https://www.tp-link.com/us/

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.

2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

EU declaration of conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/30/EU, 2014/35/EU, 2009/125/EC and 2011/65/EU.

The original EU declaration of conformity may be found at *https://www.tp-link.com/en/ce*

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSSs. Operation is subject to the following two conditions:

1) This device may not cause interference, and
2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d’Industrie Canada applicables aux appareils radio exempts de licence. L’exploitation est autorisée aux deux conditions suivantes :

1) l’appareil ne doit pas produire de brouillage;
2) l’utilisateur de l’appareil doit accepter tout brouillage radioélectrique subi, meme si le brouillage est susceptible d’en compromettre le fonctionnement.

Industry Canada Statement

CAN ICES-3 (B)/NMB-3(B)

NCC Notice

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

BSMI Notice

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

限用物質含有情況標示聲明書

產品元件名稱	限用物質及其化學符號					
	鉛 Pb	鎘 Cd	汞 Hg	六價鉻 CrVI	多溴聯苯 PBB	多溴二苯醚 PBDE
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
備考1.″○″系指該項限用物質之百分比含量未超出百分比含量基準值。 備考2.″−″ 系指該項限用物質為排除項目。						

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

EAC

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device.
- Do not use damaged charger or USB cable to charge the device.

Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

Explanation of the symbols on the product label

Symbol	Explanation
⎓	DC voltage
⌂	Indoor use only.
🗑	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.