



# User Guide

## Omada Controller Software

1910012370 REV 2.6.0

March 2018

# CONTENTS

<b>1 Quick Start.....</b>	<b>1</b>
1.1 Determine the Network Topology .....	2
1.1.1 Management in the Same Subnet.....	2
1.1.2 Management in Different Subnets.....	3
1.2 Install Omada Controller Software .....	3
1.3 Inform the EAPs of the Controller Host's Address .....	4
1.4 Start and Log In to the Omada Controller .....	5
1.4.1 Launch Omada Controller .....	6
1.4.2 Do the Basic Configurations.....	6
1.4.3 Log In to the Management Interface.....	8
1.5 Create Sites and Adopt EAPs .....	8
1.5.1 Create Sites .....	8
1.5.2 Adopt the EAPs .....	9
1.6 Monitor and Manage the EAPs.....	10
<b>2 Monitor and Manage the Network.....</b>	<b>11</b>
2.1 Monitor the Network with the Map .....	12
2.1.1 Add a Map.....	12
2.1.2 Monitor the EAPs on the Map .....	14
2.2 View the Statistics of the Network .....	15
2.2.1 View the Client Distribution on SSID .....	15
2.2.2 Have a Quick Look at EAPs and Clients .....	15
2.2.3 View Current Usage-Top EAPs .....	16
2.2.4 View Recent Activities .....	16
2.3 Monitor and Manage the EAPs.....	17
2.3.1 Manage the EAPs in Different Status.....	17
2.3.2 View the Detailed Information of EAPs.....	18
2.3.3 Manage the EAPs in the Action Column .....	18

<b>2.4</b>	<b>Monitor and Manage Clients .....</b>	<b>19</b>
2.4.1	View the Current Information of Clients .....	20
2.4.2	Manage Clients in the Action Column.....	20
<b>2.5</b>	<b>View Clients Statistics During the Specified Period .....</b>	<b>20</b>
2.5.1	Select a Specified Period .....	21
2.5.2	View the History Information of Clients .....	21
2.5.3	Manage Clients in the Action Column.....	22
<b>2.6</b>	<b>Manage the Rogue APs List .....</b>	<b>22</b>
2.6.1	Manage the Untrusted Rogue APs List .....	22
2.6.2	Manage the Trusted Rogue APs List.....	23
<b>2.7</b>	<b>View Past Guest Authorization.....</b>	<b>23</b>
<b>2.8</b>	<b>View Logs.....</b>	<b>24</b>
<b>2.9</b>	<b>View Alerts.....</b>	<b>24</b>
<b>3</b>	<b>Configure the EAPs Globally .....</b>	<b>25</b>
<b>3.1</b>	<b>Wireless Network.....</b>	<b>26</b>
3.1.1	Add Wireless Networks .....	26
3.1.2	Configure Advanced Wireless Parameters .....	31
3.1.3	Configure Band Steering .....	32
<b>3.2</b>	<b>Access Control .....</b>	<b>33</b>
<b>3.3</b>	<b>Portal Authentication.....</b>	<b>34</b>
3.3.1	No Authentication.....	35
3.3.2	Simple Password .....	39
3.3.3	Local User.....	43
3.3.4	Voucher .....	50
3.3.5	SMS.....	58
3.3.6	Facebook.....	62
3.3.7	External RADIUS Server .....	63
3.3.8	External Portal Server .....	68
<b>3.4</b>	<b>Free Authentication Policy .....</b>	<b>69</b>

3.5	MAC Filter .....	70
3.6	Scheduler .....	72
3.7	QoS.....	73
3.8	System .....	76
3.8.1	Reboot Schedule .....	76
3.8.2	Log Setting.....	77
3.8.3	Device Account.....	78
3.8.4	Backup&Restore .....	79
3.8.5	Batch Upgrade.....	79
3.8.6	More Settings.....	80

## 4 Configure the EAPs Separately .....82

4.1	View the Information of the EAP.....	83
4.1.1	Overview .....	83
4.1.2	LAN.....	83
4.1.3	Radio.....	84
4.2	View Clients Connecting to the EAP .....	84
4.2.1	User.....	84
4.2.2	Guest .....	85
4.3	Configure the EAP .....	85
4.3.1	Basic Config.....	85
4.3.2	IP Setting.....	86
4.3.3	Radio.....	86
4.3.4	Load Balance.....	88
4.3.5	WLANs .....	88
4.3.6	Trunk Settings.....	89
4.3.7	Rogue AP Detection .....	89
4.3.8	Local LAN Port Settings.....	90
4.3.9	Forget this AP .....	90

<b>5</b>	<b>Manage the Omada Controller .....</b>	<b>91</b>
5.1	Information About the Software.....	92
5.2	User Account.....	92
5.3	Controller Settings .....	93
5.3.1	Configure Controller Hostname/IP .....	93
5.3.2	Configure Mail Server .....	94
<b>6</b>	<b>Application Example .....</b>	<b>95</b>
6.1	Basic Configuration.....	96
6.2	Advanced Settings .....	96
6.2.1	Monitor the EAPs with Map.....	96
6.2.2	Configure Portal Authentication.....	97
6.2.3	Create a SSID for the Employees.....	99
6.2.4	Configure Scheduler .....	100

# 1 Quick Start

Omada Controller is a management software for TP-Link EAP devices. With this software, you can use a web browser to centrally manage your EAP devices, such as configure EAPs in batches and conduct real-time monitoring of EAPs .

Follow the steps below to complete the basic settings of Omada Controller.

1. *Determine the Network Topology*
2. *Install Omada Controller Software*
3. *Inform the EAPs of the Controller Host's Address*
4. *Start and Log In to the Omada Controller*
5. *Create Sites and Adopt the EAPs*
6. *Monitor and Manage the EAPs*

## 1.1 Determine the Network Topology

There are two kinds of network topologies to centrally manage EAPs via Omada Controller:

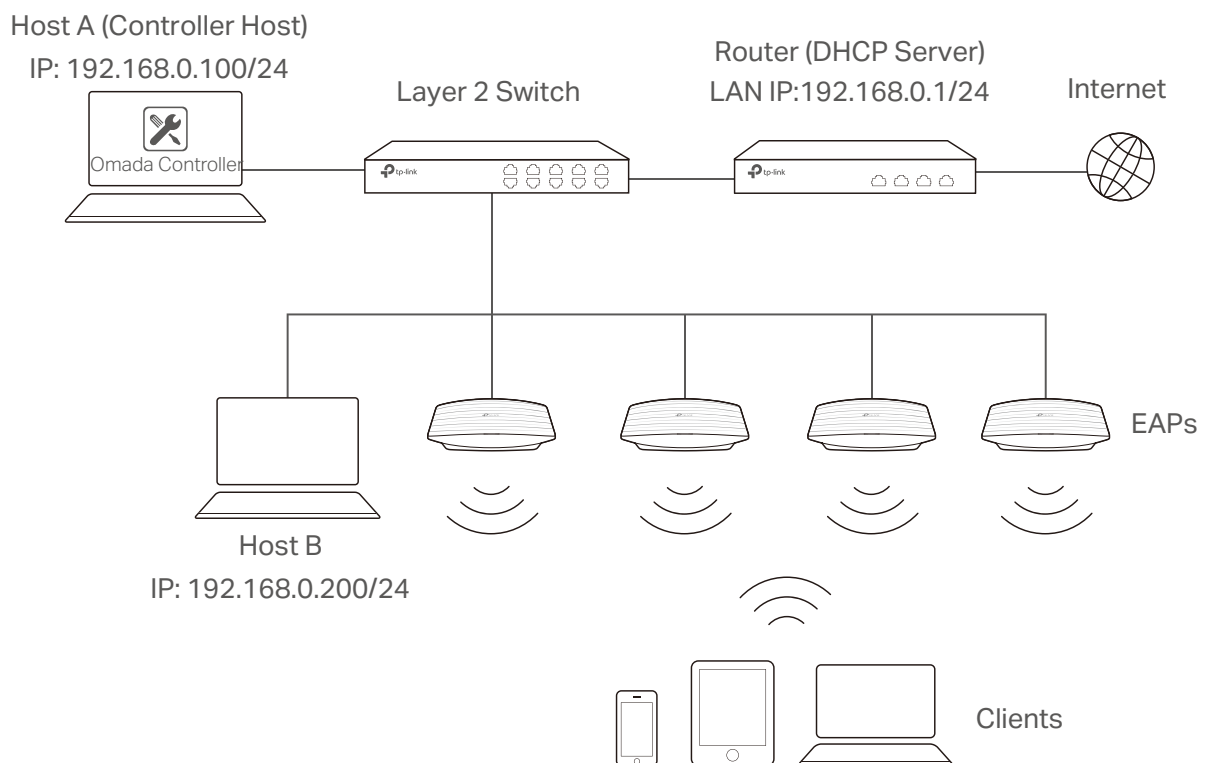
- Omada Controller and EAPs are in the same subnet.
- Omada Controller and EAPs are in different subnets.

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

### 1.1.1 Management in the Same Subnet

If your Omada Controller and EAPs are in the same subnet, refer to the following network topology.

A router acts as a DHCP server to assign IP addresses to EAPs and clients. Omada Controller should be installed on one host, which is called as Controller Host. The other hosts in the same LAN can access the Controller Host to manage the network. Taking the following topology as an example, you can enter "192.168.0.100:8043" in a web browser on Host B to visit the Omada Controller interface on Host A. It's recommended to set a static IP address to the Controller Host for the convenient login to the Omada Controller interface.



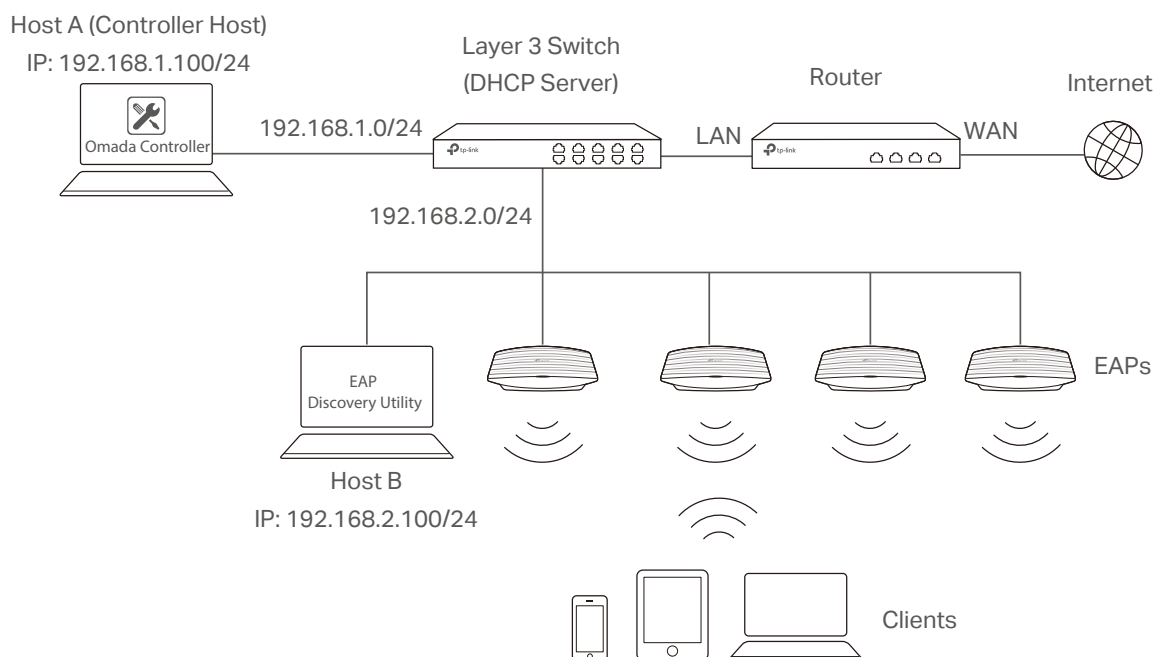
**Note:**

- Omada Controller must be running all the time when you manage the network.
- Omada Controller can be running on only one host in a LAN. When other users in the LAN try to launch Omada Controller on their own hosts, they will be redirected to the host that is already running Omada Controller.

## 1.1.2 Management in Different Subnets

If your Omada Controller and EAPs are in different subnets, refer to the following 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 and clients. The Controller Host and the EAPs are connected to the switch's different network segments. To help EAPs find the Controller Host, EAP Discover Utility should be installed on Host B which is in the same subnet with the EAPs. For how to use EAP Discovery Utility, refer to [1.3 Inform the EAPs the Controller Host's Address](#).



## 1.2 Install Omada Controller Software

Make sure your PC meets the following system requirements and then properly install the Omada Controller software.

### System Requirements

**Operating System:** Microsoft Windows 7/8/10/Server.


**Web Browser:** Mozilla Firefox 32 (or above), Google Chrome 37 (or above), Opera 24 (or above), or Microsoft Internet Explorer 11 (or above).

### Note:

We recommend that you deploy Omada Controller on a 64-bit operating system to guarantee the software stability.



## Install Omada Controller

Download the installation file of Omada Controller from the website <http://www.tp-link.com/en/download/EAP-Controller.html>. Then follow the instructions to properly install the Omada Controller software. After successful installation, a shortcut icon  of the Omada Controller will be created on your desktop.

## 1.3 Inform the EAPs of the Controller Host's Address

If your Controller Host and EAPs are in the same network segment, you can skip this section.

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

### System Requirements

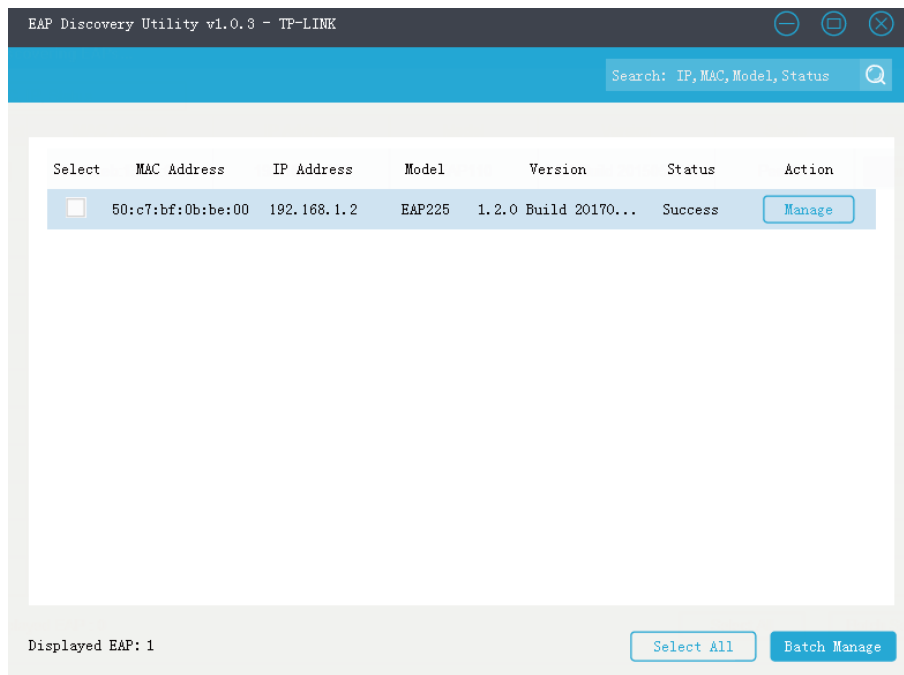
Windows 7/8/10/Server

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

### Install and Use EAP Discovery Utility

Follow the steps below to install EAP Discovery Utility and use it to inform the EAPs of the Controller Host's IP address:

1. Download the installation file from the website [http://www.tp-link.com/en/download/EAP-Controller.html#EAP\\_Discovery\\_Tool](http://www.tp-link.com/en/download/EAP-Controller.html#EAP_Discovery_Tool). Then follow the instructions to properly install EAP Discovery Utility.
2. Open the EAP Discovery Utility and the following window will pop up. This window shows the information of all EAPs in the same LAN.



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

Device Information
×

Status: Success

Model: EAP225

IP Address: 192.168.1.2

MAC Address: 50:c7:bf:0b:be:00

Controller Hostname/IP:

Username:

Password:

4. Enter the hostname or IP address of the Controller Host.


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

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

## 1.4 Start and Log In to the Omada Controller

Launch Omada Controller and follow the instructions to complete the basic configurations, and then you can log in to the management interface.

## 1.4.1 Launch Omada Controller

Double click the icon  and the following window will pop up. You can click **Hide** to hide this window but do not close it. After a while, your web browser will automatically open.



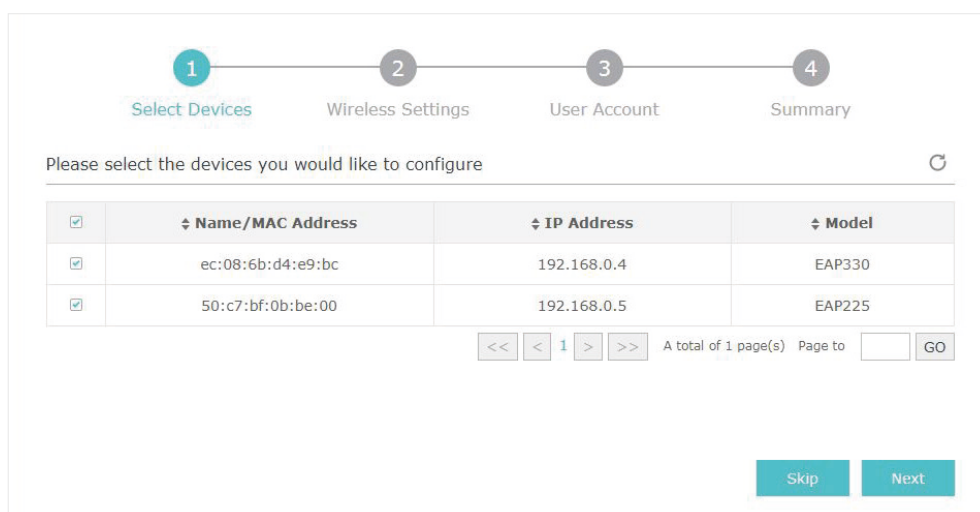
### Note:

- If your browser does not open automatically, click **Launch a Browser to Manage Wireless Network**. You can also launch a web browser and enter `http://127.0.0.1:8088` in the address bar.
- If your web browser opens but prompts a problem with the website's security certificate, click **Continue**.
- Only one Omada Controller can run in a LAN. If an Omada Controller has already been running on a host that is in your LAN, you will be redirected to the Omada Controller interface on that host.

## 1.4.2 Do the Basic Configurations

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

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

A screenshot of the Omada Controller setup wizard, step 1: "Select Devices". At the top, there's a progress bar with four steps: 1 (Select Devices), 2 (Wireless Settings), 3 (User Account), and 4 (Summary). Below the progress bar, the text says "Please select the devices you would like to configure". There's a table with three columns: "Name/MAC Address", "IP Address", and "Model". Two devices are listed, both with checkboxes in the first column. The first device has MAC address "ec:08:6b:d4:e9:bc", IP "192.168.0.4", and model "EAP330". The second device has MAC address "50:c7:bf:0b:be:00", IP "192.168.0.5", and model "EAP225". Below the table is a pagination control showing "A total of 1 page(s)" and "Page to" with a "GO" button. At the bottom right are "Skip" and "Next" buttons.

<input checked="" type="checkbox"/>	Name/MAC Address	IP Address	Model
<input checked="" type="checkbox"/>	ec:08:6b:d4:e9:bc	192.168.0.4	EAP330
<input checked="" type="checkbox"/>	50:c7:bf:0b:be:00	192.168.0.5	EAP225

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

1 Select Devices 2 **Wireless Settings** 3 User Account 4 Summary

Create a wireless network

SSID:  (1-32 characters)

Password:  (WPA2-PSK)

Back Next

3. Specify a username and password to create an administrator account. Specify the email address to receive the notification emails and reset your password if necessary. Click **Next**.

1 Select Devices 2 Wireless Settings 3 **User Account** 4 Summary

Set up your login account for the EAP Controller

Username:  (4-32 characters)

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

Confirm Password:

Email Address:  (You can reset your password with this email)

Back Next

**Note:**

After logging into Omada Controller, set a mail server so that you can receive notification emails and reset your password in case that you forget the password. Please refer to [Configure Mail Server](#).

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

1 Select Devices 2 Wireless Settings 3 User Account 4 **Summary**

Please confirm your information

SSID Name: SSID1

Password: 12345678

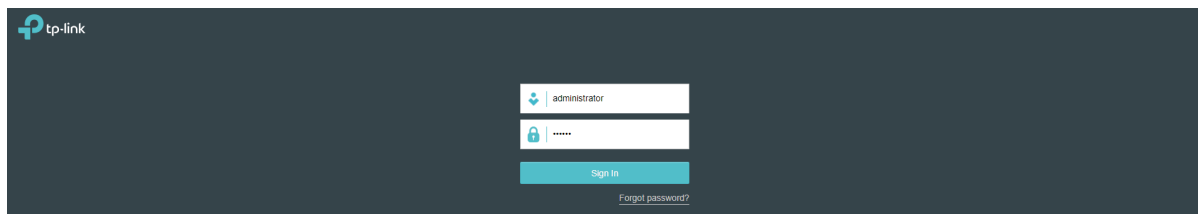
Admin Name: administrator

Email Address: administrator@tp-link.com

Back Finish

### 1.4.3 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.



#### Note:

In addition to the Controller Host, other hosts in the same LAN can also manage EAP devices via remote access to the Controller Host. For example, if the IP address of the Controller Host is 192.168.0.100 and Omada Controller is running normally on this host, you can enter **https://192.168.0.100:8043/login**, or **https://192.168.0.100:8043**, or **http://192.168.0.100:8088** in the web browser of other hosts in the same LAN to log in to the Omada Controller and manage EAP devices.

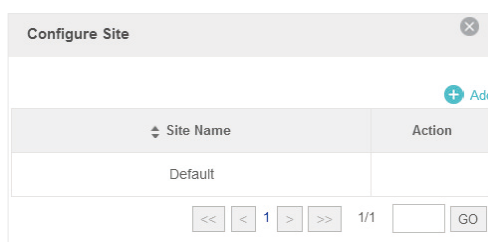
## 1.5 Create Sites and Adopt EAPs

Omada Controller 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 different 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.

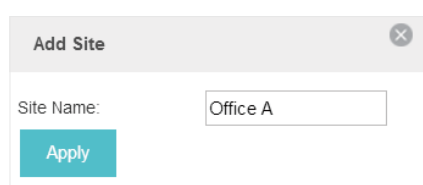
### 1.5.1 Create Sites

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.



2. Click **+ Add** and set a name for the site.



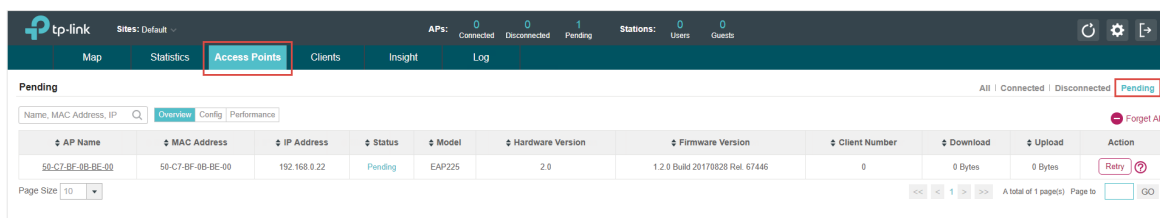
3. Click **Apply** to create the site.

## 1.5.2 Adopt the EAPs

Omada Controller 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 Omada Controller. To manage the EAPs, you need to adopt them. In the quick setup process, Omada Controller 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, Omada Controller cannot automatically adopt the them, and you need to refer to the following steps to adopt them manually.

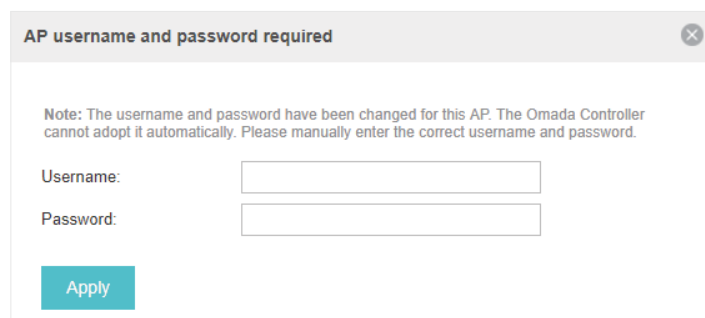
To ensure that all EAPs are adopted, follow the steps below:

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
58-C7-BF-8B-BE-00	58-C7-BF-8B-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:

**Apply**

### Tips:

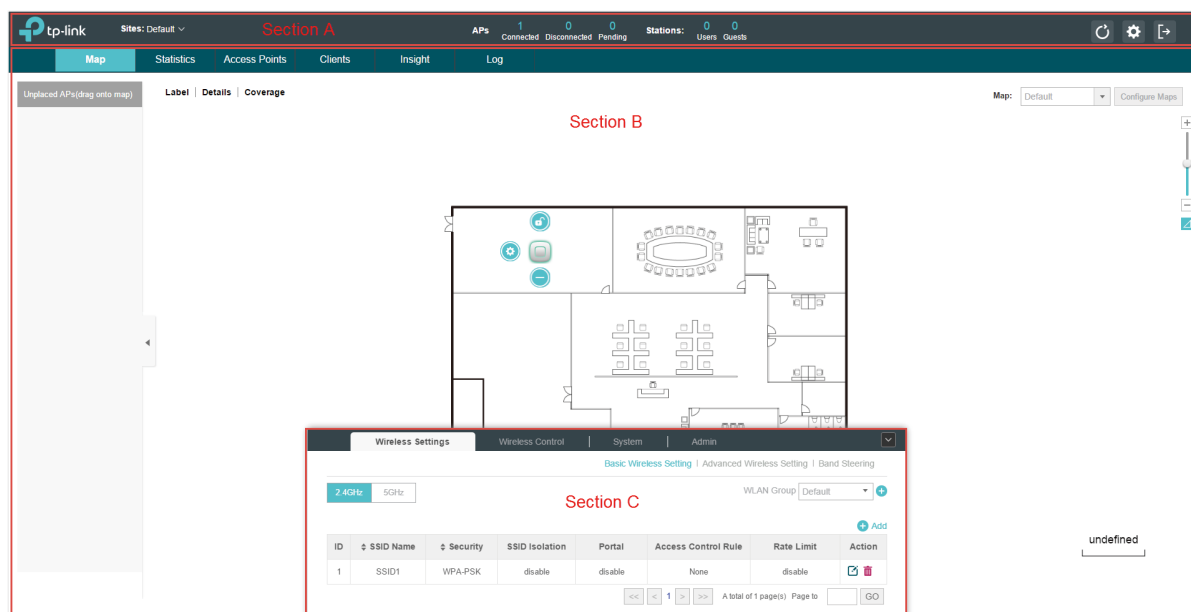
- If you have a new discovered EAP, you can click the **Adopt** button in the **Action** column to adopt the EAP. Omada Controller will automatically adopt the EAP using the default username and password (both are admin).
  - If you have multiple new discovered EAPs, and all of them have the default 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 Controller'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 Omada Controller's management interface. The management interface is divided into three sections as the following figure shows.



### 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**

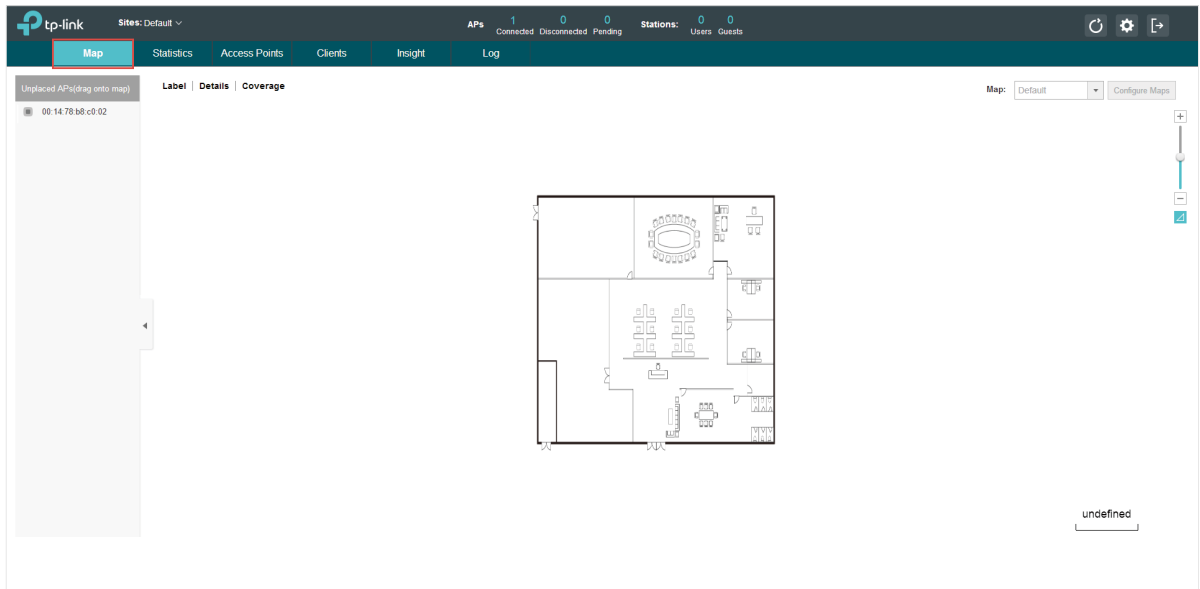
With Omada Controller you can monitor the EAP devices and centrally manage your wireless network. This chapter includes the following sections:

- *Monitor the Network with the Map*
- *View the Statistics of the Network*
- *Monitor and Manage the EAPs*
- *Monitor and Manage Clients*
- *View Clients Statistics during the Specified Period*
- *Manage the Rogue APs List*
- *View Past Guest Authorization*
- *View Logs*
- *View Alerts*



## 2.1 Monitor the Network with the Map

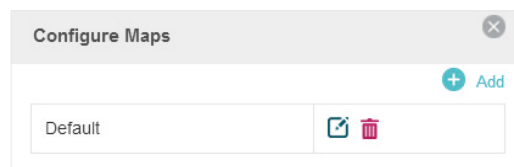
You can upload your local map images and monitor the status and coverage range of each EAP with the map. When you initially launch Omada Controller, a default map is displayed as the following figure shows. Follow the instructions below to add your own map and manage the EAPs via the map.



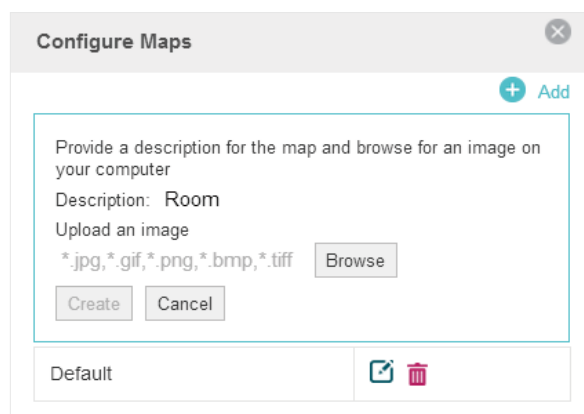
### 2.1.1 Add a Map

Prepare a map image in .jpg, .gif, or .png format. And then follow the steps below to add the map to the Omada Controller.

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




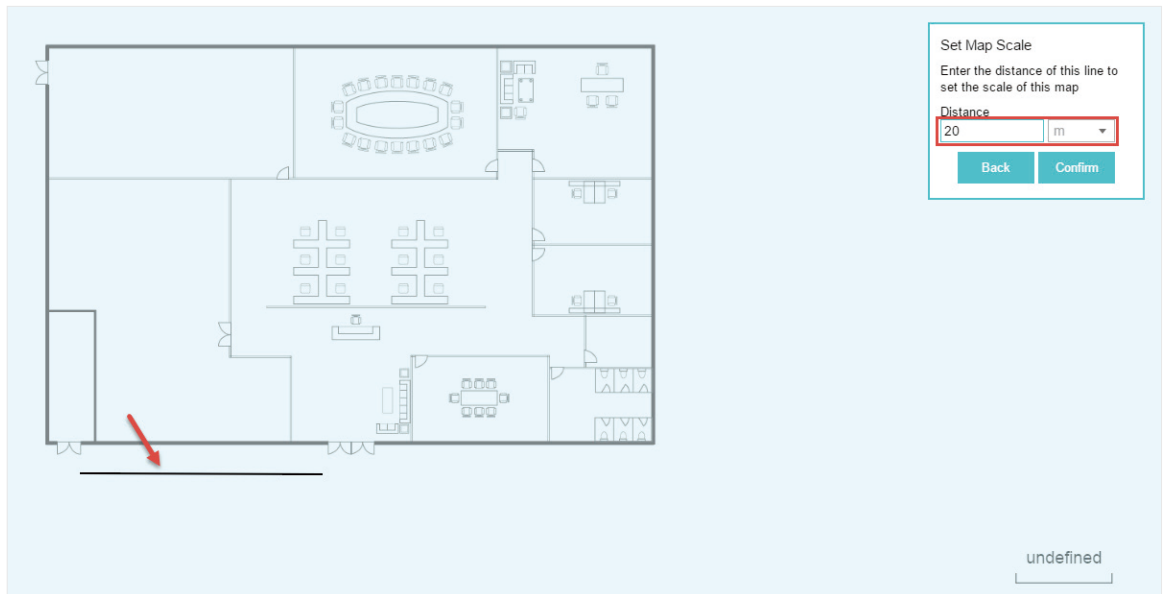
2. Enter the map description, select your map image, and click **Create**.



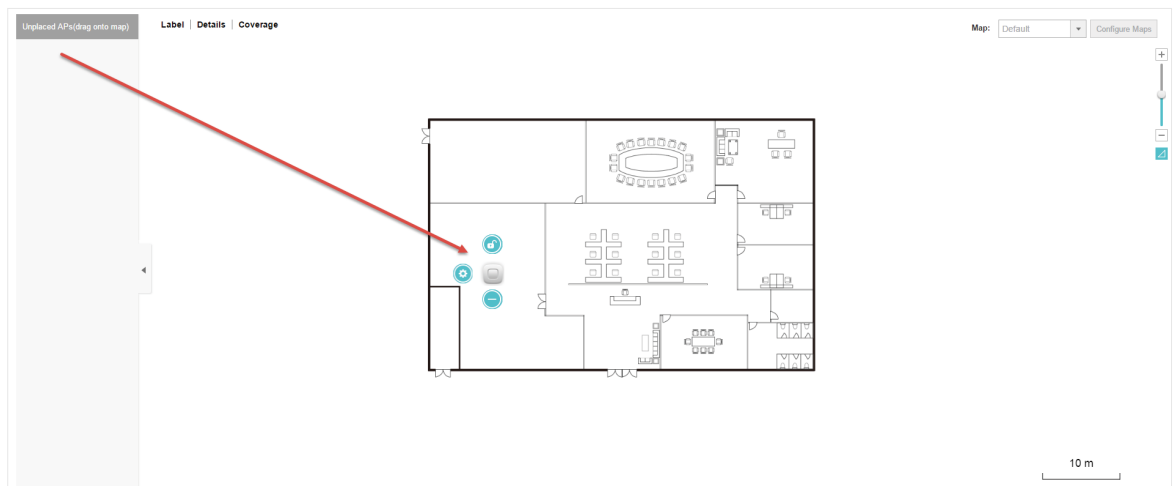
3. Select your local map from the drop-down list on the upper right corner of map area.

Map:  ▼

- Click . Draw a line on the map and enter the distance the line represents. Then the Omada Controller will compute and generate the map scale automatically based on your configuration.






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



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 <a href="#">Configure the EAPs Separately</a> .
	Remove the selected EAP back into the Unplaced APs list.

## 2.1.2 Monitor the EAPs on the Map

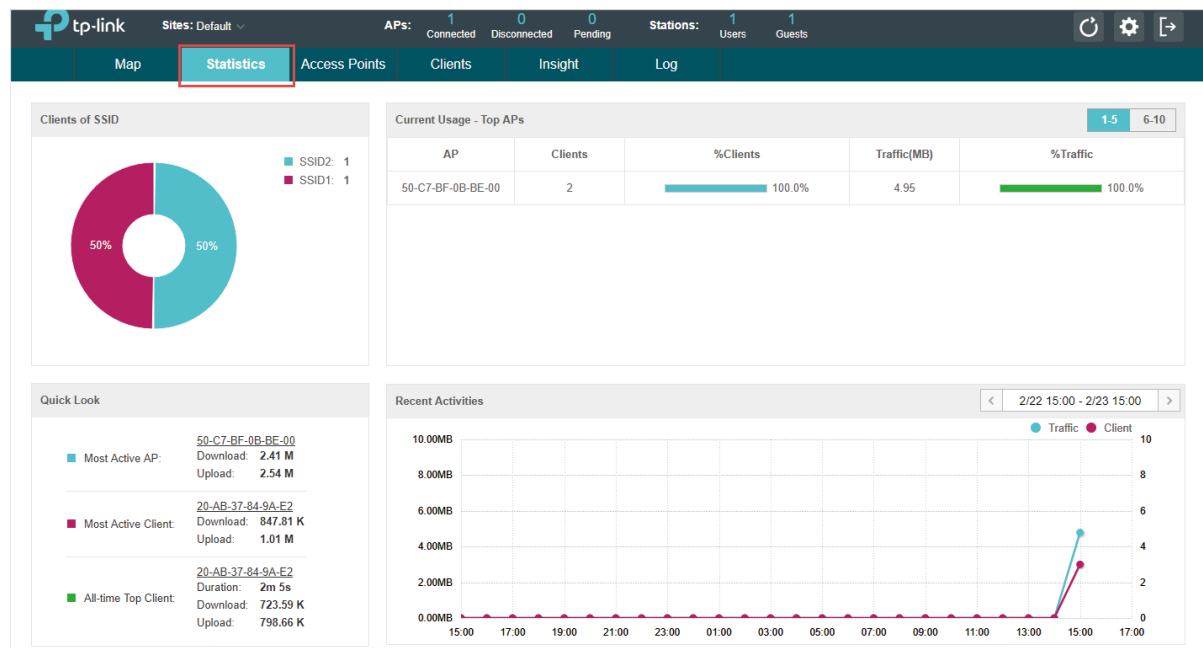
Click any of the following options to display EAP Label, Details, and Coverage on the map.

**Label** | **Details** | **Coverage**

<b>Label</b>	Display the EAP's name. The default name is the MAC address of the EAP.
<b>Details</b>	Display the EAP's name, MAC address, IP address, transmitting/receiving channel, number of connected users, and number of connected guests.
<b>Coverage</b>	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.

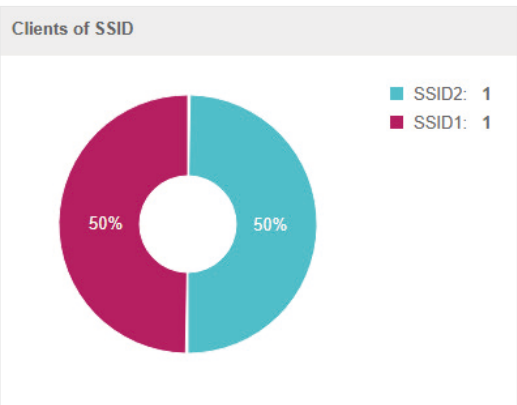
## 2.2 View the Statistics of the Network

Omada Controller 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.



### 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:	<a href="#">50-C7-BF-0B-BE-00</a> Download: <b>2.41 M</b> Upload: <b>2.54 M</b>
■ Most Active Client:	<a href="#">20-AB-37-84-9A-E2</a> Download: <b>847.81 K</b> Upload: <b>1.01 M</b>
■ All-time Top Client:	<a href="#">20-AB-37-84-9A-E2</a> Duration: <b>2m 5s</b> Download: <b>723.59 K</b> Upload: <b>798.66 K</b>

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				
				1-5 6-10
AP	Clients	%Clients	Traffic(MB)	%Traffic
50-C7-BF-0B-BE-00	2	<div></div> 100.0%	4.95	<div></div> 100.0%

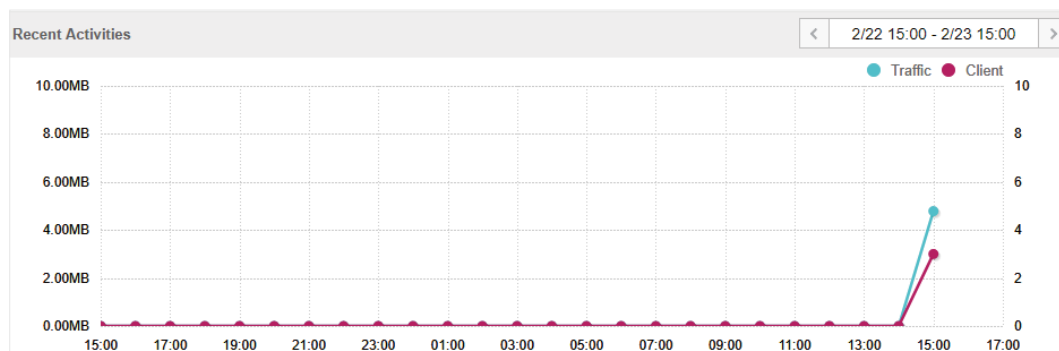
Clients	The amount of clients connected to this EAP.
%Clients	The proportion of current connected clients to the Top EAPs' total client amount.
Traffic (MB)	The total amount of data transmitted by this EAP, which equals the sum of the transmission traffic of all the current clients that connect to the 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 15 o'clock, the traffic is about 5MB and there is 3 clients connected to the AP.



## 2.3 Monitor and Manage the EAPs

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

The screenshot shows the 'Access Points' page in the Omada Controller interface. The top navigation bar includes 'Map', 'Statistics', 'Access Points' (highlighted), 'Clients', 'Insight', and 'Log'. Below the navigation bar, there are tabs for 'All', 'Connected', 'Disconnected', and 'Pending'. The 'All' tab is selected, showing a table of access points. The table has columns for AP Name, MAC Address, IP Address, Status, Model, Hardware Version, Firmware Version, Client Number, Download, Upload, and Action. One access point is listed with status 'Connected'.

AP Name	MAC Address	IP Address	Status	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
58-C7-BF-0B-BE-00	50-C7-BF-0B-BE-00	192.168.0.254	Connected	EAP225	2.0	1.2.0 Build 20170828 Rel. 67446	0	0 Bytes	0 Bytes	[Icons]

### 2.3.1 Manage the EAPs in Different Status

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

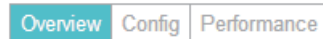
[All](#) | [Connected](#) | [Disconnected](#) | [Pending](#)

All	Displays the information of all EAPs in different status.
Pending	<p>Displays the pending EAPs.</p> <p>All the EAPs are in pending status by default when first discovered by Omada Controller, and only after they are adopted and connected, you can manage them. To adopt pending EAPs, refer to <a href="#">Adopt EAPs</a>.</p>
Connected	<p>Displays the connected EAPs.</p> <p>Only connected EAPs can be managed. After you adopt a pending EAP, its status will become provisioning and then connected. A connected EAP will turn into a pending one after you <b>forget</b> it. You can refer to <a href="#">Forget this AP</a> to forget an EAP or click <b>Forget All</b> on the page to forget all the connected EAPs.</p>

Disconnected	<p>Displays the disconnected EAPs.</p> <p>If a connected or pending EAP powers off, it will be disconnected. When a disconnected EAP is reset to factory defaults or forgot, it will turn into a pending one again. You can refer to <a href="#">Forget this AP</a> to forget a EAP or click <b>Forget All</b> on the page to forget all the disconnected EAPs.</p>
--------------	---

## 2.3.2 View the Detailed Information of EAPs

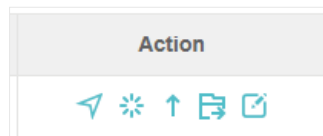
You can click **Overview**, **Config** or **Performance** tab to view different detailed information of EAPs.



Overview	Displays the EAP's name/MAC address, IP address, status, model, software version, number of connected clients and download/upload bytes.
Config	Displays the EAP's name/MAC address, IP address, status, model, software 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, software version, number of connected 2G clients and 5G clients, TX(Downloaded Traffic), RX(Uploaded Traffic), TX 2G and TX 5G.

## 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.



	Locate the EAP in the map.
	Reboot the EAP.
	<p>Upgrade the EAP.</p> <p>Click <b>Browse</b> to locate and choose the upgrade file in your computer, then click <b>Upgrade</b> to install the latest EAP firmware. The Status will appear as <b>Upgrading</b> until the process is complete and the EAP reconnects to the Omada Controller.</p> <div data-bbox="481 1650 1026 1834"> </div>



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(00:14:78:c0:a8:7b)

Move to Site: Default

Apply

Default  
Office  
Rest Room



Configure the EAP.

For detailed instructions about how to configure the EAP on this window, refer to [Configure the EAPs Separately](#).

50-C7-BF-0B-BE-00 Connected

Details | User | Guest | Configuration

Overview

MAC Address: 50-C7-BF-0B-BE-00  
IP Address: 192.168.0.254  
Model: EAP225  
Firmware Version: 1.2.0 Build 20170828 Rel. 67446  
CPU: 2%  
Memory: 48%  
Uptime: 0 days 13:31:25

LAN

Radio

#### Note:

- Only managed EAPs can be rebooted or upgraded.
- If you want to log in to the EAP's own management interface, you need to forget the EAP first.

## 2.4 Monitor and Manage Clients

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

tp-link Sites: Default

APs: 1 Connected 0 Disconnected 0 Pending Stations: 1 Users 0 Guests

Map Statistics Access Points **Clients** Insight Log

All Clients All Clients | Users | Guests

MAC, Name, IP, AP, SSID

Hostname	MAC Address	IP Address	Access Point	SSID	User/Guest	2.4GHz/5GHz	Download	Upload	Rate (Mbps)	Active Time	Signal	Action
Unknown	20-AB-37-84-9A-E2	192.168.0.103	50-C7-BF-0B-BE-00	SSID1	User	5GHz	330 Bytes	59.36 K	6.0	1m 28s		

Page Size 10

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



## 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](#).

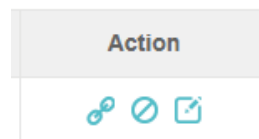
You can click the following tabs to respectively view the detailed information of users and guests.





[All Clients](#) | [Users](#) | [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:



	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 <b>Apply</b> .
	If the client is a Guest, you can click this icon to cancel the authorization for it.

Unknown (20-AB-37-84-9A-E2) ✕

[Rate Limit](#) | [Connection History](#)

Download Limit

Kbps (0-10240000. 0 means no limit)

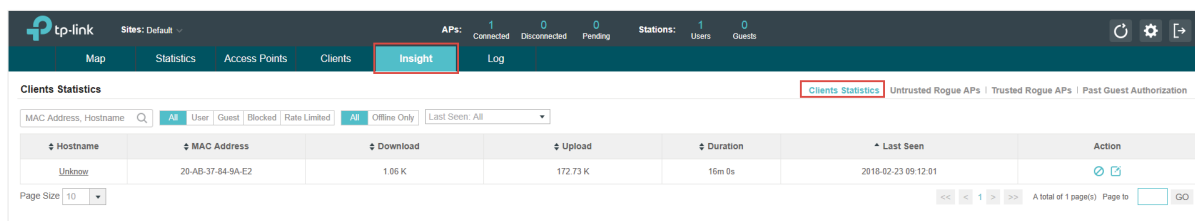
Upload Limit

Kbps (0-10240000. 0 means no limit)

Apply

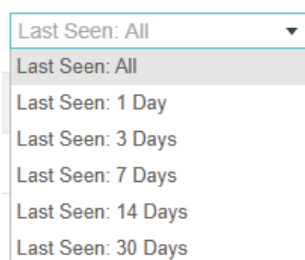
## 2.5 View Clients Statistics During the Specified Period

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



## 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 <a href="#">Portal Authentication</a> .
Guest	The page displays the history information of Guests. Guests are the clients connected to the EAP wireless network with the <a href="#">Portal Authentication</a> .
Blocked	The page displays the clients that have been blocked.



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.

## 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 Omada Controller 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.

The screenshot shows the TP-Link Omada Controller interface. The top navigation bar includes 'Map', 'Statistics', 'Access Points', 'Clients', 'Insight' (highlighted with a red box), and 'Log'. Below the navigation bar, the 'Untrusted Rogue APs' section is active, with a red box around the 'Untrusted Rogue APs' tab. The table below lists detected rogue access points with columns for MAC, SSID, Band, Channel, Security, Beacon, Signal, Last Seen, and Action. The 'Action' column contains icons for moving to the trusted list and deleting the record. A 'Delete All' button is also present.

MAC	SSID	Band	Channel	Security	Beacon	Signal	Last Seen	Action
B6-4E-26-CA-64-41	deco wifi_Guest	2.4G	7	OFF	100	-46	2018-02-23 15:49:46	
30-B5-C2-BD-04-6E	TP-Link_Outdoor_BD046E	2.4G	6	OFF	100	-62	2018-02-23 15:49:46	
C4-6E-1F-C7-4F-AE	Neostrada	2.4G	10	ON	100	-49	2018-02-23 15:49:46	
C8-E7-D8-60-1C-86	mercusys	2.4G	11	ON	100	-25	2018-02-23 15:49:46	
BA-4E-26-CA-64-1F		5G	44	ON	100	-45	2018-02-23 15:49:46	
70-4F-57-BF-31-9C	TP-Link_319A_5G	5G	44	ON	100	-64	2018-02-23 15:49:46	
7C-11-CB-F3-22-D4		5G	161	OFF	100	-101	2018-02-23 15:49:46	
B0-95-8E-42-6B-F6	TP-LINK_6BF6	2.4G	1	ON	100	-57	2018-02-23 15:49:46	
60-E3-27-29-D9-0F	server2016	5G	36	ON	100	-42	2018-02-23 15:49:46	
D4-6E-0E-AE-FE-D8	1452855	2.4G	10	ON	100	-13	2018-02-23 15:49:46	

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 records.

## 2.6.2 Manage the Trusted Rogue APs List

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

Trusted Rogue APs

MAC	SSID	Band	Channel	Security	Last Seen	Action
B6-4E-26-CA-64-41	deco wifi_Guest	2.4G	7	OFF	2018-02-23 15:51:48	
C4-6E-1F-C7-4F-AE	Neostrada	2.4G	10	ON	2018-02-23 15:51:48	

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 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

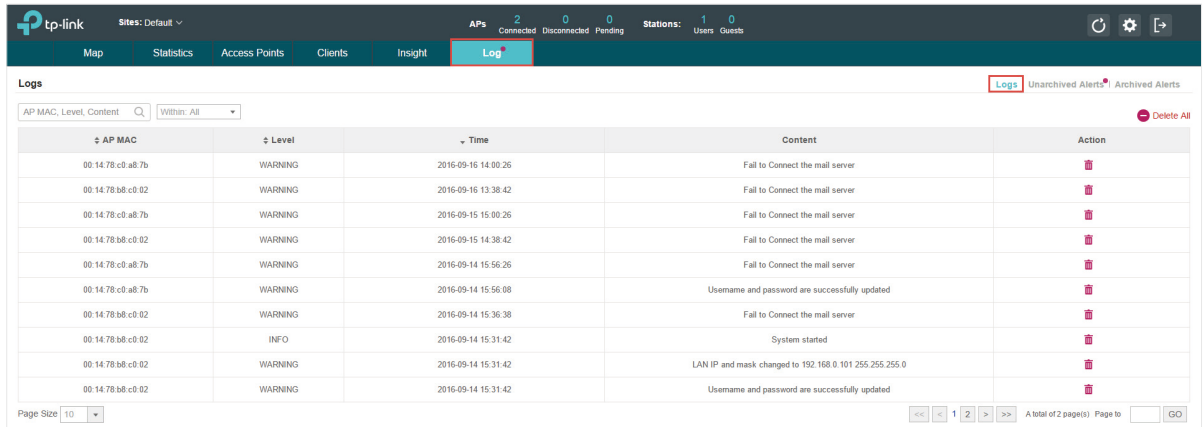
The Past Guest Authorization page displays the details about all the clients that accessed the network during a certain time period. You can select a period in the drop-down list.

Past Guest Authorization

MAC Address	SSID	Radio	Authorized By	Authorized Start Time	Download	Upload
20-AB-37-84-9A-E2	SSID1	5GHz	No Authentication	2018-02-23 15:45:24	5.83 M	3.06 M
20-AB-37-84-9A-E2	SSID1	5GHz	No Authentication	2018-02-23 15:40:35	723.51 K	789.80 K

## 2.8 View Logs

The logs of Omada Controller 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.

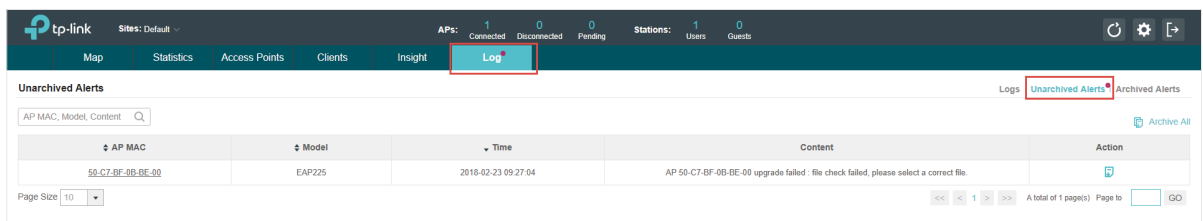


TP-Link Omada Controller Logs page. The page displays a table of logs with the following columns: AP MAC, Level, Time, Content, and Action. The 'Log' tab is selected in the top navigation bar. The table contains several entries, mostly 'WARNING' and 'INFO' level logs related to mail server connections and system updates.

AP MAC	Level	Time	Content	Action
00:14:78:c0:a8:7b	WARNING	2016-09-16 14:00:26	Fail to Connect the mail server	
00:14:78:b8:c0:02	WARNING	2016-09-16 13:38:42	Fail to Connect the mail server	
00:14:78:c0:a8:7b	WARNING	2016-09-15 15:00:26	Fail to Connect the mail server	
00:14:78:b8:c0:02	WARNING	2016-09-15 14:38:42	Fail to Connect the mail server	
00:14:78:c0:a8:7b	WARNING	2016-09-14 15:56:26	Fail to Connect the mail server	
00:14:78:c0:a8:7b	WARNING	2016-09-14 15:56:08	Username and password are successfully updated	
00:14:78:b8:c0:02	WARNING	2016-09-14 15:36:38	Fail to Connect the mail server	
00:14:78:b8:c0:02	INFO	2016-09-14 15:31:42	System started	
00:14:78:b8:c0:02	WARNING	2016-09-14 15:31:42	LAN IP and mask changed to 192.168.0.101 255.255.255.0	
00:14:78:b8:c0:02	WARNING	2016-09-14 15:31:42	Username and password are successfully updated	

## 2.9 View Alerts

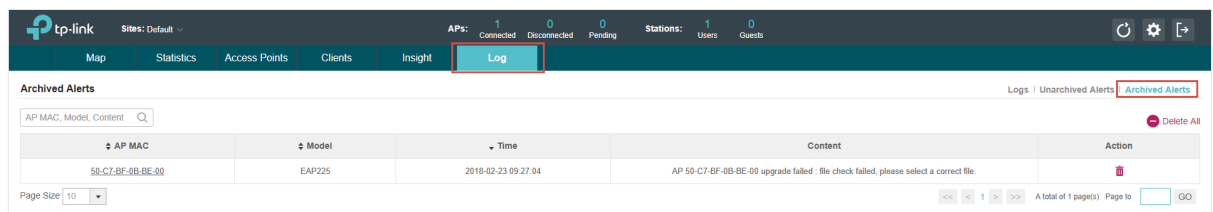
You can see the status change of your EAPs on the **Unarchived Alerts** page. You can click or **Archive All** to move unarchived alerts to the Archived Alerts page.



TP-Link Omada Controller Unarchived Alerts page. The page displays a table of unarchived alerts with the following columns: AP MAC, Model, Time, Content, and Action. The 'Log' tab is selected in the top navigation bar. The table contains one entry: AP 50-C7-BF-0B-BE-00, EAP225, 2018-02-23 09:27:04, AP 50-C7-BF-0B-BE-00 upgrade failed: file check failed, please select a correct file.

AP MAC	Model	Time	Content	Action
50-C7-BF-0B-BE-00	EAP225	2018-02-23 09:27:04	AP 50-C7-BF-0B-BE-00 upgrade failed: file check failed, please select a correct file.	

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



TP-Link Omada Controller Archived Alerts page. The page displays a table of archived alerts with the following columns: AP MAC, Model, Time, Content, and Action. The 'Log' tab is selected in the top navigation bar. The table contains one entry: AP 50-C7-BF-0B-BE-00, EAP225, 2018-02-23 09:27:04, AP 50-C7-BF-0B-BE-00 upgrade failed: file check failed, please select a correct file.

AP MAC	Model	Time	Content	Action
50-C7-BF-0B-BE-00	EAP225	2018-02-23 09:27:04	AP 50-C7-BF-0B-BE-00 upgrade failed: file check failed, please select a correct file.	

## 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 4 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*
- *System*

## 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**.

The screenshot shows the 'Basic Wireless Setting' page. At the top, there are tabs for 'Wireless Settings', 'Wireless Control', 'System', and 'Admin'. The 'Wireless Settings' tab is active. Below the tabs, there are sub-tabs for 'Basic Wireless Setting', 'Advanced Wireless Setting', and 'Band Steering'. The 'Basic Wireless Setting' sub-tab is active. On the left, there are two buttons for '2.4GHz' and '5GHz'. On the right, there is a 'WLAN Group' dropdown menu set to 'Default' with a '+' icon to its right. Below these, there is a table with the following columns: ID, SSID Name, Security, SSID Isolation, Portal, Access Control Rule, Rate Limit, and Action. The table contains one row with ID '1', SSID Name 'SSID1', Security 'WPA-PSK', SSID Isolation 'disable', Portal 'disable', Access Control Rule 'None', and Rate Limit 'disable'. To the right of the table is a '+ Add' button. At the bottom of the table, there are pagination controls showing '<<' '<' '1' '>' '>>' and a note 'A total of 1 page(s) Page to' followed by a 'GO' button.

2. Select a band frequency **2.4GHz** **5GHz** and click **+** at the right of **WLAN Group** **Default** to add a WLAN group. 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**.

The screenshot shows a 'WLAN Group' configuration dialog box. It has a title bar with a close button. Inside, there is a 'Name' label and a text input field containing 'Group1'. Below the input field is an 'Apply' button.

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:
(0-4094, 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:
seconds(30-8640000,0 means no upgrade).

SSID Isolation:
☐ Enable

Access Control Rule:
None

Rate Limit

Apply

SSID Name	Enter an SSID name contains up to 32 characters.
Wireless Vlan ID	<p>Set a VLAN ID for the wireless network. Wireless networks with the same VLAN ID are grouped to a VLAN.</p> <p>The value ranges from 0 to 4094. 0 means VLAN function is disabled.</p>
SSID Broadcast	<p>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.</p> <p>Enabled by default.</p>
Security Mode	<p>Select the security mode of the wireless network.</p> <p><b>None:</b> The hosts can access the wireless network without authentication.</p> <p><b>WEP/WPA-Enterprise/WPA-PSK:</b> 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.</p>
Portal	<p>With the option enabled, the configurations in <a href="#">Portal</a> will be applied. Portal provides authentication service for the clients who just need temporary access to the wireless network, such as the customers in shopping mall and restaurant.</p> <p>Disabled by default.</p>
SSID Isolation	<p>With the option enabled, the devices connected in the same SSID of the same AP cannot communicate with each other.</p> <p>Disabled by default.</p>
Access Control	Select an Access Control rule for this SSID. For more information, refer to <a href="#">Access Control</a> .



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:	<input type="text" value="WEP"/>
Type:	<input checked="" type="radio"/> Auto <input type="radio"/> Open System <input type="radio"/> Shared Key
Key Selected:	<input type="text" value="Key1"/>
WEP Key Format:	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal
Key Type:	<input checked="" type="radio"/> 64Bit <input type="radio"/> 128Bit <input type="radio"/> 152Bit
Key Value:	<input type="text" value="weppw"/>

Type	Select the authentication type for WEP.  <b>Auto:</b> The Omada Controller can select Open System or Shared Key automatically based on the wireless station's capability and request.  <b>Open System:</b> Clients can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission.  <b>Shared Key:</b> 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 <b>ASCII</b> or <b>Hexadecima</b> as the WEP key format.  <b>ASCII:</b> ASCII format stands for any combination of keyboard characters of the specified length.  <b>Hexadecimal:</b> 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.  <b>64Bit:</b> Enter 10 hexadecimal digits or 5 ASCII characters.  <b>128Bit:</b> Enter 26 hexadecimal digits or 13 ASCII characters.  <b>152Bit:</b> 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:	<input type="radio"/> Auto <input type="radio"/> WPA <input checked="" type="radio"/> WPA2	
Encryption:	<input type="radio"/> Auto <input type="radio"/> TKIP <input checked="" type="radio"/> AES	
RADIUS Server IP:	<input type="text" value="0.0.0.0"/>	
RADIUS Port:	<input type="text" value="0"/>	(1-65535, 0 means default port 1812.)
RADIUS Password:	<input type="text"/>	
Group Key Update Period:	<input type="text" value="0"/>	seconds(30-8640000, 0 means no upgrade).

Version	Select the version of WPA-Enterprise. <b>Auto:</b> The EAP will automatically choose the version used by each client device. <b>WPA/WPA2:</b> Two versions of Wi-Fi Protected Access.
Encryption	Select the Encryption type. <b>Auto:</b> The default setting is Auto and the EAP will select TKIP or AES automatically based on the client device's request. <b>TKIP:</b> 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, 802.11ac 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. <b>AES:</b> 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:	<div>WPA-PSK</div>	
Version:	<div><input type="radio"/> Auto <input type="radio"/> WPA-PSK <input checked="" type="radio"/> WPA2-PSK</div>	
Encryption:	<div><input type="radio"/> Auto <input type="radio"/> TKIP <input checked="" type="radio"/> AES</div>	
Wireless Password:	<div></div>	
Group Key Update Period:	<div>0</div>	seconds(30-8640000,0 means no upgrade).

Version	<p>Select the version of WPA-PSK.</p> <p><b>Auto:</b> The EAP will automatically choose the version for each client device.</p> <p><b>WPA-PSK:</b> Pre-shared key of WPA.</p> <p><b>WPA2-PSK:</b> Pre-shared key of WPA2.</p>
Encryption	<p>Select the Encryption type.</p> <p><b>Auto:</b> The default setting is Auto and the EAP will select TKIP or AES automatically based on the client request.</p> <p><b>TKIP:</b> 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, 802.11ac 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.</p> <p><b>AES:</b> Advanced Encryption Standard. We recommend you select AES as the encryption type for it is more secure than TKIP.</p>
Wireless Password	<p>Configure the wireless password with ASCII or Hexadecimal characters.</p> <p>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).</p>
Group Key Update Period	<p>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.</p>

7. Enable **Rate Limit** for the clients to guarantee the network balance. Enter the value for **Download Limit** and **Upload Limit**. 0 means unlimited.

Rate Limit		
Enable:	<input type="checkbox"/>	
Download Limit:	<div></div>	(Kbps, 0-10240000, 0 means unlimited)
Upload Limit:	<div></div>	(Kbps, 0-10240000, 0 means unlimited)
<div>Apply</div>		

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 **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**.

The screenshot shows the 'Advanced Wireless Setting' configuration page. At the top, there are tabs for 'Wireless Settings', 'Wireless Control', 'System', and 'Admin'. Under 'Wireless Settings', there are sub-tabs for 'Basic Wireless Setting', 'Advanced Wireless Setting' (which is highlighted with a red box), and 'Band Steering'. Below the sub-tabs, there are two buttons for '2.4GHz' and '5GHz'. The '2.4GHz' button is selected. The configuration parameters are as follows:

Parameter	Value	Range/Unit
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:	<input type="checkbox"/> Enable	

An 'Apply' button is located at the bottom left of the configuration area.

2. Select the band frequency **2.4GHz** **5GHz**.

3. 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.

<b>Fragmentation Threshold</b>	<p>The fragmentation function can limit the size of packets transmitted over the network. If a packet exceeds the <b>Fragmentation Threshold</b>, the fragmentation function is activated and the packet will be fragmented into several packets.</p> <p>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.</p>
<b>Airtime Fairness</b>	<p>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.</p>

4. 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 2.4 GHz band. However, if too many client devices are connected to an EAP on the 2.4 GHz band, the efficiency of communication will be diminished. Band Steering can steer clients capable of communication on both bands 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**.

The screenshot shows the 'Wireless Settings' menu with 'Band Steering' selected. The configuration page includes a checkbox for 'Band Steering' (unchecked), and three input fields for 'Connection Threshold' (20), 'Difference Threshold' (4), and 'Max Failures' (10). Each input field has a range indicator in parentheses. An 'Apply' button is at the bottom left.

Parameter	Value	Range
Band Steering	<input type="checkbox"/>	
Connection Threshold	20	(2-40)
Difference Threshold	4	(1-8)
Max Failures	10	(0-100)

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

When the number of clients on the 5GHz band reaches the value of **Connection Threshold** and the difference value between the number of clients on the 2.4GHz band and the 5GHz band reaches the value of **Difference Threshold**, EAPs will refuse the requests of communication on the 5GHz band from other clients and no longer steer other clients to the 5GHz band.

The value of **Connection Threshold** is from 2 to 40, and the default is 20.

The value of **Difference Threshold** is from 1 to 8, and the default is 4.

#### 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.

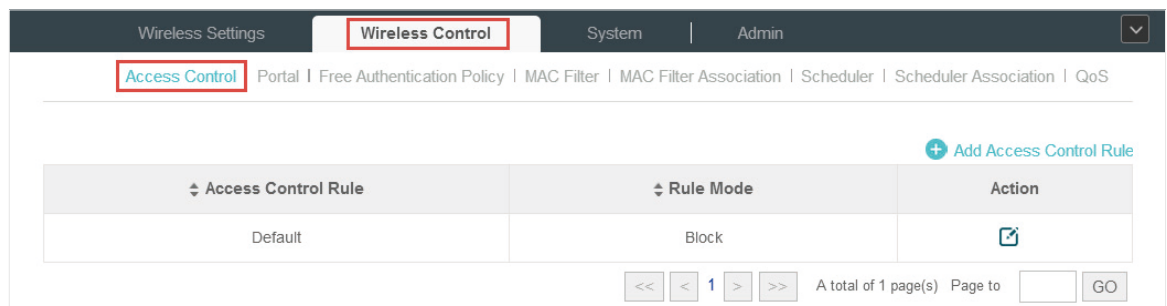
The value is from 0 to 100, and the default is 10.

4. Click **Apply**.

## 3.2 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**.



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

The dialog box titled 'Add Access Control Rule' contains the following fields and buttons:

- Rule Name:** A text input field.
- Rule Mode:** A dropdown menu currently set to 'Block'.
- Rule Members:** A section containing two subnets:
  - Subnets:** A text input field with '0.0.0.0/24' and an 'Add New' button below it.
  - Except Subnets:** A text input field with '0.0.0.0/24' and an 'Add New' button below it.
- Apply:** A large button at the bottom left.

3. Configure the following parameters.

Rule Name	Specify a name for this rule.
Rule Mode	<p>Select the mode for this rule.</p> <p><b>Block:</b> Select this mode to block clients to access the specific subnets.</p> <p><b>Allow:</b> Select this mode to allow clients to access the specific subnets.</p>
Rule Memebers	<p>Specify the member subnets for this rule.</p> <p><b>Subnets:</b> Enter the subnet that will follow the rule mode in the format X.X.X.X/X and click <a href="#">Add New</a> . Up to 16 subnets can be added.</p> <p><b>Except Subnets:</b> Enter the excepted subnet in the format X.X.X.X/X and click <a href="#">Add New</a> . 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.</p>

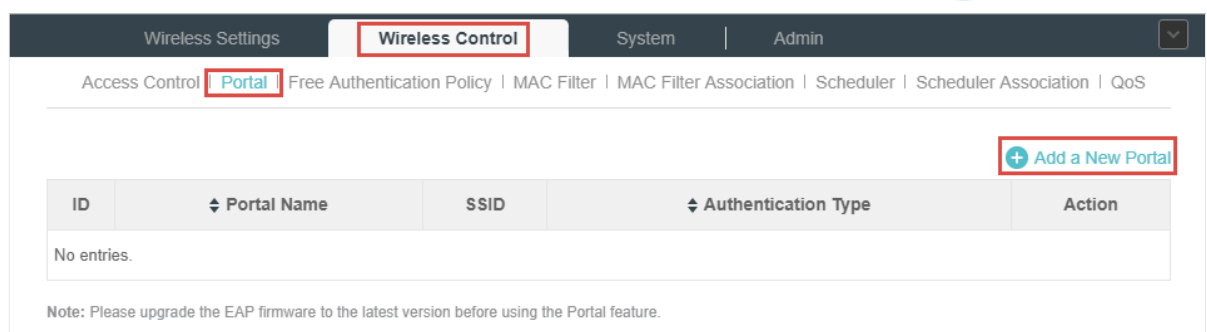
4. Click **Apply**.

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](#) .



Then the following window will pop up:

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.

Configure the following parameters:

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



Authentication Type	Select <b>No Authentication</b> .
Authentication Timeout	<p>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.</p> <p>Options include <b>1 Hour, 8 Hours, 24 Hours, 7 Days</b> and <b>Custom</b>. <b>Custom</b> allows you to define the time in days, hours and minutes. The default value is one hour.</p> <p>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.</p> <p>Options include <b>30 Minutes, 1 Hour, 2 Hours, 4 Hours</b> and <b>8 Hours, Custom</b>. <b>Custom</b> allows you to define the time in hours and minutes. The default value is 30 minutes.</p>
Daily Limit	With Daily Limit enabled, after authentication times out, the user cannot get authenticated again in the same day.
HTTPS Redirect	<p>With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.</p> <p>With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.</p>
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: ☐ Enable

Button:






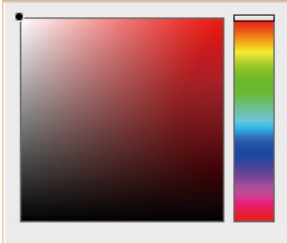


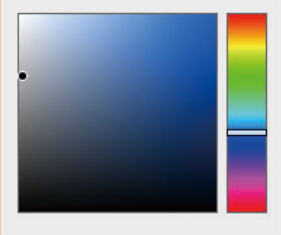
PC Mobile Phone Tablet PC Restore

tp-link

Log In

Configure the following parameters:

Background	Select the background type. Two types are supported: <b>Solid Color</b> and <b>Picture</b> .
------------	--

Background Color	<p>If <b>Solid Color</b> is selected, configure your desired background color through the color picker or by entering the RGB value manually.</p>
Background Picture	<p>If <b>Picture</b> is selected, click the <b>Choose</b> button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click <b>Confirm</b>.</p>
Logo Picture	<p>Click the <b>Choose</b> button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click <b>Confirm</b>.</p> <p>In addition, you can click  and configure the logo position. The options include <b>Middle</b>, <b>Upper</b> and <b>Lower</b>.</p> <div data-bbox="606 600 1212 703"> <div> Logo Picture: <div> Choose   </div> </div> <div> Logo Position: <div>Middle ▼</div> </div> </div>
Welcome Information	<p>Specify the welcome information.</p> <p>In addition, you can click  and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.</p> <div data-bbox="606 904 1398 1256"> <div> Welcome Information: <div></div> <div>(1-31 characters) </div> </div> <div> <div>#ffffff</div> <div>(RGB value)</div> </div> <div> Welcome Information Color: <div>  </div> </div> </div>
Copyright	<p>Specify the copyright information.</p> <p>In addition, you can click  and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.</p> <div data-bbox="606 1426 1402 1859"> <div> Copyright: <div></div> <div>(1-200 characters) </div> </div> <div> <div>#A7A9AC</div> <div>(RGB value)</div> </div> <div> Copyright Color: <div>  </div> </div> </div>

## 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**.

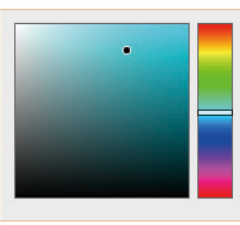
**Button Color:** Select your desired login button color through the color picker or by entering the RGB value manually.

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

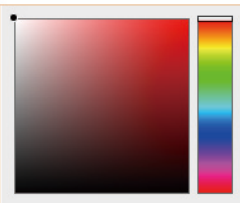
Button: 

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 <b>Allow to Skip Advertisement</b> .
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 <b>Skip</b> 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.

The screenshot shows the 'Basic Info' configuration page for a portal. It contains the following fields and settings:

- Portal Name:** A text input field.
- SSID:** A dropdown menu with the text '==Please select=='.
- Authentication Type:** A dropdown menu set to 'Simple Password'.
- Password:** A text input field.
- Authentication Timeout:** A dropdown menu set to '1 Hour'.
- HTTPS Redirect:** A checkbox labeled 'Enable' which is checked.
- Redirect:** A checkbox labeled 'Enable' which is unchecked.
- Redirect URL:** A text input field.

Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select <b>Simple Password</b> .

Password	Set the password for authentication.
Authentication Timeout	<p>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.</p> <p>Options include <b>1 Hour</b>, <b>8 Hours</b>, <b>24 Hours</b>, <b>7 Days</b> and <b>Custom</b>. <b>Custom</b> allows you to define the time in days, hours and minutes. The default value is one hour.</p>
HTTPS Redirect	<p>With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.</p> <p>With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.</p>
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.



Configure the following parameters:

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

### 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**.


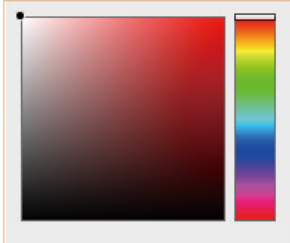
In addition, you can click  and configure the logo position. The options include **Middle**, **Upper** and **Lower**.

Logo Picture:	<input type="button" value="Choose"/>  
Logo Position:	<input type="text" value="Middle"/>

### Welcome Information


Specify the welcome information.


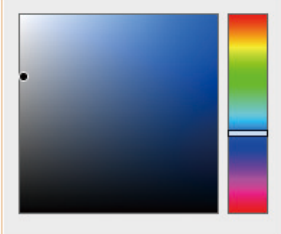
In addition, you can click  and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.

Welcome Information:	<input type="text"/>	(1-31 characters) 
	<input type="text" value="#ffffff"/>	(RGB value)
Welcome Information Color:		

### Copyright

Specify the copyright information.

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

Copyright:	<input type="text"/>	(1-200 characters) 
	<input type="text" value="#A7A9AC"/>	(RGB value)
Copyright Color:		

### Terms of Service

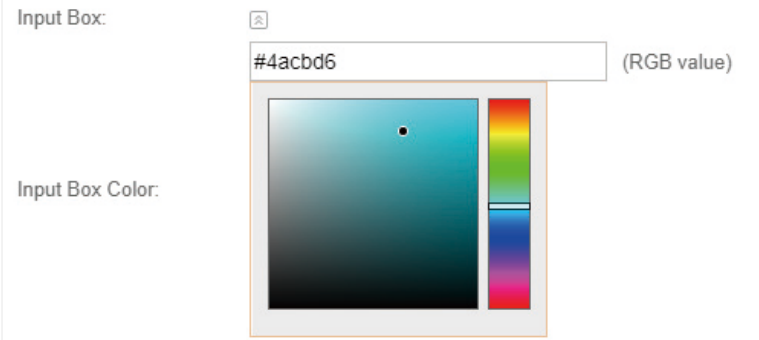
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Terms of Service:	<input checked="" type="checkbox"/> Enable
<div></div>	

## 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.



The interface shows the 'Input Box' configuration. It includes a label 'Input Box:' followed by a small icon. Below this is a text input field containing the hex value '#4acbd6' and a label '(RGB value)'. To the left of the color picker is the label 'Input Box Color:'. The color picker itself consists of a large square gradient area and a vertical color bar on the right.

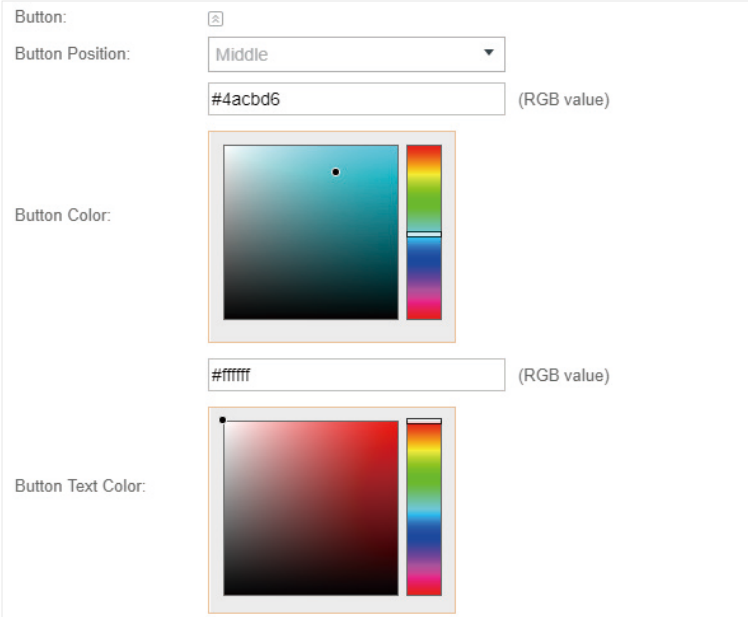
## Button

Click  and configure the button.

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

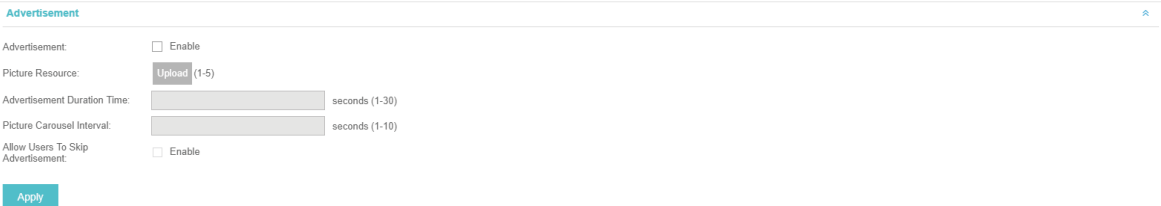
**Button Color:** Select your desired login button color through the color picker or by entering the RGB value manually.

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



The interface shows the 'Button' configuration. It includes a label 'Button:' followed by a small icon. Below this is a dropdown menu for 'Button Position' with 'Middle' selected. To the right of the dropdown is a text input field containing the hex value '#4acbd6' and a label '(RGB value)'. Below the dropdown is a color picker for 'Button Color' with a label 'Button Color:'. The color picker consists of a large square gradient area and a vertical color bar on the right. Below the color picker is a text input field containing the hex value '#ffffff' and a label '(RGB value)'. Below the text input field is a color picker for 'Button Text Color' with a label 'Button Text Color:'. The color picker consists of a large square gradient area and a vertical color bar on the right.

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



The interface shows the 'Advertisement' configuration. It includes a label 'Advertisement:' followed by a small icon. Below this is a checkbox for 'Enable'. To the right of the checkbox is a text input field containing the value '1-5'. Below the text input field is a label 'Advertisement Duration Time:'. To the right of the label is a text input field containing the value 'seconds (1-30)'. Below the text input field is a label 'Picture Carousel Interval:'. To the right of the label is a text input field containing the value 'seconds (1-10)'. Below the text input field is a label 'Allow Users To Skip Advertisement:'. To the right of the label is a checkbox for 'Enable'. At the bottom left is a button labeled '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 <b>Allow to Skip Advertisement</b> .
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 <b>Skip</b> 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 <b>Local User</b> .
User Management	You can click this button to configure user accounts for authentication later. Please refer to <a href="#">Create Local User Accounts</a> .
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.

Configure the following parameters:

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


Logo Picture: Choose


Logo Position: Middle

---

### Welcome Information

Specify the welcome information.


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


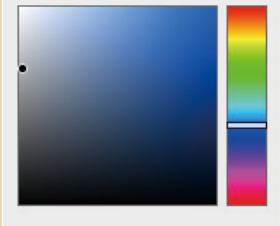
Welcome Information:	<input type="text"/>	(1-31 characters) 
	<input type="text" value="#ffffff"/>	(RGB value)
Welcome Information Color:		

---

### Copyright

Specify the copyright information.

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

Copyright:	<input type="text"/>	(1-200 characters) 
	<input type="text" value="#A7A9AC"/>	(RGB value)
Copyright Color:		

---

### Terms of Service

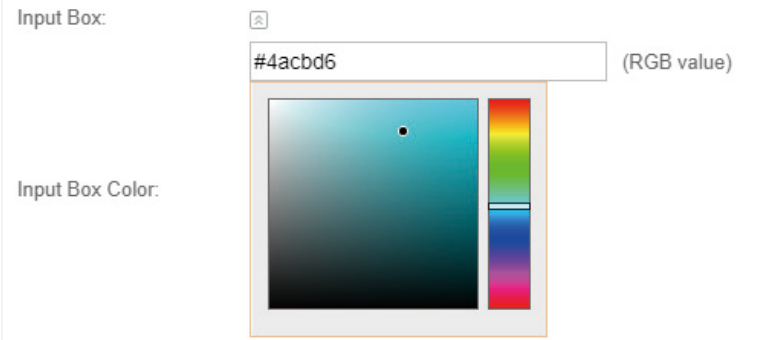
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Terms of Service:	<input checked="" type="checkbox"/> Enable
<div><div></div></div>	

## 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.



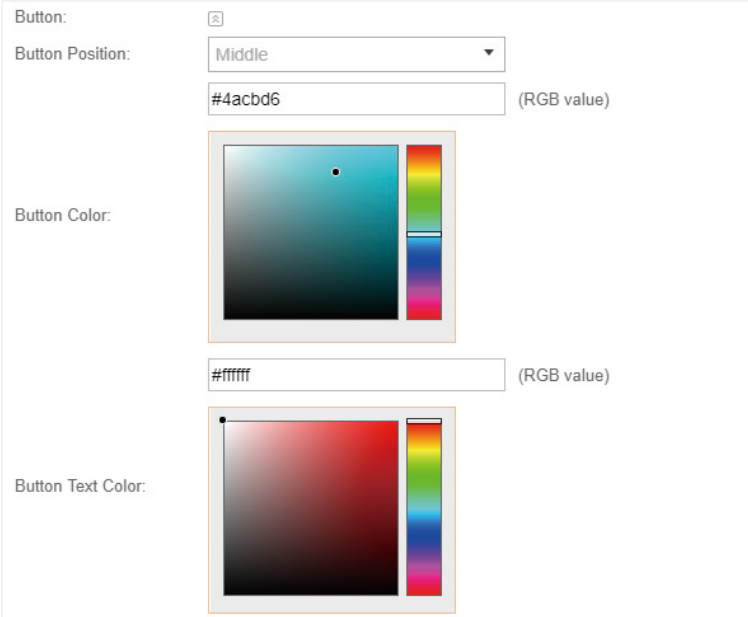
## Button

Click  and configure the button.

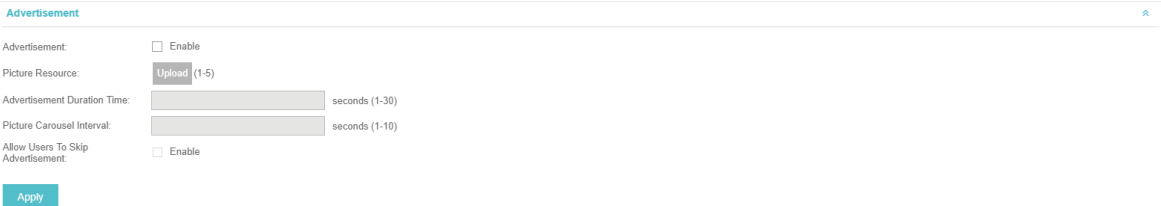
**Button Position:** Set the position of the login button. The options include **Middle**, **Upper** and **Lower**.

**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.



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




Configure the following parameters:

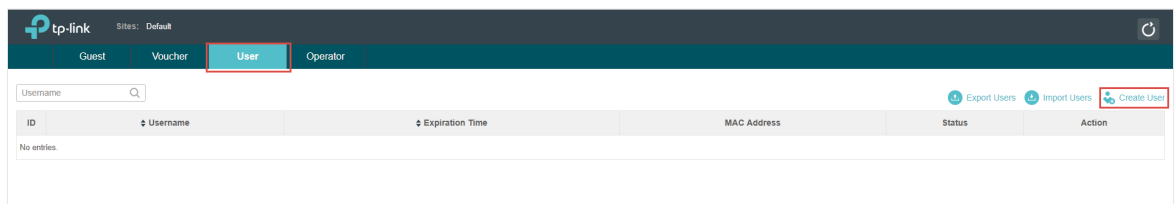
Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling <b>Allow to Skip Advertisement</b> .
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 <b>Skip</b> 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**.



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

Create New User

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)

☐

Rate Limit(Download)

Kbps (0-10240000)

Rate Limit(Upload)

☐

Rate Limit(Upload)

Kbps (0-10240000)

Traffic Limit

☐

Traffic Limit

MBytes (1-1048576)

Apply

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	<p>There are three types of MAC binding: <b>No Binding</b>, <b>Static Binding</b> and <b>Dynamic Binding</b>.</p> <p><b>Static Binding:</b> 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.</p> <p><b>Dynamic Binding:</b> 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.</p>
Maximum Users	Specify the maximum number of users able to use this account to pass the authentication.
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)

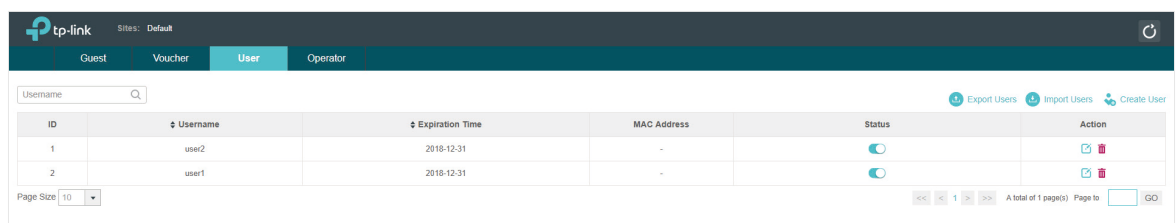
Select whether to enable upload rate limit. With this option enabled, you can specify the limit of upload rate.

### 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.



The screenshot shows the TP-Link User Management interface. At the top, there are tabs for Guest, Voucher, User, and Operator. The 'User' tab is selected. Below the tabs, there is a search bar for 'Username'. To the right of the search bar, there are buttons for 'Export Users', 'Import Users', and 'Create User'. Below these buttons is a table with the following columns: ID, Username, Expiration Time, MAC Address, Status, and Action. The table contains two rows of data. The first row has ID 1, Username user2, Expiration Time 2018-12-31, MAC Address -, and Status is enabled (indicated by a blue toggle switch). The second row has ID 2, Username user1, Expiration Time 2018-12-31, MAC Address -, and Status is enabled (indicated by a blue toggle switch). At the bottom of the table, there is a 'Page Size' dropdown set to 10, and a pagination bar showing 'A total of 1 page(s)' and 'Page to' with a 'GO' button.

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

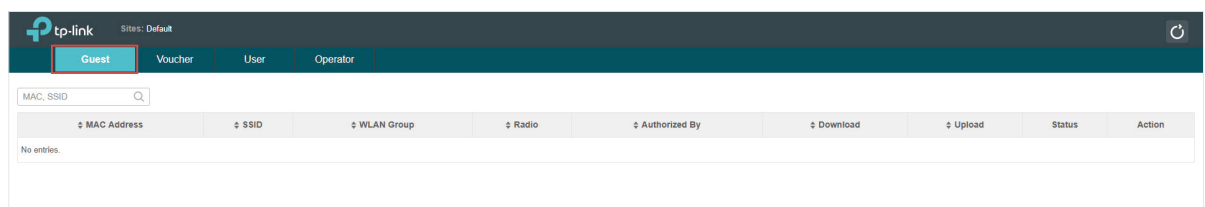
Additionally, you can click  **Export Users** to backup all the user account information into a CSV file or XLS file and save the file to your PC. If needed, you can click  **Import Users** and select the file to import the account information to the list.

### 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.



The screenshot shows the TP-Link Guest Management interface. At the top, there are tabs for Guest, Voucher, User, and Operator. The 'Guest' tab is selected. Below the tabs, there is a search bar for 'MAC, SSID'. Below the search bar is a table with the following columns: MAC Address, SSID, WLAN Group, Radio, Authorized By, Download, Upload, Status, and Action. The table is currently empty, showing 'No entries.' at the bottom.

MAC Address	SSID	WLAN Group	Radio	Authorized By	Download	Upload	Status	Action
No entries.								

You can select an icon to execute the corresponding operation:



Disconnect client.



Extend the effective time.

## Create Operator Accounts

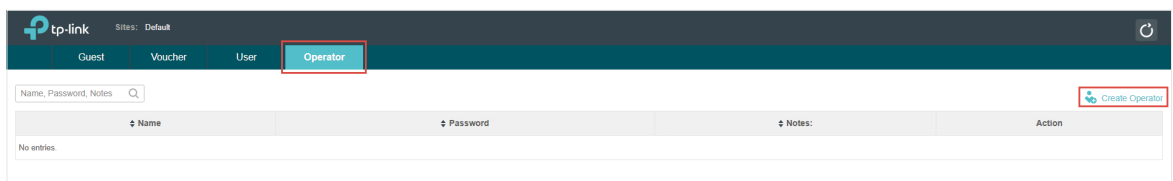
Operator account can be used to remotely manage the Local User Portal and Voucher Portal. Other users can visit the URL **https://Omada Controller Host's IP Address:8043/hotspot** (For example: https://192.168.0.64:8043/hotspot) and use the Operator account to enter the portal management page.


### Note:

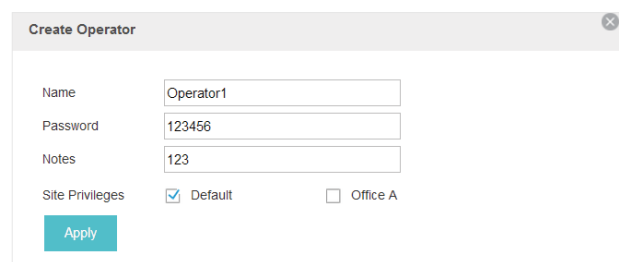
The users who enter the portal management page by Operator account can only create local user accounts and vouchers and manage the clients.

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.



The 'Create Operator' dialog box contains the following fields and options:

Name	Operator1
Password	123456
Notes	123
Site Privileges	<input checked="" type="checkbox"/> Default <input type="checkbox"/> Office A
<b>Apply</b>	

3. Specify the **Name**, **Password** and **Notes** of the Operator account.
4. Choose **Site Privileges** (more than one options can be chosen) 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 Omada Controller 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 <b>Voucher</b> .
User Management	You can click this button to configure vouchers for authentication later. Please refer to <a href="#">Create Vouchers</a> .
HTTPS Redirect	<p>With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.</p> <p>With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.</p>
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:

☐ Enable

Input Box:

Button:

PC

Mobile Phone






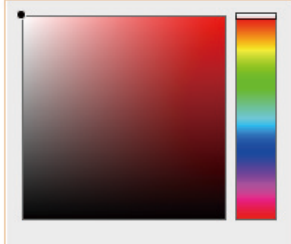


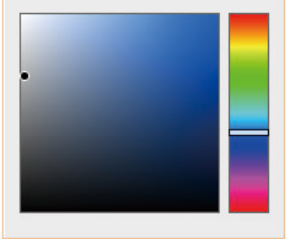
Tablet PC

Restore

Configure the following parameters:

Background	Select the background type. Two types are supported: <b>Solid Color</b> and <b>Picture</b> .
------------	--



Background Color	<p>If <b>Solid Color</b> is selected, configure your desired background color through the color picker or by entering the RGB value manually.</p>
Background Picture	<p>If <b>Picture</b> is selected, click the <b>Choose</b> button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click <b>Confirm</b>.</p>
Logo Picture	<p>Click the <b>Choose</b> button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click <b>Confirm</b>.</p> <p>In addition, you can click  and configure the logo position. The options include <b>Middle</b>, <b>Upper</b> and <b>Lower</b>.</p> <div data-bbox="606 600 1212 701"> <div> Logo Picture: <div> Choose   </div> </div> <div> Logo Position: <div>Middle ▼</div> </div> </div>
Welcome Information	<p>Specify the welcome information.</p> <p>In addition, you can click  and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.</p> <div data-bbox="606 904 1398 1256"> <div> Welcome Information: <div></div> <div>(1-31 characters) </div> </div> <div> <div>#ffffff</div> <div>(RGB value)</div> </div> <div> Welcome Information Color: <div>  </div> </div> </div>
Copyright	<p>Specify the copyright information.</p> <p>In addition, you can click  and select your desired text color for Copyright information through the color picker or by entering the RGB value manually.</p> <div data-bbox="606 1426 1398 1859"> <div> Copyright: <div></div> <div>(1-200 characters) </div> </div> <div> <div>#A7A9AC</div> <div>(RGB value)</div> </div> <div> Copyright Color: <div>  </div> </div> </div>

## 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

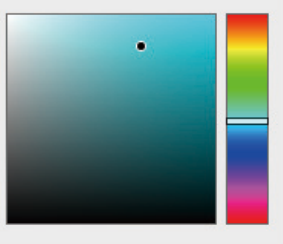
Click  and configure the input box.

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.

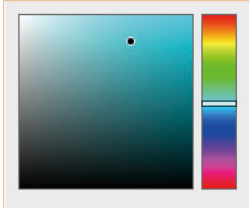
Button: 

Button Position: 

Middle

#4acbd6

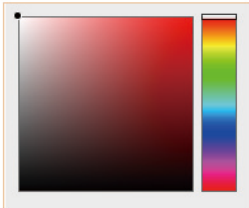
(RGB value)



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.

The screenshot shows the 'Advertisement' configuration panel. It includes the following options: 'Advertisement' with an 'Enable' checkbox; 'Picture Resource' with an 'Upload' button and '(1-5)' indicating the limit; 'Advertisement Duration Time' with a slider and 'seconds (1-30)' label; 'Picture Carousel Interval' with a slider and 'seconds (1-10)' label; and 'Allow Users To Skip Advertisement' with an 'Enable' checkbox. An 'Apply' button is at the bottom left.


Configure the following parameters:

<b>Advertisement</b>	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 <b>Allow to Skip Advertisement</b> .
<b>Picture Resource</b>	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
<b>Advertisement Duration Time</b>	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.
<b>Picture Careusel Interval</b>	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.
<b>Allow Users To Skip Advertisement</b>	Specify whether to enable this feature. With this feature enabled, the user can click the <b>Skip</b> 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** .

The screenshot shows the 'Voucher Manager' interface. At the top, there are tabs for 'Guest', 'Voucher', 'User', and 'Operator', with 'Voucher' selected. Below the tabs is a search bar labeled 'Code, Notes'. On the right, there are links for 'Print All Unused Vouchers', 'Print Selected Vouchers', 'Create Vouchers' (highlighted with a red box), and 'Delete'. Below these links is a table with columns: 'Code', 'Created Time', 'Notes', 'Duration', 'Status', and 'Action'. The table currently shows '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

(1-10000)

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)

Notes:

Apply

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	<p>Select <b>Single Use</b> or <b>Multi Use</b>.</p> <p>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.</p> <p>If you select Multi Use, enter the value of <b>Max Users</b>. 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.</p>
Duration	<p>Select the period of validity of the Voucher.</p> <p>The options include <b>8 hours</b>, <b>2 days</b> and <b>User-defined</b>. The period of valid of the voucher is reckoned from the time when it is used for the first time.</p>
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.

tp-link

Sites: Default

Guest

Voucher

User

Operator

Code, Notes

Print All Unused Vouchers

Print Selected Vouchers

Create Vouchers

Delete

<input type="checkbox"/>	Code	Created Time	Notes	Duration	Status	Action
<input type="checkbox"/>	541471	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>
<input type="checkbox"/>	446018	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>
<input type="checkbox"/>	995065	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>
<input type="checkbox"/>	787551	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>
<input type="checkbox"/>	553767	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>
<input type="checkbox"/>	529108	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>
<input type="checkbox"/>	090304	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>
<input type="checkbox"/>	635265	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>
<input type="checkbox"/>	973116	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>
<input type="checkbox"/>	904939	2018-02-22 11:45:29		8h	Valid for single use	<div><div></div><div></div></div>

Page Size




10

<<< < 1 > >>>

A total of 1 page(s)

Page to

GO

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.



2018/02/22

Voucher

<u>Valid for 8h</u> with single use	<u>Valid for 8h</u> with single use	<u>Valid for 8h</u> with single use	<u>Valid for 8h</u> with single use
<b>904939</b>	<b>973116</b>	<b>635265</b>	<b>090304</b>
<u>Valid for 8h</u> with single use	<u>Valid for 8h</u> with single use	<u>Valid for 8h</u> with single use	<u>Valid for 8h</u> with single use
<b>529108</b>	<b>553767</b>	<b>787551</b>	<b>995065</b>
<u>Valid for 8h</u> with single use	<u>Valid for 8h</u> with single use		
<b>446018</b>	<b>541471</b>		

<https://127.0.0.1:8043/tp-link/voucher/print.html>

1/1

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.

tp-link

Sites: Default

Guest

Voucher

User

Operator

MAC, SSID

MAC Address	SSID	WLAN Group	Radio	Authorized By	Download	Upload	Status	Action
No entries.								

You can select an icon to execute the corresponding operation:



Restrict the client to access the network.



Extend the effective time.

## Create Operator Accounts

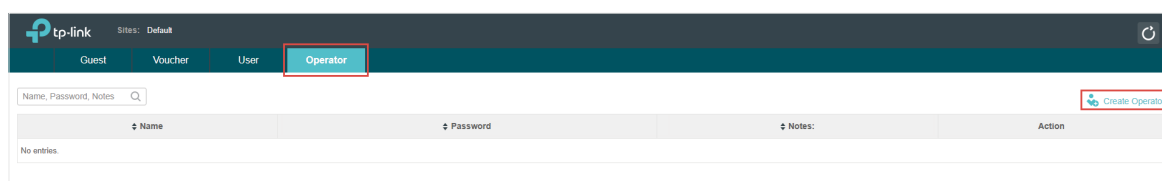
Operator account can be used to remotely manage the Local User Portal and Voucher Portal. Other users can visit the URL **https://Omda Controller Host's IP Address:8043/hotspot** (For example: **https://192.168.0.64:8043/hotspot**) and use the Operator account to enter the portal management page.

### 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

Operator1

Password

123456

Notes

123

Site Privileges

☒ Default ☐ Office A

Apply

3. Specify the **Name**, **Password** and **Notes** of the Operator account.
4. Choose **Site Privileges** (more than one options can be chosen) 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](https://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:

Authentication Type:

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

Twilio SID:

Auth Token:

Phone Number:  (E.g., +17704505791)

Maximum Users:  (0-10, 0 means no limit)

Authentication Timeout:

Preset Country Code:  (E.g., +1, optional)

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 <b>SMS</b> .
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	<p>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.</p> <p>Specify the upper limit in this field.</p>

<b>Authentication Timeout</b>	<p>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.</p> <p>Options include <b>1 Hour</b>, <b>8 Hours</b>, <b>24 Hours</b>, <b>7 Days</b> and <b>Custom</b>. <b>Custom</b> allows you to define the time in days, hours and minutes. The default value is one hour.</p>
<b>Preset Country Code</b>	Set the default country code that will be filled automatically on the authentication page.
<b>HTTPS Redirect</b>	<p>With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.</p> <p>With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.</p>
<b>Redirect</b>	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
<b>Redirect URL</b>	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.


Configure the following parameters:



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



### 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**.


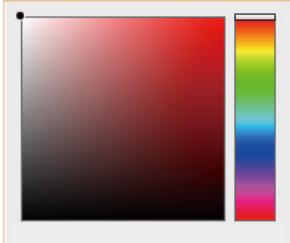
In addition, you can click  and configure the logo position. The options include **Middle**, **Upper** and **Lower**.

Logo Picture:	<input type="button" value="Choose"/>  
Logo Position:	<input type="text" value="Middle"/>

### Welcome Information


Specify the welcome information.


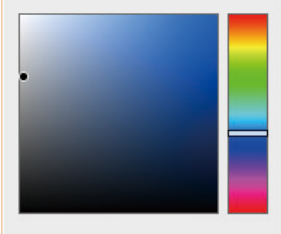
In addition, you can click  and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.

Welcome Information:	<input type="text"/>	(1-31 characters) 
	<input type="text" value="#ffffff"/>	(RGB value)
Welcome Information Color:		

### Copyright

Specify the copyright information.

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

Copyright:	<input type="text"/>	(1-200 characters) 
	<input type="text" value="#A7A9AC"/>	(RGB value)
Copyright Color:		

### Terms of Service

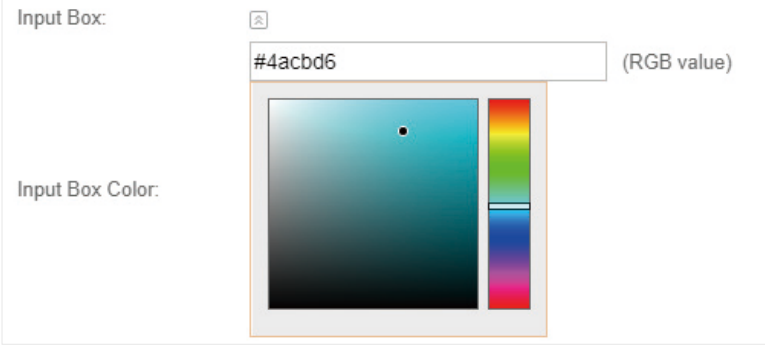
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Terms of Service:	<input checked="" type="checkbox"/> Enable
<div></div>	

## 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.



The interface shows the 'Input Box' configuration. It includes a label 'Input Box:' followed by a small icon. Below it is a text input field containing the hex value '#4acbd6' and a label '(RGB value)'. To the left of this is the label 'Input Box Color:'. Below the text input is a color picker with a square gradient and a vertical color bar.

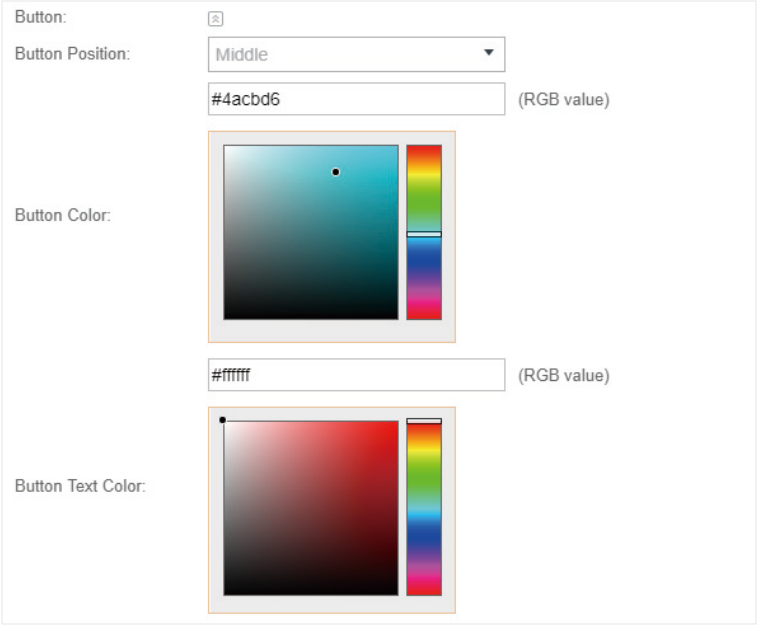
## Button

Click  and configure the button.

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

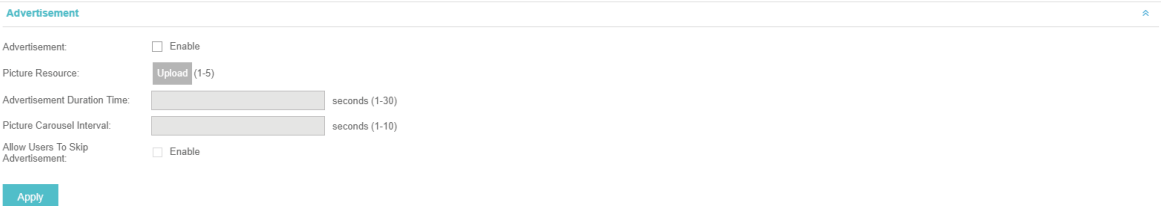
**Button Color:** Select your desired login button color through the color picker or by entering the RGB value manually.

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



The interface shows the 'Button' configuration. It includes a label 'Button:' followed by a small icon. Below it is a dropdown menu for 'Button Position:' with 'Middle' selected. To the right of the dropdown is a text input field containing the hex value '#4acbd6' and a label '(RGB value)'. Below the dropdown is a color picker with a square gradient and a vertical color bar. To the left of this is the label 'Button Color:'. Below the color picker is a text input field containing the hex value '#ffffff' and a label '(RGB value)'. To the left of this is the label 'Button Text Color:'. Below the text input is another color picker with a square gradient and a vertical color bar.

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



The interface shows the 'Advertisement' configuration. It includes a label 'Advertisement:' followed by a checkbox 'Enable'. Below it is a label 'Picture Resource:' followed by an 'Upload' button and '(1-5)'. Below that is a label 'Advertisement Duration Time:' followed by a slider and 'seconds (1-30)'. Below that is a label 'Picture Carousel Interval:' followed by a slider and 'seconds (1-10)'. Below that is a label 'Allow Users To Skip Advertisement:' followed by a checkbox 'Enable'. At the bottom is an 'Apply' button.

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 <b>Allow to Skip Advertisement</b> .
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 <b>Skip</b> 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:**

Omada Controller 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](http://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 ?

Apply

Configure the following parameters:

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

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 EAP. The External Web Portal is provided by external portal server.

#### Note:

Omada Controller 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

RADIUS Server IP:

RADIUS Port:

RADIUS Password:

Authentication Timeout:

1 Hour

HTTPS Redirect:

☒ Enable

Redirect:

☐ Enable

Redirect URL:

Portal Customization:

External Web Portal

External Web Portal URL:

Apply

Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select <b>Simple Password</b> .
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	<p>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.</p> <p>Options include <b>1 Hour, 8 Hours, 24 Hours, 7 Days, Custom</b>. <b>Custom</b> allows you to define the time in days, hours, and minutes. The default value is one hour.</p>
HTTPS Redirect	<p>With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites.</p> <p>With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.</p>
Redirect	<p>If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.</p> <p>Disabled by default.</p>
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. Put the external web portal server to a whitelist of [Free Authentication Policy](#), otherwise clients cannot access it before authenticated.

4. **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: ☐ Enable

Input Box: ☒ [?](#)

Button: ☒ [?](#)

PC Mobile Phone Tablet PC [Restore](#)

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

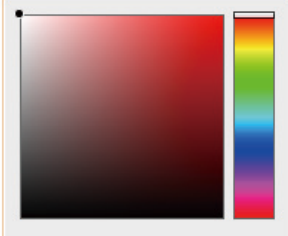
Welcome Information:

(1-31 characters) 

#ffffff

(RGB value)


Welcome Information Color:




---

### Copyright

Specify the copyright information.

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

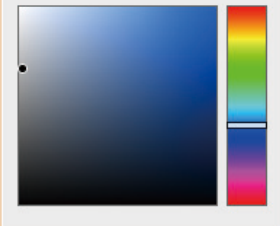
Copyright:

(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.

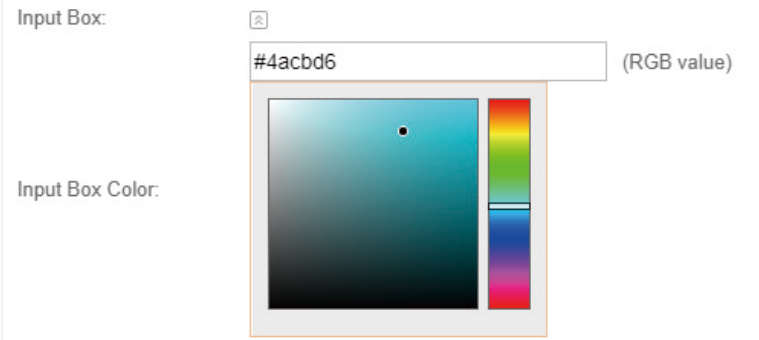
Terms of Service:

☒ 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.



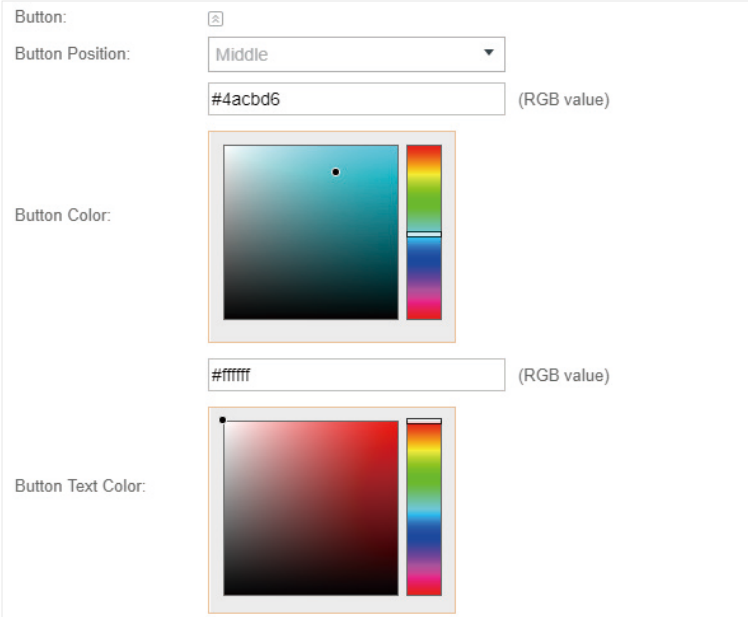
## Button

Click  and configure the button.

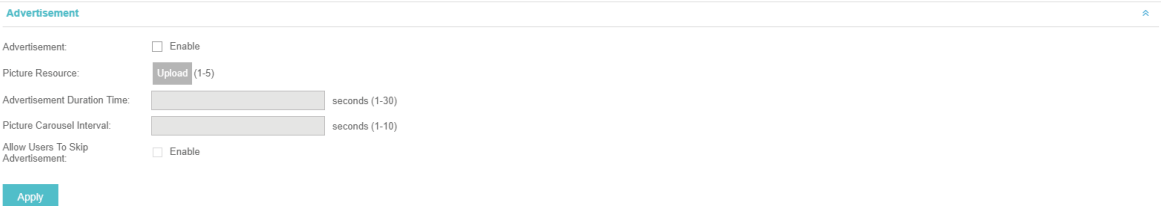
**Button Position:** Set the position of the login button. The options include **Middle**, **Upper** and **Lower**.

**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.



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



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 <b>Allow to Skip Advertisement</b> .
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 <b>Skip</b> button to skip the advertisement.

6. 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 Omada Controller, 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:

Authentication Type:

External Portal Server:  [?](#)

HTTPS Redirect: ☒ Enable [?](#)

**Apply**

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select <b>External Portal Server</b> .

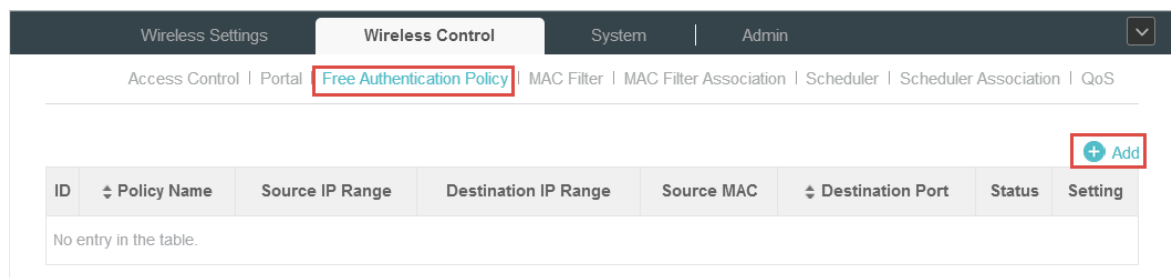
External Portal Server	<p>Enter the complete authentication URL that redirect to an external portal server, for example:</p> <p>http://192.168.0.147:8880/portal/index.php or http://192.168.0.147/portal/index.html</p>
HTTPS Redirect	<p>With this function enabled, the unauthorized clients will be redirected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

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**.



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

Add Policy

Policy Name:

Match Mode:

IP-Mac based

Source IP Range:

/

(Optional)

Destination IP Range:

/

(Optional)

Source MAC:

(Optional)

Destination Port:

(Optional)

Status:

☐ Enable

Apply

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	<p>Select the match mode for the policy. Two options are provided:</p> <p><b>URL:</b> With this option selected, configure an URL that is allowed to be visited by the clients without authentication.</p> <p><b>IP-MAC Based:</b> 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.</p>
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.

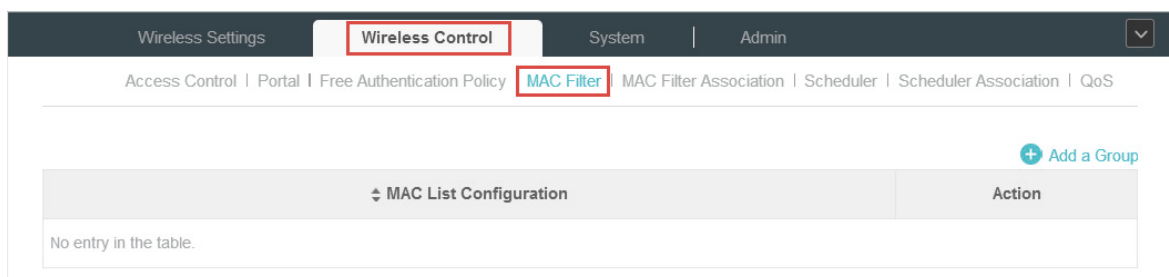
4. Click **Apply** and the policy is successfully added.

## 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.



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

Add a Group

MAC Filter Name:

Apply

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

+ Add a Group

MAC List Configuration		Action
Group1		

MAC Address

+ Add a Group Member

ID	MAC Address	Action
No entry in the table.		

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

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

**Add a Group Member** ✕

MAC Address:

**Apply**

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

+ Add a Group

MAC List Configuration		Action
Group1		

MAC Address

+ Add a Group Member

ID	MAC Address	Action
1	AA-BB-CC-DD-EE-FF	

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

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 Omada Controller.

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

Wireless Settings | 
 Wireless Control | 
 System | Admin

Access Control | Portal | Free Authentication Policy | MAC Filter | 
 MAC Filter Association | 
 Scheduler | Scheduler Association | QoS

MAC Filtering: ☒ Enable **Apply**

2.4GHz 
 5GHz 
 Default

ID	SSID Name	Band	MAC Filter Name	Action	Setting
1	SSID1	2.4GHz	<span style="border: 1px solid #ccc; padding: 2px 10px;">Group1</span>	<span style="border: 1px solid #ccc; padding: 2px 10px;">Allow</span>	<b>Apply</b>

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

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

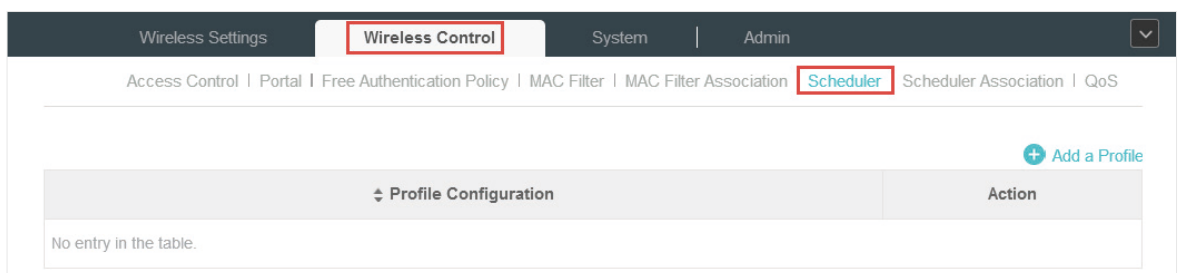
- 2) Select a band frequency (2.4GHz or 5GHz) and a WLAN group.
- 3) In the MAC Filter Name column of the specified SSID, select a MAC Filter group in the drop-down list. Then select **Allow/Deny** in the Action column to allow/deny the clients in the MAC Filter group to access the network.
- 4) Click **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**.



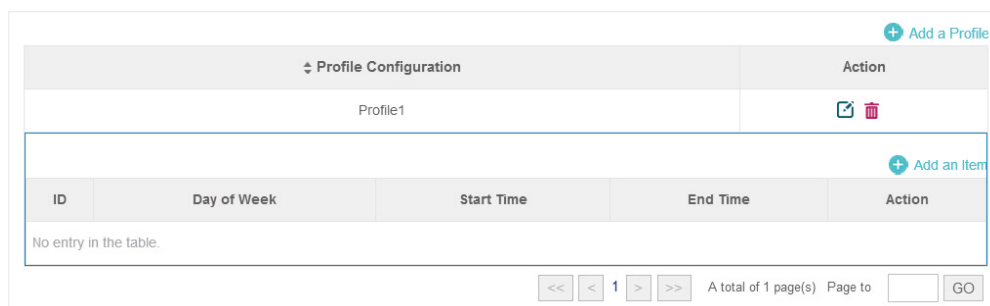
- 1) Click **+ Add a Profile** and specify a name for the profile.

**Add a Profile**
✕

Profile Name:

Apply

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



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

**Add an Item**

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

**Apply**

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

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

Wireless Settings | **Wireless Control** | System | Admin

Access Control | Portal | Free Authentication Policy | MAC Filter | MAC Filter Association | Scheduler | **Scheduler Association** | QoS

Scheduler: ☒ Enable

Association Mode: Associated with SSID

**Apply**

2.4GHz 5GHz Default

ID	SSID Name	Band	Profile Name	Action	Setting
1	SSID1	2.4GHz	Profile1	Radio On	<b>Apply</b>

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

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 Omada Controller software 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**.

Wireless Settings | **Wireless Control** | System | Admin

Access Control | Portal | Free Authentication Policy | MAC Filter | MAC Filter Association | Scheduler | Scheduler Association | **QoS**

2.4GHz | 5GHz

Restore to Default Values: **Restore**

Wi-Fi Multimedia(WMM): ☒ Enable

NoAcknowledgement: ☐ Enable

Unscheduled Automatic Power Save Delivery: ☒ Enable

**AP EDCA Parameters:** ⌵

**Station EDCA Parameters:** ⌵

**Apply**

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).

**NoAcknowledgement**

By default disabled. You can enable this function to specify that the EAP devices should not acknowledge frames with QoSNoAck. NoAcknowledgement 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	<p><b>Queue</b> 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.</p> <p><b>Data 0 (Voice)</b>—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.</p> <p><b>Data 1 (Video)</b>—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.</p> <p><b>Data 2 (Best Effort)</b>—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.</p> <p><b>Data 3 (Background)</b>—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).</p>
Arbitration Inter-Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values for <b>Arbitration Inter-Frame Space</b> are from 0 to 15.
Minimum Contention Window	<p>A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.</p> <p>This value can not be higher than the value for the <b>Maximum Contention Window</b>.</p>
Maximum Contention Window	<p>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.</p> <p>This value must be higher than the value for the <b>Minimum Contention Window</b>.</p>
Maximum Burst	<b>Maximum Burst</b> 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.

- 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)	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="1504"/>
Data 1(Video)	<input type="text" value="2"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="3008"/>
Data 2(Best Effort)	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>
Data 3(Background)	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>



Queue	<p><b>Queue</b> 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.</p> <p><b>Data 0 (Voice)</b>—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.</p> <p><b>Data 1 (Video)</b>—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.</p> <p><b>Data 2 (Best Effort)</b>—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.</p> <p><b>Data 3 (Background)</b>—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).</p>
Arbitration Inter-Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values for <b>Arbitration Inter-Frame Space</b> 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 <b>Maximum Contention Window</b> .
Maximum Contention Window	<p>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.</p> <p>This value must be higher than the value for the <b>Minimum Contention Window</b>.</p>
TXOP Limit	The <b>TXOP Limit</b> 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 System

### 3.8.1 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 **System > Reboot Schedule**.

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**.

### 3.8.2 Log Setting

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

1. Go to **System > Log Setting**.

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.

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	<p>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.</p> <div> Time Mode: <input checked="" type="radio"/> Fixation Time <input type="radio"/> Period Time </div> <div> Fixation Time: <input type="text" value="00"/> : <input type="text" value="00"/> (HH:MM) </div>
Period Time	<p>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.</p> <div> Time Mode: <input type="radio"/> Fixation Time <input checked="" type="radio"/> Period Time </div> <div> Period Time: <input type="text"/> Hours(1-24) </div>

## Server

If Server is enabled, system logs will be sent to a server. You can enable the feature and enter its IP address and port.

☒ **Enable Server**

System Log Server IP:

System Log Server Port:

### 3.8.3 Device Account

When the EAP devices are adopted at the first time, their username and password will become the same as those of the Omada Controller 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 **System > Device Account**.

Wireless Settings | Wireless Control | **System** | Admin

Reboot Schedule | Log Settings | **Device Account** | Backup&Restore | Batch Upgrade | More Settings | About

Current Username:

Current Password:

New Username:

New Password:

2. Specify a new username and password for the EAP devices.
3. Click **Apply**.

**Note::**

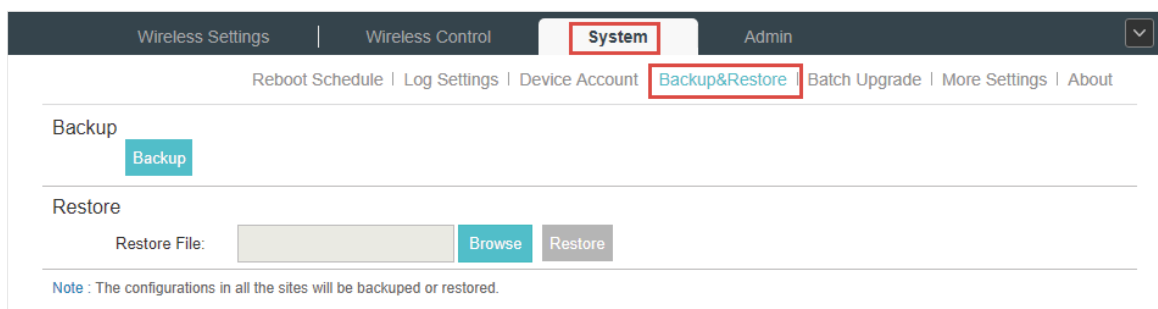
The new account will be applied to EAP devices but not the Omada Controller. To change the Omada Controller's username and password, please refer to [User Account](#).

### 3.8.4 Backup&Restore

You can save the current configuration of the EAPs as a backup file and if necessary, and restore the configuration using the backup file. We recommend you back up the settings before upgrading the device.

Follow the steps below to backup and restore the configuration.

1. Go to **System > Backup&Restore**.



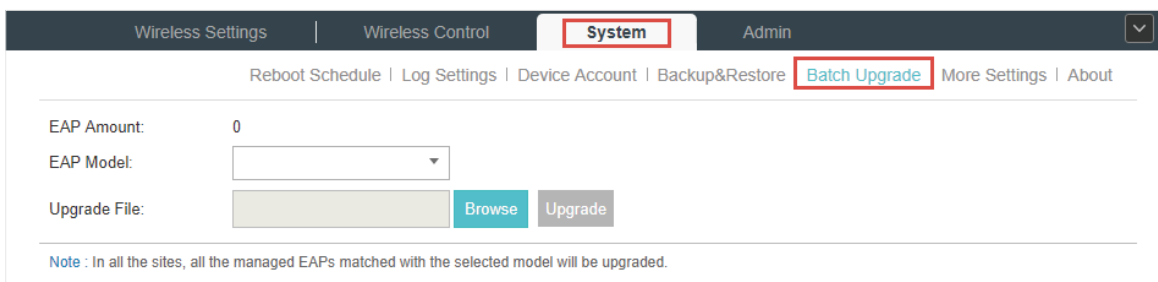
The screenshot shows the Omada Controller's web interface. The top navigation bar has tabs for 'Wireless Settings', 'Wireless Control', 'System' (highlighted with a red box), and 'Admin'. Below the navigation bar, there is a sub-menu with links: 'Reboot Schedule', 'Log Settings', 'Device Account', 'Backup&Restore' (highlighted with a red box), 'Batch Upgrade', 'More Settings', and 'About'. The main content area is titled 'Backup&Restore' and contains two sections: 'Backup' with a 'Backup' button, and 'Restore' with a 'Restore File:' label, a text input field, a 'Browse' button, and a 'Restore' button. A note at the bottom states: 'Note : The configurations in all the sites will be backed up or restored.'

2. Click **Backup** and save the backup file.
3. If necessary, click **Browse** to locate and choose the backup file. Then click **Restore** to restore the configuration.

### 3.8.5 Batch Upgrade

Follow the steps below to upgrade the EAP devices in batches 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 **System > Batch Upgrade**.



The screenshot shows the Omada Controller's web interface. The top navigation bar has tabs for 'Wireless Settings', 'Wireless Control', 'System' (highlighted with a red box), and 'Admin'. Below the navigation bar, there is a sub-menu with links: 'Reboot Schedule', 'Log Settings', 'Device Account', 'Backup&Restore', 'Batch Upgrade' (highlighted with a red box), 'More Settings', and 'About'. The main content area is titled 'Batch Upgrade' and contains three fields: 'EAP Amount:' with a value of '0', 'EAP Model:' with a dropdown menu, and 'Upgrade File:' with a text input field, a 'Browse' button, and an 'Upgrade' button. A note at the bottom states: 'Note : In all the sites, all the managed EAPs matched with the selected model will be upgraded.'

3. Select the EAP model.
4. Click **Browse** to locate and choose the proper firmware file for the model.
5. Click **Upgrade** to upgrade the device.
6. After upgrading, the device will reboot automatically.

**Note::**

To avoid damage, please do not turn off the device while upgrading.

## 3.8.6 More Settings

You can configure the following features on the **More Settings** page: Historical Data Retention, LED, SSH and Management VLAN.

Go to **System > More Settings**.

The screenshot shows the 'More Settings' page under the 'System' tab. The top navigation bar includes 'Wireless Settings', 'Wireless Control', 'System' (highlighted with a red box), and 'Admin'. Below the navigation bar, there are links for 'Reboot Schedule', 'Log Settings', 'Device Account', 'Backup&Restore', 'Batch Upgrade', 'More Settings' (highlighted with a red box), and 'About'. The main content area contains several configuration sections:

- Historical Data Retention:** A dropdown menu set to '365 days'. A note below states: '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.'
- LED:** A checkbox labeled 'Turn On' which is checked.
- SSH Server Port:** A text input field set to '22' with a range '(22, 1025-65535)'.
- SSH Login:** An unchecked checkbox.
- Management VLAN:** An unchecked checkbox labeled 'Enable'.
- Management VLAN ID:** A text input field set to '1' with a range '(1-4094)'. A note below states: '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.'

An 'Apply' button is located at the bottom left of the configuration area.

### Historical Data Retention

With this feature, logs and client statistics beyond the specified number of days will be cleared. Follow the steps below to configure Historical Data Retention:

1. Select the number of days beyond which logs and client statistics will be cleared.
2. Click **Apply**.

### LED

Follow the steps below to turn on or off the LED lights of the EAPs.

1. Check the box to change the LED light status. By default, the LED lights are on.
2. Click **Apply**.

## SSH

You can log in to the Omada Controller via SSH. Follow the steps below to configure SSH on the Omada Controller:

1. Enter the port number of the SSH server.
2. Check the box to enable SSH Login.
3. Click **Apply**.

## 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. Check the box to enable Management VLAN.
2. Specify the Management VLAN ID.
3. Click **Apply**.

## 4 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.

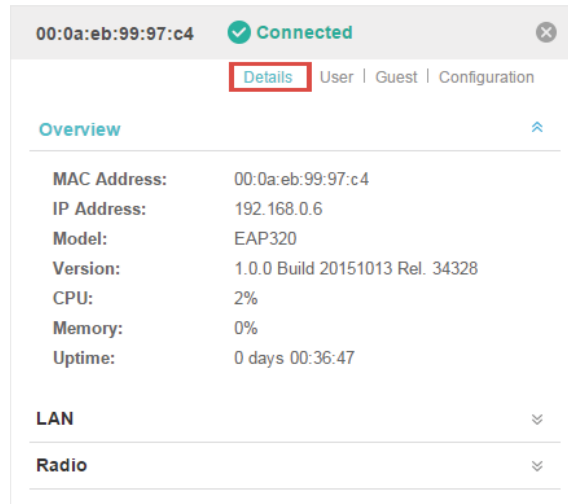
This chapter includes the following contents:

- *View the Information of the EAP*
- *View Clients Connecting to the EAP*
- *Configure the EAP*

## 4.1 View the Information of the EAP

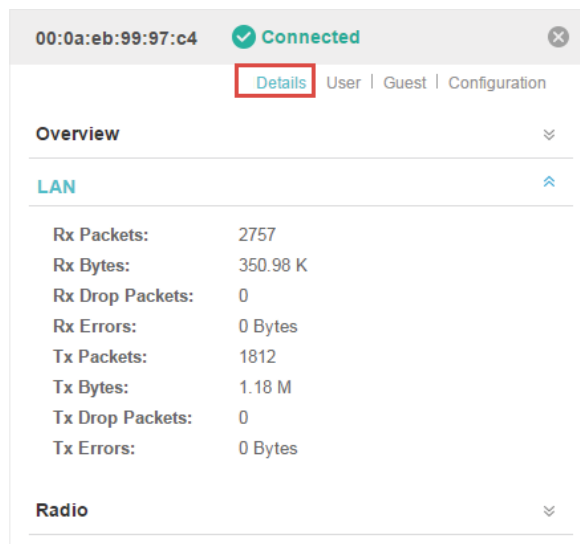
### 4.1.1 Overview

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).



### 4.1.2 LAN

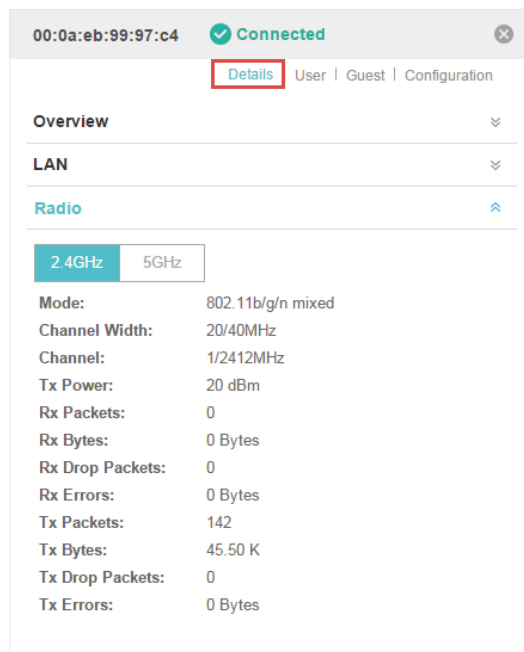
Click **LAN** to view the traffic information of the LAN port, including the total number of packets, the total size of data, the total number of packets loss, and the total size of error data in the process of receiving and transmitting data.





### 4.1.3 Radio

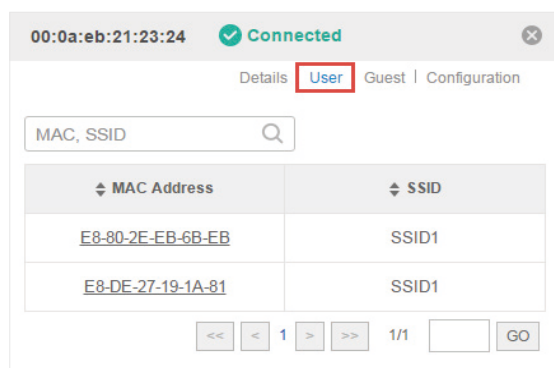
Click **Radio** to view the radio information including the frequency band, the wireless mode, the channel width, the channel, and the transmitting power. At 2.4GHz, you can also view parameters of receiving/transmitting data.



## 4.2 View Clients Connecting to the EAP

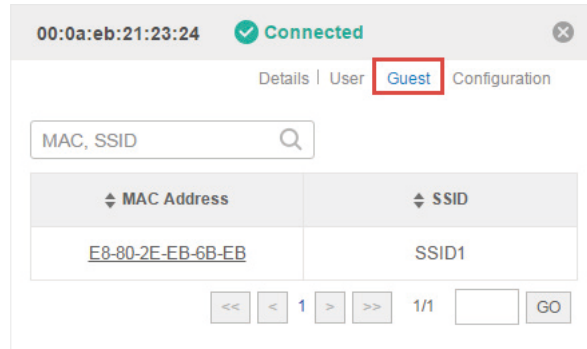
### 4.2.1 User

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.



## 4.2.2 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.



00:0a:eb:21:23:24 Connected

Details | User **Guest** | Configuration

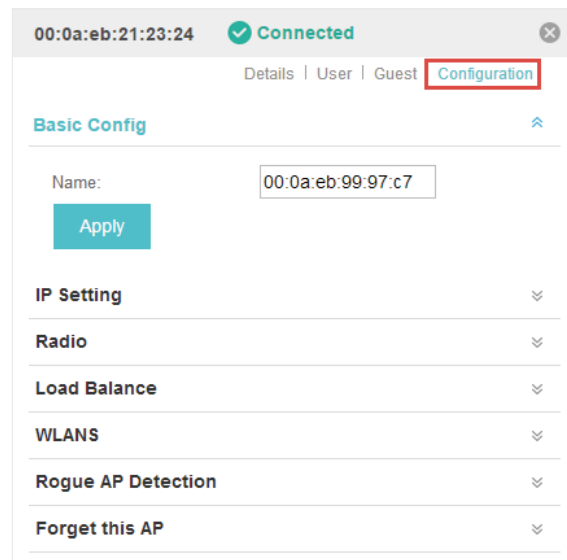
MAC, SSID

MAC Address	SSID
<a href="#">E8-80-2E-EB-6B-EB</a>	SSID1

<< < 1 > >> 1/1 GO

## 4.3 Configure the EAP

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



00:0a:eb:21:23:24 Connected

Details | User | Guest **Configuration**

**Basic Config**

Name: 00:0a:eb:99:97:c7

Apply

IP Setting

Radio

Load Balance

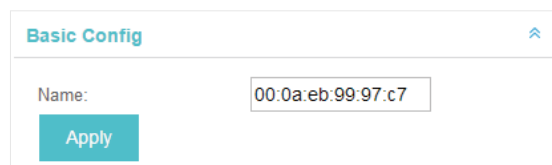
WLANS

Rogue AP Detection

Forget this AP

### 4.3.1 Basic Config

Here you can change the name of the EAP.



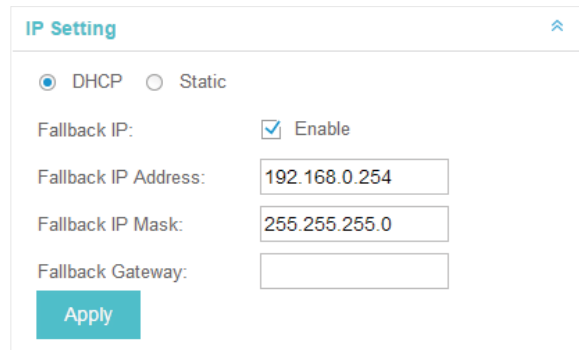
**Basic Config**

Name: 00:0a:eb:99:97:c7

Apply

## 4.3.2 IP Setting

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



The IP Setting window has a title bar with 'IP Setting' and a close button. It contains two radio buttons: 'DHCP' (selected) and 'Static'. Below these are four fields: 'Fallback IP' with a checked 'Enable' checkbox, 'Fallback IP Address' with the value '192.168.0.254', 'Fallback IP Mask' with the value '255.255.255.0', and 'Fallback Gateway' which is empty. An 'Apply' button is at the bottom left.

### Get a Dynamic IP Address From the DHCP Server

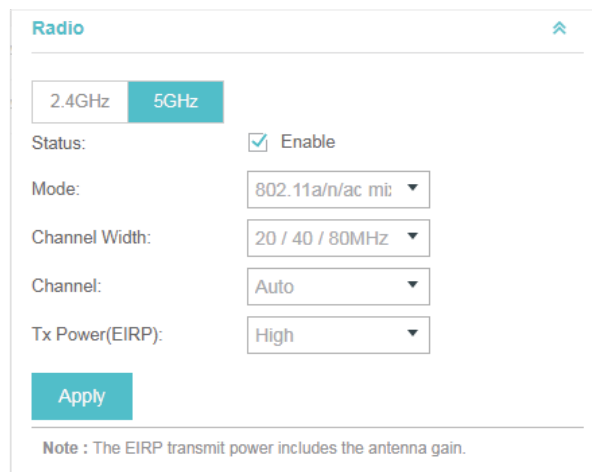
1. Configure your DHCP server.
2. Select **DHCP** on the page above.
3. Enable the Fallback IP feature. When the device cannot get a dynamic IP address, the fallback IP address will be used.
4. Set IP address, IP mask and gateway for the fallback address and click **Apply**.

### 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**.

## 4.3.3 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.



The Radio window has a title bar with 'Radio' and a close button. It features two tabs: '2.4GHz' and '5GHz' (selected). Below the tabs are five fields: 'Status' with a checked 'Enable' checkbox, 'Mode' with a dropdown menu showing '802.11a/n/ac m...', 'Channel Width' with a dropdown menu showing '20 / 40 / 80MHz', 'Channel' with a dropdown menu showing 'Auto', and 'Tx Power(EIRP)' with a dropdown menu showing 'High'. An 'Apply' button is at the bottom left. A note at the bottom states: '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	<p>Select the IEEE 802.11 mode the radio uses.</p> <p>When the frequency of 2.4GHz is selected, 802.11b/g/n mixed, 802.11b/g mixed, and 802.11n only modes are available:</p> <p><b>802.11b/g/n mixed:</b> 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.</p> <p><b>802.11b/g mixed:</b> Both 802.11b and 802.11g clients can connect to the EAP device.</p> <p><b>802.11n only:</b> Only 802.11n clients can connect to the EAP device.</p> <p>When the frequency of 5GHz is selected, 802.11 n/ac mixed, 802.11a/n mixed, 802.11 ac only, 802.11a only, and 802.11n only modes are available:</p> <p><b>802.11n/ac mixed:</b> Both 802.11n clients and 802.11ac clients operating in the 5GHz frequency can connect to the EAP device.</p> <p><b>802.11a/n mixed:</b> Both 802.11a clients and 802.11n clients operating in the 5GHz frequency can connect to the EAP device.</p> <p><b>802.11ac only:</b> Only 802.11ac clients can connect to the EAP device.</p> <p><b>802.11a only:</b> Only 802.11a clients can connect to the EAP device.</p> <p><b>802.11n only:</b> Only 802.11n clients can connect to the EAP device.</p>
Channel Width	<p>Select the channel width of the EAP device. The available options differ among different EAPs.</p> <p>For some EAPs, available options include <b>20MHz, 40MHz</b> and <b>20/40MHz</b>.</p> <p>For other EAPs, available options include <b>20MHz, 40MHz, 80MHz</b> and <b>20/40/80MHz</b>.</p> <p>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.</p>
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.
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.

#### 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 Max TxPower (maximum transmit power. It may vary among different countries and regions).

**Low:** Max TxPower \* 20% (round off the value)

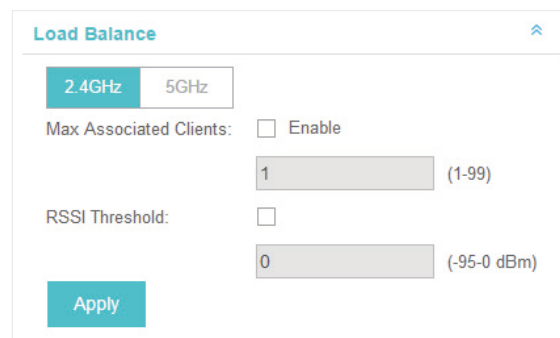
**Medium:** Max TxPower \* 60% (round off the value)

**High:** Max TxPower

**Custom:** Enter a value manually.

### 4.3.4 Load Balance

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



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

#### Max Associated Clients

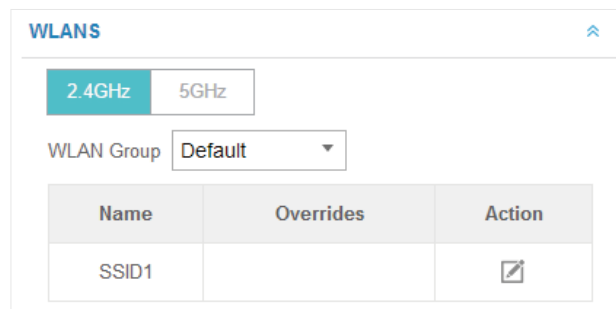
Enable this function and specify the maximum number of connected clients. While more clients requesting to connect, the EAP will disconnect those with weaker signals.

#### 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.

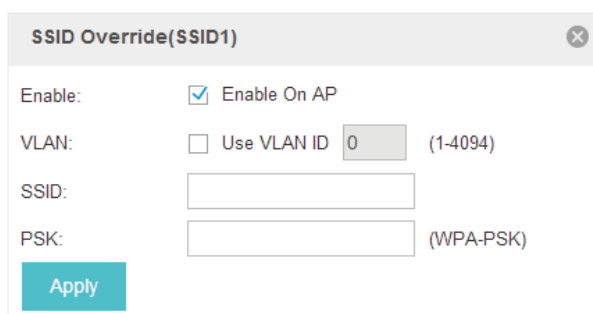
### 4.3.5 WLANs

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.



1. Select the frequency band and WLAN group.

2. Click  and the following window will pop up.



The image shows a configuration window titled "SSID Override(SSID1)". It contains the following fields and options:

- Enable:** A checkbox labeled "Enable On AP" which is checked.
- VLAN:** A checkbox labeled "Use VLAN ID" which is unchecked. To its right is a text input field containing "0" and a range "(1-4094)".
- SSID:** A text input field.
- PSK:** A text input field with "(WPA-PSK)" displayed to its right.
- Apply:** A blue button at the bottom left.

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.

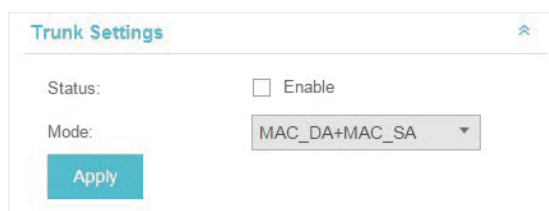
5. Specify a new name and password for the SSID.

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

### 4.3.6 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.




The image shows a configuration window titled "Trunk Settings". It contains the following fields and options:

- Status:** A checkbox labeled "Enable" which is unchecked.
- Mode:** A dropdown menu currently showing "MAC\_DA+MAC\_SA".
- Apply:** A blue button at the bottom left.

Status	<p>Enable this function.</p> <p>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).</p>
Mode	<p>Select the applied mode of Trunk Arithmetic.</p> <ul style="list-style-type: none"><li>• SRC MAC + DST MAC: When this option is selected, the arithmetic will be based on the source and destination MAC addresses of the packets.</li><li>• DST MAC: When this option is selected, the arithmetic will be based on the destination MAC addresses of the packets.</li><li>• SRC MAC: When this option is selected, the arithmetic will be based on the source MAC addresses of the packets.</li></ul>

### 4.3.7 Rogue AP Detection

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


Rogue AP Detection 

Rogue Status: ☐ Enable ☒ Disable

Apply

## 4.3.8 Local LAN Port Settings

You can configure the LAN port of the EAP.

Local LAN Port Settings 

ETH1:  
VLAN ☐ Enable

ETH2:  
VLAN ☐ Enable


ETH3:  
PoE Out ☐ Enable  
VLAN ☐ Enable

Apply

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.

## 4.3.9 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.

Forget

# 5

## **Manage the Omada Controller**

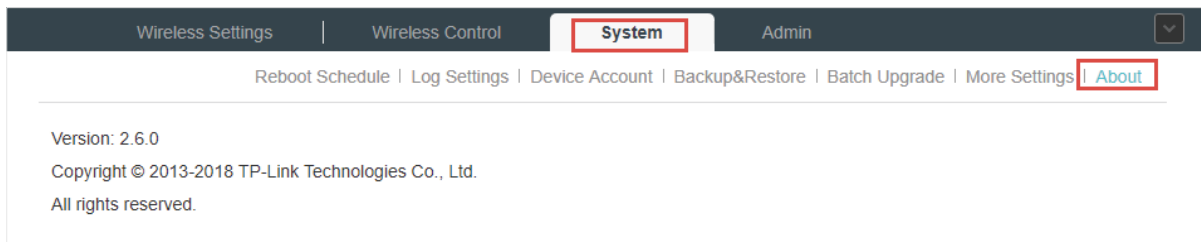
This chapter mainly introduces how to manage the user account and configure system settings. This chapter includes the following contents.

- *Information About the Software*
- *User Account*
- *Controller Settings*



## 5.1 Information About the Software

You can view the Omada Controller's version and copyright information on the **About** page.



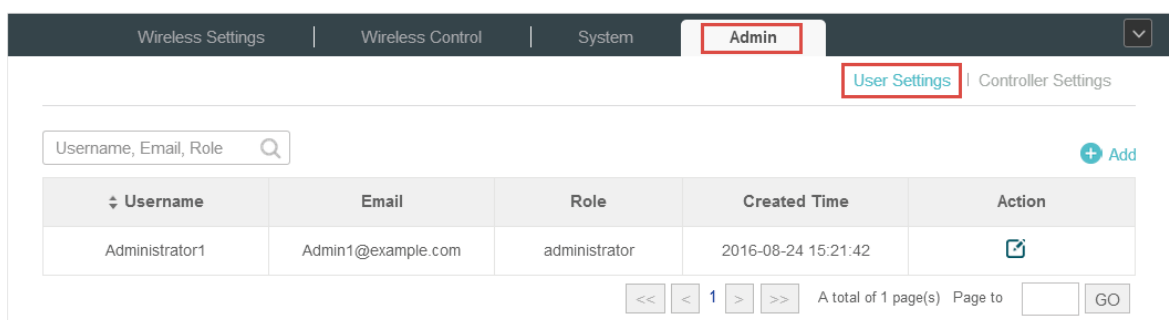
## 5.2 User Account

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

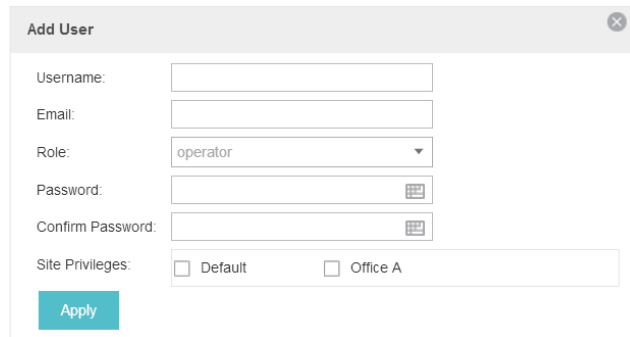
Administrator	The first administrator account is created in the Basic Configuration process and this account can not be deleted. An administrator can change the settings of the EAP network and create and delete user accounts.
Operator	An operator account can be created or deleted by the administrator. 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 **Admin > User Settings**.



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



**Add User**

Username:

Email:

Role:

Password:

Confirm Password:

Site Privileges: ☐ Default ☐ Office A

**Apply**

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.

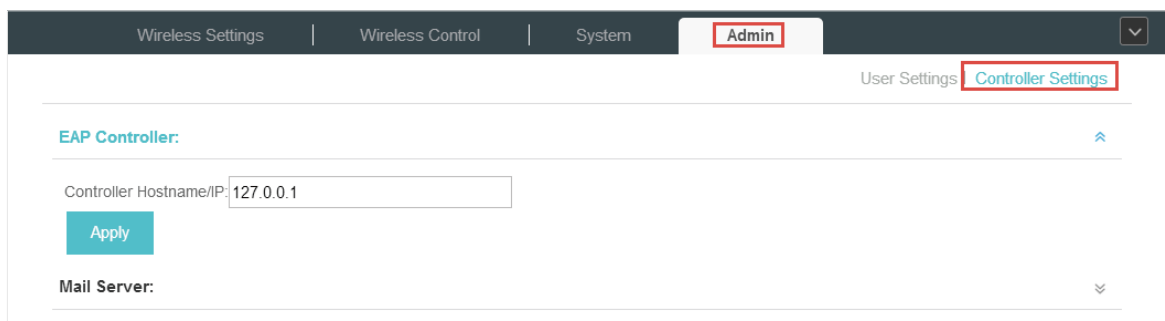
## 5.3 Controller Settings

You can configure the Omada Controller's hostname and IP address. In addition, we recommend you configure the Mail server to reset your login password when you forget it.

### 5.3.1 Configure Controller Hostname/IP

Follow the steps below to configure the hostname or IP address of the Omada Controller.

1. Go to **Admin > Controller Settings** and click **Omada Controller**.



Wireless Settings | Wireless Control | System | **Admin**

User Settings | **Controller Settings**

**EAP Controller:**

Controller Hostname/IP:

**Apply**

**Mail Server:**

2. Enter the hostname or IP address of the Omada Controller.

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

## 5.3.2 Configure Mail Server

With the Mail Server, you can reset the password of the user account and receive notifications from the Omada Controller. 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 **Admin > Controller Settings**.
2. Click **Mail Server**, check the box to enable SMTP Server, and then the following screen will appear.

The screenshot shows the Omada Controller Admin interface. The top navigation bar has 'Admin' selected. Below it, 'Controller Settings' is selected. The 'Mail Server' section is expanded, showing the following configuration options:

- ☒ Enable SMTP Server
- Mail Server: [Text Field]
- Port: [Text Field with value 25]
- ☐ Enable SSL
- ☐ Enable Auth
- Username: [Text Field]
- Password: [Text Field]
- Specify Sender Address: [Text Field]
- [Apply Button]

3. Configure the following parameters.

Mail Server	Enter the IP address or domain of SMTP Server.
Port	The default is 25.  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	Select this option to enable authentication.
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 of the warning email.

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

### Note:

Specify the account email address based on the Mail server to receive the notifications.

## 6 *Application Example*

A restaurant has a wireless network with three EAPs managed by the Omada Controller. The network administrator wants to :

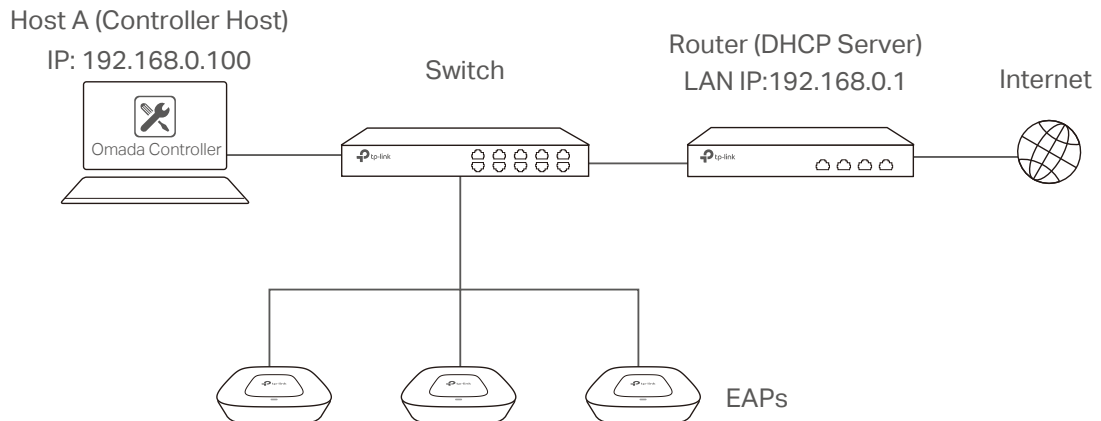
- Monitor the EAPs with the Map.
- Enable Portal function to drive customers' attention to the ads of the supermarket when customers attempt to access the network. The costumers need to use a simple password to pass the authentication.
- Allow the employees of the restaurant to access the network resources 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.

## 6.1 Basic Configuration

Follow the steps below to do the basic configuration.

1. Connect the hardware by referring to the following topology.



2. Install the Omada Controller on Host A.
3. Launch the software and follow the instructions to complete some initial configurations.
4. Log into the management interface.
5. Adopt the pending EAP devices.

## 6.2 Advanced Settings

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

### 6.2.1 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.



## 6.2.2 Configure Portal Authentication

Follow the steps below to configure Portal function.

1. Go to **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 **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:

SSID:

Authentication Type:

Password:

Authentication Timeout:

HTTPS Redirect: ☒ Enable

Redirect: ☒ Enable

Redirect URL:

- 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.

**Login Page**

Background: ☒ Solid Color ☐ Picture

Background Color:  (RGB value)

Background Color:

Logo Picture:

Welcome Information:  (1-31 characters)

Copyright:  (1-200 characters)

Terms of Service: ☐ Enable

Input Box: ☒

Button: ☒

PC Mobile Phone Tablet PC

Welcome to our restaurant

Copyright 2018

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

6. Click **Apply**.

### 6.2.3 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 **Basic Wireless Settings**.
2. Click **Add** to add a new SSID.

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.

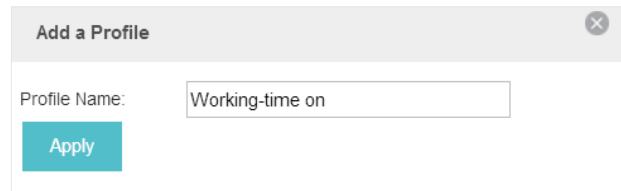


## 6.2.4 Configure Scheduler

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

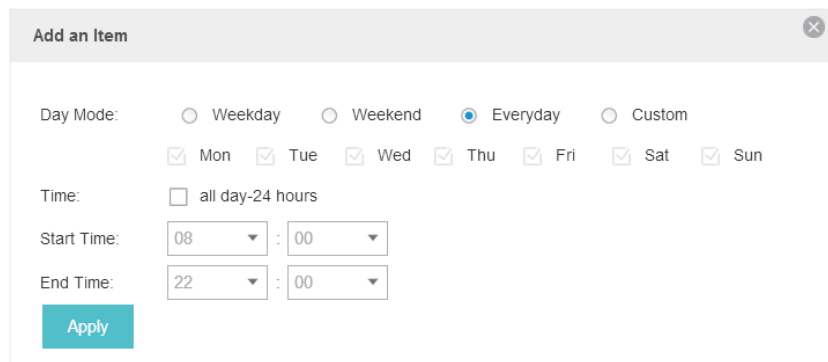
1. Open the global configuration window and go to **Scheduler**.

1) Add a profile.



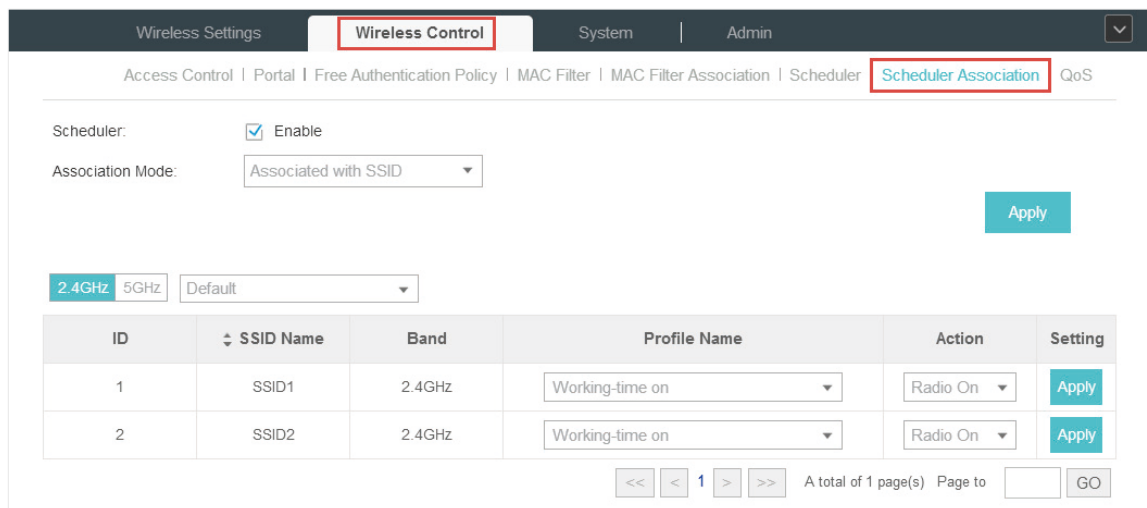
The 'Add a Profile' dialog box has a title bar with a close button. It contains a 'Profile Name' label and a text input field with the value 'Working-time on'. Below the input field is a teal 'Apply' button.

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



The 'Add an Item' dialog box has a title bar with a close button. It contains the following settings: 'Day Mode' with radio buttons for 'Weekday', 'Weekend', 'Everyday' (selected), and 'Custom'; a row of checkboxes for days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) all of which are checked; 'Time' with an unchecked checkbox for 'all day-24 hours'; 'Start Time' with dropdowns for '08' and '00'; and 'End Time' with dropdowns for '22' and '00'. A teal 'Apply' button is at the bottom.

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



The 'Scheduler Association' page is part of the 'Wireless Control' tab. It has a breadcrumb trail: 'Access Control | Portal | Free Authentication Policy | MAC Filter | MAC Filter Association | Scheduler | Scheduler Association | QoS'. The 'Scheduler' section has a checked 'Enable' checkbox and an 'Association Mode' dropdown set to 'Associated with SSID'. A teal 'Apply' button is to the right. Below this is a band selector with '2.4GHz' selected, '5GHz' as an option, and a 'Default' dropdown. A table lists two SSIDs, both associated with the 'Working-time on' profile and set to 'Radio On'. Each row has an 'Apply' button in the 'Setting' column.

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.