



User Guide

Omada Controller Software

1910012394 REV 2.7.0

July 2018

CONTENTS

1 Quick Start	1
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	5
1.4 Start and Log In to the Omada Controller	6
1.4.1 Launch Omada Controller	6
1.4.2 Do the Basic Configurations	7
1.4.3 Log In to the Management Interface	8
1.5 Create Sites and Adopt EAPs	9
1.5.1 Create Sites	9
1.5.2 Adopt the EAPs	9
1.6 Monitor and Manage the EAPs	11
2 Monitor and Manage the Network	12
2.1 Monitor the Network with the Map	13
2.1.1 Add a Map	13
2.1.2 Monitor the EAPs on the Map	15
2.2 View the Statistics of the Network	16
2.2.1 View the Client Distribution on SSID	17
2.2.2 Have a Quick Look at EAPs and Clients	17
2.2.3 View Current Usage-Top EAPs	18
2.2.4 View Recent Activities	18
2.3 Monitor and Manage the EAPs	19
2.3.1 Manage the EAPs in Different Status	19
2.3.2 View the Detailed Information of EAPs	20
2.3.3 Manage the EAPs in the Action Column	20

2.4	Monitor and Manage Clients	22
2.4.1	View the Current Information of Clients	22
2.4.2	Manage Clients in the Action Column.....	22
2.5	View Clients Statistics During the Specified Period	23
2.5.1	Select a Specified Period	23
2.5.2	View the History Information of Clients	24
2.5.3	Manage Clients in the Action Column.....	24
2.6	Manage the Rogue APs List	24
2.6.1	Manage the Untrusted Rogue APs List	25
2.6.2	Manage the Trusted Rogue APs List.....	25
2.7	View Past Guest Authorization	26
2.8	View Logs	27
2.9	View Alerts	27
3	Configure the EAPs Globally	29
3.1	Wireless Network	30
3.1.1	Add Wireless Networks	30
3.1.2	Configure Advanced Wireless Parameters	35
3.1.3	Configure Band Steering	37
3.1.4	Configure Mesh.....	38
3.2	Access Control	42
3.3	Portal Authentication	43
3.3.1	No Authentication.....	44
3.3.2	Simple Password	48
3.3.3	Local User.....	52
3.3.4	Voucher	60
3.3.5	SMS.....	68
3.3.6	Facebook.....	73
3.3.7	External RADIUS Server	74
3.3.8	External Portal Server	79

3.4	Free Authentication Policy	80
3.5	MAC Filter	81
3.6	Scheduler	83
3.7	QoS.....	85
3.8	System	88
3.8.1	Reboot Schedule	88
3.8.2	Log Setting.....	89
3.8.3	Device Account.....	90
3.8.4	Backup&Restore	91
3.8.5	Batch Upgrade.....	91
3.8.6	More Settings.....	92
4	Configure the EAPs Separately	94
4.1	View the Information of the EAP.....	95
4.1.1	Overview	95
4.1.2	LAN.....	95
4.1.3	Radio.....	96
4.2	View Clients Connecting to the EAP	96
4.2.1	User.....	96
4.2.2	Guest	97
4.3	View Mesh Information of the EAP	97
4.3.1	Uplinks	97
4.3.2	Downlinks	98
4.4	Configure the EAP	98
4.4.1	Basic Config.....	98
4.4.2	IP Setting.....	99
4.4.3	Radio.....	100
4.4.4	Load Balance.....	101
4.4.5	WLANs	102
4.4.6	Trunk Settings.....	103

4.4.7	Rogue AP Detection	103
4.4.8	Local LAN Port Settings.....	104
4.4.9	Forget this AP	104
5	Manage the Omada Controller	105
5.1	Information About the Software.....	106
5.2	User Account.....	106
5.3	Controller Settings	107
5.3.1	Configure Controller Hostname/IP	107
5.3.2	Configure Mail Server	108
6	Application Example	110
6.1	Basic Configuration.....	111
6.2	Advanced Settings	111
6.2.1	Monitor the EAPs with Map.....	111
6.2.2	Configure Portal Authentication	112
6.2.3	Create a SSID for the Employees	114
6.2.4	Configure Scheduler	115

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:

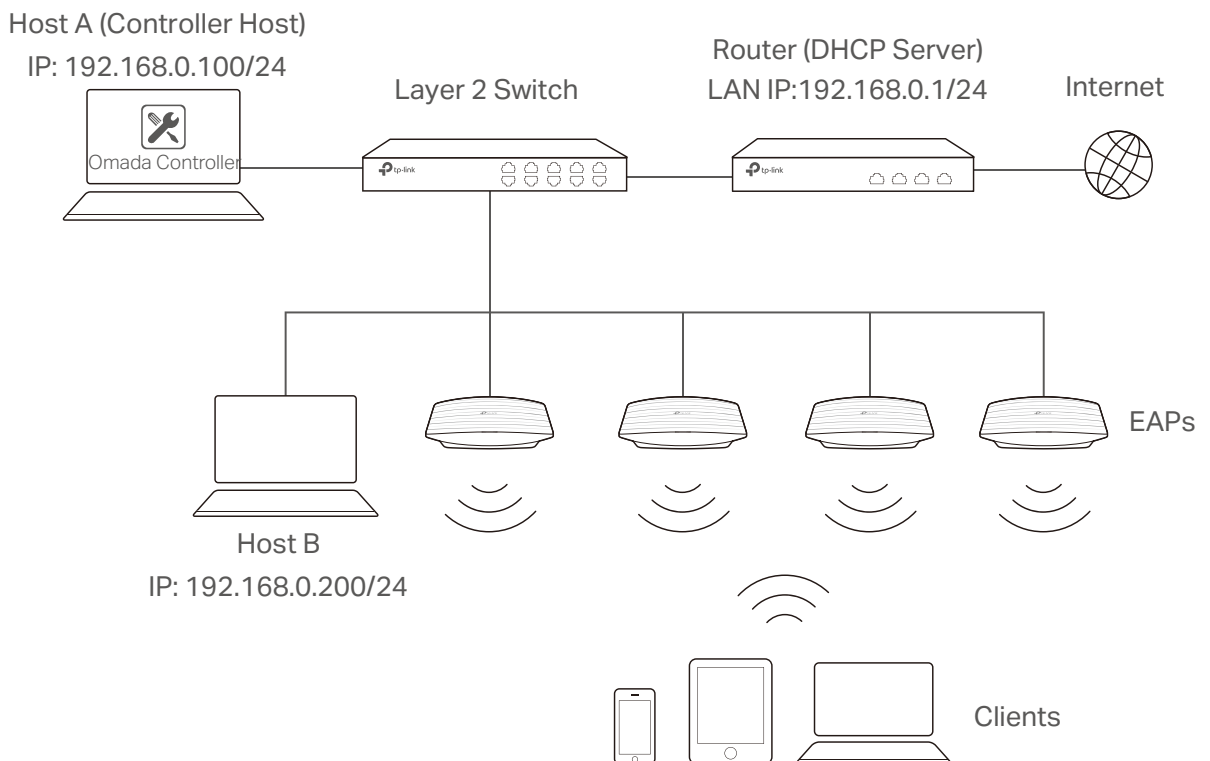
- Omada Controller and EAPs are in the same subnet.
- Omada Controller and EAPs are in different subnets.

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.



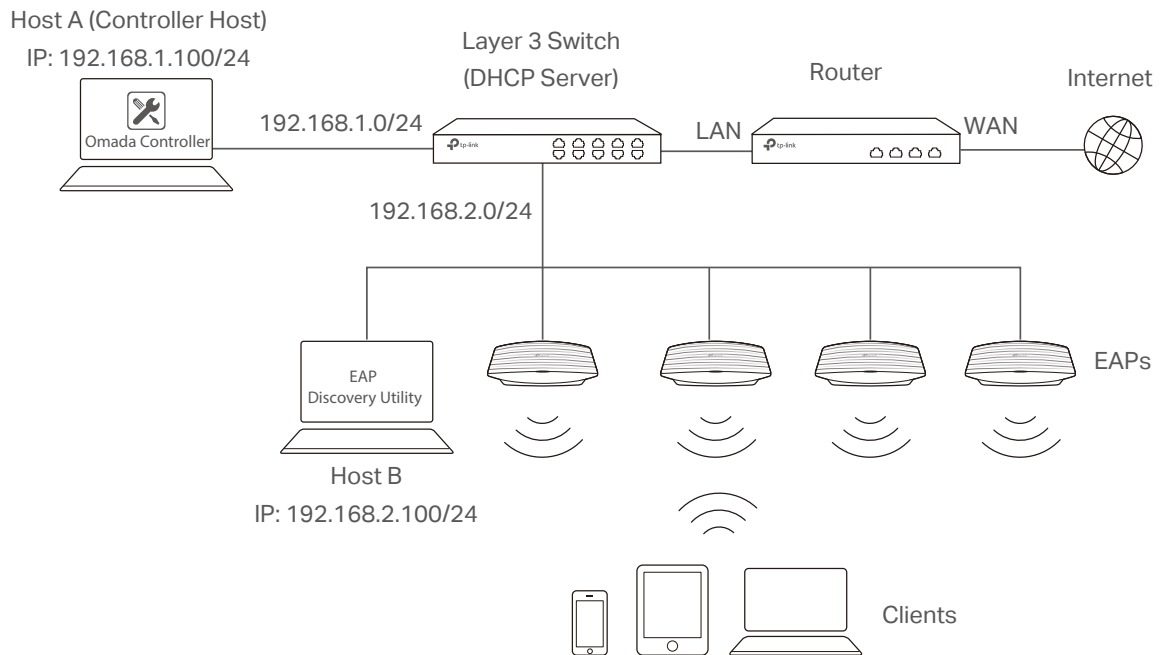
Note:

- 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, Omada Discover Utility should be installed on Host B which is in the same subnet with the EAPs. For how to use Omada Discover 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 Omada Discovery Utility on a host that is in the same network segment with the EAPs. Omada Discovery Utility can help EAPs find the Controller Host.

System Requirements

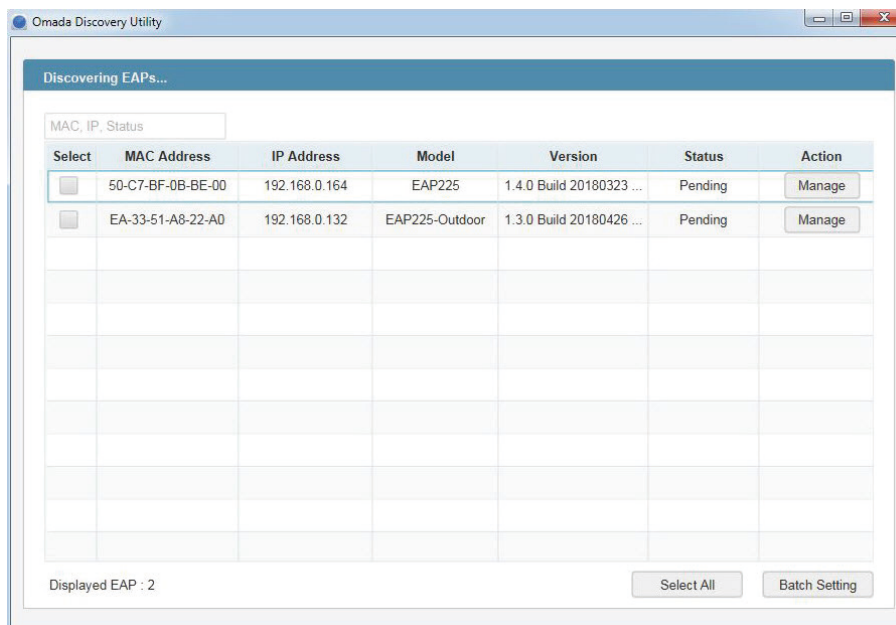
Windows 7/8//10/Server

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

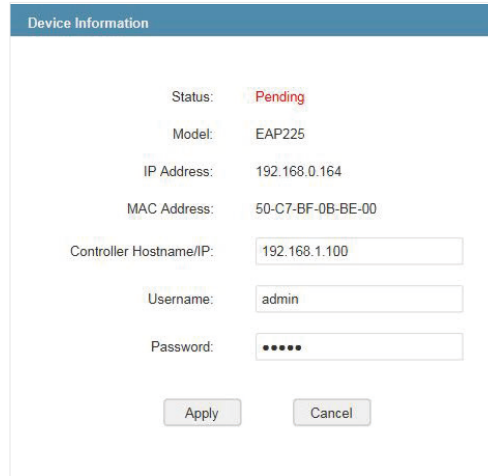
Install and Use Omada Discovery Utility

Follow the steps below to install Omada 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. Then follow the instructions to properly install Omada Discovery Utility.
2. Open the Omada Discovery Utility and the following window will pop up. This window shows the information of all EAPs in the same LAN.



3. Click **Manage** in the **Action** column or select multiple EAPs and click **Batch Setting**.
4. Enter the hostname or IP address of the Controller Host.
5. Enter the EAP's username and password (both are admin by default).



The image shows a 'Device Information' dialog box with the following fields and values:

Status:	Pending
Model:	EAP225
IP Address:	192.168.0.164
MAC Address:	50-C7-BF-0B-BE-00
Controller Hostname/IP:	<input type="text" value="192.168.1.100"/>
Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="•••••"/>


Buttons: Apply, Cancel

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**.

<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**.

SSID: (1-32 characters)

Password: (WPA2-PSK)

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 Omada 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 as the outbox 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

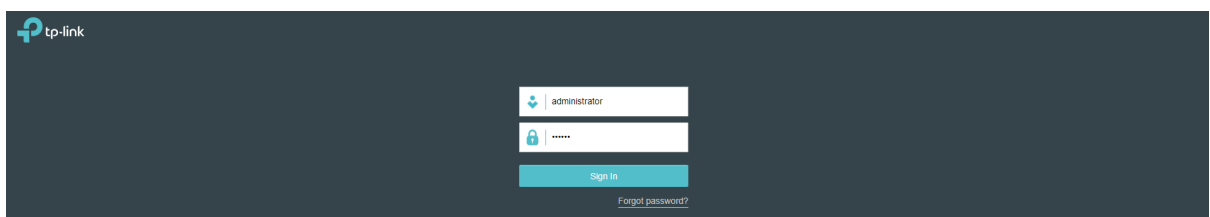
Admin Name: admin

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.

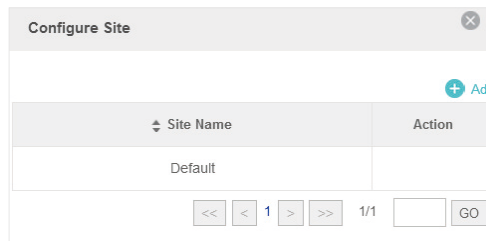
1.5 Create Sites and Adopt EAPs

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.

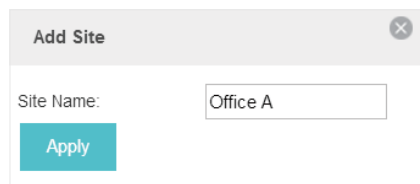
1.5.1 Create Sites

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.

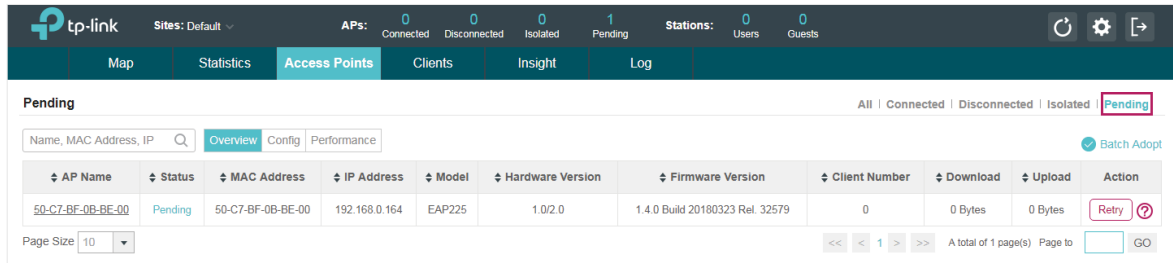
1.5.2 Adopt the EAPs

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:

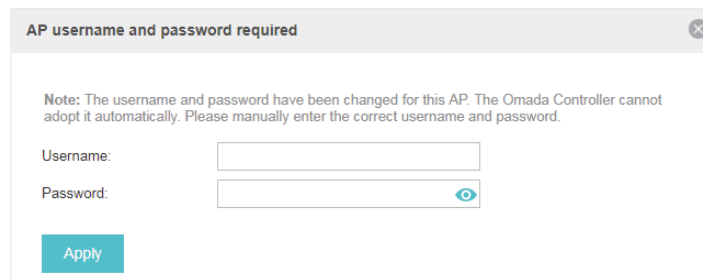
1. Select a site and go to **Access Points > Pending**. The table displays all the EAPs that have not been adopted.



The screenshot shows the Omada Controller interface. At the top, there are navigation tabs: Map, Statistics, Access Points, Clients, Insight, and Log. The 'Access Points' tab is selected. Below the navigation, there are statistics for APs: 0 Connected, 0 Disconnected, 0 Isolated, and 1 Pending. There are also statistics for Stations: 0 Users and 0 Guests. The main content area is titled 'Pending' and has a search bar and tabs for Overview, Config, and Performance. A 'Batch Adopt' button is visible. Below this is a table with the following columns: AP Name, Status, MAC Address, IP Address, Model, Hardware Version, Firmware Version, Client Number, Download, Upload, and Action. The table contains one row with the following data: AP Name: 50-C7-BF-0B-BE-00, Status: Pending, MAC Address: 50-C7-BF-0B-BE-00, IP Address: 192.168.0.164, Model: EAP225, Hardware Version: 1.0/2.0, Firmware Version: 1.4.0 Build 20180323 Rel. 32579, Client Number: 0, Download: 0 Bytes, Upload: 0 Bytes, and Action: Retry (with a help icon). 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) Page to [] GO'.

AP Name	Status	MAC Address	IP Address	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
50-C7-BF-0B-BE-00	Pending	50-C7-BF-0B-BE-00	192.168.0.164	EAP225	1.0/2.0	1.4.0 Build 20180323 Rel. 32579	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**.



The dialog box is titled 'AP username and password required'. It contains a note: '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.' Below the note are two input fields: 'Username:' and 'Password:'. The 'Password:' field has an eye icon to toggle visibility. At the bottom of the dialog is an 'Apply' button.

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.

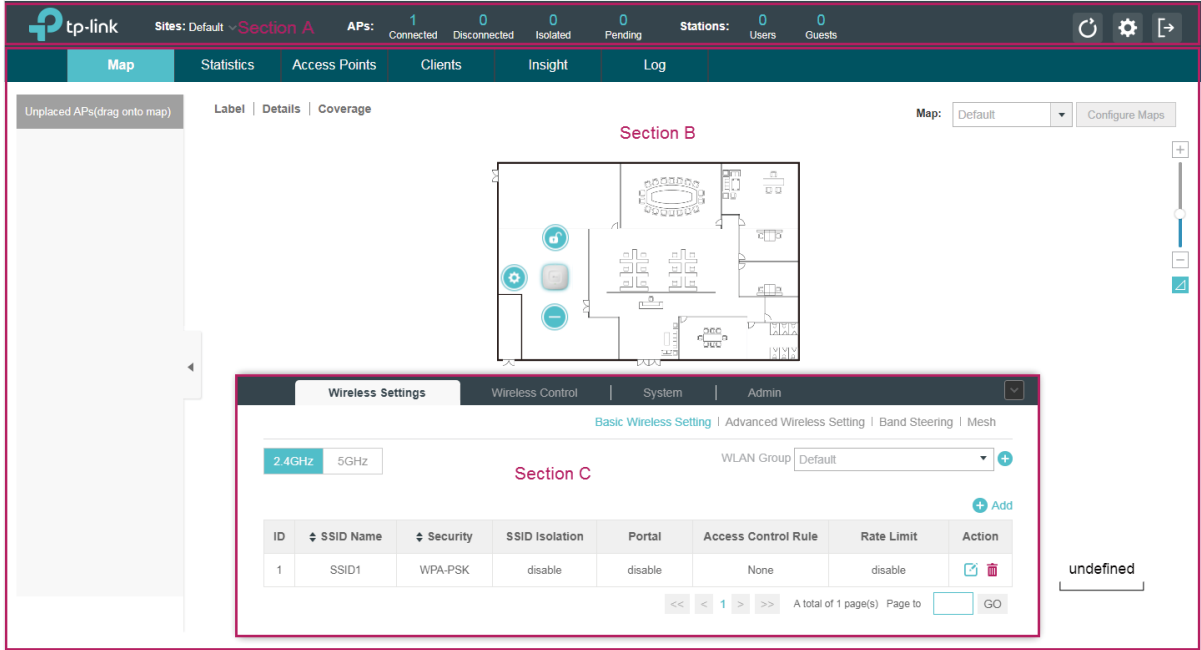
3. After EAPs are adopted, the status will change from Pending to **Connected**. All the EAPs' username and password will become the same as those of the Controller's administrator account you created in the [Basic Configuration](#).

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

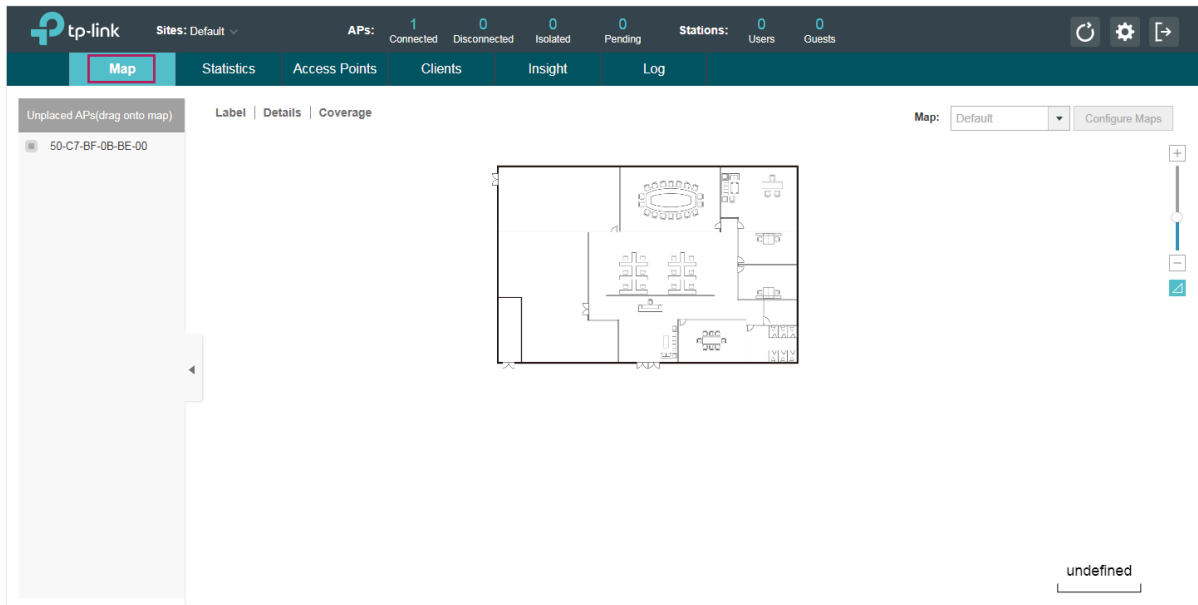
Monitor and Manage the Network

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

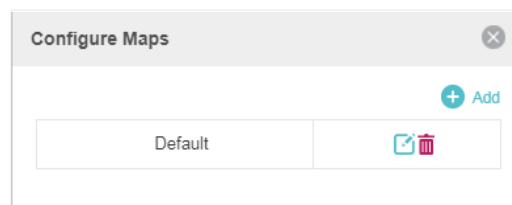
You can upload your local map images and monitor the status and coverage range of each EAP with the map. When you initially launch Omada Controller, a default map is displayed as the following figure shows. Follow the instructions below to add your own map and manage the EAPs via the map.



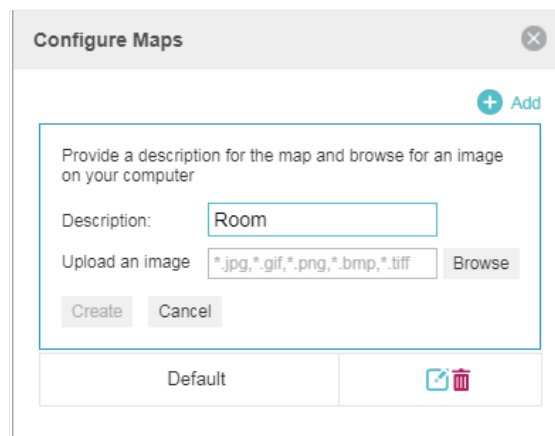
2.1.1 Add a Map

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**.




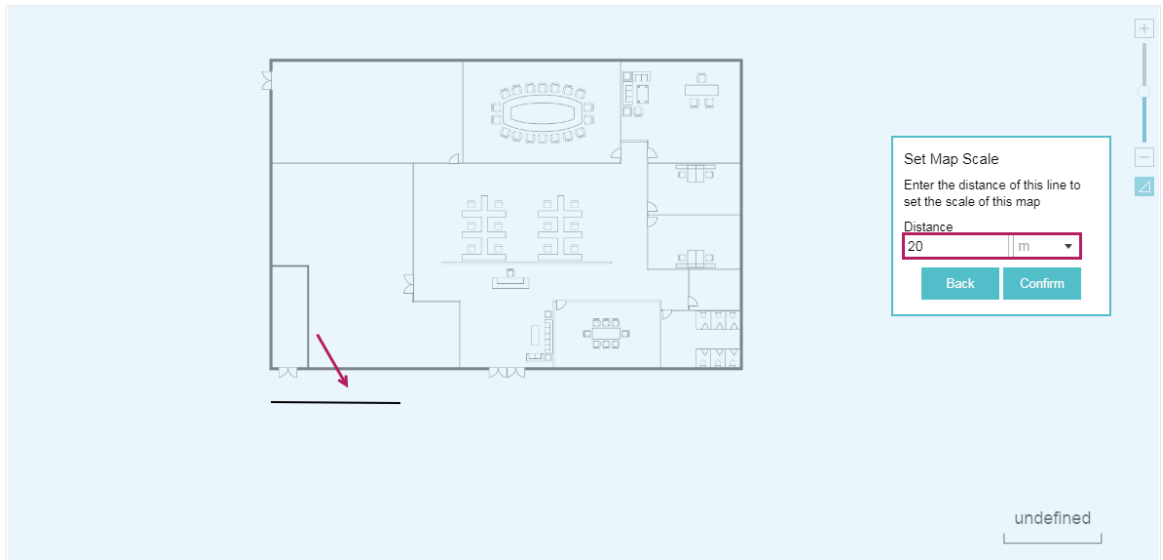
2. Enter the map description, select your map image, and click **Create**.



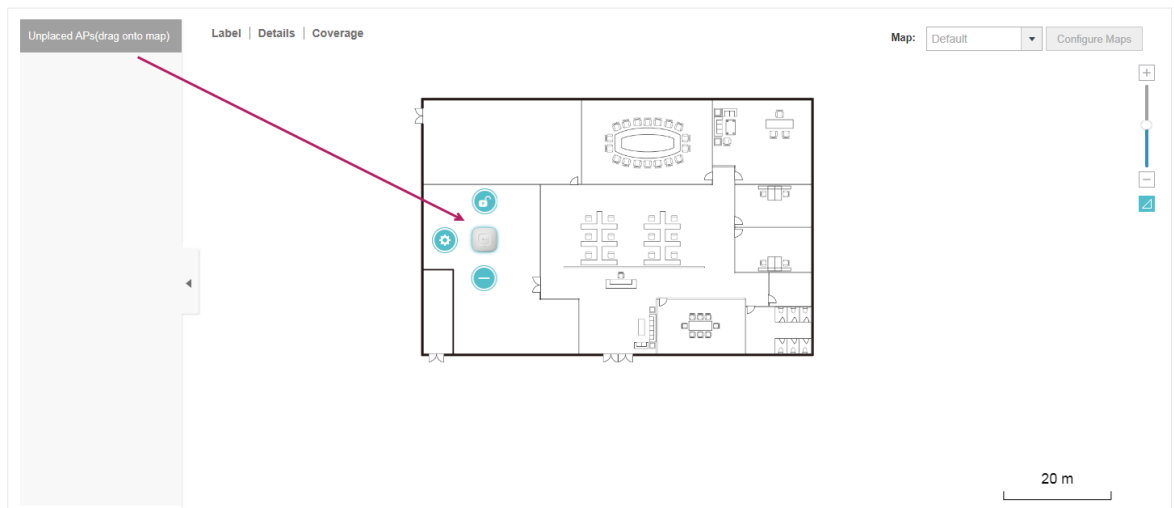
3. Select your local map from the drop-down list on the upper right corner of map area.



4. 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.







5. 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 Configure the EAPs Separately .
	Remove the selected EAP back into the Unplaced APs list.

2.1.2 Monitor the EAPs on the Map

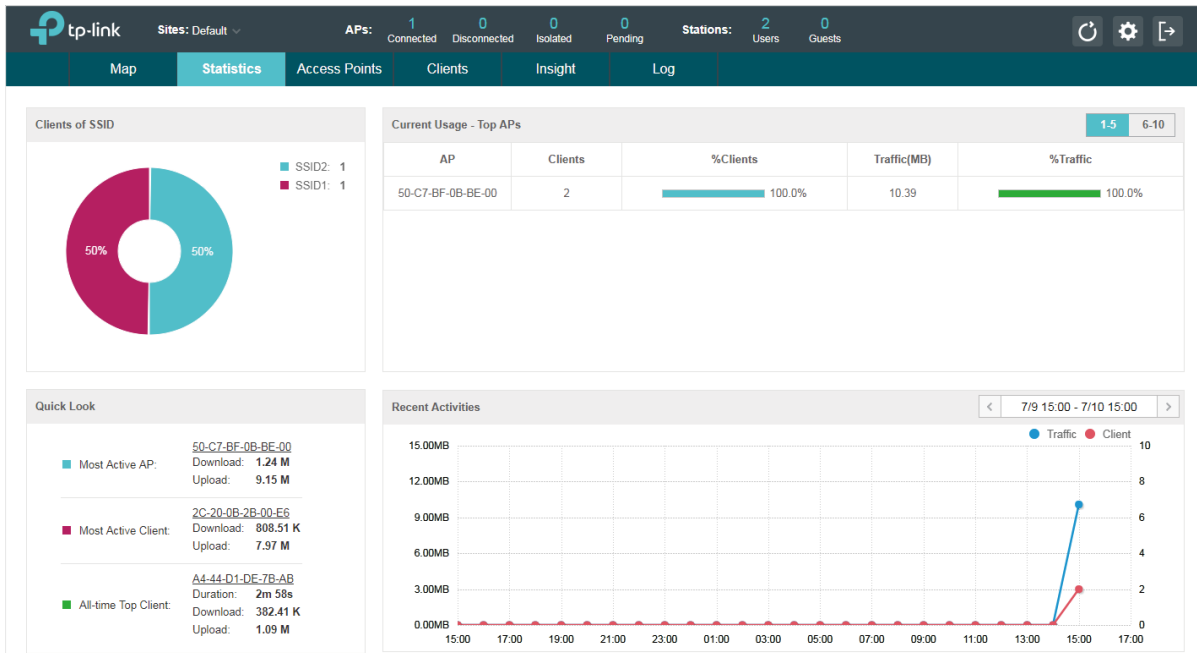
Click any of the following options to display EAP Label, Details, and Coverage on the map.

Label | Details | Coverage

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

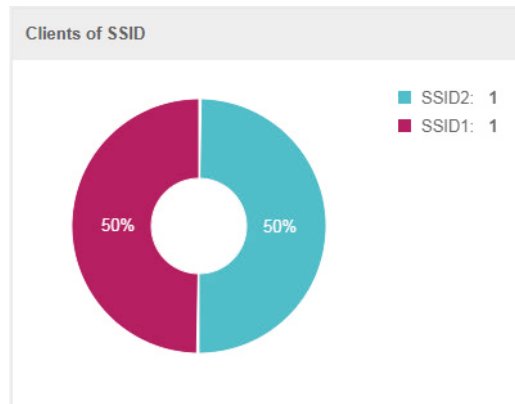
2.2 View the Statistics of the Network

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:	50-C7-BF-0B-BE-00 Download: 1.24 M Upload: 9.15 M
■ Most Active Client:	2C-20-0B-2B-00-E6 Download: 808.51 K Upload: 7.97 M
■ All-time Top Client:	A4-44-D1-DE-7B-AB Duration: 2m 58s Download: 382.41 K Upload: 1.09 M

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

2.2.3 View Current Usage-Top EAPs

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

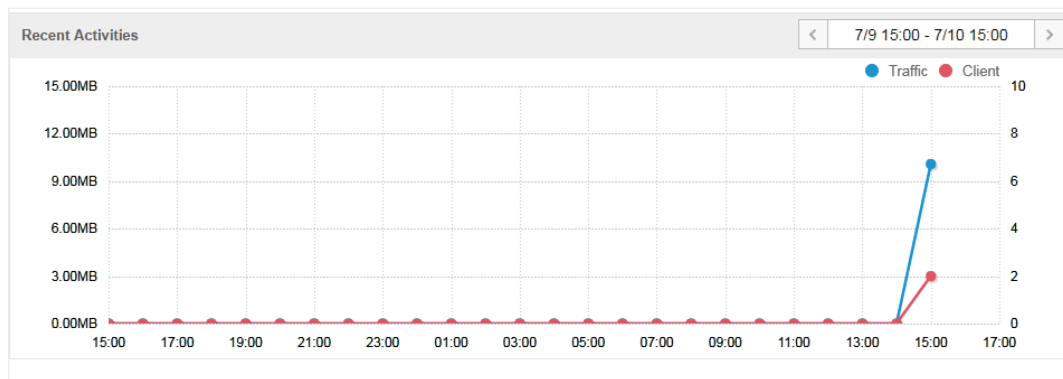
Current Usage - Top APs				
AP	Clients	%Clients	Traffic(MB)	%Traffic
50-C7-BF-0B-BE-00	2	<div style="width: 100.0%;"></div> 100.0%	10.39	<div style="width: 100.0%;"></div> 100.0%

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

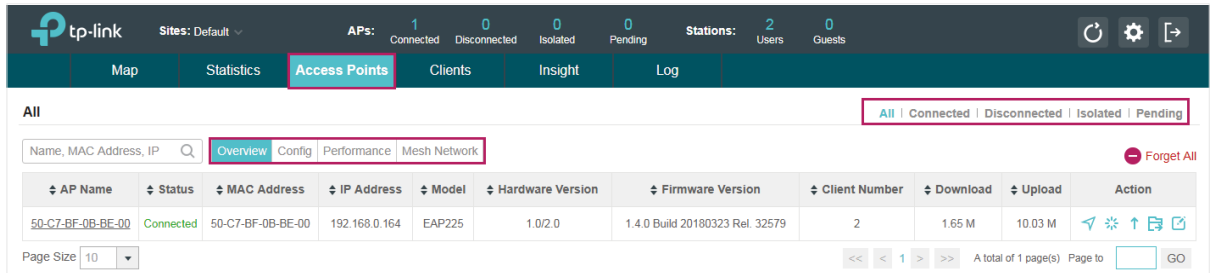
The **Recent Activities** statistics can be toggled between a view for the past specific 24 hours and one for the past specific 30 days.

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 10MB and there is 2 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 TP-Link Omada Controller interface. At the top, there's a navigation bar with 'Access Points' highlighted. Below it, there's a search bar and a table of APs. The table has columns for AP Name, Status, MAC Address, IP Address, Model, Hardware Version, Firmware Version, Client Number, Download, Upload, and Action. The first row shows an AP with MAC address 50-C7-BF-0B-BE-00, IP 192.168.0.164, and status 'Connected'.

2.3.1 Manage the EAPs in Different Status

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



All	Displays the information of all EAPs in different status.
Connected	<p>Displays the connected EAPs.</p> <p>The status of connected EAPs includes two cases: Connected and Connected (Wireless).</p> <p>Connected: After you adopt a wired EAP in Pending status, its status will become Provisioning, then Configuring and Connected eventually.</p> <p>Connected (Wireless): In a mesh network, if an EAP has a successful wireless uplink, its status will become Adopting (Wireless) and then Connected (Wireless).</p> <p>Only connected EAPs can be managed. A connected EAP will turn into a pending one after you forget it. You can refer to Forget this AP to forget an EAP or click Forget All on the page to forget all the connected EAPs.</p>
Disconnected	<p>Displays the disconnected EAPs.</p> <p>If a connected EAP powers off or disconnects from the Omada Controller, it will be in Disconnected status. When a disconnected EAP is reset to factory defaults or forgot, it will turn into a pending one again. You can refer to Forget this AP to forget a EAP or click Forget All on the page to forget all the disconnected EAPs.</p>
Isolated	<p>Displays the isolated EAPs.</p> <p>In a mesh network, when the EAP which has been managed before by Omada Controller connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state. The isolated EAP searches for wireless uplink and the LED on the device turns green and flashes off every 5 seconds. To know more about mesh network, refer to Configure Mesh.</p>

Pending	<p>Displays the pending EAPs.</p> <p>The status of pending EAPs includes three cases: Pending, Pending (Wireless) and Managed by others.</p> <p>Pending: All the EAPs with wired network connection are in pending status by default when first discovered by Omada Controller.</p> <p>Pending (Wireless): The factory default EAP with mesh functions and no wired network connection is in Pending (Wireless) status when first discovered by Omada Controller.</p> <p>Managed by others: An EAP is located on the same network as the controller, but has been already managed by an existing controller before. You can provide the username/password to unbind the EAP from the existing controller and begin adoption in current controller.</p> <p>Only after pending EAPs are adopted and connected, you can manage them. To adopt pending EAPs, refer to Adopt the EAPs.</p>
---------	---

2.3.2 View the Detailed Information of EAPs

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





Overview	Displays the EAP's name/MAC address, IP address, status, model, 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.
Mesh Network	Displays the detailed information of the EAPs that formed the mesh network. The information includes EAP's name, MAC address, IP address, status, model, hardware version, firmware version, number of connected clients, hops, uplink APs and downlink APs.

2.3.3 Manage the EAPs in the Action Column

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



	Locate the EAP in the map.
	Reboot the EAP.



Upgrade the EAP.

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

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

Model: EAP225

Upgrade File: **Browse** **Upgrade**



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: **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](#).

EA-33-51-A8-22-A0 **Connected**

Details | User | Guest | Mesh | Configuration

Overview

MAC Address: EA-33-51-A8-22-A0

IP Address: 192.168.0.132

Model: EAP225-Outdoor

Firmware Version: 1.3.0 Build 20180426 Rel. 39248

CPU: 1%

Memory: 54%

Uptime: 0 days 21:44:18

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.

↕ Hostname	↕ MAC Address	↕ IP Address	↕ Access Point	↕ SSID	↕ User / Guest	↕ 2.4GHz / 5GHz	↕ Download	↕ Upload	↕ Rate (Mbps)	↕ Active Time	↕ Signal	Action
Unknown	A4-44-D1-DE-7B-AB	192.168.0.111	50-C7-BF-0B-BE-00	SSID1	User	5GHz	78.03 K	596.80 K	150.0	24s		

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 passing the [Portal Authentication](#). Guests are the clients connected to the EAP wireless network with passing the [Portal Authentication](#).

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

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

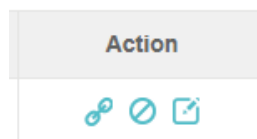
All Clients The page displays the information of all clients including users and guests.

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 **Apply**.

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](#)

Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.



If the client is a Guest, you can click this icon to cancel the authorization for it.

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.

↕ Hostname	↕ MAC Address	↕ IP Address	↕ Access Point	↕ SSID	↕ User / Guest	↕ 2.4GHz / 5GHz	↕ Download	↕ Upload	↕ Rate (Mbps)	↕ Active Time	↕ Signal	Action
Unknown	A4-44-D1-DE-7B-AB	192.168.0.111	50-C7-BF-0B-BE-00	SSID1	User	5GHz	78.03 K	596.80 K	150.0	24s		

2.5.1 Select a Specified Period

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

Last Seen: All ▼

Last Seen: All

Last Seen: 1 Day

Last Seen: 3 Days

Last Seen: 7 Days

Last Seen: 14 Days

Last Seen: 30 Days

2.5.2 View the History Information of Clients

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





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



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

2.5.3 Manage Clients in the Action Column

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

	Block the client's access to the network.
	Resume the client's access.

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.

MAC	SSID	Band	Channel	Security	Beacon	Signal	Last Seen	Action
50-C7-BF-45-E2-BE	AD7200_5G-1	5G	40	ON	100	-52	2018-07-12 11:15:09	
50-C7-BF-48-57-74		5G	40	ON	100	-59	2018-07-12 11:15:09	
50-C7-BF-48-57-1E	Deco M5	2.4G	4	ON	100	-38	2018-07-12 11:15:09	
70-4F-57-02-DB-5A		5G	36	ON	100	-49	2018-07-12 11:15:09	
06-69-6C-56-94-64	NanS	2.4G	1	ON	100	-45	2018-07-12 11:15:09	
56-C7-BF-48-57-1F		5G	40	ON	100	-48	2018-07-12 11:15:09	
DA-5D-4C-30-00-1D	TP-LINK_Guest_001D	2.4G	6	OFF	100	-50	2018-07-12 11:15:09	
CC-7B-35-48-B0-84	ChinaNet-MjLh	2.4G	11	ON	100	-42	2018-07-12 11:15:09	
B0-55-08-94-7A-DB	MAIMANG 6	2.4G	6	ON	100	-93	2018-07-12 11:15:09	
FA-8F-CA-55-D3-DA	Chromecast6460.b	2.4G	6	OFF	100	-56	2018-07-12 11:15:09	

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




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

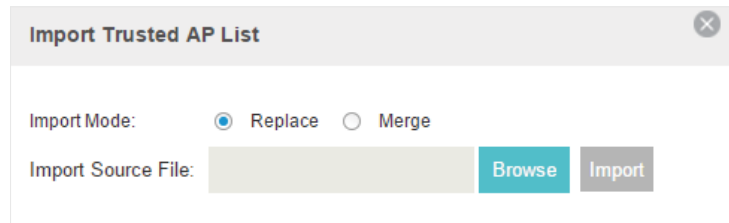
2.6.2 Manage the Trusted Rogue APs List

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

MAC	SSID	Band	Channel	Security	Last Seen	Action
50-C7-BF-45-E2-BE	AD7200_5G-1	5G	40	ON	2018-07-12 11:16:00	
50-C7-BF-48-57-1E	Deco M5	2.4G	4	ON	2018-07-12 11:16:00	

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



The dialog box titled "Import Trusted AP List" contains the following elements:

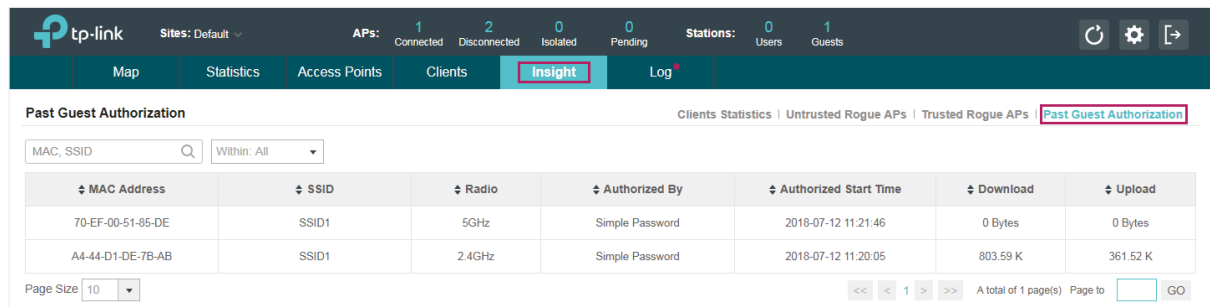
- Import Mode:** Two radio buttons, "Replace" (selected) and "Merge".
- Import Source File:** A text input field followed by "Browse" and "Import" buttons.

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.



The screenshot shows the TP-Link web interface. The top navigation bar includes "Map", "Statistics", "Access Points", "Clients", "Insight", and "Log". The "Insight" tab is active. Below the navigation bar, the "Past Guest Authorization" page is displayed. It features a search bar for "MAC, SSID" and a dropdown menu for "Within: All". The main content is a table with the following columns: "MAC Address", "SSID", "Radio", "Authorized By", "Authorized Start Time", "Download", and "Upload".

MAC Address	SSID	Radio	Authorized By	Authorized Start Time	Download	Upload
70-EF-00-51-85-DE	SSID1	5GHz	Simple Password	2018-07-12 11:21:46	0 Bytes	0 Bytes
A4-44-D1-DE-7B-AB	SSID1	2.4GHz	Simple Password	2018-07-12 11:20:05	803.59 K	361.52 K

At the bottom of the page, there is a "Page Size" dropdown set to 10, a pagination control showing "1" of 1 page, and a "GO" button.

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.

The screenshot shows the 'Logs' page in the Omada Controller interface. The top navigation bar includes 'Log' (highlighted), 'Map', 'Statistics', 'Access Points', 'Clients', and 'Insight'. The main content area has a search bar for 'AP MAC, Level, Content' and a 'Delete All' button. Below is a table with the following data:



AP MAC	Level	Time	Content	Action
EA-23-51-06-22-52	WARNING	2018-07-10 20:07:17	Username and password are successfully updated	[Delete]
EA-23-51-06-22-52	WARNING	2018-07-10 20:05:22	LAN IP and mask changed to 192.168.0.146 255.255.255.0	[Delete]
EA-23-51-06-22-52	WARNING	2018-07-10 19:57:50	LAN IP and mask changed to 192.168.0.254 255.255.255.0	[Delete]
EA-23-51-06-22-52	INFO	2018-07-10 19:57:44	System started	[Delete]
EA-33-51-A8-22-A0	WARNING	2018-07-10 19:28:27	Username and password are successfully updated	[Delete]
EA-33-51-A8-22-A0	WARNING	2018-07-10 19:24:37	LAN IP and mask changed to 192.168.0.132 255.255.255.0	[Delete]
EA-33-51-A8-22-A0	WARNING	2018-07-10 16:12:55	LAN IP and mask changed to 192.168.0.254 255.255.255.0	[Delete]
EA-33-51-A8-22-A0	INFO	2018-07-10 16:12:49	System started	[Delete]
50-C7-BF-0B-BE-00	WARNING	2018-07-10 15:27:34	Username and password are successfully updated	[Delete]
50-C7-BF-0B-BE-00	WARNING	2018-07-10 15:25:31	Username and password are successfully updated	[Delete]

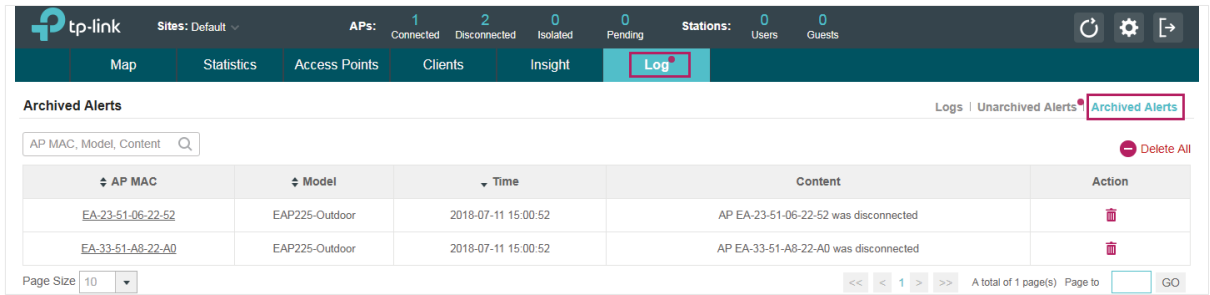
2.9 View Alerts

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.



The screenshot shows the 'Unarchived Alerts' page in the Omada Controller interface. The top navigation bar includes 'Log' (highlighted), 'Map', 'Statistics', 'Access Points', 'Clients', and 'Insight'. The main content area has a search bar for 'AP MAC, Model, Content' and an 'Archive All' button. Below is a table with the following data:

AP MAC	Model	Time	Content	Action
50-C7-BF-0B-BE-00	EAP225	2018-07-12 13:59:14	AP 50-C7-BF-0B-BE-00 was disconnected	[Archive]
EA-33-51-A8-22-A0	EAP225-Outdoor	2018-07-12 10:46:59	AP EA-33-51-A8-22-A0 was disconnected	[Archive]
50-C7-BF-0B-BE-00	EAP225	2018-07-12 10:46:59	AP 50-C7-BF-0B-BE-00 was disconnected	[Archive]
50-C7-BF-0B-BE-00	EAP225	2018-07-12 09:09:13	AP 50-C7-BF-0B-BE-00 was disconnected	[Archive]
EA-23-51-06-22-52	EAP225-Outdoor	2018-07-11 16:12:52	AP EA-23-51-06-22-52 was disconnected	[Archive]
EA-33-51-A8-22-A0	EAP225-Outdoor	2018-07-11 13:31:08	AP EA-33-51-A8-22-A0 was disconnected	[Archive]
50-C7-BF-0B-BE-00	EAP225	2018-07-11 13:31:08	AP 50-C7-BF-0B-BE-00 was disconnected	[Archive]
EA-23-51-06-22-52	EAP225-Outdoor	2018-07-11 10:38:40	AP EA-23-51-06-22-52 was disconnected	[Archive]
EA-33-51-A8-22-A0	EAP225-Outdoor	2018-07-11 10:38:40	AP EA-33-51-A8-22-A0 was disconnected	[Archive]
50-C7-BF-0B-BE-00	EAP225	2018-07-11 10:38:40	AP 50-C7-BF-0B-BE-00 was disconnected	[Archive]

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



The screenshot shows the TP-Link management interface. At the top, there is a navigation bar with the TP-Link logo and various status indicators: Sites: Default, APs: 1 Connected, 2 Disconnected, 0 Isolated, 0 Pending, Stations: 0 Users, 0 Guests. Below the navigation bar, there are tabs for Map, Statistics, Access Points, Clients, Insight, and Log (highlighted with a red box). The main content area is titled "Archived Alerts" and includes a search bar for "AP MAC, Model, Content" and a "Delete All" button. The table below contains the following data:

AP MAC	Model	Time	Content	Action
EA-23-51-06-22-52	EAP225-Outdoor	2018-07-11 15:00:52	AP EA-23-51-06-22-52 was disconnected	
EA-33-51-A8-22-A0	EAP225-Outdoor	2018-07-11 15:00:52	AP EA-33-51-A8-22-A0 was disconnected	

At the bottom of the page, there is a "Page Size" dropdown set to 10, a pagination control showing "1" of 1 page(s), and a "GO" button.

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*

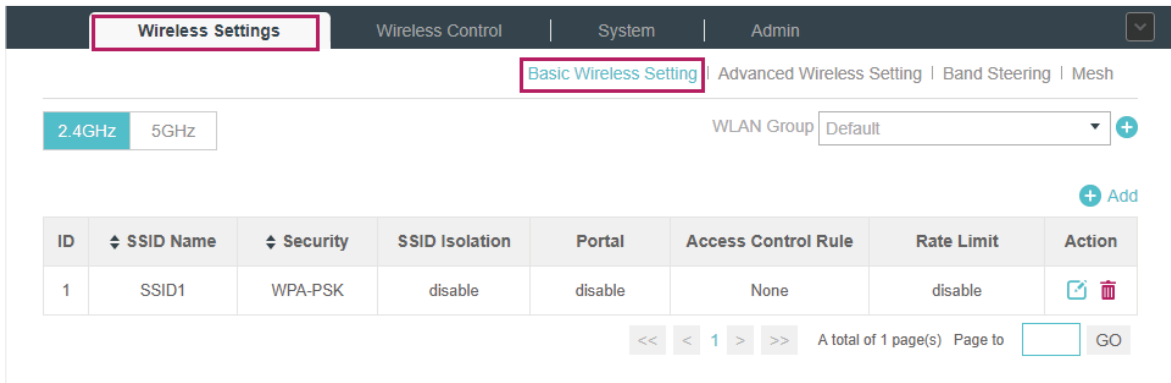
3.1 Wireless Network

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 'Wireless Settings' interface. The 'Wireless Settings' tab is selected, and the 'Basic Wireless Setting' sub-tab is active. The interface includes a frequency selector with '2.4GHz' and '5GHz' options, a 'WLAN Group' dropdown menu set to 'Default', and an '+ Add' button. Below these is a table with the following data:


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

At the bottom of the table, there are navigation controls: '<<', '<', '1', '>', '>>', 'A total of 1 page(s)', 'Page to', an input field, and a 'GO' button.

2. (Optional) Select a band frequency 2.4GHz 5GHz and click  at the right of to add a WLAN group. WLAN group is an easy way to quickly deploy EAPs by creating a template-based set of SSIDs with wireless parameters. Different WLAN groups can be applied to different EAPs. If you have no need to group your wireless networks, you can use the default WLAN group and skip this step.
3. Specify a name for the group and click **Apply**.



The screenshot shows a 'WLAN Group' dialog box with a close button (X) in the top right corner. It contains a 'Name' label and an input field with the text 'Group1'. Below the input field is a blue 'Apply' button.

- Select the brand frequency 2.4GHz 5GHz and WLAN group .
- Click  Add to add an SSID to the specific WLAN group.
- 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:

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:

Rate Limit ⌵

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

Access Control	Select an Access Control rule for this SSID. For more information, refer to Access Control .
----------------	--

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

WEP

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

Note:

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

Security Mode:	WEP
Type:	<input checked="" type="radio"/> Auto <input type="radio"/> Open System <input type="radio"/> Shared Key
Key Selected:	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:	weppw

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

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.

The screenshot shows a configuration form for WPA-Enterprise. The fields are as follows:

- Security Mode:** A dropdown menu set to "WPA-Enterprise".
- Version:** Radio buttons for "Auto", "WPA", and "WPA2". "WPA2" is selected.
- Encryption:** Radio buttons for "Auto", "TKIP", and "AES". "AES" is selected.
- RADIUS Server IP:** A text input field containing "0.0.0.0".
- RADIUS Port:** A text input field containing "0". A note next to it says "(1-65535, 0 means default port 1812.)".
- RADIUS Password:** An empty text input field.
- Group Key Update Period:** A text input field containing "0". A note next to it says "seconds(30-8640000, 0 means no upgrade)."

Version	<p>Select the version of WPA-Enterprise.</p> <p>Auto: The EAP will automatically choose the version used by each client device.</p> <p>WPA/WPA2: Two versions of Wi-Fi Protected Access.</p>
Encryption	<p>Select the Encryption type.</p> <p>Auto: The default setting is Auto and the EAP will select TKIP or AES automatically based on the client device's request.</p> <p>TKIP: Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11ac 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>AES: Advanced Encryption Standard. We recommend you select AES as the encryption type because it is more secure than TKIP.</p>
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:	<input type="text" value="WPA-PSK"/>
Version:	<input type="radio"/> Auto <input type="radio"/> WPA-PSK <input checked="" type="radio"/> WPA2-PSK
Encryption:	<input type="radio"/> Auto <input type="radio"/> TKIP <input checked="" type="radio"/> AES
Wireless Password:	<input type="text"/> <input type="button" value="👁"/>
Group Key Update Period:	<input type="text" value="0"/> seconds (30-8640000, 0 means no upgrade)

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

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

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

8. Click Apply.

3.1.2 Configure Advanced Wireless Parameters

Proper wireless parameters can improve the network's stability, reliability and communication efficiency. The advanced wireless parameters consist of **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**.

Wireless Settings | Wireless Control | System | Admin

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

Fast Roaming: Enable ?

Apply

2.4GHz | 5GHz

Beacon Interval: ms(40-100)

DTIM Period: (1-255)

RTS Threshold: (1-2347)

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

Airtime Fairness: Enable ?

Apply

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

Fast Roaming: Enable ?

Dual Band 11k Report: Enable ?

Force-disassociation: Enable ?

Fast Roaming

With this option enabled, 11k/v capable clients can have improved fast roaming experience when moving among different APs.

Dual Band 11k Report

With this feature disabled, the controller provides candidate AP report that contains the APs in the same band as the clients. With this feature enabled, the controller provides candidate AP report that contains the APs in both 2.4GHz and 5GHz bands.

Force-disassociation

The controller dynamically monitors the link quality of every associated client. When the client's current link quality drops below the predefined threshold and there are some other APs with better signal, the current AP issues an 11v roaming suggestion to the client.

With Force-disassociation disabled, the AP only issues a roaming suggestion, but whether to roam or not is determined by the client.

With Force-disassociation enabled, the AP not only issues a roaming suggestion but also disassociates the client after a while. Thus the client is supported to re-associate to a better AP. This function is recommended when there are sticky clients that don't roam.

3. Click **Apply**.

4. Select the band frequency 2.4GHz 5GHz .

5. Configure the following parameters.

Beacon Interval

Beacons are transmitted periodically by the EAP device to announce the presence of a wireless network for the clients. **Beacon Interval** value determines the time interval of the beacons sent by the device.

You can specify a value between 40 and 100ms. The default is 100ms.

DTIM Period

The DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames. It indicates whether the EAP device has buffered data for client devices. The **DTIM Period** indicates how often the clients served by this EAP device should check for buffered data still on the EAP device awaiting pickup.

You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating clients check for buffered data on the EAP device at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend you keep it by default.

RTS Threshold

RTS (Request to Send) can ensure efficient data transmission. When RTS is activated, the client will send a RTS packet to EAP to inform that it will send data before it send packets. After receiving the RTS packet, the EAP notices other clients in the same wireless network to delay their transmitting of data and informs the requesting client to send data, thus avoiding the conflict of packet. If the size of packet is larger than the **RTS Threshold**, the RTS mechanism will be activated.

If you specify a low threshold value, RTS packets are sent more frequently and help the network recover from interference or collisions that might occur on a busy network. However, it also consumes more bandwidth and reduces the throughput of the packet. We recommend you keep it by default. The recommended and default value is 2347.

Fragmentation Threshold

The fragmentation function can limit the size of packets transmitted over the network. If a packet exceeds the **Fragmentation Threshold**, the fragmentation function is activated and the packet will be fragmented into several packets.

Fragmentation helps improve network performance if properly configured. However, too low fragmentation threshold may result in poor wireless performance caused by the extra work of dividing up and reassembling of frames and increased message traffic. The recommended and default value is 2346 bytes.

Airtime Fairness

With this option enabled, each client connecting to the EAP can get the same amount of time to transmit data, avoiding low-data-rate clients to occupy too much network bandwidth and improving the network throughput. We recommend you enable this function under multi-rate wireless networks.

6. Click **Apply**.

3.1.3 Configure Band Steering

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

To configure Band Steering, follow the steps below.

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

The screenshot shows the 'Wireless Settings' page with the 'Band Steering' tab selected. The 'Band Steering' checkbox is unchecked. The 'Connection Threshold' is set to 20, 'Difference Threshold' is set to 4, and 'Max Failures' is set to 10. An 'Apply' button is visible at the bottom. A note at the bottom states: 'Note: To run the Band Steering function on a SSID, please create the SSIDs on both of the 2GHz and 5GHz band and make sure they have the same name, security mode and wireless password.'

Setting	Value	Range
Band Steering	<input type="checkbox"/> Enable	
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	<p>Connection Threshold defines the maximum number of clients connected to the 5GHz band. The value of Connection Threshold is from 2 to 40, and the default is 20.</p> <p>Difference Threshold defines the maximum difference between the number of clients on the 5GHz band and 2.4GHz band. The value of Difference Threshold is from 1 to 8, and the default is 4.</p> <p>When the following two conditions are both met, the EAP prefer to refuse the connection request on 5GHz band and no longer steer other clients to the 5GHz band:</p> <ol style="list-style-type: none"> 1. The number of clients on the 5GHz band reaches the Connection Threshold value. 2. The difference between the number of clients on the 2.4GHz band and 5GHz band reaches the Difference Threshold value.
Max Failures	<p>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.</p> <p>The value is from 0 to 100, and the default is 10.</p>

4. Click **Apply**.

3.1.4 Configure Mesh

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

Note:

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

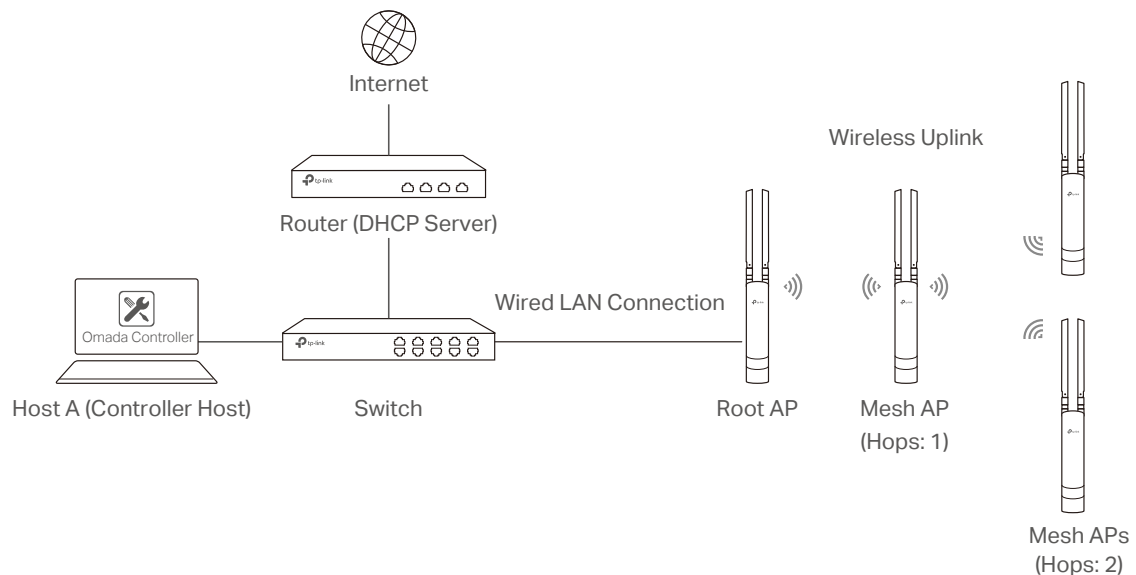
To understand how mesh can be used, the following terms used in Omada Controller will be introduced:

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

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

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

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

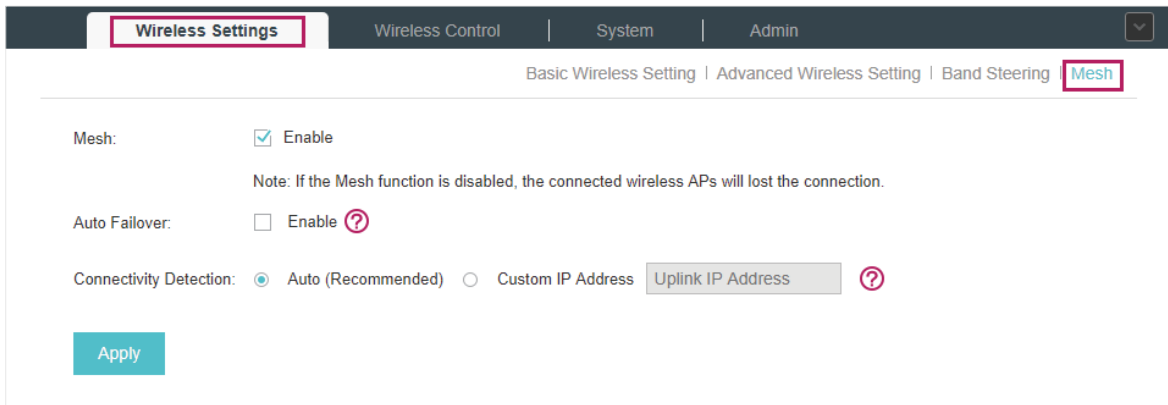


After all the EAPs are adopted, a mesh network is established. Then the EAPs connected to the network wirelessly also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

To establish a mesh network, follow the steps below.

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

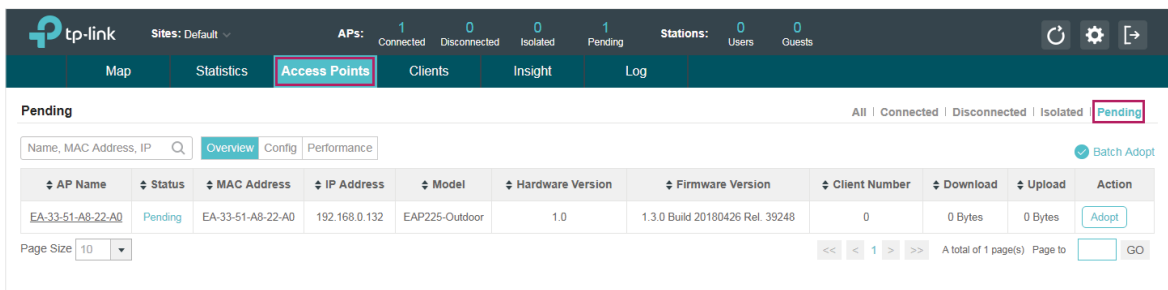
1. Go to **Wireless Settings > Mesh**.



2. Check the box to enable the Mesh function.
3. Configure the following parameters to maintain the mesh network:

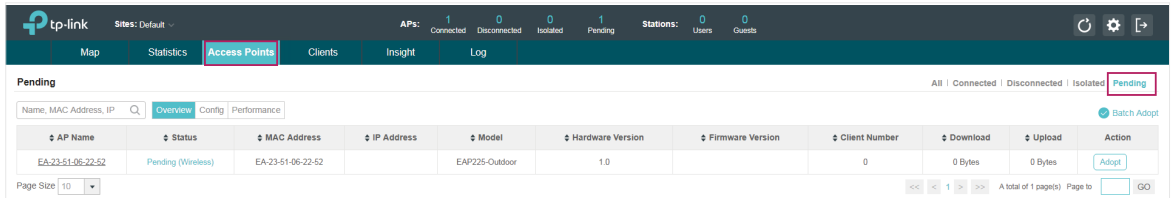
Auto Failover	<p>Enable or disable Auto Failover.</p> <p>Auto Failover is used for the controller to automatically maintain the mesh network. With this feature enabled, the controller can automatically select an uplink AP for the isolated EAP to establish Wireless Uplink. Thus the controller will automatically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

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




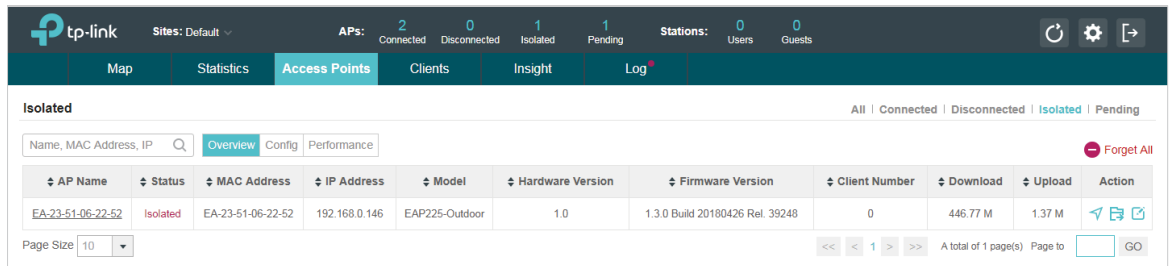
6. Install the EAP that will uplink the Root AP wirelessly. Make sure the intended location is within the range of Root AP. The EAPs that is waiting for Wireless Uplink includes two cases: factory default EAPs and EAPs that has been managed by Omada Controller before.

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

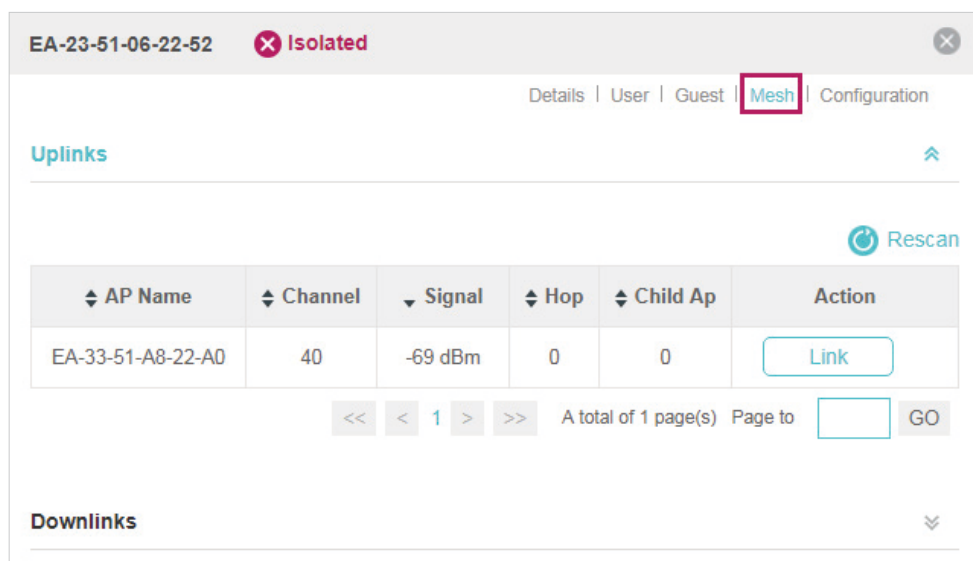


After adoption begins, the status of Pending (Wireless) EAP will become Adopting (Wireless) and then Connected (Wireless). It should take roughly 2 minutes to show up Connected (Wireless) within your controller.

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



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



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

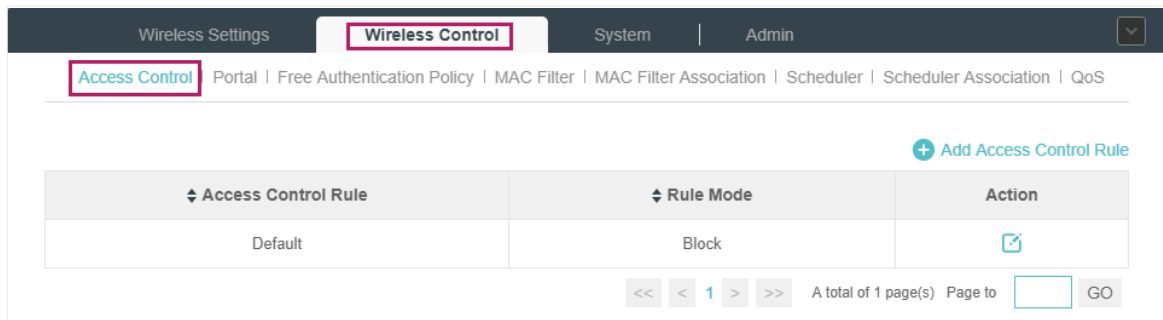
Tips:

- You can manually select the uplink AP that you want to connect in the uplink EAP list.
- You can enable Auto Failover to make the controller automatically select an uplink AP for the isolated EAP to establish Wireless Uplink. And the controller will automatically select a new uplink AP for the mesh EAPs when the original uplink fails.

3.2 Access Control

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

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



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

3. Configure the following parameters.

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

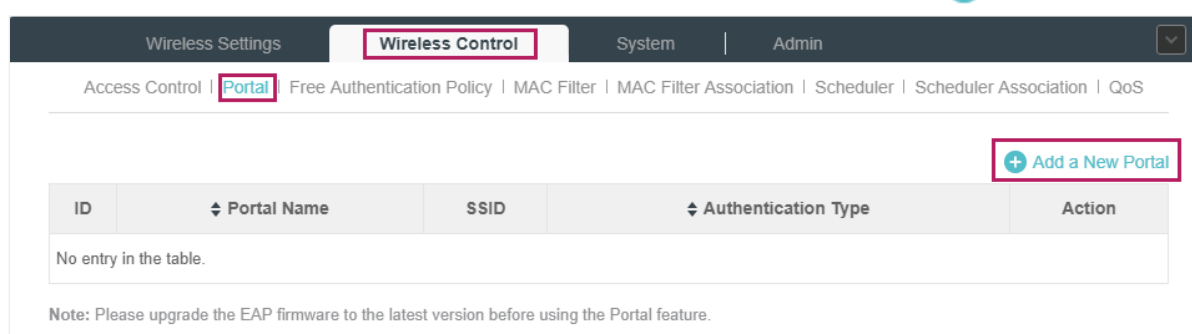
4. Click **Apply**.

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

3.3 Portal Authentication

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

To configure Portal Authentication, go to **Wireless Control > Portal** and click [+ Add a New Portal](#) .



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

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

[+ Add a New Portal](#)

ID	↕ Portal Name	SSID	↕ Authentication Type	Action
No entry in the table.				

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

Then the following window will pop up:

Add a New Portal

Basic Info

Portal Name:

SSID:

Authentication Type:

Authentication Timeout:

Daily Limit

HTTPS Redirect: Enable

Redirect: Enable

Redirect URL:

Login Page

Background: Solid Color Picture

Background Picture:

Logo Picture:

PC Mobile Phone Tablet PC Restore

Welcome Information: (1-31 characters)

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

3.3.1 No Authentication

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

Follow the steps below to configure No Authentication:

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

Basic Info

Portal Name:

SSID:

Authentication Type:

Authentication Timeout:

Daily Limit

HTTPS Redirect: Enable

Redirect: Enable

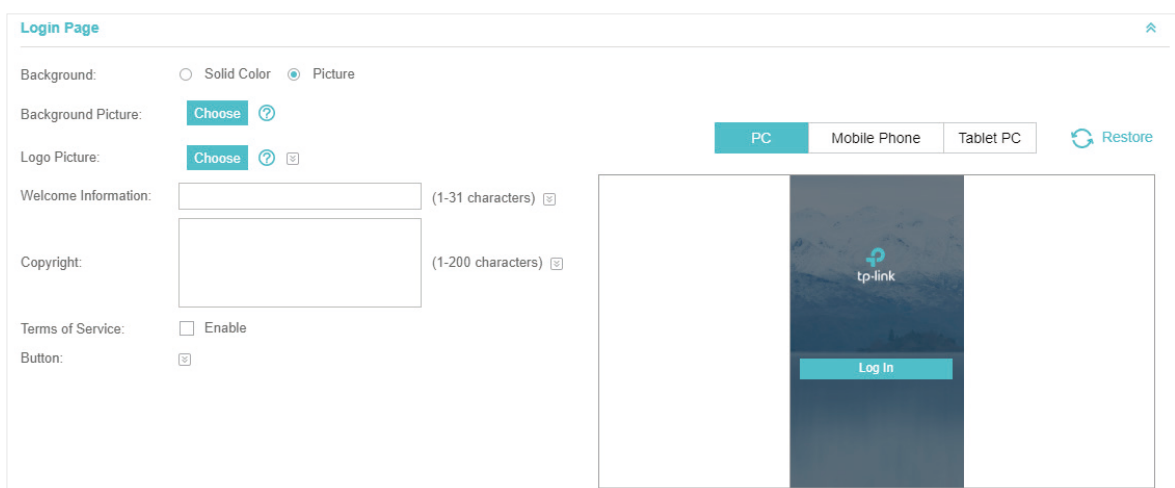
Redirect URL:

Configure the following parameters:

Portal Name	Specify a name for the Portal.
--------------------	--------------------------------







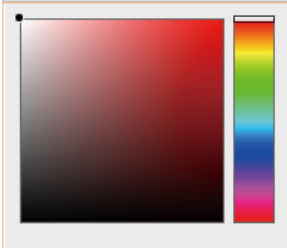


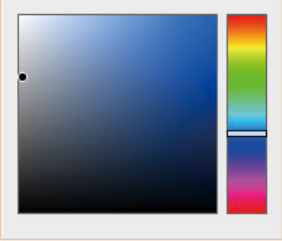
SSID	Select an SSID for the Portal.
Authentication Type	Select No Authentication .
Authentication Timeout	<p>With Daily Limit disabled, the client's authentication will expire after the time period you set and the client needs to log in on the web authentication page again to access the network.</p> <p>Options include 1 Hour, 8 Hours, 24 Hours, 7 Days and Custom. Custom allows you to define the time in days, hours and minutes. The default value is one hour.</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 30 Minutes, 1 Hour, 2 Hours, 4 Hours and 8 Hours, Custom. Custom allows you to define the time in hours and minutes. The default value is 30 minutes.</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.



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 that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. Drag and scale the clipping region to edit the picture and click Confirm .
Logo Picture	Click the Choose button and select a picture that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. 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 .
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Logo Picture: Choose  </p> <p>Logo Position: Middle </p> </div>	
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.
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Welcome Information: <input type="text" value=""/> (1-31 characters) </p> <p>#ffffff (RGB value)</p> <p>Welcome Information Color: </p> </div>	
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.
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Copyright: <input type="text" value=""/> (1-200 characters) </p> <p>#A7A9AC (RGB value)</p> <p>Copyright Color: </p> </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**.

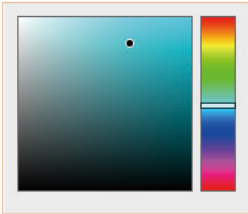
Button Color: Select your desired login button color through the color picker or by entering the RGB value manually.

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

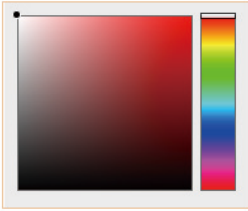
Button: 

Button Position:

(RGB value)

Button Color: 

(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: (1-5)

Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: Enable

Configure the following parameters:

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

5. Click **Apply**.

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. The fields are as follows:

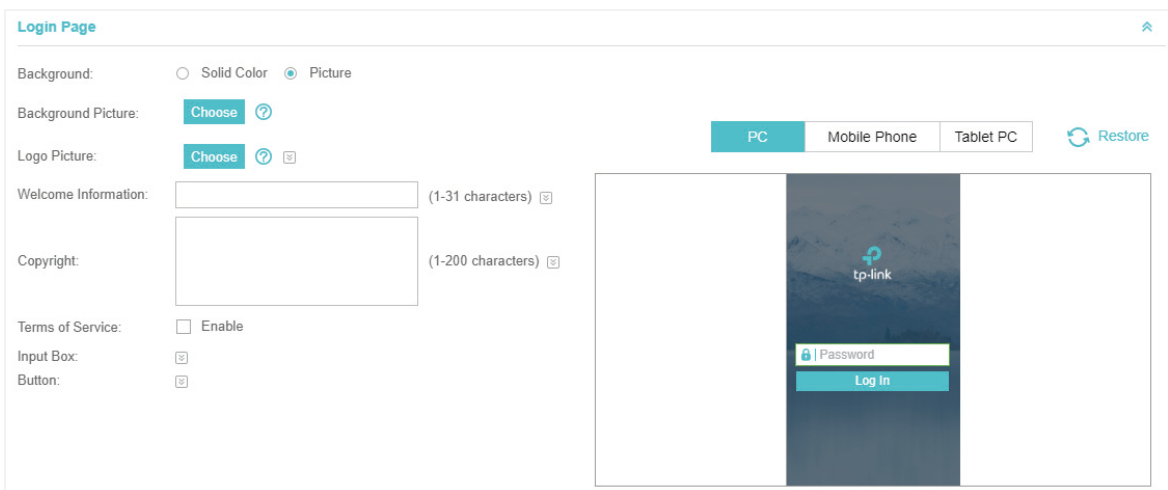
- Portal Name: [Text input field]
- SSID: [Dropdown menu showing '==Please select==']
- Authentication Type: [Dropdown menu showing 'Simple Password']
- Password: [Text input field with an eye icon for visibility toggle]
- Authentication Timeout: [Dropdown menu showing '1 Hour']
- HTTPS Redirect: Enable
- Redirect: Enable
- Redirect URL: [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 Simple Password .
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 1 Hour, 8 Hours, 24 Hours, 7 Days and Custom. Custom allows you to define the time in days, hours and minutes. The default value is one hour.</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: 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 that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. Drag and scale the clipping region to edit the picture and click Confirm .

Logo Picture

Click the **Choose** button and select a picture that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. 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:

Logo Position:

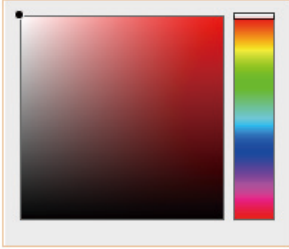
Welcome Information

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: 

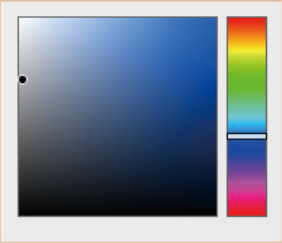
Copyright

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

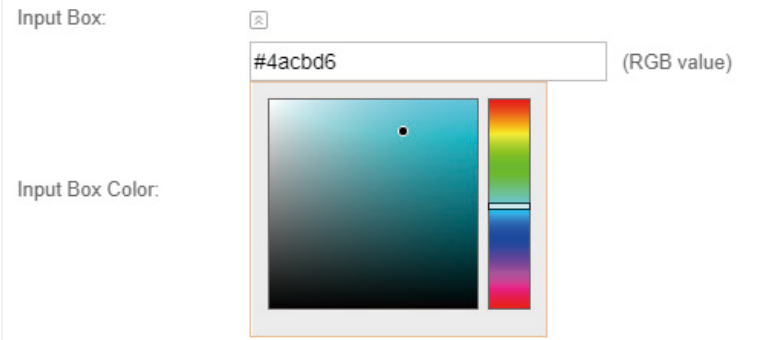
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

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.



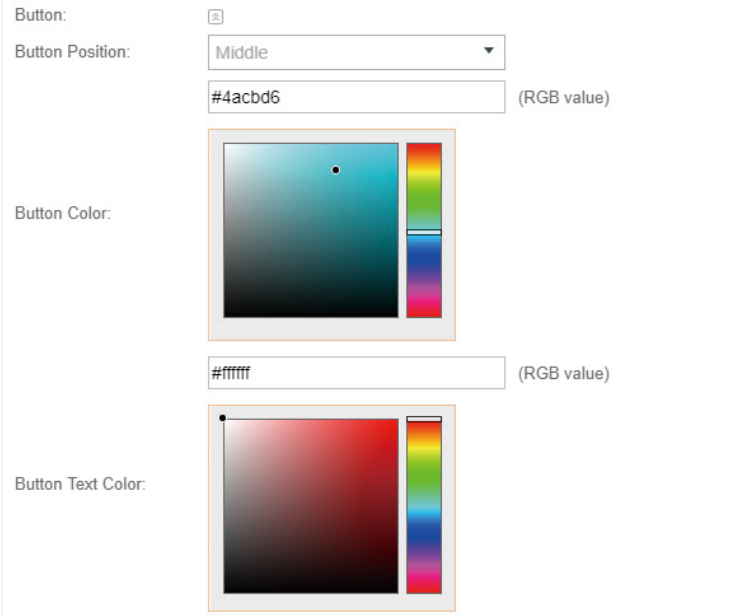
Button

Click  and configure the button.

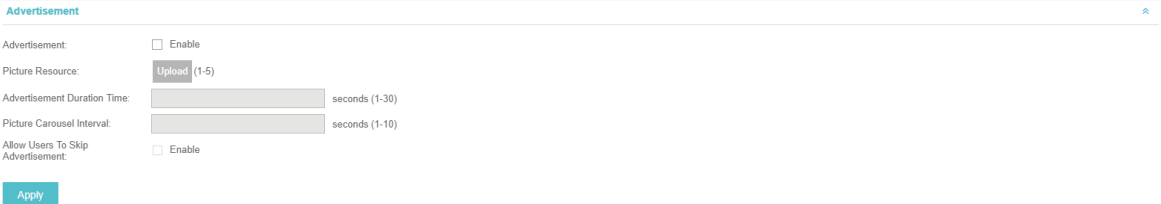
Button Position: Set the position of the login button. The options include **Middle**, **Upper** and **Lower**.

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.



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

5. Click **Apply**.

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.

The screenshot shows the 'Basic Info' configuration page for a Local User Portal. The fields are as follows:

- Portal Name: [Empty text input field]
- SSID: [Dropdown menu with '==Please select==']
- Authentication Type: [Dropdown menu with 'Local User']
- Below Authentication Type: [User Management](#)
- HTTPS Redirect: Enable [?](#)
- Redirect: Enable
- Redirect URL: [Greyed out 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 Local User .
User Management	You can click this button to configure user accounts for authentication later. Please refer to Create Local User Accounts .
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

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

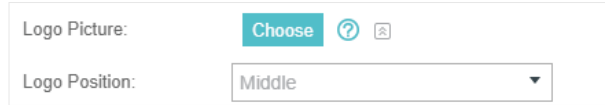
Configure the following parameters:

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 that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. Drag and scale the clipping region to edit the picture and click Confirm .

Logo Picture

Click the **Choose** button and select a picture that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. Drag and scale the clipping region to edit the picture and click **Confirm**.

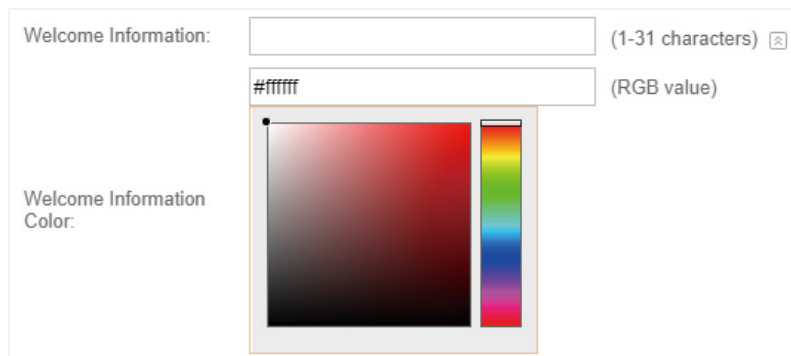
In addition, you can click and configure the logo position. The options include **Middle**, **Upper** and **Lower**.



Welcome Information

Specify the welcome information.

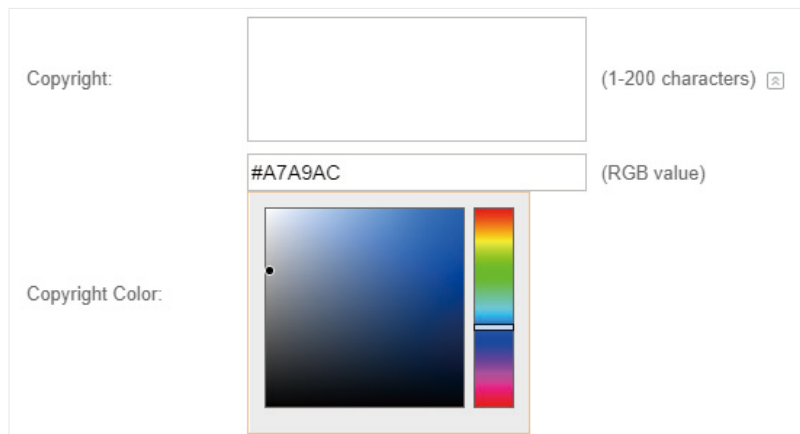
In addition, you can click and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



Copyright

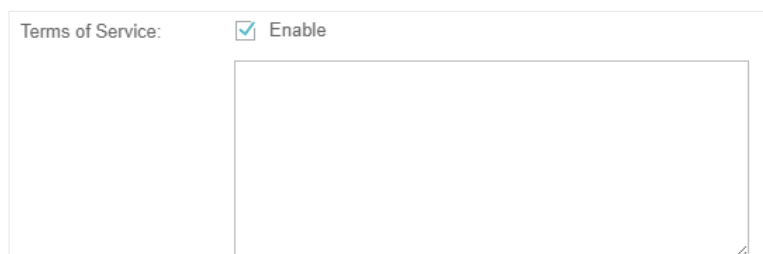
Specify the copyright information.

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.



Terms of Service


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



Input Box

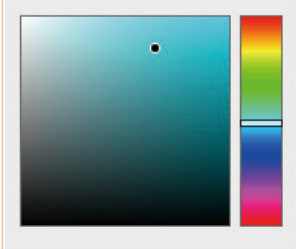
Click  and configure the input box.

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


Input Box: 

#4acbd6 (RGB value)

Input Box Color:




Button

Click  and configure the button.

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

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

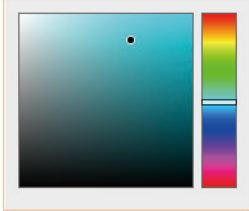
Button Text Color: Select your desired text color for the button through the color picker or by entering the RGB value manually.

Button: 

Button Position: Middle

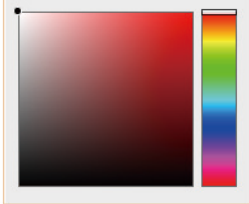
#4acbd6 (RGB value)

Button Color:




#ffffff (RGB value)

Button Text Color:



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

Advertisement 

Advertisement: Enable

Picture Resource: (1-5)

Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: Enable


Configure the following parameters:

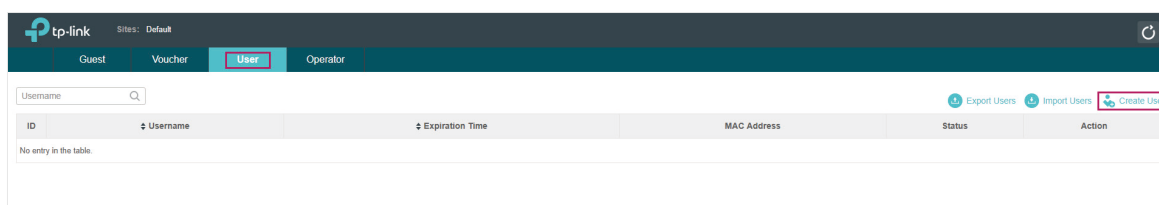
Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling Allow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

5. Click **Apply**.

Create 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	<input type="text"/>	(1-100 letters, digits or special characters)
Password	<input style="border: 1px solid #ccc; padding: 2px 5px;" type="password"/> 👁	(1-100 letters, digits or special characters)
Authentication Timeout	<input type="text" value="2018-12-31"/>	(Format: YYYY-MM-DD)
MAC Address Binding Type	<input style="border: 1px solid #ccc; padding: 2px 5px;" type="text" value="No Binding"/>	
Maximum Users	<input type="text" value="1"/>	(1-2048)
Name	<input type="text"/>	(1-50 characters, Optional)
Telephone	<input type="text"/>	(1-50 characters, Optional)
Rate Limit(Download)	<input type="checkbox"/>	
Rate Limit(Download)	<input style="width: 100%;" type="text"/>	Kbps (0-10240000)
Rate Limit(Upload)	<input type="checkbox"/>	
Rate Limit(Upload)	<input style="width: 100%;" type="text"/>	Kbps (0-10240000)
Traffic Limit	<input type="checkbox"/>	
Traffic Limit	<input style="width: 100%;" type="text"/>	MBytes (1-1048576)

Configure the following parameters:



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

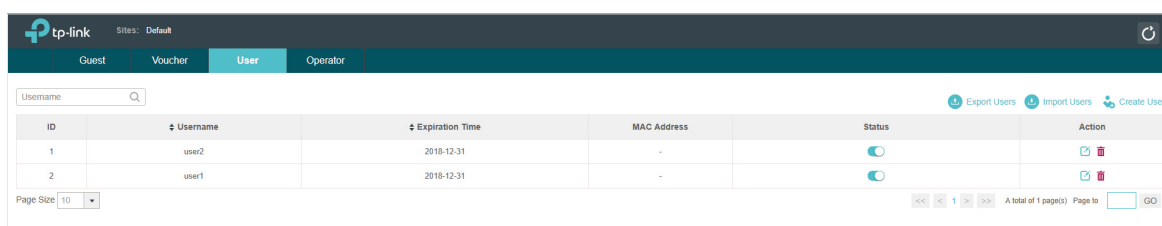
Rate Limit (Download) Select whether to enable download rate limit. With this option enabled, you can specify the limit of download rate. Note that the download rate will be limited to the minimum of the value configured in SSID, client and portal configuration.



Rate Limit (Upload) Select whether to enable upload rate limit. With this option enabled, you can specify the limit of upload rate. Note that the upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.

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.



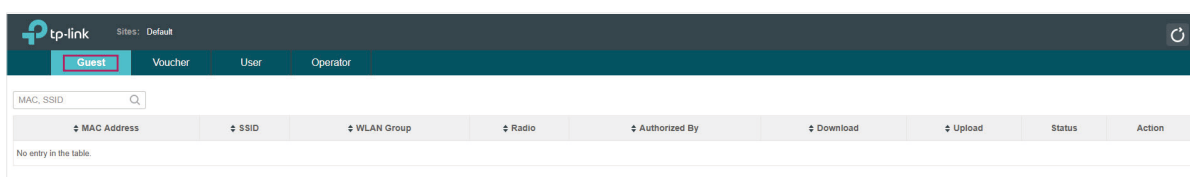
Additionally, you can click  **Export Users** to backup all the user account information into a CSV file or XLS file and save the file to your PC. If needed, you can click  **Import Users** and select the file to import the account information to the list.

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.



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.

Create Operator

Name:

Password: 

Notes:

Site Privileges: Default Office A Office 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.

The screenshot shows the 'Basic Info' configuration page for a Voucher Portal. It includes the following fields and options:

- Portal Name:** A text input field.
- SSID:** A dropdown menu with the placeholder text '==Please select=='.
- Authentication Type:** A dropdown menu set to 'Voucher'. Below it is a link labeled 'Voucher Manager'.
- 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 Voucher .
User Management	You can click this button to configure vouchers for authentication later. Please refer to Create Vouchers .
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites or be redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

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

Login Page

Background: Solid Color Picture

Background Picture: [Choose](#)

Logo Picture: [Choose](#)

Welcome Information: (1-31 characters)

Copyright: (1-200 characters)

Terms of Service: Enable

Input Box:

Button:

PC Mobile Phone Tablet PC [Restore](#)

tp-link

Voucher Code

Log In

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 that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. Drag and scale the clipping region to edit the picture and click Confirm .
Logo Picture	Click the Choose button and select a picture that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. 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 .

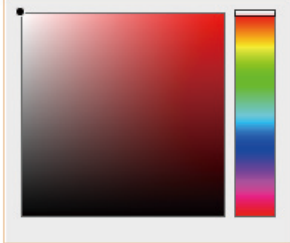
Logo Picture: [Choose](#)

Logo Position:

Welcome Information


Specify the welcome information.


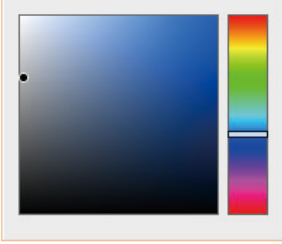
In addition, you can click  and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.

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

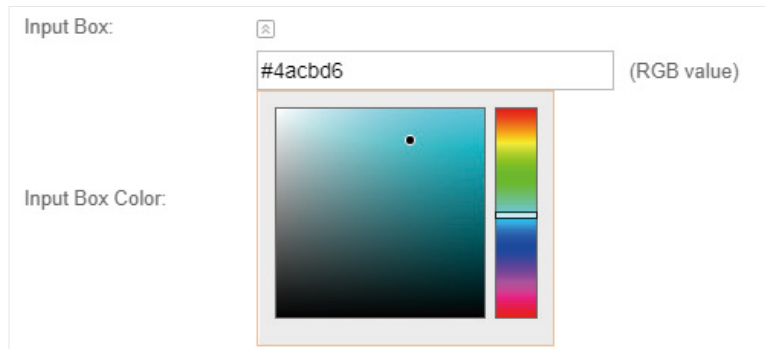
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Terms of Service:	<input checked="" type="checkbox"/> Enable
<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></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.



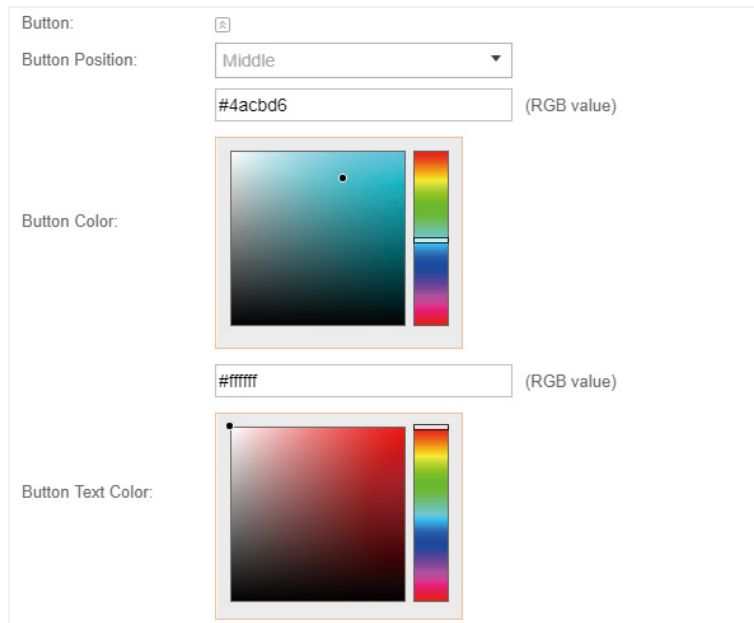
Button

Click  and configure the button.

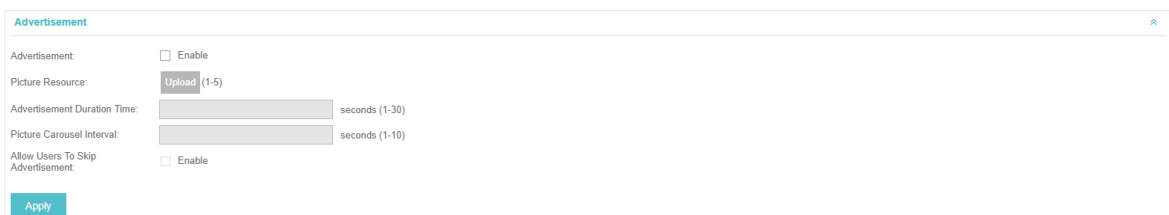
Button Position: Set the position of the login button. The options include **Middle**, **Upper** and **Lower**.

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:

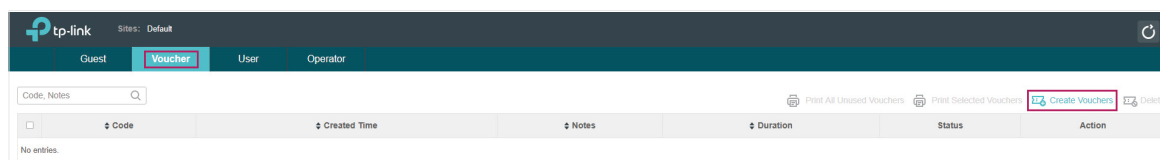
Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling Allow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

5. Click **Apply**.

Create Vouchers

Follow the steps below to create vouchers for authentication:

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



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

Create Vouchers
✕

Code Length: (6-10)

Amount: (1-500)

Type: ▼

Duration: ▼

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:

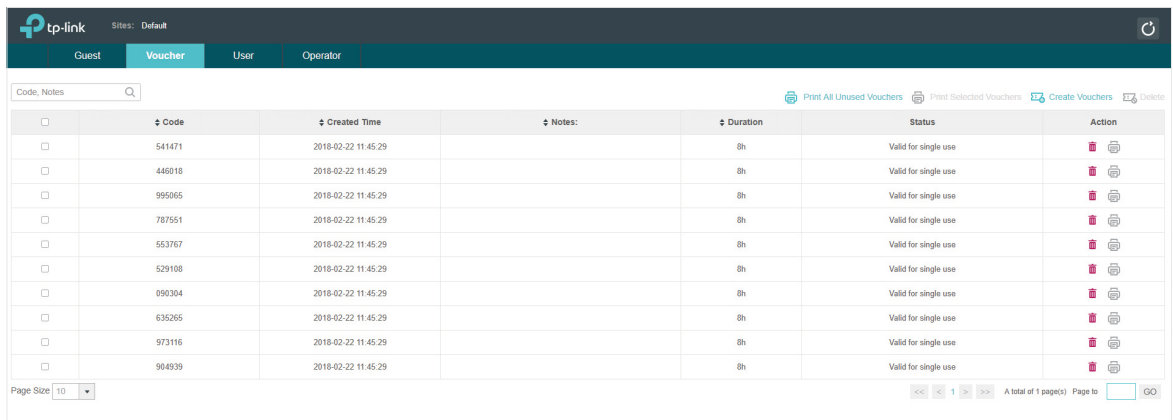
Configure the following parameters:

Code Length	Specify the length of the voucher codes to be created.
Amount	Enter the voucher amount to be generated.
Type	<p>Select Single Use or Multi Use.</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 Max Users. When the number of clients who are connected to the network with the same voucher reaches the value, no more clients can use this voucher to access the network.</p>
Duration	<p>Select the period of validity of the Voucher.</p> <p>The options include 8 hours, 2 days and User-defined. The period of valid of the voucher is reckoned from the time when it is used for the first time.</p>
Rate Limit (Download)	Select whether to enable download rate limit. With this option enabled, you can specify the limit of download rate. Note that the download rate will be limited to the minimum of the value configured in SSID, client and portal configuration.
Rate Limit (Upload)	Select whether to enable upload rate limit. With this option enabled, you can specify the limit of upload rate. Note that the upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.
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).

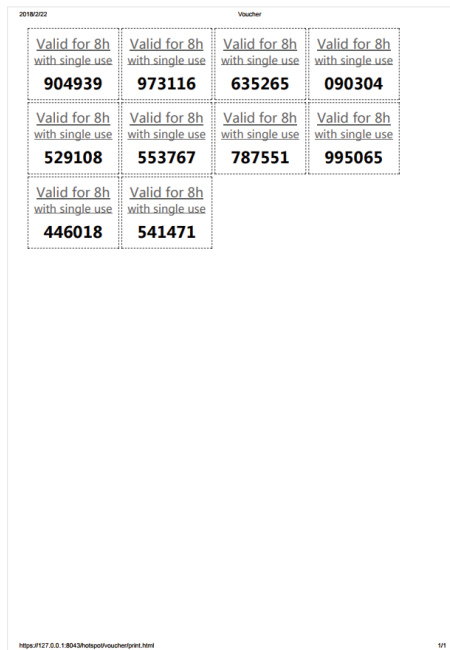
3. The Vouchers will be generated and displayed on the page.



The screenshot shows the tp-link Voucher management interface. At the top, there are tabs for Guest, Voucher, User, and Operator. Below the tabs is a search bar for Code and Notes. The main area contains a table with columns for Code, Created Time, Notes, Duration, Status, and Action. The table lists 10 vouchers, all with a duration of 8h and a status of 'Valid for single use'. The Action column contains icons for deleting and printing each voucher. At the bottom, there is a page size selector set to 10 and a pagination bar showing 'A total of 1 page(s) Page to 1 GO'.

<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	
<input type="checkbox"/>	446018	2018-02-22 11:45:29		8h	Valid for single use	
<input type="checkbox"/>	995065	2018-02-22 11:45:29		8h	Valid for single use	
<input type="checkbox"/>	787551	2018-02-22 11:45:29		8h	Valid for single use	
<input type="checkbox"/>	553767	2018-02-22 11:45:29		8h	Valid for single use	
<input type="checkbox"/>	529108	2018-02-22 11:45:29		8h	Valid for single use	
<input type="checkbox"/>	090304	2018-02-22 11:45:29		8h	Valid for single use	
<input type="checkbox"/>	635265	2018-02-22 11:45:29		8h	Valid for single use	
<input type="checkbox"/>	973116	2018-02-22 11:45:29		8h	Valid for single use	
<input type="checkbox"/>	904939	2018-02-22 11:45:29		8h	Valid for single use	

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

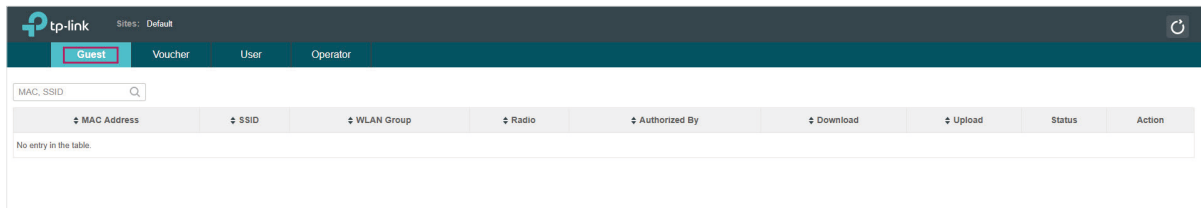


5. Distribute the vouchers to clients, and then they can use the codes to pass authentication.

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.



You can select an icon to execute the corresponding operation:



Restrict the client to access the network.



Extend the effective time.

Create Operator Accounts

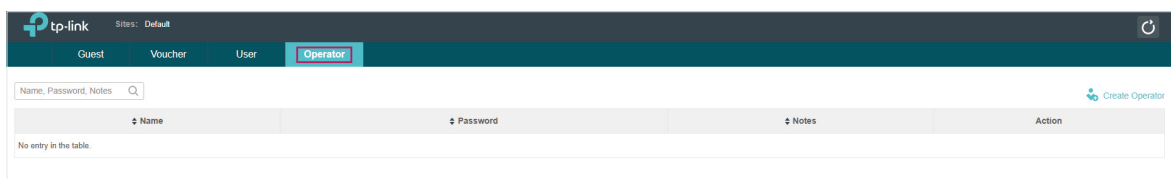
Operator account can be used to remotely manage the Local User Portal and Voucher Portal. Other users can visit the URL **https://Omda Controller Host's IP Address:8043/hotspot** (For example: **https://192.168.0.64:8043/hotspot**) and use the Operator account to enter the portal management page.


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.

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 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.

Configure the following parameters:

Portal Name	Specify a name for the Portal.
--------------------	--------------------------------

SSID	Select an SSID for the Portal.
Authentication Type	Select SMS .
Twilio SID	Enter the Account SID for Twilio API Credentials.
Auth Token	Enter the Authentication Token for Twilio API Credentials.
Phone Number	Enter the phone number that is used to send verification messages to the clients.
Maximum Users	<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 an upper limit.</p> <p>Specify the upper limit in this field.</p>
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 1 Hour, 8 Hours, 24 Hours, 7 Days and Custom. Custom allows you to define the time in days, hours and minutes. The default value is one hour.</p>
Preset Country Code	Set the default country code that will be filled automatically on the authentication page.
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.

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

Login Page

Background: Solid Color Picture

Background Picture: [Choose](#) ⓘ

Logo Picture: [Choose](#) ⓘ ⌵

Welcome Information: (1-31 characters) ⌵

Copyright: (1-200 characters) ⌵

Terms of Service: Enable

Input Box: ⌵

Button: ⌵

PC Mobile Phone Tablet PC [Restore](#)

tp-link

+1 Phone Number

Verification Code [Get Code](#)

Log In

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 that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. Drag and scale the clipping region to edit the picture and click Confirm .
Logo Picture	Click the Choose button and select a picture that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. 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 .

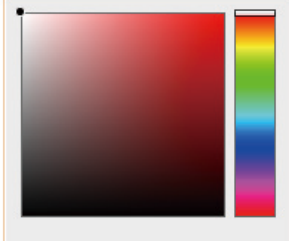
Logo Picture: [Choose](#) ⓘ ⌵

Logo Position: ⌵

Welcome Information


Specify the welcome information.


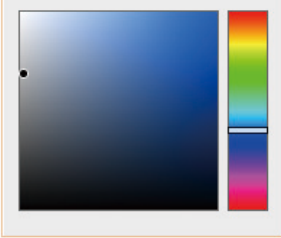
In addition, you can click  and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.

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

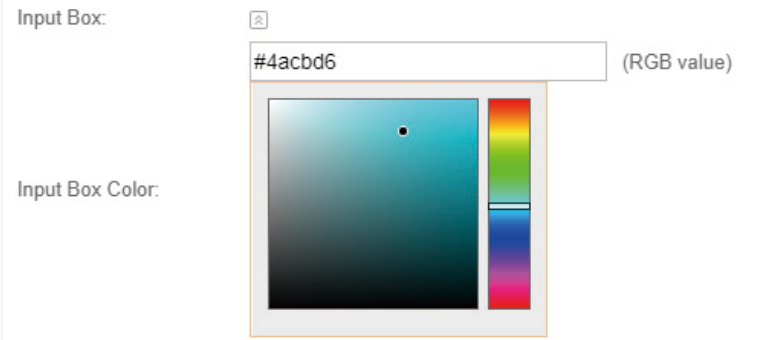
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Terms of Service:	<input checked="" type="checkbox"/> Enable
<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></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.



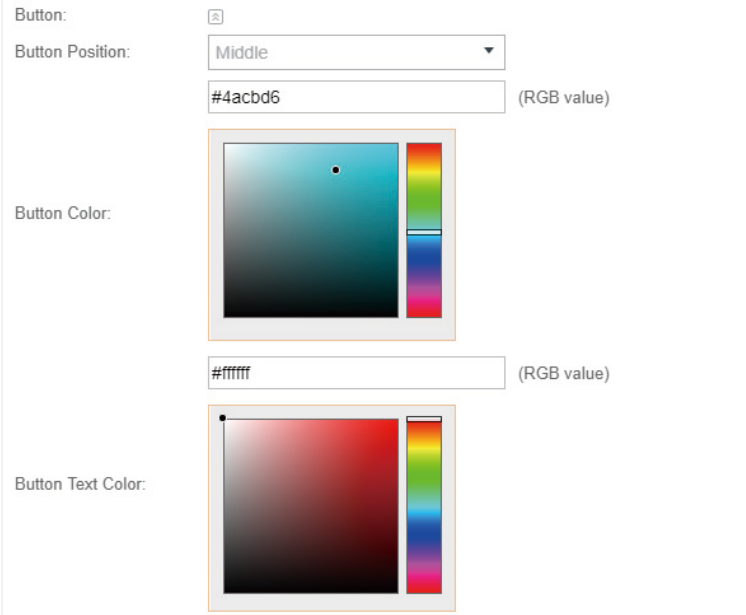
Button

Click  and configure the button.

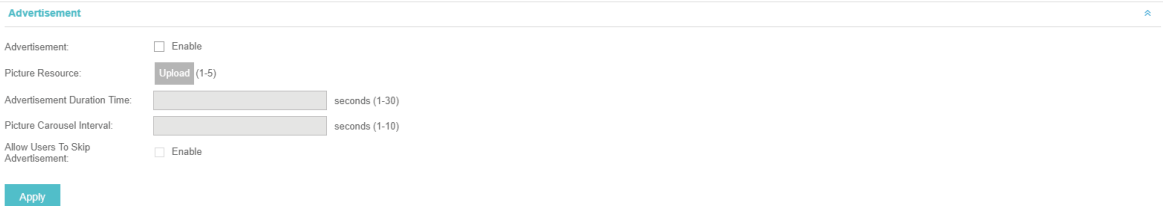
Button Position: Set the position of the login button. The options include **Middle**, **Upper** and **Lower**.

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.



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

6. Click **Apply**.

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

3.3.6 Facebook

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

Note:

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 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.

Configure the following parameters:

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

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

3.3.7 External RADIUS Server

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

Authentication Type:

RADIUS Server IP:

RADIUS Port:

RADIUS Password:

Authentication Timeout:

HTTPS Redirect: Enable

Redirect: Enable

Redirect URL:

Portal Customization:

External Web Portal URL:

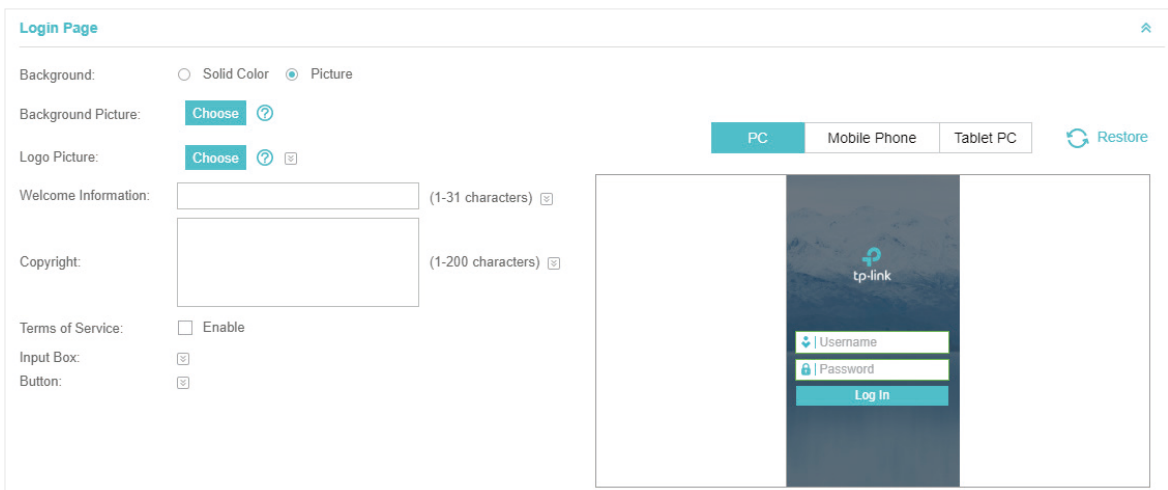
Apply

Configure the following parameters:


Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select Simple Password .
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 1 Hour, 8 Hours, 24 Hours, 7 Days, Custom. Custom allows you to define the time in days, hours, and minutes. The default value is one hour.</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>

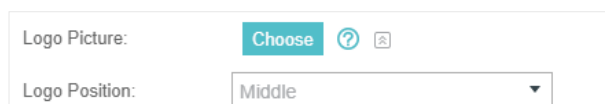
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.
Portal Customization	<p>Select Local Web Portal or External Web Portal.</p> <p>Local Web Portal: If this option is selected, refer to step 4 to configure the login page and step 5 to configure the advertisement.</p> <p>External Web Portal: If this option is selected, follow the steps below.</p> <ol style="list-style-type: none"> 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.




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 that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. Drag and scale the clipping region to edit the picture and click Confirm .
Logo Picture	<p>Click the Choose button and select a picture that is less than 2MB from your PC. And only JPG, PNG, BMP, GIF and JPEG file types are supported. Drag and scale the clipping region to edit the picture and click Confirm.</p> <p>In addition, you can click  and configure the logo position. The options include Middle, Upper and Lower.</p>



Welcome Information


Specify the welcome information.


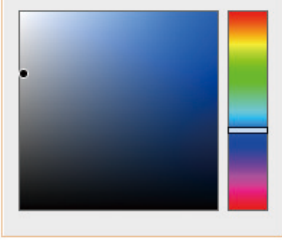
In addition, you can click  and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.

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

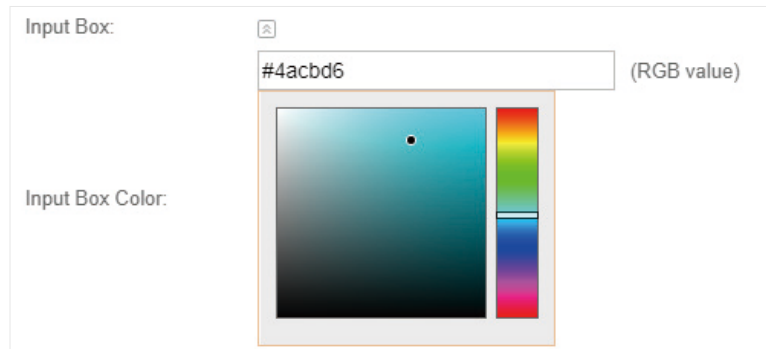
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Terms of Service:	<input checked="" type="checkbox"/> Enable
<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></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.



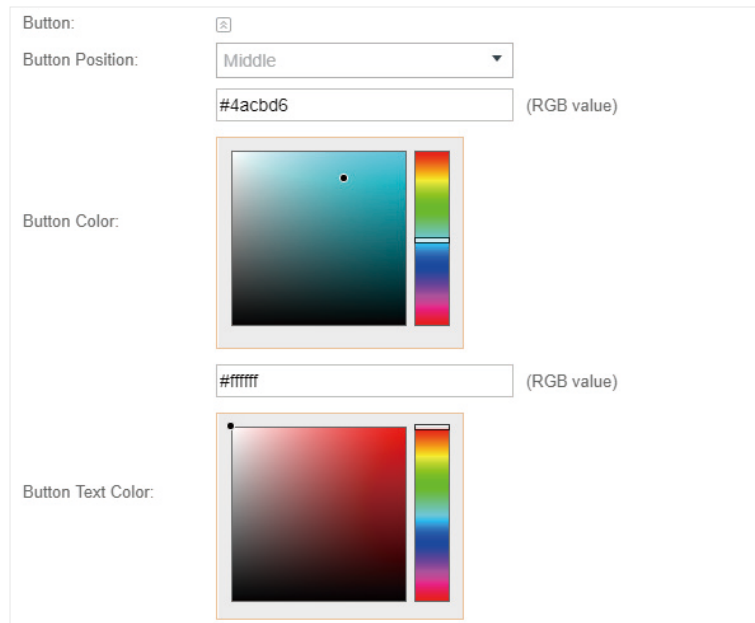
Button

Click  and configure the button.

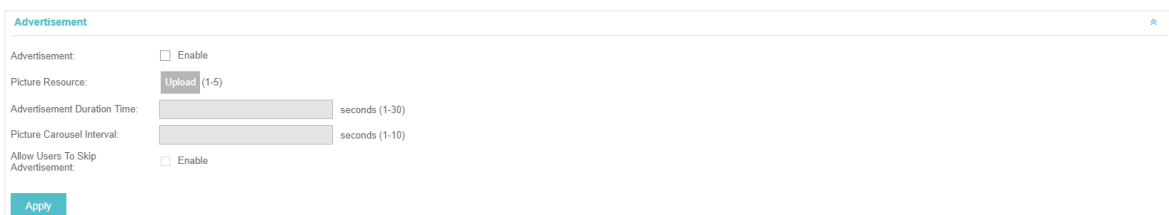
Button Position: Set the position of the login button. The options include **Middle**, **Upper** and **Lower**.

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.



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

6. Click **Apply**.

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 External Portal Server .

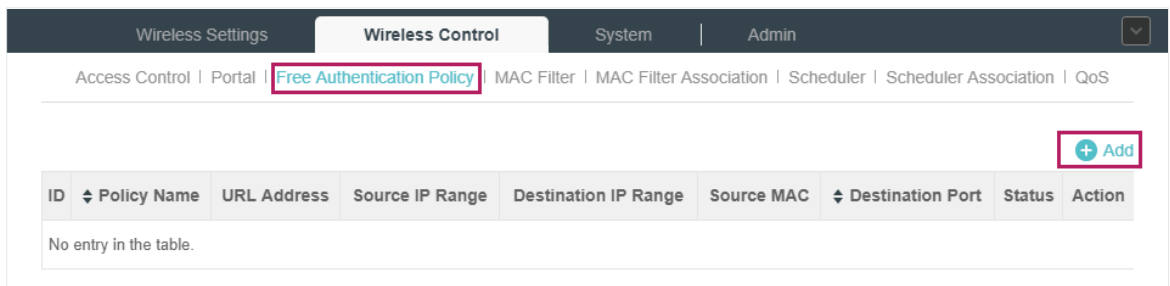
External Portal Server	Enter the complete authentication URL that redirect to an external portal server, for example: http://192.168.0.147:8880/portal/index.php or http://192.168.0.147/portal/index.html
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal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

3. Click **Apply**.

3.4 Free Authentication Policy

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

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



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

The 'Add Policy' dialog box contains the following fields and options:

- Policy Name:
- Mach Mode:
- Source IP Range: / (Optional)
- Destination IP Range: / (Optional)
- Source MAC: (Optional)
- Destination Port: (Optional)
- Status: Enable

An **Apply** button is located at the bottom left of the dialog.

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

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

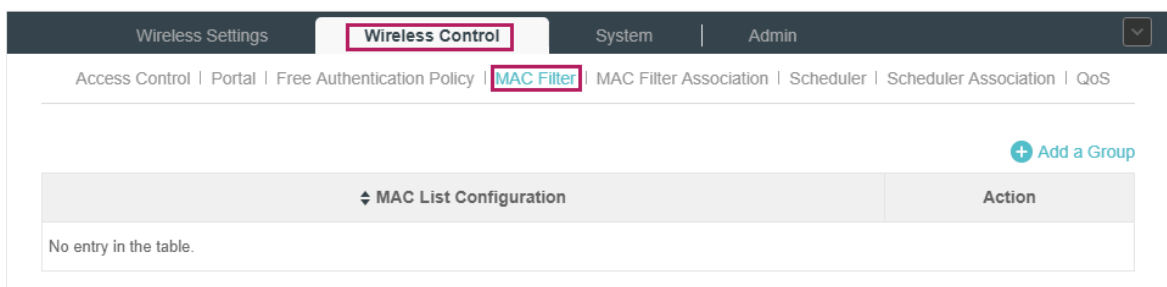
- Click **Apply** and the policy is successfully added.

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.

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

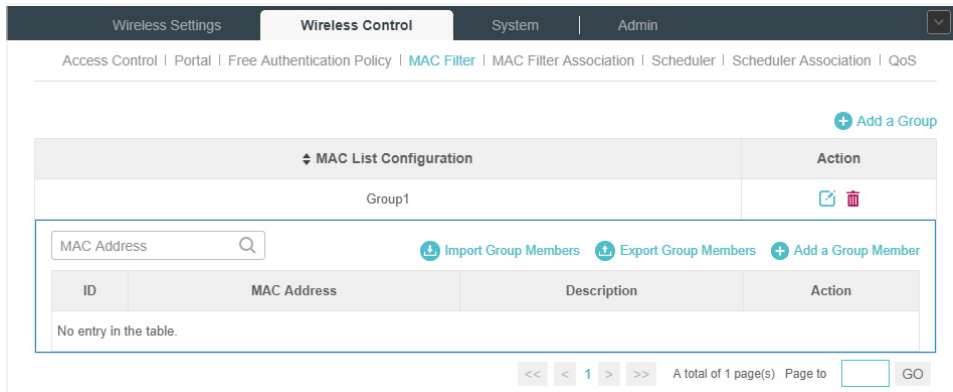


- Click **+ Add a Group** and specify a name for the group.

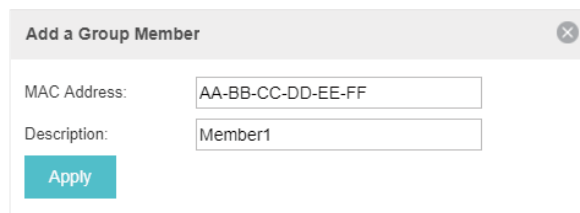
Add a Group ✕

MAC Filter Name:

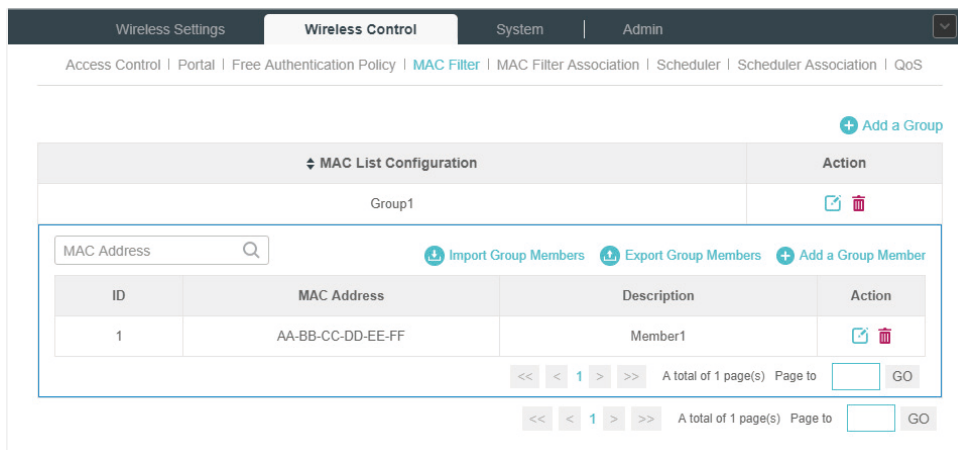
2) Click **Apply** and the group will be successfully added as shown below.



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



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

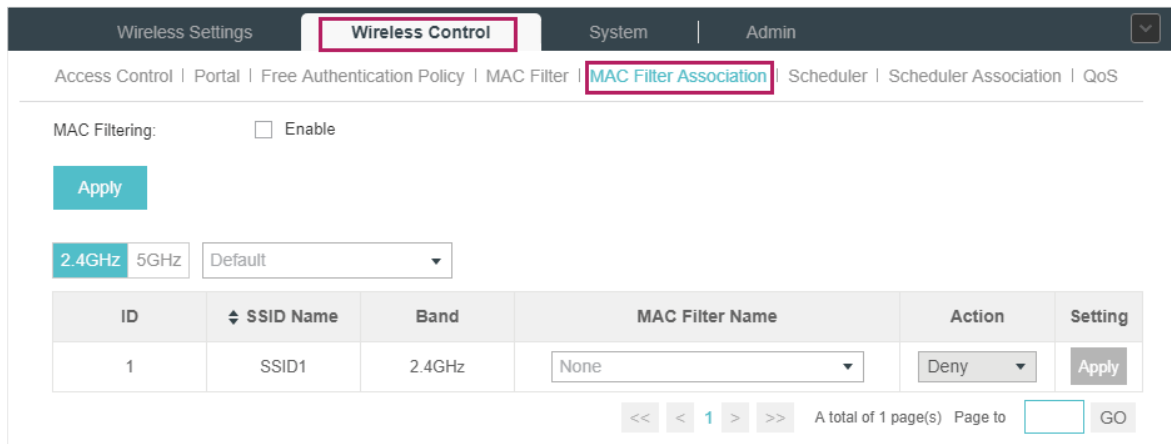


2. You can add more groups or members according to your need.

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.



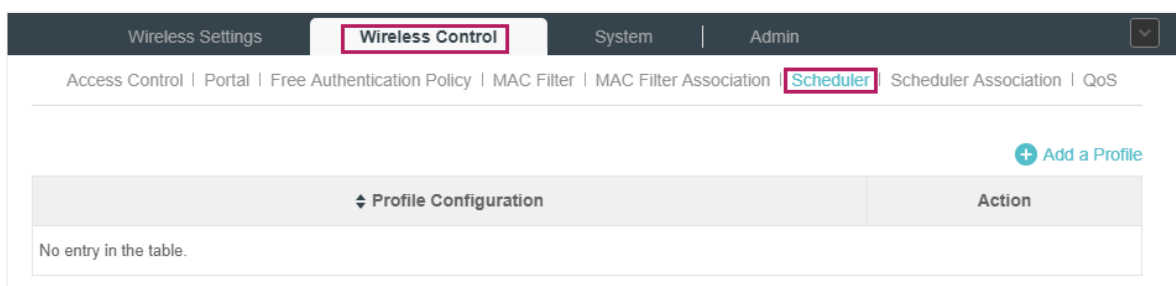
- 1) Check the box and click **Apply** to enable MAC Filtering function.
- 2) Select a band frequency (2.4GHz or 5GHz) and a WLAN group.
- 3) In the MAC Filter Name column of the specified SSID, select a MAC Filter group in the drop-down list. Then select **Allow/Deny** in the Action column to allow/deny 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.

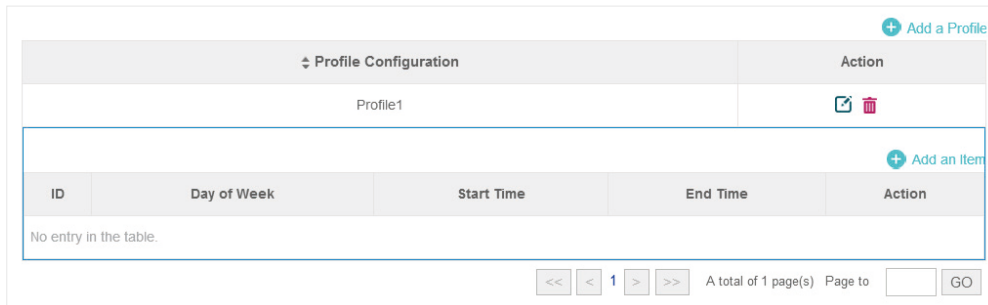


Add a Profile [Close]

Profile Name:

Apply

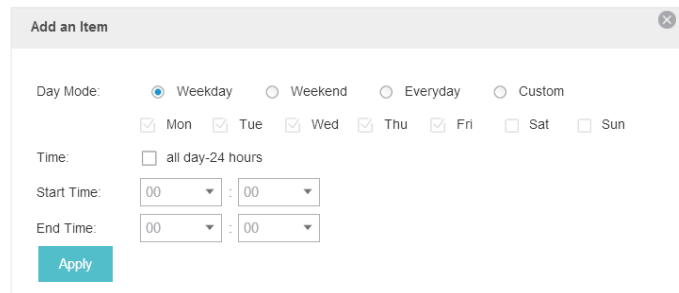
2) Click **Apply** and the profile will be added.



Profile Configuration				Action
Profile1				
ID	Day of Week	Start Time	End Time	Action
No entry in the table.				

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

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



Add an Item [Close]

Day Mode: Weekday Weekend Everyday Custom

Mon Tue Wed Thu Fri Sat Sun

Time: all day-24 hours

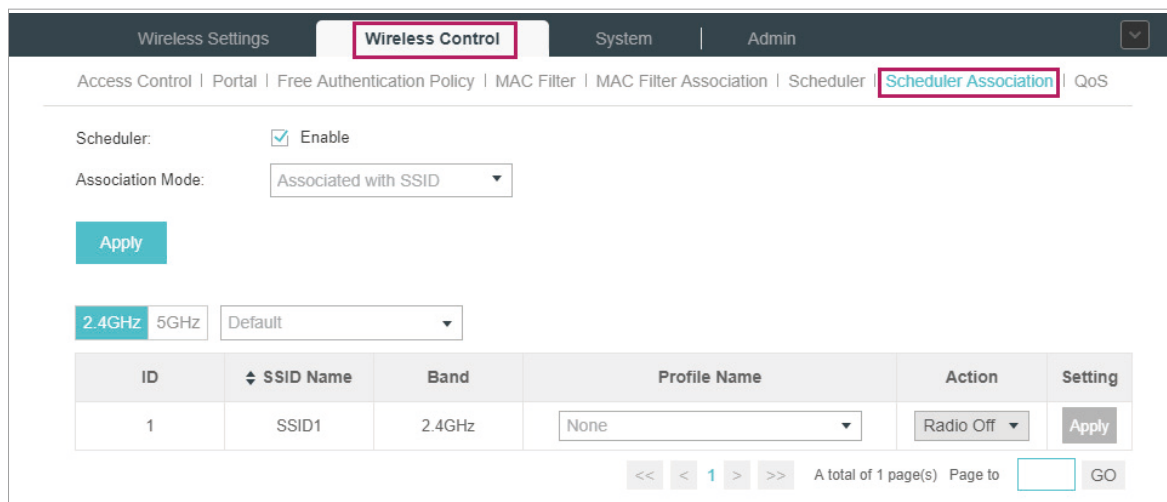
Start Time: :

End Time: :

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:

Apply

2.4GHz 5GHz

ID	SSID Name	Band	Profile Name	Action	Setting
1	SSID1	2.4GHz	<input type="text" value="None"/>	<input type="text" value="Radio Off"/>	Apply

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.

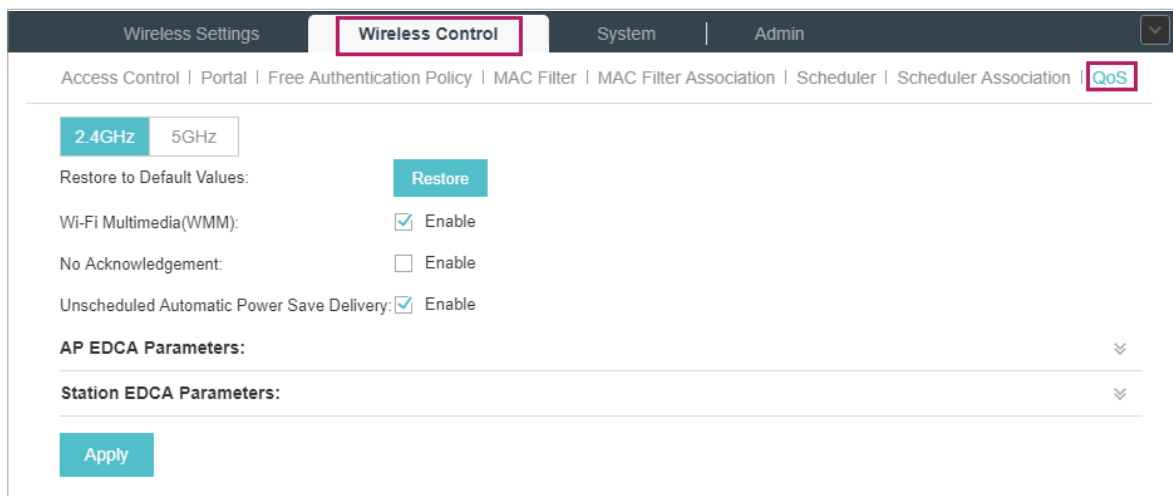
3.7 QoS

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**.



2. Enable or disable the following features.

Wi-Fi Multimedia (WMM)	By default enabled. With WMM enabled, the EAP devices have the QoS function to guarantee the high priority of the transmission of audio and video packets. If 802.11n only mode is selected in 2.4GHz (or 802.11n only, 802.11ac only, or 802.11 n/ac mixed mode in 5GHz), the WMM should be enabled. If WMM is disabled, the 802.11n only mode cannot be selected in 2.4GHz (or 802.11n only, 802.11ac only, or 802.11 n/ac mixed mode in 5GHz).
No Acknowledgment	By default disabled. You can enable this function to specify that the EAP devices should not acknowledge frames with 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	Queue displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters. Data 0 (Voice) —Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. Data 1 (Video) —High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. Data 2 (Best Effort) —Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. Data 3 (Background) —Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
Arbitration Inter-Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values for Arbitration Inter-Frame Space are from 0 to 15.
Minimum Contention Window	A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. This value can not be higher than the value for the Maximum Contention Window .

Maximum Contention Window

The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

This value must be higher than the value for the **Minimum Contention Window**.

Maximum Burst

Maximum Burst specifies the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.

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

Station EDCA Parameters:

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

Apply

Queue

Queue displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters.

Data 0 (Voice)—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.

Data 1 (Video)—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.

Data 2 (Best Effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

Data 3 (Background)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

Arbitration Inter-Frame Space

A wait time for data frames. The wait time is measured in slots. Valid values for **Arbitration Inter-Frame Space** are from 0 to 15.

Minimum Contention Window

A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. This value can not be higher than the value for the **Maximum Contention Window**.

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

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**.

The screenshot shows the 'System' settings page with the 'Reboot Schedule' sub-page selected. The 'Reboot Schedule' link is highlighted with a red box. The configuration options are:

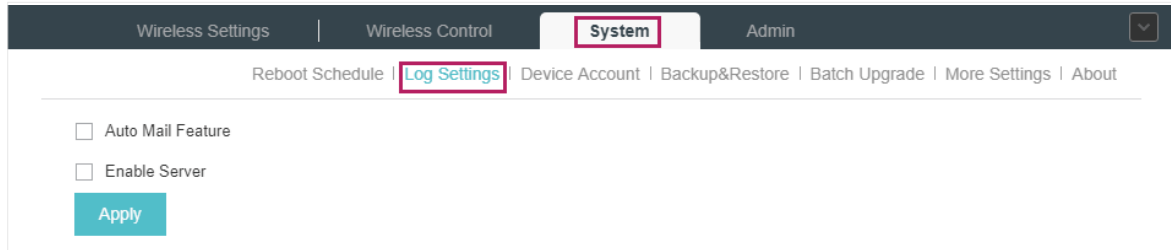
- Enable:** An unchecked checkbox.
- Timing Mode:** A dropdown menu currently set to 'Daily'.
- Reboot Time:** Three dropdown menus for hours, minutes, and seconds, all currently set to '00'.
- Apply:** A teal button at the bottom left.

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. The default port number of the SMTP server is 25 and cannot be changed. And SSL (Security Socket Layer) is not supported here.
Enable Authentication	You can check the box to enable mail server authentication. Enter the sender's mail account name and password.
Time Mode	Select Time Mode. System logs can be sent at specific time or time interval.
Fixation Time	If you select Fixation Time, specify a fixed time to send the system log mails. For example, 08:30 indicates that the mail will be sent at 8:30 am everyday.

Period Time

If you select Period Time, specify a period time to regularly send the system log mail. For example, 6 indicates that the mail will be sent every six hours.

Time Mode:	<input type="radio"/> Fixation Time	<input checked="" type="radio"/> Period Time
Period Time:	<input type="text"/>	Hours(1-24)

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.

<input checked="" type="checkbox"/> Enable Server	
System Log Server IP:	<input type="text" value="0.0.0.0"/>
System Log Server Port:	<input type="text" value="514"/>

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**.

The screenshot shows the Omada Controller web interface. The top navigation bar includes 'Wireless Settings', 'Wireless Control', 'System' (highlighted with a red box), and 'Admin'. Below the navigation bar, the breadcrumb trail is 'Reboot Schedule | Log Settings | Device Account' (with 'Device Account' highlighted in a red box) | Backup&Restore | Batch Upgrade | More Settings | About'. The main content area contains the following fields:

Current Username:	<input type="text" value="admin"/>
Current Password:	<input type="password" value="....."/> <input type="checkbox"/>
New Username:	<input type="text"/>
New Password:	<input type="password"/> <input type="checkbox"/>

At the bottom left of the form is a blue 'Apply' button.

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

Note::

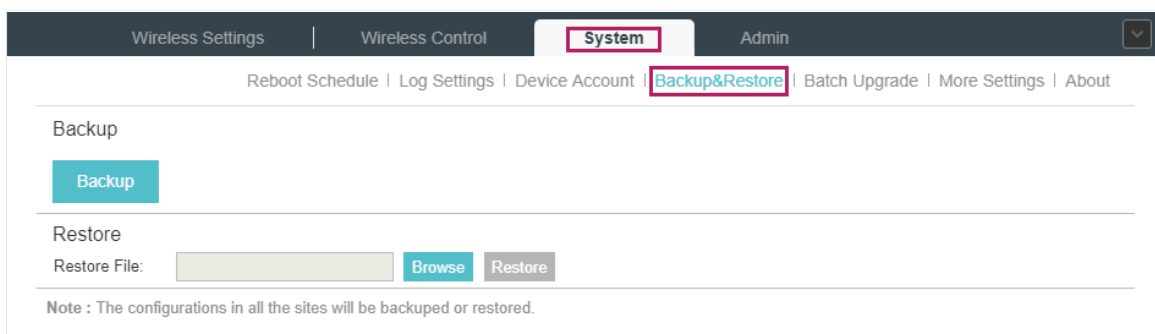
The new account will be applied to EAP devices but not the Omada Controller. To change the Omada Controller's username and password, please refer to [User Account](#).

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 'System' menu with 'Backup&Restore' highlighted. The page has a dark header with 'Wireless Settings', 'Wireless Control', 'System', and 'Admin'. Below the header is a navigation bar with 'Reboot Schedule', 'Log Settings', 'Device Account', 'Backup&Restore', 'Batch Upgrade', 'More Settings', and 'About'. The main content area is titled 'Backup' and contains a 'Backup' button. Below that is the 'Restore' section 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 backedup 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.

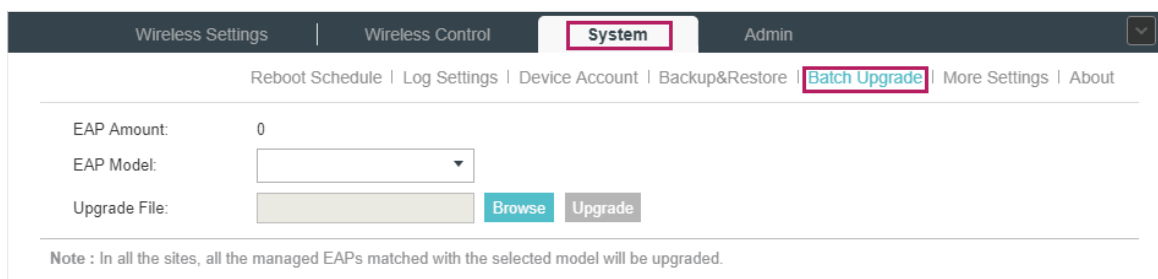
Note:

The configuration of the mesh network will not be backed up. Thus the configuration of the mesh network cannot be restored. You should configure the mesh again if necessary, please refer to [Configure Mesh](#).

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 'System' menu with 'Batch Upgrade' highlighted. The page has a dark header with 'Wireless Settings', 'Wireless Control', 'System', and 'Admin'. Below the header is a navigation bar with 'Reboot Schedule', 'Log Settings', 'Device Account', 'Backup&Restore', 'Batch Upgrade', 'More Settings', and 'About'. The main content area contains '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' menu. The page has a dark header with 'Wireless Settings', 'Wireless Control', 'System' (highlighted), and 'Admin'. Below the header is a navigation bar with 'Reboot Schedule', 'Log Settings', 'Device Account', 'Backup&Restore', 'Batch Upgrade', 'More Settings' (highlighted), and 'About'. The main content area contains several configuration sections:

- Historical Data Retention:** A dropdown menu set to '365 days'. Below it is a note: '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 containing '22' with '(22, 1025-65535)' to its right.
- SSH Login:** An unchecked checkbox.
- Management VLAN:** An unchecked checkbox labeled 'Enable'.
- Management VLAN ID:** A text input field containing '1' with '(1-4094)' to its right.

At the bottom of the form is a blue 'Apply' button. A note at the bottom of the form 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.'

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.

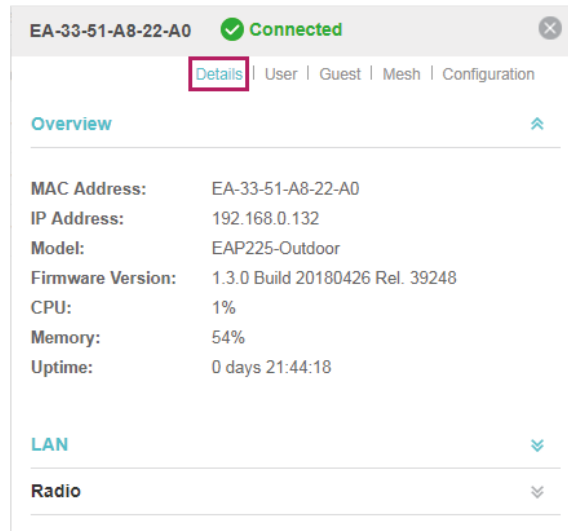
This chapter includes the following contents:

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

4.1 View the Information of the EAP

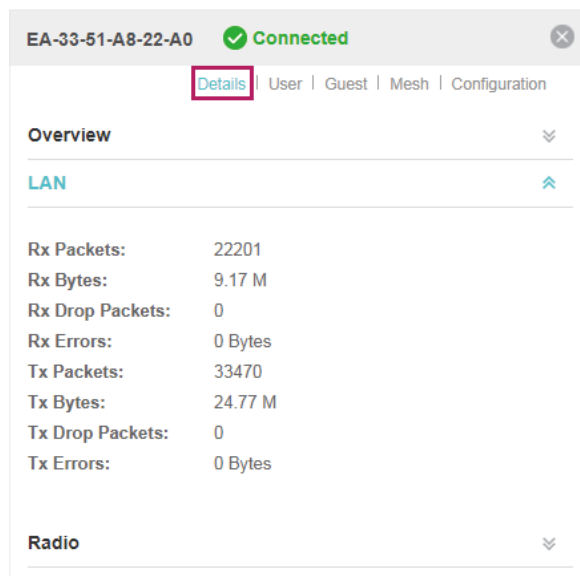
4.1.1 Overview

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.

EA-33-51-A8-22-A0 Connected

Details | User | Guest | Mesh | Configuration

Overview

LAN

Radio

2.4GHz 5GHz

Mode: 802.11b/g/n mixed
Channel Width: 20/40MHz
Channel: 6 / 2437MHz
Tx Power: 20
Rx Packets: 5733663
Rx Bytes: 1.37 G
Rx Drop Packets: 0
Rx Errors: 0 Bytes
Tx Packets: 1537749
Tx Bytes: 303.66 M
Tx Drop Packets: 0
Tx Errors: 0 Bytes

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.

EA-33-51-A8-22-A0 Connected

Details | User | Guest | Mesh | Configuration

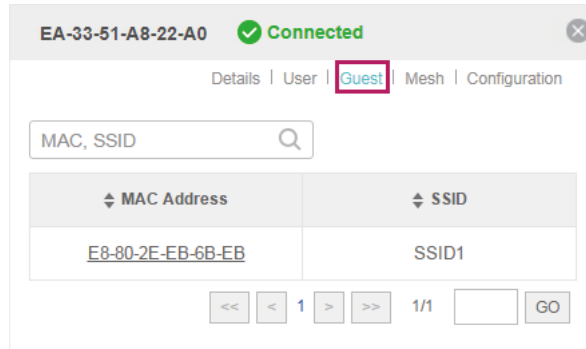
MAC, SSID

MAC Address	SSID
E8-80-2E-EB-6B-EB	SSID1
E8-DE-27-19-1A-81	SSID1

<< < 1 > >> 1/1 GO

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.

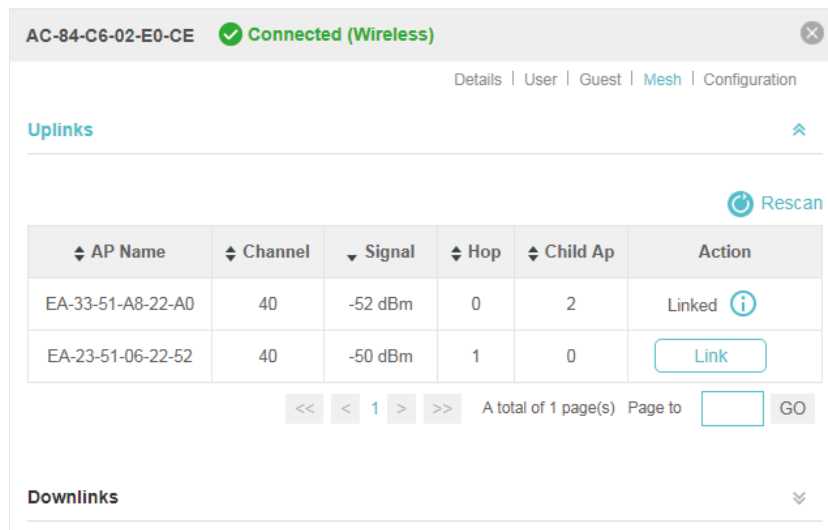


4.3 View Mesh Information of the EAP

You can view and configure mesh parameters of the EAPs on the **Mesh** page.

4.3.1 Uplinks

Here you can view the parameters of the uplink APs or click [Link](#) to change the uplink AP.

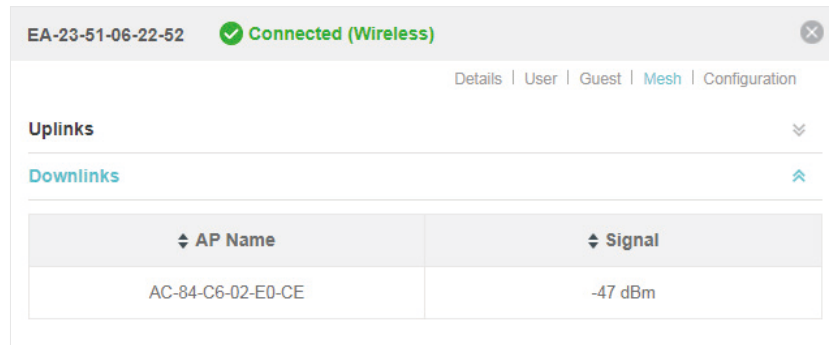


Tips:

You can click [Rescan](#) to search the available uplink APs and the Uplink list will refresh.

4.3.2 Downlinks

Here you can view the downlink APs.

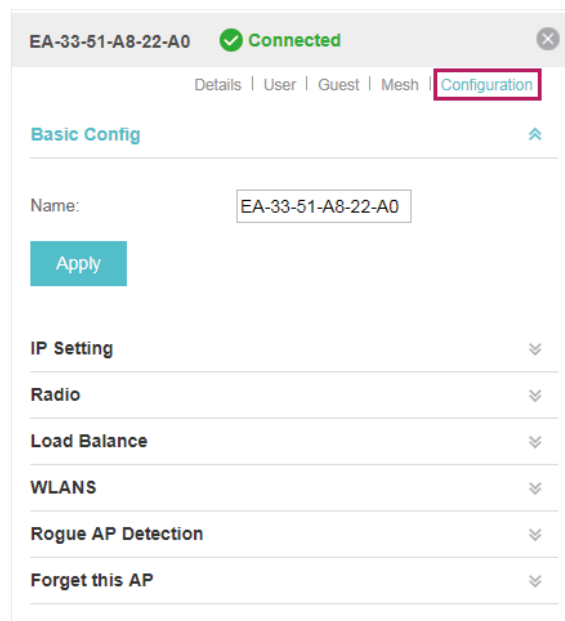


The screenshot shows a configuration window for AP EA-23-51-06-22-52, which is connected wirelessly. The 'Downlinks' section is expanded, showing a table with one entry:

AP Name	Signal
AC-84-C6-02-E0-CE	-47 dBm

4.4 Configure the EAP

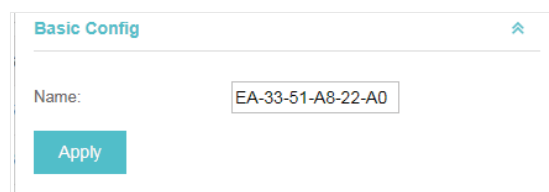
The Configuration page allows you to configure the EAP. All the configurations will only take effect on this device.



The screenshot shows the 'Configuration' page for AP EA-33-51-A8-22-A0. The 'Configuration' tab is highlighted. The 'Basic Config' section is expanded, showing the 'Name' field with the value 'EA-33-51-A8-22-A0' and an 'Apply' button. Other sections like 'IP Setting', 'Radio', 'Load Balance', 'WLANS', 'Rogue AP Detection', and 'Forget this AP' are collapsed.

4.4.1 Basic Config

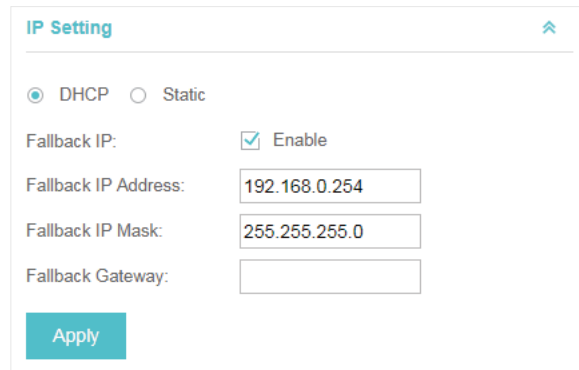
Here you can change the name of the EAP.



This is a close-up of the 'Basic Config' section from the previous screenshot. It shows the 'Name' field containing 'EA-33-51-A8-22-A0' and an 'Apply' button below it.

4.4.2 IP Setting

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



The screenshot shows a configuration window titled "IP Setting" with a close button in the top right corner. At the top, there are two radio buttons: "DHCP" (which is selected) and "Static". Below this, there is a "Fallback IP:" label followed by a checked checkbox and the word "Enable". Underneath, there are three input fields: "Fallback IP Address:" containing "192.168.0.254", "Fallback IP Mask:" containing "255.255.255.0", and "Fallback Gateway:" which is empty. At the bottom left of the form is a blue "Apply" button.

Get a Dynamic IP Address From the DHCP Server

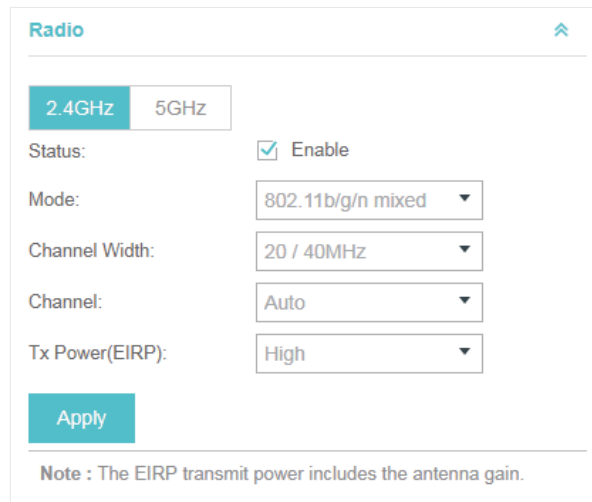
1. Configure your DHCP server.
2. Select **DHCP** on the page above.
3. Enable the Fallback IP feature. When the device cannot get a dynamic IP address, the fallback IP address will be used.
4. Set IP address, IP mask and gateway for the fallback address and click **Apply**.

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**.

4.4.3 Radio

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



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

Status	Enabled by default. If you disable the option, the radio on the frequency band will turn off.
Mode	Select the IEEE 802.11 mode the radio uses. When the frequency of 2.4GHz is selected, 802.11b/g/n mixed, 802.11b/g mixed, and 802.11n only modes are available: 802.11b/g/n mixed: All of 802.11b, 802.11g, and 802.11n clients operating in the 2.4GHz frequency can connect to the EAP device. We recommend you select the 802.11b/g/n mixed mode. 802.11b/g mixed: Both 802.11b and 802.11g clients can connect to the EAP device. 802.11n only: Only 802.11n clients can connect to the EAP device. When the frequency of 5GHz is selected, 802.11 n/ac mixed, 802.11a/n mixed, 802.11 ac only, 802.11a only, and 802.11n only modes are available: 802.11n/ac mixed: Both 802.11n clients and 802.11ac clients operating in the 5GHz frequency can connect to the EAP device. 802.11a/n mixed: Both 802.11a clients and 802.11n clients operating in the 5GHz frequency can connect to the EAP device. 802.11ac only: Only 802.11ac clients can connect to the EAP device. 802.11a only: Only 802.11a clients can connect to the EAP device. 802.11n only: Only 802.11n clients can connect to the EAP device.

Channel 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 20MHz, 40MHz and 20/40MHz.</p> <p>For other EAPs, available options include 20MHz, 40MHz, 80MHz and 20/40/80MHz.</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	<p>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.</p>
Channel Limit	<p>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.</p>
Tx Power (EIRP)	<p>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).</p> <p>Low: Max TxPower * 20% (round off the value)</p> <p>Medium: Max TxPower * 60% (round off the value)</p> <p>High: Max TxPower</p> <p>Custom: Enter a value manually.</p>

4.4.4 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.

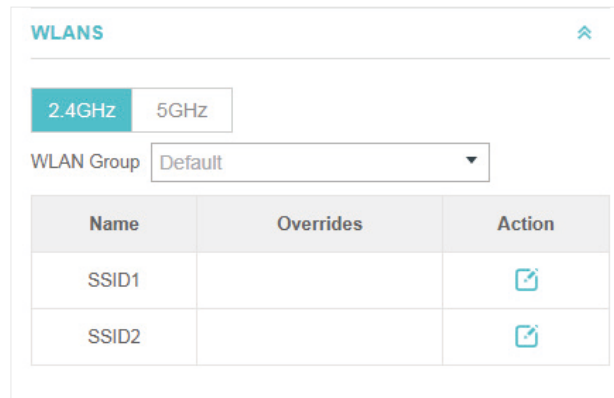
Max Associated Clients	<p>Enable this function and specify the maximum number of connected clients. While more clients requesting to connect, the EAP will disconnect those with weaker signals.</p>
------------------------	---



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.

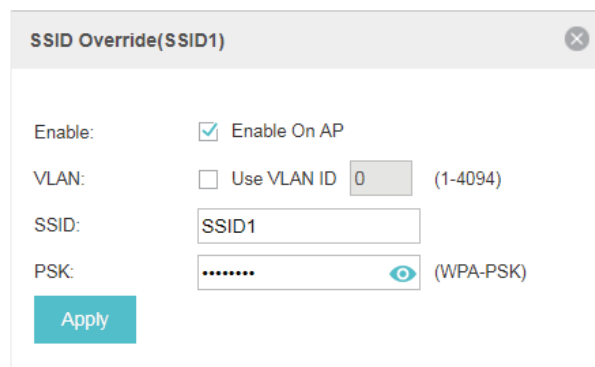
4.4.5 WLANs

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



Name	Overrides	Action
SSID1		
SSID2		


1. Select the frequency band and WLAN group.
2. Click  and the following window will pop up.



Enable: Enable On AP

VLAN: Use VLAN ID (1-4094)

SSID:

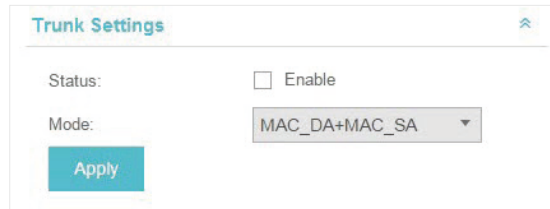
PSK:  (WPA-PSK)

3. Check the box to enable the feature.
4. You can join the overridden SSID in to a VLAN. Check the **Use VLAN ID** box and specify a VLAN ID.
5. Specify a new name and password for the SSID.
6. Click **Apply** to save the configuration.

4.4.6 Trunk Settings

Only EAP330 supports this function.

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



Trunk Settings

Status: Enable

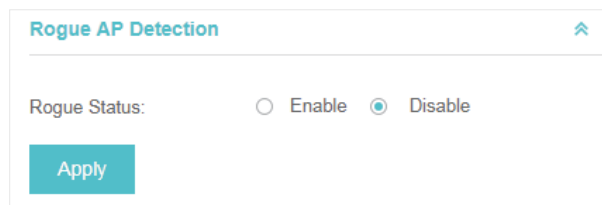
Mode: MAC_DA+MAC_SA

Apply

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">• SRC MAC + DST MAC: When this option is selected, the arithmetic will be based on the source and destination MAC addresses of the packets.• DST MAC: When this option is selected, the arithmetic will be based on the destination MAC addresses of the packets.• SRC MAC: When this option is selected, the arithmetic will be based on the source MAC addresses of the packets.

4.4.7 Rogue AP Detection

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



Rogue AP Detection

Rogue Status: Enable Disable

Apply

4.4.8 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

VLAN

With this feature enabled, you can configure the VLAN which the port belongs to. The hosts connected to this port can then 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.

4.4.9 Forget this AP

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

Forget this AP

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

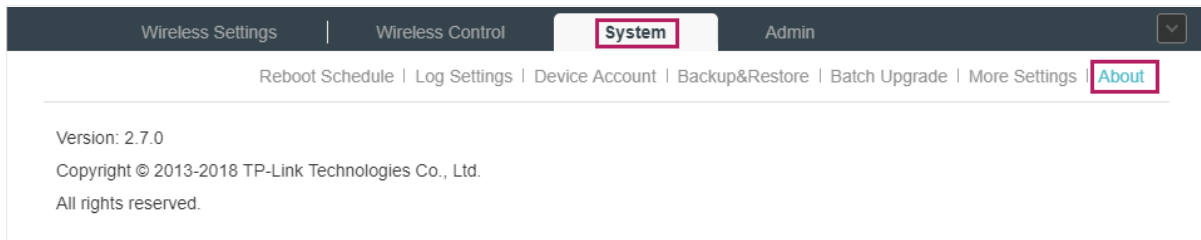
5 **Manage the Omada Controller**

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.



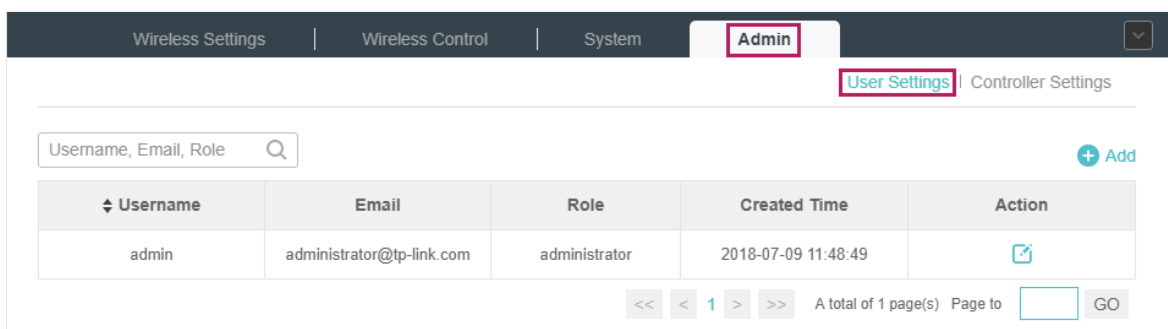
5.2 User Account

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.

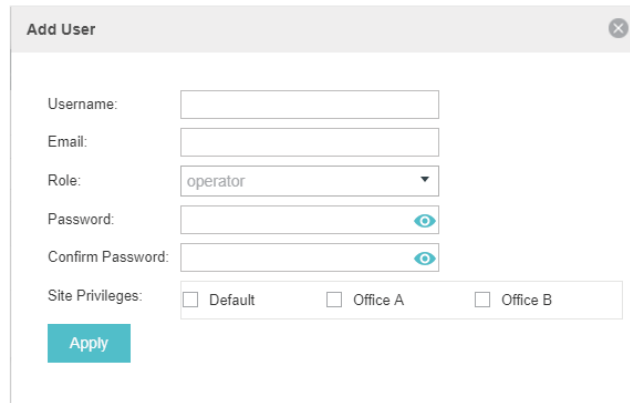
Administrator	The first administrator account is created in the Basic Configuration process and this account can not be deleted. An administrator can change the settings of the EAP network and create and delete user accounts.
Operator	An operator account can be created or deleted by the administrator.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



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.

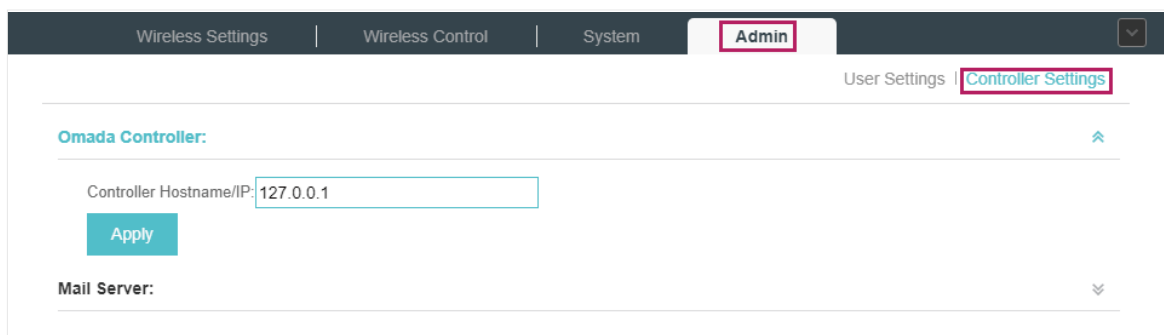
5.3 Controller Settings

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**.



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.

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

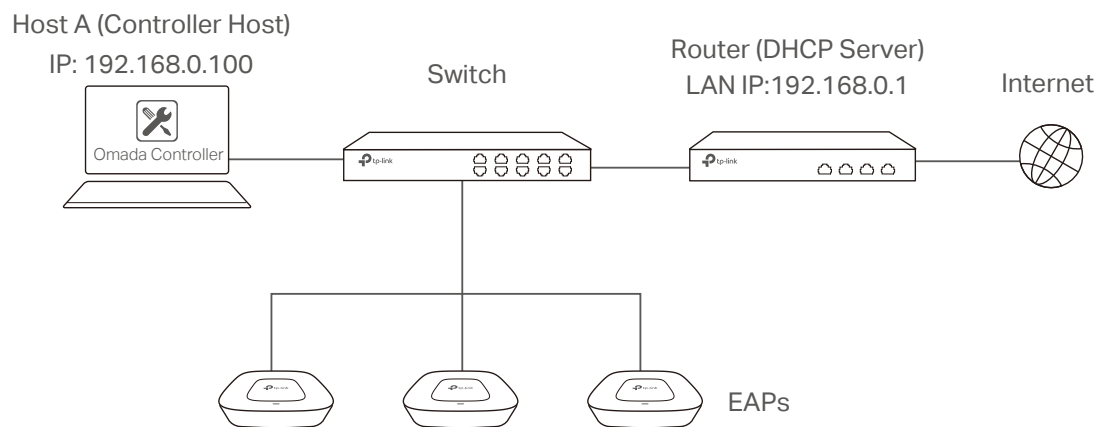
A restaurant has a wireless network with three EAPs managed by the Omada Controller. The network administrator wants to :

- 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

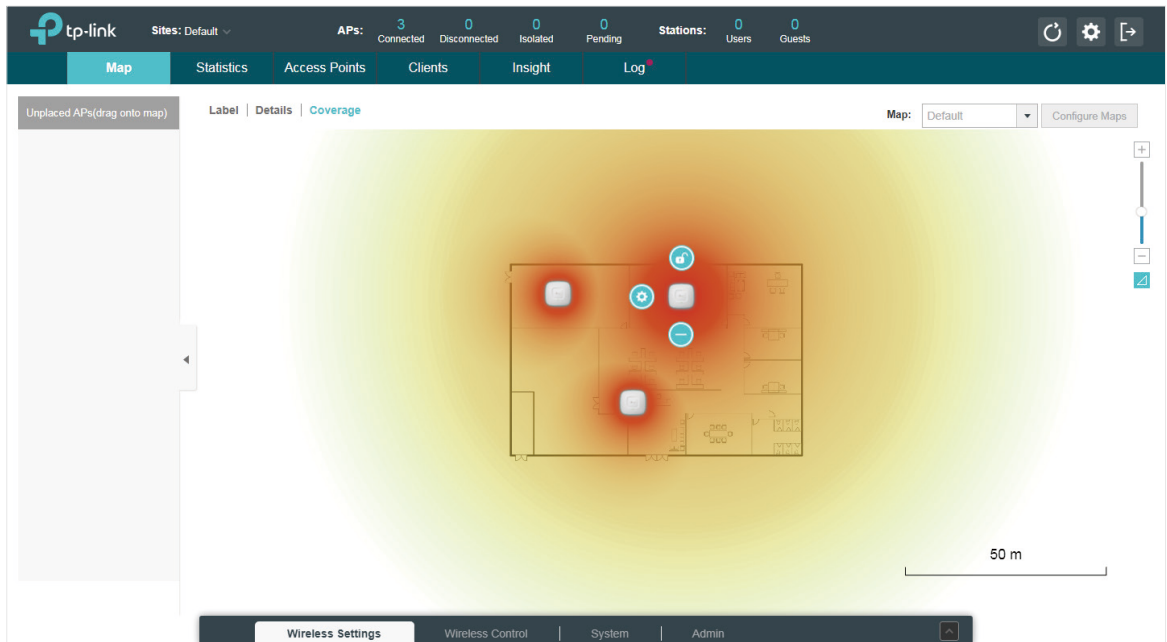
After the basic configuration, refer to the following content to meet the network administrator's requirements.

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

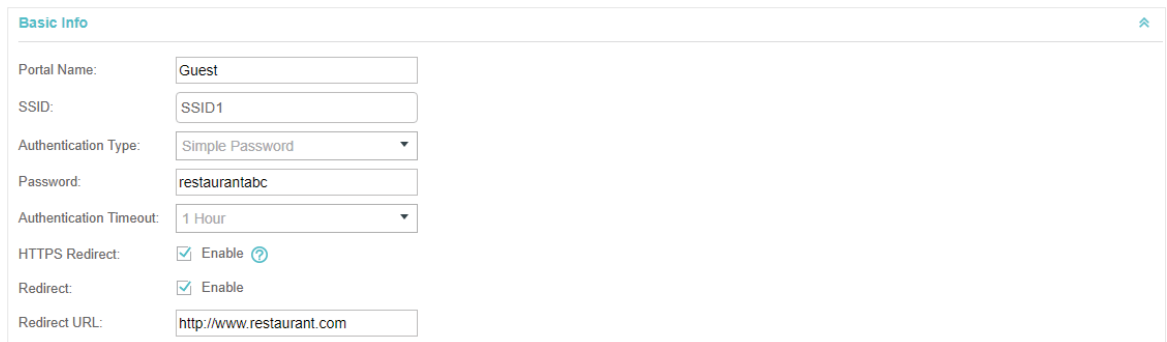
Follow the steps below to configure Portal function.

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

The screenshot shows the 'Edit SSID' configuration window. It has a title bar with 'Edit SSID' and a close button. The 'Basic Info' section is expanded, showing the following fields: 'SSID Name' (text input with 'SSID1'), 'Wireless Vlan ID' (text input with '0', with a note '(0-4094, 0 is used to disable VLAN tagging.)'), 'SSID Broadcast' (checkbox checked, labeled 'Enable'), 'Security Mode' (dropdown menu with 'None' selected), 'SSID Isolation' (checkbox unchecked, labeled 'Enable'), and 'Access Control Rule' (dropdown menu with 'None' selected). Below this is a 'Rate Limit' section which is collapsed. At the bottom, there is an 'Apply' button.

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.

- Open the global configuration window and go to **Portal**. Click  **Add a New Portal** . The configuration window will pop up.
- In the **Basic Info** section, complete the basic settings for the portal.



Basic Info


Portal Name:

SSID:

Authentication Type:

Password:

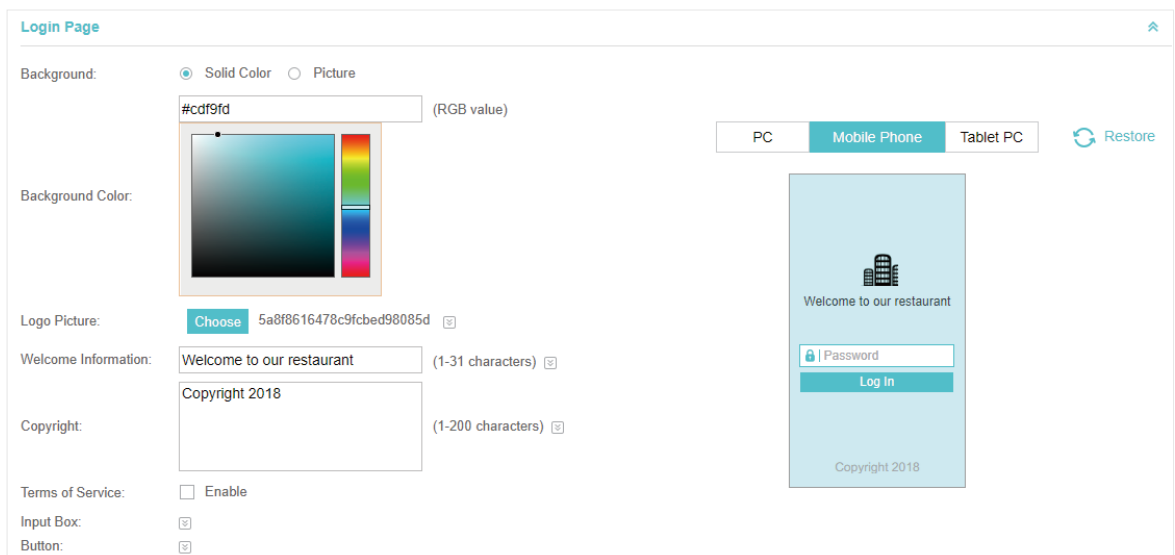
Authentication Timeout:

HTTPS Redirect: Enable 

Redirect: Enable

Redirect URL:

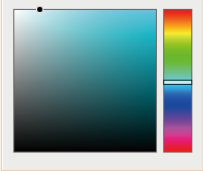
- Specify a name for the portal.
 - Select an SSID for the portal.
 - Select the Authentication Type as Simple Password. Specify a simple password for the guests.
 - Select the **Authentication Timeout**. For example, 1 Hour is suitable for the customers at the restaurant.
 - Enable the **Redirect** to drive the costumers to the restaurant's homepage after successful login. We can put some promotion information on the page.
- In the **Login Page** section, configure the login page.





Login Page


Background: Solid Color Picture

#cdf9fd (RGB value)


Background Color: 


Logo Picture: 5a8f8616478c9fcbed98085d 


Welcome Information: (1-31 characters) 

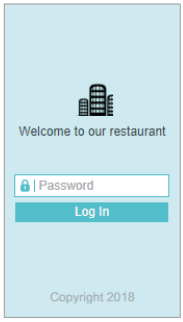
Copyright: (1-200 characters) 

Terms of Service: Enable

Input Box: 

Button: 

PC Mobile Phone Tablet PC  Restore

Preview: 

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

The screenshot shows the 'Advertisement' configuration window. It includes the following fields and options:

- Advertisement:** Enable
- Picture Resource:** (1-5)
 - 5a8f86d1478c9fcbcd980860
 - 5a8f86d5478c9fcbcd980863
- Advertisement Duration Time:** seconds (1-30)
- Picture Carousel Interval:** seconds (1-10)
- Allow Users To Skip Advertisement:** Enable
-

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.

The screenshot shows the 'Add 2.4GHz SSID' configuration window. It includes the following fields and options:

- SSID Name:**
- Wireless Vlan ID:** (0-4094, 0 is used to disable VLAN tagging.)
- SSID Broadcast:** Enable
- Security Mode:**
- 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:**
- Rate Limit**
-

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.

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


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

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.