User Guide

EAP Controller Software

REV 2.4.7
1910011915

CONTENTS

1 Quick Start 1

1.1 Determine the Network Topology 2

Manage EAPs in the LAN 2

Manage EAPs in Different Network Segment 2

1.2 Install the EAP Controller 3

System Requirements 3

Install the EAP Controller 3

1.3 Inform the EAPs of the Controller Host's Address 4

1.4 Basic Configurations and Login 5

Launch the EAP Controller 5

Do the Basic Configurations 5

Log into the Management Interface 7

1.5 Create Sites and Adopt EAPs 7

Create Sites 7

Adopt the EAPs 8

1.6 Monitor and Manage the EAPs 8

2 Monitor and Manage the Network 10

2.1 Monitor the Network with the Map 11

Add a Map 11

Monitor the EAPs on the Map 13

2.2 View the Statistics of the Network 14

View the Client Distribution on SSID 14

Have a Quick Look at EAPs and Clients 14

View Current Usage-Top APs 15

View Recent Activities 15

2.3 Monitor and Manage the EAPs 16

Manage the EAPs in Different Status 16

View the Detailed Information of EAPs 17
Manage the EAPs in the Action Column 17
2.4 Monitor and Manage Clients 18
View the Current Information of Clients 18
Manage Clients in the Action Column 18
2.5 View Clients Statistics During the Specified Period 19
Select a Specified Period 19
View the History Information of Clients 19
Manage Clients in the Action Column 20
2.6 Manage the Rogue APs List 20
Manage the Untrusted Rogue APs List 20
Manage the Trusted Rogue APs List 21
2.7 View Past Guest Authorization 22
2.8 View Logs 22
2.9 View Alerts 23
3 Configure the EAPs Globally 24
3.1 Wireless Network 25
Add Wireless Networks 25
Configure Advanced Wireless Parameters 30
Configure Band Steering 31
3.2 Access Control 32
3.3 Portal Authentication 33
No Authentication 34
Simple Password 35
Hotspot 36
External Radius Server 40
External Portal Server 42
3.4 Free Authentication Policy 43
3.5 MAC Filter 43

3.6 Scheduler 45
3.7 QoS 47
3.8 System 50
Reboot Schedule 50
Log Setting 50
Device Account 52
LED 52
SSH 53
Management VLAN 53
Backup&Restore 53
Batch Upgrade 54
4 Configure the EAPs Separately 55
4.1 View the Information of the EAP 56
Overview 56
LAN 56
Radio 57
4.2 View Clients Connecting to the EAP 57
User 57
Guest 58
4.3 Configure the EAP 58
Basic Config 58
IP Setting 59
Radio 59
Load Balance 61
WLANs 61
Trunk Settings 62
Rouge AP Detection 62
Forget this AP 63
Local LAN Port VLAN Settings 63

5 Manage the EAP Controller 64
5.1 Information About the Software 65
5.2 User Account 65
5.3 Controller Settings 66
Configure Controller Hostname/IP 66
Configure Mail Server 67
6 Application Example 68
6.1 Basic Configuration 69
6.2 Advanced Settings 69
Monitor the EAPs with Map 69
Configure Portal Authentication 70
Create a SSID for the Employees 72
Configure Scheduler 73

1 Quick Start

The EAP Controller is a management software for the TP-LINK EAP devices. It allows you to centrally manage your EAP devices using a web browser. You can configure EAPs in batches and conduct real-time monitoring of each EAP in the network.

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

1. Determine the Network Topology

2. Install the EAP Controller Software

3. Inform the EAPs of the Controller Host's Address

4. Basic Configurations and Login

5. Create Sites and Adopt the EAPs

6. Monitor and Manage the EAPs

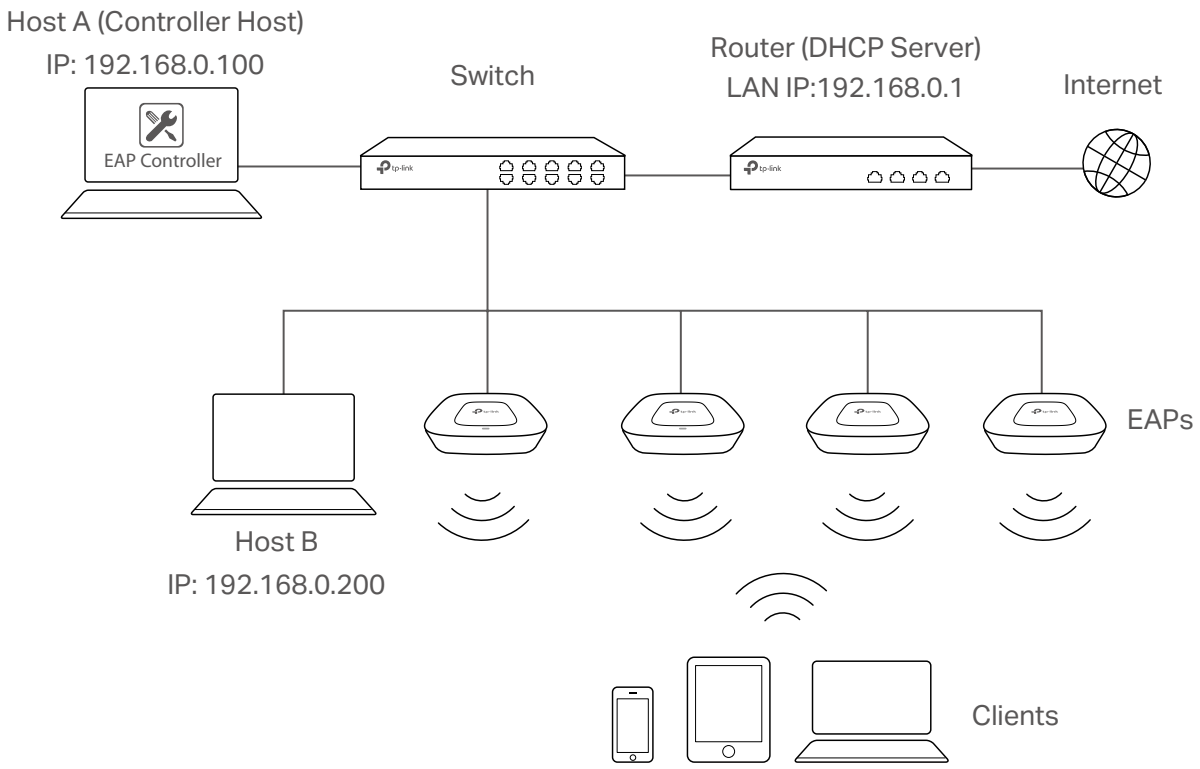
1.1 Determine the Network Topology

You can use the EAP Controller to centrally manage the EAPs in same or different network segment.

Manage EAPs in the LAN

If you want to manage the EAPs with a host in the LAN, refer to the following network topology.

A router acts as a DHCP server to assign IP addresses to EAPs and clients. In the LAN, only one host needs to install EAP Controller. The host is called as Controller Host. And the other hosts in the same LAN can access the Controller Host to manage the network. In this topology, you can visit EAP Controller interface from Host B by entering "192.168.0.100: 8043" in a web browser. It's recommended to set a static IP address to the Controller Host for the convenient login to the EAP Controller interface.



☞ Note:

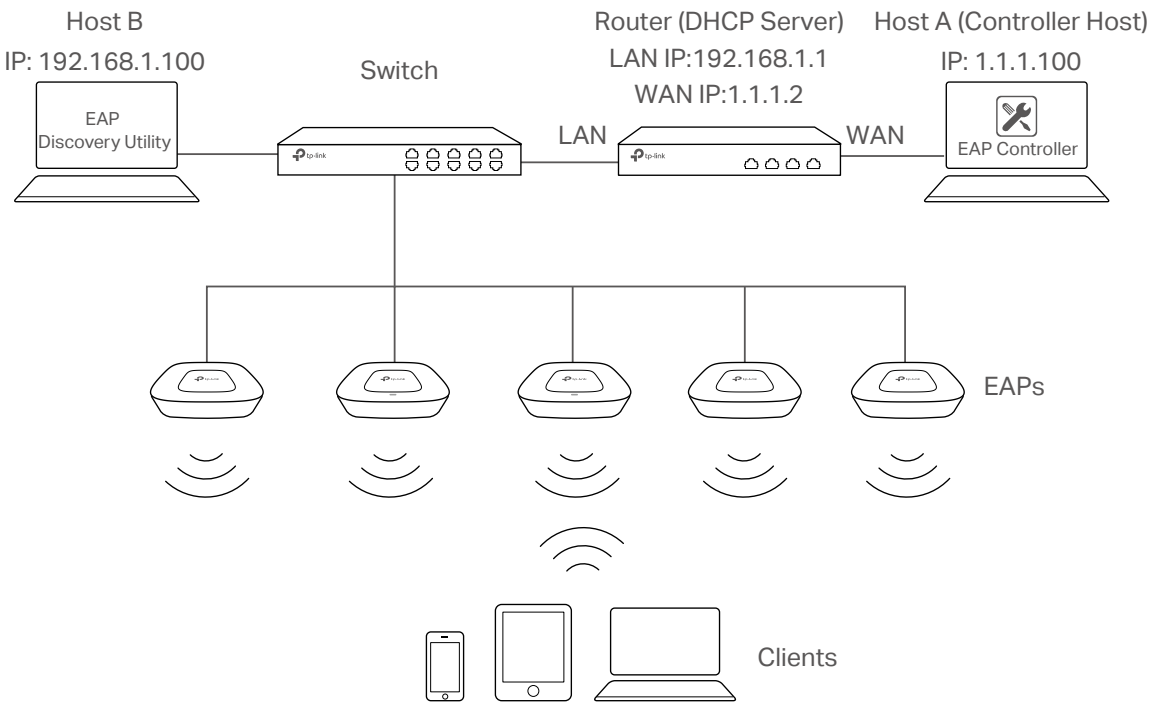
The EAP Controller must be running all the time when you manage the network.

Manage EAPs in Different Network Segment

If the Controller Host needs to manage EAPs in different network segment, refer to the following topology.

A router acts as a DHCP server to assign IP addresses to EAPs and clients. The Controller Host and the EAP devices are connected to the Router's different network segments. To help the EAPs find the Controller Host and be managed, EAP Discover Utility should be installed in the Host B which is

in the same LAN with the EAPs. Please refer to 1.3 Inform the EAPs the Controller Host's Address for detailed instructions.



1.2 Install the EAP Controller

Make sure the Controller host meets the following system requirements and properly install the EAP Controller software.

System Requirements

Operating System: Microsoft Windows XP/Vista/7/8/10.

Web Browser: Mozilla Firefox 32 (or above), Google Chrome 37 (or above), Opera 24 (or above), or Microsoft Internet Explorer 8-11.

☞ Note

We recommend you deploy the EAP controller on a 64-bit operating system to guarantee the software stability.

Install the EAP Controller

Get the installation file of EAP Controller on the resource CD provided with your EAP device or download it from our website *http://www.tp-link.com/en/support/download/*. Then follow the on-screen instructions to properly install the EAP Controller software. After successful installation, a shortcut icon of the EAP Controller will be created on your desktop.

1.3 Inform the EAPs of the Controller Host's Address

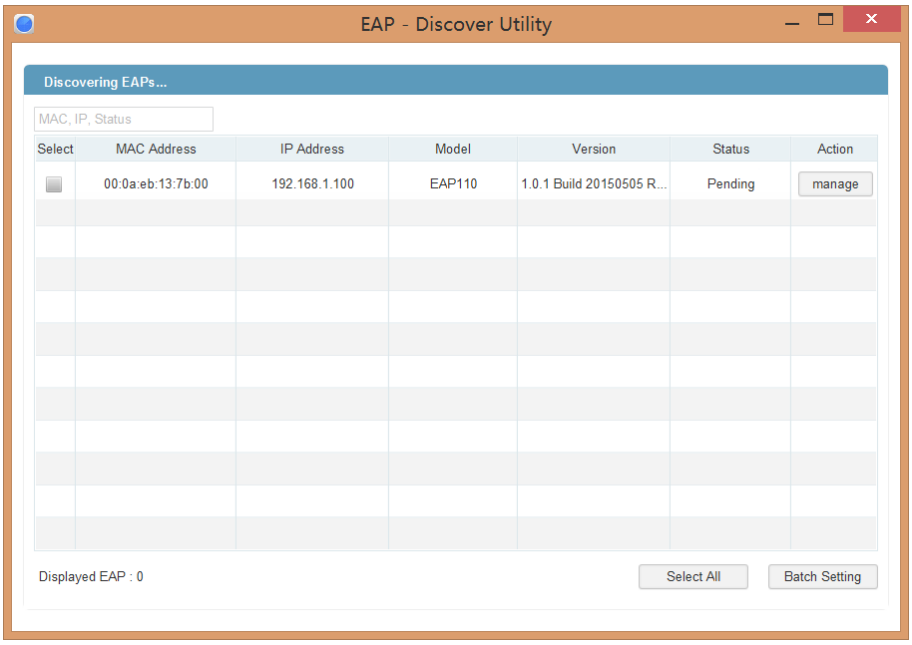
If your Controller Host is in the same LAN with the EAPs, you can skip this section.

If you want to manage EAPs in different network segment with your Controller Host, please follow the steps below to help the EAPs find the Controller Host.

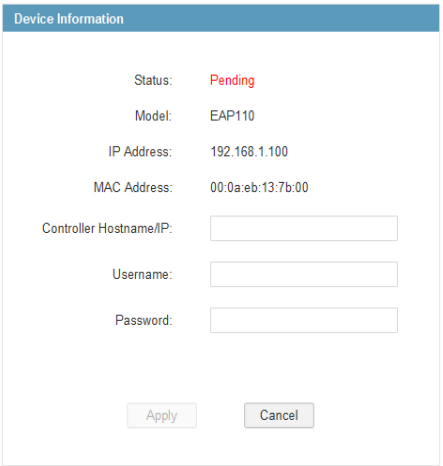
1. Install the EAP Controller on the computer that is in the same LAN with the EAPs. The EAP Discover Utility is installed automatically in the EAP Controller installation process.

2. Go to the installation path of the EAP Controller to find the EAP Discover Utility.

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



4. Click **manage** in the **Action** column or select multiple EAPs and click **Batch Setting**.



5. Enter the Controller hostname or IP address.

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

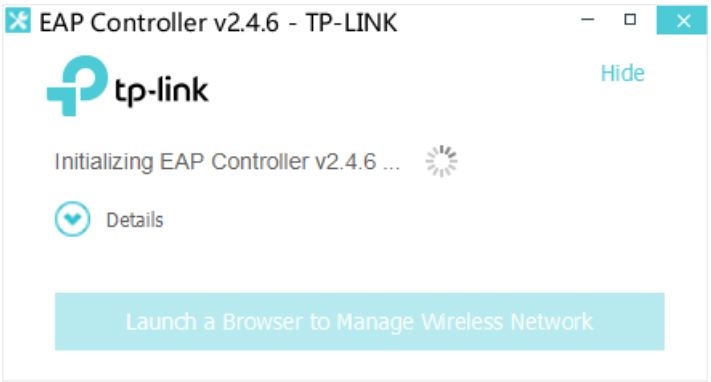
7. Click **Apply** to inform the EAP of the Controller's hostname or IP address.

1.4 Basic Configurations and Login

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

Launch the EAP Controller

Launch the EAP Controller 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.



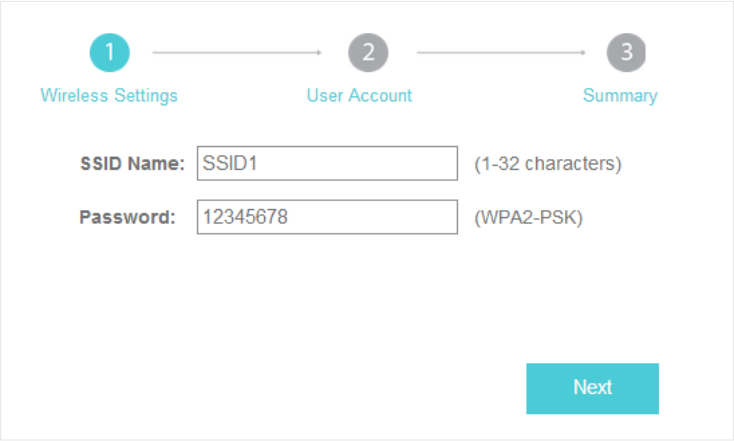
☞ **Note:**

- If your browser does not open, please click **Launch a Browser to Manage Wireless Network**.
- If it opens but prompts a problem with the website's security certificate, please click **Continue to this website**.

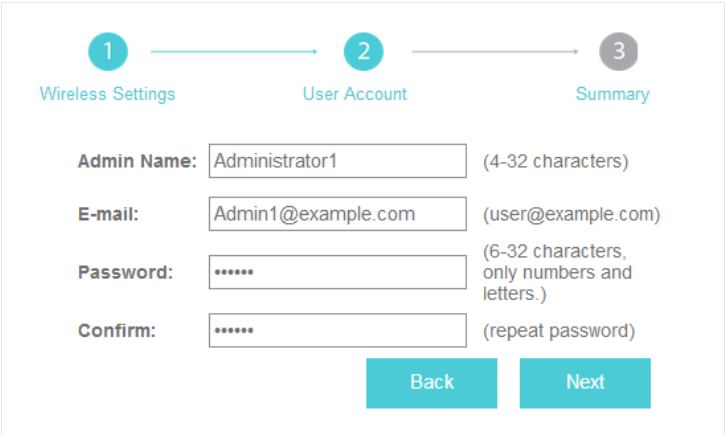
Do the Basic Configurations

In the web browser you can see the configuration page. Follow the steps below and provide the information required.

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



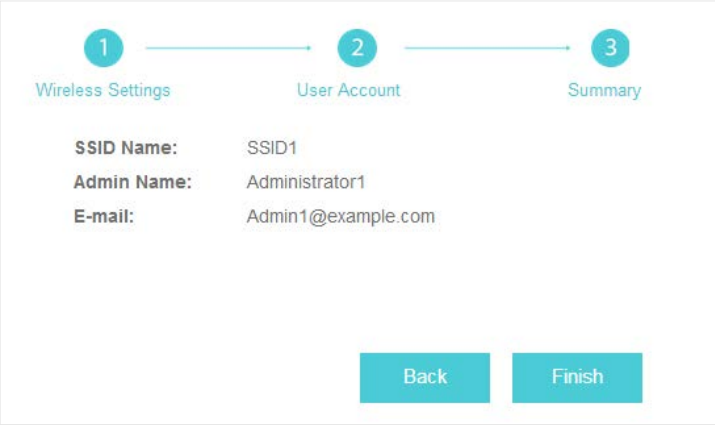
2. Configure the admin name and password to create an administrator account. Specify the email address to receive the notification emails and reset your password if necessary. Click **Next**.



☞ Note:

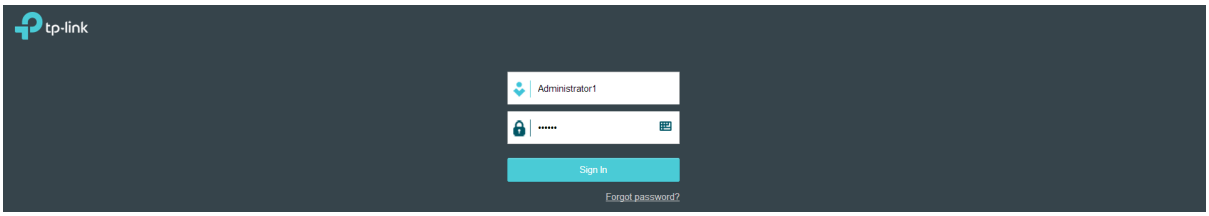
After logging into the EAP Controller, please set a mail server so that you can receive the notification emails and reset your password if necessary. Please refer to Configure Mail Server.

3. Review your settings and click **Finish** to save the configurations.



Log into the Management Interface

Once the basic configuration is finished, the browser will be redirected to the following page. Please log into the management interface of EAP Controller with the username and password you have set in the basic configuration.



☞ Note:

In addition to the Controller Host, other computers in the same LAN can also manage EAP devices via remote access to the Controller Host. For example, when the IP address of the Controller Host is 192.168.0.100 and the EAP 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 computers in the same LAN to log into the management interface and manage EAP devices.

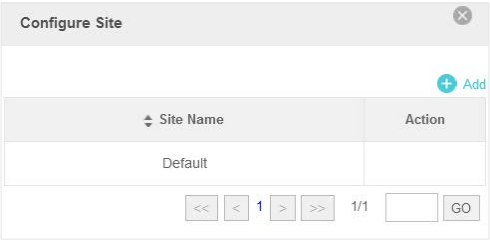
1.5 Create Sites and Adopt EAPs

The EAP Controller can manage multiple EAP networks, which are called sites. Each site has its own configurations. The multiple sites are logically separated, and the initial site is named **Default**. If you have no need to manage EAPs on different sites, you can use the default site and skip the **Create Sites** section. However, adopting the pending EAPs is a necessary step to manage the EAPs.

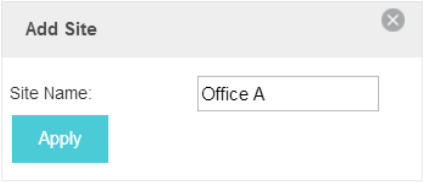
Create Sites

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.



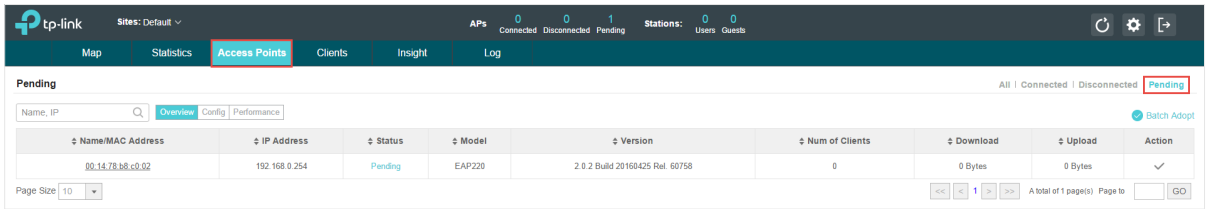
3. Click **Apply** to create the site.

Adopt the EAPs

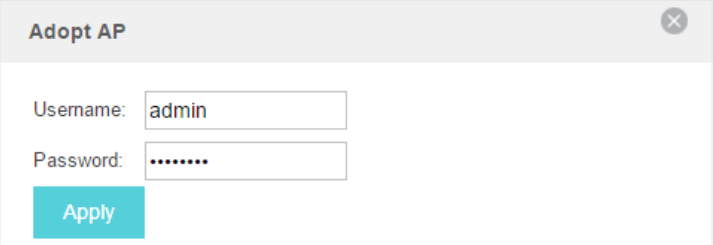
The EAP Controller can discover all EAP devices currently connected in the network and display their connection statuses on the management interface. As shown below, all the EAPs are in the **Pending** status by default. Only the **Connected** EAPs could be managed, so you need to adopt the **Pending** ones to change their status to **Connected**.

Follow the steps below to adopt EAPs on a specific site.

1. Select a site and go to **Access Points > Pending**.



2. Click ✓ in the **Action** column and enter the username and password of the EAPs (both admin by default). You can also click Batch Adopt to adopt all the **Pending** EAPs.



3. Click **Apply** to adopt the EAPs.

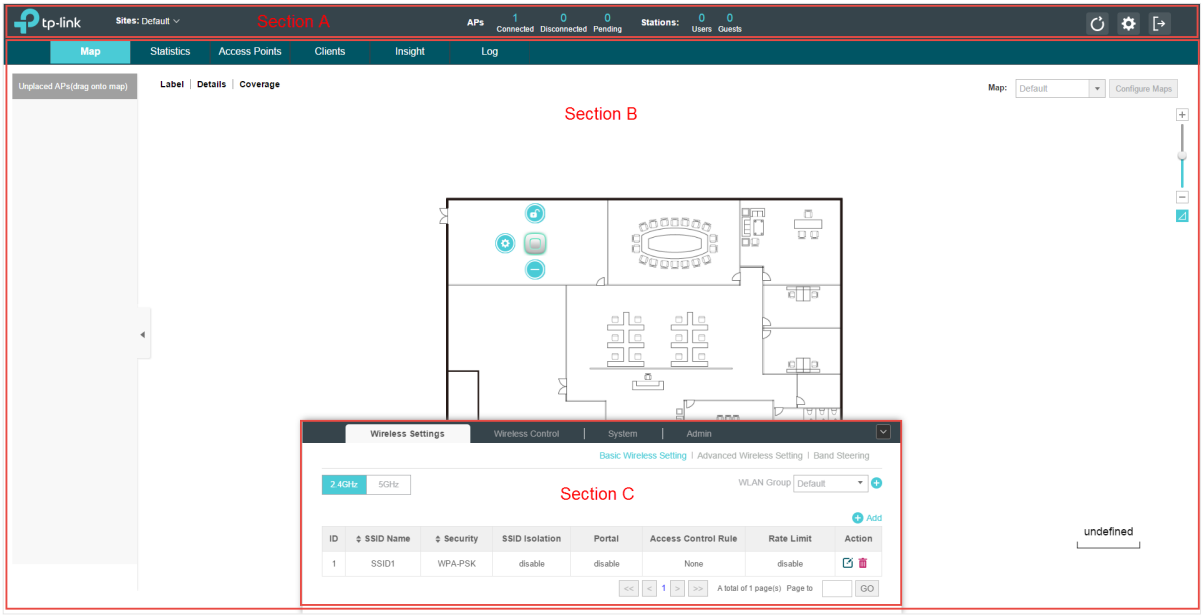
4. After a while, the EAPs will be successfully adopted. The EAPs' username and password will become the same as those of the Controller's administrator account you created in the Basic Configuration.

☞ Note

If you want to change the EAPs' username and password, please 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 EAP Controller's management interface. The management interface is mainly divided into three sections as the following screen.



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 configuration results will take effect on all the adopted EAPs.

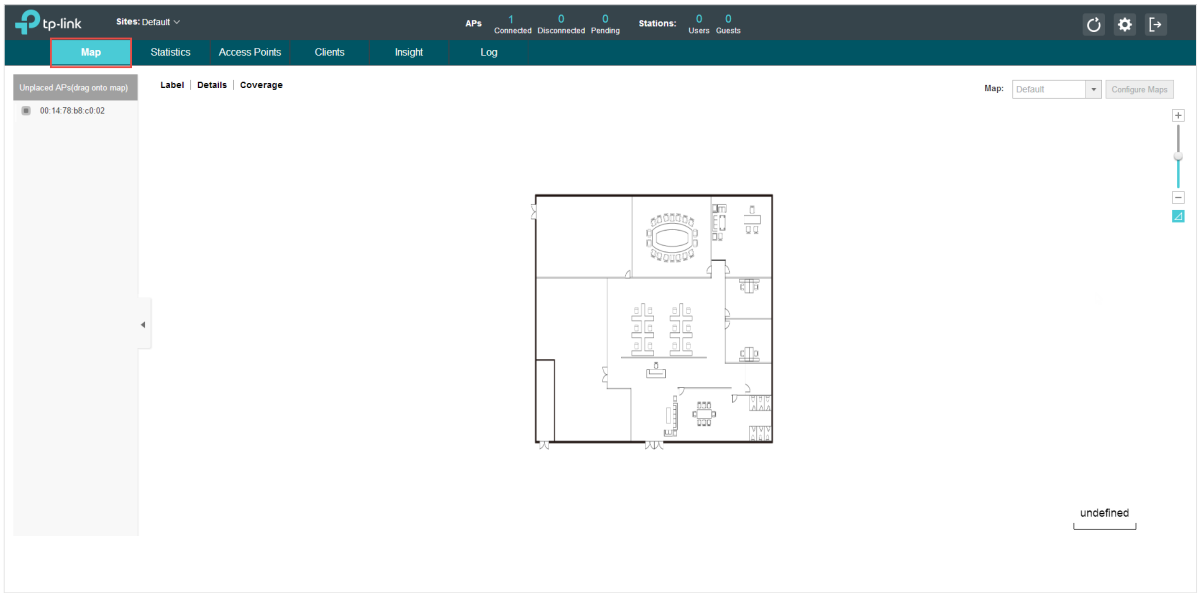
2 Monitor and Manage the Network

With the EAP 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 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

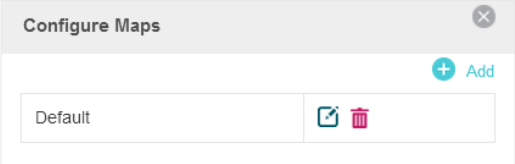
The EAP Controller allows you to upload your local map images and monitor the status and coverage range of each EAP device with the map. When you initially launch the EAP Controller, a default map is displayed. The legend at the bottom of the map shows the scale of the map.



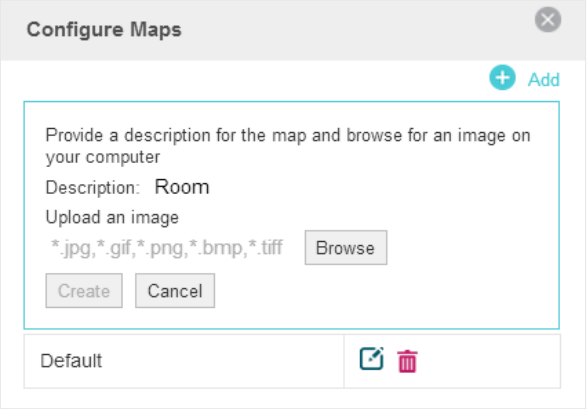
Add a Map

To add a custom map, you must first create the image in .jpg, .gif, or .png file format. And then follow the steps below to add a map.

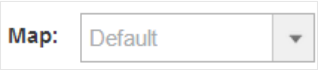
1. Click **Configure Maps** on the upper right corner of map and click **Add.**



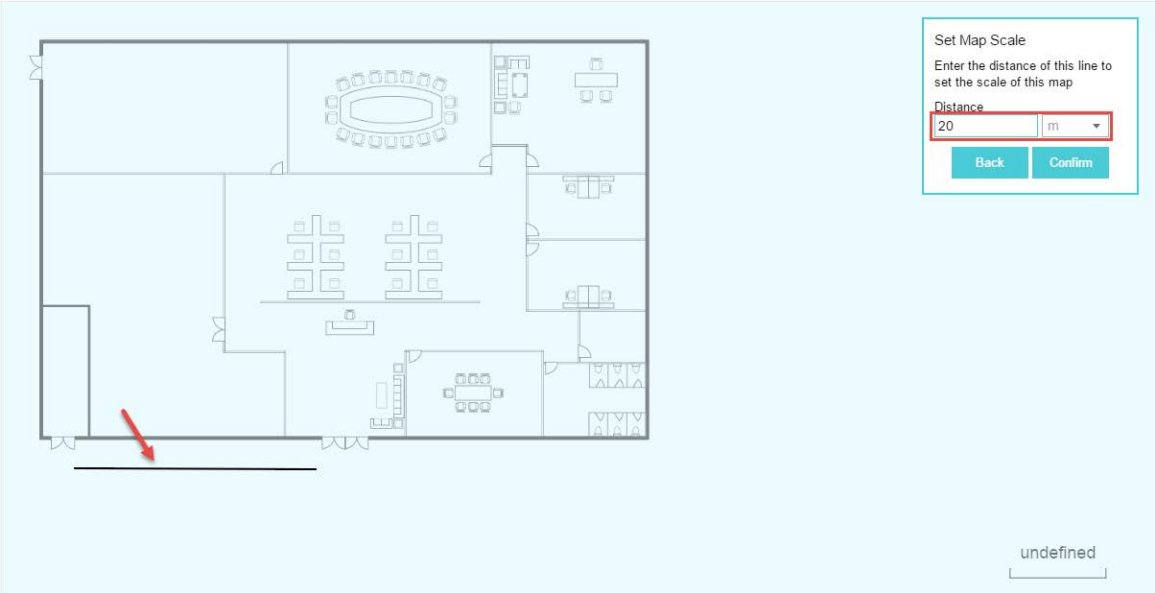
2. Enter the map description, select your customized map image, and click **Create**.



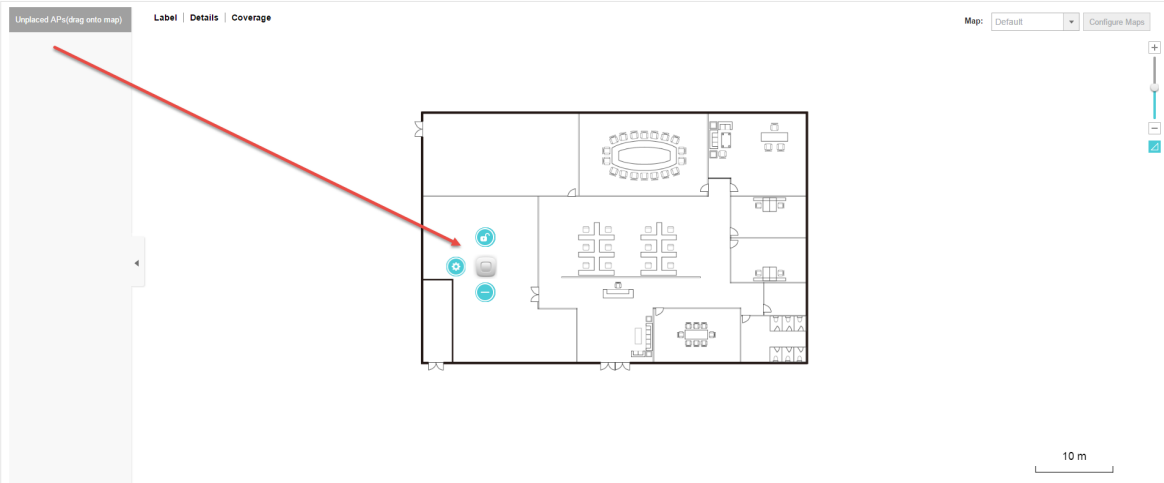
3. Select your local map from the drop-down list on the upper right corner of map area.



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



5. Drag the unplaced EAPs from the **Unplaced APs** list to 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.

Monitor the EAPs on the Map

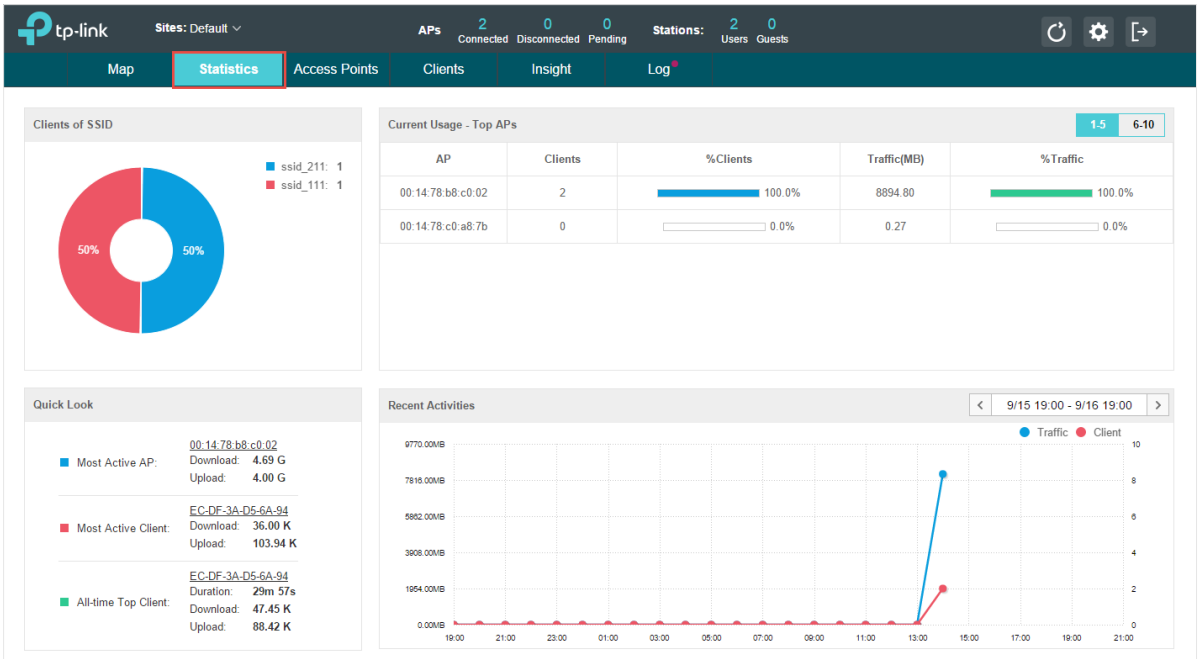
Click any of the following options to display EAP Label, Details, and Coverage on the map.

Label | Details | Coverage

Label	Display the EAP's name. The default name is EAP's MAC address.
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.

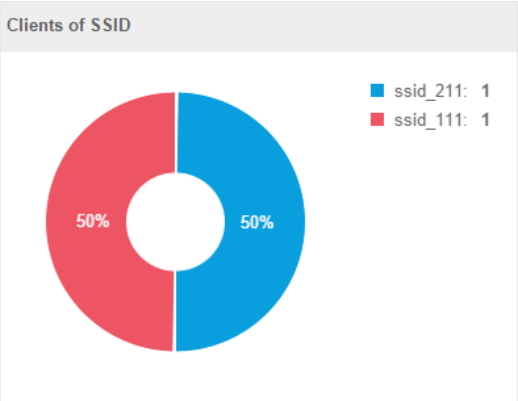
2.2 View the Statistics of the Network

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



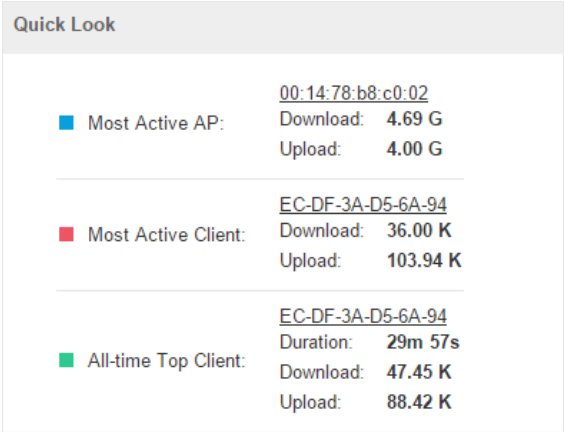
View the Client Distribution on SSID

A visual pie chart represents the client distribution on each SSID. For example, the SSID 1 has 2 clients, which occupies 67% of all the clients.



Have a Quick Look at EAPs and Clients

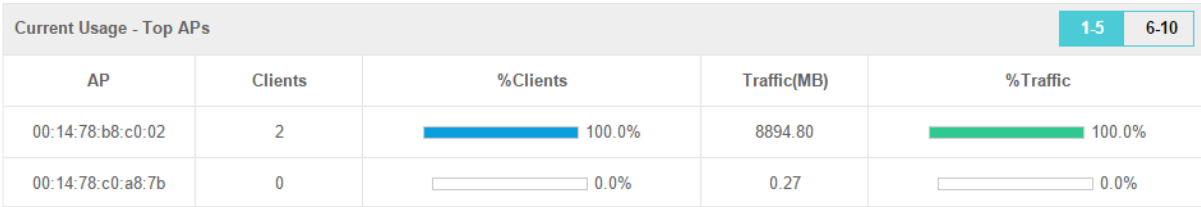
This tab displays the **Most Active AP**, the **Most Active Clients** and the **All-Time Top Client**. You can click the MAC address of the EAP or the client to see more details.



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.

View Current Usage-Top APs

This tab lists the hostname, the number of connected clients and the data traffic condition of the ten APs with the most traffic currently.



AP	Clients	%Clients	Traffic(MB)	%Traffic
00:14:78:b8:c0:02	2	100.0%	8894.80	100.0%
00:14:78:c0:a8:7b	0	0.0%	0.27	0.0%

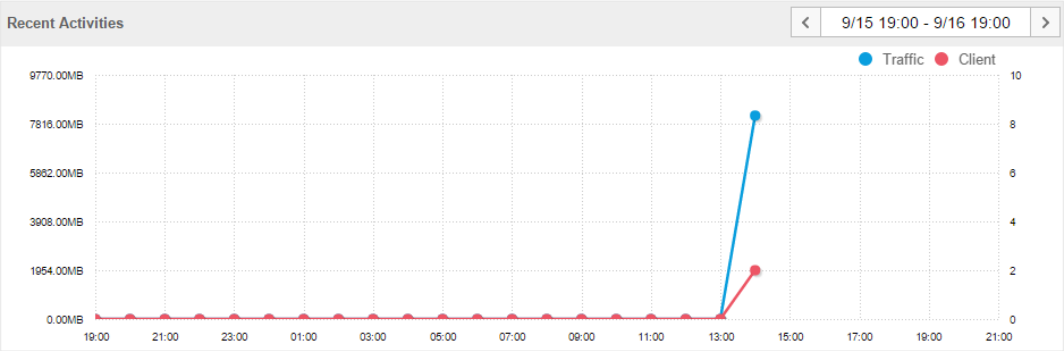
Clients	The amount of clients connected to this AP.
%Clients	The proportion of current connected clients to the Top APs' total client amount.
Traffic	The total amount of data transmitted by this AP, which equals the sum of the transmission traffic of all the current clients that connect to the AP.
%Traffic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

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.

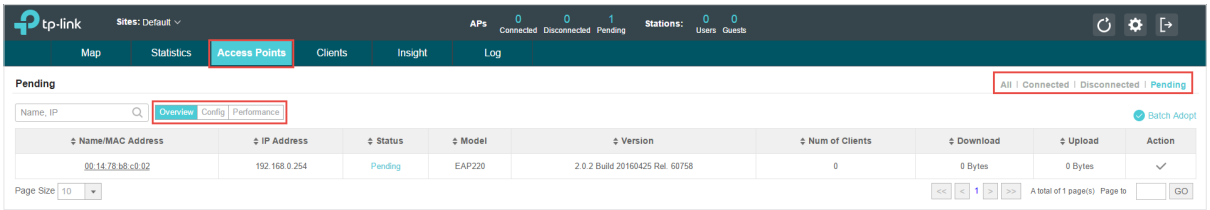
The left ordinate axis indicates the traffic and the right one represents the number of the clients. The abscissa axis shows the selected time period. **Traffic** indicates a visual graph of the network

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 10:00 indicates the traffic size and client number from 9:00 to 10:00. In the following figure, at 10 o'clock, the traffic is about 8 and there is 1 client connected to the AP.



2.3 Monitor and Manage the EAPs

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



Manage the EAPs in Different Status

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

All | Connected | Disconnected | Pending

All	Displays the information of all the EAPs in different status.
Pending	Displays the pending EAPs. All the EAPs are in pending state by default when first discovered by the EAP Controller, and only after they are adopted and connected, you can monitor and manage them. To adopt pending EAPs, please refer to Adopt EAPs.
Connected	Displays the connected EAPs. Only connected EAPs can be managed. After you adopt a pending EAP, its status will become provisioning and then connected. A connected EAP will turn into a pending one after you forget this EAP. You can refer to Forget this AP to forget a EAP or click **Forget All** on the page to forget all the connected EAPs.

Disconnected	Displays the diconnected EAPs. If a connected or pending EAP powers off, it will be disconnected. When a disconnected EAP is reset to factory default settings or you forget it, 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.

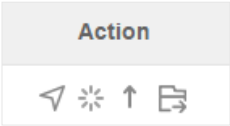
View the Detailed Information of EAPs

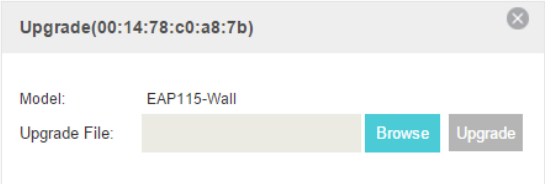
You can click **Overview**, **Config**, and **Performance** tab to view different detailed information of EAPs.

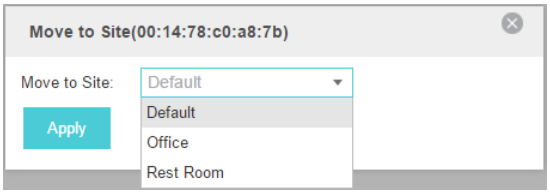
Overview	**Overview** displays the EAP's name/MAC address, IP address, status, model, software version, number of connected clients and download/upload bytes.
Config	**Config** displays the EAP's name/MAC address, IP address, status, model, software version, WLAN Group bounded with the 2G and 5G of the EAP, and radio of the 2G and 5G.
Performance	**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.

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 complete and the EAP reconnects to the EAP Controller. 

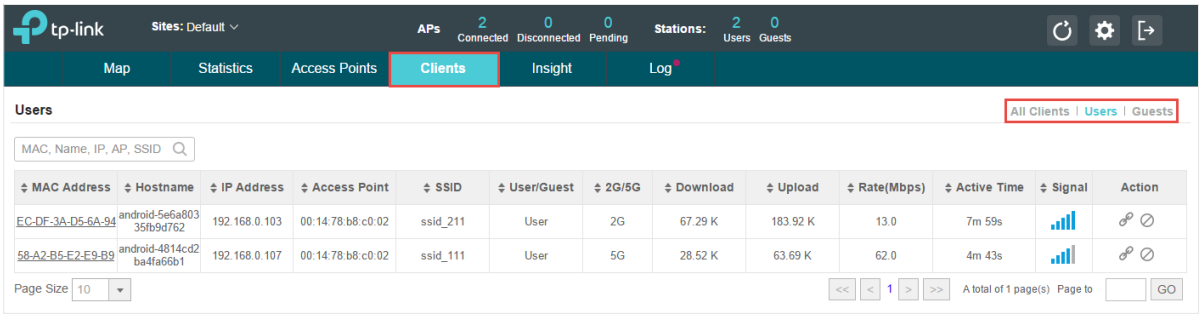
	Move the EAP to a site. Select a site that has been created and click **Apply**. You can group all the EAPs by this way and centrally manage them on each site. 

Note

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

2.4 Monitor and Manage Clients

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



View the Current Information of Clients

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

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

All Clients | Users | Guests

All Clients	The page will display the informaiton of all clients including users and guests.
Users	The page will display the informaiton of Users.
Guests	The page will display the informaiton of Guests.

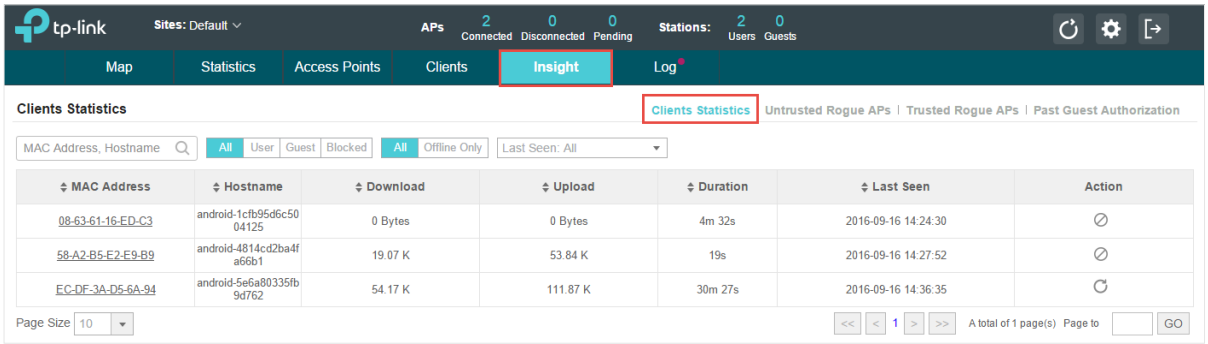
Manage Clients in the Action Column

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

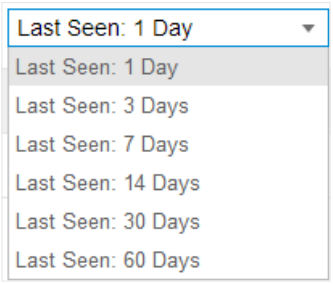
2.5 View Clients Statistics During the Specified Period

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



Select a Specified Period

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



View the History Information of Clients

You can click the client's MAC address to get its connection history or click the following tabs to view the information of different types of clients:

All	The page will display the history information of all the clients.

User	The page will display the history informaiton of Users. Users are the clients connected to the EAP wireless network without the Portal Authentication.
Guest	The page will display the history informaiton of Guests. Guests are the clients connected to the EAP wireless network with the Portal Authentication.
Blocked	The page will display the clients that have been blocked.

All	The page will display the history information of all clients.
Offline Only	The page will display the history informaiton of the offline clients.

Manage Clients in the Action Column

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

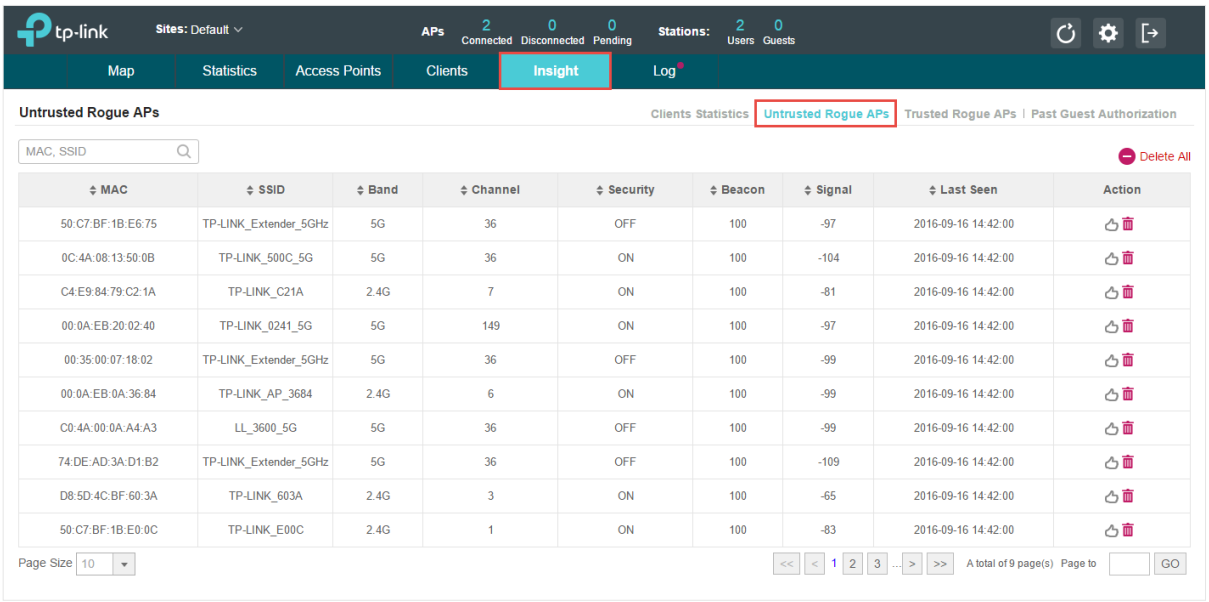
⊘	Block the client's access to the network.
↻	Resume the client's access.

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 EAP 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 rouge APs to the **Trusted Rogue APs** list.

Manage the Untrusted Rogue APs List

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

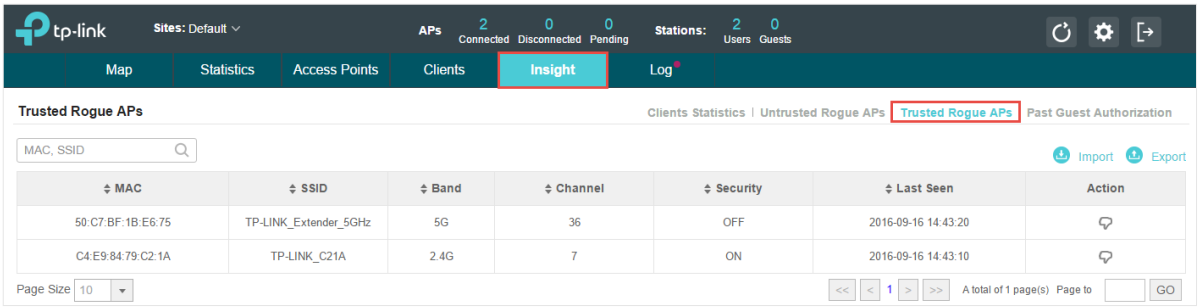


You can execute the corresponding operation to the EAP by clicking an icon in the **Action** column:

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

Manage the Trusted Rogue APs List

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

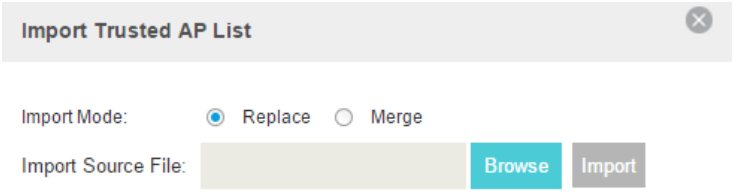


You can execute the corresponding operation to the EAP by clicking an icon in the **Action** column:

	Move the trusted rogue AP to the Untrusted Rogue APs list.
Export	Export and download the current Trusted Rogue APs list and save it on your PC.

Import

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

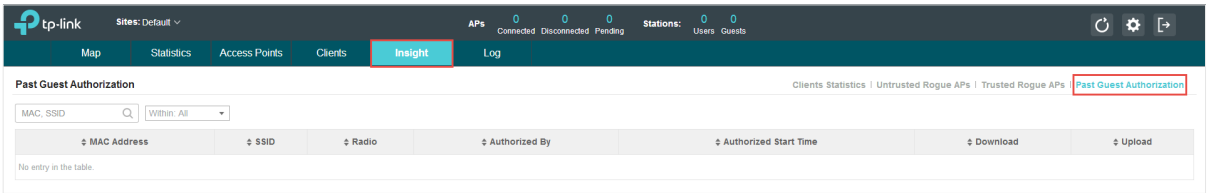


Please follow the steps below:

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.

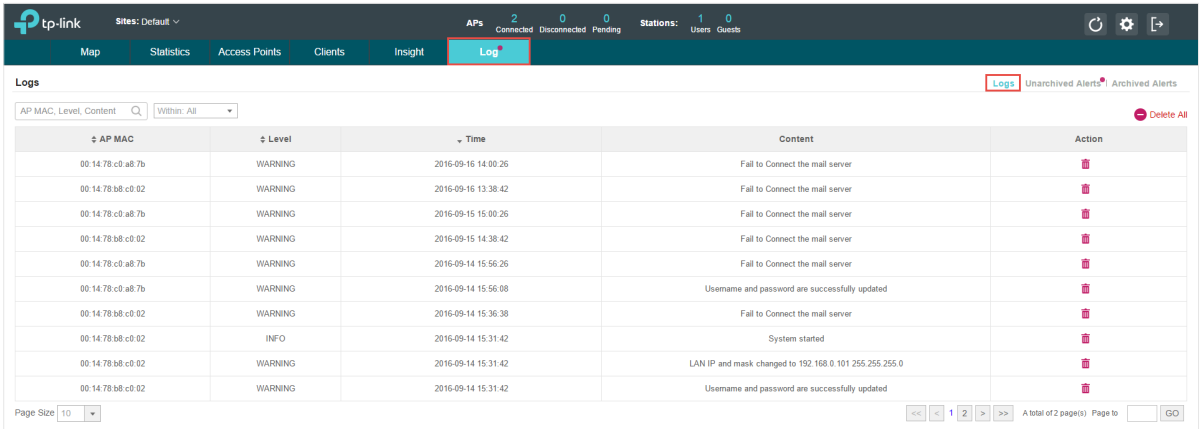
2.7 View Past Guest Authorization

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.



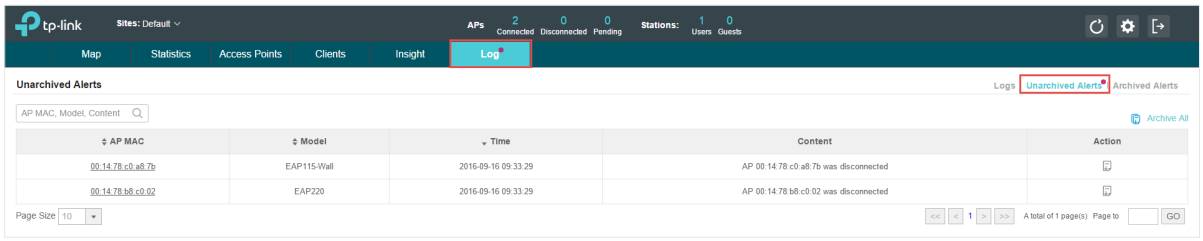
2.8 View Logs

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

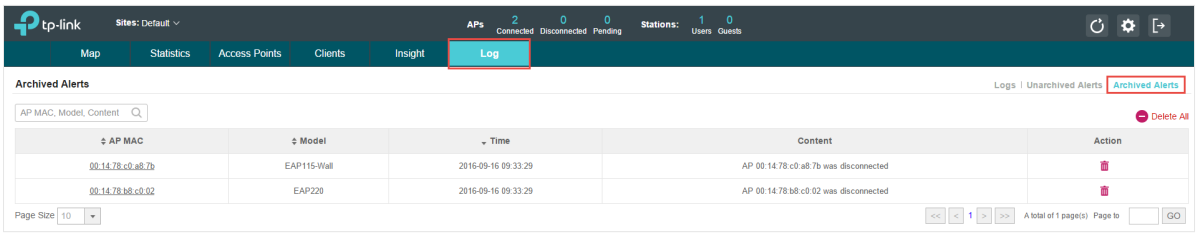


2.9 View Alerts

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.



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



3 Configure the EAPs Globally

This chapter introduces the global configuration that will be applied to all the managed EAPs. If you need to configure a specified EAP, please refer to Chapter 4 Configure the EAPs Separately.

You can configure the following items:

- *Wireless Network*
- *Access Control*
- *Portal Authentication*
- *Free Authentication Policy*
- *MAC Filter*
- *Scheduler*
- *System*

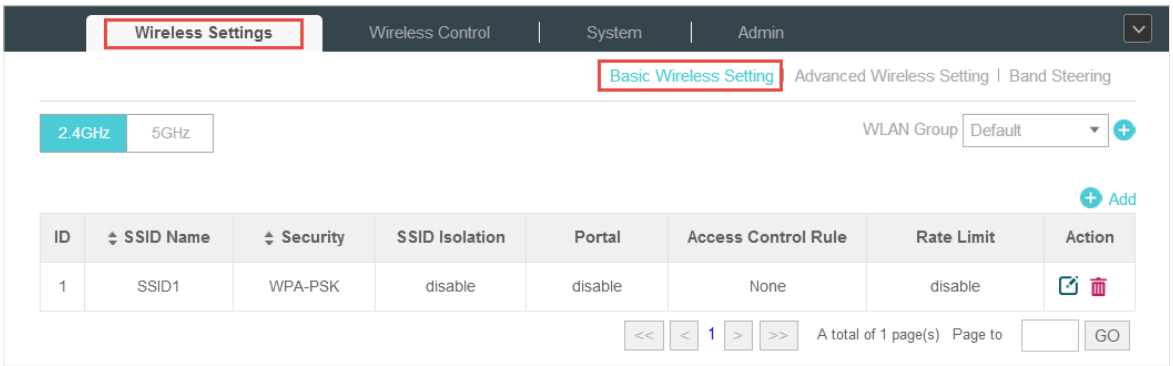
3.1 Wireless Network

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

Add Wireless Networks

To add wireless networks, follow the steps below.

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



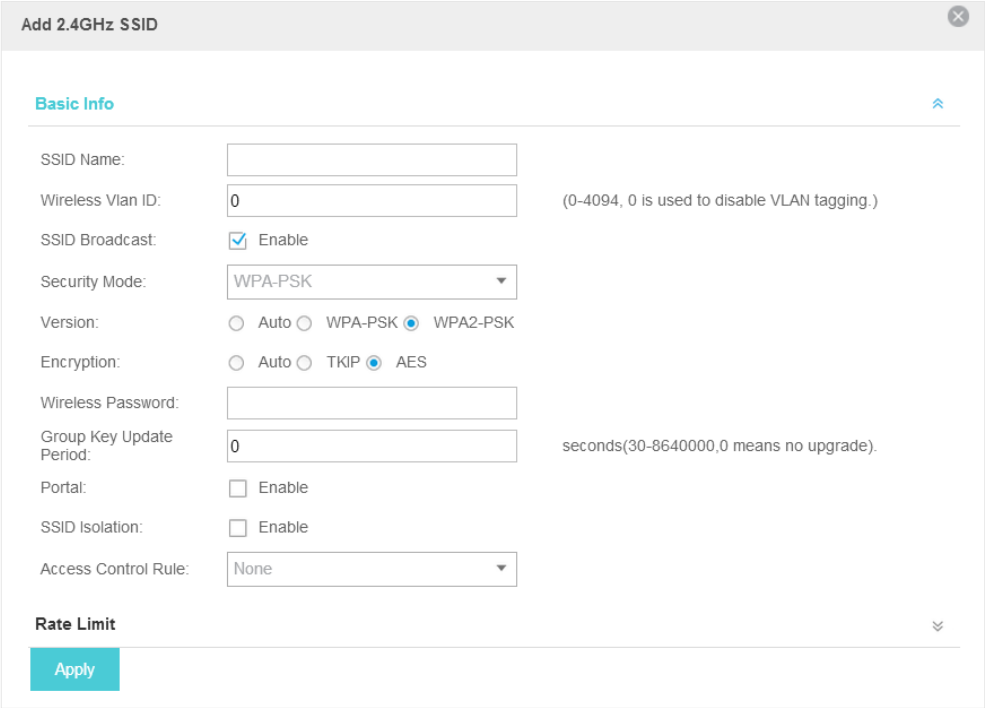
2. Select a band frequency 2.4GHz 5GHz and click + at the right of WLAN Group Default to add a WLAN group. If you have no need to group your wireless networks, you can use the default WLAN group and skip this step.

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

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

5. Click + Add to add a SSID to the specific WLAN group.

6. Configure the parameters in the following window.



SSID Name	Enter a 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.
Portal	With the option enabled, the configurations in Portal will be applied. Portal provides authentication service for the clients who just need temporary access to the wireless network, such as the customers in shopping mall and restaurant. Disabled by default.
SSID Isolation	With the option enabled, the devices connected in the same SSID 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.

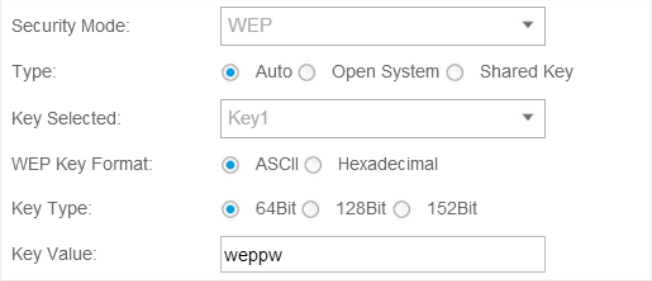
Following is the detailed introduction of **WEP, WPA-Enterprise** and **WPA-PSK**.

- ## 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.

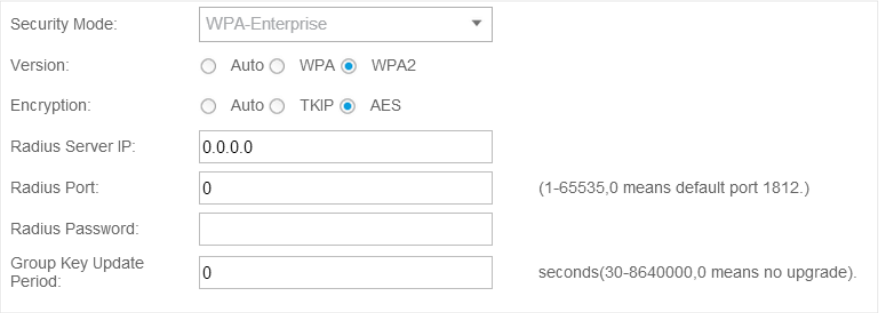


Type	Select the authentication type for WEP. **Auto**: The EAP Controller can select Open System or Shared Key automatically based on the wireless station's capability and request. **Open System**: Clients can pass the authentication and associate with the wireless network without password. However,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

- ## WPA-Enterprise

The WPA-Enterprise mode requires a RADIUS server to authenticate clients. Since the WPA-Enterprise can generate different passwords for different clients, it is much safer than WPA-PSK.

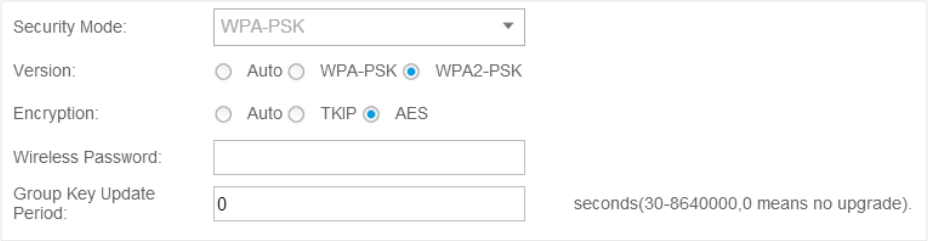
However, it costs much more to maintain and is usually used by enterprise.



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

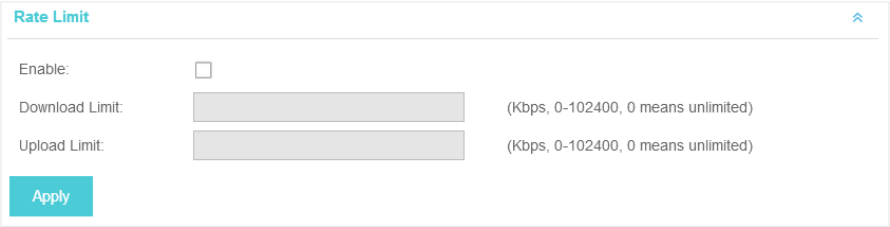
- **WPA-PSK**

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



Version	Select the version of WPA-Enterprise. **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.



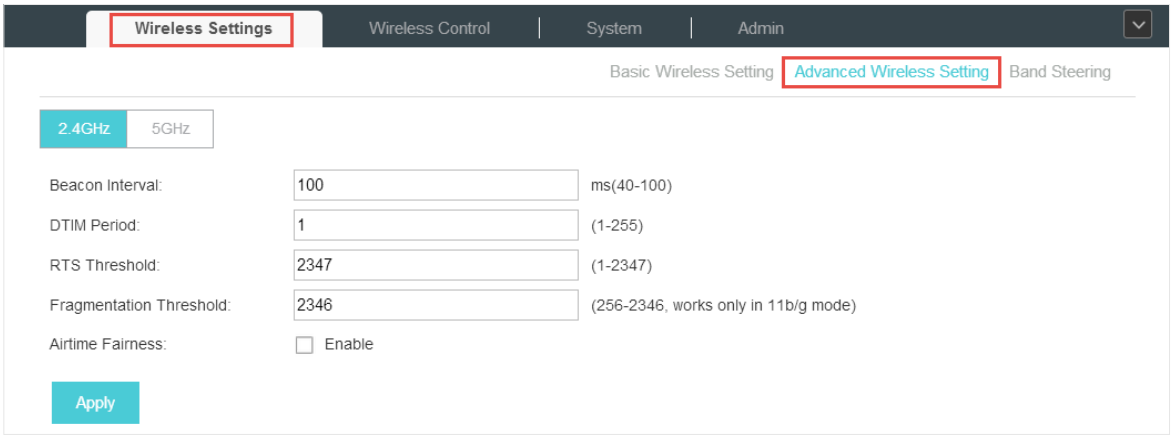
8. Click **Apply** to add the new SSID.

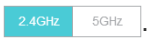
Configure Advanced Wireless Parameters

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**.



2. Select the band frequency 

.

3. Configure the following parameters.

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

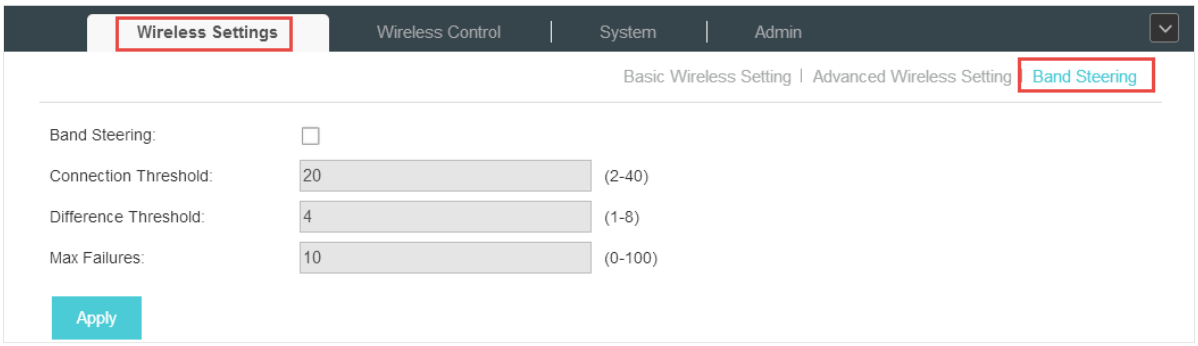
4. Click **Apply** to save the configurations.

Configure Band Steering

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

To configure Band Steering, follow the steps below.

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



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

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

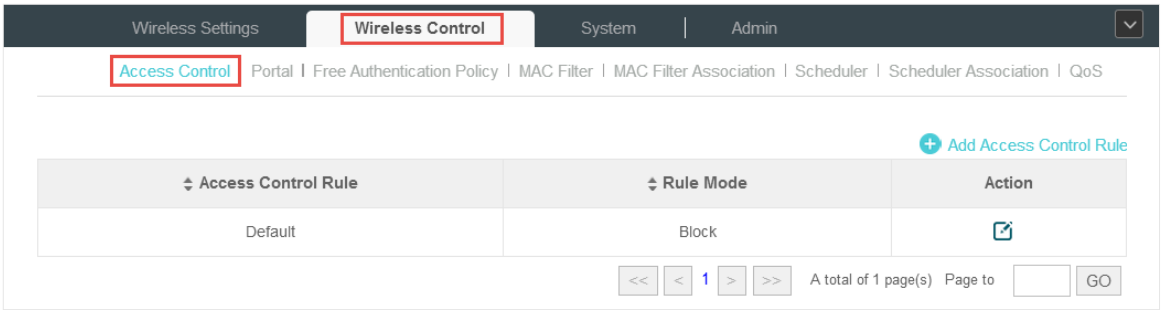
Connection Threshold/Difference Threshold	When the number of clients on the 5GHz band reaches the value of **Connection Threshold** and the difference value between the number of clients on the 2.4GHz band and the 5GHz band reaches the value of **Difference Threshold**, EAPs will refuse the requests of communication on the 5GHz band from other clients and no longer steer other clients to the 5GHz band. The value of **Connection Threshold** is from 2 to 40, and the default is 20. The value of **Difference Threshold** is from 1 to 8, and the default is 4.
Max Failures	If a client repeatedly attempts to associate with the EAP on the 5GHz band and the number of rejections reaches the value of **Max Failures**, the EAP will accept the request. The value is from 0 to 100, and the default is 10.

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

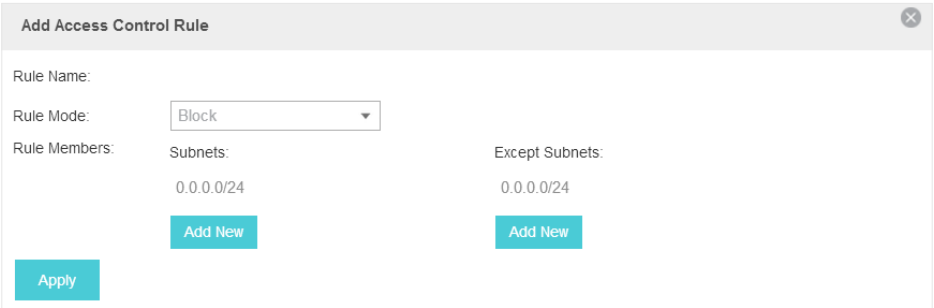
3.2 Access Control

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 the rule members to access the network. **Allow**: Select this mode to allow the rule members to access the network.
Rule Memebers	**Subnets**: Clients of the subnet will be controlled by the rule. Enter the subnet for this rule in the format X.X.X.X/X and click Add New . Up to 16 subnets can be added. **Except Subnets**: Clients of the subnet will be controlled by the rule. Enter the subnet that does not follow this rule in the format X.X.X.X/X and click Add New . Up to 16 subnets can be added. The rule will not apply to the subnets that is in both the Subnets list and the Except Subnets list.

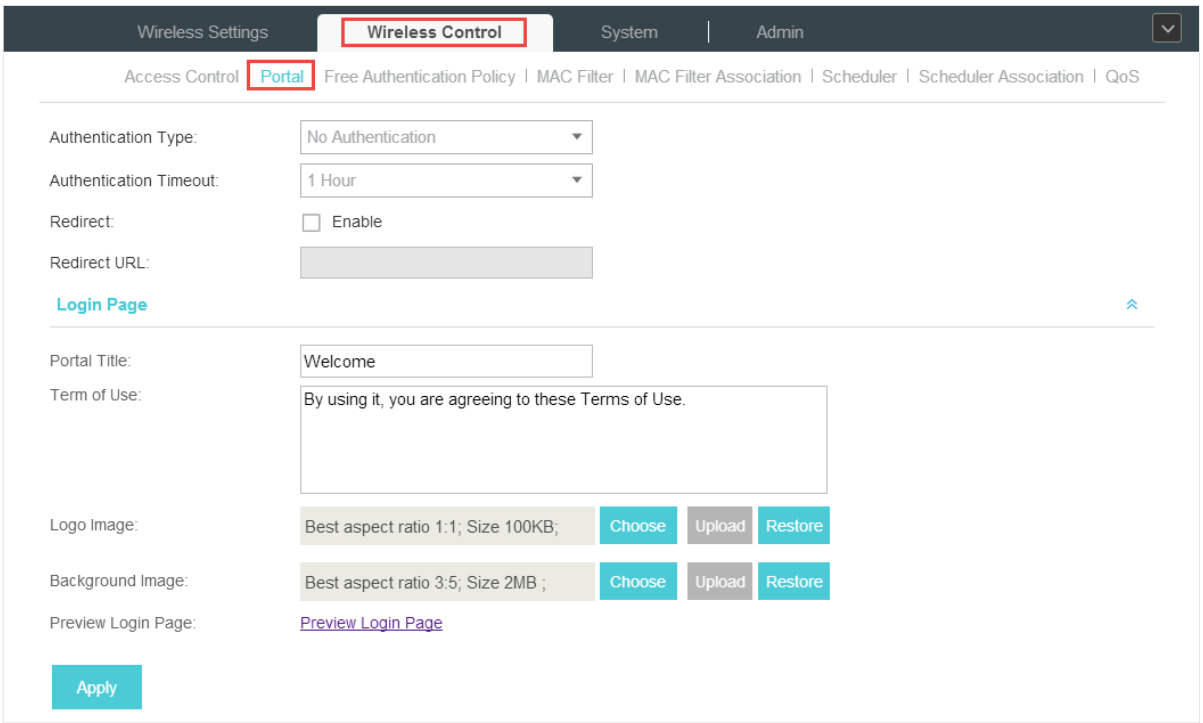
4. Click **Apply** to save the configurations.

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.

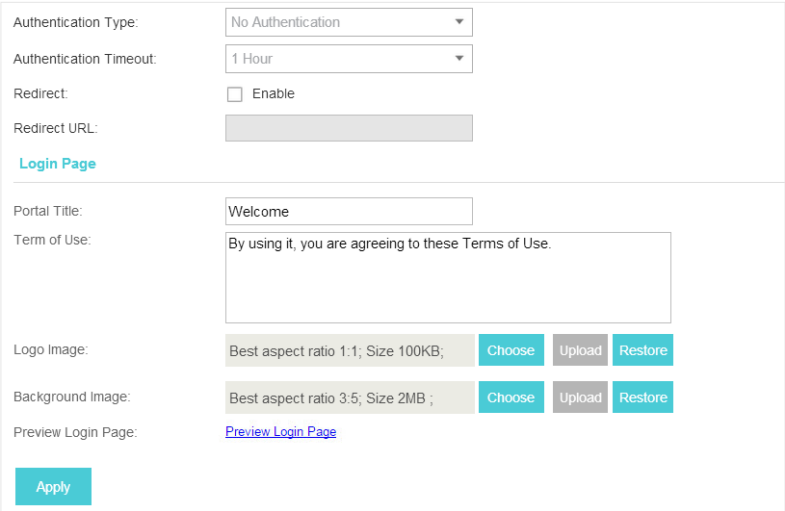
To configure Portal Authentication, go to **Wireless Control > Portal.**



Five different types of authentication methods are available: No Authentication, Simple Password, Hotspot, External Radius Server, and External Portal Server. Please refer to the following instructions to configure Portal.

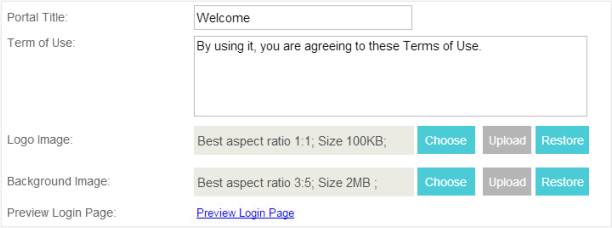
No Authentication

When this option is selected, clients can access the network without any authentication and just need to accept the term of use.



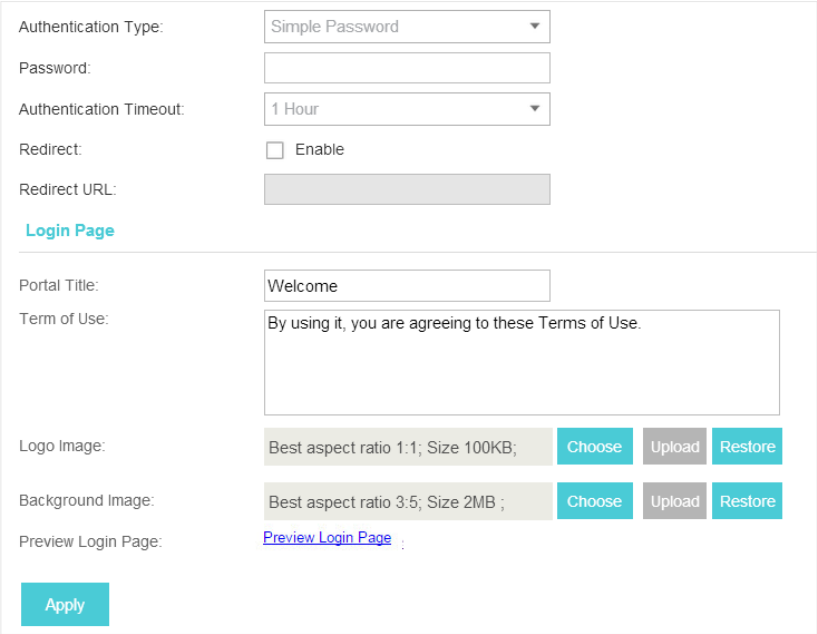
Configure the following parameters and provide the required information.

Authentication Type	Select **No Authentication**.

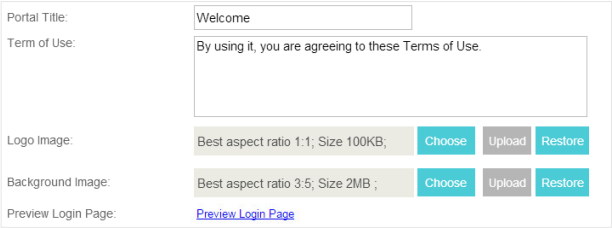
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in the web authentication page again to access the network. Options include **1 Hour, 8 Hours, 24 Hours, 7 Days, Custom**. **Custom** allows you to define the time in days, hours, and minutes. The default value is one hour.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL. Disabled by default.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.
Login Page	Customize the login page:  1. Configure the title and terms of the login page in the **Portal Title** and **Term of Use** boxes. 2. Upload a logo image and a background image from your local PC. 3. Preview the login page.

Simple Password

When this option is selected, clients are required to enter the password and accept the term of use.

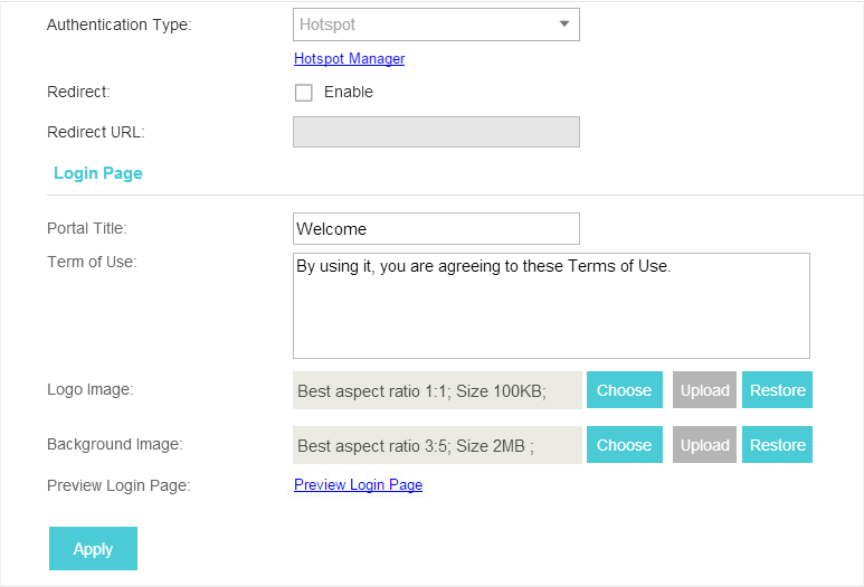


Configure the following parameters and provide the required information.

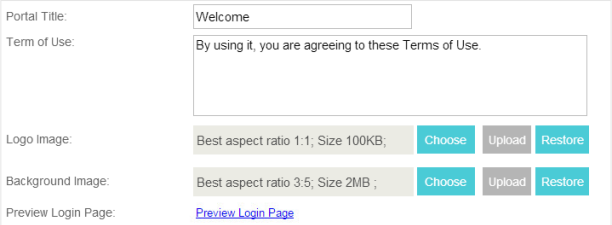
Authentication Type	Select **Simple Password**.
Password	Specify the password for the authentication.
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in the web authentication page again to access the network. Options include **1 Hour, 8 Hours, 24 Hours, 7 Days, Custom**. **Custom** allows you to define the time in days, hours, and minutes. The default value is one hour.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL. Disabled by default.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.
Login Page	Customize the login page:  1. Configure the title and terms of the login page in the **Portal Title** and **Term of Use** boxes. 2. Upload a logo image and a background image from your local PC. 3. Preview the login page.

Hotspot

With this option selected, distribute the vouchers automatically generated by the EAP Controller to the clients, who can use the vouchers to access the network. In addition, the clients that access the network by hotspot authentication type can be managed by the hotspot manager.



Configure the following parameters and provide the required information.

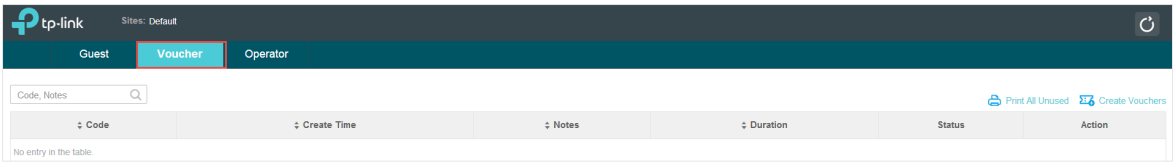
Authentication Type	Select **Hotspot**.
Hotspot Manager	Click **Hotspot Manager** to create vouchers and manage the hotspot authentication. For detailed instructions, please refer to the content below.
Redirect	Disabled by default. If you enable this function, the portal will redirect the newly authenticated 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.
Login Page	Customize the login page:  1. Configure the title and terms of the login page in the **Portal Title** and **Term of Use** boxes. 2. Upload a logo image and a background image from your local PC. 3. Preview the login page.

After you click **Hotspot Manager**, a new window will open automatically. On the page, you can create and print Vouchers, manage the guests and create the Operator account to help manage your network.

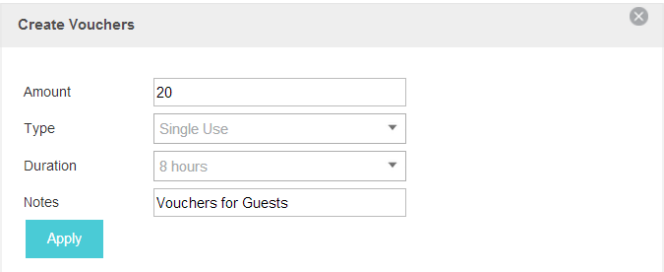
- ## Create and Print Vouchers

Please follow these steps to create and print vouchers.

1. Go to the **Voucher** page.



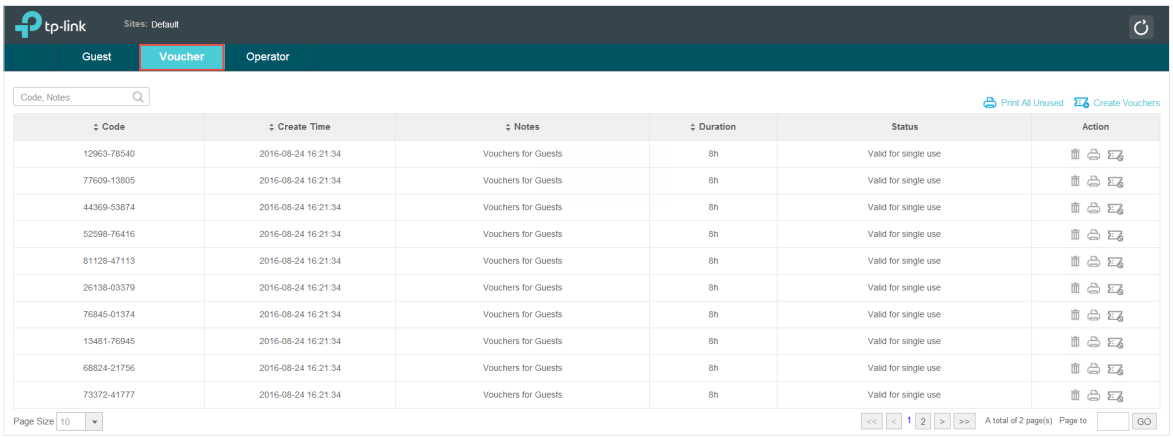
2. Click Create Vouchers and the following window will pop up.



3. Configure the parameters as follows:

Amount	Enter the voucher amount to be generated.
Type	Select **Single Use** or **Multi Use**. Single Use means one voucher can only be distributed to one client. Multi Use means one voucher can be distributed to several clients, who can use the same voucher to access the network at the same time. If you select Multi Use, enter the value of **Max Users**. When the number of clients who are connected to the network with the same voucher reaches the value, no more clients can use this voucher to access the network.
Duration	Select the period of validity of the Voucher. The options include **8 hours**, **2 days** and **User-defined**. The period of valid of the voucher is reckoned from the time when it is used for the first time.
Notes	Enter a description for the Voucher (optional).

4. Click **Apply**. The Vouchers will be generated and displayed on the page.



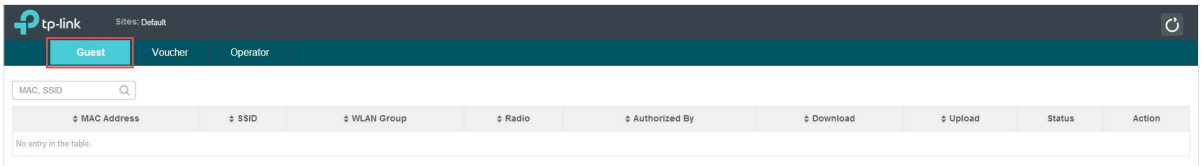
5. Click or Print All Unused to print and save the Vouchers.

6. Distribute the Vouchers to clients, and then they can use the **Code** to pass authentication for network access.

7. When the Vouchers are invalid, you can click to delete the Voucher or to delete all of them.

- ## Manage the Guests

Guest page allows you to 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 Account

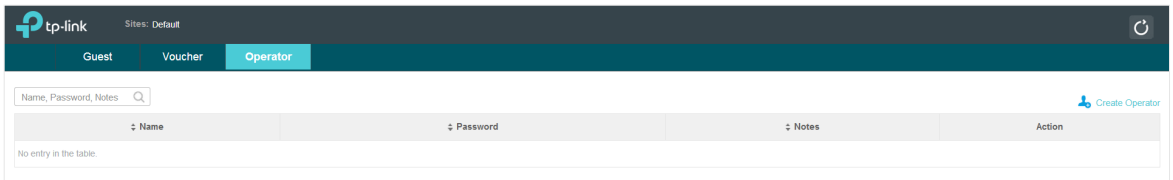
Operator account can be used to remotely manage the hotspot. Other users can visit the URL **https://EAP Controller Host's IP Address:8043/hotspot** (For example: https://192.168.0.64:8043/hotspot) and use the Operator account to enter the Hotspot administrative system.

☞ Note

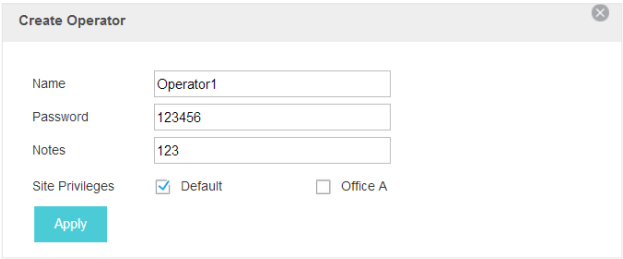
The users who enter the hotspot administrative system by Operator account can only generate vouchers and manage the clients.

Follow the steps below to create Operator account.

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



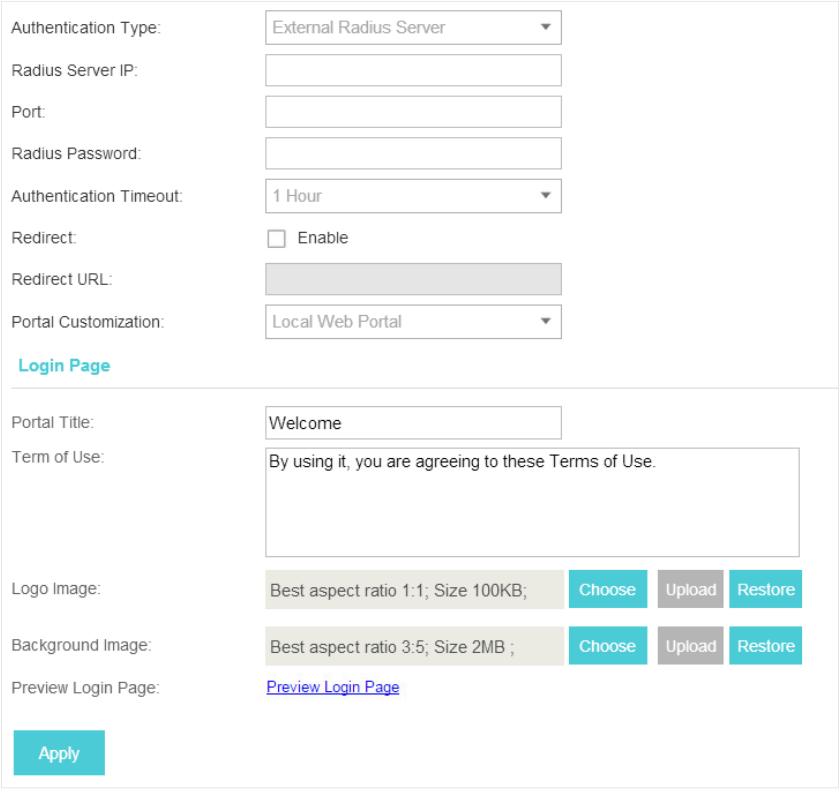
2. Click Create Operator and the following window will pop up.



3. Specify the **Name**, **Password** and **Notes** of the Operator account.
4. Choose **Site Privileges** (You can choose more than one options) 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.

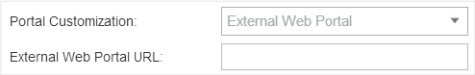
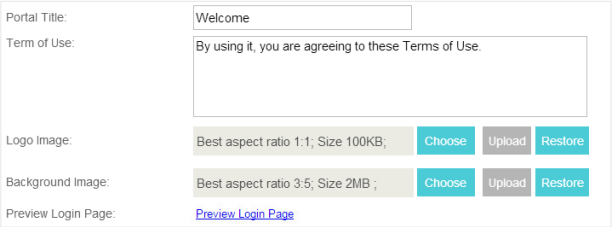
External Radius Server

If you have a Radius Server, select External Radius Server. 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.



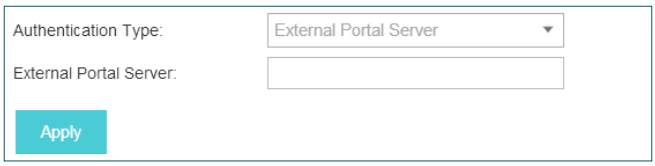
Configure the parameters and provide the required information as follows:

Authentication Type	Select **External Radius Server**.
Radius Server IP	Enter the IP address of Radius Server.
Port	Enter the port the Radius Server used.
Radius Password	Enter the password you have set on the Radius Server. Clients will be required to enter the password when they attempt to access the network.
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in the web authentication page again to access the network. Options include: 1 Hour, 8 Hours, 24 Hours, 7 Days, Custom. Custom allows you to define the time in days, hours, and minutes. The default is one hour.
Redirect	Disabled by default. 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.

Portal Customzation	Select Local Web Portal or External Web Portal. **Local Web Portal**: If this option is selected, configure the Login Page. **External Web Portal**: If this option is selected, follow the steps below. 1. Configure the external radius server. 2. Enter the authentication login page's URL provided by the external portal server on the page.  3. Put the external web portal server to a whitelist of Free Authentication Policy, otherwise clients cannot access it before authenticated.
Login Page	If you select Local Web Portal, customize the login page:  1. Configure the title and terms of the login page in the **Portal Title** and **Term of Use** boxes. 2. Upload a logo image and a background image from your local PC. 3. Preview the login page.

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 EAP Controller, e.g. message authentication and WeChat authentication etc.

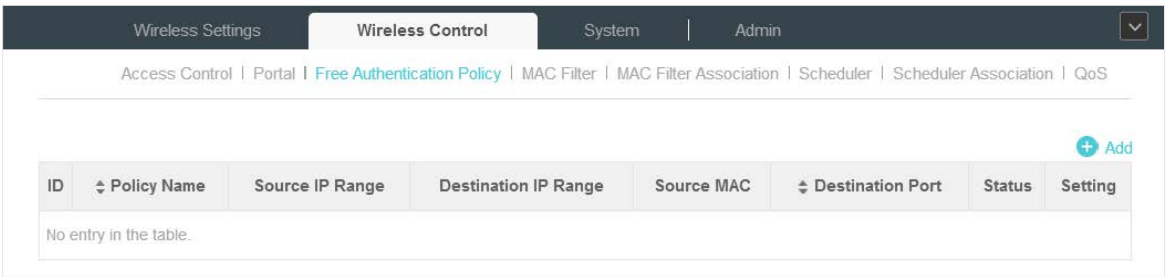


Authentication Type	Select **External Portal Server**.
Radius Server IP	Enter the complete authentication URL that redirect to an external portal server, for example: http://192.168.0.147:8880/portal/index.php or http://192.168.0.147/portal/index.html

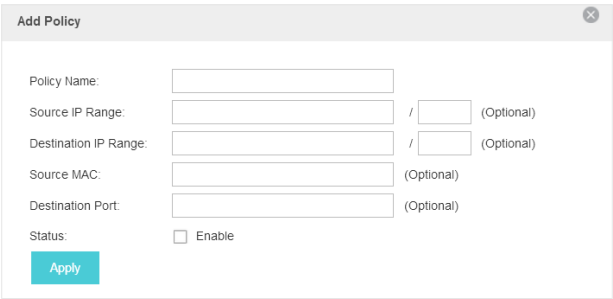
3.4 Free Authentication Policy

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.



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

Policy Name	Specify a name for the policy.
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 cilent.
Destination Port	Enter the port the service uses.
Status	Check the box to enable the policy.

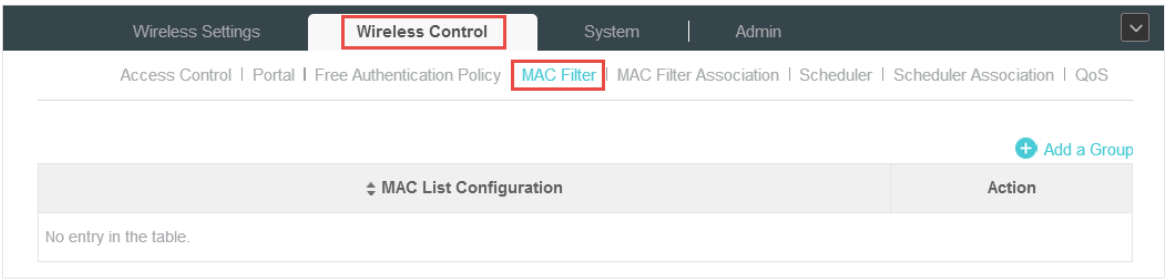
4. Click **Apply** and the policy is successfully added.

3.5 MAC Filter

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

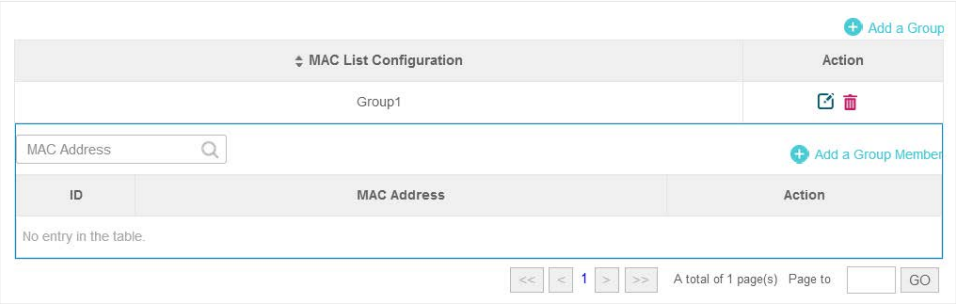
Follow the steps below to configure MAC Filter.

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



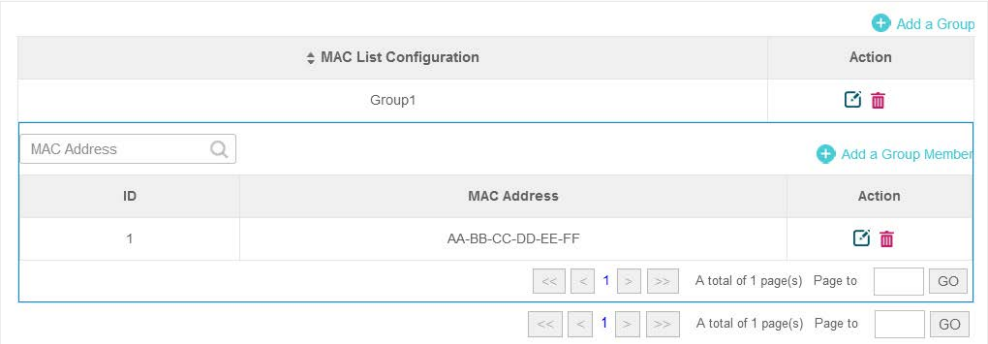
1) Click Add a Group and specify a name for the group.

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



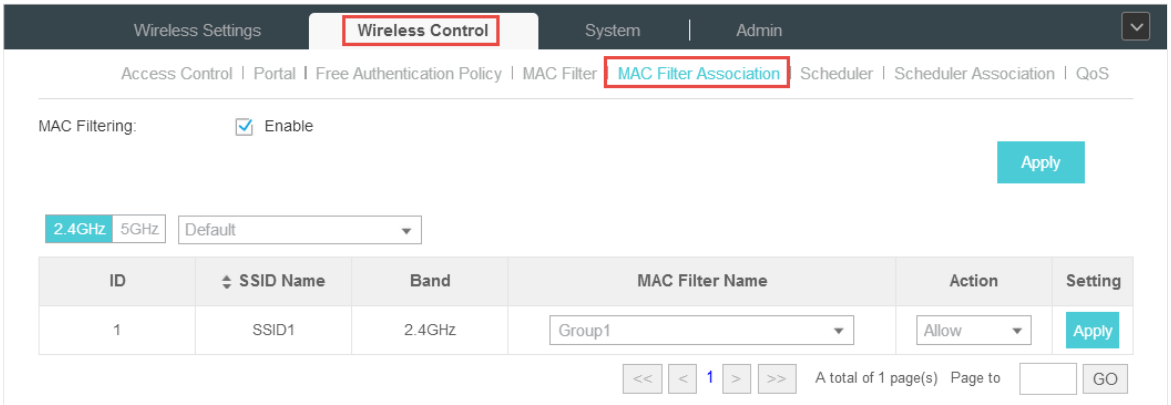
3) Click Add a Group Member and enter a MAC address in the format as shown below.

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.

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.

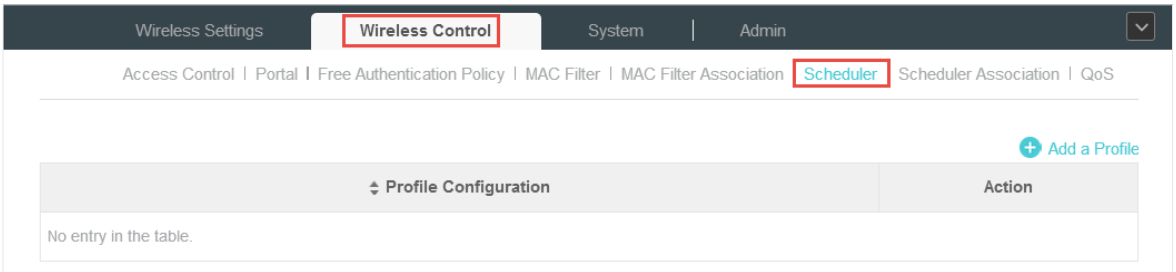
4) Click **Apply** in the Setting column to save the configurations.

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.

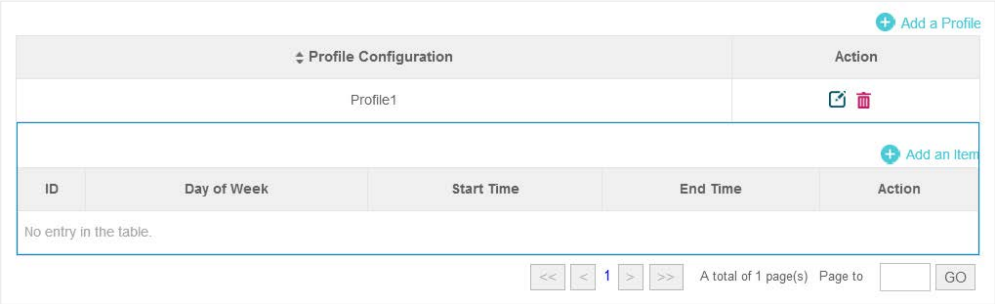
Follow the steps below to configure Scheduler.

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

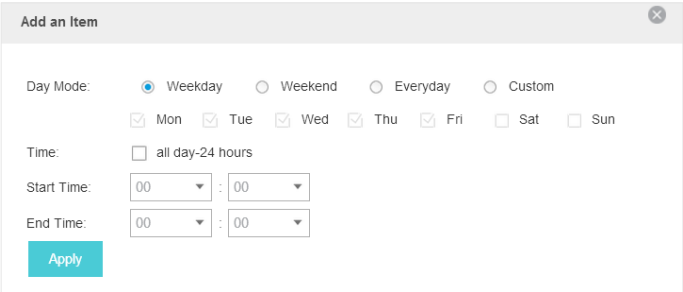


1) Click Add a Profile and specify a name for the profile.

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

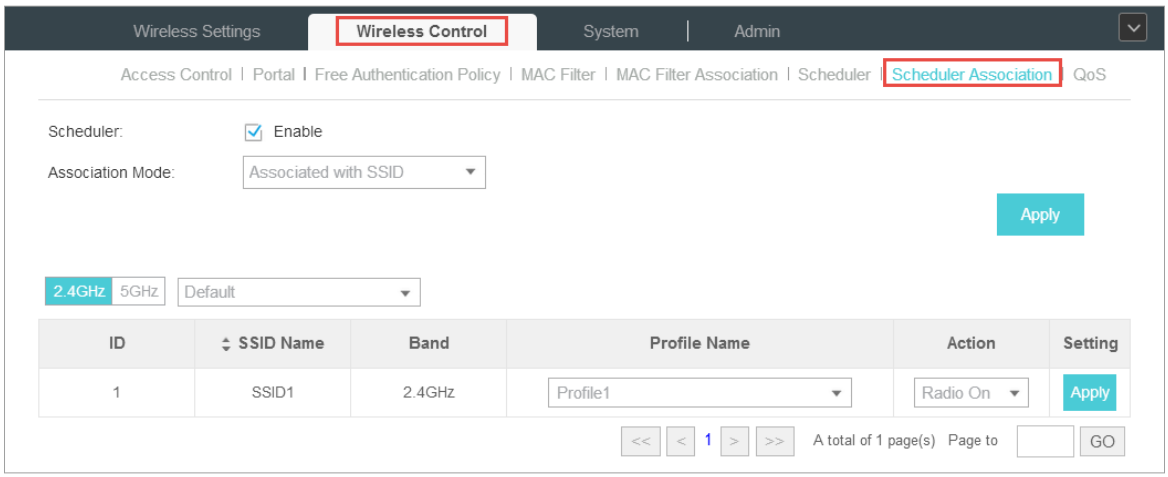


3) Click Add an Item and configure the parameters to specify a period of time.



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

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



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 to save the configurations.

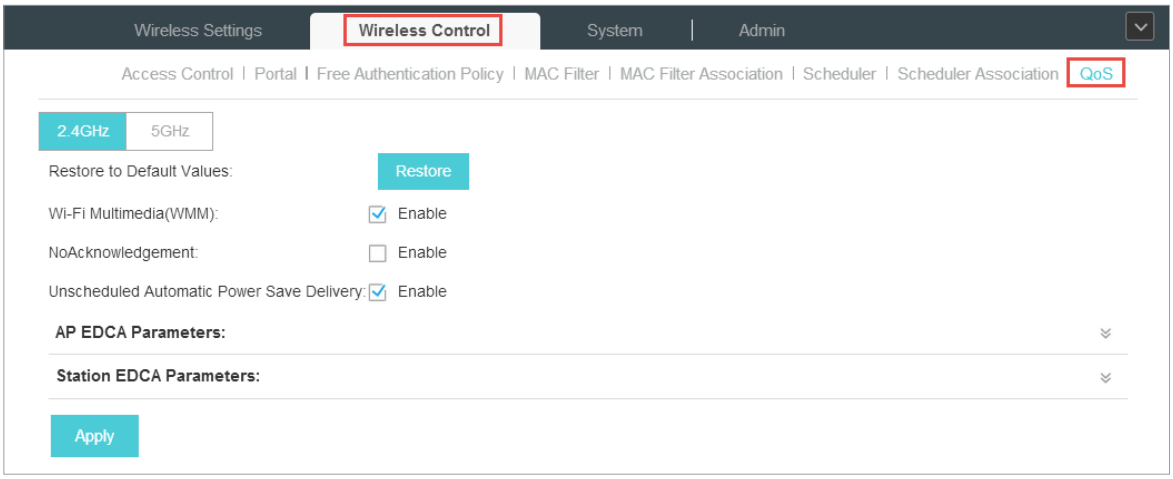
3.7 QoS

The EAP 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.

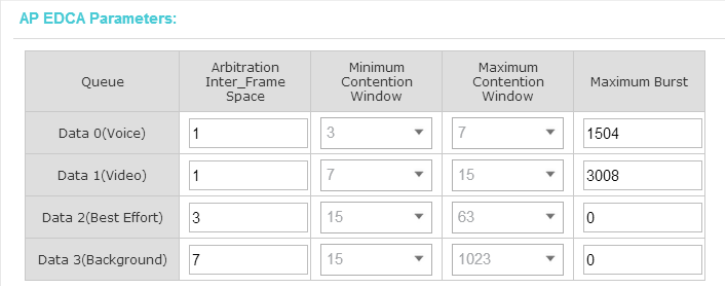
1. Go to **Wireless Control > QoS**.



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).
NoAcknowledgement	By default disabled. You can enable this function to specify that the EAP devices should not acknowledge frames with QosNoAck. NoAcknowledgement is recommended if VoIP phones access the network through the EAP device.
Unscheduled Automatic Power Save Delivery	By default enabled. As a power management method, it can greatly improve the energy-saving capacity of clients.

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



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

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

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

Station EDCA Parameters:

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

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

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

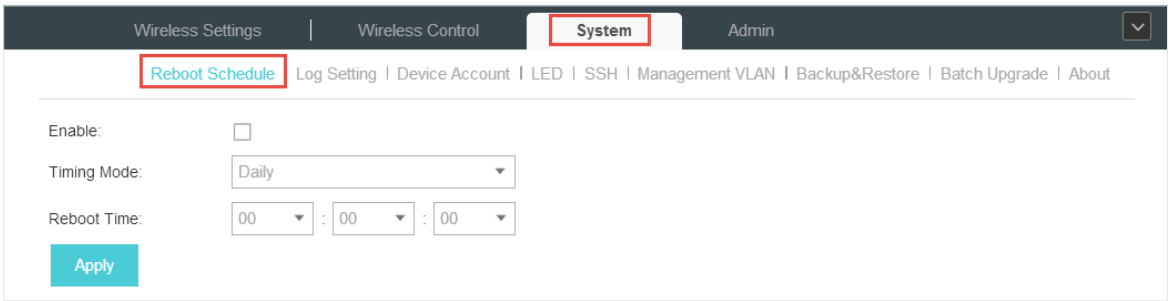
5. Click **Apply** to save the configurations.

3.8 System

Reboot Schedule

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

1. Go to **System > Reboot Schedule.**

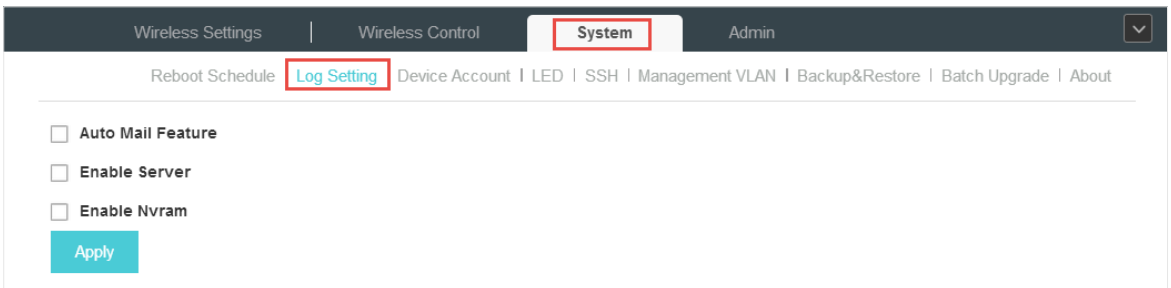


2. Check the box to enable the function.
3. Choose **Daily**, **Weekly** or **Monthly** in the **Timing Mode** drop-down list and set a specific time to reboot the EAPs.
4. Click **Apply** to save the configurations.

Log Setting

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

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

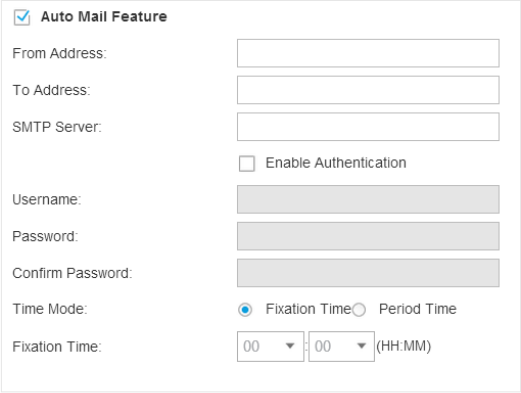


2. Check the box to choose the way to receive system logs (you can choose more than one) and

click **Apply** to save the configurations. Three ways are available: **Auto Mail Feature, Server and Nvram.**

- ## Auto Mail Feature

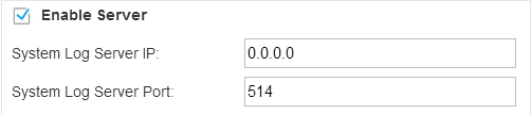
If Auto Mail Feature is enabled, system logs will be sent to a specified mailbox. Check the box to enable the feature and configure the parameters.



From Address	Enter the sender's E-mail address.
To Address	Enter the receiver's E-mail address.
SMTP Server	Enter the IP address of the SMTP server.
Enable Authentication	You can check the box to enable mail server authentication. Enter the sender's mail account name and password.
Time Mode	Select Time Mode. System logs can be sent at specific time or time interval.
Fixation Time	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.

- ## 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.



- **Nvram**

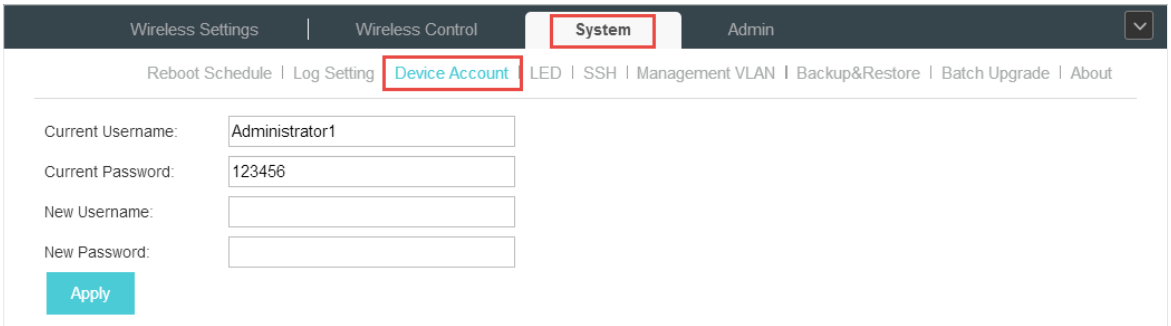
  Nvram (Non-volatile Random Access Memory) is a RAM that can still save data even if a device is power off. All TP-LINK EAPs are equipped with Nvram. With this option enabled, the Nvram feature can help reserve the system logs when an EAP device is power off.

Device Account

When the EAP devices are adopted at the first time, their username and password will become the same as those of the EAP 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.**



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

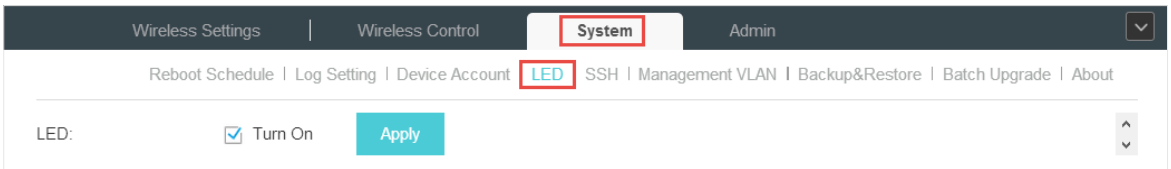
3. Click **Apply** to save the configurations.

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

LED

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

1. Go to **System > LED**.



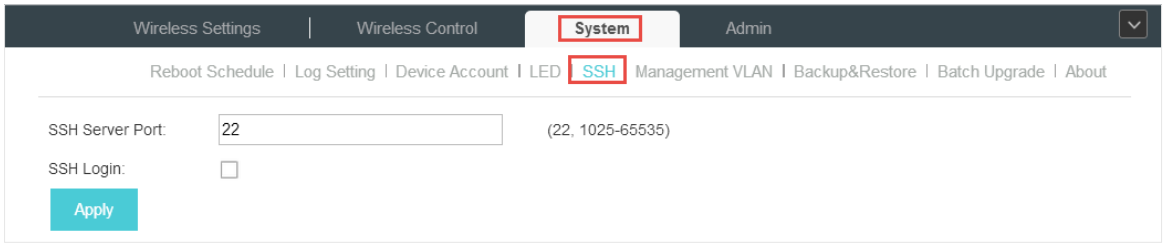
2. By default, the LED lights are on. You can check the box to change the light status.

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

SSH

You can login to the EAP Controller via SSH. Deploy an SSH server on your network and follow the steps below to configure SSH on the EAP Controller:

1. Go to **System > SSH.**



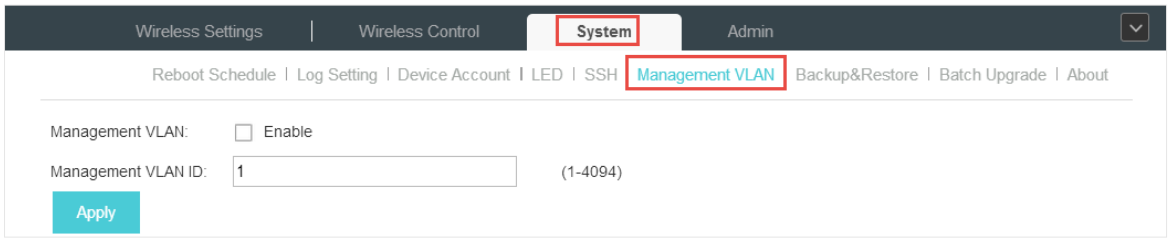
2. Enter the port number of the SSH server.
3. Check the box to enable SSH Login.
4. Click **Apply**.

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. Go to **System > Management VLAN.**



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

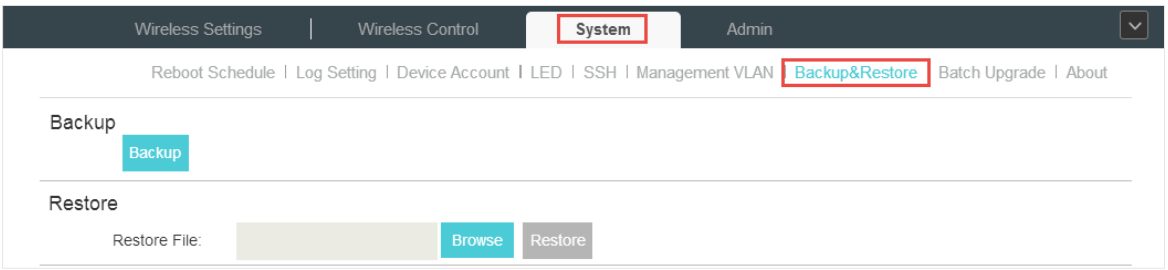
Backup&Restore

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.**



2. Click **Backup** and save the backup file.

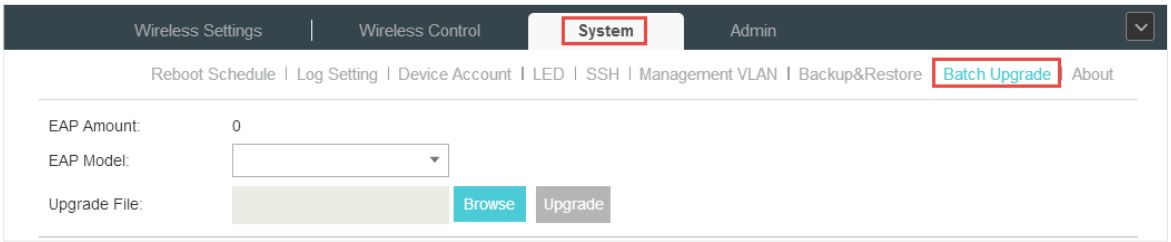
3. If necessary, click **Browse** to locate and choose the backup file. Then click **Restore** to restore the configuration.

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**.



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.

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.

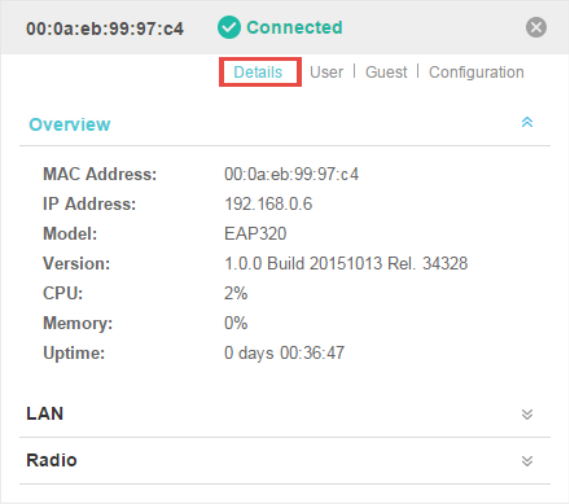
This chapter includes the following contents:

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

4.1 View the Information of the EAP

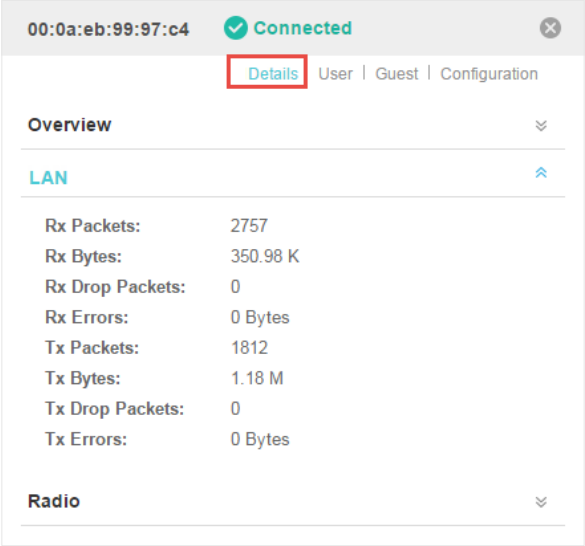
Overview

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).



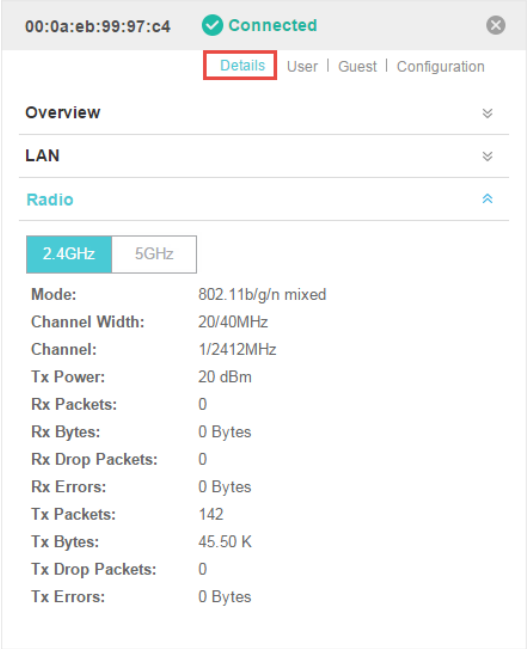
LAN

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.



Radio

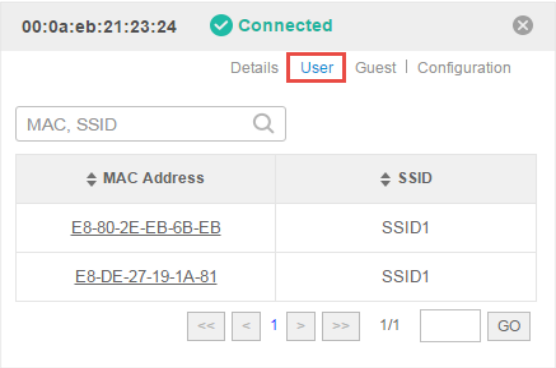
Click **Radio** to view the radio information including the frequency band, the wireless mode, the channel width, the channel, and the transmitting power. At 2.4GHz, you can also view parameters of receiving/transmitting data.



4.2 View Clients Connecting to the EAP

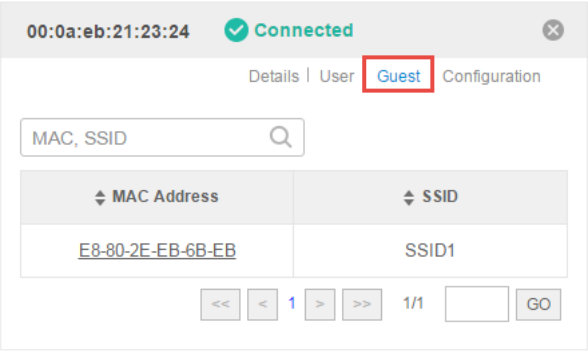
User

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.



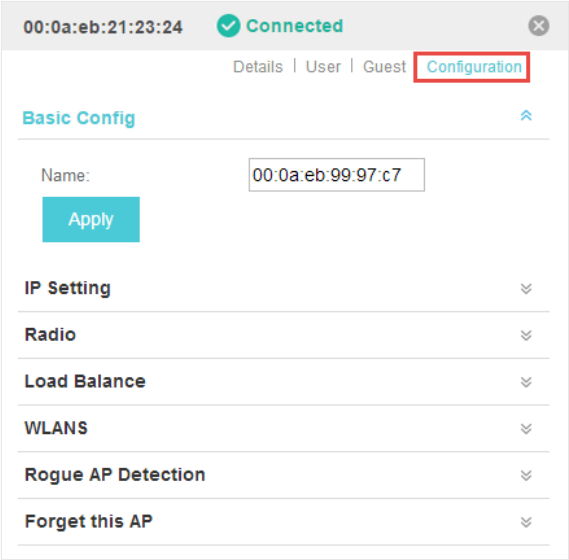
Guest

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.



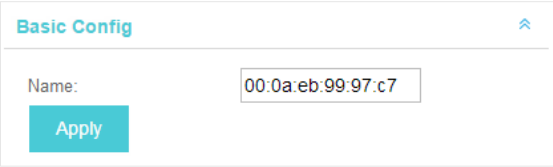
4.3 Configure the EAP

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



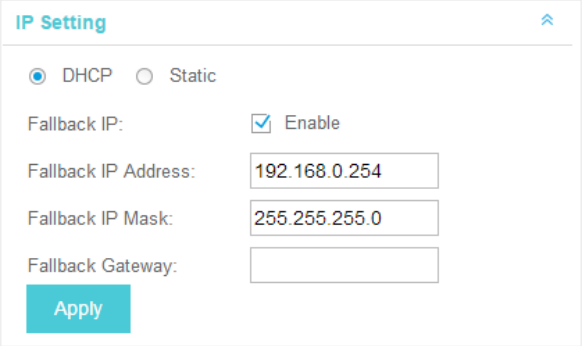
Basic Config

Here you can change the name of the EAP.



IP Setting

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



- **Get a Dynamic IP Address From the DHCP Server**

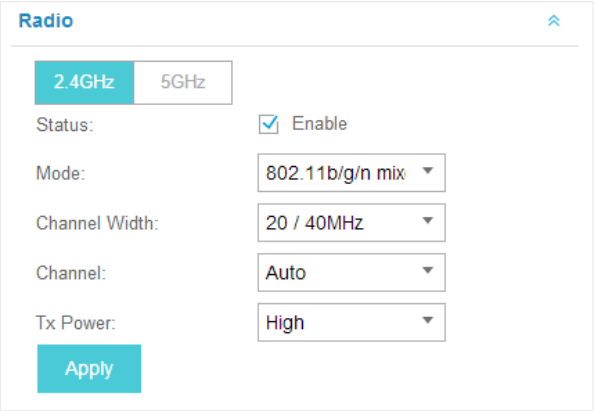
  1. Configure your DHCP server.
  2. Select **DHCP** on the page above.
  3. Enable the Fallback IP feature. When the device cannot get a dynamic IP address, the fallback IP address will be used.
  4. Set IP address, IP mask and gateway for the fallback address and click **Apply**.

- **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**.

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.

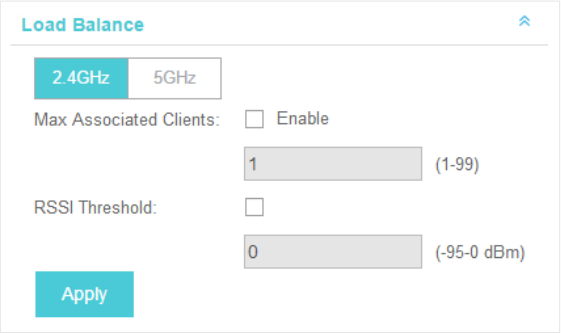


Select the frequency band (2.4GHz/5GHz) and configure the following parameters.

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 onl7, 802.11a only, and 802.11n only modes are available: **802.11n/ac mixed**: Both 802.11n clients and 802.11ac clients operating in the 5GHz frequency can connect to the EAP device. **802.11a/n mixed**: Both 802.11a clients and 802.11n clients operating in the 5GHz frequency can connect to the EAP device. **802.11ac only**: Only 802.11ac clients can connect to the EAP device. **802.11a only**: Only 802.11a clients can connect to the EAP device. **802.11n only**: Only 802.11n clients can connect to the EAP device.
Channel Width	Select the channel width of the EAP device. For EAP 110/120/220, the options includes **20MHz**, **40MHz** and **20/40MHz**. For EAP 320/330, the options includes **20MHz**, **40MHz**, **80MHz** and **20/40/80MHz**. The 20/40 MHz and 20/40/80MHz channels enable higher data rates but leave fewer channels available for use by other 2.4GHz and 5GHz devices. When the radio mode includes 802.11n, we recommend you set the channel bandwidth to 20/40 MHz or 20/40/80MHz to improve the transmission speed.
Channel	Select the channel used by the EAP device to improve wireless performance. The range of available channels is determined by the radio mode and the country setting. If you select Auto for the channel setting, the EAP device scans available channels and selects a channel where the least amount of traffic is detected.
Tx Power	Select the TX Power (transmit power) in the 4 options: **Low, Medium, High** and **Custom**. Low, Medium and High are based on the Max TxPower (maximum transmit power. It may vary among different countries and regions). **Low**: Max TxPower * 20% (round off the value) **Medium**: Max TxPower * 60% (round off the value) **High**: Max TxPower **Custom**: Enter a value manually.

Load Balance

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

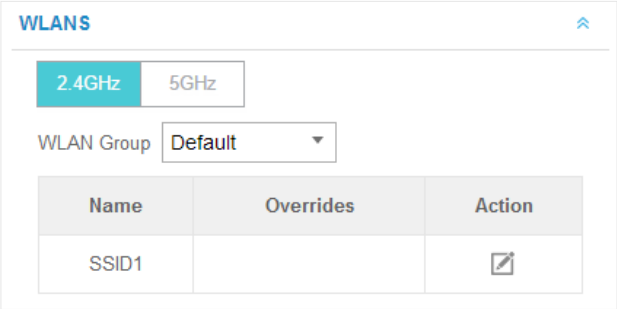


Select the frequency band (2.4GHz/5GHz) and configure the parameters.

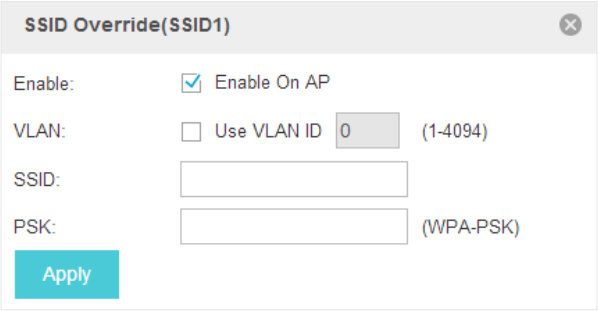
Max Associated Clients	Enable this function and specify the maximum number of connected clients. While more clients requesting to connect, the EAP will disconnect those with weaker signals.
RSSI Threshold	Enable this function and enter the threshold of **RSSI** (Received Signal Strength Indication). When the clients' signal is weaker than the **RSSI Threshold** you've set, the clients will be disconnected from the EAP.

WLANs

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



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

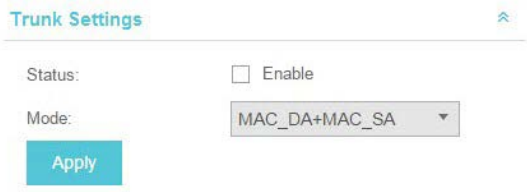


3. Check the box to enable the feature.
4. You can join the overridden SSID in to a VLAN. Check the **Use VLAN ID** box and specify a VLAN ID.
5. Specify a new name and password for the SSID.
6. Click **Apply** to save the configuration.

Trunk Settings

Only EAP330 supports this function.

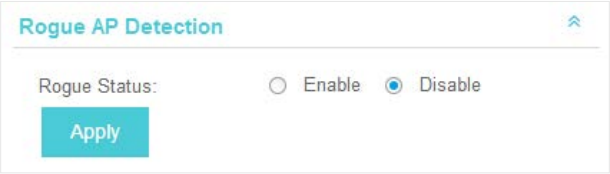
The trunk function can bundles multiple Ethernet links into a logical link to increase bandwidth and improve network reliability.



Status	Enable this function. The EAP330 has two 1000Mbps Ethernet ports. If the Trunk function is enabled and the ports are in the speed of 1000Mbps Full Duplex, the whole bandwidth of the trunk link is up to 4Gbps (2000Mbps * 2).
Mode	Select the applied mode of Trunk Arithmetic. • 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.

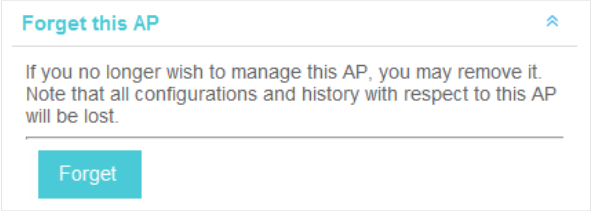
Rouge AP Detection

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



Forget this AP

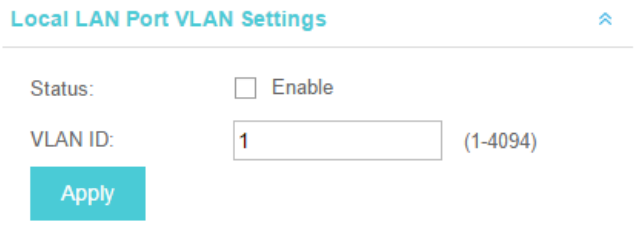
If you no longer want to manage this EAP, you may remove it. All the configurations and history about this EAP will be deleted. It is recommended to back up the configurations of this EAP before you forget it.



Local LAN Port VLAN Settings

Only EAP115-Wall supports this function.

This feature is used add the EAP to a specific VLAN. With this feature enabled, the hosts connected to this EAP can only communicate with the devices in the same VLAN.



Status	Enable this function.
Mode	Specify the VLAN that the EAP is added to. The valid values are from 1 to 4094, and the default is 1.

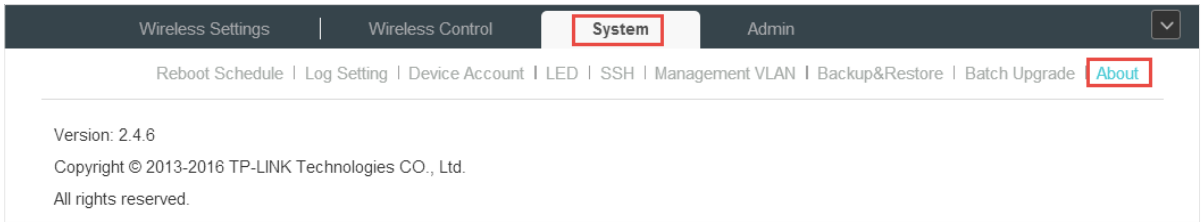
5 Manage the EAP Controller

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 EAP Controller's version and copyright information on the **About** page.



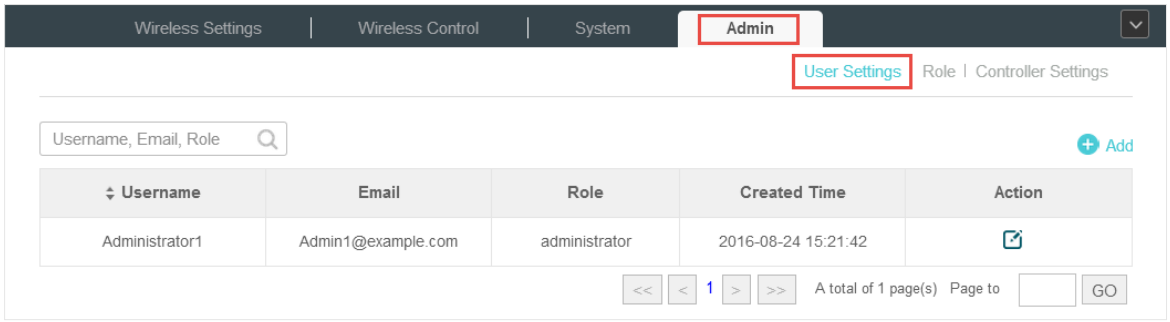
5.2 User Account

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

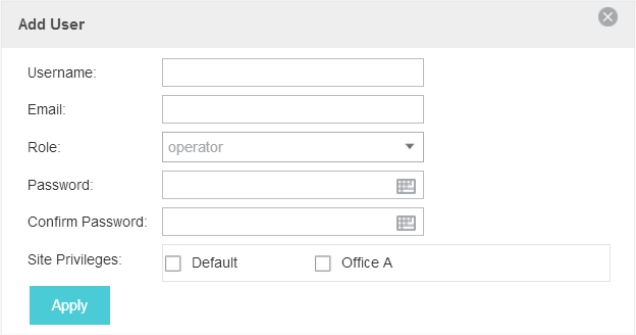
Administrator	The first administrator account is created in the Basic Configuration process and this account can not be deleted. An administrator can change the settings of the EAP network and create and delete user accounts.
Operator	An operator account can be created or deleted by the administrator.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

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.

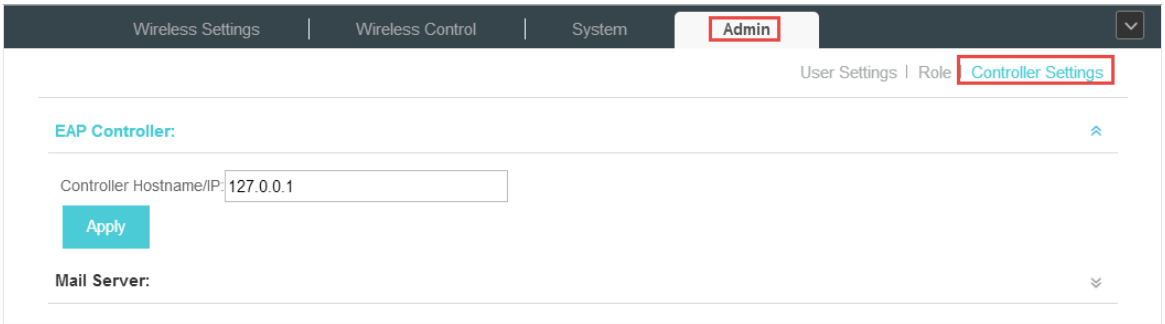
5.3 Controller Settings

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

Configure Controller Hostname/IP

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

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



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

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

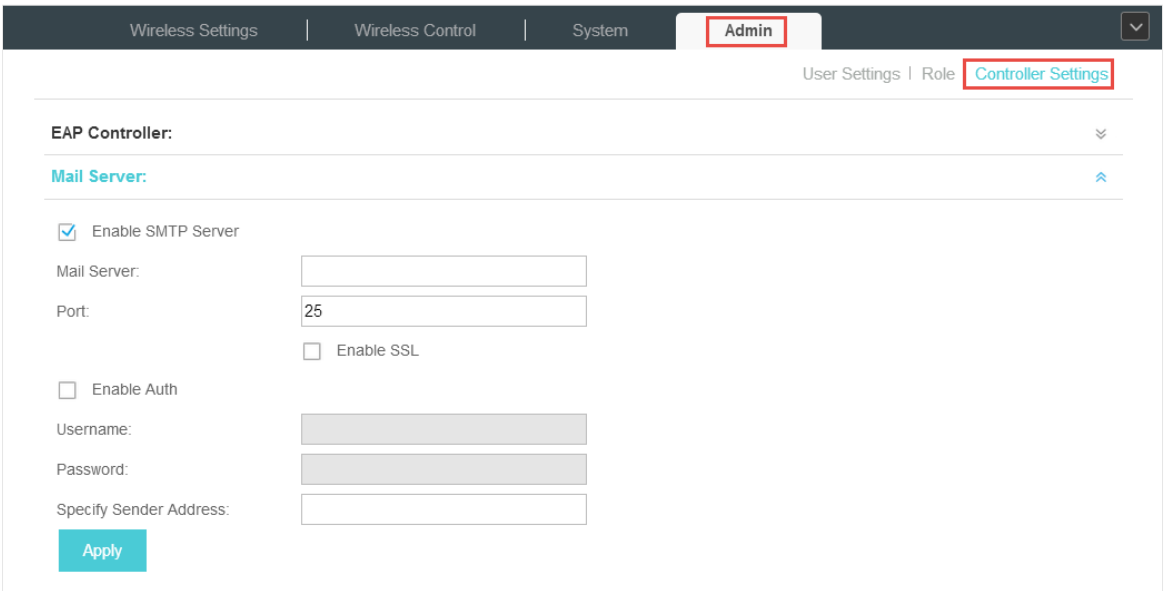
Configure Mail Server

With the Mail Server, you can reset the password of the user account and receive notifications from the EAP Controller. It is different from the SMTP Server, which is just for the syslog 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 EAP Controller. The network administrator wants to :

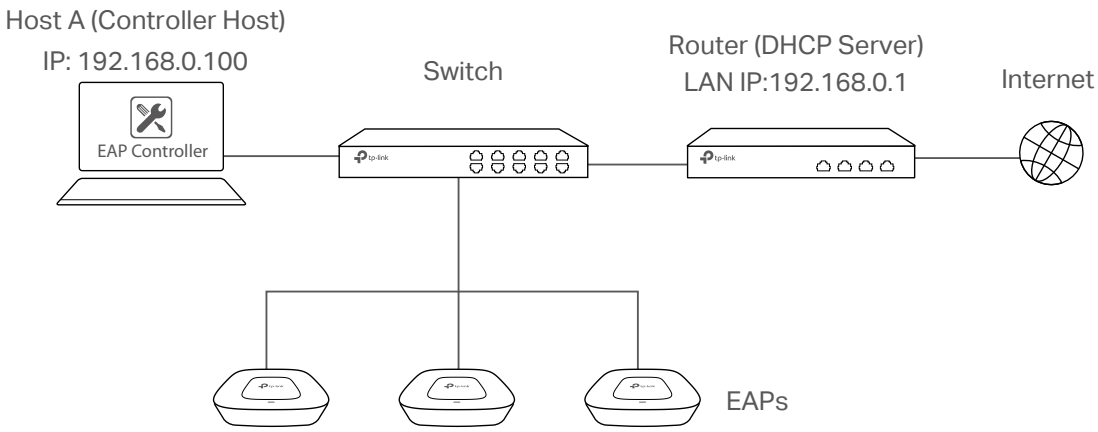
- Monitor the EAPs with the Map.
- Enable Portal function to drive customers' attention to the ads of the supermarket when customers attempt to access the wireless network. The costumers need to use a simple password to pass the authentication.
- Allow the employees of the restaurant to access the network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

Monitor the EAPs with Map

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

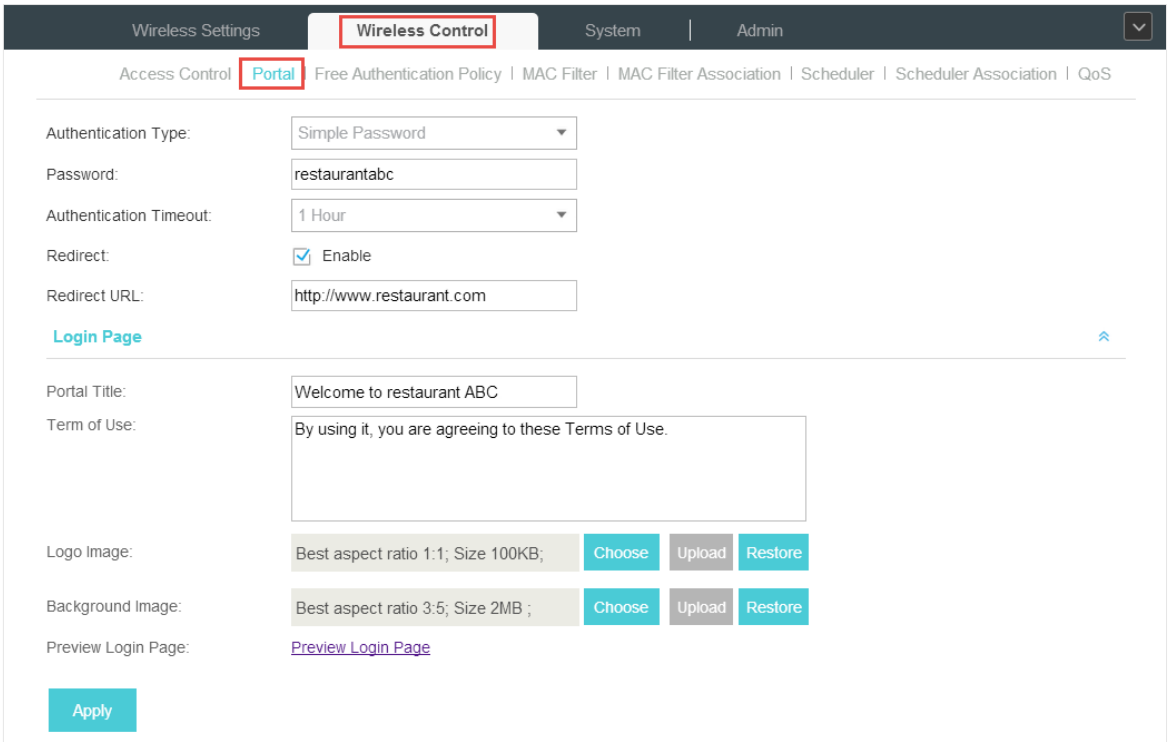
1. Go to the **Map**.
2. Import a local map and set the map scale.
3. Drag the EAPs to the appropriate locations on the map.

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

Configure Portal Authentication

Follow the steps below to configure Portal function.

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



Configure the parameters.

1) Specify a simple password for the guests.

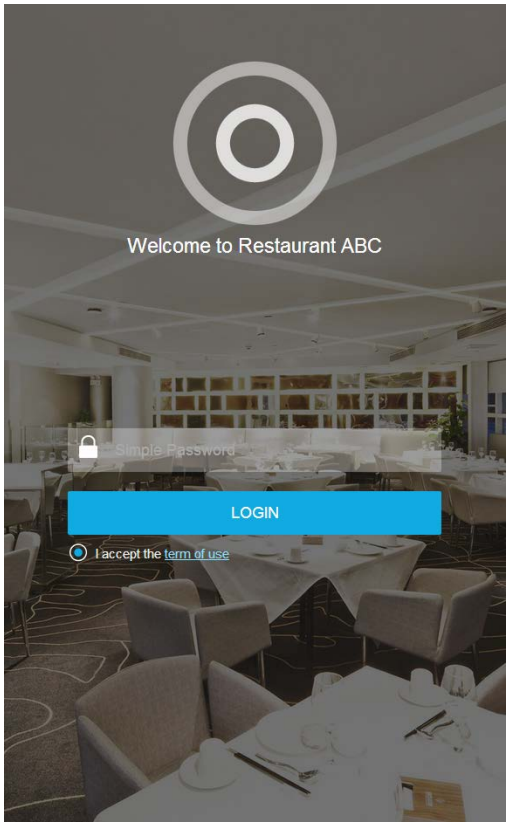
2) Select the **Authentication Timeout**. For example, 1 Hour is suitable for the customers at the restaurant.

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

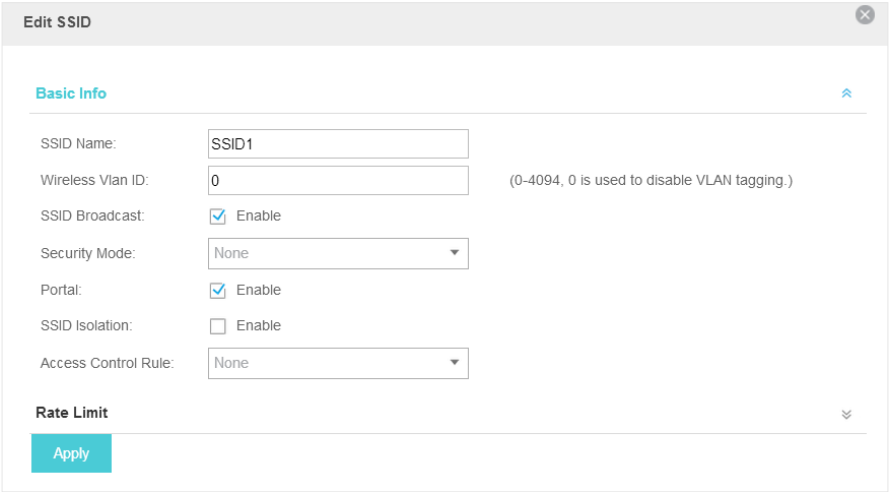
4) Configure the **Login Page**.

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

3. Click **Preview Login Page** and you can preview the login page for the customers.



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



5. Edit the parameters as follows.

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

2) Enable **Portal**.

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

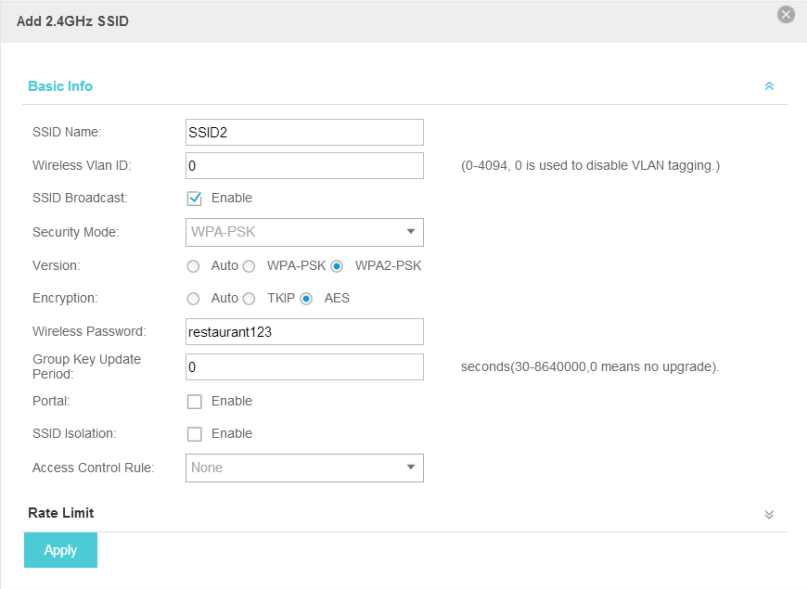
Create a SSID for the Employees

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

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

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

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



Configure the parameters.

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

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

3) Keep the **Portal** disabled for this SSID.

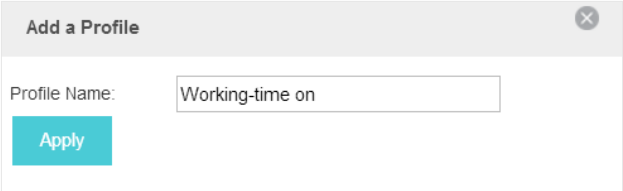
4) Click **Apply** to save the configuration.

Configure Scheduler

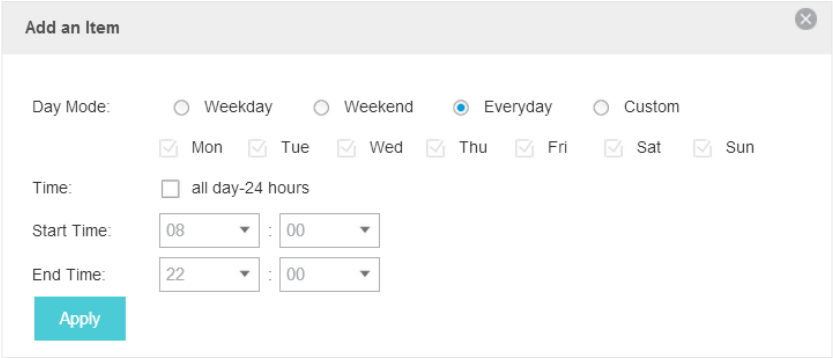
Follow the steps below to schedule the radio to operate only during the working time (from 8:00 to 22:00).

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

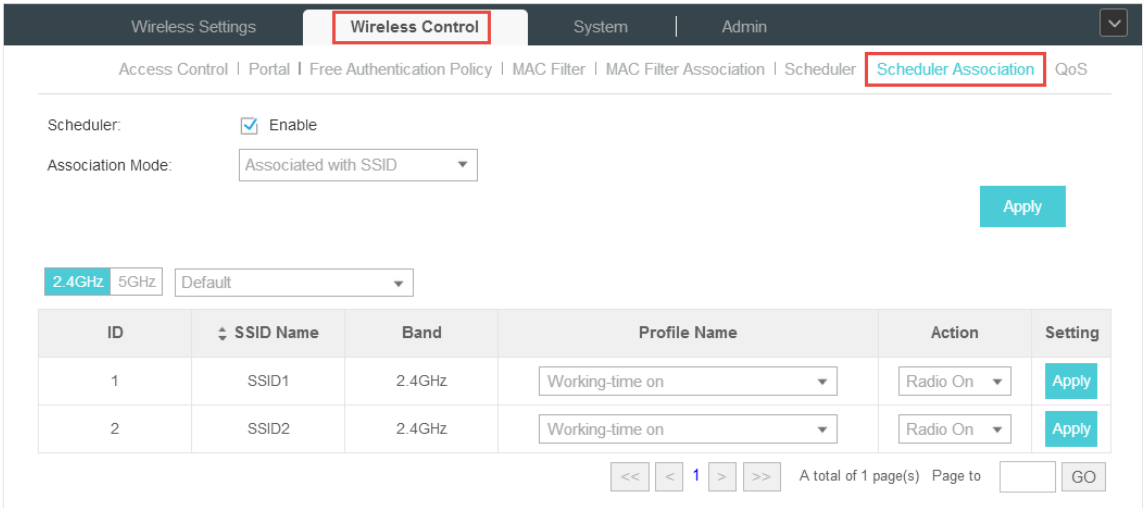
   1) Add a profile.



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



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



   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.